Configuración de la Tabla de Instancia de Acceso de Invitado en el Punto de Acceso WAP125

Objetivo

La función Acceso de invitado del punto de acceso WAP125 proporciona conectividad inalámbrica a clientes inalámbricos temporales dentro del alcance del dispositivo. Funciona haciendo que el punto de acceso difunda dos identificadores de conjunto de servicios (SSID) diferentes: uno para la red principal y el otro para la red de invitados. A continuación, se redirige a los invitados a un portal cautivo donde se les exige que introduzcan sus credenciales. De esta forma, la red principal permanecería protegida mientras que los invitados podían acceder a Internet.

La configuración del portal cautivo, como el tiempo de espera de la sesión y la redirección del localizador uniforme de recursos (URL), se configura en la tabla de instancias de acceso de invitado de la utilidad basada en web del WAP125. La función Guest Access ha sido especialmente útil en los vestíbulos, restaurantes y centros comerciales de hoteles y oficinas.

Este artículo pretende mostrarle cómo configurar la tabla de instancias de acceso de invitado del punto de acceso WAP125. Supone que la configuración de la tabla regional del portal web y de la tabla de grupos de invitados ya están configuradas. Para obtener instrucciones sobre la configuración de ambos parámetros, haga clic aquí.

Dispositivos aplicables

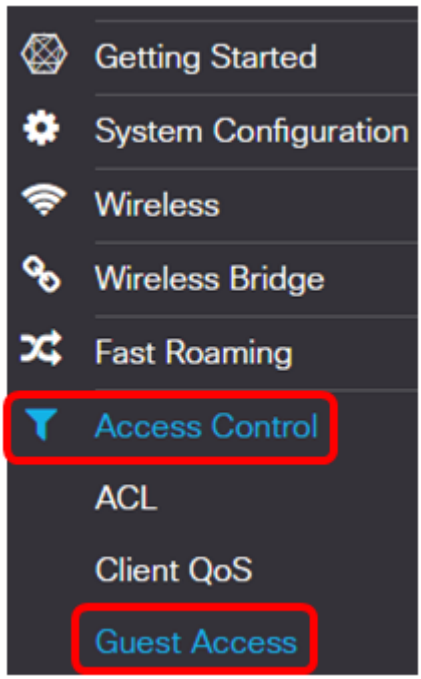
- WAP125

Versión del software

- 1.0.0.4: WAP581
- 1.0.0.5— WAP125

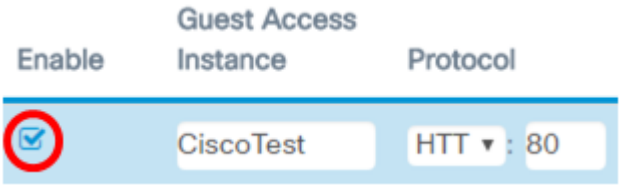
Configurar tabla de instancias de acceso de invitado

Paso 1. Inicie sesión en la utilidad basada en web del WAP125 y elija **Access Control > Guest Access**.

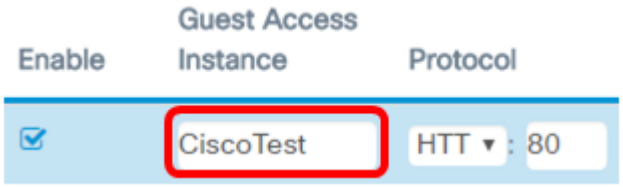


Nota: Las imágenes de este artículo son tomadas del WAP125. Las opciones de menú pueden variar en función del modelo del dispositivo.

Paso 2. Verifique que la casilla de verificación Guest Access Instance Enable esté activada para asegurarse de que Guest Access esté activo.



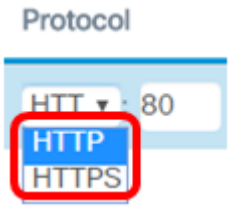
Paso 3. Introduzca un nombre para la instancia en el campo *Instancia de acceso de invitado* . Puede tener hasta 32 caracteres alfanuméricos.



Nota: En este ejemplo, se introduce CiscoTest.

Paso 4. Elija un protocolo para la instancia de acceso de invitado. Las opciones son:

- HTTP: esta opción también se conoce como protocolo de transferencia de hipertexto (HTTP). No proporciona cifrado durante la verificación de la página web solicitada.
- HTTPS: esta opción también se conoce como protocolo de transferencia de hipertexto seguro (HTTPS). Esto significa que todas las comunicaciones entre la computadora y el sitio web con el que está contactando están cifradas.



