

클라우드 등록 엔드포인트에 SNMP 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[SNMP란?](#)

[요청 가능한 정보](#)

[클라우드 등록 엔드포인트에서 SNMP 구성](#)

[제어 허브에서 SNMPv2c 모드 활성화](#)

[제어 허브에서 SNMPv3 모드 활성화](#)

[SNMP 컨피그레이션은 엔드포인트 GUI에서 어떻게 표시됩니까?](#)

[SNMPv3용 USM 사용자 구성](#)

[SNMPv2c 및 SNMPv3 컨피그레이션 테스트](#)

[엔드포인트에 SNMPv2c 및 SNMPv3이 동시에 활성 상태여야 합니까?](#)

[SNMP를 사용하는 제어 허브를 통해 여러 엔드포인트를 구성할 수 있습니까?](#)

[기억해야 할 중요한 세부 사항](#)

[엔드포인트에서 SNMP 문제 해결을 위해 TAC에 문의](#)

[관련 정보](#)

소개

이 문서에서는 클라우드 등록 엔드포인트에서 SNMP를 구성하고 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대해 숙지하는 것이 좋습니다.

- 컨트롤 허브 플랫폼
- 엔드포인트의 GUI(Graphical User Interface) 및 Control Hub Devices 섹션을 통한 엔드포인트 관리
- 엔드포인트에 관리자 사용자로 SSH
- 린 OS
- SNMP(SNMPv2c 및 SNMPv3)
- SNMP 컨피그레이션을 테스트하기 위한 Snmpwalk 또는 기타 유틸리티/툴 또는 NMS(Network Management System)

사용되는 구성 요소

여기에 나열된 장비는 이 문서에 설명된 테스트를 수행하고 결과를 생성하는 데 사용되었습니다.

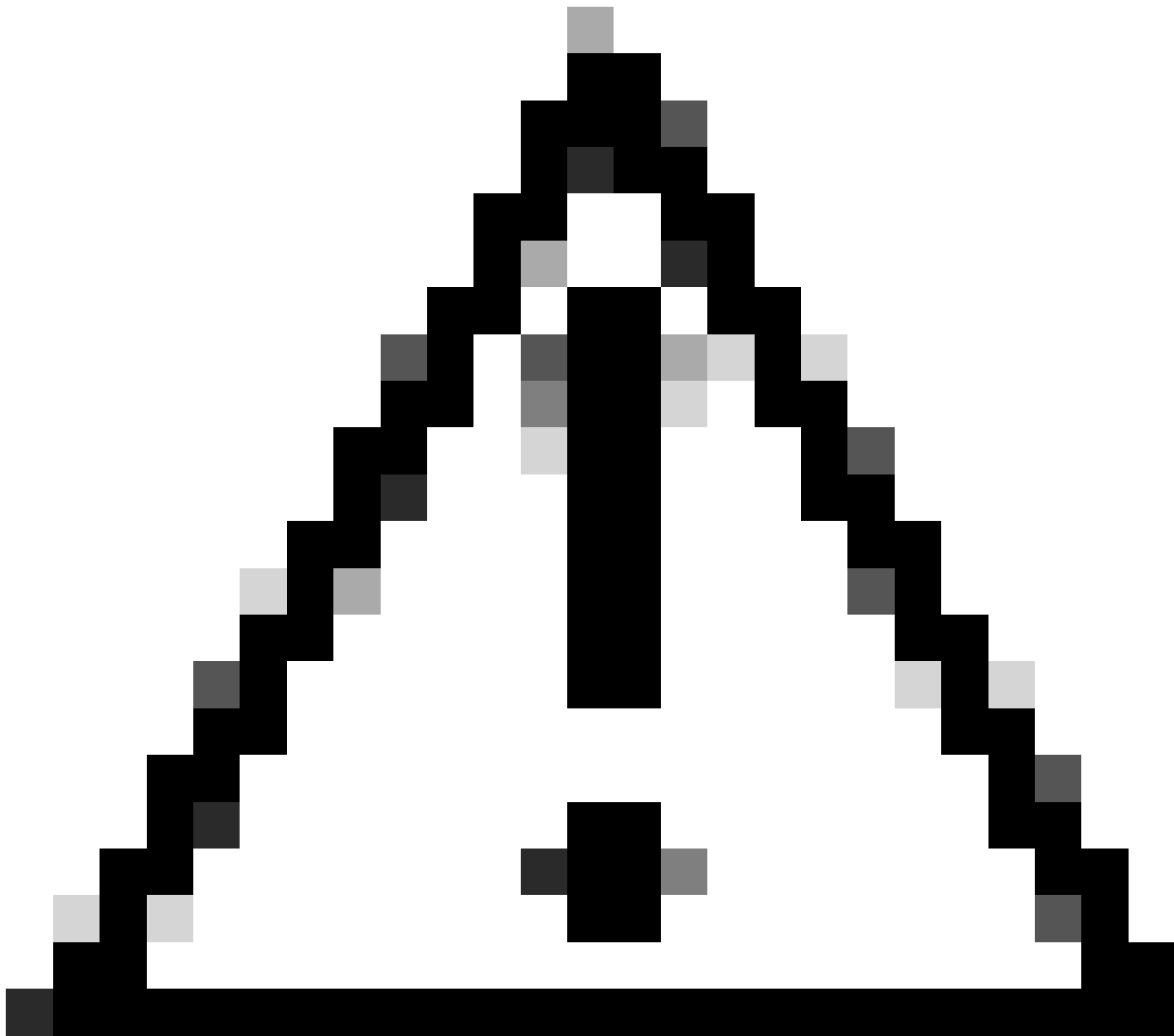
- Control Hub 조직
- Cisco Room Kit Pro
- Cisco 룸 바 프로
- SNMP 컨피그레이션을 테스트하기 위한 snmpwalk 유틸리티를 호스팅할 Linux 서버입니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

SNMP란?

SNMP는 Simple Network Management Protocol의 약자입니다. 네트워크 내의 디바이스에 대한 정보를 수집 및 관리하거나, 디바이스 상태를 모니터링하거나, 컨피그레이션을 변경하는 데 사용되는 프로토콜입니다. 이러한 디바이스는 라우터, 스위치, 서버, 프린터 또는 기타 모든 유형의 디바이스가 될 수 있습니다. 이러한 디바이스에 IP 주소가 할당되어야 합니다. SNMP에는 세 가지 버전이 있습니다. Room OS는 SNMPv2c 및 SNMPv3을 지원합니다. SNMPv1은 지원되지 않습니다.

이 문서에서는 클라우드 등록(디바이스에 Webex Edge를 사용하지 않음)된 Room OS를 실행하는 협업 엔드포인트에서 SNMP의 컨피그레이션 및 문제 해결을 중점적으로 다룹니다.



주의: 이 문서는 엔드포인트 관점에서만 SNMP 컨피그레이션에 접근하고 있습니다. 네트워크 측에서 수행한 모든 컨피그레이션 및 엔드포인트에서 SNMP 관련 정보를 요청/업데이트하는 데 사용되는 툴은 이 문서의 범위를 벗어납니다.

TAC는 네트워크 내에서 SNMP 트러블슈팅을 지원하지 않으며, 네트워크 관점에서 SNMP가 예상대로 작동하지 않는 이유에 대한 추론도 제공하지 않습니다. 네트워크 팀이 이러한 문제를 더 자세히 트러블슈팅해야 합니다.

SNMP는 다양한 툴을 사용하여 관리할 수 있습니다. 이러한 툴은 TAC에서 지원되지 않습니다. 툴이 엔드포인트에서 수집하는 정보가 일치하지 않을 경우, 먼저 네트워크 팀에서 문제를 해결한 다음, 엔드포인트 관련 문제임을 입증할 수 있는 충분한 정보가 있는 경우 TAC에서 에스컬레이션해야 합니다.

요청 가능한 정보

SNMP를 사용하면 엔드포인트에서 제한된 양의 정보를 요청할 수 있습니다. 지원되는 OID 및 MIB는 [이 링크](#)의 NetworkService SNMP Mode 명령 설명의 세부사항 아래에 표시됩니다.

Cisco RoomOS
for Collaboration Devices

Guides
xAPI
Examples
Wallpapers
Support

Feedback
Connect

snmp
sample-11.17
Any product
Any
Command
Config
Status
Event
MTR
Any role
Any back-end

XAPI
Reference
(Top Level)
AirPlay
Apps
Audio
BYOD
Bluetooth
Bookings
Call
CallHistory
CallLog
CallTransfer
Camera
Cameras
Capabilities
Conference
Diagnostics

☒ Full text search (descriptions, parameters, etc)
Items: 9 (of 2887)

Network SNMP USM User

CMD
Network SNMP USM User Add

CMD
Network SNMP USM User Delete

CMD
Network SNMP USM User List

NetworkServices SNMP

CFG
NetworkServices SNMP CommunityName

**CFG
NetworkServices SNMP Mode**

CFG
NetworkServices SNMP SystemContact

CFG
NetworkServices SNMP SystemLocation

Security Fips

CFG
Security Fips Mode

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 Rooms (MTR)
Yes

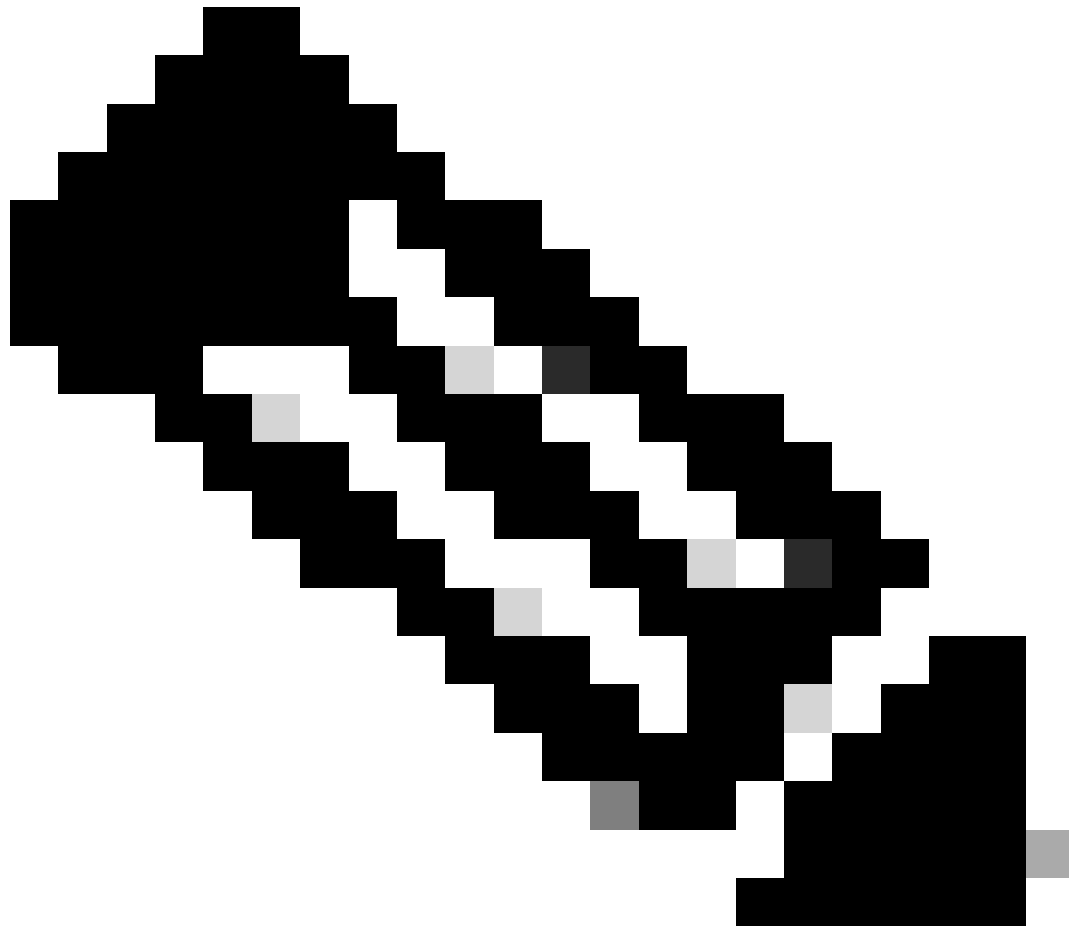
Code:
JavaScript
Command line
Webex Cloud

Get value

Room OS xAPI의 NetworkService SNMP Mode 명령 설명 문서

엔드포인트는 SNMPv2 및 SNMPv3 모두에 대해 다음 OID를 노출합니다.

