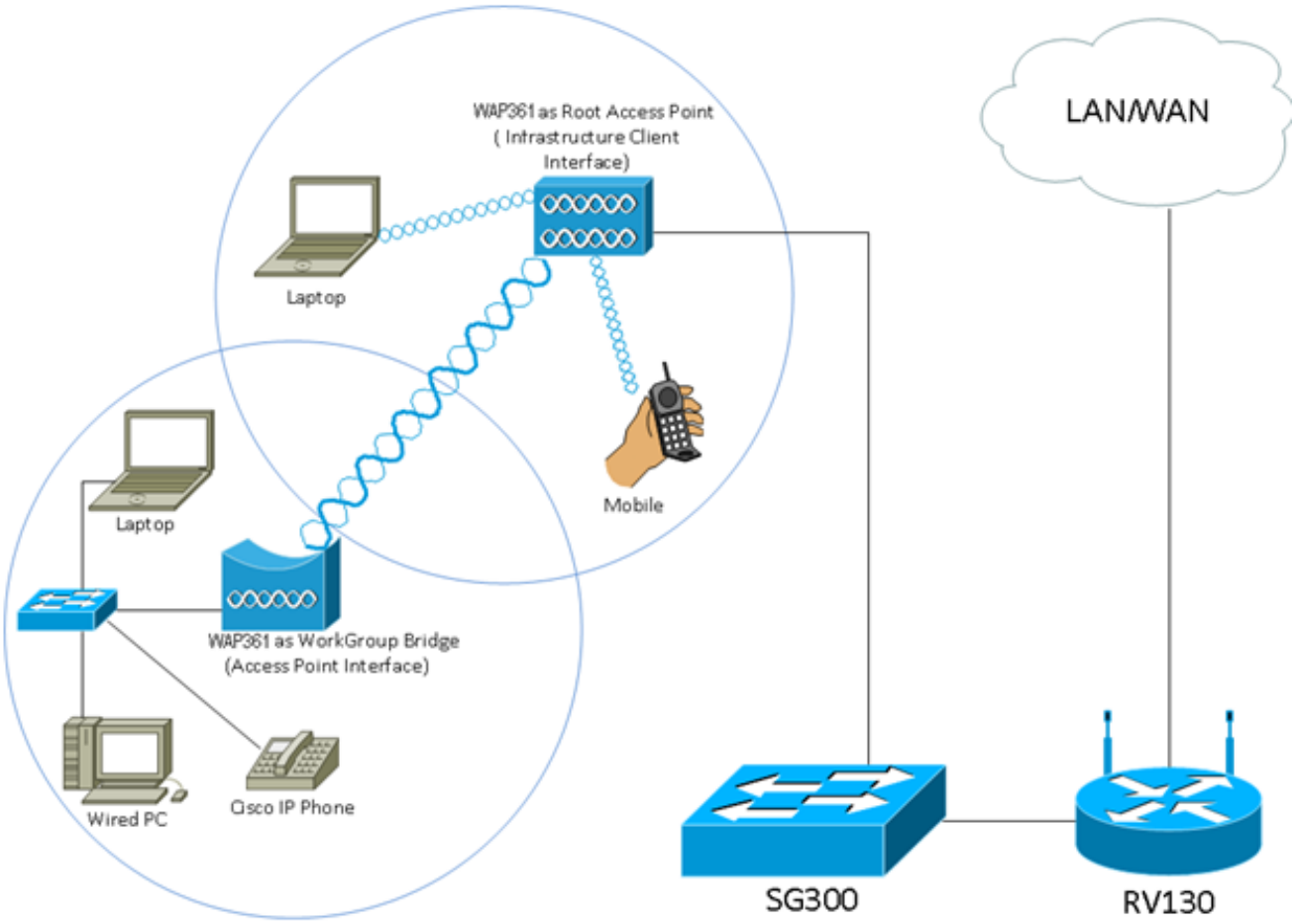
Workgroup Bridge de la configuración en un unto de acceso de red inalámbrica (WAP)

Objetivo

La característica del Workgroup Bridge permite al unto de acceso de red inalámbrica (WAP) para interligar el tráfico entre un cliente remoto y el Wireless Local Area Network (LAN) que esté conectado con el modo del Workgroup Bridge. El dispositivo WAP asociado a la interfaz remota se conoce como interfaz del Punto de acceso, mientras que el dispositivo WAP asociado al Wireless LAN se conoce como interfaz de la infraestructura. El Workgroup Bridge deja los dispositivos que hacen solamente que las conexiones alámbricas conecten con una red inalámbrica. El modo del Workgroup Bridge se recomienda como alternativa cuando la característica de Wireless Distribution System (WDS) es inasequible.



Nota: La topología antedicha ilustra un modelo del Workgroup Bridge de la muestra. Los dispositivos atados con alambre se atan a un Switch, que conecta con la interfaz LAN del WAP. El WAP actúa como interfaz del Punto de acceso, conecta con la interfaz de la infraestructura.

Este artículo apunta mostrarle cómo configurar el Workgroup Bridge entre dos WAP.

Dispositivos aplicables

- WAP100 Series
- WAP300 Series
- WAP500 Series

Versión del software

- 1.0.0.17 — WAP571, WAP571E
- 1.0.1.7 — WAP150, WAP361
- 1.0.2.5 — WAP131, WAP351
- 1.0.6.5 — WAP121, WAP321
- 1.2.1.3 — WAP551, WAP561
- 1.3.0.3 — WAP371

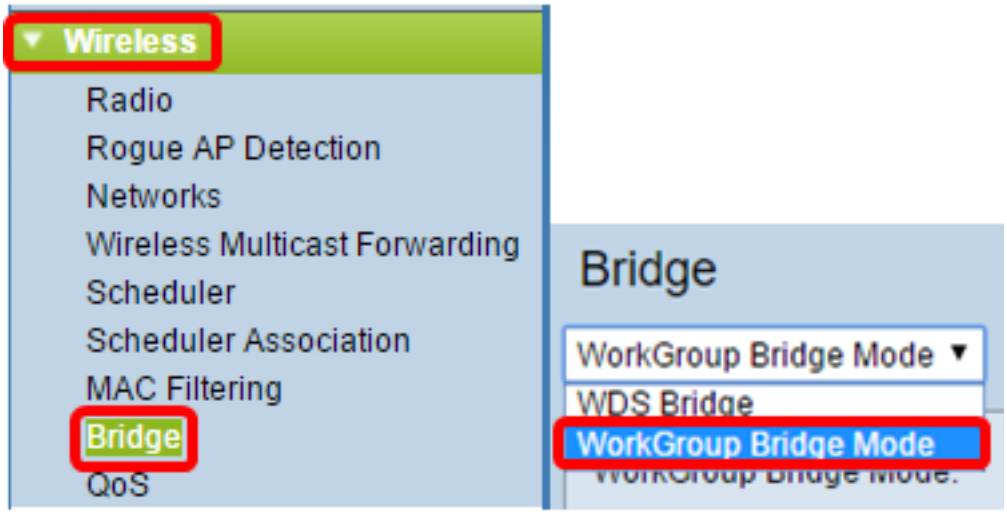
Workgroup Bridge de la configuración

Interfaz del cliente de la infraestructura

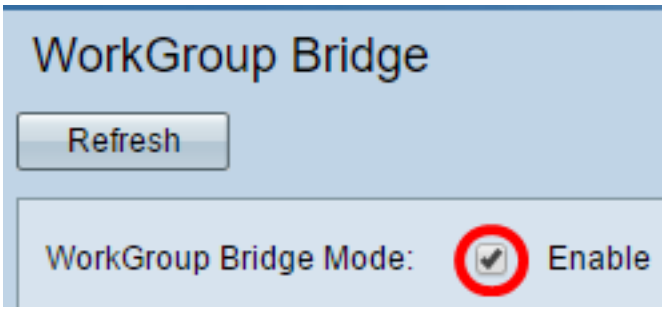
Paso 1. El login a la utilidad basada en web del WAPand elige la **Tecnología inalámbrica > el Workgroup Bridge**.

