FMC에서 Cisco RADKit 통합 구성

목차

소개

이 문서에서는 7.7 릴리스에 추가된 Cisco RADKit Integration in FMC 기능에 대해 설명합니다.

배경

방화벽 관리자가 직면한 문제

- Cisco에서 개발한 RADKit(Remote Automation Development Kit)는 사용자에게 안전한 방식으로 액세스하고 네트워크 장치의 문제를 해결할 수 있는 가능성을 제공하도록 설계된 네트워크 전반의 오케스트레이터입니다. https://radkit.cisco.com/
- Cisco FMC(Secure Firewall Management Center)는 FTD(Secure Firewall Threat Defense) 디바이스를 관리하고 운영합니다. 단일 FMC를 통해 다양한 위치에 있는 여러 디바이스를 관리할 수 있습니다.
- 사용자가 RADKit를 별도로 설치하고 FMC 및 FTD를 온보딩하는 것이 가능하지만, RADKit 서비스를 FMC에 구축하고 FMC 및 모든 관리되는 디바이스(FTD)를 자동화된 방식으로 온보딩하는 것이 최종 사용자에게 더 나은 경험이 될 수 있습니다.

사용 사례

RADKit를 FMC에 통합한 후 사용자가 얻을 수 있는 몇 가지 주요 기능은 다음과 같습니다.

- RADKit 클라이언트 CLI에서 원격으로 FMC/FTD에 액세스할 수 있는 기능.
- 필요한 모든 사람(예: Cisco TAC 엔지니어)에게 FMC/FTD에 대한 제어된 액세스를 제공할 수

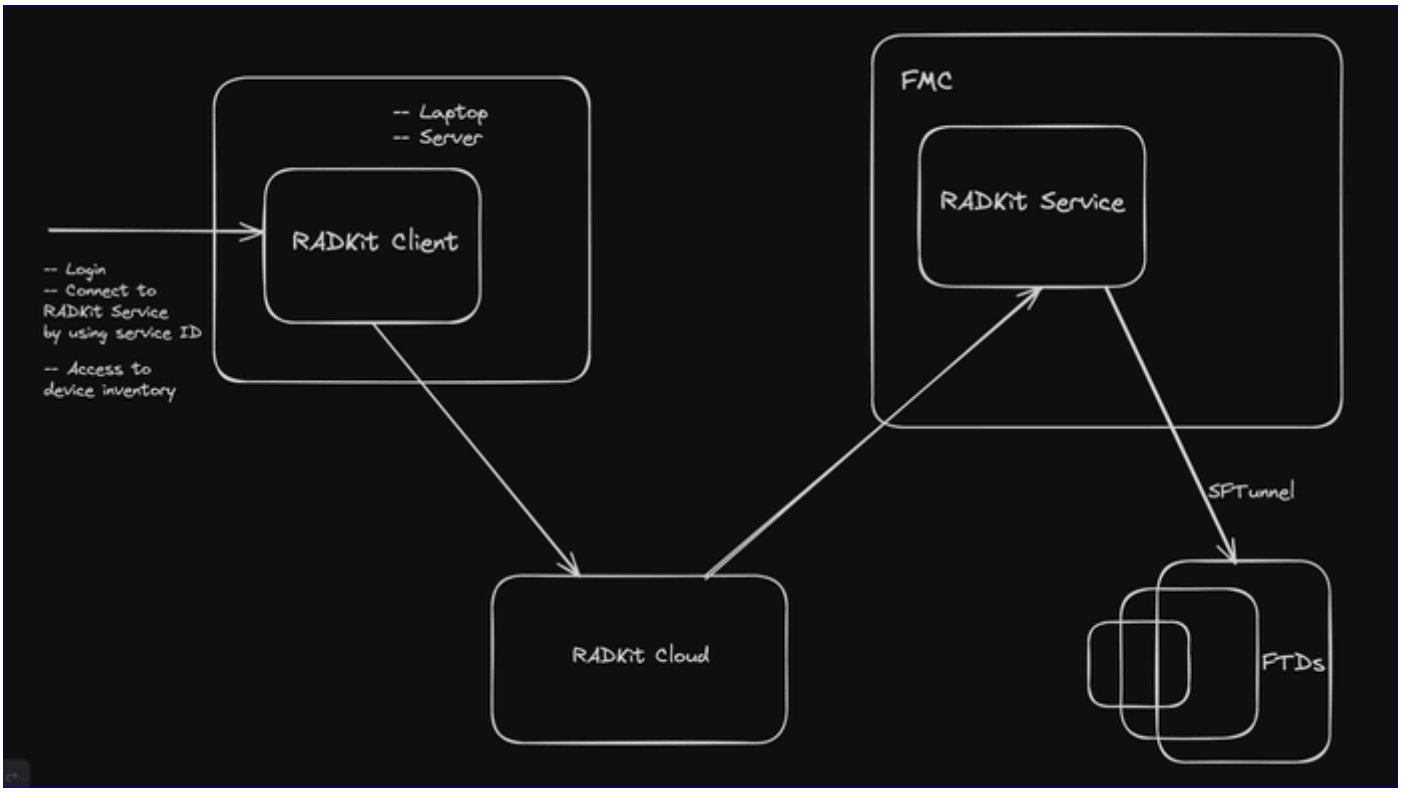
있습니다.
- RADKit 클라이언트에서 데이터를 수집하고 문제를 진단하기 위한 자동화 기능을 활용합니다(여러 디바이스에서 명령을 실행하는 스크립트를 RADKit 클라이언트에서 생성하고 사용할 수 있음).

새로운 기능 - 솔루션

- Secure Firewall 7.7.0부터 RADKit(Remote Automation Development Kit) 서비스가 FMC에 통합되었습니다.
- 사용자는 온디맨드 방식으로 RADKit 서비스를 활성화 또는 비활성화하고, RADKit 클라우드에 등록하고, 예약된 액세스 기간 동안 RADKit 클라이언트에서 특정 디바이스에 액세스하기 위한 원격 사용자 인증을 생성할 수 있습니다.
  - 권한 부여는 수정 또는 취소할 수 있습니다.
- 고급 문제 해결을 위해 디바이스에 sudo 액세스를 제공하는 옵션도 있습니다.

FMC 다이어그램의 RADKit 서비스 통합

이 다이어그램은 RADKit가 사용자(TAC 엔지니어)의 RADKit 클라이언트에서 프로덕션 FTD 디바이스로의 통신을 어떻게 활성화하는지를 보여줍니다.



기본: 지원되는 플랫폼, 라이센싱

애플리케이션 및 관리자

FTD		ASA	
FMC and FTD Platforms: All		Not supported	
FMC on 7.7.0 FMC REST API	Yes Yes	ASA CLI 9.23.1	No
FTD Supported Versions *(lowest version FMC on 7.7.0 can manage is 7.2)*	7.7.0 only	ASDM 7.23.1	No
Snort Support (Snort 3 is the only Snort version supported in 7.7)	Snort 3 Snort 2 (only for devices on 7.2.x..7.6.x)	CSM 4.30	No
FDM on 7.7.0	No		

기타 지원 측면

Platforms	
FTD	
Licenses Required	No licensing requirements for this feature.
Works in Evaluation Mode	Yes
IP Addressing	IPv4 IPv6
Multi-instances supported?	Yes
Supported with HA'd devices	Yes
Supported with clustered devices?	Yes
Other (only routed mode | transparent mode), etc.	No Special Notes
Internet access for the RADKit cloud enrollment required	Access to prod.radkit-cloud.cisco.com

기능을 작동시키기 위한 종속성

- 최소 버전은 Secure Firewall 7.7.0입니다.
- FMC 내에서 호스팅되는 RADKit 서비스에 연결하려면 지원 엔지니어의 컴퓨터에 https://radkit.cisco.com/downloads/release/에서 RADKit 클라이언트를 설치해야 합니다.
- RADKit 클라이언트의 기본 버전은 1.6.10 이상입니다.
- RADKit 서비스가 이전 RADKit 클라이언트 버전과 역호환되므로 이전 버전의 RADKit 클라이언트를 사용할 수 있습니다.

기능 설명 및 연습

기능 개요

- RADKit Service를 FMC에 통합하면 장치 관리자는 문제 해결 및 자동화 목적으로 네트워크의

특정 FMC 및 FTD 장치에 대한 원격 사용자(Cisco TAC 엔지니어)의 액세스를 제공할 수 있습니다. RADKit는 화면 공유보다 문제 해결에 훨씬 더 효율적이며, 사용자의 컴퓨터를 제어할 필요가 없으며, 네트워크에서 작업할 수 있는 더 안전한 방법이며, Webex를 훌륭하게 보완합니다.

- 따라서 장치 관리자가 RADKit 서비스를 별도로 설치 및 구성할 필요가 없으므로 기술 지원에 대한 경험이 더 우수합니다. 또한 Cisco TAC 엔지니어의 지원 시간이 단축되어 지원 문제를 해결할 수 있습니다.

구성 단계: 개요

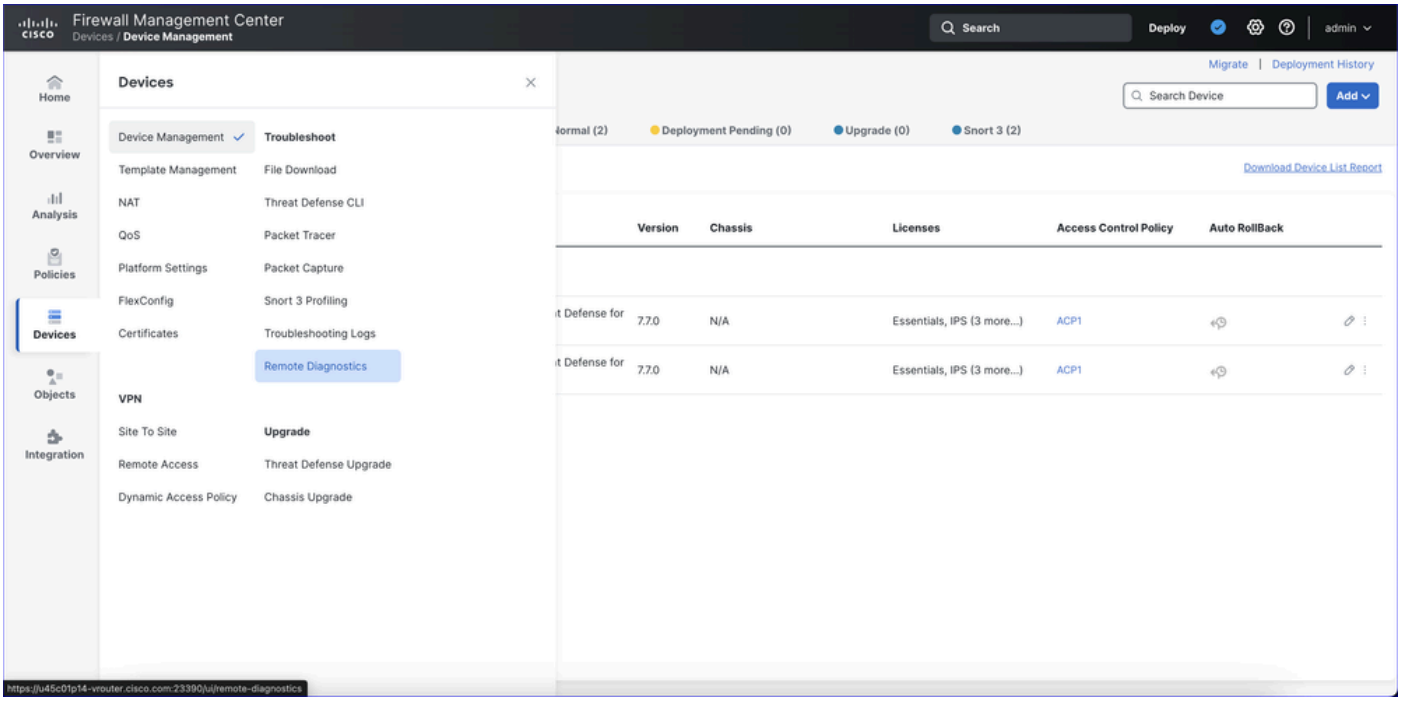
1. 장치 관리자(FMC 관리자 사용자): RADKit 서비스를 활성화 및 등록하고 FMC GUI에서 권한 부여를 구성합니다.

2. 시스코 TAC/시스코 지원: 컴퓨터에 RADKit 클라이언트를 설치하고 RADKit 클라이언트에서 장치에 액세스하고 문제를 해결합니다.

