Configuration de RADKit dans un environnement de collaboration

Table des matières

Introduction

Ce document décrit les étapes de configuration de RADKit et montre la configuration nécessaire pour commencer à l'utiliser avec les produits de collaboration.

Exigences

Cisco vous recommande d'avoir des connaissances sur les sujets suivants :

- Connaissances de base de tout produit de collaboration VOS
- Connaissances de base de l'accès CLI/SSH

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

- Cisco Unified Communications Manager 12.5 et 14.0

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.

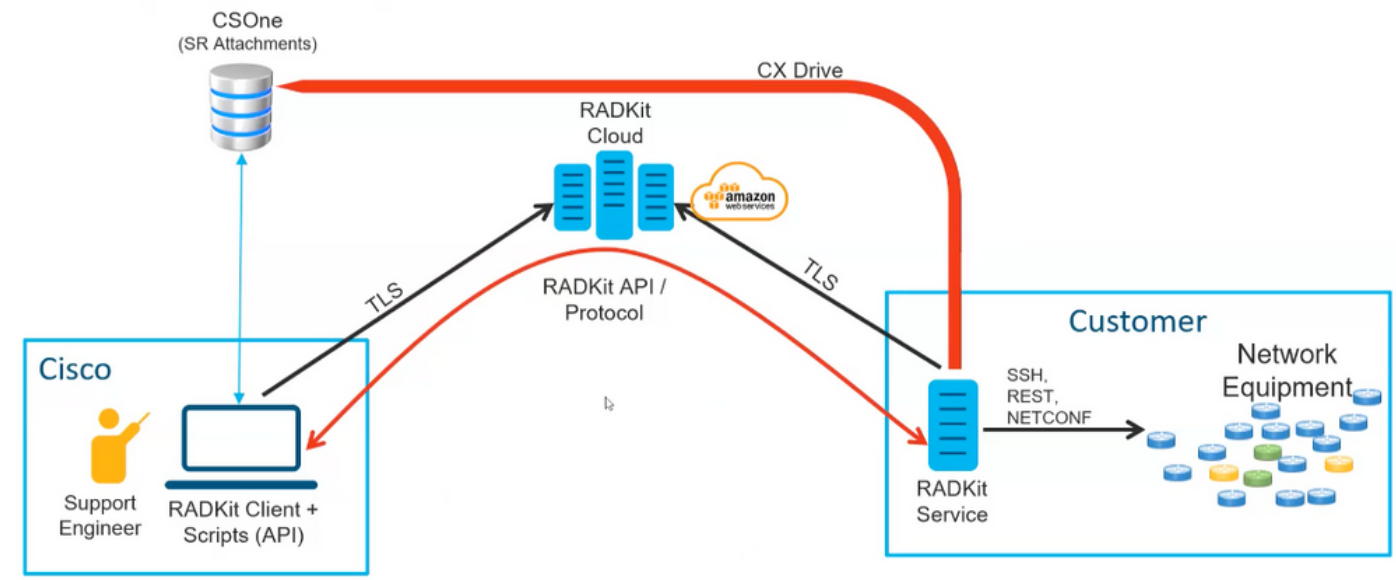
Terminologie

RADKit : Il s'agit d'un connecteur permettant aux ingénieurs et partenaires du TAC Cisco d'accéder à distance et en toute sécurité aux périphériques des utilisateurs. Il prend en charge plusieurs protocoles pour interagir avec des périphériques, tels que SSH ou HTTP/HTTP.

Service RADKit : C'est le côté serveur. Il est géré et entièrement géré par l'utilisateur. Du côté du serveur, l'utilisateur contrôle qui peut accéder aux périphériques et pendant combien de temps. Le service Radkit doit être connecté aux périphériques du réseau pour pouvoir y accéder.

Client RADKit : C'est le côté client. Il s'agit du PC utilisé pour se connecter aux périphériques du réseau utilisateur.

Architecture RADKit



Architecture RADKit

Installation de RADKit

Étape 1. Accédez à https://radkit.cisco.com et cliquez sur Downloads, puis accédez au dossier release.

Étape 2. Cliquez sur la dernière version.

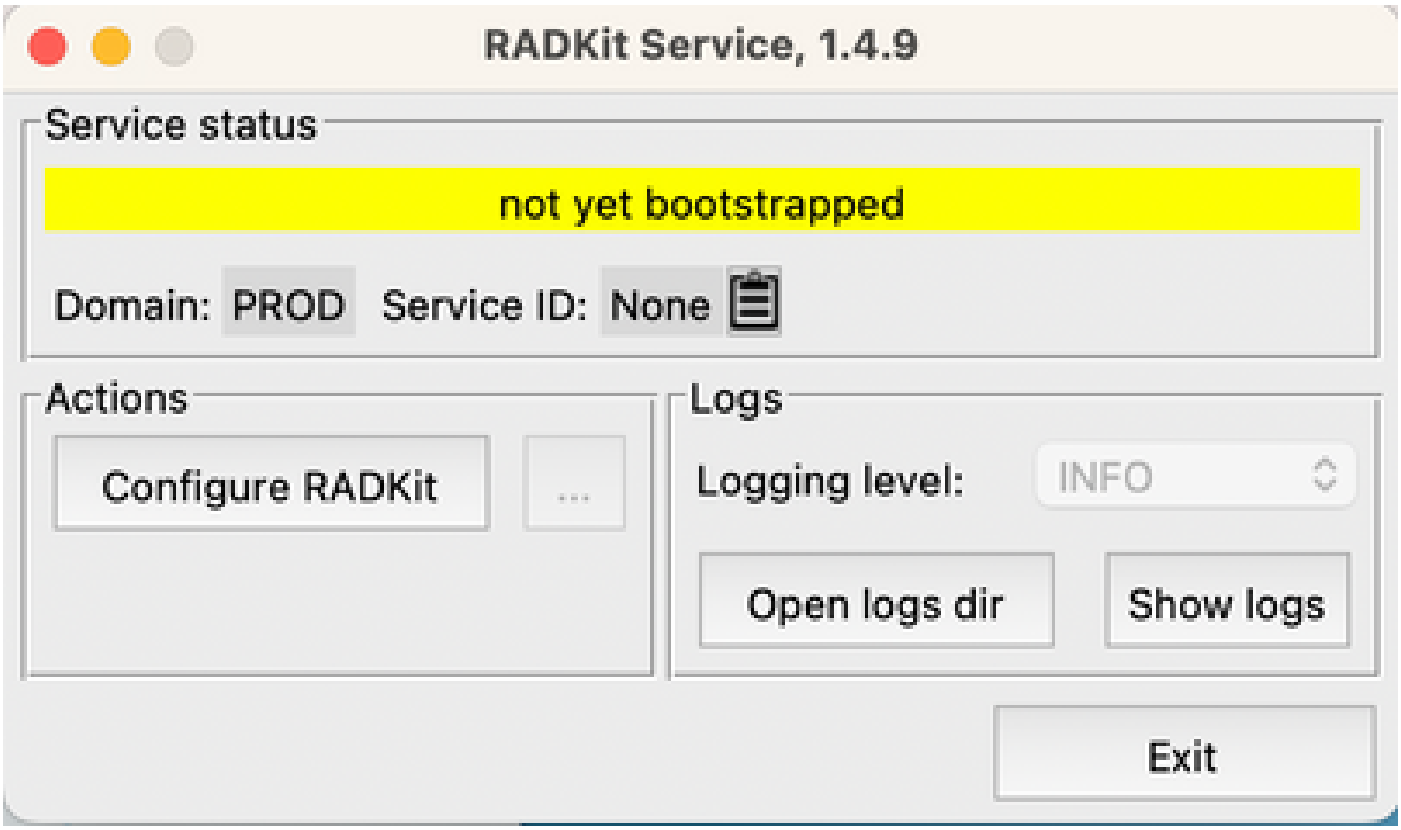
Étape 3. Téléchargez le fichier approprié en fonction de votre système d'exploitation.

Étape 4. Exécutez le programme d'installation sur le PC ou le serveur. Dans le cadre de l'installation, Radkit doit installer trois applications : Radkit Service, Radkit Client et Radkit Network Console.

Service RADKit (côté utilisateur)

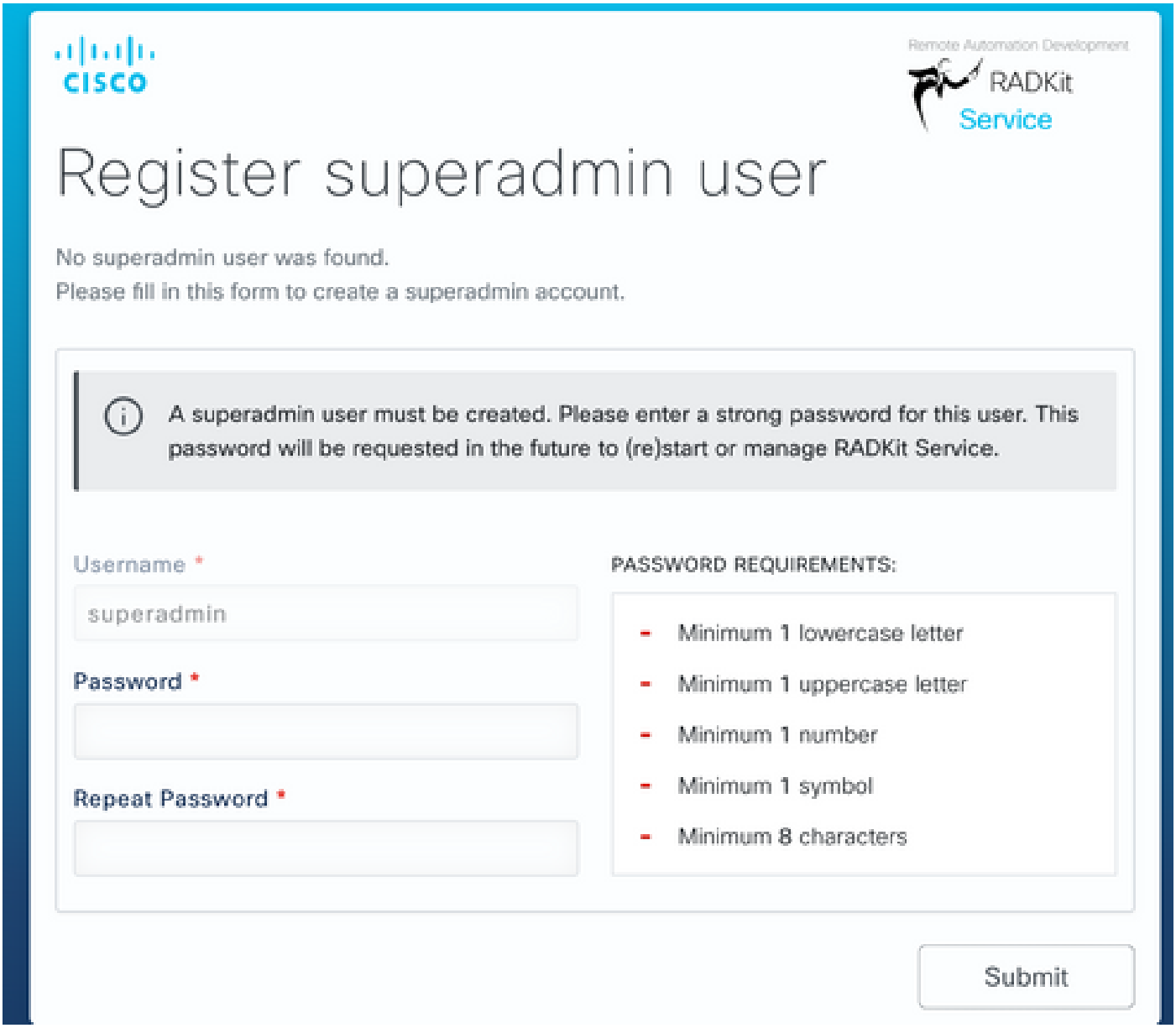
Intégration

Étape 1. Pour commencer à configurer le service RADKit, accédez à Applications et localisez RADKit Service. La première fois que vous exécutez, il affiche un message "not yet bootstrapped".



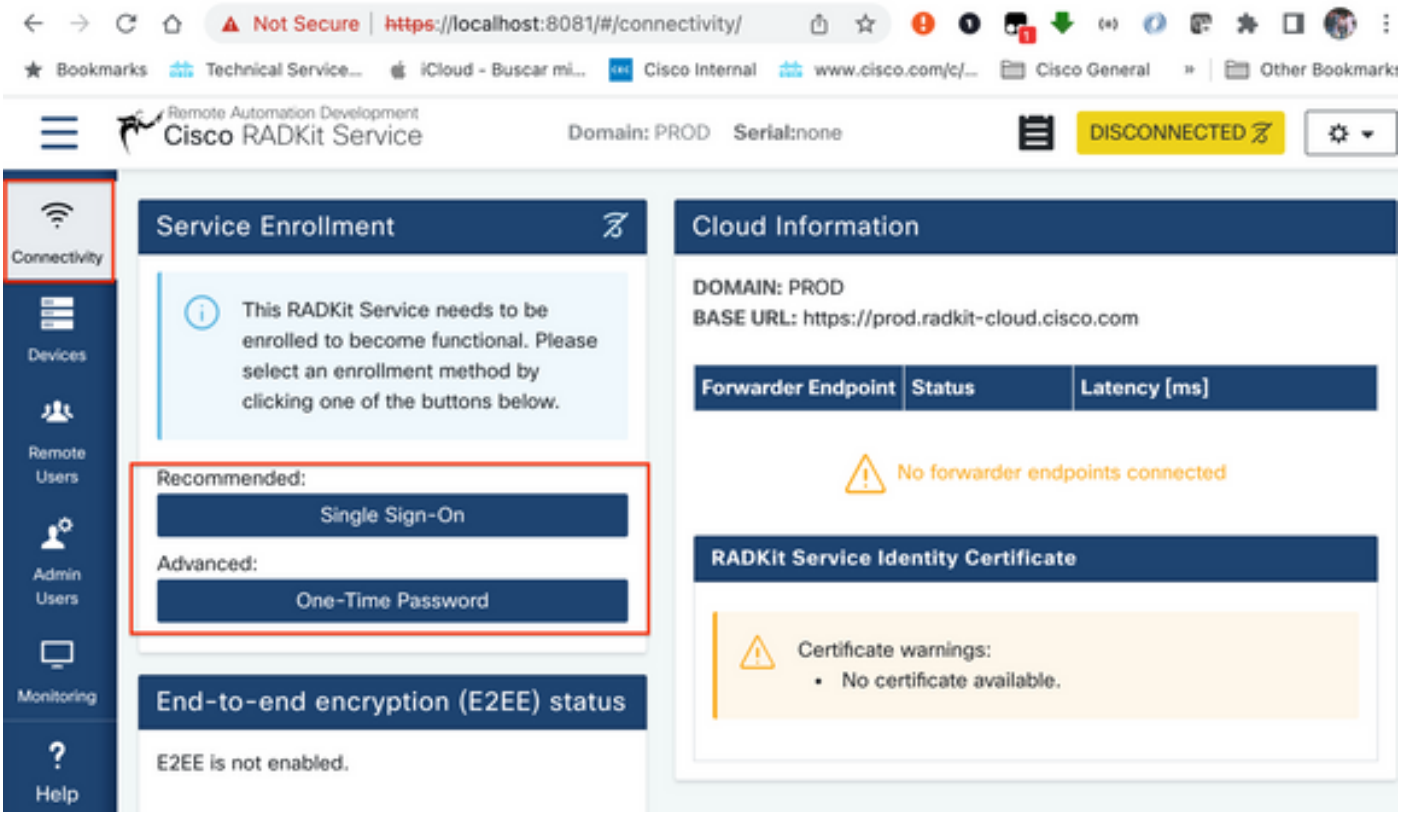
Étape 2. Cliquez sur Configure RADKit, le navigateur apparaît automatiquement avec l'URL https://localhost:8081/bootstrap.

- Créez un mot de passe pour l'utilisateur superadmin et cliquez sur Submit.
- Ce nom d'utilisateur et ce mot de passe superadmin sont demandés chaque fois que le service est démarré ou configuré.