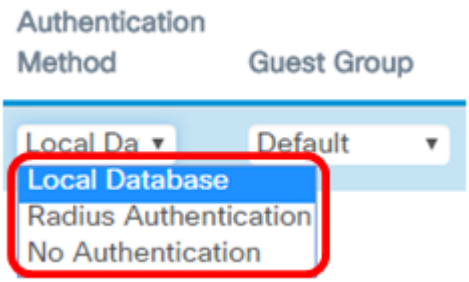
Nota: En este ejemplo, se elige HTTP.

Paso 5. Introduzca un número de puerto junto al campo Protocol (Protocolo). El número de puerto ayuda a identificar el protocolo cuando llega a un servidor.

Nota: En este ejemplo, se ingresa 80.

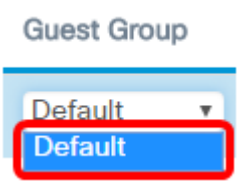
Paso 6. Elija un método de autenticación en la lista desplegable Método de autenticación. Esto será utilizado por el punto de acceso cuando los clientes se autentiquen a través del portal cautivo. Las opciones son:

- Base de datos local: esta opción permite que el dispositivo WAP verifique las credenciales del usuario desde un archivo almacenado localmente. Si se elige esta opción, complete con el Paso 7 al Paso 10 y, a continuación, continúe con la configuración de la Tabla de grupos de invitados.
- Autenticación RADIUS: esta opción permite que el punto de acceso verifique a los usuarios a través de un servidor RADIUS (Servicio de usuario de acceso telefónico de autenticación remota). Si se elige esta opción, complete con el Paso 7 al Paso 10 y luego continúe con la configuración de Autenticación RADIUS.
- Sin autenticación: esta opción inhabilita la autenticación y permite a los clientes inalámbricos conectarse a la red de invitados sin introducir sus credenciales. Si se elige esta opción, vaya directamente al Paso 11.



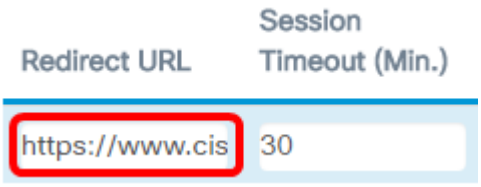
Nota: En este ejemplo, se elige Base de datos local.

Paso 7. Elija un grupo de la lista desplegable Grupo de invitados.



Nota: En este ejemplo, Default se elige automáticamente.

Paso 8. Ingrese la dirección a redirigir después de ingresar las credenciales en el campo *Redirigir URL*.

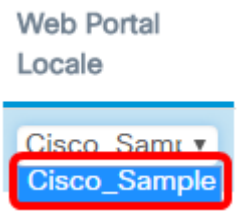


Nota: La dirección debe comenzar con HTTP o HTTPS. En este ejemplo, se ingresa https://www.cisco.com.

Paso 9. Introduzca el número de minutos antes de que se agote el tiempo de espera de una sesión en el campo *Tiempo de espera de sesión (mín.)*.

Nota: En este ejemplo, se ingresa 30.

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



Nota: En este ejemplo, Cisco_Sample se elige automáticamente. Para obtener instrucciones sobre cómo configurar la configuración regional del portal web, haga clic aquí.

La tabla de instancias de acceso de invitado debe configurarse ahora.

Configuración de la tabla de grupos de invitados

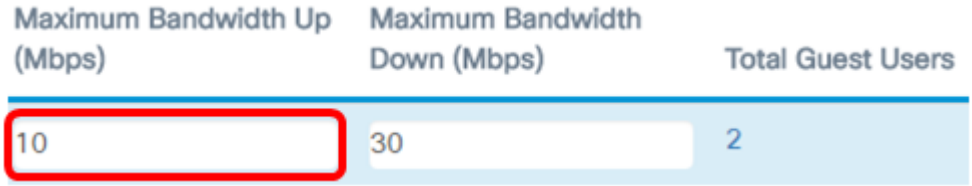
Paso 7. Introduzca un nombre para el grupo de invitados en el campo *Nombre de grupo de invitados*. El nombre del grupo de invitados puede tener hasta 32 caracteres.

Nota: En este ejemplo, se introduce CiscoInvitados.

Paso 8. Introduzca el número de minutos antes de que se agote el tiempo de espera de la indicación en el campo *Idle Timeout (Min.)*.

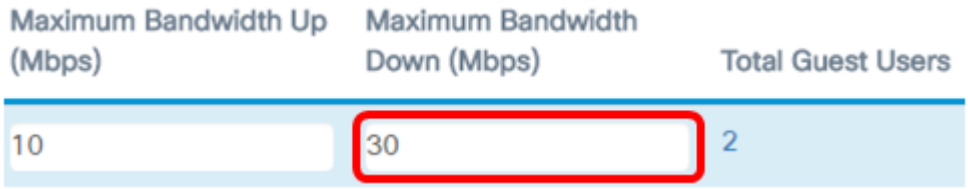
Nota: En este ejemplo, se ingresa 5.

