

Configurar SNMP em endpoints registrados na nuvem

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[O que é SNMP](#)

[Quais informações podem ser solicitadas](#)

[Configurar o SNMP em um endpoint registrado na nuvem](#)

[Ativar o modo SNMPv2c no Control Hub](#)

[Ativar o modo SNMPv3 no Control Hub](#)

[Como é a configuração do SNMP na GUI do endpoint](#)

[Configurar o usuário do USM para SNMPv3](#)

[Testando a configuração de SNMPv2c e SNMPv3](#)

[Um endpoint pode ter SNMPv2c e SNMPv3 ativos simultaneamente](#)

[Vários endpoints podem ser configurados através do hub de controle com SNMP](#)

[Detalhes importantes a serem lembrados](#)

[Entrar em contato com o TAC para solucionar um problema de SNMP em um endpoint](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar e solucionar problemas de SNMP em um endpoint registrado na nuvem.

Pré-requisitos

Requisitos

Recomenda-se que você tenha alguma familiaridade com estes tópicos:

- Plataforma de Hub de Controle
- Administração de endpoints por meio da interface gráfica do usuário (GUI) do endpoint e da seção Dispositivos do hub de controle
- SSH para um endpoint como um usuário administrador
- Sistema operacional da sala
- SNMP (SNMPv2c e SNMPv3)
- Snmpwalk ou outro utilitário/ferramenta ou Network Management System(NMS) para testar

a configuração do SNMP

Componentes Utilizados

O equipamento listado aqui foi usado para fazer os testes e produzir os resultados descritos neste documento:

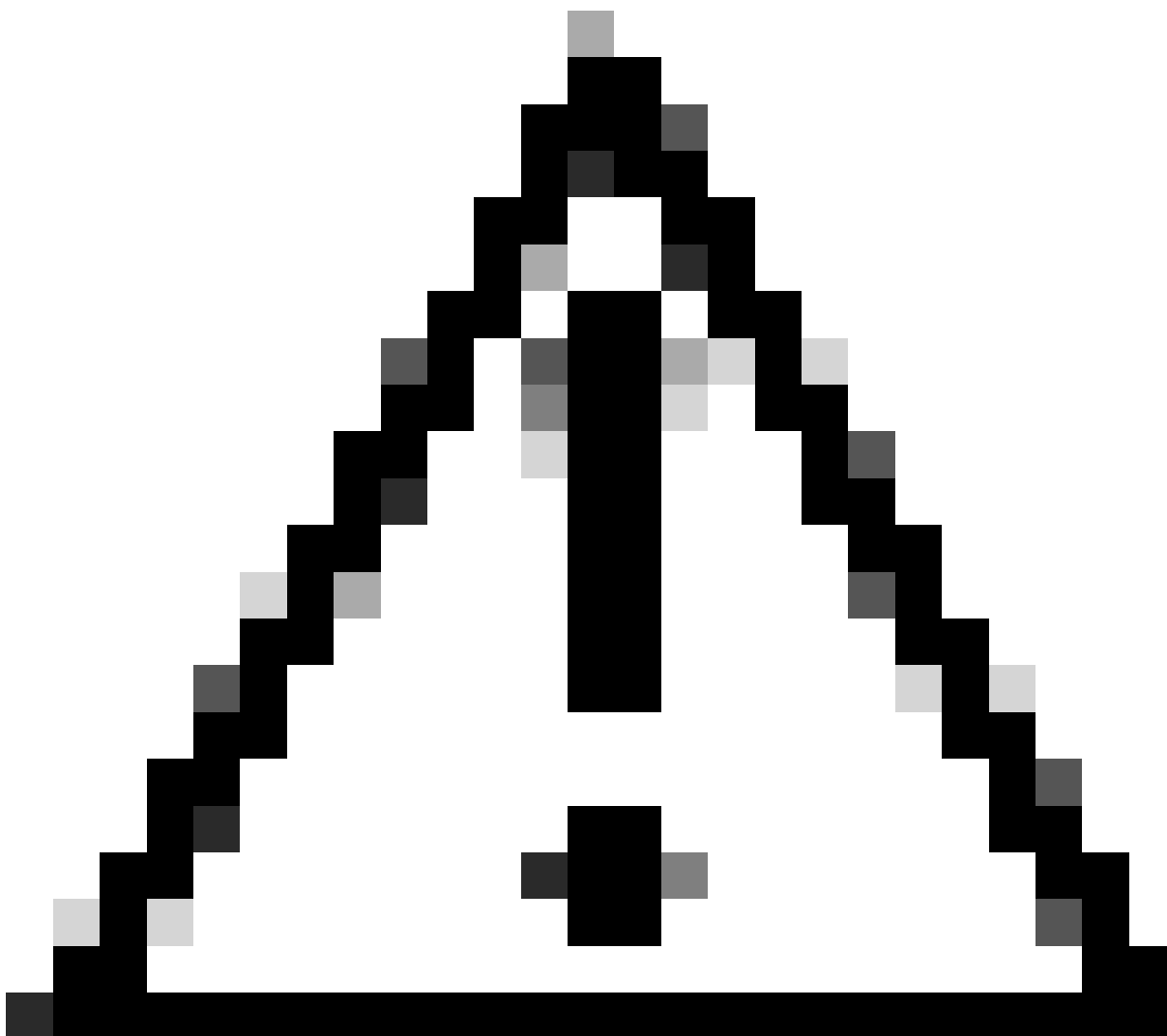
- Organização do Hub de Controle
- Kit de salas da Cisco Pro
- Cisco Room Bar Pro
- Servidor Linux para hospedar o utilitário snmpwalk para testar a configuração SNMP.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

O que é SNMP

SNMP significa Simple Network Management Protocol (protocolo de gerenciamento de rede simples). É um protocolo usado para coletar e gerenciar informações sobre os dispositivos em uma rede, monitorar o status dos dispositivos ou fazer alterações na configuração. Esses dispositivos podem ser roteadores, switches, servidores, impressoras ou qualquer outro tipo de dispositivo. É um pré-requisito que esses dispositivos tenham recebido um endereço IP. Há três versões do SNMP. O SO da sala oferece suporte a SNMPv2c e SNMPv3. Não há suporte para SNMPv1.

Este artigo concentra-se na configuração e na solução de problemas do SNMP em endpoints de colaboração que executam o SO da sala registrado na nuvem (sem usar o Webex Edge for Devices).



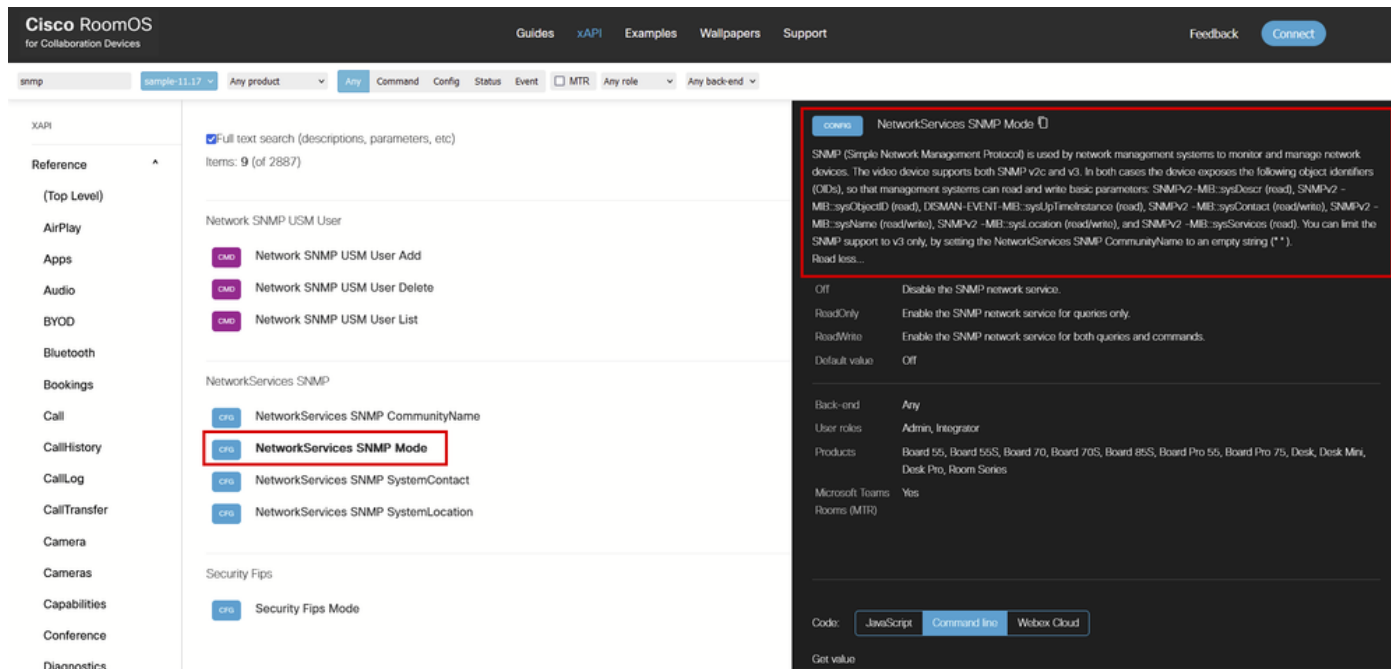
Caution: Este artigo está abordando a configuração do SNMP somente da perspectiva do endpoint. Qualquer configuração feita no lado da rede e as ferramentas usadas para solicitar/atualizar informações relacionadas ao SNMP nos endpoints estão fora do escopo deste artigo.

O TAC não está suportando a solução de problemas do SNMP dentro da rede, nem pode oferecer quaisquer inferências sobre por que o SNMP não está funcionando como esperado de uma perspectiva de rede. Sua equipe de rede deve estar envolvida na solução desses problemas.

O gerenciamento do SNMP pode ser obtido com muitas ferramentas diferentes. Essas ferramentas não são suportadas pelo TAC. Se houver uma discrepância nas informações que essas ferramentas coletam dos endpoints, o problema deve ser solucionado pela equipe de rede no início e, em seguida, escalonado no TAC se houver informações suficientes que provem que é um problema relacionado ao endpoint.

