

# Configuración de RADKit en un entorno de colaboración

## Contenido

---

[Introducción](#)

[Requirements](#)

[Componentes Utilizados](#)

[Terminology](#)

[Arquitectura RADKit](#)

[Instalación de RADKit](#)

[Servicio RADKit \(lado del usuario\)](#)

[Incorporación](#)

[Agregar dispositivos](#)

[Autorizar usuarios remotos](#)

[Cliente RADkit \(TAC\)](#)

[Inicio de sesión](#)

[Acceso SSH](#)

[Acceso a GUI](#)

[Proxy HTTP](#)

[Reenvío de puertos](#)

[Recopilación de registros](#)

[RTMT](#)

[API SOAP](#)

[Casos prácticos de RADKit](#)

[Información Relacionada](#)

---

## Introducción

Este documento describe los pasos para configurar RADKit y muestra la configuración necesaria para iniciar su uso con productos de colaboración.

## Requirements

Cisco recomienda que tenga conocimientos sobre estos temas:

- Conocimiento básico de cualquier producto de VOS Collaboration
- Conocimientos básicos de Acceso CLI/SSH

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y

hardware.

- Cisco Unified Communications Manager 12.5 y 14.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

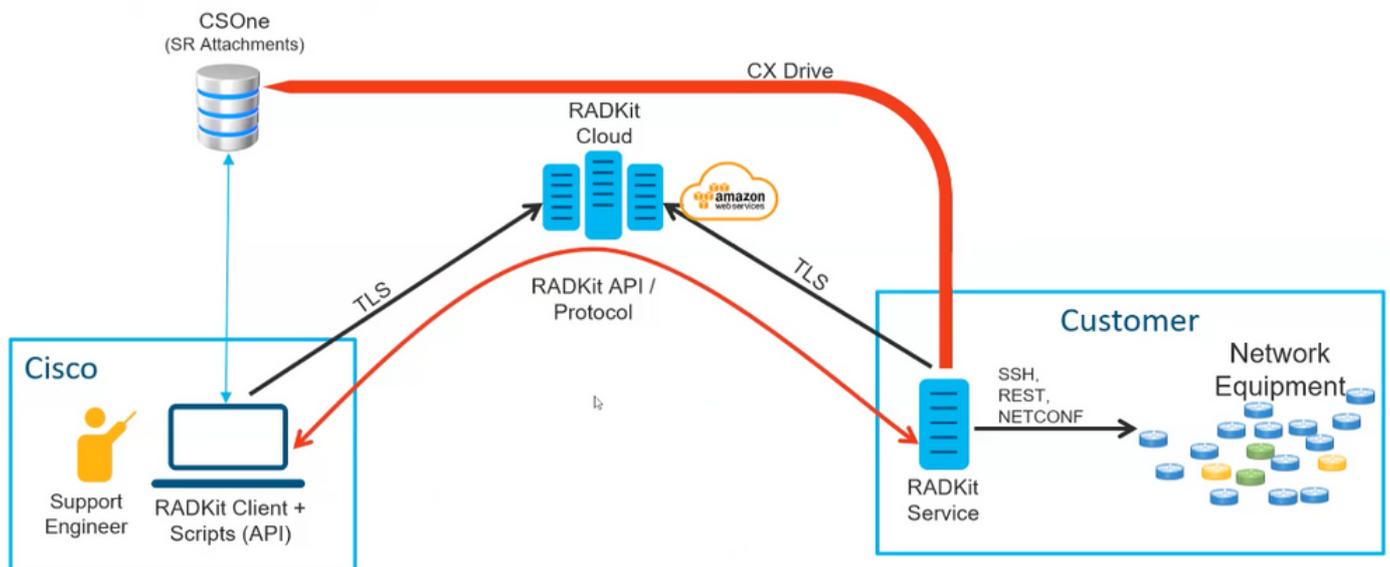
## Terminology

**RADKit:** Se trata de un conector que proporciona acceso remoto seguro a los dispositivos del usuario a los ingenieros y partners del Cisco TAC. Admite varios protocolos para interactuar con dispositivos, como SSH o HTTP/HTTPS.

**Servicio RADKit:** Este es el lado del Servidor. El Usuario se encarga de gestionarla y gestionarla en su totalidad. Desde el lado del servidor, los controles de usuario, quién puede acceder a los dispositivos y durante cuánto tiempo. El servicio Radkit debe tener conectividad con los dispositivos de la red para poder acceder a ellos.

**Cliente RADKit:** Este es el lado del Cliente. Se trata del PC utilizado para conectarse a los dispositivos de la red del usuario.

## Arquitectura RADKit



Arquitectura RADKit

## Instalación de RADKit

Paso 1. Desplácese a <https://radkit.cisco.com> y haga clic en Descargas y, a continuación, vaya a la carpeta release.

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/](#)

[release/](#)

03-Mar-2023 18:10

-

04-Apr-2023 11:45

-

Paso 2. Haga clic en la última versión.

## 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

-

Paso 3. Descargue el archivo correcto en función de su sistema operativo.

## 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

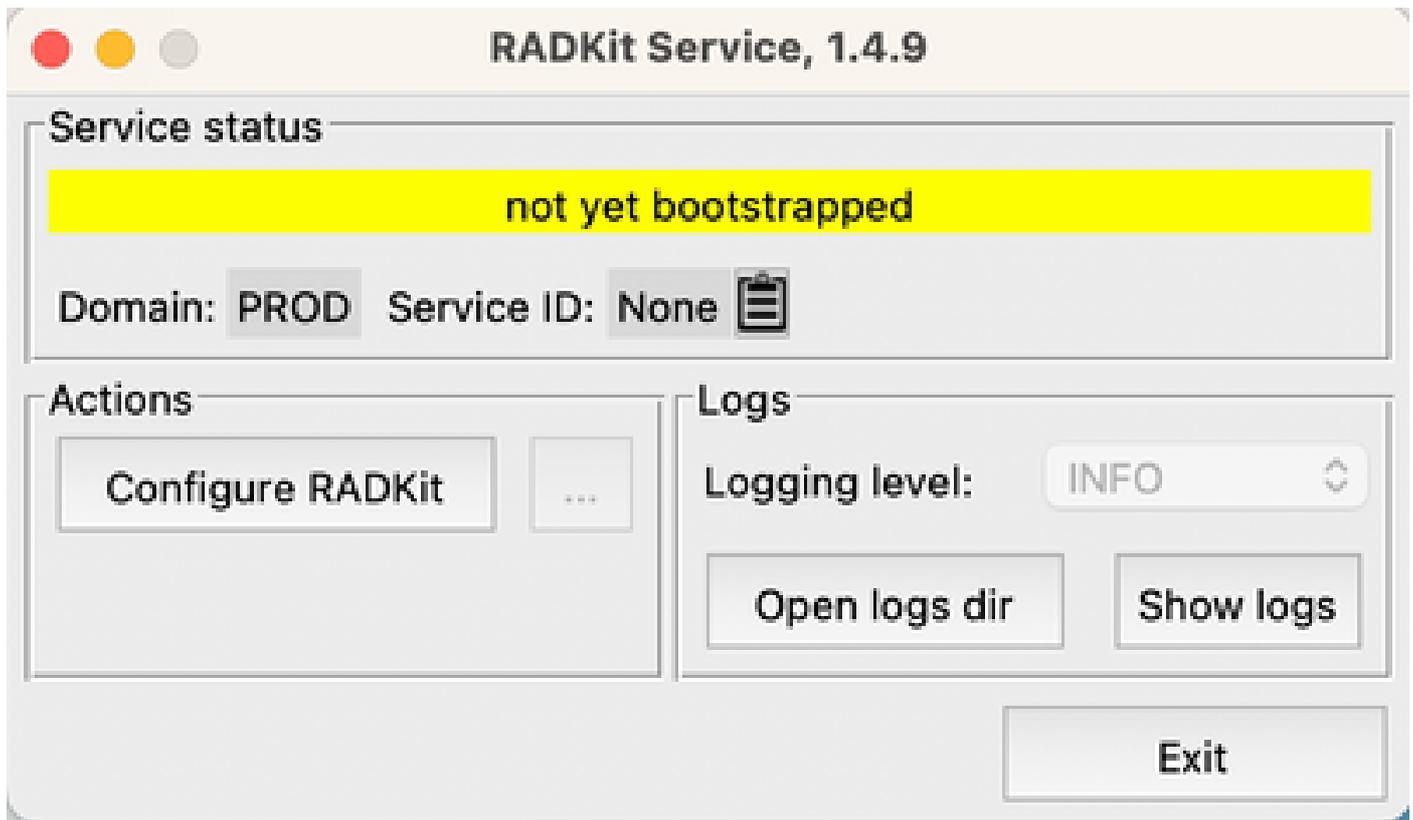
---

Paso 4. Ejecute el instalador en el PC o servidor. Como parte de la instalación, Radkit necesita instalar tres aplicaciones: Radkit Service, Radkit Client y consola de red Radkit.

### Servicio RADKit (lado del usuario)

#### Incorporación

Paso 1. Para comenzar a configurar el servicio RADKit, navegue hasta Aplicaciones y localice el servicio RADKit. La primera vez que lo ejecute, mostrará el mensaje "not yet bootstrap" (todavía sin bootstrap).



Paso 2. Haga clic en Configure RADKit, el navegador aparece automáticamente con la URL <https://localhost:8081/bootstrap>.

- Cree una contraseña para el usuario superadmin y haga clic en Enviar.
- Este nombre de usuario y contraseña de superadmin se solicita cada vez que se inicia o configura el servicio.

# 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

Paso 3. Una vez que haga clic en Enviar, el navegador le redirigirá a <https://localhost:8081/#/connectivity/>.

