クラウド登録エンドポイントでのSNMPの設定

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

SNMPとは

要求可能な情報

クラウド登録エンドポイントでのSNMPの設定

- Control HubでのSNMPv2cモードの有効化
- Control HubでのSNMPv3モードの有効化
  - エンドポイントGUIでのSNMP設定の表示
- SNMPv3のUSMユーザの設定

SNMPv2cおよびSNMPv3設定のテスト

1つのエンドポイントでSNMPv2cとSNMPv3の両方を同時にアクティブにできる

SNMPを使用してControl Hub経由で複数のエンドポイントを設定可能

重要な詳細情報

エンドポイントでのSNMPの問題を解決するためにTACに連絡する

関連情報

はじめに

このドキュメントでは、クラウド登録されたエンドポイントでSNMPを設定およびトラブルシューティングする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Control Hubプラットフォーム
- エンドポイントのグラフィカルユーザインターフェイス(GUI)およびControl Hub Devicesセクションによるエンドポイントの管理
- 管理者ユーザとしてエンドポイントにSSHで接続
- ルームOS
- SNMP（SNMPv2cおよびSNMPv3）
- Snmp設定をテストするためのsnmpwalkまたは他のユーティリティ/ツール、あるいはネットワーク管理システム(NMS)

使用するコンポーネント

次に示す機器は、テストを行い、このドキュメントで説明する結果を生成するために使用されています。

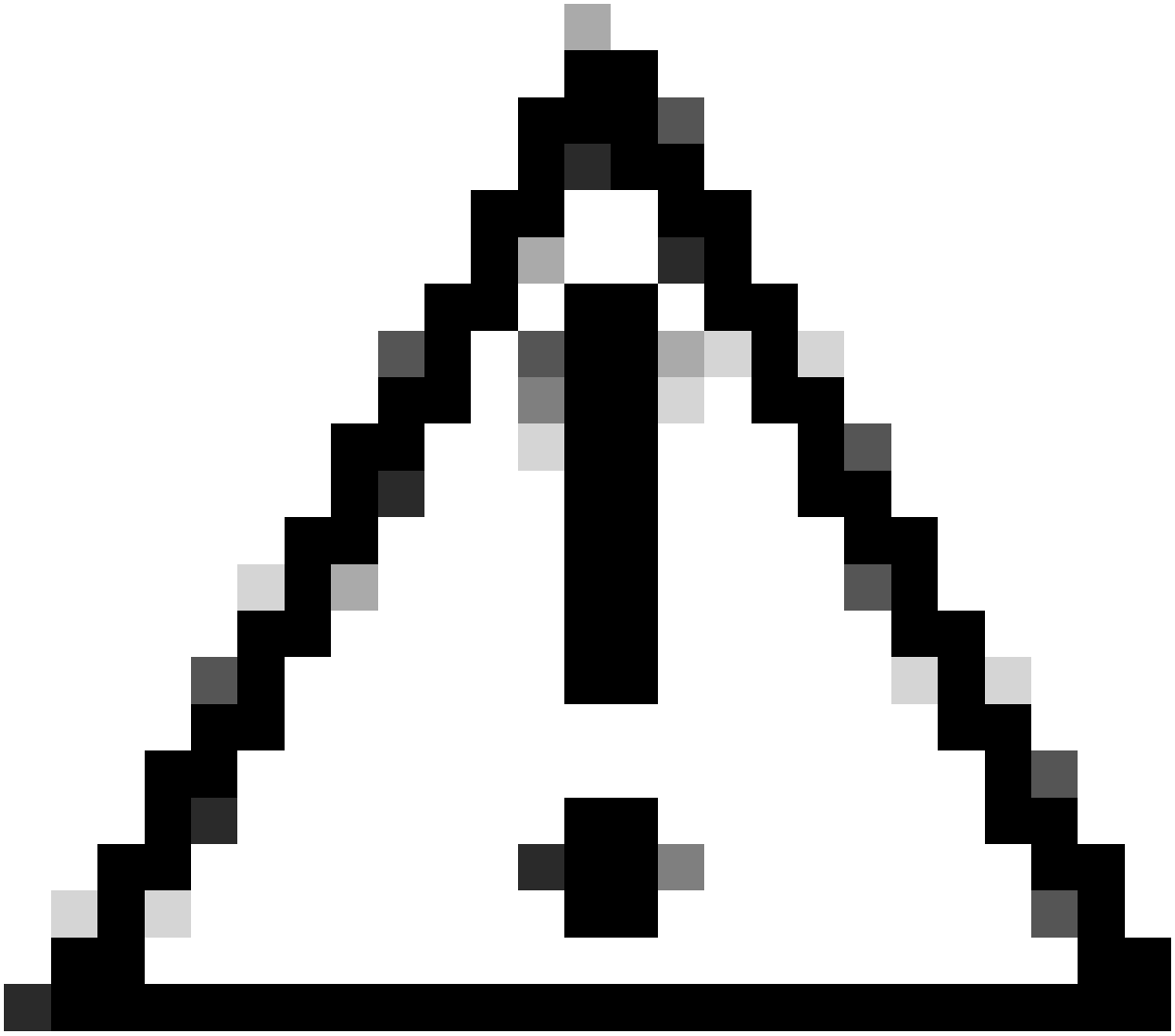
- Control Hub組織
- Ciscoルームキットプロ
- シスコルームバープロ
- SNMP設定をテストするためのsnmpwalkユーティリティをホストするLinuxサーバ。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

SNMPとは

SNMPはSimple Network Management Protocolの略です。ネットワーク内のデバイスに関する情報の収集と管理、デバイスのステータスの監視、または設定変更を行うために使用されるプロトコルです。これらのデバイスは、ルータ、スイッチ、サーバ、プリンタ、またはその他の任意のタイプのデバイスです。これらのデバイスにIPアドレスが割り当てられていることが前提条件です。SNMPには3つのバージョンがあります。ルームOSはSNMPv2cおよびSNMPv3をサポートします。SNMPv1はサポートされていません。

この記事では、クラウド登録されている（Webex Edge for Devicesを使用していない）Room OSを実行しているコラボレーションエンドポイントでのSNMPの設定とトラブルシューティングに重点を置いています。



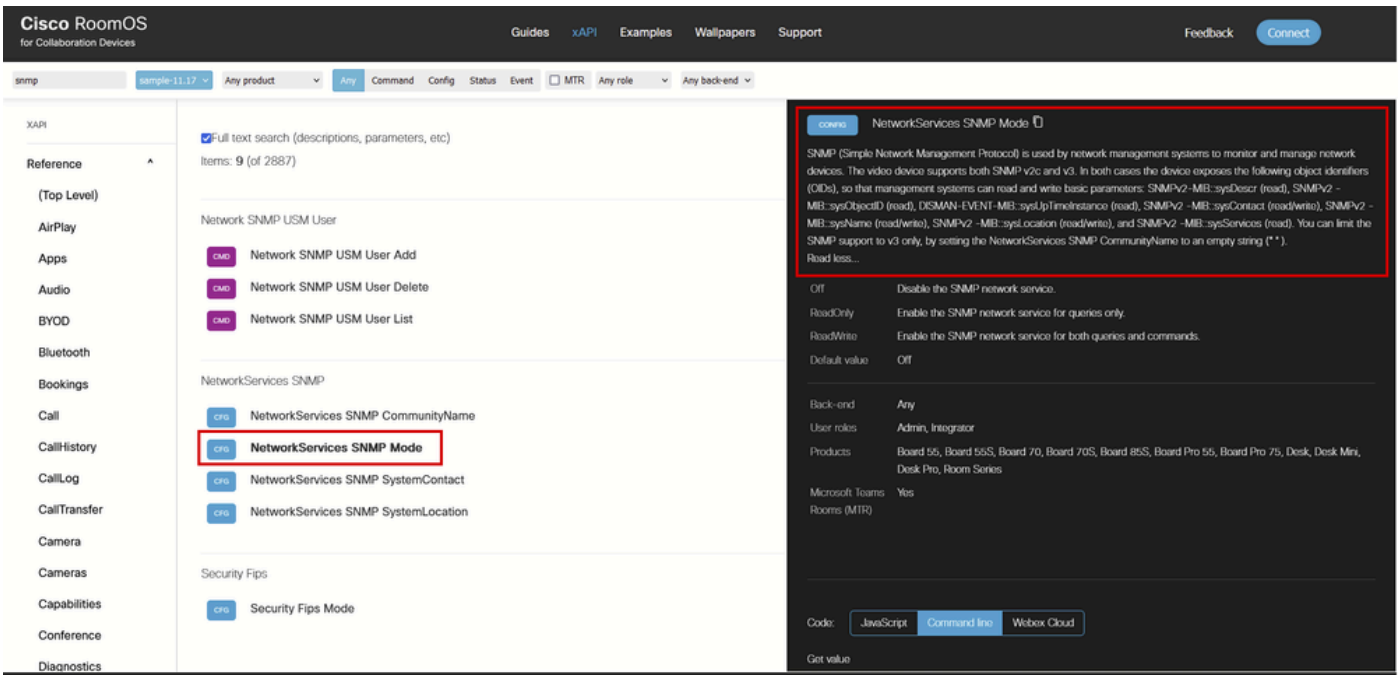
注意：この記事では、エンドポイントの観点からのみSNMP設定にアプローチしています。ネットワーク側で行う設定や、エンドポイントでSNMP関連情報の要求/更新に使用するツールは、この記事の対象外です。

TACは、ネットワーク内のSNMPのトラブルシューティングをサポートしておらず、ネットワークの観点からSNMPが期待どおりに動作しない理由についても推論を行えません。これらの問題のトラブルシューティングには、ネットワークチームがさらに関与する必要があります。

SNMPの管理は、多くの異なるツールを使用して実現できます。これらのツールはTACではサポートされていません。ツールがエンドポイントから収集する情報に不一致がある場合、最初にネットワークチームが問題をトラブルシューティングし、エンドポイント関連の問題であることを証明する十分な情報がある場合は、TACにエスカレーションする必要があります。

要求可能な情報

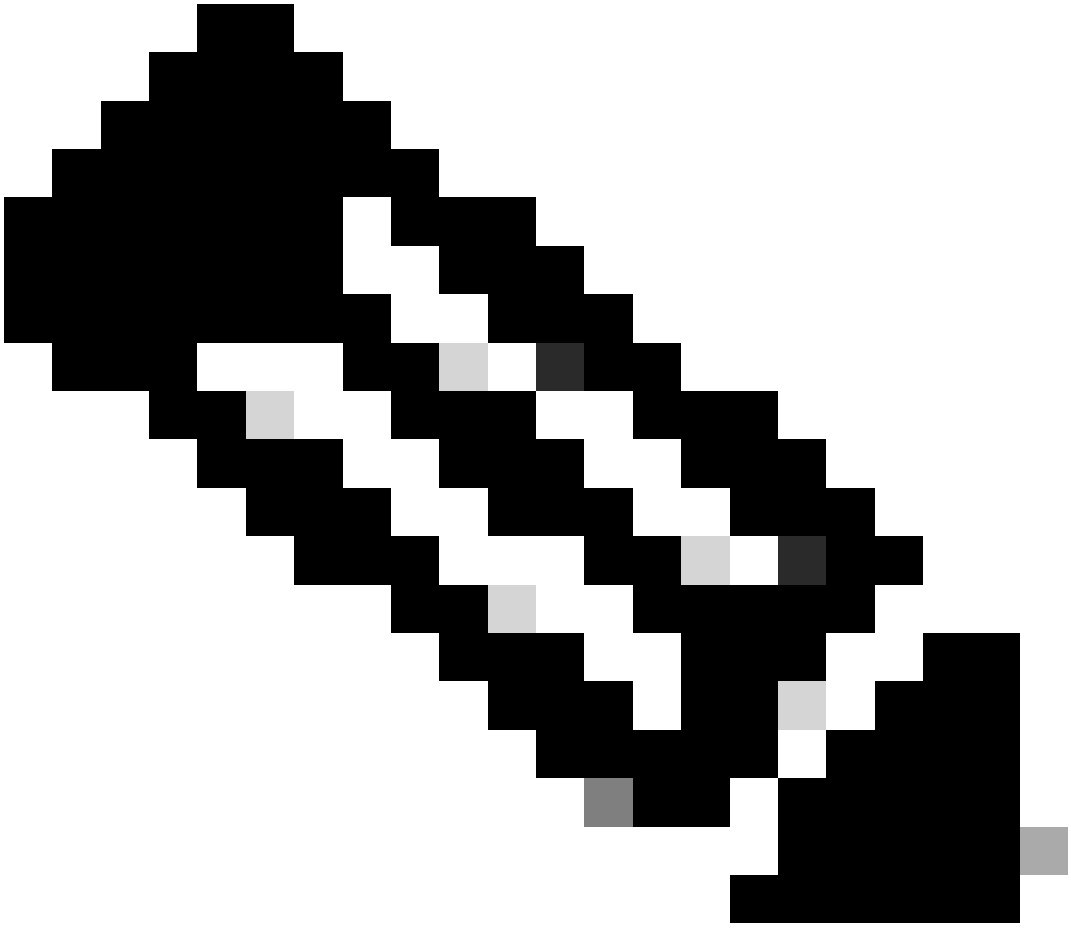
SNMPを使用すると、エンドポイントから限られた量の情報を要求できます。サポートされるOIDおよびMiBは、このリンクの、NetworkService SNMP Modeコマンドの説明の詳細の下に表示されます。



ルームOS xAPIドキュメントのNetworkService SNMPモードコマンドの説明

エンドポイントは、SNMPv2とSNMPv3の両方で次のOIDを公開します。

- SNMPv2-MIB::sysDescr（読み取り）、
- SNMPv2 -MIB::sysObjectID（読み取り）、
- DISMAN-EVENT-MIB::sysUpTimeInstance（読み取り）、
- SNMPv2 -MIB::sysContact（読み取り/書き込み）、
- SNMPv2 -MIB::sysName（読み取り/書き込み）、
- SNMPv2 -MIB::sysLocation（読み取り/書き込み）、
- SNMPv2 -MIB::sysServices（読み取り）。

