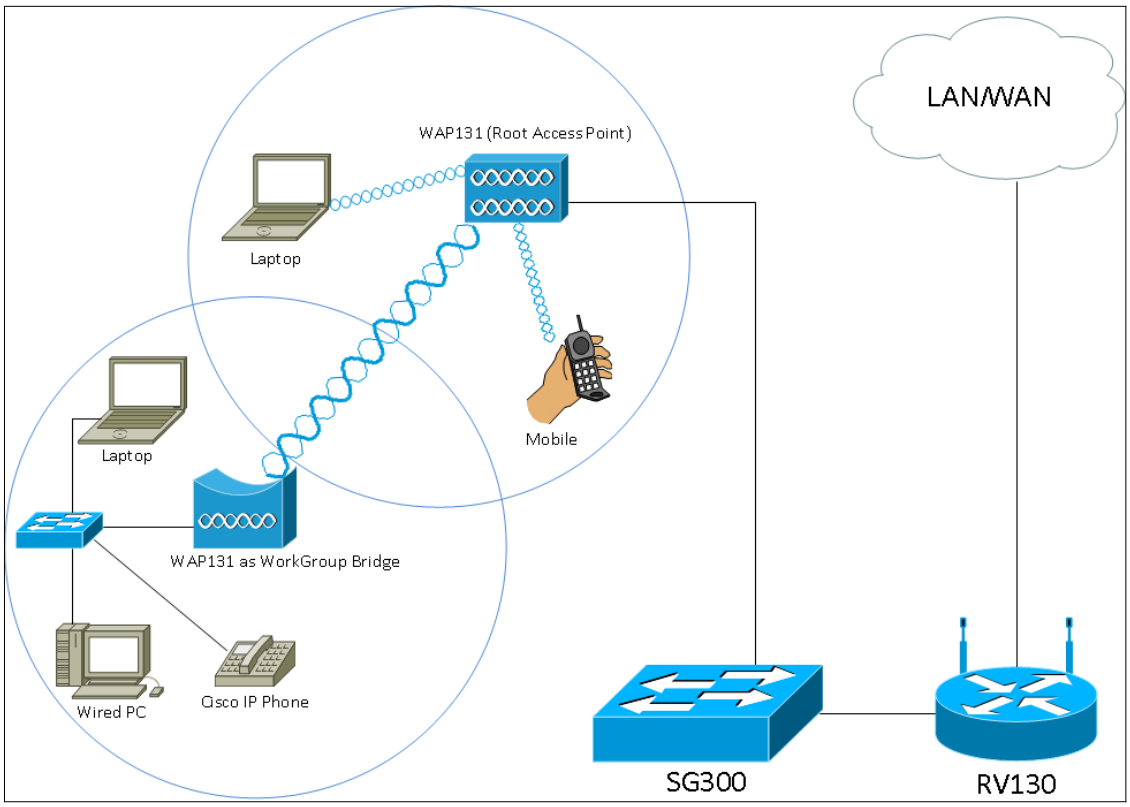
Configuración del puente de grupo de trabajo en el punto de acceso WAP131

Objetivo

La función Puente de grupo de trabajo permite al punto de acceso inalámbrico (WAP) conectar el tráfico entre un cliente remoto y la LAN inalámbrica que está 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 y el asociado con la LAN inalámbrica se denomina interfaz de infraestructura. Aunque el Wireless Distribution System (WDS) es la solución de puente preferida para el WAP131, se recomienda el modo de puente de grupo de trabajo cuando la función WDS no está disponible.



Nota: Cuando se habilita la función Workgroup Bridge, la función WDS bridge no funciona. Para ver cómo se configura el puente WDS, consulte el artículo *Configuración del puente del sistema de distribución inalámbrico (WDS) en el WAP131 y WAP351.*

El objetivo de este documento es explicar cómo configurar el puente de grupo de trabajo en el punto de acceso WAP131.

Dispositivos aplicables

·WAP131

Versión del software

•1.0.3.4

Configurar el puente de grupo de trabajo

Nota: Para habilitar el puente de grupo de trabajo, el agrupamiento debe estar habilitado en el WAP. Si la agrupación en clúster está desactivada, debe desactivar la configuración en un solo punto para activar la agrupación en clúster. Todos los dispositivos WAP que participan en el puente de grupo de trabajo deben tener la siguiente configuración idéntica:

Radio ·

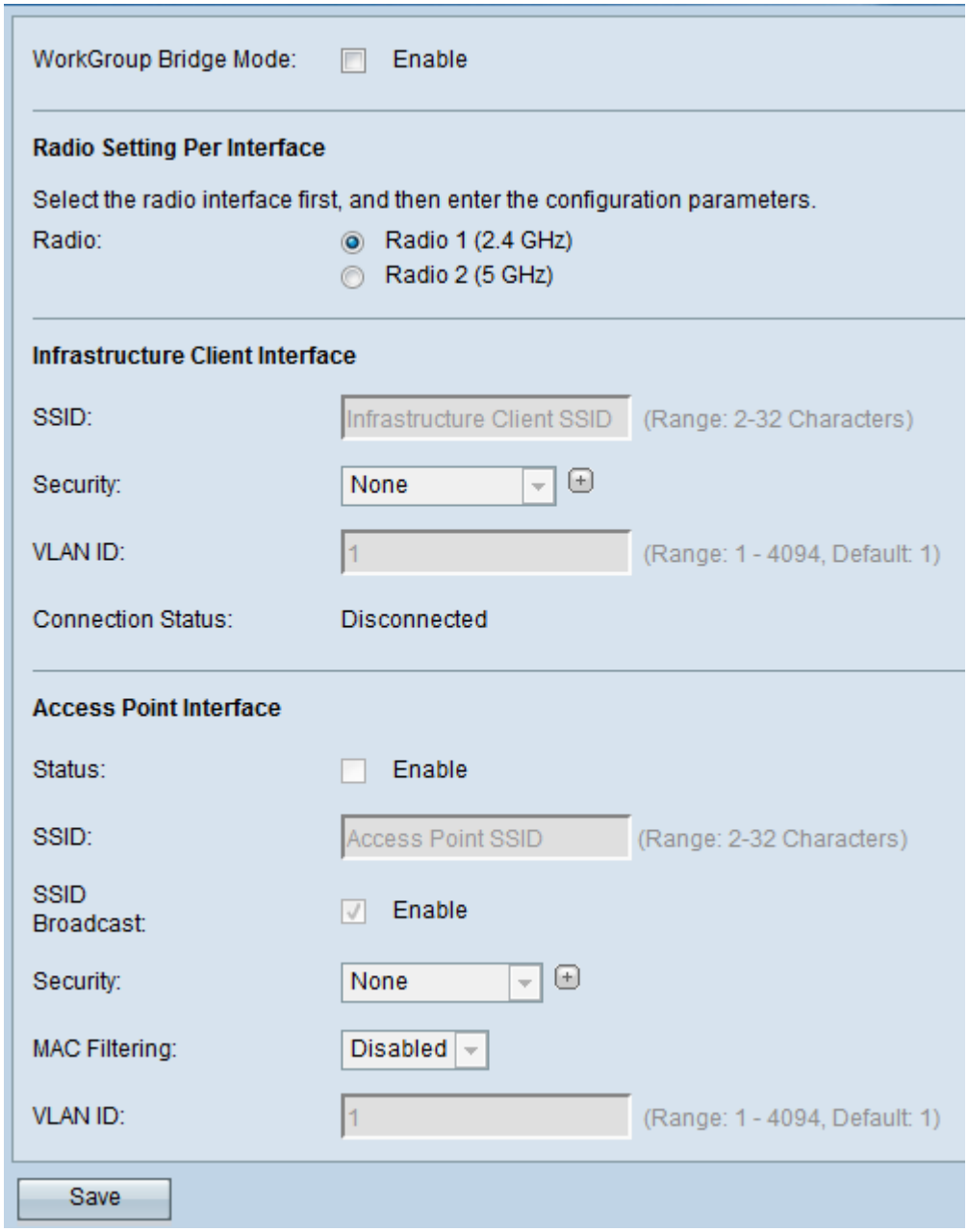
Modo · IEEE 802.11

Ancho de banda de canal ·

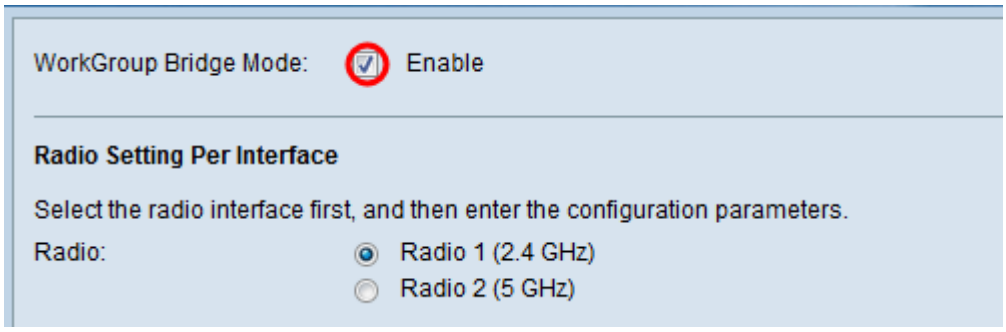
Canal · (no se recomienda automáticamente)

Para asegurarse de que estos parámetros son los mismos en todos los dispositivos, busque los parámetros de radio. Para configurar estos parámetros, refiérase al artículo *Configuración de Parámetros de Radio Inalámbricos Básicos en los Puntos de Acceso WAP131 y WAP351*.

Paso 1. Inicie sesión en Web Configuration Utility y elija **Wireless > WorkGroup** Bridge. Se abre la página *puente de grupo de trabajo*:

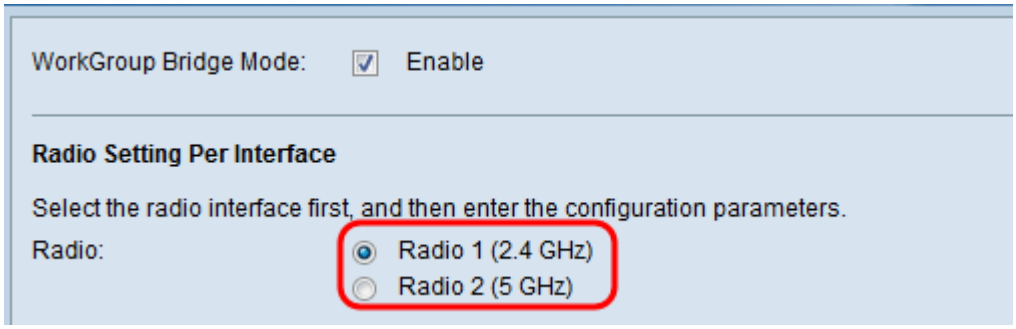


Paso 2. Marque la casilla **Enable** en el campo *WorkGroup Bridge Mode* para habilitar la función Workgroup bridge.



