

SNMP configureren op in de cloud geregistreerde eindpunten

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Wat is SNMP](#)

[Welke informatie kan worden opgevraagd](#)

[SNMP configureren op een in de cloud geregistreerd eindpunt](#)

[SNMPv2c-modus inschakelen in Control Hub](#)

[SNMPv3-modus inschakelen in Control Hub](#)

[Hoe ziet de SNMP-configuratie eruit in de Endpoint GUI](#)

[De USM-gebruiker configureren voor SNMPv3](#)

[SNMPv2c- en SNMPv3-configuratie testen](#)

[Kan een eindpunt zowel SNMPv2c als SNMPv3 tegelijkertijd actief hebben?](#)

[Meerdere eindpunten kunnen worden geconfigureerd via Control Hub met SNMP](#)

[Belangrijke details om te onthouden](#)

[Contact opnemen met TAC om een SNMP-probleem op een eindpunt op te lossen](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe SNMP op een in de cloud geregistreerd eindpunt kan worden geconfigureerd en opgelost.

Voorwaarden

Vereisten

Het wordt aanbevolen dat u enige bekendheid heeft met deze onderwerpen:

- besturingsnaafplatform
- Beheer van het eindpunt via de grafische gebruikersinterface (GUI) van het eindpunt en de sectie Apparaten van de controlehub
- SSH naar een eindpunt als admin gebruiker
- Room OS
- SNMP (SNMPv2c en SNMPv3)
- Snapwalk of een ander hulpprogramma/tool of Network Management System (NMS) om de SNMP-configuratie te testen

Gebruikte componenten

De hier vermelde apparatuur is gebruikt om de tests uit te voeren en de in dit document beschreven resultaten te produceren:

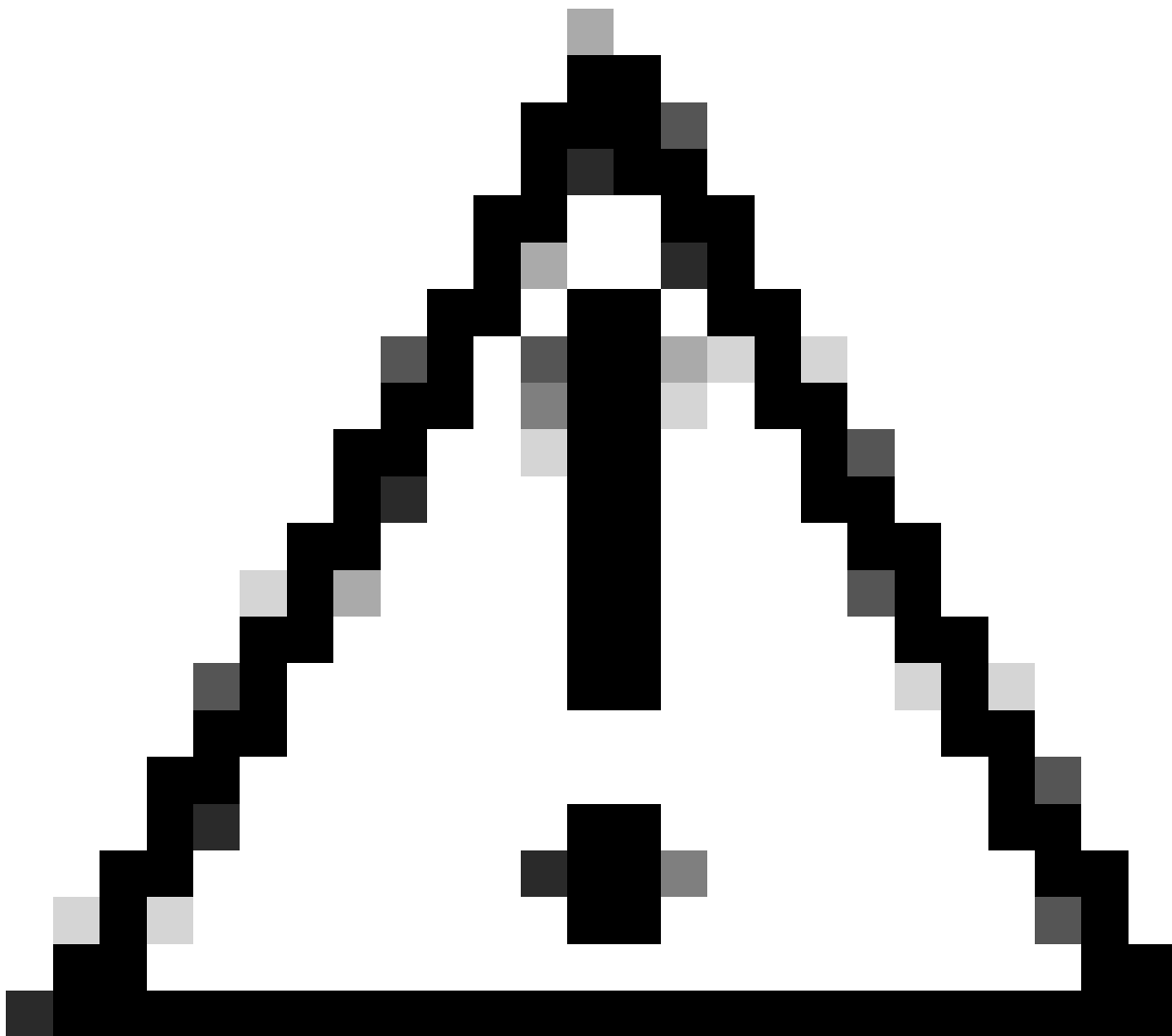
- Controlehuborganisatie
- Cisco Room Kit Pro
- Cisco Room Bar Pro
- Linux Server host het snmpwalk-hulpprogramma voor het testen van SNMP-configuratie.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Wat is SNMP

SNMP staat voor Simple Network Management Protocol. Het is een protocol dat wordt gebruikt voor het verzamelen en beheren van informatie over de apparaten in een netwerk, het bewaken van de status van het apparaat of het aanbrengen van configuratiewijzigingen. Deze apparaten kunnen routers, switches, servers, printers of andere apparaten zijn. Het is een voorwaarde dat aan deze apparaten een IP-adres is toegewezen. Er zijn drie versies van SNMP. Room OS ondersteunt SNMPv2c en SNMPv3. SNMPv1 wordt niet ondersteund.

Dit artikel is gericht op de configuratie en probleemoplossing van SNMP op samenwerkingseindpunten waarop Room OS wordt uitgevoerd dat in de cloud is geregistreerd (waarbij Webex Edge voor apparaten niet wordt gebruikt).



Let op: dit artikel benadert de SNMP-configuratie alleen vanuit het perspectief van het eindpunt. Elke configuratie aan de netwerkkant en de tools die worden gebruikt om SNMP-gerelateerde informatie op de eindpunten op te vragen/bij te werken, vallen buiten het toepassingsgebied van dit artikel.

TAC ondersteunt de probleemoplossing van SNMP binnen het netwerk niet en kan geen conclusies geven over waarom SNMP niet werkt zoals verwacht vanuit netwerkperspectief. Uw netwerkteam moet worden betrokken bij het verder oplossen van deze problemen.

Het beheer van SNMP kan met veel verschillende tools worden bereikt. Deze instrumenten worden niet ondersteund door de TAC. Als er een discrepantie is in de informatie die deze tools verzamelen van de eindpunten, moet het probleem eerst door het netwerkteam worden opgelost en vervolgens worden geëscaleerd in TAC als er voldoende informatie is die bewijst dat het een eindpuntgerelateerd probleem is.

Welke informatie kan worden opgevraagd

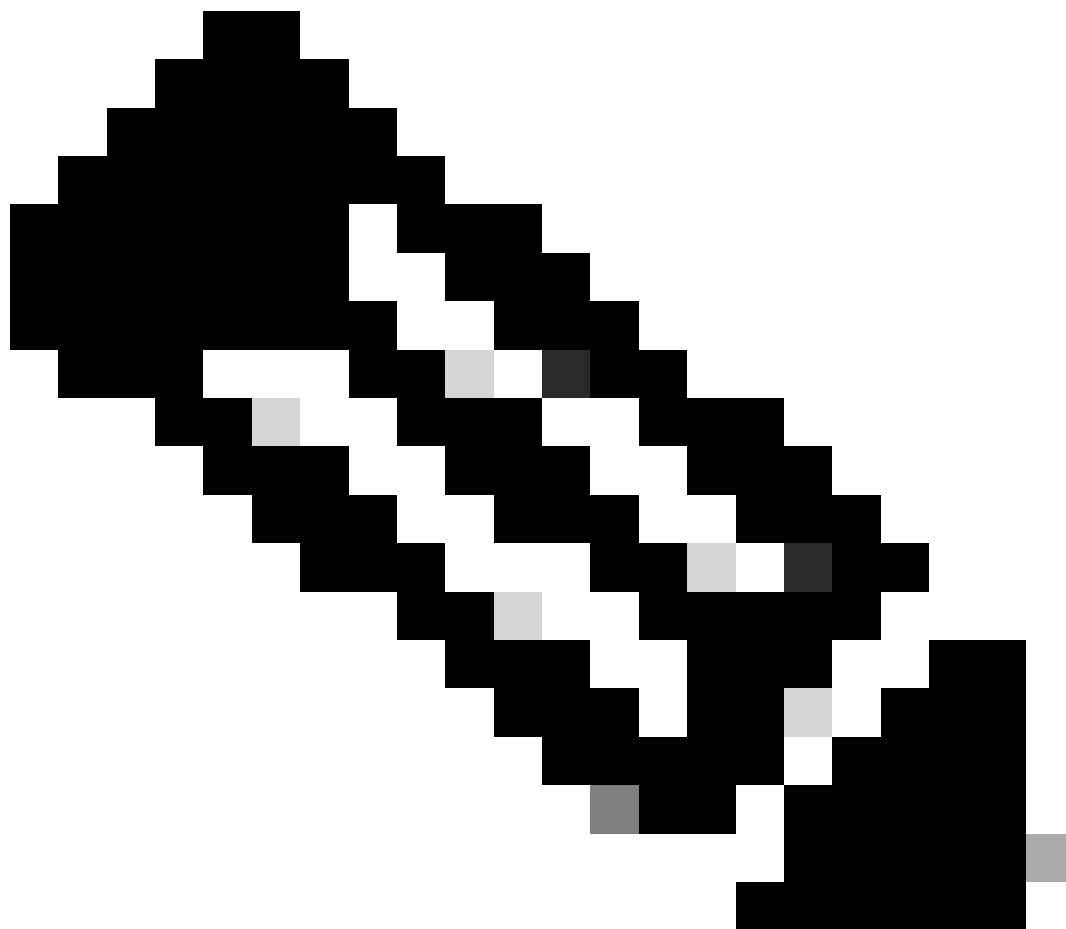
Met behulp van SNMP kunt u een beperkte hoeveelheid informatie opvragen bij het eindpunt. Ondersteunde OID's en MiBs zijn te zien in [deze link](#), onder de details van de opdrachtbeschrijving NetworkService SNMP Mode:

The screenshot displays 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 shows a search for 'snmp' with filters for 'Any product', 'Any', 'Command', 'Config', 'Status', 'Event', 'MTR', 'Any role', and 'Any back-end'. A list of results is shown, with 'NetworkServices SNMP Mode' highlighted in a red box. To the right, a detailed view of the 'NetworkServices SNMP Mode' command is shown, including a description of SNMP, a table of supported operations (OFF, ReadOnly, ReadWrite, Default value), and a table of supported products (Board 55, Board 55S, Board 70, Board 70S, Board 85S, Board Pro 55, Board Pro 75, Desk, Desk Mini, Desk Pro, Room Series). The interface also includes a 'Code' section with tabs for 'JavaScript', 'Command line', and 'Webex Cloud', and a 'Get value' button.