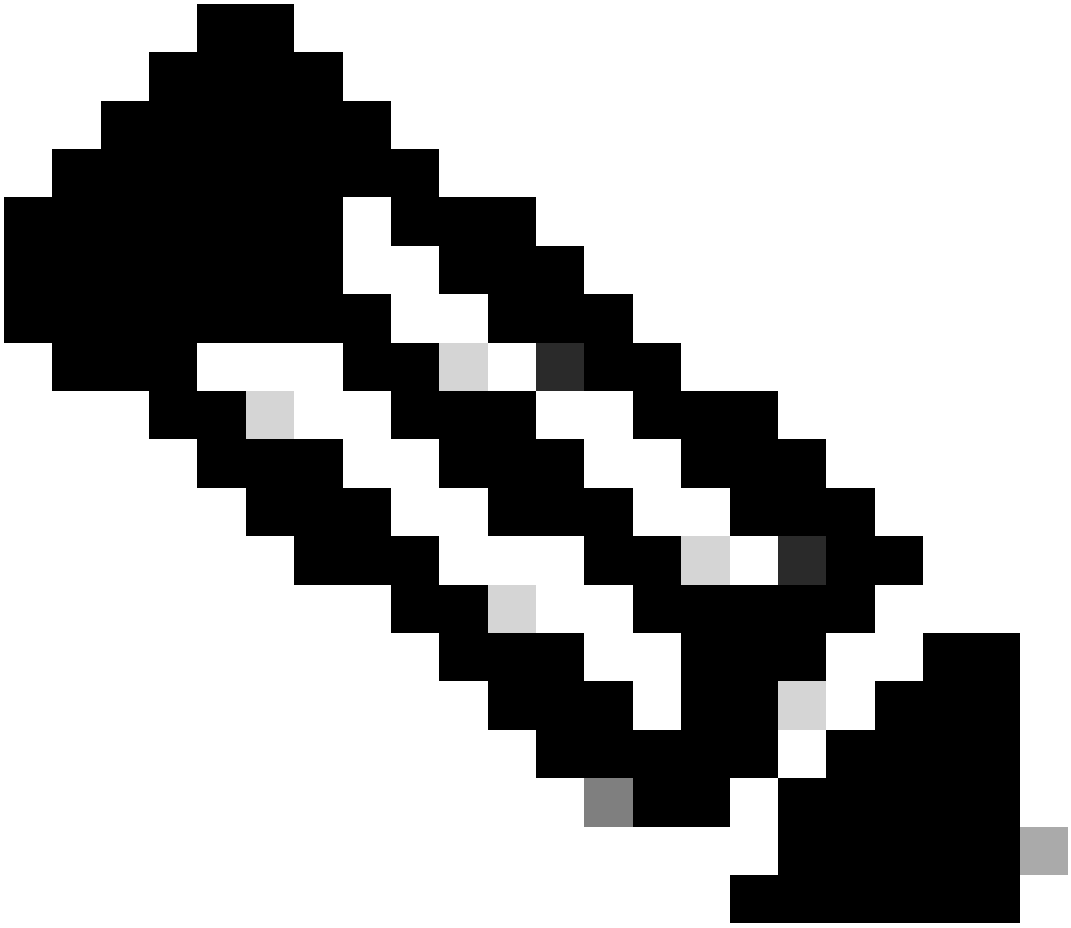


注:SNMPv3のみを使用する場合は、NetworkServices SNMP CommunityNameに空の文字列を設定できます。

クラウド登録エンドポイントでのSNMPの設定

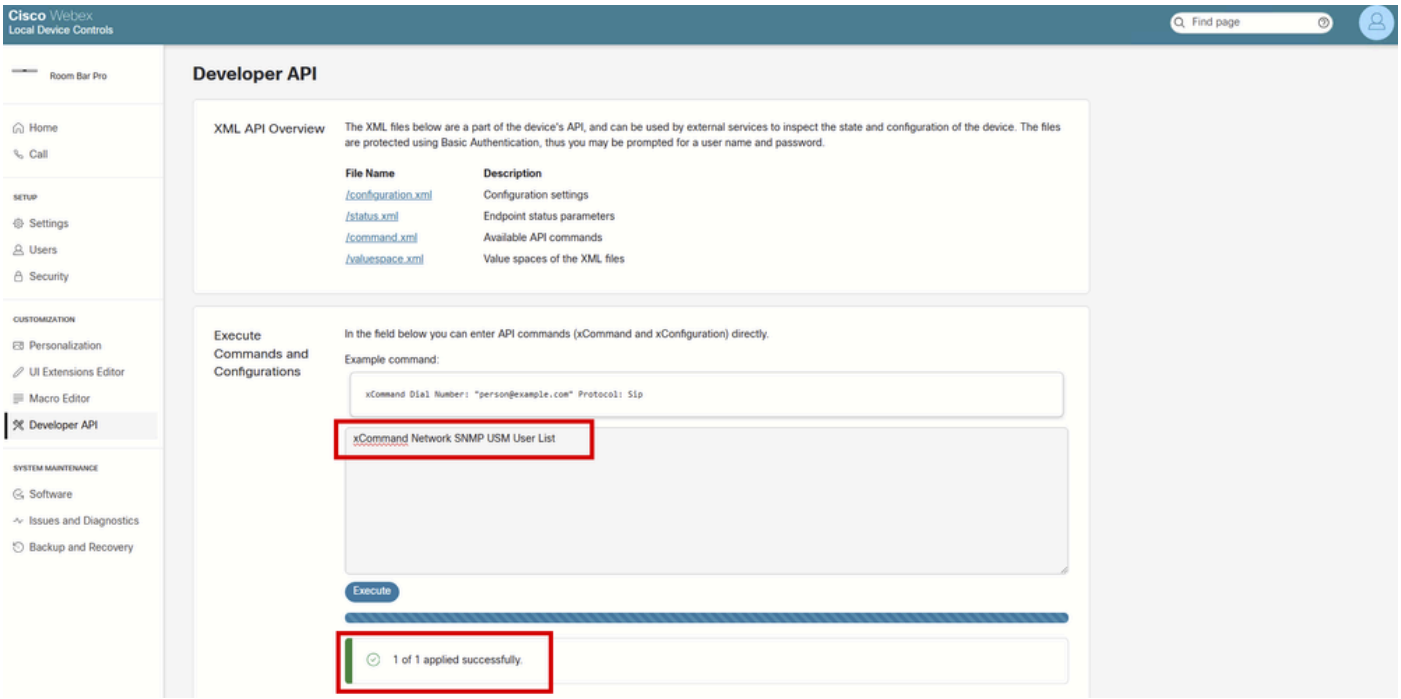
一般に、エンドポイントの設定変更は4つの異なる方法で行われます。

1. 利用可能なWebex API
2. エンドポイントGUI
3. Control Hub
4. エンドポイントへの直接SSH

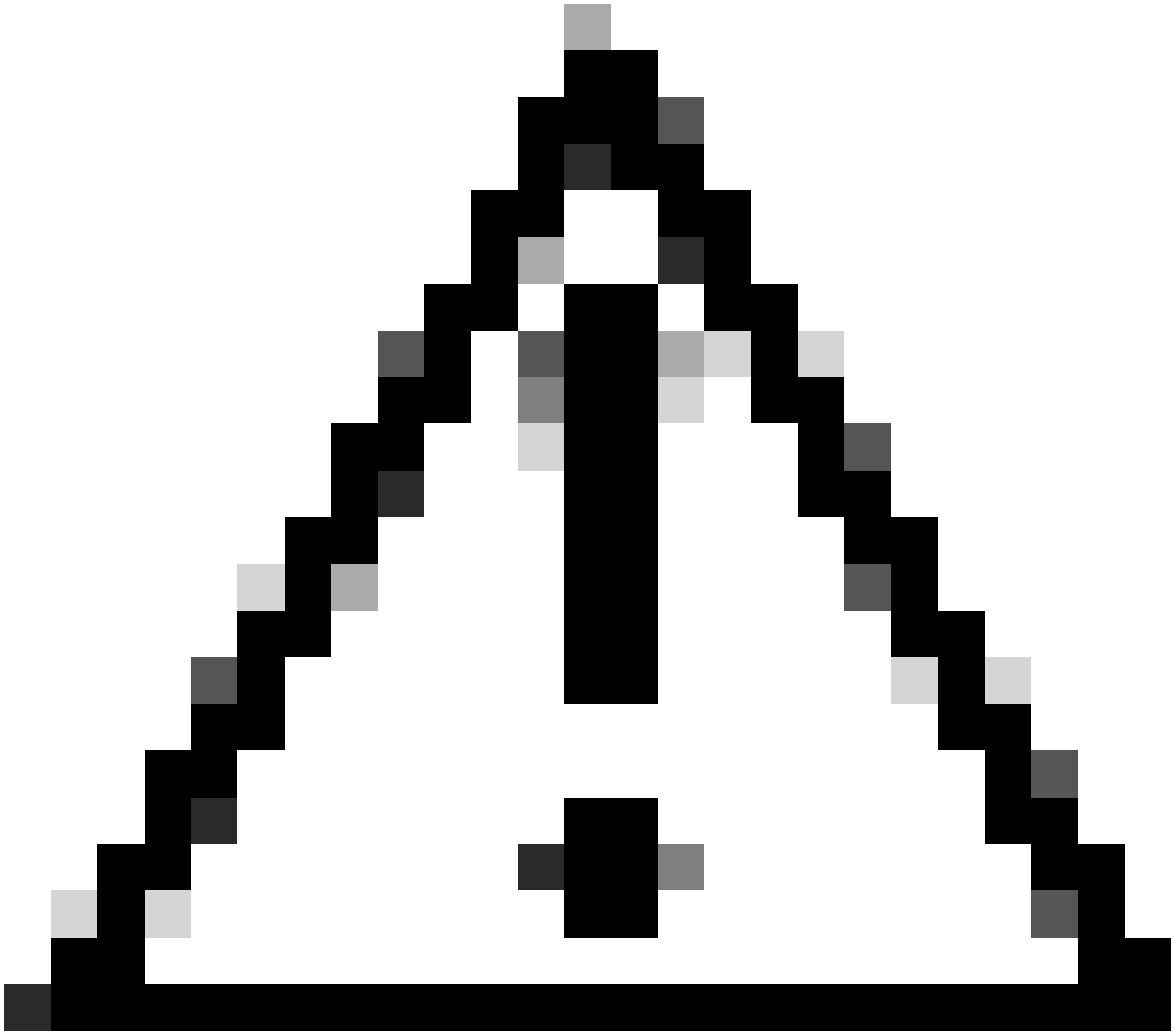


注：エンドポイントのGUIにアクセスするには、ブラウザを開き、URLバーにエンドポイントのIPアドレスを入力します。エンドポイントと同じネットワーク上に存在し、ログインするにはユーザクレデンシャルが必要です。

4つの方法すべてですべての設定を行えるわけではありません。このドキュメントのシナリオでは、SNMPモードは4つの方法すべてで有効にできますが、SNMP経由でデバイスと通信できるSNMPユーザを作成するには、エンドポイントにSSHで接続するか、Webex APIを使用するか、または「カスタマイズ」セクションの「開発者API」でエンドポイントのGUIを使用する必要があります。USMユーザは、エンドポイントのControl Hub All Configurationsセクションからは作成できません。



エンドポイントGUIのDeveloper APIセクション

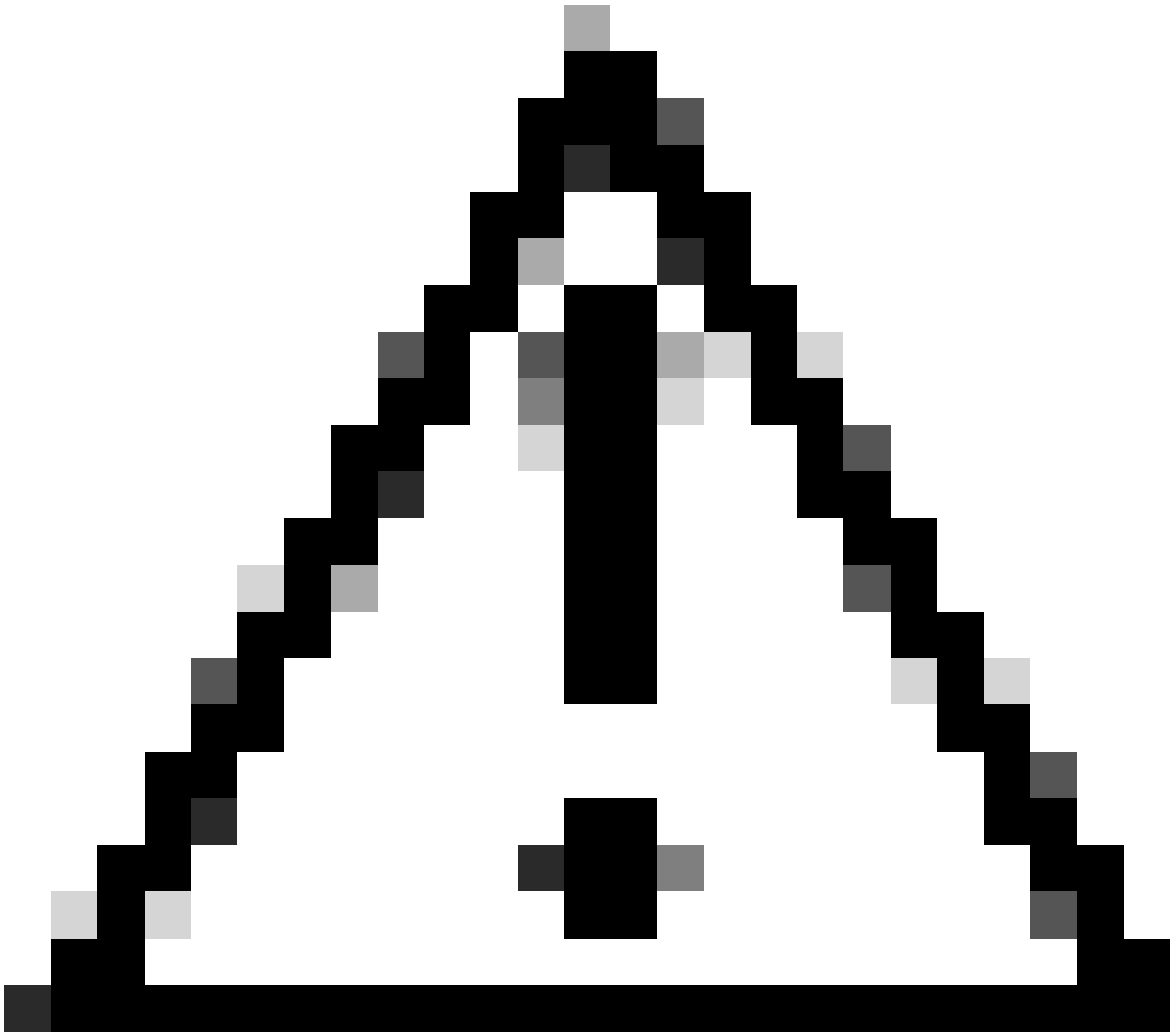


注意:「コマンドおよび構成の実行」テキスト・ボックスで発行したコマンドから結果が返されません。コマンドが正常に実行されたかどうかだけが表示されます。このため、USMユーザーを一覧表示するコマンドは、前のスクリーンショットに結果を返しません。これは、エンドポイントのGUIのこのセクションからUSMユーザを正常に作成できることを意味しますが、ユーザが作成されているかどうかを再確認するには、デバイスにSSHする必要があります。

SNMPv2cの設定では、ユーザを作成する必要はありません。認証は、エンドポイントで設定されたコミュニティ名（コミュニティストリングとも呼ばれる）を使用して行われます。デバイスにすでに存在するエンドポイントのSNMPエージェントが、デバイスに設定されているコミュニティ名と一致する要求に応答します。管理システムからのSNMP要求に一致するコミュニティ名（大文字と小文字が区別されます）が含まれていない場合、メッセージはドロップされ、ビデオデバイスのSNMPエージェントは応答を送信しません。

ただし、SNMPv3では、認証を成功させるためにUSMユーザの設定が必要です。この目的のために、Network SNMP USM Userコマンドを使用する必要があります。これは、デバイスに直接SSHを実行するか、Developer APIセクションのデバイスGUIを使用して実行できます。または、

