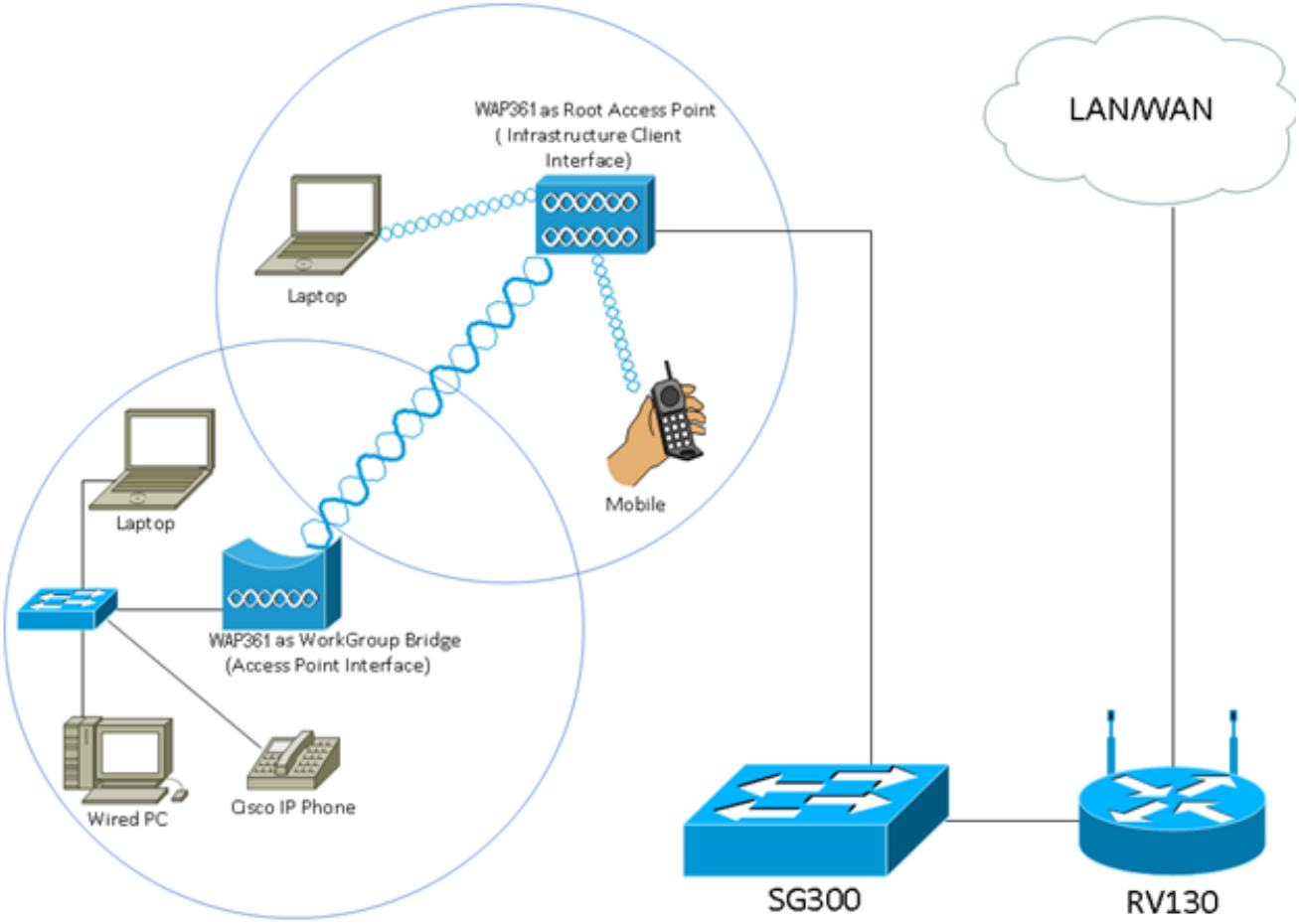
Configuración del puente de grupo de trabajo en un punto de acceso inalámbrico (WAP)

Objetivo

La función Puente de grupo de trabajo permite al punto de acceso inalámbrico (WAP) establecer un puente entre el tráfico de un cliente remoto y la red de área local (LAN) inalámbrica conectada con el modo de puente de grupo de trabajo. El dispositivo WAP asociado con la interfaz remota se conoce como interfaz de punto de acceso, mientras que el dispositivo WAP asociado con la LAN inalámbrica se conoce como interfaz de infraestructura. El puente de grupo de trabajo permite que los dispositivos que solo tienen conexiones por cable se conecten a una red inalámbrica. Se recomienda el modo de puente de grupo de trabajo como alternativa cuando la función Wireless Distribution System (WDS) no está disponible.



Nota: La topología anterior ilustra un modelo de Workgroup Bridge de ejemplo. Los dispositivos con cables están vinculados a un switch, que se conecta a la interfaz LAN del WAP. El WAP actúa como una interfaz de punto de acceso, se conecta a la interfaz de infraestructura.

En este artículo se explica cómo configurar el puente de grupo de trabajo entre dos WAP.

Dispositivos aplicables

- Serie WAP100

- Serie WAP300
- Serie WAP500

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

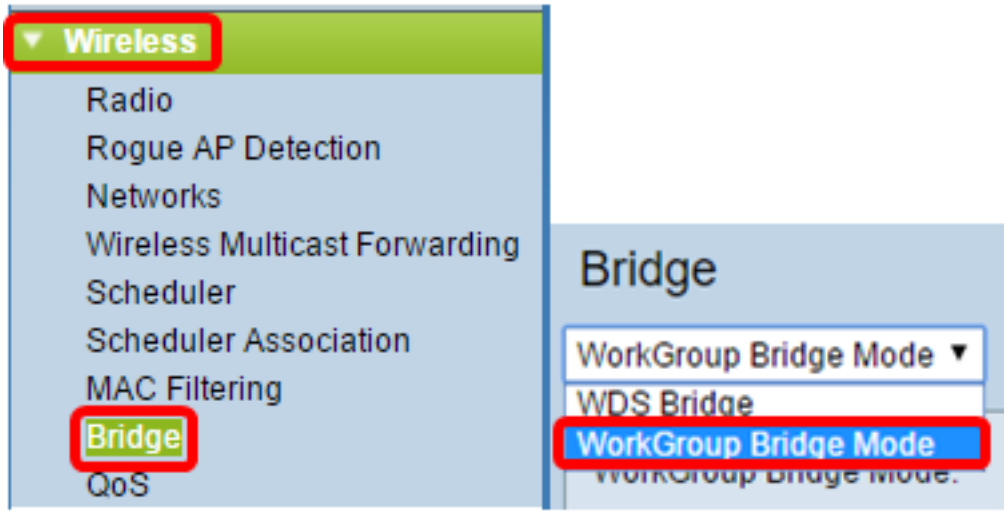
Configurar el puente de grupo de trabajo

Interfaz del cliente de infraestructura

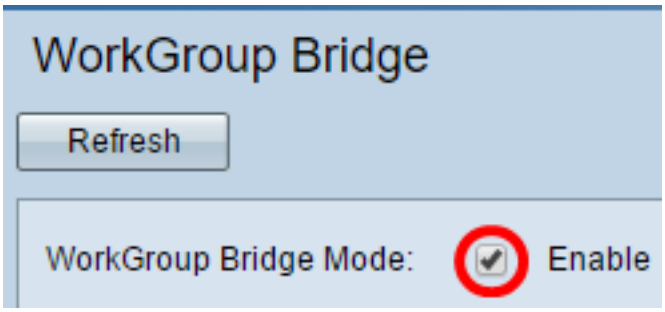
Paso 1. Inicie sesión en la utilidad basada en web del WAPy elija **Wireless > WorkGroup Bridge**.

