SNMP auf Cloud-registrierten Endgeräten konfigurieren

Inhalt

Einleitung

Dieses Dokument beschreibt die Konfiguration und Fehlerbehebung von SNMP auf einem Cloud-registrierten Endgerät.

Voraussetzungen

Anforderungen

Es wird empfohlen, dass Sie mit den folgenden Themen vertraut sind:

- Control Hub-Plattform
- Endpunktverwaltung über die grafische Benutzeroberfläche (GUI) des Endpunkts und den Abschnitt "Control Hub Devices"
- SSH zu einem Endgerät als Administrator-Benutzer
- Raumbetriebssystem
- SNMP (SNMPv2c und SNMPv3)
- SNMPwalk oder ein anderes Dienstprogramm/Tool oder Network Management System

(NMS) zum Testen der SNMP-Konfiguration

Verwendete Komponenten

Die hier aufgeführten Geräte wurden für die Durchführung der Tests und die Erzielung der in diesem Dokument beschriebenen Ergebnisse verwendet:

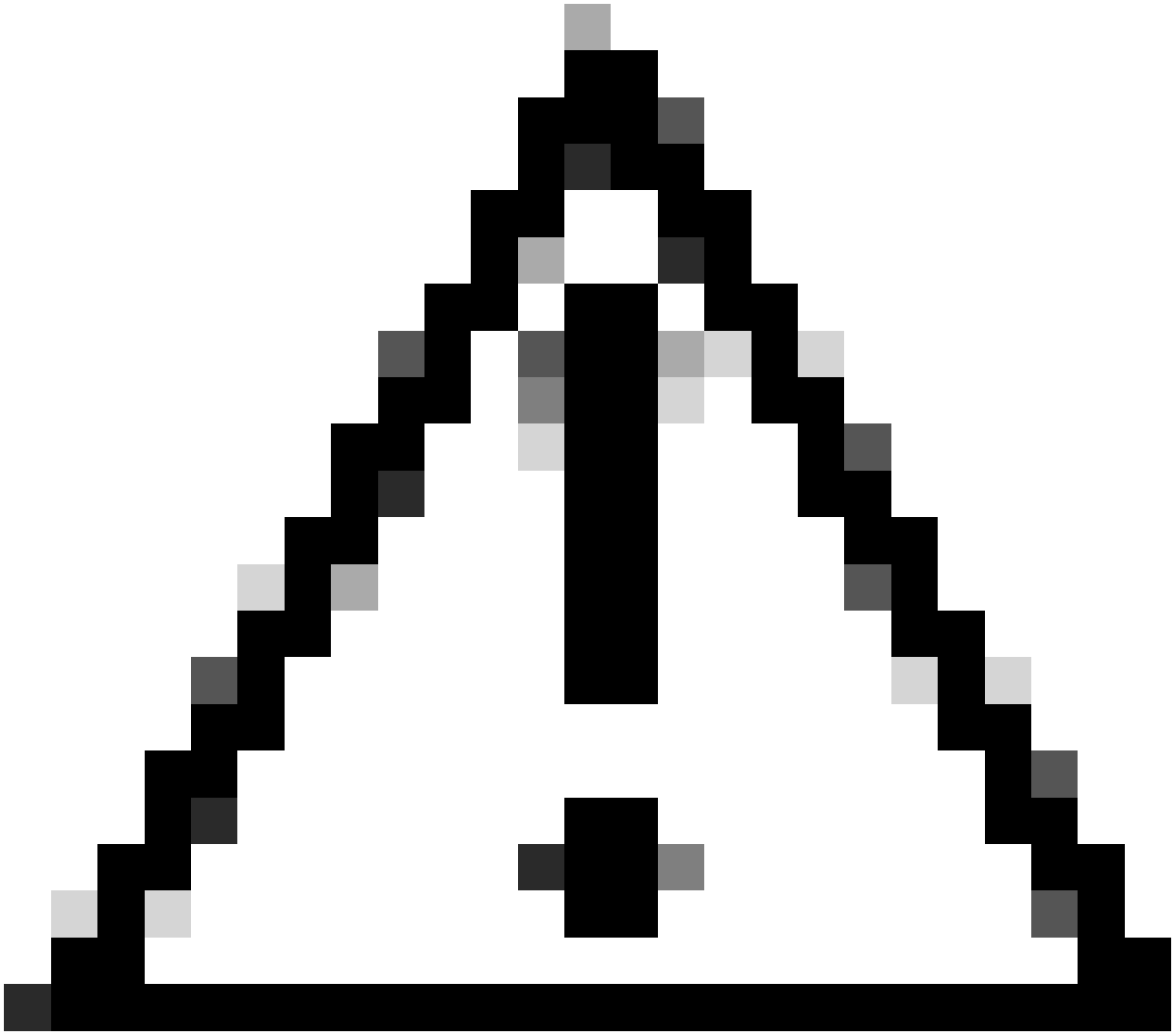
- Kontrollzentrum
- Cisco Room Kit Pro
- Cisco Room Bar Pro
- Linux Server zu Host snmpwalk Utility für das Testen der SNMP-Konfiguration.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Was ist SNMP

SNMP steht für Simple Network Management Protocol. Hierbei handelt es sich um ein Protokoll, mit dem Informationen über die Geräte in einem Netzwerk gesammelt und verwaltet, der Gerätestatus überwacht und Konfigurationsänderungen vorgenommen werden. Dabei kann es sich um Router, Switches, Server, Drucker oder andere Gerätetypen handeln. Voraussetzung ist, dass diesen Geräten eine IP-Adresse zugewiesen wurde. Es gibt drei Versionen von SNMP. Das Raumbetriebssystem unterstützt SNMPv2c und SNMPv3. SNMPv1 wird nicht unterstützt.

Der Schwerpunkt dieses Artikels liegt auf der Konfiguration und Fehlerbehebung von SNMP auf Collaboration-Endpunkten mit Raumbetriebssystem, die in der Cloud registriert sind (ohne WebEx Edge für Geräte).



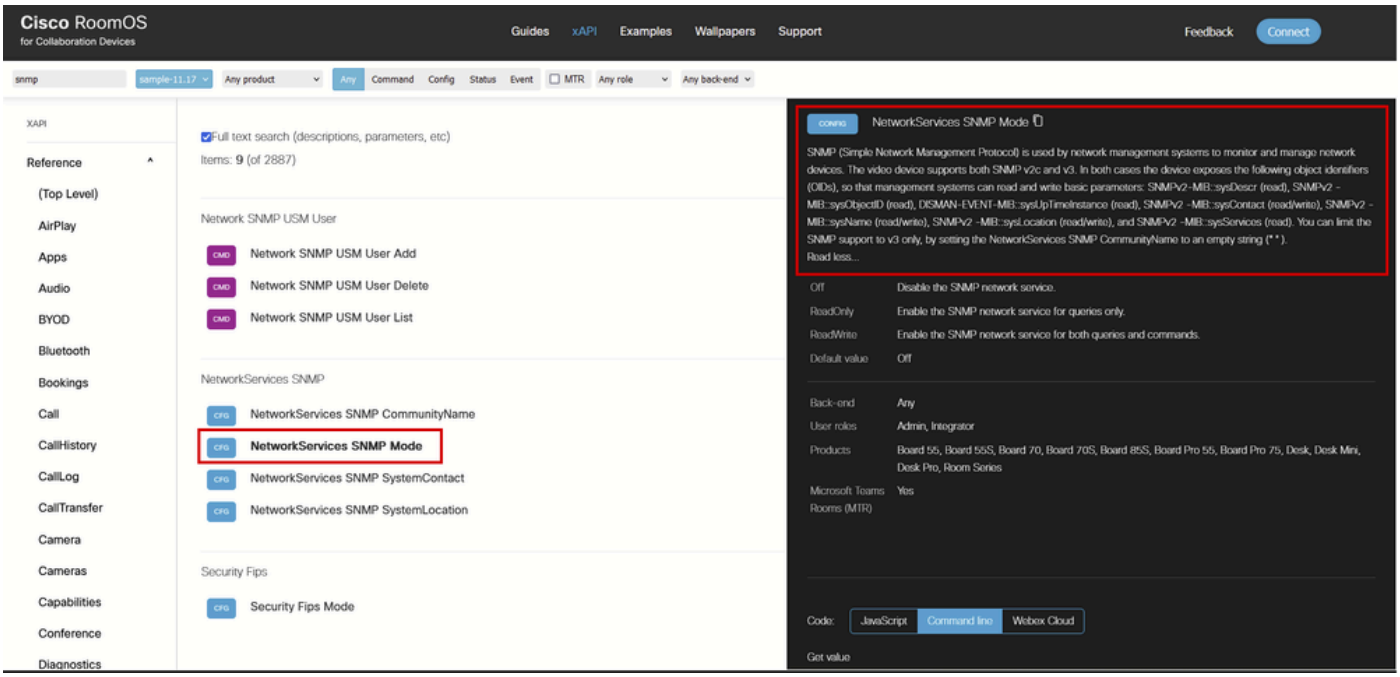
Vorsicht: In diesem Artikel wird die SNMP-Konfiguration nur aus der Perspektive der Endpunkte betrachtet. Die netzwerkseitige Konfiguration und die Tools zum Anfordern/Aktualisieren von SNMP-bezogenen Informationen über die Endgeräte sind nicht Gegenstand dieses Artikels.

Das TAC bietet keine Unterstützung für die Fehlerbehebung von SNMP im Netzwerk und kann auch keine Rückschlüsse darauf ziehen, warum SNMP aus Netzwerksicht nicht wie erwartet funktioniert. Ihr Netzwerkteam muss in die weitere Behebung dieser Probleme eingebunden werden.

Die Verwaltung von SNMP kann mit vielen verschiedenen Tools erfolgen. Diese Tools werden vom TAC nicht unterstützt. Wenn bei den Informationen, die diese Tools von den Endgeräten erfassen, eine Diskrepanz besteht, muss das Problem zunächst vom Netzwerkteam behoben und dann im TAC eskaliert werden, wenn ausreichende Informationen vorliegen, die belegen, dass es sich um ein endpunktbezogenes Problem handelt.

Welche Informationen können angefordert werden?

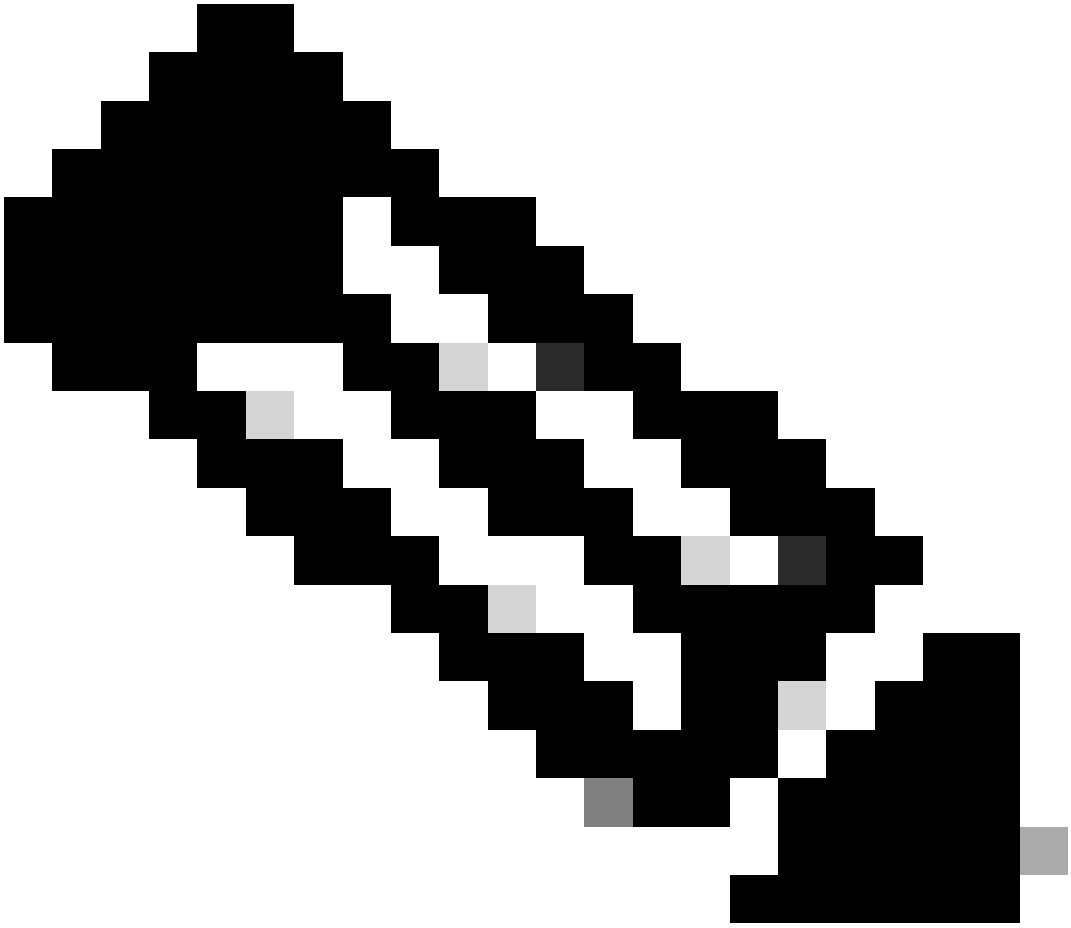
Mithilfe von SNMP können Sie eine begrenzte Informationsmenge vom Endpunkt anfordern. Die unterstützten OIDs und MiBs sind in diesem Link unter den Details des SNMP-Modus von NetworkService zu finden:



NetworkService - SNMP-Modus - Befehlsbeschreibung in Room OS xAPI-Dokumentation

Die Endpunkte stellen diese OIDs für SNMPv2 und SNMPv3 bereit:

- SNMPv2-MIB::sysDescr (gelesen),
- SNMPv2 -MIB::sysObjectID (gelesen),
- DISMAN-EVENT-MIB::sysUpTimeInstance (gelesen),
- SNMPv2 -MIB::sysContact (Lesen/Schreiben),
- SNMPv2 -MIB::sysName (Lesen/Schreiben),
- SNMPv2 -MIB::sysLocation (Lesen/Schreiben),
- SNMPv2 -MIB::sysServices (gelesen).

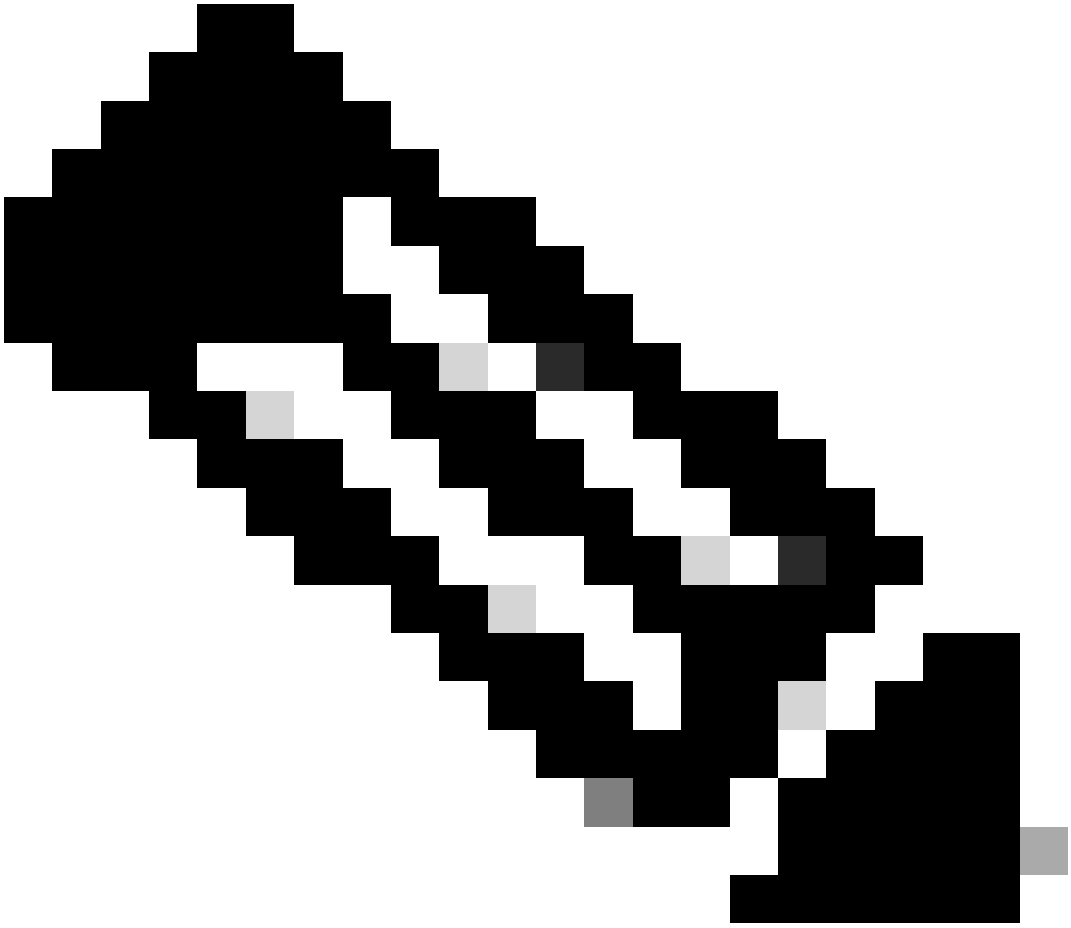


Anmerkung: Der SNMP CommunityName der Netzwerkdienste kann auf eine leere Zeichenfolge festgelegt werden, wenn nur SNMPv3 verwendet werden soll.