Webex APIを使用することもできます。

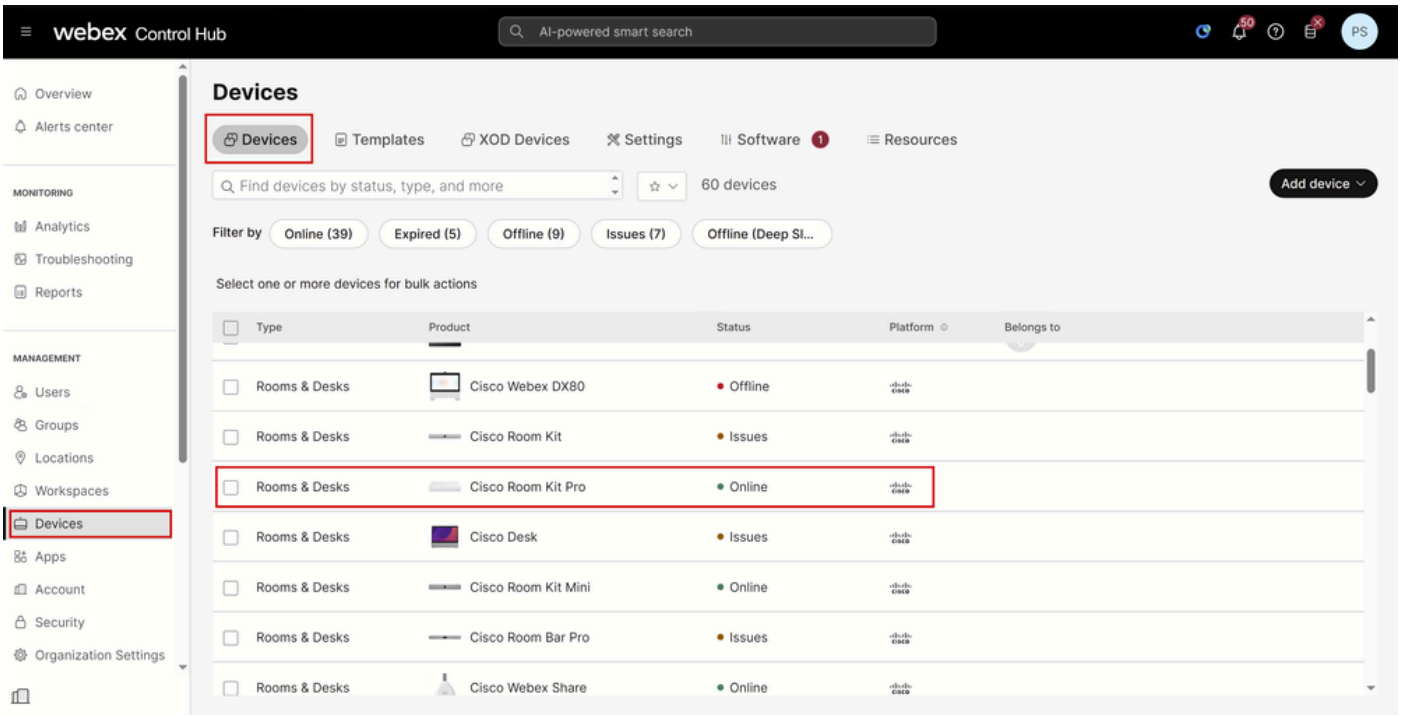


注意:SNMPv2、SNMPv3、またはその両方を有効にするかどうかを決定する必要があります。SNMPv1は、シスコのエンドポイントではサポートされていません。SNMPv1を使用しようとしても失敗します。

このドキュメントでは、SNMPv2プロトコルとSNMPv3プロトコルをイネーブルにしてControl Hubで設定しますが、SNMP3認証に必要なUSMユーザはSSHで設定します。

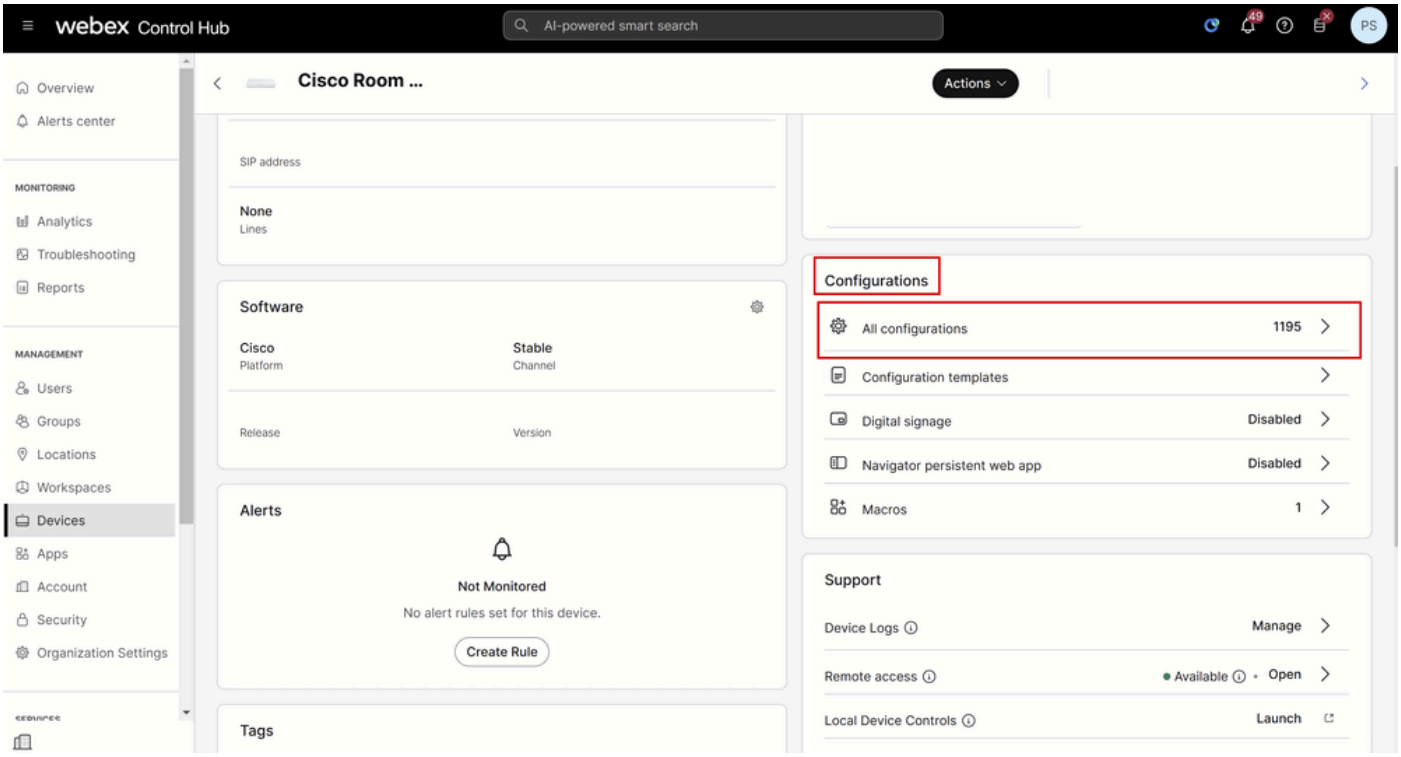
Control HubでのSNMPv2cモードの有効化

admin.webex.comに移動し、管理者クレデンシャルでログインします。フル管理者であることが推奨されます。ユーザインターフェイスの左側にあるManagementセクションの下のDevicesに移動します。Devicesタブで、設定するデバイスを選択します。この例では、Cisco Room Kit Proを使用します。



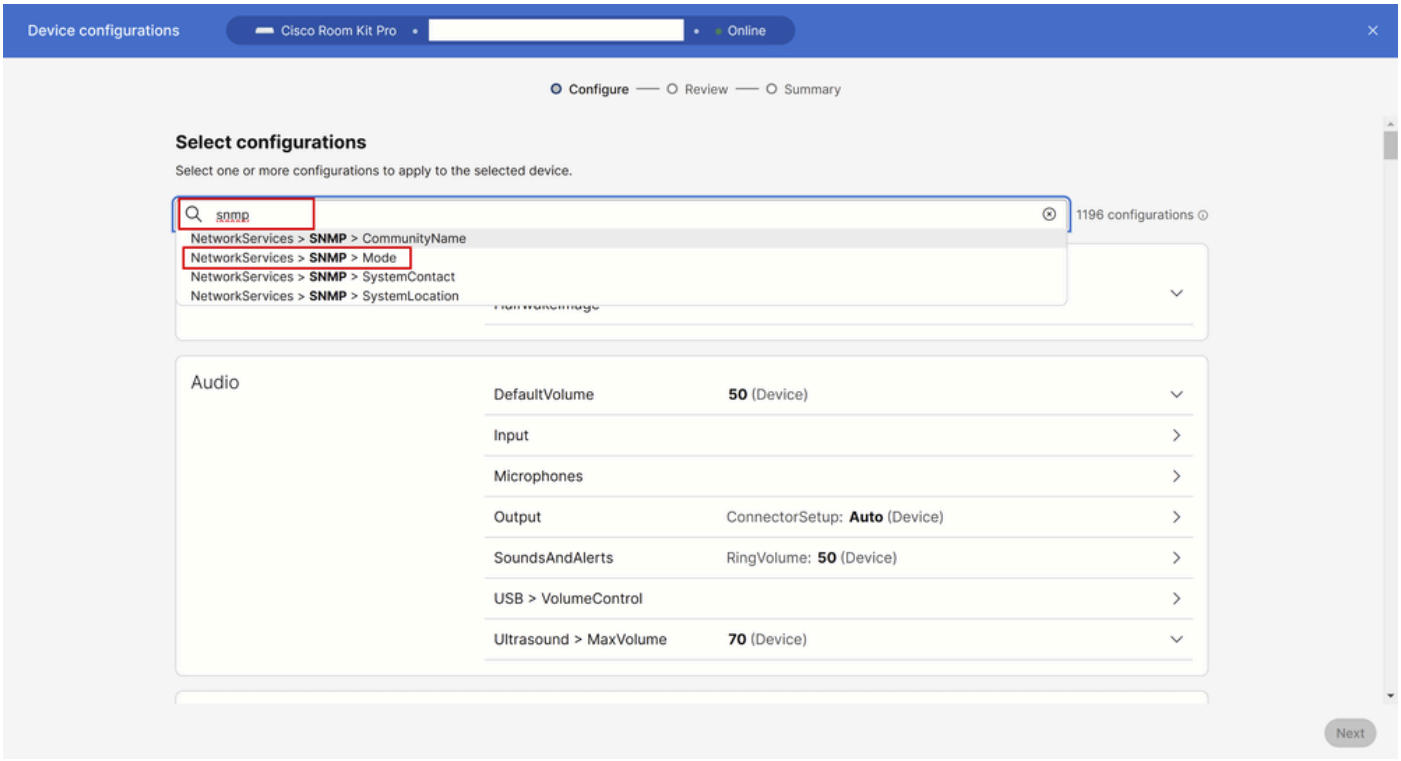
コントロールハブデバイスセクション

開いた新しいControl Hubページで、デバイスの詳細の下にあるConfigurationsセクションに移動して、All Configurationsをクリックします。



Room Kit Proのコントロールハブデバイスの詳細

検索バーでsnmpと入力し、NetworkServices > SNMP > Modeの順に選択します。

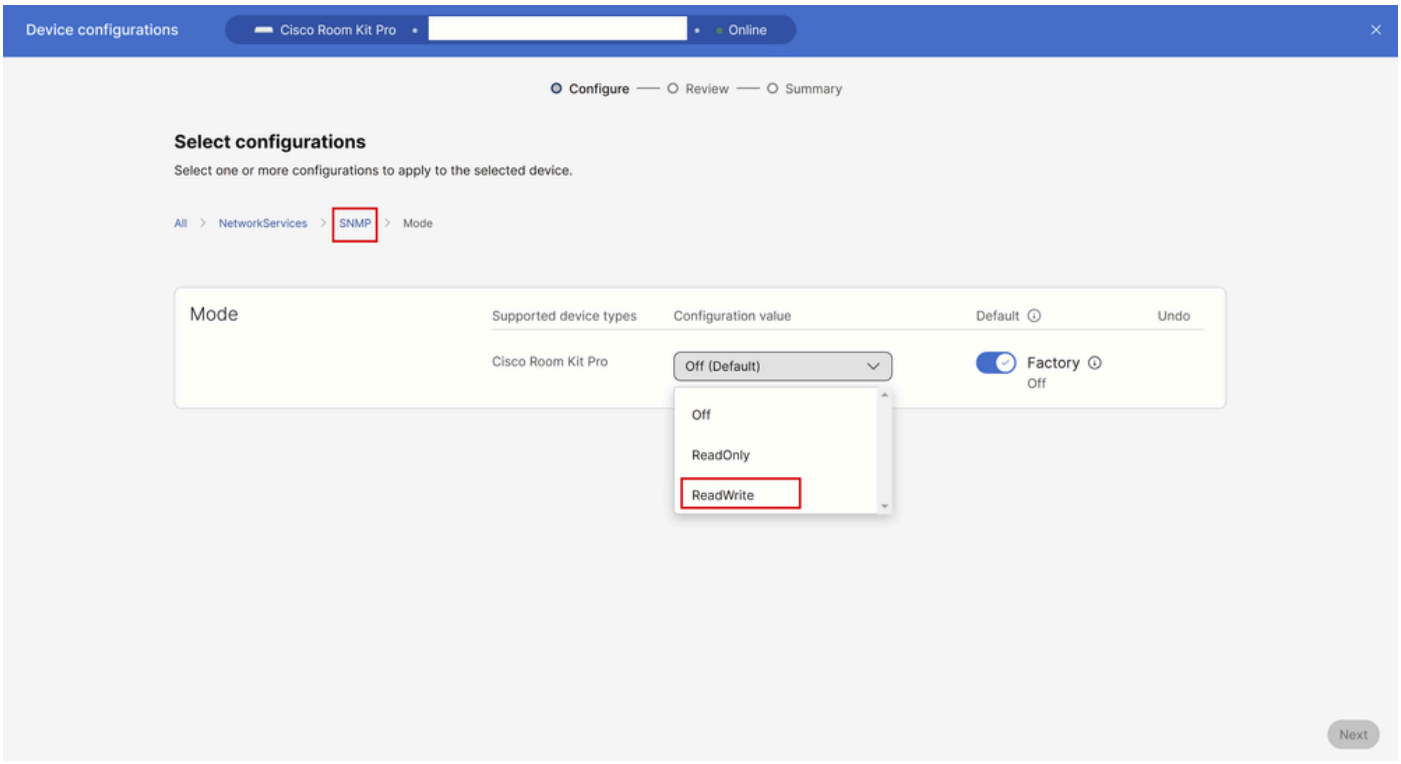


Control Hub All Configurationsウィンドウ

環境で有効にする必要があるモードを選択します。次の3つのオプションを使用できます。

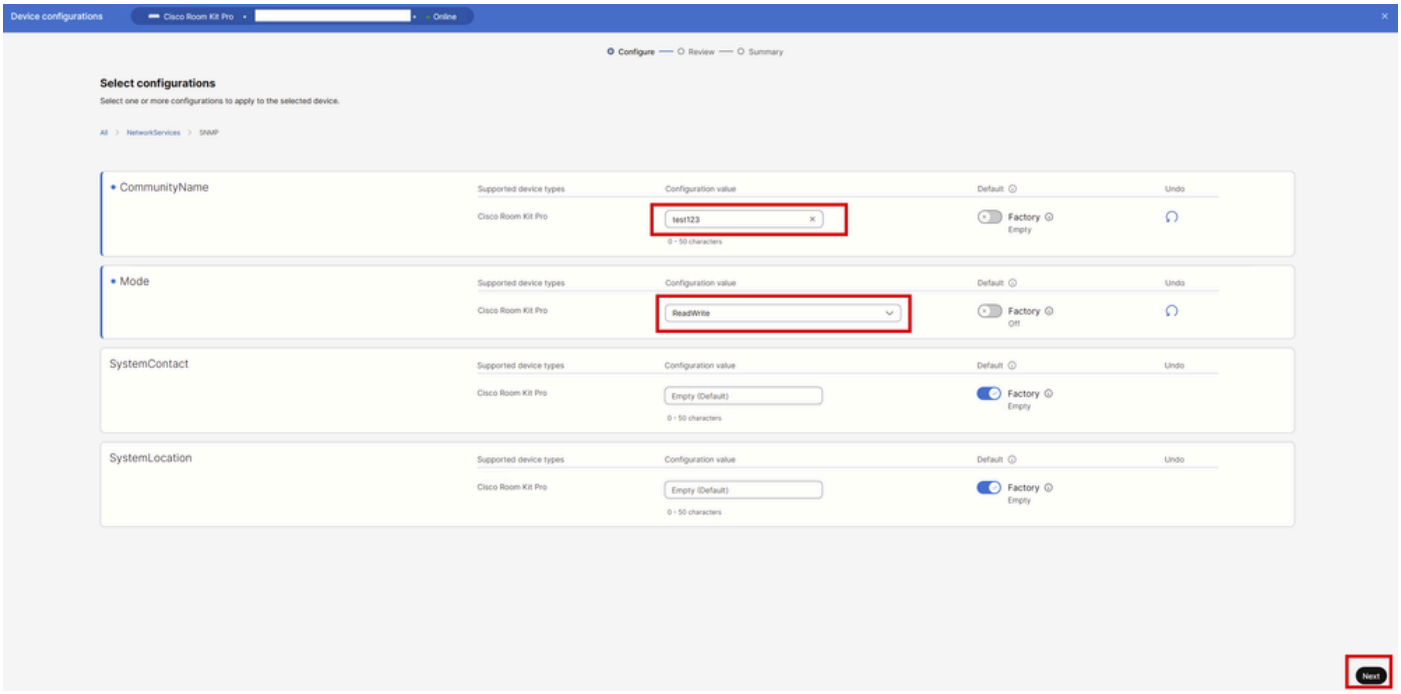
1. オフ：SNMPネットワークサービスを無効にします。
2. ReadOnly：クエリに対してのみSNMPネットワークサービスを有効にします。
3. ReadWrite：クエリとコマンドの両方に対してSNMPネットワークサービスを有効にします。

