Configure el SNMPv3 en el WAP125 y el WAP581

Objetivo

El protocolo administración de red simple versión 3 (SNMPv3) es un modelo de seguridad en el cual ponen a una estrategia de autenticación para un usuario y el grupo en quienes el usuario resida. El nivel de seguridad es el nivel de seguridad permitido dentro de un modelo de seguridad. Una combinación de un modelo de seguridad y de un nivel de seguridad determina se utiliza qué mecanismo de seguridad al manejar un paquete snmp.

En el SNMP, el Management Information Base (MIB) es una base de datos jerárquica de la información que contiene los identificadores de objeto (OID) que actúa como variable que se pueda leer o fijar vía el SNMP. El MIB se ordena en a árbol-como la estructura. Una sub-estructura dentro del objeto administrado que nombra el árbol es una sub-estructura de la visión. Una opinión MIB es una combinación de un conjunto de las sub-estructuras de la visión o de una familia de sub-estructuras de la visión. Las opiniones MIB se crean para controlar el rango OID a que los usuarios SNMPv3 pueden tener acceso. La configuración de las opiniones SNMPv3 es esencial restringir a un usuario para ver solamente el MIB limitado. Un WAP puede tener hasta 16 opiniones incluyendo las dos vistas predeterminadas.

El objetivo de este documento es mostrarle cómo recolectar, ver, y descargar la actividad CPU/RAM en el WAP125 y el WAP581.

