

# Configuración inicial de los puntos de acceso de red inalámbrica WAP150, WAP351, WAP361, y WAP371 usando el asistente para la configuración

## Objetivo

El asistente para la configuración es una característica incorporada que se utiliza para ayudar con la configuración inicial de los puntos de acceso de red inalámbrica (WAP). Hace la configuración de las configuraciones básicas fácil. El proceso gradual del asistente para la configuración le dirige con la configuración inicial del dispositivo WAP, y proporciona a un modo rápido de conseguir las funciones básicas del WAP funcionales.

El objetivo de este documento es mostrarle cómo configurar los puntos de acceso de red inalámbrica WAP150, WAP351, WAP361, y WAP371 usando el asistente para la configuración.

## Dispositivos aplicables

- WAP150
- WAP351
- WAP361
- WAP371

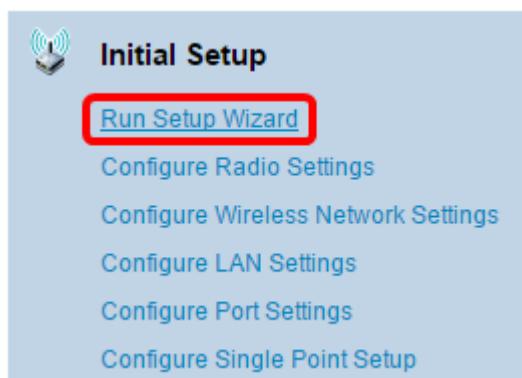
## Versión del software

- 1.0.1.7 – WAP150, WAP361
- 1.0.2.8 – WAP351
- 1.3.0.3 – WAP371

## Configuración

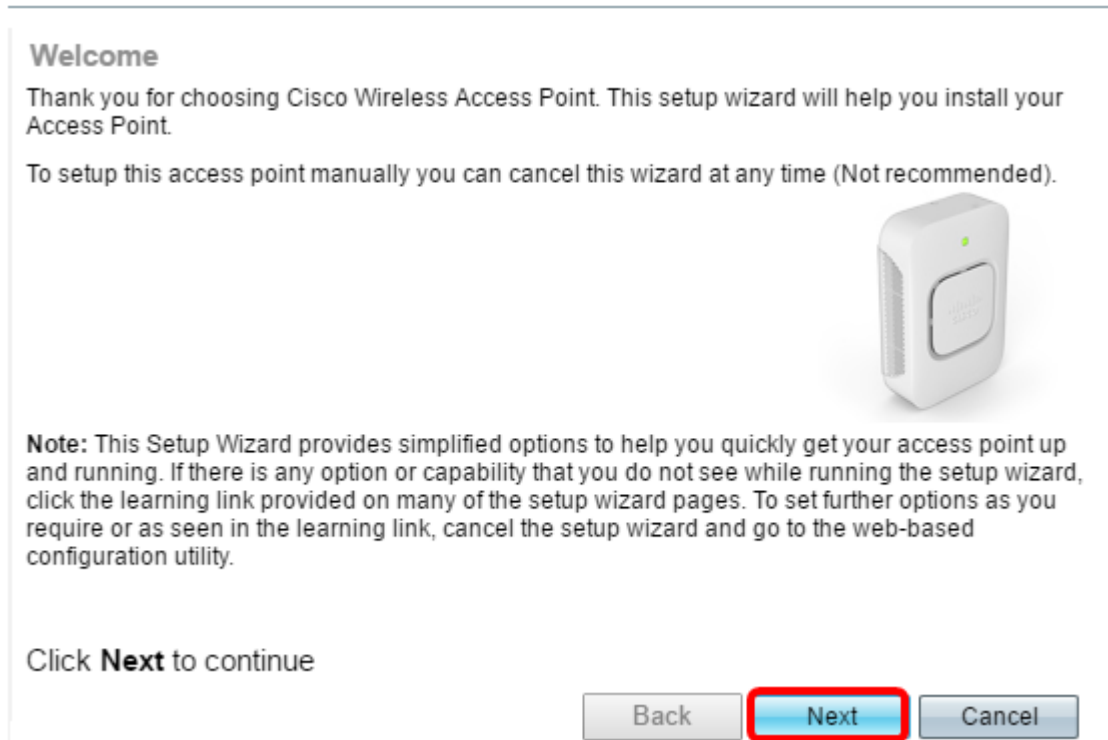
**Nota:** Las imágenes usadas abajo se toman de WAP361.