Konfigurieren von SNMP auf einem Cloud-registrierten Endgerät

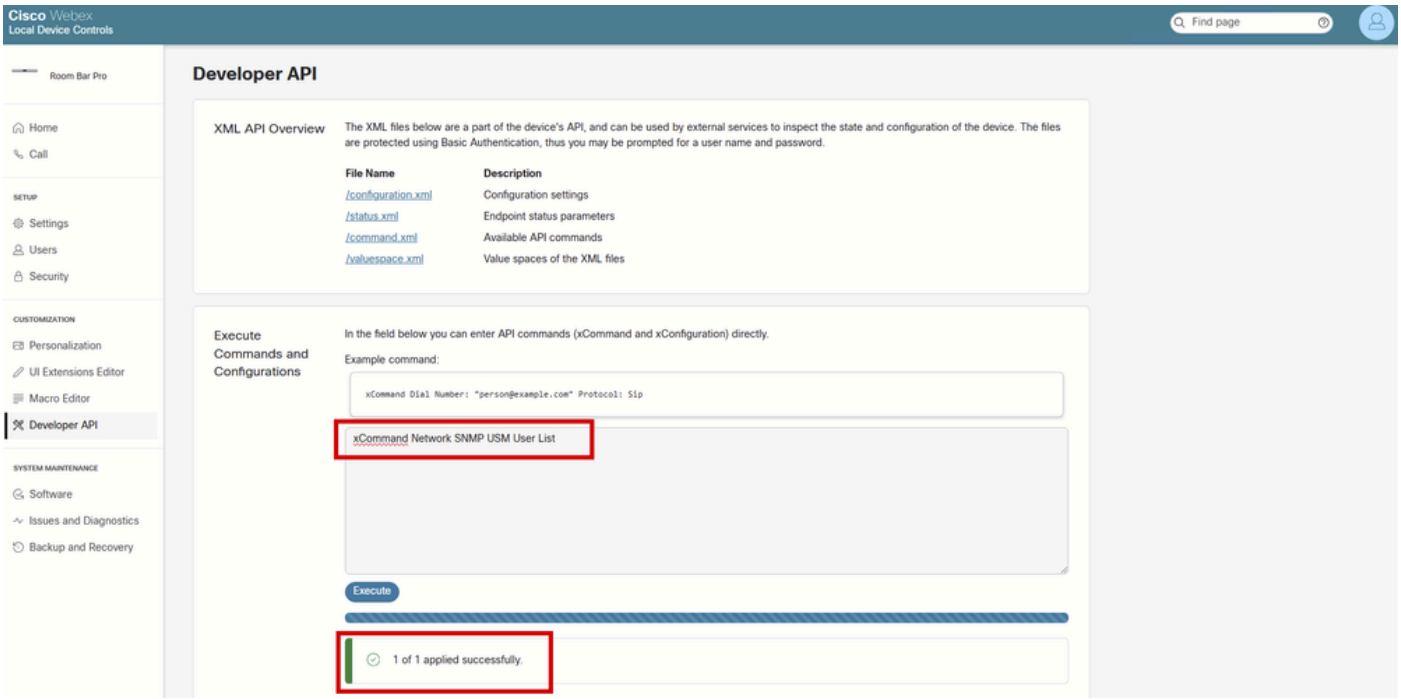
Im Allgemeinen können Konfigurationsänderungen an Endgeräten auf vier verschiedene Arten erfolgen:

1. Verfügbare WebEx APIs
2. Die Endpunkt-GUI
3. Steuerungs-Hub
4. SSH direkt zum Endgerät

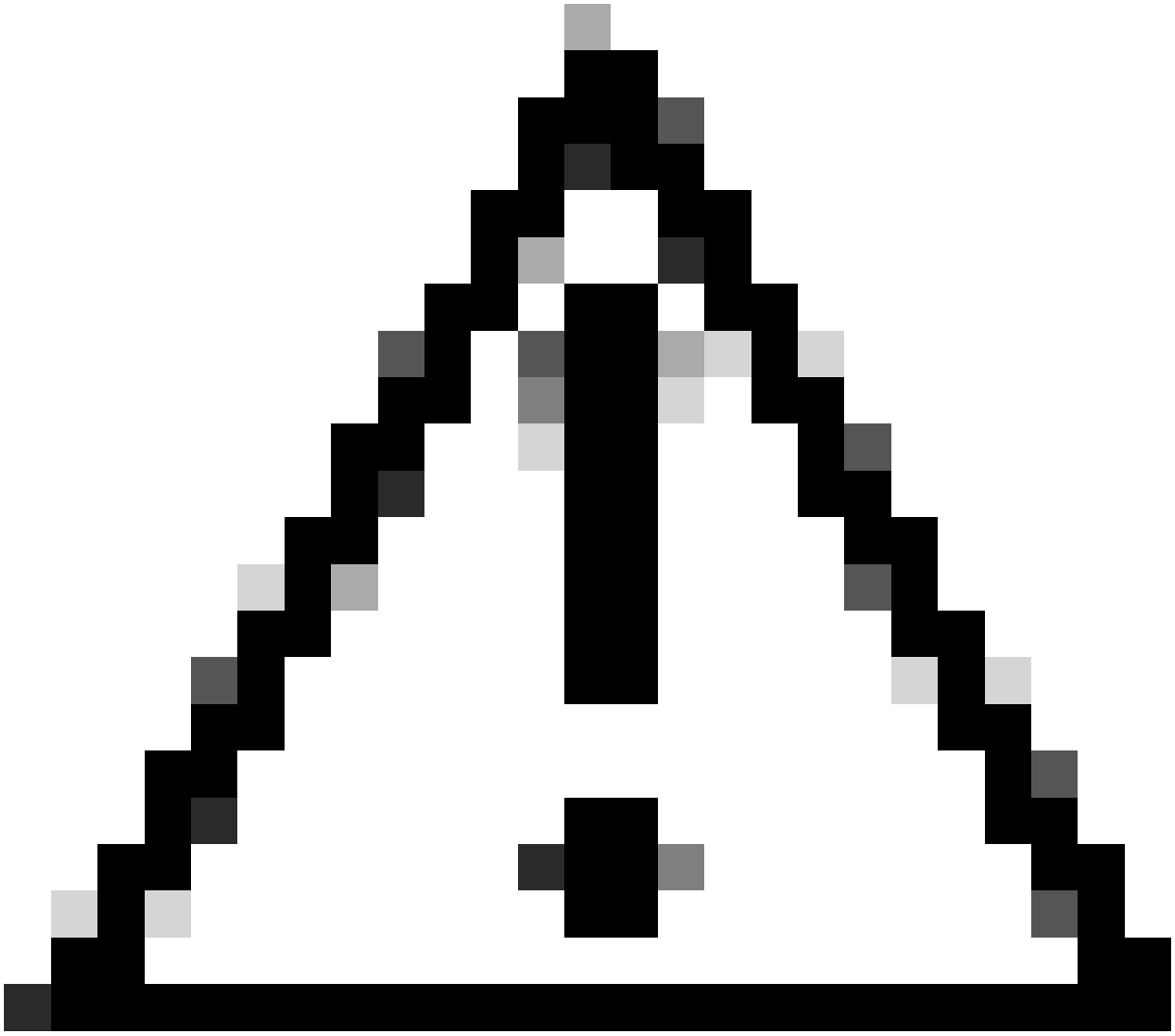


Anmerkung: Öffnen Sie einen Browser, und geben Sie in der URL-Leiste die IP-Adresse des Endpunkts ein, um auf die grafische Benutzeroberfläche eines Endpunkts zuzugreifen. Sie müssen sich im selben Netzwerk wie der Endpunkt befinden und über Benutzeranmeldeinformationen verfügen, um sich anmelden zu können.

Es können nicht alle Konfigurationen auf alle vier Arten vorgenommen werden. Für das Szenario in diesem Dokument kann der SNMP-Modus auf alle vier Arten aktiviert werden. Um jedoch einen SNMP-Benutzer zu erstellen, der über SNMP mit dem Gerät kommunizieren kann, müssen Sie SSH zum Endpunkt herstellen, die WebEx APIs verwenden oder die Benutzeroberfläche des Endpunkts bei der Entwickler-API im Abschnitt Anpassung verwenden. USM-Benutzer können nicht im Abschnitt Alle Konfigurationen des Control Hub des Endpunkts erstellt werden.



Abschnitt zur Entwickler-API auf der Endpunkt-GUI

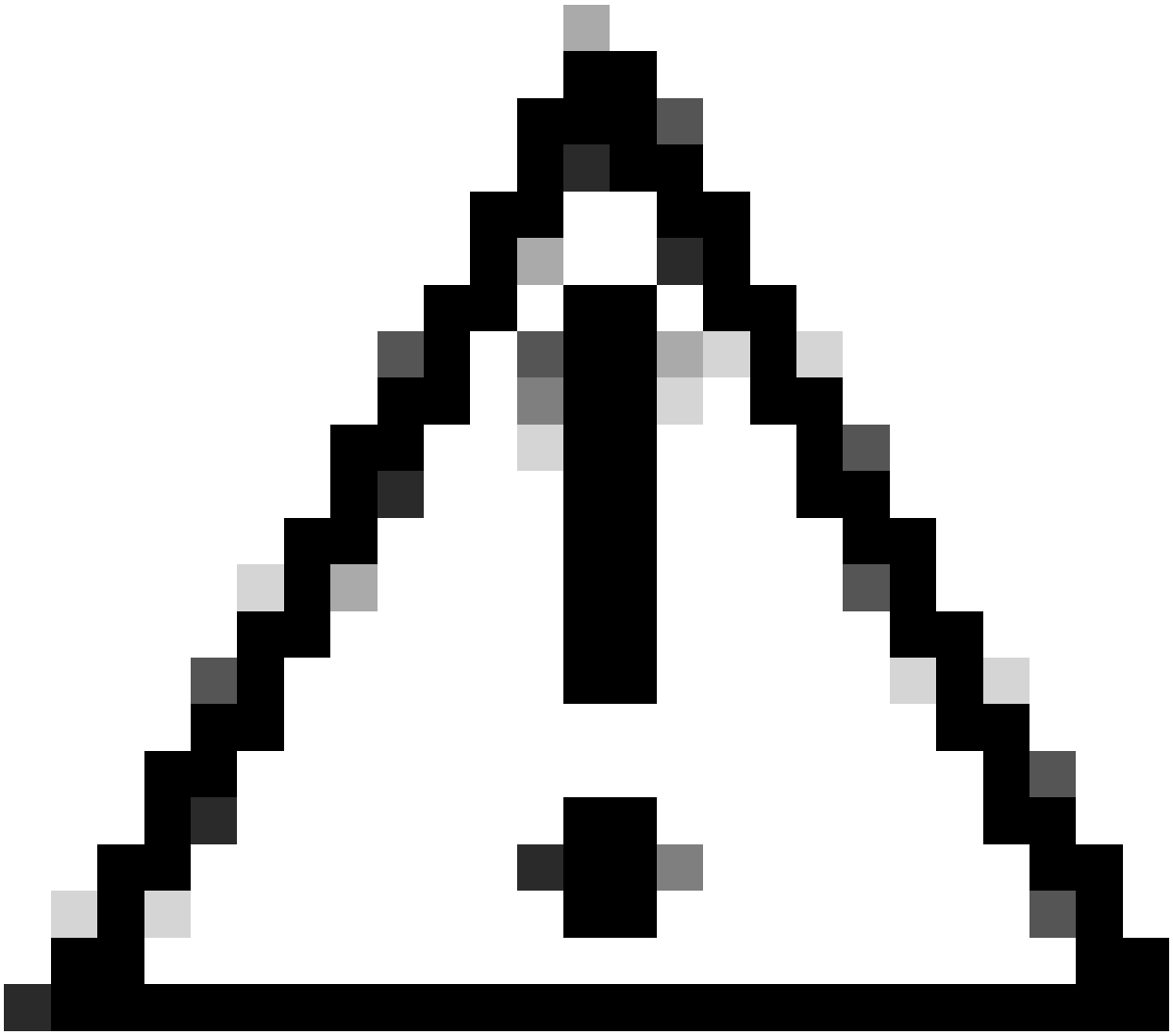


Vorsicht: Die Befehle im Textfeld "Befehle und Konfigurationen ausführen" liefern keine Ergebnisse. Sie sehen nur, ob der Befehl erfolgreich ausgeführt wurde oder nicht. Aus diesem Grund gibt der Befehl, der die USM-Benutzer auflistet, keine Ergebnisse im vorherigen Screenshot zurück. Dies bedeutet, dass Sie einen USM-Benutzer von diesem Abschnitt der GUI des Endpunkts aus erfolgreich erstellen können. Um jedoch zu überprüfen, ob der Benutzer erstellt wurde, müssen Sie SSH für das Gerät einrichten.

Für die Konfiguration von SNMPv2c ist die Erstellung eines Benutzers nicht erforderlich. Die Authentifizierung erfolgt unter Verwendung des Community-Namens (auch Community String genannt), der auf dem Endpunkt konfiguriert wird. Der SNMP-Agent des Endpunkts, der bereits auf dem Gerät vorhanden ist, antwortet auf Anfragen, die mit dem konfigurierten Community-Namen auf dem Gerät übereinstimmen. Wenn eine SNMP-Anfrage von einem Verwaltungssystem keinen passenden Communitynamen enthält (Groß- und Kleinschreibung beachten), wird die Nachricht verworfen, und der SNMP-Agent im Videogerät sendet keine Antwort.

SNMPv3 erfordert jedoch die Konfiguration eines USM-Benutzers, damit die Authentifizierung erfolgreich ist. Zu diesem Zweck sind Netzwerk-SNMP-USM-Benutzerbefehle erforderlich. Dies

kann über SSH direkt auf das Gerät erfolgen oder über die Geräte-GUI im Abschnitt zur Entwickler-API. Alternativ kann die WebEx API verwendet werden.



