

# コラボレーション環境でのRADKitの設定

## 内容

---

[はじめに](#)

[要件](#)

[使用するコンポーネント](#)

[用語](#)

[RADKitアーキテクチャ](#)

[RADKitのインストール](#)

[RADKitサービス \( ユーザ側 \)](#)

[オンボーディング](#)

[デバイスの追加](#)

[リモートユーザの許可](#)

[RADkit Client \( TAC側 \)](#)

[ログイン](#)

[SSHアクセス](#)

[GUI アクセス](#)

[HTTPプロキシ](#)

[ポート転送](#)

[ログ収集](#)

[RTMT](#)

[SOAP API](#)

[RADKitの使用例](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、RADKitをセットアップする手順について説明し、コラボレーション製品でRADKitの使用を開始するために必要な設定を示します。

## 要件

次の項目に関する知識が推奨されます。

- VOSコラボレーション製品に関する基本的な知識
- CLI/SSHアクセスの基礎知識

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Unified Communications Manager 12.5および14.0

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。

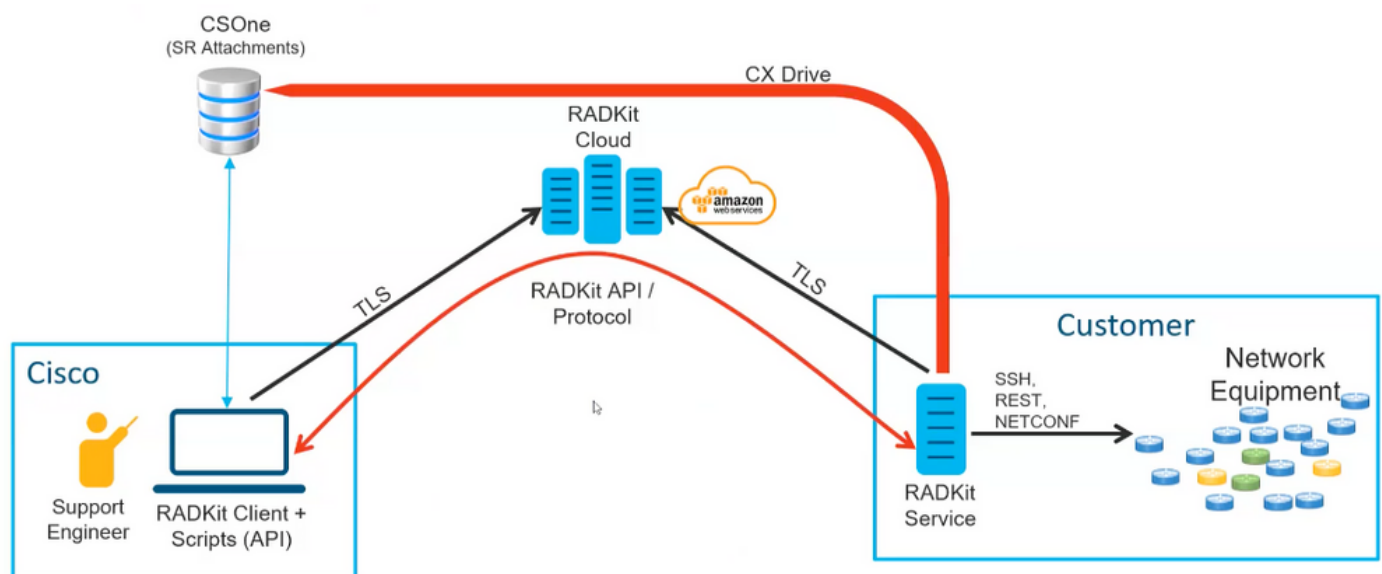
## 用語

**RADKit:** Cisco TACエンジニアおよびパートナーにユーザデバイスへの安全なリモートアクセスを提供するコネクタです。SSHやHTTP/HTTPSなどのデバイスと対話するための複数のプロトコルをサポートします。

**RADKit Service:** これはサーバ側です。これはユーザが処理し、完全に管理します。サーバ側から、デバイスにアクセスできるユーザとアクセス可能な期間を制御します。Radkitサービスは、ネットワーク内のデバイスへのアクセスを提供するために、それらのデバイスに接続する必要があります。

**RADKit Client:** これはクライアント側です。ユーザネットワーク内のデバイスへの接続に使用されるPCです。

## RADKitアーキテクチャ



RADKitアーキテクチャ

## RADKitのインストール

ステップ 1 : <https://radkit.cisco.com>に移動して、Downloadsをクリックしてから、releaseフォルダに移動します。

Cisco Remote Automation Development Kit (RADKit)

# CISCO RADKit. FROM NETOPS TO DEVOPS.

RADKit is a network-wide orchestrator.  
Experience a radical new way of addressing  
your equipment, boost your Cisco Services,  
and expand your capabilities.



## INDEX OF /DOWNLOADS/

[../](#)

[nonrelease/](#)

03-Mar-2023 18:10

-

[release/](#)

04-Apr-2023 11:45

-

ステップ 2 : 最新のリリースをクリックします。

## INDEX OF /DOWNLOADS/RELEASE/

[../](#)

[1.3.9/](#)

11-Jan-2023 13:11

-

[1.4.6/](#)

10-Mar-2023 15:05

-

[1.4.7/](#)

24-Mar-2023 13:00

-

[1.4.8/](#)

11-Apr-2023 16:05

-

[1.4.9/](#)

11-Apr-2023 16:05

-

ステップ 3 : お使いのOSシステムに応じて、正しいファイルをダウンロードしてください。

## INDEX OF /DOWNLOADS/RELEASE/1.4.9/

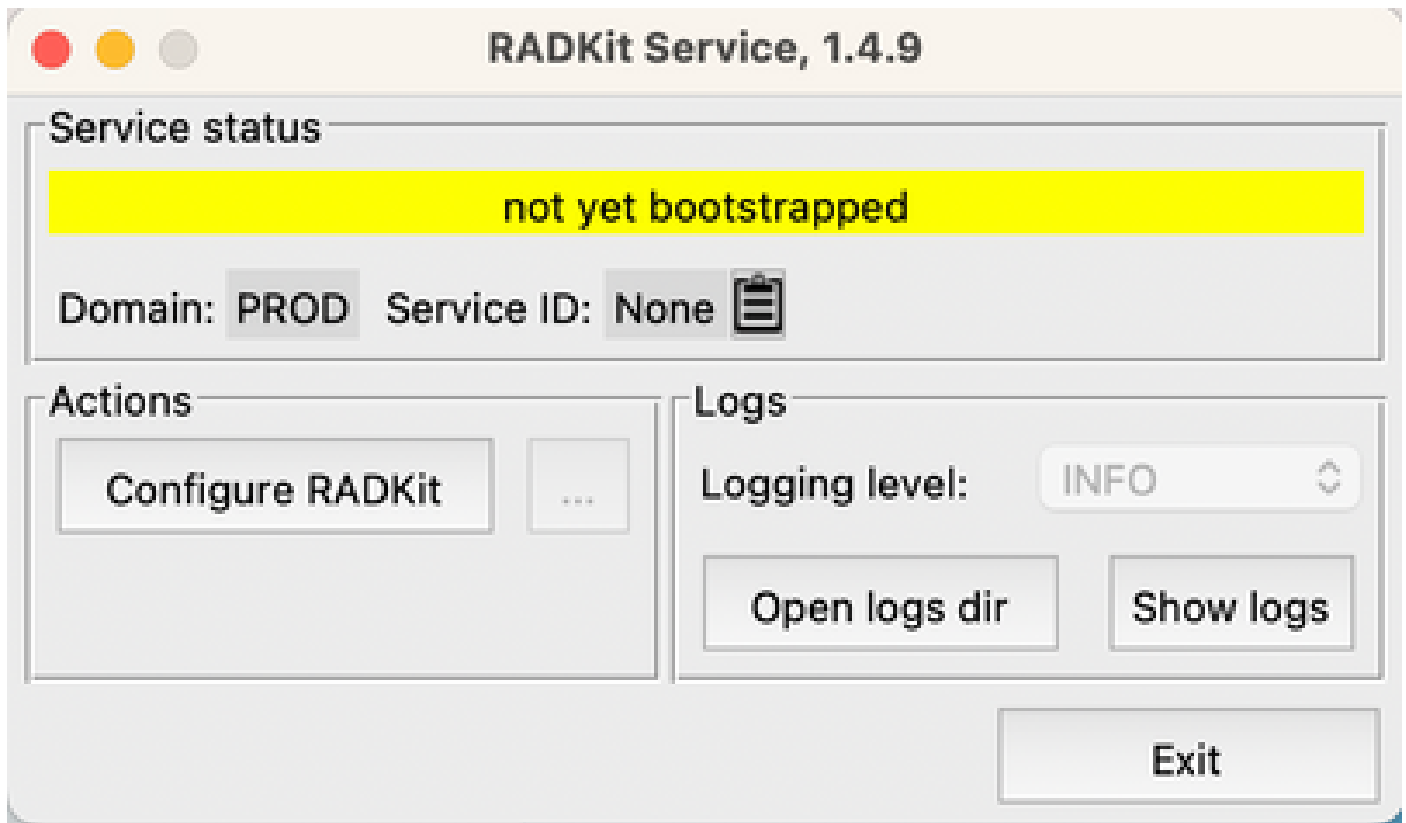
|                                                            |                   |           |
|------------------------------------------------------------|-------------------|-----------|
| <a href="#">../</a>                                        |                   |           |
| <a href="#">docs/</a>                                      | 04-Apr-2023 11:45 | -         |
| <a href="#">cisco_radkit_1.4.9_doc_html.tgz</a>            | 04-Apr-2023 11:43 | 8003863   |
| <a href="#">cisco_radkit_1.4.9_macos_arm64_signed.pkg</a>  | 11-Apr-2023 10:41 | 74142354  |
| <a href="#">cisco_radkit_1.4.9_macos_x86_64_signed.pkg</a> | 11-Apr-2023 10:41 | 77265560  |
| <a href="#">cisco_radkit_1.4.9_pip_linux.tgz</a>           | 04-Apr-2023 11:49 | 146189048 |
| <a href="#">cisco_radkit_1.4.9_pip_macos.tgz</a>           | 04-Apr-2023 11:49 | 37257192  |
| <a href="#">cisco_radkit_1.4.9_pip_win.tgz</a>             | 04-Apr-2023 11:49 | 35385652  |
| <a href="#">cisco_radkit_1.4.9_win64_signed.exe</a>        | 04-Apr-2023 13:18 | 104692424 |

ステップ4:PCまたはサーバでインストーラを実行します。インストールの一環として、Radkitは3つのアプリケーション ( Radkit Service、Radkit Client、Radkitネットワークコンソール ) をインストールする必要があります。

## RADKitサービス ( ユーザ側 )

### オンボーディング

ステップ 1 : RADKitサービスの設定を開始するには、Applicationsに移動し、RADKit Serviceを見つけてます。初めて実行すると、「まだブートストラップされていません(not yet bootstrapped)」というメッセージが表示されます。



ステップ 2 : Configure RADKitをクリックすると、ブラウザが自動的にURL <https://localhost:8081/bootstrap>でポップアップ表示されます。

- superadmin ユーザのパスワードを作成し、Submitをクリックします。
- このsuperadminユーザ名とパスワードは、サービスが開始または設定されるたびに要求されます。

# Register superadmin user

No superadmin user was found.

Please fill in this form to create a superadmin account.



A superadmin user must be created. Please enter a strong password for this user. This password will be requested in the future to (re)start or manage RADKit Service.

