



Booting, Logging In, and Getting Started

This chapter describes how to boot the CSS for the first time and on a routine basis, and how to log in. It also covers using the configuration script, which initiates automatically when you log in *and* the CSS does not detect an existing startup-config file. Information in this chapter applies to all CSS models, except where noted.

This chapter contains the following major sections:

- [Booting the CSS for the First Time](#)
- [Booting the CSS on a Routine Basis](#)
- [Logging in to the CSS](#)
- [Using the Configuration Script](#)
- [Rebooting the CSS](#)
- [Shutting Down the CSS](#)

Booting the CSS for the First Time

Upon bootup, the CSS initially:

- Performs hardware initialization and power-on diagnostics (as described in the “[Booting the CSS on a Routine Basis](#)” section)
- Prompts you to:
 - Enter the Standard software license key
 - Configure the IP address, subnet mask, and default gateway for the Ethernet management port, used for CSS configuration and Ethernet management only; this port does not route traffic
 - Change the default administrative login name (**admin**) and password (**system**)
 - Password protect the Offline Diagnostic Monitor (Offline DM) menu

This sections includes the following procedures:

- [Entering Your License Key](#)
- [Configuring the Ethernet Management Port](#)
- [Changing the Default Username and Password](#)
- [Password Protecting the Offline DM Menu](#)

Entering Your License Key

When the CSS completes hardware initialization and power-on diagnostics, you must enter a valid Standard license key for the CSS software. The CSS does not require you to enter this key on subsequent startups.

Locate your Standard software license key inside the CSS accessory kit. If you cannot locate the software license key, call the Cisco Technical Assistance Center (TAC) toll free, 24 hours a day, 7 days a week at 1-800-553-2447 or 1-408-526-7209. You can also e-mail TAC at tac@cisco.com.

The CSS prompts you to accept the license agreement. You must accept the license agreement or you cannot log in to the CSS.

The CSS prompts you to enter your Standard software license key, as follows:

```
Enter Software License Key: xxxxxxxxxxxxxx
```

If you enter:

- A valid license number, the CSS prompts you to enter an IP address for the Ethernet management port.
- An invalid license number, the CSS redisplay the license prompt until you enter a valid number. If you do not enter a valid license number, you cannot log in to the CSS.

If, during the initial CSS order placement, you purchased the Enhanced feature set, the Secure Management option (which includes Secure Shell Host and SSL strong encryption for the Device Management software), or the Proximity Database software option, locate the software Claim Certificate in the accessory kit. Follow the instructions on the Claim Certificate to obtain a license key from Cisco Systems for the additional software feature.

After you receive the software license key, use the **license** command to enter the license key. At the prompt, enter the license key. For example, enter:

```
# license
Enter Software License Key (q to quit):
```

**Note**

After you enter the software license key for the Proximity Database software option, you must reboot the CSS for the license key to take effect.

Configuring the Ethernet Management Port

Once you enter a valid license key at the boot prompt, the CSS displays the following message and prompt:

```
Use the Ethernet management port IP address to access the Content
Services Switch for configuration and management only. This port does
not route traffic and is not associated with VLAN circuits.
```

```
The current address setting (0.0.0.0) disables the Ethernet Management
port.
```

```
Do you wish to configure a valid address for the Ethernet management
port [y/n]?
```

Enter one of the following:

- **y** to configure an IP address, subnet mask, and default gateway for the Ethernet management port. The CSS prompts you for an IP address, a subnet mask, then a default gateway. You must enter a valid IP address or the CSS repeats the prompt until you do.

```
Enter IP Address [0.0.0.0]:
Enter Subnet Mask [0.0.0.0]:
Enter Default Gateway [0.0.0.0]:
```



Note

The Ethernet management port IP address must be on a different subnet from any other CSS VLAN circuit subnet. If you do not make this IP address unique, you will not be able to access the port.

- **n** to accept the default IP address (0.0.0.0), subnet mask (0.0.0.0), and gateway (0.0.0.0) and to disable the port. The CSS does not prompt you for an IP address, subnet mask, and default gateway.

The Ethernet management port default IP address of 0.0.0.0 disables the Ethernet management port. To enable the Ethernet management port, specify the **ip address** command in boot mode (see [Chapter 2, Configuring CSS Basics](#)) or use the Offline DM menu (see [Appendix B, Using the Offline Diagnostic Monitor Menu](#)).

