Parámetros inalámbricos básicos en el router VPN CVR100W

Objetivo

Una red de área local inalámbrica (WLAN) utiliza la comunicación de radio para conectar dispositivos inalámbricos a una LAN. Un ejemplo es un hotspot Wi-Fi en una cafetería. Las redes inalámbricas son útiles, ya que reducen los costes de cableado y resulta fácil de configurar.

En este artículo se explica cómo configurar los parámetros inalámbricos básicos en el router VPN CVR100W, que incluye la configuración de la seguridad de la red. Para ver los parámetros inalámbricos avanzados, consulte el artículo *Configuración inalámbrica avanzada en el router VPN CVR100W*.

Dispositivo aplicable

Router VPN · CVR100W

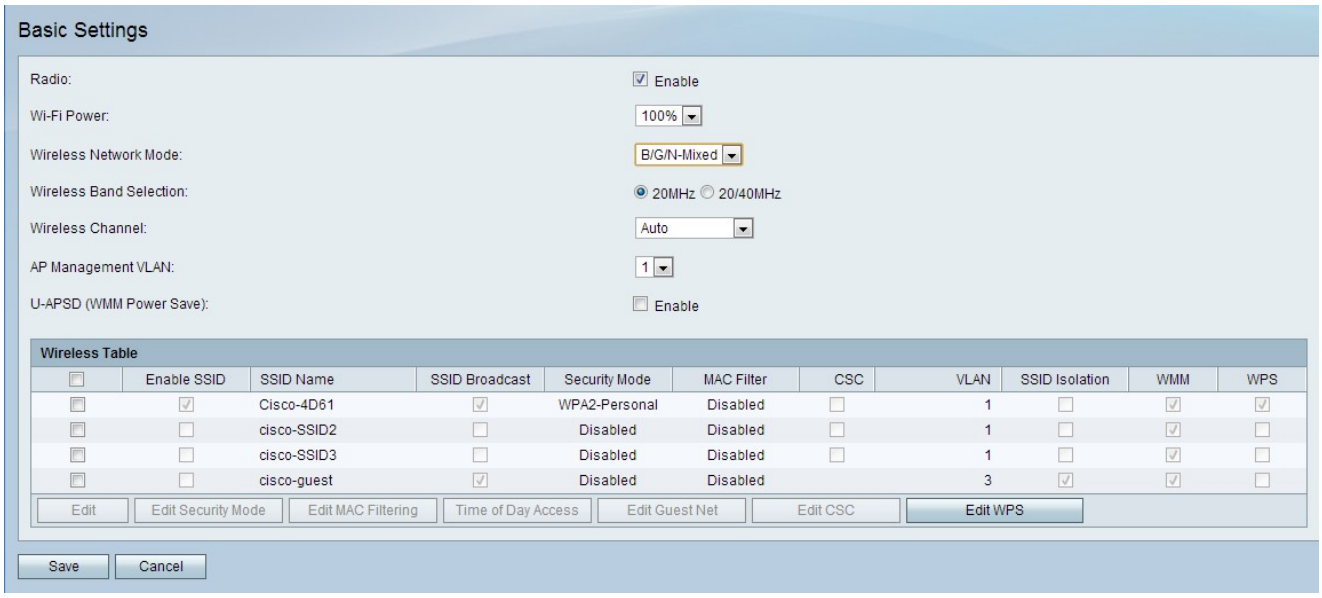
Versión del software

•1.0.1.19

Configuración básica

Configuración general

Paso 1. Inicie sesión en la utilidad de configuración web y elija **Wireless > Basic Settings**. Se abre la página *Basic Settings*:



Paso 2. Marque la casilla de verificación **Enable** en el campo Radio para activar la radio inalámbrica.

Paso 3. En la lista desplegable Wi-Fi Power (Alimentación Wi-Fi), seleccione la fuente de alimentación inalámbrica. Esta potencia wi-fi controla la potencia del transmisor de la radio wi-fi. Esta función es útil para reducir o aumentar el alcance de la señal. Esta función se utiliza para conservar la alimentación.

·100%: esta opción permite un 100% de potencia de radio transmisor.

·50%: esta opción permite un 50% de potencia del transmisor de radio.

Paso 4. En la lista desplegable Wireless Network Mode (Modo de red inalámbrica), seleccione el modo inalámbrico. Esta opción se basa en las capacidades inalámbricas de los dispositivos de la red.

·B/G/N-Mixed: la red consta de una combinación de dispositivos Wireless-B, Wireless-G y Wireless-N.

·B-Only: la red consta únicamente de dispositivos Wireless-B.

·G-Only: la red consta únicamente de dispositivos Wireless-G.

·Sólo N: la red consta únicamente de dispositivos Wireless-N.

·B/G-Mixed: la red consta de una combinación de dispositivos Wireless-B y Wireless-G.

·G/N mixto: la red consta de una combinación de dispositivos Wireless-G y Wireless-N.

Paso 5. Si el modo de red consta de dispositivos Wireless-N, haga clic en el botón de opción que corresponde al ancho de banda deseado de la señal inalámbrica en el campo Selección de banda inalámbrica. El mayor ancho de banda indica la mayor cantidad de datos que puede transportar la señal.

·20 MHz: frecuencia estándar para una señal inalámbrica.

·20/40 MHz: utiliza automáticamente una señal de 20 MHz y 40 MHz. Una señal de 40 MHz proporciona más ancho de banda, pero es susceptible a más interferencias. Esta opción sólo se utiliza si los dispositivos inalámbricos conectados son compatibles con la frecuencia de 40 MHz.

Paso 6. En la lista desplegable Wireless Channel (Canal inalámbrico), seleccione un canal inalámbrico para la radio. Elija un canal que no esté siendo utilizado actualmente por las redes vecinas. Si varias radios utilizan el mismo canal, podría producirse una interferencia.

