Configuración de SNMP en terminales registrados en la nube

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Qué es SNMP

¿Qué información se puede solicitar?

Configuración de SNMP en un terminal registrado en la nube

- Activación del modo SNMPv2c en el concentrador de control
- Activación del modo SNMPv3 en el concentrador de control
  - ¿Cómo se ve la configuración SNMP en la GUI del terminal?
- Configuración del usuario USM para SNMPv3

Prueba de la Configuración de SNMPv2c y SNMPv3

¿Puede un terminal tener SNMPv2c y SNMPv3 activos simultáneamente?

¿Se pueden configurar varios terminales mediante el concentrador de control con SNMP?

Detalles importantes que debe recordar

Contacto con el TAC para resolver un problema de SNMP en un punto final

Información Relacionada

Introducción

Este documento describe cómo configurar y resolver problemas de SNMP en un terminal registrado en la nube.

Prerequisites

Requirements

Se recomienda que esté familiarizado con estos temas:

- Plataforma del hub de control
- Administración de terminales a través de la interfaz gráfica de usuario (GUI) del terminal y la sección de dispositivos del centro de control
- SSH a un terminal como usuario administrador
- SO de sala
- SNMP (SNMPv2c y SNMPv3)
- Snmpwalk u otra utilidad/herramienta o Network Management System (NMS) para probar la

configuración SNMP

Componentes Utilizados

El equipo que se detalla a continuación se ha utilizado para realizar las pruebas y obtener los resultados descritos en este documento:

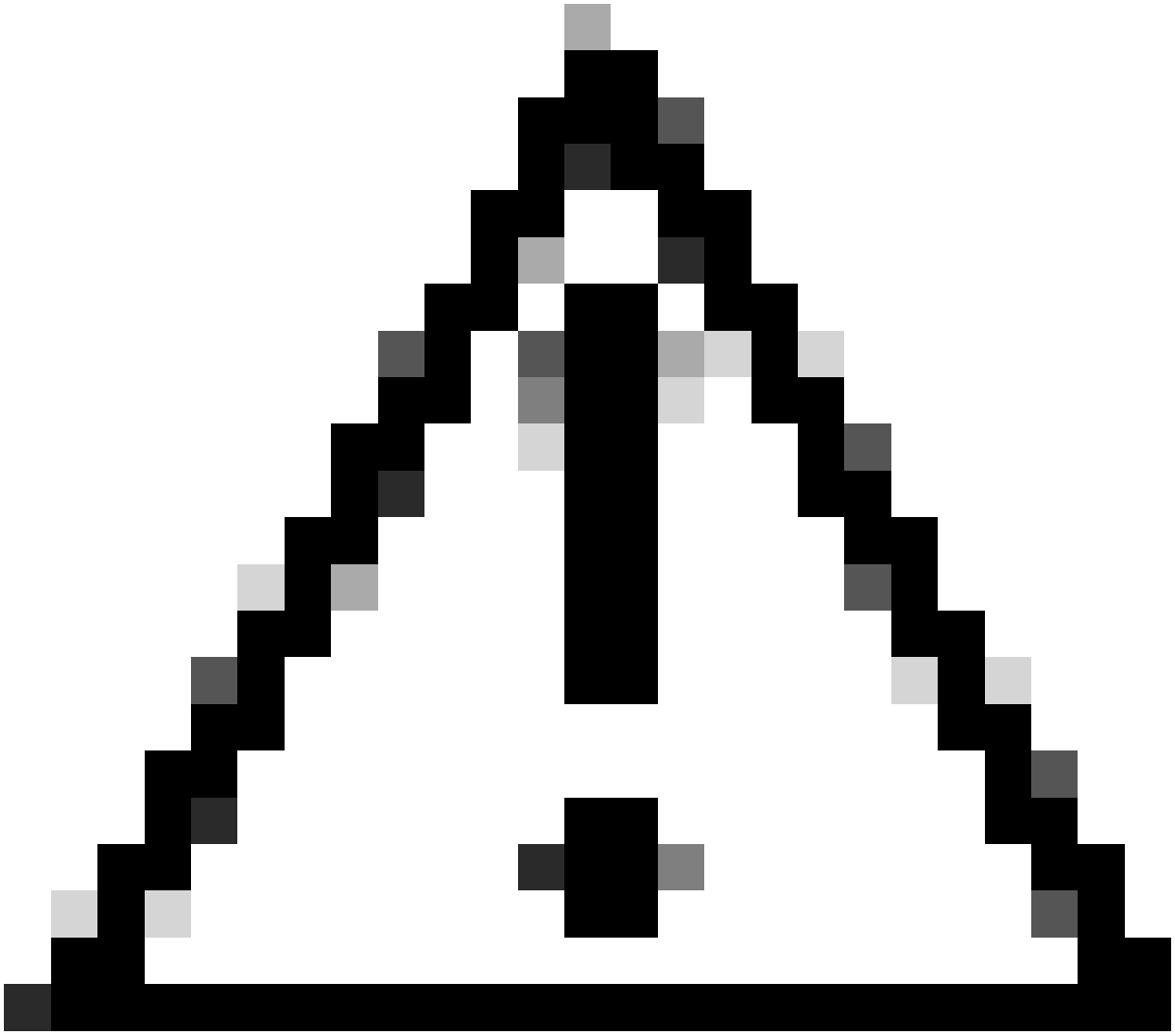
- Organización del centro de control
- Cisco Room Kit Pro
- Cisco Room Bar Pro
- Servidor Linux para alojar la utilidad snmpwalk para probar la configuración SNMP.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Qué es SNMP

SNMP significa protocolo simple de administración de red. Se trata de un protocolo que se utiliza para recopilar y administrar información sobre los dispositivos de una red, supervisar el estado de los dispositivos o realizar cambios en la configuración. Estos dispositivos pueden ser routers, switches, servidores, impresoras o cualquier otro tipo de dispositivo. Es un requisito previo que a estos dispositivos se les haya asignado una dirección IP. Hay tres versiones de SNMP. El sistema operativo de la sala admite SNMPv2c y SNMPv3. No se admite SNMPv1.

Este artículo se centra en la configuración y la resolución de problemas de SNMP en los terminales de colaboración que ejecutan el SO de la sala y están registrados en la nube (no se utiliza Webex Edge para dispositivos).



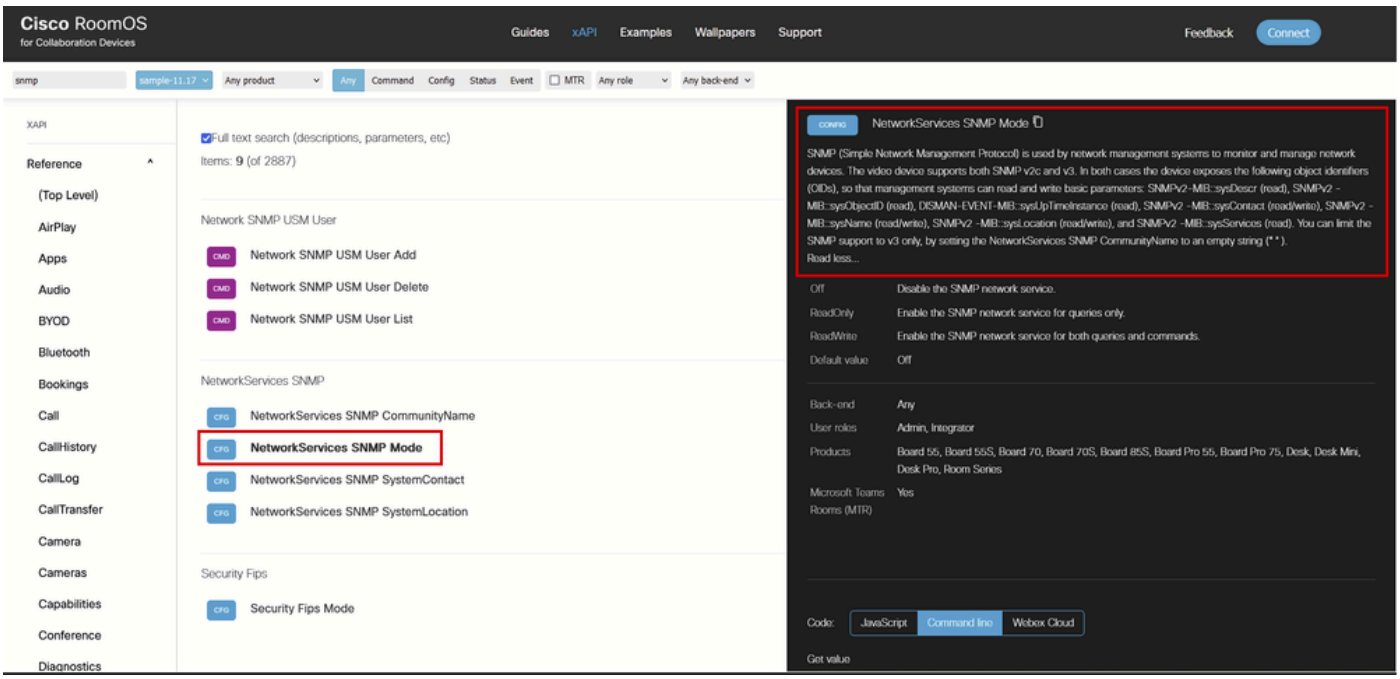
Precaución: En este artículo se aborda la configuración de SNMP sólo desde la perspectiva del terminal. Cualquier configuración realizada en el lado de la red y las herramientas utilizadas para solicitar/actualizar información relacionada con SNMP en los terminales están fuera del alcance de este artículo.

TAC no soporta la resolución de problemas de SNMP dentro de la red, ni puede ofrecer inferencias sobre por qué SNMP no funciona como se espera desde una perspectiva de red. Su equipo de red debe participar en la resolución de estos problemas.

La administración de SNMP se puede lograr con muchas herramientas diferentes. El TAC no admite estas herramientas. Si existe una discrepancia en la información que estas herramientas recopilan de los terminales, el equipo de red debe resolver el problema en primer lugar y, a continuación, derivarlo al TAC si existe suficiente información que pruebe que se trata de un problema relacionado con los terminales.

¿Qué información se puede solicitar?

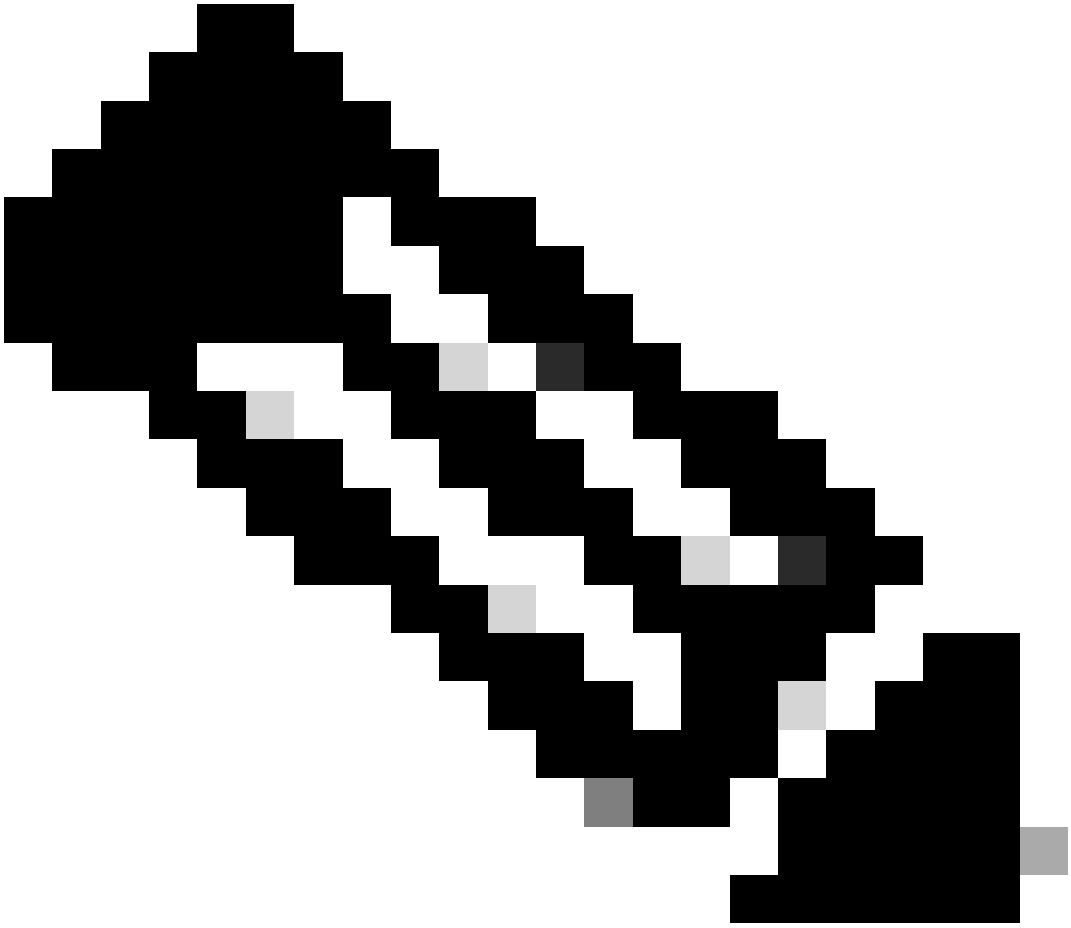
Con SNMP, puede solicitar una cantidad limitada de información del terminal. Los OID y los MiB admitidos se pueden ver en este enlace, en los detalles de la descripción del comando NetworkService SNMP Mode:



Descripción del comando NetworkService SNMP Mode en la documentación de xAPI de SO de sala

Los terminales exponen estos OID para SNMPv2 y SNMPv3:

- SNMPv2-MIB::sysDescr (lectura),
- SNMPv2 -MIB::sysObjectID (lectura),
- DISMAN-EVENT-MIB::sysUpTimeInstance (lectura),
- SNMPv2 -MIB::sysContact (lectura/escritura),
- SNMPv2 -MIB::sysName (lectura/escritura),
- SNMPv2 -MIB::sysLocation (lectura/escritura),
- SNMPv2 -MIB::sysServices (lectura).

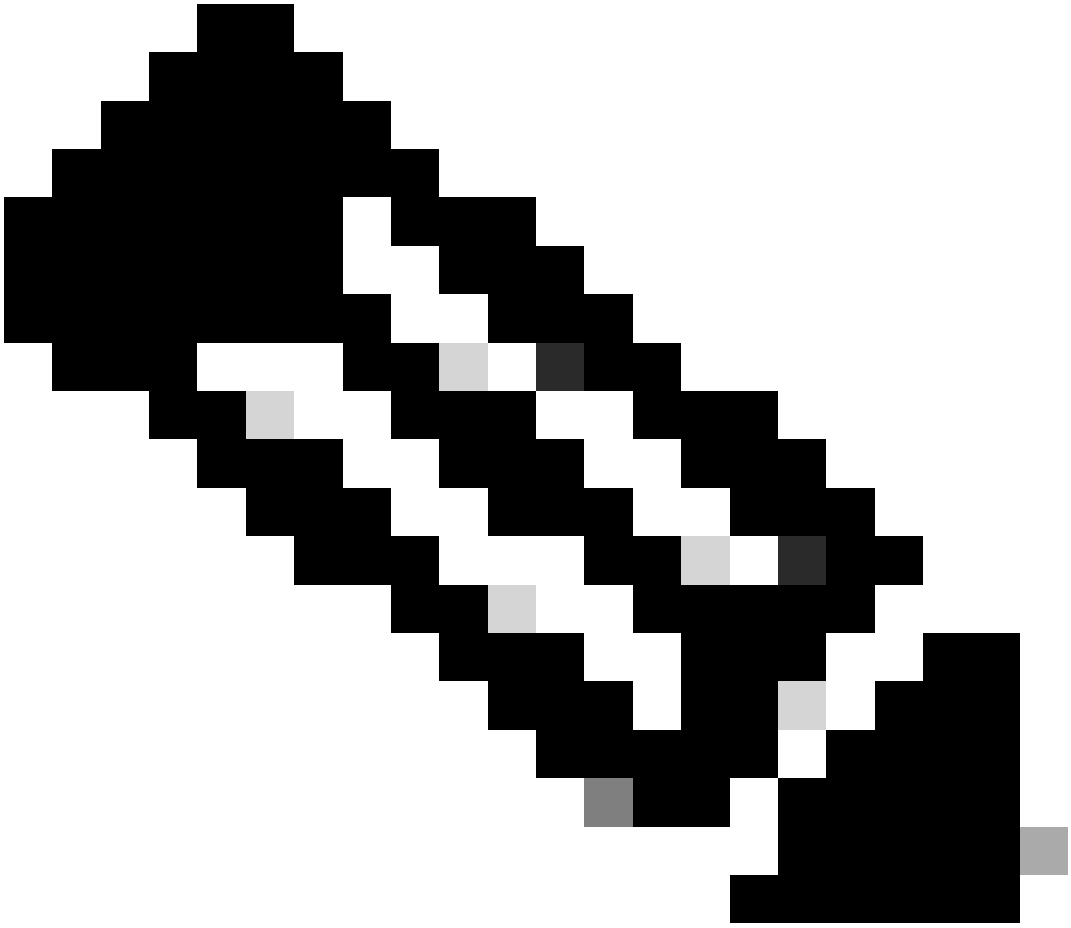


Nota: NetworkServices SNMP CommunityName se puede establecer en una cadena vacía si sólo desea utilizar SNMPv3.