Username \*

Password \*

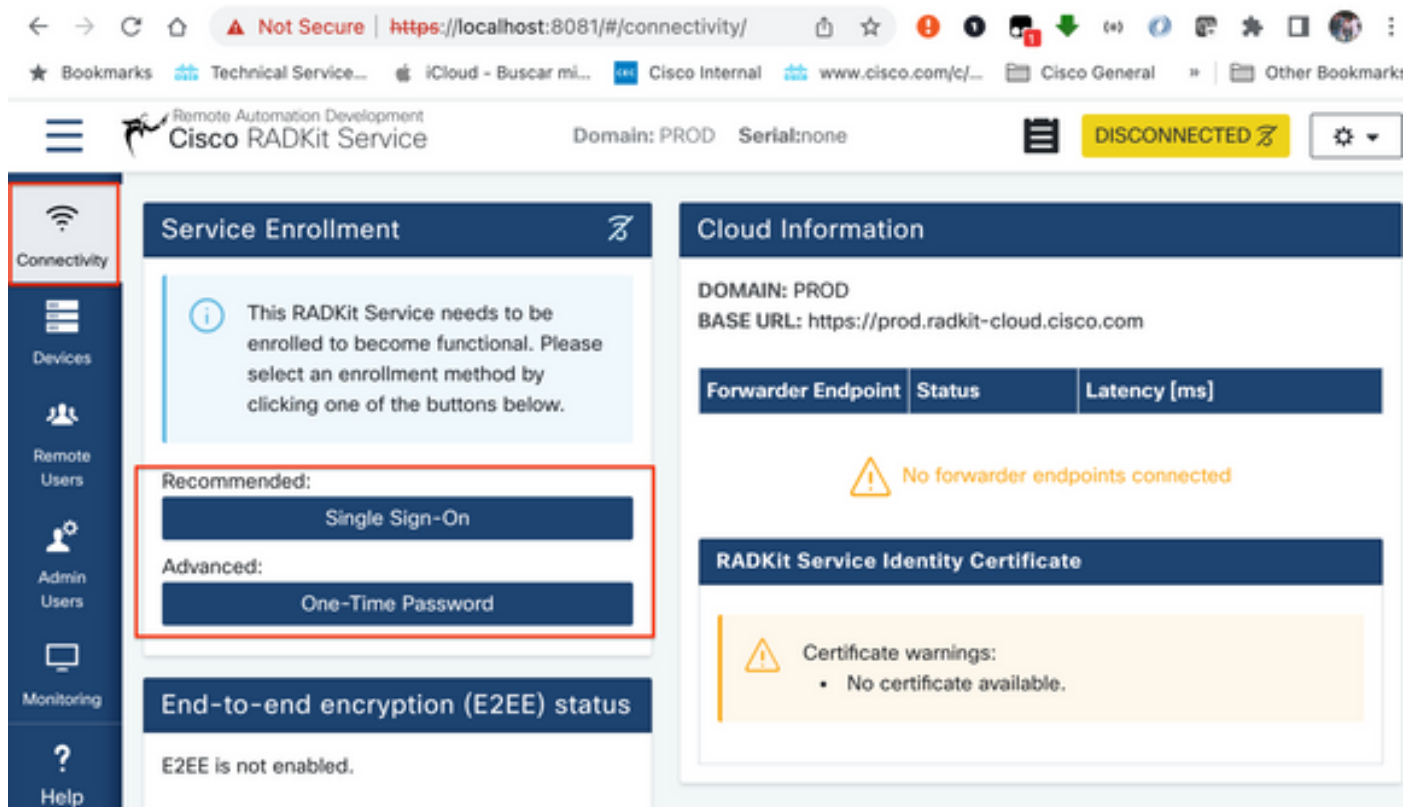
Repeat Password \*

PASSWORD REQUIREMENTS:

- Minimum 1 lowercase letter
- Minimum 1 uppercase letter
- Minimum 1 number
- Minimum 1 symbol
- Minimum 8 characters

ステップ 3 : Submitをクリックすると、ブラウザによって<https://localhost:8081/#/connectivity/>にリダイレクトされます。

Connectivity > Service Enrollmentの下に、Single Sing-OnとOne-Time Passwordの2つの認証方式があります。



ステップ 4 : CECを提供するシングルサインオンを使用できます。

# Single Sign-On Enrollment



✓

Checking prerequisites

2

Email address

Provide email address for SSO login:

Submit

3

Connecting to the Access Service

4

OAuth connect

5

Waiting for SSO

6

Requesting service certificate OTP

7

Requesting service certificate

ステップ 5 : ウィザードを完了し、「Service enrolled with new identity: xxxx-xxxx-xxxx」と表示されるまで手順を実行します。次に、Closeをクリックすると、サービスがConnectedと表示されます。



Service enrolled with new identity: k331-0evx-s94g

Close



Remote Automation Development  
Cisco RADKit Service

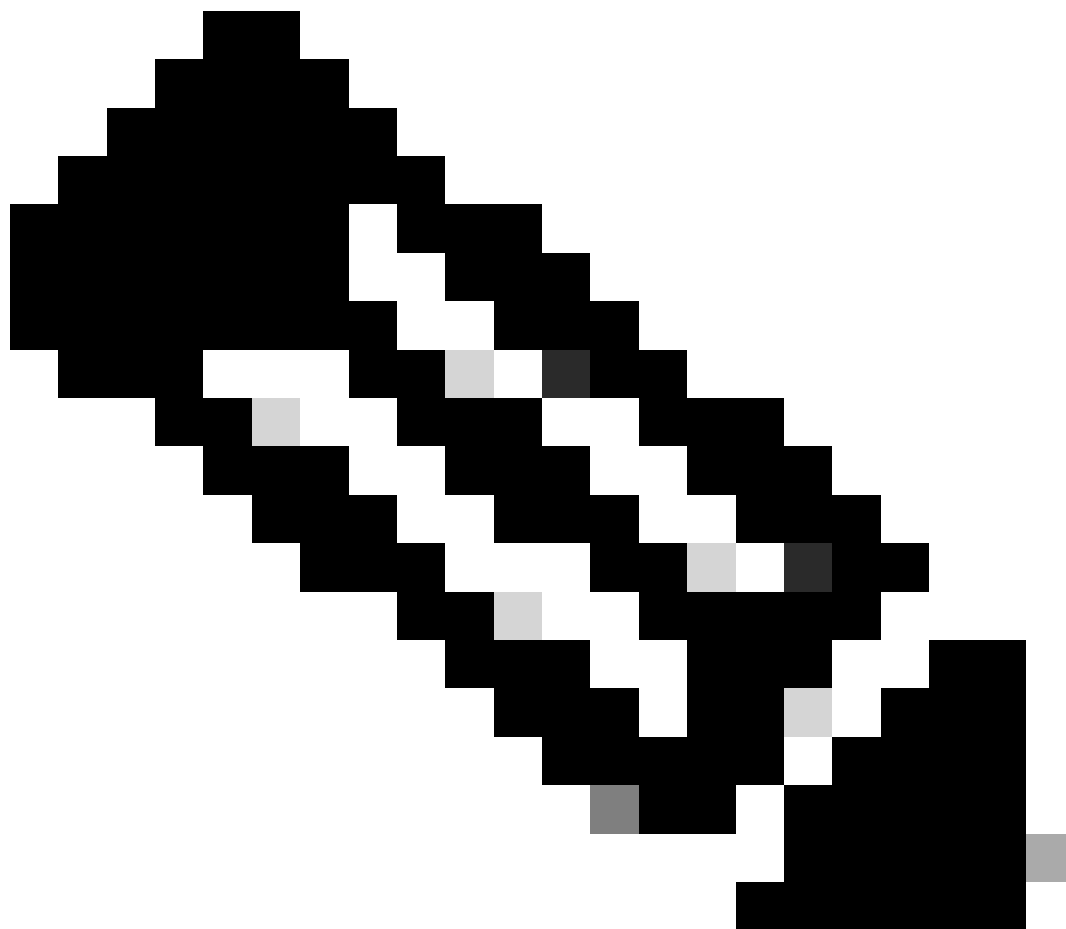
Domain: PROD Serial: k331-0evx-s94g



CONNECTED

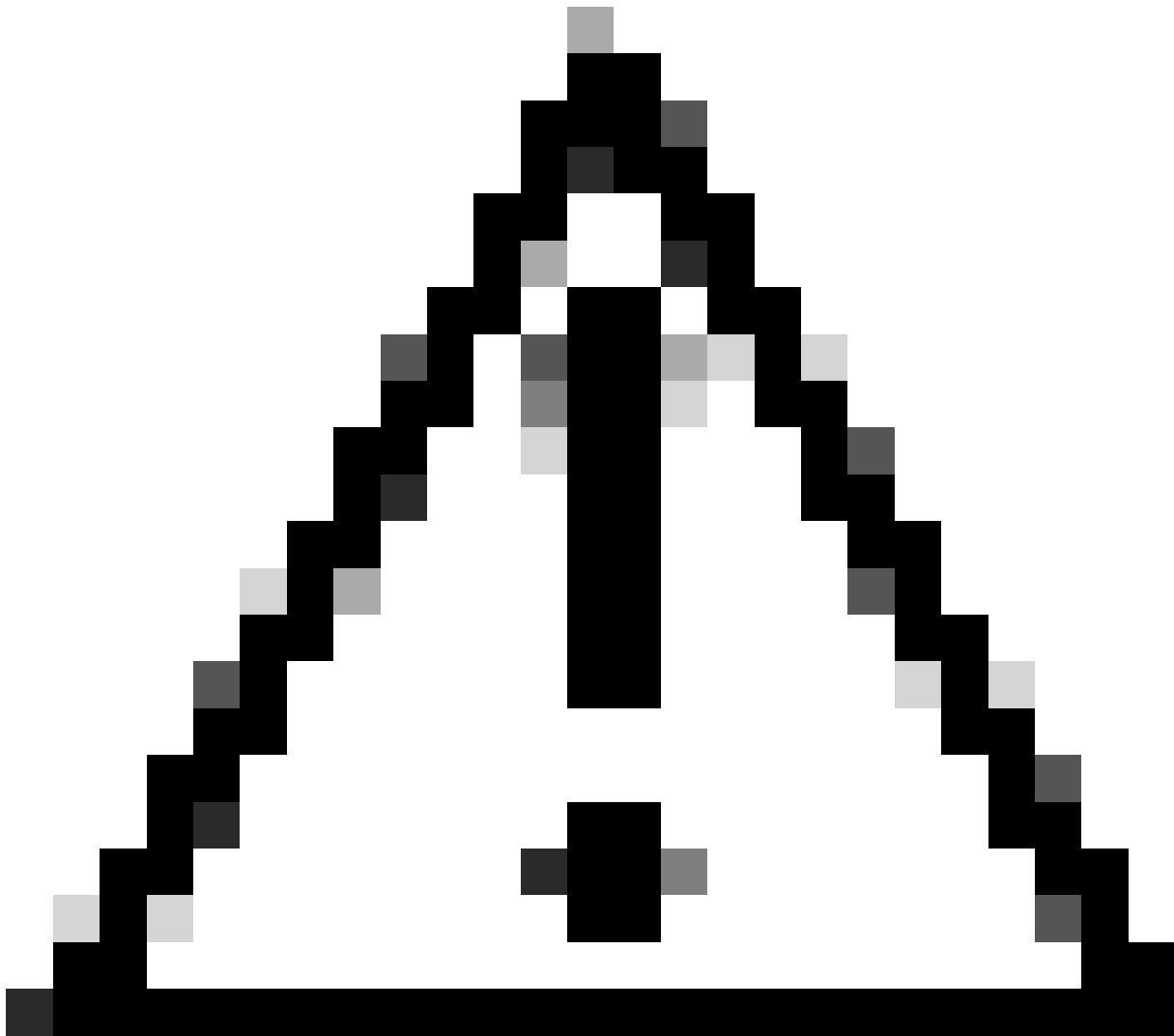






注:RADKit Serviceを有効にするには、シスコのアカウントが必要です。

---



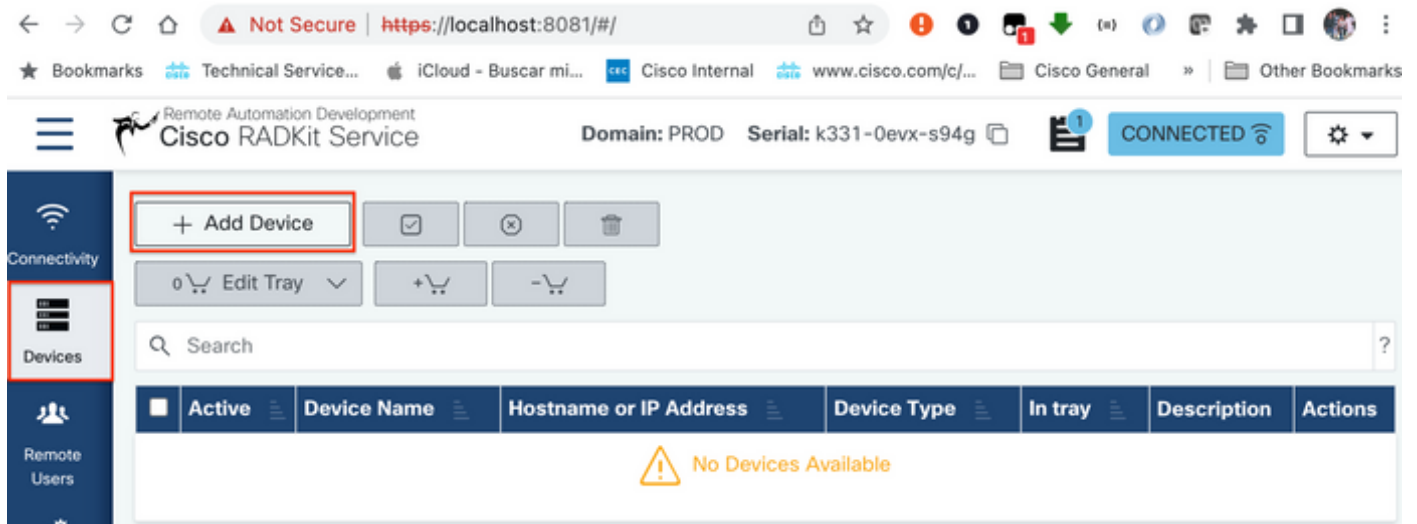
注意：

- RADKitサービスが実行されているサーバでプロキシを定義する必要がある場合は、サーバ/PC自体でプロキシを定義する以外に、RADKitサービスが `RADKIT_CLOUD_CLIENT_PROXY_URL=http://proxy.example.com:80` を機能させるための環境変数も定義する必要があります。

---

## デバイスの追加

ステップ 1 : Devicesに移動し、Add Deviceをクリックします。



ステップ 2：次の詳細を設定する必要があります。

- Device Name
- 管理IPアドレスまたはホスト名
- デバイスタイプ

さらに、転送TCPポートを設定する必要があります。これは、デバイスによって使用されるポートであり、RADKitクライアントからアクセスできる必要があります。この例では、使用されるポートはGUIアクセス用の443、RTMT用の8443です。

最後に、使用可能な管理プロトコルを選択します。この例では、TerminalとHTTPです。

## Add New Device



Device Name\*(as it will appear in RADKit)?

cesavilacum

Device Type\*

CUCM

Management IP Address or Hostname\*?