Paso 7. En la lista desplegable AP Management VLAN, elija la VLAN de administración. La VLAN de administración es la VLAN utilizada para la administración de dispositivos desde una ubicación remota.

Paso 8. (Opcional) Para habilitar la entrega automática de ahorro de energía no programada (U-APSD), marque **Enable** en el campo U-APSD. U-APSD es una función que permite que la radio conserve energía. Sin embargo, U-APSD puede reducir el rendimiento de la radio.

Paso 9. Click **Save**.

Editar tabla inalámbrica

Paso 1. Active la casilla de verificación de la red que desea editar en la tabla inalámbrica.

Paso 2. Haga clic en **Editar** para editar la red especificada.

Paso 3. Marque la casilla **Enable SSID** para habilitar la red. Service Set Identifier (SSID) es el nombre de la red inalámbrica.

Paso 4. En el campo SSID Name (Nombre de SSID), introduzca el nombre de la red. Todos los dispositivos de la red utilizan este SSID para comunicarse entre sí.

Paso 5. Marque la casilla de verificación **SSID Broadcast** para habilitar la difusión inalámbrica. Cuando se habilita la difusión SSID, la disponibilidad del router VPN CVR100W se anuncia a los dispositivos inalámbricos cercanos.

Paso 6. (Opcional) Para editar el modo de seguridad, consulte Editar modo de seguridad.

Paso 7. (Opcional) Para editar el filtro MAC, consulte Editar filtrado de MAC.

Paso 8. (Opcional) Para activar Cisco Simple Connect (CSC), marque la casilla de verificación **CSC**. CSC facilita la configuración de una red inalámbrica y facilita la conexión de dispositivos inalámbricos a la red. El dispositivo inalámbrico utiliza CSC para obtener el SSID y la contraseña de la red, lo que permite la conexión automática a la red. Para editar el CSC, consulte Editar CSC.

Nota: La VLAN de Cisco Simple Connect no puede ser la misma que la VLAN actual o de otro SSID.

Paso 9. En la lista desplegable VLAN, elija la VLAN asociada a la red.

Paso 10. Marque la casilla de verificación **Aislamiento de SSID** para evitar que los dispositivos en la red especificada se comuniquen entre sí.

Paso 11. Compruebe **WMM** para activar Wi-Fi Multimedia (WMM) en la red. WMM se utiliza para mejorar la transmisión multimedia a través de dispositivos inalámbricos. Se da mayor prioridad al tráfico multimedia que se envía a través de una conexión inalámbrica cuando se habilita WMM.

Paso 12. Marque **WPS** para asignar la red especificada como una red de configuración Wi-Fi protegida (WPS). WPS es una función que permite una configuración de red sencilla y segura. Esta función permite que los dispositivos se conecten fácilmente a la red.

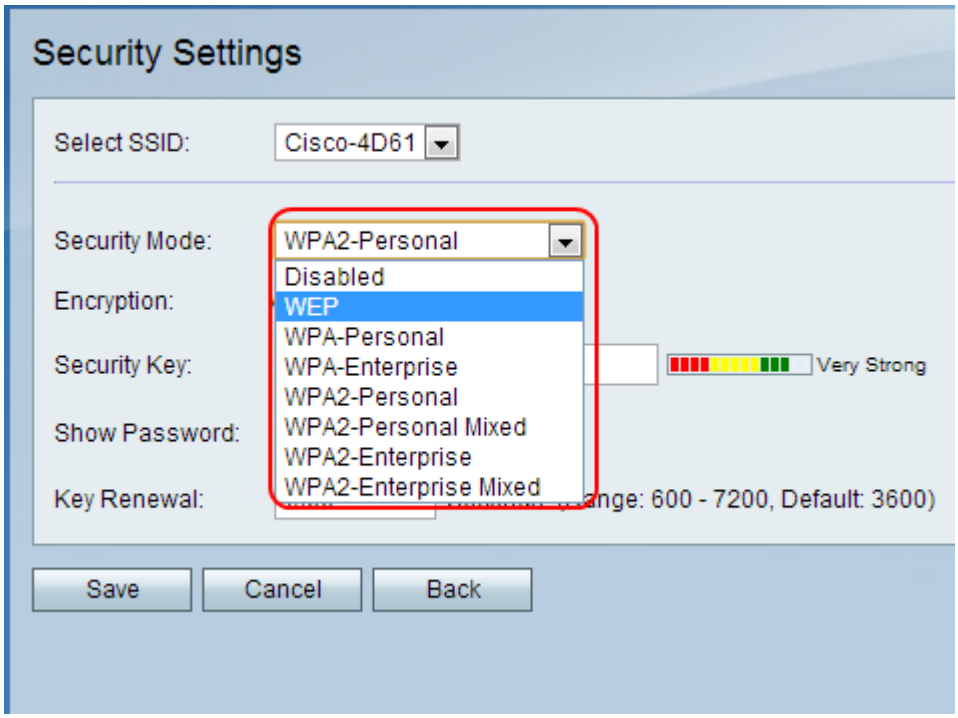
Nota: Para configurar WPS en el router VPN CVR100W, consulte el artículo *Configuración WiFi protegida (WPS) en el router VPN CVR100W*.

Paso 13. Click **Save**.

Editar modo de seguridad

Paso 1. Active la casilla de verificación de la red que desea editar en la tabla inalámbrica.

Paso 2. Haga clic en **Editar modo de seguridad** para editar la seguridad de la red especificada. Se abre la página *Configuración de seguridad*.



Paso 3. (Opcional) Para cambiar el SSID para el que desea configurar la seguridad, elija el SSID deseado en la lista desplegable Seleccionar SSID.

Paso 4. En la lista desplegable Modo de seguridad, elija el modo de seguridad que desea configurar.

·Disable Security: esta opción inhabilita la seguridad en el router VPN CVR100W.