Paso 1. Login a la utilidad basada en web del Punto de acceso. Conforme a la página del menú de la introducción, el teclado funciona con el asistente para la configuración.



**Nota:** Si esto está la primera vez usted ha abierto una sesión al WAP, el asistente para la configuración se abrirá automáticamente.

Paso 2. Haga clic **después** en la página de Bienvenida del asistente para la configuración del Punto de acceso para continuar.



Paso 3. Haga clic el botón de radio que corresponde al método que usted quiere utilizar para determinar el IP Address del WAP.

Se definen las opciones como sigue:

- (DHCP) del IP Address dinámico (recomendado) — Permite que el servidor DHCP asigne un IP Address dinámico para el WAP. Si usted elige esto, haga clic **después** entonces el salto al [paso 9](#).
- IP Address estático — Permite que usted cree una dirección IP (estática) fija para el WAP. Un IP Address estático no cambia.

**Nota:** En este ejemplo, se elige el (DHCP) del IP Address dinámico.

### 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

Paso 4. Si el IP Address estático fue elegido en el paso anterior, ingrese el IP Address del WAP en el campo de *IP Address estático*. Esta dirección IP es única al WAP y no se debe utilizar por otro dispositivo en la red.

Dynamic IP Address (DHCP) (Recommended)

Static IP Address

Static IP Address:  .  .  .

Subnet Mask:  .  .  .

Default Gateway:  .  .  .

DNS:  .  .  .

Secondary DNS (optional):  .  .  .

**Nota:** En este ejemplo, 192.168.1.121 se utiliza como el IP Address estático.

Paso 5. Ingrese a la máscara de subred en el campo de la *máscara de subred*.

Dynamic IP Address (DHCP) (Recommended)

Static IP Address

Static IP Address:  .  .  .

Subnet Mask:  .  .  .

Default Gateway:  .  .  .

DNS:  .  .  .

Secondary DNS (optional):  .  .  .

**Nota:** En este ejemplo, 255.255.255.0 se utiliza como la máscara de subred.

Paso 6. Ingrese el default gateway para el WAP en el campo del *default gateway*. Éste es el IP Address privado de su router.

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

Static IP Address:  .  .  .   
 Subnet Mask:  .  .  .   
 Default Gateway:  .  .  .   
 DNS:  .  .  .   
 Secondary DNS (optional):  .  .  .

**Nota:** En este ejemplo, 192.168.1.1 se utiliza como el default gateway.

El paso 7. (opcional) si usted quiere acceder el exterior utilitario basado en web de su red, ingresa el direccionamiento primario del Domain Name System (DNS) en el campo *DNS*. Su Proveedor de servicios de Internet (ISP) debe proporcionar el DNS Server Address a usted.

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

Static IP Address:  .  .  .   
 Subnet Mask:  .  .  .   
 Default Gateway:  .  .  .   
 DNS:  .  .  .   
 Secondary DNS (optional):  .  .  .

**Nota:** En este ejemplo, 192.168.1.2 se utiliza como la dirección de DNS.

El paso 8. (opcional) ingresa un direccionamiento de los DN secundarios en los campos de los *DN secundarios* después hace clic **después**.

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

Static IP Address:  .  .  .   
 Subnet Mask:  .  .  .   
 Default Gateway:  .  .  .   
 DNS:  .  .  .   
 Secondary DNS (optional):  .  .  .

**Nota:** En este ejemplo, 192.168.1.3 se utiliza como el direccionamiento de los DN secundarios.

## Configuración monopunto

**Paso 9.** En la configuración monopunto – Fije una pantalla del cluster, seleccione un botón de radio que corresponda a cómo usted quiere configurar las configuraciones del cluster del WAP. El clúster permite que usted maneje los múltiples puntos de acceso de un monopunto, en vez de ir a cada dispositivo y de cambiar las configuraciones individualmente.

Se definen las opciones como sigue:

- Nuevo nombre de clúster — Seleccione esta opción si usted quiere crear un nuevo cluster.

