

협업 환경에서 RADKit 설정

목차

소개
요구 사항
사용되는 구성 요소
용어
RADKit 아키텍처
RADKit 설치
RADKit 서비스(사용자측)
온보드
장치 추가
원격 사용자 권한 부여
RADKit 클라이언트(TAC 측)
로그인
SSH 액세스
GUI 액세스
HTTP 프록시
포트 전달
로그 수집
RTMT
SOAP API
RADKit 활용 사례
관련 정보

소개

이 문서에서는 RADKit를 설정하는 단계에 대해 설명하고 Collaboration 제품에서 RADKit를 사용하기 시작하는 데 필요한 컨피그레이션을 보여줍니다.

요구 사항

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

- 모든 VOS Collaboration 제품에 대한 기본 지식
- CLI/SSH 액세스에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Unified Communications Manager 12.5 및 14.0

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

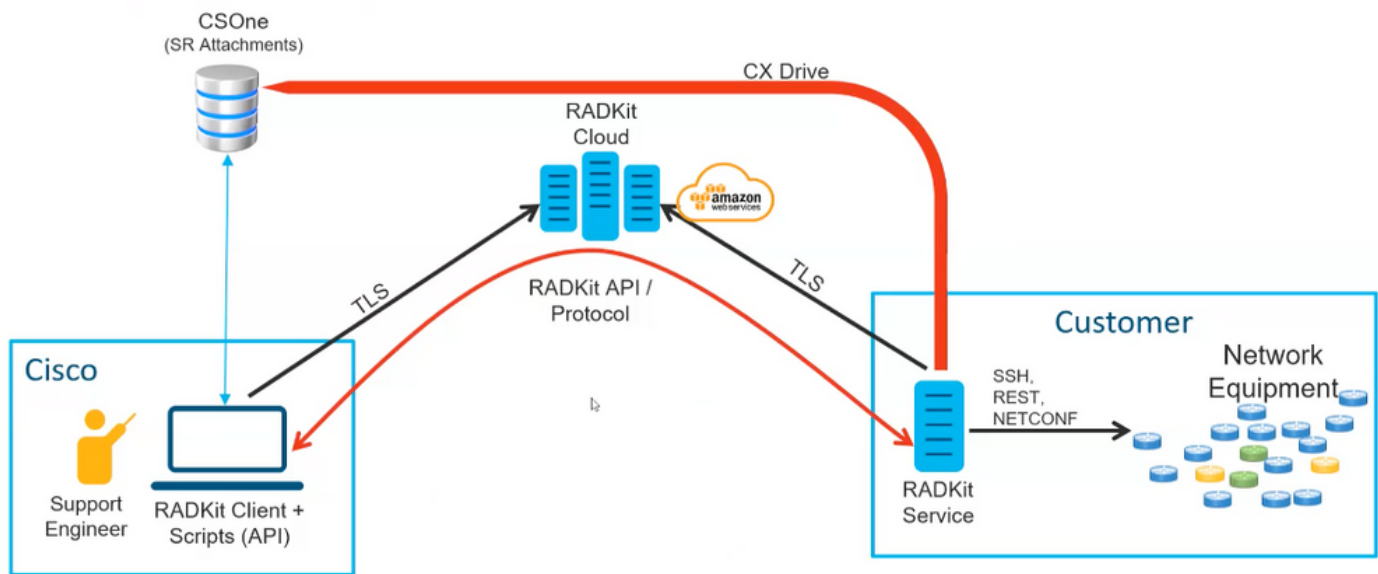
용어

RADKit: Cisco TAC 엔지니어 및 파트너에게 사용자 장치에 대한 보안 원격 액세스를 제공하는 커넥터입니다. SSH 또는 HTTP/HTTPS와 같은 디바이스와 상호 작용하는 여러 프로토콜을 지원합니다.

RADKit 서비스: 이것은 서버 측입니다. 사용자가 처리하고 전체적으로 관리합니다. 서버 측에서 사용자 제어를 통해 누가 얼마나 오랫동안 장치에 액세스할 수 있는지 알 수 있습니다. Radkit Service는 네트워크에 있는 디바이스에 대한 액세스를 제공하려면 해당 디바이스에 대한 연결이 있어야 합니다.

RADKit 클라이언트: 이것은 클라이언트 측입니다. 사용자 네트워크의 장치에 연결하는 데 사용되는 PC입니다.

RADKit 아키텍처



RADKit 아키텍처

RADKit 설치

1단계. <https://radkit.cisco.com>으로 [이동하고](#) Downloads(다운로드)를 클릭한 다음 릴리스 폴더로 이동합니다.

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

-

2단계. 최신 릴리스를 클릭합니다.

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

-

3단계. OS 시스템에 따라 올바른 파일을 다운로드합니다.

INDEX OF /DOWNLOADS/RELEASE/1.4.9/

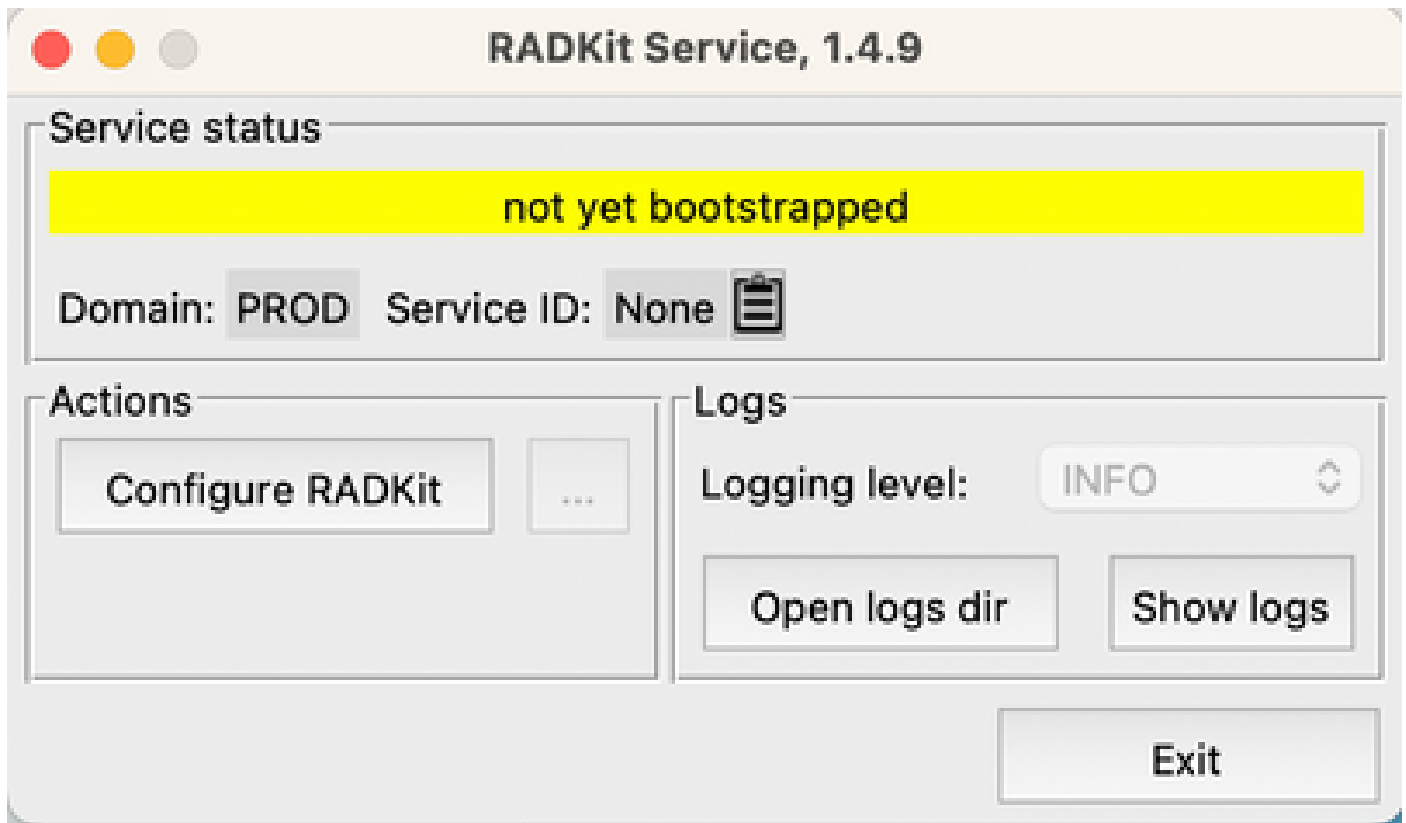
../		
docs/	04-Apr-2023 11:45	-
cisco_radkit_1.4.9_doc_html.tgz	04-Apr-2023 11:43	8003863
cisco_radkit_1.4.9_macos_arm64_signed.pkg	11-Apr-2023 10:41	74142354
cisco_radkit_1.4.9_macos_x86_64_signed.pkg	11-Apr-2023 10:41	77265560
cisco_radkit_1.4.9_pip_linux.tgz	04-Apr-2023 11:49	146189048
cisco_radkit_1.4.9_pip_macos.tgz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

4단계. PC 또는 서버에서 설치 프로그램을 실행합니다. 설치 과정에서 Radkit는 세 가지 애플리케이션을 설치해야 합니다. Radkit Service, Radkit Client 및 Radkit 네트워크 콘솔.

RADKit 서비스(사용자측)

온보드

1단계. RADKit 서비스 구성을 시작하려면 Applications(애플리케이션)로 이동하여 RADKit Service(RADKit 서비스)를 찾습니다. 처음 실행할 때 "아직 부트스트랩되지 않음" 메시지가 표시됩니다.



2단계. Configure RADKit(RADKit 구성)을 클릭하면 브라우저가 자동으로 URL <https://localhost:8081/bootstrap>으로 [팔업됩니다](#).

- 수퍼 관리자 사용자의 비밀번호를 생성하고 Submit(제출)을 클릭합니다.
- 이 수퍼관리자 사용자 이름 및 비밀번호는 서비스를 시작하거나 구성할 때마다 요청됩니다.

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 *

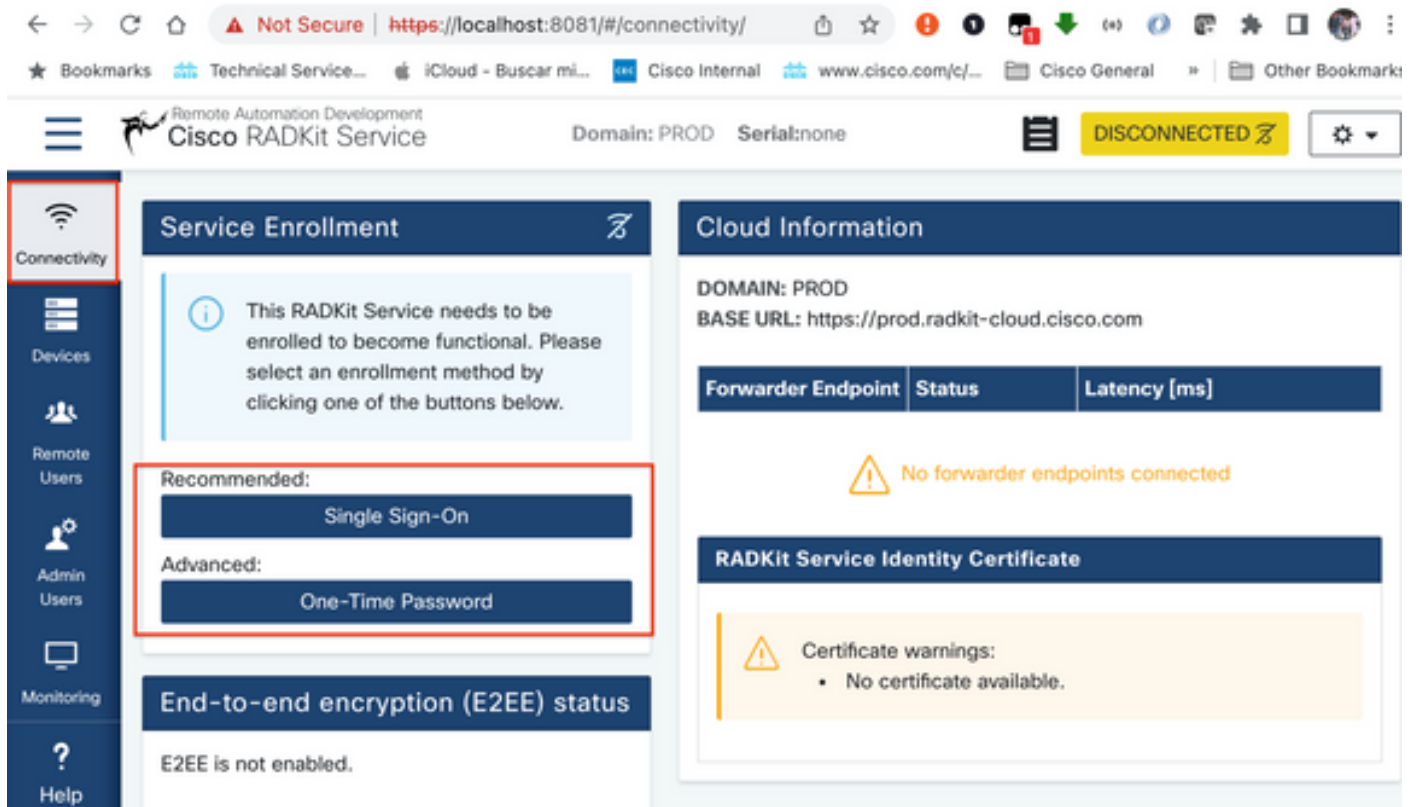
PASSWORD REQUIREMENTS:

