

在雲註冊的終端上配置SNMP

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[什麼是SNMP](#)

[可以請求哪些資訊](#)

[在雲註冊終端上配置SNMP](#)

[在控制中心啟用SNMPv2c模式](#)

[在控制中心啟用SNMPv3模式](#)

[終端GUI中的SNMP配置如何](#)

[為SNMPv3配置USM使用者](#)

[測試SNMPv2c和SNMPv3配置](#)

[終端是否可以同時啟用SNMPv2c和SNMPv3](#)

[是否可以使用SNMP通過控制中心配置多個終端](#)

[需要記住的重要詳細資訊](#)

[聯絡TAC以解決終端上的SNMP問題](#)

[相關資訊](#)

簡介

本檔案介紹如何在雲註冊終端上設定SNMP和對其進行疑難排解。

必要條件

需求

建議您熟悉以下主題：

- 控制中心平台
- 通過端點的圖形使用者介面(GUI)和控制中心裝置部分進行端點管理
- 以管理員使用者身份通過SSH連線到終端
- 會議室OS
- SNMP (SNMPv2c和SNMPv3)
- Snmpwalk或其他實用程式/工具或網路管理系統(NMS)測試SNMP配置

採用元件

此處列出的裝置已用於進行測試並產生本文檔中描述的結果：

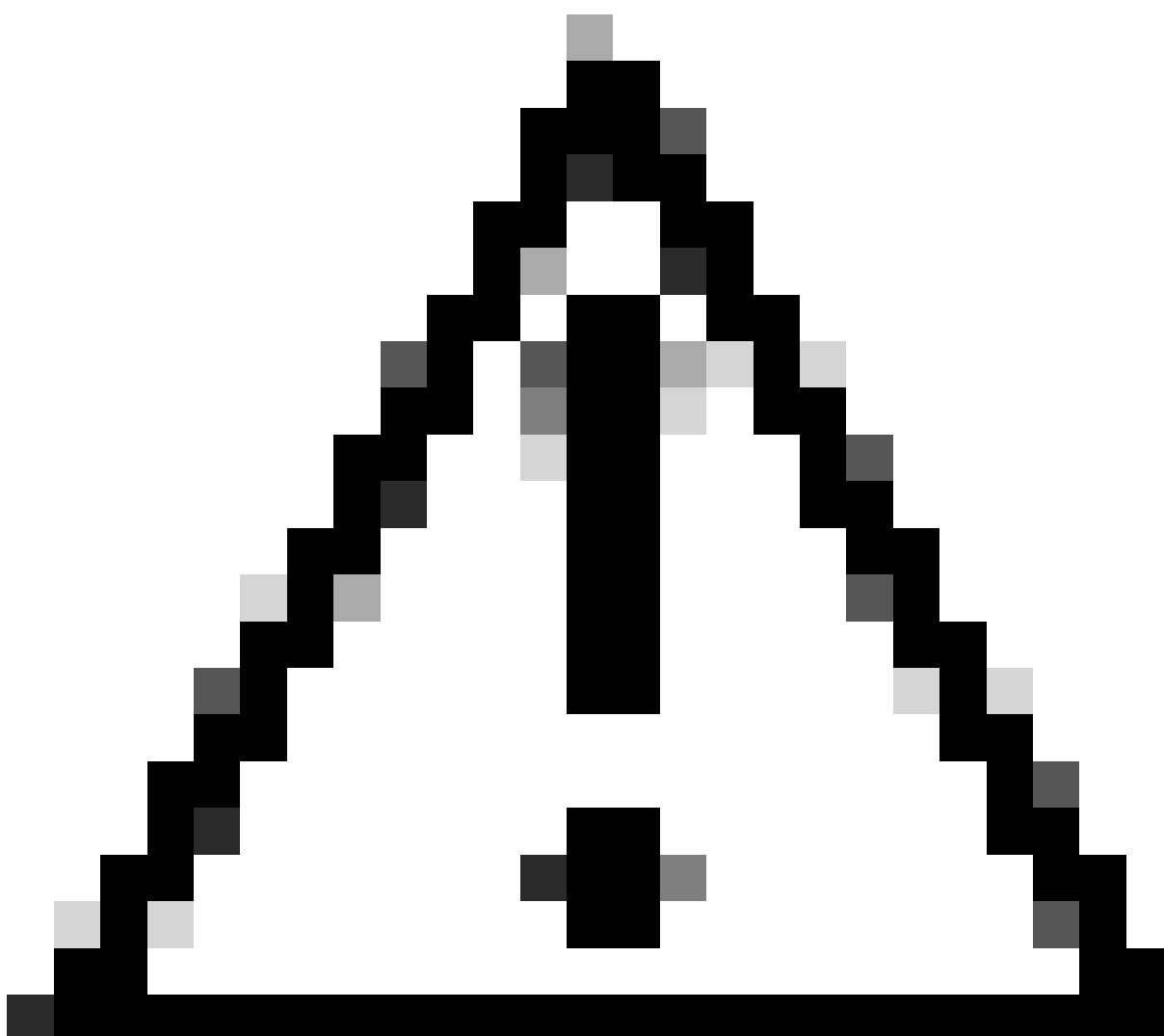
- 控制中心組織
- Cisco會議室套件Pro
- Cisco會議室欄Pro
- Linux Server to host snmpwalk utility，用於測試SNMP配置。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

什麼是SNMP

SNMP代表簡單網路管理協定。該協定用於收集和管理有關網路內裝置的資訊、監控裝置狀態或進行配置更改。這些裝置可以是路由器、交換機、伺服器、印表機或任何其他型別的裝置。必須為這些裝置分配IP地址。SNMP有三個版本。房間作業系統支援SNMPv2c和SNMPv3。不支援SNMPv1。

本文重點介紹在運行雲註冊的Room OS（不使用面向裝置的Webex Edge）的合作終端上對SNMP進行配置和故障排除。



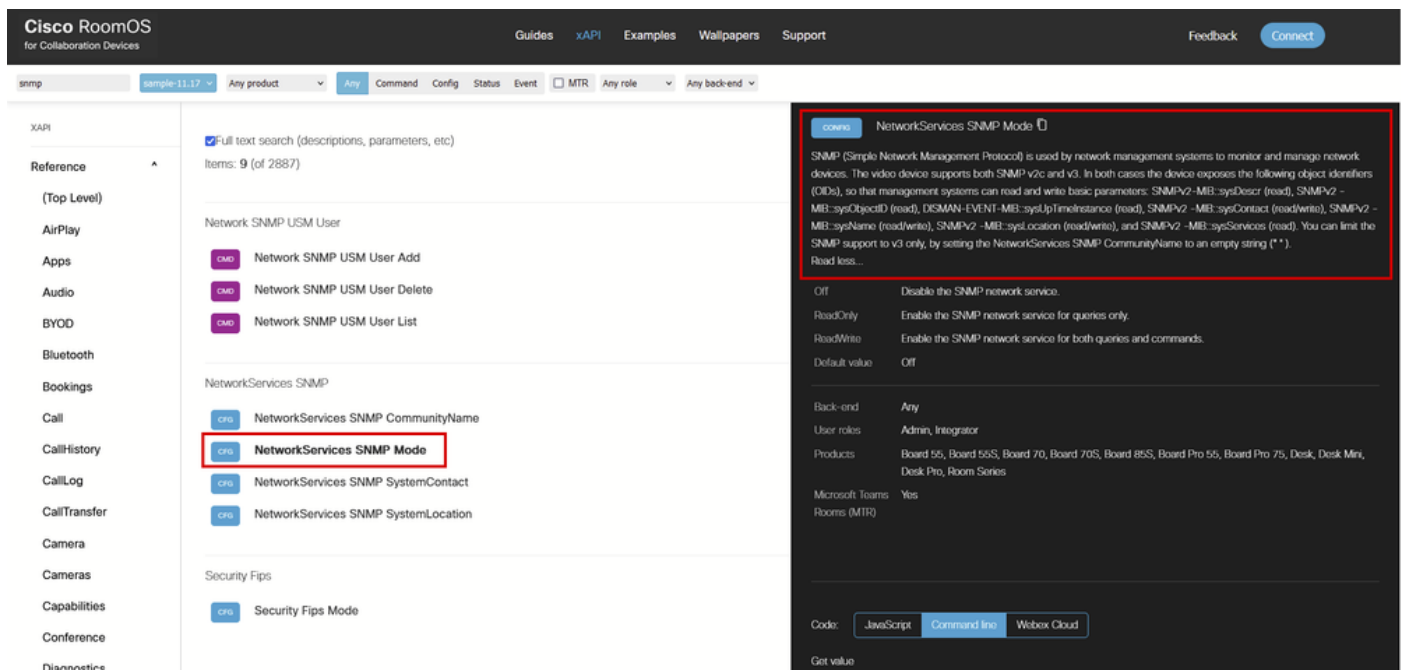
注意：本文僅從終端的角度探討SNMP配置。在網路端完成的任何配置以及用於請求/更新終端上的SNMP相關資訊的工具均不屬於本文的範圍。

TAC不支援對網路中的SNMP進行故障排除，也不能從網路角度提供有關SNMP未按預期運行的任何推斷。您的網路團隊必須參與進一步排除這些問題。

SNMP的管理可以通過多種不同的工具來實現。TAC不支援這些工具。如果這些工具從終端收集的資訊中存在差異，則網路團隊必須首先解決該問題，如果存在足夠資訊證明這是一個終端相關的問題，則必須在TAC中上報。

可以請求哪些資訊

使用SNMP，您可以從終端請求有限數量的資訊。在NetworkService SNMP Mode命令說明的[詳細信息](#)下，可在此鏈接中看到OID和MiB：



The screenshot shows the Cisco RoomOS interface for configuring NetworkServices SNMP Mode. The left 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 is titled 'NetworkServices SNMP Mode' and includes a description of SNMP and its supported parameters. The configuration options are listed in a table with checkboxes and labels.

Option	Default value
Off	Disable the SNMP network service.
ReadOnly	Enable the SNMP network service for queries only.
ReadWrite	Enable the SNMP network service for both queries and commands.
Default value	Off

Back-end: Any
User roles: Admin, Integrator
Products: Board 55, Board 55S, Board 70, Board 70S, Board 85S, Board Pro 55, Board Pro 75, Desk, Desk Mini, Desk Pro, Room Series
Microsoft Teams: Yes
Rooms (MTR): Yes

Code: JavaScript Command line Webex Cloud
Get value

NetworkService SNMP模式命令在會議室OS xAPI文檔中的說明

端點會暴露SNMPv2和SNMPv3的以下OID：

- SNMPv2-MIB::sysDescr (讀) ，
- SNMPv2 -MIB::sysObjectID (讀取) ，
- DISMAN-EVENT-MIB::sysUpTimeInstance (讀取) ，
- SNMPv2 -MIB::sysContact (讀/寫) ，
- SNMPv2 -MIB::sysName (讀/寫) ，
- SNMPv2 -MIB::sysLocation (讀/寫) ，
- SNMPv2 -MIB::sysServices (讀取) 。

