

# Configuration of Setup Wizard on the WAP551

## Objective

The Setup Wizard is set of interactive instructions that guide you through the initial configuration of the WAP551. These instructions cover the basic configurations needed to operate the WAP551. The *Access Point Setup Wizard* window automatically appears the first time you log on to the WAP, but it can also be used at any point.

This article explains how to configure the WAP551 through the use of the Setup Wizard.

## Applicable Devices

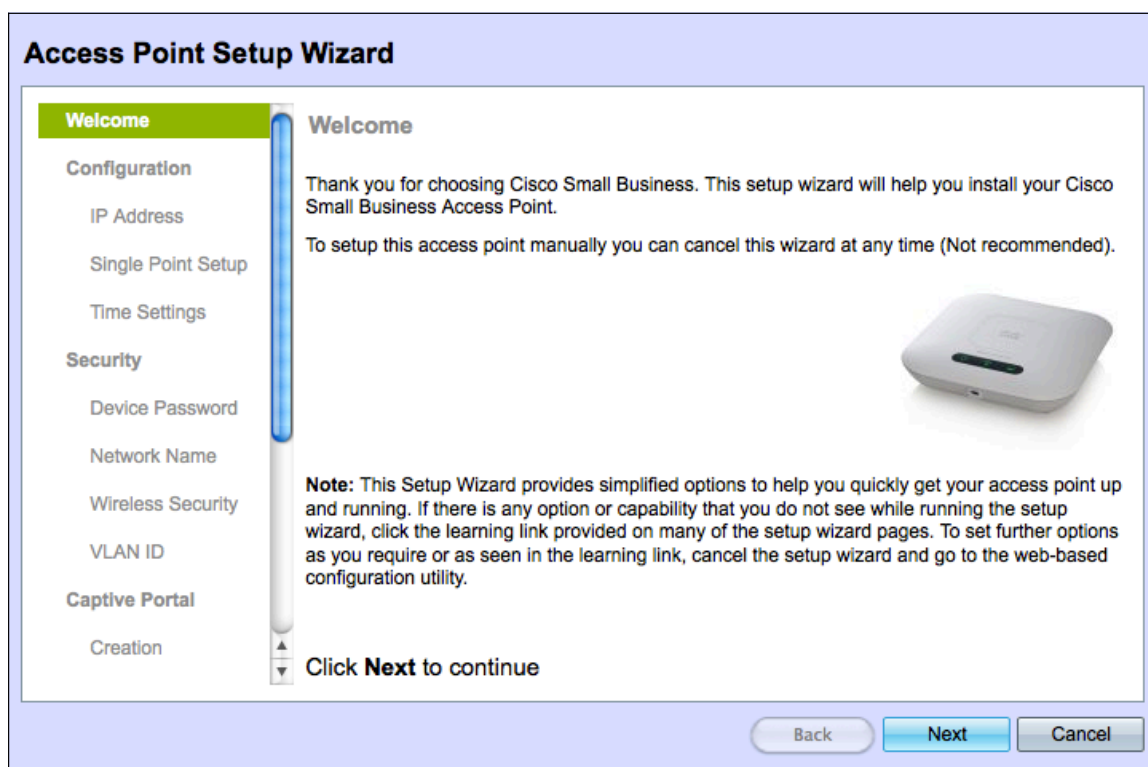
- WAP551

## Software Version

- v1.0.4.2

## Configure Setup Wizard

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



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

### Configure Device - IP Address

Select either Dynamic or Static IP address for your device.

Dynamic IP Address (DHCP) (Recommended)  
 Static IP Address

Static IP Address:  .  .  .

Subnet Mask:  .  .  .

Default Gateway:  .  .  .

DNS:  .  .  .

Secondary DNS (optional):  .  .  .

[? Learn more about the different connection types](#)

Click **Next** to continue

Step 3. Click the radio button that corresponds to the method you want to use to determine the IP address of the WAP.

- Dynamic IP Address (DHCP) (Recommended) — The IP address of the WAP is assigned by a DHCP server. If you choose Dynamic IP Address, skip to Step 9.
- Static IP Address — Allows you to create a fixed (static) IP address for the WAP. A static IP address does not change.

Step 4. In the Static IP Address field, enter the IP address of the WAP. This IP address is created by you and should not be used by another device in the network.

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

Step 6. In the Default Gateway field, enter the IP address of the default gateway for the WAP. 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 primary domain name system (DNS) server. If you want to access web pages outside of your network, the IP address of the DNS server should be given by your Internet service provider (ISP).

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

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

## Single Point Setup – Set A Cluster

A cluster provides a single point of administration and lets you view, deploy, configure, and secure the wireless network as a single entity, rather than as a series of separate wireless devices.

Create a New Cluster

Recommended for a new deployment environment.