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

Submit

3단계. Submit(제출)을 클릭하면 브라우저가 <https://localhost:8081/#/connectivity/>으로 [리디렉션합니다](#).

Connectivity(연결) > Service Enrollment(서비스 등록)에는 두 가지 인증 방법이 있습니다. 단일 Sing-On 및 일회용 비밀번호입니다.



4단계. CEC를 제공하는 Single Sign-On을 사용할 수 있습니다.

Single Sign-On Enrollment



Checking prerequisites



Email address



Provide email address for SSO login:

Submit



Connecting to the Access Service



OAuth connect



Waiting for SSO



Requesting service certificate OTP



Requesting service certificate

5단계. 마법사를 완료하고 "새 ID로 등록된 서비스: xxxx-xxxx-xxxx"와 함께 Close(닫기)를 클릭하면 서비스가 Connected(연결됨)로 표시됩니다.



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

Close



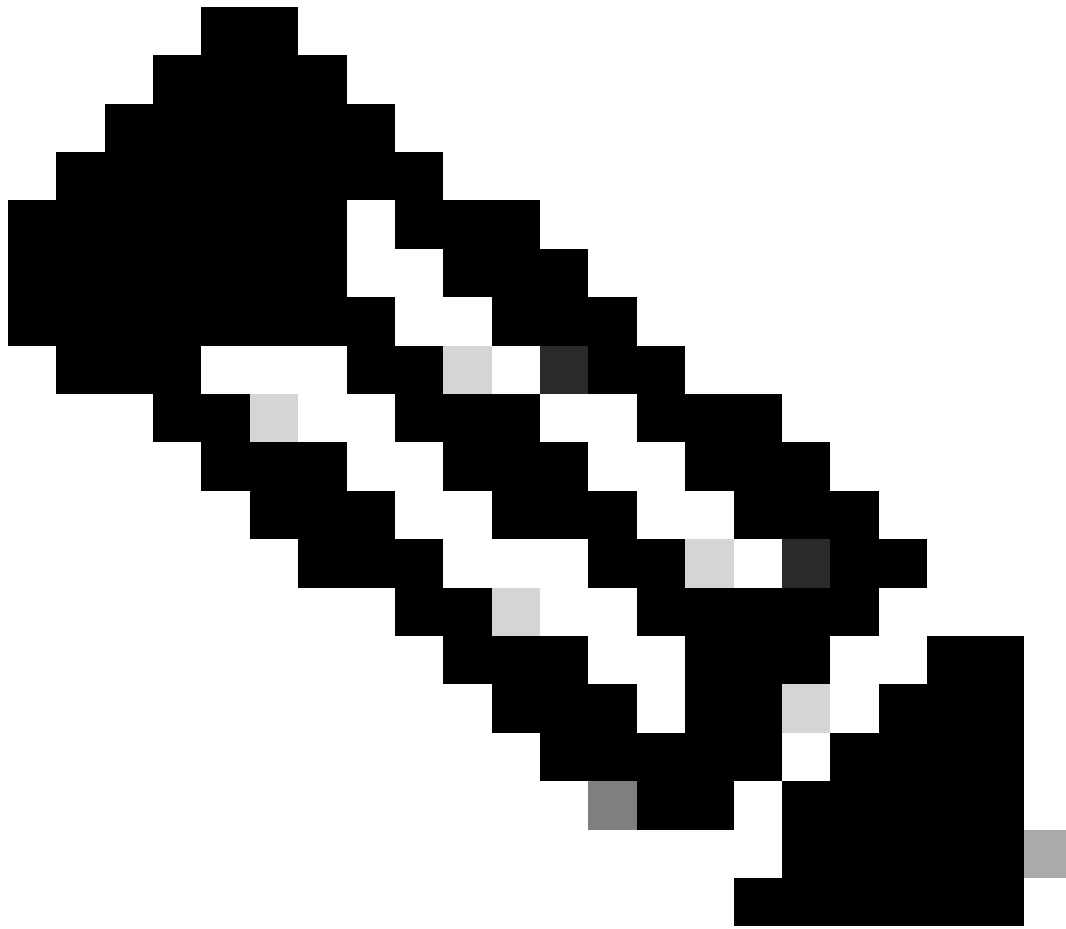
Remote Automation Development
Cisco RADKit Service

Domain: PROD Serial: k331-0evx-s94g

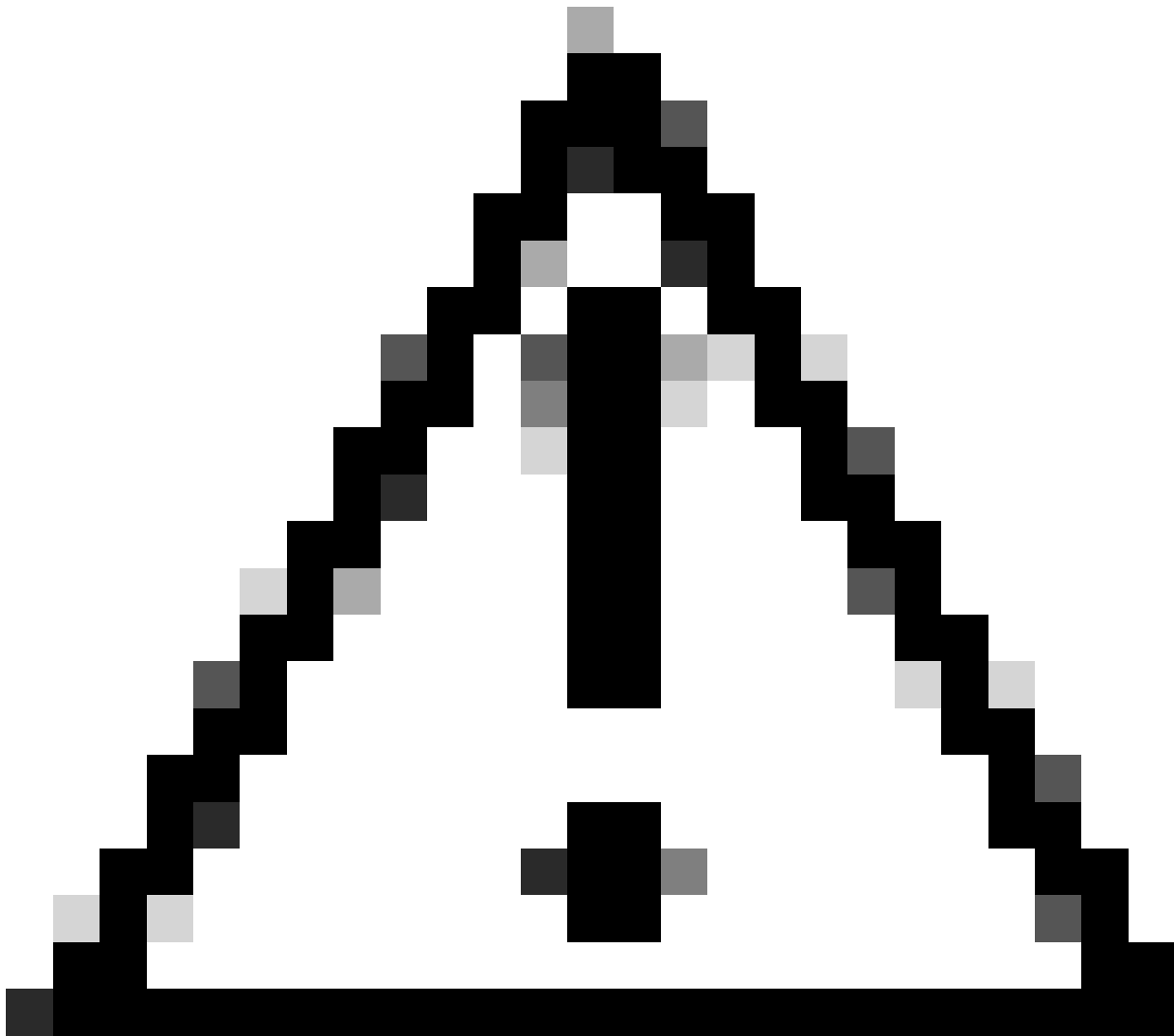


CONNECTED





참고: RADKit 서비스를 활성화하려면 Cisco 계정이 필요합니다.

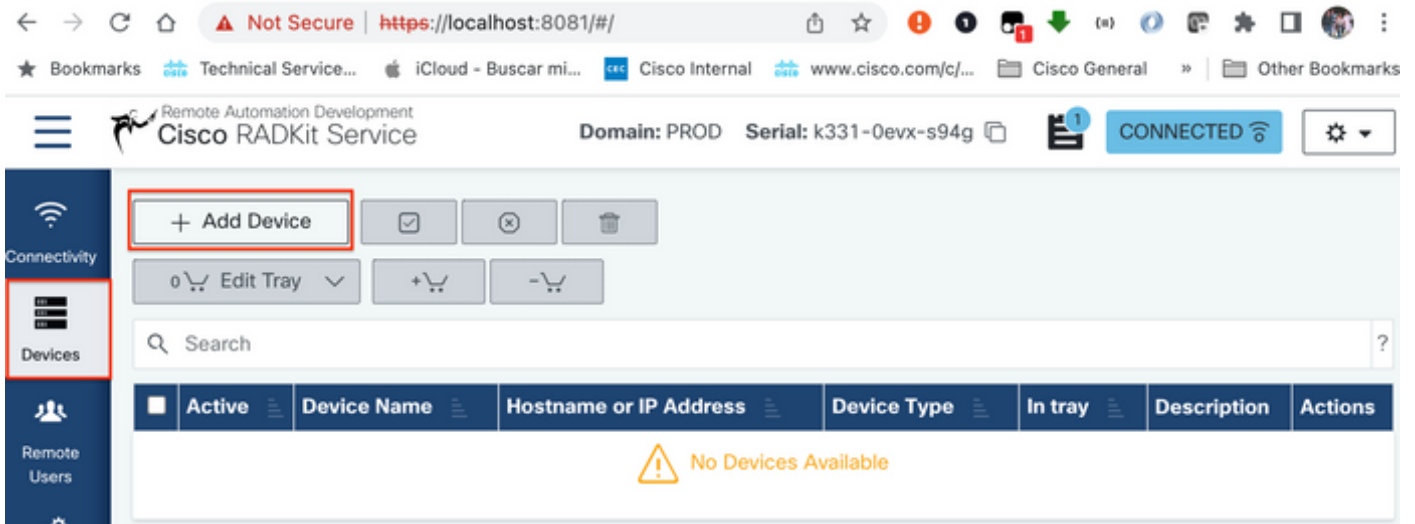


주의:

- RADKit 서비스가 실행 중인 서버에서 프록시를 정의해야 하는 경우, 서버/PC 자체에서 프록시를 정의하는 것과는 별도로 RADKit 서비스가 `RADKIT_CLOUD_CLIENT_PROXY_URL=http://proxy.example.com:80`을 작동하기 위한 환경 변수도 정의해야 [합니다](#).