Nota: Las opciones de menú pueden variar dependiendo del modelo del dispositivo que usted está utilizando. Las imágenes abajo se toman del WAP361 a menos que se indique lo contrario.

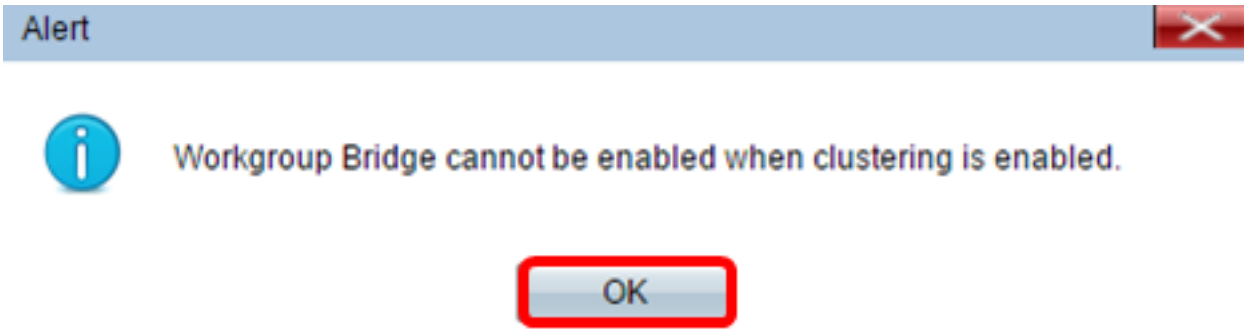
Para WAP571 y WAP571E, elija el **modo de la Tecnología inalámbrica > del Bridge > del Workgroup Bridge**.



Paso 2. Marque la casilla de verificación del modo del Workgroup Bridge del **permiso**.

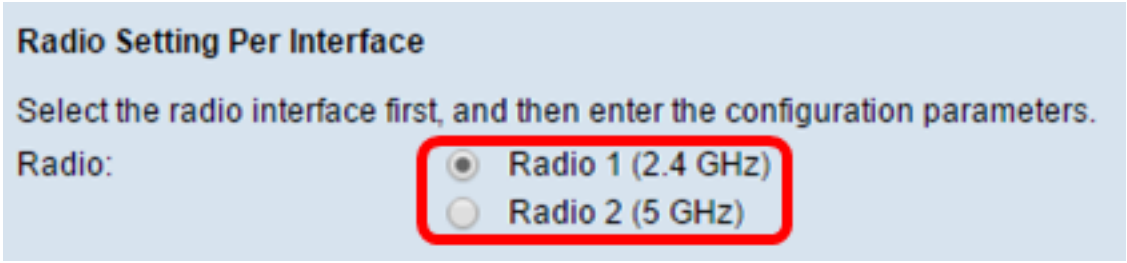


Nota: Si el agrupar se habilita en el WAP, un móvil le notificará para inhabilitar el clúster para que el Workgroup Bridge trabaje. Para continuar, haga clic en OK (Aceptar). Para inhabilitar el clúster, elegir la **configuración monopunto del** SCR_INVALID entonces elige los **Puntos de acceso > la configuración monopunto de la neutralización**.



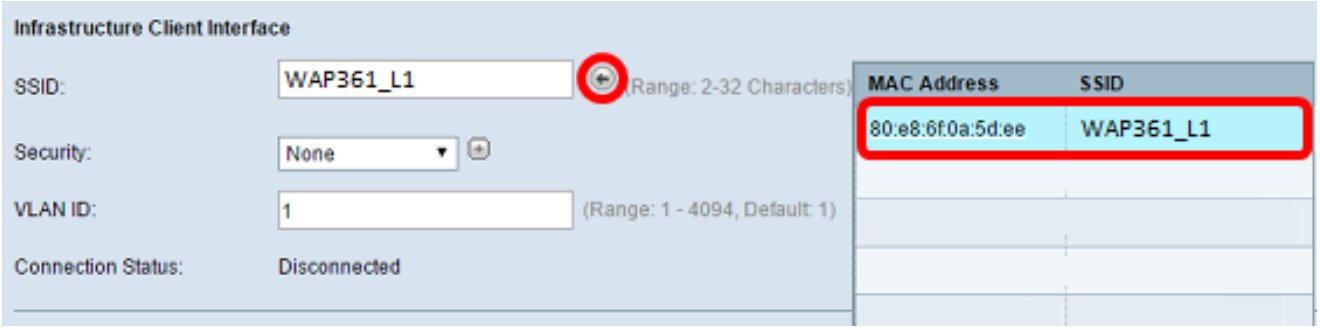
Paso 3. Haga clic la interfaz radio para el Workgroup Bridge. Cuando usted configura una radio como Workgroup Bridge, la otra radio sigue siendo operativa. Las interfaces radio corresponden a las bandas de frecuencia del WAP. El WAP se equipa para transmitir en dos diversas interfaces radio. Configurar las configuraciones para una interfaz radio no afectará a la otra. Las opciones de interfaz radio pueden variar dependiendo del modelo WAP. Algunos WAP muestran la radio 1 como 2.4 gigahertz mientras que algunos tienen Radio 2 como 2.4 gigahertz.

Nota: Este paso está solamente para los WAP siguientes con la dual-banda: WAP131, WAP150, WAP351, WAP361, WAP371, WAP561, WAP571, WAP571E. Por este ejemplo, se elige la radio 1.



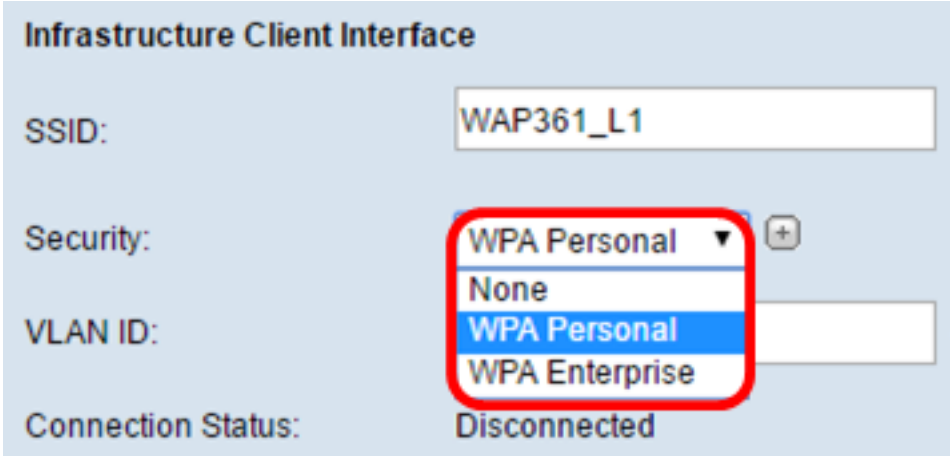
Paso 4. Ingrese el nombre del Service Set Identifier (SSID) en el campo *SSID* o haga clic el botón Arrow Button al lado del campo para explorar para los vecinos. Esto sirve como la conexión entre el dispositivo y el cliente remoto. Usted puede ingresar 2 a 32 caracteres para el cliente SSID de la infraestructura.

