

Impostazione di RADKit in un ambiente di collaborazione

Sommario

[Introduzione](#)

[Requisiti](#)

[Componenti usati](#)

[Terminologia](#)

[Architettura RADKit](#)

[Installazione di RADKit](#)

[Servizio RADKit \(lato utente\)](#)

[Carico](#)

[Aggiungi dispositivi](#)

[Autorizza utenti remoti](#)

[Client RADkit \(lato TAC\)](#)

[Accesso](#)

[Accesso SSH](#)

[Accesso GUI](#)

[Proxy HTTP](#)

[Port Forwarding](#)

[Raccolta log](#)

[RTMT](#)

[API SOAP](#)

[Casi di utilizzo di RADKit](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive i passaggi per impostare RADKit e mostra la configurazione necessaria per iniziare a utilizzarlo con i prodotti di collaborazione.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di qualsiasi prodotto VOS Collaboration
- Conoscenze base di CLI/SSH Access

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

- Cisco Unified Communications Manager 12.5 e 14.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

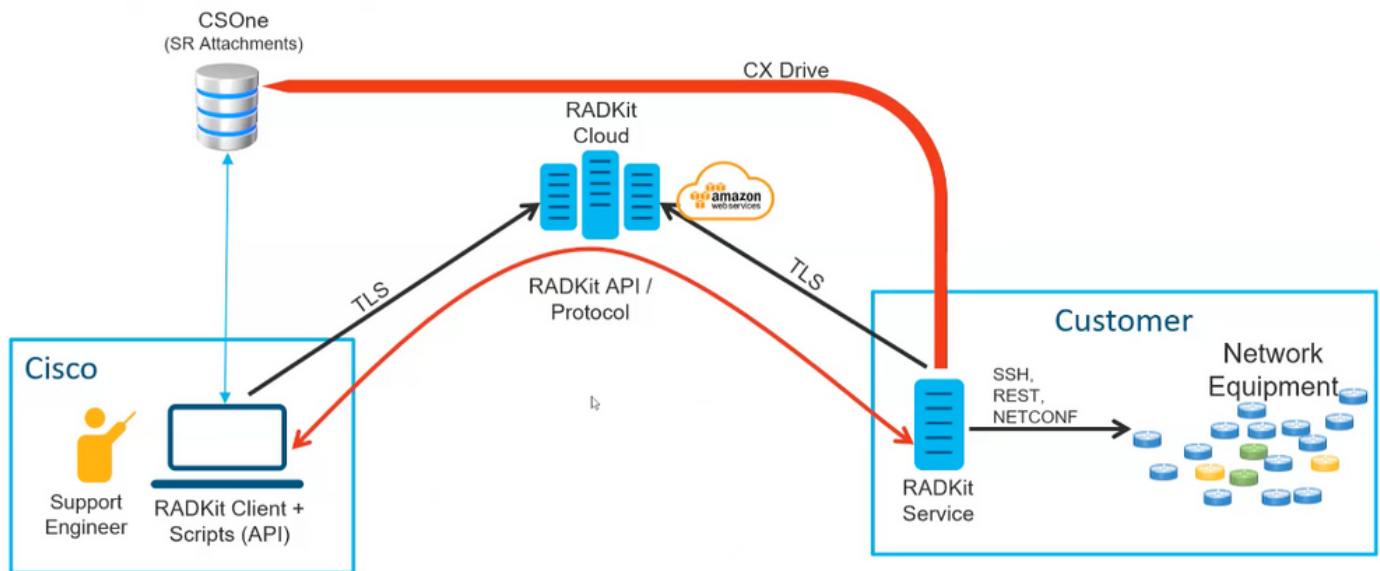
Terminologia

Radkit: Si tratta di un connettore che consente di accedere in modo sicuro ai dispositivi utente da remoto ai tecnici e ai partner Cisco TAC. Supporta più protocolli per interagire con i dispositivi, ad esempio SSH o HTTP/HTTP.

Servizio RADKit: Questo è il lato server. Viene gestito e interamente gestito dall'Utente. Dal lato server, l'utente controlla chi può accedere ai dispositivi e per quanto tempo. Radkit Service deve disporre di connettività ai dispositivi nella rete per consentire l'accesso.

Client RADKit: Questo è il lato client. Si tratta del PC utilizzato per connettersi alle periferiche nella rete dell'utente.

Architettura RADKit



Architettura RADKit

Installazione di RADKit

Passaggio 1. Passare a <https://radkit.cisco.com>, fare clic su Download, quindi andare alla cartella della versione.

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

-

Passaggio 2. Fare clic sull'ultima 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

-

Passaggio 3. Scaricare il file corretto a seconda del sistema operativo in uso.

INDEX OF /DOWNLOADS/RELEASE/1.4.9/

[../](#)

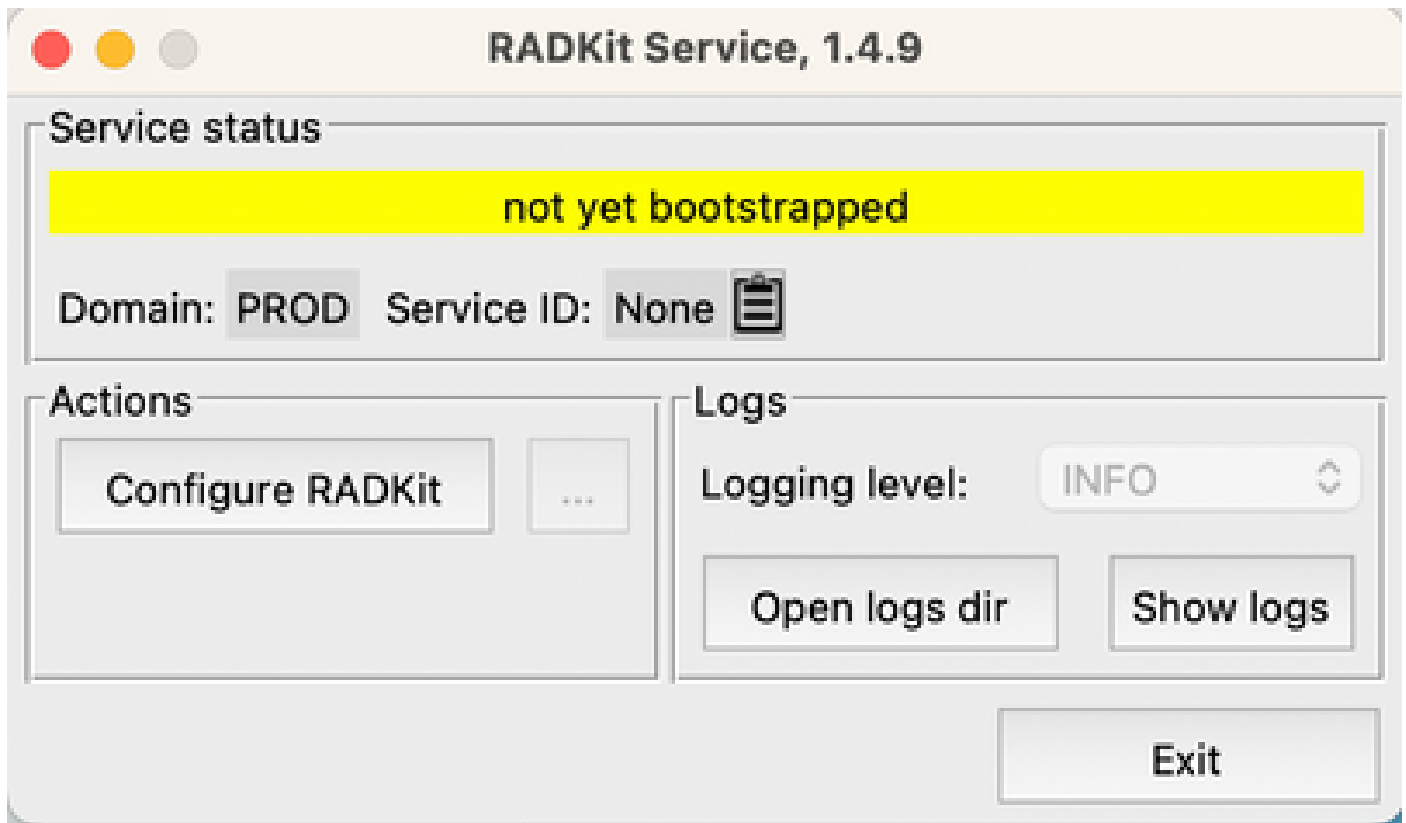
docs/	04-Apr-2023 11:45	-
cisco_radkit_1.4.9_doc_html.tgz	04-Apr-2023 11:43	8003863
cisco_radkit_1.4.9_macos_arm64_signed.pkg	11-Apr-2023 10:41	74142354
cisco_radkit_1.4.9_macos_x86_64_signed.pkg	11-Apr-2023 10:41	77265560
cisco_radkit_1.4.9_pip_linux.tgz	04-Apr-2023 11:49	146189048
cisco_radkit_1.4.9_pip_macos.tgz	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

Passaggio 4. Eseguire il programma di installazione sul PC o sul server. Nell'ambito dell'installazione, Radkit deve installare tre applicazioni: Radkit Service, Radkit Client e Radkit Network Console.

Servizio RADKit (lato utente)

Carico

Passaggio 1. Per avviare la configurazione del servizio RADKit, passare ad Applicazioni e individuare Servizio RADKit. La prima volta che viene eseguito, viene visualizzato il messaggio "not yet bootstrapped" (Non ancora avviato).



2. Fare clic su Configure RADKit, il browser viene visualizzato automaticamente con l'URL <https://localhost:8081/bootstrap>.

- Creare la password per l'utente superadmin e fare clic su Submit (Invia).
- Il nome utente e la password superadmin vengono richiesti a ogni avvio o configurazione del servizio.

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

Passaggio 3. Dopo aver fatto clic su Invia, il browser reindirizza l'utente a <https://localhost:8081/#/connectivity/>.

In Connettività > Iscrizione servizio sono disponibili due metodi di autenticazione: Single Sign-On e One-Time Password.

Single Sign-On Enrollment



✓

1

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

Passaggio 5. Completare la procedura guidata e completare i passaggi fino a visualizzare "Servizio registrato con nuova identità: xxxx-xxxx-xxxx" e quando si fa clic su Chiudi il servizio viene visualizzato come Connesso.