Dispositivos aplicables

- WAP125
- WAP581

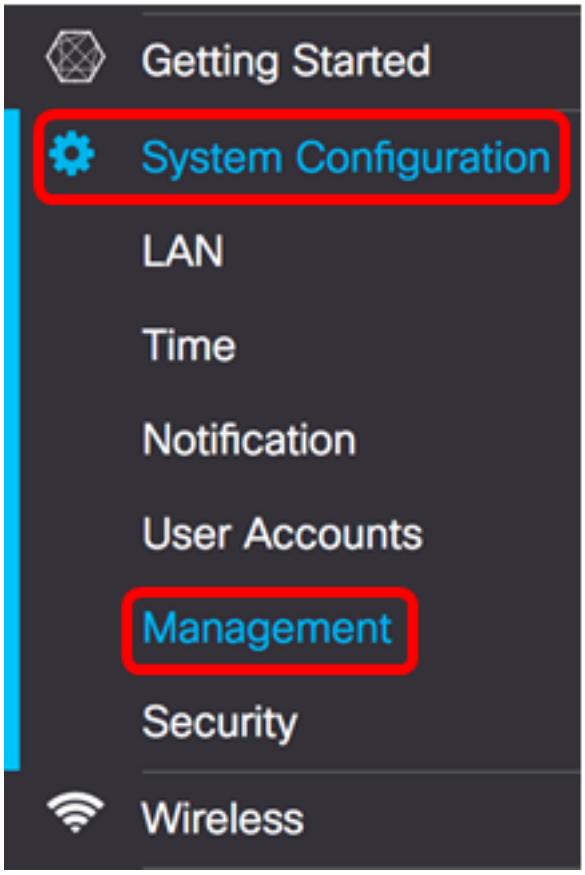
Versión de software

- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

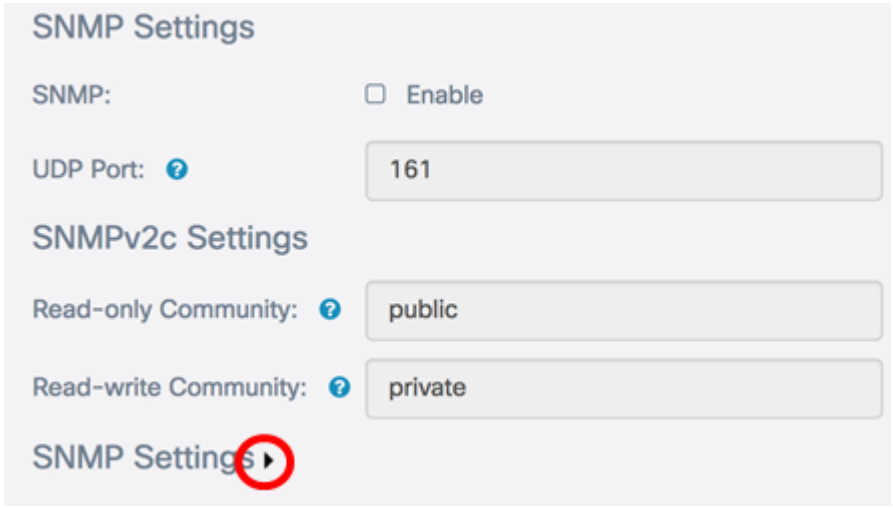
Configure las configuraciones SNMPv3

Configure las opiniones SNMPv3

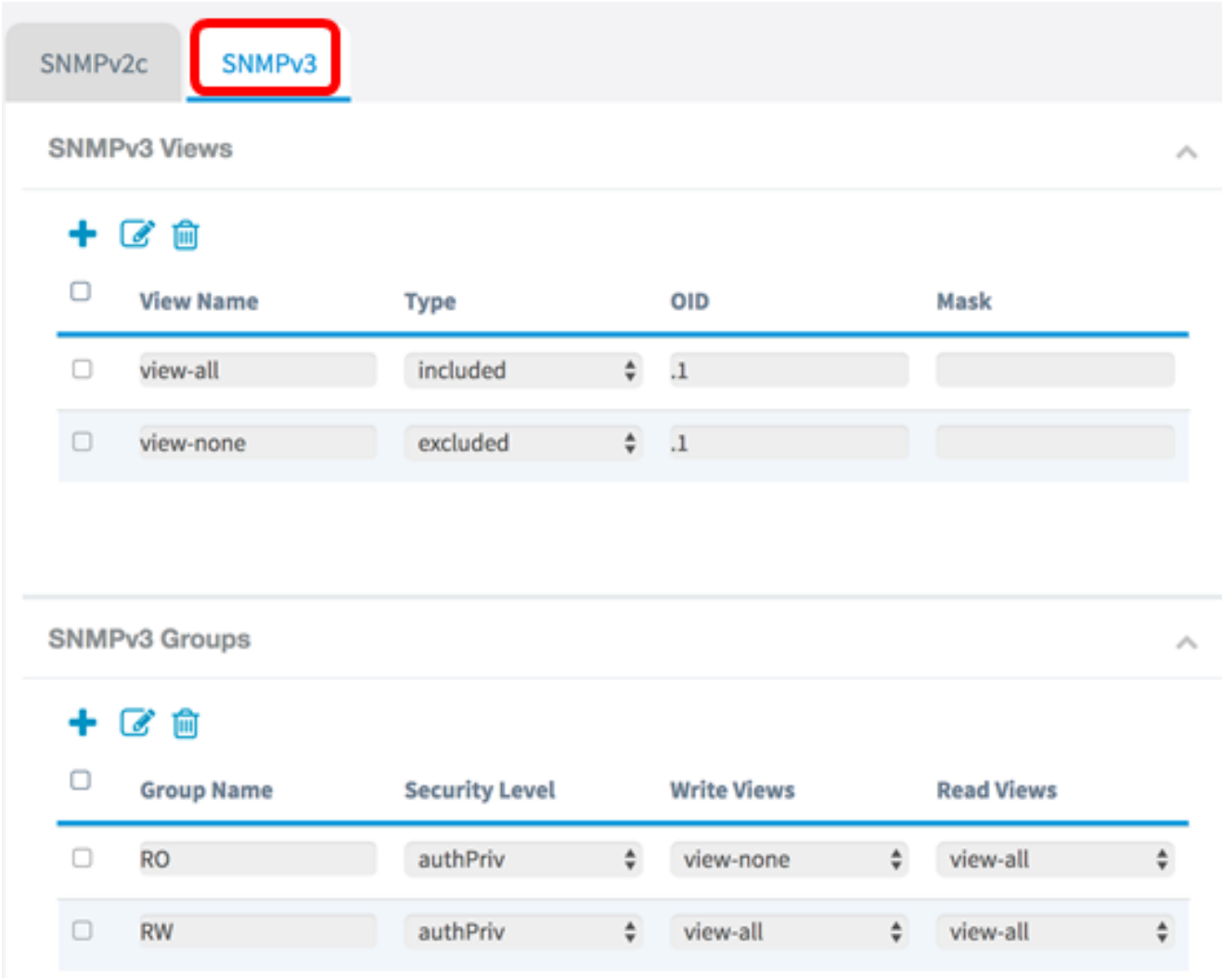
Paso 1. Ábrase una sesión a la utilidad en Internet y elija la **configuración del sistema > la Administración**.



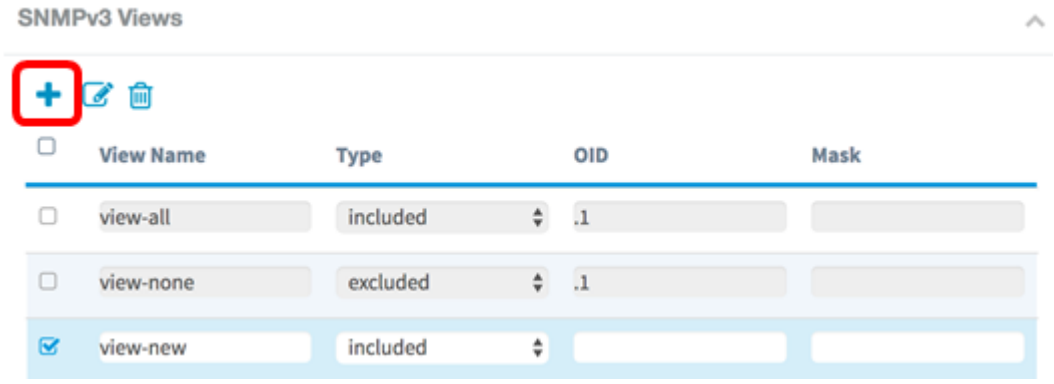
Paso 2. Haga clic la flecha correcta de las **configuraciones SNMP**.



Paso 3. Haga clic el **SNMPv3** cuadro.

