

Configuración del portal cautivo en un WAP571 o WAP571E

Objetivo

Un portal cautivo (CP) permite restringir el acceso a la red inalámbrica hasta que se hayan verificado los usuarios inalámbricos. Cuando un usuario abre un navegador web, se le redirige a una página de inicio de sesión donde debe introducir su nombre de usuario y contraseña. Se pueden autorizar dos tipos de usuarios para acceder a la red; usuarios e invitados autenticados. Los usuarios autenticados deben proporcionar un nombre de usuario y una contraseña que coincidan con una base de datos local o con la base de datos de un servidor RADIUS. Los invitados no necesitan proporcionar un nombre de usuario ni una contraseña.

En este artículo se explica cómo configurar el portal cautivo en el punto de acceso inalámbrico (WAP).

Dispositivos aplicables

- Serie WAP500: WAP571, WAP571E

Versión del software

- 1.0.0.15 - WAP571, WAP571E

Configurar el portal cautivo

Los parámetros básicos del portal cautivo se pueden configurar mediante el asistente de configuración, mientras que los parámetros avanzados se pueden configurar mediante la utilidad basada en Web. Para una configuración rápida y básica, puede utilizar el asistente de configuración para activar la función. Consulte los siguientes pasos:

Nota: Las imágenes siguientes se capturan del dispositivo WAP571.

Uso del asistente de configuración

Paso 1. Inicie sesión en la utilidad basada en Web y, a continuación, haga clic en **Ejecutar asistente de configuración**.


CISCO WAP571 Wireless-AC/N Premium Dual R

Getting Started

- Run Setup Wizard
- ▶ Status and Statistics
- ▶ Administration
- ▶ LAN
- ▶ Wireless
- ▶ Spectrum Analyzer
- ▶ System Security
- ▶ Client QoS
- ▶ ACL
- ▶ SNMP
- ▶ Captive Portal
- ▶ Single Point Setup

Getting Started

Use the following links to quickly configure your access

 **Initial Setup**

- Run Setup Wizard
- Configure Radio Settings
- Configure Wireless Network Settings
- Configure LAN Settings
- Configure Single Point Setup

 **Device Status**

Nota: Si es la primera vez que configura el WAP, el asistente de configuración aparecerá automáticamente.

Paso 2. Siga las instrucciones de las pantallas del asistente de configuración. Para una configuración paso a paso de su WAP mediante el asistente de configuración, haga clic [aquí](#) para obtener instrucciones.

Welcome

Thank you for choosing Cisco Systems, Inc. This setup wizard will help you install your Cisco Systems, Inc Access Point.

To setup this access point manually you can cancel this wizard at any time (Not recommended).



Note: This Setup Wizard provides simplified options to help you quickly get your access point up and running. If there is any option or capability that you do not see while running the setup wizard, click the learning link provided on many of the setup wizard pages. To set further options as you require or as seen in the learning link, cancel the setup wizard and go to the web-based configuration utility.

Click **Next** to continue

Back

Next

Cancel

Paso 3. Una vez que aparezca la pantalla Enable Captive Portal - Create Your Guest Network (Habilitar portal cautivo - Crear red de invitado), elija **Yes** y luego haga clic en **Next**.

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

Back

Next

Paso 4. Ingrese el nombre de la red de invitado y luego haga clic en **Next**.

Nota: El nombre de red de invitado predeterminado es ciscosb-guest.

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

Back

Next

Paso 5. Elija un tipo de seguridad para la red de invitado inalámbrica.

Nota: A continuación se muestra un ejemplo de la mejor seguridad (WPA2 Personal - 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 6. Introduzca la clave de seguridad y, a continuación, haga clic en **Siguiente**.

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)

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

Paso 7. Ingrese un ID de VLAN para su red de invitado y luego haga clic en **Next**.

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

Back

Next

Paso 8. (Opcional) Si tiene una página web específica que desea mostrar después de que los usuarios acepten los términos de servicio de la página de bienvenida, marque la casilla de verificación **Habilitar URL de redirección**. Ingrese la URL y luego haga clic en **Next**.

Nota: La URL puede ser el sitio web de su empresa.

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

Back

Next

Paso 9. Revise y confirme los parámetros y, a continuación, haga clic en **Enviar**.

Summary - Confirm Your Settings

Security Key:	Cisco1234\$
VLAN ID:	1

Radio 2 (2.4 GHz)

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

Captive Portal (Guest Network) Summary

Guest Network Radio:	Radio 1
Network Name (SSID):	ciscosb-guest
Network Security Type:	WPA2 Personal - AES
Security Key:	*****
Verification:	Guest
Redirect URL:	https://cisco.com


Click **Submit** to enable settings on your Cisco Systems, Inc Access Point

Back

Submit

Paso 10. Cuando aparezca la pantalla Device Setup Complete (Configuración del dispositivo finalizada), haga clic en **Finish** para cerrar el asistente de configuración.

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 (5 GHz)	
Network Name (SSID):	ciscosb
Network Security Type:	WPA2 Personal - AES
Security Key:	*****
Radio 2 (2.4 GHz)	
Network Name (SSID):	ciscosb
Network Security Type:	WPA2 Personal - AES
Security Key:	*****



Click **Finish** to close this wizard.

Back

Finish

Ahora debería haber configurado los parámetros básicos de la función Portal cautivo de su WAP.

Uso de la utilidad basada en Web

Para configurar los parámetros avanzados del portal cautivo en el WAP, debe seguir varios pasos:

Habilitación global del portal cautivo: esto permite que los portales cautivos entren en vigor.