NetworkService SNMP Mode Command Description in Room OS xAPI Documentatie

De eindpunten stellen deze OID's bloot voor zowel SNMPv2 als SNMPv3:

- SNMPv2-MIB::sysDescr (gelezen),
- SNMPv2 -MIB::sysObjectID (gelezen),
- DISMAN-EVENT-MIB::sysUpTimeInstance (gelezen),
- SNMPv2 -MIB::sysContact (lezen/schrijven),
- SNMPv2 -MIB::sysName (lezen/schrijven),
- SNMPv2 -MIB::sysLocation (lezen/schrijven),
- SNMPv2 -MIB::sysServices (gelezen).

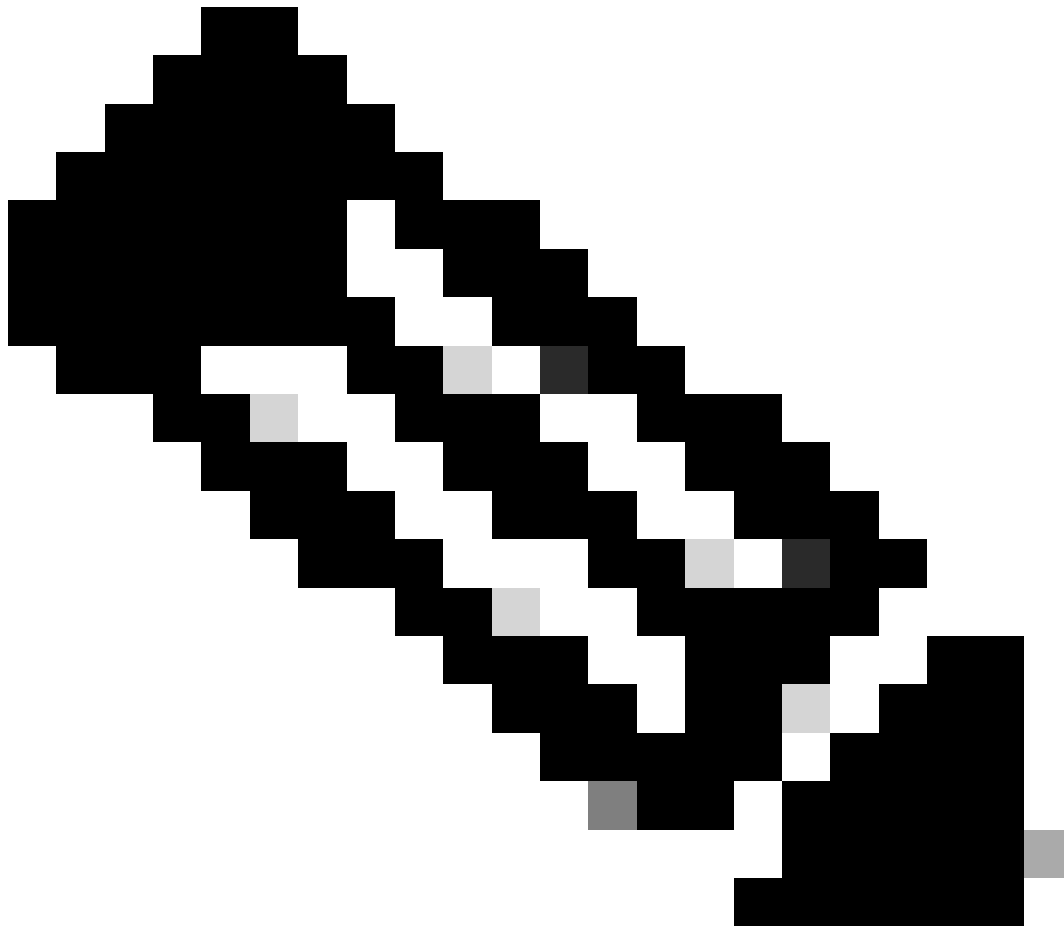


Opmerking: NetworkServices SNMP CommunityName kan worden ingesteld op een lege tekenreeks als u alleen SNMPv3 wilt gebruiken.

SNMP configureren op een in de cloud geregistreerd eindpunt

Over het algemeen kunnen configuratiewijzigingen op eindpunten op vier verschillende manieren plaatsvinden:

1. De beschikbare Webex API's
2. Het eindpunt GUI
3. Control Hub
4. SSH direct naar het eindpunt



Opmerking: om toegang te krijgen tot een endpoint-GUI, opent u een browser en typt u op de URL-balk het IP-adres van het eindpunt. U moet op hetzelfde netwerk zijn met het eindpunt en u moet gebruikersreferenties hebben om in te kunnen loggen.

Niet alle configuraties kunnen op alle vier manieren worden gemaakt. Voor het scenario van dit document kan de SNMP-modus op alle vier manieren worden ingeschakeld, maar om een SNMP-gebruiker te maken die via SNMP met het apparaat kan communiceren, moet u SSH naar het eindpunt sturen of de Webex API's gebruiken of de GUI van het eindpunt gebruiken bij de Developer API onder het gedeelte Aanpassing. USM-gebruikers kunnen niet worden gemaakt vanuit de sectie Alle configuraties van de Control Hub van het eindpunt.



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
/configuration.xml	Configuration settings
/status.xml	Endpoint status parameters
/command.xml	Available API commands
/valuespace.xml	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:

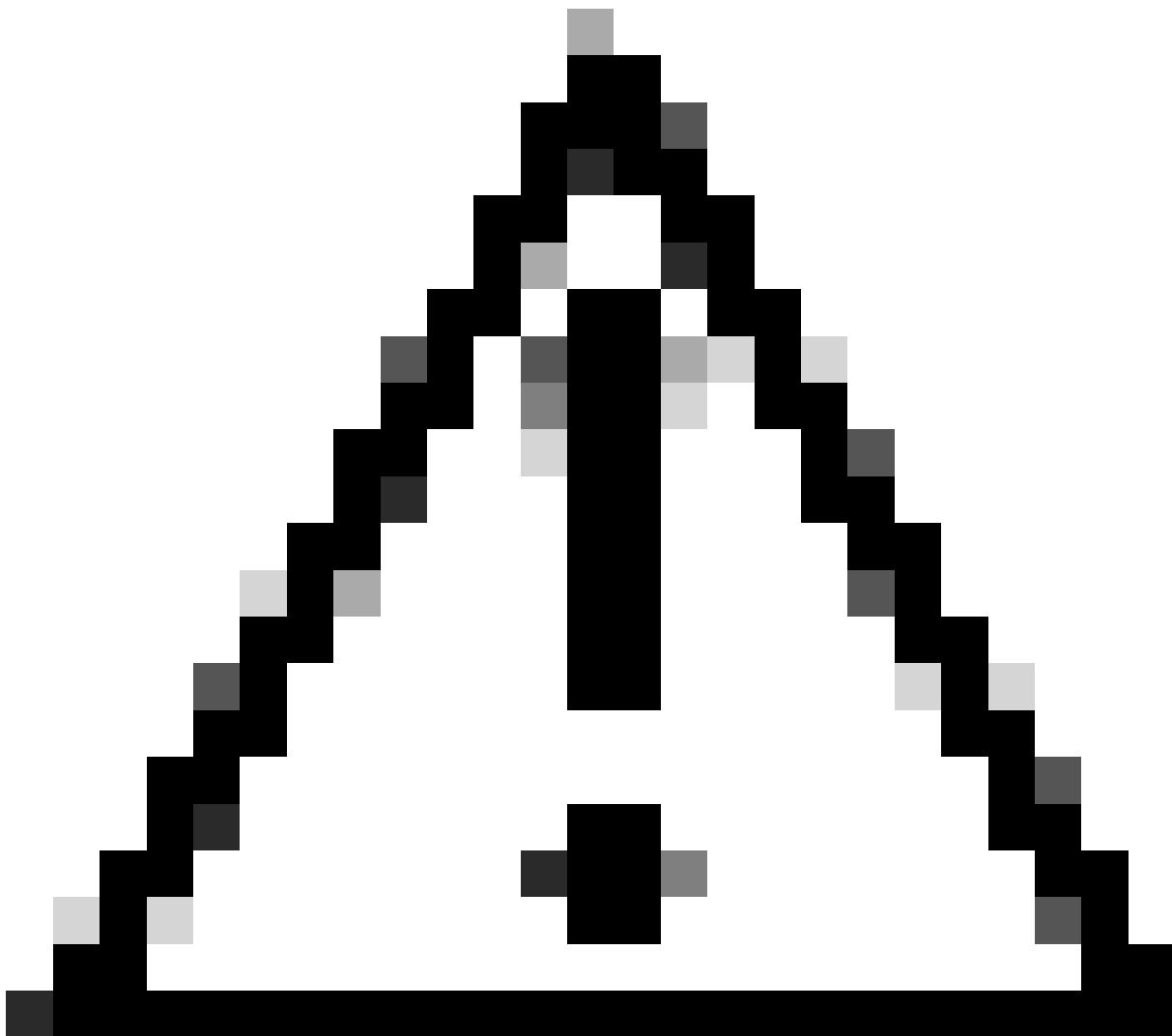
xCommand Dial Number: "person@example.com" Protocol: SIP

xCommand Network SNMP USM User List

[Execute](#)

1 of 1 applied successfully.