Changing the Default Username and Password

The CSS allows you to change the default username and password. We recommend that you change them to safeguard the CSS against unauthorized logins.

Access to this device is allowed using the default username and password. For enhanced security we recommend that you change the defaults. Do you want to change the defaults now (yes,no):

Enter one of the following:

- **yes** to change the username and password. The CSS prompts you for the following information and password confirmation.

```
Enter <administrator> username:
Enter <administrator> password:
Confirm <administrator> password:
```

- **no** to keep the default username and password.

To change the default username and password from the CLI, refer to [Chapter 3, Managing the CSS Software](#) for details.

Password Protecting the Offline DM Menu

The CSS prompts you to password-protect the Offline DM menu.

```
Set Password Protection for Offline Diagnostic Monitor menu (yes,no)
```



Caution

Use care when password protecting the Offline DM menu and ensure that you write down the new password. If you lose the new password, it cannot be recovered and you will be unable to access the Offline DM Main menu. The only solution, at that point, is to contact the Cisco Technical Assistance Center (TAC) at 1-800-553-2447 or 1-408-526-7209. You can also e-mail TAC at tac@cisco.com.

Enter one of the following:

- **yes** to password protect the Offline DM menu. When you password protect the Offline DM menu, you need to enter the administrative username and password each time you access the menu.

```
The administrative username and password are required to access  
the Offline Diagnostic Monitor menu.  
Initializing the disk.....OK
```

Refer to [Appendix B, Using the Offline Diagnostic Monitor Menu](#), for information on the Offline DM menu options.

- **no** to disable password protection on the Offline DM menu.

The CSS prompts you to access the Offline DM menu.

```
Would you like to access the Offline Diagnostic Monitor? (Y <cr>)
```

Enter **y** to access the Offline DM menu. If you do not wish to access the Offline DM menu after seeing this message, wait for the CSS to boot.

Booting the CSS on a Routine Basis

When you power up a CSS, the boot process:

- Displays the software version and build number
- Performs hardware initialization and power-on self tests
- Provides access to the Offline DM menu
- Prompts you to log in to the CSS

The duration of the boot process depends on the CSS startup configuration and, with the CSS 11503 and CSS 11506, the number of modules in the chassis.

When you boot the CSS, it initializes the hardware and performs power-on self tests. The CSS displays the following messages (shown for the CSS 11503 and CSS 11506):

```
Locked boot flash.  
Validating operational boot flash, please wait...  
Operational boot flash valid. Jumping to operational boot flash.  
Copyright 2002(c), Cisco Systems, Inc.
```

```
Operational boot flash.  
Attaching interrupt handlers...Done.  
Master SCM.  
Built Jun 22 2002 @ 15:14:20  
Version x.xx Build xx
```



Note

After the CSS begins to boot (approximately 15 seconds) the CSS allows you to access the Offline DM menu. The Offline DM Main menu allows you to set the boot configuration, display the boot configuration, select Advanced Options, or reboot the system. Refer to [Appendix B, Using the Offline Diagnostic Monitor Menu](#) for detailed information on using Offline DM.

The hardware then goes through a series of power-on self tests. The asterisks that appear indicate the completion of each test.

```
Press <ESC> to enter the Diagnostic Monitor
* * * * *
Ran 1 times, x tests. Detected 0 errors.
```

During the power-on self tests, the Status LEDs blink and change color to indicate the stages of the boot process. The left Status LED is bicolor, green or red. The right Status LED is amber.

The Ethernet connectors on the CSS 11501 and the 8- and 16-port Fast Ethernet Modules on the CSS 11503 or CSS 11506 do not contain Status LEDs. Each Ethernet connector has Link and Duplex LEDs to indicate the state of the connection.

[Table 1-1](#) defines the boot states and the blinking patterns of the Status LEDs.

