Konfigurieren der Cisco RADKit-Integration in FMC

Inhalt

Einleitung

In diesem Dokument wird die Cisco RADKit Integration in FMC-Funktion beschrieben, die in Version 7.7 hinzugefügt wurde.

Hintergrund

Problem Firewall-Administratoren

- Das Remote Automation Development Kit (RADKit) von Cisco ist ein netzwerkweiter Orchestrator, der Benutzern die Möglichkeit bietet, sicher auf Netzwerkgeräte zuzugreifen und Fehler zu beheben. https://radkit.cisco.com/
- Das Cisco Secure Firewall Management Center (FMC) verwaltet und betreibt FTD-Geräte (Secure Firewall Threat Defense). Ein einziges FMC kann mehrere Geräte an verschiedenen Standorten verwalten.
- Während es für Benutzer möglich ist, RADKit separat zu installieren und ihre FMCs und FTDs darin zu integrieren, wäre es für Endbenutzer besser, den RADKit-Service in das FMC zu integrieren und das FMC bzw. die FMCs und alle verwalteten Geräte (FTDs) automatisch zu integrieren.

Anwendungsfall

Einige der wichtigsten Funktionen, von denen die Benutzer nach der Integration von RADKit in das FMC profitieren könnten, sind:

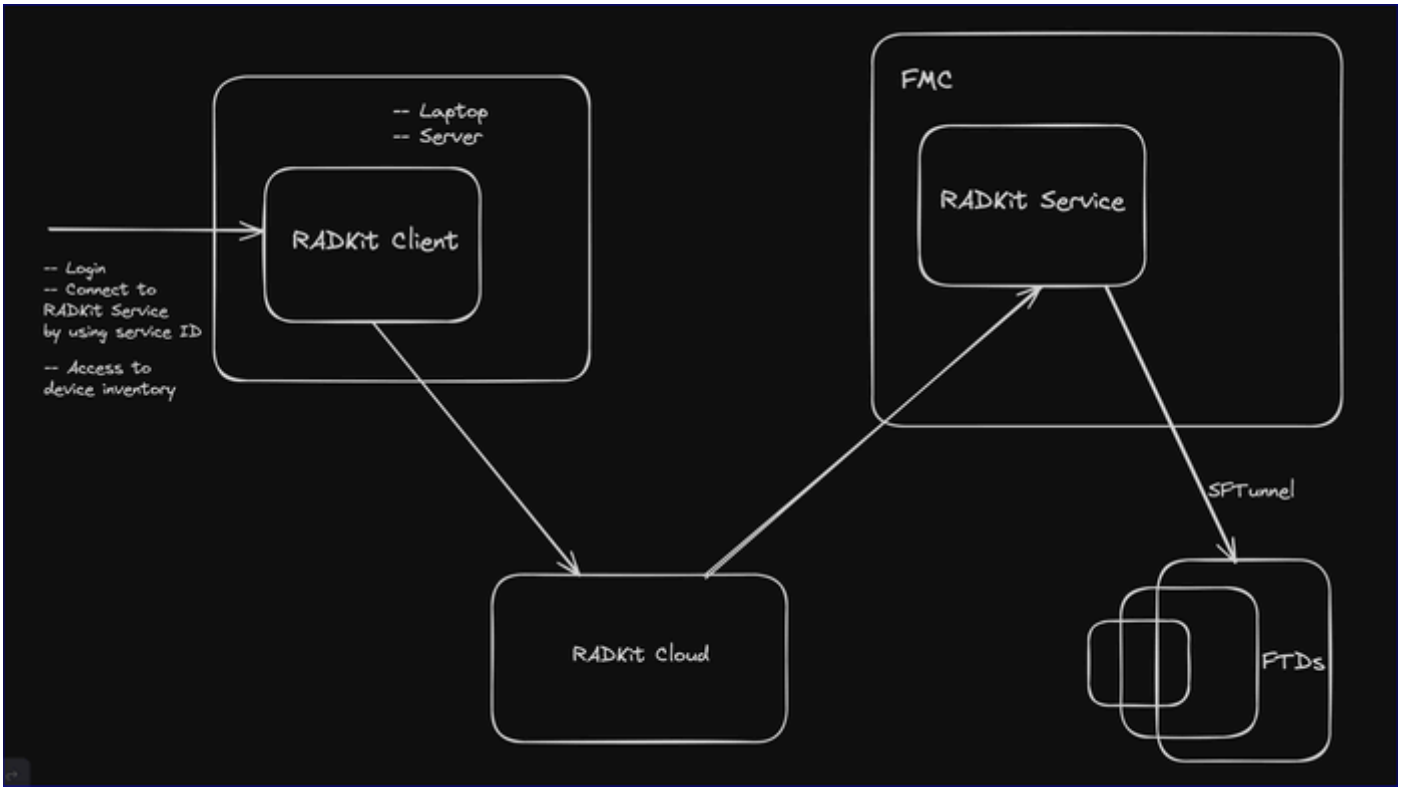
- Remote-Zugriff auf FMCs/FTDs über die RADKit-Client-CLI.
- Möglichkeit zur Bereitstellung eines kontrollierten Zugriffs auf FMCs/FTDs für jeden, der diesen benötigt (z. B. ein Cisco TAC-Techniker).
- Nutzung von Automatisierungsfunktionen zur Erfassung von Daten und Diagnose von Problemen über den RADKit-Client (Skripte, die Befehle auf mehreren Geräten ausführen, können vom RADKit-Client erstellt und verwendet werden).

Neuerungen - Lösung

- Ab Secure Firewall 7.7.0 ist der Remote Automation Development Kit (RADKit) Service in FMC integriert.
- Benutzer können den RADKit-Dienst bei Bedarf aktivieren oder deaktivieren, ihn in der RADKit-Cloud registrieren und Remote-Benutzerautorisierungen für den Zugriff auf bestimmte Geräte über den RADKit-Client für einen geplanten Zugriffszeitraum erstellen.
    - Autorisierungen können bearbeitet oder widerrufen werden.
- Es besteht auch die Möglichkeit, Geräten sudo-Zugriff für die erweiterte Fehlerbehebung bereitzustellen.

RADKit Service Integration in FMC Diagramm

Dieses Diagramm zeigt, wie RADKit die Kommunikation zwischen dem RADKit-Client des Benutzers (TAC-Techniker) und den FTD-Geräten der Produktion ermöglicht:



Grundlagen: Unterstützte Plattformen, Lizenzierung

Anwendungen und Manager

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		

Weitere Aspekte der Unterstützung

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

Abhängigkeiten für den Betrieb der Funktion

- Die Mindestversion ist Secure Firewall 7.7.0.
- Um eine Verbindung zum RADKit-Service innerhalb des FMC herzustellen, muss der RADKit-Client von https://radkit.cisco.com/downloads/release/ auf dem Computer des Supporttechnikers installiert werden.
- Die bevorzugte Version für den RADKit Client ist 1.6.10 oder höher.
- Ältere Versionen von RADKit Client können verwendet werden, da der RADKit Service abwärtskompatibel mit älteren Versionen von RADKit Client ist.

Funktionsbeschreibung und exemplarische Vorgehensweise

Funktionsüberblick

- Durch die Integration des RADKit-Service in FMC können Geräteadministratoren Remote-Benutzern (Cisco TAC-Technikern) Zugriff auf bestimmte FMC- und FTD-Geräte in ihrem Netzwerk zu Zwecken der Fehlerbehebung und Automatisierung gewähren. RADKit ist für die Fehlerbehebung viel effizienter als die Bildschirmfreigabe, es muss nicht den Computer des Benutzers steuern, ist eine sicherere Möglichkeit, an einem Netzwerk zu arbeiten, und ergänzt WebEx schön.
- Dies verbessert den technischen Support, da die Geräteadministratoren den RADKit-Service nicht separat installieren und konfigurieren müssen. Darüber hinaus verkürzt sich dadurch die Zeit, die Cisco TAC-Techniker zur Behebung von Support-Problemen benötigen.

Konfigurationsschritte: Überblick

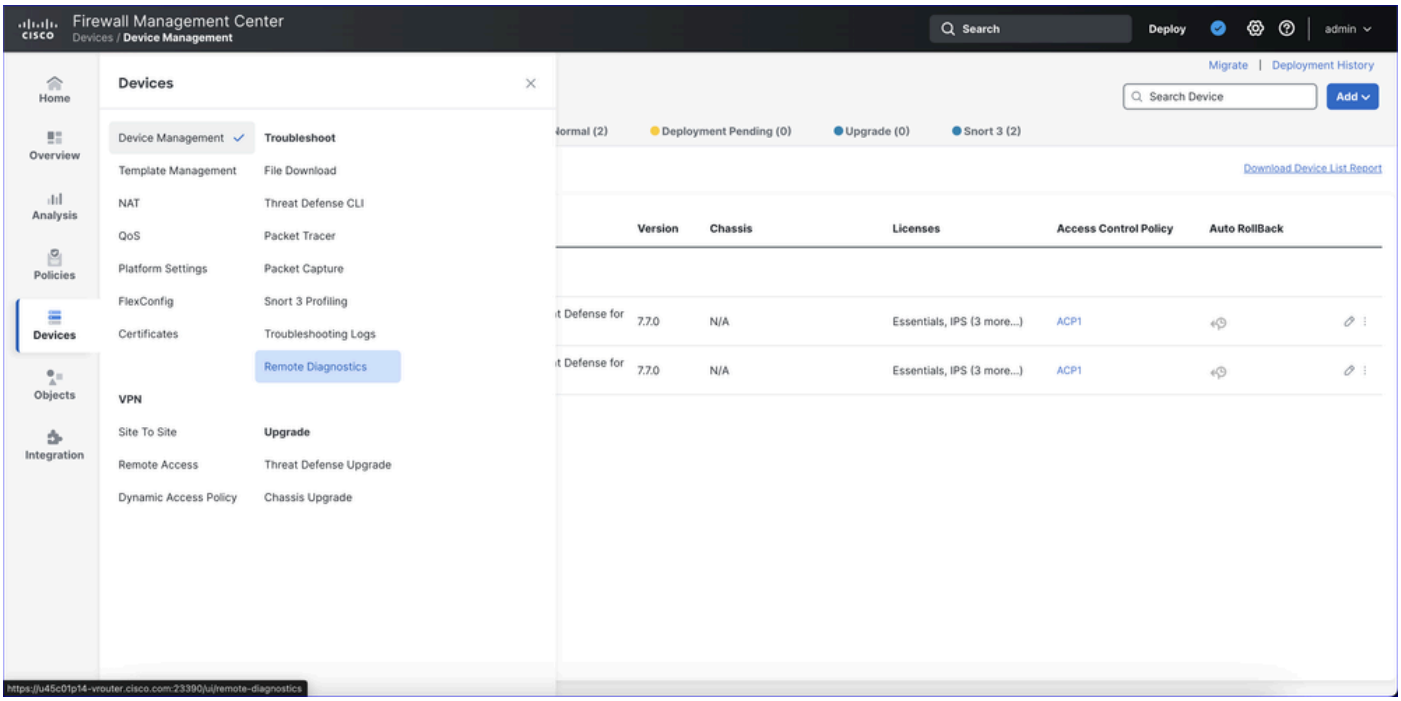
1. Geräteadministrator (FMC-Administrator-Benutzer): Aktivieren und Registrieren des RADKit-Service und Konfigurieren von Autorisierungen auf der FMC-GUI

2. Cisco TAC/Cisco Support: Installieren Sie den RADKit-Client auf dem Computer, greifen Sie auf die Geräte des RADKit-Clients zu, und beheben Sie Fehler.

