Configuraciones de la seguridad de red inalámbrica de la configuración en un WAP

Introducción

Configurar la seguridad de red inalámbrica en su unto de acceso de red inalámbrica (WAP) es alto-esencial proteger su red inalámbrica contra los intrusos que pueden comprometer la aislamiento de sus dispositivos de red inalámbrica así como de los datos que transmiten sobre su red inalámbrica. Usted puede configurar la seguridad de red inalámbrica en su red inalámbrica configurando el filtro MAC, el acceso protegido Wi-Fi (WPA/WPA2) personal, y WPA/WPA2 la empresa.

La filtración MAC se utiliza para filtrar a los clientes de red inalámbrica para acceder la red usando sus direcciones MAC. Una lista del cliente será configurada a permite que o bloquea los direccionamientos en la lista accedan la red, dependiendo de su preferencia. Para aprender más sobre el MAC que filtra, haga clic aquí.

WPA/WPA2 personal y WPA/WPA2 la empresa es protocolos de Seguridad usados para proteger la aislamiento cifrando los datos transmitidos sobre la red inalámbrica. WPA/WPA2 es compatible con las normas IEEE 802.11E y 802.11i. Comparado al Wired Equivalent Privacy (WEP) el Security Protocol, WPA/WPA2 han mejorado la autenticación y las funciones de encripción.

WPA/WPA2 personal está para el uso en el hogar y WPA/WPA2 la empresa está para la red negocio-escalada. WPA/WPA2 la empresa proporciona la mayores Seguridad y control centralizado sobre la red comparada a WPA/WPA2 personal.

En este escenario, la seguridad de red inalámbrica va a ser configurada en el WAP para proteger la red contra los intrusos que usan las configuraciones WPA/WPA2 personales y empresa.

Objetivo

Este artículo apunta mostrarle cómo configurar los protocolos WPA/WPA2 personales y empresa de Seguridad para mejorar la Seguridad y la aislamiento de su red inalámbrica.

Note: Este artículo asume que un Service Set Identifier (SSID) o un Wireless Local Area Network (red inalámbrica (WLAN)) se ha creado ya en su WAP.

Dispositivos aplicables

- WAP100 Series
- WAP300 Series
- WAP500 Series

Versión del software

- 1.0.2.14 – WAP131, WAP351
- 1.0.6.5 – WAP121, WAP321

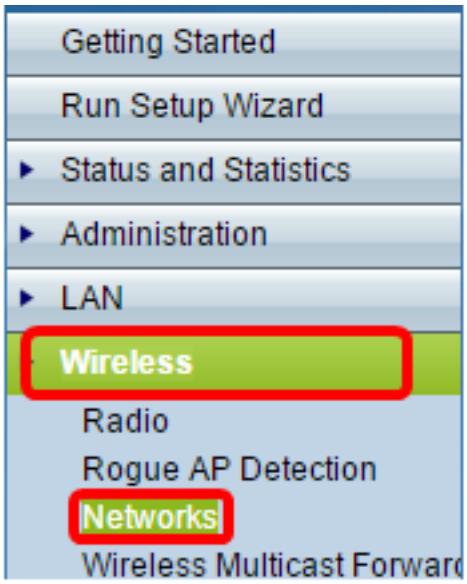
- 1.3.0.4 – WAP371
- 1.1.0.7 – WAP150, WAP361
- 1.2.1.5 - WAP551, WAP561
- 1.0.1.11 – WAP571, WAP571E

Configuraciones de la seguridad de red inalámbrica de la configuración

Configuración WPA/WPA2 personal

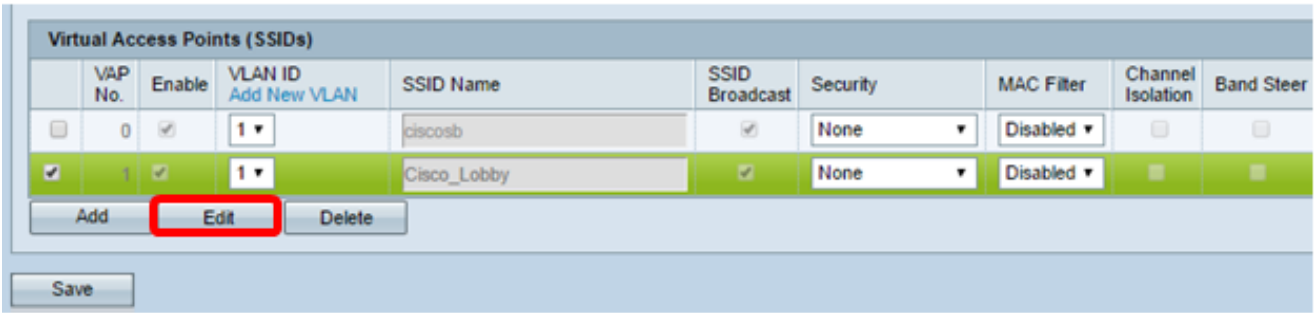
Paso 1. Inicie sesión a la utilidad basada en web de su Punto de acceso y elija la **Tecnología inalámbrica > las redes**.