10.88.247.197

Jumphost Name

- Optional jumphost -

Forwarded TCP ports ?

443;8443

Description

Label search

RBAC status: **ENABLED**

Available Labels - 2 of 2 (click to add)

active

SR697039480

Selected Labels - 0 (click to delete)

Create new

None added

☒ Active (remotely manageable)

Available Management Protocols:

☒ Terminal

☐ Netconf

☐ Swagger

☒ HTTP

☐ SNMP

ステップ 3：各管理プロトコルに正しい設定を行い、Add & Closeをクリックします。

### Terminal

Connection method:

☒ SSH

☐ Telnet

☒ Allow connecting using obsolete/insecure SSH algorithms

☐ Use SSH Tunneling when using this device as a jumphost

Username

admin

Password

\*\*\*\*\*

If left blank, will be set to "" as default

Port

22

☐ Enable Password ?

ステップ 4：追加されたデバイスは、デバイスリストに表示する必要があります。リモートアクセスに対して有効/無効にできます。

Remote Automation Development  
Cisco RADKit Service

Domain: PROD Serial: k331-0evx-s94g

CONNECTED

+ Add Device

0 Edit Tray

Search

| Active                   | Device Name  | Hostname or IP Address | Device Type | In tray | Description | Actions |
|--------------------------|--------------|------------------------|-------------|---------|-------------|---------|
| <input type="checkbox"/> | cesavilaCUCM | 10.88.247.197          | UNKNOWN     |         |             |         |

Showing 1 to 1 of 1 entries. | Selected: 0.

Page size 15 25 50 100 250

## リモートユーザの許可

ステップ 1 : RADKitサービスで設定されているデバイスへのユーザアクセスを許可するには、Remote Usersに移動して、Add Usersを選択します。

Remote Automation Development  
Cisco RADKit Service

Domain: PROD Serial: k331-0evx-s94g

CONNECTED

+ Add User

Search

| Active             | Remaining Time | User Email | Full Name | Description | Actions |
|--------------------|----------------|------------|-----------|-------------|---------|
| No Users Available |                |            |           |             |         |

Showing 0 to 0 of 0 entries. | Selected: 0.

Page size 15 25 50 100 250

ステップ 2 : ユーザの詳細を設定します。

- 電子メールアドレス
- フルネーム ( オプション )
- ユーザをアクティブにします。
- アクティベーションを手動で制御するか、そのユーザにアクセスを許可する期間を設定するかを指定します。

## Add New User



User Email\*

cesavila@cisco.com

Full Name

Cesar Avila

Description

Activate this user

☒

USER ACCESS POLICY

☒ Manual

☐ Time slice (h/m):  
24 00

Clear form

Add & close

Add & continue

ステップ 3 : Add & Closeを選択します。

## RADkit Client ( TAC側 )

### ログイン

ステップ 1 : クライアントPCで、Applicationsに移動し、RADkit Clientを見つけます。

ステップ 2 : SSOログインでクライアントインスタンスを作成します。

<#root>

>>>

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

```
cesavila — radkit-client — 117x32

Example usage:
client = sso_login("<email_address>")           # Open new client and authenticate with SSO
client = certificate_login("<email_address>")      # OR authenticate with a certificate
client = access_token_login("<access_token>")     # OR authenticate with an SSO Access Token
service = client.service("<serial>")             # Then connect to a RADKit Service
service = start_integrated_service()             # Immediately login to an integrated session
client.grant_service_otp()                       # Enroll a new service

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

ステップ 3 : ブラウザで自動的に開かれたSSO認証要求を受け入れます。



## Do you accept this authorization request?

Environment: PROD

Client IP address: 128.107.241.164

Client hostname: N/A

This page means that a RADKit instance is attempting to connect to the RADKit Cloud with your SSO credentials.

If you *did not* initiate this request, please click "Deny" now. If you are certain that this request is legitimate, click "Accept".

If you suspect that an illegitimate session may have been granted access in the past, click the "Log out all sessions" button below to immediately log out all RADKit SSO sessions associated with your user ID. This *will not* log out your SSO sessions in other applications.

Accept

Deny

Log out all sessions



## Authentication result: Success

You may now close this window and return to your application.

If you suspect that an illegitimate session may have been granted access now or in the past, click the button below to immediately log out all RADKit SSO sessions associated with your user ID. This *will not* log out your SSO sessions in other applications.

Log out all sessions

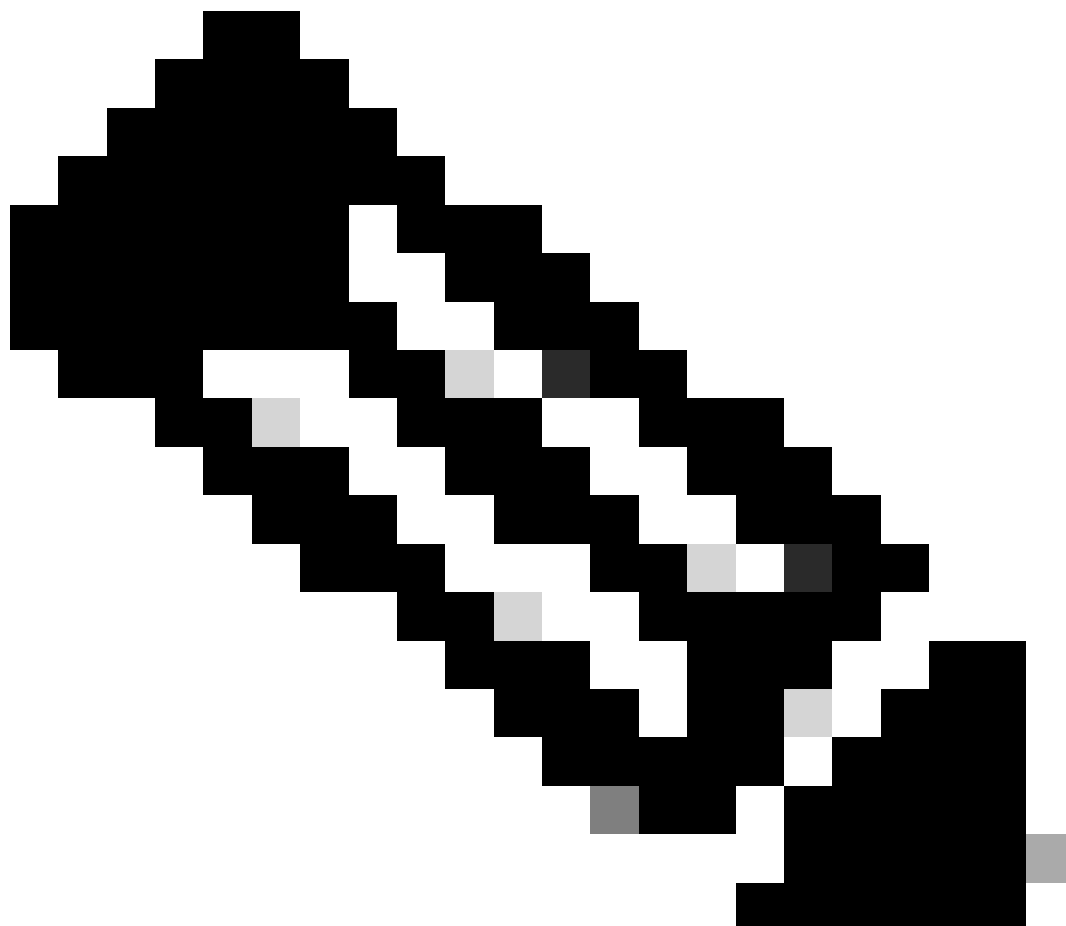
ステップ 4 : RADKit Service - Onboarding段階でユーザが生成したシリアル番号を使用して、サービスインスタンスを作成します。

<#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/websocket/']
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/websocket/']
05:16:40.333Z INFO | internal | Connection to forwarder successful [uri='wss://prod.radkit-cloud.cisco.com/forwarder-3/websocket/']
```



注：serviceは、何になる可能性もある変数です。

ステップ 5：アクセス可能なデバイスを確認します。



<#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
```

インベントリリストを更新するには、update\_inventoryコマンドを使用します。

<#root>

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

## SSHアクセス

ステップ 1：インベントリリストからオブジェクトを作成します。

<#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"]
```

ステップ 2：interactiveコマンドを使用してSSHセッションを開始します。

<#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/202304-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 ...

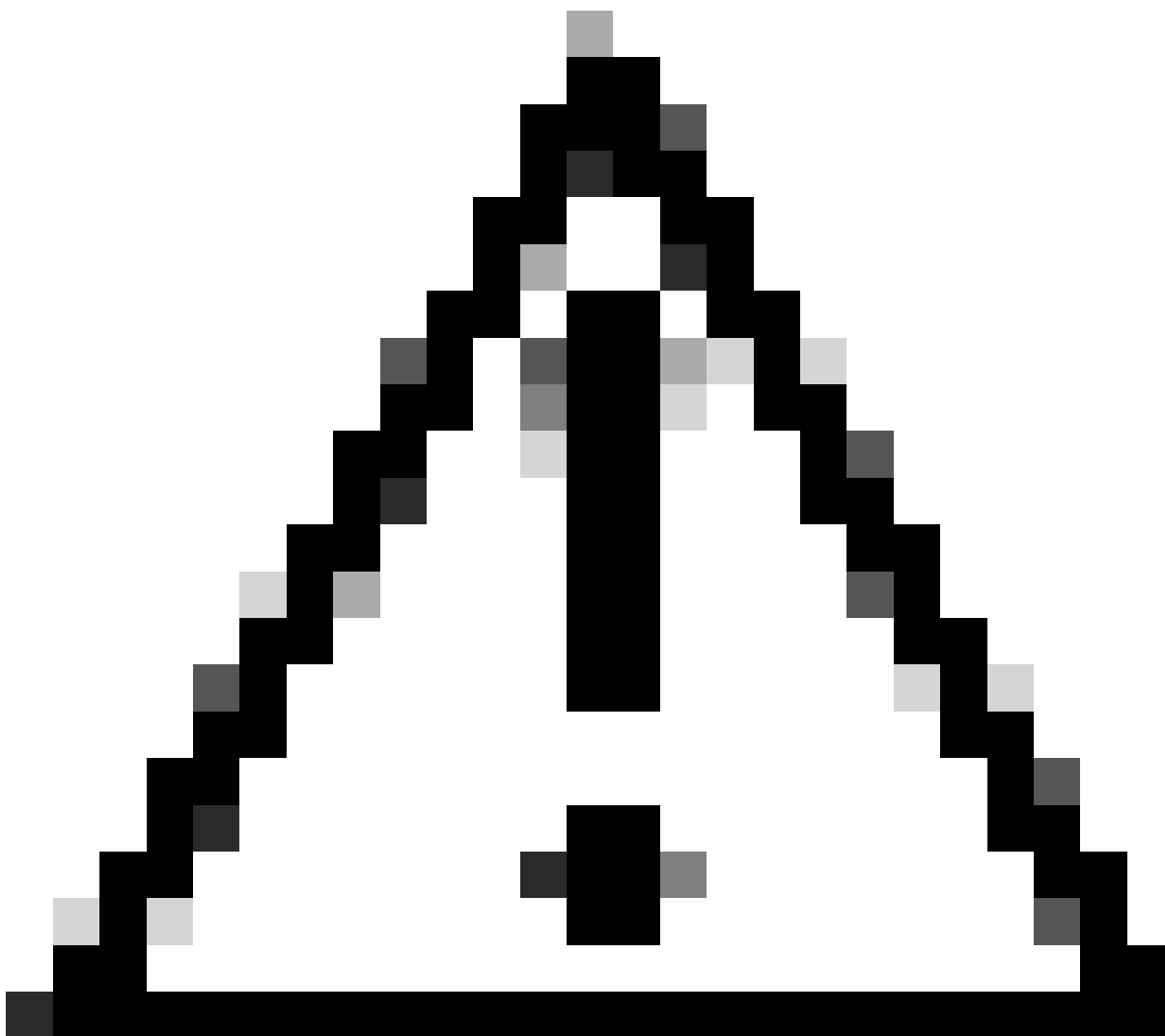
Welcome to the Platform Command Line Interface