New Cluster Name:

AP Location:

Join an Existing Cluster

Recommended for adding new wireless access points to the existing deployment environment.

Existing Cluster Name:

AP Location:

Do not Enable Single Point Setup

Recommended for single device deployments or if you prefer to configure each device individually.

Click **Next** to continue

Step 10. Click the radio button that corresponds with the cluster settings you would like to use. A cluster allows you to configure multiple access points (APs) as a single device. If you choose not to use a cluster, you will have to configure them individually.

- Create a New Cluster — Create a new cluster for APs.
- Join an Existing Cluster — Joins an existing AP cluster in your network.
- Do not Enable Single Point Setup — Single Point Setup (cluster) is not allowed. Skip to Step 13 if you choose this option.

Step 11. In the *Cluster Name* field, enter either an existing cluster name or create a new cluster name based on your decision in Step 10.

Step 12. In the AP Location field, enter the physical location of the WAP.

**Timesaver:** If you clicked the Join an Existing Cluster radio button, the WAP configures the rest of the settings based on the cluster. Click **Next**, a confirmation page will prompt and asks if you are sure that 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 13. Click **Next** to continue. The *Configure Device - Set System Date and Time* page opens:

**Configure Device - Set System Date And Time**

Enter the time zone, date and time.

Time Zone:

Set System Time:  Network Time Protocol (NTP)  
 Manually

NTP Server:

[? Learn more about time settings](#)

Click **Next** to continue

Step 14. Choose a time zone from the *Time Zone* drop-down list.

Step 15. Click the radio button that corresponds with the method that you wish to use to set the time of the WAP.

- Network Time Protocol (NTP) — The WAP gets the time from a NTP server.
- Manually — The time is manually entered into the WAP. If you choose manually, skip to Step 17.

Step 16. In the *NTP Server* field, enter the URL of the NTP server that provides the date and time. Skip to Step 19.

**Configure Device - Set System Date And Time**

Enter the time zone, date and time.

Time Zone:

Set System Time:  Network Time Protocol (NTP)  
 Manually

NTP Server:

[? Learn more about time settings](#)

Click **Next** to continue

Step 17. From the *System Date* drop-down lists, choose the month, day, and year respectively.

Step 18. From the *System Time* drop-down lists, choose the hour and minutes respectively.

Step 19. Click **Next** to continue. The *Enable Security - Set Password* page opens:

### Enable Security - Set Password


The administrative password protects your access point from unauthorized access. For security reasons, you should change the access point password from its default settings. Please write this password down for future reference.

Enter a new device password:

New password needs at least 8 characters composed of lower and upper case letters as well as numbers/symbols by default.

New Password:

Confirm Password:

Password Strength Meter:  Strong

Password Complexity:  Enable

[? Learn more about passwords](#)

Click **Next** to continue

Step 20. In the *New Password* field, enter a new password. This is the password that gives you administrative access to the WAP.

Step 21. In the *Confirm Password* field, re-enter the same password.

**Note:** As you enter a password, the number and color of vertical bars changes 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 strong.

Step 22. (Optional) To enable password complexity, check the **Enable** check box. This requires that the password is at least 8 characters long and composed of lower and upper case letters and number/symbols.

Step 23. Click **Next** to continue. The *Enable Security - Name Your Wireless Network* page opens:

## Enable Security - Name Your Wireless Network

The name of your wireless network, known as an SSID, identifies your network so that wireless devices can find it.

Enter a name for your wireless network:

Network Name (SSID):

For example: MyNetwork

[? Learn more about network names](#)

Click **Next** to continue

Step 24. 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 25. Click **Next** to continue. The *Enable Security - Secure Your Wireless Network* page opens.

## Enable Security - Secure Your Wireless Network

Select your network security strength.

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

Enter a security key with 8-63 characters.

.....

 Strong

Show Key as Clear Text

[? Learn more about your network security options](#)

Click **Next** to continue

Step 26. Click the radio button that corresponds with the network security that you would like to apply to your wireless network.

- 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 29.

Step 27. In the Security Key field, enter the password for your network.

Step 28. (Optional) To see the password as you type, check the **Show Key as Clear Text** check box.

Step 29. Click **Next** to continue. The *Enable Security - Assign The VLAN ID For Your Wireless Network* page opens.

### Enable Security - Assign The VLAN ID For Your Wireless Network

By default, the VLAN ID assigned to the management interface for your access point is 1, which is also the default untagged VLAN ID. If the management VLAN ID is the same as the VLAN ID assigned to your wireless network, then the wireless clients associated with this specific wireless network can administer this device. If needed, an access control list (ACL) can be created to disable administration from wireless clients.

Enter a VLAN ID for your wireless network:

VLAN ID:  (Range: 1 - 4094)

[? Learn more about vlan ids](#)

Click **Next** to continue

Step 30. In the VLAN ID field, enter the ID number of the VLAN to which you would like the WAP to belong.