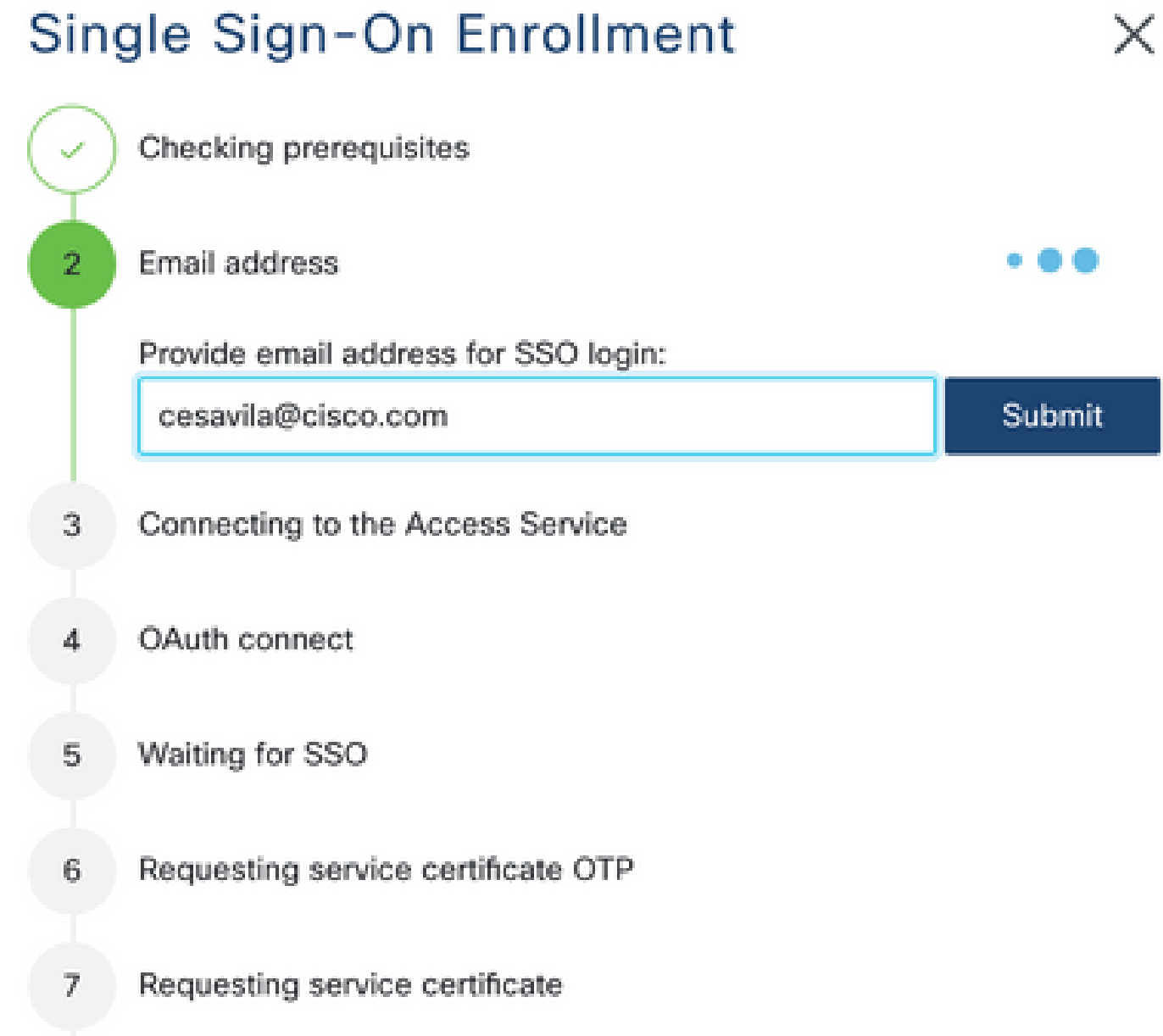


Étape 3. Une fois que vous avez cliqué sur Submit, le navigateur vous redirige vers https://localhost:8081/#/connectivity/.

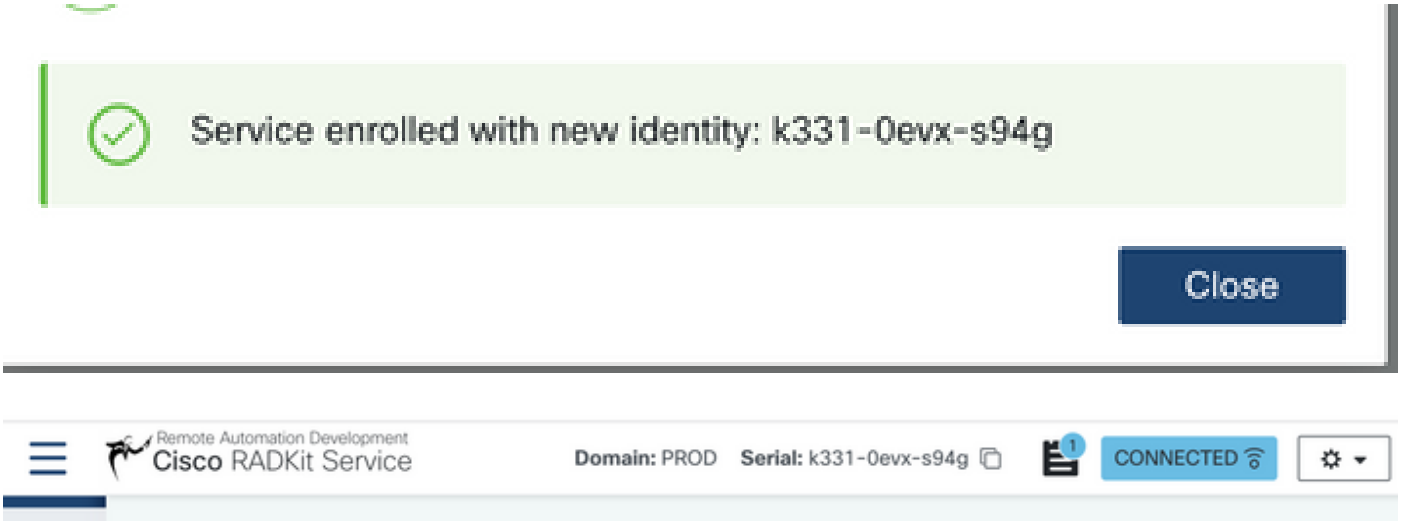
Sous Connectivity > Service Enrollment, il existe deux méthodes d'authentification : Authentification unique et mot de passe à usage unique.

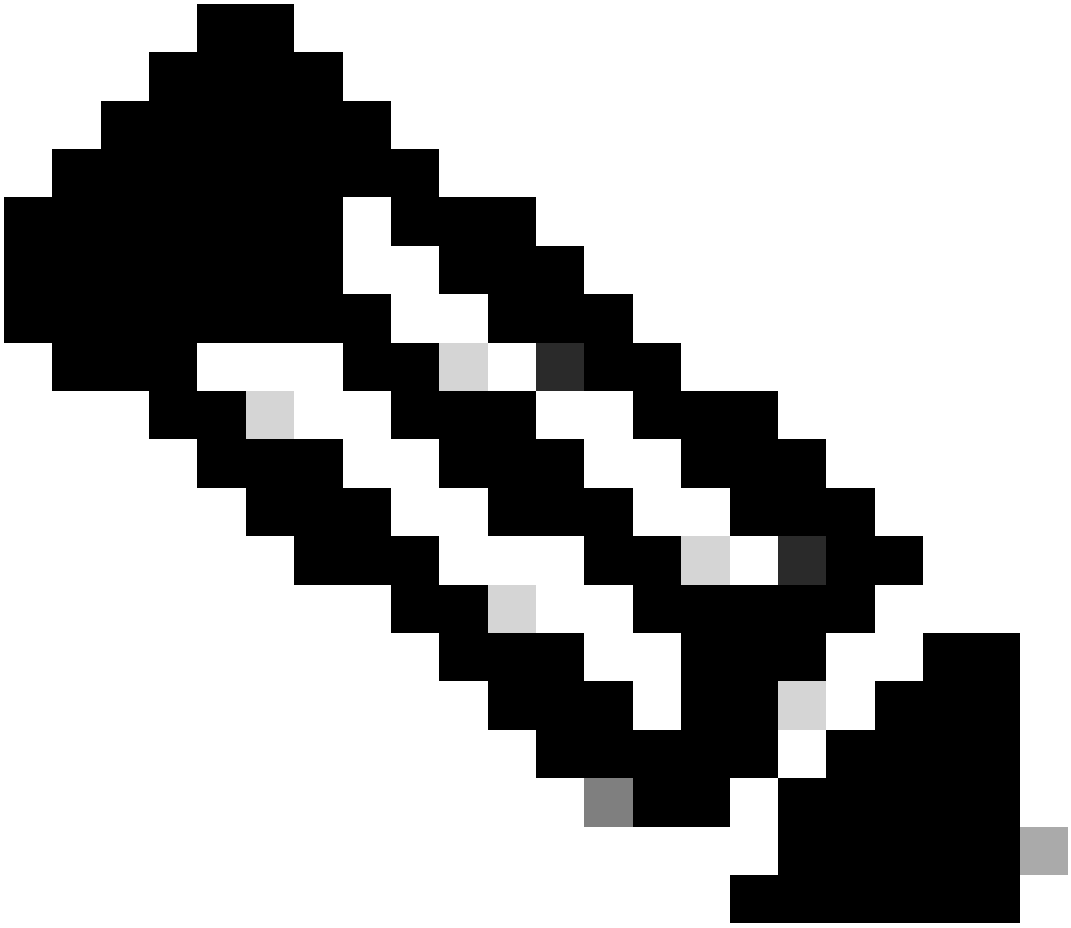


Étape 4. Vous pouvez utiliser l'authentification unique à condition que vous disposiez de votre CEC.

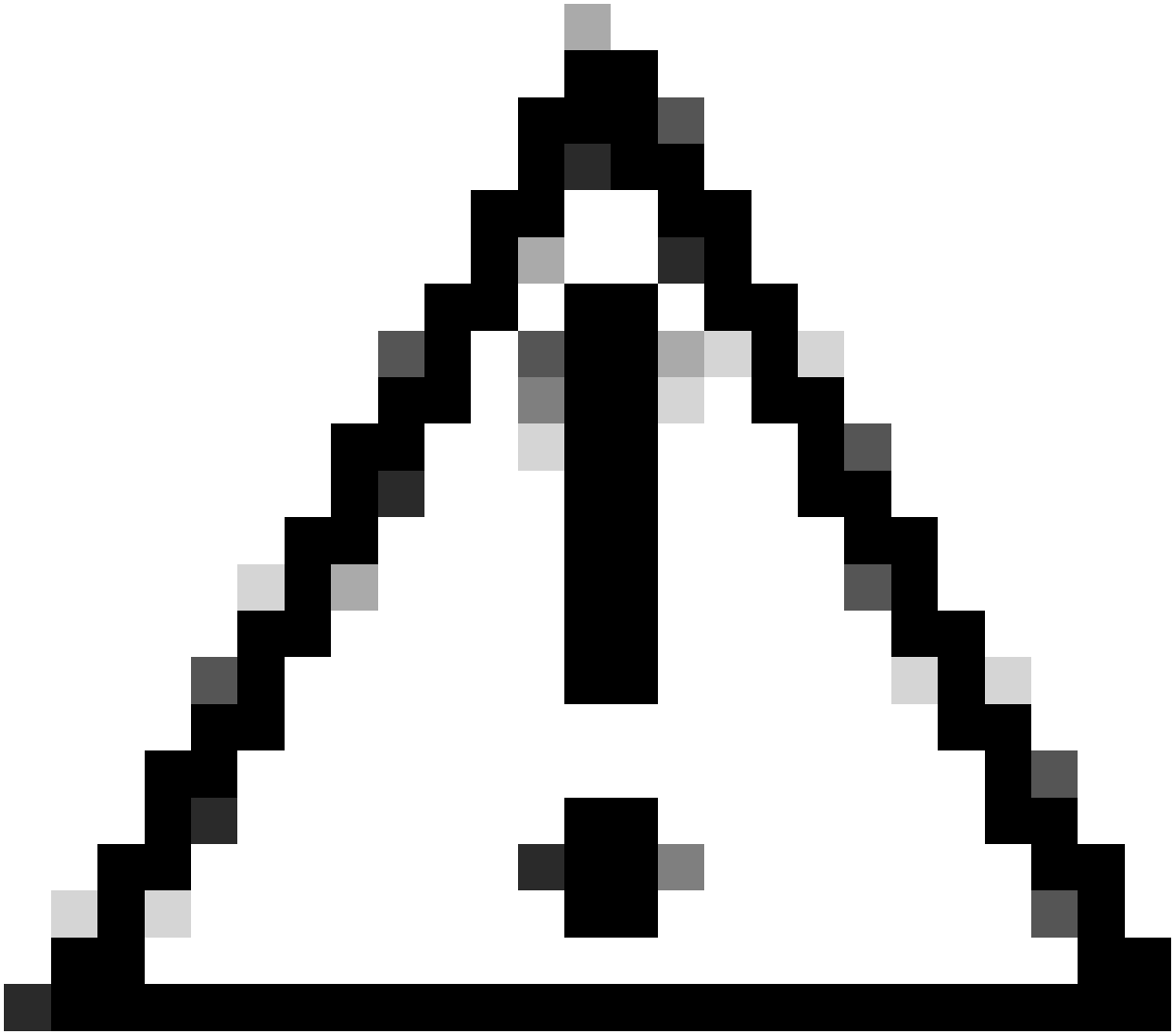


Étape 5. Terminez l'Assistant et suivez les étapes jusqu'à ce qu'il affiche « Service inscrit avec une nouvelle identité : xxxx-xxxx-xxxx", et lorsque vous cliquez sur Close, le service apparaît comme Connected.





Remarque : Un compte Cisco est nécessaire pour activer le service RADKit.

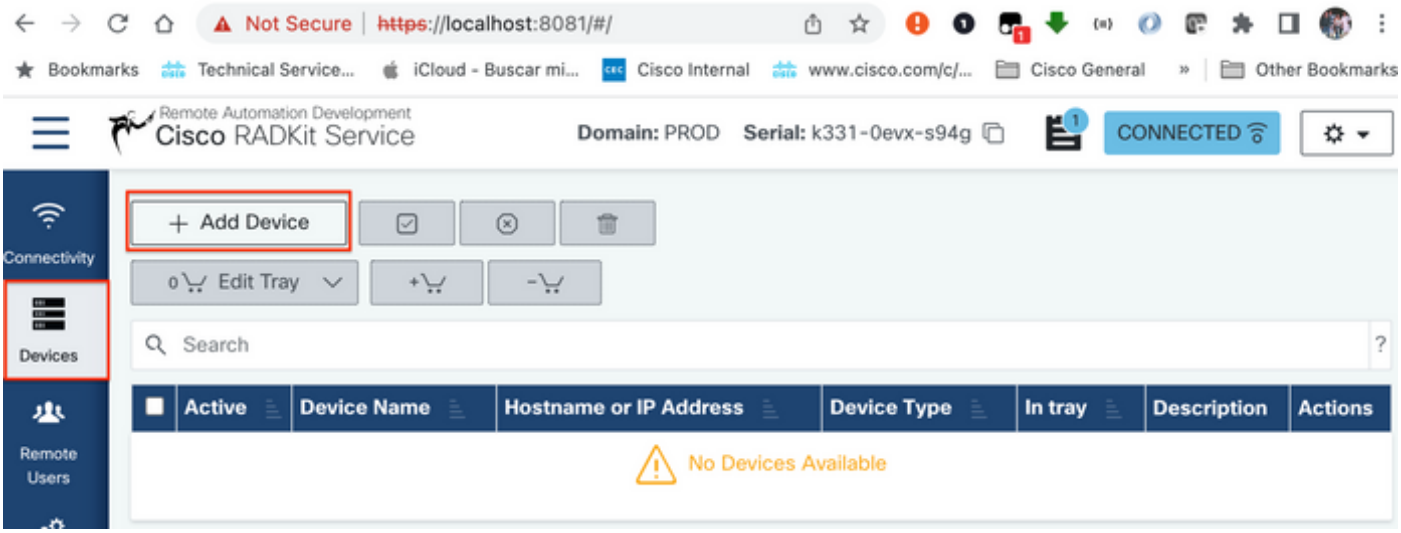


Mise en garde :

- Si le serveur sur lequel le service RADKit est exécuté nécessite la définition d'un proxy, outre la définition du proxy sur le serveur/PC lui-même, une variable d'environnement doit également être définie pour que le service RADKit fonctionne RADKIT_CLOUD_CLIENT_PROXY_URL=http://proxy.example.com:80.

Ajouter des périphériques

Étape 1. Accédez à Devices et cliquez sur Add Device.