·WEP Security: Wired Equivalent Privacy (WEP) es un algoritmo utilizado para proteger una red inalámbrica. WEP se utiliza para proporcionar un método de encriptación básico que es menos seguro que WPA. WEP se utiliza cuando los dispositivos de red conectados no admiten WPA.

·Seguridad WPA-Personal: el acceso Wi-Fi protegido (WPA) es un estándar de seguridad para las redes inalámbricas. WPA-Personal es una versión de WPA que se utiliza para redes que constan de unos pocos usuarios. WPA-Personal proporciona una clave compartida que cada usuario utiliza para acceder a la red inalámbrica. WPA se introdujo con los métodos de encriptación clave Temporal Key Integrity Protocol (TKIP) y Advanced Encryption Standard (AES).

·WPA-Enterprise Security: WPA-Enterprise es una versión de WPA recomendada para una red formada por numerosos usuarios. La autenticación para obtener acceso a la red está controlada por un servidor RADIUS. A cada usuario conectado se le da una clave única para acceder a la red inalámbrica. WPA se introdujo con los métodos de encriptación clave Temporal Key Integrity Protocol (TKIP) y Advanced Encryption Standard (AES).

·Seguridad WPA2-Personal: WPA2 es una mejora de WPA y proporciona más seguridad que WPA. WPA2-Personal es una versión de WPA2 que se utiliza para redes con pocos usuarios. WPA2-Personal es más seguro que WPA2-Personal Mixed. WPA2-Personal proporciona una clave compartida que todos los usuarios utilizan para acceder a la red inalámbrica.

·WPA2-Personal Mixed Security: WPA2-Personal Mixed es una versión de WPA2 que se utiliza para redes con pocos usuarios. WPA2-Personal Mixed admite compatibilidad con versiones anteriores para dispositivos antiguos que no pueden utilizar WPA2. WPA2-Personal Mixed es una conexión menos segura.

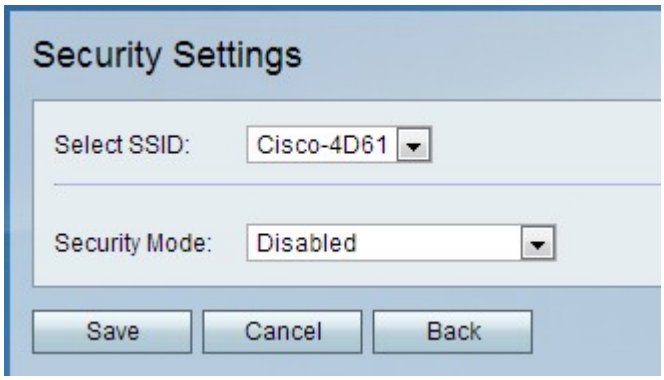
·WPA2-Enterprise Security: WPA2-Enterprise es una versión de WPA2 que se utiliza para redes con numerosos usuarios. WPA2-Enterprise es más seguro que WPA2-Enterprise mixto. La autenticación utilizada para obtener acceso es controlada por un servidor RADIUS. Esto significa que a cada usuario conectado se le dará una clave única para acceder a la red inalámbrica.

·WPA2-Enterprise Mixed Security: WPA2-Enterprise Mixed son versiones de WPA2 que se utilizan para redes con numerosos usuarios. WPA2-Enterprise Mixed admite compatibilidad con versiones anteriores para dispositivos antiguos que no pueden utilizar WPA2. WPA2-Enterprise Mixed proporciona una conexión menos segura que WPA2-Enterprise. La autenticación utilizada para obtener acceso es controlada por un servidor RADIUS. Esto significa que a cada usuario conectado se le dará una clave única para acceder a la red inalámbrica.

Desactivar seguridad

La seguridad inalámbrica puede desactivarse en el router VPN CVR100W para facilitar su uso al configurar redes de prueba.

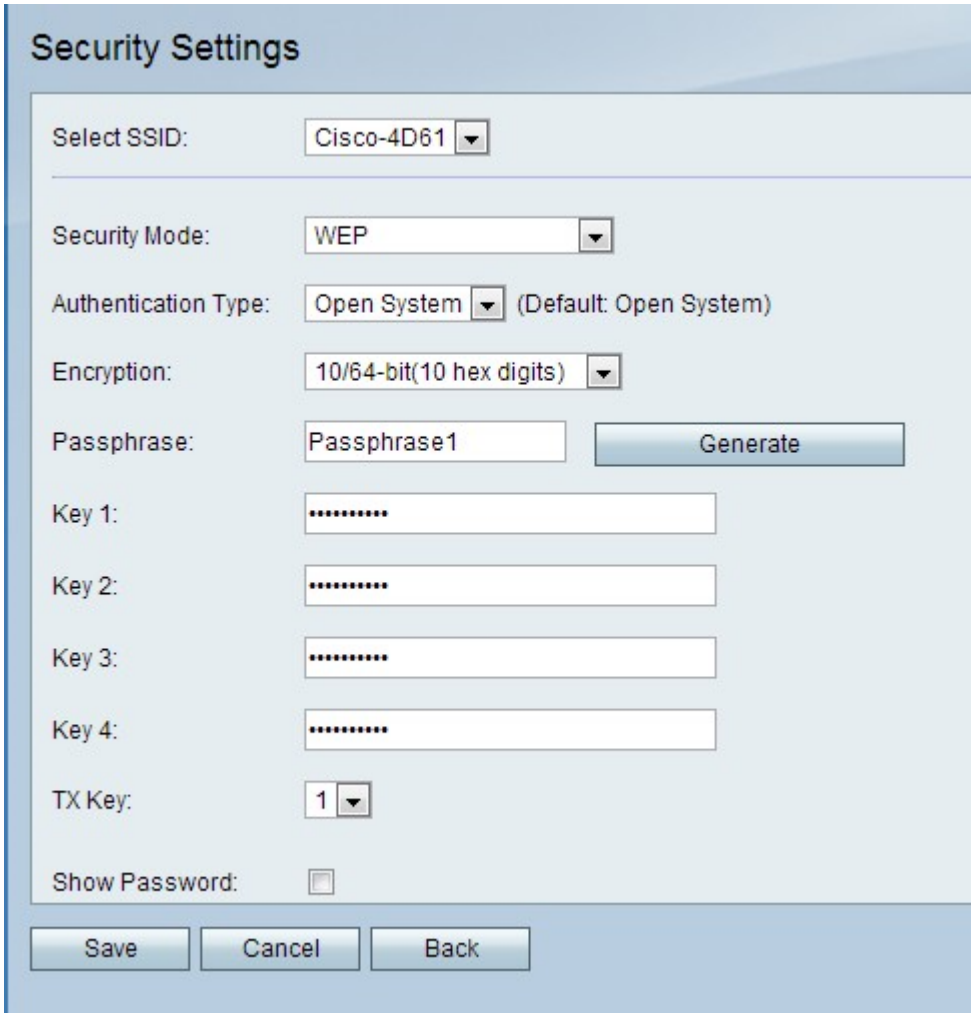
Nota: No se recomienda desactivar la seguridad.