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

Close



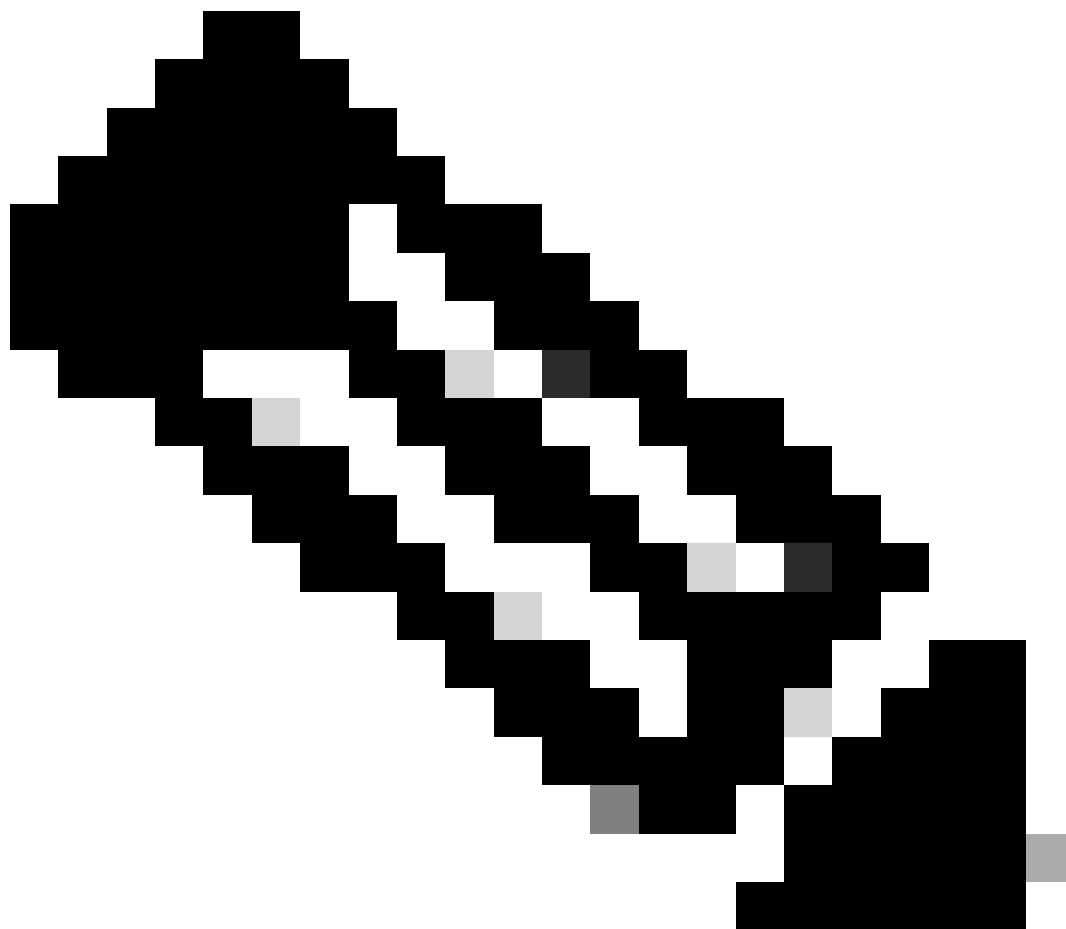
Remote Automation Development
Cisco RADKit Service

Domain: PROD Serial: k331-0evx-s94g

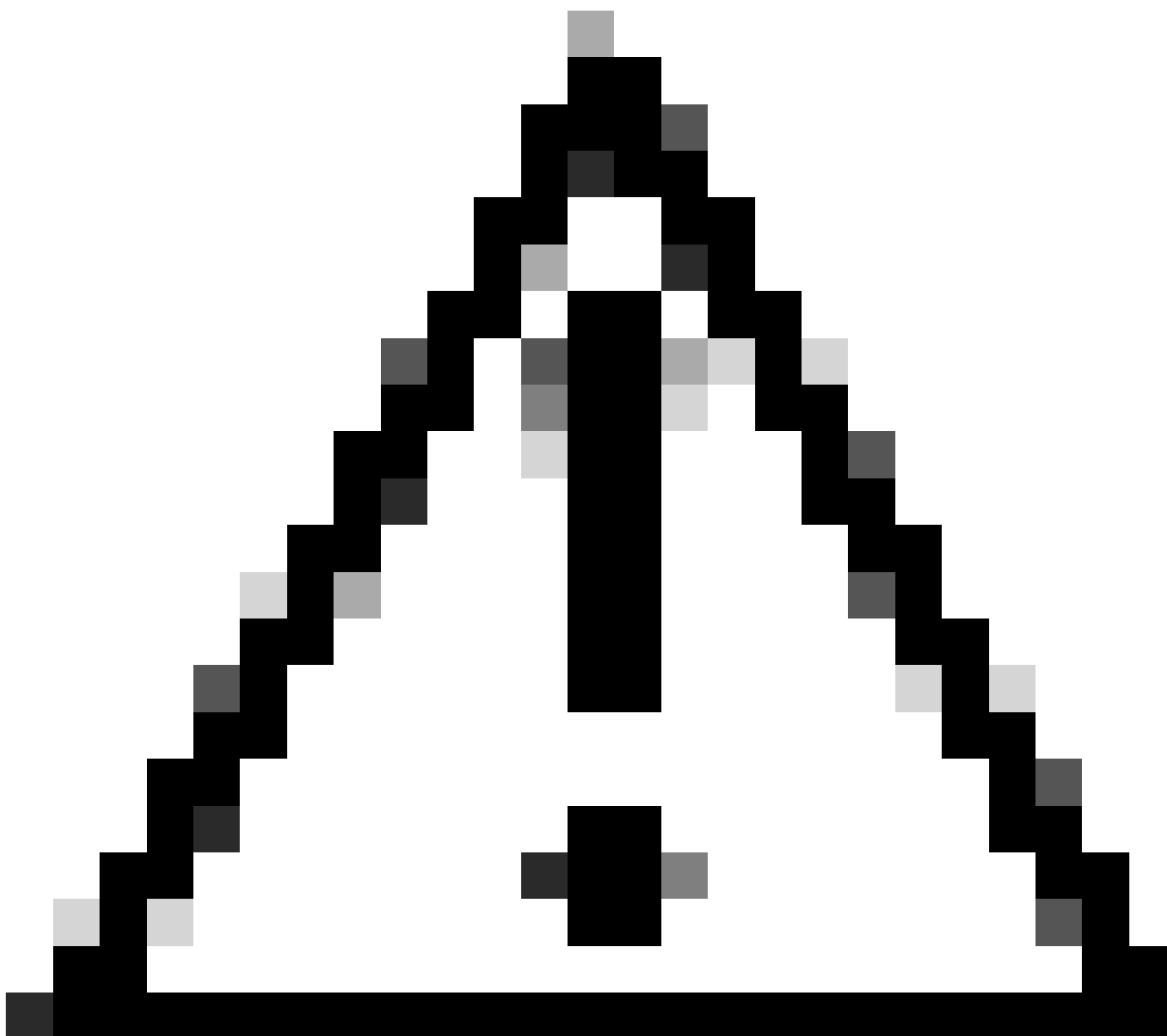


CONNECTED





Nota: Per attivare il servizio RADKit è necessario un account Cisco.

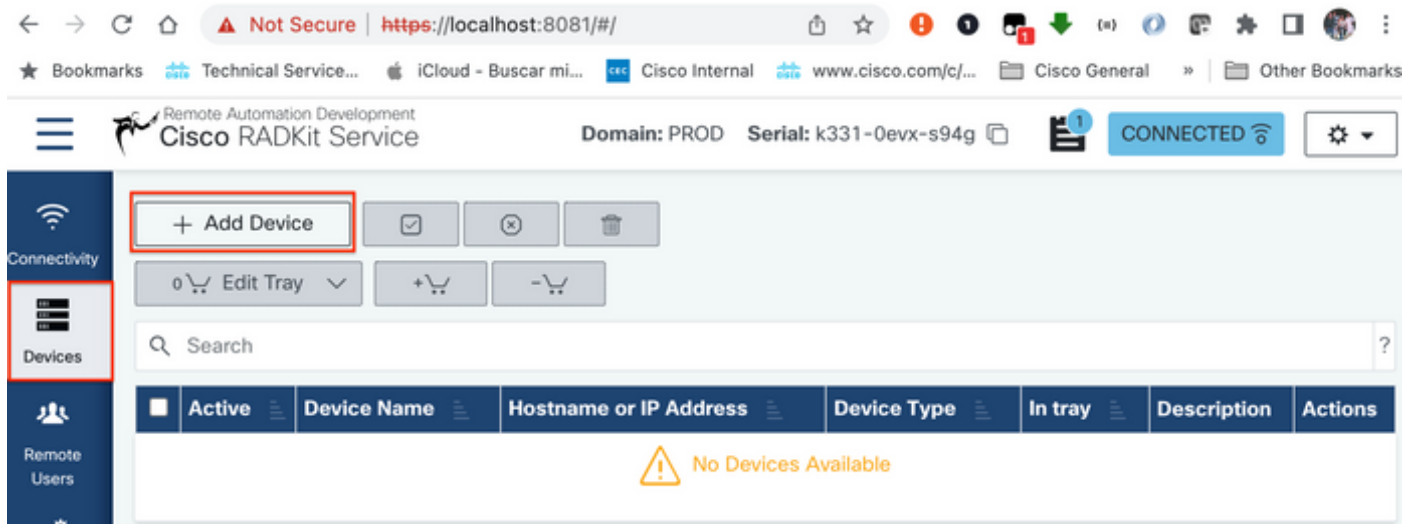


Attenzione:

- Se il server su cui è in esecuzione il servizio RADKit richiede la definizione di un proxy, oltre a definire il proxy sul server/PC stesso, è necessario definire anche una variabile di ambiente affinché il servizio RADKit funzioni
RADKIT_CLOUD_CLIENT_PROXY_URL=<http://proxy.example.com:80>.

Aggiungi dispositivi

Passaggio 1. Passare a Dispositivi e fare clic su Aggiungi dispositivo.



Passaggio 2. È necessario configurare i dettagli successivi:

- Nome dispositivo
- Indirizzo IP o nome host di gestione
- Tipo di dispositivo

È inoltre necessario configurare le porte TCP inoltrate, ovvero le porte utilizzate dal dispositivo che devono essere accessibili dal client RADKit. Nell'esempio, le porte usate sono 443 per l'accesso GUI e 8443 per RTMT.

Infine, selezionare i protocolli di gestione disponibili, in questo caso Terminal e HTTP.

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

Passaggio 3. Per ciascun protocollo di gestione configurare le impostazioni corrette e fare clic su Aggiungi e chiudi.

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 ?

