

Cisco RDKit-integratie in FMC configureren

Inhoud

[Inleiding](#)

[Achtergrond](#)

[Beschrijving en doorloop van functies](#)

[FMC REST API's](#)

[Ontvang aanvullende informatie van de apparaten](#)

[Cisco-ondersteuning: RADKit-console](#)

[Compatibiliteit met upgrades en achteruit](#)

[Probleemoplossing](#)

[Overzicht van diagnoses](#)

[RDKit-sessielogboeken](#)

[Probleem met probleemoplossing bij doorlopen van voorbeelden](#)

[telemetry](#)

[FAQ](#)

Inleiding

Dit document beschrijft de functie Cisco RADKit Integration in FMC die in release 7.7 is toegevoegd.

Achtergrond

Problemen met firewallbeheerders

- De Remote Automation Development Kit (RADKit), ontwikkeld door Cisco, is een netwerkbrede orchestrator die is ontworpen om gebruikers de mogelijkheid te bieden op een veilige manier toegang te krijgen tot netwerkapparaten en problemen op te lossen.
<https://radkit.cisco.com/>
- Cisco Secure Firewall Management Center (FMC) beheert en gebruikt FTD-apparaten (Secure Firewall Threat Defence). Een enkel VCC kan meerdere apparaten op verschillende locaties beheren.
- De gebruikers kunnen RADKit afzonderlijk en aan boord van hun VCC en FTDs installeren, maar de RADKit-dienst bouwen in het VCC en op geautomatiseerde wijze aan boord gaan van het VCC(s) en alle beheerde apparaten (FTD's) zou voor de eindgebruikers een betere ervaring zijn.

Use case

Enkele van de belangrijkste mogelijkheden waarvan de gebruikers zouden kunnen profiteren na integratie van RADKit in het VCC zijn:

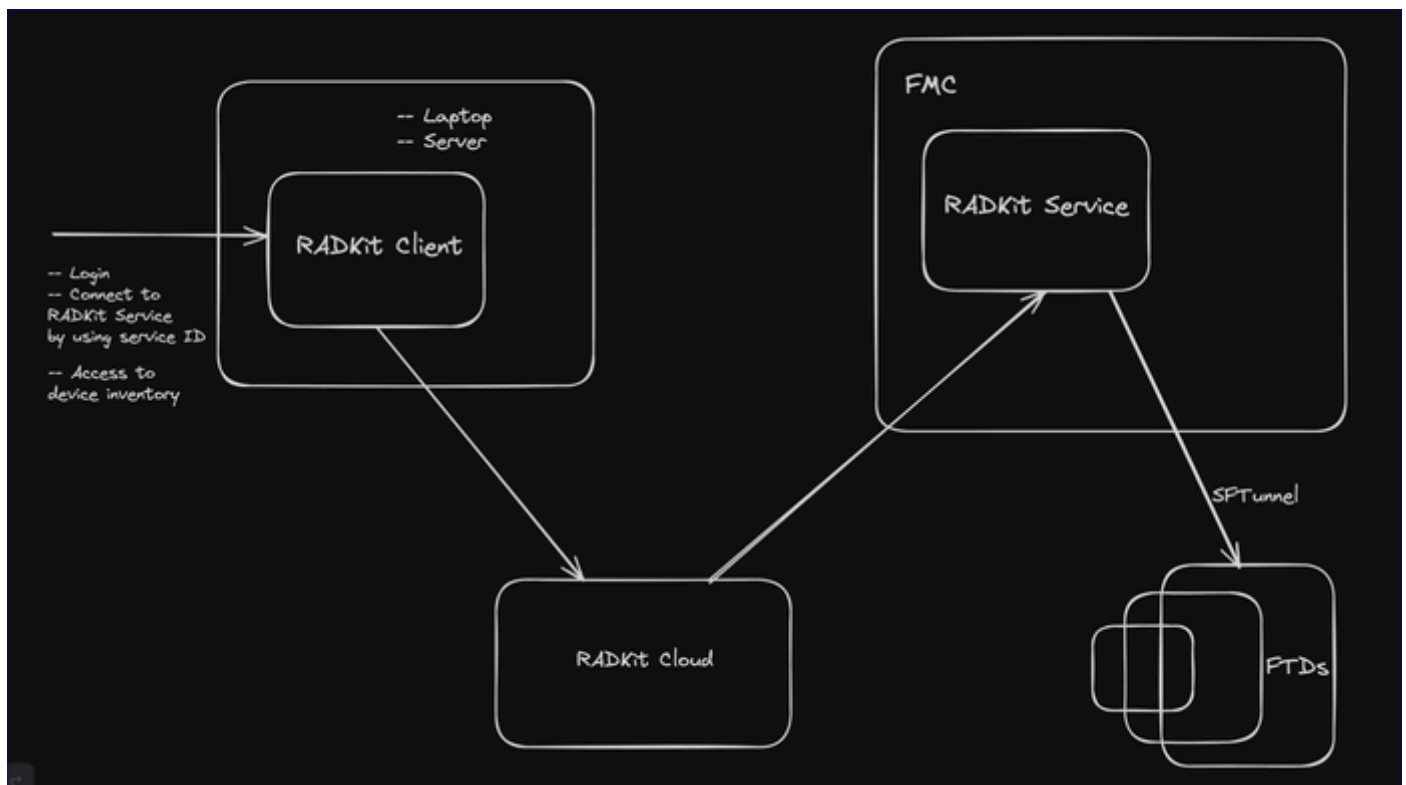
- Mogelijkheid om de FMC's/FTD's op afstand te benaderen vanuit de RADKit-client CLI.
- Vermogen om beheerste toegang tot de FMC's/FTD's te verlenen aan iedereen die dit nodig heeft (bijvoorbeeld een Cisco TAC-engineer).
- Gebruik automatiseringsmogelijkheden voor het verzamelen van gegevens en het diagnosticeren van problemen van de RADKit-client (scripts die opdrachten uitvoeren op meerdere apparaten kunnen worden gemaakt en gebruikt vanaf de RADKit-client).

Nieuw - Oplossing

- Vanaf Secure Firewall 7.7.0 is de Remote Automation Development Kit (RADKit)-service geïntegreerd in FMC.
- Gebruikers kunnen de RADKit-service op aanvraag in- of uitschakelen, inschrijven in de RADKit-cloud en externe gebruikersautorisaties maken om toegang te krijgen tot specifieke apparaten van de RADKit-client voor een geplande toegangsduur.
 - Autorisaties kunnen worden bewerkt of ingetrokken.
- Er is ook een optie om apparaten sudo toegang te bieden voor geavanceerde probleemoplossing.

RADKit-serviceintegratie in FMC-diagram

In dit diagram wordt getoond hoe RADKit communicatie van RADKit-client (TAC engineer) van gebruikers naar FTD-apparaten voor productieomgevingen mogelijk maakt:



Grondbeginselen: Ondersteunde platforms, licentiëring

Toepassingen en beheerders

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 <i>(lowest version FMC on 7.7.0 can manage is 7.2)</i>	7.7.0 only	ASDM 7.23.1	No
Snort Support <i>(Snort 3 is the only Snort version supported in 7.7)</i>	Snort 3 Snort 2 <i>(only for devices on 7.2.x - 7.6.x)</i>	CSM 4.30	No
FDM on 7.7.0	No		

Andere aspecten van de ondersteuning

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

Afhankelijkheden van te gebruiken functie

- De minimale versie is Secure Firewall 7.7.0.
- Om verbinding te kunnen maken met de RADKit-service die binnen FMC wordt gehost, moet de RADKit-client via <https://radkit.cisco.com/downloads/release/> worden geïnstalleerd op de computer van de support engineer.
- De voorkeursversie voor de RADKit-client is 1.6.10 of hoger.
- Oudere versies van RADKit Client kunnen worden gebruikt omdat de RADKit Service achterwaarts compatibel is met oudere RADKit Client versies.

Beschrijving en doorloop van functies

Overzicht van functies

- Dankzij de integratie van de RADKit-service in het FMC kunnen de apparaatbeheerders externe gebruikers (Cisco TAC-engineers) toegang verlenen tot specifieke FMC- en FTD-apparaten in hun netwerk voor problemen oplossen en automatiseringsdoeleinden. RADKit is veel efficiënter voor probleemoplossing dan scherm delen, het hoeft niet om de computer van de gebruiker te controleren, is een veiligere manier om aan een netwerk te werken en vult Webex mooi aan.
- Dit maakt een betere ervaring voor technische ondersteuning, aangezien apparaatbeheerders de RADKit-service niet afzonderlijk moeten installeren en configureren. Ook vermindert dit de ondersteuningstijd voor Cisco TAC-engineers bij het oplossen van ondersteuningsproblemen.

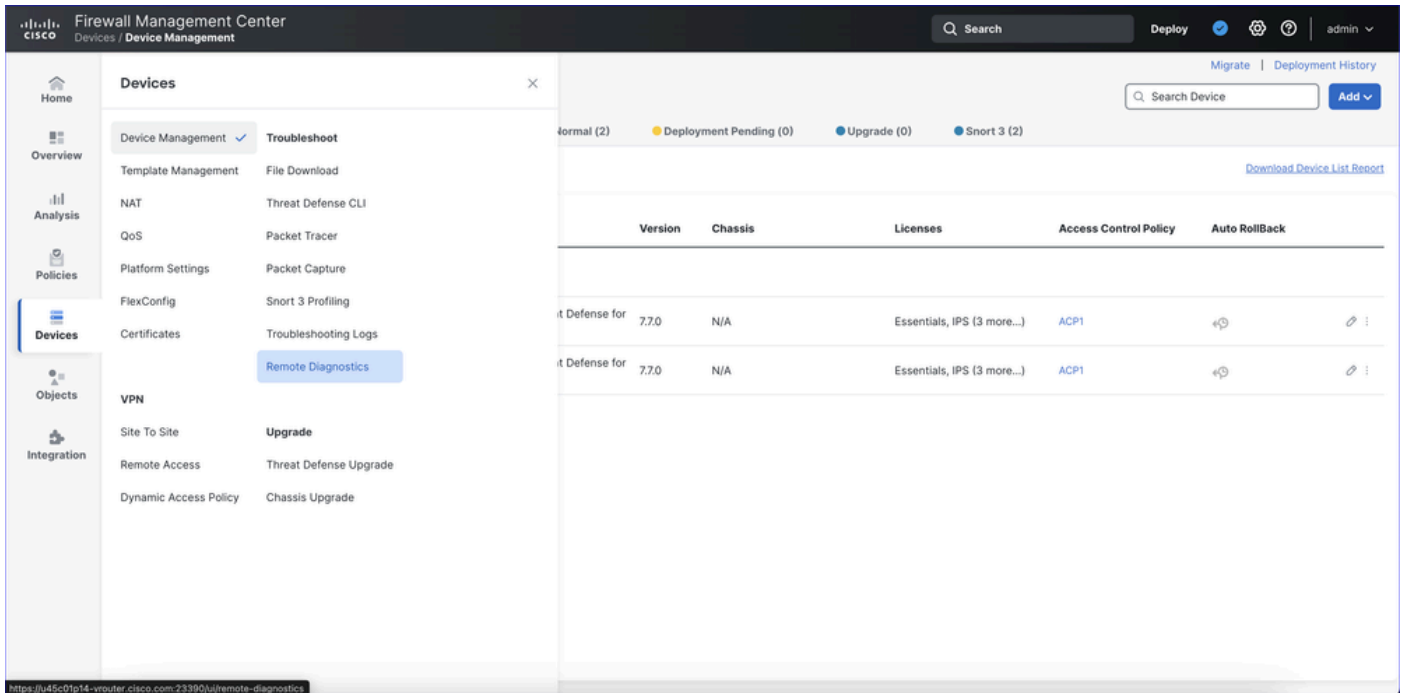
Configuratiestappen: Overzicht

1. Apparaatbeheerder (FMC-beheerder): Schakel de RADKit-service in en schrijf deze in en configureer autorisaties op FMC GUI.
2. Cisco TAC/Cisco-ondersteuning: Installeer de RADKit-client op hun computer, maak toegang tot de apparaten en los problemen op vanuit RADKit-client.