この例では、ReadWriteが選択されています。次に、図に示すように、設定ナビゲーションセクションでSNMPをクリックします。これにより、設定の1ステップに戻り、Control Hubを介してデバイスで設定できるすべてのSNMP関連の設定を確認できます。



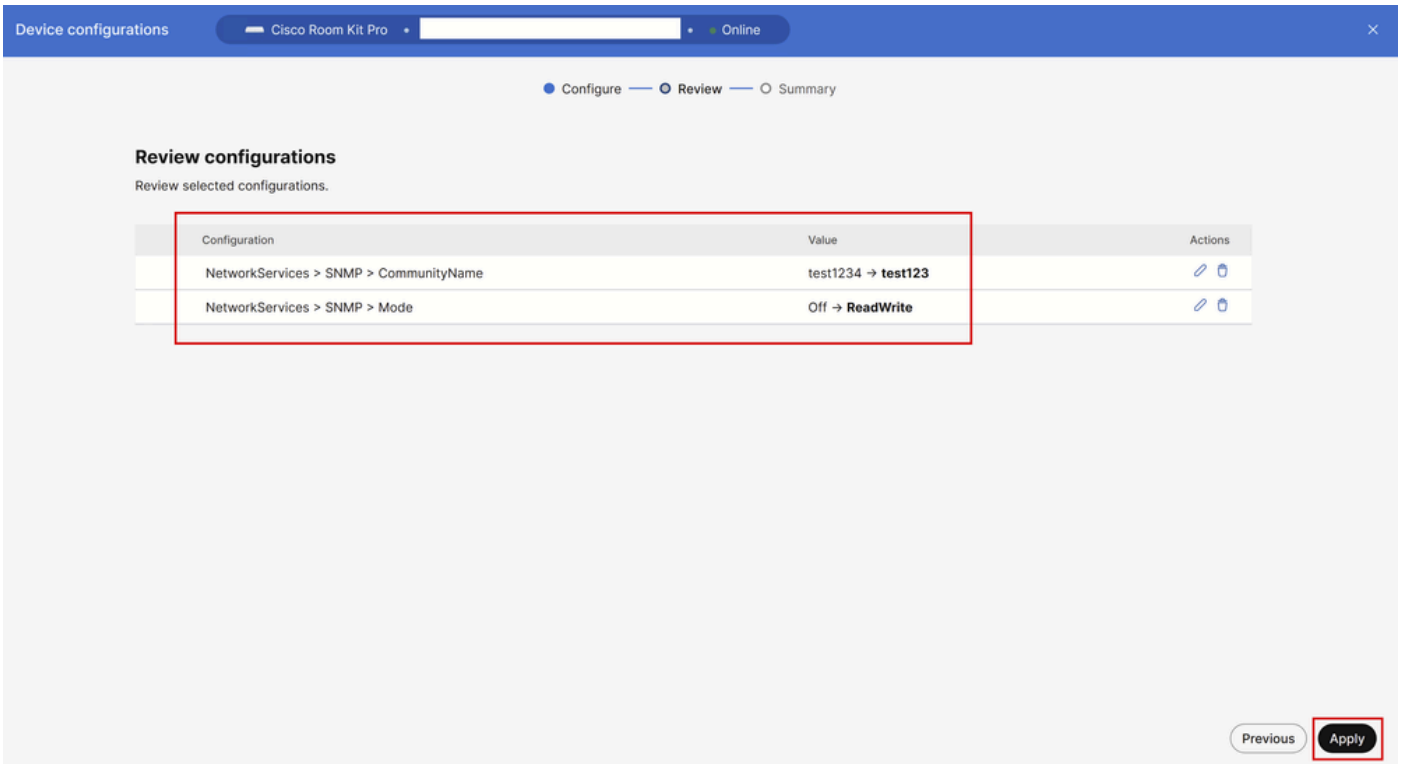
Control HubのAll ConfigurationsにおけるSNMPモードの設定

SNMPをクリックすると、次の図に示すように、使用可能なすべてのSNMPオプションが表示されます。SNMPv2を正常にセットアップするには、コミュニティ名をセットアップする必要があります。コミュニティ名は、SNMPサーバとエンドポイント上に存在するSNMPエージェント間の認証に使用されます。この例では、コミュニティ名はtest123に設定されています。右下隅のNextをクリックします。



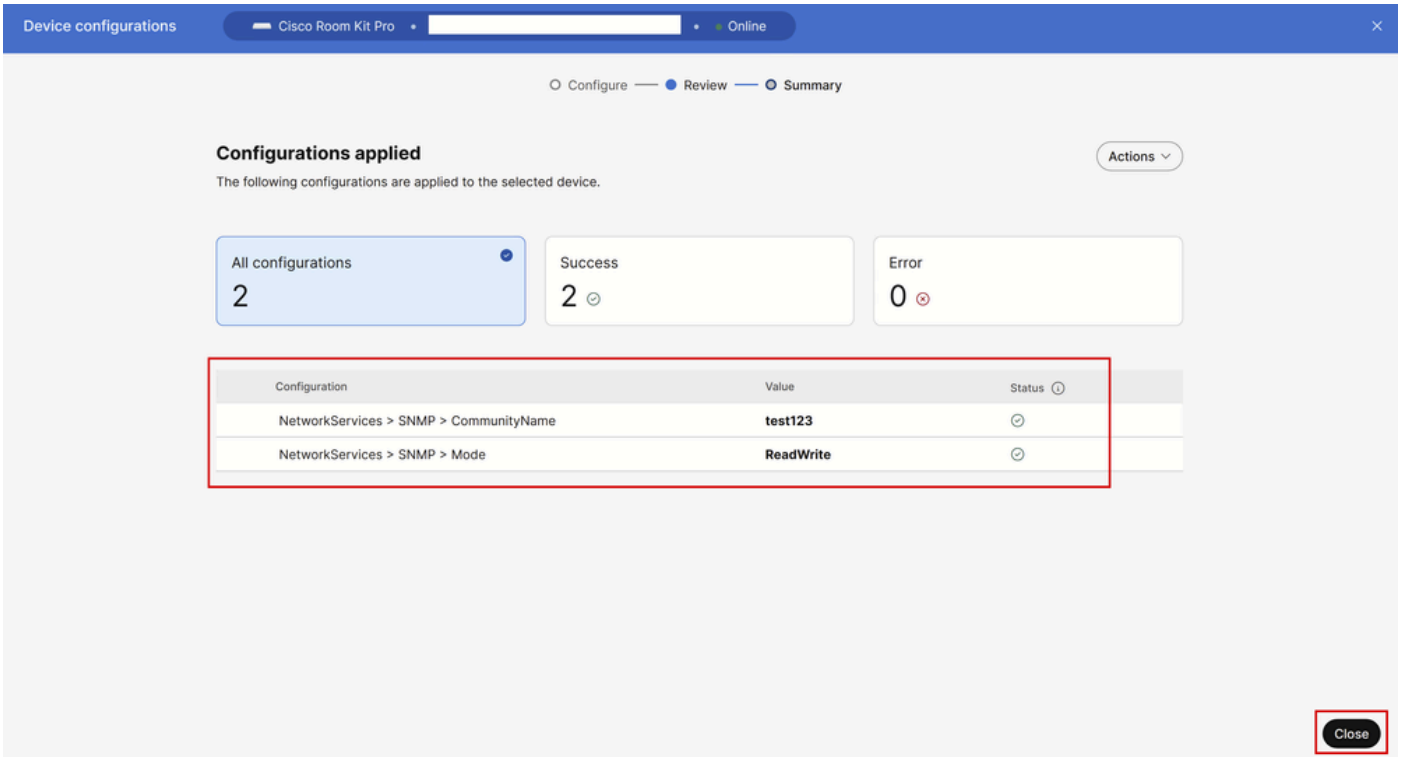
Control HubのAll ConfigurationsにおけるSNMP設定

デバイスの設定を確認し、右下隅にあるApplyをクリックします。



変更を適用する前に設定を確認する

設定変更が正常に適用されたことを確認します。次に、Closeをクリックします。



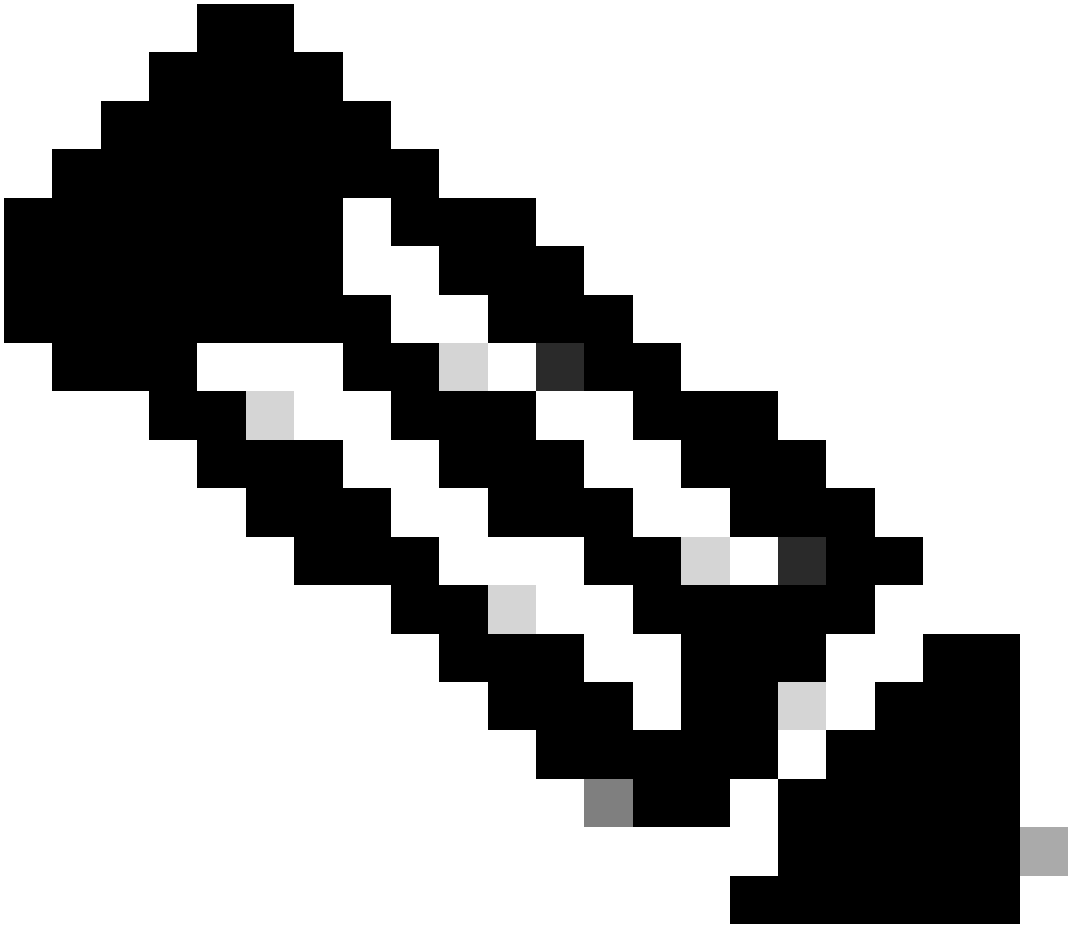
エンドポイント構成がControl Hubで正常に適用されました

この段階で、エンドポイントでSNMPv2cが正常に有効化され、コミュニティ名が設定されます。

Control HubでのSNMPv3モードの有効化

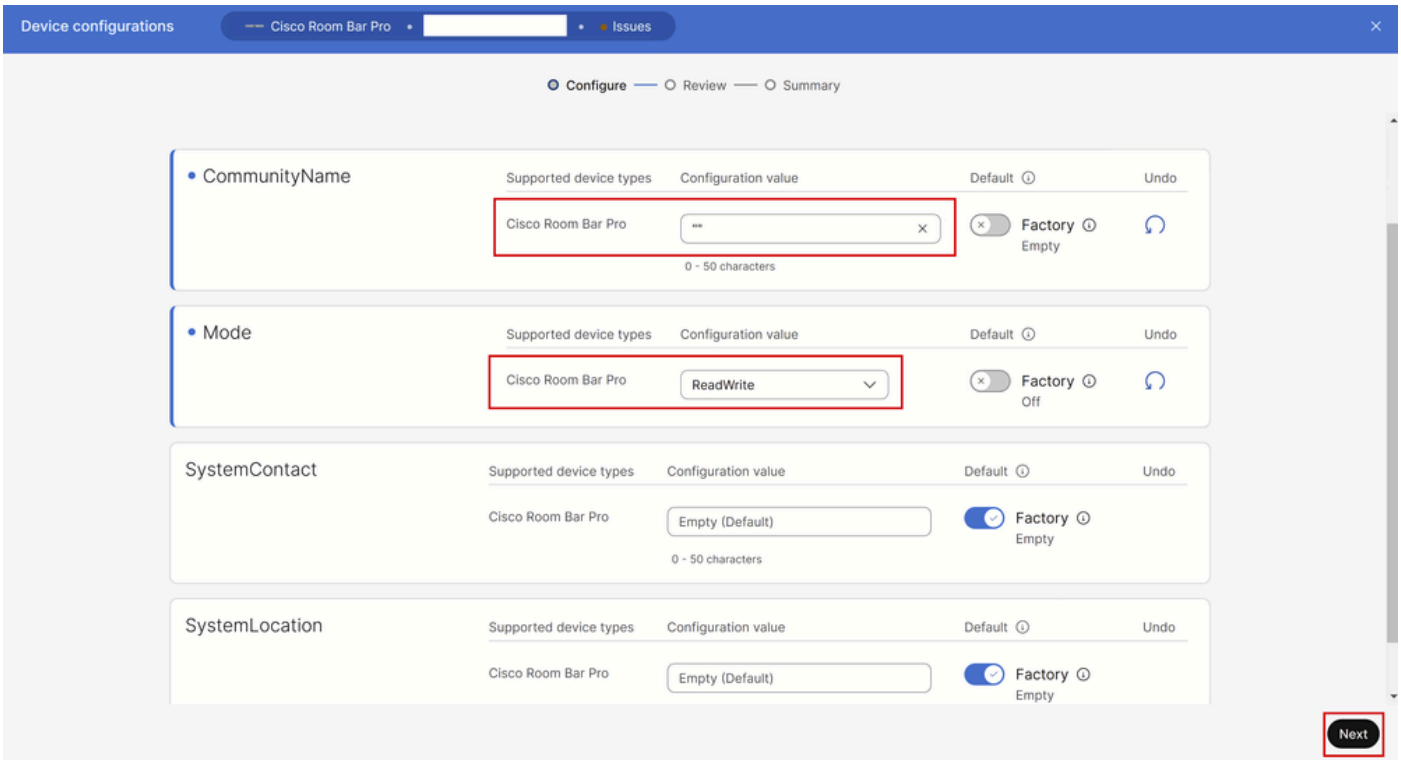
SNMPv3はSNMPv2cと比較してセキュリティが高く、エンドポイントに異なる設定が必要です。Control HubでManagementセクションの下にあるDevicesに移動します。Devicesタブの下に残り、SNMPv3を使用して設定するエンドポイントのいずれかを選択します。この例では、Cisco Room Bar Proを使用します。

