Configuración de los parámetros de seguridad inalámbrica en un WAP

Introducción

La configuración de la seguridad inalámbrica en el punto de acceso inalámbrico (WAP) es muy esencial para proteger la red inalámbrica de los intrusos que puedan poner en peligro la privacidad de los dispositivos inalámbricos, así como la transmisión de datos a través de la red inalámbrica. Puede configurar la seguridad inalámbrica en la red inalámbrica mediante la configuración de MAC Filter (Filtro de MAC), Wi-Fi Protected Access (WPA/WPA2) Personal y WPA/WPA2 Enterprise.

El filtrado de MAC se utiliza para filtrar los clientes inalámbricos para acceder a la red mediante sus direcciones MAC. Se configurará una lista de clientes para permitir o bloquear las direcciones de la lista para acceder a la red, según sus preferencias. Para obtener más información sobre el filtrado de MAC, haga clic aquí.

WPA/WPA2 Personal y WPA/WPA2 Enterprise son protocolos de seguridad utilizados para proteger la privacidad mediante el cifrado de los datos transmitidos a través de la red inalámbrica. WPA/WPA2 es compatible con los estándares IEEE 802.11E y 802.11i. En comparación con el protocolo de seguridad de privacidad equivalente a conexión con cables (WEP), WPA/WPA2 han mejorado las funciones de autenticación y cifrado.

WPA/WPA2 Personal es para uso doméstico y WPA/WPA2 Enterprise es para redes a escala empresarial. WPA/WPA2 Enterprise proporciona mayor seguridad y control centralizado de la red en comparación con WPA/WPA2 Personal.

En esta situación, la seguridad inalámbrica se configurará en el WAP para proteger la red de intrusos mediante los parámetros WPA/WPA2 Personal y Enterprise.

Objetivo

En este artículo se explica cómo configurar los protocolos de seguridad WPA/WPA2 Personal y Enterprise para mejorar la seguridad y la privacidad de la red inalámbrica.

Nota: En este artículo se supone que ya se ha creado un identificador de conjunto de servicios (SSID) o una red de área local inalámbrica (WLAN) en el WAP.

Dispositivos aplicables

- Serie WAP100
- Serie WAP300
- Serie WAP500

Versión del software

- 1.0.2.14 - WAP131, WAP351
- 1.0.6.5 - WAP121, WAP321
- 1.3.0.4 - WAP371

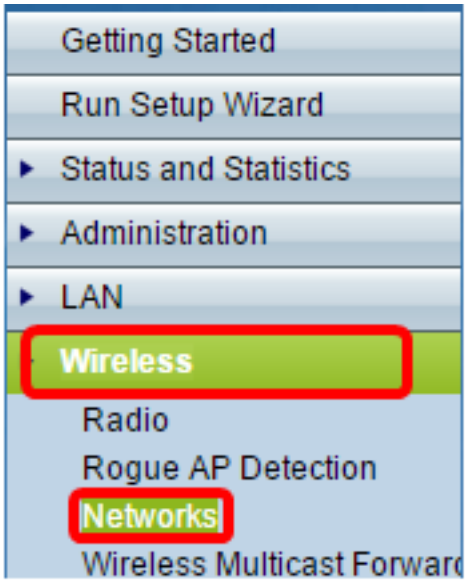
- 1.1.0.7 - WAP150, WAP361
- 1.2.1.5 - WAP551, WAP561
- 1.0.1.11 - WAP571, WAP571E

Configuración de los parámetros de seguridad inalámbrica

Configuración de WPA/WPA2 Personal

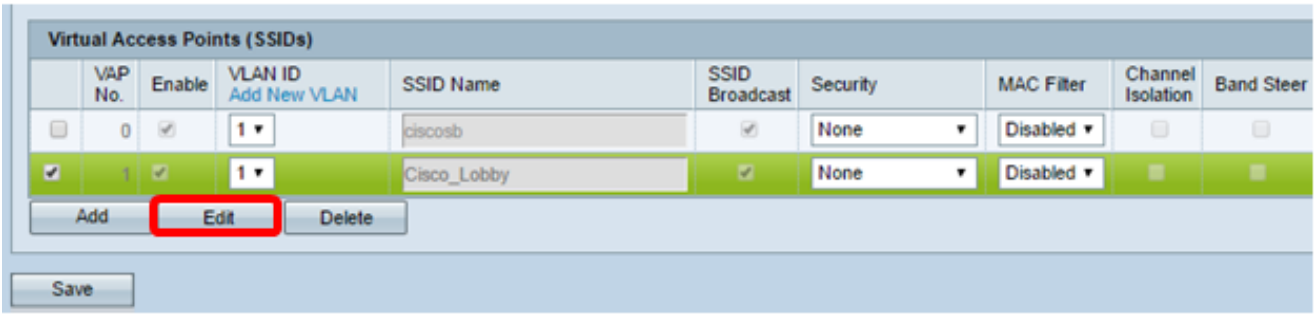
Paso 1. Inicie sesión en la utilidad basada en web de su punto de acceso y elija **Wireless > Networks**.

