Tabla del caso del acceso de invitado de la configuración en el Punto de acceso WAP125

Objetivo

La característica del acceso de invitado del Punto de acceso WAP125 proporciona la conectividad de red inalámbrica a los clientes de red inalámbrica temporales dentro del rango del dispositivo. Trabaja teniendo el Punto de acceso transmite dos diversos identificadores del conjunto de servicio (SSID): uno para la red principal, y el otro para la red del invitado. Entonces reorientan a los invitados a un portal prisionero en donde los requieren ingresar sus credenciales. En efecto, esto mantendría la red principal segura mientras que todavía daba a los invitados el acceso a Internet.

Las configuraciones del portal del cautivo tales como tiempo de espera de la sesión y reorientan el Uniform Resource Locator (URL) se configuran en la tabla del caso del acceso de invitado de la utilidad basada en web del WAP125. La característica del acceso de invitado ha sido determinado útil en los pasillos del hotel y de la oficina, los restaurantes, y las alamedas.

Este artículo apunta mostrarle cómo configurar la tabla del caso del acceso de invitado del Punto de acceso WAP125. Asume que las configuraciones para la tabla de la escena del portal web y la tabla del grupo del invitado están configuradas ya. Para las instrucciones en configurar ambas configuraciones, haga clic aquí.

Dispositivos aplicables

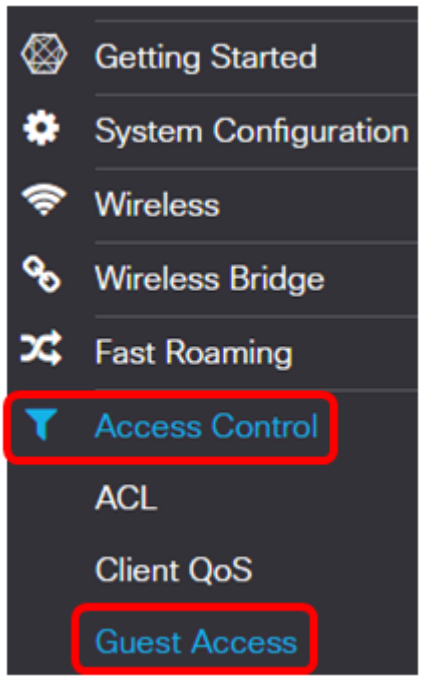
- WAP125

Versión del software

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

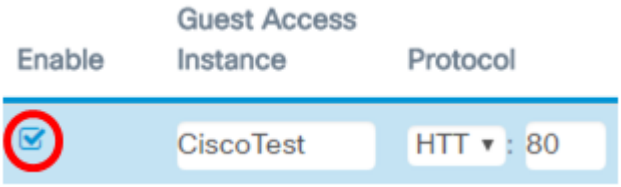
Tabla del caso del acceso de invitado de la configuración

Paso 1. Inicie sesión a la utilidad basada en web del WAP125 y elija el **control de acceso > el acceso de invitado**.

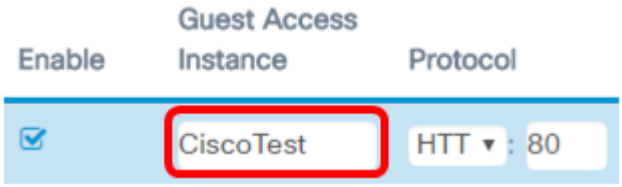


Nota: Las imágenes en este artículo se toman del WAP125. Las opciones de menú pueden variar dependiendo del modelo de su dispositivo.

Paso 2. Verifique que la casilla de verificación del **permiso del** caso del acceso de invitado esté marcada para asegurarse de que el acceso de invitado es activo.



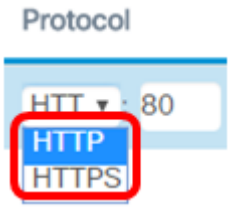
Paso 3. Ingrese un nombre para el caso en el campo del *caso del acceso del invitado*. Éste puede ser hasta 32 caracteres alfanuméricos.



Nota: En este ejemplo, se ingresa CiscoTest.

Paso 4. Elija un protocolo para el caso del acceso de invitado. Las opciones son:

- HTTP — Esta opción también se conoce como Hypertext Transfer Protocol (HTTP). No proporciona el cifrado durante la verificación de la página web pedida.
- HTTPS — Esta opción también se conoce como Protocolo de transporte de hipertexto seguro (HTTPS). Esto significa que todas las comunicaciones entre el ordenador y el sitio web que está entrando en contacto se cifra.