FMC-beheerder: Walkthrough voor Firewall Management Center

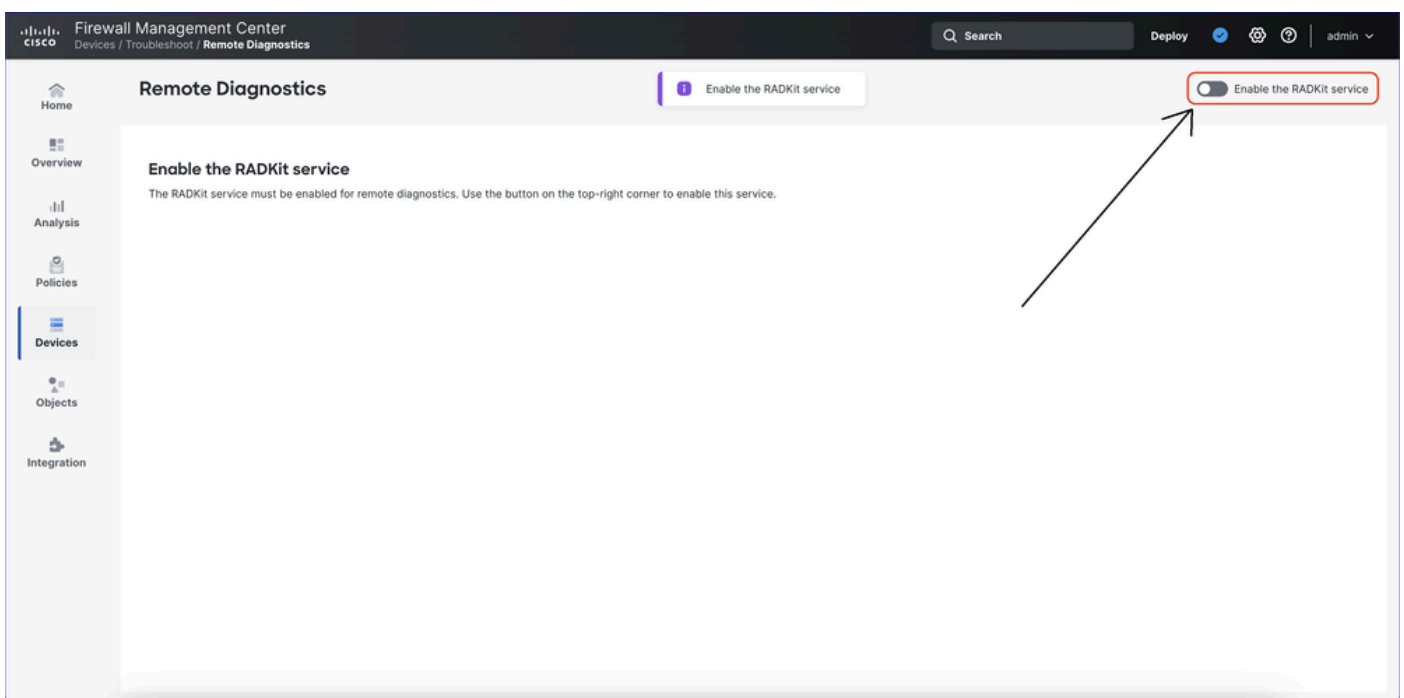
Remote Diagnostics-menu

- Voor deze functie is onder "Apparaten -> Probleemoplossing een nieuw menu-item "Remote Diagnostics" toegevoegd.
- Beheerder, Netwerkbeheerder en Onderhoudsgebruikers hebben lees- en schrijftoegang op de pagina.
- Security Analyst, Security Analyst (alleen lezen) en Security Approver-gebruikers hebben alleen toegangsrechten tot de pagina gelezen.



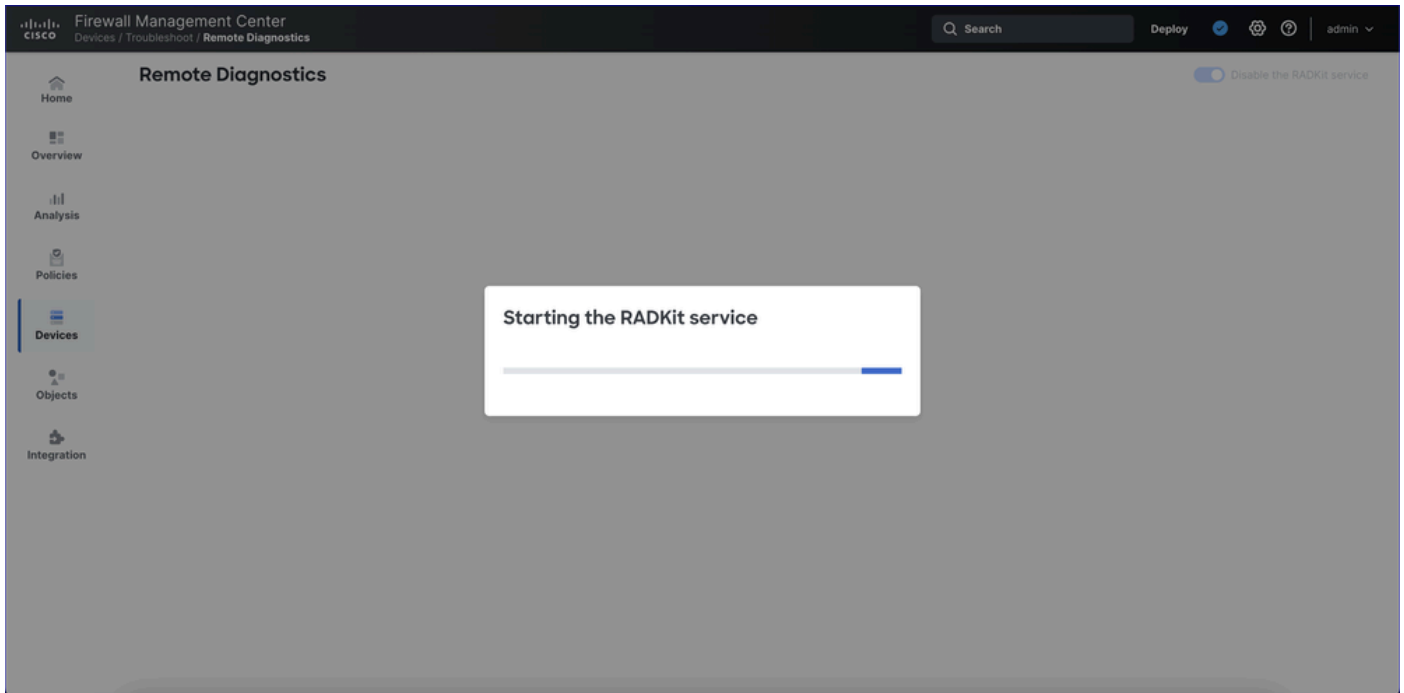
Eerste pagina voor externe diagnose

Dit is de eerste pagina voor Remote Diagnostics. De RADKit-service kan worden ingeschakeld door de switch "De RADKit-service inschakelen" om te schakelen:



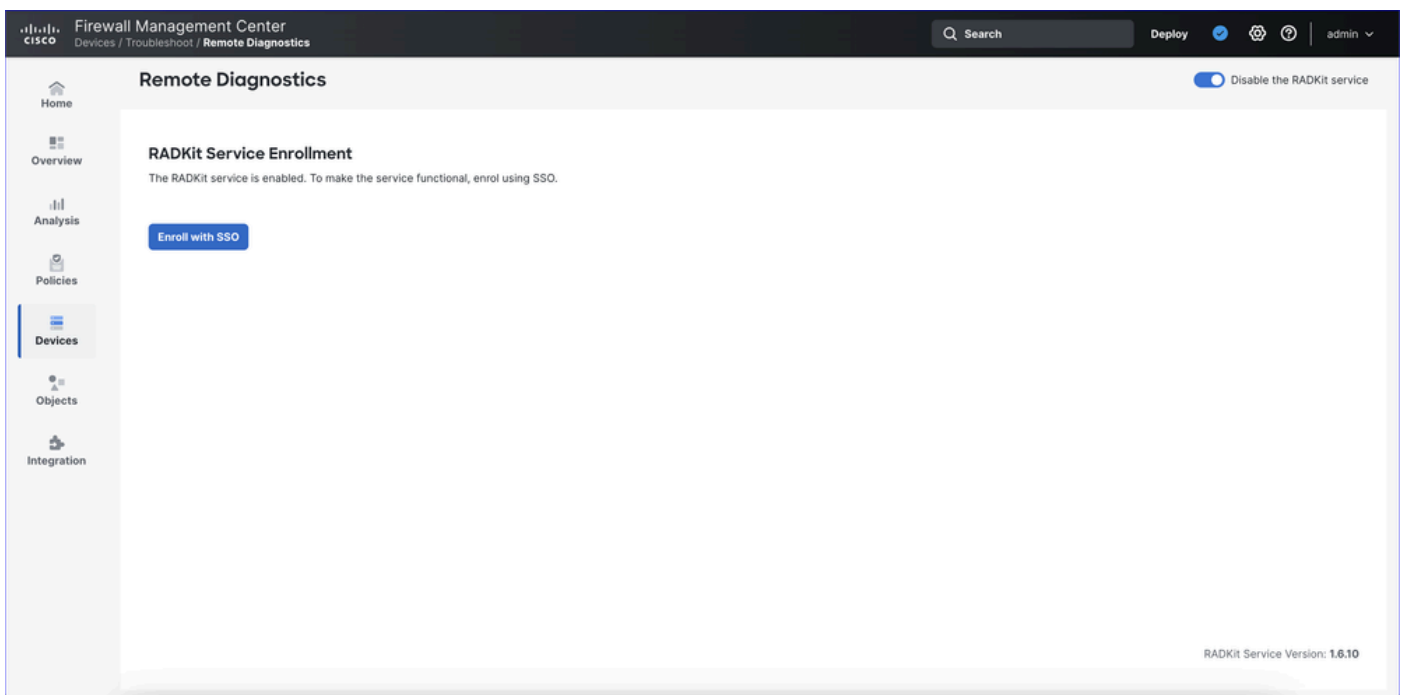
Start RADKit-service

Nadat u de RADKit-service hebt ingeschakeld, verschijnt er een voortgangsbalk totdat de RADKit-service is gestart:



RADKit-service ingeschakeld

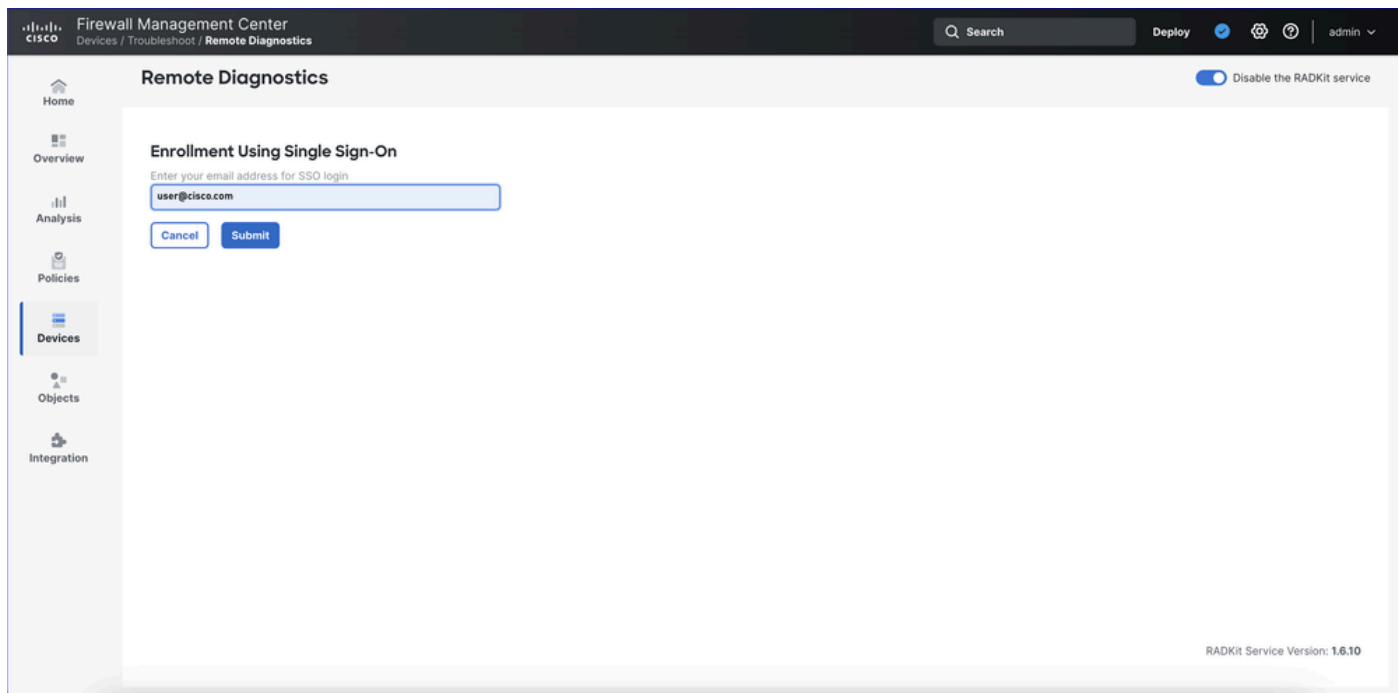
- Wanneer het inschakelproces voor de RADKit-service is voltooid, wordt deze pagina weergegeven:



De volgende stap is inschrijving in de RADKit cloud door te klikken op "Enroll with SSO" knop.