**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 31. Click **Next** to continue. The *Enable Captive Portal - Create Your Guest Network* page opens:

## Enable Captive Portal - Create Your Guest Network

Use Captive Portal to set up a guest network, which means that wireless users need to be authenticated before they can access the Internet. For example, a hotel can create a guest network to redirect new wireless users to a page for authentication.

Do you want to create your guest network now?

- Yes  
 No, thanks.

[? Learn more about captive portal guest networks](#)

Click **Next** to continue

Step 32. Click the **Yes** radio button if you would like to create a guest network. A guest network requires users to be authenticated before they can use the Internet. A guest network is not required. Click the **No** radio button if you do not want to create a guest network and skip to Step 45.

Step 33. Click **Next** to continue. The *Enable Captive Portal - Name Your Guest Network* page opens:

## Enable Captive Portal - Name Your Guest Network

Your guest network needs a new name, known as an SSID. The name identifies your guest network so that wireless users can find it.

Enter a name for your guest network:

Guest Network name:   
For example: MyGuestNetwork

[? Learn more about network names](#)

Click **Next** to continue

Step 34. In the Guest Network name field, enter the SSID of the guest network.

Step 35. Click **Next** to continue. The *Enable Captive Portal - Secure Your Guest Network* page opens:



## Enable Captive Portal - Secure Your Guest Network

Select your guest network security strength.

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

Enter a security key with 8-63 characters.



Show Key as Clear Text

[? Learn more about your network security options](#)

Click **Next** to continue

Step 36. Click the radio button that corresponds with the network security you would like to apply to your guest network.

- Best Security (WPA2 Personal - AES) — Provides the best security and is recommended if your wireless devices support this option.
- Better Security — Provides security when there are older wireless devices that do not support 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 39.

Step 37. In the Security Key field, enter the password for the guest network.

Step 38. (Optional) To see the password as you type, check the **Show Key as Clear Text** check box.

Step 39. Click **Next** to continue. The *Enable Captive Portal - Assign The VLAN ID* page opens:

### Enable Captive Portal - Assign The VLAN ID

We strongly recommend that you assign different VLAN ID for your guest network than the management VLAN ID. By doing that, your guest will have no access to your private network.

Enter a VLAN ID for your guest network:

VLAN ID:  (Range: 1 - 4094)

[? Learn more about vlan ids](#)

Click **Next** to continue

Step 40. In the VLAN ID field, enter the ID number of the VLAN to which you would like the guest network to belong.

**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 41. Click **Next** to continue. The *Enable Captive Portal - Enable Redirect URL* page opens:

### Enable Captive Portal - Enable Redirect URL

If you enable a redirect URL, when new wireless users have completed the authentication process, they can be redirected to an alternate startup page.

Enable Redirect URL

Redirect URL :

[? Learn more about redirect urls](#)

Click **Next** to continue

Step 42. (Optional) To redirect wireless users to a webpage after they log on to the guest network, check the **Enable Redirect URL** check box.

**Timesaver:** If you do not check the **Enable** check box, skip to Step 44.

Step 43. In the Redirect URL field, enter the webpage you would like to redirect users to after they log on to the guest network.

Step 44. Click **Next** to continue. The *Summary - Confirm Your Settings* page opens:

### Summary - Confirm Your Settings

Please review the following settings and ensure the data is correct.

Network Name (SSID):	ciscosb
Network Security Type:	plain-text
Security Key:	
VLAN ID:	1

Captive Portal (Guest Network) Summary

Network Name (SSID):	Guest
Network Security Type:	WPA2 Personal - AES
Security Key:	*****
Verification:	Guest
Redirect URL:	http://www.example.com
VLAN ID:	5

Note: The AP Radio will be enabled after clicking Submit.

Click **Submit** to enable settings on your Cisco Small Business Access Point

Step 45. (Optional) To edit a setting you made, click **Back**.

Step 46. (Optional) If you would like to exit the Setup Wizard and undo all the changes you made, click **Cancel**.

Step 47. Review the network and guest network settings. Click **Submit** to enable the settings on the WAP. A loading bar appears as the WAP enables your settings. When the WAP is finished, the *Finish* page opens:

**Note:** Step 48 is only applicable if you click **Submit** on the *Confirm Your Settings* page.

## Device Setup Complete



Congratulations, your access point has been set up successfully. We strongly recommend that you save these settings by writing them down or by copying and pasting them into a text document. You will need these settings later when you add other wireless computers or devices to your network.

Cluster Name:	ciscosb-cluster
Network Name (SSID):	ciscosb
Network Security Type:	plain-text
Security Key:	



Note: To configure WPS, Click "Run WPS" on the Getting Started page, under Initial Setup.

Click **Finish** to close this wizard.

Back

Finish

Cancel

Step 48. Click **Finish** to exit the Setup Wizard.