Set Up RADKit in a Collaboration Environment

Contents

Introduction

This document describes the steps to set up RADKit and shows the configuration necessary to start the use of it with Collaboration Products.

Requirements

Cisco recommends that you have knowledge on these topics:

- Basic knowledge of any VOS Collaboration product
- Basic knowledge of CLI/SSH Access

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Unified Communications Manager 12.5 and 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. If your network is live, ensure that you understand the potential impact of any command.

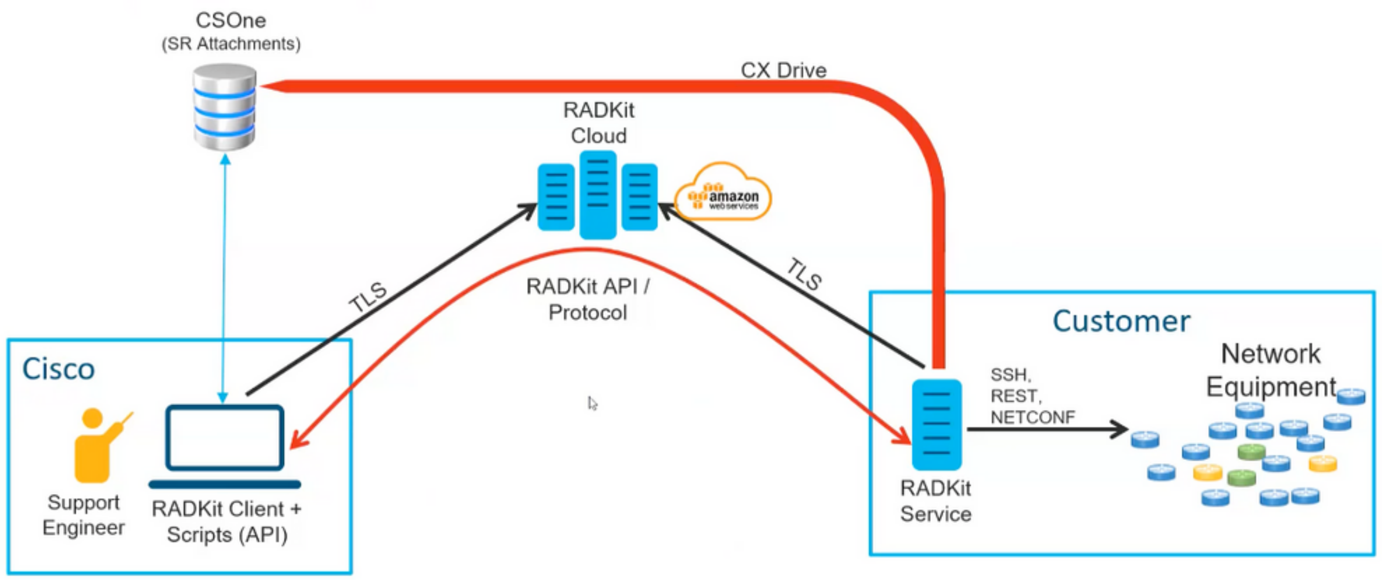
Terminology

RADKit: It is a connector providing secure remote access to the user devices to Cisco TAC engineers and partners. It supports multiple protocols to interact with devices, such as SSH or HTTP/HTTPs.

RADKit Service: This is the **Server** side. It is handled and entirely managed by the **User**. From the Server side, user controls, who canaccess the devices and for how long. Radkit Service must have conectivity to the devices in the network to provide access to them.

RADKit Client: This is the **Client** side. It is the PC used to connect to the devices in the user network.

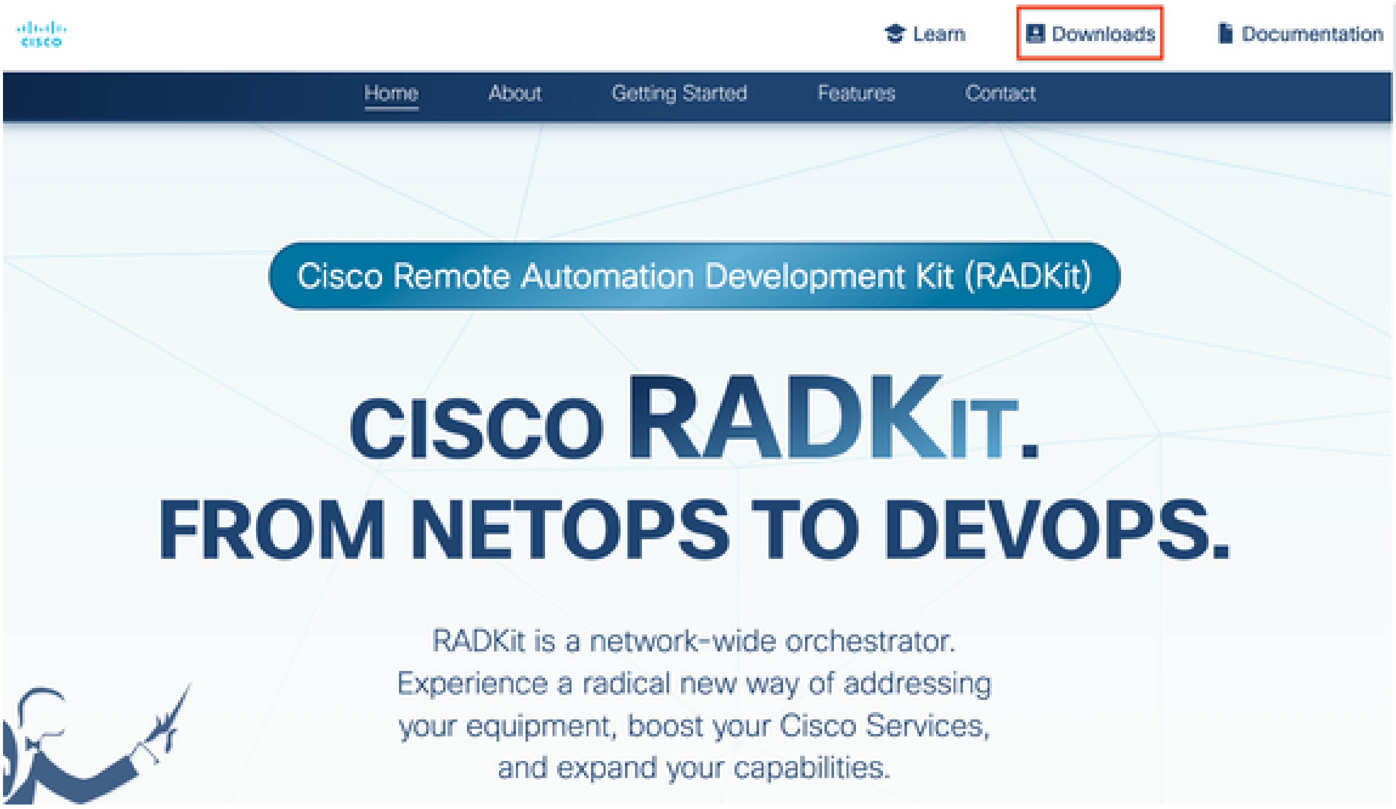
RADKit Architecture



RADKit Architecture

RADKit Installation

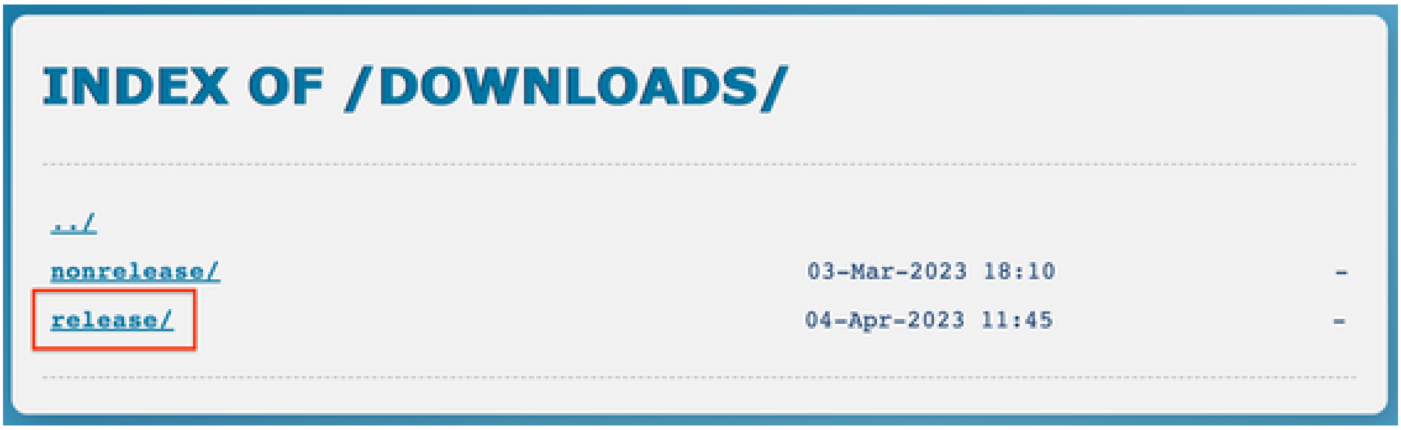
Step 1. Navigate to **https://radkit.cisco.com** and click **Downloads**, then go to the **release** folder.



Cisco Remote Automation Development Kit (RADKit)

CISCO RADKIT.
FROM NETOPS TO DEVOPS.

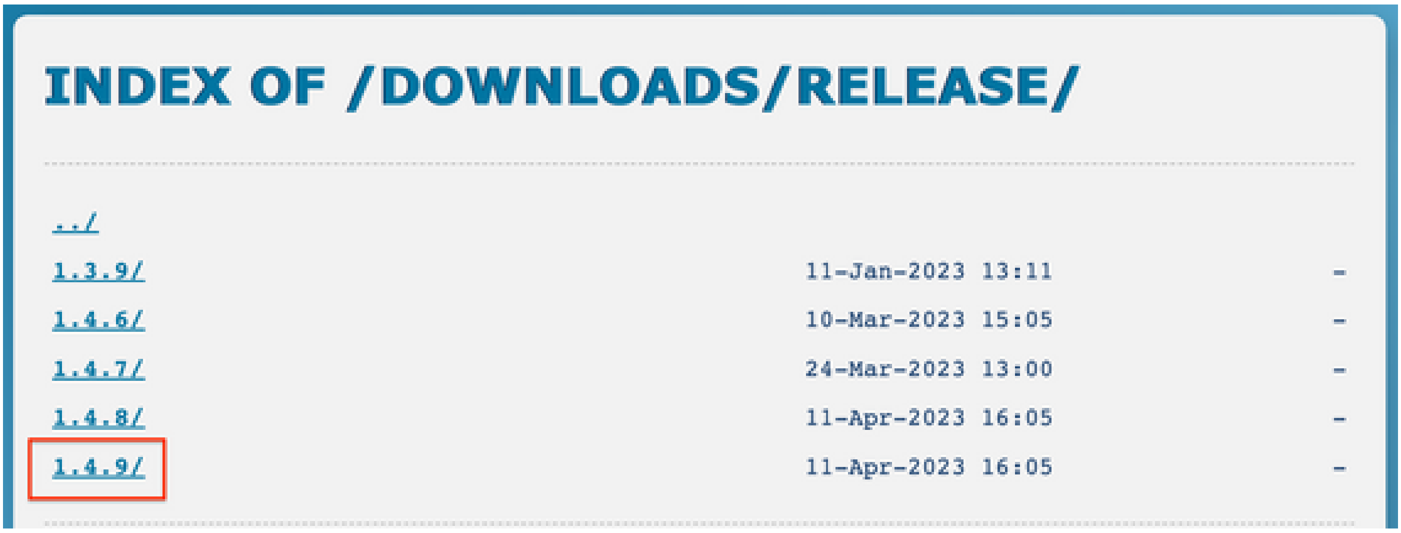
RADKit is a network-wide orchestrator. Experience a radical new way of addressing your equipment, boost your Cisco Services, and expand your capabilities.



INDEX OF /DOWNLOADS/

../		
nonrelease/	03-Mar-2023 18:10	-
release/	04-Apr-2023 11:45	-

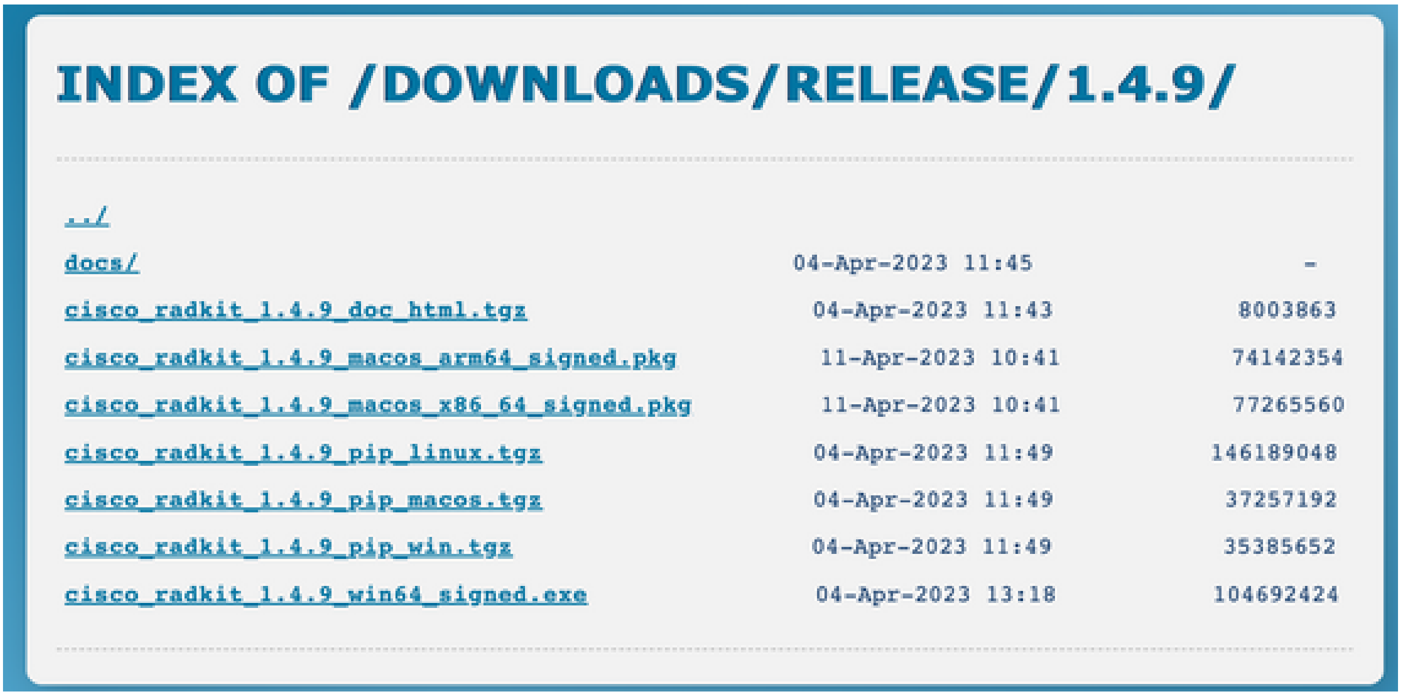
Step 2. Click the latest release.



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	-

Step 3. Download the correct file depending on your OS system.



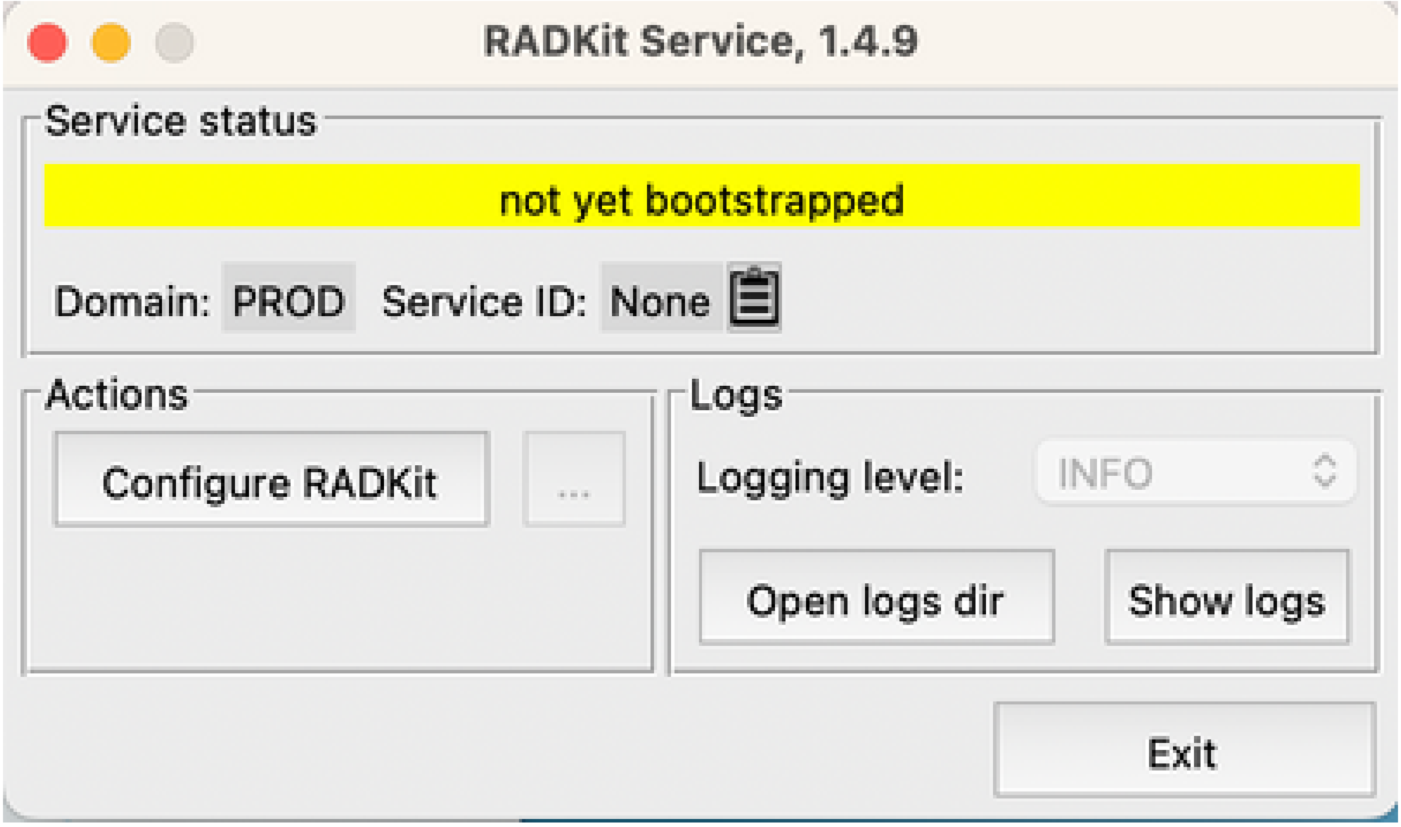
```
INDEX OF /DOWNLOADS/RELEASE/1.4.9/

../
docs/                                             04-Apr-2023 11:45                   -
cisco_radkit_1.4.9_doc_html.tgz                    04-Apr-2023 11:43             8003863
cisco_radkit_1.4.9_macos_arm64_signed.pkg          11-Apr-2023 10:41            74142354
cisco_radkit_1.4.9_macos_x86_64_signed.pkg         11-Apr-2023 10:41            77265560
cisco_radkit_1.4.9_pip_linux.tgz                   04-Apr-2023 11:49           146189048
cisco_radkit_1.4.9_pip_macos.tgz                   04-Apr-2023 11:49            37257192
cisco_radkit_1.4.9_pip_win.tgz                     04-Apr-2023 11:49            35385652
cisco_radkit_1.4.9_win64_signed.exe                04-Apr-2023 13:18           104692424
```

Step 4. Run the installer on the PC or server. As part of the installation, Radkit needs to install three applications: Radkit Service, Radkit Client and Radkit network console.