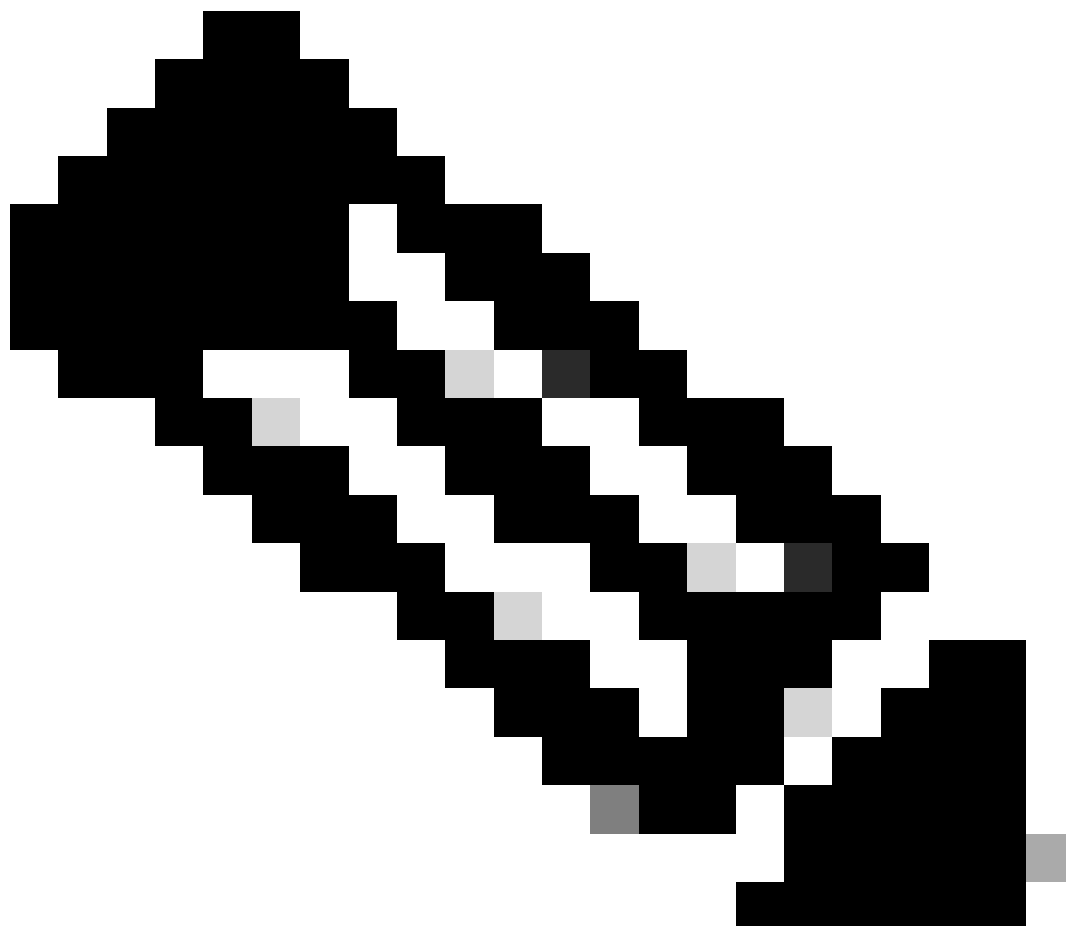


附註：如果只要使用SNMPv3，可以將NetworkServices SNMP CommunityName設定為空字串。

在雲註冊終端上配置SNMP

通常，終端上的配置更改可以通過四種不同方式進行：

1. 可用的Webex API
2. 終端GUI
3. 控制中心
4. SSH直接連線到終端



附註：要訪問終端GUI，請開啟瀏覽器，然後在URL欄中鍵入終端的IP地址。您需要與終端位於同一網路上，並且您需要具有使用者憑證才能登入。

並非所有配置都能以所有四種方式進行。在本檔案的場景中，可以採用四種方式啟用SNMP模式，但是為了建立能夠通過SNMP與裝置通訊的SNMP使用者，您需要通過SSH連線到終端，或者使用Webex API，或者在Customization部分下的Developer API使用終端的GUI。無法從終端的控制中心所有配置部分創建USM使用者。

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
/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:

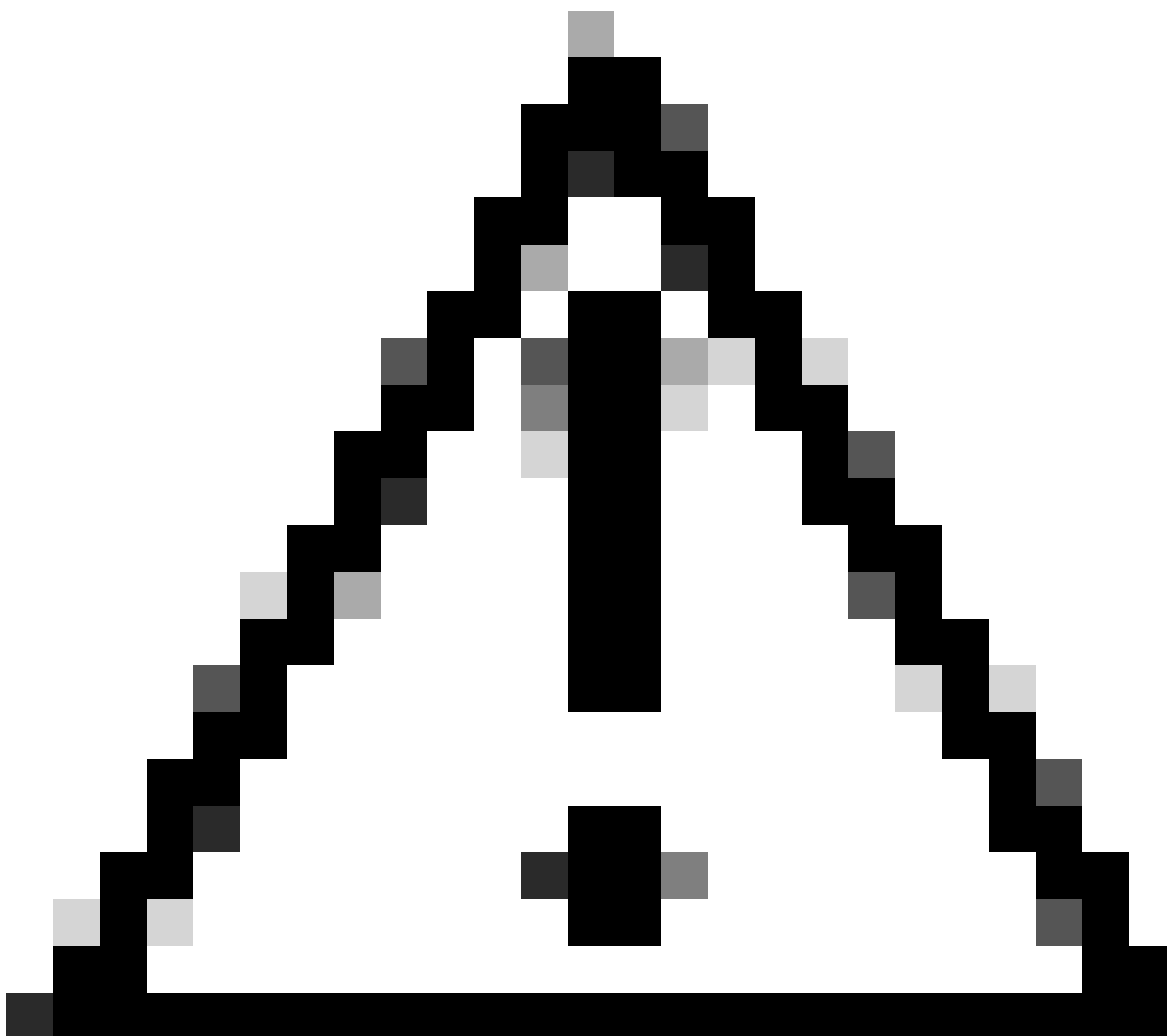
xCommand Dial Number: "person@example.com" Protocol: SIP

xCommand Network SNMP USM User List

Execute

1 of 1 applied successfully.

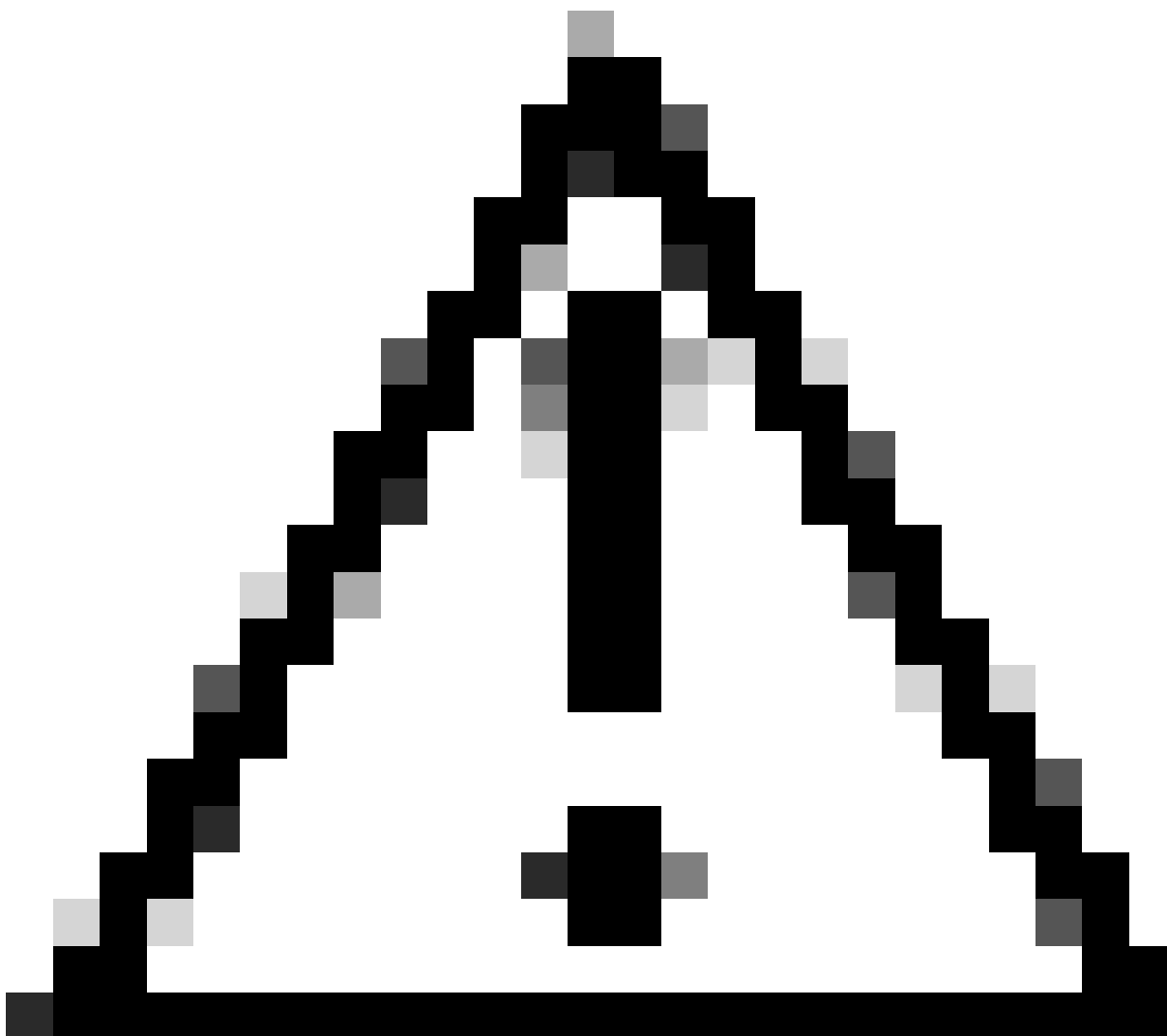
終端GUI上のDeveloper API部分



注意：在執行命令和配置文本框中發出的命令不會返回任何結果。您只會看到命令是否已成功執行。這就是列出USM使用者的命令不會返回上一個螢幕截圖中的任何結果的原因。這表示您可以成功從終端的GUI的此部分建立USM使用者，但是為了再次檢查是否建立了使用者，您需要通過SSH連線到裝置。