Paso 9. Introduzca la velocidad máxima de carga en el campo *Maximum Bandwidth Up (Mbps)*. Este será el ancho de banda máximo, en Mbps, que un cliente inalámbrico puede enviar cuando utilice el portal cautivo. El ancho de banda máximo puede estar entre 0 y 300, donde 0 es el valor predeterminado.



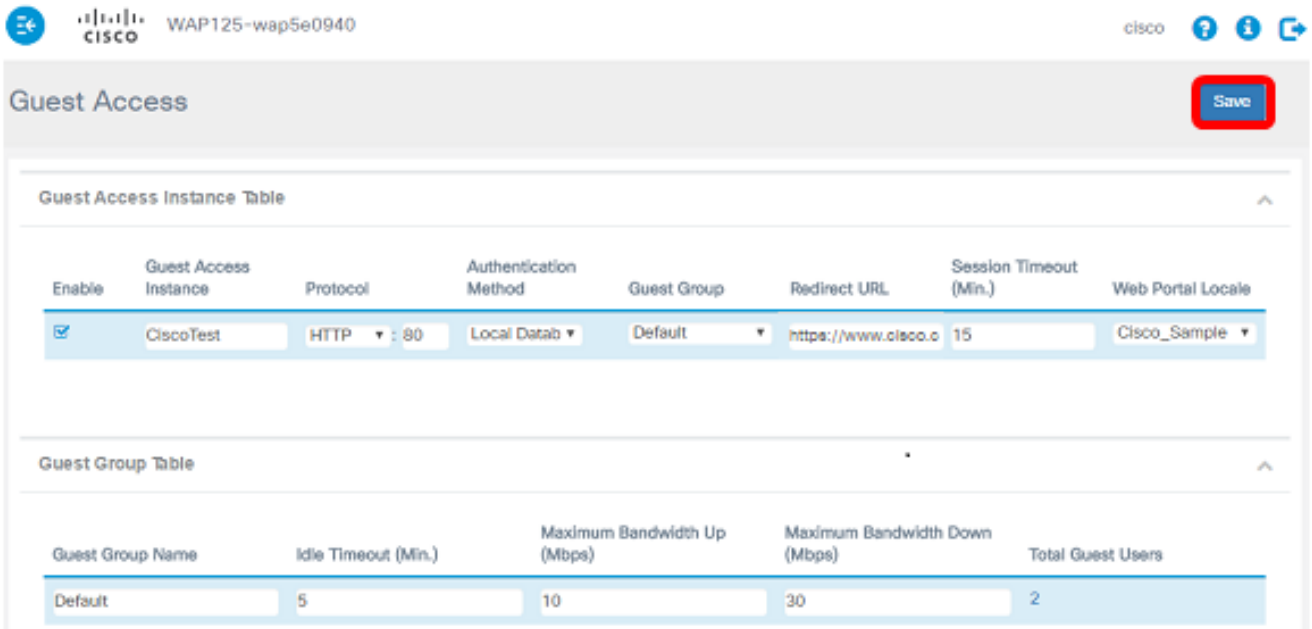
Nota: En este ejemplo, se ingresa 10.

Paso 10. Introduzca la velocidad máxima de descarga en el campo *Maximum Bandwidth Down (Mbps)*. Este será el ancho de banda máximo, en Mbps, que un cliente inalámbrico puede recibir cuando utilice el portal cautivo. El ancho de banda máximo puede estar entre 0 y 300, donde 0 es el valor predeterminado.



Nota: En este ejemplo, se ingresa 30.

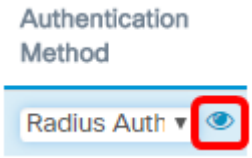
Paso 11. Click **Save**.



La Tabla de Instancia de Acceso de Invitado debe configurarse ahora con Autenticación de Base de Datos Local.

Autenticación RADIUS

Paso 1. Haga clic en el botón View (Ver).