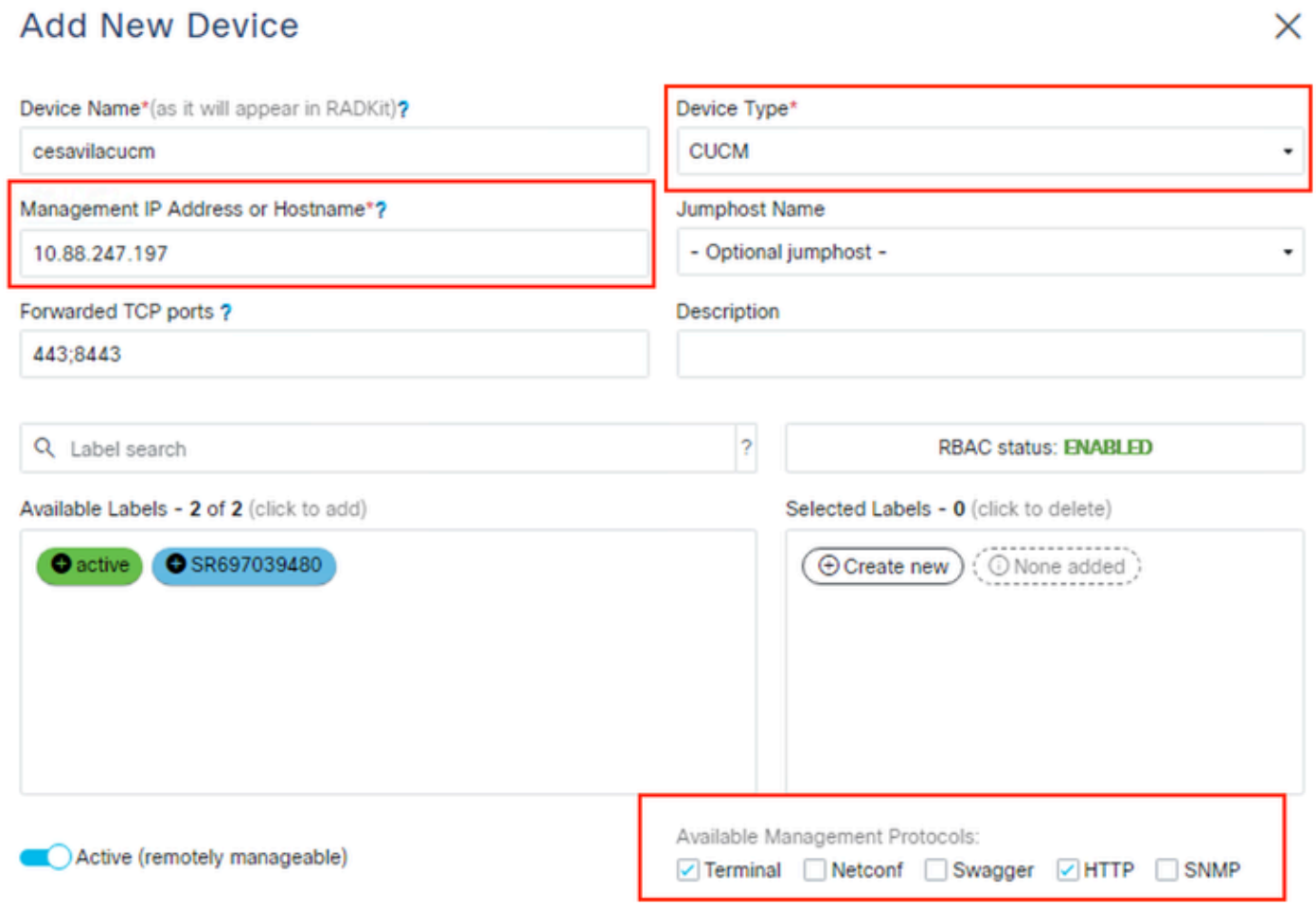


Étape 2. Vous devez configurer les détails suivants :

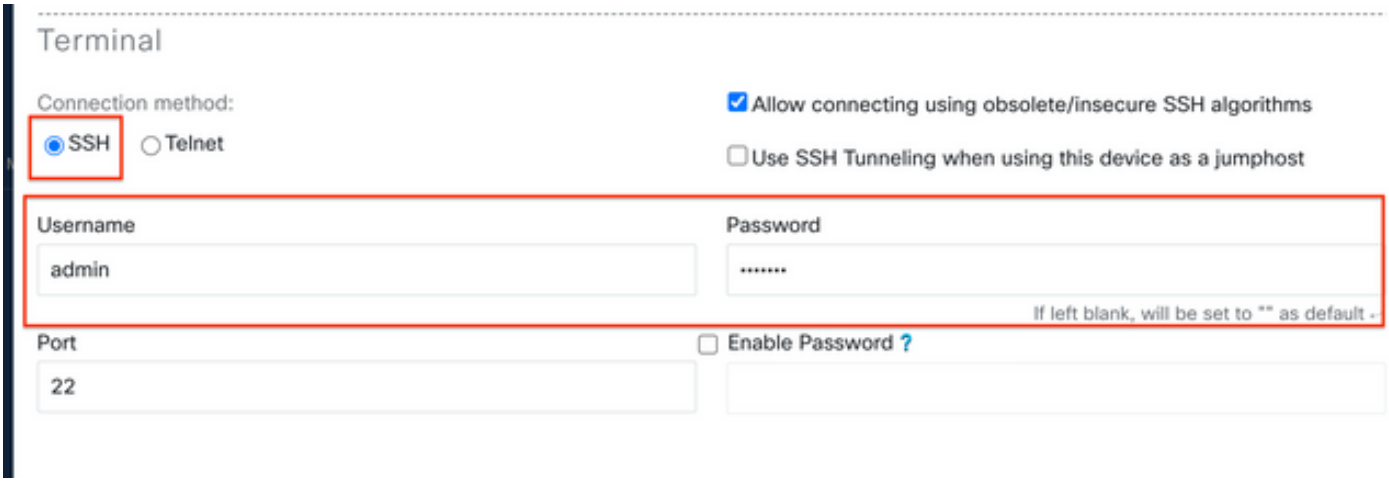
- Nom du périphérique
- Adresse IP de gestion ou nom d'hôte
- Type de périphérique

En outre, vous devez configurer les ports TCP transférés, qui sont des ports utilisés par le périphérique qui doivent être accessibles à partir du client RADKit. Dans cet exemple, les ports utilisés sont 443 pour l'accès GUI et 8443 pour RTMT.

Enfin, sélectionnez les protocoles de gestion disponibles, dans ce cas Terminal et HTTP.



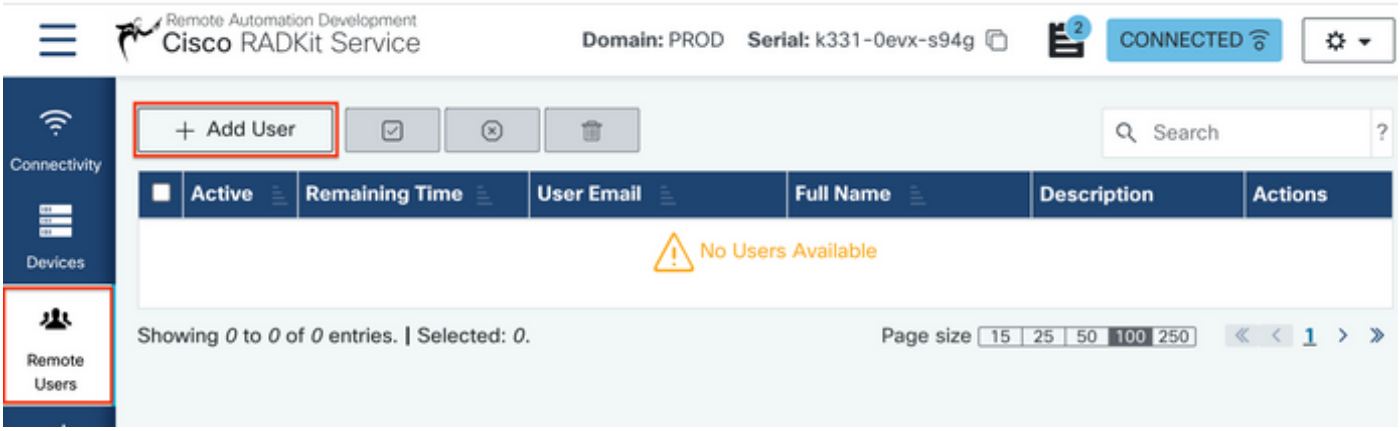
Étape 3. Pour chaque protocole de gestion, configurez les paramètres appropriés et cliquez sur Add & Close.



Étape 4. Une fois ajouté, le périphérique doit être affiché dans la liste des périphériques ; il peut être activé/désactivé pour l'accès à distance.

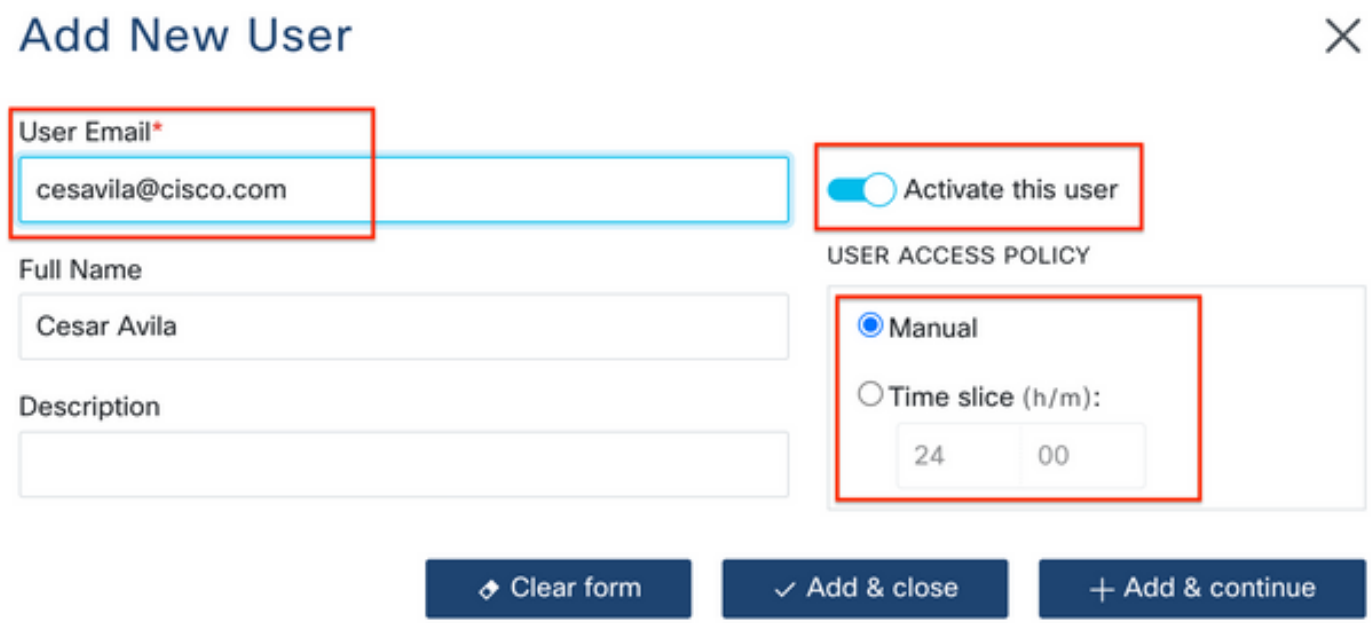
Autoriser les utilisateurs distants

Étape 1. Afin d'accorder à l'utilisateur l'accès aux périphériques configurés dans le service RADKit, accédez à Utilisateurs distants et sélectionnez Ajouter des utilisateurs.



Étape 2 : configuration des informations utilisateur :

- Adresse électronique
- Nom complet (facultatif)
- Activez l'utilisateur.
- Spécifiez si l'activation doit être contrôlée manuellement ou définissez un délai pour accorder l'accès à cet utilisateur.



Étape 3. Sélectionnez Ajouter et fermer.

Client RADkit (côté TAC)

Connexion

Étape 1. Sur le PC client, accédez à Applications et localisez RADkit Client.

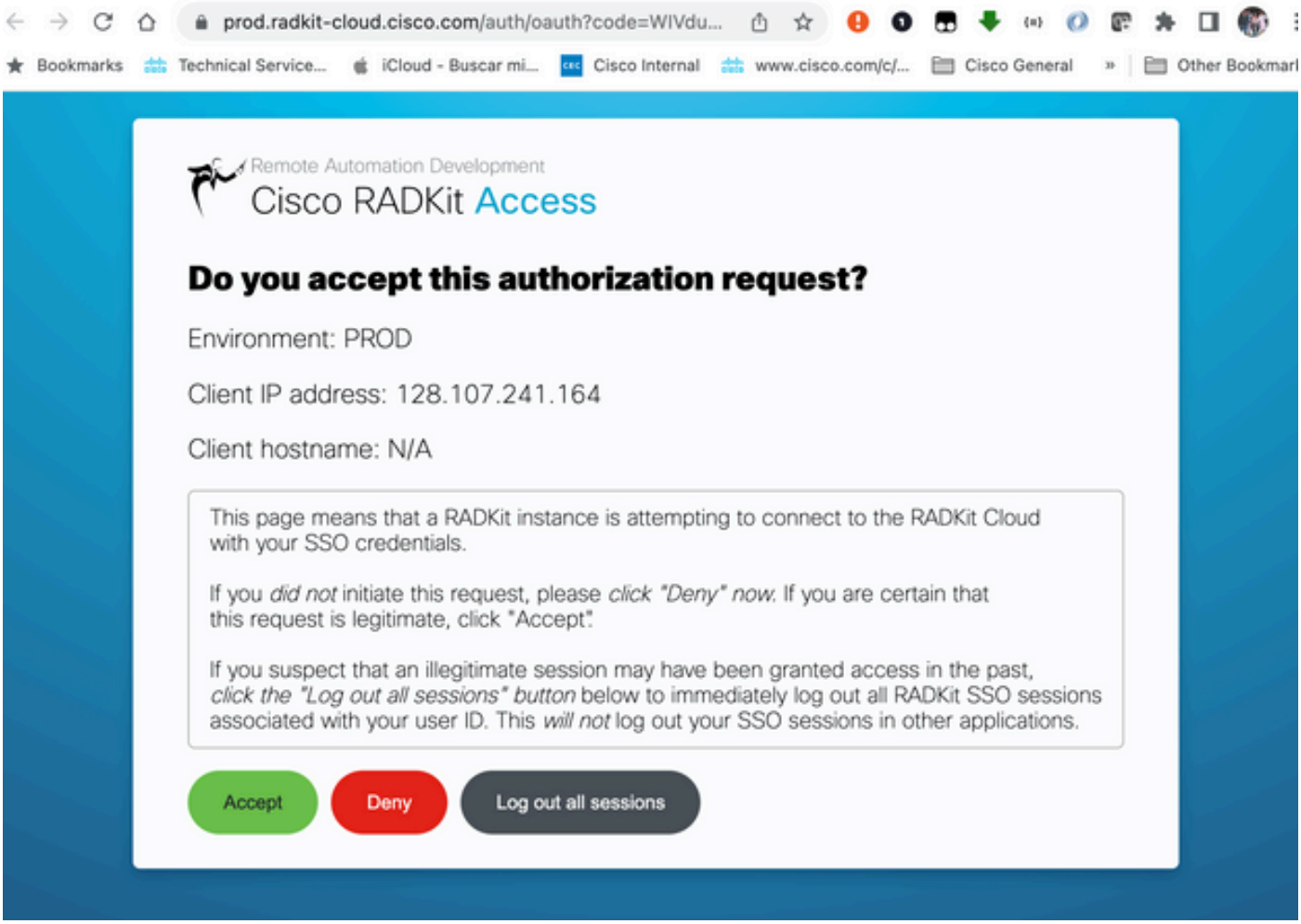
Étape 2 : création d'une instance de client avec votre connexion SSO

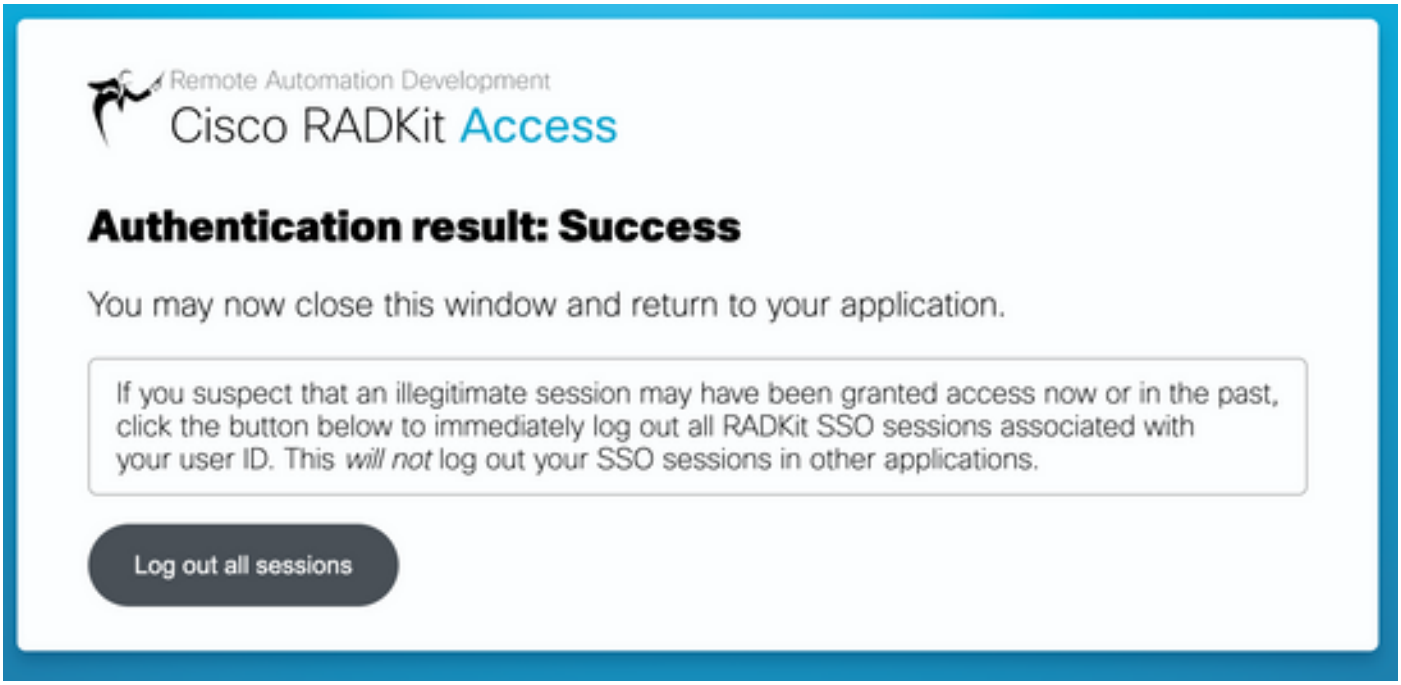
<#root>

>>>

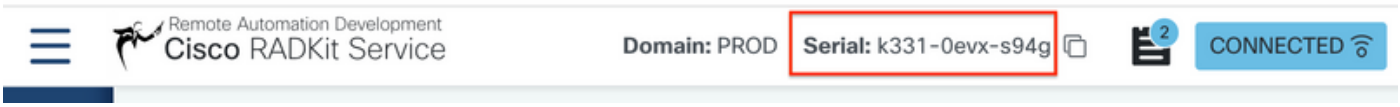
```
client = sso_login("cesavila@cisco.com")
```

Étape 3. Acceptez la demande d'autorisation SSO ouverte automatiquement sur votre navigateur.