Nota: Es importante habilitar la detección rogue AP. Para aprender más sobre cómo habilitar la característica dicha, haga clic aquí. Por este ejemplo, el botón Arrow Button se hace clic para elegir WAP361_L1 como el SSID de la interfaz del cliente de la infraestructura.



Paso 5. En el área de la interfaz del cliente de la infraestructura, elija el tipo de Seguridad para autenticar como estación del cliente en el dispositivo de la conexión en sentido ascendente WAP de la lista desplegable de la Seguridad. Las opciones son:

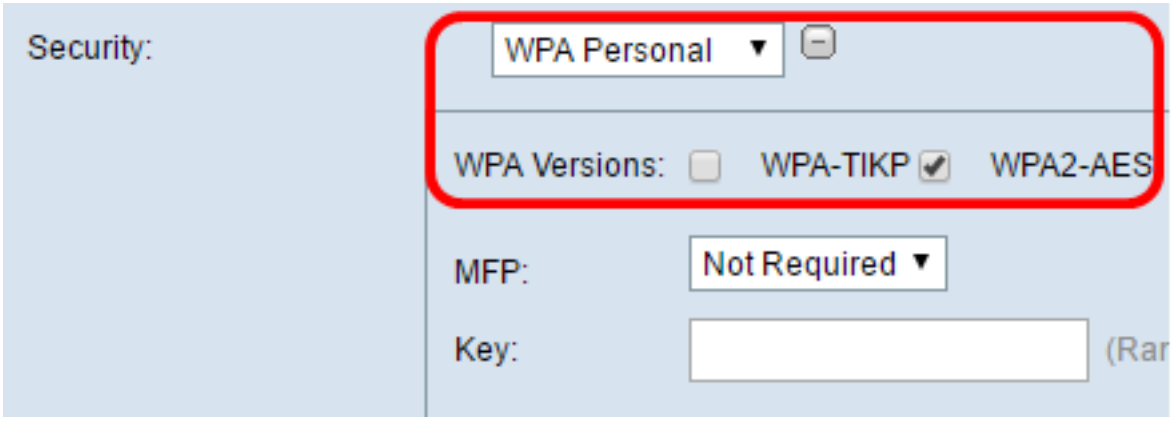
- Ninguno — Ábrase o ninguna Seguridad. Este es el valor predeterminado. Si se elige esto, salte al paso 18.
- WPA personal — El WPA personal puede soportar las claves de los caracteres de la longitud 8-63. Se recomienda el WPA2 pues tiene una norma de encripción más potente. Salto al paso 6 a configurar.
- Empresa WPA — La empresa WPA es avanzado que el WPA personal y es la Seguridad recomendada para la autenticación. Utiliza el protocolo extensible authentication protegido (PEAP) y Transport Layer Security (TLS). Salto al paso 9 a configurar. Este tipo de Seguridad es de uso frecuente en un entorno de oficina y necesita un servidor del Remote Authentication Dial-In User Service (RADIUS) configurado. Haga clic aquí para saber más sobre los servidores de RADIUS.



Nota: En este ejemplo, el WPA personal se elige.

Paso 6. Haga clic **+** y marque la casilla de verificación WPA-TKIP o WPA2-AES para determinar que la clase de cifrado WPA la interfaz del cliente de la infraestructura utilizará.

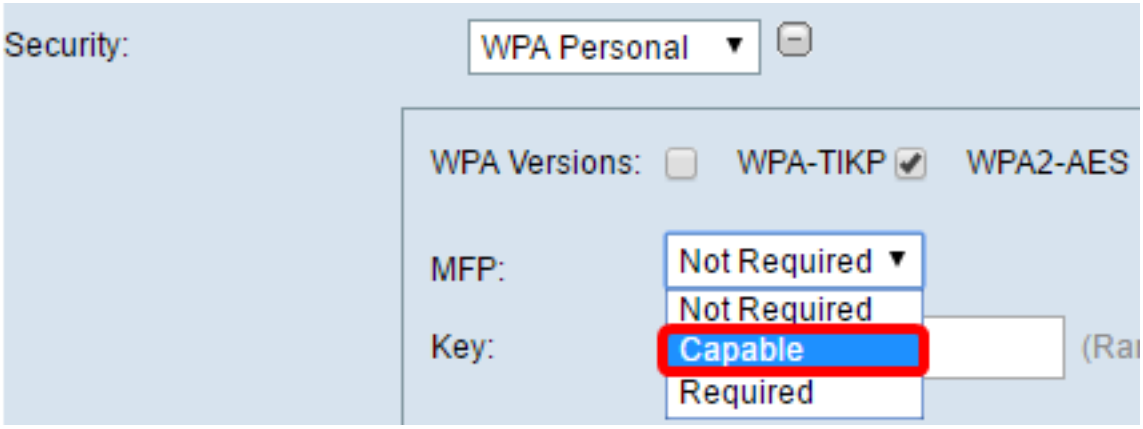
Nota: Si todo su soporte de equipo de red inalámbrica WPA2, fijó la Seguridad del cliente de la infraestructura a WPA2-AES. El método de encripción es RC4 para el WPA y el Advanced Encryption Standard (AES) para el WPA2. Se recomienda el WPA2 pues tiene una norma de encripción más potente. Por este ejemplo, se utiliza WPA2-AES.



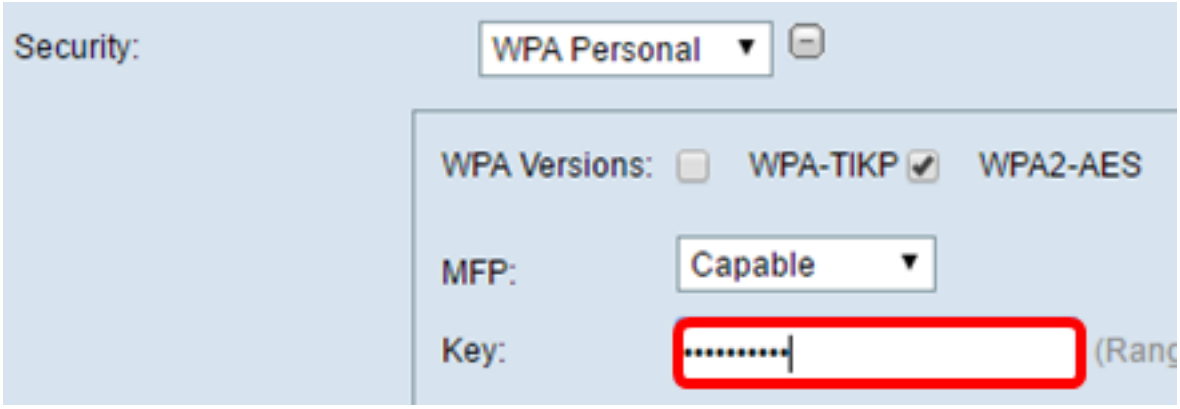
El paso 7. (opcional) si usted marcó WPA2-AES en el paso 6, elige una opción de la lista desplegable de la protección del capítulo de la Administración (MFP) si usted quisiera que el WAP requiriera para tener tramas protegidas o no. Para aprender más sobre MFP, haga clic aquí. Las opciones son:

- No requerido — Inhabilita el soporte de cliente para MFP.
- Capaz — Permite MFP-capaces y a los clientes que no soporten MFP para unirse a la red. Ésta es la configuración del valor por defecto MFP en el WAP.
- Requerido — Se permite a los clientes asociarse solamente si se negocia MFP. Si los dispositivos no soportan MFP, no se permiten unirse a la red.

Nota: Por este ejemplo, capaz se elige.



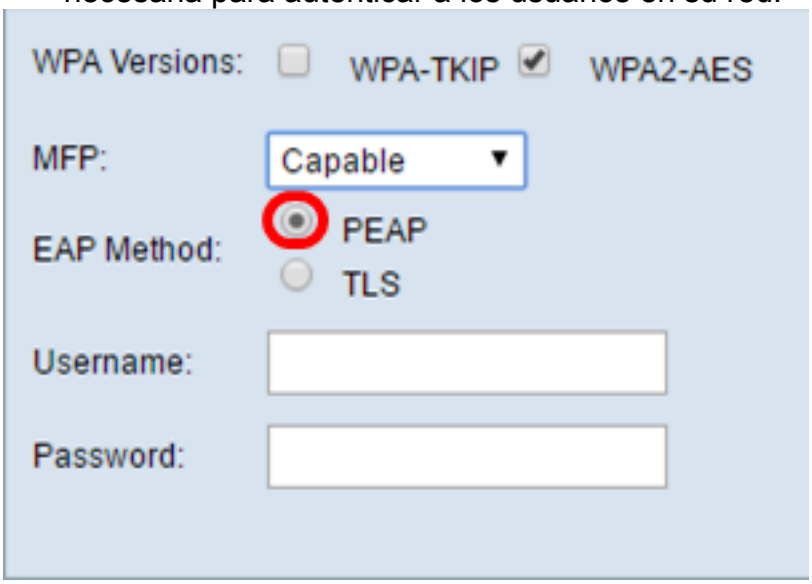
Paso 8. Ingrese la clave de encripción WPA en el *campo clave*. La clave debe ser 8-63 caracteres de largo. Ésta es una combinación de cartas, de números, y de caracteres especiales. Es la contraseña se utiliza que al conectar con la red inalámbrica por primera vez. Entonces, salto al paso 18.



Paso 9. Si usted eligió la empresa WPA en el paso 5, haga clic un botón de radio para el método EAP.

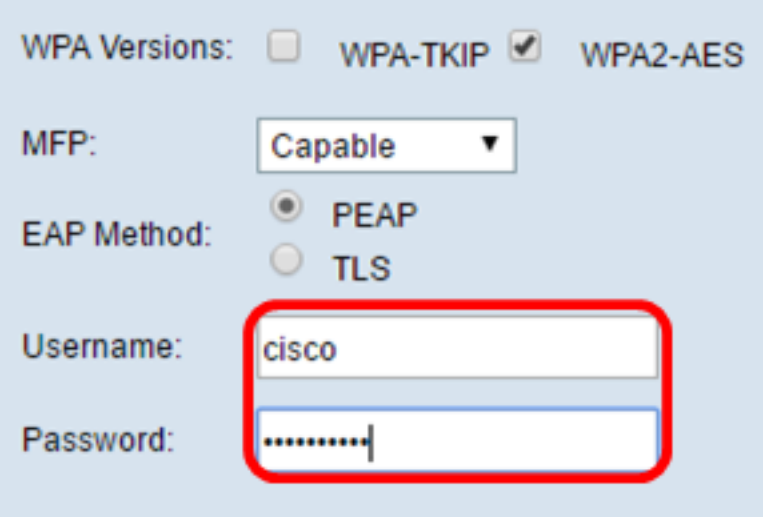
Se definen las opciones disponibles como sigue:

- PEAP — Este protocolo da a cada usuario de red inalámbrica bajo nombres de usuario y contraseña individuales WAP que soportan los estándares de la encripción AES. Puesto que el PEAP es un método de seguridad basado contraseña, su Seguridad del Wi-Fi se basa en los credenciales del dispositivo del cliente. El PEAP puede plantear potencialmente un riesgo de seguridad importante si usted tiene las contraseñas débiles o los clientes sin garantía. Confía en TLS pero evita la instalación de los Certificados digitales en cada cliente. En lugar, proporciona la autenticación con un nombre de usuario y contraseña.
- TLS — TLS requiere a cada usuario tener un certificado adicional para ser concedido el acceso. TLS es más seguro si usted tiene los servidores adicionales y la infraestructura necesaria para autenticar a los usuarios en su red.