Nota: En la siguiente imagen, se utiliza como ejemplo la utilidad basada en Web del dispositivo WAP361. Las opciones de menú pueden variar en función del modelo del dispositivo.

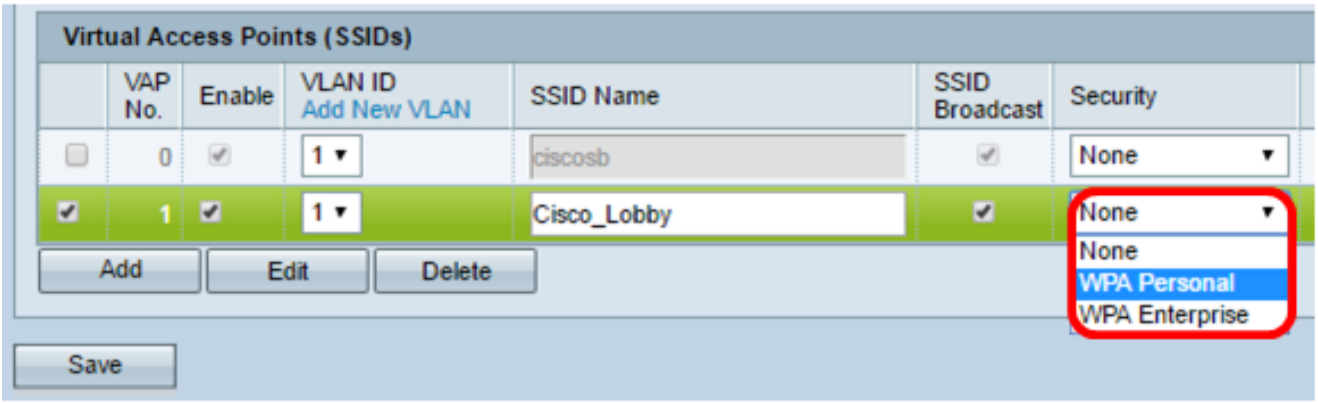


Paso 2. En el área Puntos de acceso virtuales (SSID), active la casilla de verificación del SSID que desea configurar y haga clic en **Editar**.

Nota: En este ejemplo, se elige VAP1.



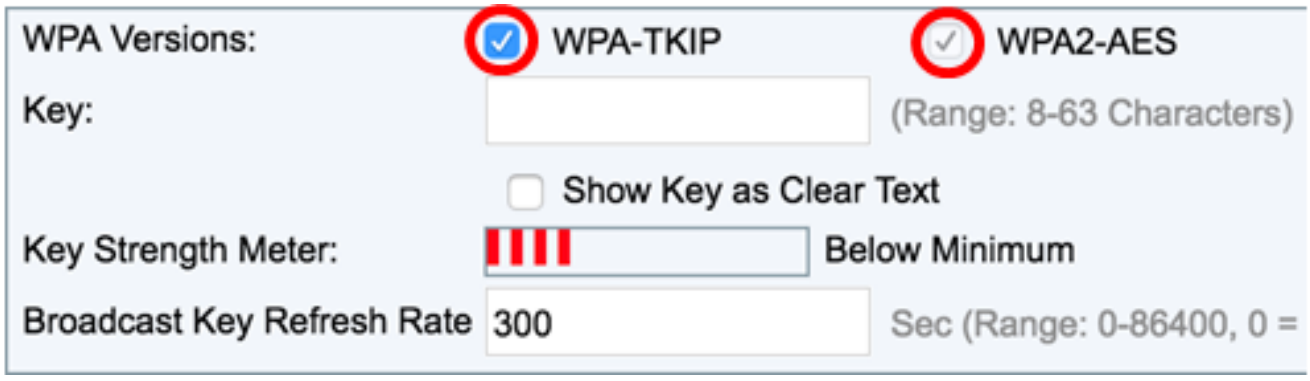
Paso 3. Haga clic en **WPA Personal** en la lista desplegable Seguridad.



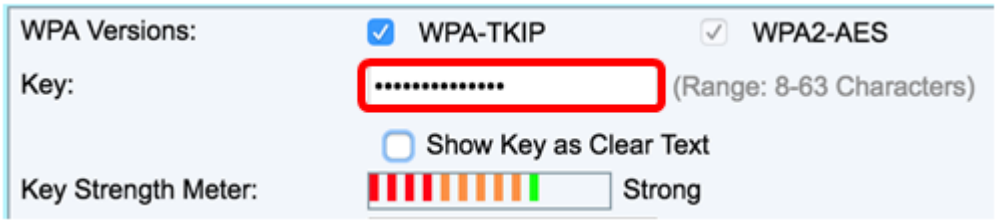
Paso 4. Seleccione la versión WPA (WPA-TKIP o WPA2-AES) activando la casilla de verificación. Se pueden elegir dos a la vez.