RADKit Service (User side)

Onboarding

Step 1. To start configuring the RADKit service, navigate to Applications and locate **RADKit Service**. The first time you run it shows a message "not yet bootstrapped".



RADKit Service, 1.4.9

Service status

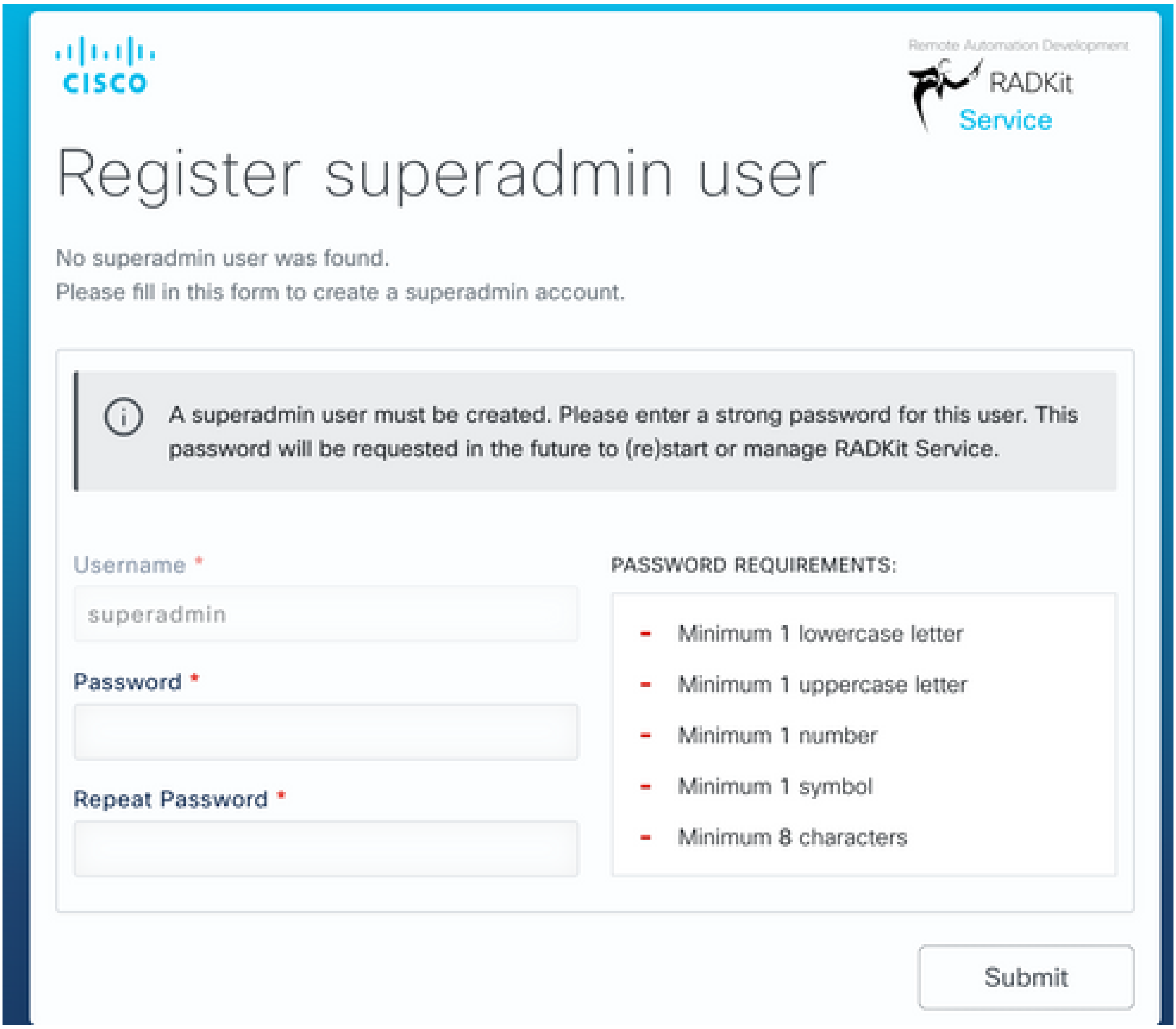
not yet bootstrapped

Domain: PROD Service ID: None

Logging level: INFO

Step 2. Click **Configure RADKit**, the browser pops up automatically with URL https://localhost:8081/bootstrap.

- Create password for **superadmin** user and click **Submit**.
- This **superadmin** username and password is requested each time the service is started or configured.



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 * superadmin

Password *

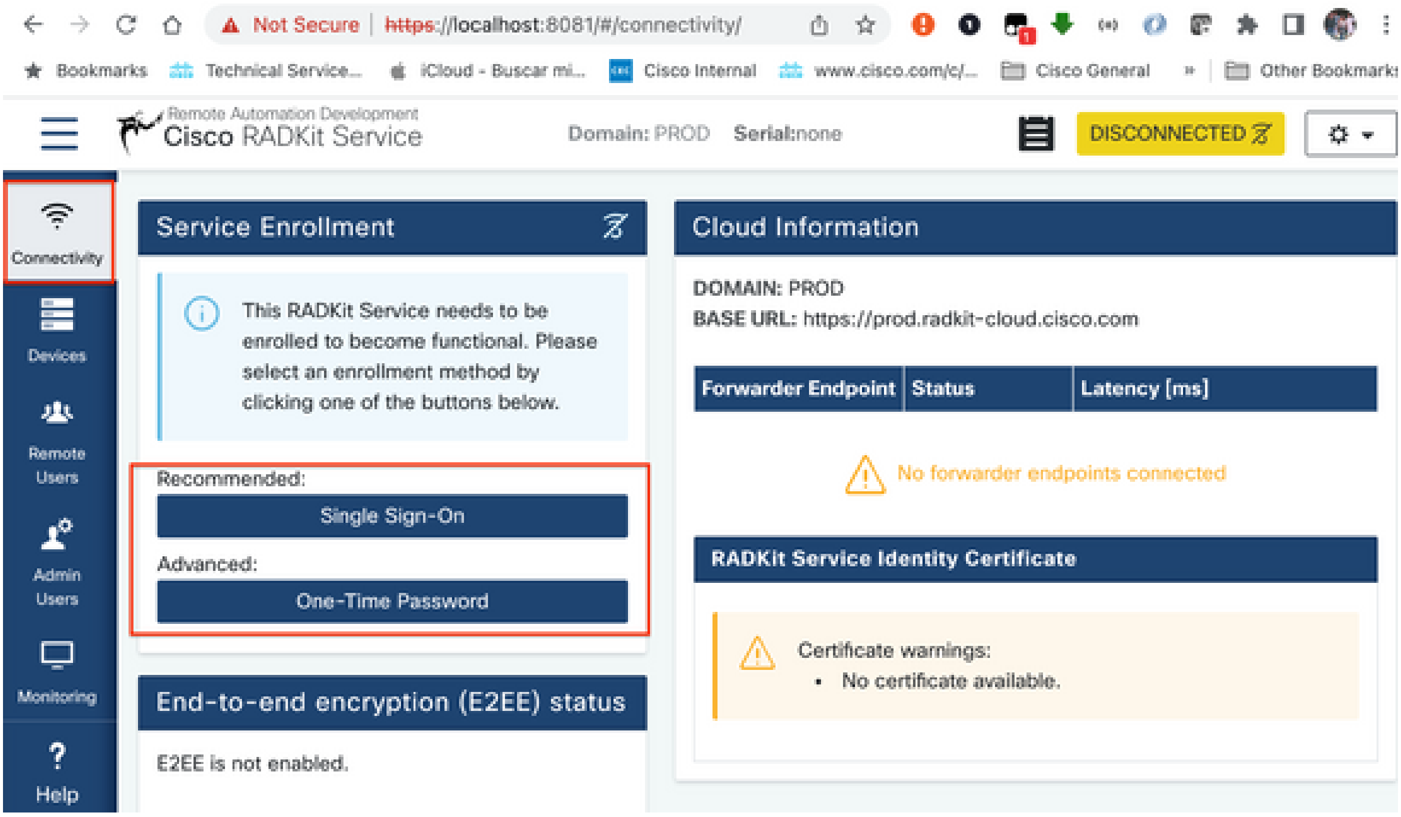
Repeat Password *

PASSWORD REQUIREMENTS:

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

Step 3. Once you click **Submit**, the browser redirects you to https://localhost:8081/#/connectivity/**.**

Under **Connectivity** > **Service Enrollment**, there are two authentications methods: **Single Sing-On** and **One-Time Password**.



Domain: PROD Serial:none

Service Enrollment

This RADKit Service needs to be enrolled to become functional. Please select an enrollment method by clicking one of the buttons below.

Recommended:

Single Sign-On

Advanced:

One-Time Password

End-to-end encryption (E2EE) status

E2EE is not enabled.

Cloud Information

DOMAIN: PROD
BASE URL: https://prod.radkit-cloud.cisco.com

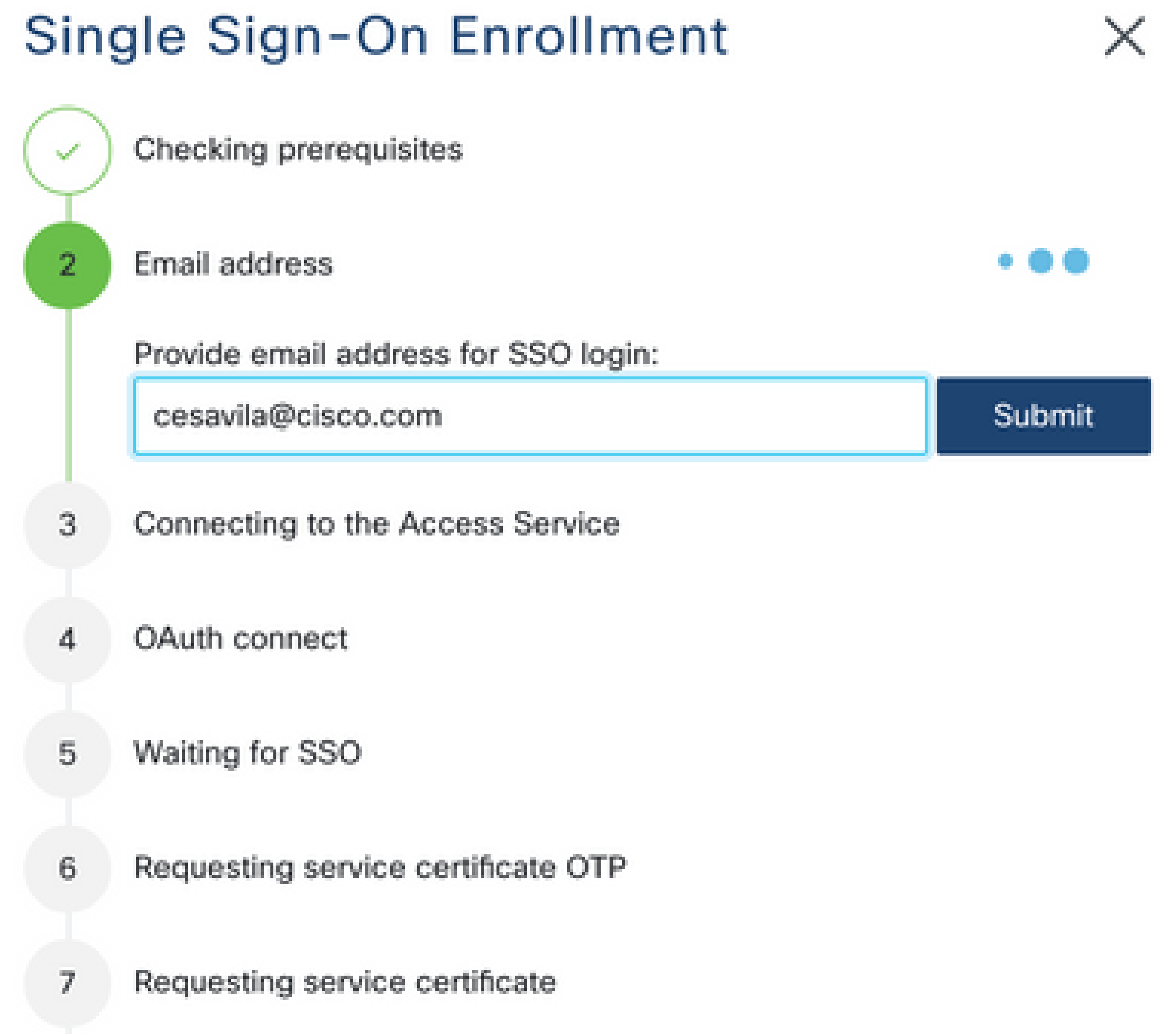
Forwarder Endpoint	Status	Latency [ms]

No forwarder endpoints connected

RADKit Service Identity Certificate

Certificate warnings:
- No certificate available.

Step 4. You can use **Single Sign-On** providing your CEC.



Single Sign-On Enrollment

✓ Checking prerequisites

2 Email address

Provide email address for SSO login:

cesavila@cisco.com

3 Connecting to the Access Service

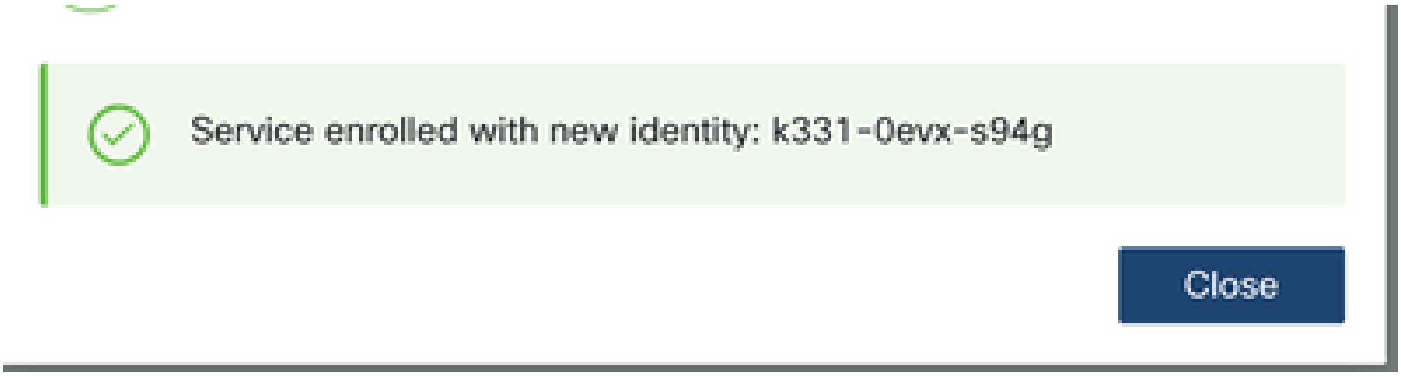
4 OAuth connect

5 Waiting for SSO

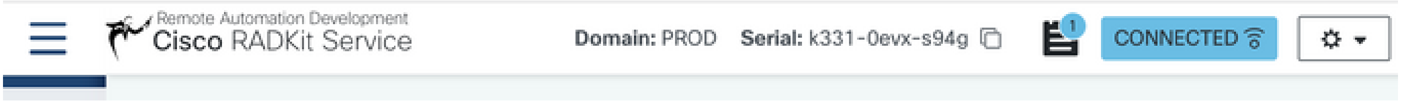
6 Requesting service certificate OTP

7 Requesting service certificate

Step 5. Complete the wizard and complete the steps until it shows "Service enrolled with new identity: xxxx-xxxx-xxxx", and when clicking on **Close** the service shows as **Connected**.



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



Domain: PROD Serial: k331-0evx-s94g

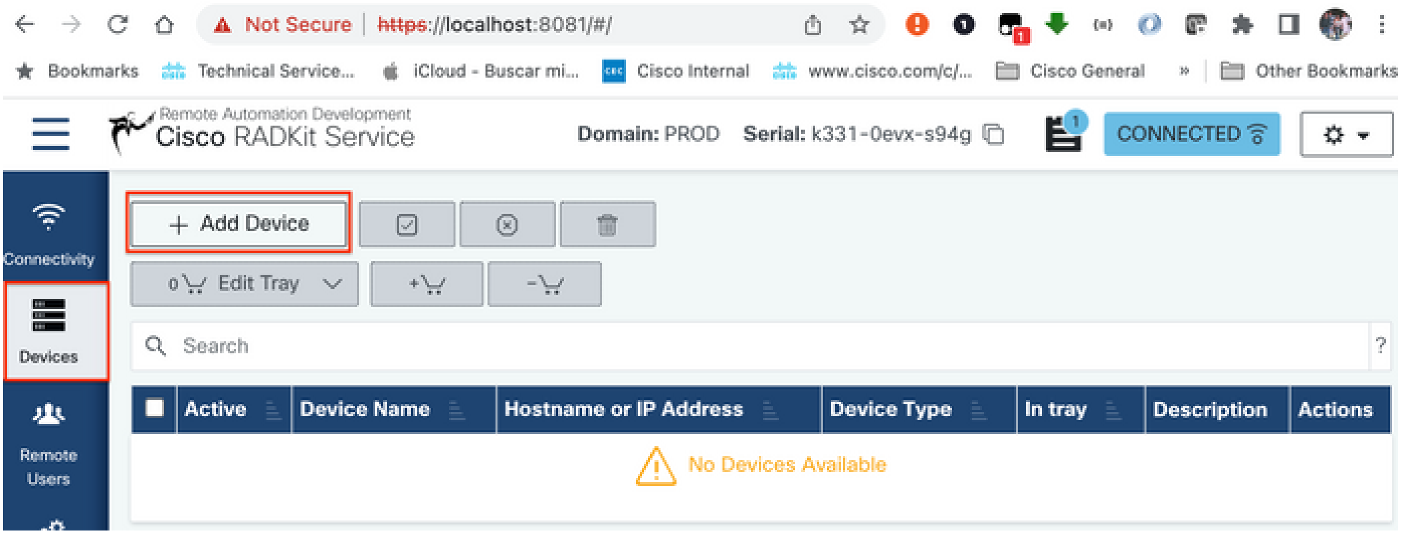
Note: A Cisco account is needed to activate RADKit Service.