Paso 1. En la lista desplegable Modo de seguridad, elija **Desactivado**. La seguridad está desactivada para la red inalámbrica.

Paso 2. Click **Save**.

Configuración de la seguridad WEP



Paso 1. En la lista desplegable Security Mode (Modo de seguridad), elija **WEP**.

Paso 2. En la lista desplegable Tipo de autenticación, elija un tipo de autenticación para la red inalámbrica.

·sistema abierto: cualquier dispositivo de red puede asociarse al punto de acceso, pero la clave WEP es necesaria para pasar el tráfico a través del punto de acceso.

·clave compartida: se necesita una clave WEP para asociarse al punto de acceso. También se utiliza para pasar el tráfico a través del punto de acceso.

Paso 3. En la lista desplegable Cifrado, elija un método de encriptación para la clave WEP.

·10/64-bit (10 dígitos hexadecimales): proporciona una clave de 40 bits.

·26/128 bits (26 dígitos hexadecimales): proporciona una clave de 104 bits. Esta opción es más segura.

Paso 4. En el campo Passphrase (Frase de paso), introduzca una frase de paso de más de ocho caracteres. Una frase de paso es útil para facilitar el recuerdo de los parámetros de seguridad de la red.

Paso 5. Haga clic en **Generar** para crear claves en los campos Clave 1, Clave 2, Clave 3 y Clave 4.

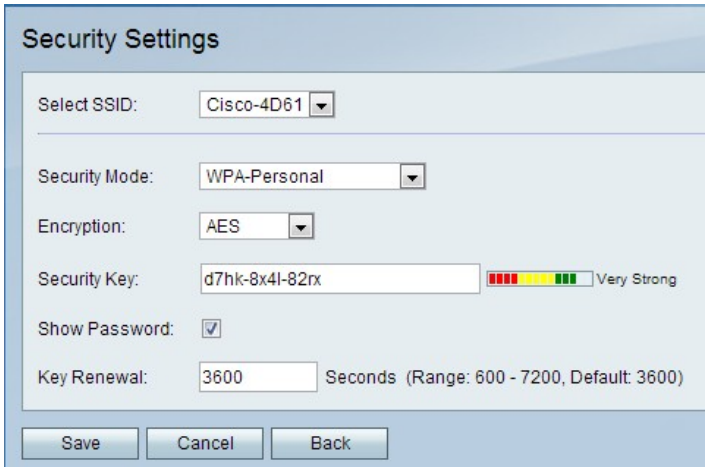
Nota: También puede introducir claves manualmente en los campos Key 1 (Clave 1), Key 2 (Clave 2), Key 3 (Clave 3) y Key 4 (Clave 4).

Paso 6. En la lista desplegable TX Key (Clave de transmisión), seleccione la clave que deben introducir los usuarios para acceder a la red inalámbrica.

Paso 7. (Opcional) Marque la casilla de verificación **Mostrar contraseña** para mostrar las cadenas de caracteres de las claves.

Paso 8. Click **Save**.

Configuración de la seguridad WPA-Personal



Paso 1. En la lista desplegable Security Mode (Modo de seguridad), elija **WPA-Personal**.

Paso 2. En la lista desplegable Cifrado, elija un método de encriptación para la clave WPA.

·TKIP/AES: esta opción se elige cuando los dispositivos conectados a la red inalámbrica no admiten AES en su totalidad.

·AES: esta opción es preferible si todos los dispositivos conectados a la red inalámbrica admiten AES.

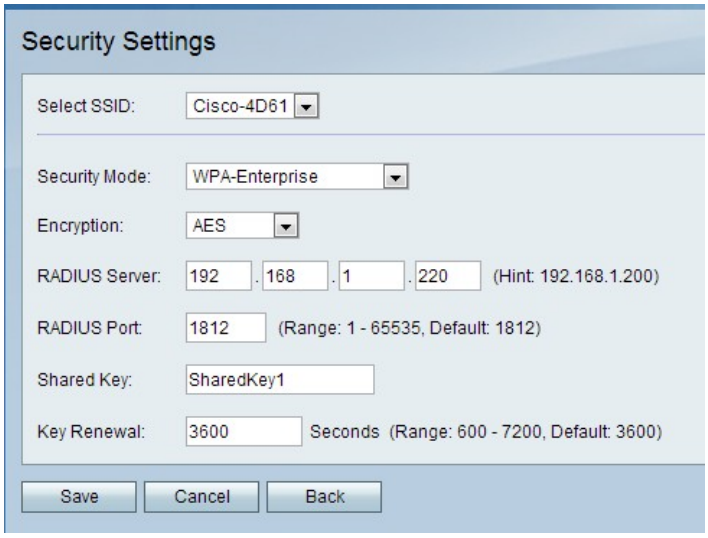
Paso 3. Introduzca una clave de seguridad en el campo Security Key (Clave de seguridad). La clave de seguridad es una frase de paso que consta de letras y dígitos. Los dispositivos utilizan la clave de seguridad para conectarse a la red.