FMC-Admin-Benutzer: Firewall Management Center - exemplarische Vorgehensweise

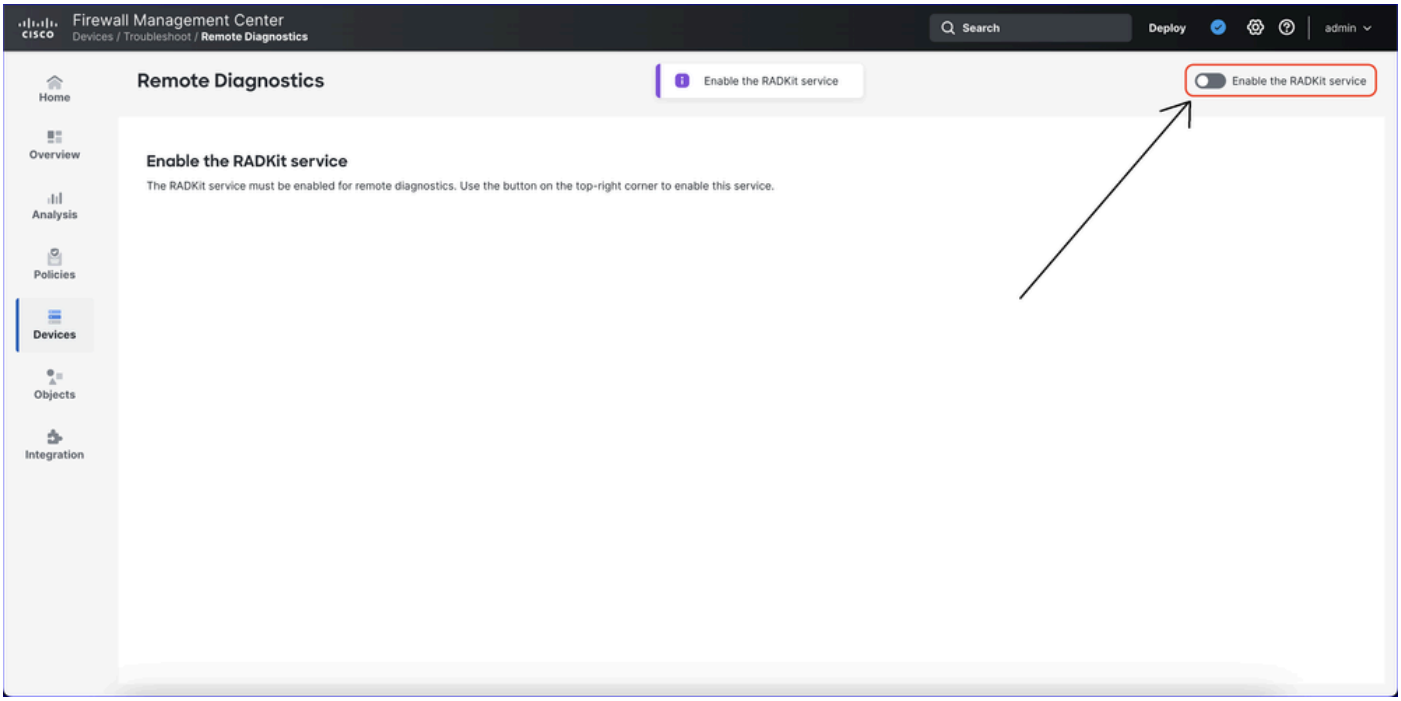
Menü "Remote Diagnostics"

- Für diese Funktion wurde unter Geräte -> Fehlerbehebung ein neuer Menüeintrag "Ferndiagnose" hinzugefügt.
- Administrator-, Netzwerkadministrator- und Wartungsbenutzer haben Lese-/Schreibzugriff auf der Seite.
- Benutzer von Sicherheitsanalyst, Sicherheitsanalyst (schreibgeschützt) und Sicherheitsgenehmiger verfügen über Leseberechtigungen für die Seite.



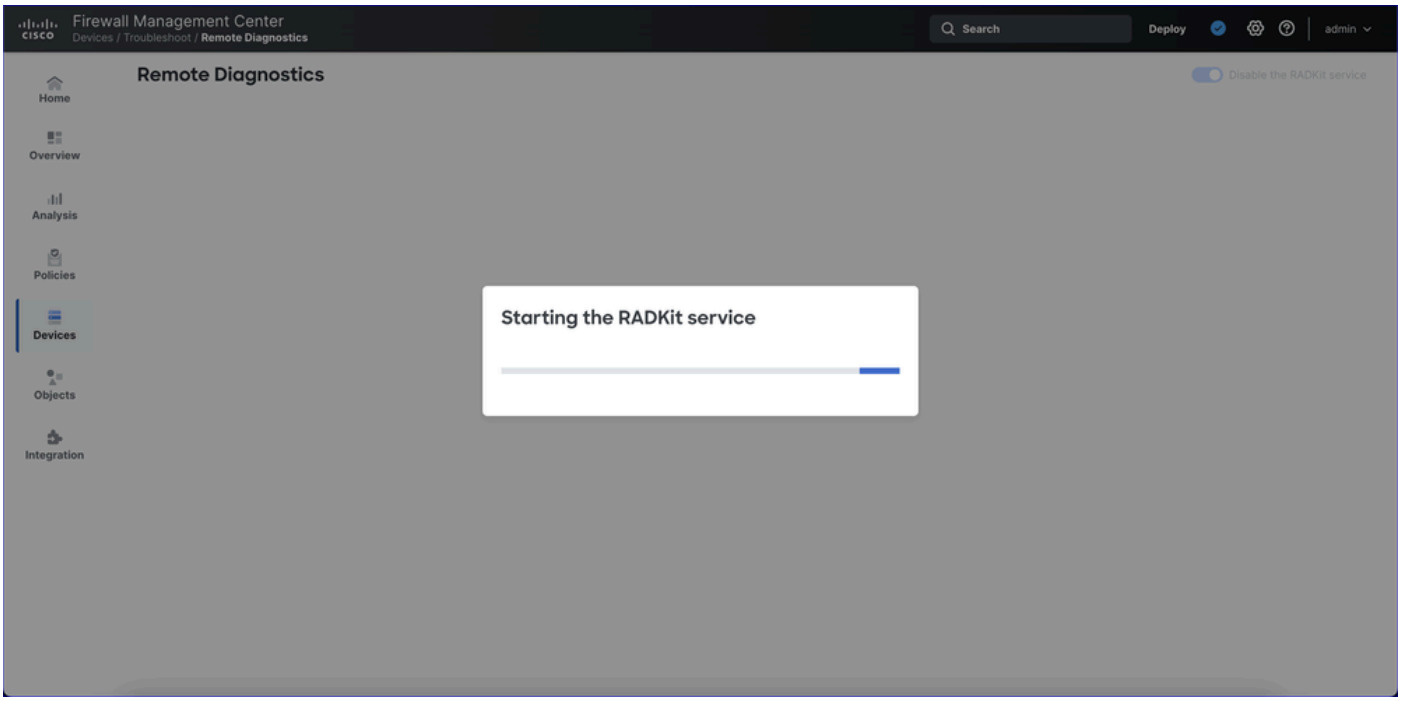
Seite "Erste Remote-Diagnose"

Dies ist die Seite Remote Diagnostics (Remote-Diagnose). Der RADKit-Dienst kann aktiviert werden, indem der Switch "Aktivieren des RADKit-Dienstes" umgeschaltet wird:



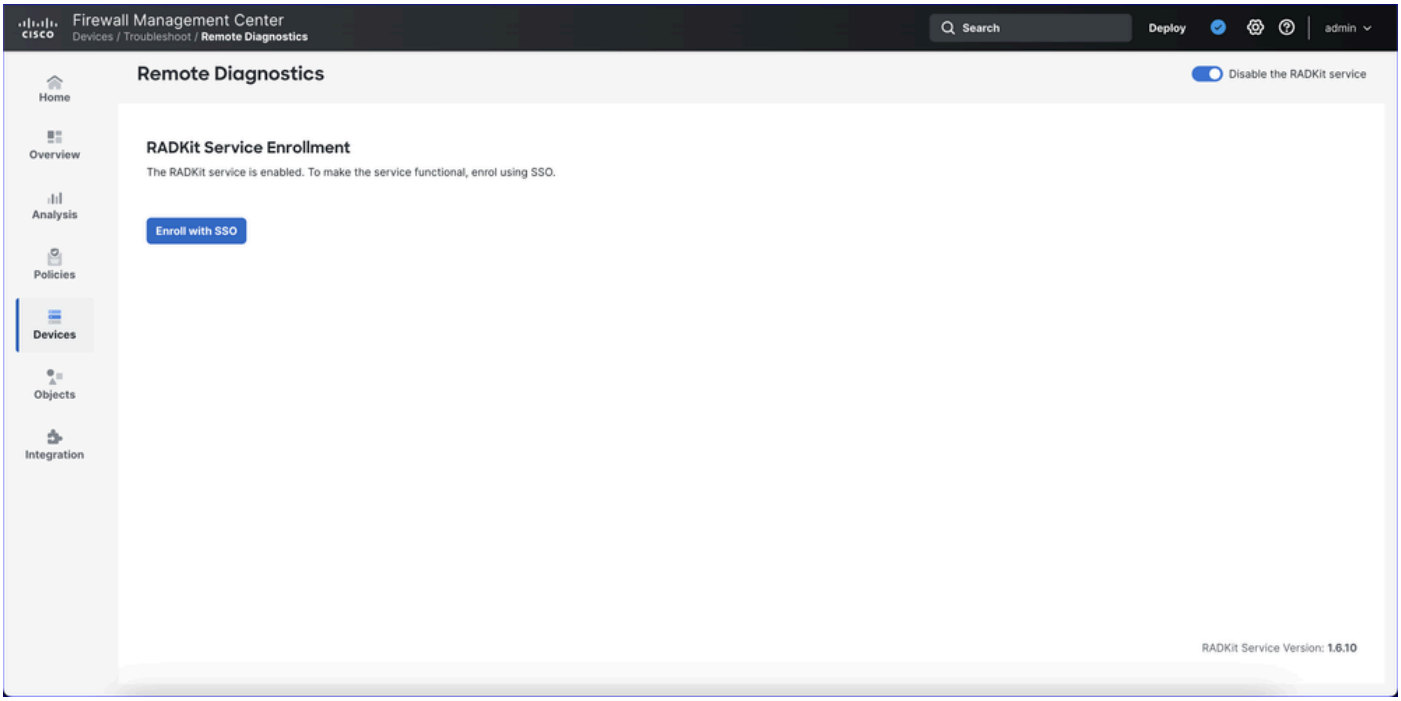
RADKit-Dienst wird gestartet

Nach der Aktivierung des RADKit-Diensts wird eine Statusanzeige angezeigt, bis der RADKit-Dienst gestartet wird:



RADKit-Dienst aktiviert

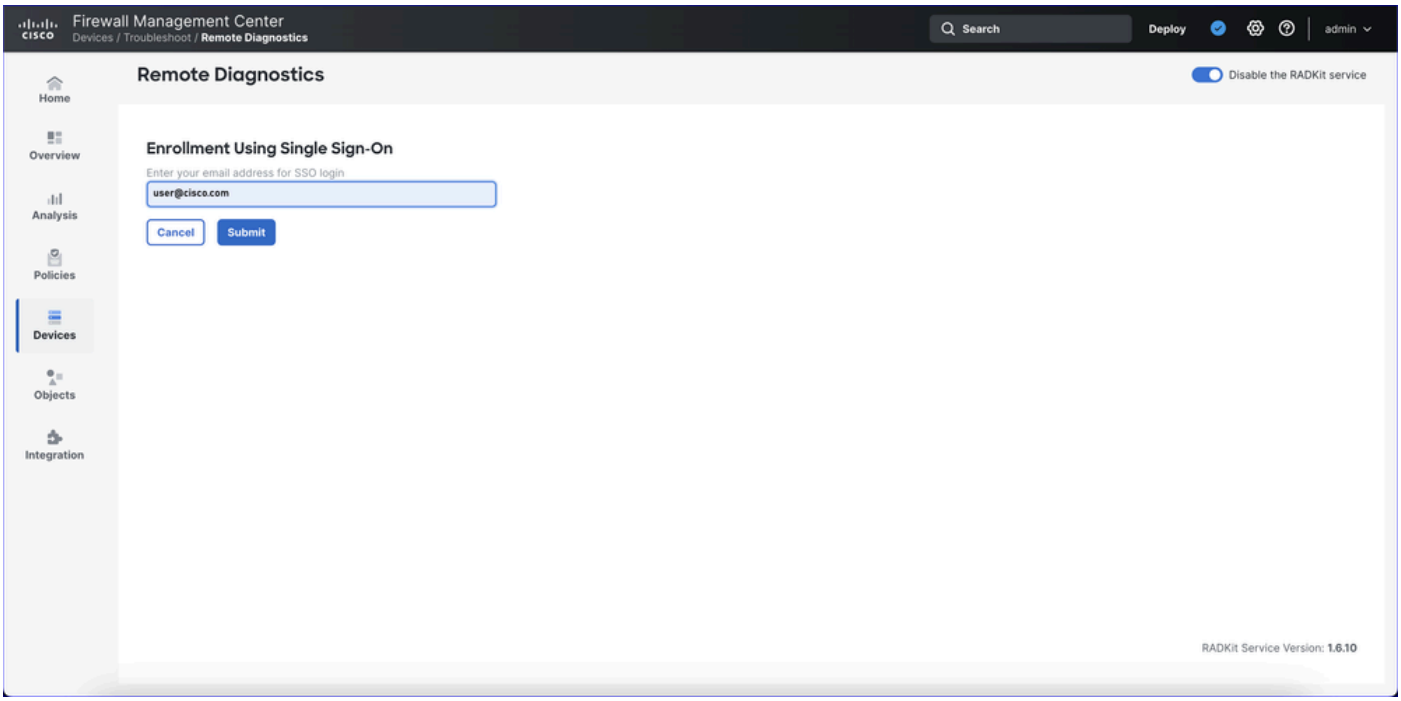
- Wenn der RADKit-Dienstaktivierungsprozess abgeschlossen ist, wird diese Seite angezeigt:



Der nächste Schritt ist die Registrierung in der RADKit-Cloud durch Klicken auf die Schaltfläche "Bei SSO anmelden".