Quais informações podem ser solicitadas

Usando o SNMP, você pode solicitar uma quantidade limitada de informações do endpoint. Os OIDs e os MiBs suportados podem ser vistos [neste link](#), sob os detalhes da descrição do comando NetworkService SNMP Mode:



The screenshot shows the Cisco RoomOS xAPI documentation interface. The search bar at the top contains 'snmp'. The search results on the left list several commands, with 'NetworkServices SNMP Mode' highlighted. The main content area on the right provides a detailed description of the command, including its purpose and supported parameters.

NetworkServices SNMP Mode

SNMP (Simple Network Management Protocol) is used by network management systems to monitor and manage network devices. The video device supports both SNMP v2c and v3. In both cases the device exposes the following object identifiers (OIDs), so that management systems can read and write basic parameters: 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). You can limit the SNMP support to v3 only, by setting the NetworkServices SNMP CommunityName to an empty string ("").

Read less...

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)	

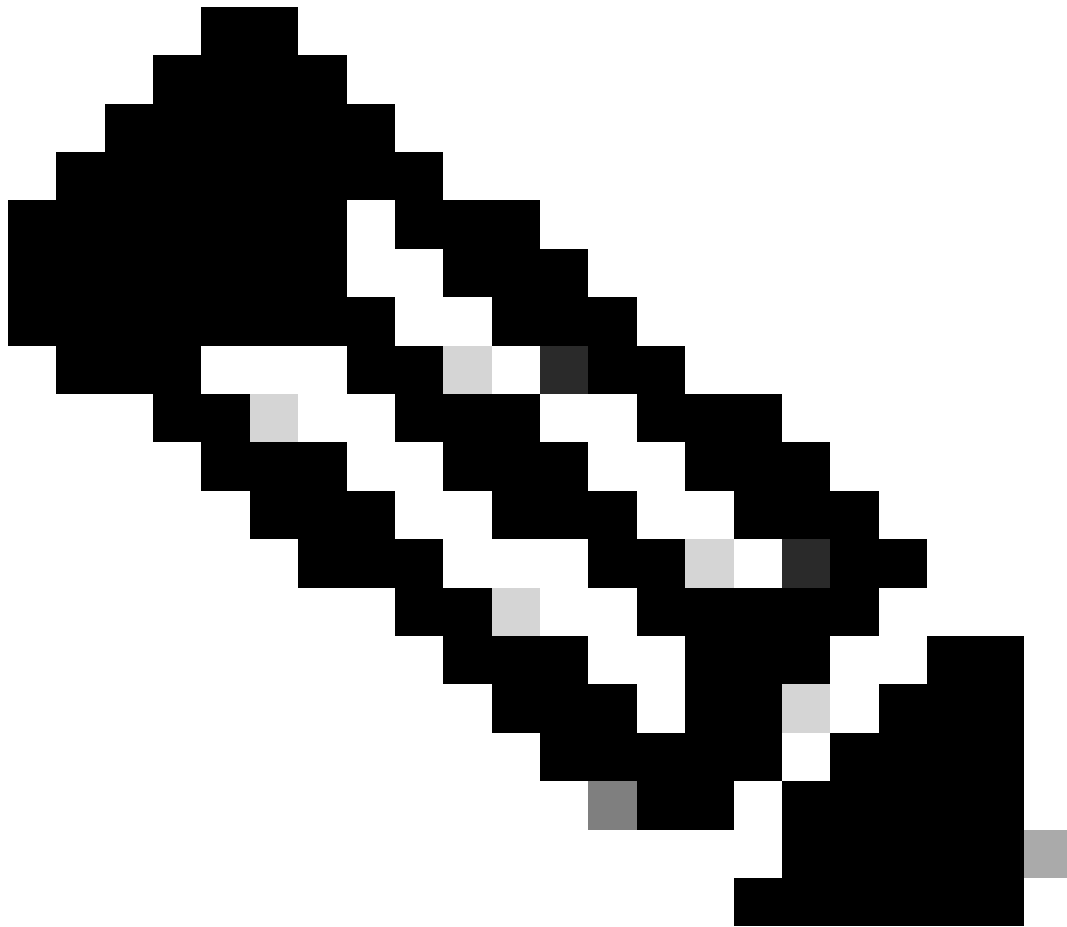
Code: [JavaScript](#) [Command line](#) [Webex Cloud](#)

Get value

Descrição do comando NetworkService SNMP Mode na documentação xAPI do SO da sala

Os endpoints expõem estes OIDs para SNMPv2 e SNMPv3:

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

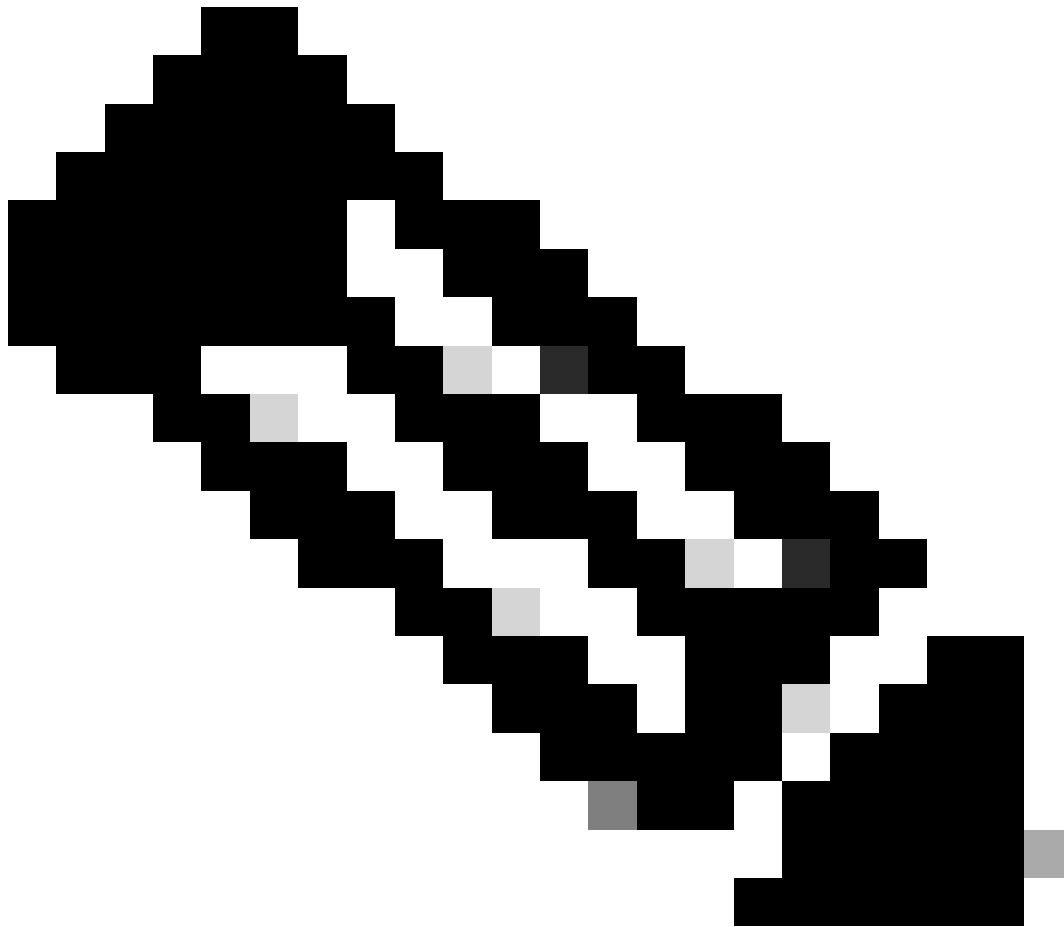


Note: NetworkServices SNMP CommunityName pode ser definido como uma sequência de caracteres vazia se você quiser usar apenas SNMPv3.

Configurar o SNMP em um endpoint registrado na nuvem

Geralmente, as alterações de configuração nos endpoints podem ocorrer de quatro maneiras diferentes:

1. As APIs do Webex disponíveis
2. A GUI do endpoint
3. Hub de controle
4. SSH diretamente para o endpoint



Note: Para acessar uma GUI de endpoint, abra um navegador e, na barra de URL, digite o endereço IP do endpoint. Você precisa estar na mesma rede que o endpoint e precisa ter credenciais de usuário para poder fazer login.

Nem todas as configurações são possíveis de serem feitas de todas as quatro maneiras. Para o cenário deste documento, o modo SNMP pode ser habilitado de todas as quatro maneiras, mas para criar um usuário SNMP que possa se comunicar com o dispositivo por SNMP, você precisa usar SSH para o endpoint, usar as APIs Webex ou usar a GUI do endpoint na API do desenvolvedor na seção Personalização. Os usuários USM não podem ser criados na seção Todas as Configurações do Hub de Controle do ponto de extremidade.

