Platform Guide: 4300

MAN-0260-00

Product Version

This manual applies to hardware platform 4300 created by F5 Networks, Inc.

Publication Date

This manual was published on February 29, 2012.

Legal Notices

Copyright

Copyright 2007-2008, F5 Networks, Inc. All rights reserved.

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

F5, F5 Networks, the F5 logo, BIG-IP, 3-DNS, Acopia, Acopia Networks, Application Accelerator, Ask F5, Application Security Manager, ASM, ARX, Data Guard, Enterprise Manager, EM, FirePass, FreedomFabric, Global Traffic Manager, GTM, iControl, Intelligent Browser Referencing, Internet Control Architecture, IP Application Switch, iRules, Link Controller, LC, Local Traffic Manager, LTM, Message Security Module, MSM, NetCelera, OneConnect, Packet Velocity, SSL Accelerator, SYN Check, Traffic Management Operating System, TMOS, TrafficShield, Transparent Data Reduction, uRoam, VIPRION, WANJet, WebAccelerator, and ZoneRunner are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent.

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

VCCI Class A Compliance

Table of Contents

1
Introducing the 4300 Platform

2
Installing the 4300 Platform

3
Operating the LCD Panel

4
Using Additional 4300 Platform Functionality

5
Changing the Fan Tray and Filter

B
Platform-Specific Hazardous Substance Levels, for China

Glossary

Index

1

Introducing the 4300 Platform

- Working with the 4300 platform

- Getting started

- Familiarizing yourself with the 4300 platform

- About this guide

- Finding help and technical support resources

Working with the 4300 platform

The 4300 platform is a powerful appliance designed for medium-to-large enterprises and can support up to 20,000 concurrent users. It works with virtually any browser, operating system, and terminal protocol to provide secure remote access to corporate applications and data.

The 4300 platform is available with two SFP GBICs (LC connector type) and four (10/100/1000) interfaces, as shown in Figure 1.1.

◆ **WARNING**

This platform supports only optics modules provided by F5 Networks.

Figure 1.1 *This is an external view of the 4300 platform*

Getting started

There are several basic tasks you must complete to get the 4300 platform installed and set up.

• Review the hardware requirements.
  For more information about the hardware requirements, read the following sections, *Components provided with the 4300 platform*, following, and *Peripheral hardware that you provide*, on page 1-4.

• Understand the environmental guidelines.
  For more information, see *Environmental requirements*, on page 8-1.

• Familiarize yourself with the 4300 platform hardware.
  For more information, see *Familiarizing yourself with the 4300 platform*, on page 1-5.

- Connect the 4300 platform to the network, and optionally connect the peripheral hardware.
  For more information on mounting the hardware and attaching cables, see *Installing and connecting the hardware*, on page 2-1.

The 4300 platform comes with the hardware that you need for installation. However, you must also provide standard peripheral hardware, such as a serial terminal, if you want to administer the 4300 platform directly.

Components provided with the 4300 platform

When you unpack the 4300 platform, you should make sure that the following components, shown in Figure 1.2, are included:

- Two power cables (only one is shown in Figure 1.2).

- One serial cable

- One failover cable

- Four rack-mounting screws

- One 10" Cat5e Straight Through cable

If you purchased a hardware-based redundant system, you also received one failover cable to connect the two 4300 platforms together (network-based redundant systems do not require a failover cable).

Additionally, a *BIG-IP® Secure Access Manager Getting Started Guide* and a *Regulatory* document are also available when you unpack the 4300 platform. These items are not shown in Figure 1.2, following.

Figure 1.2 *Components included with the 4300 platform*

◆ **Important**

The power cable included with this unit is for exclusive use with this unit and should not be used with other electrical appliances.

Peripheral hardware that you provide

For each 4300 platform in the system, you need to provide the following peripheral hardware:

◆ If you plan to use direct administrative access to the 4300 platform, you need standard output hardware and a serial terminal.

◆ If you want to use the default 4300 platform configuration, you must have an administrative workstation on the same IP network as the 4300 platform.

◆ You also need network hubs, switches, or concentrators to connect to the 4300 platform network interfaces. The devices you select must be compatible with the network interface cards installed in the 4300 platform. The devices can support 10/100 Ethernet or Gigabit Ethernet.

   • Ethernet requires either a 10 Mbps or 100 Mbps hub or switch.

   • Gigabit Ethernet requires a compatible Gigabit Ethernet switch.

◆ You can use a USB drive compatible with the system for installing upgrades and for system recovery. You can perform an upgrade or system recovery with almost any non-CDRW USB drive. Even though most USB CD-ROMS should work, we cannot guarantee compatibility with all makes and models.

If you plan on doing remote administration from your own PC workstation as most users do, we recommend that you have your workstation already in place on the same subnet to which the management interface is connected.
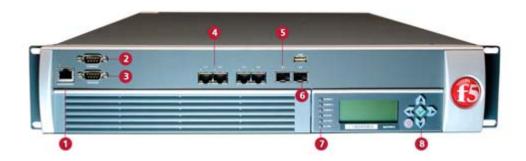
Familiarizing yourself with the 4300 platform

Before you begin to install the 4300 platform, you may want to quickly review the following figures that illustrate the controls and ports on both the front and the back of a 4300 platform.

Using the 4300 platform hardware

You need to be familiar with both the front and back layout of a 4300 platform. Figure 1.3 illustrates the front of a 4300 platform.

The interface on the 4300 platform is labeled, so it should be clear what each port is, no matter which hardware configuration you have purchased.

1. Management interface
2. Console port
3. Hard-wired failover port
4. 10/100/1000 interfaces
5. USB port
6. SFP GBICS
7. Status LEDs
8. LCD control buttons

Figure 1.3 *Front view of the 4300 platform*

If you have physical access to the unit, you can use the front-panel LEDs to assess the condition of the unit. For details about the behavior of the LEDs, see *Understanding LED behavior*, on page 4-1.

Figure 1.4, following, illustrates the back of a 4300 platform.

1. Unused bay
2. Power input panel
   Power 1 (right receptacle)
   Power 2 (left receptacle,
          optional)
3. Access panel

Figure 1.4 *Back view of the 2U 4300 platform*

About this guide

This guide describes the features of the 4300 platform. This guide contains the following information for this platform.

- **Chapter 1, Introducing the 4300 Platform**
  You can familiarize yourself with the platform and review the components provided with the hardware.

- **Chapter 2, Installing the 4300 Platform**
  You can learn how to install the platform.

- **Chapter 3, Operating the LCD Panel**
  You can learn how to understand and use the LCD panel.

- **Chapter 4, Using Additional 4300 Platform Functionality**
  You can learn about additional functionality of the platform.

- **Chapter 5, Changing the Fan Tray and Filter**
  You can learn how to replace a fan tray and filter.

- **Chapter 6, Configuring and Maintaining a FIPS Security Domain**
  You can understand how to set up FIPS configuration for the platform.

- **Chapter 7, Using Lights-Out Management**
  You can learn to manage certain aspects of the operation of the hardware unit.

- **Chapter 8, Working with Environmental Guidelines for the 4300 Platform**
  You can learn about the details of the environmental guidelines for this platform.

- **Chapter 9, Understanding System Airflow**
  You can understand detailed airflow diagrams for each platform.

- **Chapter 10, Reviewing Hardware Specifications**
  You can review details about the hardware specifications for each platform.

Additional information

In addition to this guide, there are other sources of the documentation you can use in order to work with the BIG-IP® system. The information is available in the guides and documents described below. The following printed documentation is included with the BIG-IP® Secure Access Manager system.

- *BIG-IP® Secure Access Manager Getting Started Guide*
  This guide provides you with the basic configuration steps required to get the BIG-IP® Secure Access Manager system up and running in the network. You can find this guide available online at **http://support.f5.com**.

Additionally, you can refer to the following guide for information on how to install, license, and upgrade the BIG-IP® system, as well as for other information that you will need to set up your system properly. We

recommend that you read the ***BIG-IP® Secure Access Manager Getting Started Guide*** to understand the BIG-IP® Secure Access Manager system workflow.