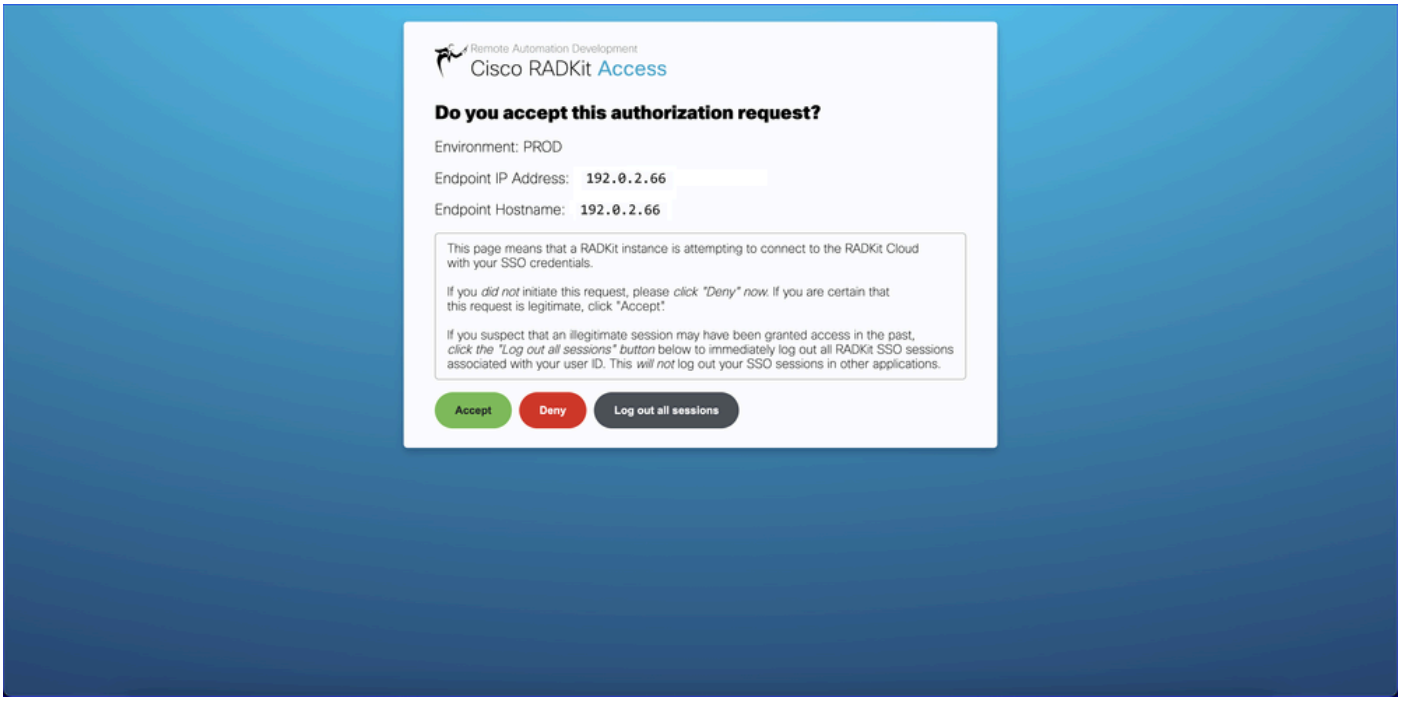
Bei SSO anmelden - E-Mail-Adresse eingeben

Schritt 1 des Registrierungsprozesses besteht in der Eingabe der Benutzer-E-Mail-Adresse für die RADKit Cloud-Registrierung:



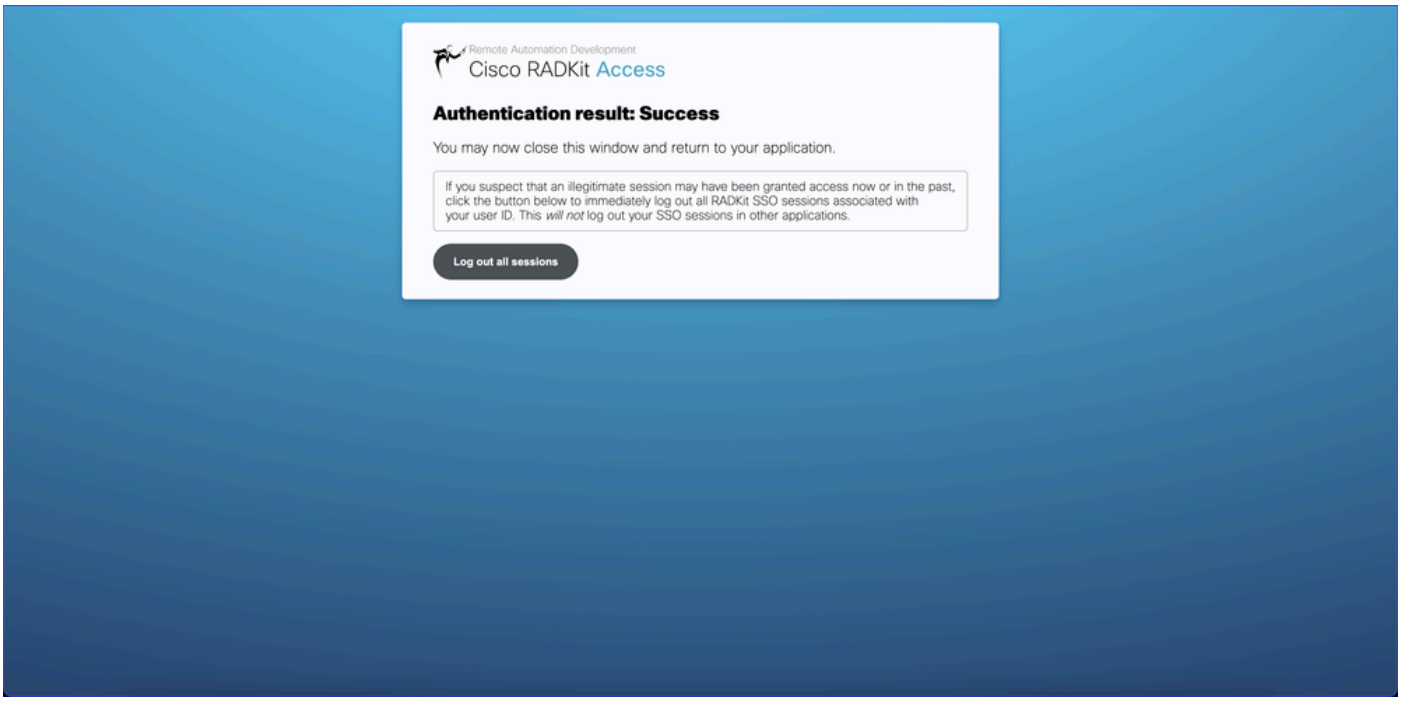
Anmeldung bei SSO - Genehmigungsanfrage annehmen

Eine neue Browserregisterkarte (oder ein neues Browserfenster, je nach Browsereinstellungen) wird geöffnet. Klicken Sie auf die Schaltfläche Akzeptieren.



Bei SSO registrieren - Authentifizierung erfolgreich

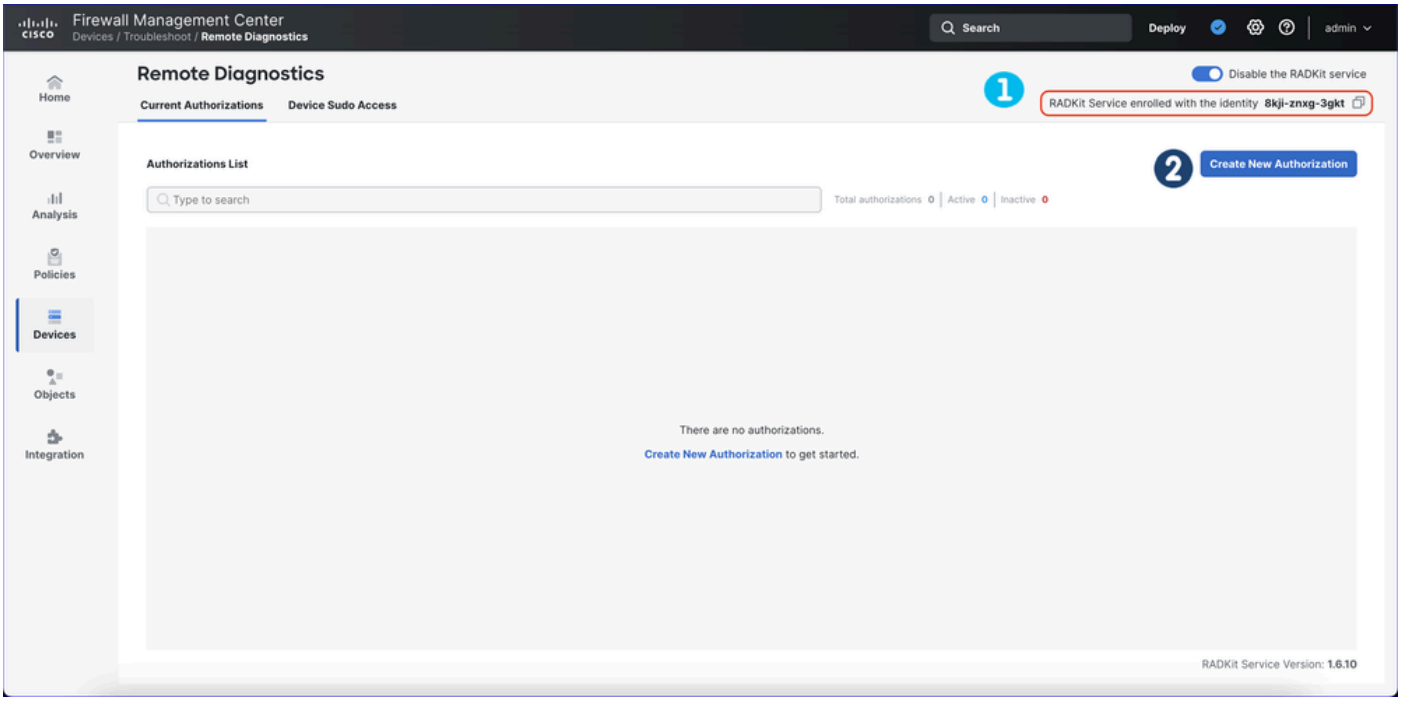
Nach erfolgreicher Authentifizierung kann der Benutzer die Browser-Registerkarte schließen und zur Seite FMC Remote Diagnostics (Remote-Diagnose für FMC) zurückkehren.



RADKit-Service angemeldet

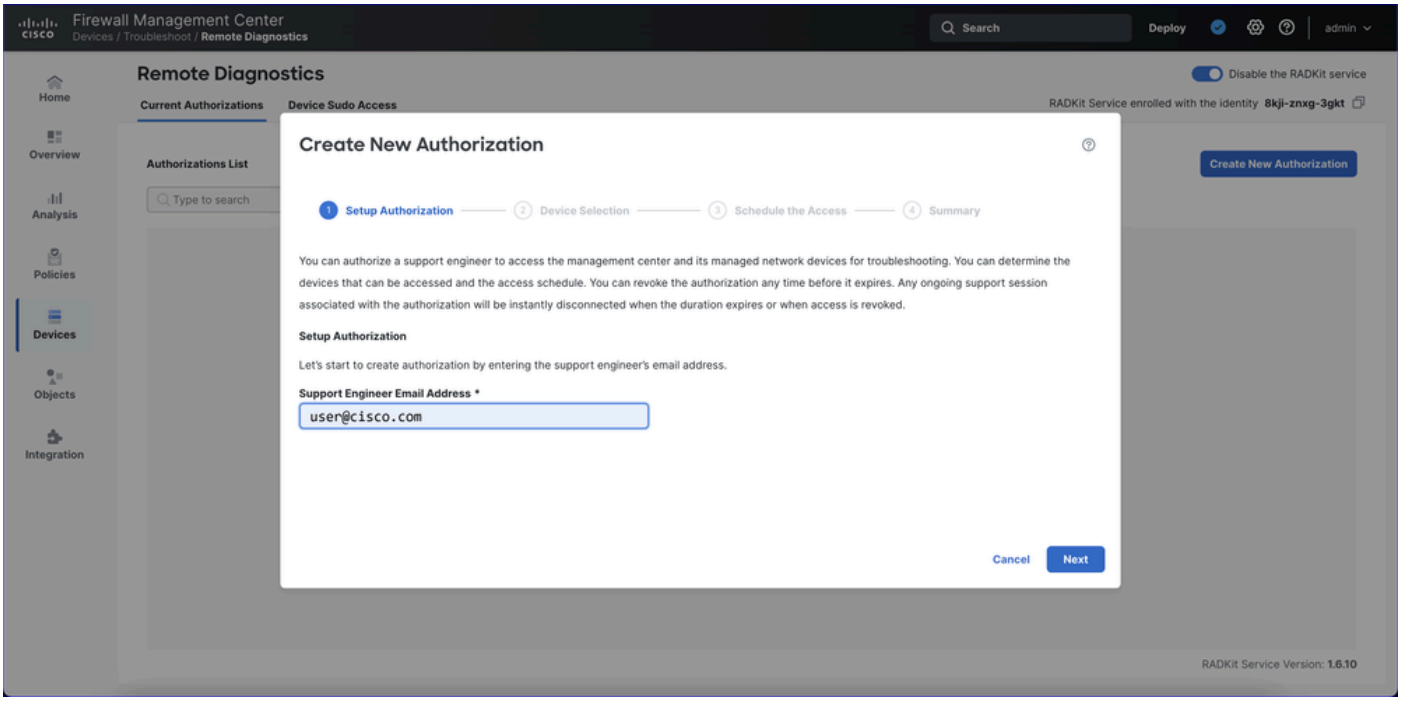
Der RADKit-Dienst wird mit der angegebenen Dienst-ID registriert (in diesem Beispiel ist die ID 8kji-znxg-3gkt). Die ID kann in die Zwischenablage kopiert werden. Er wird an den Cisco TAC-Techniker weitergeleitet, damit dieser über den RADKit-Client eine Verbindung zum RADKit-Service herstellen kann.

