Setup Wizard on the WAP571

Objective

The Setup Wizard is a set of interactive instructions that guide you through the initial configuration of the WAP571. These instructions cover the basic configurations needed to operate the WAP571. The *Access Point Setup Wizard* window will automatically appear the first time you log on to the WAP, but can also be accessed using the web GUI at any point.

The objective of this document is to explain how to configure the WAP571 through the use of the Setup Wizard.

Applicable Devices

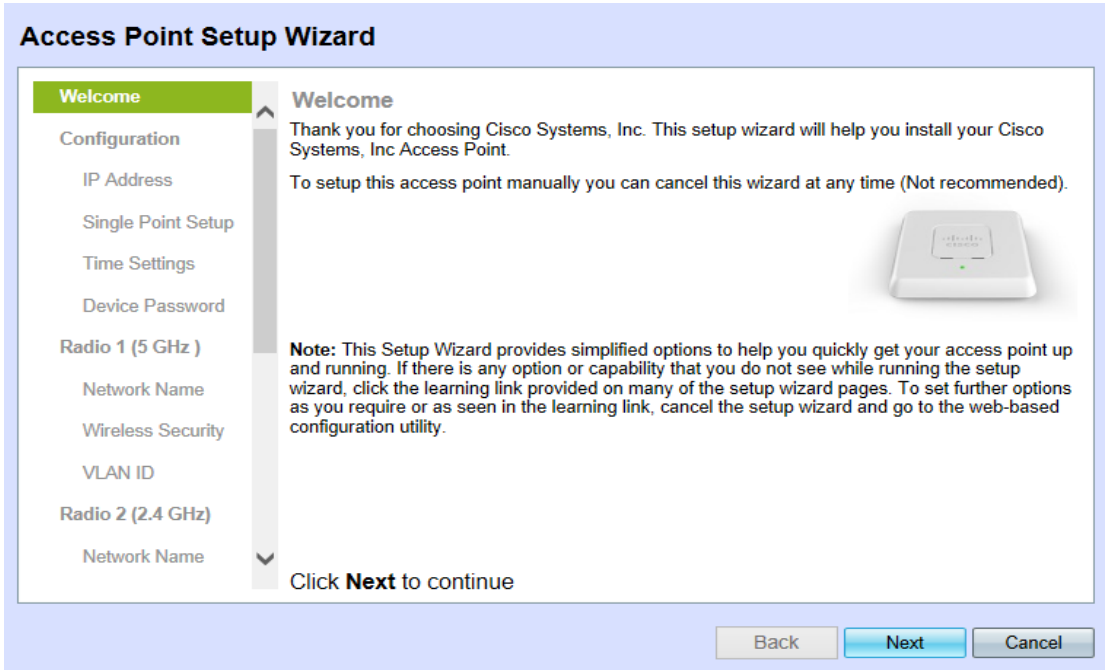
- WAP571

Software Version

- V1.0.0.1

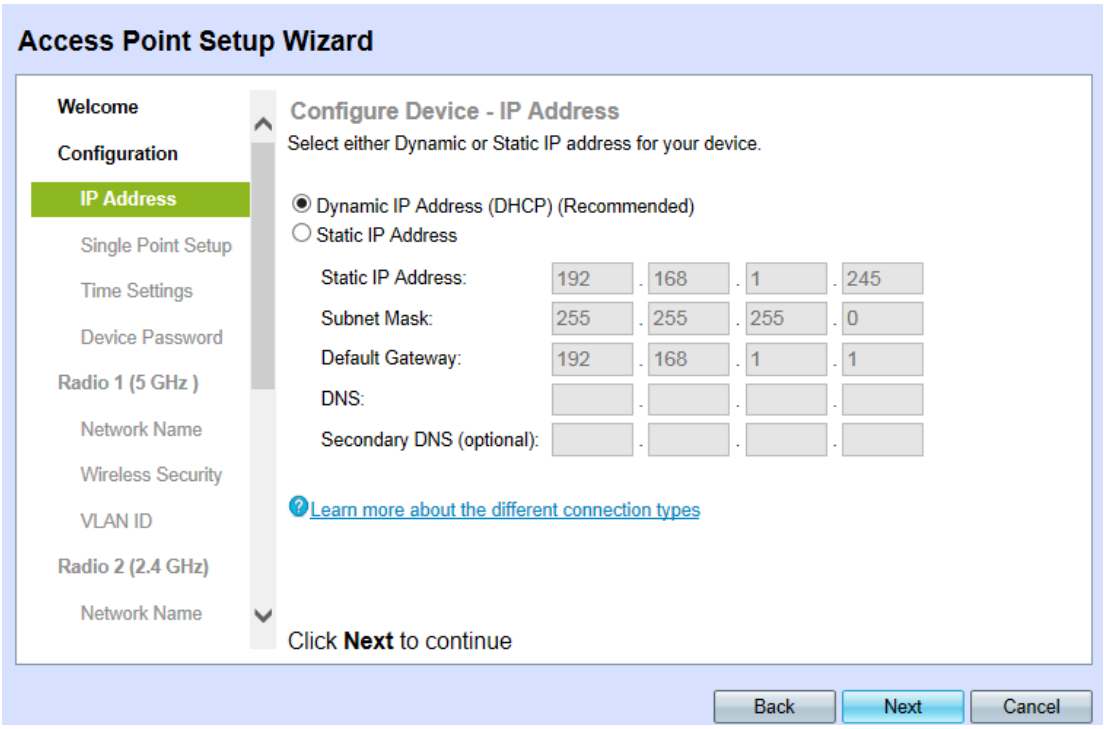
Configure Setup Wizard

Step 1. Log in to the web configuration utility and choose **Run Setup Wizard**. The *Access Point Setup Wizard* window appears.



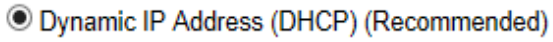
Note: If this is the first time logging into the device, this window will appear automatically.