**Nota:** Para WAP351 y WAP371, la opción es crea un nuevo cluster.

- Únase a un clúster existente — Seleccione esta opción si usted quisiera que el WAP se uniera a un clúster existente. Si usted elige esta opción, salte al [paso 11](#).
- No habilite la configuración monopunto — Elija esta opción si usted no quisiera que el WAP fuera parte de al cluster. Si usted elige esta opción, haga clic **después** entonces el salto al [paso 13](#).

**Nota:** En este ejemplo, no habilite la configuración monopunto se elige.

**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.

New Cluster Name  
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.

[Learn more about single point setup](#)

Click **Next** to continue

Back Next Cancel

Paso 10. Si usted eligió el nuevo nombre de clúster en el paso anterior, ingrese el nombre del nuevo cluster y su ubicación en los *nuevos* campos del *nombre de clúster* y de la *ubicación AP*, entonces hace clic respectivamente **después**. La ubicación AP es la ubicación física del Punto de acceso definido por el usuario (e.g. oficina). Vaya a [Step13](#).

**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.

**New Cluster Name**  
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.

[? Learn more about single point setup](#)

Click **Next** to continue

Back **Next** Cancel

**Paso 11.** Si usted eligió **únase a un clúster existente** en el paso 9, ingresan el nombre del cluster y su ubicación en los campos del *nombre del clúster existente* y de la *ubicación AP*, entonces hace clic respectivamente **después**.

**Nota:** Esta opción es ideal si hay ya una red inalámbrica existente y todas las configuraciones se han configurado ya.

**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.

**New Cluster Name**  
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.

[? Learn more about single point setup](#)

Click **Next** to continue

Back **Next** Cancel

**Paso 12.** Revise sus configuraciones para asegurarse los datos está correcto entonces hacen clic **someten**.

**Summary - Confirm Your Settings**  
Please review the following settings and ensure the data is correct.

You are about to join this cluster:      Main Point

Click **Submit** to enable settings on your Cisco Wireless Access Point

Back    **Submit**    Cancel

## Configuraciones horarias

[Paso 13](#). Elija su huso horario de la lista desplegable del huso horario.

**Configure Device - Set System Date And Time**  
Enter the time zone, date and time.

Time Zone:      USA (Pacific) ▼

Set System Time:      USA (Aleutian Islands) ▲  
USA (Arizona)  
USA (Central)  
USA (Eastern)  
USA (Mountain)  
**USA (Pacific)**

NTP Server 1:      Uzbekistan  
NTP Server 2:      Vanuatu  
NTP Server 3:      Vatican City  
NTP Server 4:      Venezuela  
Vietnam  
Wake Islands  
Wallis & Futana Islands  
Western Samoa  
Windward Islands  
Yemen  
Zaire (Kasai)  
Zaire (Kinshasa)  
Zambia  
Zimbabwe

[? Learn more about t](#)

Click **Next** to continue

Back    **Next**    Cancel

**Nota:** En este ejemplo, el USA (pacífico) se elige.

Paso 14. Haga clic el botón de radio que corresponde al método que usted desea utilizar para fijar la época del WAP.

Las opciones son como sigue:

- Network Time Protocol (NTP) — El WAP consigue el tiempo de un servidor NTP.
- Manualmente — El tiempo se ingresa manualmente en el WAP. Si se elige esta opción, salte al [paso 16](#).

**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 1:

NTP Server 2:

NTP Server 3:

NTP Server 4:

[? Learn more about time settings](#)

Click **Next** to continue

**Nota:** En este ejemplo, se utiliza el Network Time Protocol (NTP).

Paso 15. Ingrese el Domain Name del servidor NTP que proporciona la fecha y hora en el campo del *servidor NTP 1*. Usted puede agregar a hasta cuatro diversos servidores NTP ingresandolos en sus campos respectivos y después hacer clic **después**. Entonces, salto al [paso 17](#).

**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 1:

NTP Server 2:

NTP Server 3:

NTP Server 4:

[? Learn more about time settings](#)

Click **Next** to continue

**Nota:** En este ejemplo, hay cuatro servidores NTP ingresados.

[Paso 16](#). (Opcional) si usted eligió manualmente en el paso 14, seleccione la fecha en las listas desplegables de la fecha del sistema para elegir el mes, el día, y el año respectivamente. Seleccione la hora y los minutos de las listas desplegables del Tiempo del sistema después hacen clic **después**.