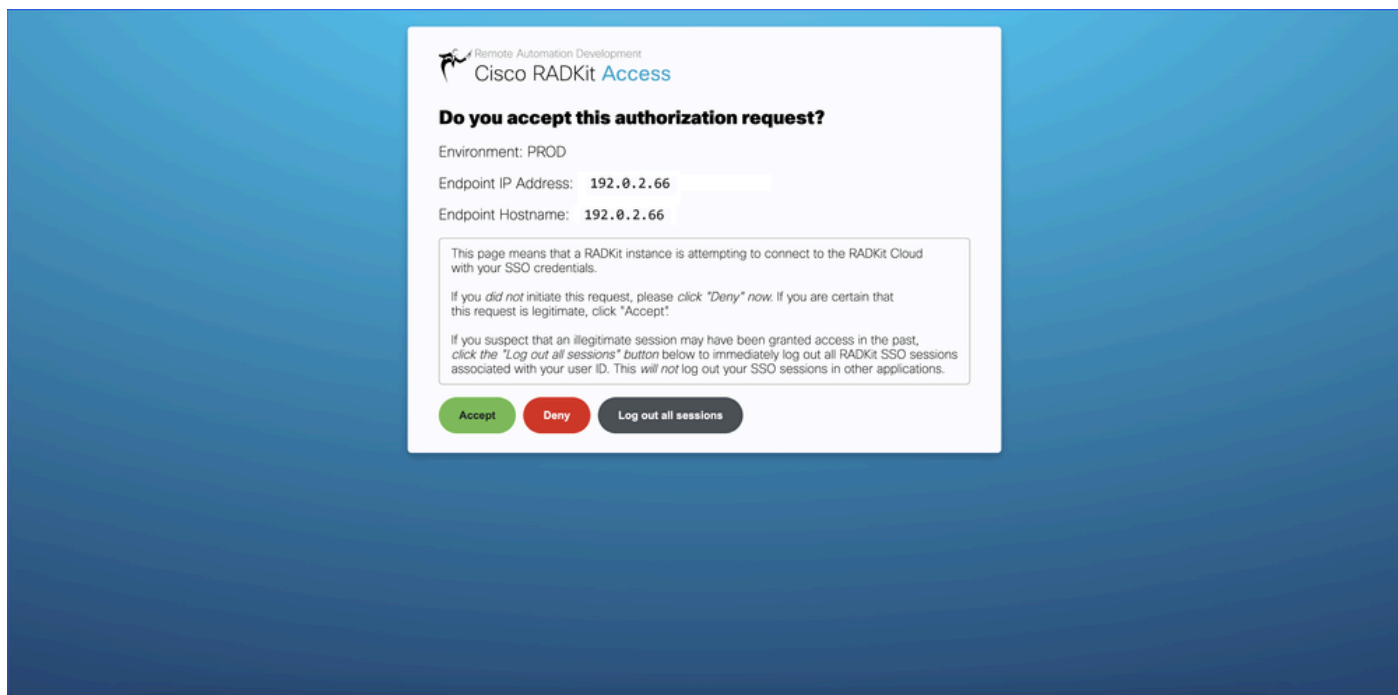
Inschrijven met SSO - E-mailadres invoeren

Stap 1 van het inschrijvingsproces bestaat uit het invoeren van het e-mailadres van de gebruiker voor de RADKit cloudinschrijving:



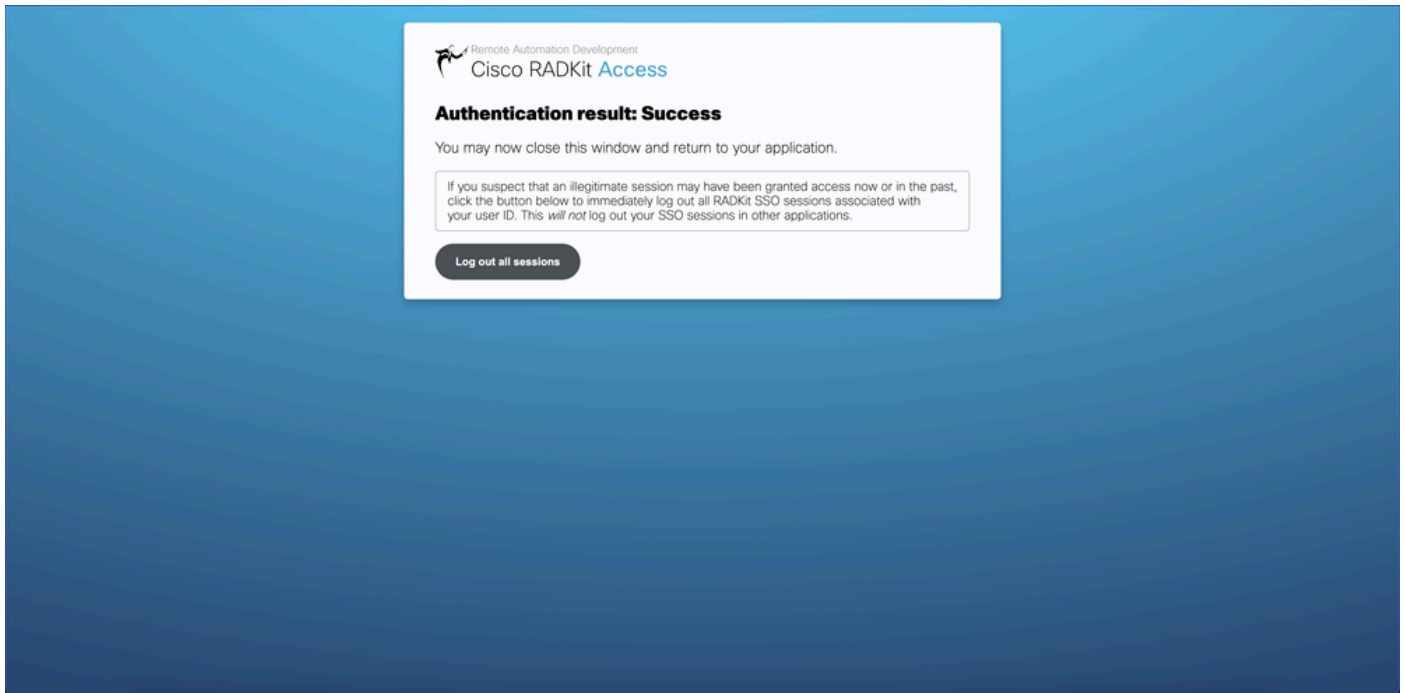
Aanmelden bij SSO - autorisatieaanvraag accepteren

Er wordt een nieuw browsertabblad (of venster, afhankelijk van de browserinstellingen) geopend. Klik op de knop Akkoord.



Inschrijven met SSO - Verificatie geslaagd

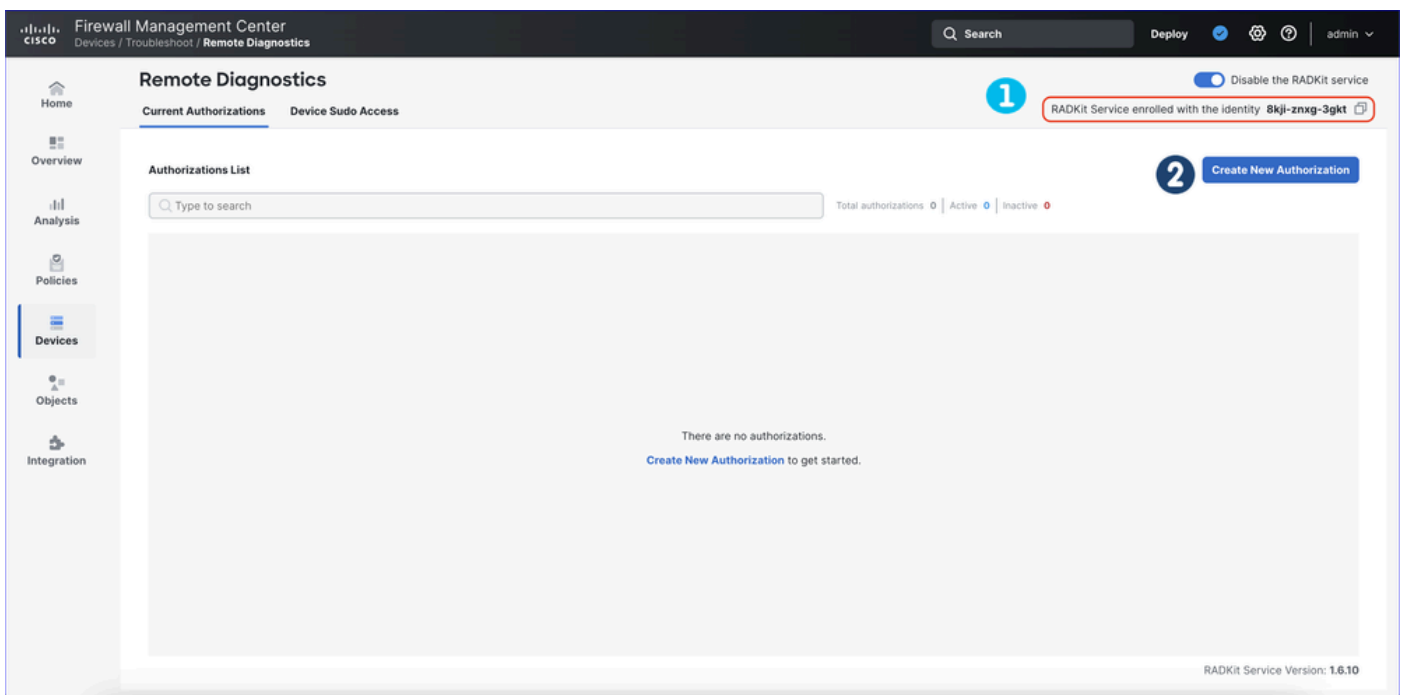
Na een succesvolle verificatie kan de gebruiker het tabblad van de browser sluiten en terugkeren naar de pagina van FMC Remote Diagnostics.



RADKit-service ingeschakeld

De RADKit-service is geregistreerd met de opgegeven service-ID (in dit voorbeeld is de ID 8kji-znxxg-3gkt). De ID kan naar het klembord worden gekopieerd. Geef het aan de Cisco TAC Engineer zodat ze verbinding kunnen maken met de RADKit service vanaf de RADKit client.

De volgende stap is het maken van een autorisatie door op de knop "Nieuwe autorisatie maken" te klikken:

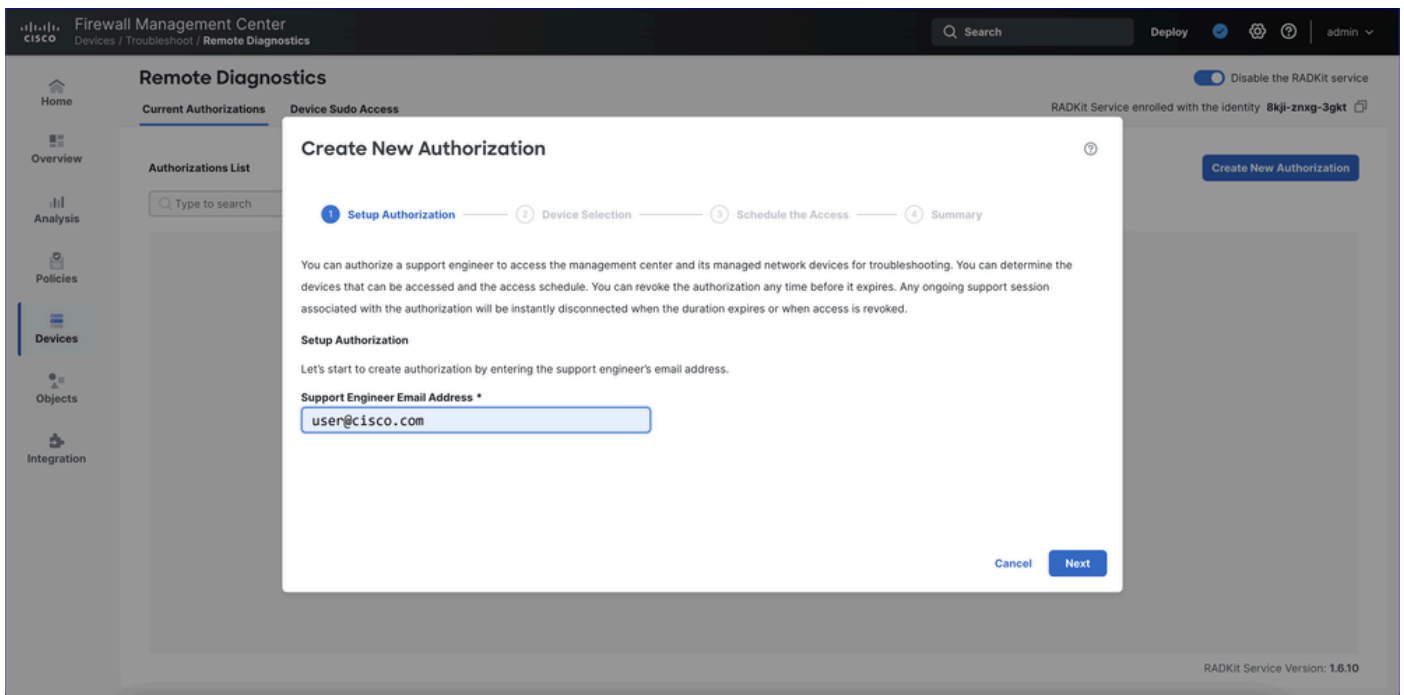


Nieuwe autorisatie maken: Stap 1

- Voor het creëren van een nieuwe autorisatie, de eerste stap is het toevoegen van de support