Étape 4. Créez une instance de service à l'aide du numéro de série généré par l'utilisateur à partir de la phase RADKit Service - Onboarding.

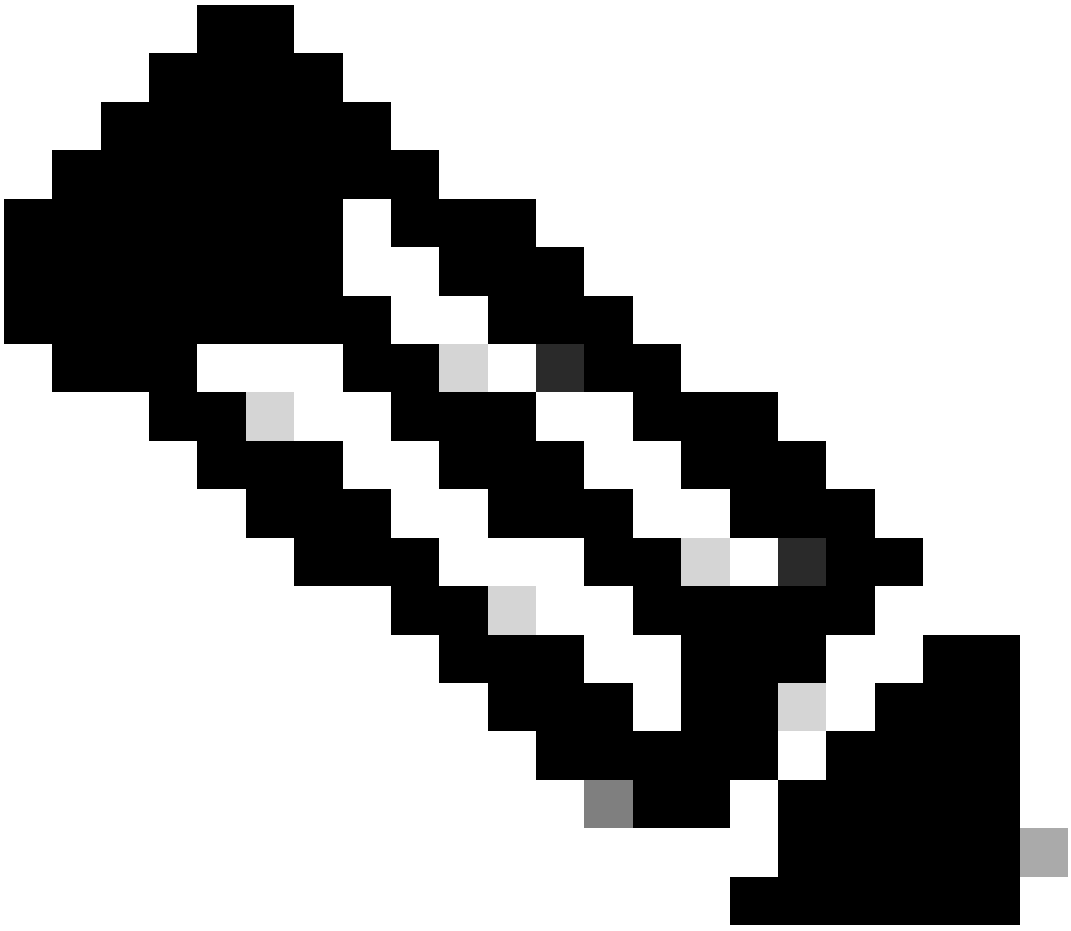


<#root>

>>>

```
 service = client.service("k331-0evx-s94g")
```

```
>>> service = client.service("k331-0evx-s94g")
05:16:36.349Z INFO  | internal | Connecting to forwarder [uri='wss://prod.radkit-cloud.cisco.com/forwarder-2/websocke
t/']
05:16:37.153Z INFO  | internal | Connection to forwarder successful [uri='wss://prod.radkit-cloud.cisco.com/forwarder
-2/websocket/']
05:16:39.523Z INFO  | internal | Connecting to forwarder [uri='wss://prod.radkit-cloud.cisco.com/forwarder-3/websocke
t/']
05:16:40.333Z INFO  | internal | Connection to forwarder successful [uri='wss://prod.radkit-cloud.cisco.com/forwarder
-3/websocket/']
```



Remarque : service est une variable qui peut être n'importe quoi.

Étape 5 : vérification des périphériques disponibles pour l’accès

<#root>

>>>

service.inventory

```
>>>
>>> service.inventory
<radkit_client.sync.device.DeviceDict object at 0x10d7728e0>
name          host           device_type    Terminal    Netconf    Swagger    HTTP    description    failed

------------  -------------  -------------  ----------  ---------  ---------  ------  -------------  --------
cesavilacucm  10.88.247.197  UNKNOWN        True        False      False      True                   False
```

Pour actualiser la liste d'inventaire, utilisez la commande update_inventory.

<#root>

>>> service.update_inventory().wait()

Accès SSH

Étape 1 : création d'un objet à partir de la liste d'inventaire

<#root>

>>> cucm = service.inventory['cesavilacucm']

```
>>> service.inventory
<radkit_client.sync.device.DeviceDict object at 0x10d7728e0>
name          host           device_type    Terminal    Netconf    Swagger    HTTP    description    failed

------------  -------------  -------------  ----------  ---------  ---------  ------  -------------  --------
cesavilacucm  10.88.247.197  UNKNOWN        True        False      False      True                   False

Untouched inventory from service k331-0evx-s94g.
>>>
>>> cucm = service.inventory["cesavilacucm"]
```

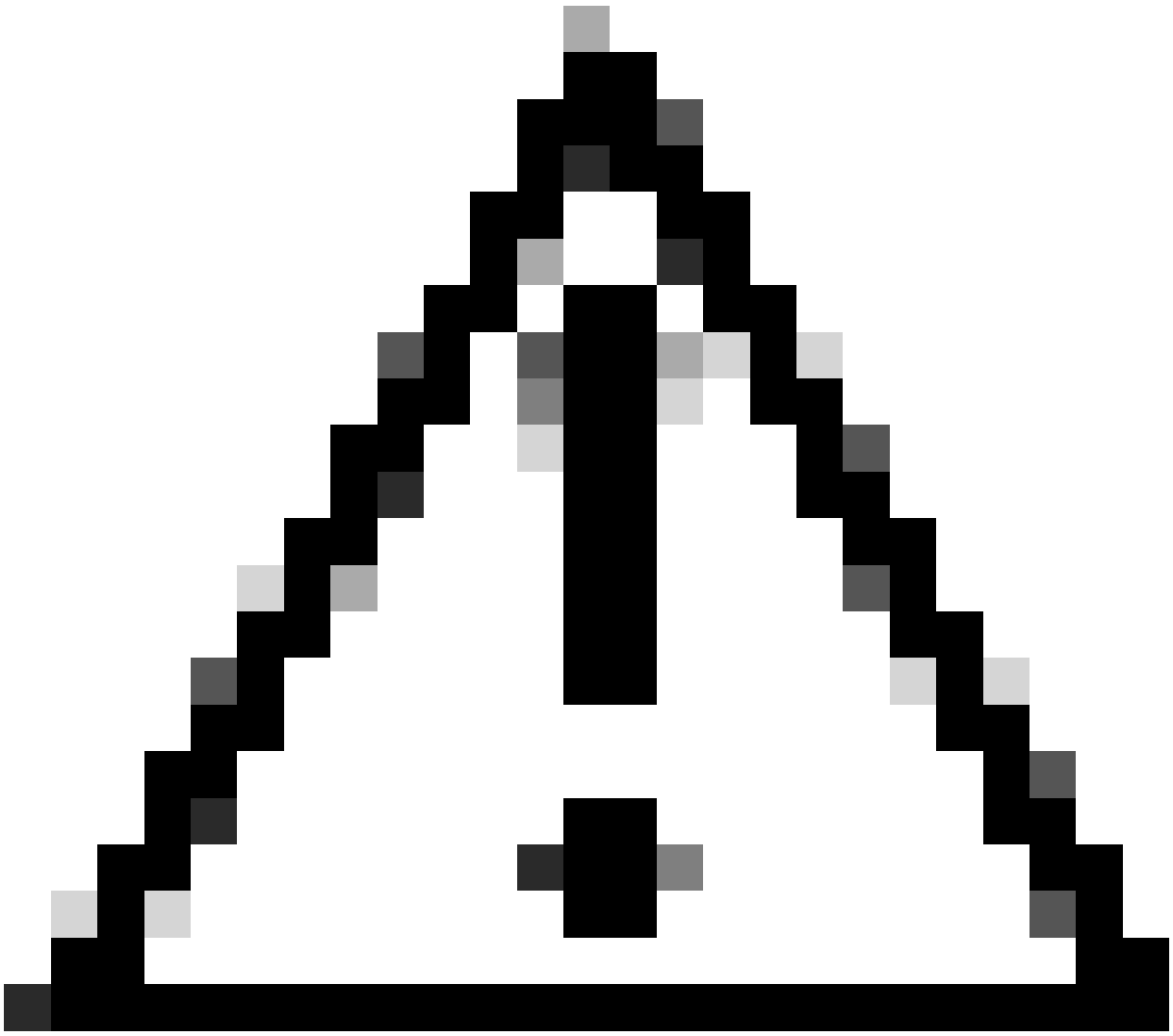
Étape 2 : Démarrez la session SSH avec la commande interactive.

<#root>

>>> cucm.interactive()

```
>>>
>>> cucm.interactive()
05:35:23.882Z INFO  | internal | starting interactive session (will be closed when detached)
05:35:24.765Z INFO  | internal | Session log initialized [filepath='/Users/cesavila/.radkit/session_logs/client/20230
-cesavilacucm.log']
[
[  Attaching to cesavilacucm ...
     Type: ~.  to detach.
           ~?  for other shortcuts.
   When using nested SSH sessions, add an extra ~ per level of nesting.

Command Line Interface is starting up, please wait ...

   Welcome to the Platform Command Line Interface

VMware Installation:
        2 vCPU: Intel(R) Xeon(R) Silver 4114 CPU @ 2.20GHz
        Disk 1: 200GB, Partitions aligned
        4096 Mbytes RAM
        WARNING: DNS unreachable
        WARNING: Ungraceful shutdown detected - A rebuild of this node is highly recommended
        to ensure no negative impact(such as configuration or file system corruption). For
        rebuild instructions, see the installation guide.

admin:
```

Étape 3. Vous pouvez maintenant gérer le périphérique normalement.



Mise en garde :

- Soyez toujours conscient de notre responsabilité lorsque vous travaillez dans un environnement utilisateur.
- RADKit doit être utilisé comme outil de collecte de données.
- N'effectuez jamais de modifications sans l'autorisation de l'utilisateur.
- Documentez toutes vos conclusions dans les notes de cas.

Accès GUI

- Proxy HTTP

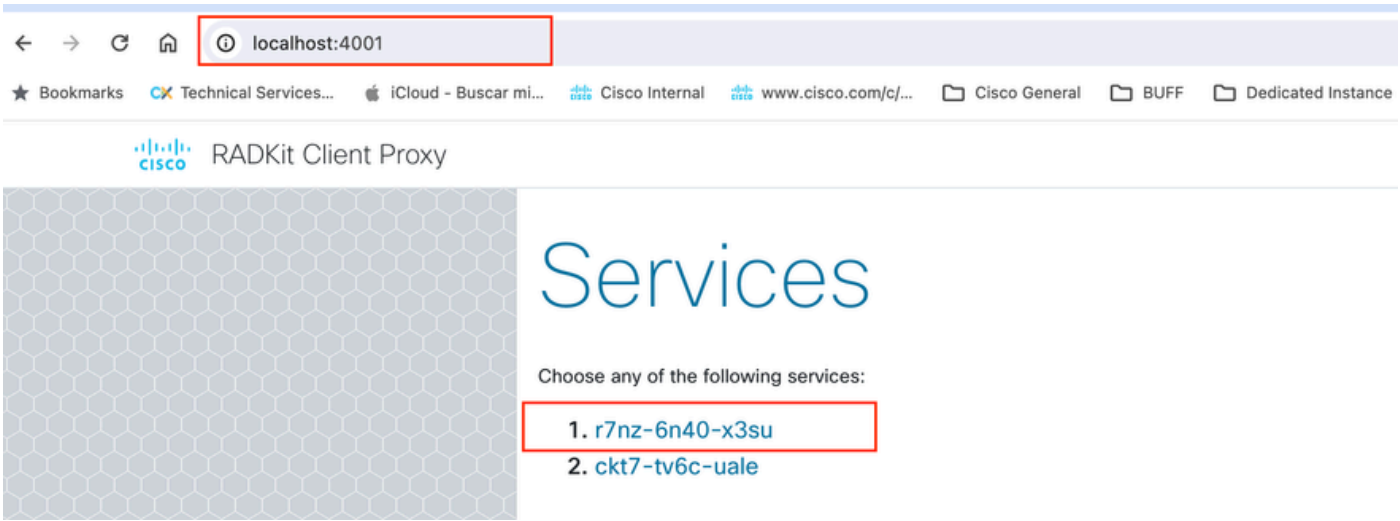
Étape 1 : assurez-vous que les informations d'identification HTTP sont ajoutées au service RADKit sur la configuration du périphérique.