◆ ***BIG-IP® Network and System Management Guide***
This guide contains any information you need to configure and maintain the network and system-related components of the BIG-IP® system. With this guide, you can perform tasks such as configuring VLANs, assigning self IP addresses, creating administrative user accounts, and managing a redundant system.

Stylistic conventions

To help you easily identify and understand important information, our documentation uses the stylistic conventions described following.

Using the solution examples

All examples in this documentation use only private class IP addresses. When you set up the solutions we describe, you must use valid IP addresses suitable to your own network in place of our sample addresses.

Identifying new terms

To help you identify sections where a term is defined, the term itself is shown in bold italic text. For example, a ***virtual server*** is a specific combination of a virtual address and virtual port, associated with a content site that is managed by a Secure Access Manager or other type of host server.

Identifying references to objects, names, and commands

We apply bold text to a variety of items to help you easily pick them out of a block of text. These items include web addresses, IP addresses, utility names, and portions of commands, such as variables and keywords. For example, with the **bigpipe pool <pool_name> show** command, you can specify a specific pool to show by specifying a pool name for the **<pool_name>** variable.

Identifying references to other documents

We use italic text to denote a reference to another document. In references where we provide the name of a book as well as a specific chapter or section in the book, we show the book name in bold, italic text, and the chapter or section name in italic text to help quickly differentiate the two. For example, refer to *Connecting a Management Workstation or Network*, in ***Installation, Licensing, and Upgrades for BIG-IP® Systems***.

Identifying command syntax

We show complete commands in bold Courier text. Note that we do not include the corresponding screen prompt, unless the command is shown in a figure that depicts an entire command line screen. For example, the following command shows the configuration of the specified pool name:

```
bigpipe pool <pool_name> show
```

or

```
b pool <pool_name> show
```

Table 1.1 explains additional special conventions used in command line syntax.

Item in text	Description
\	Indicates that the command continues on the following line, and that users should type the entire command without typing a line break.
< >	Identifies a user-defined parameter. For example, if the command has **<your name>**, type in your name, but do not include the brackets.
I	Separates parts of a command.
[ ]	Indicates that syntax inside the brackets is optional.
...	Indicates that you can type a series of items.
::=	Means **is defined as**. Indicates that an argument is followed by the description of the elements that you can use for the argument.

Table 1.1   *Command line syntax conventions*

Finding help and technical support resources

You can find additional technical documentation and product information in the following locations:

◆ **Welcome screen in the Configuration utility**
The Welcome screen in the Configuration utility contains links to many useful web sites and resources, including:

- The F5 Networks Technical Support web site

- The F5 Solution Center

- The F5 DevCentral web site

- Plug-ins, SNMP MIBs, and SSH clients

◆ **F5 Networks Technical Support web site**
The F5 Networks Technical Support web site, **http://support.f5.com**, provides the latest documentation for the product, including:

- Release notes

- Updates for guides (in PDF form)

- Technical notes

- Answers to frequently asked questions

- The Ask F5^{SM} Knowledge Base

To access this site, you need to register at **http://support.f5.com**.

2

Installing the 4300 Platform

- Installing and connecting the hardware

Installing and connecting the hardware

After you have reviewed the hardware requirements and become familiar with the 4300 platform, as described in *Working with the 4300 platform*, on page 1-1, you can install the unit.

There are two types of mounts available to hold the 4300 platform: the standard front rack mount that comes with the 4300 platform, and an optional rail mount that allows you to slide the unit in and out as needed. The tasks you need to perform to install the 4300 platform hardware differ depending on which type of mount you decide to use:

◆ **Standard front mount**
If you want to install the 4300 platform into the standard front rack mount that comes with the hardware, you need to install the unit into the rack, and then connect the peripheral hardware and the interfaces. For detailed information, see *Installing the 4300 platform hardware*, on page 2-2, and *Connecting the cables and other hardware*, on page 2-5.

◆ **Optional rail mount**
If you want to install the 4300 platform into a rail mount (using the optional rail-mount kit), you need to perform two preliminary steps.

• First, you must remove the standard mount-related hardware (known as *rack-mount ears*) from the unit, because the mount hardware is no longer necessary.

• Second, you must install the optional rail-mount kit.

Once you have completed these tasks, you can then install the unit into the rack and connect the cables and other hardware. For detailed information on installing a rail-mount kit and installing the unit into the rack, see Appendix A, *Installing a 4300 Platform Using an Optional Rail-Mount Kit*. For information on connecting the cables and other hardware, see *Connecting the cables and other hardware*, on page 2-5.

Whether you are using the standard front mount or the optional rail mount, you should read the following general recommendations before proceeding with the installation of the 4300 platform.

General recommendations for mounting a unit in a rack

We recommend that all units have 1U spacing between them when mounted in a rack to allow for a rack mounting shelf, and to provide additional air circulation for cooling the unit.

Although not required, a 1U space between units makes it easier for you to remove the unit from the rack in the event that the unit requires service. A 1U space between units also provides additional cable routing options.

We recommend 100 mm spacing from the front panel of the unit to the rack front or rack door. This provides enough room for you to route the cables without bending them excessively.

◆ **WARNING**

This product is sensitive to electrostatic discharge (ESD). We recommend that when you install or maintain the unit, you use proper ESD grounding procedures and equipment.

◆ **WARNING**

Do not turn on a 4300 platform until the management serial console and/or the management network is connected to the unit.

A shelf or similar device is required to support the unit if a single person is installing the unit. To prevent personal injury or damage to the unit, we recommend that at least two people perform the installation.

Installing the 4300 platform hardware

If you want to use the standard front mount to hold the 4300 platform unit, use the following procedure, *To install the unit into a standard-mount rack*.

If you are using the optional rail mount kit to hold the unit, use the procedures described in Appendix A, *Installing a 4300 Platform Using an Optional Rail-Mount Kit*. The appendix describes how to perform the two preliminary tasks of removing the standard mount hardware from the unit and adding the rail hardware to the unit and the rack. The appendix also describes how to install the unit into the rack.

To install the unit into a standard-mount rack

1. Lift the unit into place.

2. Secure the unit using the four rack-mounting screws that are provided.
   The unit must be securely fastened to the rack to provide adequate stability and to prevent the unit from falling out of the rack.
   Securing the rack with the screws also provides adequate grounding.

If the rack you have does not provide adequate support for the unit, you may need a shelf kit. We recommend that you use a shelf kit created by the rack manufacturer. (Some rack manufacturers provide shelf kits for their racks.)

Figure 2.1 shows the orientation of the 4300 platform and the mounting screws for installation in a standard 19" rack. Figure 2.2 shows the 4300 platform installed in the rack.
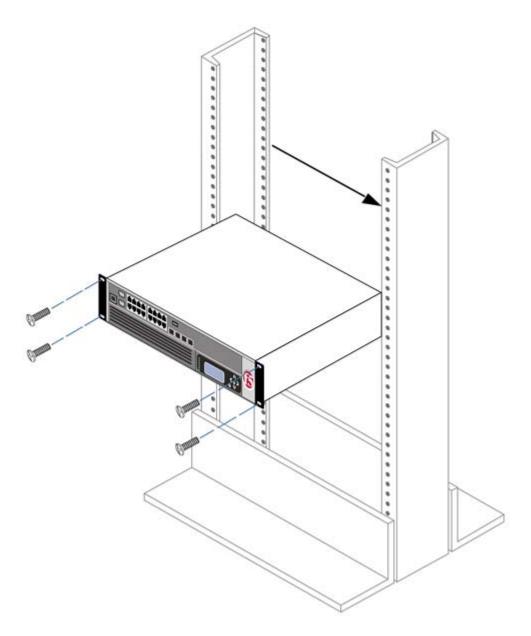
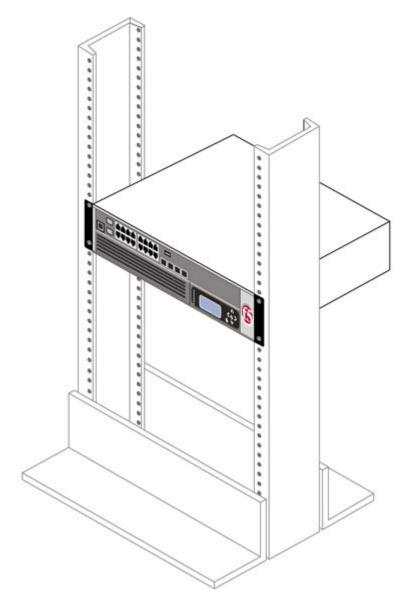*Figure 2.1* *Platform orientation for rack mounting*

Figure 2.2 *Platform installed in a 19" rack*

Regardless of which mount type you use to install the unit, you finish the installation by connecting the cables and other hardware. This procedure is described in *Connecting the cables and other hardware*, following.

