Using the Web-Browser and CLI Interfaces

This chapter describes how to initially configure and log into the controller. It contains these sections:

- Configuring the Controller Using the GUI Configuration Wizard, page 3-1
- Configuring the Controller Using the CLI Configuration Wizard, page 3-13
- Using the Controller Web GUI, page 3-16
- Loading an Externally Generated SSL Certificate, page 3-20
- Using the Controller CLI, page 3-22
- Using the AutoInstall Feature for Controllers Without a Configuration, page 3-26
- Managing the Controller System Date and Time, page 3-30
- Configuring Telnet and SSH Sessions, page 3-35
- Managing the Controller Wirelessly, page 3-37

Configuring the Controller Using the GUI Configuration Wizard

The configuration wizard enables you to configure basic settings on the controller. You can run the wizard after you receive the controller from the factory or after the controller has been reset to factory defaults. The configuration wizard is available in GUI or CLI format.

This section contains the following topics:

- Connecting the Controller’s Console Port, page 3-1
- Configuring the Controller (GUI), page 3-2
- Additional References, page 3-13

Connecting the Controller’s Console Port

Before you can configure the controller for basic operations, you need to connect it to a PC that uses a VT-100 terminal emulation program (such as HyperTerminal, ProComm, Minicom, or Tip).
Chapter 3 Using the Web-Browser and CLI Interfaces

Configuring the Controller Using the GUI Configuration Wizard

Note
On Cisco 5500 Series Controllers, you can use either the RJ-45 console port or the USB console port. If you use the USB console port, plug the 5-pin mini Type B connector into the controller’s USB console port and the other end of the cable into the PC’s USB Type A port. The first time that you connect a Windows PC to the USB console port, you are prompted to install the USB console driver. Follow the installation prompts to install the driver. The USB console driver maps to a COM port on your PC; you then need to map the terminal emulator application to the COM port.

Step 1 Connect one end of a null-modem serial cable to the controller’s console port and the other end to your PC’s serial port.

Step 2 Start the PC’s VT-100 terminal emulation program.

Step 3 Configure the terminal emulation program for these parameters:
- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- No hardware flow control

Step 4 Plug the AC power cord into the controller and a grounded 100 to 240 VAC, 50/60-Hz electrical outlet. Turn on the power supply. The bootup script displays operating system software initialization (code download and power-on self test verification) and basic configuration.

If the controller passes the power-on self test, the bootup script runs the configuration wizard, which prompts you for basic configuration input.

Configuring the Controller (GUI)

Step 1 Connect your PC to the service port and configure it to use the same subnet as the controller (for example, 209.165.200.225).

Step 2 Start Internet Explorer 6.0 SP1 (or later) or Firefox 2.0.0.11 (or later) on your PC and browse to http://209.165.200.225. The configuration wizard appears.
Step 3  In the System Name text box, enter the name that you want to assign to this controller. You can enter up to 31 ASCII characters.

Step 4  In the User Name text box, enter the administrative username to be assigned to this controller. You can enter up to 24 ASCII characters. The default username is admin.

Step 5  In the Password and Confirm Password text boxes, enter the administrative password to be assigned to this controller. You can enter up to 24 ASCII characters. The default password is admin.

Starting in release 7.0.116.0, the following password policy has been implemented:

- The password must contain characters from at least three of the following classes:
  - Lowercase letters
  - Uppercase letters
  - Digits
  - Special characters.
- No character in the password must be repeated more than three times consecutively.
- The new password must not be the same as the associated username and not be the username reversed.
- The password must not be cisco, ocsic, or any variant obtained by changing the capitalization of letters of the word Cisco. In addition, you cannot substitute 1, 1, or ! for i, 0 for o, or $ for s..

Step 6  Click Next. The SNMP Summary screen appears.
Step 7  If you want to enable Simple Network Management Protocol (SNMP) v1 mode for this controller, choose Enable from the SNMP v1 Mode drop-down list. Otherwise, leave this parameter set to Disable.

**Note**  SNMP manages nodes (servers, workstations, routers, switches, and so on) on an IP network. Currently, there are three versions of SNMP: SNMPv1, SNMPv2c, and SNMPv3.

Step 8  If you want to enable SNMPv2c mode for this controller, leave this parameter set to Enable. Otherwise, choose Disable from the SNMP v2c Mode drop-down list.

Step 9  If you want to enable SNMPv3 mode for this controller, leave this parameter set to Enable. Otherwise, choose Disable from the SNMPv3 Mode drop-down list.

Step 10  Click Next.

Step 11  When the following message appears, click OK:

Default values are present for v1/v2c community strings. Please make sure to create new v1/v2c community strings once the system comes up. Please make sure to create new v3 users once the system comes up.

The Service Interface Configuration screen appears.
### Step 12
If you want the controller’s service-port interface to obtain an IP address from a DHCP server, select the **DHCP Protocol Enabled** check box. If you do not want to use the service port or if you want to assign a static IP address to the service port, leave the check box unselected.

**Note**
The service-port interface controls communications through the service port. Its IP address must be on a different subnet from the management interface. This configuration enables you to manage the controller directly or through a dedicated management network to ensure service access during network downtime.

### Step 13
Perform one of the following:

- If you enabled DHCP in **Step 12**, clear out any entries in the IP Address and Netmask text boxes, leaving them blank.
- If you disabled DHCP in **Step 12**, enter the static IP address and netmask for the service port in the IP Address and Netmask text boxes.

### Step 14
Click **Next**. The LAG Configuration screen appears.
Step 15  To enable link aggregation (LAG), choose Enabled from the Link Aggregation (LAG) Mode drop-down list. To disable LAG, leave this text box set to Disabled.

Step 16  Click Next. The Management Interface Configuration screen appears.

Figure 3-5  Configuration Wizard — Management Interface Configuration Screen

Note  The management interface is the default interface for in-band management of the controller and connectivity to enterprise services such as AAA servers.
Step 17 In the VLAN Identifier text box, enter the VLAN identifier of the management interface (either a valid VLAN identifier or 0 for an untagged VLAN). The VLAN identifier should be set to match the switch interface configuration.

Step 18 In the IP Address text box, enter the IP address of the management interface.

Step 19 In the Netmask text box, enter the IP address of the management interface netmask.

Step 20 In the Gateway text box, enter the IP address of the default gateway.

Step 21 In the Port Number text box, enter the number of the port assigned to the management interface. Each interface is mapped to at least one primary port.

Step 22 In the Backup Port text box, enter the number of the backup port assigned to the management interface. If the primary port for the management interface fails, the interface automatically moves to the backup port.

Step 23 In the Primary DHCP Server text box, enter the IP address of the default DHCP server that will supply IP addresses to clients, the controller’s management interface, and optionally, the service port interface.

Step 24 In the Secondary DHCP Server text box, enter the IP address of an optional secondary DHCP server that will supply IP addresses to clients, the controller’s management interface, and optionally, the service port interface.

Step 25 Click Next. The AP-Manager Interface Configuration screen appears.

**Note** This screen does not appear for Cisco 5500 Series Controllers because you are not required to configure an AP-manager interface. The management interface acts like an AP-manager interface by default.

