Using the Setup Wizard on the WAP125 or WAP581

Objective

The Setup Wizard is a built-in feature that you may use to help you with the initial configuration of a Wireless Access Point (WAP) device. The Setup Wizard makes it very simple to configure settings providing step-by-step instructions.

This document shows you how to configure WAP125 and WAP581 with the Setup Wizard on the web configuration utility.

To configure your WAP using Setup Wizard on a mobile device, click here.

Applicable Devices

- WAP125
- WAP581

Software Version

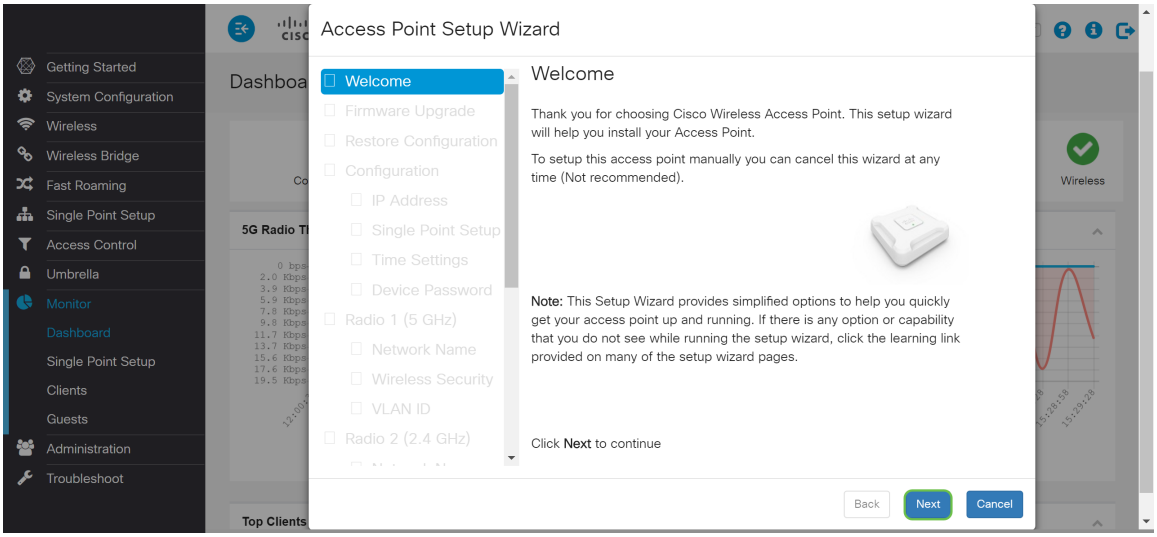
- 1.0.1.3

How to use the Setup Wizard

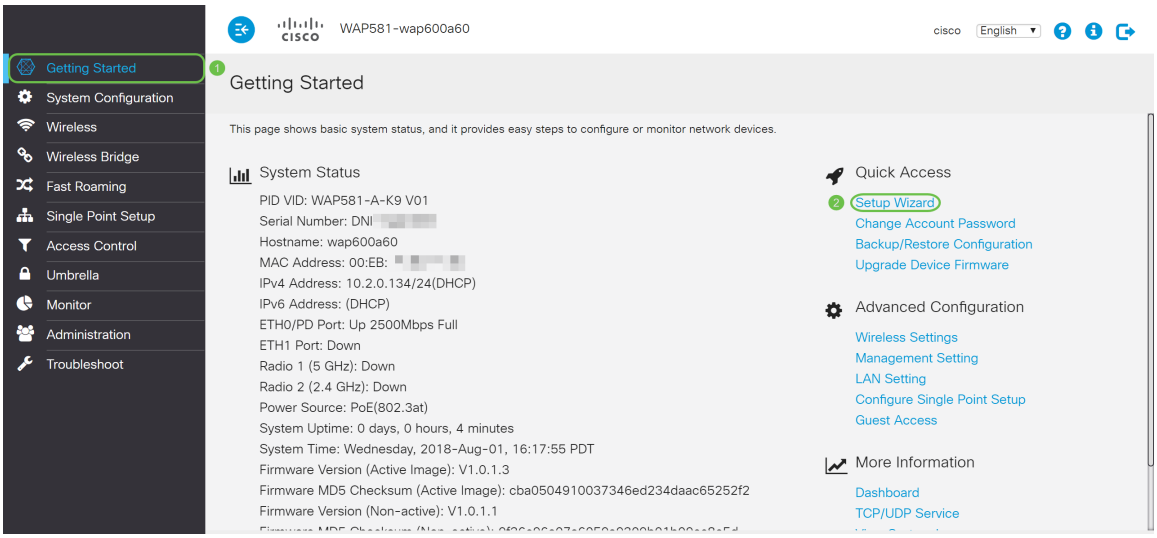
Step 1. Log in to the web configuration utility of your WAP by entering the IP address of the WAP into your web browser. If this is your first time configuring the WAP, the default IP address is 192.168.1.254.

Note: The WAP581 is used in this guide to demonstrate the Setup Wizard. The appearance may vary depending on the model.

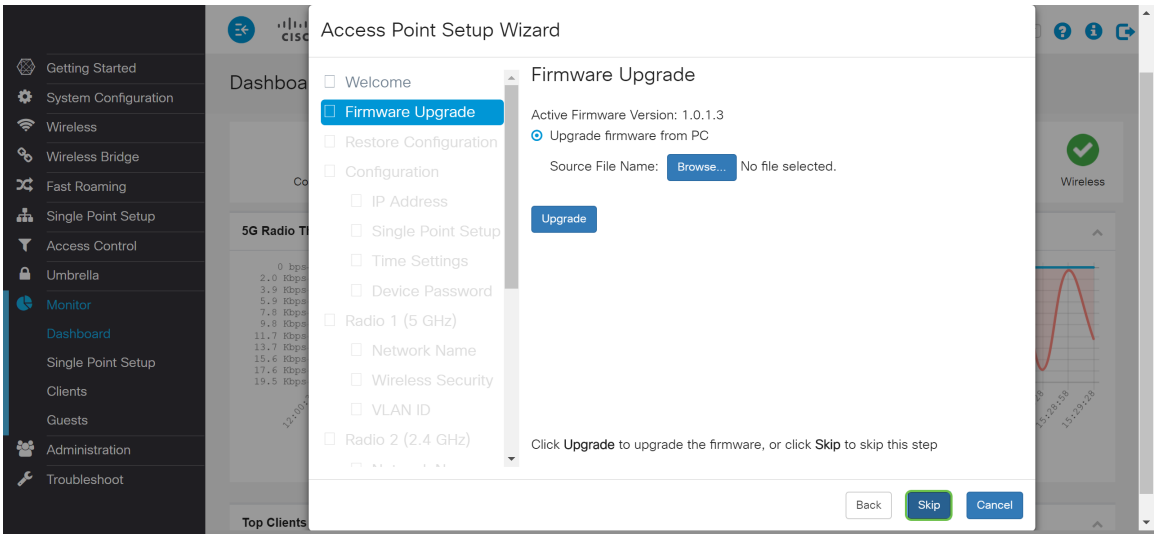
Step 2. The first time that you log into the Access Point or after it has been reset to the factory default settings, the *Access Point Setup Wizard* appears. Click **Next** to continue.



