Configuración de la integración de Cisco RADKit en FMC

Contenido

Introducción

Este documento describe la función Cisco RADKit Integration in FMC agregada en la versión 7.7.

Background

Problema al que se enfrentan los administradores de firewall

- El Remote Automation Development Kit (RADKit), desarrollado por Cisco, es un orquestador de toda la red diseñado para ofrecer a los usuarios la posibilidad de acceder de forma segura y solucionar problemas de los dispositivos de red. https://radkit.cisco.com/
- Cisco Secure Firewall Management Center (FMC) gestiona y gestiona los dispositivos de defensa frente a amenazas de firewall (FTD). Un solo FMC puede gestionar varios dispositivos en distintas ubicaciones.
- Si bien los usuarios pueden instalar RADKit por separado y a bordo de sus CSP y FTD en él, la integración del servicio RADKit en el CSP y la integración automatizada de los CSP y todos los dispositivos gestionados (FTD) sería una mejor experiencia para los usuarios finales.

caso de uso

Algunas de las capacidades clave de las que se podrían beneficiar los usuarios tras integrar RADKit en el CSP son:

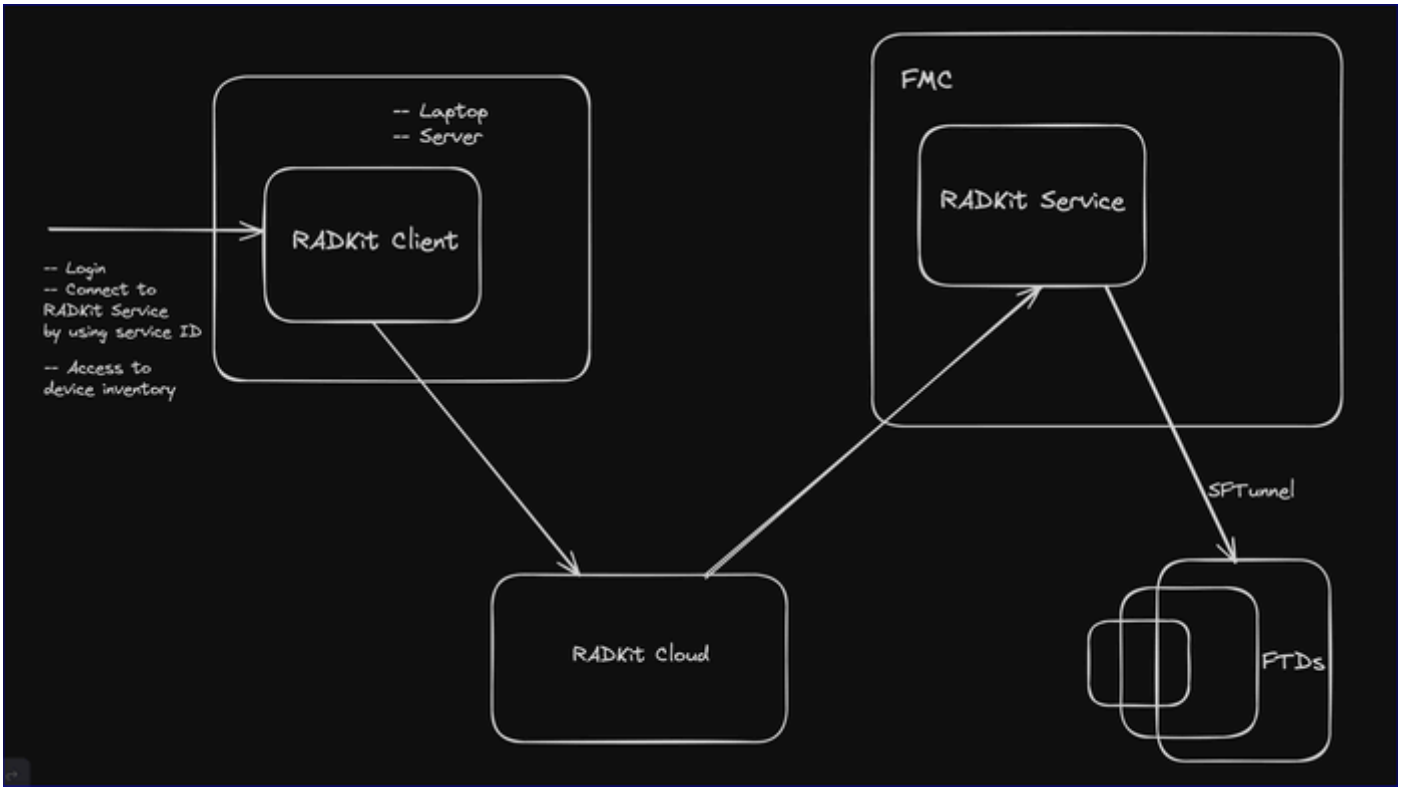
- Posibilidad de acceder a los FMC/FTD de forma remota desde la CLI del cliente RADKit.
- Capacidad para proporcionar acceso controlado a los CSP/FTD a cualquier persona que lo necesite (por ejemplo, un ingeniero del TAC de Cisco).
- Aproveche las capacidades de automatización para recopilar datos y diagnosticar problemas desde el cliente RADKit (los scripts que ejecutan comandos en varios dispositivos se pueden crear y utilizar desde el cliente RADKit).

Novedades: la solución

- A partir de Secure Firewall 7.7.0, el servicio Remote Automation Development Kit (RADKit) está integrado en FMC.
- Los usuarios pueden activar o desactivar el servicio RADKit a demanda, inscribirlo en la nube RADKit y crear autorizaciones de usuarios remotos para acceder a dispositivos específicos desde el cliente RADKit durante un tiempo de acceso programado.
    - Las autorizaciones se pueden editar o revocar.
- También existe la opción de proporcionar a los dispositivos acceso sudo para la resolución de problemas avanzada.

Integración del servicio RADKit en el diagrama FMC

Este diagrama muestra cómo RADKit permite la comunicación desde el cliente RADKit del usuario (ingeniero TAC) a los dispositivos FTD de producción:



Conceptos básicos: Plataformas admitidas, licencias

Aplicaciones y jefes

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		

Otros aspectos de la asistencia

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

Dependencias para que la función funcione

- La versión mínima es Secure Firewall 7.7.0.
- Para conectarse al servicio RADKit alojado en FMC, el cliente RADKit debe instalarse desde https://radkit.cisco.com/downloads/release/ en el equipo del ingeniero de soporte.
- La versión preferida para el cliente RADKit es 1.6.10 o superior.
- Las versiones anteriores de RADKit Client se pueden utilizar ya que el servicio RADKit es compatible con versiones anteriores de RADKit Client.

Descripción de características y tutorial

Descripción general de características

- La integración del servicio RADKit en FMC permite a los administradores de dispositivos proporcionar a los usuarios remotos (ingenieros del TAC de Cisco) acceso a dispositivos FMC y FTD específicos de su red con fines de resolución de problemas y automatización. RADKit es mucho más eficiente para la resolución de problemas que compartir la pantalla, no requiere controlar el ordenador del usuario, es una forma más segura de trabajar en una red y complementa muy bien Webex.
- Esto mejora la experiencia del soporte técnico, ya que los administradores de dispositivos no tienen que instalar y configurar el servicio RADKit por separado. Además, esto reduce el tiempo de soporte para que los ingenieros del Cisco TAC resuelvan los problemas de soporte.

Configuration Steps: Overview

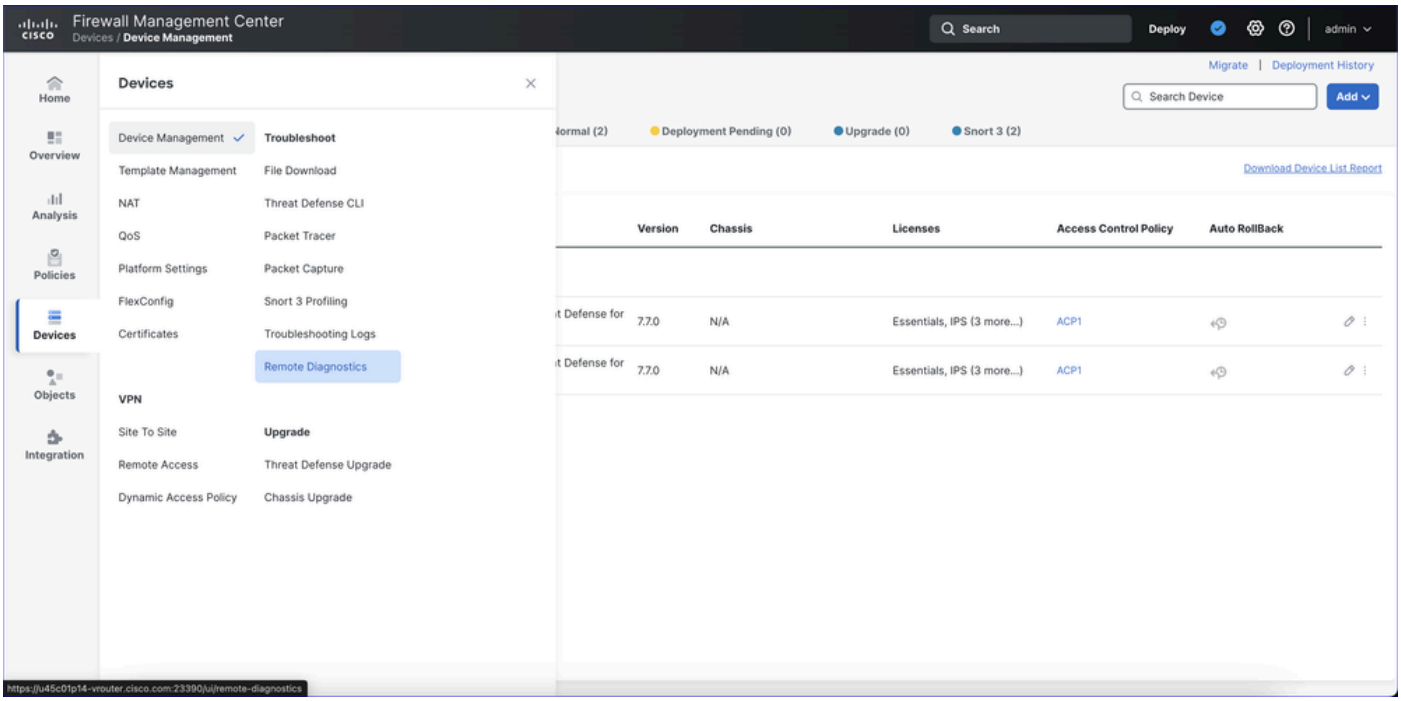
1. Administrador de dispositivos (usuario administrador de FMC): Habilite e inscriba el servicio RADKit y configure las autorizaciones en la GUI de FMC.

2. Asistencia de Cisco TAC/Cisco: Instale el cliente RADKit en su computadora, acceda y resuelva problemas de los dispositivos desde el cliente RADKit.