**Configure Device - Set System Date And Time**  
Enter the time zone, date and time.

Time Zone:

Set System Time:  Network Time Protocol (NTP)  
 Manually

System Date:

System Time:  :

[Learn more about time settings](#)

Click **Next** to continue

## Contraseña del dispositivo

[Paso el 17](#). In el dispositivo de la configuración - Fije la pantalla de la contraseña, ingrese una nueva contraseña para el WAP en el *nuevo* campo de *contraseña* y confírmela. Esta contraseña se utiliza para tener el acceso administrativo a la utilidad basada en web del WAP sí mismo y no para conectar con la red inalámbrica.

New Password:

Confirm Password:

Password Strength Meter:  Below Minimum

**Nota:** El campo del *contador de la fuerza de la contraseña* visualiza las barras verticales que cambian mientras que usted ingresa la contraseña.

Se definen los colores del contador de la fuerza de la contraseña como sigue:

- Rojo — El requisito mínimo de la complejidad de contraseñas no se cumple.
- Anaranjado — Se cumple el requisito mínimo de la complejidad de contraseñas, pero la fuerza de la contraseña es débil.
- Verde — Se cumple el requisito mínimo de la complejidad de contraseñas, y la fuerza de la contraseña es fuerte.

Paso 18. Complejidad (opcional) de la contraseña habilitada marcando la casilla de verificación de la complejidad de la **contraseña habilitada**. Esto requiere que la contraseña sea por lo menos 8 caracteres de largo e integrado por cartas más bajas y mayúsculas y los números o los símbolos. La complejidad de contraseñas se habilita por abandono.

New Password:

Confirm Password:

Password Strength Meter:  Below Minimum

Password Complexity:  Enable

[? Learn more about passwords](#)

Click **Next** to continue

Paso 19. Para continuar, haga clic en Next (Siguiente).

## El configurar radia 1 y 2 (2.4 y 5 gigahertz)

Las configuraciones de la red inalámbrica se deben configurar individualmente para cada canal de radio. El proceso para configurar la red inalámbrica es lo mismo para cada canal.

**Nota:** Para el WAP371, la radio 1 está para la banda 5 gigahertz y Radio 2 está para la banda 2.4 gigahertz.

Paso 20. En la radio 1 de la configuración - Nombre su área de la red inalámbrica, ingrese un nombre para la red inalámbrica en el campo del *nombre de red (SSID)* después haga clic **después**.

**Configure Radio 1 - 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

**Nota:** En este ejemplo, WAP361\_L2 se utiliza como el nombre de red.

Paso 21. En la radio 1 de la configuración - Asegure su área de la red inalámbrica, haga clic el botón de radio que corresponde con la seguridad de la red que usted quisiera aplicarse a su red inalámbrica.

Se definen las opciones como sigue:

- La mejor Seguridad (WPA2 personal - AES) — proporciona la mejor Seguridad y se recomienda si sus dispositivos de red inalámbrica soportan esta opción. Advanced Encryption Standard (AES) personal y una clave previamente compartida (PSK) de las aplicaciones WPA2 entre los clientes y el Punto de acceso. Utiliza una nueva clave de encriptación para cada sesión, que hace difícil comprometer.
- Una mejor Seguridad (WPA/WPA2 personal - TKIP/AES) — proporciona la Seguridad cuando hay más viejos dispositivos de red inalámbrica que no soportan el WPA2. Aplicaciones personales AES WPA y Temporal Key Integrity Protocol (TKIP). Utiliza el estándar del Wi-Fi de IEEE 802.11i.
- Ninguna Seguridad (no recomendada) — La red inalámbrica no requiere una contraseña y se puede acceder por cualquier persona. Si está elegida, una ventana emergente aparecerá que pregunta si usted quiere inhabilitar la Seguridad; haga clic **sí** para continuar. Si se elige esta opción, salte al [paso 24](#).