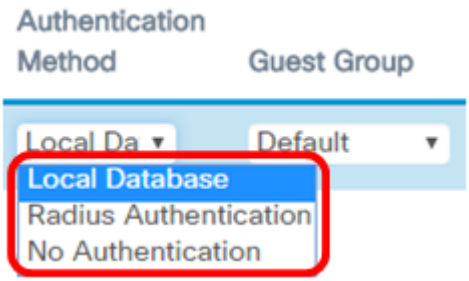
Nota: En este ejemplo, se elige el HTTP.

Paso 5. Ingrese un número del puerto al lado del campo del protocolo. Las ayudas del número del puerto identifican el protocolo cuando alcanza un servidor.

Nota: En este ejemplo, se ingresa 80.

Paso 6. Elija un método de autentificación de la lista desplegable del método de autentificación. Esto será utilizada por el Punto de acceso cuando los clientes autentican a través del portal del cautivo. Las opciones son:

- Base de datos local — Esta opción deja el dispositivo WAP verificar las credenciales del usuario de un archivo que se salve localmente. Si se elige esta opción, acabe al paso 7 al paso 10 y después proceda a configurar la tabla del grupo del invitado.
- Autenticación de RADIUS — Esta opción deja el Punto de acceso verificar a los usuarios a través de un servidor del Remote Authentication Dial-In User Service (RADIUS). Si se elige esta opción, acabe al paso 7 al paso 10 y después proceda a la autenticación de RADIUS de la configuración.
- Ninguna autenticación — Esta opción inhabilita la autenticación y permite que los clientes de red inalámbrica conecten con la red del invitado sin ingresar sus credenciales. Si se elige esta opción, salte al paso 11.

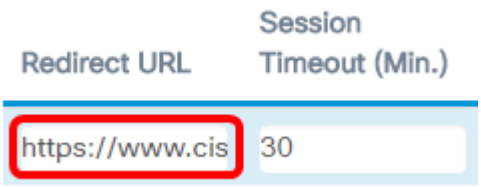


Nota: En este ejemplo, se elige la base de datos local.

Paso 7. Elija a un grupo de la lista desplegable del grupo del invitado.

Nota: En este ejemplo, el valor por defecto se elige automáticamente.

Paso 8. Ingrese el direccionamiento que se reorientará después de ingresar las credenciales en el campo *URL de la reorientación*.

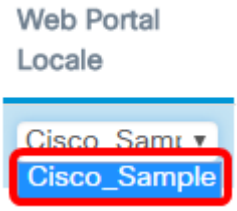


Nota: El direccionamiento debe comenzar con el HTTP o el HTTPS. En este ejemplo, se ingresa https://www.cisco.com.

Paso 9. Ingrese el número de minutos antes del los tiempos de la sesión hacia fuera en el campo *(mínimo) del tiempo de espera de la sesión*.

Nota: En este ejemplo, se ingresa 30.

Paso 10. Elija un perfil del portal web de la lista desplegable de la escena del portal web.



Nota: En este ejemplo, Cisco_Sample se elige automáticamente. Para las instrucciones en cómo configurar la escena del portal web, haga clic aquí.

La tabla del caso del acceso de invitado debe ahora ser configurada.

Tabla del grupo del invitado de la configuración

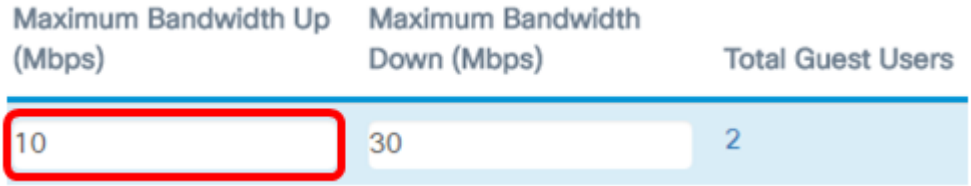
Paso 7. Ingrese un nombre para el grupo del invitado en el campo de *nombre del grupo del invitado*. El nombre del grupo del invitado puede ser hasta 32 caracteres de largo.

Nota: En este ejemplo, se ingresa CiscoGuests.

Paso 8. Ingrese el número de minutos antes de los tiempos pronto hacia fuera en el campo *(mínimo) del tiempo de inactividad*.

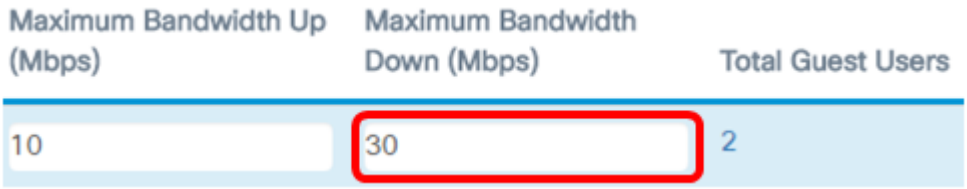
Nota: En este ejemplo, se ingresa 5.