Step 26 In the IP Address text box, enter the IP address of the AP-manager interface.

Step 27 Click Next. The Miscellaneous Configuration screen appears.

*Figure 3-6 Configuration Wizard — Miscellaneous Configuration Screen*

Step 28 In the RF Mobility Domain Name text box, enter the name of the mobility group/RF group to which you want the controller to belong.
Configuring the Controller Using the GUI Configuration Wizard

**Note**
Although the name that you enter here is assigned to both the mobility group and the RF group, these groups are not identical. Both groups define clusters of controllers, but they have different purposes. All of the controllers in an RF group are usually also in the same mobility group and vice versa. However, a mobility group facilitates scalable, system-wide mobility and controller redundancy while an RF group facilitates scalable, system-wide dynamic RF management.

**Step 29**
The Configured Country Code(s) text box shows the code for the country in which the controller will be used. If you want to change the country of operation, select the check box for the desired country.

**Note**
You can choose more than one country code if you want to manage access points in multiple countries from a single controller. After the configuration wizard runs, you need to assign each access point joined to the controller to a specific country. See the “Configuring Country Codes” section on page 9-87 for instructions.

**Step 30**
Click **Next**.

**Step 31**
When the following message appears, click **OK**:

*Warning! To maintain regulatory compliance functionality, the country code setting may only be modified by a network administrator or qualified IT professional. Ensure that proper country codes are selected before proceeding.*

The Virtual Interface Configuration screen appears.

**Figure 3-7  Configuration Wizard — Virtual Interface Configuration Screen**

**Step 32**
In the IP Address text box, enter the IP address of the controller’s virtual interface. You should enter a fictitious, unassigned IP address.

**Note**
The virtual interface is used to support mobility management, DHCP relay, and embedded Layer 3 security such as guest web authentication and VPN termination. All controllers within a mobility group must be configured with the same virtual interface IP address.
Step 33 In the DNS Host Name text box, enter the name of the Domain Name System (DNS) gateway used to verify the source of certificates when Layer 3 web authorization is enabled.

**Note** To ensure connectivity and web authentication, the DNS server should always point to the virtual interface. If a DNS host name is configured for the virtual interface, then the same DNS host name must be configured on the DNS servers used by the client.

Step 34 Click Next. The WLAN Configuration screen appears.

**Figure 3-8 Configuration Wizard — WLAN Configuration Screen**

Step 35 In the Profile Name text box, enter up to 32 alphanumeric characters for the profile name to be assigned to this WLAN.

Step 36 In the WLAN SSID text box, enter up to 32 alphanumeric characters for the network name, or service set identifier (SSID). The SSID enables basic functionality of the controller and allows access points that have joined the controller to enable their radios.

Step 37 Click Next.

Step 38 When the following message appears, click OK:

Default Security applied to WLAN is: [WPA2(AES)][Auth(802.1x)]. You can change this after the wizard is complete and the system is rebooted.

The RADIUS Server Configuration screen appears.
Step 39 In the Server IP Address text box, enter the IP address of the RADIUS server.

Step 40 From the Shared Secret Format drop-down list, choose ASCII or Hex to specify the format of the shared secret.

Note Due to security reasons, the RADIUS shared secret key reverts to ASCII mode even if you have selected HEX as the shared secret format from the Shared Secret Format drop-down list.

Step 41 In the Shared Secret and Confirm Shared Secret text boxes, enter the secret key used by the RADIUS server.

Step 42 In the Port Number text box, enter the communication port of the RADIUS server. The default value is 1812.

Step 43 To enable the RADIUS server, choose Enabled from the Server Status drop-down list. To disable the RADIUS server, leave this text box set to Disabled.

Step 44 Click Apply. The 802.11 Configuration screen appears.
Figure 3-10  Configuration Wizard — 802.11 Configuration Screen

Step 45  To enable the 802.11a, 802.11b, and 802.11g lightweight access point networks, leave the **802.11a Network Status**, **802.11b Network Status**, and **802.11g Network Status** check boxes selected. To disable support for any of these networks, unselect the check boxes.

Step 46  To enable the controller’s radio resource management (RRM) auto-RF feature, leave the **Auto RF** check box selected. To disable support for the auto-RF feature, unselect this check box.

**Note**  The auto-RF feature enables the controller to automatically form an RF group with other controllers. The group dynamically elects a leader to optimize RRM parameter settings, such as channel and transmit power assignment, for the group.

Step 47  Click **Next**. The Set Time screen appears.
Figure 3-11  Configuration Wizard — Set Time Screen

Step 48  To manually configure the system time on your controller, enter the current date in Month/DD/YYYY format and the current time in HH:MM:SS format.

Step 49  To manually set the time zone so that Daylight Saving Time (DST) is not set automatically, enter the local hour difference from Greenwich Mean Time (GMT) in the Delta Hours text box and the local minute difference from GMT in the Delta Mins text box.

Note  When manually setting the time zone, enter the time difference of the local current time zone with respect to GMT (+/−). For example, Pacific time in the United States is 8 hours behind GMT. Therefore, it is entered as −8.

Step 50  Click Next. The Configuration Wizard Completed screen appears.
Figure 3-12  Configuration Wizard — Configuration Wizard Completed Screen

Step 51  Click **Save and Reboot** to save your configuration and reboot the controller.

Step 52  When the following message appears, click **OK**:

> Configuration will be saved and the controller will be rebooted. Click ok to confirm.

Step 53  The controller saves your configuration, reboots, and prompts you to log in. Follow the instructions in the “Using the Controller Web GUI” section on page 3-16 to log into the controller.

Additional References

- “Resetting the Controller to Default Settings” section on page 4-116 for instructions on returning the controller to factory defaults.
- Chapter 13, “Configuring Radio Resource Management,”
- Chapter 15, “Configuring Mobility Groups,”
- See the“SNMP Community Strings” section on page 4-40 and the “Changing the Default Values for SNMP v3 Users” section on page 4-42.

Configuring the Controller Using the CLI Configuration Wizard

This section contains the following topics:

- **Guidelines and Limitations**, page 3-14
- **Configuring the Controller (CLI)**, page 3-14
Guidelines and Limitations

- The available options appear in brackets after each configuration parameter. The default value appears in all uppercase letters.
- If you enter an incorrect response, the controller provides you with an appropriate error message, such as “Invalid Response,” and returns you to the wizard prompt.
- Press the hyphen key if you ever need to return to the previous command line.

Configuring the Controller (CLI)

**Step 1**
When prompted to terminate the AutoInstall process, enter yes. If you do not enter yes, the AutoInstall process begins after 30 seconds.

*Note*
The AutoInstall feature downloads a configuration file from a TFTP server and then loads the configuration onto the controller automatically. See the “Using the AutoInstall Feature for Controllers Without a Configuration” section on page 3-26 for more information.

**Step 2**
Enter the system name, which is the name that you want to assign to the controller. You can enter up to 31 ASCII characters.

**Step 3**
Enter the administrative username and password to be assigned to this controller. You can enter up to 24 ASCII characters for each.