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:|
```

ステップ3：これで、デバイスを正常に管理できるようになりました。

---



注意：

- ユーザ環境で業務を行う際は、常にシスコの責任に留意してください。
- データ収集ツールとして使用する必要がある。
- ユーザーの許可なしに変更を行わないでください。
- すべての結果をケースノートに記載します。

## GUI アクセス

- HTTPプロキシ

ステップ 1：HTTPクレデンシャルがデバイス設定のRADKitサービスに追加されていることを確認します。

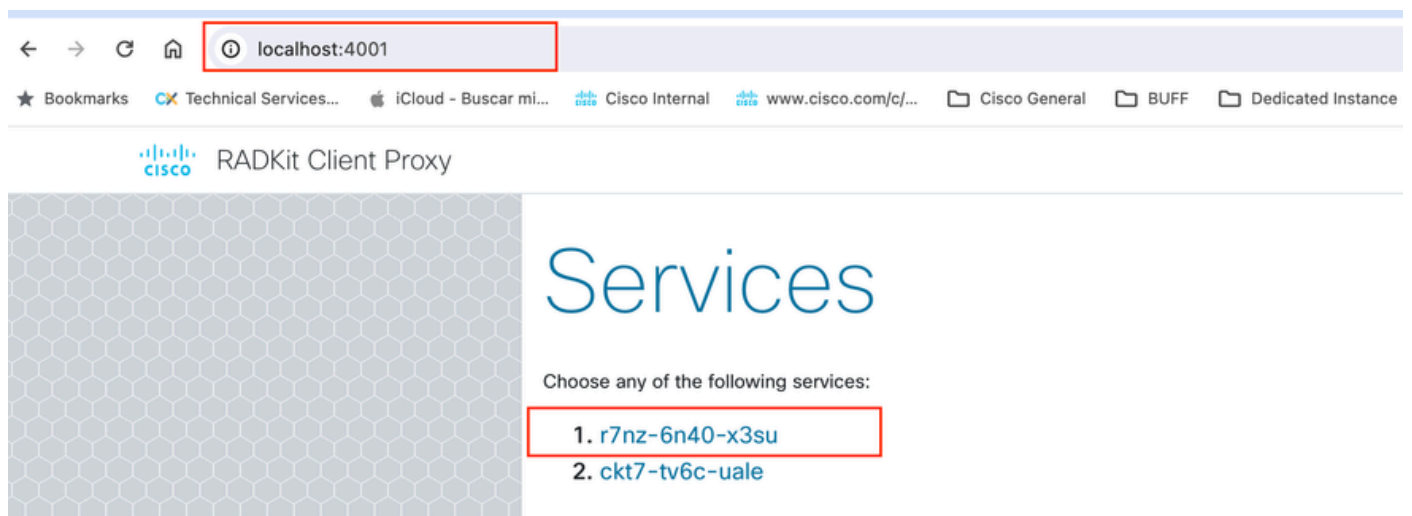
ステップ 2：RadkitクライアントでHTTPプロキシを起動し、プロキシへの接続に使用するローカルポートを定義します。

<#root>

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

```
>>>
>>> http_proxy = client.start_http_proxy(4001)
22:24:19.981Z WARNI | HTTP proxy is NOT PROTECTED by username/password
>>> █
```

ステップ 3：Webブラウザから、<https://localhost:4001>に移動し、接続先のサービスを選択します。



ステップ 4：正しいデバイスのWebページに移動オプションをクリックして、そのデバイスのWebページに接続します。

localhost:4001/service/r7nz-6n40-x3su

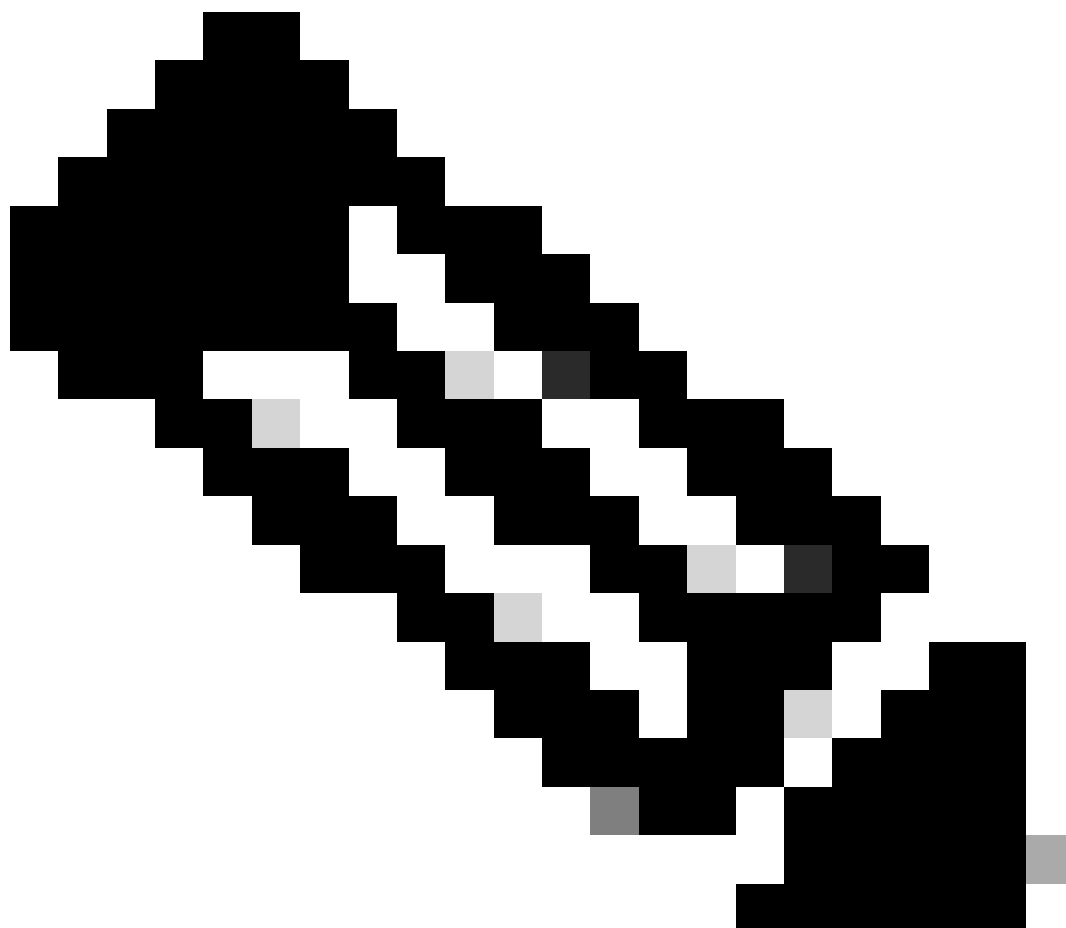
Technical Services... iCloud - Buscar mi... Cisco Internal www.cisco.com/c/... Cisco General BUFF Dedicated Instance WxC Calling Voice Ir

 RADKit Client Proxy

Service ID: r7nz-6n40-x3su

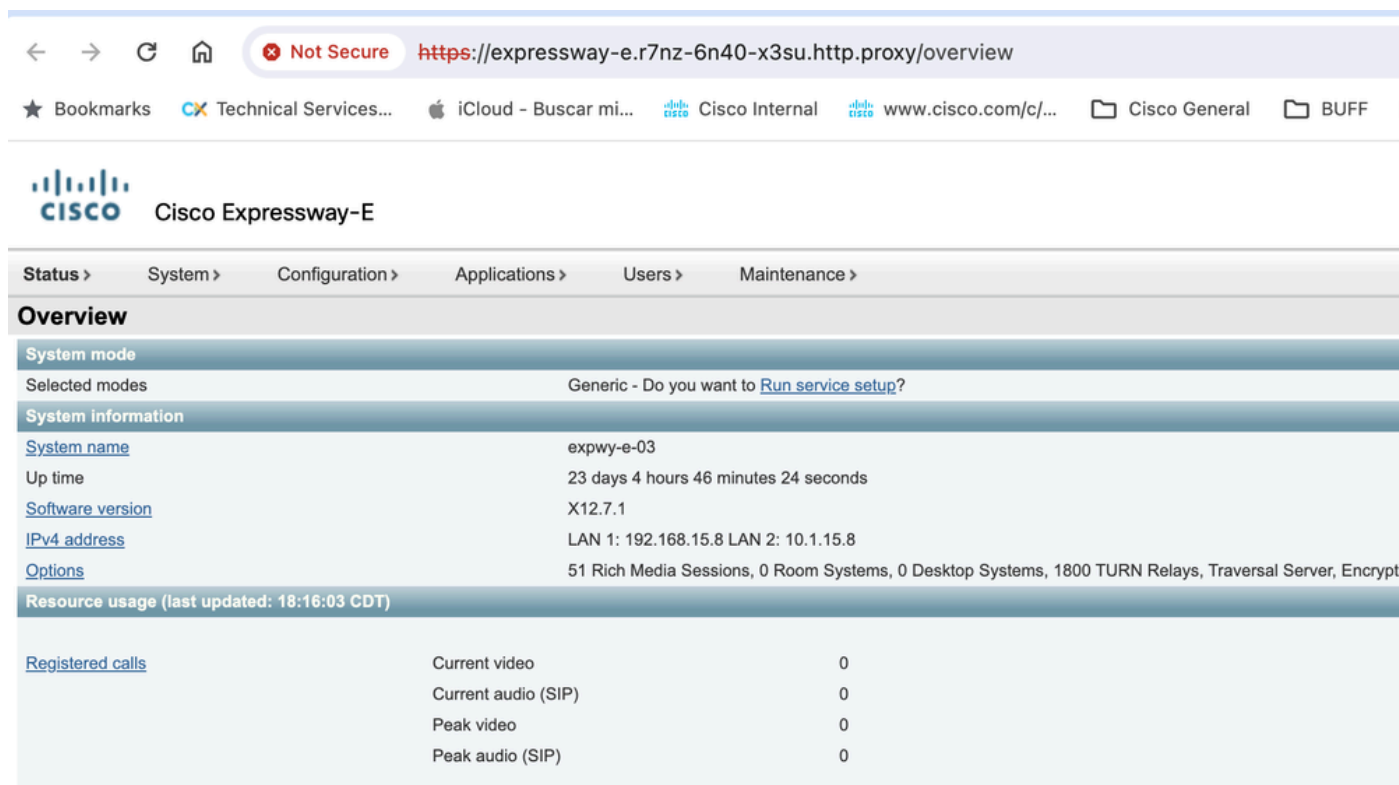
| Device name  | TCP port forwards | Supports HTTP                  | Reset Session          |
|--------------|-------------------|--------------------------------|------------------------|
| expressway-c | 443;8443          | <a href="#">Go to web page</a> | <button>Reset</button> |
| expressway-e | 443;8443          | <a href="#">Go to web page</a> | <button>Reset</button> |
| cucmhq       | 443;8443          | <a href="#">Go to web page</a> | <button>Reset</button> |

[← Go back](#)



注:RADKit Clientで初めてHTTPプロキシを設定する場合は、デバイスのWebページを開く前に各デバイスのResetオプションをクリックすることをお勧めします。

ステップ 5 : Webページが表示されます。



← → ↻ 🏠 **Not Secure** https://expressway-e.r7nz-6n40-x3su.http.proxy/overview

★ Bookmarks 🌐 Technical Services... 🍏 iCloud - Buscar mi... 🌐 Cisco Internal 🌐 www.cisco.com/c/... 📁 Cisco General 📁 BUFF

**CISCO** Cisco Expressway-E

Status > System > Configuration > Applications > Users > Maintenance >

### Overview

**System mode**

Selected modes Generic - Do you want to [Run service setup?](#)

**System information**

[System name](#) expwy-e-03

[Up time](#) 23 days 4 hours 46 minutes 24 seconds

[Software version](#) X12.7.1

[IPv4 address](#) LAN 1: 192.168.15.8 LAN 2: 10.1.15.8

[Options](#) 51 Rich Media Sessions, 0 Room Systems, 0 Desktop Systems, 1800 TURN Relays, Traversal Server, Encrypted

**Resource usage (last updated: 18:16:03 CDT)**

| <a href="#">Registered calls</a> |                     |   |
|----------------------------------|---------------------|---|
|                                  | Current video       | 0 |
|                                  | Current audio (SIP) | 0 |
|                                  | Peak video          | 0 |
|                                  | Peak audio (SIP)    | 0 |

- ポート転送

ステップ 1 : デバイスに設定されているTCP転送ポートを確認します。

<#root>

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

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

ステップ 2 : ローカルポートをデバイスの宛先ポートにマッピングするように設定します。デバイスのGUIにアクセスするには、ローカルポートを使用する必要があります。

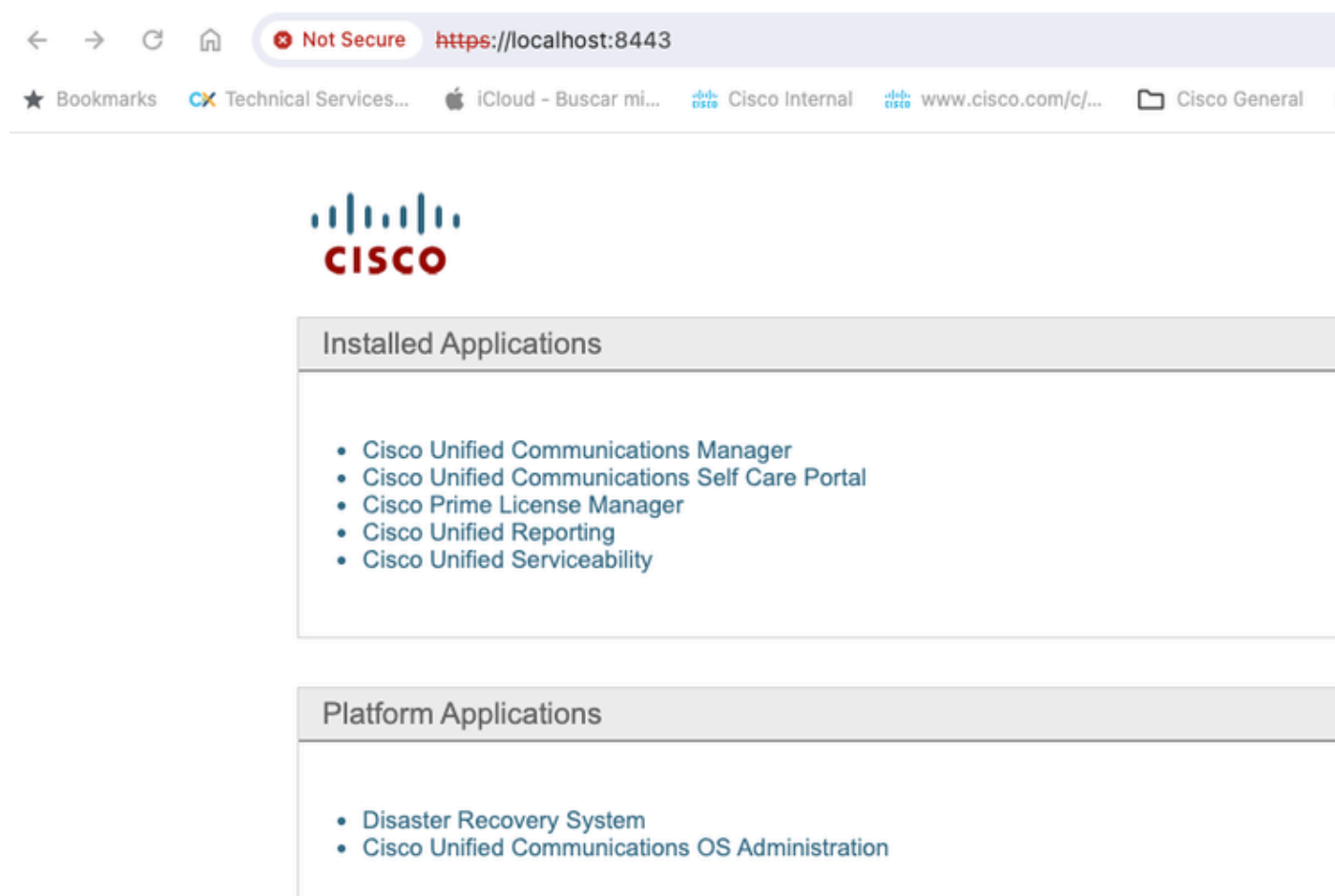
<#root>

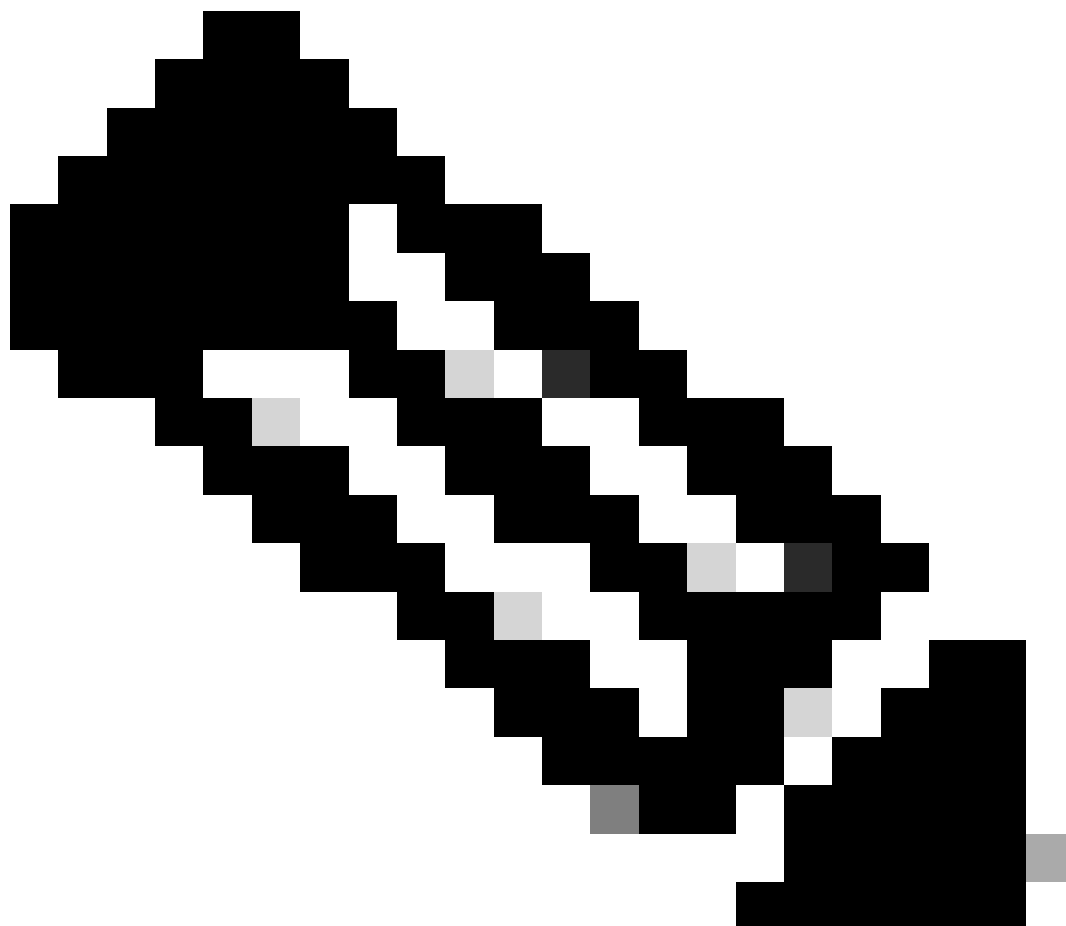
```
>>> cucm.forward_tcp_port(local_port=8443, destination_port=443)
```