- WPA-TKIP: Wi-Fi Protected Access-Temporal Key Integrity Tool. La red tiene algunas estaciones cliente que sólo admiten el protocolo de seguridad WPA y TKIP original. Tenga en cuenta que no se permite elegir solo WPA-TKIP para el punto de acceso según el último requisito de Wi-Fi Alliance.
- WPA2-AES: Wi-Fi Protected Access - Estándar de cifrado avanzado. Todas las estaciones cliente de la red admiten WPA2 y AES-CCMP cifrado/protocolo de seguridad. Esta versión de WPA proporciona la mejor seguridad según el estándar IEEE 802.11i. Según el último requisito de Wi-Fi Alliance, el WAP debe soportar este modo todo el tiempo.

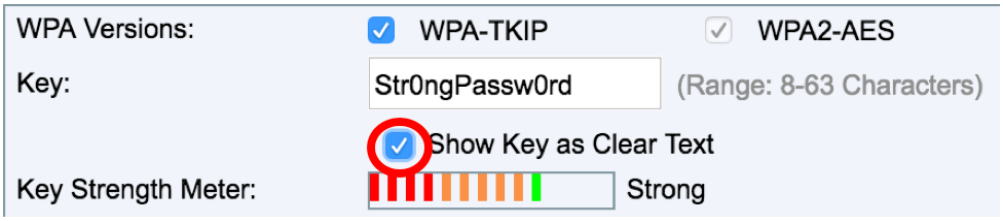
Nota: En este ejemplo, ambas casillas de verificación están marcadas.



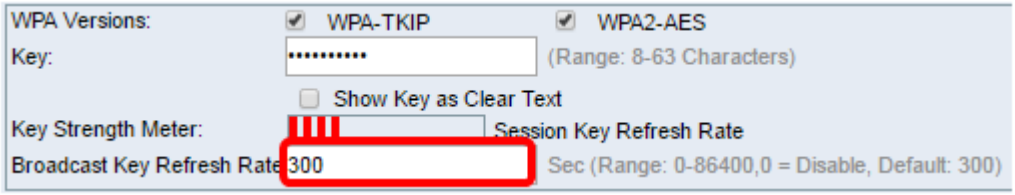
Paso 5. Cree una contraseña que contenga entre 8 y 63 caracteres e introdúzcala en el campo *Key*.



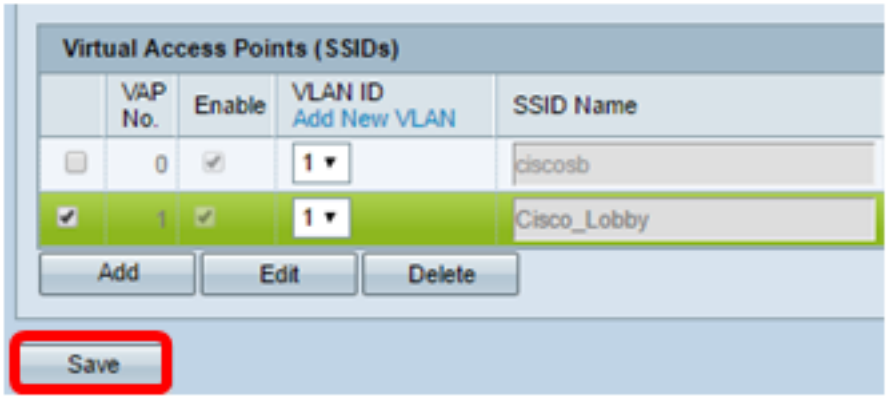
Nota: Puede marcar el cuadro **Mostrar clave como texto sin cifrar** para mostrar la contraseña que ha creado.



Paso 6. (Opcional) En el campo *Velocidad de actualización de clave de difusión*, introduzca un valor o el intervalo en el que se actualiza la clave de difusión (grupo) para los clientes asociados a este VAP. El valor predeterminado es 300 segundos y el intervalo válido es de 0 a 86400 segundos. Un valor de 0 indica que la clave de difusión no se actualiza.



Paso 7. Click Save.

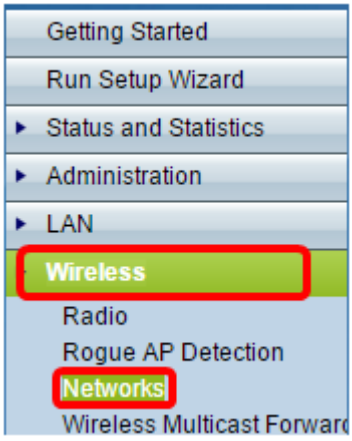


Ahora ha configurado WPA Personal en su WAP.

Configuración de WPA/WPA2 Enterprise

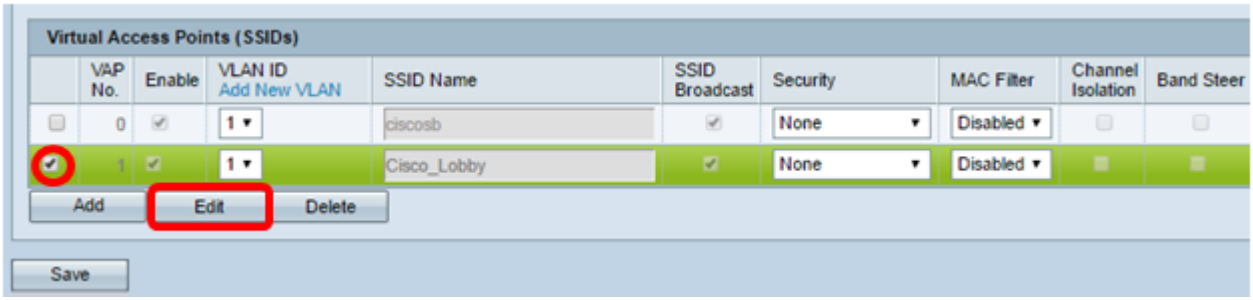
Paso 1. Inicie sesión en la utilidad basada en web de su punto de acceso y elija **Wireless > Networks**.

