Configurazione dell'integrazione di Cisco RADKit in FMC

Sommario

Introduzione

- Introduzione
- Descrizione delle funzionalità e procedura dettagliata
- API REST FMC
- Ottieni ulteriori dettagli dai dispositivi
- Supporto Cisco: Console RADKit
- Compatibilità con aggiornamenti e versioni precedenti

Risoluzione dei problemi

- Panoramica sulla diagnostica
- Registri sessione RADKit
- Esempio di problema con la risoluzione dei problemi Procedura dettagliata
- Telemetria

Domande frequenti

Introduzione

Questo documento descrive la funzionalità Cisco RADKit Integration in FMC aggiunta nella versione 7.7.

Introduzione

Problemi degli amministratori del firewall

- Il Remote Automation Development Kit (RADKit), sviluppato da Cisco, è un orchestrator a livello di rete progettato per fornire agli utenti la possibilità di accedere in modo sicuro e risolvere i problemi dei dispositivi di rete. https://radkit.cisco.com/
- Il Cisco Secure Firewall Management Center (FMC) gestisce e gestisce i dispositivi Secure Firewall Threat Defense (FTD). Un singolo CCP può gestire più dispositivi in diversi luoghi.
- Mentre è possibile per gli utenti installare il RADKit separatamente e a bordo dei loro FMC e FTD in esso, la costruzione del servizio RADKit nel FMC e l'imbarco dei FMC e di tutti i dispositivi gestiti (FTD) in modo automatizzato sarebbe un'esperienza migliore per gli utenti finali.

Scenario d'uso

Alcune delle funzionalità chiave di cui gli utenti potrebbero beneficiare dopo l'integrazione di RADKit nel FMC sono:

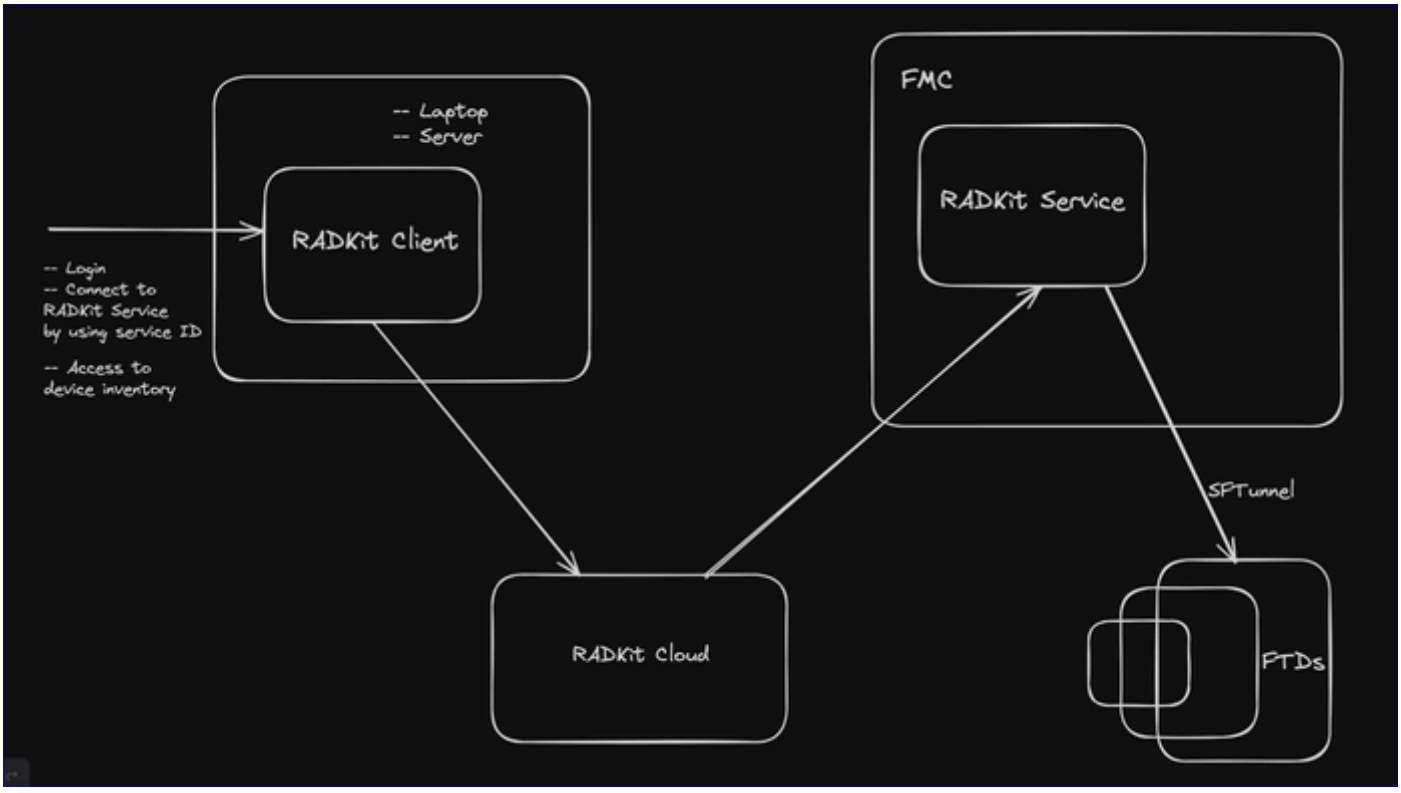
- Possibilità di accedere ai FMC/FTD in remoto dalla CLI del client RADKit.
- Capacità di fornire accesso controllato ai FMC/FTD a chiunque ne abbia bisogno (ad esempio, un tecnico TAC Cisco).
- Sfruttare le funzionalità di automazione per la raccolta dei dati e la diagnosi dei problemi dal client RADKit (gli script che eseguono i comandi su più dispositivi possono essere creati e utilizzati dal client RADKit).