Connecting the cables and other hardware

After you have installed the unit into the rack, you need to connect certain cables and other hardware. To perform these tasks, use the following procedure. Note that you use this procedure regardless of the type of mount you installed (front mount or rail mount).

To connect the cables and hardware for input/output

1. Connect the hardware that you have chosen to use for input/output. For details about connecting the system to a management workstation or network, see *Connecting a Management Workstation or Network*, in **Installation, Licensing, and Upgrades for BIG-IP® Systems**.

   • If you are using a serial terminal as the console, connect the serial cable supplied by F5 Networks to the console port (number 2 in Figure 1.3, on page 1-5).

   • If you are using an Ethernet connection, connect a management workstation to the management interface (number 1 in Figure 1.3, on page 1-5).

2. If you have a hardware-based redundant system, connect the failover cable to the failover port on each unit (number 3 in Figure 1.3, on page 1-5).

3. Connect the power cable to the power input panel (number 2 in Figure 1.4, on page 1-6), and then connect it to the power source. If the system has the DC power option, a readily accessible disconnect must be incorporated in the wiring for the installation.

4. Turn on the unit and begin licensing the system. For details about licensing, see *Licensing and Configuring the BIG-IP System*, in **Installation, Licensing, and Upgrades for BIG-IP® Systems**.

3

Operating the LCD Panel

- Introducing the LCD panel

- Using the LCD panel

- Navigating through the LCD menus

Introducing the LCD panel

The liquid crystal display, or LCD panel, provides the ability to control the unit without attaching a serial or network cable. The following menus are available on the LCD panel.

◆ **Information menu**
Use the Information menu to find information about using the LCD panel and its functionality.

◆ **System menu**
Use the System menu to reboot, netboot, or halt the unit. This menu also has options for setting the properties of the management interface (MGMT) and the serial port.

◆ **Screens menu**
Use the Screens menu to set up the informational screens you would like the LCD panel to cycle through. The information screens include system status, statistics, and system alerts.

◆ **Options menu**
Use the Options menu to configure the properties of the LCD panel.

This chapter describes how to use the LCD panel and its menus. It does not describe each function available in each menu.

Figure 3.1 *An example of the LCD panel and control buttons*

Using the LCD panel

You can configure the LCD panel to meet your needs. The following section describes how to perform a number of tasks with the LCD panel:

- Pause on a screen
- Use the LCD menus
- Power up the unit
- Halt the unit
- Power down the unit
- Reboot the unit

Pausing on a screen

Normally, the screens cycle on the LCD panel at a constant rate. However, press the Check button to toggle the LCD panel between Hold and Rotate modes. In Hold mode, a single screen is displayed. The Rotate mode changes the screen displayed on the LCD panel every four seconds.

Using LCD menus

Pressing the **X** button puts the LCD panel in Menu mode. The buttons Left Arrow, Right Arrow, Up Arrow, and Down Arrow are functional only when the LCD panel is in Menu mode.

Powering up the unit

When you want to power on a unit that is shut down, press the Check button to turn the power on.

Halting the unit

We recommend you halt the unit before you power it down or reboot it using the LCD menu options.

To halt the unit

1. Press the **X** button, then use the arrow keys to navigate to the System menu.

2. Press the Check button. Navigate to the Halt menu.

3. Press the Check button. Press the Check button again at the confirmation screen.

4. Wait 30 seconds before powering the machine off or rebooting it.

Powering down the unit

Hold the **X** button for four seconds to power down the unit. We recommend that you halt the system before you power down the system in this manner.

Rebooting the unit

Hold the Check button for four seconds to reboot the unit. You should use this option only after you halt the unit.

Clearing alerts

Press the Check button to clear any alerts on the LCD screen. You must clear any alerts on the screen before you can use the LCD panel.

Navigating through the LCD menus

To use the LCD menus, you must first put the LCD panel in Menu mode. To put the LCD panel in menu mode, press the **X** button.

After you put the LCD panel in menu mode, use the Left Arrow, Right Arrow, Up Arrow, and Down Arrow buttons to select menu options. There are four menu options:

- Information
- System
- Screens
- Options

The following tables describe each LCD menu option.

Information menu

You can use the Information menu to access help pages about using the LCD panel functionality. You can also find more information on what different LED activity means, and on the failover state of the unit in a redundant system. Table 3.1 shows the options available on the Information menu.

Option	Description
How to use the LCD	Displays a vertical scrolling text description on how to use the LCD panel.
Front Panel LEDs	Displays a vertical scrolling text description of what the front panel LEDs mean.
Port Indicators	Displays a vertical scrolling text description of what the lights above the ports mean.
Console and Failover serial port information	Displays a vertical scrolling text description of the console and failover serial ports.

Table 3.1 *The Information menu*

System menu

The System menu provides various options for rebooting, halting, or netbooting the hardware. This menu also provides options for configuring the network on the management interface. Table 3.2 lists the options available in the System menu.

Option	Description
Reboot	Select this option to reboot the unit.
Halt	Select this option to halt the unit.
Netboot	Select this option if you are installing software from a PXE server.
IP address	Type the management interface IP address. You can use only an IPv4 address.
Netmask	Set the netmask for the management interface IP address.
Default route	Type in the default route for the management interface. This route is necessary if you plan to manage the unit from a different subnetwork.
Commit	Select this option to commit your changes.
Serial port	Use this option to change the baud rate of the serial port. The following options are available: 9600 19200 38400 115200

Table 3.2 *The System menu*

Screens menu

You can use the Screens menu options to view various statistics and information about the system. Table 3.3, lists all the general information screens. You can use the Check button to place a check mark next to the name of the screens that you would want to display when the screens cycle.

Option	Description
VersionScreen (Version screen)	Displays the product version information.
InfoScreen (Information screen)	Displays the information screen menu.
DateScreen (Date and Time screen)	Displays the date and time.
MACscreen (MAC addresses screen)	Displays the MAC addresses on the unit.
SysinfoScreen (System information screen)	Displays system information.
TMMCPUScreen (CPU usage)	Displays the CPU usage percentage.
TMMMemoryScreen (Memory usage)	Displays the memory usage.
TMMAuthScreen (Auth requests)	Displays the number of authentication requests being processed.
TMMStatScreen (Statistics)	Displays simple statistics, such as bytes and packets in and out of the system.

Table 3.3 Screens menu

Options menu

You can use the Options menu to adjust the display properties of the LCD panel. Table 3.4 lists the options available on the Options menu.

Option	Description
Heartbeat	Use the Check button to turn on (checked) or off (cleared) the heartbeat displayed on the LCD screen. This heartbeat displays if the SCCP is running on the system. This heartbeat does not affect the failover mechanism of the system.
Contrast	Use the Left and Right arrow keys on the LCD panel to set the contrast of the LCD.
On Brightness	This setting provides the ability to adjust the LCD backlight brightness.
Off Brightness	This setting controls the brightness of the LCD panel when the backlight is off. Use the Left and Right arrow keys to set the brightness of the LCD panel.

Table 3.4 *The Options menu*

4

Using Additional 4300 Platform Functionality

- Understanding LED behavior

- Working with interfaces

Understanding LED behavior

The first part of this chapter describes the LED behavior on the 4300 platform.

LED indicator actions

The behavior, or action, of each of LED indicates the status of the system. The LED indicator actions are defined in Table 4.1.

