Configuration du protocole SNMP sur les terminaux enregistrés dans le cloud

Table des matières

Introduction

Ce document décrit comment configurer et dépanner SNMP sur un terminal enregistré dans le cloud.

Conditions préalables

Exigences

Nous vous recommandons de vous familiariser avec les sujets suivants :

- Plateforme de concentrateur de contrôle
- Administration du terminal via l'interface utilisateur graphique du terminal et la section Périphériques du concentrateur de contrôle
- SSH vers un terminal en tant qu'utilisateur admin
- Système d'exploitation
- SNMP (SNMPv2c et SNMPv3)
- Snmpwalk ou autre utilitaire/outil ou système de gestion de réseau (NMS) pour tester la

configuration SNMP

Composants utilisés

L'équipement répertorié ici a été utilisé pour effectuer les tests et produire les résultats décrits dans ce document :

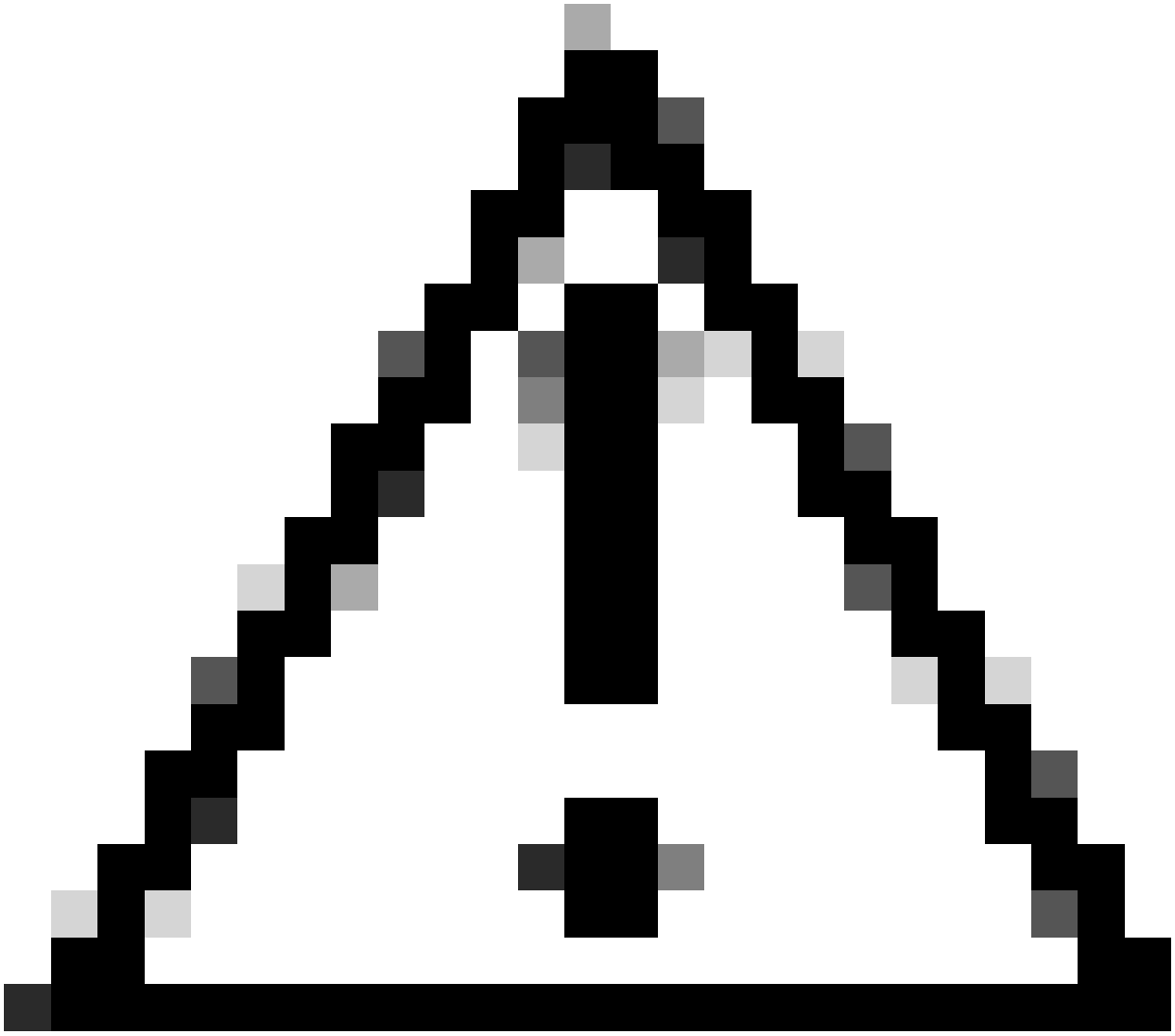
- Organisation du Control Hub
- Cisco Room Kit Pro
- Cisco Room Bar Pro
- Serveur Linux pour héberger l'utilitaire snmpwalk pour tester la configuration SNMP.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Qu'est-ce que SNMP

SNMP est l'acronyme de Simple Network Management Protocol. Il s’agit d’un protocole utilisé pour collecter et gérer des informations sur les périphériques d’un réseau, surveiller l’état des périphériques ou modifier la configuration. Ces périphériques peuvent être des routeurs, des commutateurs, des serveurs, des imprimantes ou tout autre type de périphérique. Une adresse IP a été attribuée à ces périphériques comme condition préalable. Il existe trois versions de SNMP. Le système d'exploitation de salle prend en charge SNMPv2c et SNMPv3. SNMPv1 n'est pas pris en charge.

Cet article se concentre sur la configuration et le dépannage du protocole SNMP sur les terminaux de collaboration exécutant le système d'exploitation de salle qui sont enregistrés dans le cloud (sans utiliser Webex Edge pour les périphériques).



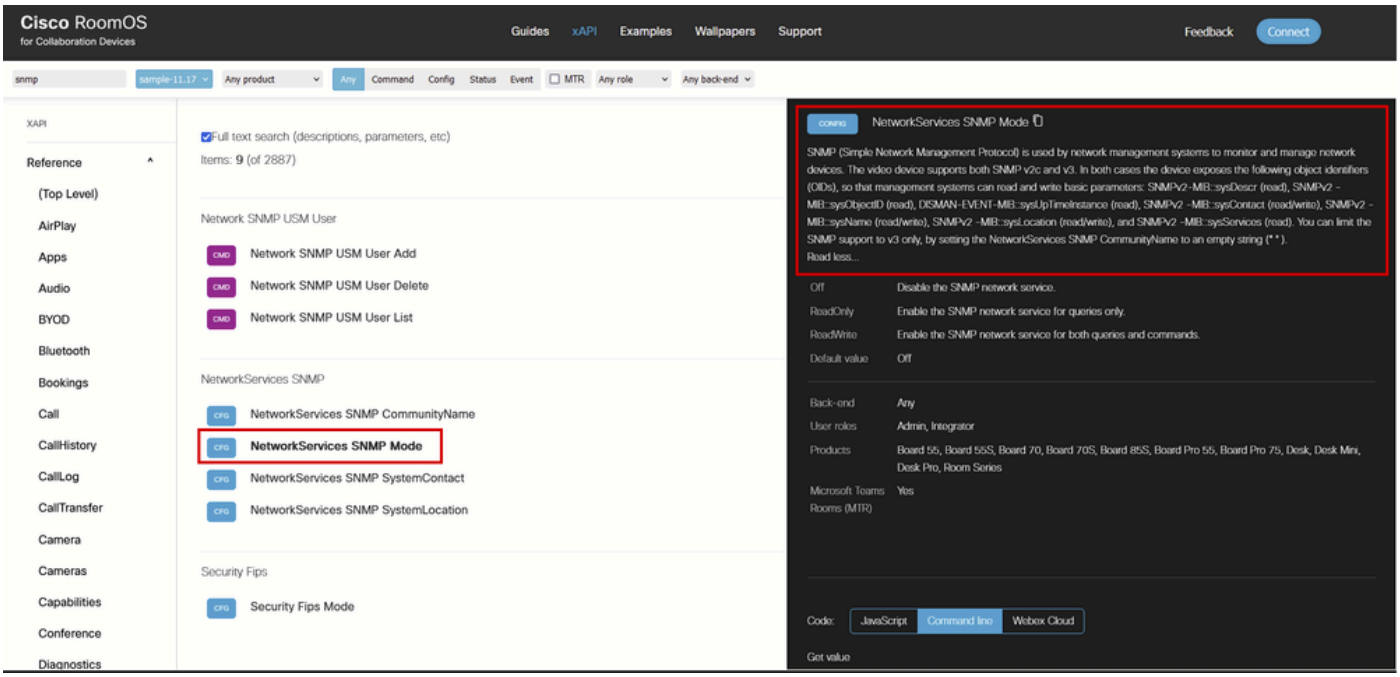
Mise en garde : Cet article aborde la configuration SNMP uniquement du point de vue des terminaux. Toute configuration effectuée du côté du réseau et les outils utilisés pour demander/mettre à jour des informations relatives au protocole SNMP sur les terminaux ne sont pas abordés dans cet article.

Le TAC ne prend pas en charge le dépannage de SNMP dans le réseau et ne peut pas non plus fournir d'inférences sur la raison pour laquelle SNMP ne fonctionne pas comme prévu du point de vue du réseau. Votre équipe réseau doit être impliquée dans le dépannage de ces problèmes.

La gestion du protocole SNMP peut être effectuée à l'aide de nombreux outils différents. Ces outils ne sont pas pris en charge par le TAC. En cas de divergence dans les informations collectées par ces outils à partir des terminaux, le problème doit d'abord être dépanné par l'équipe réseau, puis transmis au centre d'assistance technique si les informations disponibles sont suffisantes pour prouver qu'il s'agit d'un problème lié aux terminaux.

Quelles informations peuvent être demandées ?

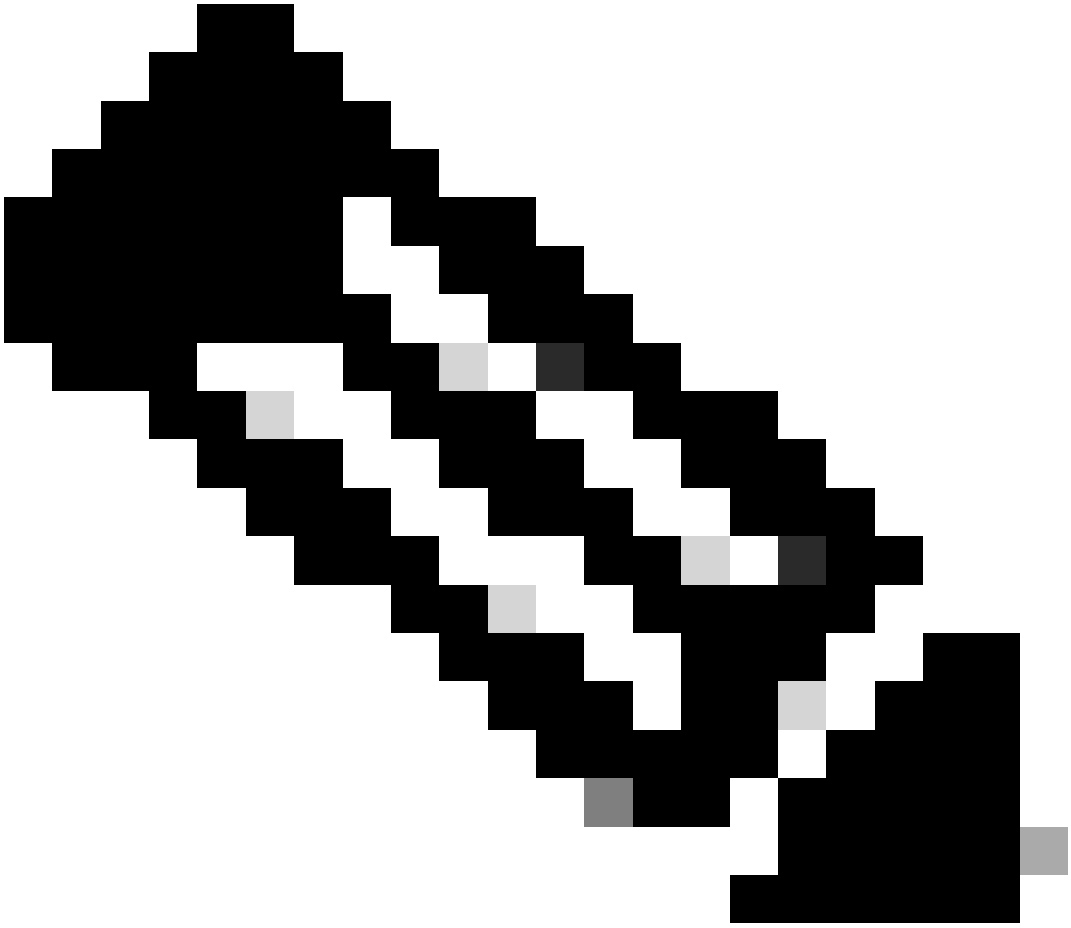
Grâce au protocole SNMP, vous pouvez demander une quantité limitée d'informations au terminal. Les OID et MiB pris en charge sont visibles dans ce lien, sous les détails de la description de commande NetworkService SNMP Mode :



Description de la commande NetworkService SNMP Mode dans la documentation xAPI de Room OS

Les points d'extrémité exposent ces OID pour SNMPv2 et SNMPv3 :

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

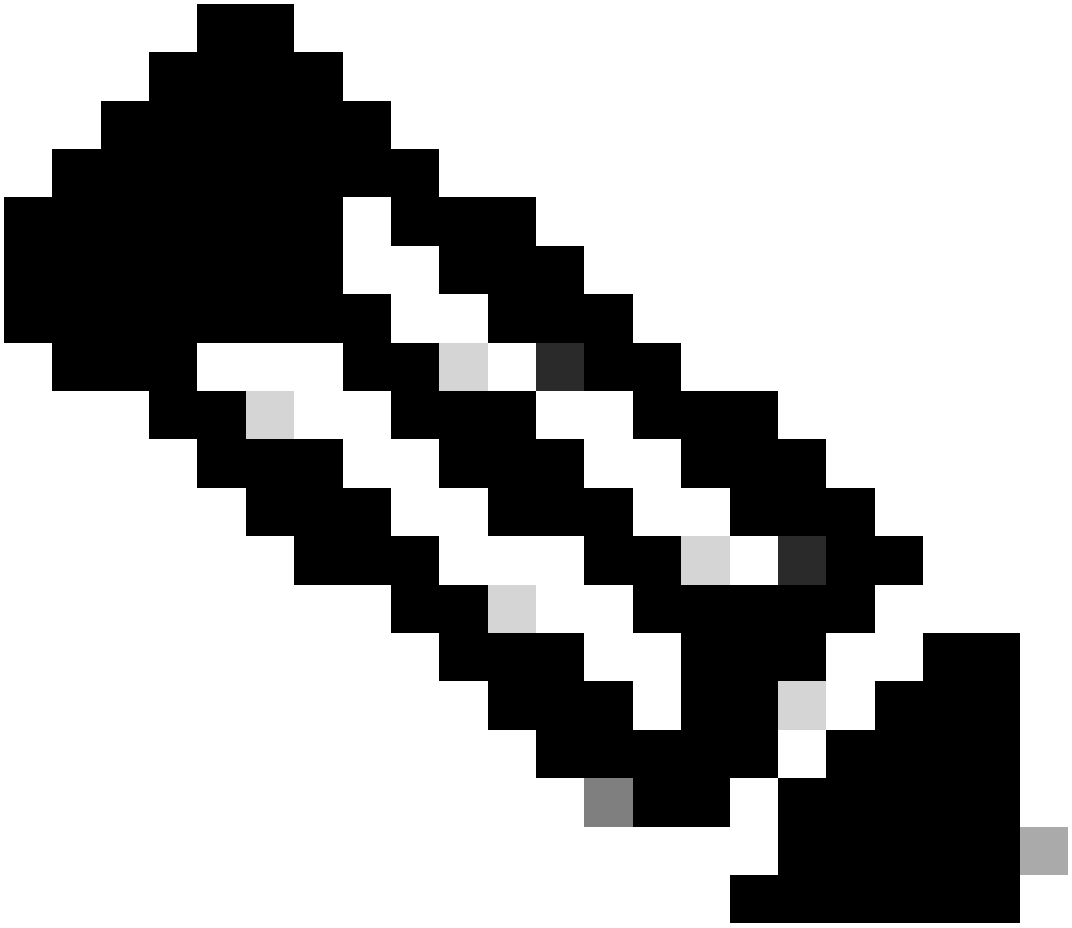


Remarque : NetworkServices SNMP CommunityName peut être défini sur une chaîne vide si vous souhaitez utiliser uniquement SNMPv3.