Novità - Soluzione

- A partire da Secure Firewall 7.7.0, il servizio Remote Automation Development Kit (RADKit) è integrato in FMC.
- Gli utenti possono abilitare o disabilitare il servizio RADKit su richiesta, registrarlo nel cloud RADKit e creare le autorizzazioni degli utenti remoti per accedere a dispositivi specifici dal client RADKit per una durata di accesso pianificata.
    - Le autorizzazioni possono essere modificate o revocate.
- È inoltre disponibile un'opzione che consente l'accesso sudo ai dispositivi per la risoluzione avanzata dei problemi.

Integrazione dei servizi RADKit nel diagramma FMC

Il diagramma mostra come RADKit consente la comunicazione dal client RADKit (tecnico TAC) dell'utente ai dispositivi FTD di produzione:



Nozioni di base: Piattaforme supportate, Licenze

Applicazioni e responsabili

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		

Altri aspetti del supporto

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

Dipendenze per il funzionamento della feature

- La versione minima è Secure Firewall 7.7.0.
- Per la connessione al servizio RADKit ospitato in FMC, il client RADKit deve essere installato da https://radkit.cisco.com/downloads/release/ sul computer del tecnico di supporto.
- La versione preferita per il client RADKit è 1.6.10 o successiva.
- È possibile utilizzare versioni precedenti del client RADKit poiché il servizio RADKit è compatibile con le versioni precedenti del client RADKit.

Descrizione delle funzionalità e procedura dettagliata

Panoramica delle funzionalità

- L'integrazione del servizio RADKit in FMC consente agli amministratori dei dispositivi di fornire agli utenti remoti (tecnici TAC di Cisco) l'accesso a specifici dispositivi FMC e FTD della rete a scopo di risoluzione dei problemi e automazione. RADKit è molto più efficiente per la risoluzione dei problemi rispetto alla condivisione dello schermo, non richiede di controllare il computer dell'utente, è un modo più sicuro di lavorare su una rete e si integra perfettamente con Webex.
- In questo modo è possibile usufruire di un supporto tecnico migliore, in quanto gli amministratori dei dispositivi non devono installare e configurare separatamente il servizio RADKit. Inoltre, ciò riduce i tempi di supporto per i tecnici Cisco TAC nella risoluzione dei problemi.