FMC 관리자 사용자: 방화벽 관리 센터 연습

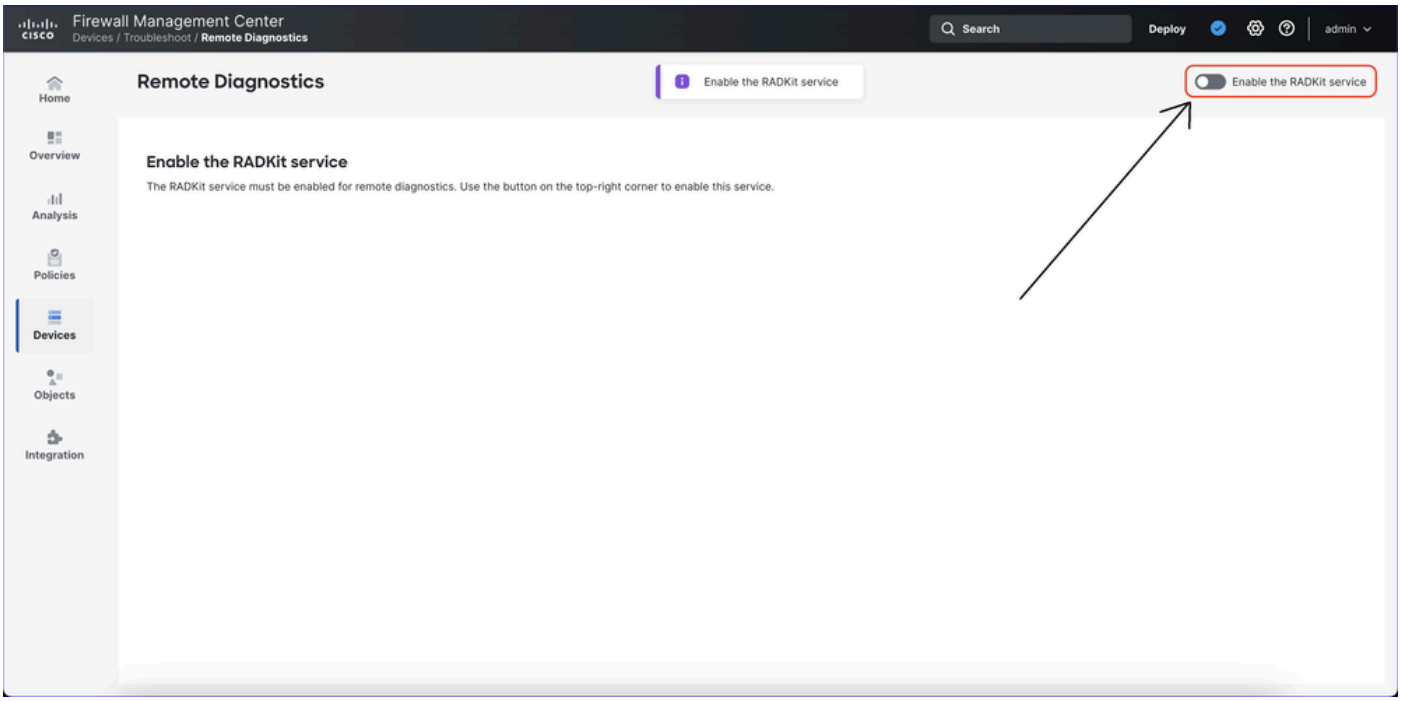
원격 진단 메뉴

- 이 기능에 대한 새 "원격 진단" 메뉴 항목이 [장치] -> [문제 해결]에 추가되었습니다.
- 관리자, 네트워크 관리자 및 유지 보수 사용자는 페이지에 대한 읽기/쓰기 권한을 갖습니다.
- Security Analyst(보안 분석가), Security Analyst(Read Only) 및 Security Approver(보안 승인자) 사용자는 이 페이지에 대한 읽기 전용 권한을 갖습니다.



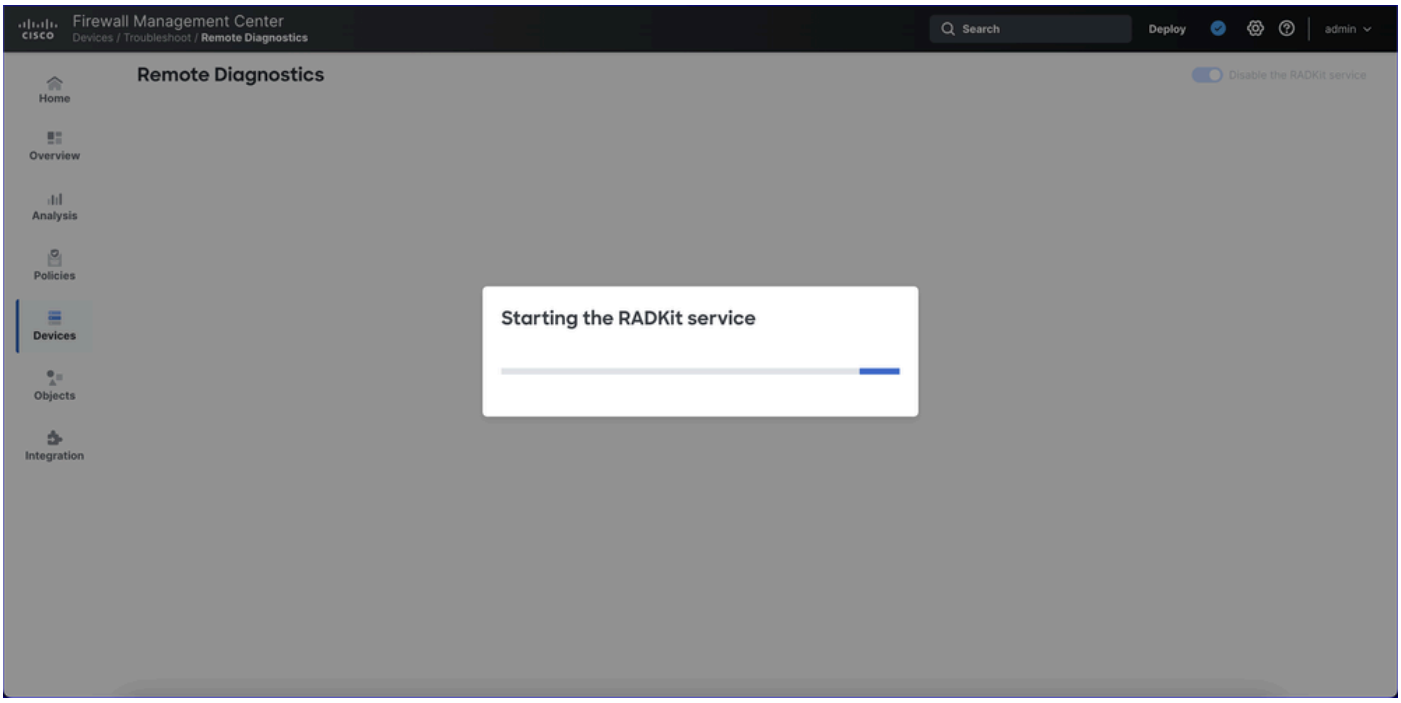
초기 원격 진단 페이지

이것은 초기 원격 진단 페이지입니다. RADKit 서비스는 "RADKit 서비스 활성화" 스위치를 전환하여 활성화할 수 있습니다.



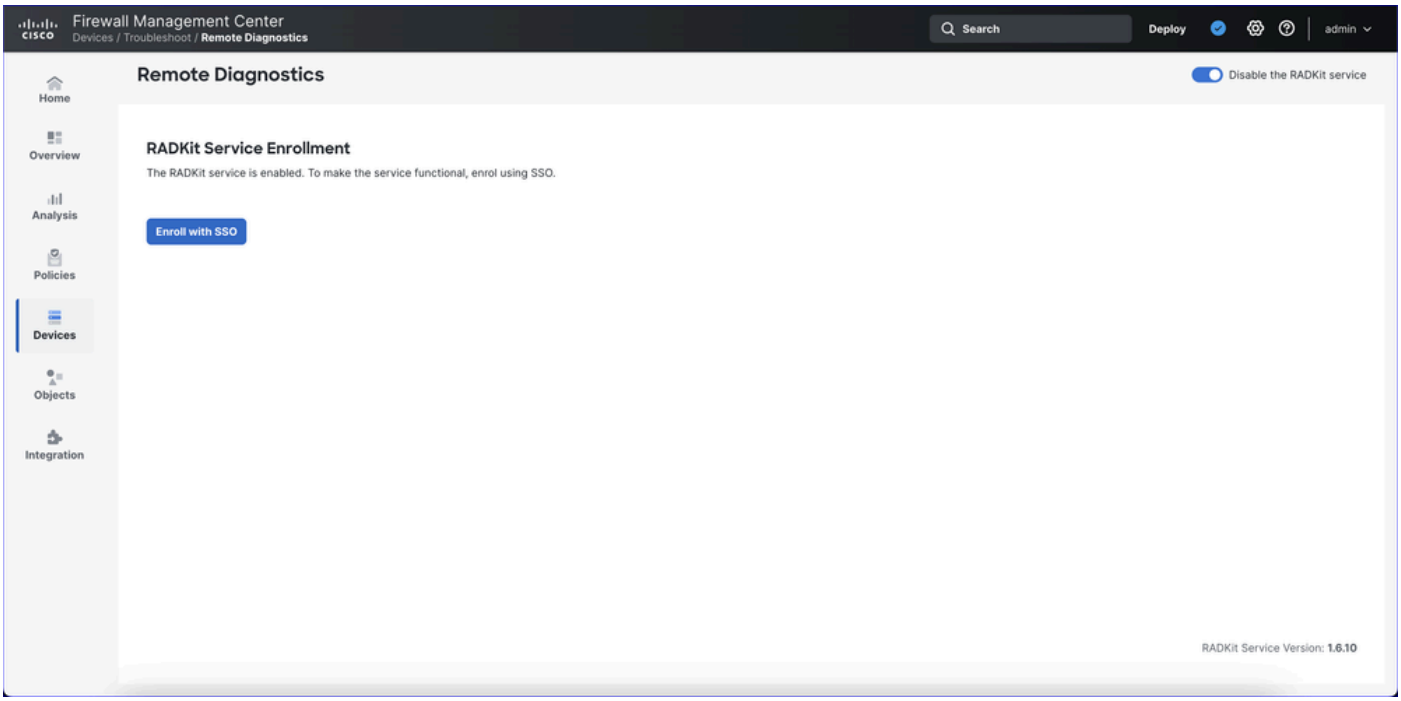
RADKit 서비스 시작

RADKit 서비스를 활성화한 후 RADKit 서비스가 시작될 때까지 진행률 표시줄이 나타납니다.



RADKit 서비스 사용

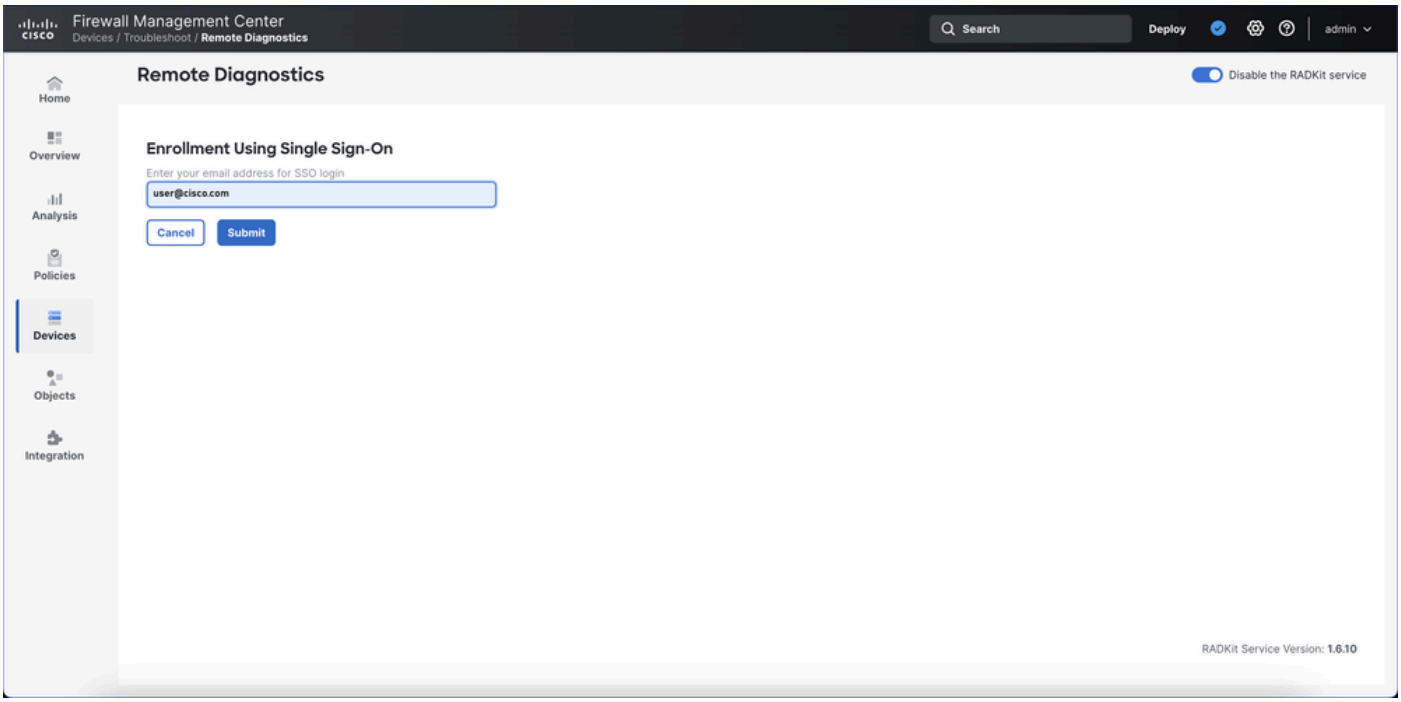
- RADKit 서비스 활성화 프로세스가 완료되면 이 페이지가 표시됩니다.



