Getting Started

This chapter contains the following sections:

Getting Started with the Configuration

This section describes the system requirements and how to access the web-based Configuration Utility.

Supported Browsers

Before you begin to use the configuration utility, make sure that you have a computer with one of the following browsers:

- Internet Explorer 11, Microsoft Edge or later

- Firefox 64 or later

- Chrome 72 or later

- Safari 5.1 or later

Browser Restrictions

- If using Internet Explorer 11, configure the following security settings:

  - Select **Tools**, **Internet Options** and then select the **Security** tab.

  - Next, select **Local Intranet** and then select **Sites**.

  - Select **Advanced** and then select **Add**. Add the intranet address of the WAP device `http://<ip-address>` to the local intranet zone. The IP address can also be specified as the subnet IP address so that all subnet addresses, are added to the local intranet zone.

• If you have multiple IPv6 interfaces on your management station, use the IPv6 global address instead of the IPv6 local address to access the WAP device from your browser.

Launching the Web-based Configuration Utility

Follow these steps to access the configuration utility from your computer to configure the WAP device:

1. Connect the WAP device to the same network (IP subnet) as your computer. The factory default IP address configuration of the WAP device is DHCP. Make sure that your DHCP server is running and can be accessed. Besides, the WAP device has a default static IP, 192.168.1.245. You may choose to connect to it by configuring your computer's IP address in the 192.168.1.xxx range.

2. Locate the IP address of the WAP device.

    a. The WAP device can be accessed and managed by using the Cisco FindIT Network Discovery Utility. This utility enables you to automatically discover all supported Cisco devices in the same local network segment as your computer. You can get a snapshot view of each device or launch the product configuration utility to view and configure the settings. For more information, see http://www.cisco.com/go/findit.

    b. The WAP device is Bonjour-enabled and automatically broadcasts its services and listens for services being advertised by other Bonjour-enabled devices. If you have a Bonjour- enabled browser, such as Microsoft Internet Explorer with a Bonjour plug-in, or the Apple Mac Safari browser, you can find the WAP device on your local network without knowing its IP address.

    You can download the complete Bonjour for Microsoft Internet Explorer browser from Apple's website by visiting: http://www.apple.com/bonjour/ .

    c. Locate the IP address assigned by your DHCP server by accessing your router or DHCP server. See your DHCP server instructions for more information.

3. Launch any of the supported web browsers.

4. In the address bar, enter the IP address obtained using the initial step and press **Enter**.

5. Enter the default user name and password: `cisco` in the **Username** and **Password** fields.

6. Click **Log In**. The **Access Point Setup Wizard** appears.

Follow the Setup Wizard instructions to finish the installation. We strongly recommend that you use the Setup Wizard for the first installation. See for more information.

Logging Out

By default, the configuration utility logs out after 10 minutes of inactivity. See Management for instructions on changing the default timeout period.

To log out, click **Logout** in the top right corner of the configuration utility.

Using the Access Point Setup Wizard

The first time that you log into the Access Point or after it has been reset to the factory default settings, the Access Point Setup Wizard appears. This helps you perform the initial configurations. Use the following steps to complete the wizard:

Note   If you click **Cancel** to bypass the wizard, the **Change Password** page appears. You can then change the default password and username for logging in. See Changing Password for more information.

You must log in again after changing your password:

Step 1   Click **Next** on the **Welcome** page of the wizard.

Step 2   In the **Firmware Upgrade** window, click **Upgrade** to upgrade the firmware.

Note   Once the firmware has been upgraded, the device will reboot automatically and direct to the login page.

Step 3   Click **Skip**.

Step 4   In the **Restore Configuration** window, choose the configuration file you want to apply to the device and click **Apply**.

Note   When you click **Apply**, the device will save the relevant configuration, reboot and direct to the login page.

Step 5   Click **Skip**.

Step 6   In the **Configure Device - IP Address** window, click **Dynamic IP Address (DHCP) (Recommended)** to receive an IP address from a DHCP server, or click **Static IP Address** to configure the IP address manually. For a description of these fields, see IPv4 Configuration.

Step 7   Click **Next**. The **Single Point Setup - Set a Cluster** window appears. For a description on Single Point Setup, see Single Point Setup.