Procedura di configurazione: Panoramica

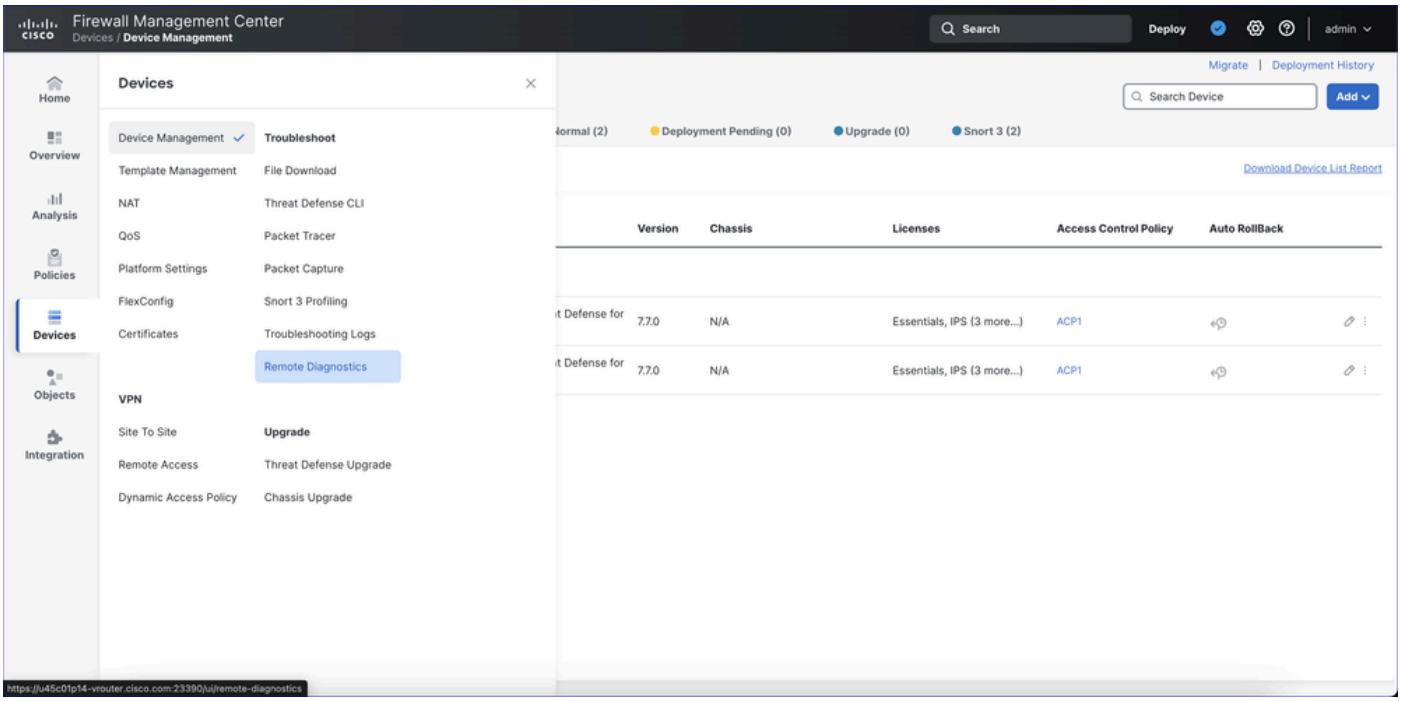
1. Amministratore del dispositivo (utente amministratore FMC): Abilitare e registrare il servizio RADKit e configurare le autorizzazioni nell'interfaccia utente grafica di FMC.

2. Supporto Cisco TAC/Cisco: Installare il client RADKit sul proprio computer, accedere e risolvere i problemi dei dispositivi dal client RADKit.