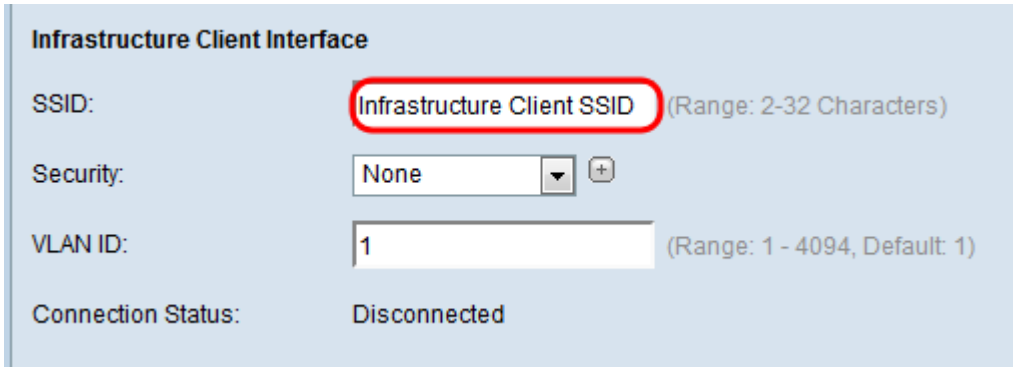
Configuración de radio

Paso 1. Seleccione la interfaz de radio para el puente del grupo de trabajo. Cuando configura una radio como puente de grupo de trabajo, la otra permanece operativa. Las interfaces de radio corresponden a las bandas de radiofrecuencia del WAP131. El WAP131 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.

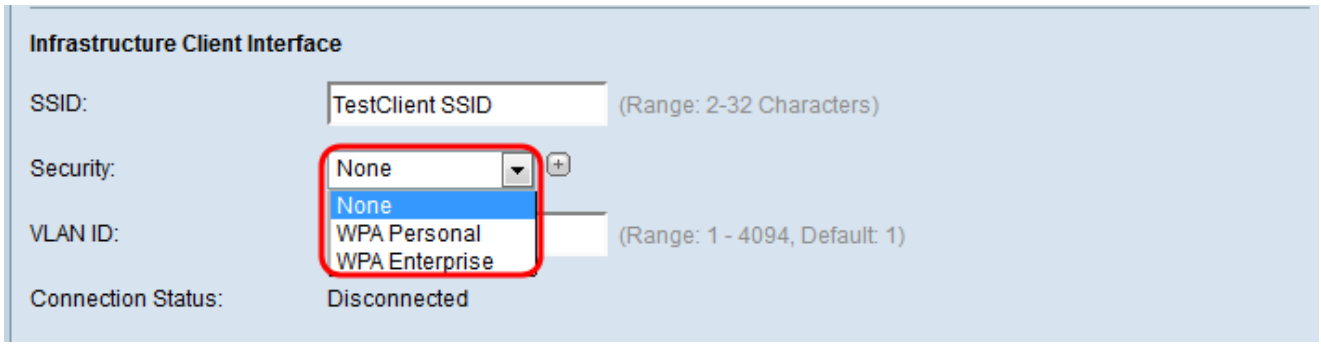


Interfaz del cliente de infraestructura

Paso 1. Introduzca el nombre del identificador del conjunto de servicios (SSID) en el campo *SSID*. El SSID debe tener entre 2 y 32 caracteres.



Paso 2. Elija el tipo de seguridad para autenticar una estación cliente en el dispositivo WAP ascendente de la lista desplegable *Seguridad*.



Las opciones disponibles se definen de la siguiente manera:

·Ninguno: abierto o sin seguridad. Este es el valor predeterminado. Si elige esto, vaya directamente al Paso 14.

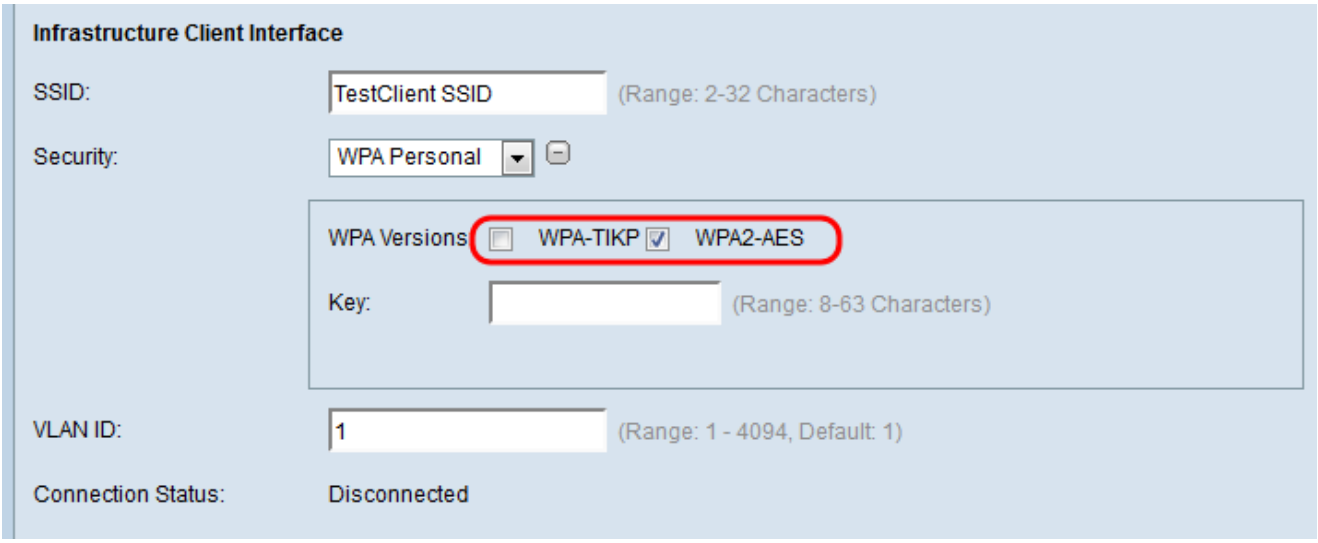
·WPA Personal: WPA Personal admite claves de entre 8 y 63 caracteres. El método de encriptación es RC4 para WPA y Advanced Encryption Standard (AES) para WPA2. Se recomienda utilizar WPA2, ya que cuenta con un estándar de encriptación más eficaz. Si elige esto, vaya al Paso 3.

·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). Si elige esto, vaya al Paso 5.

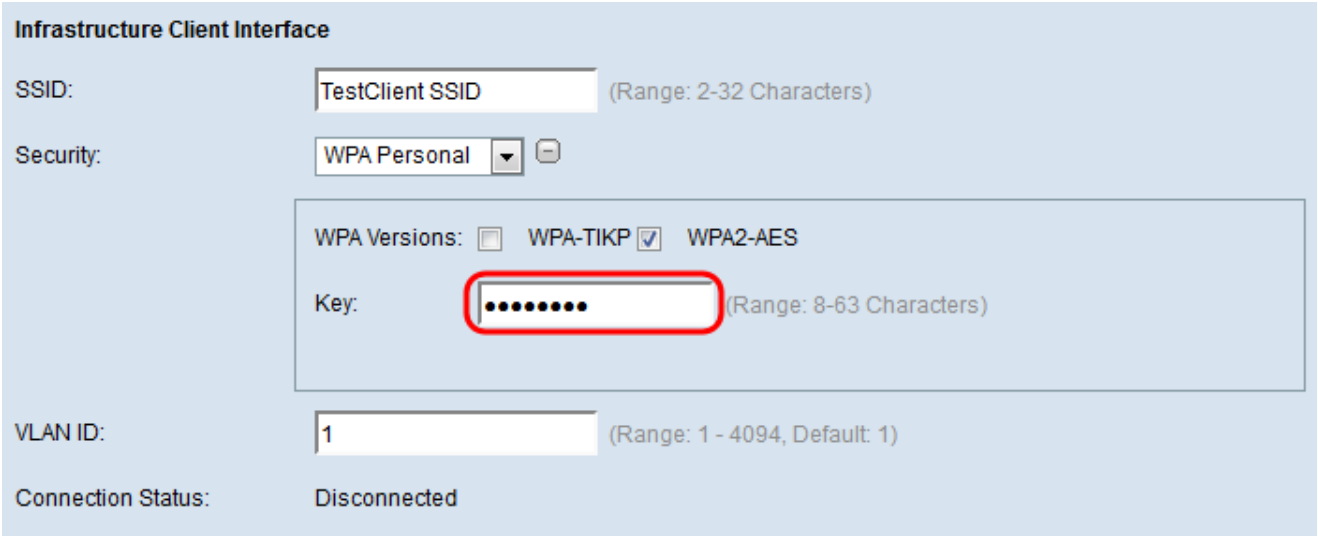
WPA Personal

Paso 3. Seleccione la casilla de verificación **WPA-TKIP** o **WPA2-AES** para determinar qué

tipo de encriptación WPA utilizará la interfaz cliente de infraestructura. Si todos los equipos inalámbricos admiten WPA2, configure la seguridad del cliente de infraestructura para WPA2-AES. Si algunos de los dispositivos inalámbricos, como los PDA y otros pequeños dispositivos de red inalámbrica, sólo se conectan con WPA-TKIP, seleccione WPA-TKIP.

