

# HyperFlex에서 원격 문제 해결을 위한 RADKit 설정

## 목차

---

### [소개](#)

### [배경 정보](#)

[RADKit란 무엇입니까?](#)

[왜 HX를 위한 RADKit일까요?](#)

[RADKit와 Intersight 비교](#)

### [개괄적 개요](#)

[연결 다이어그램](#)

[구성 요소](#)

### [준비](#)

[따라야 할 단계 개요](#)

[1단계. RADKit 서비스 다운로드 및 설치](#)

[2단계. RADKit 서비스를 시작하고 초기 설정\(부트스트랩\)을 수행합니다](#)

[3단계. RADKit Cloud에 RADKit 서비스 등록](#)

[4단계. 디바이스 및 엔드포인트 추가](#)

### [TAC SR에서 RADKit 사용](#)

[1. RADKit 서비스 ID 제공](#)

[2. 원격 사용자 추가](#)

### [관련 정보](#)

---

## 소개

이 문서에서는 Cisco HyperFlex 환경의 원격 문제 해결을 위해 RADKit 환경을 시작하고 준비하는 방법에 대해 설명합니다.

## 배경 정보

이 문서의 주된 목적은 문제 해결을 위해 RADKit를 활용하기 위해 TAC에서 사용 환경을 준비하는 방법을 설명하는 것입니다.

### RADKit란 무엇입니까?

RADKit는 네트워크 전반의 오케스트레이터입니다. 장비를 다루고, Cisco 서비스를 향상하며, 기능을 확장하는 새로운 방법을 경험할 수 있습니다.

RADKit에 대한 자세한 내용은 <https://radkit.cisco.com/>을 참조하십시오.

## 왜 HX를 위한 RADKit일까요?

Cisco HyperFlex는 패브릭 인터커넥트, UCS 서버, ESXi, vCenter, SCVM의 여러 구성 요소로 이루어져 있습니다. 많은 경우, 서로 다른 디바이스의 정보를 수집하고 연관성을 파악해야 합니다. 트러블슈팅을 하는 동안 시간이 지남에 따라 새로운 정보가 필요할 수 있으며, 이를 위해서는 긴 WebEx 세션이나 Intersight를 통해 (대규모) 지원 번들을 가져오는 것이 가장 효과적인 방법은 아닙니다. RADKit를 사용하여 TAC 엔지니어는 다양한 장치와 서비스의 문제 해결 프로세스 중에 필요한 정보를 안전하고 통제된 방법으로 요청할 수 있습니다.

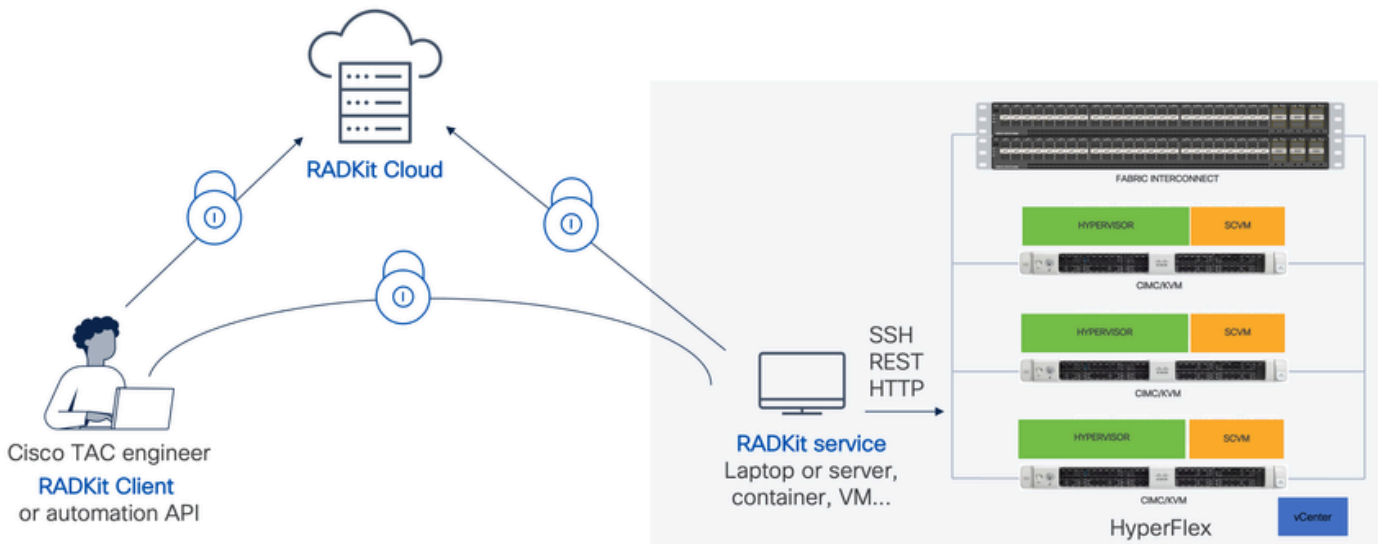
## RADKit와 Intersight 비교

Intersight는 HyperFlex 클러스터의 기본 연결 방법으로 자동 로그 수집, 텔레메트리, 하드웨어 및 기타 알려진 알림에 대한 환경 사전 모니터링 등의 다양한 이점을 제공합니다.