Passaggio 4. Una volta aggiunta, la periferica deve essere visualizzata nell'elenco delle periferiche e può essere abilitata/disabilitata per l'accesso remoto.

Remote Automation Development
Cisco RADKit Service

Domain: PROD Serial: k331-0evx-s94g

CONNECTED

Connectivity

Devices

Remote Users

+ Add Device

0 Edit Tray

Search

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

Autorizza utenti remoti

Passaggio 1. Per concedere all'utente l'accesso ai dispositivi configurati nel servizio RADKit, passare a Utenti remoti e selezionare Aggiungi utenti.

Remote Automation Development
Cisco RADKit Service

Domain: PROD Serial: k331-0evx-s94g

CONNECTED

Connectivity

Devices

Remote Users

+ 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

Passaggio 2. Configurare i dettagli dell'utente:

- Indirizzo email
- Nome e cognome (facoltativo)
- Attivare l'utente.
- Specificare se l'attivazione deve essere controllata manualmente o impostare un intervallo di tempo per concedere l'accesso all'utente.

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

Passaggio 3. Selezionare Aggiungi e chiudi.

Client RADkit (lato TAC)

Accesso

Passaggio 1. Sul PC client, passare ad Applicazioni e individuare RADkit Client.

Passaggio 2. Creare un'istanza del client con l'accesso SSO.

<#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")
```

Passaggio 3. Accettare la richiesta di autorizzazione SSO aperta automaticamente nel browser.

← → ↻ 🏠 🔒 prod.radkit-cloud.cisco.com/auth/oauth?code=WIVdu... ⚙️ ☆ ! ⓘ 🗑️ ⬇️ ⌂ 🔍 🌐 📧 ⚙️ 🗑️ 🧑

★ Bookmarks 🌐 Technical Service... 🍏 iCloud - Buscar mi... 🇸🇬 Cisco Internal 🌐 www.cisco.com/c/... 📁 Cisco General » 📁 Other Bookmarl

 Remote Automation Development
Cisco RADKit Access

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

 Remote Automation Development
Cisco RADKit Access

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

Passaggio 4. Creare un'istanza del servizio utilizzando il numero di serie generato dall'utente dalla fase RADKit Service - Onboarding.

 Remote Automation Development
Cisco RADKit Service

Domain: PROD

Serial: k331-0evx-s94g 📄

 2

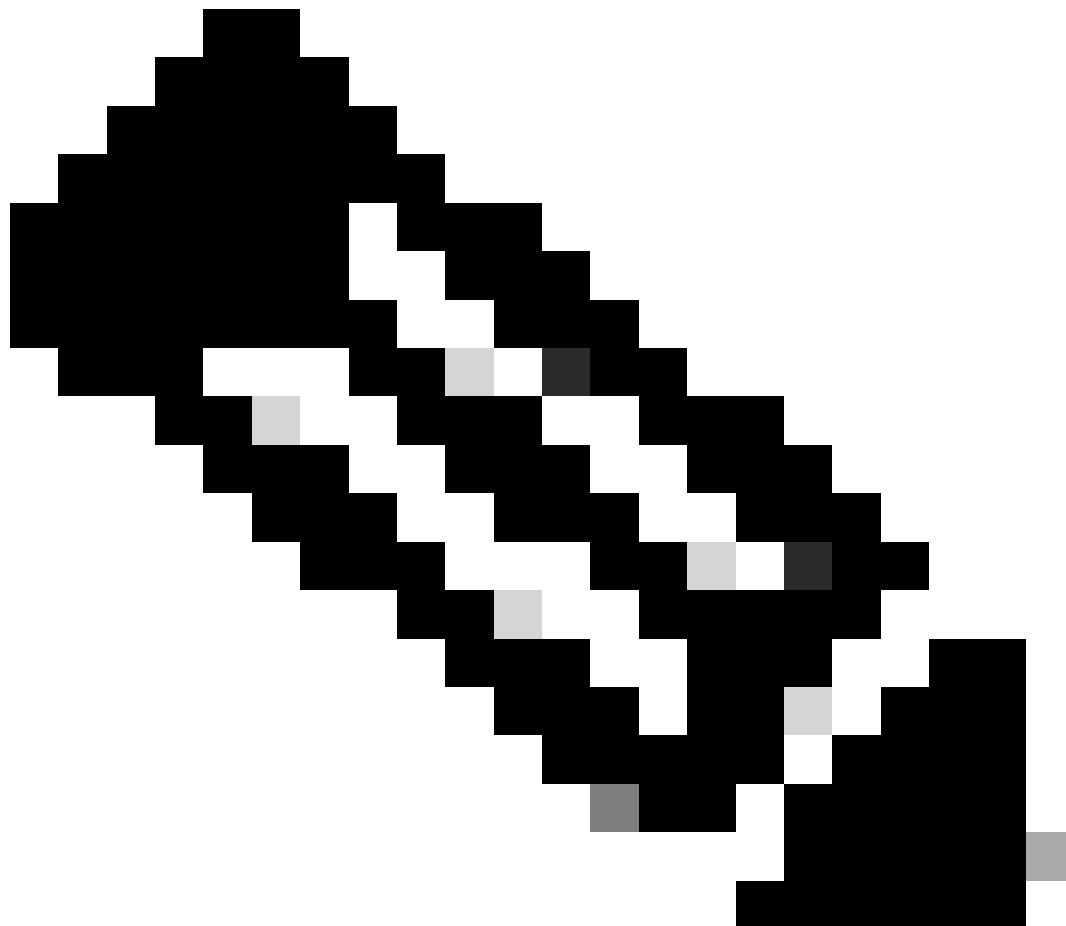
CONNECTED 📶

<#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/']
```



Nota: service è una variabile che può essere qualsiasi.

Passaggio 5. Controllare i dispositivi disponibili per l'accesso.

<#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
```

Per aggiornare l'elenco dell'inventario, utilizzare il comando `update_inventory`.

<#root>

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

Accesso SSH

Passaggio 1. Creare un oggetto dall'elenco di inventario.

<#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"]
```

Passaggio 2. Avviare la sessione SSH con il comando interattivo.

<#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 ...

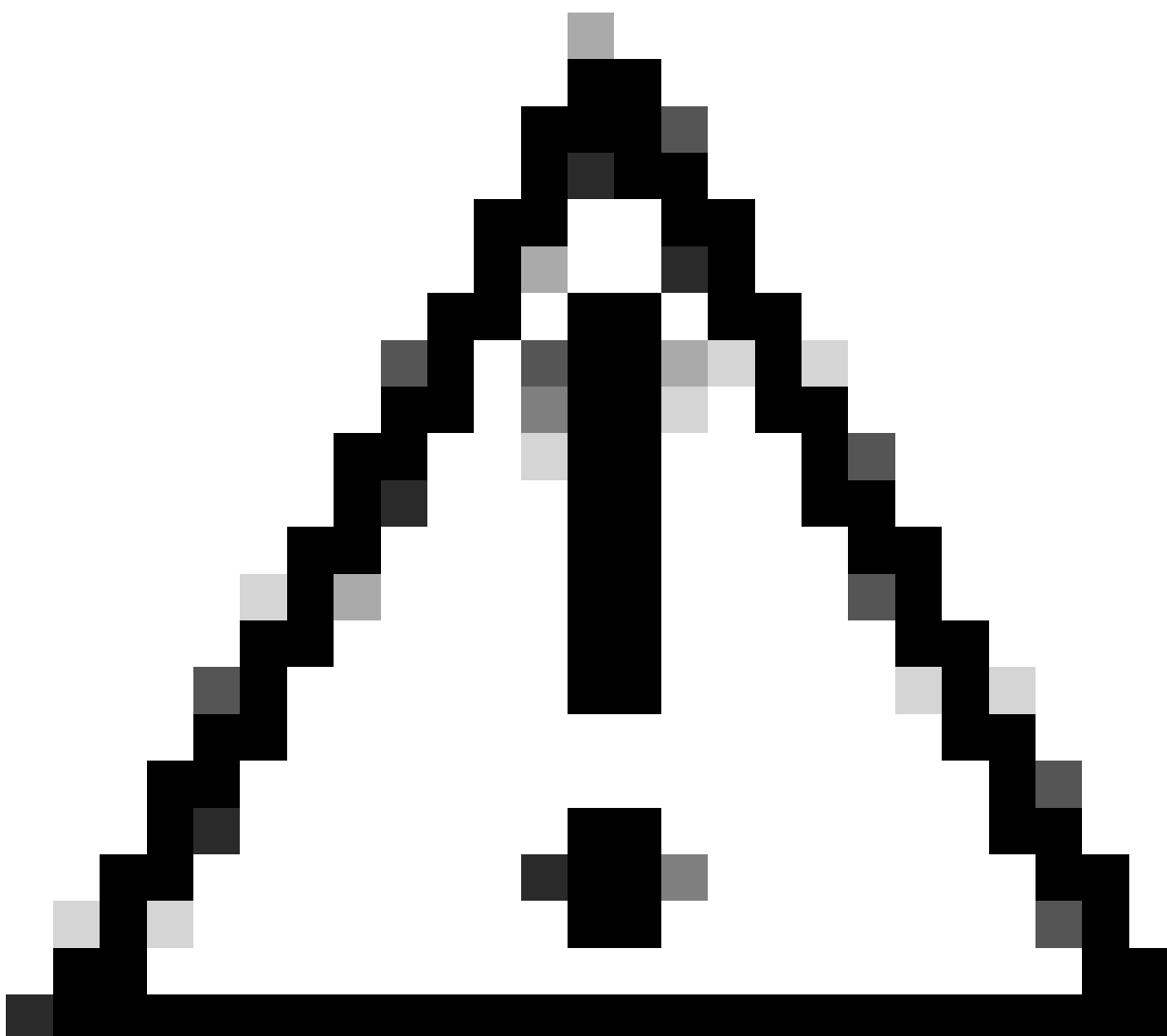
Welcome to the Platform Command Line Interface

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:

```

Passaggio 3. Ora è possibile gestire il dispositivo normalmente.



Attenzione:

- Stai sempre attento alle nostre responsabilità quando operi in un ambiente utente.
- RADKit deve essere utilizzato come strumento di raccolta dati.
- Non apportare modifiche senza l'autorizzazione dell'utente.
- Documentare tutte le scoperte nelle note sulla richiesta.

Accesso GUI

- Proxy HTTP

Passaggio 1. Verificare che le credenziali HTTP siano state aggiunte nel servizio RADKit nella configurazione del dispositivo.

Passaggio 2. Avviare il proxy HTTP sul client Radkit e definire la porta locale utilizzata per connettersi al 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
>>>
```

Passaggio 3. Dal browser, passare a <https://localhost:4001> e selezionare il servizio a cui connettersi.