Étape 2 : démarrage du proxy HTTP sur le client Radkit et définition du port local utilisé pour la connexion au proxy

<#root>

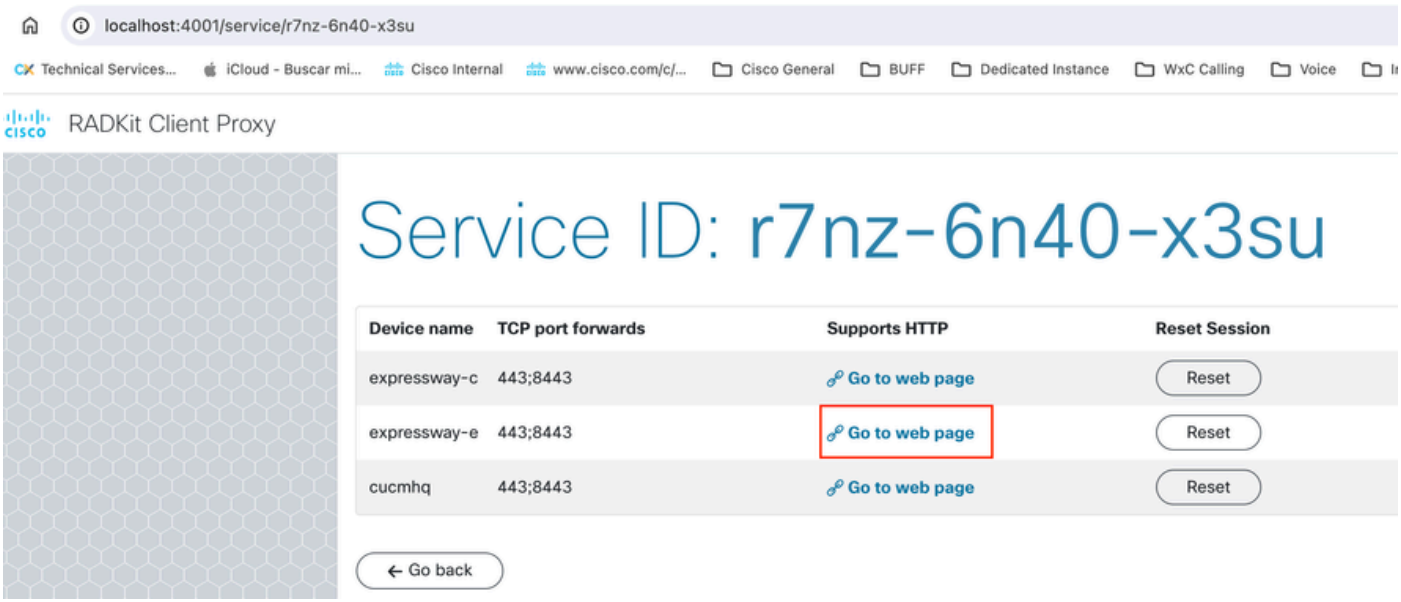
```
>>> http_proxy = client.start_http_proxy(4001)
```

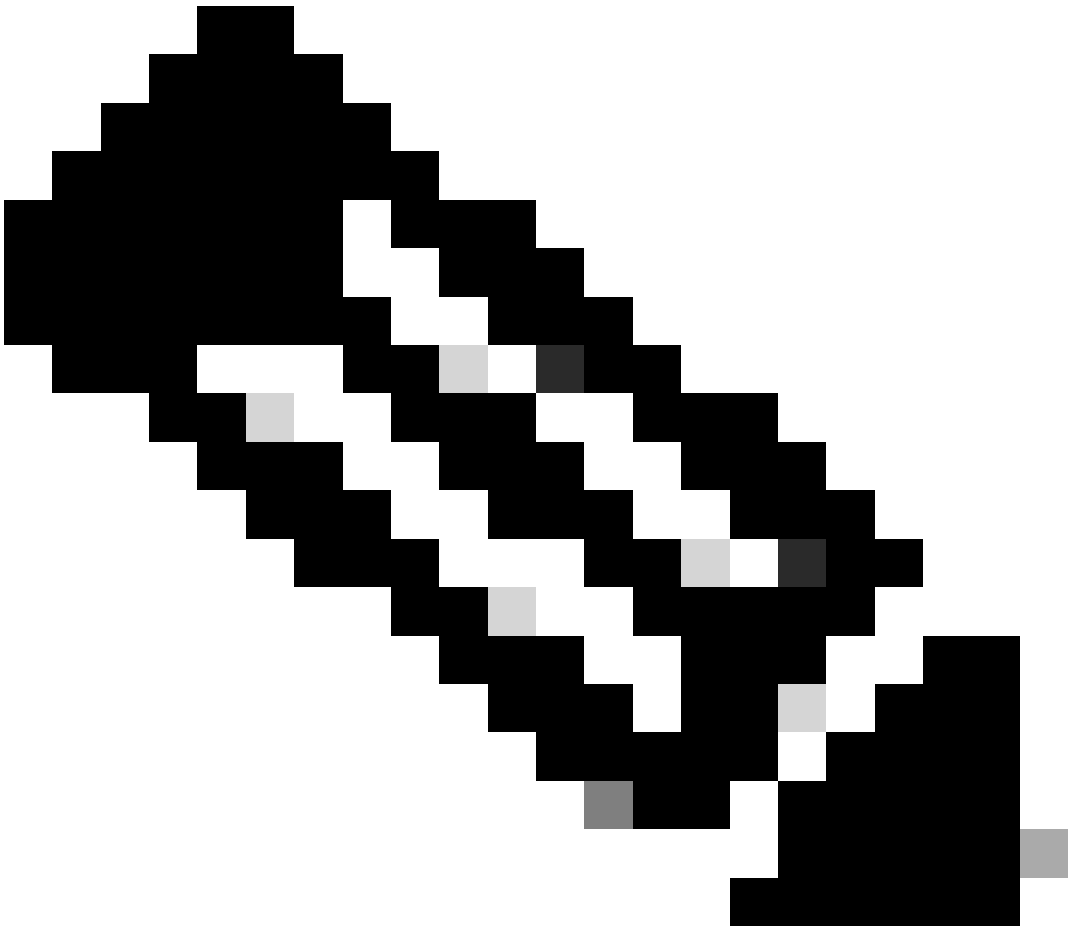
Étape 3. Dans le navigateur Web, accédez à https://localhost:4001 et sélectionnez le service auquel vous souhaitez vous connecter.



Étape 4. Cliquez sur l'option Go to Web Page sur le périphérique approprié pour vous connecter à

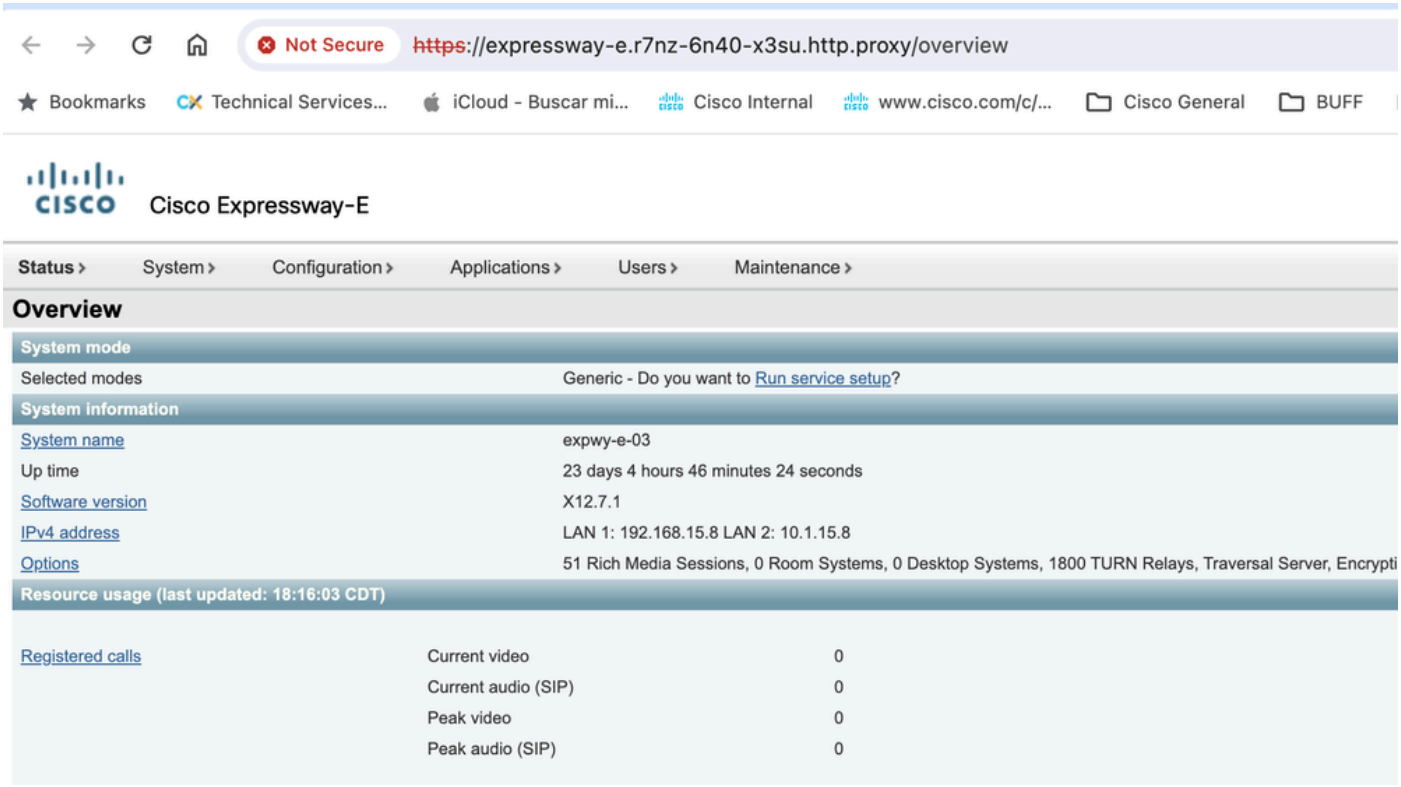
sa page Web.


localhost:4001/service/r7nz-6n40-x3su
Technical Services...
iCloud - Buscar mi...
Cisco Internal
www.cisco.com/c/...
Cisco General
BUFF
Dedicated Instance
WxC Calling
Voice
RADKit Client Proxy
Service ID: r7nz-6n40-x3su
Device name
TCP port forwards
Supports HTTP
Reset Session
expressway-c
443;8443
Go to web page
Reset
expressway-e
443;8443
Go to web page
Reset
cucmhq
443;8443
Go to web page
Reset
← Go back



Remarque : la première fois que le proxy HTTP est configuré sur un client RADKit, il est recommandé de cliquer sur l'option Reset pour chaque périphérique avant d'essayer d'ouvrir la page Web Device.

Étape 5. La page Web s’affiche.



- Transfert de port

Étape 1 : vérification des ports TCP Forwarded configurés pour le périphérique

<#root>

```
>>> cucm.forwarded_tcp_ports
```

Étape 2 : configuration d’un port local à mapper avec le port de destination du périphérique, vous devez utiliser le port local pour accéder à l’interface utilisateur graphique du périphérique.

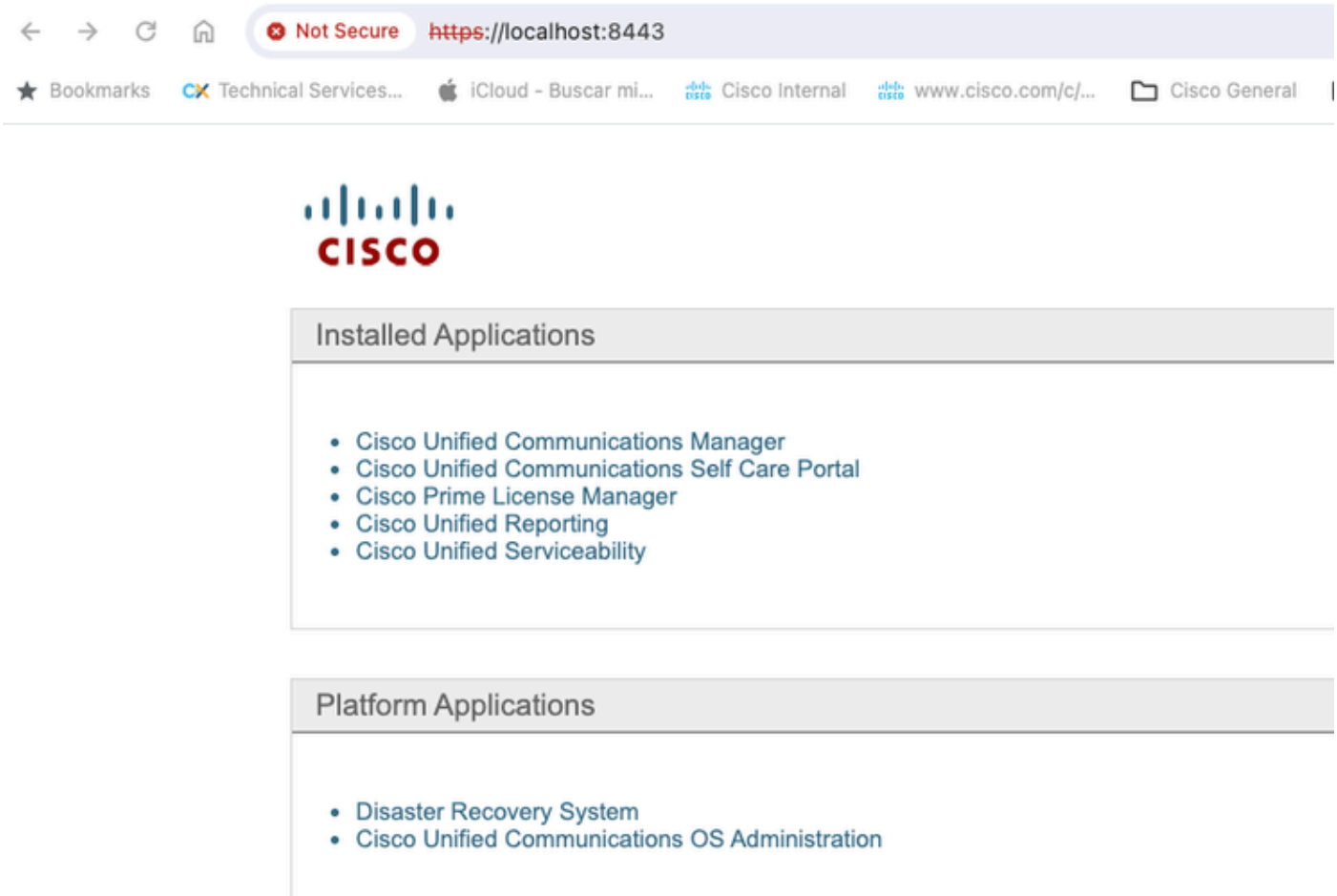
<#root>

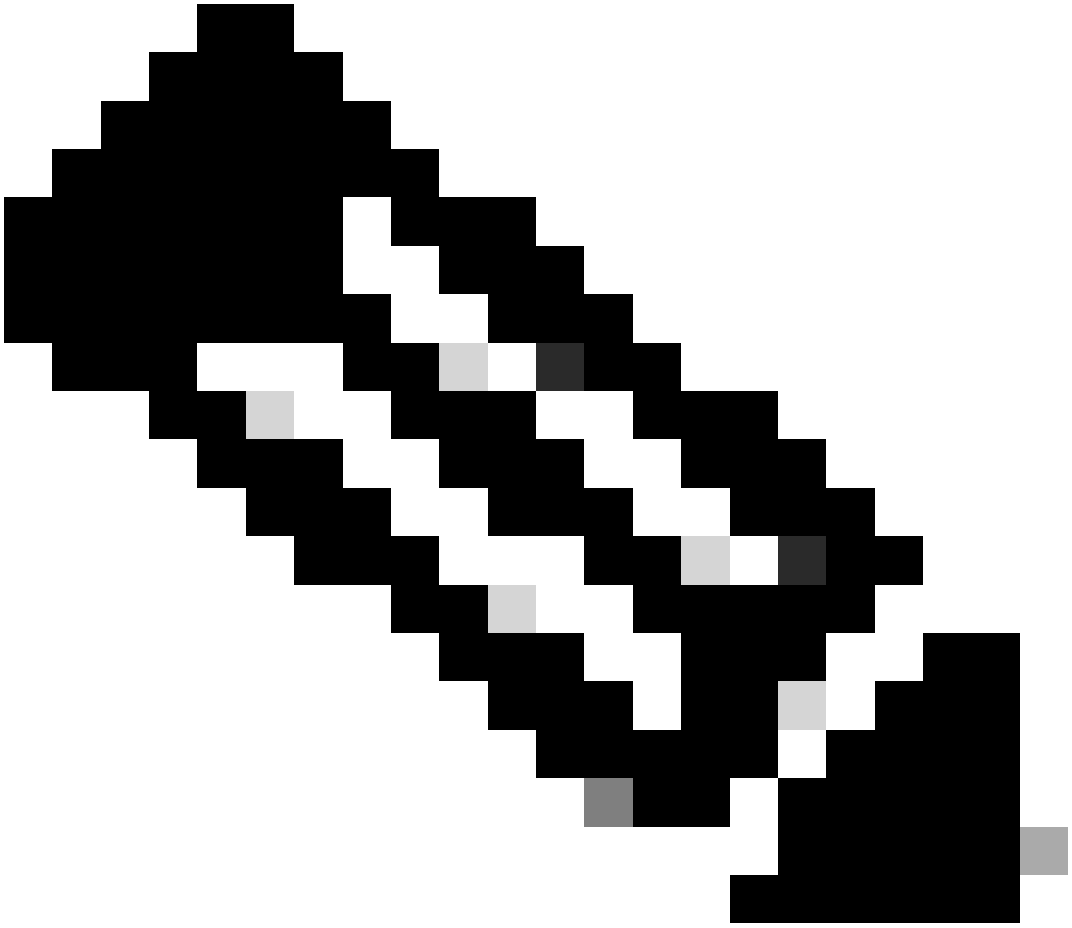
```
>>> cucm.forward_tcp_port(local_port=8443, destination_port=443)
```

```
>>>
>>> cucm.forward_tcp_port(12443,443)
[RUNNING] <radkit_client.sync.port_forwarding.TCPPortForwarder object at 0x10ceb3d60>
----------------  ------------
status            RUNNING
serial            None
device_name       cesavilacucm
local_port        12443
destination_port  443
#active           0
#failed           0
#closed           0
#total            0
bytes up          0
bytes down        0
exception         None
----------------  ------------
```

Étape 3. Ouvrez votre navigateur et tapez l'URL avec le port configuré à l'étape 2 : https://localhost:8443.