많은 HX 클러스터가 Intersight에 연결되어 있지만, Intersight는 현재 주로 HyperFlex 클러스터의 구축, 유지 관리 및 모니터링을 위한 것입니다. Intersight를 사용하면 지원 번들 및 텔레메트리 정보를 수집할 수 있습니다. 이는 일반적으로 문제 해결을 위한 좋은 출발점입니다. TAC 엔지니어가 기존 시나리오에서 WebEx 세션을 활용하는 라이브 트러블슈팅의 경우, RADKit이 제공됩니다. Intersight를 대체하지는 않지만, 대화형 세션을 사용하거나 프로그래밍 방식의 요청-응답 시퀀스를 활용하여 트러블슈팅에 다른 접근 방식을 추가합니다.

## 개괄적 개요

### 연결 다이어그램



## 구성 요소

- RADKit 서비스: 온프레미스 RADkit 서비스 구성 요소로, HX 환경에 대한 보안 게이트웨이로 사용됩니다. 고객은 어떤 장치에 액세스할 수 있는지, 그리고 누가 언제 장치에 액세스할 수 있는지에 대한 모든 권한을 보유하게 됩니다. 이 서비스는 Linux, MacOS 또는 Windows 시스템에서 호스팅할 수 있습니다.

- RADKit 클라이언트: TAC 엔지니어가 프로그래밍 방식의 문제 해결 및 모니터링, 자동화된 검색, Cisco 내부 툴을 사용한 장치 출력 분석 또는 CLI를 통한 장치와의 직접 상호 작용을 사용하여 환경에 액세스하는 데 사용하는 프론트엔드
- RADKit 클라우드: 클라이언트와 서비스 간의 안전한 전송을 제공합니다.

## 준비

### 따라야 할 단계 개요

TAC 엔지니어가 RADKit를 활용하여 HX 환경에 연결하고 문제를 해결하려면 다음 단계가 필요합니다.

1. RADKit 서비스를 다운로드하여 설치합니다. Linux, MacOS 또는 Windows 시스템에 설치할 수 있습니다.
2. RADKit 서비스를 시작하고 초기 설정(부트스트랩)을 수행합니다. 웹 인터페이스를 통해 RADKit 서비스를 추가로 관리하려면 슈퍼 관리자 계정을 생성합니다.
3. RADKit 서비스를 RADKit 클라우드에 등록합니다. RADKit 서비스를 RADKit 클라우드에 등록하고 환경을 식별하기 위한 서비스 ID를 생성합니다.
4. 디바이스 및 엔드포인트를 추가합니다. 디바이스 목록을 제공하고 액세스해야 할 디바이스에 대한 자격 증명을 저장합니다.

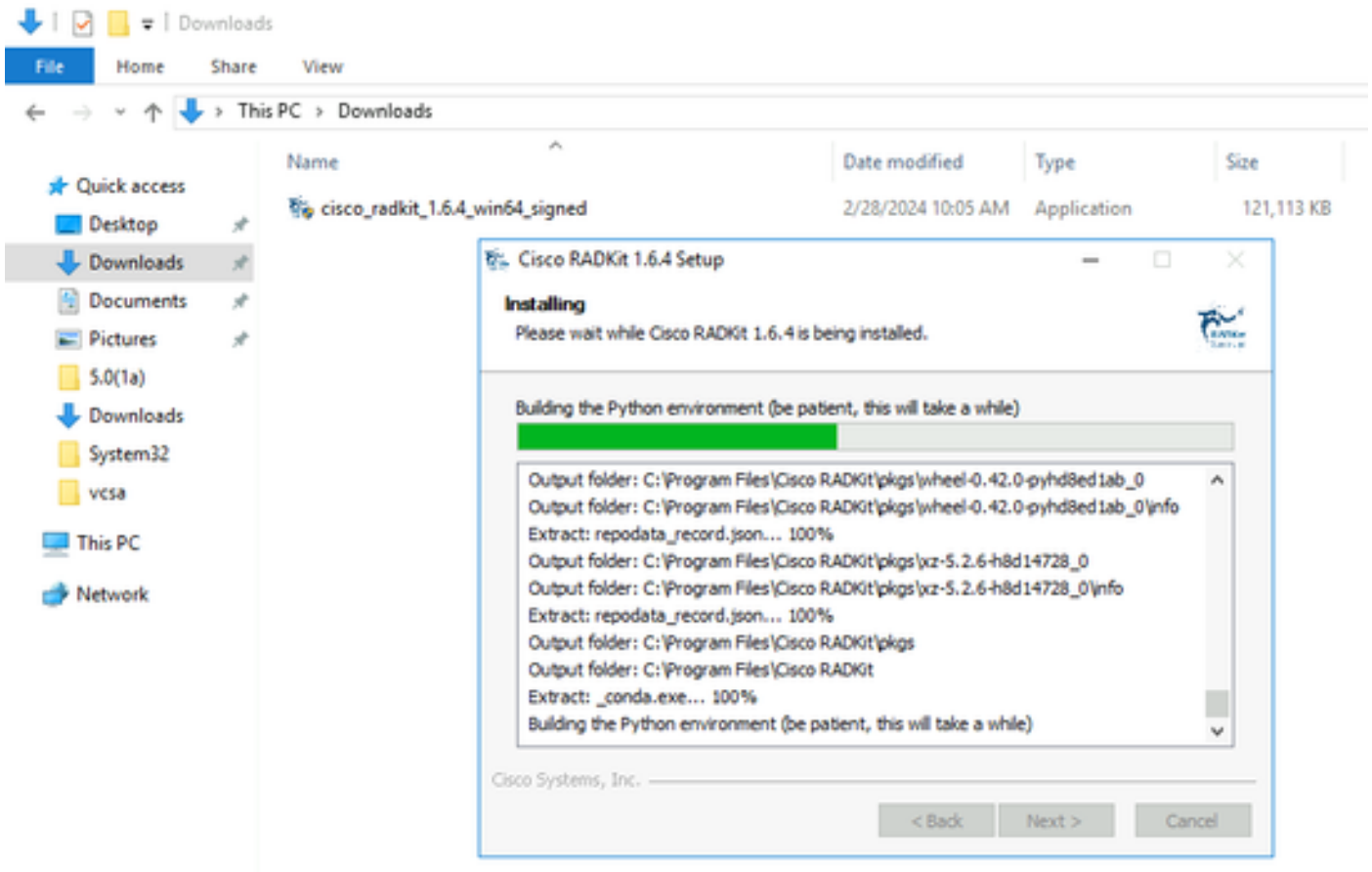
이러한 단계에 대한 자세한 설명/일반적인 설명은 다음 사이트에서 확인할 수 있습니다.