```
>>>
>>> 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
-----
```

ステップ 3 : ブラウザを開き、手順2:<https://localhost:8443>で設定したポートのURLを入力します。

これで、デバイスのGUIにアクセスできるようになります。





注：製品のGUIにアクセスするには、ログインするためのクレデンシャルが必要です。したがって、ユーザはアクセス用に読み取り専用ユーザアカウントを作成することをお勧めします。

---

## ログ収集

- RTMT

ステップ 1：デバイスに設定されたTCP転送ポートにポート8443がリストされていることを確認します。

```
<#root>
```

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

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

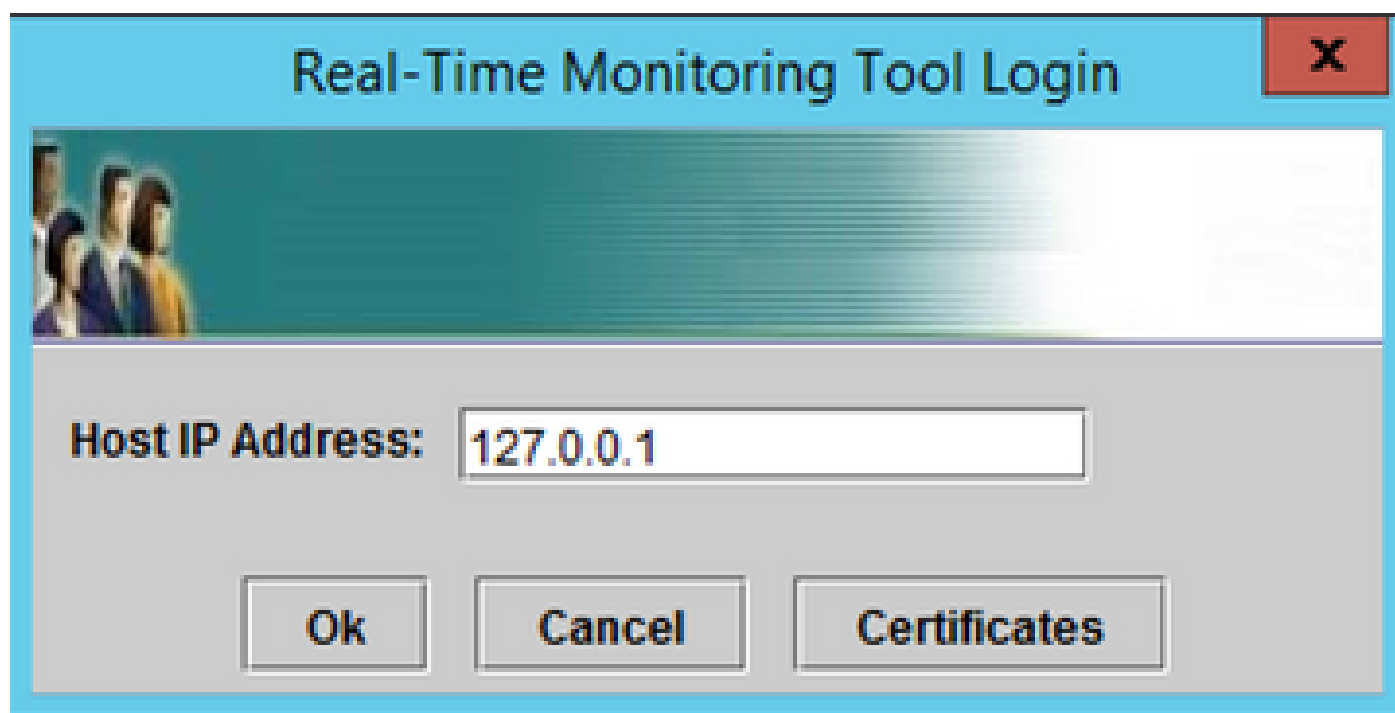
ステップ 2 : ローカルポートと同じポート8443を設定し、ポート8443をデバイスの宛先ポートとしてマッピングします。

<#root>

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

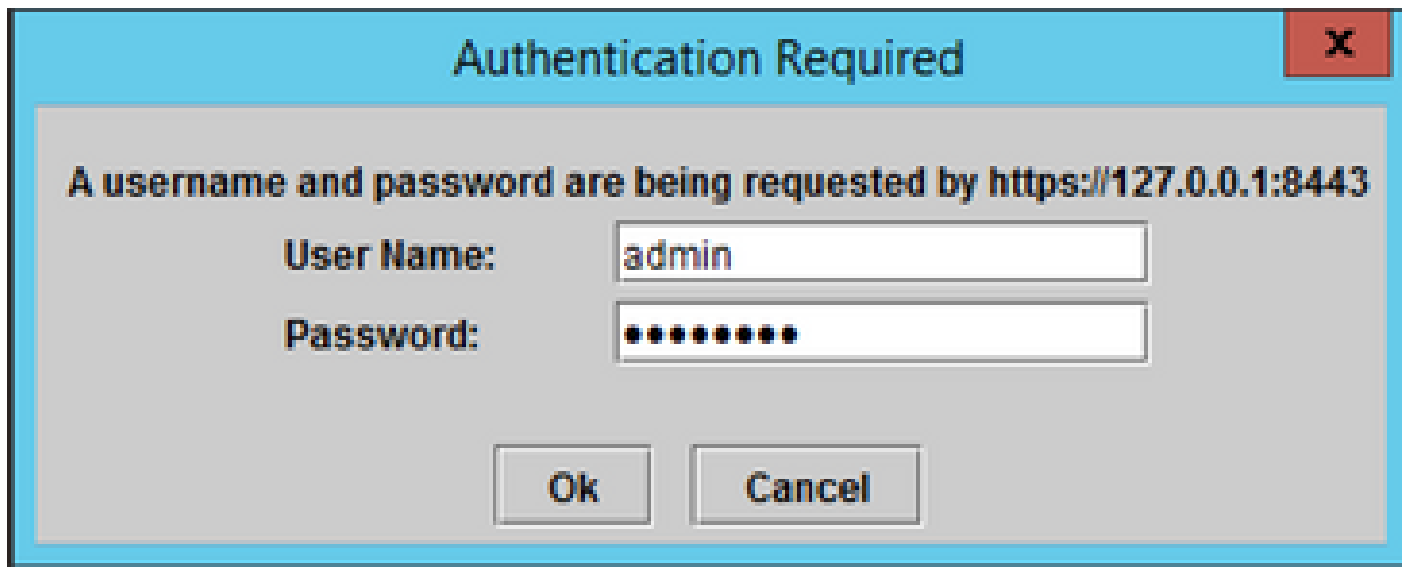
```
>>> cucm.forward_tcp_port(8443,8443)
[RUNNING] <radkit_client.sync.port_forwarding.TCPortForwarder object at 0x1077defa0>
-----
status          RUNNING
serial          None
device_name     cesavilacucm
local_port      8443
destination_port 8443
#active         0
#failed         0
#closed        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