Note: If your WAP is already configured but you still want to access the *Setup Wizard*, navigate to **Getting Started > Setup Wizard**. The *Access Point Setup Wizard* window will appear.

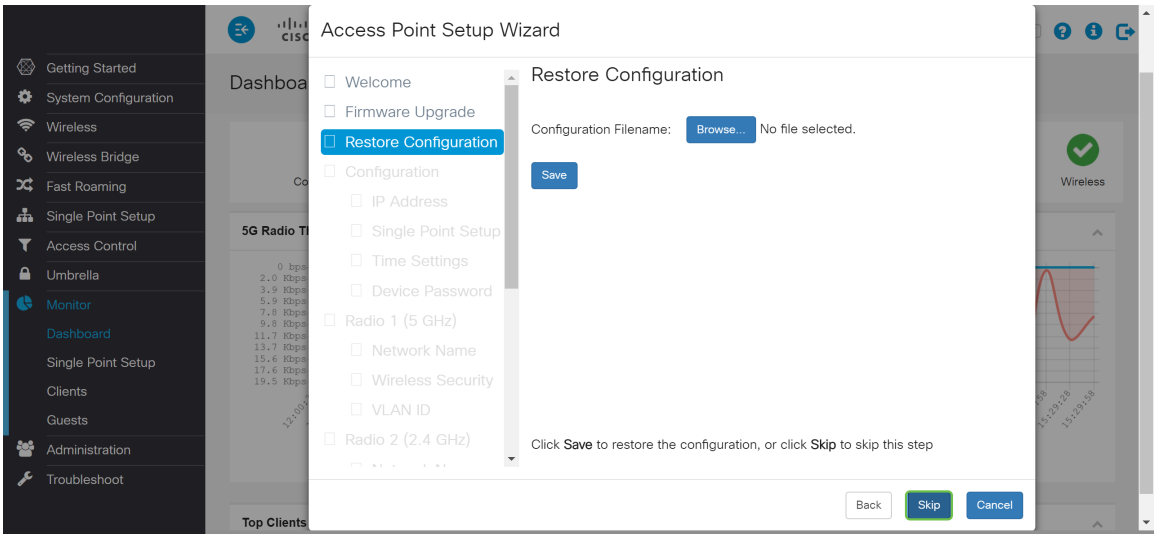


Step 3. In the *Firmware Upgrade* window, click the **Browse...** button and select the firmware file that you want to upgrade to. Then press **Upgrade** to upgrade to that firmware. Once the firmware has been upgraded, the device will reboot automatically and direct to the login page. In this example, we will be clicking **Skip** as we have the firmware version we want.



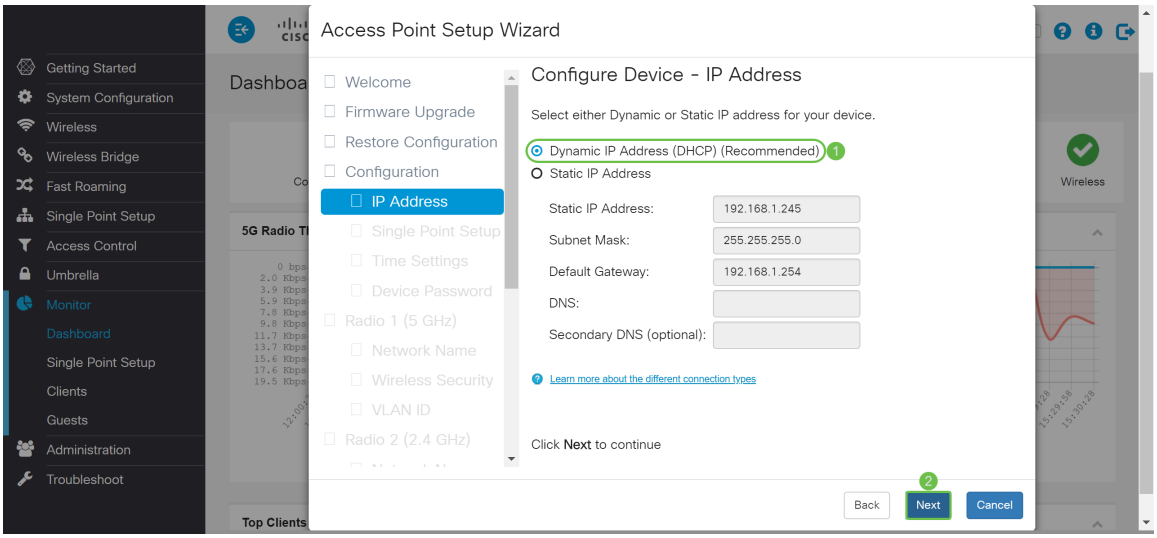
Step 4. If you have previous configuration that you want to apply to the device, click the **Browse...** button in the *Restore Configuration* window and select the configuration file that you want to apply. Then click **Save** to apply the configuration file to the device. In this example, we will be clicking **Skip**.

Note: When the device applies the relevant configuration, it will reboot and direct you to the login page.



Step 5. In the *Configure Device – IP Address* window, select **Dynamic IP Address (DHCP) (Recommended)** to obtain an IP address from a Dynamic Host Configuration Protocol (DHCP) server, or click **Static IP Address** to configure the IP address manually. Then click **Next** to continue to the next section. DHCP provides configuration parameters to internet hosts. In this case, the DHCP assigns an IP address to a client for a limited period of time or until the client explicitly relinquishes the address.

In this example, we will be selecting **Dynamic IP Address (DHCP) (Recommended)**.



Step 6. Single Point Setup provides a centralized method to administer and control wireless services across multiple devices. This will allow you to create a single group or cluster of your wireless devices which you can view, deploy, configure, and secure the wireless network as a single entity. Single Point Setup can help facilitates channel planning across your wireless service to reduce radio interference and maximize bandwidth on your wireless network.

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.