Starting in release 7.0.116.0, the following password policy has been implemented:
- The password must contain characters from at least three of the following classes:
  - Lowercase letters
  - Uppercase letters
  - Digits
  - Special characters.
- No character in the password must be repeated more than three times consecutively.
- The new password must not be the same as the associated username and not be the username reversed.
- The password must not be cisco, ocsic, or any variant obtained by changing the capitalization of letters of the word Cisco. In addition, you cannot substitute 1, I, or ! for i, 0 for o, or $ for s.

**Step 4**
If you want the controller’s service-port interface to obtain an IP address from a DHCP server, enter DHCP. If you do not want to use the service port or if you want to assign a static IP address to the service port, enter none.

*Note* The service-port interface controls communications through the service port. Its IP address must be on a different subnet from the management interface. This configuration enables you to manage the controller directly or through a dedicated management network to ensure service access during network downtime.

**Step 5**
If you entered none in Step 4, enter the IP address and netmask for the service-port interface on the next two lines.
Step 6  Enable or disable link aggregation (LAG) by choosing **yes** or **NO**.

Step 7  Enter the IP address of the management interface.

**Note**  The management interface is the default interface for in-band management of the controller and connectivity to enterprise services such as AAA servers.

Step 8  Enter the IP address of the management interface netmask.

Step 9  Enter the IP address of the default router.

Step 10 Enter the VLAN identifier of the management interface (either a valid VLAN identifier or **0** for an untagged VLAN). The VLAN identifier should be set to match the switch interface configuration.

Step 11 Enter the IP address of the default DHCP server that will supply IP addresses to clients, the controller’s management interface, and optionally, the service port interface. Enter the IP address of the AP-manager interface.

**Note**  This prompt does not appear for Cisco 5500 Series Controllers because you are not required to configure an AP-manager interface. The management interface acts like an AP-manager interface by default.

Step 12 Enter the IP address of the controller’s virtual interface. You should enter a fictitious unassigned IP address.

**Note**  The virtual interface is used to support mobility management, DHCP relay, and embedded Layer 3 security such as guest web authentication and VPN termination. All controllers within a mobility group must be configured with the same virtual interface IP address.

Step 13 If desired, enter the name of the mobility group/RF group to which you want the controller to belong.

**Note**  Although the name that you enter here is assigned to both the mobility group and the RF group, these groups are not identical. Both groups define clusters of controllers, but they have different purposes. All of the controllers in an RF group are usually also in the same mobility group and vice versa. However, a mobility group facilitates scalable, system-wide mobility and controller redundancy while an RF group facilitates scalable, system-wide dynamic RF management.

Step 14 Enter the network name or service set identifier (SSID). The SSID enables basic functionality of the controller and allows access points that have joined the controller to enable their radios.

Step 15 Enter **YES** to allow clients to assign their own IP address or **no** to require clients to request an IP address from a DHCP server.

Step 16 To configure a RADIUS server now, enter **YES** and then enter the IP address, communication port, and secret key of the RADIUS server. Otherwise, enter **no**. If you enter no, the following message appears: “Warning! The default WLAN security policy requires a RADIUS server. Please see the documentation for more details.”

Step 17 Enter the code for the country in which the controller will be used.

**Note**  Enter **help** to view the list of available country codes.
You can enter more than one country code if you want to manage access points in multiple countries from a single controller. To do so, separate the country codes with a comma (for example, US,CA,MX). After the configuration wizard runs, you need to assign each access point joined to the controller to a specific country.

Step 18
Enable or disable the 802.11b, 802.11a, and 802.11g lightweight access point networks by entering YES or no.

Step 19
Enable or disable the controller’s radio resource management (RRM) auto-RF feature by entering YES or no.

Note
The auto-RF feature enables the controller to automatically form an RF group with other controllers. The group dynamically elects a leader to optimize RRM parameter settings, such as channel and transmit power assignment, for the group.

Step 20
If you want the controller to receive its time setting from an external Network Time Protocol (NTP) server when it powers up, enter YES to configure an NTP server. Otherwise, enter no.

Note
The controller network module installed in a Cisco Integrated Services Router does not have a battery and cannot save a time setting. Therefore, it must receive a time setting from an external NTP server when it powers up.

Step 21
If you entered no in Step 20 and want to manually configure the system time on your controller now, enter YES. If you do not want to configure the system time now, enter no.

Step 22
If you entered YES in Step 21, enter the current date in MM/DD/YY format and the current time in HH:MM:SS format.

Step 23
When prompted to verify that the configuration is correct, enter yes or NO.

The controller saves your configuration, reboots, and prompts you to log in. Follow the instructions in the “Using the Controller CLI” section on page 3-22 to log into the controller.

Using the Controller Web GUI

A web browser, or graphical user interface (GUI), is built into each controller. It allows up to five users to simultaneously browse into the controller HTTP or HTTPS (HTTP + SSL) management pages to configure parameters and monitor the operational status for the controller and its associated access points.

This section contains the following topics:
- Guidelines and Limitations, page 3-17
- Logging On to the GUI, page 3-17
- Logging Out of the GUI, page 3-17
- Enabling Web and Secure Web Modes, page 3-18
Guidelines and Limitations

Follow these guidelines when using the controller GUI:

- The GUI must be used on a PC running Windows XP SP1 (or later) or Windows 2000 SP4 (or later).
- The GUI is fully compatible with Microsoft Internet Explorer version 6.0 SP1 (or later) or Mozilla Firefox 2.0.0.11 (or later). Internet Explorer 6.0 SP1 (or later) and Mozilla Firefox 2.0.0.11 (or later) are the only browsers supported for accessing the controller GUI and for using web authentication.
- Opera is not supported.
- You can use either the service port interface or the management interface to access the GUI. We recommend that you use the service-port interface. See Chapter 4, “Configuring Ports and Interfaces,” for instructions on configuring the service port interface.
- Click Help at the top of any page in the GUI to display online help. You might need to disable your browser’s pop-up blocker to view the online help.
- We recommend that you enable the HTTPS interface and disable the HTTP interface to ensure more robust security for your Cisco UWN solution.

Logging On to the GUI

**Step 1** Enter the controller IP address in your browser’s address line. For a secure connection, enter `https://ip-address`. For a less secure connection, enter `http://ip-address`.

*Note* See the “Enabling Web and Secure Web Modes” section on page 3-18 for instructions on setting up HTTPS.

**Step 2** When prompted, enter a valid username and password and click OK. The controller Summary page appears.

*Note* The administrative username and password that you created in the configuration wizard are case sensitive. The default username is *admin*, and the default password is *admin*.

Logging Out of the GUI

**Step 1** Click Logout in the top right corner of the page.

**Step 2** Click Close to complete the logoff process and prevent unauthorized users from accessing the controller GUI.

**Step 3** When prompted to confirm your decision, click Yes.
Enabling Web and Secure Web Modes

This section provides instructions for enabling the distribution system port as a web port (using HTTP) or as a secure web port (using HTTPS). You can protect communication with the GUI by enabling HTTPS. HTTPS protects HTTP browser sessions by using the Secure Socket Layer (SSL) protocol. When you enable HTTPS, the controller generates its own local web administration SSL certificate and automatically applies it to the GUI. You also have the option of downloading an externally generated certificate. This section contains the following topics:

- Enabling Web and Secure Web Modes (GUI), page 3-18
- Enabling Web and Secure Web Modes (CLI), page 3-19

Enabling Web and Secure Web Modes (GUI)

**Step 1** Choose Management > HTTP to open the HTTP Configuration page.

**Figure 3-13 HTTP Configuration Page**

To enable web mode, which allows users to access the controller GUI using “http://ip-address,” choose Enabled from the HTTP Access drop-down list. Otherwise, choose Disabled. The default value is Disabled. Web mode is not a secure connection.