Usuario administrador de FMC: Firewall Management Center (Tutorial)

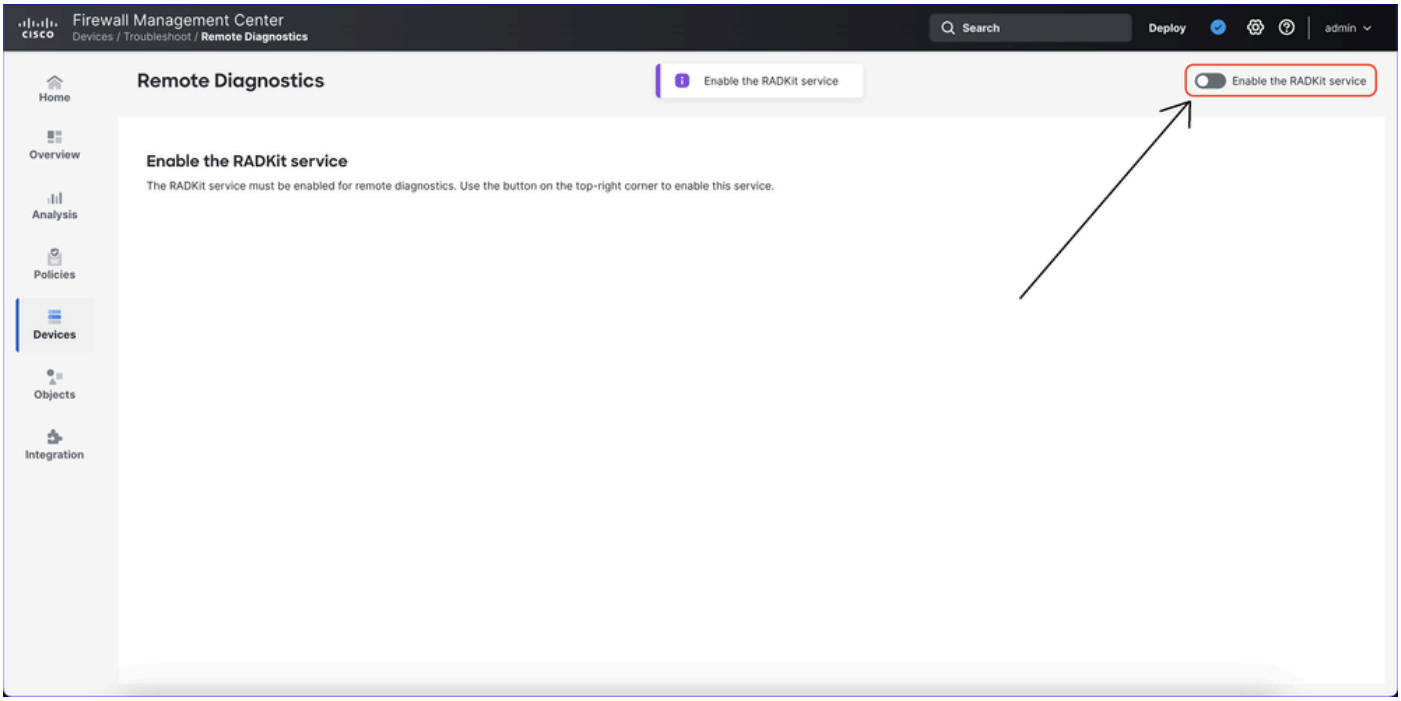
Menú Diagnóstico remoto

- Se ha agregado un nuevo elemento de menú "Diagnóstico remoto" para esta función en Dispositivos -> Solucionar problemas.
- Los usuarios Administrador, Administrador de red y Mantenimiento tienen permisos de lectura y escritura en la página.
- Los usuarios Analista de seguridad, Analista de seguridad (sólo lectura) y Aprobador de seguridad tienen permisos de sólo lectura para la página.



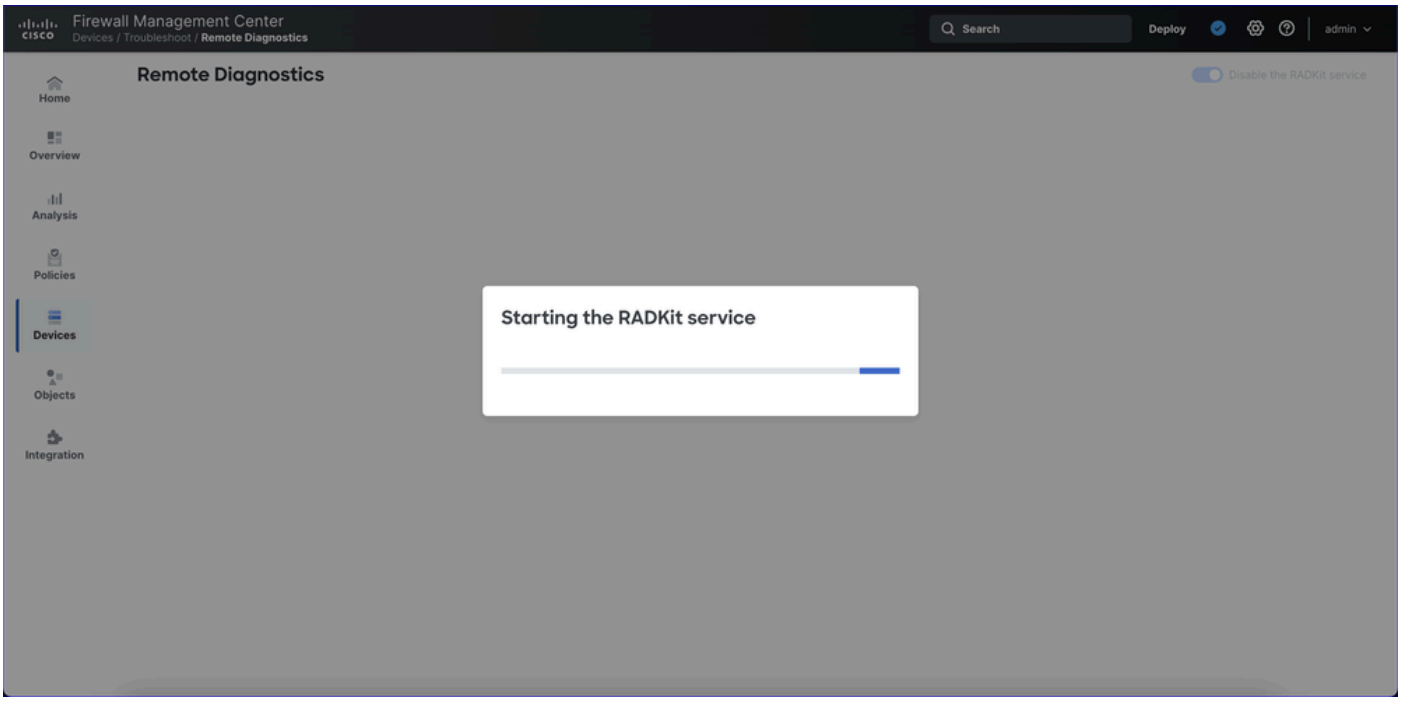
Página Diagnóstico remoto inicial

Esta es la página inicial Diagnóstico remoto. El servicio RADKit se puede habilitar activando el switch "Enable the RADKit service":



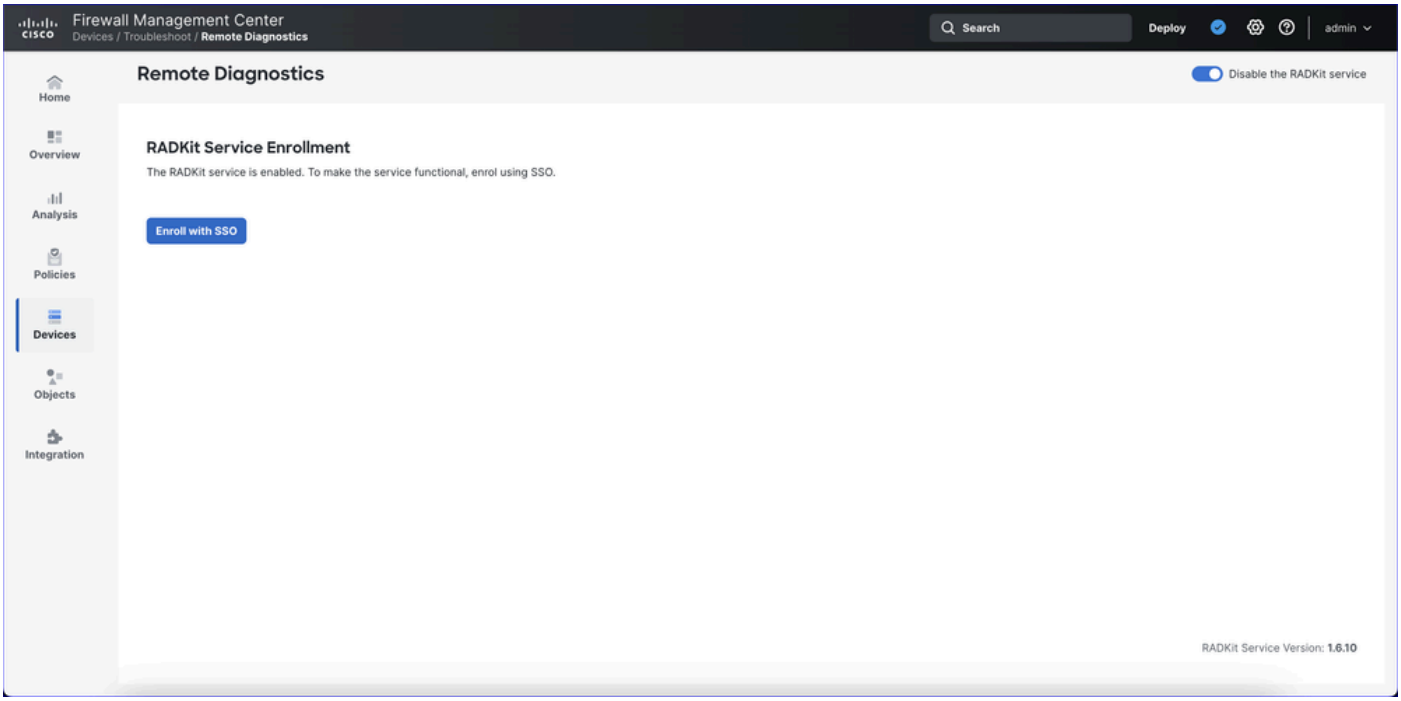
Inicio del servicio RADKit

Después de habilitar el servicio RADKit, aparecerá una barra de progreso hasta que se inicie el servicio RADKit:



Servicio RADKit habilitado

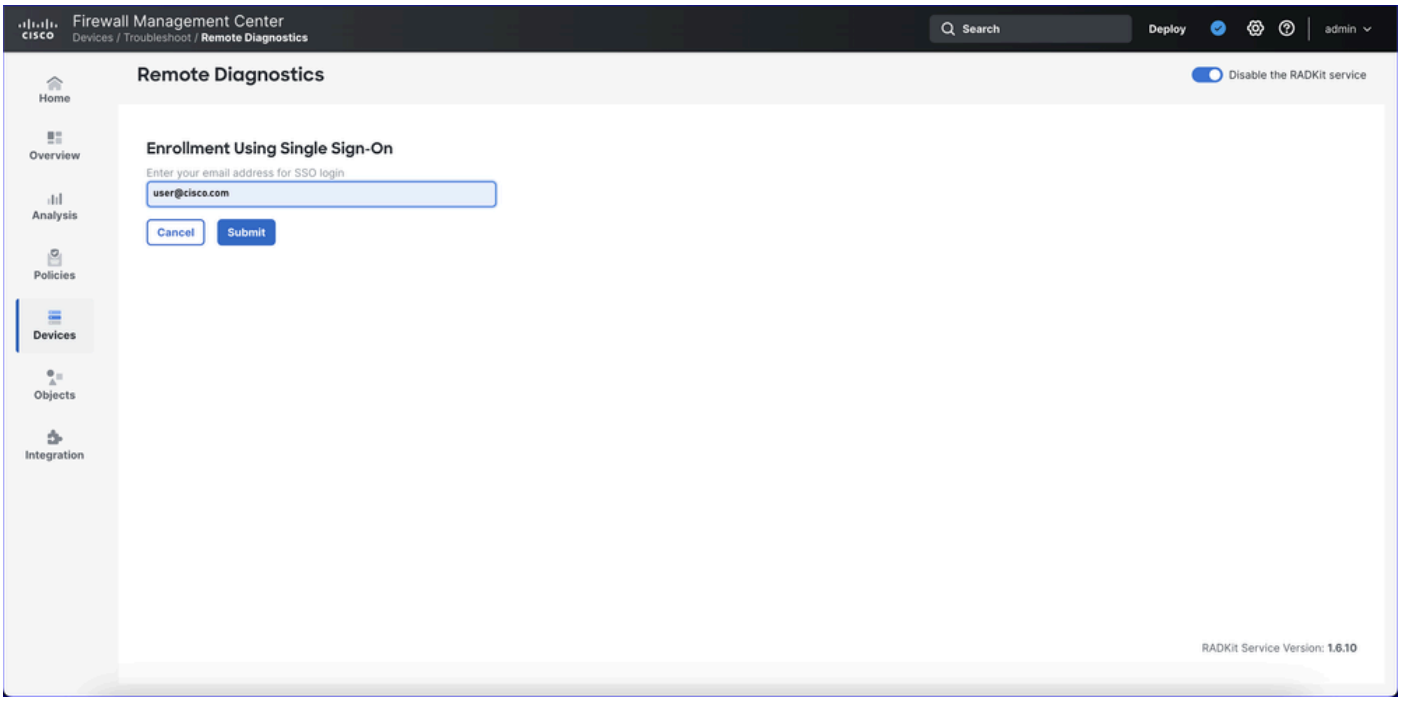
- Cuando se completa el proceso de habilitación del servicio RADKit, se muestra esta página:



El siguiente paso es la inscripción en la nube de RADKit haciendo clic en el botón "Inscribirse con SSO".