Note: En la imagen abajo, la utilidad basada en web del WAP361 se utiliza como un ejemplo. Las opciones de menú pueden variar dependiendo del modelo de su dispositivo.

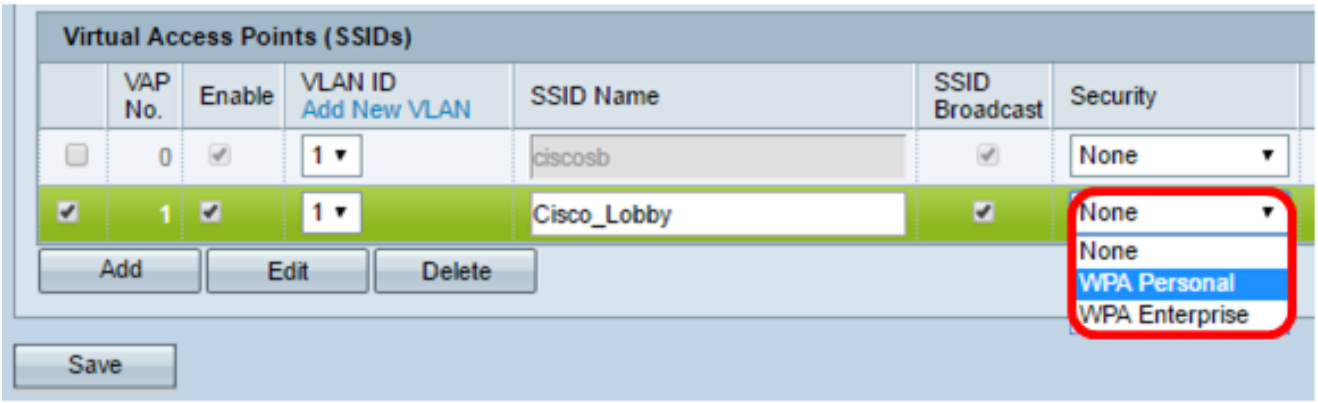


Paso 2. Bajo área de las puntas de acceso virtual (SSID), marque la casilla de verificación del SSID que usted quiere configurar y el tecleo **edita**.

Nota: En este ejemplo, se elige VAP1.



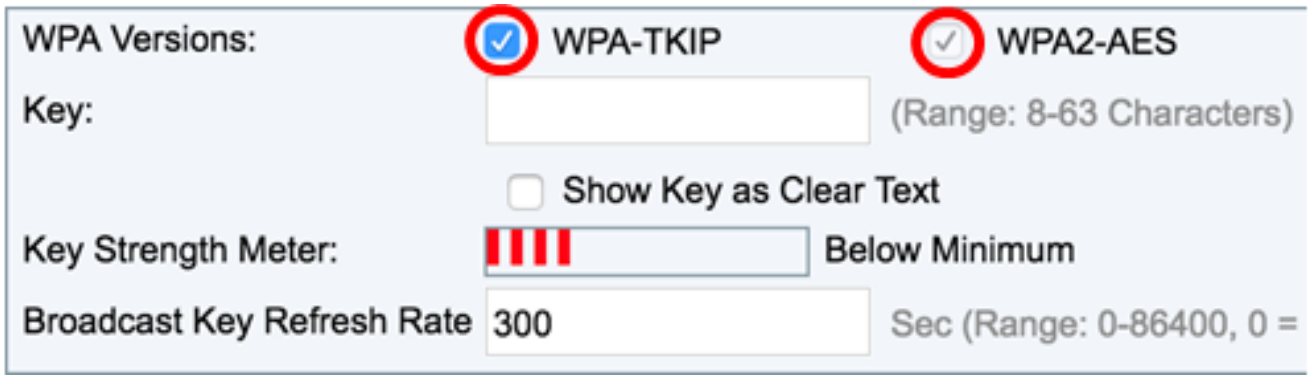
Paso 3. Tecleo **WPA personal de la** lista desplegable de la Seguridad.



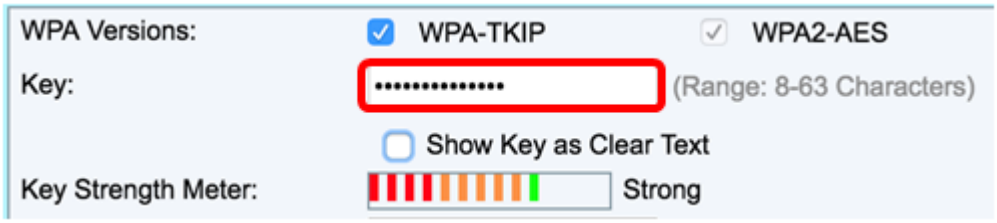
Paso 4. Elija la versión WPA (WPA-TKIP o WPA2-AES) marcando la casilla de verificación. Dos se pueden elegir inmediatamente.