Configuración de SNMP en un terminal registrado en la nube

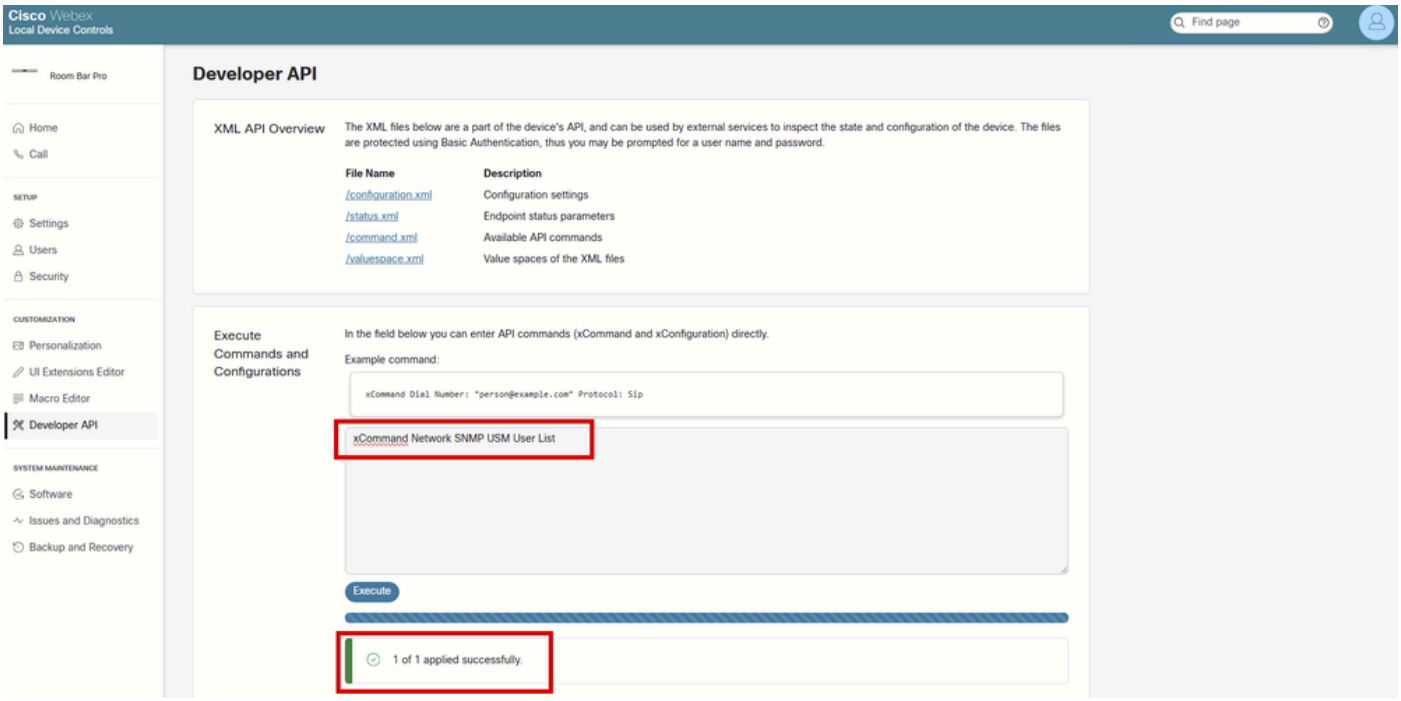
Por lo general, los cambios de configuración en los terminales se pueden producir de cuatro maneras diferentes:

1. Las API de Webex disponibles
2. La GUI del terminal
3. Concentrador de control
4. SSH directamente al terminal

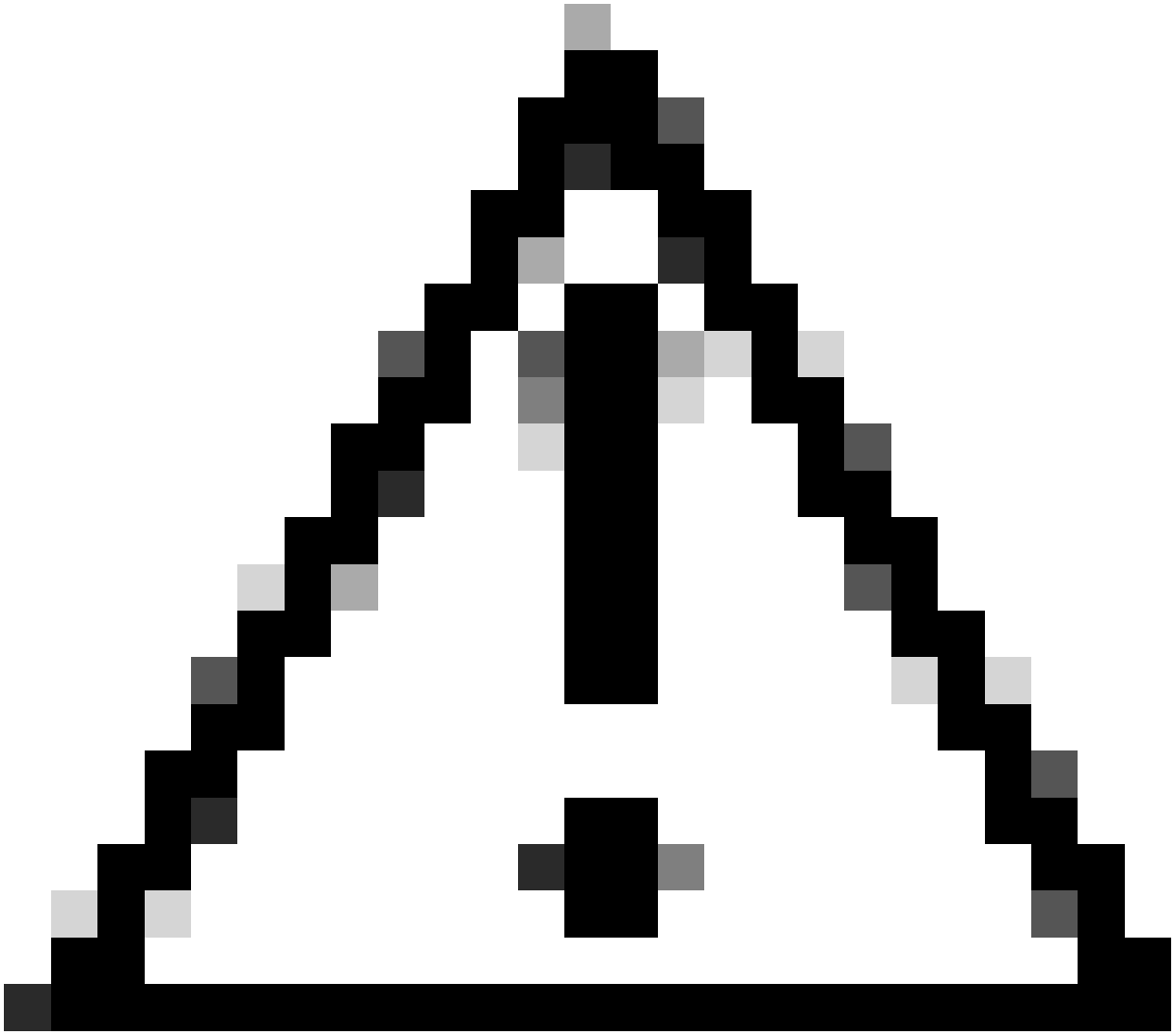


Nota: Para acceder a una GUI de terminal, abra un navegador y, en la barra de URL, escriba la dirección IP del terminal. Debe estar en la misma red que el terminal y contar con credenciales de usuario para poder iniciar sesión.

No todas las configuraciones se pueden realizar de las cuatro maneras. Para el escenario de este documento, el modo SNMP se puede habilitar de las cuatro maneras, pero para crear un usuario SNMP que pueda comunicarse con el dispositivo a través de SNMP, necesita hacer SSH al punto final, o utilizar las API de Webex, o utilizar la GUI del punto final en API del Desarrollador bajo la sección Personalización. No se pueden crear usuarios de USM desde la sección Control Hub All Configurations del terminal.



Sección API del desarrollador en la GUI del terminal

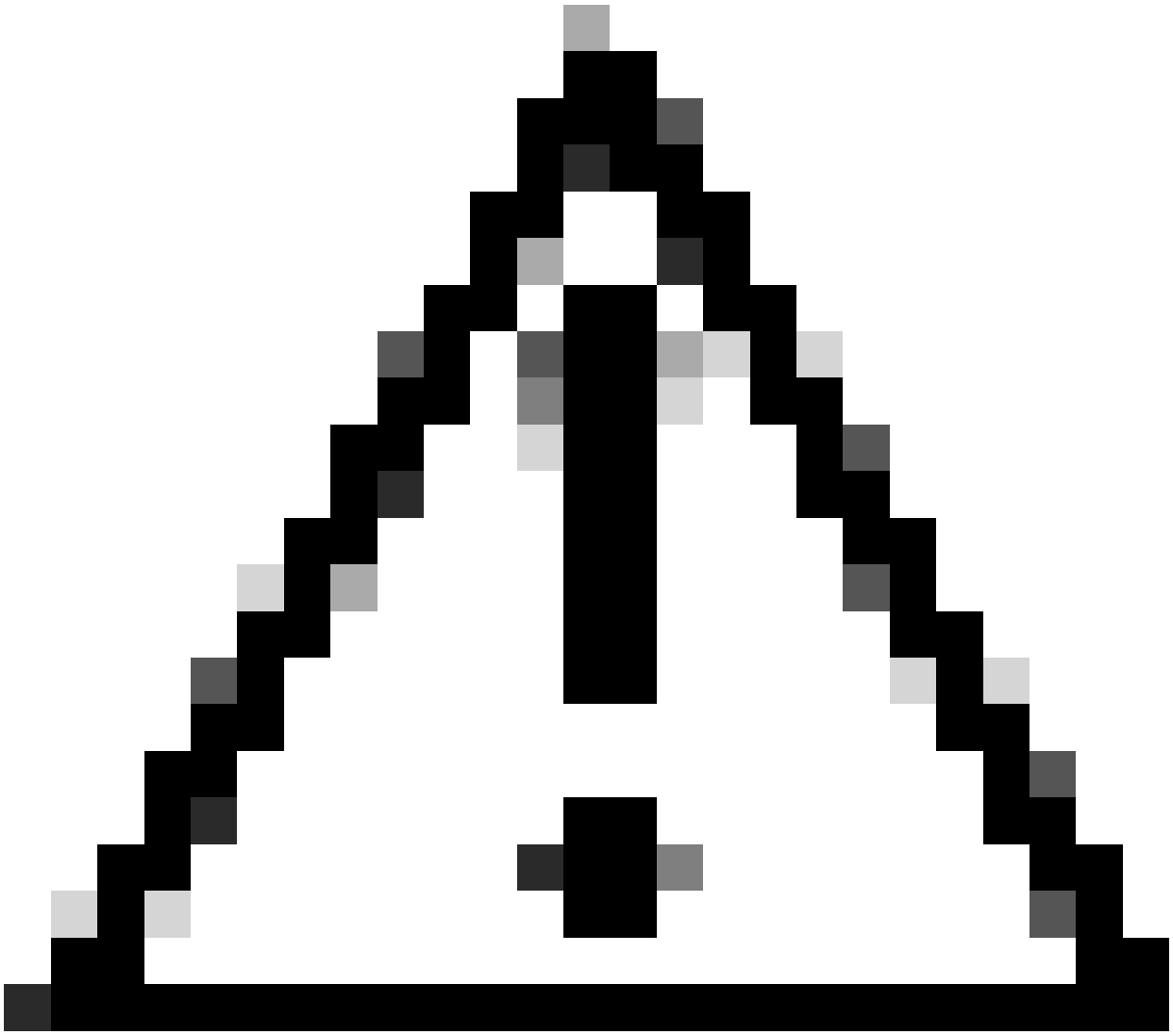


Precaución: Los comandos emitidos en el cuadro de texto Ejecutar comandos y configuraciones no devuelven ningún resultado. Sólo se ve si el comando se ejecutó correctamente o no. Esta es la razón por la que el comando que enumera los usuarios USM no devuelve ningún resultado en la captura de pantalla anterior. Esto significa que puede crear un usuario de USM desde esta sección de la GUI del terminal con éxito, pero para verificar nuevamente si el usuario se ha creado, necesita enviar SSH al dispositivo.

Para configurar SNMPv2c, no es necesario crear un usuario. La autenticación tiene lugar con el uso del nombre de comunidad (también llamado cadena de comunidad) que se configura en el terminal. El agente SNMP del terminal, que ya existe en el dispositivo, responde a las solicitudes que coinciden con el nombre de comunidad configurado en el dispositivo. Si una solicitud SNMP de un sistema de administración no incluye un nombre de comunidad coincidente (distingue entre mayúsculas y minúsculas), el mensaje se descarta y el agente SNMP del dispositivo de vídeo no va a enviar una respuesta.

Sin embargo, SNMPv3 requiere la configuración de un usuario USM para que la autenticación sea satisfactoria. Para este propósito, es necesario utilizar los comandos Network SNMP USM User .

Esto puede ocurrir mediante SSH directamente al dispositivo o mediante el uso de la GUI del dispositivo en la sección API del desarrollador. También se puede utilizar la API de Webex.