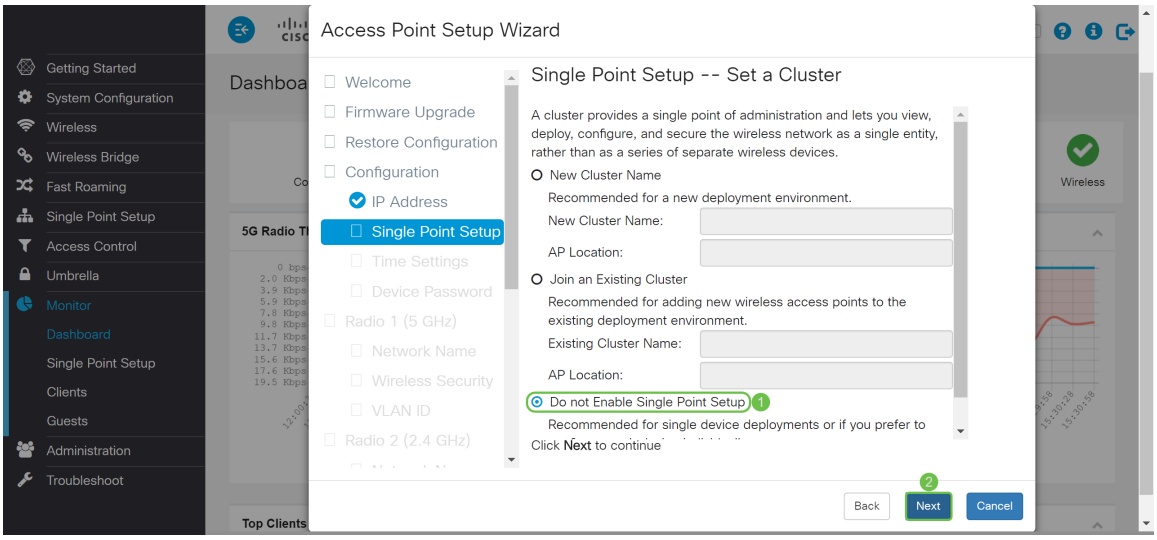
If you already have a cluster on your network, you can add this device to it by clicking **Join an Existing Cluster**, and then enter the **Existing Cluster Name**. The WAP configures the rest of the settings based on the cluster. Click **Next** and acknowledge the confirmation to join the cluster.

Click **Submit** to join the cluster. After the configuration is complete, click **Finish** to exit the *Setup Wizard*.

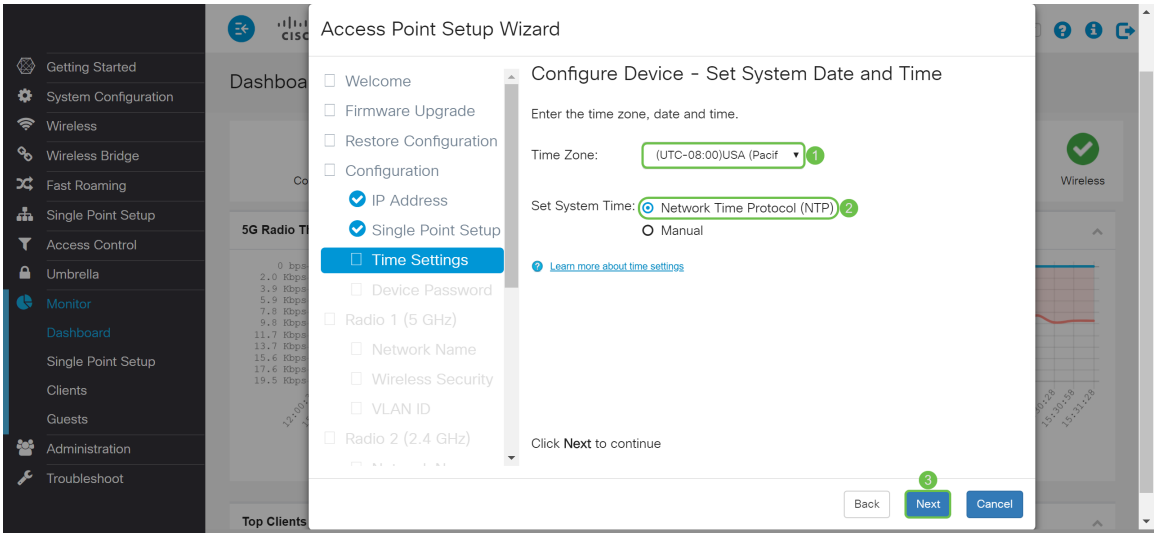
Note: You can enter the Access Point location in the **AP Location** field to note the physical location of the WAP device.

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

In this example, we will be selecting **Do not Enable Single Point Setup**. Then click **Next** to continue to the next section.



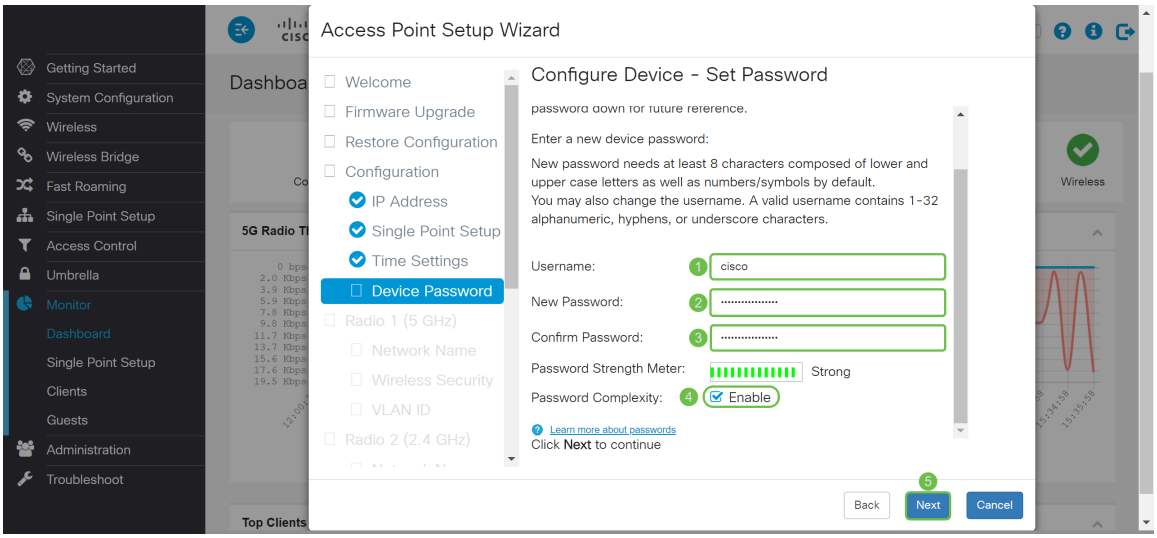
Step 7. In the *Configure Device – Set System Date and Time* window, choose your **time zone**, and then select whether you want your system time to automatically acquire the time setting from a **Network Time Protocol (NTP)** server or select **Manual** to manually configure the time settings. A system clock provides a network-synchronized time-stamping service for the message logs. The system clock can be configured manually or as a NTP client that obtains the click data from a server. Click **Next** to continue the *Setup Wizard*.