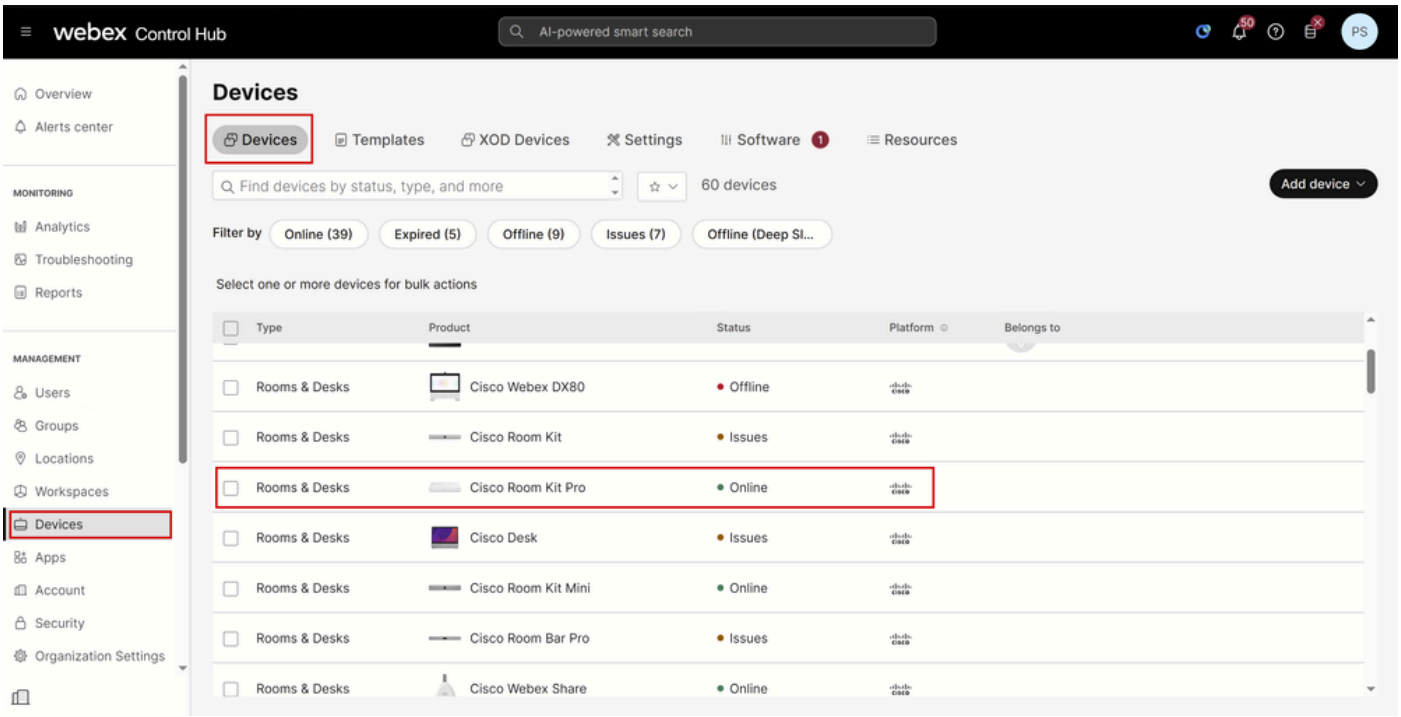
Vorsicht: Sie müssen entscheiden, ob Sie SNMPv2, SNMPv3 oder beides aktivieren möchten. SNMPv1 wird auf Cisco Endgeräten nicht unterstützt. Jeder Versuch, SNMPv1 zu verwenden, wird fehlschlagen.

In diesem Dokument werden die SNMPv2- und SNMPv3-Protokolle im Control Hub aktiviert und konfiguriert. Der für die SNMP3-Authentifizierung erforderliche USM-Benutzer wird jedoch über SSH konfiguriert.

SNMPv2c-Modus im Control Hub aktivieren

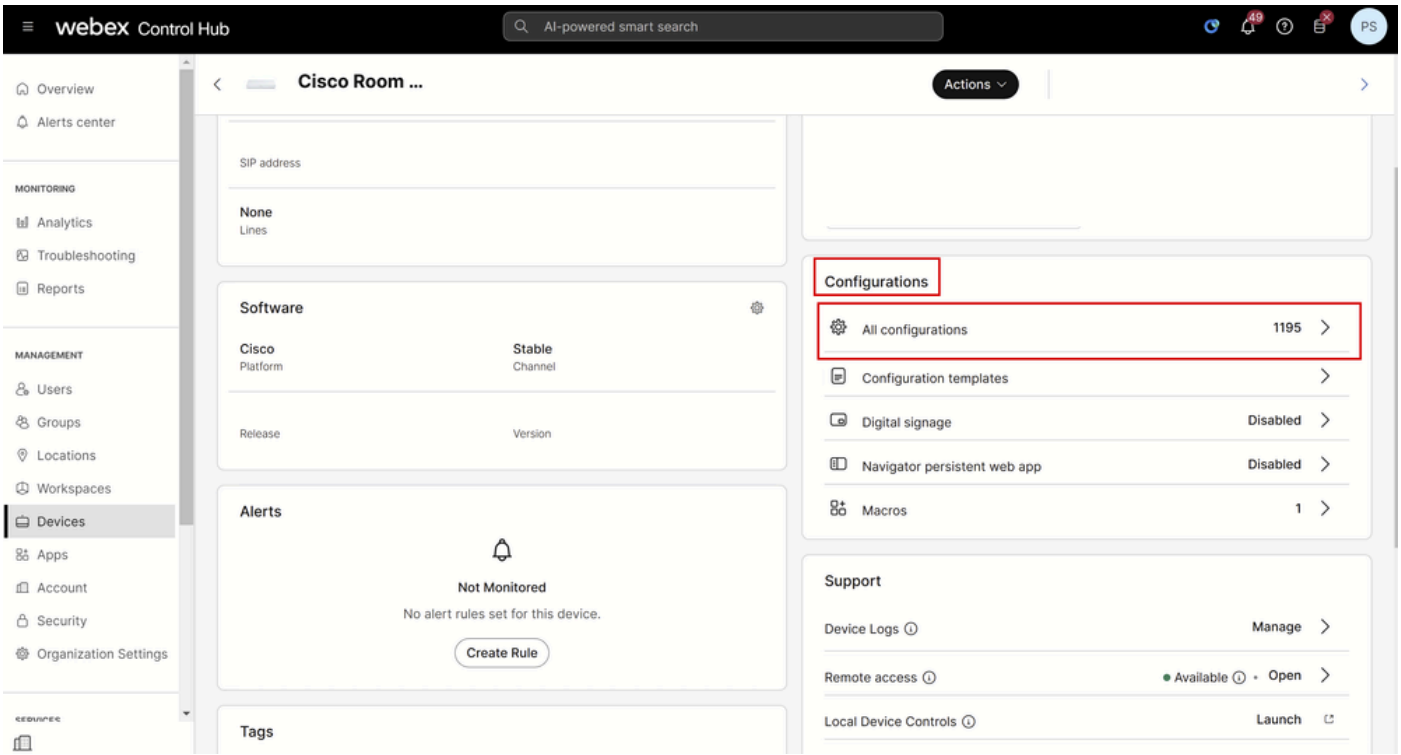
Navigieren Sie zu admin.webex.com, und melden Sie sich mit Ihren Admin-Anmeldeinformationen an. Es wird empfohlen, ein Volladministrator zu sein. Navigieren Sie im Abschnitt Verwaltung auf der linken Seite der Benutzeroberfläche zu Geräte. Wählen Sie auf der Registerkarte Geräte das Gerät aus, das Sie konfigurieren möchten. In diesem Beispiel wird ein Cisco Room Kit Pro

verwendet.



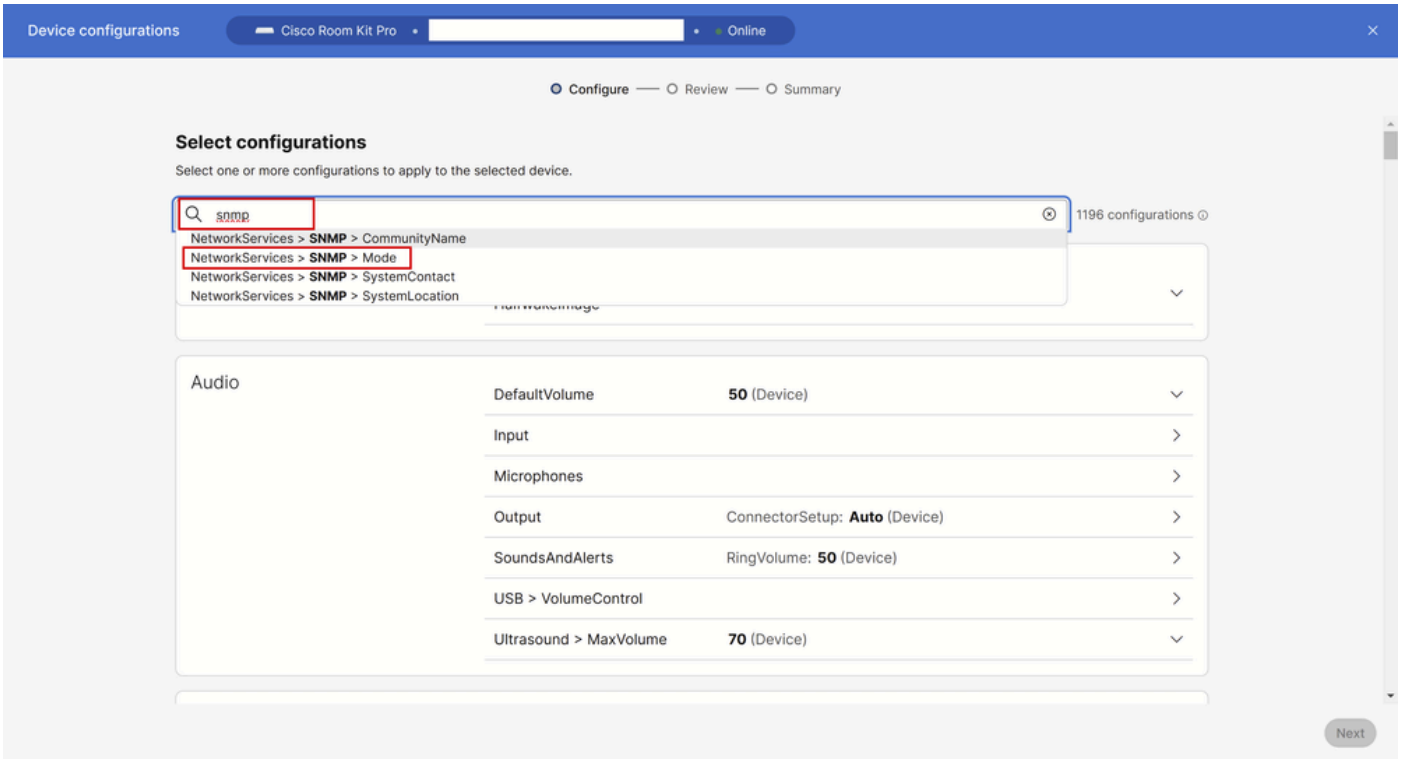
Abschnitt "Control Hub Devices"

Navigieren Sie unter den Gerätedetails auf der neuen Seite "Control Hub", die geöffnet wird, zum Abschnitt Konfigurationen, und klicken Sie auf Alle Konfigurationen:



Control Hub-Gerätedetails für Room Kit Pro

Geben Sie in der Suchleiste snmp ein, und wählen Sie Network Services > SNMP > Mode:

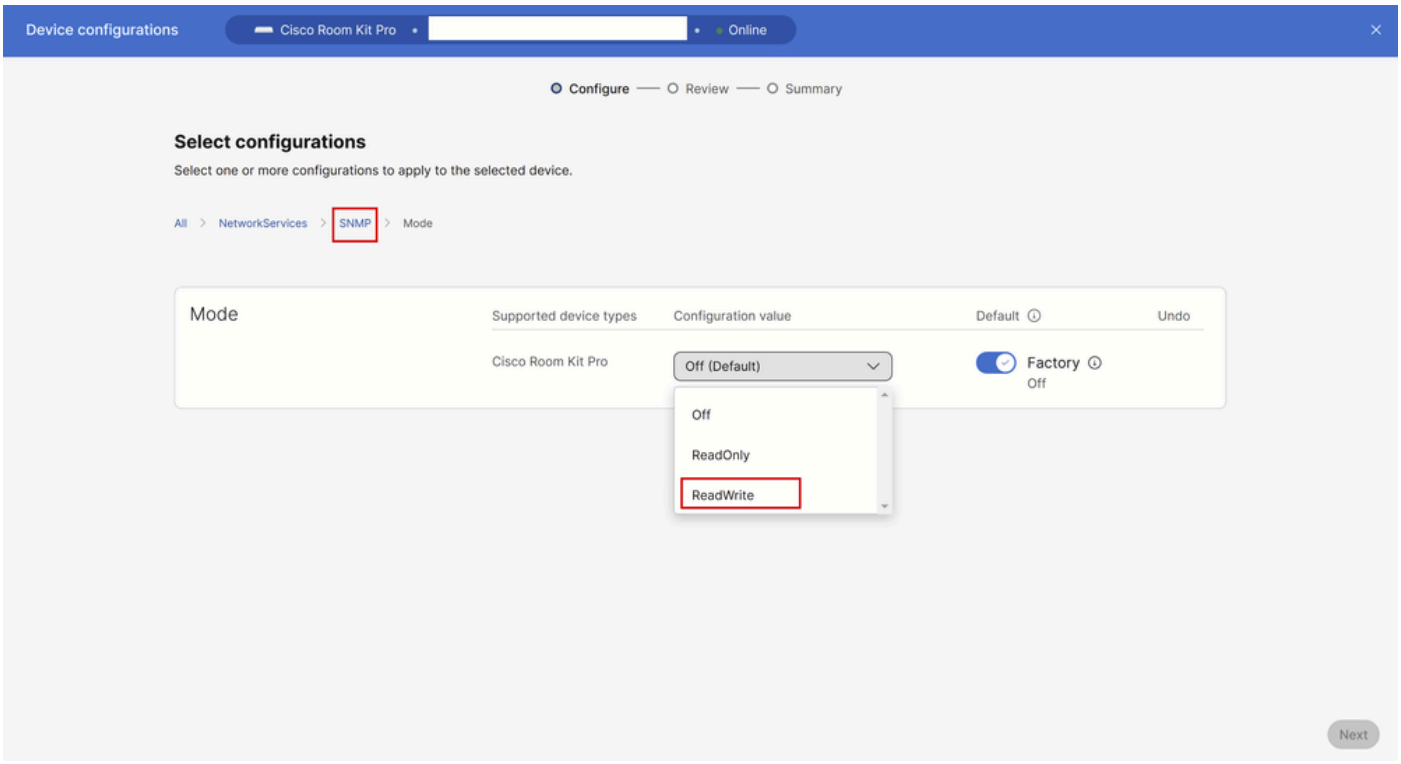


Control Hub - Fenster "Alle Konfigurationen"

Wählen Sie den Modus aus, den Sie in Ihrer Umgebung aktivieren möchten. Es stehen drei Optionen zur Verfügung:

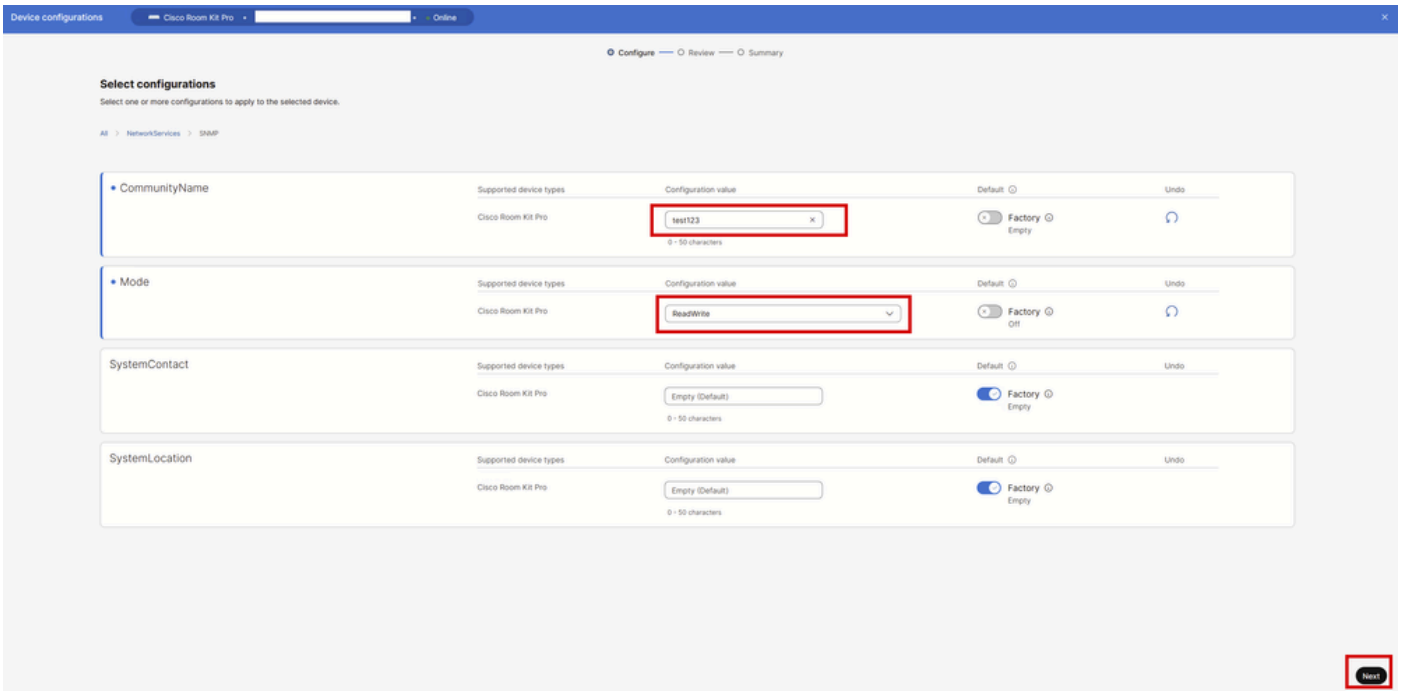
1. Off (Deaktiviert): Deaktivieren Sie den SNMP-Netzwerkdienst.
2. Schreibgeschützt: Aktivieren Sie den SNMP-Netzwerkdienst nur für Abfragen.
3. LesenSchreiben: Aktivieren Sie den SNMP-Netzwerkdienst für Abfragen und Befehle.

