Blue Coat® Systems
SG200 Series

Installation Guide

Version: SGOS 4.2.x and 5.1.x

Blue✭Coat®

Contact Information

Blue Coat Systems Inc.
420 North Mary Ave
Sunnyvale, CA 94085-4121

http://www.bluecoat.com/support/index.html

bcs.info@bluecoat.com

support@bluecoat.com

http://www.bluecoat.com

Note This equipment has been tested and found to comply with the limits for a Class A Digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, might cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the users are required to correct the interference at their own expense.

Important: **Follow all warnings and instructions marked on the product and included in this manual.**

Contents

Appendix B: Regulatory Statements

Index

Chapter 1: The SG200 Series

This *Installation Guide* provides general instructions for installing, configuring, and using the SG200.

Once you have completed the first-time configuration of the SG200 and have logged in, you must do the following:

*   Upgrade the SG200 software by downloading the latest patch release (available at *http://download.bluecoat.com*).

*   Fully configure the appliance.

    To configure the SG200, you will need to download the *Blue Coat ProxySG Configuration and Management Guide Suite*, (the CMG) available on the Blue Coat Web site at www.bluecoat.com. (Look for *WebPower Login* under *Support*.)

    This site also has the latest support bulletins and technical notes.

If you log on to the SG200 using an Internet browser (see *Section E: "Logging on to the SG200* on page 37), you can access the *Blue Coat ProxySG Configuration and Management Guide Suite* by clicking the Help button on any screen in the Management Console, the SG200 user interface.

This chapter explains how to unpack the SG200, install it on the wall or in an equipment rack, and make all necessary connections.

Unpacking the SG200

The SG200 is shipped fully assembled. When you receive and unpack the unit, verify that the package contains the following items:

*   SG200 Series Appliance
*   *Quick Start Guide*
*   Power supply adapter
*   Skid-proof rubber pads (4)
*   Rack-mounting ear brackets (2) and screws (6)

*   License and warranty
*   Crossover cable
*   AC power cable
*   Wall-mounting bracket with anchors (2) and screws (2)
*   Jumper (for pass-through card removal only—see *"Removing the Pass-Through Card"* on page 47 for information)

Important: **This product is intended for operation and servicing only by appropriately trained technical personnel.**

Dieses Produkt wird für Betrieb vorgehabt und wird nur durch passend ausgebildeten technisches Personal gewartet.

The SG200 Appliance

The Front-Panel LEDs
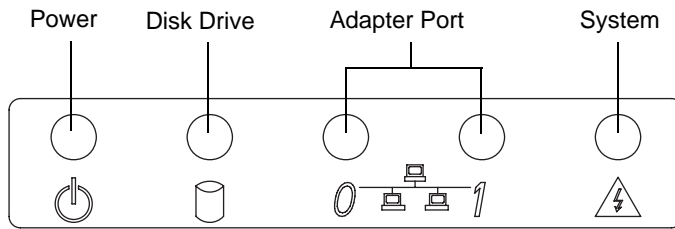
Figure 1-1: Front-Panel LEDs

Power LED

- **No color**: the SG200 is powered off or non-functional
- **Solid Amber**: the SG200 is powered on but unable to perform tasks (such as while it boots up)
- **Flashing Green to Amber**: the SG200 is powered on but is not configured
- **Green**: the SG200 is powered on and at least minimally configured

Disk Drive LED

- **Off**: no disk activity
- **Green**: at least one disk is being accessed (can also indicate compact-flash drive access)

Adapter Port LEDs (Network Adapter Ports 0 and 1)

- **Off**: no link
- **Green**: link
- **Flashing Green to Amber**: link and network activity

System

- **Off**: nothing to report (SG200 is not powered on)
- **Green**: SG200 is healthy
- **Amber**: SG200 is unhealthy, but not critically so
- **Flashing Green to Amber**: Indicates a critical system warning—the SG200 requires immediate attention. See *"The System LED Indicates Unhealthy Status"* on page 43 for information about locating the source of an unhealthy System LED reading.

The Back of the SG200
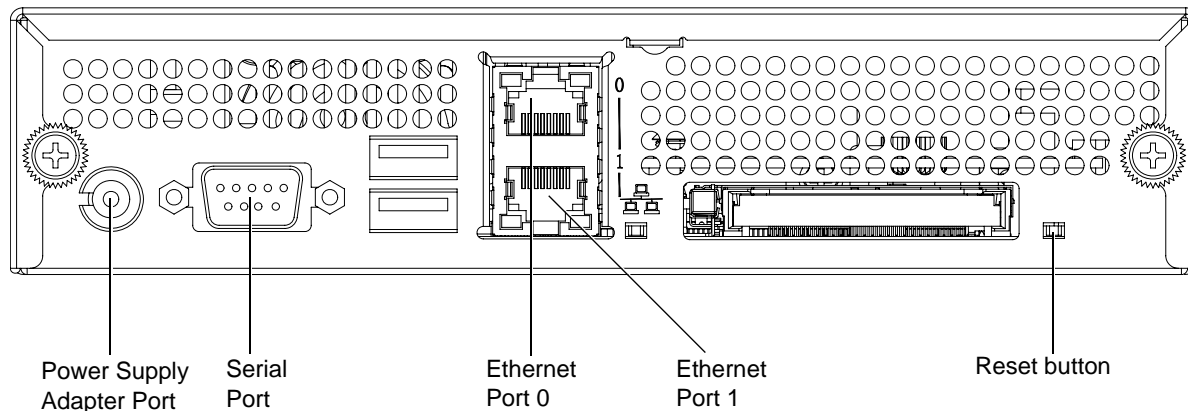
Figure 1-2: Components on the Back of the SG200

Power Supply Adapter Port

Connects to the power supply adapter. Connecting a power cable to the power supply adapter and to an electrical outlet powers on the SG200.

Serial Port

Connects to a PC, serial terminal, or standalone serial console box. Use this port to configure or maintain the SG200 using the command line interface (CLI).

Ethernet Adapter Ports 0 and 1

Two full-duplex, auto-sensing Ethernet network adapters supporting 10/100 Base-T connections.

Reset Button

Restores the appliance to its factory defaults. All configurations are lost when you reset the appliance.

Installing the SG200

There are three methods of installing the SG200 Appliance—placing it on a shelf or tabletop, mounting it on a wall, or mounting it in an equipment rack.

Placing the SG200 on a Shelf or Tabletop

For shelf or tabletop use, affix the four skid-proof rubber pads to the underside of the SG200.

Mounting the SG200 on a Wall

To mount the SG200 vertically on a wall, use the wall-mounting bracket, anchors, and screws; you also need a drill and a Phillips screwdriver.

1   Use the holes on the wall-mounting bracket to mark the positions on the wall for the two anchors; drill holes in the wall just large enough to fit each anchor.

2   Line up the holes on the wall-mounting bracket with the anchors. Use a Phillips screwdriver to secure the bracket to the wall using the wall-mount screws.
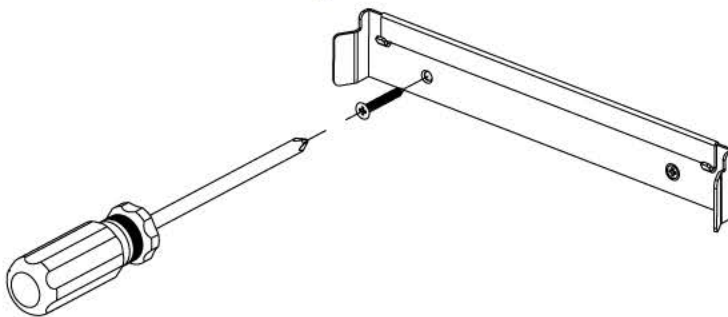
Figure 1-3:   Secure the Wall-Mount Bracket to the Wall

3   Locate the two notches on the underside of the SG200, near the front; an arrow on each side of the SG200 points to each notch.

4   Mount the SG200 on the wall-mount bracket by inserting the notches on the SG200 into the hooks on the bracket and pushing down slightly to lock the appliance into place.
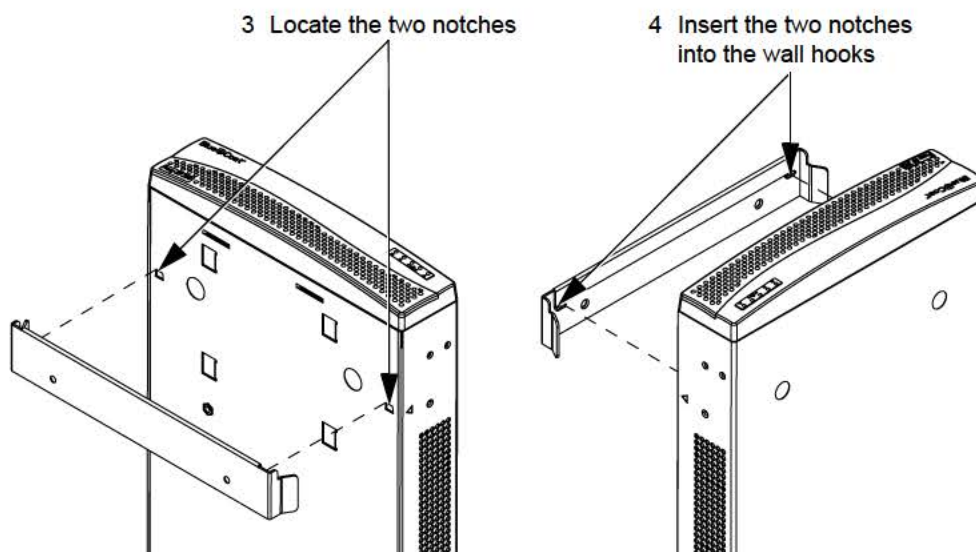
Figure 1-4:   Secure the Wall-Mount Bracket to the Wall

Mounting the SG200 in an Equipment Rack

To mount the SG200 horizontally into an equipment rack, use the rack-mounting brackets and screws; you also need a Phillips screwdriver.

1 Use a Phillips screwdriver to attach the brackets to the SG200; use three screws on each side, as shown in Figure 1-5.
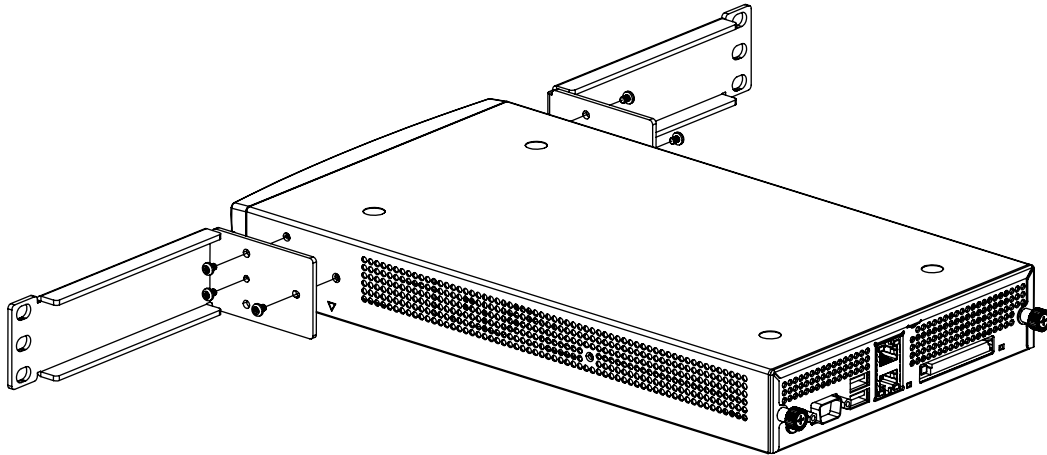
Figure 1-5:   Attach the Brackets to the SG200

Important: **Ensure that the SG200 is fully supported when mounting it in the equipment rack: do not allow the brackets to support the SG200 until they are securely placed.**

---

2 While fully supporting the weight of the SG200, mount the brackets onto the equipment rack using three equipment rack screws on each side (use the screws provided by the rack manufacturer).
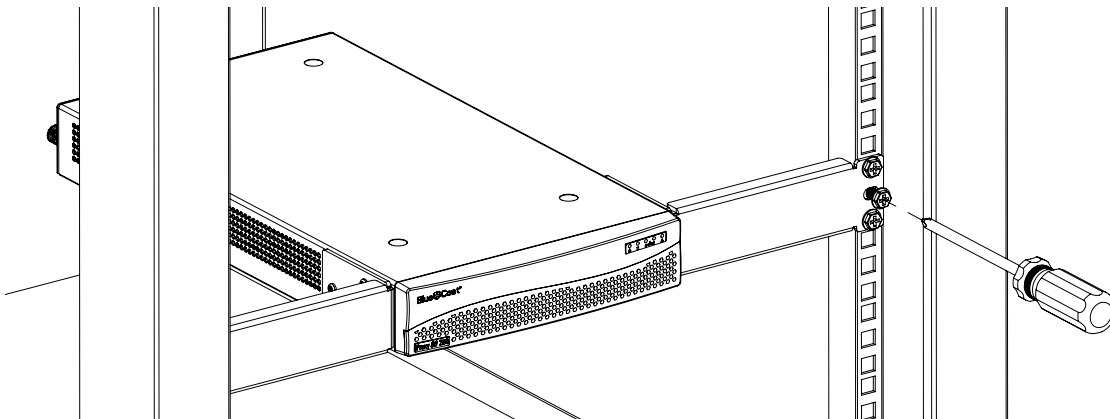
Figure 1-6:   Secure the SG200 to the Equipment Rack

Powering on the SG200

Power on the SG200 by plugging in the power supply adapter and power cable.

