

Einrichten von RADKit in einer Collaboration-Umgebung

Inhalt

[Einleitung](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Terminologie](#)

[RADKit-Architektur](#)

[RADKit-Installation](#)

[RADKit Service \(Benutzerseite\)](#)

[Integration](#)

[Geräte hinzufügen](#)

[Autorisierung von Remote-Benutzern](#)

[RADkit Client \(TAC-seitig\)](#)

[Anmelden](#)

[SSH-Zugriff](#)

[GUI-Zugriff](#)

[HTTP-Proxy](#)

[Port-Weiterleitung](#)

[Protokollsammlung](#)

[RTMT](#)

[SOAP-API](#)

[RADKit-Anwendungsfälle](#)

[Zugehörige Informationen](#)

Einleitung

Dieses Dokument beschreibt die Schritte zur Einrichtung von RADKit und zeigt die Konfiguration, die für den Einsatz mit Collaboration-Produkten erforderlich ist.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse zu folgenden Themen verfügen:

- Grundkenntnisse aller VOS Collaboration-Produkte
- Grundkenntnisse des CLI/SSH-Zugriffs

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-

Versionen:

- Cisco Unified Communications Manager 12.5 und 14.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

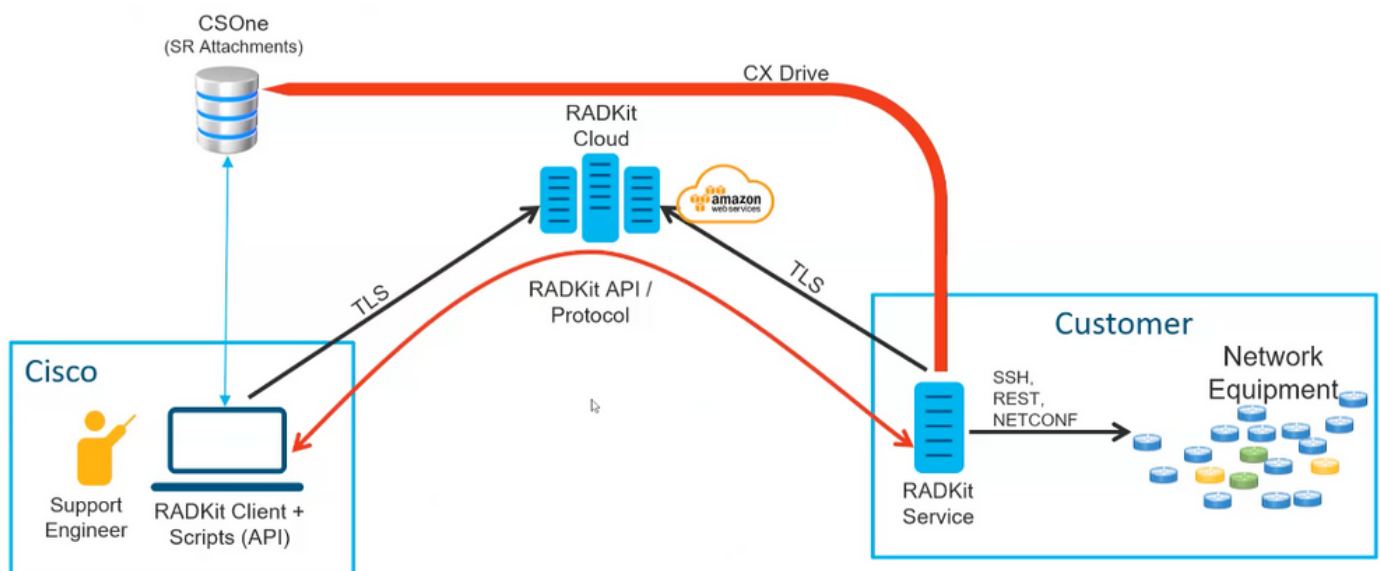
Terminologie

RADKit: Es handelt sich um einen Connector, der Cisco TAC-Technikern und -Partnern einen sicheren Remote-Zugriff auf die Benutzergeräte ermöglicht. Es unterstützt mehrere Protokolle für die Interaktion mit Geräten wie SSH oder HTTP/HTTP.

RADKit-Dienst: Dies ist die Server-Seite. Sie wird vollständig vom Benutzer verwaltet. Serverseitig steuert der Benutzer, wer wie lange auf die Geräte zugreifen kann. Der Radkit-Service muss mit den Geräten im Netzwerk verbunden sein, um den Zugriff darauf zu ermöglichen.

RADKit-Client: Dies ist die Client-Seite. Dieser PC wird für die Verbindung mit den Geräten im Benutzernetzwerk verwendet.

RADKit-Architektur



RADKit-Architektur

RADKit-Installation

Schritt 1: Navigieren Sie zu <https://radkit.cisco.com>, und klicken Sie auf Downloads, und wechseln Sie dann zum Release-Ordner.

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

-

Schritt 2: Klicken Sie auf die neueste Version.

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

-

Schritt 3: Laden Sie die richtige Datei für Ihr Betriebssystem herunter.

INDEX OF /DOWNLOADS/RELEASE/1.4.9/

[../](#)

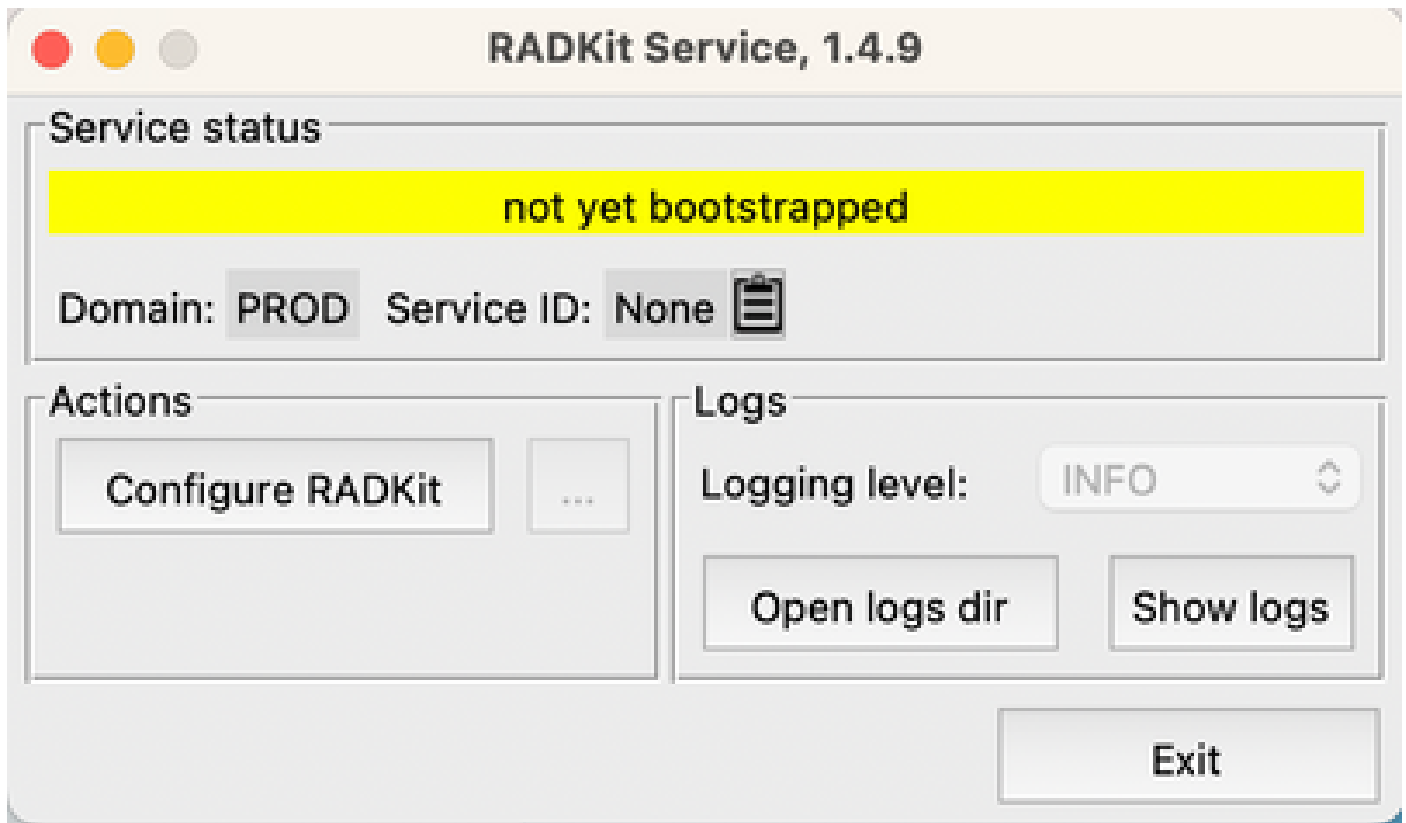
docs/	04-Apr-2023 11:45	-
cisco_radkit_1.4.9_doc_html.tgz	04-Apr-2023 11:43	8003863
cisco_radkit_1.4.9_macos_arm64_signed.pkg	11-Apr-2023 10:41	74142354
cisco_radkit_1.4.9_macos_x86_64_signed.pkg	11-Apr-2023 10:41	77265560
cisco_radkit_1.4.9_pip_linux.tgz	04-Apr-2023 11:49	146189048
cisco_radkit_1.4.9_pip_macos.tgz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

Schritt 4: Führen Sie das Installationsprogramm auf dem PC oder Server aus. Im Rahmen der Installation muss Radkit drei Anwendungen installieren: Radkit Service, Radkit Client und Radkit Netzwerkkonsole.

RADKit Service (Benutzerseite)

Integration

Schritt 1: Um mit der Konfiguration des RADKit-Dienstes zu beginnen, navigieren Sie zu Anwendungen, und suchen Sie nach RADKit-Dienst. Beim ersten Start wird die Meldung angezeigt, dass der Bootstrapper noch nicht gestartet wurde.



Schritt 2. Klicken Sie auf Konfigurieren RADKit, der Browser öffnet sich automatisch mit URL <https://localhost:8081/bootstrap>.

- Erstellen Sie ein Kennwort für den Superadmin-Benutzer, und klicken Sie auf Senden.
- Dieser Superadmin-Benutzername und dieses Kennwort werden bei jedem Start oder jeder Konfiguration des Diensts angefordert.

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

Submit

Schritt 3: Wenn Sie auf Senden klicken, werden Sie vom Browser zu <https://localhost:8081/#/connectivity/> weitergeleitet.

Unter Konnektivität > Dienstregistrierung gibt es zwei Authentifizierungsmethoden: Einmaliges Sing-On und einmaliges Passwort.

Single Sign-On Enrollment



✓

Checking prerequisites

2

Email address

Provide email address for SSO login:

Submit

3

Connecting to the Access Service

4

OAuth connect

5

Waiting for SSO

6

Requesting service certificate OTP

7

Requesting service certificate

Schritt 5: Schließen Sie den Assistenten ab, und führen Sie die Schritte aus, bis "Service registered with new identity: xxxx-xxxx-xxxx" ein, und wenn Sie auf "Schließen" klicken, wird der Service als Verbunden angezeigt.