To enable secure web mode, which allows users to access the controller GUI using “https://ip-address,” choose Enabled from the HTTPS Access drop-down list. Otherwise, choose Disabled. The default value is Enabled. Secure web mode is a secure connection.

In the Web Session Timeout text box, enter the amount of time (in minutes) before the web session times out due to inactivity. You can enter a value between 30 and 160 minutes (inclusive), and the default value is 30 minutes.

Click Apply to commit your changes.
Step 6  If you enabled secure web mode in Step 3, the controller generates a local web administration SSL certificate and automatically applies it to the GUI. The details of the current certificate appear in the middle of the HTTP Configuration page.

**Note**  If you want to download your own SSL certificate to the controller, follow the instructions in the “Loading an Externally Generated SSL Certificate” section on page 3-20.

**Note**  If desired, you can delete the current certificate by clicking **Delete Certificate** and have the controller generate a new certificate by clicking **Regenerate Certificate**.

Step 7  Click **Save Configuration** to save your changes.

### Enabling Web and Secure Web Modes (CLI)

**Step 1**  To enable or disable web mode, enter this command:
```
config network webmode {enable | disable}
```
This command allows users to access the controller GUI using “http://ip-address.” The default value is disabled. Web mode is not a secure connection.

**Step 2**  To enable or disable secure web mode, enter this command:
```
config network secureweb {enable | disable}
```
This command allows users to access the controller GUI using “https://ip-address.” The default value is enabled. Secure web mode is a secure connection.

**Step 3**  To enable or disable secure web mode with increased security, enter this command:
```
config network secureweb cipher-option high {enable | disable}
```
This command allows users to access the controller GUI using “https://ip-address” but only from browsers that support 128-bit (or larger) ciphers. The default value is disabled.

**Step 4**  To enable or disable SSLv2 for web administration, enter this command:
```
config network secureweb cipher-option sslv2 {enable | disable}
```
If you disable SSLv2, users cannot connect using a browser configured with SSLv2 only. They must use a browser that is configured to use a more secure protocol such as SSLv3 or later. The default value is enabled.

**Step 5**  To verify that the controller has generated a certificate, enter this command:
```
show certificate summary
```
Information similar to the following appears:

```
Web Administration Certificate................. Locally Generated
Web Authentication Certificate................. Locally Generated
Certificate compatibility mode:............... off
```

**Note**  If you want to download your own SSL certificate to the controller, follow the instructions in the “Loading an Externally Generated SSL Certificate” section on page 3-20.
Step 6  (Optional) If you need to generate a new certificate, enter this command:

```bash
config certificate generate webadmin
```

After a few seconds, the controller verifies that the certificate has been generated.

Step 7  To save the SSL certificate, key, and secure web password to nonvolatile RAM (NVRAM) so that your changes are retained across reboots, enter this command:

```bash
save config
```

Step 8  To reboot the controller, enter this command:

```bash
reset system
```

---

### Loading an Externally Generated SSL Certificate

You can use a TFTP server to download an externally generated SSL certificate to the controller.

This section contains the following topics:

- Guidelines and Limitations, page 3-20
- Loading an SSL Certificate, page 3-20

### Guidelines and Limitations

- If you load the certificate through the service port, the TFTP server must be on the same subnet as the controller because the service port is not routable, or you must create static routes on the controller. Also, if you load the certificate through the distribution system network port, the TFTP server can be on any subnet.

- A third-party TFTP server cannot run on the same PC as the Cisco WCS because the WCS built-in TFTP server and the third-party TFTP server require the same communication port.

- Chained certificates are supported for web authentication only and not for the management certificate.

- Every HTTPS certificate contains an embedded RSA key. The length of the key can vary from 512 bits, which is relatively insecure, to thousands of bits, which is very secure. When you obtain a new certificate from a Certificate Authority, make sure that the RSA key embedded in the certificate is at least 768 bits long.

### Loading an SSL Certificate

This section contains the following topics:

- Loading an SSL Certificate (GUI), page 3-20
- Loading an SSL Certificate (CLI), page 3-21

### Loading an SSL Certificate (GUI)

Step 1  On the HTTP Configuration page, select the **Download SSL Certificate** check box.
Figure 3-14  HTTP Configuration Page

Step 2  In the Server IP Address text box, enter the IP address of the TFTP server.
Step 3  In the Maximum Retries text box, enter the maximum number of times that the TFTP server attempts to download the certificate.
Step 4  In the Timeout text box, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.
Step 5  In the Certificate File Path text box, enter the directory path of the certificate.
Step 6  In the Certificate File Name text box, enter the name of the certificate (webadmincert_name.pem).
Step 7  (Optional) In the Certificate Password text box, enter a password to encrypt the certificate.
Step 8  Click Apply to commit your changes.
Step 9  Click Save Configuration to save your changes.
Step 10  To reboot the controller for your changes to take effect, choose Commands > Reboot > Reboot > Save and Reboot.

Loading an SSL Certificate (CLI)

Step 1  Use a password to encrypt the HTTPS certificate in a .PEM-encoded file. The PEM-encoded file is called a web administration certificate file (webadmincert_name.pem).
Step 2  Move the webadmincert_name.pem file to the default directory on your TFTP server.
Step 3  To view the current download settings, enter this command and answer n to the prompt:

```
transfer download start
```

Information similar to the following appears:

```
Mode........................................... TFTP
Data Type...................................... Admin Cert
TFTP Server IP................................. xxx.xxx.xxx.xxx
TFTP Path...................................... <directory path>
```
Step 4  Use these commands to change the download settings:

```
transfer download mode tftp
transfer download datatype weauthcert
transfer download serverip TFTP_server_IP_address
transfer download path absolute_TFTP_server_path_to_the_update_file
transfer download filename webadmincert_name.pem
```

Step 5  To set the password for the .PEM file so that the operating system can decrypt the web administration SSL key and certificate, enter this command:

```
transfer download certpassword private_key_password
```

Step 6  To confirm the current download settings and start the certificate and key download, enter this command and answer y to the prompt:

```
transfer download start
```

Information similar to the following appears:

```
Mode........................................... TFTP
Data Type...................................... Site Cert
TFTP Server IP................................. xxx.xxx.xxx.xxx
TFTP Path...................................... directory path
TFTP Filename.................................. webadmincert_name
Are you sure you want to start? (y/n) y
TFTP Weadmin cert transfer starting.
Certificate installed.
```

Step 7  To save the SSL certificate, key, and secure web password to NVRAM so that your changes are retained across reboots, enter this command:

```
save config
```

Step 8  To reboot the controller, enter this command:

```
reset system
```

## Using the Controller CLI

This section contains the following topics:

- Information About the Controller CLI, page 3-23
- Guidelines and Limitations, page 3-23
- Logging on to the Controller CLI, page 3-23
- Using a Local Serial Connection, page 3-23
- Using a Remote Ethernet Connection, page 3-24
- Logging Out of the CLI, page 3-25
- Navigating the CLI, page 3-25
Information About the Controller CLI

A Cisco UWN solution command-line interface (CLI) is built into each controller. The CLI enables you to use a VT-100 terminal emulation program to locally or remotely configure, monitor, and control individual controllers and its associated lightweight access points. The CLI is a simple text-based, tree-structured interface that allows up to five users with Telnet-capable terminal emulation programs to access the controller.