En Conectividad > Inscripción de Servicio, hay dos métodos de autenticación: Single Sing-On y 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

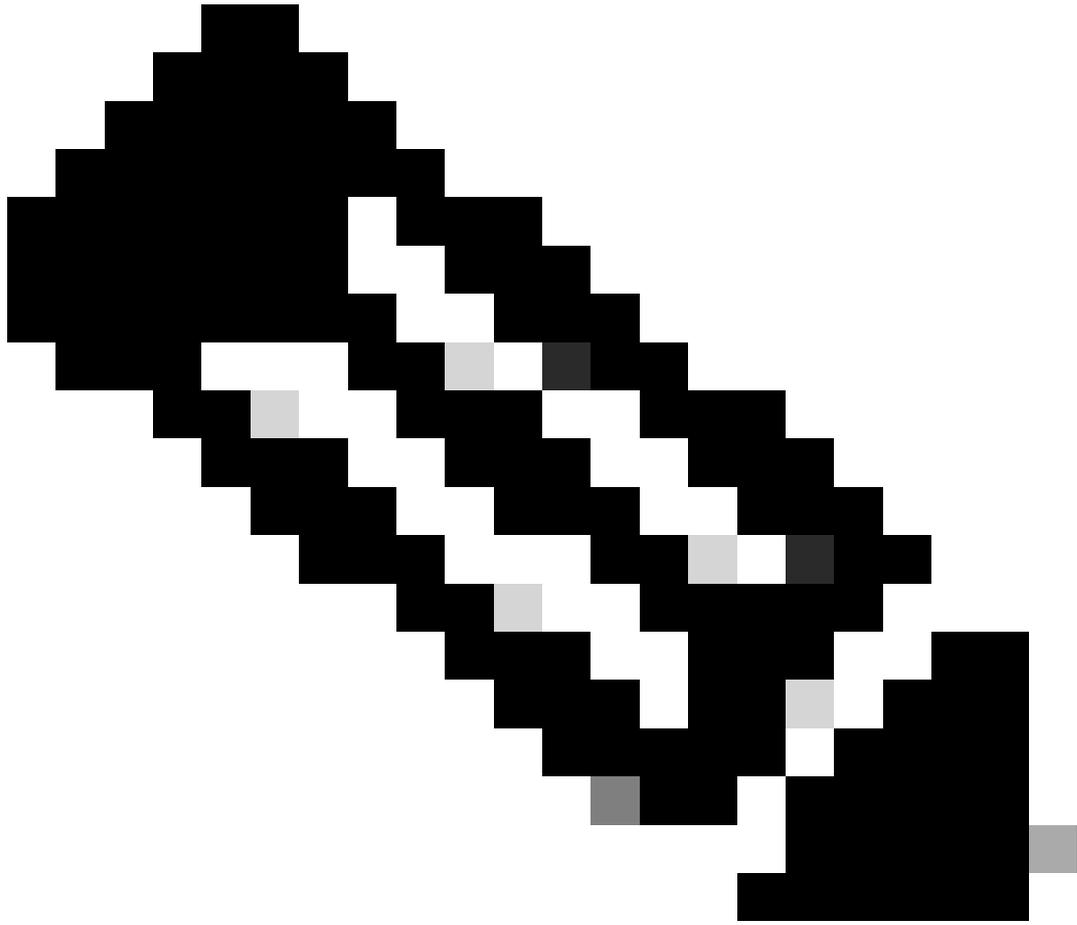
7 Requesting service certificate

Paso 5. Complete el asistente y complete los pasos hasta que aparezca "Servicio suscrito con nueva identidad: xxxx-xxxx-xxxx" y, al hacer clic en Cerrar, el servicio aparece como Conectado.

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

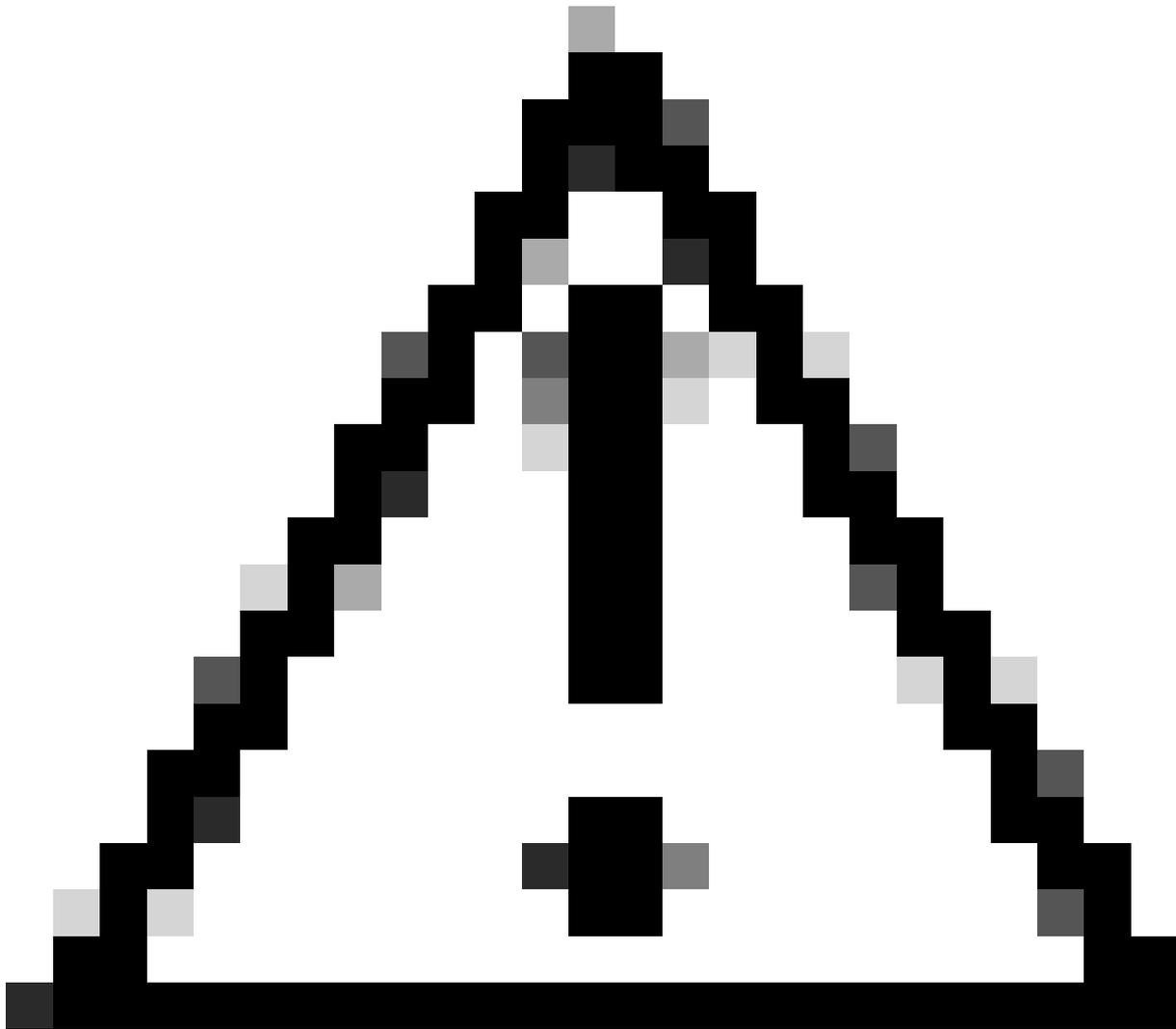
**Close**





Nota: Se necesita una cuenta de Cisco para activar el servicio RADKit.

---



Precaución:

- Si el servidor en el que se ejecuta el servicio RADKit requiere que se defina un proxy, además de definir el proxy en el servidor/PC, también debe definirse una variable de entorno para que el servicio RADKit funcione con `RADKIT_CLOUD_CLIENT_PROXY_URL=http://proxy.example.com:80`.

---

## Agregar dispositivos

Paso 1. Navegue hasta Dispositivos y haga clic en Agregar dispositivo.



## 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 jumhost -

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

Paso 3. Configure los parámetros correctos para cada protocolo de administración y haga clic en Agregar y cerrar.

### Terminal

Connection method:

SSH  Telnet

Allow connecting using obsolete/insecure SSH algorithms

Use SSH Tunneling when using this device as a jumhost

Username

admin

Password

\*\*\*\*\*

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

Port

22

Enable Password ?

Paso 4. Una vez agregado, el dispositivo debe mostrarse en la lista de dispositivos; puede activarse o desactivarse para el acceso remoto.

Remote Automation Development  
Cisco RADKit Service

Domain: PROD Serial: k331-0evx-s94g

CONNECTED

+ Add Device

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

## Autorizar usuarios remotos

Paso 1. Para otorgar acceso de usuario a los Dispositivos configurados en el Servicio RADKit, vaya a Usuarios Remotos y seleccione Agregar Usuarios.

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

Paso 2. Configure los detalles del usuario:

- Dirección de correo
- Nombre completo (opcional)
- Active el usuario.
- Especifique si la activación debe controlarse manualmente o establezca un intervalo de tiempo para conceder acceso a ese usuario.

## 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

Paso 3. Seleccione Agregar y cerrar.

## Cliente RADkit (TAC)

### Inicio de sesión

Paso 1. En el PC cliente, navegue hasta Aplicaciones y localice el cliente RADkit.