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

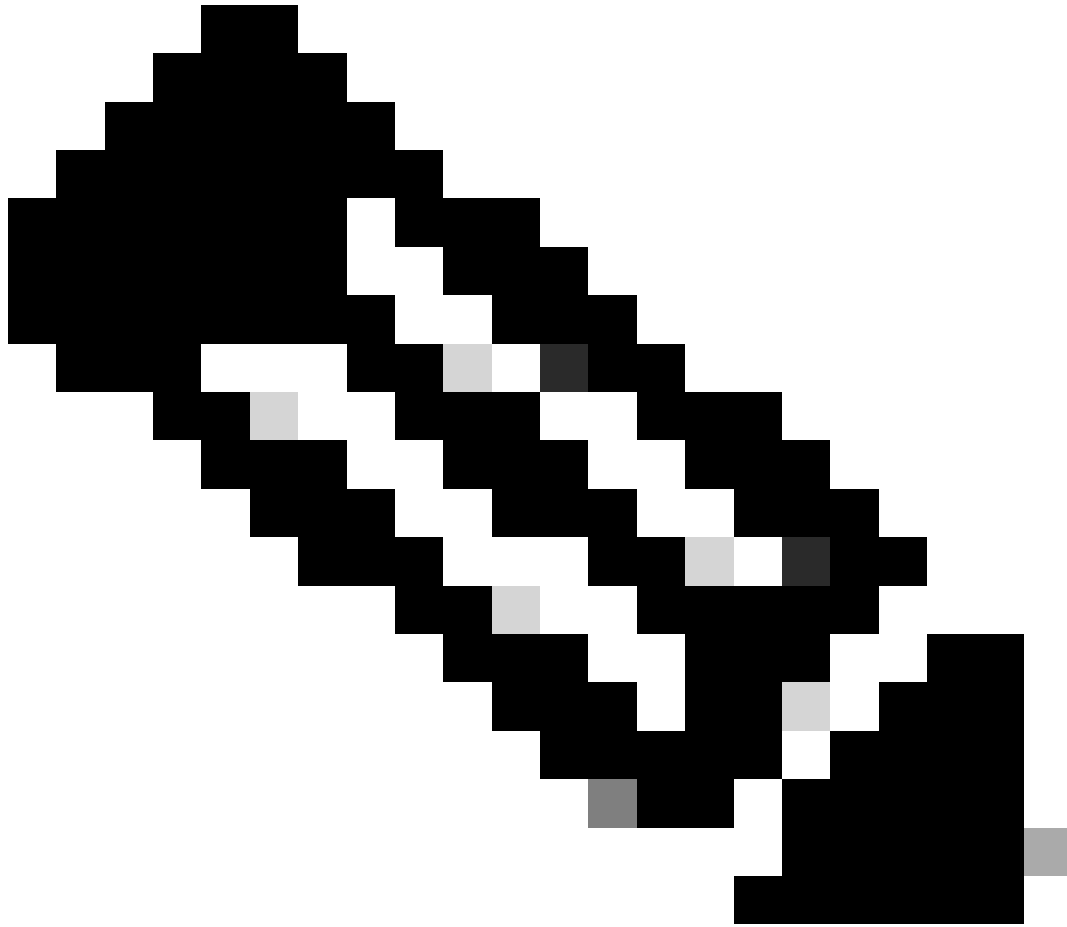


참고: SNMPv3만 사용하려면 NetworkServices SNMP CommunityName을 빈 문자열로 설정할 수 있습니다.

클라우드 등록 엔드포인트에서 SNMP 구성

일반적으로 엔드포인트의 컨피그레이션은 다음 네 가지 방법으로 변경할 수 있습니다.

1. Webex API 사용 가능
2. 엔드포인트 GUI
3. 컨트롤 허브
4. 엔드포인트에 직접 SSH



참고: 엔드포인트 GUI에 액세스하려면 브라우저를 열고 URL 표시줄에 엔드포인트의 IP 주소를 입력합니다. 엔드포인트와 동일한 네트워크에 있어야 하며, 로그인할 수 있는 사용자 자격 증명이 있어야 합니다.

모든 구성이 네 가지 방식으로 이루어지는 것은 가능하지 않다. 이 문서의 시나리오에서 SNMP 모드는 네 가지 방법으로 모두 활성화할 수 있지만 SNMP를 통해 디바이스와 통신할 수 있는 SNMP 사용자를 생성하려면 엔드포인트에 SSH를 할당하거나 Webex API를 사용하거나 Customization(사용자 지정) 섹션의 Developer API에서 엔드포인트의 GUI를 사용해야 합니다. USM 사용자는 엔드포인트의 Control Hub All Configurations(제어 허브 모든 컨피그레이션) 섹션에서 생성할 수 없습니다.



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:

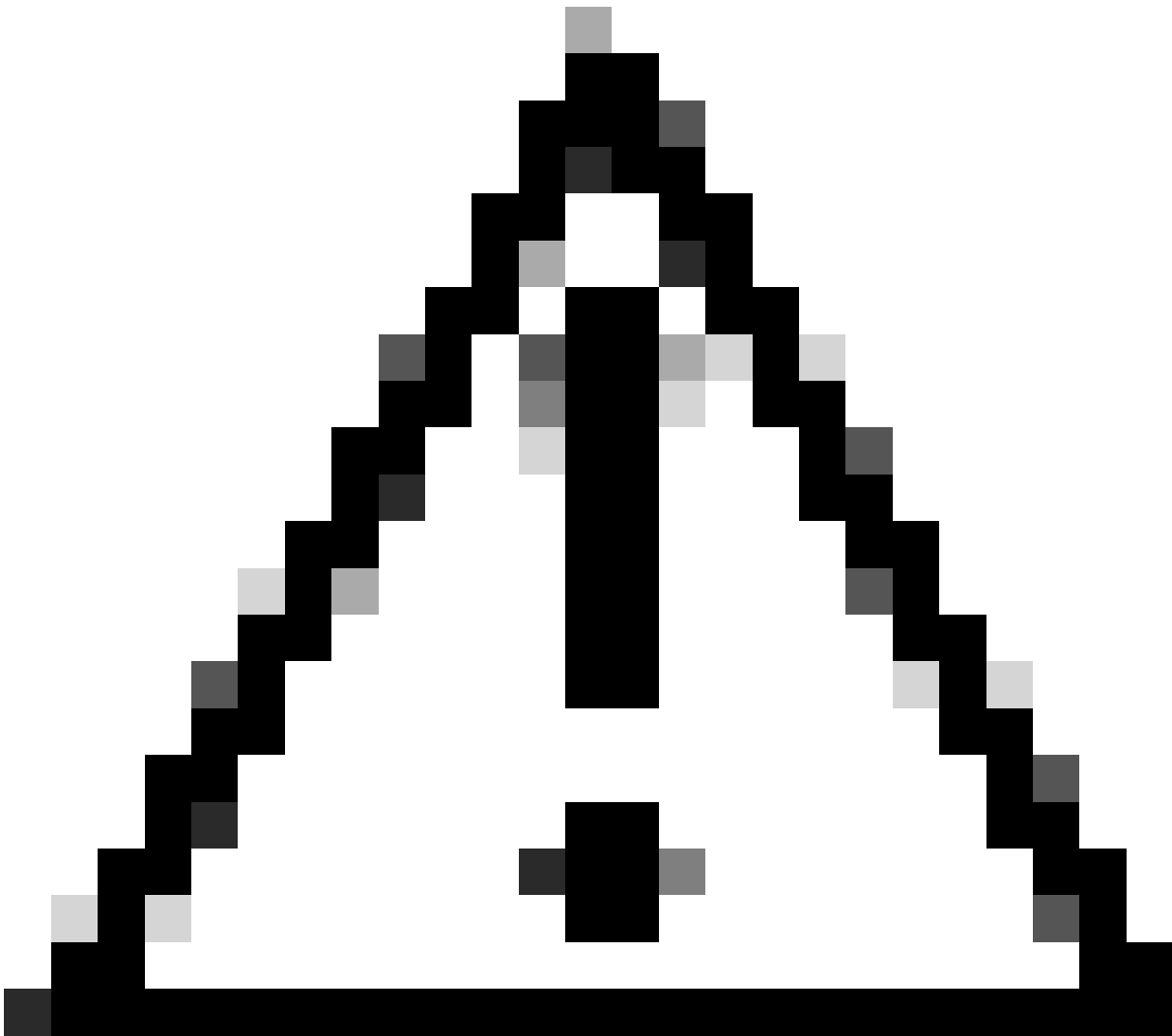
xCommand Dial Number: "person@example.com" Protocol: SIP

xCommand Network SNMP USM User List

Execute

1 of 1 applied successfully.

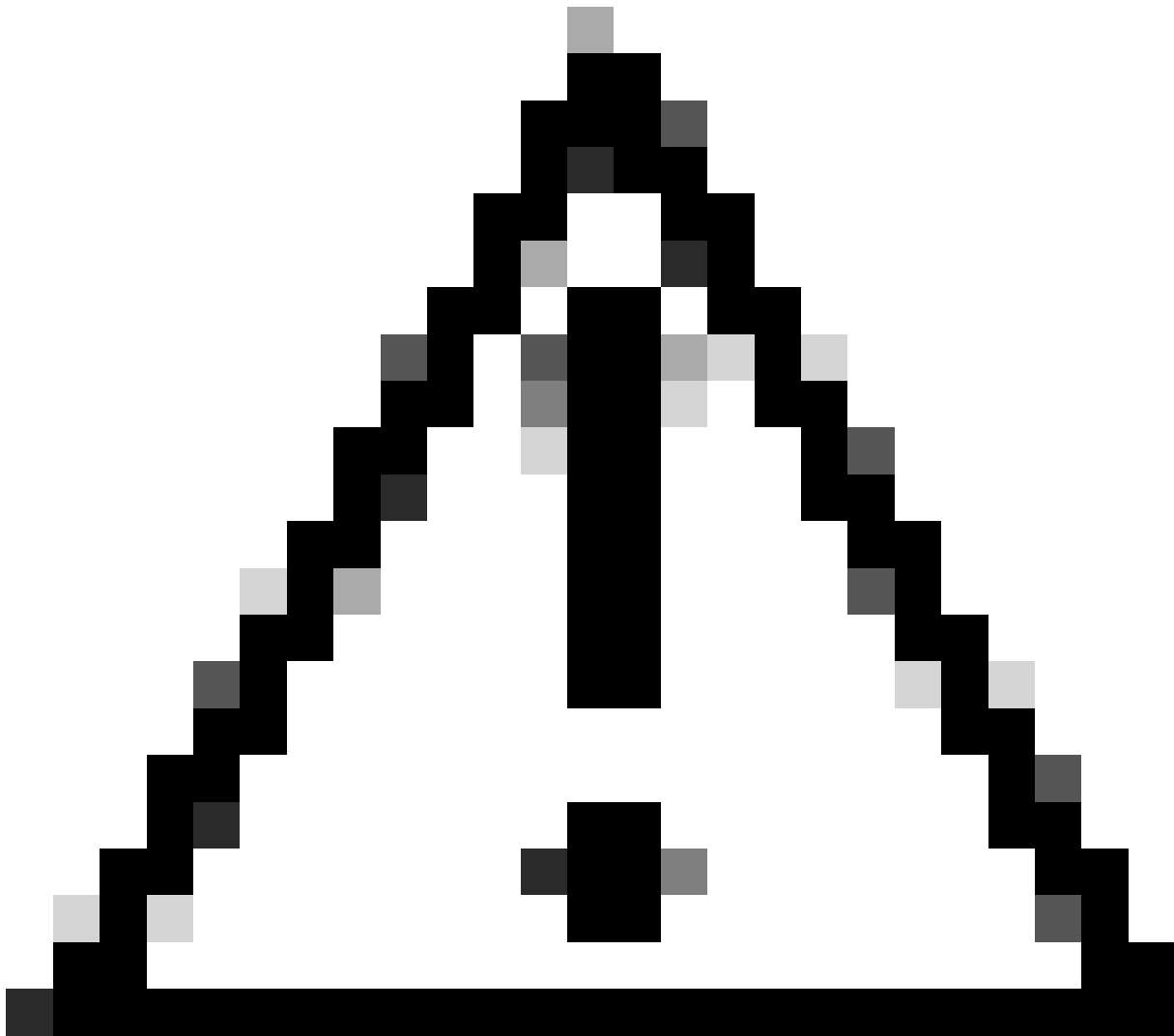
엔드포인트 GUI의 개발자 API 섹션



주의: Execute Commands and Configurations(명령 및 컨피그레이션 실행) 텍스트 상자에서 실행된 명령은 결과를 반환하지 않습니다. 명령이 성공적으로 실행되었는지 여부만 확인할 수 있습니다. USM 사용자를 나열하는 명령이 이전 스크린샷의 결과를 반환하지 않는 이유는 이 때문입니다. 즉, 엔드포인트의 GUI의 이 섹션에서 USM 사용자를 생성할 수 있지만 사용자가 생성되었는지 다시 확인하려면 디바이스에 SSH를 적용해야 합니다.