Utente amministratore FMC: Procedura dettagliata di Centro gestione firewall

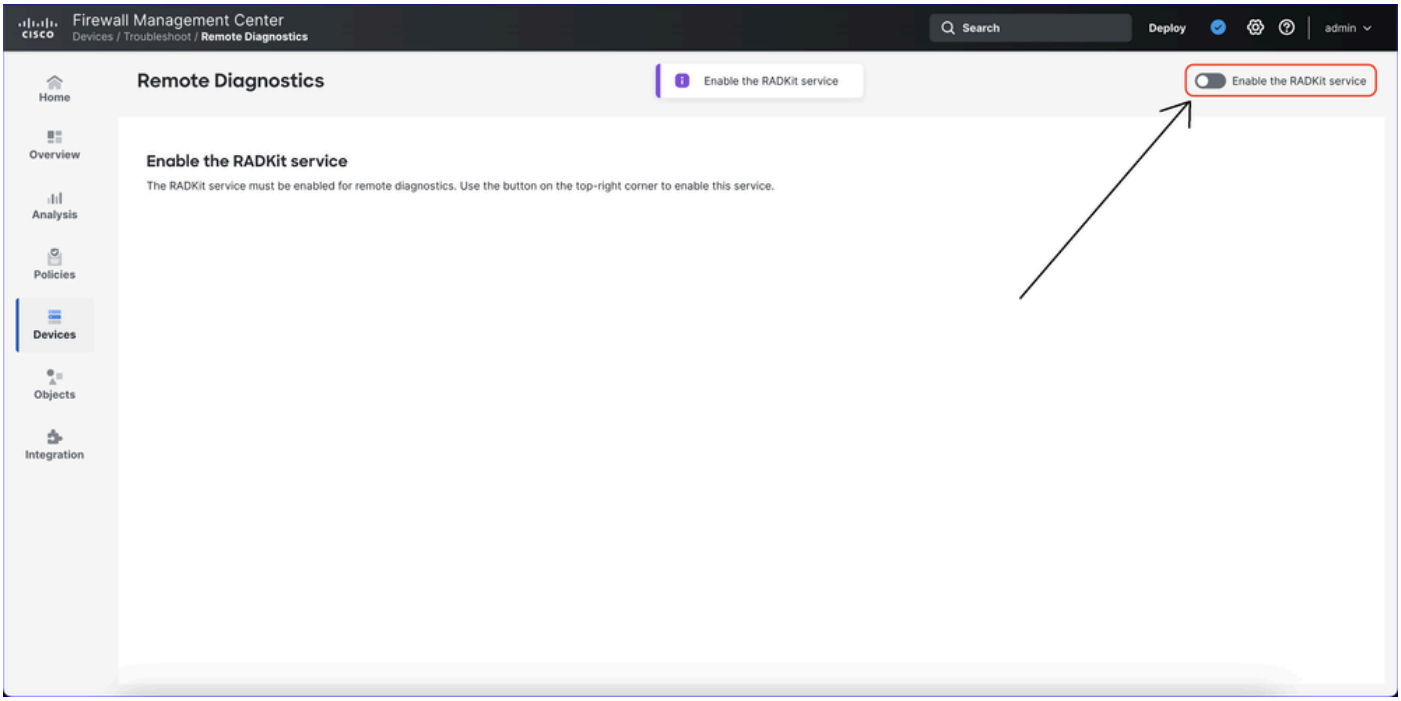
Menu Diagnostica remota

- È stata aggiunta una nuova voce di menu "Diagnostica remota" per questa funzione in Dispositivi -> Risoluzione dei problemi.
- Gli utenti Amministratore, Amministratore di rete e Manutenzione dispongono di autorizzazioni di lettura/scrittura per la pagina.
- Gli utenti Security Analyst, Security Analyst (sola lettura) e Security Approver dispongono di autorizzazioni di sola lettura per la pagina.



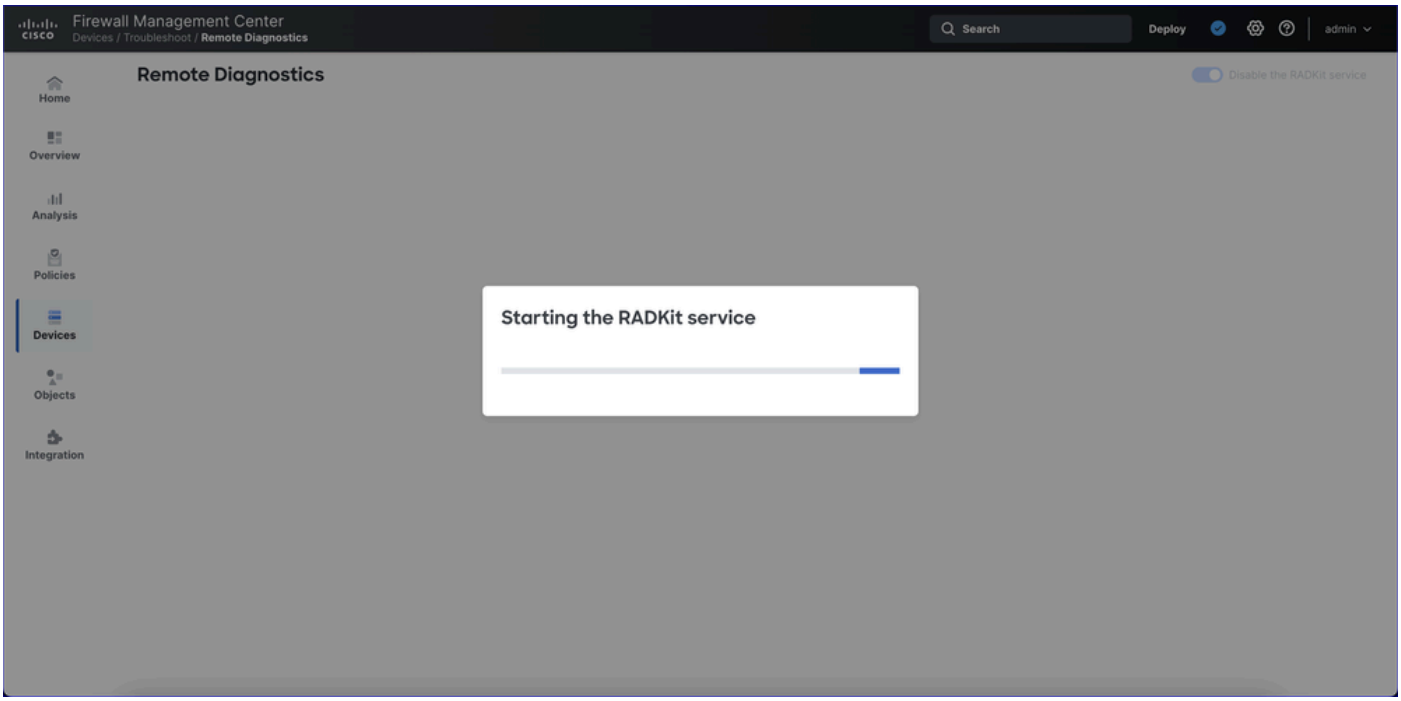
Pagina Diagnostica remota iniziale

Pagina iniziale di Diagnostica remota. Per abilitare il servizio RADKit, è possibile commutare lo switch "Abilita servizio RADKit":