Als Nächstes erstellen Sie eine Autorisierung, indem Sie auf die Schaltfläche "Create New Authorization" (Neue Autorisierung erstellen) klicken:



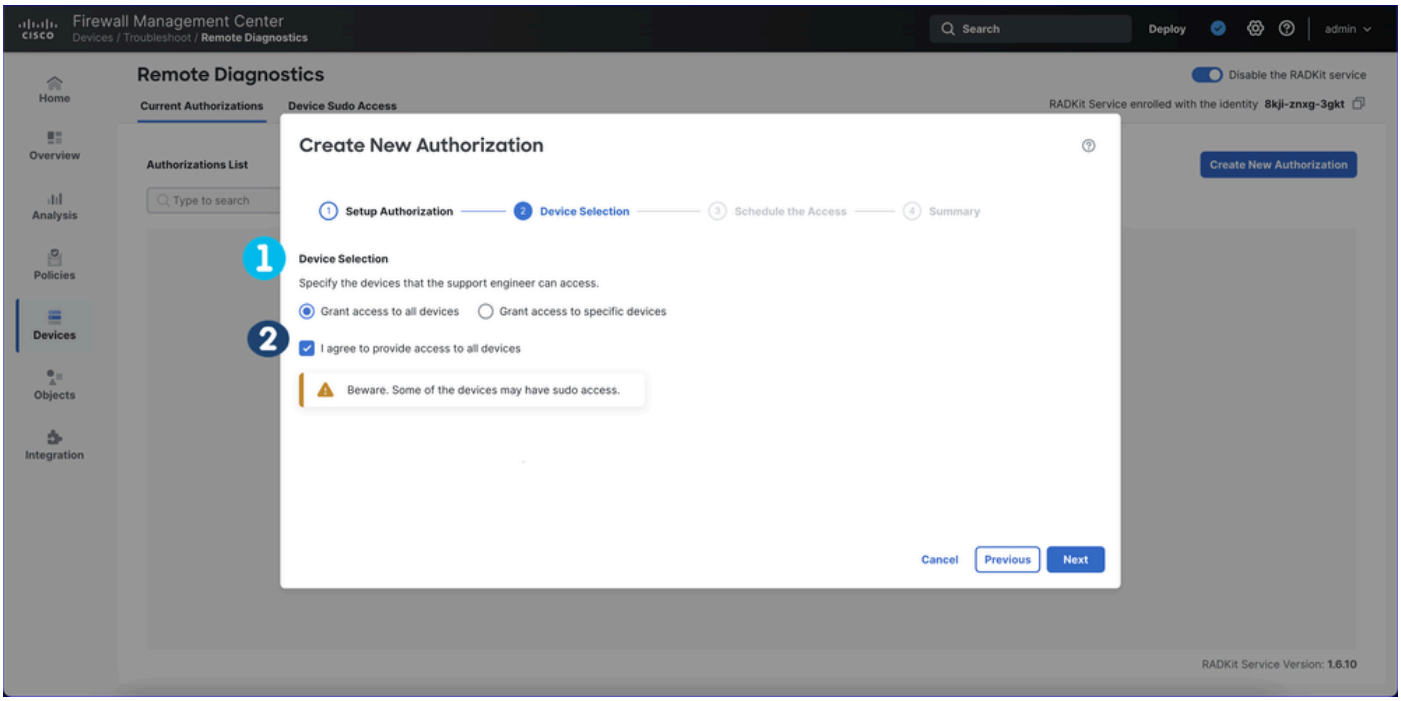
Neue Autorisierung erstellen: Schritt 1

- Um eine neue Autorisierung zu erstellen, müssen Sie zunächst die E-Mail-Adresse des Supporttechnikers eingeben.
- Es gibt vier Schritte zum Erstellen einer neuen Autorisierung. Der Fortschritt der Schritte wird oben angezeigt.



Neue Autorisierung erstellen: Schritt 2

- Schritt 1: Geben Sie die Geräte an, auf die der Supporttechniker zugreifen kann. Oder gewähren Sie, wie in diesem Beispiel, Zugriff auf alle Geräte.
- Phase 2: Aktivieren Sie das Optionsfeld für alle oder bestimmte Geräte. Für bestimmte Geräte können FMC und/oder FTD(s) ausgewählt werden. Beachten Sie, dass der Sudo-Zugriff auf einige Geräte über die Registerkarte Geräte-Sudo-Zugriff bereitgestellt werden kann. Die Schaltfläche Weiter ist erst aktiviert, wenn das Kontrollkästchen aktiviert ist.
- Der Sudo-Zugriff wird auf der Registerkarte "Device Sudo Access" (Geräte-Sudo-Zugriff) zu einem späteren Zeitpunkt (nicht beim Erstellen einer Autorisierung) pro Gerät bereitgestellt.

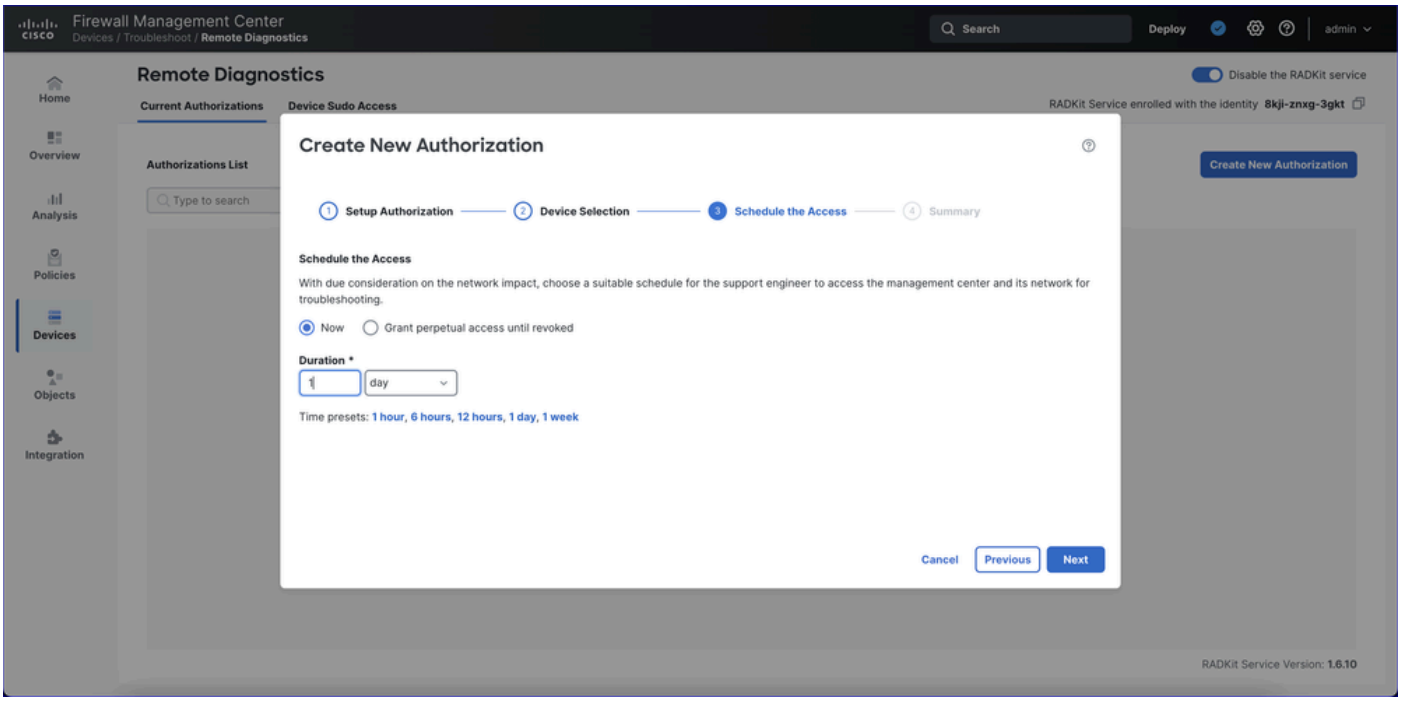


Hinweise zur Geräteauswahl

- Nur Geräte mit einem unterstützten Build (z. B. in der ersten Version nur Geräte mit 7.7.0) können ausgewählt werden.
- Deaktivierte und nicht erreichbare Geräte können nicht ausgewählt werden. RADKit greift auf die Geräte über sftunnel (TCP 8305) zu.
  - Wenn ein Problem mit der Verbindung zu einem Sftunnel vorliegt, funktioniert es nicht, wird jedoch im RADKit-Inventar angezeigt.
  - Wenn ein Gerät ausgeschaltet ist, wird es überhaupt nicht angezeigt.
- Wenn ein HA-Paar FMCs enthält, können nur die Aktiv/Primär-Module hinzugefügt werden.
- Die Geräte werden dem RADKit-Inventar beim Erstellen/Bearbeiten einer Autorisierung hinzugefügt. Wenn Geräte vom FMC abgemeldet werden, werden sie aus dem "Gerätebestand" entfernt.

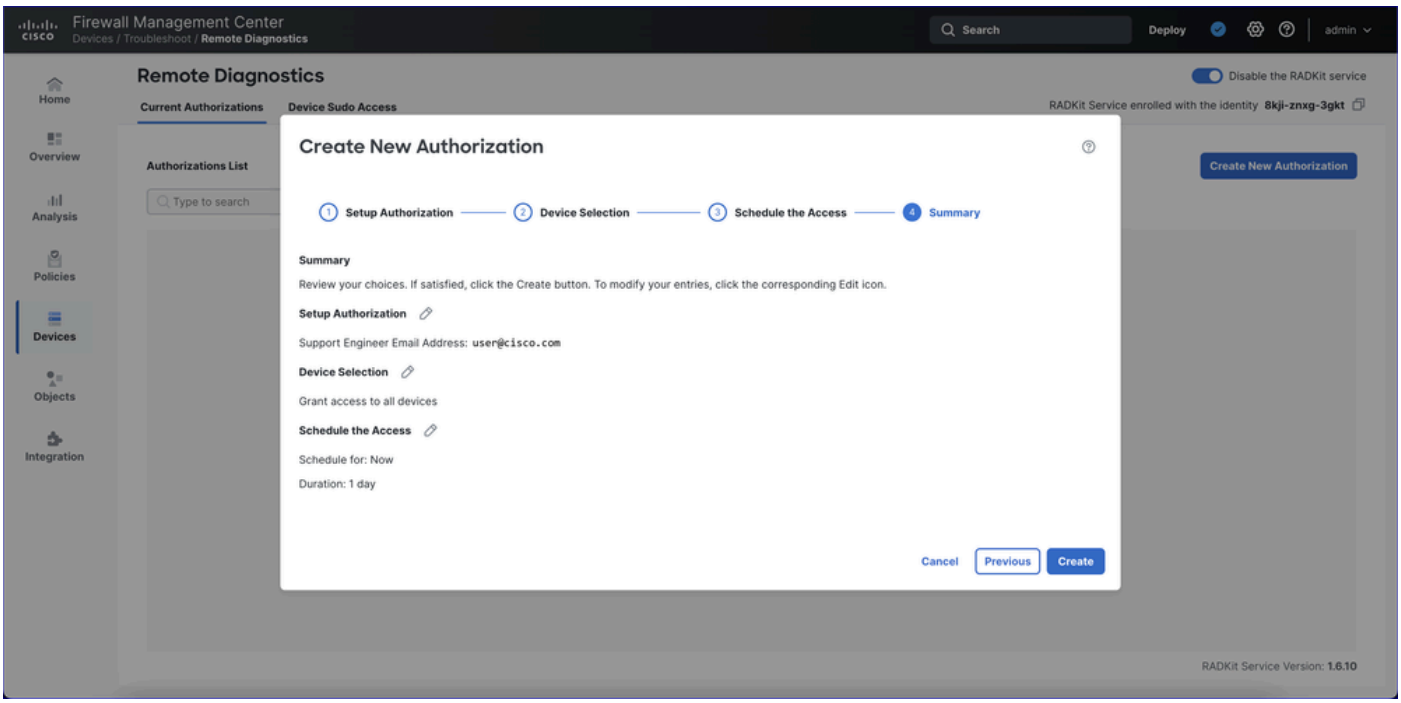
Neue Autorisierung erstellen: Schritt 3

- Schritt 3: Geben Sie die Dauer für den Support-Technikerzugriff auf die Geräte an.
- Wählen Sie "Jetzt" und geben Sie eine Dauer an, oder
- Wählen Sie "Uneingeschränkten Zugriff gewähren, bis er widerrufen wird".
- Die Standarddauer ist 1 Tag. Es kann eine beliebige Dauer festgelegt werden. Es gibt auch einige vordefinierte Werte für die Dauer.



