

在云注册终端上配置SNMP

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[什么是SNMP](#)

[可以请求哪些信息](#)

[在云注册终端上配置SNMP](#)

[在控制中心启用SNMPv2c模式](#)

[在控制中心启用SNMPv3模式](#)

[终端GUI中的SNMP配置如何](#)

[为SNMPv3配置USM用户](#)

[测试SNMPv2c和SNMPv3配置](#)

[终端是否可以同时激活SNMPv2c和SNMPv3](#)

[是否可以通过SNMP控制集线器配置多个终端](#)

[需要记住的重要详细信息](#)

[联系TAC解决终端上的SNMP问题](#)

[相关信息](#)

简介

本文档介绍如何在云注册的终端上配置SNMP并对其进行故障排除。

先决条件

要求

建议您熟悉以下主题：

- 控制中心平台
- 通过终端的图形用户界面(GUI)和控制中心设备部分进行终端管理
- 以管理员用户身份通过SSH连接到终端
- 会议室操作系统
- SNMP (SNMPv2c和SNMPv3)
- Snmpwalk或其他实用程序/工具或网络管理系统(NMS)测试SNMP配置

使用的组件

此处列出的设备已用于进行测试并生成本文档中描述的结果：

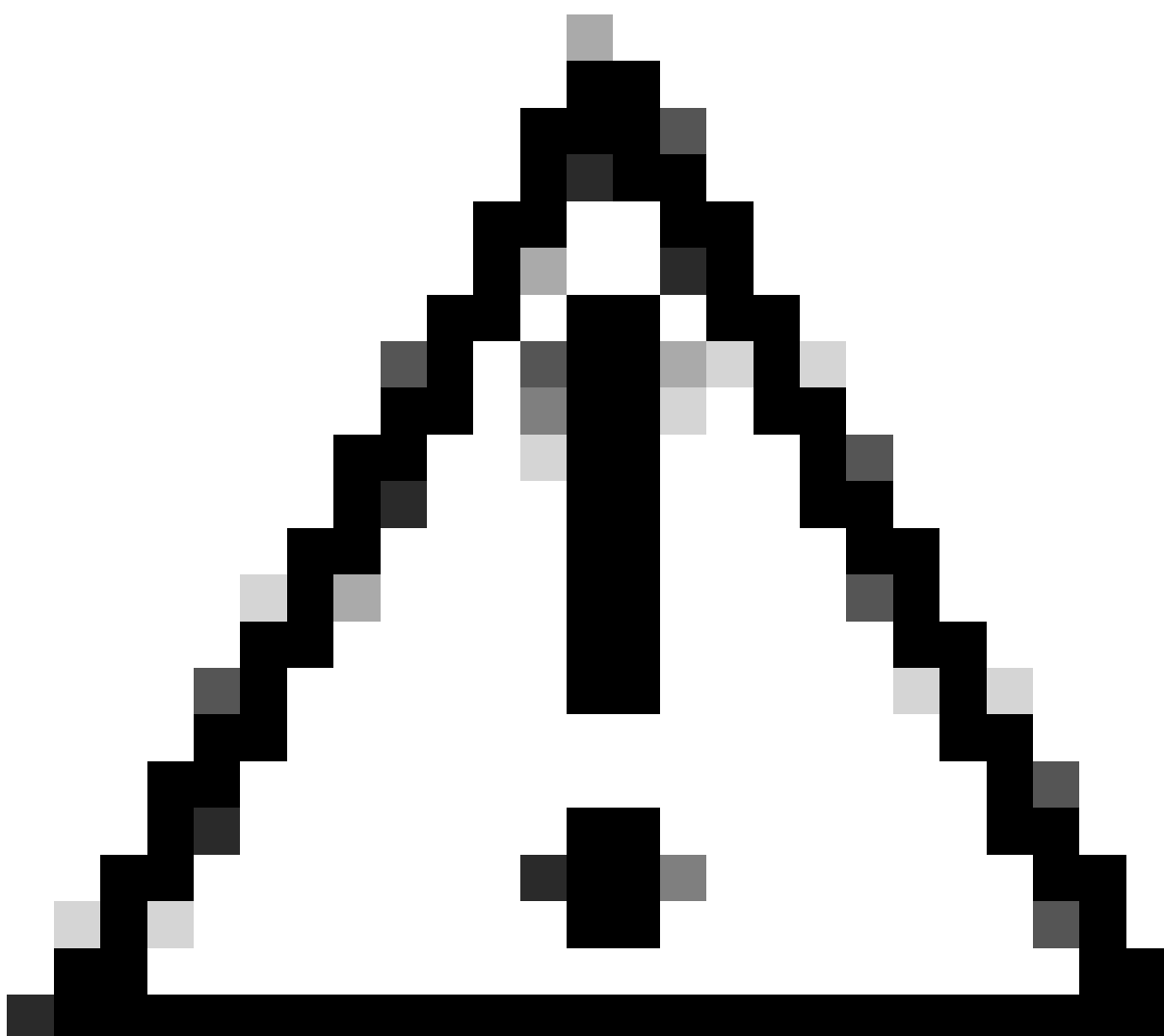
- 控制中心组织
- Cisco Room Kit Pro
- Cisco Room Bar Pro
- Linux服务器到主机snmpwalk实用程序，用于测试SNMP配置。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

什么是SNMP

SNMP代表简单网络管理协议。该协议用于收集和管理有关网络内设备的信息、监控设备状态或更改配置。这些设备可以是路由器、交换机、服务器、打印机或任何其他类型的设备。前提条件是这些设备已经分配了IP地址。SNMP有三个版本。房间操作系统支持SNMPv2c和SNMPv3。不支持SNMPv1。

本文重点介绍运行云注册的会议室操作系统（不使用面向设备的Webex Edge）的协作终端上的SNMP配置和故障排除。



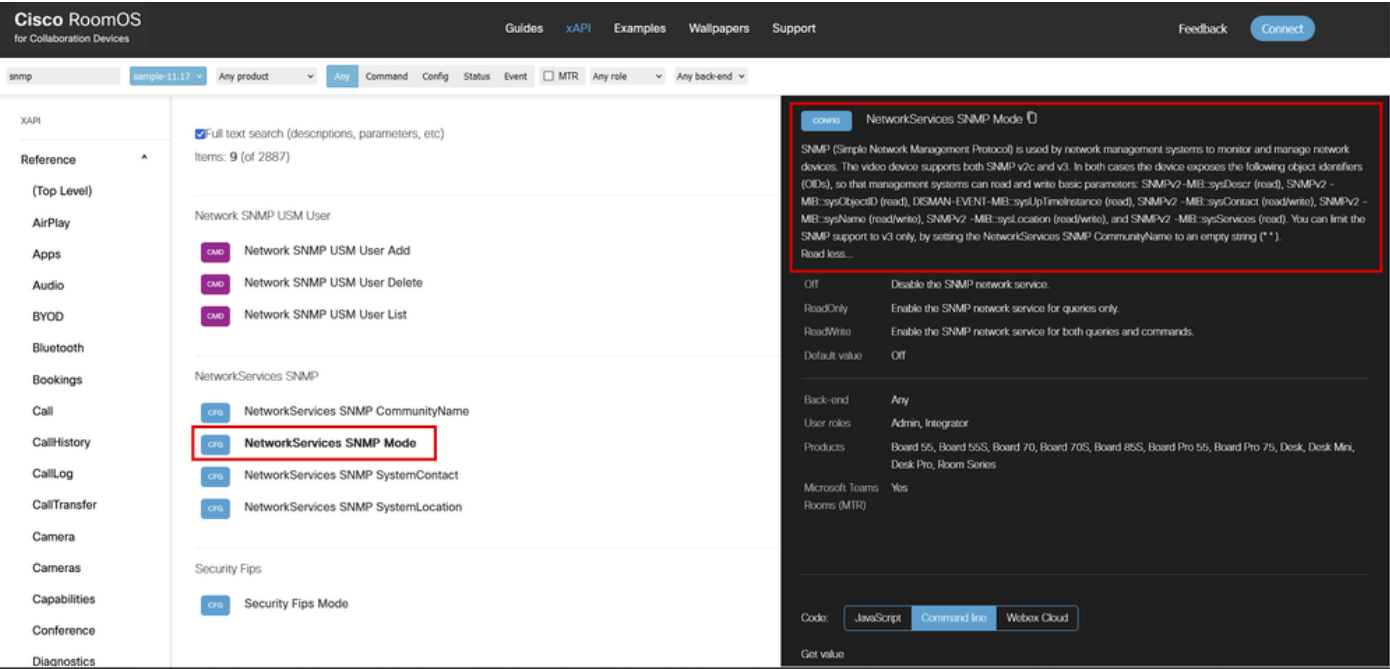
警告：本文仅从终端角度探讨SNMP配置。在网络端完成的任何配置以及用于请求/更新终端上的SNMP相关信息的工具均不属于本文的讨论范围。

TAC不支持对网络中的SNMP进行故障排除，也不能从网络角度对SNMP未按预期运行的原因提供任何推断。您的网络团队必须参与进一步排除这些问题。

SNMP管理可通过多种不同的工具实现。TAC不支持这些工具。如果这些工具从终端收集的信息中存在差异，则网络团队必须首先排除该问题，如果存在足够信息证明这是一个终端相关问题，则在TAC中上报。

可以请求哪些信息

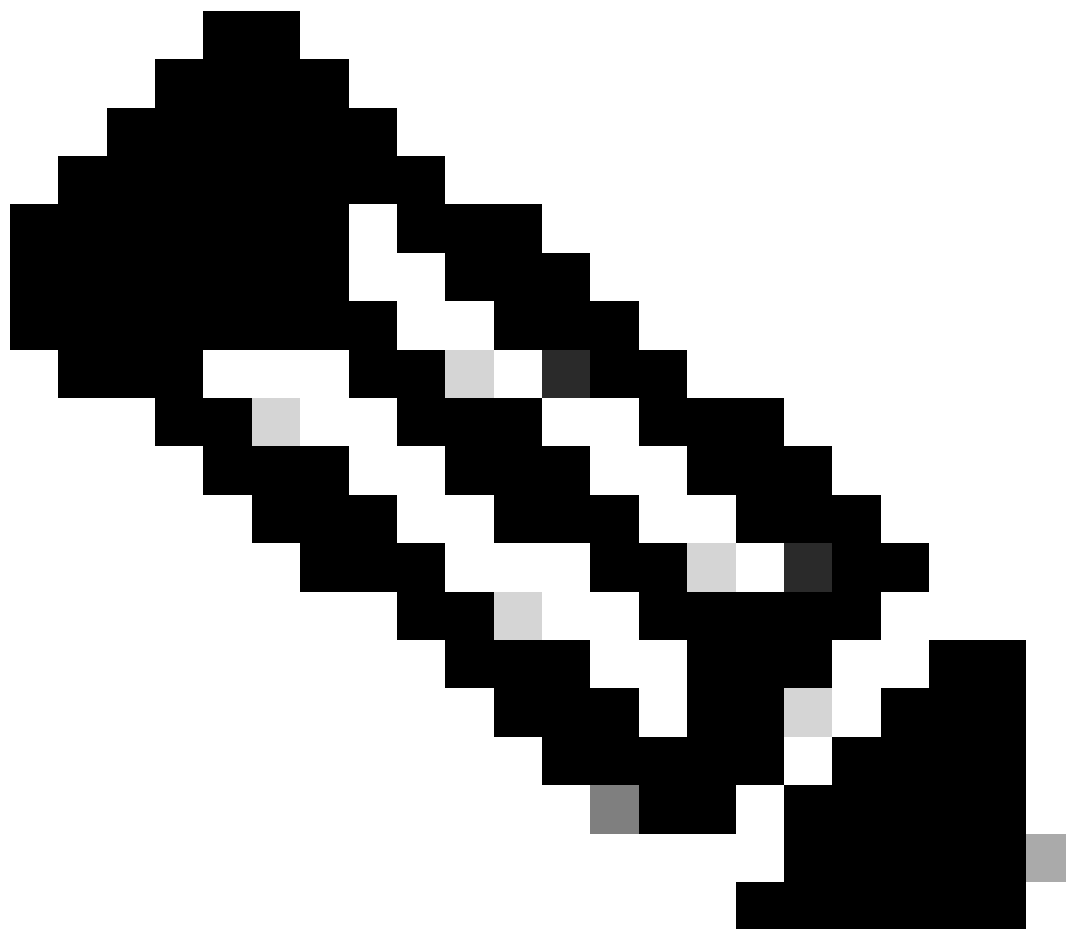
使用SNMP，您可以从终端请求有限数量的信息。在NetworkService SNMP Mode命令说明的详细信息下，可以在此链接中看到支持的OID和MiB:



NetworkService SNMP Mode命令说明，在Room OS xAPI文档中

终端会同时为SNMPv2和SNMPv3显示以下OID:

- SNMPv2-MIB::sysDescr (读取) ,
- SNMPv2 -MIB::sysObjectID (读取) ,
- DISMAN-EVENT-MIB::sysUpTimeInstance (读取) ,
- SNMPv2 -MIB::sysContact (读/写) ,
- SNMPv2 -MIB::sysName (读/写) ,
- SNMPv2 -MIB::sysLocation (读/写) ,
- SNMPv2 -MIB::sysServices (读取) 。

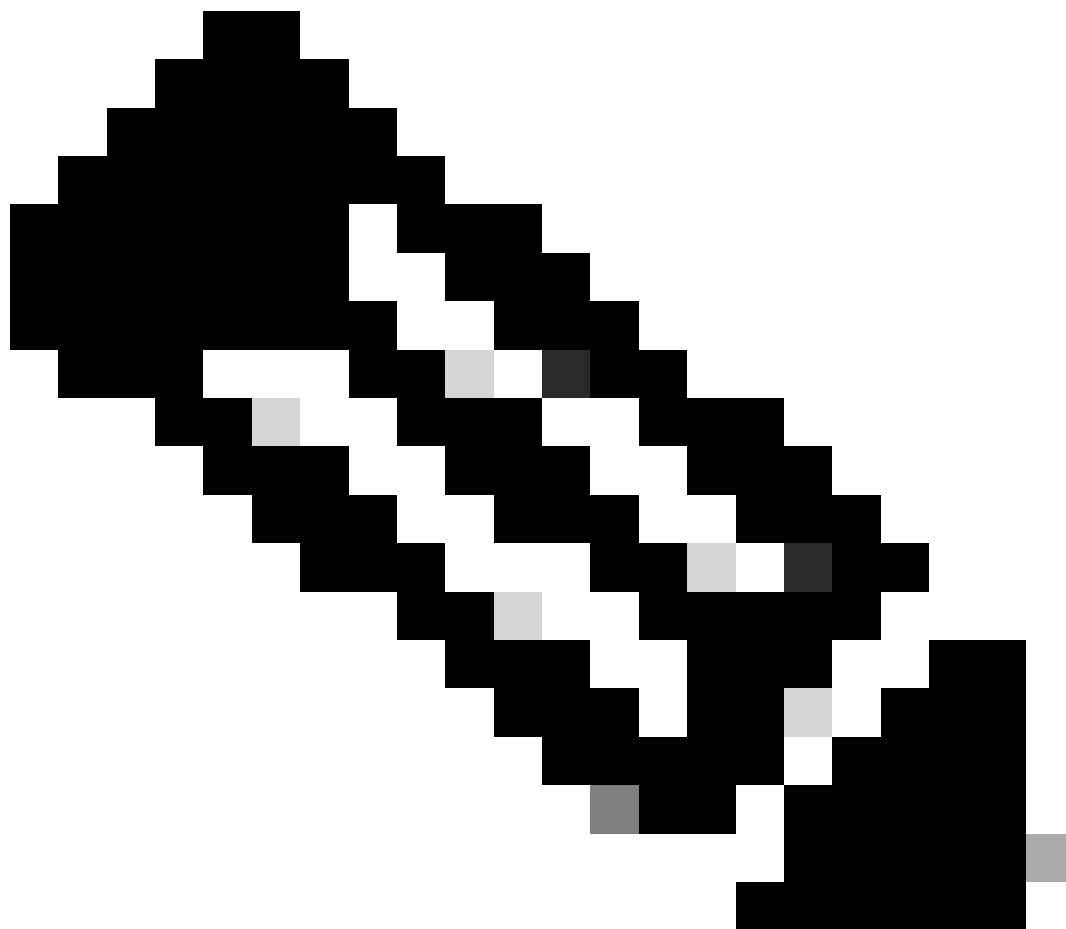


注意：如果只要使用SNMPv3,NetworkServices SNMP CommunityName可以设置为空字符串。

在云注册终端上配置SNMP

通常，终端上的配置更改可以通过四种不同方式进行：

1. 可用的Webex API
2. 终端GUI
3. 控制中心
4. 直接通过SSH连接到终端



注意：要访问终端GUI，请打开浏览器，然后在URL栏中键入终端的IP地址。您需要与终端位于同一网络中，并且您需要具有用户凭证才能登录。

并非所有配置都可以通过所有四种方式进行。对于本文档的场景，可以采用所有四种方式启用SNMP模式，但是，要创建能够通过SNMP与设备通信的SNMP用户，您需要通过SSH连接到终端，或者使用Webex API，或者在Customization部分下的Developer API使用终端的GUI。无法从终端的控制中心所有配置部分创建USM用户。



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:

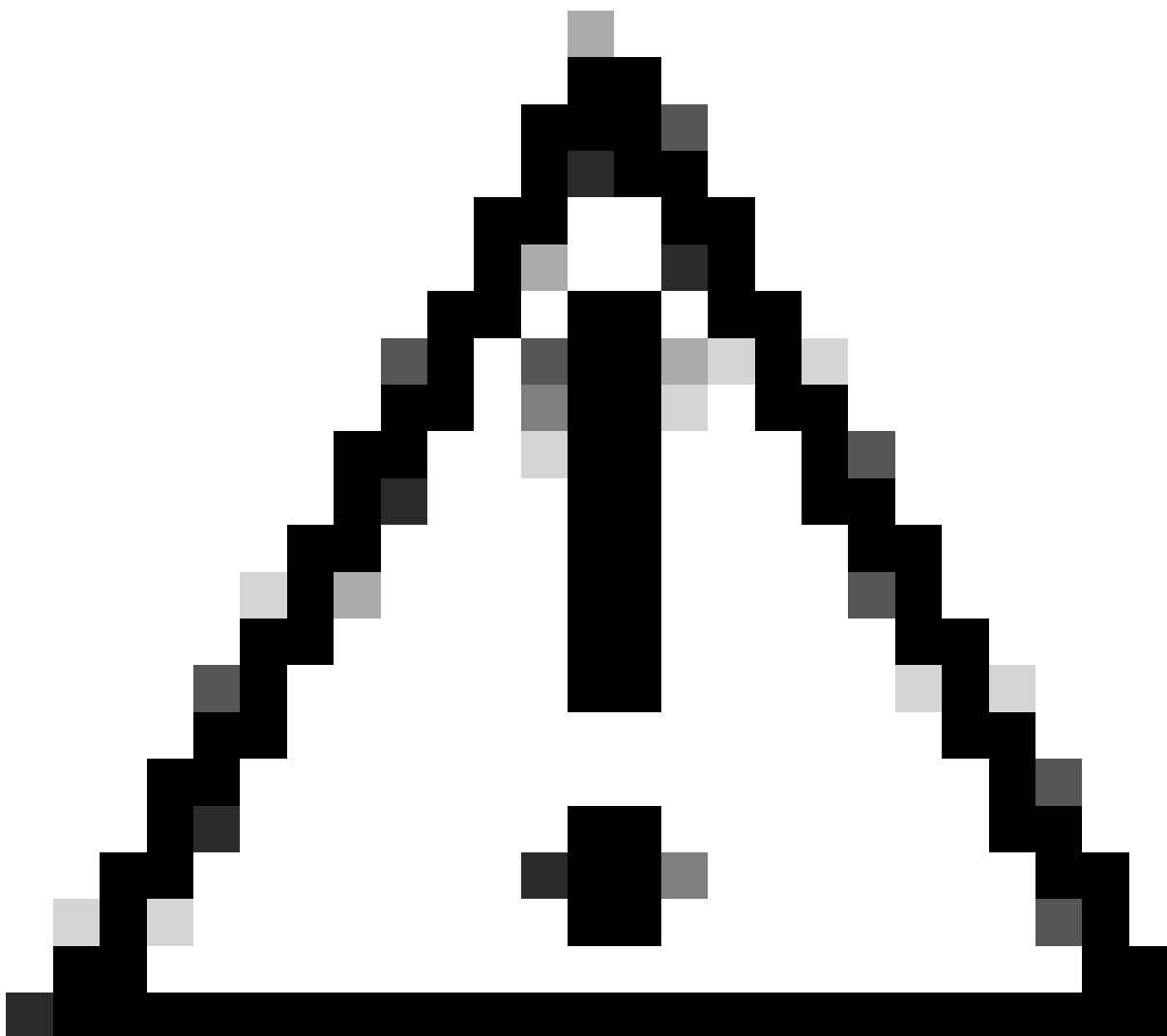
xCommand Dial Number: "person@example.com" Protocol: SIP

xCommand Network SNMP USM User List

Execute

1 of 1 applied successfully.