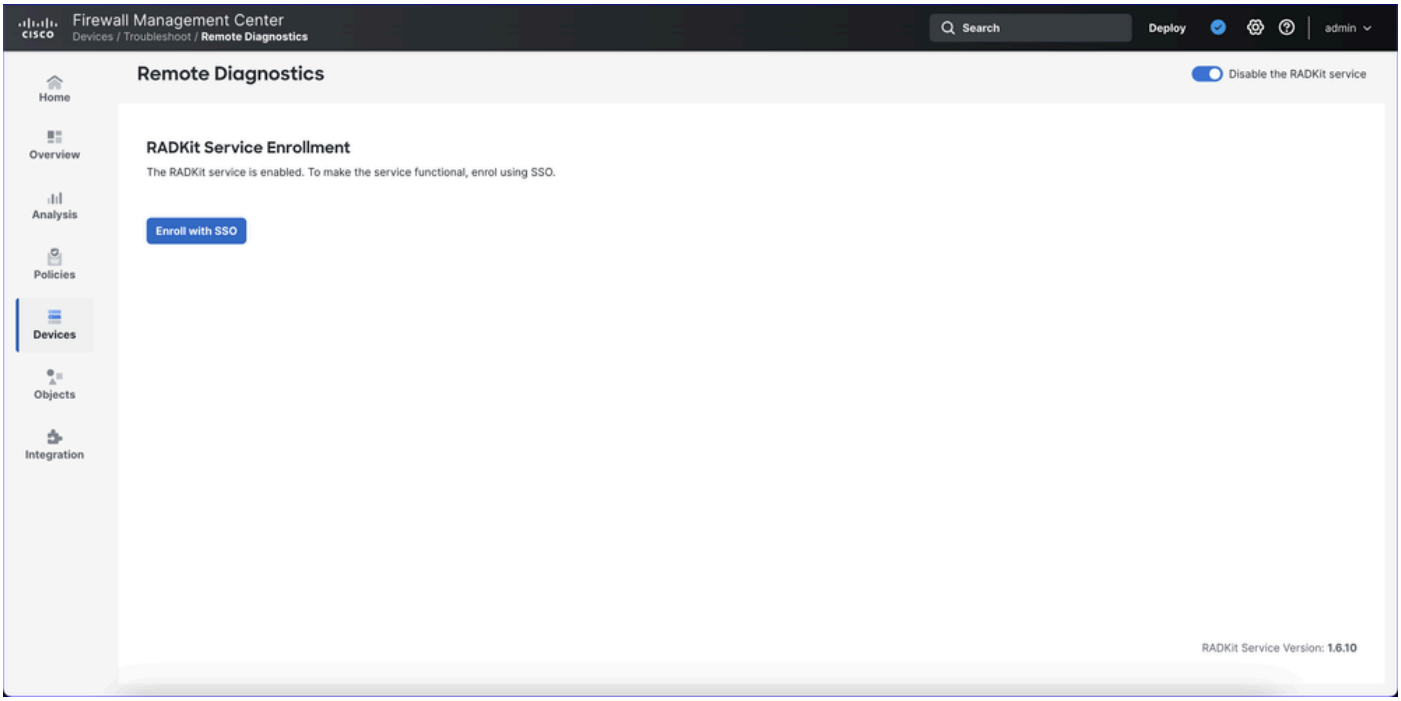
Avvio del servizio RADKit

Dopo l'attivazione del servizio RADKit, viene visualizzato un indicatore di stato fino all'avvio del servizio:



Servizio RADKit abilitato

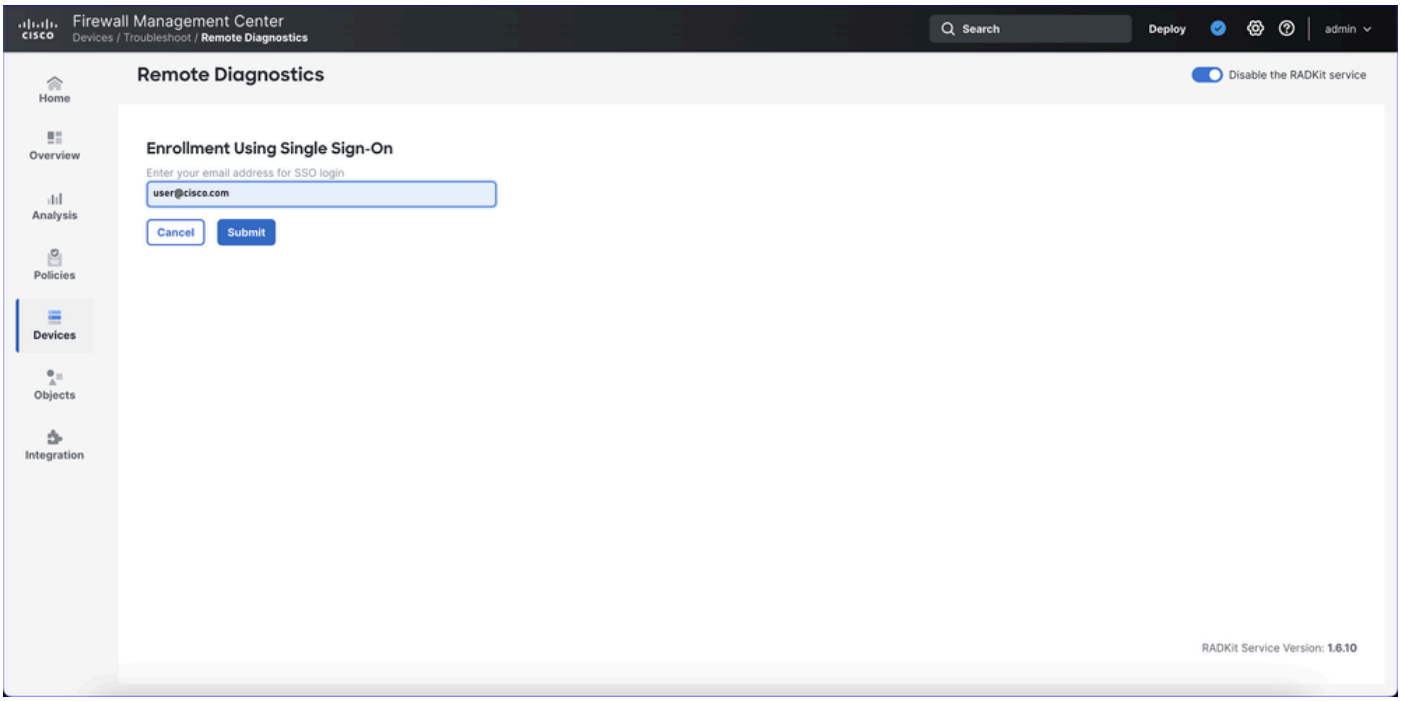
- Al termine del processo di abilitazione del servizio RADKit, viene visualizzata questa pagina:



Il passo successivo è l'iscrizione nel cloud RADKit facendo clic sul pulsante "Registra con SSO".

