Función Personal Pre-Shared Key en el punto de acceso CBW

Objetivo

En este artículo se explica la función de clave personal previamente compartida (PSK) del firmware del punto de acceso (AP) Cisco Business Wireless (CBW) versión 10.6.1.0.

Dispositivos aplicables | Versión de software

- Punto de acceso Cisco Business Wireless 140AC | 10.6.1.0 (última descarga)
- Punto de acceso Cisco Business Wireless 145AC | 10.6.1.0 (última descarga)
- Punto de acceso Cisco Business Wireless 240AC | 10.6.1.0 (última descarga)

Introducción

Si tiene equipo CBW en la red, ahora puede utilizar la función PSK personal en la versión de firmware 10.6.1.0.

El PSK personal, también conocido como PSK individual (iPSK), es una función que permite a un administrador emitir claves previamente compartidas únicas a dispositivos individuales para la misma red de área local inalámbrica (WLAN) personal Wi-Fi Protected Access II (WPA2). El PSK único está vinculado a la dirección MAC del dispositivo. Esto no se admite en las WLANs donde se habilita la política WPA3.

Esta función autentica el cliente mediante un servidor RADIUS. Generalmente, está pensada para su uso por parte de dispositivos de IoT y portátiles y dispositivos móviles de la empresa.

Table Of Contents

Prerequisites

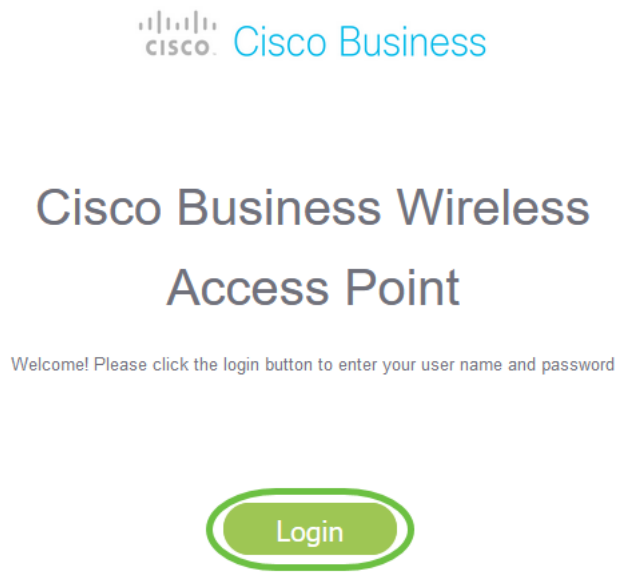
- Asegúrese de haber actualizado el firmware de CBW AP a 10.6.1.0. Haga clic si desea obtener instrucciones paso a paso para realizar una actualización del firmware.
- Necesitará un servidor RADIUS donde se deben configurar el PSK personal y la dirección MAC del dispositivo.
- Esta función CBW es compatible con tres servidores RADIUS diferentes: FreeRADIUS, Microsoft NPS y Cisco ISE. La configuración variará según el servidor RADIUS utilizado.

Configuración de los parámetros RADIUS de CBW

Para configurar los parámetros RADIUS en el AP CBW, siga los pasos.

Paso 1

Inicie sesión en la interfaz de usuario web del punto de acceso CBW.

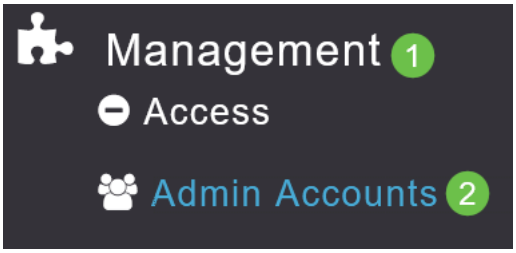


Paso 2

Haga clic en el símbolo de **flecha bidireccional** para cambiar a la vista de expertos.

