Using the Web Graphical User Interface

- Prerequisites for Using the Web GUI, page 1
- Information About Using The Web GUI, page 1
- Connecting the Console Port of the Controller, page 3
- Logging On to the Web GUI, page 3
- Enabling Web and Secure Web Modes, page 3
- Configuring the Controller Web GUI, page 4

Prerequisites for Using the Web GUI

- The controller GUI is compatible with Microsoft Internet Explorer 6.0 and 7.0, and Mozilla Firefox up to version 26.0.

Information About Using The Web GUI

A web browser, or graphical user interface (GUI), is built into each controller.

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. 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.

Web GUI Features

The controller web GUI supports the following:

The Configuration Wizard—After initial configuration of the IP address and the local username/password or auth via the authentication server (privilege 15 needed), the wizard provides a method to complete the initial wireless configuration. Start the wizard through Configuration -> Wizard and follow the nine-step process to configure the following:
Web GUI Features

- Admin Users
- SNMP System Summary
- Management Port
- Wireless Management
- RF Mobility and Country code
- Mobility configuration
- WLANs
- 802.11 Configuration
- Set Time

The Monitor tab:
- Displays summary details of controller, clients, and access points.
- Displays all radio and AP join statistics.
- Displays air quality on access points.
- Displays list of all Cisco Discovery Protocol (CDP) neighbors on all interfaces and the CDP traffic information.
- Displays all rogue access points based on their classification-friendly, malicious, ad hoc, classified, and unclassified.

The Configuration tab:
- Enables you to configure the controller for all initial operation using the web Configuration Wizard. The wizard allows you to configure user details, management interface, and so on.
- Enables you to configure the system, internal DHCP server, management, and mobility management parameters.
- Enables you to configure the controller, WLAN, and radios.
- Enables you to configure and set security policies on your controller.
- Enables you to access the controller operating system software management commands.

The Administration tab enables you to configure system logs.
Connecting the Console Port of the Controller

Before You Begin
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).

Step 1
Connect one end of a null-modem serial cable to the controller's RJ-45 console port and the other end to your PC's serial port.

Step 2
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.

Step 3
Enter yes. Proceed with basic initial setup configuration parameters in the CLI setup wizard. Specify the IP address for the service port which is the gigabitethernet 0/0 interface. After entering the configuration parameters in the configuration wizard, you can access the Web GUI. Now, the controller is configured with the IP address for service port.

Logging On to the Web GUI

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

Step 2
When prompted, enter a valid username and password and click OK.

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 cisco.

The Accessing page appears.

Enabling Web and Secure Web Modes

Step 1
Choose Configuration > Controller > Management > Protocol Management > HTTP-HTTPS.

The HTTP-HTTPS Configuration page appears.

Step 2
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. Web mode (HTTP) is not a secure connection.
Step 3 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. Secure web mode (HTTPS) is a secure connection.

Step 4 Choose to track the device in the IP Device Tracking check box.

Step 5 Choose to enable the trust point in the Enable check box.

Step 6 Choose the trustpoints from the Trustpoints drop-down list.

Step 7 Enter the amount of time, in seconds, before the web session times out due to inactivity in the HTTP Timeout-policy (1 to 600 sec) text box.

Step 8 Enter the server life time in the Server Life Time (1 to 86400 sec) text box.

Step 9 Enter the maximum number of connection requests that the server can accept in the Maximum number of Requests (1 to 86400) text box.

Step 10 Click Apply.

Step 11 Click Save Configuration.

Configuring the Controller Web GUI

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 both GUI and CLI formats.

Step 1 Connect your PC to the service port and configure an IPv4 address to use the same subnet as the controller. The controller is loaded with IOS XE image and the service port interface is configured as gigabitethernet 0/0.

Step 2 Start Internet Explorer 10 (or later), Firefox 2.0.0.11 (or later), or Google Chrome on your PC and enter the management interface IP address on the browser window. The management interface IP address is same as the gigabitethernet 0/0 (also known as service port interface). When you log in for the first time, you need to enter HTTP username and password. By default, the username is admin and the password is cisco. You can use both HTTP and HTTPS when using the service port interface. HTTPS is enabled by default and HTTP can also be enabled.

When you log in for the first time, the Accessing Cisco Controller <Model Number> <Hostname> page appears.

Step 3 On the Accessing Cisco Controller page, click the Wireless Web GUI link to access controller web GUI Home page.

Step 4 Choose Configuration > Wizard to perform all steps that you need to configure the controller initially. The Admin Users page appears.

Step 5 On the Admin Users page, enter the administrative username to be assigned to this controller in the User Name text box and the administrative password to be assigned to this controller in the Password and Confirm Password text boxes. Click Next.

The default username is admin and the default password is cisco. You can also create a new administrator user for the controller. You can enter up to 24 ASCII characters for username and password.
The SNMP System Summary page appears.