SNMPv2c를 구성하는 경우 사용자를 생성할 필요가 없습니다. 인증은 엔드포인트에 구성된 커뮤니티 이름(커뮤니티 문자열이라고도 함)을 사용하여 수행됩니다. 디바이스에 이미 존재하는 엔드포인트의 SNMP 에이전트는 디바이스에 구성된 커뮤니티 이름과 일치하는 요청에 응답합니다. 관리 시스템의 SNMP 요청에 일치하는 커뮤니티 이름(대/소문자 구분)이 포함되어 있지 않으면 메시지가 삭제되고 비디오 디바이스의 SNMP 에이전트가 응답을 보내지 않습니다.

그러나 SNMPv3에서는 인증에 성공하려면 USM 사용자를 구성해야 합니다. 이를 위해 Network SNMP USM User 명령을 사용해야 합니다. 이는 디바이스에 직접 SSH를 사용하거나 Developer API 섹션에서 디바이스 GUI를 사용하여 수행할 수 있습니다. 또는 Webex API를 사용할 수 있습니다.

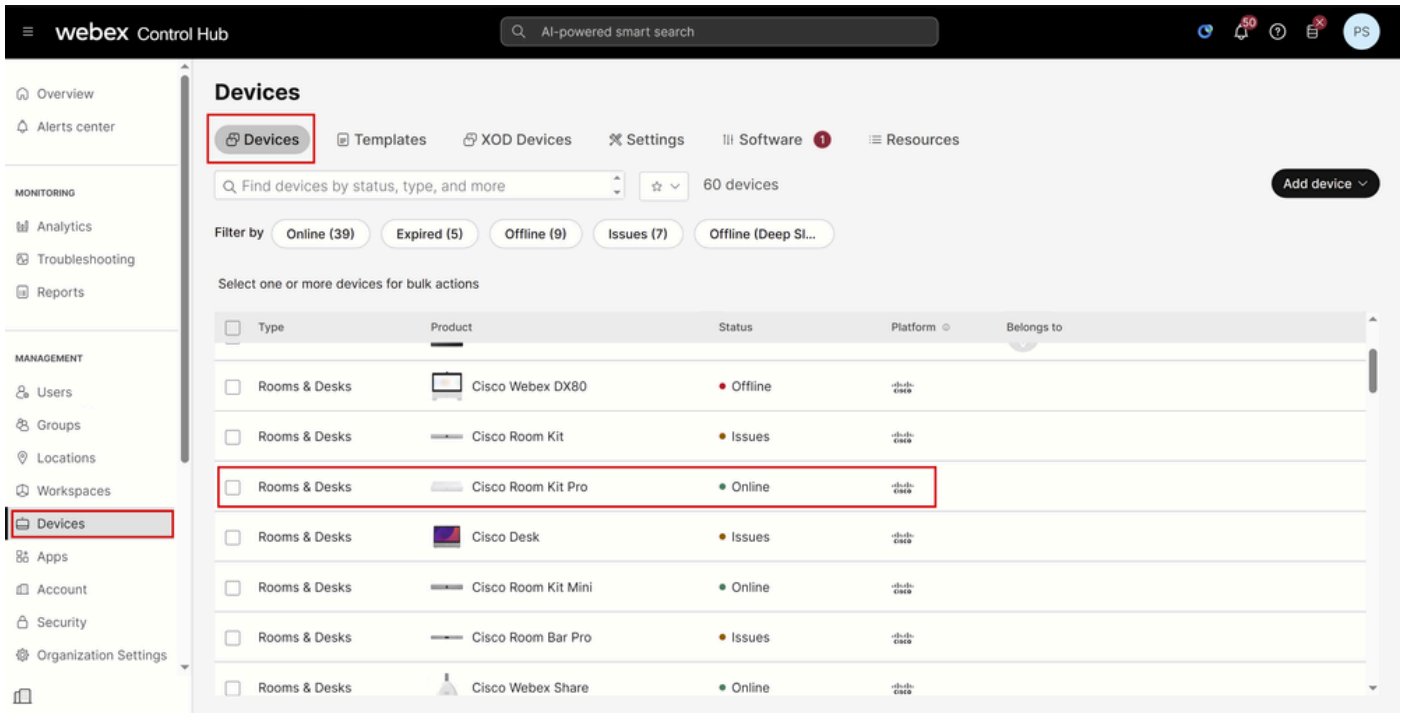


주의: SNMPv2, SNMPv3 또는 둘 모두를 활성화할지 결정해야 합니다. SNMPv1은 Cisco 엔드포인트에서 지원되지 않습니다. SNMPv1을 사용하려고 하면 실패합니다.

이 문서에서는 SNMPv2 및 SNMPv3 프로토콜이 Control Hub에서 활성화 및 구성되지만 SNMP3 인증에 필요한 USM 사용자는 SSH를 통해 구성됩니다.

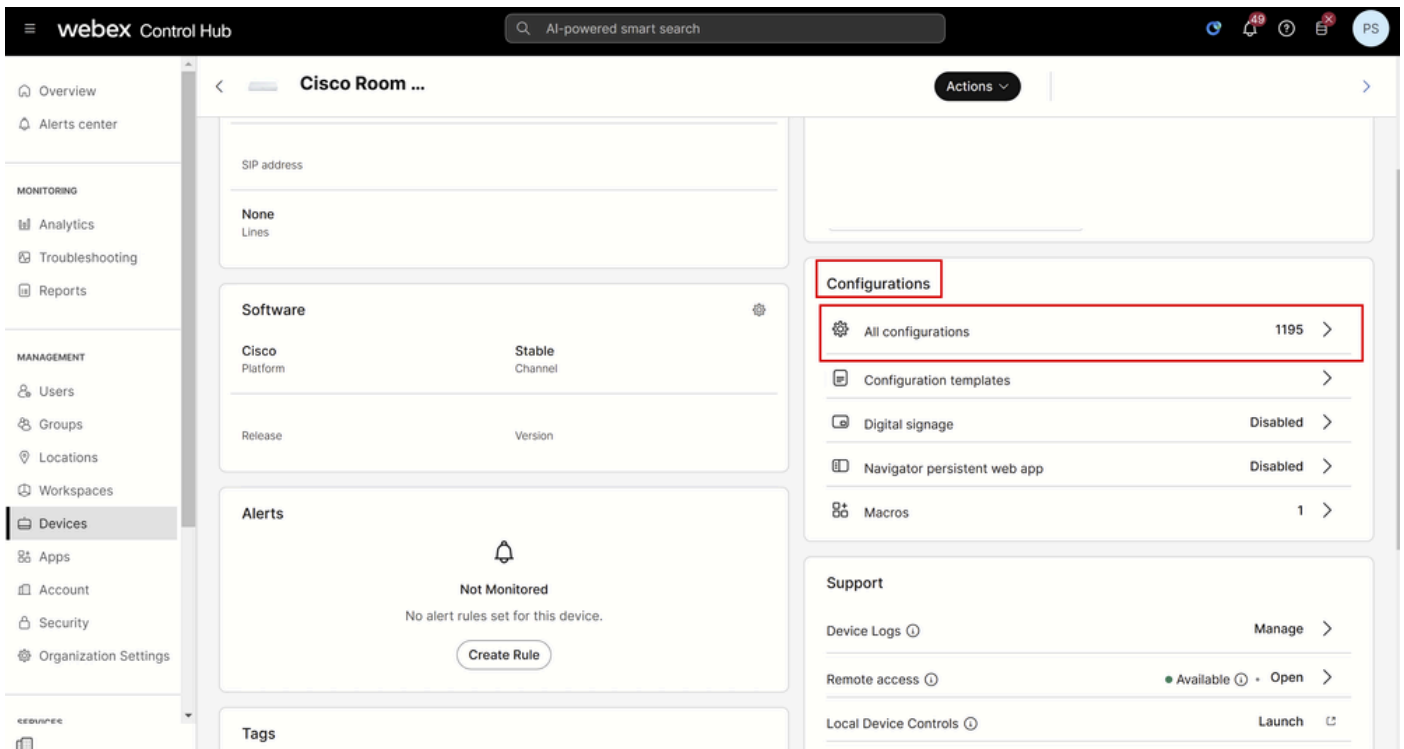
제어 허브에서 SNMPv2c 모드 활성화

admin.webex.com으로 이동하여 관리자 자격 증명으로 로그인합니다. 전체 관리자가 되는 것이 좋습니다. 사용자 인터페이스 왼쪽의 Management(관리) 섹션 아래의 Devices(디바이스)로 이동합니다. Devices 탭에서 구성하려는 디바이스를 선택합니다. 이 예제에서는 Cisco Room Kit Pro를 사용합니다.



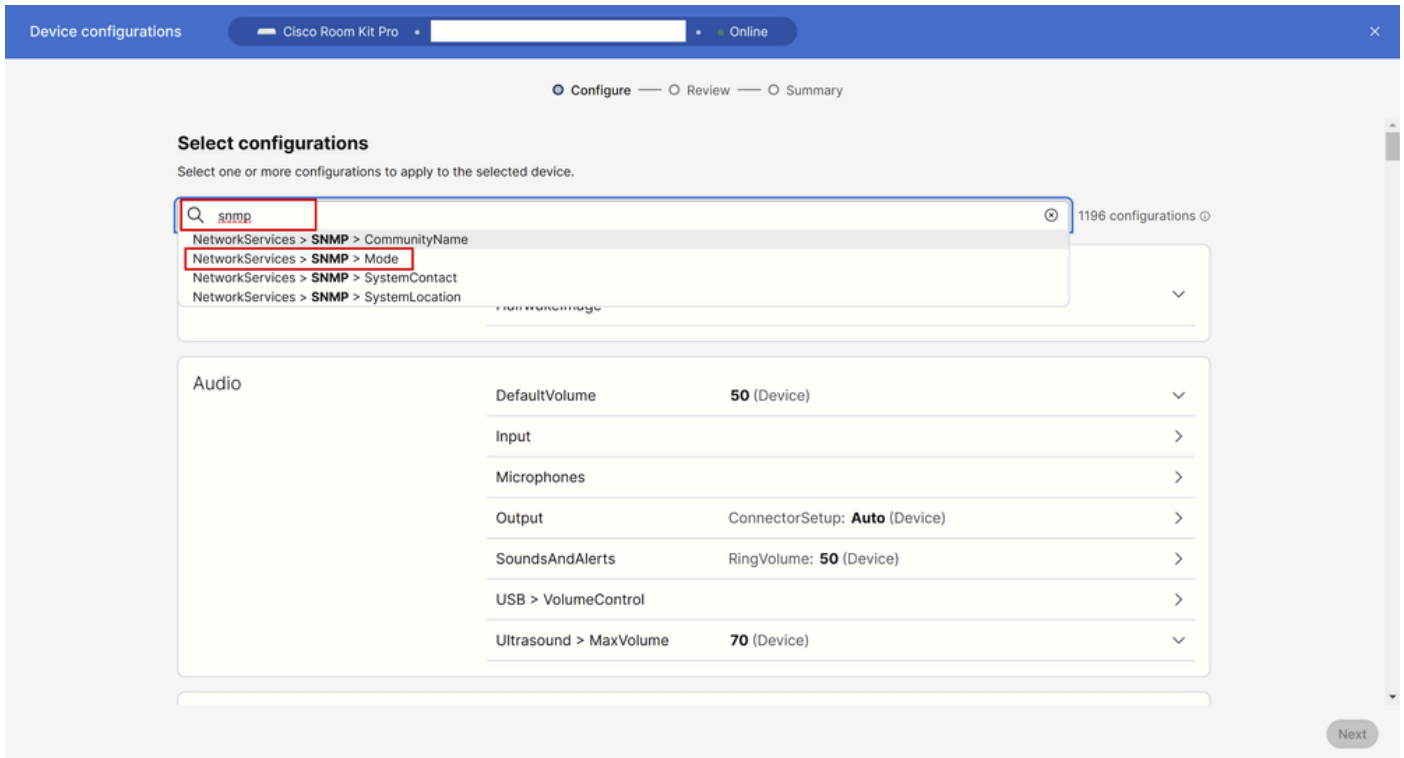
Control Hub Devices(제어 허브 디바이스) 섹션

열리는 새 Control Hub 페이지의 장비 세부사항 아래에서 Configurations(컨피그레이션) 섹션으로 이동하고 All Configurations(모든 컨피그레이션)를 클릭합니다.



Room Kit Pro의 제어 허브 장치 세부 정보

검색 표시줄에서 snmp를 입력하고 NetworkServices(네트워크 서비스) > SNMP > Mode(모드)를 선택합니다.