- WPA-TKIP — El Wi-Fi protegió la herramienta dominante Acceso-temporal de la integridad. La red tiene algunas estaciones del cliente que soporten solamente el Security Protocol WPA original y TKIP. Observe que elegir solamente WPA-TKIP para el Punto de acceso no está permitida según el último requisito del Wi-Fi Alliance.
- WPA2-AES — Norma de encripción Acceso-avanzada protegida Wi-Fi. Todas las estaciones del cliente en la red soportan el WPA2 y AES-CCMP la cifra/el Security Protocol. Esta versión WPA proporciona la mejor Seguridad por el estándar de IEEE 802.11i. Según el último requisito del Wi-Fi Alliance, el WAP tiene que soportar este modo todo el tiempo.

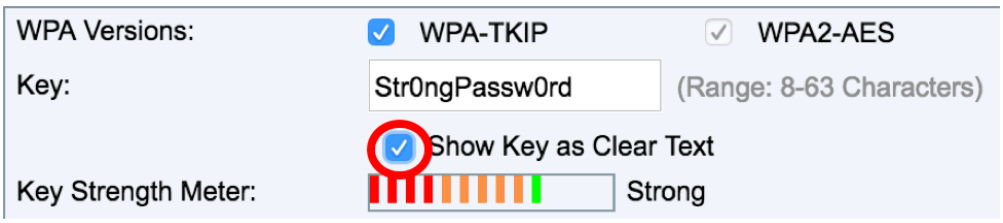
Nota: Por este ejemplo, se marcan ambas casillas de verificación.



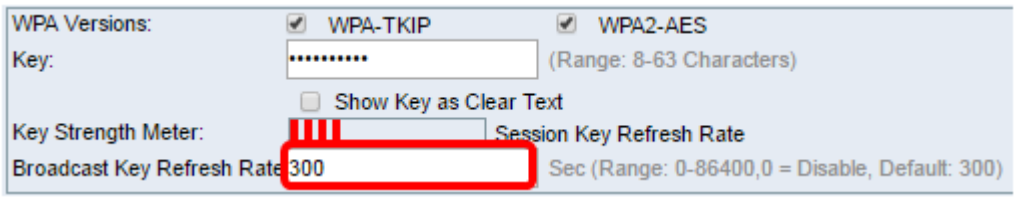
Paso 5. Cree una contraseña que consiste en 8-63 caracteres y ingresela en el *campo clave* .



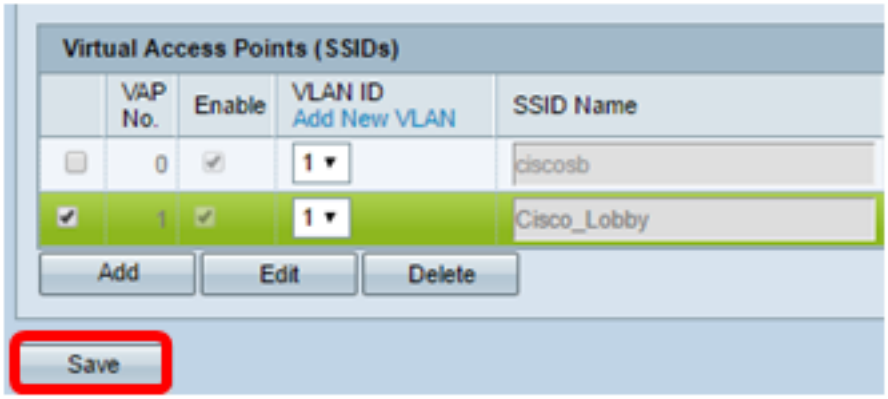
Note: Usted puede marcar la **clave de la demostración como clear text box** para mostrar la contraseña que usted creó.



El paso 6. (opcional) en el campo de la *velocidad de actualización de la clave del broadcast* , ingresa un valor o el intervalo en los cuales la clave del broadcast (grupo) se restaure para los clientes asociados a este VAP. El valor por defecto es 300 segundos y el intervalo válido es a partir 0 a 86400 segundos. Un valor de 0 indica que la clave del broadcast no está restaurada.



Paso 7. **Salvaguardia del** tecleo.

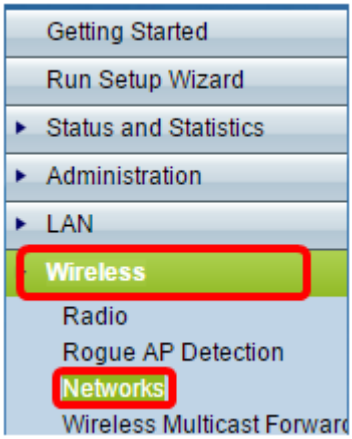


Usted ahora ha configurado el WPA personal en su WAP.