Paso 9. Ingrese la velocidad de la carga máxima en el campo *ascendente del ancho de banda máximo (Mbps)*. Éste será el ancho de banda máximo, en el Mbps, que un cliente de red inalámbrica puede enviar al usar el portal del cautivo. El ancho de banda máximo puede ser a partir la 0 a 300, donde está el valor predeterminado 0.



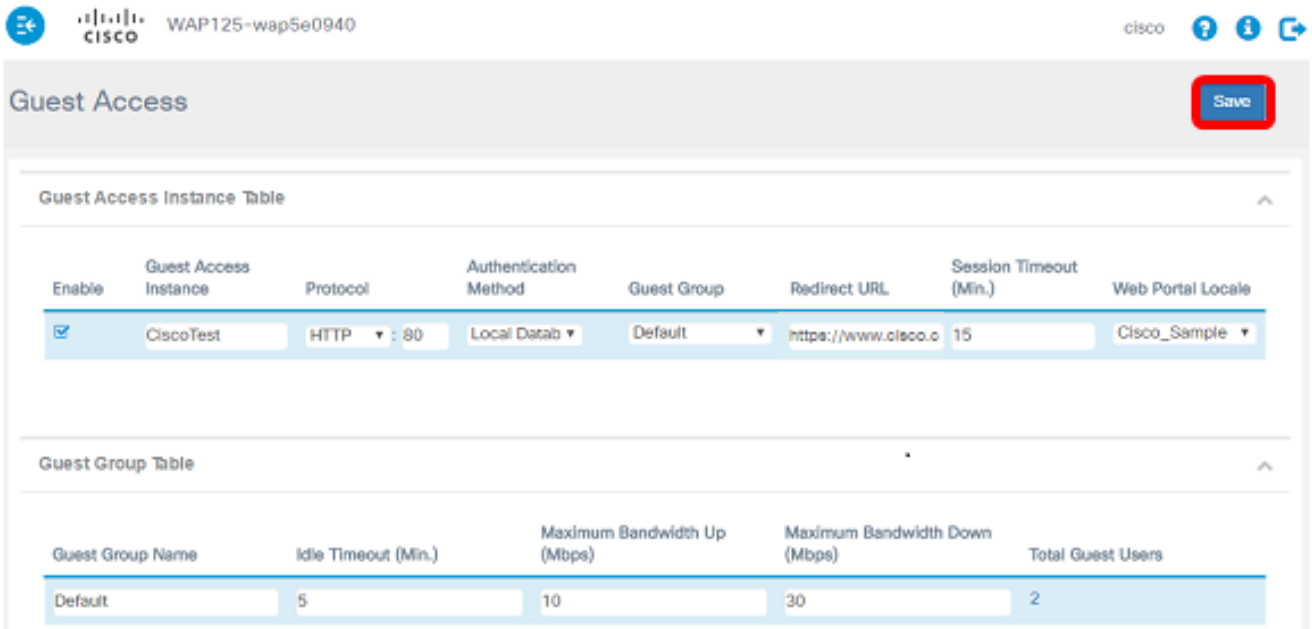
Nota: En este ejemplo, se ingresa 10.

Paso 10. Ingrese la velocidad de la descarga máxima en el *ancho de banda máximo abajo (Mbps)* colocan. Éste será el ancho de banda máximo, en el Mbps, que un cliente de red inalámbrica puede recibir al usar el portal del cautivo. El ancho de banda máximo puede ser a partir la 0 a 300, donde está el valor predeterminado 0.



Nota: En este ejemplo, se ingresa 30.

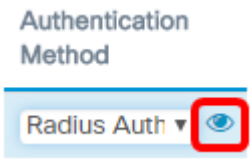
Paso 11 **Salvaguardia del** tecleo.



La tabla del caso del acceso de invitado se debe ahora configurar con la autenticación de la base de datos local.

Autenticación RADIUS

Paso 1. Haga clic el botón View Button.