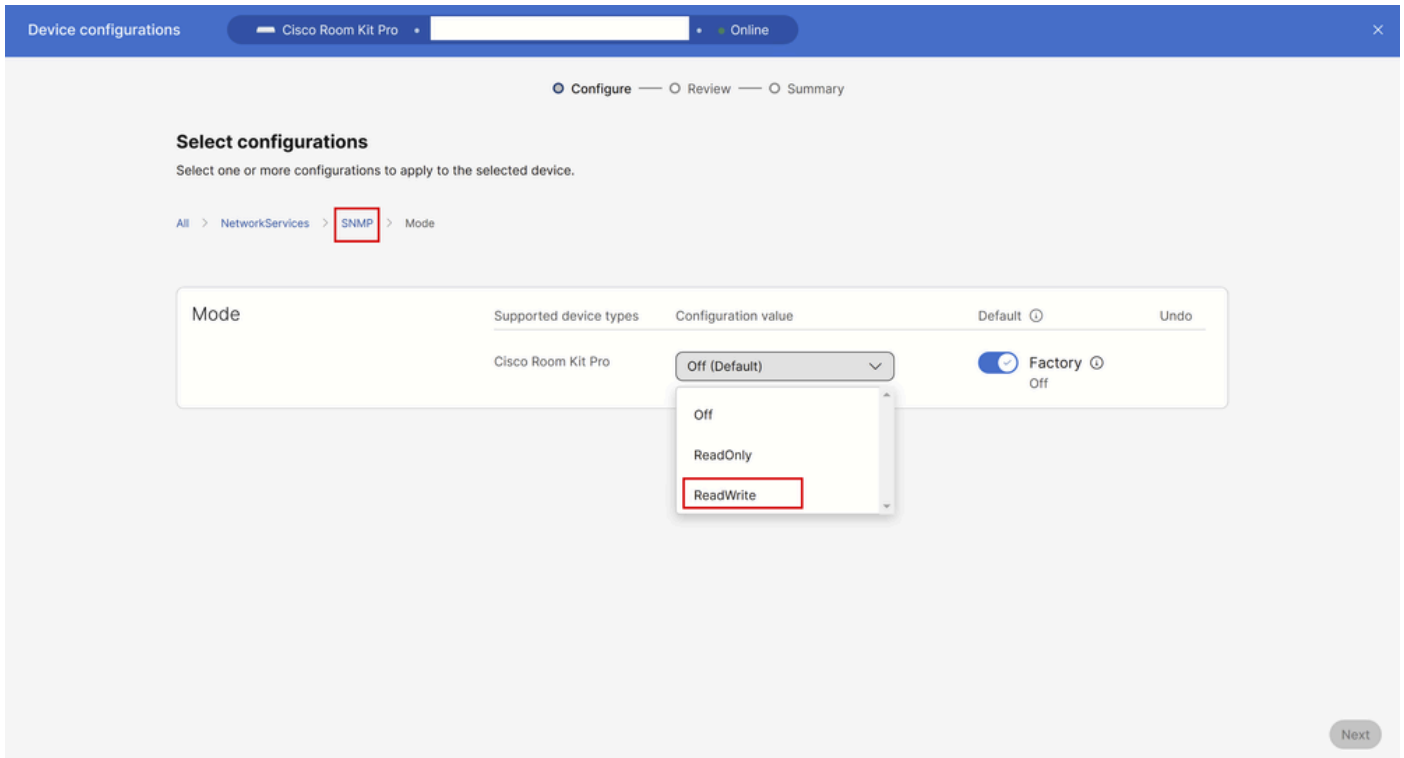


Control Hub All Configurations(제어 허브 모든 컨피그레이션) 창

해당 환경에서 활성화해야 하는 모드를 선택합니다. 다음 세 가지 옵션을 사용할 수 있습니다.

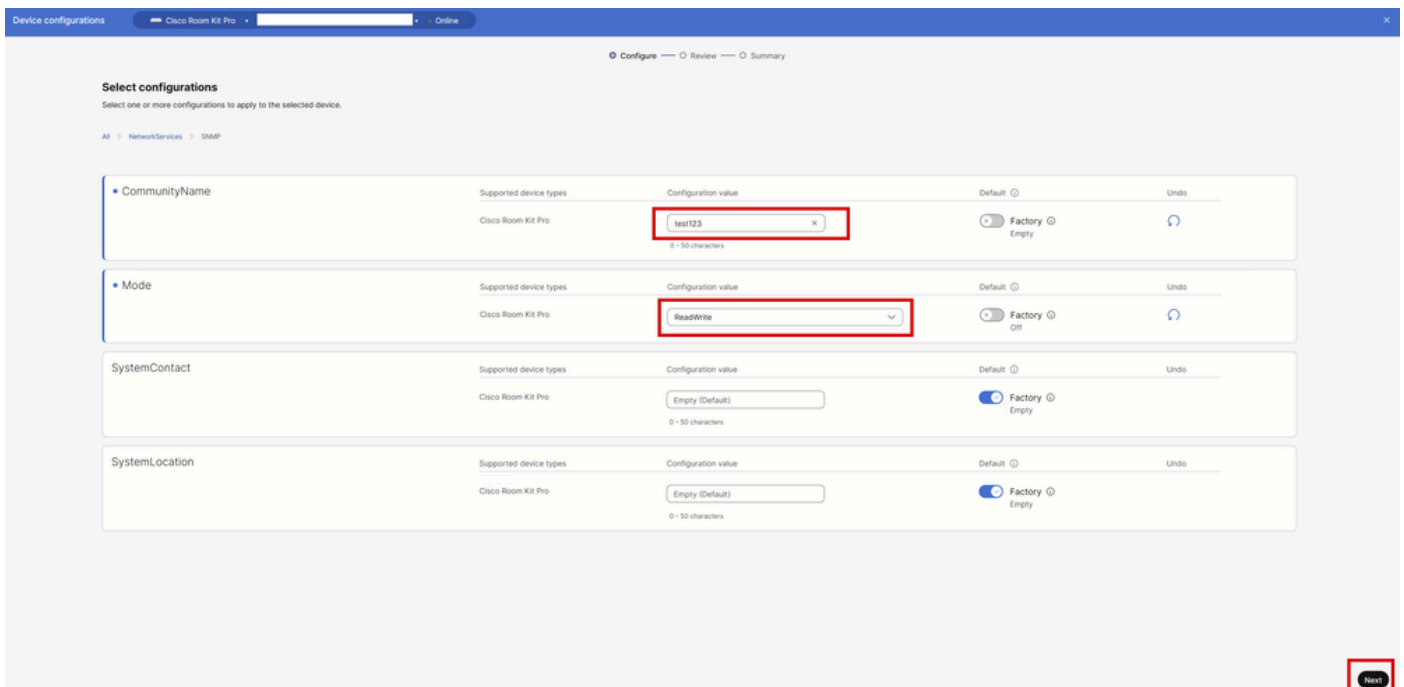
1. 끄기: SNMP 네트워크 서비스를 비활성화합니다.
2. 읽기 전용: 쿼리에만 SNMP 네트워크 서비스를 활성화합니다.
3. 읽기/쓰기: 쿼리 및 명령 모두에 대해 SNMP 네트워크 서비스를 활성화합니다.

이 예제에서는 ReadWrite를 선택합니다. 그런 다음 그림과 같이 settings(설정) 탐색 섹션에서 SNMP를 클릭합니다. 이렇게 하면 설정의 한 단계가 취소되며, Control Hub를 통해 디바이스에서 구성할 수 있는 모든 SNMP 관련 설정을 볼 수 있습니다.



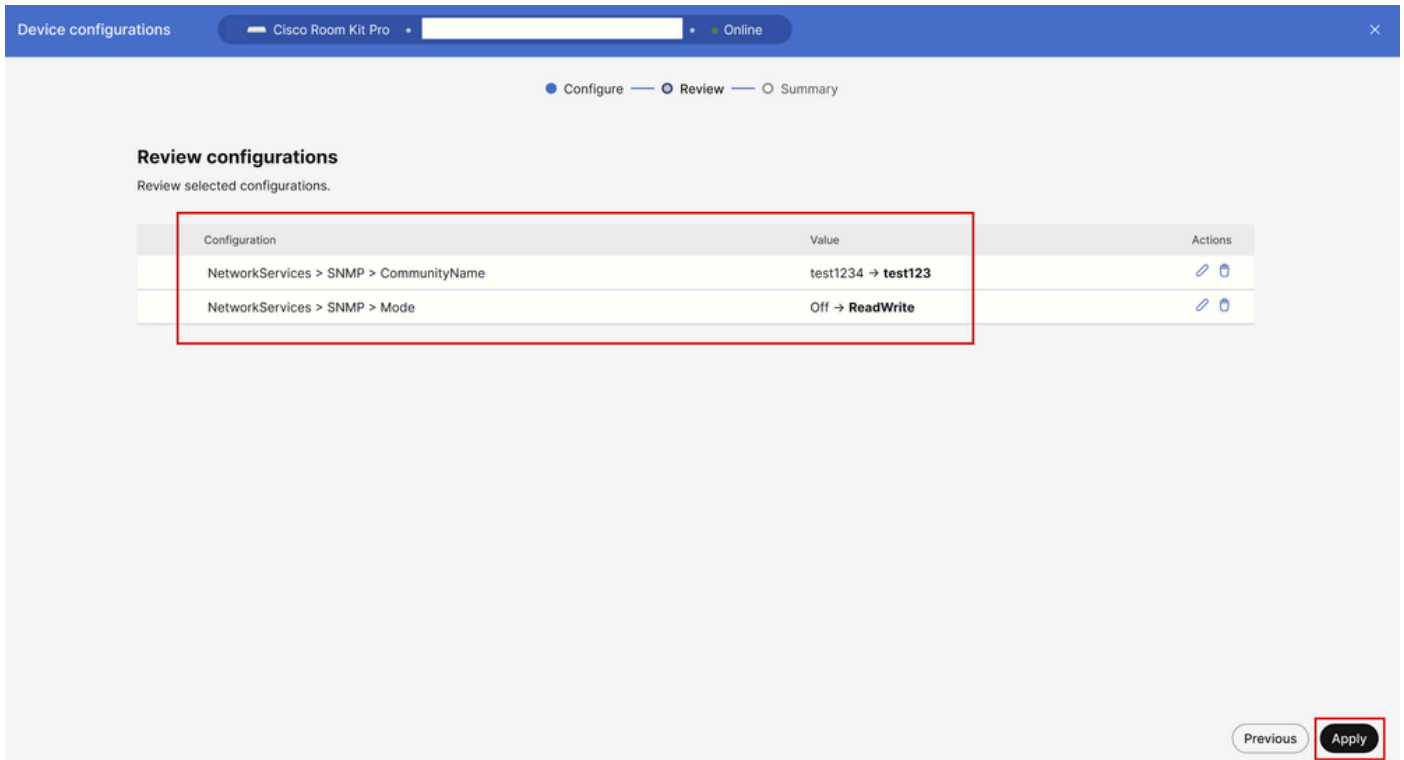
Control Hub의 All Configurations(모든 컨피그레이션)에서 SNMP 모드 설정

SNMP를 클릭하면 이 그림과 같이 사용 가능한 모든 SNMP 옵션이 나타납니다. SNMPv2를 성공적으로 설정하려면 커뮤니티 이름을 설정해야 합니다. 커뮤니티 이름은 SNMP 서버와 엔드포인트에 있는 SNMP 에이전트 간의 인증에 사용됩니다. 이 예에서 Community Name(커뮤니티 이름)은 test123으로 설정됩니다. 오른쪽 하단에서 Next(다음)를 클릭합니다.