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

Close



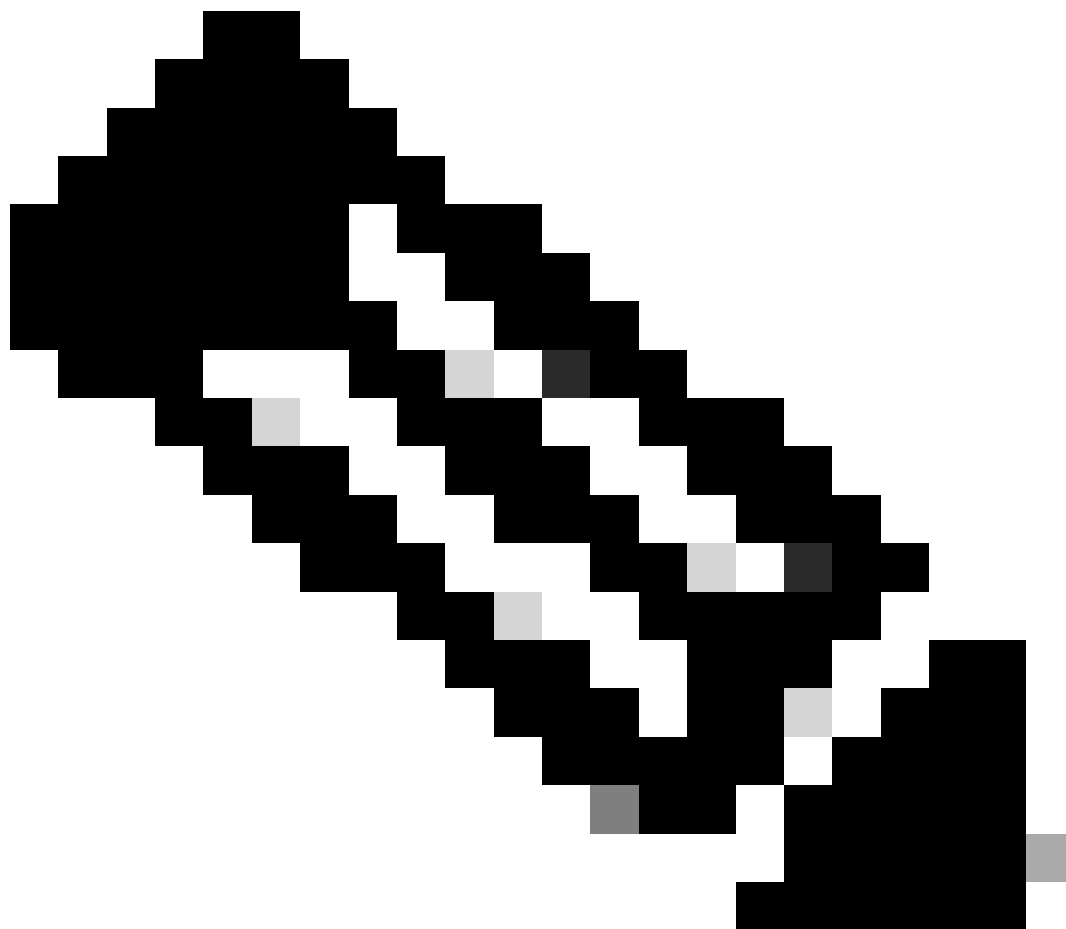
Remote Automation Development
Cisco RADKit Service

Domain: PROD Serial: k331-0evx-s94g

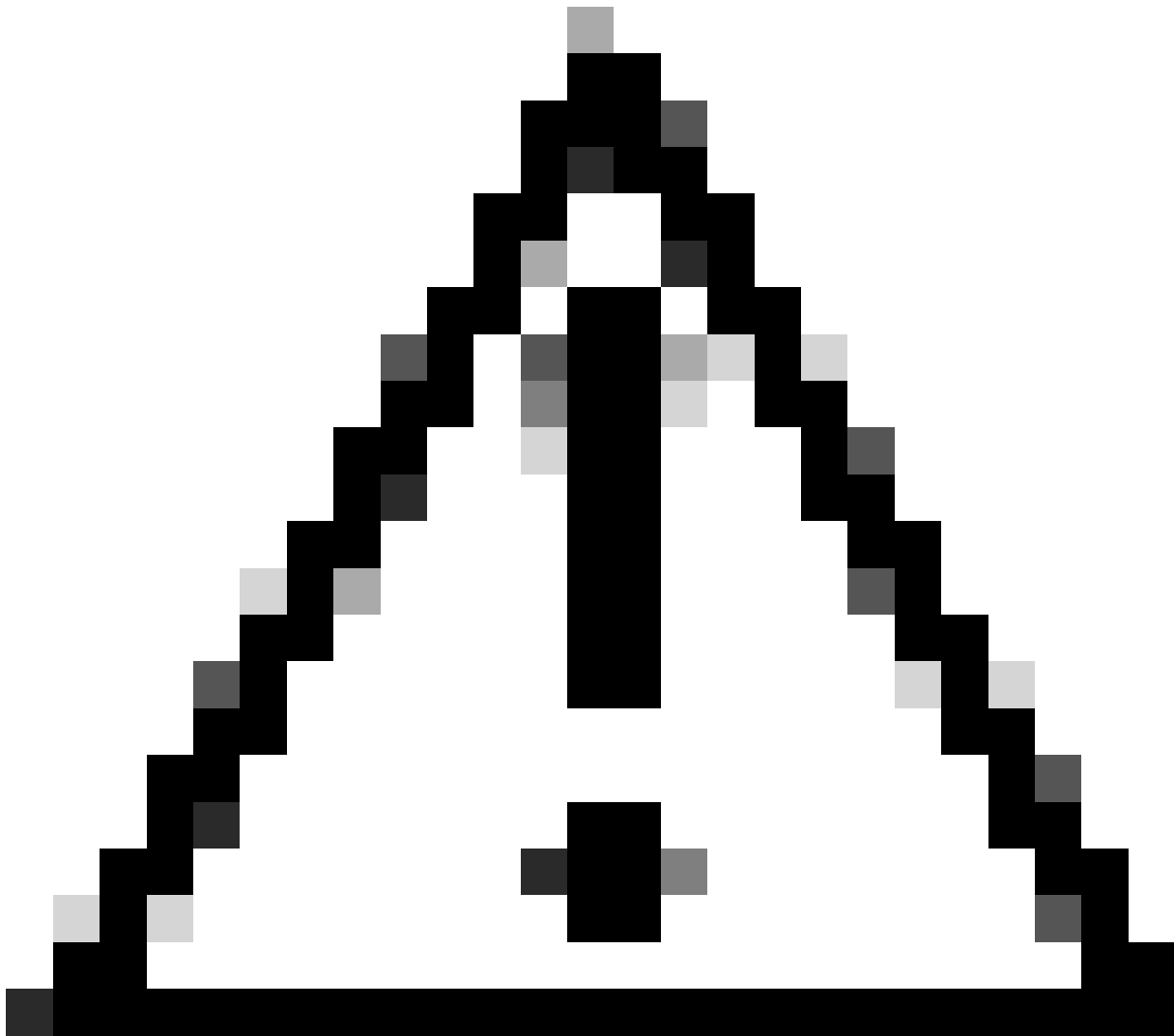


CONNECTED





Anmerkung: Für die Aktivierung des RADKit Service wird ein Cisco Konto benötigt.

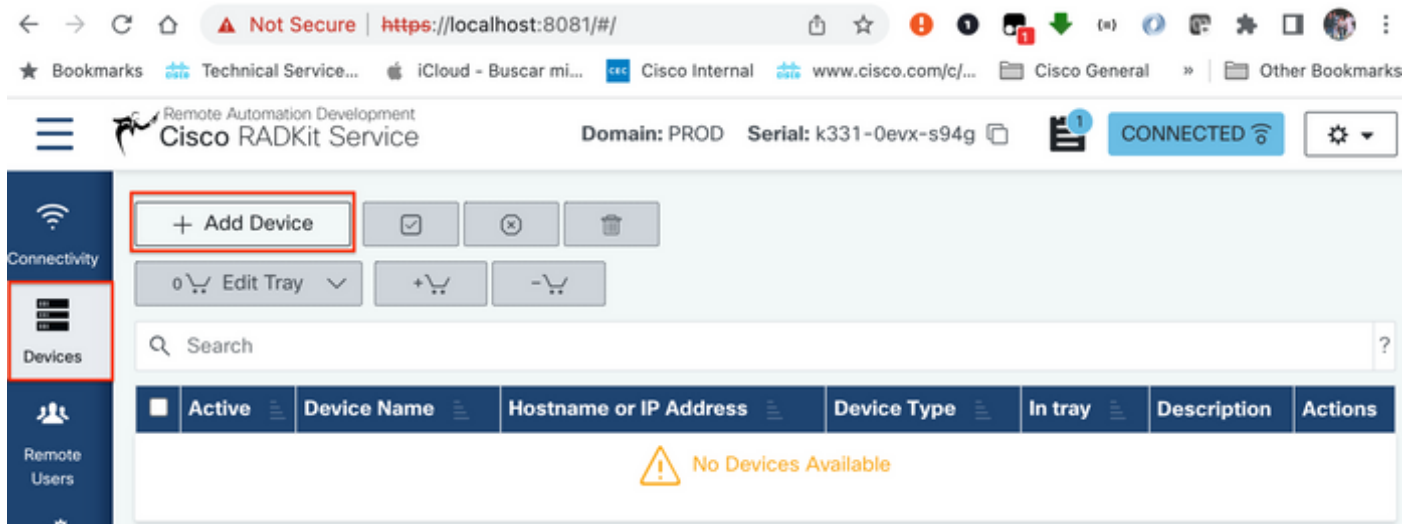


Vorsicht:

- Wenn für den Server, auf dem der RADKit-Dienst ausgeführt wird, ein Proxy definiert werden muss, muss neben der Definition des Proxys auf dem Server/PC selbst auch eine Umgebungsvariable definiert werden, damit der RADKit-Dienst mit `RADKIT_CLOUD_CLIENT_PROXY_URL=http://proxy.example.com:80` funktioniert.

Geräte hinzufügen

Schritt 1: Navigieren Sie zu Geräte, und klicken Sie auf Gerät hinzufügen.



Schritt 2. Sie müssen die nächsten Details konfigurieren:

- Device Name (Gerätename)
- Management-IP-Adresse oder Hostname
- Gerätetyp

Außerdem müssen Sie Weitergeleitete TCP-Ports konfigurieren, die vom Gerät verwendet werden und auf die vom RADKit-Client zugegriffen werden muss. In diesem Beispiel sind die verwendeten Ports 443 für GUI Access und 8443 für RTMT.

Wählen Sie abschließend die verfügbaren Management-Protokolle aus, in diesem Fall Terminal und 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

Schritt 3: Konfigurieren Sie für jedes Management-Protokoll die richtigen Einstellungen, und klicken Sie auf Hinzufügen und Schließen.

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 ?

Schritt 4: Nach dem Hinzufügen muss das Gerät in der Geräteliste angezeigt werden. Es kann für den Remote-Zugriff aktiviert/deaktiviert werden.

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

Autorisierung von Remote-Benutzern

Schritt 1: Um dem Benutzer Zugriff auf die im RADKit-Dienst konfigurierten Geräte zu gewähren, gehen Sie zu Remote Users und wählen Sie Add Users aus.

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

Schritt 2: Konfigurieren der Benutzerdetails:

- E-Mail-Adresse
- Vollständiger Name (optional)
- Aktivieren Sie den Benutzer.
- Geben Sie an, ob die Aktivierung manuell gesteuert werden muss, oder legen Sie einen Zeitrahmen fest, um diesem Benutzer Zugriff zu gewähren.

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

Schritt 3: Wählen Sie Hinzufügen und schließen.

RADkit Client (TAC-seitig)

Anmelden

Schritt 1: Navigieren Sie auf dem Client-PC zu Anwendungen, und suchen Sie nach RADkit Client.

Schritt 2: Erstellen Sie eine Client-Instanz mit Ihrer SSO-Anmeldung.