對於配置SNMPv2c，不需要建立使用者。身份驗證使用在端點上配置的社群名稱（也稱為社群字串）進行。終端的SNMP代理（已存在於裝置上）響應與裝置上配置的社群名稱相匹配的請求。如果來自管理系統的SNMP請求不包含匹配的社群名稱（區分大小寫），則消息將被丟棄，並且影片裝置中的SNMP代理將不會傳送響應。

但是，SNMPv3要求配置USM使用者才能成功進行身份驗證。為此，必須使用網路SNMP USM使用者命令。這可以通過SSH直接連線到裝置，或者通過使用Developer API部分下的裝置GUI來實現。或者，可以使用Webex API。

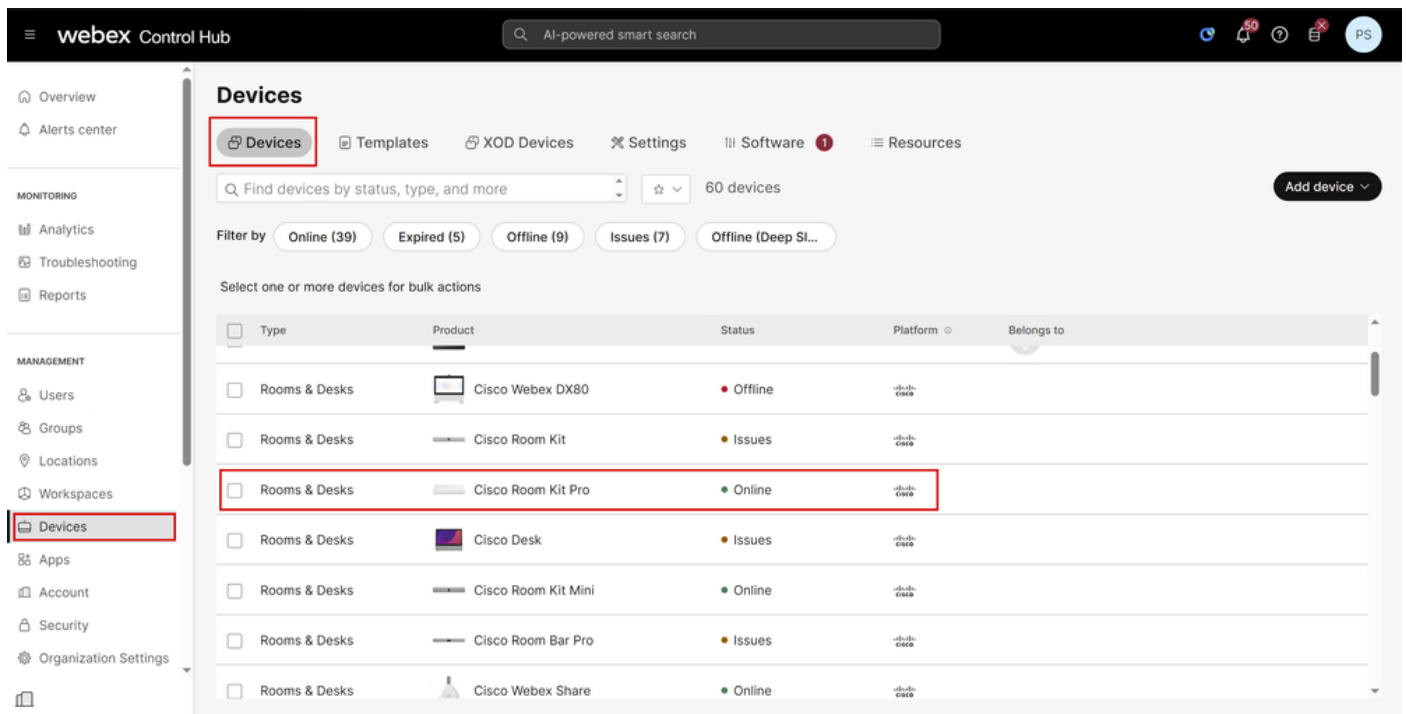


注意：您需要決定是要啟用SNMPv2、SNMPv3還是同時啟用。思科終端不支援SNMPv1。任何使用SNMPv1的嘗試都將失敗。

在本文檔中，SNMPv2和SNMPv3協定將在控制中心啟用和配置，但SNMP3身份驗證所需的USM使用者是通過SSH配置的。

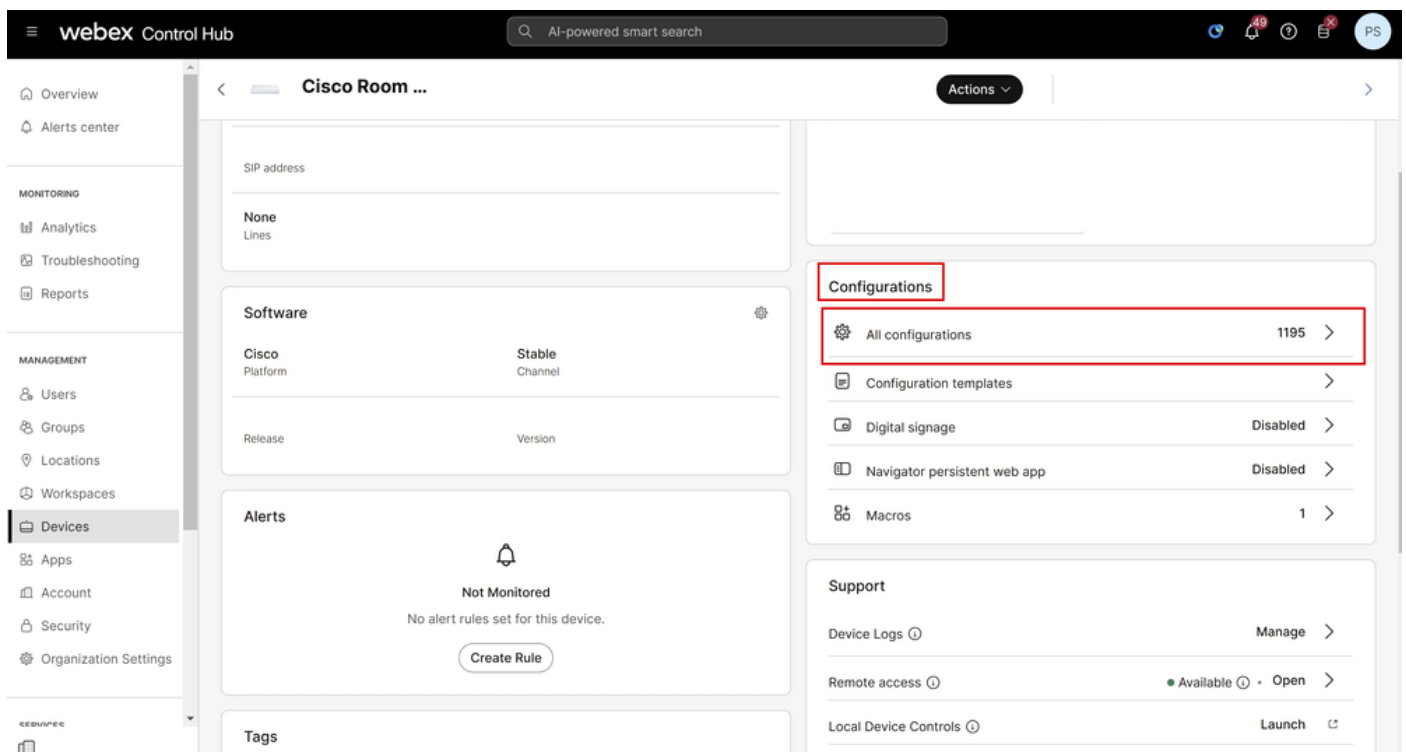
在控制中心啟用SNMPv2c模式

導航到admin.webex.com，然後使用管理員憑據登入。建議為完全管理員。導航到使用者介面左側Management部分下的Devices。在Devices頁籤下，選擇要配置的裝置。本範例中使用的是Cisco Room Kit Pro。



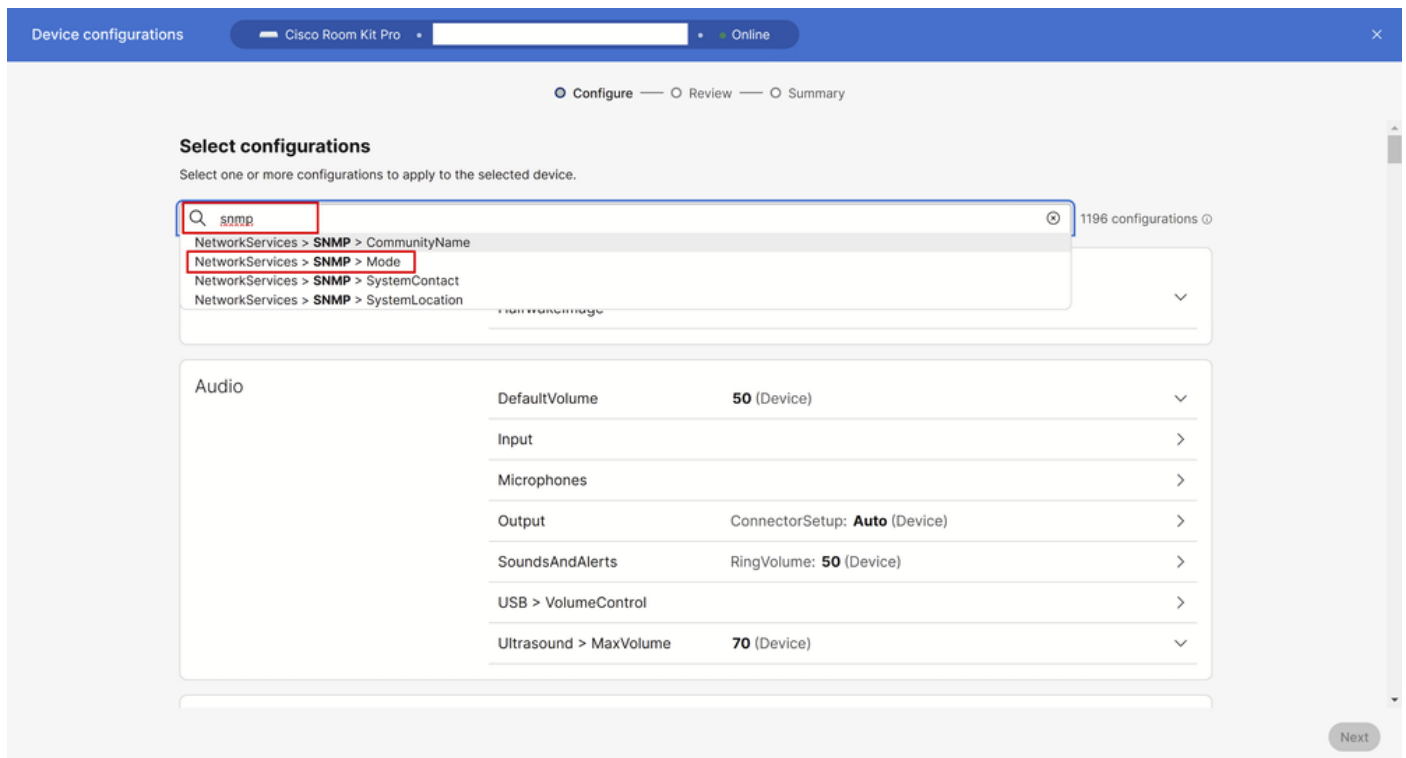
「控制集線器裝置」部分

在開啟的新Control Hub頁中的裝置詳細資訊下，導航到Configurations部分並點選All Configurations:



Room Kit Pro的控制中心裝置詳細資訊

在搜尋欄中，輸入snmp，然後選擇NetworkServices > SNMP > Mode:

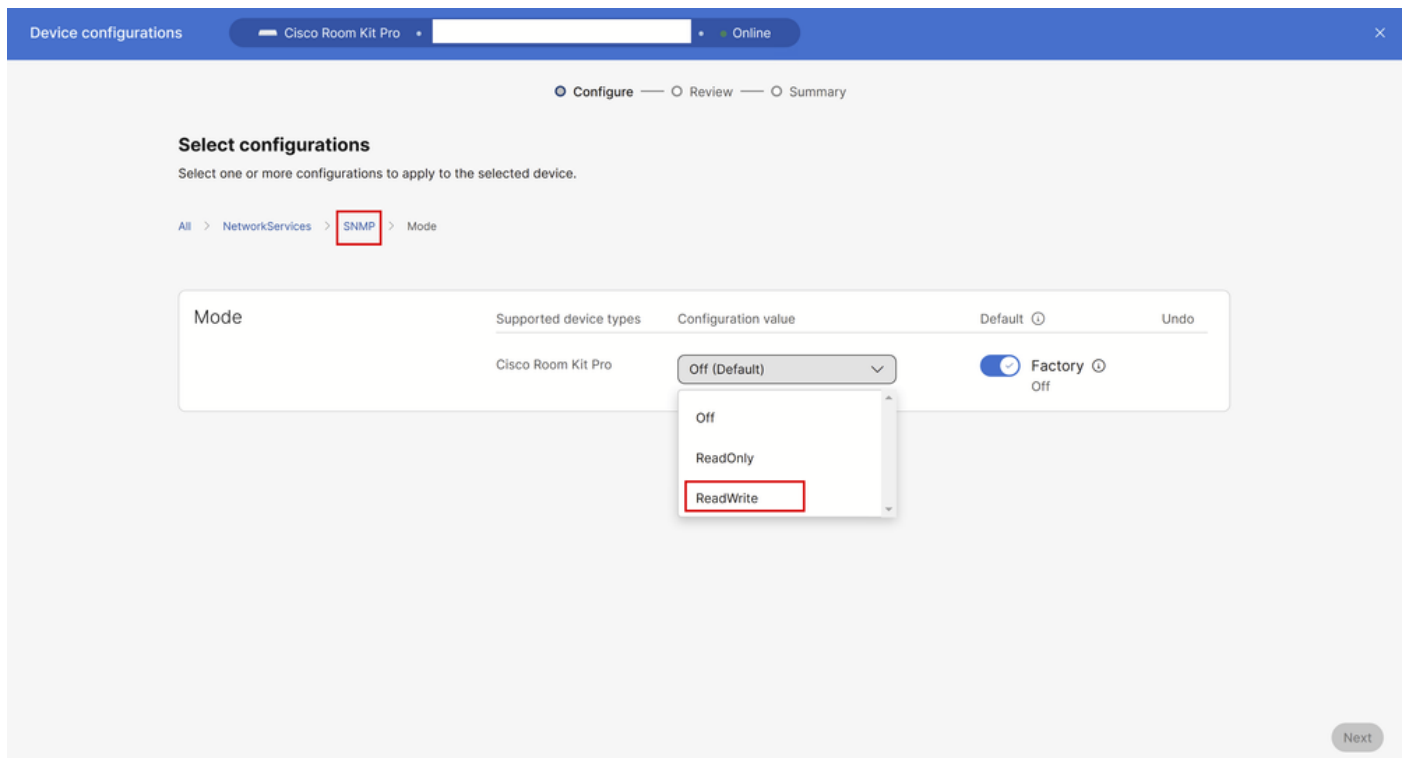


「控制中心所有配置」視窗

選擇需要在環境中啟用的模式。有三個可用選項：

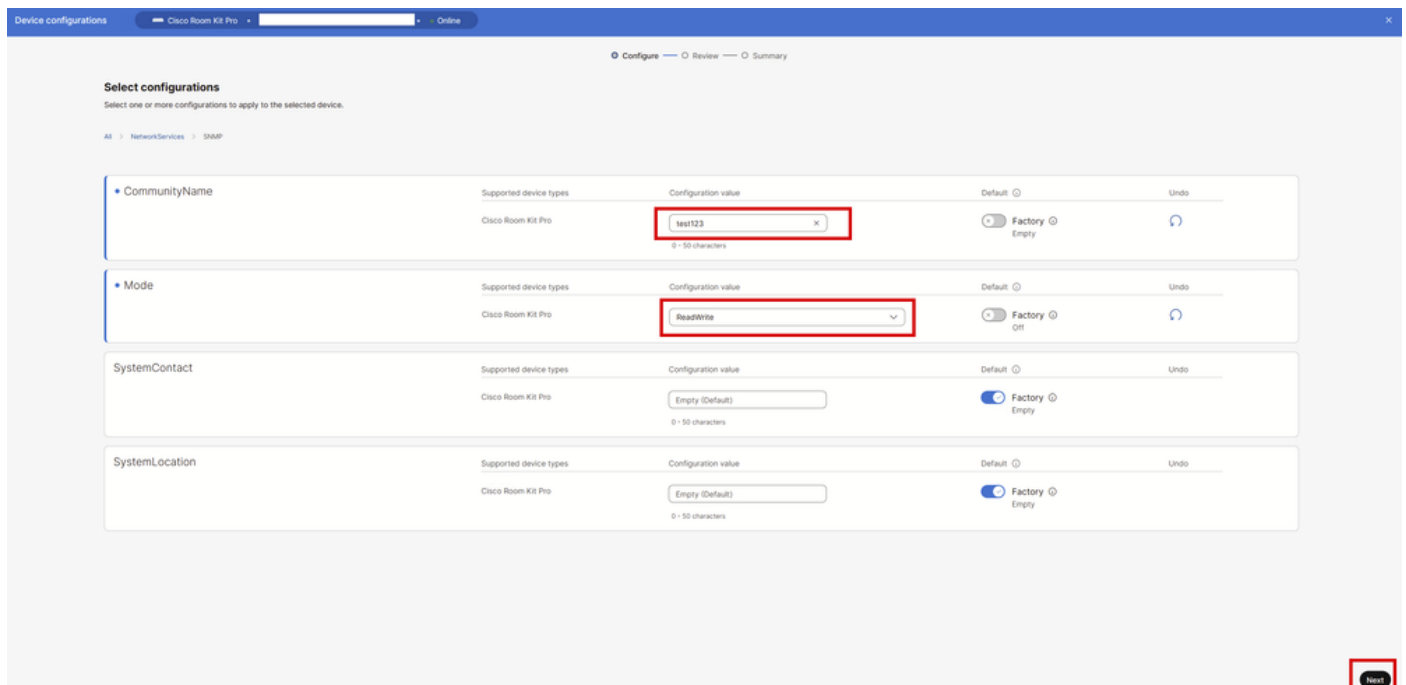
1. Off: 禁用SNMP網路服務。
2. 唯讀：僅為查詢啟用SNMP網路服務。
3. 讀取/寫入：為查詢和命令啟用SNMP網路服務。

在本示例中，ReadWrite處於選中狀態。然後，在設定導航部分按一下SNMP，如圖所示。這將使您返回到設定中的一個步驟，並且您可以檢視所有可以通過Control Hub在裝置上配置的SNMP相關設定：



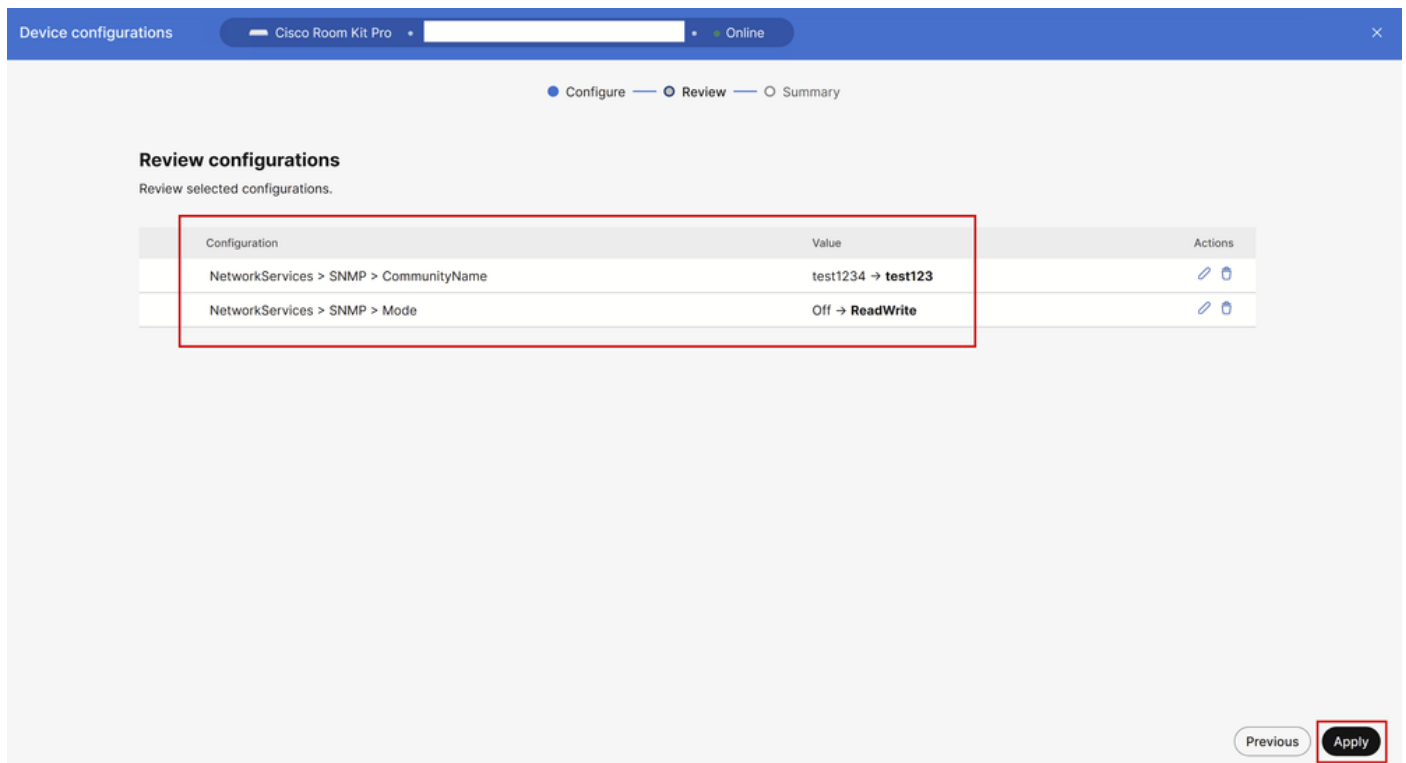
Control Hub中所有配置下的SNMP模式設定

按一下SNMP後，系統會顯示所有可用的SNMP選項，如下圖所示。要成功設定SNMPv2，需要設定社群名稱。團體名稱用於在SNMP伺服器與終端上存在的SNMP代理之間進行身份驗證。在本例中，Community Name（社群名稱）設定為test123。按一下右下角的Next。