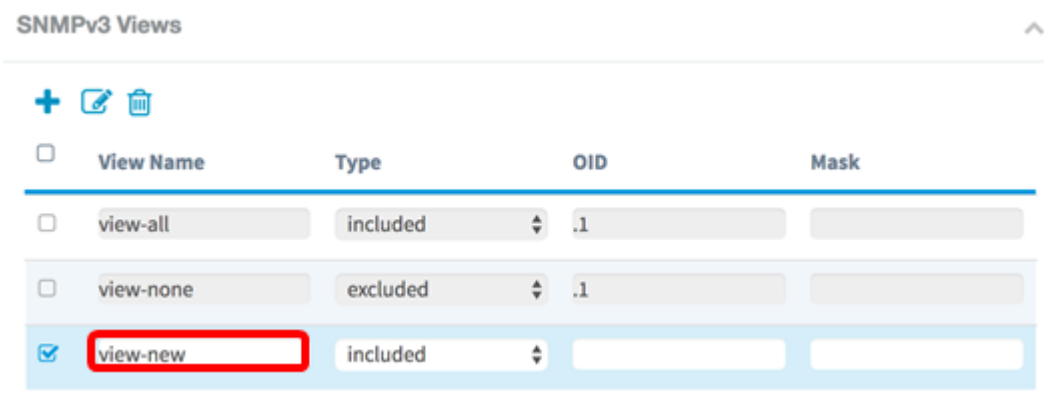


Paso 4. Haga clic **+** botón para crear una nueva entrada bajo opiniones SNMPv3.



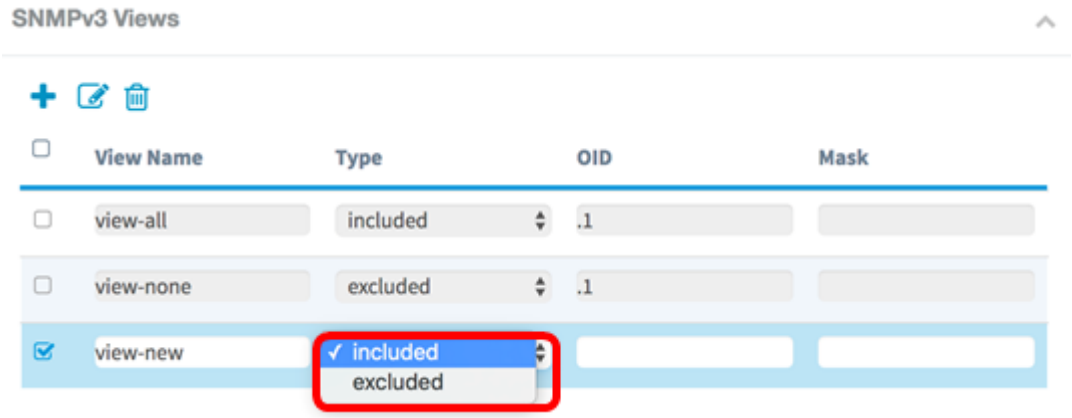
Paso 5. En el campo de *nombre a visualizar*, ingrese un nombre que identifique la opinión MIB.

Nota: En este ejemplo, vista-nuevo se crea como el nombre a visualizar. Vista-todo y vista-ninguno se crean por abandono y contiene todos los objetos de la Administración utilizados por el sistema. Éstos no pueden ser modificados ni ser suprimidos.



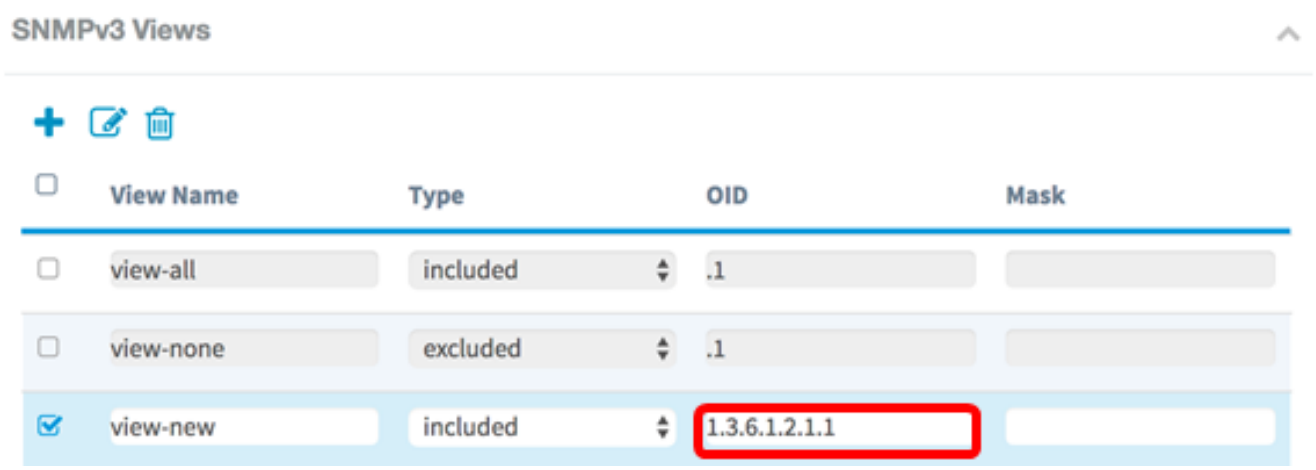
Paso 6. Del tipo lista desplegable, elija una opción si excluir o incluir la visión.