Nota: Las opciones del menú pueden variar en función del modelo del dispositivo que esté utilizando. Las imágenes siguientes se toman del WAP361 a menos que se indique lo contrario.

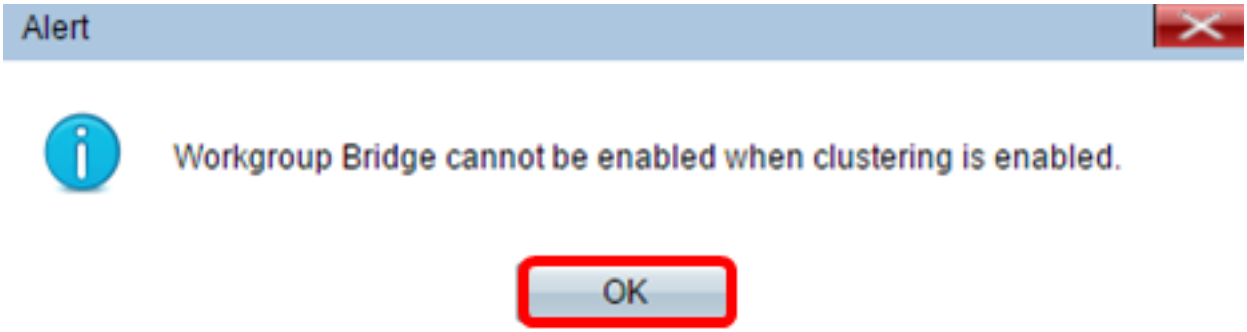
Para WAP571 y WAP571E, elija **Wireless > Bridge > WorkGroup Bridge Mode**.



Paso 2. Marque la casilla de verificación **Enable Work** Group Bridge Mode (Habilitar modo de puente de grupo de trabajo).

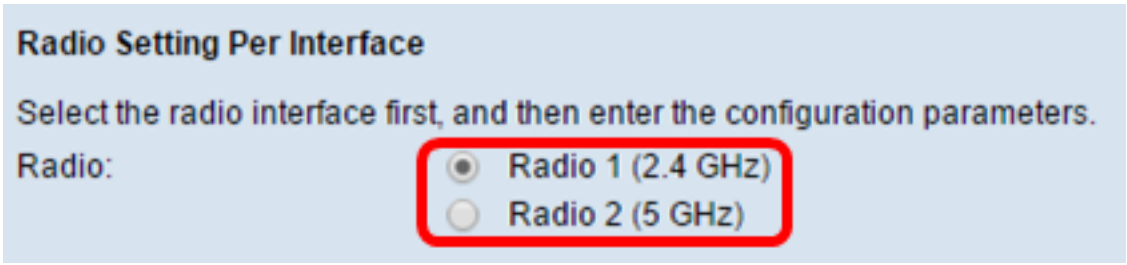


Nota: Si la agrupación en clúster está activada en WAP, una ventana emergente le notificará que deshabilite la agrupación en clúster para que funcione el puente de grupo de trabajo. Para continuar, haga clic en OK (Aceptar). Para desactivar la agrupación en clúster, elija **Single Point Setup** en el panel de navegación y luego **Access Points > Disable Single Point Setup**.



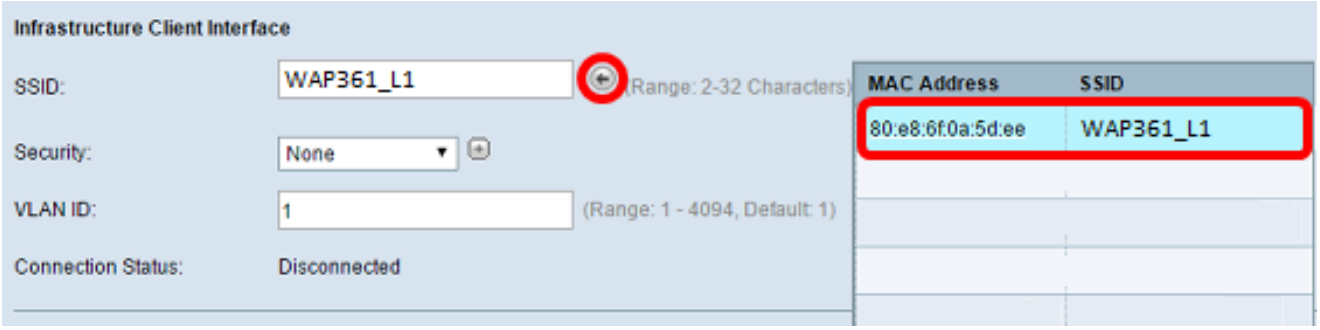
Paso 3. Haga clic en la interfaz de radio del puente de grupo de trabajo. Cuando se configura una radio como puente de grupo de trabajo, la otra permanece operativa. Las interfaces de radio corresponden a las bandas de radiofrecuencia del WAP. El WAP está equipado para transmitir en dos interfaces de radio diferentes. La configuración de la configuración de una interfaz de radio no afectará a la otra. Las opciones de la interfaz de radio pueden variar según el modelo WAP. Algunos WAP muestran Radio 1 como 2,4 GHz mientras que otros tienen Radio 2 como 2,4 GHz.

Nota: Este paso es sólo para los siguientes WAP con doble banda: WAP131, WAP150, WAP351, WAP361, WAP371, WAP561, WAP571, WAP571E. Para este ejemplo, se elige Radio 1.



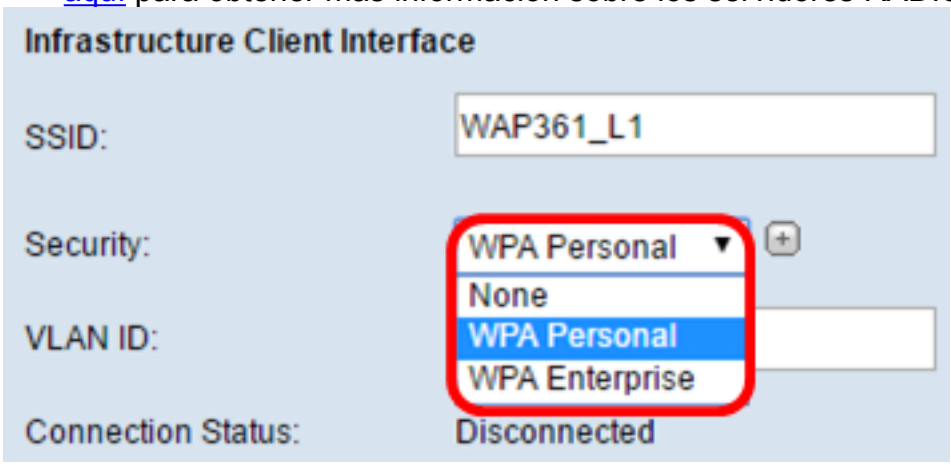
Paso 4. Introduzca el nombre del identificador del conjunto de servicios (SSID) en el campo *SSID* o haga clic en el botón de flecha situado junto al campo para buscar vecinos. Esto sirve como la conexión entre el dispositivo y el cliente remoto. Puede introducir de 2 a 32 caracteres para el SSID del cliente de infraestructura.