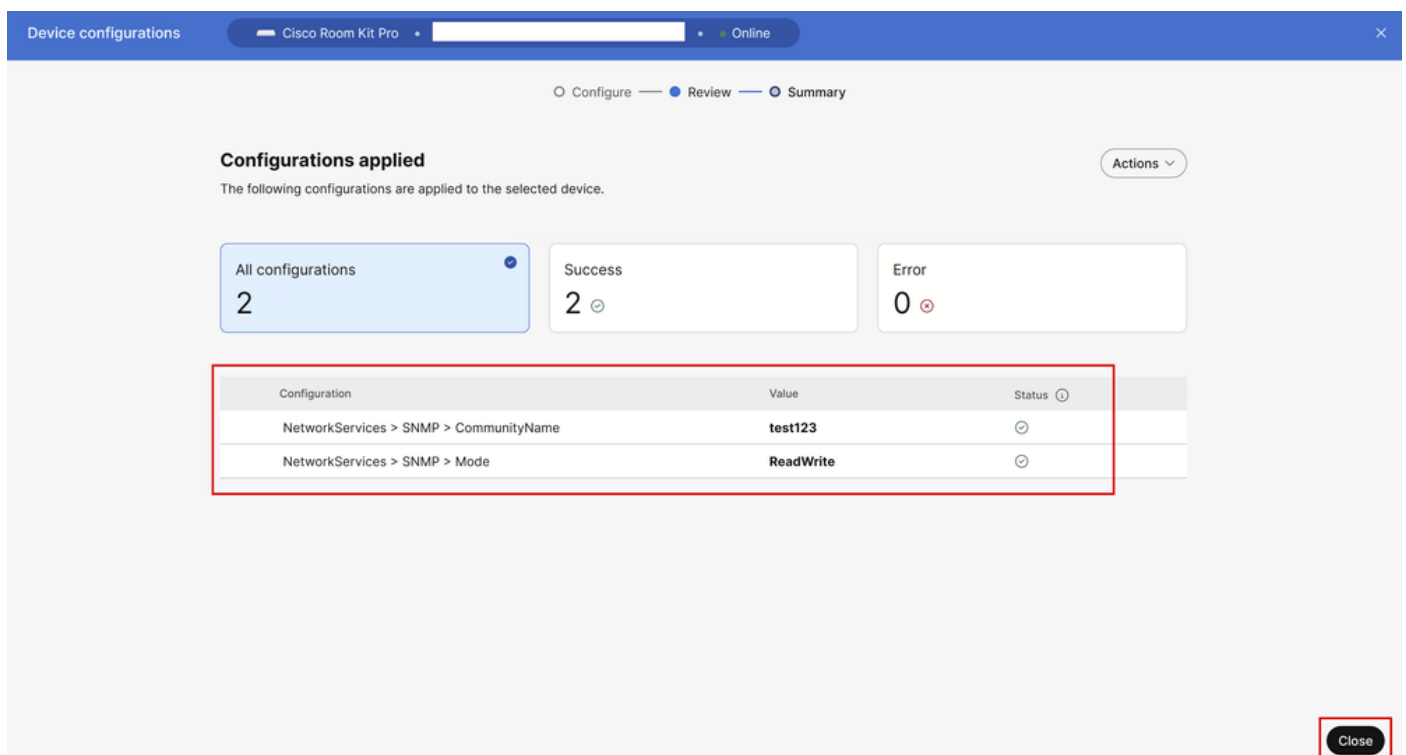
Control Hub中「所有配置」下的SNMP設定

檢視裝置配置並點選右下角的Apply:



在應用更改之前檢視配置

驗證配置更改是否已成功應用。然後按一下「Close」。



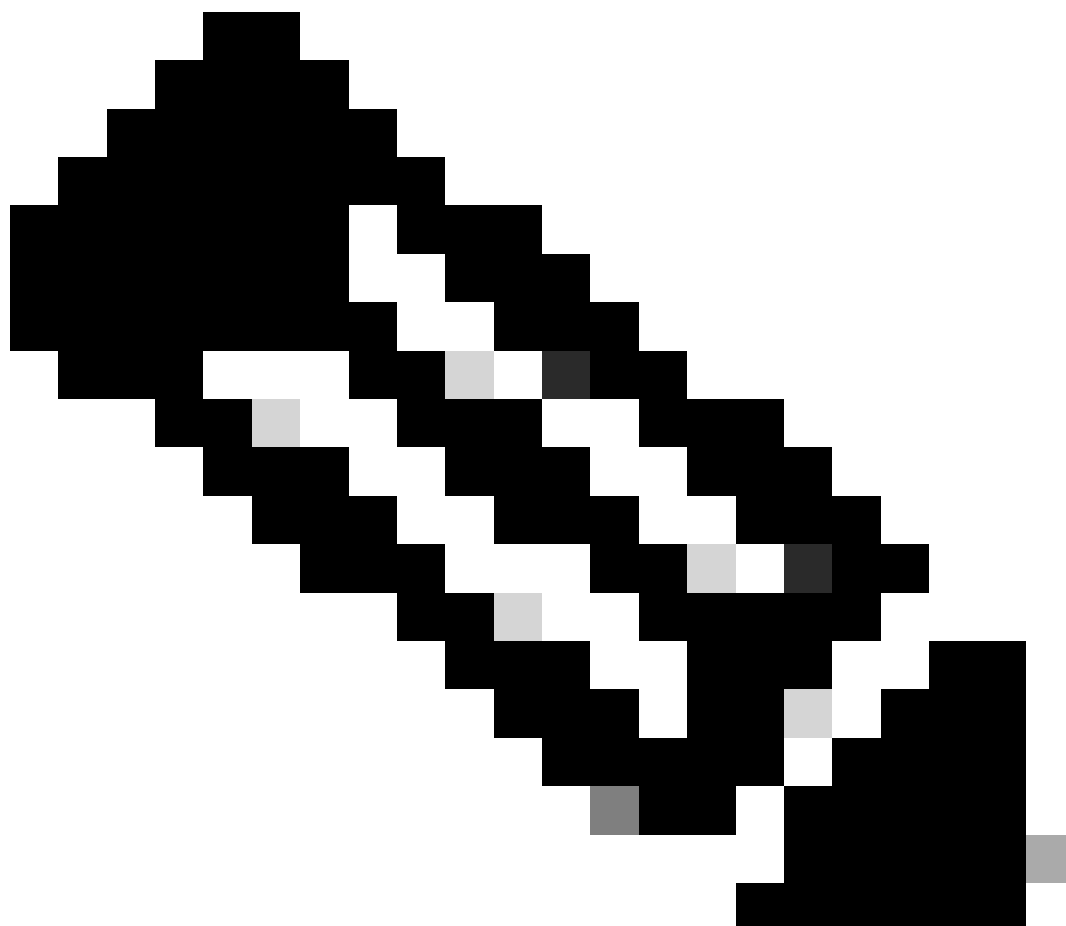
終端配置已成功應用於控制中心

在此階段，在終端上成功啟用SNMPv2c，並設定社群名稱。

在控制中心啟用SNMPv3模式

與SNMPv2c相比，SNMPv3提供了更多安全性，並且需要在終端上執行不同的配置。導航至Control Hub中Management部分下的Devices。繼續使用Devices頁籤，然後選擇要使用SNMPv3配置的其中一個終端。例如，使用思科會議室欄Pro。

在裝置詳細資訊下，導航到Configurations部分，然後按一下All Configurations。將會開啟「裝置配置」頁面。在搜尋欄中鍵入snmp，然後選擇NetworkServices > SNMP > Mode。在本例中，SNMP模式設定為ReadWrite。按一下SNMP檢視裝置上的所有可配置SNMP設定。



附註：在先前的範例中設定了SNMPv2c時，已對SNMPv3到目前為止提到的所有步驟進行了說明。因此，未提供步驟的螢幕截圖。如果對如何導航控制中心設定有任何疑問，請參閱在控制中心中啟用SNMPv2c模式部分。

要僅支援SNMPv3，您需要將社群名稱設定為用引號括起來的空字符串：""。

The screenshot displays the 'Device configurations' window for a 'Cisco Room Bar Pro'. At the top, there are tabs for 'Configure', 'Review', and 'Summary', with 'Configure' being the active tab. Below the tabs, there are four configuration sections, each with a 'Supported device types' column, a 'Configuration value' column, a 'Default' column, and an 'Undo' button.

- CommunityName:** The 'Supported device types' column lists 'Cisco Room Bar Pro'. The 'Configuration value' column has a text input field containing three asterisks (***) and a red box around it. The 'Default' column shows a toggle switch for 'Factory' (Empty) and an 'Undo' button.
- Mode:** The 'Supported device types' column lists 'Cisco Room Bar Pro'. The 'Configuration value' column has a dropdown menu set to 'ReadWrite' and a red box around it. The 'Default' column shows a toggle switch for 'Factory' (Off) and an 'Undo' button.
- SystemContact:** The 'Supported device types' column lists 'Cisco Room Bar Pro'. The 'Configuration value' column has a text input field containing 'Empty (Default)'. The 'Default' column shows a toggle switch for 'Factory' (Empty) and an 'Undo' button.
- SystemLocation:** The 'Supported device types' column lists 'Cisco Room Bar Pro'. The 'Configuration value' column has a text input field containing 'Empty (Default)'. The 'Default' column shows a toggle switch for 'Factory' (Empty) and an 'Undo' button.

In the bottom right corner, there is a 'Next' button highlighted with a red box.

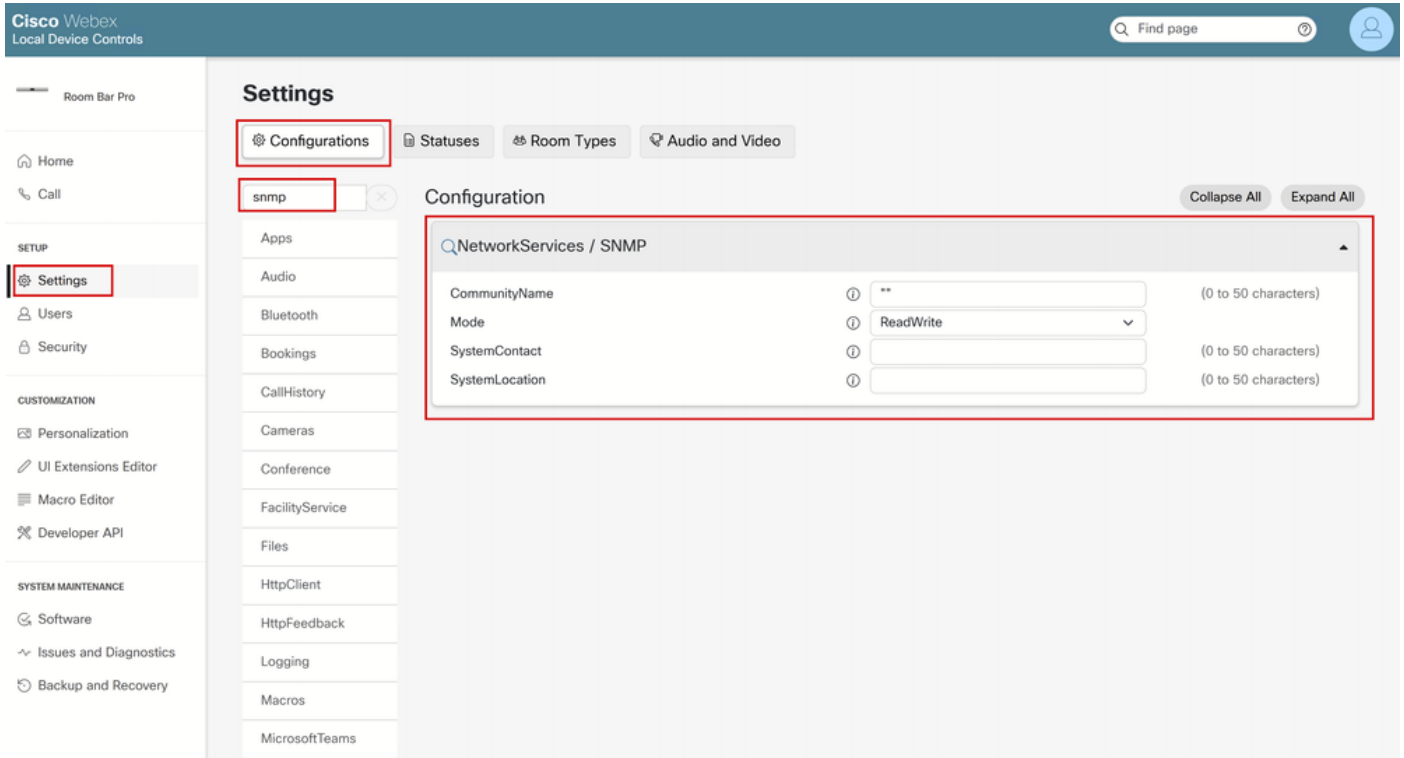
Control Hub中「所有配置」下的SNMP設定

按一下「Next」，然後檢視組態變更，然後按一下「Apply」。按一下「Close」以關閉裝置組態頁面。

可在控制中心執行的配置到此結束。在這個階段，只啟用SNMPv3。

終端GUI中的SNMP配置如何

可以從裝置GUI執行相同的配置。開啟瀏覽器頁籤並鍵入終端的IP地址（您需要與終端位於同一網路中）。以admin 使用者身份登入，在終端GUI中，導航到SETUP部分下的Settings。在Configurations頁籤上，並在設定搜尋欄上鍵入snmp。此圖顯示了在上一節的Room Bar Pro上完成的SNMPv3配置的SNMP設定是如何顯示的：