デバイスの詳細の下で、Configurationsセクションに移動し、All Configurationsをクリックします。「デバイス設定」ページが開きます。検索バーにsnmpと入力し、NetworkServices > SNMP > Modeの順に選択します。この例では、SNMPモードはReadWriteに設定されます。SNMPをクリックすると、デバイス上の設定可能なSNMP設定がすべて表示されます。



注:SNMPv3に関してこれまで説明した手順はすべて、前の例でSNMPv2cを設定したときに説明されています。このため、手順のスクリーンショットは提供されません。Control Hub設定のナビゲート方法に疑問がある場合は、「Control HubでSNMPv2cモードを有効にする」の項を参照してください。

SNMPv3のみをサポートするには、コミュニティ名を引用符で囲まれた空の文字列として設定する必要があります。""。



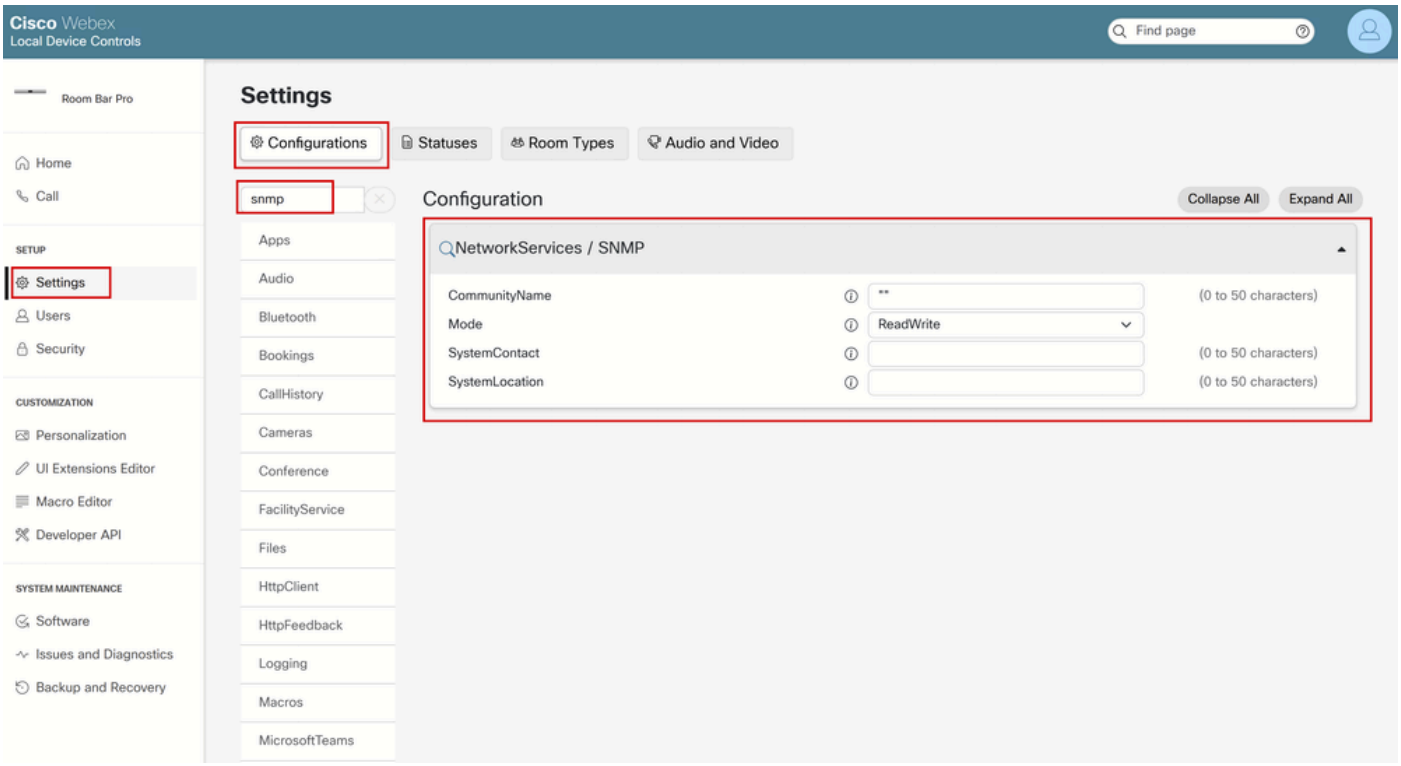
Control HubのAll ConfigurationsにおけるSNMP設定

Nextをクリックしてから設定の変更を確認し、Applyをクリックします。Closeをクリックして、デバイス設定ページを閉じます。

これで、Control Hubで実行できる設定は終了です。この段階では、SNMPv3だけが有効になっています。

エンドポイントGUIでのSNMP設定の表示

デバイスのGUIから同じ設定を実行できます。ブラウザタブを開き、エンドポイントのIPアドレスを入力します（エンドポイントと同じネットワーク内に存在する必要があります）。 管理者ユーザとしてログインし、エンドポイントのGUIで、SETUPセクションの下のSettingsに移動します。Configurationsタブにある設定の検索バーに、snmpと入力します。 次の図は、前のセクションのRoom Bar Proで実行したSNMPv3設定のSNMP設定の表示方法を示しています。



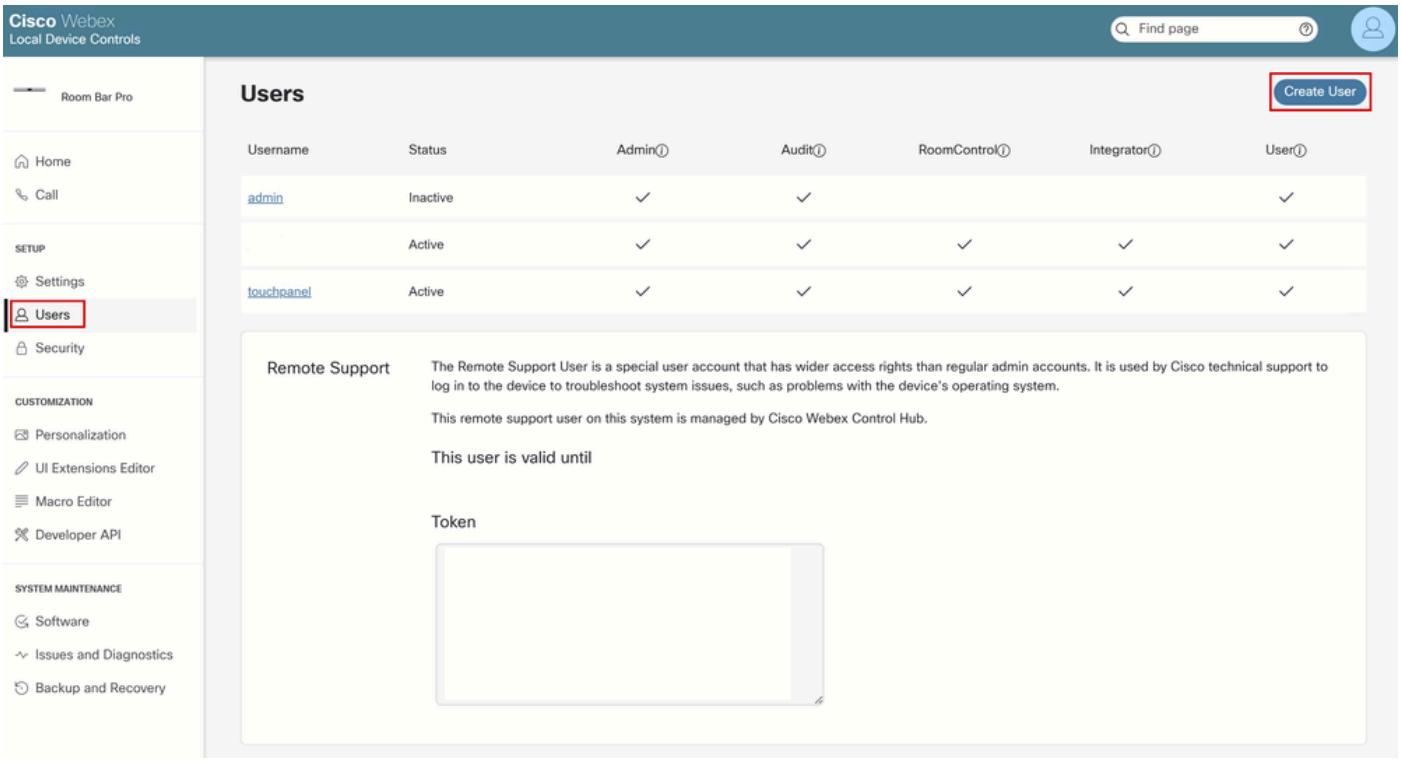
エンドポイントのGUIでのSNMPv3の設定

SNMPv3のUSMユーザの設定

SNMPv3を使用できるようにするには、USMユーザを作成する必要があります。このアクションを実行するために使用可能なコマンドは、ここにあるRoom OSのドキュメントのリンクで確認できます。 SSHを使用してデバイスに接続します。そのためには、デバイスにadminアカウントが必要です。そうでない場合は、管理者アカウントを作成する必要があります。 このセクションでは、このプロセス全体を説明します。

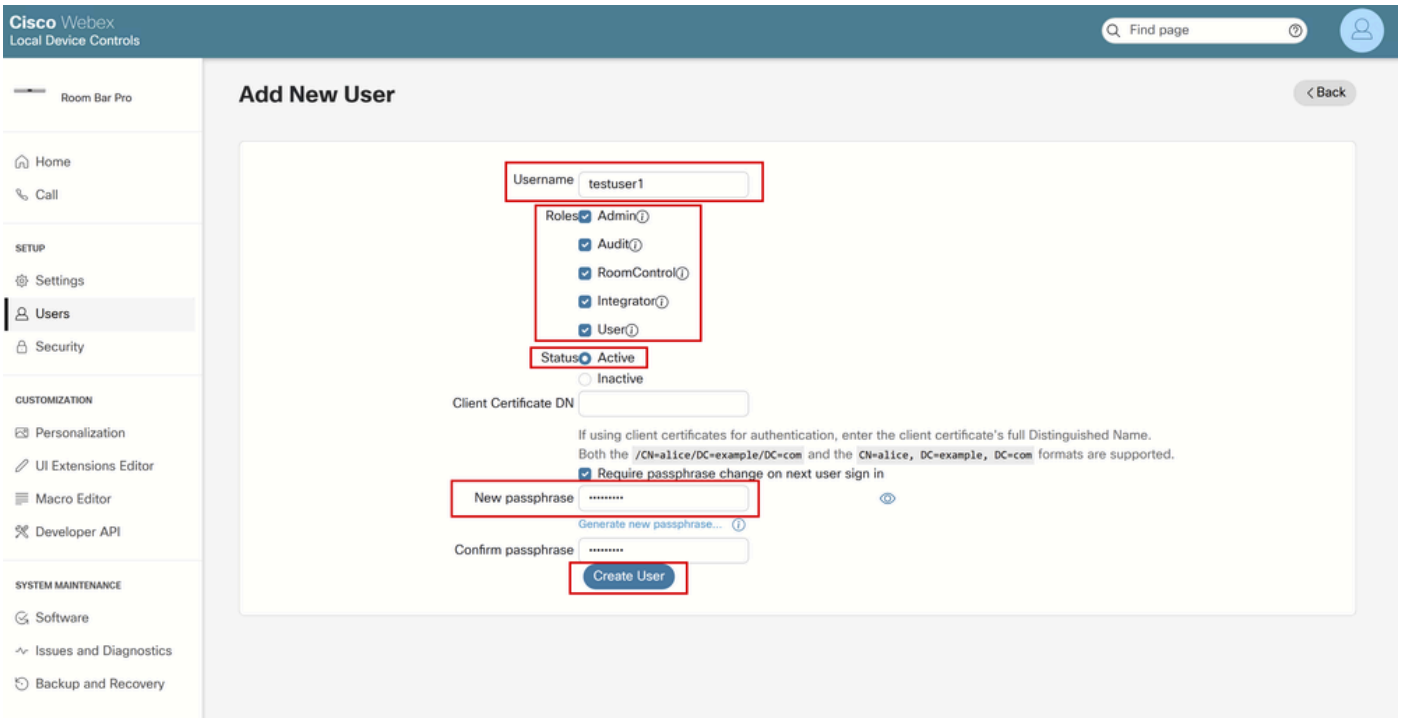
Control HubでManagementセクションの下にあるDevicesに移動します。Devicesタブの下に残り、管理者ユーザを作成するエンドポイントを1つ選択します。この例では、Cisco Room Bar Proを使用します。

デバイスの詳細の下で、Supportセクションに移動し、Local Device Controlsをクリックします（これが機能するには、エンドポイントと同じネットワーク内にある必要があります）。 デバイスのGUIが開きます。SETUPセクションにあるUsersに移動し、Create Userをクリックします。