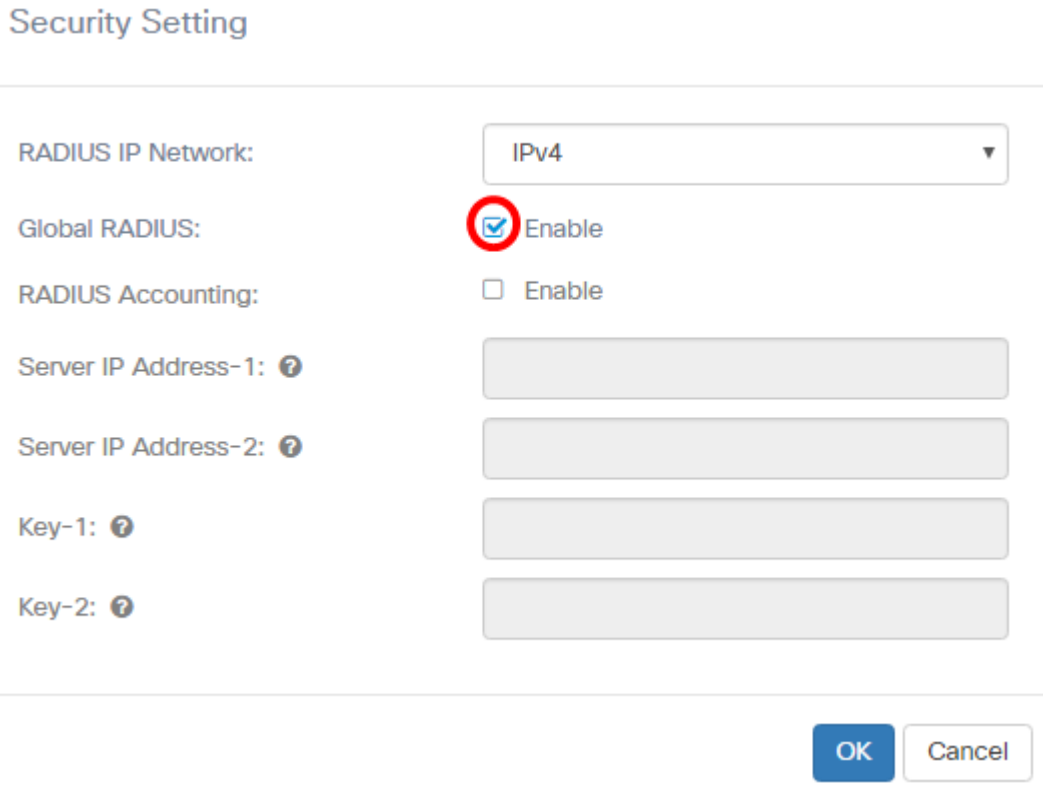


Paso 2. En la ventana emergente del ajuste de seguridad, elija la red del IP del radio de la lista desplegable de la red del IP RADIUS. Las opciones son:

- IPv4 — Esta opción es la forma más de uso general de IP Addressing en una red. Utiliza un formato de 32 bits para identificar los host en una red.
- IPv6 — Esta opción es el estándar de la dirección IP de la última generación previsto para substituir el formato del IPv4. El IPv6 soluciona el problema de la escasez del direccionamiento con el uso de un sistema direccional del 128-bit en vez de 32 bits usado en el IPv4.

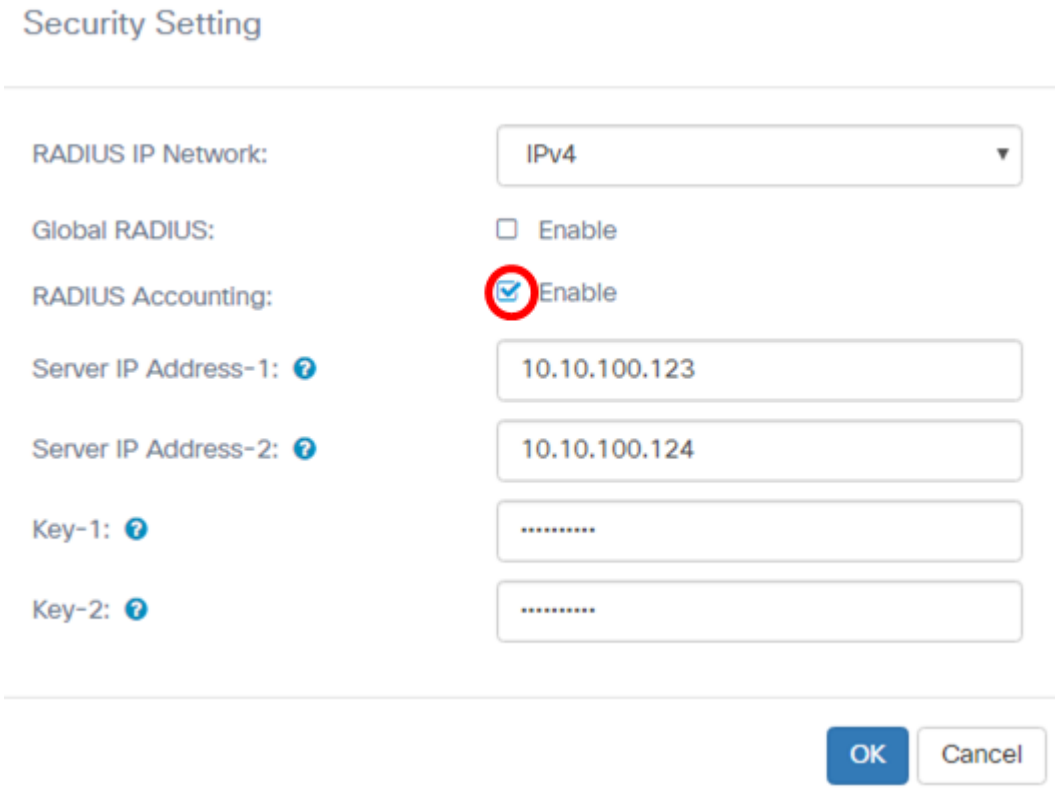
Nota: En este ejemplo, se elige el IPv4.