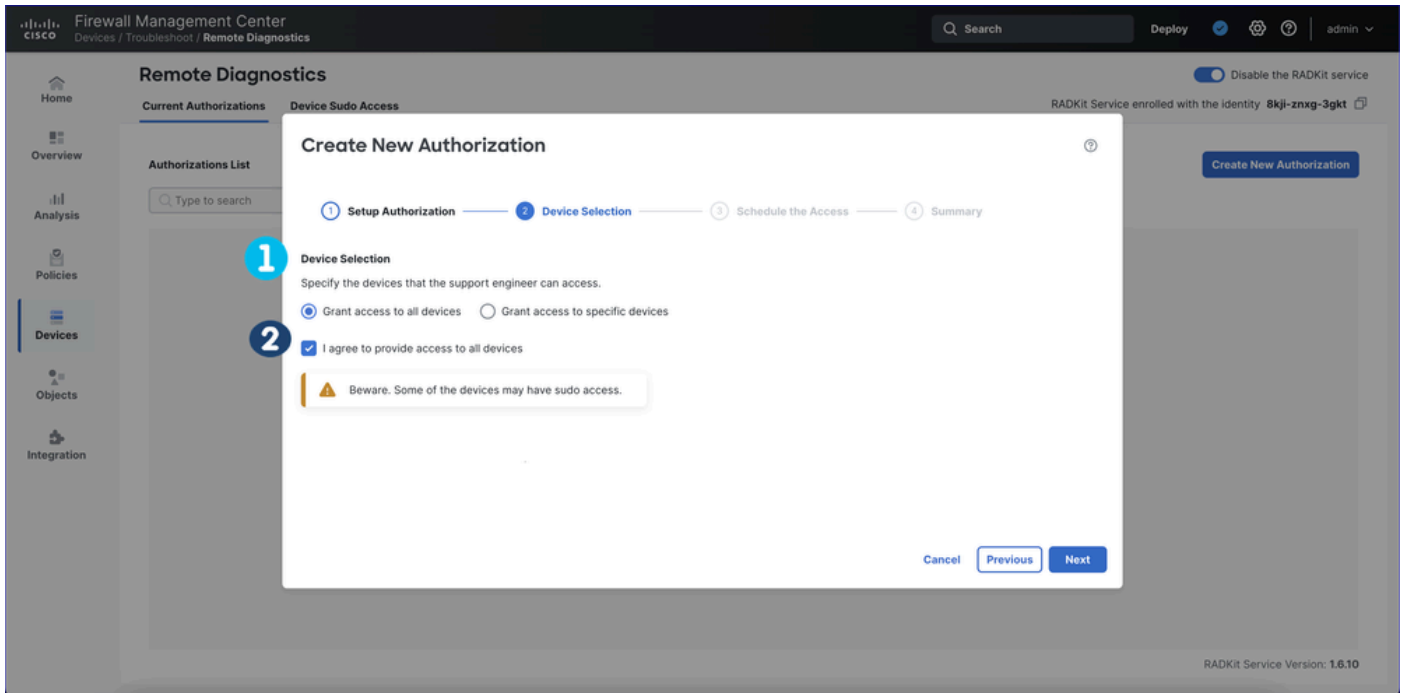
engineer e-mailadres.

- Er zijn vier stappen voor het creëren van een nieuwe autorisatie. De voortgang van de stappen wordt bovenaan weergegeven.



Nieuwe autorisatie maken: Stap 2

- Stap 1: Specificeer de apparaten waartoe de support engineer toegang heeft. Of, zoals in dit voorbeeld, toegang verlenen tot alle apparaten.
- Stap 2: Controleer de keuzerondje op alle of bepaalde apparaten. Voor specifieke apparatuur kunnen FMC's en/of FTD's worden geselecteerd. Let op de waarschuwing dat sudo toegang kan bieden aan sommige apparaten in het tabblad Device Sudo Access. De knop Volgende wordt pas ingeschakeld als het selectievakje ingeschakeld is.
- Sudo-toegang wordt later per apparaat verleend in het tabblad Device Sudo Access (niet tijdens het maken van een autorisatie).

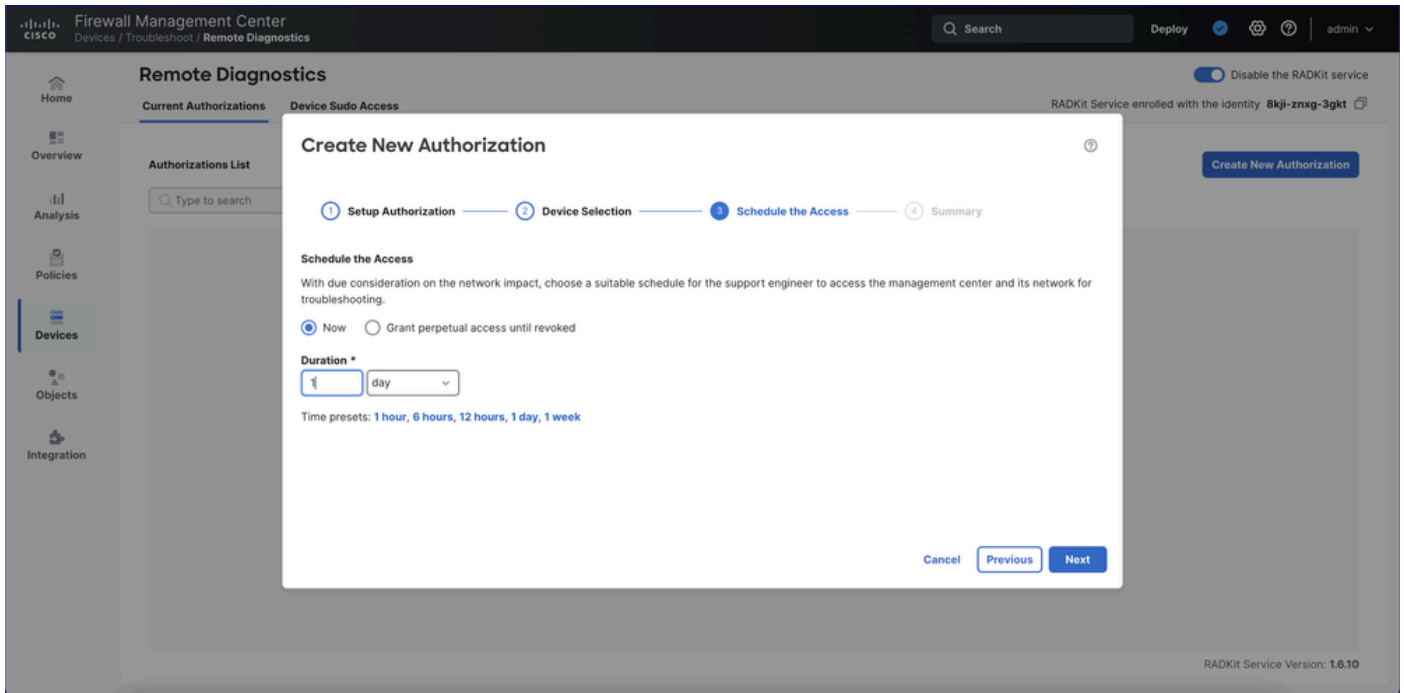


Opmerkingen over plukapparaten

- Slechts kunnen de apparaten op een gesteunde bouwstijl (bijvoorbeeld, in de aanvankelijke versie, slechts 7.7.0 apparaten) worden geoogst.
- Apparaten die uitgeschakeld en niet bereikbaar zijn, kunnen niet geselecteerd worden. RADKit vertrouwt op sftunnel (TCP 8305) om toegang te krijgen tot de apparaten.
 - Als er een probleem is met de sftunnelconnectiviteit, werkt het niet, maar het wordt nog steeds getoond in de RADKit-inventaris.
 - Als een apparaat wordt uitgeschakeld, wordt dit helemaal niet gezien.
- Als er VCC's in een HA-paar zijn, kan alleen het Active/Primary worden toegevoegd.
- De apparaten worden toegevoegd aan de RADKit inventaris bij het maken/bewerken van een autorisatie. Wanneer hulpmiddelen uit het VCC worden verwijderd, worden zij uit de "inventaris" van de hulpmiddelen verwijderd.

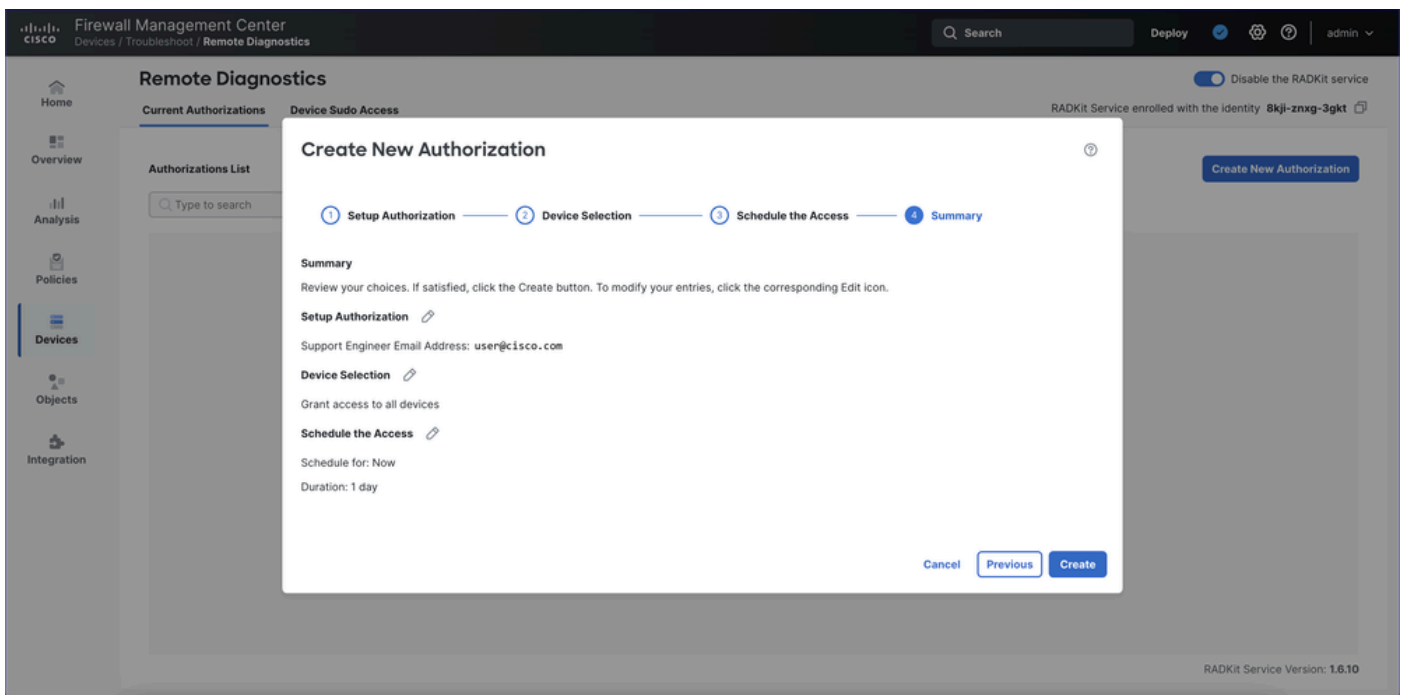
Nieuwe autorisatie maken: Stap 3

- Stap 3: Specificeer de duur voor de toegang van de steuningengineer tot apparaten.
- Selecteer "Nu" en specificeer een duur, of
- Kies "Toegestane permanente toegang tot herroepen".
- De standaardduur is 1 dag. Elke duur kan worden ingesteld; er zijn ook enkele vooraf gedefinieerde tijdswaarden.