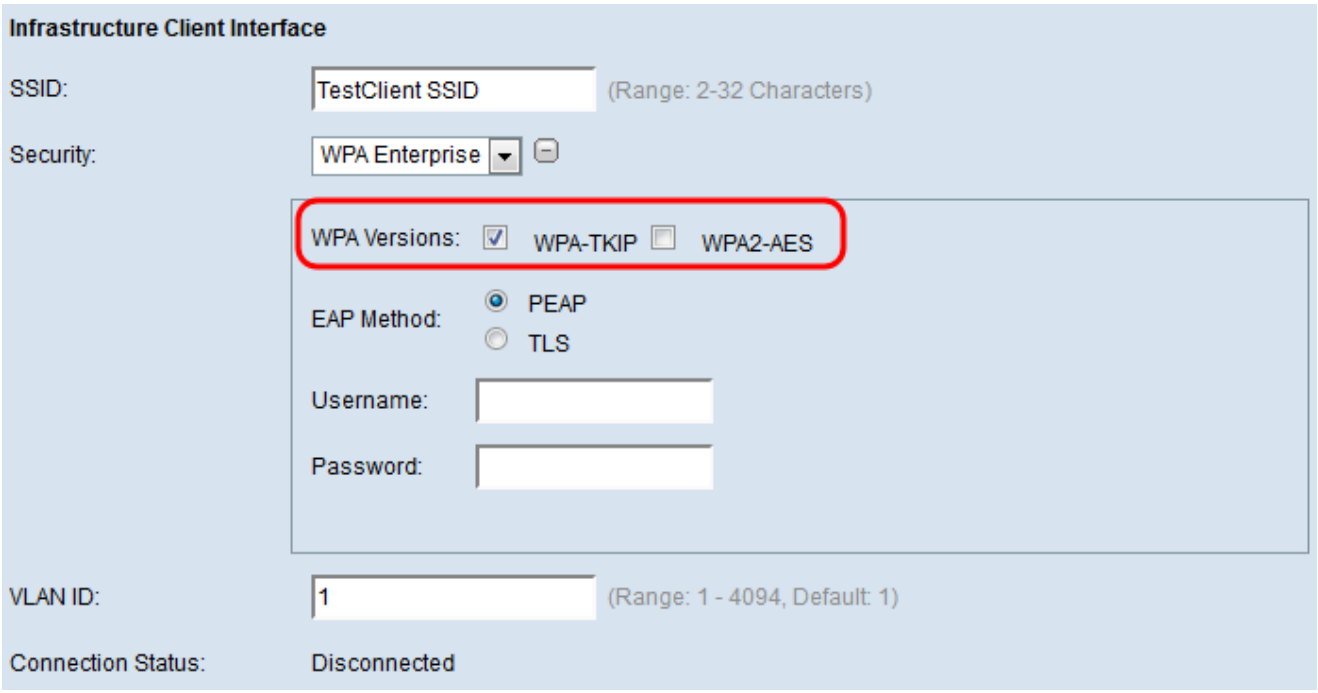


Paso 4. Introduzca la clave de encriptación WPA en el campo *Key*. La clave debe tener entre 8 y 63 caracteres. Saltar al Paso 14.

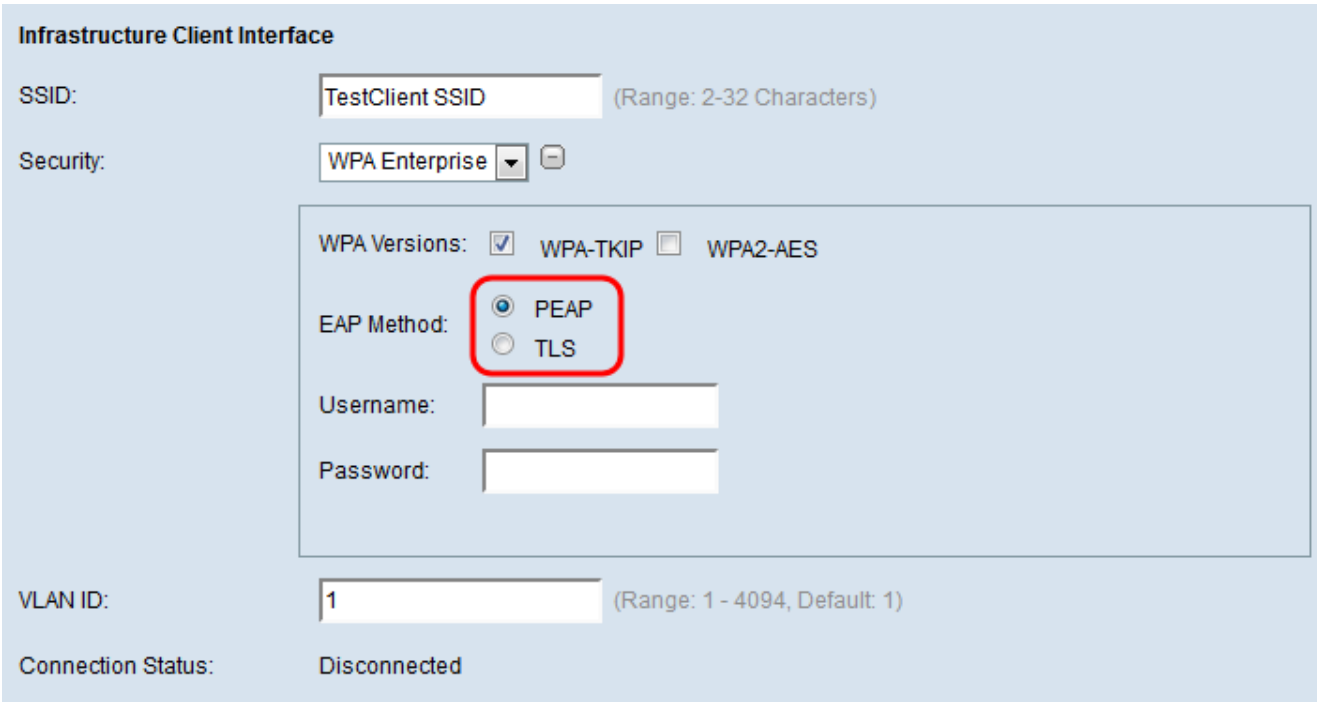


WPA Enterprise

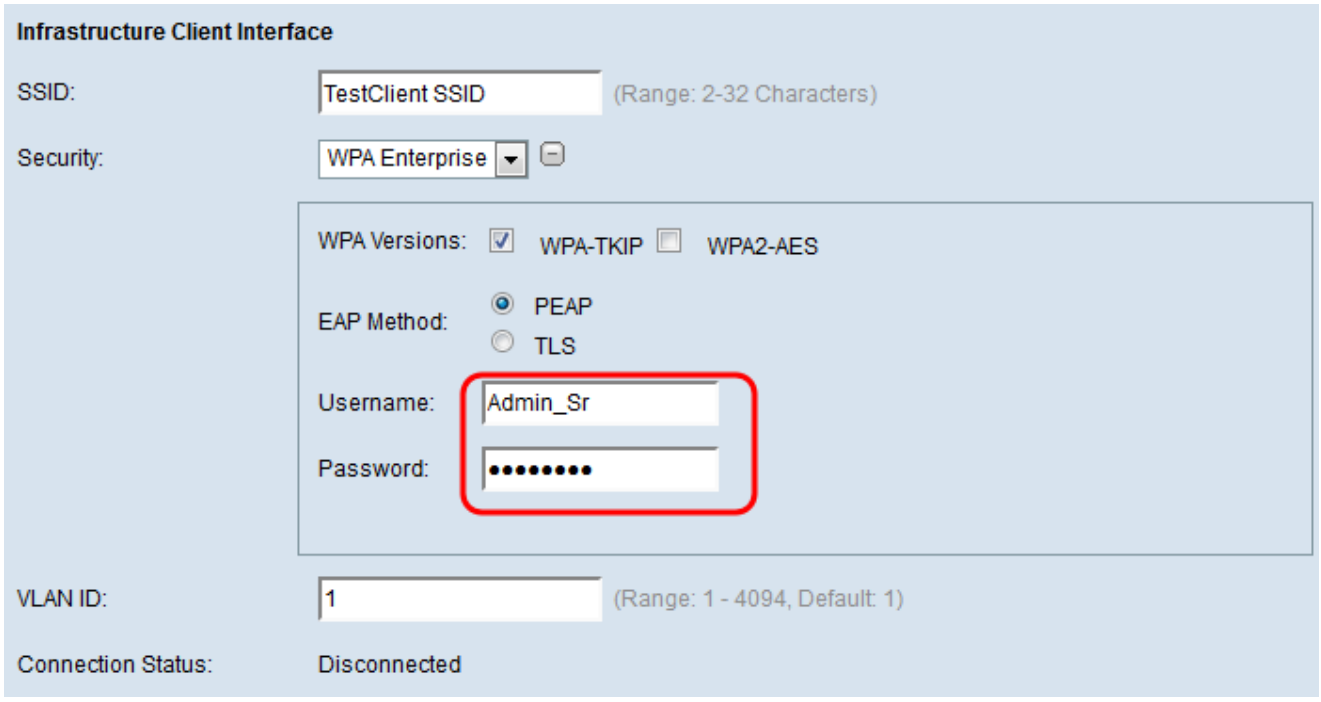
Paso 5. Seleccione la casilla de verificación **WPA-TKIP** o **WPA2-AES** para determinar qué tipo de encriptación WPA utilizará la interfaz cliente de infraestructura. Si todos los equipos inalámbricos admiten WPA2, configure la seguridad del cliente de infraestructura para WPA2-AES. Si algunos de los dispositivos inalámbricos sólo pueden conectarse con WPA-TKIP, active las casillas de verificación **WPA-TKIP** y **WPA2-AES**. En esta configuración, los dispositivos WPA2 se conectarán a WPA2 y los dispositivos WPA se conectarán a WPA.