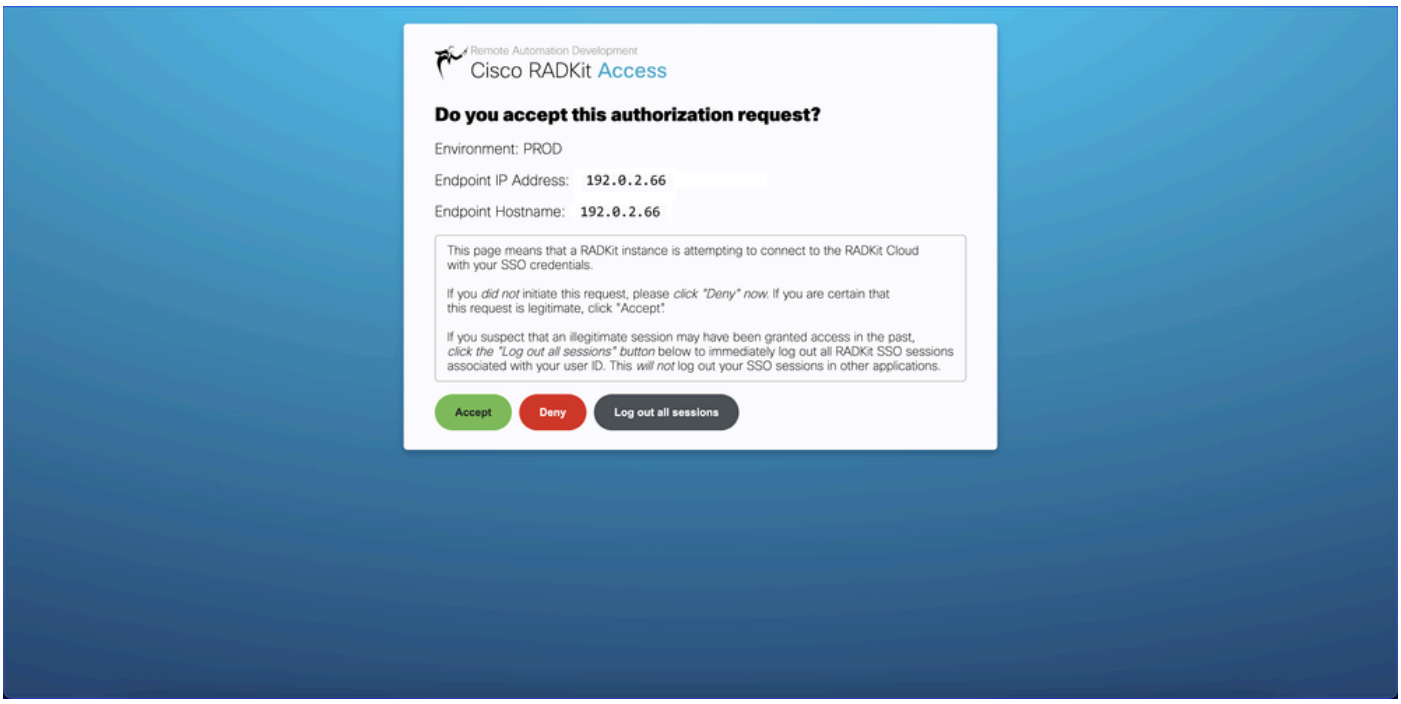
Inscríbase con SSO: introduzca la dirección de correo electrónico

El paso 1 del proceso de inscripción consiste en introducir la dirección de correo electrónico del usuario para la inscripción en la nube de RADKit:



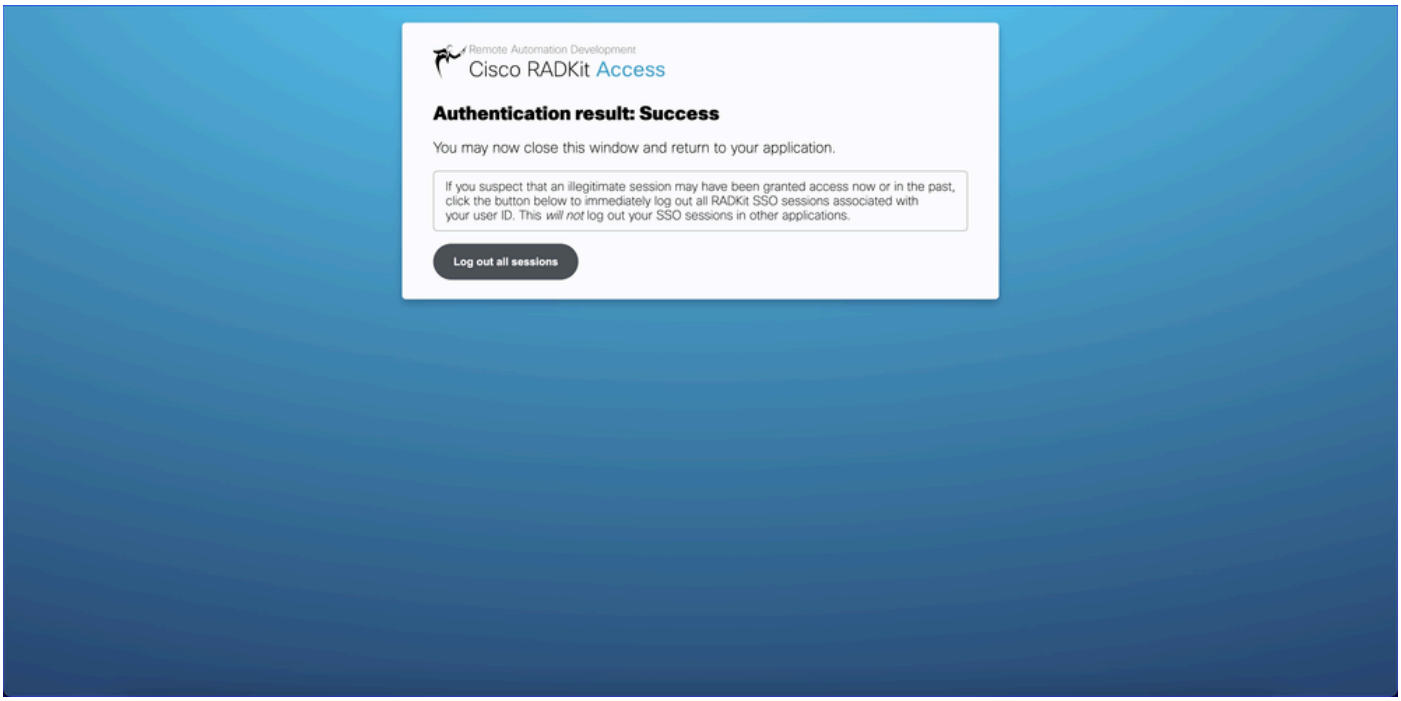
Inscribirse con SSO: aceptar solicitud de autorización

Se abre una nueva ficha (o ventana, según la configuración del explorador). Haga clic en el botón Accept.



Inscríbase con SSO: autenticación satisfactoria

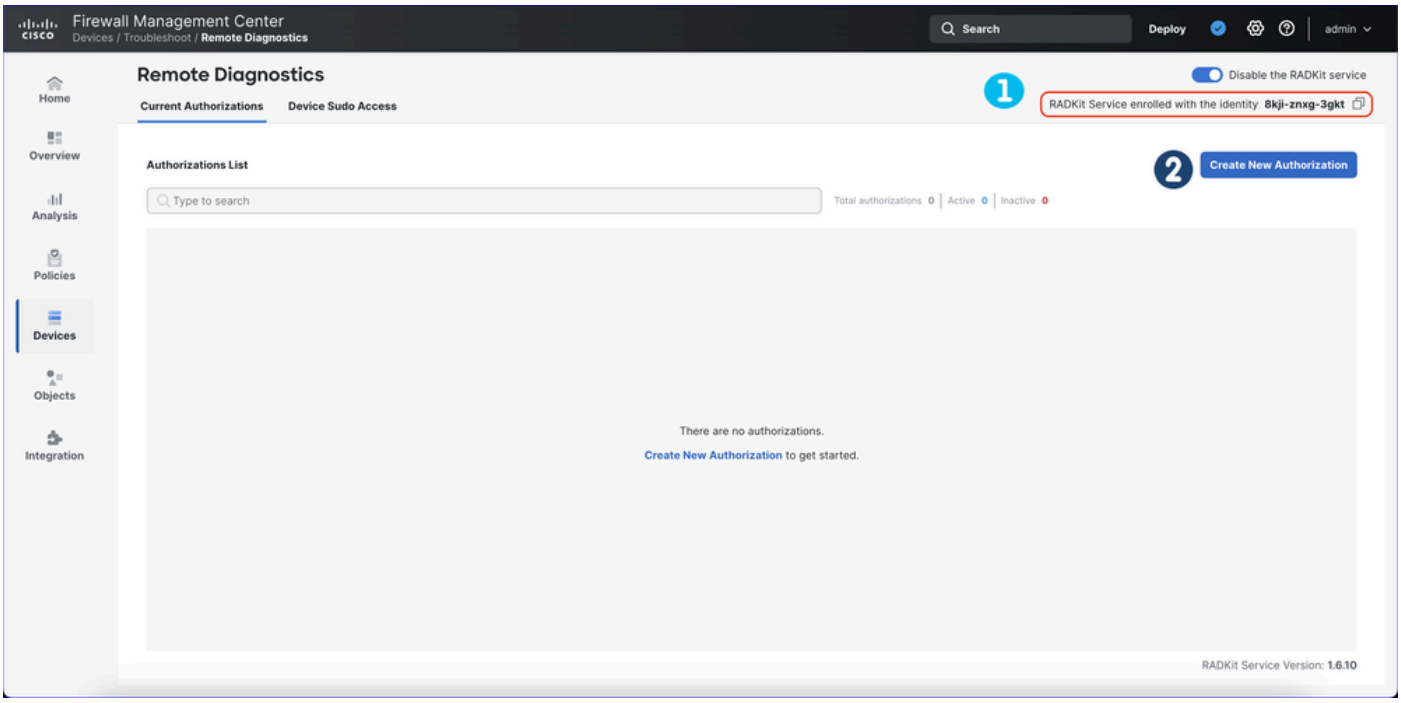
Tras la correcta autenticación, el usuario puede cerrar la ficha del explorador y volver a la página Diagnóstico remoto de FMC.



Servicio RADKit inscrito

El servicio RADKit se inscribe con el ID de servicio especificado (en este ejemplo, el ID es 8kji-znxg-3gkt). La ID. se puede copiar en el portapapeles. Dáselo al ingeniero del TAC de Cisco para que se pueda conectar al servicio RADKit desde el cliente RADKit.

