

Configurar o RADKit em um ambiente de colaboração

Contents

[Introdução](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Terminologia](#)

[Arquitetura RADKit](#)

[Instalação RADKit](#)

[Serviço RADKit \(lado do usuário\)](#)

[Integração](#)

[Adicionar dispositivos](#)

[Autorizar usuários remotos](#)

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

[Login](#)

[Acesso SSH](#)

[Acesso à GUI](#)

[Proxy HTTP](#)

[Encaminhamento de portas](#)

[Coleta de logs](#)

[RTMT](#)

[API SOAP](#)

[Casos de uso de RADKit](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve as etapas para configurar o RADKit e mostra a configuração necessária para iniciar o uso dele com os produtos de colaboração.

Requisitos

A Cisco recomenda que você tenha conhecimento sobre estes tópicos:

- Conhecimento básico de qualquer produto de colaboração VOS
- Conhecimento básico de acesso CLI/SSH

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Unified Communications Manager 12.5 e 14.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

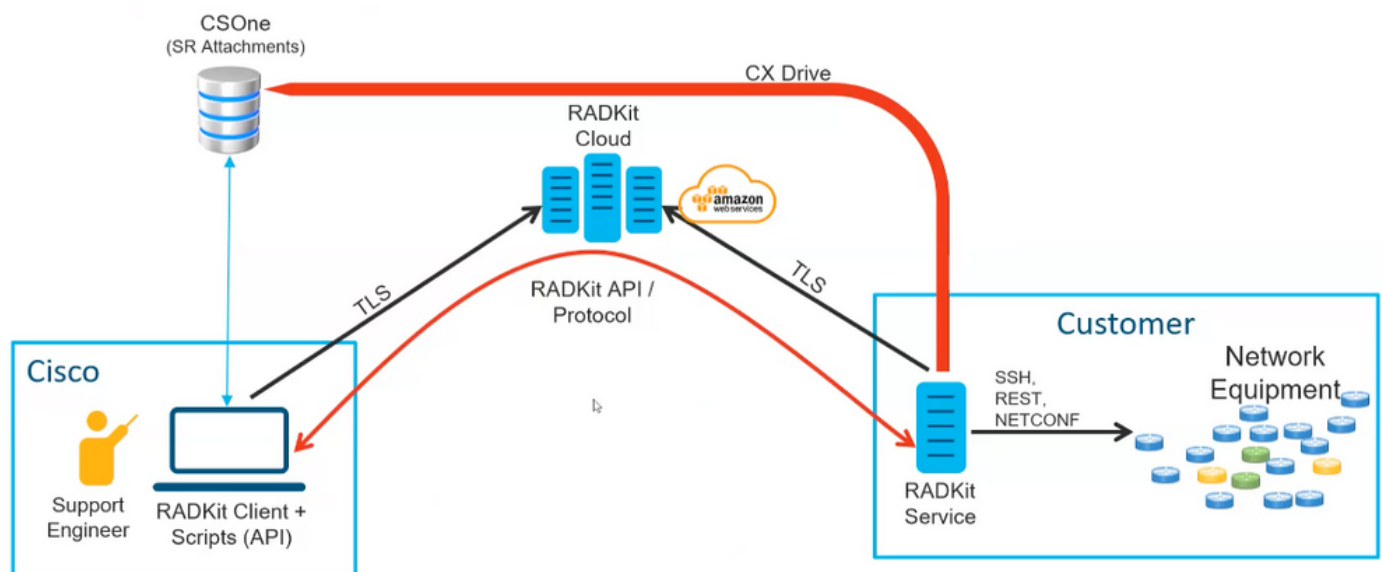
Terminologia

RADKit: É um conector que fornece acesso remoto seguro aos dispositivos do usuário para engenheiros e parceiros do Cisco TAC. Ele suporta vários protocolos para interagir com dispositivos, como SSH ou HTTP/HTTPS.

Serviço RADKit: Este é o lado do servidor. Ele é manipulado e totalmente gerenciado pelo usuário. No lado do servidor, o usuário controla quem pode acessar os dispositivos e por quanto tempo. O Serviço Radkit deve ter conectividade com os dispositivos na rede para fornecer acesso a eles.

Cliente RADKit: Este é o lado do cliente. É o PC usado para se conectar aos dispositivos na rede do usuário.

Arquitetura RADKit



Arquitetura RADKit

Instalação RADKit

Etapa 1. Navegue até <https://radkit.cisco.com> e clique em [Downloads](#), depois vá para a pasta [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/](#)

03-Mar-2023 18:10

-

[release/](#)

04-Apr-2023 11:45

-

Etapa 2. Clique na versão mais recente.

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

-

Etapa 3. Faça o download do arquivo correto dependendo do sistema operacional.

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

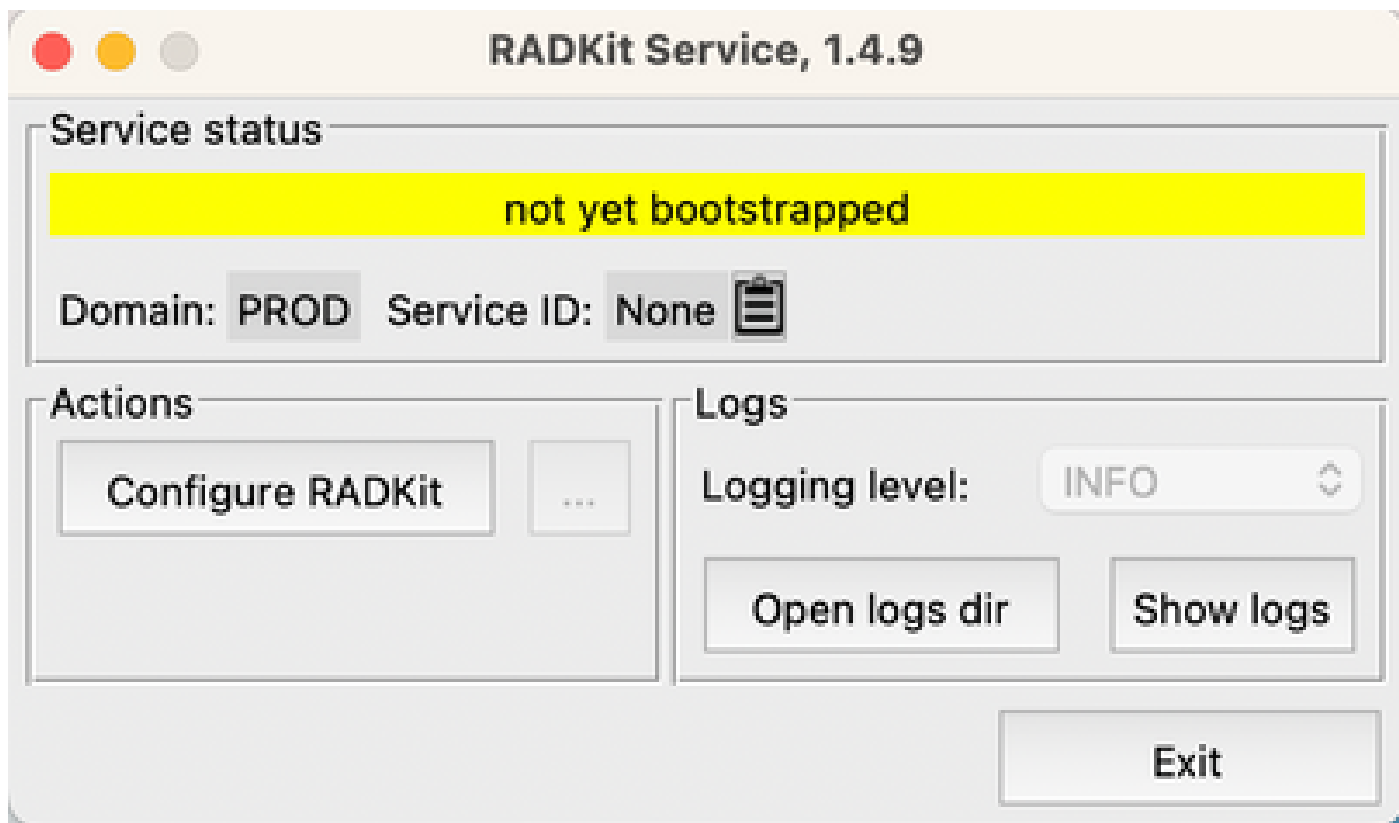
104692424

Etapa 4. Execute o instalador no PC ou no servidor. Como parte da instalação, o Radkit precisa instalar três aplicativos: Serviço Radkit, cliente Radkit e console de rede Radkit.

Serviço RADKit (lado do usuário)

Integração

Etapa 1. Para iniciar a configuração do serviço RADKit, navegue até Applications (Aplicativos) e localize RADKit Service (Serviço RADKit). A primeira vez que você o executa, ele mostra uma mensagem "ainda não inicializado".



Etapa 2. Clique em Configure RADKit, o navegador será exibido automaticamente com o URL <https://localhost:8081/bootstrap>.

- Crie a senha para o usuário superadmin e clique em Enviar.
- Esse nome de usuário e senha de superadmin são solicitados toda vez que o serviço é iniciado ou configurado.

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

Etapa 3. Depois de clicar em Submit, o navegador o redirecionará para <https://localhost:8081/#/connectivity/>.

Em Connectivity > Service Enrollment, há dois métodos de autenticação: Single Sing-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

Etapas 5. Conclua o assistente e conclua as etapas até que ele mostre "Serviço inscrito com nova identidade: xxxx-xxxx-xxxx" e, ao clicar em Close, o serviço será exibido como Connected.



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

Close



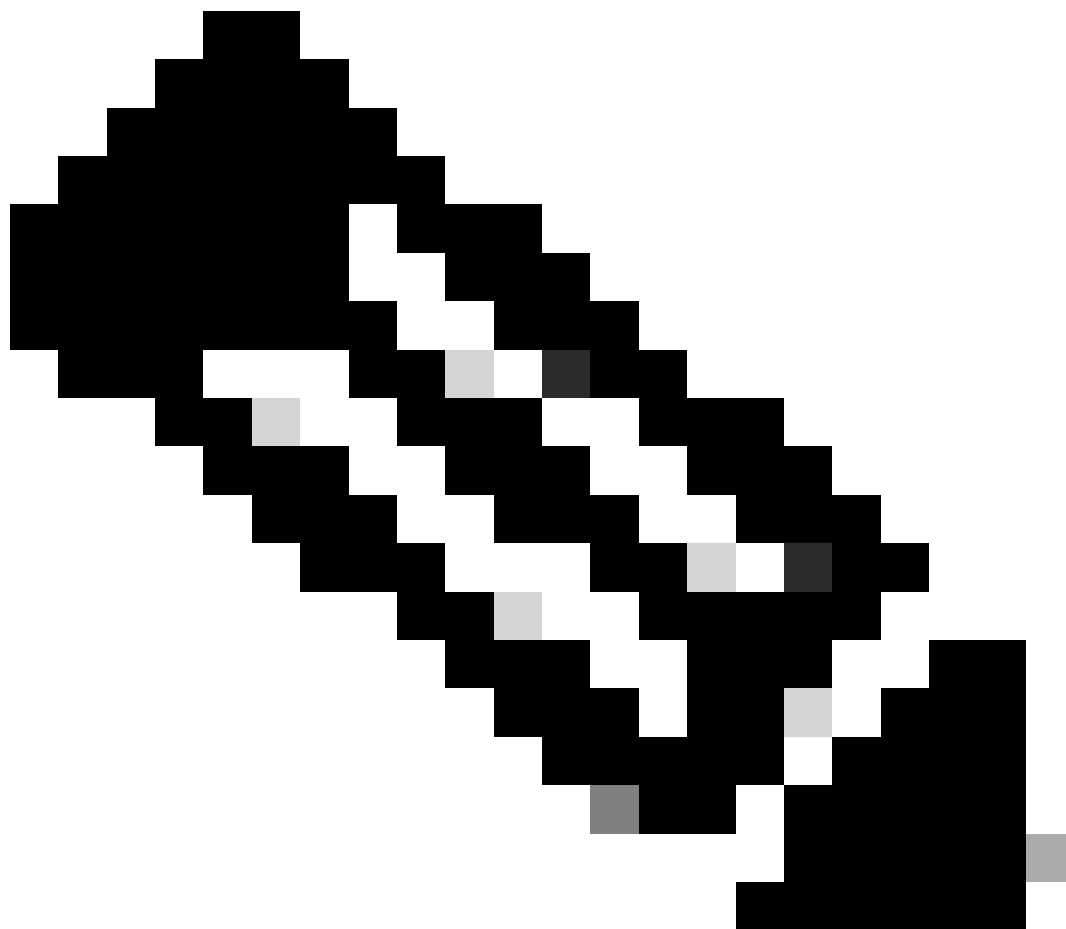
Remote Automation Development
Cisco RADKit Service