1 Plug the power supply adapter into the SG200, ensuring that the barrel of the power supply adapter is fully inserted into the SG200.

2 Plug one end of the power cable into the power supply adapter.

Plug the power supply adapter into the SG200

Plug the power cable into the power supply adapter
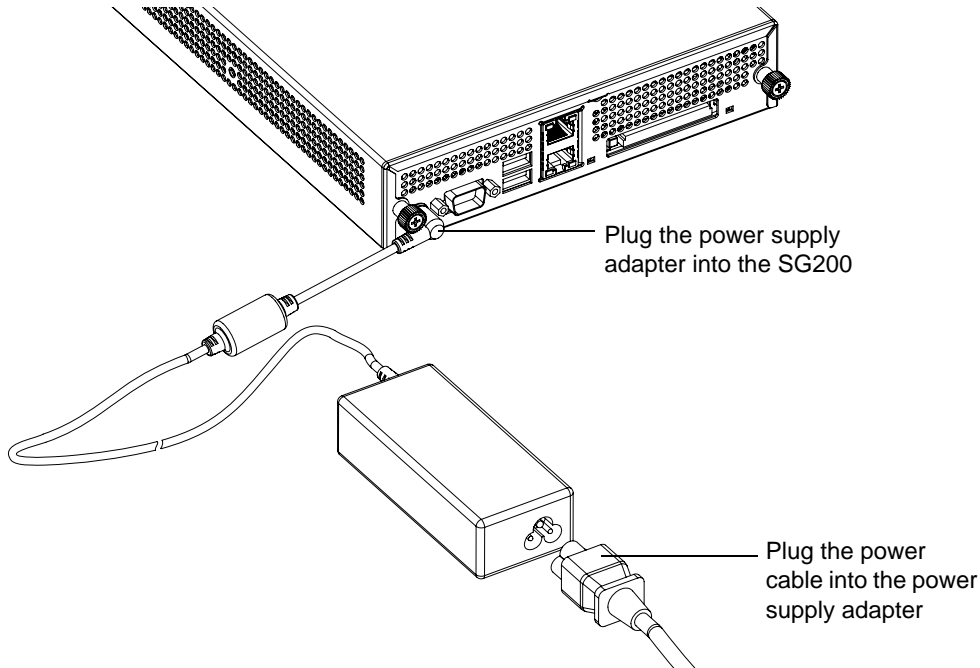
Figure 1-7:   Plug in the Power Adapter and Power Cable

3 Plug the other end of the power cable into a power outlet.

> *Important:* **The use of a wall-socket adapter is not recommended. Country-specific power cables are required to maintain product safety compliance and the warranty.**

The SG200 powers on and the operating system boots up. While the SG200 is booting up (approximately one minute), the Power LED on the front panel (the left-most LED) glows solid amber.

4 After the SG200 boots up, verify that the Power LED behaves as described below:

Configuration Status	Power LED Activity
Not completed	Flashing green and amber
Completed	Solid green
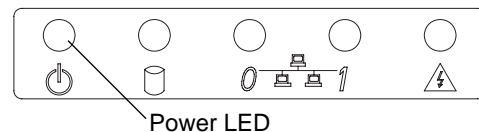
Power LED

If the Power LED is solid green after booting up, an initial configuration has already been performed. If you did not perform an initial configuration, restore the appliance to its factory defaults to restart the initial configuration (see *"Resetting the SG200 to Its Factory Defaults"* on page 46).

Chapter 2: First-Time Configuration

Overview

First-time-only configuration involves setting the basic network parameters and ensuring that the SG200 and software are working properly. To do this, use one of the following methods:

- Connect the SG200 to a PC and configure it using a Web browser, then relocate the SG200 to its final destination in the network.

  Use this method if you want to use one person to configure the SG200 and you do not want to use a standalone serial terminal or terminal emulator. This person must be in the same location as the SG200. See *Section A: "Configuring the SG200 with a Web Browser* on page 12.

- Place the SG200 into its final destination in the network, then configure it using either a direct serial port connection or a remote Web browser setup.

  Use this method under the following circumstances:

  ❐ You want to place the SG200 directly into the network and use a standalone serial terminal or terminal emulator to configure it. See *Section C: "Initial Configuration Using a Direct Serial Port Connection* on page 21.

  ❐ You want to use two people to configure the appliance—one who enters the configuration parameters from a remote location and another who places the SG200 into the network and finalizes the configuration by clicking a generated URL. See *Section D: "Configuring the SG200 from a Remote Location* on page 32.

After first-time configuration is complete, log on to the SG200 and use the command-line interface (CLI) or Management Console to fully configure the system. See *Section E: "Logging on to the SG200* on page 37 and refer to the *Blue Coat ProxySG Configuration and Management Guide Suite* for information on how to fully configure the software. Download this manual from the Blue Coat Web site at: www.bluecoat.com.

Section A: Configuring the SG200 with a Web Browser

Use the instructions in this section to configure the SG200 by first connecting it directly to a PC and then using the PC's Web browser to perform an initial configuration. After the SG200 is configured, relocate it into the network.

Connecting the SG200 to a PC

To configure the SG200 with a Web browser, you must connect the SG200 to your PC, complete the initial configuration, and then relocate the SG200 into the network.

If you plan to complete the initial configuration of the SG200 using a direct serial port connection (see *Section C: "Initial Configuration Using a Direct Serial Port Connection* on page 21), skip the procedure below and place the SG200 directly into your network (see *Section B: "Placing the SG200 into the Network* on page 20). Also skip this section if you plan to enter the configuration parameters from a remote location (see *Section D: "Configuring the SG200 from a Remote Location* on page 32).

To Connect the SG200 to a PC:

1 Unplug the Ethernet cable from your PC. Keep the other end of the cable connected to your network.

2 Plug the Ethernet cable that you removed from your PC into one of the Ethernet ports on the SG200. Keep the other end of the cable connected to your network.

3 Connect the crossover Ethernet cable by plugging one end into the PC's Ethernet port and the other end into the empty Ethernet port on the SG200.
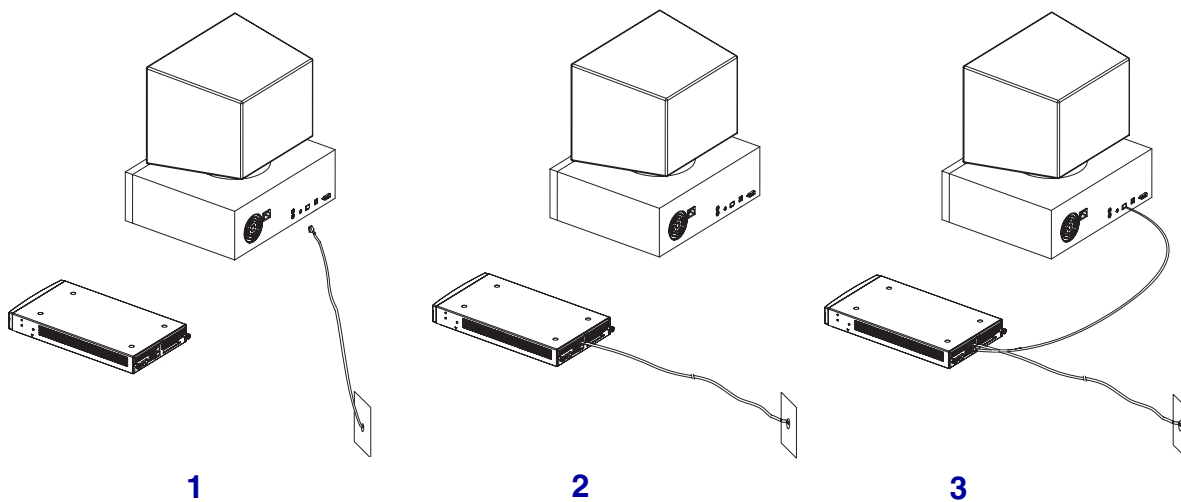
Figure 2-1:   Connect the Cables

4 Verify that the network link is established by checking the network connection LEDs at the back of the SG200. If the network connection is functioning, the left-hand LED on each connection glows green.

4 Verify that these LEDs are green
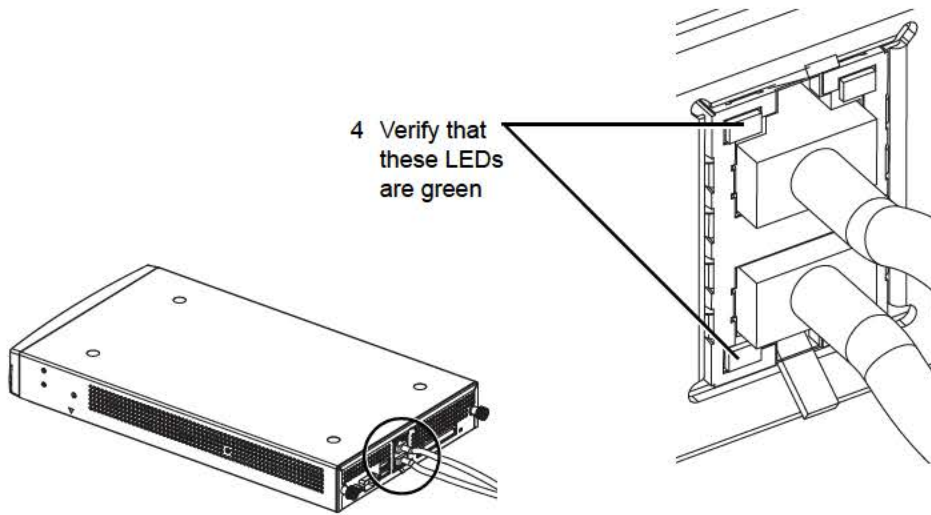
Figure 2-2: Verify the Network Connection

If the network connection LEDs are not green, check the following:

- Verify that each cable is connected properly, such as to a switch or a hub.

- Try using a different network connection cable.

5 Do one of the following:

❑ If your SG200 is a 200 A or 200 B, go to *"200 A and 200 B—Initial Configuration with a Web Browser"* on page 14.

❑ If your SG200 is a 200 C, go to *"200 C—Initial Configuration Using the Setup Wizard"* on page 18.

200 A and 200 B—Initial Configuration with a Web Browser

Important: **To configure your SG200 using a browser, the following conditions must be true:**

- **The browser must support Javascript and Javascript must be enabled.**
- **The browser must not be proxied. For information about proxied browsers, see *The Initial Configuration Page is Not Accessible* on page 42.**
- **Your proxy must not already be configured.**

To Configure the SG200 200 A and 200 B Using a Web Browser:

Note: **The following procedure is for 200 A and 200 B Appliances running SGOS 4.x or later.**

1 Complete the procedure described in *"Connecting the SG200 to a PC"* on page 12.

2 Power on the SG200.

3 Enter the following URL into your browser:

`proxysg.bluecoat.com:8083/`

A security warning dialog appears.

Note: **It is safe to click Yes or OK in this dialog because the SG200 system is directly connected to your PC. For more information about this warning dialog, see *A Security Warning Appears for the Initial Configuration Web Page* on page 46.**

The appearance of the dialog varies depending on the browser that you use.
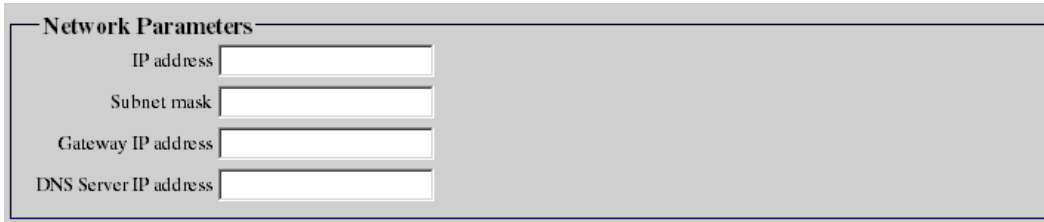
4 Click Yes (or OK) in the dialog. The SG200 Initial Configuration window opens.