[https://radkit.cisco.com/docs/pages/one\\_page\\_setup.html](https://radkit.cisco.com/docs/pages/one_page_setup.html)

### 1단계. RADKit 서비스 다운로드 및 설치

이 단계의 세부 사항은 RADKit 서비스를 설치하기 위해 사용하는 OS에 따라 약간 다를 수 있지만 일반적으로 프로세스는 매우 유사합니다. <https://radkit.cisco.com/downloads/release/>에서 OS용 최신 릴리스를 [다운로드하십시오](#).

시스템에 대한 설치 프로그램을 실행하고 설치가 완료될 때까지 프롬프트에 따릅니다.

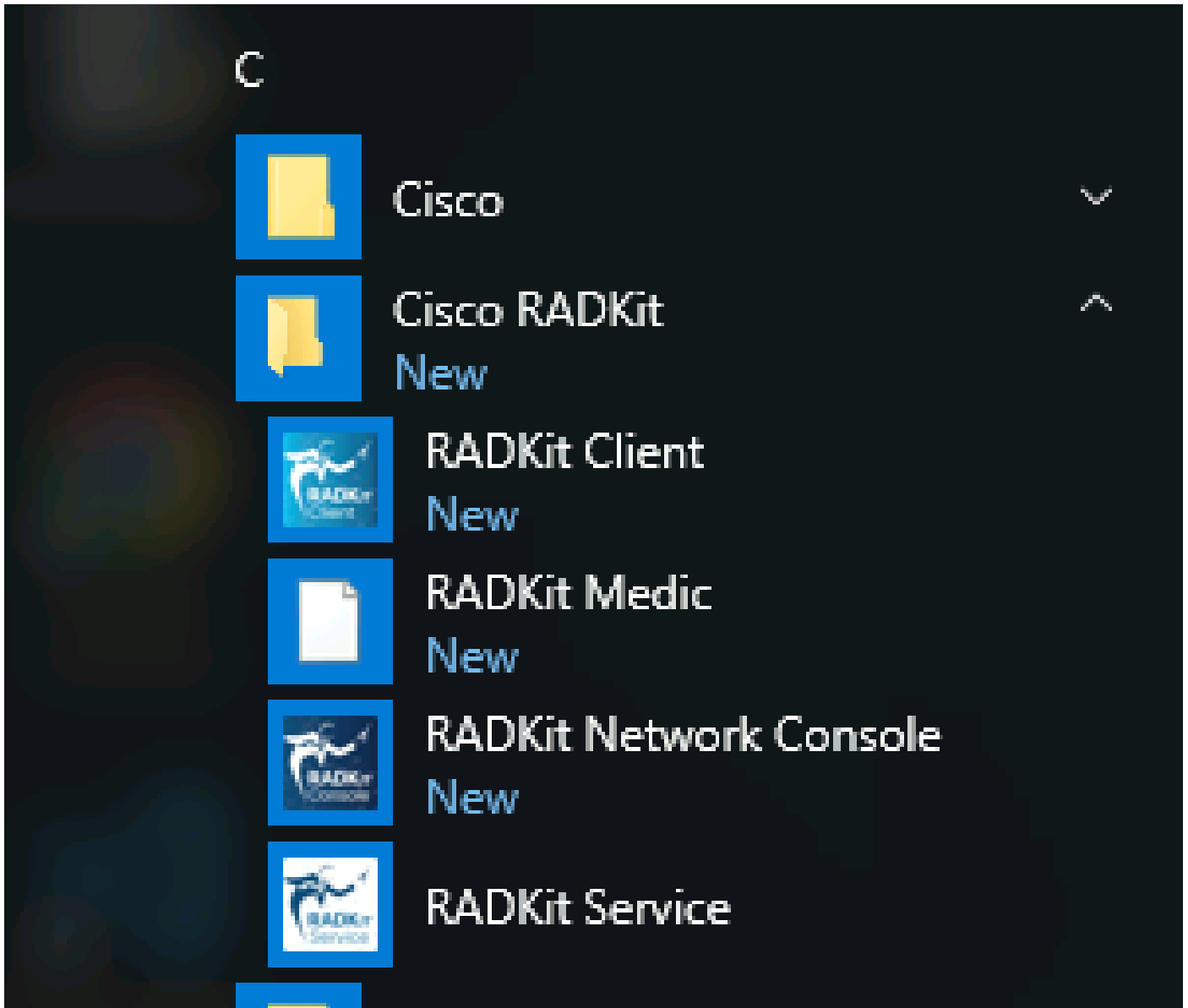


모든 RADKit 구성 요소가 설치되면 초기 설정을 진행하는 다음 단계로 진행할 수 있습니다.

## 2단계. RADKit 서비스를 시작하고 초기 설정(부트스트랩)을 수행합니다

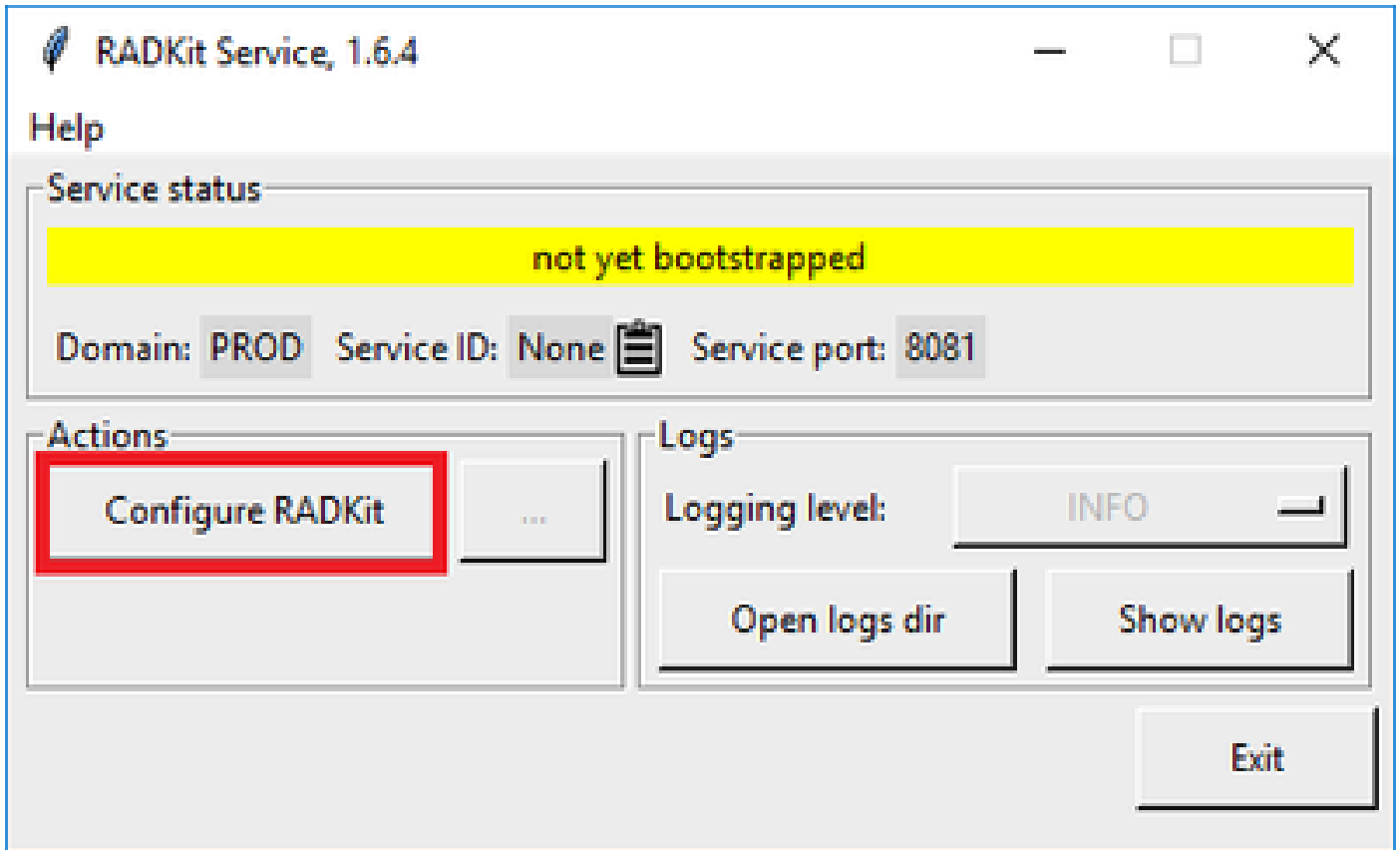
이 단계에서는 웹 인터페이스를 통해 RADKit 서비스를 추가로 관리하기 위한 슈퍼관리자 계정을 생성합니다.