Domain: PROD Serial: k331-0evx-s94g

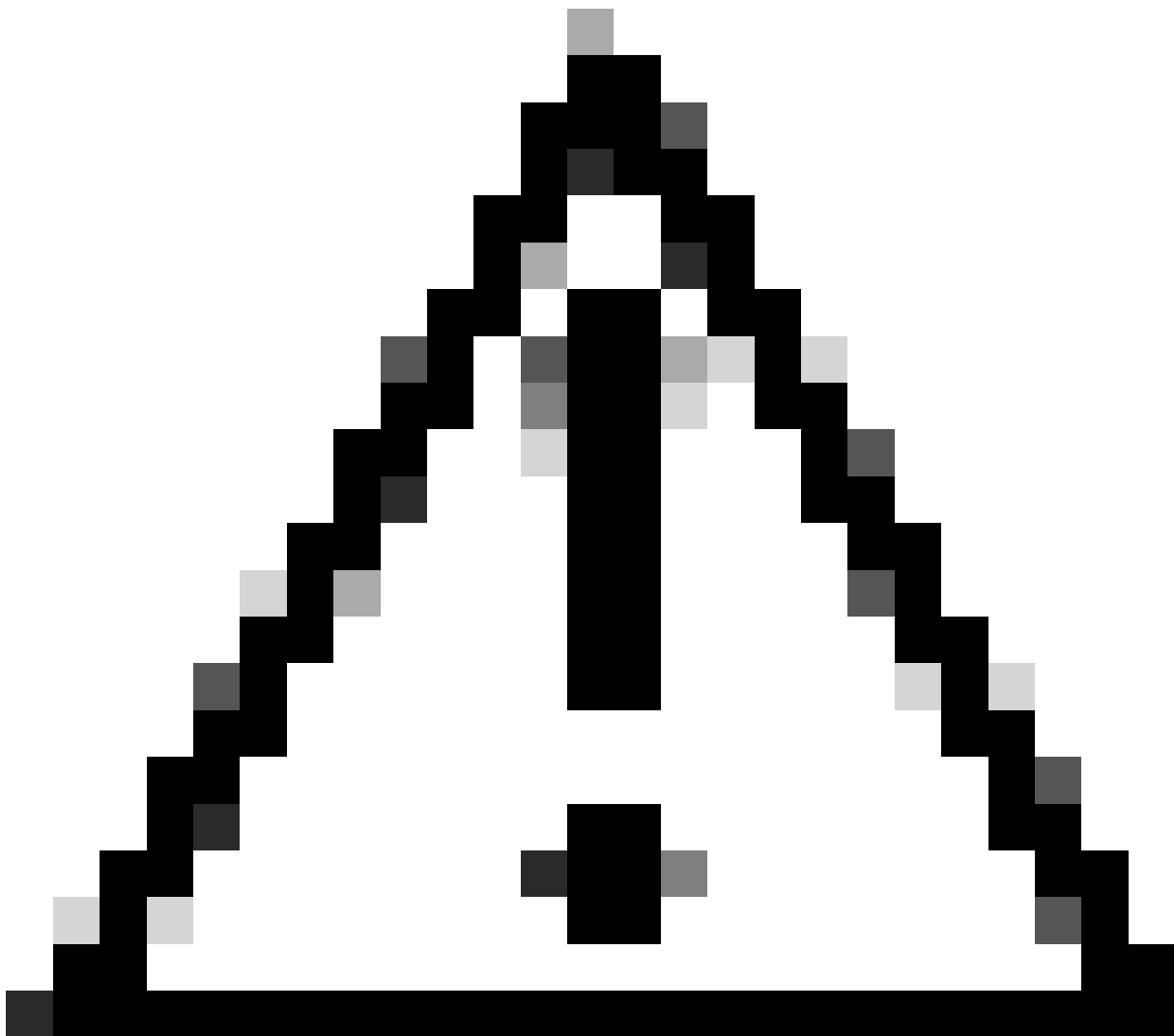


CONNECTED





Note: Uma conta da Cisco é necessária para ativar o Serviço RADKit.

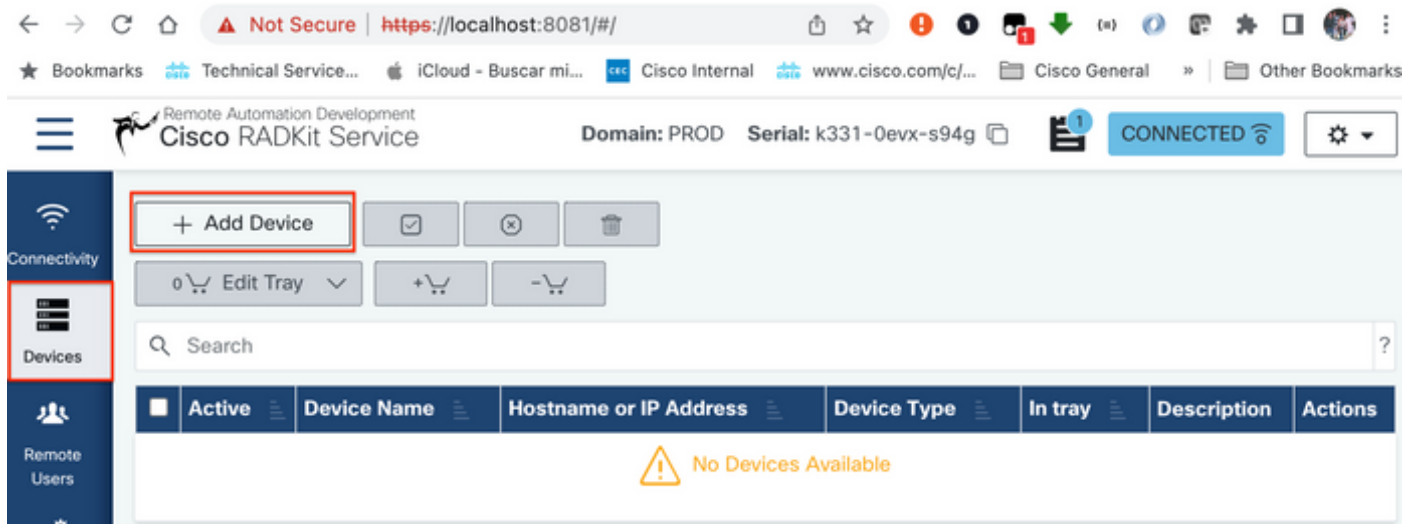


Caution:

- Se o servidor onde o serviço RADKit está sendo executado exigir que um proxy seja definido, além de definir o proxy no próprio servidor/PC, uma variável de ambiente também precisa ser definida para que o serviço RADKit funcione como `RADKIT_CLOUD_CLIENT_PROXY_URL=http://proxy.example.com:80`.

Adicionar dispositivos

Etapa 1. Navegue até Devices e clique em Add Device.



Etapa 2. Você precisa configurar os próximos detalhes:

- Nome de dispositivo
- Endereço IP ou nome de host de gerenciamento
- tipo de dispositivo

Além disso, você deve configurar as portas TCP encaminhadas, que são portas usadas pelo dispositivo que precisam estar acessíveis a partir do cliente RADKit. Neste exemplo, as portas usadas são 443 para acesso à GUI e 8443 para RTMT.

Finalmente, selecione os protocolos de gerenciamento disponíveis, neste 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

Etapa 3. Para cada protocolo de gerenciamento, defina as configurações corretas e clique em 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 ?

Etapa 4. Depois de adicionado, o dispositivo deve ser exibido na lista de dispositivos e pode ser ativado/desativado para acesso 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

Autorizar usuários remotos

Etapa 1. Para conceder ao usuário acesso aos dispositivos configurados no serviço RADKit, vá para Usuários remotos e selecione Adicionar usuários.

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

Etapa 2. Configure os detalhes do usuário:

- Endereço de e-mail
- Nome completo (opcional)
- Ative o usuário.
- Especifique se a Ativação deve ser controlada Manualmente ou defina um período para conceder acesso a esse usuário.

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

Etapa 3. Selecione Add & Close.

Cliente RADkit (lado TAC)

Login

Etapa 1. No PC cliente, navegue até Applications (Aplicativos) e localize RADkit Client.

Etapa 2. Crie uma instância do cliente com seu login SSO.