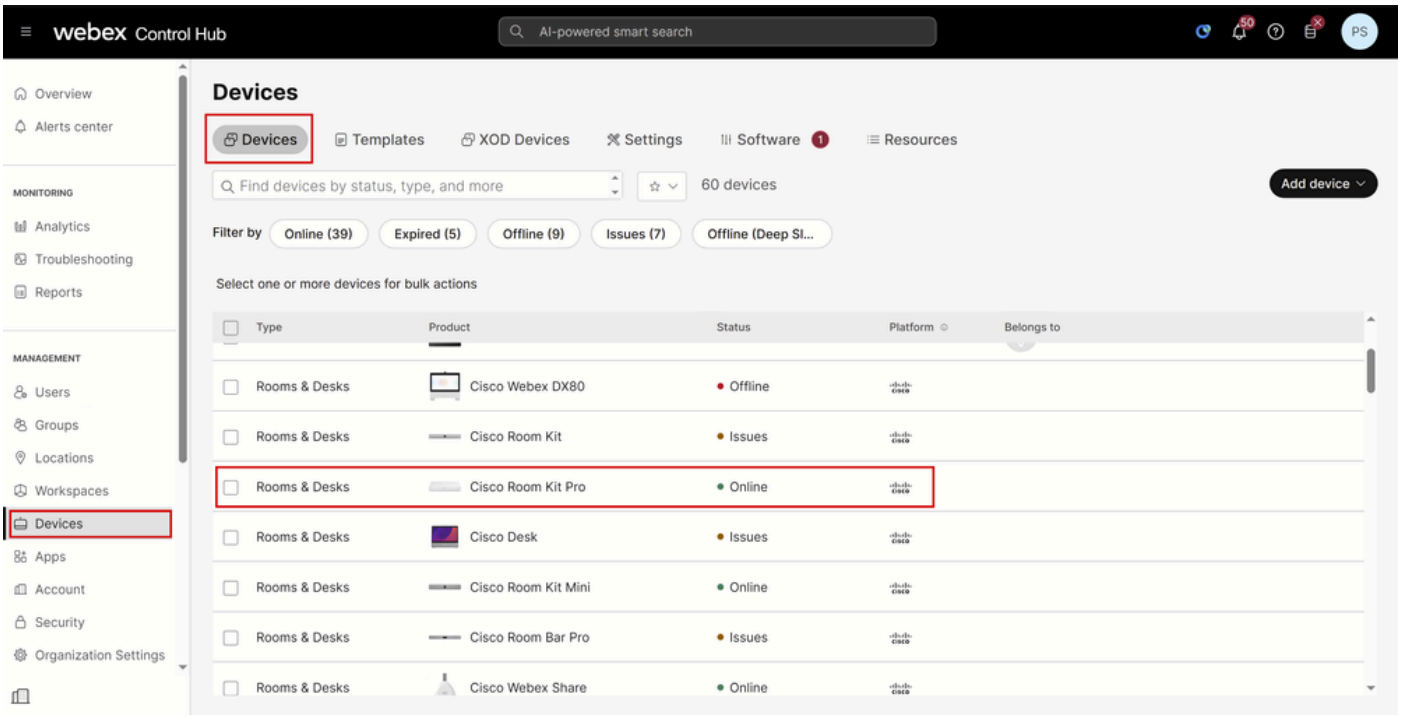


Precaución: Debe decidir si va a habilitar SNMPv2, SNMPv3 o ambos. SNMPv1 no es compatible con los terminales de Cisco. Cualquier intento de utilizar SNMPv1 va a fallar.

En este documento, los protocolos SNMPv2 y SNMPv3 se van a habilitar y configurar en el Hub de control, pero el usuario USM necesario para la autenticación SNMP3 se configura a través de SSH.

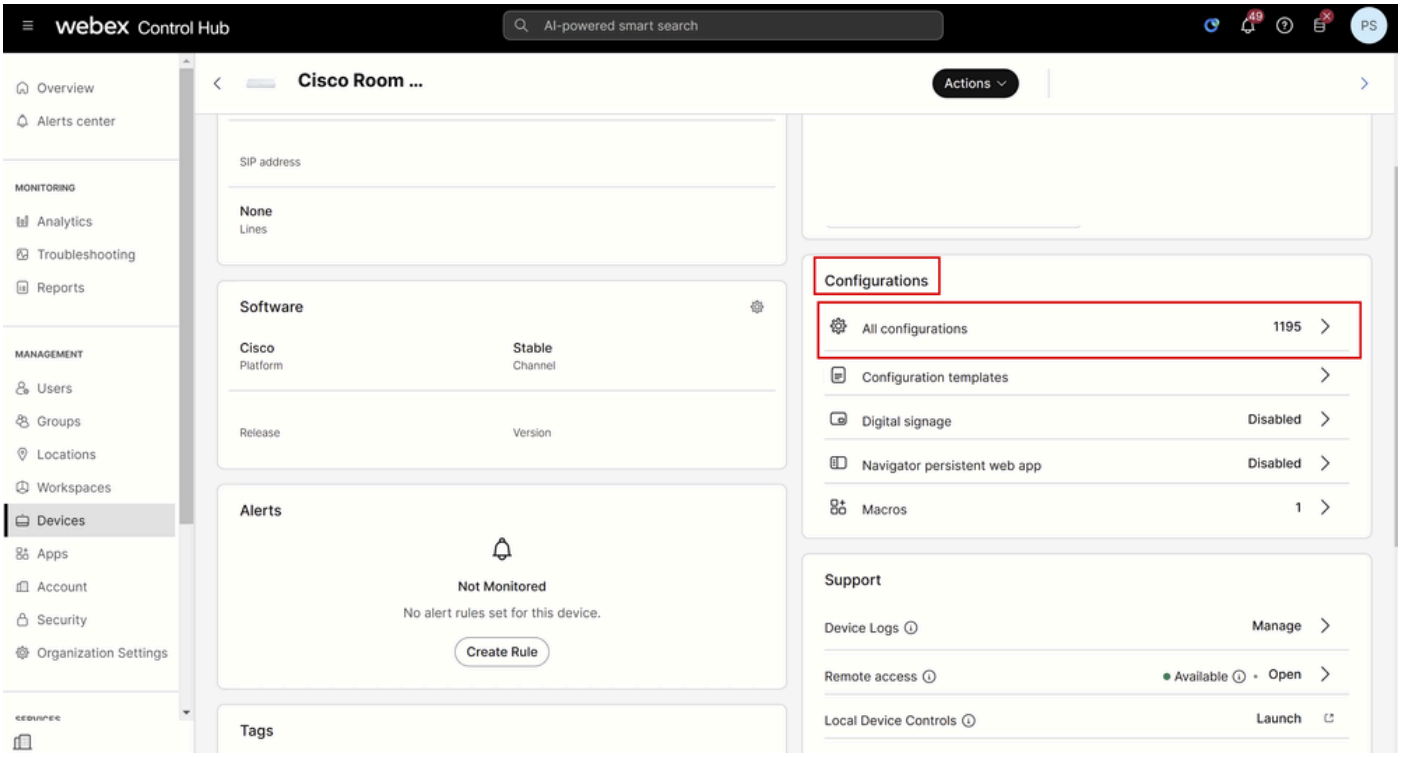
Activación del modo SNMPv2c en el concentrador de control

Navegue hasta admin.webex.com e inicie sesión con sus credenciales de administrador. Se sugiere que sea un administrador completo. Navegue hasta Dispositivos en la sección Administración en el lado izquierdo de la interfaz de usuario. En la ficha Devices, seleccione el dispositivo que desea configurar. En este ejemplo, se utiliza un Cisco Room Kit Pro.



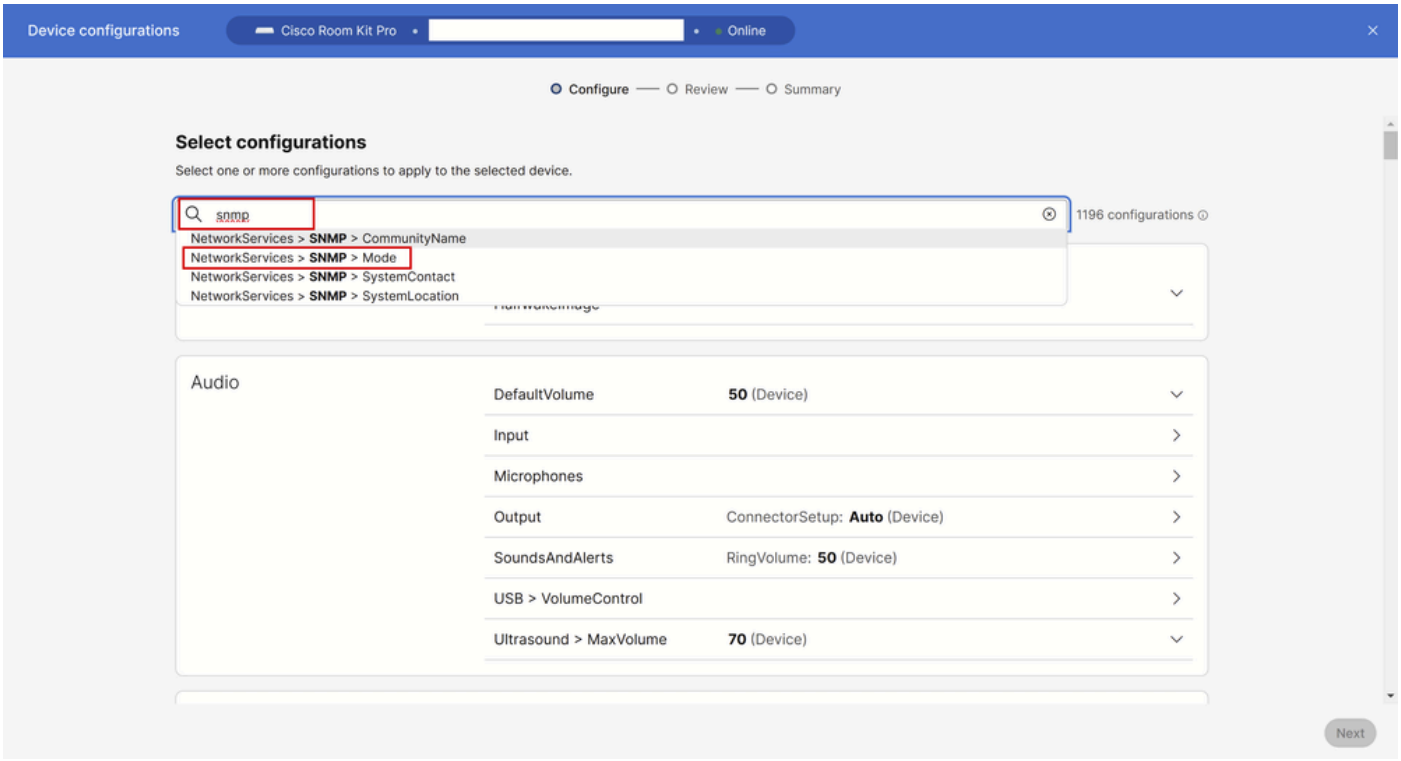
Sección Dispositivos del centro de control

En los detalles del dispositivo en la nueva página del concentrador de control que se abre, desplácese a la sección Configuraciones y haga clic en Todas las configuraciones:



Detalles del dispositivo del concentrador de control para Room Kit Pro

En la barra de búsqueda, escriba snmp y seleccione Network Services > SNMP > Mode:

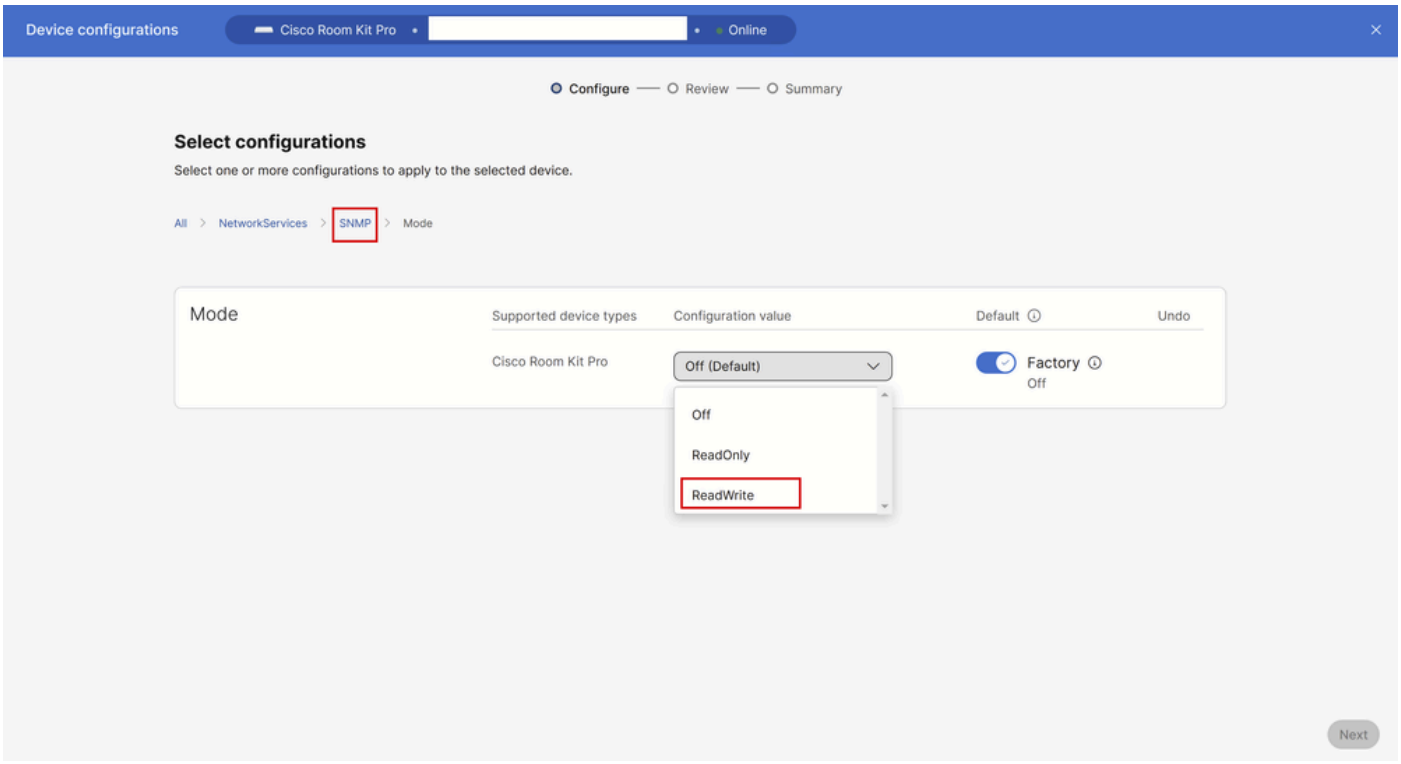


Ventana Control Hub All Configurations

Seleccione el modo que debe activar en su entorno. Hay tres opciones disponibles:

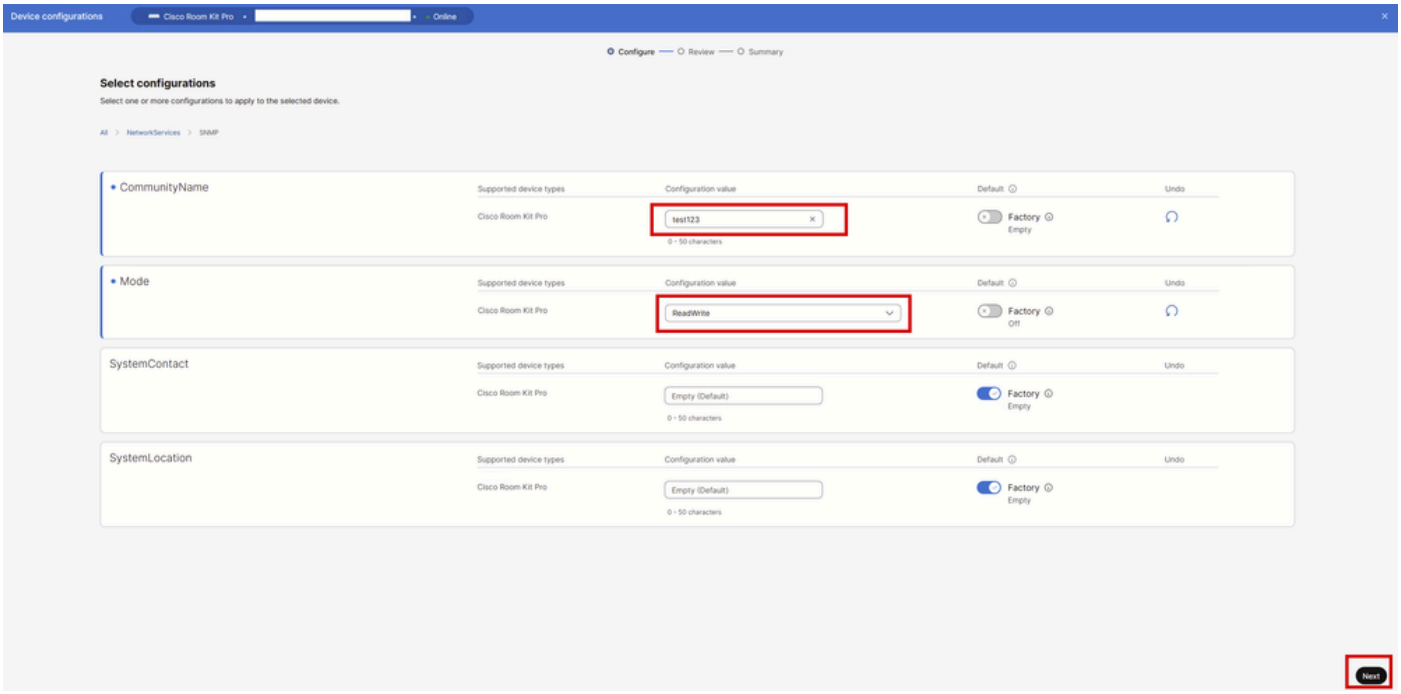
1. Desactivado: Desactive el servicio de red SNMP.
2. Sólo lectura: Active el servicio de red SNMP sólo para consultas.
3. LecturaEscritura: Habilite el servicio de red SNMP para consultas y comandos.