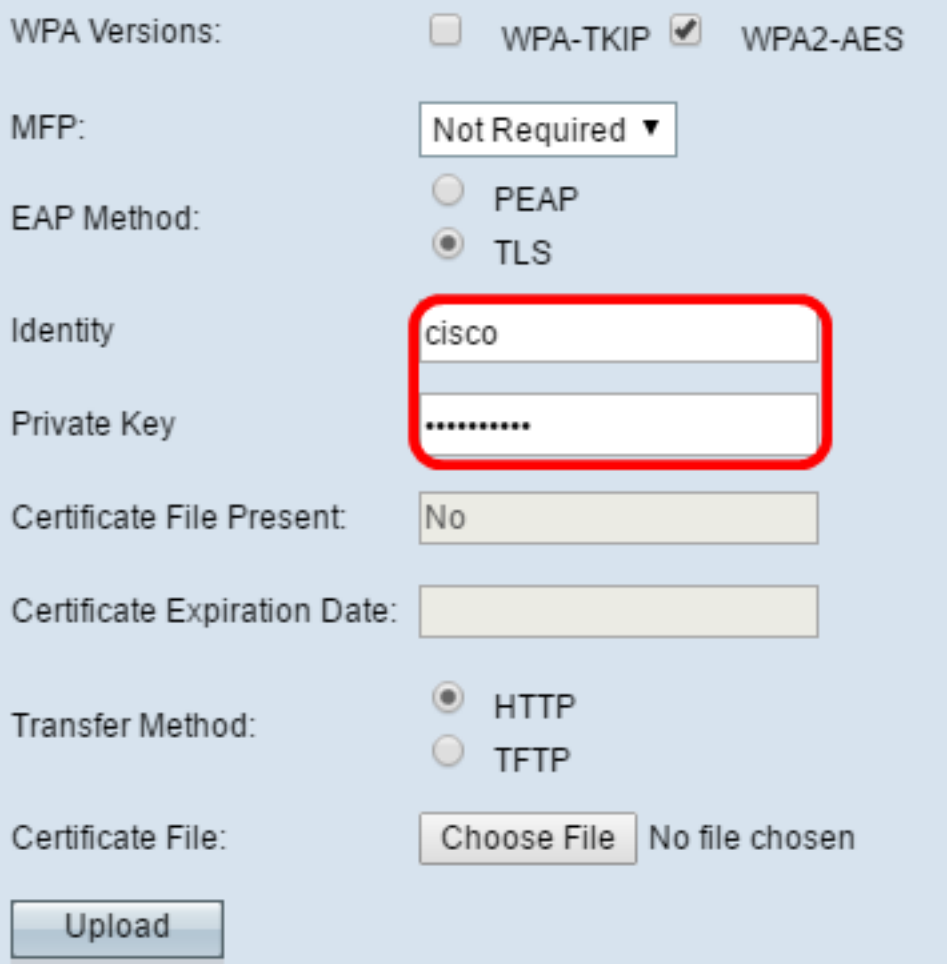


Nota: Por este ejemplo, se elige el PEAP.

Paso 10. Ingrese el nombre de usuario y contraseña para el cliente de la infraestructura en los campos *del nombre de usuario y contraseña*. Ésta es la información del login que se utiliza para conectar con la interfaz del cliente de la infraestructura; refiera a su interfaz del cliente de la infraestructura para encontrar esta información. Entonces, salto al paso 18.

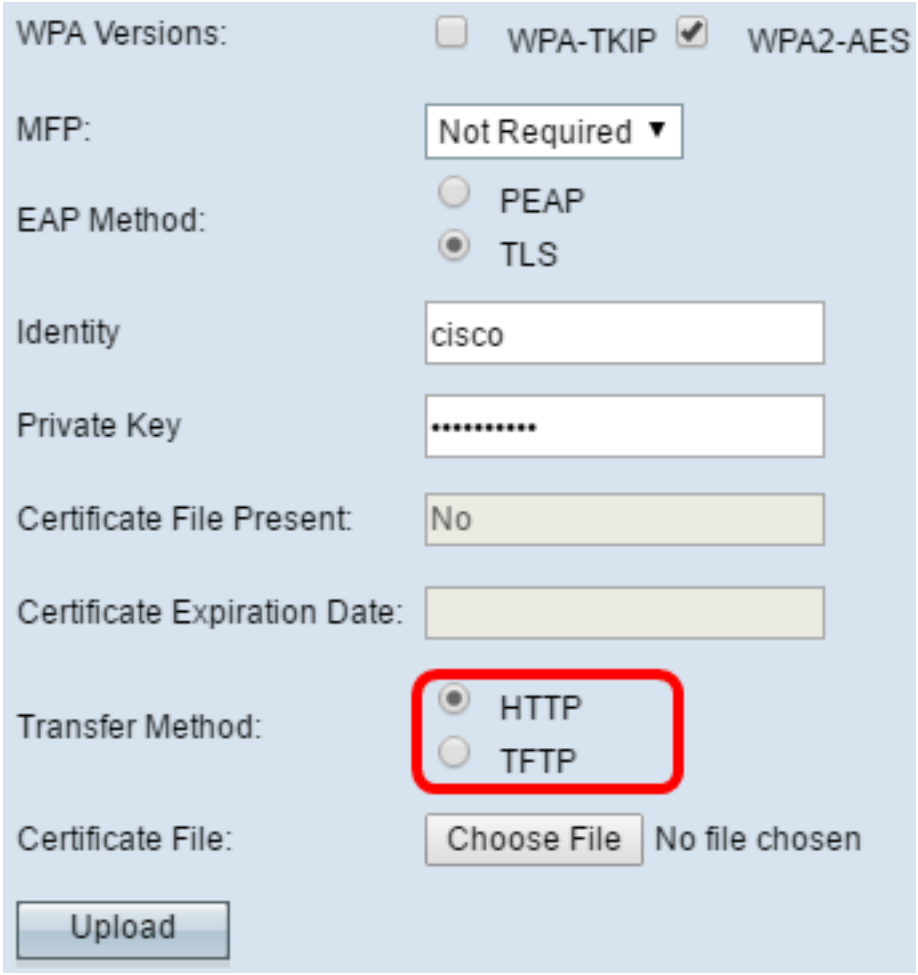


Paso 11. Si usted hizo clic el TLS en el paso 9, ingrese la identidad y la clave privada del cliente de la infraestructura en los campos de la *identidad* y de *clave privada*.



Paso 12. En el área del método de la transferencia, haga clic un botón de radio de las opciones siguientes:

- TFTP — El Trivial File Transfer Protocol (TFTP) es una versión sin garantía simplificada del File Transfer Protocol (FTP). Se utiliza principalmente para distribuir el software o para autenticar los dispositivos entre las redes corporativas. Si usted hizo clic el TFTP, salte al paso 15.
- HTTP — El Hypertext Transfer Protocol (HTTP) proporciona un marco de autenticación simple de la respuesta de seguridad que se pueda utilizar por un cliente para proporcionar el marco de autenticación.

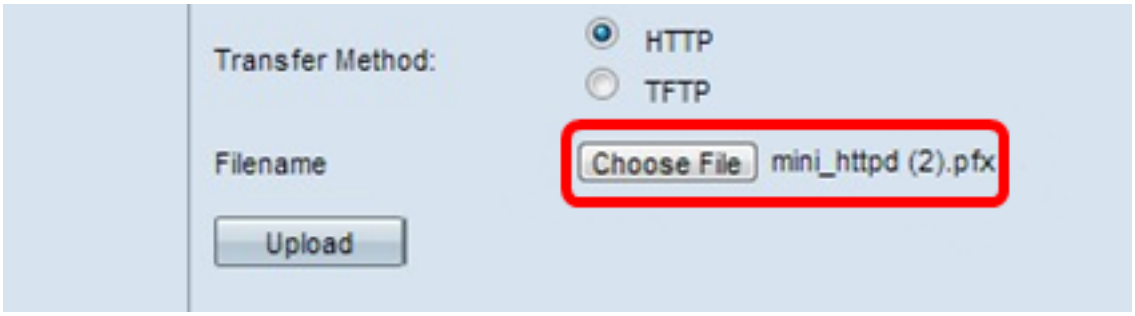


Nota: Si un archivo de certificado está ya presente en el WAP, los campos de la *fecha del presente del archivo de certificado* y del *vencimiento del certificado* serán completados ya de la información pertinente. Si no, serán en blanco.