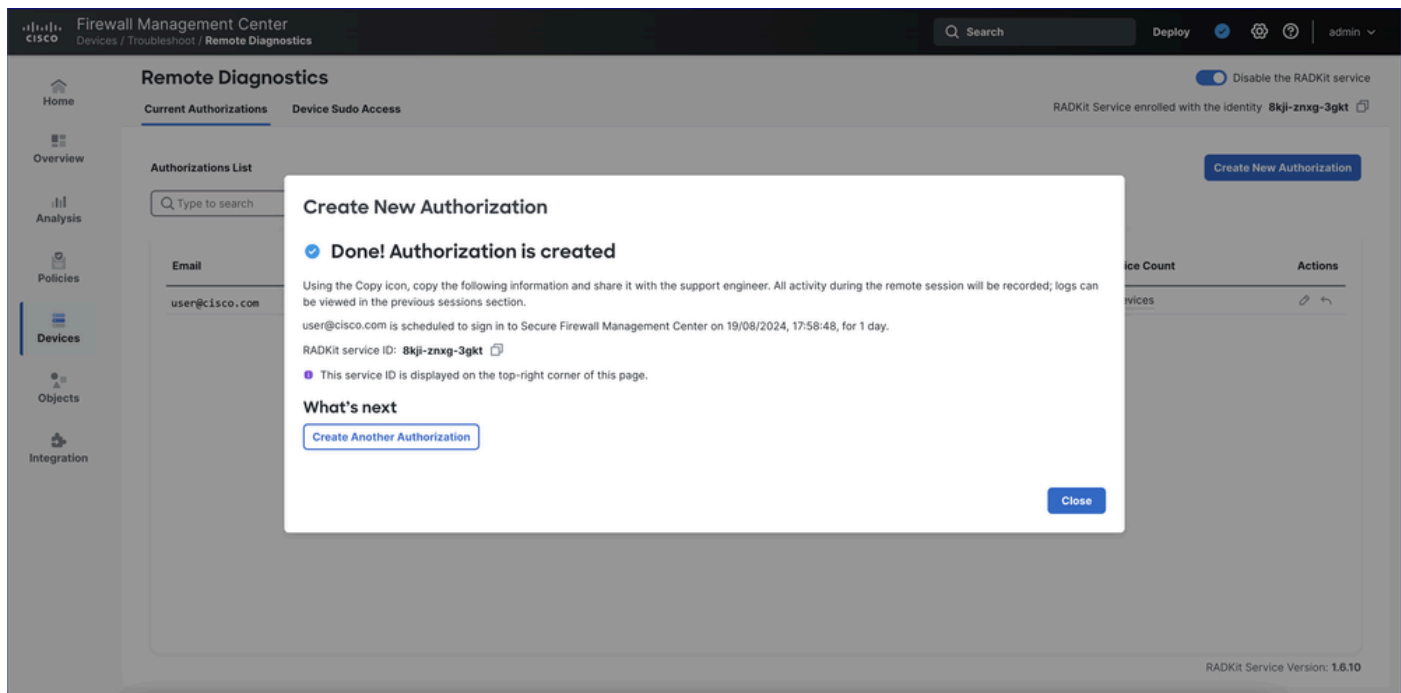
Nieuwe autorisatieoverzicht maken

De laatste stap is de samenvatting van de vergunning. Hier kan een gebruiker de configuratie bekijken en bewerken.



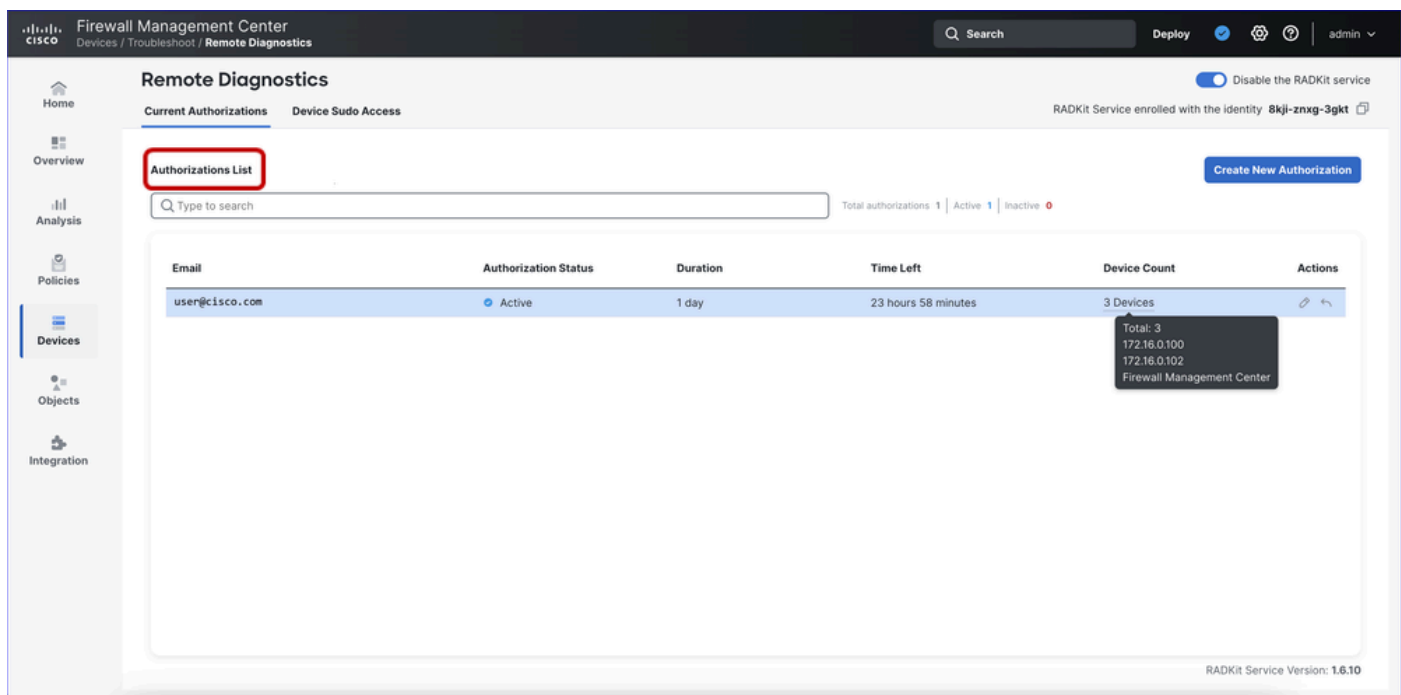
Nieuwe voltooide autorisatie maken

Er wordt een bevestigingsscherm weergegeven nadat de autorisatie is voltooid:



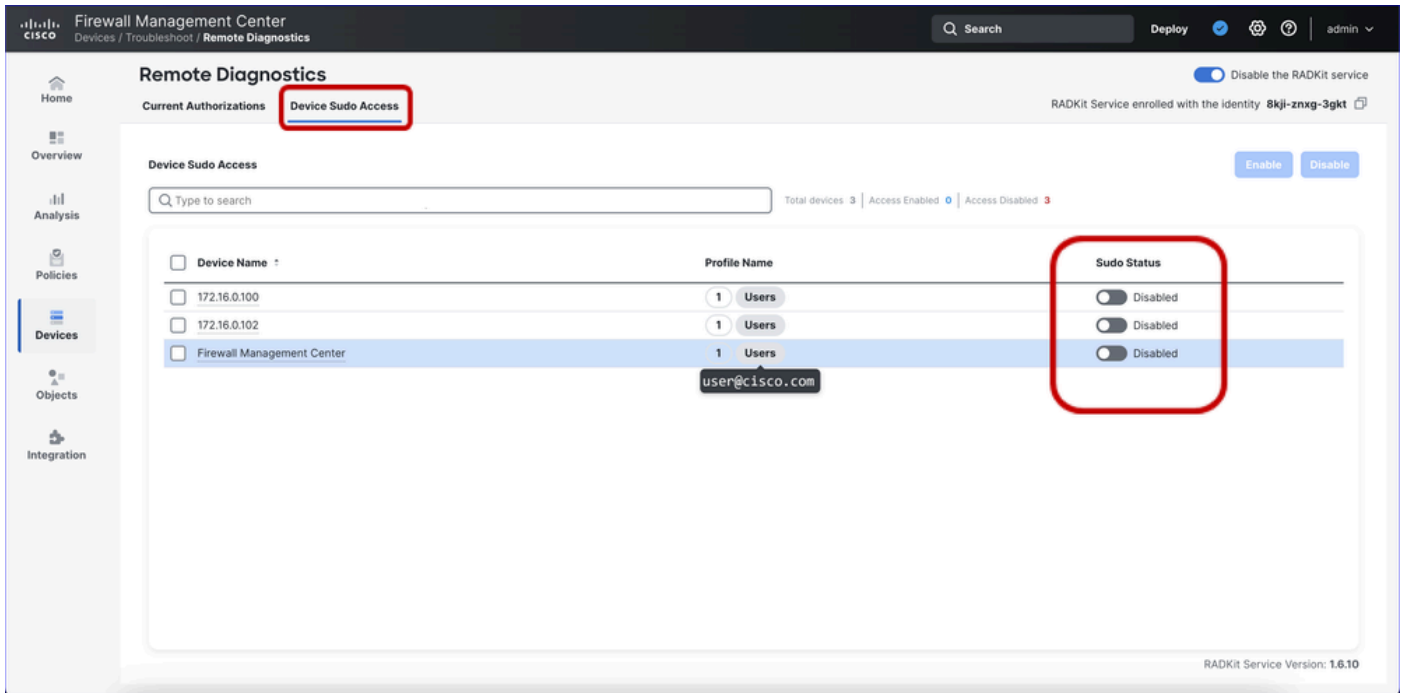
Huidige machtigingslijst, inclusief intrekking

- De huidige autorisatielijst wordt weergegeven in het tabblad Huidige autorisaties.
- De Acties (uiterst rechtse kolom) zijn Revoke access and Edit autorisatie.



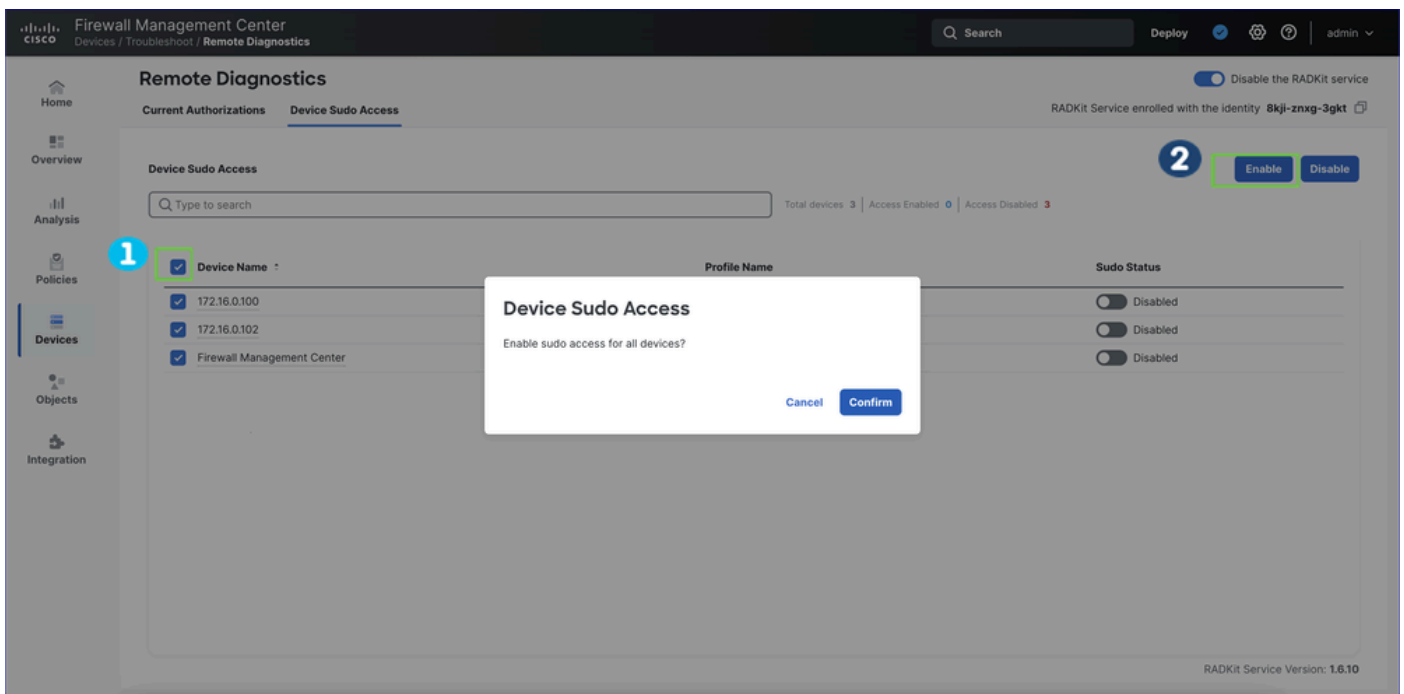
Toegangslijst apparaatbeheer

- De lijst met apparaten met sudo-toegangsinstellingen wordt weergegeven in het tabblad Apparaatsudo-toegang.
- Gebruik de schakelaar in de rechterkolom om sudotoegang in te schakelen. Standaard staat hij uit.
- Ook, bulk activeren/deactiveren sudo toegang is beschikbaar.