Para este ejemplo, se selecciona ReadWrite. A continuación, haga clic en SNMP en la sección de navegación de la configuración, como se ve en la imagen. Esto le lleva de nuevo un paso en la configuración, y puede ver todos los ajustes relacionados con SNMP que se pueden configurar en el dispositivo a través del concentrador de control:



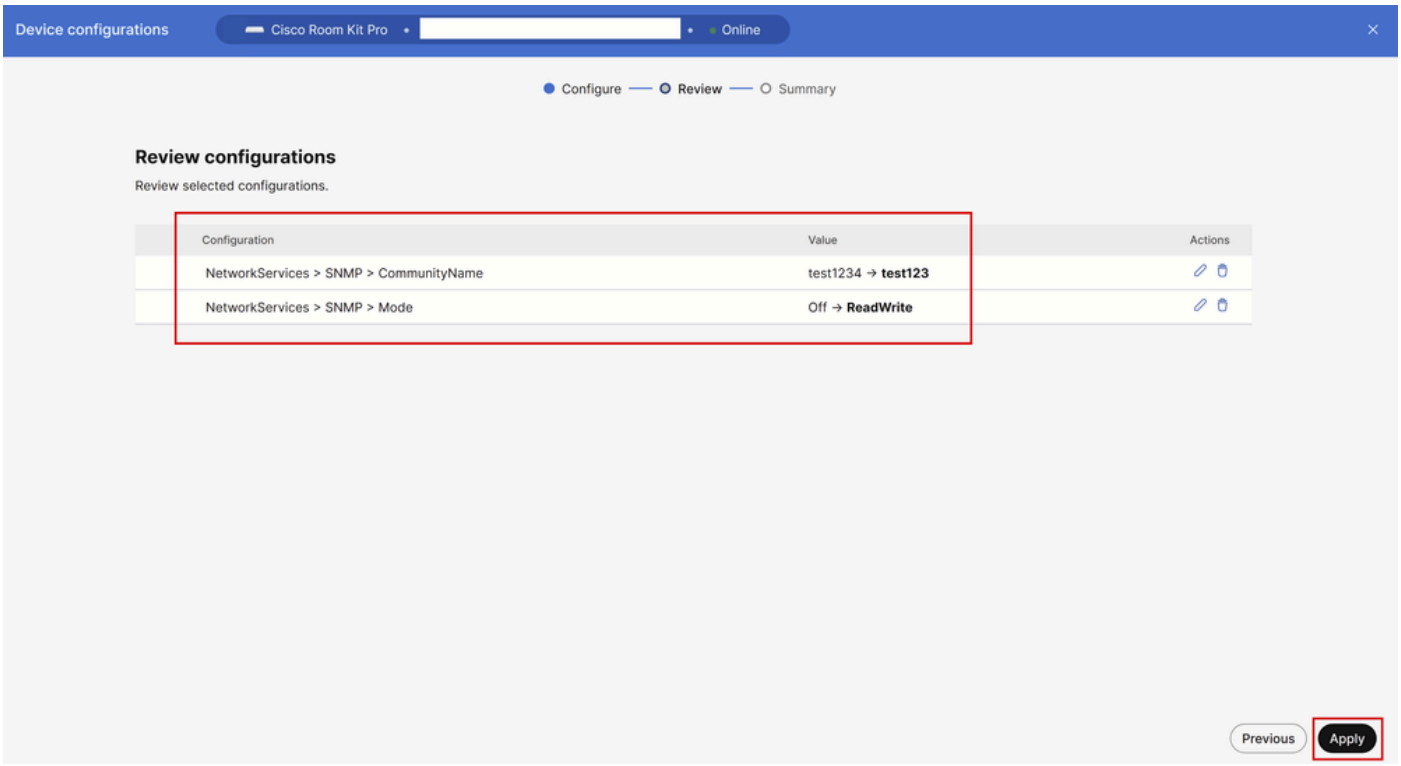
Configuración del modo SNMP en Todas las configuraciones de Control Hub

Después de hacer clic en SNMP, aparecen todas las opciones SNMP disponibles, como se ve en esta imagen. Para que SNMPv2 se configure correctamente, es necesario configurar un nombre de comunidad. El nombre de comunidad se utiliza para la autenticación entre el servidor SNMP y el agente SNMP que existe en el terminal. El nombre de comunidad se establece en test123 para este ejemplo. Haga clic en Next en la esquina inferior derecha.



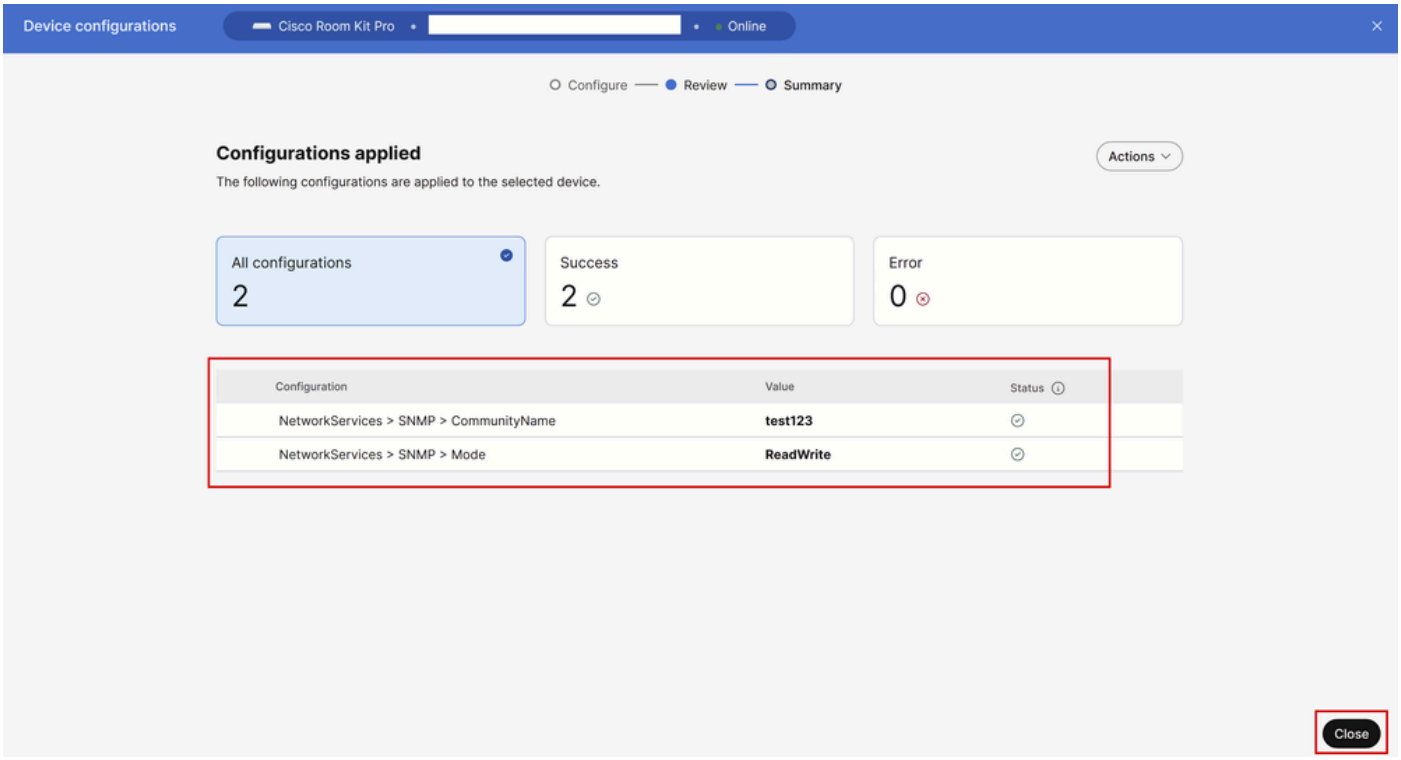
Configuración de SNMP en Todas las configuraciones del concentrador de control

Revise las configuraciones del dispositivo y haga clic en Apply en la esquina inferior derecha:



Revise las configuraciones antes de aplicar los cambios

Compruebe que los cambios de configuración se han aplicado correctamente. A continuación, haga clic en Cerrar.



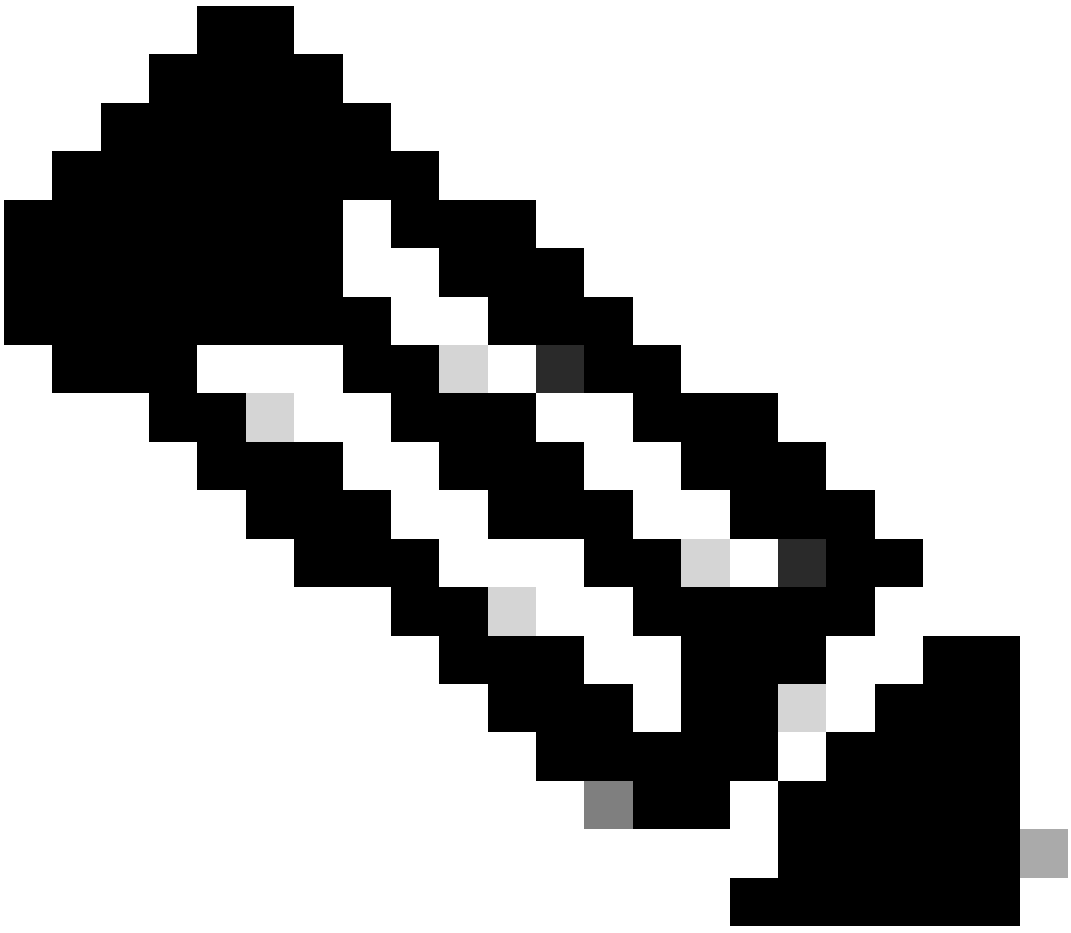
Configuraciones de terminales aplicadas correctamente en Control Hub

En esta etapa, SNMPv2c se habilita correctamente en el terminal y se configura el nombre de la comunidad.

Activación del modo SNMPv3 en el concentrador de control

SNMPv3 proporciona más seguridad y requiere una configuración diferente en el terminal en comparación con SNMPv2c. Navegue hasta Dispositivos en la sección Administración en Control Hub. Permanezca bajo la pestaña Devices y seleccione uno de sus terminales que desee configurar con SNMPv3. Para este ejemplo, se utiliza Cisco Room Bar Pro.

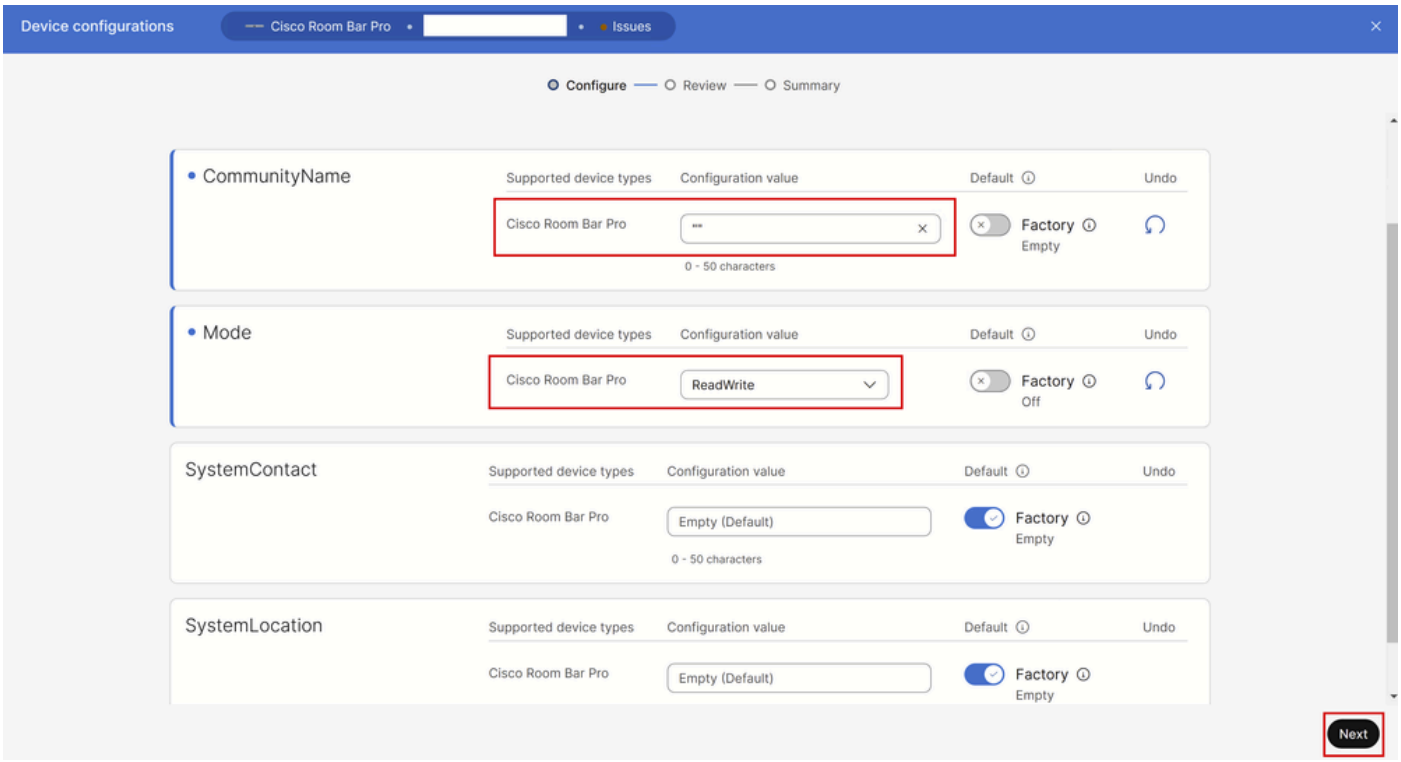
En los detalles del dispositivo, vaya a la sección Configuraciones y haga clic en Todas las configuraciones. Se abre la página Configuraciones de dispositivo. Escriba snmp en la barra de búsqueda y seleccione Network Services > SNMP > Mode. En este ejemplo, el modo SNMP se establece en ReadWrite. Haga clic en SNMP para ver todos los parámetros SNMP configurables en el dispositivo.