Paso 2. Cree una instancia de cliente con su login de 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")
```

Paso 3. Acepte la solicitud de autorización de SSO que se abre automáticamente en su navegador.



### 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

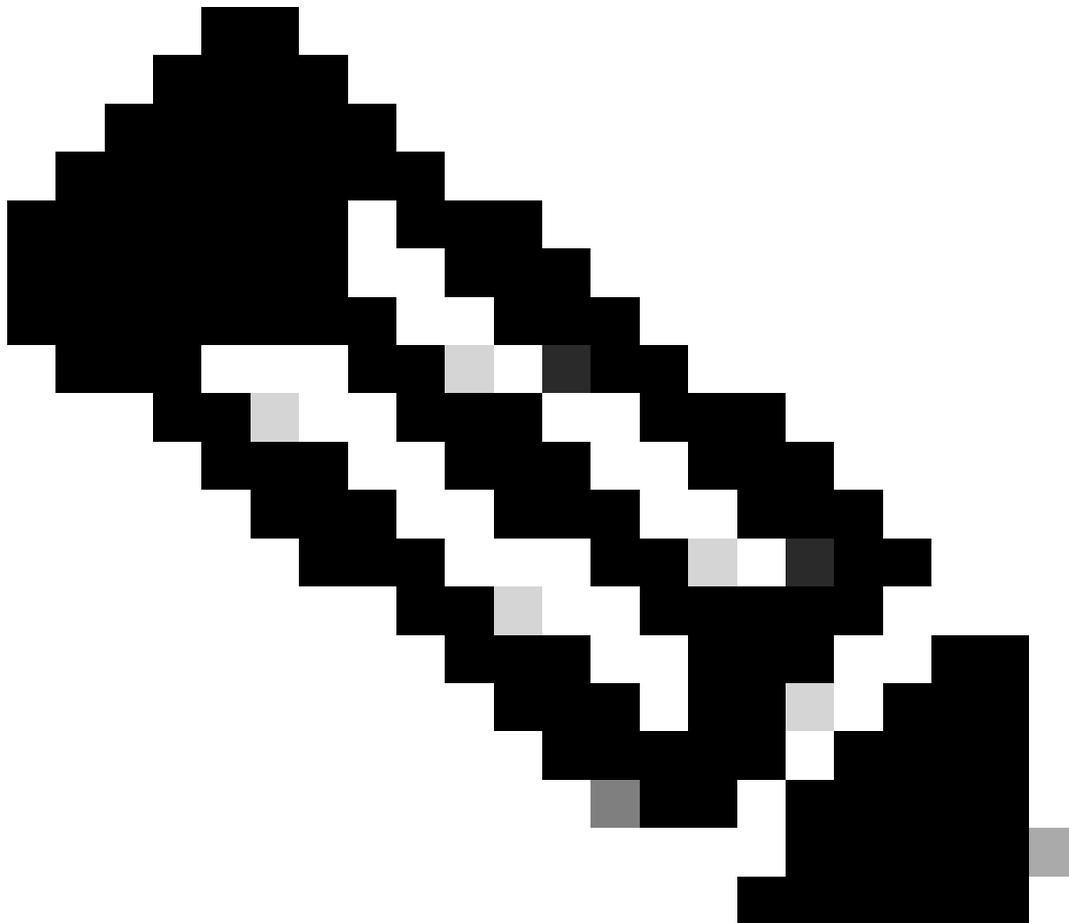
Paso 4. Cree una instancia de servicio utilizando el número de serie generado por el usuario desde la etapa RADKit Service - Onboarding.

<#root>

>>>

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

```
>>> service = client.service("k331-0evx-s94g")
05:16:36.349Z INFO | internal | Connecting to forwarder [uri='wss://prod.radkit-cloud.cisco.com/forwarder-2/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 es una variable que puede ser cualquier cosa.

Paso 5. Compruebe los dispositivos disponibles para el acceso.

```
<#root>
```

```
>>>
```

```
service.inventory
```

```
>>>
>>> service.inventory
<radkit_client.sync.device.DeviceDict object at 0x10d7728e0>
name          host          device_type  Terminal  Netconf  Swagger  HTTP  description  failed
-----
cesavilacum  10.88.247.197 UNKNOWN    True      False    False    True  -----
False
```

Para actualizar la lista de inventario, utilice el comando `update_Inventory`.

```
<#root>
```

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

## Acceso SSH

Paso 1. Crear un objeto de la lista de inventario.

```
<#root>
```

```
>>> cucm = service.inventory['cesavilacum']
```

```
>>> service.inventory
<radkit_client.sync.device.DeviceDict object at 0x10d7728e0>
name          host          device_type  Terminal  Netconf  Swagger  HTTP  description  failed
-----
cesavilacum  10.88.247.197 UNKNOWN    True      False    False    True  -----
False
Untouched inventory from service k331-0evx-s94g.
>>>
>>> cucm = service.inventory["cesavilacum"]
```

Paso 2. Inicie la sesión SSH con el comando interactivo.

```
<#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 ...

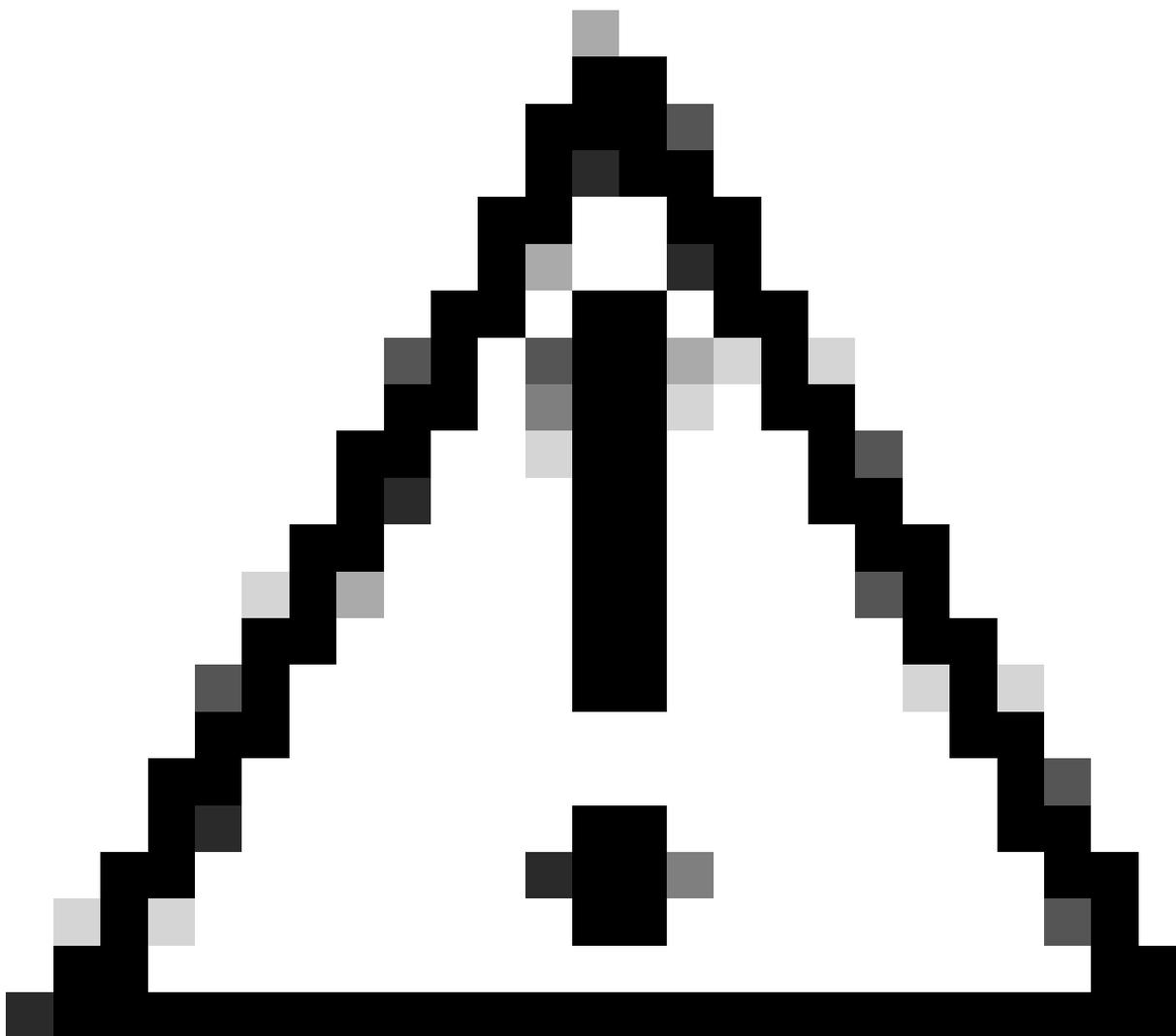
Welcome to the Platform Command Line Interface

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:|
```

Paso 3. Ahora puede administrar el dispositivo normalmente.

---



## Precaución:

- Tenga siempre presente nuestra responsabilidad cuando trabaje en un entorno de usuario.
- RADKit debe utilizarse como herramienta de recopilación de datos.
- Nunca realice ningún cambio sin el permiso del usuario.
- Documente todas sus conclusiones en las notas del caso.

## Acceso a GUI

- Proxy HTTP

Paso 1. Asegúrese de que las credenciales HTTP se agregan al servicio RADKit en la configuración del dispositivo.