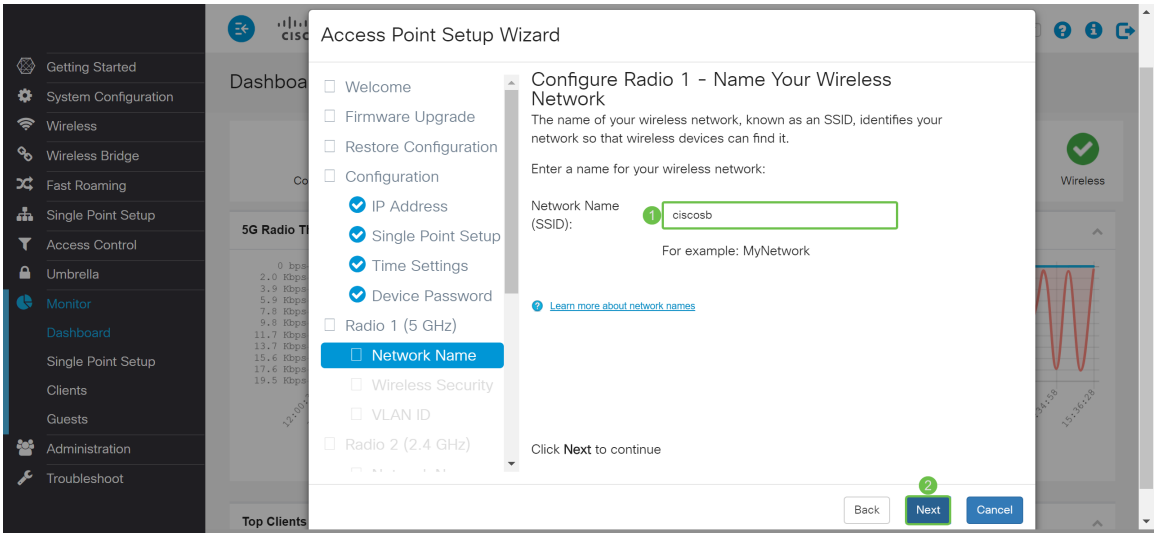
Step 8. Enter a new **Username** in the *Username* field, by default the username is cisco. Enter a **New Password** for the *Username*. Then enter in the **New Password** again in the *Confirm Password* field. You are able to uncheck *Password Complexity* to disable the password security rules. However, we strongly recommend keeping the password security rules enabled. The new password must conform 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).

Then click **Next** to configure *Radio 1*.



Step 9. Enter a name for your wireless network in the *Network Name (SSID)*. This will help identify your network so that wireless devices can find it. By default, **ciscosb** is used as the network name. Then click **Next** to continue to the next section.



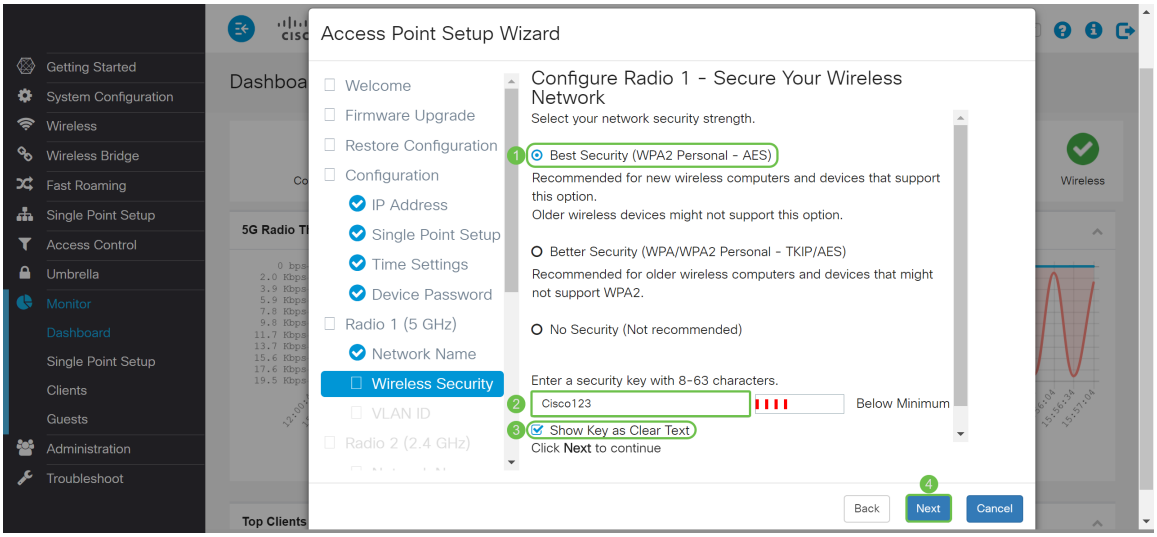
Step 10. Click the radio button that corresponds with the network security you would like to apply to your wireless network. Then enter in the password for your network in the *Security Key* field. To see the password as you type, check the **Show Key as Clear Text** check box. Click **Next** to continue.

Note: If the network has a mix of clients, some of which support WPA2 and others which support only the original WPA, select both (WPA/WPA2). This lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for client who support it. This WPA configuration allows more interoperability in place of some security.

- Best Security (Wi-Fi Protected Access 2 (WPA2) Personal – Advanced Encryption Standard (AES)) All client stations on the network support WPA2 and Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication

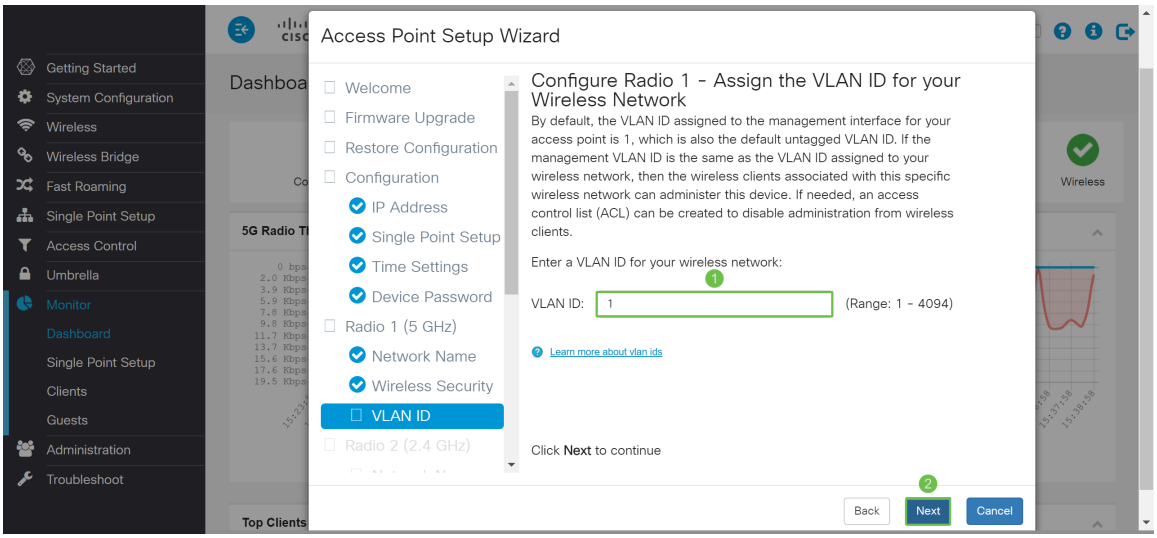
Code Protocol (AES-CCMP) cipher/security protocol. This provides the best security per IEEE 802.11i standard. As per the latest Wi-Fi Alliance requirement, the AP has to support this mode all the time.