Passaggio 4. Fare clic sull'opzione Vai a pagina Web sul dispositivo corretto per connettersi alla relativa pagina Web.

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

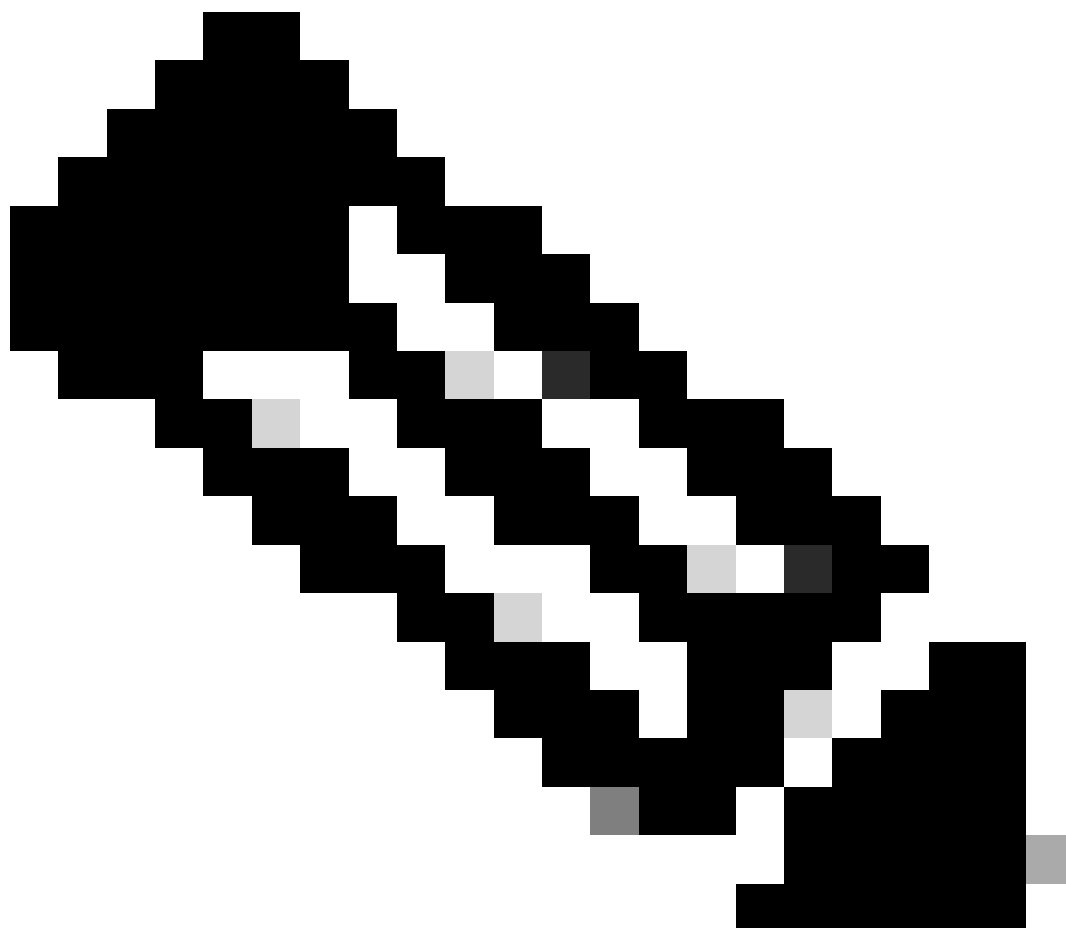
Technical Services... iCloud - Buscar mi... Cisco Internal www.cisco.com/c/... Cisco General BUFF Dedicated Instance WxC Calling Voice Ir

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	<button>Reset</button>
expressway-e	443;8443	Go to web page	<button>Reset</button>
cucmhq	443;8443	Go to web page	<button>Reset</button>

[← Go back](#)



Nota: la prima volta che il proxy HTTP viene configurato su un client RADKit, si consiglia di fare clic sull'opzione Reset for each Devices (Reimposta per ciascun dispositivo) prima

di tentare di aprire la pagina Web del dispositivo.

Passaggio 5. Viene visualizzata la pagina Web.

← → ↻ 🏠 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, Encryption

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

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

- Port Forwarding

Passaggio 1. Verificare le porte di inoltro TCP configurate per il dispositivo.

<#root>

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

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

Passaggio 2. Configurare una porta locale da associare alla porta di destinazione del dispositivo. Per accedere alla GUI del dispositivo, è necessario utilizzare la porta locale.

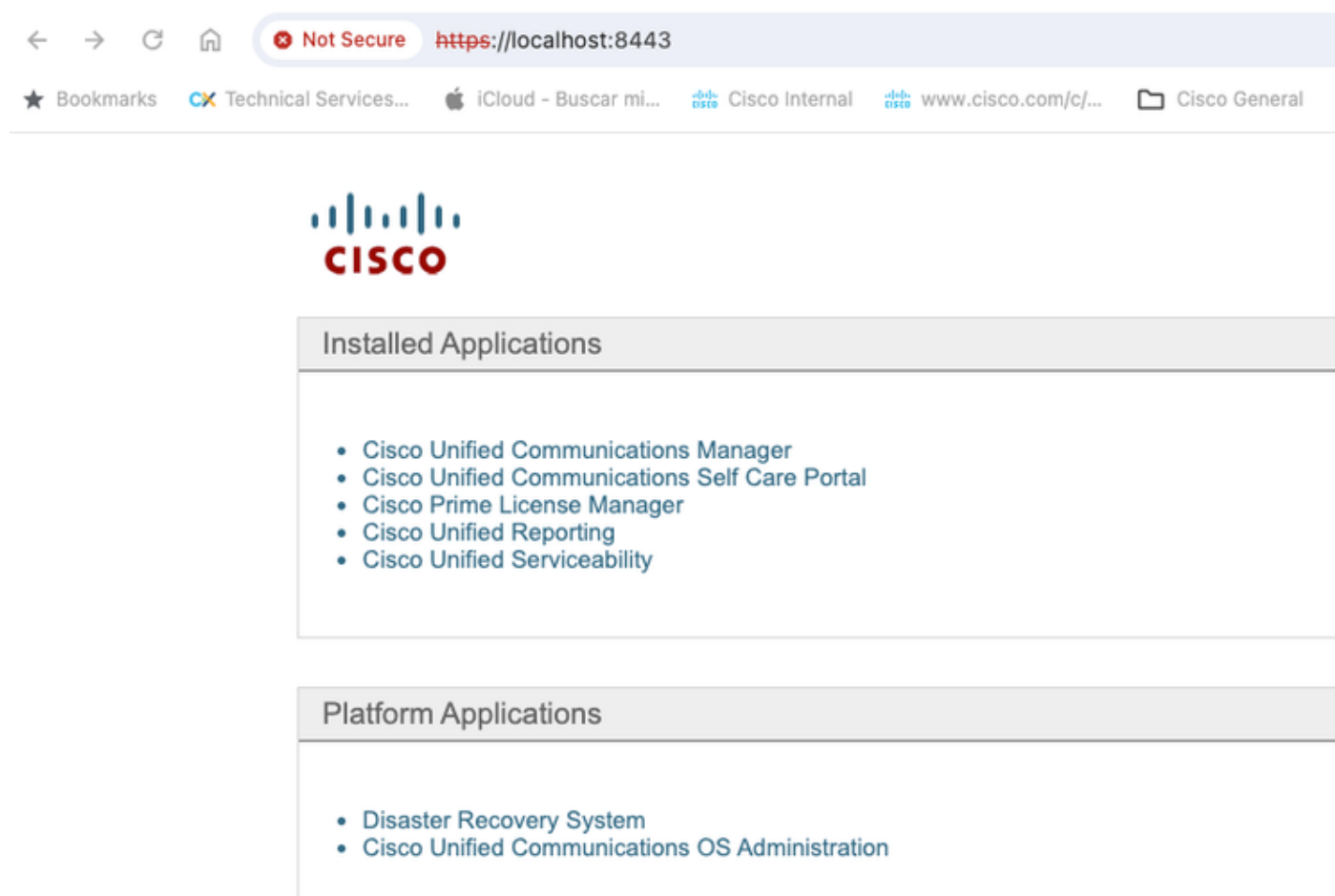
<#root>

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

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

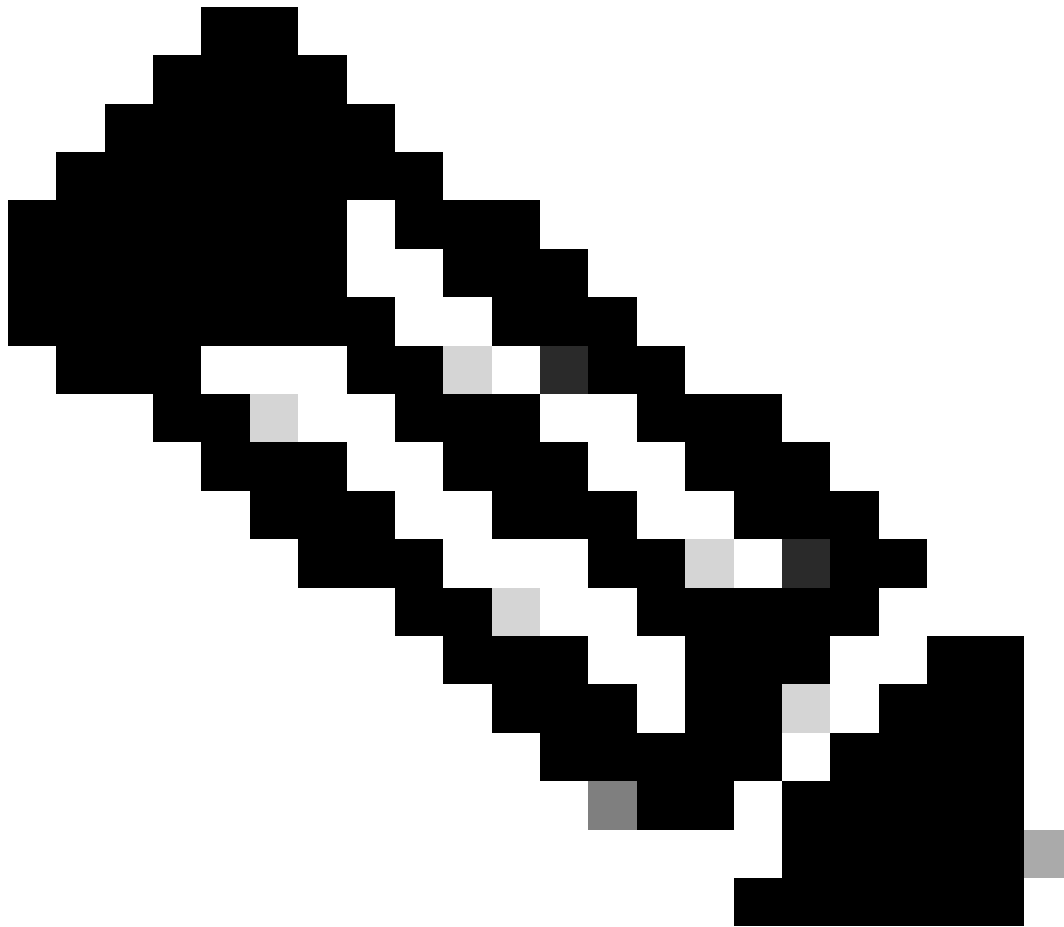
Passaggio 3. Aprire il browser e digitare l'URL con la porta configurata nel Passaggio 2:
<https://localhost:8443>.

