

# Configurazione di SNMP sugli endpoint registrati nel cloud

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Che cos'è SNMP](#)

[Quali informazioni possono essere richieste](#)

[Configurazione di SNMP su un endpoint registrato nel cloud](#)

[Abilitazione della modalità SNMPv2c nell'hub di controllo](#)

[Abilitazione della modalità SNMPv3 nell'hub di controllo](#)

[Come appare la configurazione SNMP nell'interfaccia utente dell'endpoint](#)

[Configurare l'utente USM per SNMPv3](#)

[Test della configurazione di SNMPv2c e SNMPv3](#)

[È possibile che un endpoint abbia contemporaneamente SNMPv2c e SNMPv3 attivi?](#)

[È possibile configurare più endpoint tramite Control Hub con SNMP?](#)

[Dettagli importanti da ricordare](#)

[Connessione a TAC per risolvere un problema SNMP su un endpoint](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritto come configurare SNMP su un endpoint registrato nel cloud e risolvere i relativi problemi.

## Prerequisiti

### Requisiti

Si consiglia di familiarizzare con questi argomenti:

- Control Hub Platform
- Amministrazione degli endpoint tramite l'interfaccia grafica (GUI) dell'endpoint e la sezione Control Hub Devices
- SSH su un endpoint come utente amministratore
- SO room
- SNMP (SNMPv2c e SNMPv3)
- Snmpwalk o altro strumento/utilità o Network Management System (NMS) per verificare la

### Componenti usati

Le apparecchiature qui elencate sono state utilizzate per eseguire i test e produrre i risultati descritti nel presente documento:

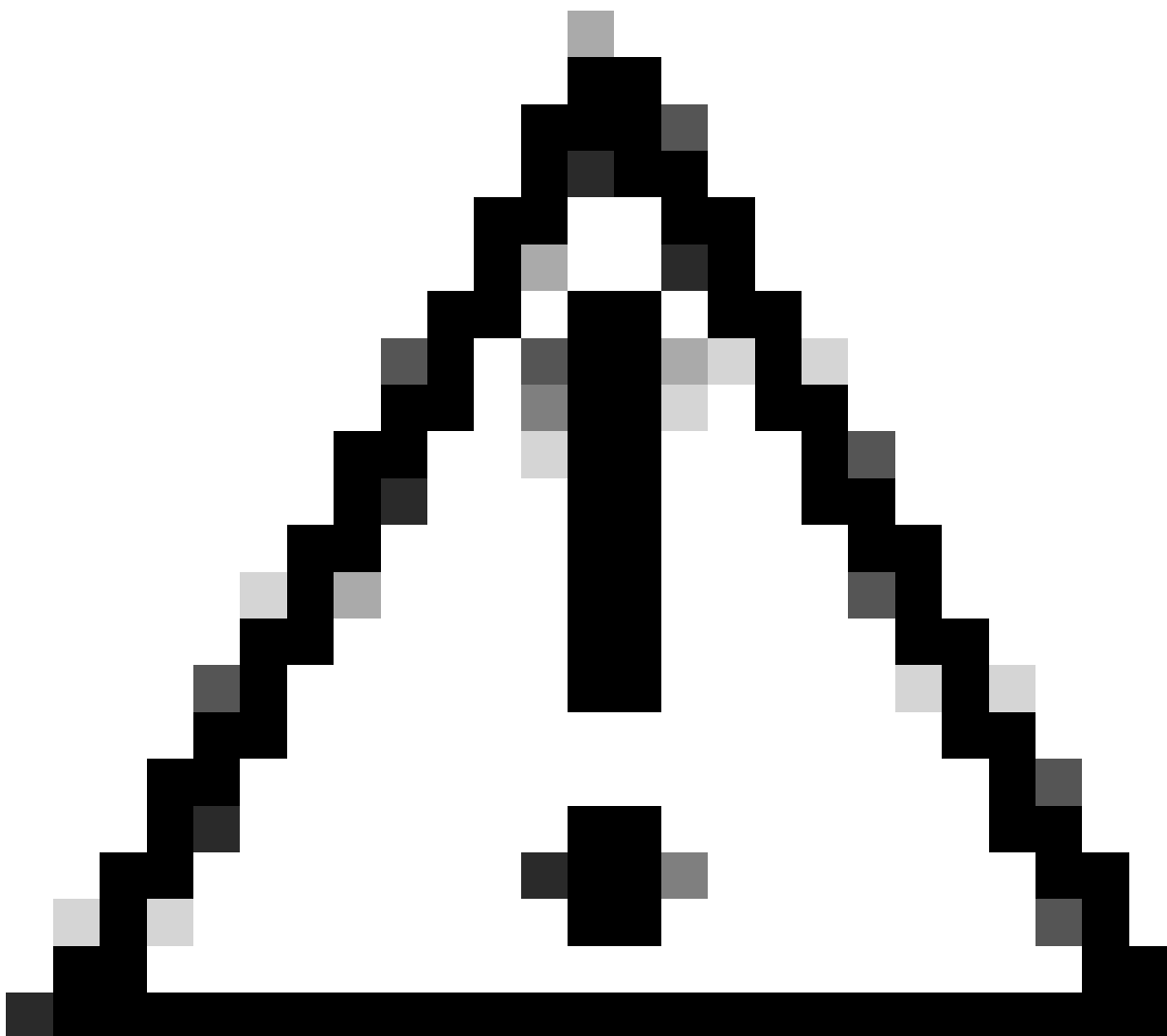
- Organizzazione hub di controllo
- Cisco Room Kit Pro
- Cisco Room Bar Pro
- Server Linux per ospitare l'utility snmpwalk per il test della configurazione SNMP.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

### Che cos'è SNMP

SNMP è l'acronimo di Simple Network Management Protocol. È un protocollo utilizzato per raccogliere e gestire informazioni sui dispositivi all'interno di una rete, monitorare lo stato dei dispositivi o apportare modifiche alla configurazione. Tali dispositivi possono essere router, switch, server, stampanti o qualsiasi altro tipo di dispositivo. È un prerequisito per l'assegnazione di un indirizzo IP a questi dispositivi. Il protocollo SNMP è disponibile in tre versioni. Il sistema operativo Room supporta SNMPv2c e SNMPv3. SNMPv1 non è supportato.

Questo articolo si concentra sulla configurazione e la risoluzione dei problemi del protocollo SNMP sugli endpoint Collaboration con sistema operativo Room registrato nel cloud (senza usare Webex Edge for Devices).



Attenzione: Questo articolo si avvicina alla configurazione SNMP solo dalla prospettiva dell'endpoint. Qualsiasi configurazione eseguita sul lato rete e gli strumenti utilizzati per richiedere/aggiornare le informazioni relative a SNMP sugli endpoint non rientrano nell'ambito di questo articolo.

TAC non supporta la risoluzione dei problemi di SNMP all'interno della rete, né può offrire alcuna deduzione sul motivo per cui SNMP non funziona come previsto da una prospettiva di rete. Il team di rete deve essere coinvolto nella risoluzione di questi problemi.

La gestione del protocollo SNMP può essere ottenuta con molti strumenti diversi. Questi strumenti non sono supportati da TAC. In caso di discrepanza nelle informazioni raccolte dagli endpoint tramite questi strumenti, il problema deve essere inizialmente risolto dal team di rete e quindi valutato in TAC, se esistono informazioni sufficienti a dimostrare che si tratta di un problema correlato all'endpoint.

---

# Quali informazioni possono essere richieste

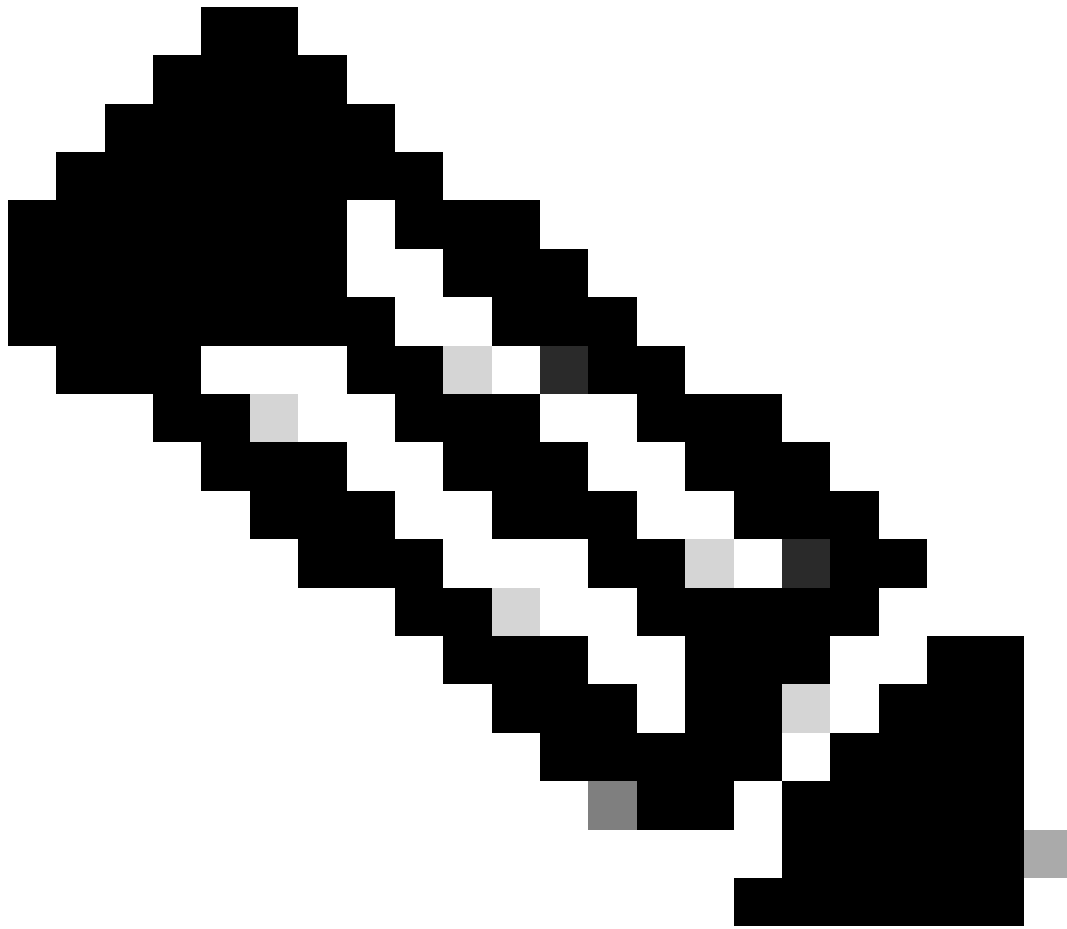
Utilizzando il protocollo SNMP, è possibile richiedere una quantità limitata di informazioni dall'endpoint. Gli OID e i MiB supportati sono illustrati in [questo collegamento](#), nella descrizione dettagliata del comando NetworkService SNMP Mode:

The screenshot shows the Cisco RoomOS xAPI documentation interface. On the left, a sidebar lists various categories like XAPI, Reference, AirPlay, Apps, Audio, BYOD, Bluetooth, Bookings, Call, CallHistory, CallLog, CallTransfer, Camera, Cameras, Capabilities, Conference, and Diagnostics. The main content area displays a search result for 'NetworkServices SNMP Mode', which is highlighted with a red box. The command is listed as 'NetworkServices SNMP Mode' with a 'config' icon. To the right, a detailed description of the command is provided, explaining that SNMP (Simple Network Management Protocol) is used by network management systems to monitor and manage network devices. It also lists supported object identifiers (OIDs) and parameters, such as 'SNMPv2-MIB::sysDescr (read)', 'SNMPv2-MIB::sysObjectID (read)', 'DISMAN-EVENT-MIB::sysUpTimeInstance (read)', 'SNMPv2-MIB::sysContact (read/write)', 'SNMPv2-MIB::sysName (read/write)', 'SNMPv2-MIB::sysLocation (read/write)', and 'SNMPv2-MIB::sysServices (read)'. Below the description, there are configuration options for 'Off', 'ReadOnly', 'ReadWrite', and 'Default value'. At the bottom, there are tabs for 'JavaScript', 'Command line', and 'Webex Cloud', and a 'Get value' button.