El siguiente paso consiste en crear una autorización haciendo clic en el botón "Crear nueva autorización":

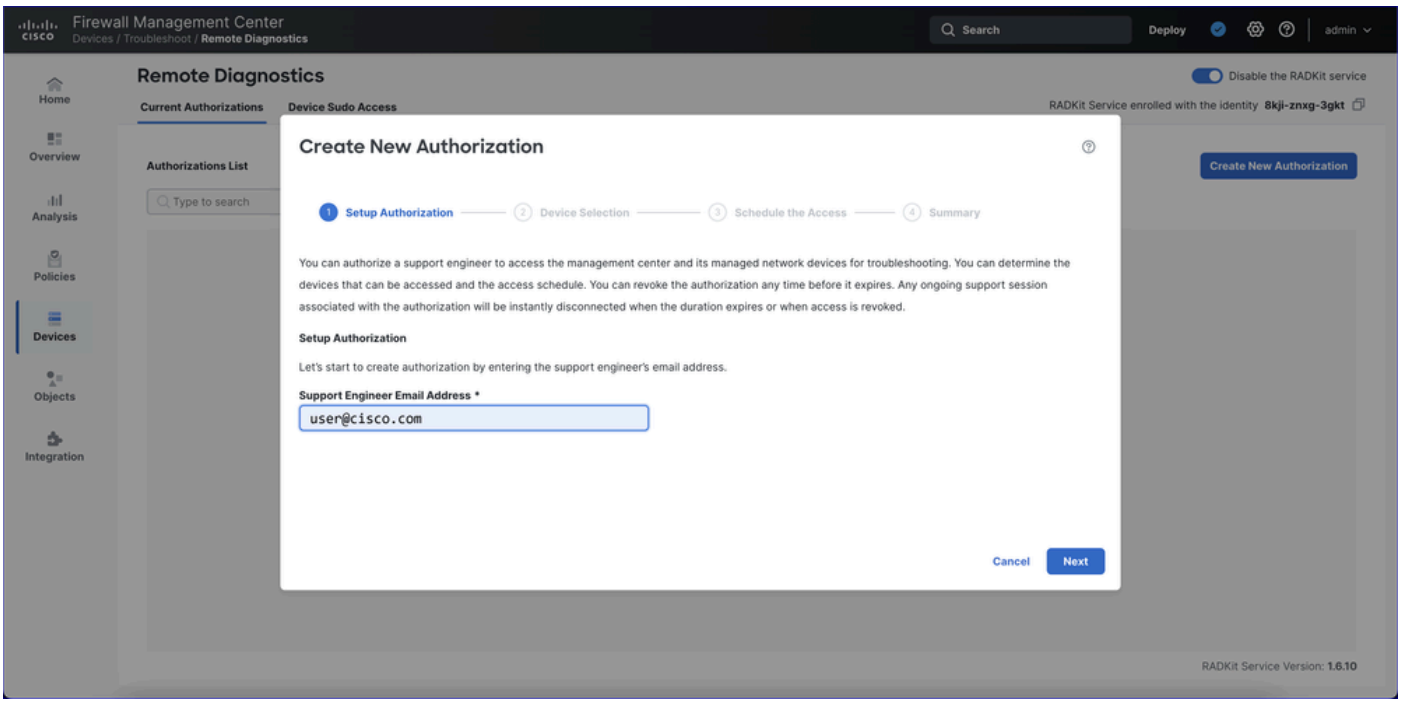


Crear nueva autorización: Paso 1

- Para crear una nueva autorización, el primer paso consiste en agregar la dirección de correo

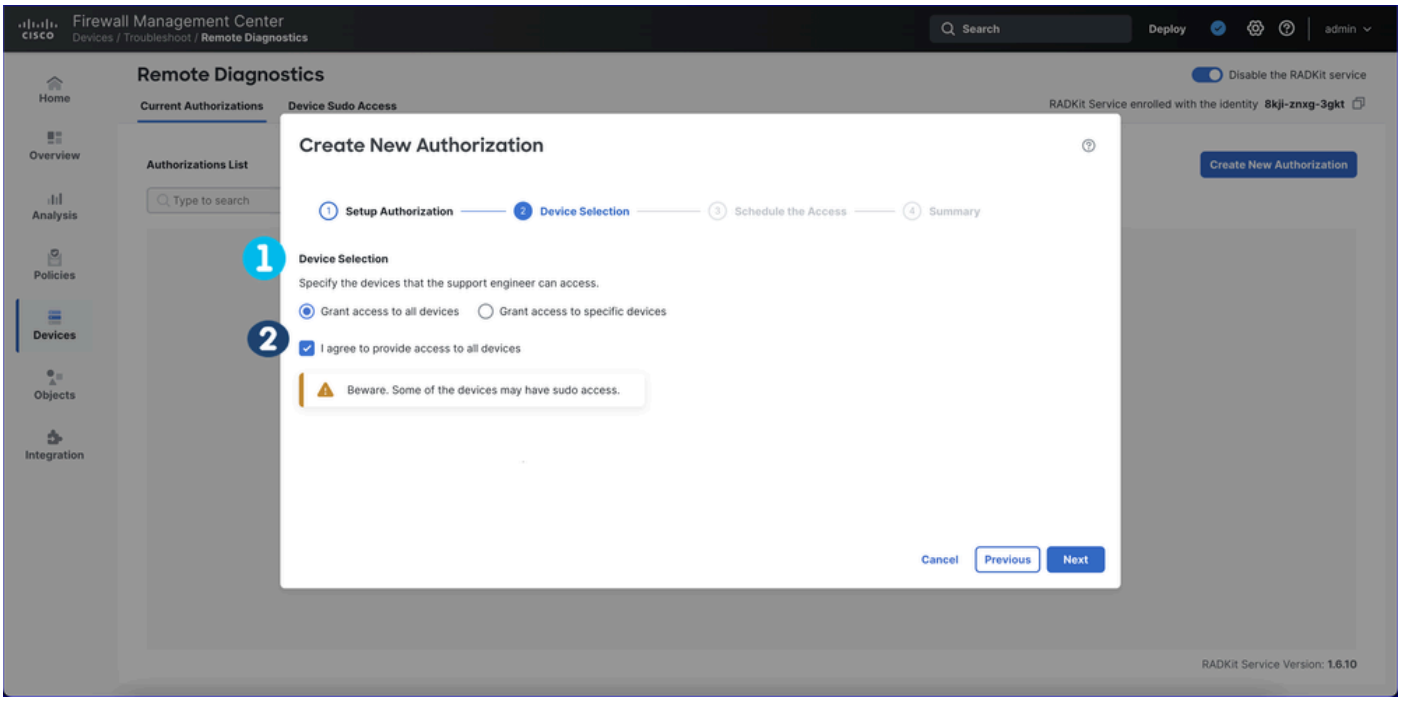
electrónico del ingeniero de soporte técnico.

- Hay cuatro pasos para crear una nueva autorización. El progreso a lo largo de los pasos se muestra en la parte superior.



Crear nueva autorización: Paso 2

- Paso 1: Especifique los dispositivos a los que puede acceder el ingeniero de soporte técnico. O, como en este ejemplo, conceder acceso a todos los dispositivos.
- Paso 2: Compruebe el botón de opción de todos los dispositivos o de dispositivos específicos. Para dispositivos específicos, se pueden seleccionar FMC y/o FTD. Observe la advertencia que el acceso sudo puede proporcionar a algunos dispositivos en la ficha Device Sudo Access . El botón Next no se habilita hasta que se marca la casilla de verificación.
- El acceso Sudo se proporciona por dispositivo en la ficha Device Sudo Access más adelante (no durante la creación de una autorización).

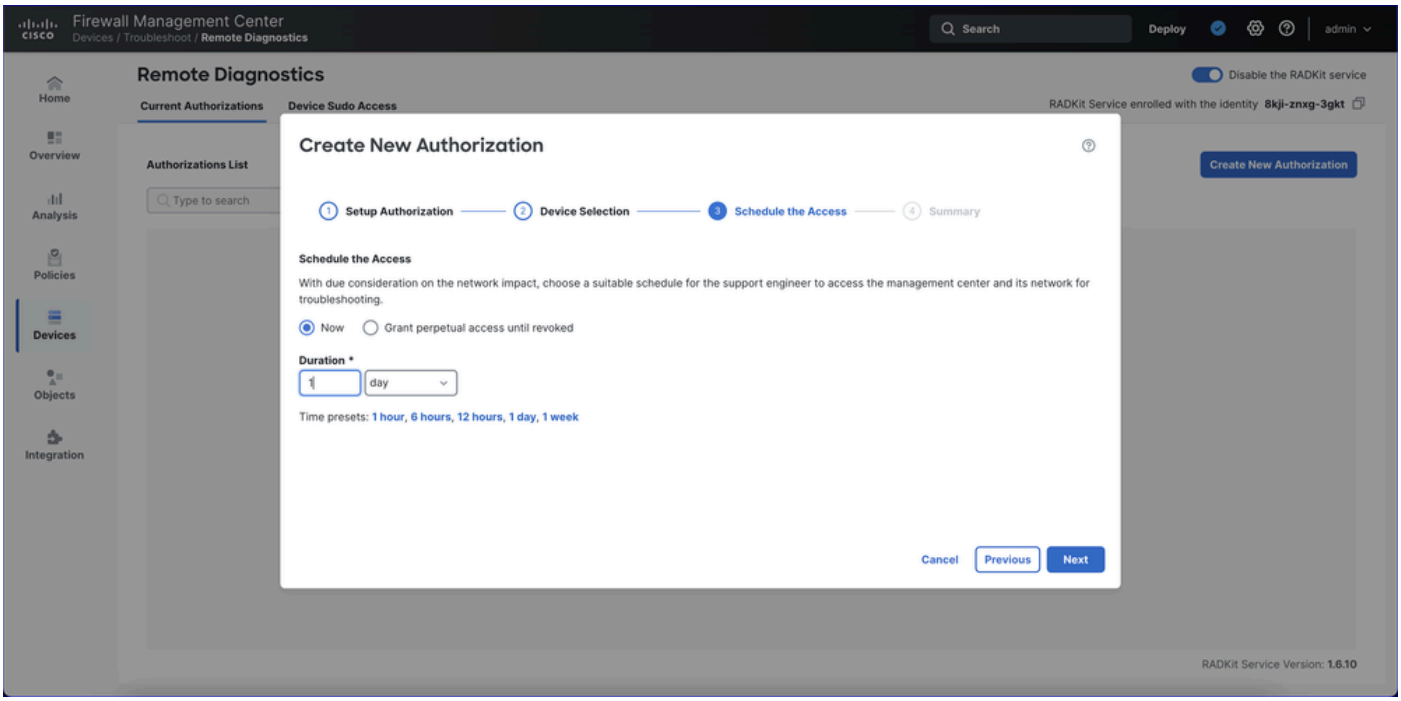


Notas sobre la selección de dispositivos

- Solo se pueden seleccionar los dispositivos de una compilación compatible (por ejemplo, en la versión inicial, solo los dispositivos 7.7.0).
- No se pueden seleccionar los dispositivos que están deshabilitados y no son accesibles. RADKit depende de sftunnel (TCP 8305) para acceder a los dispositivos.
  - Si hay un problema de conectividad sftunnel, no funciona, pero aún se muestra en el inventario RADKit.
  - Si un dispositivo está apagado, no se ve en absoluto.
- Si hay CSP en un par HA, solo se pueden añadir los activos/primarios.
- Los dispositivos se agregan al inventario RADKit al crear/editar una autorización. Cuando se cancelan los registros de FMC de los dispositivos, estos se eliminan del "inventario" de dispositivos.

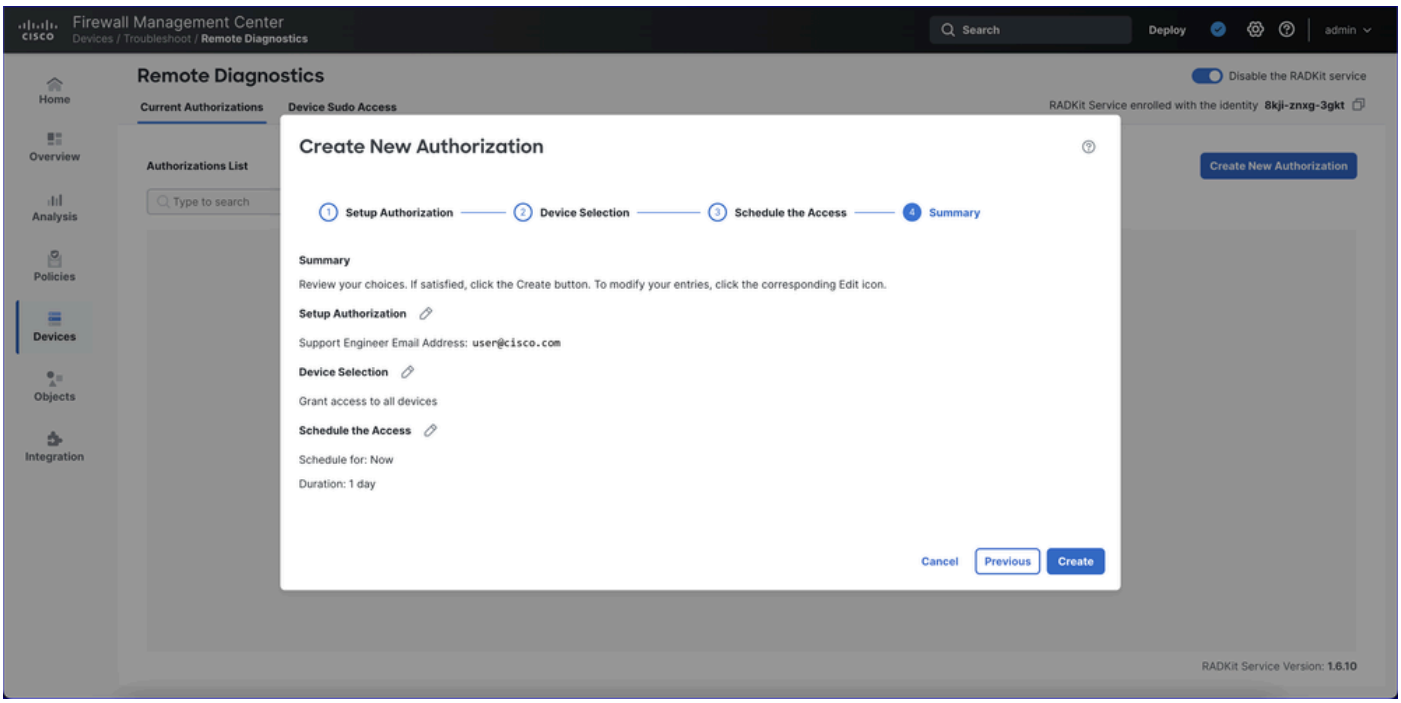
Crear nueva autorización: Paso 3

- Paso 3: Especifique la duración del acceso del ingeniero de soporte técnico a los dispositivos.
- Elija "Ahora" y especifique una duración, o bien,
- Seleccione "Conceder acceso perpetuo hasta que se revoque".
- La duración predeterminada es de 1 día. Se puede establecer cualquier duración; también hay algunos valores de duración predefinidos.