Crear una instancia de portal cautivo: una instancia de portal cautivo es un conjunto de parámetros que controla cómo un usuario inicia sesión en un punto de acceso virtual (VAP).

Asociar una instancia de portal cautivo con un VAP: los usuarios que intentan acceder al VAP deben seguir los parámetros configurados para la instancia.

Personalizar el portal web: el portal web es la página web en la que se redirige a los usuarios cuando intentan conectarse al VAP.

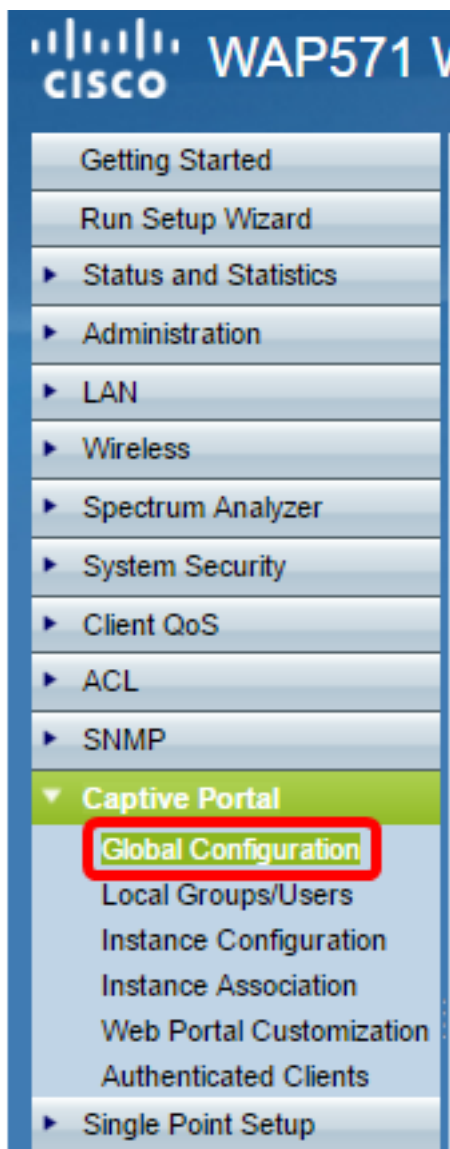
Crear grupo local: el grupo local se puede asignar a una instancia, que acepta usuarios

que pertenecen a ese grupo.

Crear usuario local: los usuarios locales se agregan a un grupo local y se les permite acceder al portal cautivo al que está configurado el grupo.

Habilitar globalmente el portal cautivo

Paso 1. En la utilidad basada en web, elija **Portal cautivo > Configuración global**.



Paso 2. (Opcional) Introduzca el número de segundos que el usuario debe introducir la información de autenticación antes de que WAP cierre la sesión de autenticación en el campo *Tiempo de espera de autenticación*.

Global Configuration

Captive Portal Mode: Enable

Authentication Timeout: Sec (Range: 60 - 600, Default: 300)

Additional HTTP Port: (Range: 1025 - 65535 or 80, 0 = Disable, Default: 0)

Additional HTTPS Port: (Range: 1025 - 65535 or 443, 0 = Disable, Default: 0)

Paso 3. (Opcional) Si desea que la información HTTP entre el WAP y el cliente utilice un puerto diferente además del predeterminado, introduzca el número de puerto HTTP que desea agregar en el campo *Puerto HTTP adicional*. HTTP y otros protocolos de Internet utilizan puertos para asegurarse de que los dispositivos saben dónde encontrar un determinado protocolo. Las opciones son 80, entre 1025 y 65535, o ingrese 0 para inhabilitar. El puerto HTTP y el puerto HTTPS no pueden ser iguales.

Paso 4. (Opcional) Si desea que la información HTTP entre el WAP y el cliente utilice un puerto diferente además del predeterminado, introduzca el número de puerto HTTPS que desea agregar en el campo *Puerto HTTPS adicional*. Las opciones son 443, entre 1025 y 65535, o ingrese 0 para inhabilitar. El puerto HTTP y el puerto HTTPS no pueden ser iguales.

La siguiente información se muestra en el área Contadores de configuración del portal cautivo y no se puede configurar.

Captive Portal Configuration Counters	
Instance Count:	0
Group Count:	1
User Count:	0

Recuento de instancias: el número de instancias de CP configuradas en el dispositivo WAP. Se puede configurar un máximo de dos CP en el WAP.

Recuento de grupos: el número de grupos CP configurados en el dispositivo WAP. Se pueden configurar hasta dos grupos. No se puede eliminar el grupo predeterminado.

Recuento de usuarios: el número de usuarios CP configurados en el dispositivo WAP. Se puede configurar un máximo de 128 usuarios en el WAP.

Paso 5. Click **Save**.

Nota: Los cambios se guardan en la configuración de inicio.