<#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")
█
```

Schritt 3. Akzeptieren Sie die SSO-Autorisierungsanfrage, die automatisch in Ihrem Browser geöffnet wird.



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

Schritt 4: Erstellen Sie eine Serviceinstanz mit der vom Benutzer generierten Seriennummer aus der Phase "RADKit Service - Onboarding".



Remote Automation Development
Cisco RADKit Service

Domain: PROD

Serial: k331-0evx-s94g



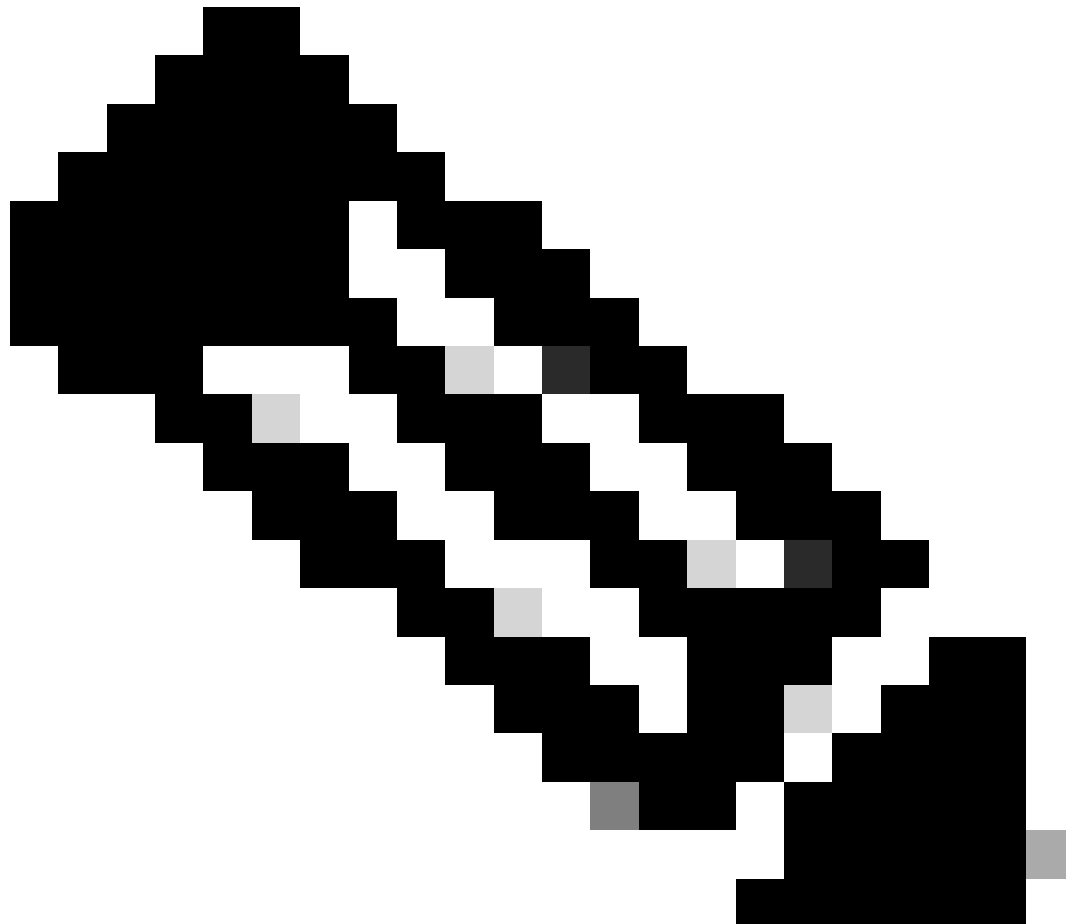
CONNECTED 📶

<#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/']
```



Anmerkung: service ist eine Variable, die beliebig sein kann.

Schritt 5: Überprüfen Sie die für den Zugriff verfügbaren Geräte.

<#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
```

Verwenden Sie den Befehl `update_inventory`, um die Inventarliste zu aktualisieren.

<#root>

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

SSH-Zugriff

Schritt 1. Erstellen Sie ein Objekt aus der Inventarliste.

<#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"]
```

Schritt 2: Starten Sie die SSH-Sitzung mit dem interaktiven Befehl.

<#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 ...

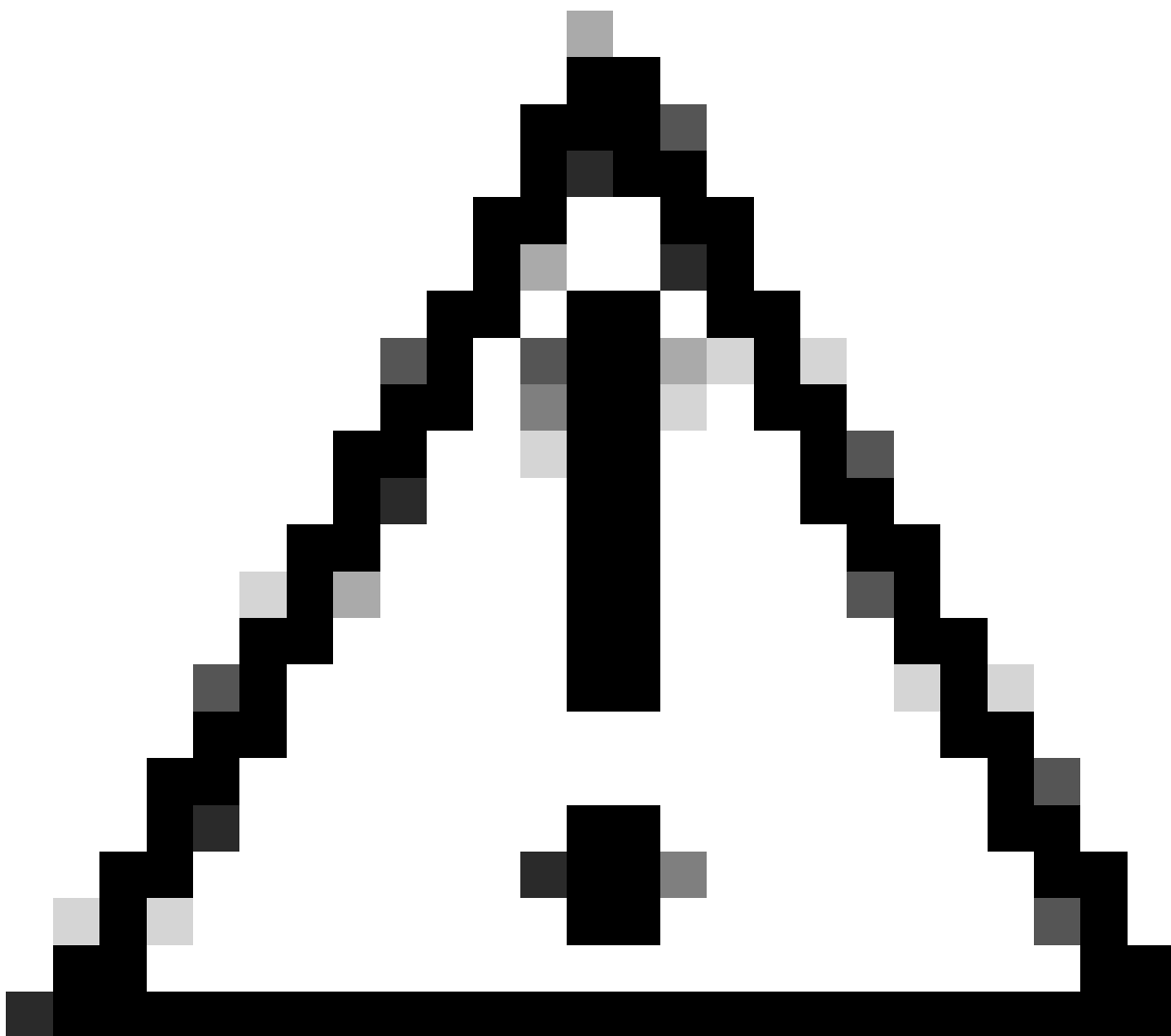
Welcome to the Platform Command Line Interface

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:

```

Schritt 3. Jetzt können Sie das Gerät normal verwalten.



Vorsicht:

- Achten Sie immer auf unsere Verantwortung, wenn Sie in einer Benutzerumgebung arbeiten.
- RADKit muss als Datenerfassungstool eingesetzt werden.
- Nehmen Sie keine Änderungen ohne die Erlaubnis des Benutzers vor.
- Dokumentieren Sie alle Ihre Ergebnisse in den Fallnotizen.

GUI-Zugriff

- HTTP-Proxy

Schritt 1: Stellen Sie sicher, dass die HTTP-Anmeldedaten dem RADKit-Dienst der Gerätekonfiguration hinzugefügt werden.

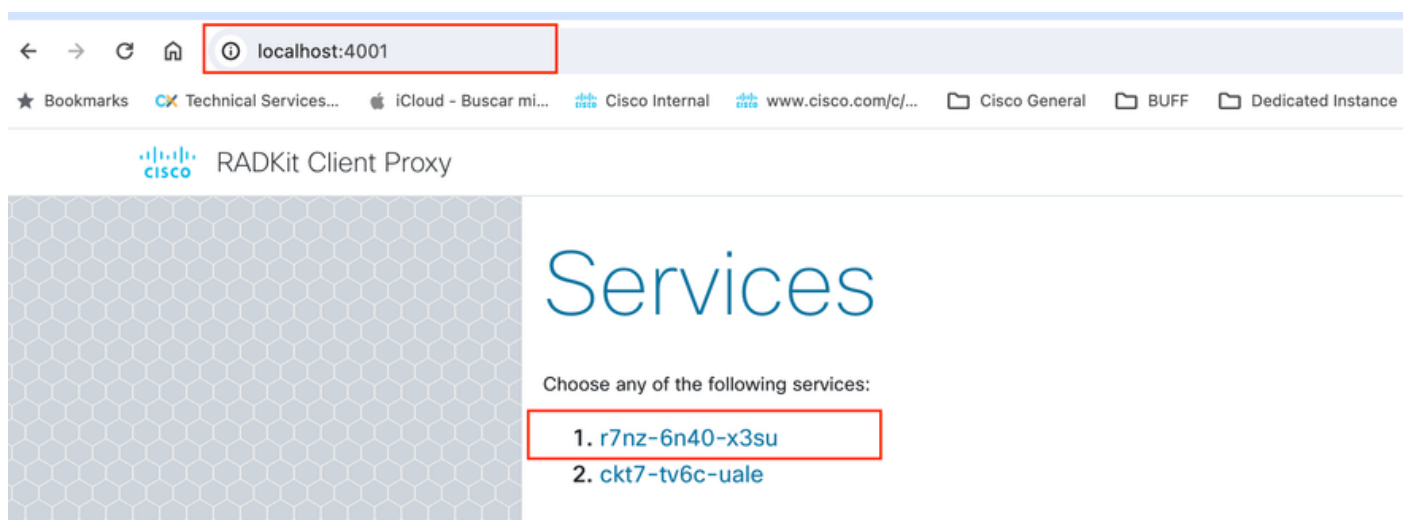
Schritt 2: Starten Sie den HTTP-Proxy auf dem Radkit Client und definieren Sie den lokalen Port, der für die Verbindung mit dem Proxy verwendet wird.

<#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
>>> █
```

Schritt 3: Navigieren Sie im Webbrowser zu <https://localhost:4001>, und wählen Sie den Dienst aus, mit dem Sie eine Verbindung herstellen möchten.