Table 1-1 Status LEDs Boot Definitions

State Sequence		LED Color	LED State
1.	The CSS powers up, flash scans, and does a power-on self test.	Amber	Fast blink
	The CSS powers on and a self test detects an error.	Red	Solid
2.	The CSS 11501 or a module in the CSS 11503 or CSS 11506 is off line and active.	Amber	Slow blink
3.	The CSS 11501 or a module in the CSS 11503 or CSS 11506 is online and not active. In the CSS 11506, a passive SCM LED remains in this state and color.	Amber	Solid

Table 1-1 Status LEDs Boot Definitions (continued)

State Sequence	LED Color	LED State
4. The CSS 11501, or a module in the CSS 11503 or CSS 11506, is on line and active.	Green	Solid
The CSS 11501 or a module in the CSS 11503 or CSS 11506 (except a Fast Ethernet Module) failed. In the CSS 11503 or 11506, if: <ul style="list-style-type: none"> • A Fast Ethernet Module fails, all of the Link and Duplex LEDs blink simultaneously. • The master SCM in slot 1 detects a module failure, its Status LED is green and blinks slowly. • The master SCM in slot 1 fails, the CSS does not boot unless there is a passive SCM in slot 2. 	Red	Blinking
5. Disk activity	Green	Variable blinking

If an error occurs during a power-on self-test, the console displays an error message, increments the detected error counter, and continues to the next test until the CSS completes all of the power-on self tests. Refer to [Chapter 8, Using the CSS Logging Features](#) and [Appendix C, Troubleshooting the Boot Process](#) for more information on boot errors and messages.

Logging in to the CSS

After the CSS completes the boot process, it displays the login banner, copyright, and login prompt.

When a startup-config file is present, the CSS displays the message: `Press CTRL-C to abort running the startup-config`

**Note**

If the CSS does not detect an existing startup-config file, the CSS automatically initiates the configuration script (see the [“Using the Configuration Script”](#) section). The configuration script prompts you to enter configuration information. Subsequent logins to the CSS do not start the configuration script.

If you abort running the startup-config file, the CSS does not use the existing startup-config file. Aborting the use of the startup-config file enables you to log in and reconfigure the CSS to create a new running-config file. Use this feature if you misconfigure your startup-config file and the CSS becomes unusable.

When you log in from:

- A console, the CSS displays the message: `Press any key to log in.`
- A Telnet session, the message is not displayed.

The CSS prompts you to enter a username and password, as follows:

```
User Access Verification
Username:
Password
```

If you connect a console to the CSS after the CSS boots, your screen will be blank. Press **Enter** to display the username and password prompts.

To initially log in to the CSS, enter the default user name **admin** and the default password **system** as lowercase text, or enter the administrative username and password you configured during the boot process. For security, the CSS does not display the password. The default username **admin** enables you to log in with SuperUser status.

If you have not changed the default administrative username and password, we recommend that you change them to safeguard the CSS against unauthorized logins. To change the default username and password from the CLI, refer to [Chapter 2, Configuring CSS Basics](#).

Using the Configuration Script

When you log in to the CSS and it does not detect an existing startup-config file, the CSS automatically initiates the configuration script. During the running of the configuration script, the CSS prompts you to enter the following information:

- IP address and subnet mask for circuit VLAN1 (all interfaces are assigned to VLAN1 by default)
- IP address for the default gateway
- IP addresses for the servers
- Virtual IP address (VIP) for the content rule

Based on your entries, the configuration script allows you to create services, owners, and content rules. For background information on configuring services, owners, and content rules, refer to the *Cisco Content Services Switch Basic Configuration Guide*.

To accept the script default values, press the **Enter** key at the prompts shown in the configuration script. To quit the script, enter **q** at any prompt. If you quit running the script, you may proceed to [Chapter 2, Configuring CSS Basics](#) to continue the initial setup of the CSS.

**Note**

You may also initiate the configuration script manually by entering the **script play setup** command.

To clear an existing running-config file, use the **clear running-config** command from SuperUser mode. To clear an existing startup-config file, use the **clear startup-config** command from SuperUser mode.

The following example illustrates the configuration script including:

- **Bold** text to indicate user entry examples
- Explanations to help you use the script

```
#####  
#Setup Script for the Content Services Switch#  
#####
```

Checking for Existing Config...

No startup-config was found, continue with the setup script [y/n]? **y**

Note: Pressing "q" after any prompt quits setup. Pressing <CR> after any [y/n] defaults to "y".

Warning: All circuit VLAN IP addresses must be on a different subnet than the Ethernet Mgt port IP address. The existing Ethernet Mgt port IP address is: 10.0.4.251

Add an IP address to VLAN1: [default = 192.168.10.1] **192.168.3.6**

Add an IP subnet mask to VLAN1: [default = 255.255.255.0]

Warning: The default gateway IP address must be on the same subnet as VLAN1. VLAN1 IP address is: 192.168.3.6

Add IP address for default gateway: [default = 192.168.3.2]
192.168.3.3

Pinging the default gateway: 100% Success.