### Configure Radio 1 - 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/WPA2 Personal - TKIP/AES)  
Recommended for older wireless computers and devices that might not support WPA2.
- No Security (Not recommended)

**Nota:** En este ejemplo, se elige la mejor Seguridad (WPA2 personal - AES).

Paso 22. Ingrese la contraseña para su red en el campo de *clave de seguridad*. La barra coloreada a la derecha de este campo muestra la complejidad de la contraseña ingresada.

### Configure Radio 1 - 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/WPA2 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.

Session Key Refresh Rate

Show Key as Clear Text

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

Paso 23. (Opcional) para ver la contraseña como usted teclea, marque la **clave de la demostración como** casilla de verificación del **texto claro** después haga clic **después**.

Enter a security key with 8-63 characters.

SecretKey1

Weak

Show Key as Clear Text

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

Click **Next** to continue

Back

Next

Cancel

Paso 24. En la radio 1 de la configuración - Asigne El VLAN ID para su área de la red inalámbrica, elija un ID para la red de la lista desplegable VLAN ID. Si el VLAN de administración es lo mismo que el VLAN asignado a la red inalámbrica, los clientes de red inalámbrica en la red pueden administrar el dispositivo. Usted puede también utilizar las listas de control de acceso (ACL) para inhabilitar la administración de los clientes de red inalámbrica.

**Nota:** Para WAP371 y WAP150, usted necesita teclear adentro el ID en el campo *VLAN ID* proporcionado. El rango VLAN ID es a partir de la 1-4094.

### Configure Radio 1 - 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:

1 ▼

[? Learn more about vlan ids](#)

Click **Next** to continue

Back

Next

Cancel

**Nota:** En este ejemplo, se utiliza el VLAN ID 1.

Paso 25. El teclado **al lado** del continúa con el asistente para la configuración configurar Radio 2.

**Note:** El proceso para configurar las configuraciones de la red inalámbrica para Radio 2 es lo mismo que el de la radio 1.

## Portal prisionero

El portal prisionero permite que usted configure una red del invitado en donde necesidad de usuarios de red inalámbrica de ser autenticado primero antes de que puedan tener acceso a Internet. Siga los pasos abajo para configurar el portal prisionero.

Paso 26. En el portal prisionero del permiso - Cree su área de la red del invitado, elija el **botón Yes Radio Button** después haga clic **después**.

**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 quest networks](#)

Click **Next** to continue

Back Next Cancel

**Nota:** Si usted prefiere no habilitar el portal prisionero, haga clic **ningún** y el asistente para la configuración le llevará a la página de resumen. Entonces, salto al [paso 35](#).

Paso 27. Seleccione la radio frecuencia deseada para la red del invitado. El soporte de 2.4 gigahertz ofertas de la banda para los dispositivos antiguos y puede propagar una señal inalámbrica más amplia a través de las paredes múltiples. La banda 5 gigahertz, por otra parte, se aprieta y puede menos proporcionar más producción tomando las 40 frecuencias en MHz de la banda en vez del MHz del estándar 20 en la banda 2.4 gigahertz. Además del menor alcance, hay también menos dispositivos que soportan la banda 5 gigahertz comparada a 2.4 gigahertz.

Radio:  Radio 1 (5 GHz)  
 Radio 2 (2.4 GHz)

Guest Network name:   
For example: MyGuestNetwork

**Nota:** En este ejemplo, se elige la radio 1 (5 gigahertz).

Paso 28. Ingrese el nombre del invitado SSID en el *campo de nombre de la red del invitado* después haga clic **después**.

**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:

Radio:  Radio 1 (5 GHz)  
 Radio 2 (2.4 GHz)

Guest Network name:   
For example: MyGuestNetwork

[? Learn more about network names](#)

Click **Next** to continue

**Nota:** ¡En este ejemplo, BeMyGuest! se utiliza como el nombre de red del invitado.

Paso 29. Haga clic el botón de radio que corresponde a la seguridad de la red que usted quisiera aplicarse a su red inalámbrica del invitado.

