

# Configuración del protocolo simple de administración de red en el punto de acceso inalámbrico Cisco Business

## Objetivo

El objetivo de este documento es mostrarle cómo configurar los parámetros del protocolo simple de administración de red (SNMP) en el punto de acceso (AP) Cisco Business Wireless (CBW).

## Dispositivos aplicables | Versión de software

- 140AC ([Ficha técnica](#)) | 10.0.1.0 ([Descargar última](#))
- 145AC ([Ficha técnica](#)) | 10.0.1.0 ([Descargar última](#))
- 240AC ([Ficha técnica](#)) | 10.0.1.0 ([última descarga](#))

## Introducción

Los puntos de acceso CBW admiten el último estándar 802.11ac Wave 2 para redes de mayor rendimiento, mayor acceso y mayor densidad. Ofrecen un rendimiento líder del sector con conexiones inalámbricas muy seguras y fiables, lo que ofrece una experiencia de usuario final sólida y móvil.

SNMP es un protocolo de administración de red popular que se utiliza para recopilar información de todos los dispositivos de la red y configurar y administrar estos dispositivos. Puede configurar los modos de acceso SNMP v2c y SNMP v3 usando la interfaz web del AP maestro. SNMPv2c es el marco administrativo de comunidad basado en cadena para SNMPv2. La cadena de comunidad es un tipo de contraseña, que se transmite en texto sin formato. La función SNMP v3 proporciona acceso seguro a los dispositivos mediante la autenticación y el cifrado de paquetes de datos a través de la red.

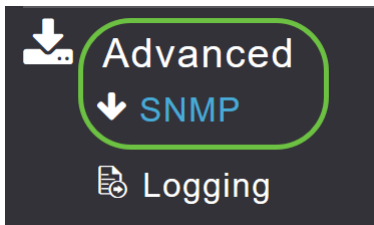
Puede configurar los siguientes modos de acceso SNMP para el AP maestro:

- SNMP v2c solamente
- SNMP v3 solamente
- SNMP v2c y SNMP v3
- Ni SNMP v2c ni SNMP v3

## Configuración de SNMP

### Paso 1

Elija **Advanced > SNMP**.



## Paso 2

Active la opción de servicio SNMP para consultar la configuración mediante el explorador MIB.

### SNMP

↓ Service Disabled

---

Service  ?

SNMP Access V2C  V3

Read Only Community

Read-Write Community

Apply

## Paso 3

En la ventana de configuración SNMP, seleccione la casilla de verificación apropiada junto al *Acceso SNMP* para habilitar el modo SNMP deseado.

El modo predeterminado es v2c (o de forma predeterminada, ambos o ninguno de los modos de acceso SNMP está seleccionado).

El modo de acceso SNMP seleccionado está habilitado.

## SNMP



Service

Disabled

Service  ?

SNMP Access **V2C**  **V3**

Read Only Community

Read-Write Community

Apply

### Paso 4

En el *campo Comunidad de sólo lectura*, introduzca el nombre de comunidad deseado. El nombre predeterminado es **public**.

## SNMP



Service

Disabled

Service  ?

SNMP Access **V2C**  **V3**

Read Only Community

Read-Write Community

Apply

### Paso 5

En el campo *Comunidad de lectura y escritura*, introduzca el nombre de comunidad deseado. El nombre predeterminado es **private**.

## SNMP



Service

Disabled

Service  ?

SNMP Access **V2C**  **V3**

Read Only Community

Read-Write Community

Apply

### Paso 6

Haga clic en Apply (Aplicar).

## SNMP



Service

Disabled

Service  ?

SNMP Access **V2C**  **V3**

Read Only Community

Read-Write Community

Apply

### Paso 7

Para configurar SNMP Trap Receiver, haga clic en **Add New SNMP Trap Receiver**. Esta herramienta recibe, registra y muestra las trampas SNMP enviadas desde los dispositivos de red. La configuración predeterminada está desactivada.

## SNMP Trap Receivers

+ Add New SNMP Trap Receiver

Action	Receiver Name	IP Address	Status	SNMPv3
--------	---------------	------------	--------	--------

### Paso 8

En la ventana *Add SNMP Trap Receiver*, configure lo siguiente:

- Nombre del receptor
- Dirección IP del servidor al que desea conectarse
- Estado
- Opción para habilitar SNMPv3

Haga clic en Apply (Aplicar).

Add SNMP Trap Receiver ×

Receiver Name  1

IP Address  2

Status  3

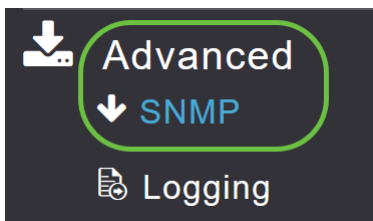
SNMPv3  4

5

## Agregar un usuario SNMPv3

### Paso 1

Elija **Advanced > SNMP**.



### Paso 2

En la ventana *SNMP Setup*, en la sección *Usuarios SNMPv3*, haga clic en el botón **Agregar nuevo usuario SNMPv3**.