Descrizione del comando della modalità SNMP del servizio di rete nella documentazione di Room OS xAPI

Gli endpoint espongono i seguenti OID sia per SNMPv2 che per SNMPv3:

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



Nota: NetworkServices SNMP CommunityName può essere impostato su una stringa vuota se si desidera utilizzare solo SNMPv3.

---

## Configurazione di SNMP su un endpoint registrato nel cloud

In genere, le modifiche alla configurazione degli endpoint possono essere apportate in quattro modi diversi:

1. API Webex disponibili
2. GUI dell'endpoint
3. Hub di controllo
4. SSH direttamente all'endpoint



Nota: Per accedere alla GUI di un endpoint, aprire un browser e digitare l'indirizzo IP dell'endpoint sulla barra dell'URL. Per accedere, è necessario essere nella stessa rete dell'endpoint e disporre delle credenziali utente.

---

Non tutte le configurazioni possono essere eseguite in tutti e quattro i modi. Per lo scenario di questo documento, la modalità SNMP può essere abilitata in tutti e quattro i modi. Tuttavia, per creare un utente SNMP in grado di comunicare con il dispositivo tramite SNMP, è necessario usare il protocollo SSH sull'endpoint, le API Webex o la GUI dell'endpoint nell'API Developer nella sezione Personalizzazione. Impossibile creare utenti USM dalla sezione Tutte le configurazioni dell'hub di controllo dell'endpoint.

Cisco Webex  
Local Device Controls

Find page

Room Bar Pro

Home

Call

SETUP

Settings

Users

Security

CUSTOMIZATION

Personalization

UI Extensions Editor

Macro Editor

Developer API

SYSTEM MAINTENANCE

Software

Issues and Diagnostics

Backup and Recovery

Developer API

XML API Overview

The XML files below are a part of the device's API, and can be used by external services to inspect the state and configuration of the device. The files are protected using Basic Authentication, thus you may be prompted for a user name and password.

| File Name                          | Description                   |
|------------------------------------|-------------------------------|
| <a href="#">/configuration.xml</a> | Configuration settings        |
| <a href="#">/status.xml</a>        | Endpoint status parameters    |
| <a href="#">/command.xml</a>       | Available API commands        |
| <a href="#">/valuespace.xml</a>    | Value spaces of the XML files |

Execute Commands and Configurations

In the field below you can enter API commands (xCommand and xConfiguration) directly.

Example command:

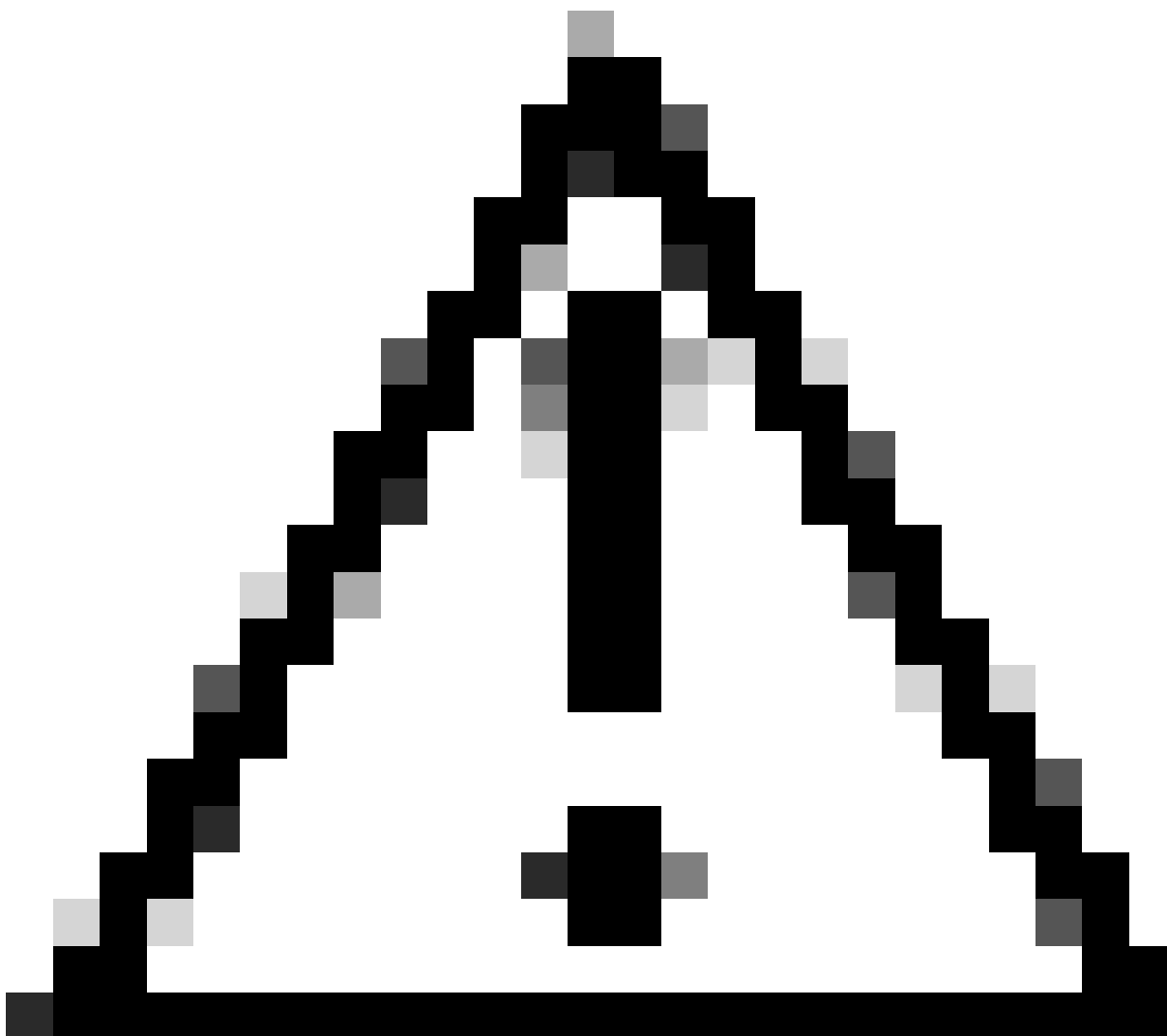
xCommand Dial Number: "person@example.com" Protocol: SIP

xCommand Network SNMP USM User List

Execute

1 of 1 applied successfully.

Sezione Developer API sulla GUI dell'endpoint



Attenzione: I comandi immessi nella casella di testo Esegui comandi e configurazioni non restituiscono alcun risultato. È possibile verificare solo se il comando è stato eseguito correttamente o meno. Ecco perché il comando che elenca gli utenti USM non restituisce alcun risultato nello screenshot precedente. Ciò significa che è possibile creare un utente USM da questa sezione della GUI dell'endpoint correttamente, ma per verificare se l'utente è stato creato è necessario eseguire il protocollo SSH sul dispositivo.

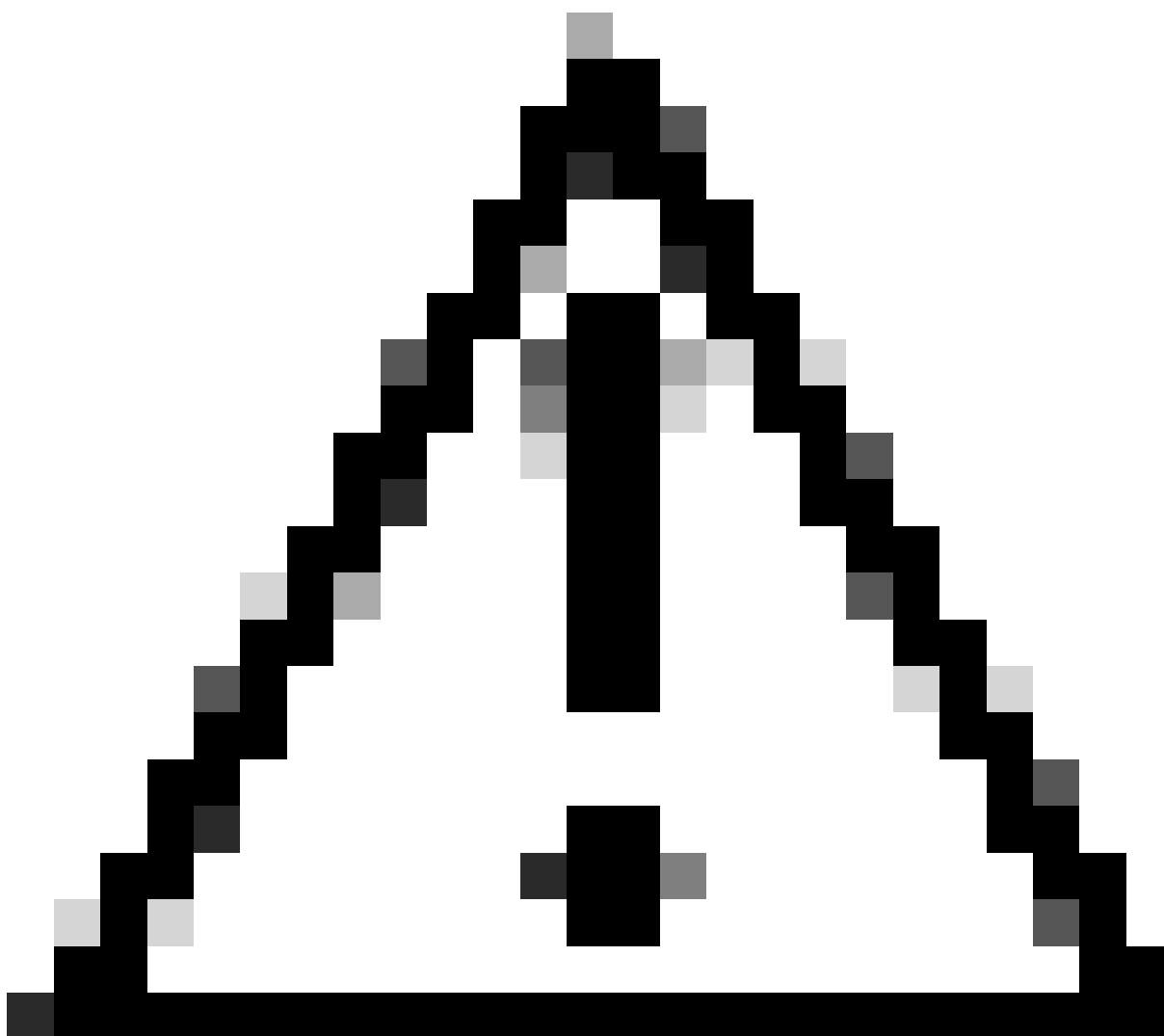
---

Per la configurazione di SNMPv2c, non è necessario creare un utente. L'autenticazione viene eseguita con l'utilizzo del nome della community (detto anche stringa della community) configurato sull'endpoint. L'agente SNMP dell'endpoint, già esistente nel dispositivo, risponde alle richieste che corrispondono al nome della community configurato nel dispositivo. Se una richiesta SNMP da un sistema di gestione non include un nome di community corrispondente (con distinzione tra maiuscole e minuscole), il messaggio viene eliminato e l'agente SNMP nel dispositivo video non invierà una risposta.