Step 2. Click **Next** to continue. *The Configure Device IP Address* page opens:

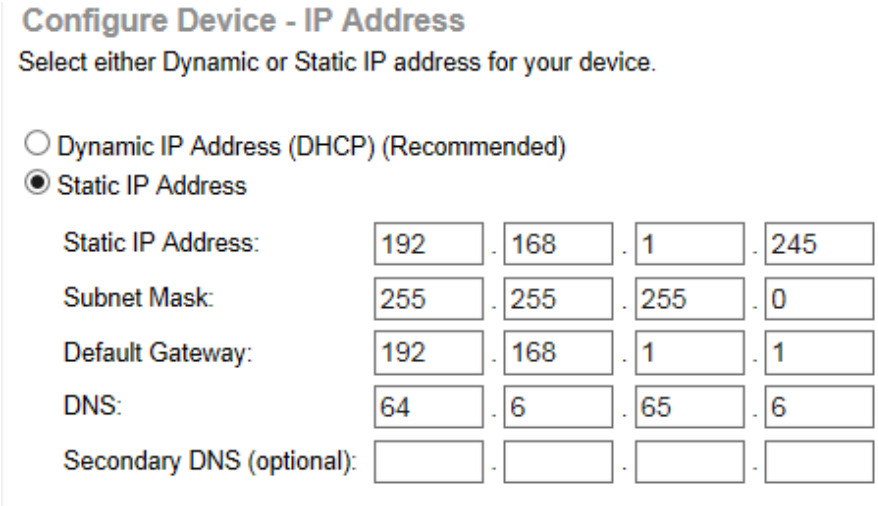


Step 3. Click the corresponding radio button for the method you want to use to determine the IP address of the device.

• Dynamic IP Address (DHCP) — The IP address of the WAP is assigned by the DHCP server. This is the recommended setting. If selected, please skip to Step 9.



• Static IP Address — Establish a fixed (static) IP address for the WAP. This address will not be changed unless reconfigured.



Step 4. In the *Static IP Address* field, enter the IP address of the WAP.

Note: This IP address is established by you, and should not be used by any other device in the network.

Step 5. In the *Subnet Mask* field, enter the desired subnet mask of the IP address.

Step 6. In the *Default Gateway* field, enter the IP address of the desired default gateway for the WAP.

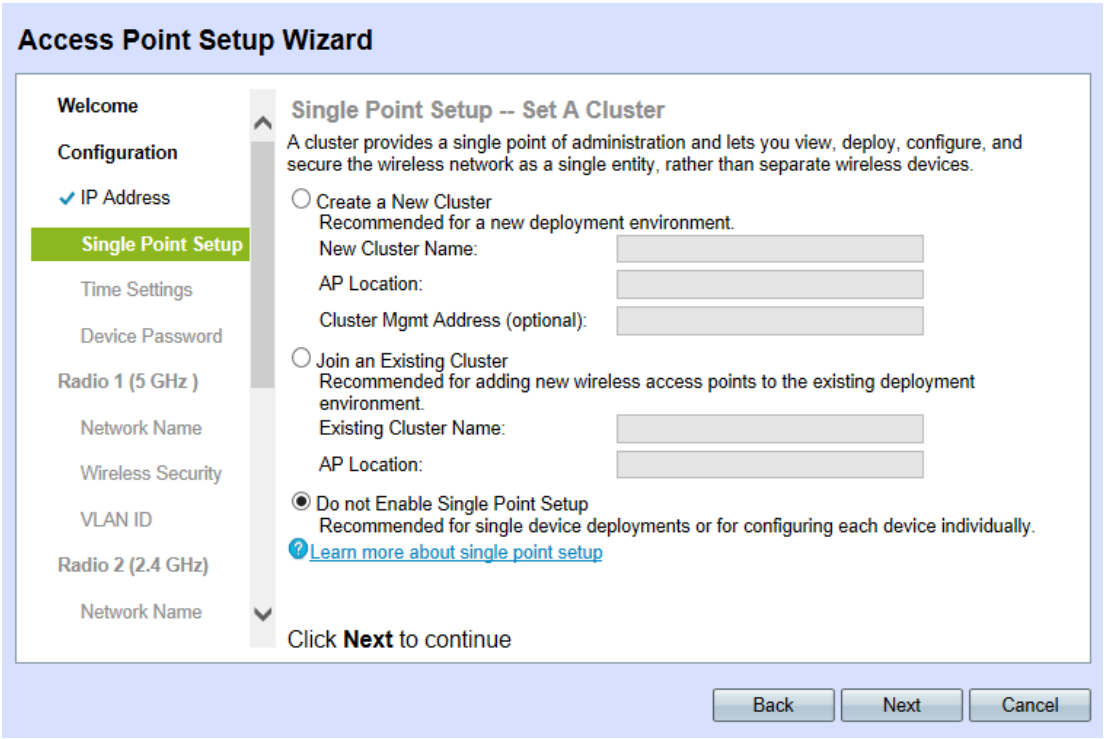
Note: The default gateway is usually the private IP address assigned to your router.

Step 7. In the *DNS* field, enter the IP address of the desired primary domain name system (DNS) server.

Note: The DNS server provided by your Internet service provider (ISP) should be used if you want to access outside web pages.

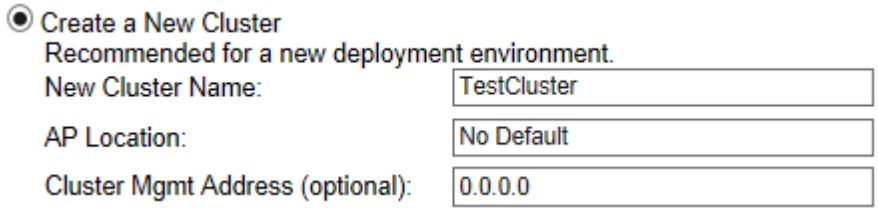
Step 8. (Optional) In the *Secondary DNS* field, enter the IP address of the desired secondary DNS.

Step 9. Click **Next** to continue. The *Single Point Setup -– Set a Cluster* page opens:



Step 10. Click the corresponding radio button for the desired cluster setting. A cluster allows you to configure multiple access points (APs) simultaneously. If you decide to not use a cluster they will need to be configured individually.

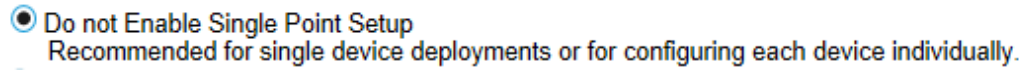
- Create a New Cluster — Create a new cluster for APs.



- Join an Existing Cluster — Join an existing AP cluster in the network**.**

- Do not Enable Single Point Setup — Single Point Setup (cluster) is not allowed. If

selected please skip to Step 14.