Paso 4. (Opcional) Para mostrar la cadena de caracteres de la clave, marque la casilla de verificación **Mostrar contraseña**.

Paso 5. En el campo Key Renewal (Renovación de claves), introduzca el tiempo en segundos que el router VPN CVR100W utiliza la clave antes de generar una nueva.

Paso 6. Click **Save**.

Configuración de WPA-Enterprise Security



Paso 1. En la lista desplegable Security Mode (Modo de seguridad), elija **WPA-Enterprise**.

Paso 2. En la lista desplegable Cifrado, elija un método de encriptación para la clave WPA.

·TKIP/AES: esta opción se elige cuando los dispositivos conectados a la red inalámbrica no admiten AES en su totalidad.

·AES: esta opción es preferible si todos los dispositivos conectados a la red inalámbrica admiten AES.

Paso 3. En el campo Servidor RADIUS, introduzca la dirección IP del servidor RADIUS.

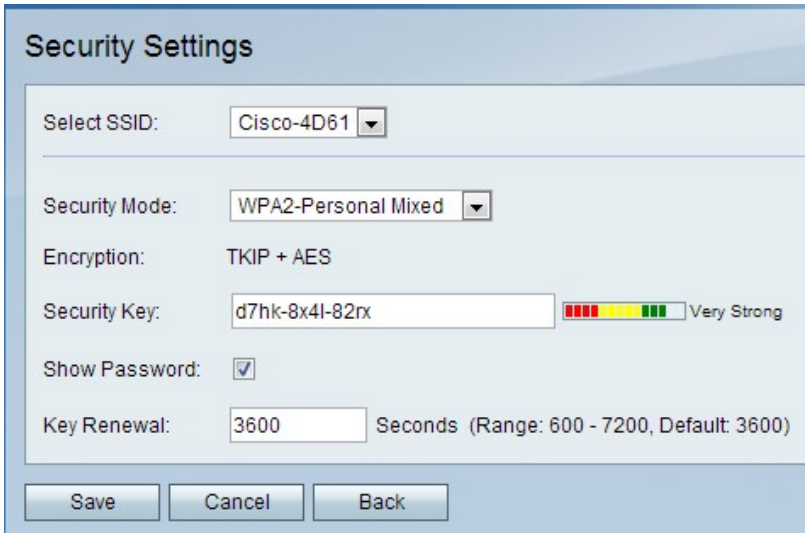
Paso 4. En el campo RADIUS Port (Puerto RADIUS), introduzca el número de puerto utilizado para acceder al servidor RADIUS.

Paso 5. En el campo Shared Key (Clave compartida), introduzca la clave previamente compartida para los usuarios inalámbricos. Una clave previamente compartida es una clave que utilizan todos los usuarios. La función de clave previamente compartida es una función de seguridad añadida.

Paso 6. En el campo Key Renewal (Renovación de claves), introduzca el tiempo en segundos que el router VPN CVR100W utiliza la clave antes de generar una nueva.

Paso 7. Click **Save**.

Configuración de la seguridad combinada WPA2-Personal/WPA2-Personal



Paso 1. En la lista desplegable Security Mode (Modo de seguridad), elija **WPA2-Personal** o **WPA2-Personal Mixed**.

Nota: WPA2-Personal se utiliza cuando todos los dispositivos de la red inalámbrica admiten AES. WPA2-Personal Mixed se utiliza cuando los dispositivos de la red no son compatibles con AES. El tipo de encriptación utilizado por el método de seguridad se muestra en el campo Encryption (Encriptación).

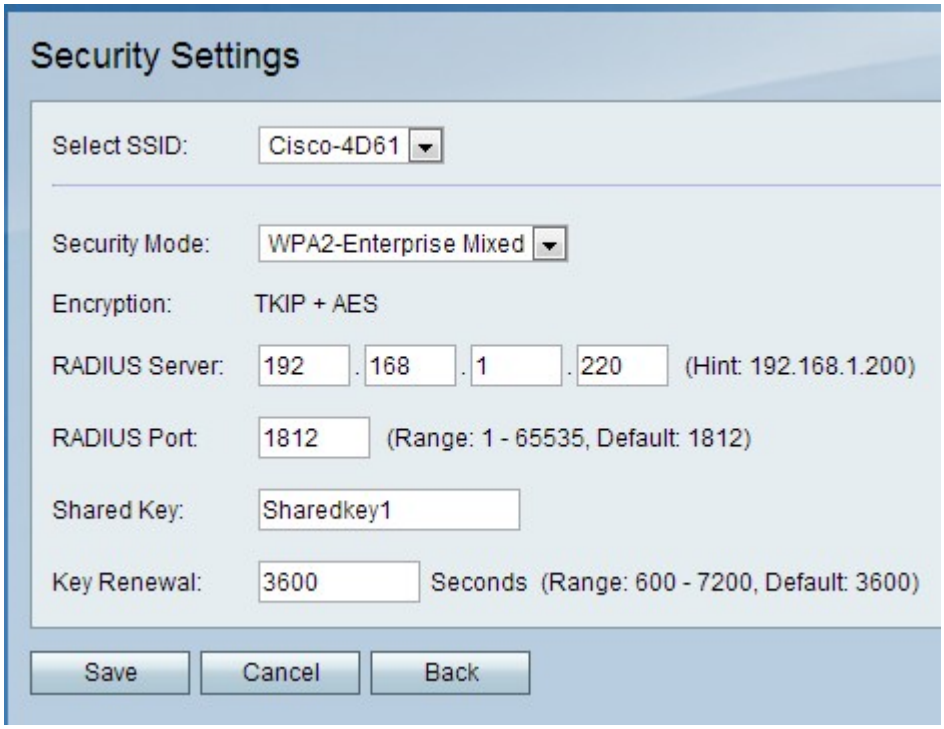
Paso 2. En el campo Clave de seguridad, introduzca una clave de seguridad. La clave de seguridad es una frase de paso que consta de letras y dígitos. Los dispositivos utilizan la clave de seguridad para conectarse a la red.