In diesem Beispiel ist ReadWrite ausgewählt. Klicken Sie anschließend im Navigationsbereich für die Einstellungen auf SNMP (siehe Abbildung). Dadurch gelangen Sie in den Einstellungen wieder zu einem Schritt zurück, und Sie können alle SNMP-bezogenen Einstellungen anzeigen, die auf dem Gerät über den Control Hub konfiguriert werden können:



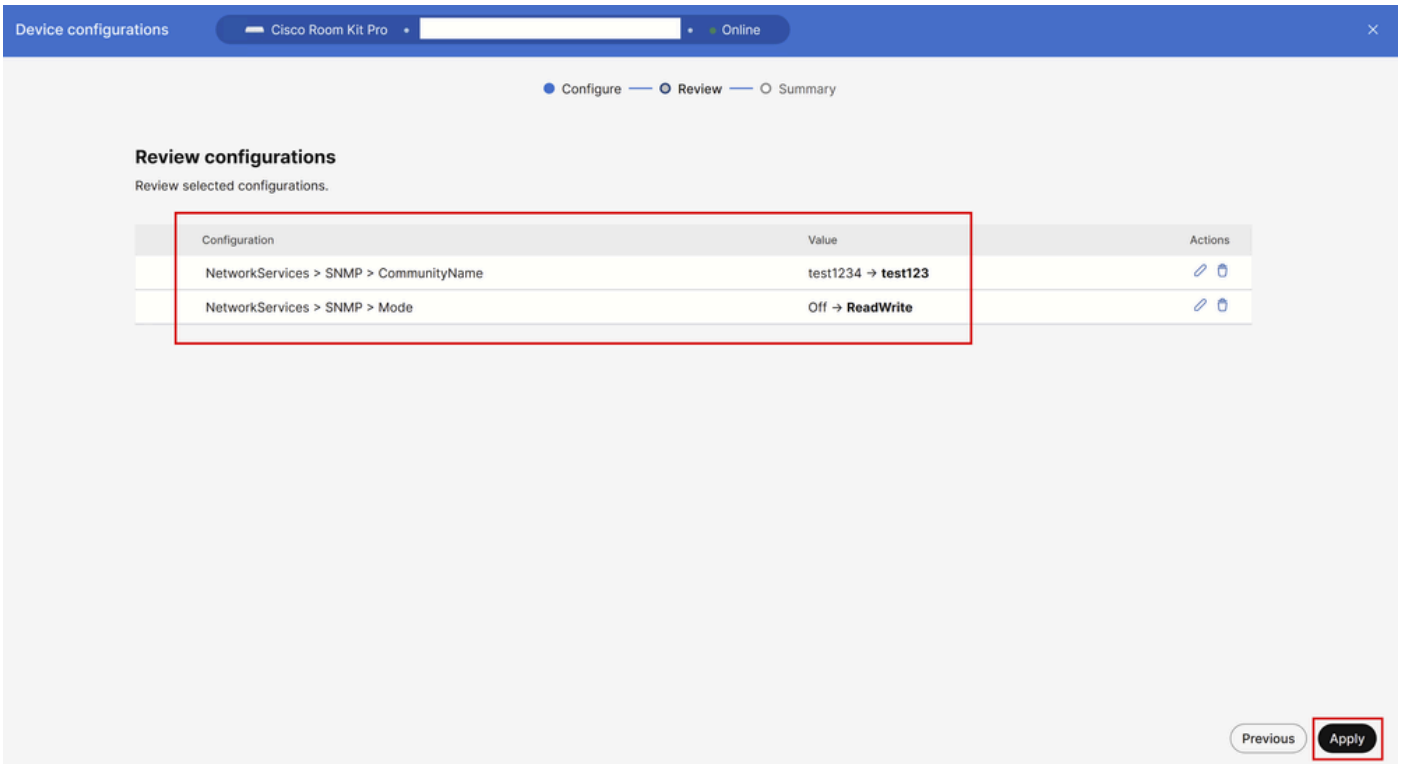
SNMP-Moduseinstellung unter "Alle Konfigurationen" im Control Hub

Wenn Sie auf SNMP klicken, werden alle verfügbaren SNMP-Optionen angezeigt, wie in dieser Abbildung dargestellt. Damit SNMPv2 erfolgreich eingerichtet werden kann, muss ein Community-Name eingerichtet werden. Der Community-Name wird für die Authentifizierung zwischen dem SNMP-Server und dem auf dem Endpunkt vorhandenen SNMP-Agenten verwendet. Der Community-Name ist für dieses Beispiel auf test123 festgelegt. Klicken Sie unten rechts auf Weiter.



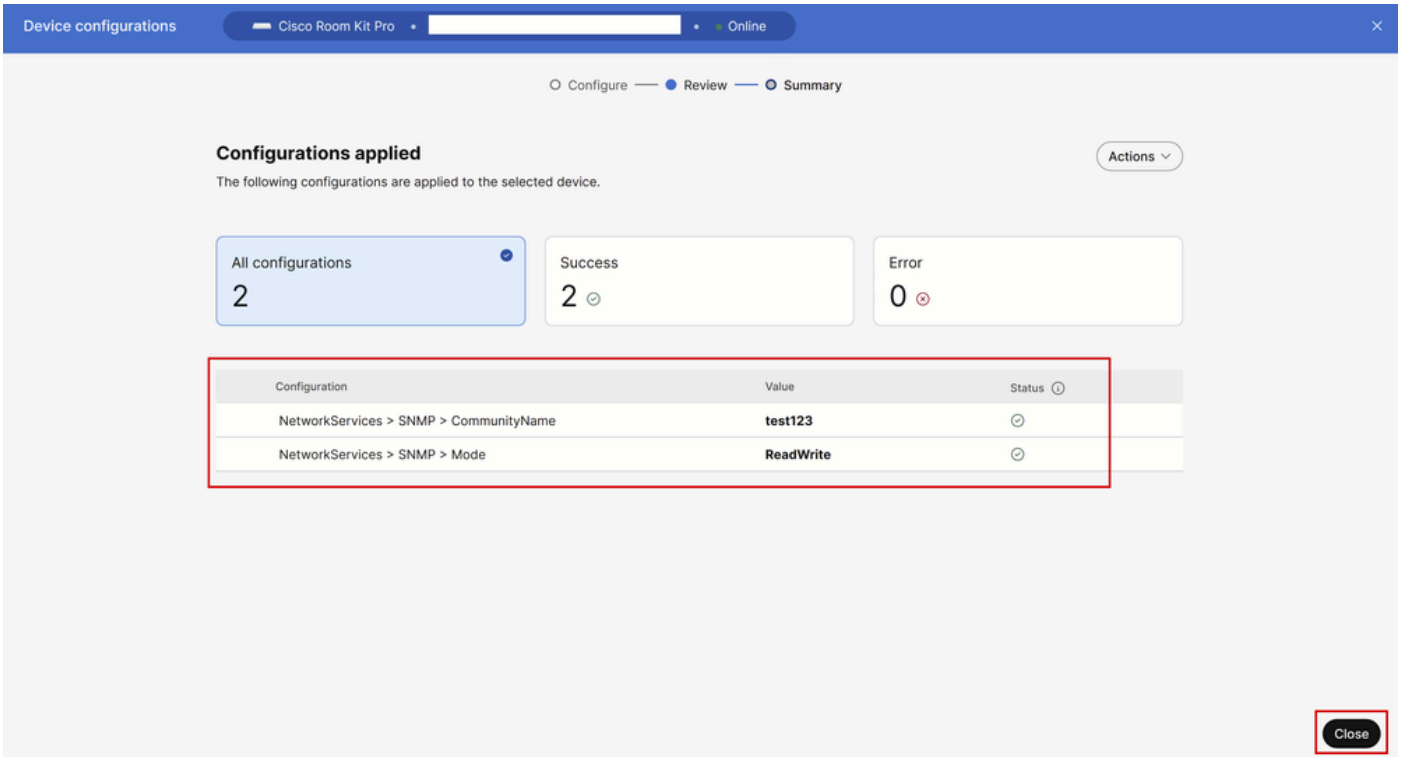
SNMP-Einstellungen unter "Alle Konfigurationen" im Control Hub

Überprüfen Sie die Gerätekonfigurationen, und klicken Sie unten rechts auf Apply (Anwenden):



Überprüfen Sie die Konfigurationen, bevor Sie die Änderungen übernehmen

Überprüfen Sie, ob die Konfigurationsänderungen erfolgreich angewendet wurden. Klicken Sie dann auf Schließen.



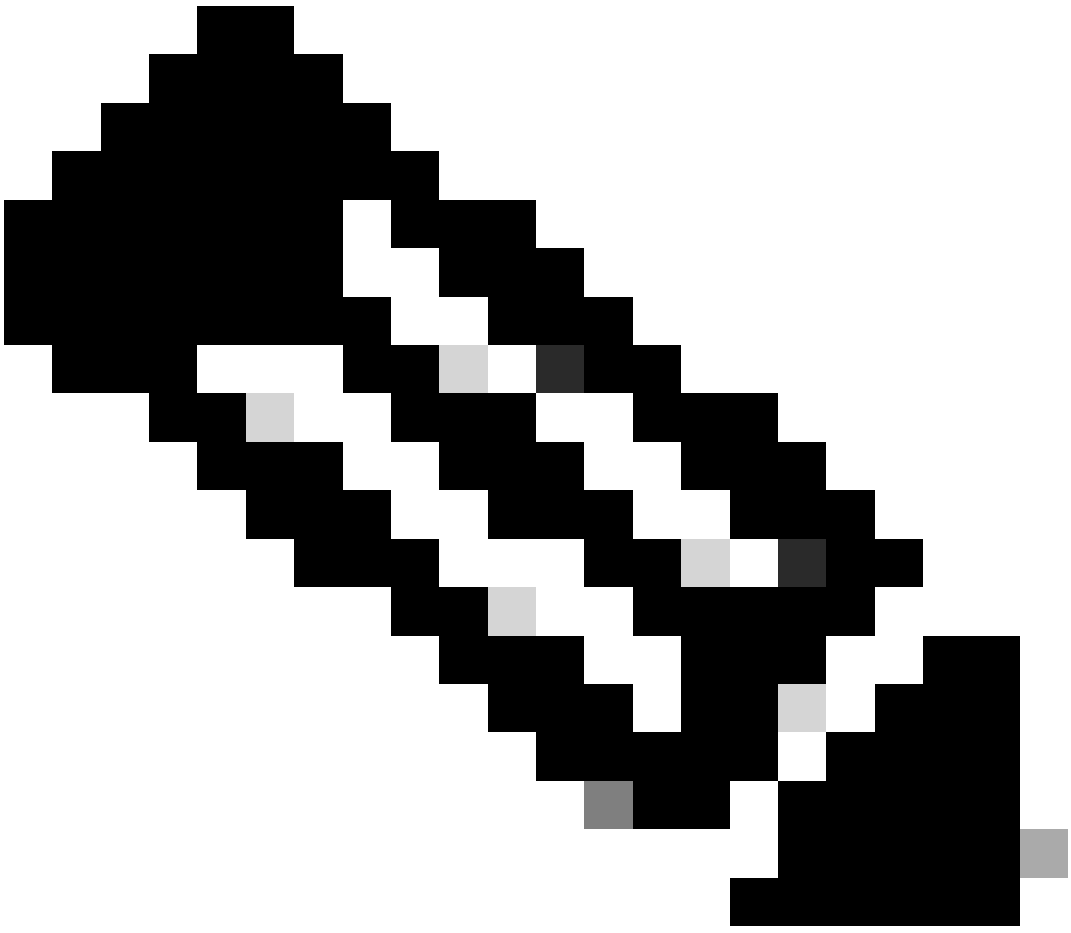
Endpunktkonfigurationen im Control Hub erfolgreich angewendet

Zu diesem Zeitpunkt ist SNMPv2c auf dem Endpunkt erfolgreich aktiviert und der Community-Name wurde eingerichtet.

SNMPv3-Modus im Control Hub aktivieren

SNMPv3 bietet mehr Sicherheit und erfordert auf dem Endpunkt eine andere Konfiguration als SNMPv2c. Navigieren Sie im Abschnitt Management unter Control Hub zu Devices. Bleiben Sie auf der Registerkarte Geräte, und wählen Sie einen Ihrer Endpunkte aus, den Sie mit SNMPv3 konfigurieren möchten. Für dieses Beispiel wird ein Cisco Room Bar Pro verwendet.

Navigieren Sie unter den Gerätedetails zum Abschnitt Konfigurationen, und klicken Sie auf Alle Konfigurationen. Die Seite Gerätekonfigurationen wird geöffnet. Geben Sie snmp in die Suchleiste ein, und wählen Sie NetworkServices > SNMP > Mode aus. In diesem Beispiel ist der SNMP-Modus auf ReadWrite festgelegt. Klicken Sie auf SNMP, um alle konfigurierbaren SNMP-Einstellungen auf dem Gerät anzuzeigen.

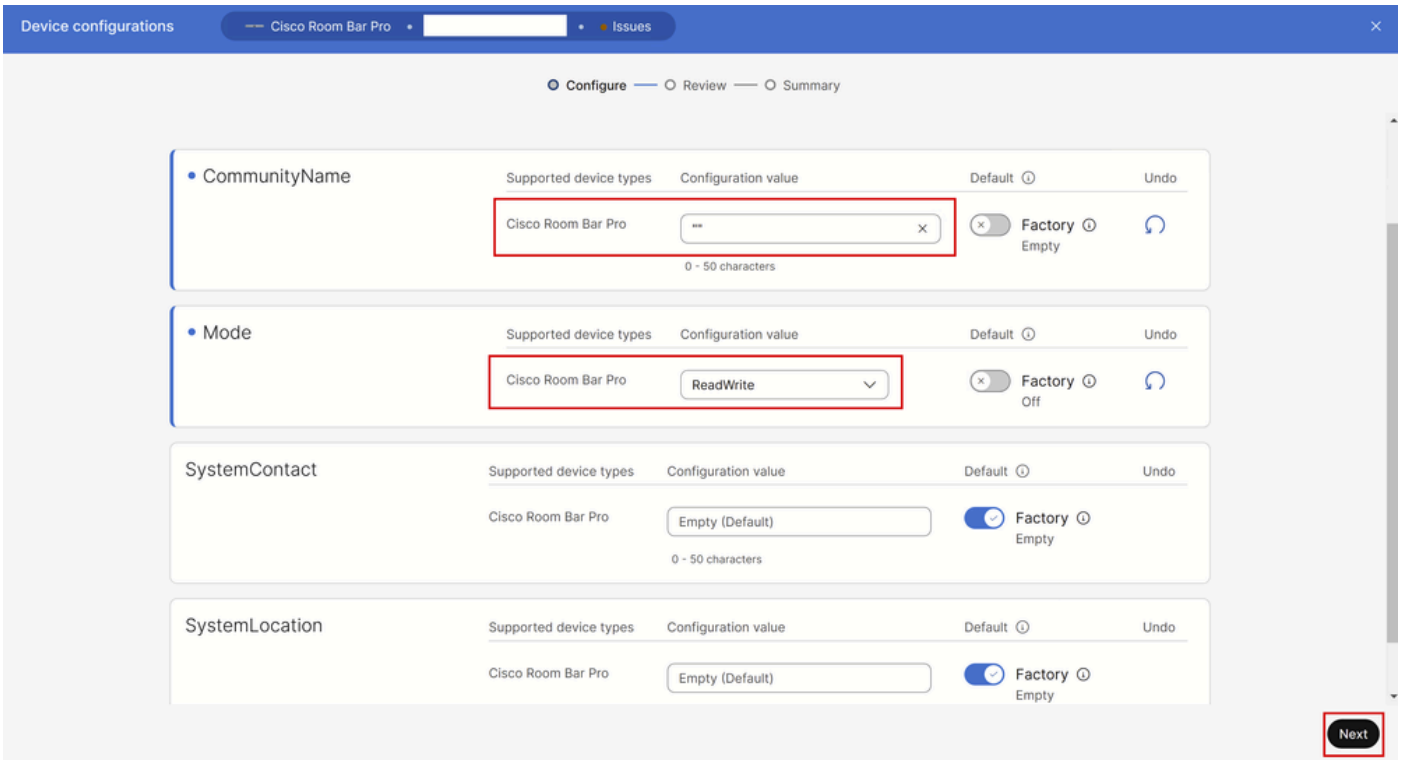


Anmerkung: Alle bisher für SNMPv3 genannten Schritte wurden bereits beschrieben, als SNMPv2c in einem vorherigen Beispiel konfiguriert wurde. Daher wird kein Screenshot der Schritte bereitgestellt. Im Abschnitt SNMPv2c-Modus aktivieren im Control Hub finden Sie weitere Informationen dazu, wie Sie durch die Control Hub-Einstellungen navigieren

---

können.