- Better Security (WPA/WPA2 Personal – TKIP/AES) WPA Personal is a Wi-Fi Alliance IEEE802.11i standard, which includes AES-CCMP and TKIP encryption. It provides security when there are older wireless devices that support the original WPA but does not support the newer WPA2.
- No Security (Not Recommended) Wireless network does not require a password and can be accessed by anyone.

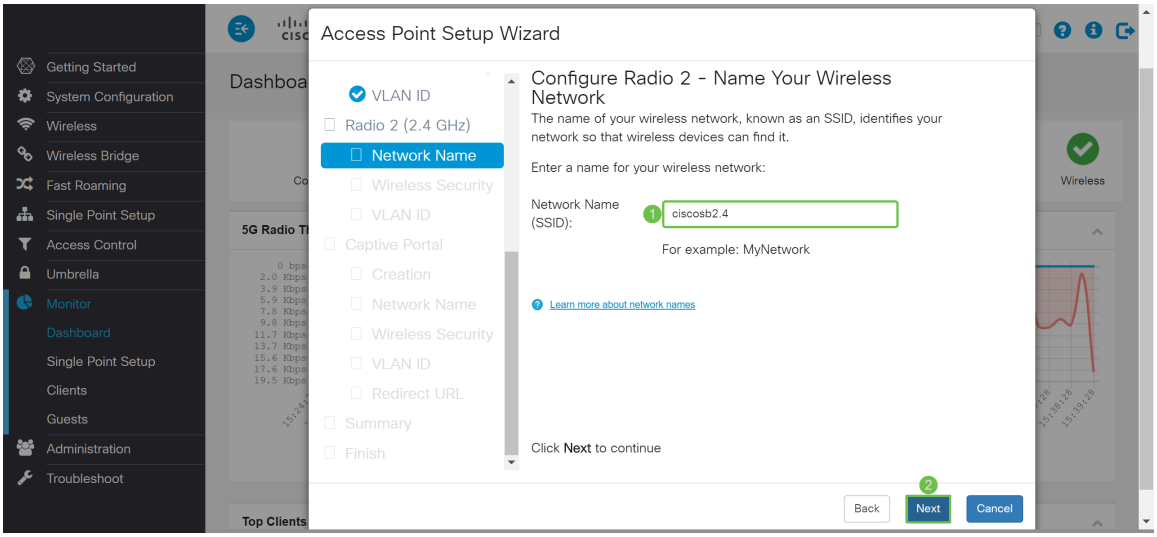


Step 11. In the *VLAN ID* field, enter the ID number of the VLAN that you would like the *Radio 1 (5 GHz)* to belong to. In this example, we will be leaving the *VLAN ID* as 1. Click **Next** to configure *Radio 2 (2.4 GHz)*.

Note: 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. Click here to learn more about Virtual Access Points (VAPs).



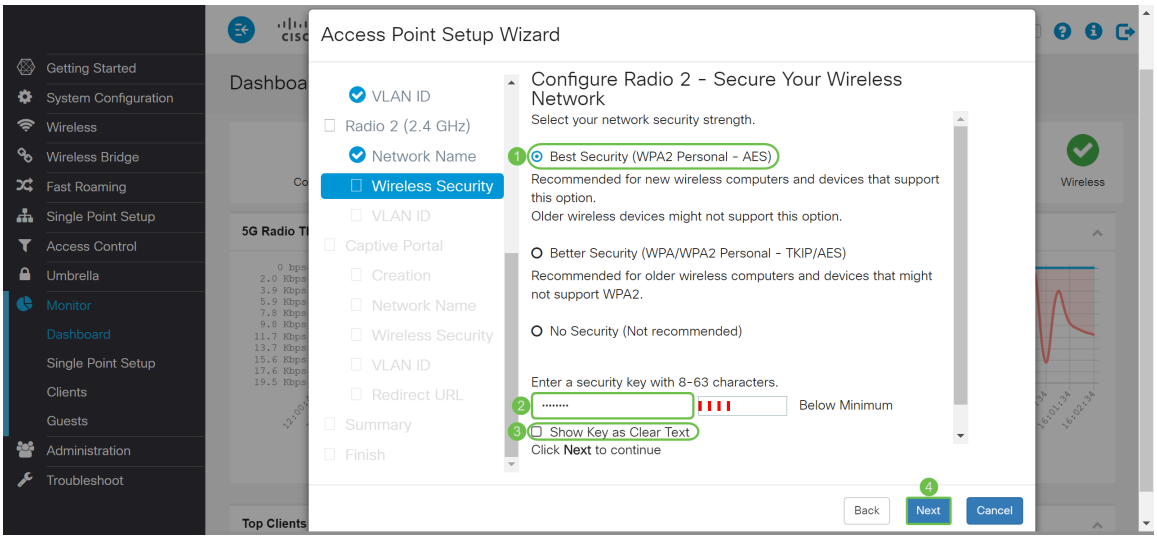
Step 12. Enter a new network name in the *Network Name (SSID)* field. By default **ciscosb** is used. Network name is known as an SSID, it identifies your network so that wireless devices can find it. In this example, **ciscosb2.4** was used to differentiate the 5 GHz network name. Click **Next** to configure the wireless security for *Radio 2 (2.4 GHz)*.



Step 13. Click the radio button that corresponds with the network security you would like to apply to your wireless network. Then enter in the password for your network in the *Security Key* field. To see the password as you type, check the **Show Key as Clear Text** check box. The **Show Key as Clear Text** is checked by default. Click **Next** to continue.

Note: If the network has a mix of clients, some of which support WPA2 and others which support only the original WPA, select both (WPA/WPA2). This lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more interoperability in place of some security.