Action	Description
Off (none)	The LED is not lit and does not display any color.
Solid	The LED is lit and does not blink.
Blinking	The LED turns on and off at a regular frequency.
Intermittent	The LED turns on and off with an irregular frequency and may sometimes appear solid.

Table 4.1 *LED indicator actions*

Standard operating states

When the unit is in a standard operating state, the LEDs behave in a defined manner. The standard operating states are defined in Table 4.2.

System State	Alarm LED	Activity LED	Status LED
Power is off	off/none	off/none	off/none
Standby mode	off/none	green or yellow intermittent	yellow solid
Active mode	off/none	green or yellow intermittent	green solid

Table 4.2 *Standard operating states of the LEDs*

Alert conditions indicated by the Alarm LED

When there is an alert condition on the unit, the Alarm LED behaves in a specific manner, as shown in Table 4.3.

System Situation	Alarm LED behavior
Emergency	The LED blinks red.
Alert or Critical	The LED is lit red.
Error	The LED blinks yellow.
Warning	The LED is lit yellow.

Table 4.3 *LED indicator functions*

Alerts that cause the indicators to change are defined in the **/etc/alertd/alert.conf** and **/config/user_alert.conf** files. You should only edit the **/config/user_alert.conf** file to add new alerts. The **/etc/alertd/alert.conf** file defines standard system alerts.

To configure LED indicators to display node status

1. Display a command-line prompt on the BIG-IP® system.

2. Type the following command:

   ```
   cd /config
   ```

3. Using a text editor, such as **vi** or **pico**, open the file **user_alert.conf**.

4. Add the lines shown in Figure 4.1 to the end of the file.

5. Save the file, and exit the text editor.
   The front panel LEDs now indicate when nodes are marked down.

```
alert BIGIP_MCPD_MCPDERR_POOL_MEMBER_MON_DOWN "Pool member (.*?):(.*?) monitor status
down." {
        snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.10";
                    lcdwarn description="Node down"  priority="1"
}
alert BIGIP_MCPD_MCPDERR_NODE_ADDRESS_MON_DOWN "Node (.*?) monitor status down." {
        snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.12";
                    lcdwarn description="Node address down"  priority="1"
}
alert BIGIP_MCPD_MCPDERR_POOL_MEMBER_MON_UP "Pool member (.*?):(.*?) monitor status
up." {
        snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.11"
}
alert BIGIP_MCPD_MCPDERR_NODE_ADDRESS_MON_UP "Node (.*?) monitor status up." {
        snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.13"
}
```

*Figure 4.1 The **user_alert.conf** file*

Specific status indicated by the LEDs

Some specific conditions are not included in the definition tables in the **/etc/alertd/alert.conf** file. These conditions include:

- Yellow intermittent Activity LED indicator
- Green intermittent Activity LED indicator
- Green solid Status LED indicator

Yellow intermittent Activity LED indicator

A yellow intermittent Activity LED indicates that host traffic is present. Also, while the kernel is loading, the Activity LED indicator flashes yellow intermittently when the disk is accessed. This condition is normal and occurs only during start up.

Green intermittent Activity LED indicator

When the Activity LED indicator flashes green intermittently, it indicates Ethernet traffic leaving the switch subsystem and going to the CPU subsystem. Because internal traffic might cause this indicator to be active, you may see the Activity indicator flicker green even though there is no external client/server traffic.

Green solid Status LED indicator

When the Status LED indicator is solid yellow or green, it indicates that the system is in a Standby state (yellow) or an Active state (green).

Working with interfaces

You can perform configuration tasks such as displaying interface status and settings, setting the media type, and setting the duplex mode using the **bigpipe** command.

When using the **bigpipe** utility, and a command calls for a list of interfaces, the list may consist of one or more interfaces, with multiple interfaces separated by spaces. For example:

```
1.1 1.2 2.1 2.2
```

Displaying status and settings for interfaces

From the command line interface, use the following syntax to display the current status and the settings for all installed interfaces:

```
b interface show
```

Figure 4.2 shows an example of the output you see when you issue this command on an active/standby unit in active mode.

```
interface  speed   pkts   pkts   pkts   pkts   bits   bits errors trunk STP
           Mb/s     in    out    drop   coll    in    out
  1.1 UP  100 HD     0    213      0      0      0  74.2K      0
  1.2 UP  100 HD    20     25      0      0  28.6K  33.9K      0
```

Figure 4.2   *The bigpipe interface show command output*

Use the following syntax to display the current status and the setting for a specific interface:

```
b interface <if_name> show
```

Media type and duplex mode

Properties that you can configure on the interfaces include media type and duplex mode, as shown in Table 4.4.

Interface Properties	Description	Default
media	You may specify a media type or use **auto** for automatic detection.	auto
duplex	Use **auto** for automatic selection.	auto

Table 4.4   *Attributes you can configure for an interface*

Setting the media type

All interfaces on the 4300 platform default to auto-negotiate speed and duplex settings. We recommend that you configure any network equipment that you plan to use with the BIG-IP® system to auto-negotiate speed and duplex settings. If you connect the BIG-IP® system to network devices with forced speed and duplex settings, you must also force the speed and duplex settings of the BIG-IP® system to match the settings of the other network device.

◆ **WARNING**

If the BIG-IP® system is attempting to auto-negotiate interface settings with an interface that has the speed and duplex settings forced, you will experience severe performance degradation.

From the command line interface, use this syntax to set the media type:

```
b interface <if name list> media <media type> | auto
```

The valid media types for this command are:

- 10baseT <duplex>
- 100baseTX <duplex>
- 1000baseFX full
- 1000baseT <duplex>
- 1000baseSX full
- 1000baseLX full
- 10GbaseSR full
- 10GbaseLR full
- 10GbaseER full | auto

To view the valid media types for an interface, type the following command at the prompt:

```
b interface <if name list> media show
```

◆ **Important**

In all Gigabit Ethernet modes, the only valid duplex mode is full duplex.

Setting the duplex mode

You can set duplex mode to full or half duplex. If the media type does not accept the duplex mode setting, a message indicates this. If media type is set to **auto**, or if the interface does not accept the duplex mode setting, the duplex setting is not saved to the **/config/bigip_base.conf** file.

From the command line interface, use this syntax to set the duplex mode:

```
b interface <if_name> duplex  full | half
```

5

Changing the Fan Tray and Filter

- Changing the fan tray and filter

Changing the fan tray and filter

The 4300 platform has a removable fan tray and filter. You can change or replace the fan tray and filter as part of the routine maintenance of the unit, or in the event of a fan failure. The air filter in the 4300 platform is designed to remove airborne contaminants and requires replacement during the life of the product. The fans in the fan tray run constantly while the unit is on. Over time, the fans will wear out, requiring you to replace the fan tray.

◆ **Note**

We recommend that you inspect the fan tray and filter every four months. Replace the fan tray if any of the fans are not functional. Replace the filter when you replace the fan tray.

Replacing the fan tray and filter

You do not need special tools to replace the fan tray and filter. You can perform this maintenance while the unit is running.

However, we recommend that you perform the fan tray and filter replacement only on the standby unit in a redundant system while the unit is powered down. After you install the fan tray and filter in the standby system, power up the unit, then force the active system to fail over and install the fan tray and filter replacement in the other unit of the redundant system.

To replace the fan tray and filter

1. Start by opening the front panel of the unit running in standby mode.

2. The fan tray is held on the chassis by a knurled fastener. Loosen the knurled fastener by turning it counter-clockwise.

3. Pull the old fan tray and filter out of the system.

4. Slide the new fan tray and filter into the fan tray and filter slot. The tray is automatically turned on when you slide the tray completely into the chassis.

5. Tighten the knurled fastener into place by turning it clockwise.

6. Close the front panel of the unit.

◆ **WARNING**

You should not leave the unit running longer than 90 seconds without the fan tray installed.

Figure 5.1 *The removable fan tray*

Figure 5.2 *The removable filter*

Figures 5.1 and 5.2 show examples of the fan and filter tray assembly partially removed from the 4300 platform (your hardware may appear slightly different). You can also replace the filter without replacing the fan tray. This requires that you remove the fan tray, take out the old filter, and insert a new one.