Nota: Todos los pasos mencionados hasta ahora para SNMPv3 ya se han descrito cuando SNMPv2c se configuró en un ejemplo anterior. Debido a esto, no se proporciona ninguna captura de pantalla de los pasos. Consulte la sección Activar el modo SNMPv2c en el concentrador de control si tiene alguna duda sobre cómo desplazarse por los

parámetros del concentrador de control.

Para soportar solamente SNMPv3, necesita configurar el nombre de la comunidad como una cadena vacía entre comillas: "".



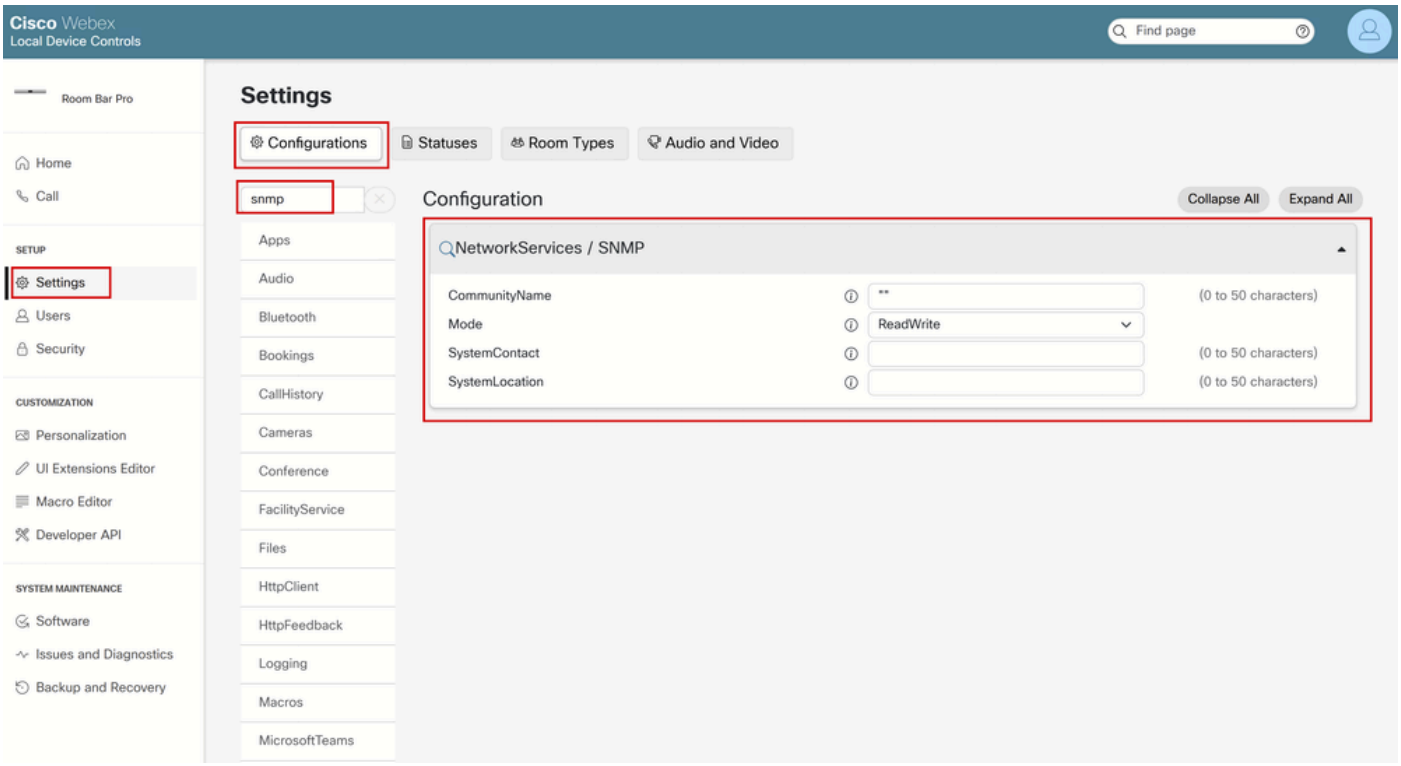
Configuración de SNMP en Todas las configuraciones del concentrador de control

Haga clic en Next, revise los cambios de configuración y haga clic en Apply. Haga clic en Cerrar para cerrar la página de configuración del dispositivo.

Esto concluye la configuración que se puede realizar en el concentrador de control. En esta etapa, sólo SNMPv3 está habilitado.

¿Cómo se ve la configuración SNMP en la GUI del terminal?

Las mismas configuraciones se pueden realizar desde la GUI del dispositivo. Abra una ficha del navegador y escriba la dirección IP del terminal (debe estar en la misma red que el terminal). Inicie sesión como un usuario admin y en la GUI del terminal, navegue hasta Settings en la sección SETUP. Permanezca en la ficha Configuraciones y en la barra de búsqueda de configuraciones escriba snmp. Esta imagen muestra cómo se muestran los parámetros SNMP para la configuración SNMPv3 realizada en Room Bar Pro en la sección anterior:



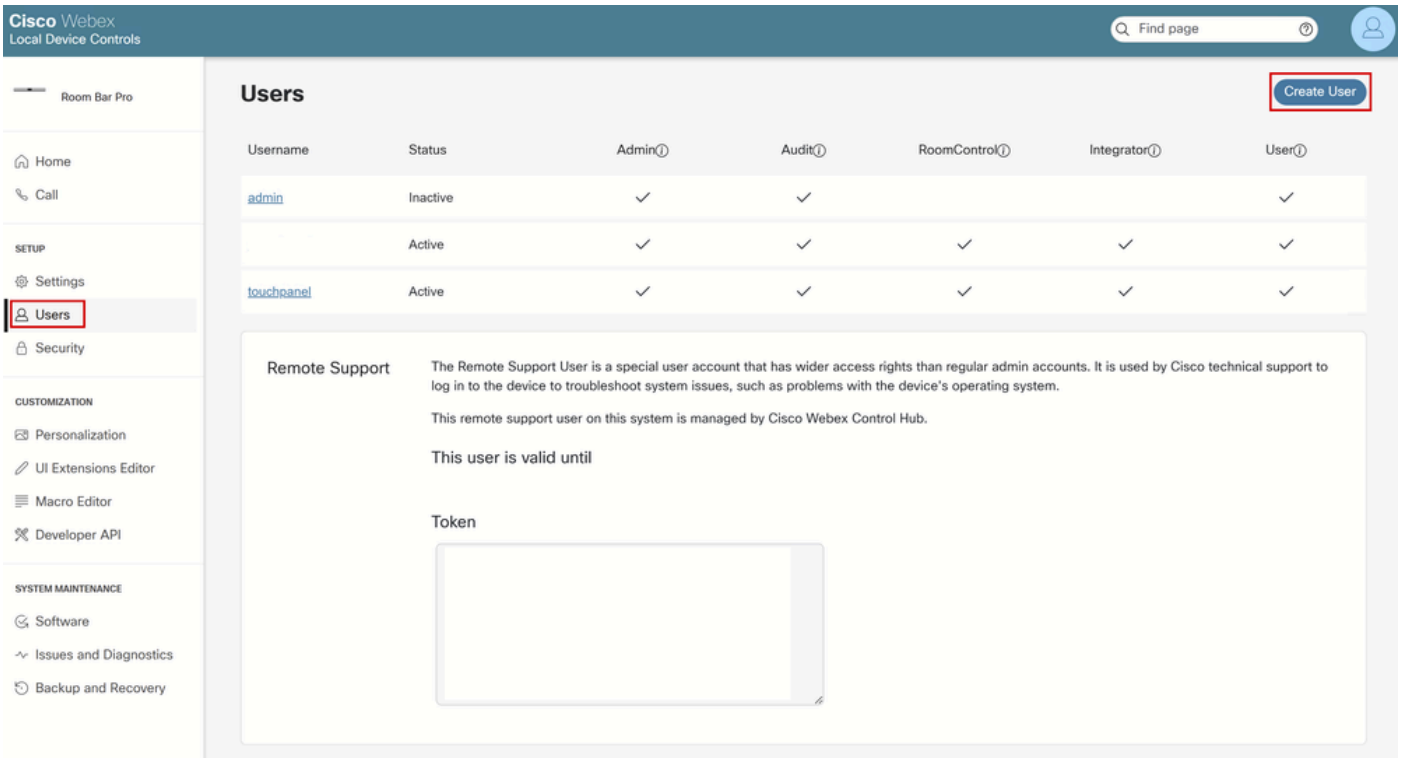
Configuración de SNMPv3 en la GUI del terminal

Configuración del usuario USM para SNMPv3

Para poder utilizar SNMPv3, debe crear un usuario USM. Los comandos disponibles para realizar esta acción se pueden encontrar en el enlace de documentación de Room OS aquí. Utilice SSH para conectarse al dispositivo. Para ello, debe tener una cuenta de administrador en el dispositivo. Si no es así, debe crear una cuenta de administrador. Esta sección pasa por todo este proceso.

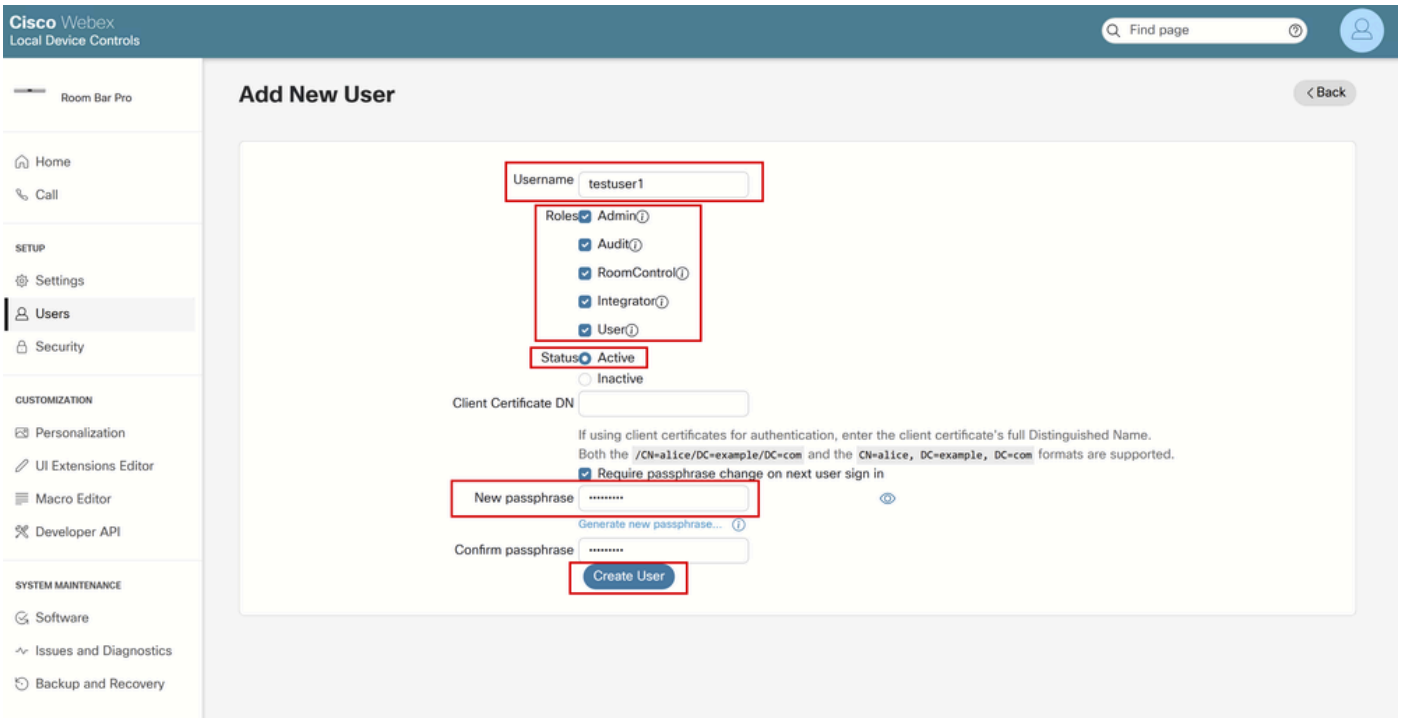
Navegue hasta Dispositivos en la sección Administración en Control Hub. Permanezca en la pestaña Devices y seleccione uno de los terminales para el que desea crear un usuario administrador. Para este ejemplo, se utiliza un Cisco Room Bar Pro.

En los detalles del dispositivo, desplácese a la sección Soporte y haga clic en Controles de dispositivo local (debe estar en la misma red que el terminal para que esto funcione). Se abre la GUI del dispositivo. Navegue hasta Usuarios en la sección CONFIGURACIÓN y haga clic en Crear usuario.



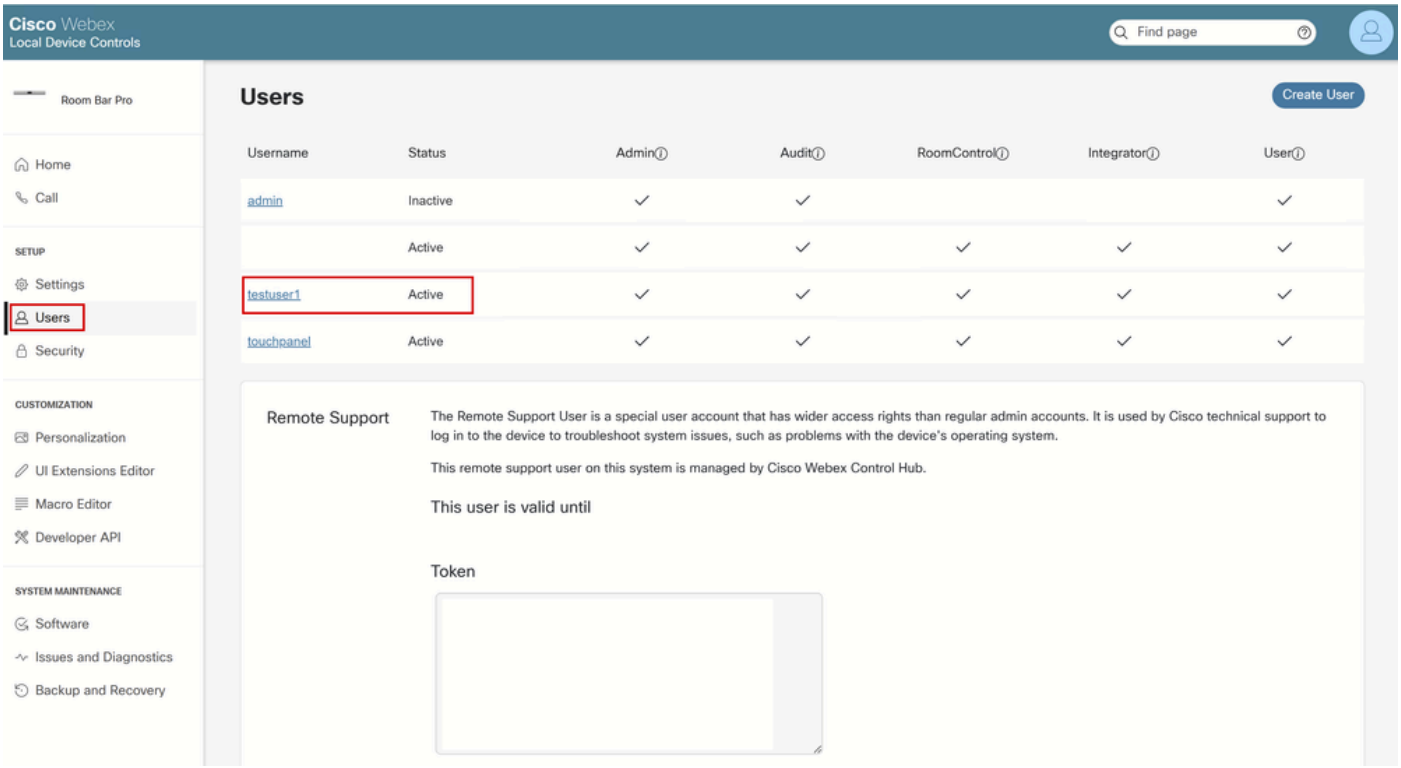
Sección Usuarios de la GUI del terminal

Proporcione un nombre de usuario y una frase de paso (contraseña). Asegúrese de que el usuario tiene privilegios de administrador completos y está activo:

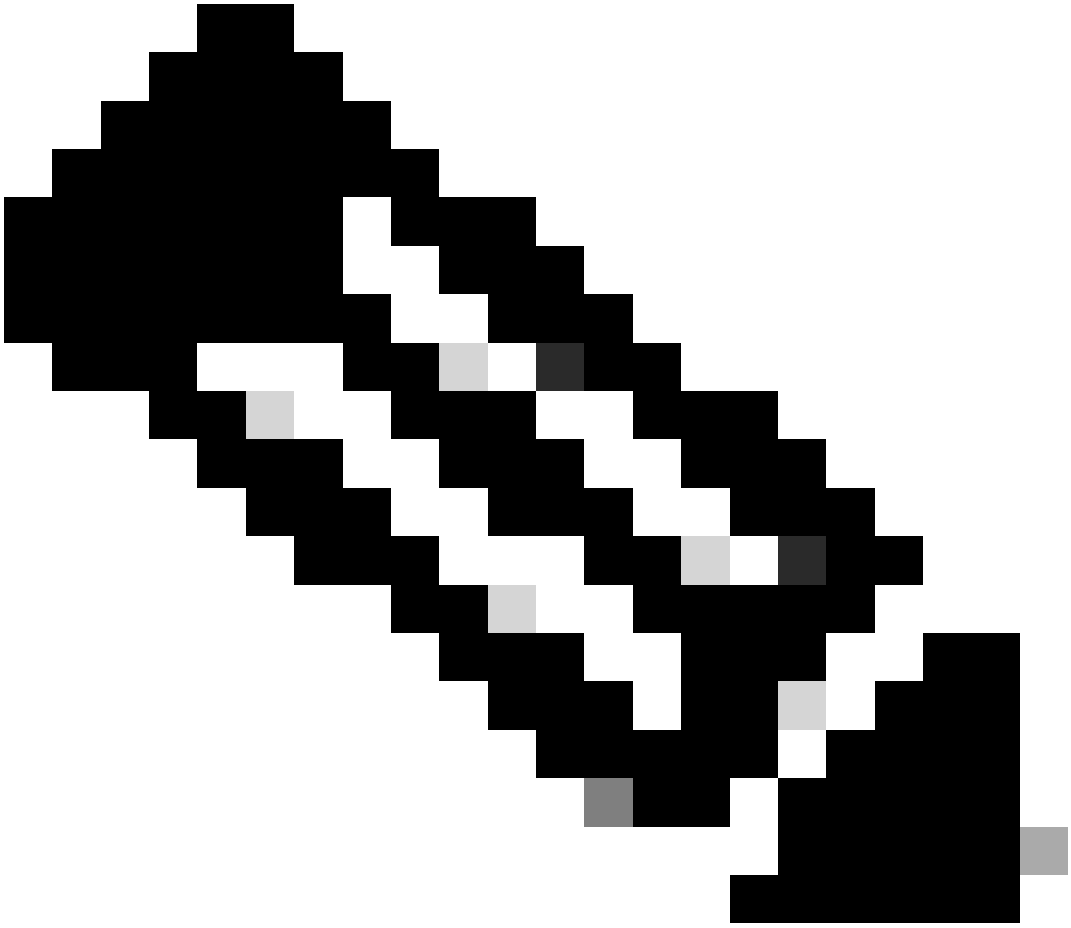


Crear un usuario desde la GUI del terminal

Verifique que el usuario se ha creado y está activo desde la página Users:



Nuevo usuario creado y listado entre otros usuarios



Nota: En el primer intento de inicio de sesión de SSH con un usuario recién creado, se le pedirá que cambie su contraseña. Aparece un mensaje similar a:

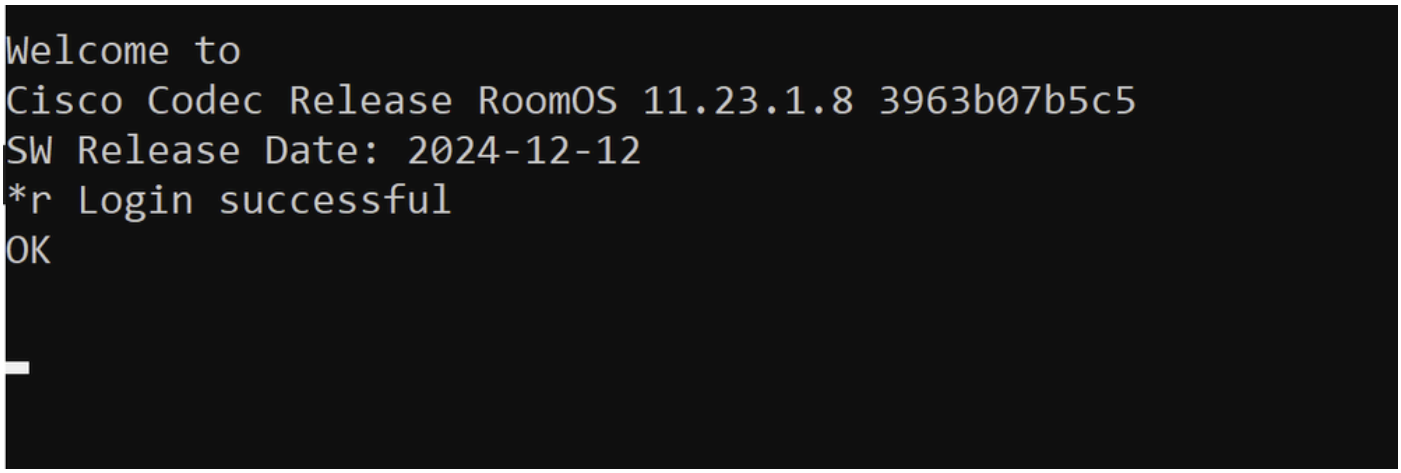
```
You are required to change your password.
Enter current password:
Enter new password:
Enter new password again:
OK
```

Cambiar contraseña cuando SSH por primera vez

Una vez que se cambia la contraseña, se le desconecta inmediatamente y necesita iniciar una nueva conexión SSH.

Una vez que el usuario administrador se haya creado correctamente, utilice un cliente SSH de su elección y conéctese al terminal. Inicie sesión con las credenciales de administrador. Este es el

mensaje que ve:



Intento de inicio de sesión correcto a través de SSH al terminal

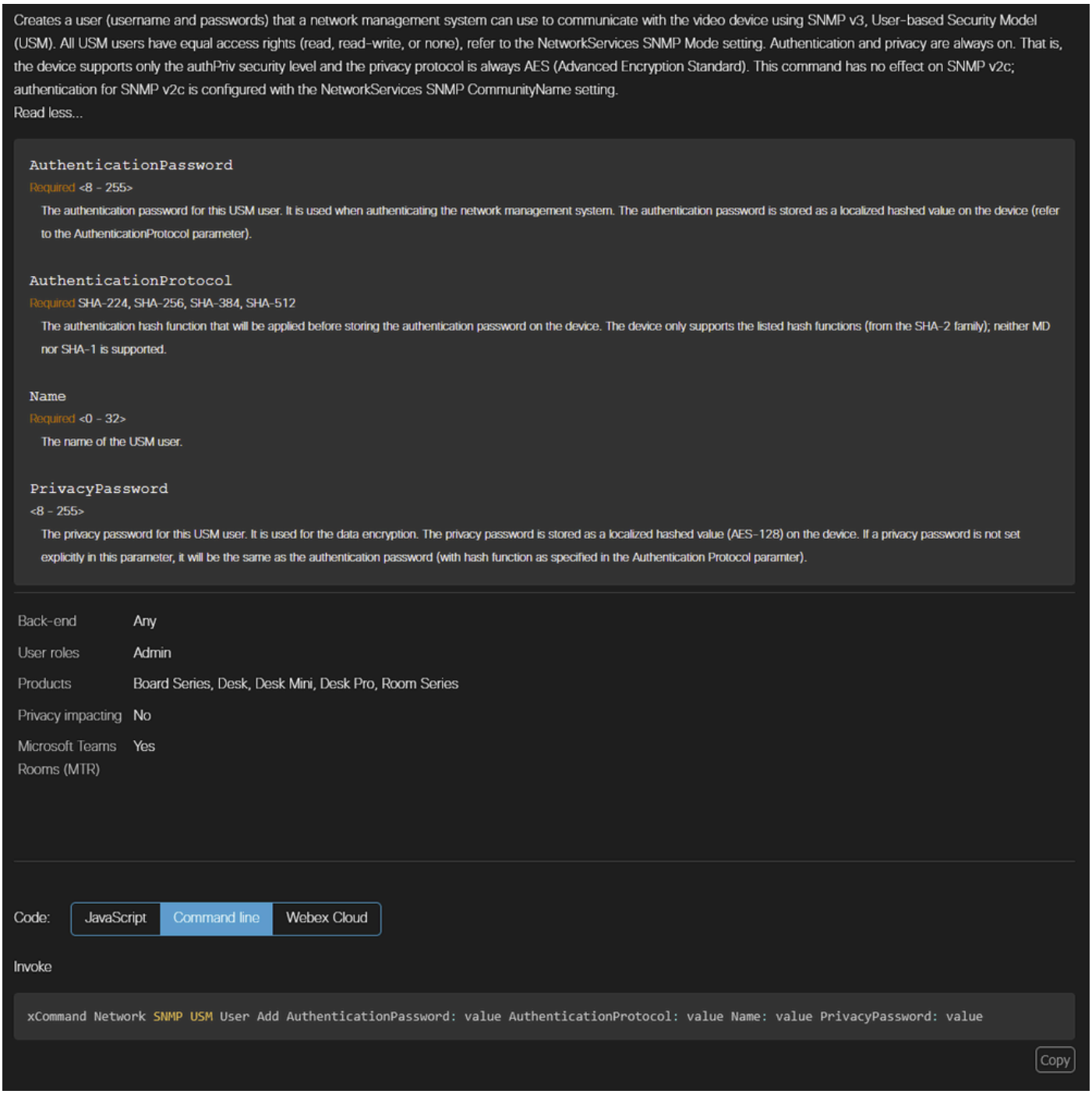
Utilice el comando Network SNMP USM User Add como se describe en este artículo. Para esta demostración, el comando utilizado es:

```
xCommand Network SNMP USM User Add AuthenticationPassword: testuser123 AuthenticationProtocol: SHA-256
```

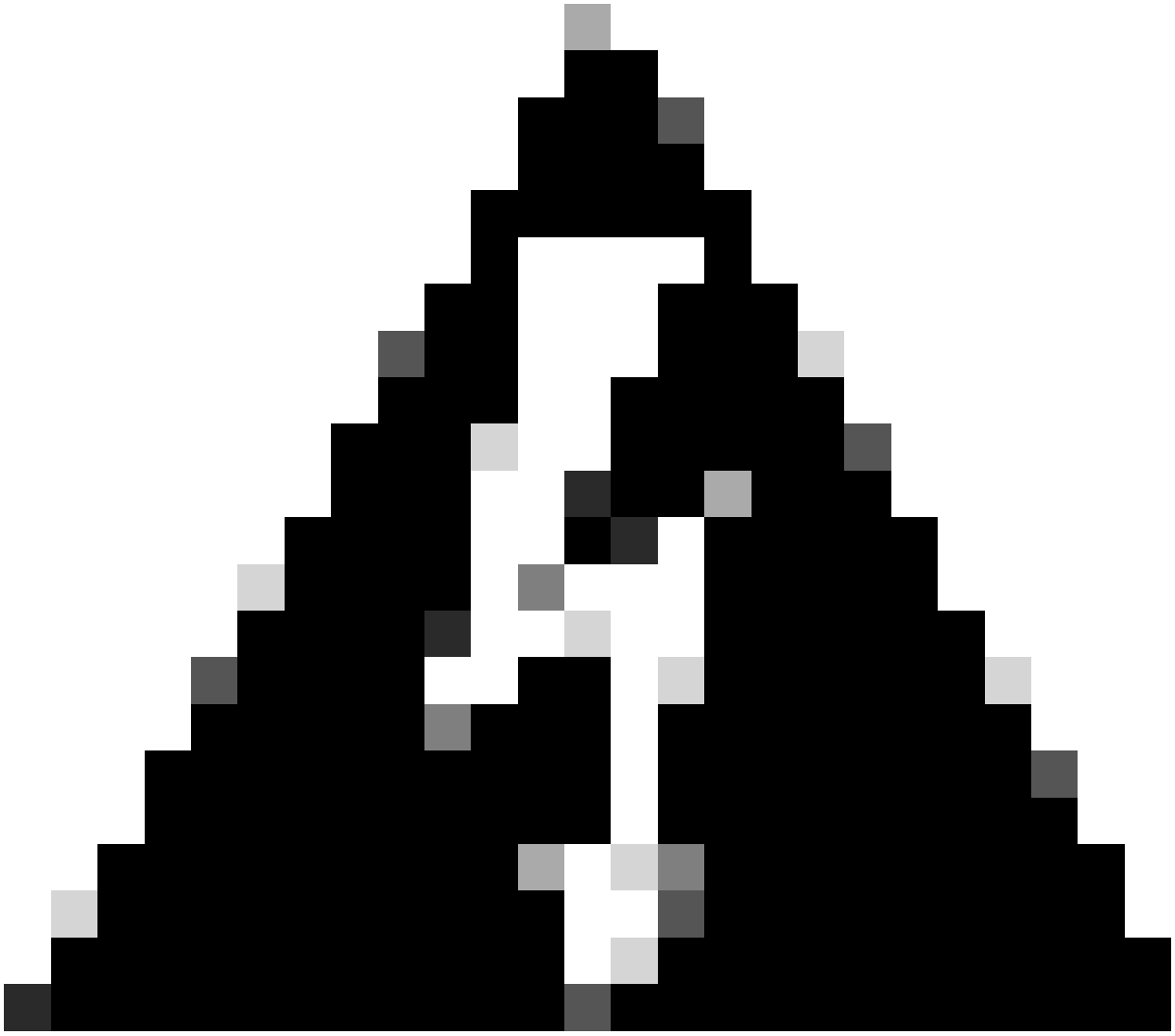
El resultado de este comando, cuando se ejecuta correctamente, es:

Creación de usuario USM mediante SSH

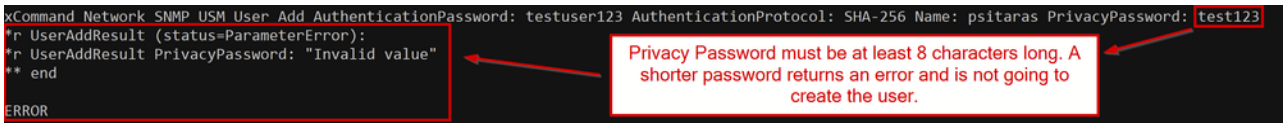
Para que el comando se ejecute sin errores, debe cumplir con ciertas reglas descritas en la documentación del comando compartida en este link. Por comodidad, los requisitos actuales en el momento de escribir este documento para este comando se pegan en esta imagen, pero debe asegurarse de hacer referencia a este link al crear su usuario. Al final de la imagen, observe que existe la sintaxis exacta del comando.