Important: **If you do not see the warning dialog or if you cannot connect to the Initial Configuration page, reset the SG200 to its factory defaults. See *Resetting the SG200 to Its Factory Defaults* on page 46.**

5 Enter the network parameters for your appliance.

Network Parameters

IP address	
Subnet mask	
Gateway IP address	
DNS Server IP address	
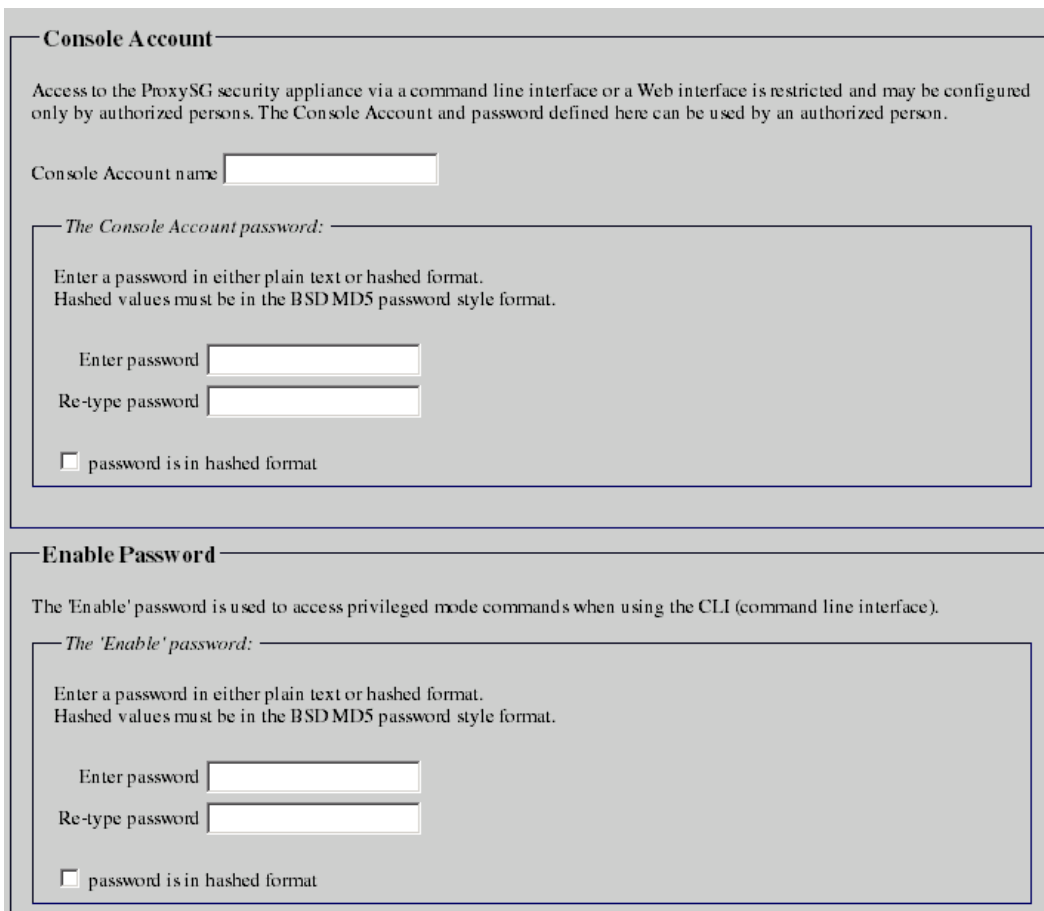
Figure 2-3:   Initial Configuration Page—Network Parameters

6 Enter the Console Account username and password and the Enable (privileged mode) password. Do not select Password is in hashed format unless the password is already in a valid hashed format.

Note: **If you want to have the password hashed for you, use the remote initial configuration method (see *Section D:Configuring the SG200 from a Remote Location* on page 32).**

Console Account

Access to the ProxySG security appliance via a command line interface or a Web interface is restricted and may be configured only by authorized persons. The Console Account and password defined here can be used by an authorized person.

Console Account name

The Console Account password:

Enter a password in either plain text or hashed format.
Hashed values must be in the BSD MD5 password style format.

Enter password
Re-type password

☐ password is in hashed format

Enable Password

The 'Enable' password is used to access privileged mode commands when using the CLI (command line interface).

The 'Enable' password:

Enter a password in either plain text or hashed format.
Hashed values must be in the BSD MD5 password style format.

Enter password
Re-type password

☐ password is in hashed format

Figure 2-4:   Initial Configuration Page—Console Account Username and Password

7 Select the default policy for proxied services:

- Selecting Allow permits all proxied transactions to pass through the SG200; you must then create policies to explicitly deny proxied transactions on a case-by-case basis.

- Selecting Deny prohibits proxied transactions from passing through the SG200; you must then create policies to explicitly grant proxied transactions on a case-by-case basis.

For more information about this option, refer to *Volume 7: The Visual Policy Manager and Advanced Policy Tasks* of the *Blue Coat ProxySG Configuration and Management Guide Suite*.

```
┌─Default Policy for Proxied Services────────────────────────────────────────────┐
│                                                                                │
│  When the appliance is initially configured, there must be a simple policy in effect which affects any traffic being intercepted │
│  by the default enabled proxied services running on the appliance (e.g. usually http and ftp). │
│  Select Allow to allow all network traffic to successfully flow through the appliance or select Deny if you want to prevent the │
│  traffic specific to the default proxied services. │
│                                                                                │
│   ○ Allow  ○ Deny                                                              │
└────────────────────────────────────────────────────────────────────────────────┘
```

Figure 2-5:   Initial Configuration Page—Default Policy for Proxied Services

8   (Optional) Secure the serial port: select Secure the Serial Port and enter the password. Do not select Password is in hashed format unless the password is already in a valid hashed format.

The serial port allows you to configure and access the SG200 using a serial cable. This can pose a security risk, because anyone with access to the appliance can reconfigure the SG200 settings. This step allows you to set a password on the serial console setup, allowing only authorized personnel the ability to reconfigure the appliance.

⚡ *WARNING!*

If you set the serial console password and then lose the password, you must restore the appliance to its original factory defaults if you want to access the Management Console or CLI (see *Resetting the SG200 to Its Factory Defaults* on page 46).

```
┌─Secure Serial Port──────────────────────────────────────────────────────────────┐
│                                                                                  │
│  Administration of the ProxySG appliance can be performed via the serial port. The serial port provides access to the ProxySG │
│  appliance Serial Console which presents you with two choices: 1) access to the Command Line Interface (CLI) and 2) access │
│  to the Setup Console. │
│  Choosing to secure the Serial Port will password protect access to both the CLI and the Setup Console. To access the CLI you │
│  will be asked for the credentials of an authorized person (like the Console Account) and to access the Setup Console you will │
│  be asked for the Setup Console password. │
│                                                                                  │
│  If you choose to secure the Serial Port, you will be prompted to provide the Setup Console password. │
│   ☐ Secure the Serial Port │
└──────────────────────────────────────────────────────────────────────────────────┘
```

Figure 2-6:   Initial Configuration Page—Secure the Serial Port

9   Click Configure Device.

- If a dialog appears with the message Errors Found, click OK and correct the errors in the Initial Configuration page. Click Configure Device again.

- If a new browser window appears with the message The initial configuration was not established, note the error messages in this window, close it, and fix the appropriate data in the Initial Configuration page. Click Configure Device again.

- If a new browser window appears with the message Proxy*SG* Initial Configuration was successful, you have successfully completed initial configuration. This window provides details about accessing the SG200 Management Console (such as the Management Console SHA1 fingerprint). Save this

information for future reference. Close the new browser window and the Initial Configuration page.

```
ProxySG Initial Configuration was successful

┌ProxySG Appliance Information────────────────────────────────────────┐
│ Model:               Blue Coat SG200-1                              │
│ Primary IP address:  10.9.44.57                                     │
│ Serial number:       0505060022                                     │
│ MAC address:         00:D0:83:04:9B:67                              │
│ Software:            SGOS 4.0.9.1                                   │
│ Management Console                                                  │
│ SHA1 Fingerprint:    26:74:46:56:54:7D:3E:F6:B1:94:2D:71:F3:98:E5:01:BB:7E:2A:F5 │
└─────────────────────────────────────────────────────────────────────┘

Now that the ProxySG appliance is configured, all future HTTP based
management must be done through the appliance's Management Console at
https://10.9.44.57:8082/
```
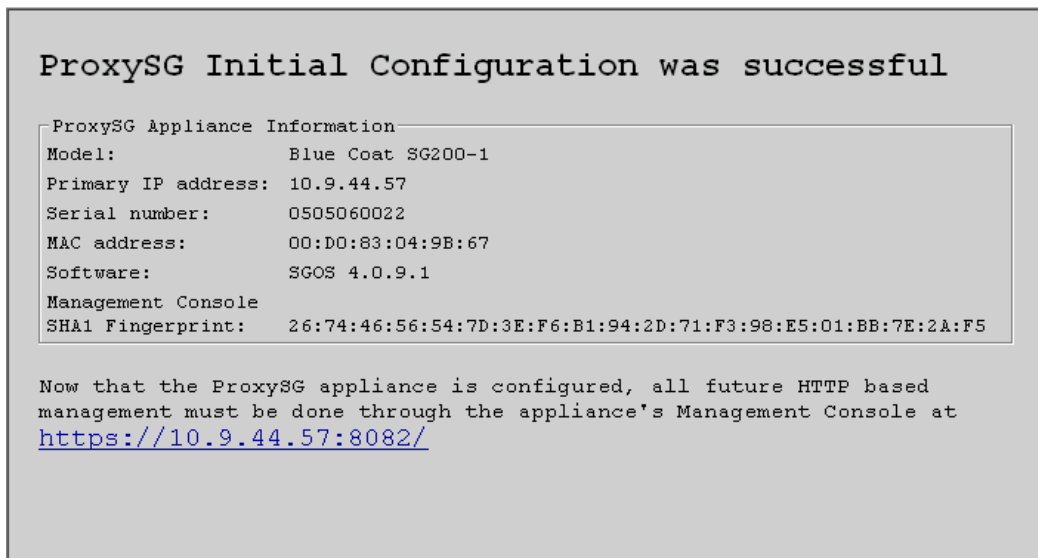
Figure 2-7:   Successful Initial Configuration Page

10 Relocate the SG200 to its final destination in the network:

   a. Power off the SG200.

   b. Remove the Ethernet cable from the SG200 and restore it to your PC.

   c. Place the SG200 into the network (see *Section B: "Placing the SG200 into the Network* on page 20).

When you have set the basic networking parameters and connected the SG200 to the network, you are ready to fully configure the appliance. For a list of all CLI commands, refer to the *Blue Coat ProxySG Command Line Reference.* For information about configuring and administering the SG200 (including information about setting policies that will explicitly grant or deny proxied transactions), refer to the *Blue Coat ProxySG Configuration and Management Guide Suite.*

200 C—Initial Configuration Using the Setup Wizard

Important: **To configure your SG200 using a browser, the following conditions must be true:**

- **The browser must support Javascript and Javascript must be enabled.**

- **The browser must not be proxied. For information about proxied browsers, see** *The Initial Configuration Page is Not Accessible* **on page 42.**

- **Your SG200 must not already be configured.**

To Configure the SG200 200 C Using the Setup Wizard:

Note: **The following procedure is for 200 C Appliances running SGOS 5.x or later.**

1 Complete the procedure described in *"Connecting the SG200 to a PC"* on page 12

2 Power on the SG200.

3 Enter the following URL into your browser:

`https://proxysg.bluecoat.com:8083/.`

A security warning dialog appears.

Note: **It is safe to click Yes or OK in this dialog because the SG200 system is directly connected to your PC. For more information about this warning dialog, see** *A Security Warning Appears for the Initial Configuration Web Page* **on page 46.**

The appearance of the dialog varies depending on the browser that you use.

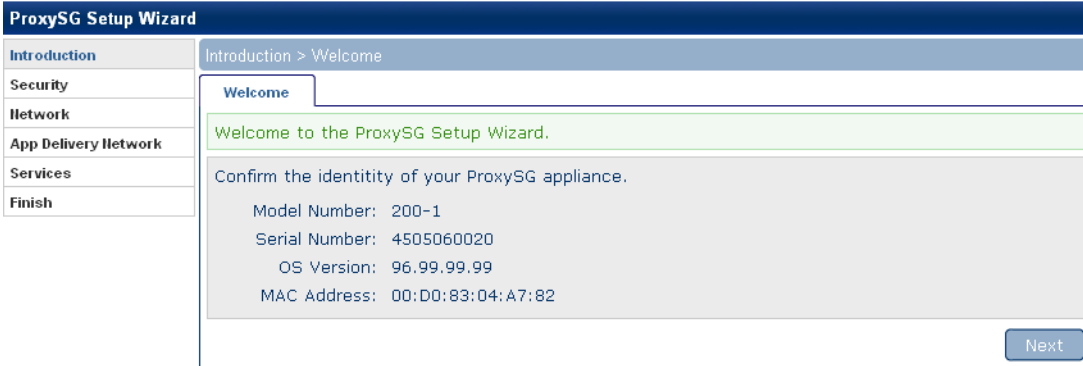**4** Click Yes (or OK) in the dialog.

Important: **If you do not see the warning dialog or if you cannot connect to the Setup Wizard, reset the SG200 to its factory defaults. See** *Chapter 3:Troubleshooting***.**

When the appliance connects, the Setup Wizard displays, as shown in the following figure.

Blue Coat

ProxySG Setup Wizard

Introduction   Introduction > Welcome

Security

Network   Welcome

App Delivery Network   Welcome to the ProxySG Setup Wizard.

Services   Confirm the identity of your ProxySG appliance.

Finish

      Model Number: 200-1
      Serial Number: 4505060020
      OS Version: 96.99.99.99
      MAC Address: 00:D0:83:04:A7:82

Next

5 Enter information on each screen, as prompted.

Each page is described; some pages include mouse-over help. If you entered network settings from the serial console, they are already filled in. To complete the Setup Wizard you must:

a. Enter the console access information.

b. Enter the CLI Enable password.

c. (Optional but highly recommended) Secure the serial port.

d. Enter the network settings:
- ❐ IP Address
- ❐ Subnet Mask
- ❐ Gateway
- ❐ DNS Server

e. (Optional) Configure the Application Delivery Network (ADN) settings.

The ADN settings optimize the delivery of applications over the WAN.

f. Select the traffic types that the appliance should intercept.

g. Set the initial policy.

h. Confirm the settings and click Configure.