Step 8   To create a new Single Point Setup of the WAP device, click **New Cluster Name** and specify a new name. When you configure your devices with the same cluster name and enable the Single Point Setup mode on other WAP devices, they automatically join the group.

If you already have a cluster on your network, you can add this device to it by clicking **Join an Existing Cluster**, and then enter the **Existing Cluster Name**.

If you do not want this device to participate in a Single Point Setup at this time, click **Do not Enable Single Point Setup**.

Optionally, you can enter the access point location in the **AP Location** field to note the physical location of the WAP device.

If you clicked the **Join an Existing Cluster** radio button, the WAP configures the rest of the settings based on the cluster. Click **Next** and acknowledge the confirmation to join the cluster. Click **Submit** to join the cluster. After the configuration is complete, click **Finish** to exit the Setup Wizard.

Note   Ensure that adding the WAP devices in the existing cluster doesn't exceed the maximum limit. If this exceeds, the device will not allow to join the cluster.

Step 9   Click **Next**. The **Configure Device - Set System Date and Time** window appears.

Step 10   Choose your time zone, and then set the system time automatically from an NTP server or manually. For a description of these options, see Time.

Step 11   Click **Next**. The **Configure Device - Set Password** window appears.

Step 12   Enter a **New Password** and enter it again in the **Confirm Password** field.

Note   Uncheck **Password Complexity** to disable the password security rules. However, we strongly recommend keeping the password security rules enabled. For more information about passwords, see Security.

Step 13   Click **Next**. The **Configure Radio 1 - Name Your Wireless Network** window appears.

Step 14   Enter a **Network Name**. This name serves as the SSID for the default wireless network.

Step 15   Click **Next**. The **Configure Radio 1 - Secure Your Wireless Network** window appears.

Step 16   Choose a security encryption type and enter a security key. For a description of these options, see Configuring Security Settings.

Step 17   Click **Next**. The **Configure Radio 1 - Assign the VLAN ID for your Wireless Network** window appears.

Step 18   Choose the **VLAN ID** for traffic received on the wireless network.

We recommend that you assign a different VLAN ID from the default (1) to the wireless traffic, in order to segregate it from the management traffic on VLAN 1.

Step 19   Click **Next**. Repeat the step 13 to step 18 to configure the settings for Radio 2 interface.

Step 20   Click **Next**. The **Enable Captive Portal - Create Your Guest Network** window appears.

Step 21   Select whether or not to set up an authentication method for guests on your network, and click **Next**.

If you click **No**, skip to Step 29.

If you click **Yes**, the **Enable Captive Portal - Name Your Guest Network** window appears.

Step 22   Specify a **Guest Network Name**.

Step 23   Click **Next**. The **Enable Captive Portal - Secure Your Guest Network** window appears.

Step 24   Choose a security encryption type for the guest network and enter a security key. For a description of these options, see Configuring Security Settings.

Step 25   Click **Next**. The **Enable Captive Portal - Assign the VLAN ID** window appears.

Step 26   Specify a **VLAN ID** for the guest network. The guest network VLAN ID should be different from the management VLAN ID.

Step 27   Click **Next**. The **Enable Captive Portal - Enable Redirect URL** window appears.

Step 28   Check **Enable Redirect URL** and enter a fully qualified domain name (FQDN) or IP address in the **Redirect URL** field (including https://). If specified, the guest network users are redirected to the specified URL after authenticating.

Step 29   Click **Next**. The **Summary - Confirm Your Settings** window appears.

Step 30   Review the settings that you configured. Click **Back** to reconfigure one or more settings. If you click **Cancel**, all settings are returned to the previous or default values.

Step 31   If they are correct, click **Submit**. Your setup settings are saved and a confirmation window appears.

Step 32   Click **Finish**.

The WAP device was configured successfully. You are required to log in again with the new password.

Using the Access Point Setup Wizard with Mobile

The first time that you log into the Access Point with your portable device or after it has been reset to the factory default setting, the Access Point Setup Wizard with mobile style appears. This helps you perform the initial configurations. To configure the Access Point using the wizard, complete the following steps:

> ✎
>
> **Note** The default SSID under factory default mode is **CiscoSB-Setup**. Associate your portable device to the Access Point with this SSID and the pre-shared key, **cisco123**. Launch a browser and enter an arbitrary IP address or a domain name. A web page with login fields is displayed. Enter the default user name and password: **cisco**. Click **Log In**. The **Access Point Setup Wizard** is displayed.