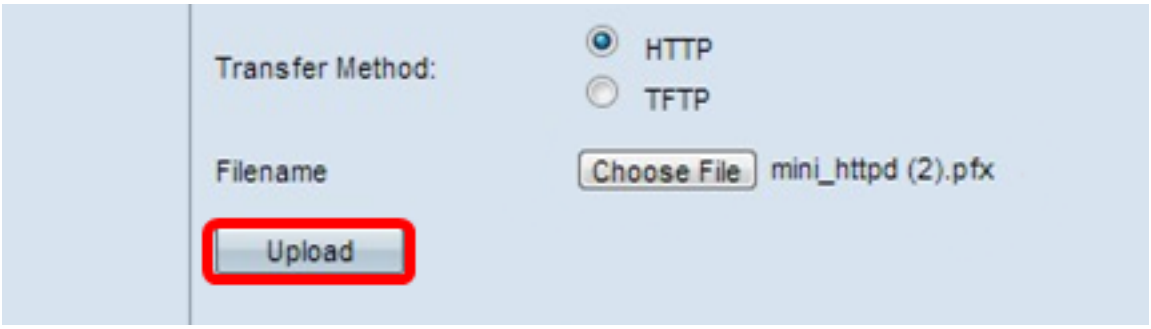
HTTP

Paso 13. Haga clic el **botón File Button del elegir** para encontrar y para seleccionar un archivo de certificado. El archivo debe tener la extensión de archivo de certificado apropiada (tal como .pem o .pfx) de otra manera, el archivo no será validado.

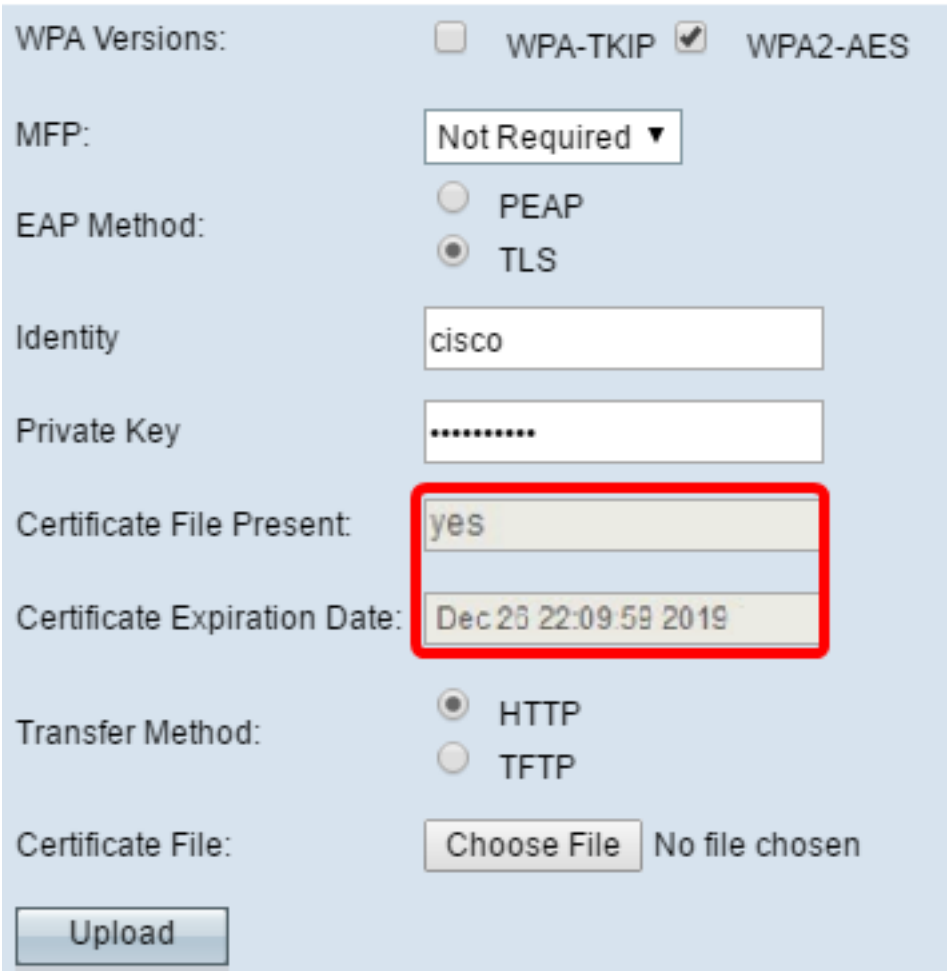
Nota: En este ejemplo, se elige mini_httpd(2).pfx.



Paso 14. **Carga del** tecleo para cargar el archivo de certificado seleccionado. Salto al paso 18.



Los campos de la *fecha del presente* y del *vencimiento del certificado del archivo de certificado* serán puestos al día automáticamente.



TFTP

Paso 15. Si usted hizo clic el TFTP en el paso 12, ingrese el nombre de fichero del archivo de certificado en el campo del *nombre de fichero*.

Nota: En este ejemplo, se utiliza mini_httpd.pem.

Paso 16. Ingrese el TFTP Server Address en el *campo de dirección del IPv4 del servidor TFTP*.

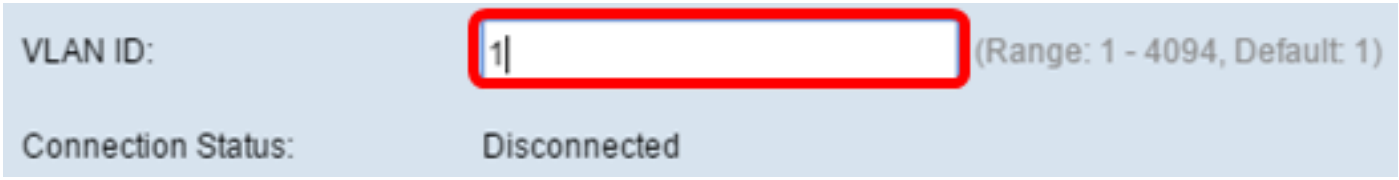
Nota: En este ejemplo. 192.168.1.20 se utiliza como el TFTP Server Address.

Paso 17. Haga clic el botón de la **carga** para cargar el archivo de certificado especificado.

Los campos de la *fecha del presente* y del *vencimiento del certificado del archivo de certificado* serán puestos al día automáticamente.

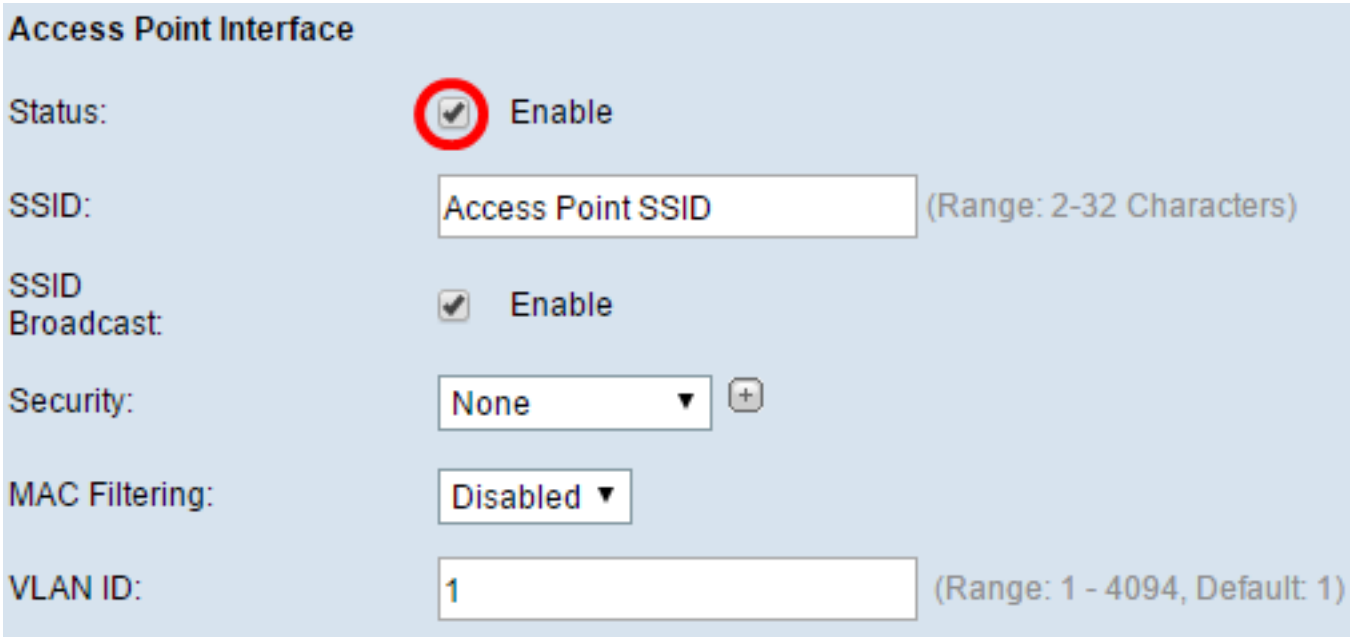
Paso 18. Ingrese el VLAN ID para la interfaz del cliente de la infraestructura. El valor por defecto es 1.