Um nur SNMPv3 zu unterstützen, müssen Sie den Community-Namen als leere Zeichenfolge in Anführungszeichen einschließen: "".



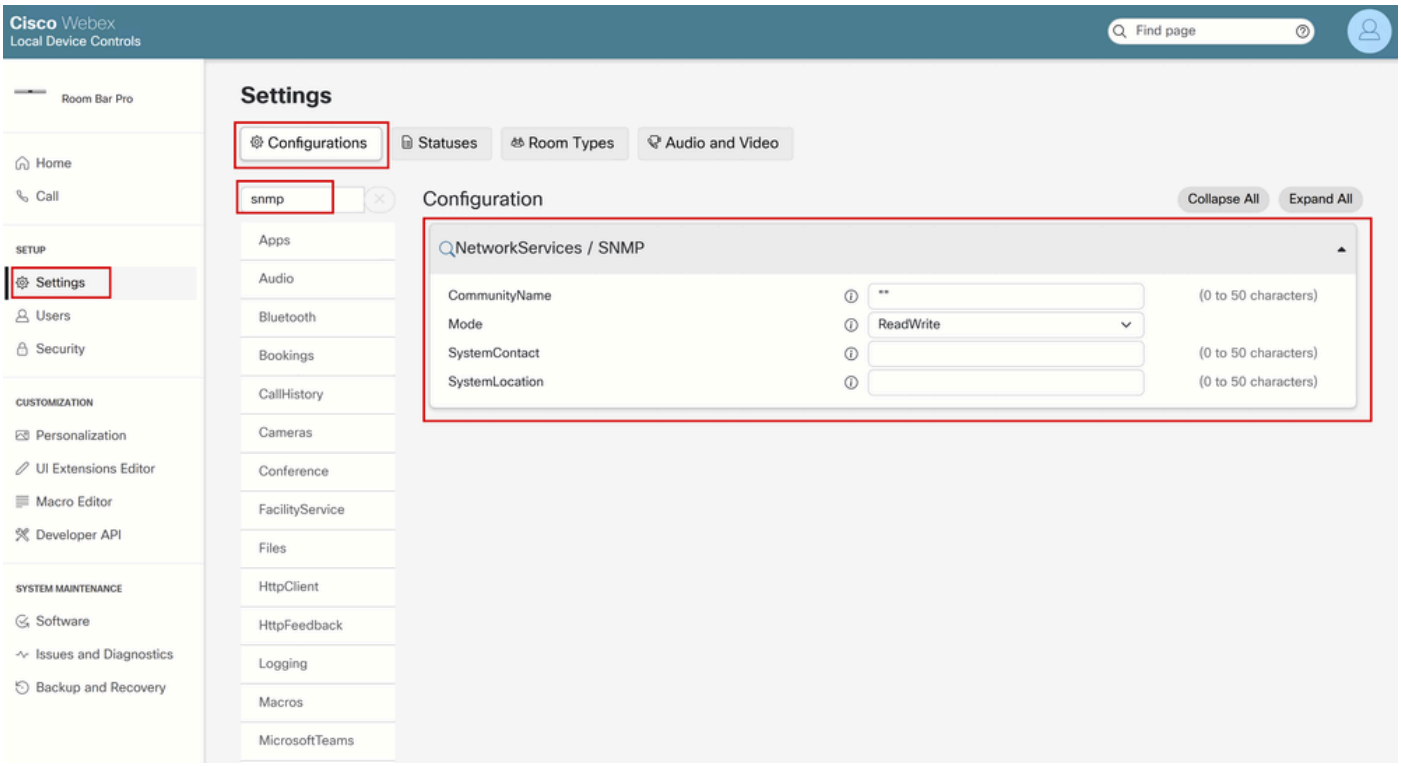
SNMP-Einstellungen unter "Alle Konfigurationen" im Control Hub

Klicken Sie auf Weiter, überprüfen Sie die Konfigurationsänderungen, und klicken Sie auf Anwenden. Klicken Sie auf Schließen, um die Gerätekonfigurationsseite zu schließen.

Damit ist die Konfiguration abgeschlossen, die im Control Hub durchgeführt werden kann. Zu diesem Zeitpunkt ist nur SNMPv3 aktiviert.

Wie sieht die SNMP-Konfiguration in der Endpunkt-GUI aus?

Die gleichen Konfigurationen können über die Geräte-GUI durchgeführt werden. Öffnen Sie eine Browser-Registerkarte, und geben Sie die IP-Adresse des Endpunkts ein (Sie müssen sich im selben Netzwerk wie das Endgerät befinden). Melden Sie sich als Admin-Benutzer an, und navigieren Sie in der Endpunkt-GUI zu Einstellungen im Abschnitt SETUP. Bleiben Sie auf der Registerkarte Konfigurationen, und geben Sie in der Suchleiste Einstellungen snmp ein. Dieses Bild zeigt, wie die SNMP-Einstellungen für die auf Room Bar Pro im vorherigen Abschnitt vorgenommene SNMPv3-Konfiguration angezeigt werden:



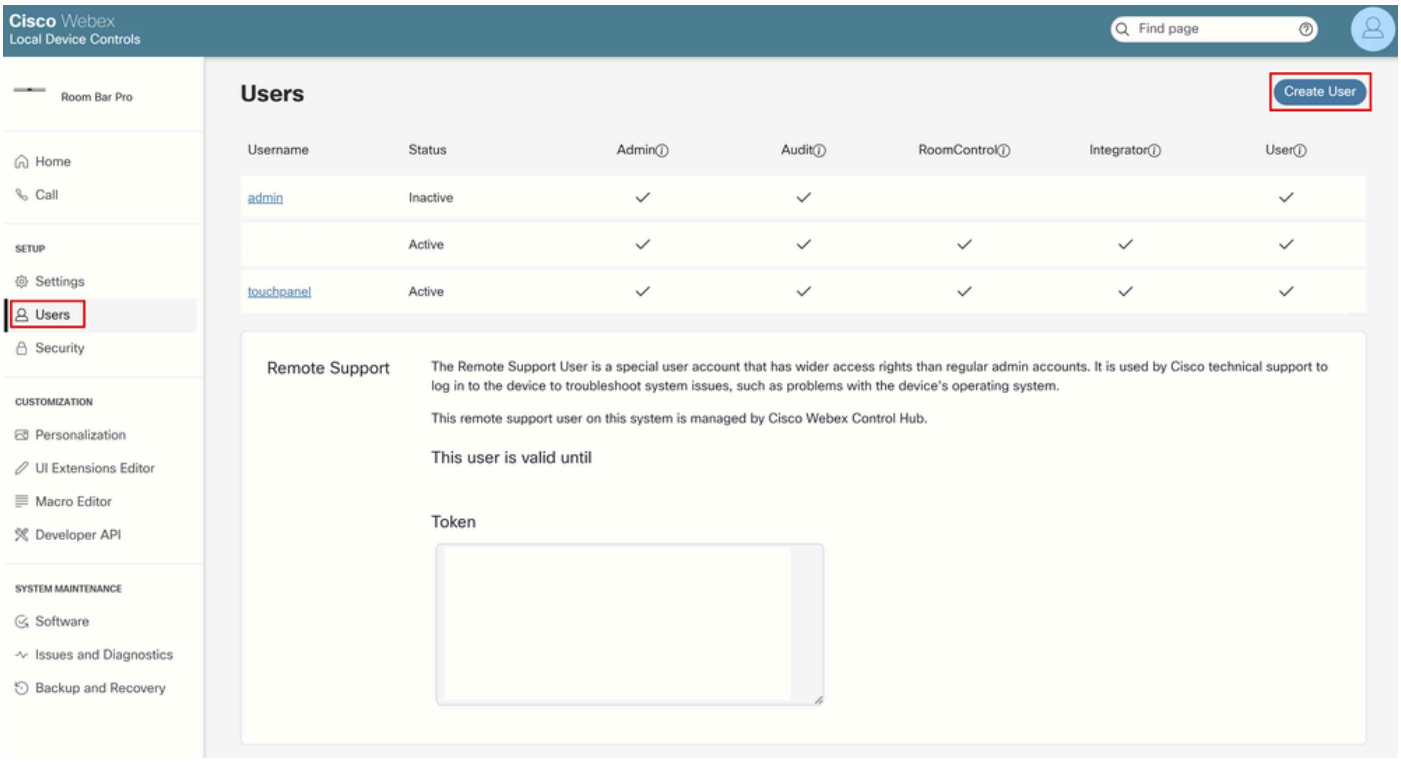
SNMPv3-Konfiguration auf der Benutzeroberfläche des Endgeräts

Konfigurieren des USM-Benutzers für SNMPv3

Um SNMPv3 verwenden zu können, müssen Sie einen USM-Benutzer erstellen. Die verfügbaren Befehle für diese Aktion finden Sie hier im Dokumentationslink für das Raumbetriebssystem. Verwenden Sie SSH, um eine Verbindung zum Gerät herzustellen. Dazu benötigen Sie ein Administratorkonto auf dem Gerät. Andernfalls müssen Sie ein Administratorkonto erstellen. Dieser Abschnitt behandelt den gesamten Prozess.

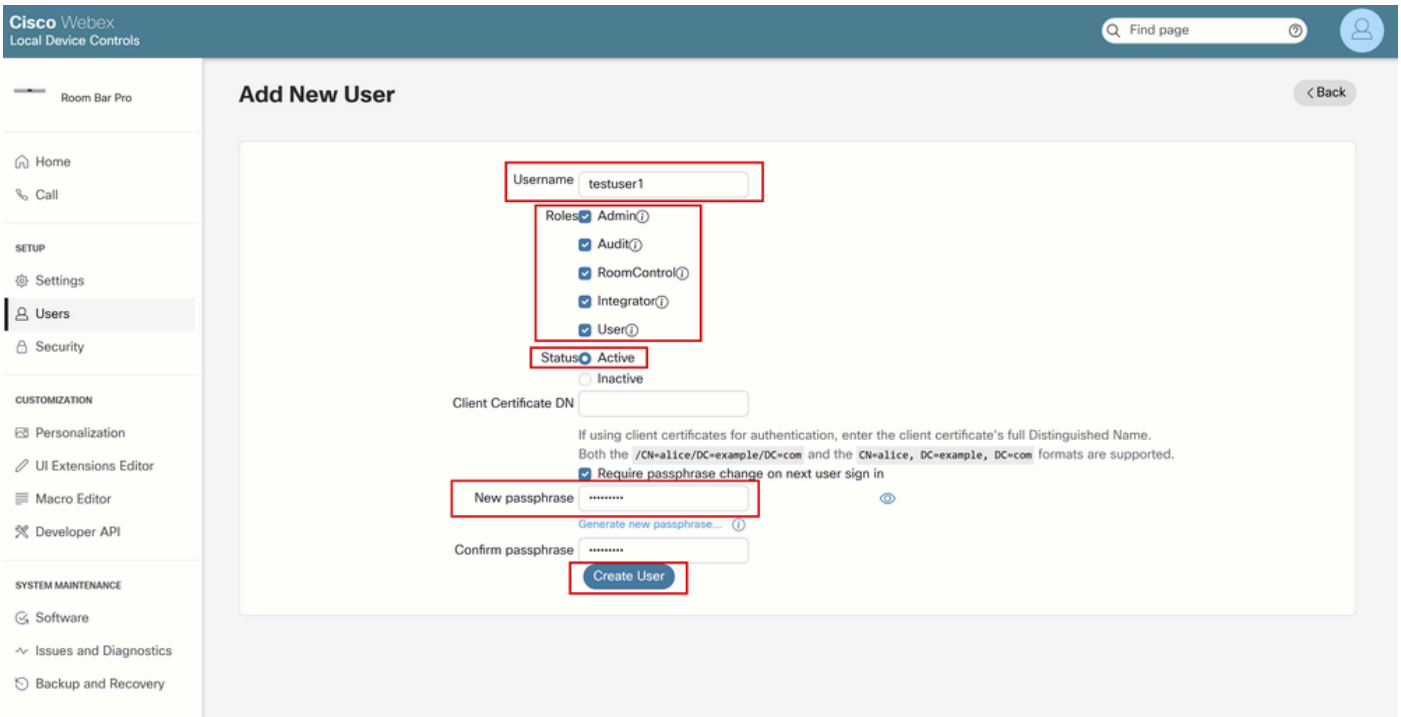
Navigieren Sie im Abschnitt Management unter Control Hub zu Devices. Wählen Sie auf der Registerkarte Geräte einen Endpunkt aus, für den Sie einen Administrator-Benutzer erstellen möchten. In diesem Beispiel wird eine Cisco Room Bar Pro verwendet.

Navigieren Sie unter den Gerätedetails zum Abschnitt Support, und klicken Sie auf Local Device Controls (Lokale Gerätesteuerung) (Sie müssen sich im gleichen Netzwerk wie der Endpunkt befinden, damit dies funktioniert). Die Geräte-GUI wird geöffnet. Navigieren Sie zu Benutzern unter dem Abschnitt SETUP, und klicken Sie auf Benutzer erstellen.



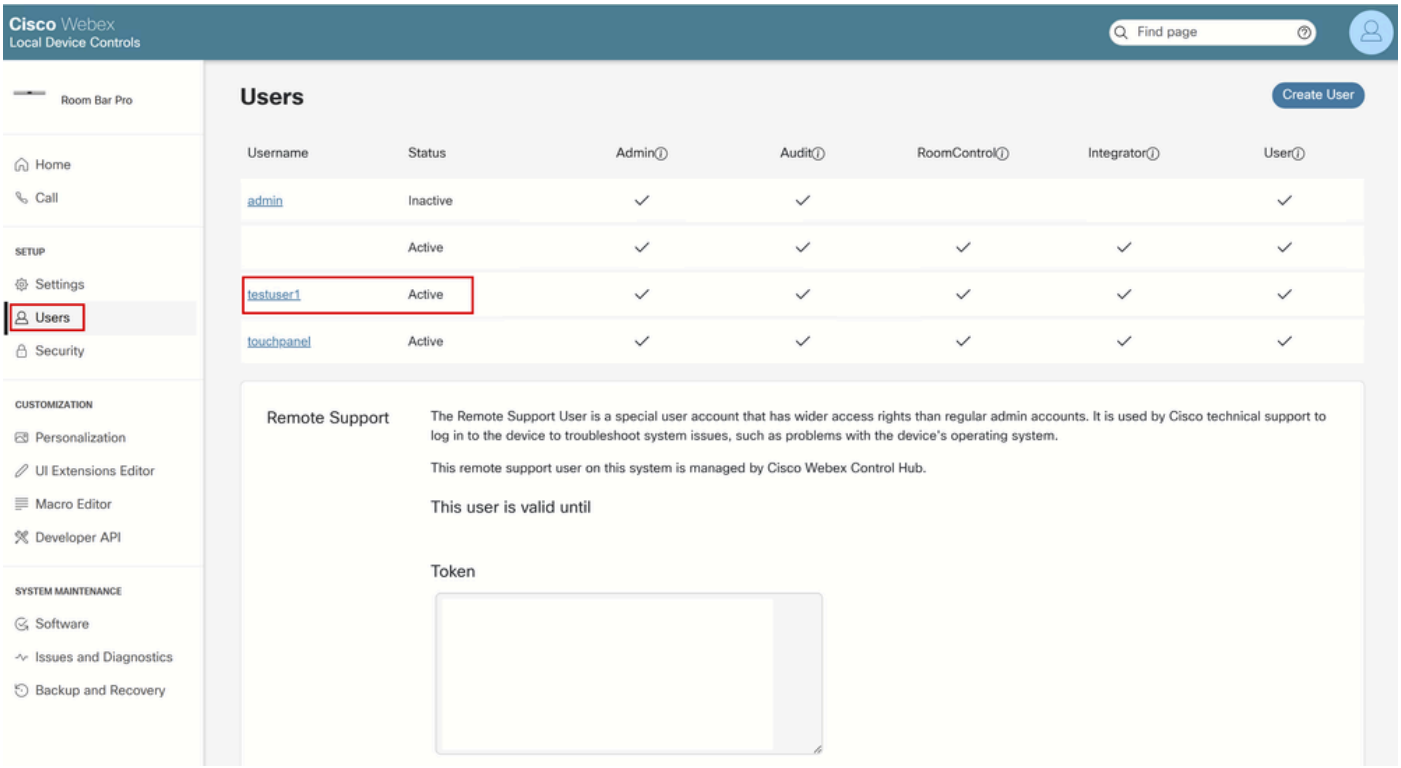
Abschnitt "Benutzer" in der GUI des Endpunkts