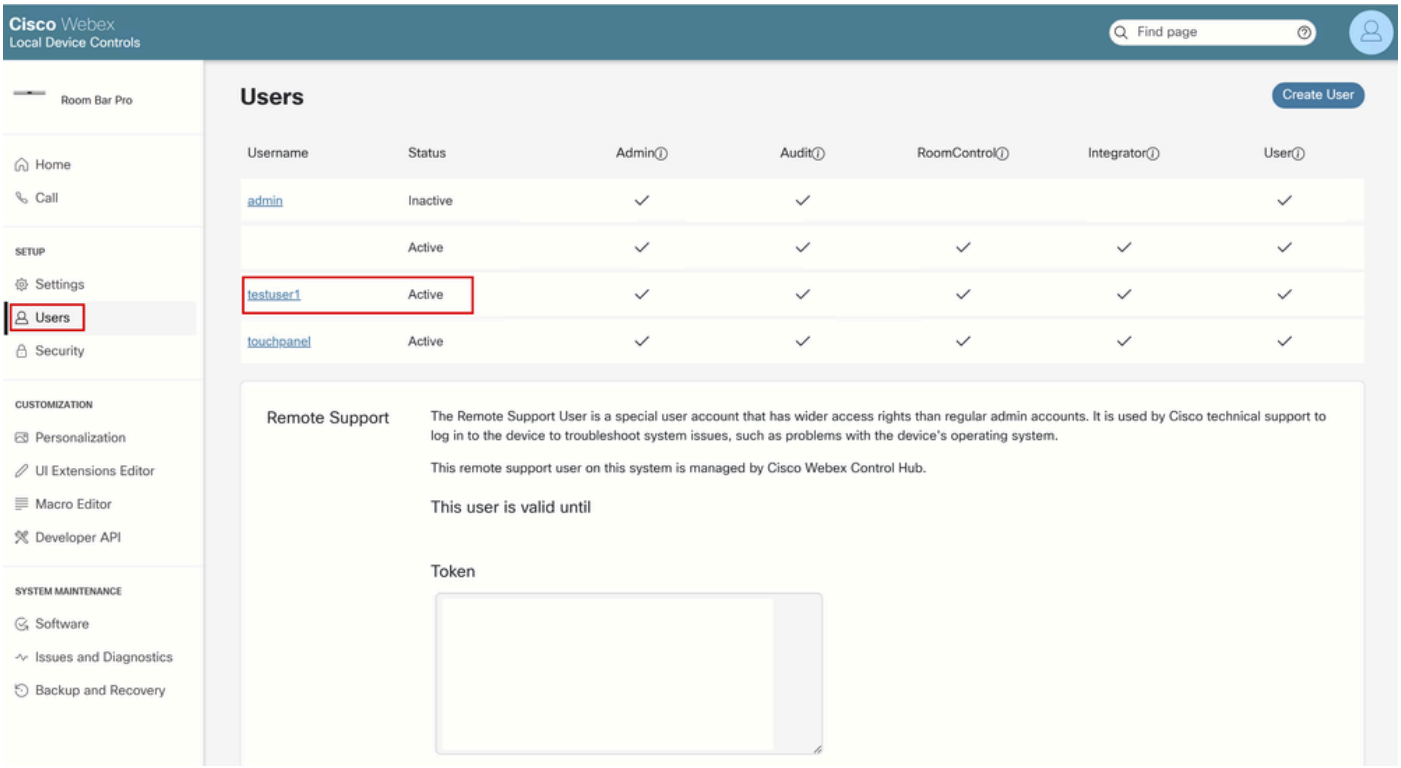
エンドポイントのGUIのUsersセクション

ユーザ名とパスフレーズ（パスワード）を入力します。 ユーザが完全な管理者権限を持ち、アクティブであることを確認します。

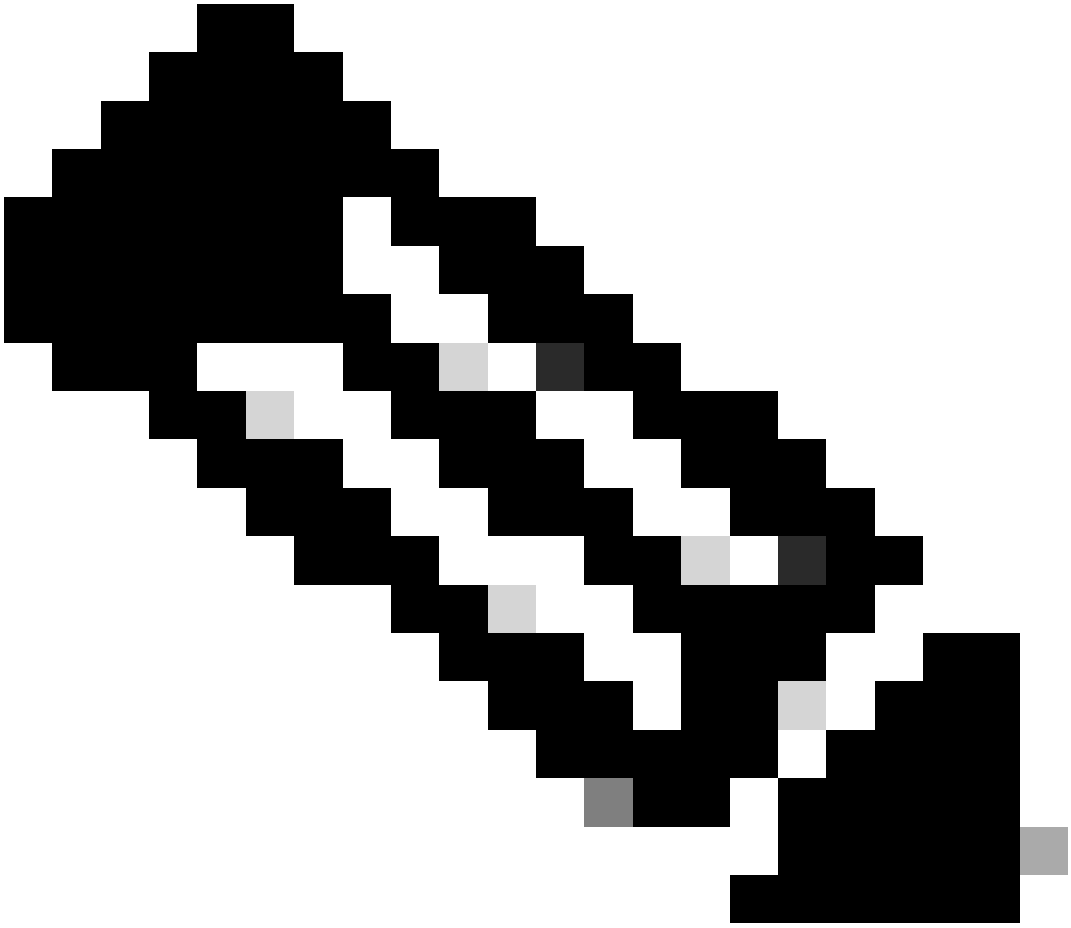


エンドポイントのGUIからのユーザの作成

ユーザが作成され、Usersページでアクティブになっていることを確認します。



新しいユーザが作成され、他のユーザの中にリストされる



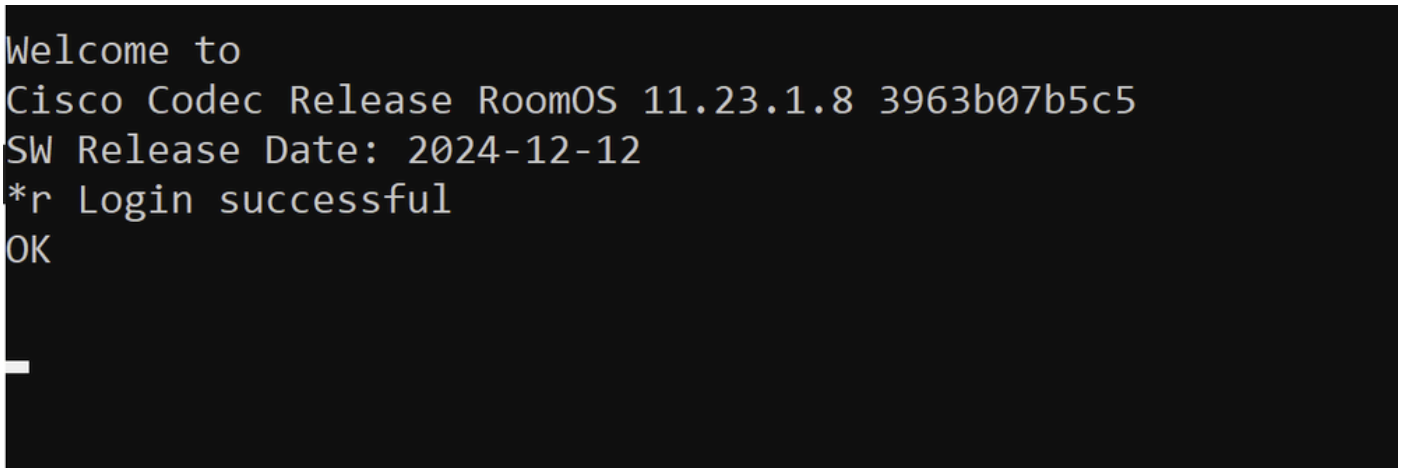
注：新しく作成したユーザに対して初めてSSHログインを試行すると、パスワードの変更を求められます。次のようなプロンプトが表示されます。

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

SSHを初めて使用する場合のパスワード変更

パスワードを変更するとすぐに切断されるため、新しいSSH接続を開始する必要があります。

管理者ユーザが正常に作成されたら、任意のSSHクライアントを使用してエンドポイントに接続します。管理者クレデンシャルでログインします。次のプロンプトが表示されます。



SSHを介したエンドポイントへのログイン試行の成功

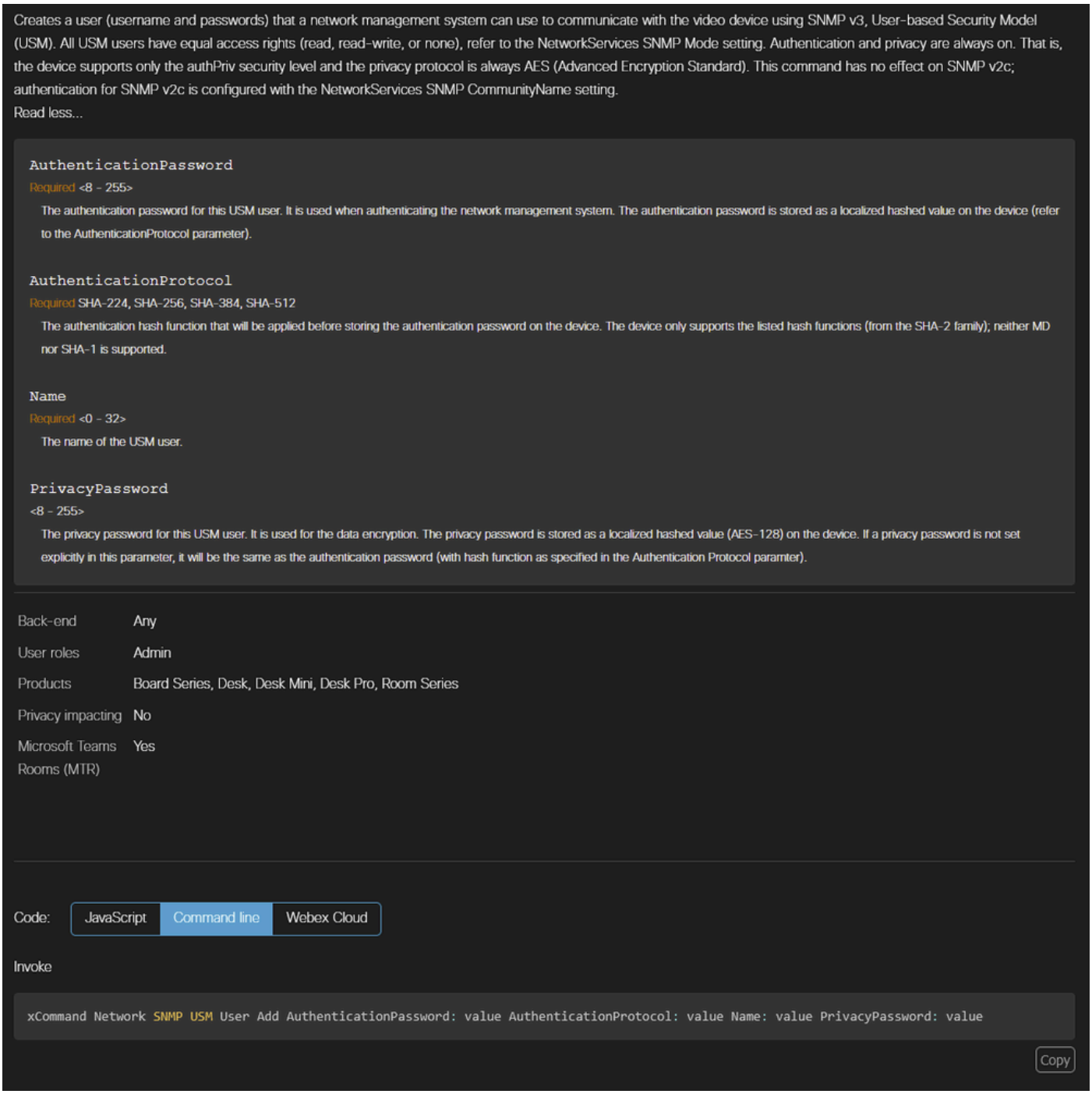
この記事の説明に従って、Network SNMP USM User Addコマンドを使用します。このデモンストレーションで使用するコマンドは次のとおりです。

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

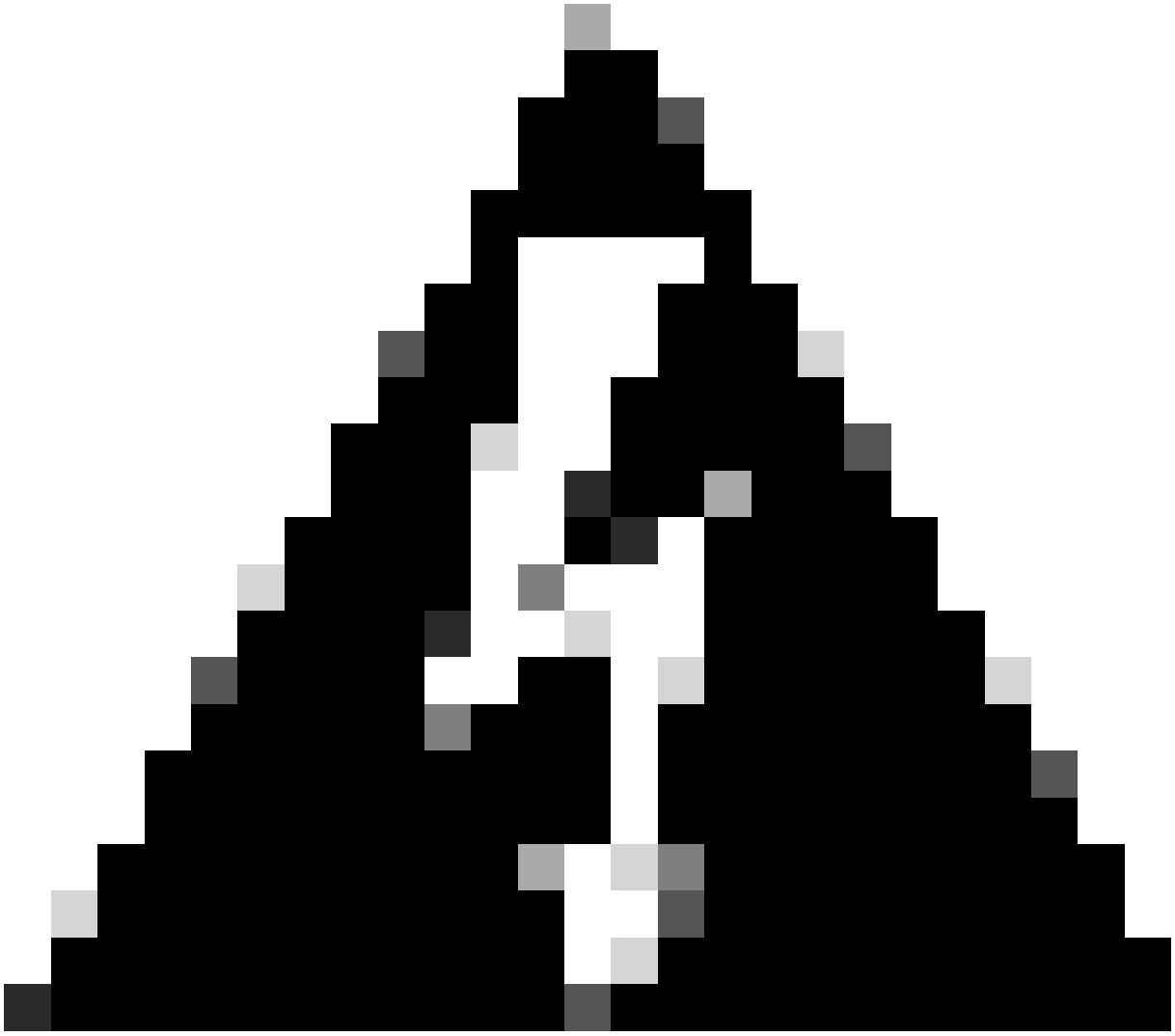
このコマンドが成功した場合、結果は次のようになります。

SSHを介したUSMユーザ作成

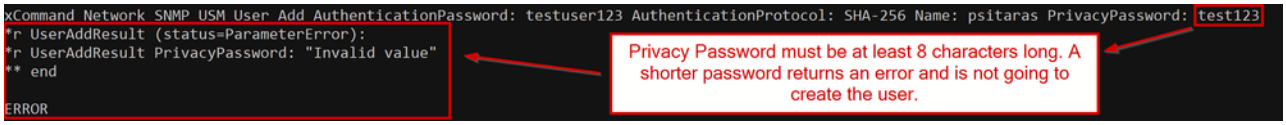
コマンドをエラーなしで実行するには、このリンクで共有されているコマンドドキュメントに記載されている特定のルールに従う必要があります。便宜上、このコマンドに関するこのドキュメントの作成時点での現在の要件はこの図に貼り付けられていますが、ユーザを作成する際には必ずこのリンクを参照してください。図の最後に、コマンドの正確な構文があることに注意してください。



xAPIドキュメントからのUSMユーザー作成コマンド構文



警告：入力ミスがあるか、要件が満たされていない場合、コマンドはエラーを返し、ユーザは作成されません。8文字以上のプライバシーパスワードを入力する代わりに、7文字以上の短いパスワードを入力する例を示します。