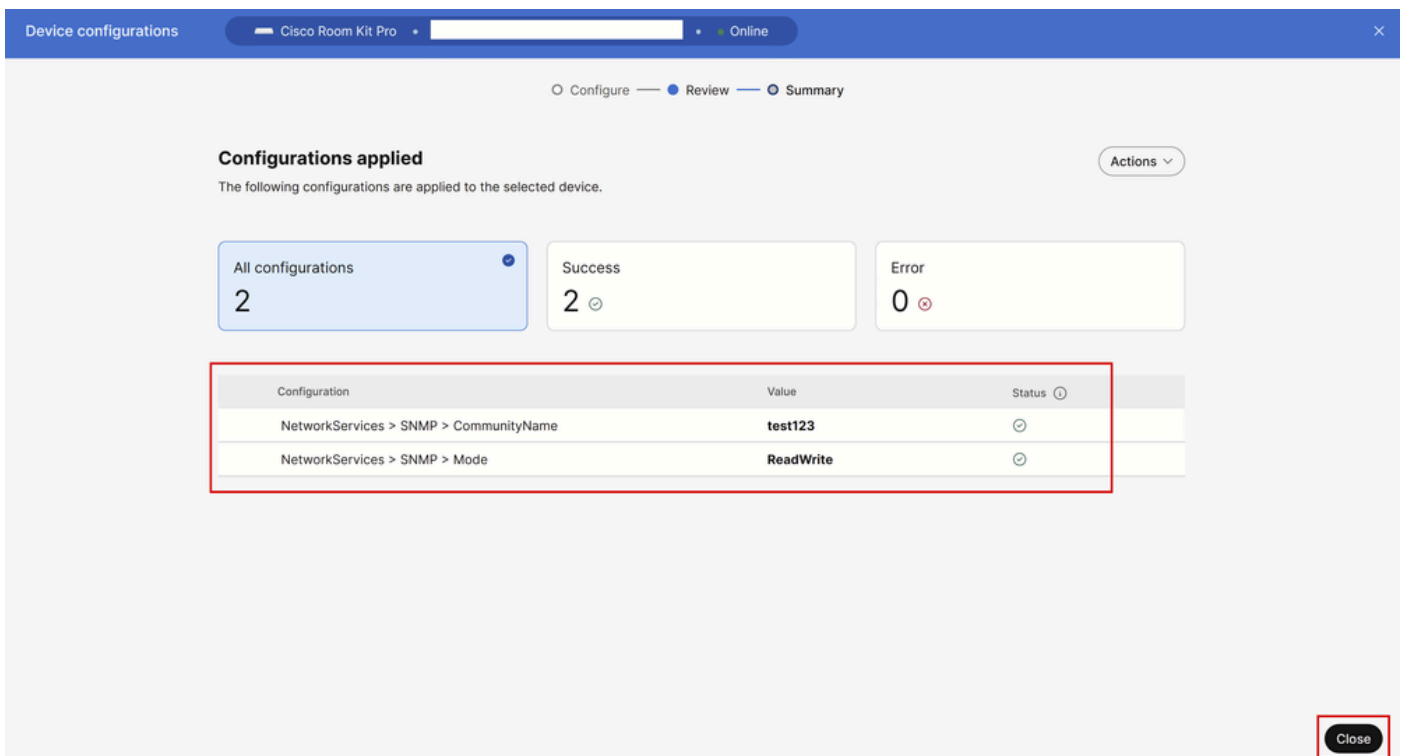
Control Hub의 All Configurations(모든 컨피그레이션) 아래에 있는 SNMP Settings(SNMP 설정)

디바이스 컨피그레이션을 검토하고 오른쪽 하단의 Apply(적용)를 클릭합니다.



변경 사항을 적용하기 전에 컨피그레이션 검토

컨피그레이션 변경 사항이 성공적으로 적용되었는지 확인합니다. 그런 다음 닫기를 클릭합니다.



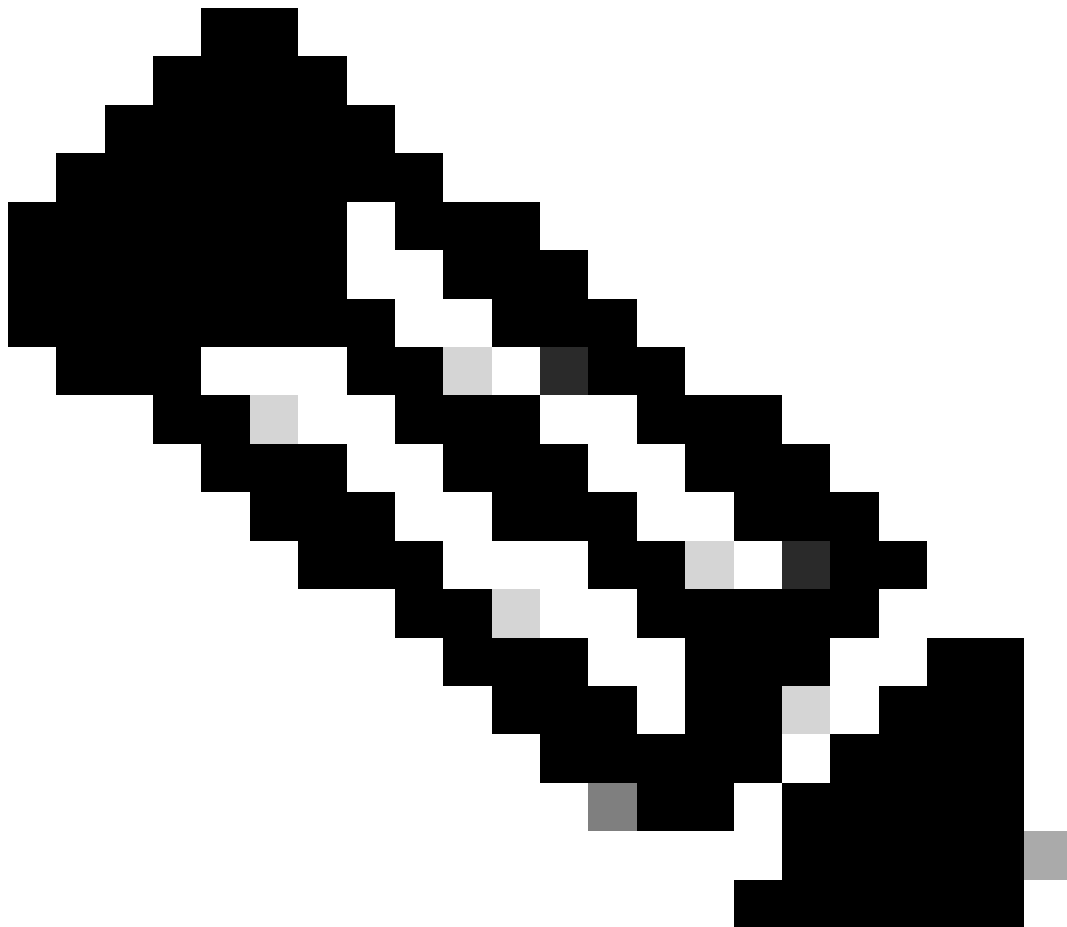
엔드포인트 컨피그레이션이 제어 허브에 성공적으로 적용됨

이 단계에서 엔드포인트에서 SNMPv2c가 성공적으로 활성화되고 커뮤니티 이름이 설정됩니다.

제어 허브에서 SNMPv3 모드 활성화

SNMPv3은 SNMPv2c에 비해 더 많은 보안을 제공하며 엔드포인트에서 다른 컨피그레이션을 필요로 합니다. Control Hub의 Management(관리) 섹션 아래의 Devices(디바이스)로 이동합니다. Devices(디바이스) 탭에서 SNMPv3으로 구성할 엔드포인트 중 하나를 선택합니다. 이 예에서는 Cisco Room Bar Pro가 사용됩니다.

장비 세부사항에서 Configurations(컨피그레이션) 섹션으로 이동하고 All Configurations(모든 컨피그레이션)를 클릭합니다. Device Configurations 페이지가 열립니다. 검색 바에 snmp를 입력하고 NetworkServices(네트워크 서비스) > SNMP > Mode(모드)를 선택합니다. 이 예에서는 SNMP 모드가 ReadWrite로 설정됩니다. SNMP를 클릭하여 디바이스에서 구성 가능한 모든 SNMP 설정을 확인합니다.



참고: 이전 예에서 SNMPv2c를 구성했을 때 SNMPv3에 대해 지금까지 언급된 모든 단계에 대해 이미 설명했습니다. 따라서 단계의 스크린샷이 제공되지 않습니다. Control Hub 설정을 탐색하는 방법에 의문이 있으면 Control Hub에서 SNMPv2c 모드 활성화 섹션을 참조하십시오.

SNMPv3만 지원하려면 커뮤니티 이름을 따옴표로 묶인 빈 문자열로 설정해야 합니다. "".

Device configurations

Cisco Room Bar Pro

Issues

Configure Review Summary

CommunityName

Supported device types Configuration value Default Undo

Cisco Room Bar Pro

0 - 50 characters

Factory Empty

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)

0 - 50 characters

Factory Empty

SystemLocation

Supported device types Configuration value Default Undo

Cisco Room Bar Pro

Empty (Default)

Factory Empty

Next

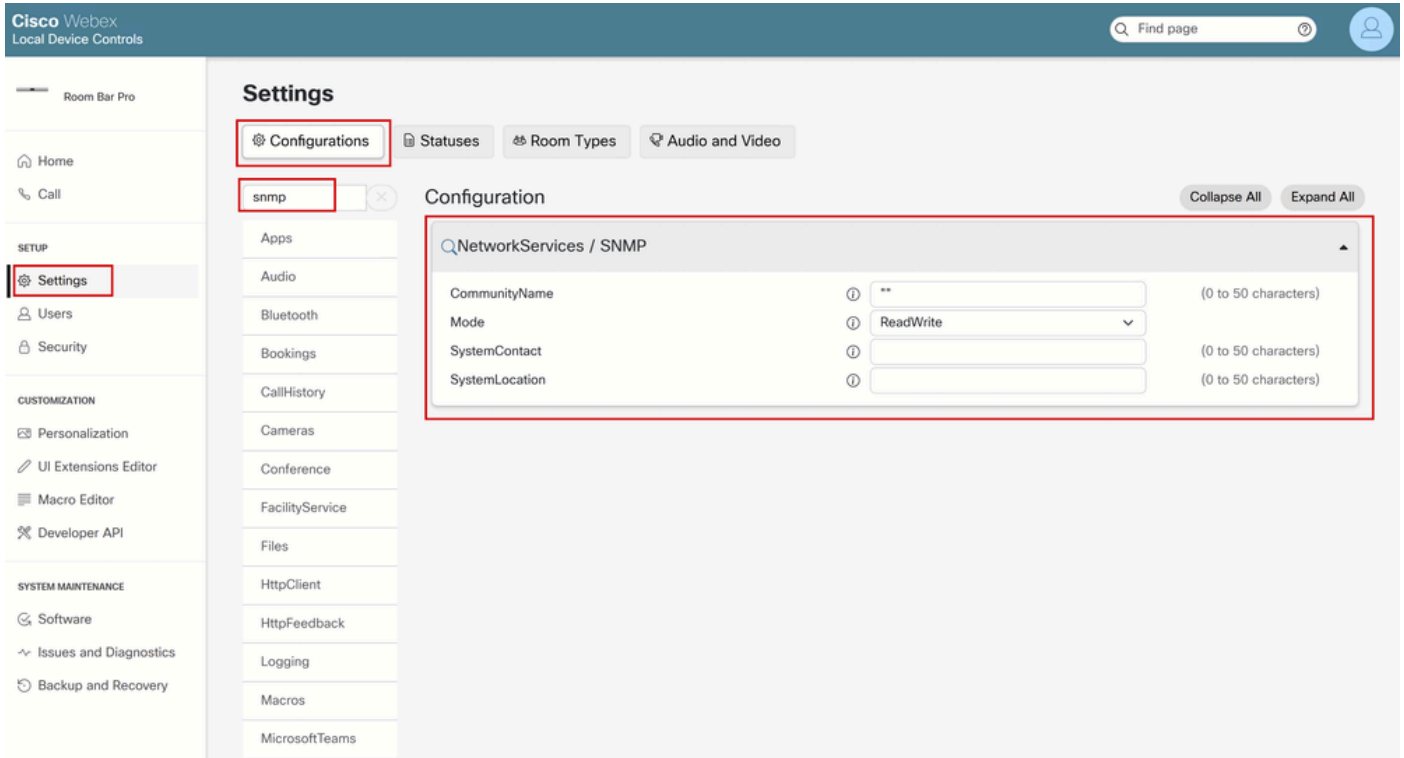
Control Hub의 All Configurations(모든 컨피그레이션) 아래에 있는 SNMP Settings(SNMP 설정)

Next(다음)를 클릭한 다음 컨피그레이션 변경 사항을 검토하고 Apply(적용)를 클릭합니다. Close(닫기)를 클릭하여 디바이스 컨피그레이션 페이지를 닫습니다.

이것으로 Control Hub에서 수행할 수 있는 컨피그레이션을 마치겠습니다. 이 단계에서는 SNMPv3만 활성화됩니다.

SNMP 컨피그레이션은 엔드포인트 GUI에서 어떻게 표시됩니까?

디바이스 GUI에서 동일한 컨피그레이션을 수행할 수 있습니다. 브라우저 탭을 열고 엔드포인트의 IP 주소를 입력합니다(엔드포인트와 동일한 네트워크에 있어야 함). 관리자 사용자로 로그인하고 엔드포인트 GUI에서 SETUP(설정) 섹션 아래의 Settings(설정)로 이동합니다. Configurations(컨피그레이션) 탭과 설정 검색 표시줄에 snmp를 계속 입력합니다. 이 그림에서는 이전 섹션에서 Room Bar Pro에서 수행한 SNMPv3 컨피그레이션에 대한 SNMP 설정이 어떻게 표시되는지 보여줍니다.