Configuration du protocole SNMP sur un terminal enregistré dans le cloud

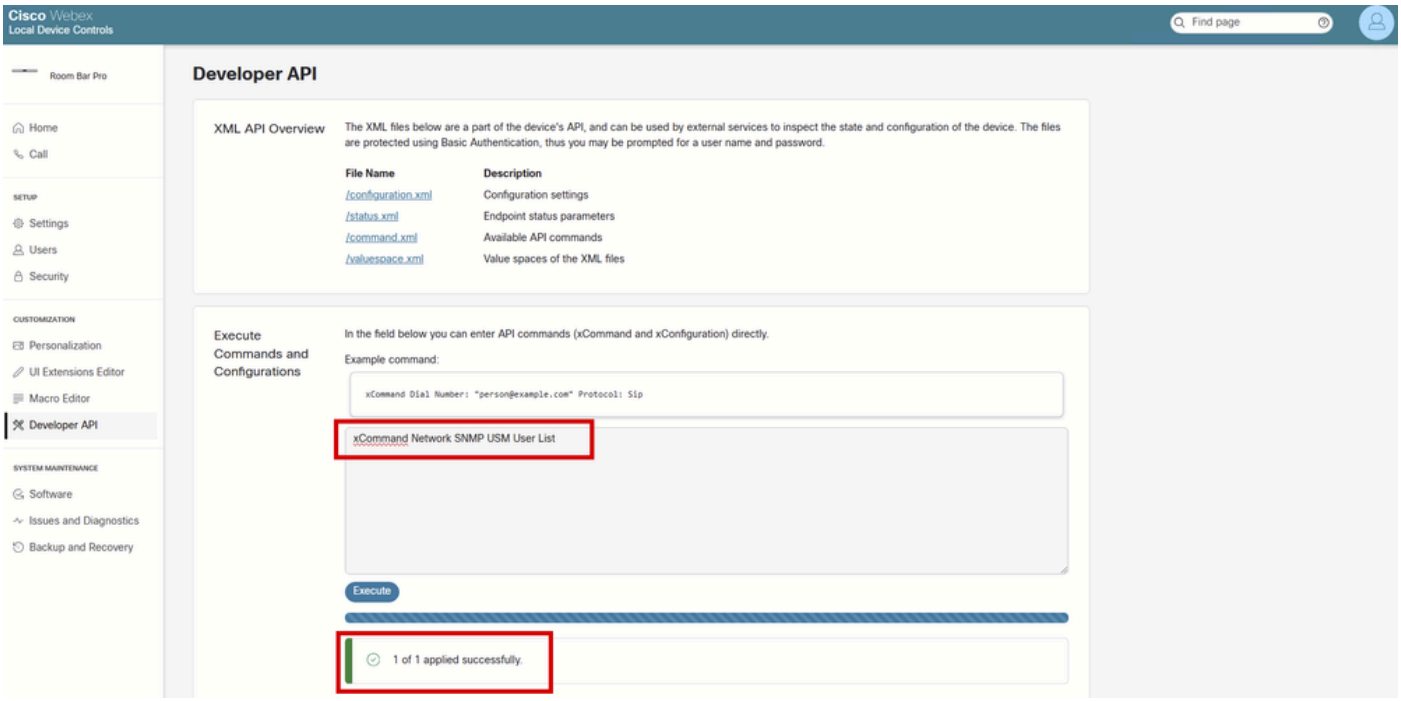
En règle générale, les modifications de configuration sur les terminaux peuvent se produire de quatre manières différentes :

1. Les API Webex disponibles
2. Interface utilisateur graphique du terminal
3. Concentrateur De Commande
4. SSH directement au point d'extrémité

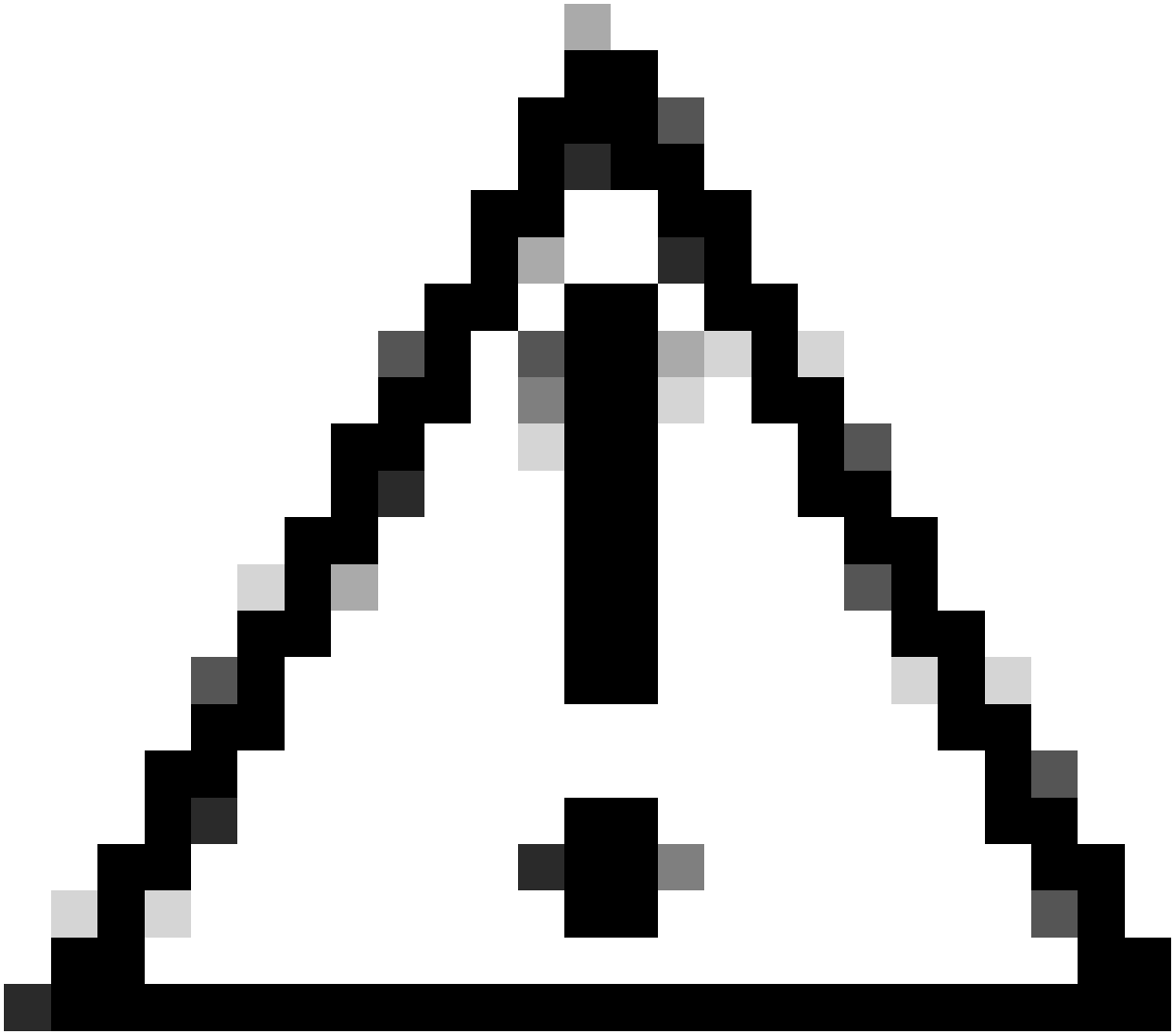


Remarque : Pour accéder à l'interface utilisateur graphique d'un terminal, ouvrez un navigateur et, dans la barre d'URL, tapez l'adresse IP du terminal. Vous devez être sur le même réseau que le point d'extrémité et vous devez disposer d'informations d'identification d'utilisateur pour pouvoir vous connecter.

Toutes les configurations ne peuvent pas être effectuées de ces quatre manières. Pour le scénario de ce document, le mode SNMP peut être activé dans les quatre manières, mais afin de créer un utilisateur SNMP qui est capable de communiquer avec le périphérique via SNMP, vous devez SSH au point d'extrémité, ou utiliser les API Webex, ou utiliser l'interface utilisateur graphique du point d'extrémité à l'API de développeur sous la section Personnalisation. Les utilisateurs USM ne peuvent pas être créés à partir de la section Control Hub All Configurations du point de terminaison.



Section Developer API sur l'interface utilisateur graphique des terminaux

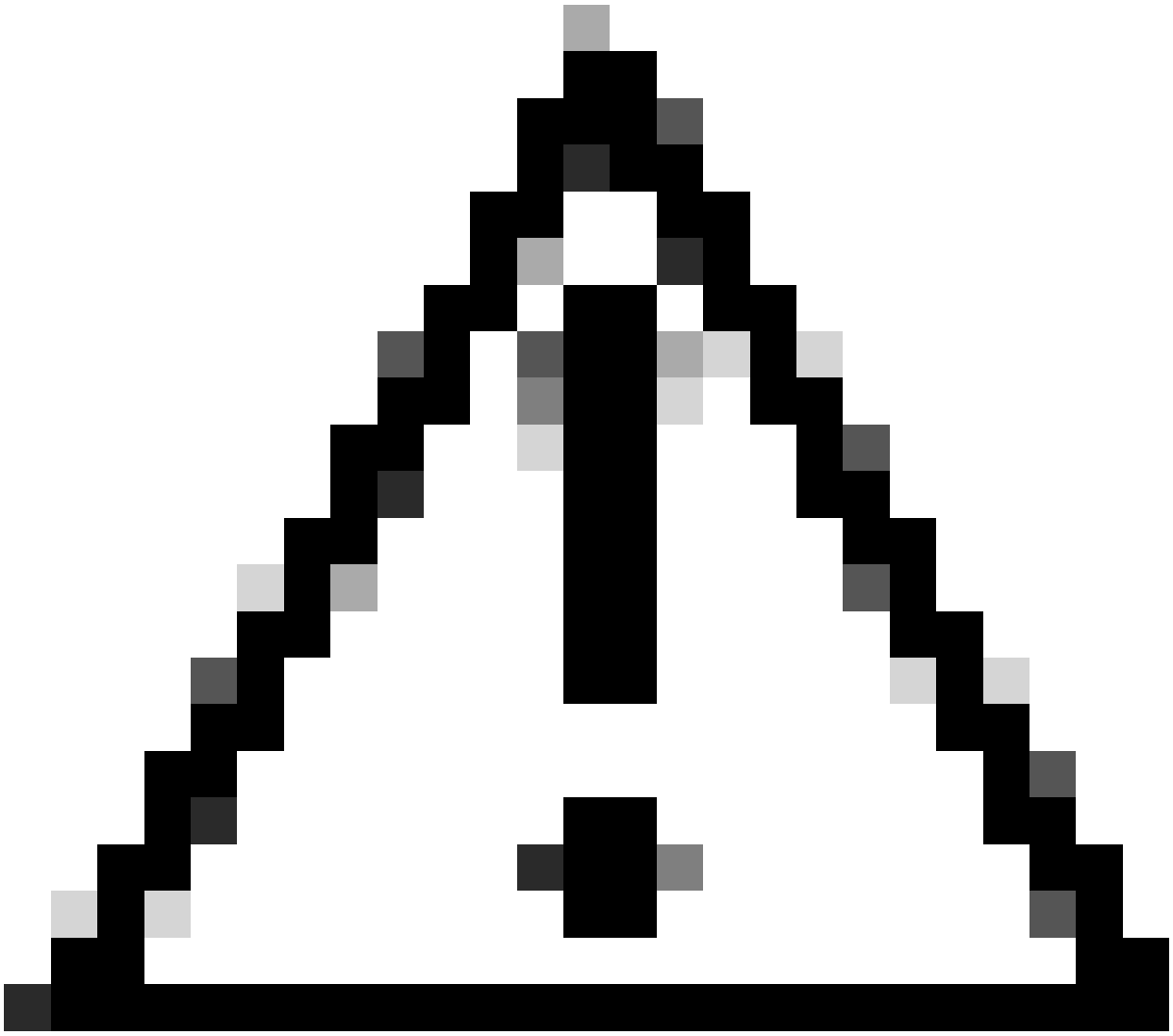


Mise en garde : Les commandes exécutées dans la zone de texte Exécuter les commandes et les configurations ne renvoient aucun résultat. Vous ne voyez que si la commande a été exécutée avec succès ou non. C'est pourquoi la commande qui répertorie les utilisateurs USM ne renvoie aucun résultat dans la capture d'écran précédente. Cela signifie que vous pouvez créer un utilisateur USM à partir de cette section de l'interface utilisateur graphique du terminal avec succès, mais afin de vérifier si l'utilisateur est créé, vous devez SSH au périphérique.

Pour configurer SNMPv2c, il n'est pas nécessaire de créer un utilisateur. L'authentification s'effectue à l'aide du nom de communauté (également appelé chaîne de communauté) configuré sur le point d'extrémité. L'agent SNMP du point d'extrémité, qui existe déjà sur le périphérique, répond aux requêtes qui correspondent au nom de communauté configuré sur le périphérique. Si une requête SNMP provenant d'un système de gestion n'inclut pas de nom de communauté correspondant (sensible à la casse), le message est abandonné et l'agent SNMP du périphérique vidéo n'enverra pas de réponse.

Cependant, SNMPv3 nécessite la configuration d'un utilisateur USM pour que l'authentification

réussisse. À cette fin, il est nécessaire d'utiliser les commandes Network SNMP USM User. Cela peut se produire par SSH directement au périphérique ou en utilisant l'interface graphique du périphérique sous la section Developer API. Vous pouvez également utiliser l'API Webex.