Step 1   Click **Next** on the **Welcome** page of the wizard.

Step 2   In the **Configure IP address** window, the **Dynamic (DHCP)** is configured by default to receive an IP address from a DHCP server, or you may click **Static** to configure the IP address manually. For a description of these fields, see IPv4 Configuration.

Step 3   Click **Next**. The **Configure Single Point Setup** window appears.

Step 4   Click **Skip** and go to Step 6.

Step 5   To join an existing cluster, enter the cluster group name and click **Next**. A summary page with the cluster information is displayed. Confirm the data and click **Submit**.

> **Note**   To create a new cluster, click **Create**, enter a cluster name, and go to Step 6.

Step 6   In the **Configure Device - Set Password** window, enter a new password and re-enter the password in the **Confirm Password** field.

Step 7   Click **Next**. The **Configure Your Wireless Network** window appears.

   a) Enter a Network Name which serves as the SSID for the default wireless network.
   b) Enter a Security key (security type, WPA2 Personal - AES is by default)
   c) Enter the VLAN ID for traffic received on the wireless network.

> **Note**   Check the check box to apply same configuration to Radio 2 or switch to another radio tab and repeat Step 7 to configure again.

Step 8   Click **Next**. The **Setup Captive Portal** window appears.

Step 9   Click **Skip**. Go to Step 12.

Step 10 Click **Yes**. The **Configure Captive Portal** window appears.

Step 11 Select **Radio 1 (5 GHz)** or **Radio 2 (2.4 GHz)**.

   a) Specify a Guest Network Name.
   b) Enter a Security key (security type, WPA2 personal - AES is by default)
   c) Specify a VLAN ID for the guest network.
   d) Optionally, you may specify a redirect URL with a fully qualified domain name (FQDN) to redirect users to the specified URL after authentication.

Step 12 Click **Next**. The **Summary** window appears.

Step 13 Review the configured settings. Click **Back** to reconfigure one or more settings.

Step 14 Ensure the data is correct and click **Submit** to save.

Step 15 The WAP device is configured successfully. You are required to log in again with a new password.

Changing Password

For security reasons, you are required to change the administrative password at a set interval. You will need to access this page when the Password Aging Time is up.

Password complexity is enabled by default. The minimum password complexity requirements are shown on the **Change Password** page. The new password must comply with the default complexity rules, or it can be disabled temporarily by disabling the **Password Complexity**. See Security for more information.

To change the default password, configure the following:

- **Username**—Enter a new username. The default name is cisco.

- **Old Password**—Enter the current password. The default password is cisco.

- **New Password**—Enter a new password.

- **Confirm Password**—Enter the new password again for confirmation.

- **Password Strength Meter**—Displays the strength of the new password.

- **Password Complexity**—The password complexity is enabled by default and requires that the new password conforms to the following complexity settings:

    - Is different from the username.

    - Is different from the current password.

    - Has a minimum length of eight characters.

    - Contains characters from at least three character classes (uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard).

Note   Check **Disable** to disable the password complexity rules. However, we strongly recommend that you keep the password complexity rules enabled.

TCP/UDP Service

The TCP/UDP Service table displays the protocols and services operating on the WAP.

- **Service** — The service name.

- **Protocol** — The underlying transport protocol that the service uses (TCP or UDP).

- **Local IP Address** — The local IP address of the connected device. All indicates that any IP address on the device can use this service.

- **Local Port** — The local port number.

- **Remote IP Address** — The IP address of a remote host using this service. All indicates that the service is available to all remote hosts that access the system.

- **Remote Port** — The port number of any remote device communicating with this service.

- **Connection State** — The state of the service. For UDP, only connections in the Active or Established states appear in the table. The TCP states are:

  - **Listening** — The service is listening for connection requests.

  - **Active** — A connection session is established and the packets are being transmitted and received.

  - **Established** — A connection session is established between the WAP device and a server or client.

  - **Time Wait** — The closing sequence has been initiated and the WAP device is waiting for a system-defined timeout period (typically 60 seconds) before closing the connection.

Note   You can modify or rearrange the order on the TCP/UDP Service Table. Click **Refresh** to refresh the screen and show the most current information.

You can also enter parameters related to Service, Protocol and other details to filter the TCP/UDP Services displayed.