Nota: En la siguiente imagen, se utiliza como ejemplo la utilidad basada en Web del dispositivo WAP361.

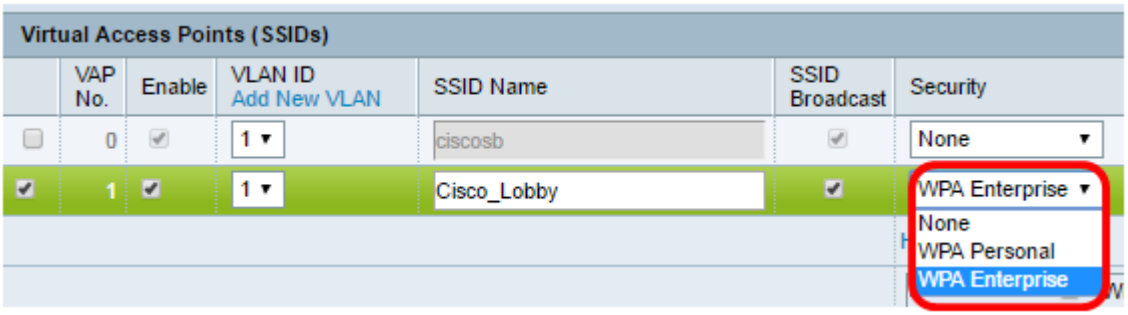


Paso 2. En el área Puntos de acceso virtuales (SSID), verifique el SSID que desea

configurar y haga clic en el botón **Editar** debajo.



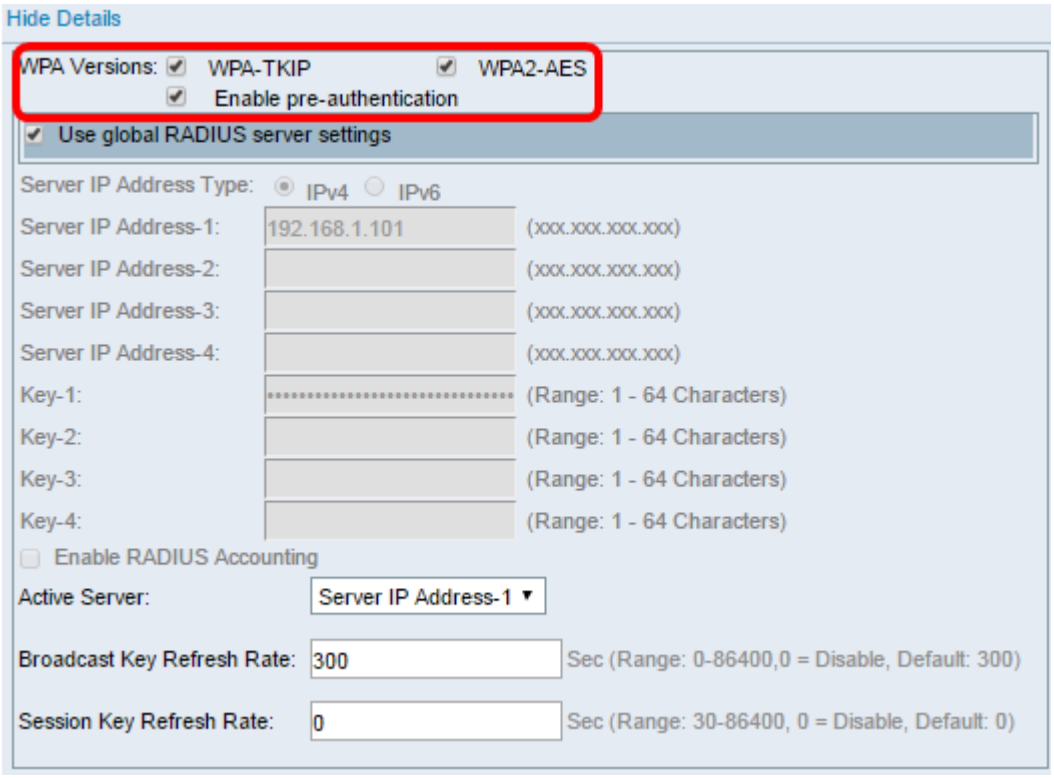
Paso 3. Elija **WPA Enterprise** en la lista desplegable Seguridad.