Global Configuration

Captive Portal Mode: Enable

Authentication Timeout: Sec (Range: 60 - 600, Default: 300)

Additional HTTP Port: (Range: 1025 - 65535 or 80, 0 = Disable, Default: 0)

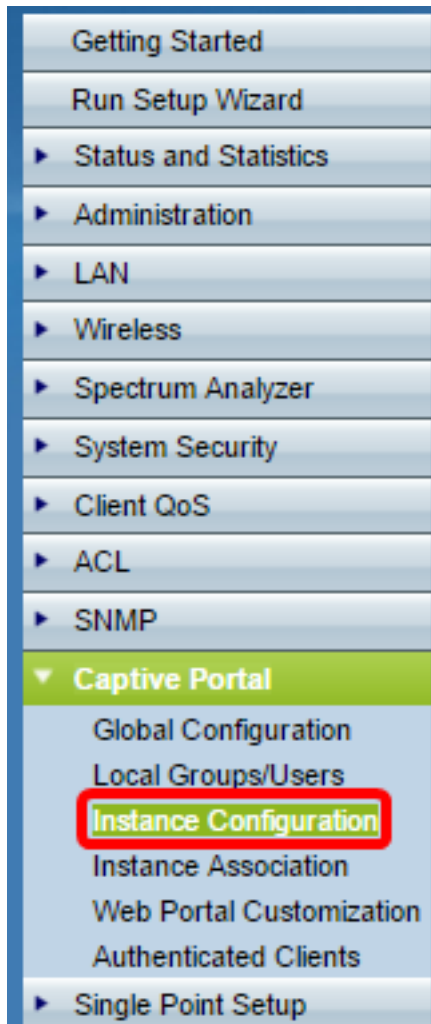
Additional HTTPS Port: (Range: 1025 - 65535 or 443, 0 = Disable, Default: 0)

Captive Portal Configuration Counters

Instance Count:	0
Group Count:	1
User Count:	0

Configuración de instancia

Paso 6. En la utilidad basada en Web, elija **Portal cautivo > Configuración de instancia**.



Paso 7. En la lista desplegable Instancias del portal cautivo, debe observar la instancia wiz-cp-inst1. Puede elegir este nombre o crear un nuevo nombre para la configuración de instancia.

Paso 8. (Opcional) En el campo *Instance Name*, ingrese un nombre para la configuración y haga clic en **Save**.

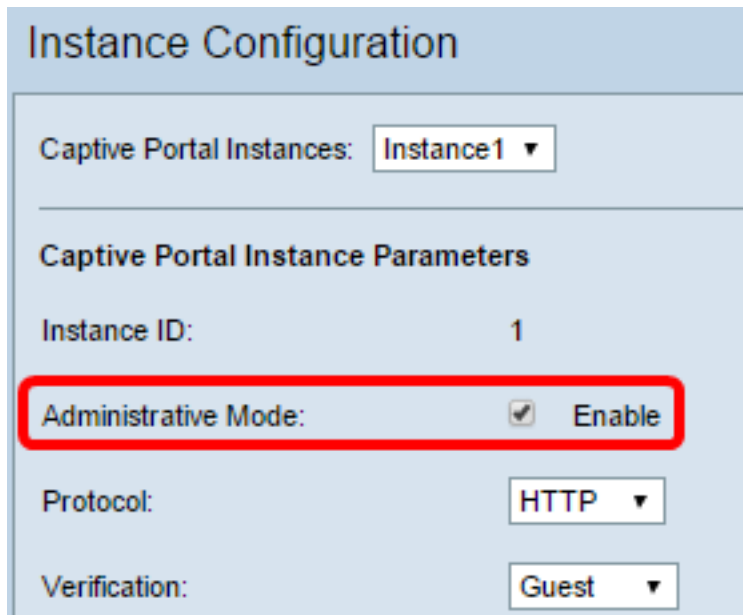
Nota: En este ejemplo, se crea una nueva instancia.

The 'Instance Configuration' form. It has a title bar 'Instance Configuration'. Below it, 'Captive Portal Instances:' with a 'Create' button and a dropdown arrow. A section titled 'Captive Portal Instance Parameters' contains an 'Instance Name:' label followed by a text input field containing 'Instance1' (highlighted with a red box) and a note '(Range: 1 - 32 Characters)'. At the bottom is a 'Save' button.

Nota: Puede crear un máximo de dos configuraciones. Si ya ha creado dos instancias, debe elegir una para editarlas.

Paso 9. La ventana Configuración de instancia muestra información adicional. El ID de instancia es un campo no configurable que muestra el ID de instancia de la instancia actual.

Paso 10. Marque la casilla de verificación **Enable** en Administrative Mode para habilitar la instancia de CP.



Instance Configuration

Captive Portal Instances: Instance 1 ▼

Captive Portal Instance Parameters

Instance ID: 1

Administrative Mode: Enable

Protocol: HTTP ▼

Verification: Guest ▼

Paso 11. En la lista desplegable Protocol , elija el protocolo que desea utilizar para el proceso de autenticación.

HTTP: no cifra la información utilizada en el proceso de autenticación.

HTTPS: proporciona cifrado para la información utilizada en el proceso de autenticación.

Nota: En este ejemplo, se utiliza HTTP.

Paso 12. Elija un método de autenticación para que CP lo utilice en la lista desplegable Verificación.

Invitado: el usuario no necesita proporcionar ninguna autenticación.

Local: WAP verifica la información de autenticación proporcionada por el usuario con una base de datos local almacenada en WAP.

RADIUS: WAP verifica la información de autenticación proporcionada por el usuario en la base de datos de un servidor RADIUS remoto.

Timesaver: Si elige Local o Guest (Invitado), vaya directamente al [Paso 28](#).

Paso 13. (Opcional) Si desea redirigir a los usuarios que se han verificado a una URL configurada, marque la casilla de verificación **Enable** Redirect. Si se desactiva esta opción, los usuarios verificados verán una página de bienvenida específica de la configuración

regional.