Caution:

- If the Server where the RADKit Service is running requires a proxy to be defined, apart from defining the Proxy on the Server/PC itself, a environment variable also needs to be defined for the RADKit Service to work RADKIT_CLOUD_CLIENT_PROXY_URL=http://proxy.example.com:80.

Add devices

Step 1. Navigate to **Devices** and click **Add Device**.



Domain: PROD Serial: k331-0evx-s94g

☐	Active	Device Name	Hostname or IP Address	Device Type	In tray	Description	Actions

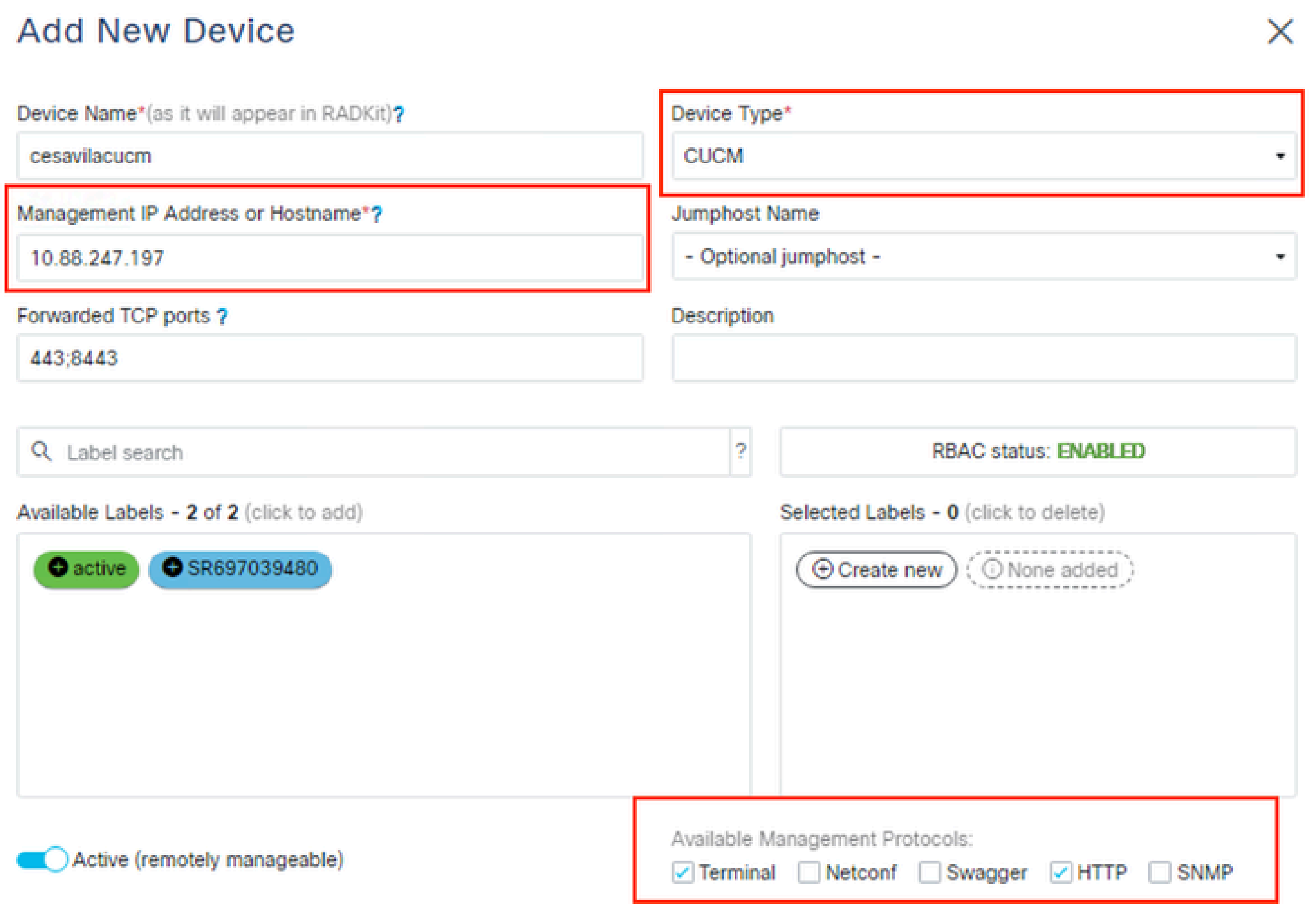
No Devices Available

Step 2. You need to configure the next details:

- Device Name
- Management IP address or Hostname
- Device Type

Additionally, you must configure **Forwarded TCP ports,** which are ports used by the device that need to be accessible from the RADKit Client. On this example,the ports used are 443 for GUI Access and 8443 for RTMT.

Finally, select the available Management Protocols, in this case **Terminal** and **HTTP**.



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

Device Type* CUCM

Management IP Address or Hostname*? 10.88.247.197

Jumphost Name - Optional jumphost -

Forwarded TCP ports ? 443;8443

Description

RBAC status: ENABLED

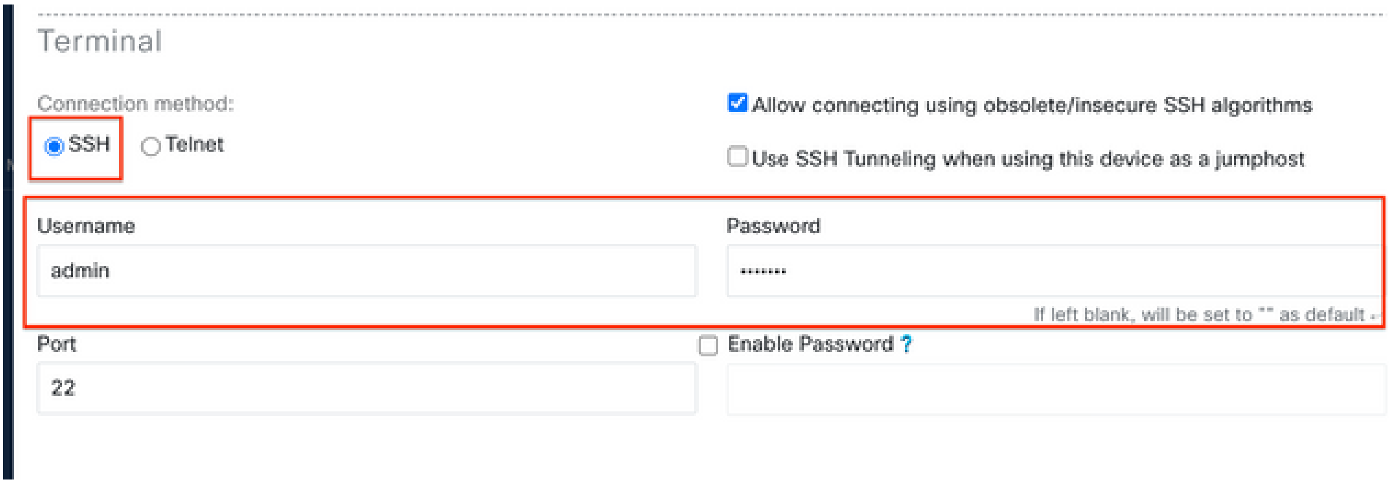
Available Labels - 2 of 2 (click to add): active, SR697039480

Selected Labels - 0 (click to delete)

Active (remotely manageable)

Available Management Protocols:
☑ Terminal ☐ Netconf ☐ Swagger ☑ HTTP ☐ SNMP

Step 3. For each Management Protocol configure the correct settings and click **Add & Close**.



Terminal

Connection method: ● SSH ○ Telnet

☑ Allow connecting using obsolete/insecure SSH algorithms

□ Use SSH Tunneling when using this device as a jumphost

Username: admin

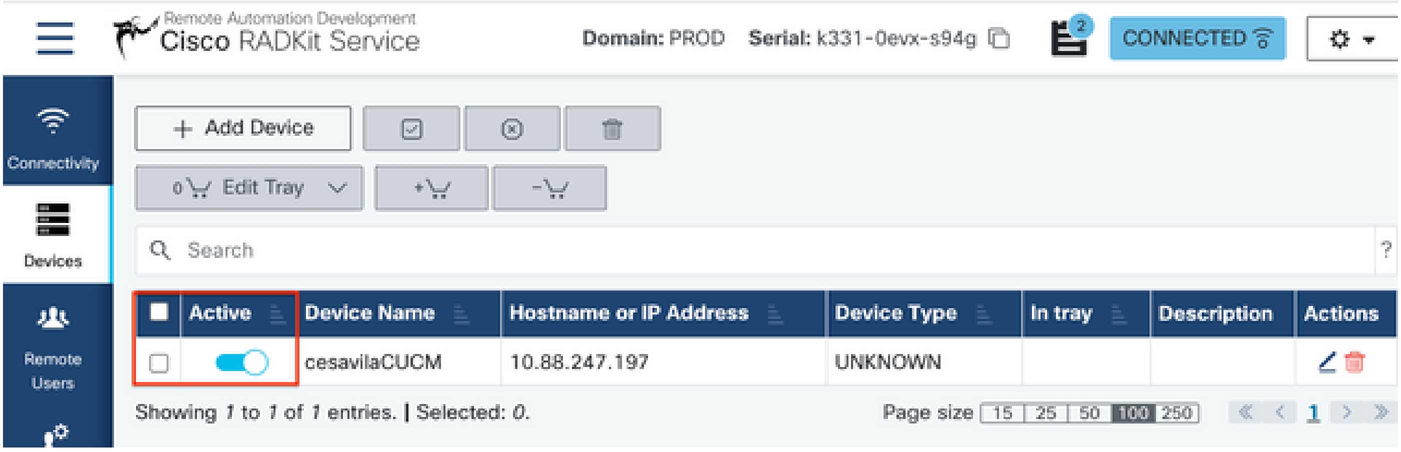
Password: ·······

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

Port: 22

□ Enable Password ?

Step 4. Once added, the device must be displayed in the device list, it can be enabled/disabled for remote access.



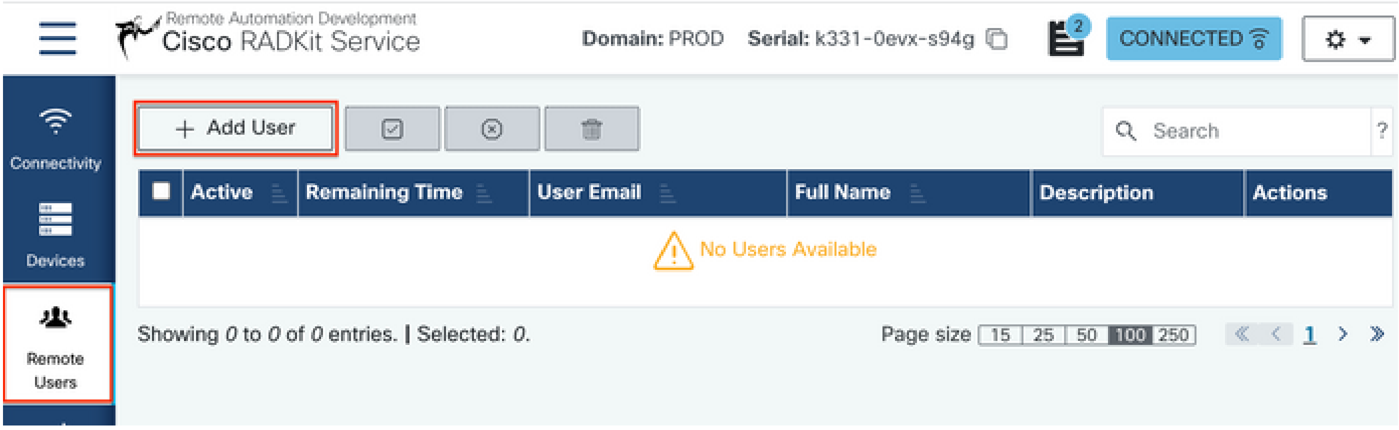
Domain: PROD Serial: k331-0evx-s94g CONNECTED

□	Active	Device Name	Hostname or IP Address	Device Type	In tray	Description	Actions
□	●	cesavilaCUCM	10.88.247.197	UNKNOWN			

Showing 1 to 1 of 1 entries. | Selected: 0. Page size 15 25 50 100 250

Authorize remote users

Step 1. In order to grant user access to the Devices configured in the RADKit Service, go to **Remote Users** and select **Add Users**.



Domain: PROD Serial: k331-0evx-s94g CONNECTED

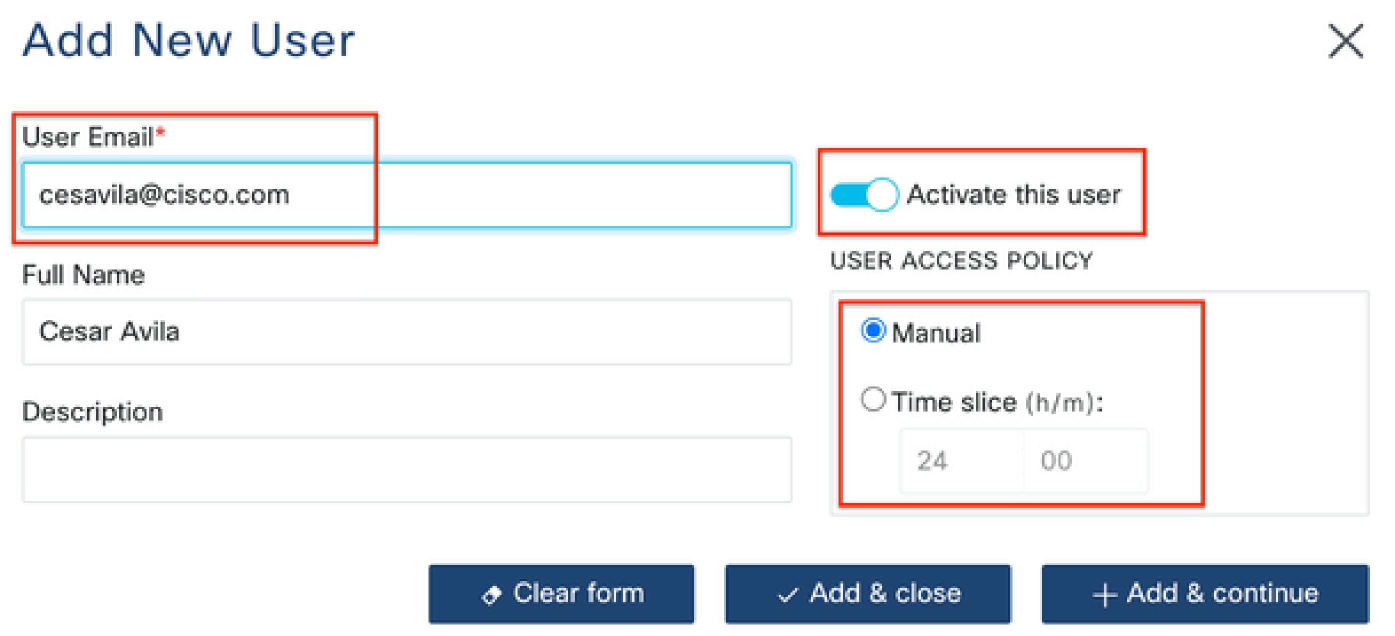
□	Active	Remaining Time	User Email	Full Name	Description	Actions
No Users Available						

Showing 0 to 0 of 0 entries. | Selected: 0. Page size 15 25 50 100 250

Step 2. Configure the user details:

- Email address
- Full Name (optional)

- Activate the user.
- Specify if the Activation must be Manually controlled or set a time frame to grant access to that user.



Add New User

User Email*: cesavila@cisco.com

☑ Activate this user

Full Name: Cesar Avila

Description:

USER ACCESS POLICY

● Manual

○ Time slice (h/m): 24 00

Step 3. Select **Add & Close**.

RADkit Client (TAC side)

Login

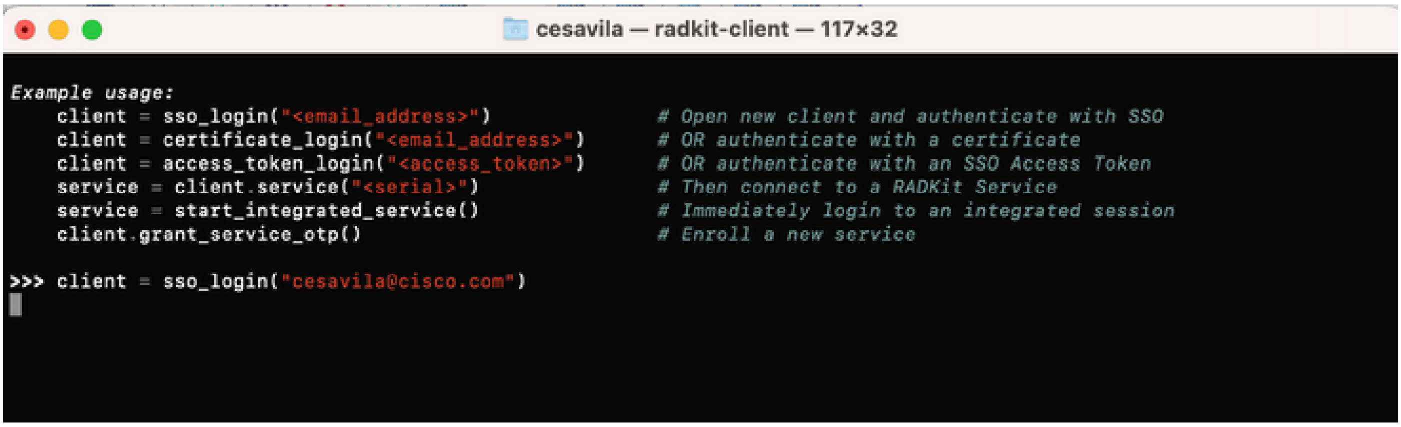
Step 1. On the Client PC, navigate to Applications and locate **RADkit Client**.