Control (opcional) del paso 3. Habilitar Radius la casilla de verificación global para dejar el uso porta prisionero un diverso conjunto de los servidores de RADIUS.

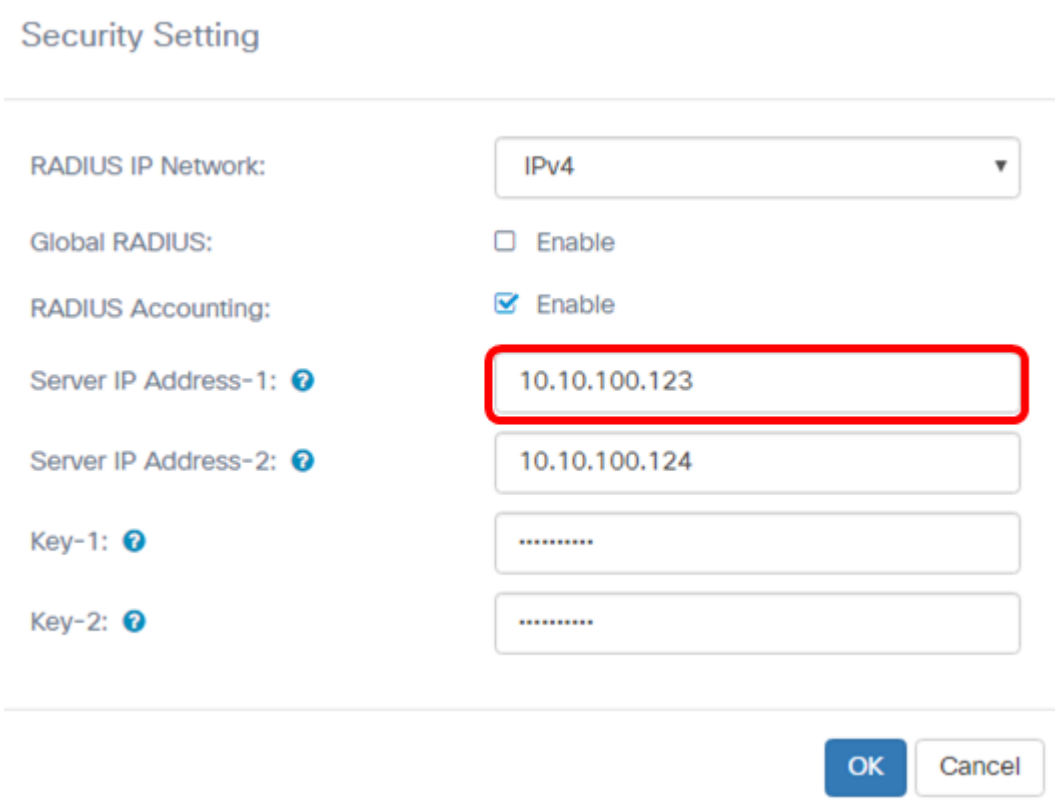


Nota: Cuando está habilitada, ninguna otra configuración para el área del ajuste de seguridad necesita ser configurada. Proceda al paso 9. En este ejemplo, se habilita el RADIUS global.

Control (opcional) del paso 4. la casilla de verificación del **permiso de las** estadísticas RADIUS para dejar el Punto de acceso seguir y medir los recursos que un usuario determinado ha consumido, por ejemplo el Tiempo del sistema y el periodo de los datos transmitidos y recibidos.