Tuttavia, per la riuscita dell'autenticazione, SNMPv3 richiede la configurazione di un utente USM. A questo scopo, è necessario utilizzare i comandi Network SNMP USM User. Il problema può

essere causato dal protocollo SSH direttamente sul dispositivo o usando l'interfaccia utente grafica del dispositivo nella sezione Developer API. In alternativa, è possibile usare l'API Webex.

---



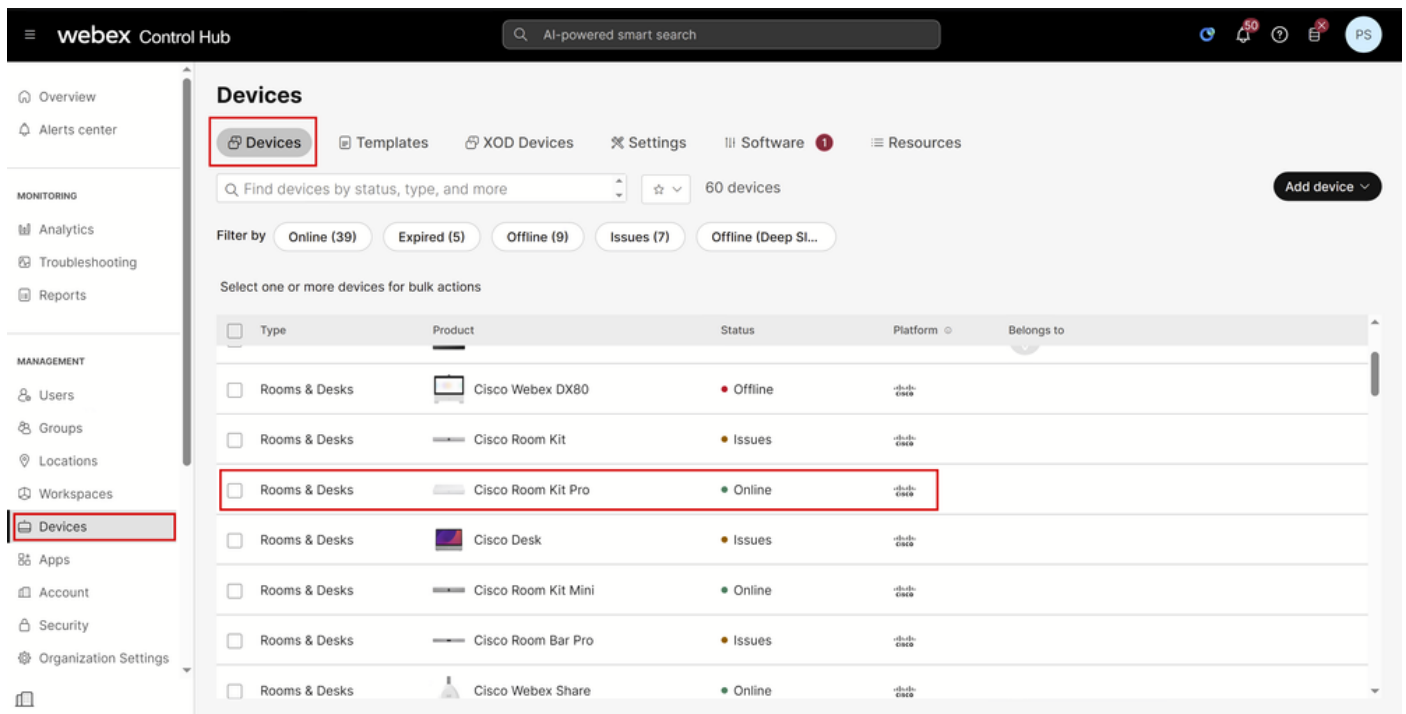
Attenzione: È necessario decidere se abilitare SNMPv2, SNMPv3 o entrambi. SNMPv1 non è supportato sugli endpoint Cisco. Qualsiasi tentativo di utilizzare SNMPv1 avrà esito negativo.

---

In questo documento, i protocolli SNMPv2 e SNMPv3 verranno abilitati e configurati in Control Hub, ma l'utente USM necessario per l'autenticazione SNMP3 verrà configurato su SSH.

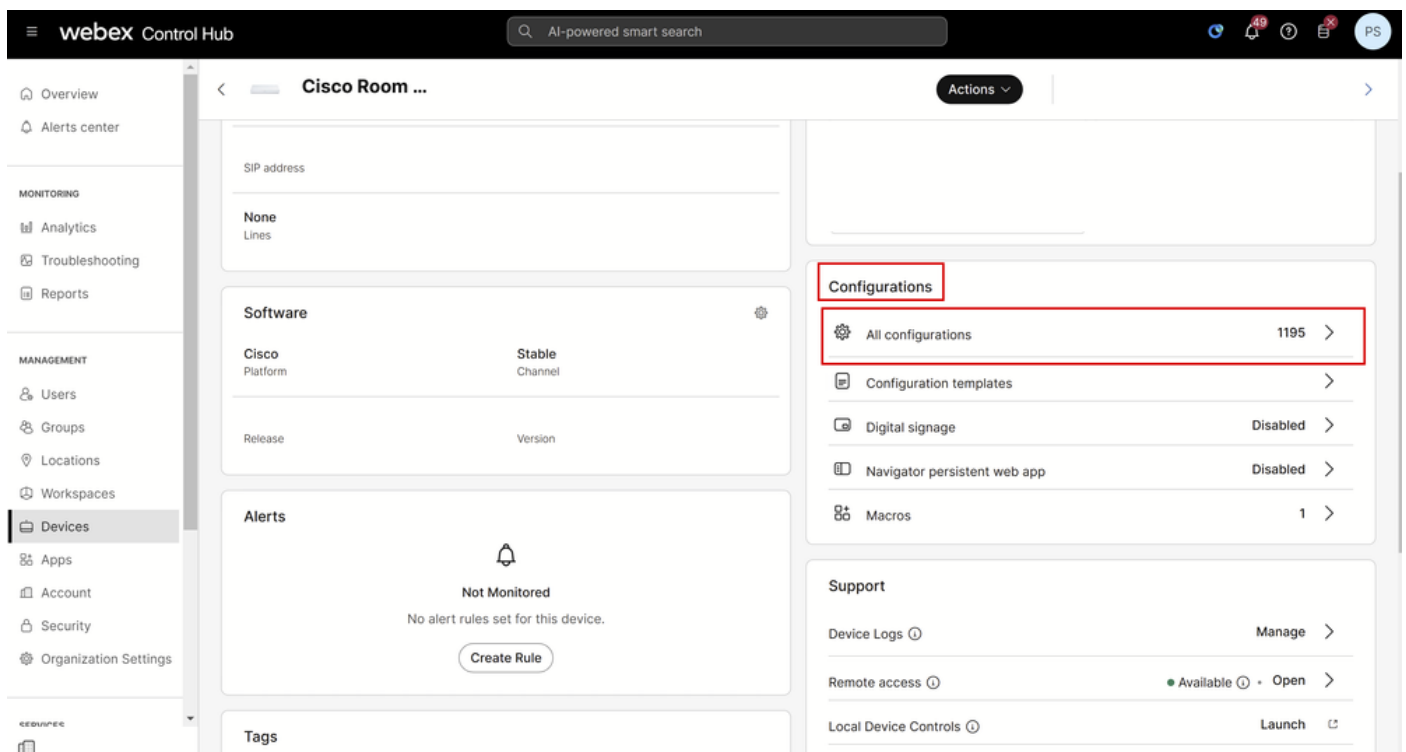
### Abilitazione della modalità SNMPv2c nell'hub di controllo

Passare a [admin.webex.com](https://admin.webex.com) ed eseguire l'accesso con le credenziali di amministratore. Si consiglia di essere un amministratore completo. Passare alla sezione Dispositivi in Gestione sul lato sinistro dell'interfaccia utente. Nella scheda Dispositivi selezionare il dispositivo da configurare. Nell'esempio, viene usato Cisco Room Kit Pro.



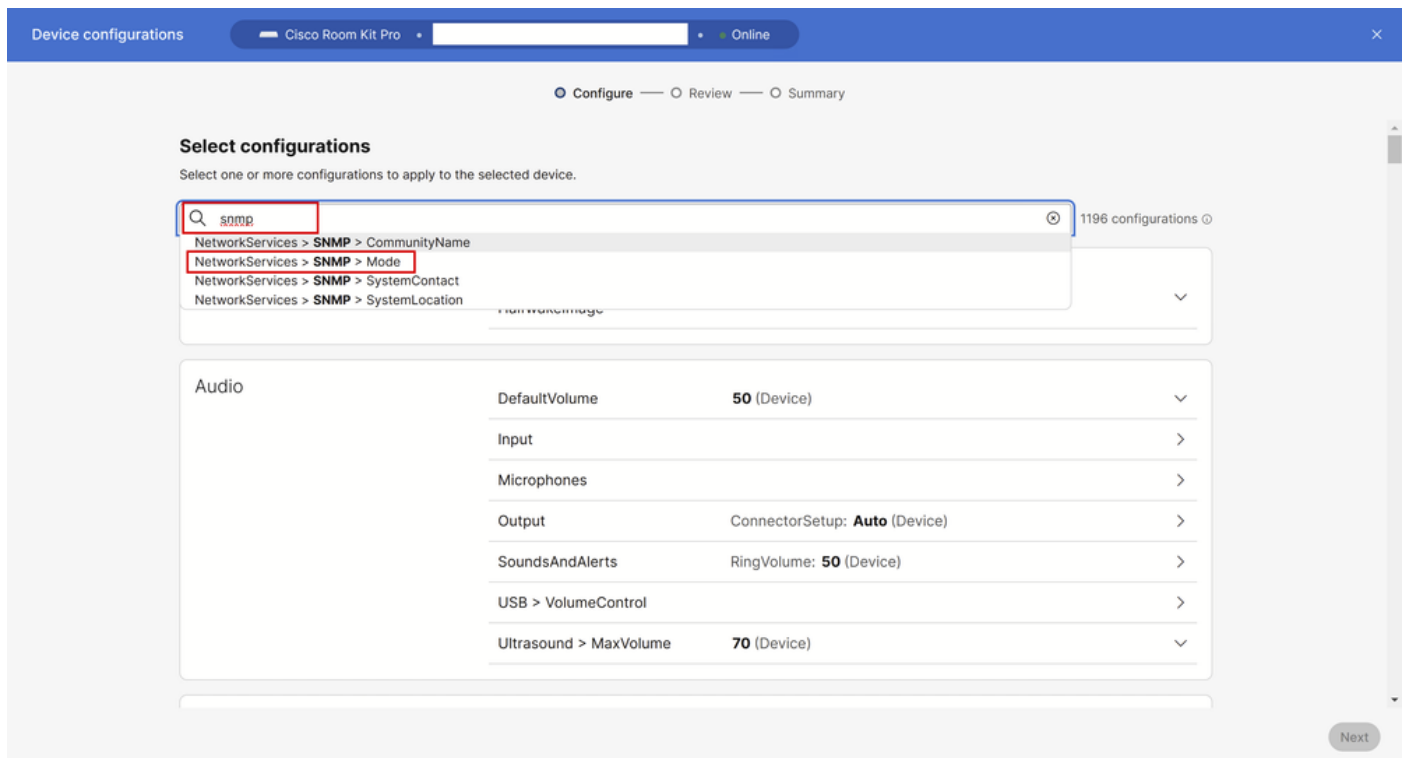
Sezione Control Hub Devices

Nella nuova pagina Control Hub visualizzata, in Dettagli dispositivo passare alla sezione Configurazioni e fare clic su Tutte le configurazioni:



Dettagli dispositivo Control Hub per Room Kit Pro

Nella barra di ricerca, digitare snmp e selezionare Network Services > SNMP > Mode (Servizi di rete > SNMP > Modalità):