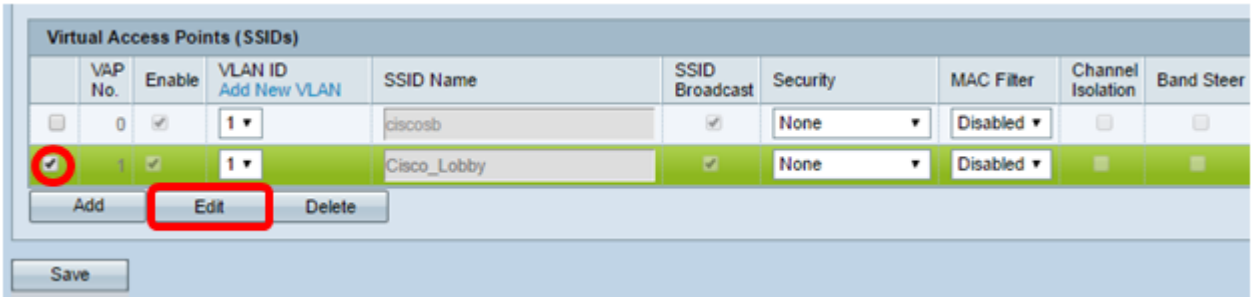
De la configuración empresa WPA/WPA2

Paso 1. Inicie sesión a la utilidad basada en web de su Punto de acceso y elija la **Tecnología inalámbrica > las redes**.

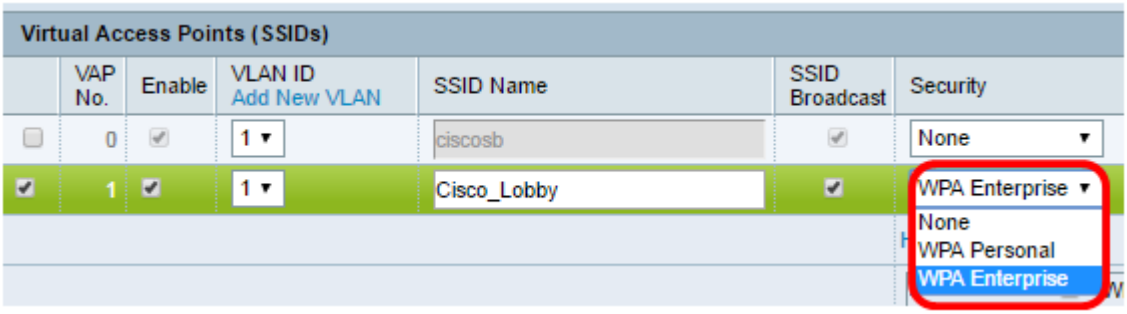
Note: En la imagen abajo, la utilidad basada en web del WAP361 se utiliza como un ejemplo.



Paso 2. Bajo área de las puntas de acceso virtual (SSID), marque el SSID que usted quiere configurar y hacer clic el **botón Edit** debajo de ella.



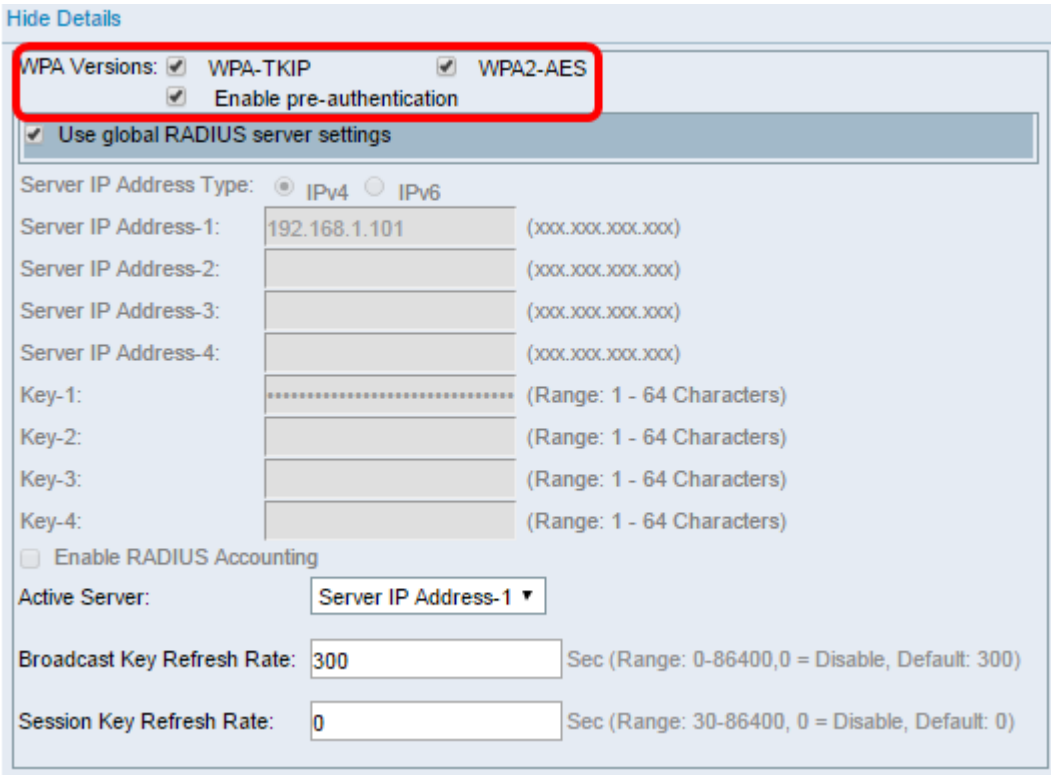
Paso 3. Elija la **empresa WPA de la** lista desplegable de la Seguridad.