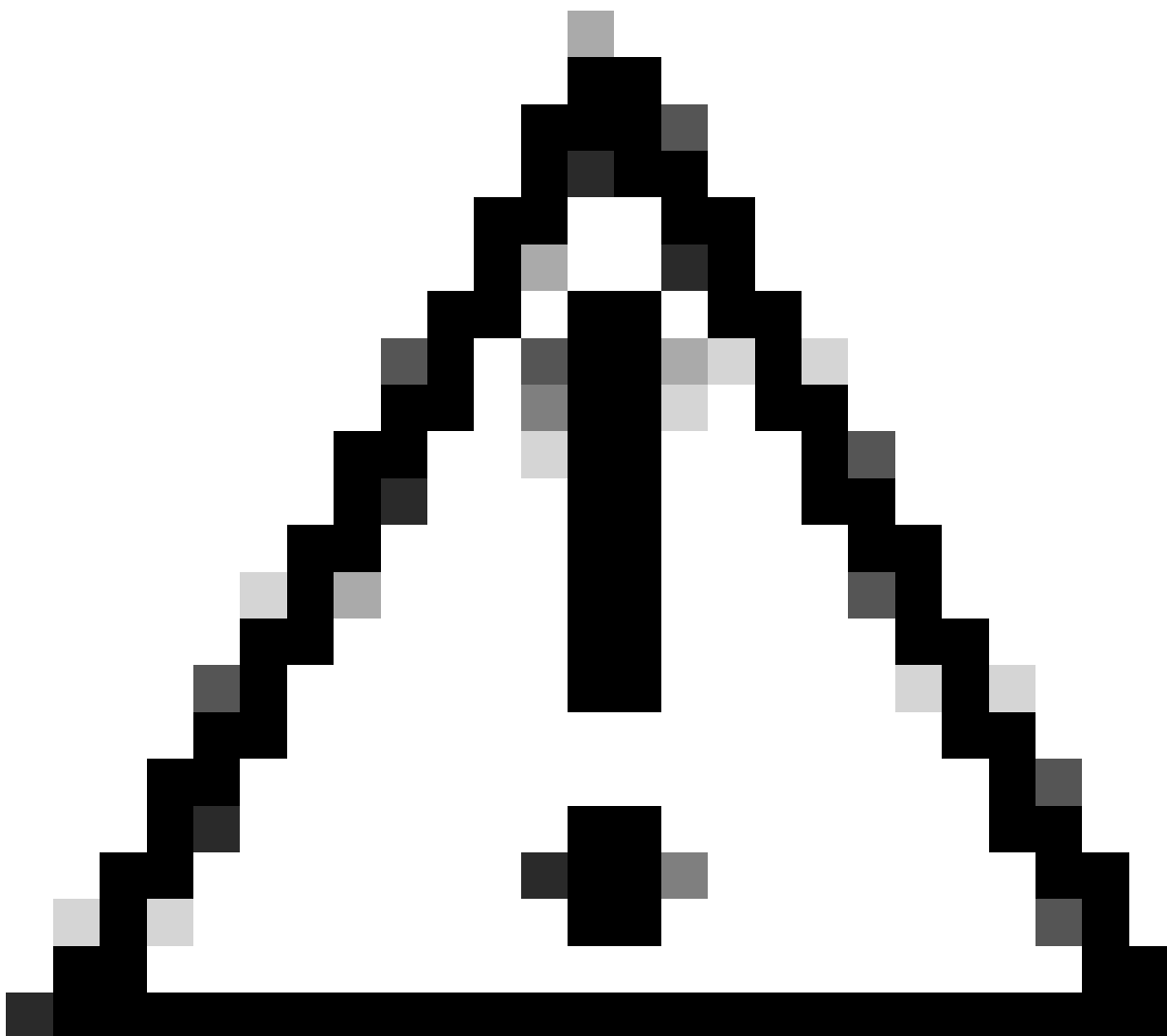
终端GUI上的Developer API部分



警告：在“执行命令和配置”文本框中发出的命令不会返回任何结果。您只看到命令是否已成功执行。这就是为什么列出USM用户的命令不会返回上一个屏幕截图中的任何结果。这意味着您可以从终端的GUI的此部分成功创建USM用户，但是为了仔细检查是否创建了用户，您需要通过SSH连接到设备。

对于配置SNMPv2c，无需创建用户。身份验证使用终端上配置的社区名称（也称为社区字符串）进行。终端的SNMP代理（已存在于设备上）响应与设备上配置的社区名称匹配的请求。如果来自管理系统的SNMP请求不包含匹配的社区名称（区分大小写），消息将被丢弃，并且网络设备中的SNMP代理不会发送响应。

但是，SNMPv3需要配置USM用户才能成功进行身份验证。为此，需要使用网络SNMP USM用户命令。这可以通过直接通过SSH连接到设备或使用开发人员API部分下的设备GUI来实现。或者，可以使用Webex API。

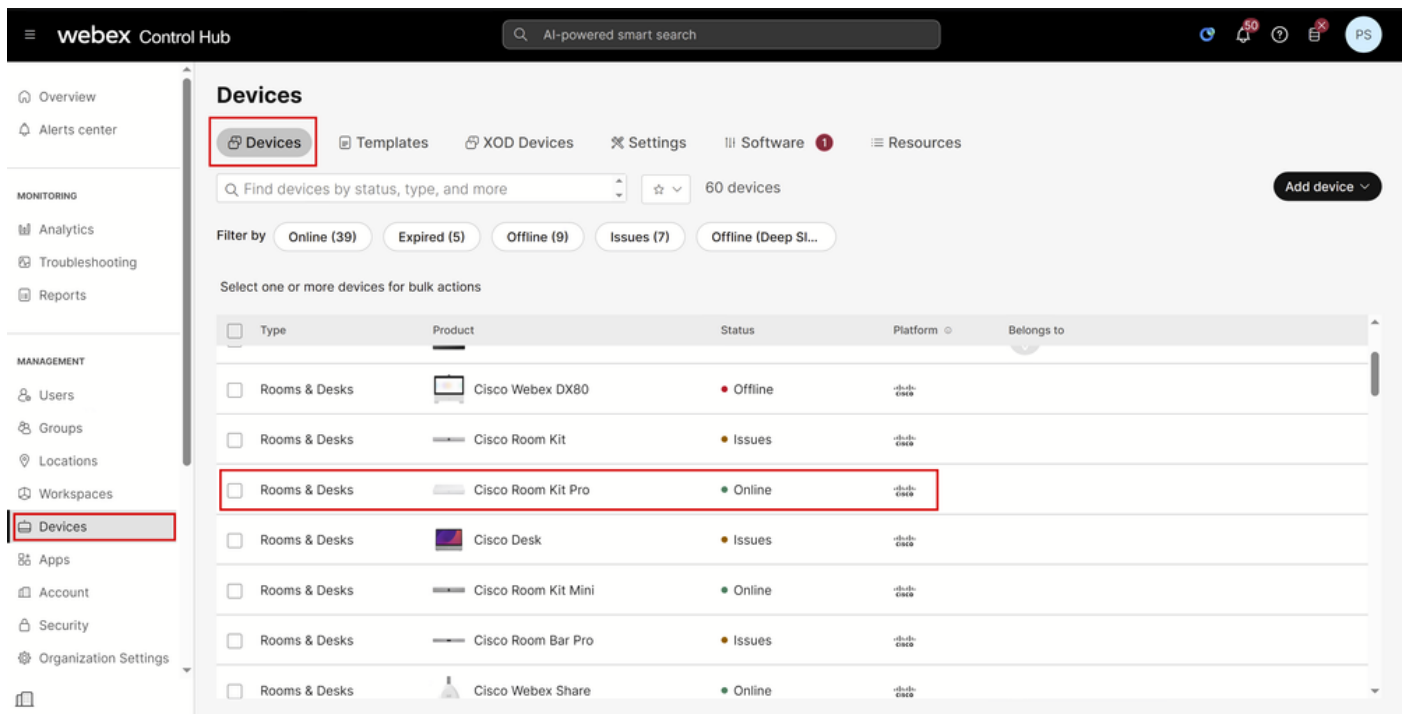


警告：您需要决定是要启用SNMPv2、SNMPv3还是同时启用。思科终端不支持SNMPv1。任何使用SNMPv1的尝试都将失败。

在本文档中，SNMPv2和SNMPv3协议将在Control Hub中启用和配置，但SNMP3身份验证所需的USM用户是在SSH上配置的。

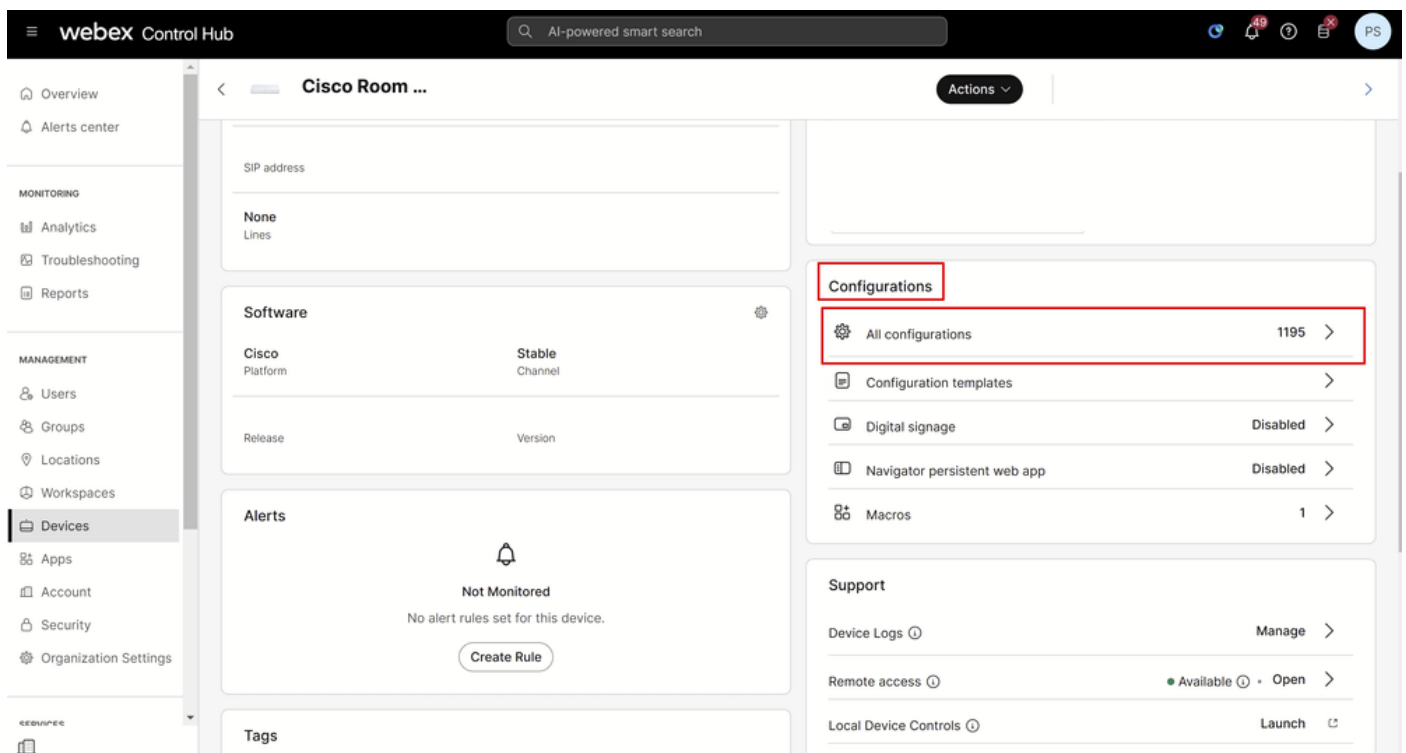
在控制中心启用SNMPv2c模式

导航到admin.webex.com，并使用您的管理员凭据登录。建议为完全管理员。导航到用户界面左侧管理部分下的设备。在Devices选项卡下，选择要配置的设备。在本例中，使用Cisco Room Kit Pro。