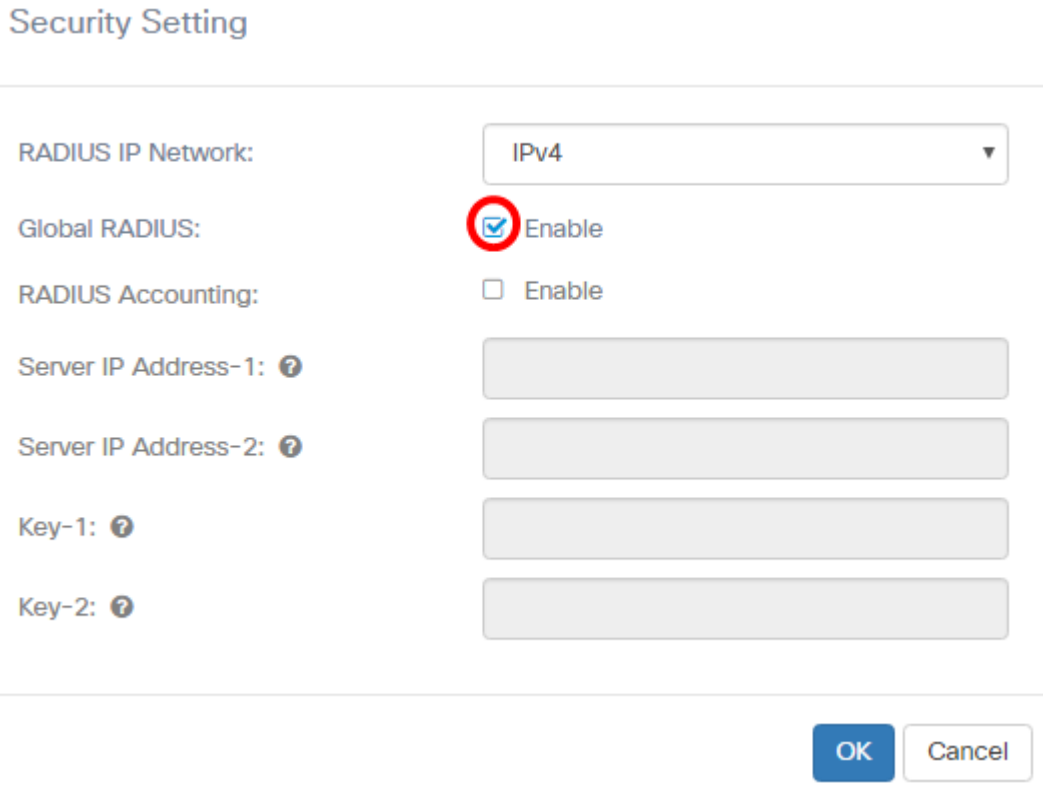


Paso 2. En la ventana emergente Security Setting (Configuración de seguridad), elija la red IP RADIUS de la lista desplegable RADIUS IP Network (Red IP RADIUS). Las opciones son:

- IPv4: esta opción es la forma de direccionamiento IP más utilizada en una red. Utiliza un formato de 32 bits para identificar los hosts en una red.
- IPv6: esta opción es el estándar de dirección IP de última generación diseñado para sustituir el formato IPv4. IPv6 resuelve el problema de escasez de direcciones con el uso de un sistema de direccionamiento de 128 bits en lugar de los 32 bits utilizados en IPv4.

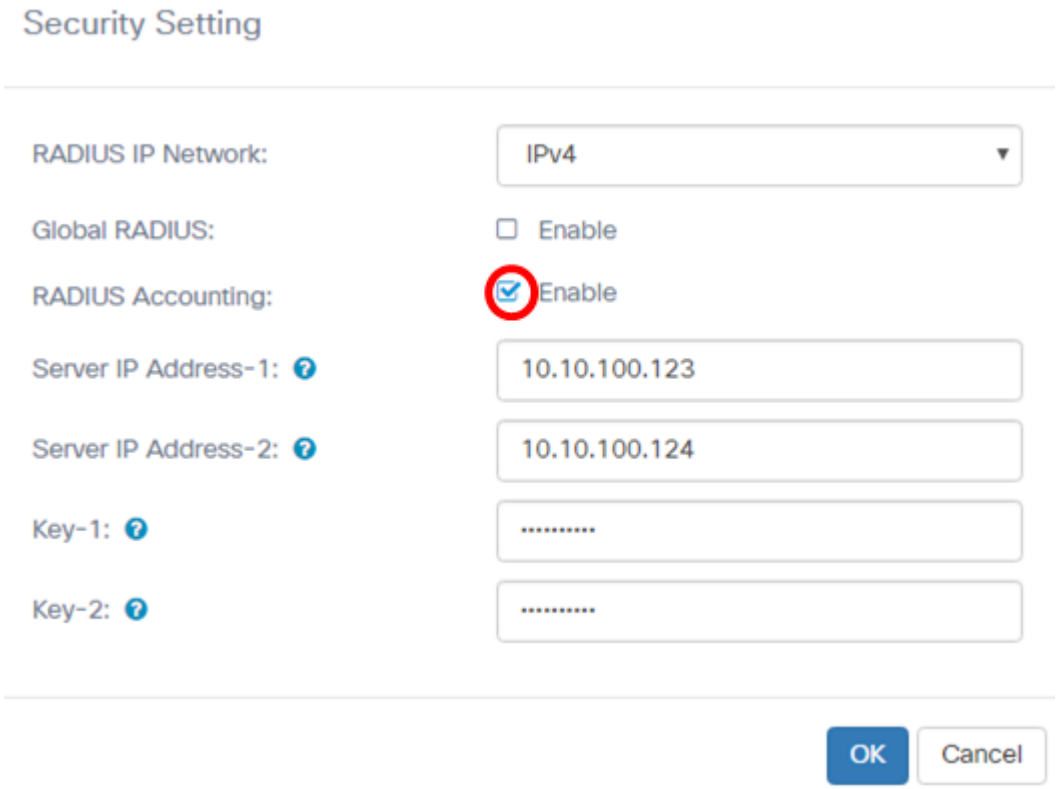
Nota: En este ejemplo, se elige IPv4.