Step 2. Create a client instance with your SSO login.

<#root>

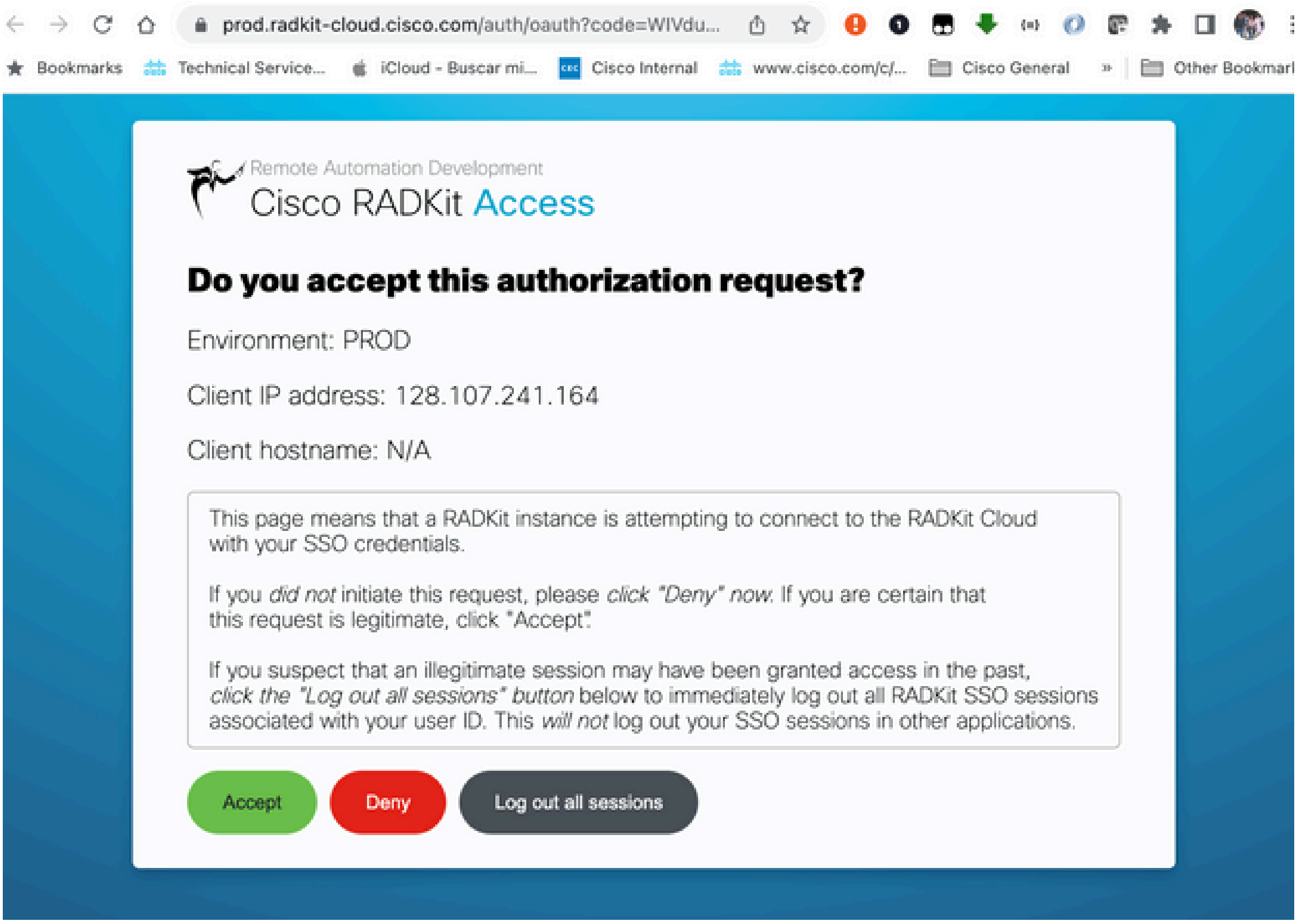
>>>

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



```
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")
```

Step 3. Accept the SSO Authorization Request opened automatically on your browser.



Do you accept this authorization request?

Environment: PROD

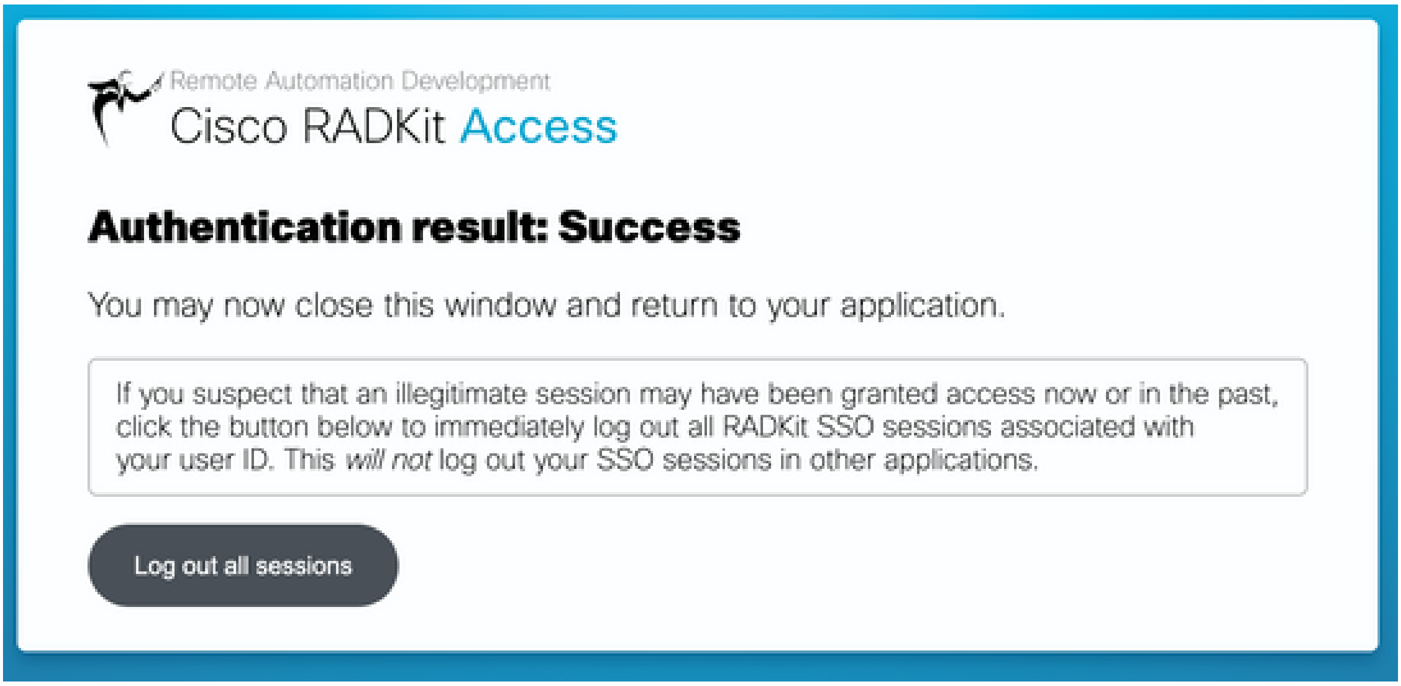
Client IP address: 128.107.241.164

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.

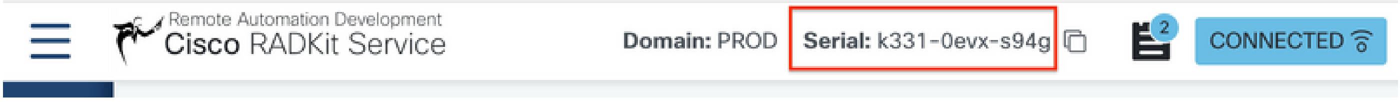


Authentication result: Success

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.

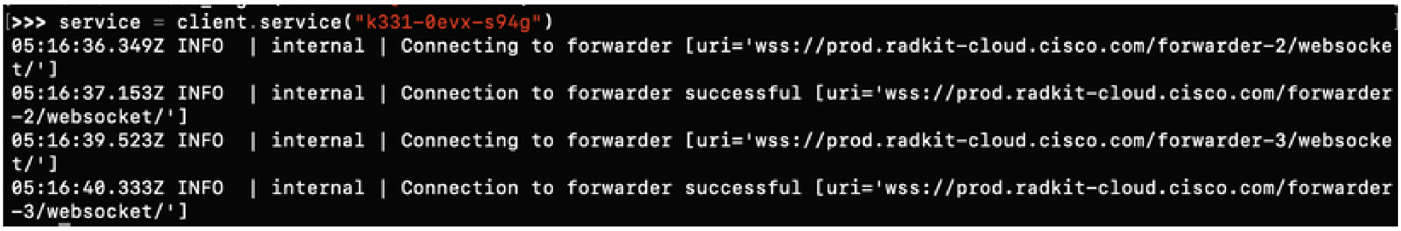
Step 4. Create a service instance using the user generated Serial Number from the RADKit Service - Onboarding stage.



Domain: PROD **Serial:** k331-0evx-s94g

<#root>

```
>>>

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



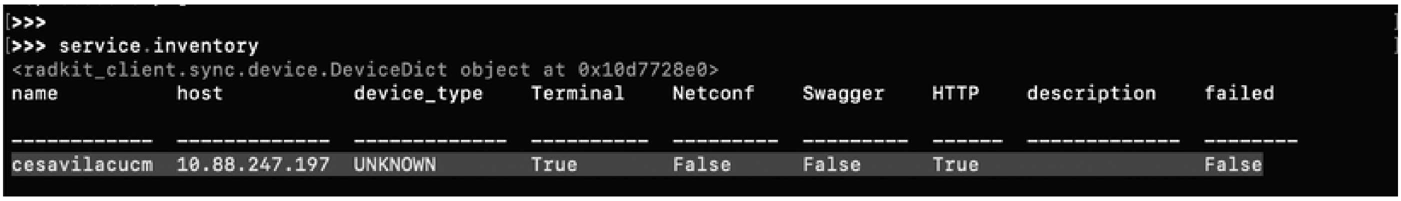
```
[>>> service = client.service("k331-0evx-s94g")
05:16:36.349Z INFO  | internal | Connecting to forwarder [uri='wss://prod.radkit-cloud.cisco.com/forwarder-2/websocke
t/']
05:16:37.153Z INFO  | internal | Connection to forwarder successful [uri='wss://prod.radkit-cloud.cisco.com/forwarder
-2/websocket/']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

Note: **service** is a variable that can be anything.

Step 5. Check the devices available for access.

<#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
```

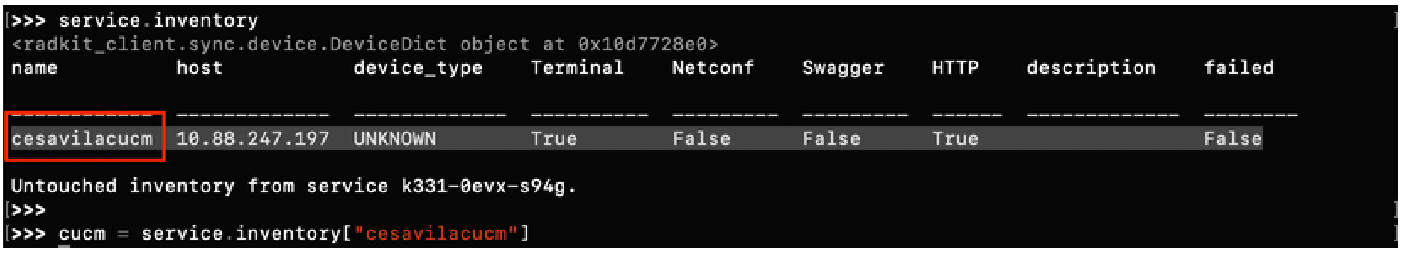
To refresh the inventory list, use the command update_inventory.

```
<#root>
>>> service.update_inventory().wait()
```

SSH Access

Step 1. Create an object from the inventory list.

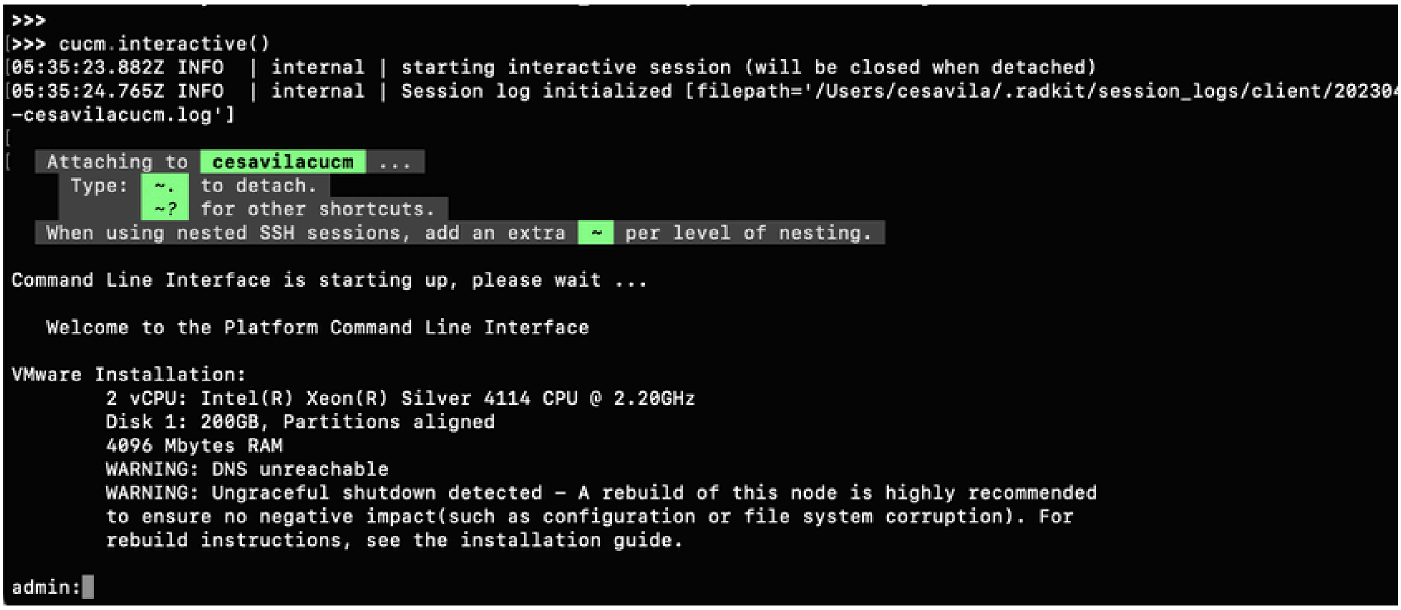
```
<#root>
>>> cucm = service.inventory['cesavilacucm']
```



```
[>>> 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"]
```

Step 2. Start the SSH session with the interactive command.

```
<#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:
```

Step 3. Now you are able to manage the device normally.

Caution:

- Always be mindful of our responsibility when operating in a user environment.
- RADKit must be used as a data collection tool.
- Never do any changes without the user permission.
- Document all your findings in the case notes.

GUI Access

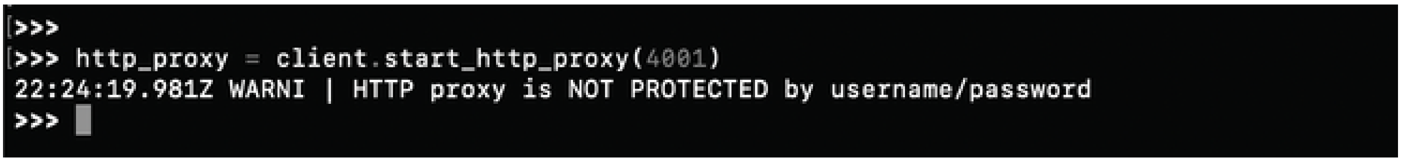
- **HTTP Proxy**

Step 1. Ensure the HTTP Credentials are added in the RADKit Service on the device configuration.

Step 2. Start the HTTP Proxy on the Radkit Client and define the Local port used to connect to the Proxy.

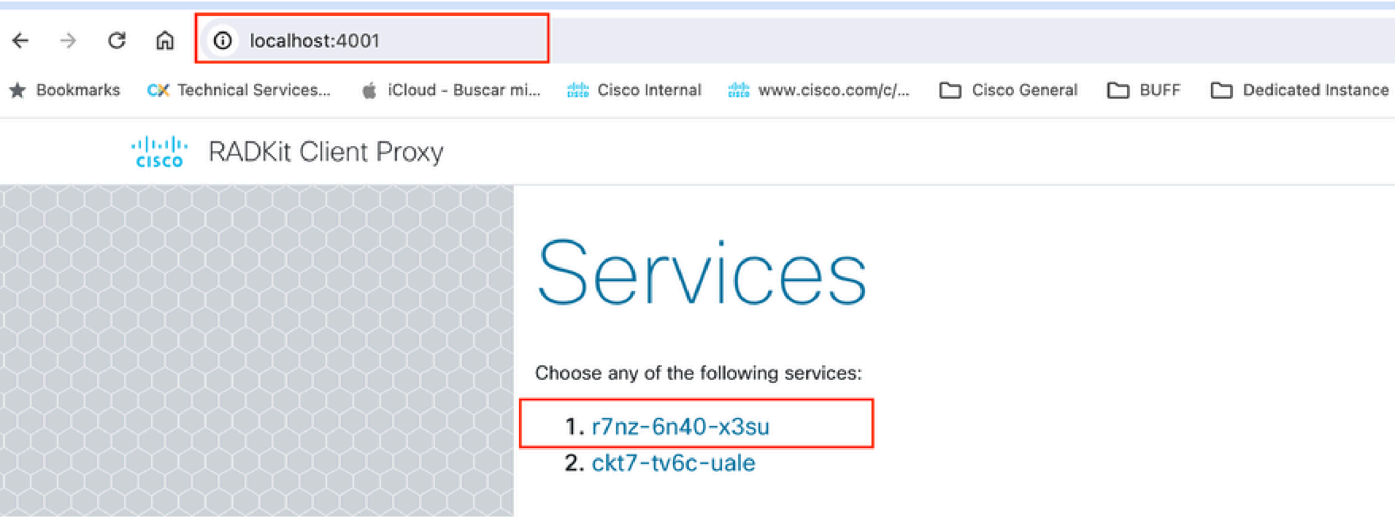
<#root>