La GUI del dispositivo è ora accessibile.



The screenshot shows a web browser window with the address bar displaying 'https://localhost:8443' and a 'Not Secure' warning. The browser's bookmark bar includes 'Bookmarks', 'Technical Services...', 'iCloud - Buscar mi...', 'Cisco Internal', 'www.cisco.com/c/...', and 'Cisco General'. The main content area features the Cisco logo at the top. Below the logo, there are two sections:

- 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



Nota: Per accedere alla GUI del prodotto sono ancora necessarie le credenziali per l'accesso, pertanto è consigliabile creare un account utente di sola lettura per l'accesso.

Raccolta log

- RTMT

Passaggio 1. Verificare che la porta 8443 sia elencata nelle porte inoltrate TCP configurate per il dispositivo.

```
<#root>
```

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

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

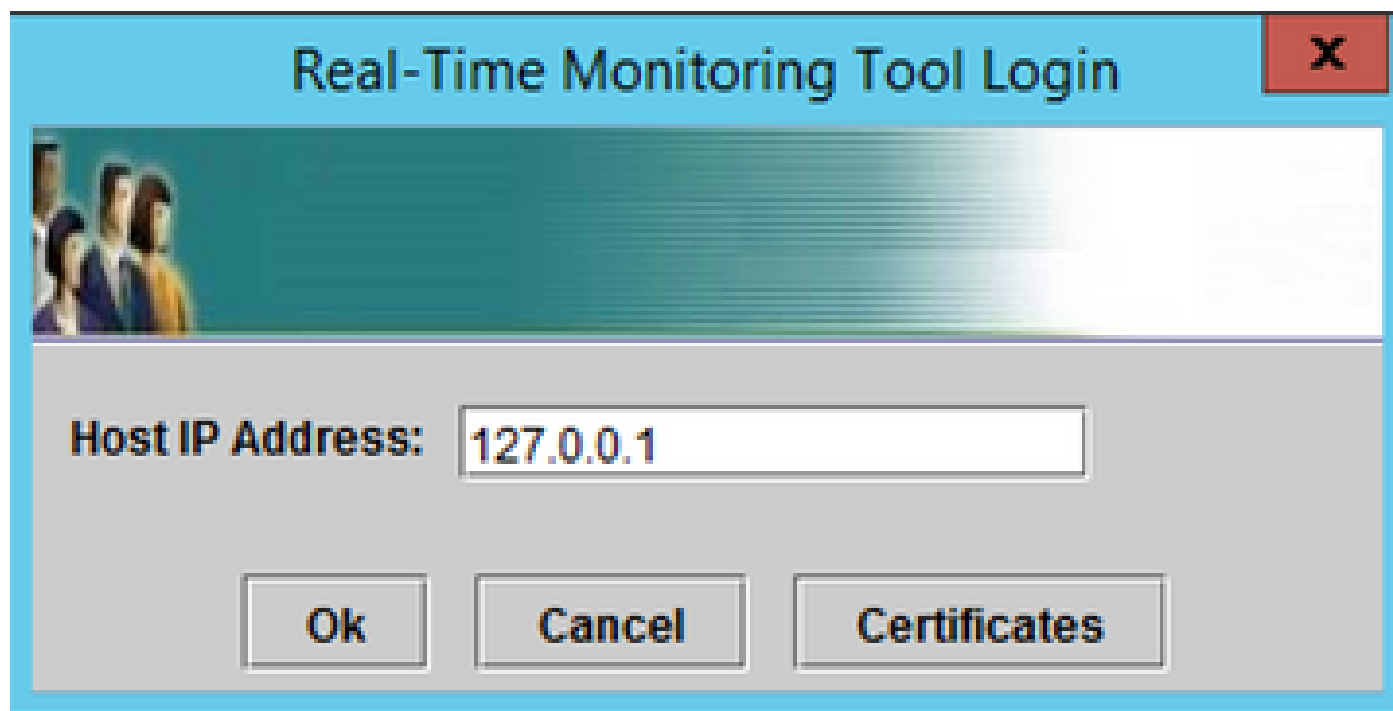
Passaggio 2. Configurare la stessa porta 8443 come porta locale da associare alla porta 8443 come porta di destinazione del dispositivo.

<#root>

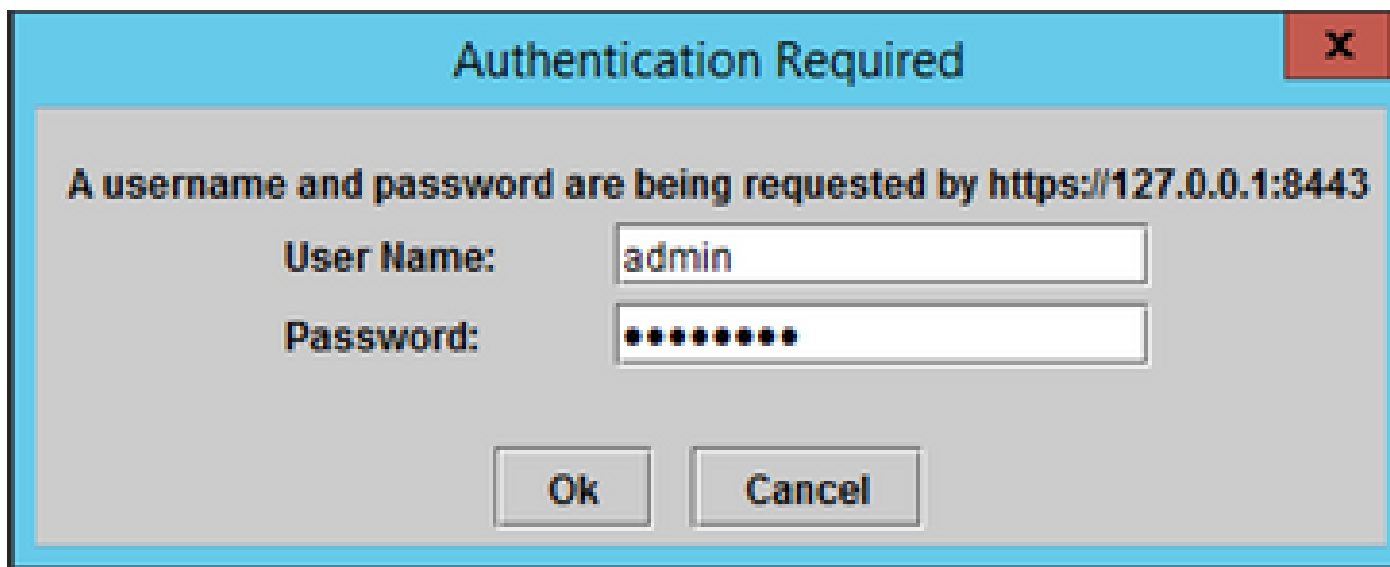
```
>>> cucm.forward_tcp_port(local_port=8443, destination_port=8443)
```

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

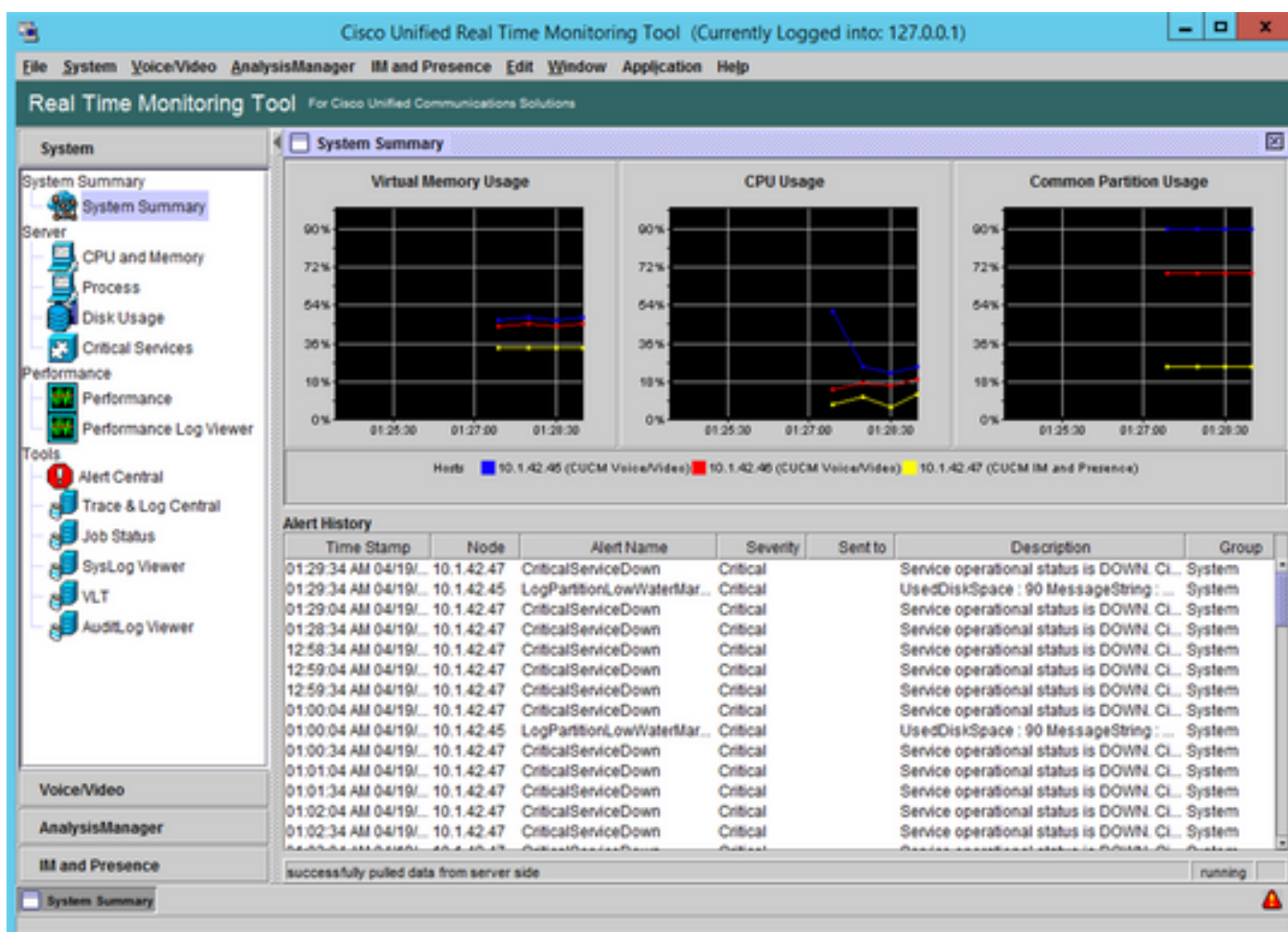
Passaggio 3. Aprire RTMT e digitare 127.0.0.1 nell'indirizzo IP dell'host, viene utilizzata automaticamente la porta 8443.



