Configure la tarea del servicio HTTP/HTTPS en un Punto de acceso WAP125 o WAP581

Objetivo

El Protocolo de transporte de hipertexto seguro (HTTPS) es un protocolo transfer que es más seguro que el HTTP. El Punto de acceso se puede manejar a través del HTTP y de las conexiones HTTPS cuando se configuran los servidores HTTP/HTTPS. Algunos buscadores Web utilizan el HTTP mientras que otros utilizan el HTTPS. Un Punto de acceso debe tener un certificado válido del Secure Socket Layer (SSL) para utilizar los servicios HTTPS.

¿Por qué necesitamos configurar la tarea del servicio HTTP/HTTPS?

Esta característica es útil para guardar hacia fuera los host rogue de acceder la utilidad basada en web. Usando la lista de control de acceso de la Administración, permite que usted especifique hasta 10 IP Addresses, cinco para el IPv4 y cinco para que el IPv6 tenga acceso a la utilidad basada en web.

El objetivo de este documento es mostrarle cómo fortificar su red por que usted muestra cómo configurar la tarea del servicio HTTP/HTTPS en el WAP125.

Dispositivos aplicables

- WAP125
- WAP581

Versión del software

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

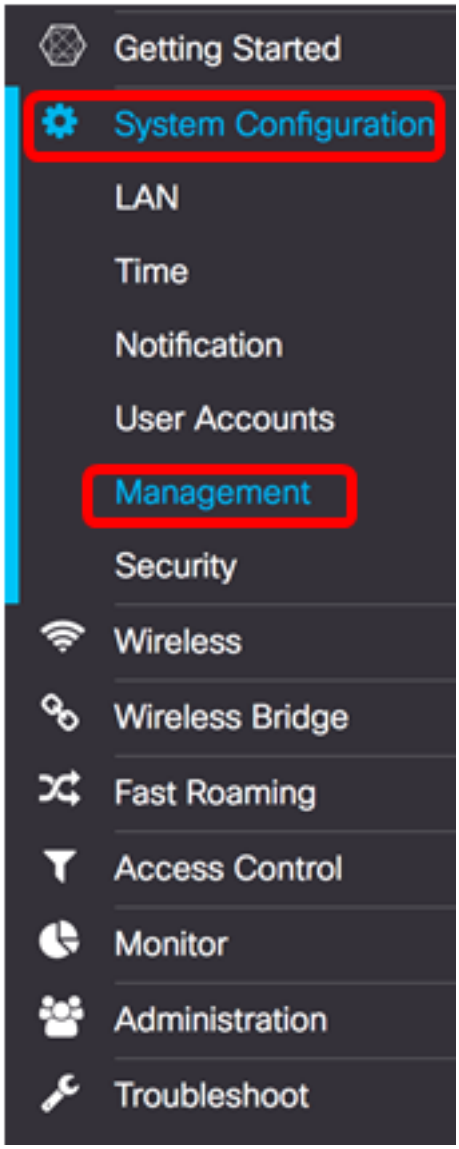
Recopile la información de servicio técnico

Paso 1. Inicie sesión a la utilidad basada en web de su WAP. El nombre de usuario predeterminado y la contraseña es Cisco/Cisco.

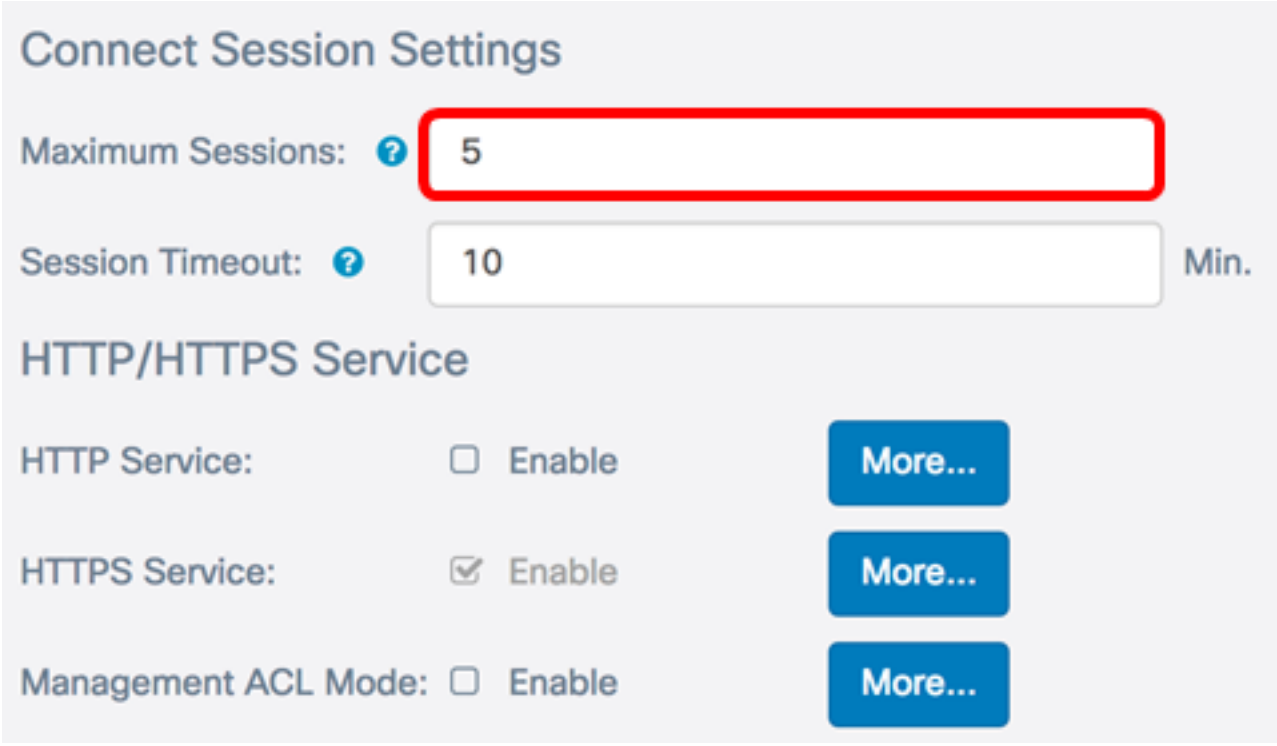
Nota: Si usted ha cambiado la contraseña o ha creado ya una nueva cuenta, ingrese sus nuevas credenciales en lugar de otro.

Paso 2. Elija la **configuración del sistema > la Administración**.

Nota: Las opciones disponibles pueden variar dependiendo del modelo exacto de su dispositivo. En este ejemplo, se utiliza WAP125.