Click **Back** to return to the **Getting Started** page.

System Status

The System Status page displays the hardware model description, software version, and the various configuration parameters such as:

- **PID VID**—The hardware model and version of the WAP device.

- **Serial Number**—The serial number of the WAP device.

- **Host Name**—The host name assigned to the WAP device.

- **MAC Address**—The MAC address of the WAP device.

- **IPv4 Address** —The IP address of the WAP device.

- **IPv6 Address**—The IPv6 address of the WAP device.

- **ETH0/PD Port**—Displays the status of Ethernet interface.

- **ETH1 Port**—Displays the status of ETH1 interface.

- **Radio 1 (5GHz)**—The 5GHz mode is enabled or disabled for the Radio 1 interface.

- **Radio 2 (2.4GHz)** —The 2.4GHz mode is enabled or disabled for the Radio 2 interface.

- **Power Source**—The system may be powered by a power adapter, or may be receiving power over Ethernet (PoE) which includes two power supply modes of 802.3.af and 802.3at from a Power Sourcing Equipment (PSE).

  When power source is insufficient (802.3af), the WAP device retains the following configuration information.

  - The Radio1(5GHZ) is disabled.

• The Radio2(2.4GHZ) antenna switches to 2 x2 from 3 x3, TX power decreases to 18dBm.

• The ETH0/PD port downgrades to 1Gbps speed.

• The ETH1 port is turned off.

• **System Uptime**—The time elapsed since the last reboot.

• **System Time**—The current system time.

• **Firmware Version (Active Image)**—The firmware version of the active image.

• **Firmware MD5 Checksum (Active Image)**—The checksum for the active image.

• **Firmware Version (Non-active)**—The firmware version of the backup image.

• **Firmware MD5 Checksum (Non-active)**—The checksum for the backup image.

Quick Start Configuration

To simplify the device configuration through quick navigation, the **Getting Started** page provides links for performing common tasks. The **Getting Started** page is the default window at start-up.

Category	Link Name (on the Page)	Linked Page
Quick Access	Setup Wizard	Using the Access Point Setup Wizard, on page 2
	Change Account Password	Adding a User
	Backup/Restore Configuration	Configuration Management
	Upgrade Device Firmware	Firmware
Advanced Configuration	Wireless Settings	Radio
	Management Setting	System Settings
	LAN Setting	IPv4 Configuration
	Configure Single Point Setup	Configuring the WAP Device for Single Point Setup
	Guest Access	Guest Access
More Information	Dashboard	Dashboard
	TCP/UDP Service	TCP/UDP Service, on page 6
	View System Log	View System Log
	Traffic Statistics	Traffic Statistics

For additional information on the device, you can access the product support page or the Cisco Support Community by:

• Click **Support** to access the product support page.

• Click **Forums** to access the Cisco Support Community page.

• Click **More info on FindIT** to see information on FindIT utility.

• Click **Download FindIT** to download the FindIT utility.

Window Navigation

Use the navigation buttons to move around the graphical user interface of the WAP.

Configuration Utility Header

The configuration utility header contains standard information and appears at the top of every page. The header provides these buttons:

Button Name	Description
(User)	The account name (Administrator or Guest) of the user logged into the WAP device. The factory default username is **cisco**.
(Language)	Hover the mouse pointer over the button, and select a language. The factory default language is English.
⤇	Click to log out of the configuration utility.
ⓘ	Click to show the WAP device type and version number.
❓	Click to show the context-sensitive online help. The online help is designed to be viewed with browsers using UTF-8 encoding. If the online help shows errant characters, verify that the encoding settings on your browser are set to UTF-8.

Navigation Pane

A navigation pane, or main menu, is located on the left of each page. The navigation pane lists the top-level features of the WAP device. If an arrow occurs after a main menu item, you can select to expand and display the submenu of each group. You can then select the desired submenu item to open the associated page.

Management Buttons

The following table describes the commonly used buttons that appear on various pages in the system:

Button Name	Description
Add	Adds a new entry to a table or database.
Cancel	Cancels a change made to the page.

Button Name	Description
Clear All	Clears all entries in a log table.
Delete	Deletes an entry in a table.
Edit	Edits an existing entry.
Refresh	Refreshes the current page with the latest data.
Apply	Applies/Saves the settings or configuration.
Update	Updates the new information to the startup configuration.