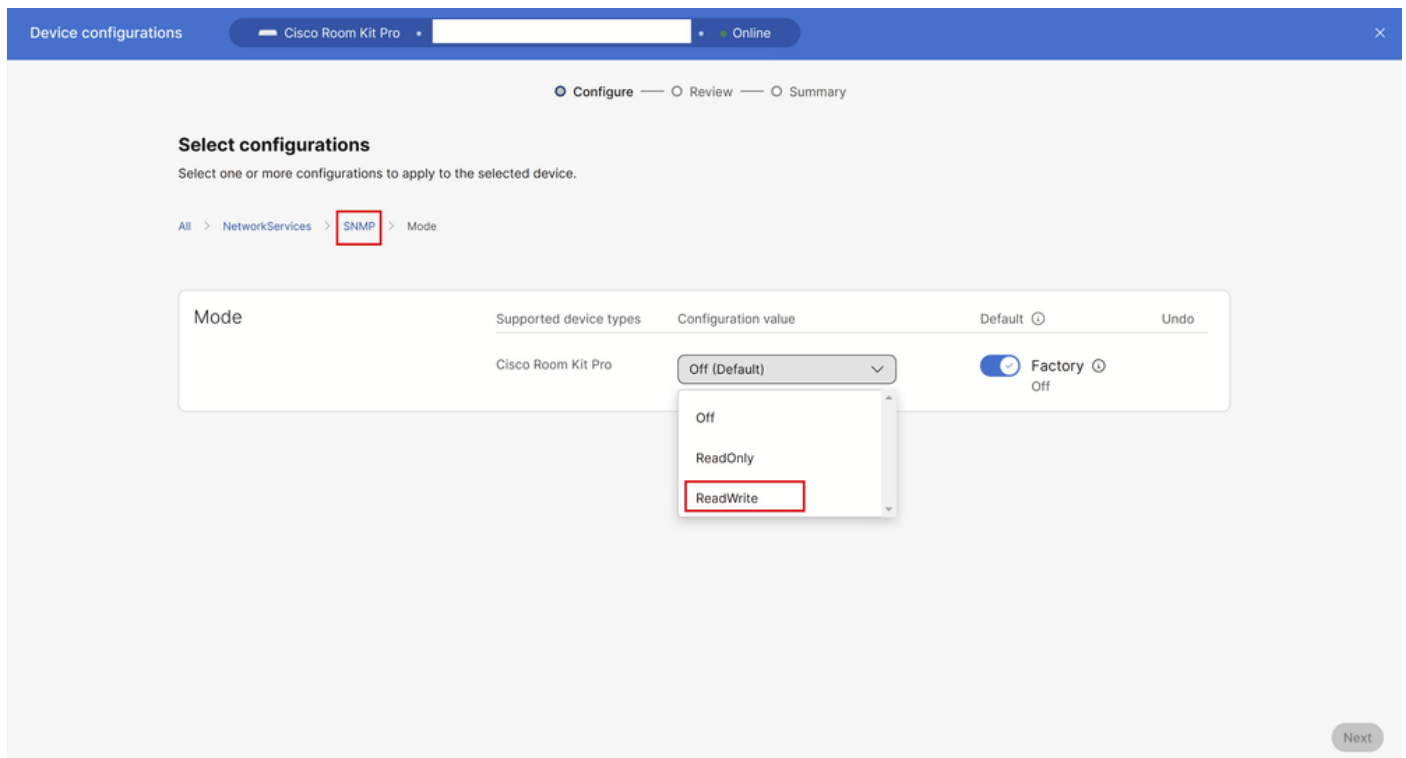


Finestra Tutte le configurazioni di Control Hub

Selezionare la modalità da attivare nell'ambiente. Sono disponibili tre opzioni:

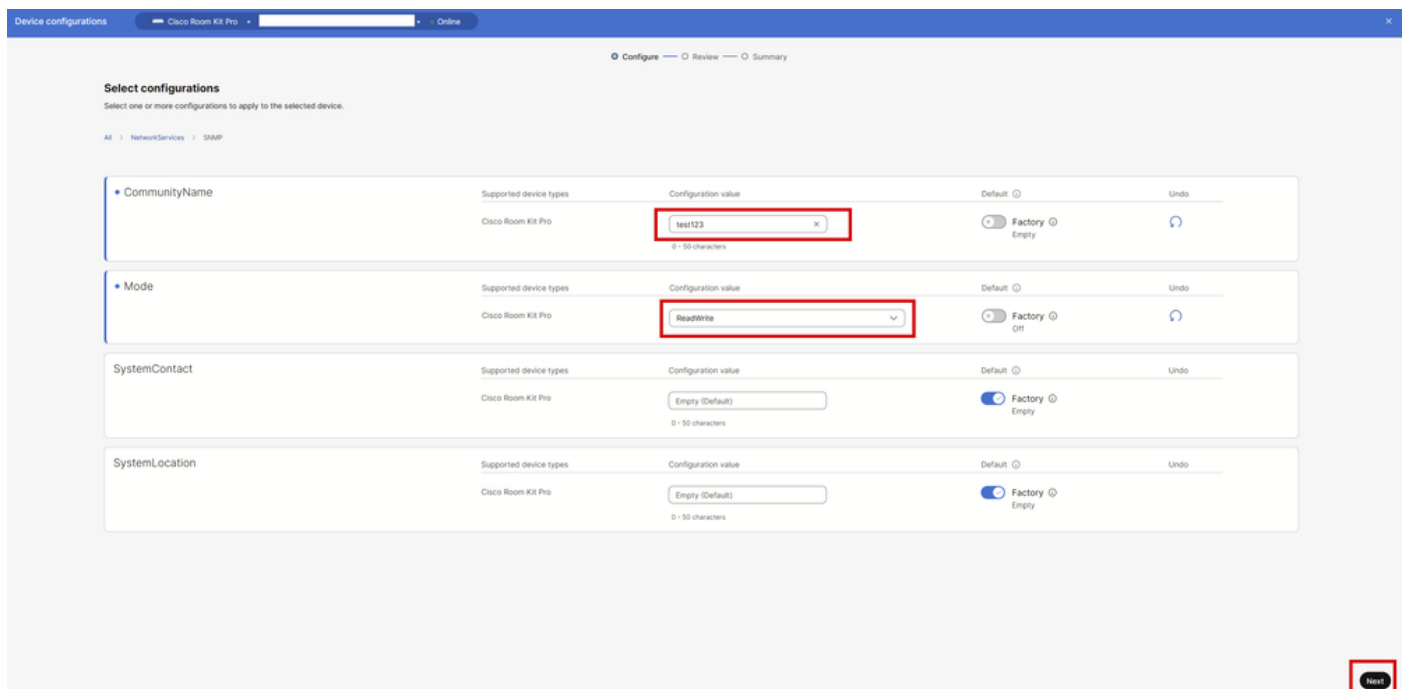
1. Spento: Disabilitare il servizio di rete SNMP.
2. ReadOnly: Abilitare il servizio di rete SNMP solo per le query.
3. ReadWrite: Abilitare il servizio di rete SNMP per query e comandi.

Per questo esempio è selezionato ReadWrite. Quindi, fare clic su SNMP nella sezione di navigazione impostazioni, come mostrato nell'immagine. In questo modo è possibile tornare indietro di un passaggio alle impostazioni e visualizzare tutte le impostazioni relative a SNMP che possono essere configurate sul dispositivo tramite l'hub di controllo:



Impostazione della modalità SNMP in Tutte le configurazioni nell'hub di controllo

Dopo aver fatto clic su SNMP, vengono visualizzate tutte le opzioni SNMP disponibili, come mostrato nella figura. Per una corretta configurazione di SNMPv2, è necessario configurare un nome di community. Il nome della community viene utilizzato per l'autenticazione tra il server SNMP e l'agente SNMP esistente sull'endpoint. Per questo esempio, il nome della community è impostato su test123. Fare clic su Next (Avanti) nell'angolo inferiore destro.



Impostazioni SNMP in Tutte le configurazioni nell'hub di controllo

Esaminare le configurazioni del dispositivo e fare clic su Apply (Applica) nell'angolo inferiore destro:

Device configurations Cisco Room Kit Pro Online

Configure Review Summary

### Review configurations

Review selected configurations.

| Configuration                          | Value                     | Actions                                   |
|----------------------------------------|---------------------------|-------------------------------------------|
| NetworkServices > SNMP > CommunityName | test1234 → <b>test123</b> | <a href="#">Edit</a> <a href="#">Copy</a> |
| NetworkServices > SNMP > Mode          | Off → <b>ReadWrite</b>    | <a href="#">Edit</a> <a href="#">Copy</a> |

Previous **Apply**

Rivedere le configurazioni prima di applicare le modifiche

Verificare che le modifiche alla configurazione siano state applicate correttamente. Fare quindi clic su Chiudi.

Device configurations Cisco Room Kit Pro Online

Configure Review Summary

### Configurations applied

The following configurations are applied to the selected device.

Actions

All configurations  
2

Success  
2

Error  
0

| Configuration                          | Value            | Status  |
|----------------------------------------|------------------|---------|
| NetworkServices > SNMP > CommunityName | <b>test123</b>   | Success |
| NetworkServices > SNMP > Mode          | <b>ReadWrite</b> | Success |

**Close**

Configurazioni degli endpoint applicate correttamente nell'hub di controllo

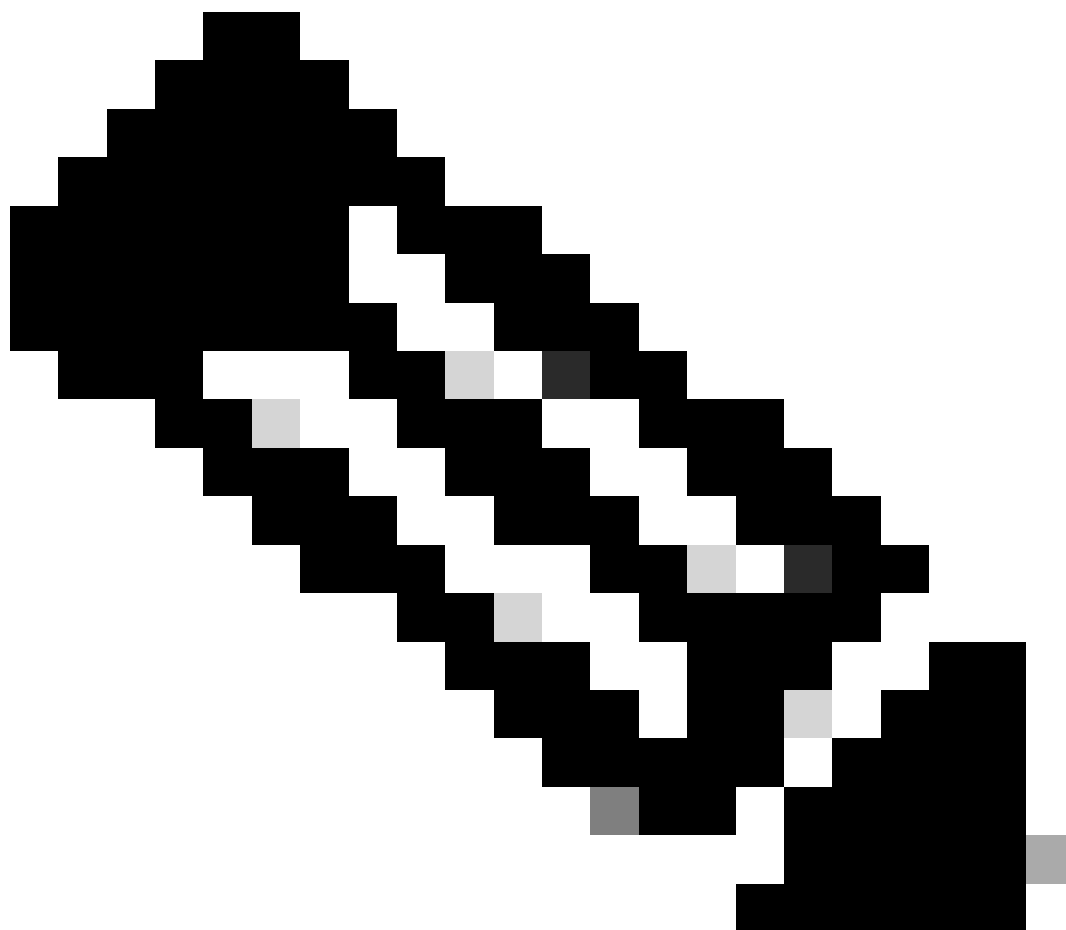
In questa fase, SNMPv2c è stato abilitato sull'endpoint e il nome della community è stato configurato.