Schritt 4. Klicken Sie auf die Option Gehe zu Webseite auf dem richtigen Gerät, um eine

Verbindung mit der Webseite herzustellen.

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

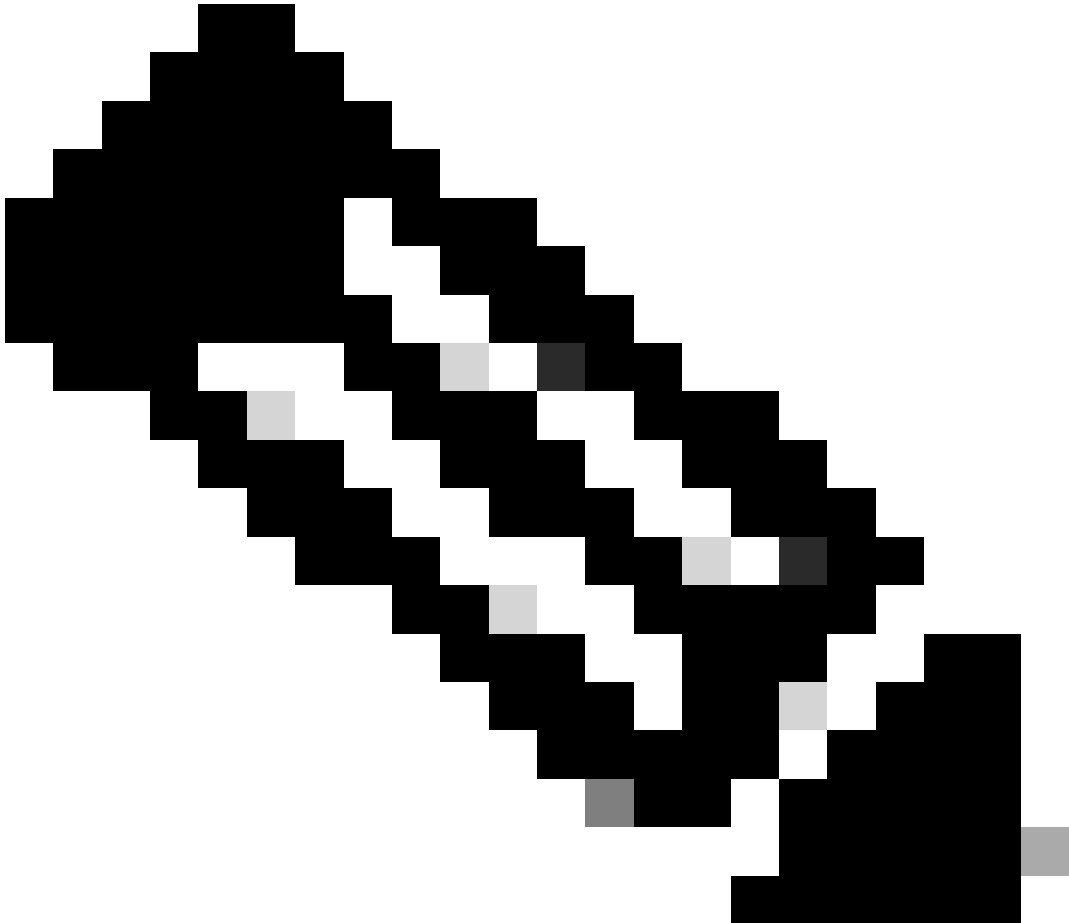
Technical Services... iCloud - Buscar mi... Cisco Internal www.cisco.com/c/... Cisco General BUFF Dedicated Instance WxC Calling Voice Ir

RADKit Client Proxy

Service ID: r7nz-6n40-x3su

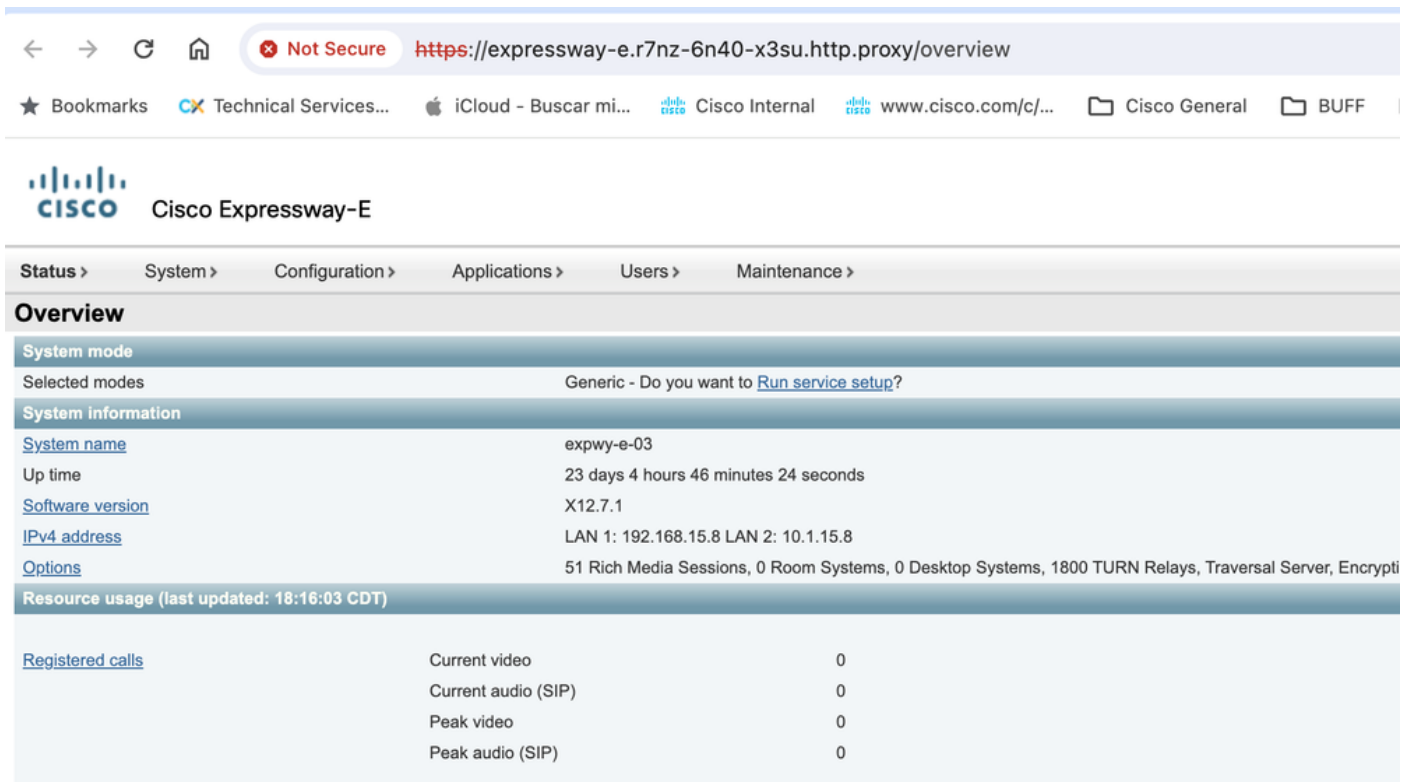
Device name	TCP port forwards	Supports HTTP	Reset Session
expressway-c	443;8443	Go to web page	<button>Reset</button>
expressway-e	443;8443	Go to web page	<button>Reset</button>
cucmhq	443;8443	Go to web page	<button>Reset</button>

[Go back](#)



Hinweis: Wenn HTTP Proxy zum ersten Mal auf einem RADKit-Client eingerichtet wird, wird empfohlen, auf die Option Reset for each Devices (Für jedes Gerät zurücksetzen) zu klicken, bevor Sie versuchen, die Webseite für das Gerät zu öffnen.

Schritt 5. Die Webseite wird angezeigt.



← → ↻ 🏠 ⚠ 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, Encryption

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-Weiterleitung

Schritt 1: Überprüfen der für das Gerät konfigurierten TCP-Forwarded-Ports

```
<#root>
```

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

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

Schritt 2: Konfigurieren Sie einen lokalen Port so, dass er dem Zielport des Geräts zugeordnet wird. Sie müssen den lokalen Port verwenden, um auf die Geräte-GUI zuzugreifen.

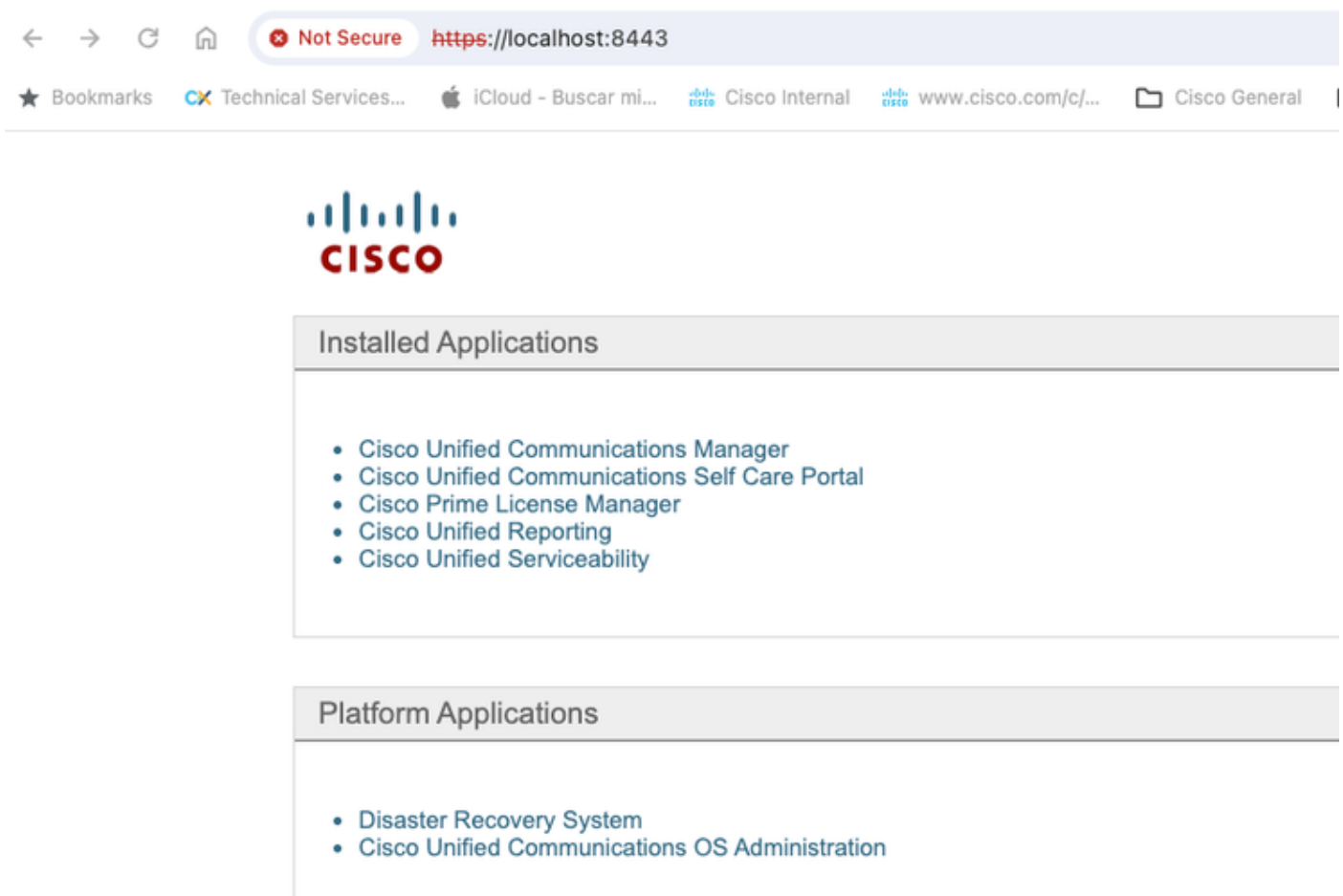
```
<#root>
```

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

Schritt 3: Öffnen Sie den Browser, und geben Sie die URL mit dem in Schritt 2 konfigurierten Port ein: <https://localhost:8443>