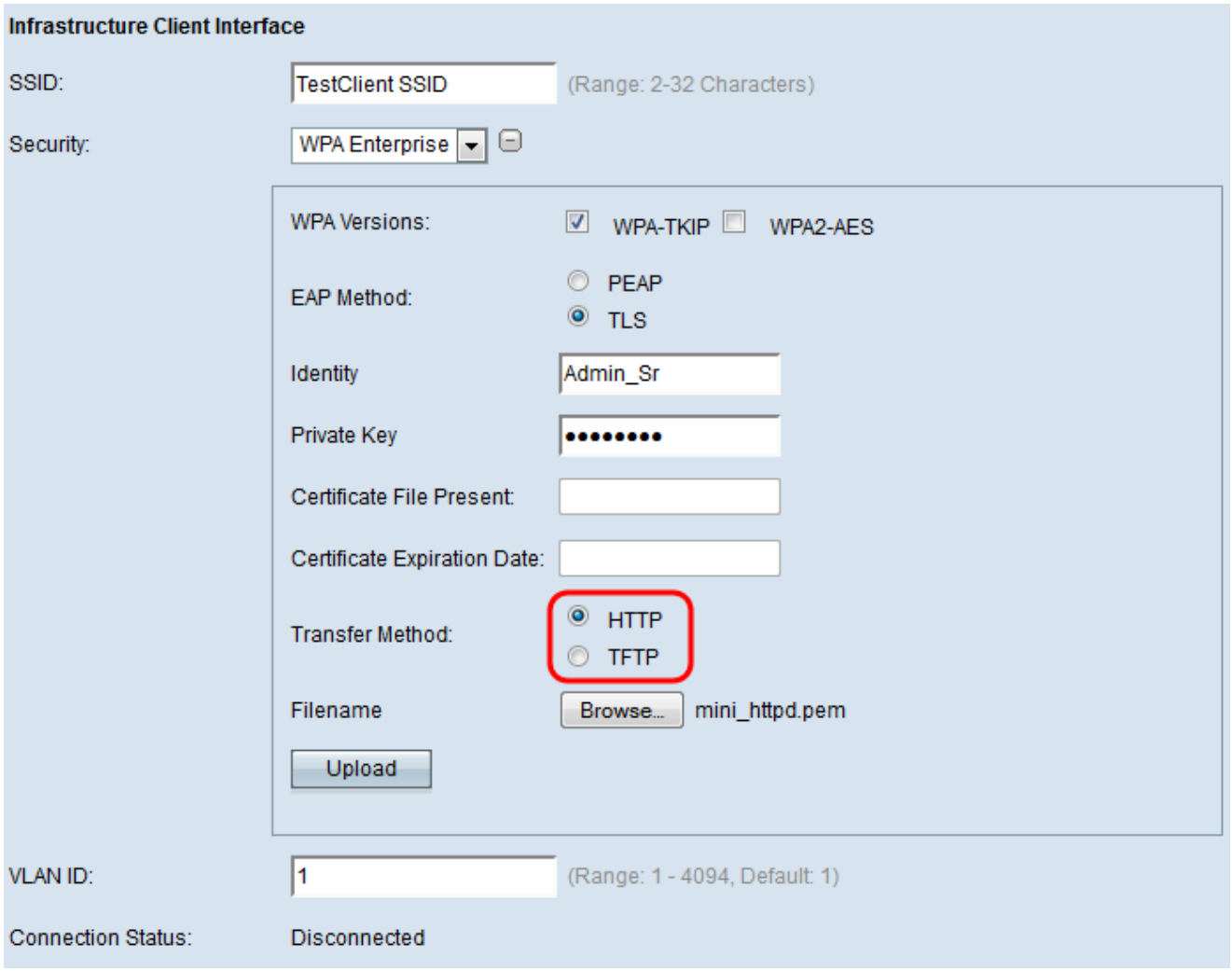
Paso 6. En el campo *EAP Method*, seleccione el botón de opción **PEAP** o **TLS**. El protocolo de autenticación extensible protegido (PEAP) proporciona a cada usuario inalámbrico los nombres de usuario y las contraseñas individuales WAP que admiten los estándares de encriptación AES. Transport Layer Security (TLS) requiere que cada usuario tenga un certificado adicional para que se le conceda acceso. Si selecciona PEAP, vaya directamente al Paso 14.



Paso 7. Ingrese el nombre de usuario y la contraseña en el campo *Nombre de usuario* y *Contraseña*.



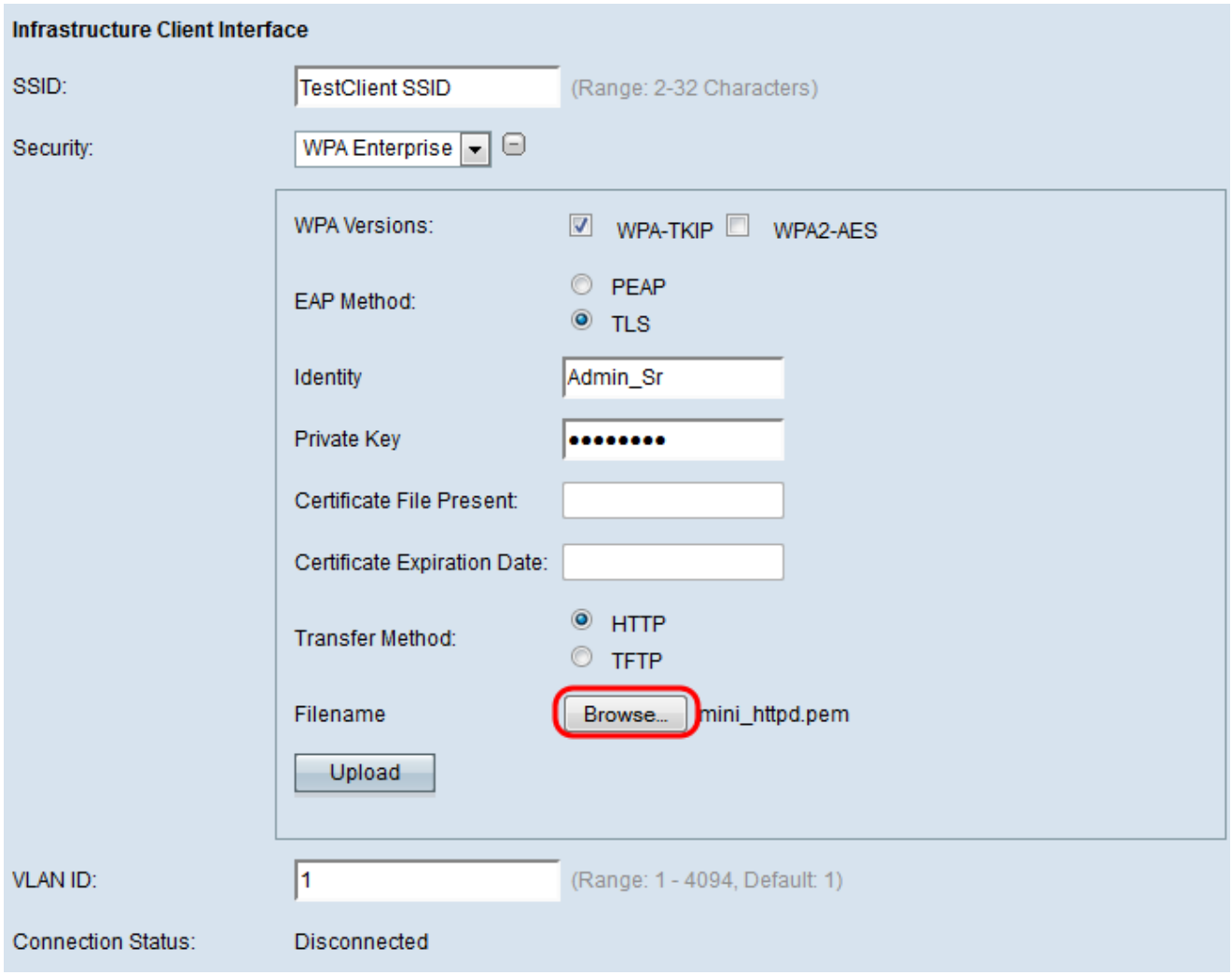
Paso 8. Seleccione los botones de radio **HTTP** o **TFTP** en el campo *Método de Transferencia*. El protocolo de transferencia de archivos trivial (TFTP) es una versión simplificada y no segura del protocolo de transferencia de archivos (FTP). Se utiliza principalmente para distribuir software o autenticar dispositivos entre redes corporativas. El protocolo de transferencia de hipertexto (HTTP) proporciona un marco de autenticación simple de respuesta a desafíos que puede utilizar un cliente para proporcionar un marco de autenticación. Si selecciona **TFTP**, vaya directamente al Paso 11.



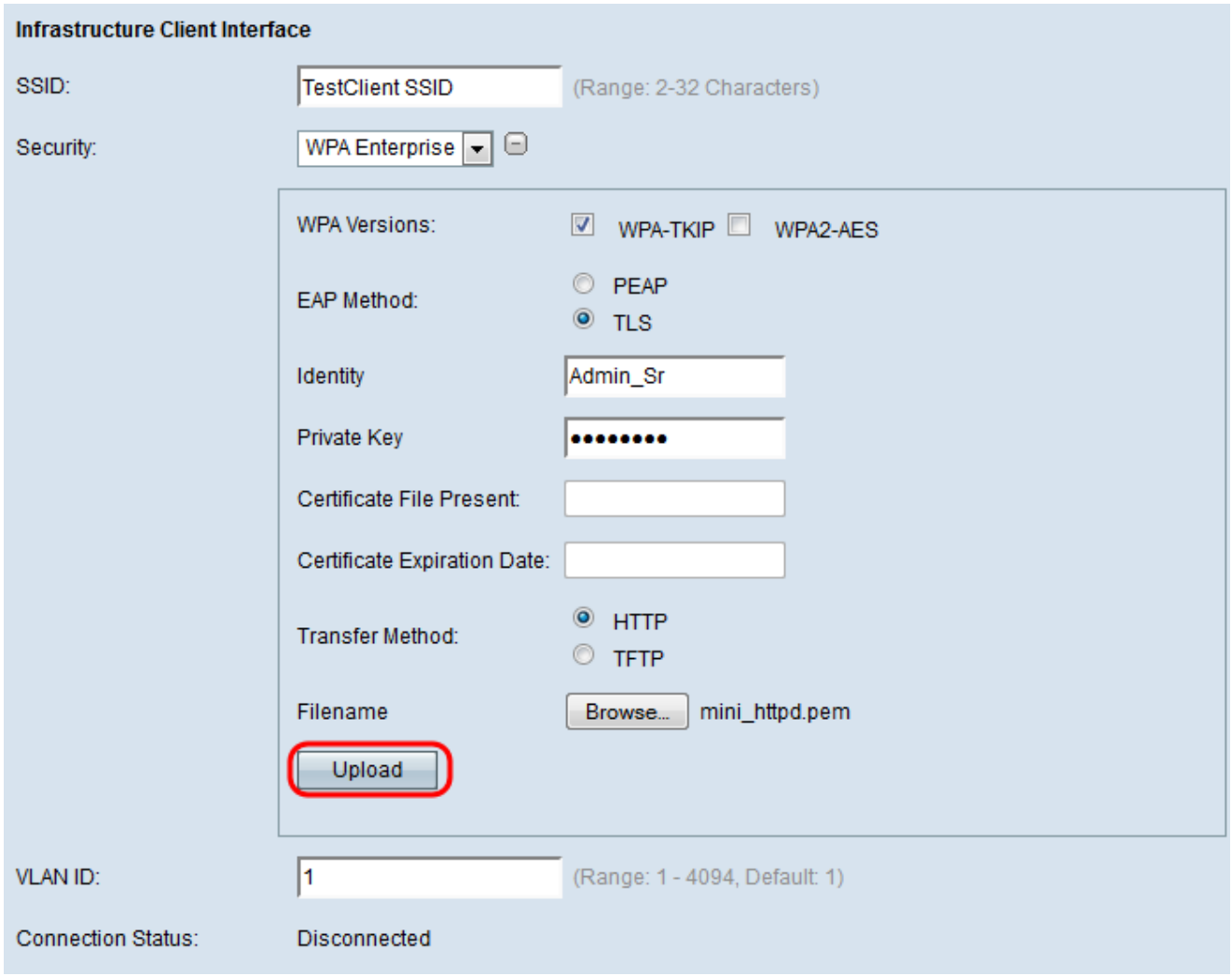
Nota: Si un archivo de certificado ya está presente en el WAP, el *campo Archivo de certificado presente* y *Fecha de vencimiento del certificado* ya se completará con la información pertinente. De lo contrario, estarán en blanco.