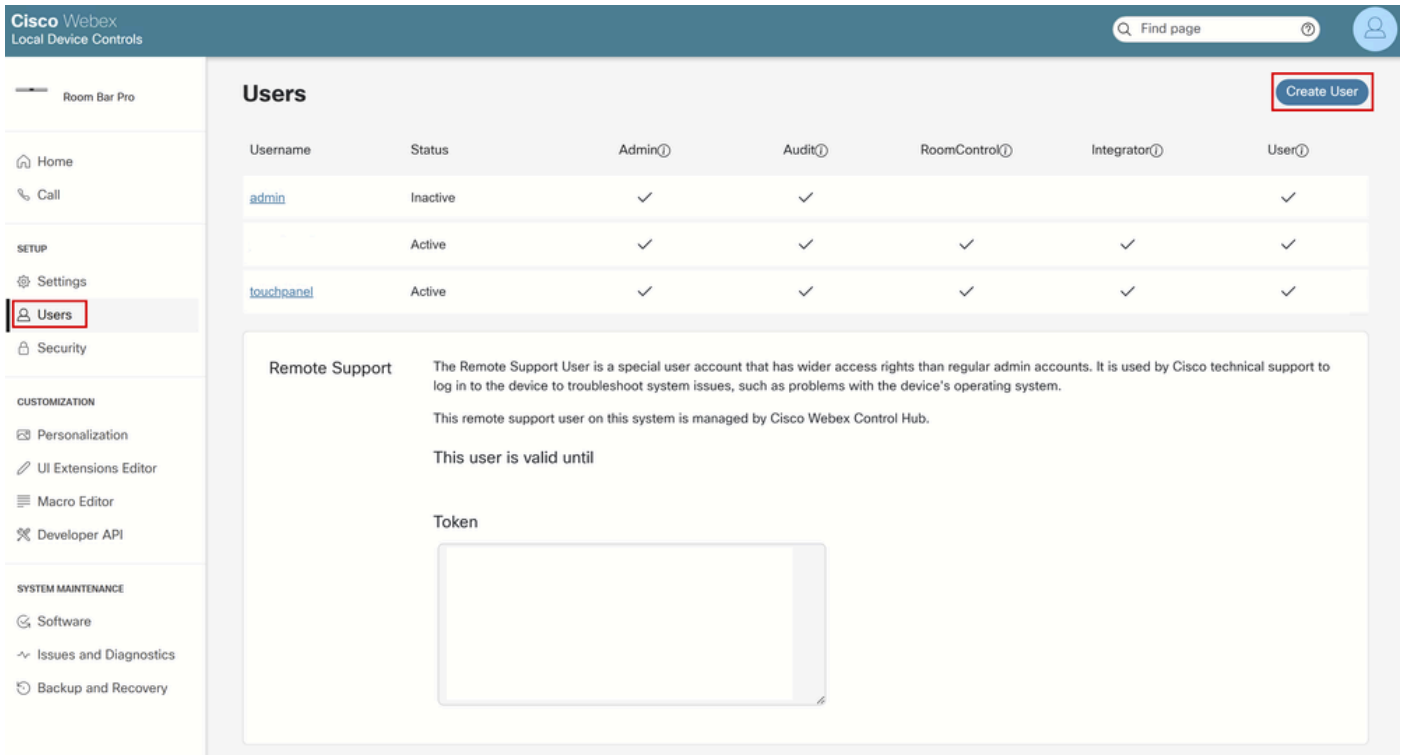
엔드포인트 GUI의 SNMPv3 컨피그레이션

SNMPv3용 USM 사용자 구성

SNMPv3를 사용하려면 USM 사용자를 생성해야 합니다. 이 작업을 수행하는 데 사용할 수 있는 명령은 [여기](#)의 Room OS 설명서 링크에서 찾을 수 있습니다. SSH를 사용하여 디바이스에 연결합니다. 이를 위해서는 디바이스에 관리자 계정이 있어야 합니다. 그렇지 않은 경우 관리자 계정을 생성해야 합니다. 이 섹션은 이 모든 과정을 거칩니다.

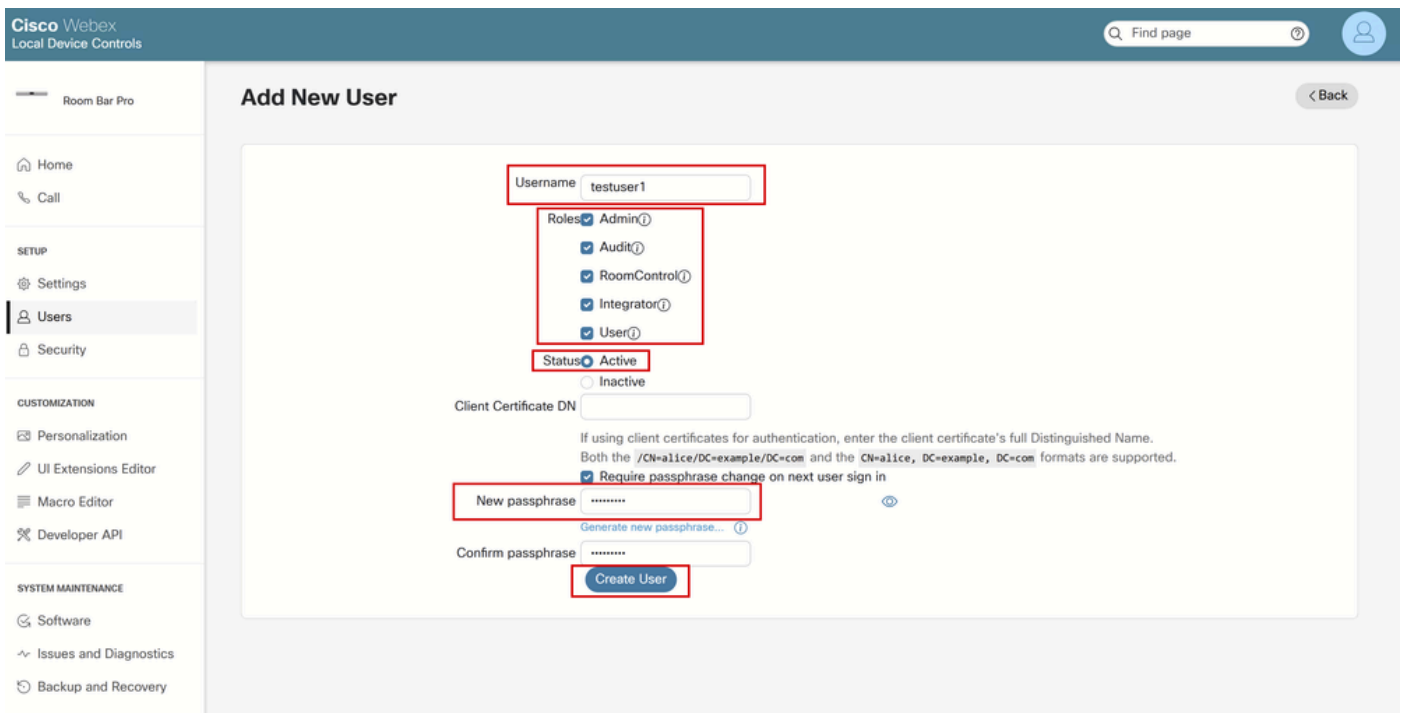
Control Hub의 Management(관리) 섹션 아래의 Devices(디바이스)로 이동합니다. Devices 탭 아래에 남아 있으며 관리자 사용자를 생성할 엔드포인트 중 하나를 선택합니다. 이 예에서는 Cisco Room Bar Pro가 사용됩니다.

디바이스 세부사항에서 Support(지원) 섹션으로 이동하고 Local Device Controls(로컬 디바이스 제어)를 클릭합니다(이 기능이 작동하려면 엔드포인트와 동일한 네트워크에 있어야 함). 디바이스 GUI가 열립니다. SETUP(설정) 섹션에서 Users(사용자)로 이동하고 Create User(사용자 생성)를 클릭합니다.



엔드포인트 GUI의 사용자 섹션

사용자 이름 및 암호(비밀번호)를 제공합니다. 사용자가 전체 관리자 권한을 가지고 있고 활성 상태인지 확인합니다.



엔드포인트의 GUI에서 사용자 생성

사용자가 생성되어 Users(사용자) 페이지에서 활성 상태인지 확인합니다.



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	✓	✓	✓	✓	✓

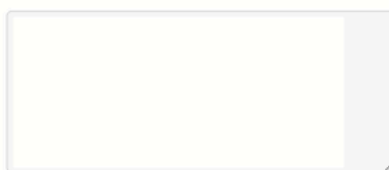
Remote Support

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.

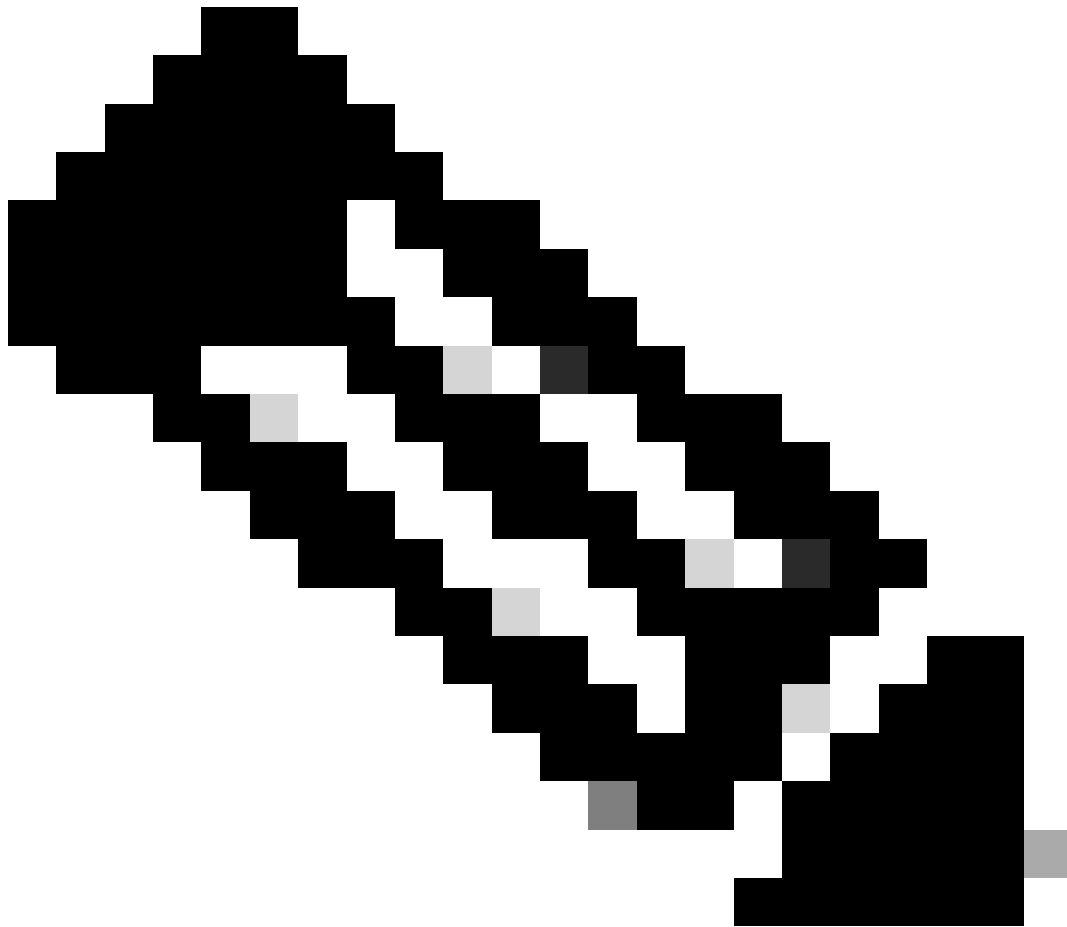
This remote support user on this system is managed by Cisco Webex Control Hub.

This user is valid until

Token



새 사용자가 생성되어 다른 사용자 사이에 나열됨



참고: 새로 생성된 사용자로 첫 번째 SSH 로그인을 시도하면 비밀번호를 변경하라는 메시지가 표시됩니다. 다음과 유사한 프롬프트가 표시됩니다.

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

SSH를 처음 사용할 때 비밀번호 변경

비밀번호가 변경되면 즉시 연결이 해제되며 새 SSH 연결을 시작해야 합니다.

관리자 사용자가 성공적으로 생성되면 원하는 SSH 클라이언트를 사용하여 엔드포인트에 연결합니다. 관리자 자격 증명으로 로그인합니다. 표시되는 프롬프트는 다음과 같습니다.

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

SSH를 통해 엔드포인트에 성공적으로 로그인했습니다.

[이](#) 문서에 설명된 대로 Network SNMP USM User Add 명령을 [사용](#)합니다. 이 데모에서 사용되는 명령은 다음과 같습니다.

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

이 명령이 정상적으로 실행되면 다음과 같은 결과가 나타납니다.