<#root>

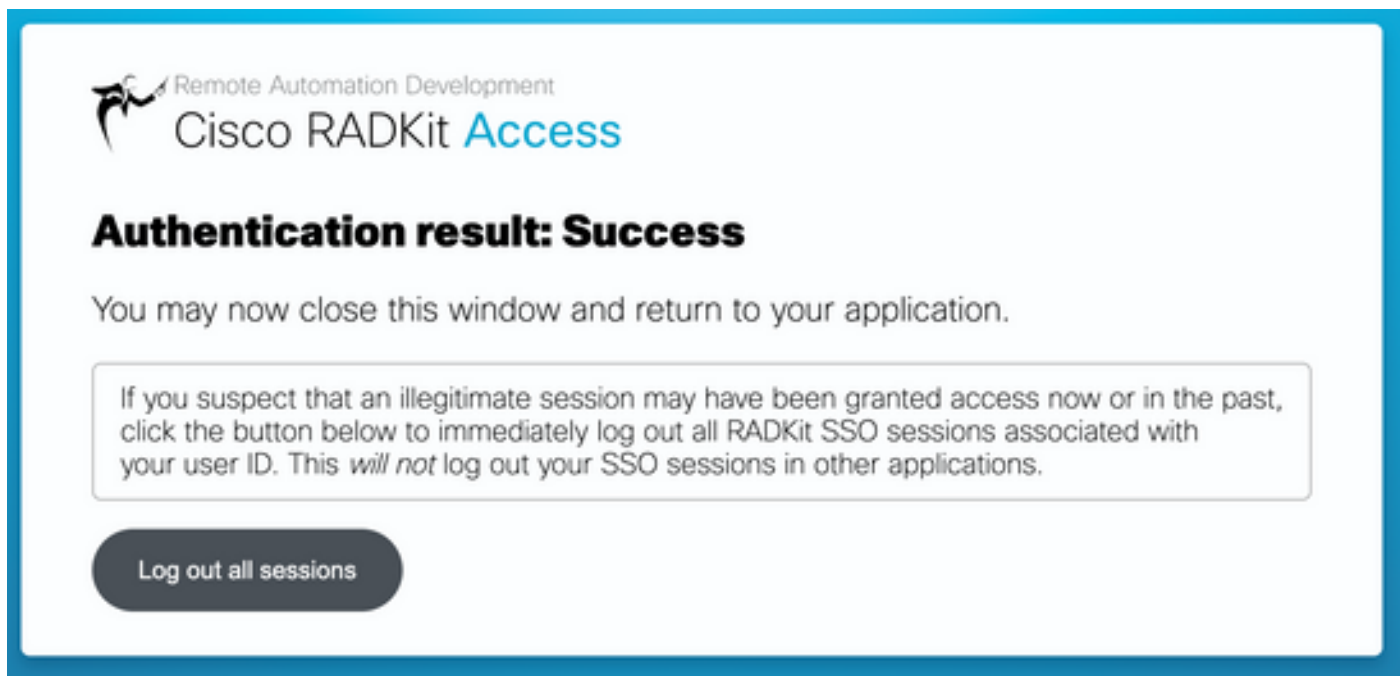
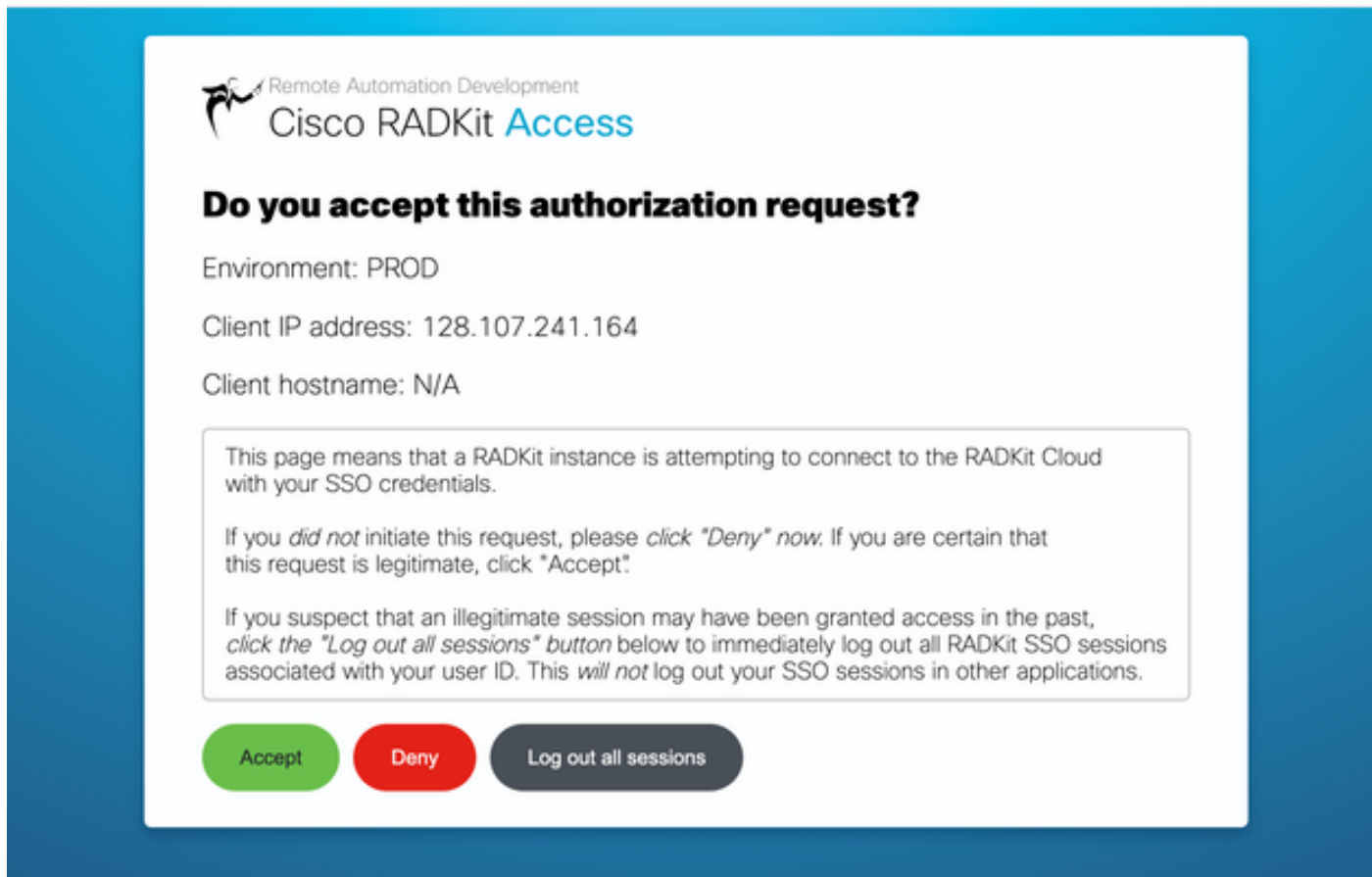
>>>

```
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")
```

Etapa 3. Aceite a Solicitação de Autorização SSO aberta automaticamente em seu navegador.



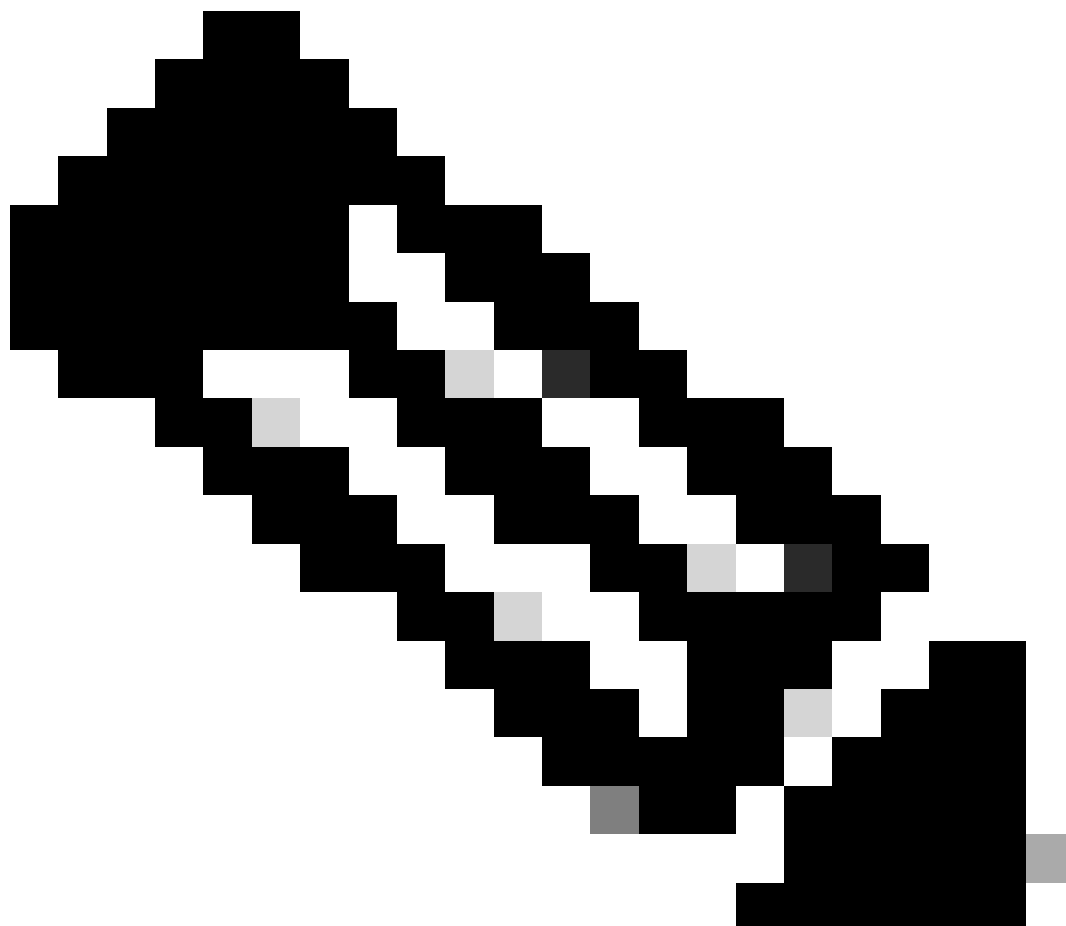

Remote Automation Development
Cisco RADKit Service
Domain: PROD
Serial: k331-0evx-s94g
2
CONNECTED

<#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/']
```



Note: serviço é uma variável que pode ser qualquer coisa.

Etapa 5. Verifique os dispositivos disponíveis para acesso.

<#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
```

Para atualizar a lista de inventário, use o comando `update_inventory`.

<#root>

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

Acesso SSH

Etapa 1. Crie um objeto a partir da lista de inventário.

<#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"]
```

Etapa 2. Inicie a sessão SSH com o comando `interactive`.

<#root>

```
>>> cucm.interactive()
```

```

>>> cucm.interactive()
05:35:23.882Z INFO | internal | starting interactive session (will be closed when detached)
05:35:24.765Z INFO | internal | Session log initialized [filepath='/Users/cesavila/.radkit/session_logs/client/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 ...

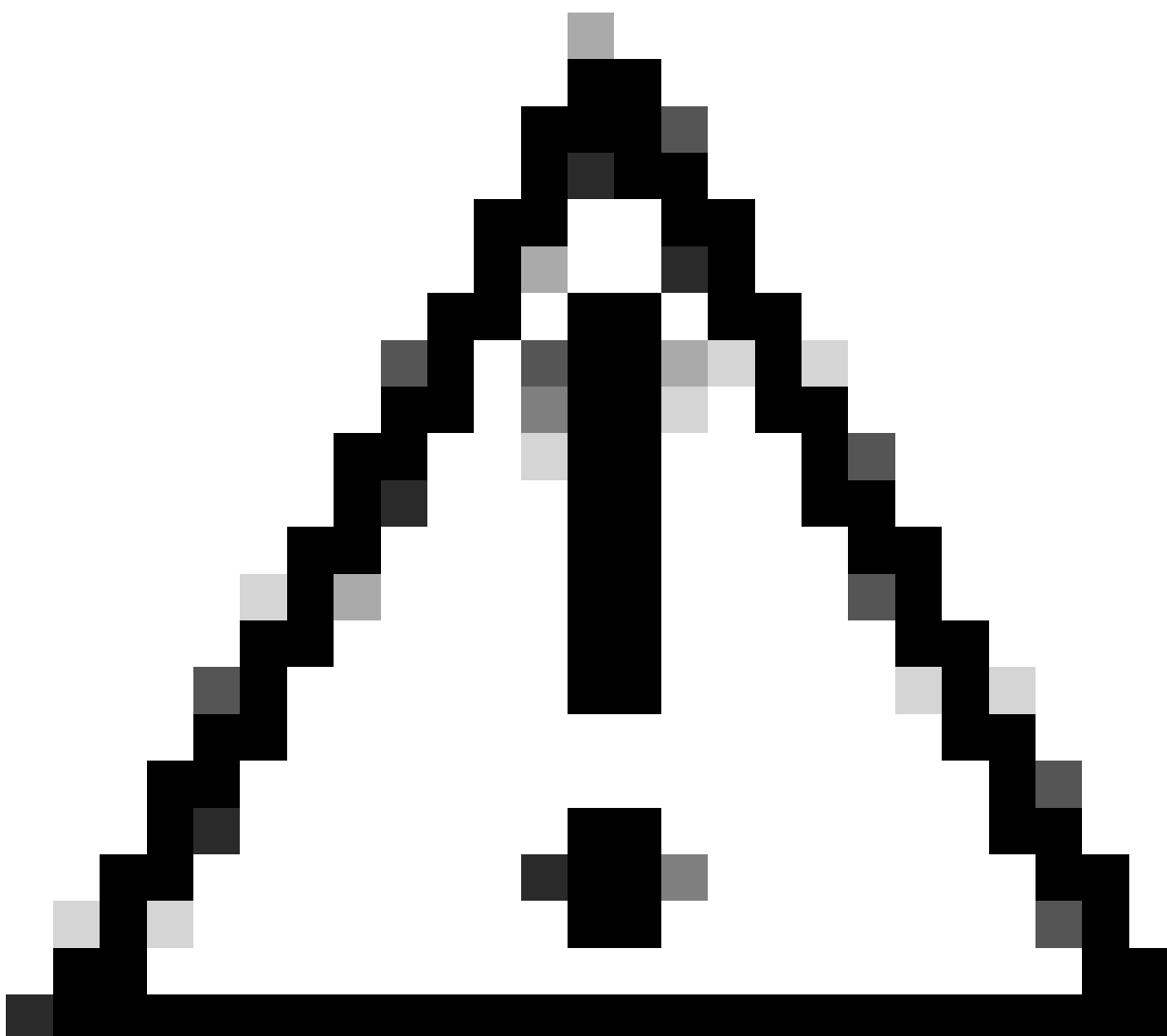
Welcome to the Platform Command Line Interface