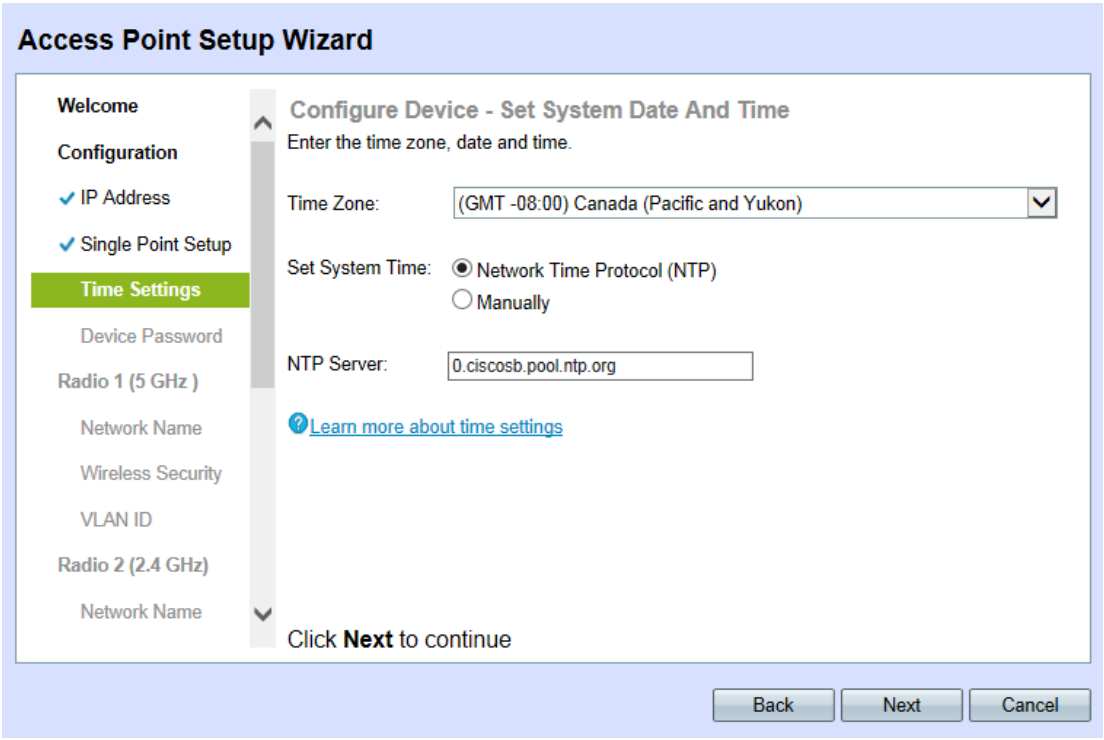
Note: If *Join an Existing Cluster* is selected, the WAP will configure the rest of the settings based on the cluster. Click **Next**, a confirmation page will ask if you want to join the cluster. Click **Submit** to join the cluster. After the configuration is complete, click **Finish** to exit the Setup Wizard.

Step 11. In the *New* or *Existing Cluster Name* field, enter the desired cluster name.

Step 12. In the *AP Location* field, enter the physical location of the WAP. This field doesn't impact the operation of the AP.

Step 13. (Optional) If creating a new cluster, enter the desired management address in the *Cluster Mgmt Address* field.

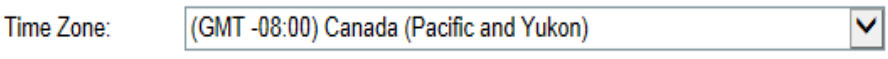
Step 14. Click **Next** to continue. The *Configure Device – Set System Date and Time* page opens:



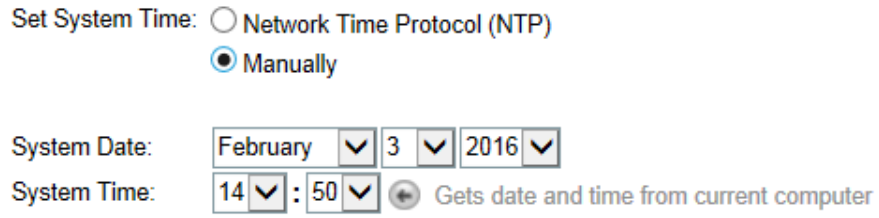
Step 15. Select the appropriate time zone from the *Time Zone* drop-down list.

Step 16. Click the corresponding radio button for the desired method to set the time of on the WAP.

- Network Time Protocol (NTP) — The WAP gets the time from an NTP server.



- Manually — The time is manually entered into the WAP. If selected, please skip to Step 18.

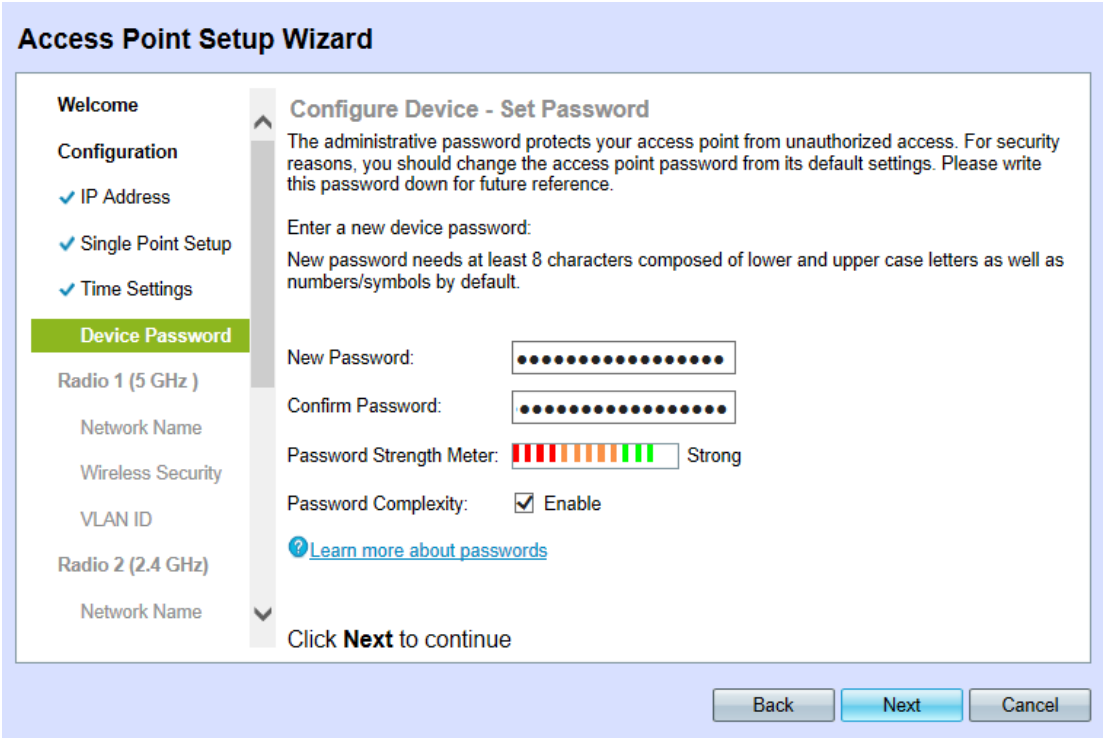


Step 17. If Network Time Protocol was selected, enter the URL of the NTP server that will provide the date and time in the *NTP Server* field. Please skip to Step 20.