Paso 3. (Opcional) Marque la casilla de verificación Global RADIUS **Enable** para permitir que el Portal cautivo utilice un conjunto diferente de servidores RADIUS.

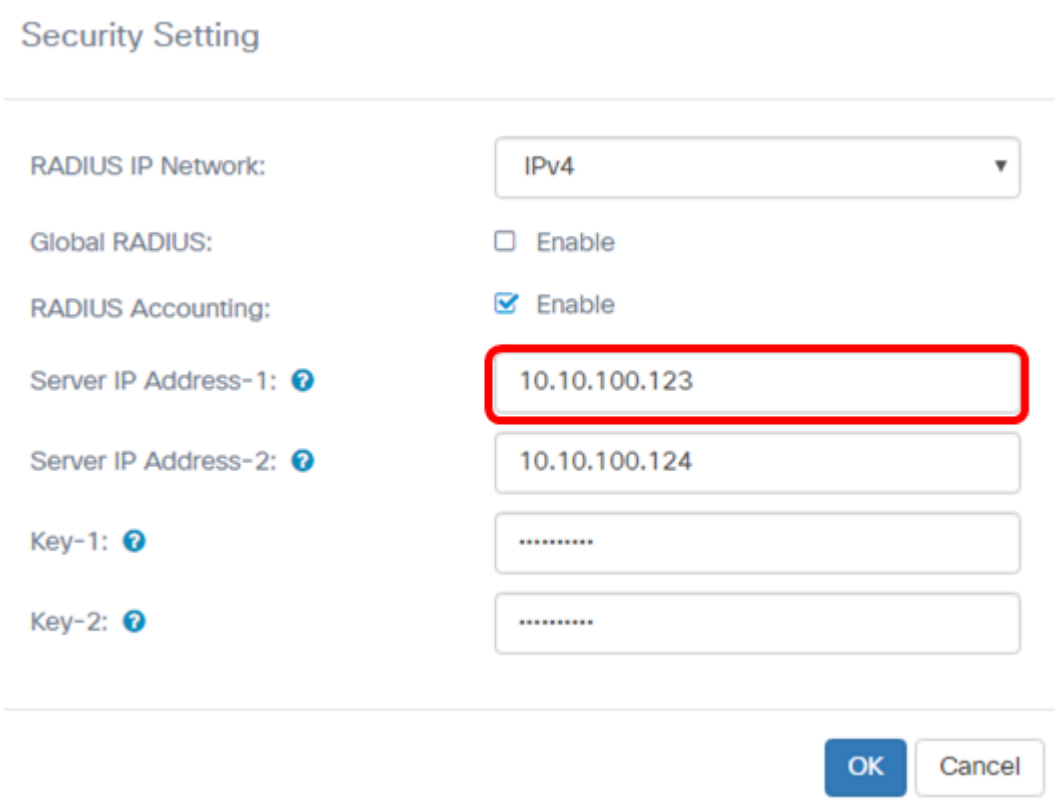


Nota: Cuando está activada, no es necesario configurar ninguna otra configuración para el área Configuración de seguridad. Proceda al Paso 9. En este ejemplo, se habilita Global RADIUS.

Paso 4. (Opcional) Marque la casilla de verificación RADIUS Accounting **Enable** para permitir que el punto de acceso realice un seguimiento y mida los recursos que un usuario en particular ha consumido, como la hora del sistema y la cantidad de datos transmitidos y recibidos.