ステップ 3 : RTMTを開き、ホストIPアドレスに127.0.0.1と入力すると、自動的にポート8443が使用されます。

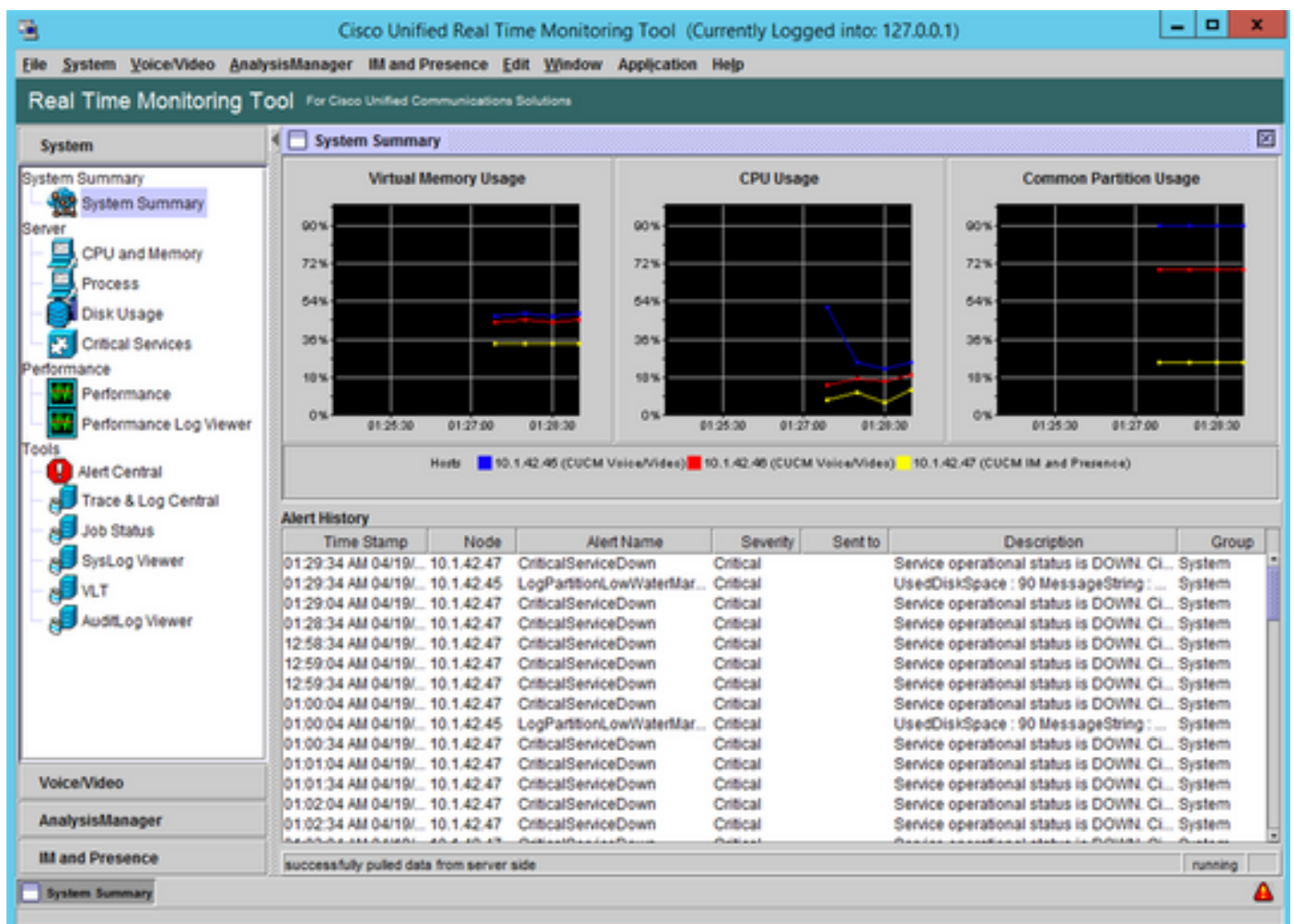


ステップ 4 : 正しいクレデンシャルでログインします。

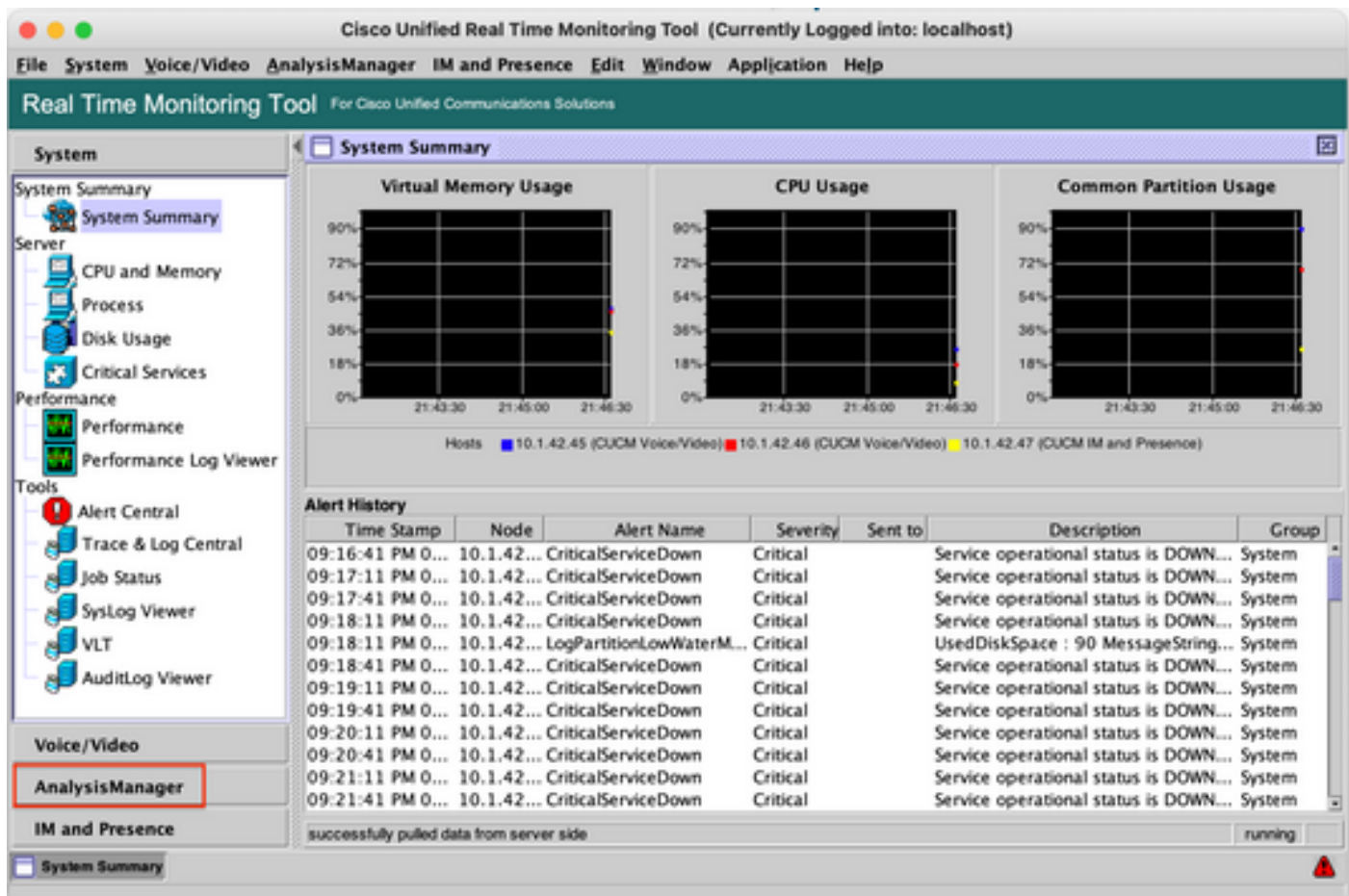




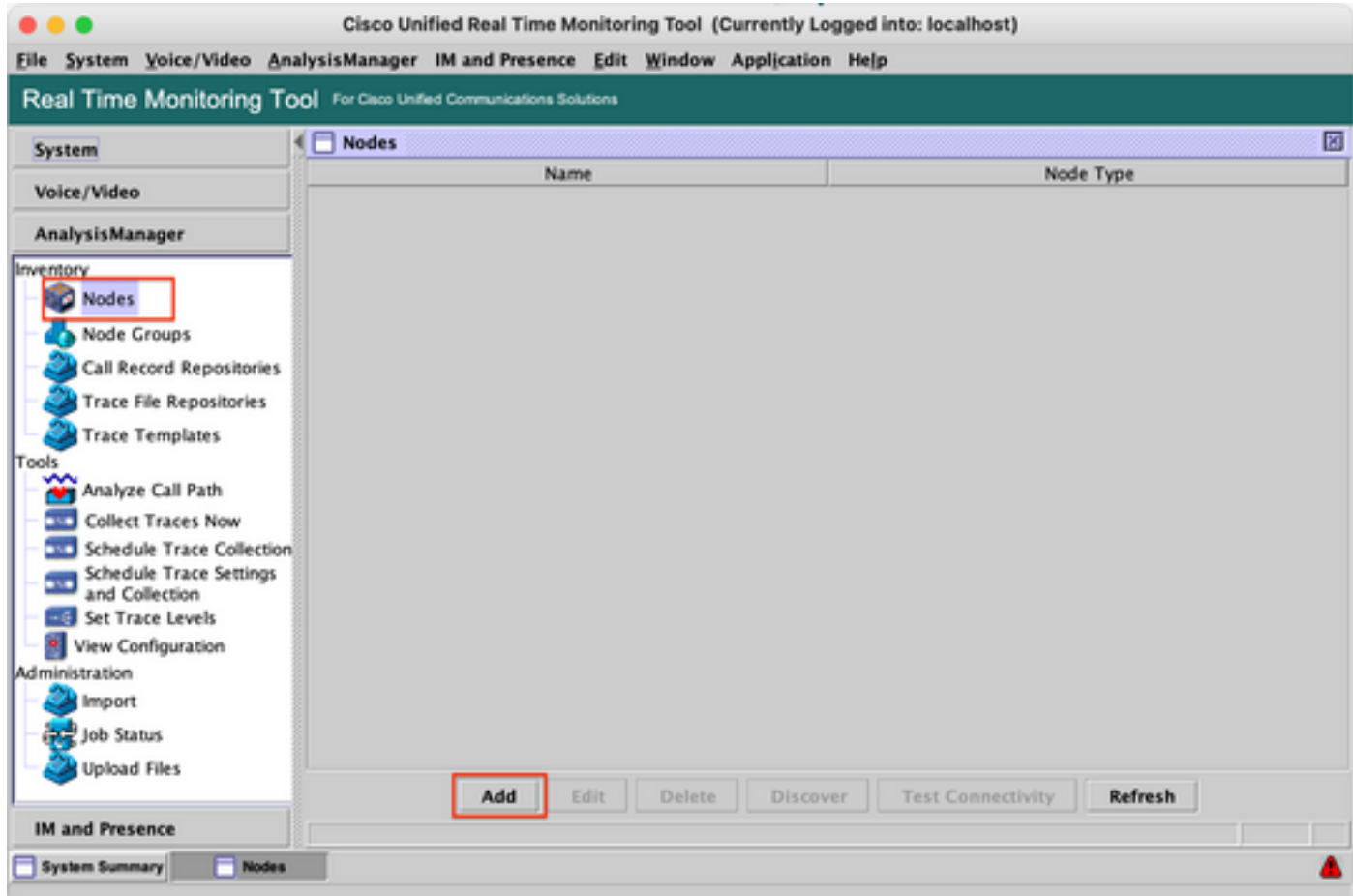
ステップ 5：RTMTが表示されます。



手順 6：左側のパネルのAnalysisManagerに移動します。



手順 7 : NodesおよびAddをクリックし、localhostおよび転送されたTCPポートを使用して追加されるデバイスの詳細を設定します。



**Add Node**

Node Type\* CUCM Voice/Video

IP/Host Name\* 127.0.0.1

Transport Protocol\* HTTPS

Port Number\* 8443

User Name\* admin

Password\* .....