L'interface utilisateur graphique du périphérique est désormais accessible.





Remarque : Pour accéder à l'interface utilisateur graphique du produit, vous avez toujours besoin des informations d'identification pour pouvoir vous connecter. Par conséquent, il est recommandé à l'utilisateur de créer un compte d'utilisateur en lecture seule pour y accéder.

Collecte des journaux

- RTMT

Étape 1 : vérifiez que le port 8443 est répertorié dans les ports TCP Forwarded configurés pour le périphérique.

<#root>

```
>>> cucm.forwarded_tcp_ports
```

```
>>> cucm.forwarded_tcp_ports
'443;8443'
>>>
```

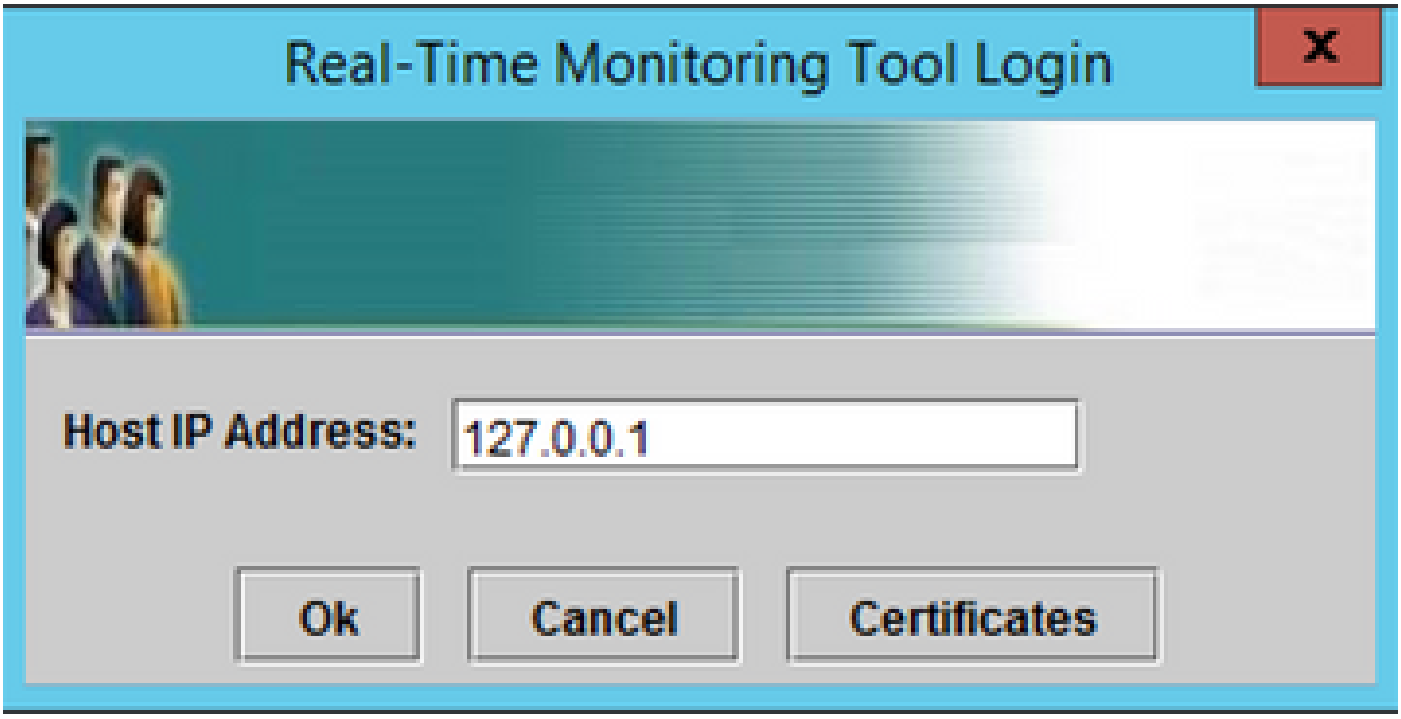
Étape 2 : configurez le même port 8443 comme port local à mapper avec le port 8443 comme port de destination du périphérique.

<#root>

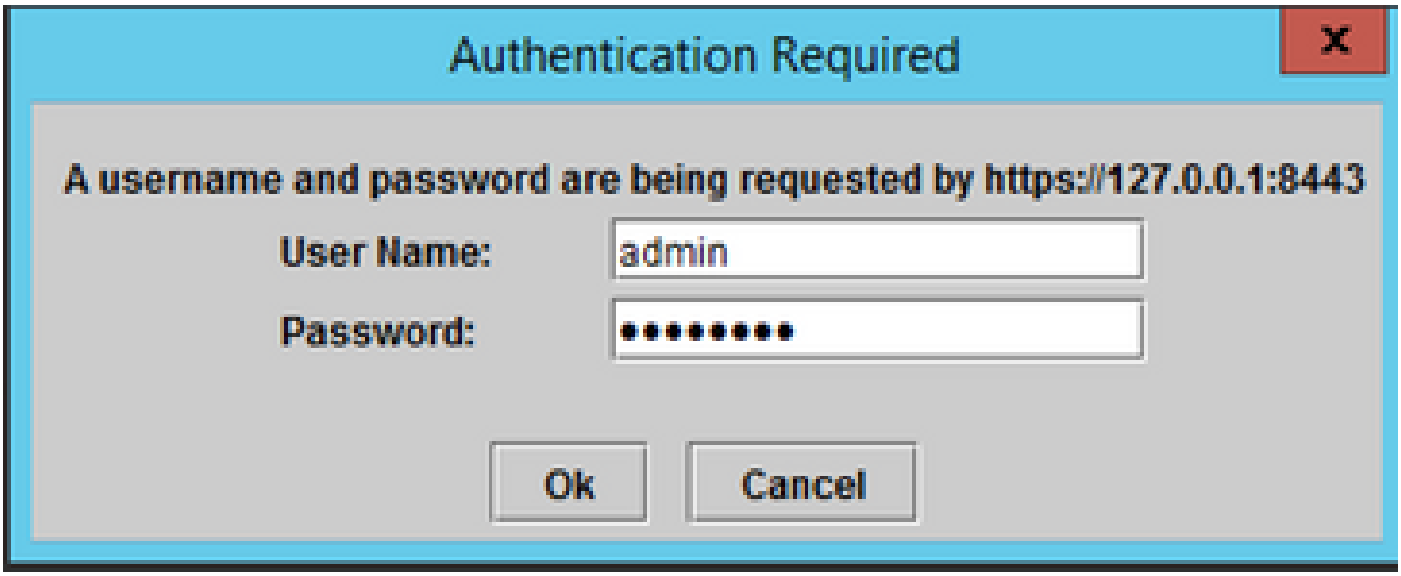
```
>>> cucm.forward_tcp_port(local_port=8443, destination_port=8443)
```

```
>>> cucm.forward_tcp_port(8443,8443)
[RUNNING] <radkit_client.sync.port_forwarding.TCPPortForwarder object at 0x1077defa0>
---------------  -----------
status           RUNNING
serial           None
device_name      cesavilacucm
local_port       8443
destination_port 8443
#active          0
#failed          0
#closed          0
#total           0
bytes up         0
bytes down       0
exception        None
---------------  -----------
```

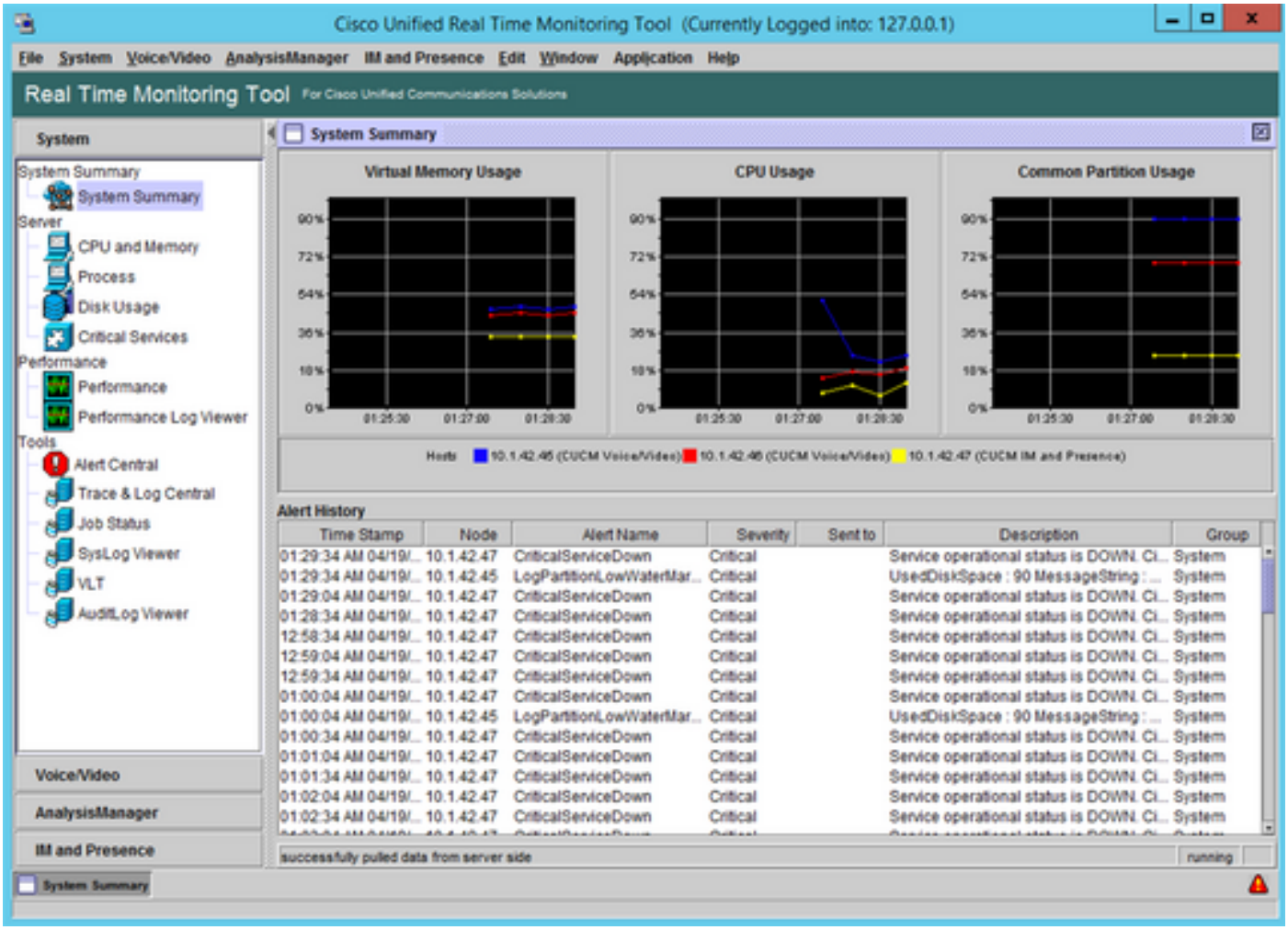
Étape 3. Ouvrez RTMT et tapez 127.0.0.1 dans l'adresse IP de l'hôte. Il utilise automatiquement le port 8443.



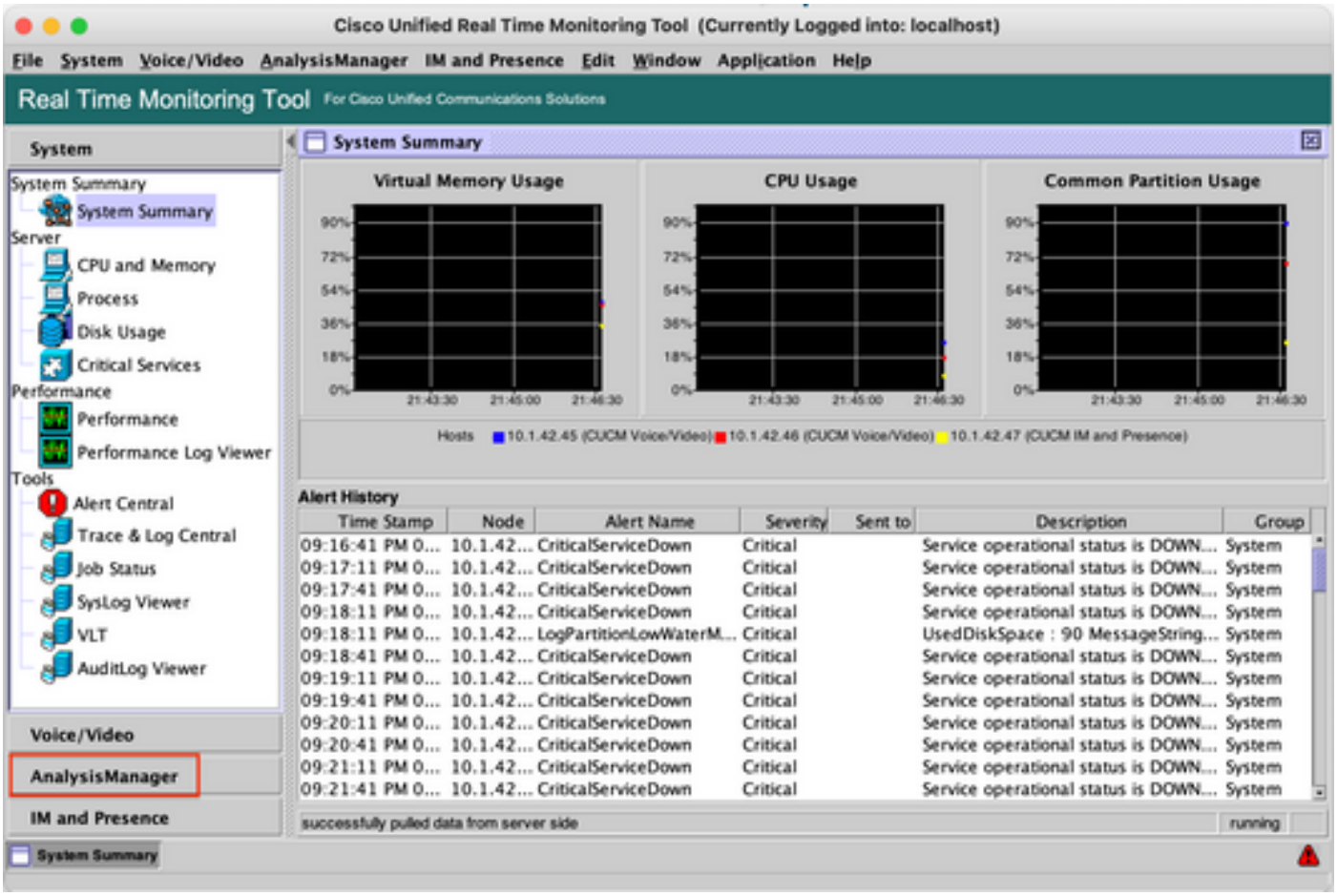
Étape 4. Connectez-vous avec les informations d'identification correctes.