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:

```

Etapa 3. Agora você pode gerenciar o dispositivo normalmente.



Caution:

- Tenha sempre em mente nossa responsabilidade ao operar em um ambiente de usuário.
 - RADKele deve ser usado como uma ferramenta de coleta de dados.
 - Nunca faça alterações sem a permissão do usuário.
 - Documente todas as suas descobertas nas notas do caso.
-

Acesso à GUI

- Proxy HTTP

Etapa 1. Verifique se as credenciais HTTP foram adicionadas ao serviço RADKit na configuração do dispositivo.

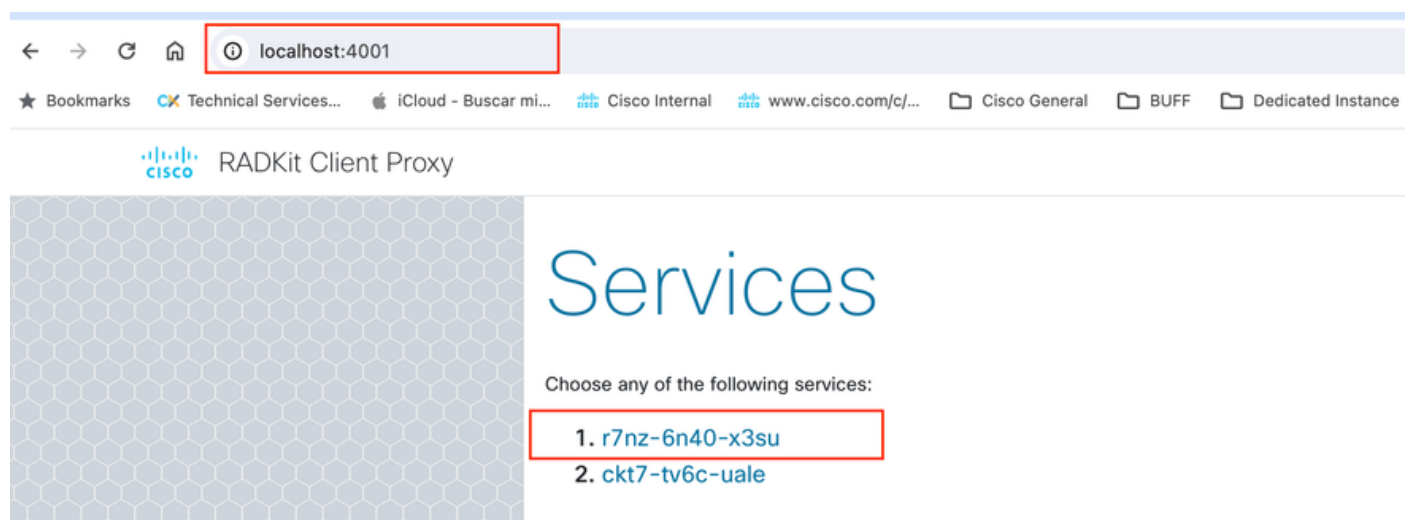
Etapa 2. Inicie o proxy HTTP no cliente Radkit e defina a porta local usada para se conectar ao proxy.

<#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
>>> █
```

Etapa 3. No navegador da Web, navegue até <https://localhost:4001> e selecione o serviço ao qual deseja se conectar.



Etapa 4. Clique na opção Ir para página da Web no dispositivo correto para se conectar à sua

página da Web.

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

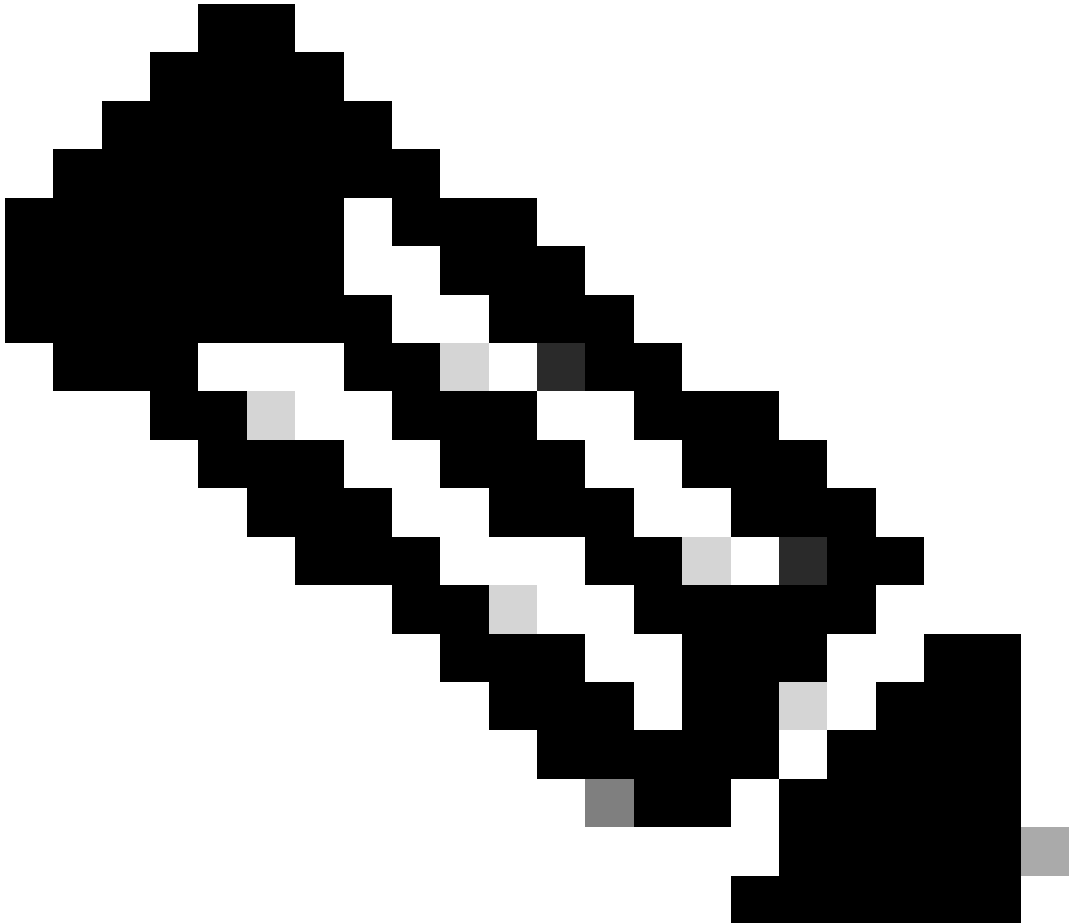
Technical Services... iCloud - Buscar mi... Cisco Internal www.cisco.com/c/... Cisco General BUFF Dedicated Instance WxC Calling Voice Ir

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](#)



Observação: na primeira vez que o Proxy HTTP for configurado em um cliente RADKit, é recomendável clicar na opção Reset for each Devices antes de tentar abrir a página da Web Device.

Etapa 5. A página da Web é exibida.

← → ↻ 🏠 ⚠ 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 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, 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

- Encaminhamento de portas

Etapa 1. Verifique as portas TCP encaminhadas configuradas para o dispositivo.

<#root>

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

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

Etapa 2. Configure uma porta local a ser mapeada com a porta de destino do dispositivo. Você deve usar a porta local para acessar a GUI do dispositivo.

<#root>

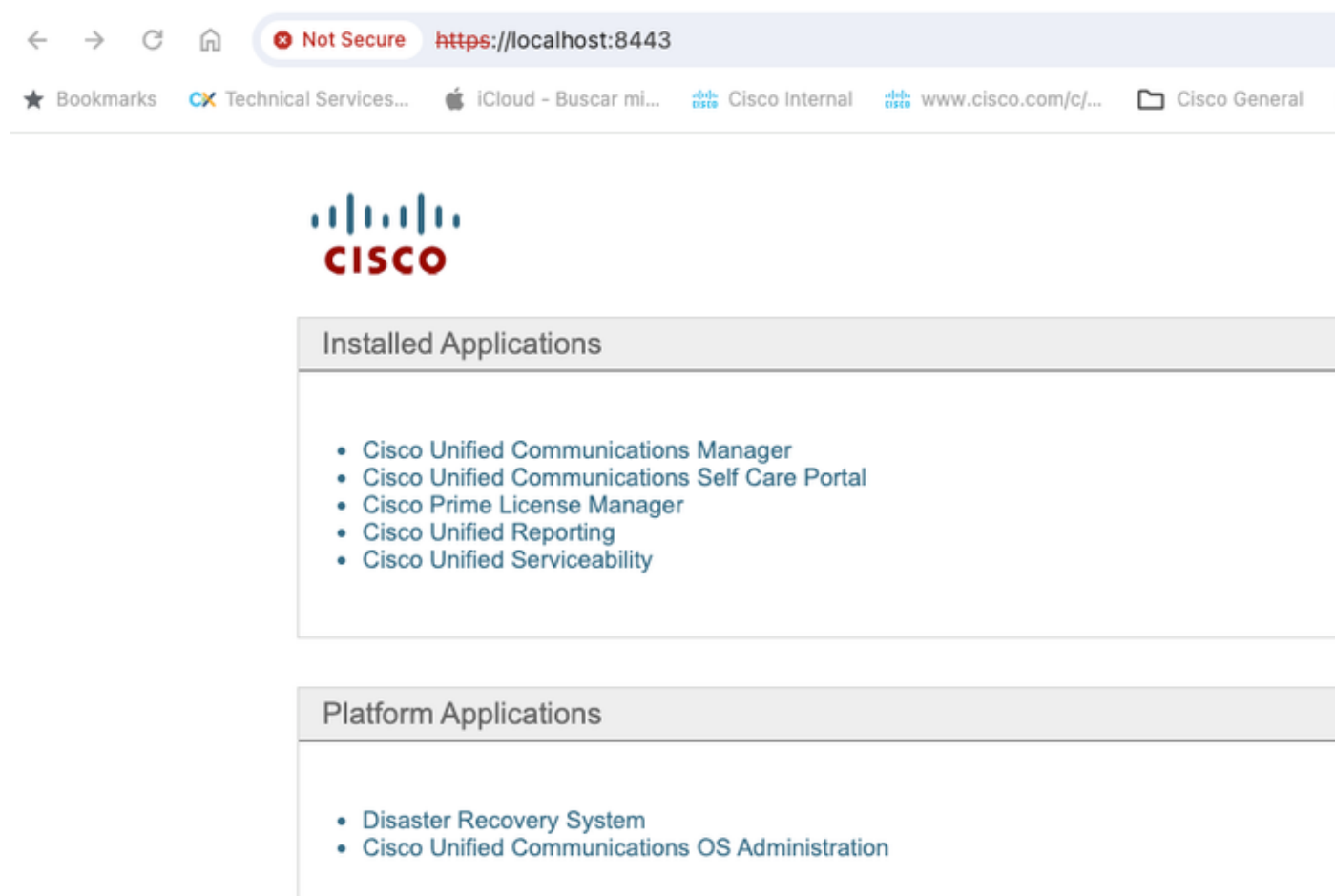
```
>>> cucm.forward_tcp_port(local_port=8443, destination_port=443)
```

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

Etapa 3. Abra o navegador e digite o URL com a porta configurada na Etapa 2:

<https://localhost:8443>.