다음 단계는 "Enroll with SSO(SSO로 등록)" 버튼을 클릭하여 RADKit 클라우드에 등록하는 것입니다.

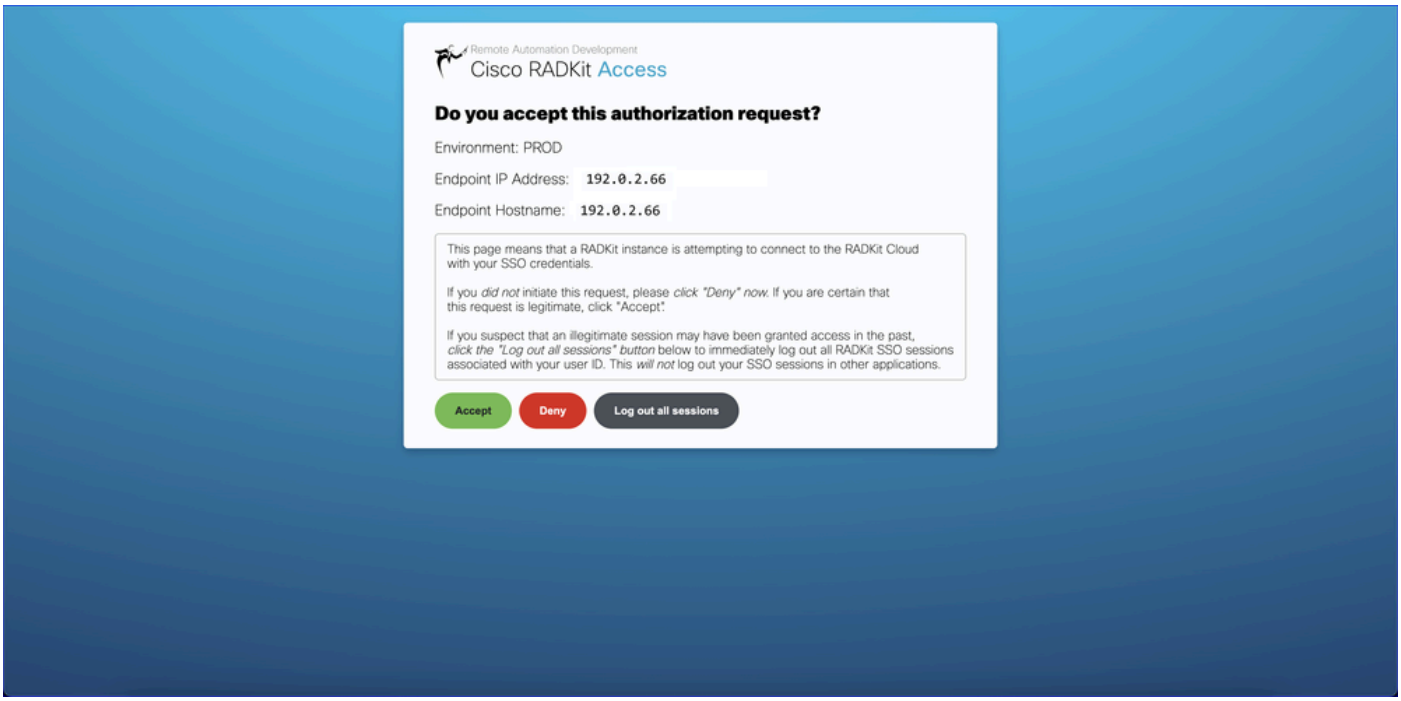
SSO 등록 - 이메일 주소 입력

등록 프로세스의 1단계는 RADKit 클라우드 등록에 대한 사용자 이메일 주소를 입력하는 것으로 구성됩니다.



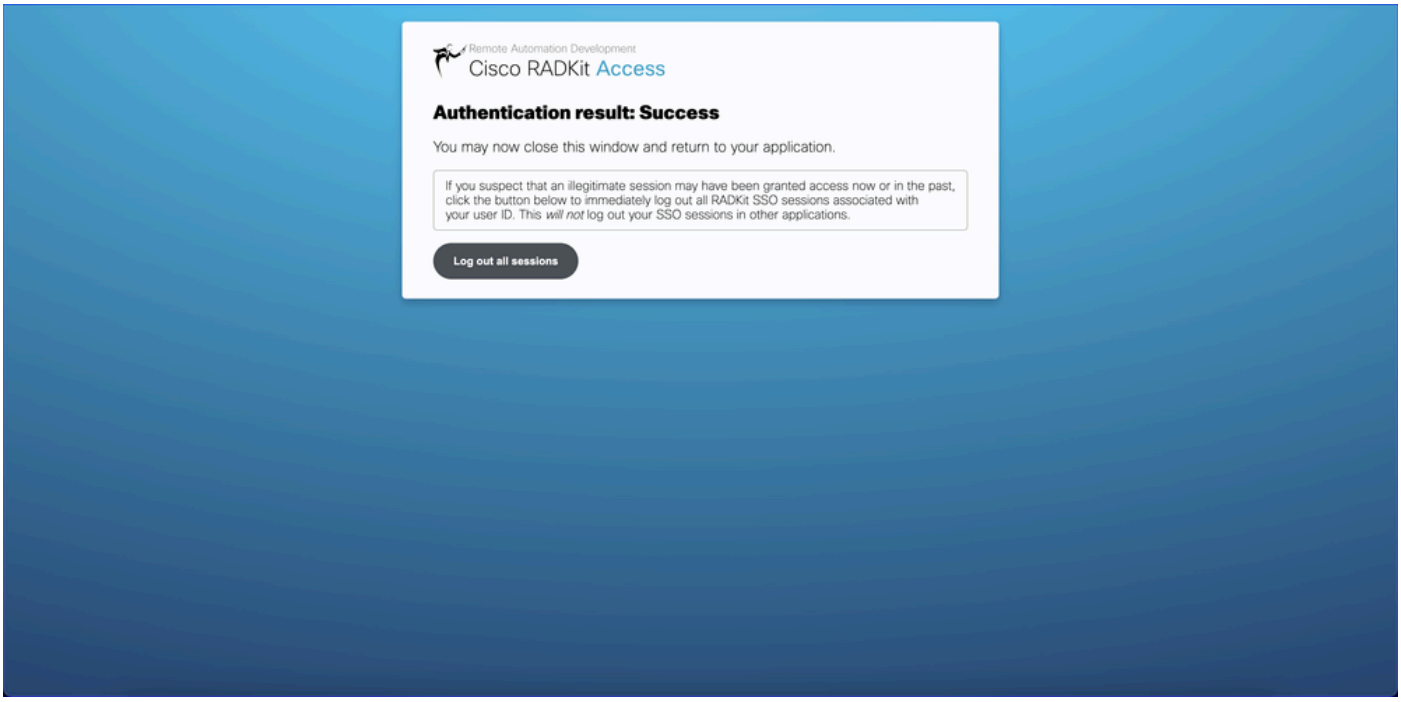
SSO에 등록 - 권한 부여 요청 수락

새 브라우저 탭(또는 브라우저 설정에 따라 창)이 열립니다. Accept(수락) 버튼을 클릭합니다.



SSO에 등록 - 인증 성공

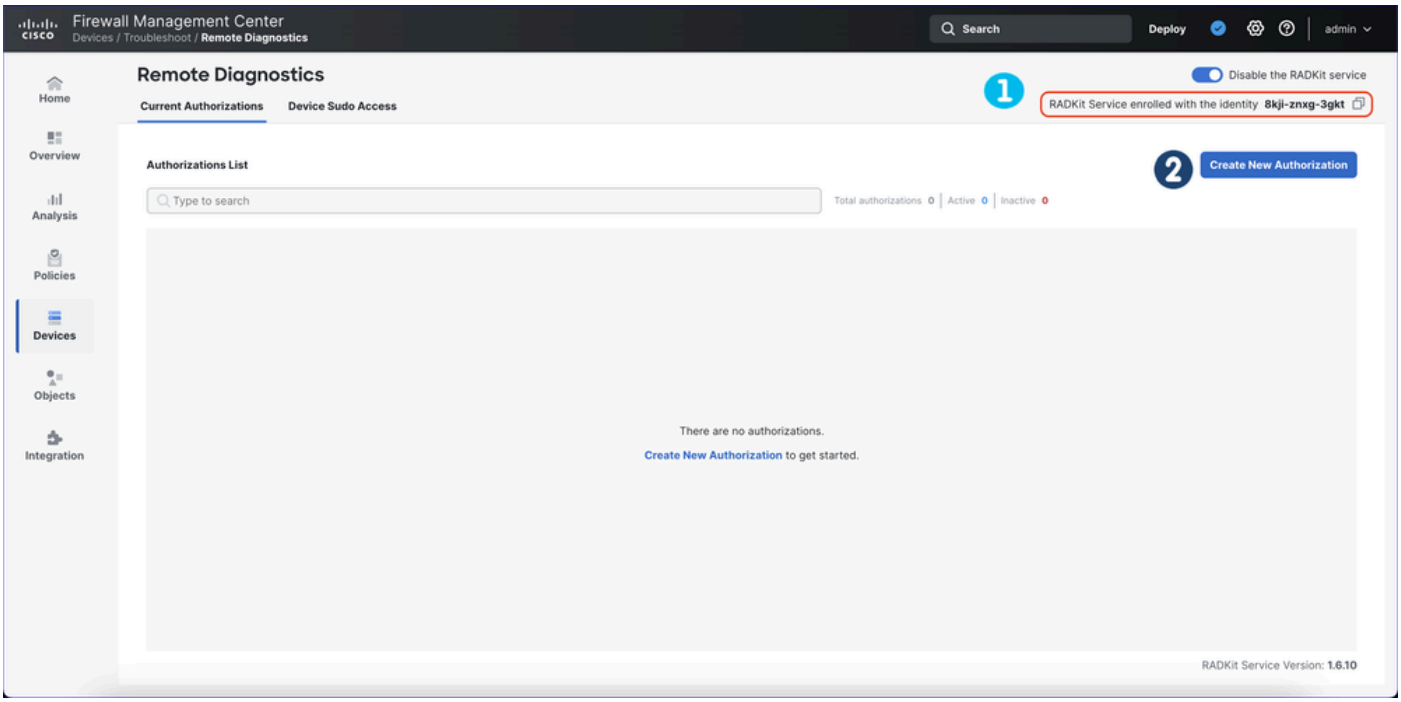
인증에 성공하면 사용자가 브라우저 탭을 닫고 FMC Remote Diagnostics 페이지로 돌아갈 수 있습니다.



RADKit 서비스 등록됨

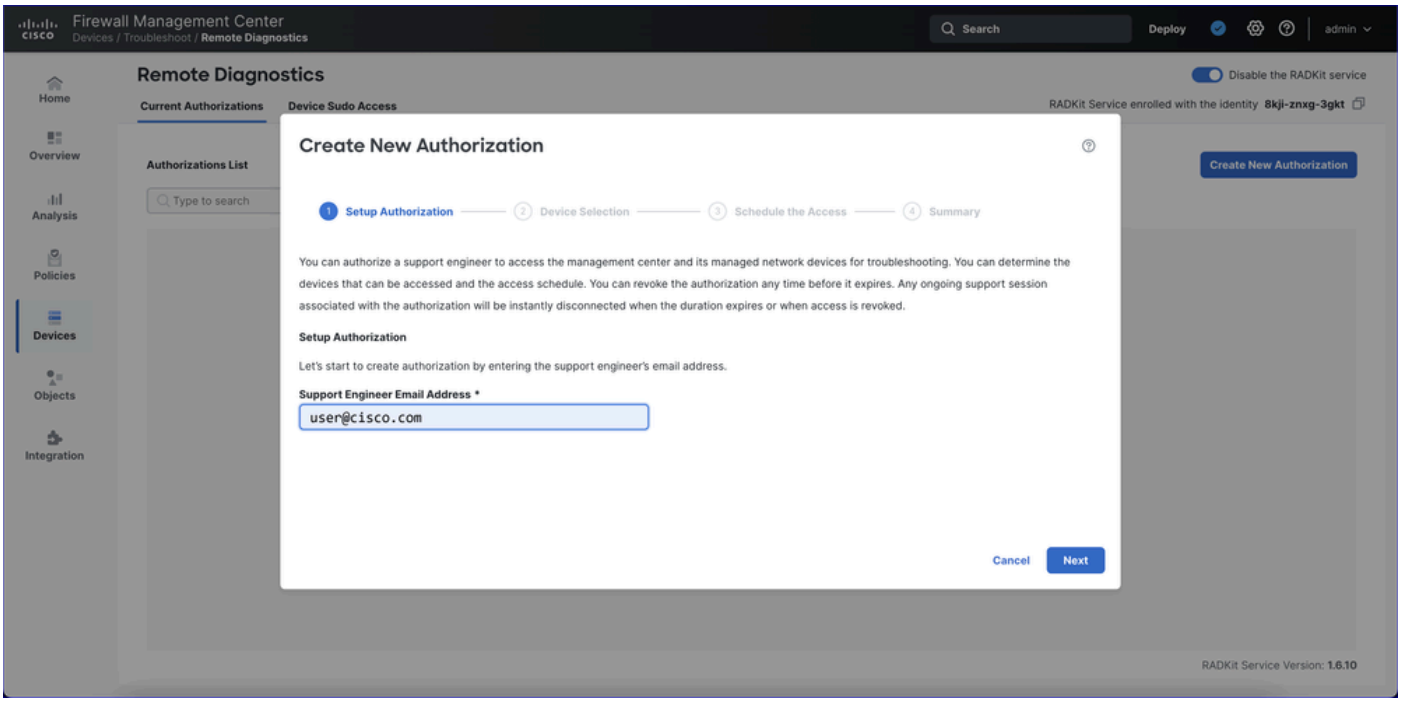
RADKit 서비스는 지정된 서비스 ID로 등록됩니다(이 예에서 ID는 8kji-znxg-3gkt). ID를 클립보드에 복사할 수 있습니다. RADKit 클라이언트에서 RADKit 서비스에 연결할 수 있도록 Cisco TAC 엔지니어에게 제공합니다.