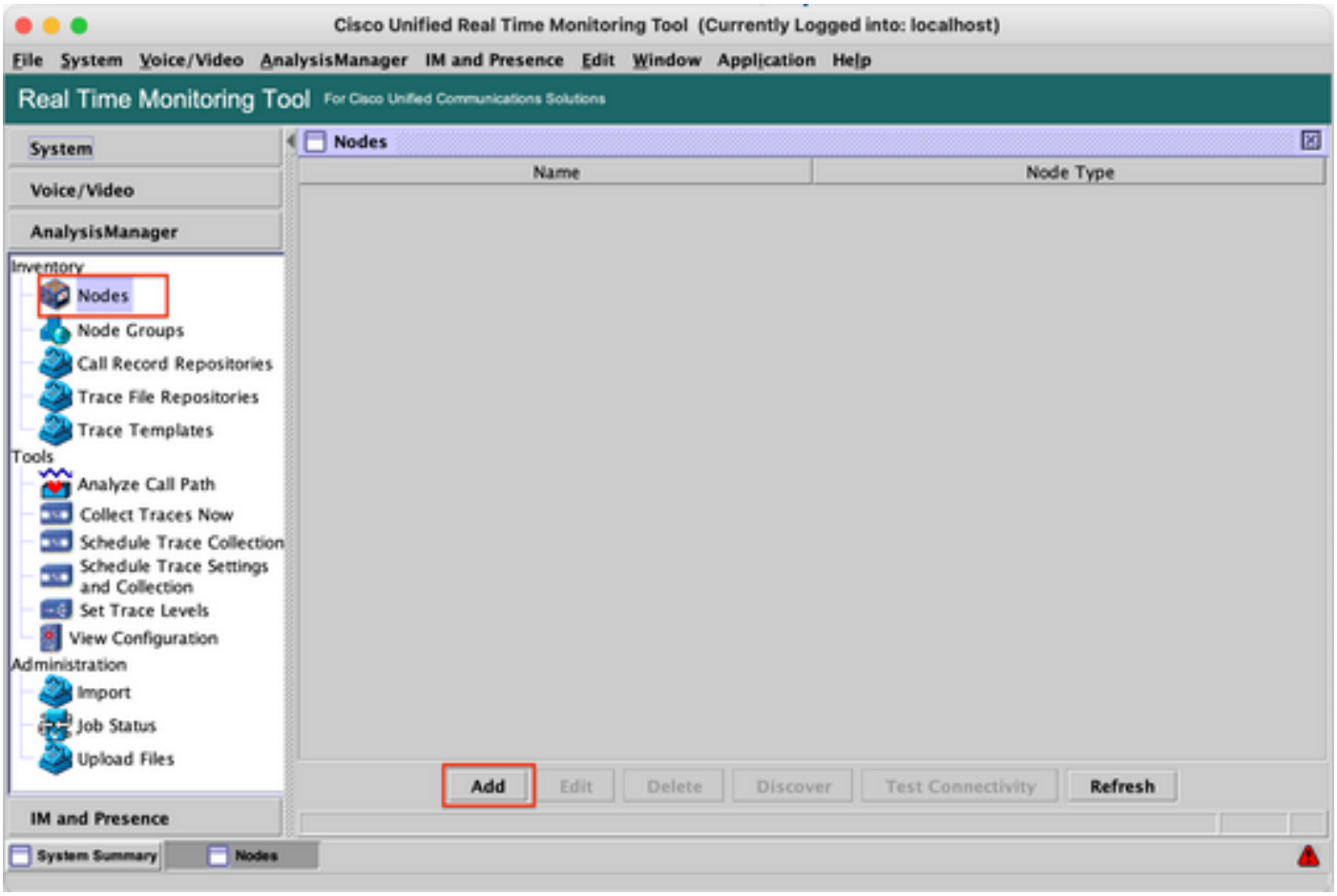
Étape 5 : RTMT s'affiche.

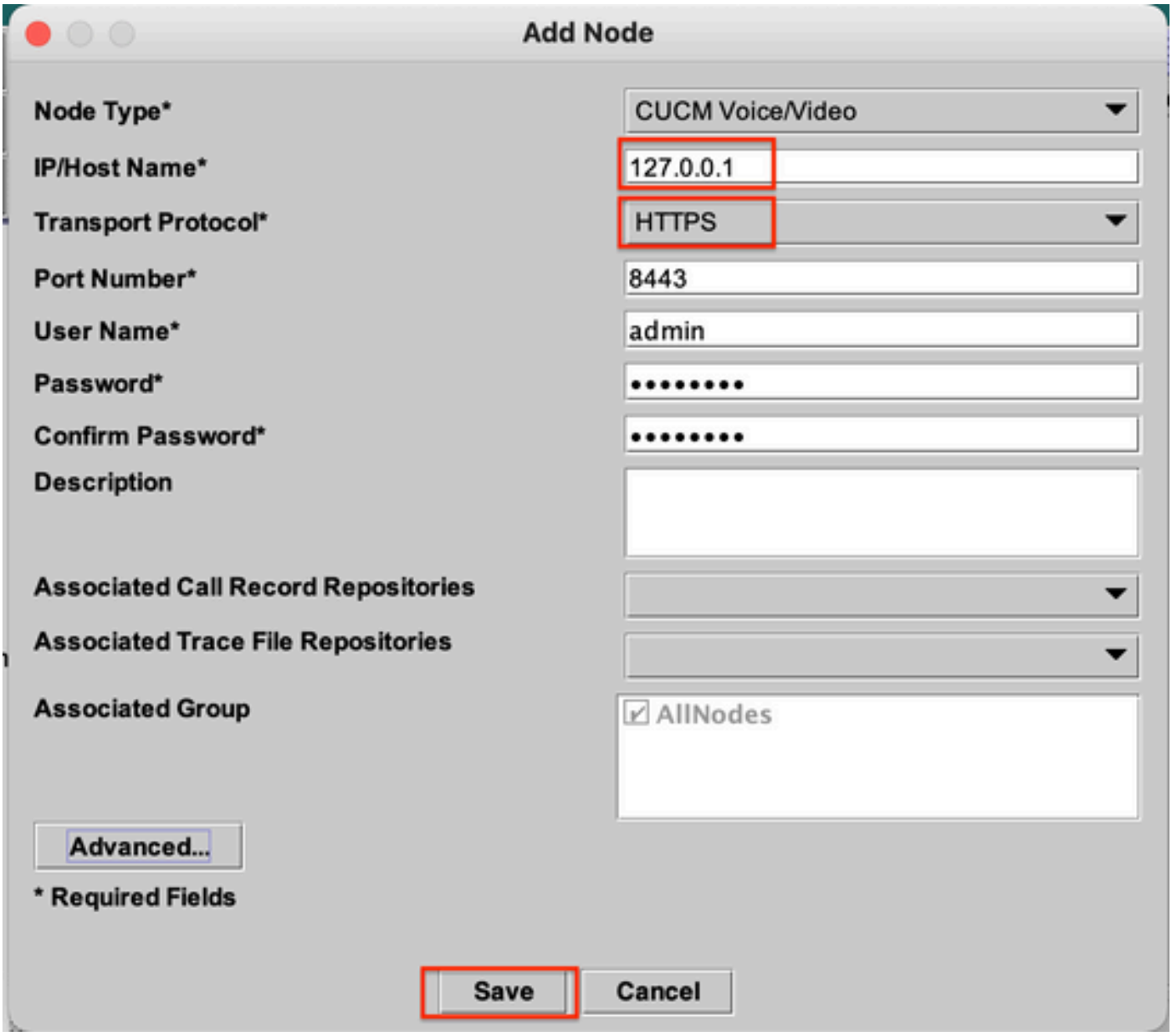


Étape 6. Accédez à AnalysisManager dans le panneau de gauche.

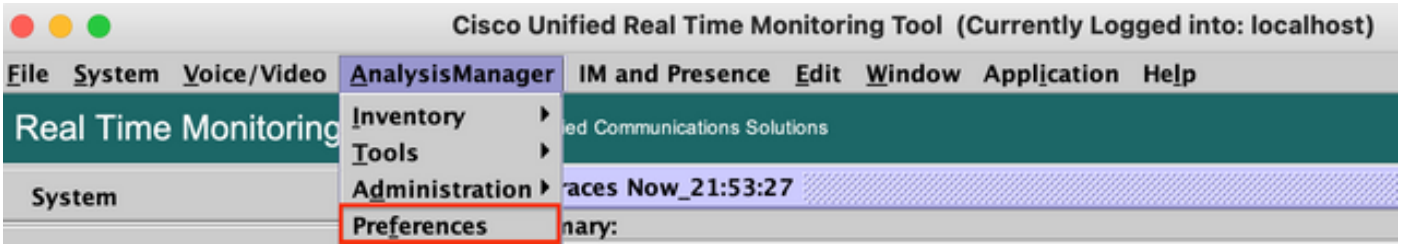


Étape 7. Cliquez sur Nodes and Add pour configurer les détails du périphérique à ajouter à l'aide de localhost et du port TCP transféré.

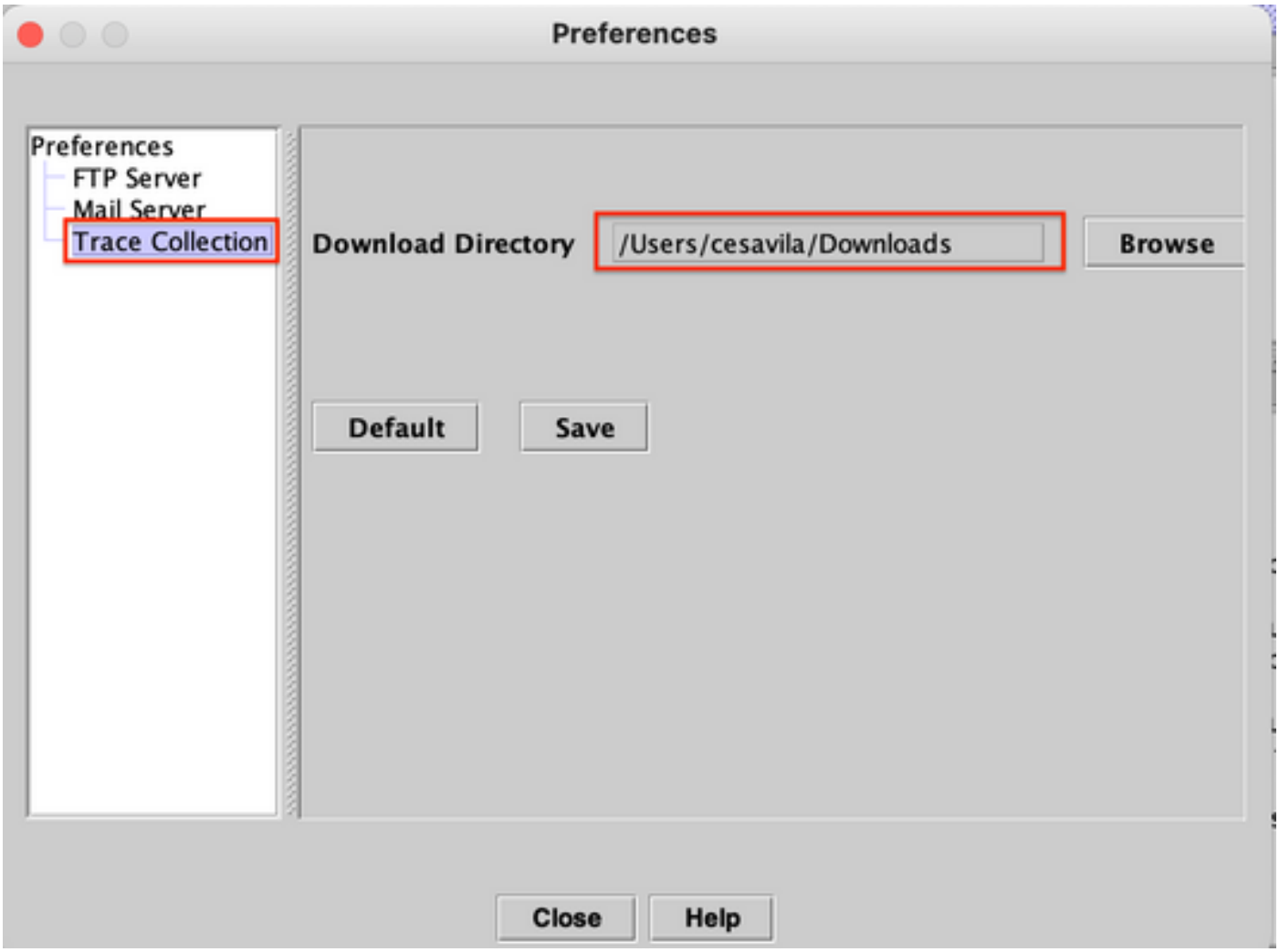

Cisco Unified Real Time Monitoring Tool (Currently Logged into: localhost)
File System Voice/Video AnalysisManager IM and Presence Edit Window Application Help
Real Time Monitoring Tool For Cisco Unified Communications Solutions
System
Voice/Video
AnalysisManager
Inventory
Nodes
Node Groups
Call Record Repositories
Trace File Repositories
Trace Templates
Tools
Analyze Call Path
Collect Traces Now
Schedule Trace Collection
Schedule Trace Settings and Collection
Set Trace Levels
View Configuration
Administration
Import
Job Status
Upload Files
IM and Presence
Nodes
Name
Node Type
Add
Edit
Delete
Discover
Test Connectivity
Refresh
System Summary
Nodes



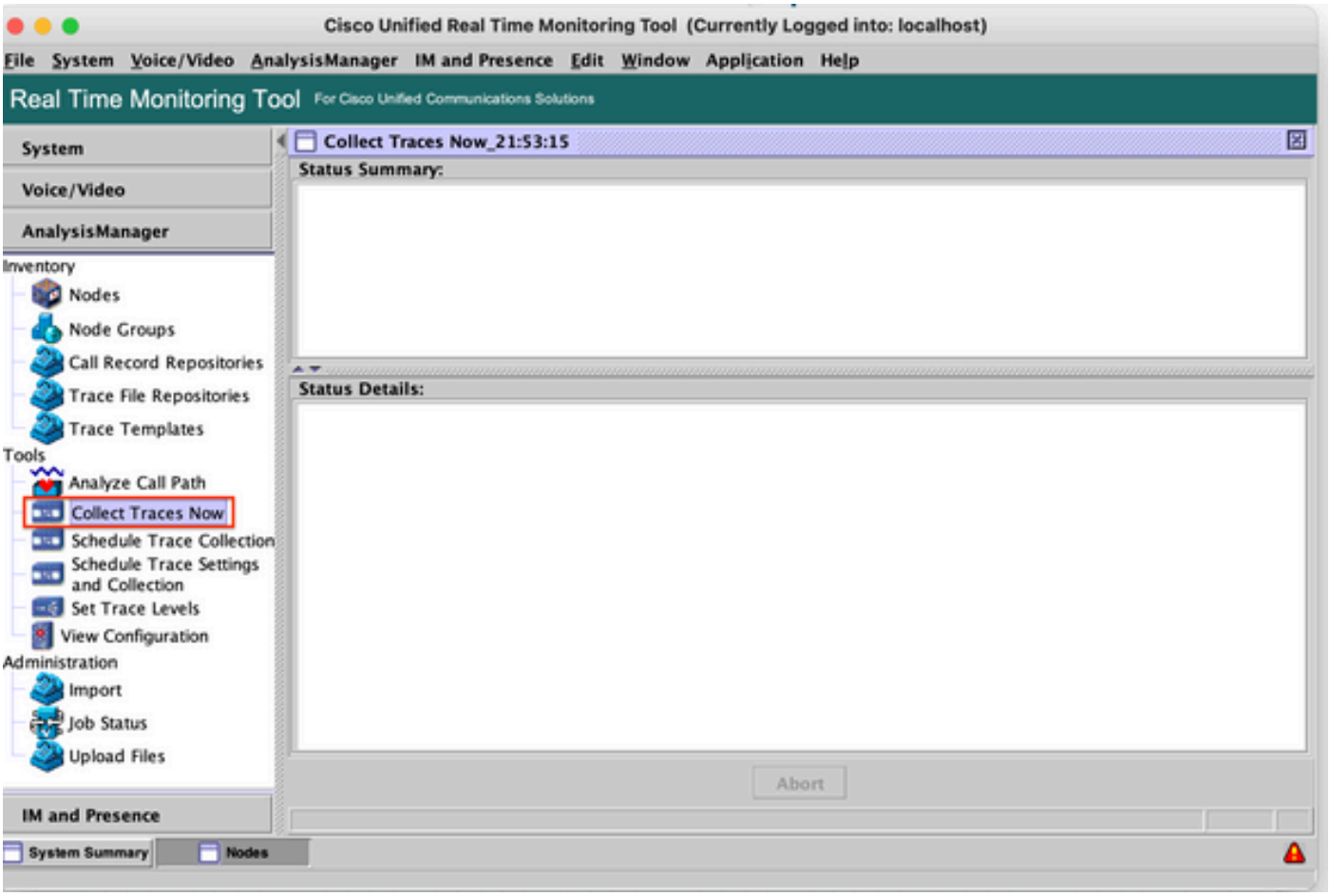
Étape 8. Cliquez sur Analysis Manager dans le menu en haut et sélectionnez Préférences.