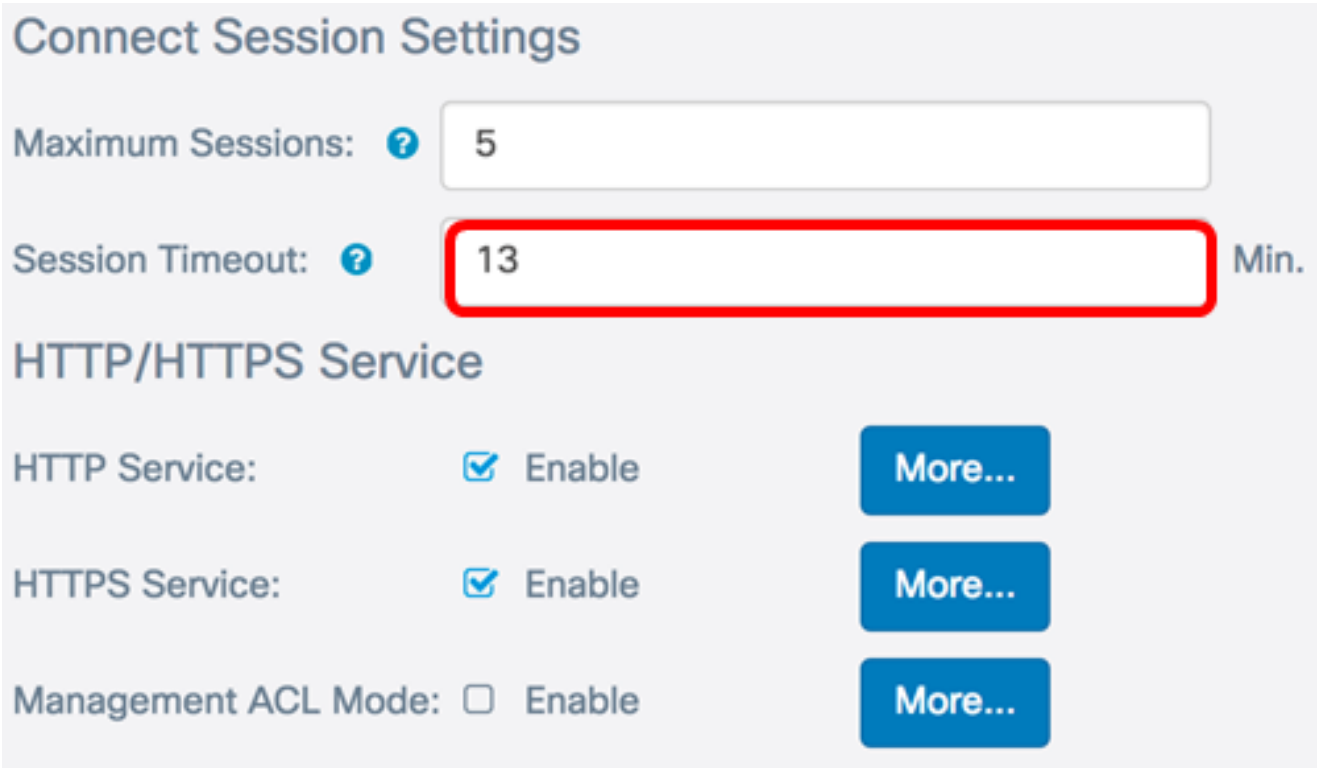


Paso 3. En las *sesiones máximas* coloque debajo conectan las Configuraciones de la sesión, ingresan un valor a partir de la 1 a 10 para fijar al número máximo de sesiones web simultáneas. Se crea una sesión cada vez que un usuario abre una sesión al dispositivo. Si entonces alcanzan a la sesión máxima rechazan al usuario siguiente que intenta abrir una sesión en el dispositivo con el servicio HTTP o HTTPS. El valor predeterminado es 5.



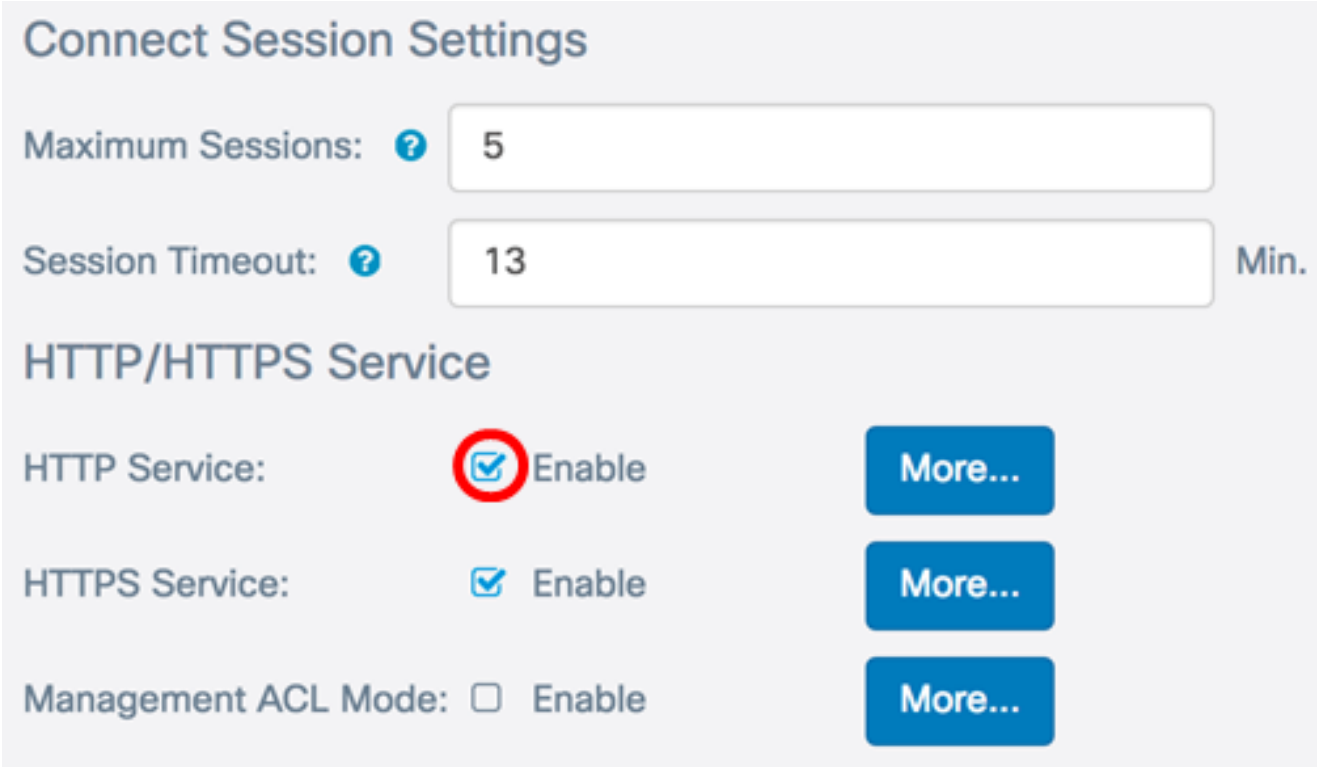
Paso 4. En el campo del *tiempo de espera de la sesión*, ingrese un valor entre 2 y 60 minutos para fijar la hora que la sesión web puede seguir siendo ociosa. El valor predeterminado es 10 minutos.