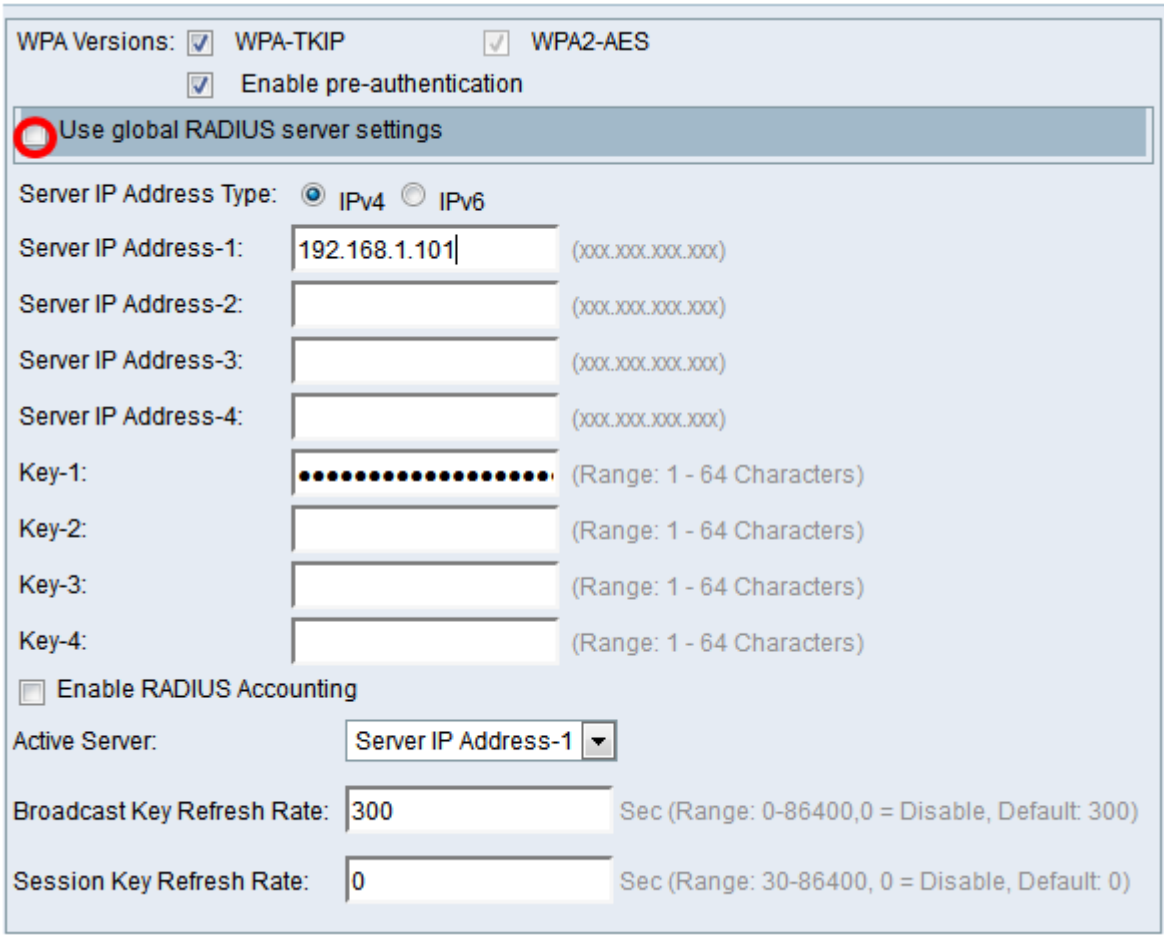
Paso 4. Elija la versión WPA (WPA-TKIP, WPA2-AES, y PRE-autenticación del permiso).

- PRE-autenticación del permiso — Si usted elige WPA2-AES solamente o WPA-TKIP y WPA2-AES como la versión WPA, usted puede habilitar la PRE-autenticación para los clientes WPA2-AES. Marque esta opción si usted quisiera que los clientes de red inalámbrica WPA2 enviaran los paquetes de la PRE-autenticación. La información de la PRE-autenticación se retransmite del dispositivo WAP que el cliente está utilizando actualmente al dispositivo de la blanco WAP. Habilitar esta característica puede ayudar a acelerar la autenticación para los clientes de itinerancia que conectan con los múltiples puntos de acceso (AP).

Nota: Esta opción no se aplica si usted seleccionó WPA-TKIP para las versiones WPA porque el WPA original no soporta esta característica.