장치 추가

1단계. Devices(디바이스)로 이동하고 Add Device(디바이스 추가)를 클릭합니다.



2단계. 다음 세부 정보를 구성해야 합니다.

- 디바이스 이름
- 관리 IP 주소 또는 호스트 이름
- 디바이스 유형

또한 RADKit 클라이언트에서 액세스해야 하는 디바이스에서 사용하는 포트인 Forwarded TCP 포트를 구성해야 합니다. 이 예에서 사용되는 포트는 GUI 액세스용 443 및 RTMT용 8443입니다.

마지막으로, 사용 가능한 관리 프로토콜(이 경우 Terminal 및 HTTP)을 선택합니다.

Add New Device ✕

Device Name^{*}(as it will appear in RADKit)?

Management IP Address or Hostname[?]

Forwarded TCP ports ?

Device Type^{*}

Jumphost Name

Description

?

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

3단계. 각 관리 프로토콜에 대해 올바른 설정을 구성하고 Add & Close(추가 및 닫기)를 클릭합니다.

4단계. 추가된 디바이스는 디바이스 목록에 표시되어야 하며, 원격 액세스에 대해 활성화/비활성화할 수 있습니다.

원격 사용자 권한 부여

1단계. RADKit 서비스에 구성된 디바이스에 대한 사용자 액세스 권한을 부여하려면 Remote Users(원격 사용자)로 이동하여 Add Users(사용자 추가)를 선택합니다.

2단계. 사용자 세부사항을 구성합니다.

- 이메일 주소
- 전체 이름(선택 사항)
- 사용자를 활성화합니다.
- 활성화를 수동으로 제어해야 하는지 여부를 지정하거나 해당 사용자에게 액세스 권한을 부여할 시간 프레임을 설정합니다.

Add New User



User Email*

cesavila@cisco.com

Full Name

Cesar Avila

Description

Activate this user

USER ACCESS POLICY

Manual

Time slice (h/m):

2400

Clear form

Add & close

Add & continue

3단계. Add & Close(추가 및 닫기)를 선택합니다.

RADkit 클라이언트(TAC 측)

로그인

1단계. 클라이언트 PC에서 Applications(애플리케이션)로 이동하여 RADkit Client(RADkit 클라이언트)를 찾습니다.

2단계. SSO 로그인으로 클라이언트 인스턴스를 생성합니다.

```
<#root>
```

```
>>>
```

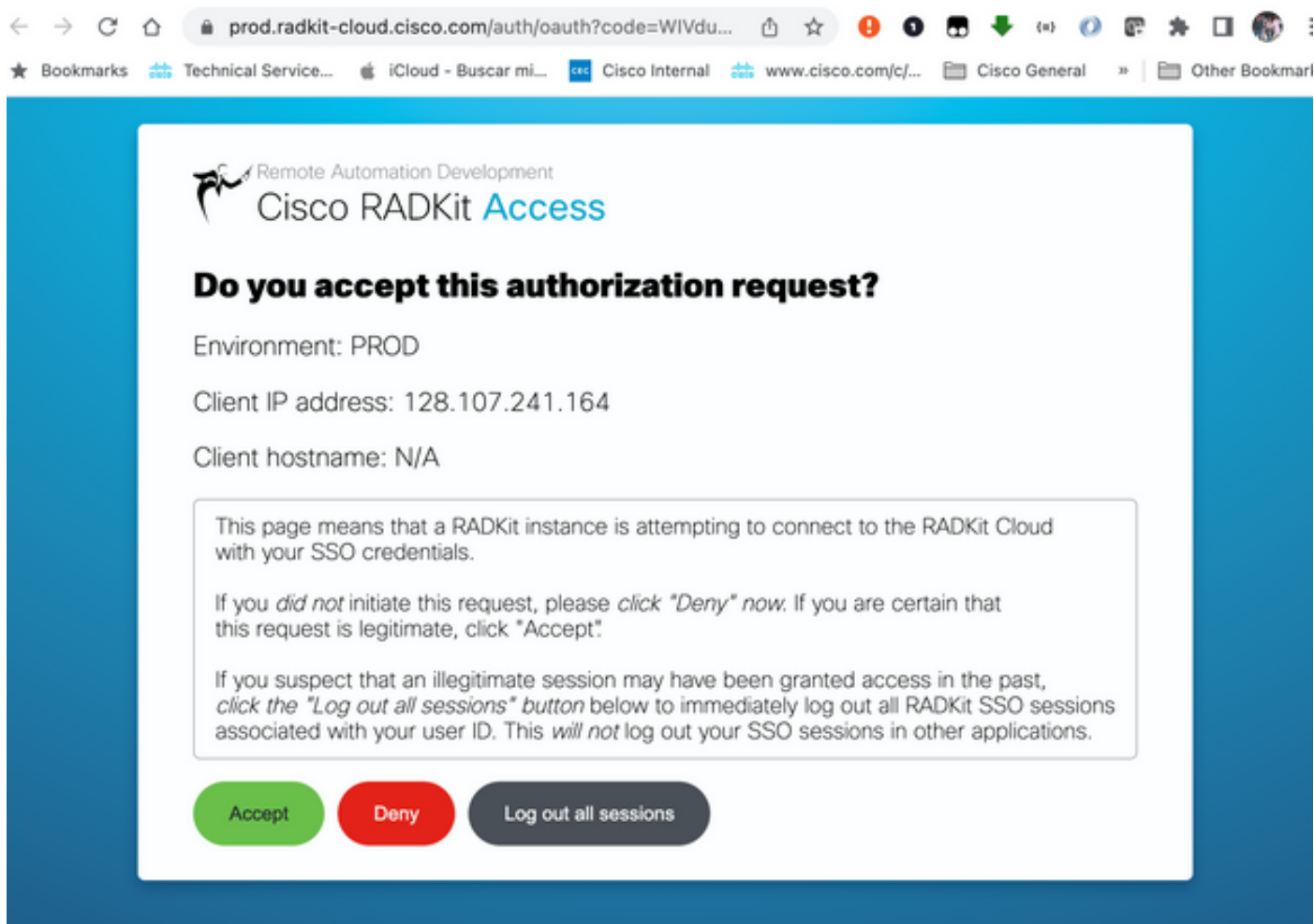
```
client = sso_login("cesavila@cisco.com")
```

```
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")
█
```

3단계. 브라우저에서 자동으로 열리는 SSO 권한 부여 요청을 수락합니다.



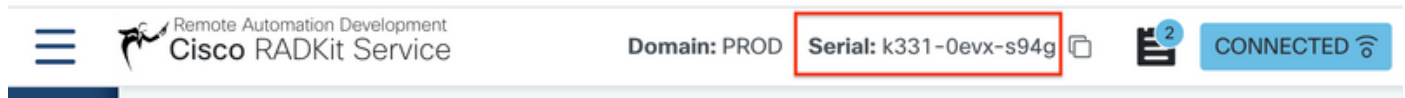
Authentication result: Success

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

4단계. RADKit 서비스 - 온보딩 단계에서 사용자가 생성한 일련 번호를 사용하여 서비스 인스턴스를 생성합니다.

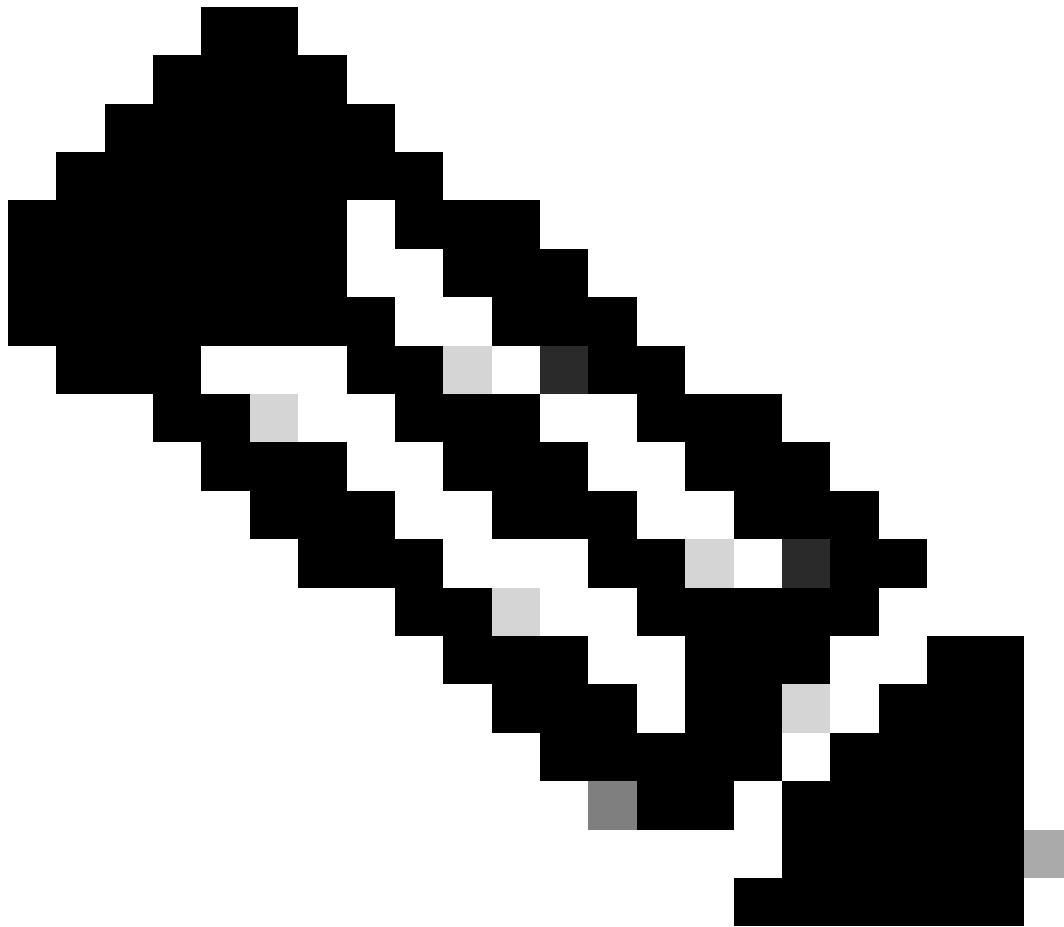


<#root>

>>>

```
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/']
```



참고: 서비스는 무엇이든 될 수 있는 변수입니다.

5단계. 액세스 가능한 디바이스를 확인합니다.

<#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
```

인벤토리 목록을 새로 고치려면 update_inventory 명령을 사용합니다.

```
<#root>
```

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

SSH 액세스

1단계. 인벤토리 목록에서 객체를 생성합니다.

```
<#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   Untouched inventory from service k331-0evx-s94g.
False
>>>
>>> cucm = service.inventory["cesavilacucm"]
```

2단계. interactive 명령을 사용하여 SSH 세션을 시작합니다.

```
<#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.