Nota: Es importante habilitar la detección de AP rogue. Para obtener más información sobre cómo habilitar dicha función, haga clic aquí. Para este ejemplo, se hace clic en el botón de flecha para elegir WAP361_L1 como SSID de la interfaz cliente de infraestructura.



Paso 5. En el área Infrastructure Client Interface , elija el tipo de seguridad para autenticar como estación cliente en el dispositivo WAP ascendente de la lista desplegable Security . Las opciones son:

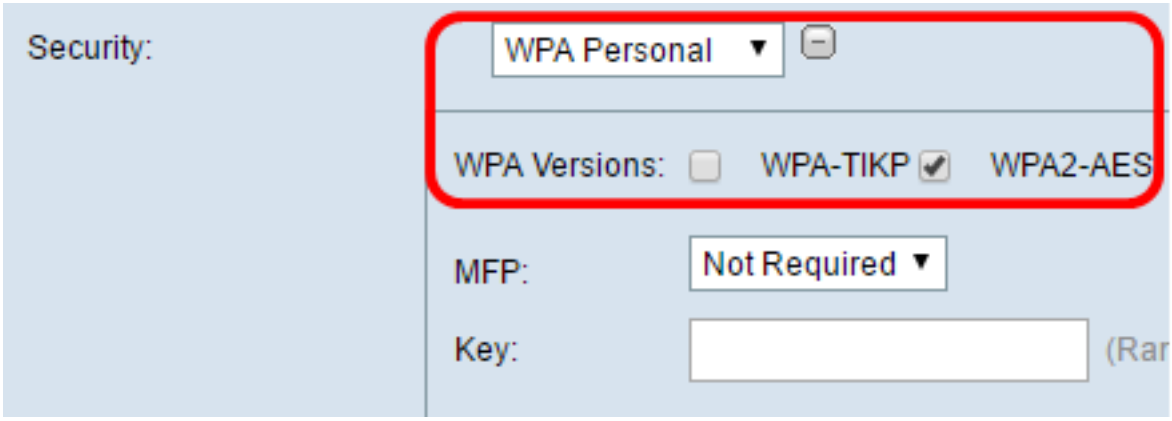
- Ninguno: seguridad abierta o no. Este es el valor predeterminado. Si selecciona esta opción, vaya directamente al Paso 18.
- WPA Personal: WPA Personal admite claves de entre 8 y 63 caracteres. Se recomienda utilizar WPA2, ya que cuenta con un estándar de encriptación más eficaz. Vaya al Paso 6 para configurar.
- WPA Enterprise: WPA Enterprise es más avanzado que WPA Personal y es la seguridad recomendada para la autenticación. Utiliza protocolo de autenticación extensible protegido (PEAP) y seguridad de la capa de transporte (TLS). Vaya al paso 9 para configurar. Este tipo de seguridad se suele utilizar en un entorno de oficina y necesita un servidor RADIUS (servicio de usuario de acceso telefónico de autenticación remota) configurado. Haga clic aquí para obtener más información sobre los servidores RADIUS.



Nota: En este ejemplo, se elige WPA Personal.

Paso 6. Haga clic en **+** y marque la casilla de verificación WPA-TKIP o WPA2-AES para determinar qué tipo de encriptación WPA utilizará la interfaz cliente de infraestructura.

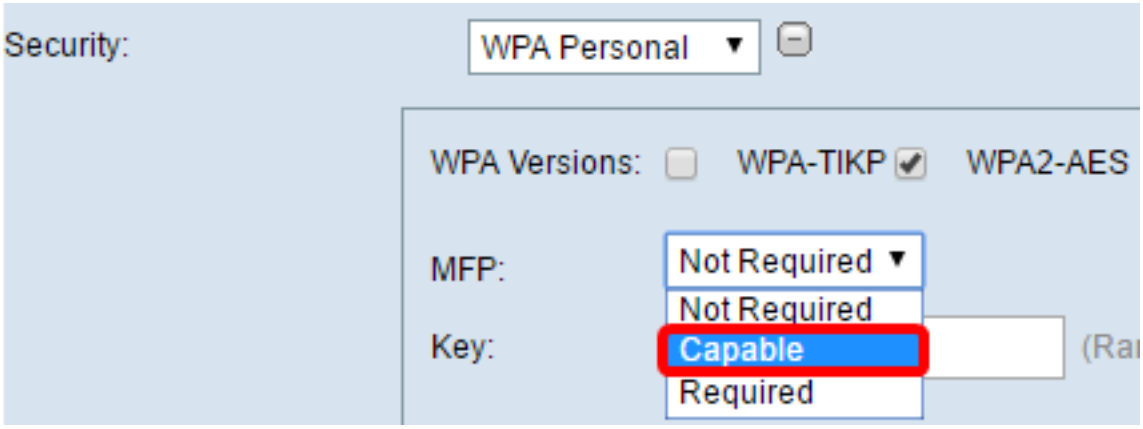
Nota: Si todos los equipos inalámbricos admiten WPA2, establezca la seguridad del cliente de infraestructura en WPA2-AES. El método de encriptación es RC4 para WPA y Advanced Encryption Standard (AES) para WPA2. Se recomienda utilizar WPA2, ya que cuenta con un estándar de encriptación más eficaz. Para este ejemplo, se utiliza WPA2-AES.



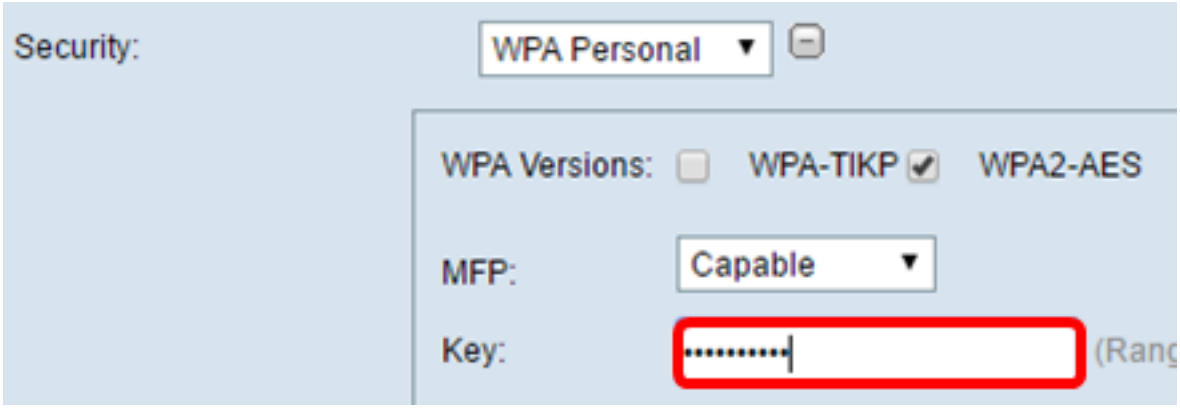
Paso 7. (Opcional) Si ha activado WPA2-AES en el paso 6, elija una opción en la lista desplegable Management Frame Protection (MFP), tanto si desea que WAP requiera que haya tramas protegidas como si no. Para obtener más información sobre MFP, haga clic aquí. Las opciones son:

- No es necesario: desactiva el soporte de cliente para MFP.
- Capaz: permite que tanto los clientes con capacidad MFP como los que no admiten MFP se unan a la red. Esta es la configuración MFP predeterminada en el WAP.
- Obligatorio: los clientes pueden asociarse sólo si se negocia MFP. Si los dispositivos no admiten MFP, no se les permite unirse a la red.