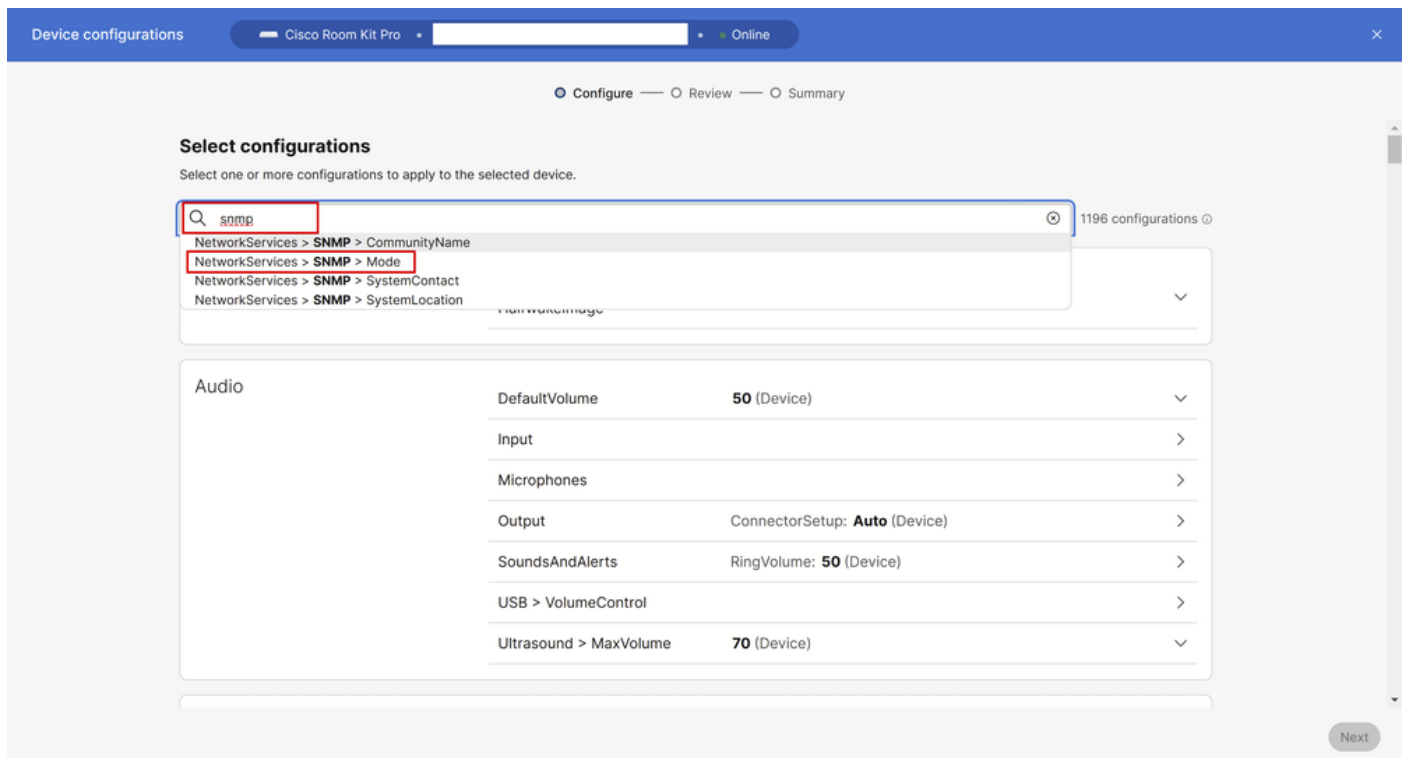
Control Hub Devices部分

在打开的新Control Hub页面中的设备详细信息下，导航到配置部分并点击所有配置：



Room Kit Pro的控制中心设备详细信息

在搜索栏中，键入snmp，然后选择NetworkServices > SNMP > Mode:

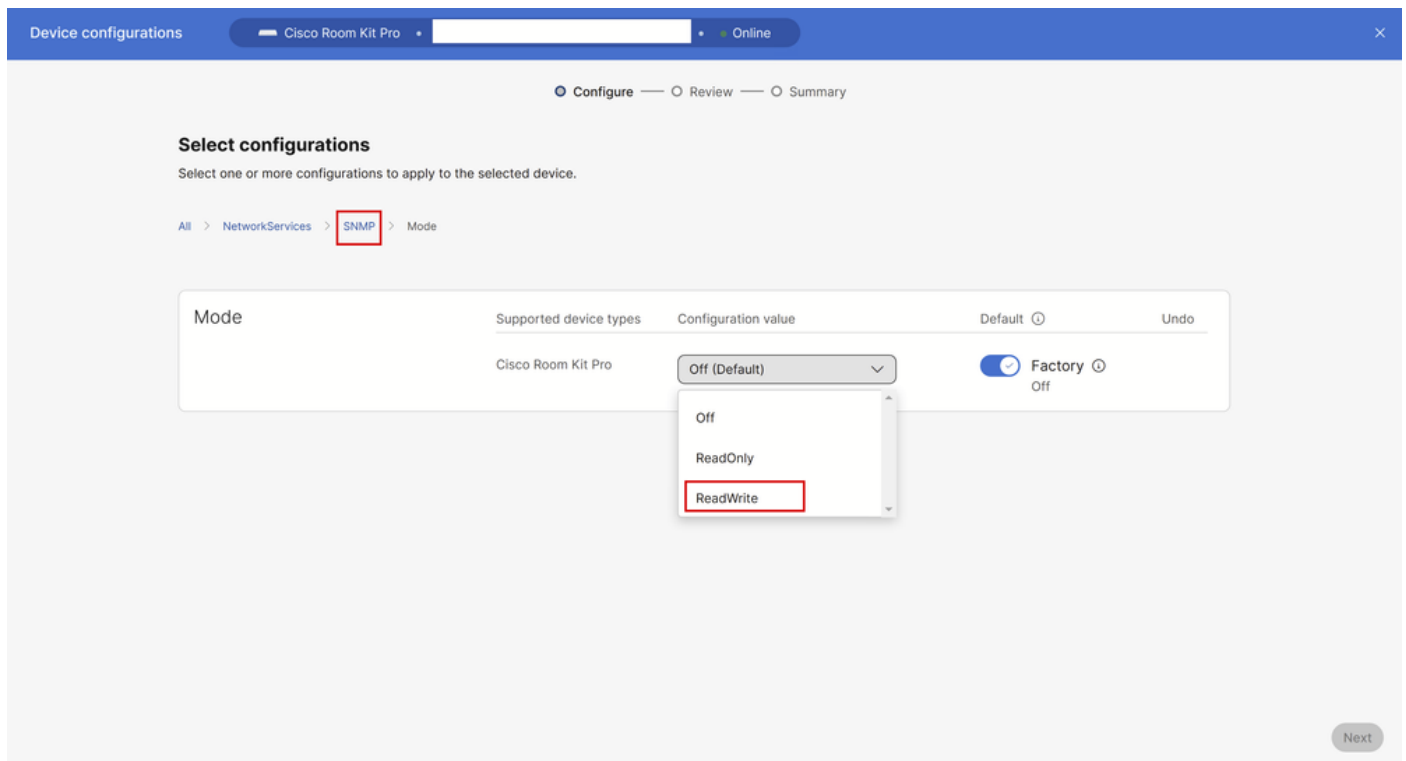


控制中心所有配置窗口

选择需要在环境中启用的模式。有三种选项可供选择：

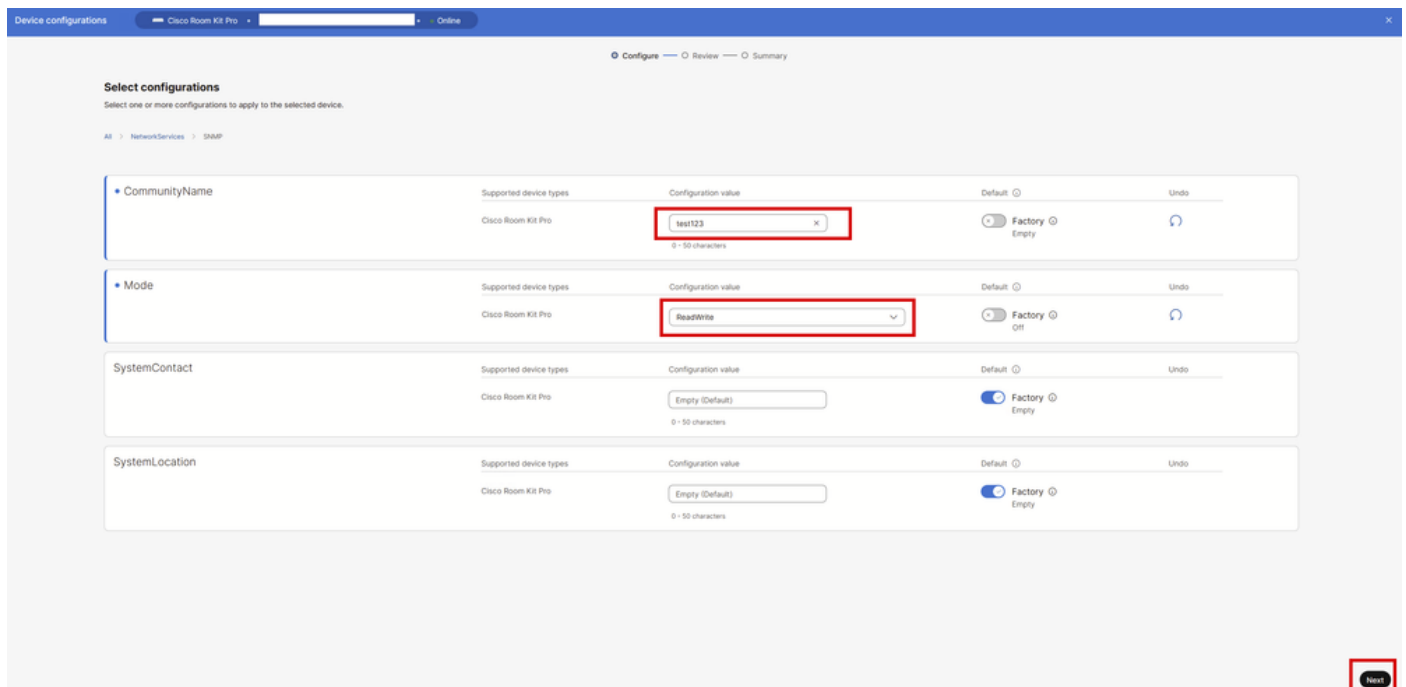
1. 关闭:禁用SNMP网络服务。
2. 只读：仅为查询启用SNMP网络服务。
3. 读写：为查询和命令启用SNMP网络服务。

在本示例中，ReadWrite处于选中状态。然后，单击“设置”导航部分中的SNMP，如图所示。这将使您返回到设置中的一个步骤，并且您可以查看所有可以通过Control Hub在设备上配置的SNMP相关设置：



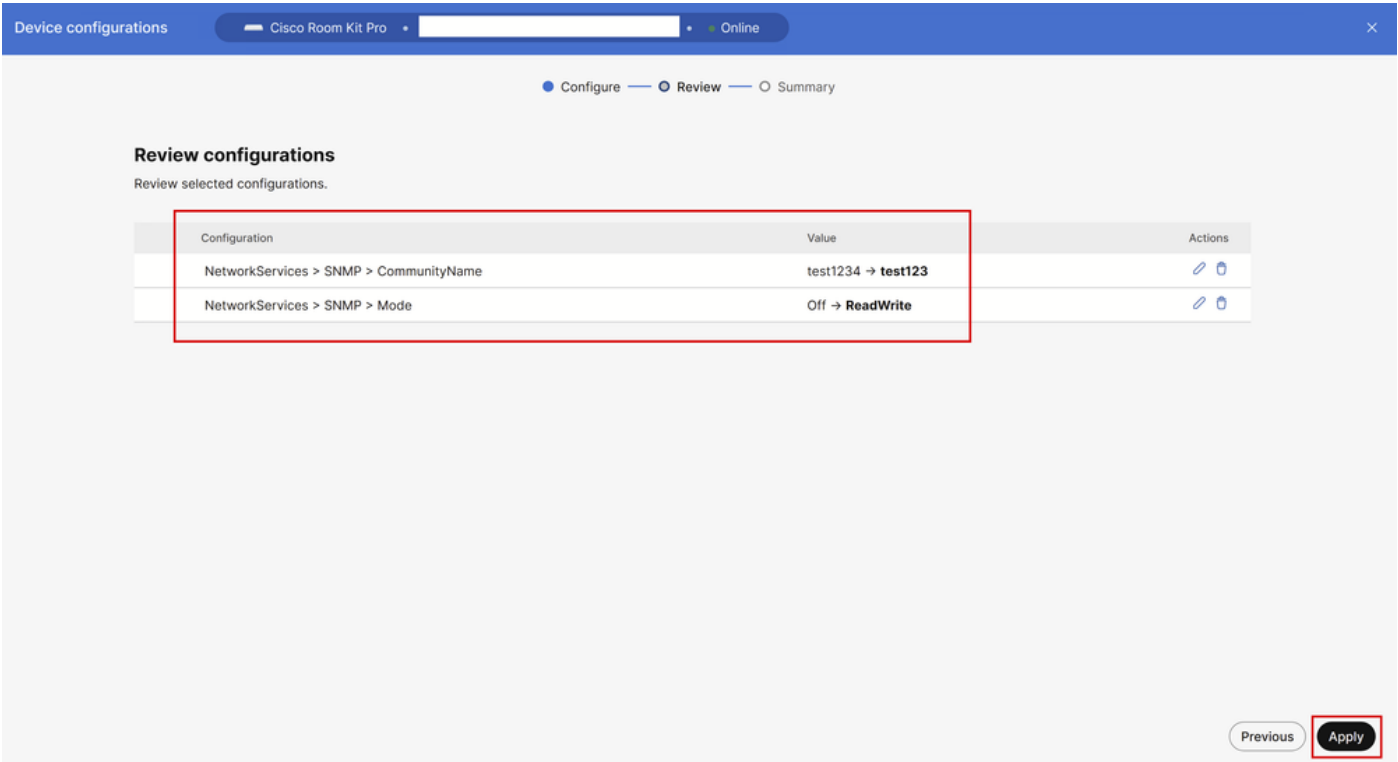
控制中心中所有配置下的SNMP模式设置

单击SNMP后，将显示所有可用的SNMP选项，如图所示。要成功设置SNMPv2，需要设置社区名称。社区名称用于在SNMP服务器与终端上存在的SNMP代理之间进行身份验证。在本示例中，社区名称设置为test123。点击右下角的Next。