Paso 3. (Opcional) Para ver las cadenas de caracteres de la clave, marque la casilla de verificación **Mostrar contraseña**.

Paso 4. En el campo Key Renewal (Renovación de claves), introduzca el tiempo en segundos durante el que el router VPN CVR100W utiliza la clave antes de que genere una nueva.

Paso 5. Click **Save**.

Configuración de WPA2-Enterprise/WPA2-Enterprise Mixed Security



Paso 1. En la lista desplegable Security Mode (Modo de seguridad), elija **WPA2-Enterprise** o **WPA2-Enterprise Mixed**.

Nota: WPA2-Enterprise se utiliza cuando todos los dispositivos de la red inalámbrica admiten AES. WPA2-Enterprise Mixed se utiliza cuando los dispositivos de la red no todos admiten AES. El tipo de encriptación utilizado por el método de seguridad se muestra en el campo Encryption (Encriptación).

Paso 2. En el campo Servidor RADIUS, introduzca la dirección IP del servidor RADIUS.

Paso 3. En el campo RADIUS Port (Puerto RADIUS), introduzca el número de puerto utilizado para acceder al servidor RADIUS.

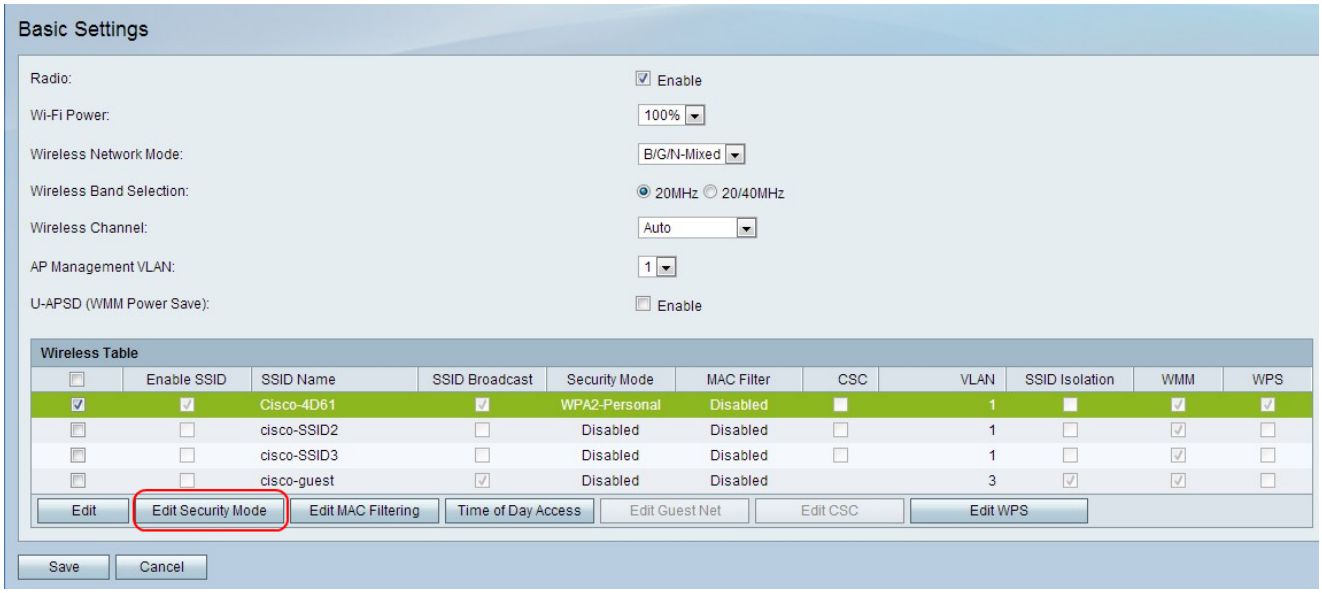
Paso 4. En el campo Shared Key (Clave compartida), introduzca la clave previamente compartida para los usuarios inalámbricos. Una clave previamente compartida es una clave que utilizan todos los usuarios. La función de clave previamente compartida es una función de seguridad añadida.

Paso 5. En el campo Key Renewal (Renovación de claves), introduzca el tiempo en segundos que el router VPN CVR100W utiliza la clave antes de generar una nueva.

Paso 6. Click **Save**.