Nota: Para este ejemplo, se elige Capable.



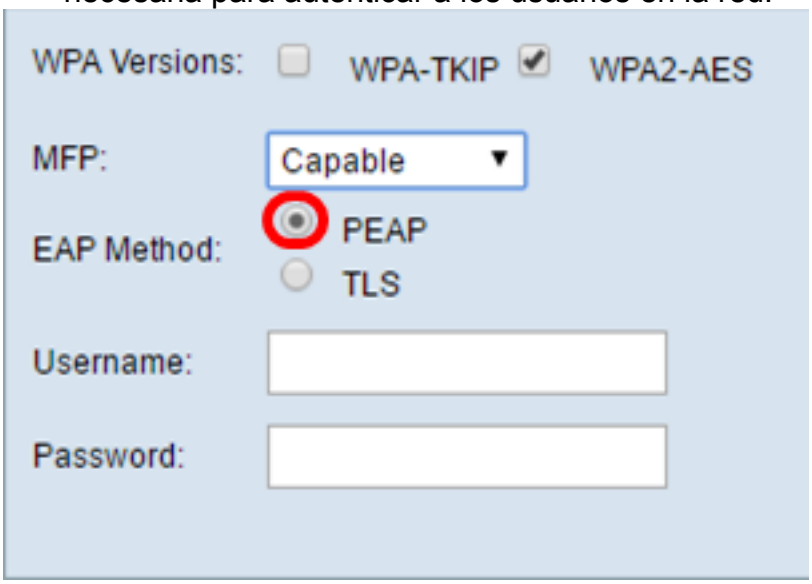
Paso 8. Introduzca la clave de encriptación WPA en el campo *Key*. La clave debe tener entre 8 y 63 caracteres. Se trata de una combinación de letras, números y caracteres especiales. Se trata de la contraseña que se utiliza al conectarse a la red inalámbrica por primera vez. Luego, vaya directamente al Paso 18.



Paso 9. Si selecciona WPA Enterprise en el paso 5, haga clic en un botón de opción para el método EAP.

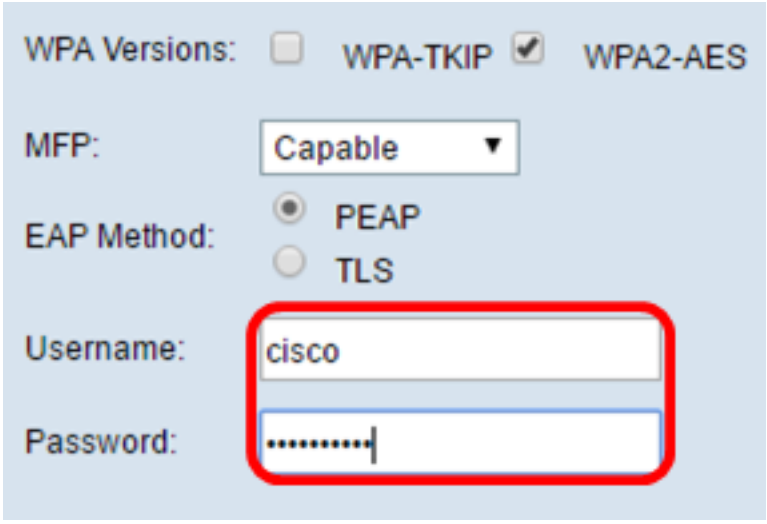
Las opciones disponibles se definen de la siguiente manera:

- PEAP: este protocolo proporciona a cada usuario inalámbrico bajo los nombres de usuario y contraseñas individuales WAP que soportan los estándares de encriptación AES. Dado que PEAP es un método de seguridad basado en contraseña, su seguridad Wi-Fi se basa en las credenciales del dispositivo del cliente. PEAP puede suponer un riesgo de seguridad potencialmente grave si tiene contraseñas débiles o clientes no seguros. Se basa en TLS pero evita la instalación de certificados digitales en cada cliente. En su lugar, proporciona autenticación a través de un nombre de usuario y una contraseña.
- TLS: TLS requiere que cada usuario tenga un certificado adicional para que se le conceda acceso. TLS es más seguro si dispone de los servidores adicionales y la infraestructura necesaria para autenticar a los usuarios en la red.

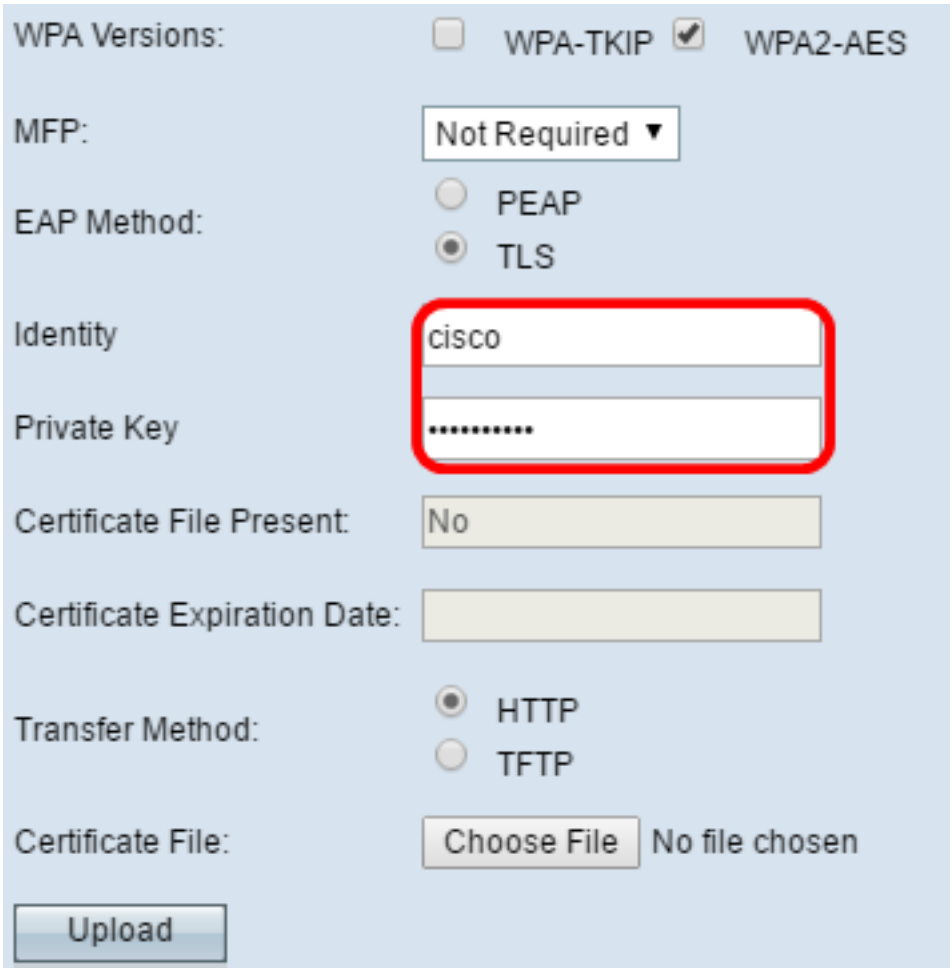


Nota: Para este ejemplo, se elige PEAP.