## Abilitazione della modalità SNMPv3 nell'hub di controllo

SNMPv3 offre maggiore sicurezza e richiede una configurazione dell'endpoint diversa rispetto a SNMPv2c. Passare alla sezione Dispositivi in Gestione in Control Hub. Rimanere nella scheda Devices (Dispositivi) e selezionare uno degli endpoint che si desidera configurare con SNMPv3. Per questo esempio, viene usata una Cisco Room Bar Pro.

Nella sezione Configurazioni della scheda Dettagli dispositivo fare clic su Tutte le configurazioni. Viene visualizzata la pagina Configurazioni dispositivo. Digitare snmp nella barra di ricerca e selezionare Network Services > SNMP > Mode (Servizi di rete > SNMP > Modalità). Per questo esempio, la modalità SNMP è impostata su ReadWrite. Fare clic su SNMP per visualizzare tutte le impostazioni SNMP configurabili sul dispositivo.

---



Nota: Tutti i passaggi finora menzionati per SNMPv3 sono già stati descritti quando SNMPv2c è stato configurato in un esempio precedente. Per questo motivo, non viene fornita alcuna schermata dei passaggi. In caso di dubbi su come spostarsi tra le impostazioni dell'hub di controllo, consultare la sezione Attivazione della modalità

---

SNMPv2c nell'hub di controllo.

Per supportare solo SNMPv3, è necessario impostare il nome della community come stringa vuota racchiusa tra virgolette: "".

The screenshot shows the 'Device configurations' page for a 'Cisco Room Bar Pro' device. The interface has a blue header with 'Device configurations', 'Cisco Room Bar Pro', and 'Issues' tabs. Below the header is a navigation bar with 'Configure', 'Review', and 'Summary' tabs. The main content area displays four configuration sections: 'CommunityName', 'Mode', 'SystemContact', and 'SystemLocation'. Each section has a 'Supported device types' column, a 'Configuration value' column, a 'Default' column, and an 'Undo' button. The 'CommunityName' section shows 'Cisco Room Bar Pro' as the supported device type, with a text input field containing '""' (highlighted with a red box). The 'Mode' section shows 'Cisco Room Bar Pro' as the supported device type, with a dropdown menu set to 'ReadWrite' (highlighted with a red box). The 'SystemContact' and 'SystemLocation' sections show 'Cisco Room Bar Pro' as the supported device type, with text input fields containing 'Empty (Default)'. Each section also has a 'Factory' button and a 'Default' button. A 'Next' button is located at the bottom right of the configuration area (highlighted with a red box).

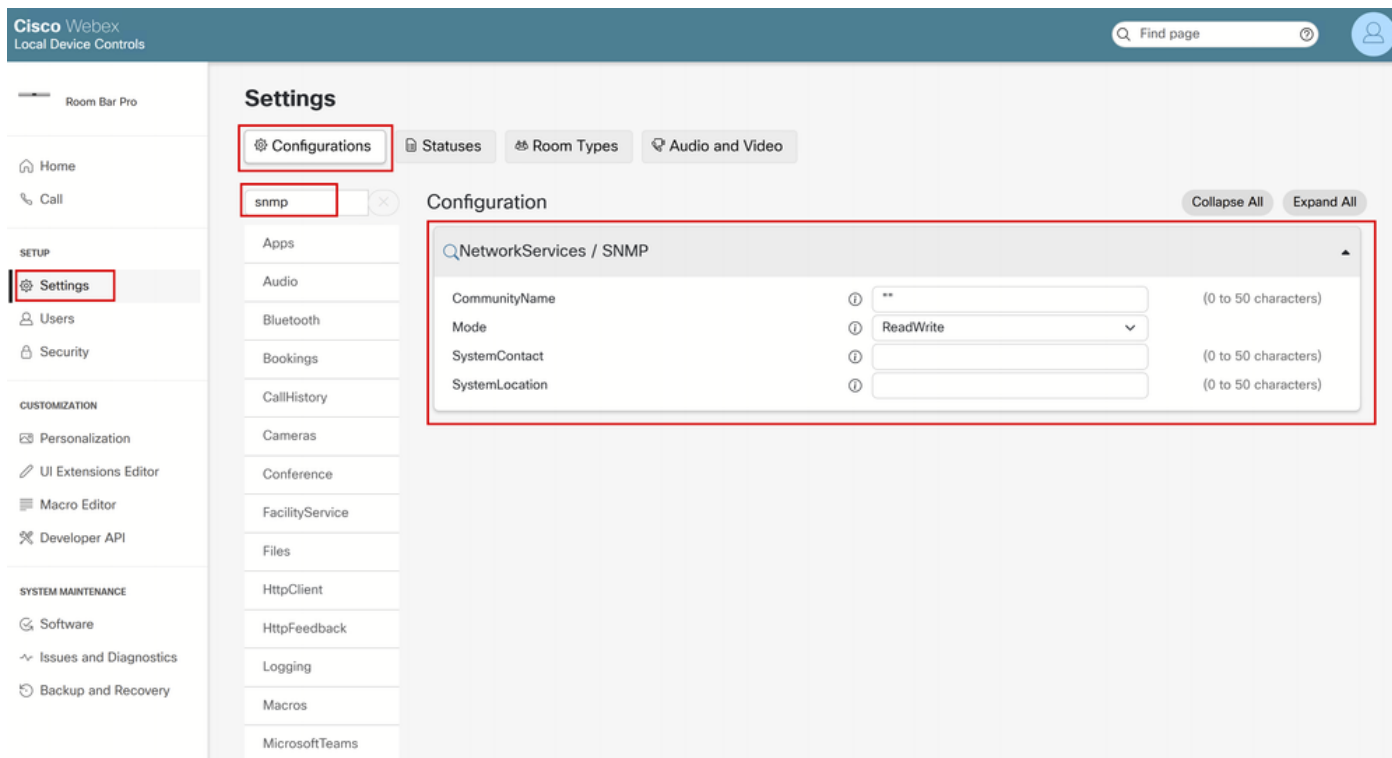
Impostazioni SNMP in Tutte le configurazioni nell'hub di controllo

Fare clic su Avanti, quindi rivedere le modifiche alla configurazione e fare clic su Applica. Fare clic su Chiudi per chiudere la pagina di configurazione del dispositivo.

La configurazione che può essere eseguita nell'hub di controllo è terminata. In questa fase, è abilitato solo SNMPv3.

Come appare la configurazione SNMP nell'interfaccia utente dell'endpoint

Le stesse configurazioni possono essere eseguite dalla GUI del dispositivo. Aprire una scheda del browser e digitare l'indirizzo IP dell'endpoint (è necessario trovarsi nella stessa rete dell'endpoint). Accedere come utente admin e nella GUI dell'endpoint, selezionare Settings nella sezione SETUP. Rimanere nella scheda Configurazioni e nella barra di ricerca delle impostazioni digitare snmp. Questa immagine mostra come vengono visualizzate le impostazioni SNMP per la configurazione SNMPv3 eseguita sulla barra spaziatrice Pro nella sezione precedente:



Configurazione di SNMPv3 sull'interfaccia utente dell'endpoint

## Configurare l'utente USM per SNMPv3

Per poter utilizzare SNMPv3, è necessario creare un utente USM. I comandi disponibili per eseguire questa azione sono disponibili nel collegamento [qui](#) alla documentazione del sistema operativo della room. Utilizzare SSH per connettersi al dispositivo. A tale scopo, è necessario disporre di un account amministratore sul dispositivo. In caso contrario, è necessario creare un account amministratore. Questa sezione tratta l'intero processo.

Passare alla sezione Dispositivi in Gestione in Control Hub. Rimanere nella scheda Dispositivi e selezionare uno degli endpoint per cui si desidera creare un utente amministratore. Nell'esempio, viene usata una Cisco Room Bar Pro.

In Dettagli dispositivo passare alla sezione Supporto e fare clic su Controlli dispositivo locale (per il corretto funzionamento di questa sezione è necessario che ci sia la stessa rete dell'endpoint). Viene visualizzata l'interfaccia utente del dispositivo. Passare a Utenti nella sezione IMPOSTAZIONE e fare clic su Crea utente.

Cisco Webex Local Device Controls

Find page

Room Bar Pro

Home

Call

SETUP

Settings

**Users**

Security

CUSTOMIZATION

Personalization

UI Extensions Editor

Macro Editor

Developer API

SYSTEM MAINTENANCE

Software

Issues and Diagnostics

Backup and Recovery

### Users

Create User

| Username                   | Status   | Admin <sup>1</sup> | Audit <sup>1</sup> | RoomControl <sup>1</sup> | Integrator <sup>1</sup> | User <sup>1</sup> |
|----------------------------|----------|--------------------|--------------------|--------------------------|-------------------------|-------------------|
| <a href="#">admin</a>      | Inactive | ✓                  | ✓                  |                          |                         | ✓                 |
|                            | Active   | ✓                  | ✓                  | ✓                        | ✓                       | ✓                 |
| <a href="#">touchpanel</a> | Active   | ✓                  | ✓                  | ✓                        | ✓                       | ✓                 |

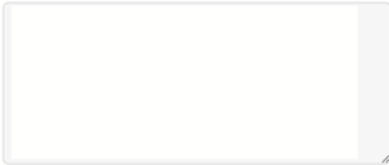
**Remote Support**

The Remote Support User is a special user account that has wider access rights than regular admin accounts. It is used by Cisco technical support to log in to the device to troubleshoot system issues, such as problems with the device's operating system.

This remote support user on this system is managed by Cisco Webex Control Hub.

This user is valid until

Token



Sezione Users nell'interfaccia utente dell'endpoint

Fornire un nome utente e una passphrase (password). Verificare che l'utente disponga dei privilegi di amministratore completi e che sia attivo:

Cisco Webex Local Device Controls

Find page

Room Bar Pro

Home

Call

SETUP

Settings

**Users**

Security

CUSTOMIZATION

Personalization

UI Extensions Editor

Macro Editor

Developer API

SYSTEM MAINTENANCE

Software

Issues and Diagnostics

Backup and Recovery

### Add New User

< Back

Username

Roles ☒ Admin<sup>1</sup>

☒ Audit<sup>1</sup>

☒ RoomControl<sup>1</sup>

☒ Integrator<sup>1</sup>

☒ User<sup>1</sup>

Status ☒ Active

☐ Inactive

Client Certificate DN

If using client certificates for authentication, enter the client certificate's full Distinguished Name. Both the /CN=alice/DC=example/DC=com and the CN=alice, DC=example, DC=com formats are supported.