Redirect: Enable

Redirect URL: (Range: 0 - 256 Characters)

Away Timeout: (Range: 0 - 1440 Min, Default: 60)

Session Timeout: (Range: 0 - 1440 Min, Default: 0)

Maximum Bandwidth Upstream: (Range: 0 - 1300 Mbps, Default: 0)

Maximum Bandwidth Downstream: (Range: 0 - 1300 Mbps, Default: 0)

Paso 14. (Opcional) Introduzca la dirección URL a la que desea redirigir a los usuarios verificados.

Nota: Este paso sólo se aplica si ha activado Redirigir en el [Paso 13](#).

Paso 15. En el campo *Away Timeout*, ingrese la cantidad de tiempo (en minutos) que un usuario puede ser desasociado del WAP y permanecer en la lista de clientes WAP autenticados. Si el usuario no está conectado al WAP durante más tiempo que el valor *Away Timeout*, deben volver a autorizarse antes de que puedan utilizar el WAP.

Paso 16. En el campo *Session Timeout*, introduzca la cantidad de tiempo (en minutos) que el WAP espera antes de que termine la sesión. Un valor de 0 significa que el tiempo de espera no se aplica.

Paso 17. En el campo *Maximum Bandwidth Upstream*, introduzca la velocidad máxima de carga (en Mbps) que un cliente puede enviar datos a través del portal cautivo.

Paso 18. En el campo *Maximum Bandwidth Downstream*, ingrese la velocidad máxima de descarga (en Mbps) que un cliente puede recibir datos a través del portal cautivo.

Paso 19. En la lista desplegable Nombre de grupo de usuarios, elija el grupo que desea asignar a la instancia de CP. Cualquier usuario que sea miembro del grupo que elija podrá acceder al WAP.

User Group Name:

RADIUS IP Network:

Global RADIUS: Enable

Nota: El modo Verificación en el [Paso 12](#) debe ser Local o RADIUS para asignar un grupo.

Paso 20. En la lista desplegable Red IP RADIUS, elija el tipo de protocolo de Internet que utiliza el cliente RADIUS.

IPv4: la dirección del cliente RADIUS tendrá el formato xxx.xxx.xxx.xxx (192.0.2.10).

IPv6: la dirección del cliente RADIUS tendrá el formato

xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91).

Paso 21. (Opcional) Marque la casilla de verificación **Enable** Global RADIUS si desea utilizar la lista global de servidores RADIUS para la autenticación. Si desea utilizar un conjunto independiente de servidores RADIUS, deje la casilla de verificación desactivada y configure los servidores RADIUS en esta página.

Timesaver: Vaya al [Paso 28](#) si habilita Global RADIUS.

Nota: En este ejemplo, RADIUS global no está habilitado.

Paso 22. (Opcional) Marque la casilla de verificación **Enable** RADIUS Accounting si desea realizar un seguimiento y medir el uso de tiempo y datos de los clientes en la red WAP.

Nota: Si la casilla de verificación Global RADIUS estaba habilitada en el [Paso 21](#), no necesita configurar servidores RADIUS adicionales.

Paso 23. En el campo *Server IP Address-1*, ingrese la dirección IP del servidor RADIUS que desea utilizar como servidor primario. La dirección IP debe ajustarse al formato de dirección correspondiente de IPv4 o IPv6.

Global RADIUS:	<input type="checkbox"/>	Enable
RADIUS Accounting:	<input checked="" type="checkbox"/>	Enable
Server IP Address-1:	<input type="text" value="202.123.123.123"/>	(xxx.xxx.xxx.xxx)
Server IP Address-2:	<input type="text"/>	(xxx.xxx.xxx.xxx)
Server IP Address-3:	<input type="text"/>	(xxx.xxx.xxx.xxx)
Server IP Address-4:	<input type="text"/>	(xxx.xxx.xxx.xxx)

Paso 24. (Opcional) Puede configurar hasta tres servidores RADIUS de respaldo que se comprobarán en secuencia hasta que se encuentre una coincidencia. Si no se encuentra ninguna coincidencia, se denegará el acceso al usuario. En los campos *Server IP Address-2* a *4* (Dirección IP del servidor), introduzca la dirección IP de los servidores RADIUS de respaldo que se utilizarán si la autenticación falla con el servidor primario.

Paso 25. En el campo *Key-1*, ingrese la clave secreta compartida que el dispositivo WAP utiliza para autenticar al servidor RADIUS primario. Ésta debe ser la misma clave que se configuró en el servidor RADIUS.

Key-1:	<input type="password" value="....."/>	(Range
Key-2:	<input type="password" value="....."/>	(Range
Key-3:	<input type="text"/>	(Range
Key-4:	<input type="text"/>	(Range
Locale Count:	0	
Delete Instance:	<input type="checkbox"/>	

Paso 26. En el resto de los campos Key (Clave) (2-4), introduzca la clave secreta compartida que el dispositivo WAP utiliza para autenticarse en los servidores RADIUS de respaldo respectivos.