Paso 10. Ingrese el nombre de usuario y la contraseña para el cliente de infraestructura en los campos *Nombre de usuario* y *Contraseña*. Esta es la información de inicio de sesión que se utiliza para conectarse a la interfaz de cliente de infraestructura; consulte la interfaz del cliente de infraestructura para encontrar esta información. Luego, vaya directamente al Paso 18.

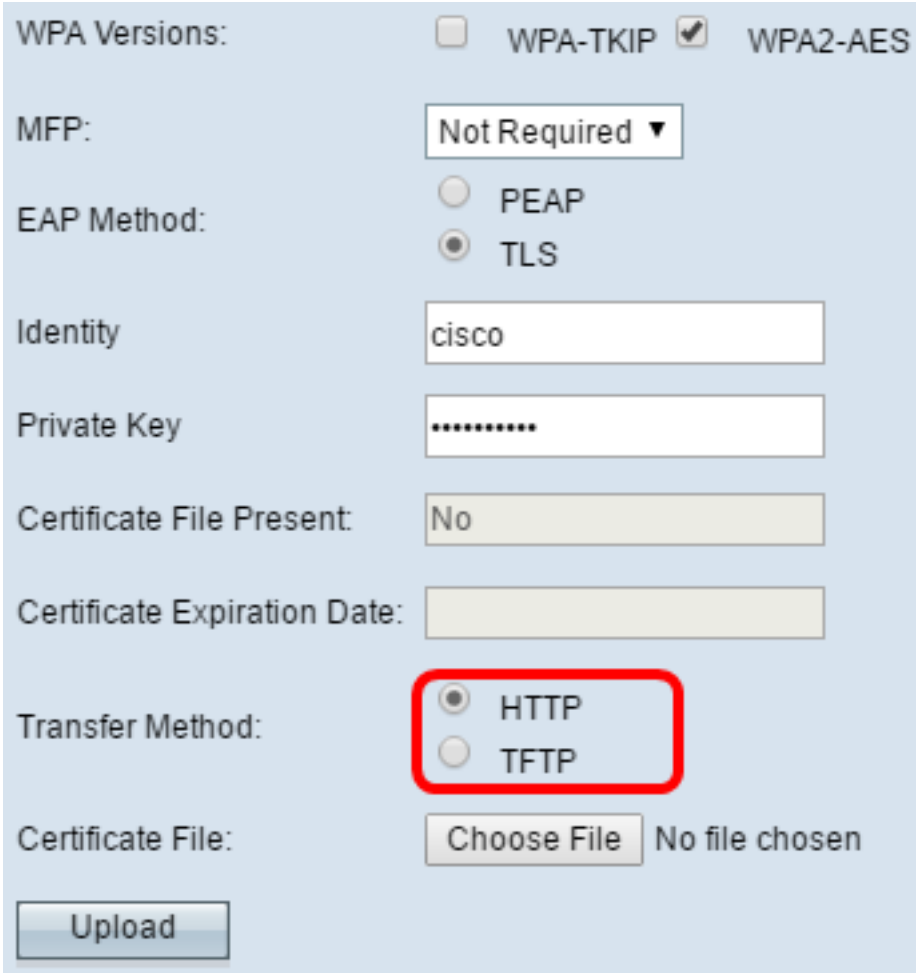


Paso 11. Si hizo clic en TLS en el Paso 9, introduzca la identidad y la clave privada del cliente de infraestructura en los campos *Identity* y *Private Key*.



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

- TFTP: el protocolo de transferencia de archivos trivial (TFTP) es una versión simplificada y no segura del protocolo de transferencia de archivos (FTP). Se utiliza principalmente para distribuir software o autenticar dispositivos entre redes corporativas. Si hizo clic en TFTP, vaya directamente al Paso 15.
- HTTP: el protocolo de transferencia de hipertexto (HTTP) proporciona un marco de autenticación simple de respuesta al desafío que puede utilizar un cliente para proporcionar un marco de autenticación.

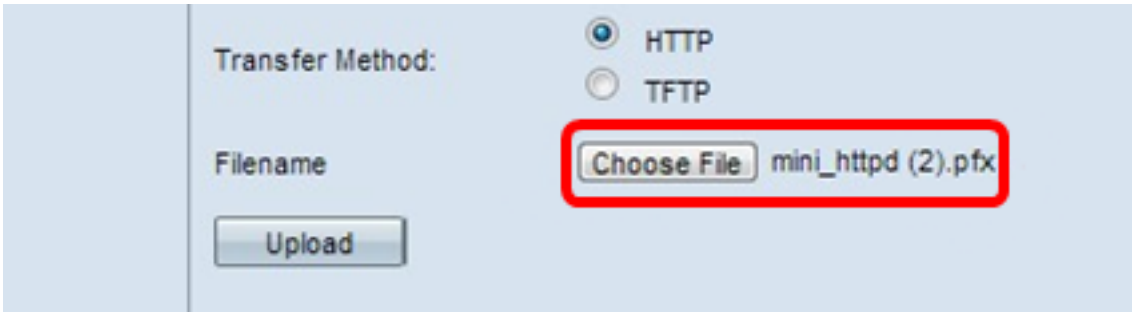


Nota: Si ya hay un archivo de certificado en el WAP, los campos *Archivo de certificado presente* y *Fecha de vencimiento del certificado* ya se rellenarán con la información pertinente. De lo contrario, estarán en blanco.

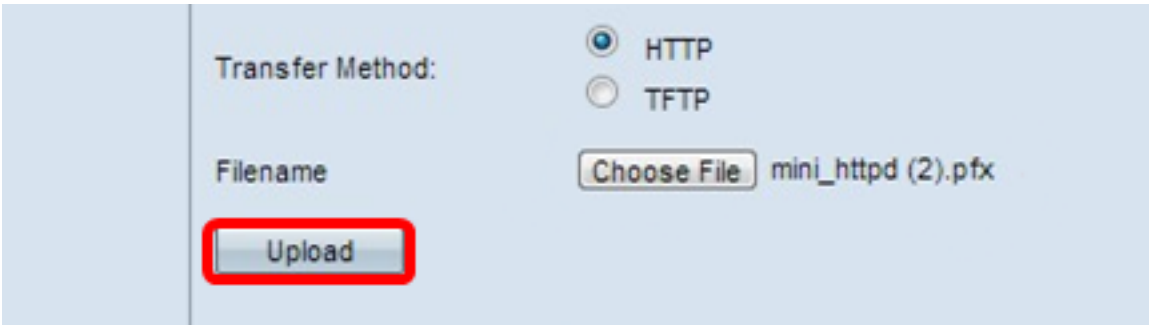
HTTP

Paso 13. Haga clic en el botón **Elegir archivo** para buscar y seleccionar un archivo de certificado. El archivo debe tener la extensión de archivo de certificado adecuada (como .pem o .pfx) de lo contrario, el archivo no se aceptará.