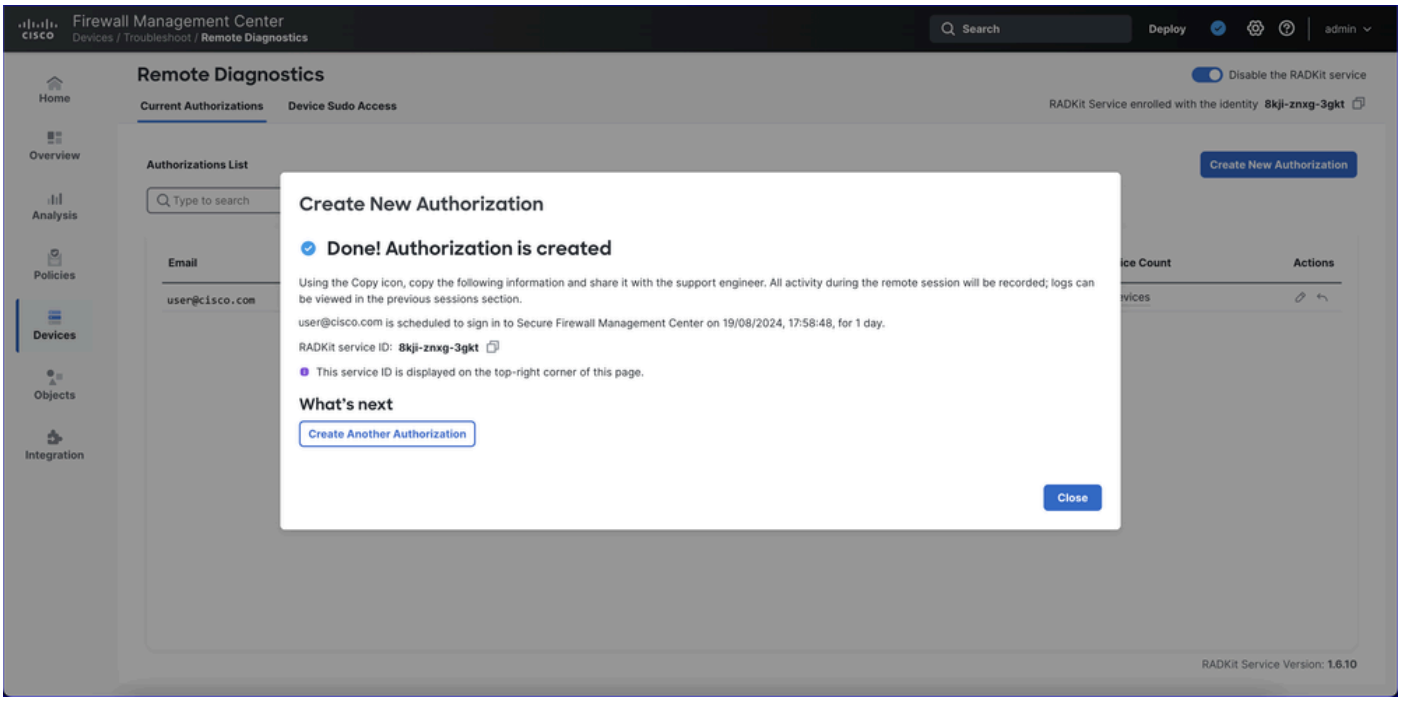
Crear nuevo resumen de autorización

El paso final es el resumen de autorización. Aquí, un usuario puede revisar y editar la configuración.



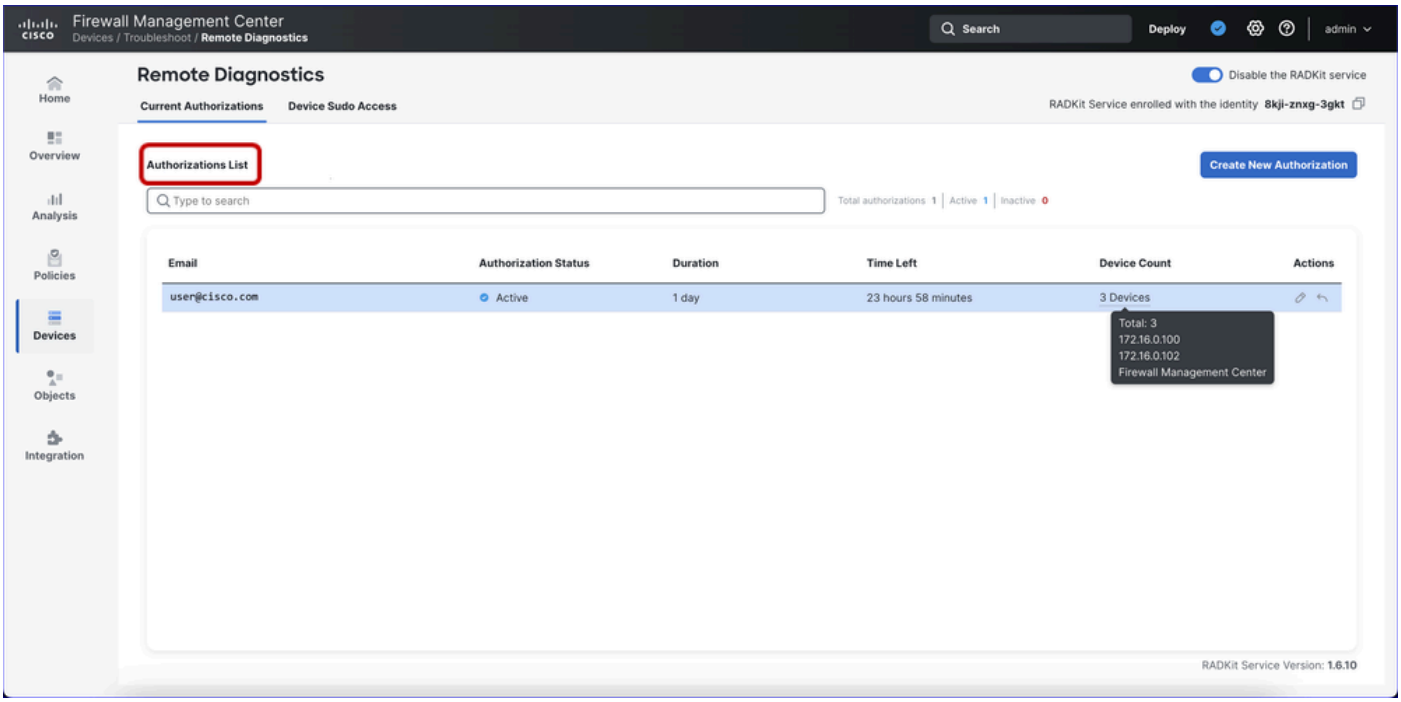
Creación de nueva autorización completada

Una vez finalizada la creación de la autorización, se muestra una pantalla de confirmación:



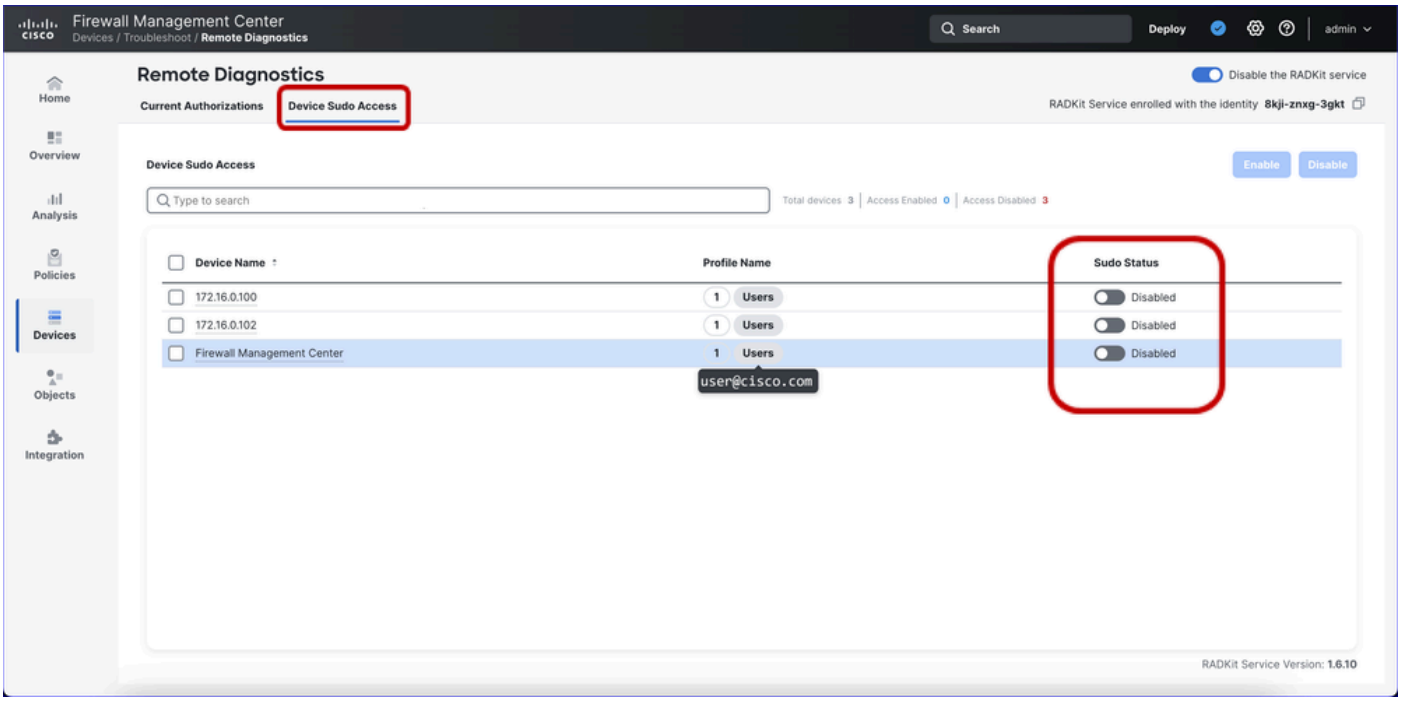
Lista de autorizaciones actuales, incluida la revocación

- La lista de autorizaciones actuales se muestra en la pestaña Autorizaciones actuales.
- Las acciones (columna derecha) son Revocar acceso y Editar autorización.