API-sectie voor ontwikkelaars op Endpoint GUI

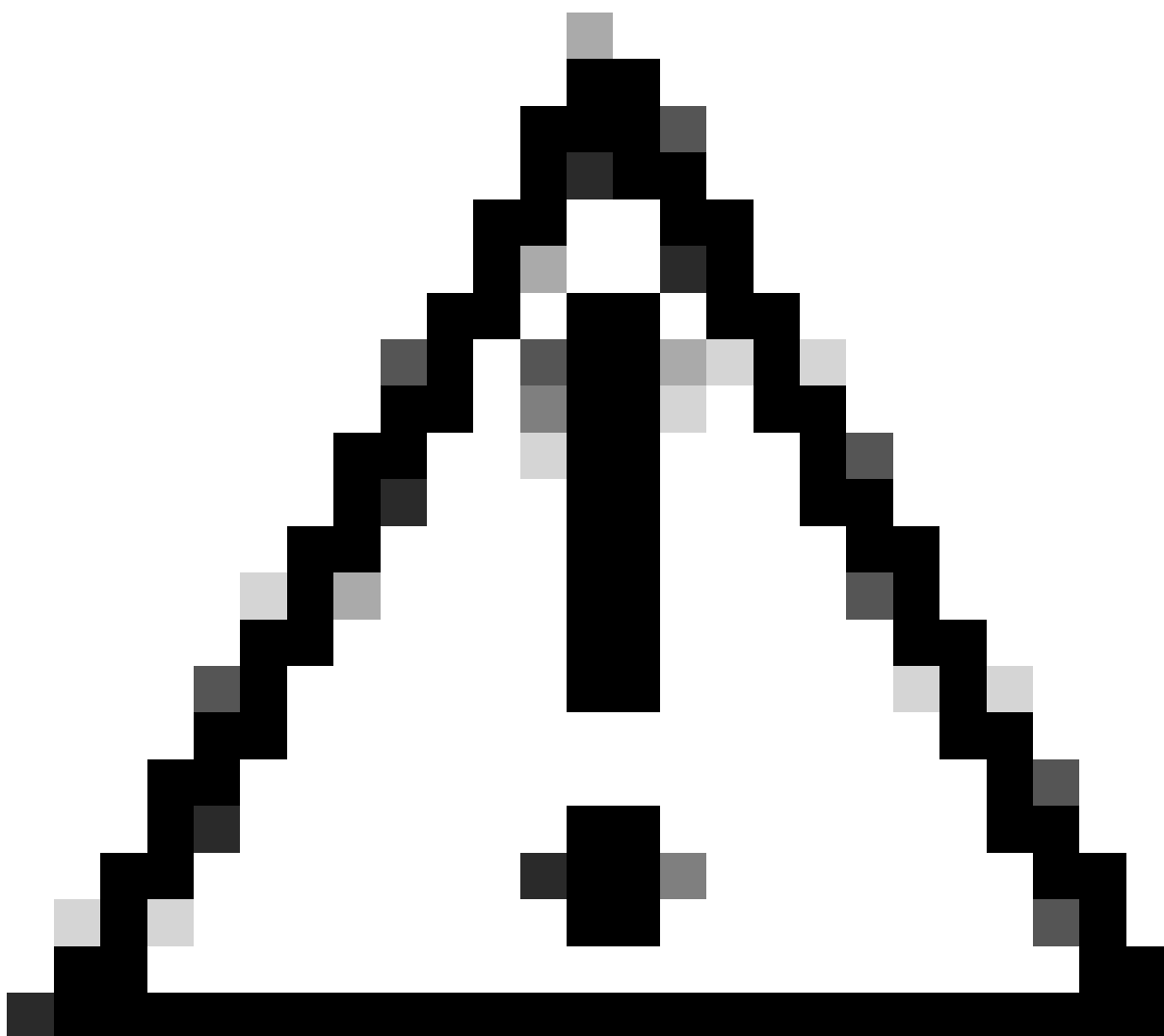


Let op: de opdrachten die worden gegeven in het tekstvak Opdrachten en configuraties uitvoeren, geven geen resultaten terug. Je ziet alleen of de opdracht succesvol is uitgevoerd of niet. Dit is de reden waarom de opdracht die de USM-gebruikers weergeeft geen resultaten in de vorige screenshot. Dit betekent dat u met succes een USM-gebruiker kunt maken vanuit dit gedeelte van de GUI van het eindpunt, maar om te controleren of de gebruiker is gemaakt, moet u SSH naar het apparaat sturen.

Voor het configureren van SNMPv2c is het niet nodig om een gebruiker te maken. Authenticatie vindt plaats met behulp van de community-naam (ook wel community-string genoemd) die is geconfigureerd op het eindpunt. De SNMP-agent van het eindpunt, die al op het apparaat bestaat, reageert op verzoeken die overeenkomen met de geconfigureerde communitynaam op het apparaat. Als een SNMP-verzoek van een beheersysteem geen overeenkomende communitynaam bevat (hoofdlettergevoelig), wordt het bericht verwijderd en verzendt de SNMP-agent in het videoapparaat geen reactie.

SNMPv3 vereist echter de configuratie van een USM-gebruiker om de verificatie succesvol te laten zijn. Hiervoor zijn Network SNMP USM User commando's nodig. Dit kan gebeuren door SSH

rechtstreeks naar het apparaat te sturen of door de GUI van het apparaat te gebruiken onder het gedeelte Developer API. Als alternatief kan de Webex API worden gebruikt.



Let op: U moet beslissen of u SNMPv2, SNMPv3 of beide wilt inschakelen. SNMPv1 wordt niet ondersteund op Cisco-eindpunten. Elke poging om SNMPv1 te gebruiken zal mislukken.

In dit document worden de SNMPv2- en SNMPv3-protocollen ingeschakeld en geconfigureerd in Control Hub, maar de USM-gebruiker die nodig is voor SNMP3-verificatie wordt geconfigureerd via SSH.

SNMPv2c-modus inschakelen in Control Hub

Navigeer naar admin.webex.com en log in met uw beheerdersreferenties. Het is aan te raden om een volledige admin te zijn. Navigeer naar Apparaten onder Beheer sectie aan de linkerkant van de gebruikersinterface. Selecteer onder het tabblad Apparaten het apparaat dat u wilt configureren. In dit voorbeeld wordt een Cisco Room Kit Pro gebruikt.

webex Control Hub

AI-powered smart search

Devices

Find devices by status, type, and more

60 devices

Add device

Filter by: Online (39) Expired (5) Offline (9) Issues (7) Offline (Deep SI...)

Select one or more devices for bulk actions

Type	Product	Status	Platform	Belongs to
Rooms & Desks	Cisco Webex DX80	Offline		
Rooms & Desks	Cisco Room Kit	Issues		
Rooms & Desks	Cisco Room Kit Pro	Online		
Rooms & Desks	Cisco Desk	Issues		
Rooms & Desks	Cisco Room Kit Mini	Online		
Rooms & Desks	Cisco Room Bar Pro	Issues		
Rooms & Desks	Cisco Webex Share	Online		

Sectie Apparaten van besturingshub

Navigeer onder de apparaatgegevens op de nieuwe pagina Control Hub die wordt geopend naar de sectie Configurations en klik op All Configurations:

webex Control Hub

AI-powered smart search

Cisco Room ...

Actions

SIP address

None Lines

Software

Cisco Platform Stable Channel

Release Version

Alerts

Not Monitored

No alert rules set for this device.

Create Rule

Tags

Configurations

All configurations 1195

Configuration templates

Digital signage Disabled

Navigator persistent web app Disabled

Macros 1

Support

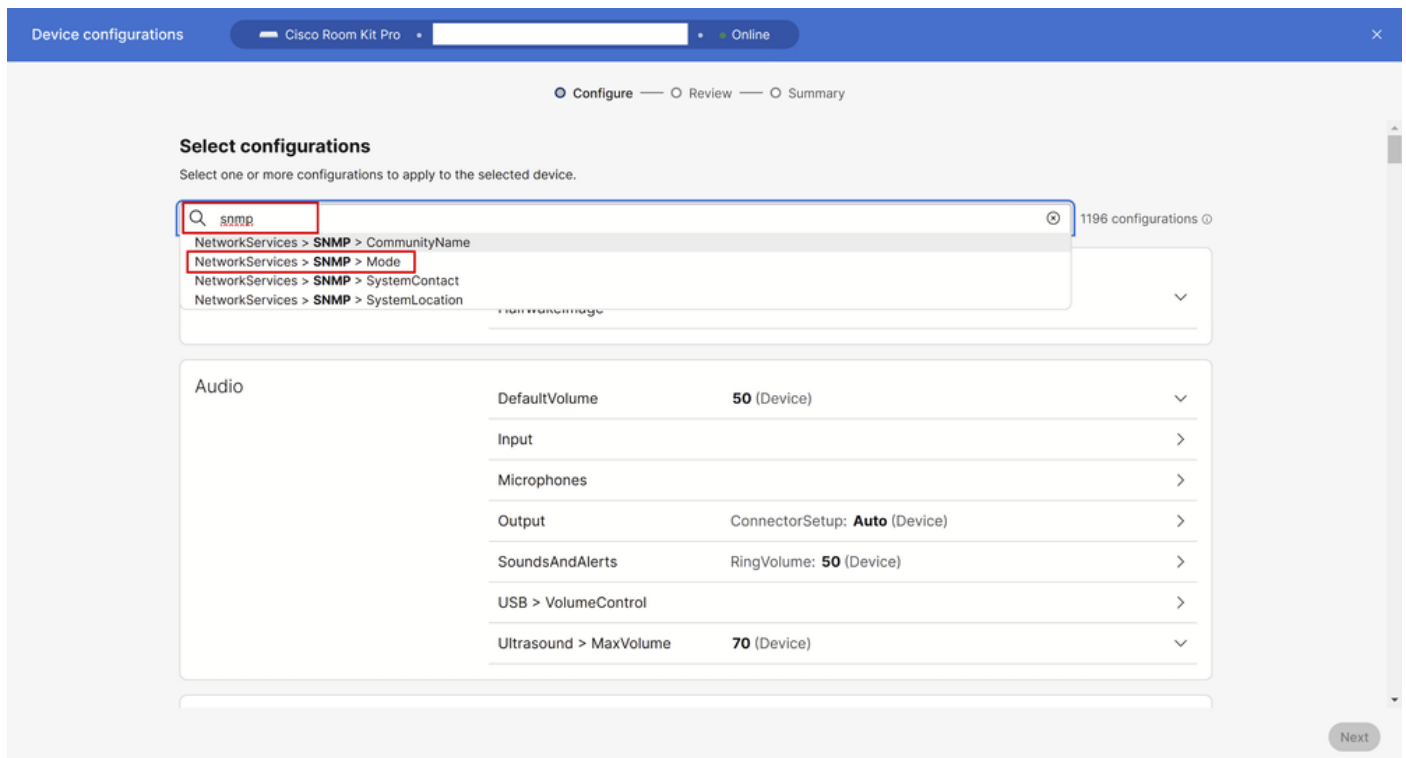
Device Logs Manage

Remote access Available Open

Local Device Controls Launch

Apparaatgegevens van de Control Hub voor Room Kit Pro

Typ in de zoekbalk snmp en selecteer NetworkServices > SNMP > Modus:

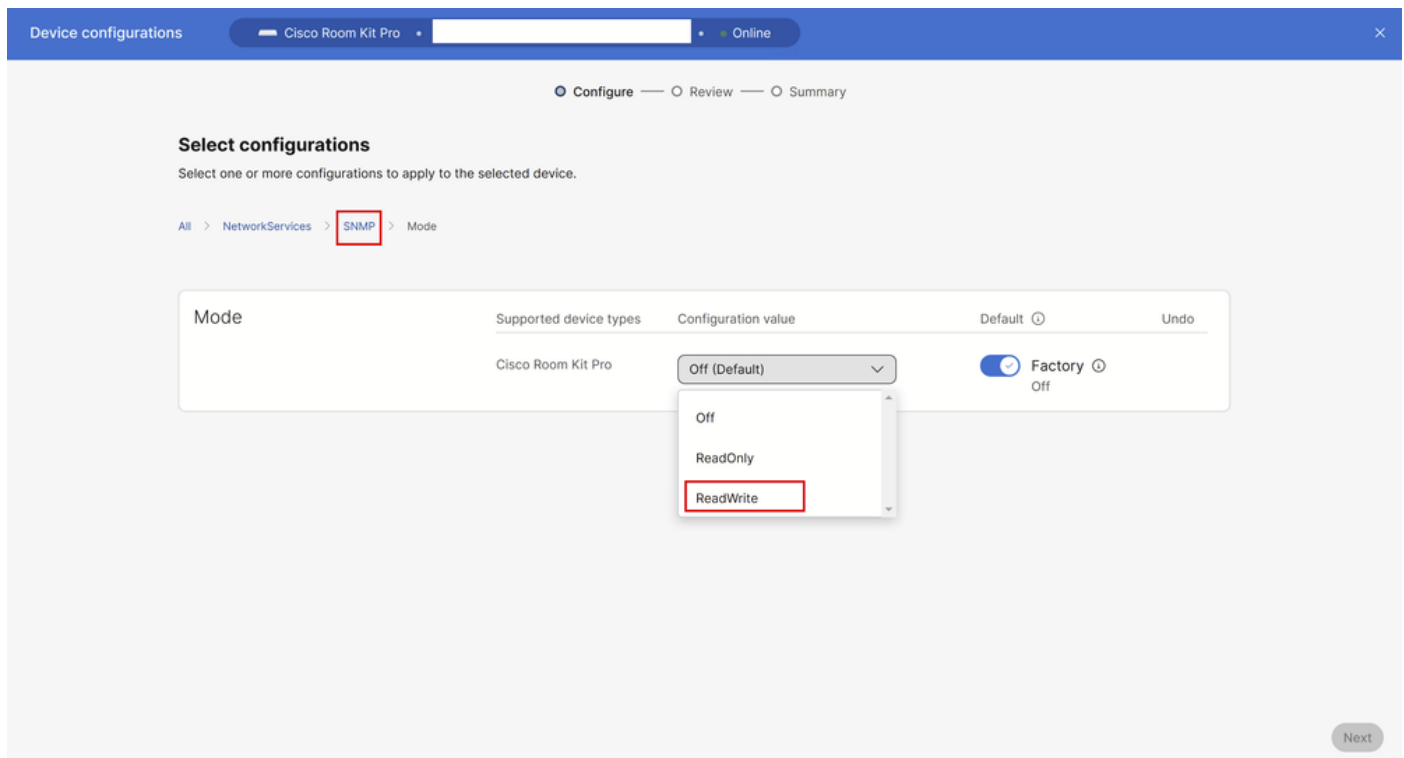


Venster Alle configuraties van Control Hub

Selecteer de modus die u in uw omgeving wilt inschakelen. Er zijn drie opties beschikbaar:

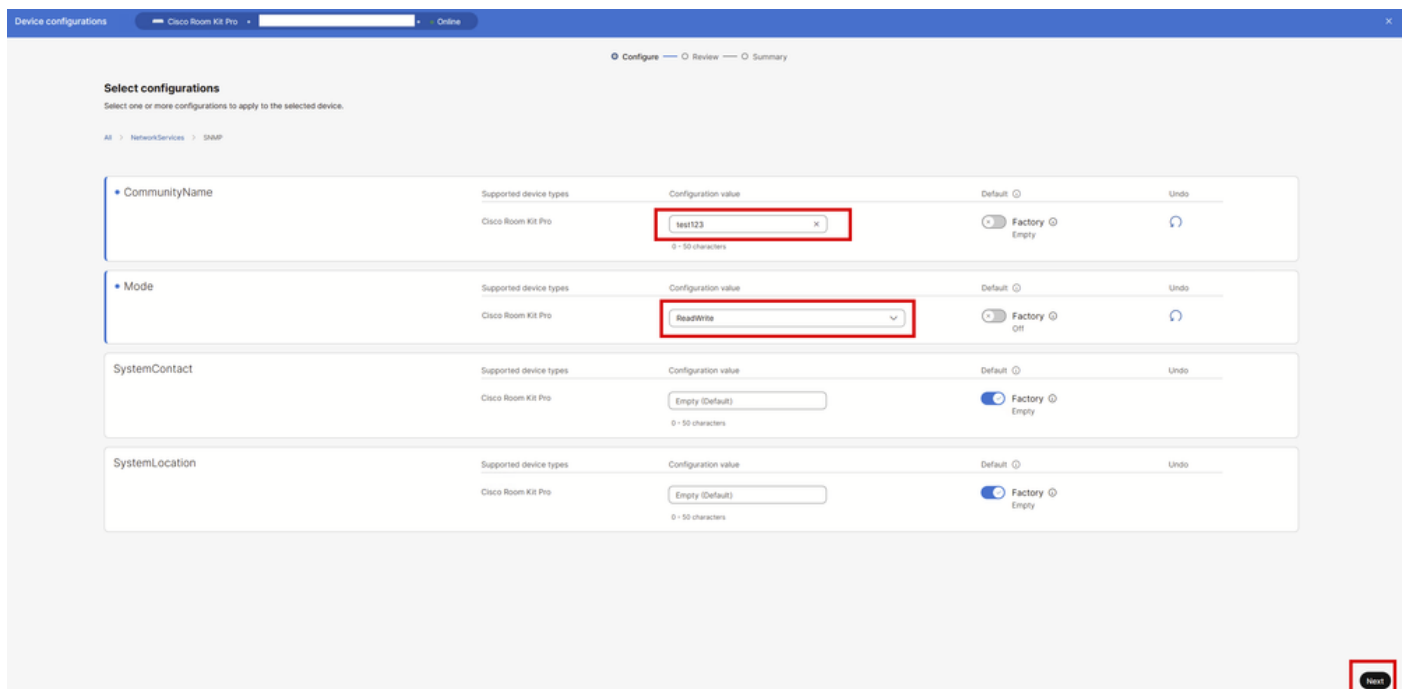
1. Uit: Schakel de SNMP-netwerkservice uit.
2. Alleen-lezen: schakel de SNMP-netwerkservice alleen in voor query's.
3. ReadWrite: Schakel de SNMP-netwerkservice in voor zowel query's als opdrachten.

In dit voorbeeld is ReadWrite geselecteerd. Klik vervolgens op SNMP in het gedeelte Instellingen navigatie, zoals te zien is in de afbeelding. Dit brengt u een stap terug in de instellingen en u kunt alle SNMP-gerelateerde instellingen zien die via Control Hub op het apparaat kunnen worden geconfigureerd:



Instelling SNMP-modus onder Alle configuraties in Control Hub

Nadat u op SNMP hebt geklikt, worden alle beschikbare SNMP-opties weergegeven, zoals te zien is in deze afbeelding. Om SNMPv2 succesvol in te stellen, moet een Community Name worden ingesteld. De naam van de community wordt gebruikt voor verificatie tussen de SNMP-server en de SNMP-agent die op het eindpunt bestaat. De Community Name is ingesteld om voor dit voorbeeld 123 te testen. Klik rechtsonder op Volgende.



SNMP-instellingen onder Alle configuraties in Control Hub

Controleer de apparaatconfiguraties en klik rechtsonder op Toepassen:

Device configurations Cisco Room Kit Pro Online

Configure Review Summary

Review configurations

Review selected configurations.

Configuration	Value	Actions
NetworkServices > SNMP > CommunityName	test1234 → test123	Edit Copy
NetworkServices > SNMP > Mode	Off → ReadWrite	Edit Copy

Previous **Apply**

Configuraties controleren voordat u de wijzigingen toepast

Controleer of de configuratiewijzigingen met succes zijn toegepast. Klik vervolgens op Sluiten.