Confirm Password\* .....

Description

Associated Call Record Repositories

Associated Trace File Repositories

Associated Group

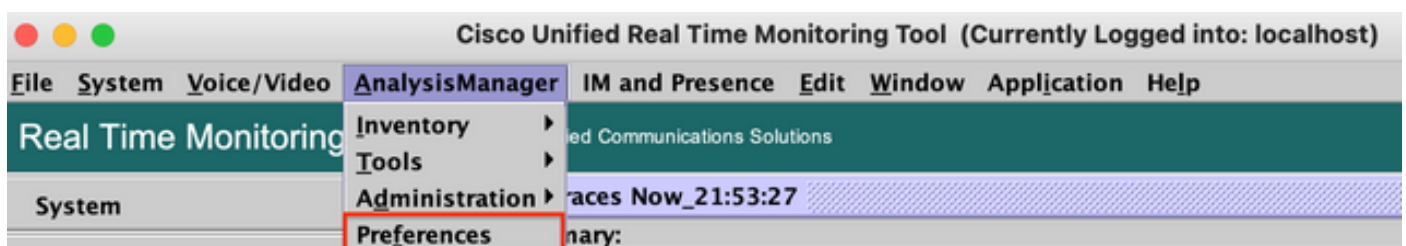
☒ AllNodes

Advanced...

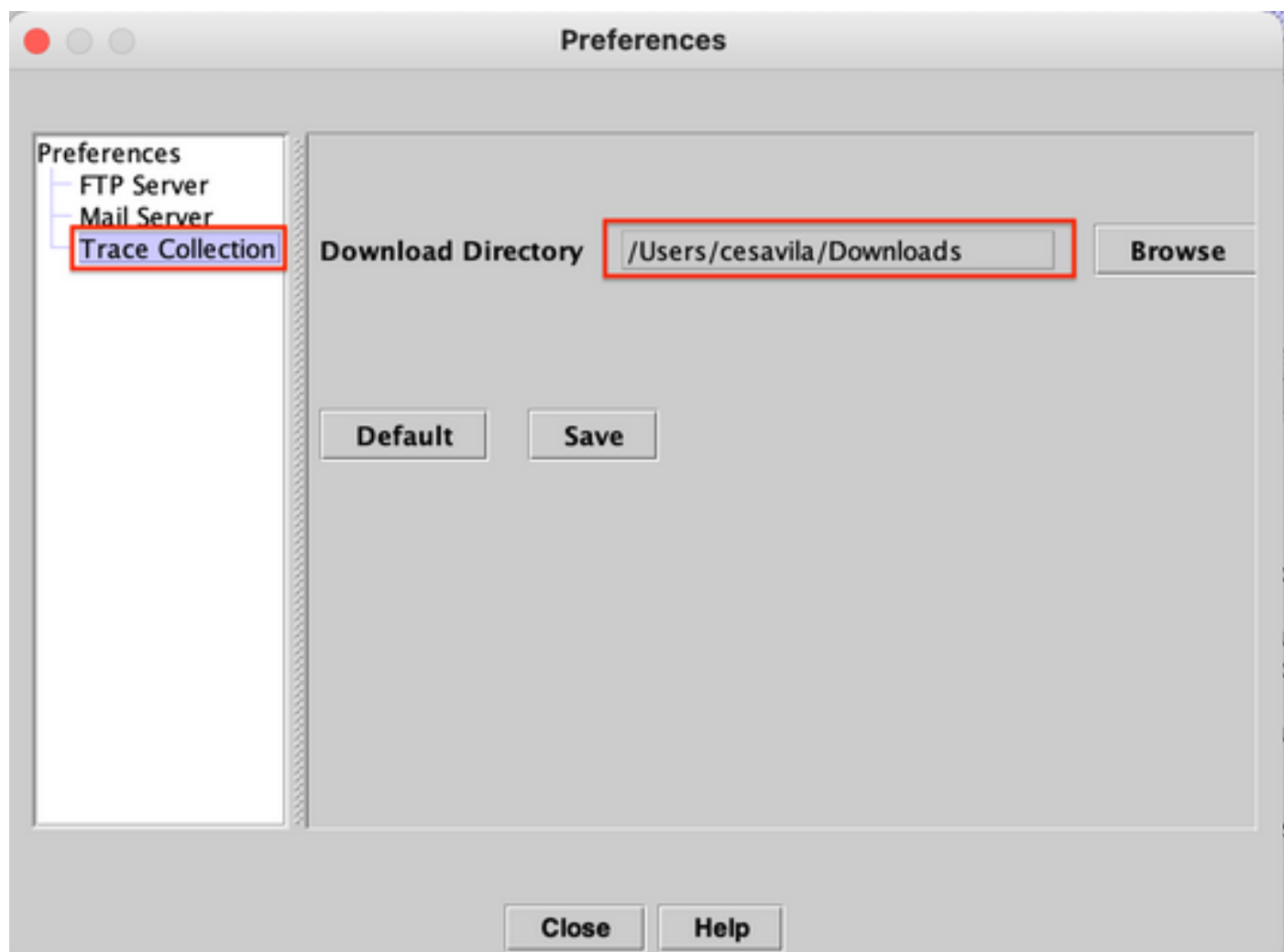
\* Required Fields

Save Cancel

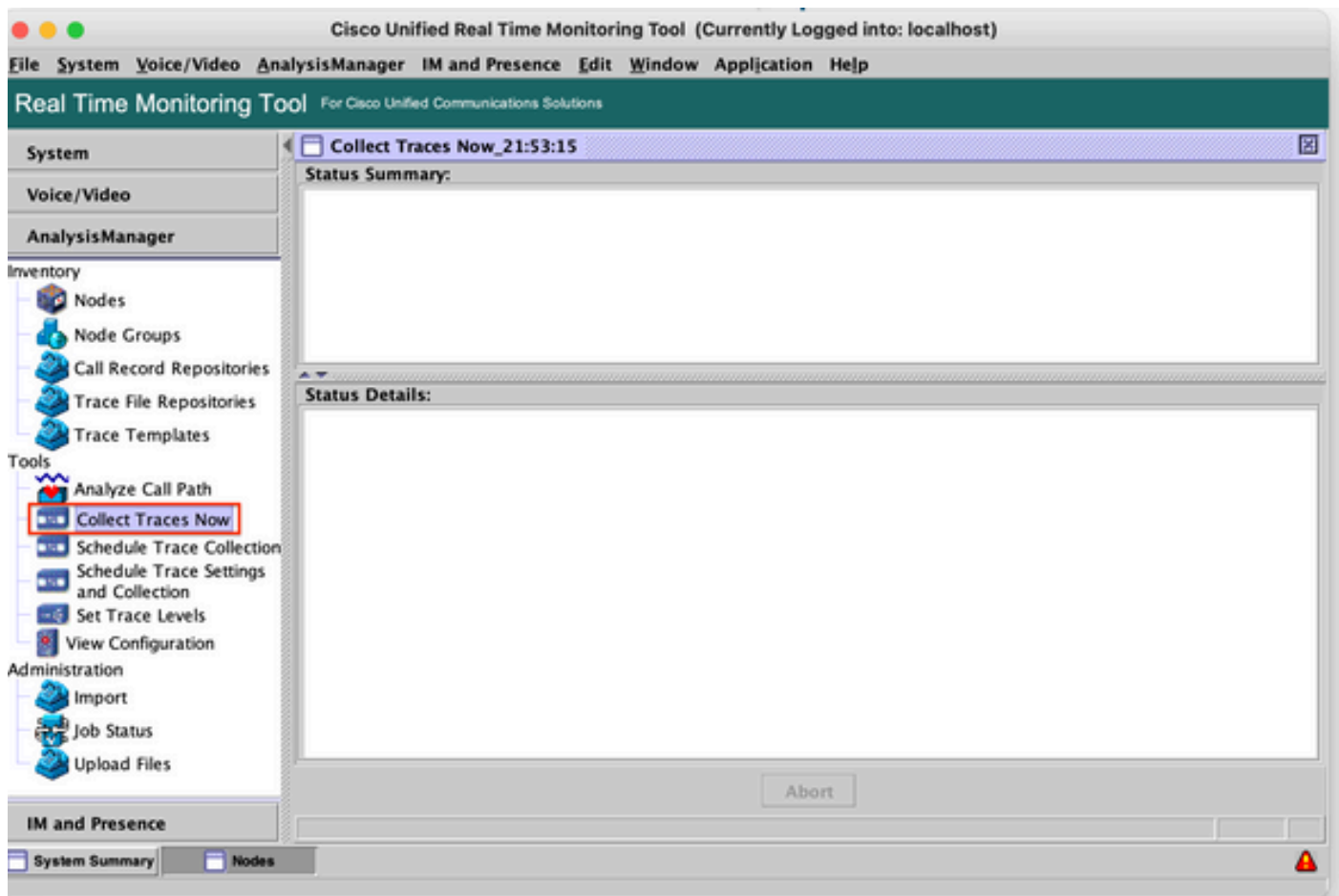
ステップ 8：上部のメニューでAnalysis Managerをクリックして、Preferencesを選択します。



ステップ 9：Trace Collectionに移動し、Correct folder to download the logsを選択します。  
Saveをクリックし、Closeをクリックします。



ステップ 10 : 「トレースの収集」に移動します。



ステップ 11 オプション Node を選択し、ステップ 7 で追加したデバイスを選択して、Customize をクリックします。

**Collect Traces Now**

Choose a Node or Group to perform query on:

☐ Group ☒ Node

| Name      | Node Type        | Description |
|-----------|------------------|-------------|
| 127.0.0.1 | CUCM Voice/Video |             |