Lista de acceso de sudo de dispositivos

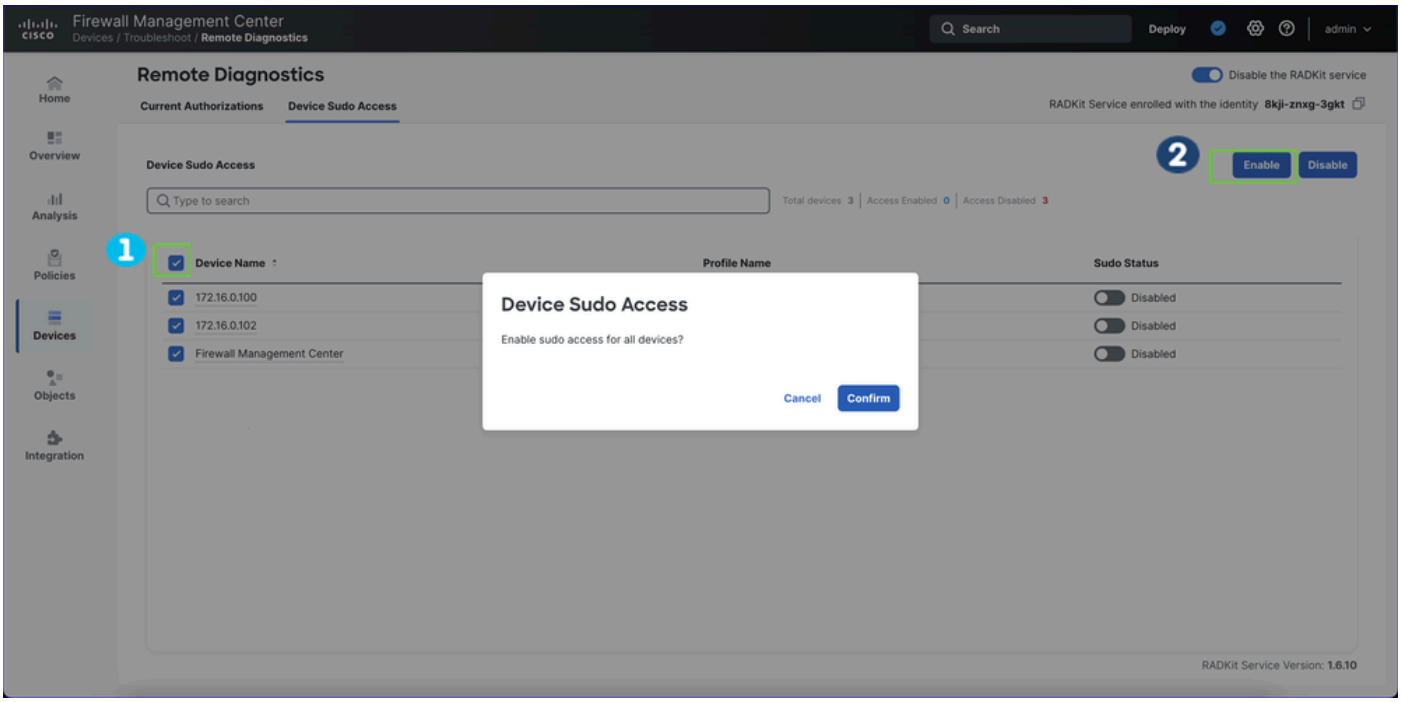
- La lista de dispositivos con configuración de acceso sudo se presenta en la pestaña Device Sudo Access.
- Utilice el botón de alternancia de la columna derecha para activar el acceso sudo. Está desactivada de forma predeterminada.
- Además, está disponible el acceso sudo de activación/desactivación masiva.



Confirmar activación del acceso de sudo de los dispositivos

1. El acceso Sudo se puede habilitar para todos o solo para algunos dispositivos específicos seleccionando los dispositivos y luego haciendo clic en el botón "Enable".

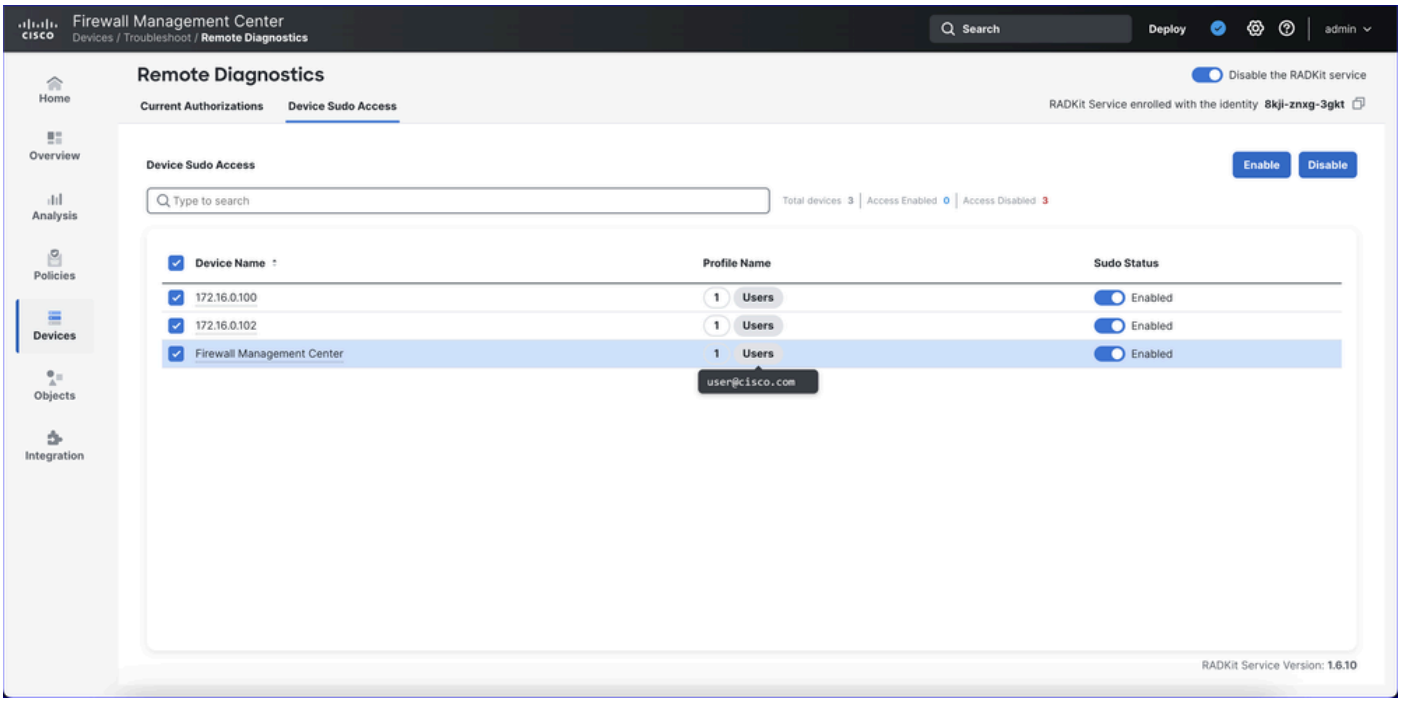
2. Cuando se activa, aparece un cuadro de diálogo de confirmación y se hace clic en Confirmar es necesario.



Dispositivos con Sudo Access activado

- Después de habilitar o deshabilitar el acceso sudo para un dispositivo, se actualiza la columna Estado de sudo a la derecha de la página.

- El ingeniero de soporte puede ejecutar sudo su en el dispositivo; esto es sin contraseña. El ingeniero de soporte técnico no necesita tener la contraseña raíz.



Otras notas

- Solo los dispositivos del dominio a los que el usuario de FMC tiene acceso son visibles y se puede autorizar el acceso remoto.
- Si los CSP se encuentran en alta disponibilidad:
  - El servicio RADKit solo se puede habilitar en el activo/principal.
  - El FMC secundario no se puede agregar actualmente como dispositivo al que se accederá desde el cliente RADKit.
- La autorización solo se puede realizar para un ingeniero de soporte técnico a la vez.
  - Si necesita que otro ingeniero de soporte técnico tenga acceso, cree otra autorización para el ingeniero adicional. El ID de servicio sería el mismo.

API REST FMC

API REST del servicio RADKit

Para permitir las operaciones de creación y lectura en el servicio RADKit, se han introducido estas nuevas URL:

- GET: /api/fmc_Troubleshoot/v1/domain/{domainUUID}/radkit/services
  - Recupera todos los datos del servicio RADKit del FMC.
- GET: /api/fmc_Troubleshoot/v1/domain/{domainUUID}/radkit/services/{id}
  - Recupera/recupera los datos del servicio RADKit del ID especificado.
- POST: /api/fmc_Troubleshoot/v1/domain/{domainUUID}/radkit/services
  - Crea el servicio RADKit en el FMC (activar/desactivar el servicio).

Modelo de servicio RADKit

El modelo de servicio RADKit consta de:

- tipo
- id
- estado
- isEnrollado
- serviceId
- versión


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


Soporte de Cisco: Uso del cliente RADKit

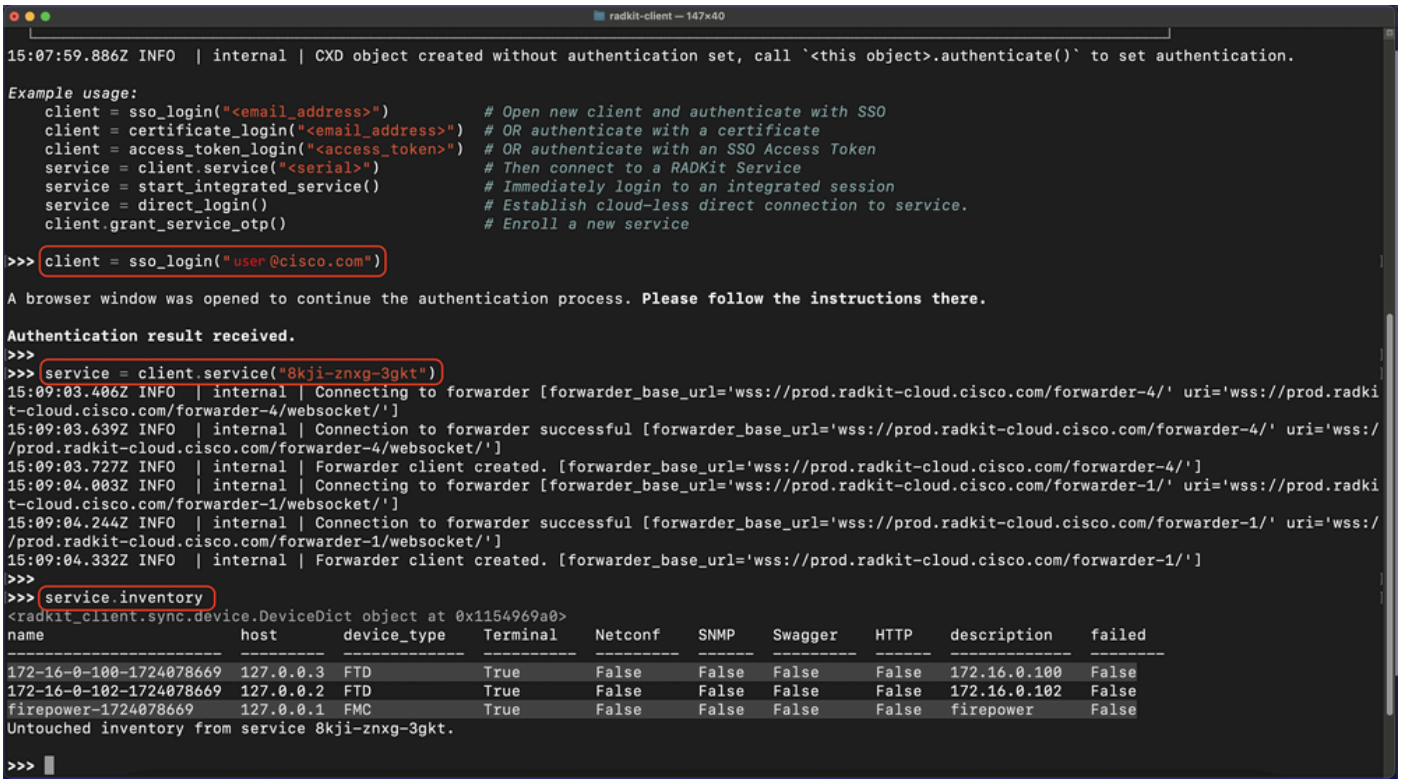
Lado de soporte: Instalación del cliente RADKit

- Para acceder a los FMC/FTD, el soporte debe tener instalado el cliente RADKit.
    - El cliente funciona en sistemas operativos Windows, Mac y Linux.
- La asistencia puede tener acceso a varios dispositivos de varios usuarios. Cada autorización de RADKit tiene su propio "inventario" de dispositivos.
    - Para cada inventario de dispositivos de usuario que soporte desea acceder, se necesita el ID de servicio de RADKit.
    - Para un único inventario, el acceso es posible tanto para el CSP como para sus FTD gestionados desde el cliente RADKit, según lo especificado por el usuario al autorizar el acceso.

Obtener e instalar el cliente RADKit

El cliente RADKit se puede instalar localmente desde https://radkit.cisco.com/downloads/release/ y luego se inicia desde el terminal con el comando: radkit-client

Los instaladores están disponibles para Windows, MacOS y Linux.



Captura de pantalla del cliente RADKit con comandos de inicio de sesión (detalles en la siguiente sección).