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:

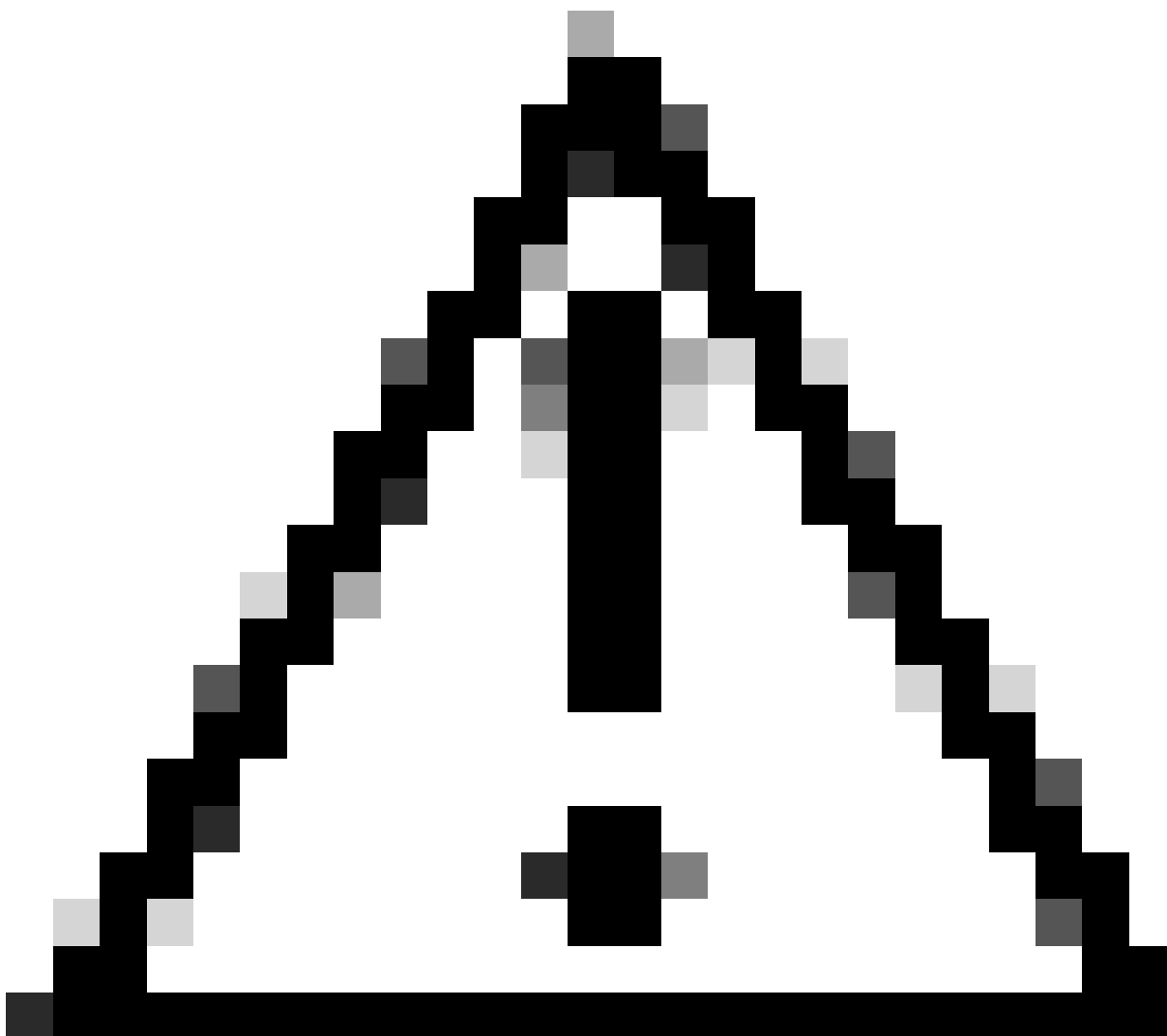
xCommand Dial Number: "person@example.com" Protocol: SIP

xCommand Network SNMP USM User List

Execute

1 of 1 applied successfully.

Seção da API do Desenvolvedor na GUI do Endpoint

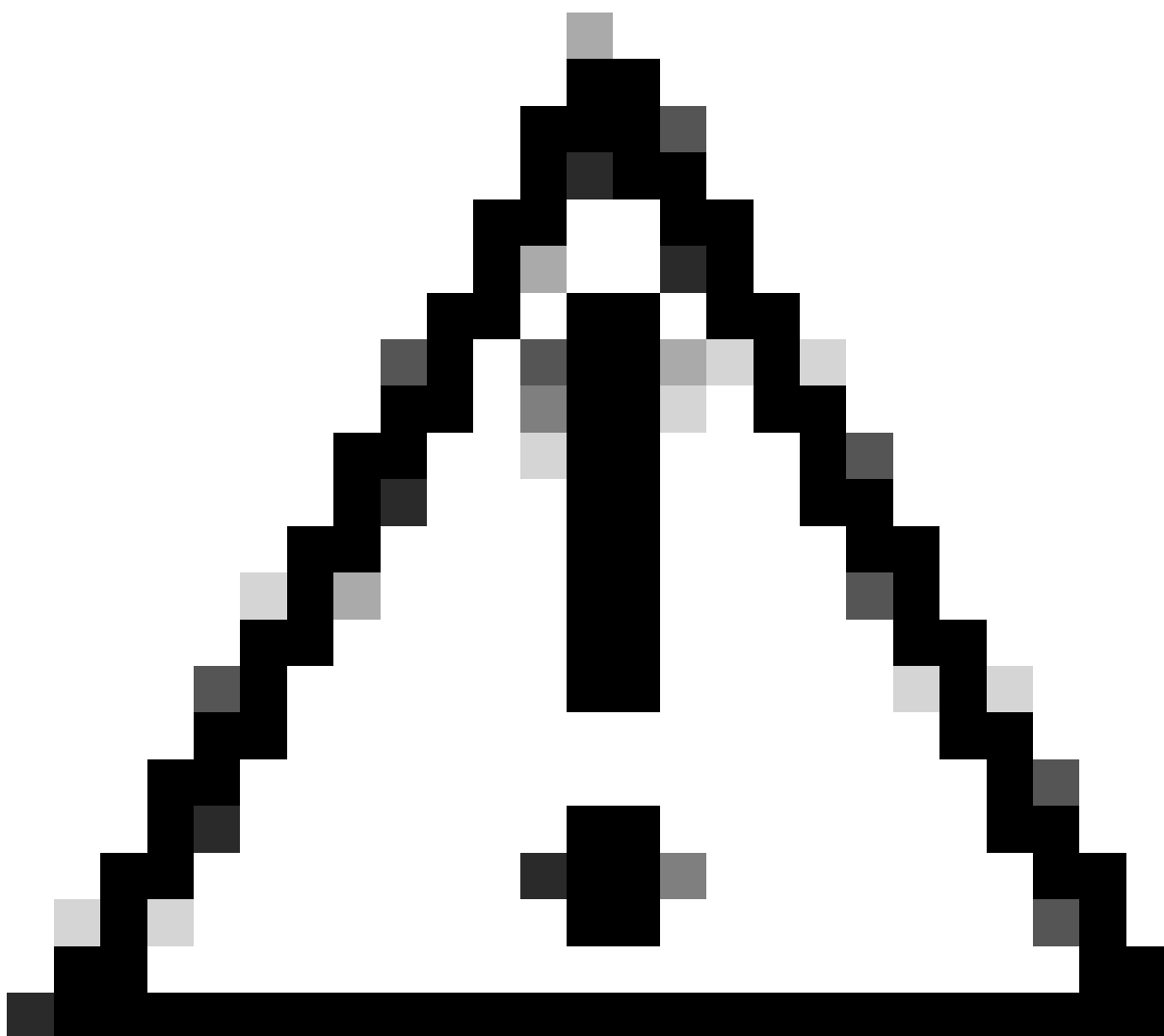


Caution: Os comandos emitidos na caixa de texto Executar comandos e configurações não estão retornando nenhum resultado. Você verá apenas se o comando foi executado com êxito ou não. É por isso que o comando que lista os usuários do USM não retorna nenhum resultado na captura de tela anterior. Isso significa que você pode criar um usuário USM a partir desta seção da GUI do endpoint com êxito, mas para verificar novamente se o usuário é criado, você precisa usar SSH para o dispositivo.

Para configurar o SNMPv2c, não é necessário criar um usuário. A autenticação ocorre com o uso do nome da comunidade (também chamado de sequência de caracteres de comunidade) que é configurado no endpoint. O agente SNMP do ponto de extremidade, que já existe no dispositivo, responde a solicitações que correspondem ao nome de comunidade configurado no dispositivo. Se uma solicitação SNMP de um sistema de gerenciamento não incluir um nome de comunidade correspondente (diferencia maiúsculas de minúsculas), a mensagem será descartada e o agente SNMP no dispositivo de vídeo não enviará uma resposta.

No entanto, o SNMPv3 exige a configuração de um usuário do USM para que a autenticação seja bem-sucedida. Para essa finalidade, é necessário usar os comandos Network SNMP USM User.

Isso pode acontecer pelo SSH diretamente para o dispositivo ou usando a GUI do dispositivo na seção Developer API. Como alternativa, a API do Webex pode ser usada.



Caution: Você precisa decidir se vai habilitar SNMPv2, SNMPv3 ou ambos. O SNMPv1 não é suportado nos endpoints da Cisco. Qualquer tentativa de usar o SNMPv1 falhará.

Neste documento, os protocolos SNMPv2 e SNMPv3 serão habilitados e configurados no Control Hub, mas o usuário USM necessário para a autenticação SNMP3 é configurado no SSH.

Ativar o modo SNMPv2c no Control Hub

Navegue até admin.webex.com e faça login com suas credenciais de administrador. É sugerido ser um administrador completo. Navegue até Devices na seção Management no lado esquerdo da interface do usuário. Na guia Devices, selecione o dispositivo que deseja configurar. Neste exemplo, é usado um Cisco Room Kit Pro.