다음 단계는 "Create New Authorization(새 권한 부여 생성)" 버튼을 클릭하여 권한 부여를 생성하는 것입니다.



새 권한 부여 만들기: 1단계

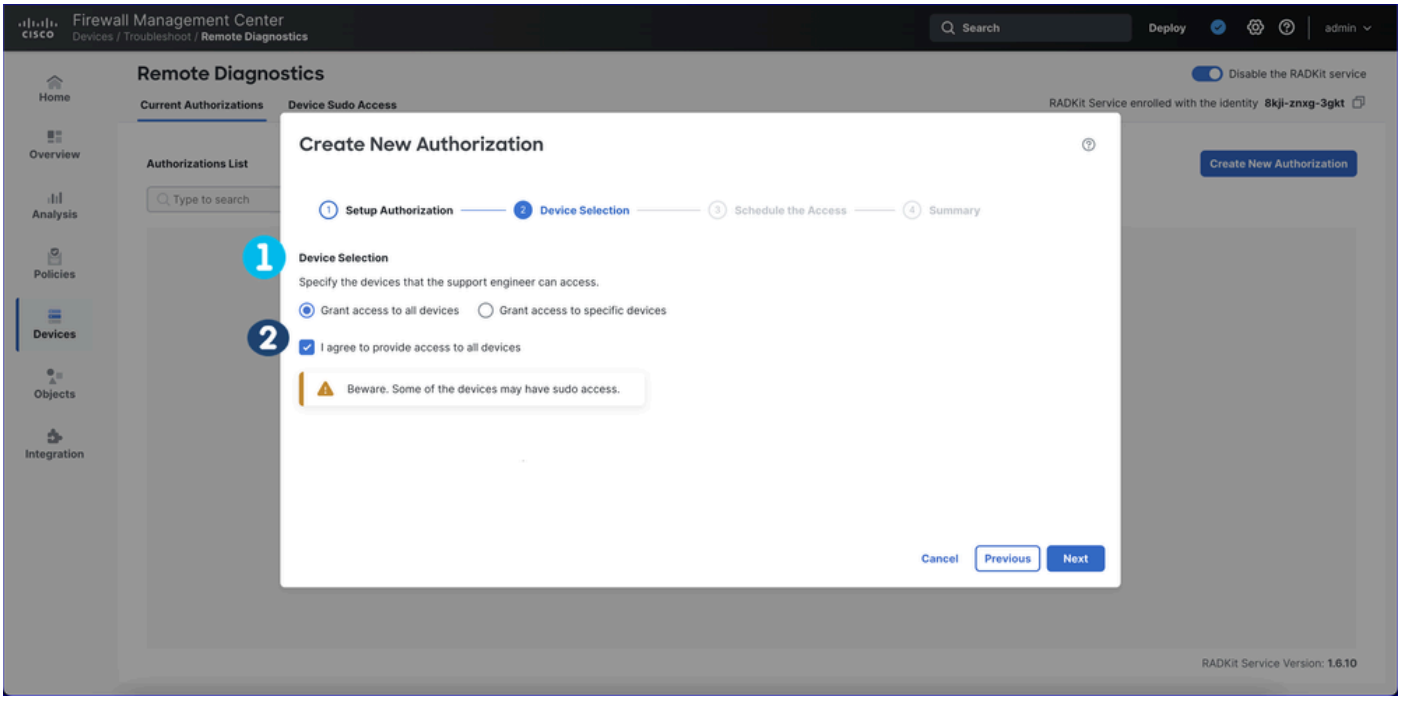
- 새 권한 부여를 생성하기 위한 첫 번째 단계는 지원 엔지니어 이메일 주소를 추가하는 것입니다.
- 새 권한 부여를 생성하는 네 가지 단계가 있습니다. 단계를 따라 진행이 상단에 표시됩니다.



새 권한 부여 만들기: 2단계

- 1단계: 지원 엔지니어가 액세스할 수 있는 디바이스를 지정합니다. 또는 이 예와 같이 모든 디바이스에 대한 액세스 권한을 부여합니다.

- 2단계: 모든 디바이스 또는 특정 디바이스의 라디오 버튼을 선택합니다. 특정 디바이스의 경우 FMC 및/또는 FTD를 선택할 수 있습니다. Device Sudo Access(디바이스 Sudo 액세스) 탭의 일부 디바이스에 sudo 액세스가 제공될 수 있다는 경고를 참고하십시오. 확인란을 선택해야 다음 단추가 활성화됩니다.
- Sudo 액세스는 나중에 권한 부여 생성 중이 아니라 Device Sudo Access(디바이스 Sudo 액세스) 탭에서 디바이스별로 제공됩니다.

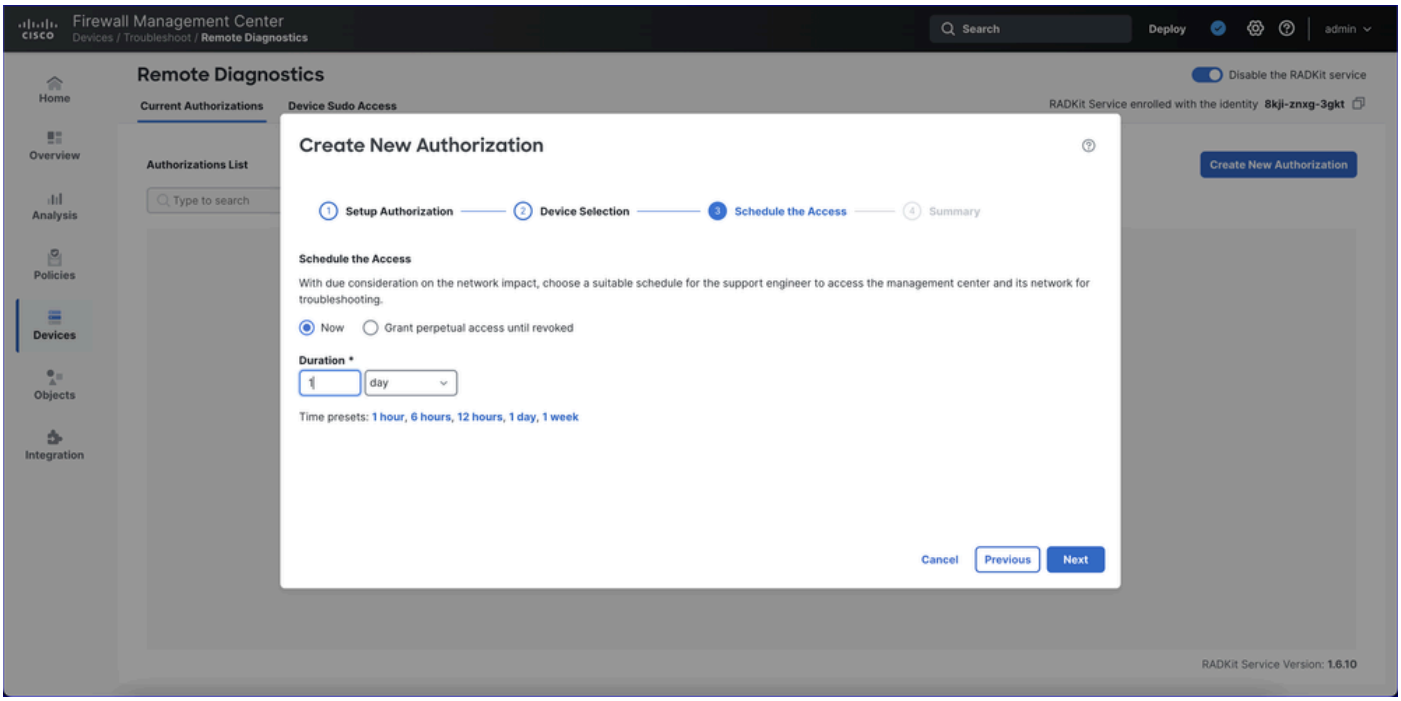


디바이스 선택 관련 참고 사항

- 지원되는 빌드의 디바이스(예: 초기 릴리스에서는 7.7.0 디바이스만)만 선택할 수 있습니다.
- 비활성화되어 있고 연결할 수 없는 디바이스는 선택할 수 없습니다. RADKit는 sftunnel(TCP 8305)을 사용하여 디바이스에 액세스합니다.
  - sftunnel 연결 문제가 있는 경우 작동하지 않지만 RADKit 인벤토리에 계속 표시됩니다.
  - 디바이스의 전원이 꺼진 경우에는 디바이스가 전혀 표시되지 않습니다.
- HA 쌍에 FMC가 있는 경우 Active/Primary만 추가할 수 있습니다.
- 권한 부여를 생성/수정할 때 디바이스가 RADKit 인벤토리에 추가됩니다. FMC에서 디바이스의 등록을 취소하면 디바이스의 "인벤토리"에서 제거됩니다.

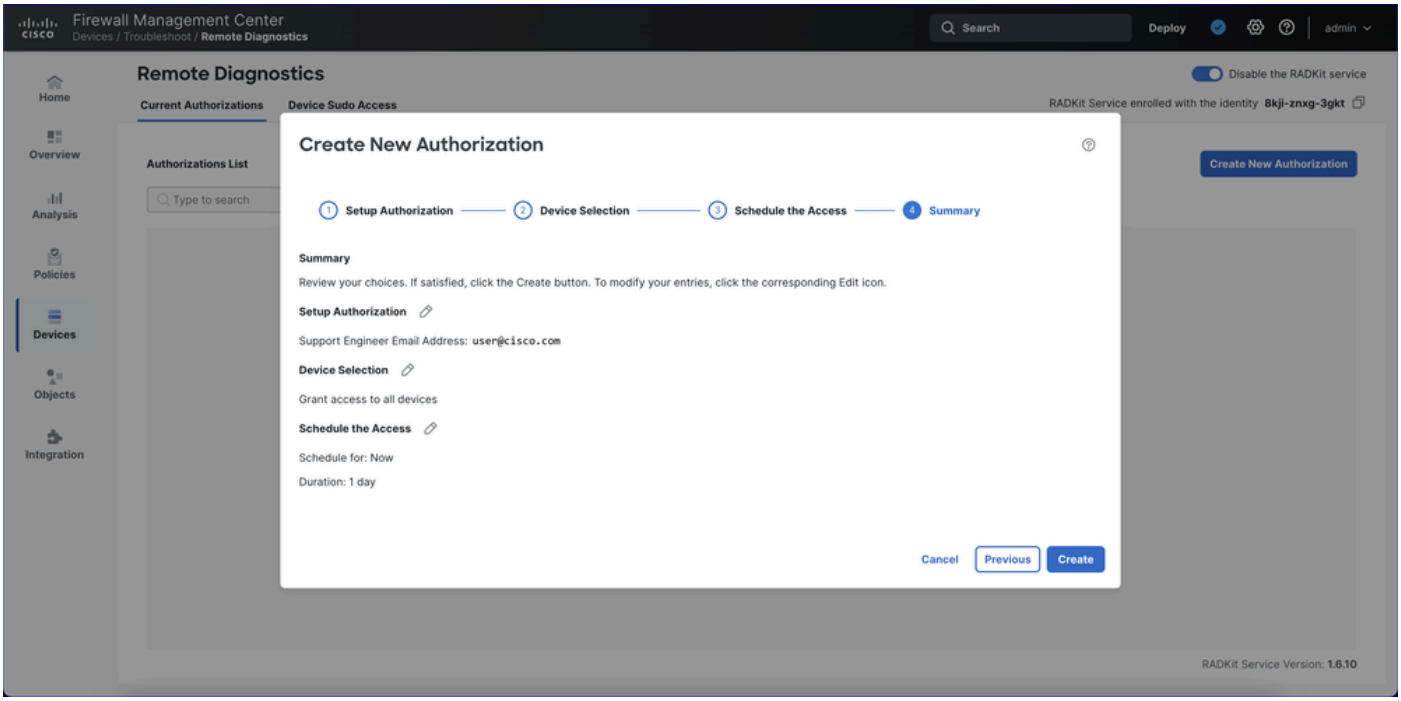
새 권한 부여 만들기: 3단계

- 3단계: 지원 엔지니어가 장치에 액세스하는 기간을 지정합니다.
- "지금"을 선택하고 기간을 지정하거나,
- "해지될 때까지 영구 액세스 허용"을 선택하십시오.
- 기본 기간은 1일입니다. 모든 기간을 설정할 수 있습니다. 일부 미리 정의된 기간 값도 있습니다.