Comandos de Login del Cliente RADKit

- Utilice la dirección de correo electrónico introducida por el usuario durante la autorización en FMC.
- El inicio de sesión del cliente RADKit y la conexión a los comandos de ID de servicio especificados. El ID del servicio RADKit, en este ejemplo 8abc-znxg-3abc, debe coincidir con lo que ve el administrador del firewall en 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
```

Comando RADKit Client Service Inventory

Comando para enumerar el inventario al que el usuario remoto (ingeniero de Cisco TAC) está autorizado a acceder:

```
<#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.
```

Hay un comando de filtro para los dispositivos del inventario (sección siguiente). Utilice el nombre de la columna de la izquierda para iniciar una sesión interactiva con el dispositivo (comando de la próxima sección).

Consejo: Si el inventario está obsoleto, puede actualizarlo mediante el comando: **>>>** service.update_Inventory()

Cliente RADKit: Filtrar dispositivos

Comando para filtrar dispositivos en el inventario:

```
<#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.
```

Comando RADKit Client Device Interactive Session

Iniciar una sesión interactiva para un dispositivo (en este caso, un FMC) con el nombre "firepower-1724078669" tomado del comando anterior "service.Inventory":

<#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)
```

Comandos de ejecución del cliente RADKit en dispositivos

Ejecute los comandos en los dispositivos.

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

Obtenga detalles adicionales de los dispositivos

Considerando este inventario:

```
<#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
```

Para obtener los detalles de 'show version' de los dispositivos FTD:

<#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
```

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

>
```

Enfoque alternativo:

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

Obtención de archivos desde dispositivos

- A través del cliente RADKit, un ingeniero del TAC de Cisco puede realizar SSH a los dispositivos y realizar diversas operaciones, incluida la generación de archivos de solución de problemas.

Soporte de Cisco: Consola RADKit

Uso de la consola de red RADKit

- Como alternativa al uso del cliente RADKit, un ingeniero de soporte del TAC de Cisco podría utilizar la consola de red RADKit. La consola de red es parte del cliente RADKit.
- La consola de red RADKit es una función que proporciona una interfaz de línea de comandos (CLI) sencilla para las funciones básicas del cliente RADKit. Se ha diseñado para que se pueda conectar rápidamente a una instancia del servicio RADKit, establecer sesiones interactivas y descargar/cargar archivos sin problemas y con una formación mínima.
- Inicie la consola de red mediante la línea de comandos: radkit-network-console
- Consulte la documentación de RADKit para obtener más información.

Compatibilidad con actualizaciones y versiones anteriores

Actualización a 7.7 y a partir de 7.7

- El servicio RADKit se agrega en Secure Firewall 7.7.0.
    - Los dispositivos actualizados a la versión 7.7.0+ tienen la configuración requerida para el servicio RADKit. conservado

Experiencia con FTD no compatibles

- Los CSP y FTD deben tener la versión mínima 7.7.0 para que esta función funcione (los FTD con una versión inferior a 7.7 no pueden añadirse a una autorización RADKit de FMC 7.7).
- Los FTD registrados que no se encuentran en la versión 7.7.0 no están disponibles para su selección con el fin de habilitar la autorización.

Resolución de problemas

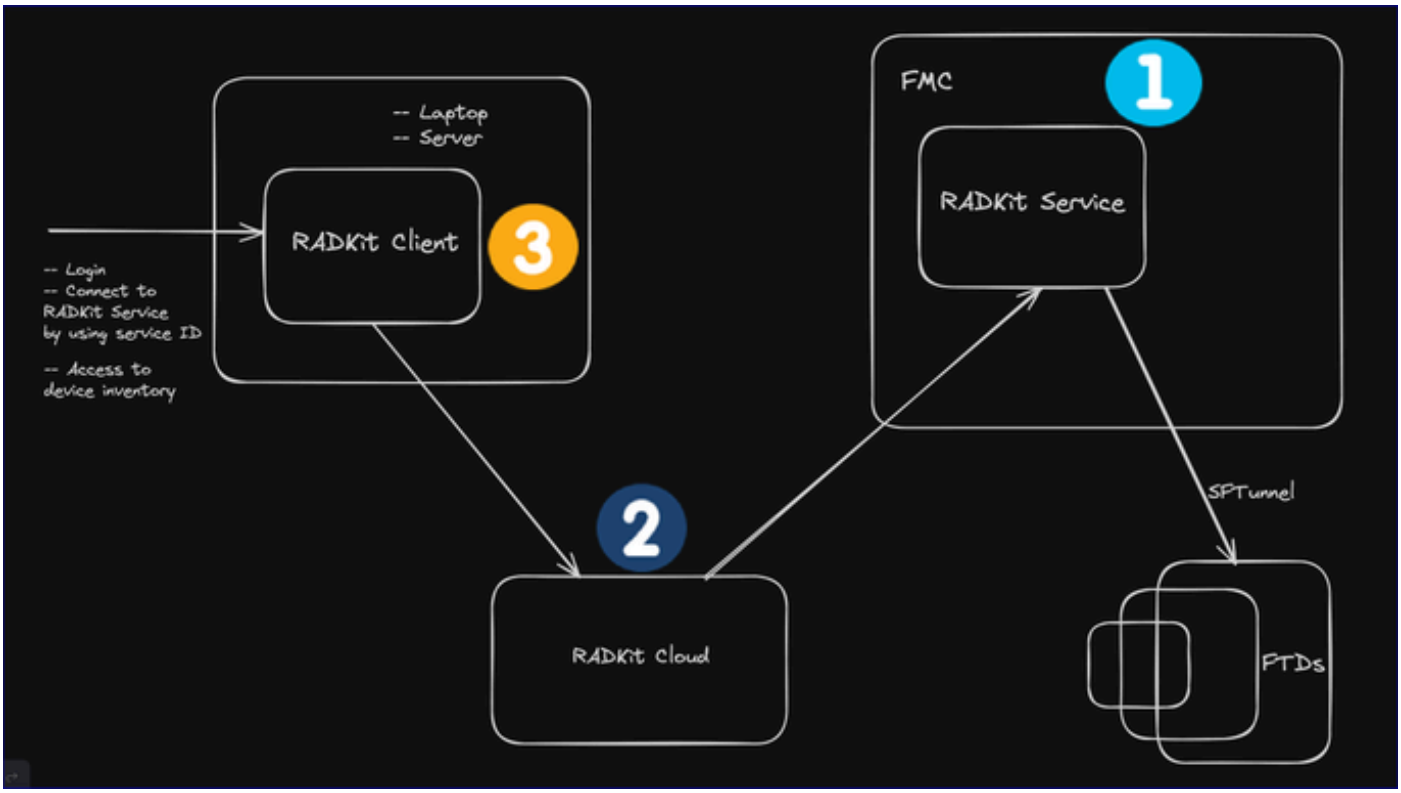
Descripción general del diagnóstico

Puntos de resolución de problemas

1. Utilice las herramientas de desarrollo de navegadores y los registros de FMC para ver lo que sucede en FMC.

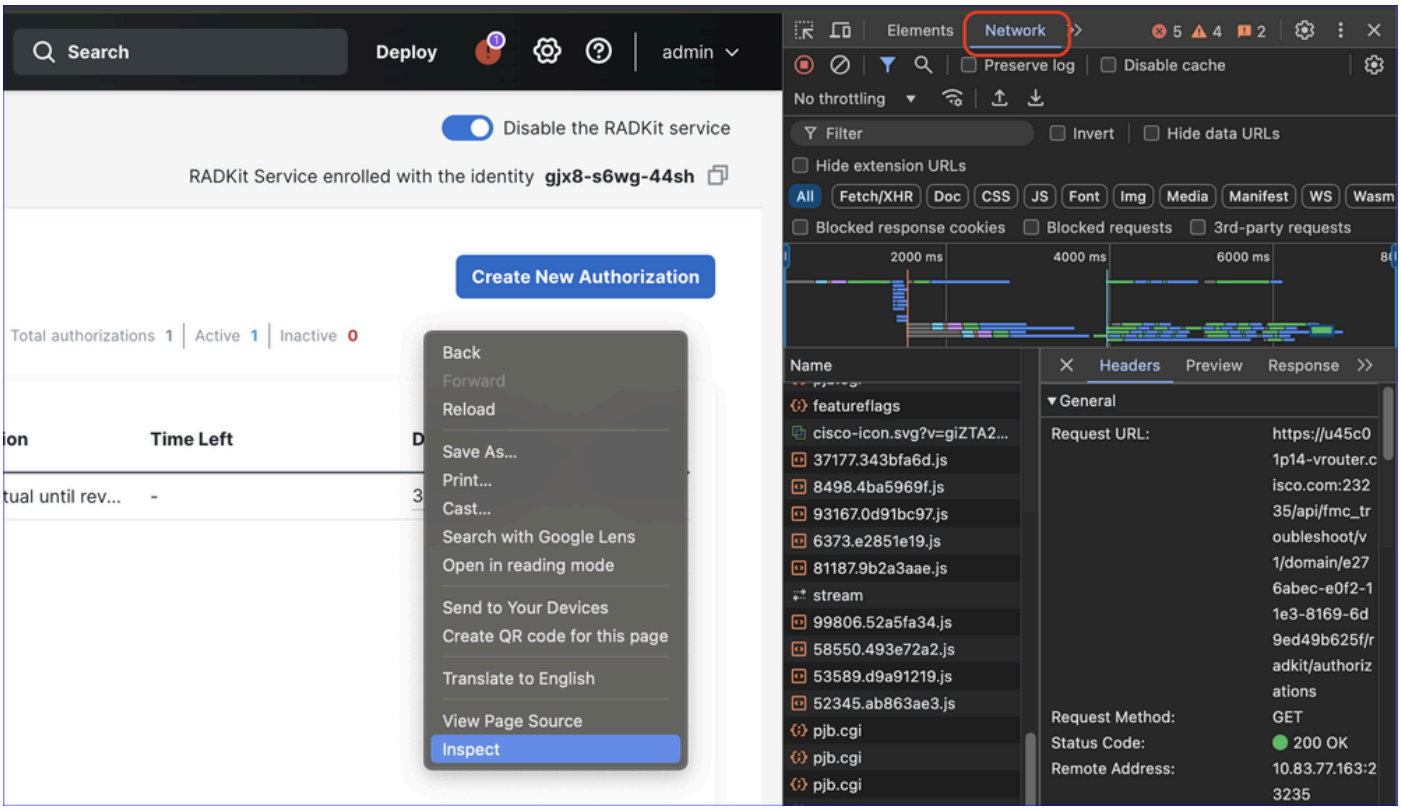
2. Para problemas de comunicación entre el Servicio RADKit en FMC, RADkit Cloud y el cliente RADKit, mire en el registro del cliente RADKit.

3. Cliente RADKit.



Cómo solucionar problemas: Herramientas de desarrollo del navegador

- La pestaña Developer Tools, Network del navegador muestra las llamadas de API que se ejecutaron en la página, que se pueden utilizar para solucionar problemas en FMC. Para iniciarlo, haga clic con el botón derecho del ratón en la página y, a continuación, haga clic en Inspeccionar.
- Compruebe el código de estado de llamada API y la vista previa de respuesta en la ficha Red.



API de middleware de RADKit Service Go

Go Middleware para la integración RADKit utiliza llamadas API que no están disponibles públicamente a través del explorador de API FMC. El registro de las API de Go Middleware está disponible en /var/log/auth-daemon.log. La funcionalidad que Go Middleware lleva a cabo incluye:

- Inscriba el servicio RADKit en la nube RADKit con el proceso de inicio de sesión único.
- Obtenga una lista de todas las autorizaciones de los usuarios remotos de RADKit y los dispositivos asociados.
- Obtenga una autorización de usuario de RADKit remota específica y los dispositivos asociados mediante un correo electrónico.
- Cree una autorización de usuario de RADKit remota y conceda permisos para acceder a dispositivos (todos los dispositivos o una lista de dispositivos seleccionados) durante un período de tiempo especificado.
- Modifique una autorización de usuario de RADKit remoto.
- Eliminar una autorización de usuario de RADKit remota.

Registros para solucionar problemas del servicio RADKit

- Registros generales del CSP: comando pigtail desde una sesión de FMC ssh.
- API Go Middleware: /var/log/auth-daemon.log
- Registros que contienen datos de procesos RADKit y auth-daemon:

/var/log/process_stdout.log

/var/log/process_stderr.log

Todos estos registros se incluyen en los Resoluciones de problemas de FMC/FTD.