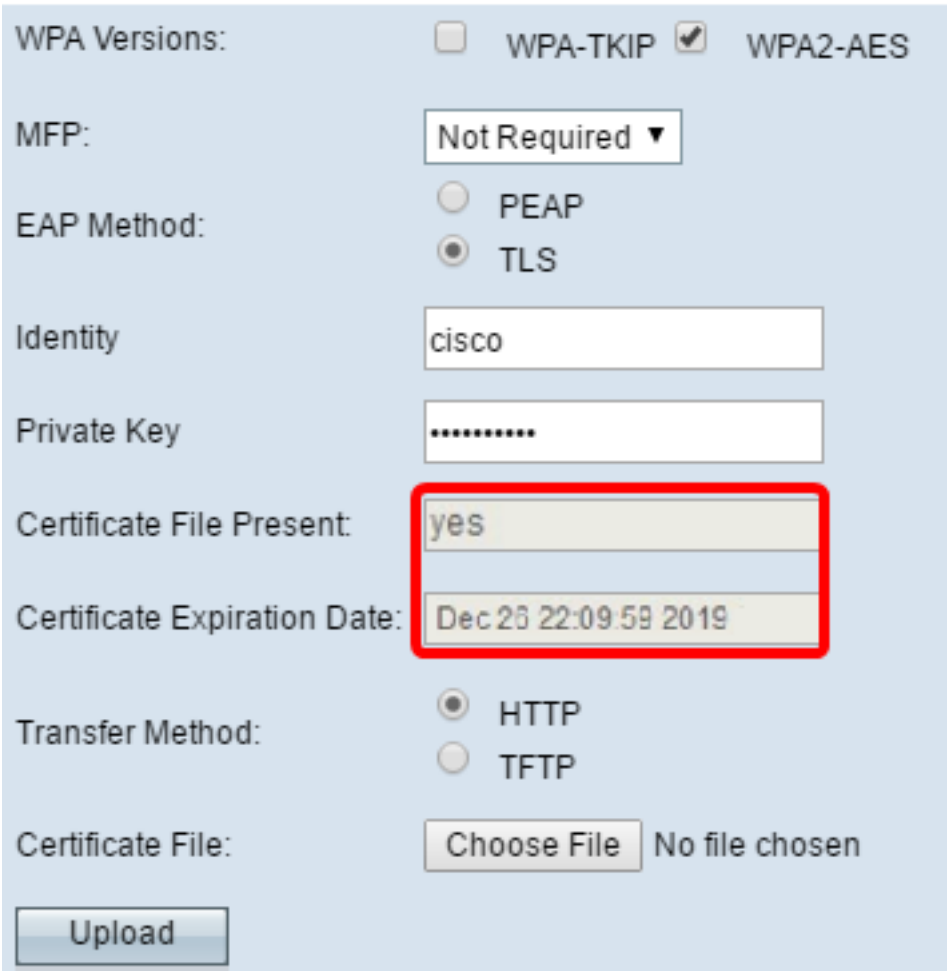
Nota: En este ejemplo, se elige mini_httpd(2).pfx.



Paso 14. Haga clic en **Cargar** para cargar el archivo de certificado seleccionado. Saltar al Paso 18.



Los campos *Archivo de certificado presente* y *Fecha de vencimiento del certificado* se actualizarán automáticamente.



TFTP

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

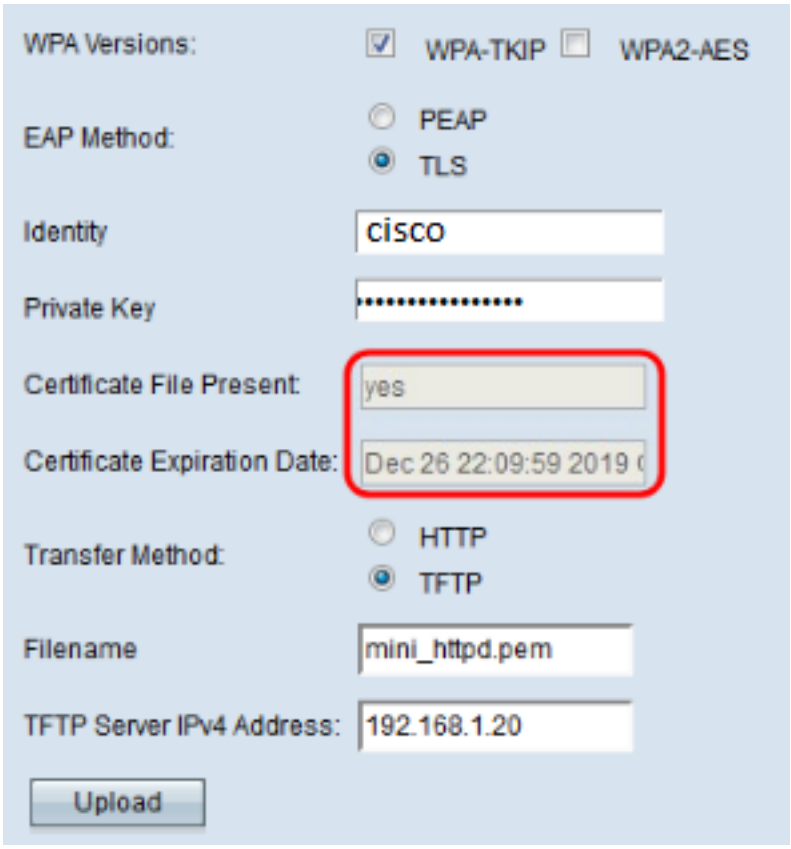
Nota: En este ejemplo, se utiliza mini_httpd.pem.

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

Nota: En este ejemplo. 192.168.1.20 se utiliza como dirección del servidor TFTP.

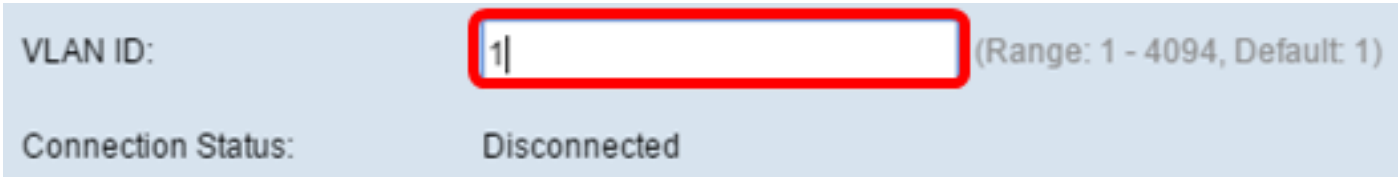
Paso 17. Haga clic en el botón **Cargar** para cargar el archivo de certificado especificado.

Los campos *Archivo de certificado presente* y *Fecha de vencimiento del certificado* se actualizarán automáticamente.