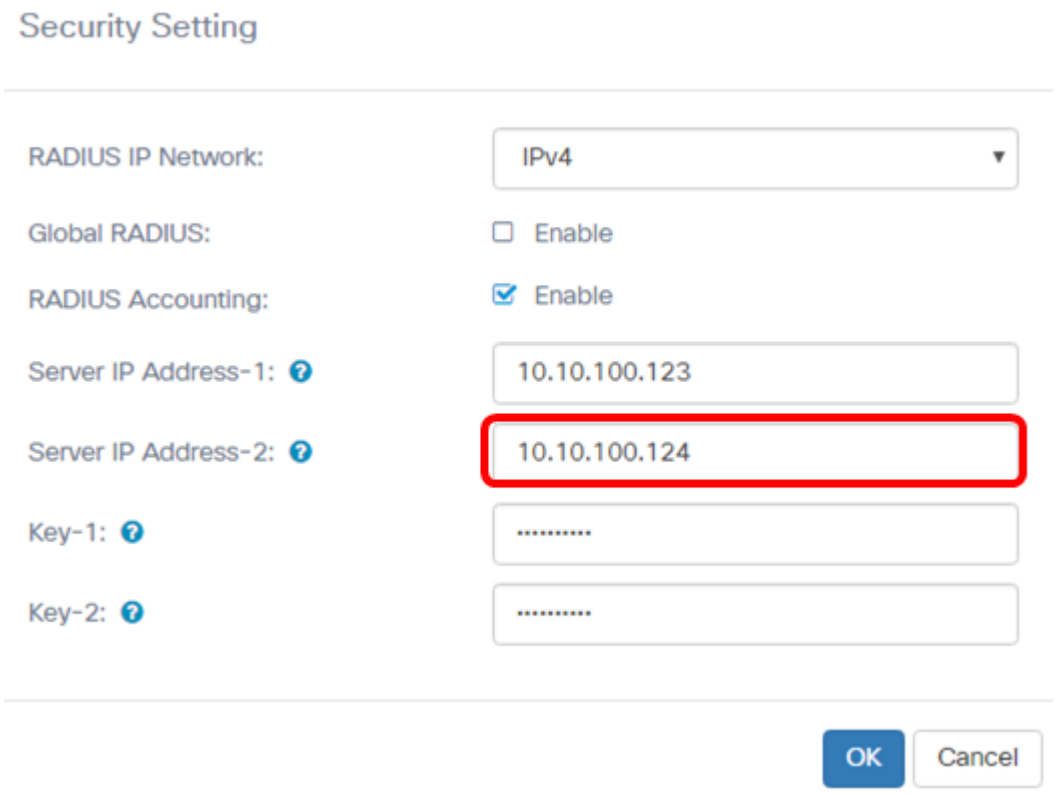


Paso 5. (Opcional) Introduzca la dirección IPv4 o IPv6 del servidor RADIUS primario en el campo *Server IP Address-1* (Dirección IP del servidor-1).



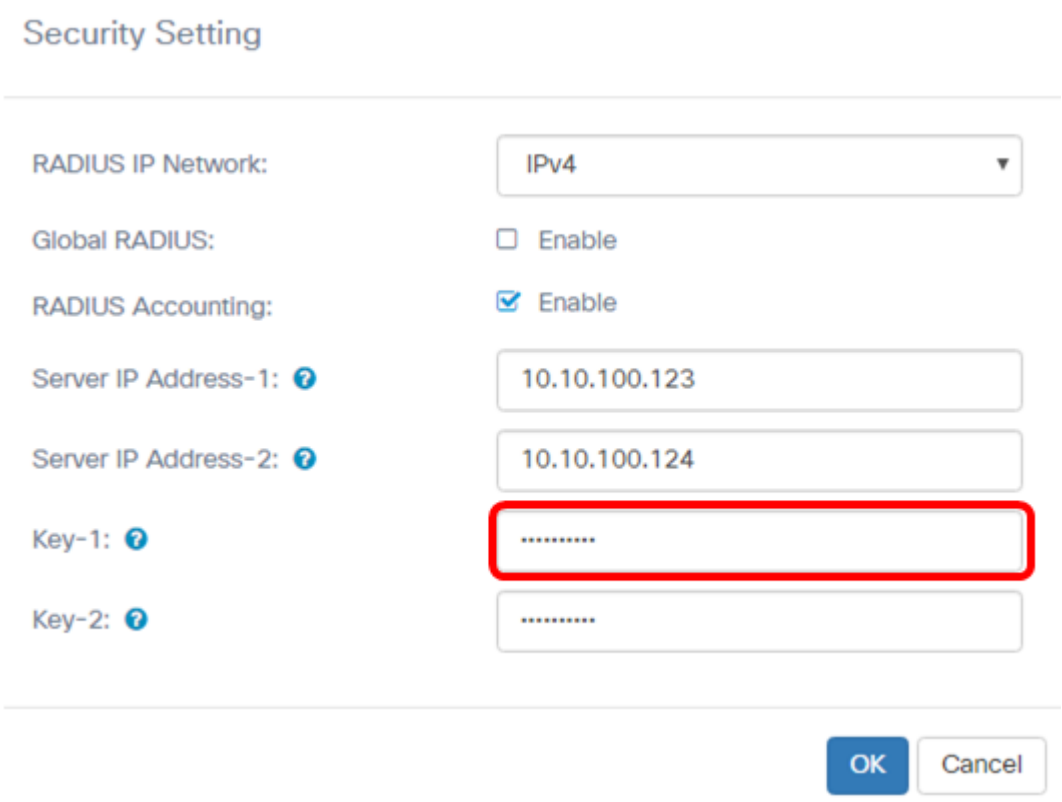
Nota: En este ejemplo, se ingresa 10.10.100.123.