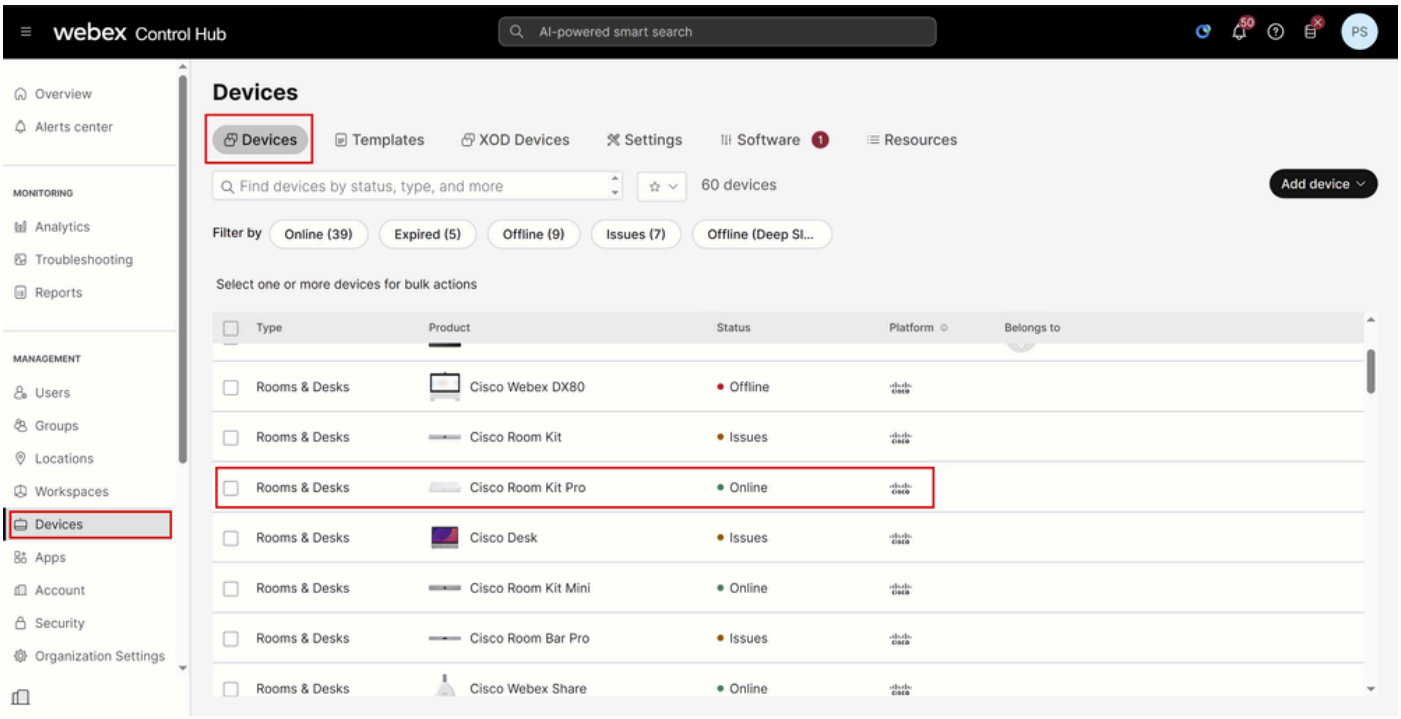
Mise en garde : Vous devez décider si vous allez activer SNMPv2, SNMPv3 ou les deux. SNMPv1 n'est pas pris en charge sur les terminaux Cisco. Toute tentative d'utilisation de SNMPv1 va échouer.

Dans ce document, les protocoles SNMPv2 et SNMPv3 vont être activés et configurés dans Control Hub, mais l'utilisateur USM nécessaire pour l'authentification SNMP3 est configuré sur SSH.

Activer le mode SNMPv2c dans le Control Hub

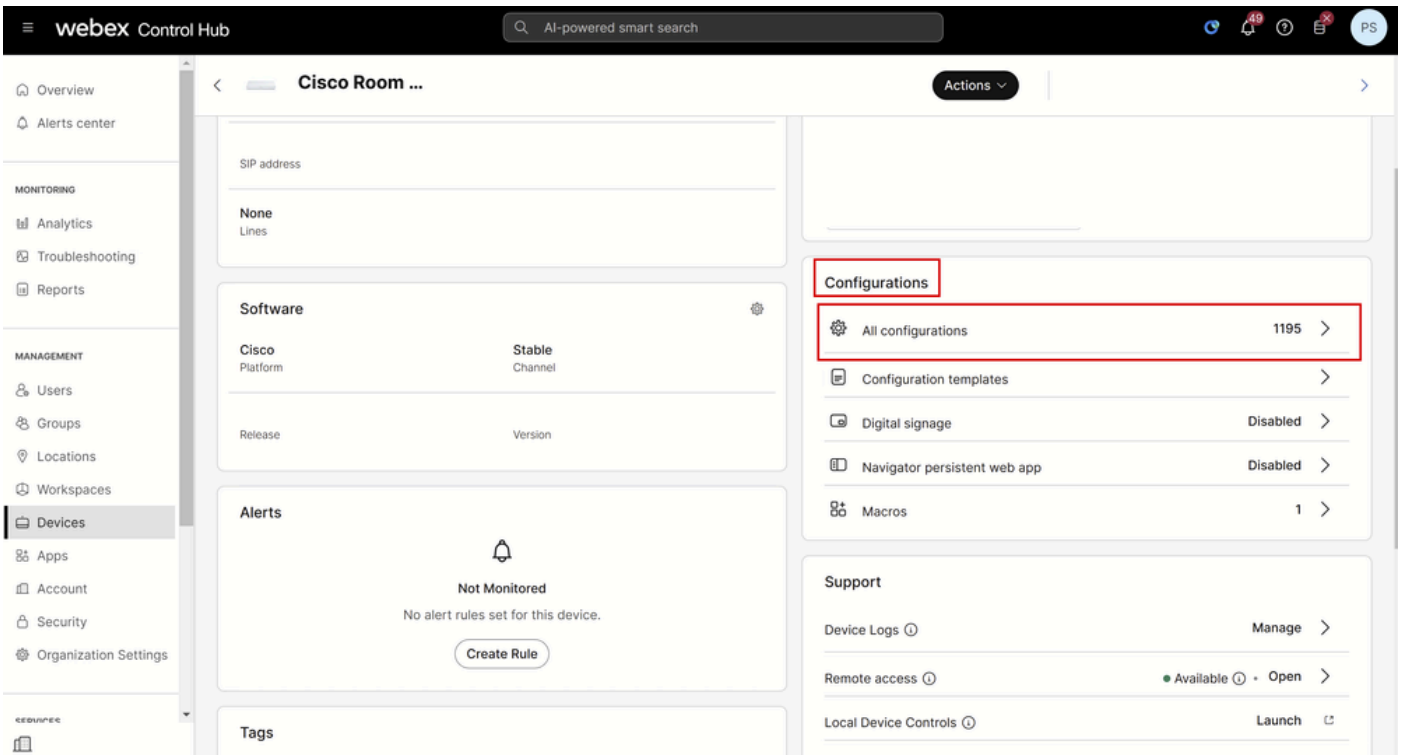
Accédez à admin.webex.com et connectez-vous avec vos informations d'identification d'administrateur. Il est conseillé d'être un administrateur complet. Accédez à Devices sous Management section sur le côté gauche de l'interface utilisateur. Sous l'onglet Devices,

sélectionnez le périphérique que vous souhaitez configurer. Dans cet exemple, un kit de salle Cisco Pro est utilisé.



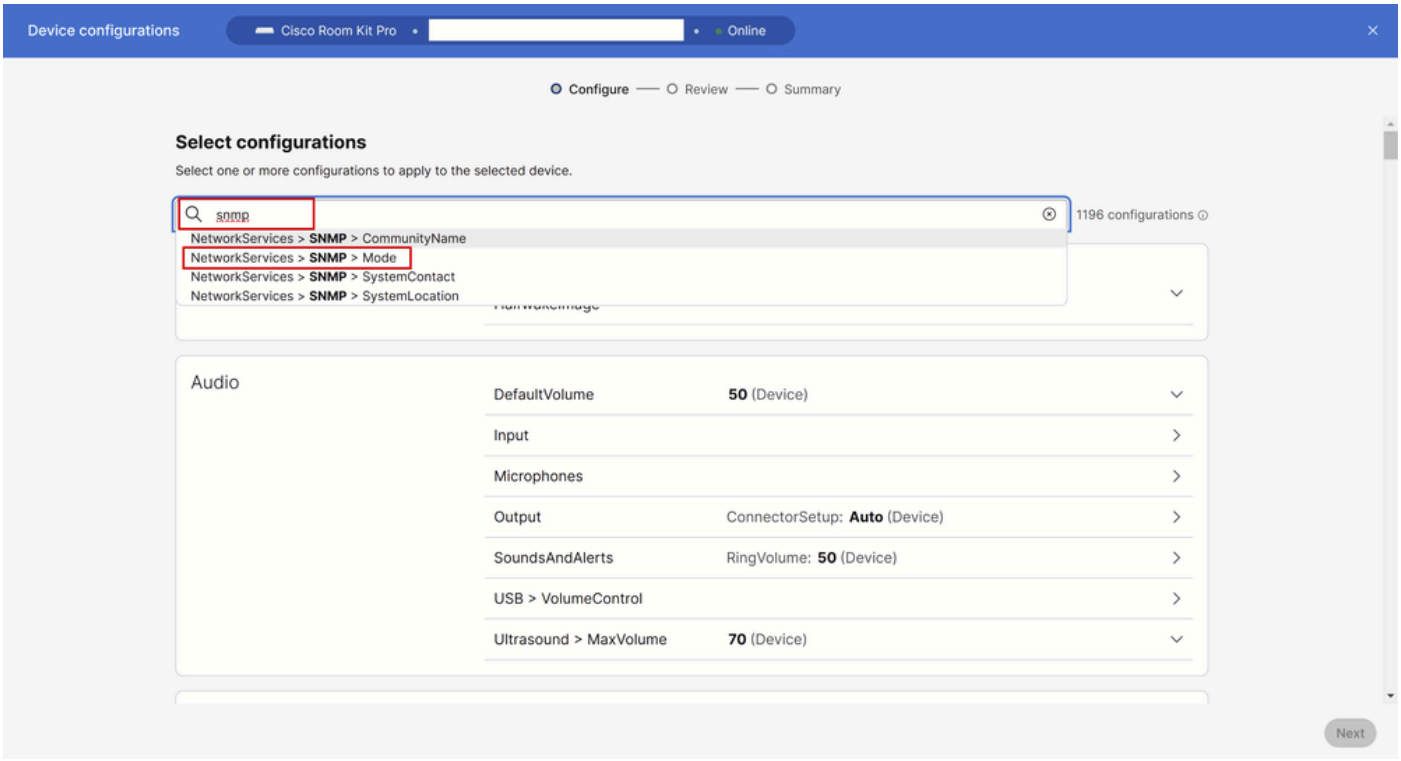
Section Control Hub Devices

Sous les détails du périphérique dans la nouvelle page Control Hub qui s'ouvre, accédez à la section Configurations et cliquez sur All Configurations :



Détails du dispositif de concentrateur de contrôle pour Room Kit Pro

Dans la barre de recherche, tapez snmp et sélectionnez NetworkServices > SNMP > Mode :

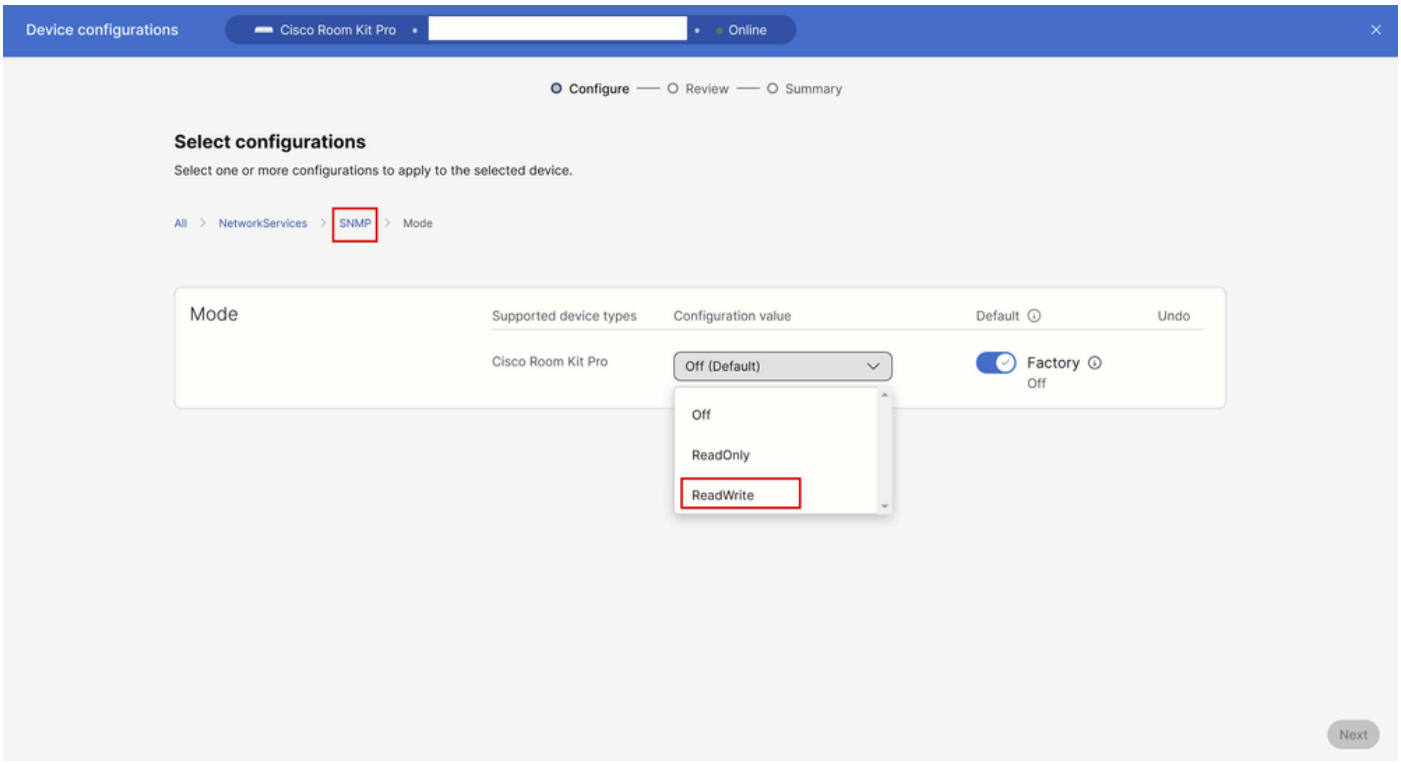


Fenêtre Toutes les configurations du concentrateur de contrôle

Sélectionnez le mode à activer dans votre environnement. Trois options sont disponibles :

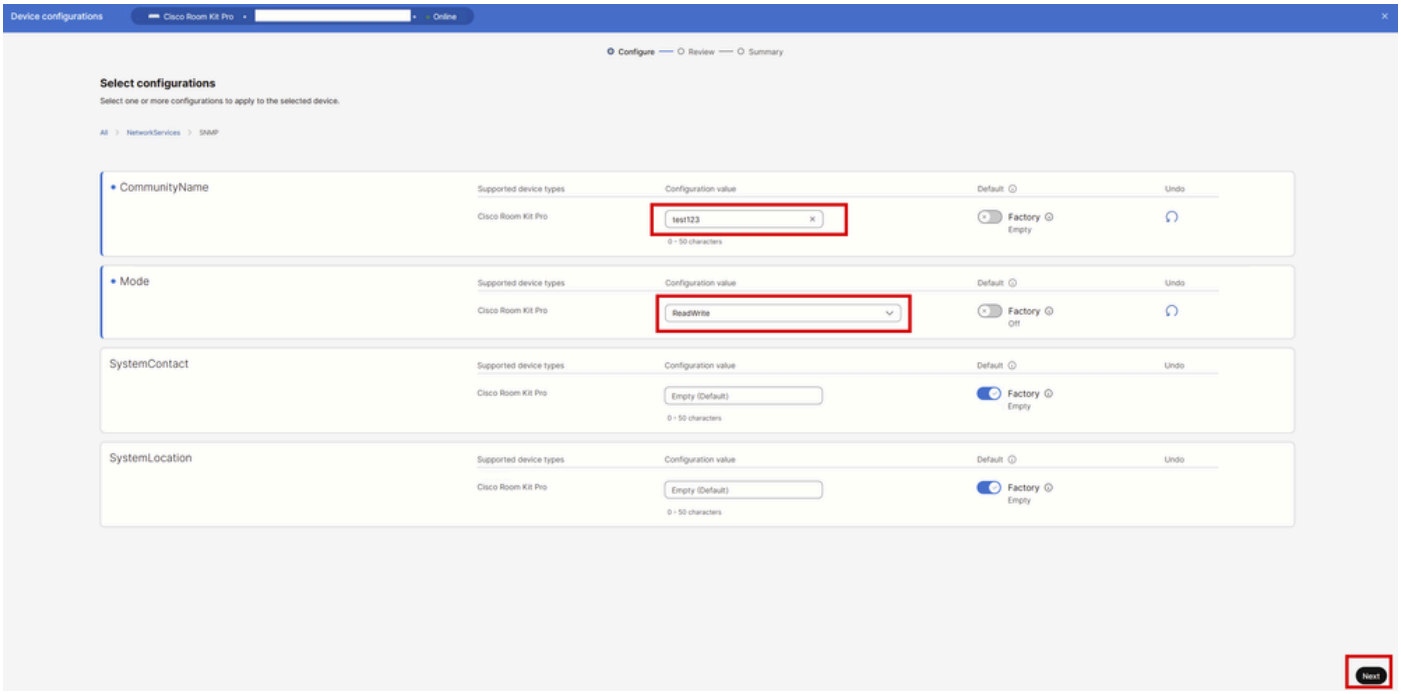
1. Désactivé: Désactivez le service réseau SNMP.
2. Lecture seule : Activez le service réseau SNMP pour les requêtes uniquement.
3. LectureÉcriture : Activez le service réseau SNMP pour les requêtes et les commandes.