Nota: En este ejemplo, se utiliza 13.

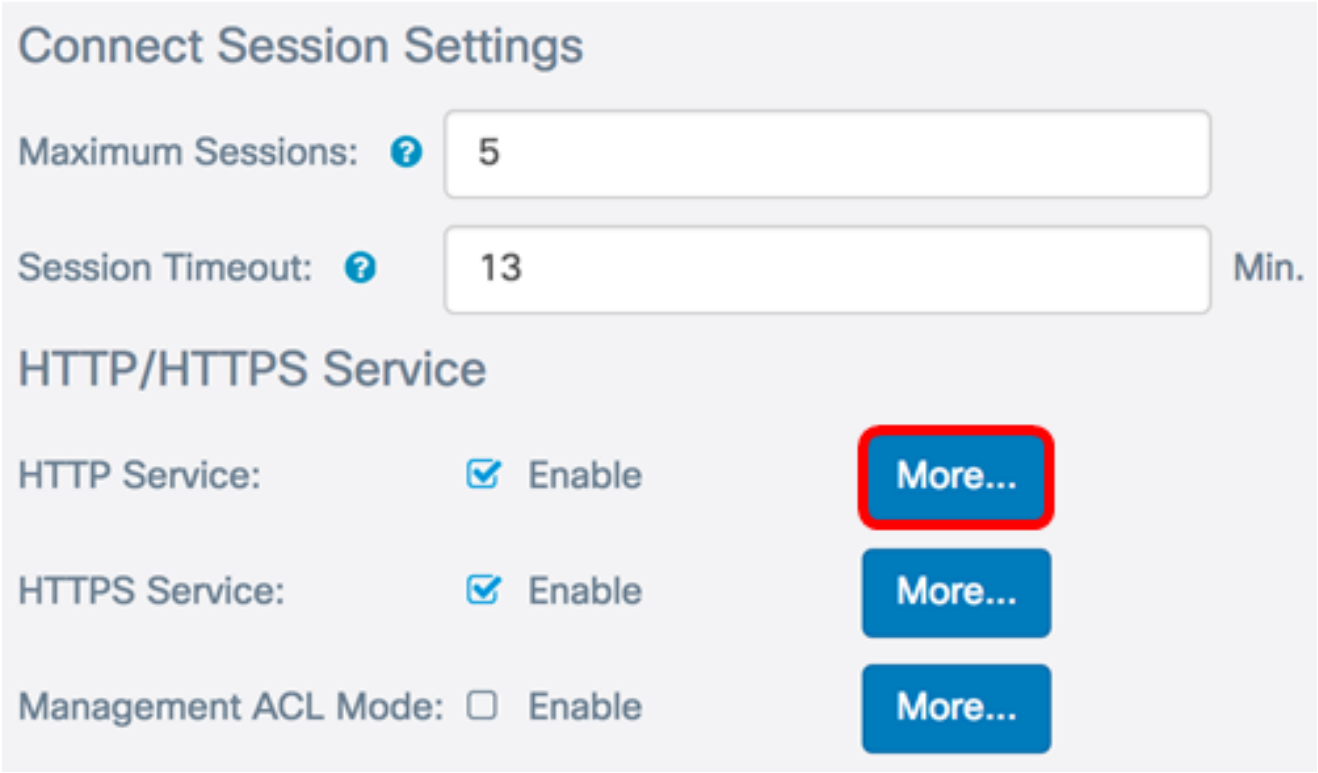


Servicio HTTP

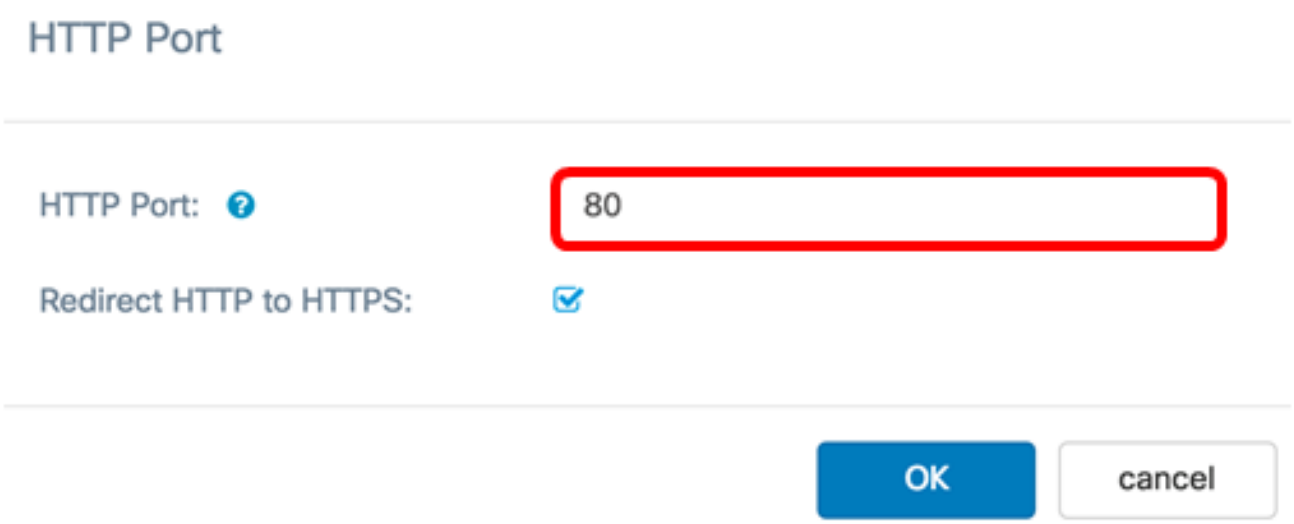
Paso 5. Marque la casilla de verificación del servicio del **permiso** HTTP para permitir que las sesiones web sean conectadas con el HTTP.



Tecleo (opcional) del paso 6. **más** para ver más opciones y para configurar un número del puerto.