```
>>> 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
>>> █
```

Step 3. From the Web Browser, navigate to https://localhost:4001 and select the Service you want to connect to.



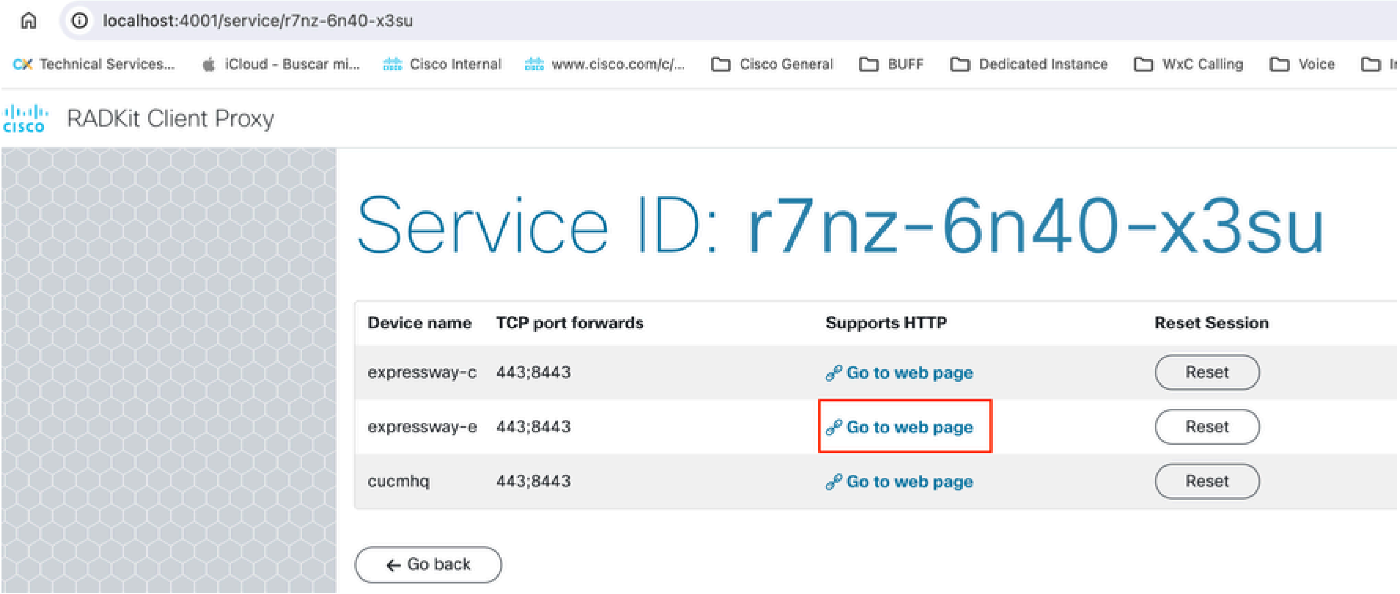
RADKit Client Proxy

Services

Choose any of the following services:

1. r7nz-6n40-x3su
2. ckt7-tv6c-uale

Step 4. Click the option **Go to Web Page** on the correct device to connect to its Web Page.



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

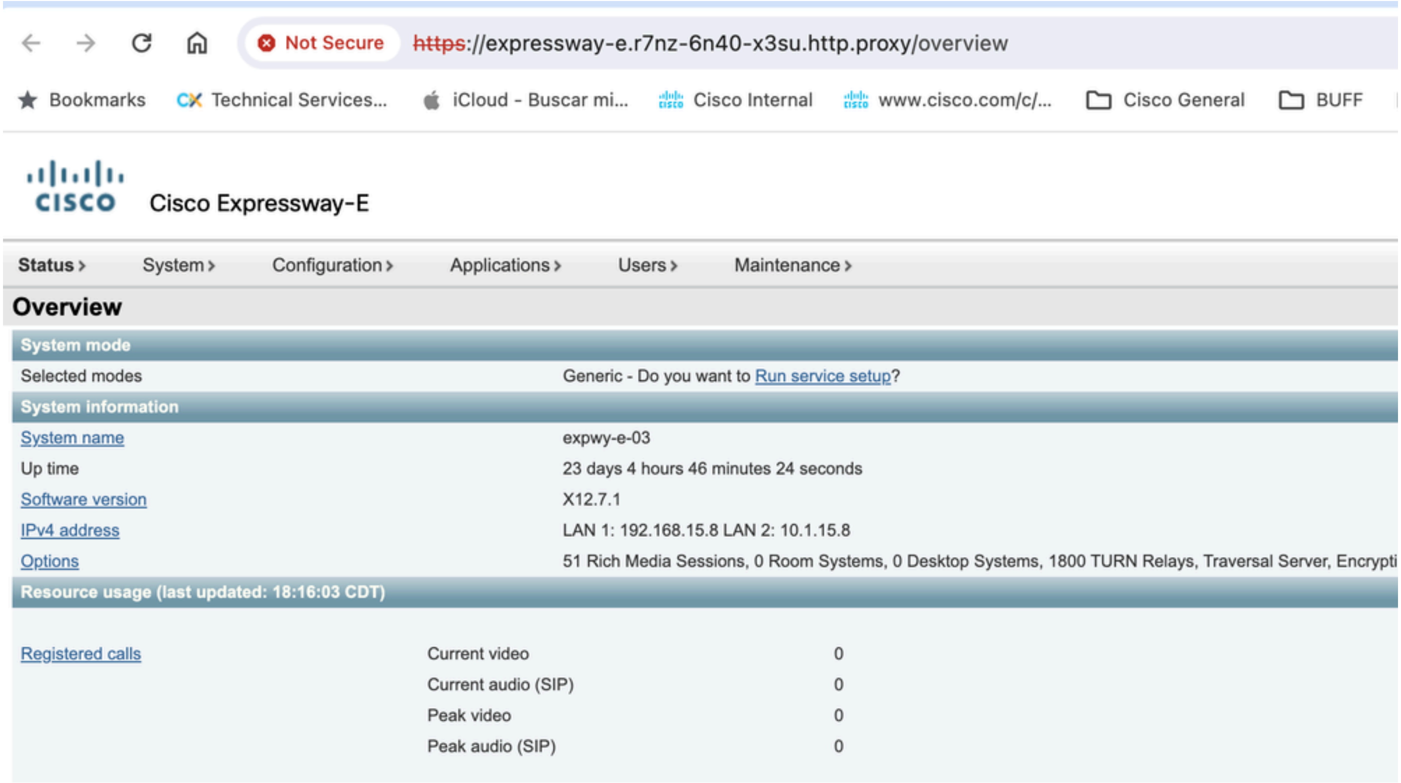
RADKit Client Proxy

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

Note: The first time HTTP Proxy is setup on a RADKit Client, it is recommended to click on the option Reset for each Devices before attempting to open the Device Web Page.

Step 5. The Web Page is displayed.



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, Encrypti

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

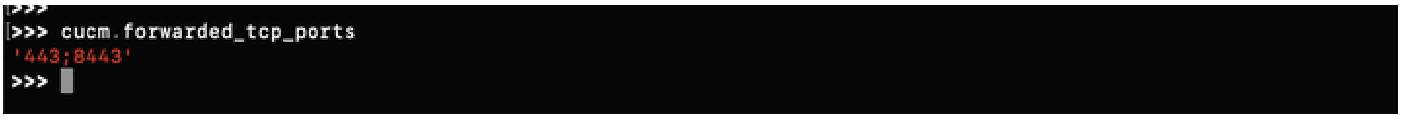
Registered calls	Current video	0
	Current audio (SIP)	0
	Peak video	0
	Peak audio (SIP)	0

- **Port Forwarding**

Step 1. Verify the TCP Forwarded ports configured for the device.

<#root>

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

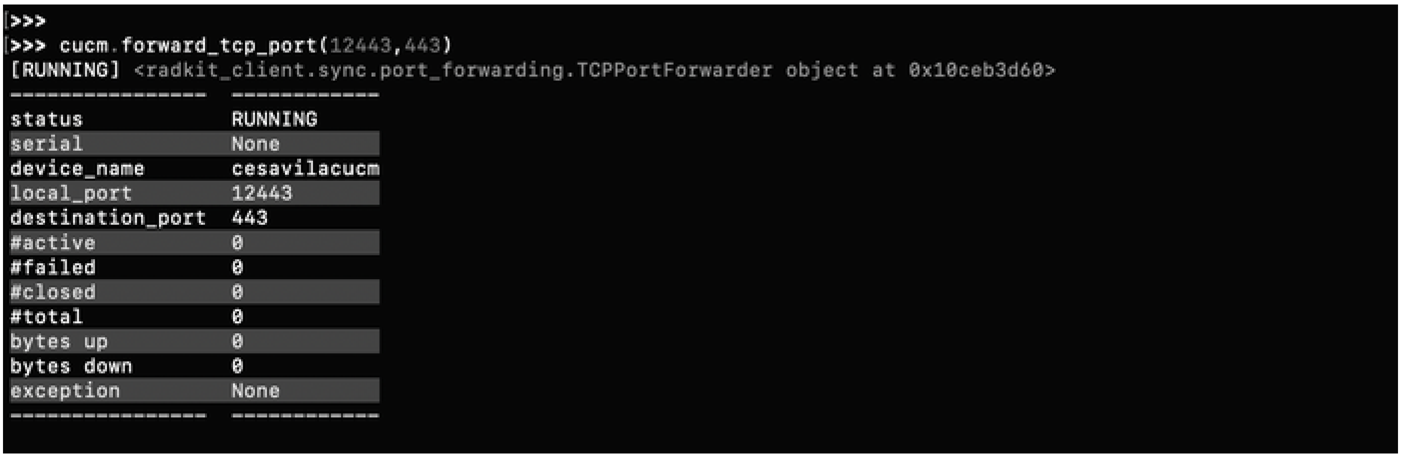


```
>>> cucm.forwarded_tcp_ports
'443;8443'
>>> 
```

Step 2. Configure a local port to be mapped with the destination port of the device, you must use the local port to access the device GUI.

<#root>

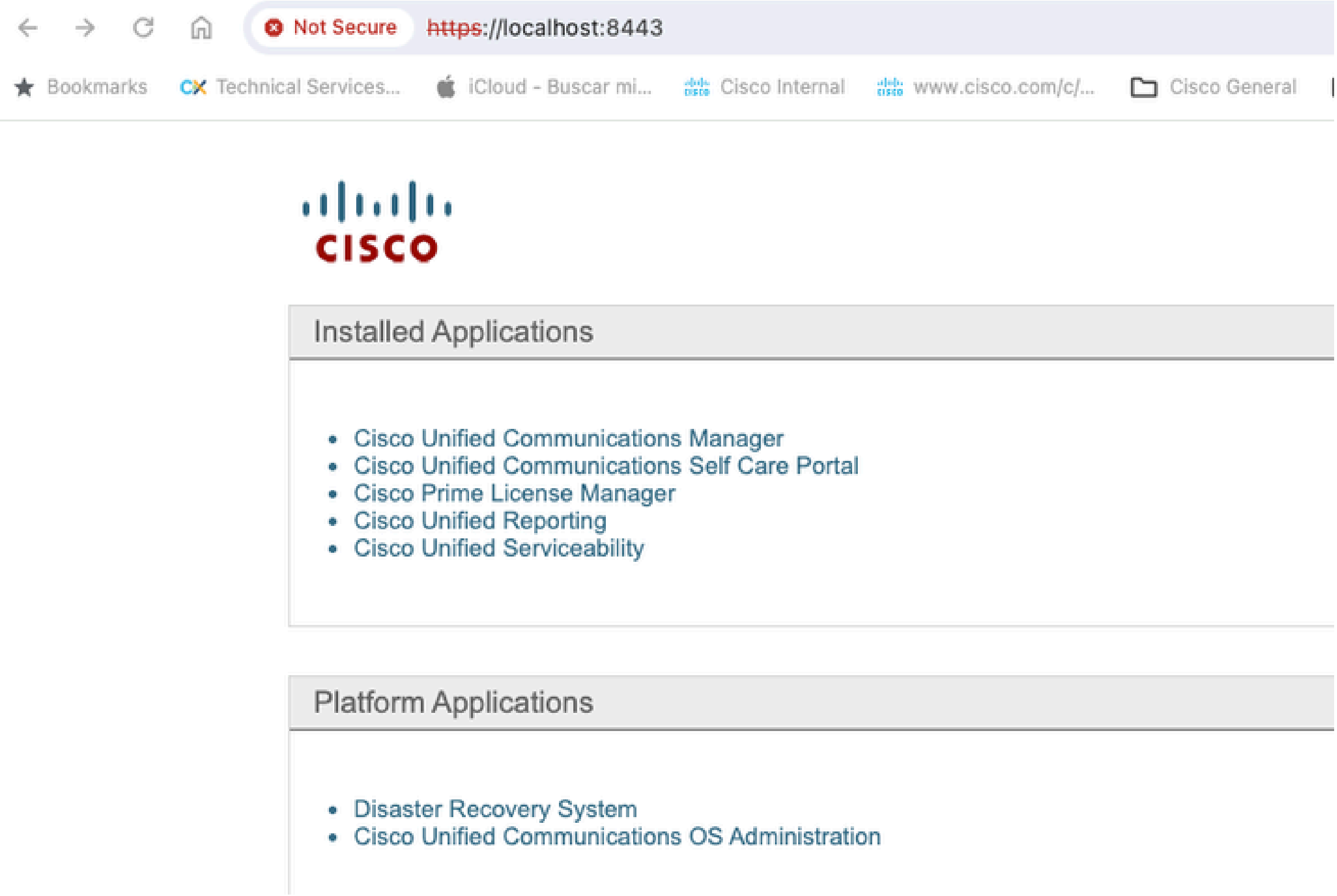
```
>>> cucm.forward_tcp_port(local_port=8443, destination_port=443)
```



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

Step 3. Open your browser and type the URL with the port configured in Step 2: **https://localhost:8443**.

The GUI of the device is now accessible.



Installed Applications

- Cisco Unified Communications Manager
- Cisco Unified Communications Self Care Portal
- Cisco Prime License Manager
- Cisco Unified Reporting
- Cisco Unified Serviceability

Platform Applications

- Disaster Recovery System
- Cisco Unified Communications OS Administration

Note: To access the GUI of the product you still need the credentials to be able to login, therefore it is recommended for user to create a Read-Only User Account for access.

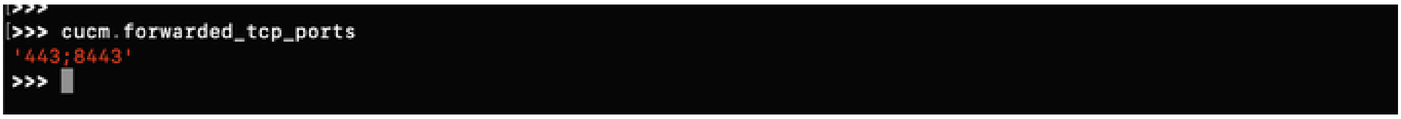
Log Collection

- **RTMT**

Step 1. Verify that port **8443** is listed in the TCP Forwarded ports configured for the device.

<#root>

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

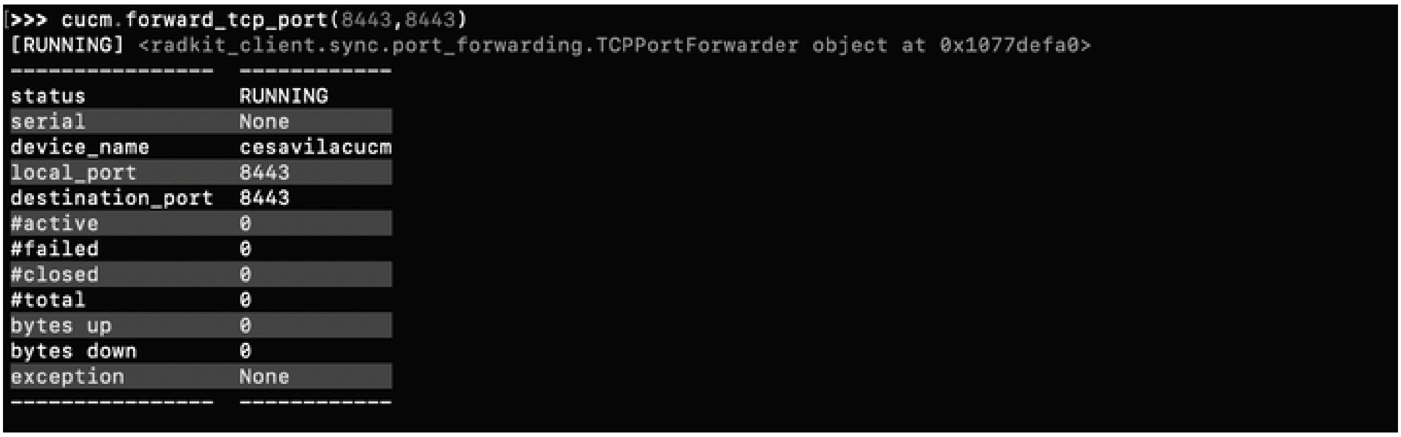