Dans cet exemple, ReadWrite est sélectionné. Cliquez ensuite sur SNMP dans la section de navigation des paramètres, comme le montre l'image. Ceci vous ramène à une étape dans les paramètres, et vous pouvez voir tous les paramètres liés au SNMP qui peuvent être configurés sur le périphérique via le Control Hub :



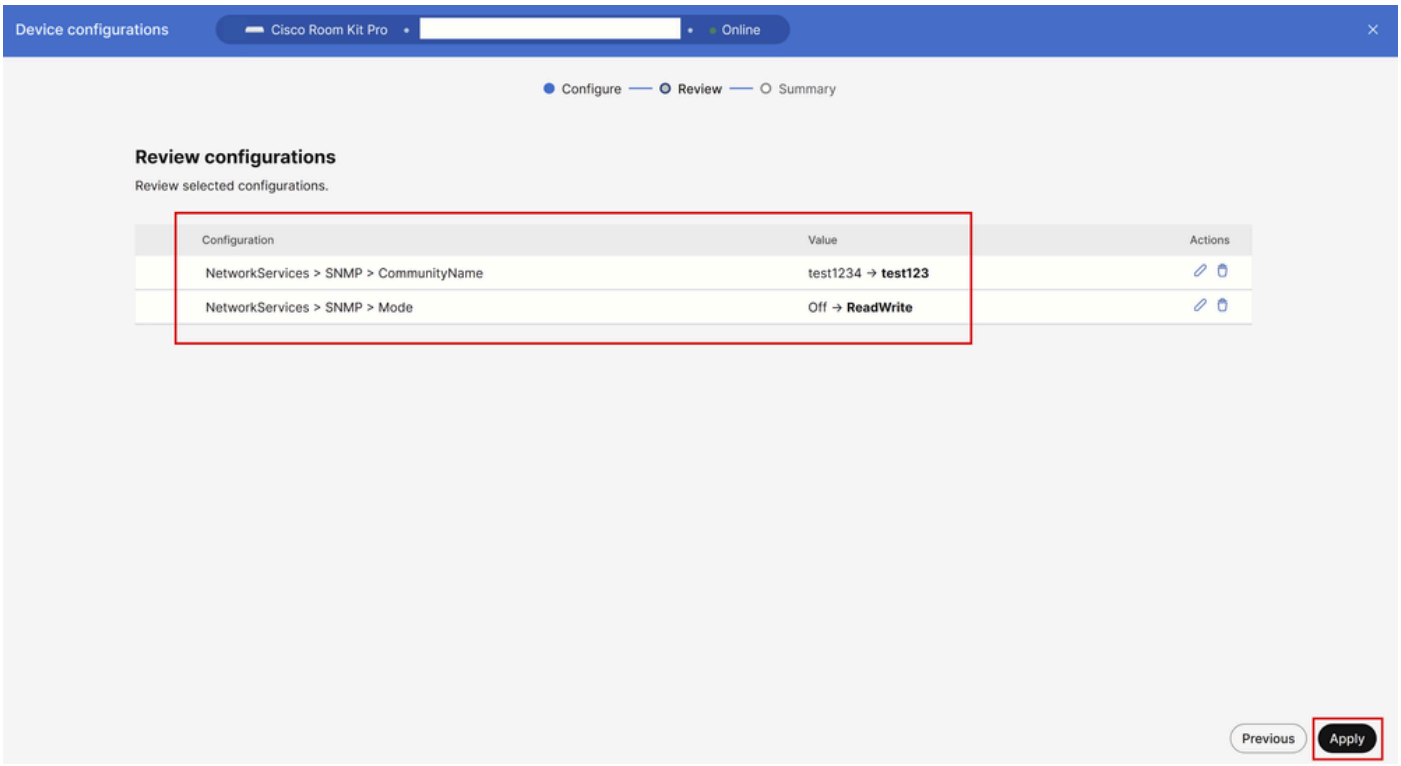
Paramètre du mode SNMP sous Toutes les configurations dans Control Hub

Après avoir cliqué sur SNMP, toutes les options SNMP disponibles apparaissent, comme le montre cette image. Pour que SNMPv2 soit correctement configuré, un nom de communauté doit être configuré. Le nom de communauté est utilisé pour l'authentification entre le serveur SNMP et l'agent SNMP qui existe sur le point d'extrémité. Le nom de la communauté est défini sur test123 pour cet exemple. Cliquez sur Next dans l'angle inférieur droit.



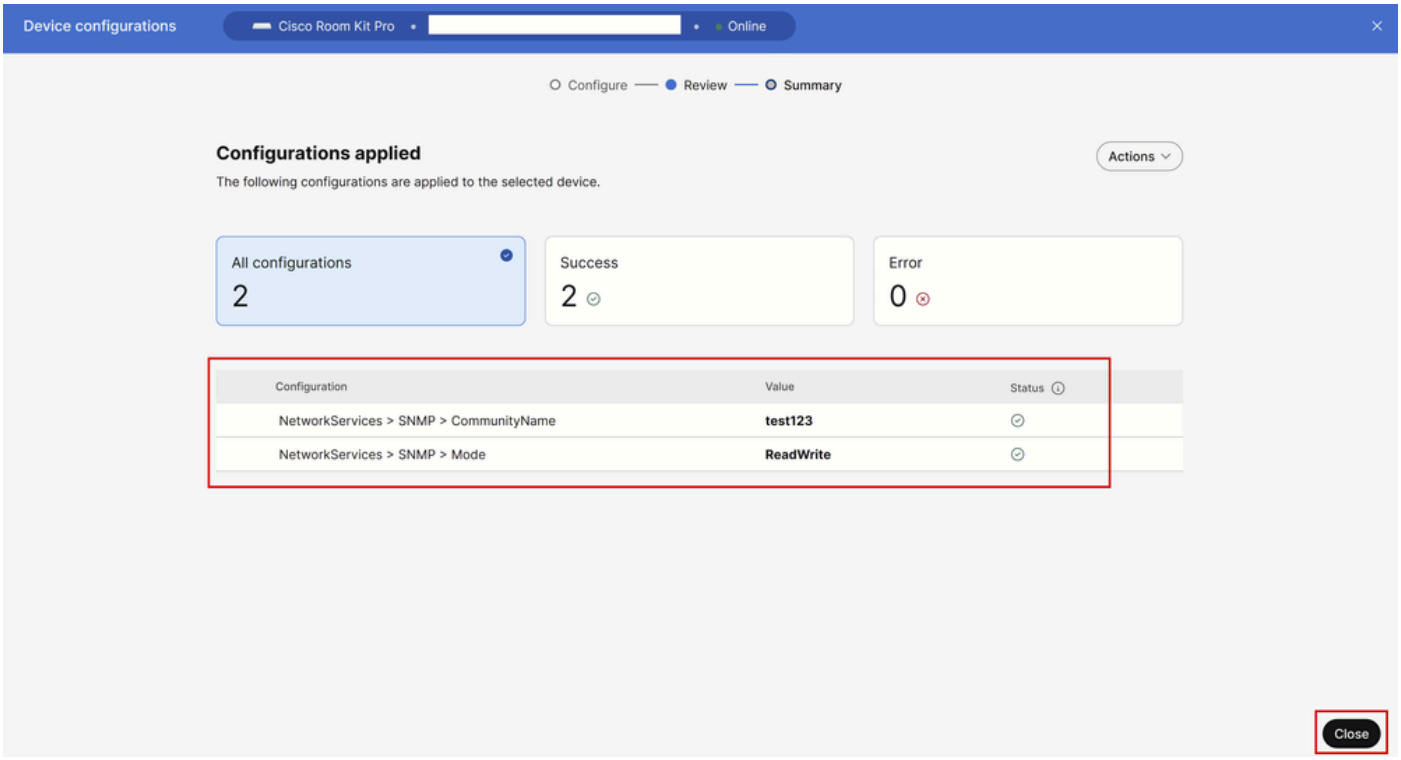
Paramètres SNMP sous Toutes les configurations dans Control Hub

Vérifiez les configurations du périphérique et cliquez sur Apply dans le coin inférieur droit :



Vérifier les configurations avant d'appliquer les modifications

Vérifiez que les modifications de configuration ont bien été appliquées. Cliquez ensuite sur Fermer.



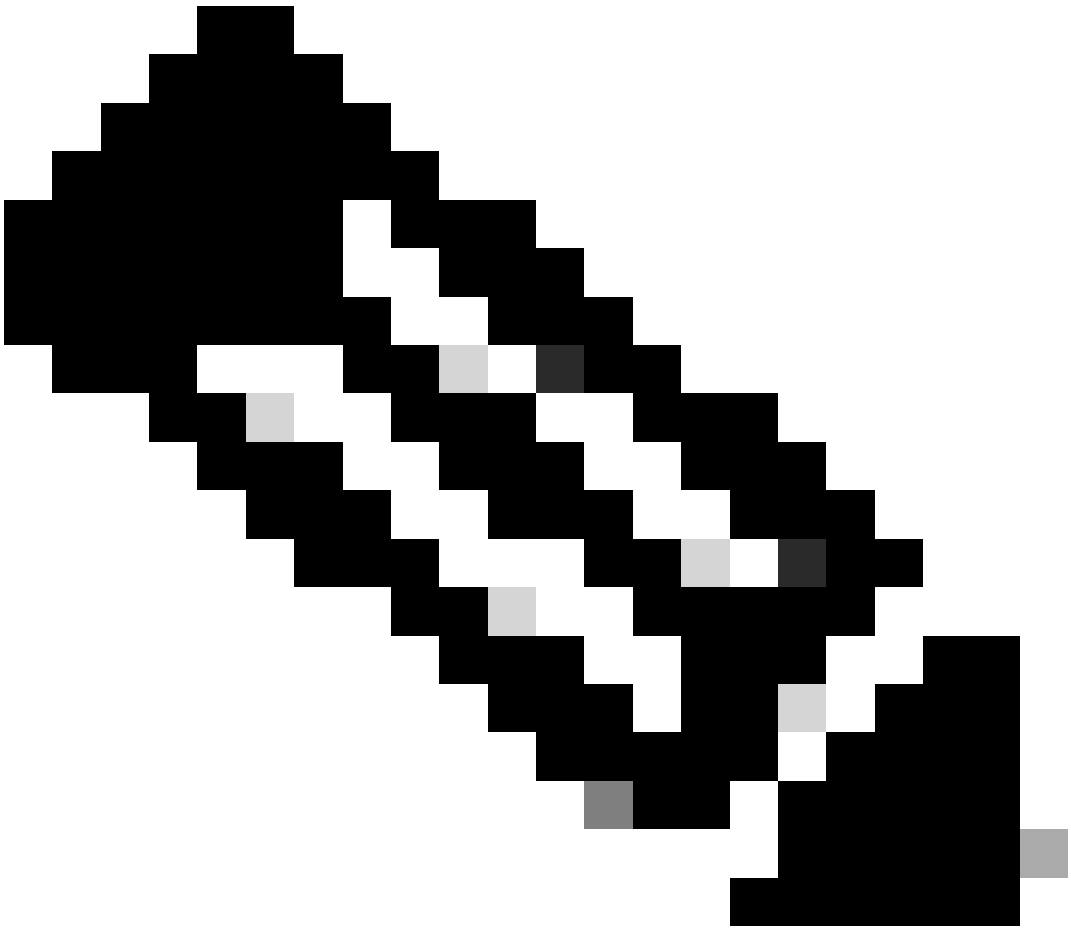
Configurations des points de terminaison appliquées avec succès dans Control Hub

À ce stade, SNMPv2c est correctement activé sur le terminal et le nom de la communauté est configuré.

Activer le mode SNMPv3 dans le Control Hub

Le protocole SNMPv3 offre plus de sécurité et nécessite une configuration différente sur le terminal par rapport au protocole SNMPv2c. Accédez à Devices sous Management section dans Control Hub. Restez sous l'onglet Devices et sélectionnez l'un de vos terminaux que vous souhaitez configurer avec SNMPv3. Pour cet exemple, un Cisco Room Bar Pro est utilisé.

Sous les détails du périphérique, accédez à la section Configurations et cliquez sur All Configurations. La page Device Configurations s'ouvre. Tapez snmp dans la barre de recherche et sélectionnez NetworkServices > SNMP > Mode. Dans cet exemple, le mode SNMP est défini sur ReadWrite. Cliquez sur SNMP pour afficher tous les paramètres SNMP configurables sur le périphérique.

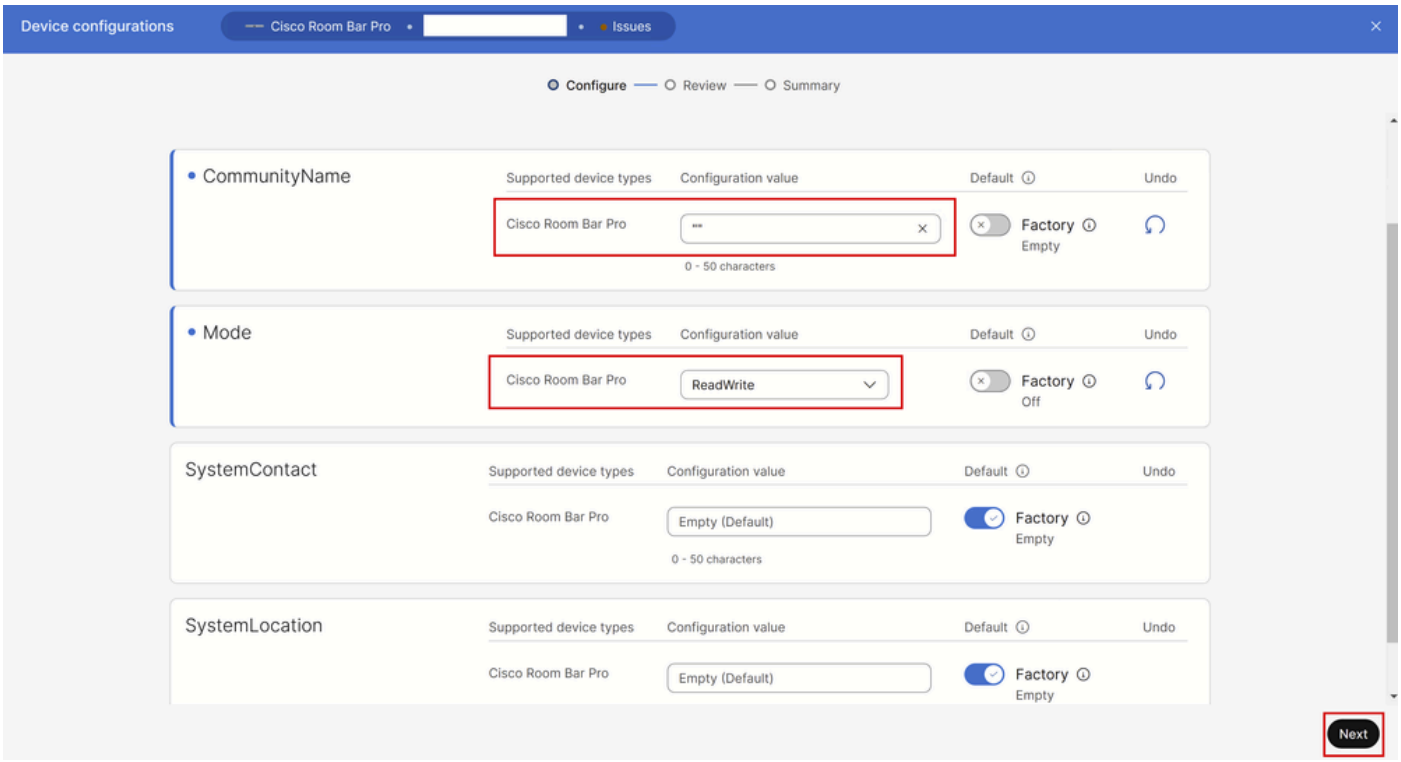


Remarque : Toutes les étapes mentionnées jusqu'à présent pour SNMPv3 ont déjà été décrites lors de la configuration de SNMPv2c dans un exemple précédent. Pour cette raison, aucune capture d'écran des étapes n'est fournie. Reportez-vous à la section Activer le mode SNMPv2c dans le Control Hub si vous avez des doutes sur la façon de

---

naviguer dans les paramètres du Control Hub.