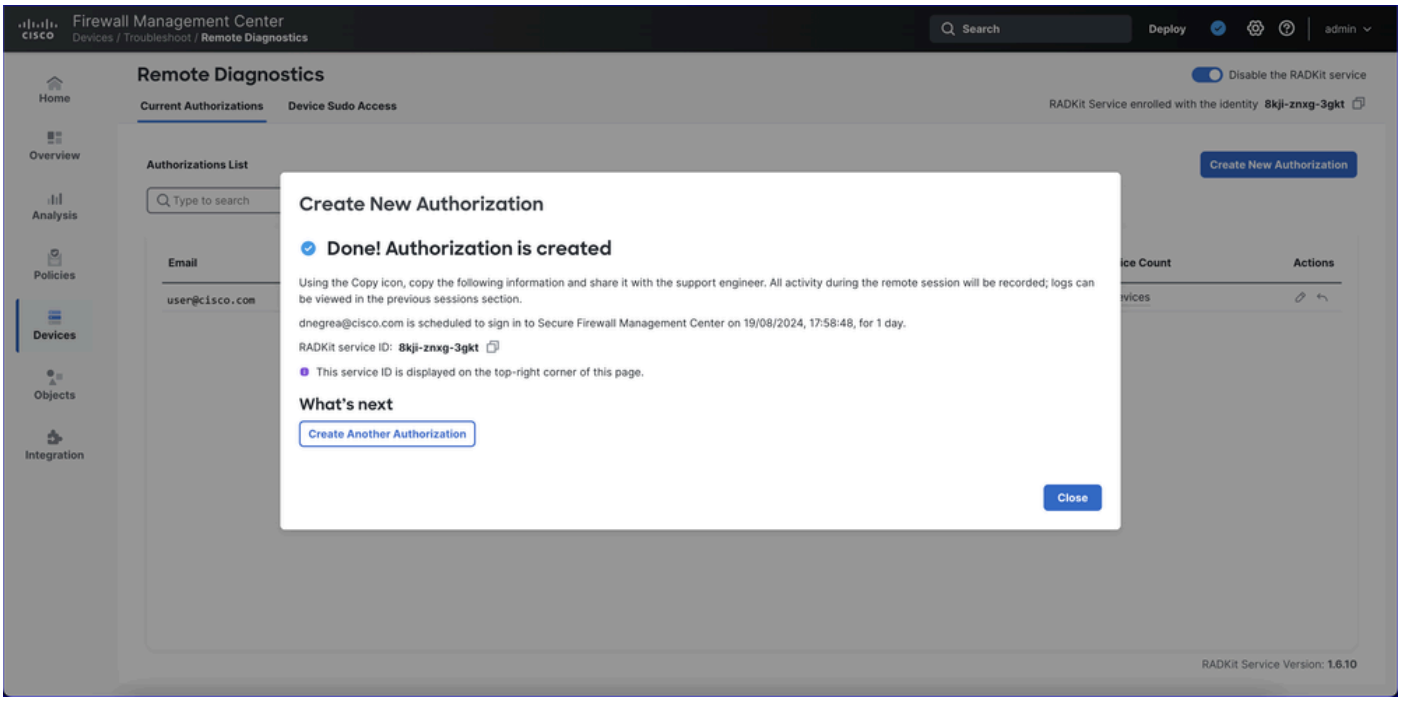
새 권한 부여 요약 만들기

마지막 단계는 권한 부여 요약입니다. 여기서 사용자는 구성을 검토하고 수정할 수 있습니다.



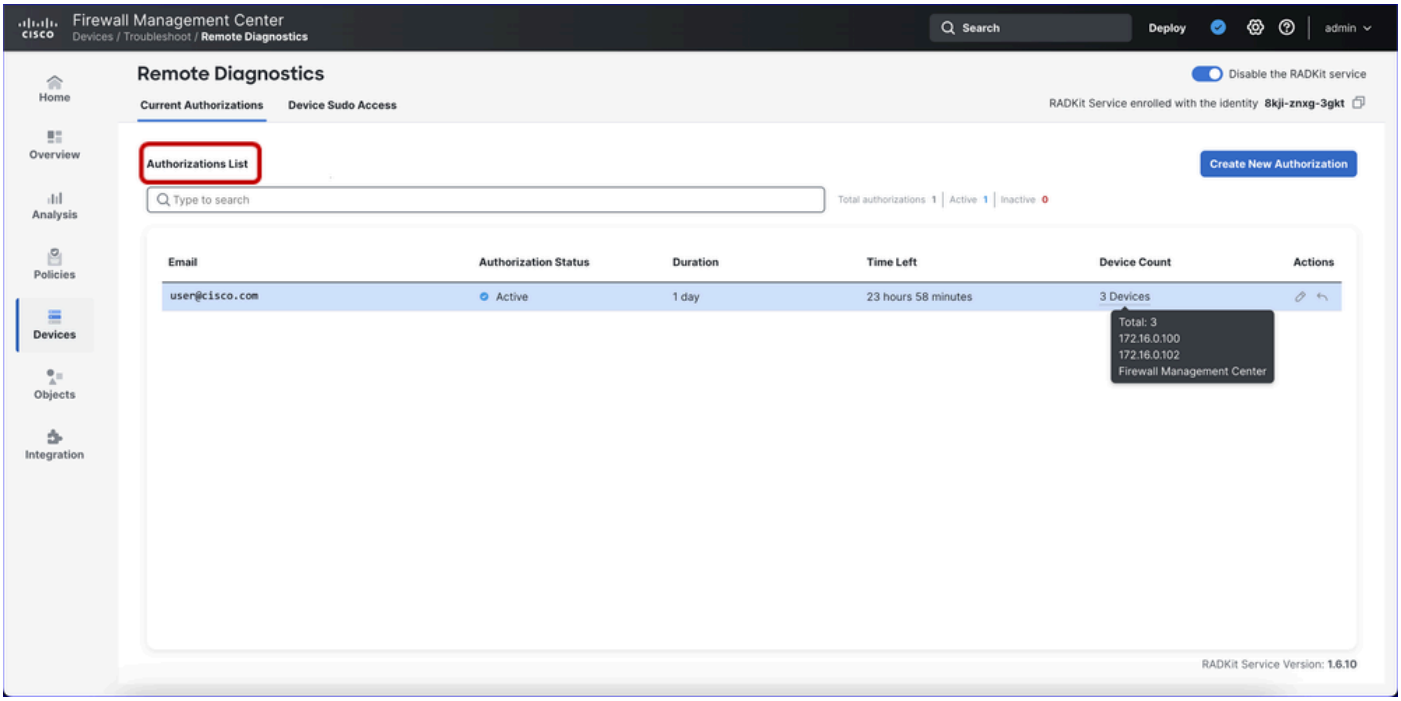
새 권한 부여 만들기 완료

승인 생성이 완료되면 확인 화면이 표시됩니다.



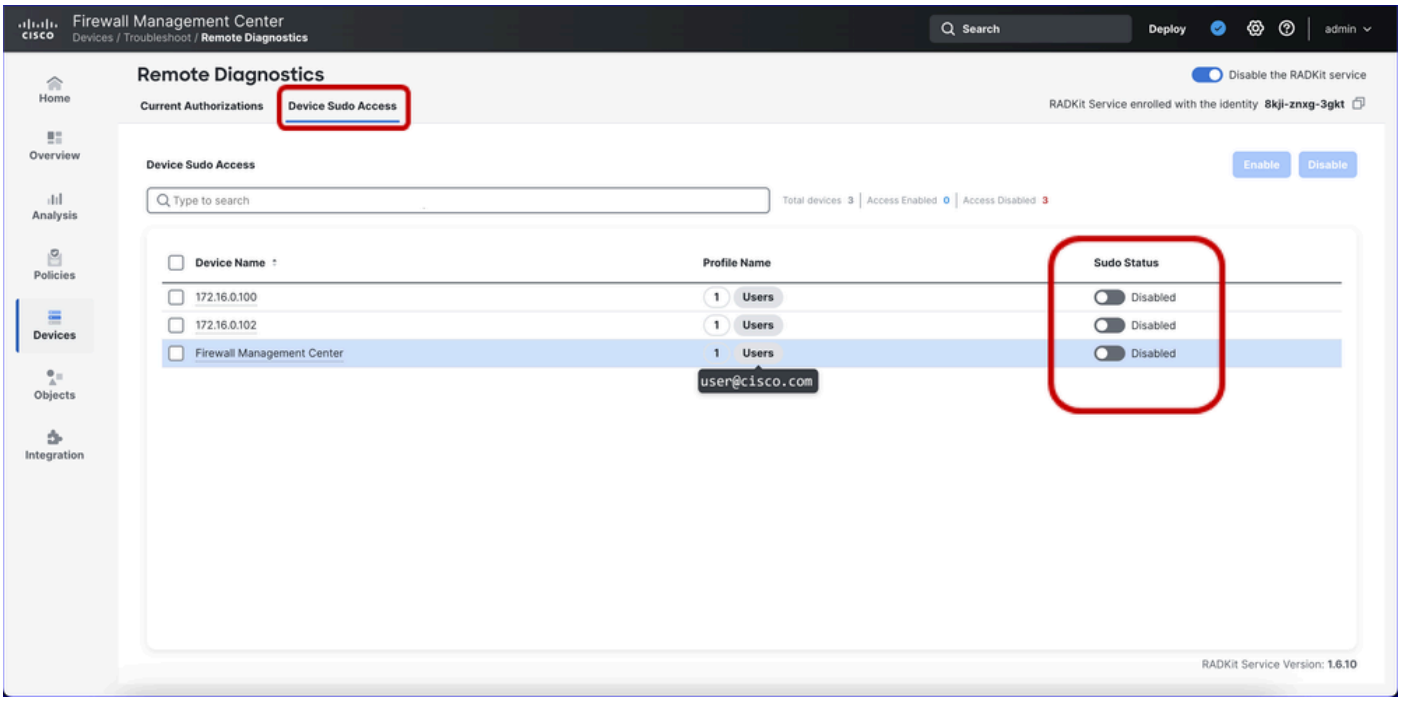
Revoke를 포함한 현재 Authorizations 목록

- 현재 인증 목록이 현재 인증 탭에 표시 됩니다.
- Actions(작업)(맨 오른쪽 열)는 Revoke access(액세스 취소) 및 Edit authorization(권한 부여 수정)입니다.



디바이스 Sudo 액세스 목록

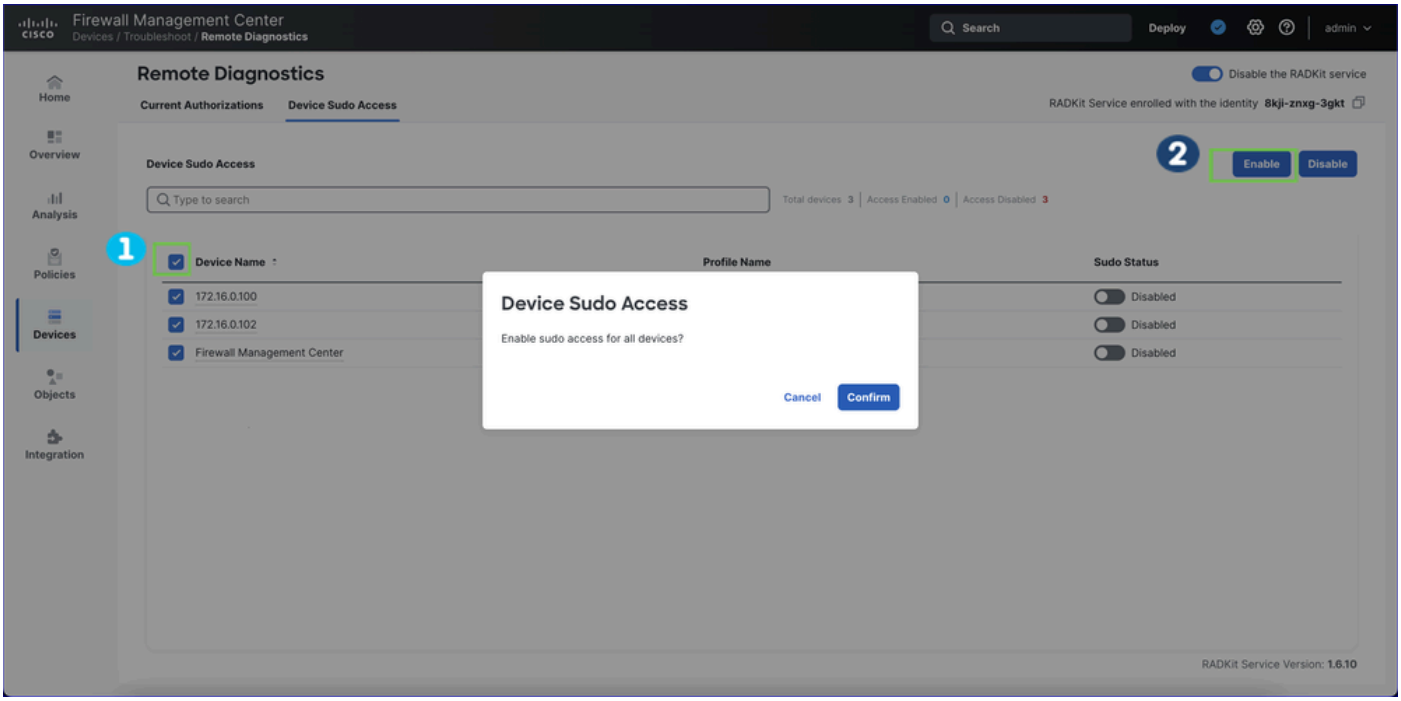
- Sudo 액세스 설정이 있는 디바이스의 목록은 Device Sudo Access(디바이스 Sudo 액세스) 탭에 표시됩니다.
- sudo 액세스를 전환하려면 오른쪽 열의 전환을 사용합니다. 기본적으로 꺼져 있습니다.
- 또한 대량 Sudo 액세스를 활성화/비활성화할 수 있습니다.