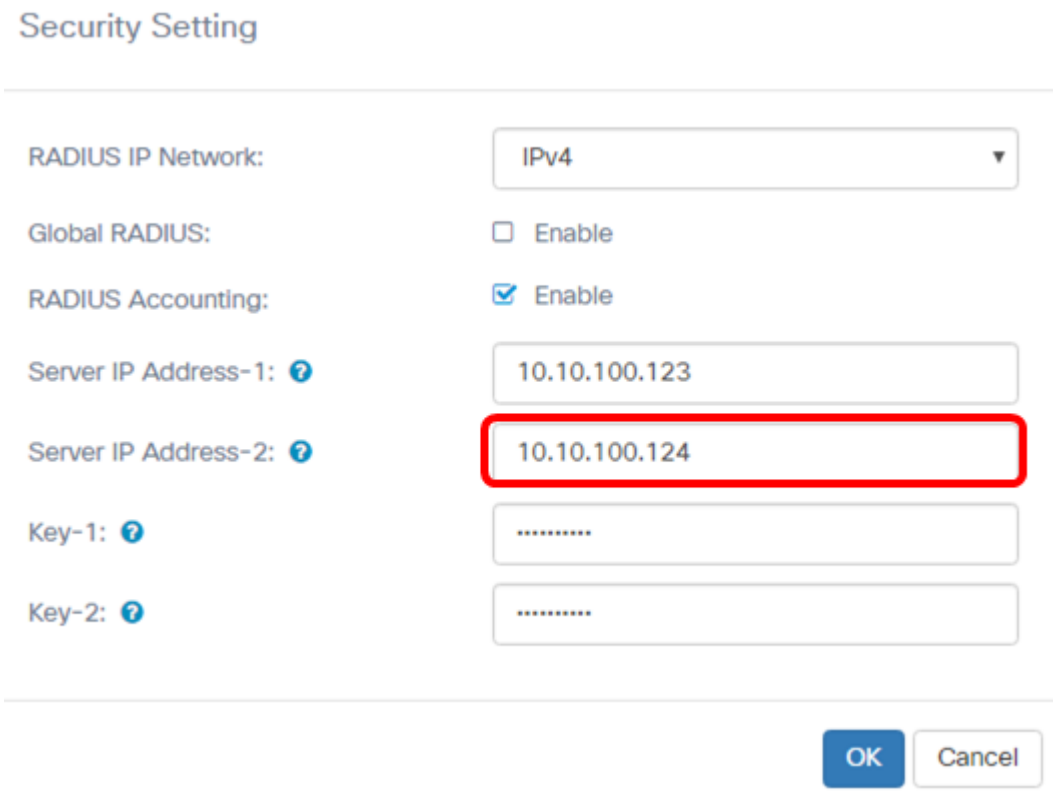


El paso 5. (opcional) ingresa el direccionamiento del IPv4 o del IPv6 del servidor de RADIUS primario en *IP del servidor el* campo *Address-1*.



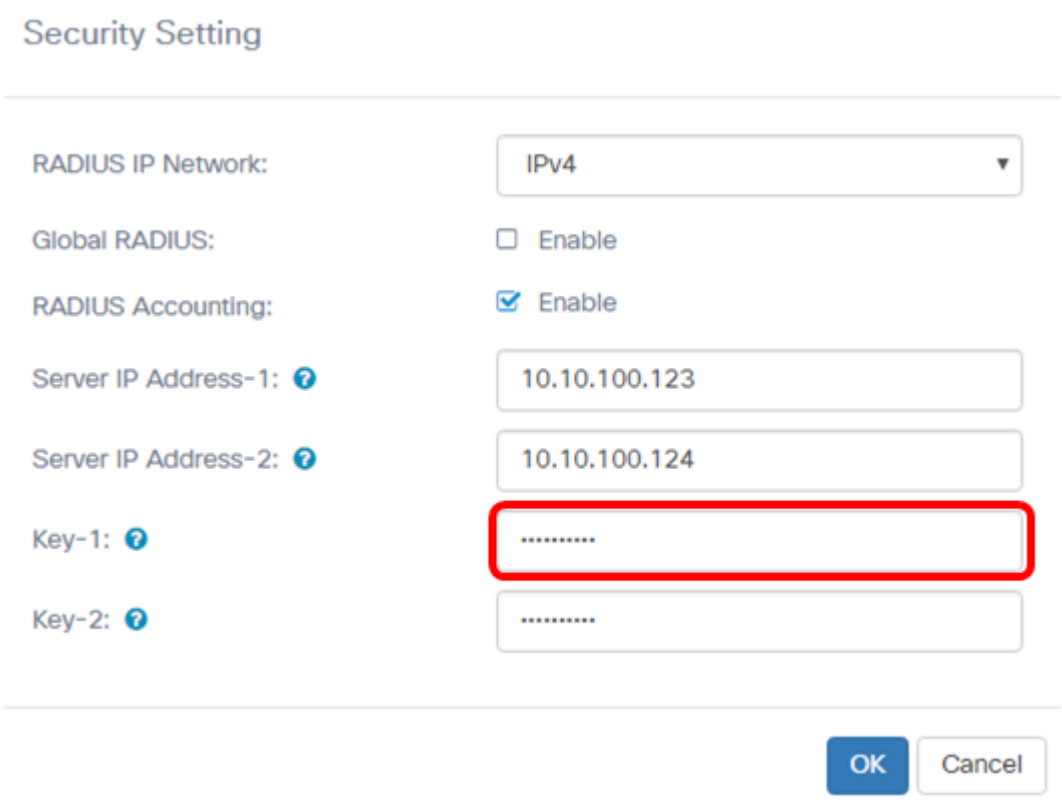
Nota: En este ejemplo, se ingresa 10.10.100.123.