```
>>>
>>> cucm.forwarded_tcp_ports
'443;8443'
>>> 
```

Step 2. Configure the same port **8443** as local port to be mapped with port **8443** as the destination port of the device.

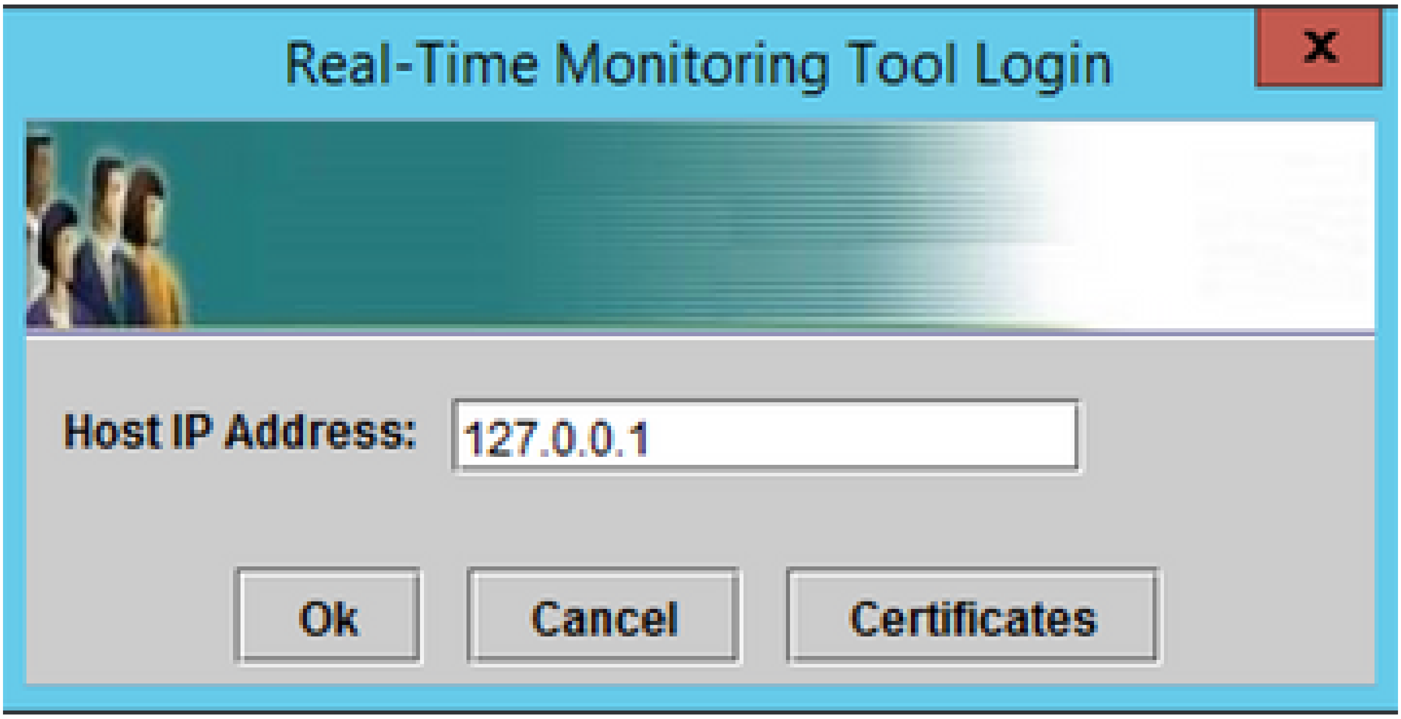
<#root>

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

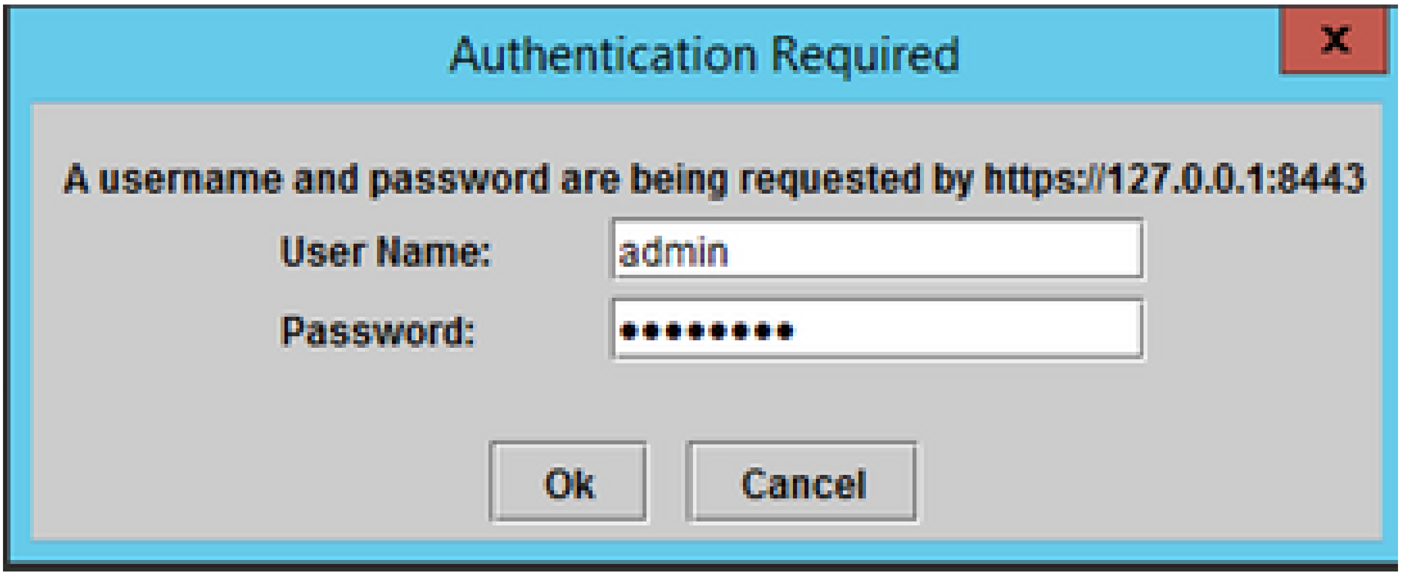
Step 3. Open RTMT and type **127.0.0.1** in the Host IP Address, it automatically uses port **8443**.



Real-Time Monitoring Tool Login

Host IP Address: 127.0.0.1

Step 4. Login with the correct credentials.



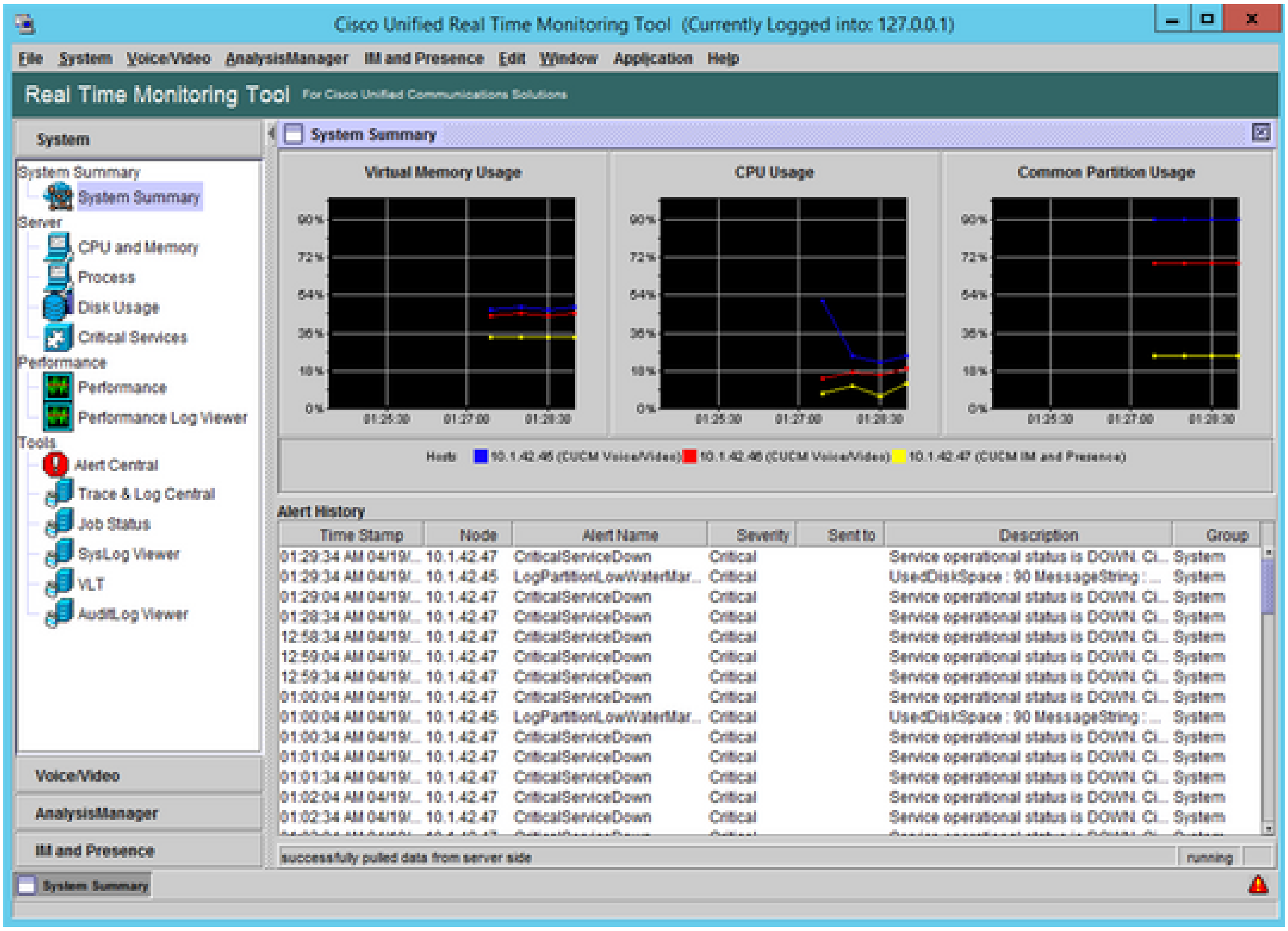
Authentication Required

A username and password are being requested by https://127.0.0.1:8443

User Name: admin

Password: ••••••••

Step 5. RTMT displays.



Cisco Unified Real Time Monitoring Tool (Currently Logged into: 127.0.0.1)

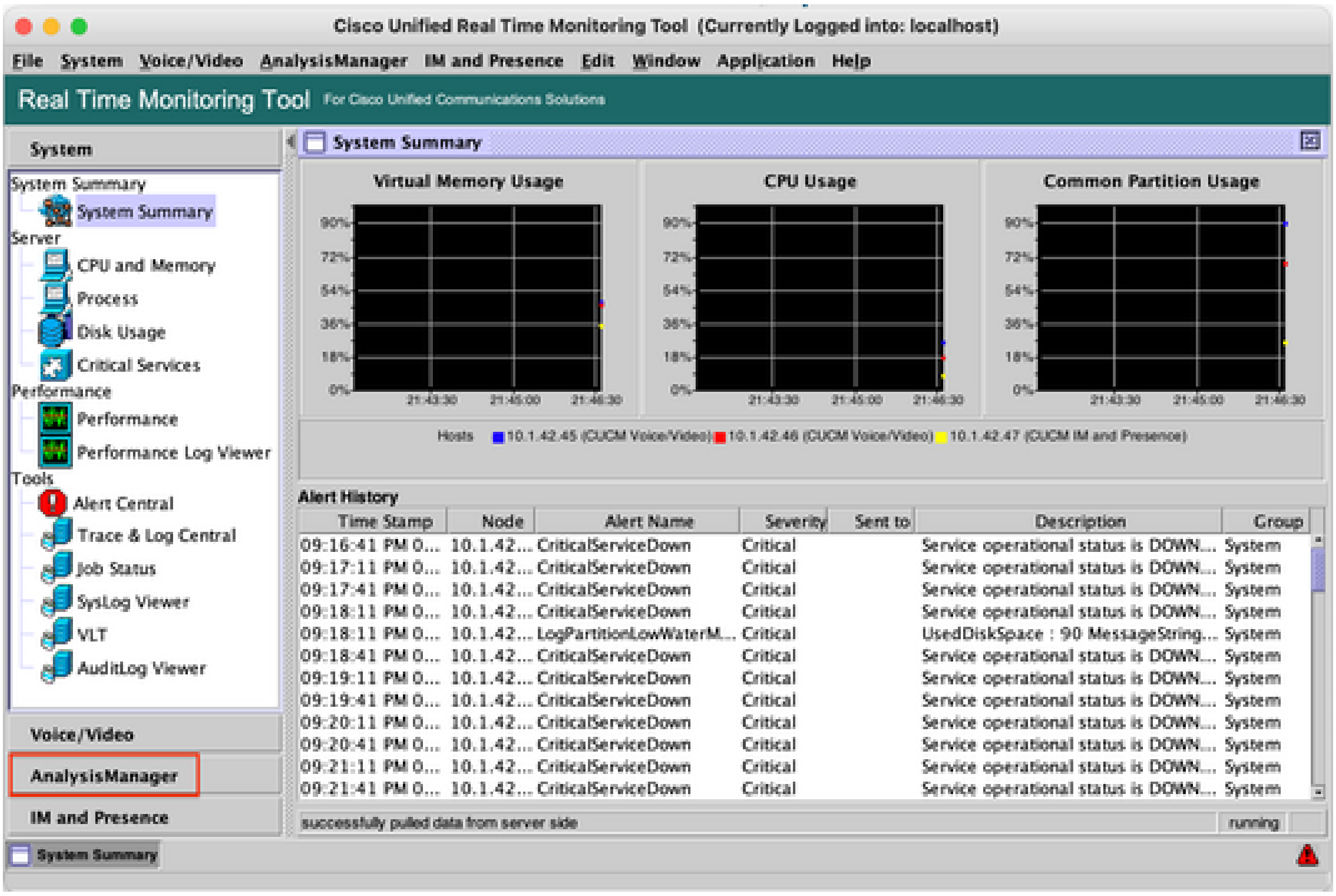
Alert History

Time Stamp	Node	Alert Name	Severity	Sent to	Description	Group
01:29:34 AM 04/19/...	10.1.42.47	CriticalServiceDown	Critical		Service operational status is DOWN. Ci...	System
01:29:34 AM 04/19/...	10.1.42.45	LogPartitionLowWaterMar...	Critical		UsedDiskSpace : 90 MessageString : ...	System
01:29:04 AM 04/19/...	10.1.42.47	CriticalServiceDown	Critical		Service operational status is DOWN. Ci...	System
01:28:34 AM 04/19/...	10.1.42.47	CriticalServiceDown	Critical		Service operational status is DOWN. Ci...	System
12:58:34 AM 04/19/...	10.1.42.47	CriticalServiceDown	Critical		Service operational status is DOWN. Ci...	System
12:59:04 AM 04/19/...	10.1.42.47	CriticalServiceDown	Critical		Service operational status is DOWN. Ci...	System
12:59:34 AM 04/19/...	10.1.42.47	CriticalServiceDown	Critical		Service operational status is DOWN. Ci...	System
01:00:04 AM 04/19/...	10.1.42.47	CriticalServiceDown	Critical		Service operational status is DOWN. Ci...	System
01:00:04 AM 04/19/...	10.1.42.45	LogPartitionLowWaterMar...	Critical		UsedDiskSpace : 90 MessageString : ...	System
01:00:34 AM 04/19/...	10.1.42.47	CriticalServiceDown	Critical		Service operational status is DOWN. Ci...	System
01:01:04 AM 04/19/...	10.1.42.47	CriticalServiceDown	Critical		Service operational status is DOWN. Ci...	System
01:01:34 AM 04/19/...	10.1.42.47	CriticalServiceDown	Critical		Service operational status is DOWN. Ci...	System
01:02:04 AM 04/19/...	10.1.42.47	CriticalServiceDown	Critical		Service operational status is DOWN. Ci...	System
01:02:34 AM 04/19/...	10.1.42.47	CriticalServiceDown	Critical		Service operational status is DOWN. Ci...	System

successfully pulled data from server side

running

Step 6. Go to **AnalysisManager** on the left panel.

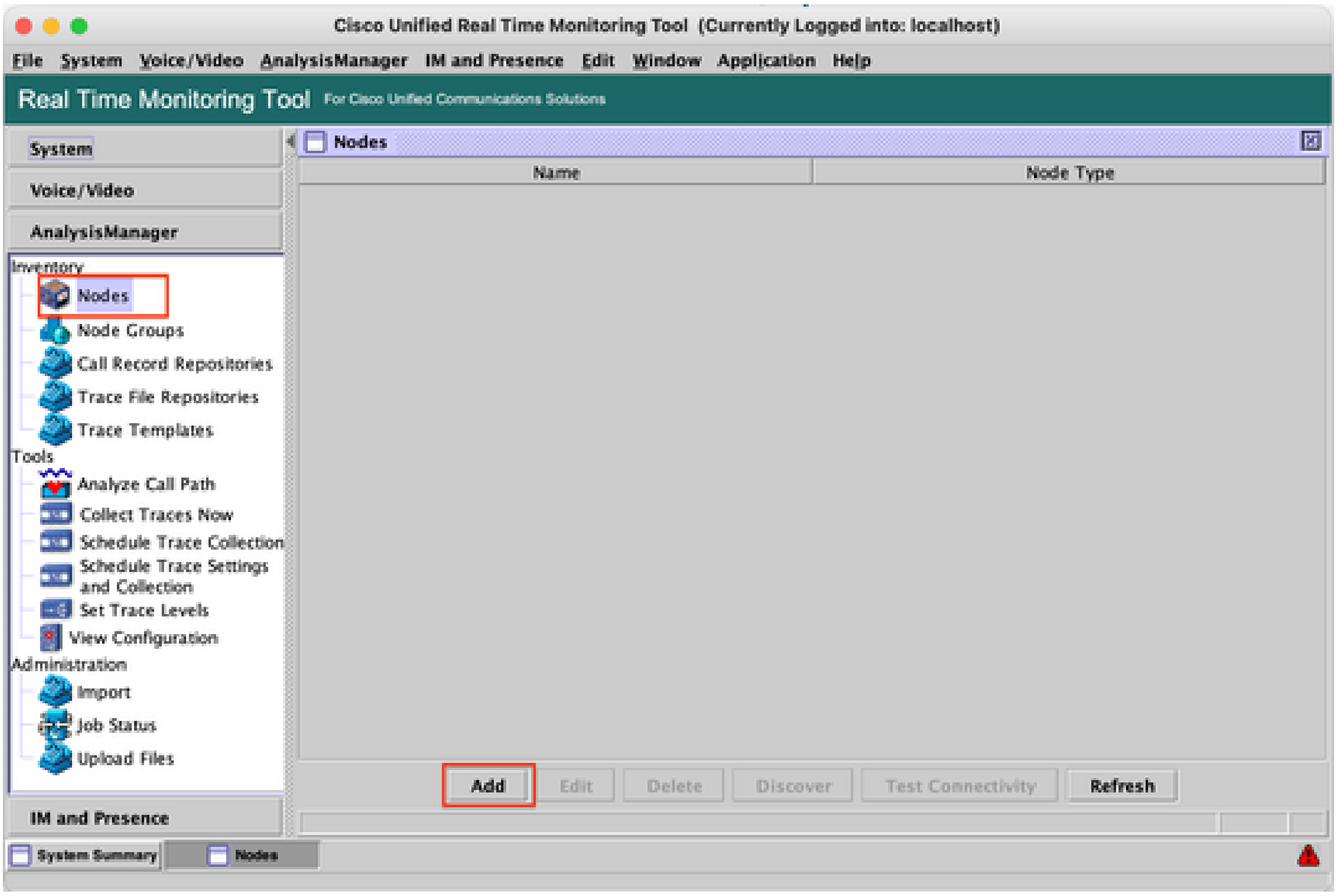


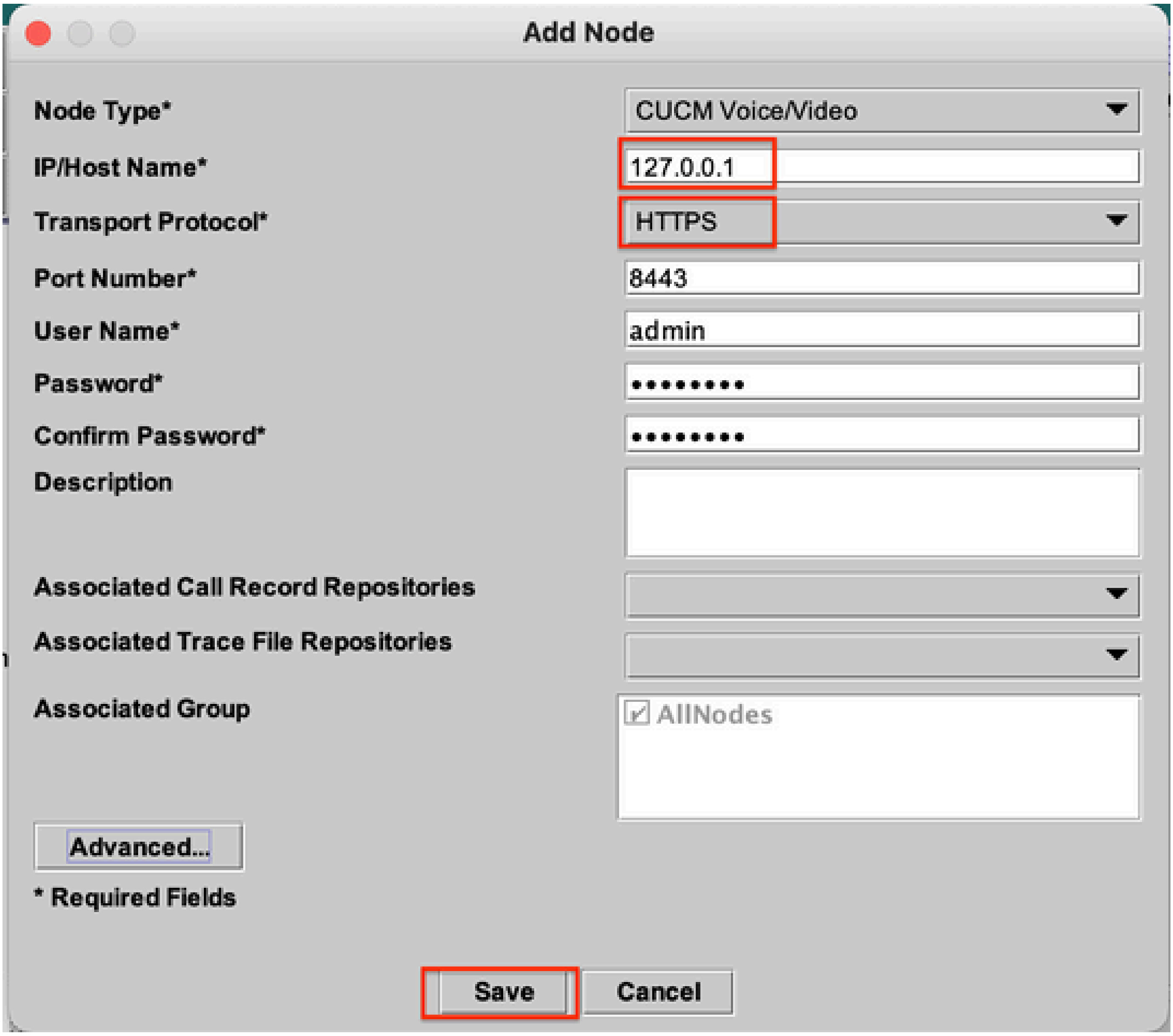
Alert History

Time Stamp	Node	Alert Name	Severity	Sent to	Description	Group
09:16:41 PM 0...	10.1.42...	CriticalServiceDown	Critical		Service operational status is DOWN...	System
09:17:11 PM 0...	10.1.42...	CriticalServiceDown	Critical		Service operational status is DOWN...	System
09:17:41 PM 0...	10.1.42...	CriticalServiceDown	Critical		Service operational status is DOWN...	System
09:18:11 PM 0...	10.1.42...	CriticalServiceDown	Critical		Service operational status is DOWN...	System
09:18:11 PM 0...	10.1.42...	LogPartitionLowWaterM...	Critical		UsedDiskSpace : 90 MessageString...	System