- Registros de servicio RADKit internos: /var/lib/radkit/logs/service/
- Registros de las operaciones realizadas desde el cliente RADKit en dispositivos (FMC y FTD): /var/lib/radkit/session_logs/service

Registros para enviar a Cisco TAC

- Capturas de pantalla de errores.
- Descripción del problema.
- Pasos para reproducir.
- Pigtail y /var/log/auth-daemon.log registran los extractos que contienen los errores.

Supervisión del acceso

El registro de a quién se ha concedido acceso durante cuánto tiempo y quién lo ha concedido se encuentra en los registros de auditoría de FMC.

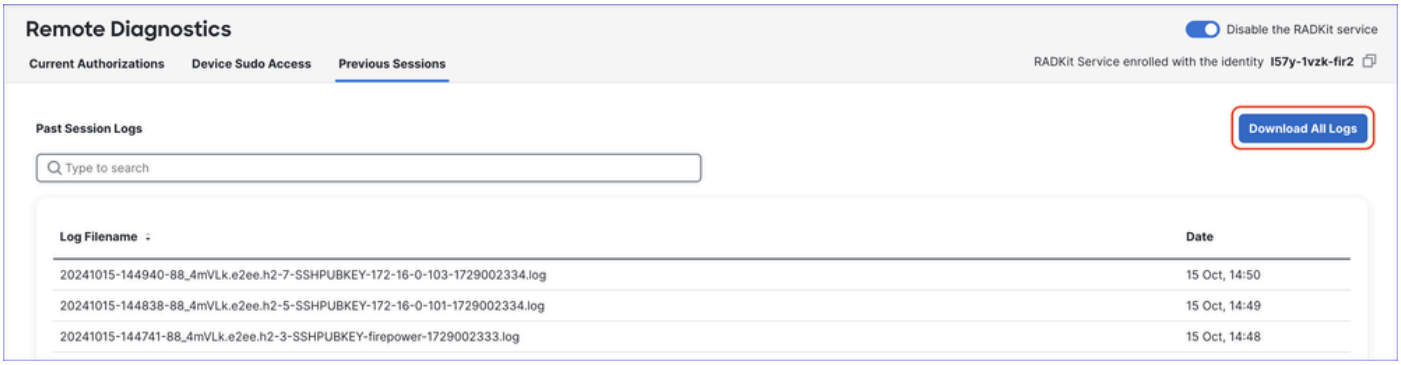
Registros de sesión de RADKit

Los registros de sesión de RADKit para las operaciones realizadas desde el cliente RADKit en dispositivos (FMCs y FTDs) están presentes en FMC en /var/lib/radkit/session_logs/service:

- Los registros provienen del propio servicio RADKit.
- Estos registros se incluyen en un paquete de solución de problemas.
- También se puede acceder a los registros desde la interfaz de usuario (consulte la siguiente sección).
- Hay varios archivos de registro de sesión; una por sesión.

Registros de sesiones anteriores de RADKit

Los registros de sesiones de RADKit para las operaciones del dispositivo realizadas desde el cliente RADKit están disponibles para su descarga como un archivo que contiene todos los registros de la pestaña Sesiones anteriores haciendo clic en el botón "Descargar todos los registros".



Ejemplo de problema con la resolución de problemas

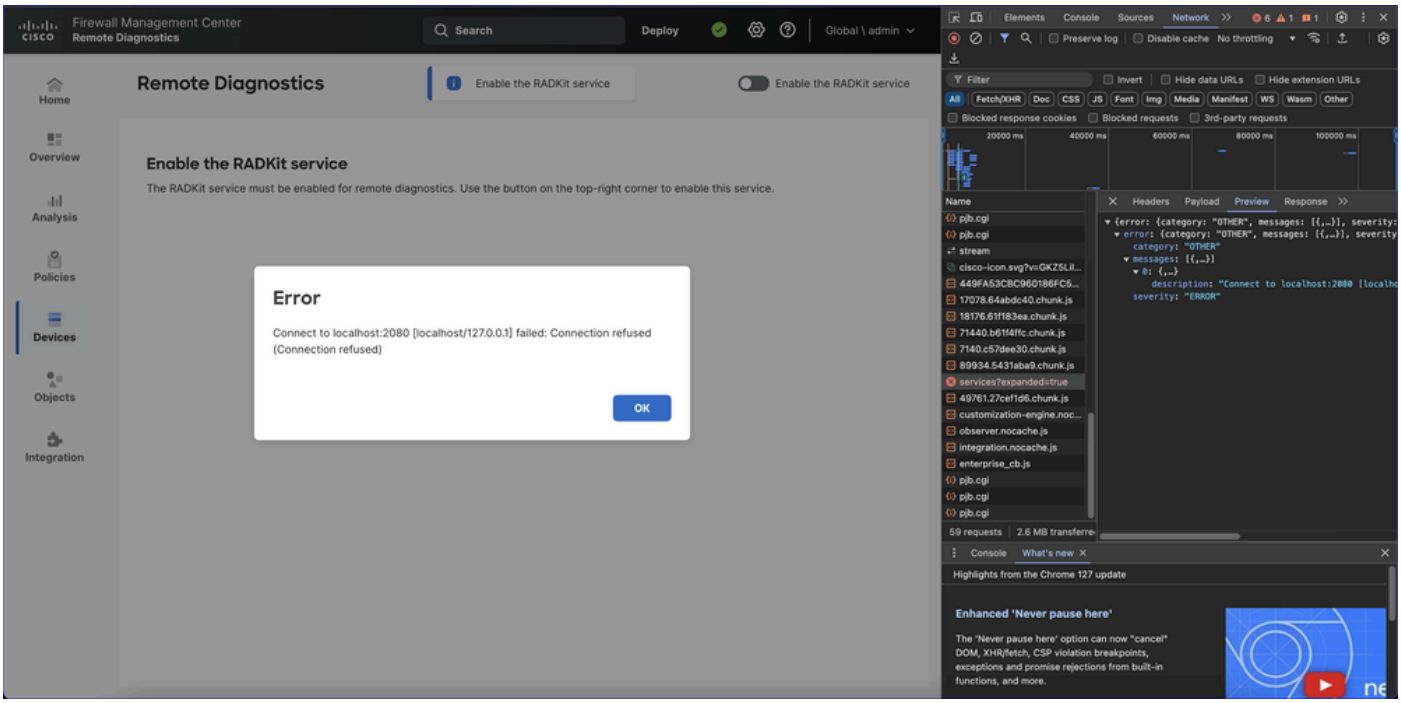
Ejemplo de Troubleshooting

En caso de error como "Connect to localhost:2080 [localhost/127.0.0.1] failed: Conexión rechazada (conexión rechazada)", intente reiniciar auth-daemon desde una sesión FMC SSH:

<#root>

root@firepower:~$

sudo pmtool restartbyid auth-daemon



Telemetría

Se agregó la salida de telemetría para esta función:

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

Preguntas frecuentes

Preguntas más Frecuentes: Inicio de sesión e inscripción

P. ¿La inscripción funciona con proxy si FMC no tiene acceso directo a Internet?

R. Sí, si el proxy tiene acceso a prod.radkit-cloud.cisco.com que se utiliza para el proceso de inscripción.

P. ¿Puede un usuario utilizar su propio IdP para este servicio?

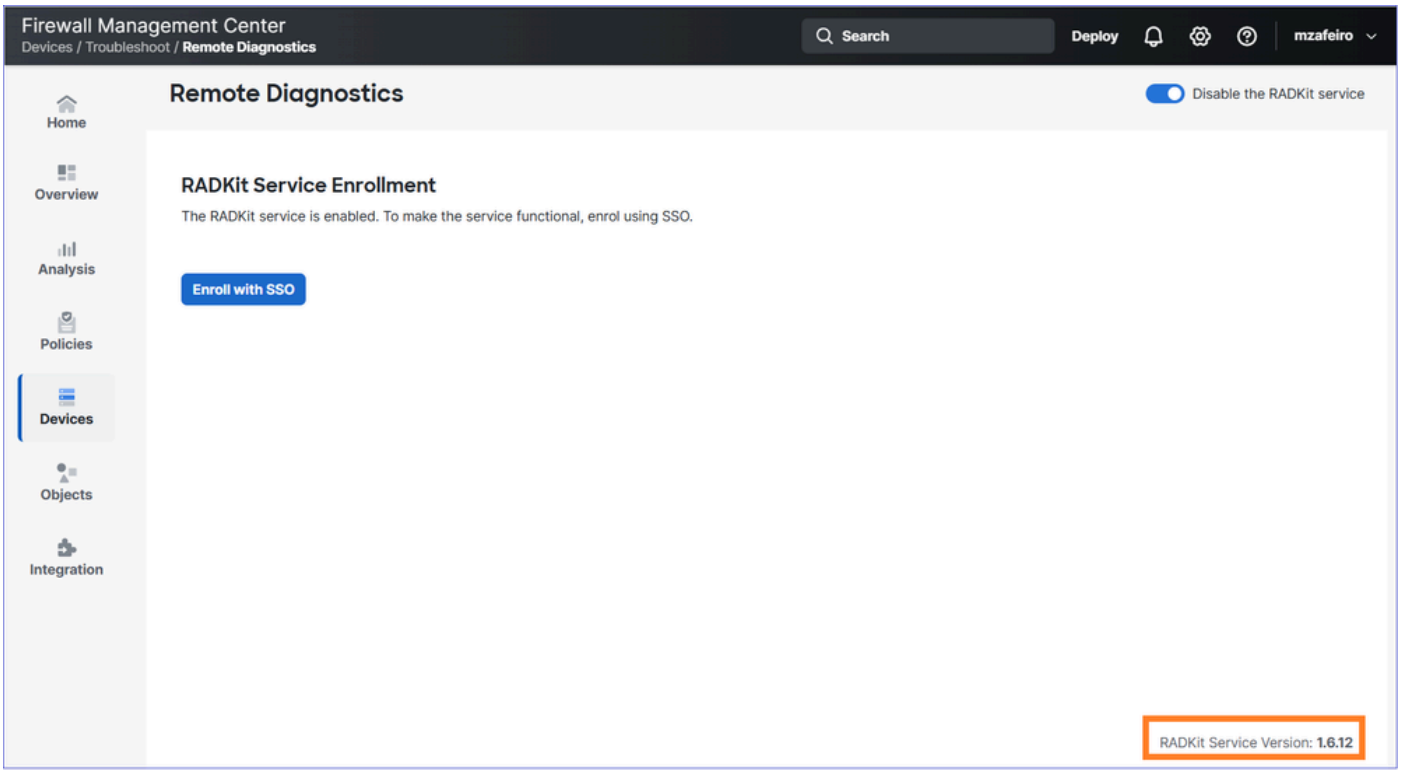
R. Solo se acepta Cisco SSO en la nube de RADKit. Existe la opción de asociar la cuenta de su empresa a una cuenta de Cisco, de modo que la inscripción al servicio RADKit sea posible con un correo electrónico que no sea de Cisco.

Preguntas más Frecuentes: Versiones de RADKit

P. ¿Qué versión de RADkit se incluye en FMC en la versión 7.7? ¿Cómo podemos saber qué versión de RADKit está incluida en FMC? ¿Es algo que se pueda actualizar sin una actualización de FMC?

A.

- La versión de RADKit que viene con 7.7.0 es 1.6.12.
- La versión del servicio RADKit se muestra en la parte inferior de la página Diagnóstico remoto de FMC: "Versión del servicio RADKit: 1.6.12.".



- RADKit se incluye con paquetes de actualización FMC/revisiones. No se admite la actualización del servicio RADKit en FMC por separado.

Preguntas más Frecuentes: Otro

P. ¿Podrían incluirse dispositivos externos (no gestionados por el CSP)?

R. Solo los dispositivos gestionados por el CSP pueden añadirse al inventario RADKit y, a continuación, se puede acceder a ellos a través de una autorización.

P. ¿Se realiza una copia de seguridad de la configuración de RADKit como parte de la copia de seguridad de FMC?

A.

- No se realiza una copia de seguridad de la configuración como parte de la copia de seguridad de FMC.
- No está respaldada porque prevemos que, por lo general, no se proporcionará acceso perpetuo; el acceso suele ser solo durante un tiempo limitado.

Referencias

Enlaces útiles:

- Guía de configuración de FMC - RADKit
- https://radkit.cisco.com/
- https://radkit.cisco.com/docs/index.html
- https://radkit.cisco.com/downloads/release/
- https://github.com/Cisco-RADKit/Intro

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).