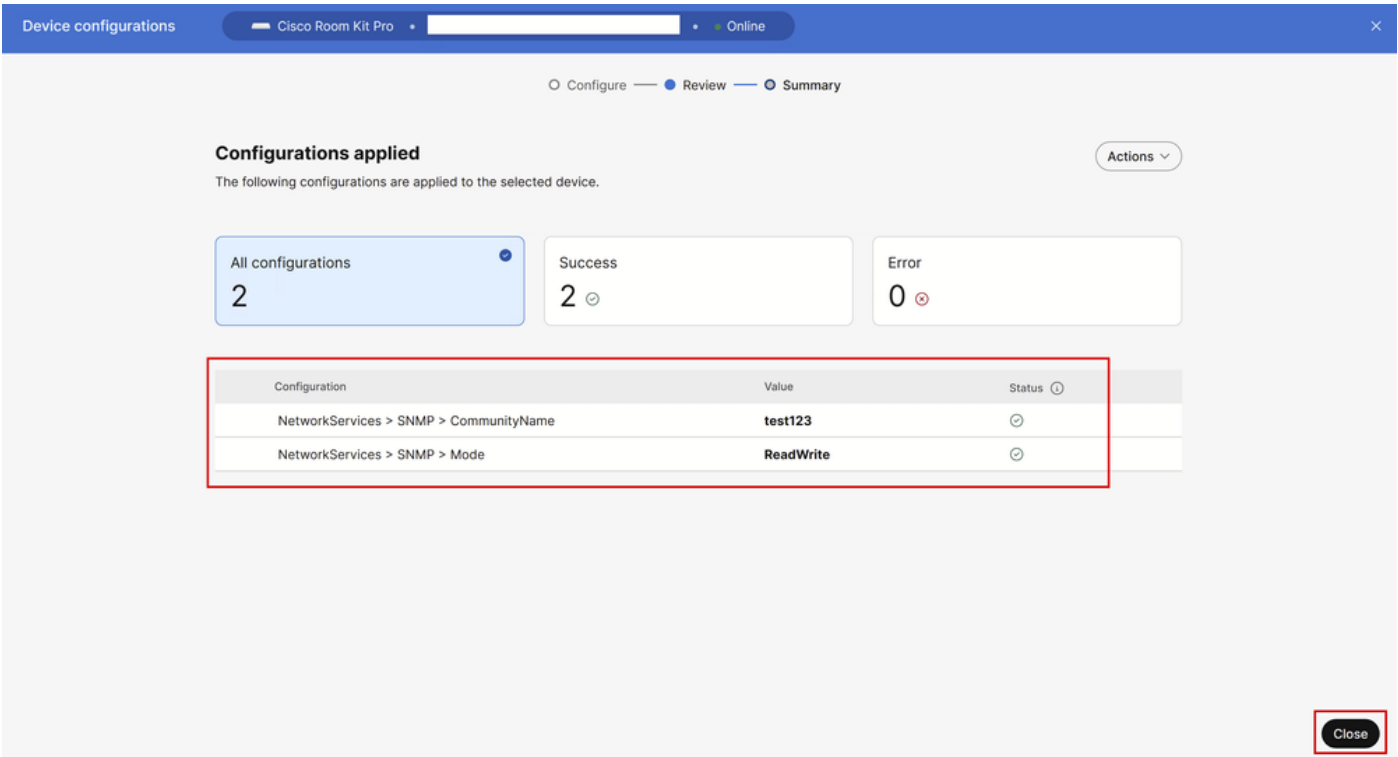
Control Hub中所有配置下的SNMP设置

查看设备配置，然后点击右下角的Apply:



在应用更改之前检查配置

确认配置更改已成功应用。然后，单击Close。



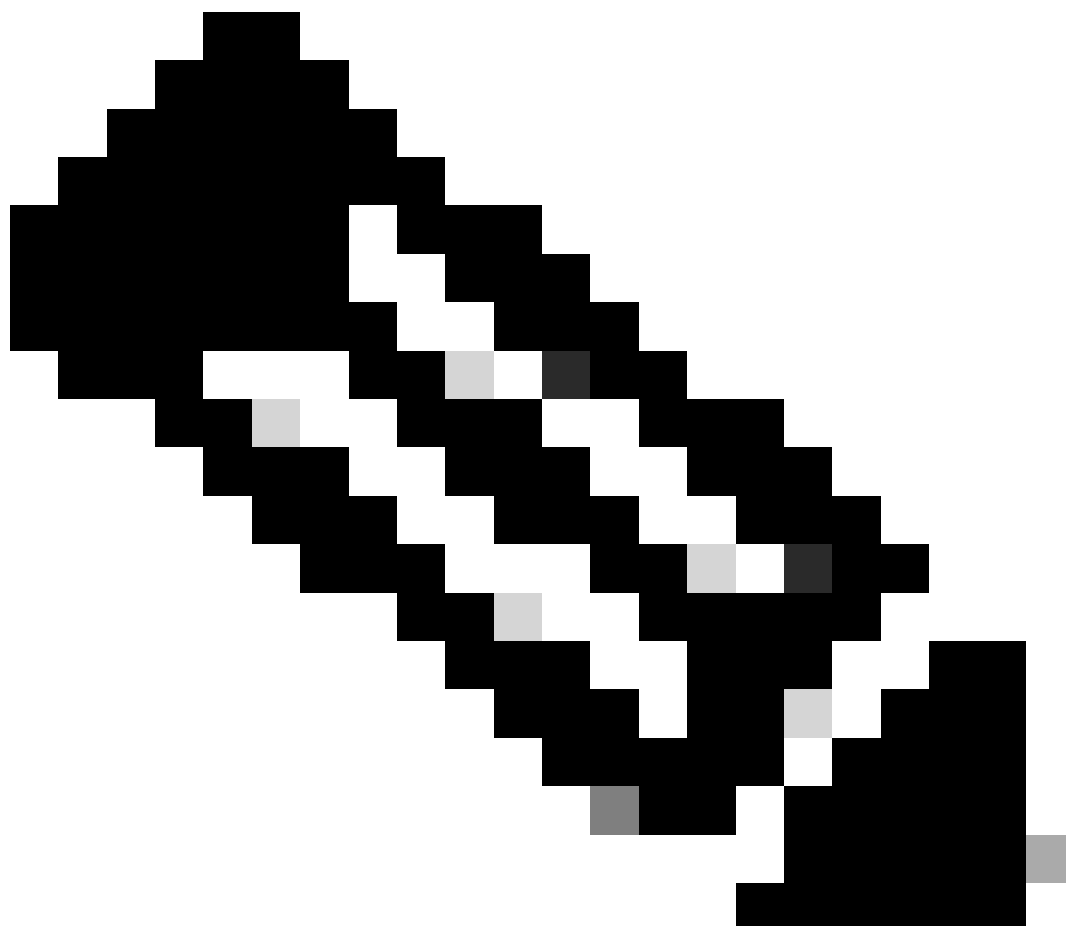
终端配置已成功应用于控制中心

在此阶段，在终端上成功启用SNMPv2c，并设置社区名称。

在控制中心启用SNMPv3模式

与SNMPv2c相比，SNMPv3可提供更高的安全性，并且需要在终端上进行不同的配置。导航至Control Hub中的Management部分下的Devices。在设备选项卡下并选择要使用SNMPv3配置的终端之一。在本示例中，使用思科房间栏专业版。

在设备详细信息下，导航到配置部分并点击所有配置。系统将打开“设备配置”(Device Configurations)页面。在搜索栏中键入snmp，然后选择NetworkServices > SNMP > Mode。在本示例中，SNMP模式设置为ReadWrite。单击SNMP查看设备上的所有可配置SNMP设置。



注意：在前一个示例中配置SNMPv2c时，已经介绍了至今提到的SNMPv3的所有步骤。因此，未提供步骤的截图。如果在如何浏览控制中心设置方面有任何疑问，请参阅在控制中心启用SNMPv2c模式部分。