A GUI do dispositivo agora está acessível.



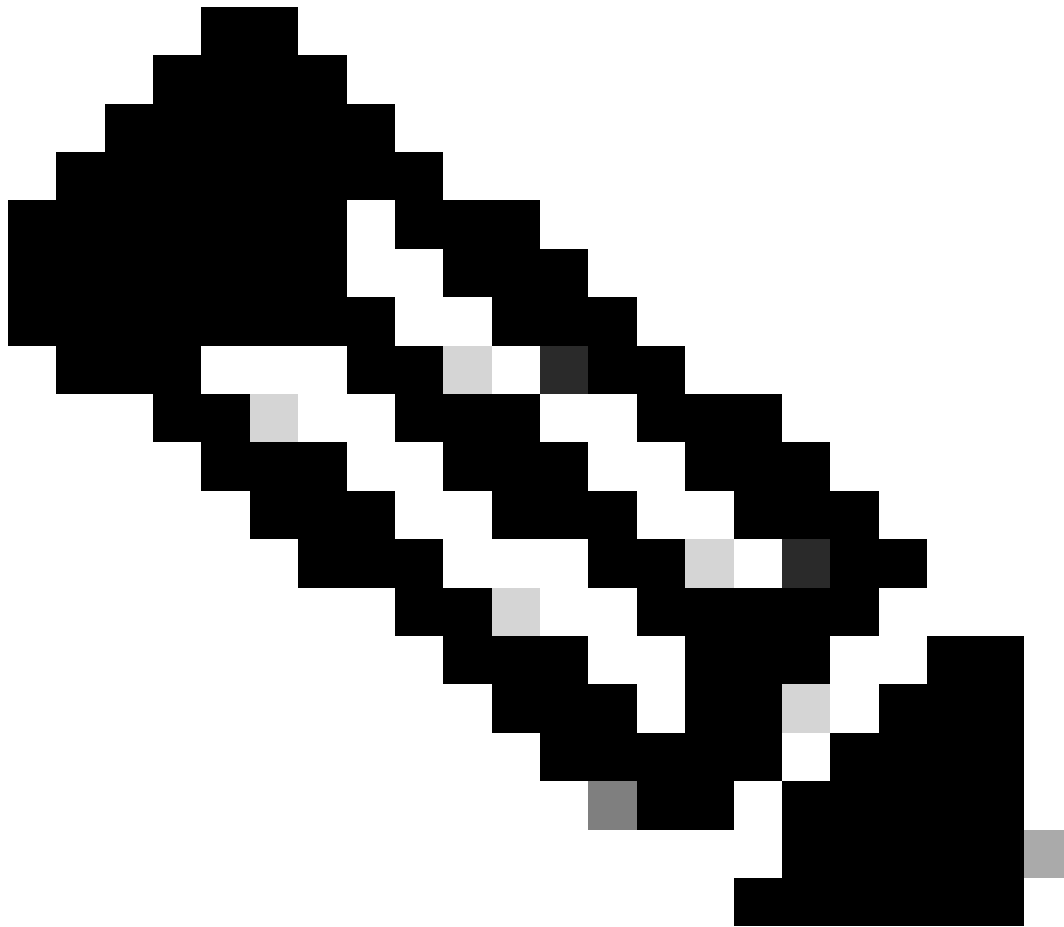
The screenshot shows a web browser window with the address bar displaying 'https://localhost:8443' and a 'Not Secure' warning. The browser's bookmark bar includes 'Bookmarks', 'Technical Services...', 'iCloud - Buscar mi...', 'Cisco Internal', 'www.cisco.com/c/...', and 'Cisco General'. The main content area features the Cisco logo at the top. Below the logo, there are two sections: 'Installed Applications' and 'Platform Applications'. The 'Installed Applications' section lists five items: Cisco Unified Communications Manager, Cisco Unified Communications Self Care Portal, Cisco Prime License Manager, Cisco Unified Reporting, and Cisco Unified Serviceability. The 'Platform Applications' section lists two items: Disaster Recovery System and Cisco Unified Communications OS Administration.

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: Para acessar a GUI do produto, você ainda precisa das credenciais para poder fazer login, portanto, é recomendável que o usuário crie uma conta de usuário somente leitura para acesso.

Coleta de logs

- RTMT

Etapa 1. Verifique se a porta 8443 está listada nas portas TCP encaminhadas configuradas para o dispositivo.

```
<#root>
```

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

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

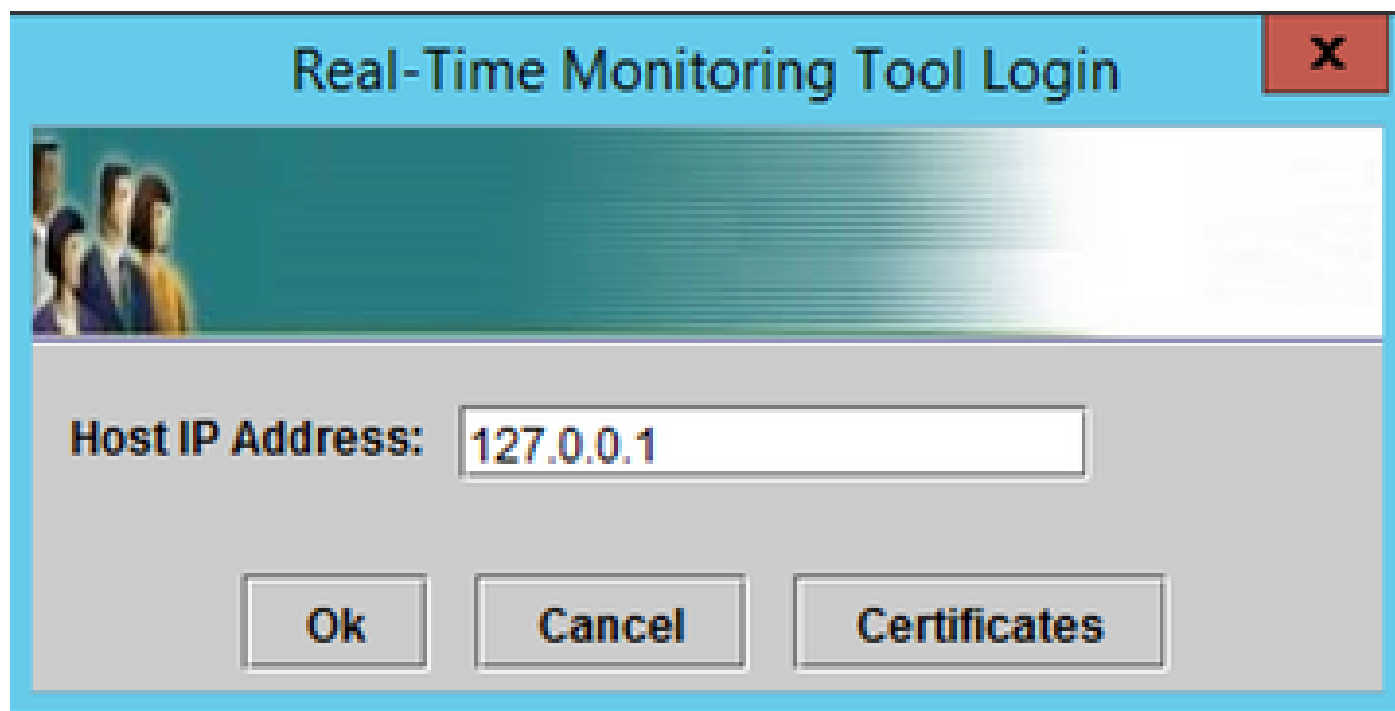
Etapa 2. Configure a mesma porta 8443 como porta local a ser mapeada com a porta 8443 como a porta de destino do dispositivo.

<#root>

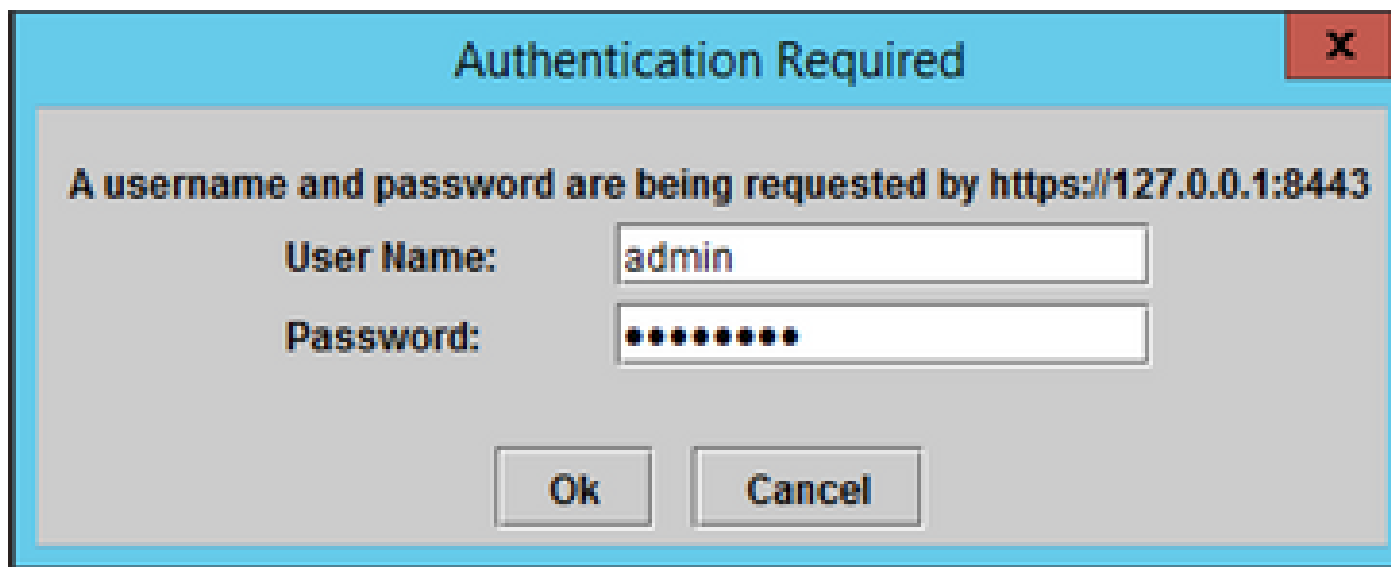
```
>>> cucm.forward_tcp_port(local_port=8443, destination_port=8443)
```