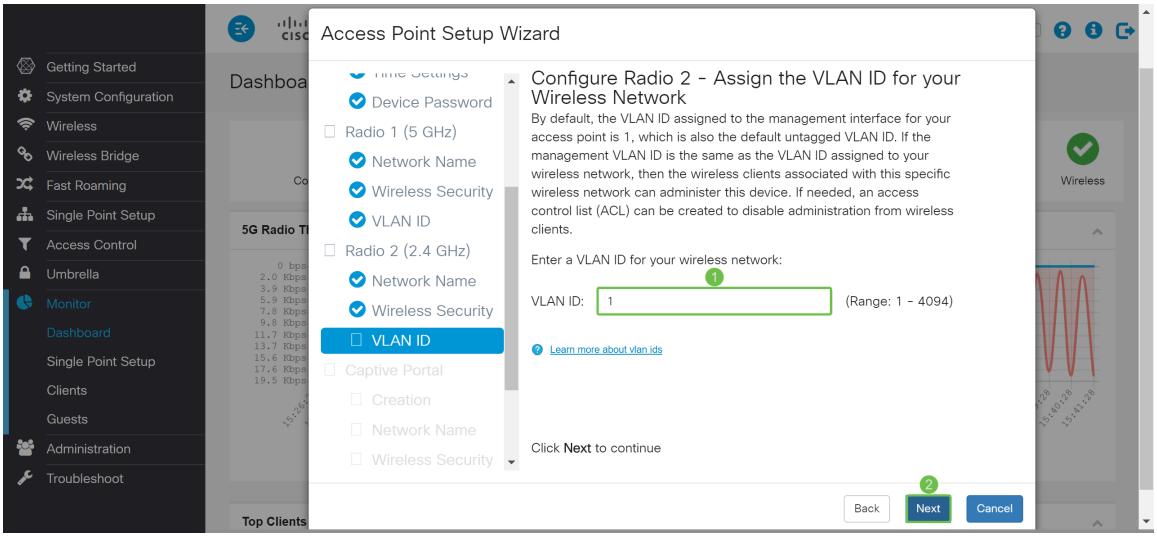
- Best Security (Wi-Fi Protected Access 2 (WPA2) Personal – Advanced Encryption Standard (AES)) All client stations on the network support WPA2 and Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP) cipher/security protocol. This provides the best security per IEEE 802.11i standard. As per the latest Wi-Fi Alliance requirement, the AP has to support this mode all the time.
- Better Security (WPA/WPA2 Personal – TKIP/AES) WPA Personal is a Wi-Fi Alliance IEEE802.11i standard, which includes AES-CCMP and TKIP encryption. It provides security when there are older wireless devices that support the original WPA but does not support the newer WPA2.
- No Security (Not Recommended) Wireless network does not require a password and can be accessed by anyone.



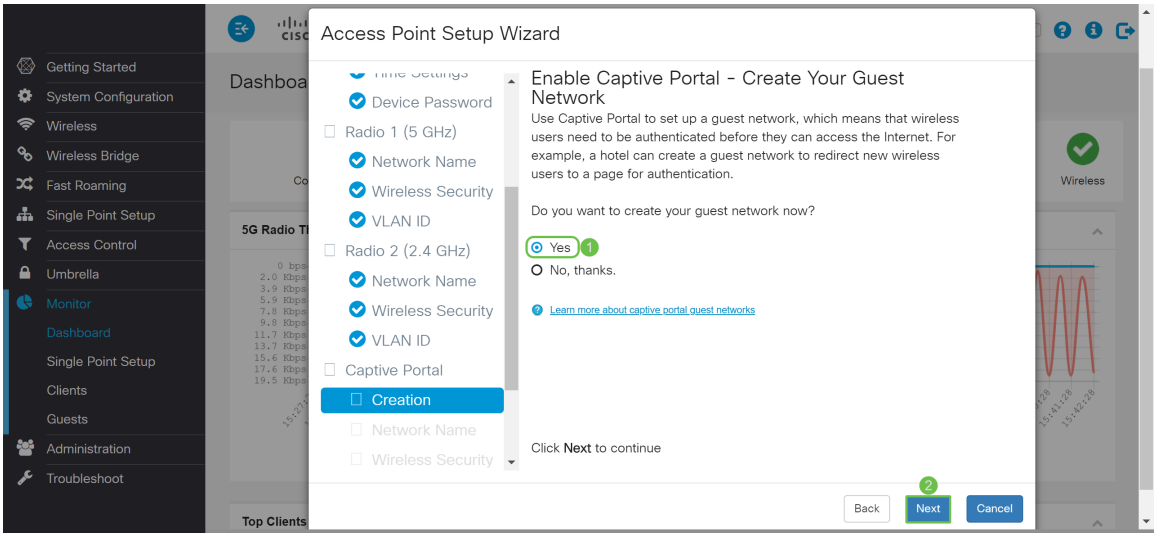
Step 14. In the *VLAN ID* field, enter the ID number of the VLAN that you would like the *Radio 1*

(2.4 GHz) to belong to. In this example, we will be using the default value of 1 as our *VLAN ID*. Click **Next** to configure *Captive Portal*.

Note: 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. Click here to learn more about Virtual Access Points (VAPs).

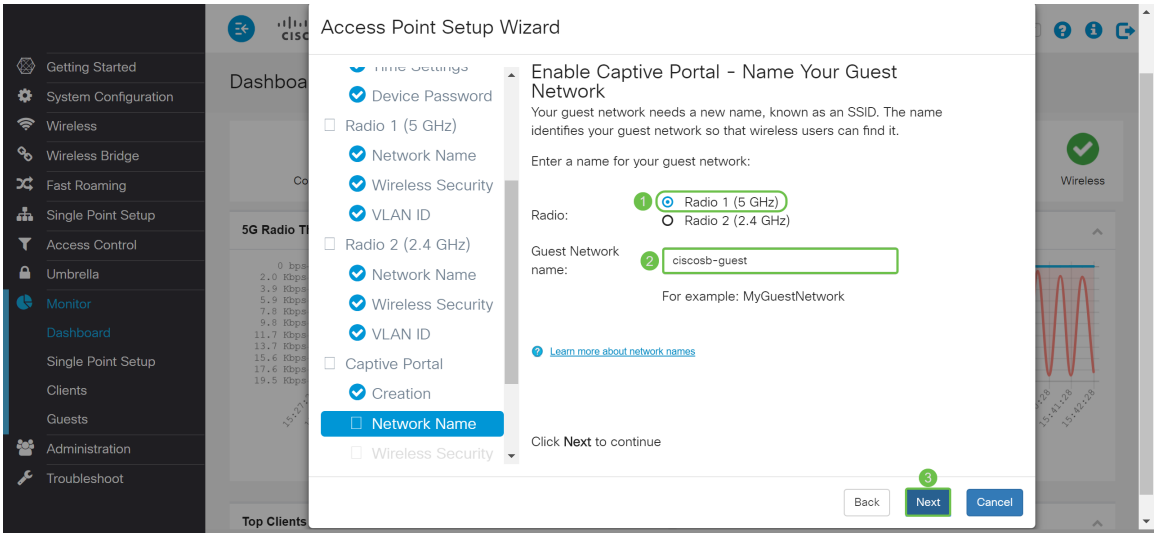


Step 15. (Optional) A guest network is not required. Click the **Yes** radio button if you would like to create a guest network. Click the **No** radio button if you do not want to create a guest network and skip to Step 20. Click the **Next** button to continue.