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	

Seção Dispositivos do Hub de Controle

Sob os detalhes do dispositivo na nova página Control Hub que é aberta, navegue para a seção Configurações e clique em Todas as configurações:

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

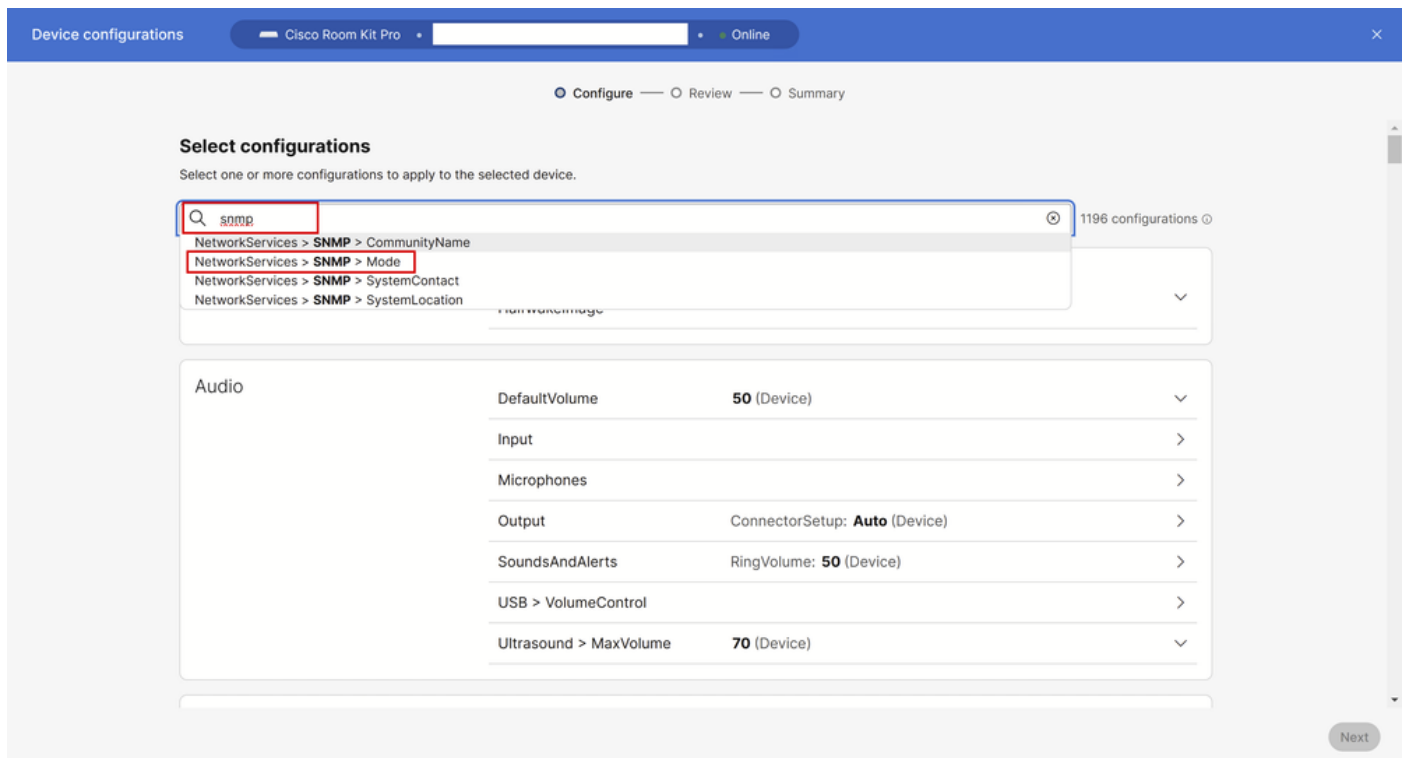
- All configurations 1195 >
- Configuration templates >
- Digital signage Disabled >
- Navigator persistent web app Disabled >
- Macros 1 >

Support

- Device Logs ⓘ Manage >
- Remote access ⓘ Available ⓘ Open >
- Local Device Controls ⓘ Launch >

Detalhes do dispositivo do hub de controle para o kit de sala Pro

Na barra de pesquisa, digite snmp e selecione NetworkServices > SNMP > Mode:

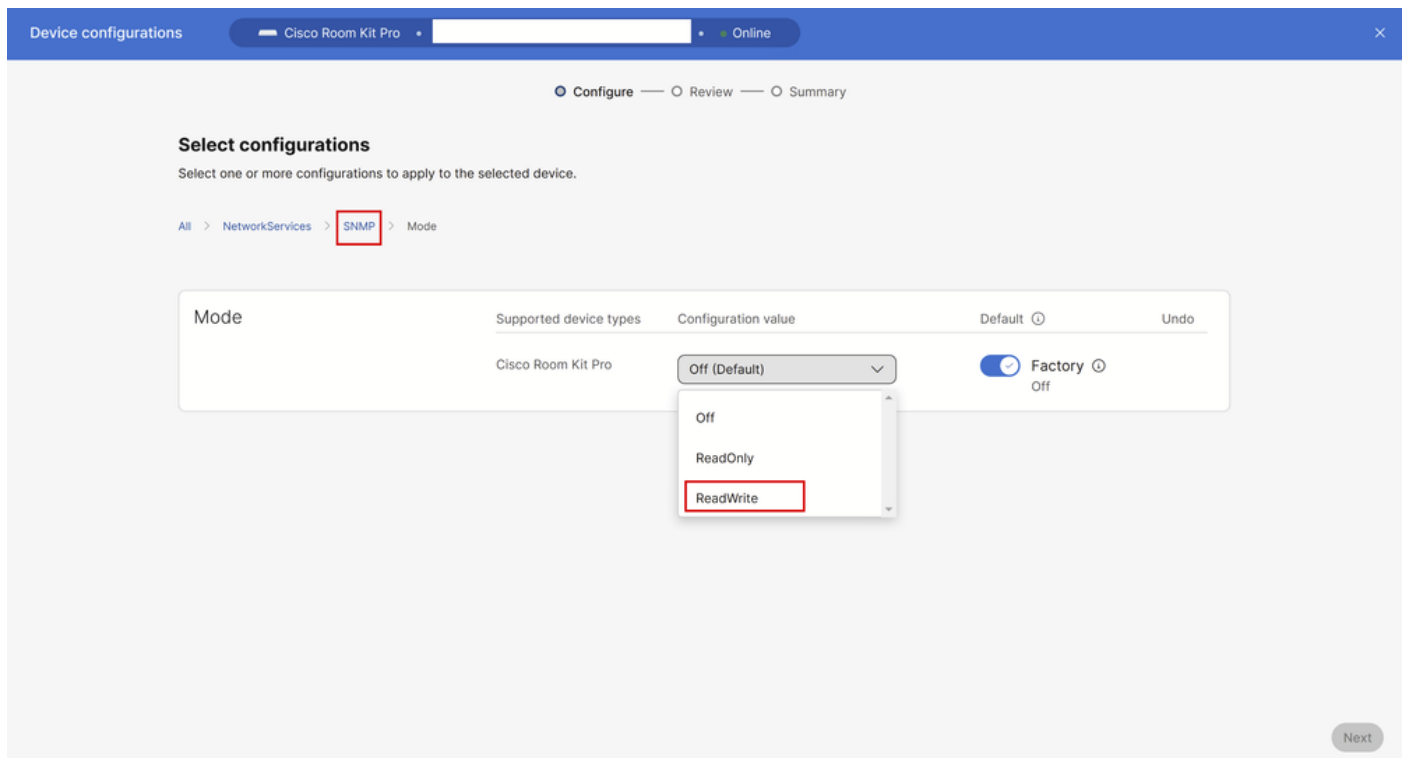


Janela Todas as Configurações de Hub de Controle

Selecione o modo que você precisa para ativar em seu ambiente. Há três opções disponíveis:

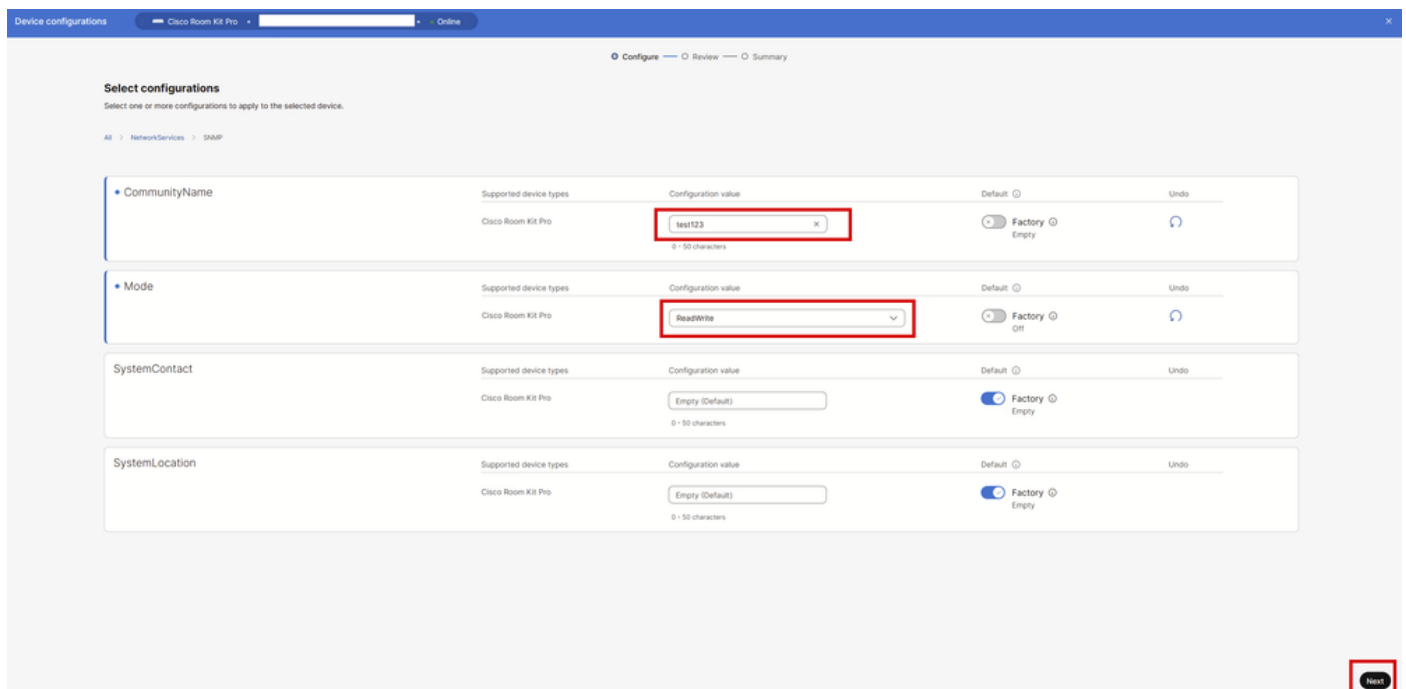
1. Off: Desative o serviço de rede SNMP.
2. Somente Leitura: Habilite o serviço de rede SNMP somente para consultas.
3. Leitura e gravação: Habilite o serviço de rede SNMP para consultas e comandos.