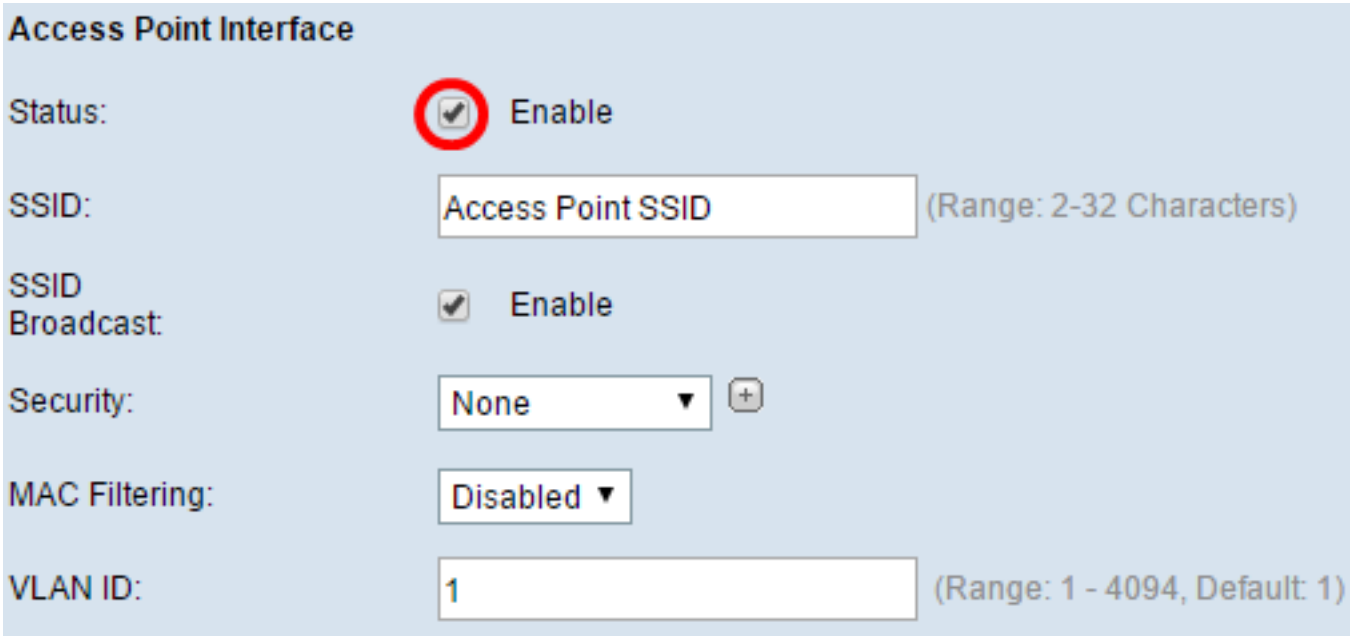
Paso 18. Introduzca el ID de VLAN para la interfaz de cliente de infraestructura. El valor por defecto es 1.

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



Interfaz del punto de acceso

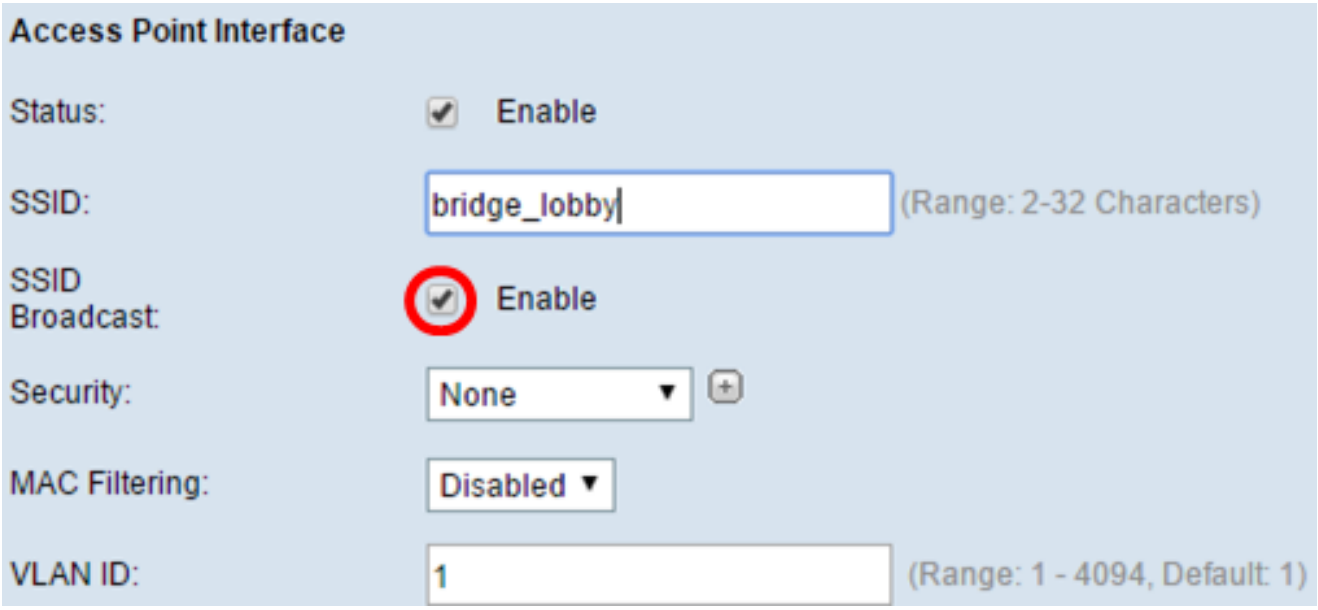
Paso 1. Marque la casilla de verificación **Enable** Status para habilitar el bridging en la interfaz del punto de acceso.



Paso 2. Ingrese el SSID para el punto de acceso en el campo *SSID*. La longitud de SSID debe estar entre 2 y 32 caracteres. El valor predeterminado es Access Point SSID (SSID del punto de acceso).

Nota: Para este ejemplo, el SSID utilizado es bridge_hall.

Paso 3. (Opcional) Si no desea difundir el SSID, desmarque la casilla de verificación **Habilitar** difusión SSID. De esta forma, el punto de acceso será invisible para quienes busquen puntos de acceso inalámbricos; sólo puede ser conectado por alguien que ya conoce el SSID. SSID Broadcast (Difusión de SSID) está habilitado de forma predeterminada.

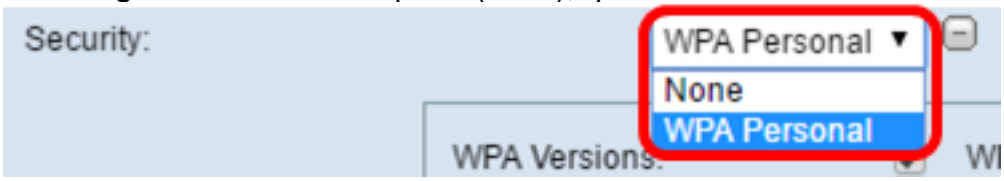


Paso 4. Elija el tipo de seguridad para autenticar las estaciones de cliente descendentes en el WAP de la lista desplegable Seguridad.

Las opciones disponibles se definen de la siguiente manera:

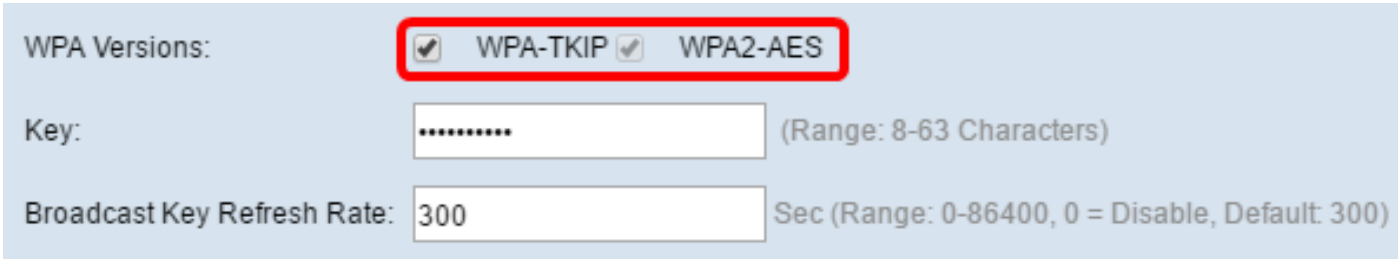
- Ninguno: abierto o sin seguridad. Este es el valor predeterminado. Vaya al Paso 10 si lo elige.
- WPA Personal: el acceso Wi-Fi protegido (WPA) Personal admite claves de 8 a 63 caracteres. El método de encriptación es TKIP o Counter Cipher Mode with Block Chaining

Message Authentication Code Protocol (CCMP). Se recomienda utilizar WPA2 con CCMP, ya que cuenta con un estándar de encriptación avanzado (AES) más eficaz que el protocolo de integridad de clave temporal (TKIP), que utiliza sólo un estándar RC4 de 64 bits.