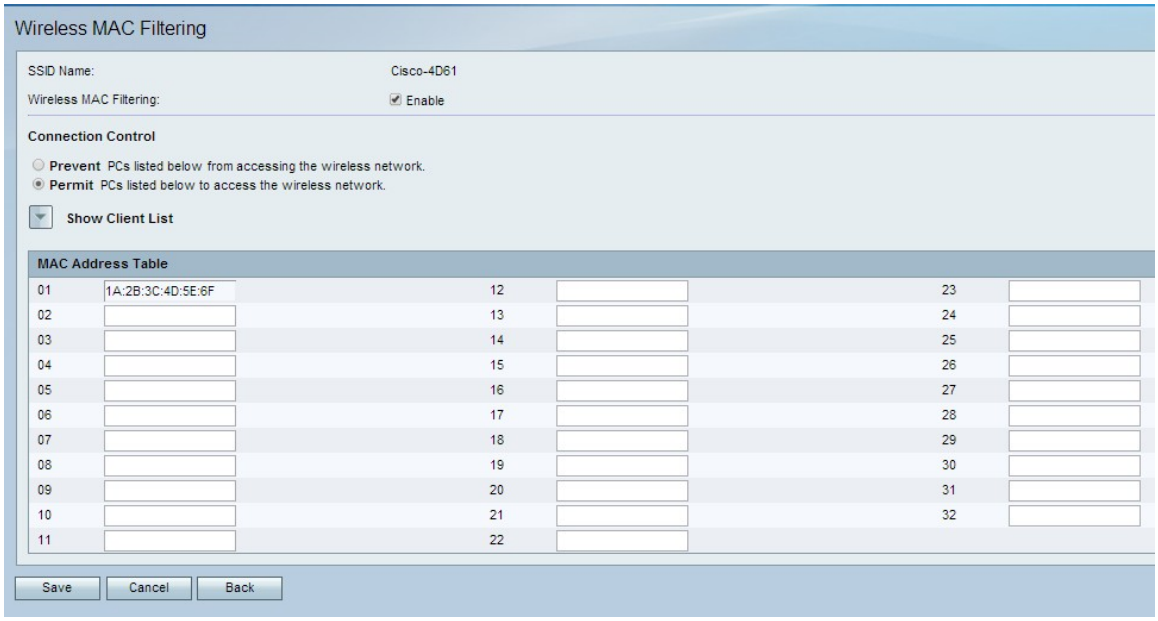
Editar filtrado de MAC

El filtrado de MAC se utiliza para permitir o denegar el acceso a la red inalámbrica en función de la dirección MAC del dispositivo de conexión.



Paso 1. Active la casilla de verificación de la red que desea editar.

Paso 2. Haga clic en **Edit MAC Filtering** para crear una lista de control de acceso MAC para la red especificada. Se abre la página *Wireless MAC Filter*:



Paso 3. Marque **Enable** para habilitar el filtrado MAC en la red.

Paso 4. Haga clic en el botón de opción correspondiente al tipo de lista deseado en el campo Control de conexión.

·Evitar que PC: evita que los PC con las direcciones MAC enumeradas entren en la red.

·Permitir PC: permite que los PC con las direcciones MAC enumeradas entren en la red.

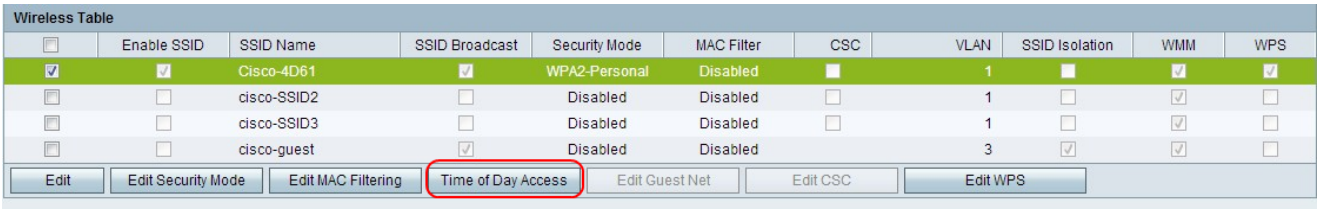
Paso 5. En la tabla de direcciones MAC, introduzca las direcciones MAC deseadas.

Paso 6. Click **Save**.

Acceso por hora del día

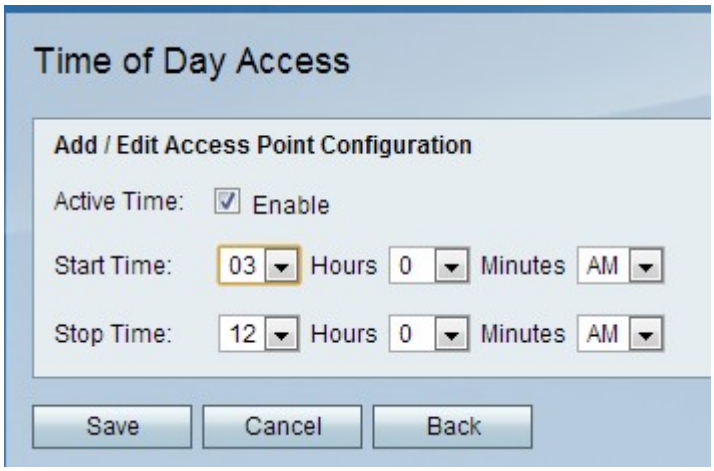
La función de acceso por hora del día se utiliza para permitir el acceso a los usuarios según

una programación configurada.



Paso 1. Active la casilla de verificación de la red que desea editar.

Paso 2. Haga clic en **Time of Day Access** para configurar cuándo los usuarios pueden acceder a la red especificada. Se abre *la* página *Acceso a hora del día*:



Paso 3. Marque **Enable** en el campo Active Time para habilitar el acceso a la hora del día para la red.