- incluido — Incluye la visión en la sub-estructura o la familia de sub-estructuras de la opinión MIB.
- excluido — Excluye la visión en la sub-estructura o la familia de sub-estructuras de la opinión MIB.



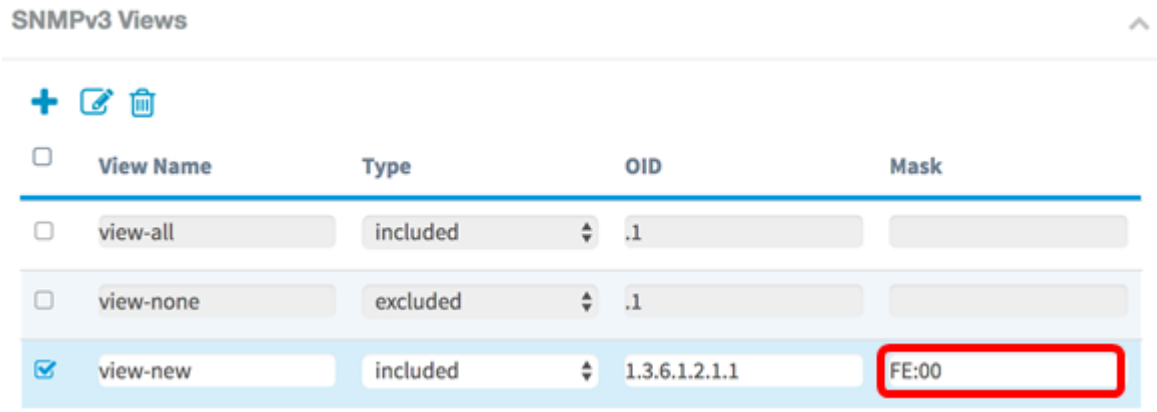
Paso 7. En el campo *OID*, ingrese una cadena OID para que la sub-estructura incluya o excluya de la visión. Cada número se utiliza para encontrar la información y cada número corresponde a una bifurcación específica del árbol OID. Los OID son Identificadores únicos de los objetos administrados en la jerarquía MIB. Los ID del objeto a nivel superior MIB pertenecen a diversas organizaciones de estándares, mientras que los ID del objeto de nivel inferior son afectados un aparato por las organizaciones asociadas. Las centrales privadas se pueden definir por los vendedores para incluir los objetos administrados para sus propios Productos. Números de la correspondencia de archivos MIB OID al formato legible. Para traducir el número OID al nombre del objeto, haga clic aquí.

Nota: En este ejemplo, se utiliza 1.3.6.1.2.1.1.



Paso 8. Ingrese una máscara OID en el campo de la *máscara*. El campo de la *máscara* se utiliza para controlar los elementos de la sub-estructura OID que se debe considerar como relevante cuando usted determina la visión en la cual un OID está, y el máximo es 47 caracteres de largo. El formato es 16 octetos de largo y cada octeto contiene dos caracteres hexadecimales separados por un período o los dos puntos. Para determinar la máscara, cuente el número de elementos OID y fije que muchos bits a uno. Solamente los formatos hexadecimales se validan en este campo. Considere el ejemplo OID 1.3.6.1.2.1.1, tiene siete elementos, así que si usted fijado siete 1s consecutivos siguió por un 0 en el primer octeto y todos los ceros adentro segundo, usted consigue FE:00 como la máscara.

Nota: En este ejemplo, se utiliza FE:00.



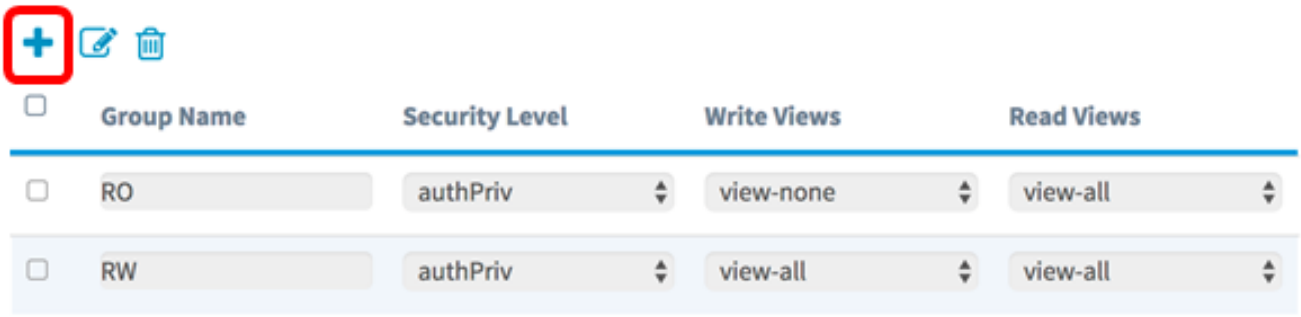
Paso 9. Tecleo 

.

Usted debe ahora haber configurado con éxito las opiniones SNMPv3 sobre el WAP125.