Geben Sie einen Benutzernamen und eine Passphrase (Kennwort) ein. Vergewissern Sie sich, dass der Benutzer über vollständige Administratorberechtigungen verfügt und aktiv ist:

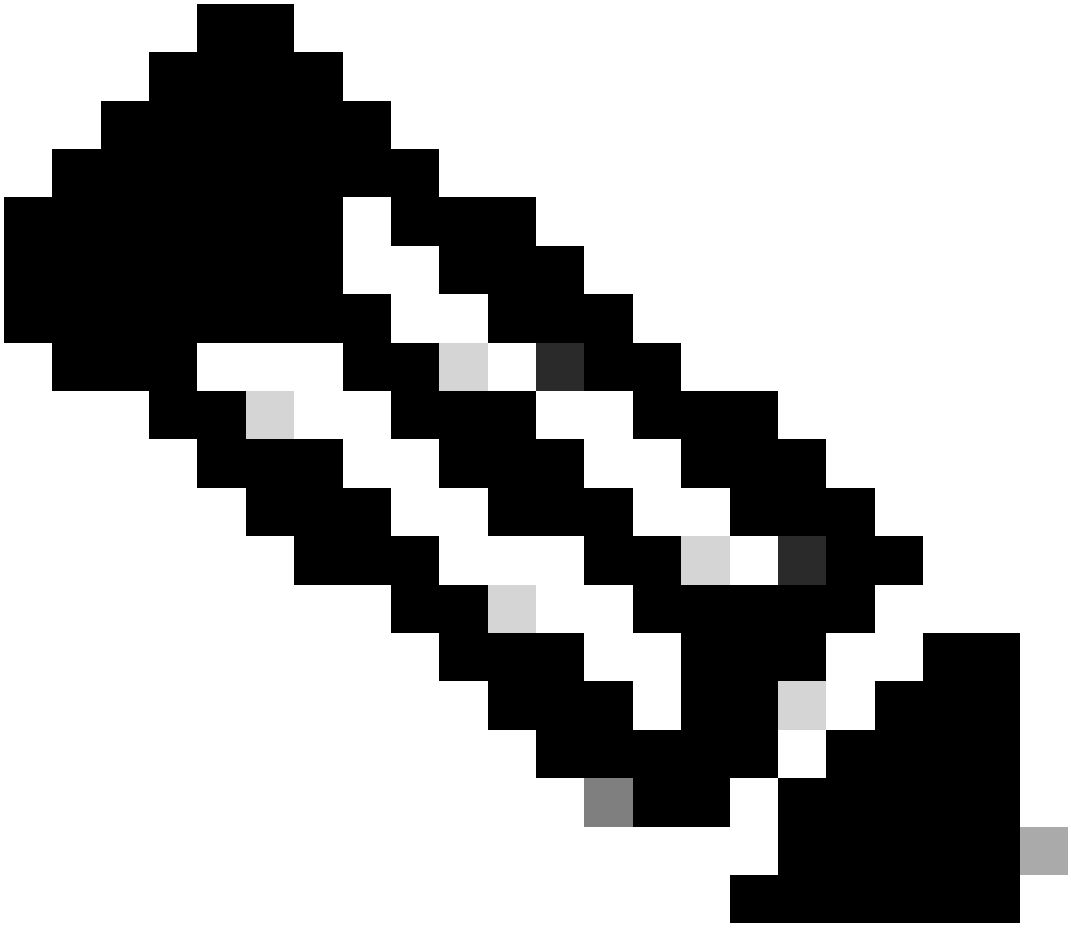


Erstellen eines Benutzers über die Endpunkt-GUI

Stellen Sie sicher, dass der Benutzer erstellt wurde und auf der Seite Users (Benutzer) aktiv ist:



Neuer Benutzer erstellt und unter anderen Benutzern aufgeführt



Anmerkung: Beim ersten SSH-Anmeldeversuch mit einem neu erstellten Benutzer werden Sie aufgefordert, Ihr Kennwort zu ändern. Es wird eine Eingabeaufforderung ähnlich der folgenden angezeigt:

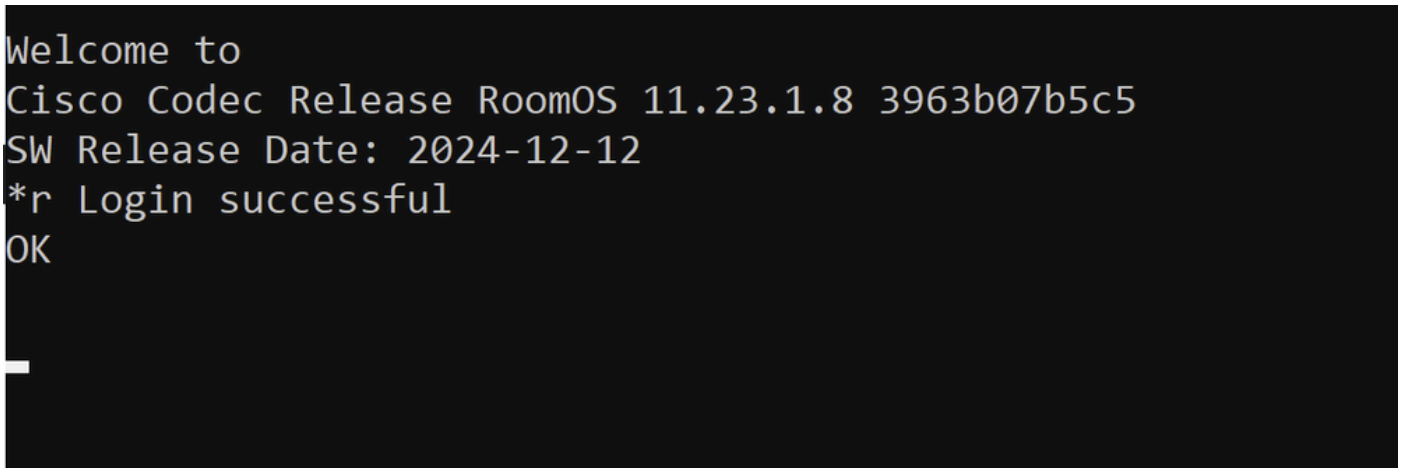
```
You are required to change your password.
Enter current password:
Enter new password:
Enter new password again:
OK
```

Kennwort bei erstmaligem SSH-Zugriff ändern

Sobald das Kennwort geändert wurde, wird die Verbindung sofort getrennt, und Sie müssen eine neue SSH-Verbindung starten.

Sobald der Admin-Benutzer erfolgreich erstellt wurde, verwenden Sie einen SSH-Client Ihrer

Wahl, und stellen Sie eine Verbindung zum Endpunkt her. Melden Sie sich mit den Administratoranmeldeinformationen an. Die folgende Eingabeaufforderung wird angezeigt:



Erfolgreicher Anmeldeversuch über SSH beim Endpunkt

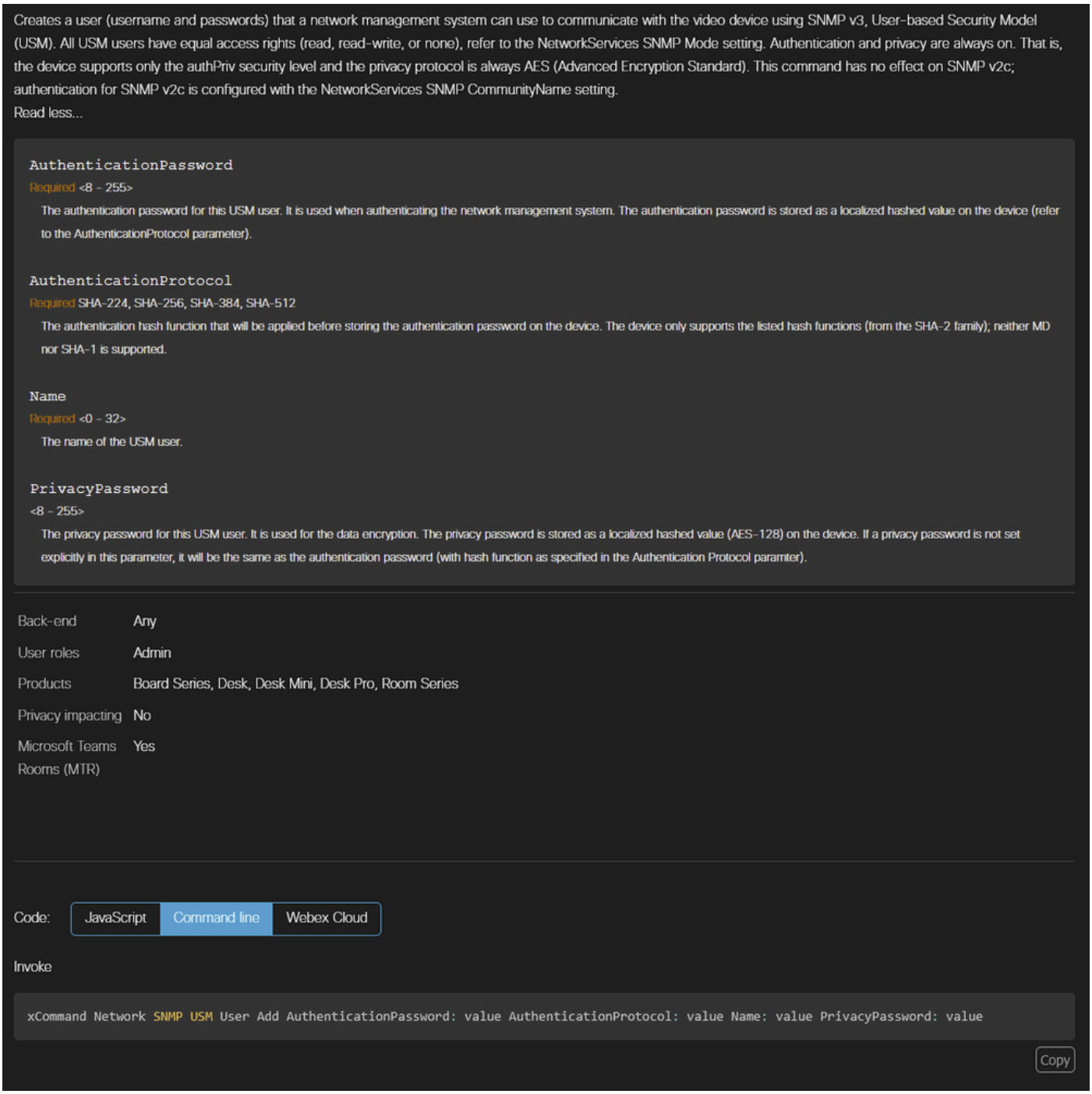
Verwenden Sie den Befehl Network SNMP USM User Add wie in diesem Artikel beschrieben. Für diese Demonstration wird der folgende Befehl verwendet:

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

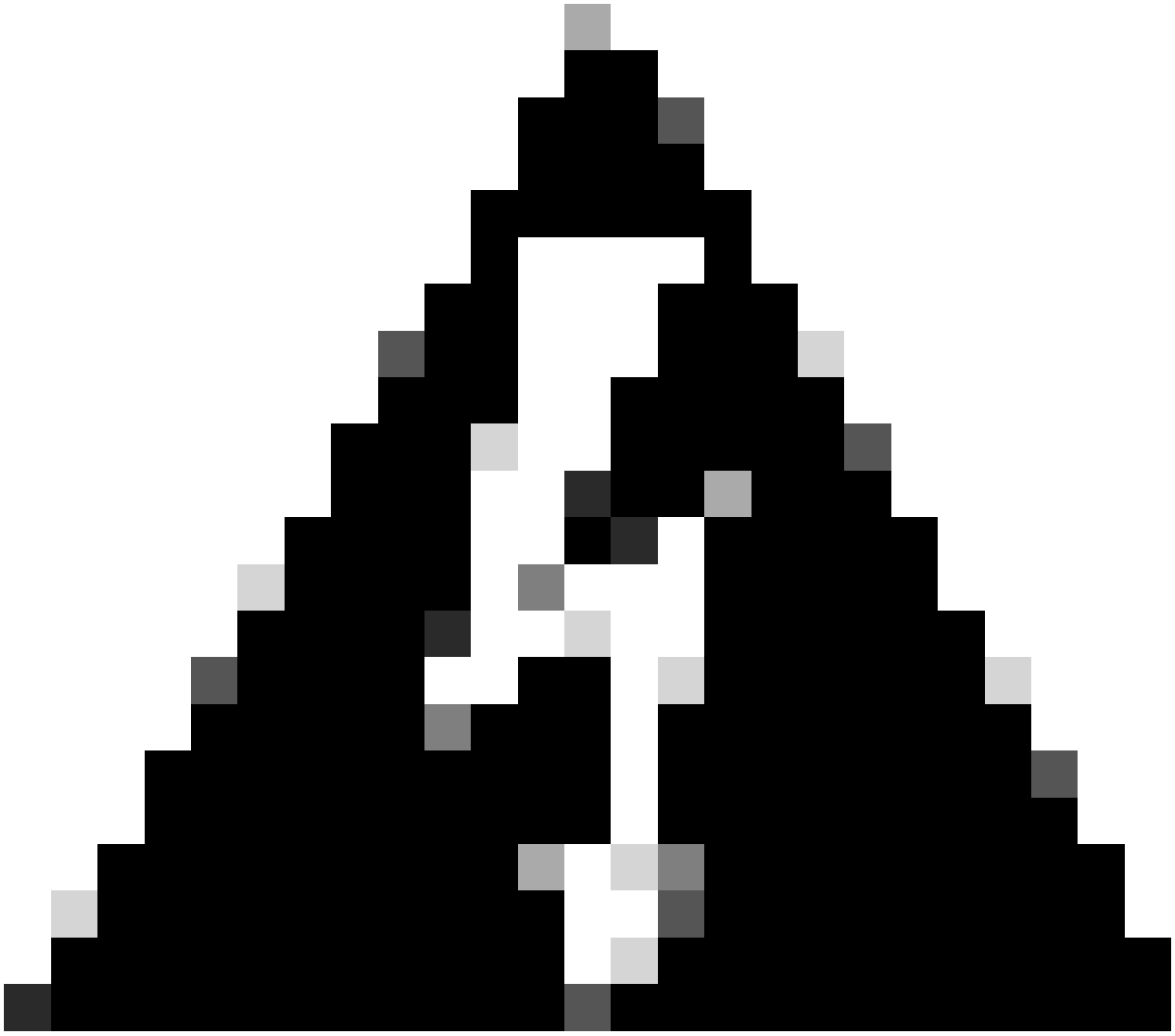
Wenn dieser Befehl erfolgreich ausgeführt wurde, lautet das Ergebnis:

Erstellung von USM-Benutzern über SSH

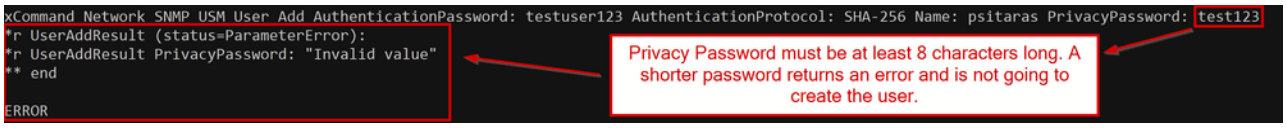
Damit der Befehl ohne Fehler ausgeführt werden kann, müssen Sie bestimmte Regeln befolgen, die in der Befehlsdokumentation unter diesem Link beschrieben werden. Zur Vereinfachung werden die aktuellen Anforderungen zum Zeitpunkt der Erstellung dieses Dokuments für diesen Befehl in dieses Bild eingefügt, aber Sie müssen sicherstellen, dass Sie auf diesen Link verweisen, wenn Sie Ihren Benutzer erstellen. Beachten Sie am Ende des Bildes, dass die genaue Syntax des Befehls vorhanden ist.