Para este exemplo, ReadWrite está selecionado. Em seguida, clique em SNMP na seção de navegação de configurações, conforme ilustrado na figura. Isso o levará de volta uma etapa nas configurações e você poderá ver todas as configurações relacionadas ao SNMP que podem ser configuradas no dispositivo através do Hub de controle:



Configuração do modo SNMP em todas as configurações no Control Hub

Depois de clicar em SNMP, todas as opções de SNMP disponíveis são exibidas, conforme ilustrado nesta imagem. Para que o SNMPv2 seja configurado com êxito, é necessário configurar um nome de comunidade. O nome da comunidade é usado para autenticação entre o servidor SNMP e o agente SNMP existente no endpoint. O nome da comunidade é definido como test123 neste exemplo. Clique em Avançar no canto inferior direito.



Configurações de SNMP em todas as configurações no Control Hub

Revise as Configurações do dispositivo e clique em Aplicar no canto inferior direito:

Device configurationsCisco Room Kit ProOnline

ConfigureReviewSummary

Review configurations
Review selected configurations.

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

PreviousApply

Revisar configurações antes de aplicar as alterações

Verifique se as alterações de configuração foram aplicadas com êxito. Em seguida, clique em Fechar.

Device configurationsCisco Room Kit ProOnline

ConfigureReviewSummary

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

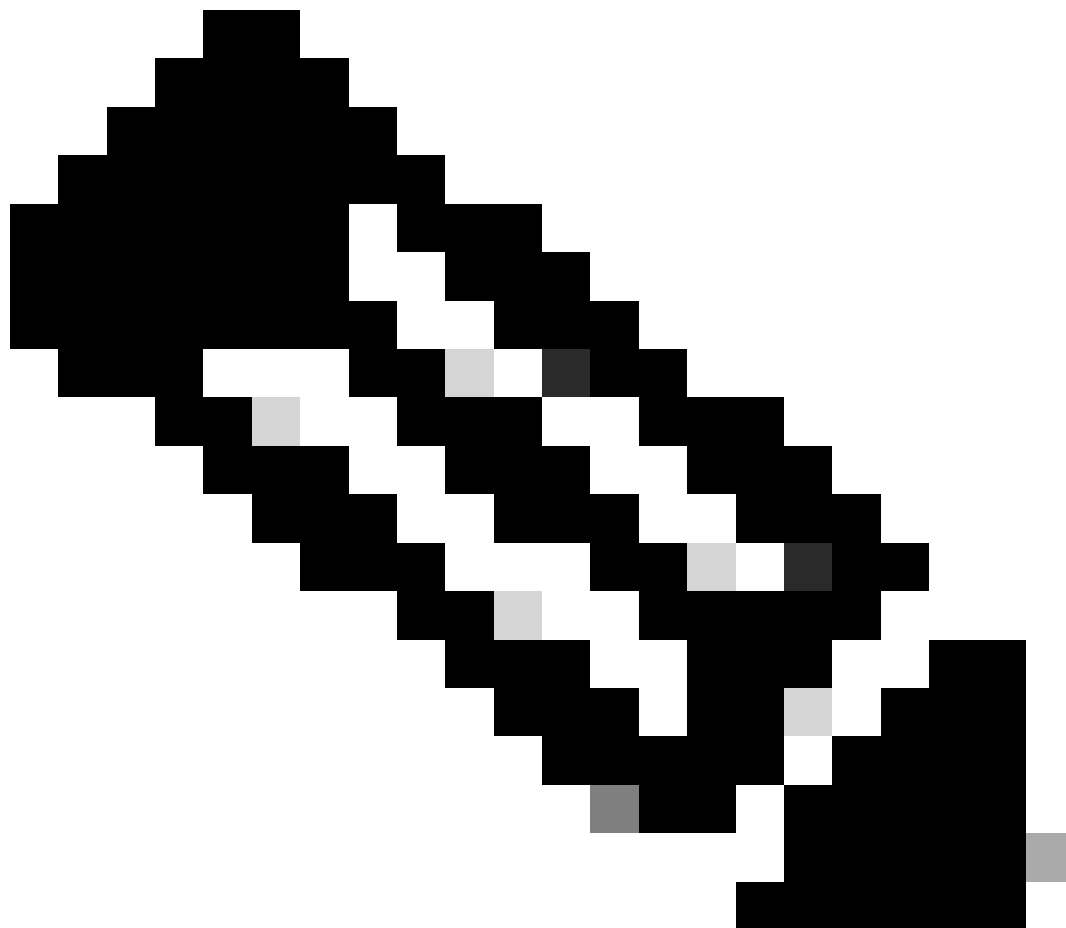
Configurações de Ponto de Extremidade Aplicadas com Êxito no Hub de Controle

Nesse estágio, o SNMPv2c é habilitado com êxito no endpoint e o nome da comunidade é configurado.

Ativar o modo SNMPv3 no Control Hub

O SNMPv3 fornece mais segurança e requer uma configuração diferente no endpoint em comparação com o SNMPv2c. Navegue até Devices na seção Management no Control Hub. Permaneça na guia Dispositivos e selecione um dos seus endpoints que você deseja configurar com SNMPv3. Para este exemplo, um Cisco Room Bar Pro é usado.

Nos detalhes do dispositivo, navegue até a seção Configurações e clique em Todas as configurações. A página Device Configurations (Configurações do dispositivo) é aberta. Digite snmp na barra de pesquisa e selecione NetworkServices > SNMP > Mode. Para este exemplo, o modo SNMP é definido como ReadWrite. Clique em SNMP para ver todas as configurações SNMP configuráveis no dispositivo.



Note: Todas as etapas mencionadas até agora para o SNMPv3 já foram descritas quando o SNMPv2c foi configurado em um exemplo anterior. Por causa disso, nenhuma captura de tela das etapas é fornecida. Consulte a seção Ativar o modo SNMPv2c no Control Hub se houver alguma dúvida sobre como navegar pelas configurações do Control Hub.

Para suportar apenas o SNMPv3, você precisa configurar o nome da comunidade como uma sequência de caracteres vazia entre aspas: "".

The screenshot displays the 'Device configurations' page for a 'Cisco Room Bar Pro' device. The interface includes a top navigation bar with 'Device configurations', 'Cisco Room Bar Pro', and 'Issues' tabs. Below this is a sub-navigation bar with 'Configure', 'Review', and 'Summary' options. The main configuration area is divided into four sections: 'CommunityName', 'Mode', 'SystemContact', and 'SystemLocation'. Each section has a 'Supported device types' dropdown (all set to 'Cisco Room Bar Pro'), a 'Configuration value' input field, a 'Default' button, and an 'Undo' button. In the 'CommunityName' section, the 'Configuration value' field contains two empty quotes (''), highlighted by a red box. In the 'Mode' section, the 'Configuration value' dropdown is set to 'ReadWrite', also highlighted by a red box. The 'SystemContact' and 'SystemLocation' sections have their 'Configuration value' fields set to 'Empty (Default)'. A 'Next' button is located at the bottom right of the configuration area, highlighted by a red box.

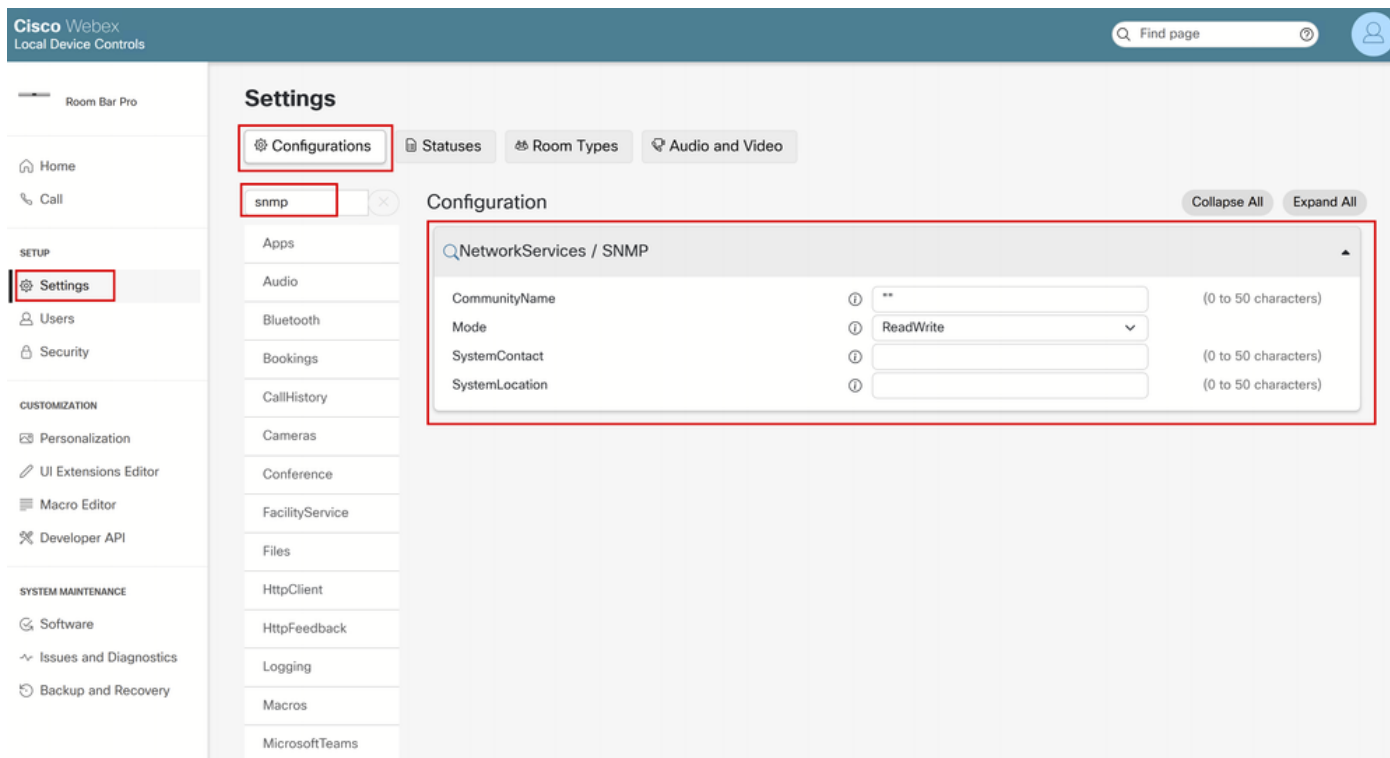
Configurações de SNMP em todas as configurações no Control Hub

Clique em Next, revise as alterações de configuração e clique em Apply. Clique em Fechar para fechar a página de configuração do dispositivo.