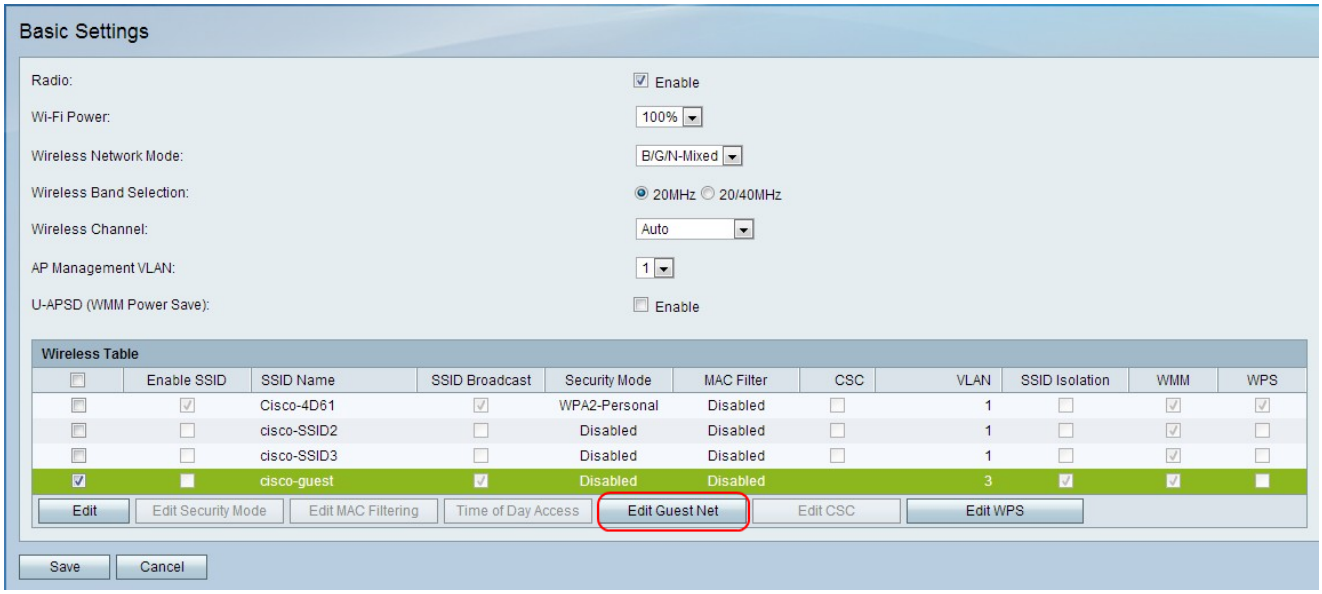
Paso 4. En el campo Hora de inicio, introduzca la hora a la que comienza el acceso a la red.

Paso 5. En el campo Tiempo de detención, introduzca la hora a la que finaliza el acceso de la red.

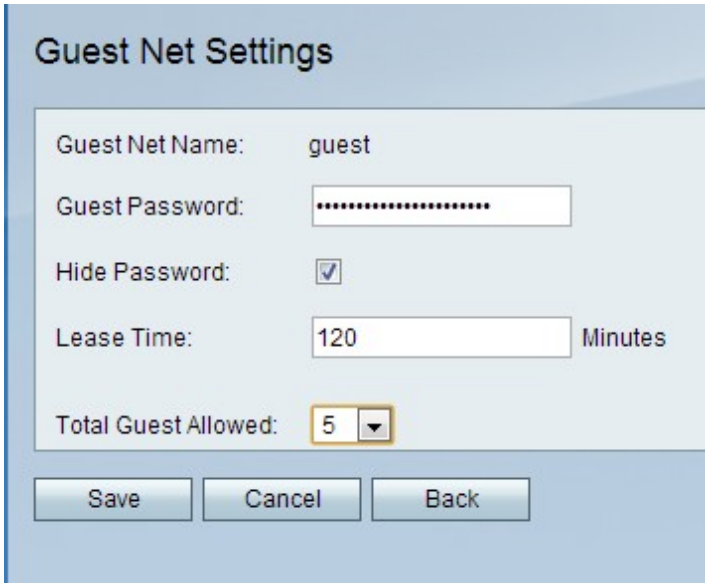
Paso 6. Click **Save**.

Editar red de invitado

Una red de invitado es una sección de una red diseñada para usuarios temporales. Esto se utiliza para permitir a los invitados acceder a la red sin necesidad de exponer claves Wi-Fi privadas. Se puede configurar una red de invitado para restringir el tiempo de acceso y el uso del ancho de banda de un usuario.



Paso 1. Haga clic en **Editar red de invitado** para configurar la red de invitado. Se abre la página *Configuración de red de invitado*:



Paso 2. En el campo Contraseña de invitado, introduzca una contraseña que los usuarios utilizarán para introducir la red de invitado.

Paso 3. (Opcional) Para ocultar la contraseña en la página, active la casilla de verificación en el campo Ocultar contraseña.

Paso 4. En el campo Tiempo de concesión, introduzca la hora en minutos en la que los usuarios pueden permanecer conectados a la red para invitados.

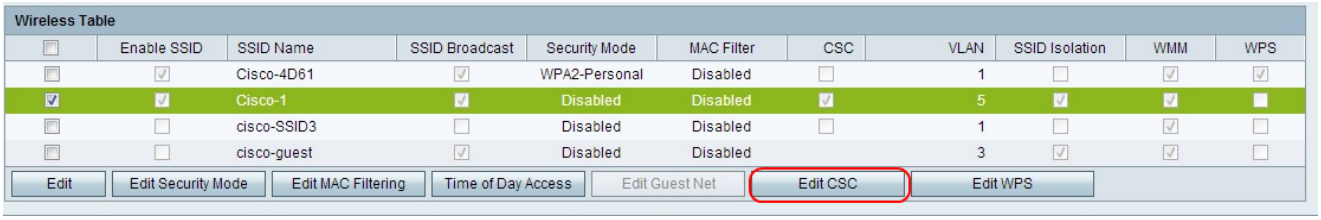
Paso 5. En la lista desplegable Total de invitados permitidos, elija el número total de invitados permitidos.

Paso 6. Click **Save**.

Editar CSC

CSC facilita la configuración de una red inalámbrica y facilita la conexión de dispositivos inalámbricos a la red. El dispositivo inalámbrico utiliza CSC para obtener el SSID y la

contraseña de la red, lo que permite la conexión automática a la red.



Paso 1. Active la casilla de verificación de la red que desea editar.

Paso 2. Haga clic en **Editar CSC** para editar Cisco Simple Connect.

Paso 3. Marque la casilla de verificación CSC.

Paso 4. En la lista desplegable VLAN, elija la VLAN que se utiliza para CSC.

Nota: La VLAN de conexión simple de Cisco no puede ser la misma que la VLAN SSID actual u otra. Para crear una nueva VLAN, consulte el artículo *Pertenencia a VLAN en el router CVR100W*.

Nota: CSC solo puede aplicar el sistema de distribución inalámbrica (WDS) en SSID1. Consulte el artículo *Wireless Distribution System (WDS) en el router CVR100W*.

Paso 5. Click **Save**.