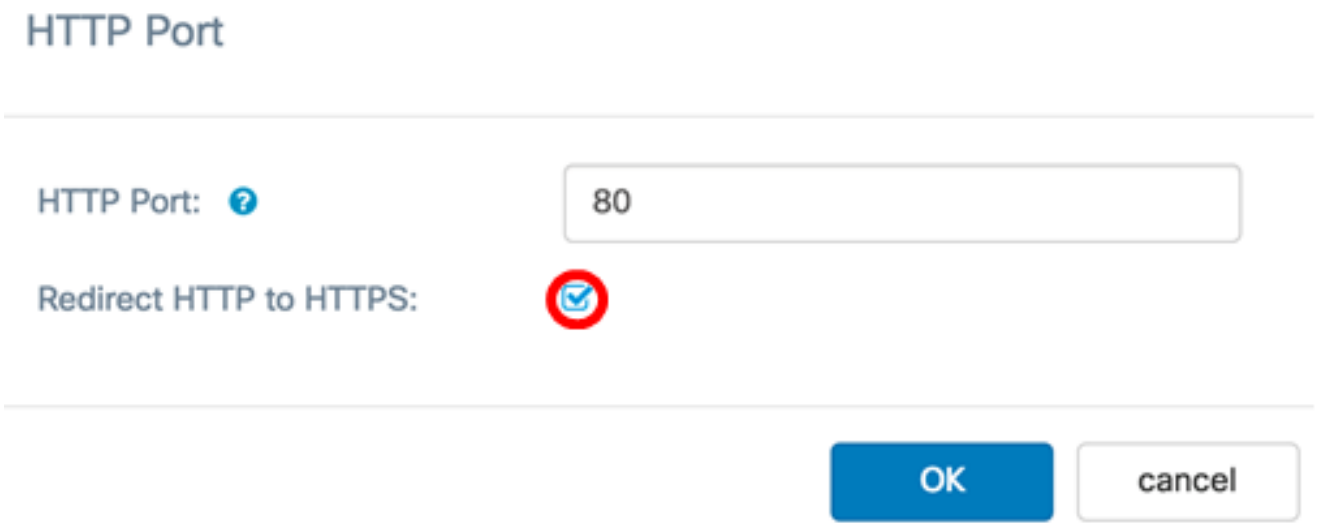


Paso 7. En el campo de *puerto HTTP*, ingrese un número del puerto lógico para utilizar para las conexiones HTTP. El valor de puerto se extiende a partir de 1025 a 65535. El puerto conocido predeterminado para las conexiones HTTP es 80.

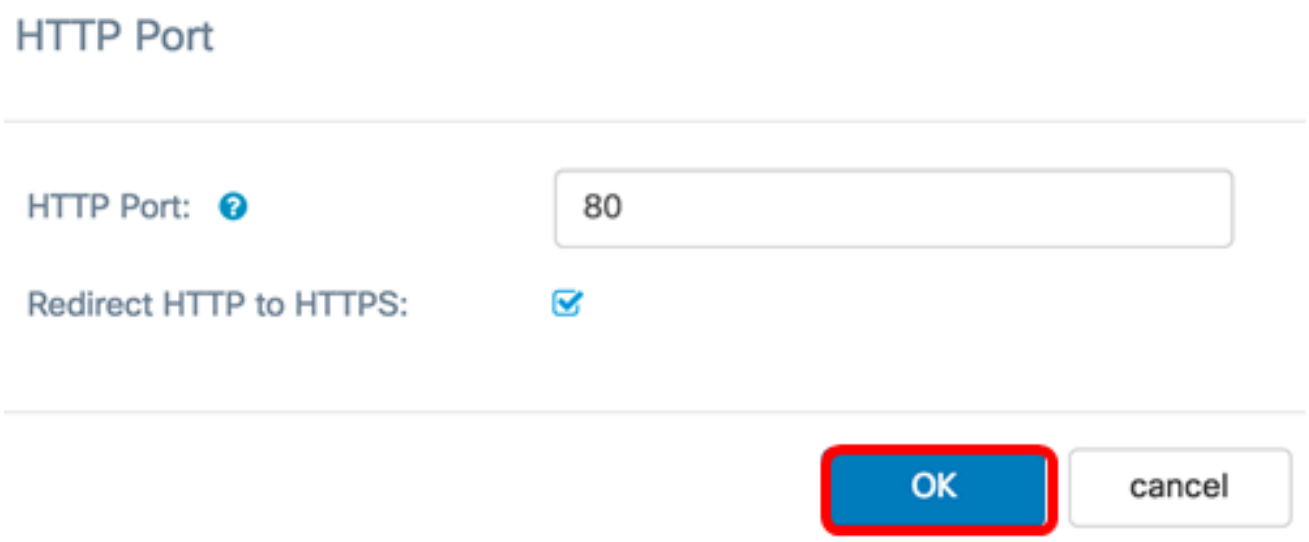


Control (opcional) del paso 8. la **reorientación HTTP a casilla de verificación HTTPS** para permitir que el navegador le reoriente a un protocolo más seguro, HTTPS sobre el establecimiento de una sesión web.

Nota: Esta opción está solamente disponible si la casilla de verificación del servicio HTTP se inhabilita en el paso 4. En este ejemplo, se marca esta opción.



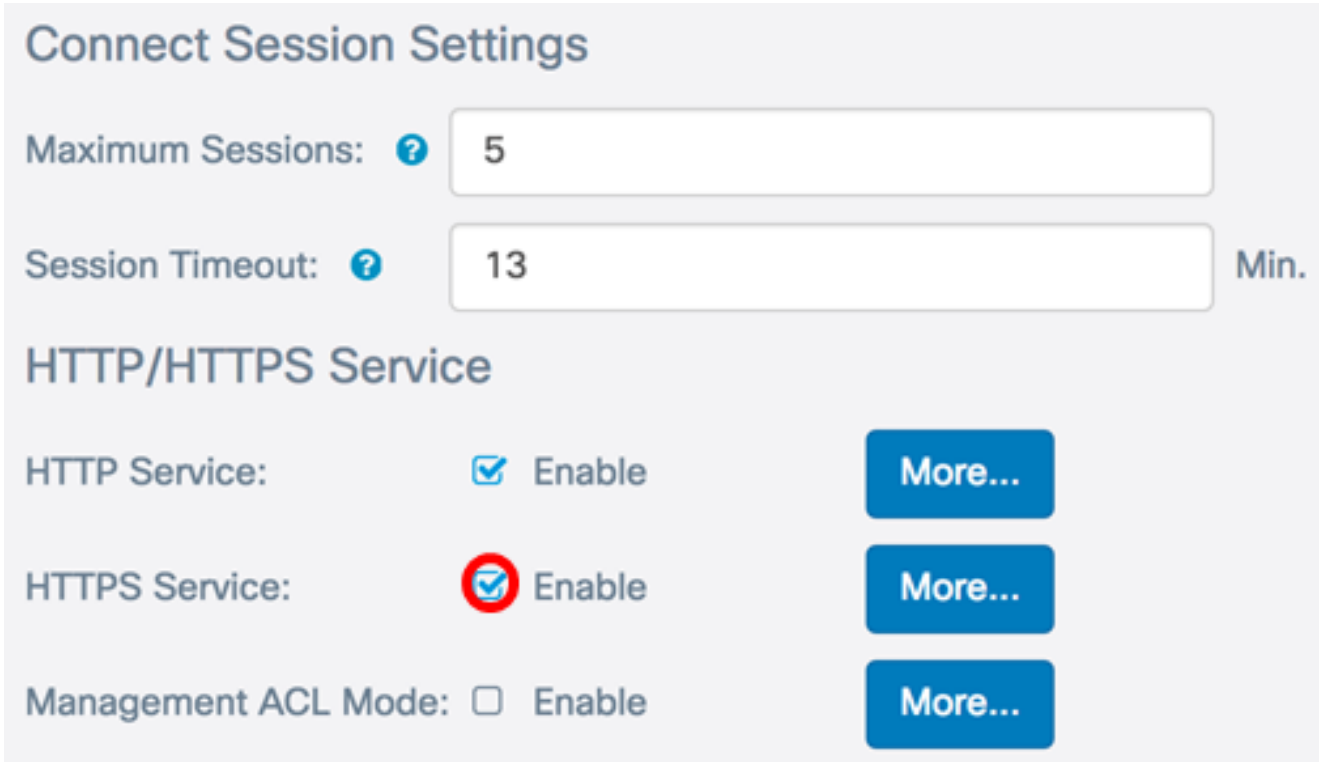
Paso 9. Haga Click en OK a volver a la página de la Administración y a continuar con la configuración.