Paso 2. Inicie el proxy HTTP en el cliente Radkit y defina el puerto local utilizado para conectarse 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
>>> █
```

Paso 3. En el explorador Web, vaya a <https://localhost:4001> y seleccione el servicio al que desea conectarse.



The screenshot shows a web browser window with the address bar set to 'localhost:4001'. The page content includes the Cisco logo and the text 'RADKit Client Proxy'. The main heading is 'Services'. Below this, there is a prompt: 'Choose any of the following services:'. Two service options are listed: '1. r7nz-6n40-x3su' and '2. ckt7-tv6c-uale'. The first option is highlighted with a red rectangular box.

Paso 4. Haga clic en la opción Ir a la página web en el dispositivo correcto para conectarse a su

página web.

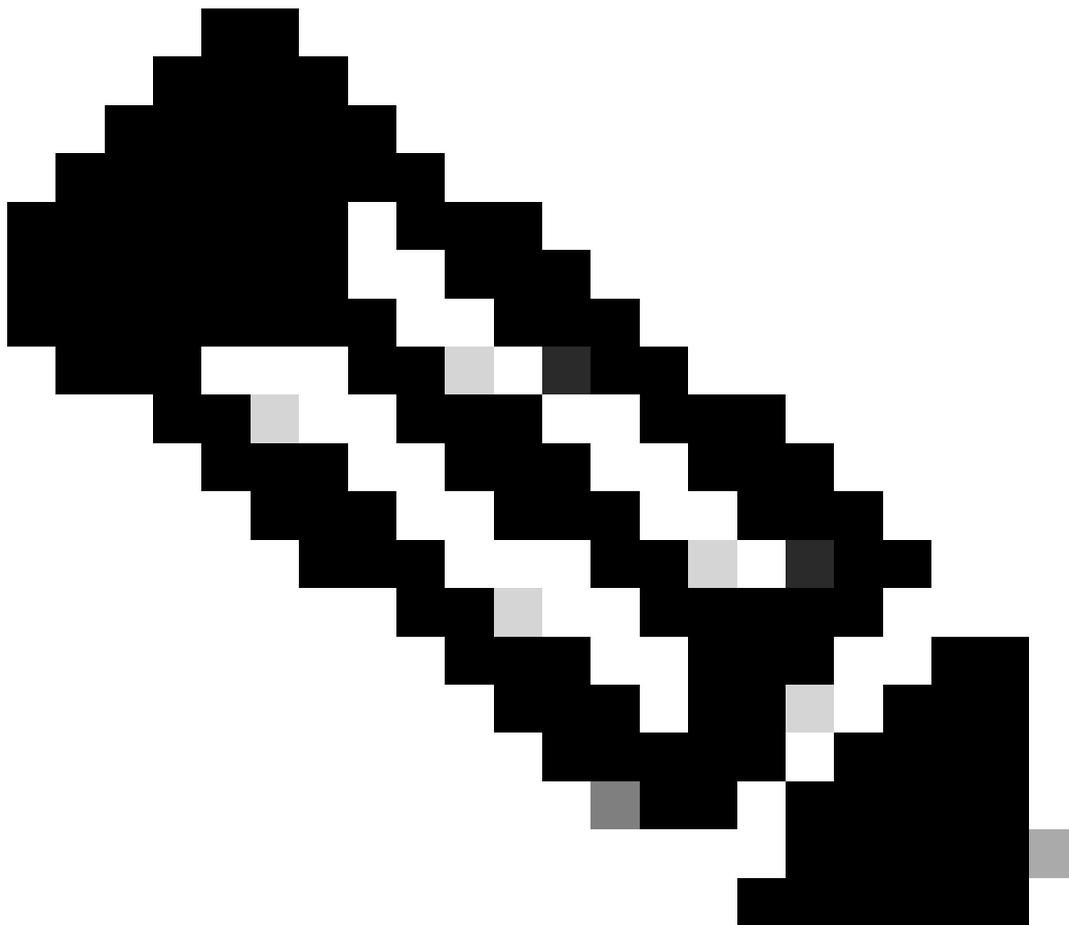
localhost:4001/service/r7nz-6n40-x3su

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

RADKit Client Proxy

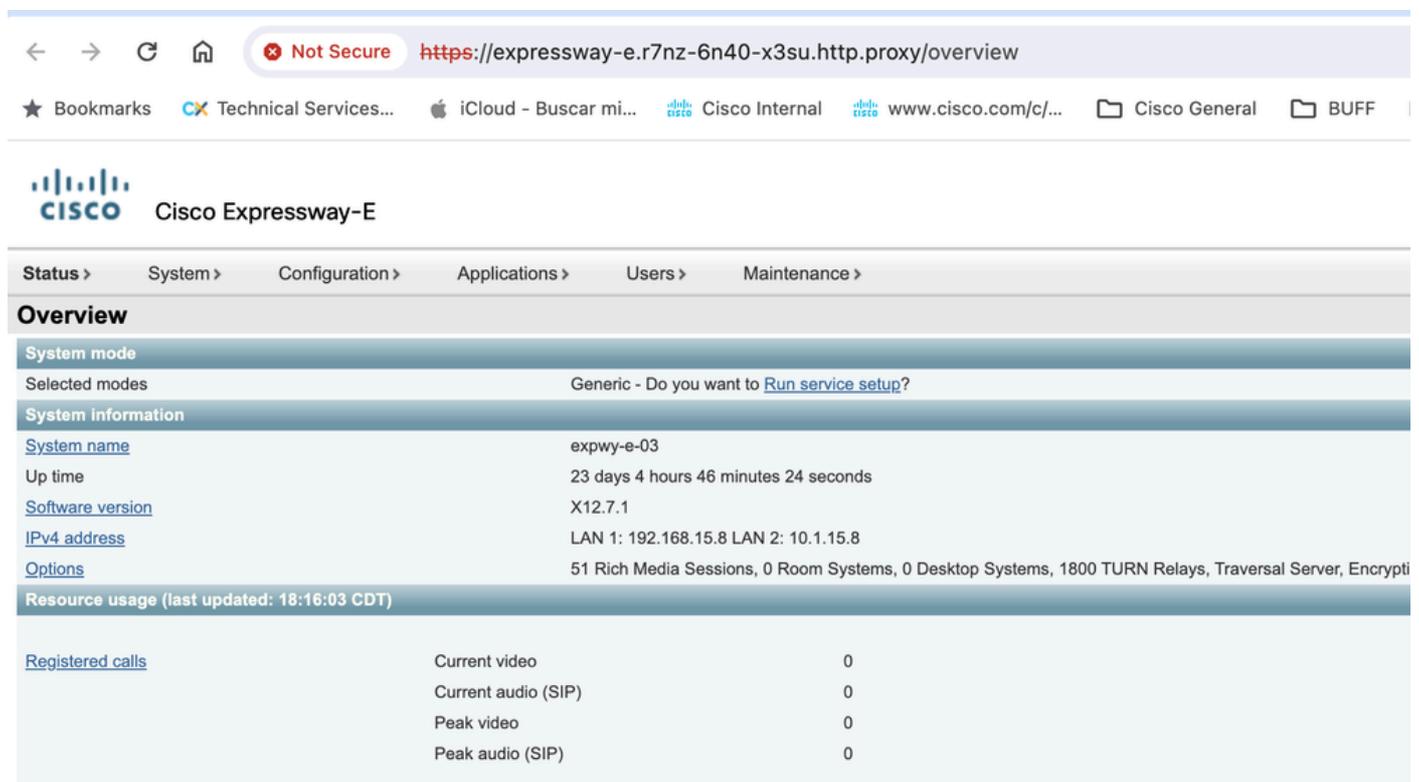
# Service ID: r7nz-6n40-x3su

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



Nota: La primera vez que se configura el proxy HTTP en un cliente RADKit, se recomienda hacer clic en la opción Reset for each Devices (Restablecer para cada dispositivo) antes de intentar abrir la página web Device (Dispositivo).

Paso 5. Se muestra la página Web.



The screenshot shows a web browser window with the URL `https://expressway-e.r7nz-6n40-x3su.http.proxy/overview`. The page title is "Cisco Expressway-E". The navigation menu includes "Status", "System", "Configuration", "Applications", "Users", and "Maintenance". The "Overview" section is active, displaying system information:

- 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

- Reenvío de puertos

Paso 1. Verifique los puertos TCP Forwarded configurados para el dispositivo.

```
<#root>
```

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

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

Paso 2. Configure un puerto local que se asignará al puerto de destino del dispositivo; debe utilizar el puerto local para acceder a la GUI del dispositivo.

```
<#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
-----
```

Paso 3. Abra el navegador y escriba la URL con el puerto configurado en el Paso 2:  
<https://localhost:8443>.

Ahora se puede acceder a la GUI del dispositivo.

← → ↻ 🏠 Not Secure <https://localhost:8443>

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

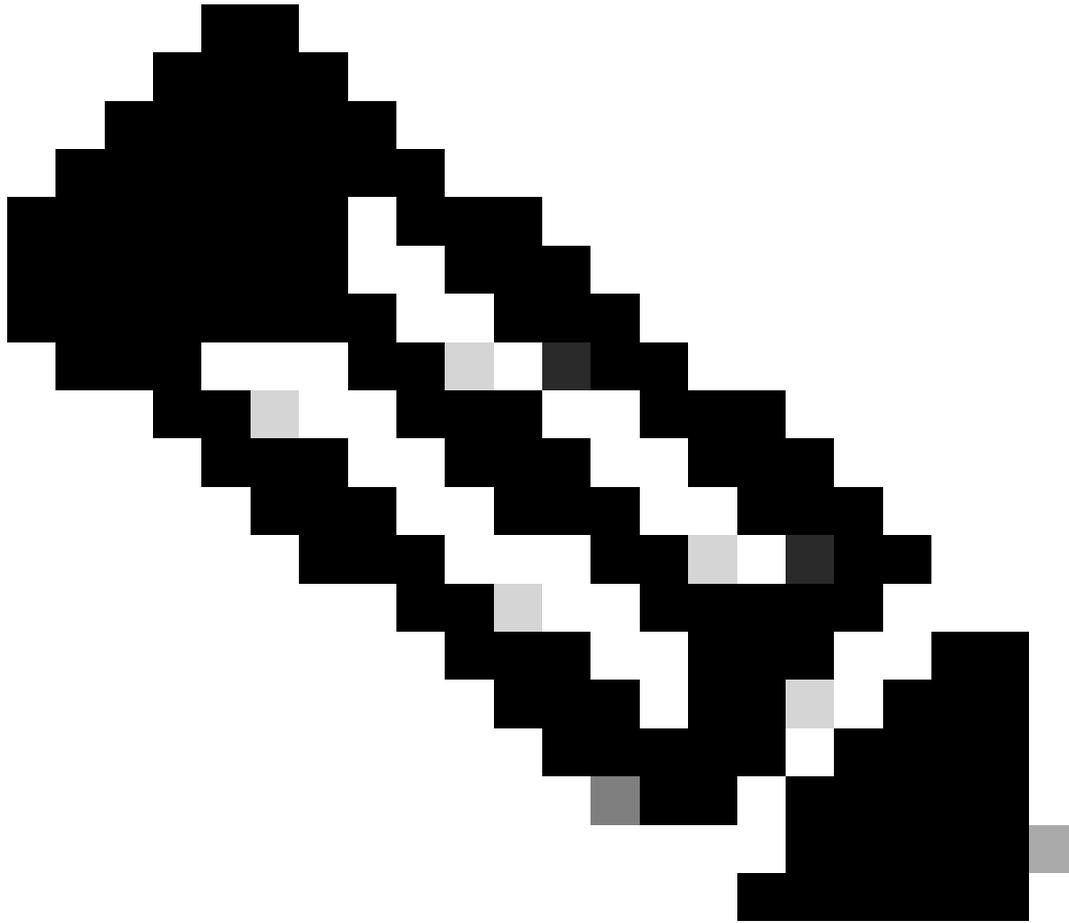
  
**CISCO**

#### 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: Para acceder a la GUI del producto, aún necesita las credenciales para poder iniciar sesión, por lo que se recomienda que el usuario cree una cuenta de usuario de solo lectura para acceder.

---

## Recopilación de registros

- RTMT

Paso 1. Verifique que el puerto 8443 aparezca en los puertos reenviados TCP configurados para el dispositivo.