Isso conclui a configuração que pode ser executada no Control Hub. Neste estágio, somente o SNMPv3 está habilitado.

Como é a configuração do SNMP na GUI do endpoint

As mesmas configurações podem ser executadas na GUI do dispositivo. Abra uma guia do navegador e digite o endereço IP do ponto final (você precisa estar na mesma rede do ponto final). Faça login como um usuário admin e, na GUI do endpoint, navegue para Configurações na seção CONFIGURAÇÃO. Permaneça na guia Configurações e na barra de pesquisa de configurações digite snmp. Esta imagem mostra como as configurações SNMP são exibidas para a configuração SNMPv3 feita no Room Bar Pro na seção anterior:



Configuração de SNMPv3 na GUI do endpoint

Configurar o usuário do USM para SNMPv3

Para poder usar o SNMPv3, você precisa criar um usuário do USM. Os comandos disponíveis para executar essa ação podem ser encontrados no link de documentação do SO da sala [aqui](#). Use SSH para se conectar ao dispositivo. Para isso, você precisa ter uma conta de administrador no dispositivo. Caso contrário, você precisará criar uma conta de administrador. Esta seção passa por todo este processo.

Navegue até Devices na seção Management no Control Hub. Permaneça na guia Devices e selecione um dos endpoints para o qual deseja criar um usuário administrador. Para este exemplo, um Cisco Room Bar Pro é usado.

Sob os detalhes do dispositivo, navegue até a seção Suporte e clique em Controles de dispositivo local (você precisa estar na mesma rede que o endpoint para que isso funcione). A GUI do dispositivo é aberta. Navegue até Users na seção SETUP e clique em Create User.

Cisco Webex Local Device Controls

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

Seção Usuários na GUI do endpoint

Forneça um nome de usuário e senha (senha). Verifique se o usuário tem privilégios totais de administrador e se está ativo:

Cisco Webex Local Device Controls

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

Criar um usuário a partir da GUI do endpoint

Verifique se o usuário foi criado e está ativo na página Usuários:



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	✓	✓	✓	✓	✓

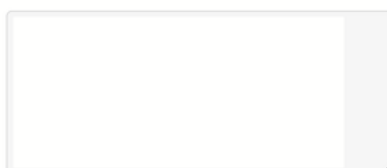
Remote Support

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.

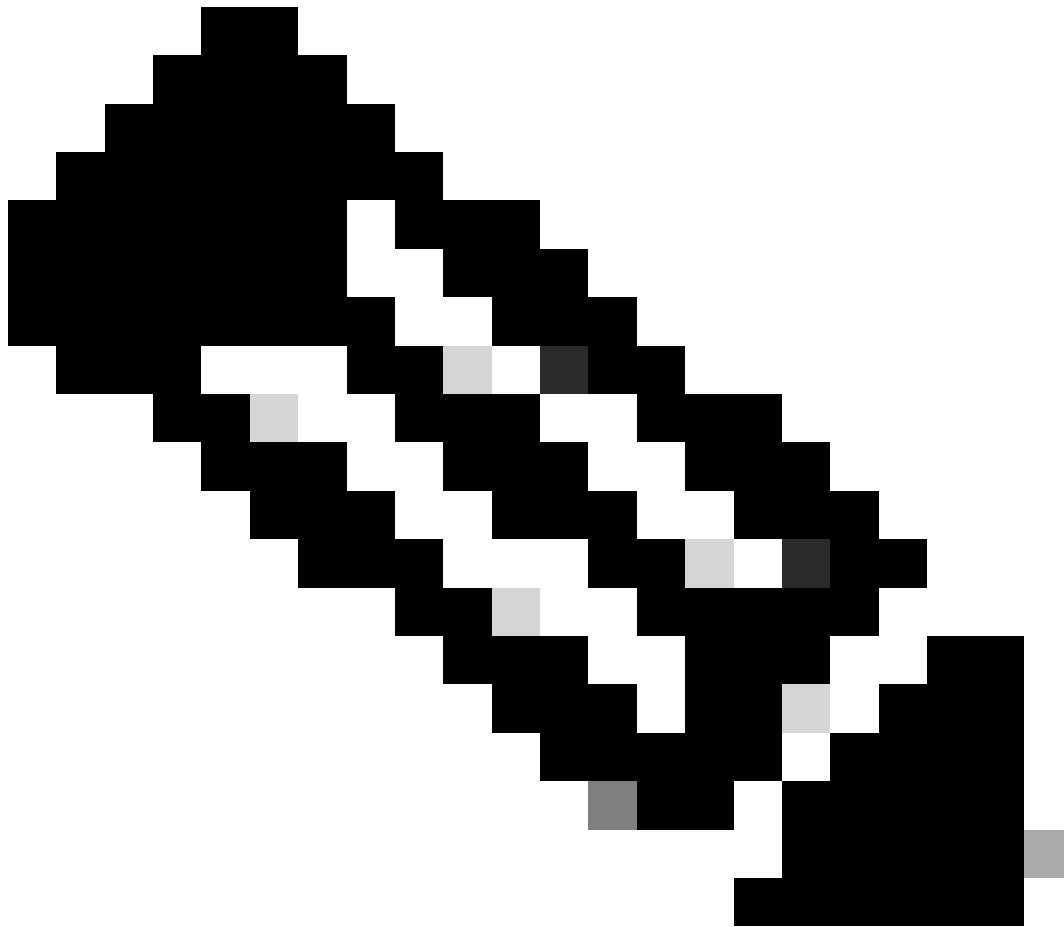
This remote support user on this system is managed by Cisco Webex Control Hub.

This user is valid until

Token



Novo usuário criado e listado entre outros usuários



Note: No primeiro log SSH em tentativa com um usuário recém-criado, você será solicitado a alterar sua senha. Você verá um prompt semelhante a:

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

Alterar senha quando SSH for pela primeira vez

Quando a senha for alterada, você será imediatamente desconectado e precisará iniciar uma nova conexão SSH.

Depois que o usuário administrador for criado com êxito, use um cliente SSH de sua escolha e conecte-se ao endpoint. Faça login com as credenciais de administrador. Este é o prompt exibido:

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

Tentativa de login bem-sucedida via SSH para o ponto de extremidade

Use o comando Network SNMP USM User Add conforme descrito [neste](#) artigo. Para esta demonstração, o comando usado é:

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

O resultado desse comando, quando bem-sucedido, é:

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

Criação de usuário USM via SSH

Para que o comando seja executado sem erros, você precisa seguir determinadas regras descritas na documentação do comando compartilhada neste [link](#). Por conveniência, os requisitos atuais no momento em que este documento foi escrito para este comando são colados nesta imagem, mas você deve certificar-se de consultar este [link](#) ao criar seu usuário. No final da imagem, observe que há a sintaxe exata do 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

Sintaxe de comando de criação de usuário USM da documentação xAPI



aviso: Caso haja um erro de digitação ou haja um requisito não atendido, o comando retorna um erro e o usuário não será criado. Um exemplo é fornecido, em que, em vez de fornecer uma senha de privacidade com pelo menos 8 caracteres, uma senha mais curta com 7 caracteres é fornecida:

```
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.

Criação de usuário USM malsucedida devido à senha de privacidade curta

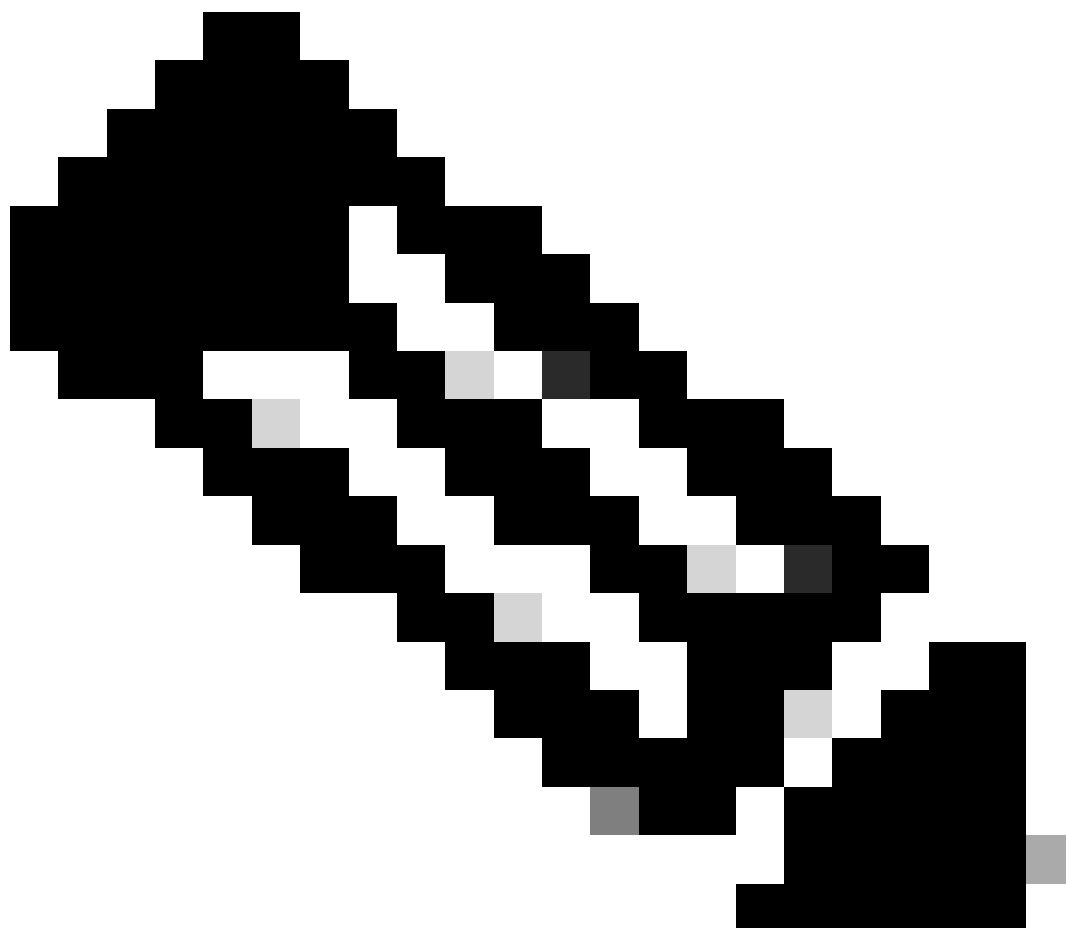
Você pode testar se o usuário foi criado usando o comando Network SNMP USM User List. Esse comando lista todos os usuários do USM que estão armazenados no dispositivo:

```
xCommand Network SNMP USM User List

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

Comando Network SNMP USM User List usado para confirmar a criação do usuário

Nesta fase, foi confirmado que o psitaras do usuário foi criado com sucesso. A configuração do SNMPv3 foi concluída.