Guidelines and Limitations

- On Cisco 5500 Series Controllers, you can use either the RJ-45 console port or the USB console port. If you use the USB console port, plug the 5-pin mini Type B connector into the controller’s USB console port and the other end of the cable into the PC’s USB Type A port. The first time that you connect a Windows PC to the USB console port, you are prompted to install the USB console driver. Follow the installation prompts to install the driver. The USB console driver maps to a COM port on your PC; you then need to map the terminal emulator application to the COM port.
- If you want to input any strings from the XML configuration into CLI commands, you must enclose the strings in quotation marks.

Logging on to the Controller CLI

You access the controller CLI using one of two methods:

- A direct serial connection to the controller console port
- A remote console session over Ethernet through the preconfigured service port or the distribution system ports

Before you log on to the CLI, configure your connectivity and environment variables based on the type of connection you use.

Using a Local Serial Connection

You need these items to connect to the serial port:

- A PC that is running a VT-100 terminal emulation program (such as HyperTerminal, ProComm, Minicom, or Tip)
- A null-modem serial cable

To log into the controller CLI through the serial port, follow these steps:

**Step 1** Connect one end of a null-modem serial cable to the controller’s console port and the other end to your PC’s serial port.

**Step 2** Start the PC’s VT-100 terminal emulation program. Configure the terminal emulation program for these parameters:
- 9600 baud
Using the Controller CLI

- 8 data bits
- 1 stop bit
- No parity
- No hardware flow control

**Note**  The controller serial port is set for a 9600 baud rate and a short timeout. If you would like to change either of these values, enter `config serial baudrate baudrate` and `config serial timeout timeout` to make your changes. If you enter `config serial timeout 0`, serial sessions never time out.

**Step 3**  When prompted, enter a valid username and password to log into the controller. The administrative username and password that you created in the configuration wizard are case sensitive.

**Note**  The default username is `admin`, and the default password is `admin`.

The CLI displays the root level system prompt:

```
#(system prompt)>
```

**Note**  The system prompt can be any alphanumeric string up to 31 characters. You can change it by entering the `config prompt` command.

---

**Using a Remote Ethernet Connection**

You need these items to connect to a controller remotely:

- A PC with access to the controller over the Ethernet network
- The IP address of the controller
- A VT-100 terminal emulation program or a DOS shell for the Telnet session

**Note**  By default, controllers block Telnet sessions. You must use a local connection to the serial port to enable Telnet sessions.

To log into the controller CLI through a remote Ethernet connection, follow these steps:

**Step 1**  Verify that your VT-100 terminal emulation program or DOS shell interface is configured with these parameters:

- Ethernet address
- Port 23

**Step 2**  Use the controller IP address to Telnet to the CLI.
Step 3  When prompted, enter a valid username and password to log into the controller. The administrative username and password that you created in the configuration wizard are case sensitive.

Note  The default username is admin, and the default password is admin.

The CLI displays the root level system prompt:

```
# (system prompt) >
```

Note  The system prompt can be any alphanumeric string up to 31 characters. You can change it by entering the `config prompt` command.

---

**Logging Out of the CLI**

When you finish using the CLI, navigate to the root level and enter `logout`. The system prompts you to save any changes you made to the volatile RAM.

Note  The CLI automatically logs you out without saving any changes after 5 minutes of inactivity. You can set the automatic logout from 0 (never log out) to 160 minutes using the `config serial timeout` command.

---

**Navigating the CLI**

The CLI is organized around five levels:
- Root Level
- Level 2
- Level 3
- Level 4
- Level 5

When you log into the CLI, you are at the root level. From the root level, you can enter any full command without first navigating to the correct command level. Table 3-1 lists commands you use to navigate the CLI and to perform common tasks.

**Table 3-1  Commands for CLI Navigation and Common Tasks**

<table>
<thead>
<tr>
<th>Command</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>help</td>
<td>At the root level, view system wide navigation commands</td>
</tr>
<tr>
<td>?</td>
<td>View commands available at the current level</td>
</tr>
<tr>
<td>command ?</td>
<td>View parameters for a specific command</td>
</tr>
<tr>
<td>exit</td>
<td>Move down one level</td>
</tr>
<tr>
<td>Ctrl-Z</td>
<td>Return from any level to the root level</td>
</tr>
</tbody>
</table>
Using the AutoInstall Feature for Controllers Without a Configuration

This section contains the following topics:

- Information About the AutoInstall Feature, page 3-26
- Guidelines and Limitations, page 3-27
- Obtaining an IP Address Through DHCP and Downloading a Configuration File from a TFTP Server, page 3-27
- Selecting a Configuration File, page 3-28
- Example: AutoInstall Operation, page 3-29
- Additional References, page 3-30

Information About the AutoInstall Feature

When you boot up a controller that does not have a configuration, the AutoInstall feature can download a configuration file from a TFTP server and then load the configuration onto the controller automatically.

If you create a configuration file on a controller that is already on the network (or through a WCS filter), place that configuration file on a TFTP server, and configure a DHCP server so that a new controller can get an IP address and TFTP server information, the AutoInstall feature can obtain the configuration file for the new controller automatically.

When the controller boots, the AutoInstall process starts. The controller does not take any action until AutoInstall is notified that the configuration wizard has started. If the wizard has not started, the controller has a valid configuration.

If AutoInstall is notified that the configuration wizard has started (which means that the controller does not have a configuration), AutoInstall waits for an additional 30 seconds. This time period gives you an opportunity to respond to the first prompt from the configuration wizard:

Would you like to terminate autoinstall? [yes]:

---

Table 3-1 Commands for CLI Navigation and Common Tasks

<table>
<thead>
<tr>
<th>Command</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>save config</td>
<td>At the root level, save configuration changes from active working RAM</td>
</tr>
<tr>
<td></td>
<td>(NVRAM) so they are retained after reboot</td>
</tr>
<tr>
<td>reset system</td>
<td>At the root level, reset the controller without logging out</td>
</tr>
</tbody>
</table>

Additional References

- See the Cisco Wireless LAN Controller Command Reference for information on specific commands.
- See the “Configuring Telnet and SSH Sessions” section on page 3-35 for information on enabling Telnet sessions.
When the 30-second abort timeout expires, AutoInstall starts the DHCP client. You can abort the AutoInstall task even after this 30-second timeout if you enter Yes at the prompt. However, AutoInstall cannot be aborted if the TFTP task has locked the flash and is in the process of downloading and installing a valid configuration file.