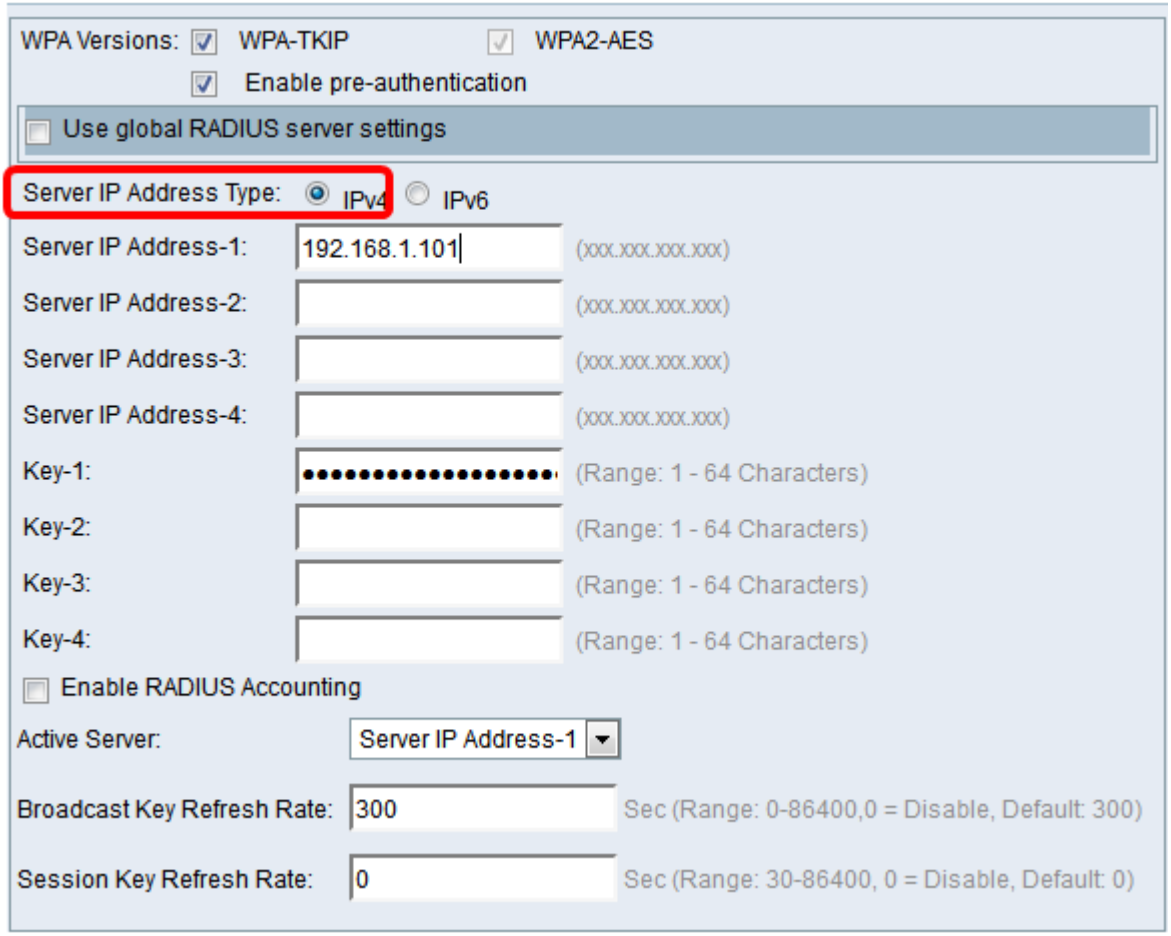


El paso 5. (opcional) desmarca la **casilla de verificación Settings (Configuración) global del servidor de RADIUS del uso** para editar las configuraciones.



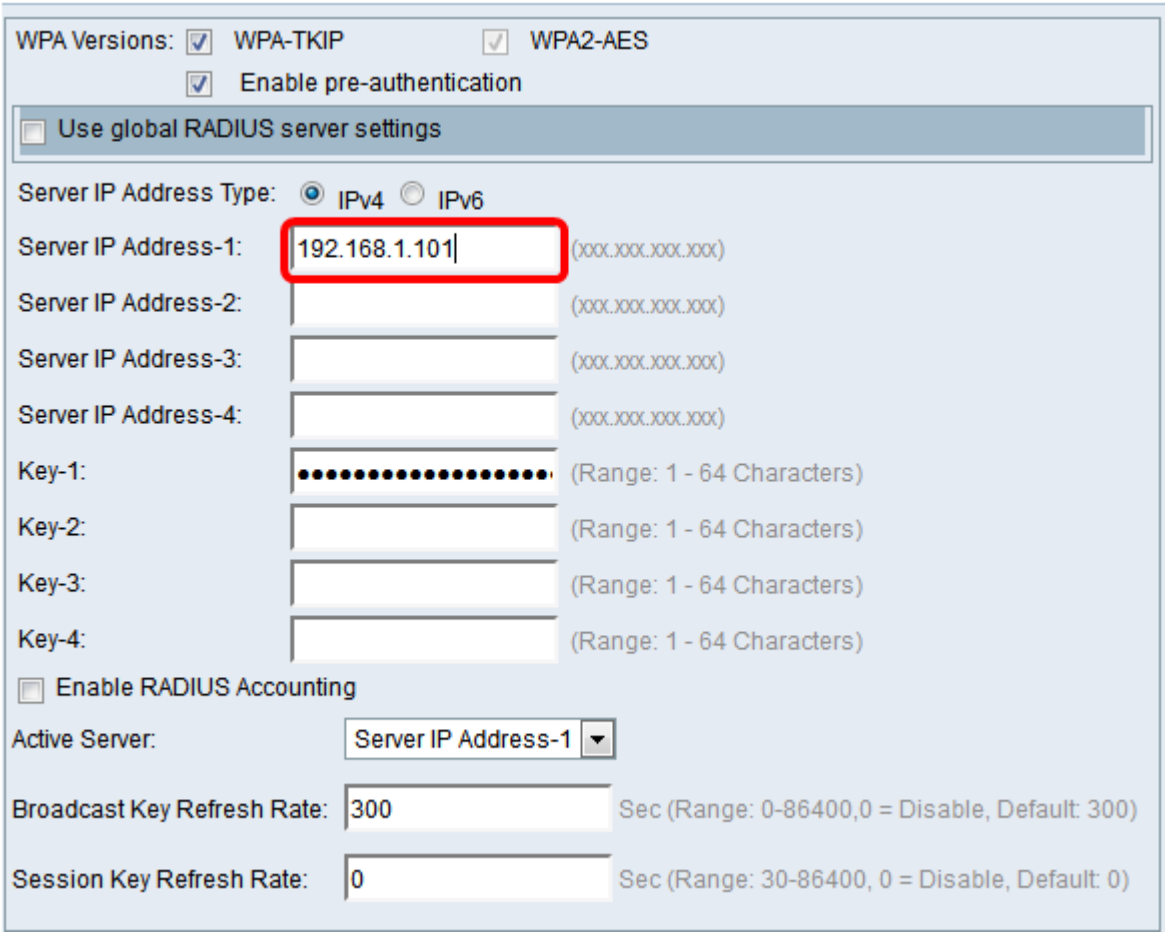
Tecleo (opcional) del paso 6. el botón de radio para el **tipo** correcto del **dirección IP del servidor**.