Which feature do you want to configure?

- [1] Layer3 load balancing
- [2] Layer5 load balancing
- [3] Proxy cache
- [4] Transparent cache
- [5] Exit script

[Table 1-2](#) describes each Configuration Script menu item.

Table 1-2 Configuration Script Menu Options

Menu Option	Function
Layer3 Load Balancing	Configure Layer 3 load balancing to enable the CSS to use a Virtual IP address (VIP) to load balance Web traffic to Web servers based on IP addresses
Layer5 Load Balancing	Configure Layer 5 load balancing to enable the CSS to use a VIP address to load balance Web traffic to Web servers based on URLs.
Proxy Cache	Configure proxy cache to enables the CSS to use a Virtual IP address (VIP) to load balance Web traffic to proxy cache servers based on domain name.
Transparent Cache	Configure transparent cache to enable the CSS to redirect cacheable HTTP traffic to transparent cache servers based on IP address and port (80).
Exit Script	Exit from the script and save the information you entered to the CSS running-config file. The CSS displays the running-config file.

Refer to the following sections for details about each item in the Configuration Script menu:

- [Configuring Layer 3 Load Balancing](#)
- [Configuring Layer 5 Load Balancing](#)
- [Configuring Proxy Cache](#)
- [Configuring Transparent Cache](#)

Configuring Layer 3 Load Balancing

A Layer 3 load-balancing configuration enables the CSS to use a Virtual IP address (VIP) to load balance Web traffic to Web servers based on IP addresses.

When you select Layer 3 load balancing, the script automatically:

- Creates an owner (L3_Owner)
- Creates a Layer 3 content rule (L3_Rule) and defines ArrowPoint Content Awareness (ACA) as the load balance method
- Activates the services
- Activates the content rule
- Saves the running configuration to the startup-config file

The script prompts you to configure:

- Service name (default name is Server1)
- Service IP address
- VIP for the content rule

To configure Layer 3 load balancing, enter **1** at the Configuration Script menu.

Which feature do you want to configure?

```
[1] Layer3 load balancing
[2] Layer5 load balancing
[3] Proxy cache
[4] Transparent cache
```

Enter the number for the feature you want to configure: **1**

To accept the script default values, press the **Enter** key at the prompts.

```
Creating Layer3 load balancing
```

```
Enter service name: [default = Server1]
```

```
Enter service IP address: [default = 192.168.10.3] 192.168.3.58
```

```
Create another service? [y/n]? y
```

```
Enter service name: [default = Server2]
```

```
Enter service IP address: [default = 192.168.10.3] 192.168.3.59
```

Create another service? [y/n]? **n**

Enter Virtual IP address for L3_Rule: [default = 192.168.10.4]
192.168.3.6

After you specify the configuration, the script automatically:

- Displays the running-config file
- Saves the running configuration to the startup-config file

Showing the Running Config

!Generated MAR 6 17:53:49

```
!***** GLOBAL *****
ip route 0.0.0.0 0.0.0.0 192.168.3.3
!***** CIRCUIT *****
circuit VLAN1
ip address 192.168.3.6 255.255.255.0
!***** SERVICE *****
service Server1
    ip address 192.168.3.58
    active
service Server2
    ip address 192.168.3.59
    active
!***** OWNER *****
owner L3_Owner
    content L3_Rule
    add service Server1
    add service Server2
    vip address 192.168.3.6
    balance aca
    active
#####
## Setup Completed Successfully!!! ##
#####
```

Configuring Layer 5 Load Balancing

A Layer 5 load-balancing configuration enables the CSS to use a VIP address to load balance Web traffic to Web servers based on URLs.