Note: O usuário USM psitaras não está visível na GUI do endpoint na seção Usuários. Isso é esperado.

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

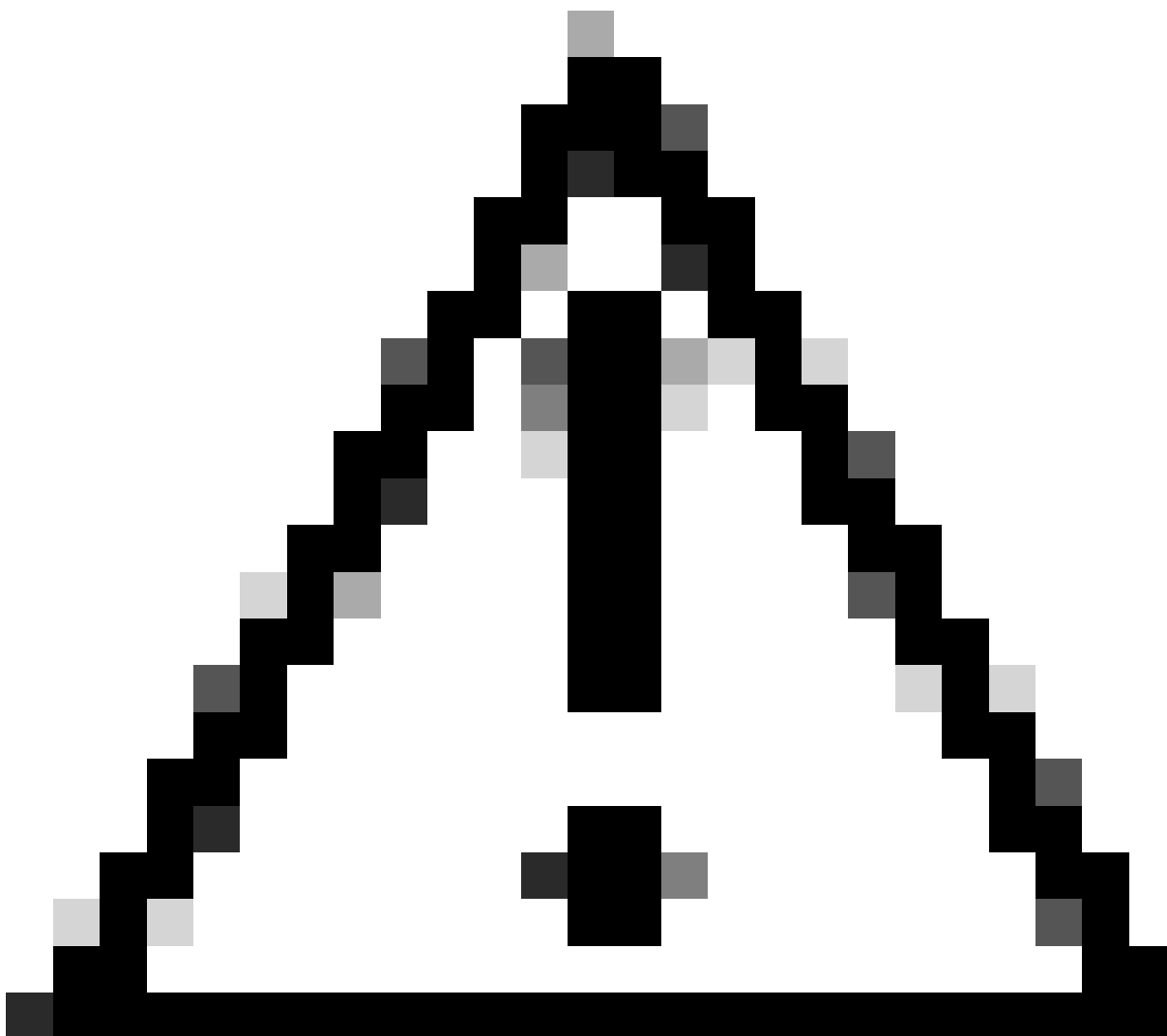
Token

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

Usuários do USM não estão visíveis em Usuários na GUI do endpoint

Testando a configuração de SNMPv2c e SNMPv3

Neste estágio, você pode continuar com o teste da configuração de SNMPv2c e/ou SNMPv3 com seu NMS (Network Management System). Para este artigo, a configuração do laboratório não contém nenhum servidor NMS ou SNMP executando um serviço SNMP. Para testar a configuração, o utilitário chamado snmpwalk é usado. Este utilitário é instalado em um servidor Linux.



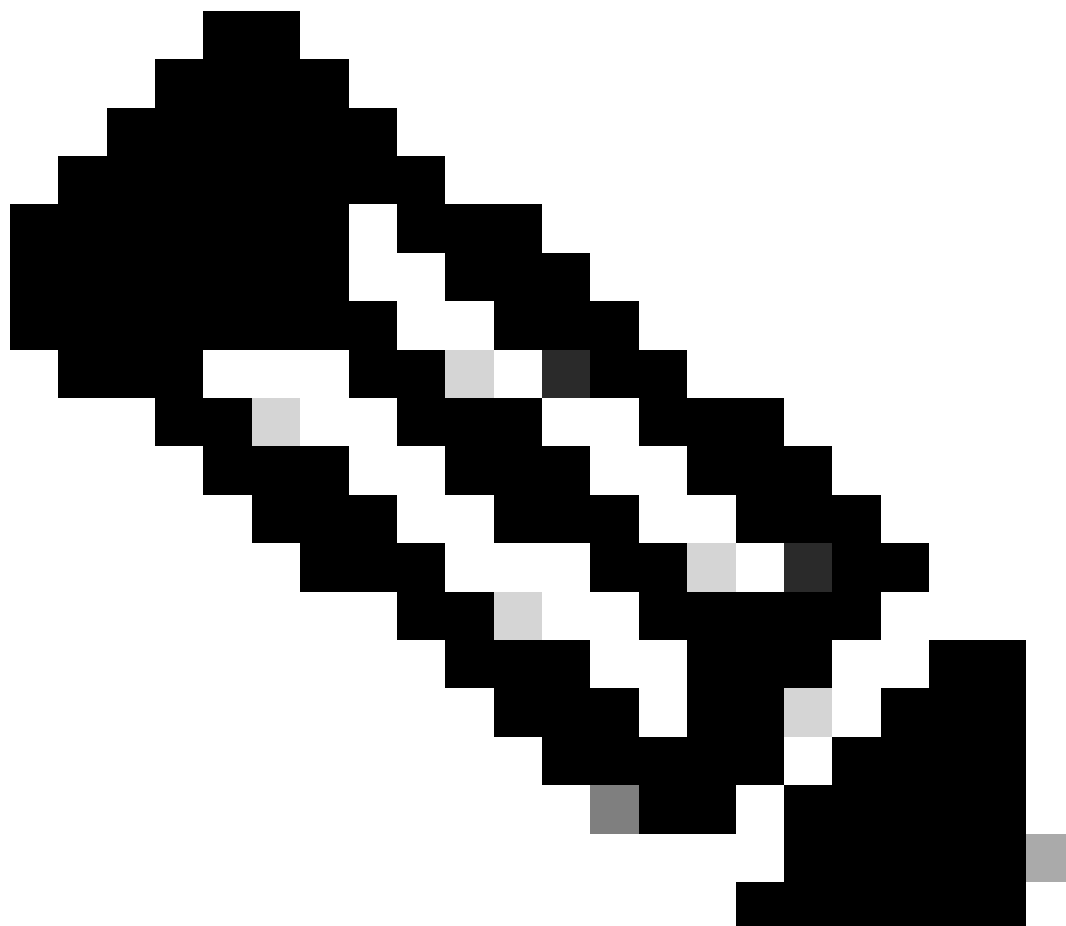
Caution: O Snmpwalk não é uma ferramenta sugerida para testar a configuração do SNMP em seus endpoints de colaboração. Ele não é suportado pelos engenheiros do TAC e você precisa estar familiarizado com como usar a ferramenta antes de prosseguir com o teste. Em vez de snmpwalk, você pode usar qualquer outra ferramenta SNMP ou seu NMS para testar sua configuração. O Snmpwalk é usado neste artigo apenas como um exemplo (uma ferramenta é necessária para testar a configuração para fins de demonstração), e não há compromisso ou promoção relacionada ao seu uso.

A instalação do snmpwalk não faz parte deste guia e foi omitida. Dependendo do sistema operacional (SO) da máquina que você está usando para o teste, os requisitos de instalação podem variar. Você deve trabalhar para instalá-lo com êxito antes de testar.

O Snmpwalk é uma ferramenta que pode ser usada para verificar a configuração do SNMP. Ele executa uma caminhada pelos MiBs do endpoint e retorna as informações disponíveis. Os endpoints registrados na nuvem expõem 7 identificadores de objeto (OIDs):

- SNMPv2-MIB::sysDescr (leitura),

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



Note: Os IPs internos usados para os testes snmpwalk listados são IPs privados e não estão mais em uso. O laboratório usado para este guia foi desativado e os dispositivos são redefinidos de fábrica.