Paso 6. (Opcional) Introduzca la dirección IPv4 o IPv6 del servidor RADIUS de respaldo en el campo *Server IP Address-2* (Dirección IP del servidor 2).

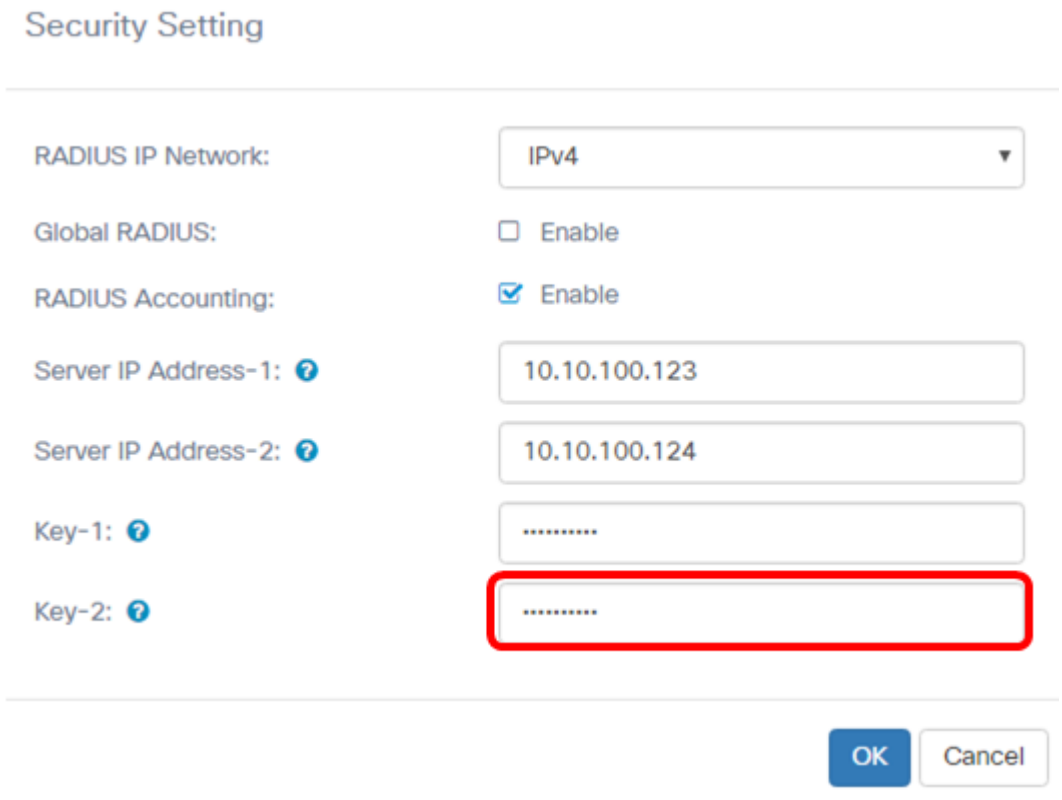


Nota: En este ejemplo, se ingresa 10.10.100.124.