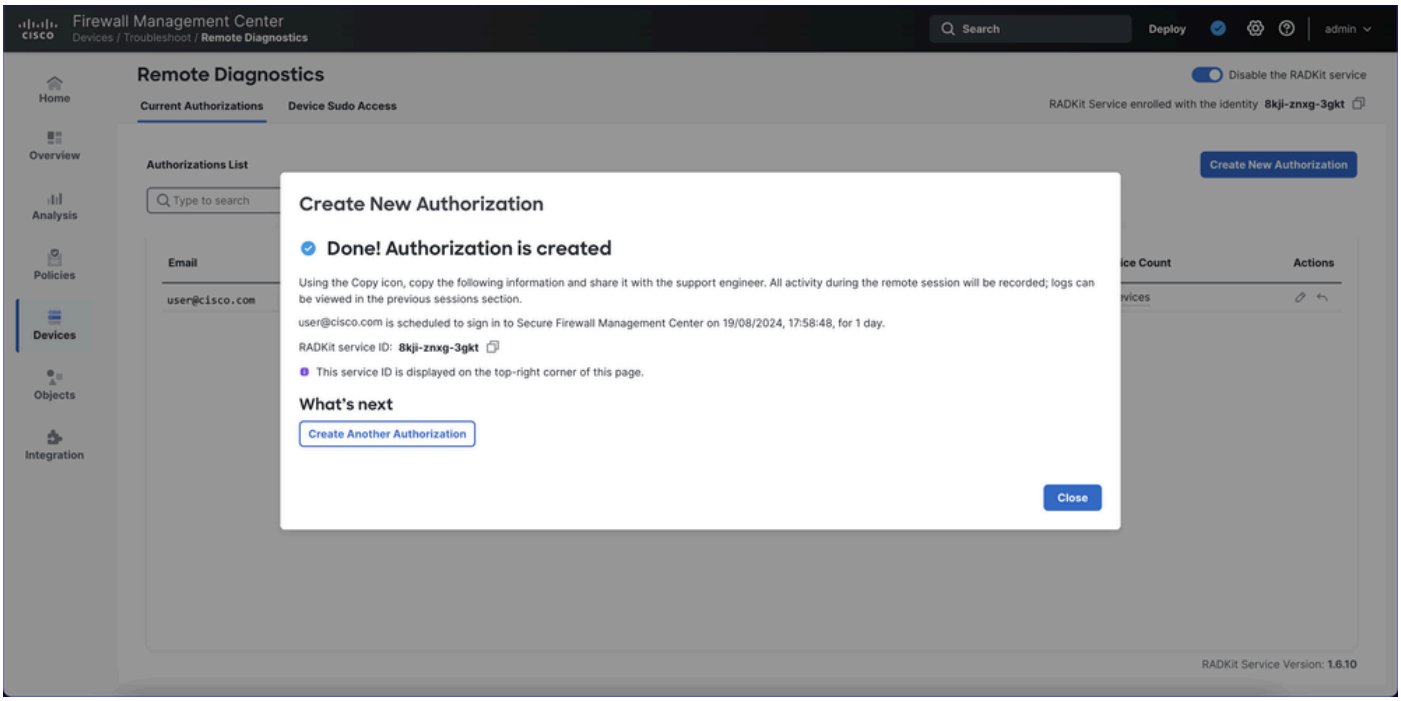
Neue Autorisierungsübersicht erstellen

Der letzte Schritt ist die Autorisierungszusammenfassung. Hier kann der Benutzer die Konfiguration überprüfen und bearbeiten.



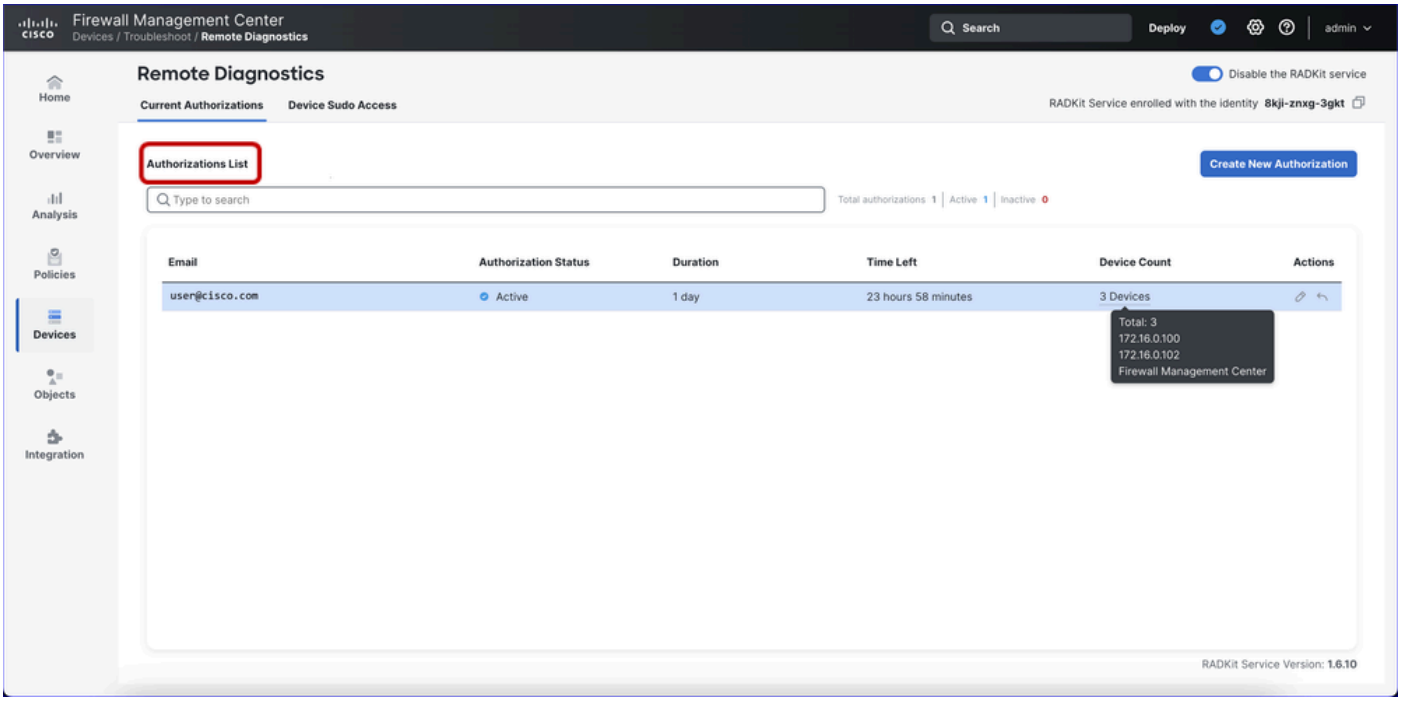
Neue Autorisierung erstellen abgeschlossen

Nach Abschluss der Autorisierungserstellung wird ein Bestätigungsbildschirm angezeigt:



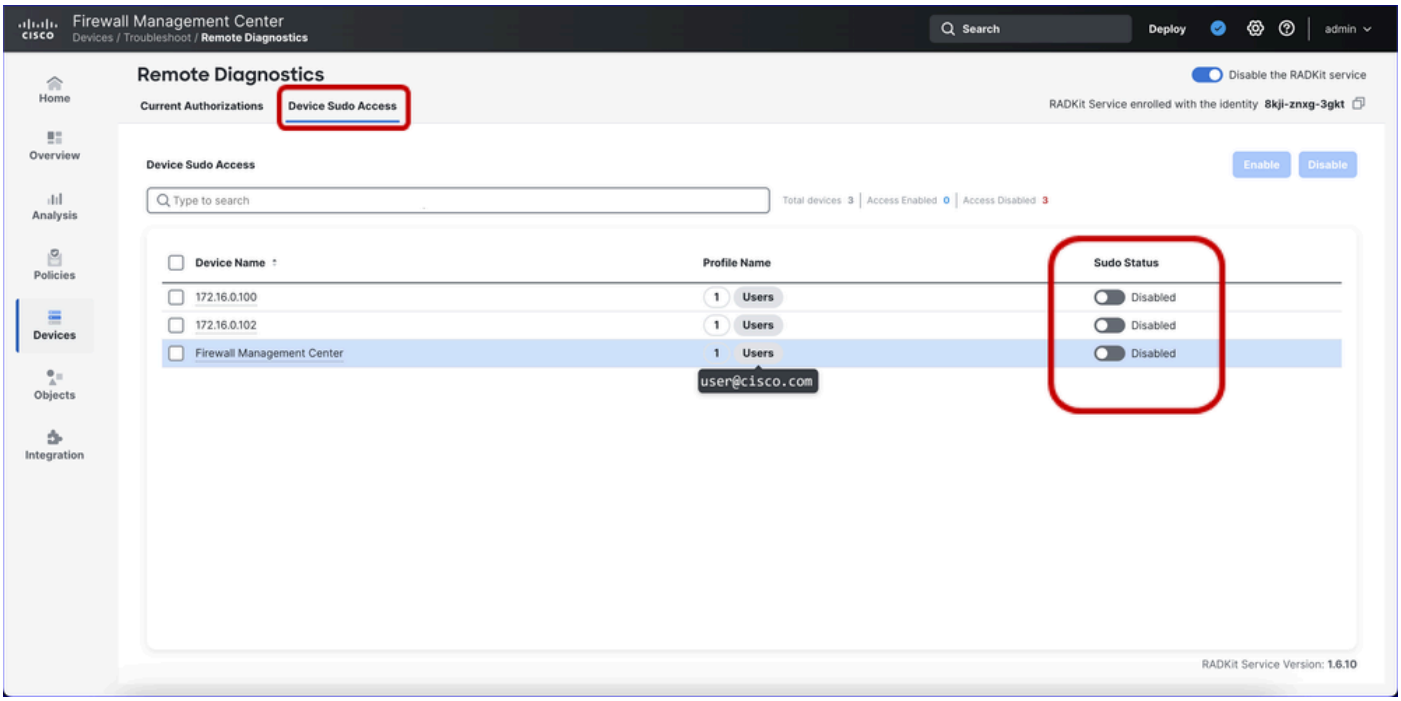
Liste der aktuellen Autorisierungen, einschließlich Widerruf

- Die Liste der aktuellen Autorisierungen wird auf der Registerkarte Aktuelle Autorisierungen angezeigt.
- Die Aktionen (Spalte ganz rechts) sind Zugriff widerrufen und Berechtigung bearbeiten.