Step 18. Select the month, day and year respectively in the *System Date* drop-down list.

Step 19. Select the hour and minute respectively in the *System Time* drop-down list.

Step 20. Click **Next** to continue. The *Configure Device – Set Password* page opens:



Step 21. In the *New Password* field, enter a new password. This password will give you administrative access to the WAP.

Step 22. In the *Confirm Password* field, re-enter the same password.

Note: As you enter the password, the number and color of vertical bars change to indicate the password strength as follows:

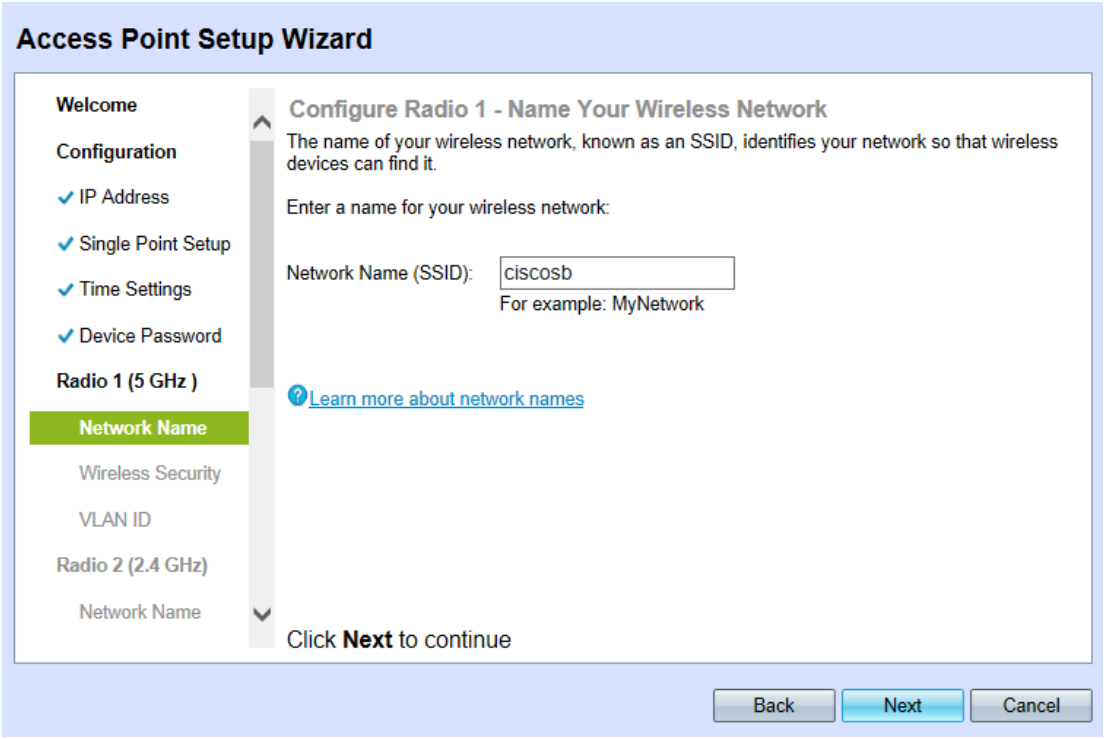
- Red — The password fails to meet the minimum complexity requirements.
- Orange — The password meets the minimum complexity requirements but the password strength is weak.
- Green — The password is a strong password and exceeds the minimum complexity requirements.

Step 23. (Optional) To enable/disable password complexity, check the **Enable** checkbox.

Note: Password complexity requires that the password is at least 8 characters and

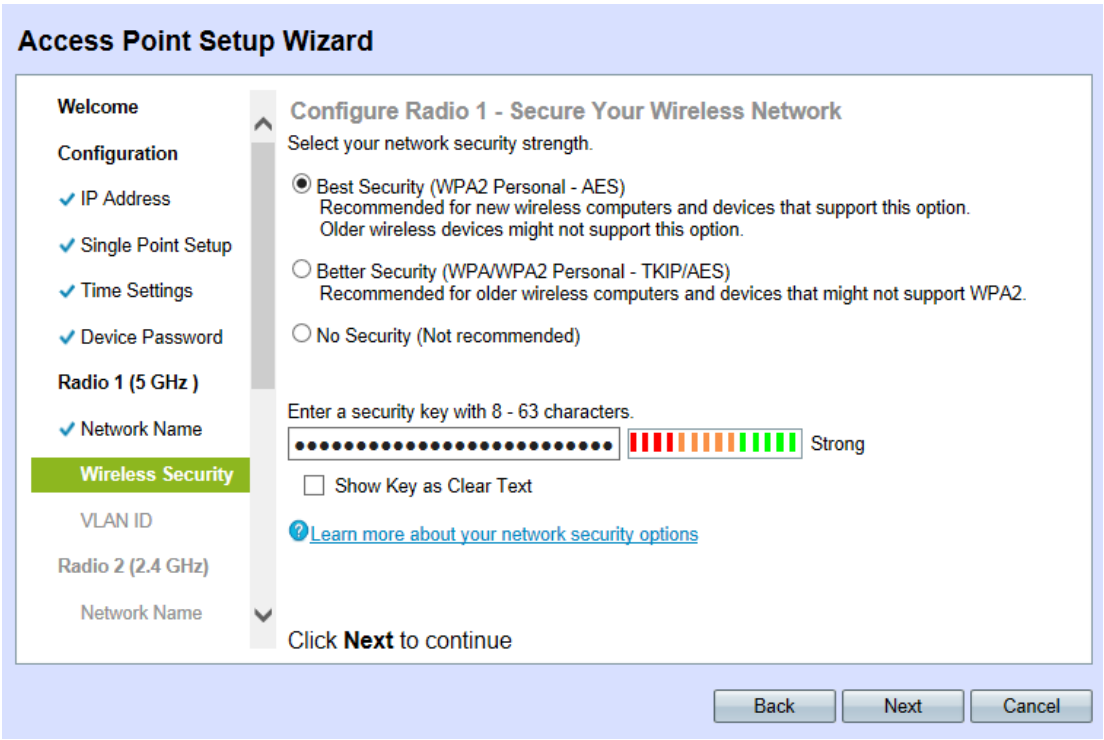
composed of lower and upper case letters and numbers or symbols.

Step 24. Click **Next** to continue. The *Configure Radio 1|2 – Name Your Wireless Network* page opens:



Step 25. In the *Network Name (SSID)* field, enter the Service Set Identification (SSID) of the wireless network. The SSID is the name of the wireless local area network.