Nota: Por este ejemplo, se elige el IPv4.



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

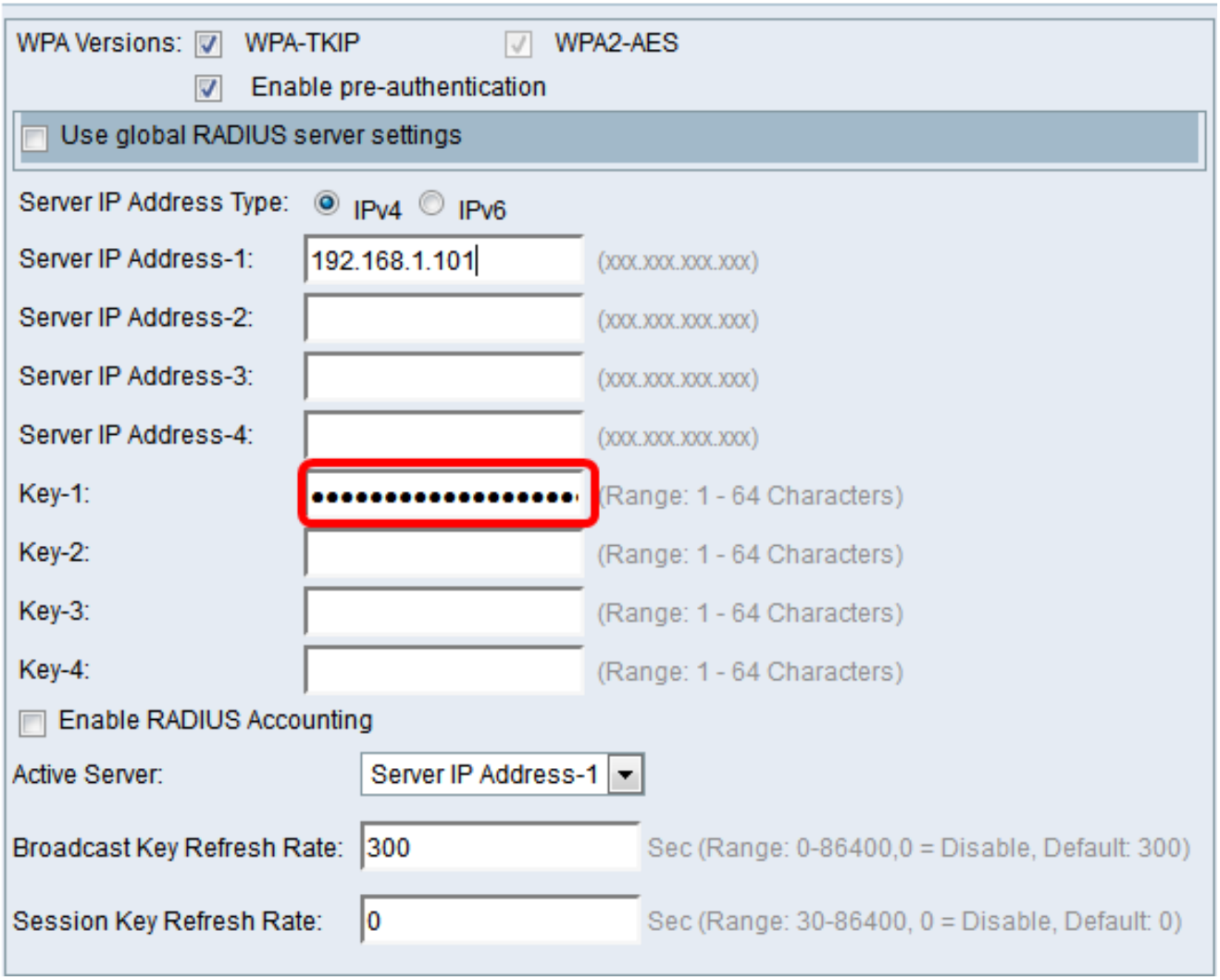
Nota: Por este ejemplo se utiliza 192.168.1.101.