Note: **The Web-based wizard is available only for initial appliance configuration (or following a reset to factory defaults). After you click** Configure **during the final step, the wizard is no longer available.**

Section B: Placing the SG200 into the Network

This procedure describes a typical scenario for placing the SG200 into your network. Use this procedure for the following circumstances:

- You have already completed an initial configuration on the SG200.

- You are going to complete an initial configuration on the SG200 using a direct serial port connection or a remote Web browser setup.

Because the appliance comes with a pass-through card, bridging is set up by default. You do not need to set up a bridge between the two interfaces.

The following instructions are an example of a typical network scenario—placing the SG200 between the LAN and a router or firewall connected to the WAN. If you do not know how to place the SG200 into your own network, consult with your IT administrator. For less common network configurations, such as using WCCP or a Layer 4 switch, refer to the *Blue Coat ProxySG Configuration and Management Guide Suite*.

To Place the SG200 into the Network:

1 Connect the SG200 to the WAN—connect one end of an Ethernet cable (straight or crossover depending on your network topology) to one of the SG200's Ethernet ports (either one). Connect the other end to the router or firewall connected to the WAN.

2 Connect the SG200 to the LAN—connect one end of an Ethernet cable (straight or crossover depending on your network topology) into the other Ethernet port on the SG200. Connect the other end to the LAN (such as a PC or a hub).

3 Verify that the network link is established by checking the network connection LEDs at the back of the SG200. If the network connection is functioning, the left-hand LED on each connection glows green (see Figure 2-2 on page 13).

If the network connection does not function, see *"A Network Link is Not Established"* on page 41.

Note: **The SG200 Series is designed to fail open. For example, if the appliance loses power, it is designed to allow network traffic to pass through its bridge ports. If you prefer the appliance to fail closed and block all traffic in the event of a power loss, you must remove the pass-through card. See *Removing the Pass-Through Card* on page 47.**

Section C: Initial Configuration Using a Direct Serial Port Connection

This section describes how to configure the SG200 using a direct serial port connection. Before configuring the SG200 using the serial port connection, you must place the SG200 into the network as described in *Section B: "Placing the SG200 into the Network* on page 20

The serial port connection setup differs by model:

- If your SG200 is a 200 A or 200 B, complete the procedure described in *"200 A and 200 B—Configuring the SG200 Using a Direct Serial Port Connection"*

- If your SG200 is a 200 C, complete the procedure described in *"200 C—Configuring the SG200 Using a Direct Serial Port Connection"*

200 A and 200 B—Configuring the SG200 Using a Direct Serial Port Connection

If your SG200 is a 200 A or 200 B, use the following procedure to configure it with a direct serial port connection.

Use a standalone serial terminal or a PC and the SG200 command-line interface (CLI) to perform a first-time configuration of the following basic network information:

- IP address
- IP gateway address
- Console username
- Enable password

- IP subnet mask
- DNS server
- Console password
- Serial port password (optional)

PC Note: **If the PC is using standard serial port settings, you should have a problem-free connection. Problems can occur if there are non-standard PC serial port settings.**

The following procedure is for 200 A and 200 B Appliances running SGOS 4.x or later. Do the procedure by reading on-screen material and entering data where necessary. The on-screen instructions display as five separate pages. In the procedure below, places that require you to enter data are illustrated by example entries in bold text.

Initial Configuration Using a Direct Serial Port Connection

Five screens display, one at a time, as shown in the following steps.

1 Power on and connect the serial terminal or PC as described below (the SG200 must be powered off):

Serial terminal: Connect the terminal's serial cable to the SG200's serial console port; start the terminal and verify that it is set using the parameters described below.

PC: Connect a serial cable to a serial port on the PC and to the SG200's serial console port; start the PC, open a terminal emulator (such as HyperTerminal), and connect to the serial port to which you attached the cable. Create and name a new connection (either a COM or TCP/IP), and verify that the port is set using the parameters described below.

- Baud rate: 9600 bps
- Parity: none
- Flow control: none

- Data bits: 8
- Stop bits: 1
- Smooth-scroll: disabled

- Emulation: VT 100

If you have set flow control to *none*, and if you have *smooth-scroll* as an option in your terminal settings, disable smooth-scroll in your terminal settings to reduce the chance of losing output.

2 Power on the SG200 and wait for the system to finish booting.

The following configuration alert displays:

```
****************** CONFIGURATION ALERT ******************

System startup cannot continue for one of these reasons:

    (a) Need at least one adapter (or bridge) configured with an IP
    address and
        subnet.

    (b) Need the console password and enable password.

********* SYSTEM STARTUP TEMPORARILY SUSPENDED  *********

Press "enter" three times to activate the serial console
```

Figure 2-8:   Initial Setup—Configuration Alert

3 Press <Enter> three times.

When the `Welcome to the ProxySG Appliance Setup Console` prompt appears, the system is ready for the first-time network configuration.

4 On page 1, press <Enter> to enter the bridge name `passthru-0` and enter the IP address, IP subnet mask, IP gateway, and DNS server parameters.

Note: **If you have removed the pass-through card, you are asked if you want to configure a software bridge. If you enter `YES`, you must configure at least one bridge port and associate a network interface with it.**

```
Welcome to the ProxySG Appliance Setup Console

-------------------- (page 1 of 5) --------------------

    Press <ESC> at any time to return to the main menu

DIRECTIONS:

    This setup console is used to assign IP addresses to the ProxySG
    Appliance. After assigning the IP addresses you can connect to the
    command line interface or Web interface to perform additional
    management tasks.

    If you have a pass through card, you can configure it by using the
    bridge name passthru-<slot number>. For example if the pass through
    card is at slot 2, the bridge name would be passthru-2.

    In order to create a new bridge, you would have to

    1. assign a name to the bridge
    2. associate one or more interfaces to the bridge
Enter bridge name to configure [passthru-0]:
IP address [0.0.0.0]: 10.25.36.47
IP subnet mask [255.255.255.0]: 255.255.255.0
IP gateway [0.0.0.0]: 10.25.36.1
DNS server [0.0.0.0]: 101.52.23.100

You have entered the following IP addresses:

IP address: 10.25.36.47
IP subnet mask: 255.255.255.0
IP gateway: 10.25.36.1
DNS server: 101.52.23.101

Would you like to change any of them? Y/N [No] N
```

Figure 2-9: Initial Setup—Page One

5 On page 2, enter a console username and a console and enable password. A default username (admin) is already in place—change it for stronger security.

Usernames and passwords can each be from 1 to 64 characters in length. Passwords that contain special characters (such as an exclamation point) must be in quotes.

```
-------------------- (page 2 of 5) --------------------

    Press <ESC> at any time to return to the main menu

DIRECTIONS:

    The console username, password and enable password are special
    administrative credentials which can be used to log in to the command
    line interface or web management interface.

    WARNING - The console password and enable password are not defined.
    The system cannot start up until these are defined.

You must configure the console user account now.

Enter console username [admin]: name123
Enter console password: "******"
Verify console password: "******"
Enter enable password: "******"
Verify enable password: "******"
```

Figure 2-10:   Initial Setup—Page Two

6   (Optional) For maximum security, secure the serial port.

The serial port allows you to configure and access the SG200 using a serial cable. This can pose a security risk because anyone with access to the appliance can reconfigure the SG200 settings. This optional step sets a password for the serial console setup, allowing only authorized personnel the ability to reconfigure the appliance.

⚡ *WARNING!*

If you set the serial console password and then lose the password, you must restore the appliance to its original factory defaults to access the Management Console or CLI (see *"Resetting the SG200 to Its Factory Defaults"* **on page 46).**

```
Do you want to secure the serial port? Y/N [Yes] Y
Enter setup password: "******"
Verify setup password: "******"

WARNING:

    If you continue and enable the secure serial port it will not be
    possible to enter the setup console without the setup password. If
    the setup password is lost, assistance from Blue Coat Systems will be
    required and all system configuration may be lost. It is recommended
    that this password be stored in a physically secure location. Access
    to the CLI on the serial port will challenge for credentials.

To enable the secure serial port, re-enter the setup password: "******"
```

Figure 2-11:   Initial Setup—Secure the Serial Port (Optional)

7   (Optional) The options on page 3 restrict access to the SG200.

Note: **For maximum security, restrict physical access to the SG200.**

```
-------------------- (page 3 of 5) --------------------

    Press <ESC> at any time to return to the main menu

DIRECTIONS:

    The console username and password are special: they can be used to
    log in to the CLI or Web Management interface even in circumstances
    where this is denied by VPM or CPL policy. This makes the console
    account useful in emergencies, as a way to log in when policy is
    broken, but it may also create a security hole.

    To close the security hole, we recommend that you restrict the use of
    the console account to specific workstations, identified by their IP
    address.

    This dialog allows you to add one IP address to the list of
    workstations that are authorized to use the console account. (This
    same list is also used to restrict which workstations can use SSH
    with RSA authentication.) Additional workstations may be configured
    later, from the command line interface or the Web interface.

    WARNING: The console account can currently be used to log in from any
    workstation.

Would you like to restrict access to an authorized workstation? Y/N
[Yes] Y

Authorized workstation [0.0.0.0]:10.2.33.1
```

Figure 2-12:   Initial Setup—Page Three

Note: **After completing the initial configuration, you can change the workstation restriction settings through the security commands in the CLI or the Console Access page in the Management Console (under Authentication). You can add or remove IP addresses or you can enable or disable workstation restrictions. Refer to *Volume 5: Securing the ProxySG* of the *Blue Coat ProxySG Configuration and Management Guide Suite* for details.**

---

8   On page 4, press <Enter> or type **No** if you do not want to enter a forwarding host at this time, or type **Yes** to enter a forwarding host.

If you type **Yes**, you must also provide a host alias and a host name or IP address.

```
-------------------- (page 4 of 5) --------------------

    Press <ESC> at any time to return to the main menu

DIRECTIONS:

    This setup console is used to configure a proxy forwarding host as
    the forwarding default (a one member default fail-over sequence).
    After assigning a host alias and the host name you can connect to the
    command line interface to perform additional management tasks.

Would you like to setup the forwarding host now? Y/N [No] **N**
```

Figure 2-13: Initial Setup—Page Four

Page 5 displays. This page explains how to access the SG200 from an SSH Client or with a Web browser. See *Section E: "Logging on to the SG200* on page 37 for more information.

```
-------------------- (page 5 of 5) --------------------

DIRECTIONS:

    The ProxySG Appliance has been successfully configured to use IP
    address: "10.25.36.47"

    You can connect to the command line interface or Web interface to
    perform additional management tasks.

    To connect to the command line interface, open the following location
    from your SSH application: 10.25.36.47

    To connect to the Web management interface, go to the following
    location with your web browser: https://10.25.36.47:8082/

--------------- CONFIGURATION COMPLETE -----------------

Press "enter" three times to activate the serial console
```

Figure 2-14: Initial Setup—Page Five

9 To log in to the serial console right away, press <Enter> three times.

A menu displays offering two choices:

```
    1) Command Line Interface
    2) Setup Console
```

10 Access the CLI or Management Console:

❐ Enter **1** in the serial console menu to select the CLI.

See *"Logging on to the SG200 CLI"* on page 38 for information about using the SG200 CLI.

❐ To access the SG200 Management Console, enter the following address into your Web browser:

`https://proxysg_IP:8082/`

where *proxysg_IP* is the IP address that you configured for this SG200.

See *Section E: "Logging on to the SG200* on page 37 for more information about accessing the SG200.

 When you have set the basic networking parameters and connected the SG200 to the network, you are ready to fully configure the appliance. For a list of all CLI commands, refer to the *Blue Coat ProxySG Command Line Reference.* For information about configuring and administering the SG200 (including information about setting policies that will explicitly grant or deny proxied transactions), refer to the *Blue Coat ProxySG Configuration and Management Guide Suite.*

200 C—Configuring the SG200 Using a Direct Serial Port Connection

If your SG200 is a 200 C, use the following procedure to configure it with a direct serial port connection.

Use a standalone serial terminal or a PC and the SG200 command-line interface (CLI) to perform a first-time configuration of the following basic network information:

- IP address
- IP gateway address
- Console username
- Enable password

- IP subnet mask
- DNS server
- Console password
- Serial port password (optional)

PC Note: **If the PC is using standard serial port settings, you should have a problem-free connection. Problems can occur if there are non-standard PC serial port settings.**

The following procedure is for 200 C Appliances running SGOS 5.x or later. Do the procedure by reading on-screen material and entering data where necessary. The on-screen instructions display as five separate pages. In the procedure below, places that require you to enter data show example entries in bold text.

To Configure the SG200 200 C Using a Direct Serial Port Connection:

Five screens display, one at a time, as shown in the following steps.

1 Power on and connect the serial terminal or PC as described below (the SG200 must be powered off):

Serial terminal: Connect the terminal's serial cable to the SG200's serial console port; start the terminal and verify that it is set using the parameters described below.

PC: Connect a serial cable to a serial port on the PC and to the SG200's serial console port; start the PC, open a terminal emulator (such as HyperTerminal), and connect to the serial port to which you attached the cable. Create and name a new connection (either a COM or TCP/IP), and verify that the port is set using the parameters described below.