Step 26. Click **Next** and the *Configure Radio 1|2 - Secure Your Wireless Network* page opens:



Step 27. Click the corresponding radio button for the desired network security method. The methods are as follows:

• Best Security (WPA2 Personal – AES) — WPA2 is the second version of WPA security and access control technology for Wi-Fi wireless networking, which includes AES-CCMP encryption. This protocol version provides the best security per the IEEE 802.11i standard. All client stations on the network will need to be able to support WPA2. WPA2 does not allow use of the protocol TKIP (Temporal Key Integrity Protocol), since it has known limitations.

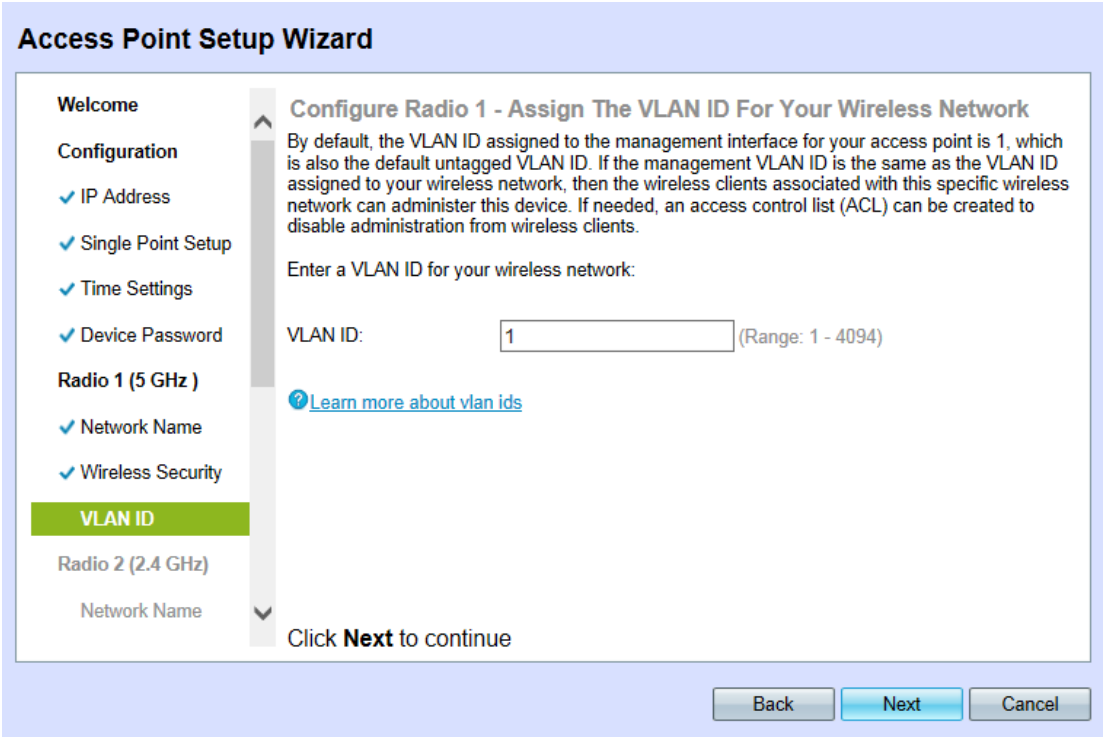
• Better Security (WPA Personal – TKIP/AES) — WPA Personal is a Wi-Fi Alliance IEEE 802.11i standard, which includes AES-CCMP and TKIP encryption. It provides security when there are older wireless devices that support the original WPA but do not support the newer WPA2.

• No Security — The wireless network does not require a password and can be accessed by anyone. If you choose No Security, skip to Step 30.

Step 28. In the *Security Key* field, enter the desired password for your network.

Step 29. (Optional) To see the password as you type, check the **Show Key as Clear Text** check box.

Step 30. Click **Next** to continue. The *Configure Radio 1|2 – Assign The VLAN ID For Your Wireless Network* page opens:



Note: If *No Security* is selected, the device will prompt you to confirm your decision.

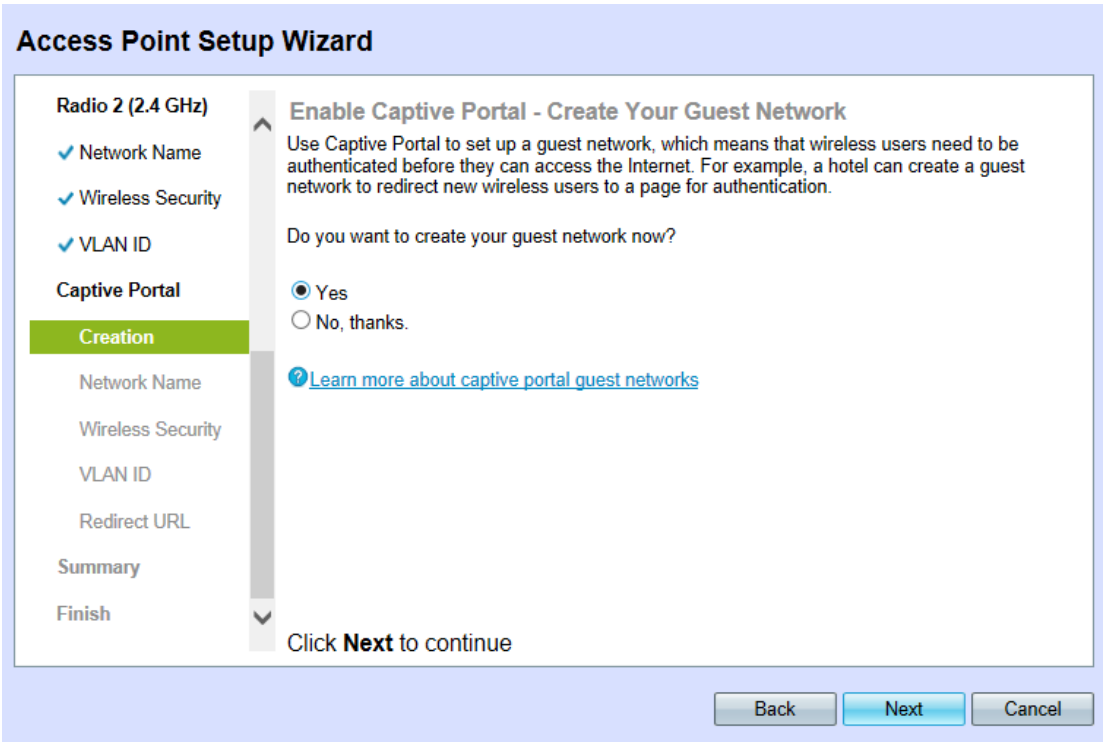
Step 31. In the *VLAN ID* field, enter the ID number of the desired VLAN to which the WAP belongs to.