☒ Require passphrase change on next user sign in

New passphrase

Generate new passphrase... <sup>1</sup>

Confirm passphrase

Create User

Creazione di un utente dalla GUI dell'endpoint

Verificare che l'utente sia stato creato e sia attivo dalla pagina Utenti:



Room Bar Pro

Home

Call

## SETUP

Settings

Users

Security

## CUSTOMIZATION

Personalization

UI Extensions Editor

Macro Editor

Developer API

## SYSTEM MAINTENANCE

Software

Issues and Diagnostics

Backup and Recovery

## Users

Create User

| Username                   | Status   | Admin <sup>1</sup> | Audit <sup>1</sup> | RoomControl <sup>1</sup> | Integrator <sup>1</sup> | User <sup>1</sup> |
|----------------------------|----------|--------------------|--------------------|--------------------------|-------------------------|-------------------|
| <a href="#">admin</a>      | Inactive | ✓                  | ✓                  |                          |                         | ✓                 |
|                            | Active   | ✓                  | ✓                  | ✓                        | ✓                       | ✓                 |
| <a href="#">testuser1</a>  | Active   | ✓                  | ✓                  | ✓                        | ✓                       | ✓                 |
| <a href="#">touchpanel</a> | Active   | ✓                  | ✓                  | ✓                        | ✓                       | ✓                 |

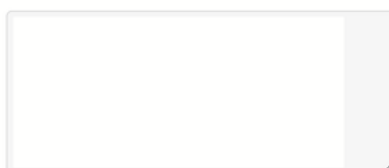
## Remote Support

The Remote Support User is a special user account that has wider access rights than regular admin accounts. It is used by Cisco technical support to log in to the device to troubleshoot system issues, such as problems with the device's operating system.

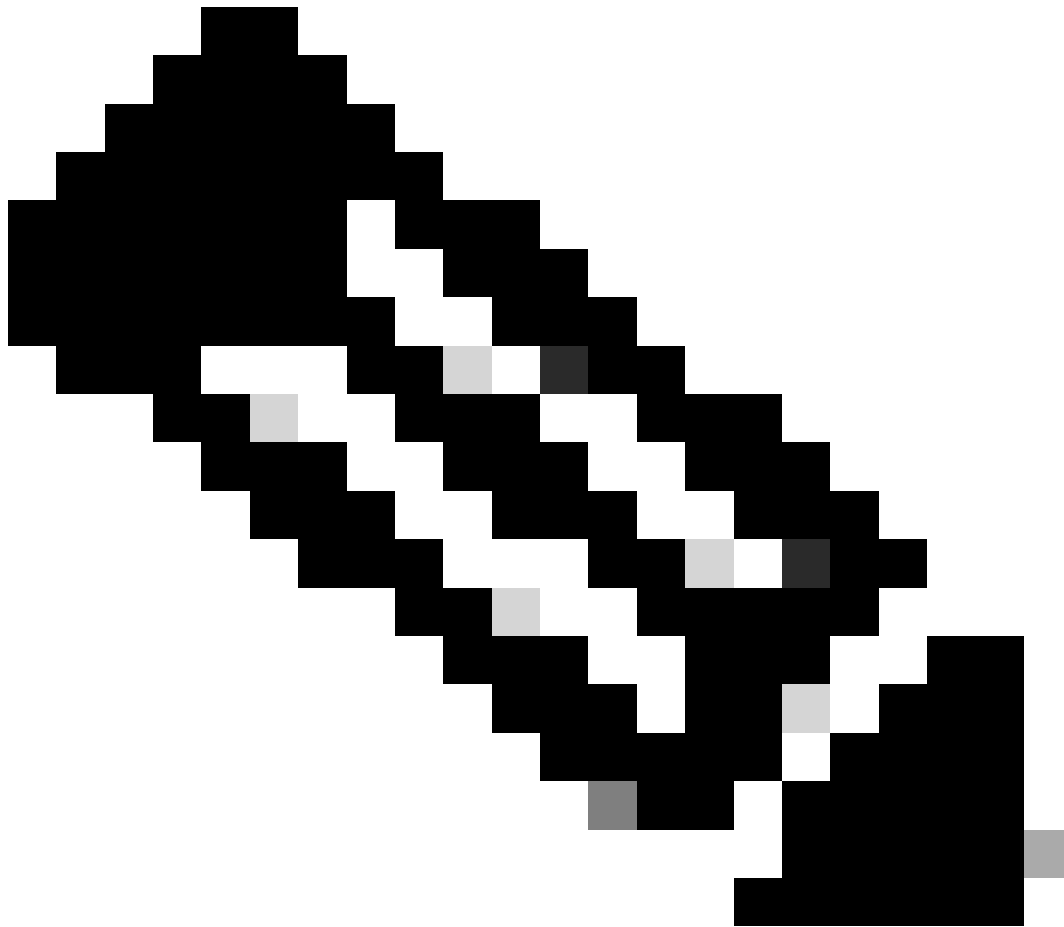
This remote support user on this system is managed by Cisco Webex Control Hub.

This user is valid until

Token



Nuovo utente creato ed elencato tra altri utenti



Nota: Al primo tentativo di accesso SSH con un utente appena creato, viene chiesto di modificare la password. Verrà visualizzato un messaggio simile al seguente:

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

Modifica della password al primo avvio di SSH

Dopo aver cambiato la password, la connessione viene immediatamente interrotta e occorre avviare una nuova connessione SSH.

---

Dopo aver creato l'utente admin, usare un client SSH a scelta e connettersi all'endpoint. Accedere con le credenziali di amministratore. Viene visualizzato il seguente prompt:

```
Welcome to
Cisco Codec Release RoomOS 11.23.1.8 3963b07b5c5
SW Release Date: 2024-12-12
*r Login successful
OK
```

Tentativo di accesso all'endpoint tramite SSH riuscito

Utilizzare il comando Network SNMP USM User Add come descritto in [questo](#) articolo. Per questa dimostrazione, il comando utilizzato è:

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

Se eseguito correttamente, il risultato del comando è:

```
xCommand Network SNMP USM User Add AuthenticationPassword: testuser123 AuthenticationProtocol: SHA-256 Name: psitaras PrivacyPassword: test1234
OK
*r UserAddResult (status=OK):
** end
```

Creazione di utenti USM tramite SSH

per eseguire il comando senza errori, è necessario attenersi a determinate regole descritte nella documentazione dei comandi condivisa in questo [collegamento](#). Per comodità, i requisiti correnti al momento della scrittura di questo documento per questo comando vengono incollati in questa immagine, ma è necessario accertarsi di fare riferimento a questo [collegamento](#) durante la creazione dell'utente. Alla fine dell'immagine, si noti che esiste la sintassi esatta del comando.

Creates a user (username and passwords) that a network management system can use to communicate with the video device using SNMP v3, User-based Security Model (USM). All USM users have equal access rights (read, read-write, or none), refer to the NetworkServices SNMP Mode setting. Authentication and privacy are always on. That is, the device supports only the authPriv security level and the privacy protocol is always AES (Advanced Encryption Standard). This command has no effect on SNMP v2c; authentication for SNMP v2c is configured with the NetworkServices SNMP CommunityName setting.

[Read less...](#)

#### AuthenticationPassword

Required <8 - 255>

The authentication password for this USM user. It is used when authenticating the network management system. The authentication password is stored as a localized hashed value on the device (refer to the AuthenticationProtocol parameter).

#### AuthenticationProtocol

Required SHA-224, SHA-256, SHA-384, SHA-512

The authentication hash function that will be applied before storing the authentication password on the device. The device only supports the listed hash functions (from the SHA-2 family); neither MD nor SHA-1 is supported.

#### Name

Required <0 - 32>

The name of the USM user.

#### PrivacyPassword

<8 - 255>

The privacy password for this USM user. It is used for the data encryption. The privacy password is stored as a localized hashed value (AES-128) on the device. If a privacy password is not set explicitly in this parameter, it will be the same as the authentication password (with hash function as specified in the Authentication Protocol parameter).

|                             |                                                      |
|-----------------------------|------------------------------------------------------|
| Back-end                    | Any                                                  |
| User roles                  | Admin                                                |
| Products                    | Board Series, Desk, Desk Mini, Desk Pro, Room Series |
| Privacy impacting           | No                                                   |
| Microsoft Teams Rooms (MTR) | Yes                                                  |

Code: JavaScript Command line Webex Cloud

Invoke

```
xCommand Network SNMP USM User Add AuthenticationPassword: value AuthenticationProtocol: value Name: value PrivacyPassword: value
```

Copy

Sintassi dei comandi di creazione utenti USM dalla documentazione di xAPI



Avviso: In caso di errore o di mancato rispetto di un requisito, il comando restituisce un errore e l'utente non verrà creato. Viene fornito un esempio, in cui invece di fornire una Password per la privacy con almeno 8 caratteri, viene fornita una password più breve di 7 caratteri:

```
xCommand Network SNMP USM User Add AuthenticationPassword: testuser123 AuthenticationProtocol: SHA-256 Name: psitaras PrivacyPassword: test123
*r UserAddResult (status=ParameterError):
*r UserAddResult PrivacyPassword: "Invalid value"
** end
ERROR
```

Privacy Password must be at least 8 characters long. A shorter password returns an error and is not going to create the user.

Creazione dell'utente USM non riuscita a causa della password per la privacy breve

È possibile verificare se l'utente è stato creato utilizzando il comando Network SNMP USM User List. Con questo comando vengono elencati tutti gli utenti USM archiviati nel dispositivo:

```
xCommand Network SNMP USM User List
```

```
OK
```

```
*r UserListResult (status=OK):
```

```
*r UserListResult User 1 AuthenticationProtocol: "SHA-256"
```

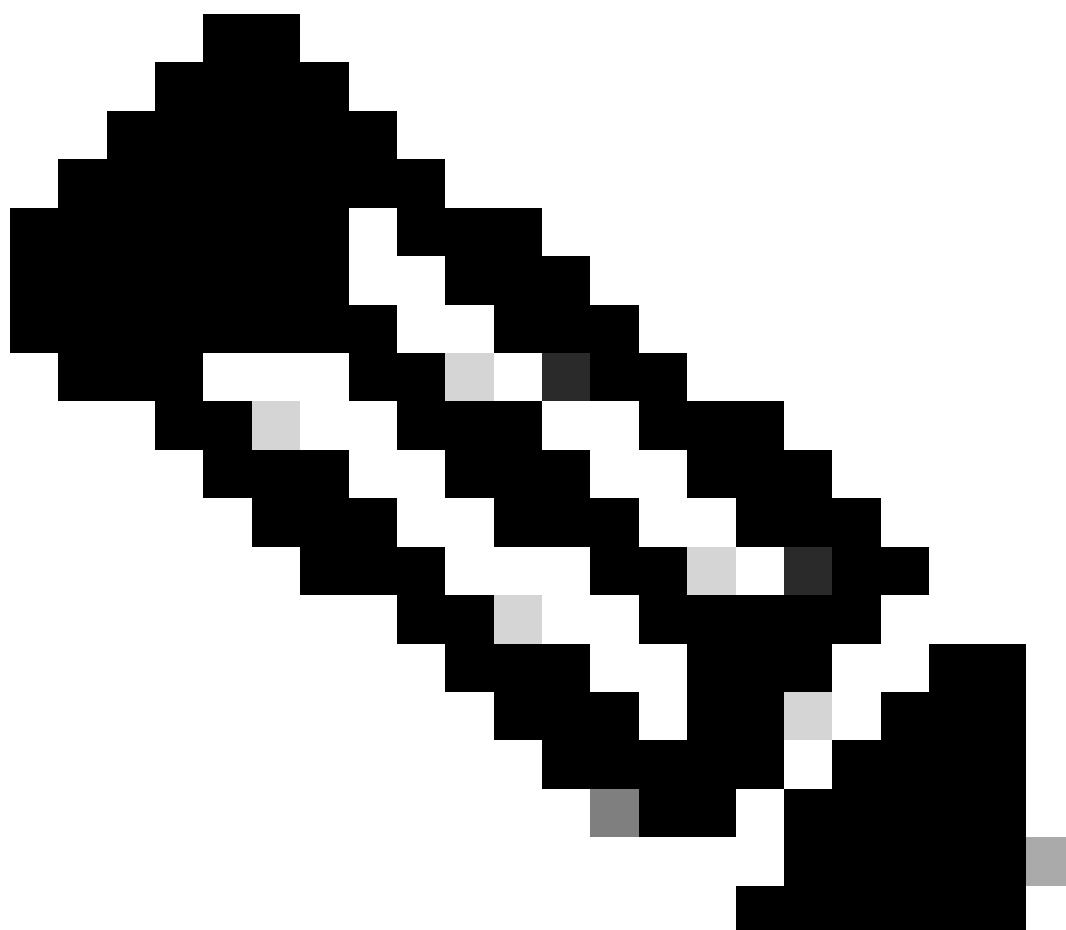
```
*r UserListResult User 1 Name: "psitaras"
```

```
** end
```

Comando elenco utenti SNMP USM di rete utilizzato per confermare la creazione dell'utente

In questa fase, è stato confermato che la creazione dell'utente psitara è stata completata. Configurazione di SNMPv3 completata.