HTTP

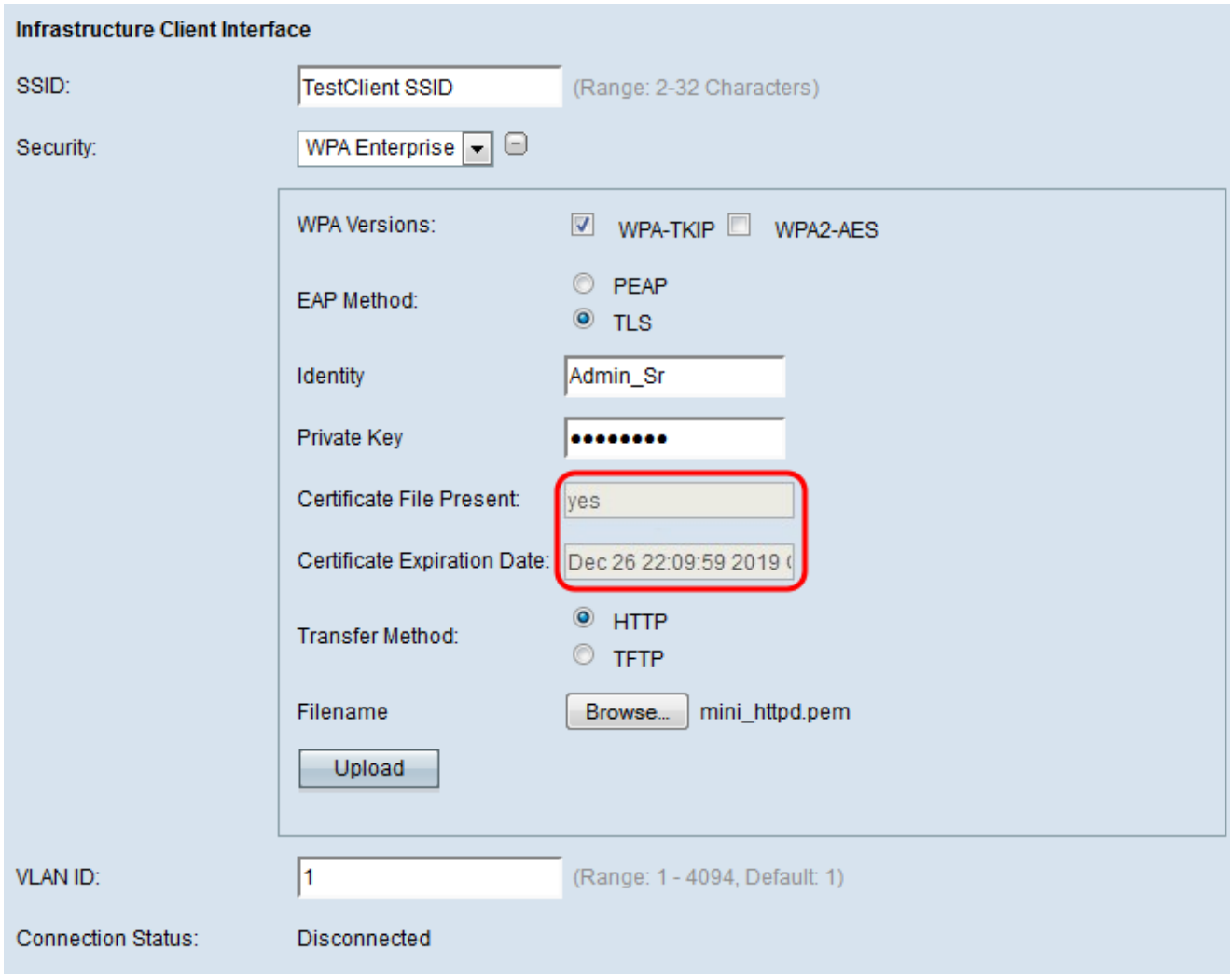
Paso 9. Haga clic en el botón **Examinar** para buscar y seleccionar un archivo de certificado. El archivo debe tener la extensión de archivo de certificado adecuada (como .pem o .pfx); de lo contrario, el archivo no se aceptará.



Paso 10. Haga clic en **Cargar** para cargar el archivo de certificado seleccionado. Saltar al Paso 14.

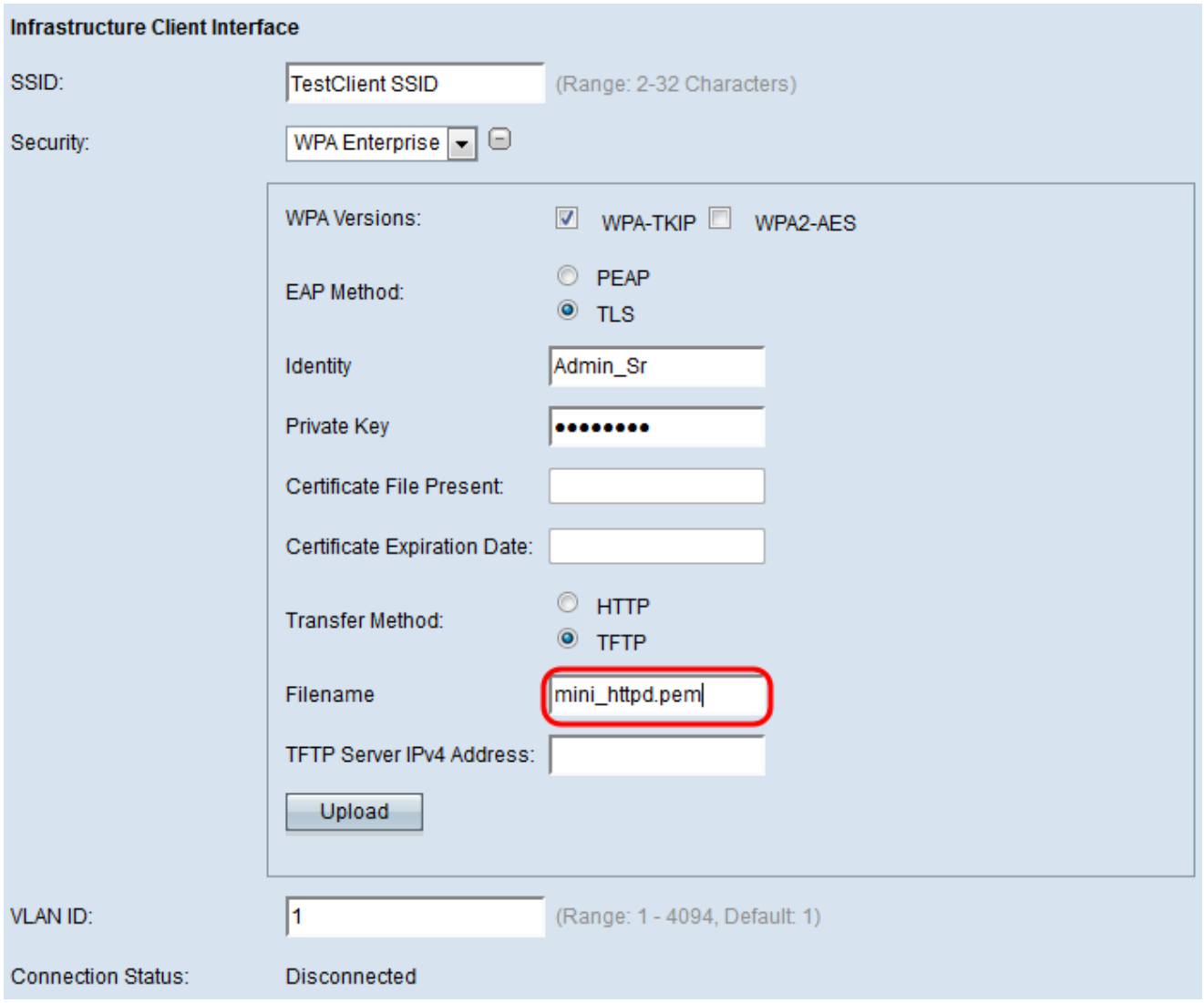


Los campos *Archivo de certificado presente* y *Fecha de vencimiento del certificado* se actualizarán automáticamente.