Pour ne prendre en charge que SNMPv3, vous devez configurer le nom de la communauté sous la forme d'une chaîne vide entourée de guillemets : "".



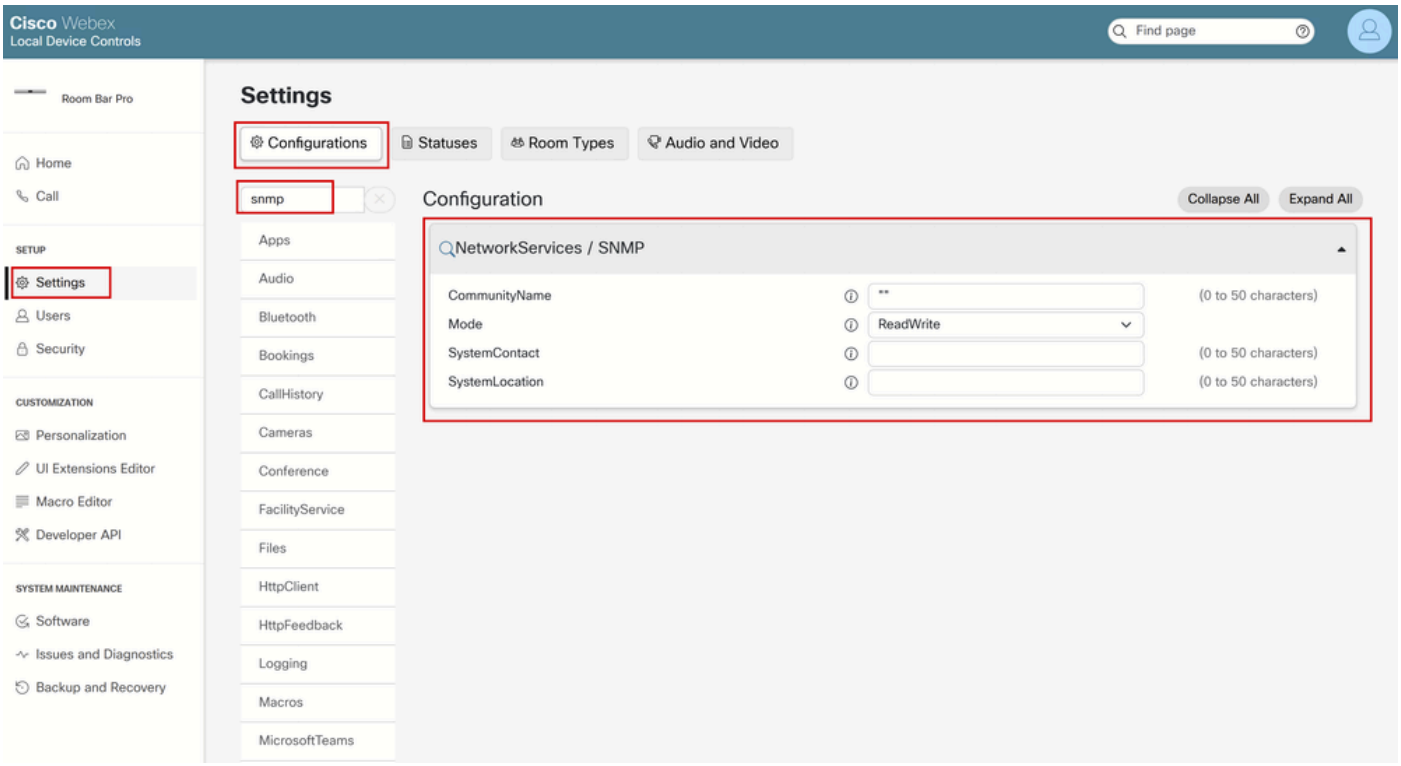
Paramètres SNMP sous Toutes les configurations dans Control Hub

Cliquez sur Next, puis vérifiez les modifications de configuration et cliquez sur Apply. Cliquez sur Close pour fermer la page de configuration du périphérique.

Nous voici à la fin de la configuration qui peut être effectuée dans le Control Hub. À ce stade, seul SNMPv3 est activé.

À quoi ressemble la configuration SNMP dans l'interface utilisateur graphique du terminal ?

Les mêmes configurations peuvent être effectuées à partir de l'interface utilisateur graphique du périphérique. Ouvrez un onglet de navigateur et tapez l'adresse IP du point d'extrémité (vous devez vous trouver dans le même réseau que le point d'extrémité). Connectez-vous en tant qu'utilisateur admin et, dans l'interface utilisateur graphique du terminal, accédez à Settings sous la section SETUP. Restez dans l'onglet Configurations, et dans la barre de recherche des paramètres, tapez snmp. Cette image montre comment les paramètres SNMP s'affichent pour la configuration SNMPv3 effectuée sur la barre de la salle Pro dans la section précédente :



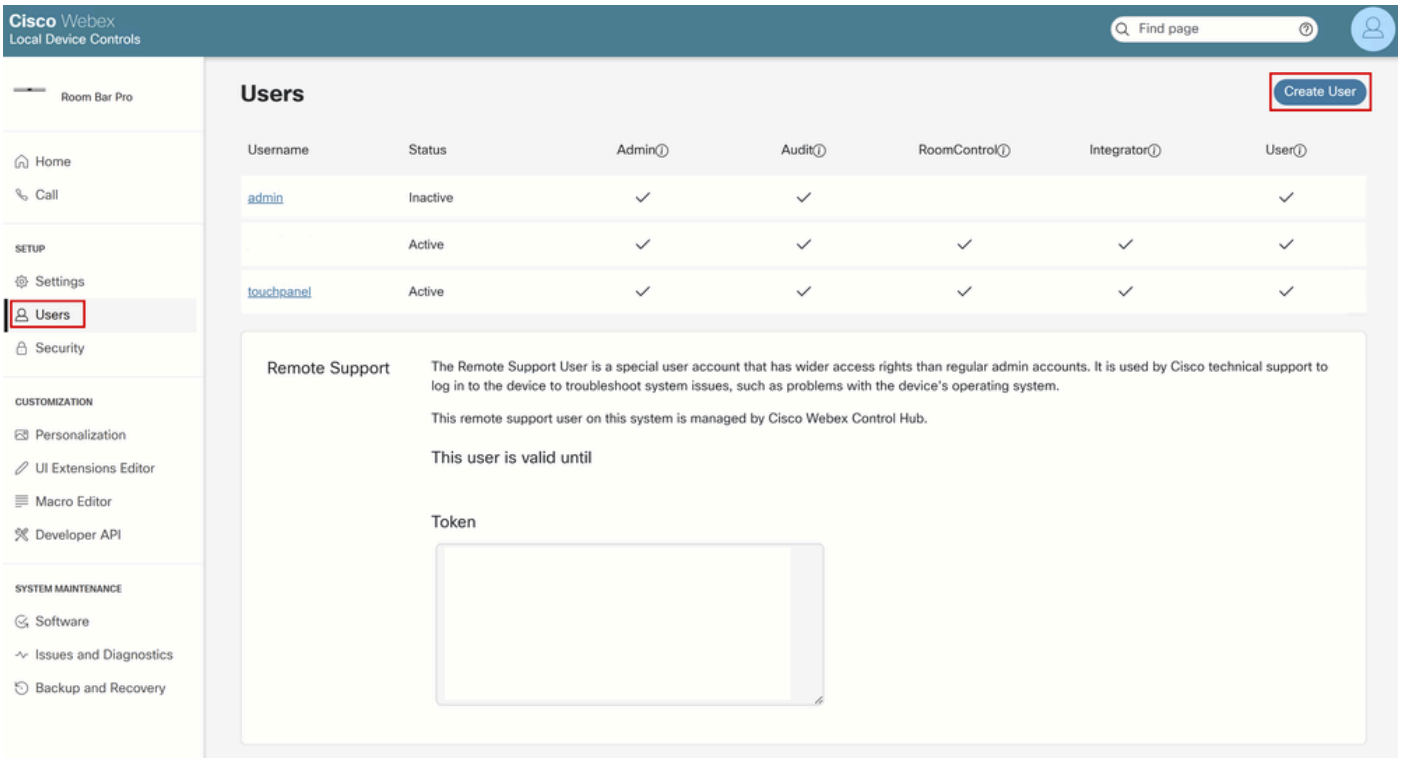
Configuration SNMPv3 sur l'interface utilisateur graphique du terminal

Configuration de l'utilisateur USM pour SNMPv3

Pour pouvoir utiliser SNMPv3, vous devez créer un utilisateur USM. Les commandes disponibles pour effectuer cette action sont disponibles dans le lien de documentation du système d'exploitation de la salle ici. Utilisez SSH pour vous connecter au périphérique. Pour cela, vous devez disposer d'un compte d'administrateur sur le périphérique. Si ce n'est pas le cas, vous devez créer un compte administrateur. Cette section passe en revue tout le processus.

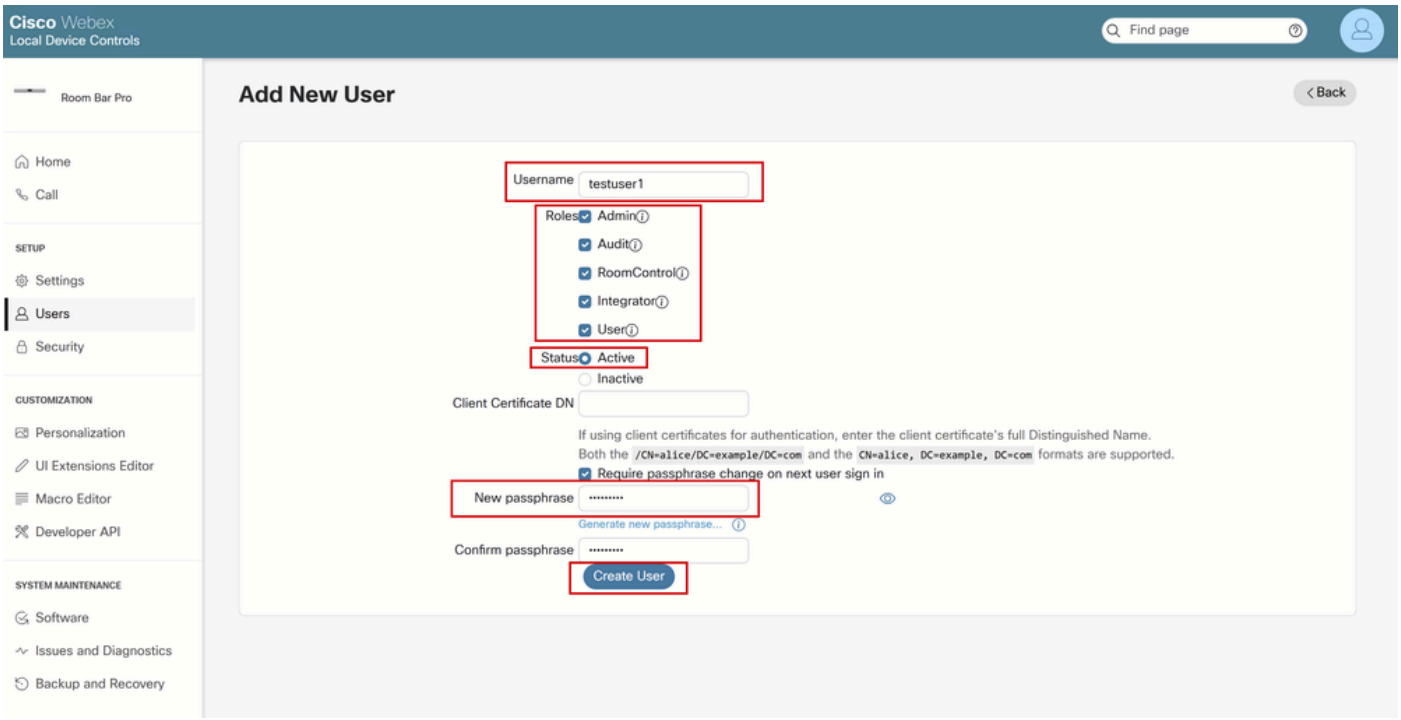
Accédez à Devices sous Management section dans Control Hub. Restez sous l'onglet Devices et sélectionnez l'un de vos terminaux pour lequel vous souhaitez créer un utilisateur admin. Dans cet exemple, un Cisco Room Bar Pro est utilisé.

Sous les détails du périphérique, accédez à la section Prise en charge et cliquez sur Contrôles des périphériques locaux (vous devez être dans le même réseau que le point d'extrémité pour que cela fonctionne). L'interface utilisateur graphique du périphérique s'ouvre. Accédez à Users sous SETUP section et cliquez sur Create User.