Sintaxis del comando USM User Creation de la documentación de xAPI



Advertencia: En caso de que haya un error tipográfico o de que no se cumpla un requisito, el comando devuelve un error y el usuario no se va a crear. Se proporciona un ejemplo en el que, en lugar de proporcionar una contraseña de privacidad de al menos 8 caracteres, se proporciona una contraseña más corta de 7 caracteres:



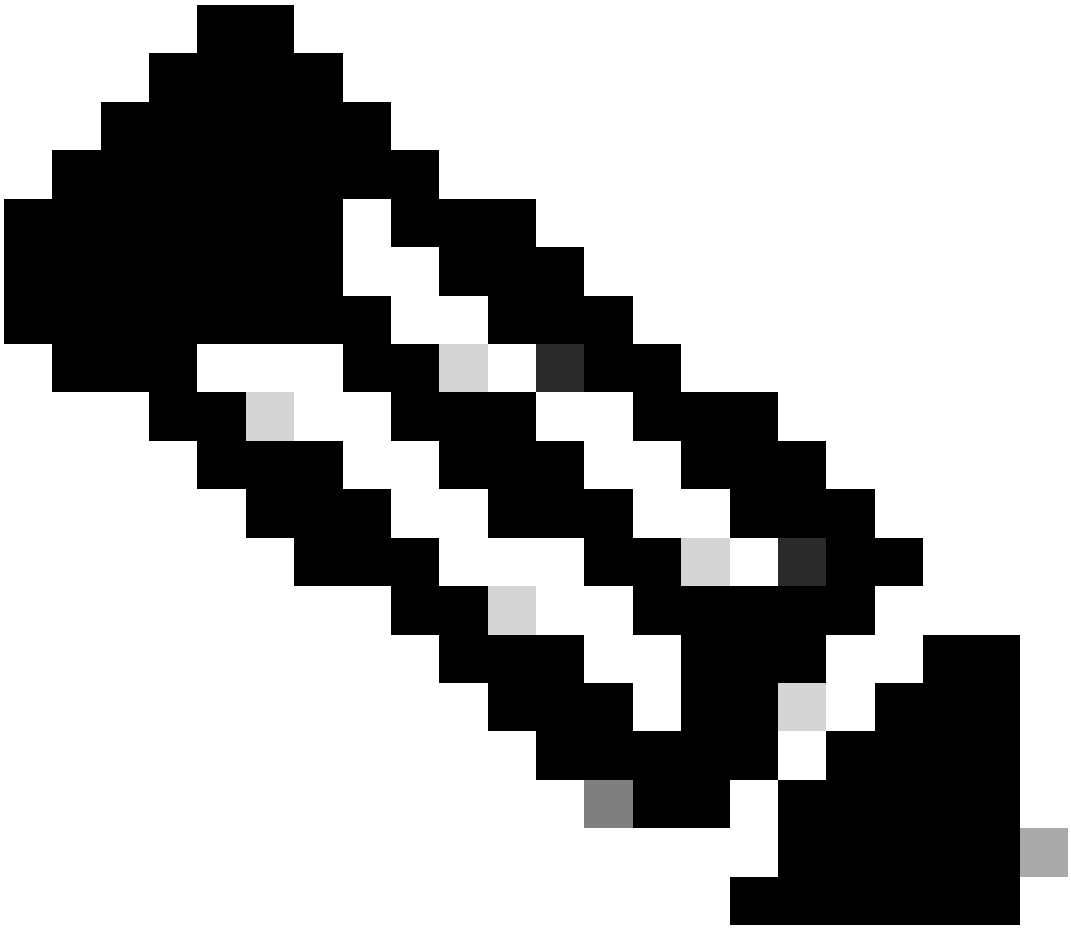
Creación de usuario USM incorrecta debido a una contraseña de privacidad breve

Puede probar si su usuario fue creado mediante el comando Network SNMP USM User List. Este comando enumera todos los usuarios de USM que están almacenados en el dispositivo:

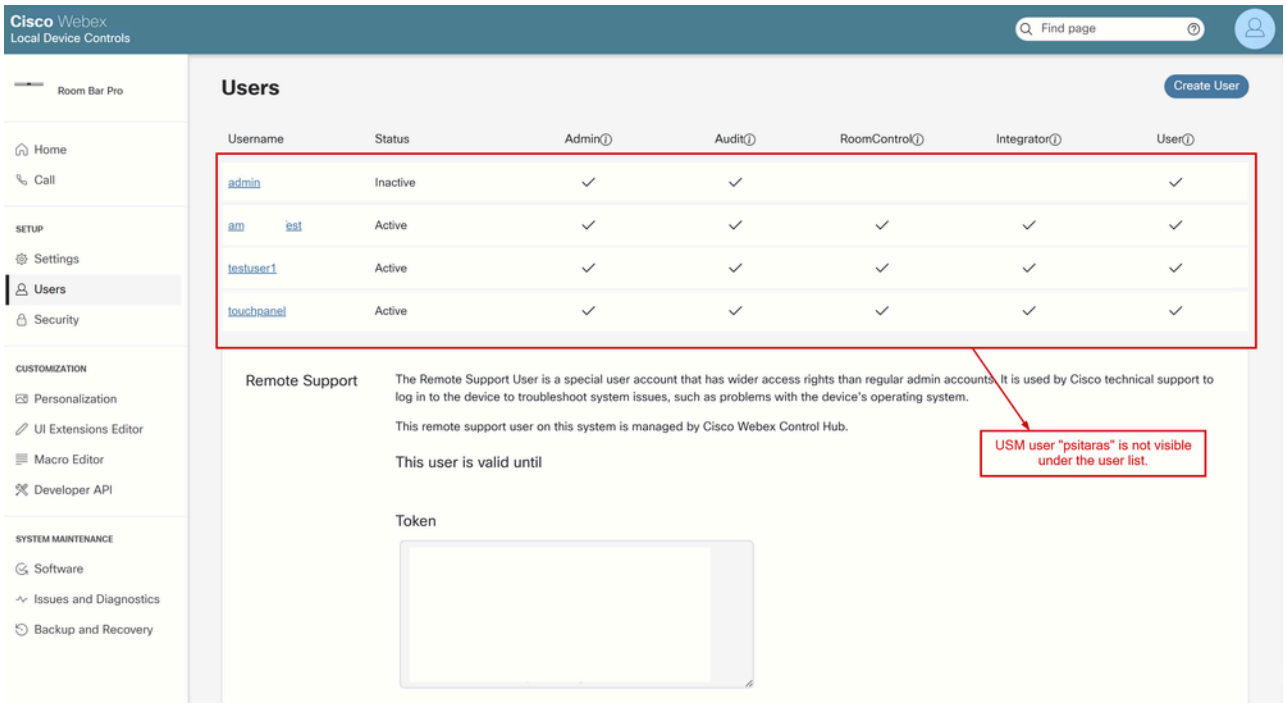
```
xCommand Network SNMP USM User List

OK
*r UserListResult (status=OK):
*r UserListResult User 1 AuthenticationProtocol: "SHA-256"
*r UserListResult User 1 Name: "psitaras"
** end
```

Comando Network SNMP USM User List Utilizado para Confirmar la Creación del Usuario

En esta etapa, se ha confirmado que el usuario psitaras ha sido creado con éxito. La configuración de SNMPv3 se ha completado.



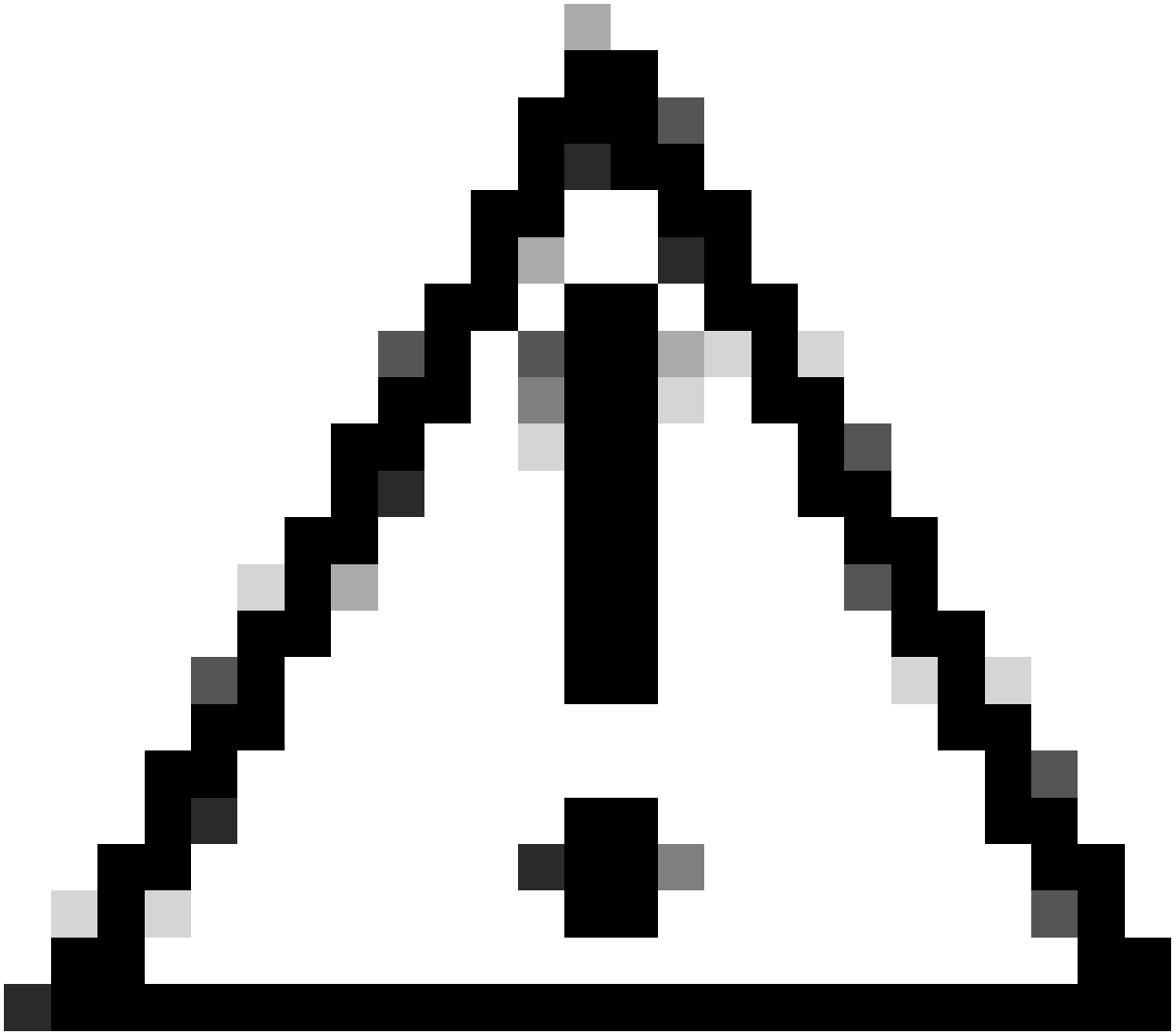
Nota: El usuario USM psitaras no está visible en la GUI del terminal en la sección Usuarios. Esto es esperable.



Los usuarios de USM no están visibles en Usuarios de la GUI del terminal

Prueba de la Configuración de SNMPv2c y SNMPv3

En esta etapa, puede continuar con la prueba de la configuración de SNMPv2c y/o SNMPv3 con el sistema de administración de redes (NMS). Para este artículo, la configuración de laboratorio no contiene ningún servidor NMS o SNMP que ejecute un servicio SNMP. Para probar la configuración, se utiliza la utilidad llamada snmpwalk. Esta utilidad se instala en un servidor Linux.

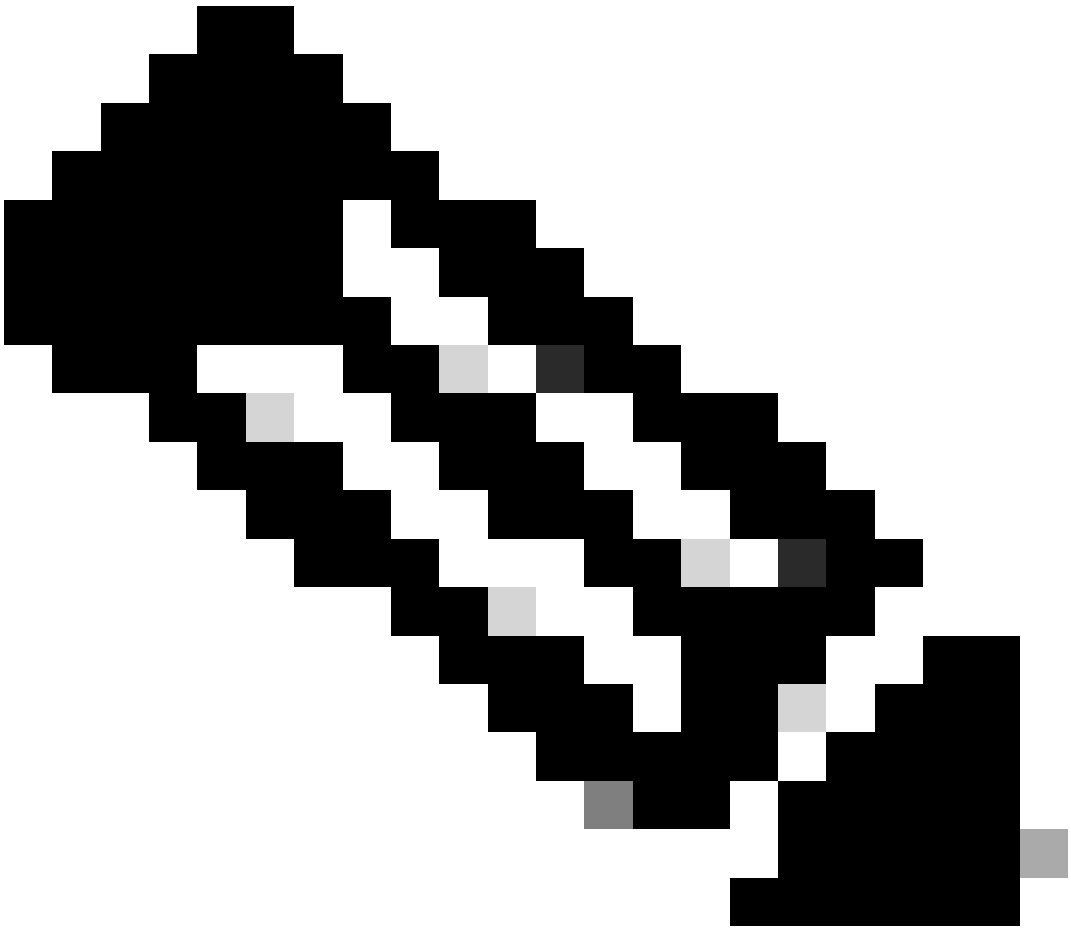


Precaución: Snmpwalk no es una herramienta recomendada para probar la configuración de SNMP en los terminales de colaboración. No es compatible con los ingenieros del TAC, por lo que debe estar familiarizado con el uso de la herramienta antes de continuar con las pruebas. En lugar de snmpwalk, puede utilizar cualquier otra herramienta SNMP o su NMS para probar su configuración. Snmpwalk se utiliza en este artículo como ejemplo (se necesita una herramienta para probar la configuración con fines de demostración) y no hay ningún compromiso o promoción relacionados con su uso.

La instalación de snmpwalk no forma parte de esta guía y se omite. Dependiendo del sistema operativo (SO) de la máquina que esté utilizando para la prueba, los requisitos de instalación pueden variar. Debe continuar instalándolo correctamente antes de realizar la prueba.

Snmpwalk es una herramienta que se puede utilizar para verificar la configuración SNMP. Realiza un recorrido por los MiB del terminal y devuelve la información disponible. Los terminales registrados en la nube exponen 7 identificadores de objeto (OID):

- SNMPv2-MIB::sysDescr (lectura),
- SNMPv2 -MIB::sysObjectID (lectura),
- DISMAN-EVENT-MIB::sysUpTimeInstance (lectura),
- SNMPv2 -MIB::sysContact (lectura/escritura),
- SNMPv2 -MIB::sysName (lectura/escritura),
- SNMPv2 -MIB::sysLocation (lectura/escritura),
- SNMPv2 -MIB::sysServices (lectura).



> Nota: Las IP internas utilizadas para las pruebas snmpwalk enumeradas son IP privadas y ya no se utilizan. El laboratorio utilizado para esta guía se ha retirado del servicio y los dispositivos se han restablecido de fábrica.