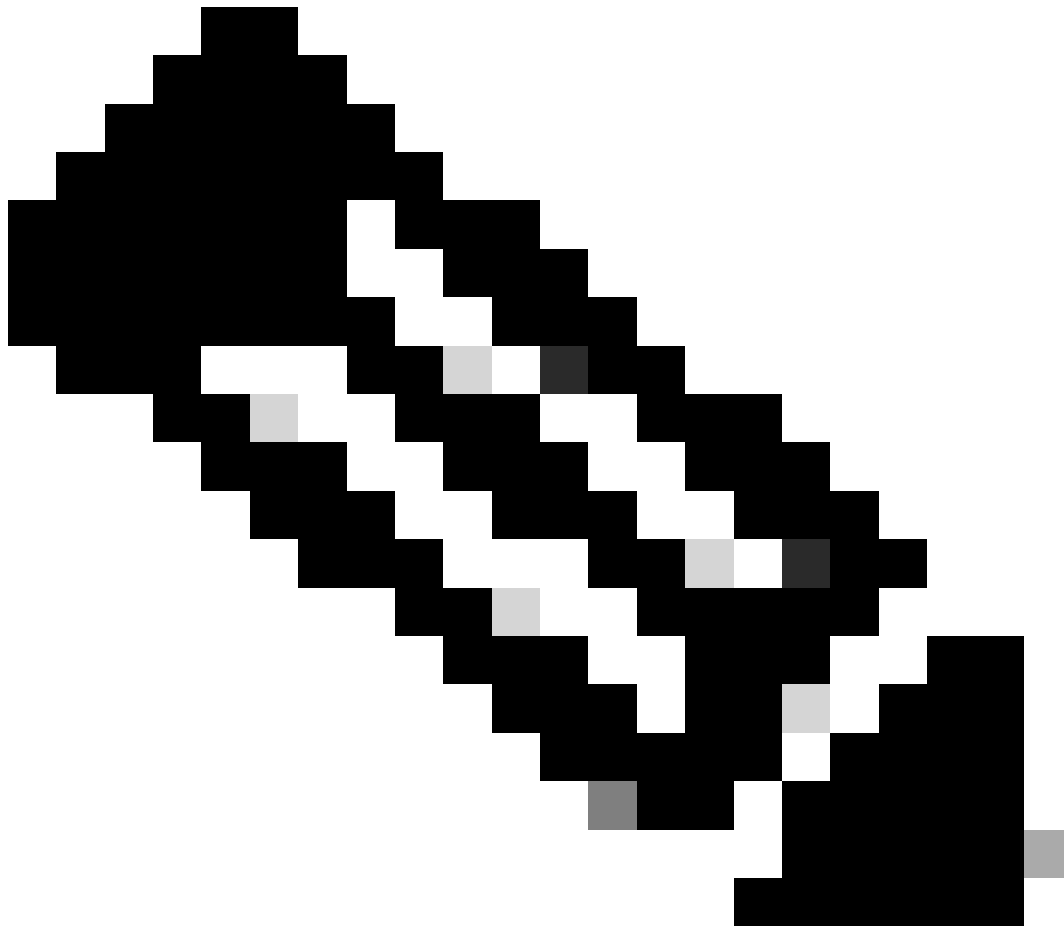
Auf die grafische Benutzeroberfläche des Geräts kann jetzt zugegriffen werden.



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



Anmerkung: Um auf die grafische Benutzeroberfläche des Produkts zugreifen zu können, benötigen Sie die Anmeldeinformationen. Es wird daher empfohlen, dass der Benutzer ein schreibgeschütztes Benutzerkonto für den Zugriff erstellt.

Protokollsammlung

- RTMT

Schritt 1: Überprüfen Sie, ob der Port 8443 in den für das Gerät konfigurierten TCP Forwarded-Ports aufgeführt ist.

```
<#root>
```

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

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

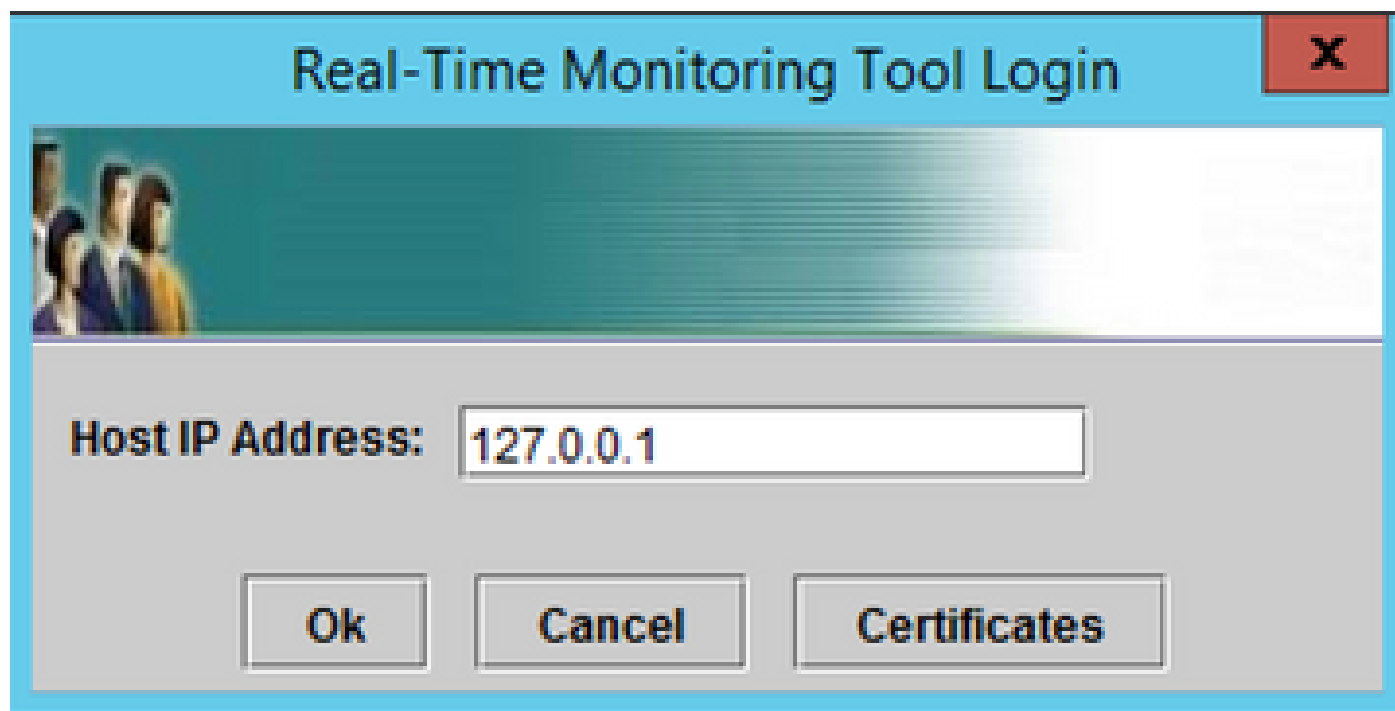
Schritt 2: Konfigurieren Sie den gleichen Port 8443 wie den lokalen Port, der dem Port 8443 als Zielport des Geräts zugeordnet werden soll.