When you select Layer 5 load balancing, the script automatically:

- Creates an owner (L5_Owner)
- Creates a Layer 3 content rule (L3_Rule)
- Creates a Layer 5 content rule (L5_Rule) and defines:
 - Protocol TCP
 - Port 80
 - URL "/*"
 - Load balance method as ACA
- Activates the services
- Activates the content rule
- Saves the running configuration to the startup-config file

The script prompts you to configure:

- Service name (default name is Server1)
- VIP for the content rule

To configure Layer 5 load balancing, enter **2** at the Configuration Script menu..

```
Which feature do you want to configure?
```

```
[1] Layer3 load balancing
[2] Layer5 load balancing
[3] Proxy cache
[4] Transparent cache
```

```
Enter the number for the feature you want to configure: 2
```

To accept the script default values, press the **Enter** key at the prompts.

```
Creating Layer5 load balancing
```

```
Enter service name: [default= Server1]
```

```
Enter service IP address: [default = 192.168.10.3] 192.168.3.58
```

Create another service? [y/n]? **n**

Enter Virtual IP address for L5_Rule: [default = 192.168.10.4]
192.168.3.8

After you specify the configuration, the script automatically:

- Displays the running-config file
- Saves the running configuration to the startup-config file

Showing the Running Config

!Generated MAR 6 17:53:49

```
!***** GLOBAL *****
ip route 0.0.0.0 0.0.0.0 192.168.3.3
!***** CIRCUIT *****
circuit VLAN1
ip address 192.168.3.6 255.255.255.0
!***** SERVICE *****
service Server1
    ip address 192.168.3.58
    active
!***** OWNER *****
owner L5_Owner
content L3_Rule
    add service Server1
    vip address 192.168.3.8
    balance aca
    active
content L5_Rule
    add service Server1
    vip address 192.168.3.8
    protocol tcp
    port 80
    url "/*"
    balance aca
    active
#####
##      Setup Completed Successfully!!!  ##
#####
```

Configuring Proxy Cache

A proxy cache configuration enables the CSS to use a Virtual IP address (VIP) to load balance Web traffic to proxy cache servers based on domain name.

When you select Proxy Cache, the script automatically:

- Creates an owner (Proxy_Owner)
- Creates a content rule (Proxy_Rule) and defines:
 - Service type as proxy-cache
 - Protocol TCP
 - Port 8080
 - URL "/*"
 - Load balance method as domain
 - Application type HTTP
- Activates the services
- Activates the content rule

The script prompts you to configure:

- Service name (default name is Proxy_Cache1)
- VIP for the content rule

To configure a proxy cache configuration, enter **3** at the Configuration Script menu.

Which feature do you want to configure?

```
[1] Layer3 load balancing
[2] Layer5 load balancing
[3] Proxy cache
[4] Transparent cache
```

Enter the number for the feature you want to configure: **3**

To accept the script default values, press the **Enter** key at the prompts.

Creating Proxy Cache Configuration

Enter service name: [default=Proxy_Cache1]

Enter service IP address: [default = 192.168.10.3] **192.168.3.60**

```
Create another service? [y/n]? n
```

```
Enter Virtual IP address for Proxy_Rule: [default = 192.168.10.4]
192.168.3.9
```

After you specify the configuration, the script automatically:

- Displays the running-config file
- Saves the running configuration to the startup-config file

```
Showing the Running Config
!Generated MAR 6 17:53:49
!***** GLOBAL *****
ip route 0.0.0.0 0.0.0.0 192.168.3.3
!***** CIRCUIT *****
circuit VLAN1
ip address 192.168.3.6 255.255.255.0
!***** SERVICE *****
service Proxy_Cache1
    ip address 192.168.3.60
    type proxy-cache
    port 8080
    protocol tcp
    active
!***** OWNER *****
owner Proxy_Owner
content Proxy_Rule
    add service Proxy_Cache1
    vip address 192.168.3.9
    port 8080
    protocol tcp
    url "/*"
    balance domain
    application http
    active

#####
##      Setup Completed Successfully!!!  ##
#####
```

Configuring Transparent Cache

A transparent cache configuration enables the CSS to redirect cacheable HTTP traffic to transparent cache servers based on IP address and port (80). The CSS directs non-cacheable HTTP traffic to the origin servers.

When you select Transparent Cache, the script automatically:

- Creates an owner (Transparent_Owner)
- Creates a content rule (Transparent_Rule) and defines:
 - Service type as transparent-cache
 - Protocol TCP
 - Port 80
 - Extension Qualifier List (EQL) named *Cacheable* that contains the file types displayed in the sample running-config file
 - URL "/"* eql cacheable
 - Load balance method as domain
 - Failover type as bypass
 - Application type HTTP
- Activates the services
- Activates the content rule

The script enables you to:

- Configure a service name (Transparent_Cache1)
- Define whether to direct only cacheable content or all content to the cache servers

To configure a transparent cache configuration, enter **4** at the Configuration Script menu.