Guidelines and Limitations

AutoInstall uses the following interfaces:

- Cisco 5500 Series Controllers
  - eth0—Service port (untagged)
  - dtl0—Gigabit port 1 through the NPU (untagged)

Obtaining an IP Address Through DHCP and Downloading a Configuration File from a TFTP Server

AutoInstall attempts to obtain an IP address from the DHCP server until the DHCP process is successful or until you abort the AutoInstall process. The first interface to successfully obtain an IP address from the DHCP server registers with the AutoInstall task. The registration of this interface causes AutoInstall to begin the process of obtaining TFTP server information and downloading the configuration file.

Following the acquisition of the DHCP IP address for an interface, AutoInstall begins a short sequence of events to determine the host name of the controller and the IP address of the TFTP server. Each phase of this sequence gives preference to explicitly configured information over default or implied information and to explicit host names over explicit IP addresses.

The process is as follows:

- If at least one Domain Name System (DNS) server IP address is learned through DHCP, AutoInstall creates a /etc/resolv.conf file. This file includes the domain name and the list of DNS servers that have been received. The Domain Name Server option provides the list of DNS servers, and the Domain Name option provides the domain name.
- If the domain servers are not on the same subnet as the controller, static route entries are installed for each domain server. These static routes point to the gateway that is learned through the DHCP Router option.
- The host name of the controller is determined in this order by one of the following:
  - If the DHCP Host Name option was received, this information (truncated at the first period [.]) is used as the host name for the controller.
  - A reverse DNS lookup is performed on the controller IP address. If DNS returns a hostname, this name (truncated at the first period [.]) is used as the hostname for the controller.
- The IP address of the TFTP server is determined in this order by one of the following:
  - If AutoInstall received the DHCP TFTP Server Name option, AutoInstall performs a DNS lookup on this server name. If the DNS lookup is successful, the returned IP address is used as the IP address of the TFTP server.
  - If the DHCP Server Host Name (sname) text box is valid, AutoInstall performs a DNS lookup on this name. If the DNS lookup is successful, the IP address that is returned is used as the IP address of the TFTP server.
If AutoInstall received the DHCP TFTP Server Address option, this address is used as the IP address of the TFTP server.

AutoInstall performs a DNS lookup on the default TFTP server name (cisco-wlc-tftp). If the DNS lookup is successful, the IP address that is received is used as the IP address of the TFTP server.

If the DHCP server IP address (siaddr) text box is nonzero, this address is used as the IP address of the TFTP server.

The limited broadcast address (255.255.255.255) is used as the IP address of the TFTP server.

- If the TFTP server is not on the same subnet as the controller, a static route (/32) is installed for the IP address of the TFTP server. This static route points to the gateway that is learned through the DHCP Router option.

Selecting a Configuration File

After the hostname and TFTP server have been determined, AutoInstall attempts to download a configuration file. AutoInstall performs three full download iterations on each interface that obtains a DHCP IP address. For example, if a Cisco 4400 Series Controller obtains DHCP IP addresses on both eth0 and dtl0, each interface tries to download a configuration. If the interface cannot download a configuration file successfully after three attempts, the interface does not attempt further.

The first configuration file that is downloaded and installed successfully triggers a reboot of the controller. After the reboot, the controller runs the newly downloaded configuration.

AutoInstall searches for configuration files in the order in which the names are listed:

- The filename that is provided by the DHCP Boot File Name option
- The filename that is provided by the DHCP File text box
- `host name-confg`
- `host name.cfg`
- `base MAC address-confg` (for example, 0011.2233.4455-confg)
- `serial number-confg`
- `ciscowlc-confg`
- `ciscowlc.cfg`

AutoInstall runs through this list until it finds a configuration file. It stops running if it does not find a configuration file after it cycles through this list three times on each registered interface.

---

**Note**
The downloaded configuration file can be a complete configuration, or it can be a minimal configuration that provides enough information for the controller to be managed by WCS. Full configuration can then be deployed directly from WCS.

**Note**
The autoinstall does not expect the switch connected to the controller to be configured for either channels. Autoinstall works with service port in lag-configuration.
Note

For information about creating and uploading a configuration file that AutoInstall can obtain from a TFTP server, see Chapter 11, “Managing Controller Software and Configurations.”

Note

WCS release 5.0 and later releases provide AutoInstall capabilities for controllers. A WCS administrator can create a filter that includes the host name, the MAC address, or the serial number of the controller and associate a group of templates (a configuration group) to this filter rule. WCS pushes the initial configuration to the controller when the controller boots up initially. After the controller is discovered, WCS pushes the templates that are defined in the configuration group. For more information about the AutoInstall feature and WCS, see Chapter 15 of the Cisco Wireless Control System Configuration Guide, Release 7.0.172.0.

Example: AutoInstall Operation

The following is an example of an AutoInstall process from start to finish:

Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
Would you like to terminate autoinstall? [yes]:
AUTO-INSTALL: starting now...
AUTO-INSTALL: interface 'service-port' - setting DHCP TFTP Filename ==> 'abcd-confg'
AUTO-INSTALL: interface 'service-port' - setting DHCP TFTP Server IP ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP siaddr ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP Domain Server[0] ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP Domain Name ==> 'engtest.com'
AUTO-INSTALL: interface 'service-port' - setting DHCP yiaddr ==> 172.19.29.253
AUTO-INSTALL: interface 'service-port' - setting DHCP Netmask ==> 255.255.255.0
AUTO-INSTALL: interface 'service-port' - setting DHCP Gateway ==> 172.19.29.1
AUTO-INSTALL: interface 'service-port' registered
AUTO-INSTALL: iteration 1 -- interface 'service-port'
AUTO-INSTALL: DNS reverse lookup 172.19.29.253 ==> 'wlc-1'
AUTO-INSTALL: hostname 'wlc-1'
AUTO-INSTALL: TFTP server 1.100.108.2 (from DHCP Option 150)
AUTO-INSTALL: attempting download of 'abcd-confg'
AUTO-INSTALL: TFTP status - 'TFTP Config transfer starting.' (2)
AUTO-INSTALL: interface 'management' - setting DHCP file ==> 'bootfile1'
AUTO-INSTALL: interface 'management' - setting DHCP TFTP Filename ==> 'bootfile2-confg'
AUTO-INSTALL: interface 'management' - setting DHCP siaddr ==> 1.100.108.2
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[0] ==> 1.100.108.2
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[1] ==> 1.100.108.3
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[2] ==> 1.100.108.4
AUTO-INSTALL: interface 'management' - setting DHCP Domain Name ==> 'engtest.com'
AUTO-INSTALL: interface 'management' - setting DHCP yiaddr ==> 1.100.108.238
AUTO-INSTALL: interface 'management' - setting DHCP Netmask ==> 255.255.254.0
AUTO-INSTALL: interface 'management' - setting DHCP Gateway ==> 1.100.108.1
AUTO-INSTALL: interface 'management' registered
AUTO-INSTALL: TFTP status - 'Config file transfer failed - Error from server: File not found' (3)
AUTO-INSTALL: attempting download of 'wlc-1-confg'
AUTO-INSTALL: TFTP status - 'TFTP Config transfer starting.' (2)
AUTO-INSTALL: TFTP status - 'TFTP receive complete... updating configuration.' (2)
AUTO-INSTALL: TFTP status - 'TFTP receive complete... storing in flash.' (2)
AUTO-INSTALL: TFTP status - 'System being reset.' (2)