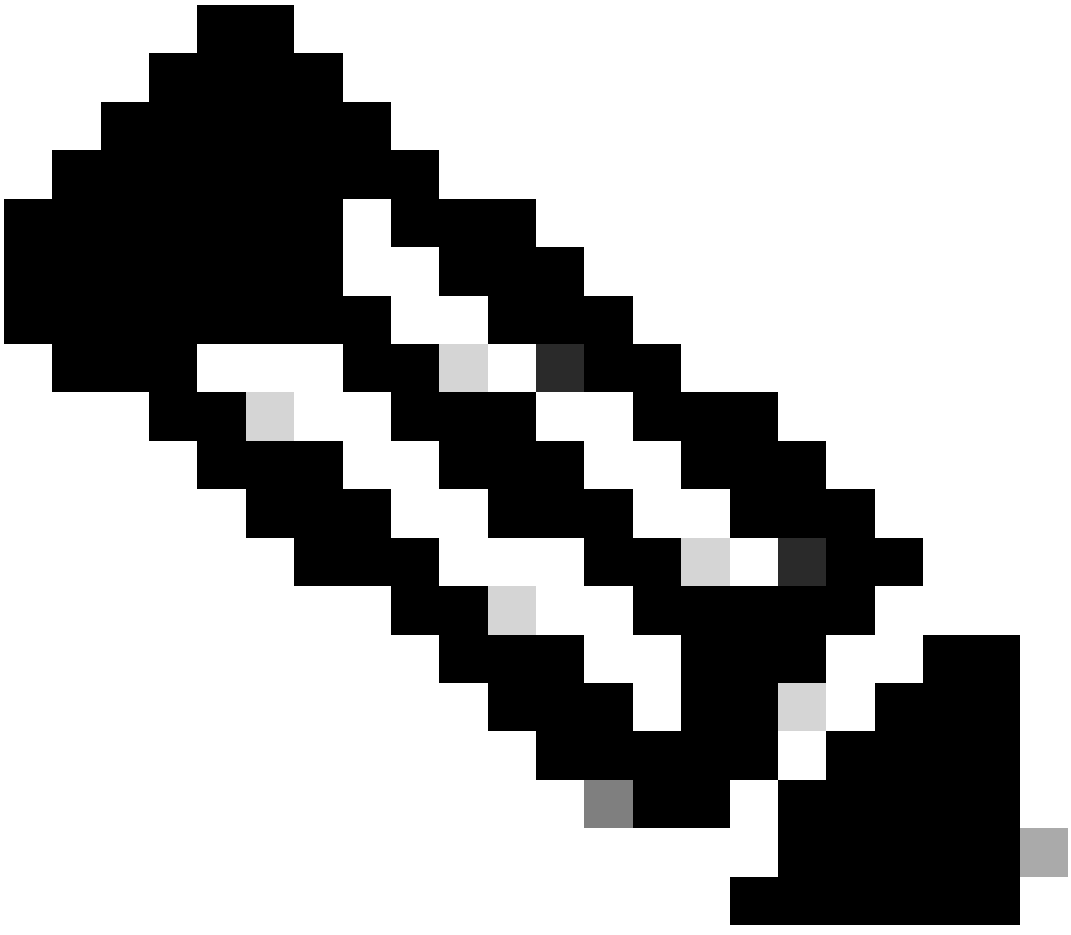
プライバシーパスワードが短いため、USMユーザーの作成に失敗しました

ユーザが作成されたかどうかをテストするには、Network SNMP USM User Listコマンドを使用します。このコマンドは、デバイスに保存されているすべてのUSMユーザを一覧表示します。

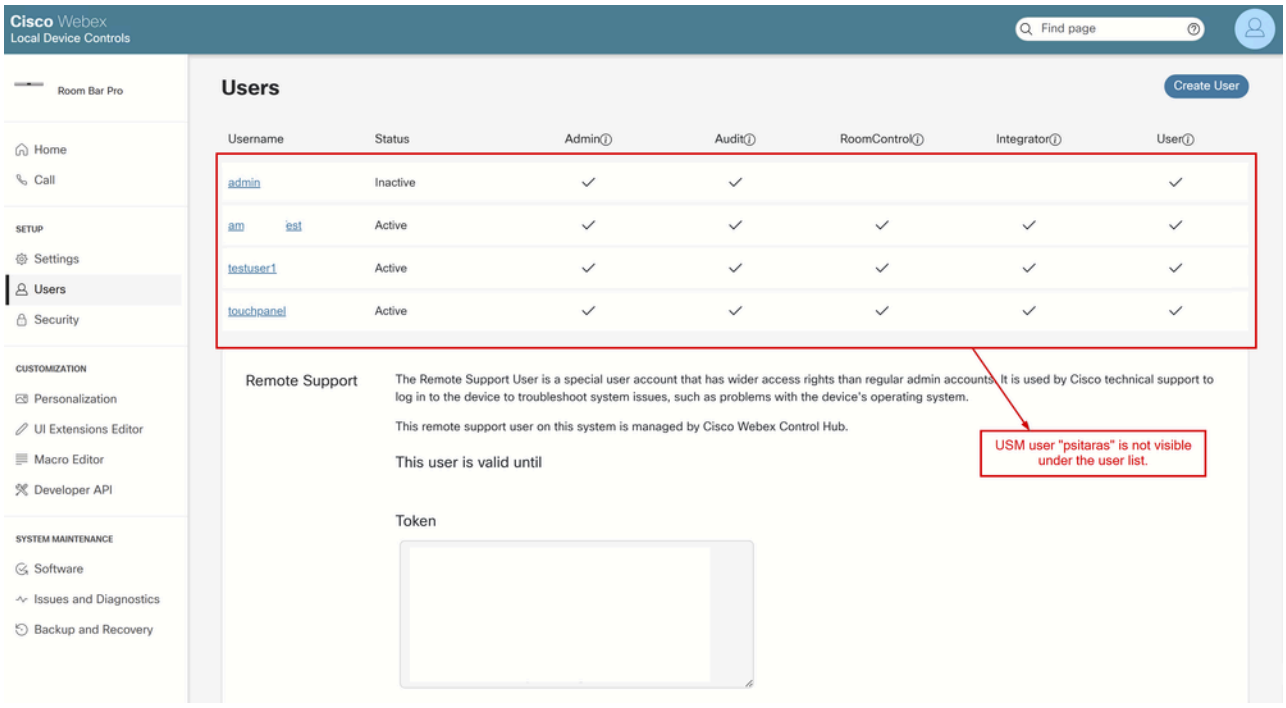
```
xCommand Network SNMP USM User List

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

Network SNMP USM User Listコマンドを使用したユーザ作成の確認

この段階で、ユーザーpsitarasが正常に作成されたことが確認されました。SNMPv3の設定が完了しました。



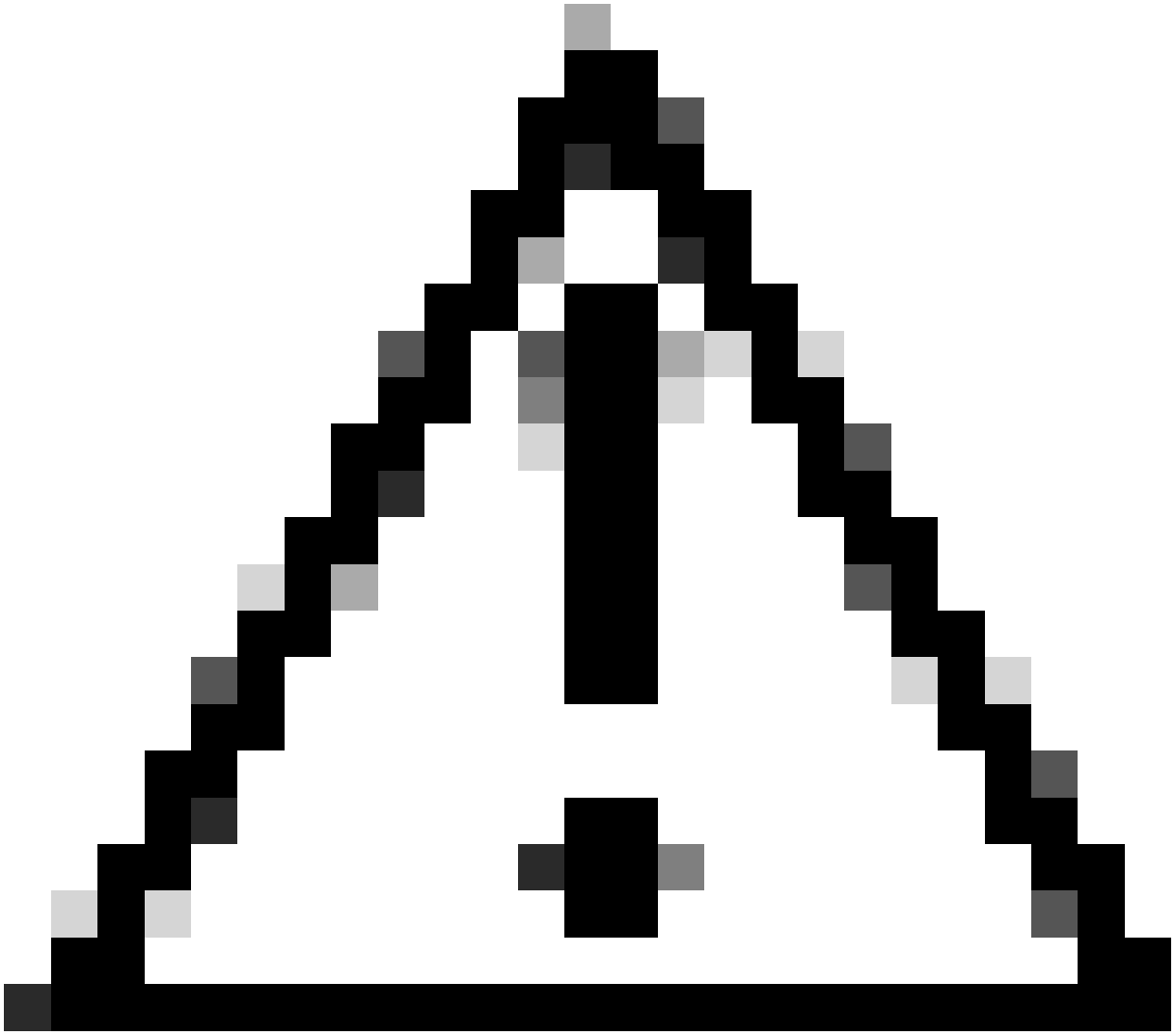
注:USMユーザpsitarasは、エンドポイントのGUIのUsersセクションには表示されません。これは予想どおりの結果です。



USMユーザがエンドポイントのGUIのユーザの下に表示されない

SNMPv2cおよびSNMPv3設定のテスト

この段階で、ネットワーク管理システム(NMS)を使用したSNMPv2cやSNMPv3の設定のテストに進むことができます。 この記事のラボ設定には、SNMPサービスを実行するNMSサーバやSNMPサーバは含まれていません。設定をテストするには、snmpwalkというユーティリティを使用します。このユーティリティはLinuxサーバにインストールされます。



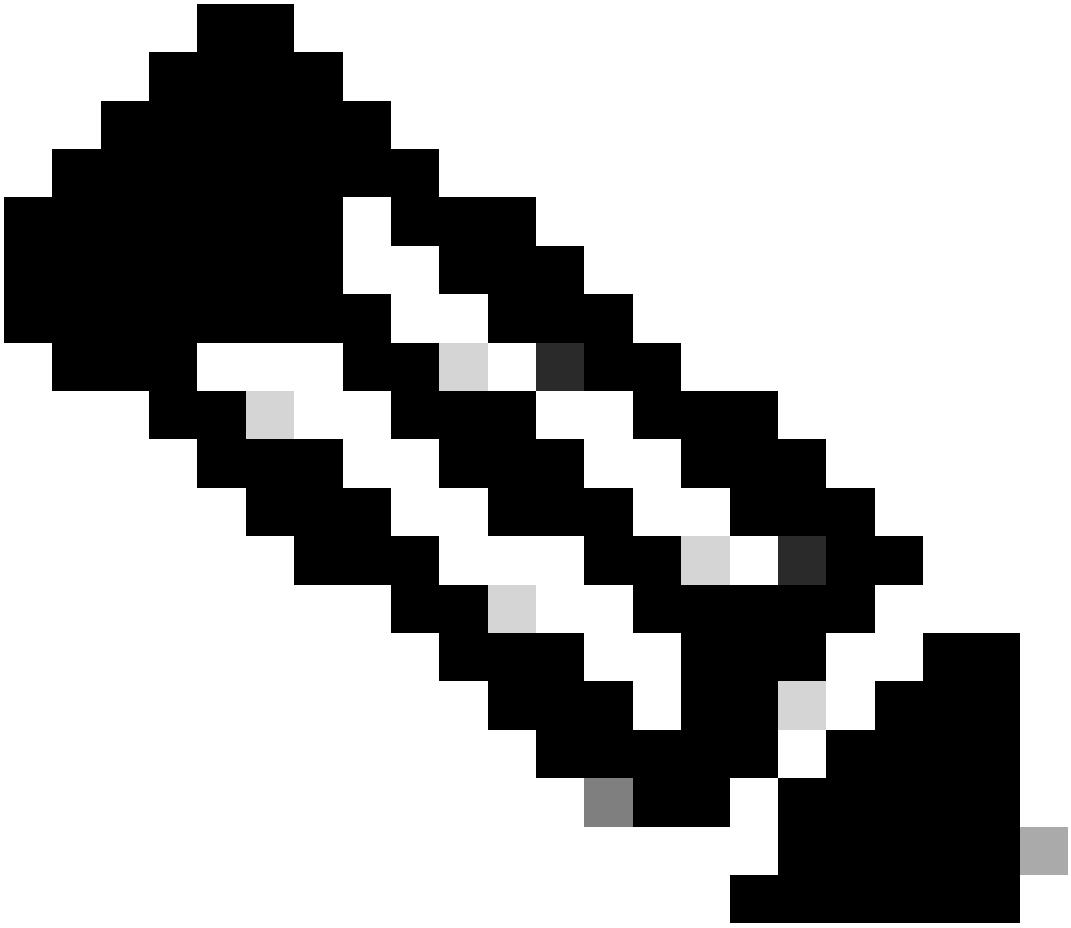
注意:Snmpwalkは、コラボレーションエンドポイントでSNMP設定をテストするための推奨ツールではありません。TACエンジニアはこのツールをサポートしていないため、テストに進む前にツールの使用方法に精通している必要があります。snmpwalkの代わりに、他の任意のSNMPツールまたはNMSを使用して設定をテストできます。この記事では、snmpwalkを例として使用しています（デモ用に設定をテストするにはツールが必要です）。このツールの使用に関する確約やプロモーションはありません。

snmpwalkのインストールはこのガイドには含まれておらず、省略されています。テストに使用するマシンのオペレーティングシステム(OS)によっては、インストール要件が異なる場合があります。テストを行う前に、正しくインストールできるように作業する必要があります。

Snmpwalkは、SNMP設定の確認に使用できるツールです。エンドポイントのMiBをウォークスルーし、利用可能な情報を返すクラウド登録エンドポイントは、次の7つのオブジェクト識別子(OID)を公開します。

- SNMPv2-MIB::sysDescr（読み取り）、

- SNMPv2 -MIB::sysObjectID（読み取り）、
- DISMAN-EVENT-MIB::sysUpTimeInstance（読み取り）、
- SNMPv2 -MIB::sysContact（読み取り/書き込み）、
- SNMPv2 -MIB::sysName（読み取り/書き込み）、
- SNMPv2 -MIB::sysLocation（読み取り/書き込み）、
- SNMPv2 -MIB::sysServices（読み取り）。



注：上記のsnmpwalkテストに使用される内部IPはプライベートIPであり、現在は使用されていません。このガイドで使用されているラボは廃止され、デバイスは工場出荷時の状態にリセットされています。

Cisco Room Kit ProエンドポイントはSNMPv2cで設定されます。認証はコミュニティストリングを使用して行われます。次のコマンドを発行します。