To replace the filter only

1. Start by opening the front panel of the unit running in standby mode.

2. The fan tray is held on the chassis by a knurled fastener. Loosen the knurled fastener by turning it counter-clockwise.

3. Pull the old fan tray and filter out of the system.

4. Slide the old filter out of the fan tray filter slot. Slide the new filter into the filter slot.

5. Push the fan tray and filter back into the system.
   The tray is automatically turned on when you slide the tray completely into the chassis.

6. Tighten the knurled fastener into place by turning it clockwise.

7. Close the front panel of the unit.

6

Configuring and Maintaining a FIPS Security Domain

- Understanding the FIPS implementation

- Installing the BIG-IP system and connecting a serial console

- Creating the FIPS security domain

- Running the Configuration utility

- Running the fipscardsync utility to synchronize the FIPS HSMs

- Generating and managing FIPS keys

- Planning for system recovery

- Recovering FIPS information after a system failure

Understanding the FIPS implementation

The 4300 platform includes the option to install a FIPS hardware security module (HSM). The HSM and the BIG-IP® management software provide FIPS-140 level 2 support by leveraging security keys. Keys are basically codes used within the HSM to prevent hackers from entering the system. This level of support provides the following security benefits.

* Keys are stored in the HSM where they are protected from physical and software attacks.

* Keys can never be extracted in plain text format.

This chapter describes how to configure a redundant system from the factory with one FIPS HSM installed in each unit. To implement a FIPS solution in a BIG-IP® redundant system, you must perform the following tasks.

* Install the BIG-IP® system and connect a serial console.

* Create the FIPS security domain from the console.

* Open the Configuration utility.

* Run the **fipscardsync** utility to synchronize the FIPS HSMs from the console.

Some of these tasks are described in other documents. When a section in this document has tasks described in other documents, it contains links or pointers to the related documentation.

Installing the BIG-IP system and connecting a serial console

The first two tasks that you need to complete when setting up a FIPS configuration on a redundant system are to install the systems and connect a serial console. For details about performing these tasks, refer to the following sections:

* For details about installing the hardware, see *Installing and connecting the hardware*, on page 2-1.

* For information on connecting a serial console, see *Connecting the cables and other hardware*, on page 2-5

After you set up the systems and configure a serial console, you can create the FIPS security domain.

Creating the FIPS security domain

The first task in creating a FIPS security domain is to initialize the FIPS HSM and create a security officer (SO) password. The SO password is required to re-initialize the HSM. When you are configuring a redundant system, you need to initialize the security domain on one unit, and then initialize the card on the peer unit using the same security domain name you used on the first unit.

To create a FIPS security domain, you must perform the following tasks:

*   Initialize the first unit in the redundant system.

*   Initialize the peer system.

◆ **Note**

You can initialize the FIPS HSM and create the security domain before you license the system and create a traffic management configuration.

Initializing the first unit in a redundant system

To initialize the first unit in a redundant system and create a security domain, you must use the **fipsutil** utility. To initialize the HSM and create an SO password, type the following command:

```
fipsutil -f init
```

After the utility starts, you are prompted to create a security officer password, and then confirm the password. After you create a password and confirm it, you are prompted for the security domain name. Remember the security domain name you use. You need the domain name when you initialize the HSM on the peer unit. The domain name cannot be extracted or displayed by the software or hardware once you use it.

After you complete the initialization process on the first unit, you can initialize the peer system.

Initializing the peer system

To initialize the peer unit in the redundant system and add it to the security domain of the first unit, you must use the **fipsutil** utility. Type the following command:

```
fipsutil -f init
```

After the utility starts, you are prompted to create a security officer (SO) password. You can use the SO password that you created on the first unit; however, you are not required to use it.

When you are prompted for the security domain name, you must type the security domain name you created on the first unit.

After you initialize the HSMs in both units, you can log on to each unit and run the Configuration utility.

Running the Configuration utility

After you complete the initialization of the HSMs and create a security domain on the redundant system, you need to run the Configuration utility.

The Configuration utility provides the ability to license the system, configure the management interface, configure failover, and create a base network configuration. After you configure failover and run the **fipscardsync** utility, every time you synchronize the configuration of the redundant system you are synchronizing card and key information for the FIPS security domain. The following section describes how to run the **fipscardsync** utility.

For details about running the Configuration utility and creating a base network configuration, see the *BIG-IP® Quick Start Instructions*. These instructions are included in the BIG-IP® Resource Kit shipped with each unit. You can also access these instructions at **http://support.f5.com**.

Running the fipscardsync utility to synchronize the FIPS HSMs

After you set up the system with the Configuration utility, you can synchronize the FIPS HSMs with the **fipscardsync** utility. Synchronizing the HSMs provides the ability to exchange keys. To run the **fipscardsync** utility, type the following command at the console.

```
fipscardsync peer
```

After you synchronize the HSMs, you can create a traffic management configuration.

The remainder of this chapter describes additional FIPS system maintenance tasks, including:

• Generating and managing FIPS keys

• Planning for system recovery

• Recovering FIPS information after a system failure

Generating and managing FIPS keys

The browser-based Configuration utility provides a key management interface. You can use the Configuration utility to create FIPS keys, convert existing keys to FIPS keys, and import existing keys into the system.

◆ **WARNING**

Once a key is converted to FIPS, the process cannot be reversed.

To create FIPS keys using the Configuration utility

1. On the Main tab of the navigation pane, expand **Local Traffic**, and click **SSL Certificates**.
   This opens the SSL Certificates screen which lists all certificates installed on the Local Traffic Manager system.

2. On the upper-right portion of the screen, click **Create**.
   The New SSL Certificates screen opens.

3. In the **Name** box, type a unique name for the certificate.

4. Using the **Issuer** setting, specify the type of certificate you want to use:

   • For a self-signed certificate, select **Self**.

   • To request a certificate from a CA, select **Certificate Authority**.

5. Configure the **Common Name** setting, and any other settings you want.

6. In the Key Properties section, select the security type **FIPS**, and a key size.

7. Click **Finished**.

To convert existing keys using the Configuration utility

1. On the Main tab of the navigation pane, expand **Local Traffic** and click **SSL Certificates**.
   This opens the SSL Certificates screen which lists all certificates installed on the Local Traffic Manager system.

2. Click a certificate name.
   This displays the properties of that certificate.

3. If you want to see information about the key that is associated with that certificate, click **Key** on the menu bar.
   This displays the type and size of the key.

4. To convert the key to a FIPS key, click the **Convert to FIPS** button.
   The key is converted. Once the key is converted, this process cannot be reversed.

To import existing keys using the Configuration utility

1. On the Main tab of the navigation pane, expand **Local Traffic** and click **SSL Certificates**.
   This displays the list of existing certificates.

2. In the upper right corner of the screen, click **Import**.

3. Select the type of import **Key**.

4. Select the import method (**File** or **Text**).

5. In the **Certificate** box, type the name of the key.
   You can click the **Browse** button and browse for the key and select it.

6. Click **Import**.

   After you import the key, you can convert it to FIPS using the procedure *To convert existing keys using the Configuration utility*, on page 6-4.

Planning for system recovery

You can plan for a system recovery in three different ways.

- You can maintain a redundant system. In the event of a failure, the standby unit becomes active and handles incoming traffic.

- Another option is to configure a third unit with the same configuration, and store it in a safe place.

- A last option, that is not FIPS approved, is to copy the keys to a disk and put the disk in a safe place.

Each of these options is described, following.

Configuring a redundant system

The first option is to maintain a redundant system. In the event of a failure, the standby unit becomes active and handles the incoming traffic. This chapter describes how to create a redundant system configuration as part of the initial configuration. After you configure failover properly, every time you synchronize the configuration of the redundant system, you are synchronizing card and key information for the security domain.

Configuring an additional unit for recovery

For additional system backup, you can take a third unit, fully configure it, add it to the security domain, and synchronize the configurations. Remove the unit from the network and store it in a safe location. If the BIG-IP system in production is damaged or destroyed, you can take the backup unit from storage, and reconstitute the security domain.