---



Nota: Le aree utente USM non sono visibili nella GUI dell'endpoint nella sezione Users. Questo è previsto.

---

Cisco Webex Local Device Controls

Find page

Room Bar Pro

Home

Call

SETUP

Settings

Users

Security

CUSTOMIZATION

Personalization

UI Extensions Editor

Macro Editor

Developer API

SYSTEM MAINTENANCE

Software

Issues and Diagnostics

Backup and Recovery

### Users

Create User

| Username                                | Status   | Admin | Audit | RoomControl | Integrator | User |
|-----------------------------------------|----------|-------|-------|-------------|------------|------|
| <a href="#">admin</a>                   | Inactive | ✓     | ✓     |             |            | ✓    |
| <a href="#">am</a> <a href="#">test</a> | Active   | ✓     | ✓     | ✓           | ✓          | ✓    |
| <a href="#">testuser1</a>               | Active   | ✓     | ✓     | ✓           | ✓          | ✓    |
| <a href="#">touchpanel</a>              | Active   | ✓     | ✓     | ✓           | ✓          | ✓    |

**Remote Support**

The Remote Support User is a special user account that has wider access rights than regular admin accounts. It is used by Cisco technical support to log in to the device to troubleshoot system issues, such as problems with the device's operating system.

This remote support user on this system is managed by Cisco Webex Control Hub.

This user is valid until

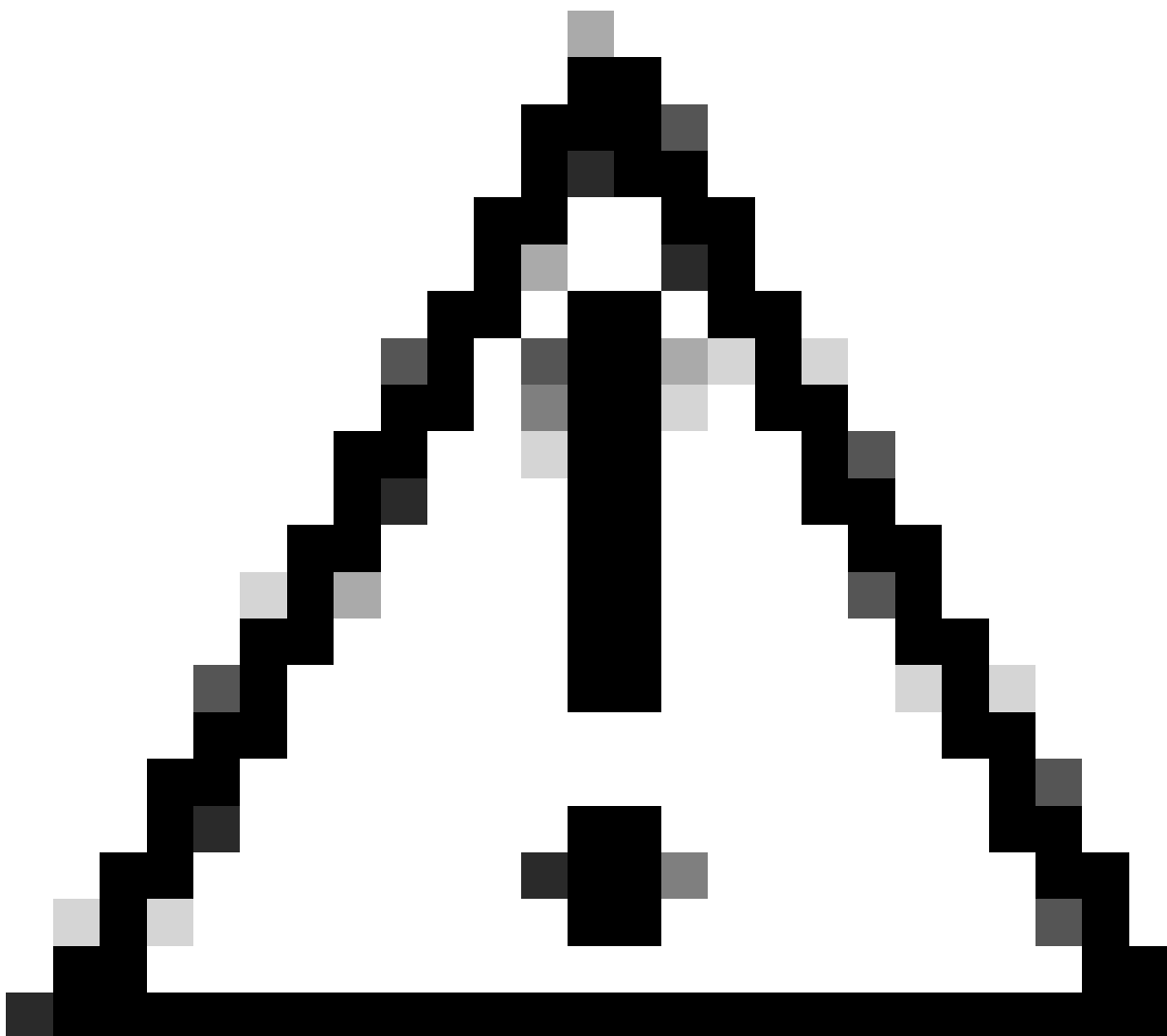
Token

USM user "psitaras" is not visible under the user list.

Gli utenti USM non sono visibili sotto gli utenti nella GUI dell'endpoint

## Test della configurazione di SNMPv2c e SNMPv3

In questa fase è possibile procedere con il test della configurazione di SNMPv2c e/o SNMPv3 con il sistema di gestione della rete (NMS, Network Management System). Per questo articolo, la configurazione lab non contiene alcun server NMS o SNMP che esegue un servizio SNMP. Per verificare la configurazione, viene utilizzata l'utilità snmpwalk. Questa utilità viene installata su un server Linux.



Attenzione: Snmpwalk non è uno strumento consigliato per il test della configurazione SNMP sugli endpoint di collaborazione. Non è supportata dai tecnici TAC ed è necessario avere familiarità con l'utilizzo dello strumento prima di procedere con il test. Anziché snmpwalk, è possibile utilizzare qualsiasi altro strumento SNMP o il sistema NMS per verificare la configurazione. Snmpwalk è utilizzato in questo articolo solo come esempio (è necessario uno strumento per testare la configurazione a scopo dimostrativo) e non vi è alcun impegno o promozione correlato al suo utilizzo.

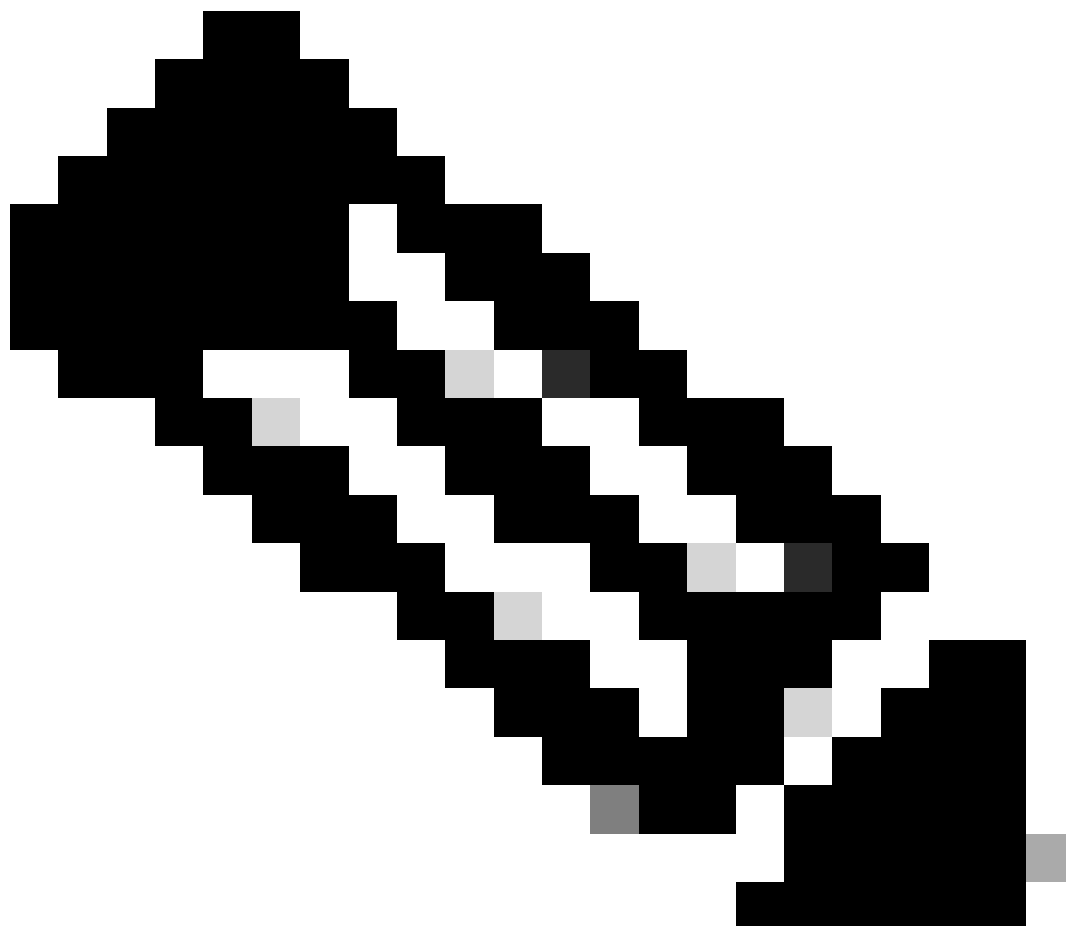
L'installazione di snmpwalk non fa parte di questa guida e viene omessa. A seconda del sistema operativo del computer utilizzato per il test, i requisiti di installazione possono variare. Prima di eseguire il test, è necessario procedere all'installazione.

---

Snmpwalk è uno strumento che può essere utilizzato per verificare la configurazione SNMP. Esegue una passeggiata tra i MiB dell'endpoint e restituisce le informazioni disponibili. Gli endpoint registrati nel cloud espongono 7 identificatori di oggetto (OID, Object Identifier):

- SNMPv2-MIB::sysDescr (lettura),

- SNMPv2 -MIB::sysObjectID (lettura),
  - DISMAN-EVENT-MIB::sysUpTimeInstance (lettura),
  - SNMPv2 -MIB::sysContact (lettura/scrittura),
  - SNMPv2 -MIB::sysName (lettura/scrittura),
  - SNMPv2 -MIB::sysLocation (lettura/scrittura),
  - SNMPv2 -MIB::sysServices (lettura).
- 



Nota: Gli IP interni utilizzati per i test snmpwalk elencati sono IP privati e non sono più in uso. Il laboratorio utilizzato per questa guida è stato smantellato e i dispositivi sono stati ripristinati in fabbrica.