시작 메뉴(Windows) 또는 응용 프로그램 폴더(macOS)에서 찾아 RADKit Service 시작합니다.



처음 시작할 때 RADKit 서비스를 시작하는 데 약간의 시간이 걸릴 수 있습니다(시스템 속도에 따라 약 10~30초). 후속 실행이 훨씬 빨라집니다.

시작이 완료되면 RADKit Service(RADKit 서비스) 대화 상자에서 상태가 다음으로 변경되면 not yet bootstrapped을 Configure RADKit 누릅니다.



이렇게 하면 웹 브라우저가 열리고 RADKit 서비스를 관리할 수 있는 웹 기반 관리 인터페이스인 RADKit Service WebUI로 이동합니다.

이 URL에 연결할 때 자체 서명 인증서를 사용하므로 건너뛸 수 있는 인증서 경고가 표시됩니다.

수퍼관리자 사용자가 아직 없으므로 WebUI에서 이 사용자의 암호를 만들도록 요청합니다.

# 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 **8** characters
- Minimum **1** lowercase letter
- Minimum **1** uppercase letter
- Minimum **1** digit
- Minimum **1** symbol

오른쪽에 표시된 비밀번호 강도 요구 사항을 준수하는 비밀번호를 선택합니다.

이 계정의 암호는 개인 키 및 장치 자격 증명과 같은 암호를 보호하는 데 사용됩니다. 암호를 분실할 경우 모든 암호가 손실되며 RADKit 서비스를 다시 초기화해야 하므로 신중하게 선택하고 안전한 위치에 기록해 두십시오. 나중에 필요에 따라 변경할 수 있습니다.

수퍼관리자 계정을 생성한 후 이를 사용하여 WebUI에 로그인합니다.



# Log in

Username \*

superadmin

Password \*

.....



Login

슈퍼관리자 계정이 생성되고 WebUI에 성공적으로 로그인했다면 RADKit 서비스가 RADKit 클라우드 구성 요소에 등록되는 다음 단계로 진행할 수 있습니다.

3단계. RADKit Cloud에 RADKit 서비스 등록

이 단계에서는 RADKit 클라우드에 RADKit 서비스를 등록하고 서비스 ID를 생성하여 환경을 식별합니다.

슈퍼관리자 사용자로 WebUI에 로그인한 후(2단계 참조) 연결 화면으로 이동합니다.

Remote Automation Development Kit  
Cisco RADKit Service

Domain: PROD Service ID: none

Connectivity

Devices

Remote

+ Add Device

Active	Device Name	Hostname or IP Address	Device Type
No devices available			

Showing 0 to 0 of 0 entries. | Selected: 0.




인터넷에 연결하기 위해 프록시가 필요한 경우 [https://radkit.cisco.com/docs/pages/one\\_page\\_setup.html](https://radkit.cisco.com/docs/pages/one_page_setup.html)에서 자세한 설정 지침을 참조하십시오.


이제 서비스를 등록하여 RADKit 클라우드에 연결해야 합니다. 이 작업은 Cisco.com(CCO) 계정을 사용하여 서비스 WebUI를 통해 로그인하는 방식으로 수행됩니다. 계속하려면 [Enroll with SSO](#) 을 클릭하십시오.

## Cloud Connectivity

DOMAIN: PROD  
BASE URL: <https://prod.radkit-cloud.cisco.com>

Forwarder Endpoint	Status	Latency [ms]
 <b>No forwarder endpoints connected</b>		

## Service Identity Certificate

 This RADKit Service needs to be enrolled to become functional. Please select an enrollment method by clicking one of the buttons below.

**Recommended:** [Enroll with SSO](#) **Advanced:** [Enroll with OTP](#)

2단계의 이메일 주소 필드에 Cisco.com(CCO) 계정에 해당하는 이메일 주소를 입력하고 다음을 클릭합니다Submit as shown in the image.

# Single Sign-On Enrollment



✓ Checking prerequisites

2 Email address

Provide email address for SSO login:

example@your.com

Submit

3 Connecting to the Access Service

RADKit Service가 권한 부여를 위해 RADKit Cloud에 연결한 후 [CLICK HERE] Cisco SSO 서버로 이동하여 인증할 수 있는 링크가 표시됩니다. 계속하려면 링크를 클릭합니다. 새 브라우저 탭/창에서 열립니다. 앞에서 설명한 단계에서 입력한 것과 동일한 이메일 주소를 사용하여 SSO에 로그인해야 합니다.

✓ OAuth connect

5 Waiting for SSO

Follow the SSO login link to continue: [\[CLICK HERE\]](#)

6 Requesting service certificate OTP

SSO 인증이 완료되면(또는 이미 인증된 경우 즉시) RADKit 액세스 확인 페이지로 이동합니다. 페이지에 있는 정보를 읽고 RADKit 서비스가 CCO 계정을 소유자로 등록하도록 승인하려면 클릭하십시오 Accept.