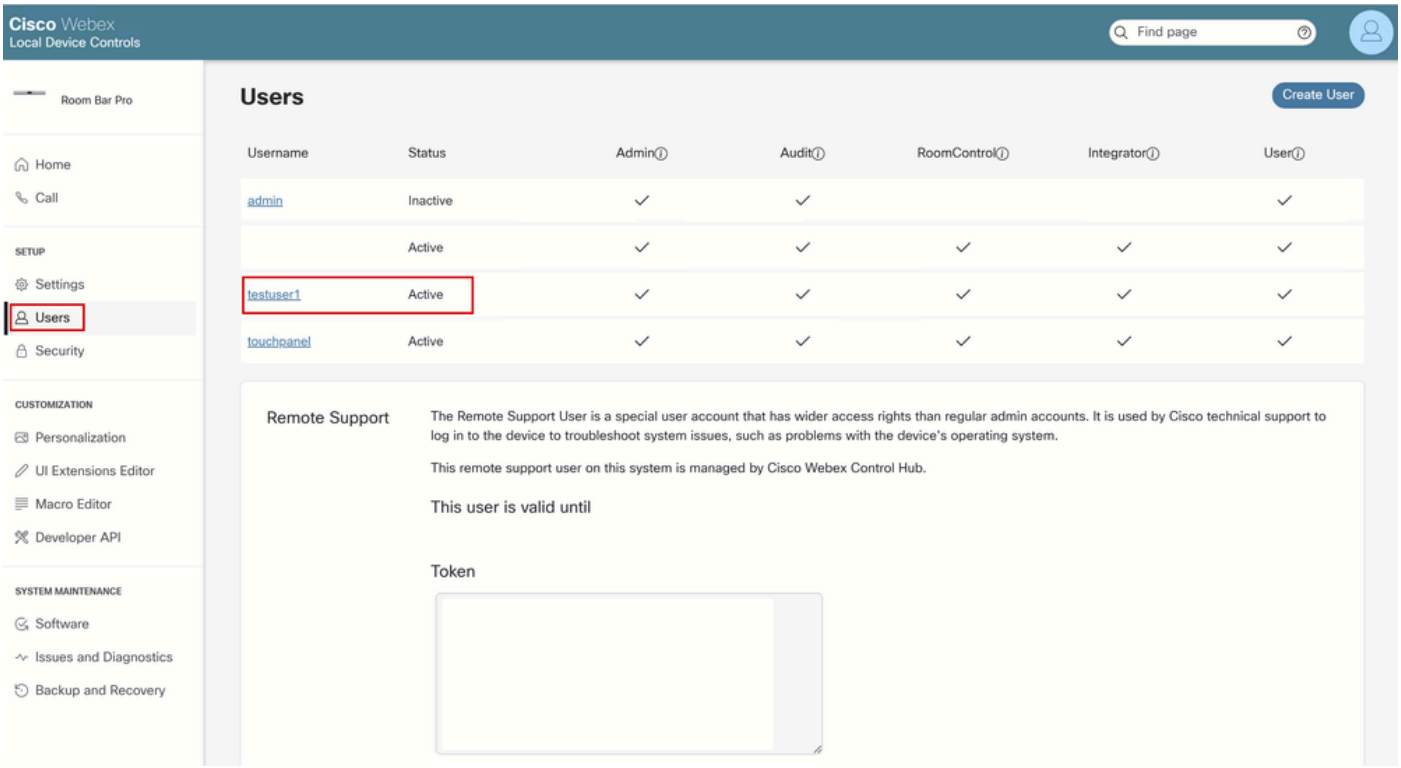
Section Users dans l'interface utilisateur du terminal

Entrez un nom d'utilisateur et une phrase de passe. Assurez-vous que l'utilisateur dispose de privilèges d'administrateur complets et qu'il est actif :

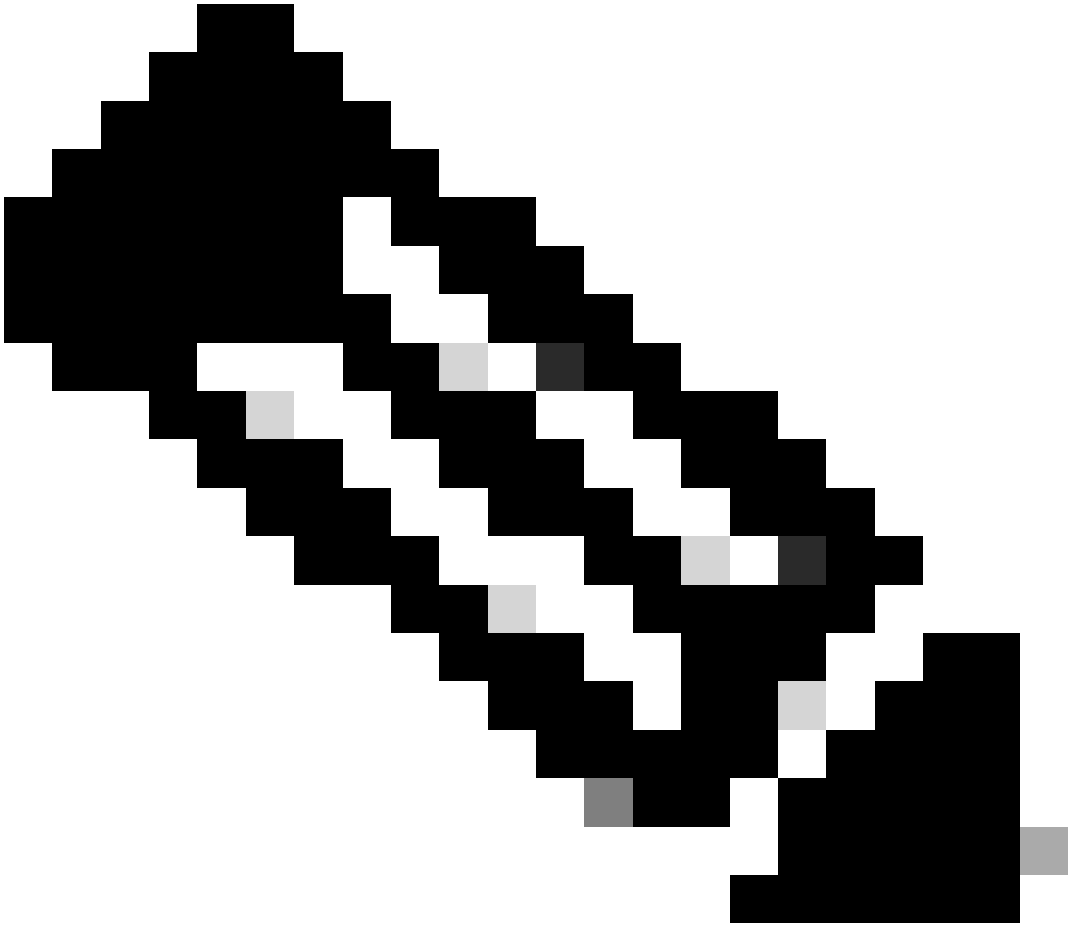


Créer un utilisateur à partir de l'interface utilisateur graphique du terminal

Vérifiez que l'utilisateur a été créé et qu'il est actif à partir de la page Users :



Nouvel utilisateur créé et répertorié parmi les autres utilisateurs



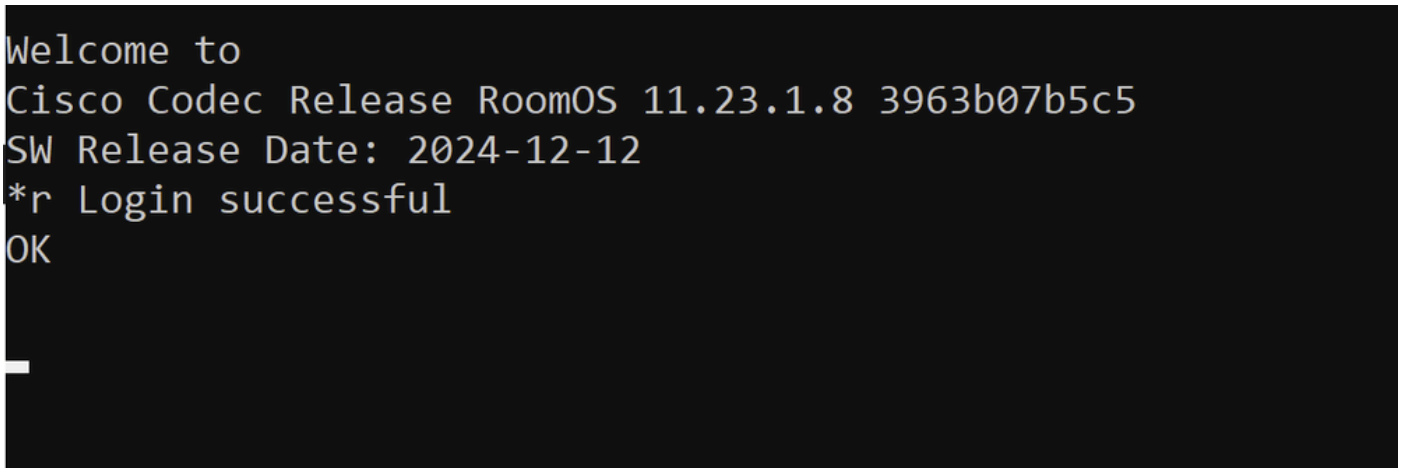
Remarque : Lors de la première tentative de connexion SSH avec un nouvel utilisateur, vous êtes invité à modifier votre mot de passe. Vous voyez une invite semblable à :

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

Modifier le mot de passe lorsque SSH est utilisé pour la première fois

Une fois le mot de passe modifié, vous êtes immédiatement déconnecté et vous devez démarrer une nouvelle connexion SSH.

Une fois l'utilisateur admin créé, utilisez un client SSH de votre choix et connectez-vous au terminal. Connectez-vous avec les identifiants d'administrateur. Voici l'invite qui s'affiche :



Tentative de connexion réussie via SSH au point d'extrémité

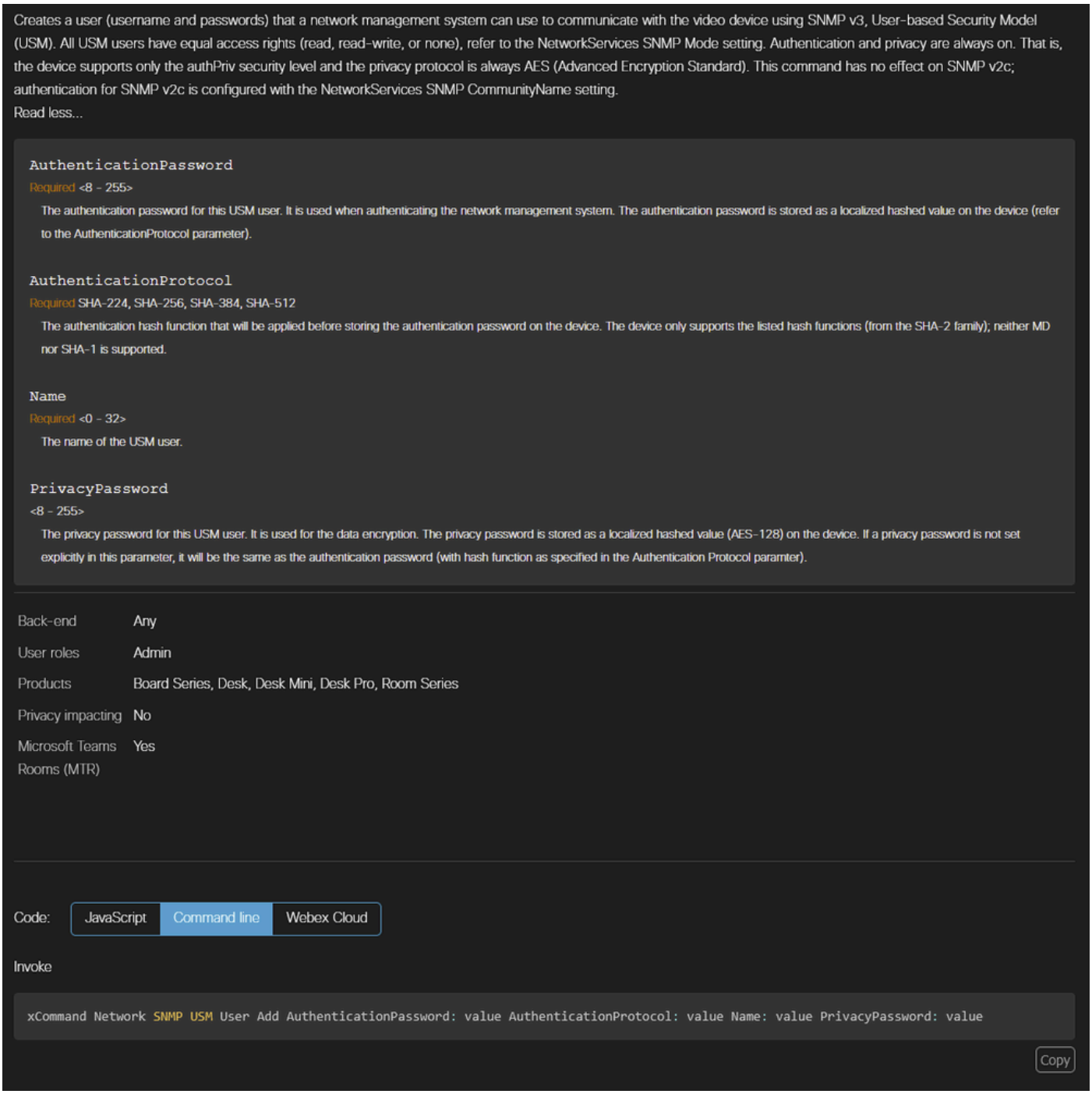
Utilisez la commande Network SNMP USM User Add comme décrit dans cet article. Pour cette démonstration, la commande utilisée est la suivante :

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

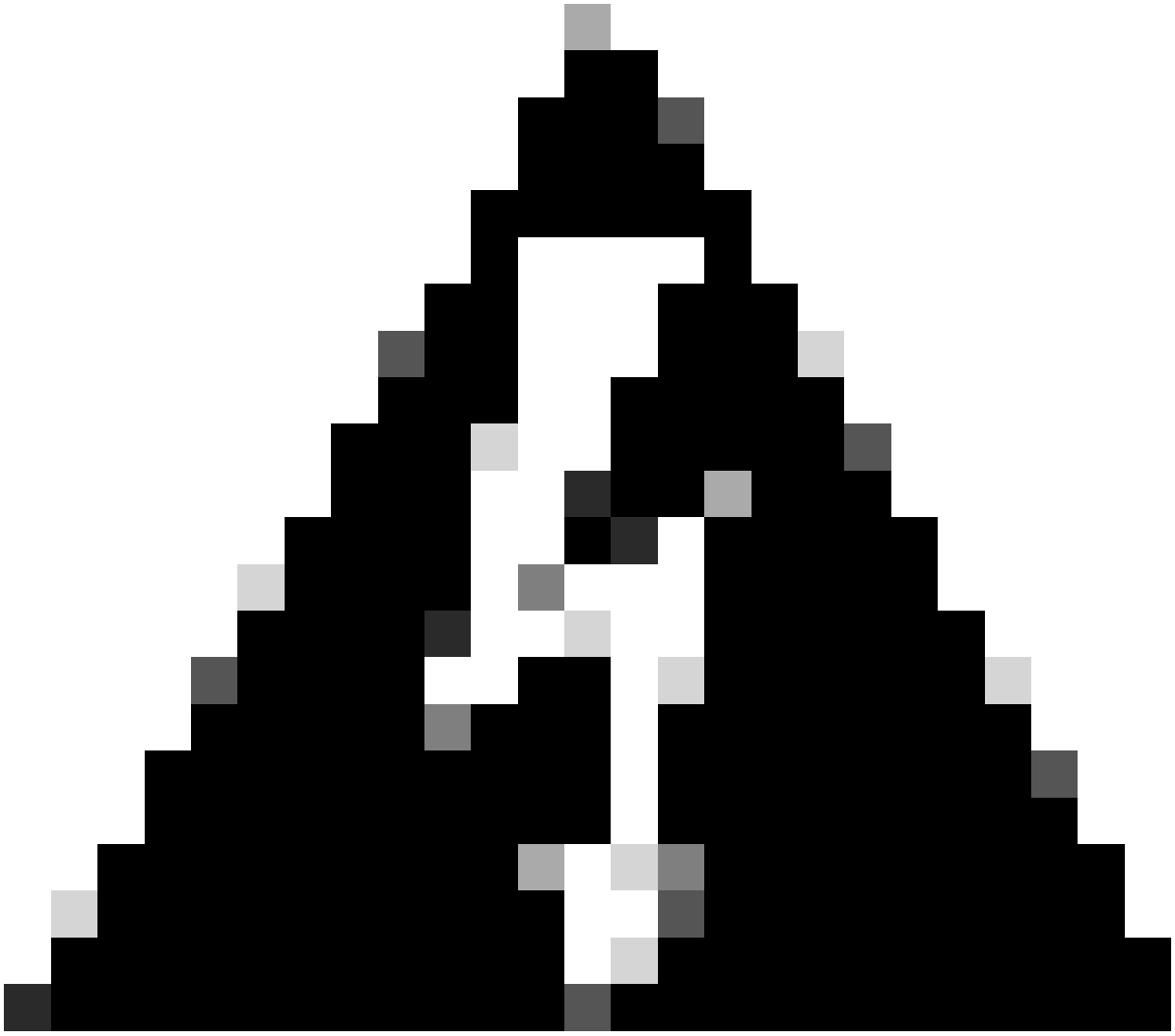
Le résultat de cette commande, lorsqu'elle réussit, est :

Création d'utilisateurs USM via SSH

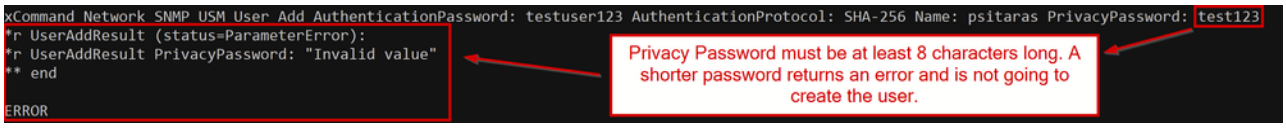
Pour que la commande s'exécute sans erreur, vous devez respecter certaines règles décrites dans la documentation de commande partagée dans ce lien. Pour plus de commodité, les exigences actuelles au moment de la rédaction de ce document pour cette commande sont collées dans cette image, mais vous devez vous assurer de vous référer à ce lien lors de la création de votre utilisateur. À la fin de l'image, notez que la syntaxe exacte de la commande est indiquée.