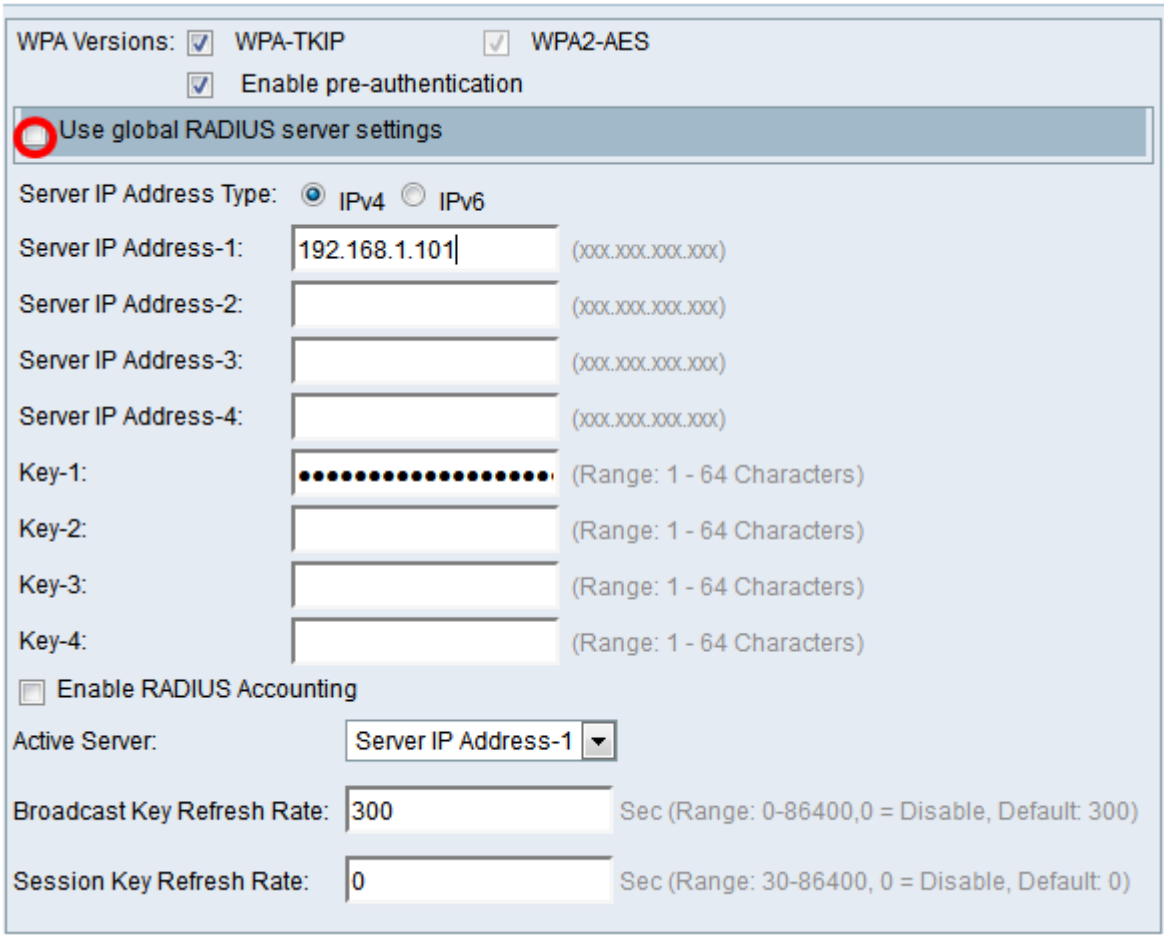
Paso 4. Elija la versión WPA (WPA-TKIP, WPA2-AES y Enable pre-authentication).

- Habilitar la autenticación previa: si elige WPA2-AES solamente o WPA-TKIP y WPA2-AES como versión WPA, puede habilitar la autenticación previa para los clientes WPA2-AES. Marque esta opción si desea que los clientes inalámbricos WPA2 envíen los paquetes de autenticación previa. La información de autenticación previa se retransmite desde el dispositivo WAP que el cliente está utilizando actualmente al dispositivo WAP de destino. La activación de esta función puede ayudar a acelerar la autenticación de los clientes de roaming que se conectan a varios puntos de acceso (AP).

Nota: Esta opción no se aplica si ha seleccionado WPA-TKIP para las versiones WPA porque el WPA original no admite esta función.