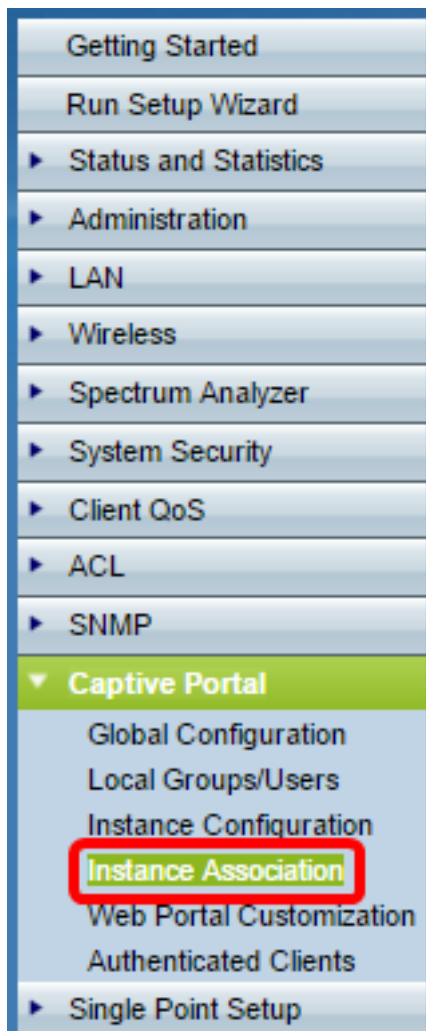
Nota: El recuento de configuración regional es un campo no configurable que muestra el número de configuraciones regionales asociadas a esta instancia.

Paso 27. (Opcional) Para eliminar la instancia actual, marque la casilla de verificación **Eliminar instancia**.

Paso 28. Click **Save**.

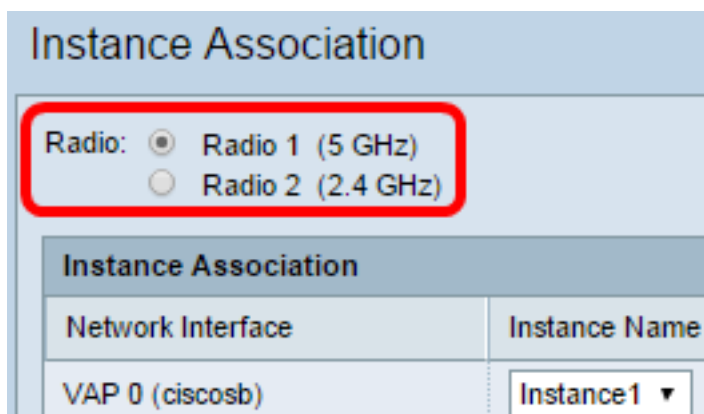
Asociar instancia con VAP

Paso 29. En la utilidad basada en web, elija **Portal cautivo > Asociación de instancias**.



Paso 30. Haga clic en el botón de opción de la radio a la que desea asociar una instancia en el área Radio.

Nota: En este ejemplo, se elige Radio 1 (5 GHz).



Paso 31. Elija una configuración de instancia de la lista desplegable Nombre de instancia para asociarla con el VAP dado.

Nota: En este ejemplo, la Instancia 1 creada en el [Paso 8](#) se utiliza para VAP 1 (Punto de acceso virtual 2).

Instance Association	
Network Interface	Instance Name
VAP 0 (CHICCO)	<input type="text"/>
VAP 1 (Virtual Access Point 2)	Instance 1
VAP 2 (Virtual Access Point 3)	<input type="text"/>
VAP 3 (Virtual Access Point 4)	Instance 1
VAP 4 (Virtual Access Point 5)	<input type="text"/>

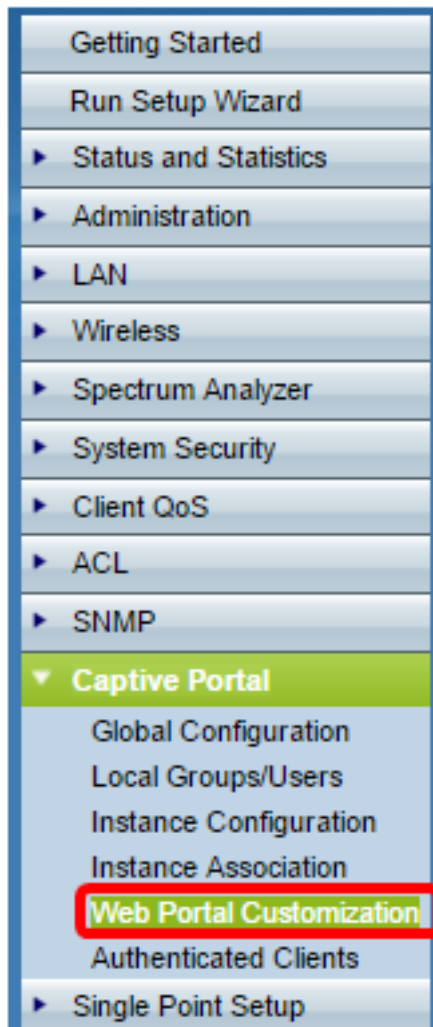
Paso 32. Click **Save**.

VAP 11 (Virtual Access Point 12)	<input type="text"/>
VAP 12 (Virtual Access Point 13)	<input type="text"/>
VAP 13 (Virtual Access Point 14)	<input type="text"/>
VAP 14 (Virtual Access Point 15)	<input type="text"/>
VAP 15 (Virtual Access Point 16)	<input type="text"/>

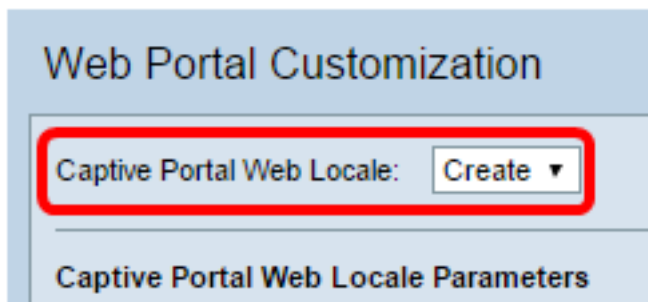
Personalizar portal web

Una configuración regional (página web de autenticación) es la página web que el usuario de WAP ve cuando intenta acceder a Internet. La página Personalización del portal web permite personalizar una configuración regional y asignarla a una instancia del portal cautivo.