<#root>

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

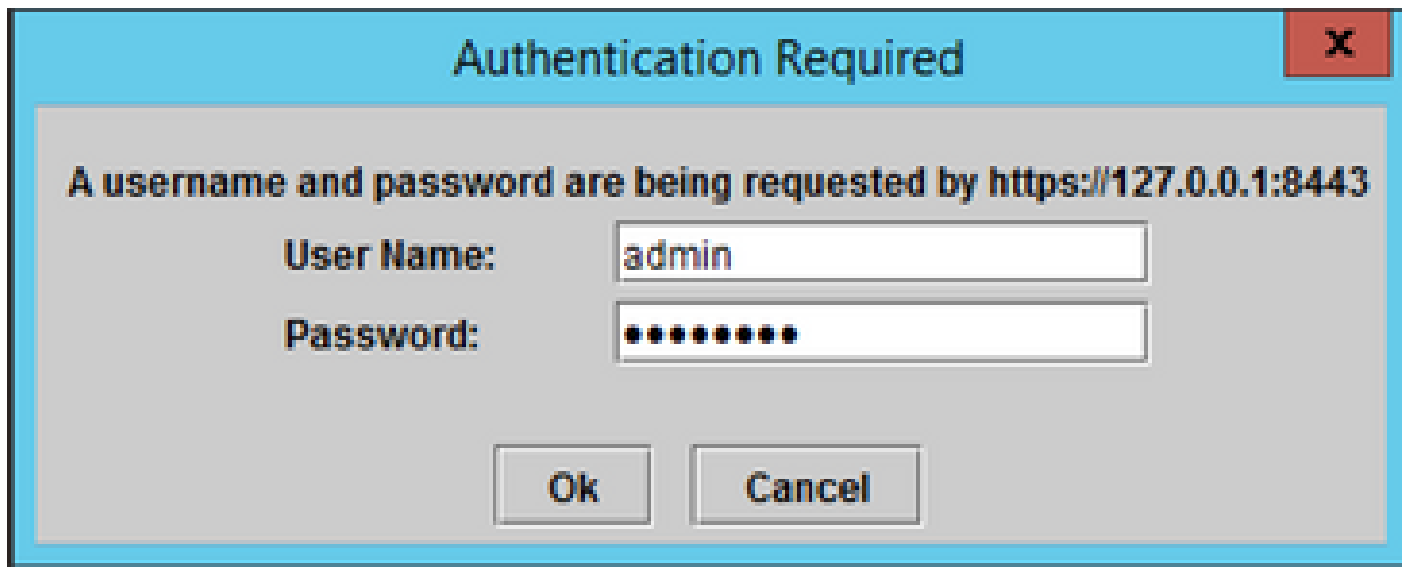
```
>>> cucm.forward_tcp_port(8443,8443)
[RUNNING] <radkit_client.sync.port_forwarding.TCPSocketForwarder object at 0x1077defa0>
-----
status          RUNNING
serial          None
device_name     cesavilacucm
local_port      8443
destination_port 8443
#active         0
#failed         0
#closed     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

Schritt 3: Öffnen Sie RTMT, und geben Sie 127.0.0.1 in die Host-IP-Adresse ein. Diese verwendet automatisch den Port 8443.

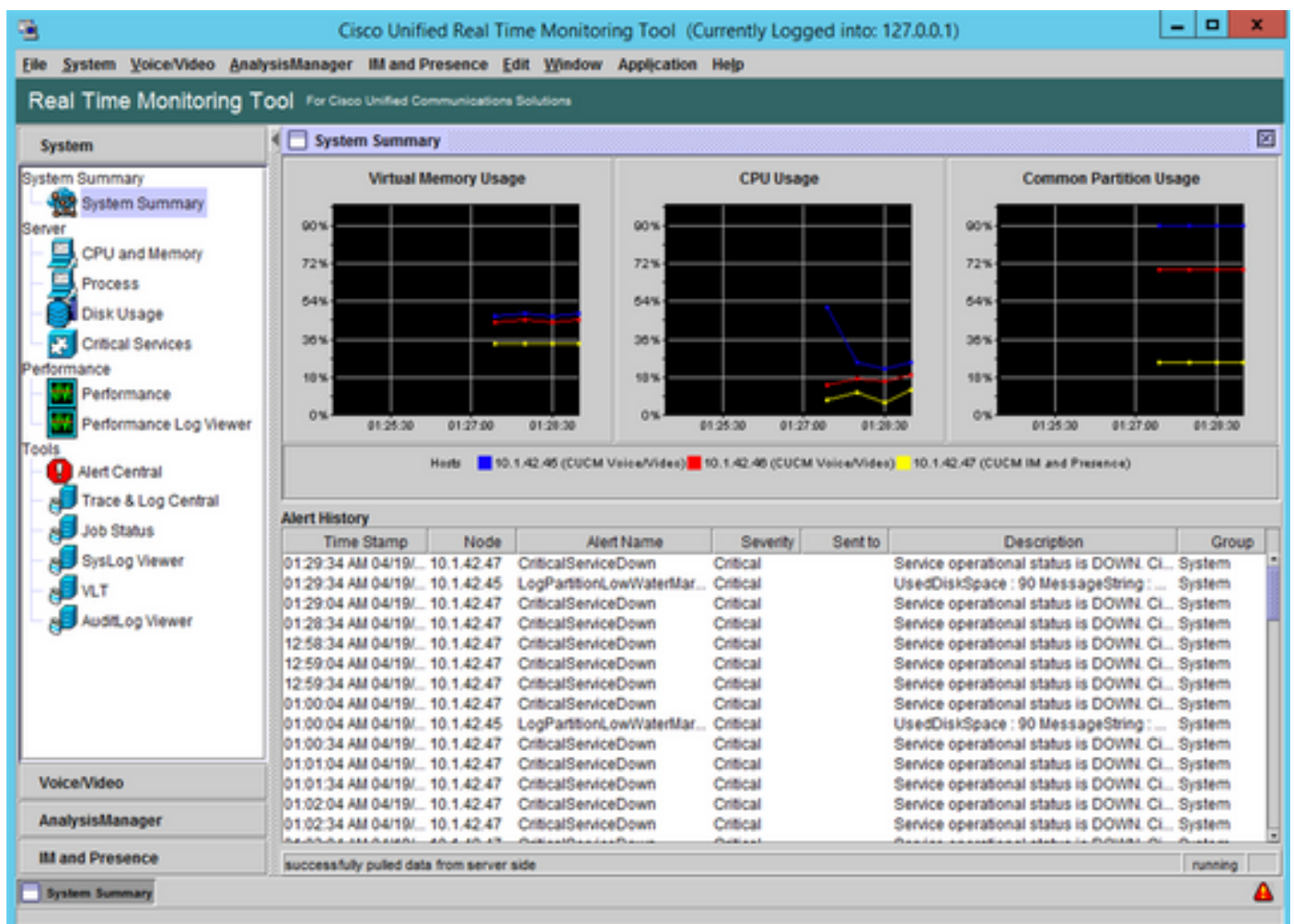


The image shows a 'Real-Time Monitoring Tool Login' dialog box. It has a blue title bar with a red 'X' button in the top right corner. Below the title bar is a banner image showing three people. The main area is light gray and contains a label 'Host IP Address:' followed by a text input field containing '127.0.0.1'. At the bottom, there are three buttons: 'Ok', 'Cancel', and 'Certificates'.

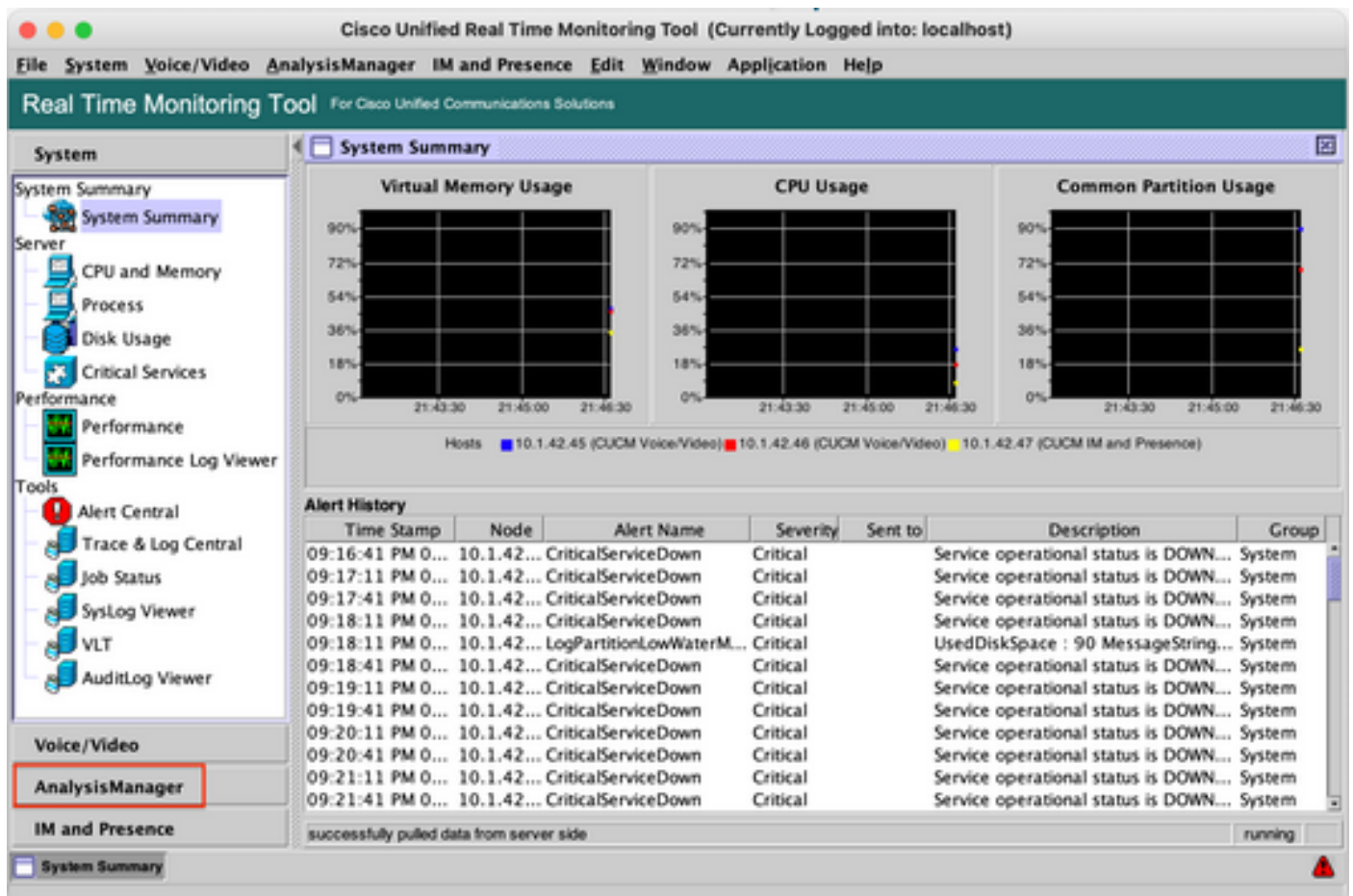
Schritt 4: Melden Sie sich mit den richtigen Anmeldeinformationen an.



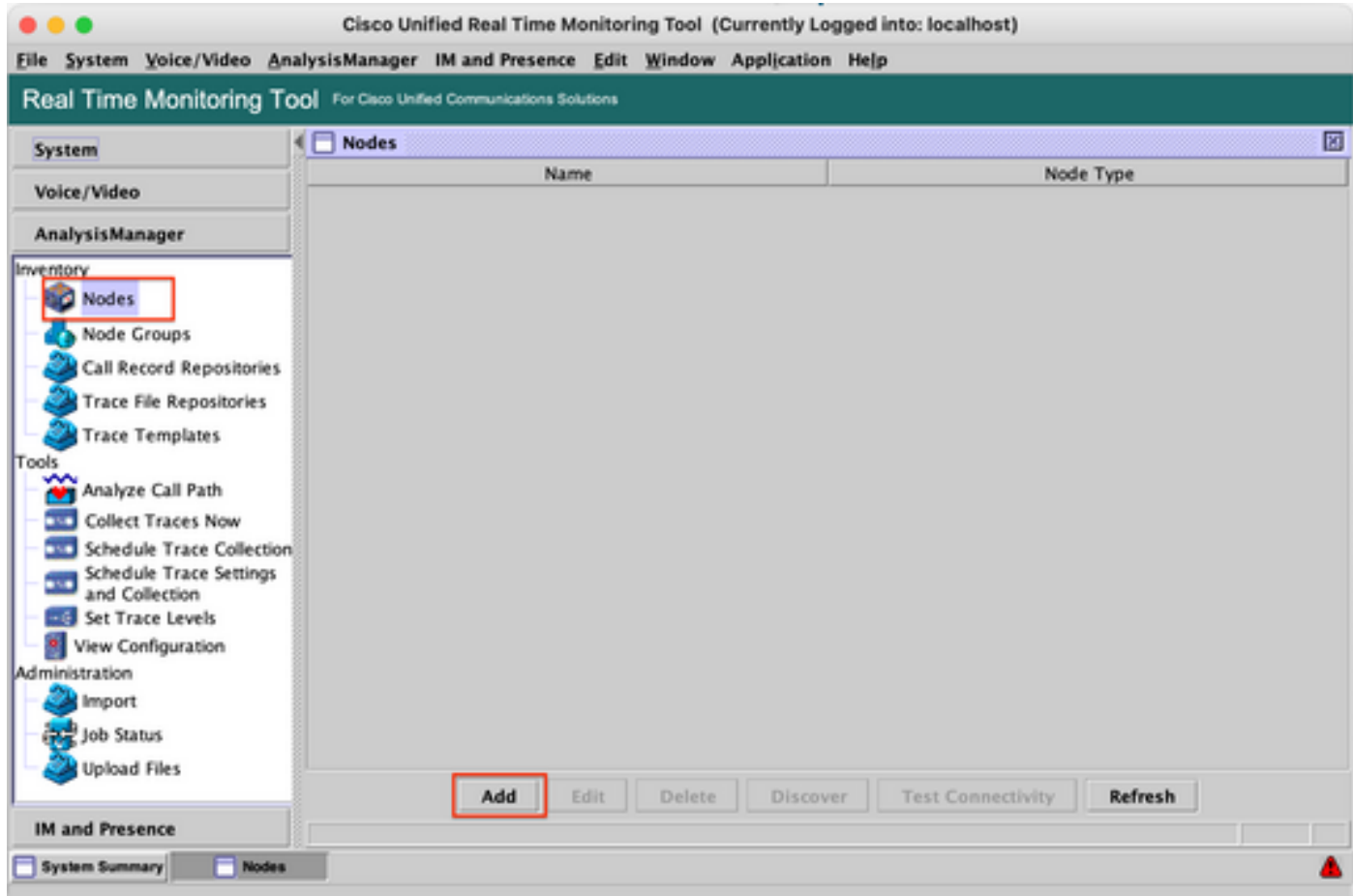
Schritt 5. RTMT wird angezeigt.



Schritt 6. Gehen Sie zu AnalysisManager im linken Bereich.



Schritt 7: Klicken Sie auf Nodes und Add, um die Details des Geräts zu konfigurieren, das mithilfe von localhost und dem weitergeleiteten TCP-Port hinzugefügt werden soll.



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

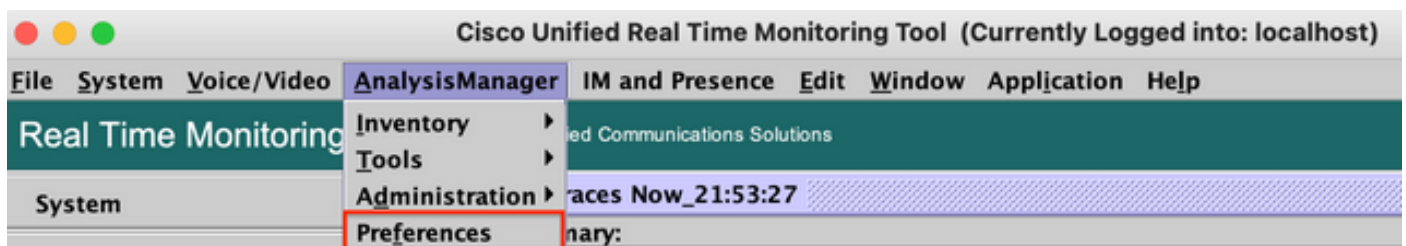
Associated Group ☒ AllNodes

Advanced...

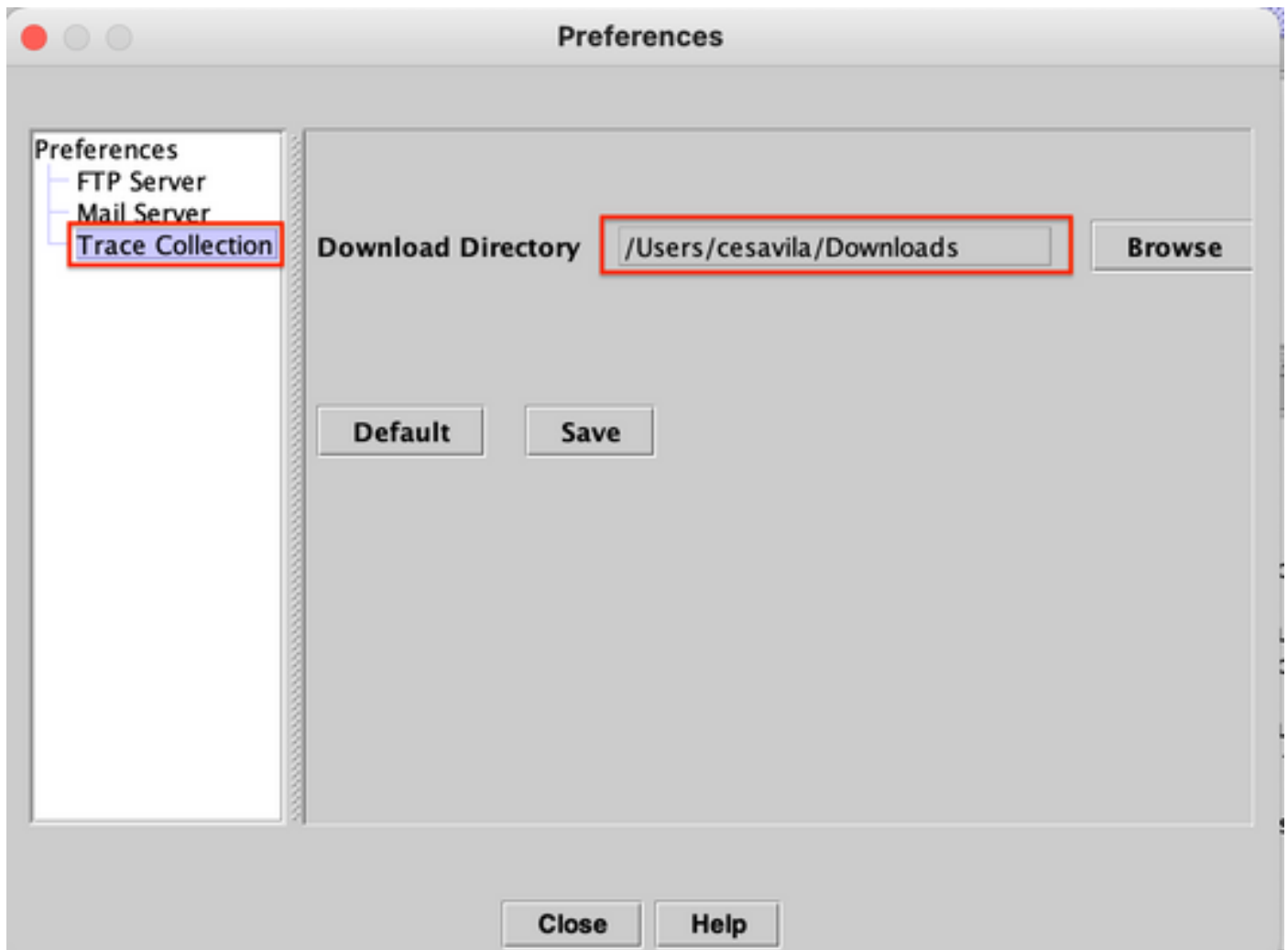
* Required Fields

Save **Cancel**

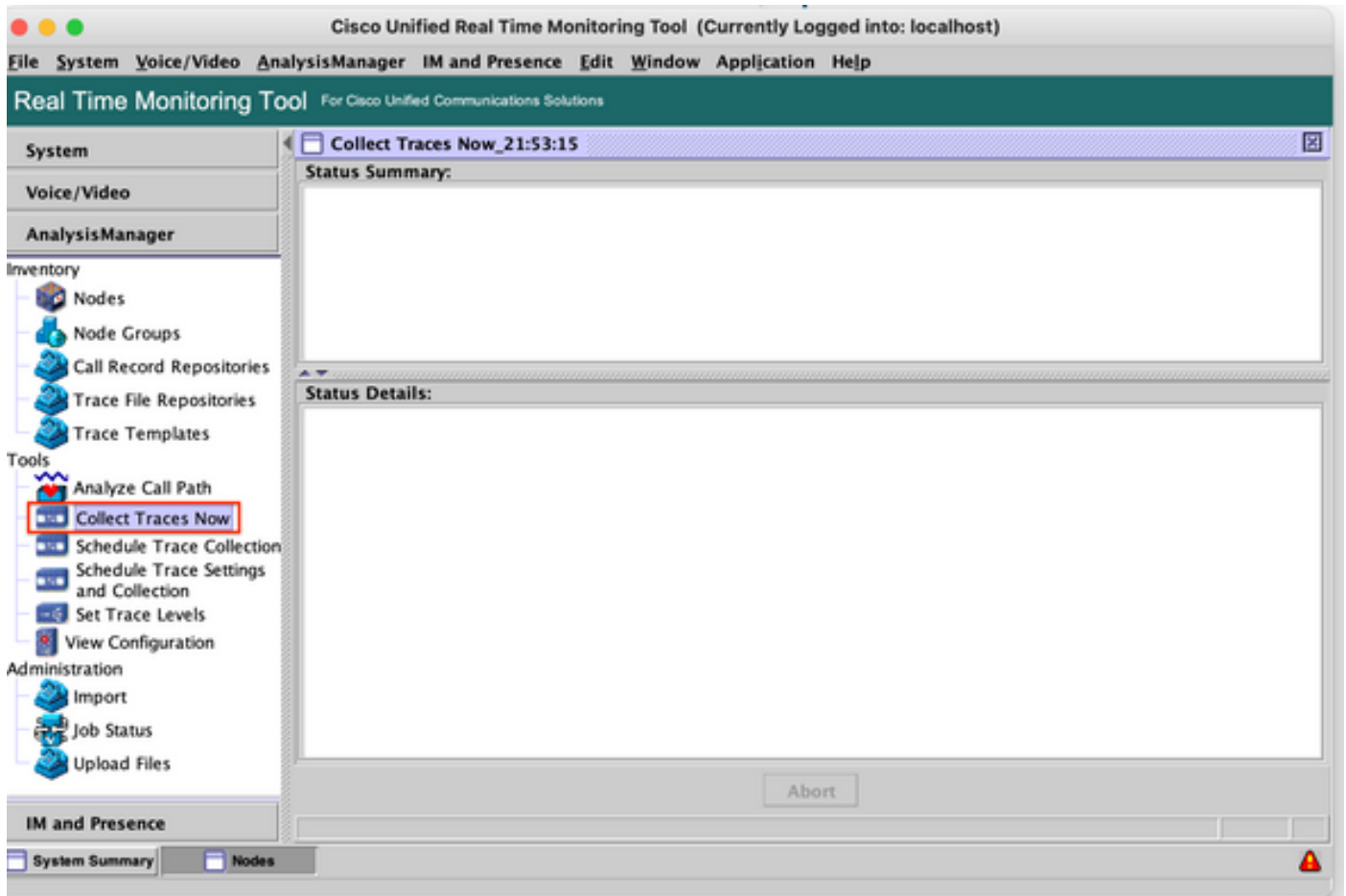