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	test123	✓
NetworkServices > SNMP > Mode	ReadWrite	✓

Close

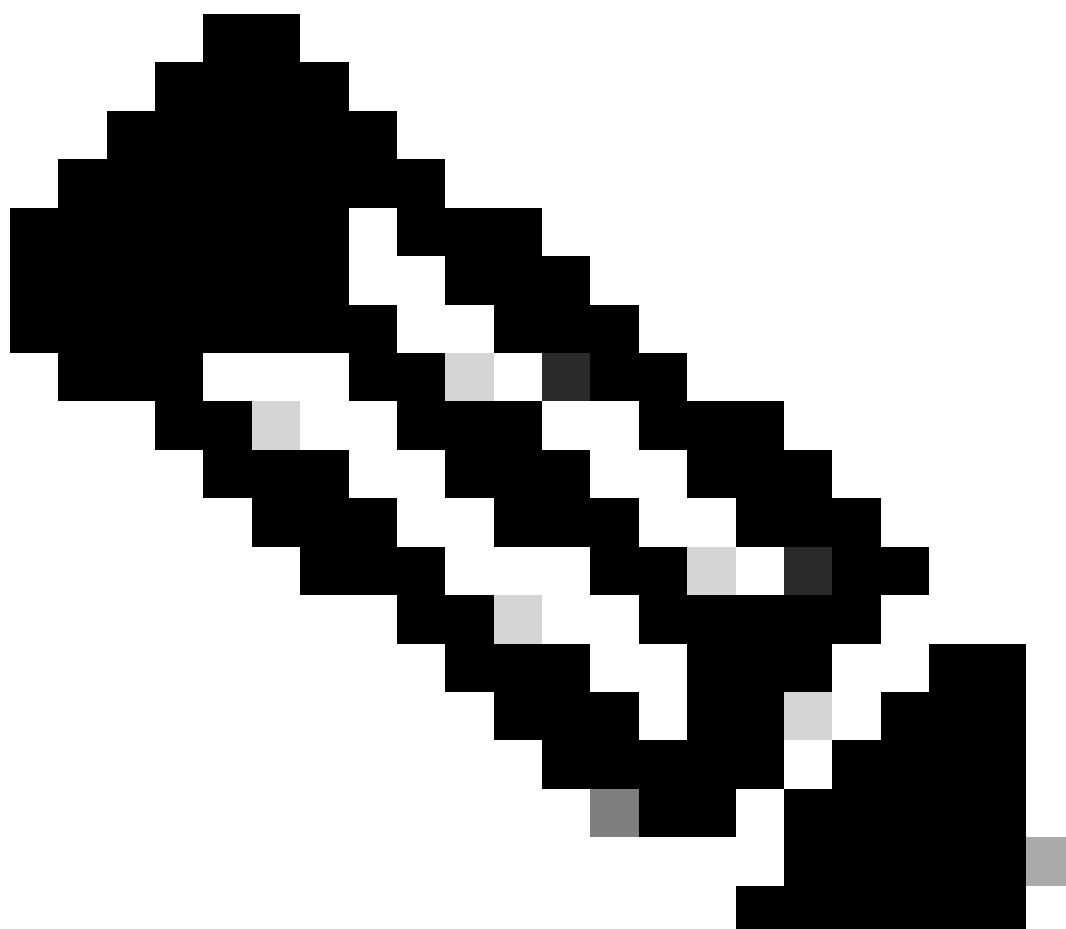
Eindpuntconfiguraties met succes toegepast in Control Hub

In dit stadium is SNMPv2c met succes ingeschakeld op het eindpunt en is de naam van de community ingesteld.

SNMPv3-modus inschakelen in Control Hub

SNMPv3 biedt meer beveiliging en vereist een andere configuratie op het eindpunt in vergelijking met SNMPv2c. Navigeer naar Apparaten onder Beheer sectie in Control Hub. Ga naar het tabblad Apparaten en selecteer een van de eindpunten die u met SNMPv3 wilt configureren. In dit voorbeeld wordt een Cisco Room Bar Pro gebruikt.

Navigeer onder de apparaatgegevens naar de sectie Configuraties en klik op Alle configuraties. De pagina Apparaatconfiguraties wordt geopend. Typ snmp in de zoekbalk en selecteer NetworkServices > SNMP > Modus. In dit voorbeeld is de SNMP-modus ingesteld op ReadWrite. Klik op SNMP om alle configureerbare SNMP-instellingen op het apparaat weer te geven.



Opmerking: alle stappen die tot nu toe voor SNMPv3 zijn genoemd, zijn al beschreven toen SNMPv2c in een eerder voorbeeld werd geconfigureerd. Hierdoor wordt er geen screenshot van de stappen gegeven. Raadpleeg de sectie SNMPv2c-modus inschakelen in Control Hub als u twijfelt over hoe u door de instellingen van Control Hub kunt navigeren.

Als u alleen SNMPv3 wilt ondersteunen, moet u de communitynaam instellen als een lege

tekenreeks omgeven door aanhalingstekens: "".

Device configurations

Cisco Room Bar Pro

Issues

Configure Review Summary

CommunityName

Supported device types Configuration value Default Undo

Cisco Room Bar Pro

Factory Empty

0 - 50 characters

Mode

Supported device types Configuration value Default Undo

Cisco Room Bar Pro

ReadWrite

Factory Off

SystemContact

Supported device types Configuration value Default Undo

Cisco Room Bar Pro

Empty (Default)

Factory Empty

0 - 50 characters

SystemLocation

Supported device types Configuration value Default Undo

Cisco Room Bar Pro

Empty (Default)

Factory Empty

Next

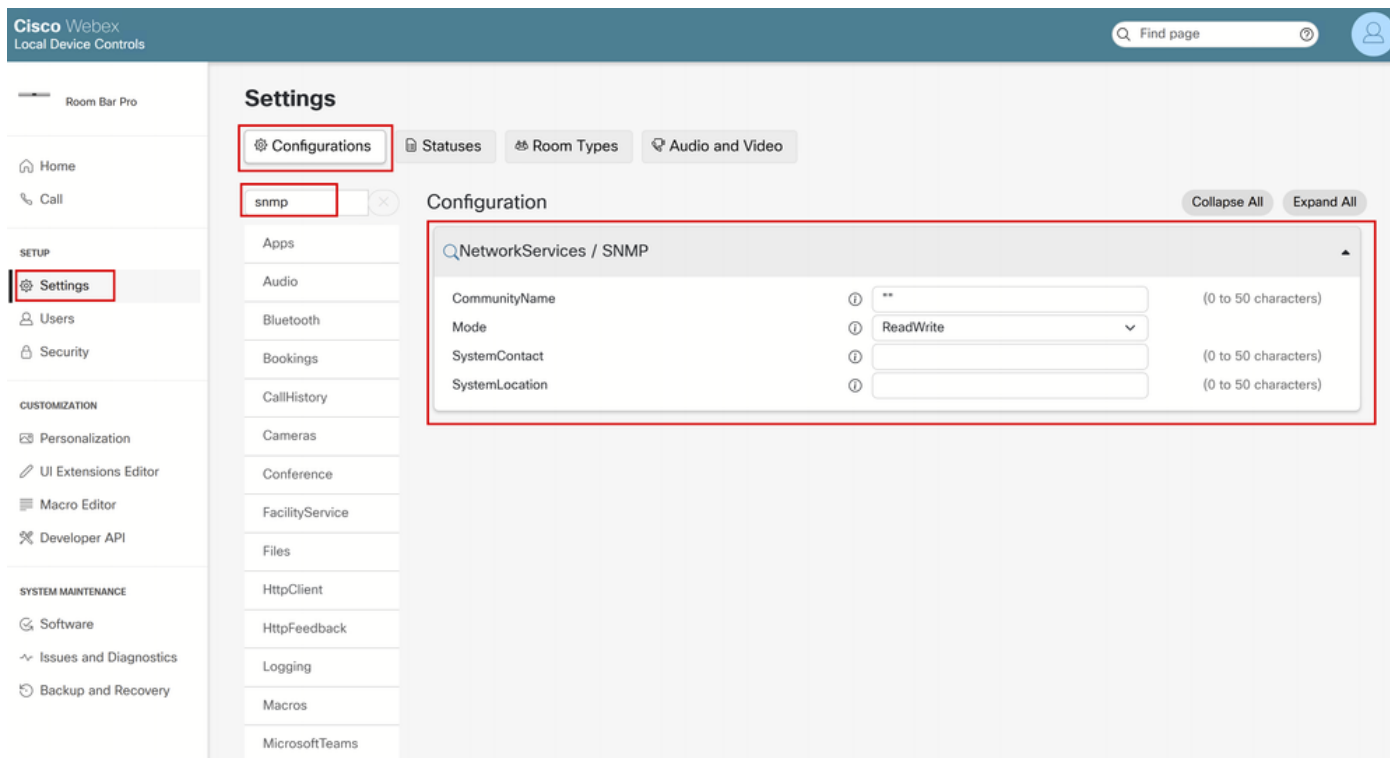
SNMP-instellingen onder Alle configuraties in Control Hub

Klik op Volgende, bekijk de configuratiewijzigingen en klik op Toepassen. Klik op Sluiten om de apparaatconfiguratiepagina te sluiten.

Hiermee wordt de configuratie afgesloten die kan worden uitgevoerd in Control Hub. In dit stadium is alleen SNMPv3 ingeschakeld.

Hoe ziet de SNMP-configuratie eruit in de Endpoint GUI

Dezelfde configuraties kunnen worden uitgevoerd vanaf de GUI van het apparaat. Open een browsertabblad en typ het IP-adres van het eindpunt (u moet zich in hetzelfde netwerk bevinden als het eindpunt). Log in als een admin-gebruiker en navigeer in de endpoint GUI naar Instellingen onder de SETUP-sectie. Blijf op het tabblad Configuraties en typ snmp op de zoekbalk voor instellingen. Deze afbeelding laat zien hoe de SNMP-instellingen worden weergegeven voor de SNMPv3-configuratie die is uitgevoerd op de Room Bar Pro in de vorige sectie:



SNMPv3-configuratie op de gebruikersinterface van het eindpunt

De USM-gebruiker configureren voor SNMPv3

Om SNMPv3 te kunnen gebruiken, moet u een USM-gebruiker maken. De beschikbare opdrachten voor het uitvoeren van deze actie vindt u [hier](#) in de documentatie van het Room OS. Gebruik SSH om verbinding te maken met het apparaat. Hiervoor heb je een admin account nodig op het apparaat. Als dat niet het geval is, moet u een beheerdersaccount aanmaken. Deze sectie gaat door dit hele proces.

Navigeer naar Apparaten onder Beheer sectie in Control Hub. Blijf onder het tabblad Apparaten en selecteer een van uw eindpunten waarvoor u een beheerdersgebruiker wilt maken. In dit voorbeeld wordt een Cisco Room Bar Pro gebruikt.

Navigeer onder de apparaatgegevens naar de sectie Ondersteuning en klik op Besturingselementen lokaal apparaat (u moet zich in hetzelfde netwerk bevinden als het eindpunt om dit te laten werken). De GUI van het apparaat wordt geopend. Navigeer naar Gebruikers onder het gedeelte SETUP en klik op Gebruiker maken.