디바이스 Sudo 액세스 활성화 확인

1. Sudo 액세스는 장치를 선택한 다음 "Enable(활성화)" 버튼을 클릭하여 모든 장치에 대해 또는 일부 특정 장치에 대해서만 활성화할 수 있습니다.

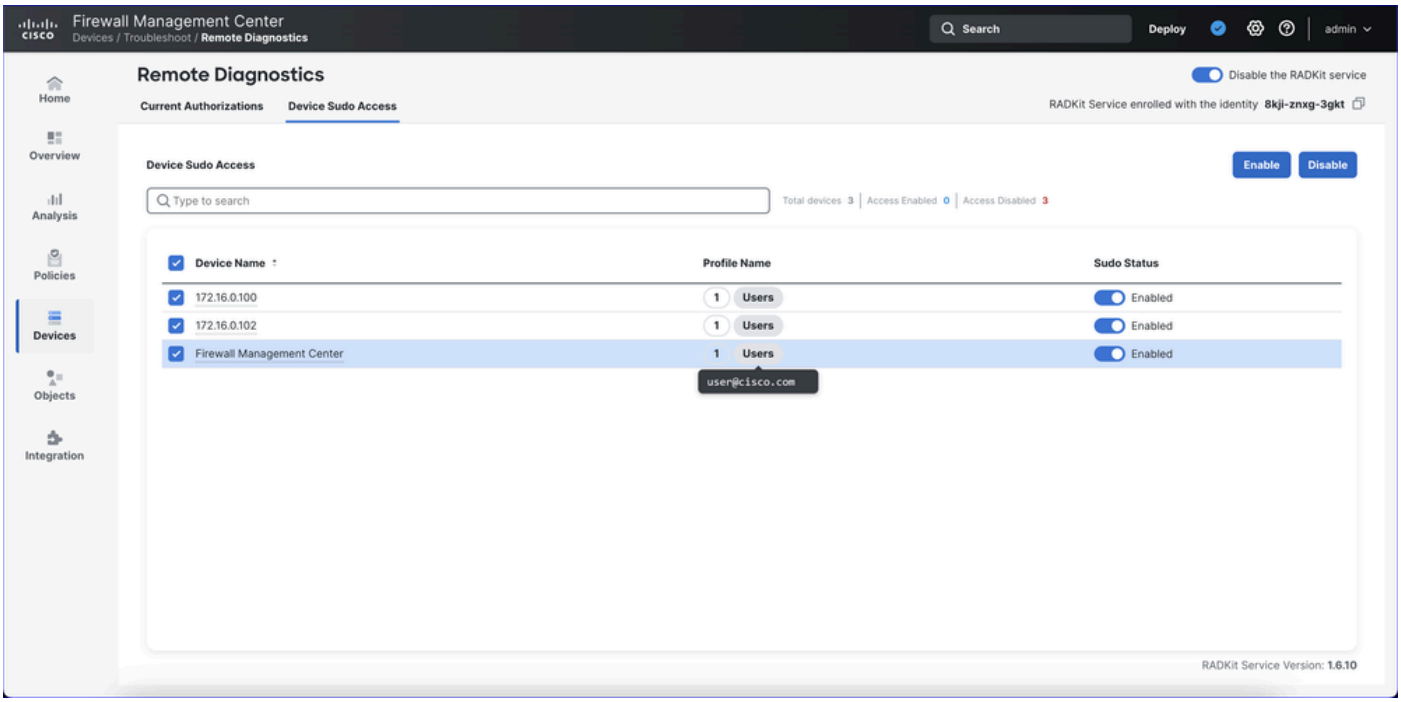
2. 활성화하면 확인 대화 상자가 나타나고 확인을 클릭해야 합니다.



장치 Sudo 액세스 사용

- 디바이스에 대한 sudo 액세스를 활성화하거나 비활성화한 후 페이지 오른쪽의 Sudo Status 열이 업데이트됩니다.
- 지원 엔지니어는 디바이스에서 sudo su를 실행할 수 있습니다. 비밀번호도 없습니다. 지원 엔

지니어가 루트 비밀번호를 가질 필요가 없습니다.



기타 참고 사항

- FMC 사용자가 액세스할 수 있는 도메인의 디바이스만 표시되며 원격 액세스를 위해 인증될 수 있습니다.
- FMC가 HA에 있는 경우:
  - RADKit 서비스는 Active/Primary에서만 활성화할 수 있습니다.
  - 보조 FMC는 현재 RADKit 클라이언트에서 액세스할 디바이스로 추가할 수 없습니다.
- 한 번에 하나의 지원 엔지니어에만 권한을 부여할 수 있습니다.
  - 다른 지원 엔지니어가 액세스할 수 있어야 하는 경우, 추가 엔지니어에 대한 다른 권한 부여를 생성합니다. 서비스 ID는 동일합니다.

FMC REST API

RADKit 서비스 REST API

RADKit Service에서 생성 및 읽기 작업을 지원하기 위해 다음과 같은 새로운 URL이 도입되었습니다.

- 가져오기: /api/fmc_troubleshoot/v1/domain/{domainUUID}/radkit /services
  - FMC에서 모든 RADKit 서비스 데이터를 검색합니다.
- 가져오기: /api/fmc_troubleshoot/v1/domain/{domainUUID}/radkit/services/{id}
  - 지정된 ID에서 RADKit 서비스 데이터를 가져오거나 가져옵니다.
- POST: /api/fmc_troubleshoot/v1/domain/{domainUUID}/radkit/services
  - FMC에서 RADKit 서비스를 생성합니다(서비스 활성화/비활성화).

RADKit 서비스 모델

RADKit 서비스 모델은 다음과 같이 구성됩니다.

- 유형
- ID
- 상태
- 등록됨
- 서비스 ID
- 버전


```
{
  "type": "RADKitService",
  "id": "DummyContainerId",
  "status": "RUNNING",
  "isEnrolled": true,
  "serviceId": "8kji-znxg-3gkt",
  "version": "1.6.10"
}
```


Cisco 지원: RADKit 클라이언트 사용

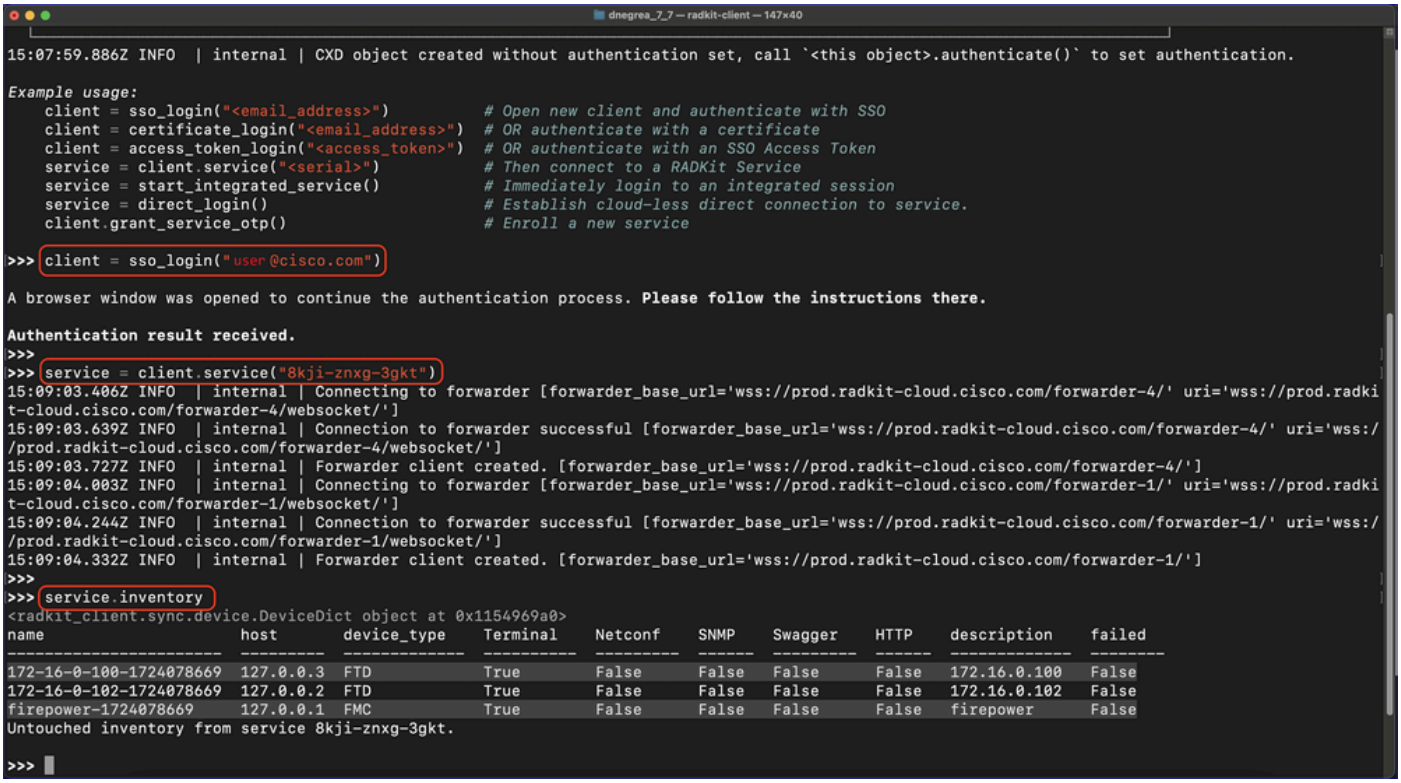
지원 측: RADKit 클라이언트 설치

- FMC/FTD에 액세스하려면 RADKit 클라이언트가 설치되어 있어야 합니다.
  - 클라이언트는 Windows, Mac 및 Linux 운영 체제에서 작동합니다.
- 지원에서는 여러 사용자의 여러 디바이스에 액세스할 수 있습니다. 각 RADKit 권한 부여에는 자체 "인벤토리"가 있습니다.
  - 지원을 받는 각 사용자 디바이스 인벤토리에 대해 RADKit 서비스 ID가 필요합니다.
  - 단일 인벤토리의 경우, 액세스 권한 부여 시 사용자가 지정한 대로 RADKit 클라이언트에서 FMC 및 해당 관리 FTD에 모두 액세스할 수 있습니다.

RADKit 클라이언트 가져오기 및 설치

RADKit 클라이언트는 https://radkit.cisco.com/downloads/release/에서 로컬로 설치한 다음 명령을 사용하여 터미널에서 시작할 수 있습니다. radkit 클라이언트

Windows, MacOS 및 Linux용 설치 프로그램을 사용할 수 있습니다.



로그인 명령이 포함된 RADKit 클라이언트 스크린샷(다음 섹션의 세부 사항).

RADKit 클라이언트 로그인 명령

- FMC에서 권한 부여 중에 사용자가 입력한 이메일 주소를 사용합니다.
- RADKit 클라이언트가 로그인하고 지정된 서비스 ID 명령에 연결합니다. 이 예에서 8abc-znxg-3abc의 RADKit 서비스 ID는 FMC에서 방화벽 관리자에게 표시되는 것과 일치해야 합니다.

<#root>

>>>

client = sso_login("user@cisco.com")

A browser window was opened to continue the authentication process.

Please follow the instructions there.

Authentication result received.

```
>>>
service = client.service("8abc-znxg-3abc")


15:09:03.639Z INFO  | internal | Connection to forwarder successful [forwarder_base_url='wss://prod.radk
15:09:03.727Z INFO  | internal | Forwarder client created. [forwarder_base_url='wss://prod.radkit-cloud
15:09:04.244Z INFO  | internal | Connection to forwarder successful [forwarder_base_url='wss://prod.radk
15:09:04.332Z INFO  | internal | Forwarder client created. [forwarder_base_url='wss://prod.radkit-cloud
```

RADKit 클라이언트 서비스 인벤토리 명령

원격 사용자(Cisco TAC 엔지니어)에게 액세스 권한이 부여된 인벤토리 목록을 표시하는 명령:

```
<#root>
>>>
service.inventory


<radkit_client.sync.device.DeviceDict object at 0x1154969a0>
name                      host       device_type    Terminal    Netconf    SNMP    Swagger    HTTP    de
------------------------  ---------  -------------  ----------  ---------  ------  ---------  ------  --
172-16-0-100-1724078669   127.0.0.3  FTD            True        False      False   False      False   17
172-16-0-102-1724078669   127.0.0.2  FTD            True        False      False   False      False   17
firepower-1724078669      127.0.0.1  FMC            True        False      False   False      False   fi
Untouched inventory from service 8kji-znxg-3gkt.
```

인벤토리의 디바이스에 대한 filter 명령이 있습니다(다음 섹션). 왼쪽 열의 이름을 사용하여 디바이스와의 인터랙티브 세션을 시작합니다(다음 섹션의 명령).