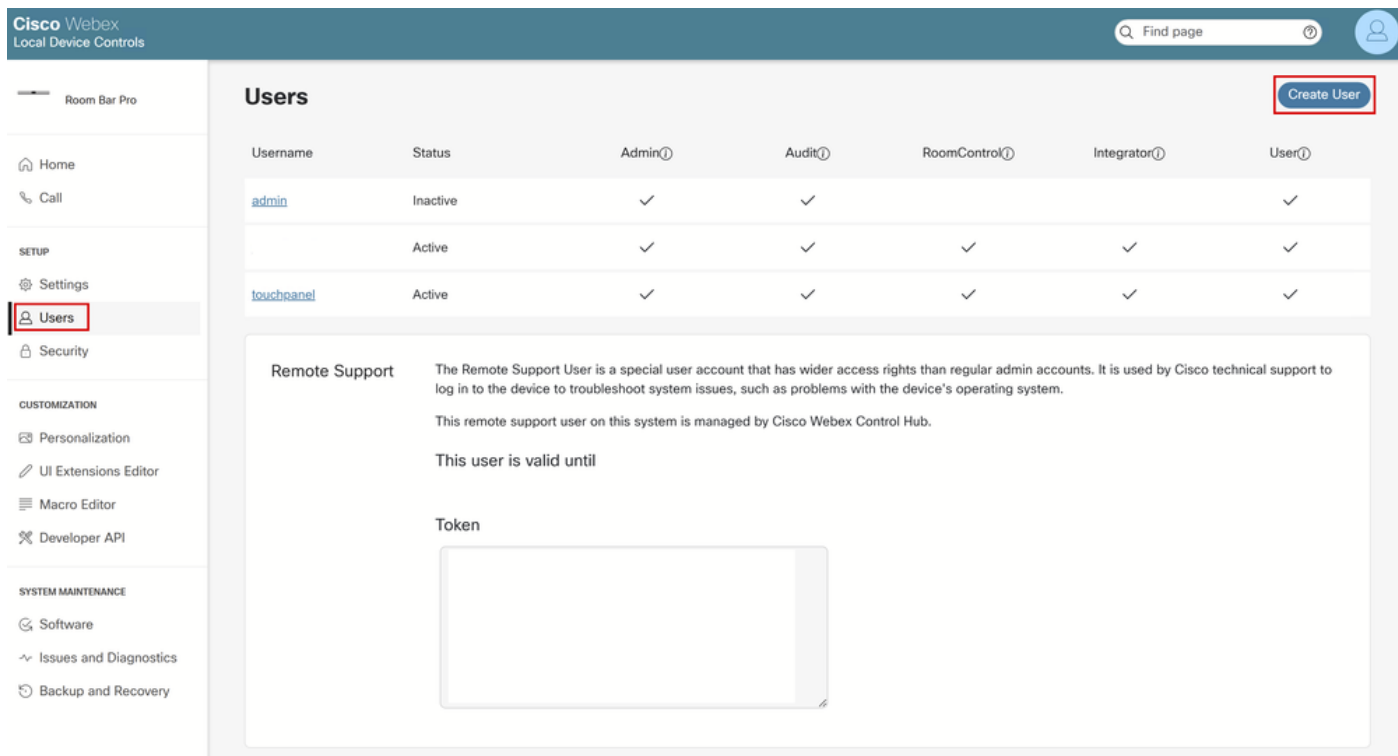
終端的GUI上的SNMPv3配置

為SNMPv3配置USM使用者

為了能夠使用SNMPv3，您需要建立一個USM使用者。執行此操作的可用命令可以在[此處](#)的Room OS文檔連結中找到。使用SSH連線到裝置。為此，需要在裝置上擁有管理員帳戶。如果不是，則需要建立管理員帳戶。這一部分貫穿整個過程。

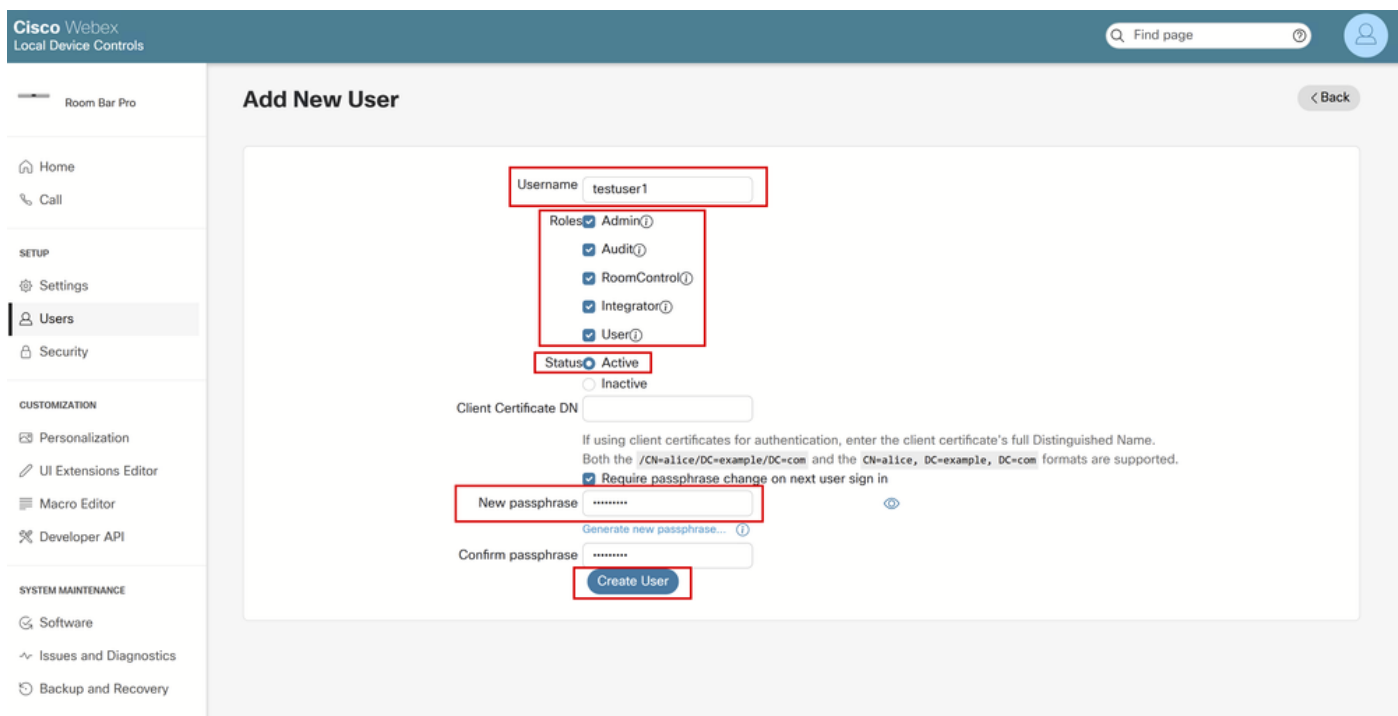
導航至Control Hub中Management部分下的Devices。在Devices頁籤下並選擇要為其建立管理員使用者的終端之一。在本示例中，使用的是Cisco Room Bar Pro。

在裝置詳細資訊下，導航到支援部分，然後按一下本地裝置控制（您需要與終端位於同一網路中才能使用此功能）。裝置GUI開啟。導覽至SETUP部分下的Users，然後按一下Create User。



終端GUI中的Users部分

提供使用者名稱和密碼短語（密碼）。確保使用者具有完全管理員許可權並且處於活動狀態：



從終端的GUI建立使用者

從Users頁面驗證使用者是否已建立且處於活動狀態：

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

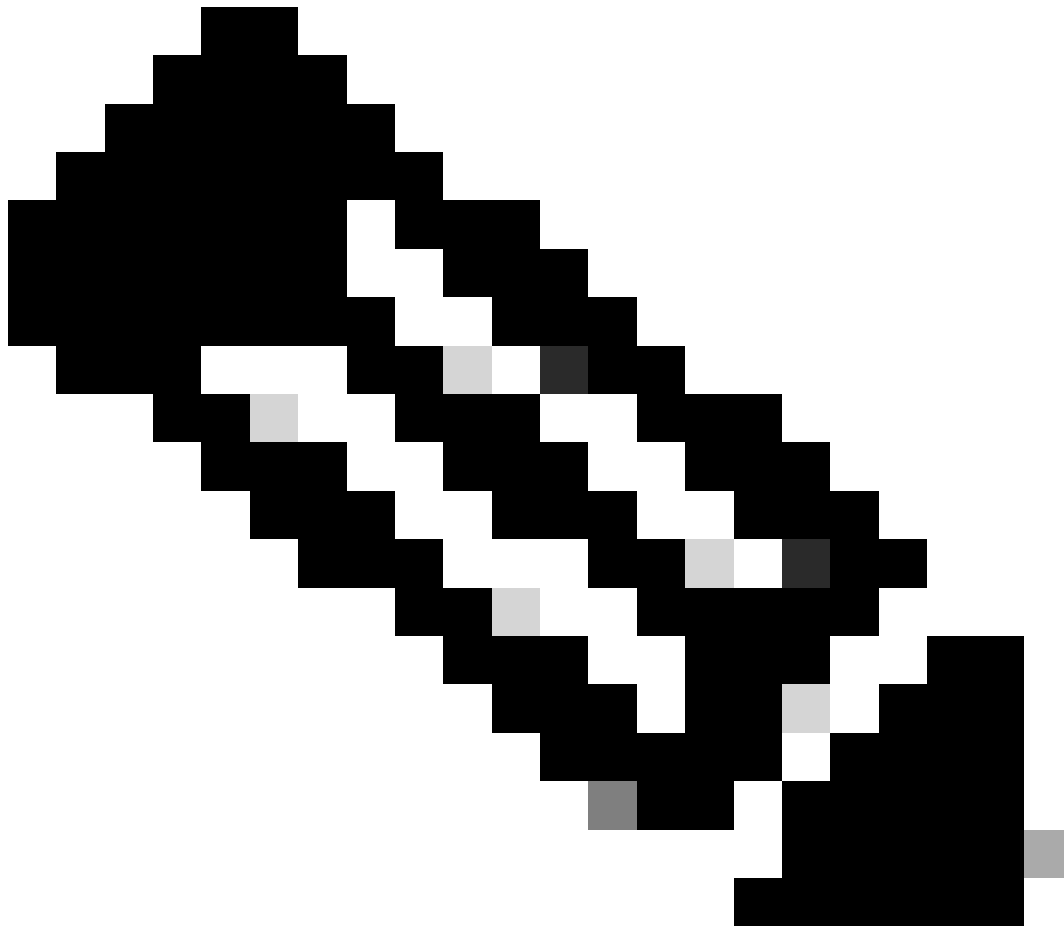
The Remote Support User is a special user account that has wider access rights than regular admin accounts. It is used by Cisco technical support to log in to the device to troubleshoot system issues, such as problems with the device's operating system.