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

SSH를 통한 USM 사용자 생성

오류 없이 명령을 실행하려면 이 링크에서 공유하는 명령 설명서에 설명된 특정 규칙을 따라야 [합니](#)
[다](#). 편의상 이 명령을 위해 이 문서를 작성할 때의 현재 요구 사항을 이 그림에 붙여 넣었지만 사
용자를 작성할 때 이 [링크](#)를 참조해야 합니다. 그림의 끝에 명령의 정확한 구문이 있음을 알 수 있습
니다.

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 설명서의 USM 사용자 생성 명령 구문



경고: 오차가 있거나 충족되지 않는 요구 사항이 있는 경우 명령은 오류를 반환하고 사용자가 만들어지지 않습니다. 예를 들어, 8자 이상의 개인 정보 암호를 제공하는 대신 7자 미만의 암호를 입력할 수 있습니다.

```
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.

짧은 개인 정보 암호로 인해 USM 사용자 생성 실패

Network SNMP USM User List 명령을 사용하여 사용자가 생성되었는지 테스트할 수 있습니다. 이 명령은 디바이스에 저장된 모든 USM 사용자를 나열합니다.

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

```
OK
```

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

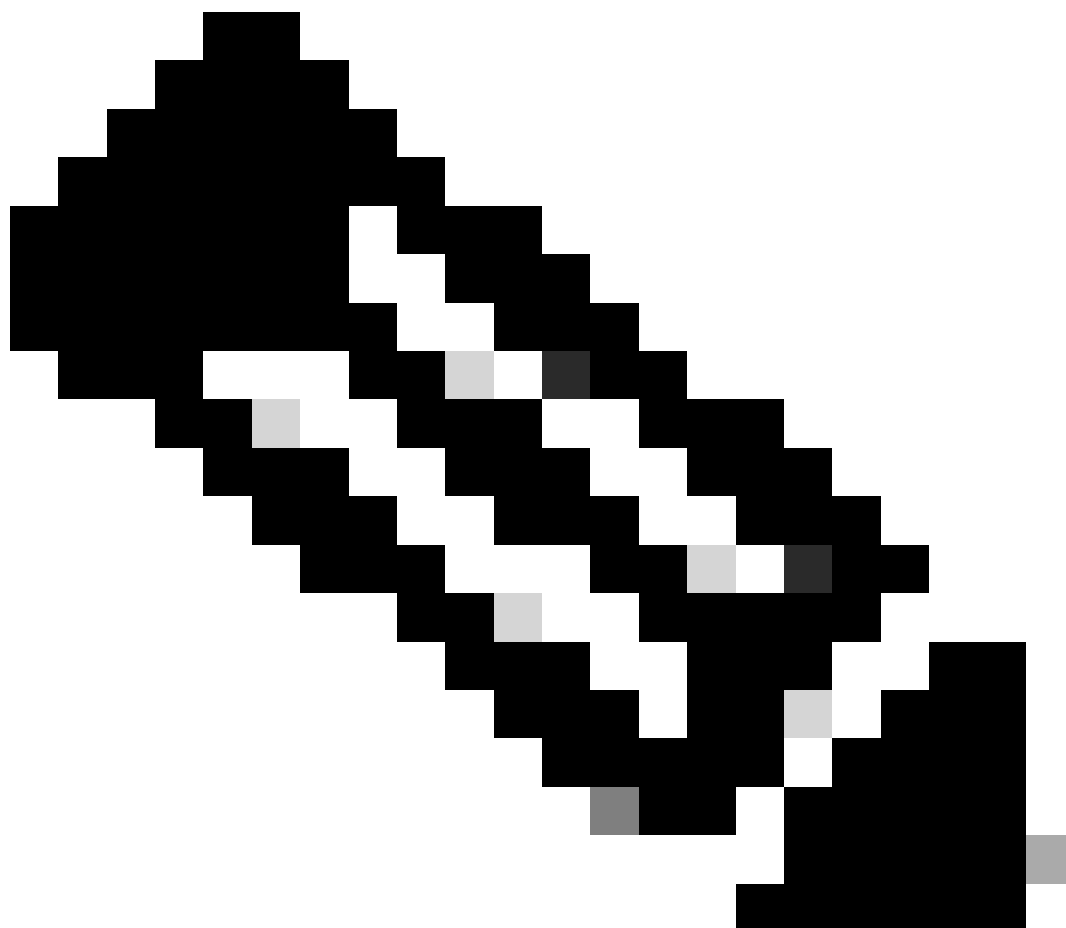
```
*r UserListResult User 1 AuthenticationProtocol: "SHA-256"
```

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

```
** end
```

사용자 생성을 확인하는 데 사용되는 네트워크 SNMP USM 사용자 목록 명령

이 단계에서는 사용자 psitaras가 성공적으로 생성된 것으로 확인되었습니다. SNMPv3 컨피그레이션이 완료되었습니다.



참고: USM 사용자 페이지는 엔드포인트의 GUI의 Users(사용자) 섹션에 표시되지 않습니다. 이것은 당연한 일입니다.

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

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

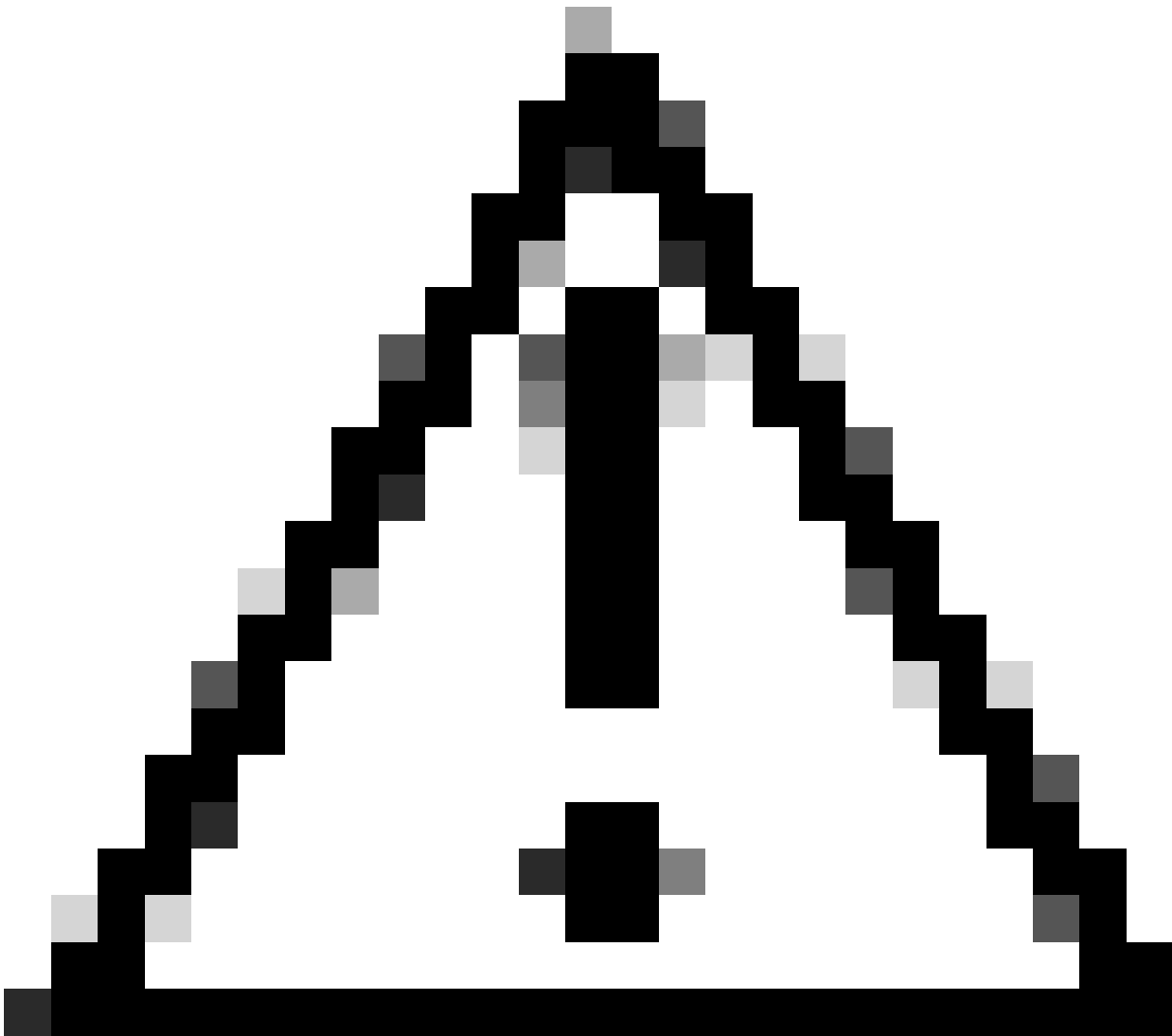
Token

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

USM 사용자는 엔드포인트 GUI의 사용자 아래에 표시되지 않습니다.

SNMPv2c 및 SNMPv3 컨피그레이션 테스트

이 단계에서는 NMS(Network Management System)를 사용하여 SNMPv2c 및/또는 SNMPv3 컨피그레이션 테스트를 진행할 수 있습니다. 이 문서의 경우 실습 컨피그레이션에는 SNMP 서비스를 실행하는 NMS 또는 SNMP 서버가 포함되어 있지 않습니다. 컨피그레이션을 테스트하기 위해 snmpwalk라는 유틸리티가 사용됩니다. 이 유틸리티는 Linux 서버에 설치됩니다.



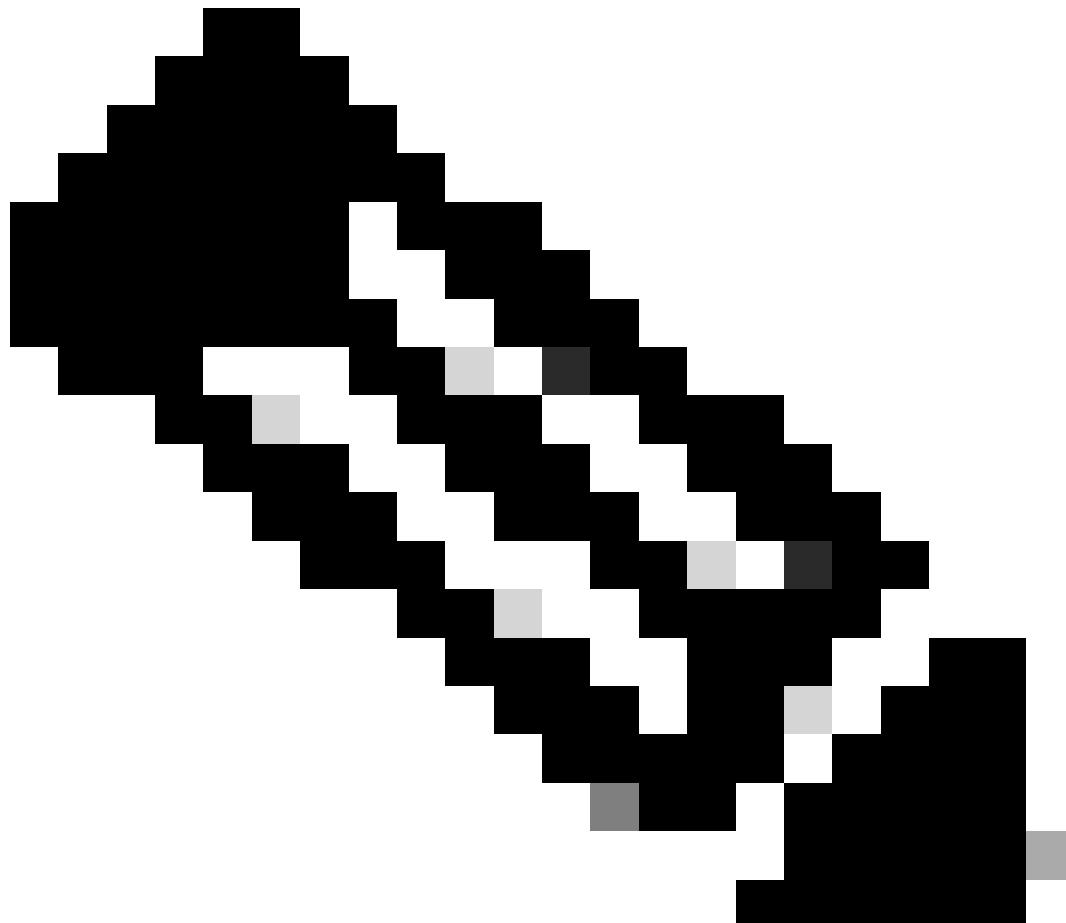
주의: Snmpwalk는 협업 엔드포인트에서 SNMP 컨피그레이션을 테스트하는 데 권장되는
툴이 아닙니다. TAC 엔지니어의 지원을 받지 않으며, 테스트를 진행하기 전에 툴 사용 방법
을 숙지해야 합니다. snmpwalk 대신 다른 SNMP 툴 또는 NMS를 사용하여 컨피그레이션을
테스트할 수 있습니다. 이 문서에서는 Snmpwalk를 예로 들며(데모를 위해 컨피그레이션을
테스트하기 위한 툴이 필요함), 그 사용과 관련된 약속이나 프로모션은 없습니다.

snmpwalk 설치에 이 가이드의 일부가 아니므로 생략됩니다. 테스트에 사용 중인 시스템의
OS(운영 체제)에 따라 설치 요구 사항이 달라질 수 있습니다. 테스트하기 전에 성공적으로
설치해야 합니다.

Snmpwalk는 SNMP 컨피그레이션을 확인하는 데 사용할 수 있는 툴입니다. 엔드포인트의 MIB를 살
펴보고 사용 가능한 정보를 반환합니다. 클라우드 등록 엔드포인트는 7개의 OID(Object
Identifier)를 노출합니다.

- SNMPv2-MIB::sysDescr(읽기),
- SNMPv2-MIB::sysObjectID(읽기),
- DISMAN-EVENT-MIB::sysUpTimeInstance(읽기),

- SNMPv2 -MIB::sysContact(읽기/쓰기),
 - SNMPv2 -MIB::sysName(읽기/쓰기),
 - SNMPv2 -MIB::sysLocation(읽기/쓰기),
 - SNMPv2 -MIB::sysServices(읽기).
-



참고: 나열된 snmpwalk 테스트에 사용되는 내부 IP는 프라이빗 IP이며 더 이상 사용되지 않습니다. 이 가이드에 사용된 Lab이 서비스 해제되었으며 디바이스가 공장 초기화 상태입니다.

Cisco Room Kit Pro 엔드포인트는 SNMPv2c로 구성됩니다. 인증은 커뮤니티 문자열을 사용하여 수행됩니다. 다음 명령을 실행합니다.