RADKit 클라이언트: 장치 필터링

인벤토리에서 디바이스를 필터링하기 위한 명령:

```
<#root>
>>>
ftds = service.inventory.filter(attr='name',pattern='172-16-0’)


>>>
ftds


<radkit_client.sync.device.DeviceDict object at 0x111a93130>
name host device_type Terminal Netconf SNMP Swagger HTTP description failed
```

```
---------------------- --------- ------------ ---------- --------- ------ --------- ------ ----------
172-16-0-100-1724078669 127.0.0.3 FTD True False False False False 172.16.0.100 False
172-16-0-102-1724078669 127.0.0.2 FTD True False False False False 172.16.0.102 False
2 device(s) from service 8kji-znxg-3gkt.
```

RADKit 클라이언트 장치 인터랙티브 세션 명령

이전 "service.inventory" 명령에서 가져온 "firepower-1724078669" 이름으로 디바이스(이 예에서는 FMC)에 대한 대화형 세션을 시작합니다.

```
<#root>

>>>

service.inventory["firepower-1724078669"].interactive()



08:56:10.829Z INFO | internal | Starting interactive session (will be closed when detached)
08:56:11.253Z INFO | internal | Session log initialized [filepath='/Users/use/.radkit/session_logs/clie

Attaching to firepower-1724078669 ...
Type: ~. to terminate.
~? for other shortcuts.
When using nested SSH sessions, add an extra ~ per level of nesting.

Warning: all sessions are logged. Never type passwords or other secrets, except at an echo-less passwor


Copyright 2004-2024, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Firepower Extensible Operating System (FX-OS) v82.17.0 (build 170)
Cisco Secure Firewall Management Center for VMware v7.7.0 (build 1376)
```

RADKit 클라이언트가 디바이스에서 명령 실행

디바이스에서 명령을 실행합니다!

```
<#root>

>>>

result = ftds.exec(['show version', 'show interface'])


>>>
>>>

result.status
```

```
<RequestStatus.SUCCESS: 'SUCCESS'>

>>>
>>>
result.result['172-16-0-100-1724078669']['show version'].data | print


> show version
-------------------[ firepower ]--------------------
Model : Cisco Secure Firewall Threat Defense for VMware (75) Version 7.7.0 (Build 1376)
UUID : 989b0f82-5e2c-11ef-838b-b695bab41ffa
LSP version : lsp-rel-20240815-1151
VDB version : 392
----------------------------------------------------
```

장치에서 파일 가져오기

- Cisco TAC 엔지니어는 RADKit 클라이언트를 통해 장치에 SSH를 적용하고 문제 해결 파일 생성을 비롯한 다양한 작업을 수행할 수 있습니다.

Cisco 지원: RADKit 콘솔

RADKit 네트워크 콘솔 사용

- RADKit 클라이언트를 사용하는 대신 Cisco TAC 지원 엔지니어가 RADKit Network Console을 사용할 수 있습니다. 네트워크 콘솔은 RADKit 클라이언트의 일부입니다.
- RADKit Network Console은 기본적인 RADKit Client 기능을 위해 간단한 CLI(Command Line Interface)를 제공하는 기능입니다. RADKit Service 인스턴스에 빠르게 연결하여 대화형 세션을 설정하고 번거롭지 않고 최소한의 교육으로 파일을 다운로드/업로드하는 데 사용됩니다.
- 명령줄을 사용하여 네트워크 콘솔을 시작합니다. radkit 네트워크 콘솔
- 자세한 내용은 RADKit 설명서를 참조하십시오.

업그레이드 및 이전 버전과의 호환성

7.7 이상 7.7로 업그레이드

- RADKit Service는 Secure Firewall 7.7.0에 추가되었습니다.
  - 버전 7.7.0 이상으로 업그레이드된 디바이스에는 RADKit 서비스에 필요한 컨피그레이션이 있습니다.

지원되지 않는 FTD가 있는 환경

- FMC 및 FTD가 이 기능을 작동하려면 최소 버전 7.7.0이 있어야 합니다(7.7 미만의 버전을 사용하는 FTD는 7.7 FMC RADKit 권한 부여에 추가할 수 없음).

- 7.7.0에 없는 등록된 FTD는 권한 부여를 활성화하기 위해 선택할 수 없습니다.

문제 해결

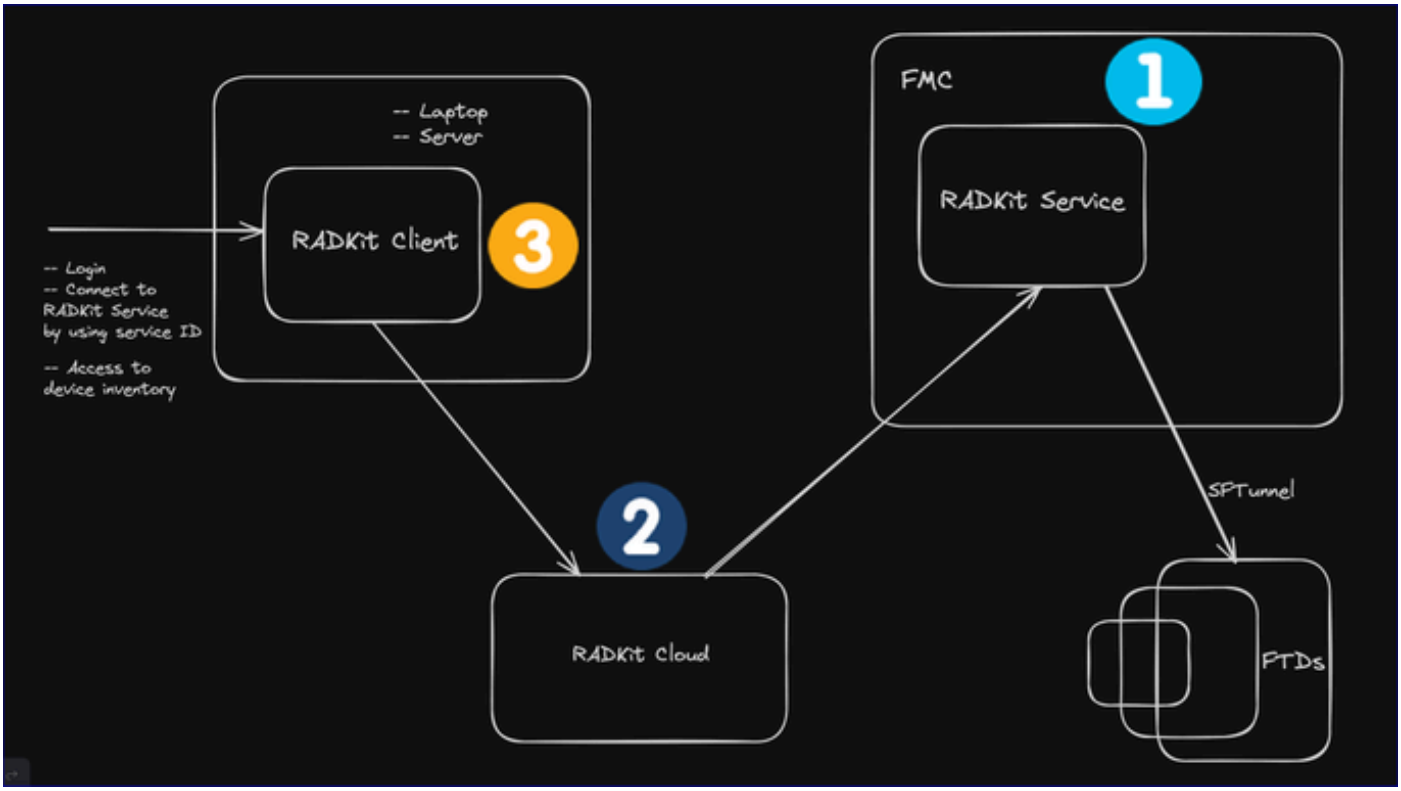
진단 개요

문제 해결 지점

1. 브라우저 개발 도구 및 FMC 로그를 사용하여 FMC에서 발생하는 상황을 확인합니다.

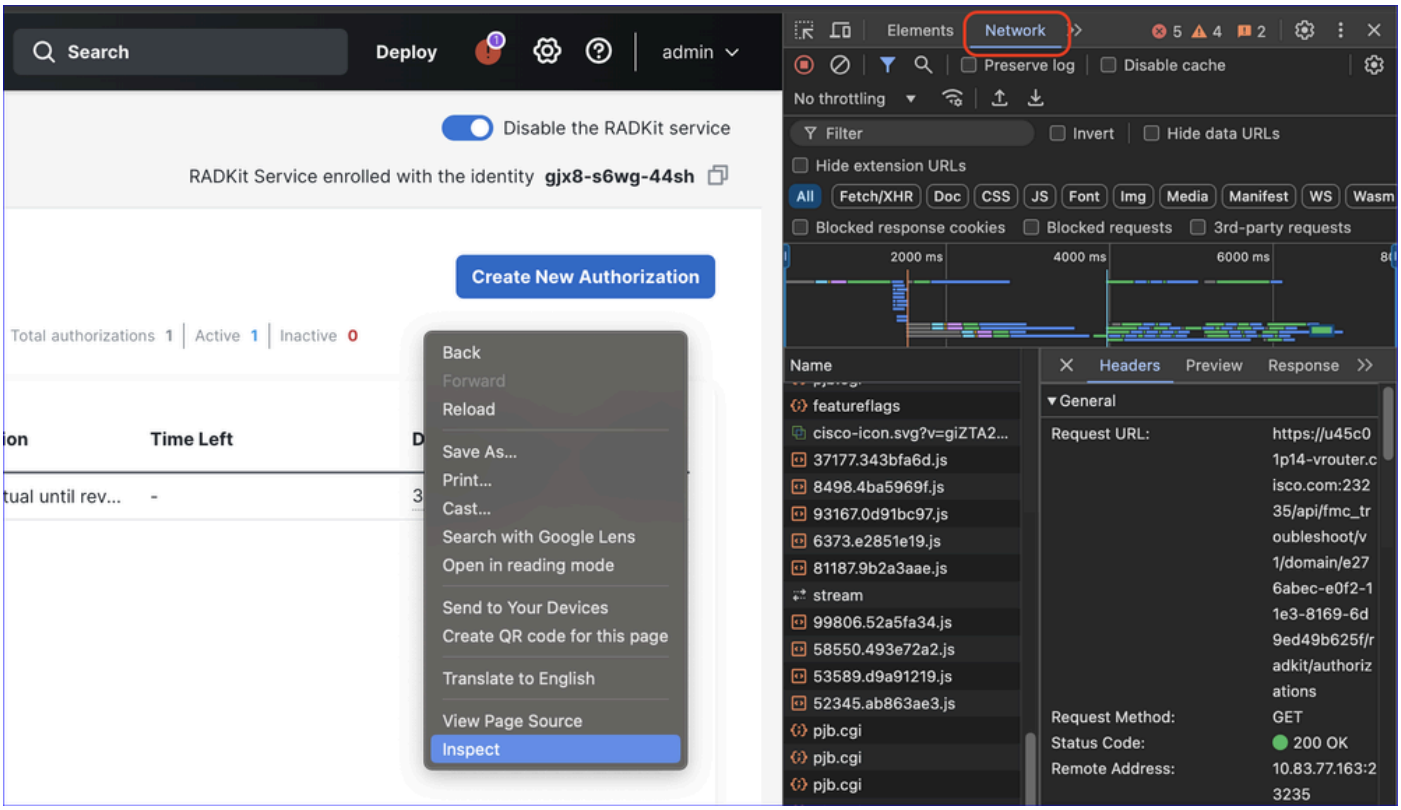
2. FMC의 RADKit Service, RADkit Cloud, RADKit 클라이언트 간 통신 문제는 RADKit 클라이언트 로깅을 참조하십시오.

3. RADKit 클라이언트



문제 해결 방법: 브라우저의 개발자 도구

- 브라우저의 Developer Tools, Network 탭에는 페이지에서 실행된 API 호출이 표시되며, 이는 FMC에서 문제를 해결할 때 사용할 수 있습니다. 페이지를 마우스 오른쪽 버튼으로 클릭한 다음 Inspect(검사)를 클릭하여 이 작업을 시작할 수 있습니다.
- Network(네트워크) 탭에서 API 호출 상태 코드 및 응답 미리 보기를 확인합니다.



RADKit Service Go 미들웨어 API

RADKit 통합용 Go 미들웨어는 FMC API 탐색기를 통해 공개적으로 사용할 수 없는 API 호출을 사용합니다. Go Middleware API 로그는 /var/log/auth-daemon.log에서 사용할 수 있습니다. Go Middleware가 수행하는 기능은 다음과 같습니다.

- Single Sign On 프로세스를 사용하여 RADKit 클라우드에 RADKit 서비스를 등록합니다.
- 모든 원격 RADKit 사용자의 권한 부여 및 연결된 장치 목록을 가져옵니다.
- 이메일을 사용하여 특정 원격 RADKit 사용자 권한 부여 및 관련 장치를 가져옵니다.
- 원격 RADKit 사용자 권한 부여를 생성하고 지정된 기간 동안 디바이스(모든 디바이스 또는 선택한 디바이스 목록)에 액세스할 수 있는 권한을 부여합니다.
- 원격 RADKit 사용자 권한 부여를 수정합니다.
- 원격 RADKit 사용자 권한 부여 삭제

RADKit 서비스 트러블슈팅을 위한 로그

- 일반 FMC 로그: pigtail 명령을 사용합니다.
- Go 미들웨어 API: /var/log/auth-daemon.log
- RADKit 및 auth-daemon이 데이터를 처리하는 로그:

/var/log/process_stdout.log

/var/log/process_stderr.log

이 모든 로그는 FMC/FTD 트러블슈트에 포함됩니다.