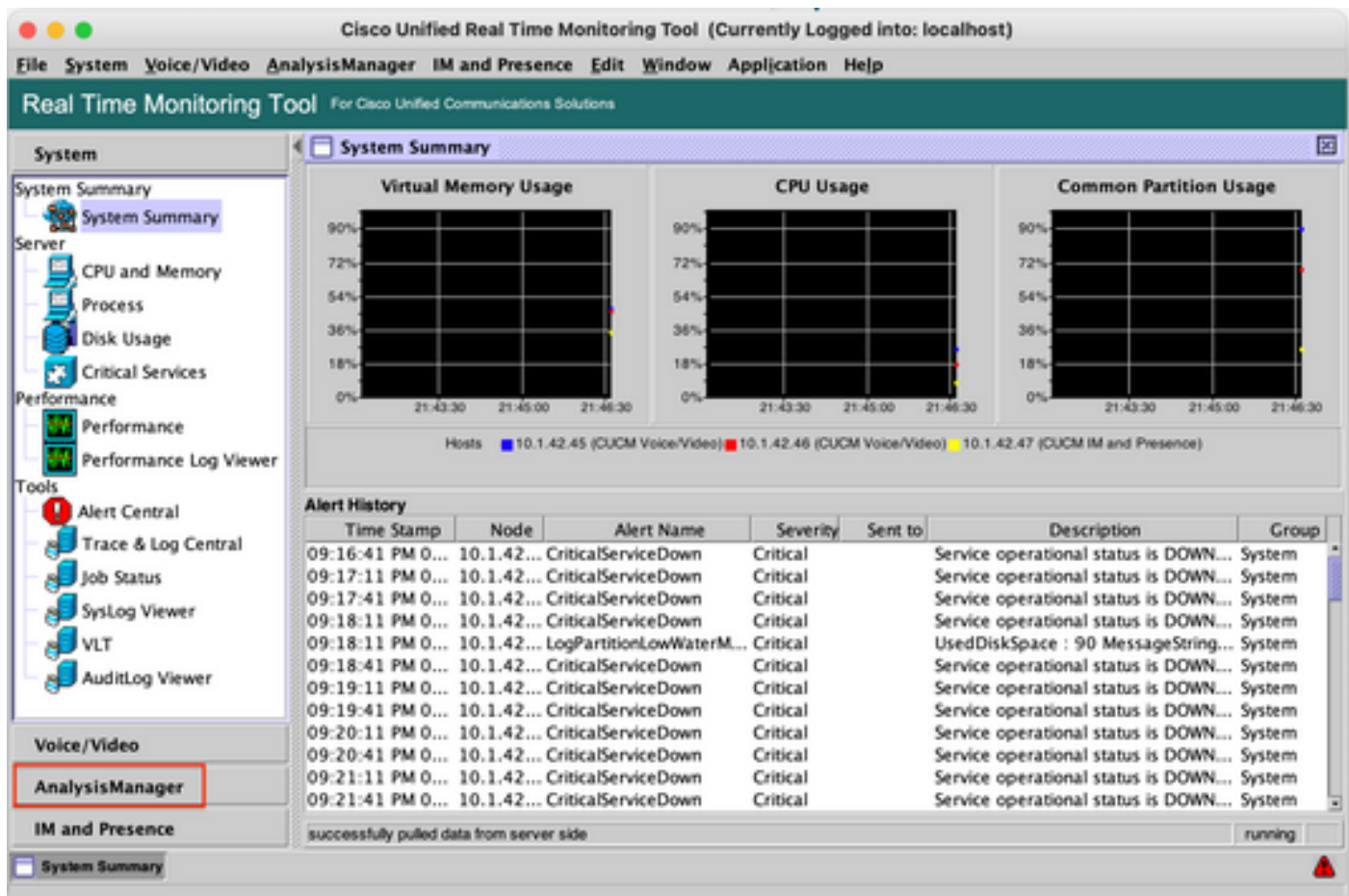
Passaggio 4. Accedere con le credenziali corrette.



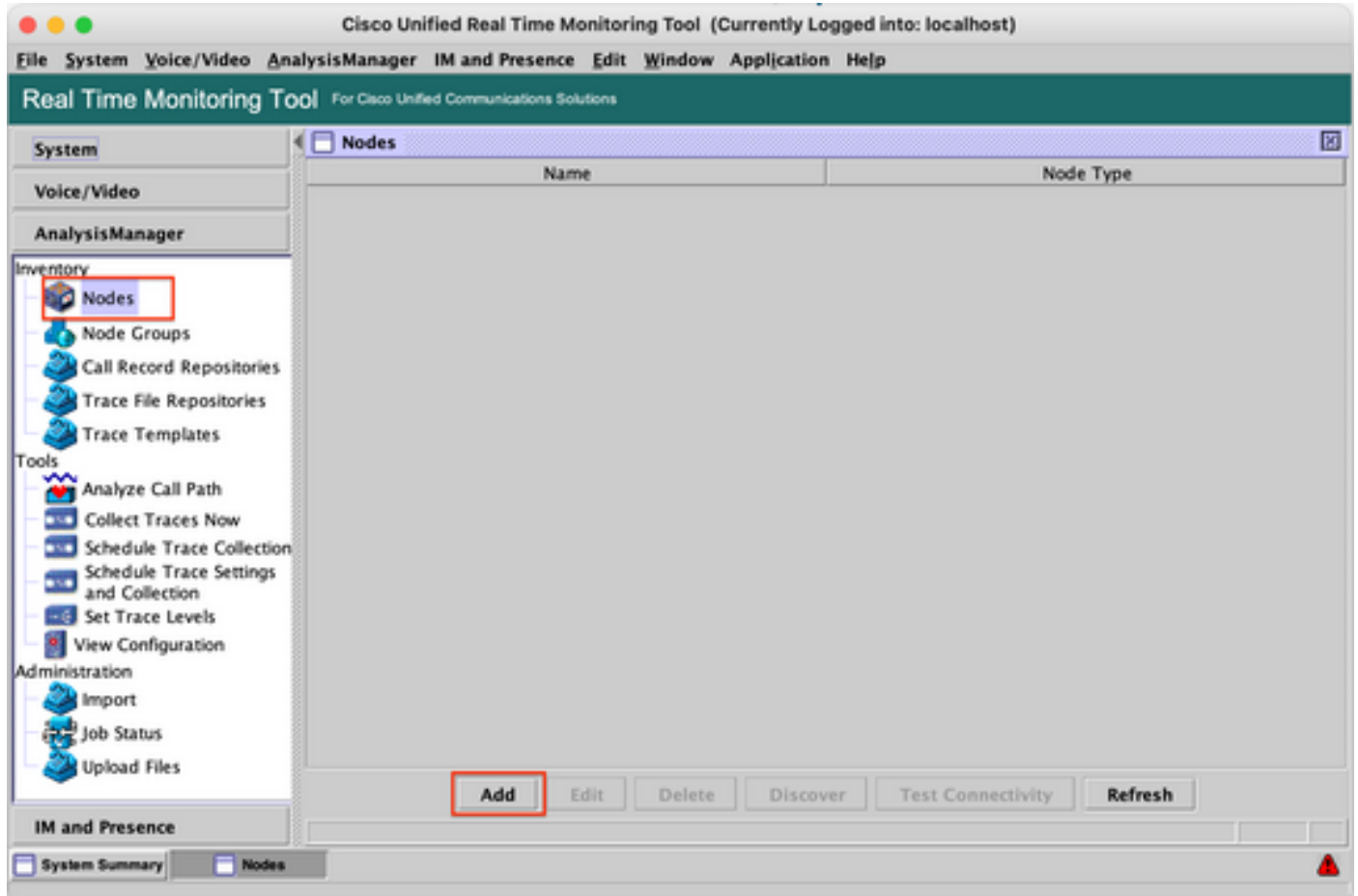
Passaggio 5. Viene visualizzato RTMT.



Passaggio 6. Andare a Analysis Manager nel pannello sinistro.



Passaggio 7. Fare clic su Nodi e Aggiungi per configurare i dettagli della periferica da aggiungere utilizzando localhost e la porta TCP inoltrata.



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

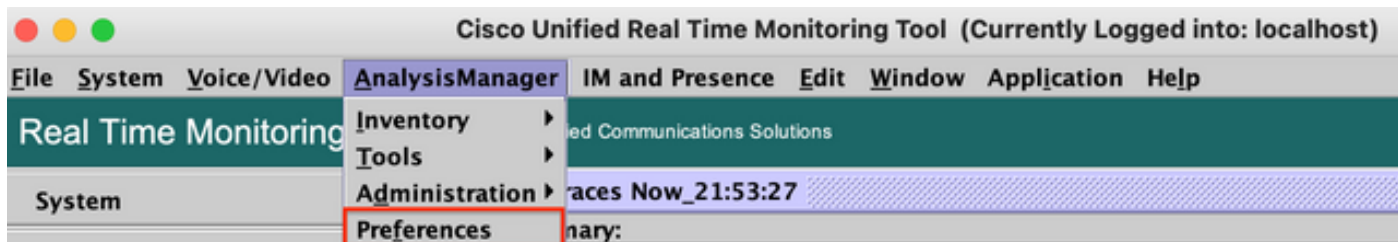
Associated Group ☒ AllNodes

Advanced...