Syntaxe de la commande USM User Creation de la documentation xAPI



Avertissement : En cas de faute de frappe ou de condition non satisfaite, la commande renvoie une erreur et l'utilisateur ne sera pas créé. Un exemple est fourni, où au lieu de fournir un mot de passe de confidentialité d'au moins 8 caractères, un mot de passe de 7 caractères plus court est fourni :



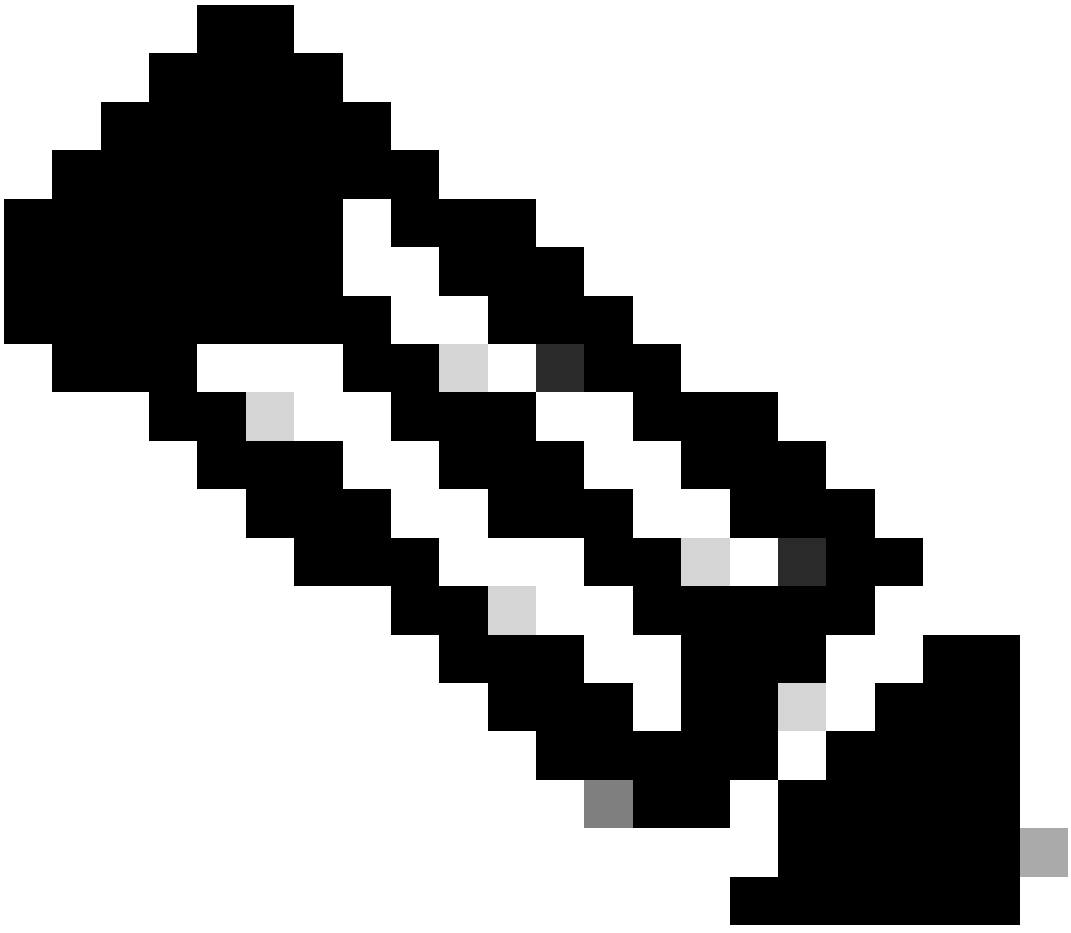
Échec de la création de l'utilisateur USM en raison du mot de passe de confidentialité court

Vous pouvez tester si votre utilisateur a été créé à l'aide de la commande Network SNMP USM User List. Cette commande répertorie tous les utilisateurs USM qui sont stockés sur le périphérique :

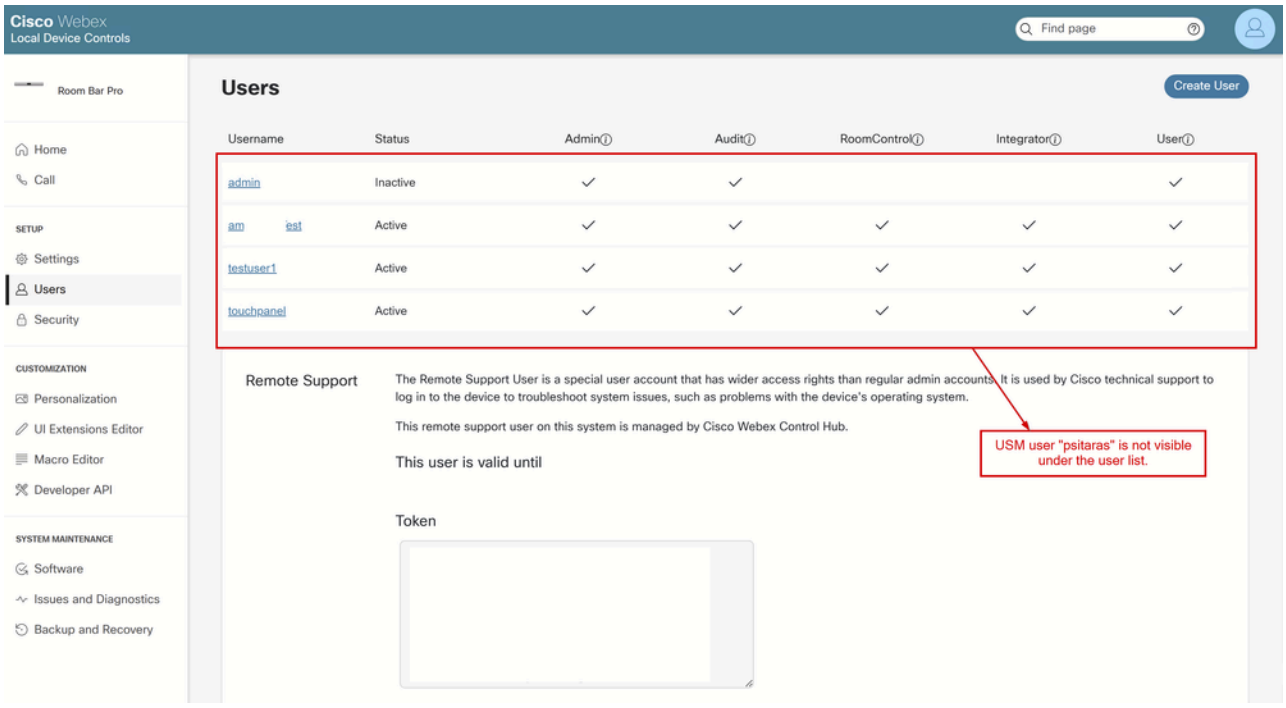
```
xCommand Network SNMP USM User List

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

Commande Network SNMP USM User List utilisée pour confirmer la création de l'utilisateur

À ce stade, il a été confirmé que l'utilisateur psitaras a été créé avec succès. La configuration SNMPv3 est terminée.



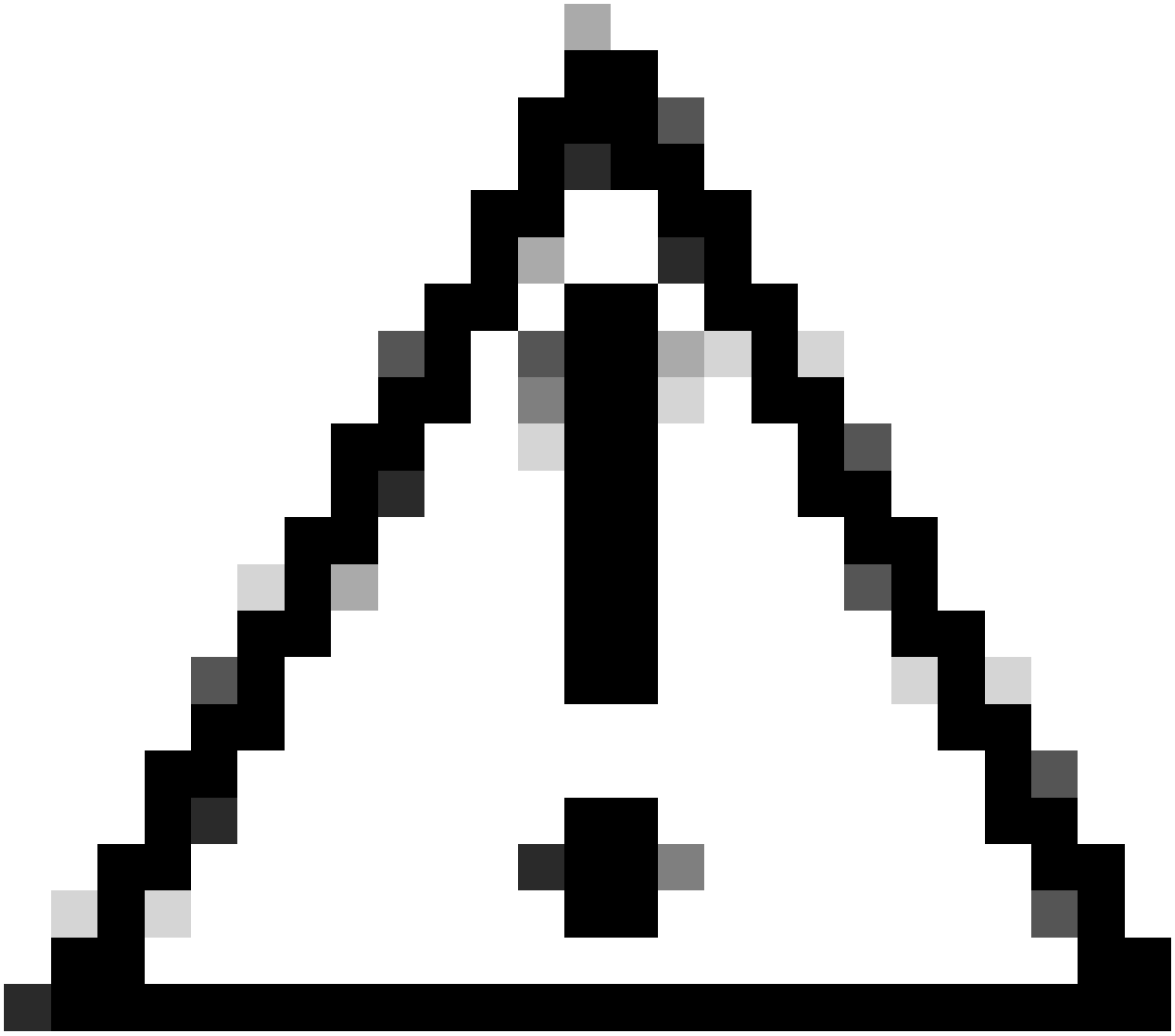
> Remarque : L'utilisateur USM psitaras n'est pas visible dans l'interface utilisateur du terminal sous la section Users. C'est prévu.



Les utilisateurs USM ne sont pas visibles sous Utilisateurs dans l'interface utilisateur graphique du terminal

Test de la configuration SNMPv2c et SNMPv3

À ce stade, vous pouvez tester la configuration SNMPv2c et/ou SNMPv3 avec votre système de gestion de réseau (NMS). Pour cet article, la configuration des travaux pratiques ne contient aucun serveur NMS ou SNMP exécutant un service SNMP. Pour tester la configuration, l'utilitaire appelé snmpwalk est utilisé. Cet utilitaire est installé sur un serveur Linux.



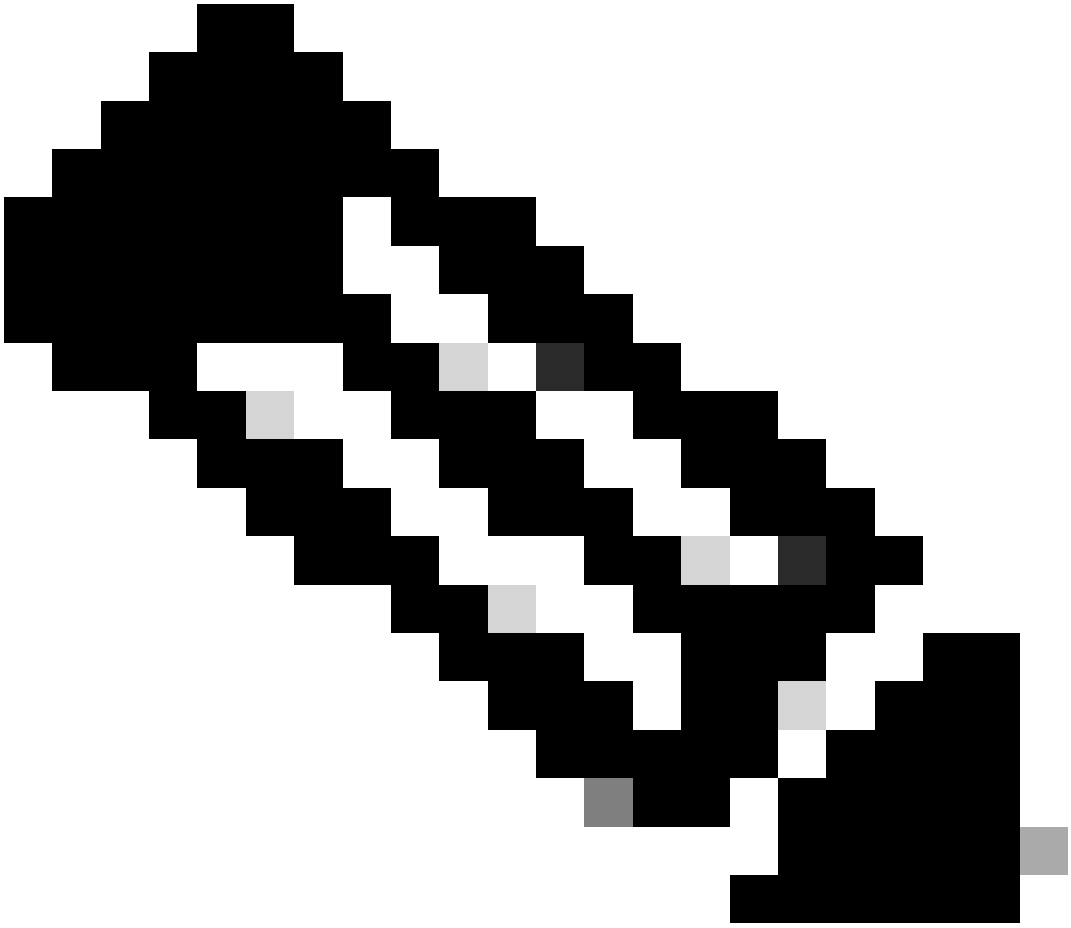
Mise en garde : Snmpwalk n'est pas un outil conseillé pour tester la configuration SNMP sur vos terminaux de collaboration. Il n'est pas pris en charge par les ingénieurs du centre d'assistance technique et vous devez vous familiariser avec l'utilisation de l'outil avant de passer aux tests. Au lieu de snmpwalk, vous pouvez utiliser tout autre outil SNMP ou votre NMS pour tester votre configuration. Snmpwalk est utilisé dans cet article uniquement à titre d'exemple (un outil est nécessaire pour tester la configuration à des fins de démonstration) et il n'y a aucun engagement ou promotion liés à son utilisation.

L'installation de snmpwalk ne fait pas partie de ce guide et est omise. Selon le système d'exploitation de l'ordinateur que vous utilisez pour les tests, les conditions d'installation peuvent varier. Vous devez travailler à son installation avant de procéder au test.

Snmpwalk est un outil qui peut être utilisé pour vérifier la configuration SNMP. Il parcourt les MiB du point d'extrémité et renvoie les informations disponibles. Les terminaux enregistrés dans le cloud exposent 7 identificateurs d'objet (OID) :

- SNMPv2-MIB::sysDescr (lecture),

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



> Remarque : Les adresses IP internes utilisées pour les tests snmpwalk répertoriés sont des adresses IP privées et ne sont plus utilisées. Les travaux pratiques utilisés pour ce guide ont été mis hors service et les périphériques ont été réinitialisés en usine.

Le terminal Cisco Room Kit Pro est configuré avec SNMPv2c. L'authentification se fait à l'aide de chaînes de communauté. Exécutez la commande suivante :

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

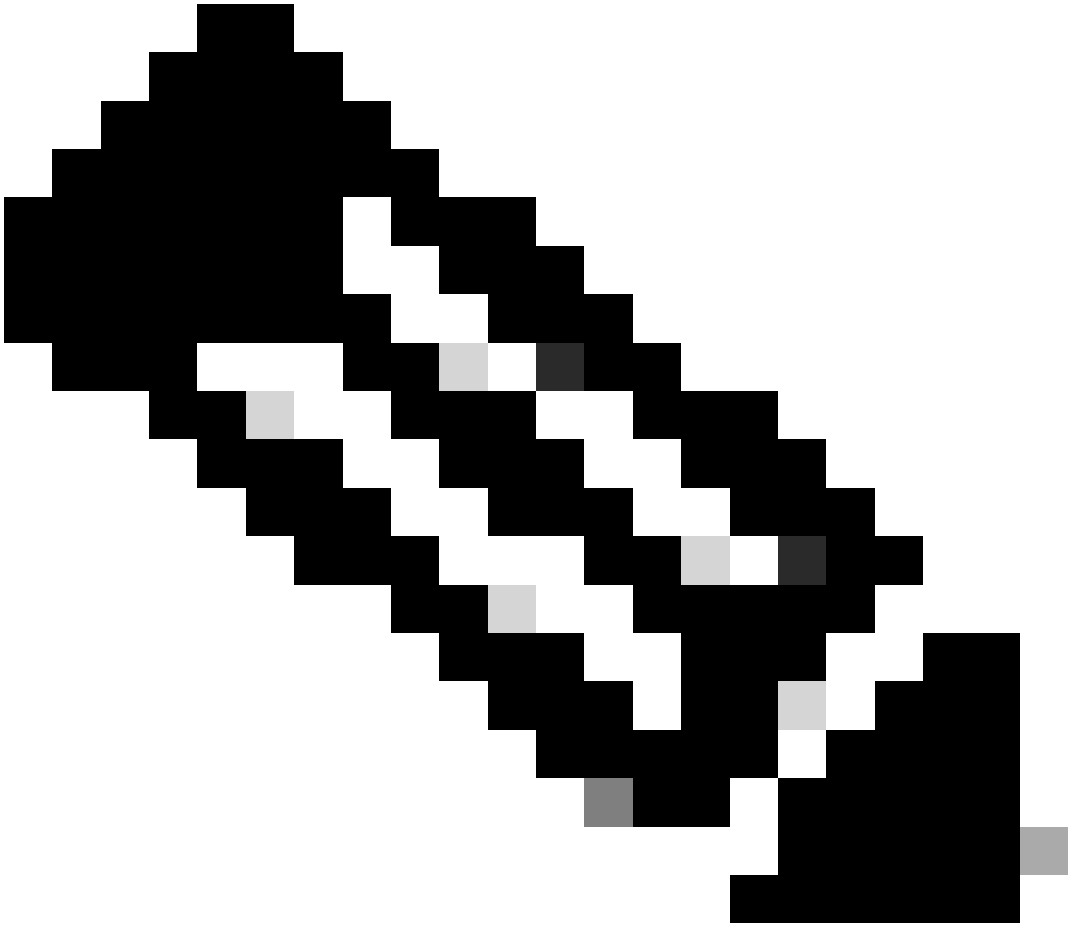
```
# The IP provided is the endpoint's IP