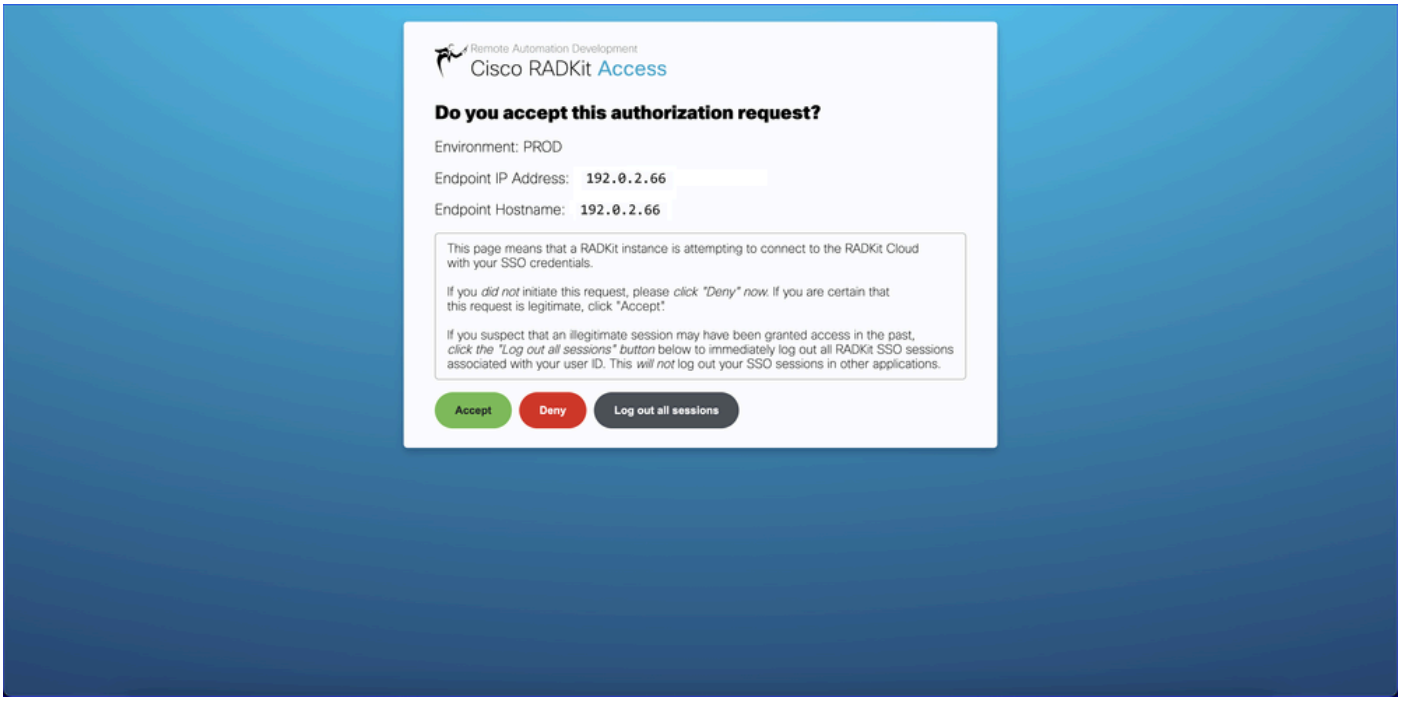
Registrati con SSO - Immetti indirizzo e-mail

Il passo 1 del processo di registrazione consiste nell'immettere l'indirizzo e-mail dell'utente per l'iscrizione al cloud RADKit:



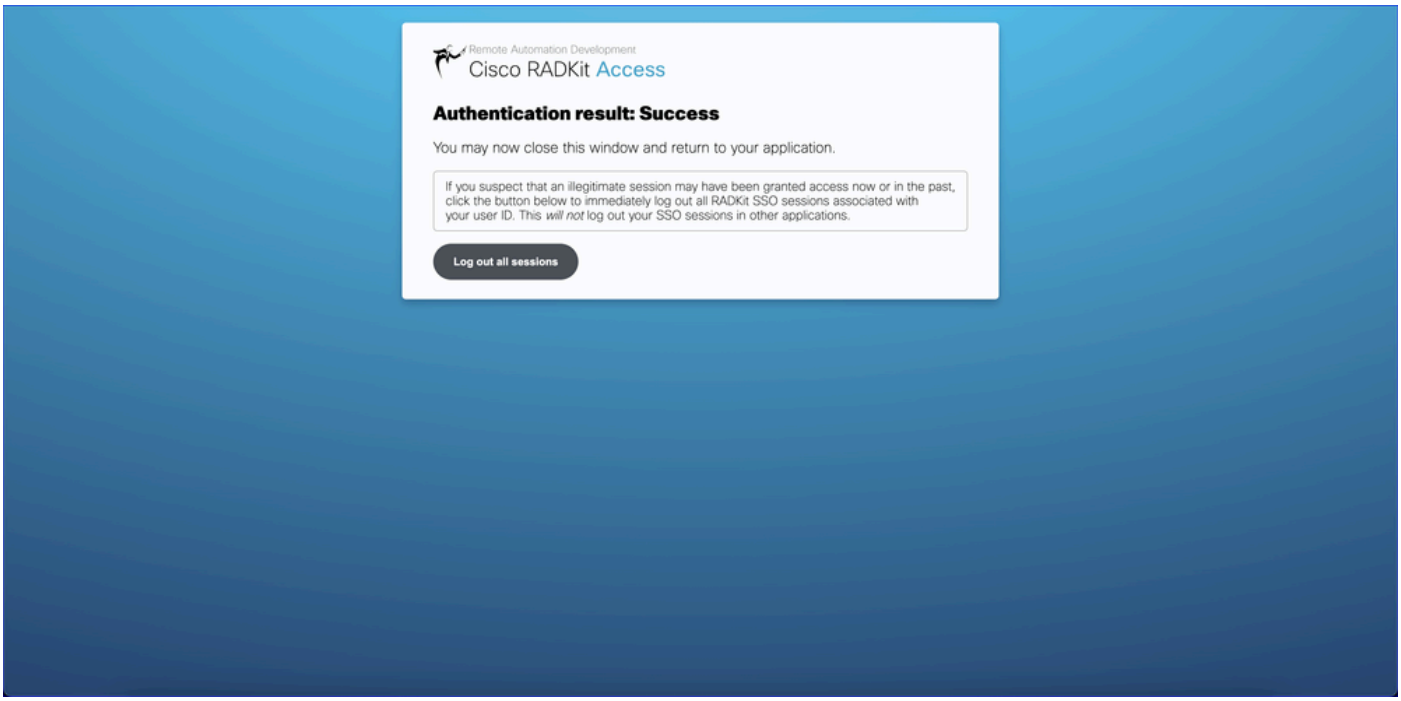
Registra con SSO - Accetta richiesta di autorizzazione