## Do you accept this authorization request?

Environment: PROD

Endpoint IP Address: 209.14.28.209:8000:8000

Endpoint Hostname: 209.14.28.209:8000:8000

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

그런 다음 Authentication result: Success 이라고 표시된 화면이 나타납니다.

버튼을 Log out all sessions 클릭하지 말고 SSO 탭/창을 닫고 RADKit Service WebUI로 돌아가십시오.

이 그림에서는 을(를) 보여 Service enrolled with the identity: ... 줍니다. 다음의 고유 식별자는 서비스 일련 번호라고도 하는 RADKit 서비스 ID입니다. 예제 스크린샷에서는 귀하가 보유한 서비스 IDdaxt9-kplb-5dwc가 달라집니다.

- ✓ Requesting service certificate
- ✓ Saving the identity
- ✓ Starting/Restarting the service

✓ Service enrolled with the identity: axt9-kplb-5dwc

**Close**

Close 대화 상자를 닫고 화면으로 돌아가려면 클릭하십시오Connectivity.

WebUI를 새로 고치면 서비스 ID가 RADKit GUI 위에 표시되며 연결 상태도 여기에 표시됩니다.



TAC 엔지니어가 해당 환경의 디바이스에 액세스해야 할 때마다 RADKit 서비스를 식별하기 위해 이 서비스 ID가 필요합니다.

이제 RADKit Cloud 구성 요소와 연결이 설정되고 서비스 ID가 생성되었으므로 다음 단계에서는 RADKit를 통해 연결할 수 있는 디바이스를 추가합니다.

#### 4단계. 디바이스 및 엔드포인트 추가

이 단계에서는 RADKit를 통해 액세스할 수 있는 디바이스에 대한 디바이스 및 해당 자격 증명을 추가합니다. HyperFlex의 경우, 이상적으로는 이러한 디바이스와 해당 자격 증명을 추가해야 합니다.

디바이스	디바이스 유형	관리 프로토콜	자격 증명	전달된 TCP 포트	비고
하이퍼바이저(ESXi 호스트)	Linux	터미널(SSH)	루트		

스토리지 컨트롤러 (SCVM)	하이퍼플렉스	터미널 (SSH)Swagger	관리자 루트(사용)	443	enable password 필드에 루트 비밀번호를 입력합니다. 이는 동의 토큰이 필요할 때 사용됩니다. Swagger의 경우: "Verify TLS Certificate(TLS 인증서 확인)"의 선택을 취소하고 Base URL 필드를 비워 둡니다
vCenter	Linux	터미널(SSH)	루트		
UCSM	일반	터미널(SSH)	관리자		
설치 프로그램(선택 사항)	Linux	터미널(SSH)	루트	443	
CIMC(에지 클러스터에만 해당)	일반	터미널(SSH)	관리자		
감시(스트레치된 클러스터에만 해당)	Linux	터미널(SSH)	루트		
Intersight CVA/PCA(선택 사항)	Linux	터미널(SSH)	관리자	443	

동일한 클러스터에 속한 디바이스를 상호 연결하기 위해서는 호스트 이름이 아닌 해당 IP 주소를 사용해서만 디바이스를 추가해야 합니다.

이러한 디바이스를 추가하려면 RADKit WebUI에서 Devices(디바이스) 화면으로 이동합니다.

Remote Automation Development Kit  
Cisco RADKit Service

Domain: PROD Service ID: axt9-kplb-5dwc

Connectivity

+ Add Device

☑ ☒ ☒

0 Edit Cart

+ -

☰  
☰  
☰  
Devices

☰  
☰  
☰  
Remote Users

<input type="checkbox"/>	Active	Device Name	Hostname or IP Address	Device Type	In
⚠ No devices available					

Showing 0 to 0 of 0 entries. | Selected: 0.

위에 나열된 각 디바이스에 대해 를 클릭하여 새 항목을 생성합니다 Add Device. IP 주소를 입력하고, 디바이스 유형을 선택하고, 클러스터의 모든 노드에 대해 각 디바이스 유형에 따라 세부사항을 제공합니다. 완료되면 를 클릭하여 Add & closeDevices 화면으로 돌아가거나 다른 디바이스를 Add & continue 추가합니다.

여기에서 각 디바이스 유형에 대한 예제 항목과 해당 컨피그레이션을 찾을 수 있습니다.

ESXi 호스트의 예:

## Edit Device ✕

**Device Name\*** (as it will appear in RADICL) ?

**Device Type\***

**Management IP Address or Hostname\*** ?

**Jumphost Name**

**Forwarded TCP ports** ?

**Description**

?

**PSAC status: DISABLED**

**Available Labels - 0 of 0** (click to add)

NO LABELS AVAILABLE

**Selected Labels - 0** (click to delete)

+ Create new - None added

**Active** (remotely manageable)

**Available Management Protocols:**

Terminal
  Netconf
  Swagger
  HTTP
  SNMP

---

### Terminal

**Connection method:**

SSH (Password)
  SSH (Public key)
  Telnet

Allow connecting using obsolete/insecure SSH algorithms

Use SSH Tunneling when using this device as a jumphost

**Username**

**Password**

if left blank, will be set to "" as default ?