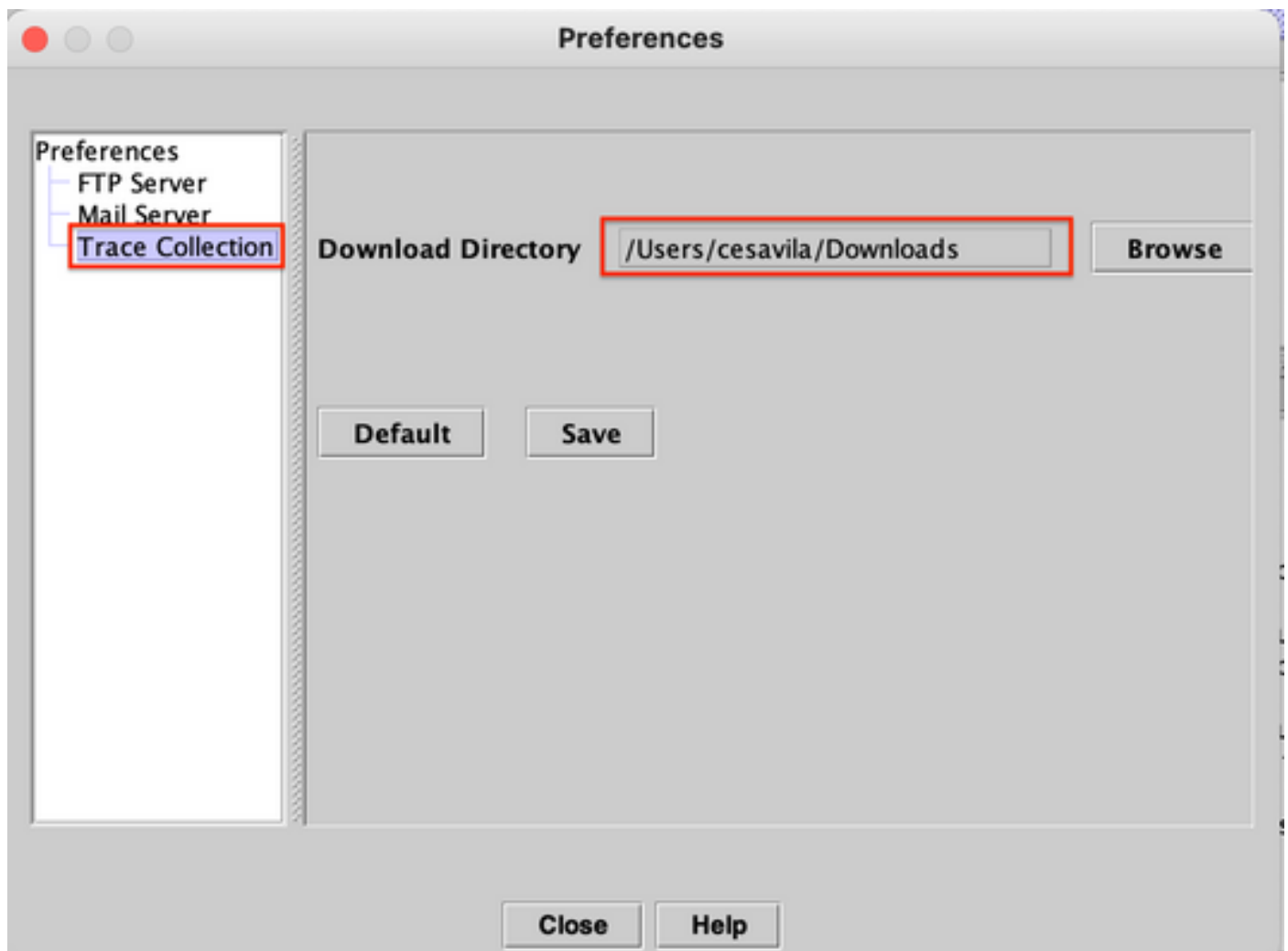
* Required Fields

Save **Cancel**

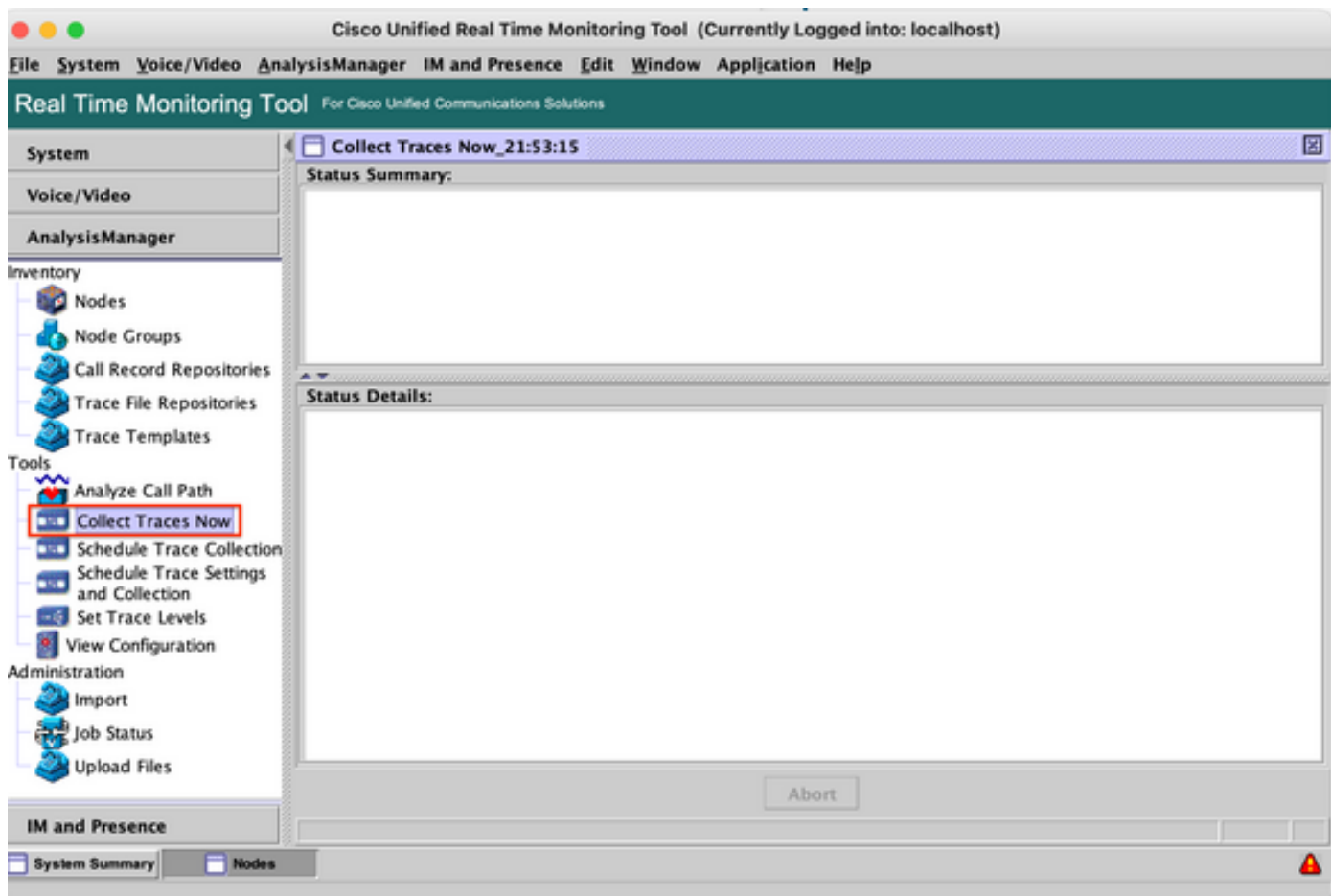
Passaggio 8. Fare clic su Analysis Manager nel menu nella parte superiore e selezionare Preferenze.



Passaggio 9. Accedere a Raccolta di tracce e selezionare la cartella corretta per scaricare i log, fare clic su Salva e quindi su Chiudi.



Passaggio 10. Passare a Raccolta tracce.



Passaggio 11. Selezionare l'opzione Nodo, selezionare il dispositivo aggiunto al passaggio 7 e fare clic su Personalizza.

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...**

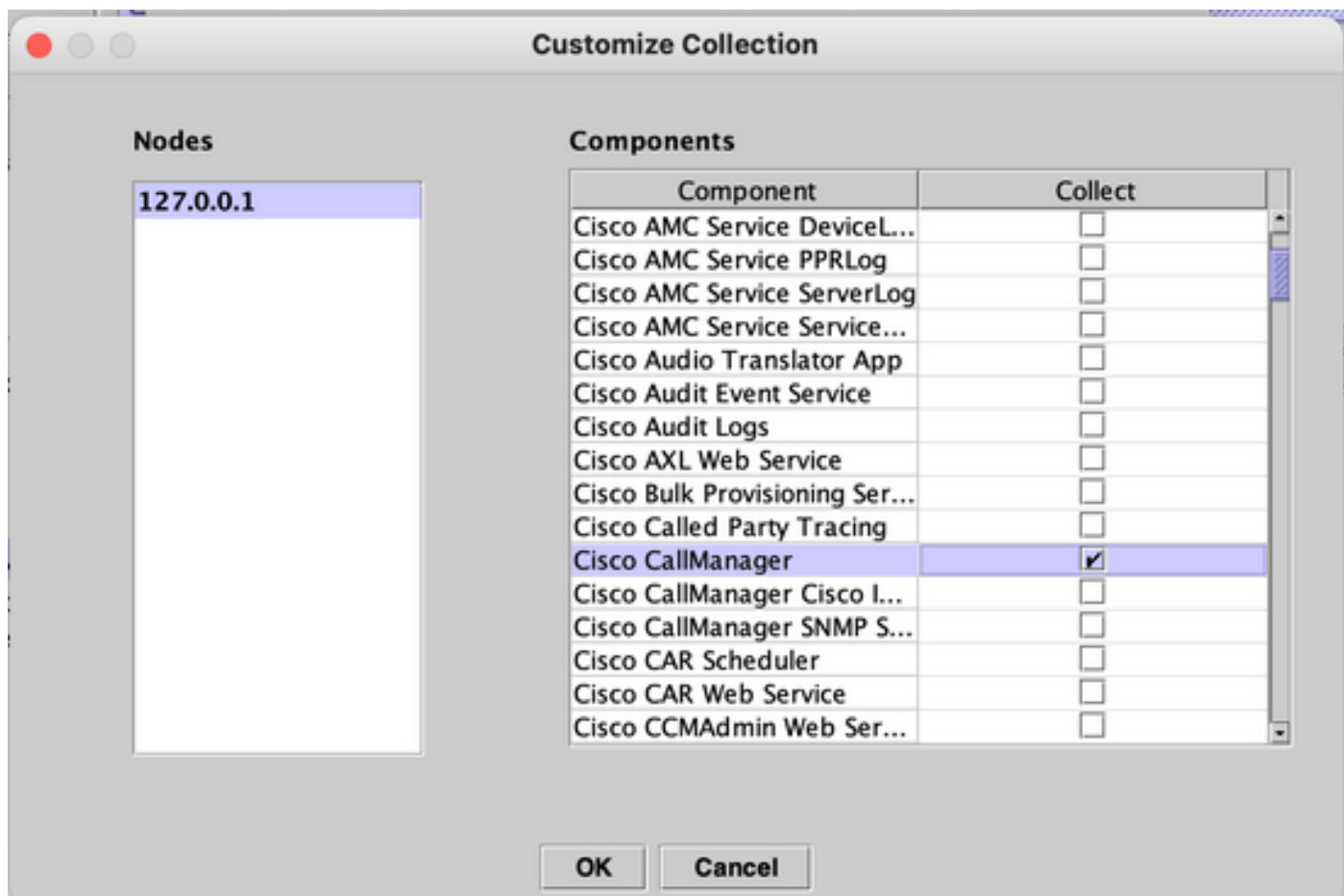
Start Time:

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

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

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

Passaggio 12. Selezionare i log da raccogliere dal dispositivo e fare clic su OK.