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 ¹	Audit ¹	RoomControl ¹	Integrator ¹	User ¹
admin	Inactive	✓	✓			✓
	Active	✓	✓	✓	✓	✓
touchpanel	Active	✓	✓	✓	✓	✓

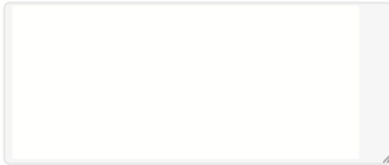
Remote Support

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



Gebruikerssectie in de gebruikersinterface van het eindpunt

Geef een gebruikersnaam en wachtwoord op (wachtwoord). Zorg ervoor dat de gebruiker volledige beheerdersrechten heeft en actief is:

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 ☒ Admin¹

☒ Audit¹

☒ RoomControl¹

☒ Integrator¹

☒ User¹

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... ¹

Confirm passphrase

Create User

Een gebruiker maken op basis van de GUI van Endpoint

Controleer of de gebruiker is gemaakt en actief is vanaf de pagina Gebruikers:

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	Admin①	Audit①	RoomControl①	Integrator①	User①
admin	Inactive	✓	✓			✓
	Active	✓	✓	✓	✓	✓
testuser1	Active	✓	✓	✓	✓	✓
touchpanel	Active	✓	✓	✓	✓	✓

Remote Support

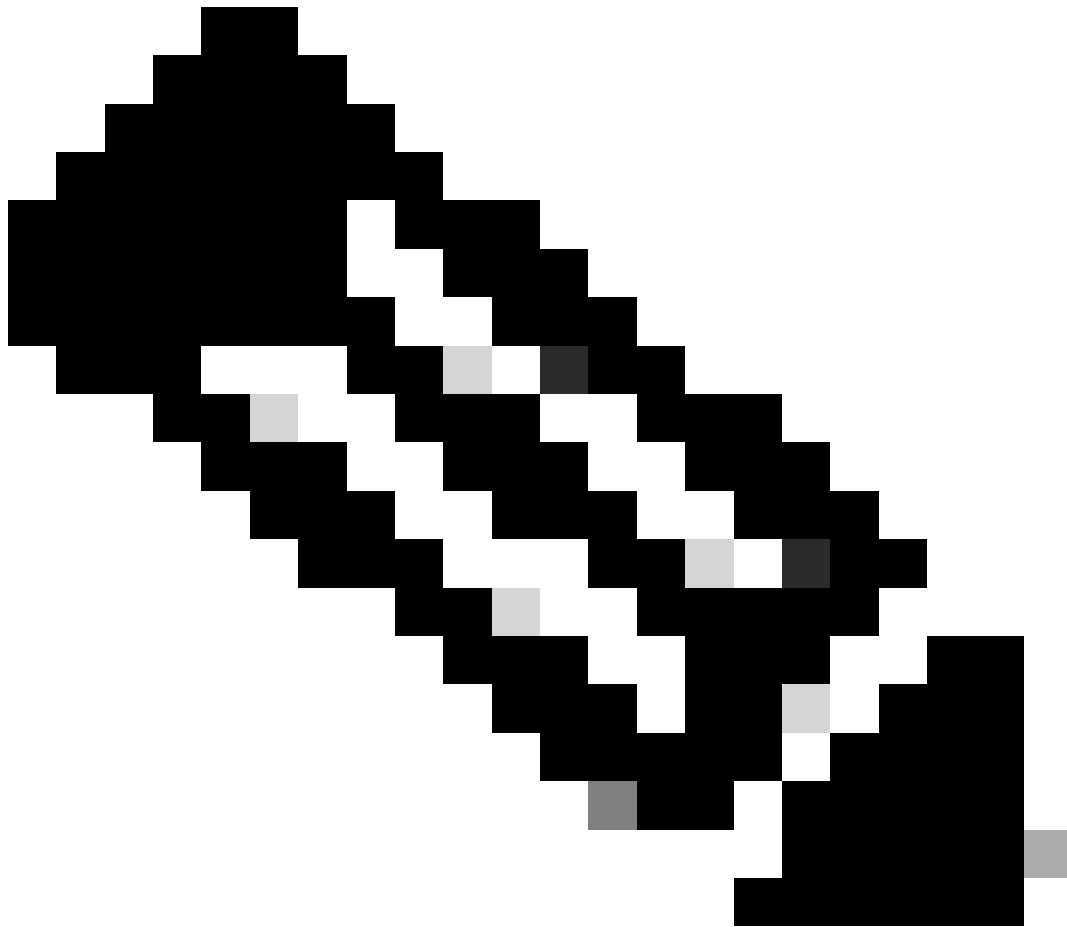
The Remote Support User is a special user account that has wider access rights than regular admin accounts. It is used by Cisco technical support to log in to the device to troubleshoot system issues, such as problems with the device's operating system.

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

This user is valid until

Token

Nieuwe gebruiker gemaakt en vermeld onder andere gebruikers



Opmerking: bij de eerste SSH-inlogpoging met een nieuw aangemaakte gebruiker wordt u gevraagd uw wachtwoord te wijzigen. U ziet een prompt die lijkt op:

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

Wachtwoord wijzigen wanneer SSH voor de eerste keer

Zodra het wachtwoord is gewijzigd, wordt de verbinding onmiddellijk verbroken en moet u een nieuwe SSH-verbinding starten.

Zodra de admin-gebruiker met succes is gemaakt, gebruikt u een SSH-client van uw keuze en maakt u verbinding met het eindpunt. Log in met de beheerdersreferenties. Dit is de prompt die je

ziet:

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

Succesvolle inlogpoging via SSH naar het eindpunt

Gebruik de opdracht Network SNMP USM User Add zoals beschreven in [dit](#) artikel. Voor deze demonstratie wordt de volgende opdracht gebruikt:

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

Het resultaat van deze opdracht, wanneer succesvol, is:

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

USM-gebruikerscreatie via SSH

Om de opdracht zonder fouten uit te voeren, moet u zich houden aan bepaalde regels die worden beschreven in de opdrachtdocumentatie die in deze [link wordt](#) gedeeld. Gemakshalve worden de huidige vereisten op het moment van schrijven van dit document voor deze opdracht in deze afbeelding geplakt, maar u moet ervoor zorgen dat u naar deze [link](#) verwijst bij het maken van uw gebruiker. Aan het einde van de afbeelding ziet u de exacte syntaxis van de opdracht.

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

USM User Creation Command Syntax van xAPI-documentatie



Waarschuwing: Als er een typefout is of als er niet aan een vereiste wordt voldaan, retourneert de opdracht een fout en wordt de gebruiker niet gemaakt. Een voorbeeld wordt gegeven, waarbij in plaats van het verstrekken van een Privacy Password met ten minste 8 karakters, een korter 7-karakters wachtwoord wordt gegeven:

```
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.

Maken van USM-gebruiker mislukt vanwege kort privacywachtwoord

U kunt testen of de gebruiker is gemaakt met de opdracht Network SNMP USM-gebruikerslijst. Deze opdracht geeft alle USM-gebruikers weer die op het apparaat zijn opgeslagen:

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

```
OK
```

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

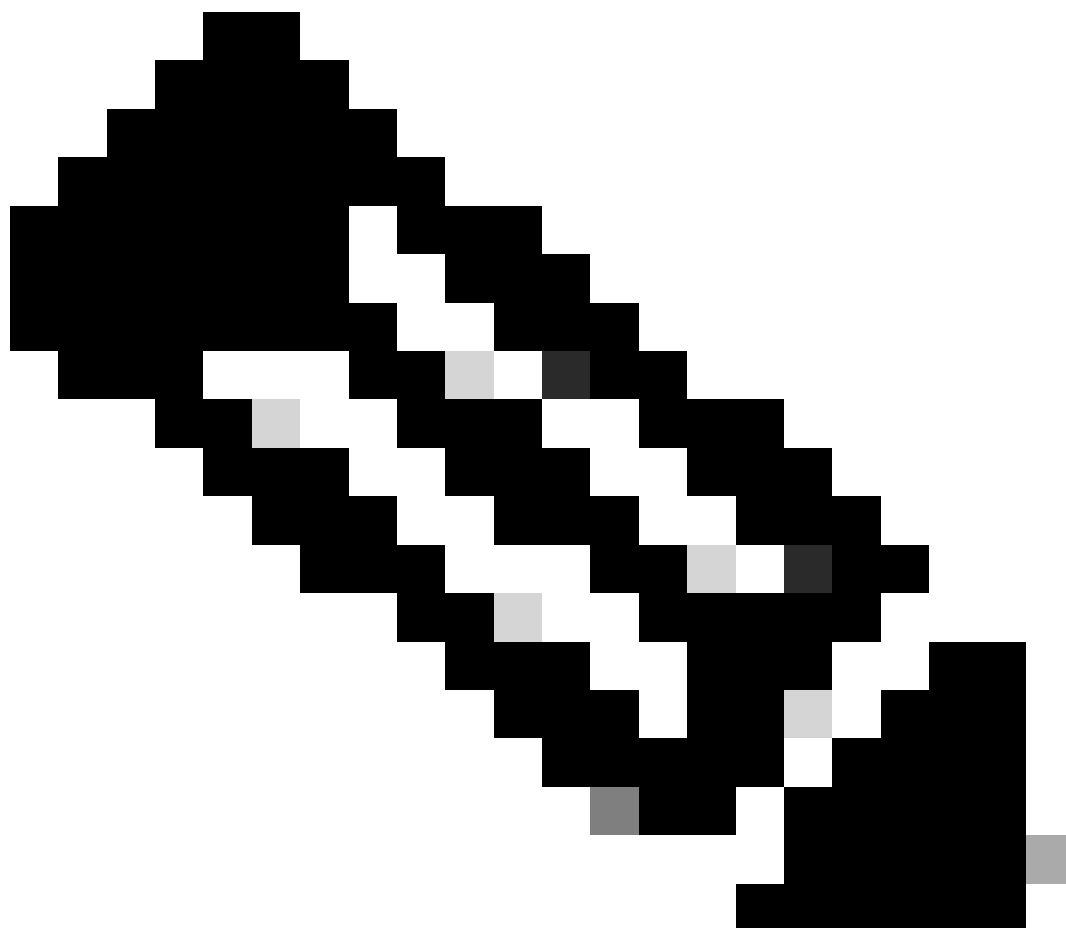
```
*r UserListResult User 1 AuthenticationProtocol: "SHA-256"
```

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