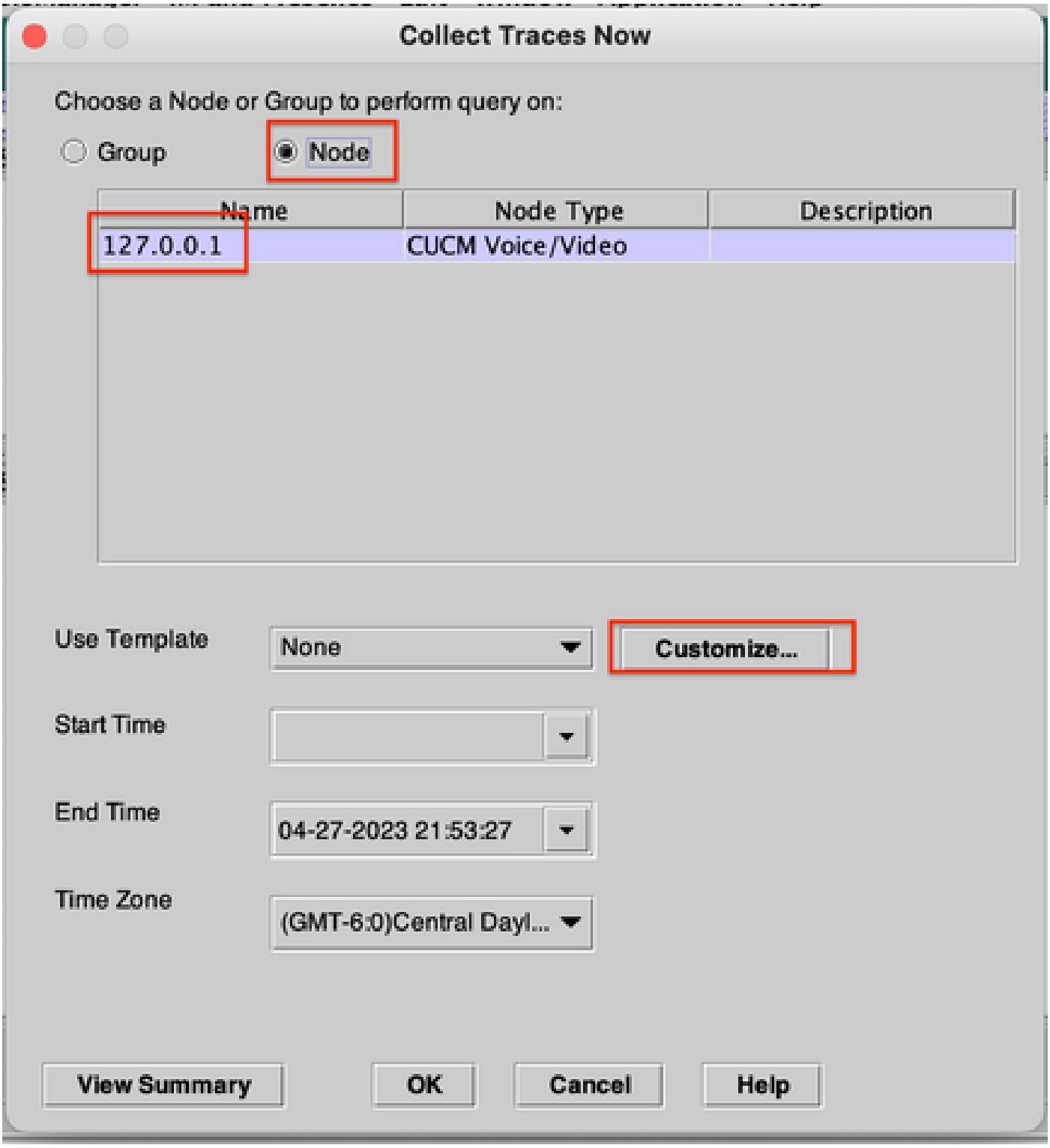
Étape 9. Accédez à Trace Collection et sélectionnez le dossier correct pour télécharger les journaux, cliquez sur Save, puis sur Close.



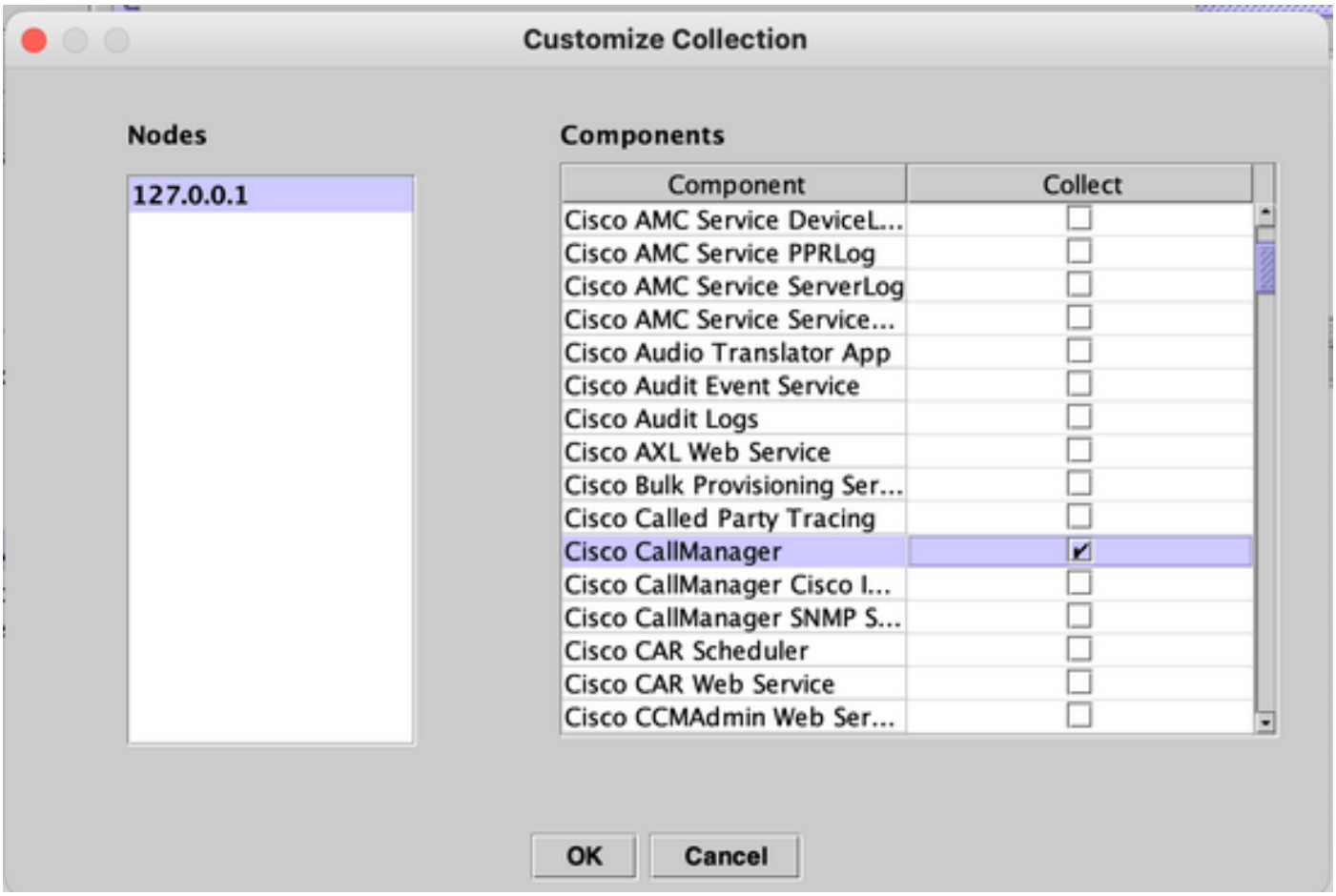
Étape 10. Accédez à Collecter les traces maintenant.



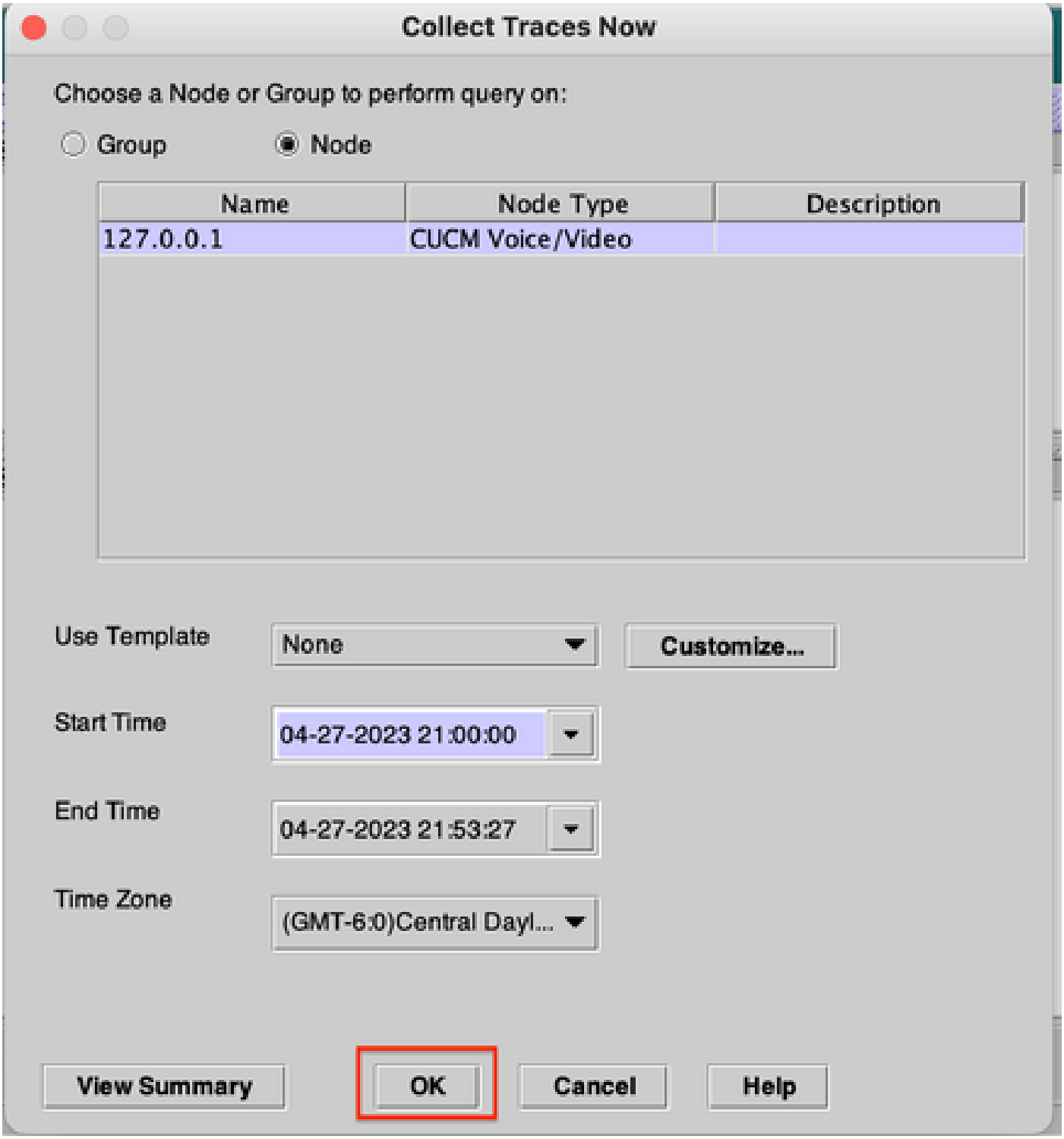
Étape 11. Sélectionnez l’option Noeud, sélectionnez le périphérique qui a été ajouté à l’étape 7 et cliquez sur Personnaliser.



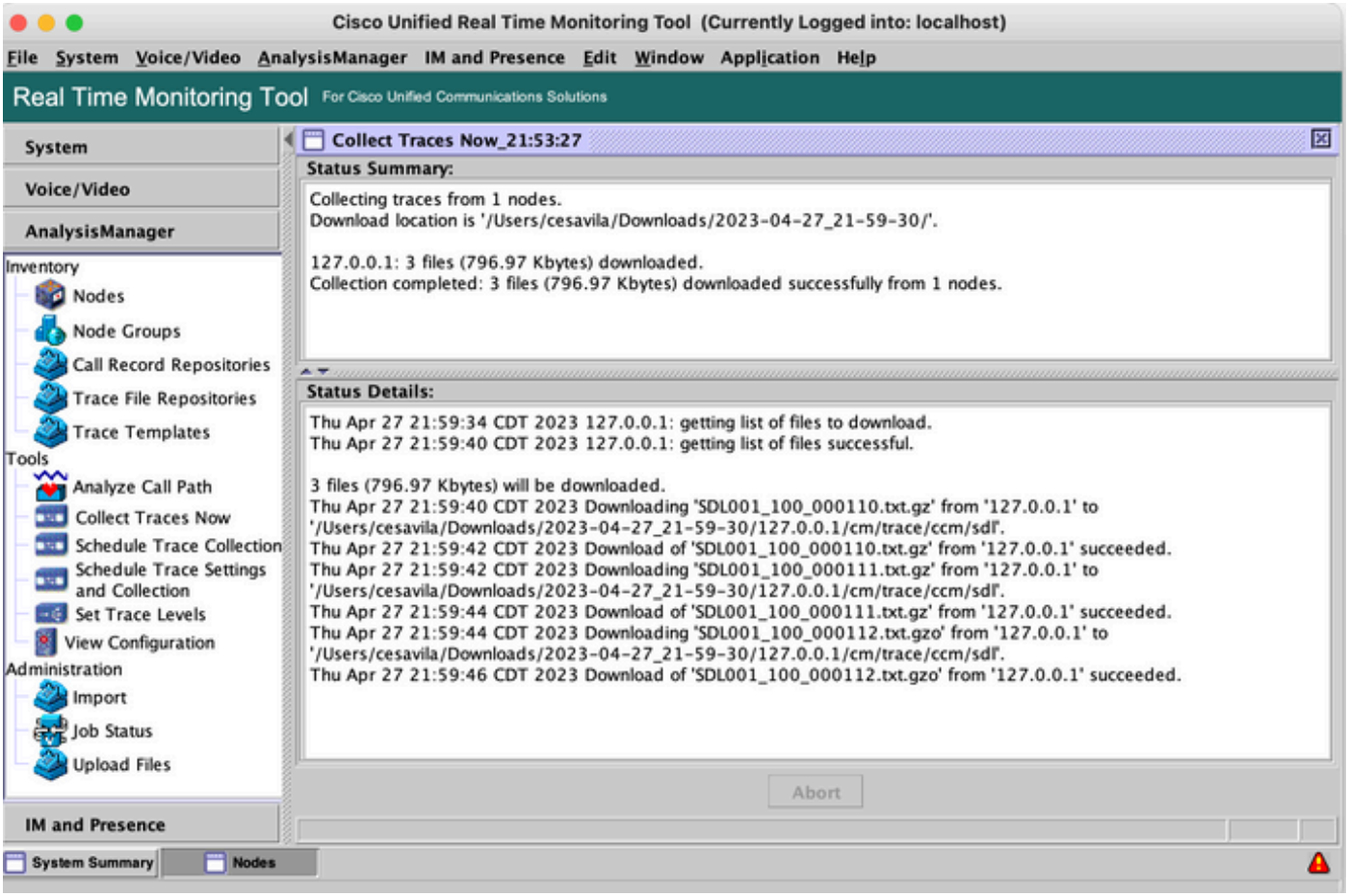
Étape 12. Sélectionnez les journaux à collecter auprès du périphérique et cliquez sur OK.



Étape 13. Sélectionnez enfin Heure de début et Heure de fin des journaux à collecter, puis cliquez sur OK.



Étape 14. Les fichiers sont téléchargés sur le PC local (RADKit Client PC).



- API SOAP

L'API SOAP est actuellement prise en charge pour CUCM. En outre, Swagger est pris en charge pour CMS, Expressway, CVP, etc.

Étape 1 : assurez-vous que les informations d'identification HTTP sont ajoutées au service RADKit sur la configuration du périphérique.

Étape 2 : exécutez la commande HTTP Post sur le client RADKit, spécifiez le chemin d'accès à la ressource, le corps de la requête avec les paramètres et les en-têtes nécessaires.

```
>>>
... r = cucm.http.post('/logcollectionservice2/services/LogCollectionPortTypeService', content = '''<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/so
... ap/envelope/" xmlns:soap="http://schemas.cisco.com/ast/soap">
... <soapenv:Header/>
... <soapenv:Body>
... <soap:FileName>/var/log/active/cm/trace/ccm/sdl/SDL002_100_000819.txt.gz</soap:FileName>
... </soapenv:Body>
... </soapenv:Envelope>''', headers = {"Content-Type": "text/xml; charset=utf-8", "SOAPAction": "GetOneFile"}, postprocessors = ['cucm-extract'])
>>>
>>>
```

Remarque : L'option de post-processeurs 'cucm-extraction' est utilisée pour supprimer les en-têtes de réponse HTTP afin de pouvoir enregistrer le journal dans un fichier.

Étape 3. Enregistrez le contenu dans un fichier pour que le fichier de trace soit enregistré sur le PC local.

<#root>

```
>>> content = r.content
>>> with open('SDL002_100_000819.txt.gz', 'wb') as file:
        file.write(content)
```

Exemples d'utilisation RADKit

Comme cela a été souligné, RADKit fournit une connexion sécurisée aux périphériques réseau, y compris les serveurs de collaboration, sans avoir besoin d'être sur un WebEx. L'idée est de simplifier certains des défis liés à la collecte de données en fournissant un accès à la demande aux périphériques requis.

En ce qui concerne plus particulièrement les déploiements de solutions de collaboration, RADKit peut actuellement s'avérer très utile pour de nombreux problèmes tels que :

- Problèmes de réplication DB.
- Procédures de régénération de certificat.
- Vérification de l'état du système
- Validation de la configuration dans GUI / CLI.
- Collecte des journaux via l'interface Web (par exemple, CER, Expressway, CIMC, etc.).
- Journaux de débogage via CLI sur les passerelles vocales.

Informations connexes

- Page principale de RADKit https://radkit.cisco.com/
- Page d'assistance RADKit externe https://community.cisco.com/t5/radkit-discussions/bd-p/disc-radkit

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.