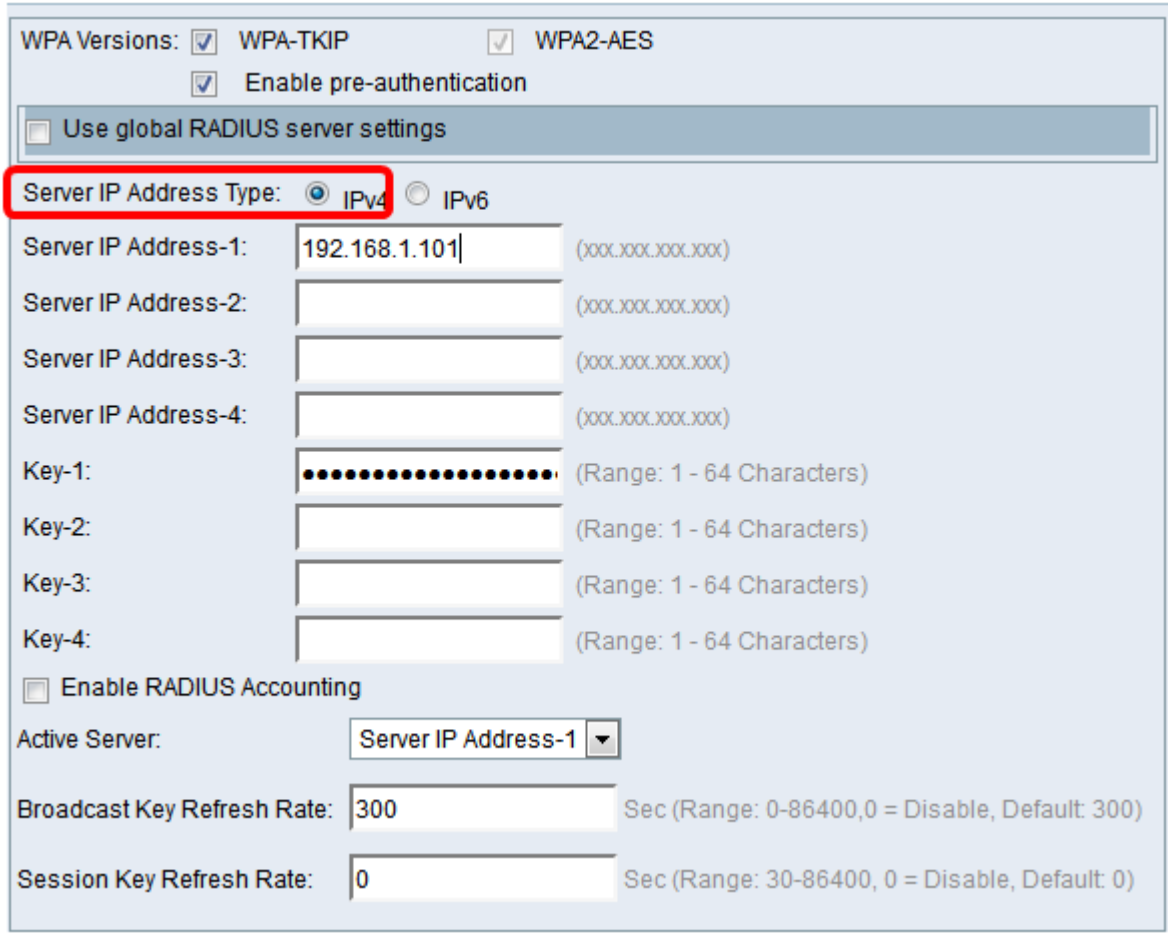


Paso 5. (Opcional) Desmarque la casilla de verificación **Usar configuración global del servidor RADIUS** para editar la configuración.



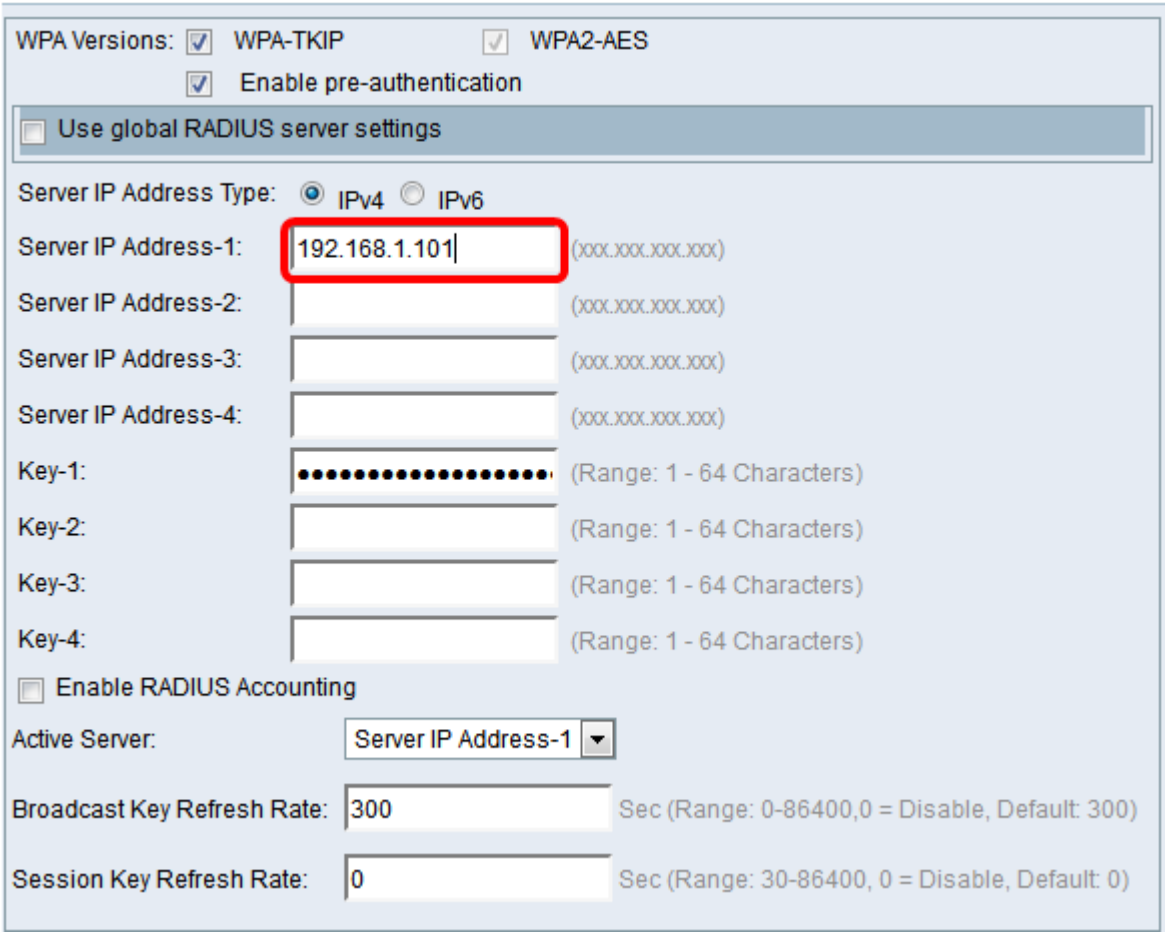
Paso 6. (Opcional) Haga clic en el botón de opción del **tipo de dirección IP del servidor** correcto.