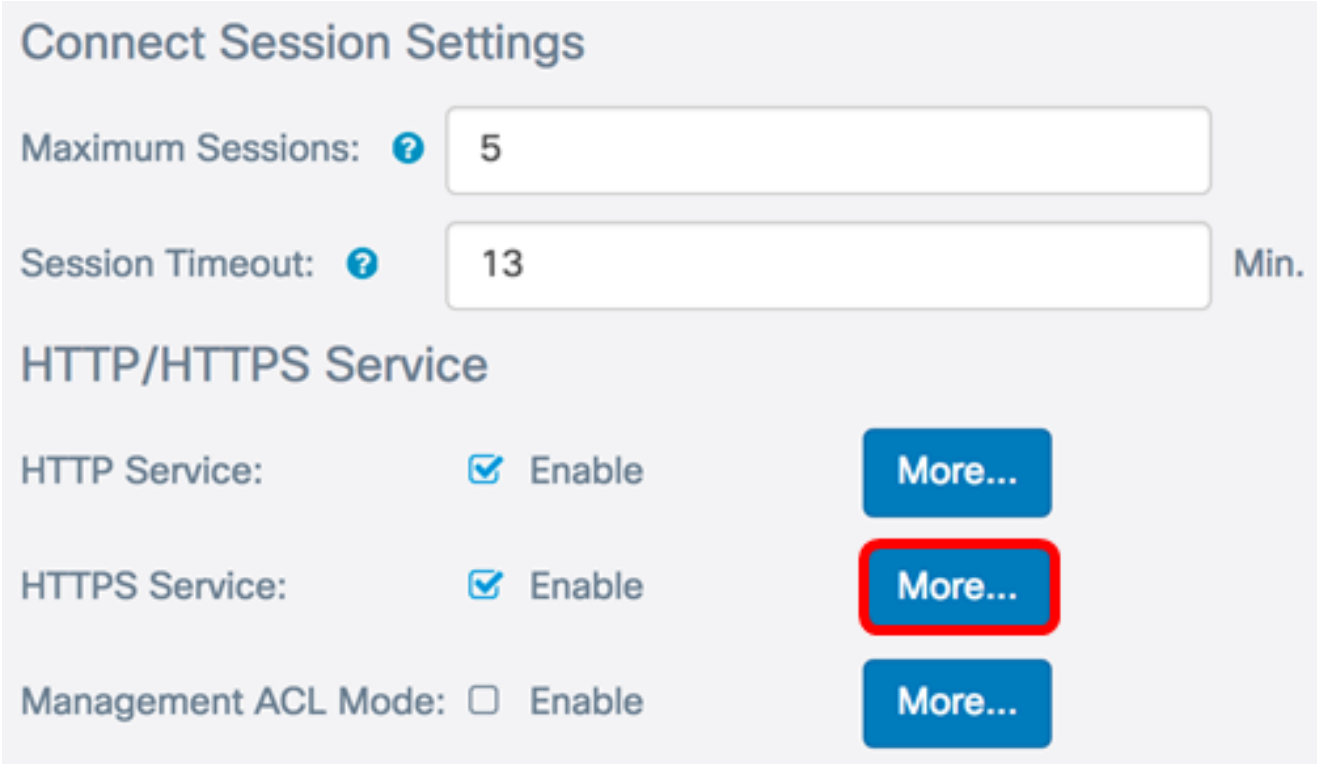
Servicio HTTPS

Paso 10. Marque la casilla de verificación del servicio del **permiso** HTTPS para permitir que establezcan a las sesiones web con un protocolo asegurado, HTTPS. Esta opción se habilita por abandono.

Nota: Si se inhabilita esta opción, cualquier conexión existente usando el HTTPS es disconnected.



Paso 11 Haga clic **más** para definir un puerto que se utilizará por el HTTPS y para elegir las versiones de Transport Layer Security que se utilizarán en el HTTPS.

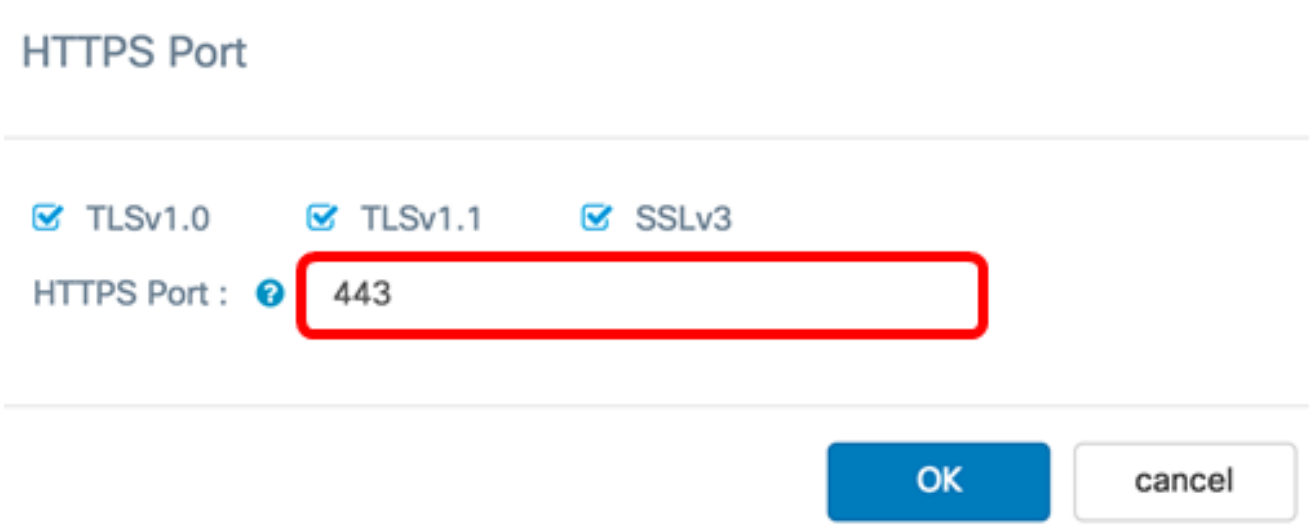


Paso 12. Bajo zona portuaria HTTPS, marque las casillas de verificación de los protocolos de Seguridad siguientes que se utilizan sobre el HTTPS:

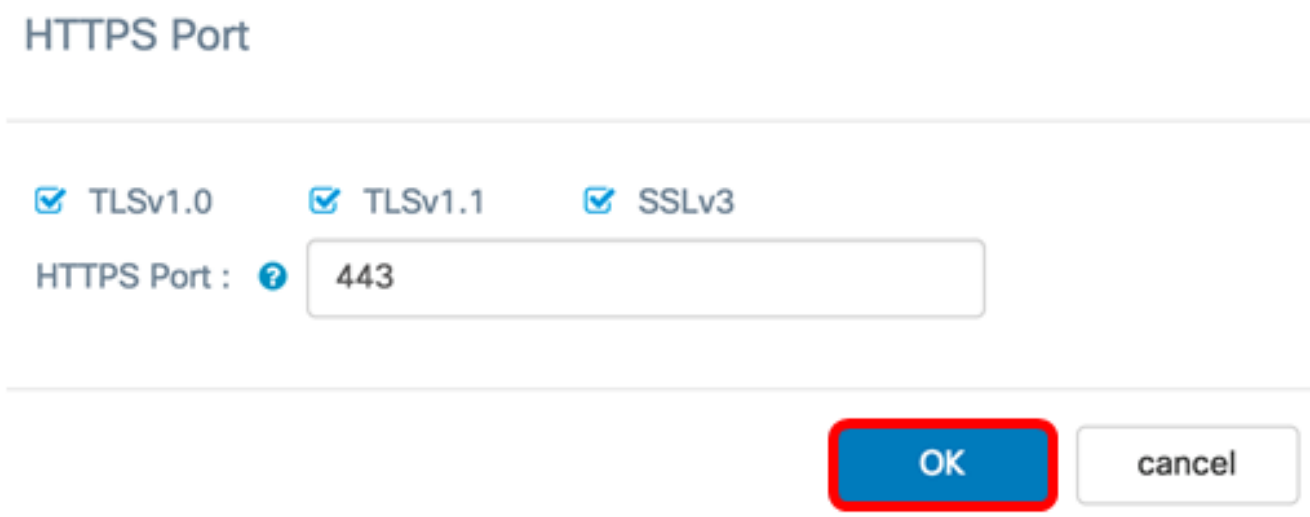
- TLSv1.0 — La versión 1 (TLSv1) de Transport Layer Security es un protocolo criptográfico que proporciona la Seguridad y la integridad de los datos para la comunicación sobre Internet.
- TLSv1.1 — Una versión mejorada de la primera versión del TSLv1, mejora la seguridad de datos y la integridad para la comunicación.
- SSLv3 — El Socket Layer asegurado versión 3 (SSLv3) es un protocolo que se utiliza sobre el HTTPS para establecer las sesiones y la comunicación aseguradas sobre Internet.

Nota: En este ejemplo, se marcan todas las casillas de verificación.

Paso 13. En el campo de *puerto HTTPS*, ingrese un número del puerto lógico para utilizar para las conexiones HTTPS. El puerto conocido predeterminado es 443.

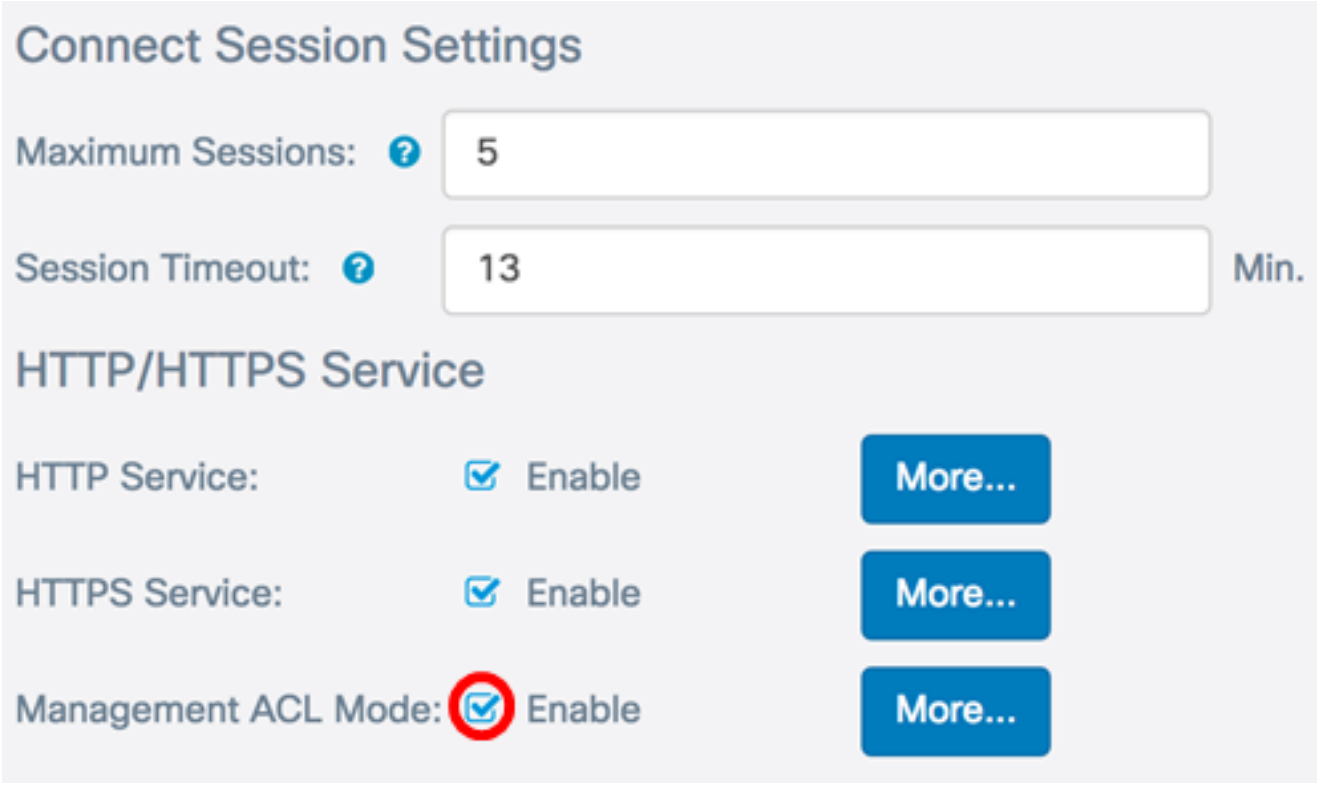


Paso 14. Para continuar, haga clic en OK (Aceptar).