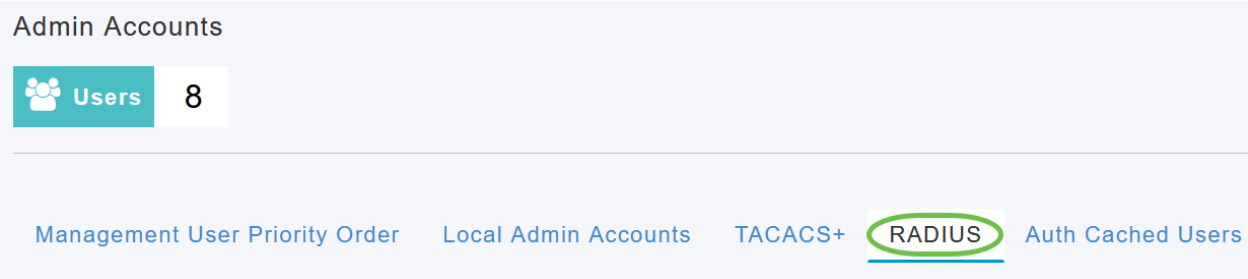
Paso 3

Vaya a **Administración > Cuentas de administración.**



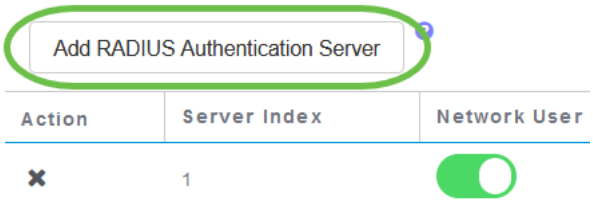
Paso 4

Seleccione la pestaña **RADIUS**.



Paso 5

Haga clic en **Add RADIUS Authentication Server**.

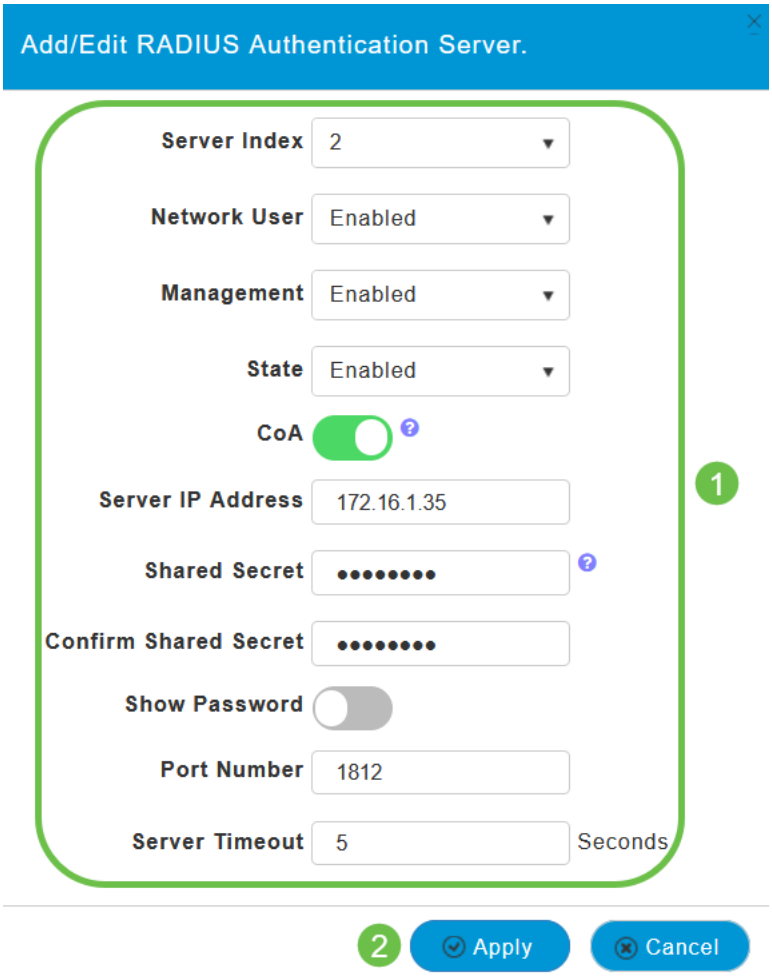


Paso 6

Configure lo siguiente:

- *Índice de servidores*: seleccione de 1 a 6
- *Usuario de red*: active el estado. De forma predeterminada, está activado
- *Administración*: habilita el estado. De forma predeterminada, está activado
- *Estado*: habilita el estado. De forma predeterminada, está activado
- *CoA*: asegúrese de que la carga de autoridad (CoA) esté habilitada.
- *Dirección IP del servidor*: introduzca la dirección IPv4 del servidor RADIUS
- *Secreto compartido*: introduzca la clave secreta compartida
- *Número de puerto*: introduzca el número de puerto que se utiliza para comunicarse con el servidor RADIUS.
- *Tiempo de espera del servidor*: introduzca el tiempo de espera del servidor

Haga clic en Apply (Aplicar).



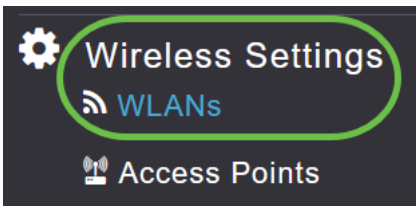
Configuración de los parámetros de WLAN

Cree una WLAN como WLAN WPA2 Personal Asegurada estándar.

La clave previamente compartida no se utilizará para los dispositivos PSK personales. Esto sólo se usaría para dispositivos que NO están autenticados en el servidor RADIUS. Debe agregar las direcciones MAC de CUALQUIER dispositivo que se conectará a esta WLAN a la lista de permitidos de este dispositivo.

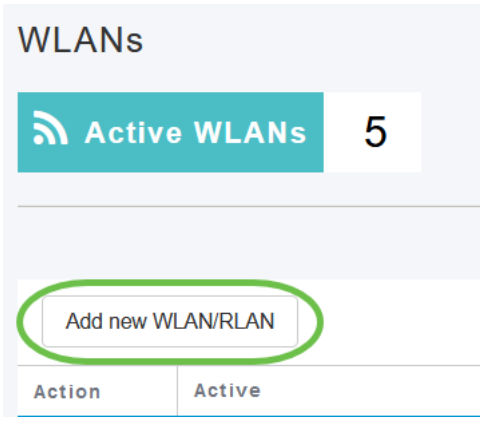
Paso 1

Vaya a **Wireless Settings > WLAN**.