**Port**

**Enable Password** ?

Update

스토리지 컨트롤러의 예:

# Edit Device



Device Name (as it will appear in RedBox)

cluster2-node1-rcvm

Device Type

HyperFlex

Management IP Address or Hostname

172.16.2.14

Jumpshot Name

- Optional jumpshot -

Forwarded TCP ports

443

Description

Label search

RBAC status: **DISABLED**

Available Labels - 0 of 0 (click to add)

NO LABELS AVAILABLE

Selected Labels - 0 (click to delete)

Create New

None added

Active (remotely manageable)

Available Management Protocols:

Terminal  Netconf  Swagger  HTTP  SNMP

## Terminal

Connection method

SSH (Password)  SSH (Public key)  Telnet

Allow connecting using obsolete/insecure SSH algorithms

Use SSH tunneling when using this device as a jumpshot

Username

admin

Password

\*\*\*\*\*

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

Port

22

Enable Password

\*\*\*\*\*

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

## Swagger

Verify TLS certificate

\* Leave unchecked if the device presents a self-signed certificate

Allow connecting using obsolete/insecure TLS algorithms

Username

admin

Password

\*\*\*\*\*

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

Base URL

\* Leave blank if unused

Update



vCenter 예:

## Edit Device ✕

Device Name\* (as it will appear in RADIX) [?](#)

Device Type\*

Management IP Address or Hostname\* [?](#)

Jumphost Name

Forwarded TCP ports [?](#)

Description

[?](#) RBAC status: **DISABLED**

Available Labels - 0 of 0 (click to add)  

NO LABELS AVAILABLE

Selected Labels - 0 (click to delete)  

Create new None added

Active (remotely manageable)

Available Management Protocols:  
 Terminal  Netconf  Swagger  HTTP  SNMP

---

### Terminal

Connection method:  
 SSH (Password)  SSH (Public key)  Telnet

Allow connecting using obsolete/insecure SSH algorithms  
 Use SSH Tunneling when using this device as a jumphost

Username

Password  
  
If left blank, will be set to "" as default [?](#)

Port

Enable Password [?](#)

**Update**

UCSM의 예:

## Edit Device ✕

**Device Name\*** (as it will appear in RADKit) ?

**Device Type\***

**Management IP Address or Hostname\*** ?

**Jumphost Name**

**Forwarded TCP ports** ?

**Description**

?

**RBAC status: DISABLED**

**Available Labels** - 0 of 0 (click to add)

NO LABELS AVAILABLE

**Selected Labels** - 0 (click to delete)

Create new None added

**Active** (remotely manageable)

**Available Management Protocols:**

Terminal  Netconf  Swagger  HTTP  SNMP

---

**Terminal**

Connection method:

SSH (Password)  SSH (Public key)  Telnet

Allow connecting using obsolete/insecure SSH algorithms

Use SSH Tunneling when using this device as a jumphost

**Username**

**Password**

 gi

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

**Port**

**Enable Password** ?

 gi

Update

### TAC SR에서 RADKit 사용

모든 준비가 완료되었고 TAC 엔지니어에게 장치에 대한 액세스를 제공하려는 경우 다음 단계를 수행할 수 있습니다.

엔지니어는 필요한 시간 동안 RADKit 서비스 ID와 사용자 환경 또는 선택한 디바이스(RBAC 사용 시)에 대한 액세스가 필요합니다.

#### 1. RADKit 서비스 ID 제공

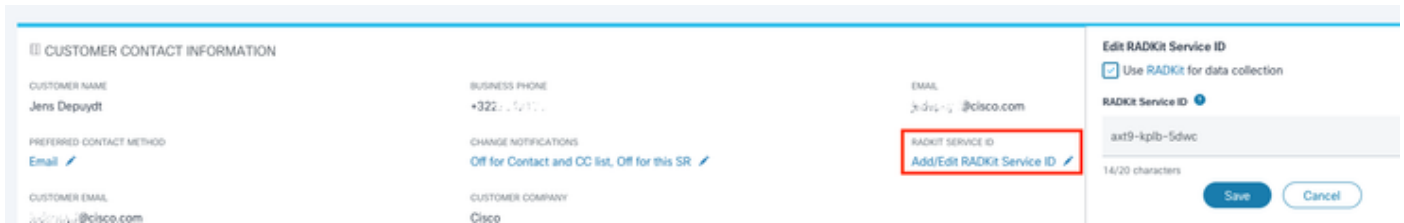
아직 TAC 케이스를 열지 않은 경우 Cisco.com의 Support Case Manager에서 언급할 Use RADKit for data collection 수 있습니다.

## Use RADKit for data collection

### RADKit Service ID

axt9-kplb-5dwc

이미 열려 있는 서비스 요청이 있는 경우 Support Case Manager(지원 케이스 관리자)의 Customer Contact Information(고객 연락처 정보) 섹션에 RADKit 서비스 ID를 추가할 수 있습니다.