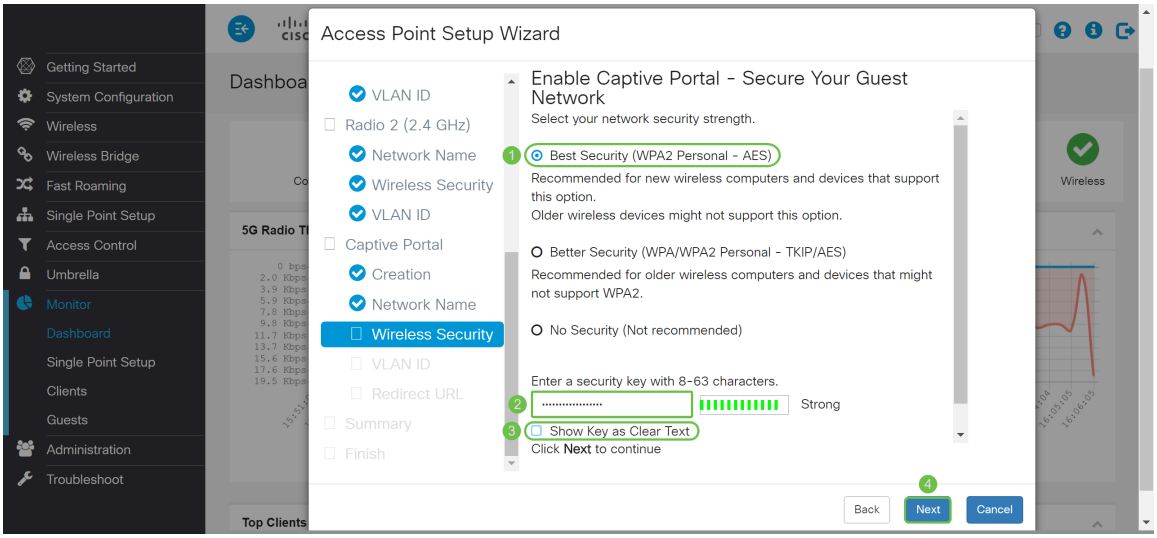
Step 16. (Optional) Select the radio button that corresponds with the *Radio* in which you would like to place the guest network. Then create a network name in the *Guest Network name* field. Click **Next** to configure the *Wireless Security* settings for the *Guest Network*.

In this example, we will be selecting **Radio 1 (5 GHz)** as our *Radio* and leaving the default network name as **ciscosb-guest** so your wireless guest users can find the network name.

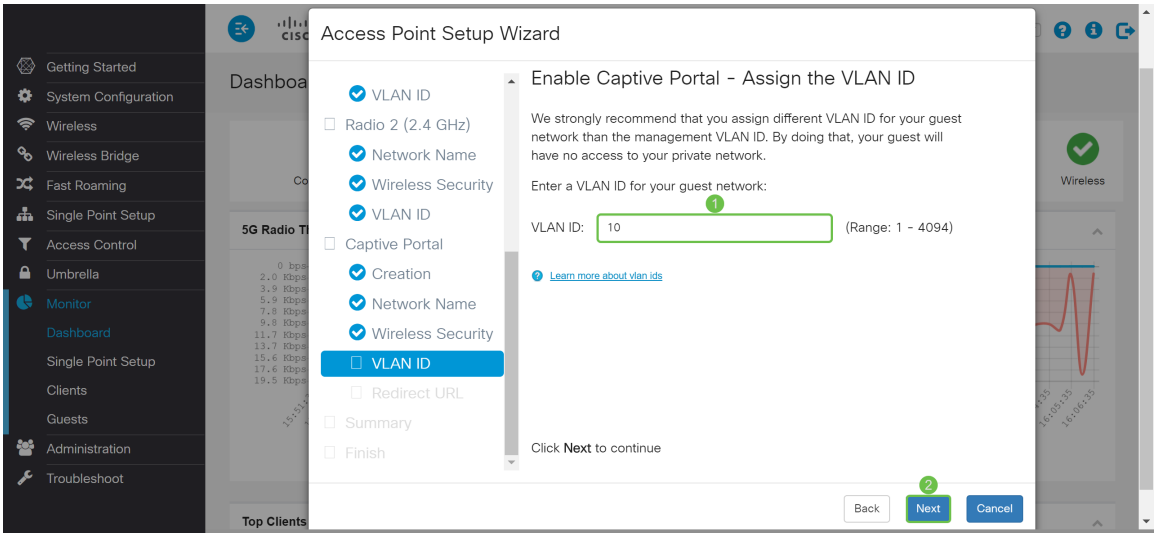


Step 17. (Optional) Select the radio button that corresponds with the network security you would like to apply to your guest network. Then enter a password for the guest network in the *Security Key* field if applicable. To **Show Key as Clear Text** check the check box to show your security key as plaintext. This is enabled by default. Click **Next** to continue. The network security options are:

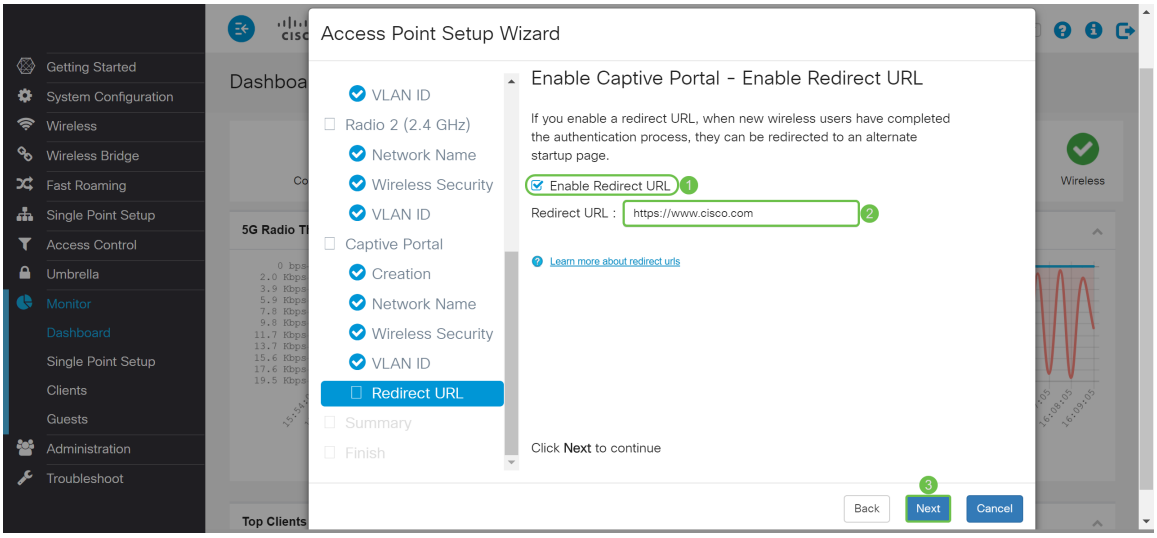
- Best Security (WPA2 Personal – AES) – Recommended for new wireless computers and devices that support this option.
- Better Security (WPA/WPA2 Personal – TKIP/AES) – Recommended for older wireless computers and devices that might not support WPA2.
- No Security (Not recommended) – This is the default selection.



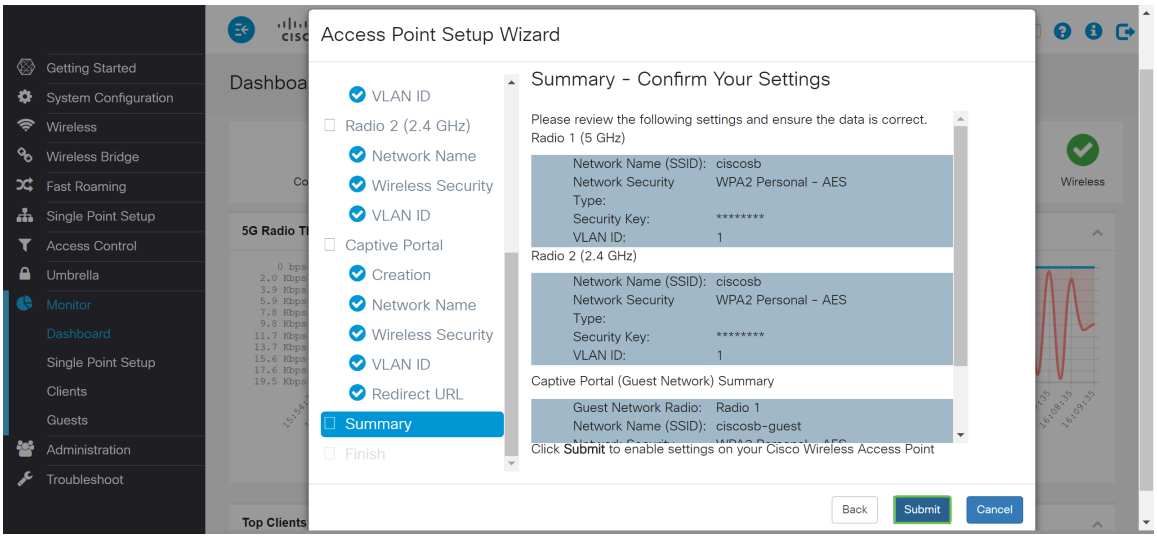
Step 18. (Optional) Specify a *VLAN ID* for the guest network. The guest network VLAN ID should be different from the management VLAN ID. In this example, we used *VLAN ID* **10** as our VLAN ID for the guest network. Click **Next** to configure the *Redirect URL* for the guest network.



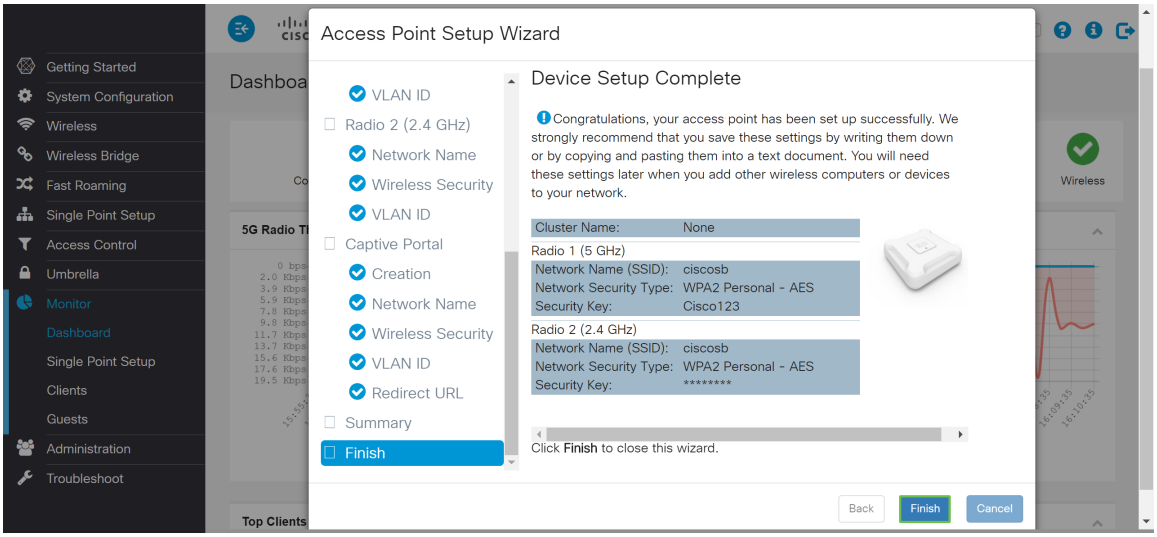
Step 19. (Optional) Check **Enable Redirect URL** check box to redirect new wireless users to an alternative startup page. Enter a Fully Qualified Domain Name (FQDN) or IP address in the *Redirect URL* field (including http:// or https://). Then click **Next** to continue to the *Summary* page.



Step 20. In the *Summary – Confirm Your Settings* page, review the settings that you configured. Click the **Back** button to reconfigure one or more settings. If you click **Cancel**, all settings are returned to the previous or default values. If your configurations are correct, click **Submit**. Your setup settings are saved and a confirmation window appears.



Step 21. Once your settings are configured, the *Device Setup Complete* page will appear to let you know that your Access Point has been successfully set up. Click **Finish** and you will be required to log in again with the new password.



Conclusion

You have now successfully configured your WAP using the Setup Wizard. You should see your SSIDs that you have just configured in your list of Wi-Fi networks. To configure other features on your WAP, you are required to log in again.