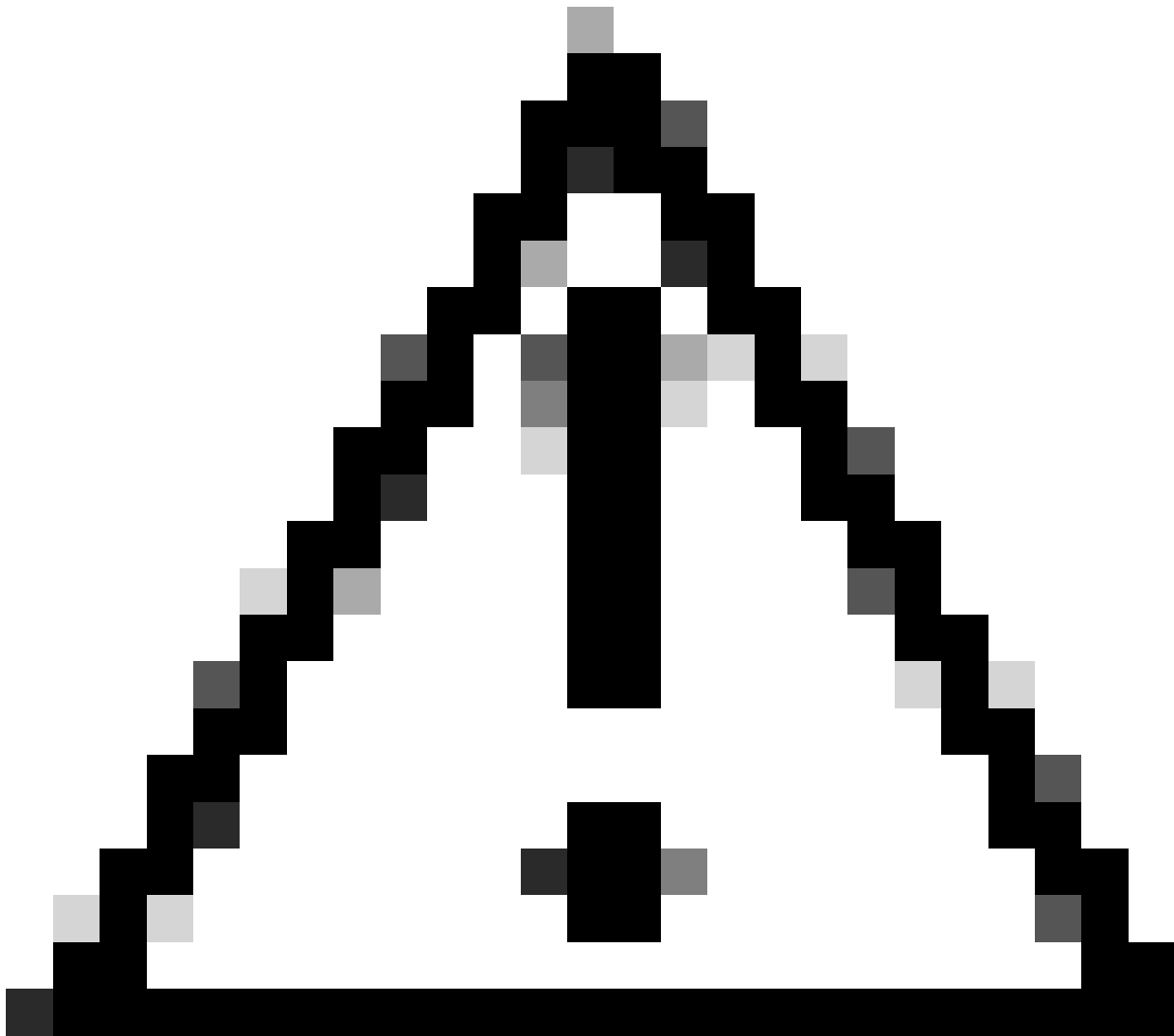
Command Line Interface is starting up, please wait ...