Nota: Para este ejemplo, se elige IPv4.



Paso 7. Ingrese la dirección IP del servidor RADIUS en el campo *Server IP Address* .

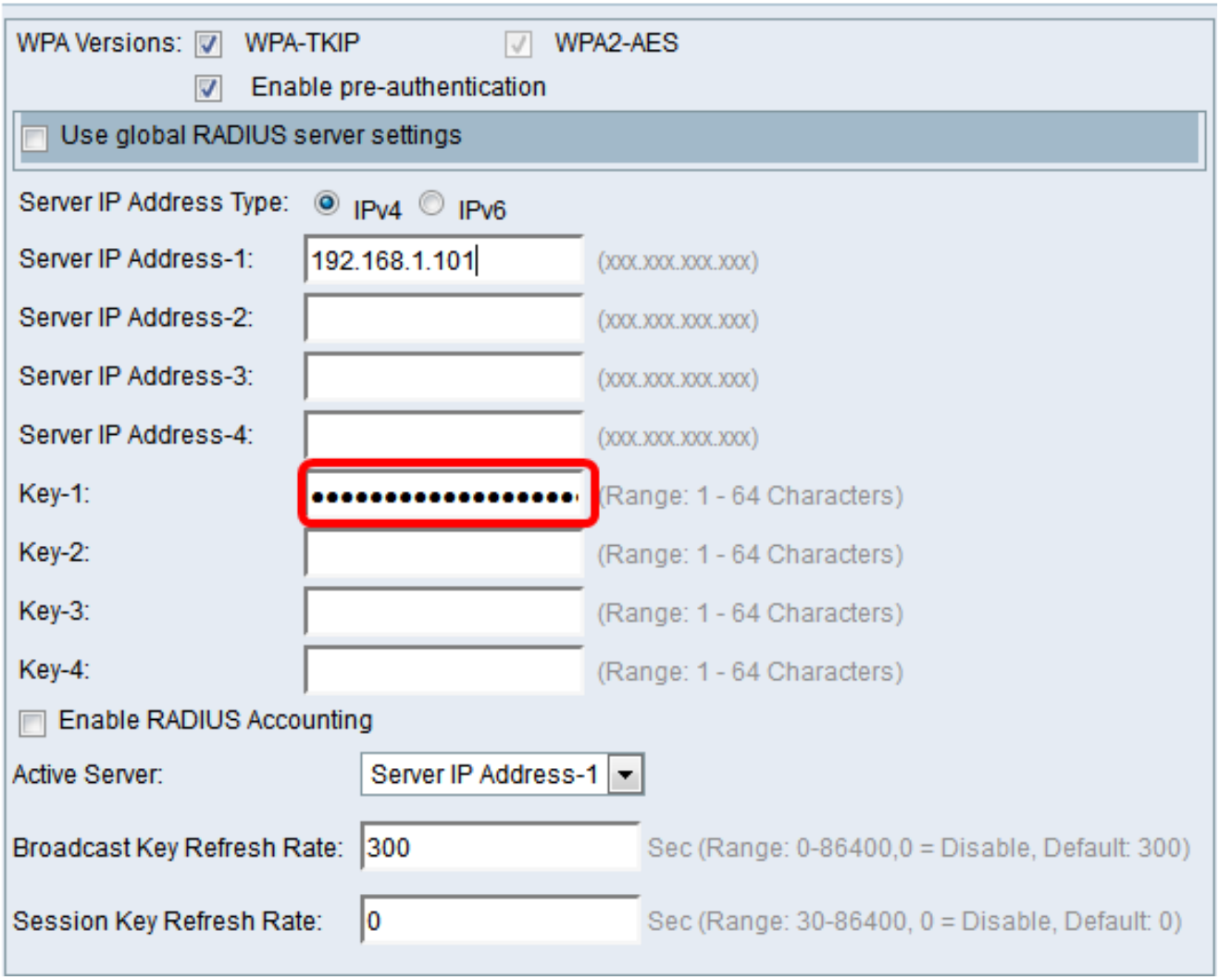
Nota: Para este ejemplo se utiliza 192.168.1.101.