Passaggio 13. Infine, selezionare Ora inizio e Ora fine dei log da raccogliere e fare clic su 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 ▼ Customize...

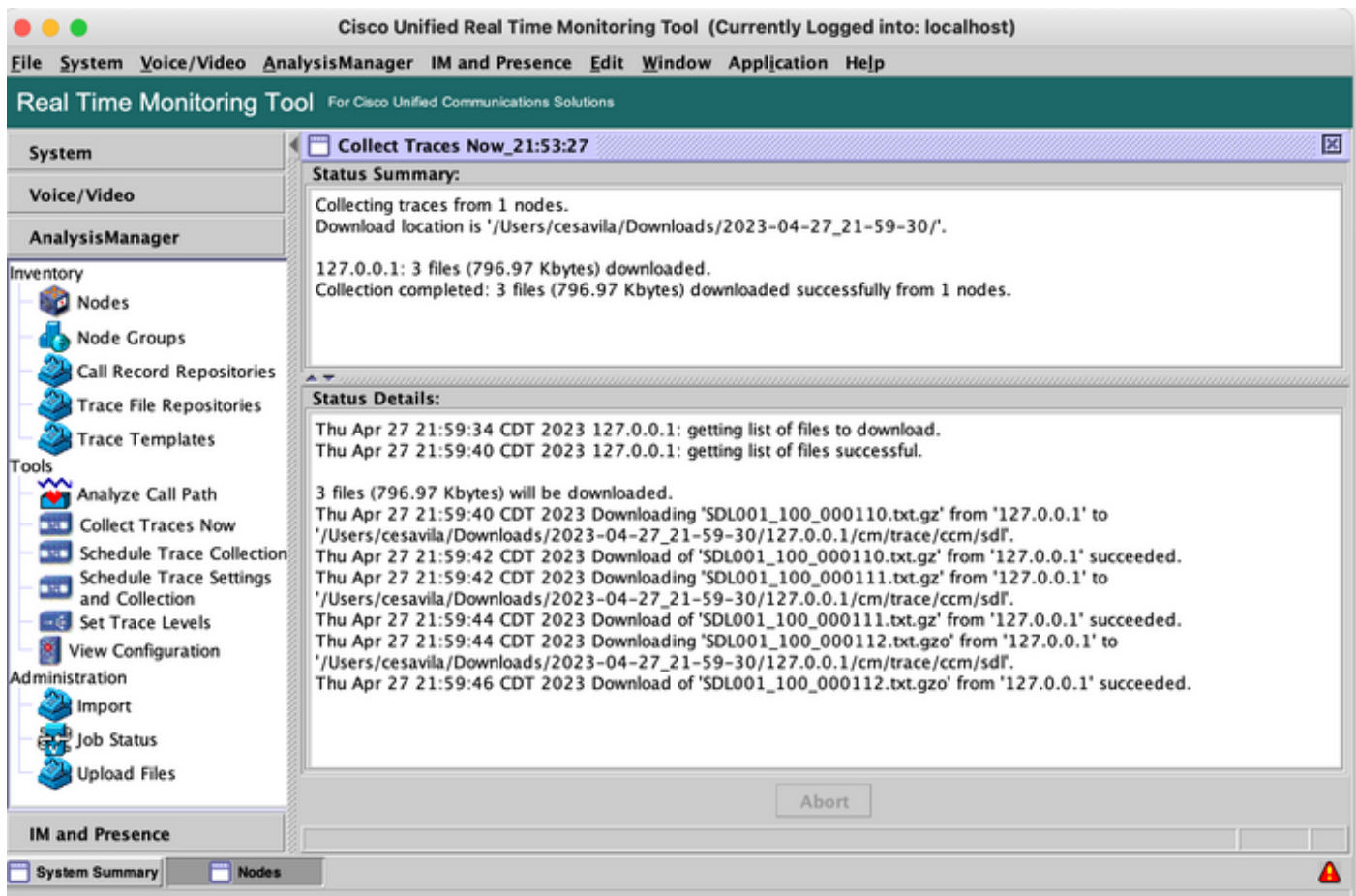
Start Time: 04-27-2023 21:00:00 ▼

End Time: 04-27-2023 21:53:27 ▼

Time Zone: (GMT-6:0)Central Dayl... ▼

View Summary **OK** Cancel Help

Passaggio 14. I file vengono scaricati correttamente nel PC locale (RADKit Client PC).



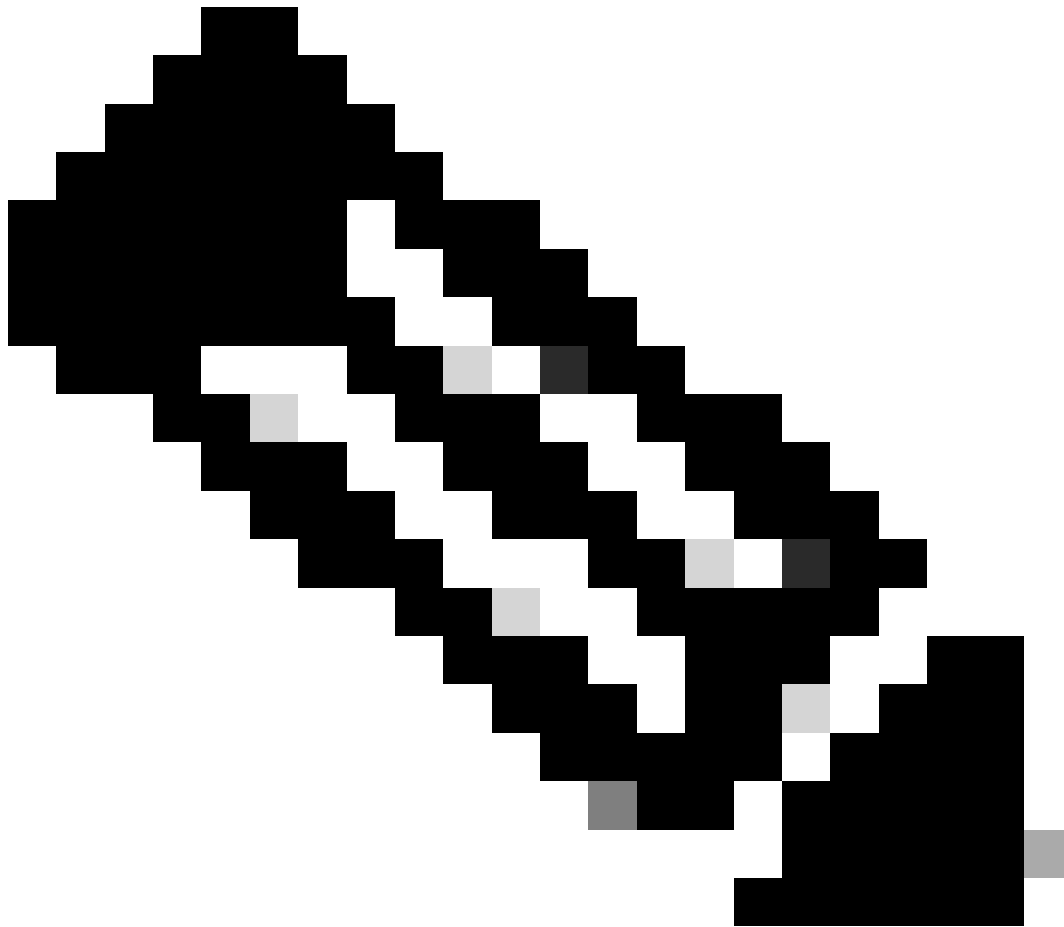
- API SOAP

L'API SOAP è attualmente supportata per CUCM. Inoltre, Swagger è supportato per CMS, Expressway, CVP e così via.

Passaggio 1. Verificare che le credenziali HTTP siano state aggiunte nel servizio RADKit nella configurazione del dispositivo.

Passaggio 2. Eseguire il comando HTTP Post sul client RADKit, specificare il percorso della risorsa e il corpo della richiesta con i parametri e le intestazioni necessari.

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



Nota: L'opzione 'cucm-extract' viene utilizzata per rimuovere le intestazioni delle risposte HTTP in modo da poter salvare il registro in un 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\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...'
-----
```

Passaggio 3. Salvare il contenuto in un file per ottenere il file di traccia salvato nel PC locale.

<#root>

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

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

Casi di utilizzo di RADKit

Come è stato evidenziato, RADKit fornisce una connessione sicura ai dispositivi di rete, inclusi i server di collaborazione, senza la necessità di essere su un WebEx. L'idea è di semplificare alcune delle sfide relative alla raccolta dei dati fornendo l'accesso on demand ai dispositivi richiesti.

Parlando in modo specifico di installazioni di collaborazione, RADKit può attualmente essere molto utile per una serie di problemi, ad esempio:

- Problemi di replica del database.
- Procedure di rigenerazione dei certificati.
- Controllo dello stato del sistema.
- Convalida della configurazione nella GUI/CLI.
- Raccolta dei log tramite interfaccia Web (ad esempio, CER, Expressway, CIMC, ecc.).
- Registri di debug tramite CLI su gateway voce.

Informazioni correlate

- Pagina principale RADKit <https://radkit.cisco.com/>
- Pagina di supporto per la tecnologia RADKit esterna <https://community.cisco.com/t5/radkit-discussions/bd-p/disc-radkit>

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).