Note: The VLAN ID should match one of the VLAN IDs that is supported on the port of the remote device that is connected to the WAP.

Note: Repeat Steps 24 – 31 to configure Radio 2; the configuration process is identical for both radios.

Step 32. Click Next to continue. The Enable Captive Portal – Create Your Guest

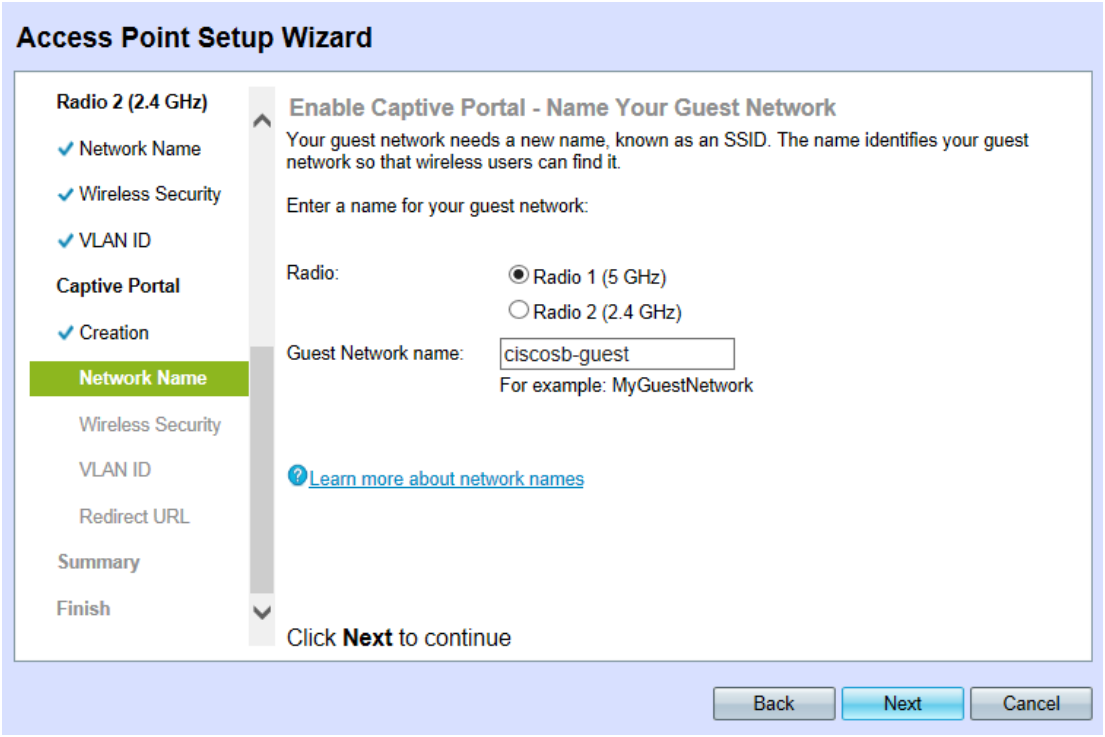
Network page opens:



Step 33. To create a guest network click **Yes.** A guest network requires users to be authenticated before being allowed access to the internet. If **No** is selected, skip to Step 47.

Note: This will be a separate network from the ones configured during Steps 24 – 31.

Step 34. Click **Next** to continue. The *Enable Captive Portal – Name Your Guest Network* page opens:



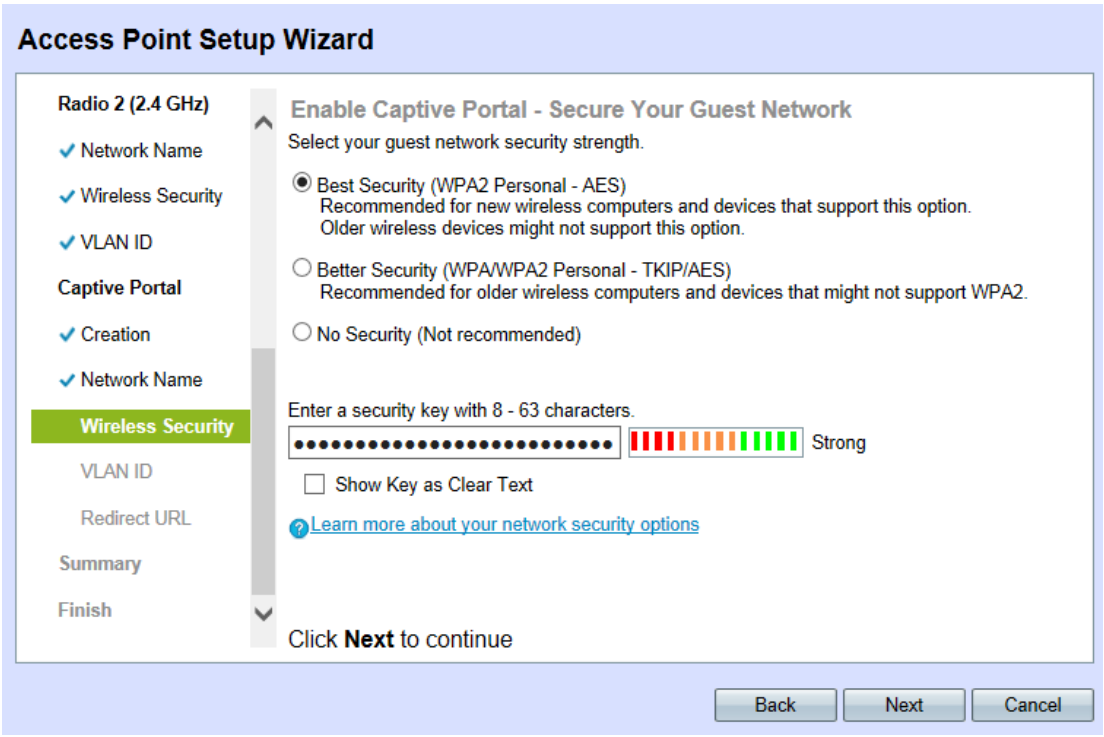
Step 35. Click the corresponding radio button for the desired radio wave in the *Radio* field.

- Radio 1 (5 GHz)

• Radio 2 (2.4 GHz)

Step 36. In the *Guest Network name* field, enter the SSID of the guest network.