Saving keys on a disk

Another possible method for preserving the keys is not FIPS-approved. With this option, you generate your keys in software. Copy the keys to a disk and put the disk in a secure place. Then you can import the keys into the FIPS HSM. If there is a catastrophic system failure, you can use these backup keys to create the security domain. This is not a FIPS-compliant method for backup.

Recovering FIPS information after a system failure

If one unit of a redundant system fails, the failover unit becomes active and maintains FIPS information. However, after you replace the failed unit in a redundant system, you need to restore FIPS information on the replacement unit.

To copy FIPS information from the currently active original system to a new replacement system

1. Ensure that current BIG-IP system software is configured, and install your saved UCS on the new replacement system.
   See the ***BIG-IP® Network and System Management Guide*** on **http://support.f5.com** for information on backup and recovery of a BIG-IP® UCS file.

2. Connect the currently active unit to new replacement unit.

3. On the new replacement unit, run the **fipsutil -f init** command. Ensure that you use the exact same security domain that you specified when you initially set up the currently active unit.

4. On the currently active unit, run the **fipscardsync peer** command. This copies the information in the FIPS module from the currently active unit to the new replacement unit.

   *WARNING: Ensure that you run the **fipscardsync peer** command from the currently active unit. If you run the **fipscardsync peer** command from the new replacement unit, you will lose the original FIPS information.*

5. On the currently active unit, run **configsync** to copy the full configuration to the replacement system.
   The new replacement system is now ready to function as the failover device in a redundant system configuration.

7

Using Lights-Out Management

- • Introducing lights-out management

- • Accessing the command menu

Introducing lights-out management

A lights-out management system is available with the latest F5 Networks platforms. The *lights-out* management system provides the ability to remotely manage certain aspects of the operation of the platform and the BIG-IP® system in the event the traffic management software becomes incapacitated.

The lights-out management system consists of the following elements.

◆ **Switch card control processor (SCCP)**
The hardware that provides the hardware control over the whole unit.

◆ **Host console shell (hostconsh)**
The shell that provides access to the command menu.

◆ **Command menu**
The menu that contains the options for lights-out management.

◆ **Traffic management operating system (TMOS)**
The software that you configure to manage the traffic for your site.

◆ **Out-of-band management commands**
The commands that provide the ability to control various aspects of the system with a series of keystrokes.

The command menu operates independently of the traffic management operating system through the management port, the serial port console, and remotely through the traffic management ports.

• You can use the command menu to reset the unit, even if the BIG-IP traffic management system has locked up.

• You can remotely set a unit to netboot for a software re-install from an ISO image.

• You can get console access to the BIG-IP traffic management system itself, so you can configure the traffic management system from the command line interface.

The lights-out management system and the BIG-IP traffic management system function independently within the hardware unit. Figure 7.1 shows the relationship between the lights-out management system and the traffic management system.

The lights-out management system is accessible through the management interface (number 1 in Figure 7.1) and the console port (number 2 in Figure 7.1). This functionality is independent of the traffic management system (number 3 in Figure 7.1).
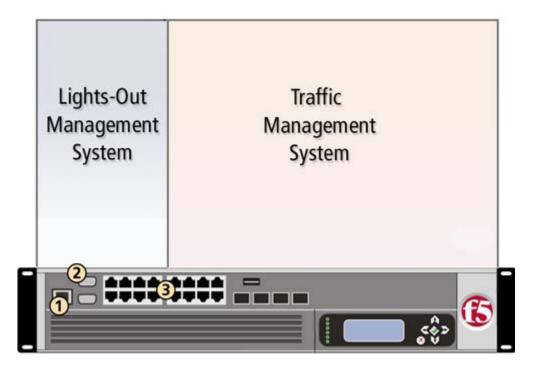
Figure 7.1 *The lights-out management system and the traffic management system interfaces*

Accessing the command menu

You can access the command menu through the host console shell (**hostconsh**) using the front panel serial console, or remotely through SSH. The following section describes how to access the command menu both through the serial console and with an SSH client to the management interface.

Options for accessing the command menu

There are two methods you can use to access the command menu. You can access the menu from the serial console, or from an SSH client to the management interface.

To access the command menu from the serial console

From the serial console connected to the CONSOLE port, type the following key sequence.

```
Esc (
```

The command menu opens.
For details about each option on the command menu, see *Using the command menu*, on page 7-5.

To access the command menu using SSH

Before you can access the command menu using SSH, you must also have an IP address configured for remote lights-out management. For more information, see *Setting up remote lights-out SSH access*, on page 7-4.

1. Open the SSH client on a management workstation connected to the MGMT port on the 4300 platform.

2. Type the following command, where **<IP addr>** is the IP address you configured for the lights-out system.
   The host console shell opens.

   ```
   ssh console@<ip addr>
   ```

3. To open the command menu, type the following key sequence.

   ```
   Esc (
   ```

   For details about each option on the command menu, see *Using the command menu*, on page 7-5.

Setting up remote lights-out SSH access

You can use the command menu to set up remote SSH access to the BIG-IP system. To set up remote access, run the SCCP network Configuration utility to configure an IP address, netmask, and gateway for the lights-out system. You can connect remotely with the SSH client only through the management network connected to the management port (MGMT).

To configure remote SSH lights-out access

1. Log on to the system through the serial console.

2. Type the following key sequence.

   ```
   Esc (
   ```

3. After the command menu opens, type **N**.
   This starts the network configuration utility for the SCCP.

4. Add an IP address, netmask, and gateway on the management network.

Using out-of-band management commands

The host console shell implements a subset of the Microsoft® standard out-of-band management protocol. These commands provide the ability to use a series of key strokes to manage the host processor. Table 7.1 lists the key-stroke options that are available.

Keystroke combination	Result
Esc + R + Esc + r + Esc + R	You can use this sequence during pass-through mode to reboot the platform. We do not recommend using this method to reboot the platform.
Esc (	Brings up the command menu.

Table 7.1 *Out-of-band management key combinations*

Using the command menu

The command menu provides the lights-out management options for the system (see Figure 7.2).

```
1 --- Connect to Host subsystem console
2 --- Select Host subsystem boot mode: boot from local drive
3 --- Select Host subsystem boot mode: netboot from SCCP
4 --- Select Host subsystem boot mode: netboot from external server
5 --- Reboot Host subsystem (sends reboot command)
6 --- Halt   Host subsystem (sends halt command)
7 --- Reset  Host subsystem (issues hardware reset--USE WITH CARE!)
8 --- Reboot SCCP subsystem (issues hardware reset--USE WITH CARE!)
9 --- Halt   SCCP subsystem (issues hardware shutdown--USE WITH CARE!)
B --- SCCP baud rate configurator
L --- SCCP login
N --- SCCP network configurator
```

Figure 7.2 A console view of the host processor console command menu

Each of these options is described in Table 7.2. Note that some of these commands are not intended for use by end users. Table 7.2 also specifies which commands are not recommended for use.

Option	Description
1	Exits the command menu and returns to terminal emulation mode.
2	Configures the BIG-IP® Traffic Management Operating System™ (TMOS™) to boot from the local hard drive or CompactFlash card.
3	Configures the host subsystem to netboot from the host subsystem processor. This option is only for factory testing.
4	Configures the SCCP to netboot the host processor from an external server attached to the management network interface. This option provides the ability to start the PXE installation process remotely.
5	Reboots the host subsystem. In this case, the BIG-IP® Traffic Management Operating System (TMOS) is rebooted.
6	Halts the host subsystem. In this case, the BIG-IP® Traffic Management Operating System (TMOS) is halted.
7	Resets the host subsystem. In this case, the system is reset with a hardware reset.
8	Reboots the switch card control processor (SCCP). This resets the entire unit.