要仅支持SNMPv3，您需要将社区名称设置为由引号括起的空字符串。

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

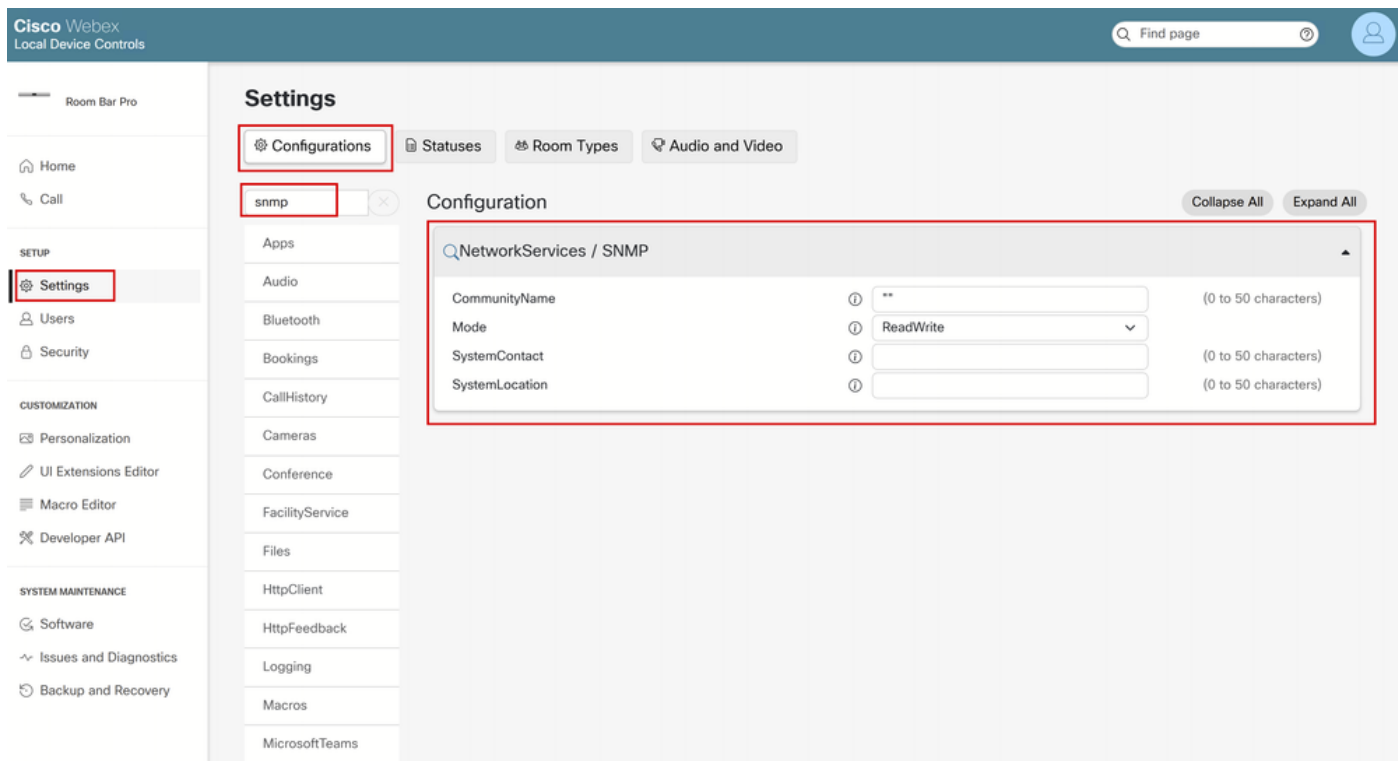
Control Hub中所有配置下的SNMP设置

单击下一步，然后查看配置更改，然后单击应用。单击Close关闭设备配置页面。

可在控制中心执行的配置到此结束。在此阶段，仅启用SNMPv3。

终端GUI中的SNMP配置如何

可以从设备GUI执行相同的配置。打开浏览器选项卡并键入终端的IP地址（您需要与终端位于同一网络中）。以admin用户身份登录，在终端GUI中，导航到SETUP部分下的Settings。在配置选项卡上，并在设置搜索栏中键入snmp。此图显示了如何显示前一部分的Room Bar Pro上完成的SNMPv3配置的SNMP设置：



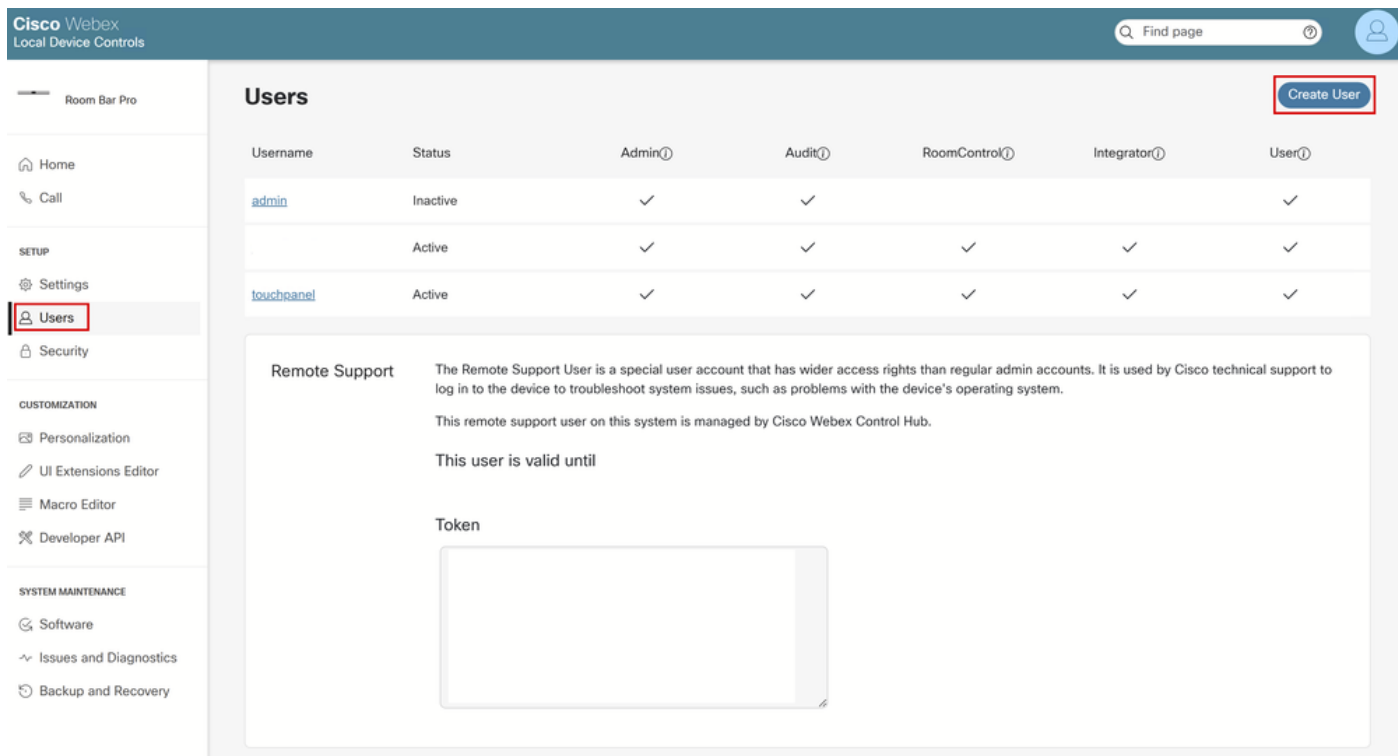
终端GUI上的SNMPv3配置

为SNMPv3配置USM用户

为了能够使用SNMPv3，您需要创建USM用户。执行此操作的可用命令可在此处[的Room OS文档链接](#)中找到。使用SSH连接到设备。为此，需要在设备上拥有管理员帐户。如果不是，则需要创建管理员帐户。本节将介绍整个过程。

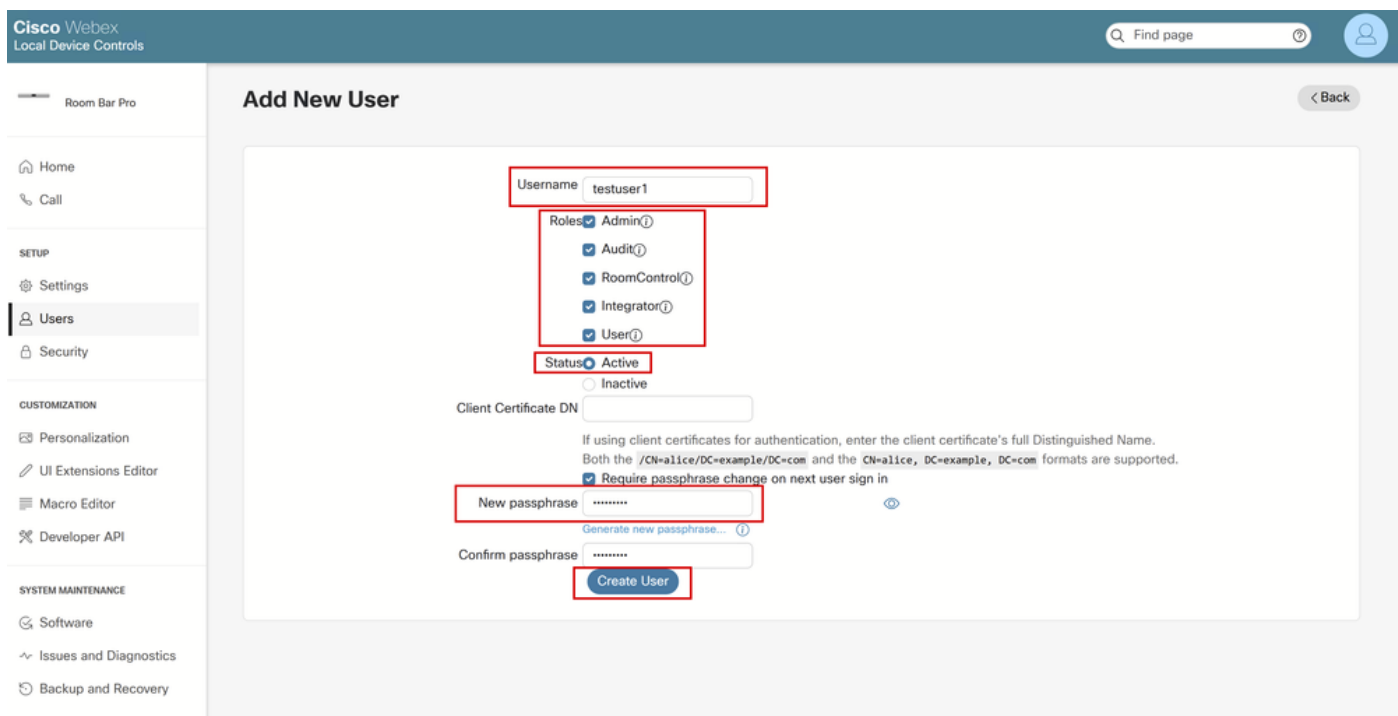
导航至Control Hub中的Management部分下的Devices。保留在设备选项卡下，并选择要为其创建管理员用户的终端之一。在本例中，使用Cisco Room Bar Pro。

在设备详细信息下，导航到Support部分并点击Local Device Controls（您需要与终端位于同一网络中才能使用此功能）。设备GUI打开。导航到SETUP部分下的Users，然后单击Create User。



终端GUI中的Users部分

提供用户名和口令（密码）。确保用户具有完全管理员权限并且处于活动状态：



从终端的GUI创建用户

从Users页面验证用户是否已创建且处于活动状态：



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	✓	✓	✓	✓	✓
testuser1	Active	✓	✓	✓	✓	✓
touchpanel	Active	✓	✓	✓	✓	✓

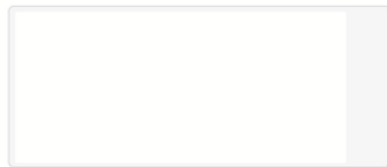
Remote Support

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.

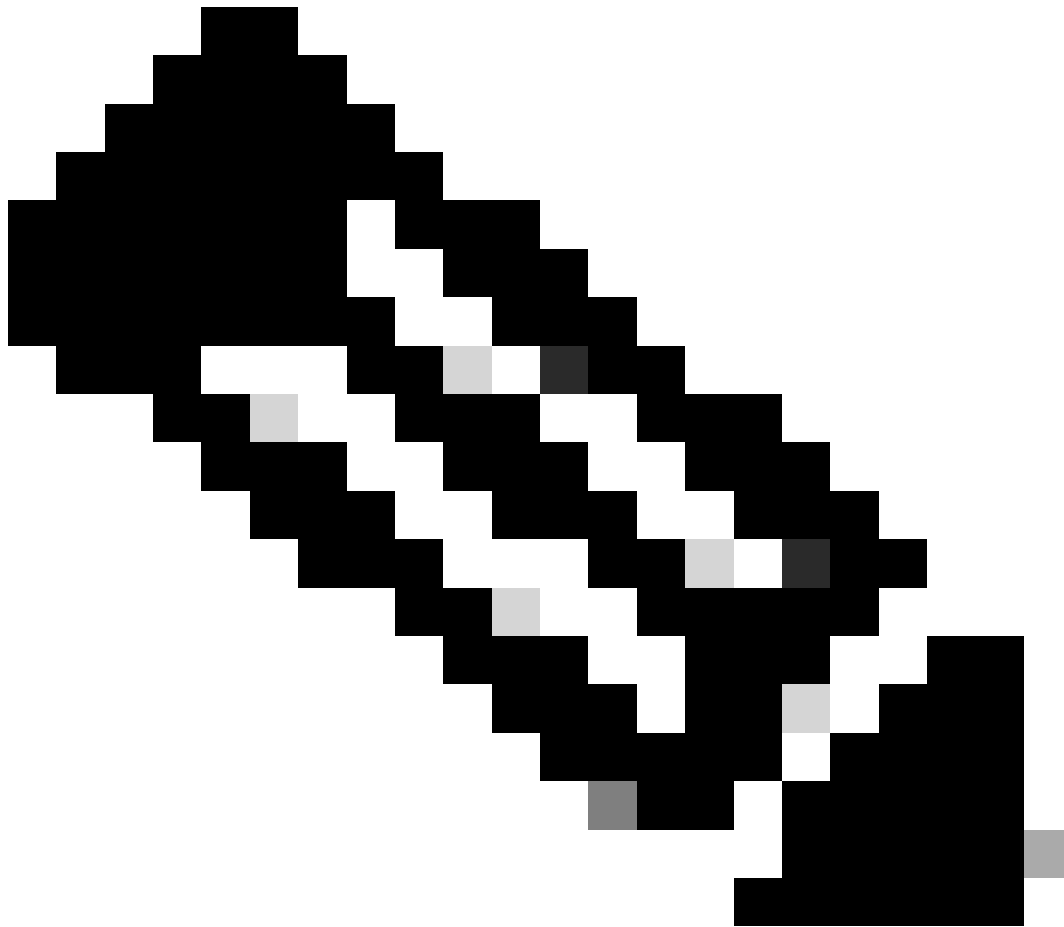
This remote support user on this system is managed by Cisco Webex Control Hub.