```
# '-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
```

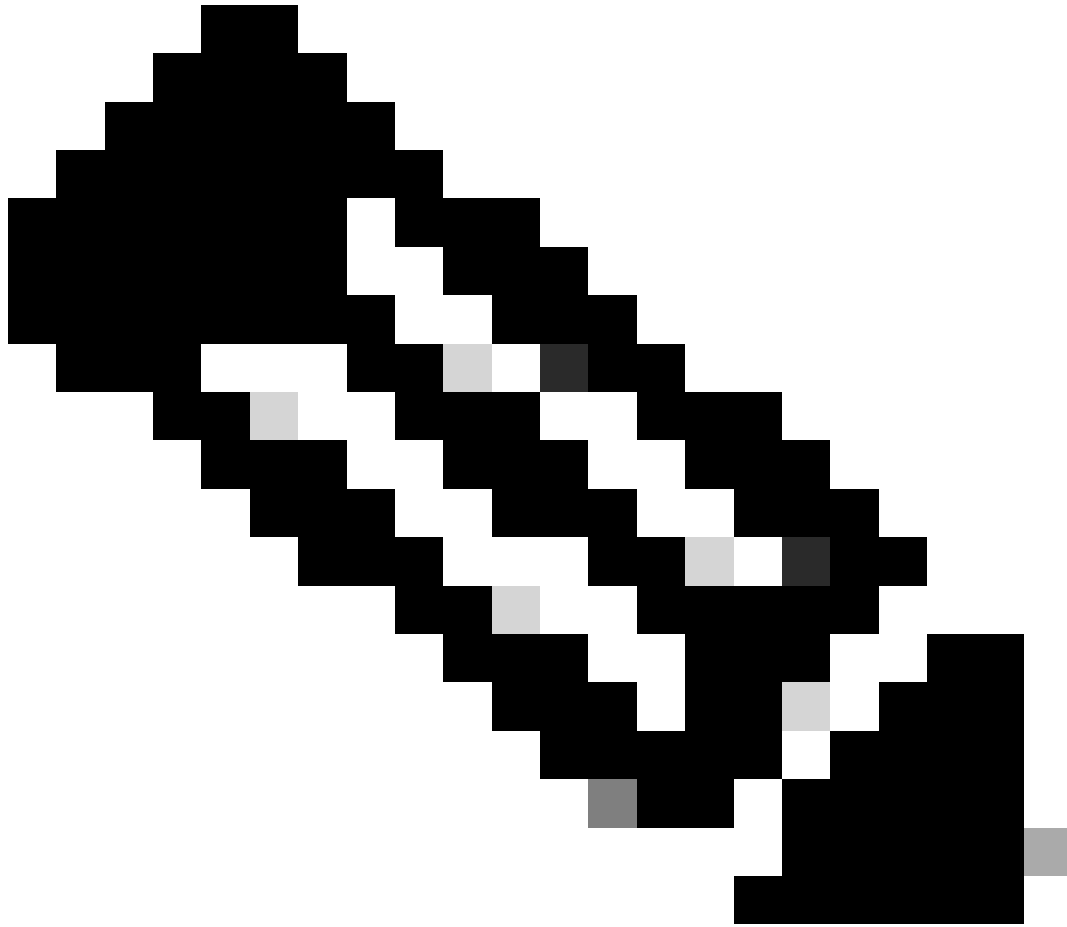
```
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco Codec  
SoftW: ce11.26.1.5.53ff615d0d9  
MCU: Cisco Codec Pro  
Date: 2025-02-28  
S/N: FD02706JG49"  
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.5596.150.6.4.1  
iso.3.6.1.2.1.1.3.0 = Timeticks: (106770681) 12 days, 8:35:06.81  
iso.3.6.1.2.1.1.4.0 = ""  
iso.3.6.1.2.1.1.5.0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

Snmpwalk는 예상대로 7개의 결과를 반환합니다. 비어 있는 MiB는 3개입니다.

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

이러한 MiB에 값을 설정하는 데 사용할 수 있는 세 가지 xConfiguration 명령이 있습니다. SSH를 엔드포인트에 연결하고 다음 명령을 실행합니다.

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



참고: 이 세 명령을 사용하는 대신 Control Hub, 엔드포인트 GUI 또는 Webex API에서 이러한 설정을 변경할 수 있습니다.

위 명령이 실행되면 동일한 엔드포인트에서 snmpwalk를 다시 사용합니다. 이전에 비어 있던 MiB는 xConfiguration 명령을 통해 제공된 값으로 채워집니다.

```
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)
```

이 단계에서는 Room Kit Pro 디바이스에서 만든 SNMPv2c 컨피그레이션이 작동 중임을 확인합니다.

Cisco Room Bar Pro 엔드포인트는 SNMPv3로 구성됩니다. SNMPv3의 경우 적절한 인증을 사용해야 합니다. 커뮤니티 문자열은 사용되지 않습니다. 대신 SNMPv3는 사용자 이름 및 비밀번호를 사용합니다.

```
# '-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)
```

이 단계에서는 Room Bar Pro 디바이스에서 만든 SNMPv3 컨피그레이션이 작동 중인지 확인합니다.

엔드포인트에 SNMPv2c 및 SNMPv3이 동시에 활성화 상태여야 합니까?

네, 가능합니다. 그러나 SNMPv2c 인증을 사용하려면 SNMP 컨피그레이션 중에 커뮤니티 이름을 설정해야 합니다. 이 테스트에서는 이전 예제의 Room Bar Pro가 사용됩니다. 엔드포인트의 Control Hub All Configurations 섹션에 있는 현재 컨피그레이션은 다음과 같습니다.

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	

제어 허브의 엔드포인트 SNMP 컨피그레이션

커뮤니티 이름이 비어 있지 않습니다. 커뮤니티 이름이 빈 문자열임을 나타내는 두 개의 따옴표가 있습니다. NetworkServices SNMP CommunityName을 빈 문자열("")로 설정하여 SNMP 지원을 버전 3으로만 제한할 수 있습니다. 이 문자열을 커뮤니티 이름(예: testbothSNMPv2_v3)으로 대체해야 합니다.

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	

Control Hub 엔드포인트 컨피그레이션 설정에서 SNMPv2c에 대한 커뮤니티 이름 추가

SNMPv3이 Room Bar Pro에서 작동 중인 것으로 이미 확인되었습니다. Snmpwalk는 커뮤니티 이름을 설정한 후 SNMPv2c도 작동하는지 여부를 테스트하는 데 사용됩니다.

```
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)
```

SNMP를 사용하는 제어 허브를 통해 여러 엔드포인트를 구성할 수 있습니까?

예. Control Hub에서 여러 디바이스를 한 번에 구성할 수 있습니다. 이 [문서](#)는 여러 디바이스 구성 섹션의 단계별 실행 방법에 대한 정보를 제공합니다.

기억해야 할 중요한 세부 사항

- 특정 MiB만 사용할 수 있습니다. 엔드포인트를 설계하는 엔지니어링 팀의 설계에 따라 사용할 가능한 MiB 수가 제한됩니다. MiB는 더 많은 정보를 제공하기 위해 확장하거나 개선할 수 없습니다.
- SNMPv2c는 커뮤니티 이름(커뮤니티 문자열이라고도 함)을 사용하여 인증하는 반면, SNMPv3는 사용자 이름과 비밀번호를 사용하여 인증하고 암호화도 제공합니다. 테스트할 때는 구성된 프로토콜에 대해 올바른 인증 방법(snmpwalk 또는 다른 툴/NMS 사용)을 사용하고 있는지 확인합니다.
- 인증 및 개인 정보는 항상 SNMPv3에서 사용됩니다. 엔드포인트는 authPriv 보안 수준만 지원하며 개인 정보 프로토콜은 항상 AES(Advanced Encryption Standard)입니다.
- SNMPv3은 USM(User-based Security Model) 옵션에서만 지원됩니다. TLS를 통한 SNMPv3에 대한 지원은 없습니다.
- SNMP 인증을 위해 사용자를 구성하는 데 사용되는 USM 사용자 명령은 SNMPv2c에 영향을 주지 않습니다.
- 엔드포인트의 SNMP CommunityName 설정은 SNMPv3 컨피그레이션에 영향을 주지 않습니다.
- SNMP CommunityName은 대/소문자를 구분합니다.
- NetworkServices SNMP CommunityName을 빈 문자열("")로 설정하여 SNMP 지원을 v3으로만 제한할 수 있습니다.
- SNMPv1은 지원되지 않습니다.
- SNMPv2c 및 SNMPv3 모두에서 엔드포인트는 동일한 OID(object identifier)를 노출합니다.
- SNMPv3의 경우 인증 프로토콜이 SHA-2 제품군에 있어야 합니다(MD와 SHA-1은 지원되지 않음). 그렇지 않은 경우 SNMP 요청은 인증에 실패하고 응답하지 않습니다.
- 프라이버시 비밀번호는 디바이스에 현지화된 해시된 값(AES-128)으로 저장됩니다. 프라이버시 비밀번호가 이 매개변수에 명시적으로 설정되지 않은 경우 인증 비밀번호와 동일하게 설정됩니다(Authentication Protocol 매개변수에 지정된 해시 함수 사용).
- 비밀번호/암호 및 사용자 이름은 특정 길이 범위 내에 있어야 합니다. 예를 들어, USM 사용자 이름은 최대 32자여야 하며 인증 비밀번호는 최소 8자, 최대 255자여야 합니다. 이러한 요구 사항이 충족되지 않으면 Network SNMP USM User Add 명령이 사용자를 생성하지 못하고 오류를 반환합니다.

엔드포인트에서 SNMP 문제 해결을 위해 TAC에 문의

엔드포인트의 SNMP 컨피그레이션이 완료되었지만 문제가 발생한 경우 TAC에 문의하여 다음 정보를 공유해야 합니다.

- Control Hub의 조직 ID 및 영향을 받는 엔드포인트의 SN(Serial Number)을 입력합니다.

- 직면한 시나리오에 대해 설명하십시오.
- 구성하려는 SNMP 버전을 제공합니다.
- 표시되는 오류 메시지를 제공합니다.
- 디바이스 컨피그레이션에 문제가 있는 경우 컨피그레이션 프로세스가 중단된 단계를 명확하게 설명하고 스크린샷을 제공합니다. 오류를 반환하는 컨피그레이션 명령을 공유합니다.
- 엔드포인트 로그를 수집하여 케이스에 업로드합니다.
- SNMP 컨피그레이션을 테스트하는 데 사용되는 유틸리티\NMS 또는 기타 도구를 공유합니다. 유틸리티를 사용하여 엔드포인트의 SNMP 에이전트에 대해 테스트하는 경우 사용된 전체 명령을 제공합니다.

관련 정보

[Room OS xAPI 설명서 - SNMP 관련 명령](#)

[보드, 데스크 및 Room Series 장치에 대한 장치 구성](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.