Use Template: None **Customize...**

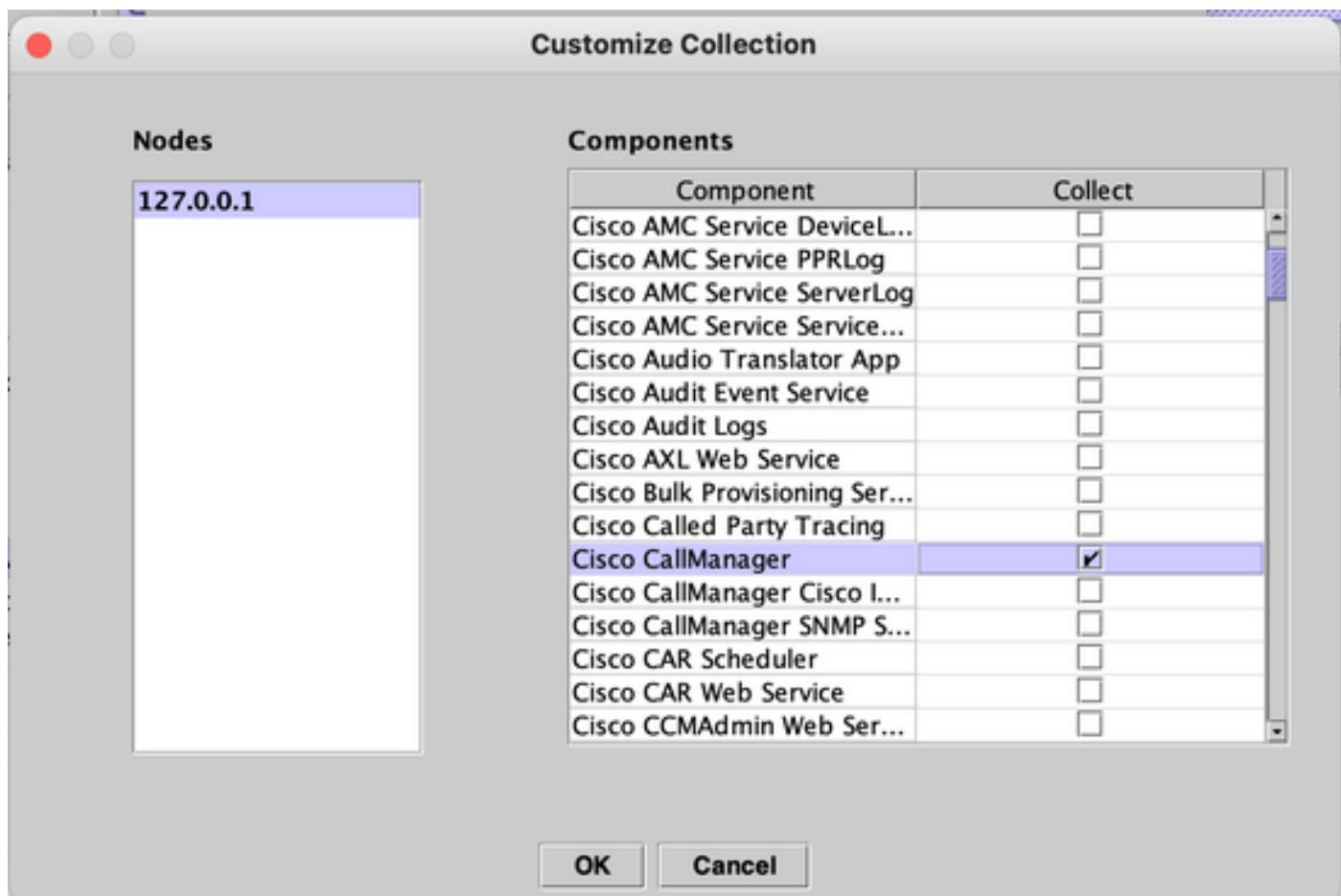
Start Time:

End Time: 04-27-2023 21:53:27

Time Zone: (GMT-6:0)Central Dayl...

**View Summary** **OK** **Cancel** **Help**

ステップ 12 デバイスから収集するログを選択し、OKをクリックします。



ステップ 13最後に、収集するログのStart TimeとEnd Timeを選択して、OKをクリックします。



**Collect Traces Now**

Choose a Node or Group to perform query on:

☐ Group ☒ Node

| Name      | Node Type        | Description |
|-----------|------------------|-------------|
| 127.0.0.1 | CUCM Voice/Video |             |

Use Template: None ▼ Customize...

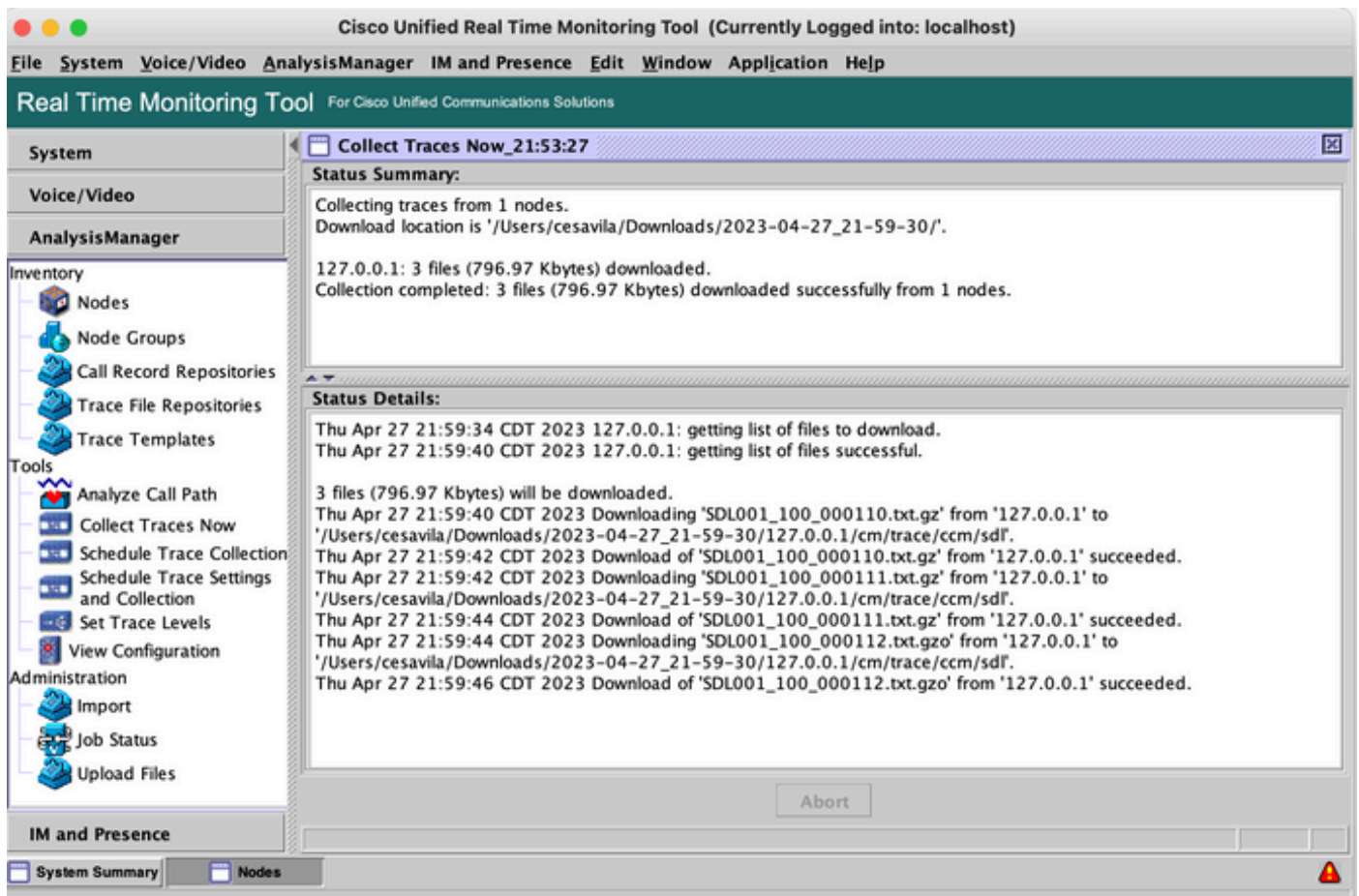
Start Time: 04-27-2023 21:00:00 ▼

End Time: 04-27-2023 21:53:27 ▼

Time Zone: (GMT-6:0)Central Dayl... ▼

View Summary **OK** Cancel Help

ステップ 14 : ファイルはローカルPC ( RADKitクライアントPC ) に正常にダウンロードされます。



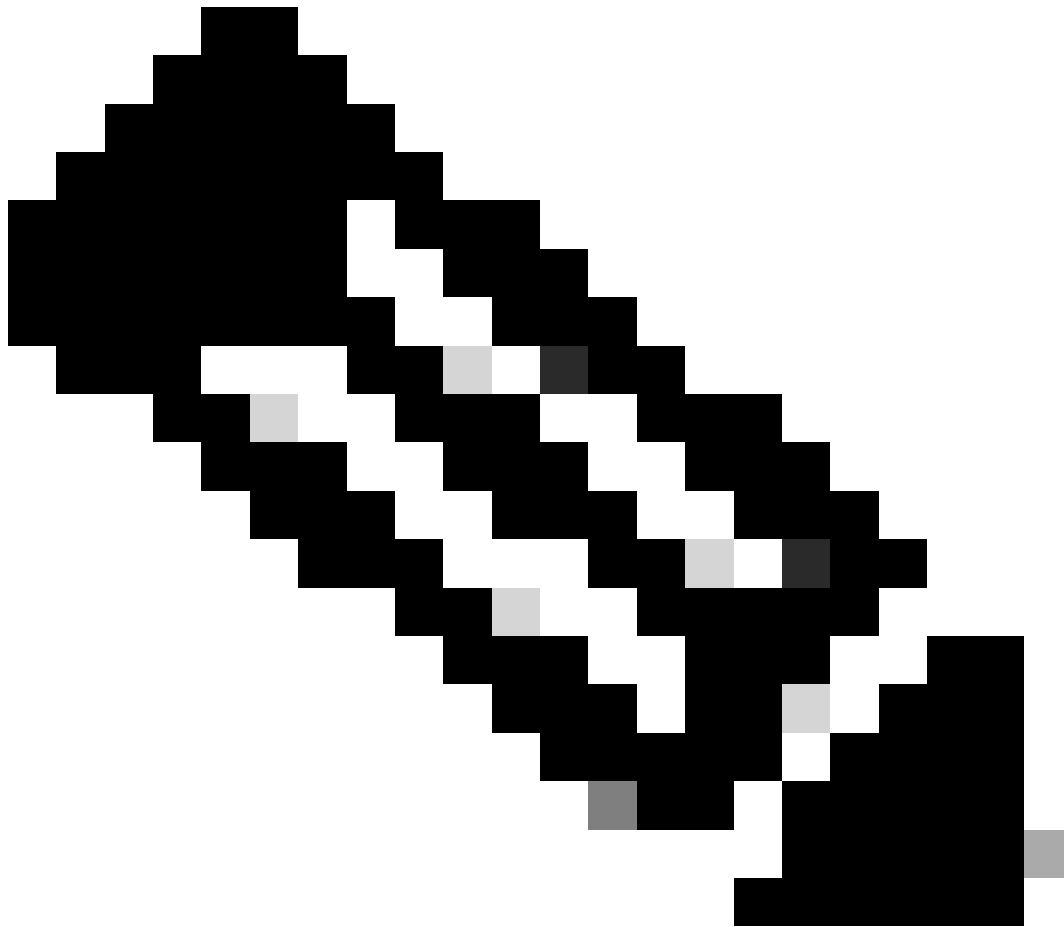
- SOAP API

SOAP APIは、現在CUCMでサポートされています。また、CMS、Expressway、CVPなどでもSwaggerがサポートされています。

ステップ 1： HTTPクレデンシャルがデバイス設定のRADKitサービスに追加されていることを確認します。

ステップ 2： RADKitクライアントでHTTP Postコマンドを実行し、リソースパス、要求の本文、必要なパラメータとヘッダーを指定します。

```
>>>
... 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'])
>>>
```



注：ポストプロセッサオプション「cucm-extract」は、ログをファイルに保存できるようにHTTP応答ヘッダーを削除するために使用されます。

```
>>> r
[SUCCESS] HttpResponse(device_name='cucmsiteb', method='POST', url='/logcollectionservice2/services/LogCollectionPortTypeService', status_code=200)
-----
identity      cesavila@cisco.com
service_id    ckt7-tv6c-uale
device_name   cucmsiteb
method        POST
url           /logcollectionservice2/services/LogCollectionPortTypeService
status_code   200 OK
content       b'\x1f\x8b\x08\x00\x00\x00\x00\x04\x03\xd4X[\x8f\xdaF\x14~G\xe2?\x9c\xbe%\x95\x81\xc1\x170N\xa9\xca\x1aH\xac,\xae\xae\xcd\xf6\xa6\xd6\x1a\xdb\x03
X16\xb1\xc7\xc9n\xb5?\xbeg\xcc%\xf6n\xd8\x90\xaaUU\xb4f\x99\xe3\xb9|s\xae\xdf\x0cQ\xd4...'
-----
```

ステップ 3：内容をファイルに保存して、トレースファイルをローカルPCに保存します。

<#root>

```
>>> content = r.content
```

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

## RADKitの使用例

強調表示されているように、RADKitはWebExを使用せずに、コラボレーションサーバなどのネットワークデバイスへのセキュアな接続を提供します。これは、必要なデバイスへのオンデマンドアクセスを提供することで、データ収集に関する課題の一部を簡素化することを目的としています。

特にコラボレーションの導入について話すと、RADKitは現在、次のようなさまざまな問題に非常に役立ちます。

- DBレプリケーションの問題。
- 証明書の再生手順。
- システムのヘルスチェック。
- GUI/CLIでの設定検証
- Webインターフェイスを介したログ収集 ( CER、Expressway、CIMCなど )
- 音声ゲートウェイ上のCLIを介したデバッグログ

## 関連情報

- RADKitメインページ <https://radkit.cisco.com/>
- 外部RADKitサポートページ <https://community.cisco.com/t5/radkit-discussions/bd-p/disc-radkit>

## 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。