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:|
```

3단계. 이제 디바이스를 정상적으로 관리할 수 있습니다.



주의:

- 사용자 환경에서 작업할 때는 항상 Cisco의 책임에 유의하십시오.
- RADKit는 데이터 수집 도구로 사용되어야 합니다.
- 사용자 권한 없이 변경하지 마십시오.
- 모든 결과를 사례 노트에 기록하십시오.

GUI 액세스

- HTTP 프록시

1단계. HTTP 자격 증명이 디바이스 컨피그레이션의 RADKit 서비스에 추가되었는지 확인합니다.

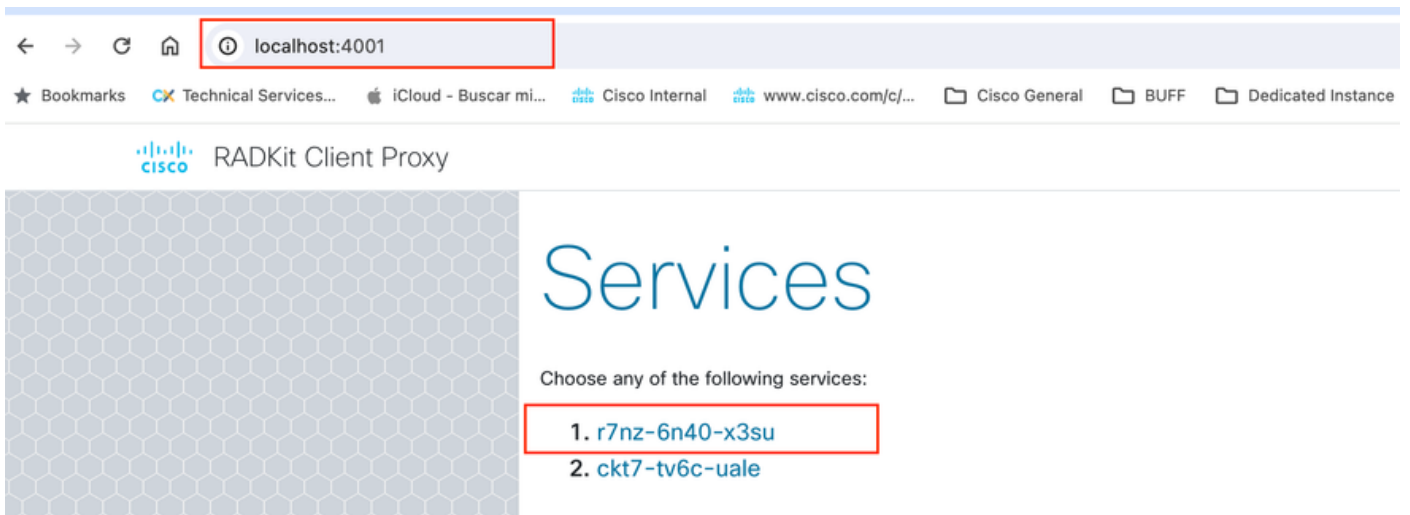
2단계. Radkit 클라이언트에서 HTTP 프록시를 시작하고 프록시에 연결하는 데 사용되는 로컬 포트를 정의합니다.

<#root>

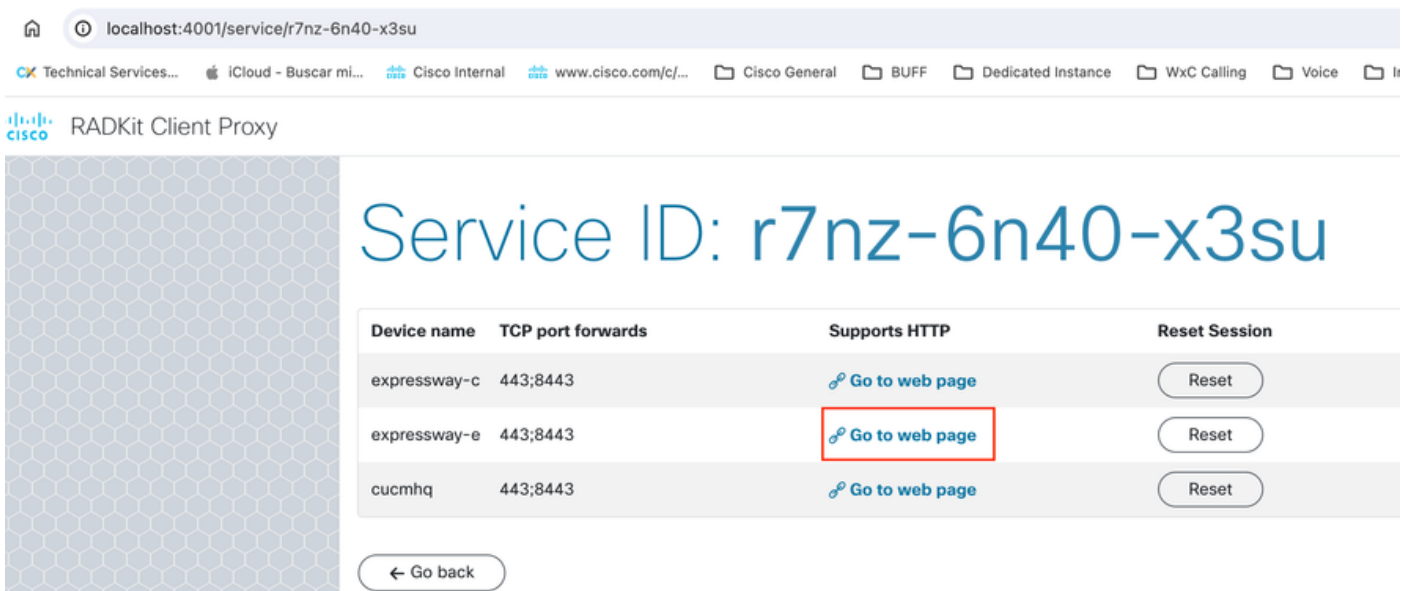
```
>>> http_proxy = client.start_http_proxy(4001)
```

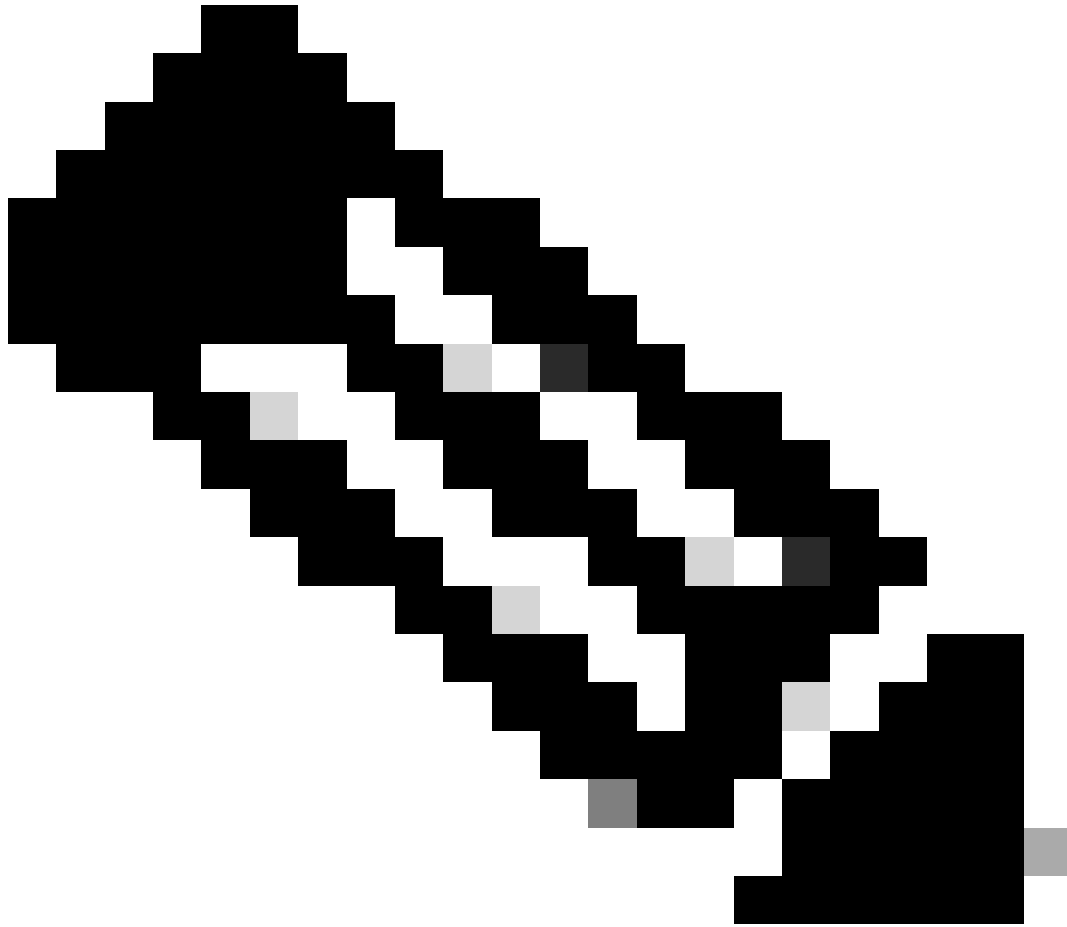
```
>>>
>>> http_proxy = client.start_http_proxy(4001)
22:24:19.981Z WARNI | HTTP proxy is NOT PROTECTED by username/password
>>> █
```

3단계. 웹 브라우저에서 <https://localhost:4001>으로 [이동하고](#) 연결할 서비스를 선택합니다.



4단계. 올바른 장치에서 웹 페이지로 이동 옵션을 클릭하여 해당 웹 페이지에 연결합니다.





참고: RADKit 클라이언트에서 HTTP 프록시를 처음 설정하는 경우 Reset for each Devices(각 디바이스에 대해 재설정) 옵션을 클릭한 후 Device Web Page(디바이스 웹 페이지)를 여는 것이 좋습니다.

5단계. 웹 페이지가 표시됩니다.

← → ↻ 🏠 ⚠ 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

- 포트 전달

1단계. 디바이스에 대해 구성된 TCP 전달 포트를 확인합니다.

<#root>

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

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

2단계. 로컬 포트를 디바이스의 대상 포트와 매핑하도록 구성합니다. 로컬 포트를 사용하여 디바이스 GUI에 액세스해야 합니다.

<#root>

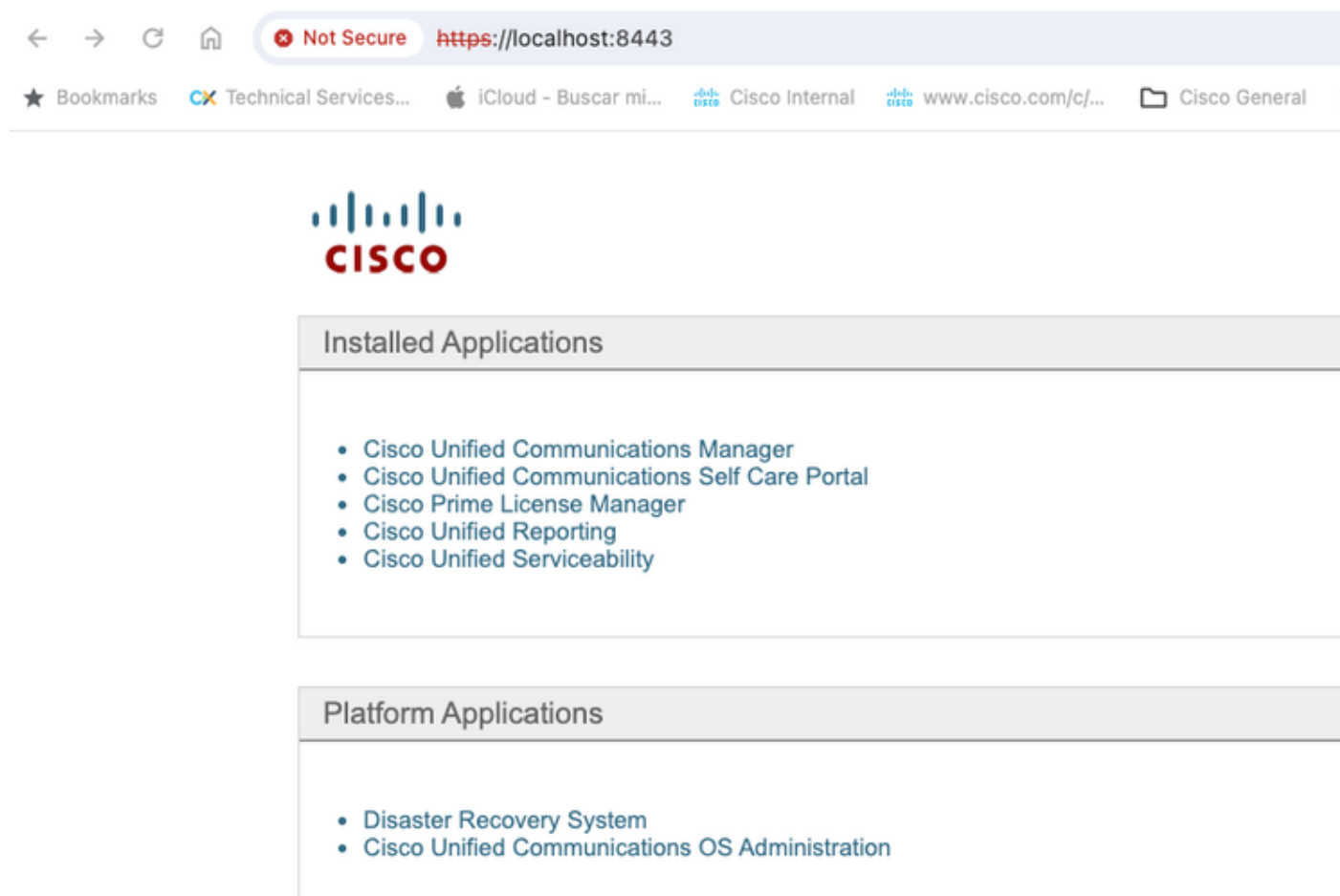
```
>>> cucm.forward_tcp_port(local_port=8443, destination_port=443)
```

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

3단계. 브라우저를 열고 2단계에서 구성한 포트를 사용하여 URL을 입력합니다.

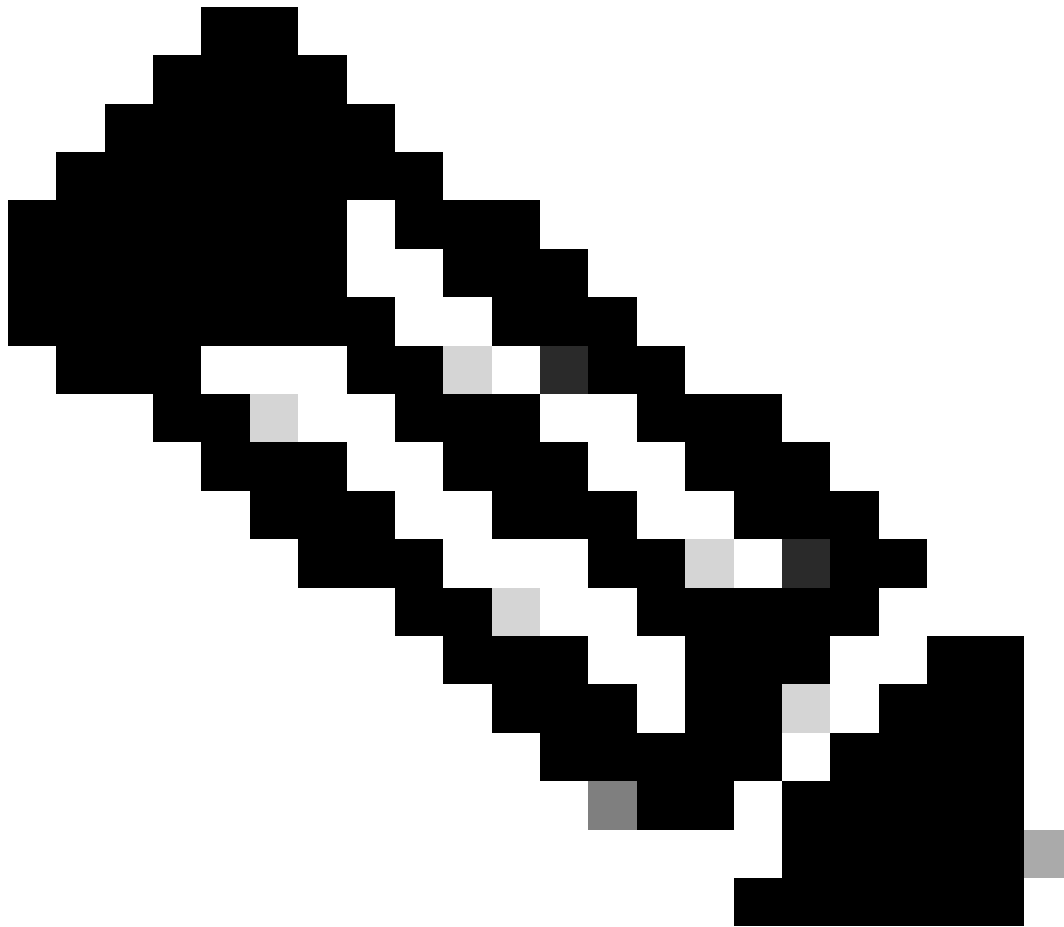
<https://localhost:8443>

이제 디바이스의 GUI에 액세스할 수 있습니다.



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



참고: 제품의 GUI에 액세스하려면 여전히 로그인할 수 있는 자격 증명이 필요합니다. 따라서 사용자가 액세스를 위한 읽기 전용 사용자 계정을 생성하는 것이 좋습니다.

로그 수집

- RTMT

1단계. 포트 8443이 디바이스에 대해 구성된 TCP Forwarded 포트에 나열되는지 확인합니다.