O endpoint do Cisco Room Kit Pro é configurado com SNMPv2c. A autenticação acontece usando strings de comunidade. Emita o seguinte 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 retorna 7 resultados como esperado. Há três MiBs vazios:

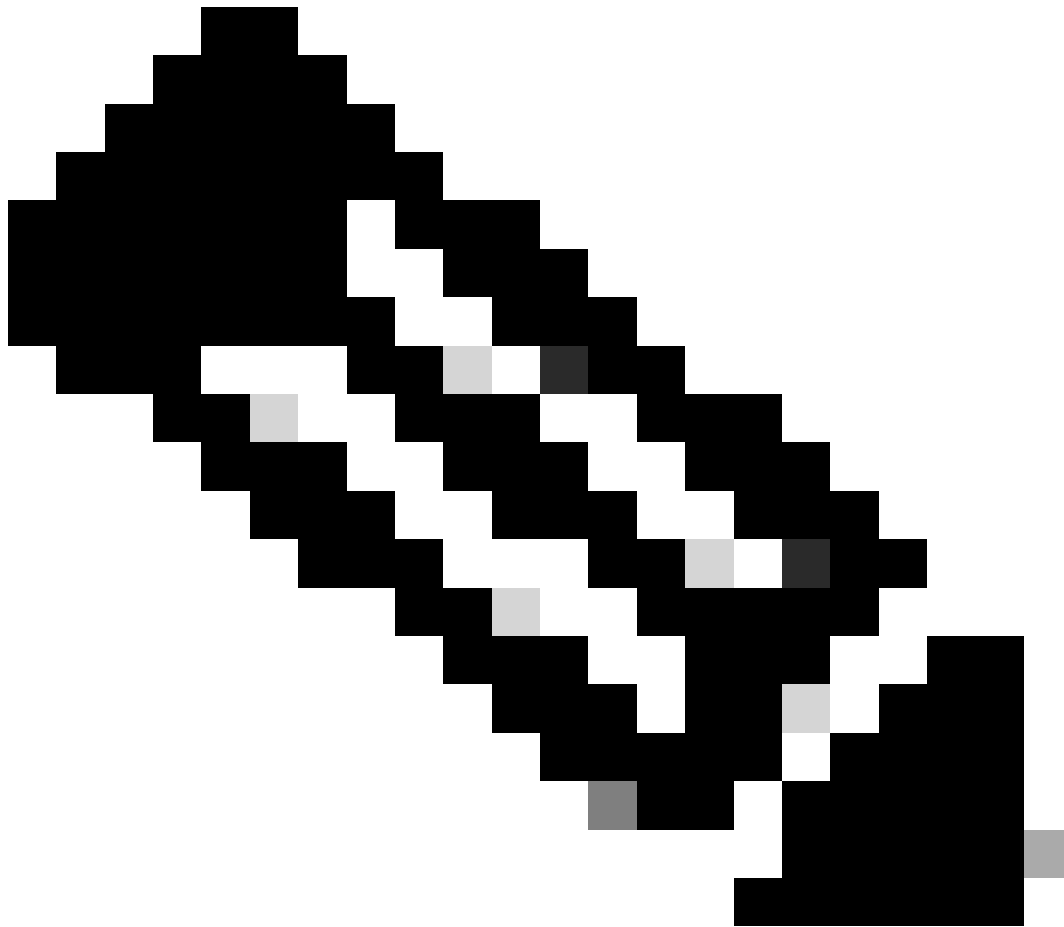
1. SNMPv2 -MIB::sysContact (leitura/gravação), (iso.3.6.1.2.1.1.4.0)
2. SNMPv2 -MIB::sysName (leitura/gravação), (iso.3.6.1.2.1.1.5.0)
3. SNMPv2 -MIB::sysLocation (leitura/gravação), (iso.3.6.1.2.1.1.6.0)

Há três comandos xConfiguration que podem ser usados para definir valores para esses MiBs. Use SSH para o endpoint e emita estes comandos:

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

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

```
xConfiguration SystemUnit Name: My_Room_Kit_Pro
```



Note: Em vez de usar esses três comandos, você pode realizar alterações nessas configurações a partir do Control Hub, da GUI do endpoint ou das APIs do Webex.

Depois que os comandos acima forem emitidos, use `snmpwalk` novamente no mesmo ponto final. Você observa que os MiBs anteriormente vazios são preenchidos com os valores fornecidos por meio dos comandos `xConfiguration`:

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

```
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco Codec  
SoftW: ce11.26.1.5.53ff615d0d9  
MCU: Cisco Codec Pro  
Date: 2025-02-28  
S/N: 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)
```

Nesse estágio, é confirmado que a configuração SNMPv2c feita no dispositivo Room Kit Pro está operacional.

O ponto de extremidade do Cisco Room Bar Pro está configurado com SNMPv3. Para SNMPv3, você precisa garantir o uso da autenticação adequada. As sequências de caracteres de comunidade não são usadas. Em vez disso, o SNMPv3 usa nomes de usuário e senhas.

```
# '-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)
```

Nesse estágio, é confirmado que a configuração de SNMPv3 feita no dispositivo Room Bar Pro está operacional.

Um endpoint pode ter SNMPv2c e SNMPv3 ativos simultaneamente

Sim, é possível. No entanto, durante a configuração do SNMP, você precisa configurar um nome de comunidade para poder ter a autenticação SNMPv2c. Para este teste, o Room Bar Pro dos exemplos anteriores é usado. A configuração atual na seção Todas as Configurações do Hub de Controle do endpoint é:

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	

Configurações de SNMP de endpoint no hub de controle

Observe que o nome da comunidade não está vazio. Há duas aspas, que indicam que o nome da comunidade é uma sequência de caracteres vazia. Você pode limitar o suporte SNMP apenas à versão 3, definindo NetworkServices SNMP CommunityName como uma sequência de caracteres vazia (""). Você precisa substituir essa string por um nome de comunidade, por exemplo, 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	Factory ⓘ Empty	
		0 - 50 characters		

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

Adicionar o nome da comunidade para SNMPv2c nas definições de configuração do ponto final do hub de controle

Já foi confirmado que o SNMPv3 está funcionando no Room Bar Pro. O Snmpwalk é usado para testar se o SNMPv2c também está funcionando, depois de configurar o nome da comunidade:

```
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)
```

Vários endpoints podem ser configurados através do hub de controle com SNMP

Sim, é possível configurar vários dispositivos de uma vez no Control Hub. Este [artigo](#) fornece informações sobre como executá-lo passo a passo na seção Configurar vários dispositivos.

Detalhes importantes a serem lembrados

- Apenas MiBs específicos estão disponíveis. O número de MiBs disponíveis é limitado pelo projeto da equipe de engenharia que projeta os endpoints. Os MiBs não podem ser expandidos ou aprimorados para fornecer mais informações.
- O SNMPv2c autentica usando o nome da comunidade (também conhecido como sequência de caracteres da comunidade), enquanto o SNMPv3 autentica usando o nome de usuário e a senha e também oferece criptografia. Durante o teste, certifique-se de estar usando o método de autenticação correto (com snmpwalk ou outra ferramenta/NMS) para o protocolo configurado.
- A autenticação e a privacidade estão sempre ativas no SNMPv3. Os pontos de extremidade suportam apenas o nível de segurança authPriv e o protocolo de privacidade é sempre o AES (Advanced Encryption Standard).
- O SNMPv3 é suportado apenas com as opções do Modelo de Segurança Baseado no Usuário (USM - User-based Security Model). Não há suporte para SMNPv3 sobre TLS.
- Os comandos de usuário do USM usados para configurar usuários para autenticação SNMP não têm efeito no SNMPv2c.
- A configuração do SNMP CommunityName em endpoints não tem efeito na configuração do SNMPv3.
- O SNMP CommunityName diferencia maiúsculas de minúsculas.
- Você pode limitar o suporte SNMP apenas a v3, definindo o NetworkServices SNMP CommunityName como uma sequência de caracteres vazia ("").
- Não há suporte para SNMPv1.
- Tanto para SNMPv2c quanto para SNMPv3, os pontos finais expõem os mesmos identificadores de objeto (OIDs).
- Para o SNMPv3, o protocolo de autenticação precisa estar na família SHA-2 (nem MD nem SHA-1 são suportados). Caso contrário, as solicitações SNMP não serão autenticadas e permanecerão sem resposta.
- A senha de privacidade é armazenada como um valor de hash localizado (AES-128) no dispositivo. Se uma senha de privacidade não for definida explicitamente nesse parâmetro, ela será definida para ser igual à senha de autenticação (com uma função de hash conforme especificado no parâmetro Authentication Protocol).
- As senhas/senhas e os nomes de usuário precisam estar dentro de limites de comprimento específicos. Por exemplo, o nome de usuário do USM precisa ter até 32 caracteres e a senha de autenticação precisa ter um mínimo de 8 caracteres e um máximo de 255. Se esses requisitos não forem atendidos, o comando Network SNMP USM User Add falhará ao criar o usuário e retornará um erro.

Entrar em contato com o TAC para solucionar um problema de SNMP em um endpoint

Se a configuração do SNMP do endpoint foi concluída, mas um problema foi levantado, você precisa entrar em contato com o TAC e compartilhar estas informações:

- Forneça sua ID de organização no Control Hub e o número de série (SN) do endpoint afetado.
- Descreva o cenário enfrentado.
- Forneça a versão do SNMP que você está tentando configurar.
- Forneça todas as mensagens de erro vistas.
- Se houver um problema com a configuração do dispositivo, explique claramente em que etapa o processo de configuração parou e forneça capturas de tela. Compartilhe o comando de configuração que retorna um erro.
- Colete registros de endpoint e carregue-os em seu caso.
- Compartilhe o utilitário NMS ou outra ferramenta usada para testar a configuração do SNMP. Se você estiver usando um utilitário para testar o agente SNMP dos endpoints, forneça o comando completo usado.

Informações Relacionadas

[Documentação xAPI do SO da sala - Comandos relacionados ao SNMP](#)

[Configurações de dispositivo para dispositivos de placa, mesa e sala](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.