Nota: Por este ejemplo, se utiliza el VLAN predeterminado ID.



Interfaz del Punto de acceso

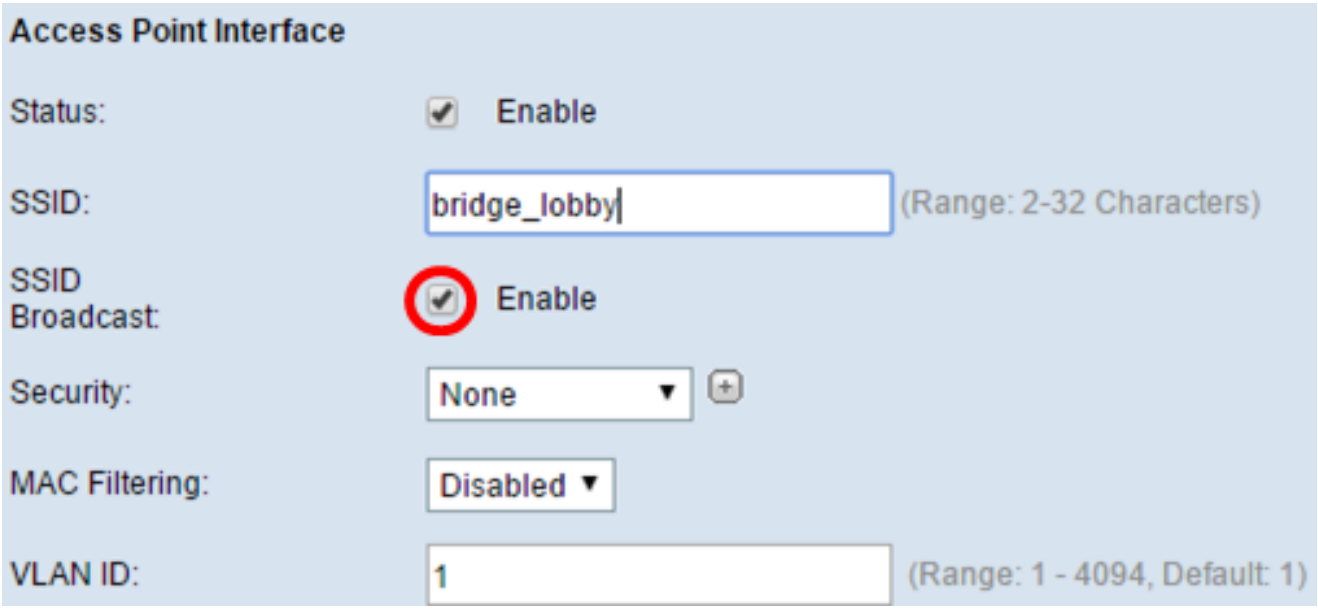
Paso 1. Marque el cuadro de revisión de estado del **permiso** para habilitar el bridging en la interfaz del Punto de acceso.



Paso 2. Ingrese el SSID para el Punto de acceso en el campo *SSID*. La longitud SSID debe estar entre 2 a 32 caracteres. El valor por defecto es el Punto de acceso SSID.

Nota: Por este ejemplo, el SSID usado es bridge_lobby.

El paso 3. (opcional) si usted no quiere transmitir el SSID, desmarca la casilla de verificación del broadcast del **permiso** SSID. El hacer tan hará el Punto de acceso invisible a ésos que buscan para los untos de acceso de red inalámbrica; puede ser conectado solamente con por alguien que conoce ya el SSID. El broadcast SSID se habilita por abandono.

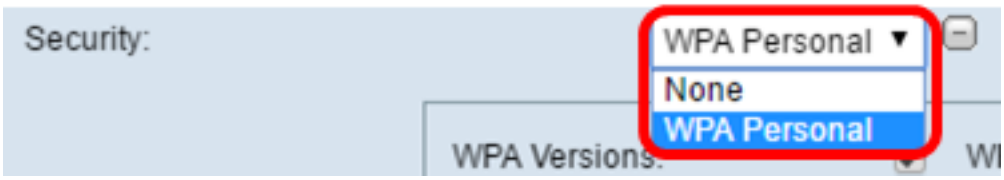


Paso 4. Elija el tipo de Seguridad para autenticar las estaciones del cliente descendiente al WAP de la lista desplegable de la Seguridad.

Se definen las opciones disponibles como sigue:

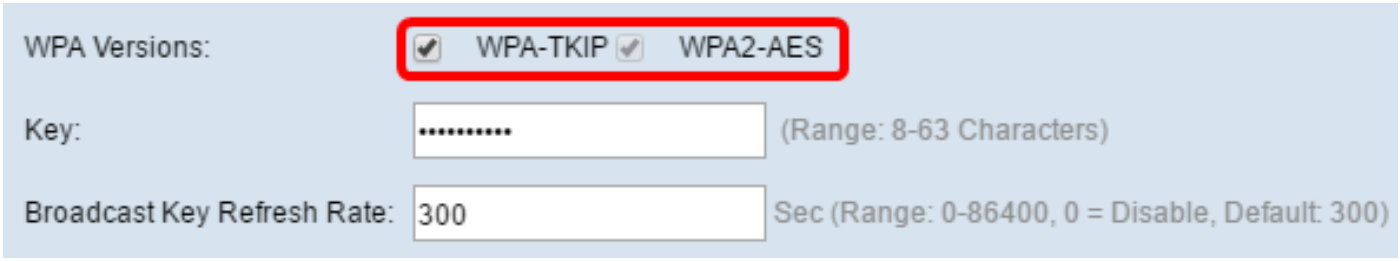
- Ninguno — Ábrase o ninguna Seguridad. Éste es el valor predeterminado. Salte al paso 10 si usted elige esto.
- WPA personal — El Acceso protegido de Wi-Fi (WPA) personal puede soportar las claves de 8 a 63 caracteres de largo. El método de encripción es TKIP o modo contrario de la cifra con

el bloque que encadena el protocolo del Message Authentication Code (CCMP). El WPA2 con el CCMP se recomienda pues tiene una norma de encripción más potente, Advanced Encryption Standard (AES), comparado al Temporal Key Integrity Protocol (TKIP) que utilice solamente un estándar 64-bit RC4.