```
<#root>
```

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

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

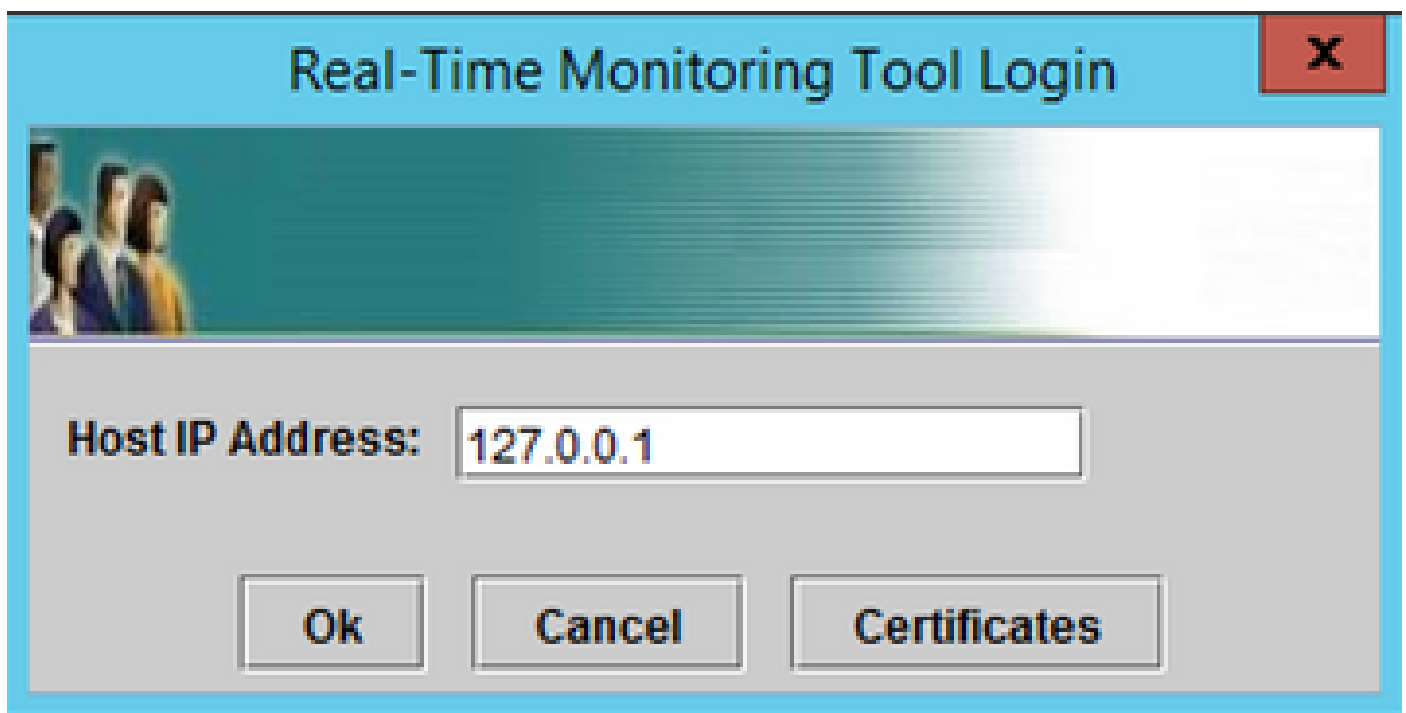
2단계. 로컬 포트와 동일한 포트 8443을 디바이스의 목적지 포트인 포트 8443과 매핑하도록 구성합니다.

<#root>

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

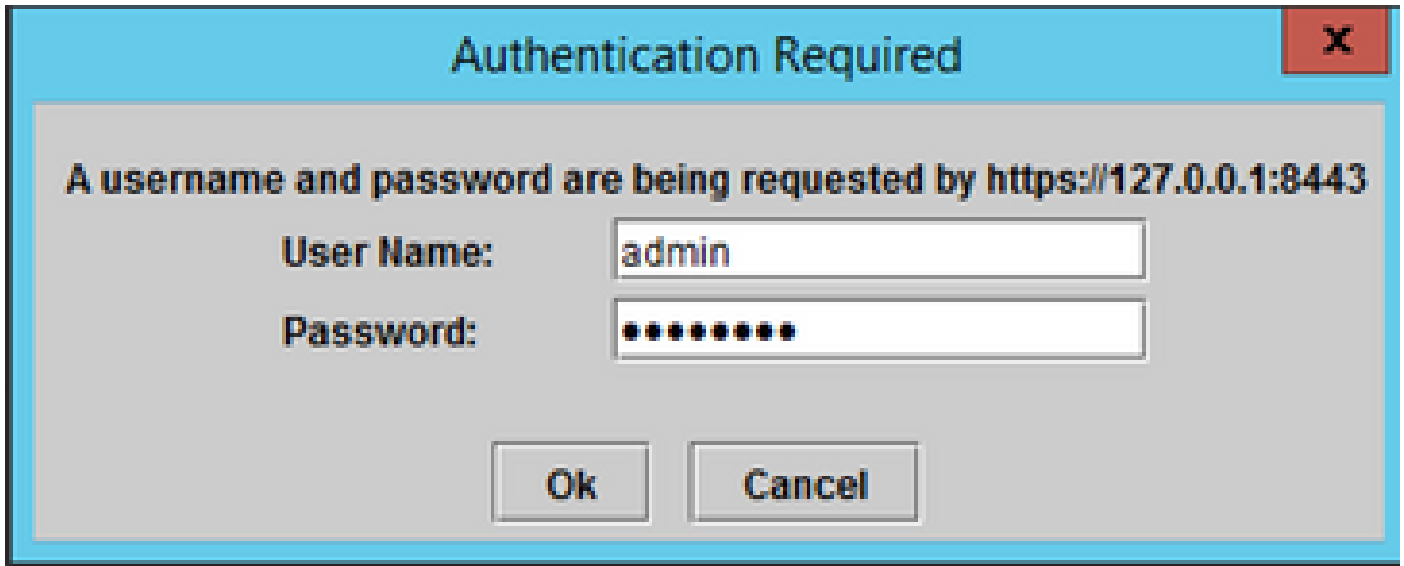
```
>>> cucm.forward_tcp_port(8443,8443)
[RUNNING] <radkit_client.sync.port_forwarding.TCPPortForwarder object at 0x1077defa0>
-----
status          RUNNING
serial          None
device_name     cesavilacucm
local_port      8443
destination_port 8443
#active         0
#failed         0
#closed       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

3단계. RTMT를 열고 호스트 IP 주소에 127.0.0.1을 입력하면 자동으로 포트 8443이 사용됩니다.

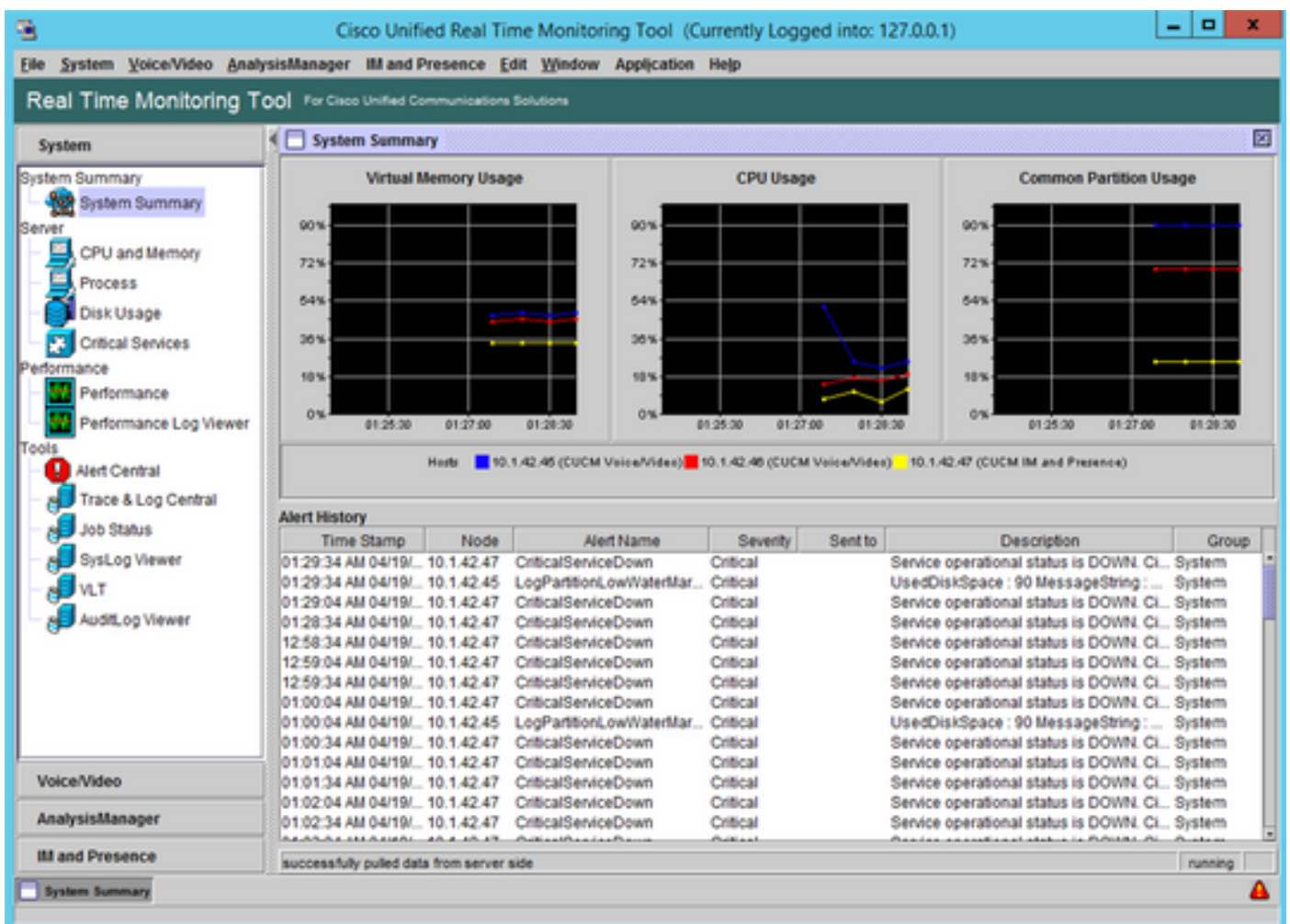


The image shows a Windows-style dialog box titled "Real-Time Monitoring Tool Login". It has a blue header bar with a red "X" button in the top right corner. Below the header is a blurred image of three people. The main area is light gray and contains a label "Host IP Address:" followed by a text input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

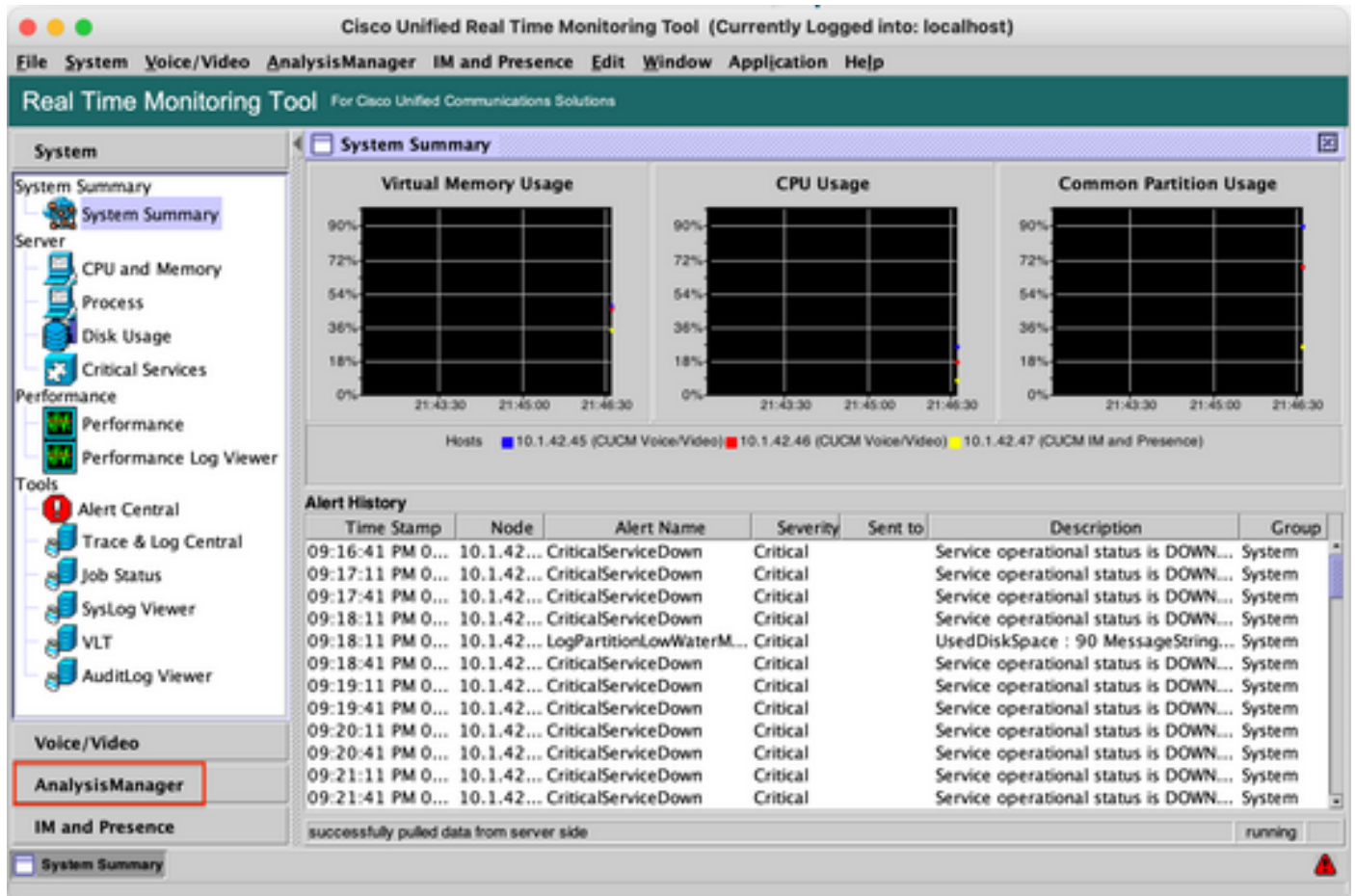
4단계. 올바른 자격 증명으로 로그인합니다.