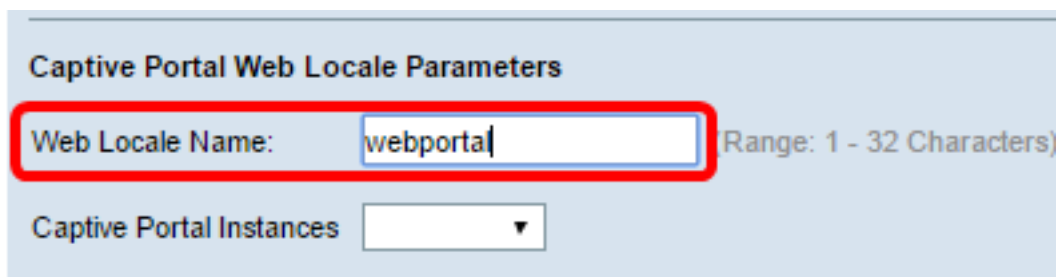
Paso 33. En la utilidad basada en web, elija **Portal cautivo > Personalización del portal web**.



Paso 34. Elija **Crear** en la lista desplegable Captive Portal Web Locale para crear una nueva configuración regional.



Paso 35. Introduzca el nombre de la configuración regional en el campo *Web Locale Name*.



Paso 36. Elija una instancia del portal cautivo con la que se asocia la configuración regional en la lista desplegable Instancias del portal cautivo. Puede asociar varias configuraciones regionales a una única instancia del portal cautivo. El usuario puede hacer clic en un enlace para cambiar a una configuración regional diferente.

Web Portal Customization

Captive Portal Web Locale:

Captive Portal Web Locale Parameters

Web Locale Name: (Range: 1 - 32 Characters)

Captive Portal Instances

Paso 37. Haga clic en **Guardar** para crear una nueva configuración regional.

Nota: La página Personalización del portal web muestra información adicional.

Web Portal Customization

Captive Portal Web Locale:

Captive Portal Web Locale Parameters

Locale ID: 1

Instance Name: Instance1

Background Image Name:

Logo Image Name:

Foreground Color: (Range: 1 - 32 Characters, Default: #999999)

Background Color: (Range: 1 - 32 Characters, Default: #BFBFBF)

Separator: (Range: 1 - 32 Characters, Default: #BFBFBF)

Locale Label: (Range: 1 - 32 Characters, Default: English)

Locale: (Range: 1 - 32 Characters, Default: en)

El ID de configuración regional es un campo no configurable que muestra el número de ID de la configuración regional actual.

El nombre de instancia es un campo no configurable que muestra el nombre de instancia del portal cautivo asociado a la configuración regional.

Paso 38. En la lista desplegable Background Image Name (Nombre de imagen de fondo), elija una imagen para mostrarla en el fondo de la configuración regional. Haga clic en el botón **Cargar/Eliminar imagen personalizada** para agregar su propia imagen. Vaya a la sección Cargar/Eliminar imagen personalizada para obtener más información.

Paso 39. En la lista desplegable Nombre de imagen del logotipo, elija una imagen para mostrarla en la esquina superior izquierda de la página.

Paso 40. En el campo *Color de primer plano*, introduzca el código de protocolo de transferencia de hipertexto (HTML) de 6 dígitos para el color de primer plano de la configuración regional.

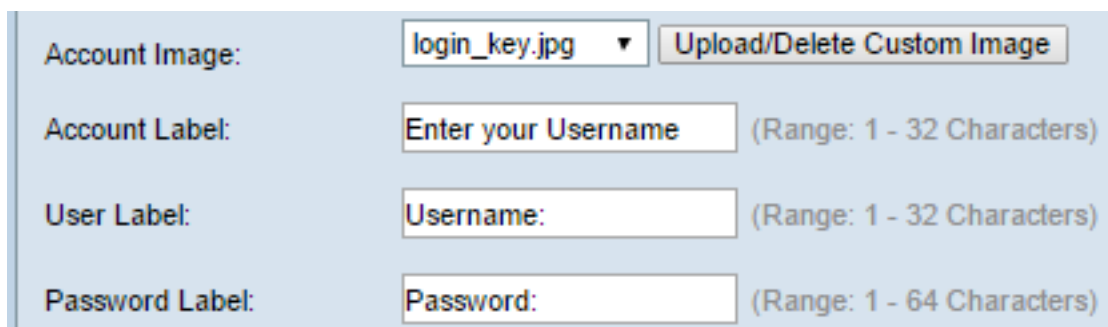
Paso 41. En el campo *Color de fondo*, introduzca el código HTML de 6 dígitos para el color de fondo de la configuración regional.

Paso 42. En el campo *Separador*, introduzca el código HTML de 6 dígitos para el color de la línea horizontal que separa el encabezado de la página del cuerpo de la página.

Paso 43. Introduzca un nombre descriptivo para la configuración regional en el campo *Etiqueta de configuración regional*. Si tiene varias configuraciones regionales, éste es el nombre del enlace en el que hace clic para cambiar entre configuraciones regionales. Por ejemplo, si tiene una configuración regional en inglés y español, puede que desee indicarlo en su nombre de configuración regional.

Paso 44. Introduzca una abreviatura para la configuración regional en el campo *Configuración regional*.

Paso 45. En la lista desplegable Imagen de cuenta, elija una imagen para mostrarla encima del campo de inicio de sesión.