Schritt 8: Klicken Sie im Menü oben auf Analysis Manager, und wählen Sie Voreinstellungen.



Schritt 9. Gehen Sie zu Trace Collection und wählen Sie den korrekten Ordner, um die Protokolle herunterzuladen, klicken Sie auf Speichern und dann Schließen.



Schritt 10. Gehe zu Spuren sammeln jetzt.



Schritt 11: Wählen Sie die Option Node (Knoten), wählen Sie das Gerät aus, das in Schritt 7 hinzugefügt wurde, und klicken Sie auf Customize (Anpassen).

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...**

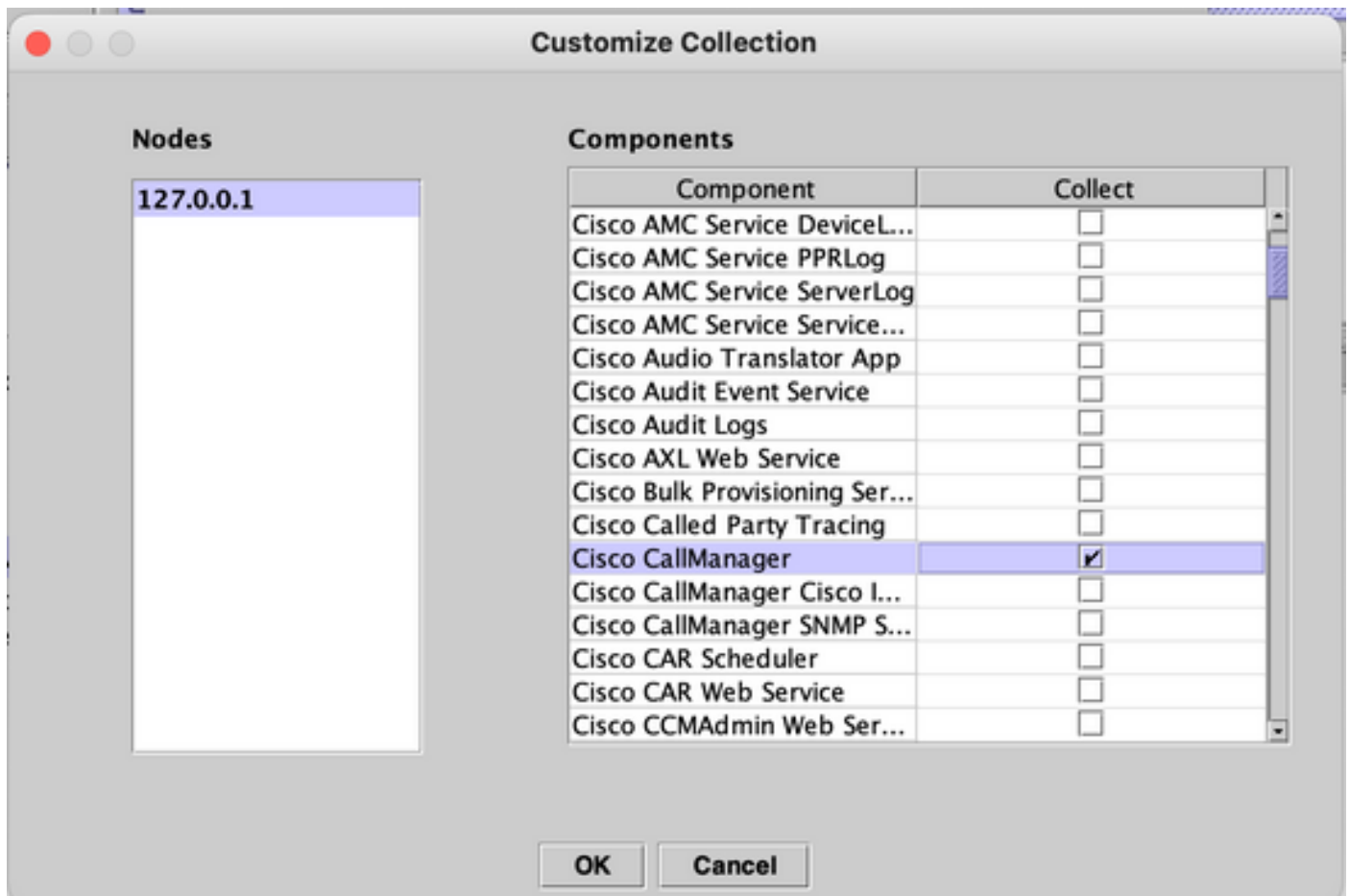
Start Time:

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

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

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

Schritt 12: Wählen Sie die Protokolle aus, die vom Gerät erfasst werden sollen, und klicken Sie auf OK.



Schritt 13. Wählen Sie schließlich Start Time (Startzeit) und End Time (Endzeit) der zu sammelnden Protokolle aus, und klicken Sie auf 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...

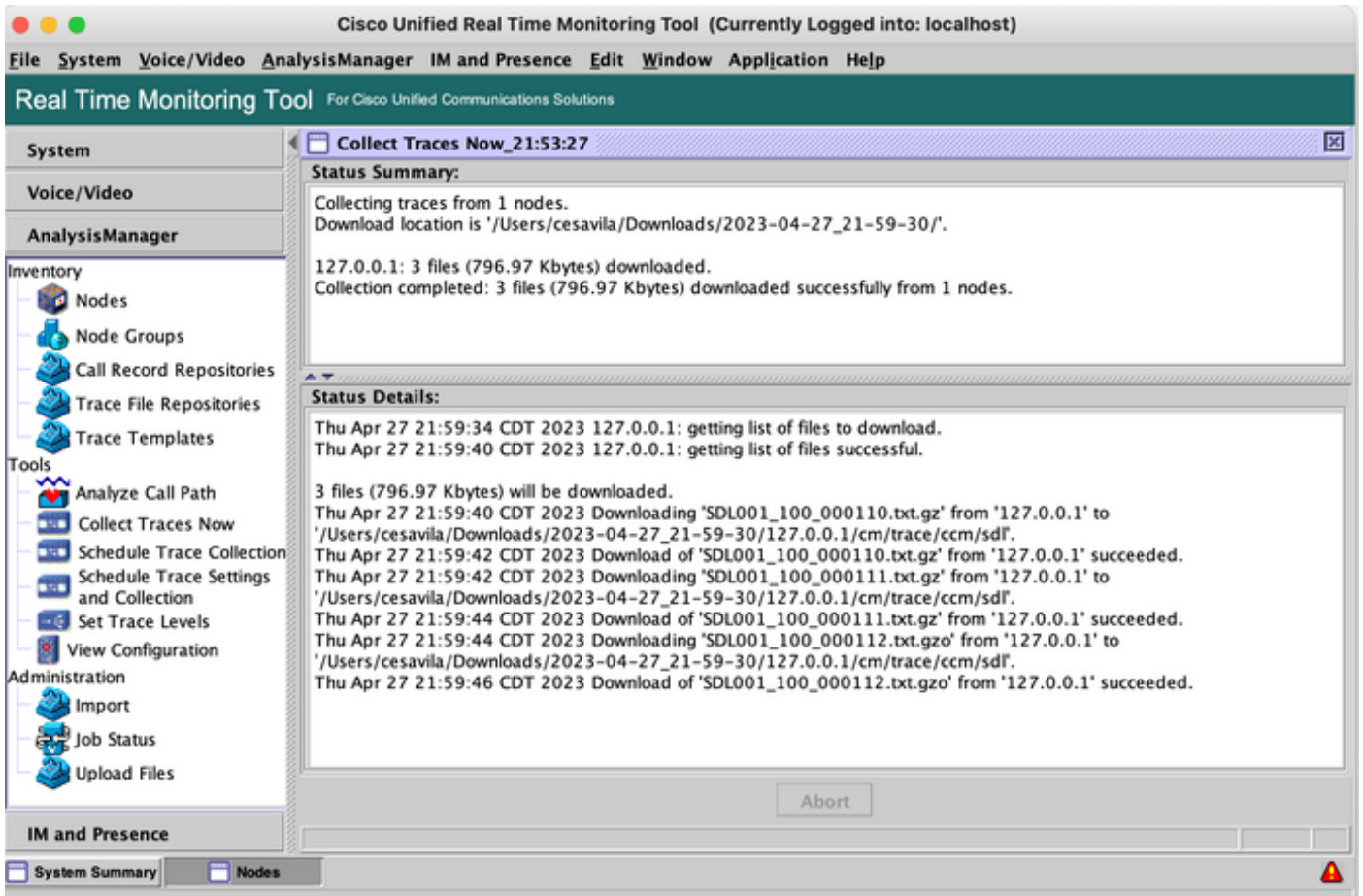
Start Time: 04-27-2023 21:00:00 ▼

End Time: 04-27-2023 21:53:27 ▼

Time Zone: (GMT-6:0)Central Dayl... ▼

View Summary **OK** Cancel Help

Schritt 14. Dateien werden erfolgreich auf den lokalen PC (RADKit Client PC) heruntergeladen.



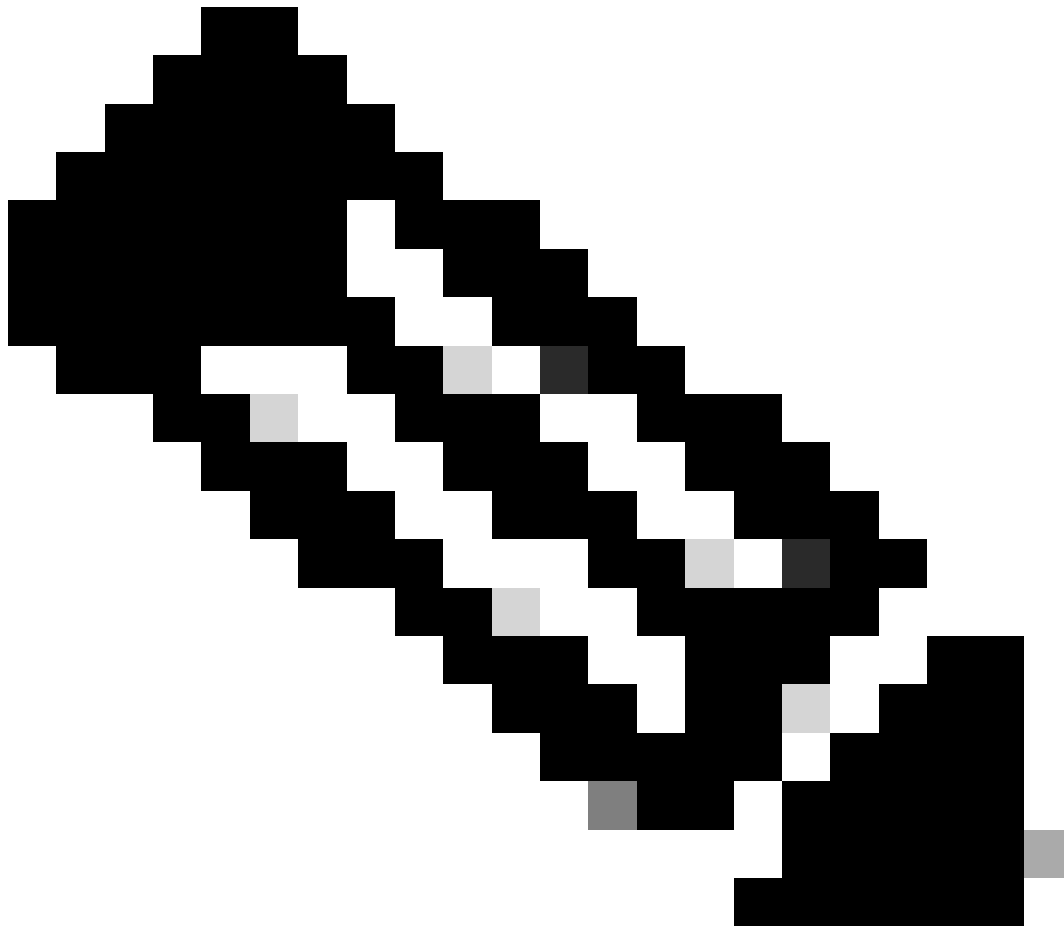
- SOAP-API

Die SOAP-API wird derzeit für CUCM unterstützt. Außerdem wird Swagger für CMS, Expressway, CVP usw. unterstützt.

Schritt 1: Stellen Sie sicher, dass die HTTP-Anmeldedaten dem RADKit-Dienst der Gerätekonfiguration hinzugefügt werden.

Schritt 2: Führen Sie den HTTP-Post-Befehl auf dem RADKit-Client aus, geben Sie den Ressourcenpfad an, fordern Sie den Text mit den erforderlichen Parametern und Headern an.