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

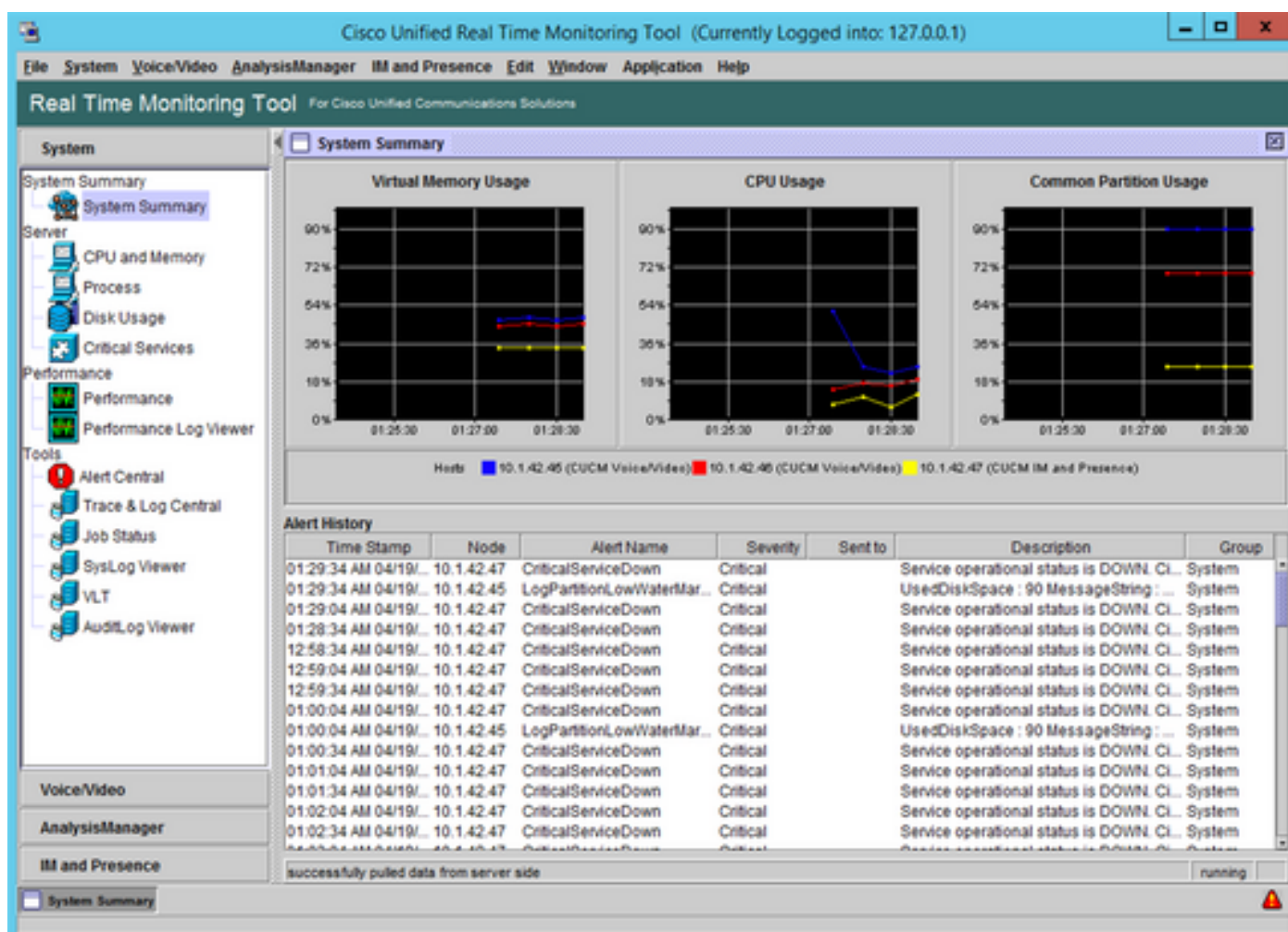
Etapa 3. Abra o RTMT e digite 127.0.0.1 no Endereço IP do Host, ele usa automaticamente a porta 8443.

A screenshot of the 'Real-Time Monitoring Tool Login' dialog box. The dialog has a blue title bar with the text 'Real-Time Monitoring Tool Login' and a red close button with a white 'X'. Below the title bar is a decorative banner with a blurred image of people. The main area is light gray and contains the label 'Host IP Address:' followed by a text input field containing '127.0.0.1'. At the bottom, there are three buttons: 'Ok', 'Cancel', and 'Certificates'.

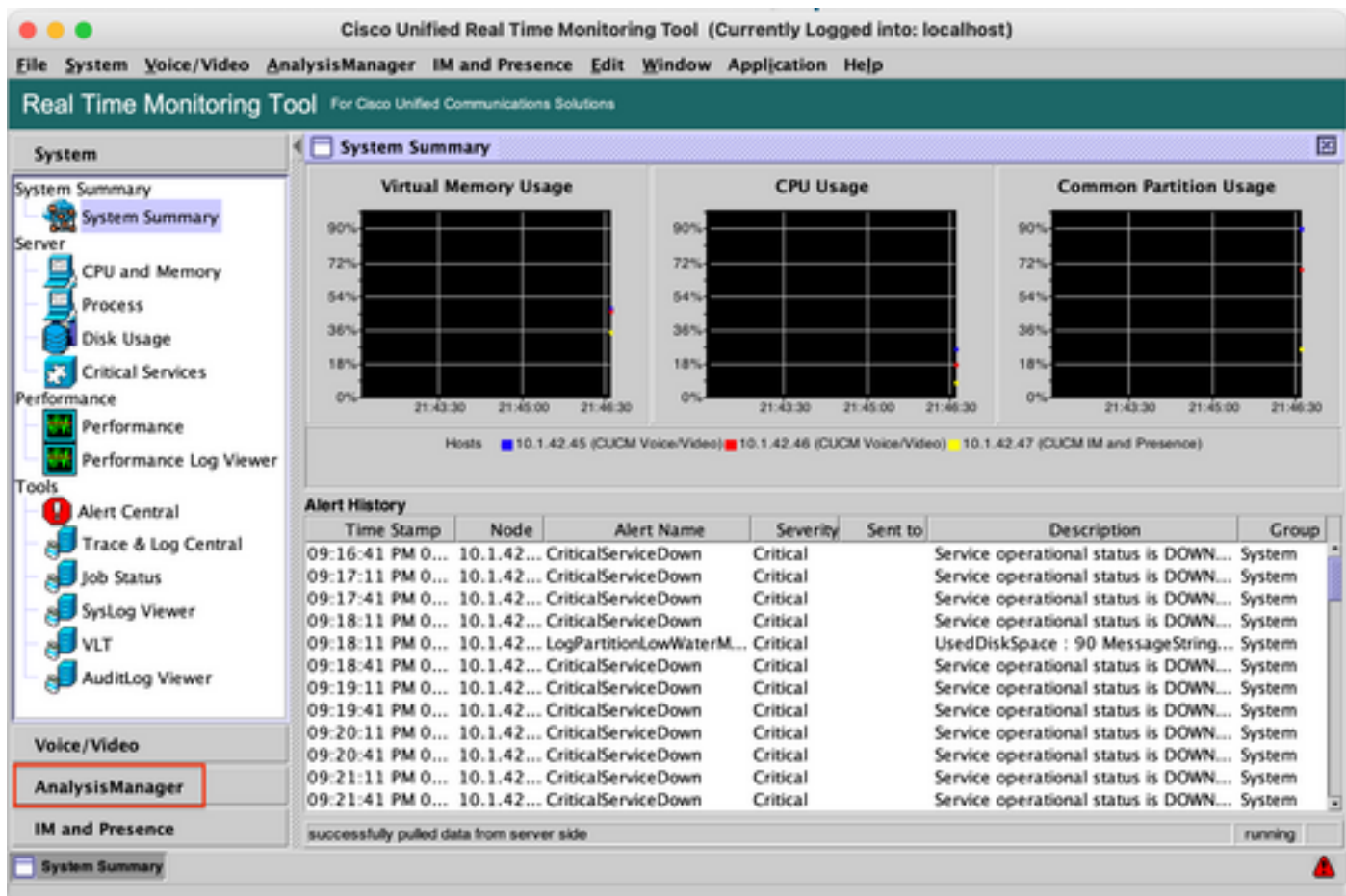
Etapa 4. Faça login com as credenciais corretas.



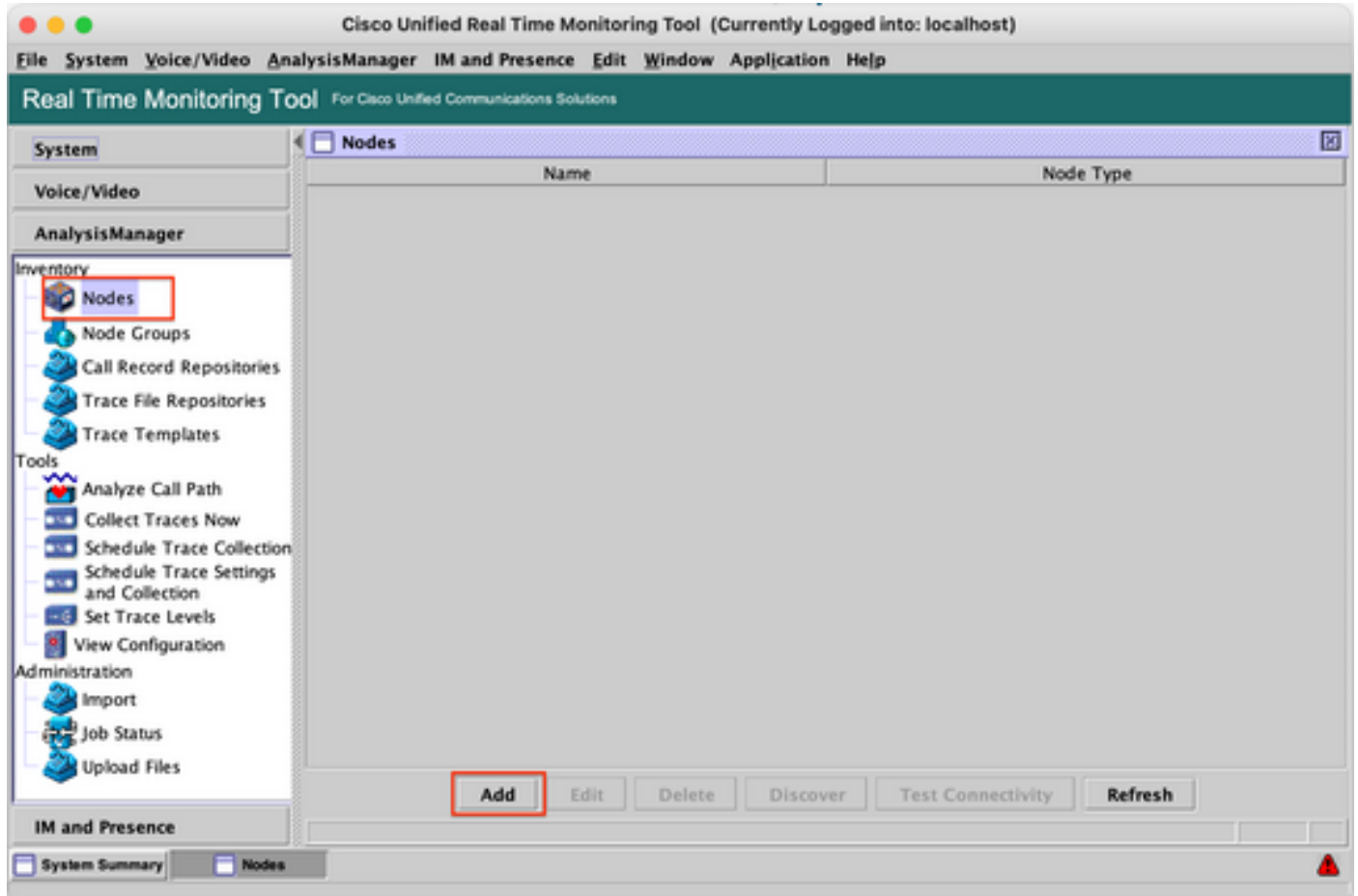
Etapa 5. RTMT é exibido.