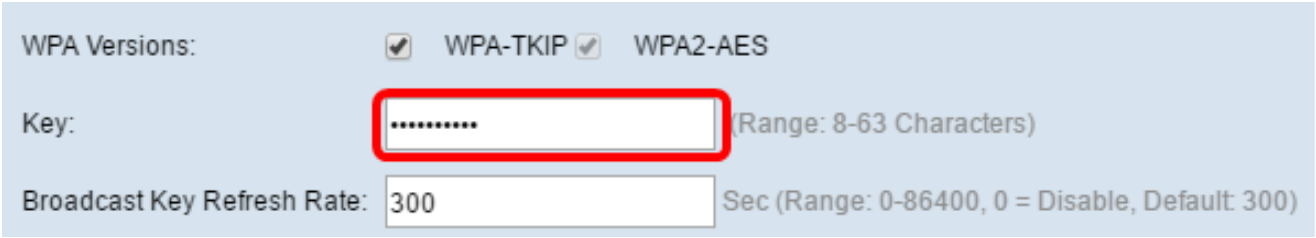


Paso 5. Marque la casilla de verificación **WPA-TKIP** o **WPA2-AES** para determinar que la clase de cifrado WPA la interfaz del Punto de acceso utilizará. Éstos se habilitan por abandono.

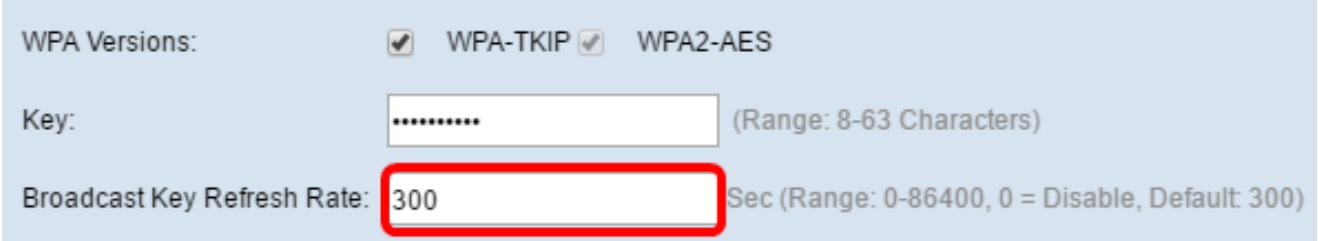
Nota: Si todo su soporte de equipo de red inalámbrica WPA2, entonces fijó la Seguridad del cliente de la infraestructura a WPA2-AES. El método de encripción es RC4 para el WPA y el Advanced Encryption Standard (AES) para el WPA2. Se recomienda el WPA2 pues tiene una norma de encripción más potente. Por este ejemplo, se utiliza WPA2-AES.



Paso 6. Ingrese la clave compartida WPA en el *campo clave*. La clave debe ser 8-63 caracteres de largo y puede incluir los caracteres alfanuméricos, las mayúsculas y minúsculas, y los caracteres especiales.



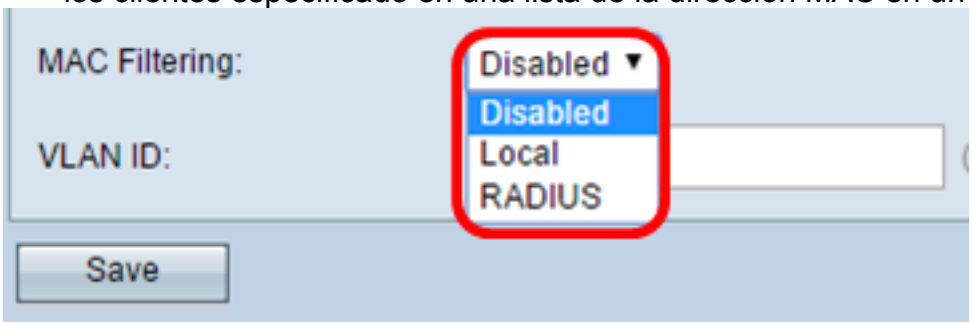
Paso 7. Ingrese la tarifa en el campo de la *velocidad de actualización dominante del broadcast*. La velocidad de actualización de la clave del broadcast especifica el intervalo en el cual la clave de seguridad se restaura para los clientes asociados a este Punto de acceso. La tarifa debe estar entre 0-86400, con un valor de 0 inhabilitando la característica. El valor por defecto es 300.



Paso 8. Elija el tipo de MAC que le filtra deseo para configurar para la interfaz del Punto de acceso de la lista desplegable de filtración MAC. Cuando están habilitados, conceden los usuarios o el acceso negado al WAP se basa en la dirección MAC del cliente que utilizan.

Se definen las opciones disponibles como sigue:

- Discapacitado — Todos los clientes pueden acceder la red ascendente. Éste es el valor predeterminado.
- Local — El conjunto de los clientes que pueden acceder la red ascendente se restringe a los clientes especificado en una lista localmente definida de la dirección MAC.
- RADIUS — El conjunto de los clientes que pueden acceder la red ascendente se restringe a los clientes especificado en una lista de la dirección MAC en un servidor de RADIUS.

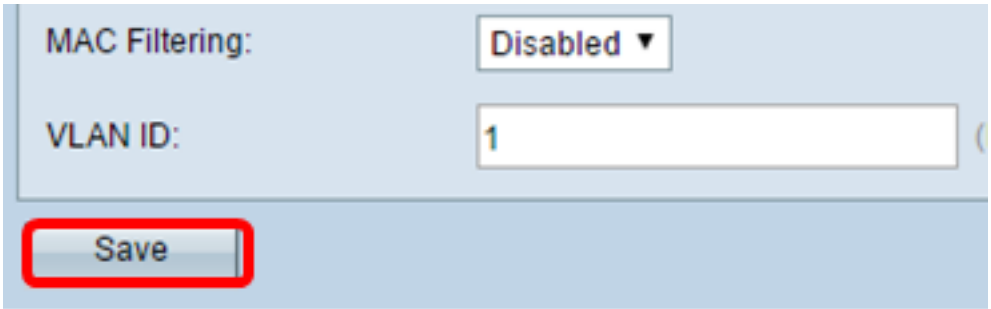


Nota: Por este ejemplo, eligen al minusválido.

Paso 9. Ingrese el VLAN ID en el campo *VLAN ID* para la interfaz del Punto de acceso.

Nota: Para permitir el bridging de los paquetes, la configuración de VLAN para la interfaz del Punto de acceso y la interfaz atada con alambre debe hacer juego el de la interfaz del cliente de la infraestructura.

Paso 10. **Salvaguardia del** tecleo para salvar sus cambios.



Usted debe ahora haber configurado con éxito un Workgroup Bridge en un unto de acceso de red inalámbrica.