El terminal Cisco Room Kit Pro se configura con SNMPv2c. La autenticación se realiza mediante cadenas de comunidad. Ejecute el comando this:

```
# '-c' option is used to provide the community string
```

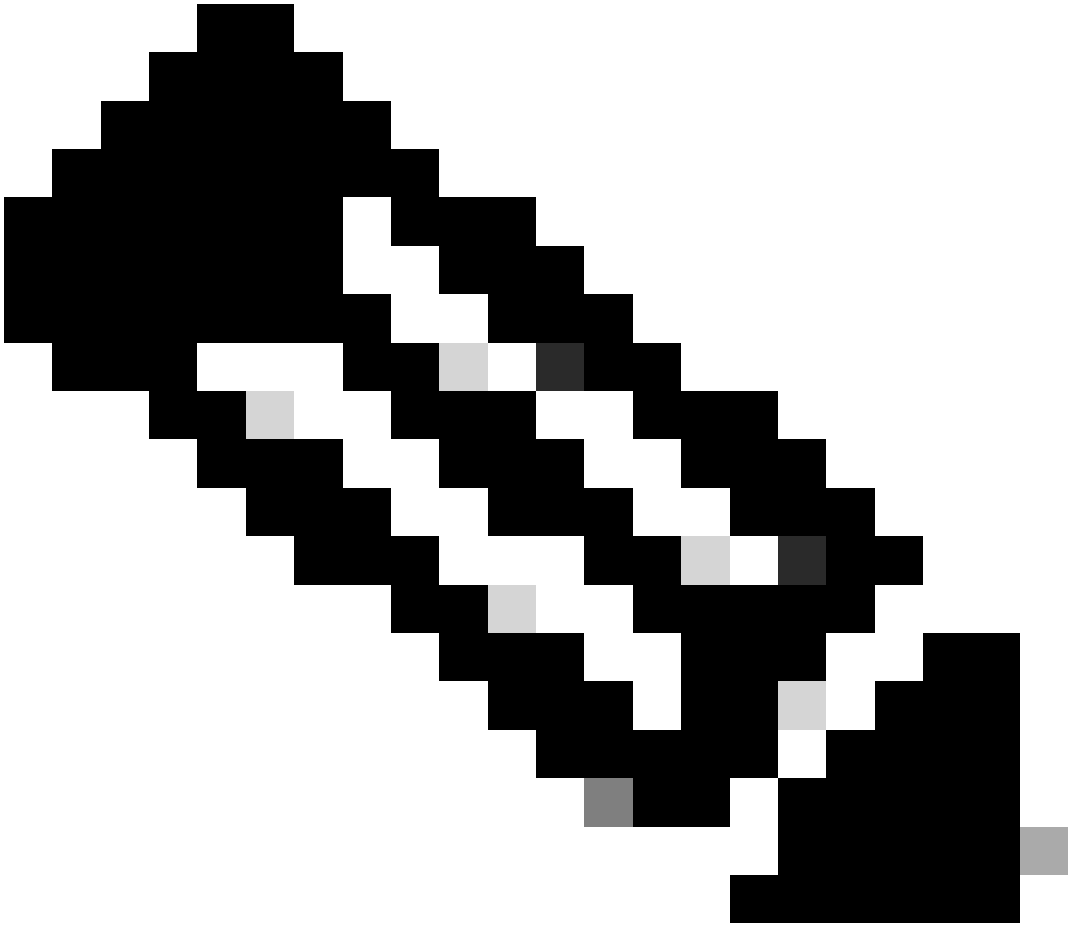
```
# '-v' option is used to provide the SNMP version used
# The IP provided is the endpoint's IP

snmpwalk -c test123 -v 2c 172.16.5.9

iso.3.6.1.2.1.1.1.0 = STRING: "Cisco Codec
SoftW: ce11.26.1.5.53ff615d0d9
MCU: Cisco Codec Pro
Date: 2025-02-28
S/N: FDO2706JG49"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.5596.150.6.4.1
iso.3.6.1.2.1.1.3.0 = Timeticks: (106770681) 12 days, 8:35:06.81
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = ""
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.7.0 = No more variables left in this MIB View (It is past the end of the MIB tree)
```

Snmpwalk devuelve 7 resultados como se esperaba. Hay tres MiB vacíos:

1. SNMPv2 -MIB::sysContact (lectura/escritura), (iso.3.6.1.2.1.1.4.0)
2. SNMPv2 -MIB::sysName (lectura/escritura), (iso.3.6.1.2.1.1.5.0)
3. SNMPv2 -MIB::sysLocation (lectura/escritura), (iso.3.6.1.2.1.1.6.0)

Hay tres comandos xConfiguration que se pueden utilizar para establecer valores en estos MiB. SSH al punto final y ejecute estos comandos:

```
xConfiguration NetworkServices SNMP SystemContact: testuser1
xConfiguration NetworkServices SNMP SystemLocation: Room1
xConfiguration SystemUnit Name: My_Room_Kit_Pro
```



Nota: En lugar de utilizar estos tres comandos, puede realizar cambios en estos parámetros desde el concentrador de control, desde la GUI del terminal o desde las API de Webex.

Una vez que se emitan los comandos anteriores, utilice snmpwalk nuevamente en el mismo punto final. Observe que los MiB previamente vacíos se llenan con los valores provistos a través de los comandos xConfiguration:

```
snmpwalk -c test123 -v 2c 172.16.5.9

iso.3.6.1.2.1.1.1.0 = STRING: "Cisco Codec
SoftW: ce11.26.1.5.53ff615d0d9
MCU: Cisco Codec Pro
Date: 2025-02-28
S/N: FDO2706JG49"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.5596.150.6.4.1
iso.3.6.1.2.1.1.3.0 = Timeticks: (107047446) 12 days, 9:21:14.46
iso.3.6.1.2.1.1.4.0 = STRING: "testuser1"
```

```
iso.3.6.1.2.1.1.5.0 = STRING: "My_Room_Kit_Pro"
iso.3.6.1.2.1.1.6.0 = STRING: "Room1"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.7.0 = No more variables left in this MIB View (It is past the end of the MIB tree)
```

En esta etapa, se confirma que la configuración SNMPv2c realizada en el dispositivo Room Kit Pro está operativa.

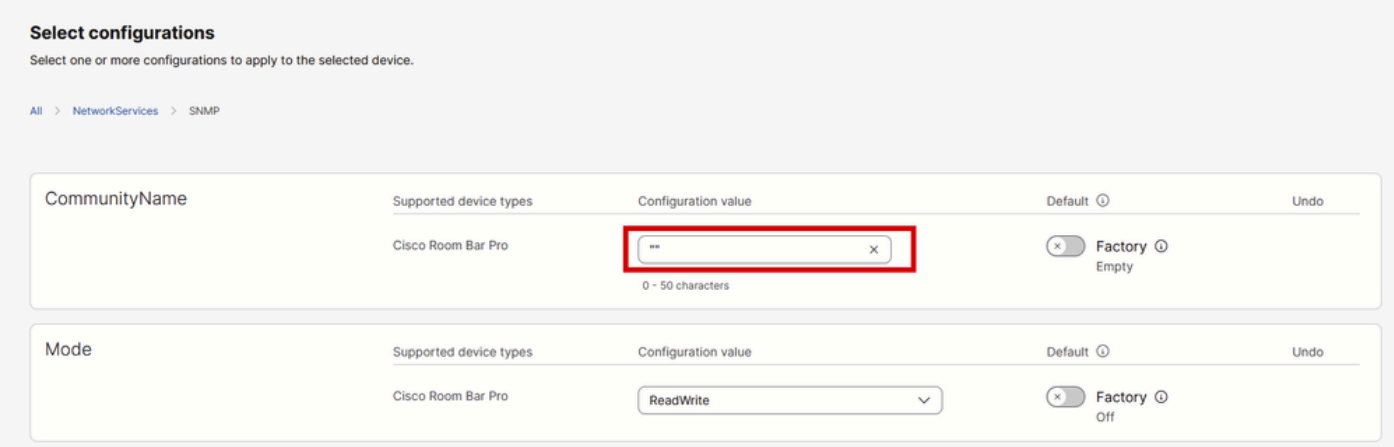
El punto final de Cisco Room Bar Pro se configura con SNMPv3. Para SNMPv3, debe asegurarse de utilizar la autenticación adecuada. No se utilizan cadenas de comunidad. En su lugar, SNMPv3 utiliza nombres de usuario y contraseñas.

```
# '-v3' option selects SNMPv3.
# '-u' option provides the USM username configured.
# '-x' option provides the privacy protocol (encryption algorithm). Options are DES and AES. Cloud-regi
# '-l' option specifies the security level. Options are 'noAuthNoPriv', 'authNoPriv', and 'authPriv'. C
# '-a' option specifies the authentication protocol. Cloud-registered endpoints support only SHA-2 prot
# '-A' option specifies the authentication passphrase.
# '-X' specifies the privacy pass phrase for the encrypted SNMPv3 messages.

snmpwalk -v3 -u psitaras -x AES -l authPriv -a SHA-256 -A testuser123 -X test1234 172.16.5.23

iso.3.6.1.2.1.1.1.0 = STRING: "Cisco Codec
SoftW: ce11.23.1.8.3963b07b5c5
MCU: Cisco Room Bar Pro
Date: 2024-12-12
S/N: FOC2732H1VU"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.5596.150.6.4.1
iso.3.6.1.2.1.1.3.0 = Timeticks: (112579044) 13 days, 0:43:10.44
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = ""
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.7.0 = No more variables left in this MIB View (It is past the end of the MIB tree)
```

En esta etapa, se confirma que la configuración SNMPv3 realizada en el dispositivo Room Bar Pro está operativa.

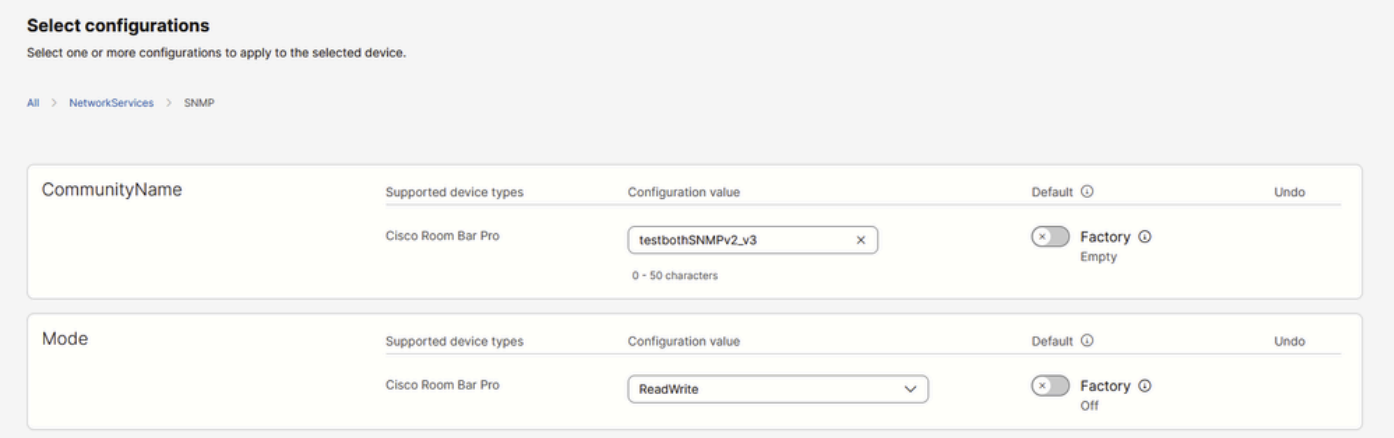
¿Puede un terminal tener SNMPv2c y SNMPv3 activos simultáneamente?

Sí, es posible. Sin embargo, durante la configuración de SNMP, debe configurar un nombre de comunidad para poder tener autenticación SNMPv2c. Para esta prueba, se utiliza la Room Bar Pro de ejemplos anteriores. La configuración actual de la sección Control Hub All Configurations del terminal es:



Configuraciones SNMP de terminales en el concentrador de control

Observe que el nombre de la comunidad no está vacío. Hay dos comillas, que indican que el nombre de la comunidad es una cadena vacía. Puede limitar el soporte SNMP a la versión 3 solamente, configurando NetworkServices SNMP CommunityName en una cadena vacía (""). Debe reemplazar esta cadena por un nombre de comunidad, por ejemplo, testbothSNMPv2_v3.



Agregar nombre de comunidad para SNMPv2c en los parámetros de configuración del extremo del concentrador de control

Ya se ha confirmado que SNMPv3 funciona en Room Bar Pro. Snmpwalk se utiliza para probar si SNMPv2c también funciona, después de configurar el nombre de la comunidad:

```
snmpwalk -c testbothSNMPv2_v3 -v 2c 172.16.5.23

iso.3.6.1.2.1.1.1.0 = STRING: "Cisco Codec
SoftW: ce11.23.1.8.3963b07b5c5
MCU: Cisco Room Bar Pro
Date: 2024-12-12
S/N: FOC2732H1VU"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.5596.150.6.4.1
iso.3.6.1.2.1.1.3.0 = Timeticks: (112696957) 13 days, 1:02:49.57
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = ""
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.7.0 = No more variables left in this MIB View (It is past the end of the MIB tree)
```

¿Se pueden configurar varios terminales mediante el concentrador de control con SNMP?

Sí, es posible configurar varios dispositivos a la vez en el concentrador de control. En este artículo se proporciona información sobre cómo realizarlo paso a paso en la sección Configuración de varios dispositivos.

Detalles importantes que debe recordar

- Solo hay disponibles MiB específicos. El número de MiB disponibles está limitado por el diseño del equipo de ingeniería que diseña los terminales. Los MiB no se pueden ampliar ni mejorar para proporcionar más información.
- SNMPv2c se autentica mediante el nombre de comunidad (también denominado cadena de comunidad), mientras que SNMPv3 se autentica mediante el nombre de usuario y la contraseña, y también ofrece cifrado. Cuando realice la prueba, asegúrese de utilizar el método de autenticación correcto (con snmpwalk u otra herramienta/NMS) para el protocolo que ha configurado.
- La autenticación y la privacidad siempre están activas en SNMPv3. Los terminales sólo admiten el nivel de seguridad authPriv y el protocolo de privacidad siempre es el Estándar de cifrado avanzado (AES).
- SNMPv3 sólo es compatible con las opciones del modelo de seguridad basado en el usuario (USM). No hay soporte para SNMPv3 sobre TLS.
- Los comandos de usuario USM utilizados para configurar usuarios para la autenticación SNMP no tienen ningún efecto en SNMPv2c.
- La configuración de SNMP CommunityName en los terminales no tiene ningún efecto en la configuración de SNMPv3.
- SNMP CommunityName distingue entre mayúsculas y minúsculas.
- Puede limitar el soporte SNMP a v3 solamente, configurando NetworkServices SNMP CommunityName en una cadena vacía ("").
- SNMPv1 no es compatible.
- Tanto para SNMPv2c como para SNMPv3, los terminales exponen los mismos identificadores de objeto (OID).
- Para SNMPv3, el protocolo de autenticación debe estar en la familia SHA-2 (no se admite MD ni SHA-1). Si no es así, las solicitudes SNMP no se autentican y permanecen sin respuesta.
- La contraseña de privacidad se almacena en el dispositivo como un valor hash traducido (AES-128). Si una contraseña de privacidad no se establece explícitamente en este parámetro, se establece para que sea la misma que la contraseña de autenticación (con una función hash como se especifica en el parámetro Authentication Protocol).
- Las contraseñas, frases de contraseña y nombres de usuario deben estar dentro de límites de longitud específicos. Por ejemplo, el nombre de usuario USM debe tener hasta 32 caracteres y la contraseña de autenticación debe tener un mínimo de 8 caracteres y un máximo de 255. Si no se cumplen estos requisitos, el comando Network SNMP USM User Add no puede crear el usuario y devuelve un error.

Contacto con el TAC para resolver un problema de SNMP en un punto final

Si se ha completado la configuración SNMP del punto final, pero se ha planteado un problema, debe comunicarse con el TAC y compartir esta información:

- Proporcione la ID de su organización en el centro de control y el número de serie (SN) del terminal afectado.
- Describa el escenario al que se enfrenta.
- Proporcione la versión de SNMP que intenta configurar.
- Proporcione los mensajes de error que se hayan visto.
- Si hay algún problema con la configuración del dispositivo, explique claramente en qué paso se ha detenido el proceso de configuración y proporcione capturas de pantalla. Comparta el comando de configuración que devuelve un error.
- Recopile los registros de los terminales y cárguelos en su caso.
- Comparta la utilidad\NMS u otra herramienta utilizada para probar la configuración de SNMP. Si utiliza una utilidad para realizar pruebas con el agente SNMP de los terminales, proporcione el comando completo utilizado.

Información Relacionada

Documentación de xAPI de SO de sala - Comandos relacionados con SNMP

Configuraciones de dispositivos para dispositivos de las series de sala, escritorio y placa

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).