- Baud rate: 9600 bps
- Parity: none
- Flow control: none
- Emulation: VT 100

- Data bits: 8
- Stop bits: 1
- Smooth-scroll: disabled

If you have set flow control to *none*, and if you have *smooth-scroll* as an option in your terminal settings, disable smooth-scroll in your terminal settings to reduce the chance of losing output.

2 Power on the SG200 and wait for the system to finish booting.

The following configuration alert displays:

```
****************** CONFIGURATION ALERT ******************

System startup cannot continue for one of these reasons:

    (a) Need at least one adapter (or bridge) configured with an IP
    address and
        subnet.

    (b) Need the console password and enable password.

********* SYSTEM STARTUP TEMPORARILY SUSPENDED  *********

Press "enter" three times to activate the serial console
```

Figure 2-15:   Initial Setup—Configuration Alert

3 Press <Enter> three times.

When the `Welcome to the ProxySG Appliance Setup Console` prompt appears, the system is ready for the first-time network configuration.

4 On page 1, enter the interface number, IP address, IP subnet mask, IP gateway, and DNS server parameters.

```
Welcome to the ProxySG Appliance Setup Console

--------------------- (page 1 of 5) --------------------

    Press <ESC> at any time to return to the main menu

DIRECTIONS:

    This setup console is used to assign IP addresses to the ProxySG
    Appliance. After assigning the IP addresses you can connect to the
    command line interface or Web interface to perform additional
    management tasks.

Enter interface number to configure [0:0]:
IP address [0.0.0.0]: 10.25.36.47
IP subnet mask [255.255.255.0]: 255.255.255.0
IP gateway [0.0.0.0]: 10.25.36.1
DNS server [0.0.0.0]: 101.52.23.100

You have entered the following IP addresses:

IP address: 10.25.36.47
IP subnet mask: 255.255.255.0
IP gateway: 10.25.36.1
DNS server: 101.52.23.101

Would you like to change any of them? Y/N [No] N
```

Figure 2-16:   Initial Setup—Page One

5 On page 2, you are asked if you want to finish configuration using the Setup Wizard.

```
-------------------- (page 2 of 5) --------------------

A comprehensive Setup Wizard is available if you use your
Web browser. You can either use the Web Setup Wizard or you
can continue the initial configuration using this serial console.
Note that this serial console initial configuration method
contains a subset of the configuration options available in the
Web Setup Wizard.

Would you like to use the ProxySG Web Setup Wizard? Y/N [No] N
```

Figure 2-17:   Initial Setup—Page Two

If you choose to use the Setup Wizard, go to *"200 C—Initial Configuration Using the Setup Wizard"* on page 18.

6   On page 3, enter a console username and a console and enable password. A default username (admin) is already in place—change it for stronger security.

Usernames and passwords can each be from 1 to 64 characters in length. Passwords that contain special characters (such as an exclamation point) must be in quotes.

```
-------------------- (page 3 of 5) --------------------

     Press <ESC> at any time to return to the main menu

DIRECTIONS:

   The console username, password and enable password are special
   administrative credentials which can be used to log in to the command
   line interface or web management interface.

   WARNING - The console password and enable password are not defined.
   The system cannot start up until these are defined.

You must configure the console user account now.

Enter console username [admin]: name123
Enter console password: "******"
Verify console password: "******"
Enter enable password: "******"
Verify enable password: "******"
```

Figure 2-18:   Initial Setup—Page Three

7   (Optional) For maximum security, secure the serial port.

The serial port allows you to configure and access the SG200 using a serial cable. This can pose a security risk because anyone with access to the appliance can reconfigure the SG200 settings. This optional step sets a password for the serial console setup, allowing only authorized personnel the ability to reconfigure the appliance.

⚡ *WARNING!*

If you set the serial console password and then lose the password, you must restore the appliance to its original factory defaults to access the Management Console or CLI (see *Resetting the SG200 to Its Factory Defaults* on page 46).

```
Do you want to secure the serial port? Y/N [Yes] Y
Enter setup password: "******"
Verify setup password: "******"

WARNING:

    If you continue and enable the secure serial port it will not be
    possible to enter the setup console without the setup password. If
    the setup password is lost, assistance from Blue Coat Systems will be
    required and all system configuration may be lost. It is recommended
    that this password be stored in a physically secure location. Access
    to the CLI on the serial port will challenge for credentials.

To enable the secure serial port, re-enter the setup password: "******"
```

Figure 2-19: Initial Setup—Secure the Serial Port (Optional)

8 (Optional) On page 4, you can restrict access to the SG200.

Note: **For maximum security, restrict physical access to the SG200.**

```
-------------------- (page 4 of 5) --------------------

    Press <ESC> at any time to return to the main menu

DIRECTIONS:

    The console username and password are special: they can be used to
    log in to the CLI or Web Management interface even in circumstances
    where this is denied by VPM or CPL policy. This makes the console
    account useful in emergencies, as a way to log in when policy is
    broken, but it may also create a security hole.

    To close the security hole, we recommend that you restrict the use of
    the console account to specific workstations, identified by their IP
    address.

    This dialog allows you to add one IP address to the list of
    workstations that are authorized to use the console account. (This
    same list is also used to restrict which workstations can use SSH
    with RSA authentication.) Additional workstations may be configured
    later, from the command line interface or the Web interface.

    WARNING: The console account can currently be used to log in from any
    workstation.

Would you like to restrict access to an authorized workstation? Y/N
[Yes] Y

Authorized workstation [0.0.0.0]:10.2.33.1
```

Figure 2-20: Initial Setup—Page Four

Page 5 displays. This page explains how to access the SG200 from an SSH Client or with a Web browser. See *Section E: "Logging on to the SG200* on page 37 for more information.

```
-------------------- (page 5 of 5) --------------------

DIRECTIONS:

    The ProxySG Appliance has been successfully configured to use IP
    address: "10.25.36.47"

    You can connect to the command line interface or Web interface to
    perform additional management tasks.

    To connect to the command line interface, open the following location
    from your SSH application: 10.25.36.47

    To connect to the Web management interface, go to the following
    location with your web browser: https://10.25.36.47:8082/

--------------- CONFIGURATION COMPLETE -----------------

Press "enter" three times to activate the serial console
```

Figure 2-21: Initial Setup—Page Five

9 To log in to the serial console right away, press <Enter> three times.

A menu displays offering two choices:

```
1) Command Line Interface
2) Setup Console
```

10 Access the CLI or Management Console:

❏ Enter **1** in the serial console menu to select the CLI.

See *"Logging on to the SG200 CLI"* on page 38 for information about using the SG200 CLI.

❏ To access the SG200 Management Console, enter the following address into your Web browser:

`https://proxysg_IP:8082/`

where *proxysg_IP* is the IP address that you configured for this SG200.

See *Section E: "Logging on to the SG200* on page 37 for more information about accessing the SG200.

When you have set the basic networking parameters and connected the SG200 to the network, you are ready to fully configure the appliance. For a list of all CLI commands, refer to the *Blue Coat ProxySG Command Line Reference*. For information about configuring and administering the SG200 (including information about setting policies that will explicitly grant or deny proxied transactions), refer to the *Blue Coat ProxySG Configuration and Management Guide Suite*.

Section D: Configuring the SG200 from a Remote Location

Important: **This procedure pertains only to SGOS 4.2.2.x and later. If you are running SGOS 5.1.1.x or later, you must use the serial console connection or Web Setup Wizard to configure the SG200. See *"200 C—Configuring the SG200 Using a Direct Serial Port Connection" on page 27* and *"200 C—Initial Configuration Using the Setup Wizard" on page 18* for more information.**

About Remote Configuration

The goal of the remote configuration method is to allow an administrator to provide the initial configuration settings of an appliance *before* the physical installation of the system. Using the remote configuration method, an administrators uses an HTML page to specify the initial configuration settings, which are then embedded into a URL. To configure the appliance, a remote installer only has to place the appliance into the network and click the generated URL. After the appliance has its initial configuration, the administrator can finish configuring the appliance—either remotely or locally.

The remote configuration method is useful in the following circumstances:

- You have appliances destined for multiple locations but do not want to have to first ship them to a single location for initial configuration.

- The personnel at the remote locations are not technical and cannot be trusted to properly configure the appliance.
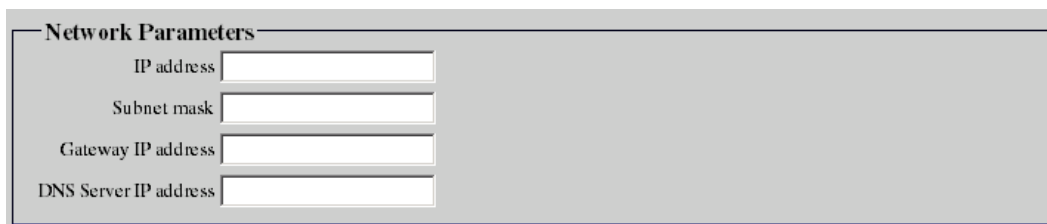
Configuring the SG200 remotely is a two-step process—use the following procedures if you want to enter the SG200 configuration parameters from a remote location (Step 1), and then have an on-site administrator place the SG200 into the network and complete the configuration (Step 2).

Step One—Enter the Configuration Parameters Using a Web Browser

Perform this procedure if you plan to enter configuration parameters for the SG200 from a remote location and then have an on-site administrator place the SG200 into the network and complete the configuration.

To Enter Configuration Parameters from a Remote Location:

1 Enter the following URL into your browser:

`http://download.bluecoat.com/initial-remote/initial-remote.html`

2 The SG200 Initial Configuration Setup for Remote Appliances window opens.

3 Enter the network parameters for the remote appliance.

Figure 2-22:   Remote Initial Configuration Page—Network Parameters

4 Enter the Console Account username and password; enter the Enable (privileged mode) password.

- If you enter the passwords in plain text, click hash the password for each password.
- If you enter the passwords in hashed format, select password is in hashed format for each password. A hashed password must be in the BSD MD5 password format.

Figure 2-23:   Remote Initial Configuration Page—Console Account Username and Password

5 Select the default policy for proxied services:

- Selecting Allow permits any and all proxy-types access to the SG200; you must then create policies to explicitly deny access on a case-by-case basis.

- Selecting Deny prohibits proxy-type access to the SG200; you must then create policies to explicitly grant access on a case-by-case basis.

For more information about this option, refer to *Volume 7: The Visual Policy Manager and Advanced Policy Tasks* of the *Blue Coat ProxySG Configuration and Management Guide Suite*.
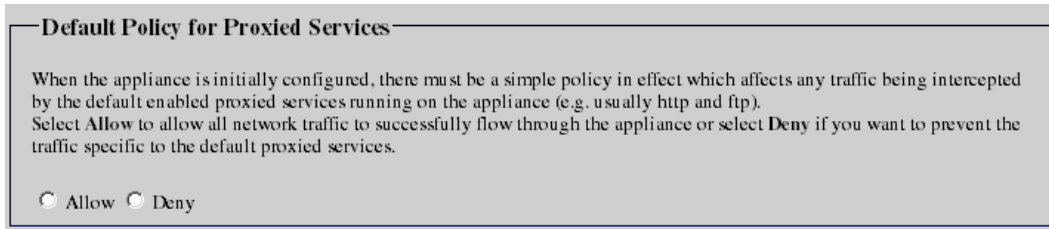
Figure 2-24:   Remote Initial Configuration Page—Default Policy for Proxied Services

6 (Optional) Secure the serial port: select Secure the Serial Port and enter the password.

- If you enter the password in plain text, click hash the password.

- If you enter the password in hashed format, select password is in hashed format. A hashed password must be in the BSD MD5 password format

The serial port allows you to configure and access the SG200 using a serial cable. This can pose a security risk, because anyone with access to the appliance can reconfigure the SG200 settings. This optional step allows you to set a password on the serial console setup, allowing only authorized personnel the ability to reconfigure the appliance.

⚡ *WARNING!*

If you set the serial console password and then lose the password, you must restore the appliance to its original factory defaults to access the Management Console or CLI (see *Resetting the SG200 to Its Factory Defaults* on page 46).
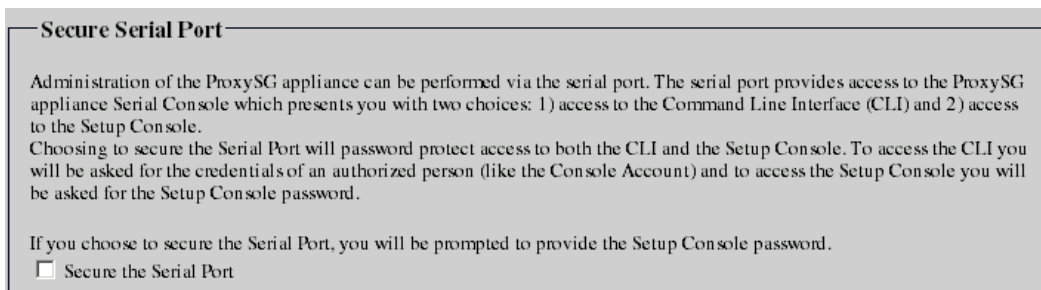

Figure 2-25:   Remote Initial Configuration Page—Secure the Serial Port

> *Note:* **Do not select the Secure the Front Panel Display option; the SG200 Series Appliance does not have a front panel display.**

7 Click Generate URLs.

- If a dialog appears with the message Errors Found, click OK and correct the errors in the Initial Configuration page. Click Generate URLs again.