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

This user is valid until

Token

在其他使用者之間建立並列出的新使用者



附註：在首次嘗試使用新建立的使用者進行SSH登入時，系統會要求您更改密碼。您會看到類似以下的提示：

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

首次使用SSH時更改密碼

更改密碼後，您將立即斷開連線，需要啟動新的SSH連線。

成功建立管理員使用者後，使用您選擇的SSH客戶端並連線到終端。使用管理員憑據登入。這是您看到的提示：

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

通過SSH成功登入終端嘗試

使用本文[所述](#)Network SNMP USM User Add命令。在本演示中，使用的命令為：

```
xCommand Network SNMP USM User Add AuthenticationPassword: testuser123 AuthenticationProtocol: SHA-256 Name: psitaras PrivacyPassword: test1234
```

此命令的結果是：

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

通過SSH建立USM使用者

要使命令執行時沒有錯誤，您需要遵守此連結中共用的命令文檔中所述的某些[規則](#)。為方便起見，在此圖片中貼上了編寫此命令時此文檔的當前要求，但您必須在建立使用者時參考[此連結](#)。在圖的最後，請注意該命令的確切語法。

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

xAPI文檔中的USM使用者建立命令語法



警告：如果出現拼寫錯誤或存在未滿足的要求，該命令將返回錯誤，並且不會建立使用者。此處提供了一個示例，其中不提供至少8個字元的隱私密碼，而是提供較短的7個字元密碼：

```
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.

由於密碼短，USM使用者建立失敗

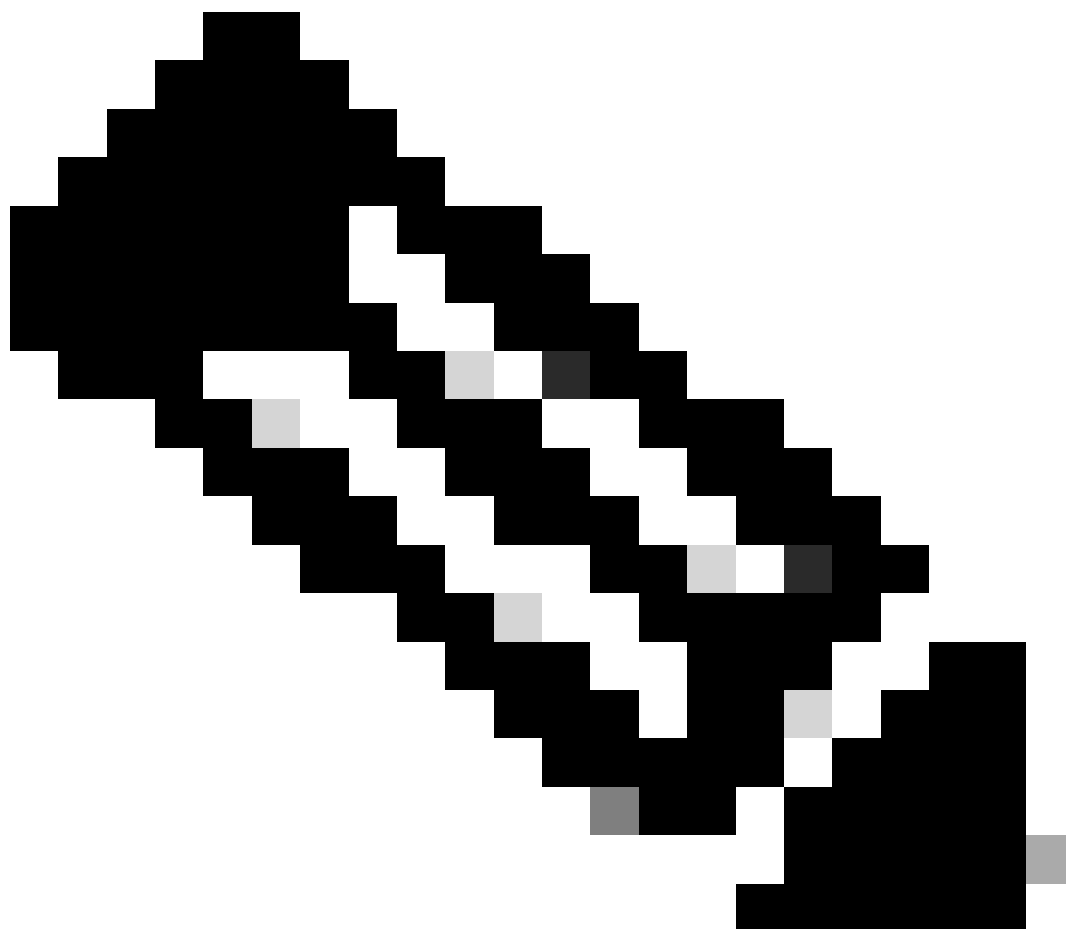
您可以使用Network SNMP USM User List命令測試您的使用者是否已建立。此命令列出裝置上儲存的所有USM使用者：

```
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
```

用於確認使用者建立的網路SNMP USM使用者清單命令

在此階段，已確認已成功建立使用者主題。SNMPv3配置已完成。



附註：在終端的GUI的Users部分下，USM使用者類別不可見。這是意料之中的。

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	✓	✓			✓
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

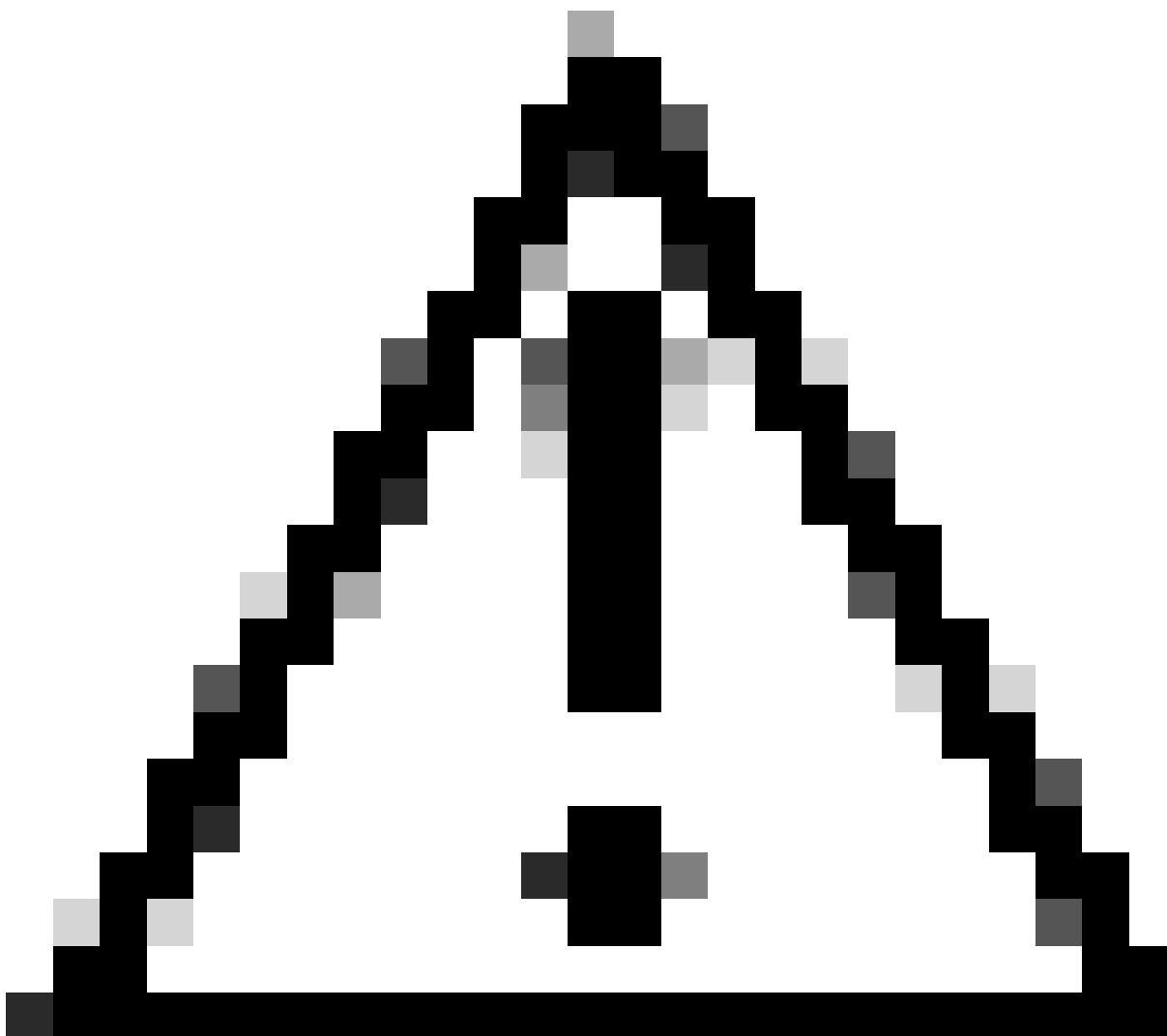
Token

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

在終端的GUI中，使用者下不可見USM使用者

測試SNMPv2c和SNMPv3配置

在這個階段，您可以繼續使用您的網路管理系統(NMS)測試SNMPv2c和/或SNMPv3配置。本文的實驗配置不包含運行SNMP服務的任何NMS或SNMP伺服器。為了測試配置，使用名為snmpwalk的實用程式。此應用工具安裝在Linux伺服器上。



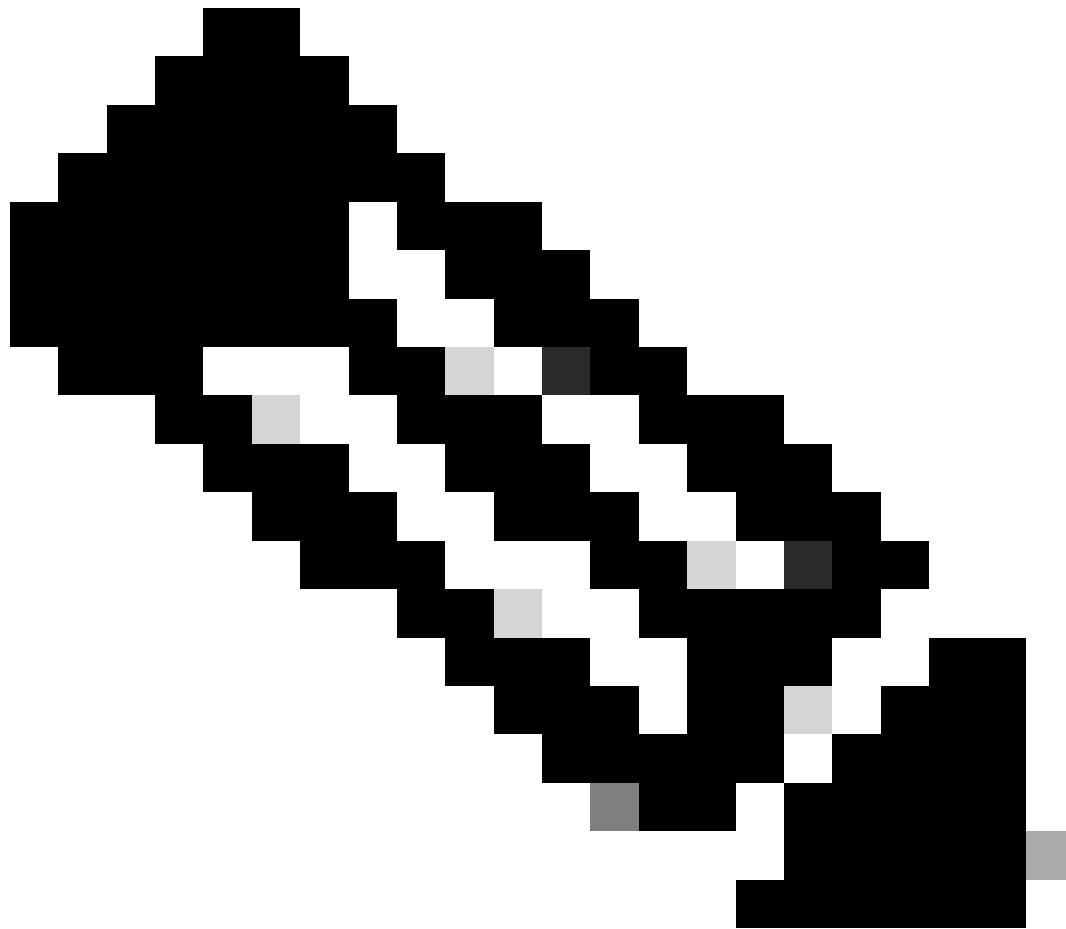
注意：建議不要使用Snmpwalk來測試合作終端上的SNMP配置。TAC工程師不支援該工具，您需要先熟悉該工具的使用方法，然後才能繼續測試。您可以使用任何其他SNMP工具或NMS來測試您的配置，而不是使用snmpwalk。本文使用Snmpwalk只是一個示例（需要工具測試配置以進行演示），並且沒有與其使用相關的承諾或促銷。

安裝snmpwalk不屬於本指南的一部分，因此省略。根據您用於測試的電腦的作業系統(OS)，安裝要求可能有所不同。在測試之前，必須設法成功安裝。

Snmpwalk是一個可用於驗證SNMP配置的工具。它執行終端的MiB遍歷並返回可用資訊。雲註冊的終端公開了7個對象識別符號(OID):

- SNMPv2-MIB::sysDescr (讀) ,
- SNMPv2 -MIB::sysObjectID (讀取) ,
- DISMAN-EVENT-MIB::sysUpTimeInstance (讀取) ,
- SNMPv2 -MIB::sysContact (讀/寫) ,
- SNMPv2 -MIB::sysName (讀/寫) ,
- SNMPv2 -MIB::sysLocation (讀/寫) ,

- SNMPv2 -MIB::sysServices (讀取) 。
-



附註：用於所列舉的snmpwalk測試的內部IP是私有IP，不再使用。用於本指南的實驗室已停用，裝置已出廠重置。

Cisco Room Kit Pro端點配置了SNMPv2c。使用社群字串進行驗證。發出以下命令：