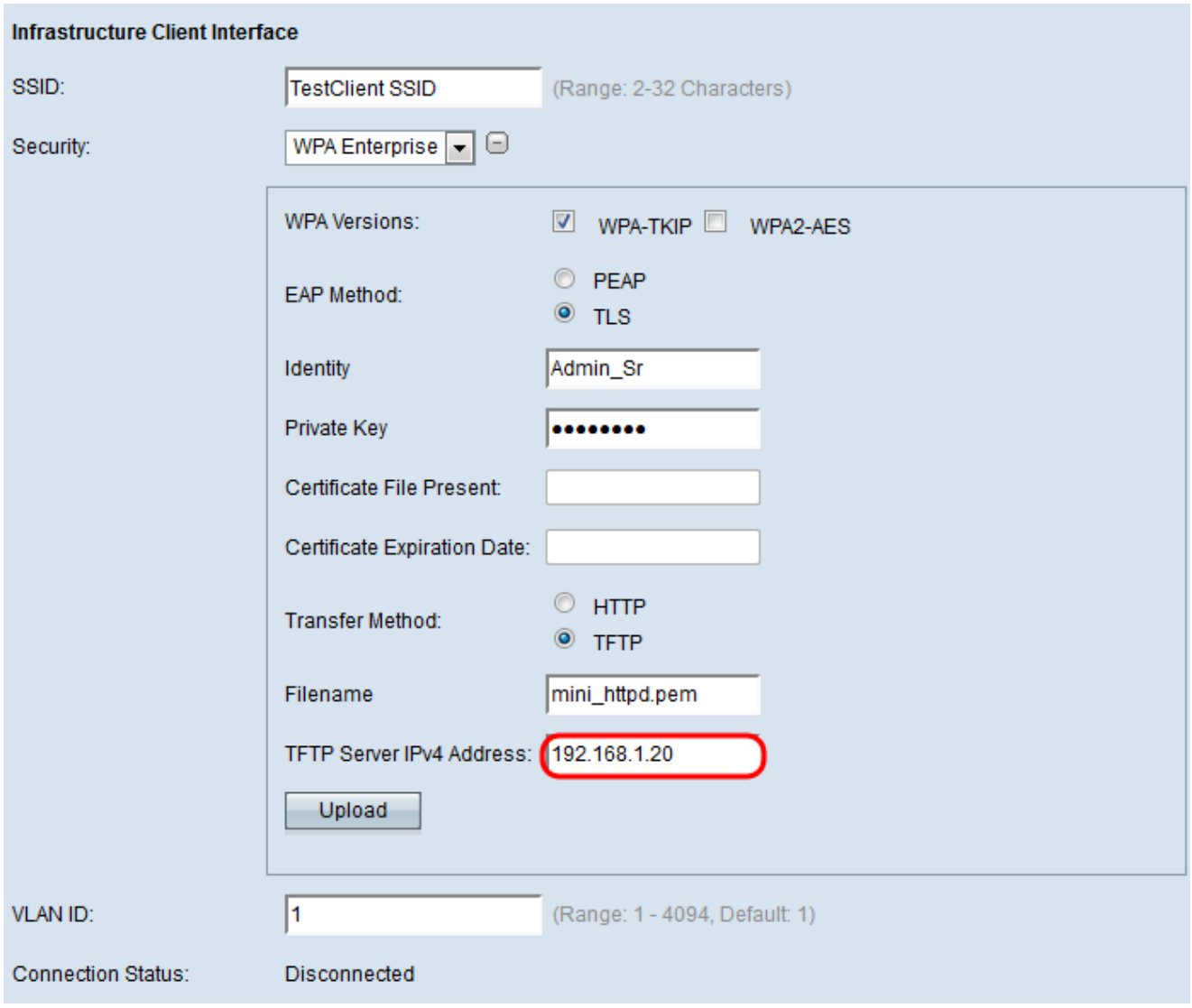


TFTP

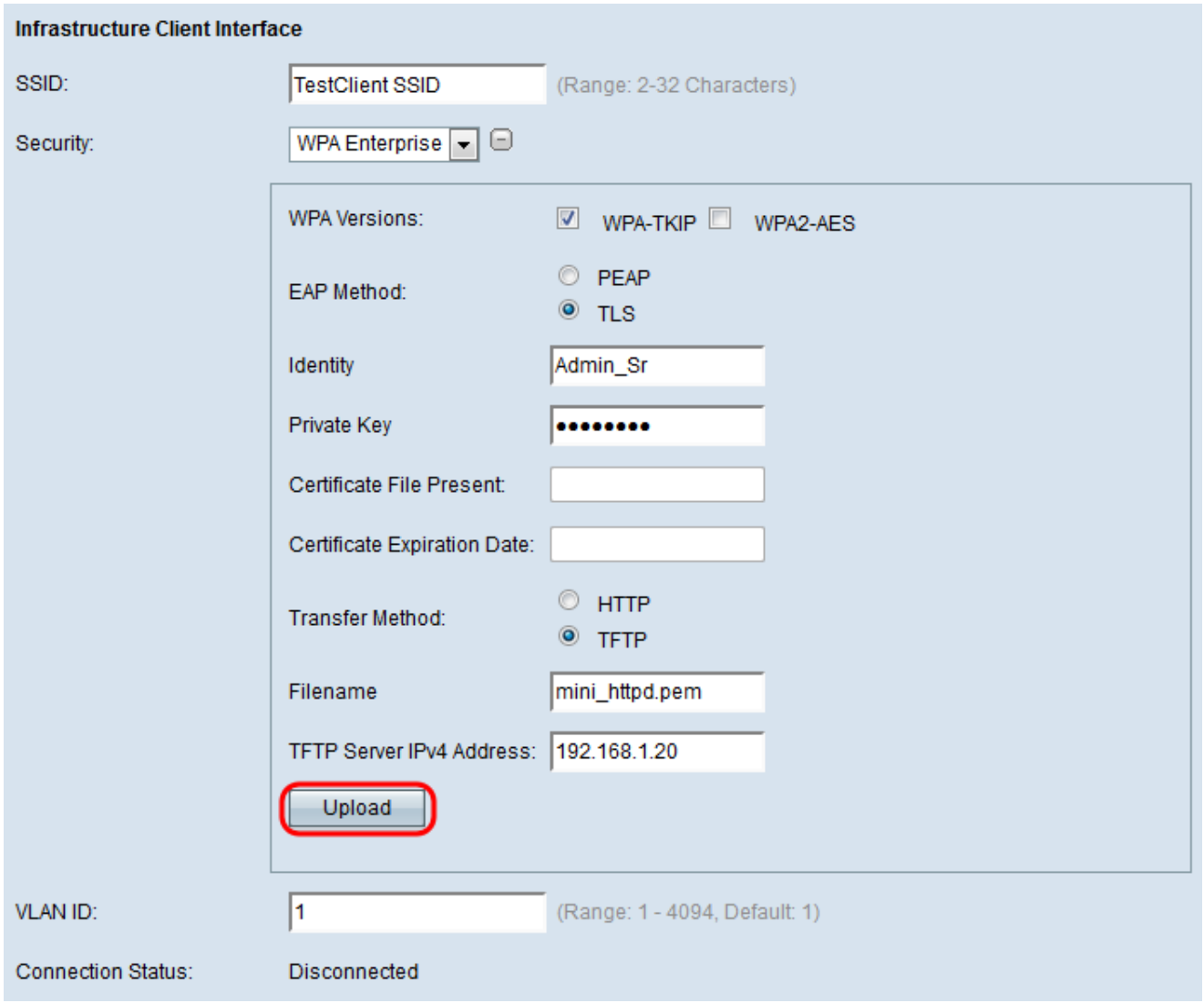
Paso 11. Introduzca el nombre del archivo del certificado en el campo *Nombre de archivo*.



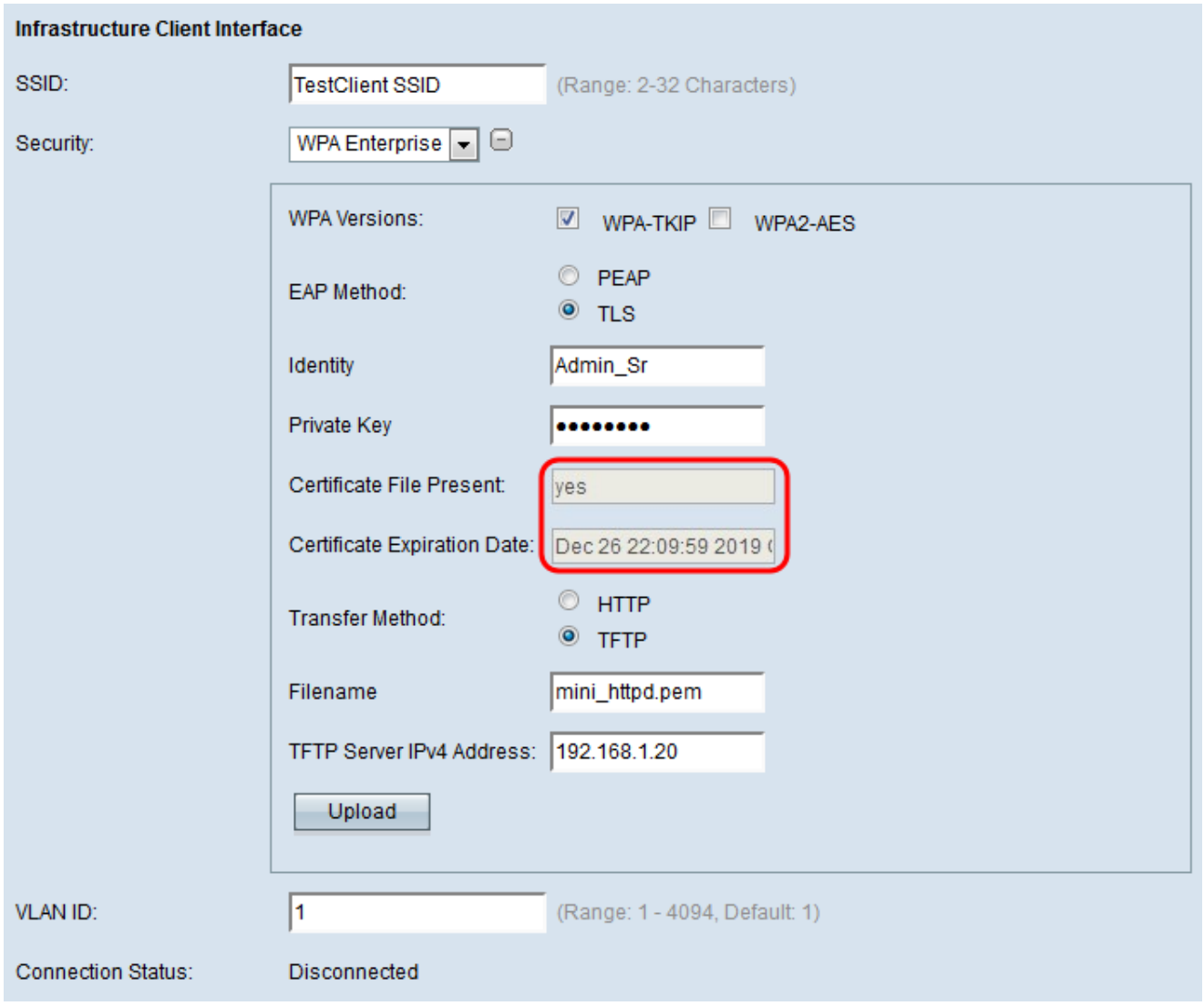
Paso 12. Ingrese la dirección del servidor TFTP en el campo *TFTP Server IPv4 Address* .



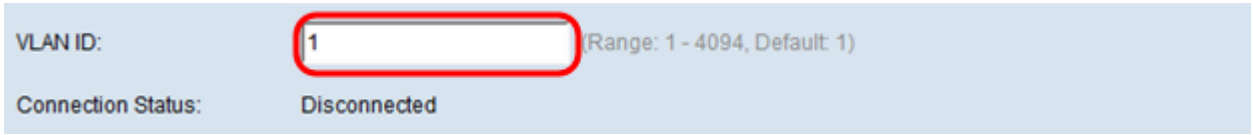
Paso 13. Haga clic en el botón **Cargar** para cargar el archivo de certificado especificado.



El *archivo de certificado presente* y el campo *Fecha de vencimiento del certificado* se actualizarán automáticamente.