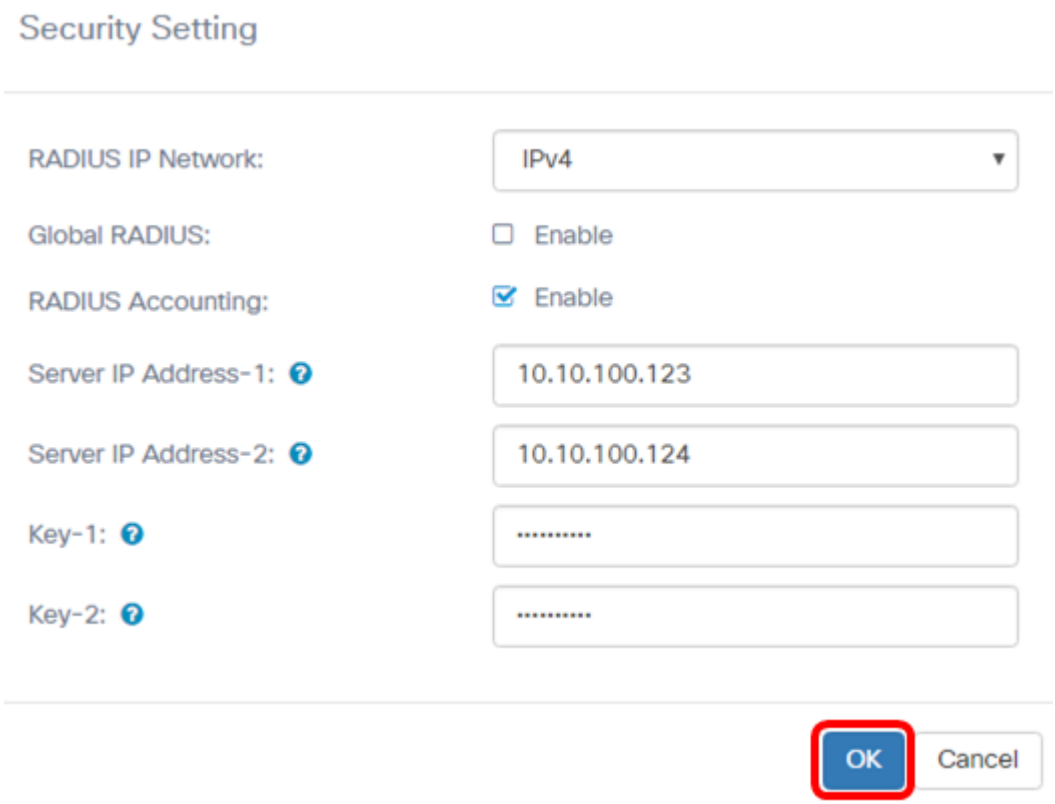
Paso 7. (Opcional) Introduzca la contraseña que el punto de acceso utiliza para autenticar el servidor RADIUS primario en el campo *Key-1*. La entrada en este campo distingue entre mayúsculas y minúsculas y debe coincidir con la entrada configurada en el servidor RADIUS primario. La clave puede tener hasta 63 caracteres alfanuméricos.



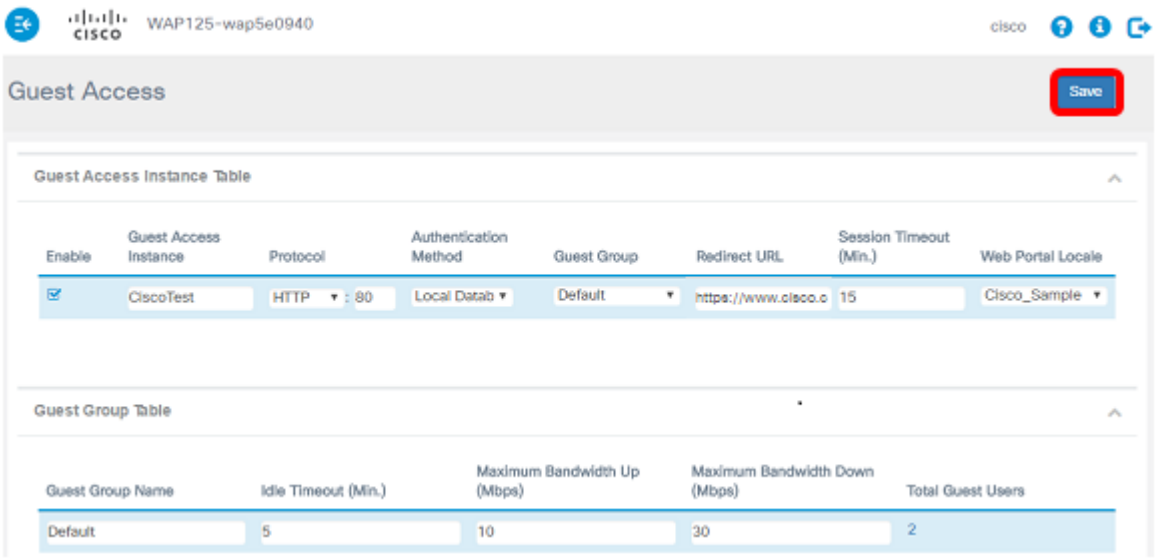
Paso 8. (Opcional) Introduzca la contraseña que el punto de acceso utiliza para autenticar el servidor RADIUS secundario en el campo *Key-2*. La entrada en este campo distingue entre mayúsculas y minúsculas y debe coincidir con la entrada configurada en el servidor RADIUS primario. La clave puede tener hasta 63 caracteres alfanuméricos.



Paso 9. Click OK.



Paso 10. Click **Save**.



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