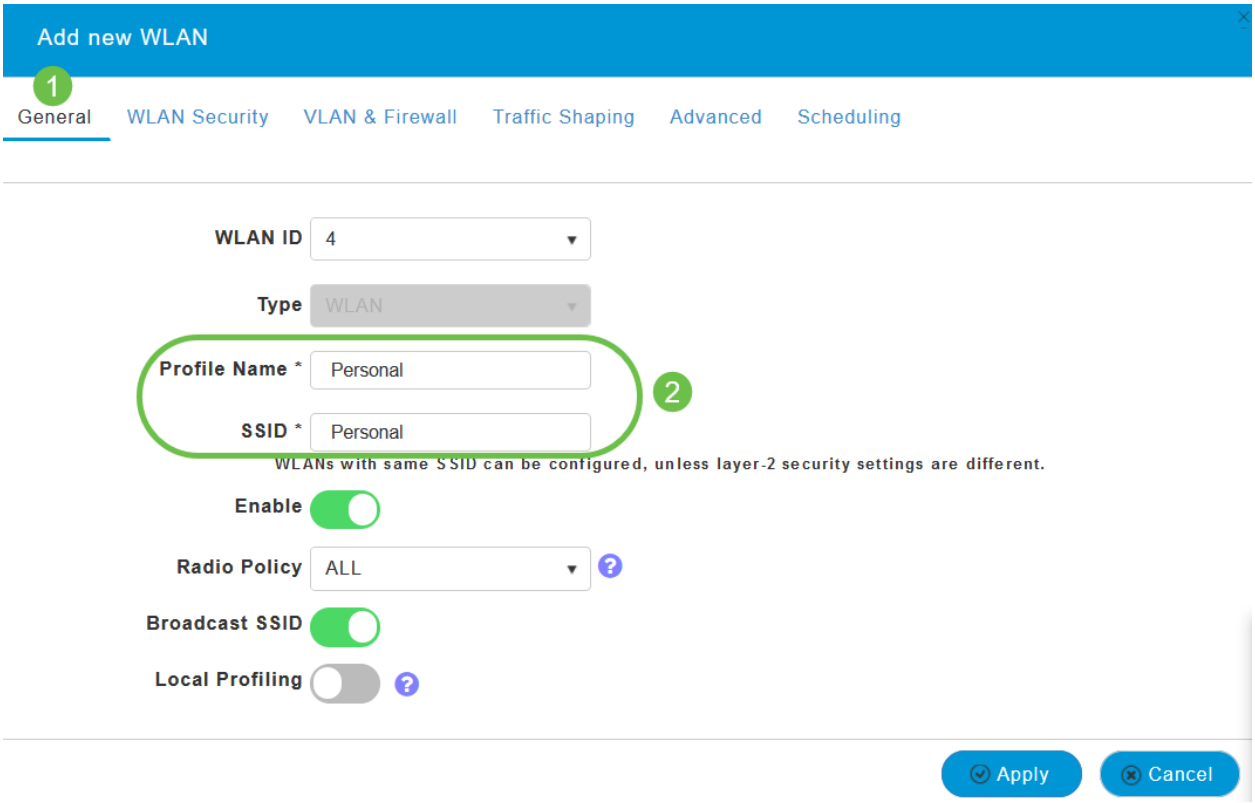
Paso 2

Haga clic en **Add new WLAN/RLAN**.



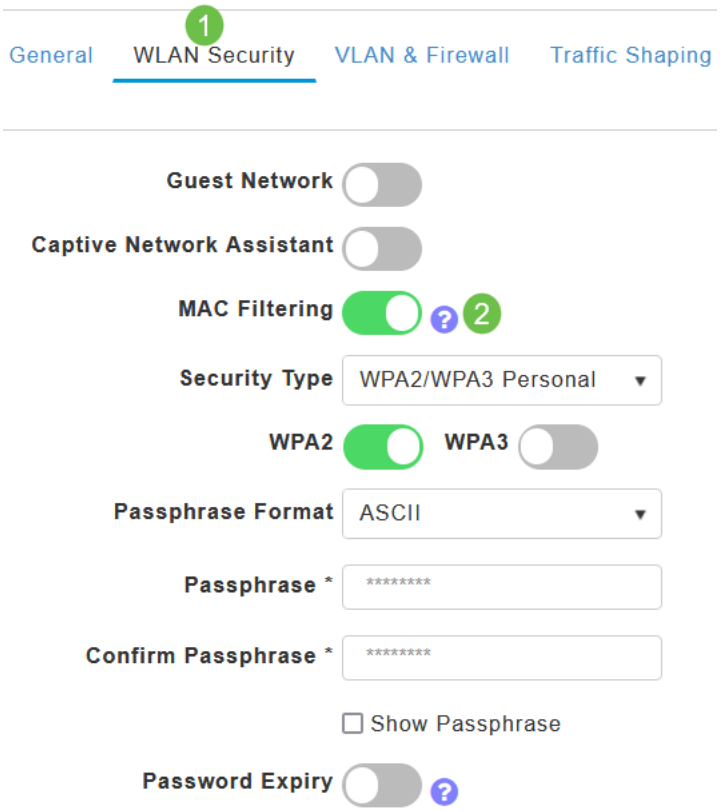
Paso 3

En la pestaña *General*, ingrese un *Nombre de Perfil* para la WLAN.