El paso 6. (opcional) ingresa el direccionamiento del IPv4 o del IPv6 del servidor de RADIUS de reserva en *IP del servidor el* campo *Address-2*.

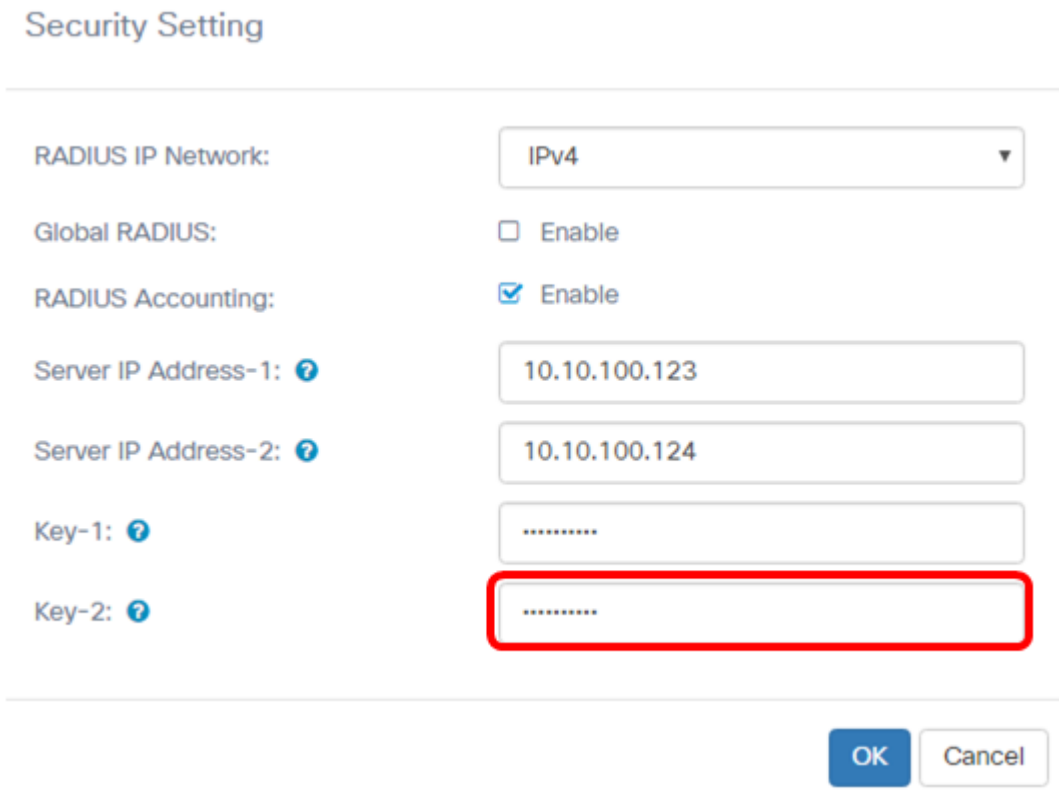


Nota: En este ejemplo, se ingresa 10.10.100.124.