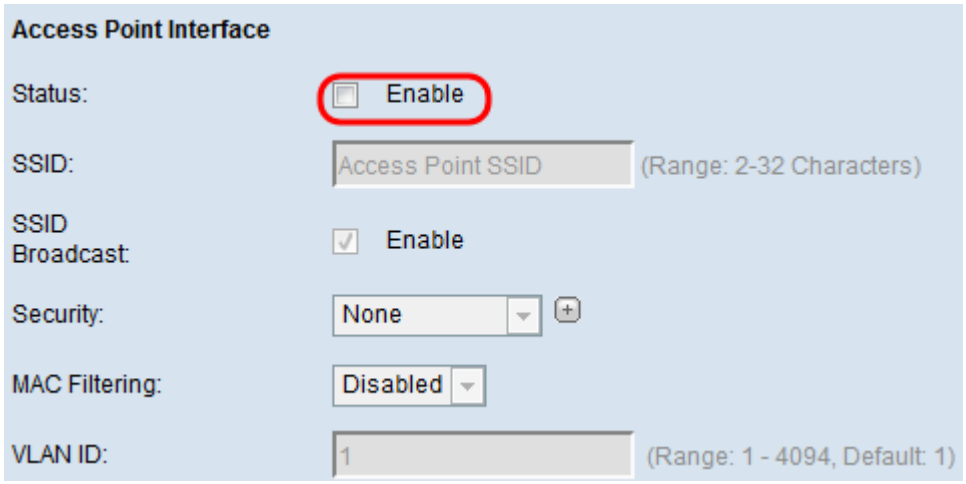


Paso 14. Introduzca el ID de VLAN para la interfaz de cliente de infraestructura.

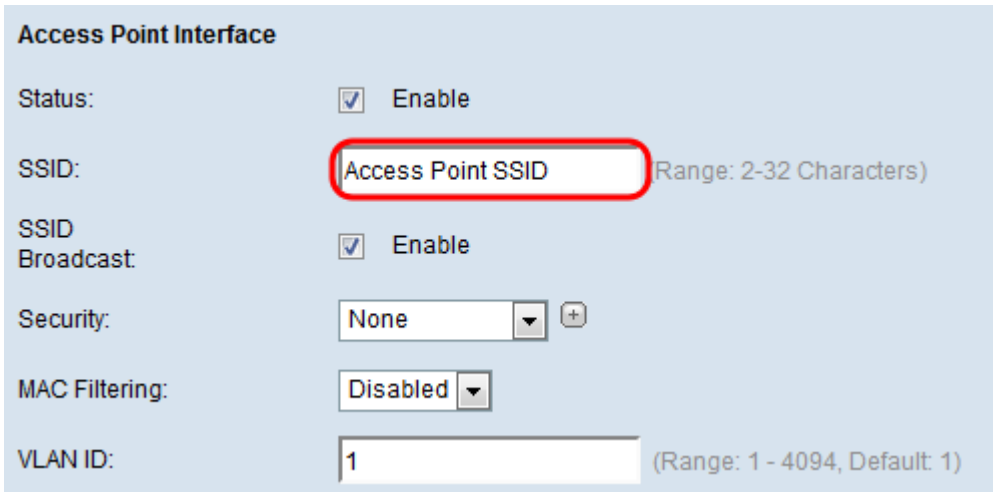


Interfaz del punto de acceso

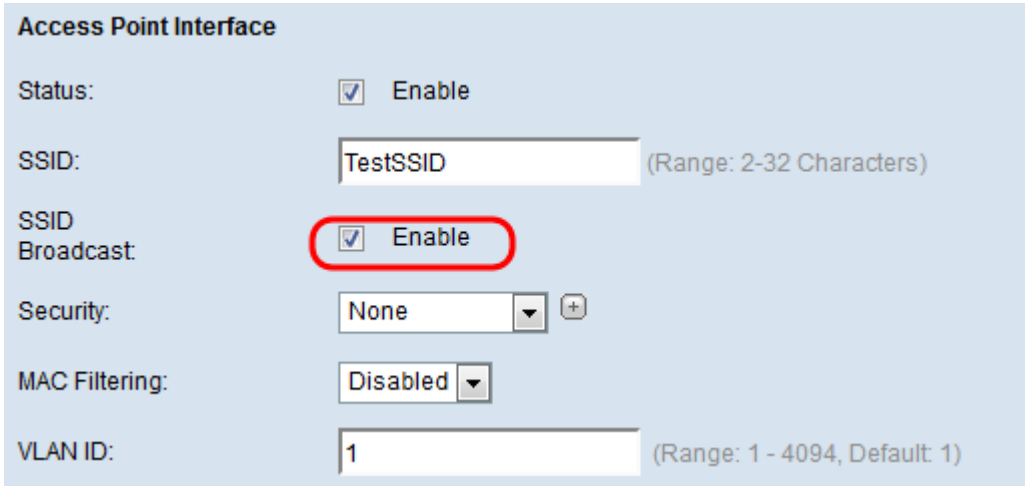
Paso 1. Marque la casilla **Enable** en el campo *Status* para habilitar el bridging en la interfaz del punto de acceso.



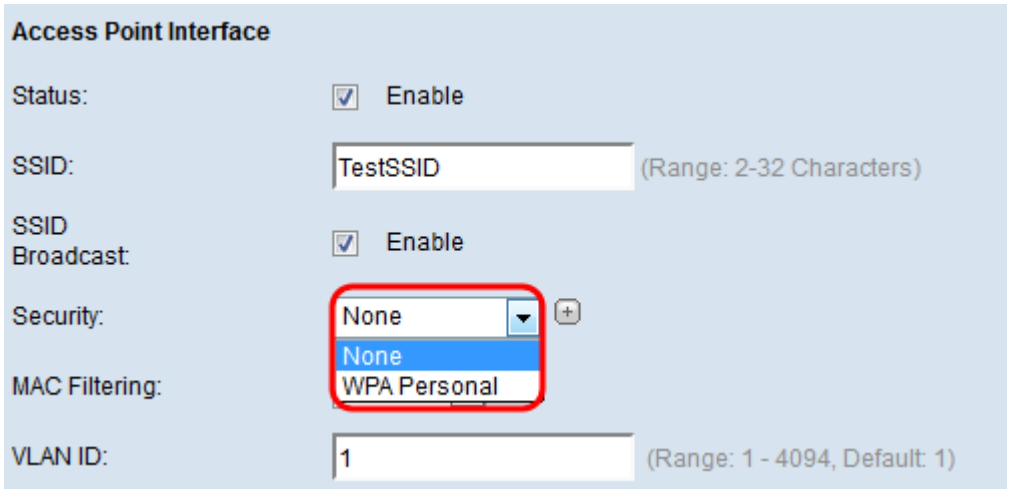
Paso 2. Introduzca el identificador del conjunto de servicios (SSID) para el punto de acceso en el campo *SSID*. La longitud de SSID debe estar entre 2 y 32 caracteres.



Paso 3. (Opcional) Si no desea difundir el SSID de flujo descendente, desmarque la casilla de verificación **Enable** en el campo SSID Broadcast. Está habilitado de forma predeterminada.



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

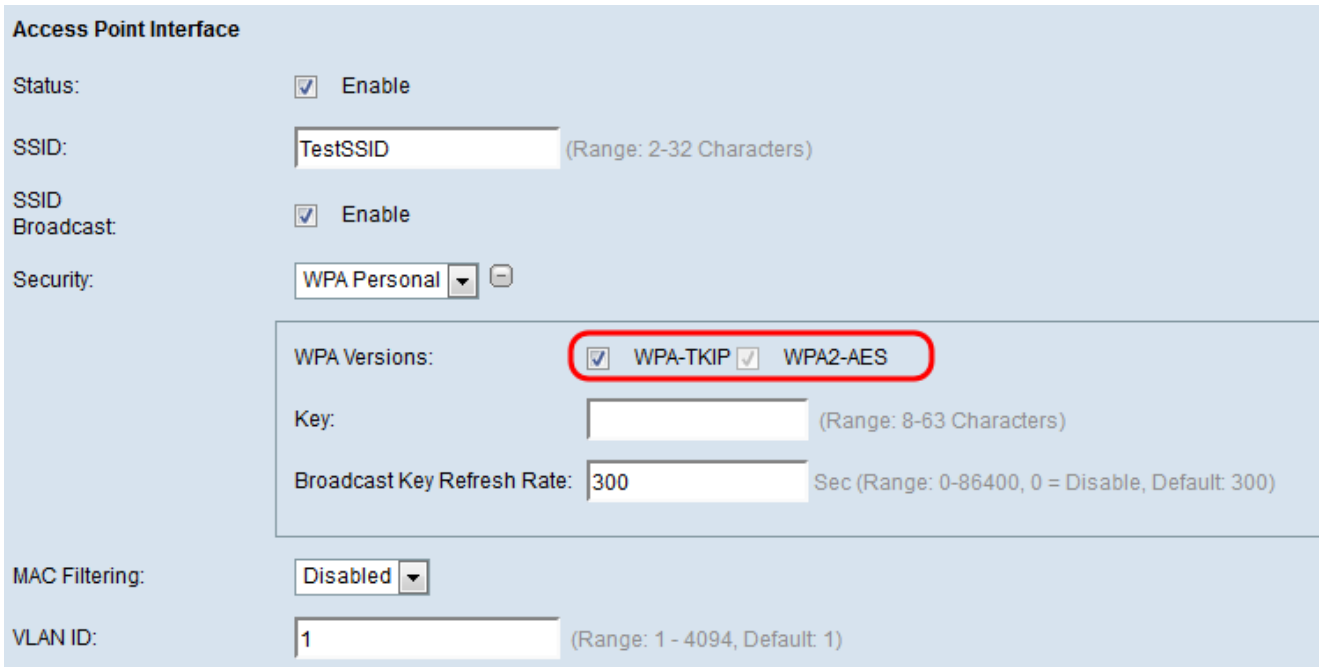


Las opciones disponibles se definen de la siguiente manera:

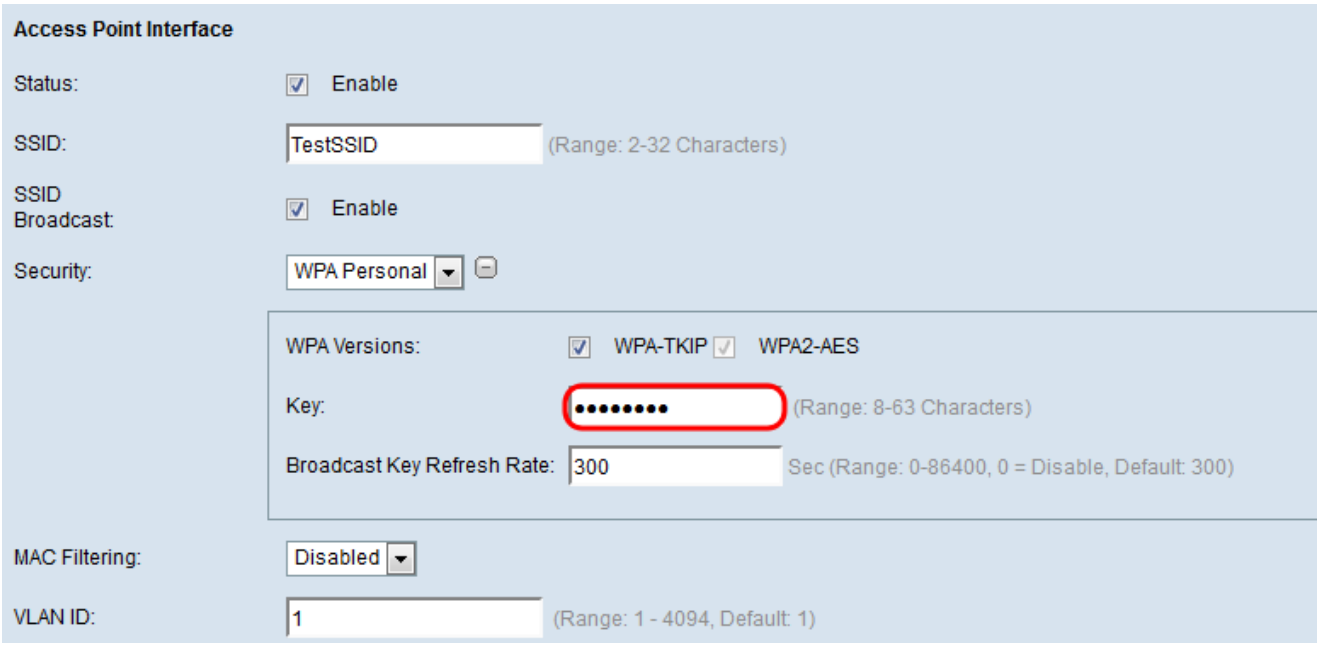
·Ninguno: abierto o sin seguridad. Este es el valor predeterminado. Vaya al Paso 10 si lo elige.

·WPA Personal: WPA Personal y admite claves de entre 8 y 63 caracteres. El método de encriptación es el protocolo de integridad de clave temporal (TKIP) o el modo cifrado de contador con protocolo de código de autenticación de mensaje de encadenamiento de bloques (CCMP). Se recomienda utilizar WPA2 con CCMP, ya que cuenta con un estándar de encriptación más potente, el estándar de encriptación avanzado (AES), en comparación con el TKIP, que solo utiliza un estándar RC4 de 64 bits.

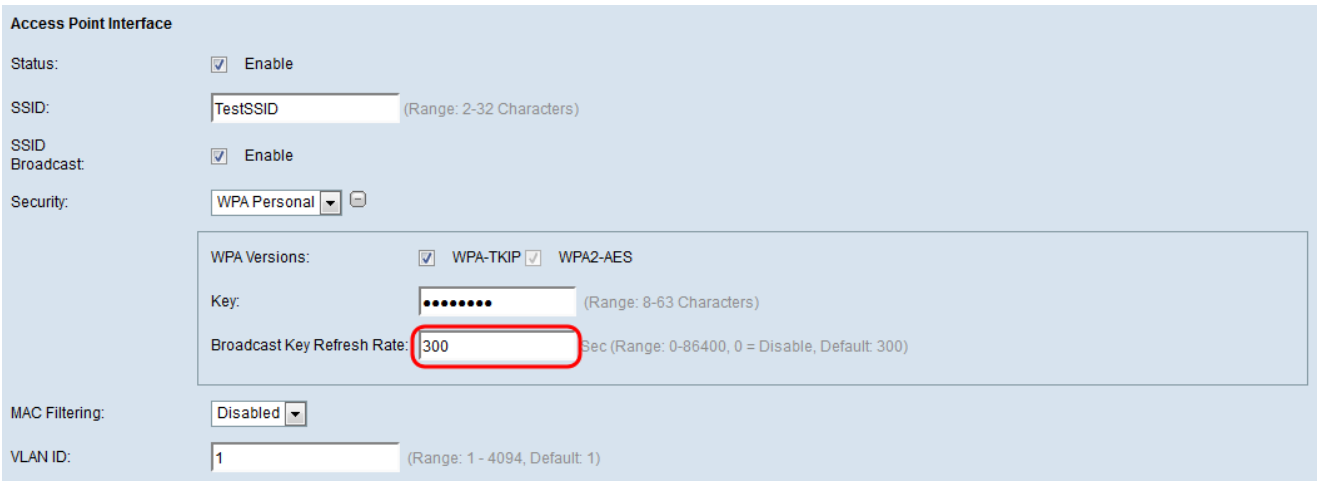
Paso 5. Compruebe las versiones WPA deseadas desde el campo *Versiones WPA*. Normalmente, WPA sólo se elige si algunos de los WAP involucrados no admiten WPA2; de lo contrario, se recomienda WPA2. WPA2-AES siempre está habilitado.



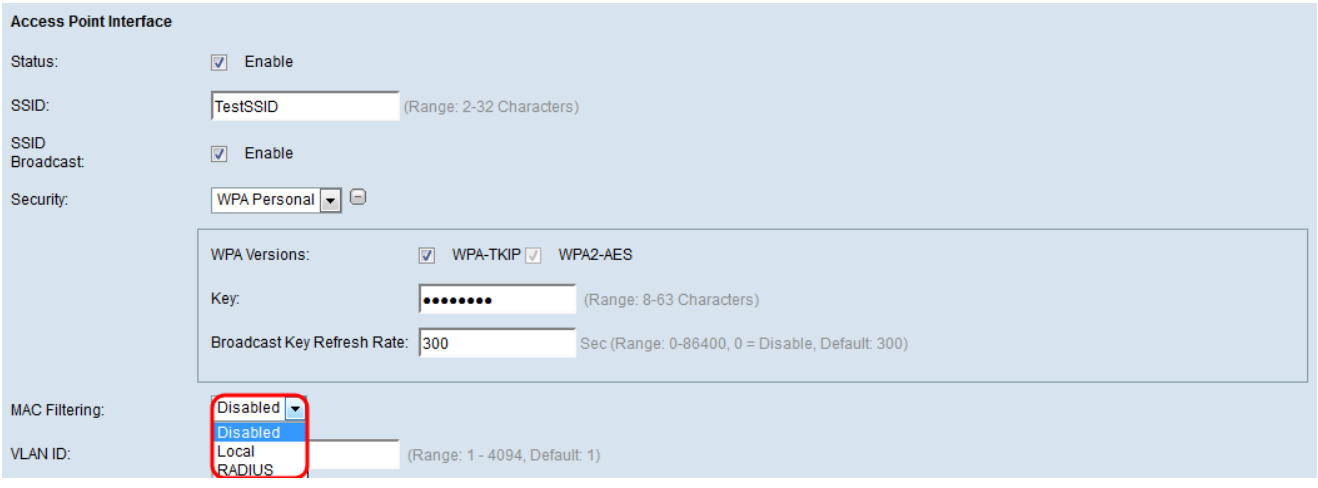
Paso 6. Introduzca la clave WPA compartida en el campo *Key*. La clave debe tener entre 8 y 63 caracteres y puede incluir caracteres alfanuméricos, mayúsculas y minúsculas y caracteres especiales.



Paso 7. Introduzca la velocidad en la *Velocidad de actualización de la clave de difusión*. 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.



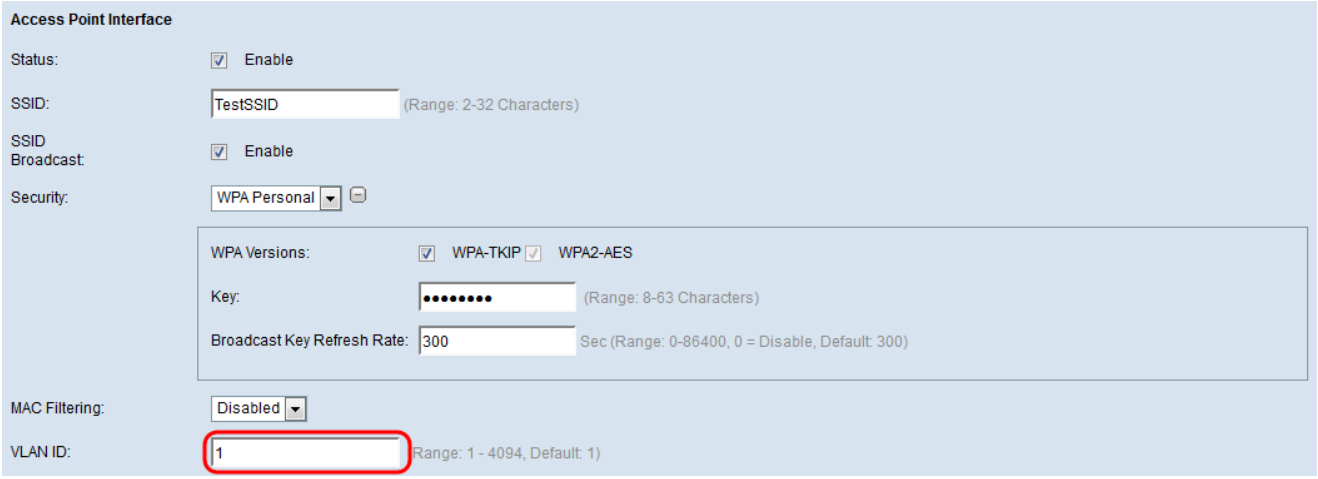
Las opciones disponibles se definen de la siguiente manera:

·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.

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



Nota: Para permitir el bridging de paquetes, la configuración de VLAN para la interfaz de punto de acceso y la interfaz cableada debe coincidir con la de la interfaz de cliente de infraestructura.

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

WorkGroup Bridge Mode: Enable

Radio Setting Per Interface

Select the radio interface first, and then enter the configuration parameters.

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

Infrastructure Client Interface

SSID: TestClient SSID (Range: 2-32 Characters)

Security: WPA Personal

VLAN ID: 1 (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Access Point Interface

Status: Enable

SSID: TestSSID (Range: 2-32 Characters)

SSID Broadcast: Enable

Security: WPA Personal

MAC Filtering: Disabled

VLAN ID: 1 (Range: 1 - 4094, Default: 1)

Save