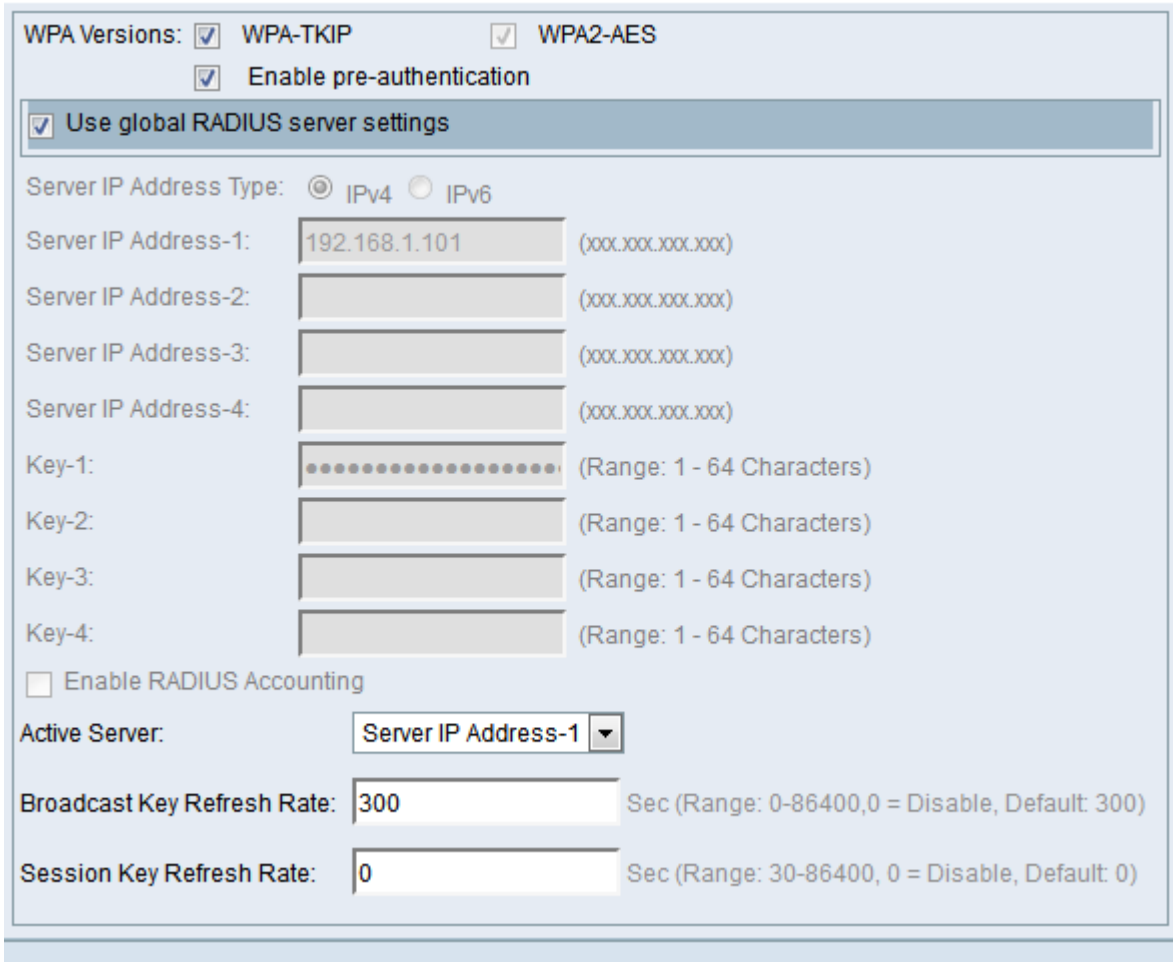
Paso 8. En el campo *Key*, ingrese la clave de contraseña correspondiente a su servidor RADIUS que el WAP utiliza para autenticar al servidor RADIUS. Puede utilizar de 1 a 64 caracteres alfanuméricos estándar y caracteres especiales.

Nota: Las claves distinguen entre mayúsculas y minúsculas y deben coincidir con la clave configurada en el servidor RADIUS.

Paso 9. (Opcional) Repita los pasos 7-8 para cada servidor RADIUS de la red con el que desee que WAP se comunique.



Paso 10. (Opcional) Marque la casilla de verificación **EnableRADIUS Accounting** para habilitar el seguimiento y la medición de los recursos que ha consumido un usuario (tiempo del sistema, cantidad de datos transmitidos). Al activar esta función, se permitirá la contabilización RADIUS tanto para los servidores primarios como de respaldo.



Paso 11. Haga clic Save.

Ahora ha configurado correctamente la seguridad WPA/WPA2 Enterprise en su WAP.