Befehlssyntax für die USM-Benutzererstellung aus der xAPI-Dokumentation



Warnung: Wenn ein Tippfehler vorliegt oder eine Anforderung nicht erfüllt wird, gibt der Befehl einen Fehler zurück, und der Benutzer wird nicht erstellt. Es wird ein Beispiel angeführt, bei dem statt eines Datenschutzkennworts mit mindestens 8 Zeichen ein kürzeres, 7 Zeichen umfassendes Kennwort angegeben wird:



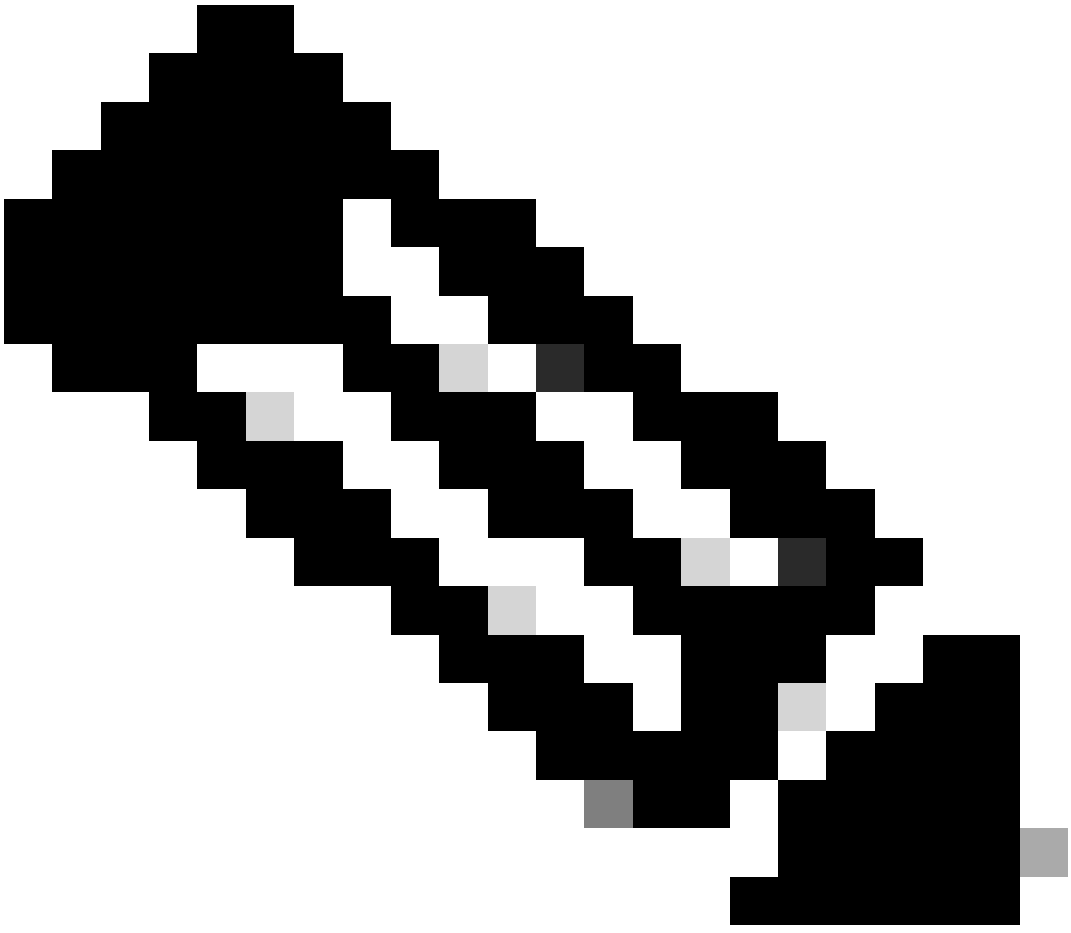
Fehlgeschlagene Erstellung des USM-Benutzers aufgrund des kurzen Datenschutzkennworts

Sie können testen, ob der Benutzer mit dem Befehl Netzwerk SNMP USM Benutzerliste erstellt wurde. Dieser Befehl listet alle USM-Benutzer auf, die auf dem Gerät gespeichert sind:

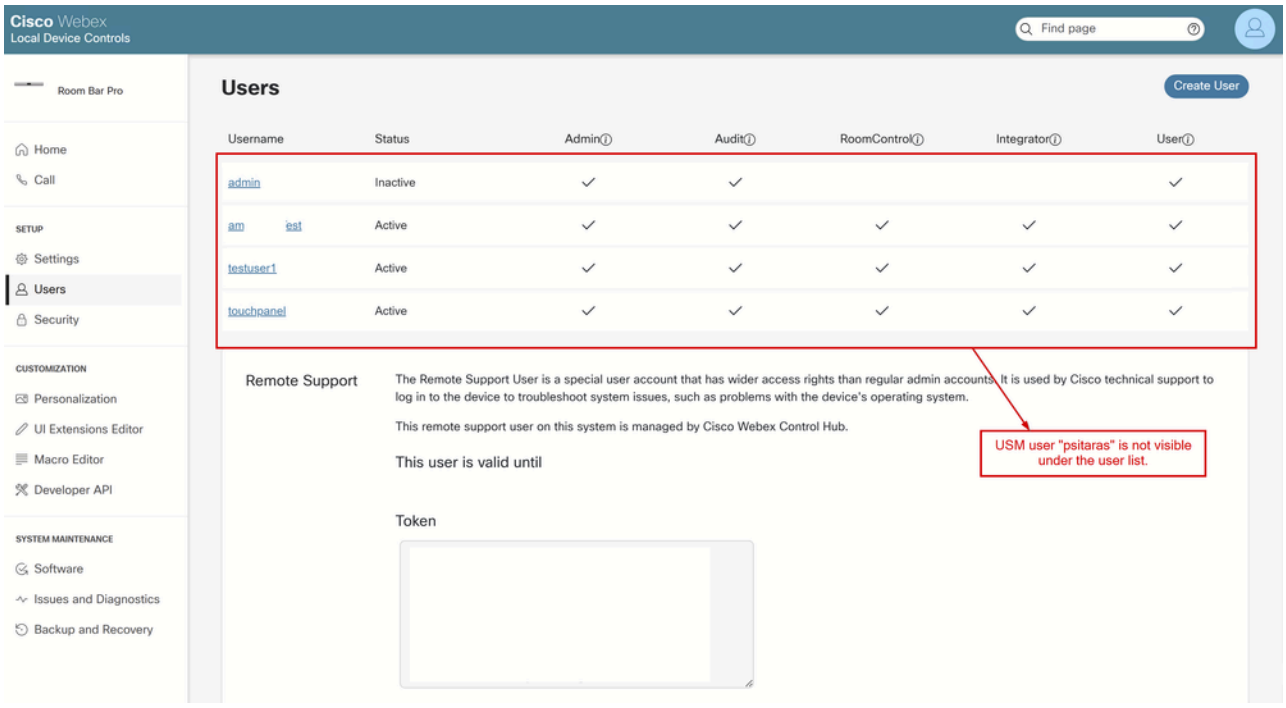
```
xCommand Network SNMP USM User List

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

Netzwerk SNMP USM-Benutzerlistenbefehl zur Bestätigung der Benutzererstellung

In dieser Phase wurde bestätigt, dass der Anwender psitaras erfolgreich erzeugt wurde. Die SNMPv3-Konfiguration wurde abgeschlossen.



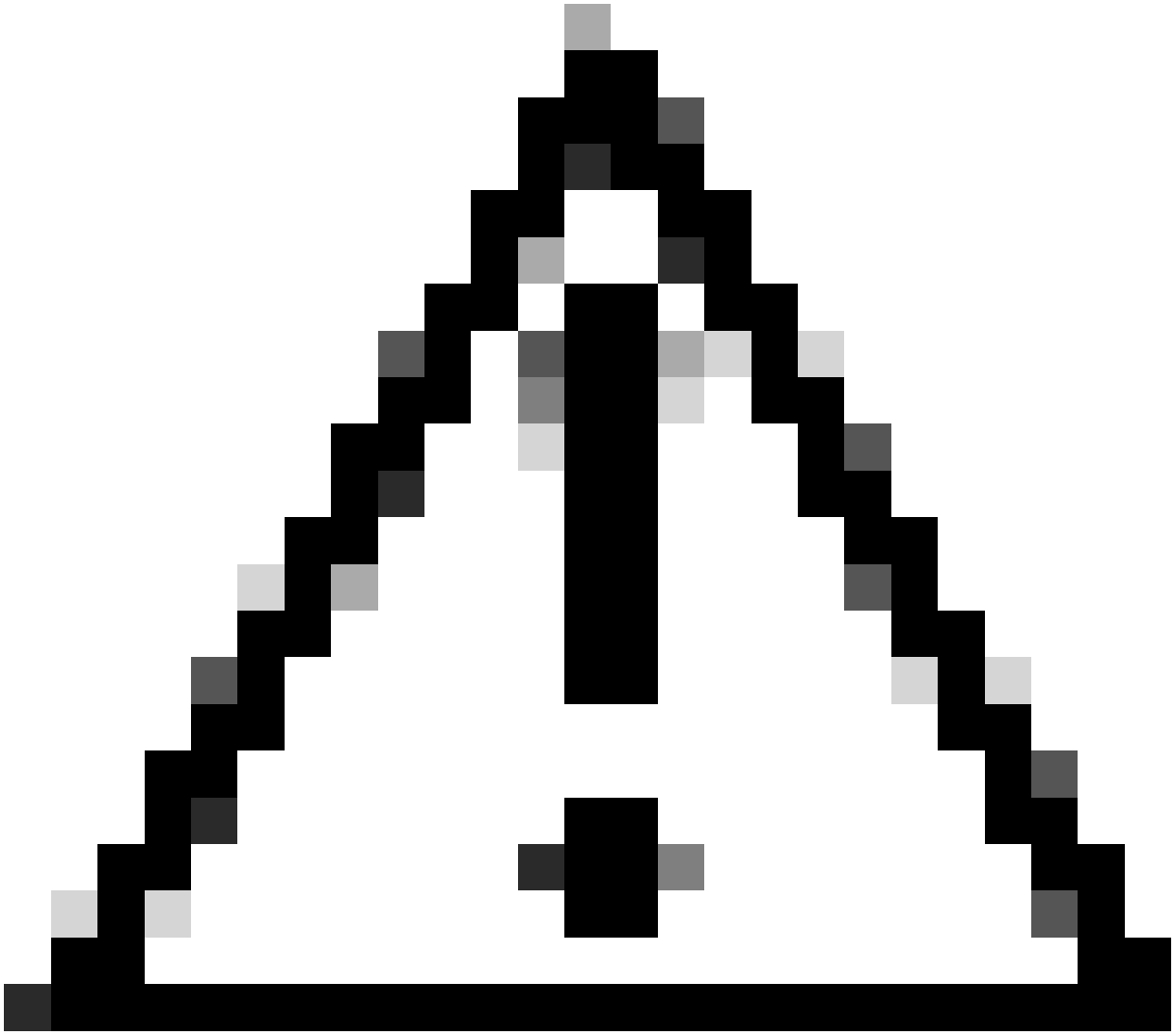
Anmerkung: Der USM-Benutzer psitaras ist in der grafischen Benutzeroberfläche des Endpunkts im Abschnitt "Users" (Benutzer) nicht sichtbar. Das wird erwartet.



USM-Benutzer sind in der Endpunkt-GUI unter Benutzer nicht sichtbar.

Testen der SNMPv2c- und SNMPv3-Konfiguration

Zu diesem Zeitpunkt können Sie mit dem Testen der SNMPv2c- und/oder SNMPv3-Konfiguration mit dem Netzwerkmanagementsystem (NMS) fortfahren. Für diesen Artikel enthält die Laborkonfiguration keine NMS- oder SNMP-Server, auf denen ein SNMP-Dienst ausgeführt wird. Zum Testen der Konfiguration wird das Dienstprogramm snmpwalk verwendet. Dieses Dienstprogramm ist auf einem Linux-Server installiert.

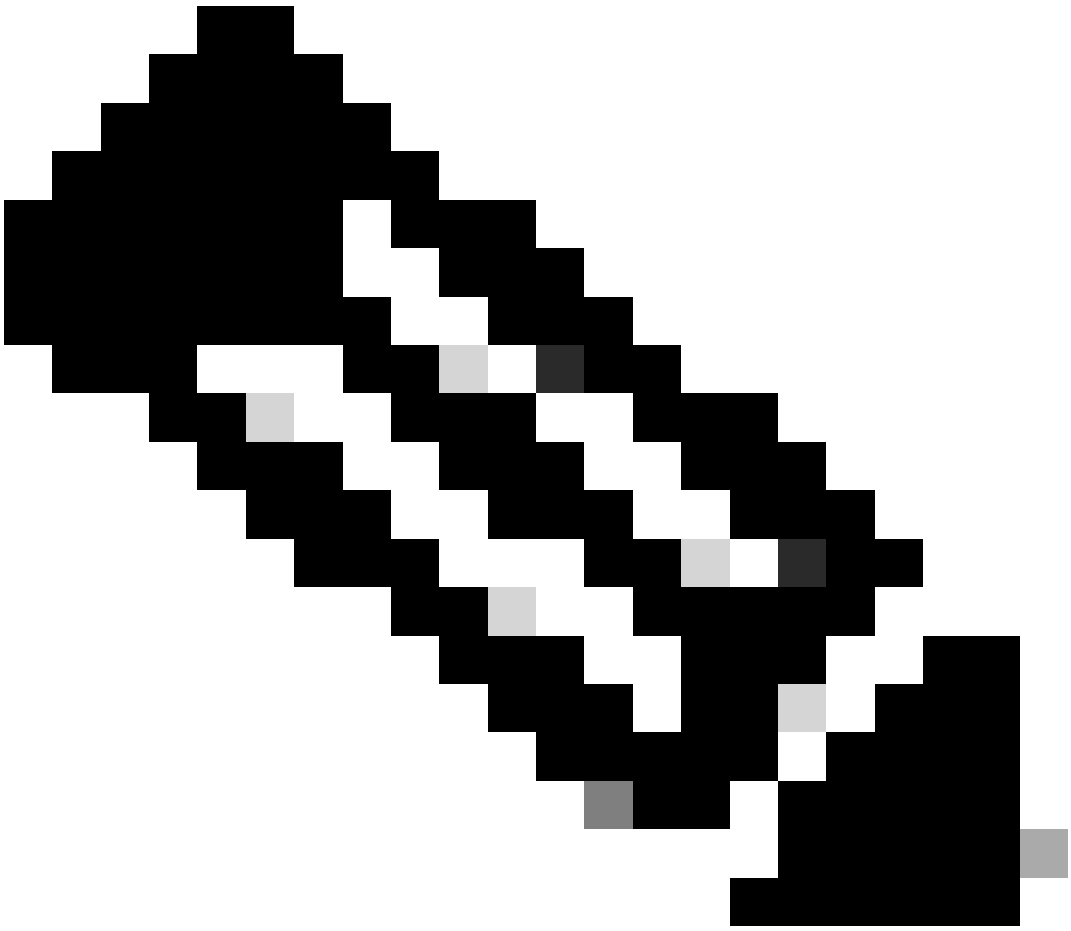


Vorsicht: SNMPwalk ist kein empfohlenes Tool zum Testen der SNMP-Konfiguration auf Ihren Collaboration-Endgeräten. Es wird nicht von TAC-Technikern unterstützt, und Sie müssen mit der Verwendung des Tools vertraut sein, bevor Sie mit den Tests fortfahren. Anstelle von snmpwalk können Sie Ihre Konfiguration mit einem beliebigen anderen SNMP-Tool oder Ihrem NMS testen. SNMPwalk wird in diesem Artikel nur als Beispiel verwendet (ein Tool ist erforderlich, um die Konfiguration zu Demonstrationszwecken zu testen), und es gibt keine Verpflichtung oder Promotion im Zusammenhang mit ihrer Verwendung.

Die Installation von snmpwalk ist nicht Teil dieser Anleitung und wird weggelassen. Je nach Betriebssystem des Systems, das Sie zum Testen verwenden, können die Installationsanforderungen variieren. Vor dem Testen müssen Sie an der erfolgreichen Installation arbeiten.

SNMPwalk ist ein Tool, mit dem Sie die SNMP-Konfiguration überprüfen können. Es führt einen Spaziergang durch die MiBs des Endpunkts durch und gibt die verfügbaren Informationen zurück. Cloud-registrierte Endgeräte stellen 7 Object Identifiers (OIDs) bereit:

- SNMPv2-MIB::sysDescr (gelesen),
- SNMPv2 -MIB::sysObjectID (gelesen),
- DISMAN-EVENT-MIB::sysUpTimeInstance (gelesen),
- SNMPv2 -MIB::sysContact (Lesen/Schreiben),
- SNMPv2 -MIB::sysName (Lesen/Schreiben),
- SNMPv2 -MIB::sysLocation (Lesen/Schreiben),
- SNMPv2 -MIB::sysServices (gelesen).



> Anmerkung: Die internen IPs, die für die aufgelisteten snmpwalk-Tests verwendet werden, sind private IPs und werden nicht mehr verwendet. Die für diesen Leitfaden verwendete Übung wurde außer Betrieb genommen, und die Geräte werden auf die Werkseinstellungen zurückgesetzt.

Der Cisco Room Kit Pro-Endpunkt ist mit SNMPv2c konfiguriert. Die Authentifizierung erfolgt mithilfe von Community-Strings. Geben Sie den folgenden Befehl ein:

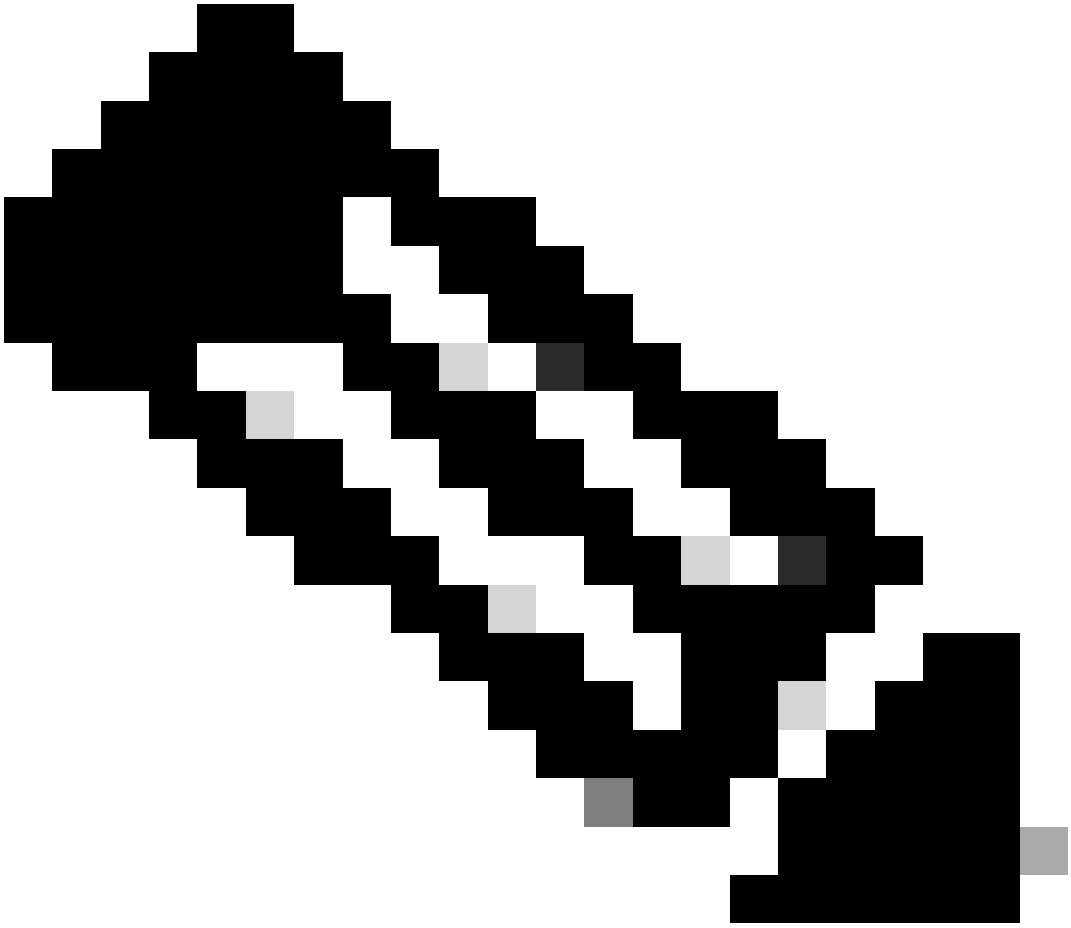
```
# '-c' option is used to provide the community string
# '-v' option is used to provide the SNMP version used
# The IP provided is the endpoint's IP