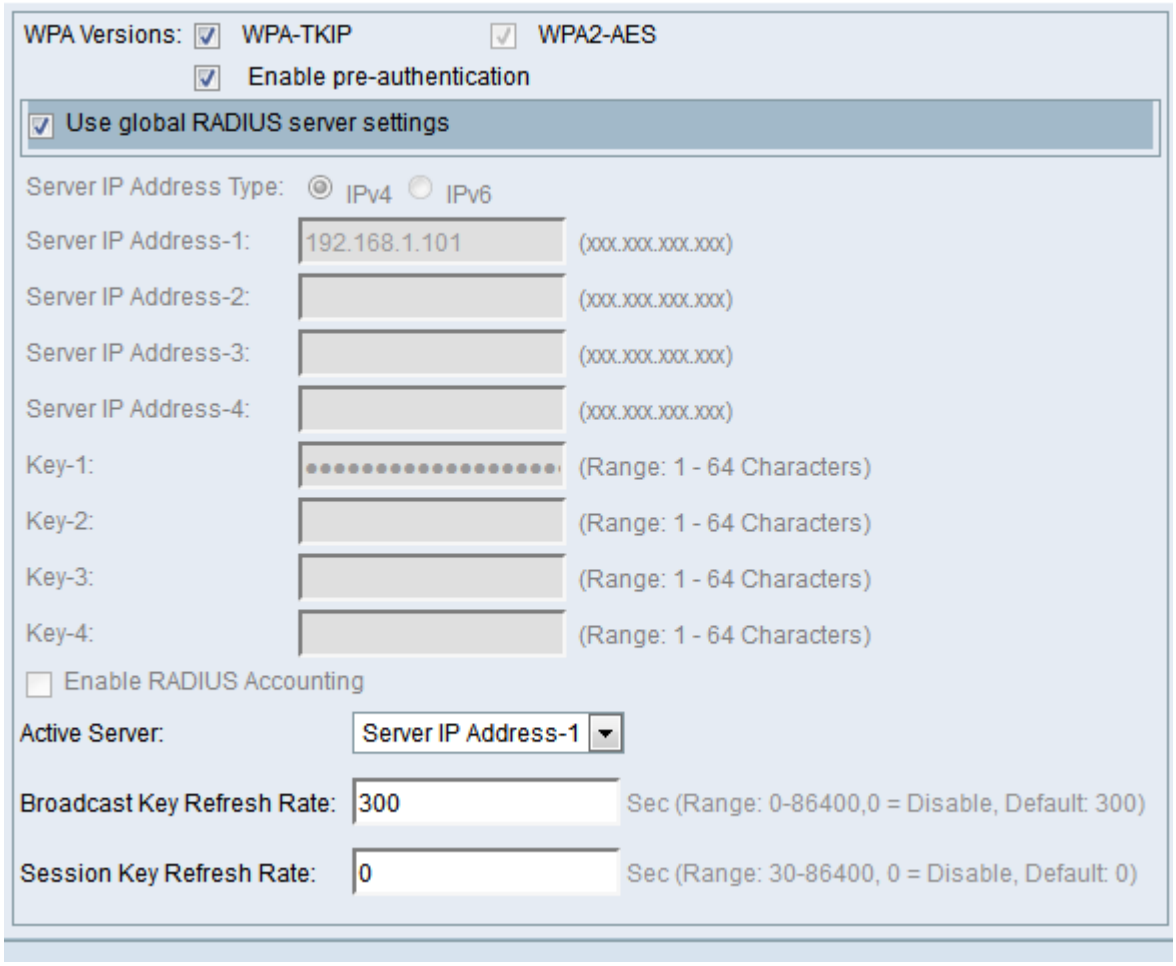
Paso 8. En el *campo clave*, ingrese la clave de la contraseña correspondiente a su servidor de RADIUS que el WAP utilice para autenticar al servidor de RADIUS. Usted puede utilizar a partir 1 a 64 alfanuméricos estándar y los caracteres especiales.

Note: Las claves son con diferenciación entre mayúsculas y minúsculas y deben hacer juego la clave configurada en el servidor de RADIUS.

El paso 9. (opcional) relanza los pasos 7-8 para cada servidor de RADIUS en su red que usted quisiera que el WAP comunicara con.



Control (opcional) del paso 10. la casilla de verificación de las **estadísticas de EnableRADIUS** para habilitar el seguimiento y la medición de los recursos que un usuario ha consumido (Tiempo del sistema, el periodo de los datos transmitidos). Habilitar esta característica permitirá el RADIUS que explica ambos los servidores primarios y de backup.



Paso 11 Tecleo Save.

Usted ahora ha configurado con éxito WPA/WPA2 la Seguridad de la empresa en su WAP.