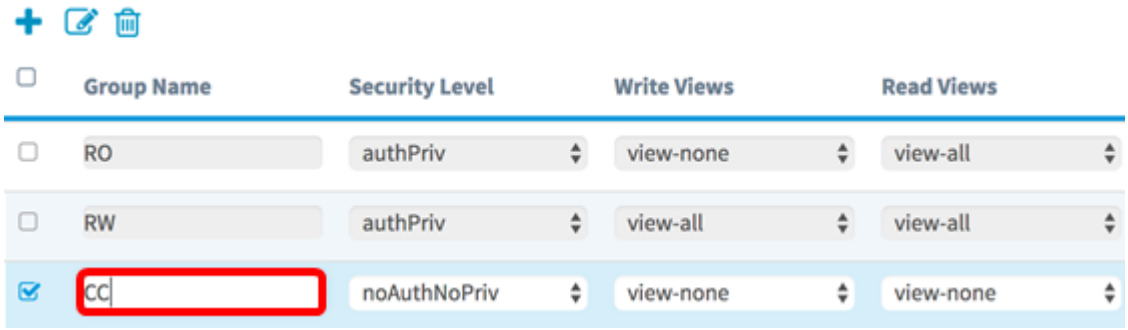
Configure los grupos SNMPv3

Paso 1. Haga clic **+** botón para crear una nueva entrada bajo grupos SNMPv3.



Paso 2. Ingrese un nombre usado para identificar al grupo en el campo de *nombre del grupo* . Los nombres predeterminados del RO y del RW no pueden ser reutilizados. Los nombres del grupo pueden contener hasta 32 caracteres alfanuméricos.

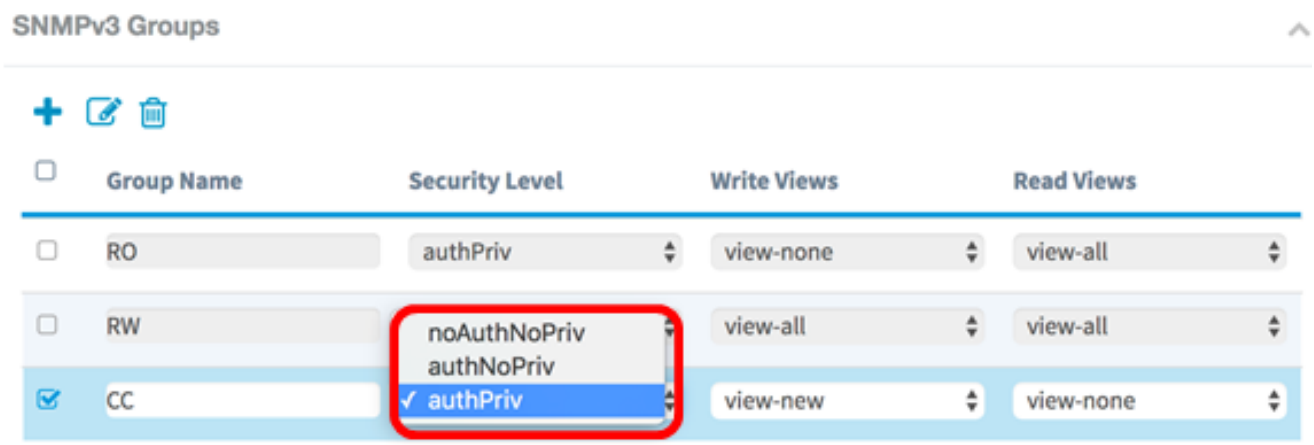
Nota: En este ejemplo, se utiliza el CC.



Paso 3. De la lista desplegable del nivel de seguridad, elija un nivel adecuado de autenticación.

- noAuthNoPriv — No proporciona a ninguna autenticación y a ninguna encripción de datos (ninguna Seguridad).
- authNoPriv — Provee autenticación pero ninguna encripción de datos (ninguna Seguridad). La autenticación es proporcionada por una frase de contraseña segura de la autenticación del hash (SHA).
- authPriv — Autenticación y encripción de datos. La autenticación es proporcionada por una frase de contraseña SHA. La encripción de datos es proporcionada por la frase de contraseña DES.

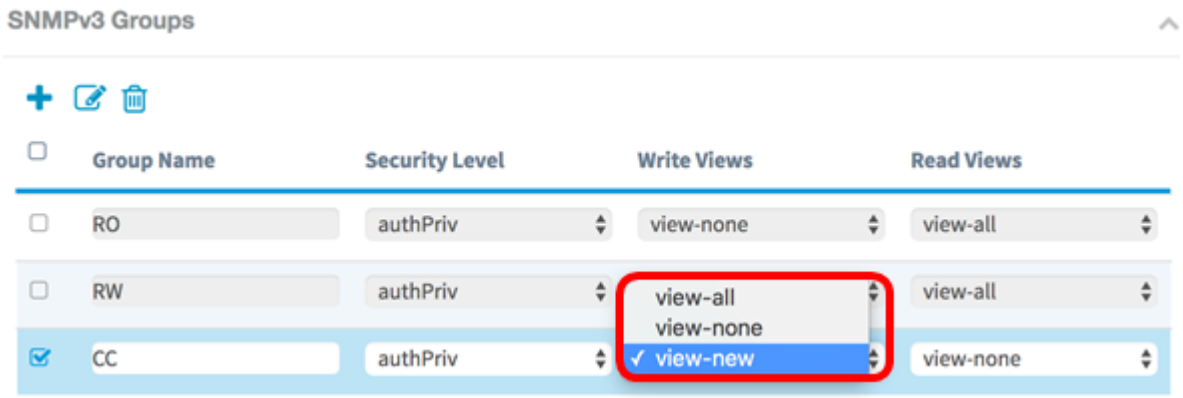
Nota: En este ejemplo, se utiliza el authPriv.