```
>>> r = cucm.http.post('/logcollectionservice2/services/LogCollectionPortTypeService', content = '''<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/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'])
>>>
```



Anmerkung: Die Postprozessoroption 'cucm-extract' wird verwendet, um die HTTP-Antwort-Header zu entfernen, damit das Protokoll in einer Datei gespeichert werden kann.

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

Schritt 3: Speichern Sie den Inhalt in einer Datei, um die Trace-Datei auf dem lokalen PC zu speichern.

<#root>

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

RADKit-Anwendungsfälle

Wie bereits hervorgehoben wurde, stellt RADKit eine sichere Verbindung zu den Netzwerkgeräten, einschließlich Collaboration-Servern, her, ohne dass es dazu eines WebEx Systems bedarf. Die Idee dahinter ist, einige der Herausforderungen im Zusammenhang mit der Datenerfassung zu vereinfachen, indem On-Demand-Zugriff auf die erforderlichen Geräte bereitgestellt wird.

Im Speziellen zu Collaboration-Bereitstellungen kann RADKit derzeit für eine Vielzahl von Problemen sehr nützlich sein, z. B.:

- DB-Replikationsprobleme.
- Verfahren zur Erneuerung von Zertifikaten.
- Systemstatusprüfung.
- Konfigurationsvalidierung in GUI/CLI.
- Protokollerfassung über Webschnittstelle (z. B. CER, Expressway, CIMC usw.)
- Debugging-Protokolle über CLI auf Sprach-Gateways.

Zugehörige Informationen

- RADKit-Hauptseite <https://radkit.cisco.com/>
- Externe RADKit-Support-Seite <https://community.cisco.com/t5/radkit-discussions/bd-p/disc-radkit>

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.