Bevestig de toegang tot het apparaat of de apparaten

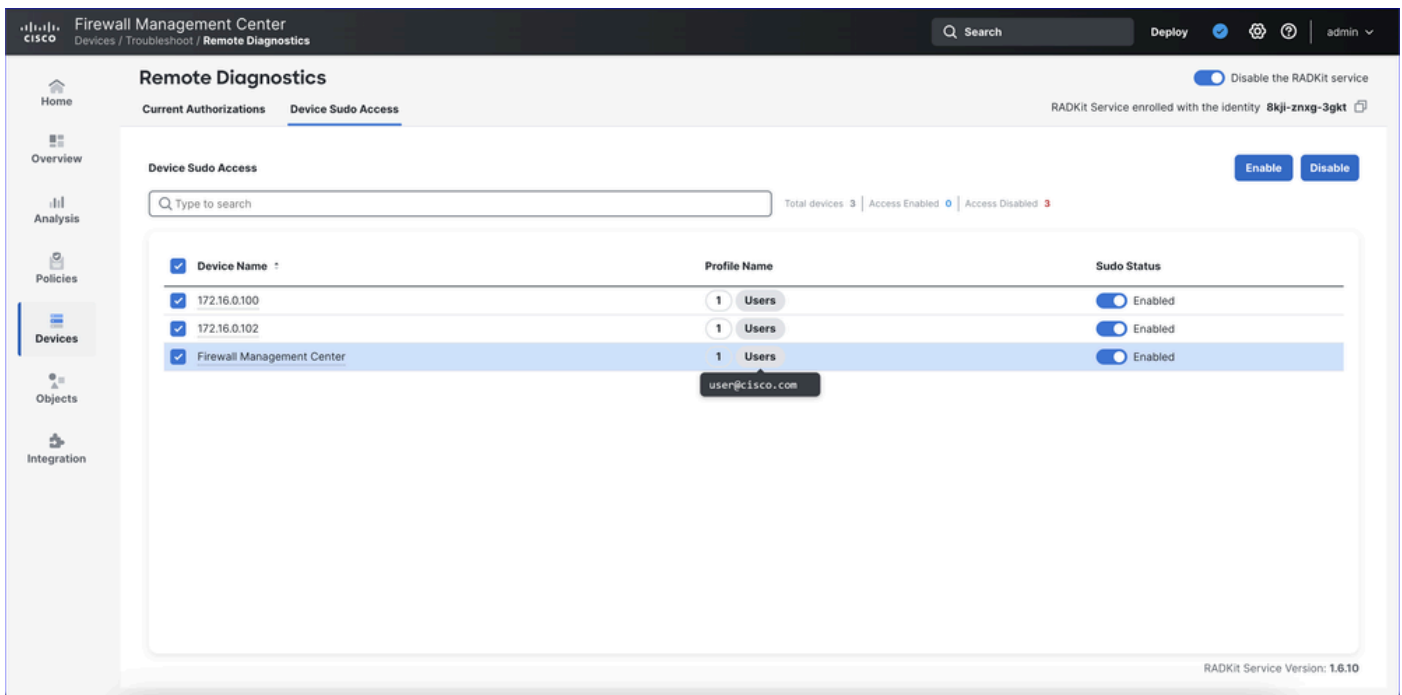
1. Sudo-toegang kan voor alle of alleen voor bepaalde apparaten worden ingeschakeld door de apparaten te selecteren en vervolgens op de knop Inschakelen te klikken.
2. Wanneer u het apparaat inschakelt, verschijnt er een bevestigingsvenster en klikt u op Bevestigen.



Toegang tot sudo voor apparaten ingeschakeld

- Na het in- of uitschakelen van sudo-toegang voor een apparaat, wordt de kolom Sudo Status rechts op de pagina bijgewerkt.

- De support engineer kan sudo su op het apparaat uitvoeren; dit is wachtwoordloos. De support engineer heeft geen hoofdwachtwoord nodig.



Overige opmerkingen

- Alleen apparaten in het domein waartoe de FMC-gebruiker toegang heeft, zijn zichtbaar en kunnen worden geautoriseerd voor toegang op afstand.
- Als VCC's in HA zijn:
 - De RADKit-service kan alleen worden ingeschakeld op de Active/Primary.
 - Het secundaire FMC kan momenteel niet worden toegevoegd als een apparaat dat via RADKit-client kan worden benaderd.
- Toestemming kan slechts worden gegeven aan één support engineer per keer.
 - Als u een andere support engineer nodig hebt om toegang te hebben, maak dan een andere autorisatie aan voor de extra engineer. De service-ID zou hetzelfde zijn.

FMC REST API's

RADKit-API's voor serviceproviders

Om het maken en lezen van bewerkingen op RADKit Service te ondersteunen, zijn deze nieuwe URL's geïntroduceerd:

- KRIJG: `/api/fmc_troubleshoot/v1/domein/{domainUID}/radkit/services`
 - Wint alle RADKit-servicegegevens van het VCC op.
- KRIJG: `/api/fmc_troubleshoot/v1/domain/{domainUID}/radkit/services/{id}`
 - De RADKit-servicegegevens ophalen/ophalen uit de opgegeven ID.
- POST: `/api/fmc_troubleshoot/v1/domain/{domainUID}/radkit/services`
 - Hiermee maakt u de RADKit-service op het VCC (inschakelen/uitschakelen van de

service).

RADK-servicemodel

Het RADKit servicemodel bestaat uit:

- type
- id
- status
- ingesloten
- service-id
- versie

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

Cisco-ondersteuning: RADKit-clientgebruik

Ondersteunende zijde: De RADKit-client installeren

- Voor toegang tot de FMC/FTD(s) moet de RADKit-client zijn geïnstalleerd.
 - De client werkt op Windows, Mac en Linux besturingssystemen.
- Ondersteuning kan toegang hebben tot meerdere apparaten van meerdere gebruikers. Elke RADKit autorisatie heeft zijn eigen "inventaris" van apparaten.
 - Voor elke gebruiker apparaat inventaris die ondersteuning wil toegang hebben, is de RADKit service-ID nodig.
 - Voor één inventaris is toegang mogelijk voor zowel het VCC als zijn beheerde FTD's van de RADKit-client, zoals door de gebruiker gespecificeerd bij het verlenen van toegang.

RDKit-client verkrijgen en installeren

De RADKit-client kan lokaal worden geïnstalleerd vanaf

<https://radkit.cisco.com/downloads/release/> en vervolgens vanaf de terminal worden gelanceerd met de opdracht: radkit-client

Installateurs zijn beschikbaar voor Windows, MacOS en Linux.

```
radkit-client -- 147x40
15:07:59.886Z INFO | internal | CXD object created without authentication set, call '<this object>.authenticate()' to set authentication.

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
  service = direct_login()                        # Establish cloud-less direct connection to service.
  client.grant_service_otp()                      # Enroll a new service

>>> 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("8kji-znxg-3gkt")
15:09:03.406Z INFO | internal | Connecting to forwarder [forwarder_base_url='wss://prod.radkit-cloud.cisco.com/forwarder-4/' uri='wss://prod.radkit-cloud.cisco.com/forwarder-4/websocket/']
15:09:03.639Z INFO | internal | Connection to forwarder successful [forwarder_base_url='wss://prod.radkit-cloud.cisco.com/forwarder-4/' uri='wss://prod.radkit-cloud.cisco.com/forwarder-4/websocket/']
15:09:03.727Z INFO | internal | Forwarder client created. [forwarder_base_url='wss://prod.radkit-cloud.cisco.com/forwarder-4/']
15:09:04.003Z INFO | internal | Connecting to forwarder [forwarder_base_url='wss://prod.radkit-cloud.cisco.com/forwarder-1/' uri='wss://prod.radkit-cloud.cisco.com/forwarder-1/websocket/']
15:09:04.244Z INFO | internal | Connection to forwarder successful [forwarder_base_url='wss://prod.radkit-cloud.cisco.com/forwarder-1/' uri='wss://prod.radkit-cloud.cisco.com/forwarder-1/websocket/']
15:09:04.332Z INFO | internal | Forwarder client created. [forwarder_base_url='wss://prod.radkit-cloud.cisco.com/forwarder-1/']
>>> service.inventory
<radkit_client.sync.device.DeviceDict object at 0x1154969a0>
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
firepower-1724078669   127.0.0.1  FMC         True      False    False False    False  firepower    False
Untouched inventory from service 8kji-znxg-3gkt.

>>> 
```

RADKit client screenshot met inlogopdrachten (details in de volgende sectie).

Aanmeldingsopdrachten voor RDKit-client

- Gebruik het e-mailadres dat de gebruiker tijdens de autorisatie in het VCC heeft ingevoerd.
- De RADKit client login en verbinding met de opgegeven service-ID opdrachten. De RADKit service-ID, in dit voorbeeld 8abc-znxg-3abc, moet overeenkomen met wat de firewall-beheerder ziet in FMC.

```
<#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.rad
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.rad
15:09:04.332Z INFO | internal | Forwarder client created. [forwarder_base_url='wss://prod.radkit-cloud
```

Opdracht voor inventarisatie van clientservices voor RDK

Opdracht voor het weergeven van de inventaris waartoe de externe gebruiker (Cisco TAC Engineer) is geautoriseerd:

<#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.
```

Er is een filteropdracht voor de apparaten in de inventaris (volgende sectie). Gebruik de naam in de linkerkolom om een interactieve sessie met het apparaat te starten (opdracht voor komende sectie).



Tip: Als de inventaris verouderd is, kunt u deze bijwerken met de opdracht:

```
>> service.update_inventaris()
```

RDKit-client: Filterapparaten

Opdracht voor filterapparaten in de inventaris:

<#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.
```

Opdracht voor interactieve sessie voor RDKit-clientapparaat

Een interactieve sessie starten voor een apparaat (in dit geval een VCC) met de naam "FirePOWER-1724078669", overgenomen van de vorige opdracht "service.inventaris".

```
<#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/client.log']
```

```
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 password prompt.
```

```
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)
```

RDKit-client voert opdrachten uit op apparaten

Voer de opdrachten uit op apparaten!

```
<#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
-----
```

Ontvang aanvullende informatie van de apparaten

Rekening houdend met deze inventaris:

```
<#root>

>>>

service.inventory

[READY] <radkit_client.sync.device.DeviceDict object at 0x192cdb77110>
name             host      device_type  Terminal  Netconf  SNMP  Swagger  HTTP  desc
-----
10-62-184-69-1743156301  127.0.0.4  FTD          True      False    None  False    False  10.6
fmc1700-1-1742391113    127.0.0.1  FMC          True      False    None  False    False  FMC1
ftd3120-3-1743154081    127.0.0.2  FTD          True      False    None  False    False  FTD3
ftd3120-4-1743152281    127.0.0.3  FTD          True      False    None  False    False  FTD3
```

Om 'toon versie' details van de FTD apparaten:

```
<#root>
```

```
>>>
```

```
command = "show version"
```

```
>>>
```

```
ftds = service.inventory.filter("device_type", "FTD").exec(command).wait()
```

```
>>>
```

```
>>>
```

```
# Print the results
```

```
>>>
```

```
for key in ftds.result.keys():
```

```
...
```

```
print(key)
```

```
...
```

```
ftds.result.get(key).data | print
```

```
...
```

```
<- Press Enter twice
```

```
ftd3120-3-1743154081
```

```
> show version
```

```
-----[ FTD3100-3 ]-----
```

```
Model : Cisco Secure Firewall 3120 Threat Defense (80) Version 7.7.0 (Build 89)
```

```
UUID : 123a456a-cccc-bbbb-aaaa-a123456abcde
```

```
LSP version : lsp-rel-20250327-1959
```

```
VDB version : 404
```

```
-----
```

```
>
```

```
10-62-184-69-1743156301
```

```
> show version
```

```
-----[ KSEC-FPR1010-10 ]-----
```

```
Model : Cisco Firepower 1010 Threat Defense (78) Version 7.7.0 (Build 89)
```

```
UUID : 123a456a-cccc-bbbb-aaaa-a123456abcde
```

```
LSP version : lsp-rel-20250327-1959
```

```
VDB version : 404
```

```
-----
```

```
>
```

```
ftd3120-4-1743152281
```

```
> show version
```

```
-----[ FTD3100-4 ]-----
```

```
Model : Cisco Secure Firewall 3120 Threat Defense (80) Version 7.7.0 (Build 89)
```

```
UUID : 123a456a-cccc-bbbb-aaaa-a123456abcde
```

```
LSP version : lsp-rel-20250327-1959
```

```
VDB version : 404
```

>

Alternatieve benadering:

<#root>

```
>>> # Get the FTDs. This returns a DeviceDict object:
```

```
...
```

```
ftds = service.inventory.filter("device_type","FTD")
```

```
>>> # Access the dictionary of devices from the _async_object attribute
```

```
...
```

```
devices_obj = ftds.__dict__['_async_object']
```

```
>>> # Extract the 'name' from each AsyncDevice object
```

```
...
```

```
names = [device.name() for device in devices_obj.values()]
```

```
>>> # Get the 'show version' output from all FTD devices:
```

```
...
```

```
command = "show version"
```

```
...
```

```
show_ver_ftds = []
```

```
...
```

```
for name in names:
```

```
...
```

```
ftd = service.inventory[name]
```

```
...
```

```
req = ftd.exec(command)
```

```
...
```

```
req.wait(30)
```

```
    # depending on the number of devices you might need to increase the timeout value
```

```
...
```

```
show_ver_ftds.append(req.result.data)
```

```
>>> # Print the inventory device name + 'show version' output from each device:
...

for name, show_version in zip(names, show_ver_ftds):

...

print(f"Inventory name: {name}")

...

print(show_version[2:-2]) # Remove the leading '>' and trailing '\n>'

...

print("\n")
```

```
Inventory name: ftd3120-3-1743154081
show version
-----[ FTD3100-3 ]-----
Model : Cisco Secure Firewall 3120 Threat Defense (80) Version 7.7.0 (Build 89)
UUID : 123a456a-cccc-bbbb-aaaa-a123456abcde
LSP version : lsp-rel-20250327-1959
VDB version : 404
-----
```

```
Inventory name: ftd3120-4-1743152281
show version
-----[ FTD3100-4 ]-----
Model : Cisco Secure Firewall 3120 Threat Defense (80) Version 7.7.0 (Build 89)
UUID : 123a456a-cccc-bbbb-aaaa-a123456abcde
LSP version : lsp-rel-20250327-1959
VDB version : 404
-----
```

```
Inventory name: 10-62-184-69-1743156301
show version
-----[ KSEC-FPR1010-10 ]-----
Model : Cisco Firepower 1010 Threat Defense (78) Version 7.7.0 (Build 89)
UUID : 123a456a-cccc-bbbb-aaaa-a123456abcde
LSP version : lsp-rel-20250327-1959
VDB version : 404
-----
```

Bestanden van apparaten verkrijgen

- Via de RADKit-client kan een Cisco TAC-engineer SSH naar apparaten sturen en verschillende bewerkingen uitvoeren, waaronder het genereren van probleemoplossingsbestanden.