Sudo-Zugriffsliste für Geräte

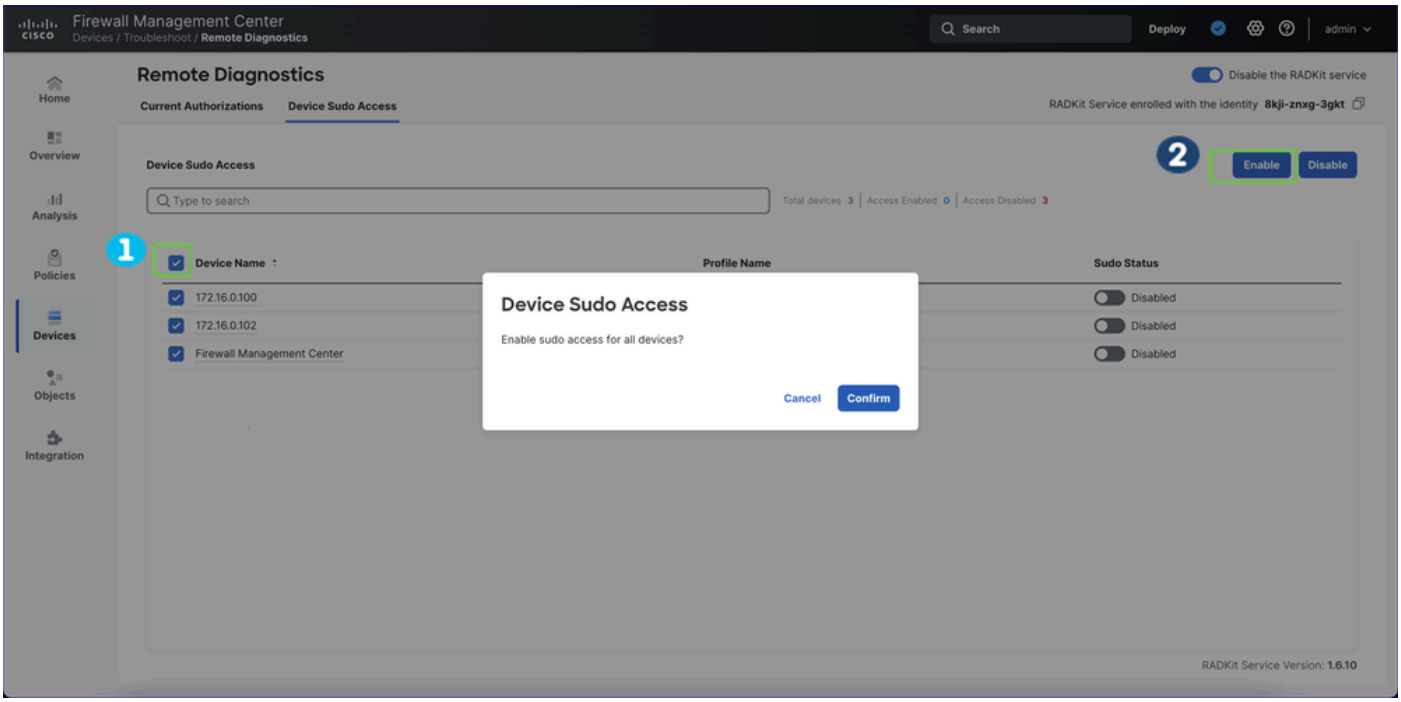
- Die Liste der Geräte mit Sudo-Zugriffseinstellungen wird auf der Registerkarte Geräte-Sudo-Zugriff angezeigt.
- Verwenden Sie den Umschalter in der rechten Spalte, um den Sudozugriff einzuschalten. Standardmäßig ist diese Option deaktiviert.
- Darüber hinaus steht ein Sudo-Bulk-Enable/Disable-Zugriff zur Verfügung.



Aktivieren von Geräten für den Sudo-Zugriff bestätigen

1. Der Sudo-Zugriff kann für alle oder nur für bestimmte Geräte aktiviert werden, indem Sie die Geräte auswählen und dann auf die Schaltfläche "Aktivieren" klicken.

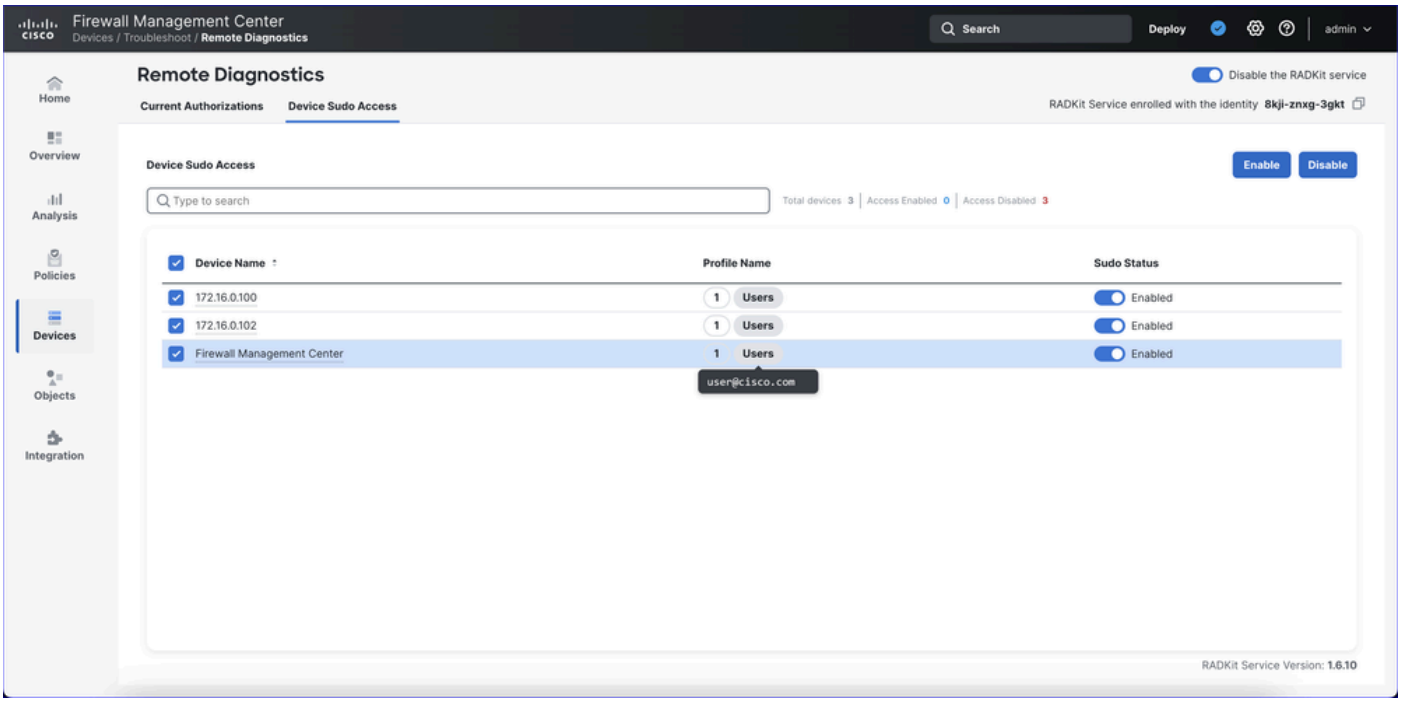
2. Bei der Aktivierung erscheint ein Bestätigungsdialogfeld, und Sie müssen auf Bestätigen klicken.



Geräte Sudo-Zugriff aktiviert

- Nach dem Aktivieren oder Deaktivieren des Sudo-Zugriffs für ein Gerät wird die Spalte Sudo-Status rechts auf der Seite aktualisiert.

- Der Support-Techniker kann sudo su auf dem Gerät ausführen. ist passwortlos. Der Support-Techniker muss nicht über das Root-Kennwort verfügen.



Weitere Hinweise

- Nur Geräte in der Domäne, auf die der FMC-Benutzer Zugriff hat, sind sichtbar und können für den Remote-Zugriff autorisiert werden.
- Wenn FMCs in HA vorhanden sind:
  - Der RADKit-Dienst kann nur auf dem Active/Primary aktiviert werden.
  - Das sekundäre FMC kann derzeit nicht als Gerät hinzugefügt werden, auf das vom RADKit-Client zugegriffen werden kann.
- Die Autorisierung kann jeweils nur für einen Support-Techniker erfolgen.
  - Wenn Sie für den Zugriff einen weiteren Supporttechniker benötigen, erstellen Sie eine weitere Autorisierung für den weiteren Techniker. Die Dienst-ID ist die gleiche.

FMC REST-APIs

RADKit Service REST APIs

Zur Unterstützung der Erstellung und des Lesens von RADKit Service wurden die folgenden neuen URLs eingeführt:

- ABRUFEN: /api/fmc_troubleshoot/v1/domain/{domainUUID}/radkit/services
  - Ruft alle RADKit Service-Daten vom FMC ab.
- ABRUFEN: /api/fmc_troubleshoot/v1/domain/{domainUUID}/radkit/services/{id}
  - Ruft die RADKit Service-Daten von der angegebenen ID ab bzw. ruft sie ab.
- POST: /api/fmc_troubleshoot/v1/domain/{domainUUID}/radkit/services
  - Erstellt den RADKit-Dienst auf dem FMC (aktiviert/deaktiviert den Dienst).

RADKit-Servicemodell

Das RADKit-Servicemodell besteht aus:

- typ
- ID
- status
- ist angemeldet
- DienstID
- version


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


Cisco Support: RADKit-Client-Verwendung

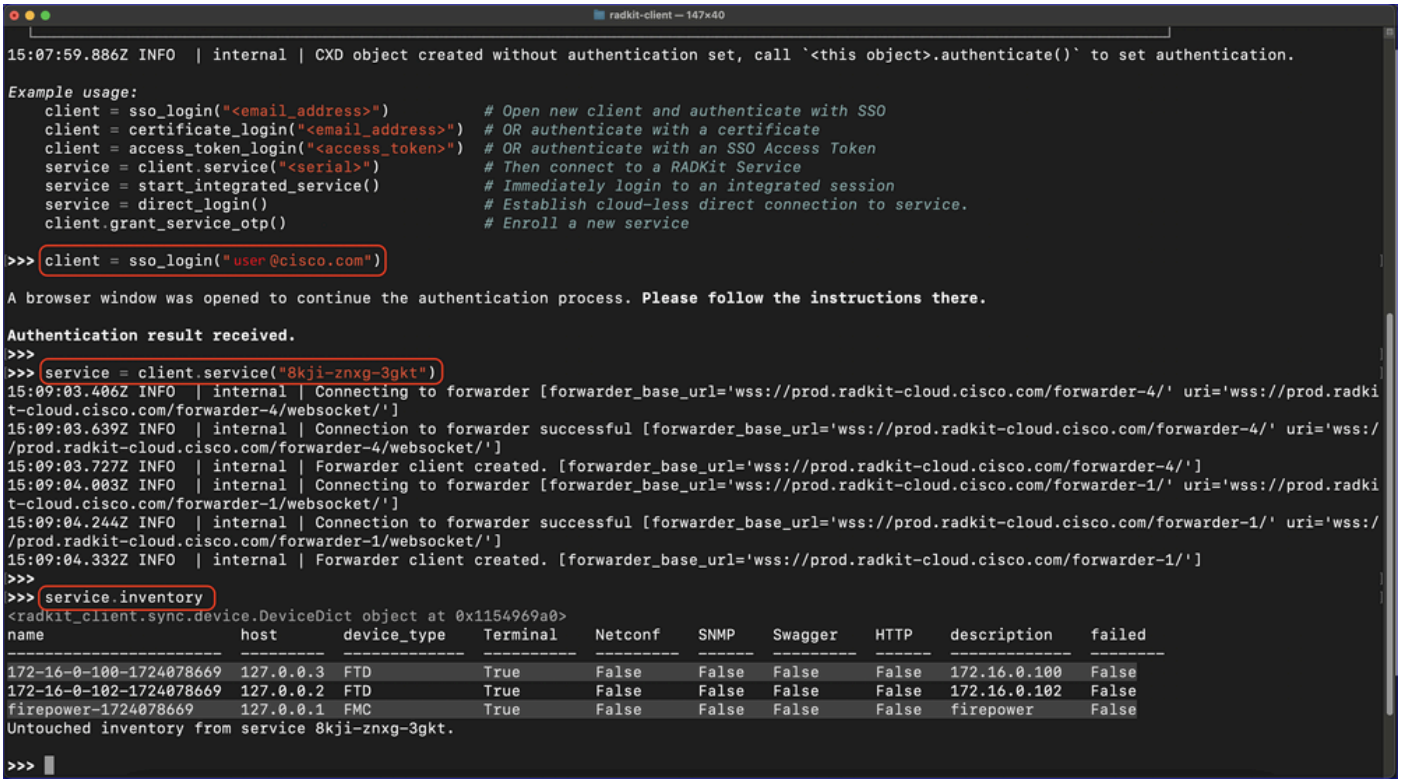
Support: RADKit-Client installieren

- Um auf FMC/FTD(s) zugreifen zu können, muss der Support den RADKit-Client installiert haben.
  - Der Client funktioniert mit Windows-, Mac- und Linux-Betriebssystemen.
- Der Support kann von mehreren Benutzern auf mehrere Geräte zugreifen. Jede RADKit-Autorisierung verfügt über einen eigenen "Bestand" an Geräten.
  - Für jeden Benutzer, auf den der Support zugreifen möchte, wird die RADKit-Service-ID benötigt.
  - Bei einem einzigen Bestand ist der Zugriff sowohl für das FMC als auch für die von ihm verwalteten FTDs vom RADKit-Client möglich, wie vom Benutzer bei der Zugangsberechtigung festgelegt.

RADKit-Client beziehen und installieren

Der RADKit-Client kann lokal von https://radkit.cisco.com/downloads/release/ installiert werden und dann vom Terminal mit dem folgenden Befehl gestartet werden: Radkit-Client

Installationsprogramme sind für Windows, MacOS und Linux verfügbar.



RADKit-Client-Screenshot mit Anmeldebefehlen (Details im nächsten Abschnitt).

RADKit-Client-Anmeldebefehle

- Verwenden Sie die E-Mail-Adresse, die der Benutzer bei der Autorisierung in FMC eingegeben hat.
- Der RADKit-Client meldet sich an und stellt eine Verbindung zu den angegebenen Service-ID-Befehlen her. Die RADKit-Dienst-ID, in diesem Beispiel 8abc-znxg-3abc, muss mit der ID übereinstimmen, die der Firewall-Administrator in FMC sieht.