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 renvoie 7 résultats comme prévu. Il y a trois MiB vides :

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

Il existe trois commandes xConfiguration qui peuvent être utilisées pour définir des valeurs pour ces MiB. Établissez une connexion SSH avec le terminal et exécutez les commandes suivantes :

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



Remarque : Au lieu d'utiliser ces trois commandes, vous pouvez modifier ces paramètres à partir du Control Hub, de l'interface utilisateur graphique du terminal ou des API Webex.

Une fois que les commandes ci-dessus sont émises, utilisez snmpwalk à nouveau sur le même terminal. Vous remarquerez que les MiB précédemment vides sont remplis avec les valeurs fournies par les commandes 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: 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)
```

À ce stade, il est confirmé que la configuration SNMPv2c effectuée sur le périphérique Room Kit Pro est opérationnelle.

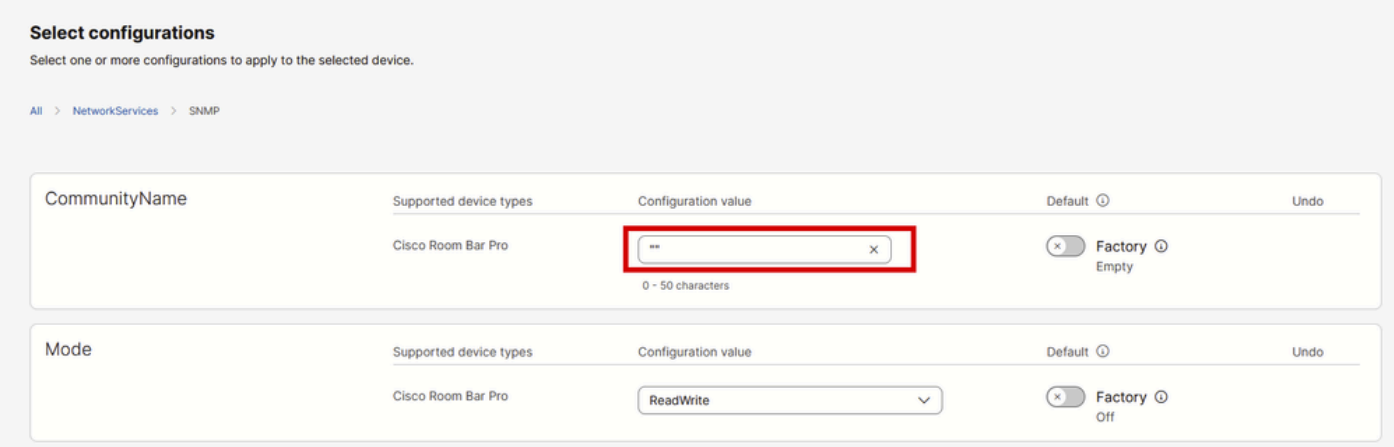
Le point d'extrémité Cisco Room Bar Pro est configuré avec SNMPv3. Pour SNMPv3, vous devez vous assurer d'utiliser l'authentification appropriée. Les chaînes de communauté ne sont pas utilisées. SNMPv3 utilise plutôt des noms d'utilisateur et des mots de passe.

```
# '-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)
```

À ce stade, il est confirmé que la configuration SNMPv3 effectuée sur le périphérique Room Bar Pro est opérationnelle.

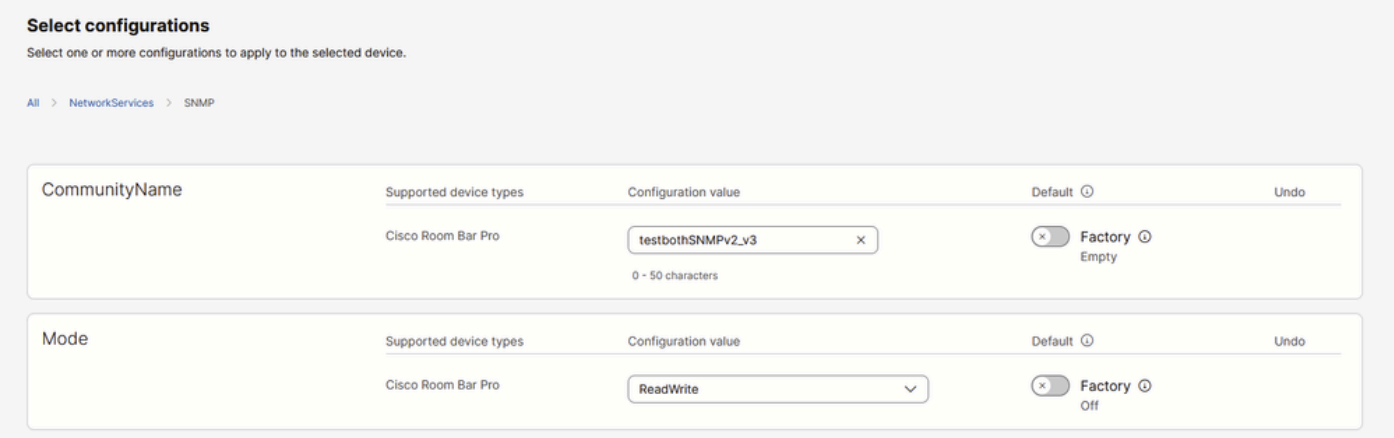
Les protocoles SNMPv2c et SNMPv3 peuvent-ils être actifs simultanément sur un terminal ?

C'est possible. Cependant, pendant la configuration SNMP, vous devez configurer un nom de communauté afin de pouvoir avoir l'authentification SNMPv2c. Pour ce test, le Room Bar Pro des exemples précédents est utilisé. La configuration actuelle de la section Toutes les configurations du Control Hub du terminal est la suivante :



Configurations SNMP des terminaux dans le Control Hub

Notez que le nom de la communauté n'est pas vide. Deux guillemets indiquent que le nom de la communauté est une chaîne vide. Vous pouvez limiter la prise en charge SNMP à la version 3 uniquement, en définissant NetworkServices SNMP CommunityName sur une chaîne vide (""). Vous devez remplacer cette chaîne par un nom de communauté, par exemple, testbothSNMPv2_v3.



Ajouter un nom de communauté pour SNMPv2c dans les paramètres de configuration des terminaux du Control Hub

Il est déjà confirmé que SNMPv3 fonctionne sur le Room Bar Pro. Snmpwalk est utilisé pour tester si SNMPv2c fonctionne également, après avoir configuré le nom de la communauté :

```
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)
```

Plusieurs terminaux peuvent-ils être configurés via le Control Hub avec SNMP ?

Oui, il est possible de configurer plusieurs périphériques à la fois dans le Control Hub. Cet article fournit des informations sur la façon de l'effectuer étape par étape sous la section Configurer plusieurs périphériques.

Détails importants à retenir

- Seuls des MiB spécifiques sont disponibles. Le nombre de MiB disponibles est limité par la conception de l'équipe d'ingénierie qui conçoit les terminaux. Les MiB ne peuvent pas être étendus ou améliorés pour fournir plus d'informations.
- SNMPv2c s'authentifie à l'aide du nom de communauté (également appelé chaîne de communauté), tandis que SNMPv3 s'authentifie à l'aide du nom d'utilisateur et du mot de passe, et offre également le cryptage. Lors du test, assurez-vous que vous utilisez la méthode d'authentification correcte (avec snmpwalk ou un autre outil/NMS) pour le protocole que vous avez configuré.
- L'authentification et la confidentialité sont toujours activées sur SNMPv3. Les points d'extrémité prennent uniquement en charge le niveau de sécurité authPriv et le protocole de confidentialité est toujours AES (Advanced Encryption Standard).
- SNMPv3 est pris en charge uniquement avec les options USM (User-based Security Model). SMNPv3 sur TLS n'est pas pris en charge.
- Les commandes utilisateur USM utilisées pour configurer les utilisateurs pour l'authentification SNMP n'ont aucun effet sur SNMPv2c.
- Le paramètre SNMP CommunityName sur les terminaux n'a aucun effet sur la configuration SNMPv3.
- SNMP CommunityName est sensible à la casse.
- Vous pouvez limiter la prise en charge SNMP à v3 uniquement, en définissant NetworkServices SNMP CommunityName sur une chaîne vide ("").
- SNMPv1 n'est pas pris en charge.
- Pour SNMPv2c et SNMPv3, les points d'extrémité exposent les mêmes identificateurs d'objet (OID).
- Pour SNMPv3, le protocole d'authentification doit faire partie de la famille SHA-2 (ni MD ni SHA-1 n'est pris en charge). Si ce n'est pas le cas, les requêtes SNMP ne s'authentifient pas et restent sans réponse.
- Le mot de passe de confidentialité est stocké en tant que valeur hachée localisée (AES-128) sur le périphérique. Si un mot de passe de confidentialité n'est pas défini explicitement dans ce paramètre, il est défini pour être identique au mot de passe d'authentification (avec une fonction de hachage comme spécifié dans le paramètre Authentication Protocol).
- Les mots de passe/phrases de passe et les noms d'utilisateur doivent être dans des limites de longueur spécifiques. Par exemple, le nom d'utilisateur USM doit comporter jusqu'à 32 caractères et le mot de passe d'authentification doit comporter au moins 8 caractères et au maximum 255 caractères. Si ces conditions ne sont pas remplies, la commande Network

SNMP USM User Add ne parvient pas à créer l'utilisateur et renvoie une erreur.

Contacter le TAC pour résoudre un problème SNMP sur un terminal

Si la configuration SNMP du terminal est terminée, mais qu'un problème a été soulevé, vous devez contacter le TAC et partager ces informations :

- Indiquez votre ID d'entreprise dans le Control Hub et le numéro de série (SN) du terminal concerné.
- Décrivez le scénario auquel vous êtes confronté.
- Indiquez la version SNMP que vous essayez de configurer.
- Fournissez tous les messages d'erreur détectés.
- En cas de problème de configuration du périphérique, expliquez clairement à quelle étape le processus de configuration s'est arrêté et fournissez des captures d'écran. Partagez la commande de configuration qui renvoie une erreur.
- Collectez les journaux des terminaux et téléchargez-les sur votre dossier.
- Partagez l'utilitaire\NMS ou tout autre outil utilisé pour tester votre configuration SNMP. Si vous utilisez un utilitaire pour effectuer un test par rapport à l'agent SNMP des terminaux, fournissez la commande complète utilisée.

Informations connexes

Documentation xAPI du système d'exploitation de la salle - Commandes SNMP

Configurations de périphériques pour les périphériques de la gamme Board, Desktop et Room

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.