The image shows a configuration form with the following fields and options:

- Account Image:** A dropdown menu showing 'login_key.jpg' and a button labeled 'Upload/Delete Custom Image'.
- Account Label:** A text input field containing 'Enter your Username' with a note '(Range: 1 - 32 Characters)'.
- User Label:** A text input field containing 'Username:' with a note '(Range: 1 - 32 Characters)'.
- Password Label:** A text input field containing 'Password:' with a note '(Range: 1 - 64 Characters)'.

Paso 46. En el campo *Account Label*, ingrese las instrucciones que le piden al usuario que introduzca su nombre de usuario.

Paso 47. En el campo *User Label*, ingrese la etiqueta para el cuadro de texto user name.

Paso 48. En el campo *Password Label*, ingrese la etiqueta para el cuadro de texto password.

Paso 49. En el campo *Button Label*, ingrese la etiqueta del botón en el que los usuarios hacen clic para enviar su nombre de usuario y contraseña.

Button Label:	<input type="text" value="Connect"/>	(Range: 2 - 32 Characters, Default: Connect)
Fonts:	<input type="text" value="'MS UI Gothic', arial, sans-serif"/>	(Range: 1 - 512 C)
Browser Title:	<input type="text" value="Captive Portal"/>	(Range: 1 - 128 C)
Browser Content:	<input type="text" value="Welcome to the Wireless Network"/>	(Range: 1 - 128 C)
Content:	<input type="text" value="To start using this service, enter your credentials and click the connect button."/>	(Range: 1 - 256 C)
Acceptance Use Policy:	<input type="text" value="Acceptance Use Policy."/>	(Range: 1 - 4096)

Paso 50. En el campo *Fuentes*, introduzca el nombre de fuente utilizado para la configuración regional. Puede introducir varios nombres de fuente separados por una coma. Si el dispositivo cliente no encuentra el primer estilo de fuente, se utiliza la fuente siguiente. Si un nombre de fuente tiene varias palabras separadas por espacios, utilice comillas simples para rodear el nombre de fuente. Por ejemplo, 'MS UI Gothic' , arial, sans-serif, etc.

Paso 51. En el campo *Título del explorador*, introduzca el texto que desea mostrar en la barra de título del explorador.

Paso 52. En el campo *Contenido del explorador*, introduzca el texto que desea mostrar en el encabezado de la página.

Paso 53. En el campo *Contenido*, introduzca el texto que indica al usuario qué hacer. Este campo se muestra debajo de los cuadros de texto nombre de usuario y contraseña.

Paso 54. En el campo *Política de uso de aceptación*, introduzca los términos con los que los usuarios deben aceptar si desean acceder al WAP.

Paso 55. En el campo *Aceptar etiqueta*, introduzca el texto que indica a los usuarios que verifiquen que han leído y aceptado la política de uso de aceptación.

Accept Label:	<input type="text" value="Check here to indicate that you have read and accepted the Acceptance Use Policy."/>	(Range: 1 - 128)
No Accept Text:	<input type="text" value="Error: You must acknowledge the Acceptance Use Policy before connecting!"/>	(Range: 1 - 128)
Work In Progress Text:	<input type="text" value="Connecting, please be patient..."/>	(Range: 1 - 128)
Denied Text:	<input type="text" value="Error: Invalid Credentials, please try again!"/>	(Range: 1 - 128)
Welcome Title:	<input type="text" value="Congratulations!"/>	(Range: 1 - 128)

Paso 56. En el campo *No aceptar texto*, introduzca el texto que solicita al usuario si envía credenciales de inicio de sesión pero no acepta la política de uso de aceptación.

Paso 57. En el campo *Texto de trabajo en curso*, ingrese el texto que se muestra mientras el WAP verifica las credenciales dadas.

Paso 58. En el campo *Texto denegado*, ingrese el texto que se muestra cuando un usuario falla la autenticación.

Paso 59. En el campo *Título de bienvenida*, introduzca el texto del título que se muestra cuando un cliente se autentica correctamente.

Paso 60. En el *campo Contenido de bienvenida*, ingrese el texto que se muestra a un cliente que se ha conectado a la red.

Welcome Title: Congratulations! (Range: 1 - 12)

Welcome Content: You are now authorized and connected to the network. (Range: 1 - 25)

Delete Locale:


Save Preview...

Paso 61. (Opcional) Para eliminar la configuración regional actual, marque la casilla de verificación **Eliminar configuración regional**.


Paso 62. Click **Save**.

Paso 63. (Opcional) Para ver su configuración regional actual, haga clic en **Vista previa**. Si realiza cambios, haga clic en **Guardar** antes de obtener una vista previa para actualizar los cambios.

Nota: La pantalla de inicio de sesión del portal cautivo es similar a la siguiente imagen:



Welcome to the Wireless Network



Enter your Username

Username:

To start using this service, enter your credentials and click the connect button.

Acceptance Use Policy.

Check here to indicate th
the Acceptance Use Policy.