```
<#root>
```

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

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

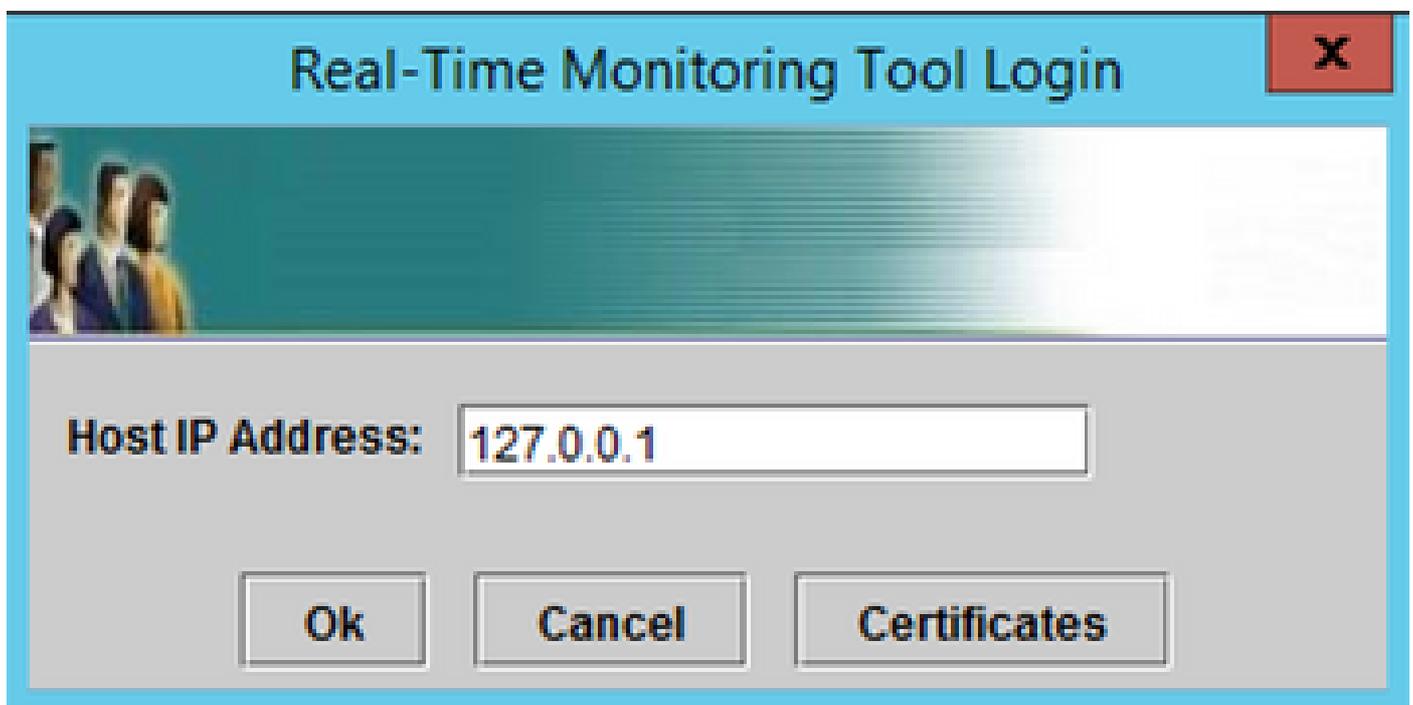
Paso 2. Configure el mismo puerto 8443 como puerto local para asignarlo con el puerto 8443 como puerto de destino del dispositivo.

<#root>

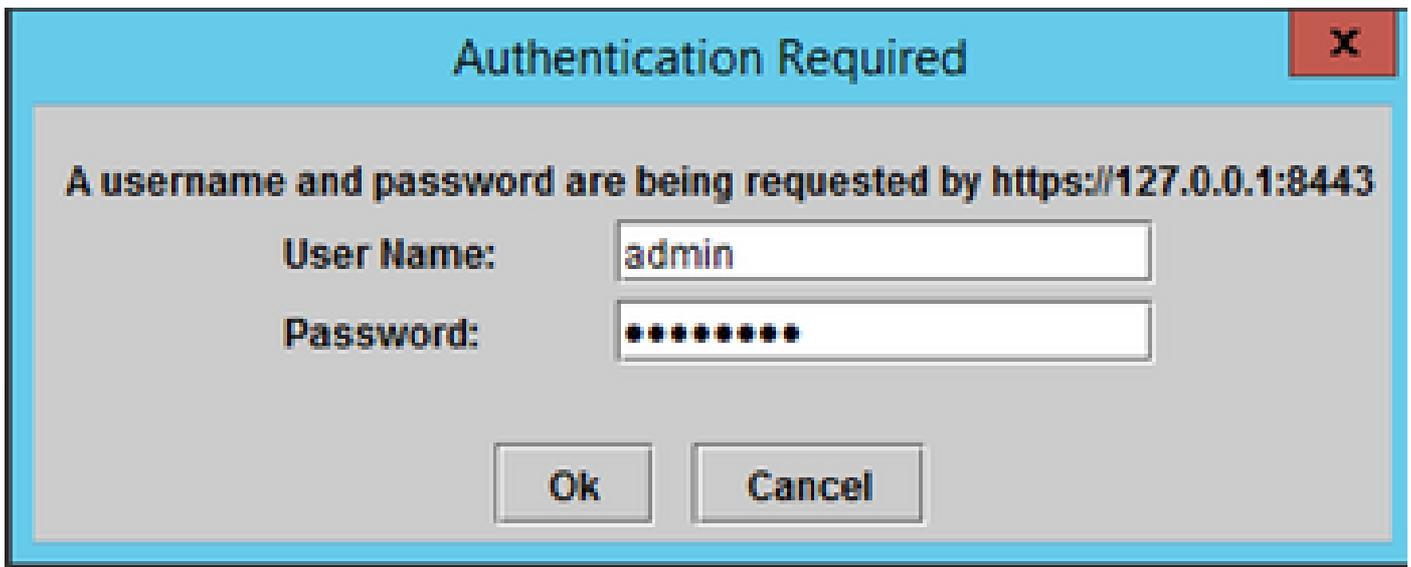
```
>>> cucm.forward_tcp_port(local_port=8443, destination_port=8443)
```

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

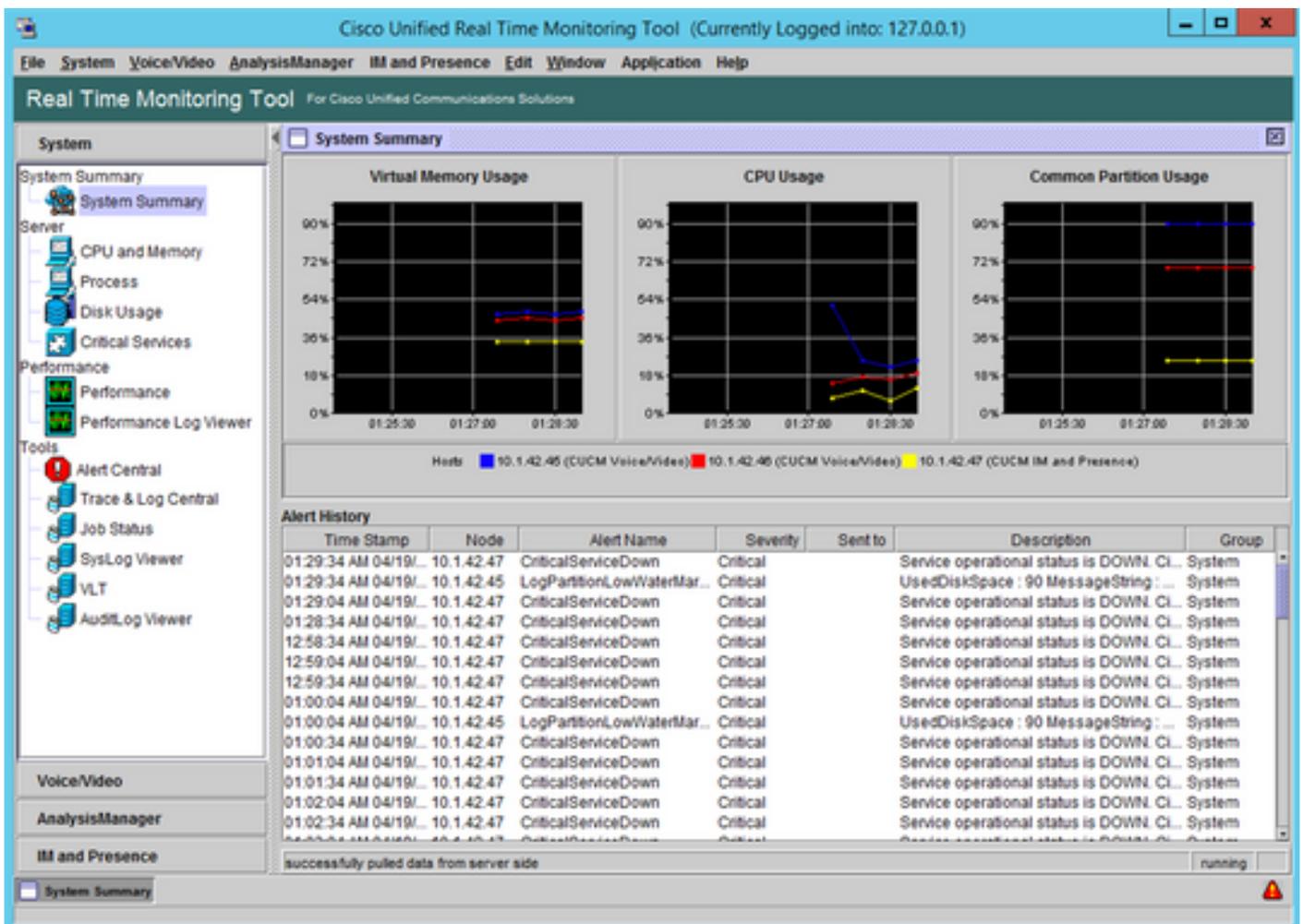
Paso 3. Abra RTMT y escriba 127.0.0.1 en la dirección IP del host, utiliza automáticamente el puerto 8443.



Paso 4. Inicie sesión con las credenciales correctas.



Paso 5. Se muestra RTMT.



Paso 6. Vaya a AnalysisManager en el panel izquierdo.

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**

System Summary

- System Summary

Server

- CPU and Memory
- Process
- Disk Usage
- Critical Services

Performance

- Performance
- Performance Log Viewer

Tools

- Alert Central
- Trace & Log Central
- Job Status