```
# '-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
```

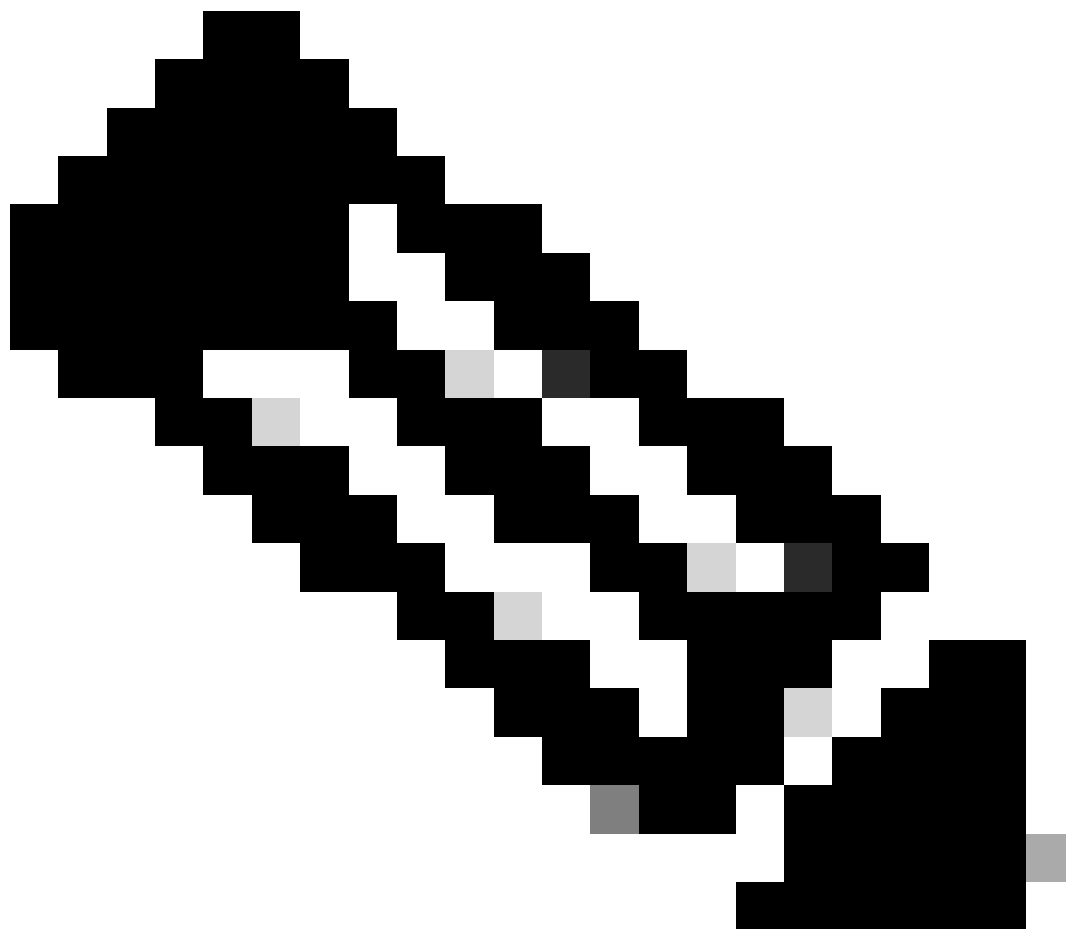
```
iso.3.6.1.2.1.1.3.0 = Timeticks: (106770681) 12 days, 8:35:06.81
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = ""
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.7.0 = No more variables left in this MIB View (It is past the end of the MIB tree)
```

Snmpwalk按預期返回7個結果。有三個管理學碩士是空的：

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

有三個xConfiguration命令可用於設定這些MiB的值。通過SSH連線到終端並發出以下命令：

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



附註：您可以從Control Hub、終端GUI或Webex API對這些設定進行更改，而不是使用這三種命令。

發出上述命令後，在同一端點上再次使用snmpwalk。您會注意到以前空的MiB填充了通過xConfiguration命令提供的值：

```
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)

在此階段，確認在Room Kit Pro裝置上建立的SNMPv2c配置可正常運行。

Cisco Room Bar Pro端點配置了SNMPv3。對於SNMPv3，您需要確保使用正確的身份驗證。未使用社群字串。相反，SNMPv3使用使用者名稱和密碼。

```
# '-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)
```

在此階段，確認在Room Bar Pro裝置上建立的SNMPv3配置可正常運行。

終端是否可以同時啟用SNMPv2c和SNMPv3

是的，這是可能的。但是，在SNMP配置期間，您需要設定社群名稱才能進行SNMPv2c身份驗證。對於此測試，使用前面示例中的Room Bar Pro。終端的控制中心所有配置部分中的當前配置為：

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	

請注意，團體名稱不為空。有兩個引號，表示團體名稱是一個空字串。通過將NetworkServices SNMP CommunityName設定為空字串(""), 可以將SNMP支援限制為版本3。 您需要將此字串替換為團體名稱，例如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	testbothSNMPv2_v3 0 - 50 characters	☒ Factory Empty	

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

在控制中心端點配置設定中新增SNMPv2c的社群名稱

已確認SNMPv3正在使用Room Bar Pro。Snmpwalk用於在設定社群名稱后，測試SNMPv2c是否也正常工作：

```
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)
```

是否可以使用SNMP通過控制中心配置多個終端

可以，可以在控制中心中同時配置多個裝置。本文[在配置多裝置一節](#)中提供了有關如何逐步執行此操作的資訊。

需要記住的重要詳細資訊

- 只有特定的MiB可用。可用的MiB數量受到設計端點的工程團隊設計的限制。不能擴展或增強MiB以提供更多資訊。
- SNMPv2c使用社群名稱（也稱為社群字串）進行身份驗證，而SNMPv3使用使用者名稱和密

碼進行身份驗證，並提供加密。測試時，請確保針對您配置的協定使用正確的身份驗證方法（使用snmpwalk或其他工具/NMS）。

- SNMPv3上始終啟用身份驗證和隱私。端點僅支援authPriv安全級別，並且隱私協定始終為高級加密標準(AES)。
- SNMPv3僅支援基於使用者的安全模型(USM)選項。不支援SNMPv3 over TLS。
- 用於配置使用者以進行SNMP身份驗證的USM使用者命令對SNMPv2c沒有影響。
- 端點上的SNMP CommunityName設定對SNMPv3配置沒有影響。
- SNMP CommunityName區分大小寫。
- 通過將NetworkServices SNMP CommunityName設定為空字串(""), 可以將SNMP支援限制為僅v3。
- 不支援SNMPv1。
- 對於SNMPv2c和SNMPv3，終端公開相同的對象識別符號(OID)。
- 若是SNMPv3，驗證通訊協定必須位於SHA-2系列中（不支援MD或SHA-1）。如果不是，則SNMP請求無法進行身份驗證，並且保持未應答狀態。
- 隱私密碼在裝置上儲存為本地化雜湊值(AES-128)。如果未在此引數中顯式設定隱私密碼，則將其設定為與身份驗證密碼相同（使用在Authentication Protocol引數中指定的雜湊函式）。
- 密碼/密碼和使用者名稱必須位於特定的長度界限內。例如，USM使用者名稱需要最多32個字元，身份驗證密碼需要最少8個字元，最多255個字元。如果未滿足這些要求，Network SNMP USM User Add命令無法建立使用者並返回錯誤。

聯絡TAC以解決終端上的SNMP問題

如果終端的SNMP配置已完成，但出現了問題，則需要聯絡TAC並共用以下資訊：

- 在Control Hub中提供您的組織ID以及受影響終端的序列號(SN)。
- 描述所面臨的場景。
- 提供您嘗試設定的SNMP版本。
- 提供出現的任何錯誤消息。
- 如果裝置的配置有問題，請清楚說明配置過程在哪個步驟停止並提供螢幕截圖。共用返回錯誤的配置命令。
- 收集終端日誌並將其上傳到您的案例。
- 共用用於測試SNMP配置的實用程式\NMS或其他工具。如果使用實用程式測試終端的SNMP代理，請提供使用的完整命令。

相關資訊

[會議室OS xAPI文檔 — SNMP相關命令](#)

[主機板、案頭和房間系列裝置的裝置配置](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。