- 내부 RADKit 서비스 로그: /var/lib/radkit/logs/service/
- 디바이스(FMC 및 FTD)에서 RADKit 클라이언트에서 수행된 작업에 대한 로그:

/var/lib/radkit/session_logs/service

Cisco TAC에 제출할 로그

- 오류 스크린샷.
- 문제에 대한 설명입니다.
- 재현할 단계.
- Pigtail 및 /var/log/auth-daemon.log 로그 추출에서 오류가 발생했습니다.

액세스 모니터링

액세스 권한을 부여받은 사용자의 FMC 감사 로그 기록

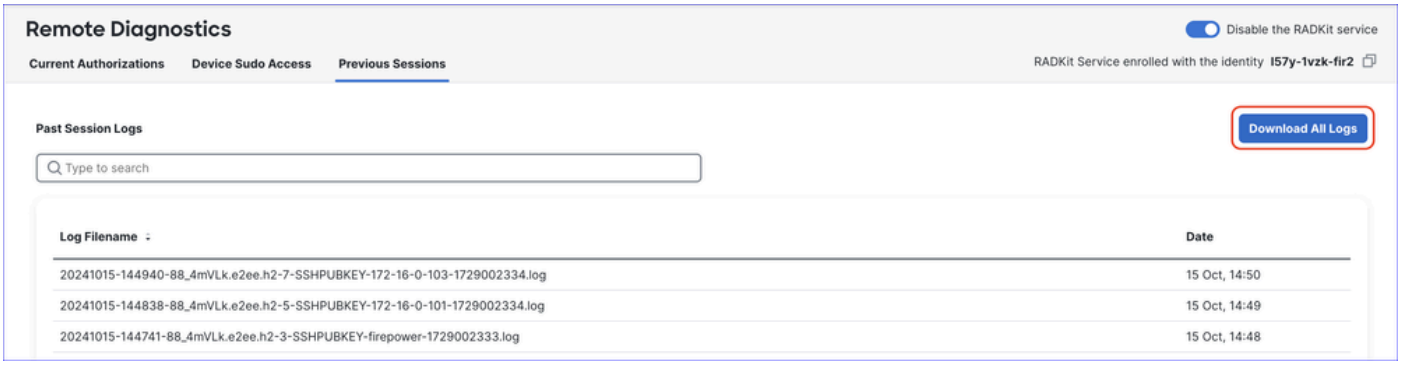
RADKit 세션 로그

디바이스(FMC 및 FTD)의 RADKit 클라이언트에서 수행된 작업에 대한 RADKit 세션 로그는 FMC의 /var/lib/radkit/session_logs/service에 있습니다.

- 로그는 RADKit 서비스 자체에서 가져온 것입니다.
- 이러한 로그는 트러블슈팅 번들에 포함됩니다.
- UI에서도 로그에 액세스할 수 있습니다(다음 섹션 참조).
- 여러 세션 로그 파일이 있습니다. 한 세션당 하나씩.

RADKit 이전 세션 로그

RADKit 클라이언트에서 수행된 디바이스 작업에 대한 RADKit 세션 로그는 "Download All Logs(모든 로그 다운로드)" 버튼을 클릭하여 Previous Sessions(이전 세션) 탭의 모든 로그가 포함된 아카이브로 다운로드할 수 있습니다.



트러블슈팅의 샘플 문제 연습

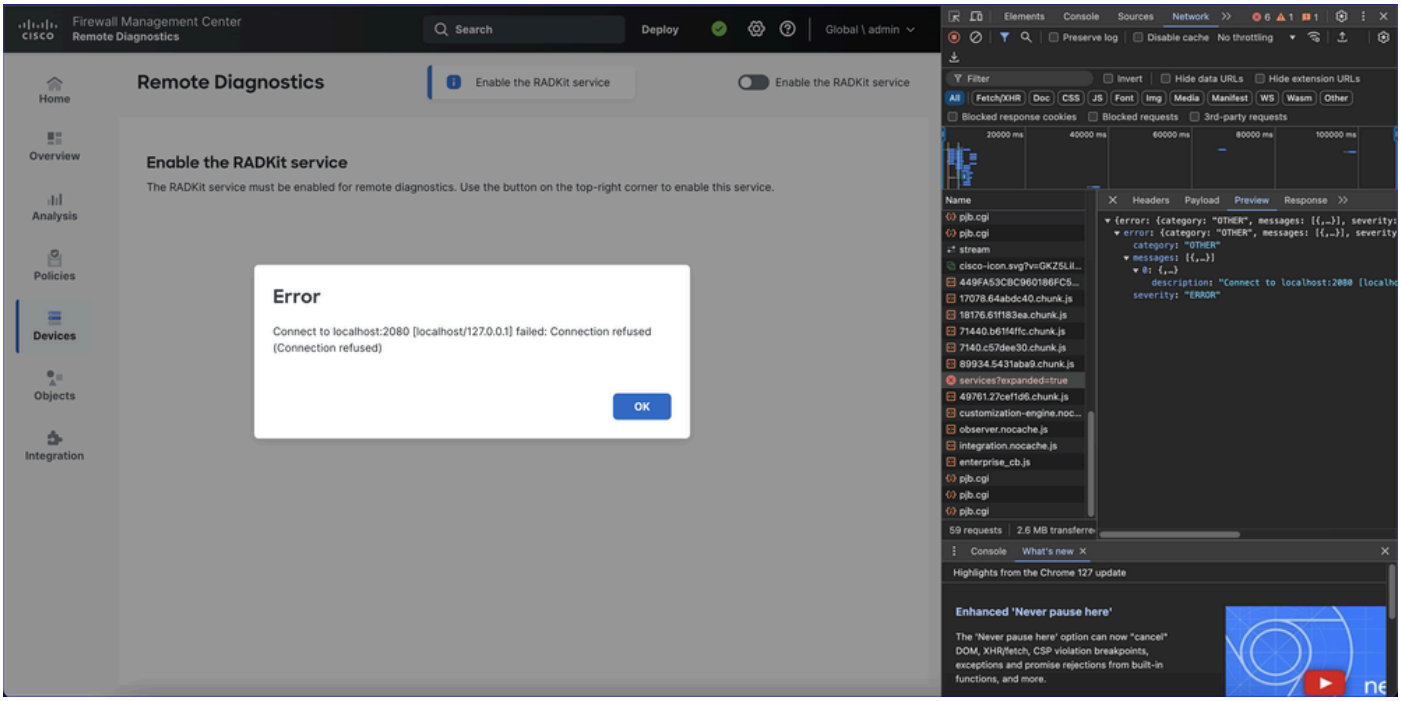
문제 해결 예

"Connect to localhost:2080 [localhost/127.0.0.1](localhost/127.0.0.1에 연결)과 같은 오류가 발생한 경우: Connection refused (Connection refused)", FMC SSH 세션에서 auth-daemon을 다시 시작해 보십시오.

<#root>

root@firepower:~$

sudo pmtool restartbyid auth-daemon



텔레메트리

이 기능에 대한 텔레메트리 출력이 추가되었습니다.

```
"remoteDiagnostics" : {
   "isRemoteDiagnosticsEnabled": 0 // 0 = false , 1 = true
}
```

FAQ

FAQ: 로그인 및 등록

Q. FMC에 직접 인터넷 액세스가 없는 경우 등록이 프록시와 연동됩니까?

A. 예. 프록시에서 등록 프로세스에 사용되는 prod.radkit-cloud.cisco.com에 액세스할 수 있는 경우.

Q. 사용자가 이 서비스에 대해 자신의 IdP를 사용할 수 있습니까?

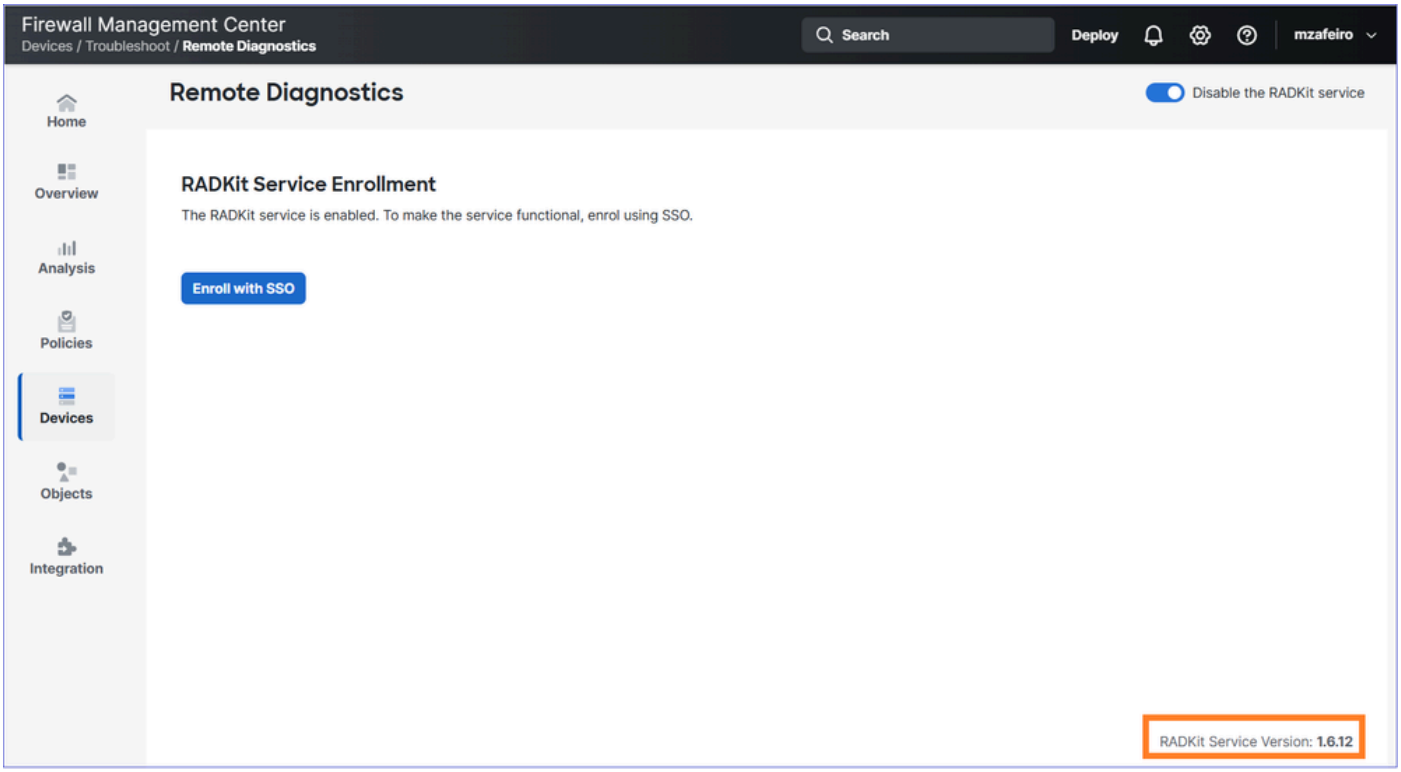
A. RADKit 클라우드에서는 Cisco SSO만 허용됩니다. Cisco 이외의 이메일을 통해 RADKit 서비스 등록이 가능하도록, 귀사 계정을 Cisco 계정과 연동하는 옵션이 있습니다.

FAQ: RADKit 버전

Q. 7.7 릴리스의 FMC에는 어떤 버전의 RADkit가 포함됩니까? FMC에 어떤 버전의 RADKit가 포함되어 있는지 어떻게 알 수 있습니까? FMC 업그레이드 없이 업데이트할 수 있는 내용입니까?

A.

- 7.7.0이 포함된 RADKit의 버전은 1.6.12입니다.
- RADKit 서비스의 버전은 FMC Remote Diagnostics 페이지 하단에 표시됩니다. "RADKit 서비스 버전: 1.6.12"



- RADKit는 FMC 업그레이드 패키지/핫픽스와 함께 번들로 제공됩니다. FMC에서 RADKit 서비스를 별도로 업그레이드하는 것은 지원되지 않습니다.

FAQ: 기타

Q. FMC에서 관리하지 않는 외부 장치를 포함할 수 있습니까?

A. FMC에서 관리하는 디바이스만 RADKit 인벤토리에 추가한 다음 권한 부여를 통해 액세스할 수

있습니다.

Q. RADKit 구성은 FMC 백업의 일부로 백업됩니까?

A.

- 컨피그레이션은 FMC 백업의 일부로 백업되지 않습니다.
- 일반적으로 영구 액세스가 제공되지 않을 것으로 예상하기 때문에 백업되지 않습니다. 액세스는 일반적으로 제한된 시간 동안만 가능합니다.

참조

유용한 링크:

- FMC 컨피그레이션 가이드 - RADKit
- https://radkit.cisco.com/
- https://radkit.cisco.com/docs/index.html
- https://radkit.cisco.com/downloads/release/
- https://github.com/Cisco-RADKit/Intro

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.