Cisco-ondersteuning: RADKit-console

RADKit-netwerkconsole gebruiken

- In plaats van de RADKit-client te gebruiken, kan een Cisco TAC-ondersteuningsengineer ook de RADKit-netwerkconsole gebruiken. De Netwerkconsole maakt deel uit van de RADKit-client.
- De RADKit Network Console is een voorziening die een eenvoudige opdrachtregelinterface (CLI) biedt voor de RADKit-clientfuncties. Het is bedoeld om te worden gebruikt voor een snelle verbinding met een RADKit Service-instantie, het opzetten van interactieve sessies en het downloaden/uploaden van bestanden zonder gedoe en minimale training.
- Start de netwerkconsole met de opdrachtregel: `radkit-netwerkconsole`
- Raadpleeg de RADKit documentatie voor meer informatie.

Compatibiliteit met upgrades en achteruit

Upgraden naar 7.7 en vanaf 7.7

- RADKit Service wordt toegevoegd in Secure Firewall 7.7.0.
 - Apparaten die zijn geüpgraded naar versie 7.7.0+ hebben de vereiste configuratie voor de RADKit Service.

Ervaring met niet-ondersteunde FTD's

- VCC's en FTD's moeten beschikken over de minimale versie 7.7.0 voor deze functie (FTD's met een versie lager dan 7.7 mogen niet worden toegevoegd aan een 7.7 FMC RADKit-autorisatie).
- Geregistreerde FTD's die niet onder 7.7.0 vallen, kunnen niet worden geselecteerd voor autorisatie.

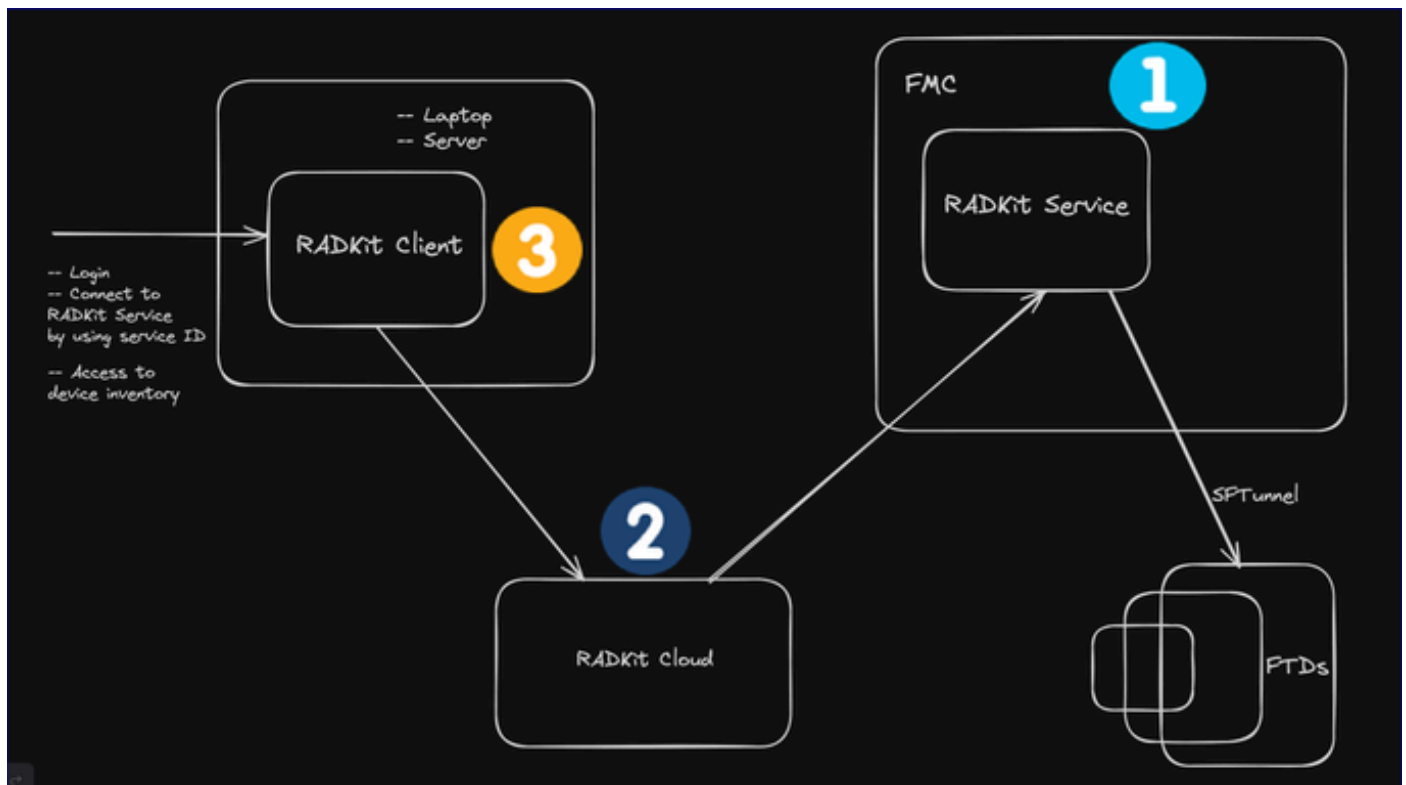
Probleemoplossing

Overzicht van diagnoses

Punten voor probleemoplossing

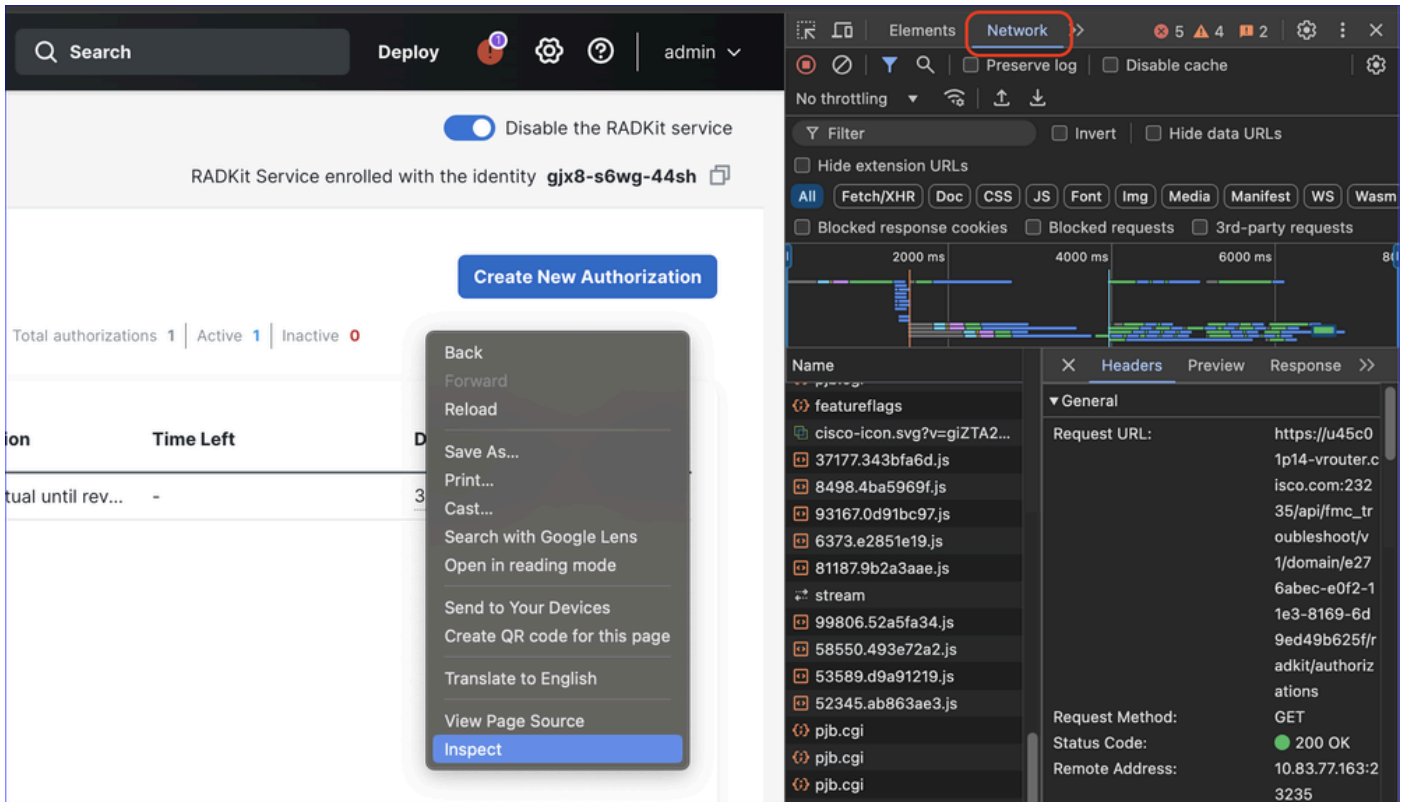
1. Gebruik Browser Development tools en FMC logs om te zien wat er gebeurt in FMC.
2. Voor communicatieproblemen tussen RADKit Service op FMC, RADkit Cloud, en RADKit client, kijk in RADKit client logging.

3. RADKit-client.



Probleemoplossing: Browser's Developer Tools

- De browser Developer Tools, Network tabblad toont de API-oproepen die op de pagina werden uitgevoerd, dit kan worden gebruikt bij problemen oplossen op FMC. Dit kan worden gestart door met de rechtermuisknop op pagina te klikken en vervolgens op Inspect te klikken.
- Controleer de API-gespreksstatuscode en de reactievoorvertooning in het tabblad Netwerk.



RADKit Service Go Middleware API's

Go Middleware voor de RADKit-integratie maakt gebruik van API-oproepen die niet publiekelijk beschikbaar zijn via de FMC API-verkenner. Het logboek van Go Middleware APIs is beschikbaar in `/var/log/auth-daemon.log`. Functionality Go Middleware voert onder meer uit:

- Schrijf de RADKit Service in in de RADKit cloud met Single Sign On proces.
- Zoek een lijst met alle autorisaties en bijbehorende apparaten van alle externe RADKit-gebruikers.
- Ontvang een specifieke externe RADKit gebruikersautorisatie en bijbehorende apparaten door het gebruik van een e-mail.
- Maak een externe RADKit gebruikersautorisatie en geef toegang tot apparaten (alle apparaten of een lijst van geselecteerde apparaten) voor een opgegeven tijdsbestek.
- Wijzig een externe RADKit gebruikersautorisatie.
- Verwijder een externe RADKit gebruikersautorisatie.

Logbestanden voor probleemoplossing bij de RADKit-service

- Algemene VCC-logbestanden: `pigtail` commando van een FMC ssh sessie.
- Go Middleware API's: `/var/log/auth-daemon.log`
- Logbestanden die RADKit en auth-daemon bevatten, verwerken gegevens:

`/var/log/process_stdout.log`

`/var/log/process_stderr.log`

Al deze logbestanden worden opgenomen in FMC/FTD Troubleshoots.

- Interne RADKit-servicelogboeken: `/var/lib/radkit/logs/service/`
- Logbestanden voor de bewerkingen uitgevoerd vanuit de RADKit-client op apparaten (FMC's en FTD's): `/var/lib/radkit/session_logs/service`

Logbestanden om in te dienen bij Cisco TAC

- Screenshots van fouten.
- Beschrijving van probleem.
- Stappen om te reproduceren.
- Uittreksels van de varkensstaart en `/var/log/auth-daemon.log` bevatten de fouten.