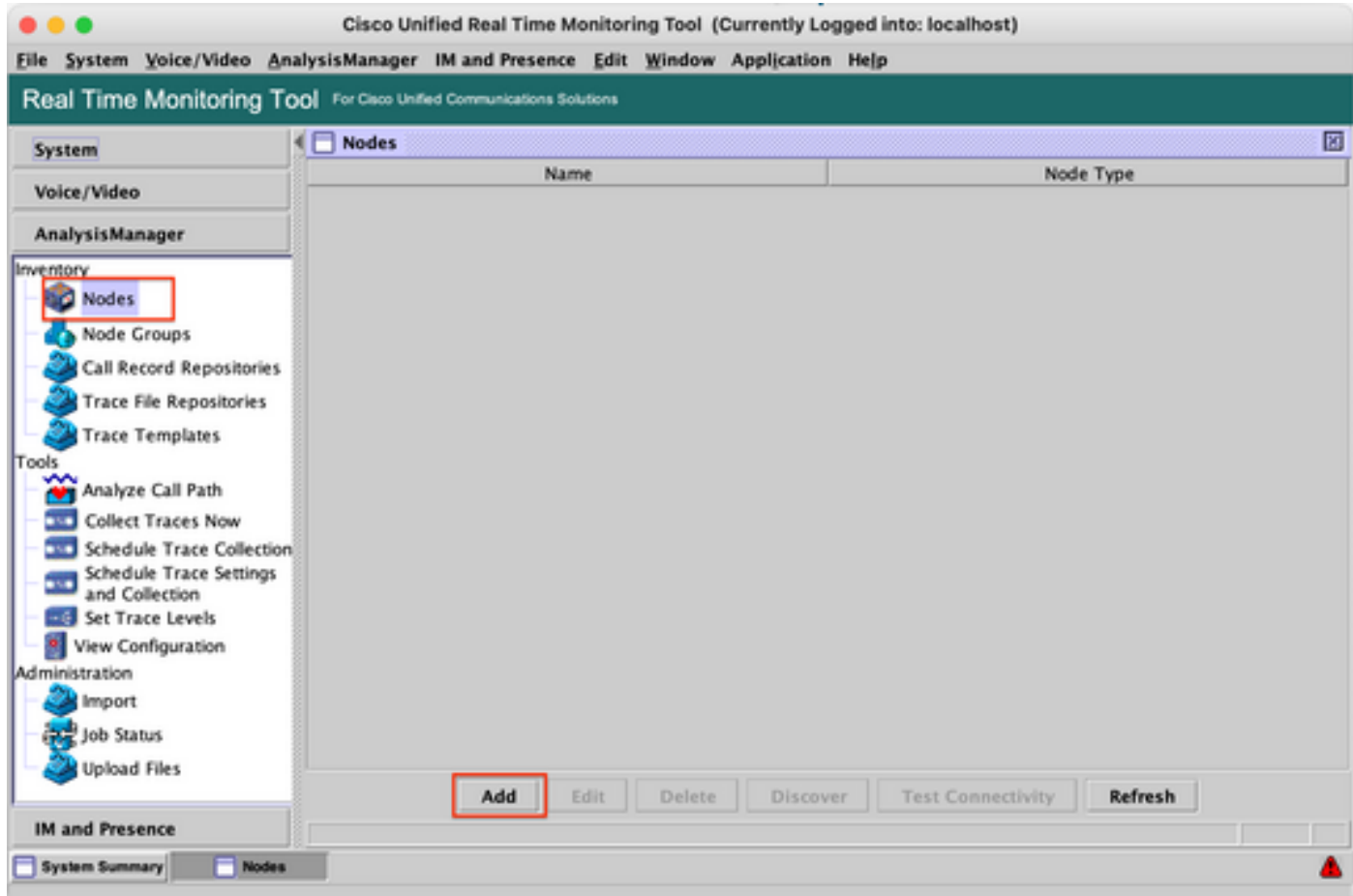
5단계. RTMT가 표시됩니다.



6단계. 왼쪽 패널에서 AnalysisManager로 이동합니다.



7단계. Nodes and Add(노드 및 추가)를 클릭하여 localhost 및 전달된 TCP 포트를 사용하여 추가할 디바이스의 세부사항을 구성합니다.



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

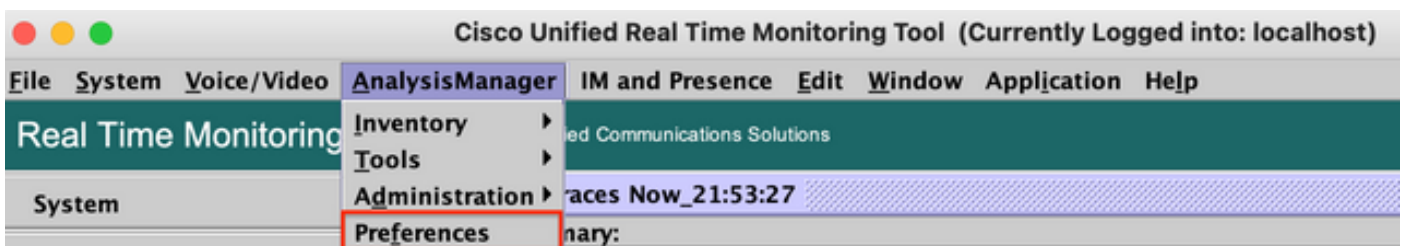
Associated Group ☒ AllNodes

Advanced...

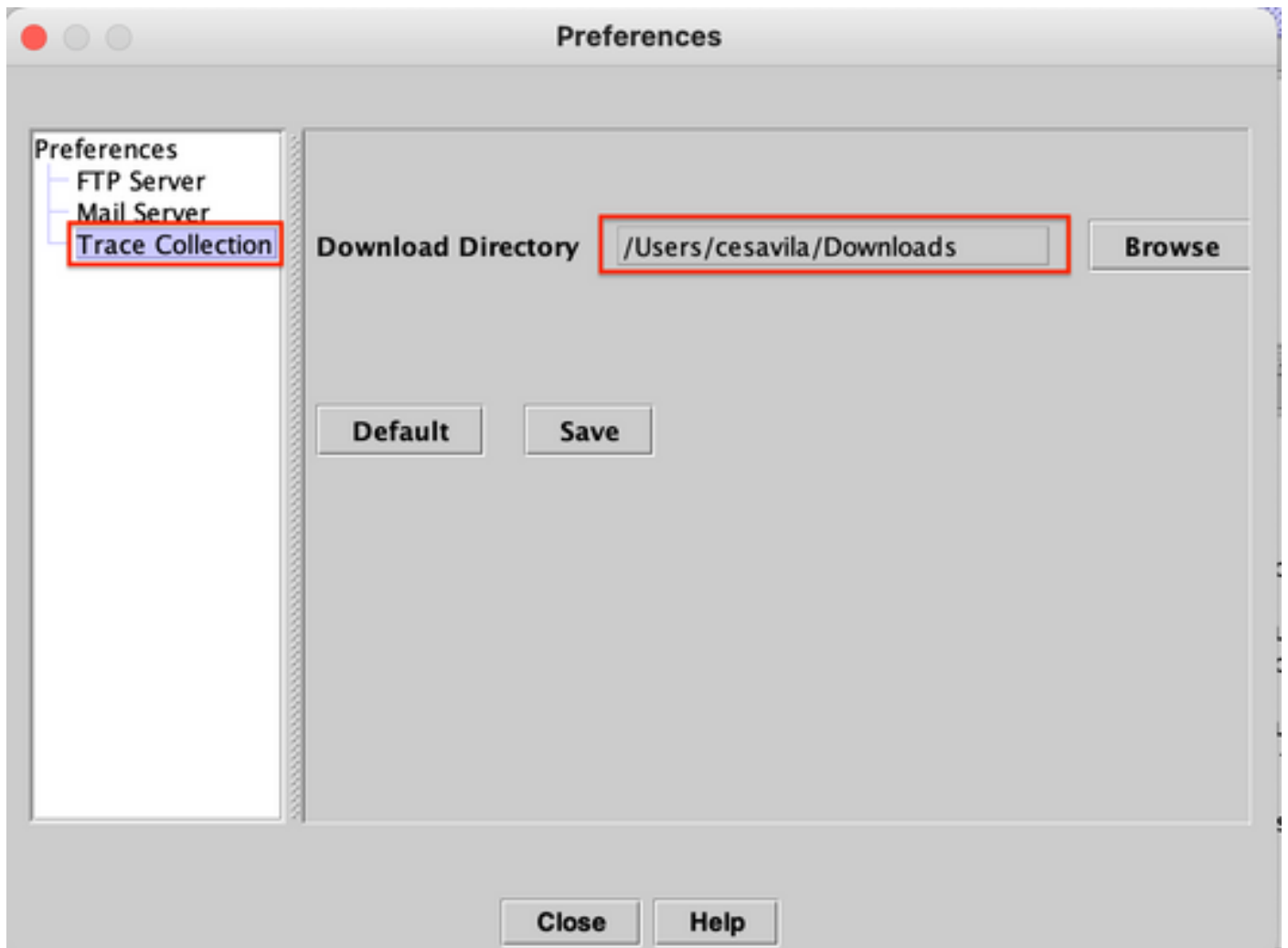
* Required Fields

Save Cancel

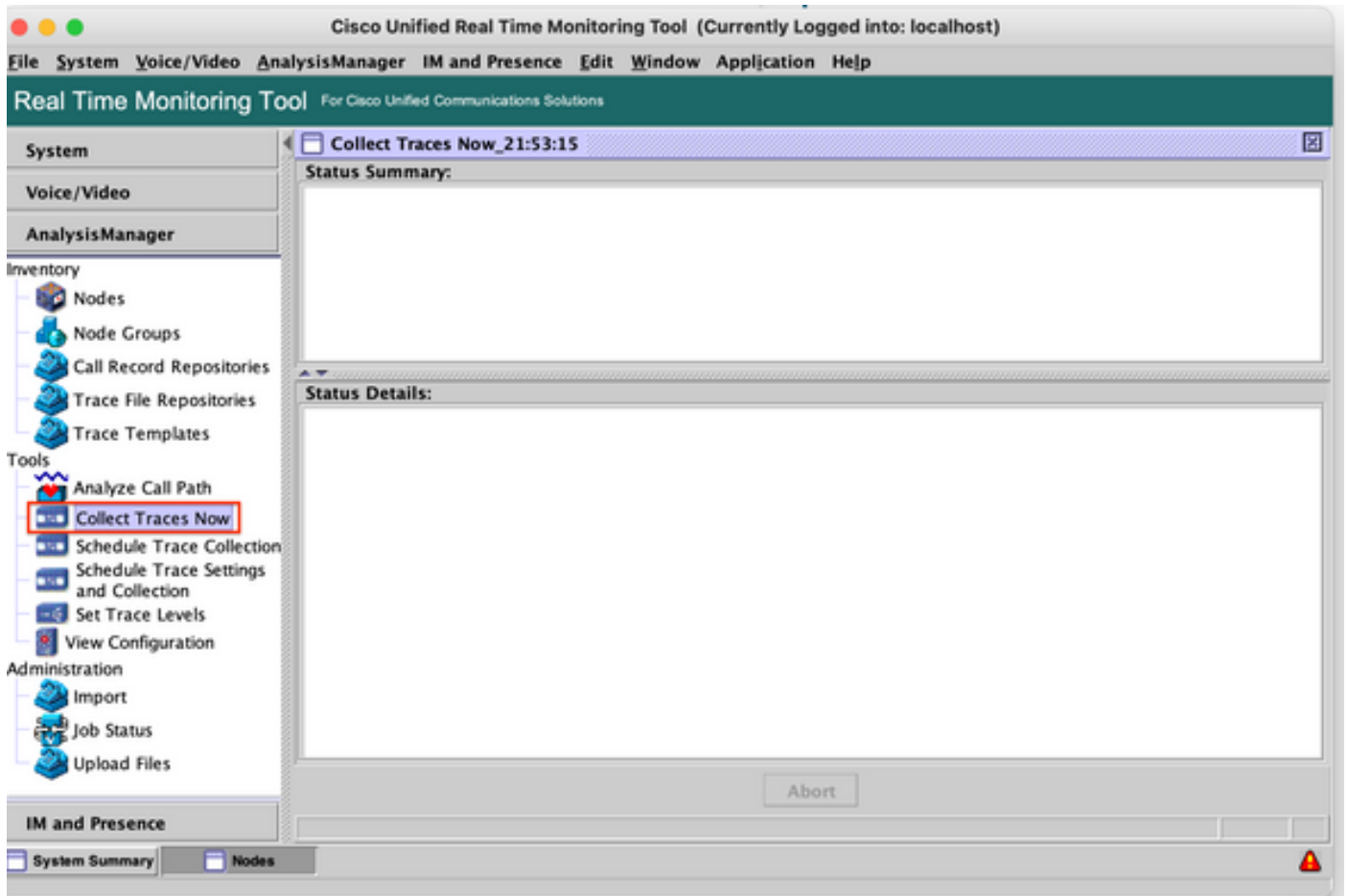
8단계. 상단의 메뉴에서 Analysis Manager를 클릭하고 Preferences를 선택합니다.