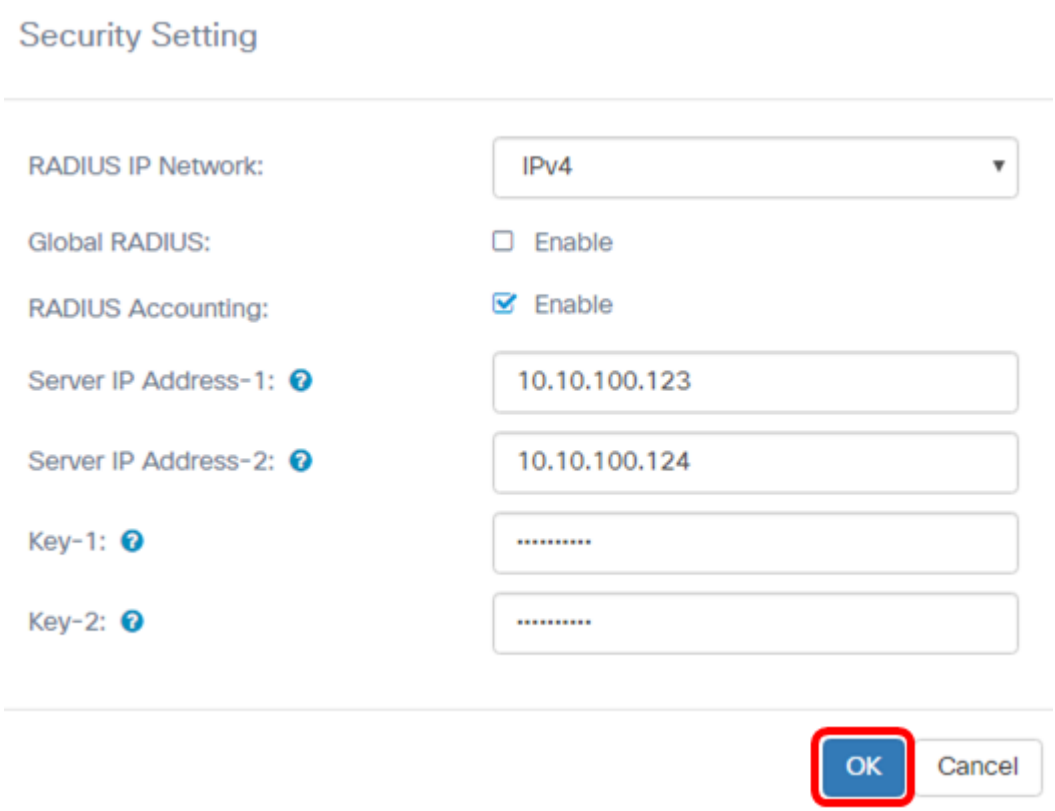
El paso 7. (opcional) ingresa la contraseña que el Punto de acceso utiliza para autenticar al servidor de RADIUS primario en el campo *Key-1*. La entrada en este campo es con diferenciación entre mayúsculas y minúsculas y debe hacer juego la entrada configurada en el servidor de RADIUS primario. La clave puede ser hasta 63 caracteres alfanuméricos.



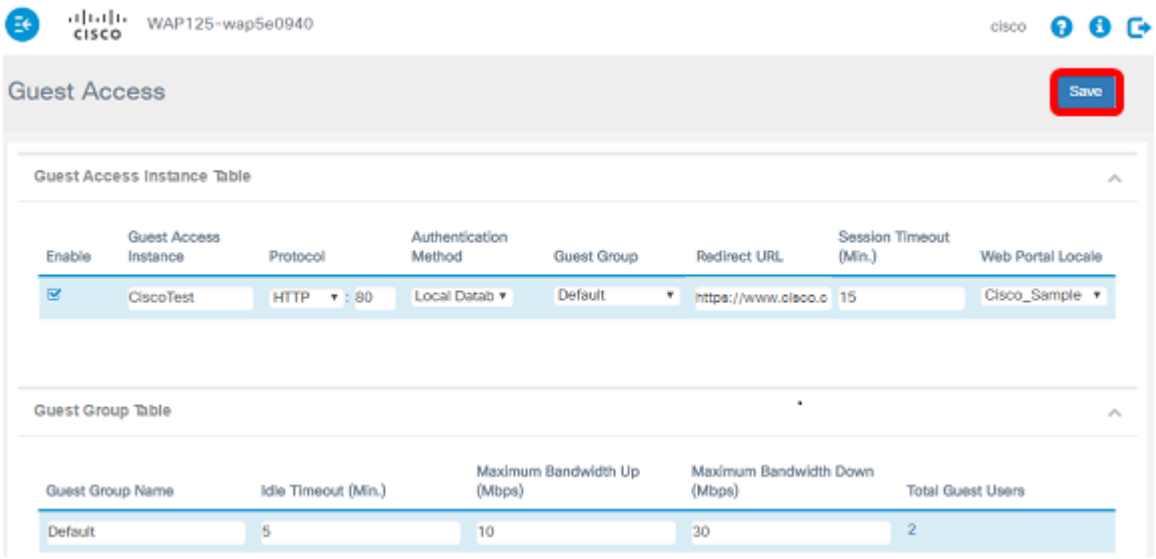
El paso 8. (opcional) ingresa la contraseña que el Punto de acceso utiliza para autenticar al servidor RADIUS secundario en el campo *Key-2*. La entrada en este campo es con diferenciación entre mayúsculas y minúsculas y debe hacer juego la entrada configurada en el servidor de RADIUS primario. La clave puede ser hasta 63 caracteres alfanuméricos.



Paso 9. Haga Click en OK.



Paso 10. **Salvaguardia del** tecleo.



La tabla del caso del acceso de invitado se debe ahora configurar con el método de autenticación de RADIUS.