```
** end
```

Netwerk SNMP USM-gebruikerslijst, opdracht gebruikt om het maken van de gebruiker te bevestigen

In dit stadium is bevestigd dat de gebruikerssitaras met succes zijn gemaakt. De SNMPv3-configuratie is voltooid.



Opmerking: de USM-gebruikerssitaras zijn niet zichtbaar in de GUI van het eindpunt onder de sectie Gebruikers. Dit wordt verwacht.

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
admin	Inactive	✓	✓			✓
am test	Active	✓	✓	✓	✓	✓
testuser1	Active	✓	✓	✓	✓	✓
touchpanel	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

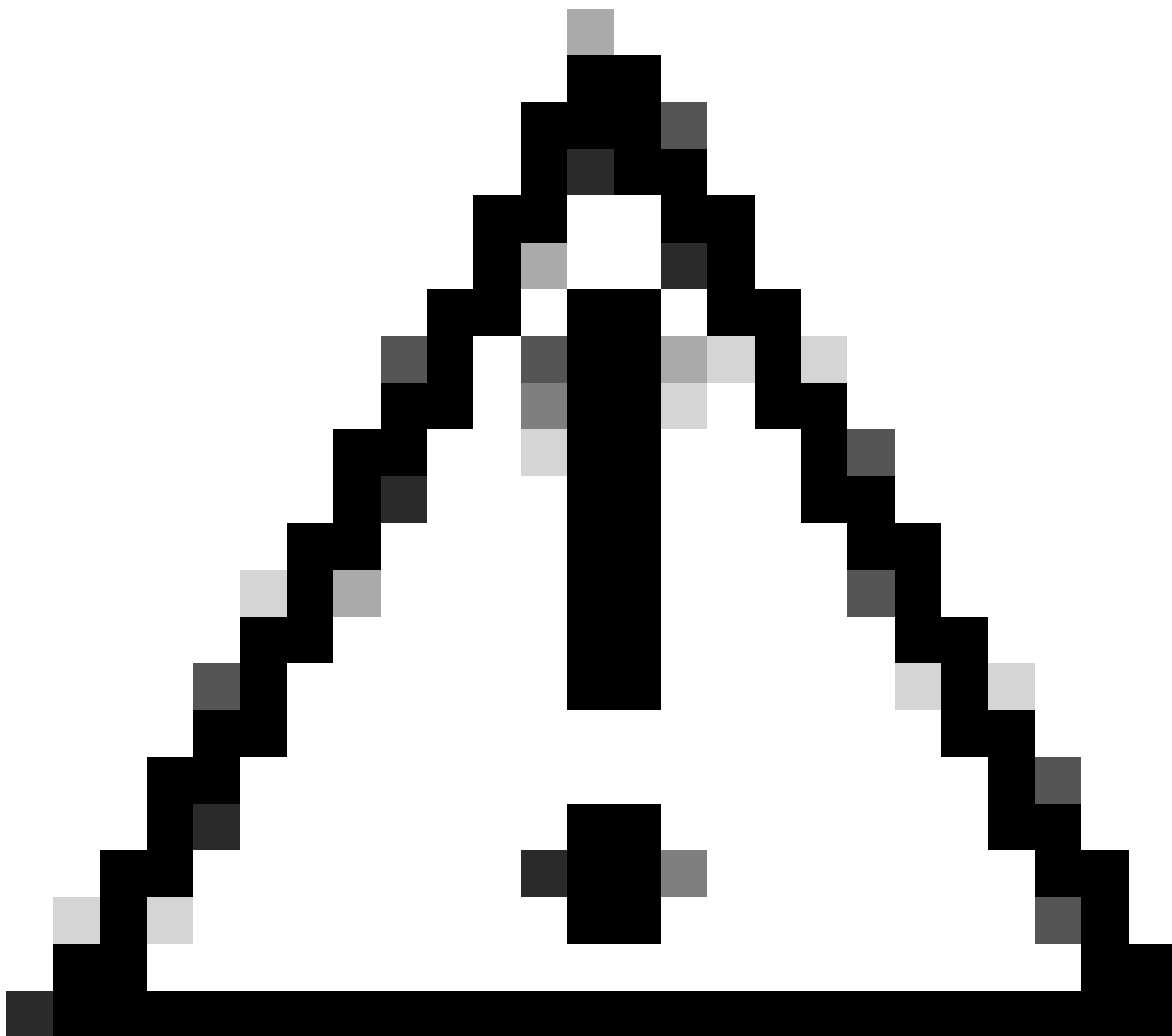
Token

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

USM-gebruikers zijn niet zichtbaar onder Gebruikers in de gebruikersinterface van Endpoint

SNMPv2c- en SNMPv3-configuratie testen

In dit stadium kunt u doorgaan met het testen van de SNMPv2c- en/of SNMPv3-configuratie met uw Network Management System (NMS). Voor dit artikel bevat de laboratoriumconfiguratie geen NMS- of SNMP-server waarop een SNMP-service wordt uitgevoerd. Om de configuratie te testen, wordt het hulpprogramma snmpwalk gebruikt. Dit hulpprogramma is geïnstalleerd op een Linux-server.

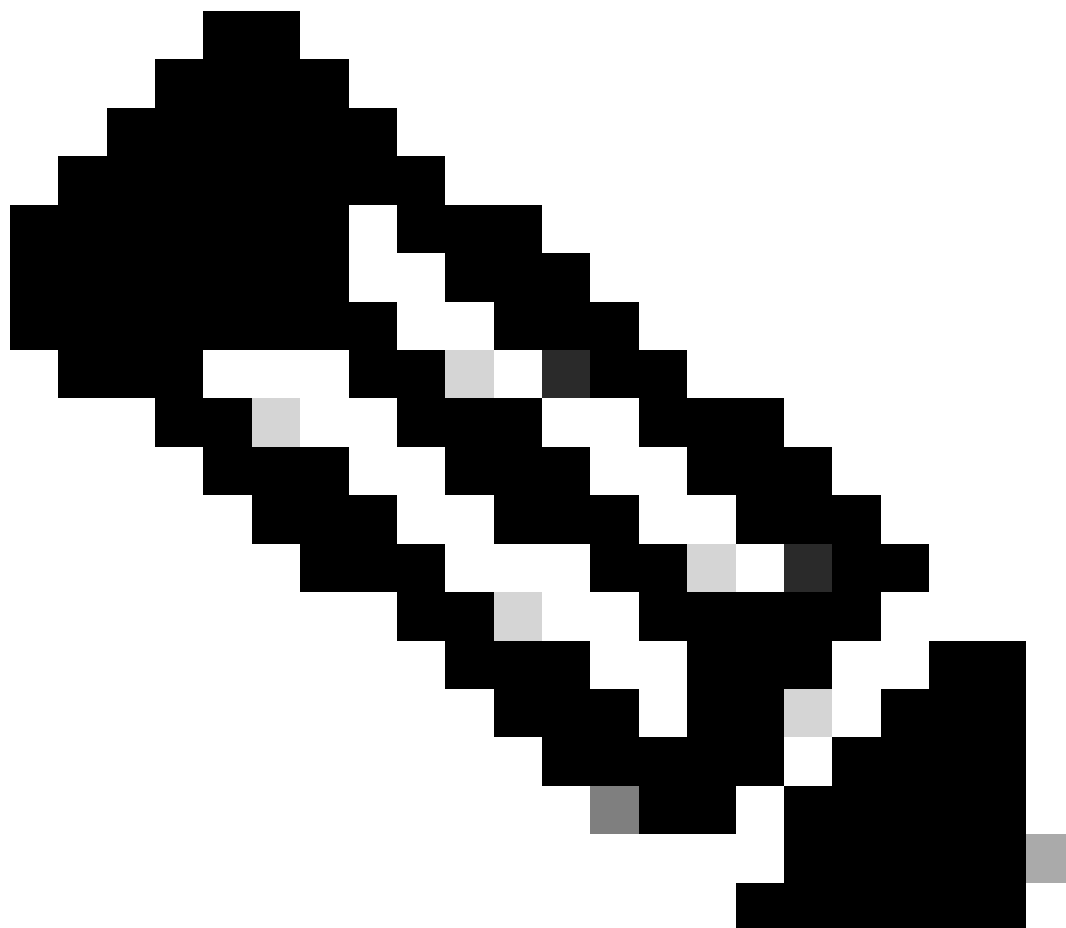


Let op: Snapwalk is geen aanbevolen tool voor het testen van de SNMP-configuratie op uw samenwerkingseindpunten. Het wordt niet ondersteund door TAC-ingenieurs en u moet bekend zijn met het gebruik van de tool voordat u doorgaat met testen. In plaats van snmpwalk, kunt u elke andere SNMP-tool of uw NMS gebruiken om uw configuratie te testen. Snapwalk wordt in dit artikel alleen als voorbeeld gebruikt (er is een tool nodig om de configuratie te testen voor demonstratiedoeleinden) en er is geen verbintenis of promotie met betrekking tot het gebruik ervan.

De installatie van de snapwalk maakt geen deel uit van deze gids en wordt weggelaten. Afhankelijk van het besturingssysteem (OS) van de machine die u gebruikt voor het testen, kunnen de installatievereisten variëren. U moet werken aan het succesvol installeren voordat u het test.

Snapwalk is een tool die kan worden gebruikt voor het verifiëren van de SNMP-configuratie. Het voert een wandeling door de MiBs van het eindpunt uit en retourneert de beschikbare informatie. Cloud-geregistreerde eindpunten tonen 7 Object Identifiers (OID's):

- SNMPv2-MIB::sysDescr (gelezen),
 - SNMPv2-MIB::sysObjectID (gelezen),
 - DISMAN-EVENT-MIB::sysUpTimeInstance (gelezen),
 - SNMPv2-MIB::sysContact (lezen/schrijven),
 - SNMPv2-MIB::sysName (lezen/schrijven),
 - SNMPv2-MIB::sysLocation (lezen/schrijven),
 - SNMPv2-MIB::sysServices (gelezen).
-



Opmerking: de interne IP's die worden gebruikt voor de vermelde snapwalk-tests zijn privé-IP's en worden niet meer gebruikt. Het laboratorium dat voor deze handleiding is gebruikt, is uit bedrijf genomen en de apparaten zijn in de fabriek gereset.

Het Cisco Room Kit Pro-eindpunt is geconfigureerd met SNMPv2c. Authenticatie gebeurt met behulp van community strings. Geef deze opdracht op:

```
# '-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
```

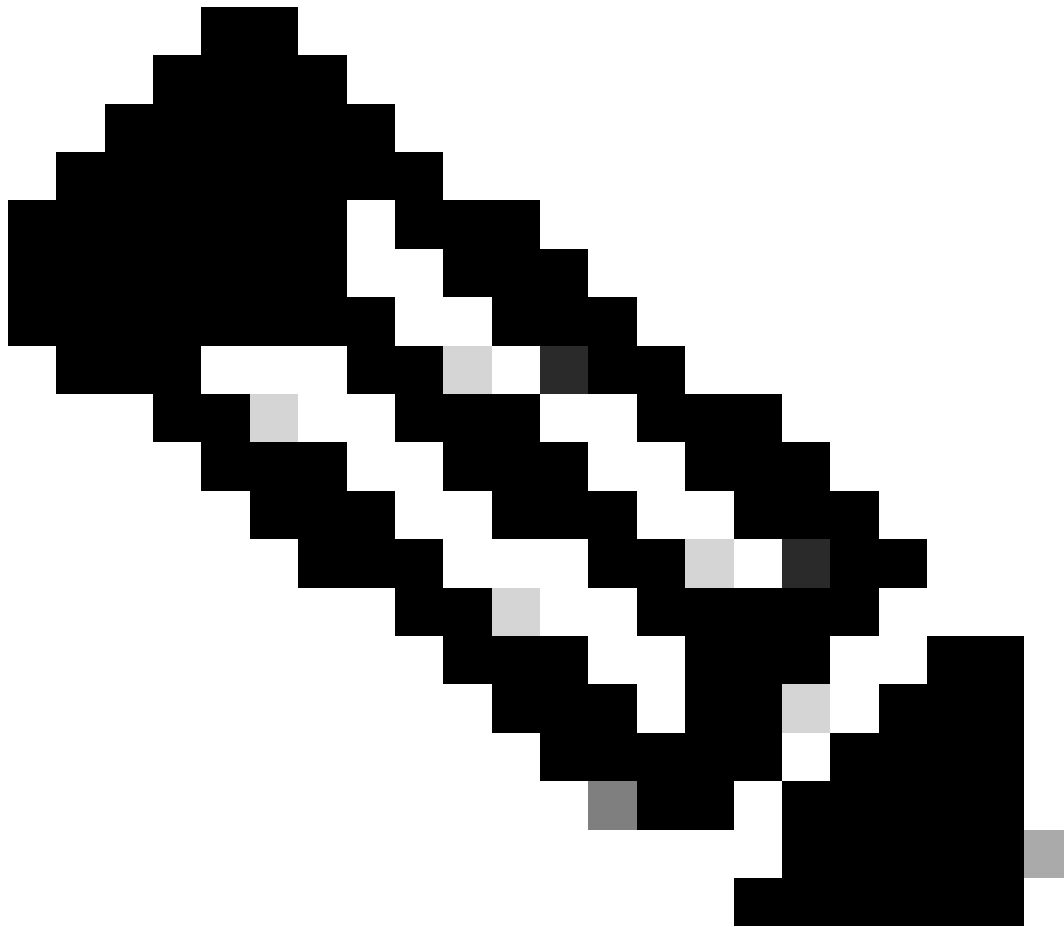
```
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco Codec
SoftW: ce11.26.1.5.53ff615d0d9
MCU: Cisco Codec Pro
Date: 2025-02-28
S/N: FD02706JG49"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.5596.150.6.4.1
iso.3.6.1.2.1.1.3.0 = Timeticks: (106770681) 12 days, 8:35:06.81
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = ""
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)
```

Snapwalk geeft 7 resultaten terug zoals verwacht. Er zijn drie MiB's die leeg zijn:

1. SNMPv2 -MIB::sysContact (lezen/schrijven), (ISO.3.6.1.2.1.1.4.0)
2. SNMPv2 -MIB::sysName (lezen/schrijven), (ISO.3.6.1.2.1.1.5.0)
3. SNMPv2 -MIB::sysLocation (lezen/schrijven), (ISO.3.6.1.2.1.1.6.0)

Er zijn drie xConfiguration-opdrachten die kunnen worden gebruikt om waarden in te stellen op deze MiBs. SSH naar het eindpunt en geef deze opdrachten:

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



Opmerking: In plaats van deze drie opdrachten te gebruiken, kunt u wijzigingen in deze instellingen uitvoeren vanuit Control Hub, vanuit de GUI voor het eindpunt of vanuit Webex API's.

Zodra de bovenstaande opdrachten zijn uitgegeven, gebruikt u snmpwalk opnieuw op hetzelfde eindpunt. U merkt dat de eerder lege MiBs worden gevuld met de waarden die worden opgegeven via de xConfiguration-opdrachten:

```
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 dit stadium wordt bevestigd dat de SNMPv2c-configuratie die op het Room Kit Pro-apparaat is gemaakt, operationeel is.

Het Cisco Room Bar Pro-eindpunt is geconfigureerd met SNMPv3. Voor SNMPv3 moet u ervoor zorgen dat u de juiste verificatie gebruikt. Er worden geen community strings gebruikt. In plaats daarvan gebruikt SNMPv3 gebruikersnamen en wachtwoorden.

```
# '-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 dit stadium wordt bevestigd dat de SNMPv3-configuratie die op het Room Bar Pro-apparaat is gemaakt, operationeel is.

Kan een eindpunt zowel SNMPv2c als SNMPv3 tegelijkertijd actief hebben?

Ja, het is mogelijk. Tijdens de SNMP-configuratie moet u echter een communitynaam instellen om SNMPv2c-verificatie te kunnen hebben. Voor deze test wordt de Room Bar Pro uit eerdere voorbeelden gebruikt. De huidige configuratie in de sectie Control Hub All Configurations van het eindpunt is:

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		☒ Factory ⓘ Empty	
		0 - 50 characters		

Mode	Supported device types	Configuration value	Default ⓘ	Undo
	Cisco Room Bar Pro	ReadWrite	☒ Factory ⓘ Off	

SNMP-configuraties van het eindpunt in Control Hub

Merk op dat de naam van de community niet leeg is. Er zijn twee aanhalingstekens, die aangeven dat de naam van de community een lege tekenreeks is. U kunt de SNMP-ondersteuning beperken tot versie 3 door de SNMP CommunityName van NetworkServices in te stellen op een lege tekenreeks ("). U moet deze tekenreeks vervangen door een communitynaam, bijvoorbeeld test bothSNMPv2_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	testbothSNMPv2_v3	☒ Factory ⓘ Empty	
		0 - 50 characters		

Mode	Supported device types	Configuration value	Default ⓘ	Undo
	Cisco Room Bar Pro	ReadWrite	☒ Factory ⓘ Off	

Communitynaam voor SNMPv2c toevoegen in Configuratie-instellingen van Control Hub Endpoint

Het is al bevestigd dat SNMPv3 werkt aan de Room Bar Pro. Snapwalk wordt gebruikt om te testen of SNMPv2c ook werkt, na het instellen van de communitynaam:

```
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)
```

Meerdere eindpunten kunnen worden geconfigureerd via Control Hub met SNMP

Ja, het is mogelijk om meerdere apparaten tegelijk te configureren in Control Hub. Dit [artikel](#) geeft informatie over hoe u het stap voor stap kunt uitvoeren onder de sectie Meerdere apparaten configureren.

Belangrijke details om te onthouden

- Er zijn alleen specifieke MiB's beschikbaar. Het aantal beschikbare MiBs is beperkt door het ontwerp van het engineeringteam dat de eindpunten ontwerpt. MiBs kunnen niet worden uitgebreid of verbeterd om meer informatie te bieden.
- SNMPv2c authenticceert met behulp van Community Name (ook wel Community String genoemd), terwijl SNMPv3 authenticceert met behulp van gebruikersnaam en wachtwoord en ook codering biedt. Zorg er bij het testen voor dat u de juiste verificatiemethode gebruikt (met snmpwalk of een andere tool/NMS) voor het protocol dat u hebt geconfigureerd.
- Authenticatie en privacy staan altijd op SNMPv3. De eindpunten ondersteunen alleen het authPriv-beveiligingsniveau en het privacyprotocol is altijd Advanced Encryption Standard (AES).
- SNMPv3 wordt alleen ondersteund met USM-opties (User-based Security Model). Er is geen ondersteuning voor SMNPv3 via TLS.
- USM-gebruikersopdrachten die worden gebruikt om gebruikers te configureren voor SNMP-verificatie hebben geen effect op SNMPv2c.
- De instelling SNMP CommunityName op eindpunten heeft geen effect op de SNMPv3-configuratie.
- SNMP CommunityName is hoofdlettergevoelig.
- U kunt de SNMP-ondersteuning beperken tot alleen v3 door de SNMP CommunityName van NetworkServices in te stellen op een lege tekenreeks ("").
- SNMPv1 wordt niet ondersteund.
- Voor zowel SNMPv2c als SNMPv3 stellen eindpunten dezelfde object-id's (OID's) bloot.
- Voor SNMPv3 moet het verificatieprotocol zich in de SHA-2-familie bevinden (MD en SHA-1 worden niet ondersteund). Als dit niet het geval is, kunnen SNMP-verzoeken niet worden geverifieerd en blijven ze onbeantwoord.
- Het privacywachtwoord wordt opgeslagen als een gelokaliseerde hashwaarde (AES-128) op het apparaat. Als een privacywachtwoord niet expliciet in deze parameter is ingesteld, is dit hetzelfde als het verificatiewachtwoord (met een hashfunctie zoals opgegeven in de parameter Authentication Protocol).
- Wachtwoorden/wachtwoordgroepen en gebruikersnamen moeten binnen specifieke lengtegrenzen vallen. De USM-gebruikersnaam moet bijvoorbeeld maximaal 32 tekens bevatten en het verificatiewachtwoord moet minimaal 8 tekens en maximaal 255 tekens bevatten. Als niet aan deze vereisten wordt voldaan, kan de opdracht Network SNMP USM User Add de gebruiker niet aanmaken en wordt een fout geretourneerd.

Contact opnemen met TAC om een SNMP-probleem op een eindpunt op te lossen

Als de SNMP-configuratie van het eindpunt is voltooid, maar er een probleem is opgeworpen, moet u contact opnemen met TAC en deze informatie delen:

- Geef uw organisatie-ID op in Control Hub en het serienummer (SN) van het betreffende eindpunt.
- Beschrijf het scenario.
- Geef de SNMP-versie op die u probeert te configureren.
- Geef eventuele foutmeldingen op.
- Als er een probleem is met de configuratie van het apparaat, leg dan duidelijk uit in welke stap het configuratieproces is gestopt en geef screenshots. Deel de configuratieopdracht die een fout retourneert.
- Verzamel eindpuntlogs en upload ze op uw case.
- Deel het hulpprogramma\NMS of andere tool die wordt gebruikt om uw SNMP-configuratie te testen. Als u een hulpprogramma gebruikt om te testen met de SNMP-agent van de eindpunten, geeft u de volledige gebruikte opdracht op.

Gerelateerde informatie

[Room OS xAPI-documentatie - SNMP-gerelateerde opdrachten](#)

[Apparaatconfiguraties voor apparaten uit de Board-, Desk- en Room-reeks](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.