Etapa 6. Vá para AnalysisManager no painel esquerdo.



Etapa 7. Clique em Nodes e em Add para configurar os detalhes do dispositivo a ser adicionado usando localhost e a Porta TCP encaminhada.



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

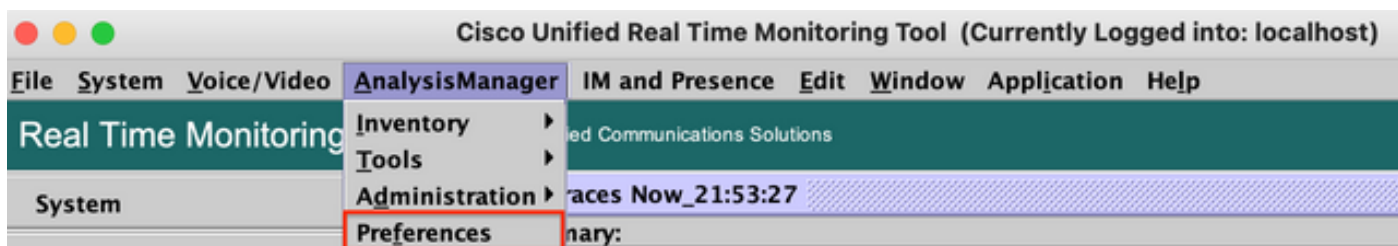
Associated Group ☒ AllNodes

Advanced...

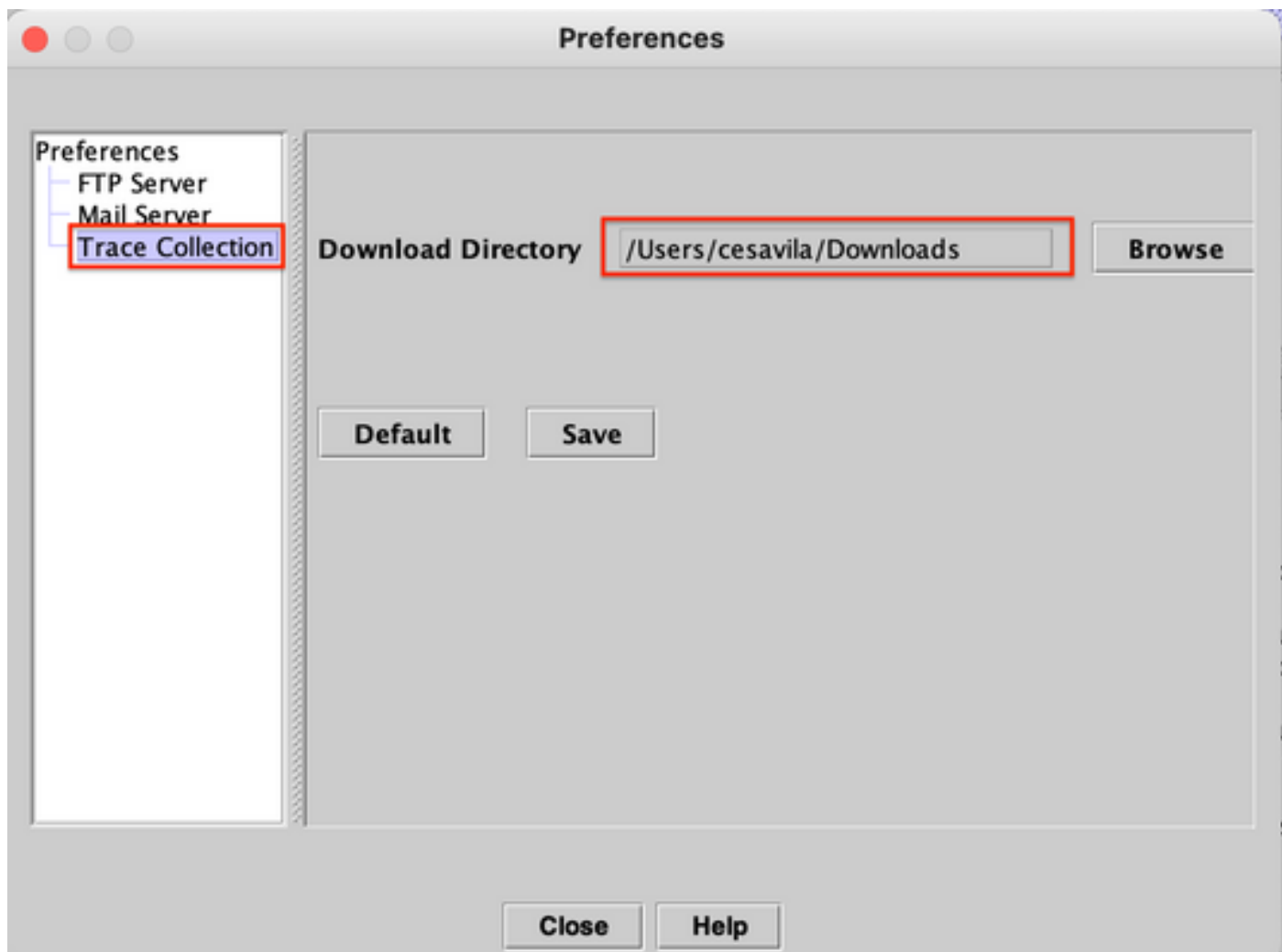
* Required Fields

Save Cancel

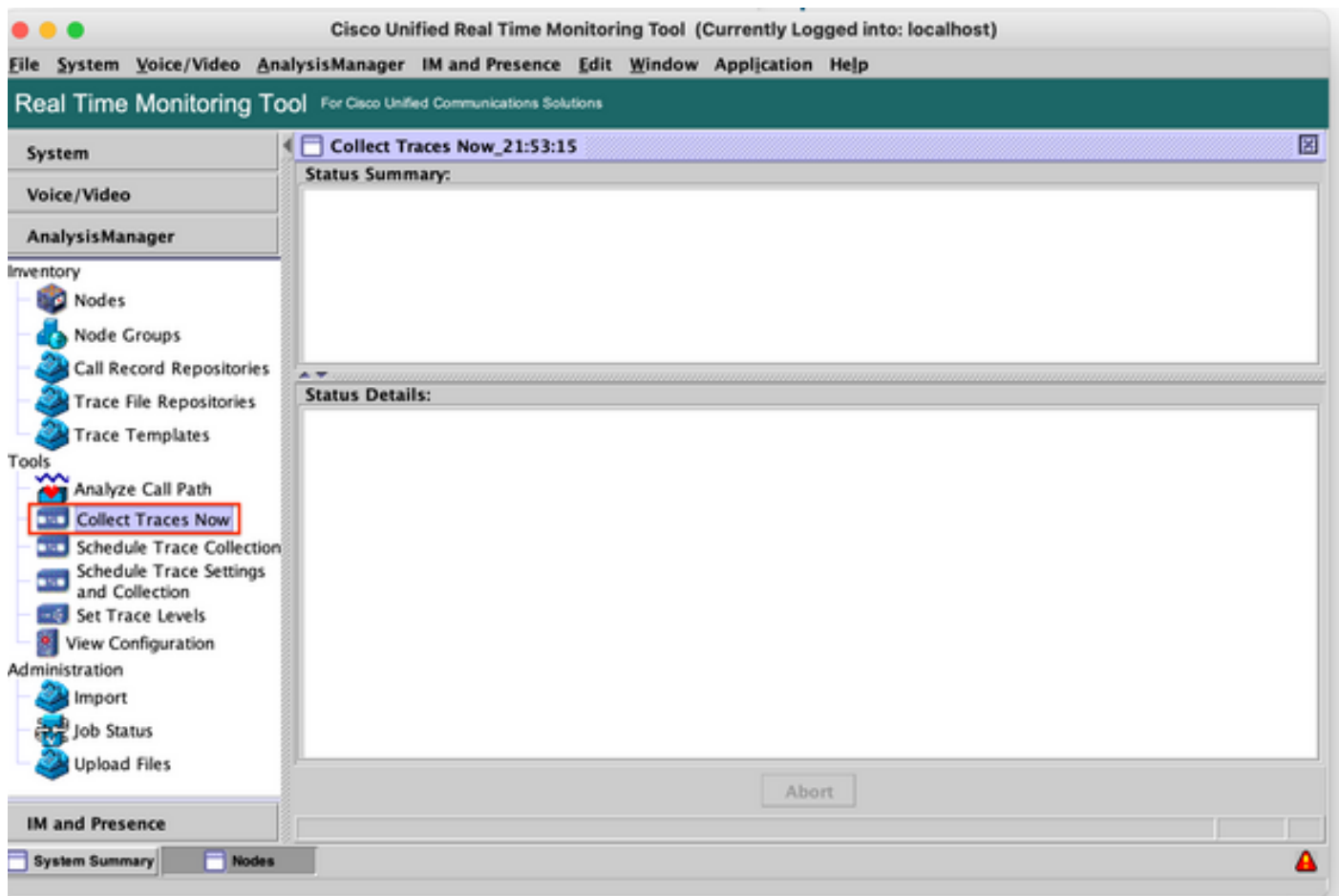
Etapa 8. Clique em Analysis Manager no menu na parte superior e selecione Preferences.



Etapa 9. Vá para Trace Collection e selecione a pasta Correct para fazer o download dos logs, clique em Save e depois em Close.



Etapa 10. Vá para Coletar rastreamentos agora.