9단계. Trace Collection(컬렉션 추적)으로 이동하여 Correct(올바른) 폴더를 선택하여 로그를 다운로드하고 Save(저장)를 클릭한 다음 Close(닫기)를 클릭합니다.



10단계. 지금 추적을 수집하기로 이동합니다.



11단계. 노드 옵션을 선택하고 7단계에서 추가한 장치를 선택한 후 사용자 정의를 누릅니다.

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...**

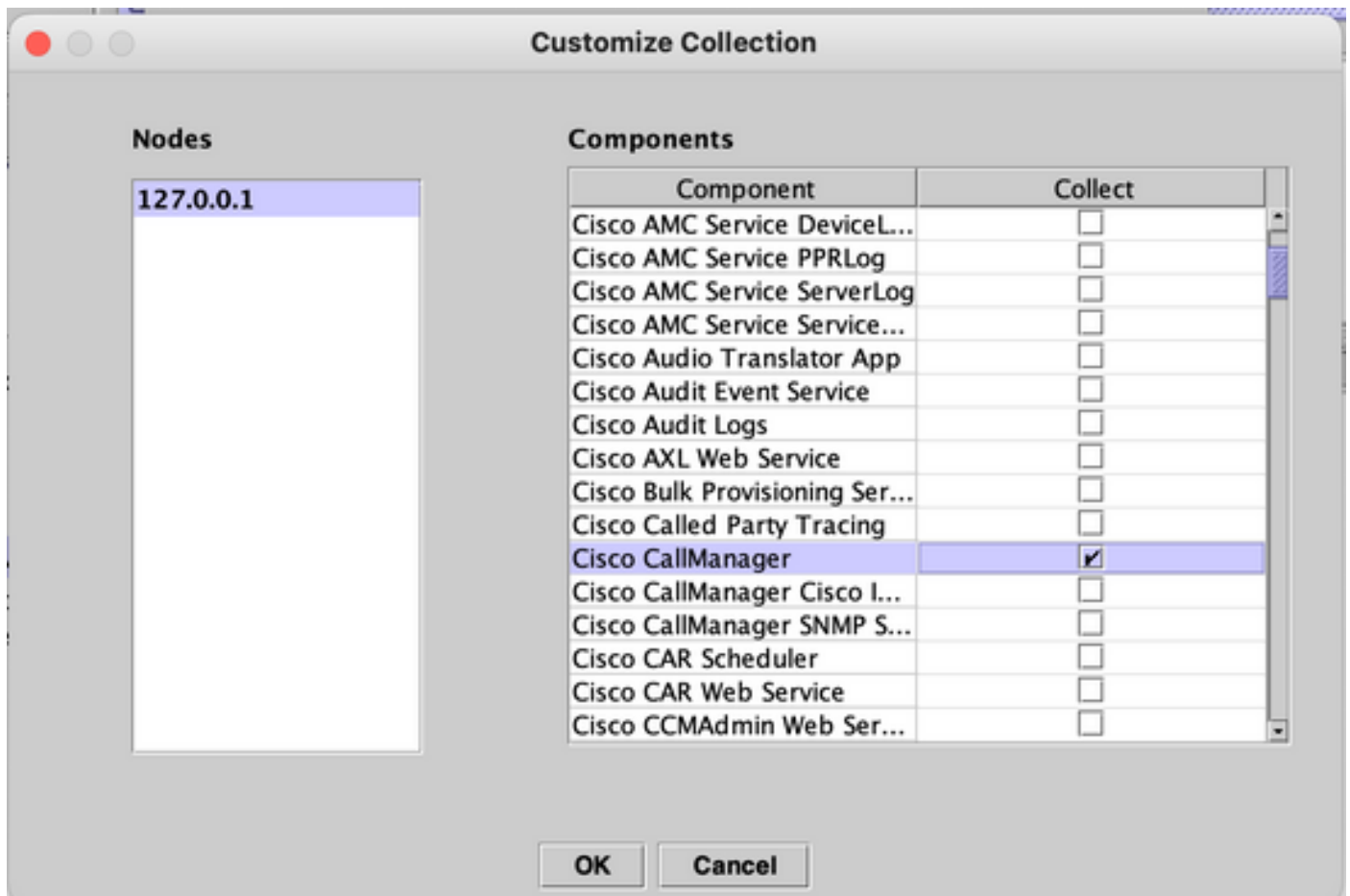
Start Time:

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

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

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

12단계. 디바이스에서 수집할 로그를 선택하고 OK(확인)를 클릭합니다.



13단계. 마지막으로 수집할 로그의 Start Time(시작 시간)과 End Time(종료 시간)을 선택하고 OK(확인)를 클릭합니다.

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...

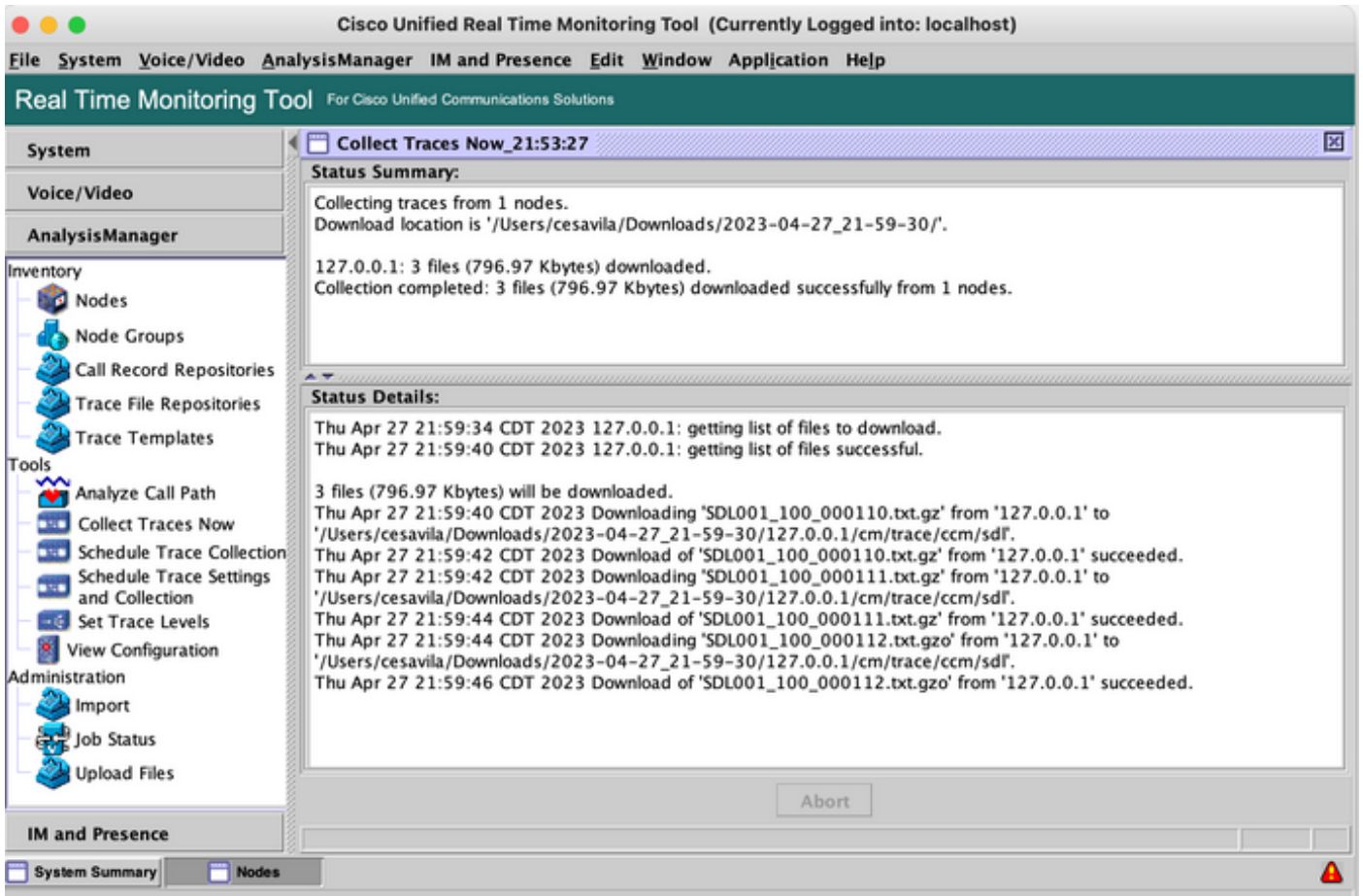
Start Time: 04-27-2023 21:00:00

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

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

View Summary **OK** Cancel Help

14단계. 파일이 로컬 PC(RADKit 클라이언트 PC)에 성공적으로 다운로드되었습니다.



- SOAP API

SOAP API는 현재 CUCM에서 지원됩니다. 또한 Swagger는 CMS, Expressway, CVP 등에서 지원됩니다.

1단계. HTTP 자격 증명이 디바이스 컨피그레이션의 RADKit 서비스에 추가되었는지 확인합니다.

2단계. RADKit 클라이언트에서 HTTP Post 명령을 실행하고, 리소스 경로를 지정하고, 필요한 매개 변수 및 헤더가 있는 본문을 요청합니다.

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

참고: postprocessors 옵션 'cucm-extract'는 로그를 파일에 저장할 수 있도록 HTTP 응답 헤더를 제거하는 데 사용됩니다.

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

3단계. 콘텐츠를 파일에 저장하여 로컬 PC에 저장된 추적 파일을 가져옵니다.

<#root>

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

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

RADKit 활용 사례

강조했듯이 RADKit는 WebEx를 사용하지 않고도 협업 서버를 비롯한 네트워크 장치에 안전하게 연결할 수 있습니다. 이 아이디어는 필요한 장치에 대한 온디맨드 액세스를 제공하여 데이터 수집과 관련된 몇 가지 문제를 단순화하는 것입니다.

협업 구축에 대해 구체적으로 이야기할 때 RADKit는 현재 다음과 같은 다양한 문제에 매우 유용할 수 있습니다.

- DB 복제 문제.
- 인증서 재생성 절차
- 시스템 상태 검사.
- GUI/CLI에서 구성 검증
- 웹 인터페이스(예: CER, Expressway, CIMC 등)를 통한 로그 수집
- 음성 게이트웨이에서 CLI를 통해 로그를 디버깅합니다.

관련 정보

- RADKit 기본 페이지 <https://radkit.cisco.com/>
- 외부 RAIDit 지원 페이지 <https://community.cisco.com/t5/radkit-discussions/bd-p/disc-radkit>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.