Table 7.2 *Command menu options*

Option	Description
9	Halts the switch card control processor (SCCP). This shuts down the entire unit.
B	Runs the switch card control processor (SCCP) baud rate configuration utility. This utility provides the ability to configure the SCCP serial speed and parameters. This option is only available through the front panel serial console.
L	Presents a login prompt for the switch card control processor (SCCP) subsystem. This subsystem cannot be configured by end users. This option is only available through the front panel serial console.
N	Runs the switch card control processor (SCCP) network configuration utility. This utility provides the ability to reconfigure the IP address, netmask, and default gateway used by the SCCP. If you change these settings, your session is disconnected. This option is only available through the front panel serial console.

◆ Important

*We do not recommend using the reset option, option **7**, under normal circumstances. It does not allow for graceful shutdown of the 4300 platform.*

8

Working with Environmental Guidelines for the 4300 Platform

- Environmental requirements

Environmental requirements

Before you install the 4300 platform, review the following guidelines to make sure that you are installing and using the 4300 platform in the appropriate environment.

General environmental guidelines

A 4300 platform is an industrial network appliance, designed to be mounted in a standard 19-inch rack. To ensure safe installation and operation of the unit:

• Install the rack according to the manufacturer's instructions, and check the rack for stability before placing equipment in it.

• Build and position the rack so that once you install the 4300 platform, the power supply and the vents on both the front and back of the unit remain unobstructed. The 4300 platform must have adequate ventilation around the unit at all times.

• Do not allow the air temperature in the room to exceed 40° C.

• Do not plug the unit into a branch circuit shared by more electronic equipment than the circuit is designed to manage safely at one time.

• This product is sensitive to electrostatic discharge (ESD). We recommend that when you install or maintain the unit you use proper ESD grounding procedures and equipment.

> ⚠ The unit must be connected to Earth ground, and it should have a reliable ground path maintained at all times.
>
> L'appareil doit être mis à la terre et disposer en tout temps d'une voie fiable vers la terre.

> ⚠ This equipment is not intended for operator serviceability. To prevent injury and to preserve the manufacturer's warranty, allow only qualified service personnel to service the equipment.
>
> Cet appareil n'a pas été conçu de sorte à être réparé par l'utilisateur. Pour prévenir les blessures et préserver la garantie du fabricant, l'appareil ne doit être réparé que par du personnel de réparation qualifié.

> ⚠ The controller contains a lithium battery. There is danger of an explosion if you replace the lithium battery incorrectly. We recommend that you replace the battery only with the same type of battery originally installed in the unit, or with an equivalent type recommended by the battery manufacturer. Be sure to discard all used batteries according to the manufacturer's instructions.
>
> Le contrôleur contient une pile au lithium. Le remplacement incorrect de la pile au lithium risque de provoquer une explosion. Nous vous recommandons de remplacer la pile uniquement par un type de pile identique à celui qui était installé à l'origine dans l'appareil ou par un type équivalent recommandé par le fabricant de pile. Assurez-vous de jeter toutes les piles usées conformément aux instructions du fabricant et aux lois locales.

Guidelines for DC-powered equipment

A DC-powered installation must meet the following requirements:

- Install the unit using a 20 Amp external branch circuit protection device.
- For permanently connected equipment, incorporate a readily accessible disconnect in the fixed wiring.
- Use only copper conductors.

> ⚠ Install DC powered equipment only in restricted access areas, such as dedicated equipment rooms, equipment closets, or similar locations.
>
> Installer le matériel alimenté par courant continu uniquement dans des zones à accès réglementé, telles que des salles de matériel, des armoires de matériel ou tout emplacement similaire.

9

Understanding System Airflow

- Understanding system airflow

Understanding system airflow

When you install the 4300 platform into a rack, it is important to understand the unit's airflow direction to ensure proper cooling.

Airflow for the 4300 platform

The 4300 platform employs a positive pressure fan system, in which cold air outside the unit is blown into the platform. The airflow shown exiting the rear of the platform is from the power supply, which in this platform is located in the front of the unit.

Figure 9.1 illustrates the airflow pattern for the 4300 platform.

Figure 9.1 *Airflow in the 4300 platform (top view)*

10

Reviewing Hardware Specifications

- Reviewing hardware specifications

- 4300 specifications

- Additional acoustic, airflow, and altitude specifications

Reviewing hardware specifications

The following table contains general information about the 4300 platform.

Item	Specification
Server/Node Operating System Compatibility	Load balancing of any TCP/IP OS, including Windows NT, Windows 95, all UNIX platforms, and Mac/OS
Internet/Intranet Protocol Support	All TCP services, UDP, SIP, and SSL; nearly all IP-based protocols
Administrative Environment Support	DNS proxy, SMTP, SSH, SNMP, dynamic/static network monitoring, scheduled batch job processing, system status reports, and alarms event notification
Network Management & Monitoring	Secure SSL browser-based interface, remote encrypted login and file transfer using SSH monitor, network monitoring utilities and additional contributed software; SNMP gets and traps, iControl API using CORBA & SOAP/XML
Dynamic Content Support	ASP (active server pages), VB (Visual Basic script), ActiveX, JAVA,VRML, CGI, Cool Talk, Net Meeting, Real Audio, Real Video, Netshow, Quick Time, PointCast, any HTTP encapsulated data
Device Redundancy	Watchdog timer, fail-safe cable (primary & secondary)
SFP hot swap	These devices support hot swap of the SFP modules
Web Server Application Compatibility	Any IP-based web or application server
Routing Protocols	RIP, OSPF, and BGP with optional ZebOS Advanced Routing Modules
Operating Temperature	41° to 104° F (5° to 40° C)
Relative Humidity	20 to 90% @ 40º C
Safety Agency Approval	UL 60950 (UL1950-3) CSA-C22.2 No. 60950-00 (Bi-national standard with UL 60950) CB TEST CERTIFICATION TO IEC 950 EN 60950
Electromagnetic Emissions Certifications	EN55022 1998 Class A EN55024 1998 Class A FCC Part 15B Class A VCCI Class A
Non-operational specification	Temperature -40º to 149º F (-40º to 65º C) Humidity 10 to 95% at 40º non-condensing

Table 10.1 *General information about the 4300 platform*

4300 specifications

The specifications in Table 10.2 apply to only the 4300 platform.

Item	Specification
Dimensions	3.5"H x 17.5"W x 23.5"D (per unit) 2U industry standard rack-mount chassis
Weight	43 lbs. (dual power) per unit
Processor	Dual Opteron 2.2GHz
Power Supply	Dual power supplies
Network Interface	4 x 10/100/1000 2 x Fiber Gigabit Ethernet interfaces (SFP GBIC) 1000BASE-LX - 850nm SFP or 1310nm) (LC Connector) The 1310nm SFP is expansive and must be ordered separately 1 x 10/100 Ethernet Management port
Hard Drive Capacity	160 Gigabyte hard drive
RAM	8 GB
Power supply	Dual 475W 90/240 +/- 10% VAC AUTO Switching
Typical power consumption	275W
Heat generated	939 BTU/hour

Table 10.2 The 4300 platform specifications

◆ **Important**

Specifications are subject to change without notification.

Additional acoustic, airflow, and altitude specifications

This section describes additional specifications such as acoustic levels, airflow movement, and operational altitude for the 4300 platform.

	Detail	Units	1500	3400	4300	6400/6800
Acoustic [1]						
	Front face	db	57	58	65	65
	Left face	db	61	59	64	64
	Right face	db	58	65	68	68
	Rear face	db	59	63	65	65
Altitude [2]						
	Operational	Feet	5905	5905	5905	5905
	Non-operational	Feet	40000	40000	40000	40000
Airflow						
	Entire chassis	cfm	32.1	52.6	117.6	117.6

Table 10.3 *Acoustic, altitude, and airflow specifications*

[1] All measurements taken at 1 meter - A-weighting

[2] Per BELCORE GR-63-CORE, section 4.1.3. 60m (197ft) below sea level to 1800m (5905ft) above sea level.

A

Installing a 4300 Platform Using an Optional Rail-Mount Kit

• Installing the optional rail-mount kit

Installing the optional rail-mount kit

When you received your 4300 platform, the unit included rack-mount ears, suited for a standard type of mount. With rack-mount ears, the unit is bolted directly to the rack.