<#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
```

RADKit Client Service Inventory-Befehl

Befehl zum Auflisten des Bestands, auf den der Remote-Benutzer (Cisco TAC-Techniker) zugreifen darf:

```
<#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.
```

Es gibt einen Filterbefehl für die Geräte im Inventar (nächster Abschnitt). Verwenden Sie den Namen in der linken Spalte, um eine interaktive Sitzung mit dem Gerät zu starten (Befehl im nächsten Abschnitt).

Tipp: Wenn der Bestand veraltet ist, können Sie ihn mit dem folgenden Befehl aktualisieren: **>>** service.update_Inventory()

RADKit-Client: Geräte filtern

Befehl zum Filtern von Geräten im Bestand:

```
<#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.
```

Interaktiver Sitzungsbefehl für RADKit-Client-Gerät

Starten einer interaktiven Sitzung für ein Gerät (in diesem Fall ein FMC) mit dem Namen "firepower-1724078669", der aus dem vorherigen Befehl "service.Inventory" stammt:

<#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-Client Befehle auf Geräten ausführen

Führen Sie die Befehle auf den Geräten aus!

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

Weitere Gerätedetails

In Anbetracht dieser Bestandsaufnahme:

<#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
```

So erhalten Sie Details zur Version von FTD-Geräten:

<#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
```

```
--------------------------------------------------

>
```

Alternativer Ansatz:

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

Abrufen von Dateien von Geräten

- Über den RADKit-Client kann ein Cisco TAC-Techniker per SSH Verbindungen zu Geräten herstellen und verschiedene Vorgänge durchführen, darunter das Generieren von Problembehebungsdateien.

Cisco Support: RADKit-Konsole

Verwenden der RADKit-Netzwerkkonsole

- Alternativ zur Verwendung des RADKit-Client kann ein Cisco TAC-Supporttechniker die RADKit-Netzwerkkonsole verwenden. Die Netzwerkkonsole ist Teil des RADKit-Clients.
- Die RADKit-Netzwerkkonsole ist eine Funktion, die eine einfache Befehlszeilenschnittstelle (CLI) für grundlegende RADKit-Clientfunktionen bereitstellt. Es ist für eine schnelle Konnektivität mit einer RADKit Service-Instanz, die Einrichtung interaktiver Sitzungen und das problemlose Herunterladen/Hochladen von Dateien und minimalen Schulungen vorgesehen.
- Starten Sie die Netzwerkkonsole über die Befehlszeile: radkit-netzwerkkonsole
- Weitere Informationen finden Sie in der RADKit-Dokumentation.

Upgrade- und Abwärtskompatibilität

Upgrade auf 7.7 und 7.7 oder höher

- RADKit Service wurde in Secure Firewall 7.7.0 hinzugefügt.
    - Geräte, die auf Version 7.7.0+ aktualisiert werden, verfügen über die erforderliche Konfiguration für den RADKit-Dienst.

Erfahrungen mit nicht unterstützten FTDs

- FMCs und FTDs müssen die Mindestversion 7.7.0 aufweisen, damit diese Funktion verwendet werden kann (FTDs mit einer niedrigeren Version als 7.7 können einer RADKit-Autorisierung für 7.7 FMC nicht hinzugefügt werden).
- Registrierte FTDs, die nicht unter 7.7.0 aufgeführt sind, können nicht zur Genehmigung ausgewählt werden.

Fehlerbehebung

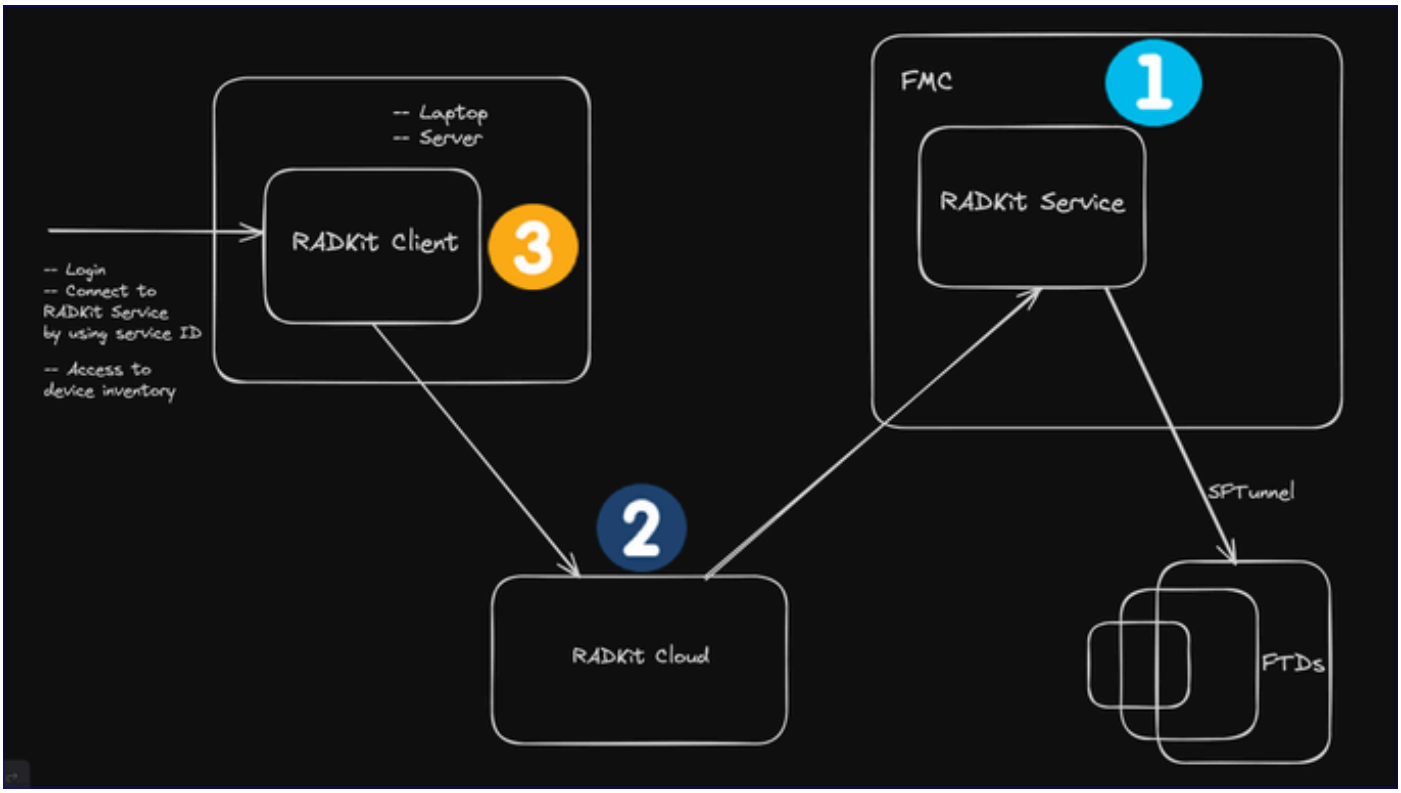
Diagnoseübersicht

Fehlerbehebung:

1. Verwenden Sie Browser Development Tools und FMC-Protokolle, um zu sehen, was in FMC passiert.

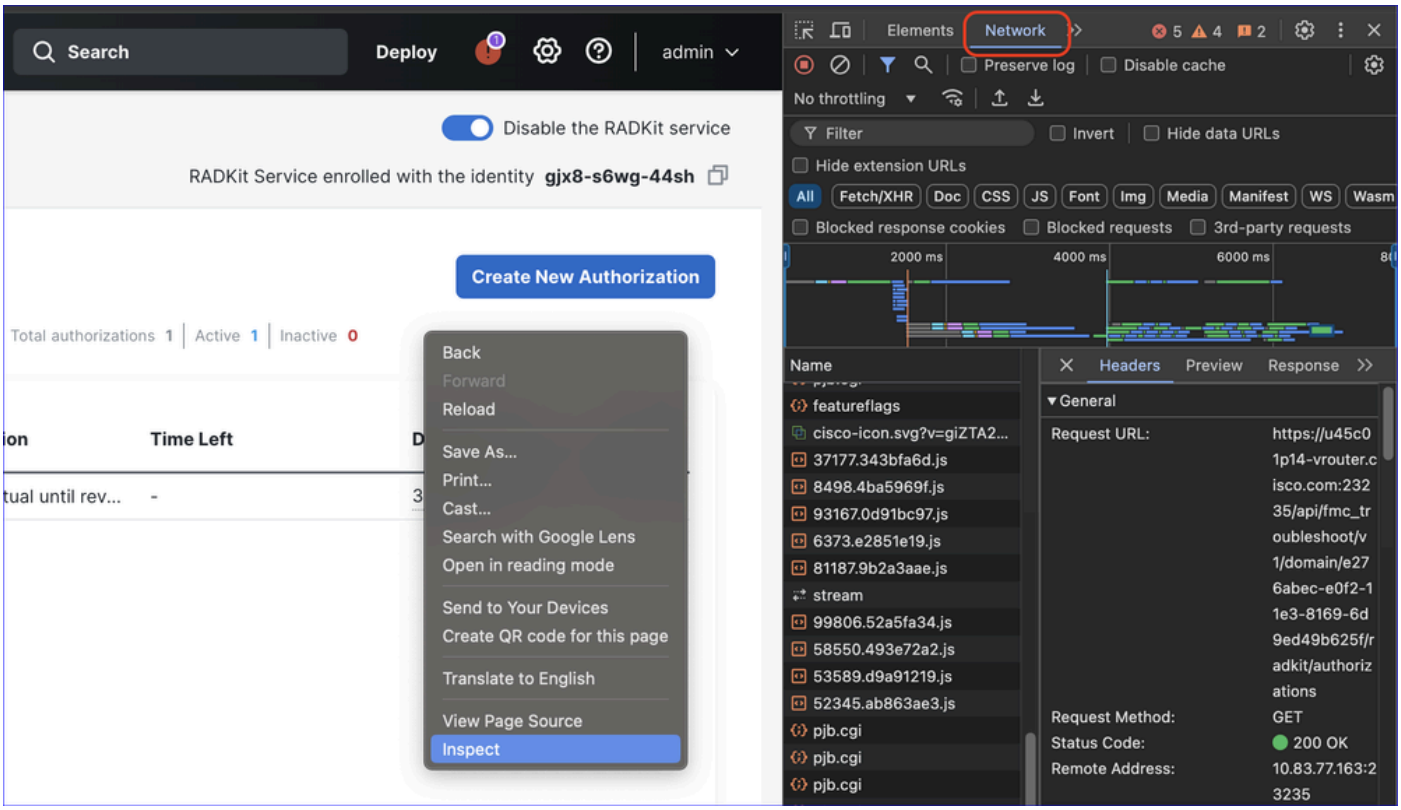
2. Bei Kommunikationsproblemen zwischen RADKit Service auf FMC, RADkit Cloud und RADKit Client schauen Sie in RADKit Client Logging nach.

3. RADKit-Client.



Fehlerbehebung: Browser-Entwicklertools

- Die Registerkarte Developer Tools, Network (Entwicklertools, Netzwerk) des Browsers zeigt die API-Aufrufe an, die auf der Seite ausgeführt wurden. Dies kann zur Fehlerbehebung bei FMC-Problemen verwendet werden. Dies kann durch einen Rechtsklick auf die Seite und dann auf Inspizieren gestartet werden.
- Überprüfen Sie den API-Anrufstatuscode und die Antwortvorschau auf der Registerkarte "Network" (Netzwerk).



RADKit Service Go Middleware APIs

Go Middleware für die RADKit-Integration verwendet API-Aufrufe, die nicht über den FMC API Explorer öffentlich zugänglich sind. Das Protokoll der Go Middleware APIs finden Sie unter /var/log/auth-daemon.log. Zu den Funktionen von Go Middleware gehören:

- Registrieren Sie den RADKit Service in der RADKit Cloud mit Single Sign On Prozess.
- Rufen Sie eine Liste aller RADKit-Remote-Benutzerautorisierungen und der zugehörigen Geräte ab.
- Rufen Sie eine bestimmte Remote-RADKit-Benutzerautorisierung und die zugehörigen Geräte per E-Mail ab.
- Erstellen Sie eine Remote-RADKit-Benutzerautorisierung, und erteilen Sie Zugriffsberechtigungen für Geräte (alle Geräte oder eine Liste ausgewählter Geräte) für einen festgelegten Zeitraum.
- Ändern einer RADKit-Remote-Benutzerautorisierung
- Löschen Sie eine Remote-RADKit-Benutzerautorisierung.

Protokolle zur Fehlerbehebung des RADKit-Dienstes

- Allgemeine FMC-Protokolle: Befehl "pigtail" aus einer FMC SSH-Sitzung aus.
- Go Middleware-APIs: /var/log/auth-daemon.log
- Protokolle, die RADKit und auth-daemon enthalten, verarbeiten Daten:

/var/log/process_stdout.log

/var/log/process_stderr.log

Alle diese Protokolle sind in FMC/FTD-Fehlerbehebungen enthalten.

- Interne RADKit-Dienstprotokolle: /var/lib/radkit/logs/service/
- Protokolle für die vom RADKit-Client auf Geräten (FMCs und FTDs) ausgeführten Vorgänge: /var/lib/radkit/session_logs/service

Protokolle für Übermittlung an Cisco TAC

- Screenshots von Fehlern.
- Beschreibung des Problems
- Schritte zur Reproduktion.
- Pigtail und /var/log/auth-daemon.log Log-Extrakte mit den Fehlern.

Überwachung des Zugriffs

Die Protokollierung der Zugriffsberechtigungen für die Dauer und der Zugriffsberechtigungen finden Sie in den FMC-Audit-Protokollen.

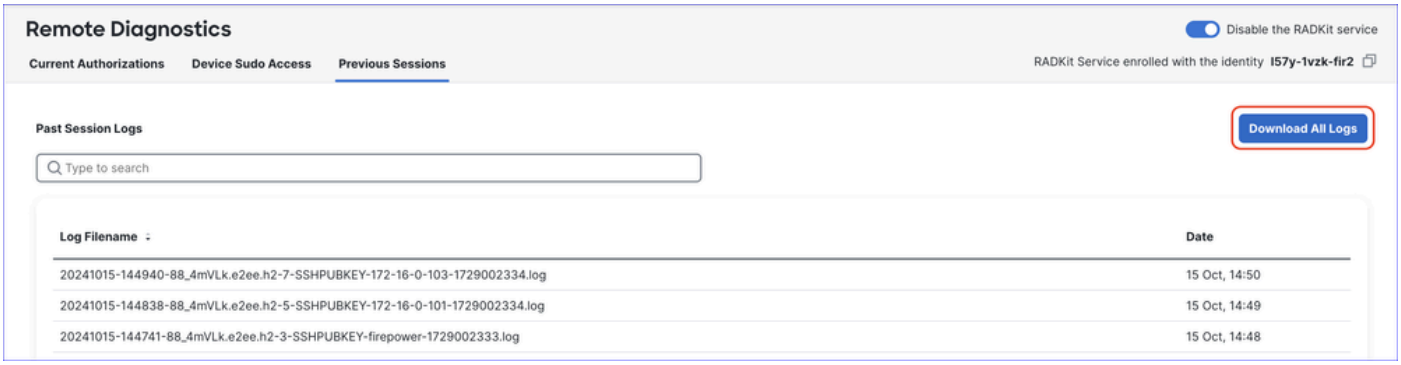
RADKit-Sitzungsprotokolle

RADKit-Sitzungsprotokolle für die vom RADKit-Client an Geräten (FMCs und FTDs) ausgeführten Vorgänge sind auf FMC unter /var/lib/radkit/session_logs/service:

- Die Protokolle stammen vom RADKit-Dienst selbst.
- Diese Protokolle sind in einem Fehlerbehebungspaket enthalten.
- Auf die Protokolle kann auch über die Benutzeroberfläche zugegriffen werden (siehe nächster Abschnitt).
- Es sind mehrere Sitzungsprotokolldateien vorhanden. eine pro Sitzung.

Protokolle der vorherigen RADKit-Sitzungen

Die RADKit-Sitzungsprotokolle für die vom RADKit-Client ausgeführten Gerätevorgänge stehen als Archiv mit allen Protokollen auf der Registerkarte "Previous Sessions" (Vorherige Sitzungen) zum Download zur Verfügung. Klicken Sie dazu auf die Schaltfläche "Alle Protokolle herunterladen".



Beispielproblem bei der Fehlerbehebung - exemplarische Vorgehensweise

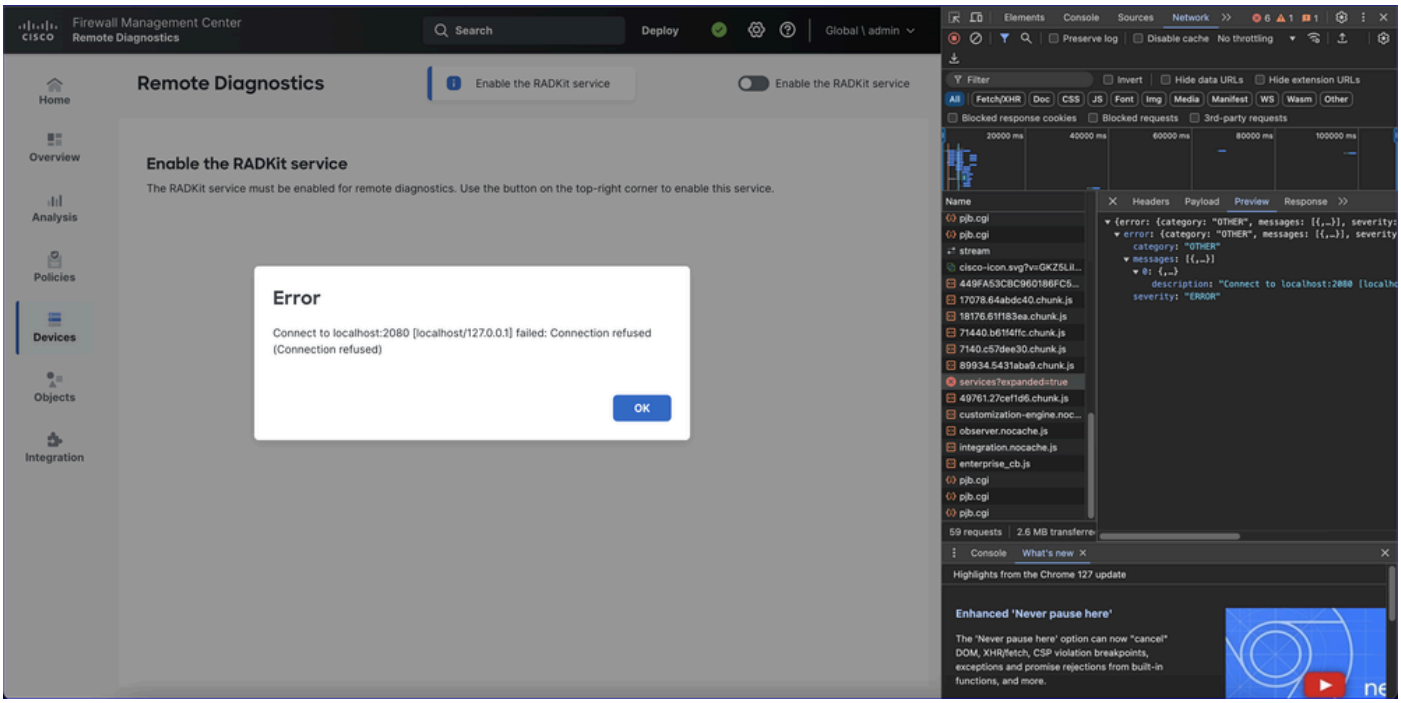
Beispiel für Fehlerbehebung

Falls ein Fehler wie "Connect to localhost:2080 [localhost/127.0.0.1] fehlgeschlagen ist: Verbindung verweigert (Verbindung verweigert)", versuchen Sie, den auth-daemon von einer FMC SSH-Sitzung neu zu starten:

<#root>

root@firepower:~$

sudo pmtool restartbyid auth-daemon



Telemetrie

Die Telemetriedaten wurden für diese Funktion hinzugefügt:

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

Häufig gestellte Fragen

Häufig gestellte Fragen: Anmeldung

Frage: Funktioniert die Registrierung mit dem Proxy, wenn FMC keinen direkten Internetzugang hat?

A. Ja, wenn der Proxy Zugriff auf prod.radkit-cloud.cisco.com hat, die für den Registrierungsprozess verwendet wird.

Frage: Kann ein Benutzer seine eigene IDp für diesen Dienst verwenden?

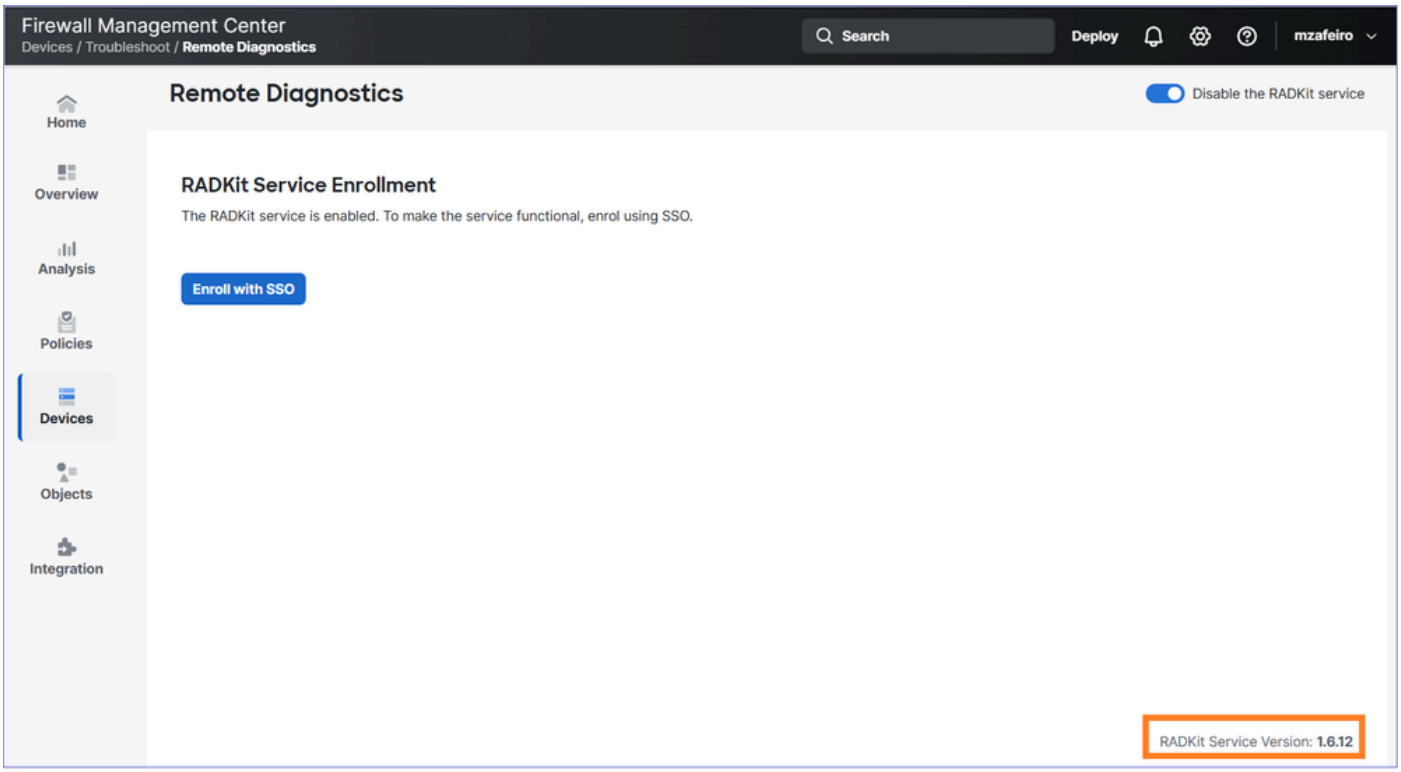
Antwort: In der RADKit-Cloud wird nur Cisco SSO akzeptiert. Es besteht die Möglichkeit, Ihr Firmenkonto mit einem Cisco Konto zu verknüpfen, sodass die RADKit-Service-Anmeldung mit einer E-Mail möglich ist, die nicht von Cisco stammt.

Häufig gestellte Fragen: RADKit-Versionen

Frage: Welche Version von RADkit ist in FMC in Version 7.7 enthalten? Wie können wir wissen, welche Version von RADKit in FMC enthalten ist? Kann das ohne FMC-Upgrade aktualisiert werden?

Antwort:

- Die im Lieferumfang von 7.7.0 enthaltene Version von RADKit ist 1.6.12.
- Die Version des RADKit-Service wird unten auf der Seite FMC Remote Diagnostics (FMC-Ferndiagnose) angezeigt: "RADKit Service Version: 1.6.12



- RADKit ist im Paket mit FMC Upgrade-Paketen/Hotfixes. Ein separates Upgrade des RADKit-Dienstes in FMC wird nicht unterstützt.

Häufig gestellte Fragen: Andere

Frage: Könnten externe Geräte - die nicht vom FMC verwaltet werden - einbezogen werden?

Antwort: Nur vom FMC verwaltete Geräte können dem RADKit-Inventar hinzugefügt werden. Der Zugriff ist dann über eine Autorisierung möglich.

Frage: Wird die RADKit-Konfiguration als Teil des FMC-Backups gesichert?

Antwort:

- Die Konfiguration wird nicht als Teil des FMC-Backups gesichert.
- Es wird nicht gesichert, da wir davon ausgehen, dass kein unbefristeter Zugriff gewährt wird. der Zugriff ist in der Regel nur für eine begrenzte Zeit möglich.

Referenzen

Nützliche Links:

- FMC Konfigurationsanleitung - RADKit
- https://radkit.cisco.com/
- https://radkit.cisco.com/docs/index.html
- https://radkit.cisco.com/downloads/release/

- https://github.com/Cisco-RADKit/Intro

Informationen zu dieser Übersetzung

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