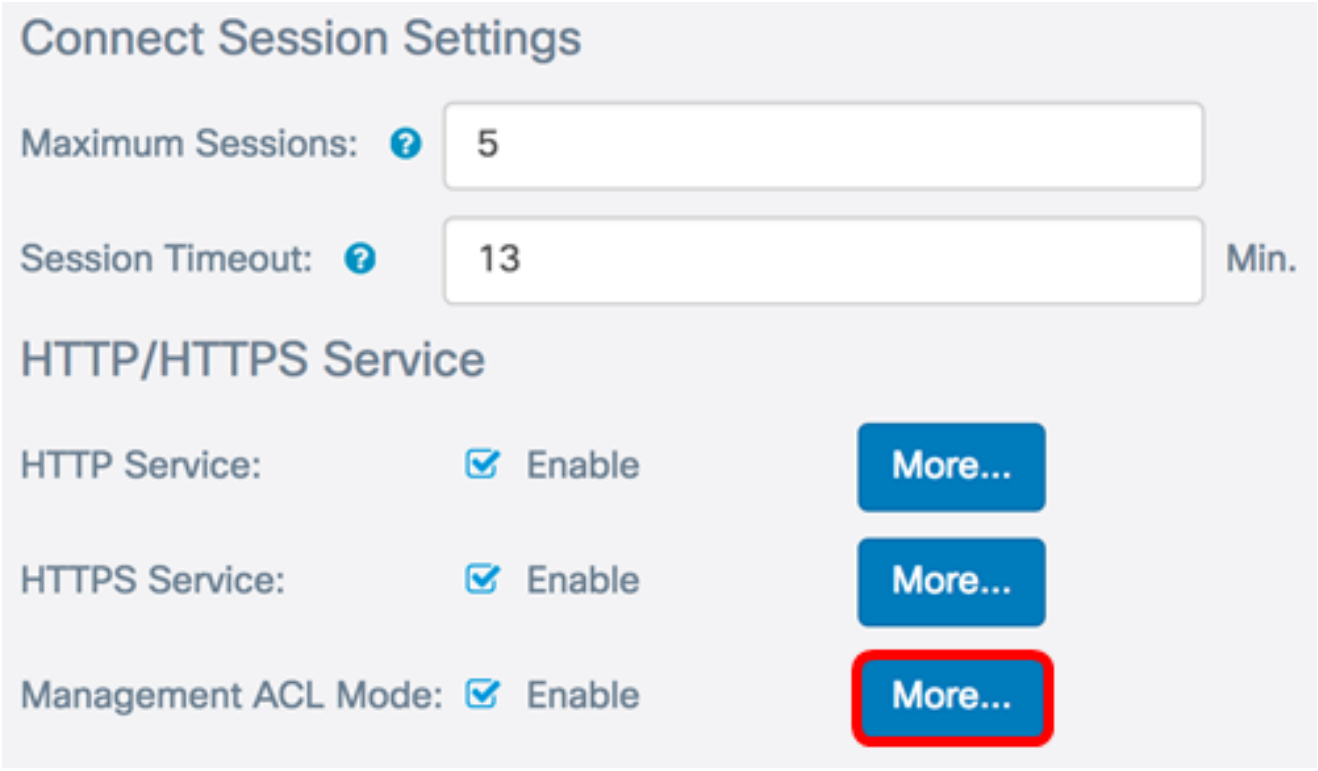


Modo de la Administración ACL

Paso 15. Marque la casilla de verificación del modo del **permiso** ACL para especificar una lista de control de acceso (ACL) de IP Addresses que se permite para acceder la utilidad basada en web. Si se inhabilita esta característica, después ésta concede el acceso a la utilidad basada en web.



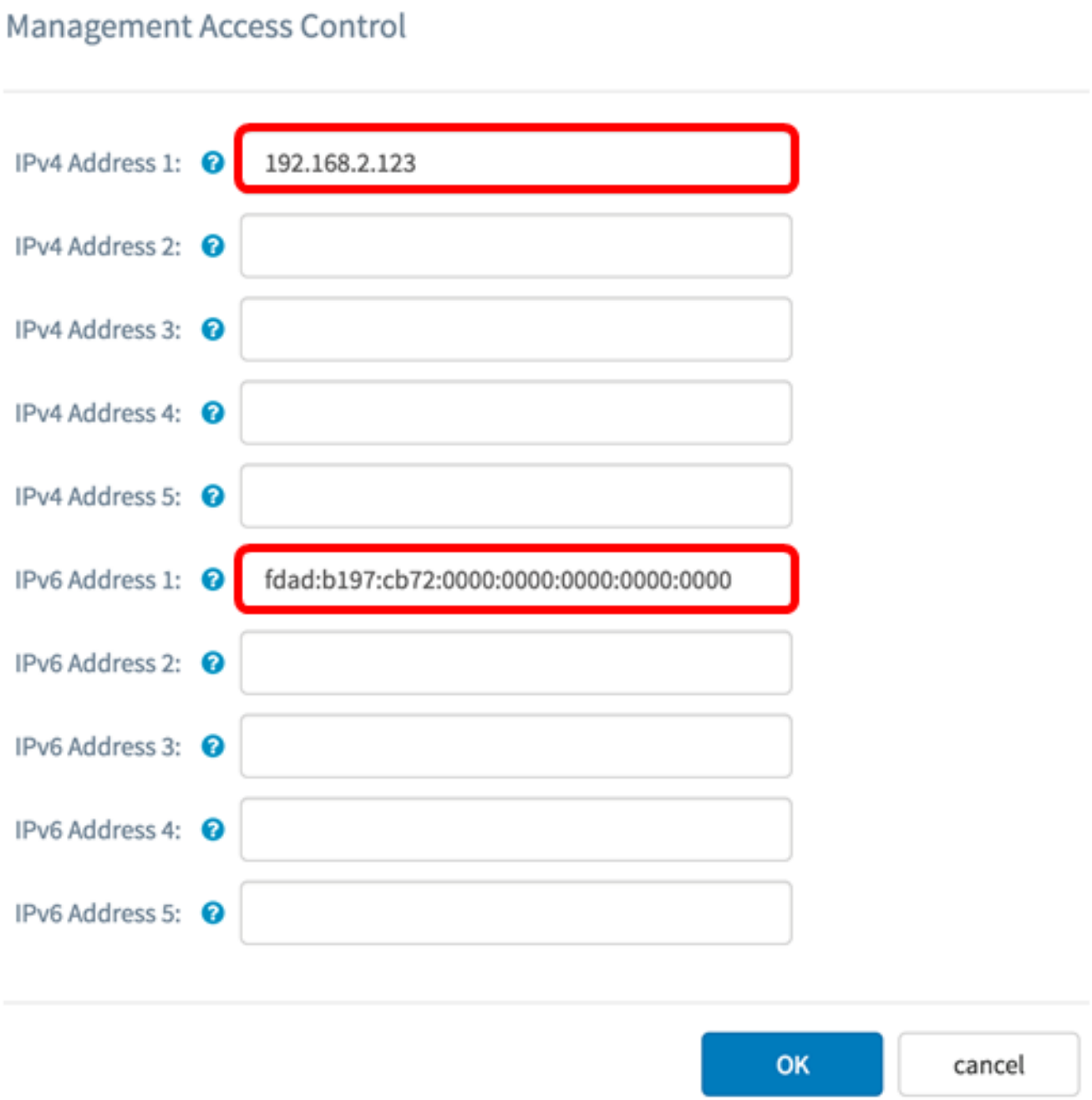
Paso 16. Haga clic **más** para especificar una lista de direccionamientos del IPv4 y del IPv6 permitidos para acceder la utilidad basada en web.