## SNMP V3 Users

+ Add New SNMP V3 User

Action	User Name	Access Mode	Authentication protocol	Privacy Protocol
--------	-----------	-------------	-------------------------	------------------

### Paso 3

En la ventana *Add SNMP v3 User*, ingrese los siguientes detalles:

- *User Name*: introduzca el nombre de usuario deseado para el nuevo usuario SNMPv3.
- *Modo de acceso*: en la lista desplegable, elija uno de los modos deseados: *Sólo lectura* o *Lectura/Escritura*. El valor predeterminado es **Read Only**.
- *Protocolo de autenticación* - En la lista desplegable *Authentication Protocol*, elija una de las opciones: HMAC-MD5, HMAC-SHA o Ninguno. El protocolo de autenticación predeterminado es **HMAC-SHA**.
- *Contraseña de autenticación*: introduzca la contraseña de autenticación deseada. Utilice una longitud mínima de contraseña de 12 a 31 caracteres.
- *Confirmar contraseña de autenticación*: confirme la contraseña de autenticación especificada anteriormente. Puede seleccionar la casilla de verificación *Mostrar contraseña* para mostrar las entradas en los campos *Contraseña de autenticación* y *Confirmar contraseña de autenticación* y verificar si los caracteres coinciden.
- *Protocolo de privacidad*: en la lista desplegable, seleccione una de las opciones siguientes: CBC-DES, CFB-AES-128 o Ninguno. El protocolo de privacidad predeterminado es **CFB-AES-128**.
- *Contraseña de privacidad*: introduzca la contraseña de privacidad deseada. Utilice una longitud mínima de contraseña de 12 a 31 caracteres.
- *Confirmar contraseña de privacidad*: confirme la contraseña de privacidad especificada anteriormente. Puede seleccionar la casilla de verificación *Mostrar contraseña* para mostrar las entradas en los campos *Contraseña de privacidad* y *Confirmar contraseña de privacidad* y verificar si los caracteres coinciden.

## Add SNMP V3 User



User Name \*

Access Mode

Authentication protocol

Authentication Password

Confirm Authentication Password

Show Password

Privacy Protocol

Privacy Password

Confirm Privacy Password

Show Password

### Paso 4

Haga clic en **Aplicar** para crear un nuevo usuario SNMPv3.

## Add SNMP V3 User

User Name \*

Access Mode

Authentication protocol

Authentication Password

Confirm Authentication Password

Show Password

Privacy Protocol

Privacy Password

Confirm Privacy Password

Show Password

Apply

Cancel

El usuario SNMPv3 recién agregado aparece en la tabla *Usuarios SNMP V3* en la ventana Configuración SNMP.

### SNMP V3 Users

+ Add New SNMP V3 User

Action	User Name	Access Mode	Authentication protocol	Privacy Protocol
✘	Test	Read Only(Default)	HMAC-SHA(Default)	CFB-AES-128(Default)
✘	ciscoA2	Read Only(Default)	HMAC-SHA(Default)	CFB-AES-128(Default)

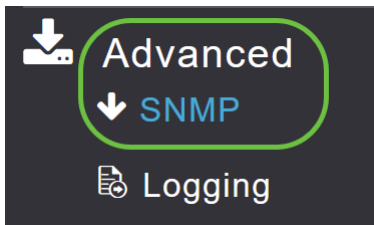
Puede agregar hasta un máximo de 7 usuarios SNMPv3.

## Eliminar usuario SNMPv3

### Paso 1


Elija **Advanced > SNMP**.





## Paso 2

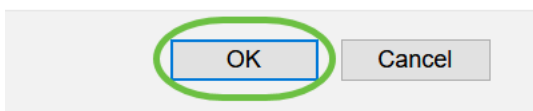
En *SNMP Setup*, haga clic en el icono X de la fila que contiene el usuario SNMPv3 que desea eliminar.

Action	User Name	Access Mode	Authentication protocol	Privacy Protocol
	Test	Read Only(Default)	HMAC-SHA(Default)	CFB-AES-128(Default)

## Paso 3

Aparecerá una ventana emergente para confirmar la acción. Click OK.

Are you sure? You want to delete this User.



La tabla Usuarios de SNMPv3 se actualiza y la entrada eliminada se elimina de la tabla.

## Conclusión

¡Todos están listos! Ahora ha configurado correctamente SNMP en su AP CBW. Para obtener más información, lea los siguientes artículos y gestione su red con facilidad.

[Preguntas Frecuentes](#) [Actualización del firmware](#) [RLAN](#) [Definición de perfiles de aplicaciones](#) [Perfiles de clientes](#) [Herramientas de punto de acceso maestro](#) [Umbrella](#) [Usuarios de WLAN](#) [Registro](#) [Modelado de tráfico](#) [Rogues](#) [Interferentes](#) [Administración de la Configuración](#) [Modo de malla de configuración de puertos](#)