Paso 4. De la lista desplegable de las opiniones de la escritura, elija el acceso de escritura a

todos los objetos de la Administración (MIB) para el nuevo grupo. Esto define la acción que un grupo puede realizarse en el MIB. Esta lista también incluirá cualquier nueva opinión SNMP que se haya creado en el WAP.

Nota: En este ejemplo, vista-nuevo se utiliza.



Paso 5. Elija el acceso de lectura para todos los objetos de la Administración (MIB) para el nuevo grupo de la lista desplegable leída de las opiniones. Las opciones predeterminadas dadas abajo aparecen junto con cualquier otra visión creada en el WAP.

- vista-todo — Esto permite que los grupos vean y que lean todo el MIB.
- vista-ningunos — Esto restringe al grupo de modo que nadie pueda ver o leer cualquier MIB.
- vista-nuevo — Visión creada por el usuario.

Nota: En este ejemplo, se utiliza vista-ninguno.

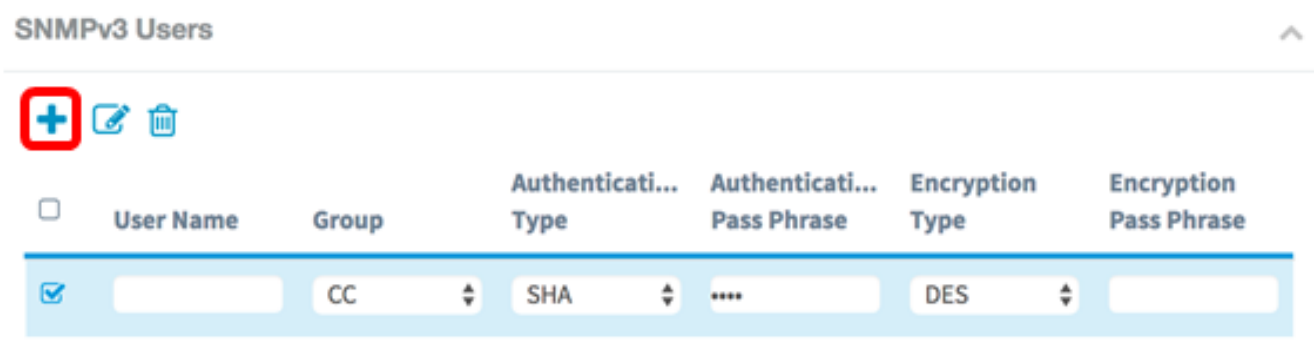
Paso 6. Tecleo Save.

Usted debe ahora haber configurado con éxito los grupos SNMPv3.

Configure a los usuarios SNMPv3

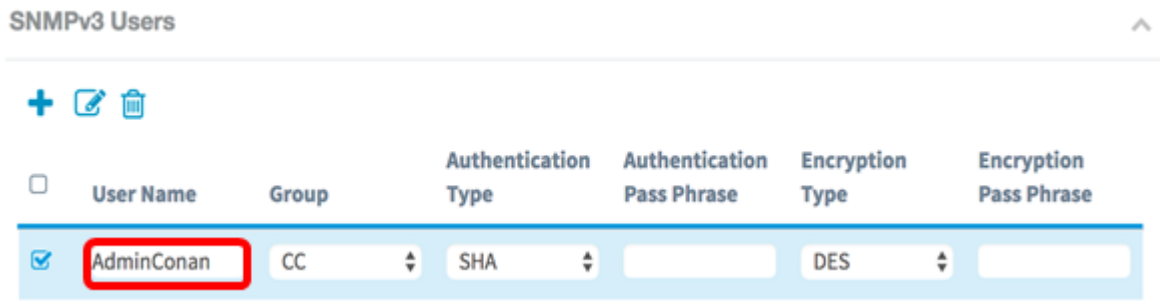
Sus credenciales de la clave define a un usuario SNMP (username, contraseñas, y método de autenticación) y se actúa en asociación con un grupo y el ID del motor SNMP. Solamente SNMPv3 utiliza a los usuarios SNMP. Asocian a los usuarios con los privilegios de acceso a una opinión SNMP.

Paso 1. Haga clic **+** botón para crear una nueva entrada bajo los usuarios SNMPv3.



Paso 2. En el campo de *Nombre de usuario*, cree un Nombre de usuario que denotaría a un usuario SNMP.

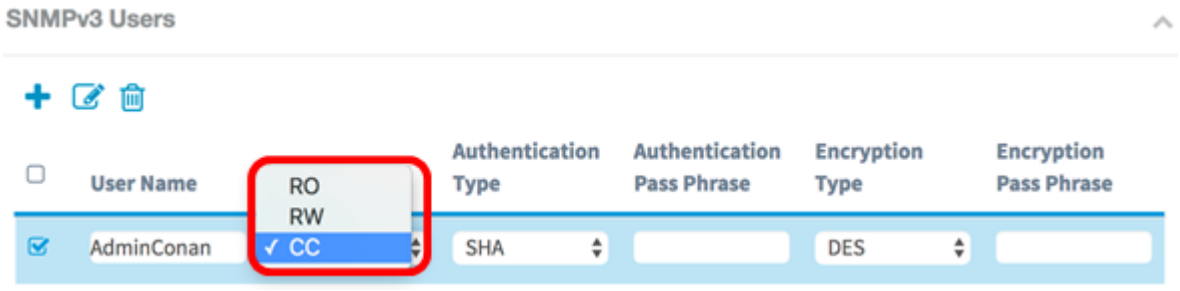
Nota: En este ejemplo, se utiliza AdminConan.