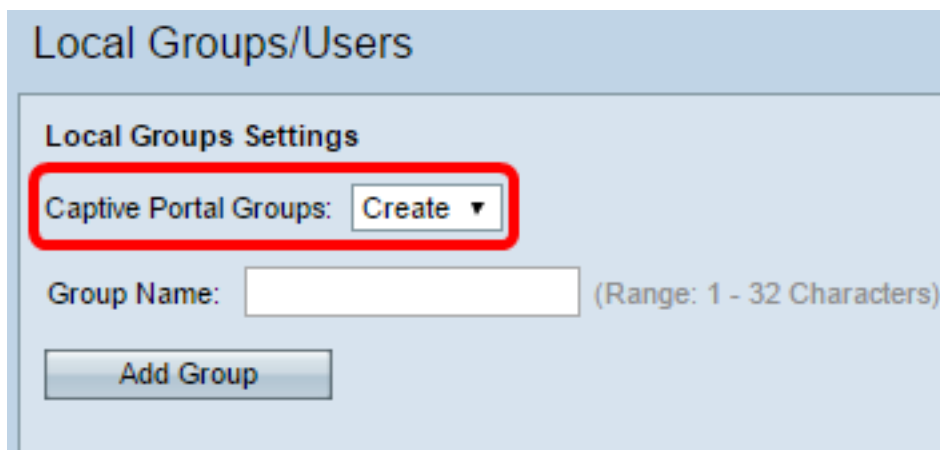
Crear grupo local

Un portal cautivo que no sea invitado requiere que los usuarios inicien sesión en función de su nombre de usuario y contraseña. El WAP crea un grupo local que contiene un grupo de usuarios locales. A continuación, el grupo local se asocia a una instancia. Los usuarios locales que son miembros del grupo local pueden obtener acceso a través del portal cautivo. El grupo local predeterminado siempre está activo y no se puede eliminar. Se pueden agregar hasta dos grupos locales adicionales al WAP.

Paso 64. En la utilidad basada en web, elija **Portal cautivo > Grupos/Usuarios locales**.



Paso 65. Elija **Crear** en la lista desplegable Grupos de portal cautivos.



Paso 66. Introduzca el nombre del grupo local en el campo *Group Name*.

The screenshot shows the 'Local Groups/Users' configuration page. Under 'Local Groups Settings', there is a 'Captive Portal Groups' dropdown menu set to 'Create'. Below it, the 'Group Name' field contains the text 'Group1' and is highlighted with a red rectangular box. To the right of the field, it says '(Range: 1 - 32 Characters)'. At the bottom of the section is a blue 'Add Group' button.

Paso 67. Haga clic en **Agregar grupo** para guardar el grupo.

This screenshot shows the same 'Local Groups/Users' configuration page. The 'Captive Portal Groups' dropdown menu is now open, showing three options: 'Create', 'Default', and 'Group1'. The 'Group1' option is highlighted in blue. The 'Group Name' field is currently empty. The 'Add Group' button is now greyed out.

Nota: Puede asignar un grupo local a una instancia en el [Paso 19](#) de la sección titulada Configuración de instancia.

Crear usuario local

Los usuarios locales se agregan a un grupo local. Estos usuarios pueden acceder a un portal cautivo que tiene una instancia con su grupo local configurado. Parte de la información configurada en la página Usuarios locales también se configura en la página Configuración de instancias. El valor configurado para un usuario local tiene prioridad sobre el valor configurado para una instancia. Puede configurar hasta 128 usuarios autorizados en la base de datos local.

Paso 68. Elija **Crear** en la lista desplegable Usuarios del portal cautivo.

The screenshot shows the 'Local Users Settings' configuration page. The 'Captive Portal Users' dropdown menu is set to 'Create' and is highlighted with a red rectangular box. Below it is an empty 'User Name' field with the text '(Range: 1 - 32 Characters)' to its right. At the bottom is a greyed-out 'Add User' button.

Paso 69. En el campo *User Name*, ingrese el nombre de usuario que desea agregar.

Local Users Settings

Captive Portal Users: Create ▾

User Name: User1 (Range: 1 - 32 Characters)

Add User

Paso 70. Haga clic en **Agregar usuario** para crear el nuevo usuario. La ventana Configuración de usuarios locales muestra información adicional.

Local Users Settings

Captive Portal Users: User1 ▾

User Password: (Range: 8 - 64 Alphanumeric & Special)

Show Password as Clear Text

Away Timeout: 60 (Range: 0 - 1440 Min, Default: 60)

Group Name: Default ▾
Group1

Maximum Bandwidth Upstream: 0 (Range: 0 - 1300 Mbps, Default: 0)

Maximum Bandwidth Downstream: 0 (Range: 0 - 1300 Mbps, Default: 0)

Delete User:

Save

Paso 71. En el campo *User Password*, ingrese la contraseña asociada al usuario.

Paso 72. (Opcional) Para que la contraseña se muestre en texto sin cifrar, marque la casilla de verificación **Mostrar contraseña como texto sin formato**. Si la casilla de verificación no está marcada, la contraseña se enmascara.

Paso 73. En el campo *Away Timeout*, ingrese la cantidad de tiempo (en minutos) que un usuario puede desasociarse del WAP y permanecer en la lista de clientes WAP autenticados. Si el usuario no está conectado al WAP durante más tiempo que el tiempo de espera de ausencia, deben volver a autorizarse antes de poder utilizar el WAP.

Paso 74. En el campo *Group Name*, haga clic en el grupo local al que desea que se una el usuario.

Paso 75. En el campo *Maximum Bandwidth Upstream*, ingrese la velocidad máxima de carga en Mbps que un cliente puede enviar datos a través del portal cautivo.

Paso 76. En el campo *Maximum Bandwidth Downstream*, ingrese la velocidad máxima de descarga en Mbps que un cliente puede recibir datos a través del portal cautivo.

Paso 77. (Opcional) Para eliminar un usuario local, marque la casilla de verificación **Eliminar usuario**.

Paso 78. Click **Save**.

Ahora debería haber configurado los parámetros avanzados del portal cautivo de su WAP571 o WAP571E.