As an option, you can use an alternative type of mount, called a *rail mount*, which allows you to slide the unit in and out of the rack at will. To install this rail-mount kit and install the unit into the rack, you need to perform the following tasks:

- Remove standard mount hardware from the unit

- Install the rail-mount kit hardware

- Install the unit into the rack

- Connect cables and other hardware

To perform these tasks, follow the instructions in the following sections.

Removing standard mount hardware from the unit

The first step in installing a rail-mount kit is to remove the rack-mount ears from the unit itself. Commonly referred to as rack-mount ears, this hardware must be removed before you can install a rail-mount kit.

Figure A.1 shows one of the rack-mount ears on a 4300 platform.

Figure A.1 *A rack-mount ear on a 4300 platform*

Figure A.2 shows the 4300 platform after you have removed the rack-mount ear.

Figure A.2 *A 4300 platform with both rack-mount ears removed*

To remove the rack-mount ears from the unit

To remove the rack-mount ears from the unit, locate the four screws that hold the rack-mount ears to the unit and unscrew them. You must do this for both rack-mount ears, one on either side of the unit. Save the screws you removed for the next procedure.

Installing the kit hardware

After you have removed the rack-mount ears from the unit, you must install the rail-mount kit. The rail-mount kit consists of these parts:

• Two inner rails that you attach to either side of the unit. Once the kit is installed, these inner rails slide into the outer rails that you install onto the rack.

• Two stops that you attach to either side of the unit.

• Two outer rails that you attach to the rack. The inner rails that you install on the sides of the unit will slide into these outer rails.

• Four optional brackets and screws for use on square-holed racks.

Attaching the inner rails and stops

The first task in installing the optional rail-mount kit is to attach an inner rail and a stop to each side of the unit. Figure A.3 shows the unit with an inner rail and stop attached to one side.

Figure A.3 *An inner rail with stop installed*

To attach the inner rails and stops to the unit

1. Attach an inner rail to each side of the unit, as shown in Figure A.3, using the four screws that you removed from each rack-mount ear. Note that each side requires four screws.

2. Attach a stop to each side of the unit, near the front, as shown in Figure A.3, using the screws provided in the kit.

Attaching the outer rails

Once you have installed the inner rails and stops to the unit, you can attach the two outer rails to the rack. One outer rail is made specifically for the left side of the rack, while the other outer rail is made specifically for the right side of the rack.

Each outer rail includes a bracket on the front, with a square hole and a round hole. Figure A.4 shows a bracket with the square and the round holes.

Figure A.4 *Outer rail and attached bracket*

If the rack is a round-holed rack, use your own standard rack screws to attach the rail and bracket directly to the rack.

If the rack is a square-holed rack, you must use the additional, separate brackets included in the kit to attach the rail and bracket to the rack.

To attach the outer rails to the rack

1. Find the upper rail that corresponds to the side of the rack onto which you are installing the rail.

2. Attach the outer rail and bracket onto the rack as shown in Figure A.5.
    Note the following:

    •   If the rack is a round-holed rack, use standard rack screws.

    •   If the rack is a square-holed rack, hang one of the separate brackets provided with the kit onto each end of an outer rail, and then use the screws provided to attach each rail onto the rack. To accomplish this task, you will use a total of four separate brackets (two per rail), and eight screws (two per bracket).

Figure A.5 shows a rack with an outer rail attached.

Figure A.5 *Outer rail with attached bracket installed*

Once the inner and outer rails are installed, you can easily install the unit into the rack.

Installing the unit into a rail-mount rack

Use the following procedure to install the unit into the rail-mount rack.

To install the unit into the rack

1. Slide the unit into the rack, fitting the inner rails of the unit to the outer rails of the rack.

2. On each side of the unit, screw a nut into the stop that you installed on the unit.

Connecting cables and other hardware

After you have installed the unit into the rack, you need to connect certain cables and other hardware. To perform these tasks, see the appropriate section in Chapter 2, *Installing the 4300 Platform*.

B

Platform-Specific Hazardous Substance Levels, for China

- 4300 platform

4300 platform

This table lists hazardous substances controlled by China, and shows how the F5 Networks® 4300 platform components conform to the standards.

4300 平台危害物质表

4300 Platform Hazardous Substance Table

部件名称 Part Name	有毒有害物质 Hazardous Substance					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	铬 6+ (Cr⁶⁺)	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
金属部件 Metal Parts	o	o	o	o	o	o
交换机 Switchboard	X	o	o	o	o	o
电源 Power Supplies	X	o	o	o	o	o
可移动的卡片 Removable Cards	X	o	o	o	o	o
主板 Motherboard	X	o	o	o	o	o
排热器部件 Heatsink Assemblies	o	o	o	o	o	o
硬盘 Hard Drives	X	o	o	o	o	o
风扇装置 Fan Assembly	o	o	o	o	o	o

o: 表示该有毒有害物质在该部件所有均质材料中的含量均在SJ/T 11363-2006标准规定的限量要求以下
Expresses that this hazardous substance is below the specified limits as described in SJ/T 11363-2006.

x: 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T 11363-2006标准规定的限量要求
（企业可在此处，根据实际情况对上表中打"×"的技术原因进行进一步说明）
Expresses that this hazardous substance is above the specified limits as described in SJ/T 11363-2006.

除非另外特别的标注,此标志为针对所涉及产品的环保使用期标志. 某些零部件会有一个不同的环保使用期(例如,电池单元模块)贴在其产品上.

此环保使用期限只适用于产品是在产品手册中所规定的条件下工作.

The Environmentally Friendly Use Period (EFUP) for all enclosed products and their parts are per the symbol shown here, unless otherwise marked. Certain parts may have a different EFUP (for example, battery modules) and so are marked to reflect such. The Environmentally Friendly Use Period is valid only when the product is operated under the conditions defined in the product

Glossary

ASIC

An ASIC is an application-specific integrated circuit.

bigpipe

The **bigpipe** utility provides command line access to the BIG-IP® software.

Configuration utility

The Configuration utility is the browser-based application that you use to configure the software.

DNS

DNS stands for Domain Name System. It is a service that translates domain names into IP addresses. For example, the domain name **www.sample.com** might translate to **101.102.103.104**.

FIPS

FIPS stands for Federal Information Processing Standards. These are publicly announced standards developed by the US. Federal government for use by all (non-military) government agencies and by government contractors. The BIG-IP system can be configured with FIPS 140-encryption hardware, which stores certificates and private keys in the FIPS hardware.

LCD

LCD stands for liquid crystal display. An LCD panel is available on the front of the 4300 platform. You can use the LCD panel and its associated controls to configure the management port on the unit and view basic statistics.

LED

LED stands for light-emitting diode. An LED indicator is available on the front of the 4300 platform. You can use the LED to monitor any alert conditions occurring on your unit.

NIC

NIC stands for Network Interface Card. It is an expansion board used to connect a computer to a network.

port

A port is represented by a number that is associated with a specific service supported by a host. Refer to the Services and Port Index for a list of port numbers and corresponding services.

PXE

PXE stands for Preboot Execution Environment. It is used to boot computers using a network interface independently of available data storage devices such as hard disks, or installed operating systems.

SCCP

SCCP stands for Signaling Connection Control Part. It is a routing protocol used in Layer 4, and provides end-to-end routing for TCA messages to their proper database.

SFP GBIC

SFP GBIC stands for small form factor pluggable (SFP) gigabit interface converter (GBIC).

SSH

SSH is a protocol for secure remote login and other secure network services over a non-secure network.

SSL

SSL stands for Secure Sockets Layer. It is a protocol that uses a public key to encrypt data transmitted through the Internet over an SSL connection. URLs using an SSL connection start with **HTTPS:** instead of **HTTP:**.

subnetwork

The portion of a network that shares a common address component is called a subnetwork. For instance, on TCP/IP networks, a subnetwork is all devices whose IP addresses have the same prefix segment.

terminal emulator

A terminal emulator is a program that mimics a terminal.

virtual server

Virtual servers are a specific combination of virtual address and virtual port, associated with a content site that is managed by BIG-IP® system or other type of host server.

Index