Paso 3. De la lista desplegable del grupo, elija a un grupo para asociar al usuario. Las opciones son:

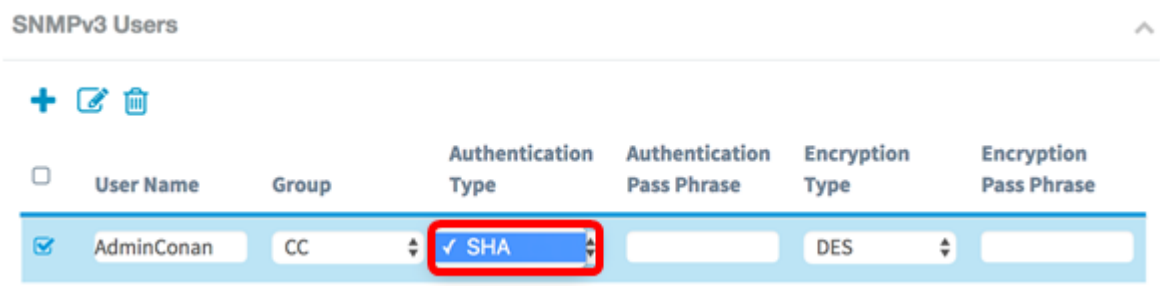
- RO — Grupo inalterable, creado por abandono. Este grupo permite que un usuario vea solamente la configuración.
- RW — Grupo de lectura/grabación, creado por abandono. Este grupo permite que un usuario vea y realice los cambios necesarios a la configuración.
- CC — CC, un grupo definido por el usario. El grupo definido por el usario aparece solamente si han definido a un grupo.

Nota: En este ejemplo, se elige el CC como definido en el paso 2 debajo configure los grupos SNMPv3.

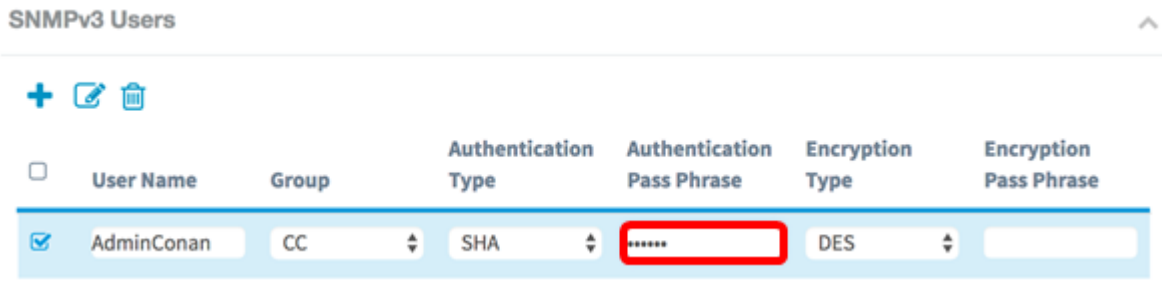


Paso 4. De la lista desplegable de la autenticación, elija **SHA**.

Nota: Esta área es greyed hacia fuera si el nivel de seguridad del grupo elegido en el paso 3 fue fijado al noAuthNoPriv.



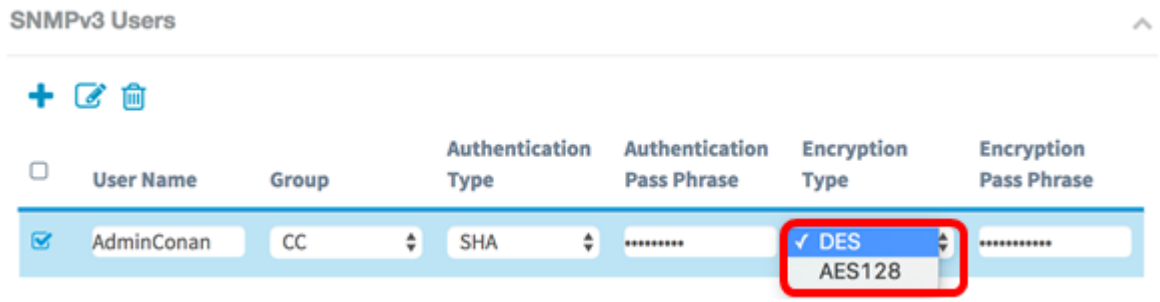
Paso 5. En el campo de la *palabra clave de la autenticación*, ingrese el passphrase asociado para el usuario. Ésta es la contraseña del SNMP que tiene que ser configurada para autenticar los dispositivos para que conecten con uno a.