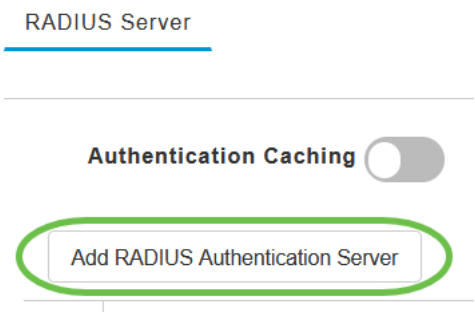
Paso 4

Navegue hasta la ficha **Seguridad WLAN** y habilite **Filtrado MAC** deslizando la alternancia.



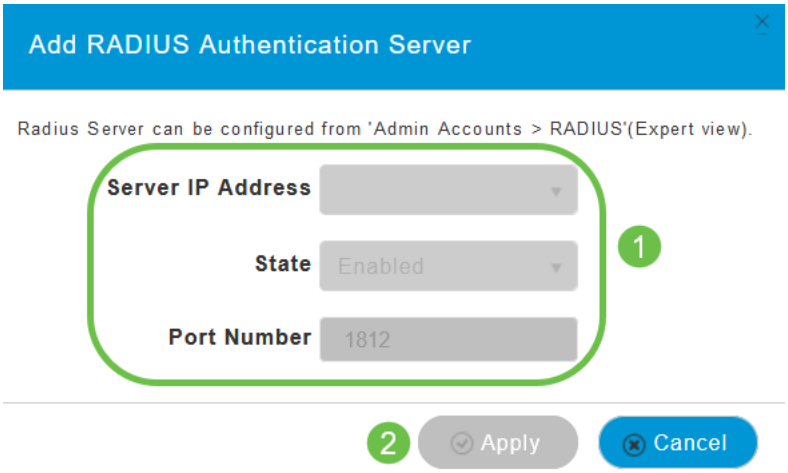
Paso 5

Haga clic en **Add RADIUS Authentication Server** para agregar el servidor RADIUS configurado en la sección anterior para proporcionar autenticación para esta WLAN.



Paso 6

Aparecerá una ventana emergente. Ingrese la *dirección IP, el estado y el número de puerto del servidor*. Haga clic en Apply (Aplicar).

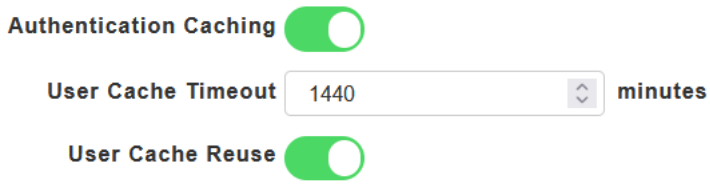


Paso 7

(Opcional)

Habilitar *almacenamiento en caché de autenticación*. Al activar esta opción, se muestran los campos siguientes.

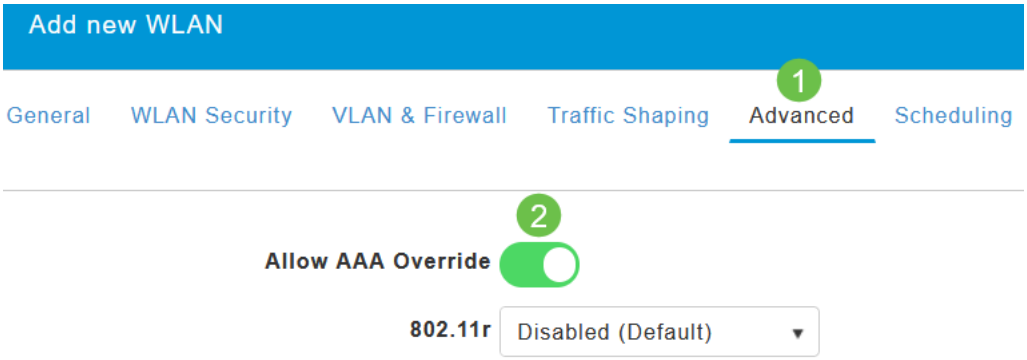
- *Tiempo de espera de caché de usuario:* especifica el período de tiempo en el que caduca la credencial autenticada en la caché.
- *Reutilización de la memoria caché de usuario*: utilice la información de la memoria caché de credenciales antes del tiempo de espera de la memoria caché. De forma predeterminada, esto
está desactivado.