**Step 6**
On the SNMP System Summary page, enter the following SNMP system parameters for the controller, and click Next:

- Customer-definable controller location in the Location text box.
- Customer-definable contact details such as phone number with names in the Contact text box.
- Choose enabled to send SNMP notifications for various SNMP traps or disabled not to send SNMP notifications for various SNMP traps from the SNMP Global Trap drop-down list.
- Choose enabled to send system log messages or disabled not to send system log messages from the SNMP Logging drop-down list.

**Note**  The SNMP trap server, must be reachable through the distribution ports (and not through the gigabitethernet0/0 service or management interface).

The Management Port page appears.

**Step 7**
In the Management Port page, enter the following parameters for the management port interface (gigabitethernet 0/0) and click Next.

- Interface IP address that you assigned for the service port in the IP Address text box.
- Network mask address of the management port interface in the Netmask text box.
- The IPv4 Dynamic Host Configuration Protocol (DHCP) address for the selected port in the IPv4 DHCP Server text box.

The Wireless Management page appears.

**Step 8**
In the Wireless Management page, enter the following wireless interface management details, and click Next.

- Choose the interface—VLAN, or Ten Gigabit Ethernet from the Select Interface drop-down list.
- VLAN tag identifier, or 0 for no VLAN tag in the VLAN id text box.
- IP address of wireless management interface where access points are connected in the IP Address text box.
- Network mask address of the wireless management interface in the Netmask text box.
- DHCP IPv4 IP address in the IPv4 DHCP Server text box.

When selecting VLAN as interface, you can specify the ports as –Trunk or Access ports from the selected list displayed in the Switch Port Configuration text box.

The RF Mobility and Country Code page appears.

**Step 9**
In the RF Mobility and Country Code page, enter the RF mobility domain name in the RF Mobility text box, choose current country code from the Country Code drop-down list, and click Next. From the GUI, you can select only one country code.

**Note**  Before configuring RF grouping parameters and mobility configuration, ensure that you refer to the relevant conceptual content and then proceed with the configuration.

The Mobility Configuration page with mobility global configuration settings appears.

**Step 10**
In the Mobility Configuration page, view and enter the following mobility global configuration settings, and click Next.

- Displays Mobility Controller in the Mobility Role text box.
• Displays mobility protocol port number in the Mobility Protocol Port text box.
• Displays the mobility group name in the Mobility Group Name text box.
• Displays whether DTLS is enabled in the DTLS Mode text box.
  DTLS is a standards-track Internet Engineering Task Force (IETF) protocol based on TLS.
• Displays mobility domain identifier for 802.11 radios in the Mobility Domain ID for 802.11 radios text box.
• Displays the number of members configured on the controller in the Mobility Domain Member Count text box.
• To enable the controller as a Mobility Oracle, select the Mobility Oracle Enabled check box.
  Note Only the controller can be configured as Mobility Oracle. You cannot configure the switch as Mobility Oracle.
  The Mobility Oracle is optional, it maintains the client database under one complete mobility domain.
• The amount of time (in seconds) between each ping request sent to an peer controller in the Mobility Keepalive Interval (1-30)sec text box.
  Valid range is from 1 to 30 seconds, and the default value is 10 seconds.
• Number of times a ping request is sent to an peer controller before the peer is considered to be unreachable in the Mobility Keepalive Count (3-20) text box.
  The valid range is from 3 to 20, and the default value is 3.
• The DSCP value that you can set for the mobility controller in the Mobility Control Message DSCP Value (0-63) text box.
  The valid range is 0 to 63, and the default value is 0.

The WLANs page appears.

**Step 11**
In the WLANs page, enter the following WLAN configuration parameters, and click Next.
• WLAN identifier in the WLAN ID text box.
• SSID of the WLAN that the client is associated with in the SSID text box.
• Name of the WLAN used by the client in the Profile Name text box.

The 802.11 Configuration page appears.

**Step 12**
In the 802.11 Configuration page, check either one or both 802.11a/n/ac and 802.11b/g/n check boxes to enable the 802.11 radios, and click Next.
The Set Time page appears.

**Step 13**
In the Set Time page, you can configure the time and date on the controller based on the following parameters, and click Next.
• Displays current timestamp on the controller in the Current Time text box.
• Choose either Manual or NTP from the Mode drop-down list.
  On using the NTP server, all access points connected to the controller, synchronizes its time based on the NTP server settings available.
• Choose date on the controller from the Year, Month, and Day drop-down list.
• Choose time from the Hours, Minutes, and Seconds drop-down list.

• Enter the time zone in the Zone text box and select the offset setting required when compared to the current time configured on the controller from the Offset drop-down list.

The **Save Wizard** page appears.

**Step 14**

In the **Save Wizard** page, you can review the configuration settings performed on the controller using these steps, and if you wish to change any configuration value, click **Previous** and navigate to that page.

You can save the controller configuration created using the wizard only if a success message is displayed for all the wizards. If the **Save Wizard** page displays errors, you must recreate the wizard for initial configuration of the controller.