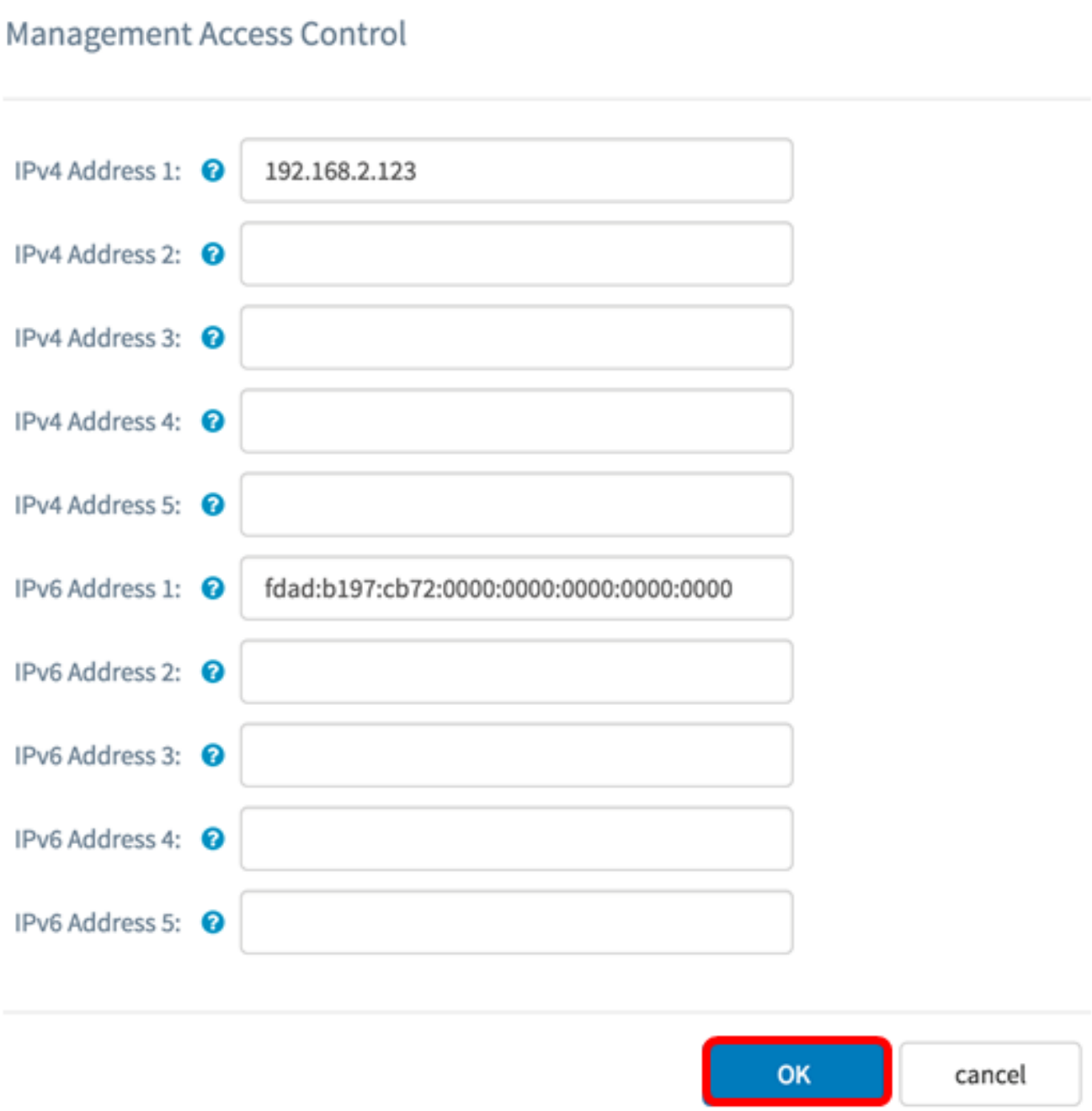
Paso 17. En el *direccionamiento del IPv4* y los *campos de dirección del IPv6*, ingrese los IP Addresses administrativos en los formatos respectivos que serán concedidos el acceso a la utilidad basada en web.

Consejo: Asigne los IP Address estáticos a los IP Addresses administrativos.

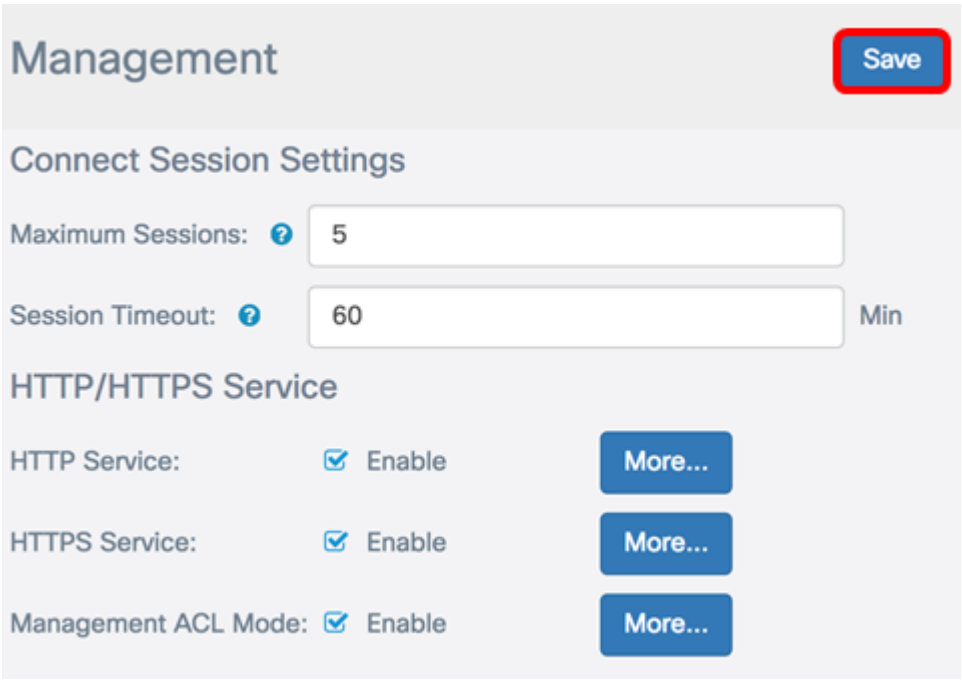
Nota: En este ejemplo, se utiliza 192.168.2.123 mientras que el direccionamiento del IPv4 y el fdad:b197:cb72:0000:0000:0000:0000:0000 administrativos se utiliza como el direccionamiento administrativo del IPv6.



Paso 18. Click OK.



Paso 19. **Botón Save Button del** tecleo para salvar las configuraciones configuradas.



Usted debe ahora haber configurado con éxito la tarea del servicio HTTP/HTTPS en su Punto de acceso WAP125 o WAP581.