Resetting system
Managing the Controller System Date and Time

This section contains the following topics:

- Information About Controller System Date and Time, page 3-30
- Guidelines and Limitations, page 3-30
- Configuring an NTP Server to Obtain the Date and Time, page 3-30
- Configuring NTP Authentication, page 3-31
- Configuring the Date and Time, page 3-32

Information About Controller System Date and Time

You can configure the controller system date and time at the time of configuring the controller using the configuration wizard. If you did not configure the system date and time through the configuration wizard or if you want to change your configuration, you can follow the instructions in this section to configure the controller to obtain the date and time from a Network Time Protocol (NTP) server or to configure the date and time manually. Greenwich Mean Time (GMT) is used as the standard for setting the time zone on the controller.

You can also configure an authentication mechanism between various NTP servers.

Guidelines and Limitations

- If you are configuring wIPS, you must set the controller time zone to UTC.
- Cisco Aironet lightweight access points might not connect to the controller if the date and time are not set properly. Set the current date and time on the controller before allowing the access points to connect to it.
- Starting in the 7.0.116.0 release, you can configure an authentication channel between the controller and the NTP server.

Configuring an NTP Server to Obtain the Date and Time

Each NTP server IP address is added to the controller database. Each controller searches for an NTP server and obtains the current time upon reboot and at each user-defined polling interval (daily to weekly).

Additional References

- For information about configuring DHCP on a controller, See the “Configuring WLANs” section on page 8-8.
- For information about configuring a TFTP server on a controller, see Chapter 11, “Managing Controller Software and Configurations.”
- For information about configuring DHCP and TFTP servers through WCS, see Chapter 10 of the Cisco Wireless Control System Configuration Guide.
Use these commands to configure an NTP server to obtain the date and time:

- To specify the NTP server for the controller, enter this command:
  \[\text{config time ntp server index ip_address}\]
- To specify the polling interval (in seconds), enter this command:
  \[\text{config time ntp interval}\]

### Configuring NTP Authentication

This section contains the following topics:

- Configuring NTP Authentication (GUI), page 3-31
- Configuring NTP Authentication (CLI), page 3-31

#### Configuring NTP Authentication (GUI)

1. Choose Controller > NTP > Servers to open the NTP Servers page.
2. Click New to add an NTP server.
   - The NTP Servers > New page appears
3. Select a server priority from the Server Index (Priority) from the drop-down list.
4. Enter the NTP server IP Address in the Server IP Address text box.
5. Enable NTP server authentication by selecting the NTP Server Authentication check box.
6. Click Apply.
7. Choose Controller > NTP > Keys.
8. Click New to create a key.
9. Enter the key index in the Key Index text box.
10. Select the key format from the Key Format drop-down list.
11. Enter the Key in the Key text box.
12. Click Apply.

#### Configuring NTP Authentication (CLI)

**Note** By default MD5 is used.

- \[\text{config time ntp auth enable server-index key-index}\]
- \[\text{config time ntp auth disable server-index}\]
- \[\text{config time ntp key-auth add key-index md5 key-format key}\]
- To delete an authentication key, use the following command:
  \[\text{config time ntp key-auth delete key-index}\]
To view the list of NTP key Indices, use the following command:

```show ntp-keys```

### Configuring the Date and Time

This section contains the following topics:

- Configuring the Date and Time (GUI), page 3-32
- Configuring the Date and Time (CLI), page 3-33

### Configuring the Date and Time (GUI)

**Step 1** Choose **Commands > Set Time** to open the Set Time page.

**Figure 3-15 Set Time Page**

The current date and time appear at the top of the page.

**Step 2** In the Timezone area, choose your local time zone from the Location drop-down list.

**Note** When you choose a time zone that uses Daylight Saving Time (DST), the controller automatically sets its system clock to reflect the time change when DST occurs. In the United States, DST starts on the second Sunday in March and ends on the first Sunday in November.

**Note** You cannot set the time zone delta on the controller GUI. However, if you do so on the controller CLI, the change is reflected in the Delta Hours and Mins text boxes on the controller GUI.

**Step 3** Click **Set Timezone** to apply your changes.

**Step 4** In the Date area, choose the current local month and day from the Month and Day drop-down lists, and enter the year in the Year text box.
Managing the Controller System Date and Time

Step 5 In the Time area, choose the current local hour from the Hour drop-down list, and enter the minutes and seconds in the Minutes and Seconds text boxes.

---

Note: If you change the time zone location after setting the date and time, the values in the Time area are updated to reflect the time in the new time zone location. For example, if the controller is currently configured for noon Eastern time and you change the time zone to Pacific time, the time automatically changes to 9:00 a.m.

Step 6 Click Set Date and Time to apply your changes.

Step 7 Click Save Configuration to save your changes.

Configuring the Date and Time (CLI)

Step 1 To configure the current local date and time in GMT on the controller, enter this command:

```
config time manual mm/dd/yy hh:mm:ss
```

---

Note: When setting the time, the current local time is entered in terms of GMT and as a value between 00:00 and 24:00. For example, if it is 8:00 a.m. Pacific time in the United States, you would enter 16:00 because the Pacific time zone is 8 hours behind GMT.

Step 2 Perform one of the following to set the time zone for the controller:

- To set the time zone location in order to have Daylight Saving Time (DST) set automatically when it occurs, enter this command:

```
config time timezone location location_index
```

where `location_index` is a number representing one of the following time zone locations:

1. (GMT-12:00) International Date Line West
2. (GMT-11:00) Samoa
3. (GMT-10:00) Hawaii
4. (GMT-9:00) Alaska
5. (GMT-8:00) Pacific Time (US and Canada)
6. (GMT-7:00) Mountain Time (US and Canada)
7. (GMT-6:00) Central Time (US and Canada)
8. (GMT-5:00) Eastern Time (US and Canada)
9. (GMT-4:00) Atlantic Time (Canada)
10. (GMT-3:00) Buenos Aires (Argentina)
11. (GMT-2:00) Mid-Atlantic
12. (GMT-1:00) Azores
13. (GMT) London, Lisbon, Dublin, Edinburgh (default value)
14. (GMT +1:00) Amsterdam, Berlin, Rome, Vienna
15. (GMT +2:00) Jerusalem
16. (GMT +3:00) Baghdad
17. (GMT +4:00) Muscat, Abu Dhabi
18. (GMT +4:30) Kabul
19. (GMT +5:00) Karachi, Islamabad, Tashkent
20. (GMT +5:30) Colombo, Kolkata, Mumbai, New Delhi
21. (GMT +5:45) Katmandu
22. (GMT +6:00) Almaty, Novosibirsk
23. (GMT +6:30) Rangoon
24. (GMT +7:00) Saigon, Hanoi, Bangkok, Jakarta
25. (GMT +8:00) Hong Kong, Beijing, Chongqing
26. (GMT +9:00) Tokyo, Osaka, Sapporo
27. (GMT +9:30) Darwin
28. (GMT+10:00) Sydney, Melbourne, Canberra
29. (GMT+11:00) Magadan, Solomon Is., New Caledonia
30. (GMT+12:00) Kamchatka, Marshall Is., Fiji
31. (GMT+12:00) Auckland (New Zealand)

Note: If you enter this command, the controller automatically sets its system clock to reflect DST when it occurs. In the United States, DST starts on the second Sunday in March and ends on the first Sunday in November.

- To manually set the time zone so that DST is not set automatically, enter this command:

```
config time timezone delta_hours delta_mins
```

where `delta_hours` is the local hour difference from GMT, and `delta_mins` is the local minute difference from GMT.

When manually setting the time zone, enter the time difference of the local current time zone with respect to GMT (+/-). For example, Pacific time in the United States is 8 hours behind GMT. Therefore, it is entered as –8.

Note: You can manually set the time zone and prevent DST from being set only on the controller CLI.

Step 3 To save your changes, enter this command:

```
save config
```

Step 4 To verify that the controller shows the current local time with respect to the local time zone, enter this command:

```
show time
```

Information similar to the following appears:

```
Time......................... Thu Apr 7 13:56:37 2011
Timezone delta................. 0:0
Timezone location............... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
```
Configuring Telnet and SSH Sessions

This section contains the following topics:

- Information About Telnet and SSH, page 3-35
- Guidelines and Limitations, page 3-35
- Configuring Telnet and SSH Sessions, page 3-35
- Additional References, page 3-37

Information About Telnet and SSH

Telnet is a network protocol used to provide access to the controller’s CLI. Secure Shell (SSH) is a more secure version of Telnet that uses data encryption and a secure channel for data transfer. You can use the controller GUI or CLI to configure Telnet and SSH sessions.

Guidelines and Limitations

- Only the FIPS approved algorithm aes128-cbc is supported when using SSH to control WLANs.
- The controller does not support raw Telnet mode.

Configuring Telnet and SSH Sessions

This section contains the following topics:

- Configuring Telnet and SSH Sessions (GUI), page 3-35
- Configuring Telnet and SSH Sessions (CLI), page 3-36

Configuring Telnet and SSH Sessions (GUI)

Step 1  Choose Management > Telnet-SSH to open the Telnet-SSH Configuration page.
Step 2 In the Telnet Login Timeout text box, enter the number of minutes that a Telnet session is allowed to remain inactive before being terminated. The valid range is 0 to 160 minutes (inclusive), and the default value is 5 minutes. A value of 0 indicates no timeout.

Step 3 From the Maximum Number of Sessions drop-down list, choose the number of simultaneous Telnet or SSH sessions allowed. The valid range is 0 to 5 sessions (inclusive), and the default value is 5 sessions. A value of zero indicates that Telnet/SSH sessions are disallowed.

Step 4 From the Allow New Telnet Sessions drop-down list, choose Yes or No to allow or disallow new Telnet sessions on the controller. The default value is No.

Step 5 From the Allow New SSH Sessions drop-down list, choose Yes or No to allow or disallow new SSH sessions on the controller. The default value is Yes.

Step 6 Click Apply to commit your changes.

Step 7 Click Save Configuration to save your changes.

Step 8 To see a summary of the Telnet configuration settings, choose Management > Summary. The Summary page appears. This page shows whether additional Telnet and SSH sessions are permitted.

### Configuring Telnet and SSH Sessions (CLI)

**Step 1** To allow or disallow new Telnet sessions on the controller, enter this command:

```
config network telnet { enable | disable }
```

The default value is disabled.

**Step 2** To allow or disallow new SSH sessions on the controller, enter this command:

```
config network ssh { enable | disable }
```

The default value is enabled.

**Step 3** To specify the number of minutes that a Telnet session is allowed to remain inactive before being terminated, enter this command:

```
config sessions timeout timeout
```
where \textit{timeout} is a value between 0 and 160 minutes (inclusive). The default value is 5 minutes. A value of 0 indicates no timeout.

**Step 4** To specify the number of simultaneous Telnet or SSH sessions allowed, enter this command:

\texttt{config sessions maxsessions session\_num}

where \textit{session\_num} is a value between 0 and 5 (inclusive). The default value is 5 sessions. A value of zero indicates that Telnet/SSH sessions are disallowed.

**Step 5** To save your changes, enter this command:

\texttt{save config}

**Step 6** To see the Telnet and SSH configuration settings, enter this command:

\texttt{show network summary}

Information similar to the following appears:

<table>
<thead>
<tr>
<th>RF-Network Name</th>
<th>Web Mode</th>
<th>Secure Web Mode</th>
<th>Secure Web Mode Cipher-Option High</th>
<th>Secure Web Mode Cipher-Option SSLv2</th>
<th>Secure Shell (ssh)</th>
<th>Telnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>TestNetwork1</td>
<td>Enable</td>
<td>Enable</td>
<td>Disable</td>
<td>Enable</td>
<td>Enable</td>
<td>Disable</td>
</tr>
</tbody>
</table>

**Step 7** To see the Telnet session configuration settings, enter this command:

\texttt{show sessions}

Information similar to the following appears:

<table>
<thead>
<tr>
<th>CLI Login Timeout (minutes)</th>
<th>Maximum Number of CLI Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

**Step 8** To see all active Telnet sessions, enter this command:

\texttt{show loginsession}

Information similar to the following appears:

<table>
<thead>
<tr>
<th>ID</th>
<th>User Name</th>
<th>Connection From</th>
<th>Idle Time</th>
<th>Session Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>admin</td>
<td>EIA-232</td>
<td>00:00:00</td>
<td>00:19:04</td>
</tr>
</tbody>
</table>

**Step 9** If you ever want to close all active Telnet sessions or a specific Telnet session, enter this command:

\texttt{config loginsession close \{all | session\_id\}}

### Additional References

See the “Troubleshooting” section on page 18-1 for instructions on using Telnet or SSH to troubleshoot lightweight access points.

### Managing the Controller Wirelessly

This section contains the following topics:
Information About Managing the Controller Wirelessly

You can monitor and configure controllers using a wireless client. This feature is supported for all management tasks except uploads from and downloads to the controller.

Before you can open the GUI or the CLI from a wireless client device, you must configure the controller to allow the connection.

Enabling Wireless Connections

This section contains the following topics:

- Enabling Wireless Connections (GUI), page 3-38
- Enabling Wireless Connections (CLI), page 3-38

Enabling Wireless Connections (GUI)

Step 1 Log on to the controller GUI.
Step 2 Choose Management > Mgmt Via Wireless page.
Step 3 Enable the Enable Controller Management to be accessible from Wireless Clients checkbox.
Step 4 Click Apply.

Enabling Wireless Connections (CLI)

Step 1 Log on to the controller CLI.
Step 2 Enter the `config network mgmt-via-wireless enable` command.
Step 3 Use a wireless client to associate to a lightweight access point connected to the controller.
Step 4 On the wireless client, open a Telnet session to the controller, or browse to the controller GUI.