Which feature do you want to configure?

```
[1] Layer3 load balancing
[2] Layer5 load balancing
[3] Proxy cache
[4] Transparent cache
```

Enter the number for the feature you want to configure: **4**

To accept the script default values, press the **Enter** key at the prompts.

Creating Transparent Cache Configuration

Enter service name: [default = Transparent_Cache1]

Enter service IP address: [default = 0.0.0.0] **192.168.3.7**

Create another service? [y/n]? **n**

Transparent caching can be configured to direct only cacheable content to the cache server. Non-cacheable content is sent directly to the origin server.

The alternative is to direct all traffic to the cache server regardless of whether the content is cacheable.

Should only cacheable content be directed to the cache server? [y/n]?

Enter one of the following:

- **y** to define URL “/*” as epl-cacheable in the content rule and allow the CSS to direct only cacheable content to the cache servers.
- **n** to define URL “/*” in the content rule and allow the CSS to direct all content to the cache servers.

After you specify the configuration, the script automatically:

- Displays the running-config file
- Saves the running configuration to the startup-config file

Showing the Running Config

!Generated MAR 6 17:53:49

```
!***** GLOBAL *****
ip route 0.0.0.0 0.0.0.0 192.168.3.3
!***** CIRCUIT *****
circuit VLAN1
ip address 192.168.3.6 255.255.255.0
!***** SERVICE *****
service Transparent_Cache1
    ip address 192.168.3.7
    type transparent-cache
    port 80
    protocol tcp
    active
```

```
!***** EQL *****
eql Cacheable
description "This EQL contains
  extensions of cacheable content"
extension pdf "Acrobat"
extension fdf "Acrobat Forms Document"
extension au "Sound audio/basic"
extension bmp "Bitmap Image"
extension z "Compressed data
  application/x-compress"
extension gif "GIF Image image/gif"
extension html "Hypertext Markup
  Language text/html"
extension htm
extension js "Java script
  application/x-javascript"
extension mocha
extension jpeg "JPEG image image/jpeg"
extension jpg
extension jpe
extension jfif
extension pjpeg
extension pjp
extension mp2 "MPEG Audio audio/x-mpeg"
extension mpa
extension abs
extension mpeg "MPEG Video video/mpeg"
extension mpg
extension mpe
extension mpv
extension vbs
extension mlv
extension pcx "PCX Image"
extension txt "Plain text text/plain"
extension text
extension mov "QuickTime video/quicktime"
extension tiff "TIFF Image image/tiff"
extension tar "Unix Tape Archive
  application/x-tar"
extension avi "Video for Windows
  video/x-msvideo"
extension wav "Wave File audio/x-wav"
extension gz "application/x-gzip"
extension zip "ZIP file
  application/x-zip-compressed"
```

```

!***** OWNER *****
owner Transparent_Owner
content Transparent_Rule
    add service Transparent_Cache1
        port 80
        protocol tcp
        url "/" eq1 Cacheable or url "/"
        balance domain
        failover bypass
        application http
        active
#####
##      Setup Completed Successfully!!!  ##
#####

```

Rebooting the CSS

Use the **reboot** command to reboot the CSS. This command is supported in all modes except user mode.

Before you enter the **reboot** command, save an existing running-config file prior to rebooting the CSS by using the **copy running-config startup-config** command from SuperUser mode. If you are not in expert mode, the CSS displays the prompts to save profile and configuration changes before it reboots. To save an existing running-config file prior to rebooting the CSS, use the **copy running-config startup-config** command from SuperUser mode.

To reboot the CSS:

```
(config)# reboot
```

Shutting Down the CSS

Use the **shutdown** command to shut down the CSS. This command shuts down all CSS processes so you can power cycle the unit safely. The **shutdown** command is supported in all modes except in user mode.

To shut down the CSS:

```
(config)# shutdown
```

Where to Go Next

[Chapter 2, Configuring CSS Basics](#) describes the initial configuration procedures for the CSS, such as changing the administrative username and password, creating usernames and passwords, configuring the Ethernet management port, specifying a static IP address and subnet mask, and changing the date and time.

■ Where to Go Next