Etapa 11. Selecione a opção Node, selecione o dispositivo que foi adicionado na Etapa 7 e clique em 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 **Customize...**

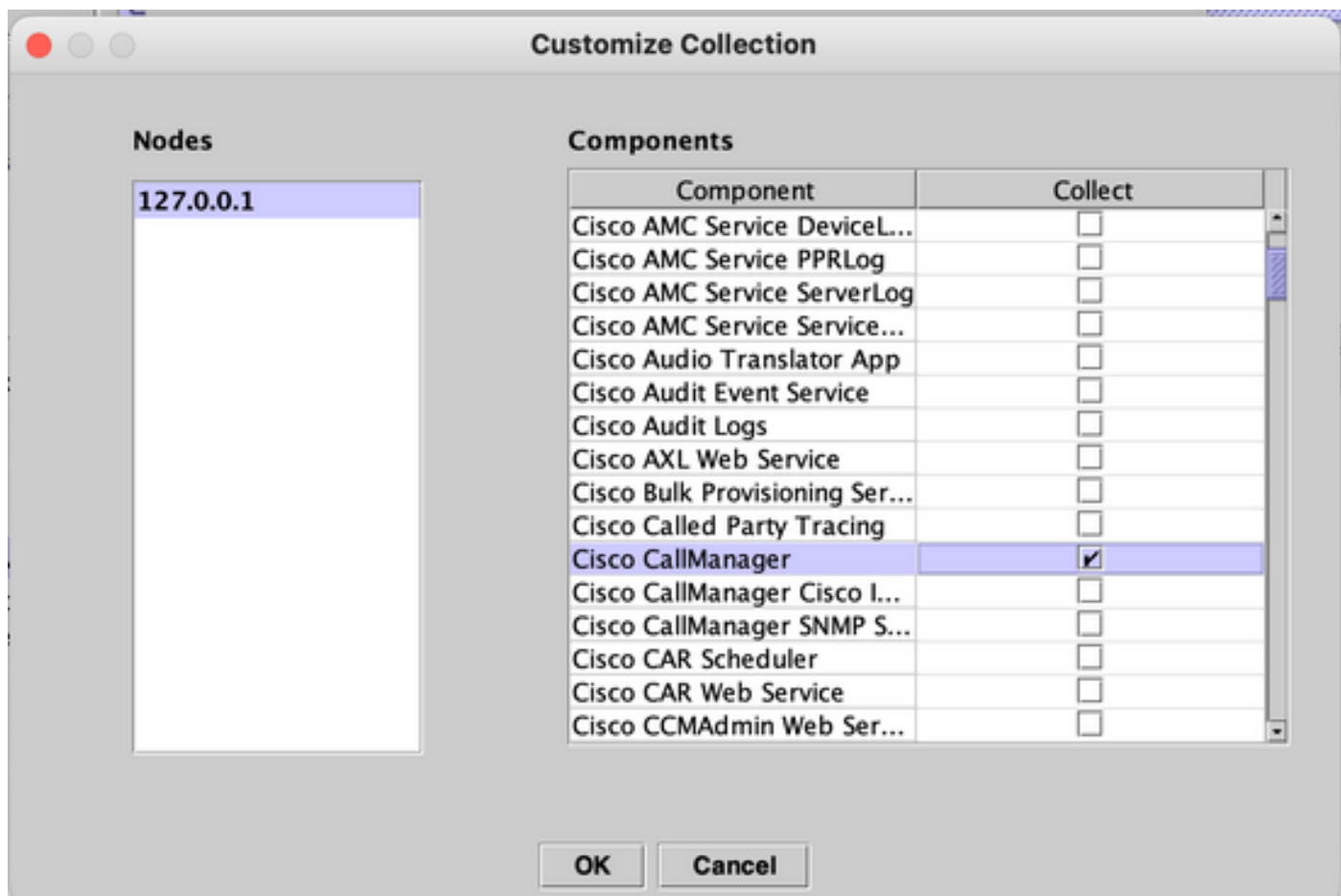
Start Time:

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

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

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

Etapa 12. Selecione os logs a serem coletados do dispositivo e clique em OK.



Etapa 13. Finalmente, selecione Hora de Início e Hora de Término dos logs a serem coletados e clique em 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...

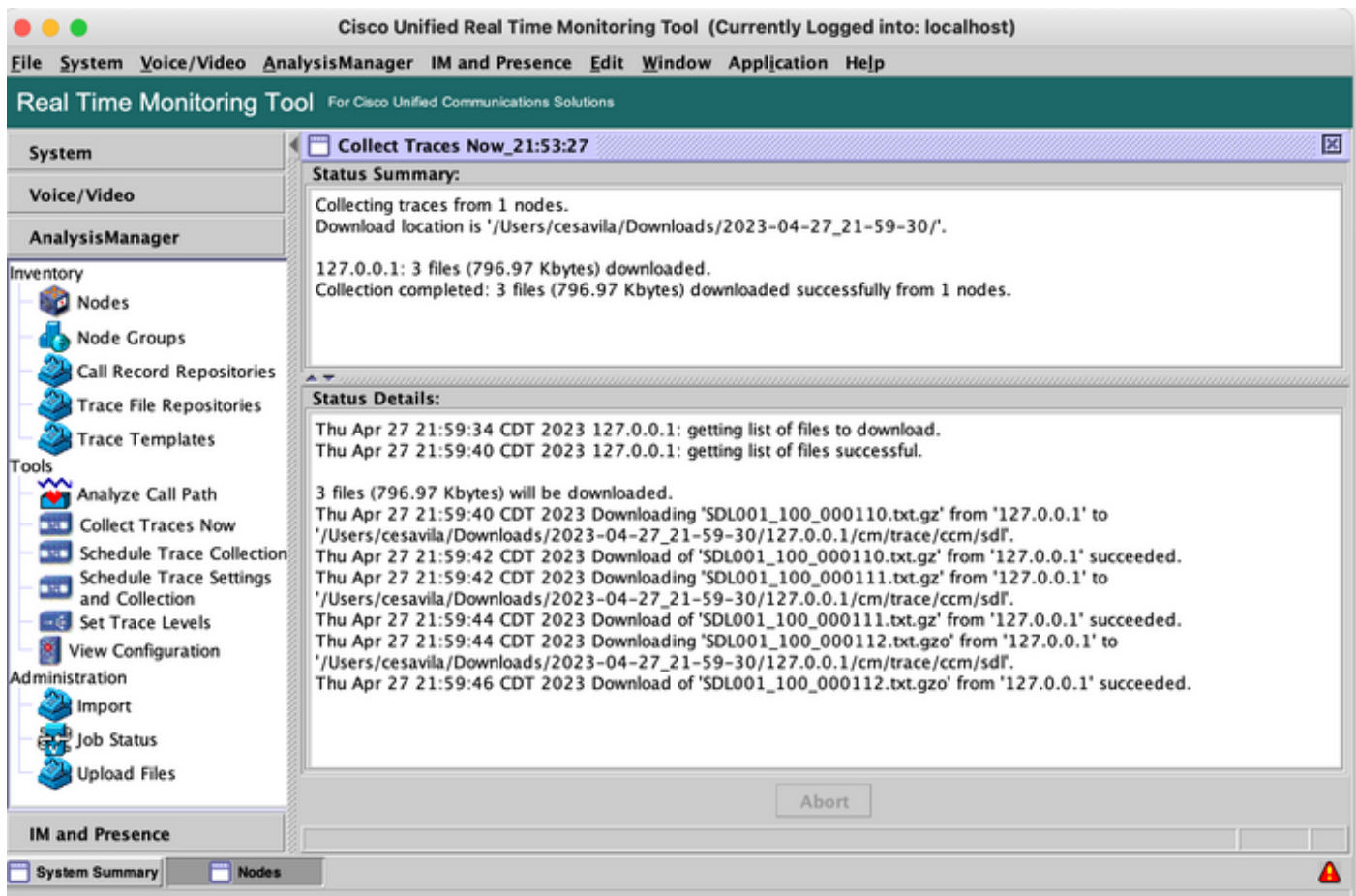
Start Time: 04-27-2023 21:00:00

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

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

View Summary **OK** Cancel Help

Etapa 14. Os arquivos são baixados para o PC local (PC cliente RADKit) com êxito.



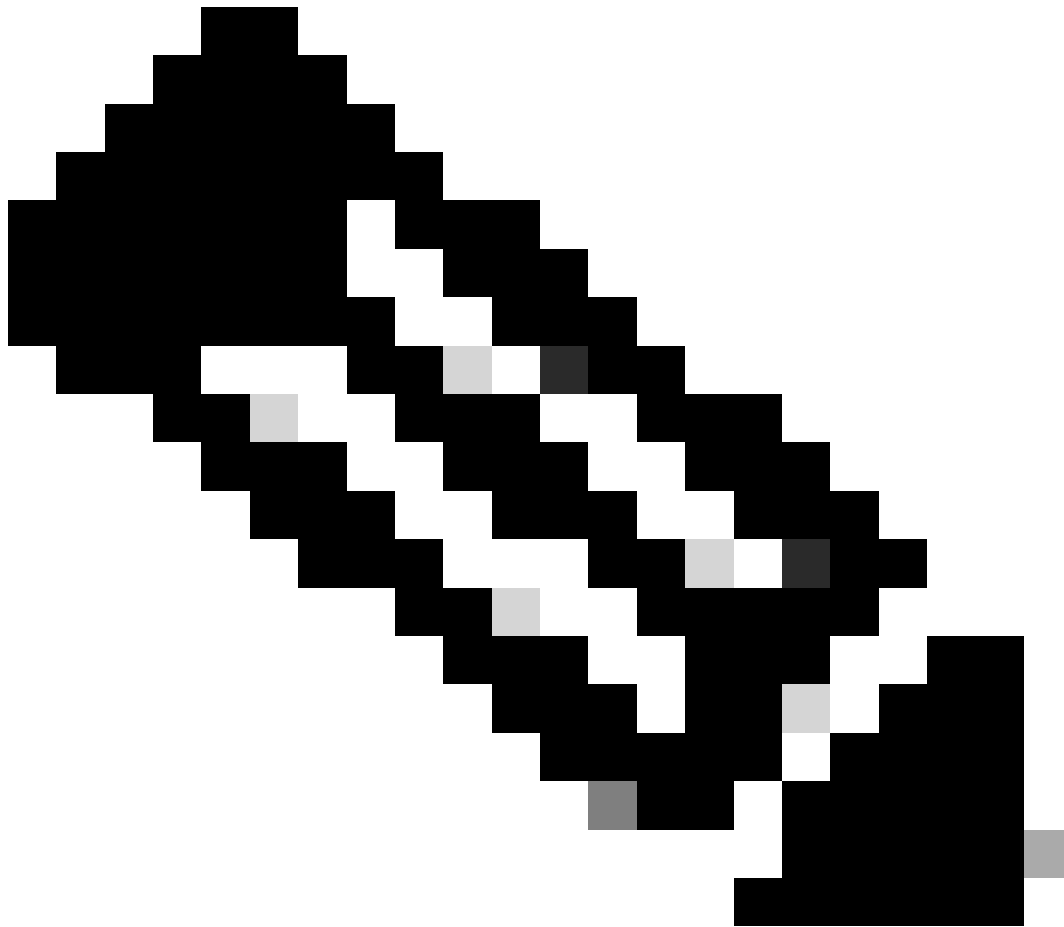
- API SOAP

A API SOAP atualmente é compatível com o CUCM. Além disso, o Swagger é compatível com CMS, Expressway, CVP, etc.

Etapa 1. Verifique se as credenciais HTTP foram adicionadas ao serviço RADKit na configuração do dispositivo.

Etapa 2. Execute o comando HTTP Post no cliente RADKit, especifique o caminho do recurso, o corpo da solicitação com os parâmetros e cabeçalhos necessários.

```
>>>
... 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/sdfl/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: A opção de pós-processadores 'cucm-extract' é usada para remover os cabeçalhos de Resposta HTTP para poder salvar o log em um arquivo.

```
>>> 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\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...'
-----
```

Etapa 3. Salve o conteúdo em um arquivo para salvar o arquivo de rastreamento no PC local.

<#root>

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

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

Casos de uso de RADKit

Como foi destacado, o RADKit fornece uma conexão segura aos dispositivos de rede, incluindo servidores de colaboração sem a necessidade de estar em um webex. A ideia é simplificar alguns dos desafios relacionados à coleta de dados, fornecendo acesso sob demanda aos dispositivos necessários.

Falando especificamente sobre implantações de colaboração, o RADKit pode ser muito útil atualmente para uma variedade de problemas, como:

- Problemas de Replicação de BD.
- Procedimentos de regeneração de certificado.
- Verificação de integridade do sistema.
- Validação da configuração na GUI/CLI.
- Coleta de logs por meio da interface da Web (por exemplo, CER, Expressway, CIMC etc.).
- Logs de depuração via CLI em gateways de voz.

Informações Relacionadas

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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.