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: FDO2706JG49"
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 liefert 7 Ergebnisse wie erwartet. Es gibt drei MiBs, die leer sind:

1. SNMPv2 -MIB::sysContact (Lesen/Schreiben), (iso.3.6.1.2.1.1.4.0)
2. SNMPv2 -MIB::sysName (Lese-/Schreibzugriff), (ISO 3.6.1.2.1.1.5.0)
3. SNMPv2 -MIB::sysLocation (Lese-/Schreibzugriff), (iso.3.6.1.2.1.1.6.0)

Es gibt drei xConfiguration-Befehle, mit denen Werte auf diese MiBs festgelegt werden können. SSH an den Endpunkt senden und die folgenden Befehle ausführen:

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



> Anmerkung: Anstatt diese drei Befehle zu verwenden, können Sie Änderungen an diesen Einstellungen über den Control Hub, die Endpunkt-GUI oder über WebEx APIs vornehmen.

Sobald die oben genannten Befehle ausgegeben wurden, verwenden Sie erneut snmpwalk auf demselben Endpunkt. Sie sehen, dass die zuvor leeren MiBs mit den Werten gefüllt werden, die über die xConfiguration-Befehle bereitgestellt werden:

```
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: FDO2706JG49"
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)
```

Zu diesem Zeitpunkt wird bestätigt, dass die auf dem Room Kit Pro-Gerät vorgenommene SNMPv2c-Konfiguration betriebsbereit ist.

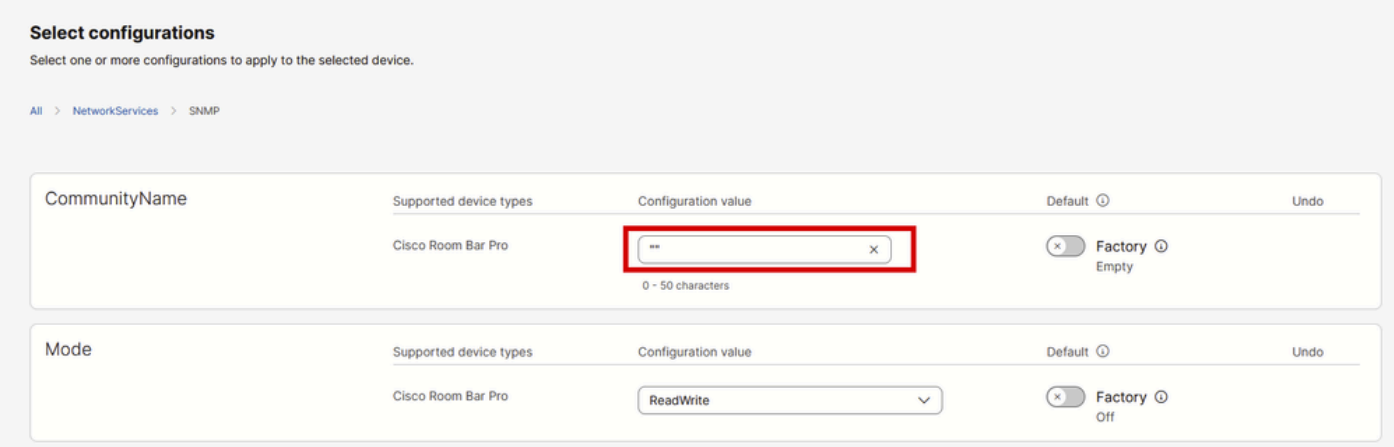
Der Cisco Room Bar Pro-Endpunkt ist mit SNMPv3 konfiguriert. Für SNMPv3 müssen Sie sicherstellen, dass Sie die richtige Authentifizierung verwenden. Community-Strings werden nicht verwendet. Stattdessen verwendet SNMPv3 Benutzernamen und Kennwörter.

```
# '-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)
```

Zu diesem Zeitpunkt wird bestätigt, dass die auf dem Room Bar Pro-Gerät vorgenommene SNMPv3-Konfiguration betriebsbereit ist.

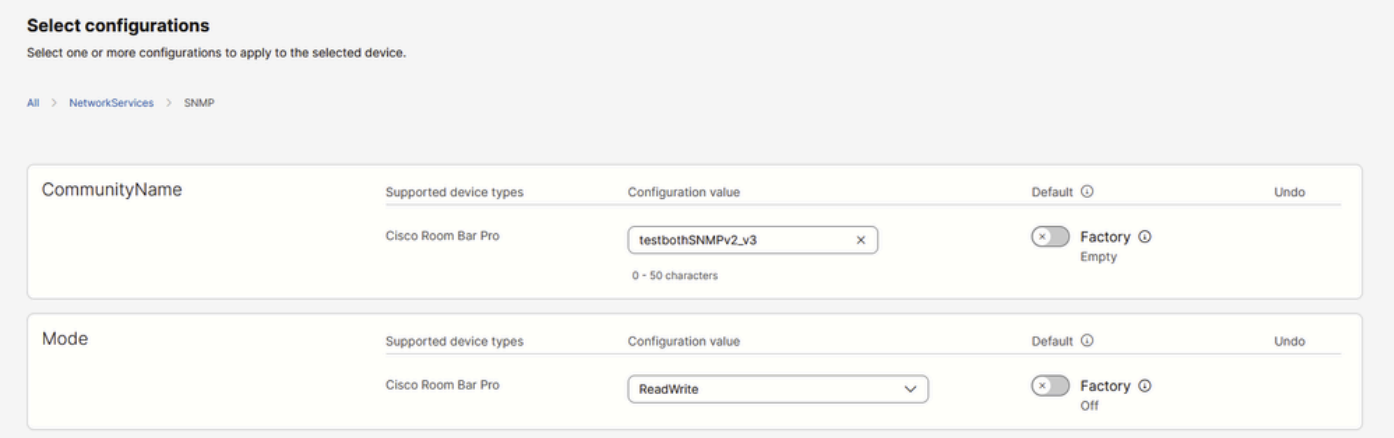
Können auf einem Endgerät SNMPv2c und SNMPv3 gleichzeitig aktiv sein?

Ja, es ist möglich. Sie müssen jedoch während der SNMP-Konfiguration einen Community-Namen einrichten, um SNMPv2c-Authentifizierung zu erhalten. Für diesen Test wird die Room Bar Pro aus den vorherigen Beispielen verwendet. Die aktuelle Konfiguration im Abschnitt "Control Hub - Alle Konfigurationen" des Endpunkts lautet:



Endpunkt-SNMP-Konfigurationen im Control Hub

Beachten Sie, dass der Community-Name nicht leer ist. Es gibt zwei Anführungszeichen, die angeben, dass der Community-Name eine leere Zeichenfolge ist. Sie können die SNMP-Unterstützung auf Version 3 beschränken, indem Sie NetworkServices SNMP CommunityName auf eine leere Zeichenfolge ("") festlegen. Sie müssen diese Zeichenfolge durch einen Community-Namen ersetzen, z. B. testbothSNMPv2_v3.



Hinzufügen eines Community-Namens für SNMPv2c in den Konfigurationseinstellungen des Control Hub-Endpunkts

Es wurde bereits bestätigt, dass SNMPv3 auf der Room Bar Pro funktioniert. SNMPwalk wird verwendet, um zu testen, ob SNMPv2c auch funktioniert, nachdem der Community-Name eingerichtet wurde:

```
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)
```

Konfiguration mehrerer Endpunkte über Control Hub mit SNMP möglich

Ja, im Control Hub können mehrere Geräte gleichzeitig konfiguriert werden. In diesem Artikel finden Sie Informationen dazu, wie Sie die Konfiguration Schritt für Schritt im Abschnitt Mehrere Geräte konfigurieren durchführen.

Wichtige Informationen zur Erinnerung

- Es sind nur bestimmte MiBs verfügbar. Die Anzahl der verfügbaren MIBs ist durch das Design des Entwicklungsteams, das die Endgeräte entwirft, begrenzt. MiBs können nicht erweitert oder erweitert werden, um weitere Informationen bereitzustellen.
- SNMPv2c authentifiziert sich mithilfe des Community-Namens (auch Community String genannt), während SNMPv3 sich anhand von Benutzername und Kennwort authentifiziert und außerdem Verschlüsselung bietet. Stellen Sie beim Testen sicher, dass Sie die richtige Authentifizierungsmethode (mit snmpwalk oder einem anderen Tool/NMS) für das von Ihnen konfigurierte Protokoll verwenden.
- Authentifizierung und Datenschutz sind auf SNMPv3 immer aktiviert. Die Endpunkte unterstützen nur die authPriv-Sicherheitsstufe, und das Datenschutzprotokoll ist immer Advanced Encryption Standard (AES).
- SNMPv3 wird nur mit USM-Optionen (User-Based Security Model) unterstützt. SMNPv3 über TLS wird nicht unterstützt.
- USM-Benutzerbefehle, die zum Konfigurieren von Benutzern für die SNMP-Authentifizierung verwendet werden, haben keine Auswirkungen auf SNMPv2c.
- Die Einstellung "SNMP CommunityName" auf Endpunkten hat keine Auswirkungen auf die SNMPv3-Konfiguration.
- Bei SNMP CommunityName wird die Groß-/Kleinschreibung beachtet.
- Sie können die SNMP-Unterstützung auf Version 3 beschränken, indem Sie für den NetworkServices SNMP CommunityName eine leere Zeichenfolge ("") festlegen.
- SNMPv1 wird nicht unterstützt.
- Sowohl für SNMPv2c als auch für SNMPv3 stellen die Endpunkte die gleichen Objektkennungen (OIDs) bereit.
- Für SNMPv3 muss das Authentifizierungsprotokoll zur SHA-2-Familie gehören (weder MD noch SHA-1 werden unterstützt). Wenn dies nicht der Fall ist, werden SNMP-Anforderungen nicht authentifiziert und bleiben unbeantwortet.
- Das Datenschutzkennwort wird als lokalisierter Hashwert (AES-128) auf dem Gerät gespeichert. Wenn ein Datenschutzkennwort in diesem Parameter nicht explizit festgelegt wird, wird es auf dasselbe wie das Authentifizierungskennwort festgelegt (mit einer Hashfunktion, wie im Authentifizierungsprotokollparameter angegeben).
- Kennwörter/Passphrasen und Benutzernamen müssen innerhalb bestimmter Längengrenzen sein. Der USM-Benutzername muss beispielsweise bis zu 32 Zeichen lang sein, und das Authentifizierungskennwort muss mindestens 8 und höchstens 255 Zeichen

lang sein. Wenn diese Anforderungen nicht erfüllt werden, erstellt der Befehl "Network SNMP USM User Add" den Benutzer nicht und gibt einen Fehler zurück.

Kontaktaufnahme mit dem TAC zur Behebung eines SNMP-Problems auf einem Endgerät

Wenn die SNMP-Konfiguration des Endpunkts abgeschlossen wurde, aber ein Problem aufgetreten ist, wenden Sie sich an das TAC und teilen Sie diese Informationen mit:

- Geben Sie Ihre Organisations-ID im Control Hub und die Seriennummer (SN) des betroffenen Endpunkts an.
- Beschreiben Sie das jeweilige Szenario.
- Geben Sie die SNMP-Version an, die Sie konfigurieren möchten.
- Geben Sie alle erkannten Fehlermeldungen an.
- Wenn bei der Konfiguration des Geräts ein Problem auftritt, erläutern Sie genau, in welchem Schritt der Konfigurationsprozess gestoppt wurde, und geben Sie Screenshots an. Geben Sie den Konfigurationsbefehl frei, der einen Fehler zurückgibt.
- Sammeln Sie Endgeräteprotokolle, und laden Sie sie auf Ihr Ticket hoch.
- Geben Sie das Dienstprogramm\NMS oder ein anderes Tool zum Testen der SNMP-Konfiguration frei. Wenn Sie ein Dienstprogramm zum Testen mit dem SNMP-Agenten der Endpunkte verwenden, geben Sie den vollständigen verwendeten Befehl ein.

Zugehörige Informationen

xAPI-Dokumentation für Raumbetriebssysteme - SNMP-bezogene Befehle

Gerätekonfigurationen für Mainboard-, Schreibtisch- und Raumgeräte

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.