Step 37. Click **Next** to continue. The *Enable Captive Portal – Secure Your Guest Network* page opens:



Step 38. Click the corresponding radio button for the desired network security method. The methods are as follows:

• Best Security (WPA2 Personal – AES) — WPA2 is the second version of WPA security and access control technology for Wi-Fi wireless networking, which includes AES-CCMP encryption. This protocol version provides the best security per the IEEE 802.11i standard. All client stations on the network will need to be able to support WPA2. WPA2 does not allow use of the protocol TKIP (Temporal Key Integrity Protocol) that has known limitations.

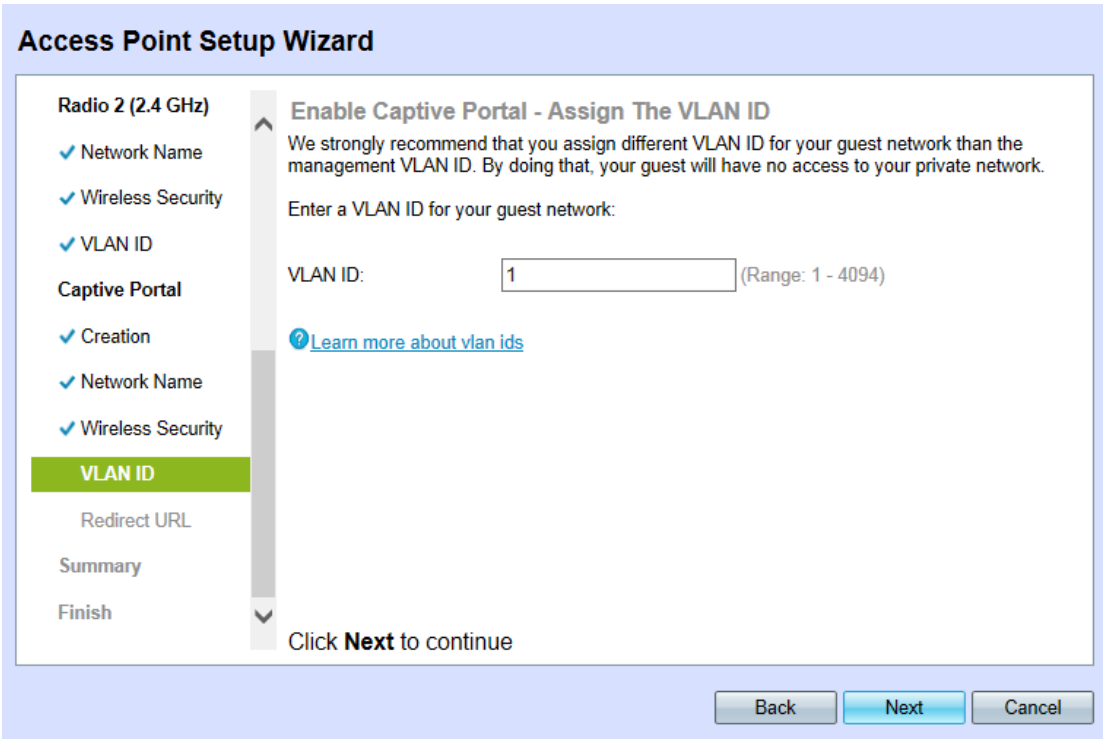
• Better Security (WPA Personal – TKIP/AES) — WPA Personal is a Wi-Fi Alliance IEEE 802.11i standard, which includes AES-CCMP and TKIP encryption. It provides security when there are older wireless devices that support the original WPA but do not support the newer WPA2.

• No Security — The wireless network does not require a password and can be accessed by anyone. If you choose No Security, skip to Step 42.

Step 39. In the *Security Key* field, enter the desired password for your network.

Step 40. (Optional) To see the password as you type, check the **Show Key as Clear Text** check box.

Step 41. Click **Next** to continue. The *Enable Captive Portal – Assign The VLAN ID For Your Wireless Network* page opens:

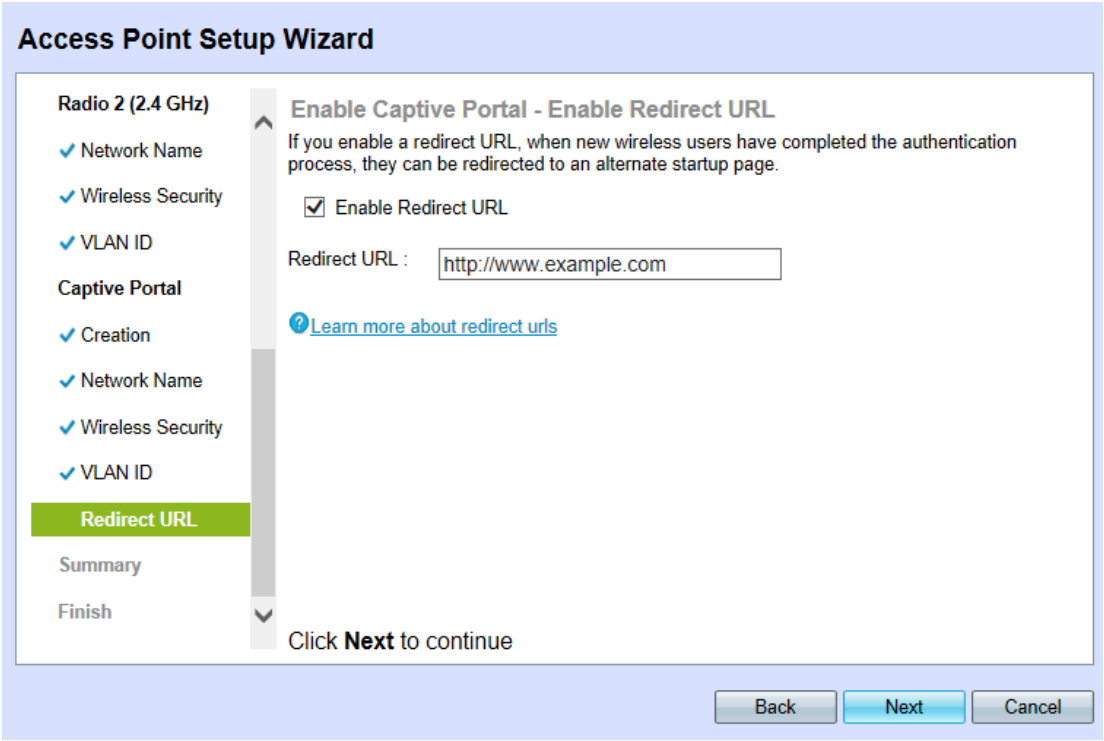


Note: If *No Security* is selected, the device will prompt you to confirm your decision.

Step 42. In the *VLAN ID* field, enter the ID number of the desired VLAN to which the WAP belongs to.