Se definen las opciones como sigue:

- La mejor Seguridad (WPA2 personal - AES) — proporciona la mejor Seguridad y se recomienda si sus dispositivos de red inalámbrica soportan esta opción. WPA2 aplicaciones personales AES y una clave previamente compartida (PSK) entre los clientes y el Punto de acceso. Utiliza una nueva clave de encriptación para cada sesión que haga difícil comprometer.
- Una mejor Seguridad (WPA personal - TKIP/AES) — proporciona la Seguridad cuando hay más viejos dispositivos de red inalámbrica que no soportan el WPA2. Aplicaciones personales AES y TKIP WPA. Utiliza el estándar del Wi-Fi de IEEE 802.11i.
- Ninguna Seguridad (no recomendada) — La red inalámbrica no requiere una contraseña y se puede acceder por cualquier persona. Si está elegida, una ventana emergente aparecerá que pregunta si usted quiere inhabilitar la Seguridad; haga clic **sí** para continuar. Si se elige esta opción, haga clic **después** entonces el salto al [paso 35](#).

**Nota:** En este ejemplo, se elige una mejor Seguridad (WPA personal - TKIP/AES).

### 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/WPA2 Personal - TKIP/AES)  
Recommended for older wireless computers and devices that might not support WPA2.
- No Security (Not recommended)

Paso 30. Ingrese la contraseña para su red en el campo de *clave de seguridad*. La barra coloreada a la derecha de este campo muestra la complejidad de la contraseña ingresada.

Enter a security key with 8-63 characters.

.....

Show Key as Clear Text

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

Click **Next** to continue

Back Next Cancel

Paso 31. (Opcional) para ver la contraseña como usted teclea, marque la **clave de la demostración como** casilla de verificación del **texto claro** después haga clic **después**.

Enter a security key with 8-63 characters.

GuestPassw0rd

Show Key as Clear Text

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

Click **Next** to continue

Back Next Cancel

Paso 32. En el portal prisionero theEnable – Asigne el área VLAN ID, elija un ID para la red del invitado de la lista desplegable VLAN ID después haga clic **después**.

**Nota:** Para WAP371 y WAP150, usted necesita teclear adentro el ID en el campo *VLAN ID* proporcionado. El rango VLAN ID es a partir de la 1-4094.

**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: 2 ▼

[Learn more about vlan ids](#)

Click **Next** to continue

Back Next Cancel

**Nota:** En este ejemplo, se elige el VLAN ID 2.

Paso 33. (Opcional) si usted quisiera que reorientaran a los usuarios nuevos a una página de lanzamiento alternativa, marque el **permiso reorientan la** casilla de verificación **URL** en el portal prisionero del permiso – el permiso reorienta la pantalla URL.

### 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 :

Paso 34. (Opcional) ingrese el URL para su reorientan el URL en el campo *URL de la reorientación* después hacen clic **después**.

### 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

**Nota:** En este ejemplo, <http://newuser.com> se utiliza como la reorientación URL.

## Resumen

**Paso 35.** Revise las configuraciones mostradas y asegúrese de que la información está correcta. Si usted quisiera cambiar una configuración, haga clic el **botón Back Button** hasta que se alcance la página deseada. Si no, el tecleo **some** para habilitar sus configuraciones en el WAP.



### Summary - Confirm Your Settings

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

Radio 1 (2.4 GHz)

Network Name (SSID):	WAP361_L2
Network Security Type:	WPA2 Personal - AES
Security Key:	SecretKey1
VLAN ID:	1

Radio 2 (5 GHz)

Network Name (SSID):	WAP361_L 2 _5ghz
Network Security Type:	WPA2 Personal - AES
Security Key:	SecretKey2
VLAN ID:	1

Captive Portal (Guest Network) Summary

Guest Network Radio:	Radio 1
Network Name (SSID):	BeMyGuest!
Network Security	WPA2 Personal - AES

Click **Submit** to enable settings on your Cisco Wireless Access Point

Paso 36. La pantalla completa de la configuración de dispositivo entonces aparecerá confirmar que su dispositivo se ha configurado con éxito. Haga clic en Finish (Finalizar).

### 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

Radio 1 (2.4 GHz)

Network Name (SSID):	WAP361_L2
Network Security Type:	WPA2 Personal - AES
Security Key:	SecretKey1

Radio 2 (5 GHz)

Network Name (SSID):	WAP361_L 2 _5ghz
Network Security Type:	WPA2 Personal - AES
Security Key:	SecretKey2



Click **Finish** to close this wizard.

Usted debe ahora haber configurado con éxito su unto de acceso de red inalámbrica usando

el asistente para la configuración.