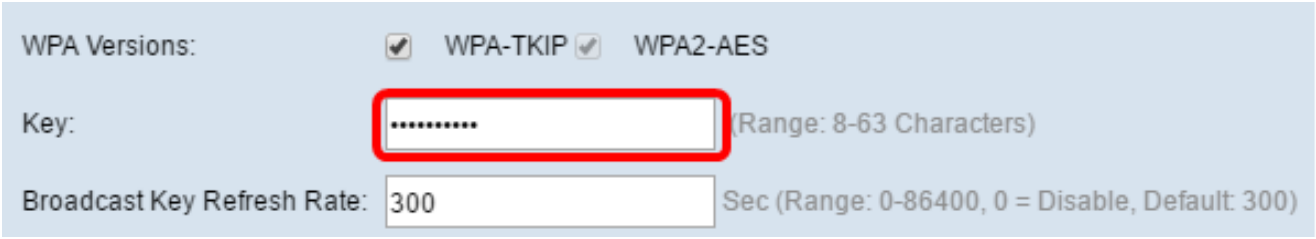


Paso 5. Marque la casilla de verificación **WPA-TKIP** o **WPA2-AES** para determinar qué tipo de encriptación WPA utilizará la interfaz del punto de acceso. Éstos se habilitan de forma predeterminada.

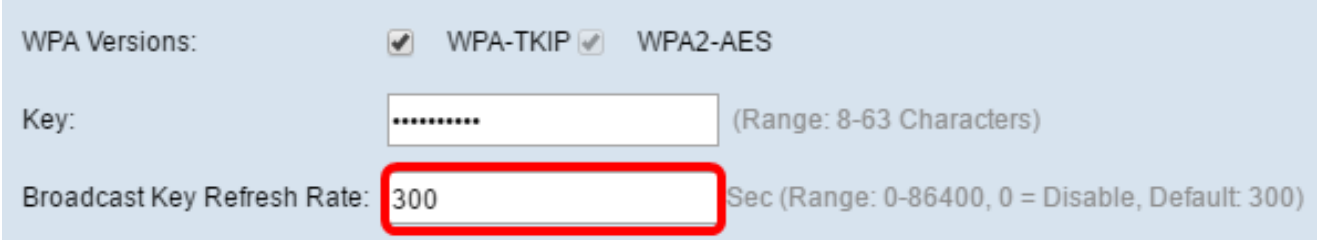
Nota: Si todos los equipos inalámbricos admiten WPA2, configure la seguridad del cliente de infraestructura en WPA2-AES. El método de encriptación es RC4 para WPA y Advanced Encryption Standard (AES) para WPA2. Se recomienda utilizar WPA2, ya que cuenta con un estándar de encriptación más eficaz. Para este ejemplo, se utiliza WPA2-AES.



Paso 6. Introduzca la clave WPA compartida en el campo *Key*. La clave debe tener entre 8 y 63 caracteres y puede incluir caracteres alfanuméricos, mayúsculas y minúsculas y caracteres especiales.



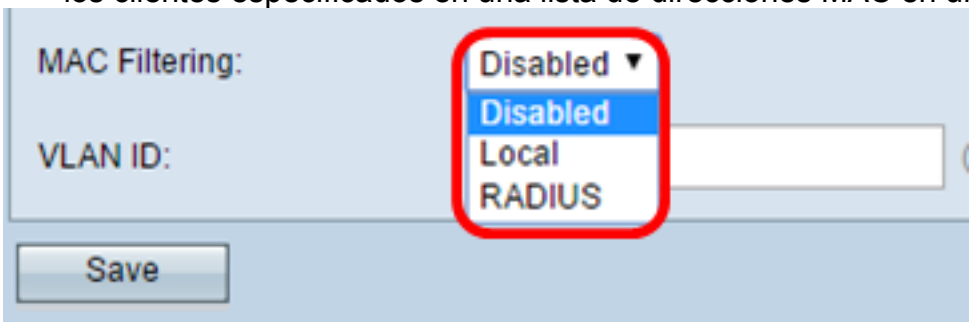
Paso 7. Introduzca la velocidad en el campo *Velocidad de actualización de la clave de difusión*. La velocidad de actualización de la clave de difusión especifica el intervalo en el que se actualiza la clave de seguridad para los clientes asociados a este punto de acceso. La velocidad debe estar entre 0-86400, con un valor de 0 desactivando la función. El valor predeterminado es 300.



Paso 8. Elija el tipo de filtrado MAC que desea configurar para la interfaz de punto de acceso en la lista desplegable Filtrado de MAC. Cuando se habilita, se concede o se deniega a los usuarios el acceso al WAP en función de la dirección MAC del cliente que utilizan.

Las opciones disponibles se definen de la siguiente manera:

- Desactivado: todos los clientes pueden acceder a la red ascendente. Este es el valor predeterminado.
- Local: el conjunto de clientes que pueden acceder a la red ascendente está restringido a los clientes especificados en una lista de direcciones MAC definida localmente.
- RADIUS: el conjunto de clientes que pueden acceder a la red ascendente está restringido a los clientes especificados en una lista de direcciones MAC en un servidor RADIUS.

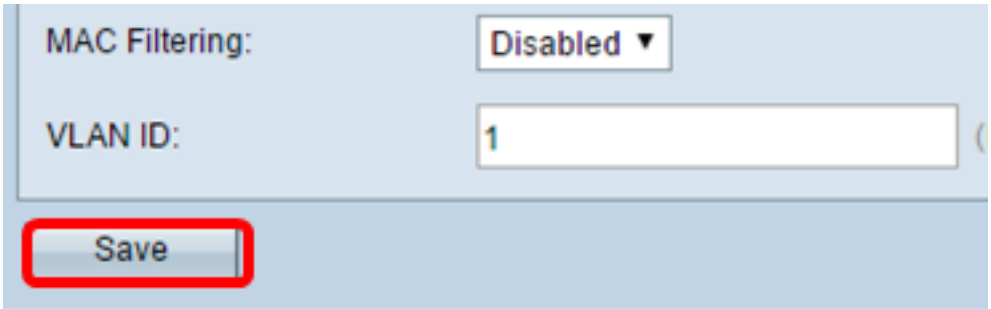


Nota: Para este ejemplo, se elige Desactivado.

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

Nota: Para permitir la conexión en puente de paquetes, la configuración de VLAN para la interfaz de punto de acceso y la interfaz por cable debe coincidir con la de la interfaz de cliente de infraestructura.

Paso 10. Haga clic en **Guardar** para guardar los cambios.



Ahora debería haber configurado correctamente un puente de grupo de trabajo en un punto de acceso inalámbrico.