- SysLog Viewer
- VLT
- AuditLog Viewer

Voice/Video

**AnalysisManager**

IM and Presence

System Summary

**System Summary**

**Virtual Memory Usage**

**CPU Usage**

**Common Partition Usage**

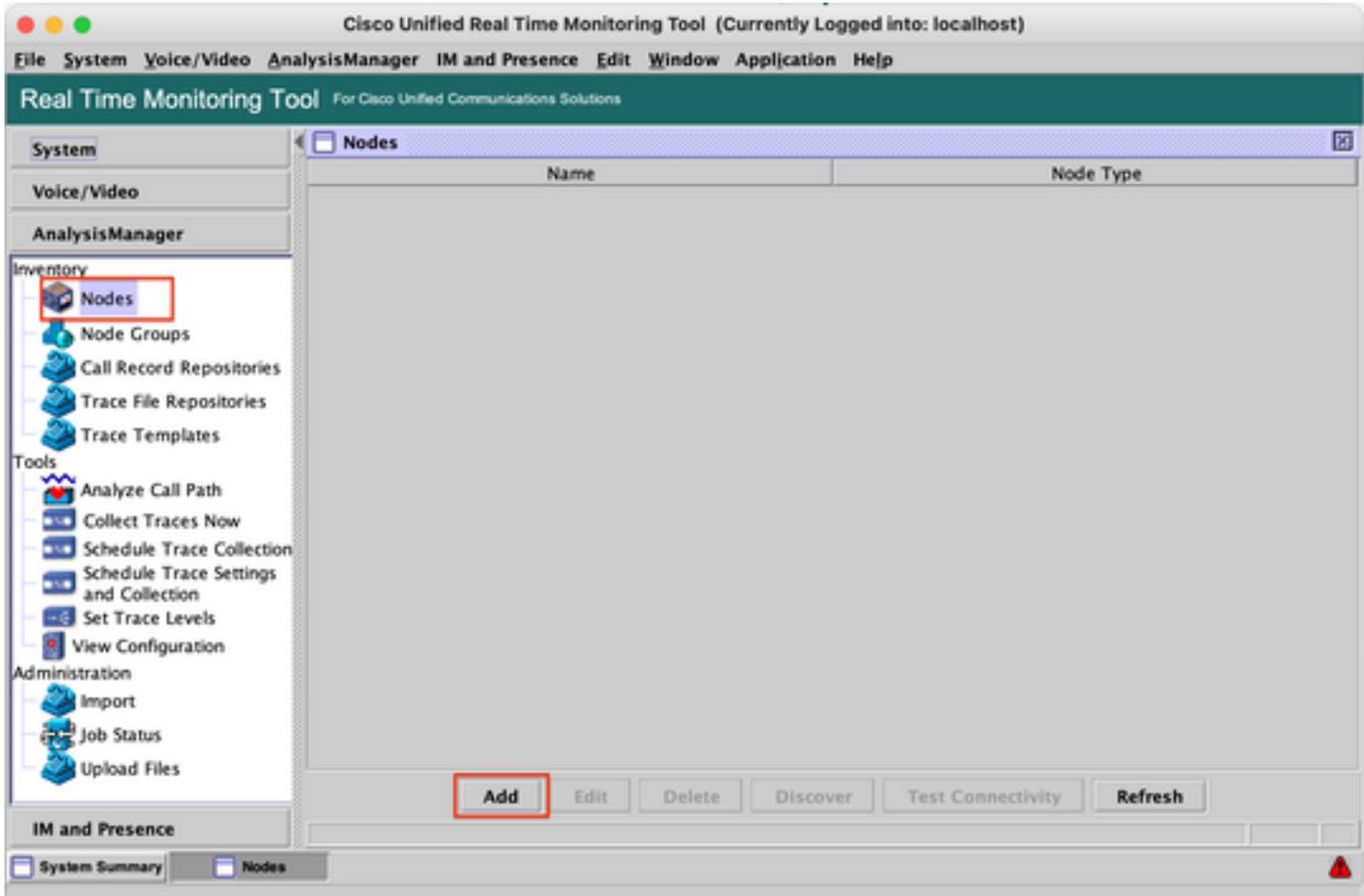
Hosts: 10.1.42.45 (CUCM Voice/Video) 10.1.42.46 (CUCM Voice/Video) 10.1.42.47 (CUCM IM and Presence)

**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 running

Paso 7. Haga clic en Nodes y en Add para configurar los detalles del dispositivo que se agregará mediante localhost y el puerto TCP reenviado.



**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

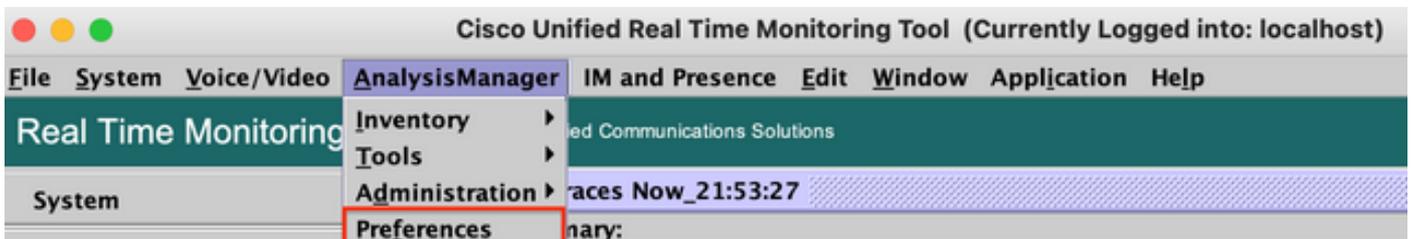
AllNodes

Advanced...

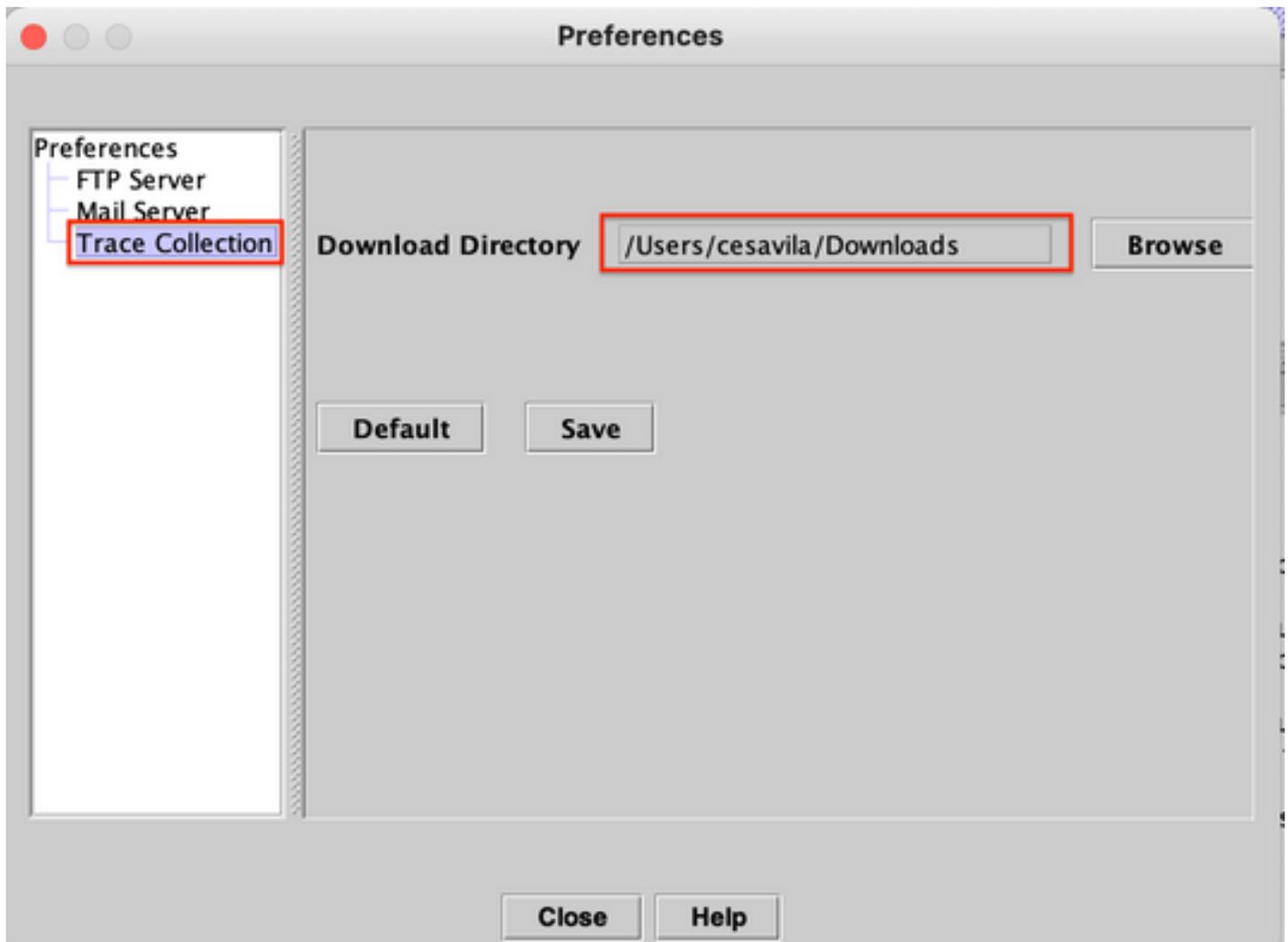
\* Required Fields

Save Cancel

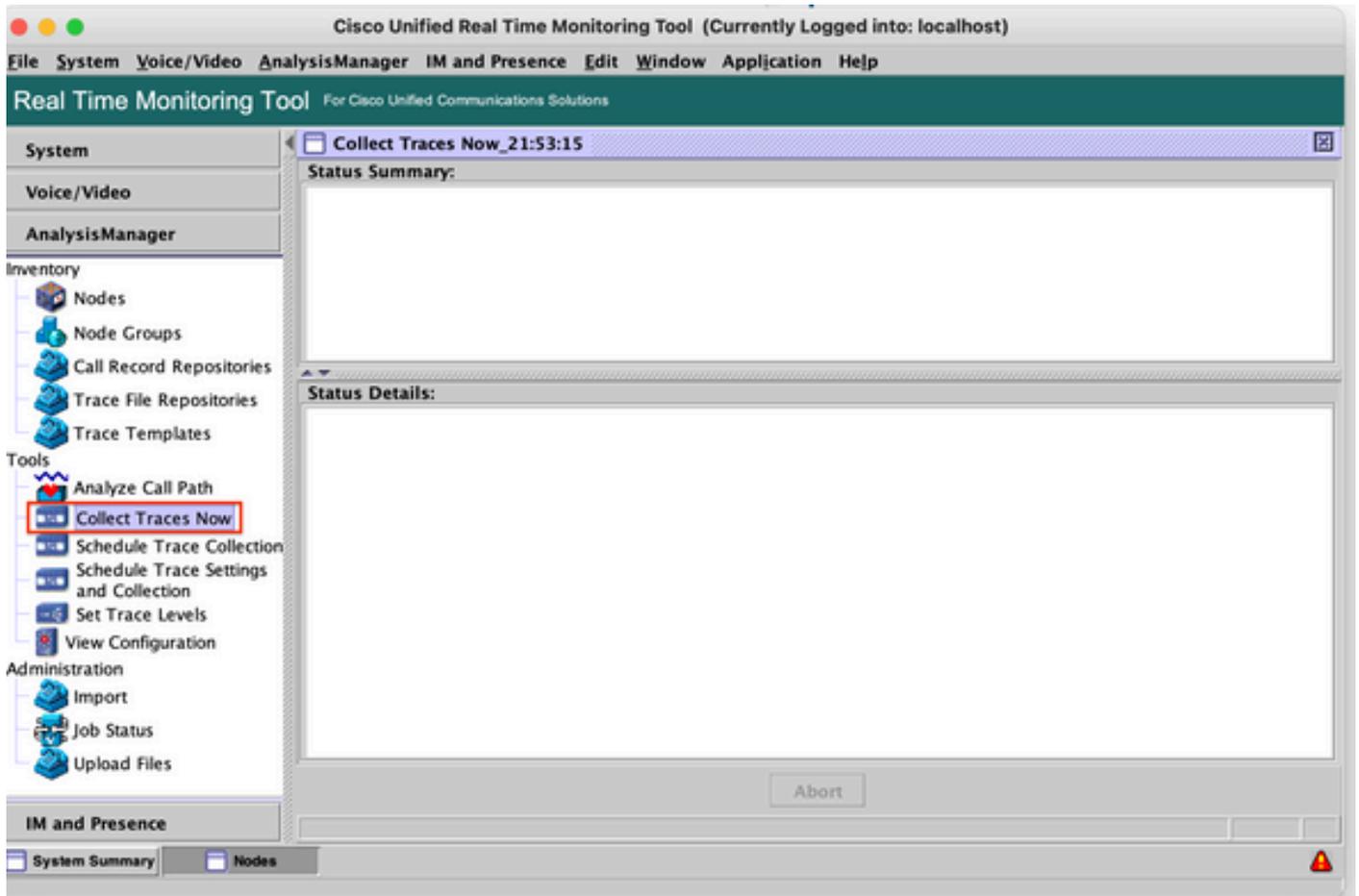
Paso 8. Haga clic en Administrador de análisis en el menú de la parte superior y seleccione Preferencias.



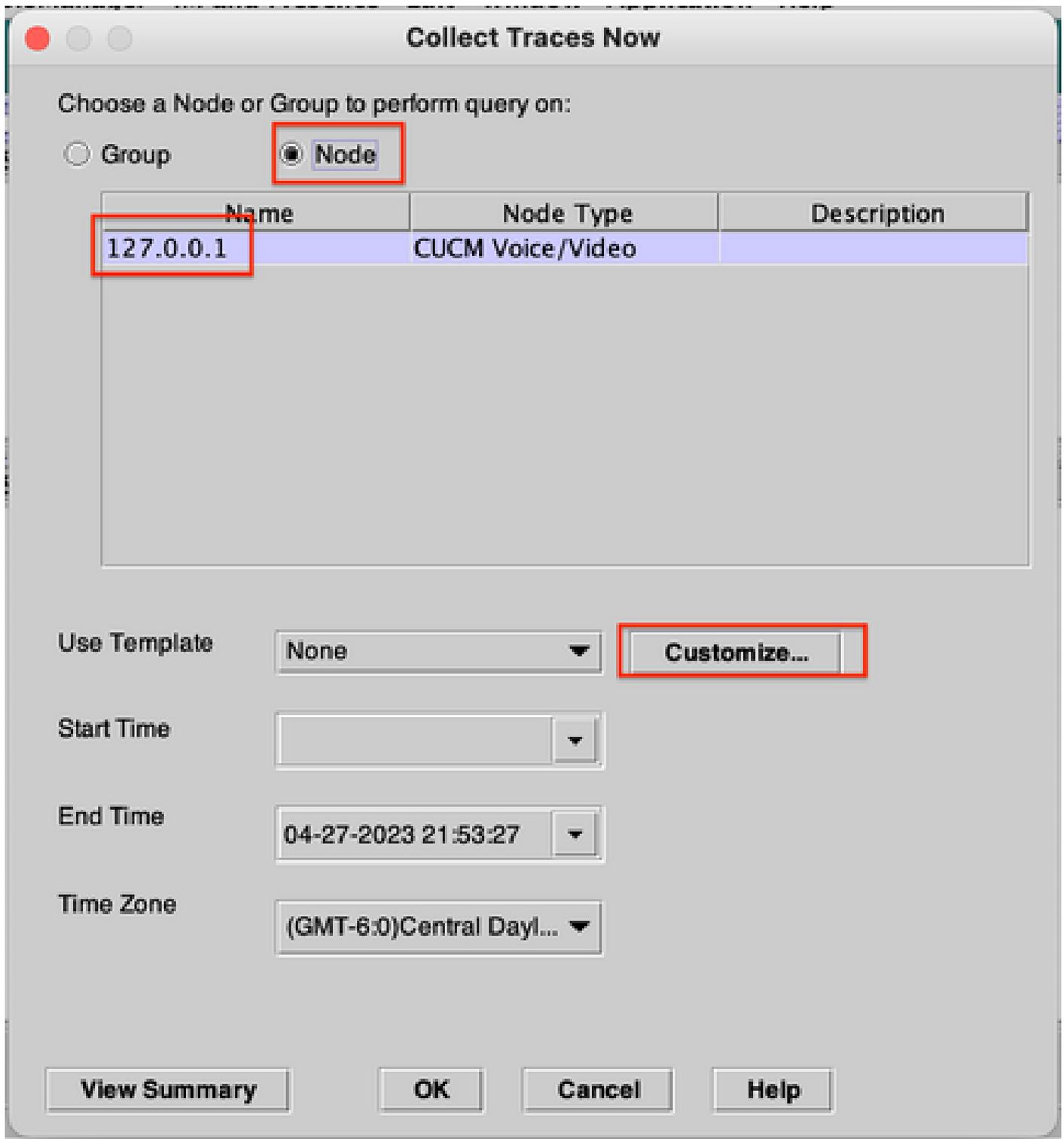
Paso 9. Vaya a Trace Collection y seleccione la carpeta Correct para descargar los registros, haga clic en Save y luego en Close.