09:18:41 PM 0...	10.1.42...	CriticalServiceDown	Critical		Service operational status is DOWN...	System
09:19:11 PM 0...	10.1.42...	CriticalServiceDown	Critical		Service operational status is DOWN...	System
09:19:41 PM 0...	10.1.42...	CriticalServiceDown	Critical		Service operational status is DOWN...	System
09:20:11 PM 0...	10.1.42...	CriticalServiceDown	Critical		Service operational status is DOWN...	System
09:20:41 PM 0...	10.1.42...	CriticalServiceDown	Critical		Service operational status is DOWN...	System
09:21:11 PM 0...	10.1.42...	CriticalServiceDown	Critical		Service operational status is DOWN...	System
09:21:41 PM 0...	10.1.42...	CriticalServiceDown	Critical		Service operational status is DOWN...	System

successfully pulled data from server side

Step 7. Click **Nodes** and **Add** to configure the details of the device to be added using localhost and the forwarded TCP Port.


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



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*: •••••••••

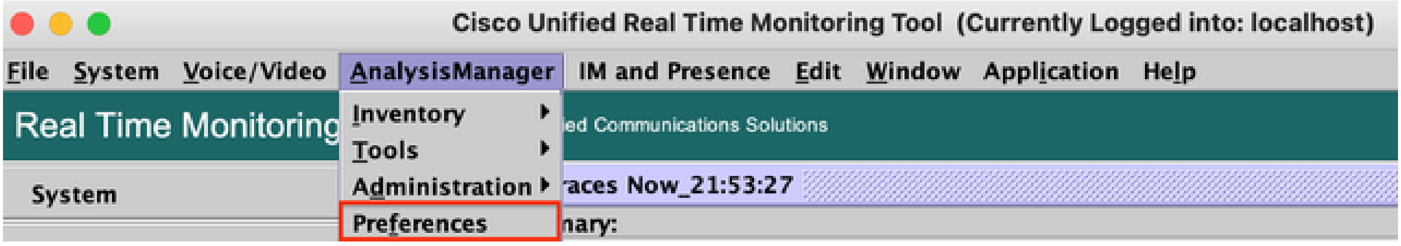
Description:

Associated Call Record Repositories:

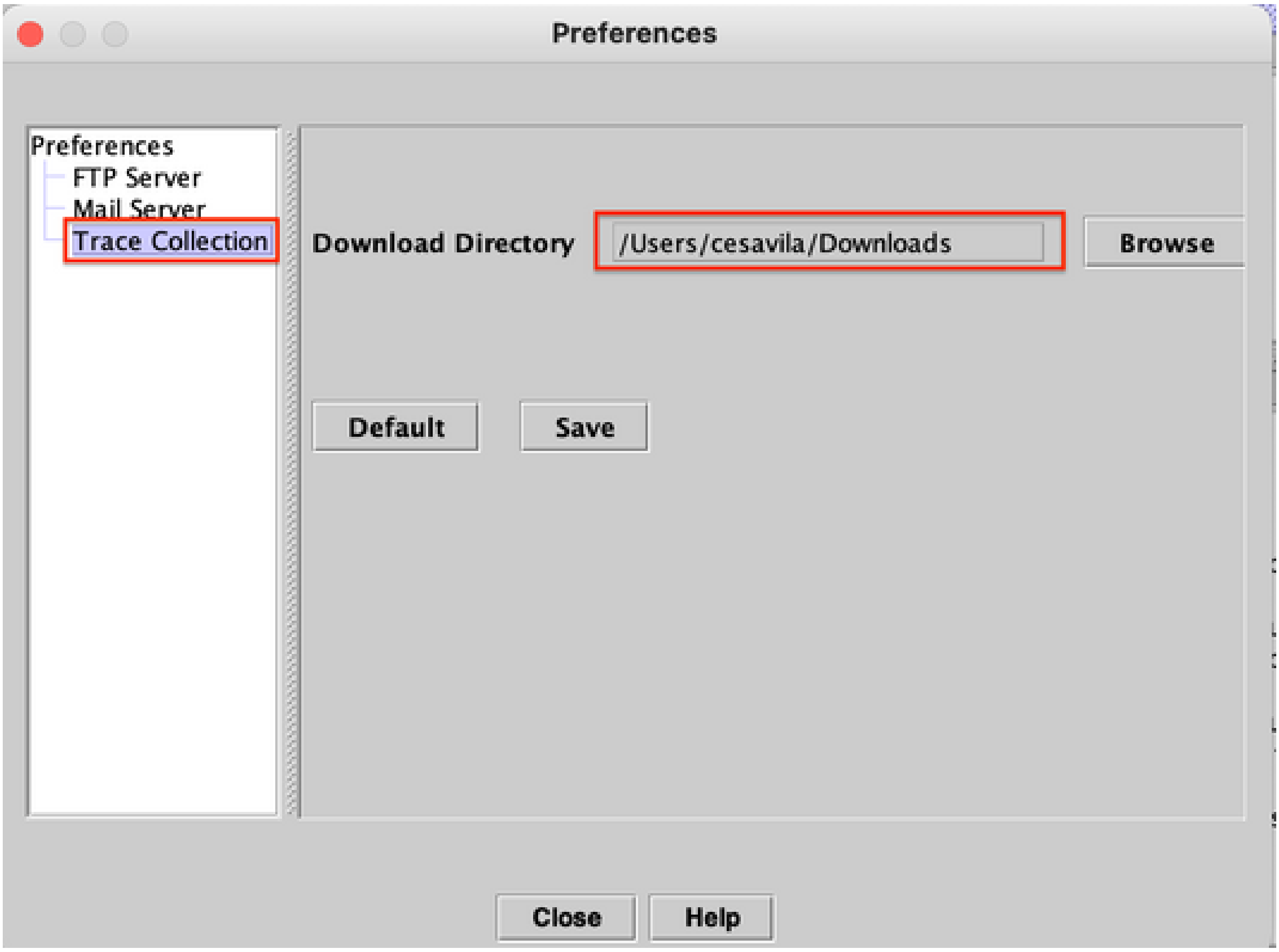
Associated Trace File Repositories:

Associated Group: ☑ AllNodes

Step 8. Click **Analysis Manager** on the menu at the top and select **Preferences**.

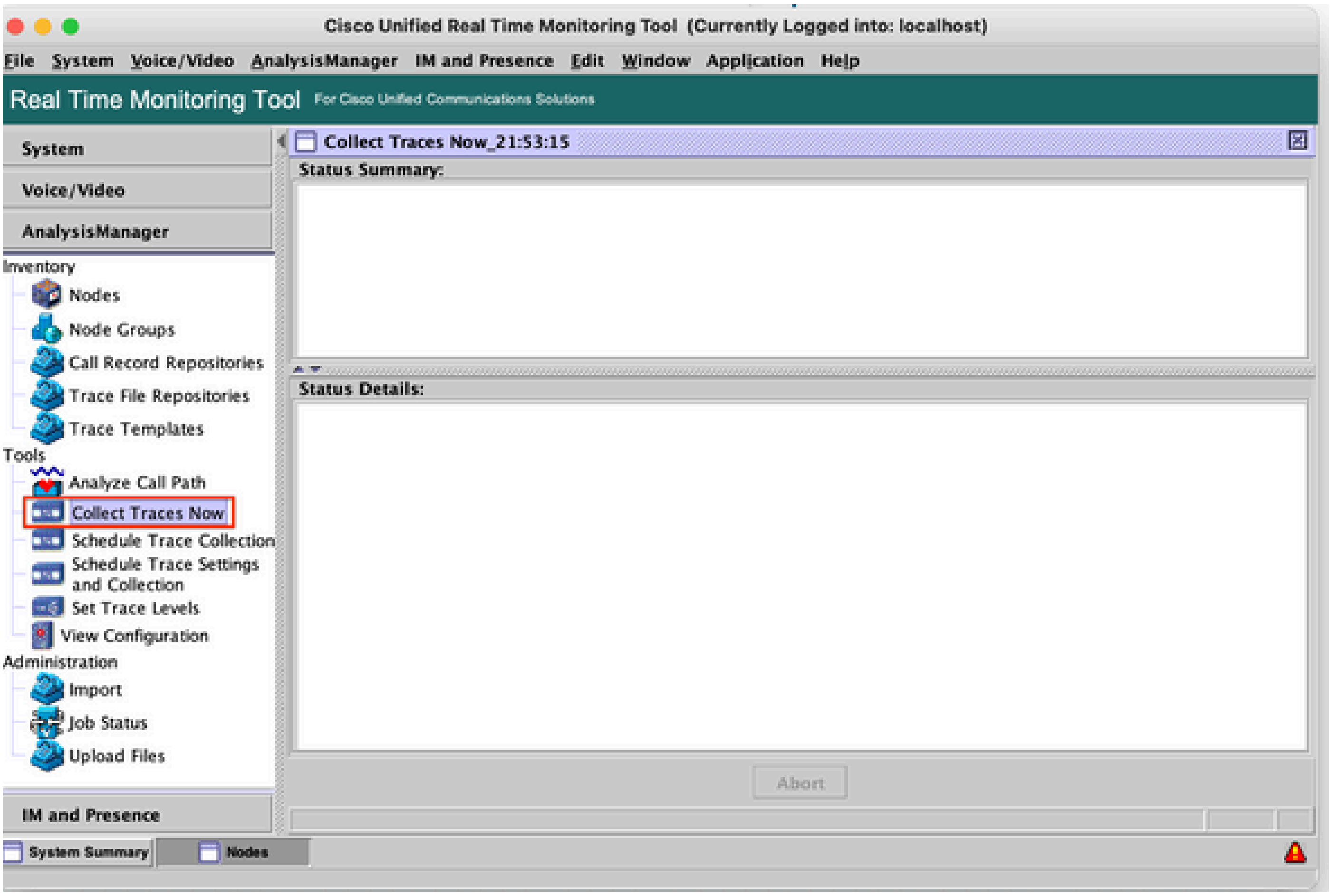


Step 9. Go to **Trace Collection** and select the Correct folder to download the logs, Click **Save** and then **Close**.

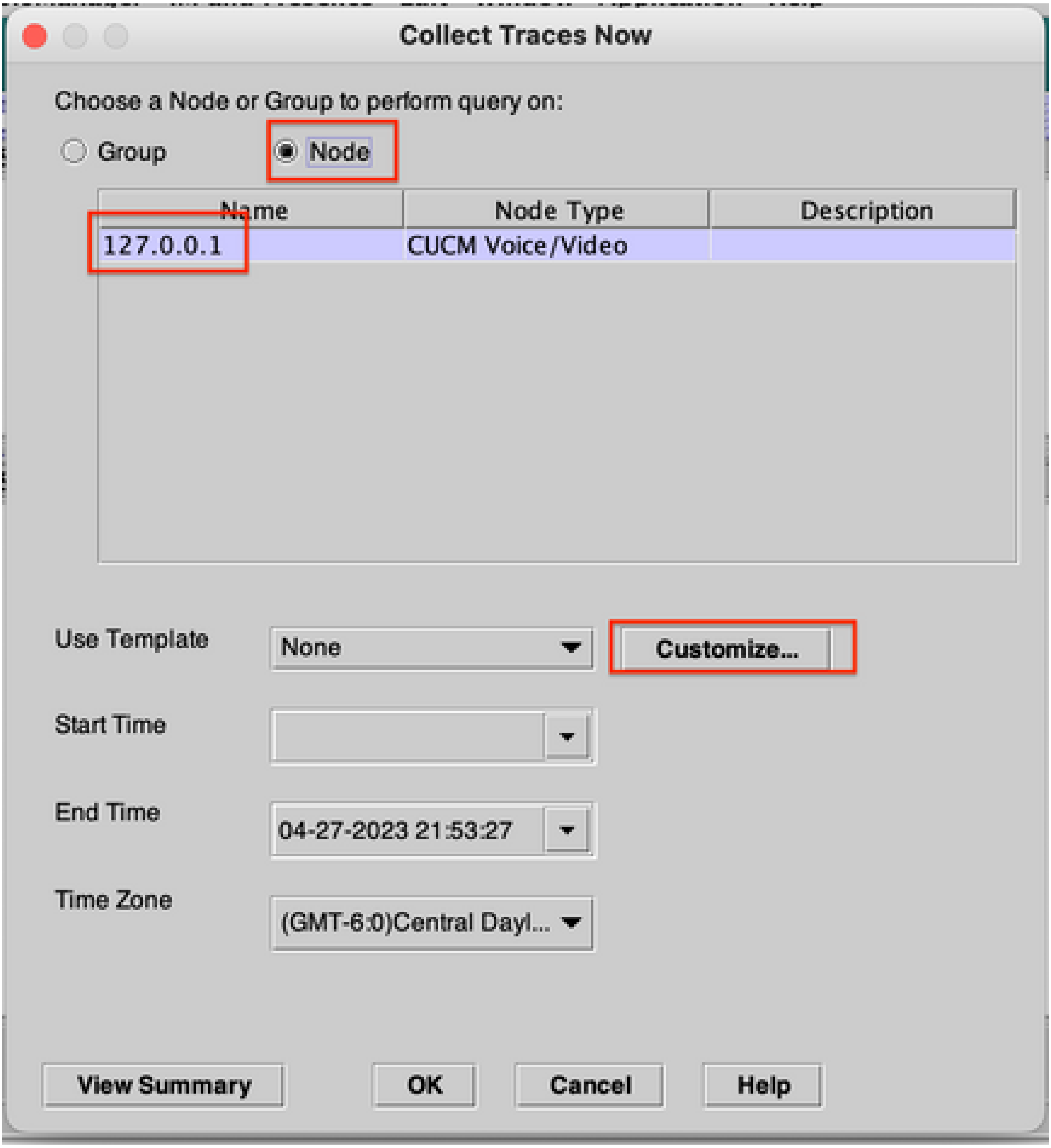


Download Directory /Users/cesavila/Downloads

Step 10. Go to **Collect Traces now**.


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
System Summary
Nodes
Collect Traces Now_21:53:15
Status Summary:
Status Details:
Abort

Step 11. Select the option **Node**, select the device that was added on Step 7 and click **Customize**.



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	

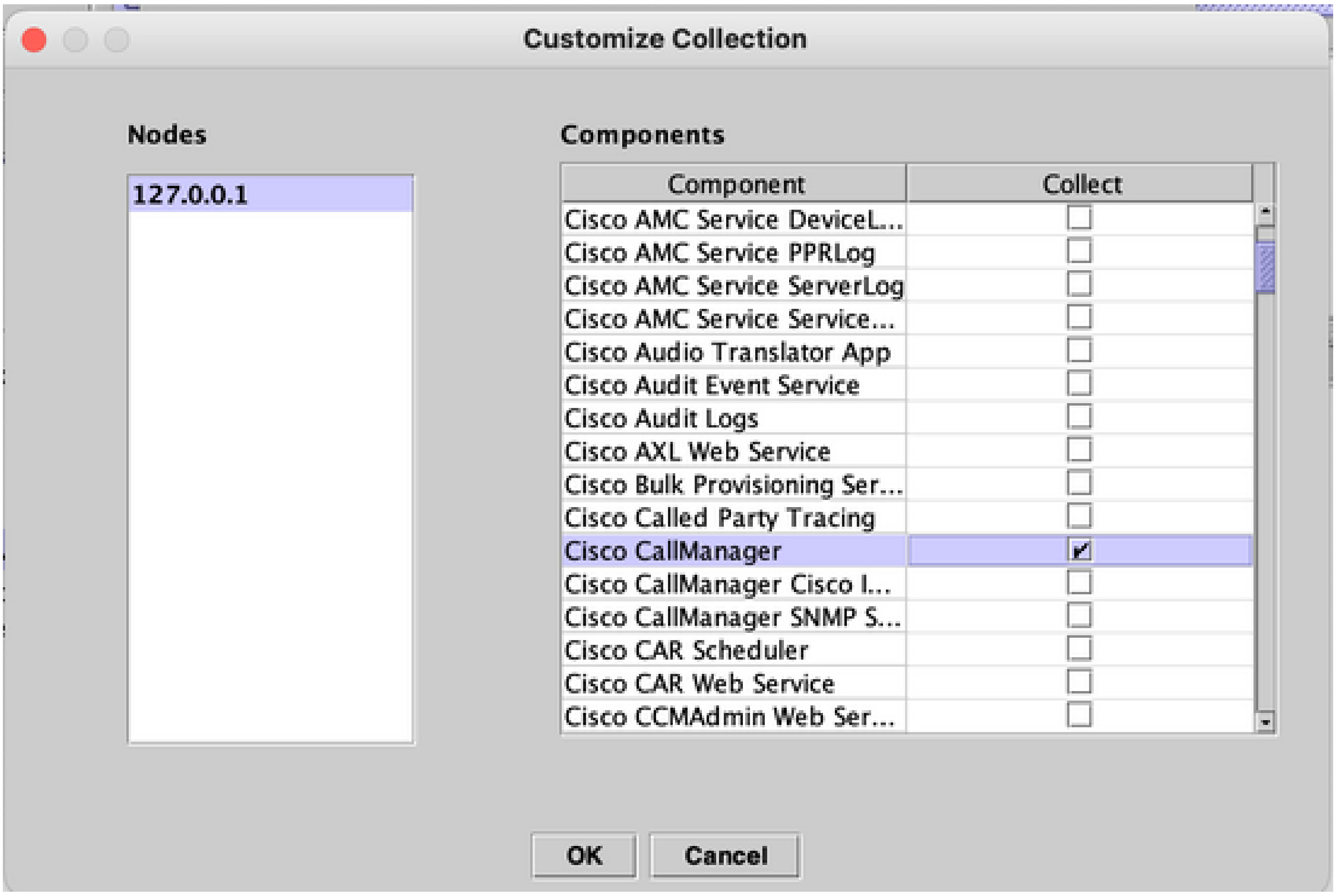
Use Template: None

Start Time:

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

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

Step 12. Select the logs to be collected from the device and click **OK**.



Customize Collection

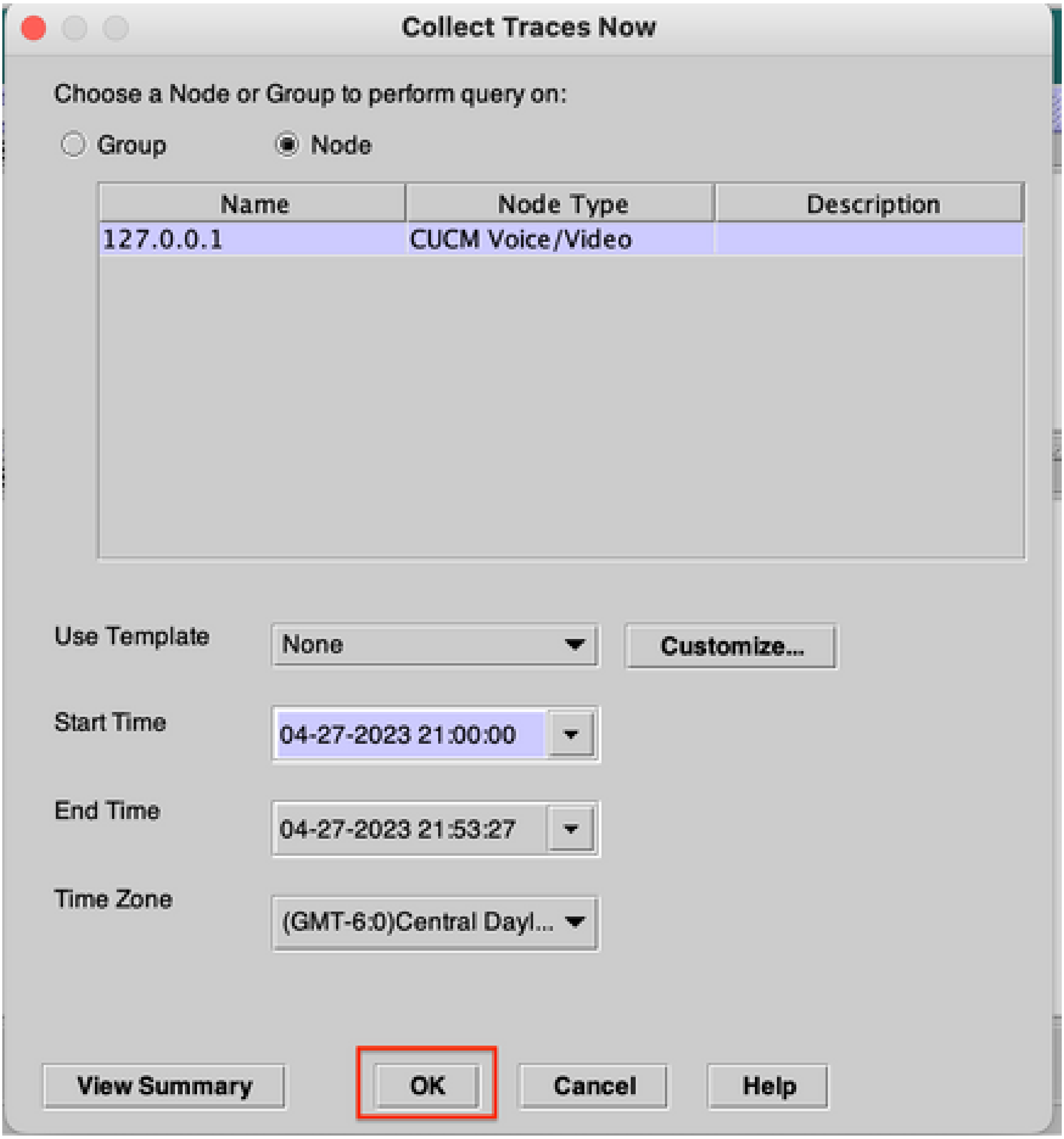
Nodes

127.0.0.1

Components

Component	Collect
Cisco AMC Service DeviceL...	□
Cisco AMC Service PPRLog	□
Cisco AMC Service ServerLog	□
Cisco AMC Service Service...	□
Cisco Audio Translator App	□
Cisco Audit Event Service	□
Cisco Audit Logs	□
Cisco AXL Web Service	□
Cisco Bulk Provisioning Ser...	□
Cisco Called Party Tracing	□
Cisco CallManager	☑
Cisco CallManager Cisco I...	□
Cisco CallManager SNMP S...	□
Cisco CAR Scheduler	□
Cisco CAR Web Service	□
Cisco CCMAdmin Web Ser...	□

Step 13. Finally select **Start Time** and **End Time** of the logs to be collected and click **OK**.



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	

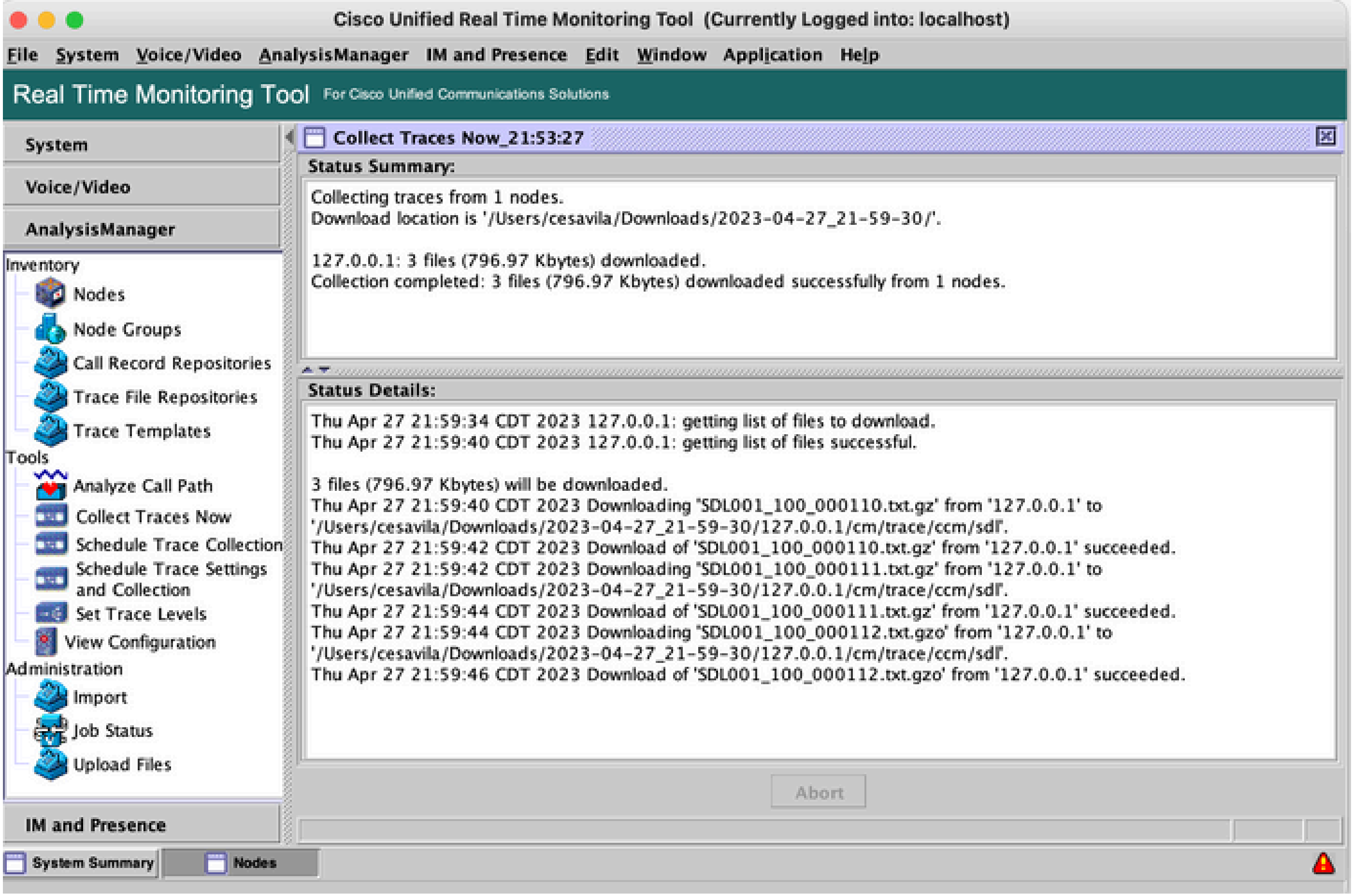
Use Template: None

Start Time: 04-27-2023 21:00:00

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

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

Step 14. Files are downloaded to the local PC (RADKit Client PC) successfully.


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
Collect Traces Now_21:53:27
Abort
System Summary
Nodes

Status Summary:

```
Collecting traces from 1 nodes.
Download location is '/Users/cesavila/Downloads/2023-04-27_21-59-30/'.

127.0.0.1: 3 files (796.97 Kbytes) downloaded.
Collection completed: 3 files (796.97 Kbytes) downloaded successfully from 1 nodes.
```

Status Details:

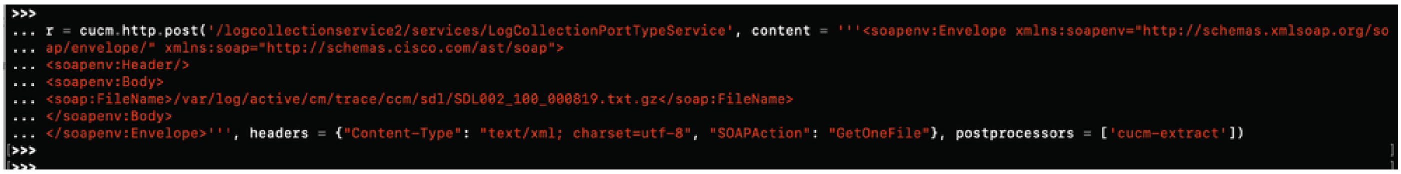
```
Thu Apr 27 21:59:34 CDT 2023 127.0.0.1: getting list of files to download.
Thu Apr 27 21:59:40 CDT 2023 127.0.0.1: getting list of files successful.

3 files (796.97 Kbytes) will be downloaded.
Thu Apr 27 21:59:40 CDT 2023 Downloading 'SDL001_100_000110.txt.gz' from '127.0.0.1' to
'/Users/cesavila/Downloads/2023-04-27_21-59-30/127.0.0.1/cm/trace/ccm/sdl'.
Thu Apr 27 21:59:42 CDT 2023 Download of 'SDL001_100_000110.txt.gz' from '127.0.0.1' succeeded.
Thu Apr 27 21:59:42 CDT 2023 Downloading 'SDL001_100_000111.txt.gz' from '127.0.0.1' to
'/Users/cesavila/Downloads/2023-04-27_21-59-30/127.0.0.1/cm/trace/ccm/sdl'.
Thu Apr 27 21:59:44 CDT 2023 Download of 'SDL001_100_000111.txt.gz' from '127.0.0.1' succeeded.
Thu Apr 27 21:59:44 CDT 2023 Downloading 'SDL001_100_000112.txt.gzo' from '127.0.0.1' to
'/Users/cesavila/Downloads/2023-04-27_21-59-30/127.0.0.1/cm/trace/ccm/sdl'.
Thu Apr 27 21:59:46 CDT 2023 Download of 'SDL001_100_000112.txt.gzo' from '127.0.0.1' succeeded.
```

- **SOAP API**

SOAP API is currently supported for CUCM. Additionally, Swagger is supported for CMS, Expressway, CVP, and so on.

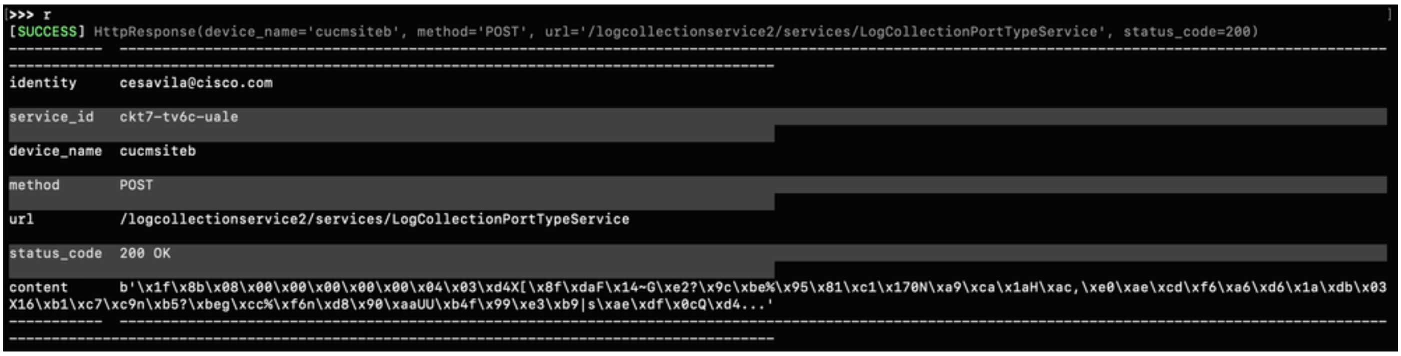
Step 1. Ensure the HTTP Credentials are added in the RADKit Service on the device configuration.

Step 2. Run the HTTP Post command on the RADKit Client, specify the resource path, request body with the necessary parameters and headers.



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

Note: The postprocessors option **'cucm-extract'** is used to remove the HTTP Response headers to be able to save the log to a file.



```
>>> 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\x00\x04\x03\xd4X[\x8f\xdaF\x14~G\xe2?\x9c\xbe%\x95\x81\xc1\x170N\xa9\xca\x1aH\xac,\xe0\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...'
-----------  ------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------
```

Step 3. Save the content to a file to get the Trace File saved in the local PC.

<#root>

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

RADKit Use Cases

As it has been highlighted, RADKit provides a secure connection to the network devices including Collaboration servers without the need of being on a webex. The idea is to simplify some of the challenges around data collection by providing on demand access to the required devices.

Talking specifically about Collaboration deployments, RADKit currently can be very useful for a variety of issues such as:

- DB Replication issues.
- Certificate regeneration procedures.
- System Health check.
- Configuration validation in GUI / CLI.
- Log Collection through Web Interface (E.g. CER, Expressway, CIMC, etc).
- Debug logs via CLI on Voice Gateways.

Related Information

- RADKit Main page https://radkit.cisco.com/
- External RADKit support page https://community.cisco.com/t5/radkit-discussions/bd-p/disc-radkit