```
# '-c' option is used to provide the community string
# '-v' option is used to provide the SNMP version used
```

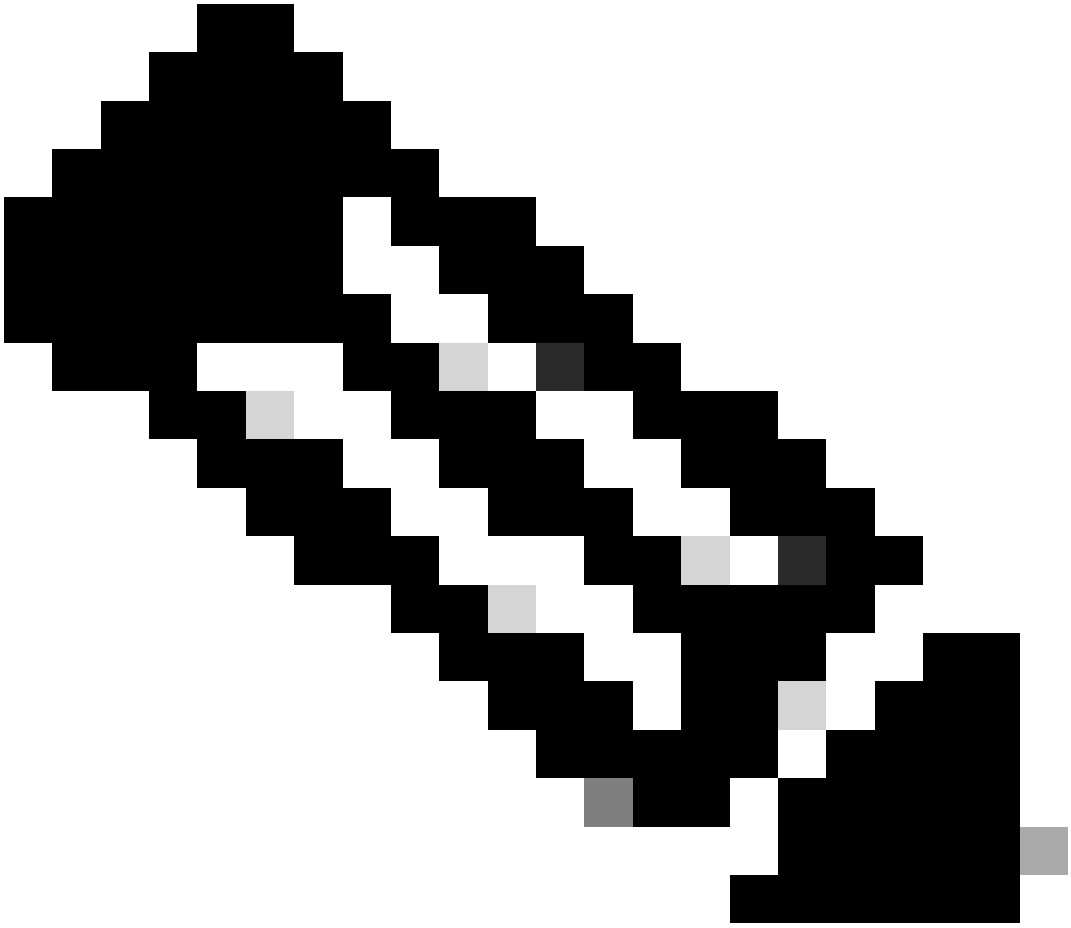
```
# The IP provided is the endpoint's IP

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は、期待どおりに7つの結果を返します。空のMiBが3つあります。

1. SNMPv2 -MIB::sysContact (読み取り/書き込み ）、(iso.3.6.1.2.1.1.4.0)
2. SNMPv2 -MIB::sysName (読み取り/書き込み ）、(iso.3.6.1.2.1.1.5.0)
3. SNMPv2 -MIB::sysLocation (読み取り/書き込み ）、(iso.3.6.1.2.1.1.6.0)

これらのMiBに値を設定するために使用できるxConfigurationコマンドは3つあります。エンドポイントにSSHで接続し、次のコマンドを発行します。

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



注：この3つのコマンドを使用する代わりに、Control Hub、エンドポイントGUI、またはWebex APIから、これらの設定の変更を実行できます。

上記のコマンドを発行したら、同じエンドポイントでsnmpwalkを再度使用します。先ほど空だったMiBには、xConfigurationコマンドで指定された値が入力されています。

```
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)
```

この段階で、Room Kit Proデバイス上で作成されたSNMPv2c設定が動作していることが確認されます。

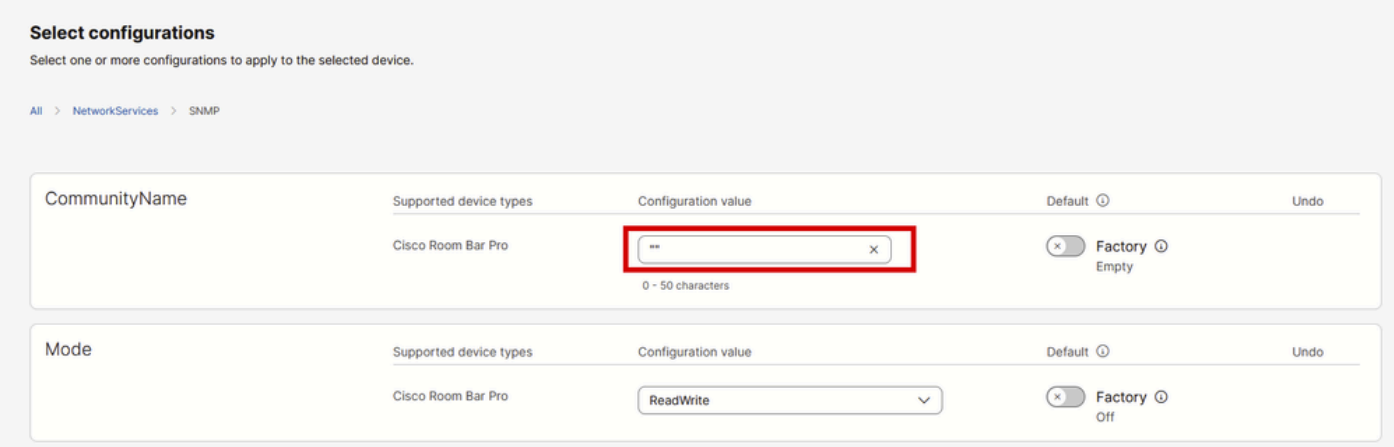
Cisco Room Bar ProエンドポイントはSNMPv3で設定されます。SNMPv3では、適切な認証を使用していることを確認する必要があります。コミュニティストリングは使用されません。代わりに、SNMPv3はユーザ名とパスワードを使用します。

```
# '-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)
```

この段階で、Room Bar Proデバイス上で作成されたSNMPv3設定が動作していることが確認されます。

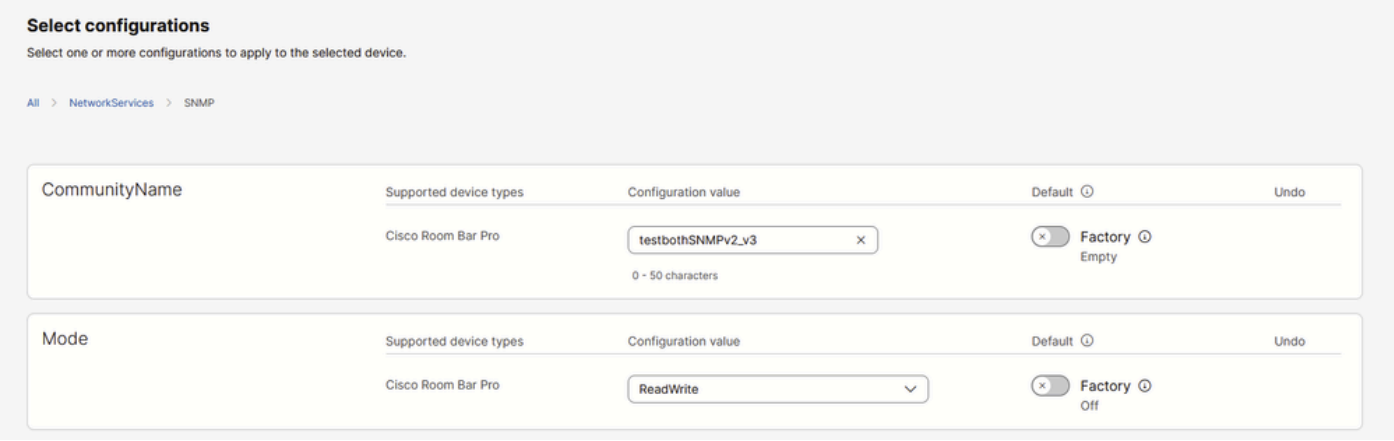
1つのエンドポイントでSNMPv2cとSNMPv3の両方を同時にアクティブにできる

はい、できます。ただし、SNMPの設定時に、SNMPv2c認証を使用できるようにするには、コミュニティ名を設定する必要があります。このテストでは、前の例のRoom Bar Proを使用します。エンドポイントのControl Hub All Configurationsセクションの現在の設定は次のとおりです。



Control HubでのエンドポイントSNMPの設定

コミュニティ名が空ではないことに注意してください。引用符は2つあり、コミュニティ名が空の文字列であることを示します。NetworkServices SNMP CommunityNameを空の文字列("")に設定することにより、SNMPサポートをバージョン3だけに制限できます。 この文字列を、testbothSNMPv2_v3などのコミュニティ名に置き換える必要があります。



Control Hubエンドポイントの構成設定でのSNMPv2cのコミュニティ名の追加

SNMPv3がRoom Bar Proで動作していることはすでに確認されています。コミュニティ名を設定した後、SNMPv2cが機能しているかどうかをテストするためにsnmpwalkが使用されます。

```
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)
```

SNMPを使用してControl Hub経由で複数のエンドポイントを設定可能

はい。Control Hubでは、複数のデバイスを一度に設定できます。この記事では、「複数のデバイスの設定」セクションで手順を追って実行する方法について説明します。

重要な詳細情報

- 特定のMiBのみを使用できます。使用可能なMiBの数は、エンドポイントを設計するエンジニアリングチームの設計によって制限されます。MiBを拡張して詳細情報を提供することはできません。
- SNMPv2cはコミュニティ名（コミュニティストリングとも呼ばれる）を使用して認証しますが、SNMPv3はユーザ名とパスワードを使用して認証し、暗号化も提供します。テスト時には、設定したプロトコルに対して正しい認証方式（snmpwalkまたは別のツール/NMSを使用）を使用していることを確認します。
- SNMPv3では、認証とプライバシーが常にオンになっています。エンドポイントはauthPrivセキュリティレベルのみをサポートし、プライバシープロトコルは常にAdvanced Encryption Standard(AES)です。
- SNMPv3は、User-Based Security Model(USM)オプションでのみサポートされます。TLSを介したSMNPv3はサポートされていません。
- SNMP認証用にユーザを設定するために使用されるUSMユーザコマンドは、SNMPv2cには影響しません。
- エンドポイントでのSNMP CommunityNameの設定は、SNMPv3の設定には影響しません。
- SNMP CommunityNameでは大文字と小文字が区別されます。
- NetworkServices SNMP CommunityNameを空の文字列("")に設定することにより、SNMPサポートをv3だけに制限できます。
- SNMPv1はサポートされていません。
- SNMPv2cとSNMPv3の両方について、エンドポイントは同じオブジェクト識別子(OID)を公開します。
- SNMPv3の場合、認証プロトコルはSHA-2ファミリに属している必要があります（MDもSHA-1もサポートされていません）。 そうでない場合、SNMP要求は認証に失敗し、応答されません。
- プライバシーパスワードは、ローカライズされたハッシュ値(AES-128)としてデバイスに保存されます。プライバシーパスワードがこのパラメータで明示的に設定されていない場合、認証パスワードと同じになるように設定されます（認証プロトコルパラメータで指定されたハッシュ関数を使用）。
- パスワード/パスフレーズとユーザ名は、特定の長さの境界内に収まっている必要があります。たとえば、USMユーザー名は最大32文字で、認証パスワードは8文字以上255文字以下である必要があります。これらの要件が満たされていない場合、Network SNMP USM User Addコマンドでのユーザの作成が失敗し、エラーが返されます。

エンドポイントでのSNMPの問題を解決するためにTACに連絡する

エンドポイントのSNMP設定が完了したが、問題が発生した場合は、TACに連絡して次の情報を共有する必要があります。

- Control Hubで組織ID(Organization ID)を入力し、影響を受けるエンドポイントのシリアル番号(SN)を入力します。
- 直面しているシナリオについて説明してください。
- 設定しようとしているSNMPのバージョンを指定します。
- 表示されたエラーメッセージを入力します。
- デバイスの設定に問題がある場合は、設定プロセスが停止したステップを明確に説明し、スクリーンショットを提供します。エラーを返すコンフィギュレーションコマンドを共有します。
- エンドポイントログを収集し、ケースにアップロードします。
- SNMP設定のテストに使用するutility\NMSまたはその他のツールを共有します。ユーティリティを使用してエンドポイントのSNMPエージェントに対してテストする場合は、使用する完全なコマンドを入力します。

関連情報

ルームOS xAPIドキュメント – SNMP関連コマンド

ボード、デスク、およびルームシリーズデバイスのデバイス設定

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。