---

L'endpoint Cisco Room Kit Pro è configurato con SNMPv2c. L'autenticazione viene eseguita utilizzando le stringhe della community. Utilizzare questo comando:

```
# '-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: FD02706JG49"
```

```
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 restituisce 7 risultati come previsto. Ci sono tre MiB vuoti:

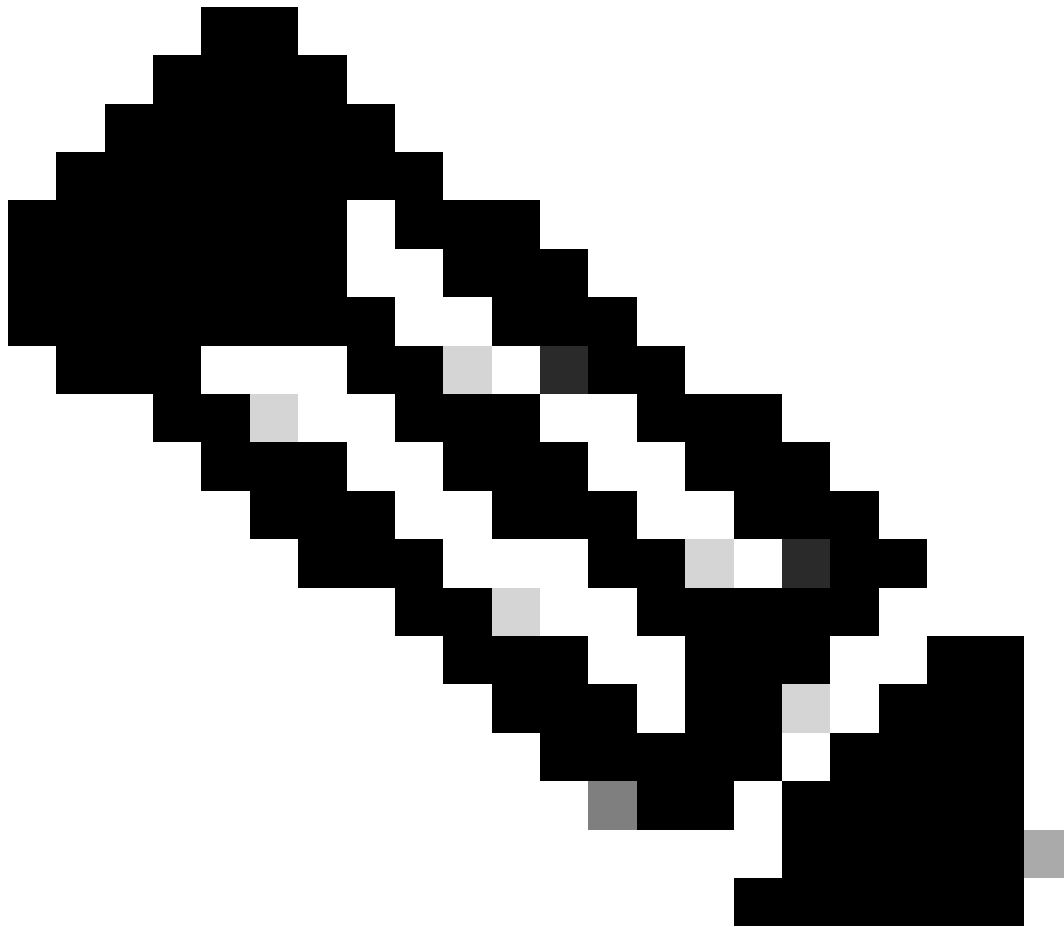
1. SNMPv2 -MIB::sysContact (lettura/scrittura), (iso.3.6.1.2.1.1.4.0)
2. SNMPv2 -MIB::sysName (lettura/scrittura), (iso.3.6.1.2.1.1.5.0)
3. SNMPv2 -MIB::sysLocation (lettura/scrittura), (iso.3.6.1.2.1.1.6.0)

Per impostare i valori di questi MiB è possibile utilizzare tre comandi xConfiguration. SSH all'endpoint e usare questi comandi:

```
xConfiguration NetworkServices SNMP SystemContact: testuser1
```

```
xConfiguration NetworkServices SNMP SystemLocation: Room1
```

```
xConfiguration SystemUnit Name: My_Room_Kit_Pro
```



Nota: Anziché utilizzare questi tre comandi, è possibile modificare queste impostazioni da Control Hub, dall'interfaccia utente dell'endpoint o dalle API Webex.

---

Una volta eseguiti i comandi precedenti, utilizzare nuovamente snmpwalk sullo stesso endpoint. I MiB precedentemente vuoti vengono popolati con i valori forniti tramite i comandi 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: FD02706JG49"  
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)

In questa fase, viene confermato che la configurazione SNMPv2c creata sul dispositivo Room Kit Pro è operativa.

L'endpoint Cisco Room Bar Pro è configurato con SNMPv3. Per SNMPv3, è necessario accertarsi di utilizzare l'autenticazione corretta. Le stringhe della community non vengono utilizzate. Al suo posto, SNMPv3 utilizza nomi utente e password.

```
# '-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)
```

In questa fase, viene confermato che la configurazione di SNMPv3 creata sul dispositivo Room Bar Pro è operativa.

## È possibile che un endpoint abbia contemporaneamente SNMPv2c e SNMPv3 attivi?

Sì, è possibile. Tuttavia, durante la configurazione SNMP, è necessario impostare un nome di community per poter disporre dell'autenticazione SNMPv2c. Per questo test, viene utilizzata la barra della stanza Pro degli esempi precedenti. La configurazione corrente nella sezione Tutte le configurazioni dell'hub di controllo dell'endpoint è:

**Select configurations**  
Select one or more configurations to apply to the selected device.

All > NetworkServices > SNMP

| CommunityName | Supported device types | Configuration value           | Default ⓘ                                              | Undo |
|---------------|------------------------|-------------------------------|--------------------------------------------------------|------|
|               | Cisco Room Bar Pro     | <input type="text" value=""/> | <input checked="" type="checkbox"/> Factory ⓘ<br>Empty |      |
|               |                        | 0 - 50 characters             |                                                        |      |

| Mode | Supported device types | Configuration value                    | Default ⓘ                                            | Undo |
|------|------------------------|----------------------------------------|------------------------------------------------------|------|
|      | Cisco Room Bar Pro     | <input type="text" value="ReadWrite"/> | <input checked="" type="checkbox"/> Factory ⓘ<br>Off |      |

Configurazioni SNMP degli endpoint nell'hub di controllo

Il nome della community non è vuoto. Sono disponibili due virgolette, che indicano che il nome della community è una stringa vuota. È possibile limitare il supporto SNMP solo alla versione 3, impostando NetworkServices SNMP CommunityName su una stringa vuota (""). È necessario sostituire questa stringa con un nome di community, ad esempio testbothSNMPv2\_v3.

**Select configurations**  
Select one or more configurations to apply to the selected device.

All > NetworkServices > SNMP

| CommunityName | Supported device types | Configuration value                            | Default ⓘ                                              | Undo |
|---------------|------------------------|------------------------------------------------|--------------------------------------------------------|------|
|               | Cisco Room Bar Pro     | <input type="text" value="testbothSNMPv2_v3"/> | <input checked="" type="checkbox"/> Factory ⓘ<br>Empty |      |
|               |                        | 0 - 50 characters                              |                                                        |      |

| Mode | Supported device types | Configuration value                    | Default ⓘ                                            | Undo |
|------|------------------------|----------------------------------------|------------------------------------------------------|------|
|      | Cisco Room Bar Pro     | <input type="text" value="ReadWrite"/> | <input checked="" type="checkbox"/> Factory ⓘ<br>Off |      |

Aggiungi nome community per SNMPv2c nelle impostazioni di configurazione degli endpoint dell'hub di controllo

È già stato confermato che SNMPv3 funziona su Room Bar Pro. Snmpwalk consente di verificare il corretto funzionamento di SNMPv2c dopo aver configurato il nome della community:

```
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)
```

# È possibile configurare più endpoint tramite Control Hub con SNMP?

Sì, è possibile configurare più dispositivi contemporaneamente in Control Hub. In questo [articolo](#) vengono fornite informazioni su come eseguirlo passo per passo nella sezione Configurazione di più dispositivi.

## Dettagli importanti da ricordare

- Sono disponibili solo MiB specifici. Il numero di MiB disponibili è limitato dal progetto del team di progettazione che progetta gli endpoint. Non è possibile espandere o migliorare i MiB per ottenere ulteriori informazioni.
- SNMPv2c esegue l'autenticazione utilizzando il nome della community (definito anche stringa della community), mentre SNMPv3 esegue l'autenticazione utilizzando il nome utente e la password e offre anche la crittografia. Durante il test, accertarsi di utilizzare il metodo di autenticazione corretto (con snmpwalk o un altro strumento/NMS) per il protocollo configurato.
- L'autenticazione e la privacy sono sempre attive su SNMPv3. Gli endpoint supportano solo il livello di sicurezza authPriv e il protocollo di privacy è sempre AES (Advanced Encryption Standard).
- SNMPv3 è supportato solo con le opzioni User-based Security Model (USM). SNMPv3 over TLS non è supportato.
- I comandi utente USM utilizzati per configurare gli utenti per l'autenticazione SNMP non hanno alcun effetto su SNMPv2c.
- L'impostazione di SNMP CommunityName sugli endpoint non ha alcun effetto sulla configurazione di SNMPv3.
- SNMP CommunityName fa distinzione tra maiuscole e minuscole.
- È possibile limitare il supporto SNMP solo a v3 impostando NetworkServices SNMP CommunityName su una stringa vuota ("").
- SNMPv1 non è supportato.
- Sia per SNMPv2c che per SNMPv3, gli endpoint espongono gli stessi identificatori di oggetto (OID).
- Per il protocollo SNMPv3, il protocollo di autenticazione deve essere incluso nella famiglia SHA-2 (non sono supportati né MD né SHA-1). In caso contrario, le richieste SNMP non verranno autenticate e rimarranno senza risposta.
- La password per la privacy viene memorizzata come valore hash localizzato (AES-128) sul dispositivo. Se in questo parametro non è impostata in modo esplicito una password per la privacy, verrà impostata in modo che sia uguale alla password di autenticazione (con una funzione hash come specificato nel parametro Authentication Protocol).
- Le password/passphrase e i nomi utente devono rientrare in limiti di lunghezza specifici. Ad esempio, il nome utente USM deve essere composto da un massimo di 32 caratteri e la password di autenticazione deve essere composta da un minimo di 8 e un massimo di 255 caratteri. Se questi requisiti non vengono soddisfatti, il comando Network SNMP USM User Add non riesce a creare l'utente e restituisce un errore.

# Connessione a TAC per risolvere un problema SNMP su un endpoint

Se la configurazione SNMP dell'endpoint è stata completata ma è stato rilevato un problema, è necessario contattare TAC e condividere le seguenti informazioni:

- Specificare l'ID organizzazione nell'hub di controllo e il numero di serie (SN) dell'endpoint interessato.
- Descrivere lo scenario da affrontare.
- Specificare la versione SNMP che si sta tentando di configurare.
- Fornire gli eventuali messaggi di errore visualizzati.
- In caso di problemi di configurazione del dispositivo, spiegare chiaramente in quale fase il processo di configurazione è stato interrotto e fornire gli screenshot. Condividere il comando di configurazione che restituisce un errore.
- Raccogliere i log degli endpoint e caricarli sulla richiesta.
- Condividere l'utilità NMS o un altro strumento utilizzato per verificare la configurazione SNMP. Se si utilizza un'utilità per eseguire il test sull'agente SNMP degli endpoint, specificare il comando completo utilizzato.

## Informazioni correlate

[Documentazione xAPI per il sistema operativo Room - Comandi relativi a SNMP](#)

[Configurazioni dei dispositivi per schede madri, scrivanie e dispositivi serie Room](#)

### Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).