This user is valid until

Token



已创建新用户并在其他用户中列出



注意：首次尝试使用新创建的用户进行SSH登录时，系统会要求您更改密码。您会看到类似以下内容的提示：

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

首次使用SSH时更改密码

更改密码后，您将立即断开连接，需要启动新的SSH连接。

成功创建管理员用户后，使用您选择的SSH客户端并连接到终端。使用管理员凭证登录。以下是您看到的提示符：

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

通过SSH成功登录终端尝试

如本文所述，使用Network SNMP USM User Add命令。在本演示中，使用的命令为：

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

此命令的结果是，成功后：

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

通过SSH创建USM用户

要使命令执行无错误，您需要遵守此链接中共享的命令文档中所述的某些[规则](#)。为方便起见，在撰写本文时此命令的当前要求已粘贴在此图片中，但您必须在创建用户时确保参考此[链接](#)。在图片末尾，请注意该命令有确切的语法。

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文档中的USM用户创建命令语法



警告：如果出现拼写错误或未满足要求，该命令将返回错误，并且不会创建用户。提供了一个示例，其中不提供至少包含8个字符的隐私密码，而是提供长度较短的7个字符的密码：

```
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.

由于密码短，USM用户创建失败

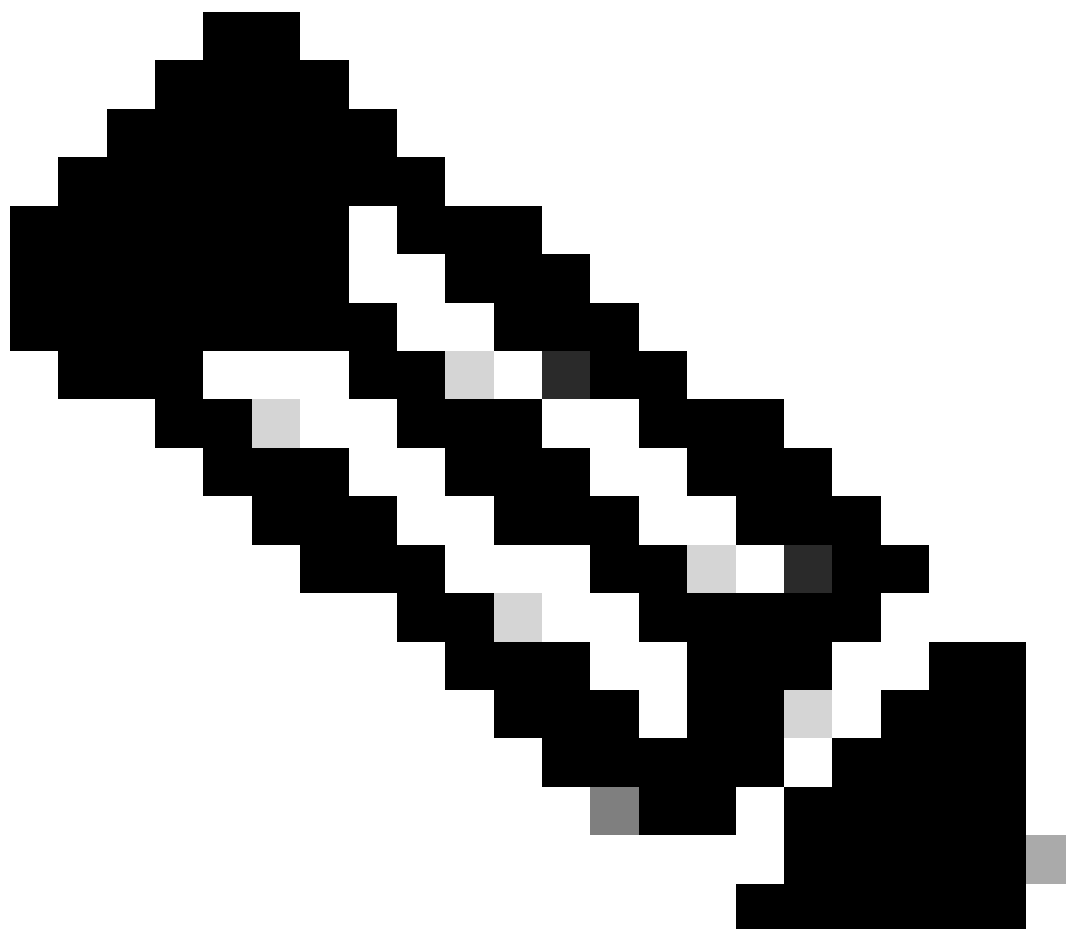
您可以使用Network SNMP USM User List命令测试您的用户是否已创建。此命令列出设备上存储的所有USM用户：

```
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
```

用于确认用户创建的网络SNMP USM用户列表命令

在此阶段，已确认已成功创建用户psitaras。SNMPv3配置已完成。



注意：在终端的GUI的Users部分下，USM用户窗格不可见。这是预期结果。

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

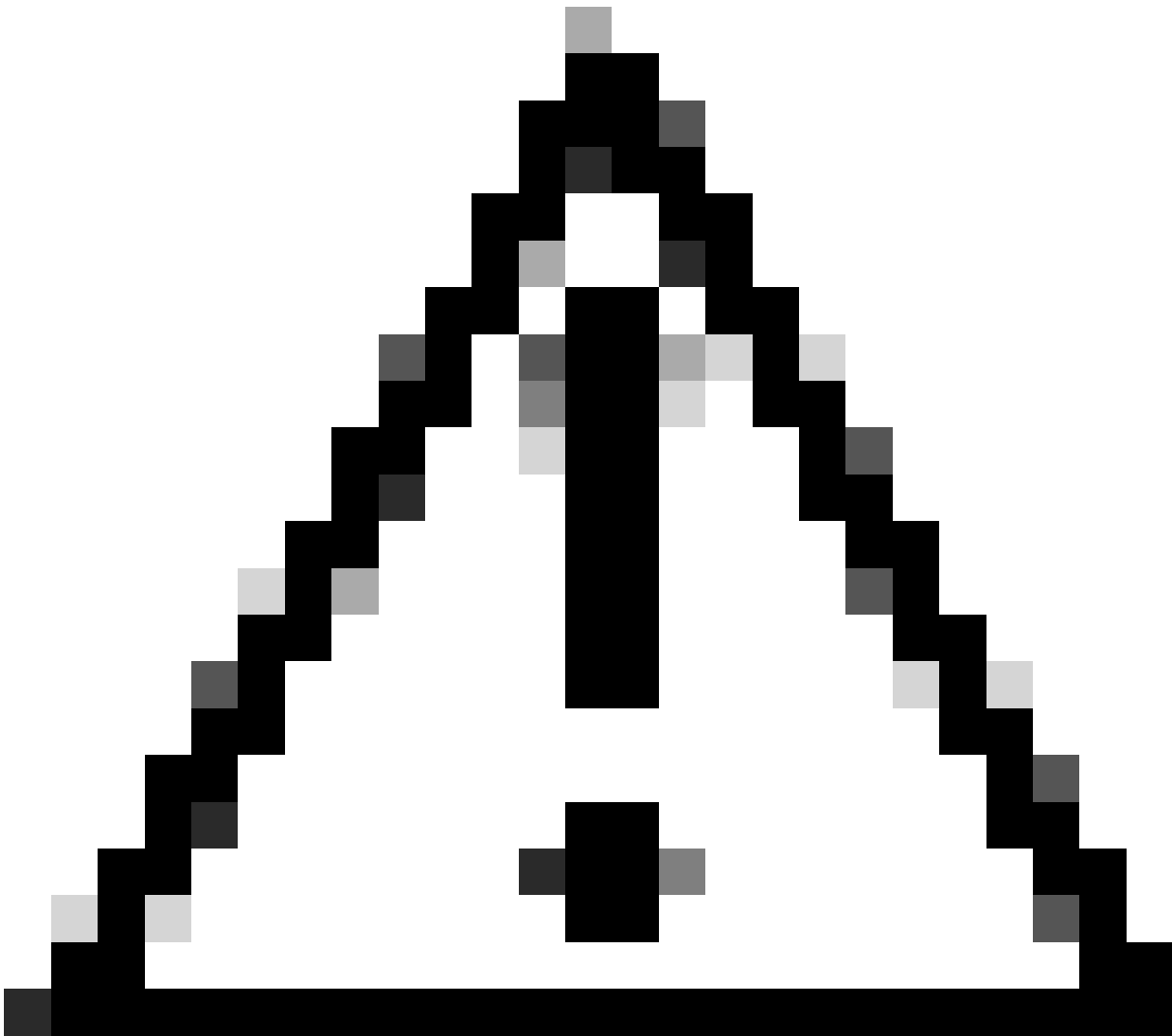
Token

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

USM用户在终端的GUI中的用户下不可见

测试SNMPv2c和SNMPv3配置

在此阶段，您可以继续使用网络管理系统(NMS)测试SNMPv2c和/或SNMPv3配置。对于本文而言，实验配置不包含任何运行SNMP服务的NMS或SNMP服务器。为了测试配置，使用名为snmpwalk的实用程序。此实用程序安装在Linux服务器上。



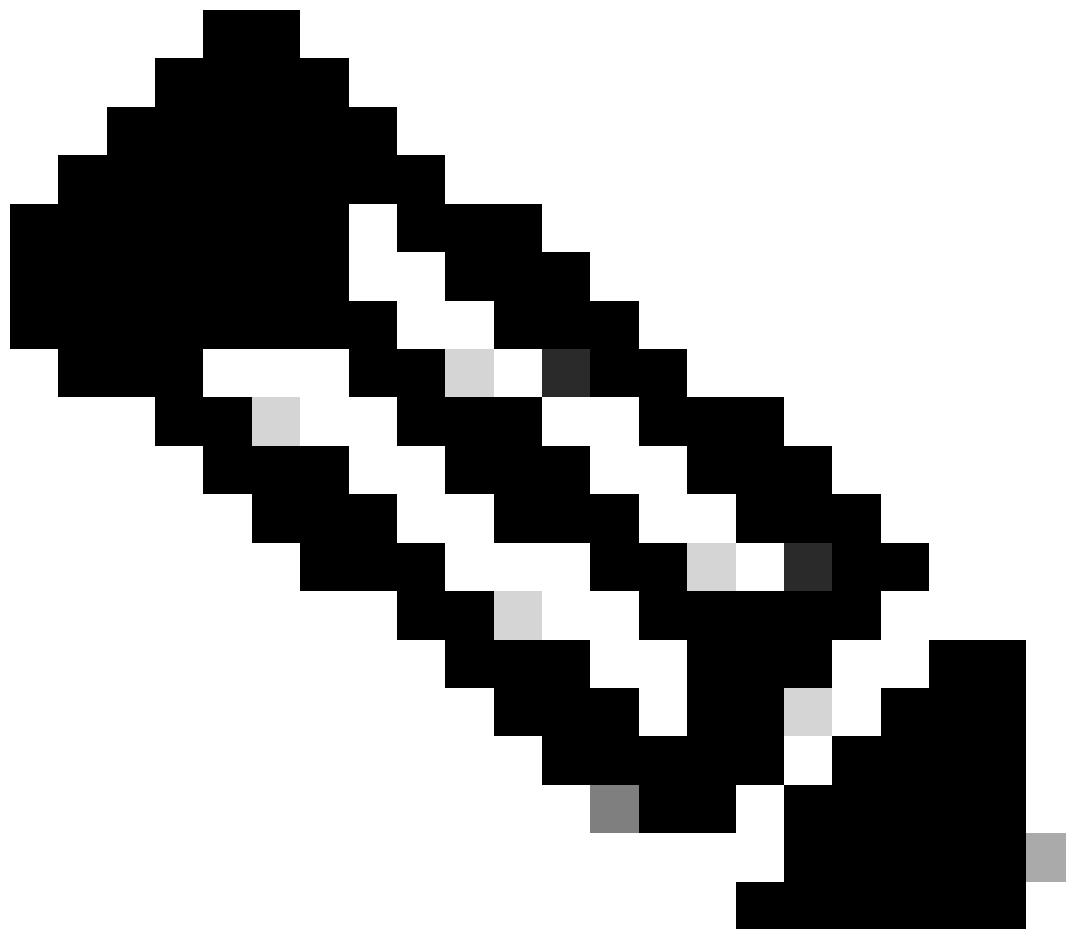
警告：建议不要使用Snmpwalk来测试协作终端上的SNMP配置。TAC工程师不支持该工具，您在继续测试之前需要熟悉该工具的使用方法。您可以使用任何其他SNMP工具或NMS来测试配置，而非snmpwalk。在本文中，Snmpwalk仅用作示例（需要工具测试配置以用于演示目的），并且没有与使用相关的承诺或促销。

安装snmpwalk不属于本指南的一部分，因此省略。根据您用于测试的计算机的操作系统(OS)，安装要求可能有所不同。在测试之前，您必须设法成功安装它。

Snmpwalk是一个可用于验证SNMP配置的工具。它执行终端的MiB遍历并返回可用信息。云注册的终端公开7个对象标识符(OID):

- SNMPv2-MIB::sysDescr (读取) ,
- SNMPv2 -MIB::sysObjectID (读取) ,
- DISMAN-EVENT-MIB::sysUpTimeInstance (读取) ,
- SNMPv2 -MIB::sysContact (读/写) ,
- SNMPv2 -MIB::sysName (读/写) ,
- SNMPv2 -MIB::sysLocation (读/写) ,

- SNMPv2 -MIB::sysServices (读取) 。
-



注意：用于所列举的snmpwalk测试的内部IP是私有IP，不再使用。本指南使用的实验已停用，设备已重置为出厂设置。

Cisco Room Kit Pro终端配置了SNMPv2c。身份验证使用社区字符串进行。发出以下命令：