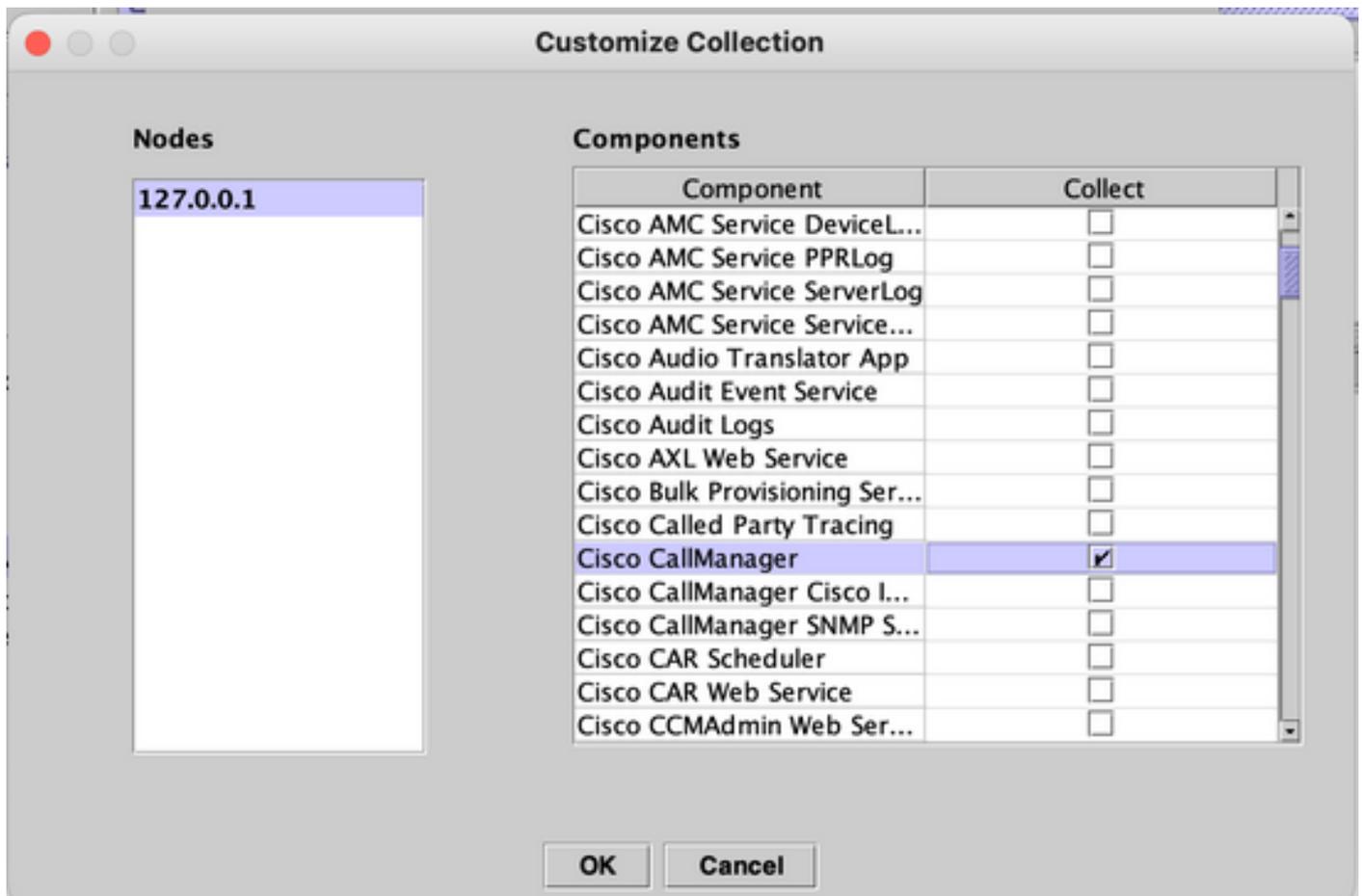
Paso 10. Vaya a Recopilar seguimientos ahora.



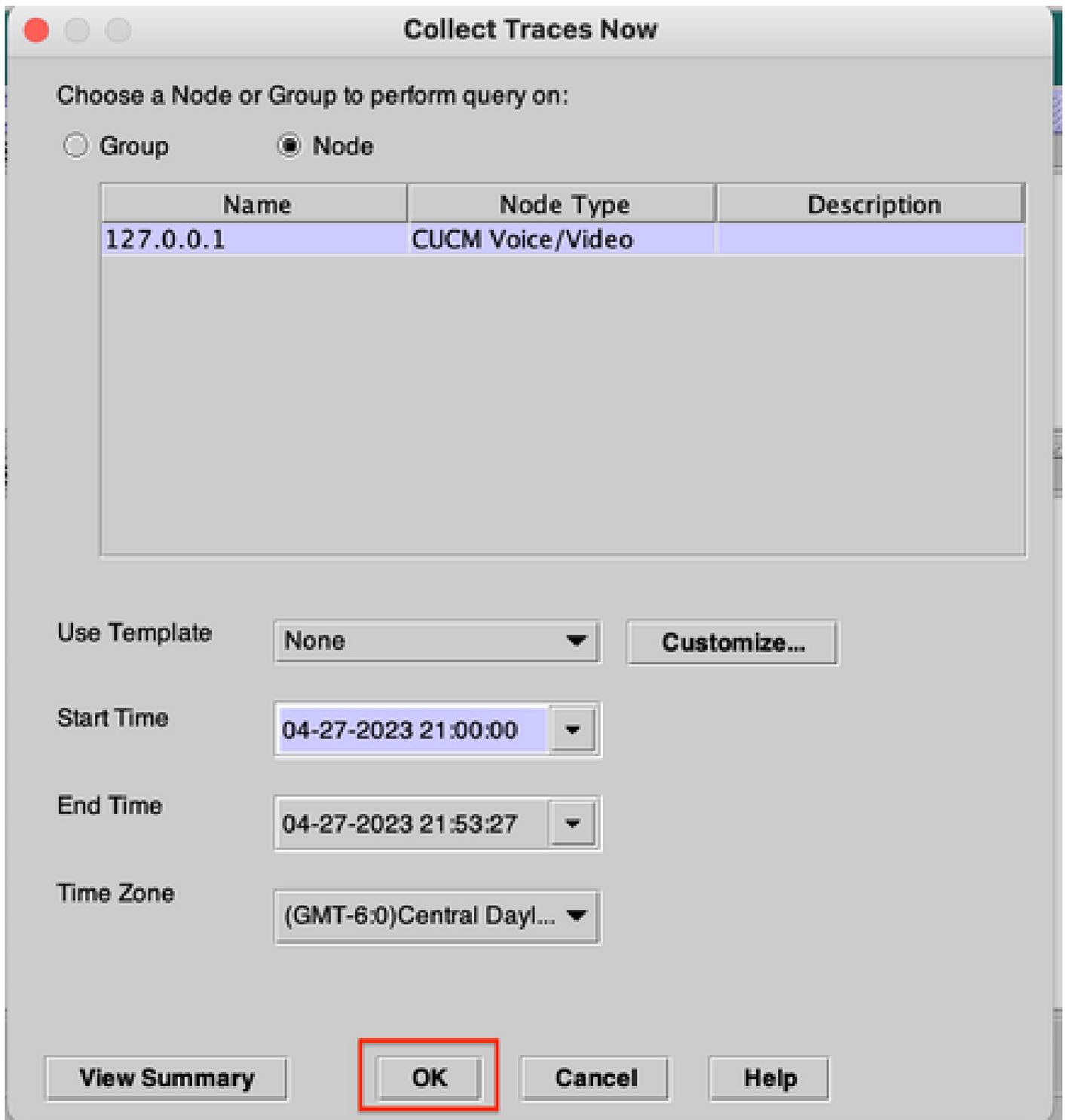
Paso 11. Seleccione la opción Nodo, seleccione el dispositivo agregado en el Paso 7 y haga clic en Personalizar.



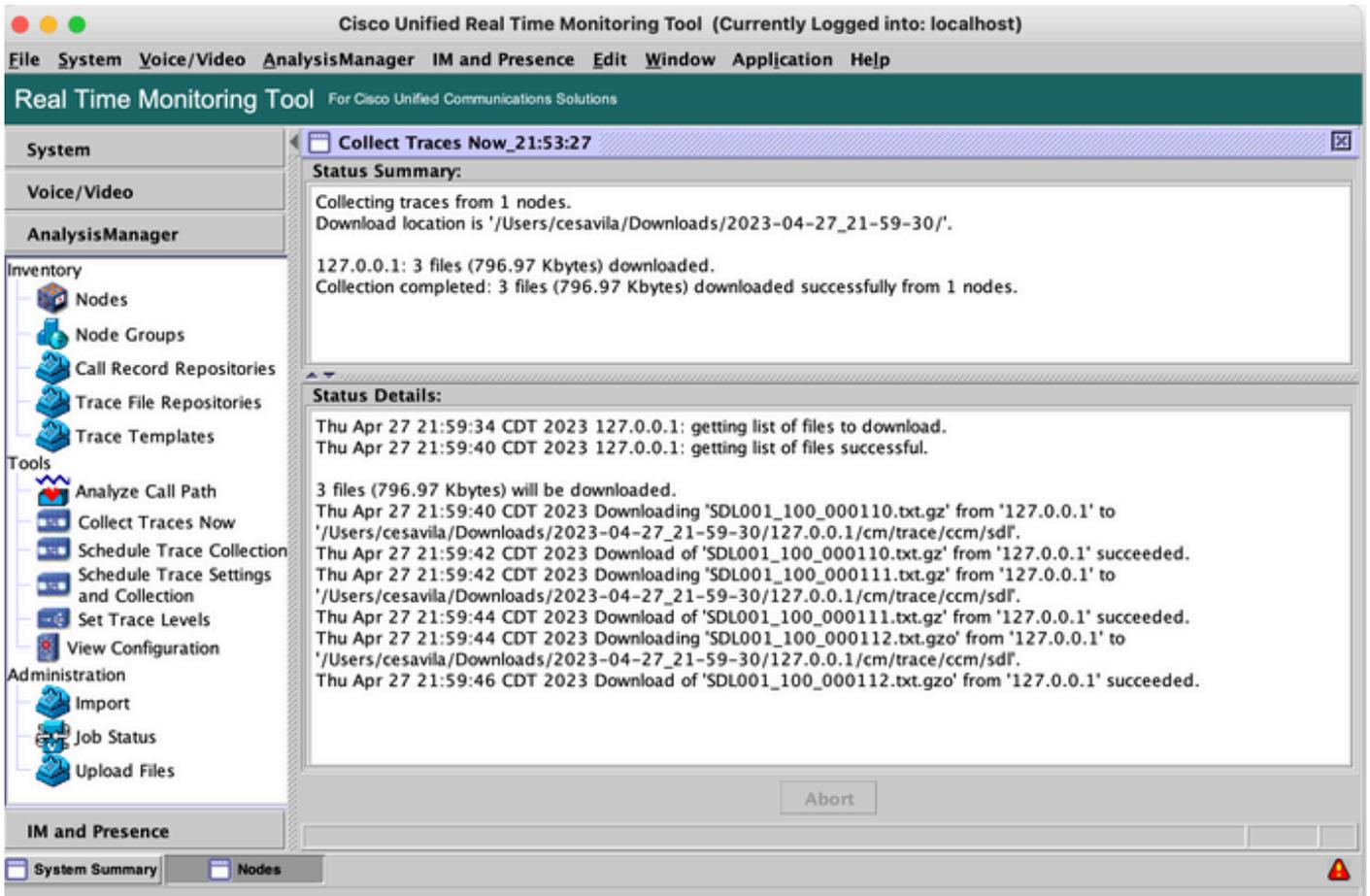
Paso 12. Seleccione los registros que se recopilarán del dispositivo y haga clic en Aceptar.



Paso 13. Por último, seleccione Hora de inicio y Hora de finalización de los registros que se van a recopilar y haga clic en Aceptar.



Paso 14. Los archivos se descargan en el equipo local (RADKit Client PC) correctamente.



- API SOAP

CUCM admite actualmente la API SOAP. Además, Swagger es compatible con CMS, Expressway, CVP, etc.

Paso 1. Asegúrese de que las credenciales HTTP se agregan al servicio RADKit en la configuración del dispositivo.

Paso 2. Ejecute el comando HTTP Post en el cliente RADKit, especifique la ruta de acceso del recurso, solicite el cuerpo con los parámetros y encabezados necesarios.