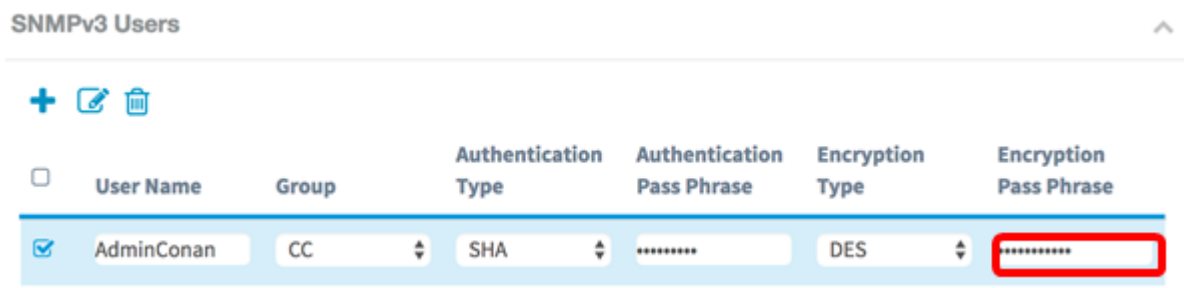
Paso 6. Del menú desplegable del tipo de encripción, elija un método de encripción para cifrar las peticiones SNMPv3. Las opciones son:

- DES — El Data Encryption Standard (DES) es un cifrado en bloque simétrico que utiliza una clave secreta compartida 64-bit.
- AES128 — Estándar de la encripción avanzado que utiliza una clave del 128-bit.

Nota: En este ejemplo, se elige el DES.



Paso 7. En el campo de la *palabra clave del cifrado*, ingrese el passphrase asociado para el usuario. Esto se utiliza para cifrar los datos enviados a los otros dispositivos en la red. Esta contraseña también se utiliza para desencriptar los datos sobre el otro extremo. La frase de contraseña tiene que hacer juego en los dispositivos de comunicación. La frase de contraseña puede extenderse a partir del ocho a 32 caracteres de largo.



Paso 8. Tecleo Save.

Usted debe ahora haber configurado con éxito a los usuarios SNMPv3 en el WAP125.

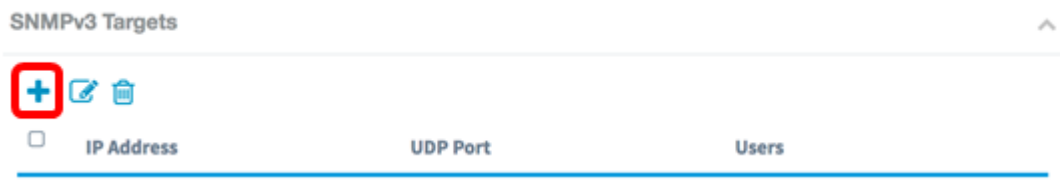
Configure las blancos SNMPv3

Una blanco SNMP refiere al mensaje enviado y al dispositivo de administración a los cuales se envían las notificaciones del agente. Cada blanco es identificada por el nombre objetivo, la dirección IP, el puerto UDP, y el Nombre de usuario.

SNMPv3 envían las notificaciones de la blanco SNMP como informan los mensajes al SNMP Manager bastante que los desvíos. Esto se asegura que salida lo haga de la blanco puesto que los desvíos no utilizan reconocen pero informe.

Paso 1. Haga clic **+** botón para crear una nueva entrada bajo blancos SNMPv3.

Nota: Un total de hasta 16 blancos pueden ser configuradas.



Paso 2. En el campo del *IP address*, ingrese el IP address de la blanco donde todo el SNMP traps será enviado. Éste es típicamente el direccionamiento del sistema de administración de red. Esto puede ser un direccionamiento IPv4 o del IPv6.

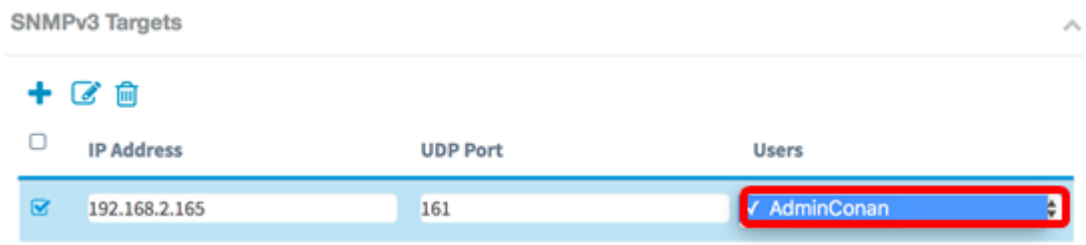
Nota: En este ejemplo, se utiliza 192.168.2.165.

Paso 3. Ingrese un número del puerto del User Datagram Protocol (UDP) en el campo de *puerto UDP*. El agente SNMP controla este puerto para saber si hay peticiones del acceso. El valor por defecto es 161. El intervalo válido está a partir de 1025 a 65535.

Nota: Por este ejemplo, se utiliza 161.

Paso 4. Elija al usuario para asociarse a la blanco de la lista desplegable de los usuarios. Esta lista muestra una lista de todos los usuarios creados en la página de los usuarios.

Nota: AdminConan se elige como el usuario.



Paso 5. Tecleo Save.

Usted debe ahora haber configurado con éxito las blancos SNMPv3 en el WAP125 y el WAP581.