- If all the fields in the form are correct, a section called Configuration URLs appears at the bottom of the page. A list of URLs are provided in this section—one for each of the four potential network addresses to which the SG200 might respond. Which URL works best depends on the network topology into which the SG200 is placed. At least one of the URLs should work in your network environment.

8 Copy and send one or more of the URLs to the local administrator who is completing the configuration. Verify that the local administrator has all required information, such as how to properly place the SG200 into the network and, if necessary, how to modify the network parameters on the PC so that the generated URL works to configure the appliance.

Step Two—Complete the Configuration

Perform the following procedure if you are at the same location as the SG200 and you are planning to complete the initial configuration using a URL provided to you by a remote administrator.

To Configure the SG200 Using a Remotely Generated URL:

1 Place the SG200 into your network using one of the following methods:

- Change the IP address of the PC so that it is on one of the subnets the appliance uses for initial configuration:

    ❏ https://10.0.0.254:8083/

    ❏ https://172.16.0.254:8083/

    ❏ https://192.168.0.254:8083/

    ❏ https://192.168.1.254:8083/

- On the PC, create a static route to the SG200. Refer to *"Creating a Static Route to the SG200"* on page 47 for information about creating a static route.

- Deploy the SG200 inline using the bridging feature.

2 On your PC, open a Web browser using the Initial Configuration URL that you received from the remote administrator. If the URL is a link in an e-mail, click the link.

- If a new browser window appears with the message Proxy*SG* Initial Configuration was successful, you have successfully completed initial configuration. This window provides details about accessing the SG200 Management Console, including the Management Console SHA1 fingerprint (see Figure 2-7 on page 17). Save this information for future reference. Close the new browser window and the Initial Configuration page.

- If the URL was not entered correctly or was corrupted, an error page displays. Fix the problem indicated and click Configure Device again.

- If the SG200 is unavailable (for example, it is not connected to the network properly or is already configured), you either fail to connect to the Web page (and see a browser error page) or you see a Blue Coat Web page that describes some of the potential problems you might have. Fix the problem, if possible, and click Configure Device again. If you cannot fix the problem, contact the remote administrator for assistance.

Note: **You might need to modify the network parameters on your PC so that the URL works to configure the SG200. Consult the remote administrator if you suspect that this is required.**

When you have set the basic networking parameters and connected the SG200 to the network, you are ready to fully configure the appliance. For a list of all CLI commands, refer to the *Blue Coat ProxySG Command Line Reference*. For information about configuring and administering the SG200 (including information about setting policies that will explicitly grant or deny proxied transactions), refer to the *Blue Coat ProxySG Configuration and Management Guide Suite*.

Section E: Logging on to the SG200

After you have performed the initial configuration and connected the SG200 to the network, you must log on to the SG200 to fully configure the appliance. There are two ways to do this:

- Use a browser to access the SG200 Management Console Web interface.
- Use a direct serial connection or an SSH Client to access the SG200 command-line interface (CLI).

Logging on to the SG200 Management Console

The Management Console is a graphical user interface for configuring and managing all aspects of the SG200. You can log on to the Management Console using a browser.

To Log on to the Management Console Using a Browser:

1 Start the SG200.

2 Open a browser. The SG200 Management Console supports Microsoft Internet Explorer 6, Netscape® Communicator 7.2, and Firefox 1.0.

3 Enter the IP address configured during initial configuration, followed by the port number `8082`. For example, enter: `https://10.25.36.47:8082`.

A security warning dialog appears.

Note: **If you performed the initial configuration of the appliance using a browser, you can validate the credentials in the security warning dialog with the SHA1 fingerprint information that you received after successfully completing the initial configuration (see Figure 2-7 on page 17).**

---

4 If you are satisfied that this certificate was generated from the correct appliance, click Yes or OK in the security warning dialog.

An Enter Network Password dialog appears.

5 Enter the username and password that you configured during initial configuration into the Enter Network Password dialog.

The SG200 home page displays.

6 Click the Management Console link from the top of the list on the left.
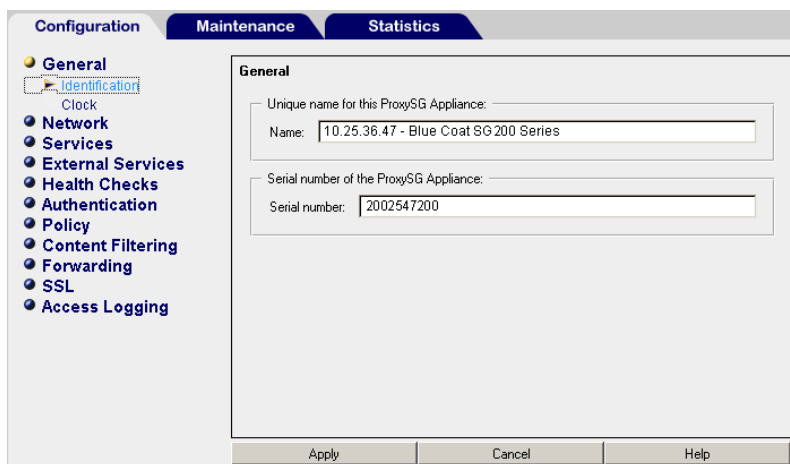
The Management Console page displays.

Figure 2-26:   The Management Console Page

7 Navigate among Configuration, Maintenance, and Statistics by clicking one of the three tabs near the top of the screen; click the links on the left to select a configurable component. Click Help on any screen to display information for that screen.

The online help contains the complete text of the *Blue Coat ProxySG Configuration and Management Guide Suite.* Once you are in the online help, use the TOC (Table of Contents) and Index links to navigate through the manual.

Logging on to the SG200 CLI

Connect to the SG200 CLI using a direct serial connection or an SSH client, such as PuTTY or F-Secure. To connect to the SG200 CLI using Telnet, you must first enable the Telnet Console. Refer to *Volume 3: Proxies and Proxy Services* of the *Blue Coat ProxySG Configuration and Management Guide Suite*.

Note: **The CLI enable password restricts access to the privileged mode configuration options.**

To Log on to the SG200 CLI Using a Direct Serial Connection:

1 To set up the serial connection, complete steps 1 through 3 in the section *"200 A and 200 B—Configuring the SG200 Using a Direct Serial Port Connection"* on page 21.

The following text displays:

```
Welcome to the ProxySG Appliance Serial Console

    Version: SGOS 4.1.0.1, Release id: 22527

------------------------ MENU--------------------------

1) Command Line Interface
2) Setup Console

--------------------------------------------------------

Enter option:
```

Figure 2-27:   Serial Connection Login Page

2 Enter **1** to access the Command Line Interface.

3 At the command prompt, enter **enable**, then enter the enable password that you configured during initial configuration:

```
SGOS> enable
Enable Password:
SGOS#
```

You are now in privileged mode.

4 At the privileged-mode command prompt, enter **configure terminal** to configure SG200 settings:

```
SGOS# configure terminal
Enter configuration commands, one per line.  End with CTRL-Z.
SGOS#(config)
```

Refer to the *Blue Coat ProxySG Configuration and Management Guide Suite* or the *Blue Coat ProxySG Command Line Reference* for information about using the CLI to configure the SG200.

To Log on to the SG200 CLI Using an SSH Client:

Note: **You must already have an SSH Client installed before proceeding with the following steps.**

1 Start the SG200.

2 Launch your SSH Client—enter the following settings as necessary:

- The IP address that you configured during initial configuration.

- A port number, if necessary (Port 22 is the default).

- The username and password that you configured during initial configuration.

3 At the command prompt, enter **enable**, then enter the enable password that you configured during initial configuration:

```
SGOS> enable
Enable Password: ******
SGOS#
```

You are now in privileged mode.

4 At the privileged-mode command prompt, enter **configure terminal** to configure SG200 settings:

```
SGOS# configure terminal
Enter configuration commands, one per line.  End with CTRL-Z.
SGOS#(config)
```

Refer to the *Blue Coat ProxySG Configuration and Management Guide Suite* or the *Blue Coat ProxySG Command Line Reference* for information about using the CLI to configure the SG200.

Chapter 3: Troubleshooting

This chapter describes how to isolate and solve common problems during the installation of the SG200.

A Network Link is Not Established

At the back of the appliance, each of the two network connections has two LEDs—the LED on the right flashes amber to indicate network activity and the LED on the left glows green to indicate a functional network connection.
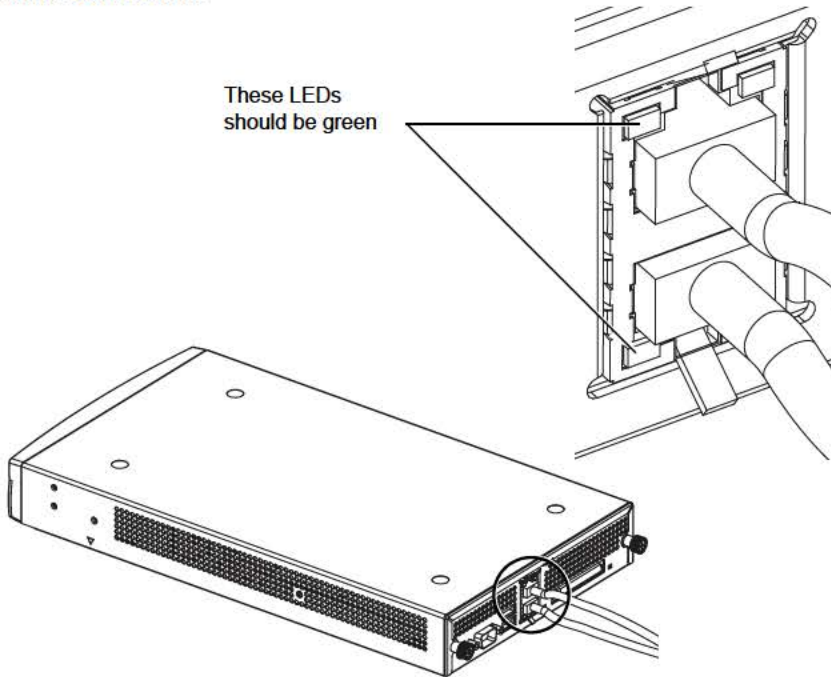
These LEDs should be green

Figure 3-1: Verify the Network Link

If the LED on the left is not green for either connection, a network link is not established. Check the following:

- Verify that each cable is connected properly, such as to a switch or a hub. If you are connecting your SG200 to your PC (see *"Connecting the SG200 to a PC"* on page 12), verify that the crossover cable is connected between the PC and the SG200, and not between the SG200 and the LAN.

- Try using a different network cable.

The Initial Configuration Page is Not Accessible

This is a networking problem or you entered an incorrect network address. Attempt the following:

• Verify that the SG200 is powered on—the barrel of the power supply adapter must be fully inserted into the SG200.

• Verify that both interfaces have established a network link (see *"A Network Link is Not Established"* above). The Ethernet cables should be connected as follows:

  ❐ A crossover cable (such as the one included with the SG200) is connected between the SG200 and the PC.

  ❐ A straight cable (patch cord) is connected between the SG200 and other networking equipment (such as a switch).

• Verify that you entered the correct initial configuration URL:
  `https://proxysg.bluecoat.com:8083/`.

• Try one of the following URLs to access the Initial Configuration page:

        `https://10.0.0.254:8083/`

        `https://172.16.0.254:8083/`

        `https://192.168.0.254:8083/`

        `https://192.168.1.254:8083/`

        `https://204.94.89.100:8083/`

  To use the preceding URLs, the host client must be on the same subnet as one of the IP-addresses. Or, you can add a static route on the host client.

• Verify that the browser is not proxied. To change or check the browser settings, complete one of the following steps:

  ❐ In a Windows browser, select Tools>Internet Options>Connections. Click LAN Settings and deselect Proxy server if it is selected.

  ❐ In a Firefox browser, select Tools>Options>General. Click the Connection Settings button and deselect Manual or Automatic Proxy Configuration if one of them is selected (select Direct Connection to the Internet).

  ❐ In a Netscape Communicator browser, select Edit>Preferences>Advanced>Proxies and deselect Manual or Automatic Proxy Configuration if one of them is selected (select Direct Connection to the Internet).

• Restore the appliance to its factory defaults (the Initial Configuration page is not accessible to an appliance that has already been configured). See *"Resetting the SG200 to Its Factory Defaults"* on page 46.

The SG200 Does Not Power On

If the SG200 does not power on, check that the power supply adapter is fully inserted into the back of the SG200 and that the power cable is fully inserted into the power supply adapter and a working electrical outlet.

Cannot Access the Serial Console

If you have connected a serial cable to the SG200 but you cannot open the serial console, do the following:

- Check cable connections.

- Check configuration information at the terminal emulator for the correct settings (see *"200 A and 200 B—Configuring the SG200 Using a Direct Serial Port Connection"* on page 21 for information).

- Verify that the serial cable is a Null Modem type cable. You can review the cable pin outs at *http://www.bluecoat.com/support/self-service/1/pinouts.html*

- Use a different cable.

Cannot Access the Management Console

If you successfully complete an initial configuration but the browser fails to connect to the SG200 successfully, verify the following information:

- Verify the correct IP address and port for the SG200 in the Web browser (the default port is 8082).

- Verify that the workstation is configured and working properly by connecting to other Web sites. This test might fail if your browser is configured to use the SG200 as a proxy server and there is a problem with the SG200.