```
>>>
... r = cucm.http_post('/logcollectionsevice2/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: La opción de postprocesadores 'cucm-extract' se utiliza para quitar los encabezados de respuesta HTTP para poder guardar el registro en un archivo.

```
>>> r
[SUCCESS] HttpResponse(device_name='cucmsiteb', method='POST', url='/logcollectionsservice2/services/LogCollectionPortTypeService', status_code=200)
-----
identity      cesavila@cisco.com
service_id    ckt7-tv6c-uale
device_name   cucmsiteb
method        POST
url           /logcollectionsservice2/services/LogCollectionPortTypeService
status_code   200 OK
content       b'\x1f\x8b\x08\x00\x00\x00\x00\x00\x04\x03\xd4[\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...'
-----
```

Paso 3. Guarde el contenido en un archivo para que el archivo de seguimiento se guarde en el equipo local.

<#root>

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

## Casos prácticos de RADKit

Como se ha destacado, RADKit proporciona una conexión segura a los dispositivos de red, incluidos los servidores de colaboración, sin necesidad de estar en un webex. La idea es simplificar algunos de los retos relacionados con la recopilación de datos proporcionando acceso a demanda a los dispositivos necesarios.

Hablando específicamente sobre las implementaciones de colaboración, RADKit actualmente puede ser muy útil para una variedad de problemas tales como:

- Problemas de replicación de BD.
- Procedimientos de regeneración de certificados.
- Comprobación del estado del sistema.
- Validación de la configuración en GUI/CLI.
- Recopilación de registros a través de la interfaz web (por ejemplo, CER, Expressway, CIMC, etc.).
- Registros de depuración mediante CLI en gateways de voz.

## Información Relacionada

- RADKit Página principal <https://radkit.cisco.com/>
- Página de soporte externo de RADKit <https://community.cisco.com/t5/radkit-discussions/bd-p/disc-radkit>

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).