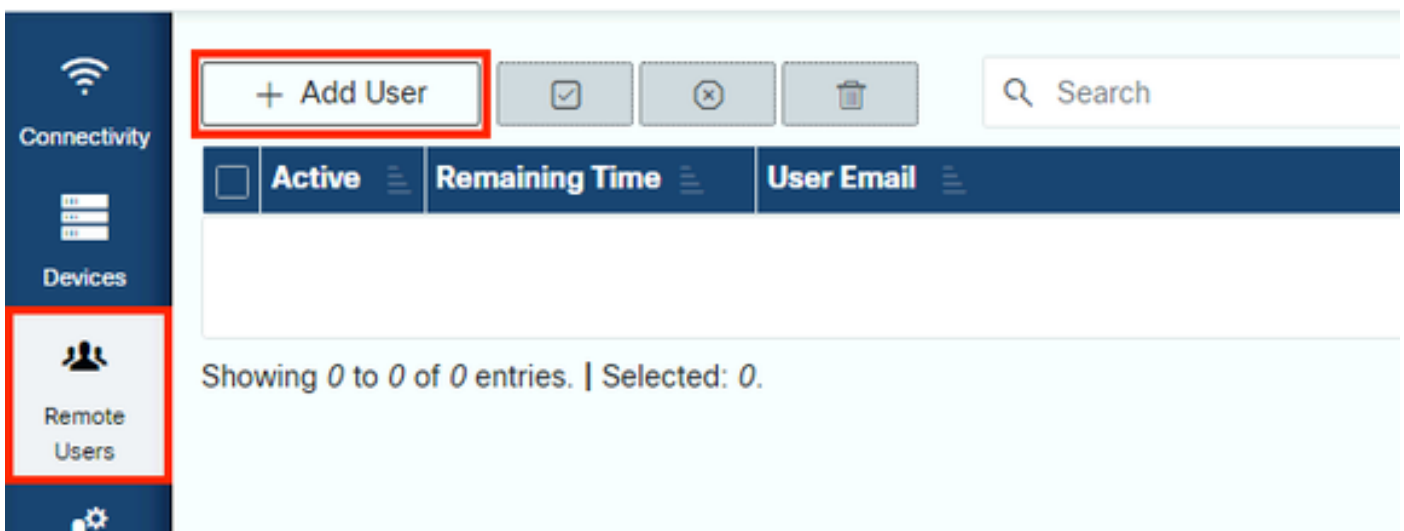


The screenshot shows a 'CUSTOMER CONTACT INFORMATION' form. On the right side, there is a section titled 'Edit RADKit Service ID'. It contains a checkbox 'Use RADKit for data collection' which is checked. Below it, the 'RADKit Service ID' is displayed as 'axt9-kplb-5dwc'. A red box highlights the 'Add/Edit RADKit Service ID' link. At the bottom of this section are 'Save' and 'Cancel' buttons.

또는 해당 케이스를 담당하는 TAC 엔지니어에게 ID를 언급하기만 하면 됩니다.

### 2. 원격 사용자 추가

어떤 사용자가 디바이스를 사용하여 작업할 수 있으려면 먼저 명시적 액세스를 제공하고 이 액세스가 유효한 상태로 유지되는 기간을 구성해야 합니다. 이렇게 하려면 RADKit WebUI에서 화면으로 이동하여 **Remote Users** 클릭하여 새 원격 사용자를 만듭니다 **Add User**.



The screenshot shows the 'Remote Users' management interface. On the left sidebar, 'Remote Users' is highlighted with a red box. The main area features a '+ Add User' button, also highlighted with a red box. To the right of the button are icons for checkmark, close, and delete. A search bar is visible on the right. Below the button is a table with columns: 'Active', 'Remaining Time', and 'User Email'. The table is currently empty, and the text 'Showing 0 to 0 of 0 entries. | Selected: 0.' is displayed below it.

TAC 엔지니어의 @cisco.com 이메일 주소를 입력합니다(오타 주의). 확인란과 또는 Activate this user 설정에 Time slice Manual 주의하

십시오.

사용자가 활성 상태일 때 RADKit 서비스를 통해 구성된 디바이스에 액세스할 수 있습니다. 단, 해당 디바이스가 활성화되어 있고 RBAC 정책에서 허용하는 경우에 한합니다.

타임 슬라이스는 사용자가 자동으로 비활성화되기까지의 시간을 나타냅니다. 즉, 타임 슬라이스는 시간 제한 문제 해결 세션을 나타냅니다. 사용자의 세션은 해당 사용자의 타임 슬라이스 기간까지 확장할 수 있습니다. 사용자를 수동으로 활성화/비활성화하려면 대신을 선택합니다Manual.

사용자는 타임 슬라이스를 구성했는지 여부에 관계없이 항상 수동으로 활성화/비활성화할 수 있습니다. 사용자가 비활성화되면 RADKit Service를 통한 모든 세션이 즉시 연결 해제됩니다.

완료되면 를 클릭하여 Remote Users(원격 사용자) 화면으로 돌아갑니다Add & close.

#### 관련 정보

- 일반적인 질문에 대한 자세한 정보와 답변은 RADKit 웹 사이트(<https://radkit.cisco.com/>)에서 확인할 수 있습니다.
- [Cisco 기술 지원 및 다운로드](#)

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.