- If accessing a SG200 located on a remote network (any segment other than the segment to which the workstation is attached), verify that other servers on that network are accessible.

- Ping the IP address to verify that the SG200 is accessible from the workstation. If the SG200 does not respond to the ping, verify that the SG200 is operational (as described earlier).

The System LED Indicates Unhealthy Status

The front-panel System LED indicates the health of the SG200, as described in the table below.

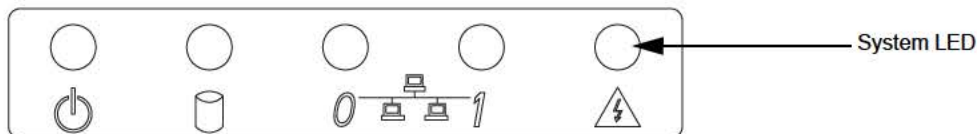| System LED Activity	Meaning
Off	Nothing to report (SG200 is not powered on)
Green	SG200 is healthy
Amber	SG200 is unhealthy, but not critically so
Flashing Green to Amber	SG200 is critically unhealthy and requires immediate attention

Figure 3-2:   Front Panel LEDs—System LED

To identify the problem, check the environmental statistics, either through the Management Console or the command line interface (CLI), as described in the following two procedures.

To Identify a System Problem or Failure through the Management Console:

1   Log on to the SG200 Management Console (see *"Logging on to the SG200 Management Console"* on page 37 for information).

2   Click the Statistics tab, click General, and select the Environment tab.
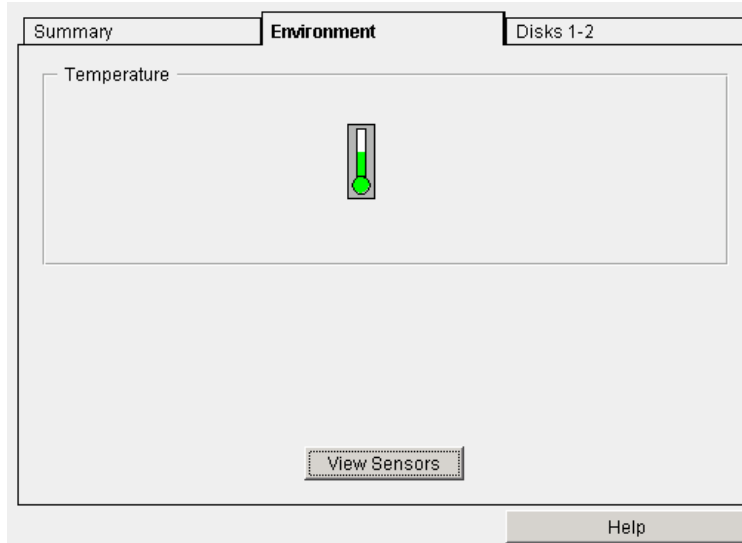
The Environment tab displays.

Figure 3-3:   The Environment Tab

3   Click View Sensors to see the environment statistics for the motherboard and CPU temperatures.

The Sensor statistics window opens—the Status column is green and displays OK for healthy environment statistics, or is red and displays the problem for unhealthy environment statistics.

Sensor statistics

Sensor Name	Reading	Status
MB Temperature	34.6 C	OK
CPU Temperature	35.6 C	OK

Figure 3-4:   Sensor Statistics Window

4   Close the Sensor statistics window when you are finished.

4.2.2.x—To Identify a System Problem or Failure through the CLI:

Use the following procedure if your software release is 4.2.2.x or later. If you are running 5.1.1.x or later see *"5.1.1.x—To Identify a System Problem or Failure through the CLI:"* on page 45.

1   Log on to the SG200 CLI (see *"Logging on to the SG200 CLI"* on page 38 for information).

2   From any CLI mode, enter the following command:

```
sgos# show environmental
```

The environmental statistics display. These include the range for upper and lower critical readings for each environmental statistic followed by the current reading and threshold status.

```
SGOS#(config) show environmental

Environmental Sensor Information


Baseboard Temperature # 1 :

Temperature Reading: 31.7 C
Current Threshold Status : NOMINAL -- OK

% UPPER CRITICAL        : 75.0
% UPPER NON CRITICAL    : 65.0

Processor Temperature # 1 :

Temperature Reading: 32.0 C
Current Threshold Status : NOMINAL -- OK

% UPPER CRITICAL        : 90.0
% UPPER NON CRITICAL    : 75.0
```

Figure 3-5:   Environmental Statistics through the CLI

5.1.1.x—To Identify a System Problem or Failure through the CLI:

Use the following procedure if your software release is 5.1.1.x or later. If you are running 4.2.2.x or later see *"4.2.2.x—To Identify a System Problem or Failure through the CLI:"* on page 44.

1 Log on to the SG200 CLI (see *"Logging on to the SG200 CLI"* on page 38 for information).

2 From any CLI mode, enter the following command:

        sgos# **show system-resource-metrics**

The hardware and software system resource metrics display. These include the range for upper and lower critical readings for each environmental statistic followed by the current reading and threshold status.

```
SGOS#(config) show system-resource-metrics

System Resource Statistics

CPU utilization
Current Value: 0 percent
Current Status: ok
Critical Threshold: 95 percent
Critical Interval: 120 seconds
Warning Threshold: 80 percent
Warning Interval: 120 seconds
Notification Type: SNMP trap

Memory pressure
Current Value: 62 percent
Current Status: ok
Critical Threshold: 95 percent
Critical Interval: 120 second
Warning Threshold: 90 percent
```

Figure 3-6:   System Resource Metrics CLI output

A Security Warning Appears for the Initial Configuration Web Page

When you open the Initial Configuration page, a security warning dialog appears. This warning indicates that the SG200 credentials could not be verified by a known certificate authority (such as VeriSign®). This is because the SG200 dynamically generated the self-signed credentials at the time of the last factory reset—they are not registered with a known certificate authority.

Normally, accepting such a credential represents a security risk because of the possibility of a man-in-the-middle attack. However, when you have connected your PC directly to the SG200, as described in this guide, a man-in-the-middle attack is impossible. The SG200 has not yet been configured and is connected directly to your PC. The Initial Configuration Web page is accessible only through a SG200 that has not yet been configured.

You can verify that the serial number in the credential matches the serial number printed on the SG200 if you want to be absolutely certain that you have connected to the correct device.

Resetting the SG200 to Its Factory Defaults

When the SG200 is powered on and has booted up, but an initial configuration has not yet been performed, the Power LED flashes green and amber. If the Power LED is solid green, the initial configuration has already been performed. If you did not perform an initial configuration, but the Power LED is solid green, reset the appliance to its factory defaults. Also reset the appliance if you cannot connect to the Initial Configuration page through your browser. The initial configuration Web page is accessible only to an appliance that has not been configured.

Important: **Using the reset button returns the SG200 to its factory defaults. Any configurations currently set are lost.**

To Restore the SG200 to Its Factory Defaults:

1 Power on the SG200 if it is off and locate the Reset button at the back of the appliance. It is a recessed button to the right of the compact flash port and to the left of the right-hand cover screw.
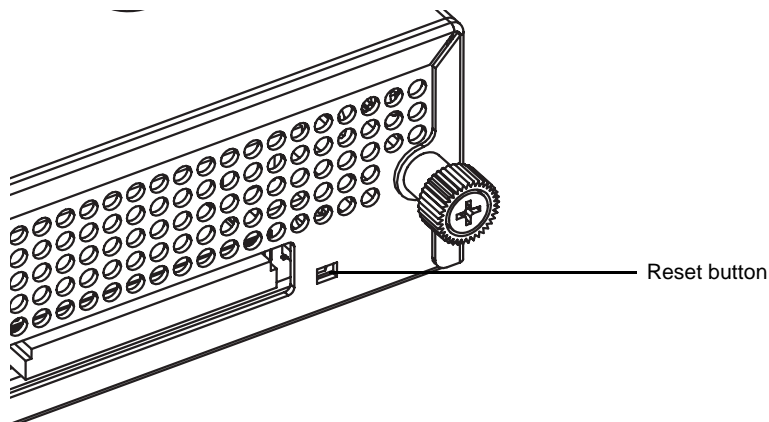

Reset button

Figure 3-7:   The Reset Button

2 Use a pen to push in the reset button—hold it in until the appliance powers off (about five seconds).

The appliance performs a soft restart. The power LED turns amber during the restart. Wait until the reset is complete (about one minute) before trying to complete the initial configuration.

Creating a Static Route to the SG200

I f your SG200 is running 4.2.2.x or later and you want to use the Web-based initial configuration method, you might need to create a static route from your PC to one of the "soft" initial configuration IP addresses.

To create a static route to the SG200

1 Access the Windows command prompt.

2 Enter the following command:

> C:\>**route add** *proxySG_ip_address* **mask** *subnet_mask* *client_ip_address*

In the preceding command, *soft_ip_address* is one of the "soft" IP addresses the SG200 listens for and *client_ip_address* is the address of the PC.

For example:

> C:\>**route add 10.0.0.254 mask 255.255.255.255 10.2.11.155**

3 Verify the static route by entering the following command:

> C:\>**route print**

Removing the Pass-Through Card

Important: **This procedure is not necessary under most circumstances.**

The SG200 Series Appliance comes with a pass-through card—a 10/100 dual port Ethernet adapter designed by Blue Coat to provide an efficient fault-tolerant bridging solution. If this card is installed on a SG200, SGOS detects the card upon system bootup and automatically creates a bridge—the two Ethernet ports on the appliance serve as the bridge ports. If the SG200 is powered down or loses power for any reason, the bridge fails open; that is, Web traffic passes from one Ethernet port to the other. Therefore, Web traffic is uninterrupted, but does not route through the appliance.

Because the pass-through card fails open, it can create a security risk. If you prefer that the appliance fail closed, blocking all traffic if the appliance loses power, you must remove the pass-through card.

WARNING! **ALWAYS observe proper electrostatic discharge (ESD) conventions. Attach an ESD protective wrist strap to your wrist and to the SG200 chassis. Ensure that the SG200 is on an ESD-safe work surface or ground the unit appropriately. Blue Coat *does not assume responsibility or liability for damage resulting from ESD*.**

To Remove the Pass-Through Card:

1 While the SG200 is still powered on, attach the disposable ESD wrist strap: wrap the adhesive side of the ESD wrist strap around your wrist, remove the backing from the copper tape, and attach the copper tape to a non-painted metal surface of the SG200 chassis.

2 Remove the Ethernet cables and, if necessary, the serial cable.

3 Power off the SG200 by removing the power supply adapter from the SG200.

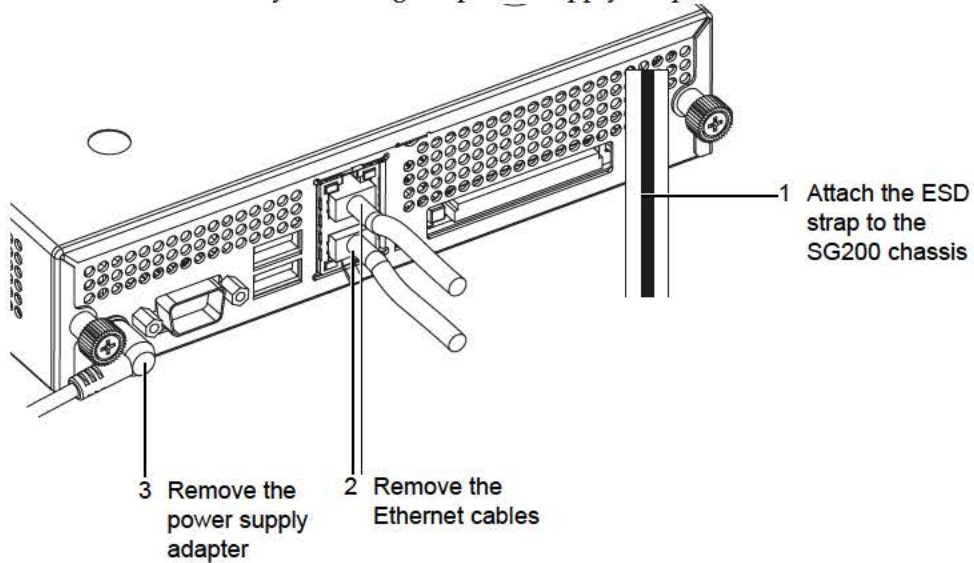3 Remove the power supply adapter 2 Remove the Ethernet cables 1 Attach the ESD strap to the SG200 chassis

Figure 3-8: Attach the ESD Strap and Remove the Cables

Important: **The appliance will not remain grounded if you take off the wrist strap after you have removed the power supply adapter. To reground the appliance, connect the power supply adapter (powering on the appliance), then reattach the wrist strap before removing the power supply adapter.**

4 Remove the SG200 from the wall or equipment rack, if necessary.

5 Remove the cover from the SG200: loosen the two cover screws at the back of the SG200 and use them to pull the cover toward you slightly. You might need to push the SG200 chassis away from you at the same time. Lift the cover up and off.