```
# '-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
```

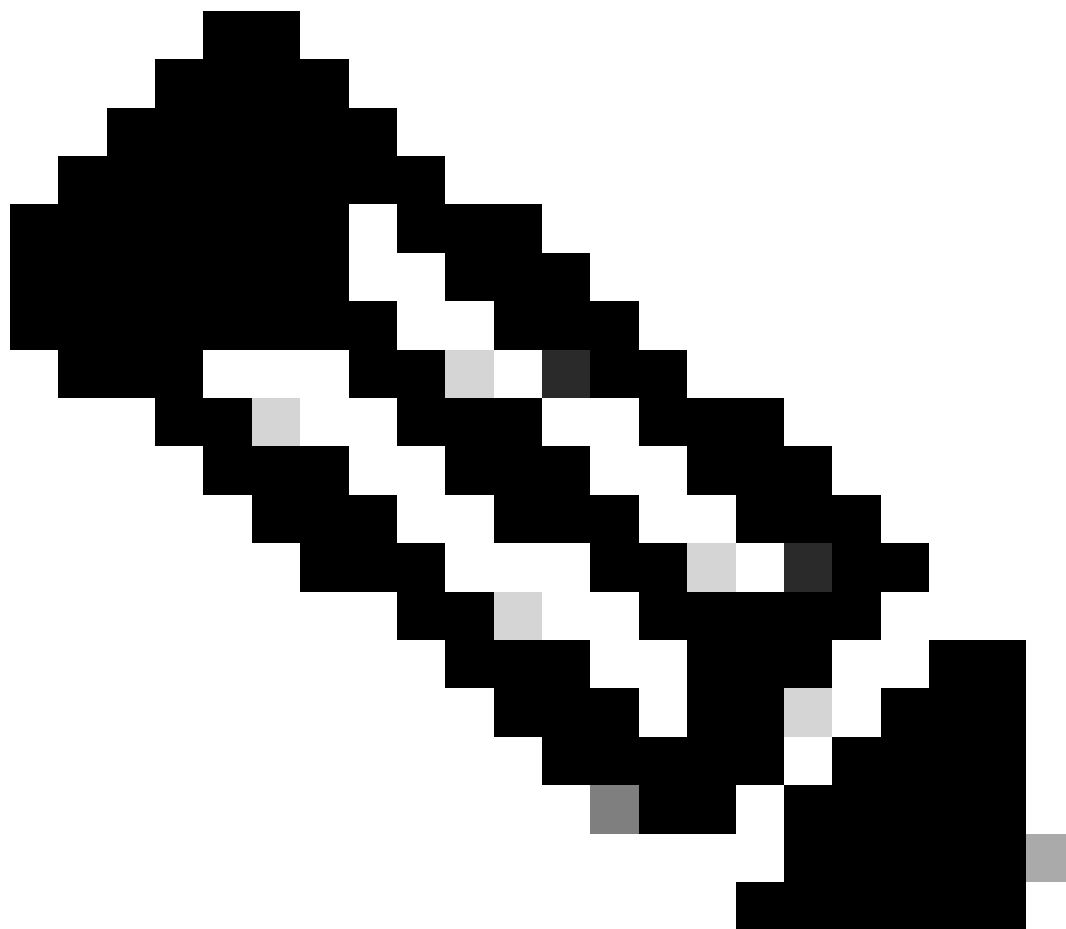
```
iso.3.6.1.2.1.1.3.0 = Timeticks: (106770681) 12 days, 8:35:06.81
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = ""
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.7.0 = No more variables left in this MIB View (It is past the end of the MIB tree)
```

Snmpwalk按预期返回7个结果。有三个MiB是空的：

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

有三个xConfiguration命令可用于设置这些MiB的值。通过SSH连接到终端并发出以下命令：

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



注意：您可以从Control Hub、终端GUI或Webex API对这些设置进行更改，而不是使用这三个命令。

发出上述命令后，在同一终端上再次使用snmpwalk。您会发现，以前空的MiB会填充通过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)

在此阶段，确认在Room Kit Pro设备上进行的SNMPv2c配置运行正常。

Cisco Room Bar Pro端点配置了SNMPv3。对于SNMPv3，您需要确保使用正确的身份验证。未使用社区字符串。相反，SNMPv3使用用户名和密码。

```
# '-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)
```

在此阶段，确认在Room Bar Pro设备上创建的SNMPv3配置运行正常。

终端是否可以同时激活SNMPv2c和SNMPv3

是的，这是可能的。但是，在SNMP配置期间，您需要设置社区名称以便能够进行SNMPv2c身份验证。在本测试中，使用先前示例中的Room Bar Pro。终端的Control Hub All Configurations部分的当前配置为：

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

Mode

Supported device types

Configuration value

Default

Undo

Cisco Room Bar Pro

ReadWrite

Off

请注意，社区名称不为空。有两个引号，表示社区名称为空字符串。通过将NetworkServices SNMP CommunityName设置为空字符串(""), 可以将SNMP支持限制为仅版本3。 您需要将此字符串替换为团体名称，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Control Hub终端配置设置中添加SNMPv2c的社区名称

已确认SNMPv3在Room Bar Pro上运行。Snmpwalk用于在设置社区名称后测试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)
```

是否可以通过SNMP控制集线器配置多个终端

可以，可以在控制中心中同时配置多个设备。本文[在配置多个设备部分](#)下提供了有关如何逐步执行该操作的信息。

需要记住的重要详细信息

- 只有特定的MiB可用。可用MiB的数量受设计端点的工程团队的设计限制。MiB无法展开或增强以提供更多信息。
- SNMPv2c使用社区名称（也称为社区字符串）进行身份验证，而SNMPv3使用用户名和密码

进行身份验证，并提供加密。测试时，确保您对已配置的协议使用正确的身份验证方法（使用 snmpwalk 或其他工具/NMS）。

- SNMPv3 上始终启用身份验证和隐私。终端仅支持 authPriv 安全级别，并且隐私协议始终为高级加密标准(AES)。
- SNMPv3 仅支持基于用户的安全模型(USM)选项。不支持 TLS 上的 SNMPv3。
- 用于配置用户以进行 SNMP 身份验证的 USM 用户命令对 SNMPv2c 没有影响。
- 终端上的 SNMP CommunityName 设置对 SNMPv3 配置没有影响。
- SNMP CommunityName 区分大小写。
- 通过将 NetworkServices SNMP CommunityName 设置为空字符串(""), 可以将 SNMP 支持限制为仅 v3。
- 不支持 SNMPv1。
- 对于 SNMPv2c 和 SNMPv3，终端显示相同的对象标识符(OID)。
- 对于 SNMPv3，身份验证协议需要在 SHA-2 系列中（不支持 MD 或 SHA-1）。如果不是，则 SNMP 请求无法进行身份验证且保持未应答状态。
- 隐私密码作为本地散列值(AES-128)存储在设备上。如果未在此参数中显式设置隐私密码，则将其设置为与身份验证密码相同（使用在 Authentication Protocol 参数中指定的哈希函数）。
- 密码/口令和用户名需要位于特定的长度范围内。例如，USM 用户名需要最多 32 个字符，身份验证密码需要最少 8 个字符，最多 255 个字符。如果不满足这些要求，则 Network SNMP USM User Add 命令无法创建用户并返回错误。

联系 TAC 解决终端上的 SNMP 问题

如果终端的 SNMP 配置已完成，但出现了问题，您需要联系 TAC 并共享以下信息：

- 在 Control Hub 中提供您的组织 ID 以及受影响终端的序列号(SN)。
- 描述所面临的场景。
- 提供您正在尝试配置的 SNMP 版本。
- 提供看到的任何错误消息。
- 如果设备配置有问题，请明确说明配置过程在哪个步骤中停止并提供屏幕截图。共享返回错误的配置命令。
- 收集终端日志并将其上传到您的案例。
- 共享用于测试 SNMP 配置的实用程序\NMS 或其他工具。如果使用实用程序测试终端的 SNMP 代理，请提供使用的完整命令。

相关信息

[Room OS xAPI 文档 — SNMP 相关命令](#)

[主板、桌面和房间系列设备的设备配置](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。