Toegang tot bewaking

In de auditlogboeken van het VCC wordt geregistreerd wie gedurende welke periode toegang heeft gekregen en wie toegang heeft verleend.

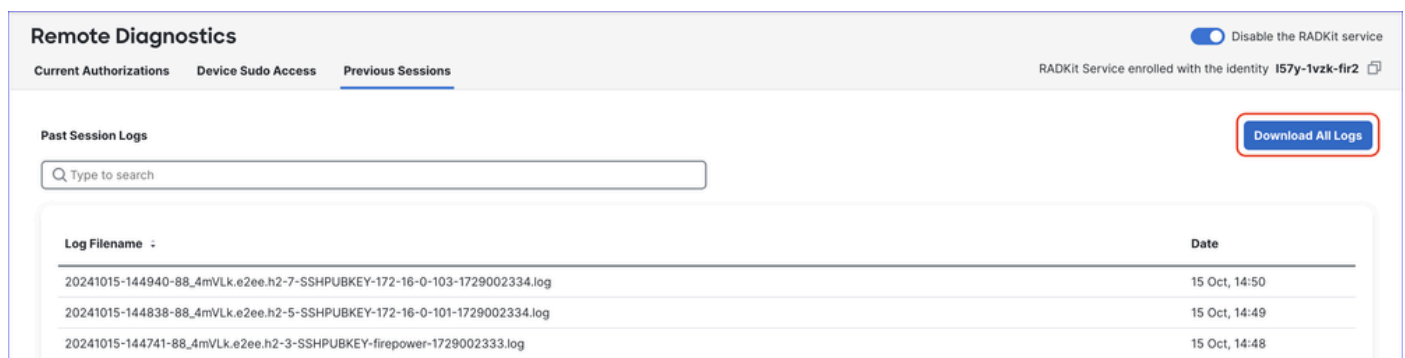
RADKit-sessielogboeken

RADKit-sessielogboeken voor de bewerkingen uitgevoerd vanuit de RADKit-client op apparaten (FMC's en FTD's) zijn aanwezig op FMC op `/var/lib/radkit/sessie_logs/service`:

- De logboeken zijn van de RADKit-dienst zelf.
- Deze logbestanden worden opgenomen in een bundel Probleemoplossing.
- De logboeken zijn ook toegankelijk vanuit UI (zie de volgende sectie).
- Er zijn meerdere sessielogbestanden; één per sessie.

Logbestanden van vorige RADKit-sessies

De RADKit sessielogboeken voor de apparaatbewerkingen uitgevoerd vanuit de RADKit-client zijn beschikbaar voor downloaden als een archief met alle logbestanden in het tabblad Vorige sessies door te klikken op "Download All Logs" knop.



Remote Diagnostics Disable the RADKit service

Current Authorizations Device Sudo Access **Previous Sessions** RADKit Service enrolled with the identity `IS7y-1vzk-fir2`

Past Session Logs Download All Logs

Q Type to search

Log Filename	Date
20241015-144940-88_4mVLk.e2ee.h2-7-SSHPUBKEY-172-16-0-103-1729002334.log	15 Oct, 14:50
20241015-144838-88_4mVLk.e2ee.h2-5-SSHPUBKEY-172-16-0-101-1729002334.log	15 Oct, 14:49
20241015-144741-88_4mVLk.e2ee.h2-3-SSHPUBKEY-firepower-1729002333.log	15 Oct, 14:48

Probleem met probleemoplossing bij doorlopen van voorbeelden

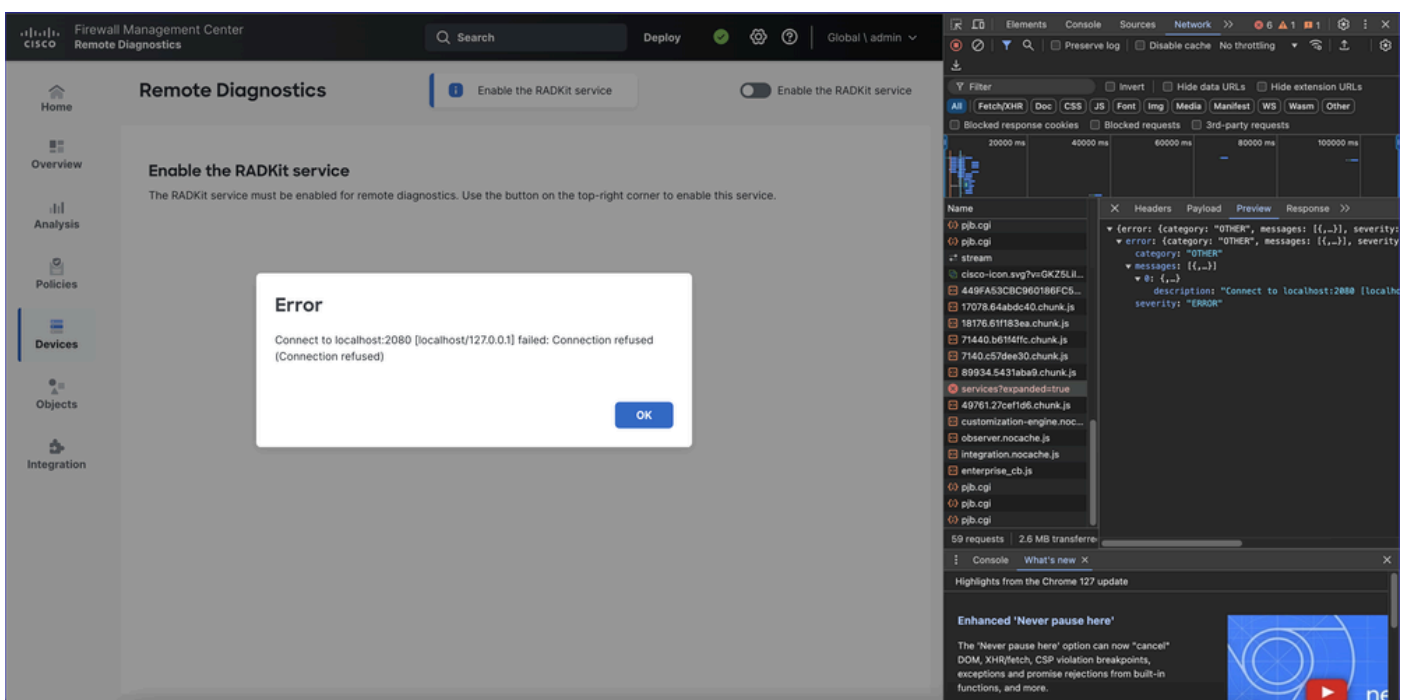
Voorbeeld van probleemoplossing

In het geval van een fout zoals "Connect to localhost:2080 [localhost/127.0.0.1] is mislukt: Verbinding geweigerd (verbinding geweigerd)", probeer auth-daemon opnieuw te starten vanaf een FMC SSH sessie:

```
<#root>
```

```
root@firepower:~$
```

```
sudo pmtool restartbyid auth-daemon
```



telemetrie

De telemetrieuitvoer werd voor deze eigenschap toegevoegd:

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

FAQ

Veelgestelde vragen: Aanmelden en inschrijving

V. Werkt de inschrijving bij volmacht als FMC geen rechtstreekse internettoegang heeft?

A. Ja, als de proxy toegang heeft tot prod.radkit-cloud.cisco.com die wordt gebruikt voor het inschrijvingsproces.

Q. Kan een gebruiker hun eigen IDp voor deze dienst gebruiken?

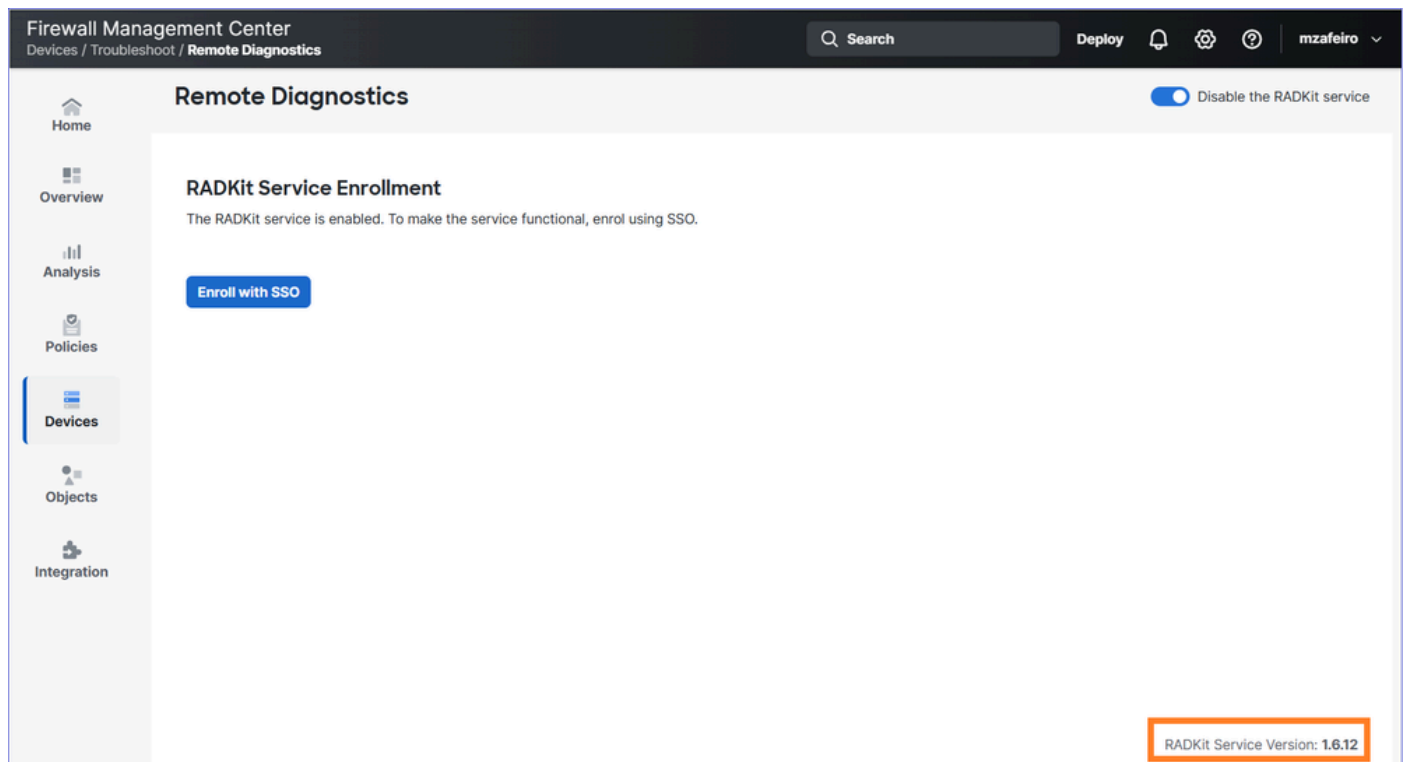
A. Alleen Cisco SSO wordt geaccepteerd in de RADKit-cloud. Er is een optie om uw bedrijfsaccount te koppelen aan een Cisco-account, zodat de inschrijving voor de RADKit-service mogelijk is met een e-mail die niet door Cisco is verzonden.

Veelgestelde vragen: RADKit versies

V. Welke versie van RADkit is opgenomen in FMC in 7.7 release? Hoe weten we welke versie van RADKit in FMC is opgenomen? Is dit iets dat kan worden bijgewerkt zonder een FMC upgrade?

A.

- De versie van RADKit die met 7.7.0 komt is 1.6.12.
- De versie van de RADKit-service wordt weergegeven op de onderkant van de FMC Remote Diagnostics-pagina: "RDKit-serviceversie: 1.6.12."



- RADKit is gebundeld met FMC upgrade pakketten/hotfixes. Het afzonderlijk upgraden van de RADKit-service in het VCC wordt niet ondersteund.

Veelgestelde vragen: Other (Overig)

V. Kunnen externe apparaten - die niet door het VCC worden beheerd - worden meegenomen?

A. Alleen door het VCC beheerde apparaten kunnen aan de RADKit-inventaris worden toegevoegd en kunnen via een vergunning worden geraadpleegd.

V. Wordt van RADKit configuratie een back-up gemaakt als onderdeel van FMC back-up?

A.

- Van de configuratie wordt geen back-up gemaakt als onderdeel van de FMC-back-up.
- Het wordt niet ondersteund omdat we verwachten dat er in het algemeen geen permanente toegang zal worden verschaft; de toegang is doorgaans slechts voor een beperkte tijd.

Referenties

Handige links:

- [FMC-configuratiehandleiding - RADKit](#)
- <https://radkit.cisco.com/>
- <https://radkit.cisco.com/docs/index.html>
- <https://radkit.cisco.com/downloads/release/>
- <https://github.com/Cisco-RADKit/Intro>

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.