Loosen the cover screws and use them to remove the cover
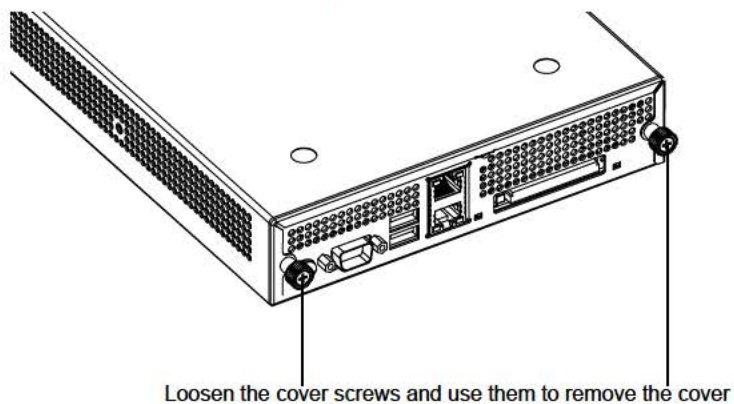
Figure 3-9: Remove the Rack-Mounting Brackets and the Cover

6 Locate the pass-through card and remove the pass-through-card screw: if you are facing the front of the SG200, the pass-through card is located near the back of the SG200 on the left.
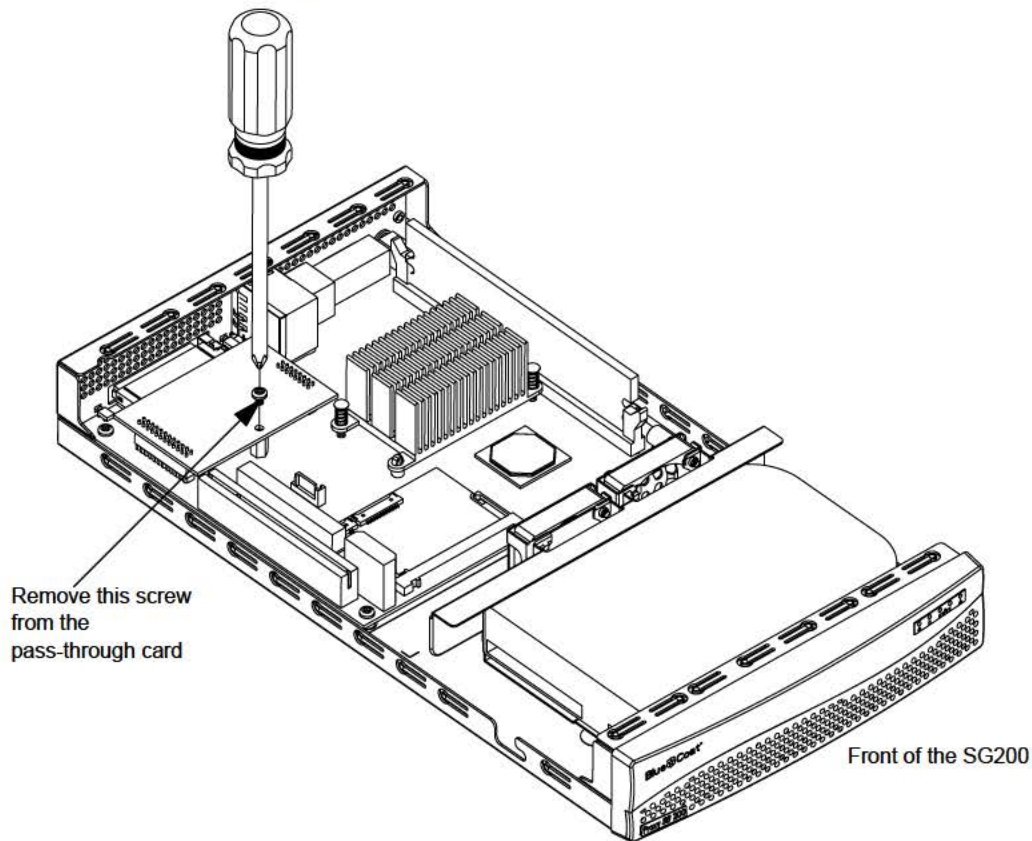
Figure 3-10:   Remove the Pass-Through Card Screw

7 Remove the pass-through card (grasp it on two sides and lift up until it disconnects).

8 Install the jumper onto the exposed header. Ensure that all of the pins are connected (that the jumper is not offset).

Install the jumper onto this header

Jumper installed
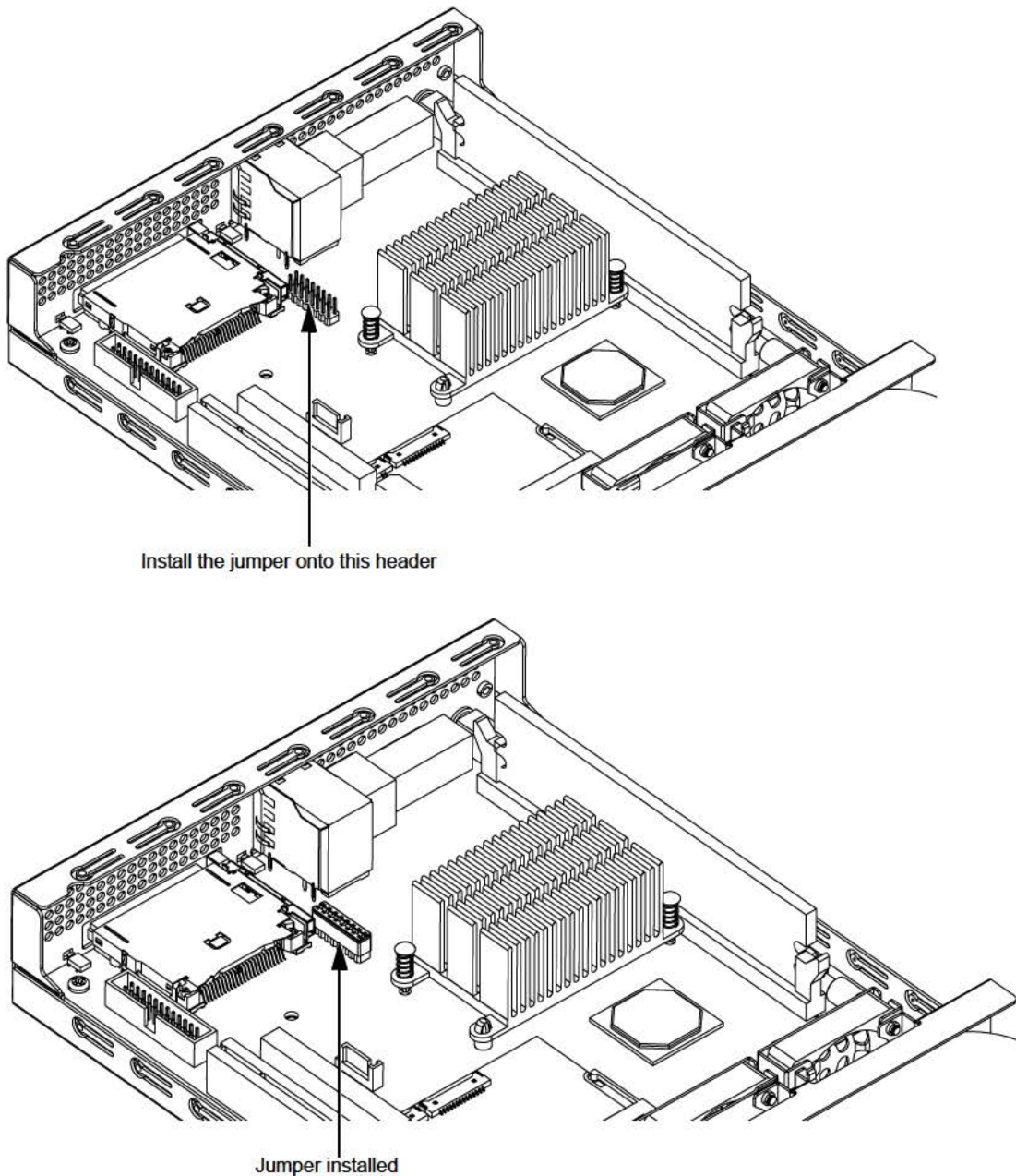
Figure 3-11:   Install the Jumper

9 Replace the cover on the SG200 and tighten the cover screws.

Now that the pass-through card has been removed, you can configure software bridging, which, unlike hardware bridging, allows you to configure failover. Failover is accomplished by creating virtual IP addresses on each proxy, creating a failover group, and attaching the bridge configuration. One of the proxies must be designated with a higher priority (a master proxy). Refer to *Volume 2: Getting Started* in the *Blue Coat ProxySG Configuration and Management Guide Suite* for information.

The SG200's Certificate is No Longer Valid After the IP Address Changes

If you move the SG200 from its original location or change the IP address for any reason, the SG200's security certificate might not be accepted the next time you open the Management Console. This is because the hostname no longer matches the hostname on the certificate. You must create a new certificate and then edit the HTTPS-Console service to use it. For information about creating a new certificate and editing the HTTPS-Console service, refer to *Volume 5: Securing the ProxySG* of the *Blue Coat ProxySG Configuration and Management Guide Suite*.

The SG200 Does Not Come Back Up After Rebooting

If the appliance is not coming back up after rebooting and the serial port is connected to terminal server (terminal concentrator) try the following:

1 Open an active session on the terminal server, noting any traffic being outputted.

2 Unplug the terminal server from the appliance.

Appendix A: Specifications

Environmental and Electrical

Important: **Any modifications to the unit, unless expressly approved by Blue Coat, can void the user's authority to operate the equipment.**

Enclosure (Einschließung)	19 inch rack-mountable with optional brackets, desktop, wall mount
Height (Höhe)	43.7 mm (1.72 in); 1 rack unit
Width (Breite)	191 mm (7.5 in)
Length (Länge)	356 mm (14 in)
Weight (Gewicht)	System 2.5 kg (5.6 lb), Power adapter 0.5 kg (1 lb)
Power Input, AC (for external adapter) (Stromversorgung)	100-240V, 1.8 A, 50/60 Hz
DC (for Server)	19V 3.42A
Disk Drives (Festplatte)	1 x 40 GB IDE ATA-100
Processors (Prozessor)	Transmeta TM5900 Crusoe Family
RAM (Speicher)	256 MB, 512 MB
Network (Netzwerk)	(2 on board) 10/100 Base-T Ethernet
Regulations (Regelungen)	
Safety (Schutz)	CSA C22.2 No. 60950-1/ UL60950-1 First edition, EN60950-1
Emissions (Emissionen)	FCC Class A, EN55022 Class A, VCCI Class A No. 1247859
Environmental (Umweltsmäßig)	
Temperature (Betriebstemperatur)	5° C to 35° C (41° F to 95° F)
Relative Humidity (Relative Luftfeuchte)	Less than 90% relative humidity, non-condensing
Maximum Altitude (Maximale Höhe)	Up to 2000 m (6561 ft)

Important: **The use of a wall-socket adapter is not recommended. Country-specific power cords are required to maintain product safety compliance and the warranty.**

Appendix B: Regulatory Statements

Any modification to this product, unless expressly approved by Blue Coat Systems, Inc., could void the user's authority to operate the equipment.

Class A Digital Warning

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

EC Community EMC Warning

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

Canadian EC EMC Warning

This Class A digital apparatus complies with Canadian ICES-003. Cet appareil numerique de la class A est conforme a la norme NMB-003 du Canada.

Australia/New Zealand EMC Warning

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

Taiwan BSMI Notification

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Japan VCCI EMC Notification

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

China CCC Notification

声　明
此为 A 级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

Battery Warning Notification

小心：如果电池安装不正确，会有爆炸危险。请仅使用生产厂家推荐的或同类型的电池进行更换。请根据生产厂家的说明处理用过的旧电池。

注意事項：如果電池未正確安裝，可能有爆炸的危險。請選用與製造商所推薦相同或相等型式的電池來進行替換。請依據製造商的指示處理使用過的電池。

CAUTION: Danger of explosion if battery is incorrectly placed. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

ATTENTION: Il y a danger d'explosion s'il y a remplacement incorrect de la batterie. Remplacer uniquement avec une batterie de meme type ou d'un type equivalent recommande par le constructeur. Metter au rebut less batteries usagees conformement aux instructions du fabricant.

VORSICHT! Explosionsgefahr bei unsachgemäßem Austausch der Batterie. Ersatz nur durch denselben oder einen vom Hersteller empfohlenen glelchwertigen Typ.

Entsorgung gebrauchter Batterien nach Angaben des Herstellers.

PRECAUCIÓN: Peligro de explosión si la batería es colocada incorrectamente. Substituya solo

con el modelo original o la recomendación del fabricante. Disponga de las baterías usadas según las instrucciones del fabricante.

Connection to ports not defined for normal operation, according to this manual, might result in excessive radiated emissions. The user is then responsible for all corrective action in the event of any problem.

Declaration of Conformity

Blue Coat Systems, Inc.
650 Almanor Avenue
Sunnyvale, CA 94085-3515 USA

Declaration of Conformity

We, Blue Coat Systems, Inc.
650 Almanor Avenue
Sunnyvale, CA 94085 USA

Declare under our sole responsibility that the products

Model 200

To which this declaration relates is in conformity with the following
Standards:

EN 60950-1: 2001
EN 55022: 1994
EN 50024: 1998

Following the provisions of the 73/23/EEC and 89/336/EEC Directives,
Including the Amending Directive 93/68/EEC

Sunnyvale, CA 94085 USA
Date: 11/12/04

Tim Redjaian
Director of Engineering

866.30.BCOAT Toll Free   408.220.2200 Direct   408.220.2250 Fax   www.bluecoat.com

Index