Note: The VLAN ID should match one of the VLAN IDs that is supported on the port of the remote device that is connected to the WAP.

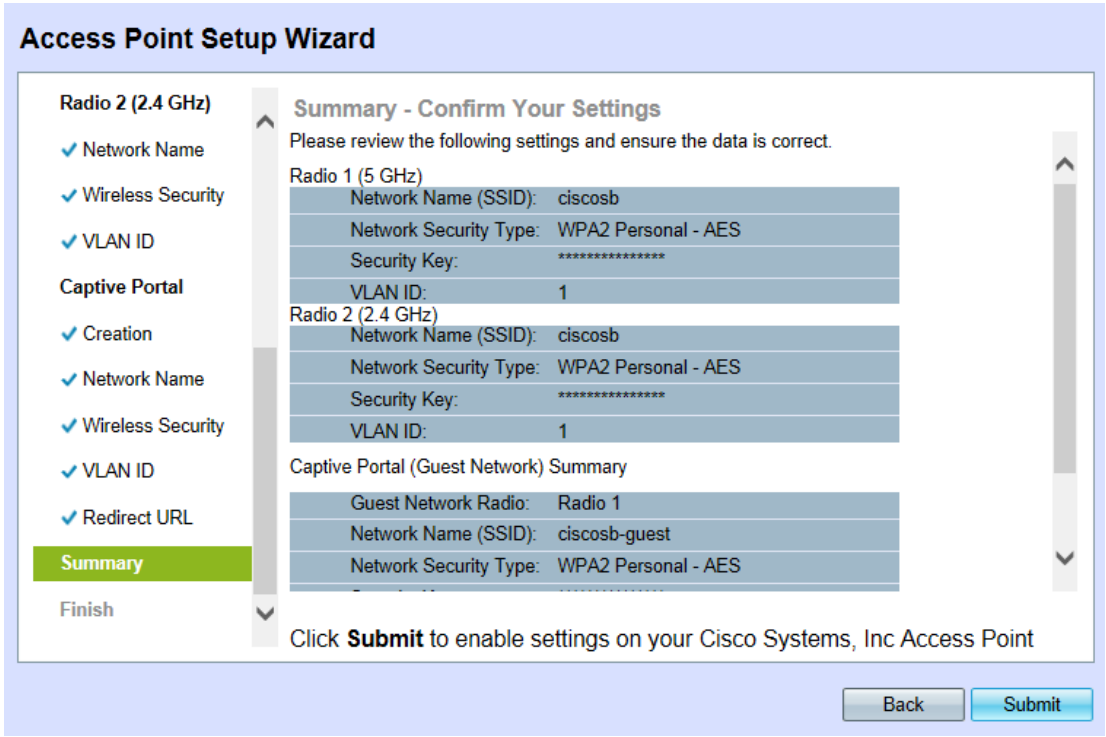
Step 43. Click **Next** to continue. The *Enable Captive Portal – Enable Redirect URL* page opens:



Step 44. (Optional) To redirect wireless users to a webpage after they log on to the guest network, check the **Enable Redirect URL** check box. If not enabled, skip to Step 46.

Step 45. In the *Redirect URL* field, enter the webpage you would like to redirect users to after they long on to the guest network.

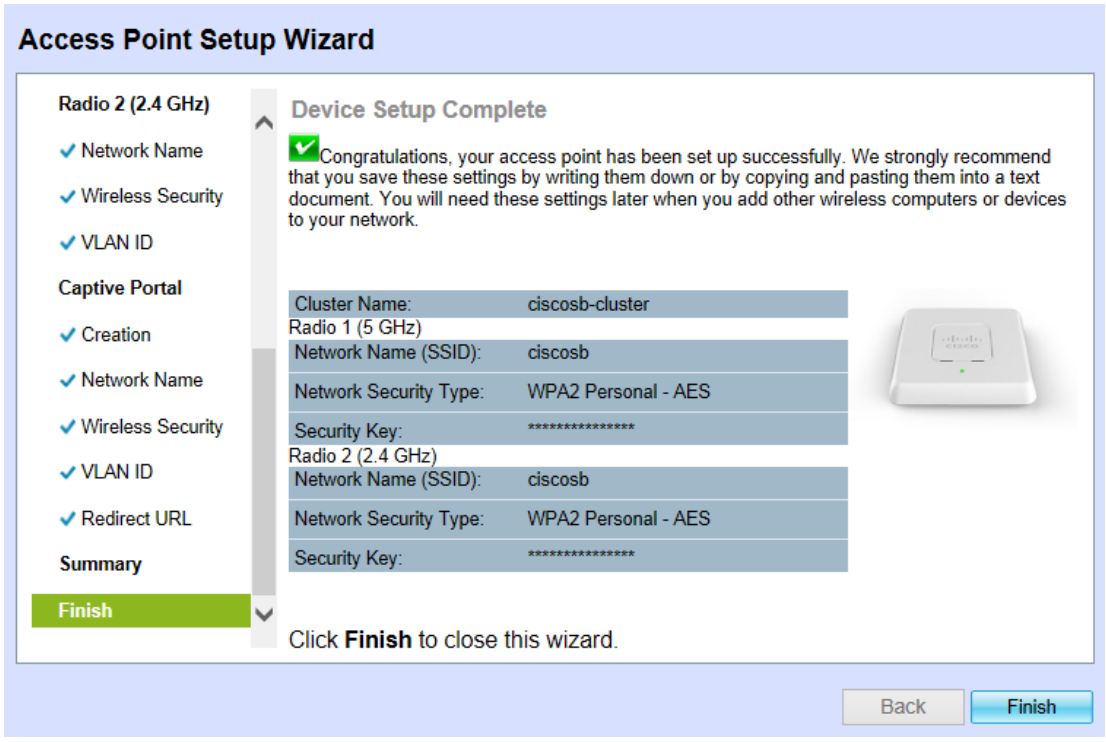
Step 46. Click **Next** to continue. The *Summary – Confirm Your Settings* page opens:



Step 47. (Optional) To edit a setting you made, click **Back** until you reach the desired page.

Step 48. (Optional) If you would like to exit the Setup Wizard and undo all the changes you made, click **Cancel**.

Step 49. Review the network and guest network settings. Click **Submit** to enable the settings on the WAP.



Step 50. Click **Finish** to exit the Setup Wizard.

Conclusion

Your WAP device should now have its basic settings configured. Along with the device password now being configured, both the device’s 2.4 GHz and 5 GHz radios are now configured with their own respective SSID and password configuration. The existence and configuration of a guest network is also now complete along with a potential URL redirect. These settings can be reconfigured at any point by following the appropriate page. The Setup Wizard can also be accessed again at any time.