Si se habilita esta función, un cliente que ya se ha autenticado en este servidor no tendrá que pasar datos al servidor RADIUS cuando se vuelvan a conectar a esta WLAN en las próximas 24 horas.

Paso 8

Vaya a la ficha Opciones avanzadas. Habilite **Allow AAA Override** deslizando la alternancia.

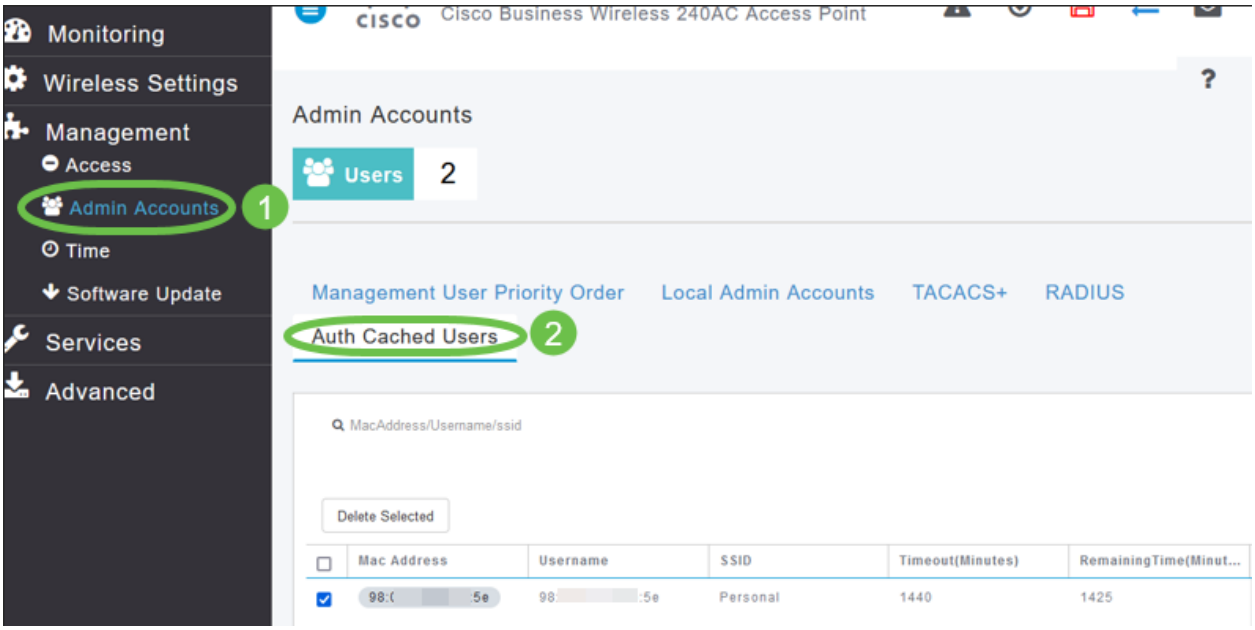


La pestaña *Avanzadas* sólo estará visible si está en la *Vista de expertos*.

Pasos siguientes

Una vez que haya configurado los parámetros en su CBW AP y configurado su servidor RADIUS, debería poder conectar su dispositivo. Introduzca el PSK personalizado configurado para esa dirección MAC y se unirá a la red.

Si ha configurado el almacenamiento en caché de autenticación, podrá ver los dispositivos que se han unido a la WLAN mediante la pestaña *Auth Cached Users* bajo *Admin Accounts*. Si es necesario, se puede eliminar.



Conclusión

¡Ahí tienes! Ahora puede disfrutar de las ventajas de la función PSK personal en su punto de acceso CBW.