Viene visualizzata una nuova scheda o finestra del browser, a seconda delle impostazioni del browser. Fare clic sul pulsante Accetta.



Registra con SSO - Autenticazione riuscita

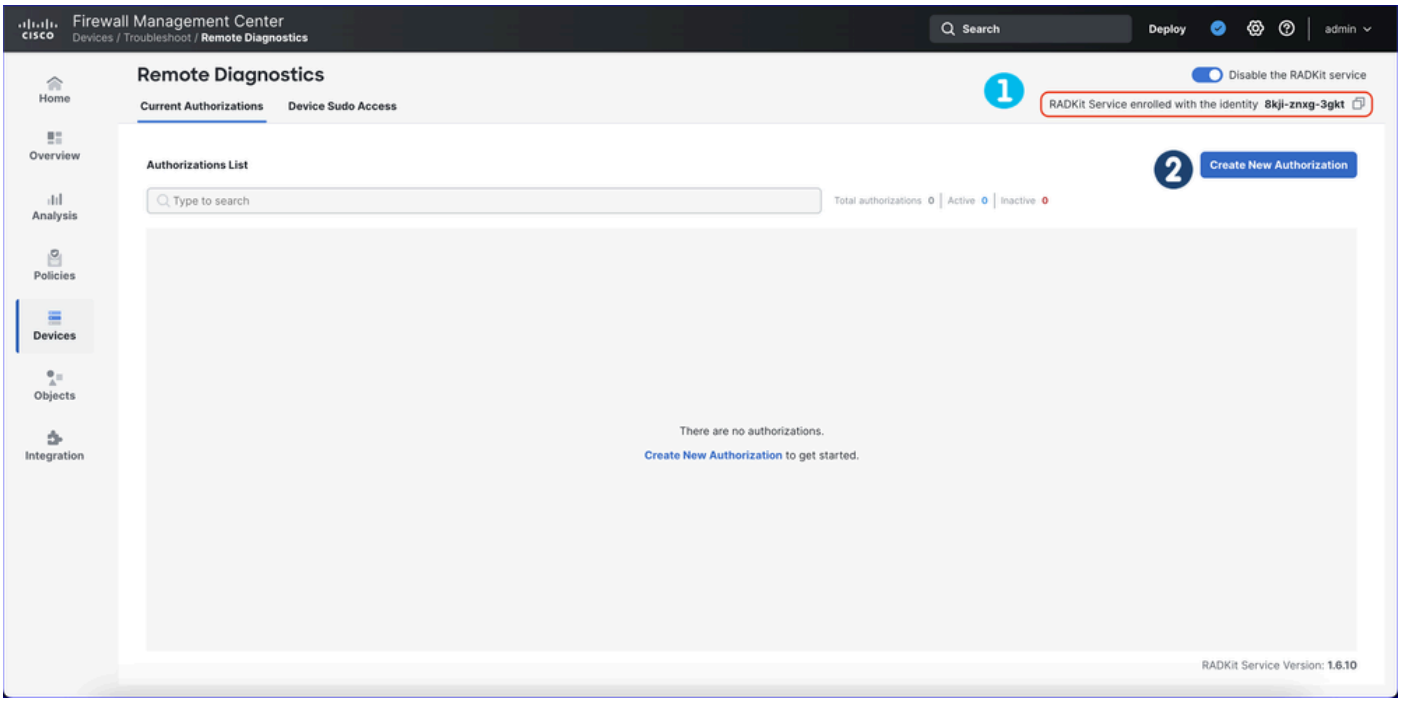
Dopo l'autenticazione, l'utente può chiudere la scheda del browser e tornare alla pagina Diagnostica remota FMC.



Servizio RADKit registrato

Il servizio RADKit è registrato con l'ID servizio specificato (in questo esempio l'ID è 8kji-znxg-3gkt). L'ID può essere copiato negli Appunti. Consegnarlo al tecnico Cisco TAC in modo che possa connettersi al servizio RADKit dal client RADKit.

Il passaggio successivo consiste nel creare un'autorizzazione facendo clic sul pulsante "Crea nuova autorizzazione":

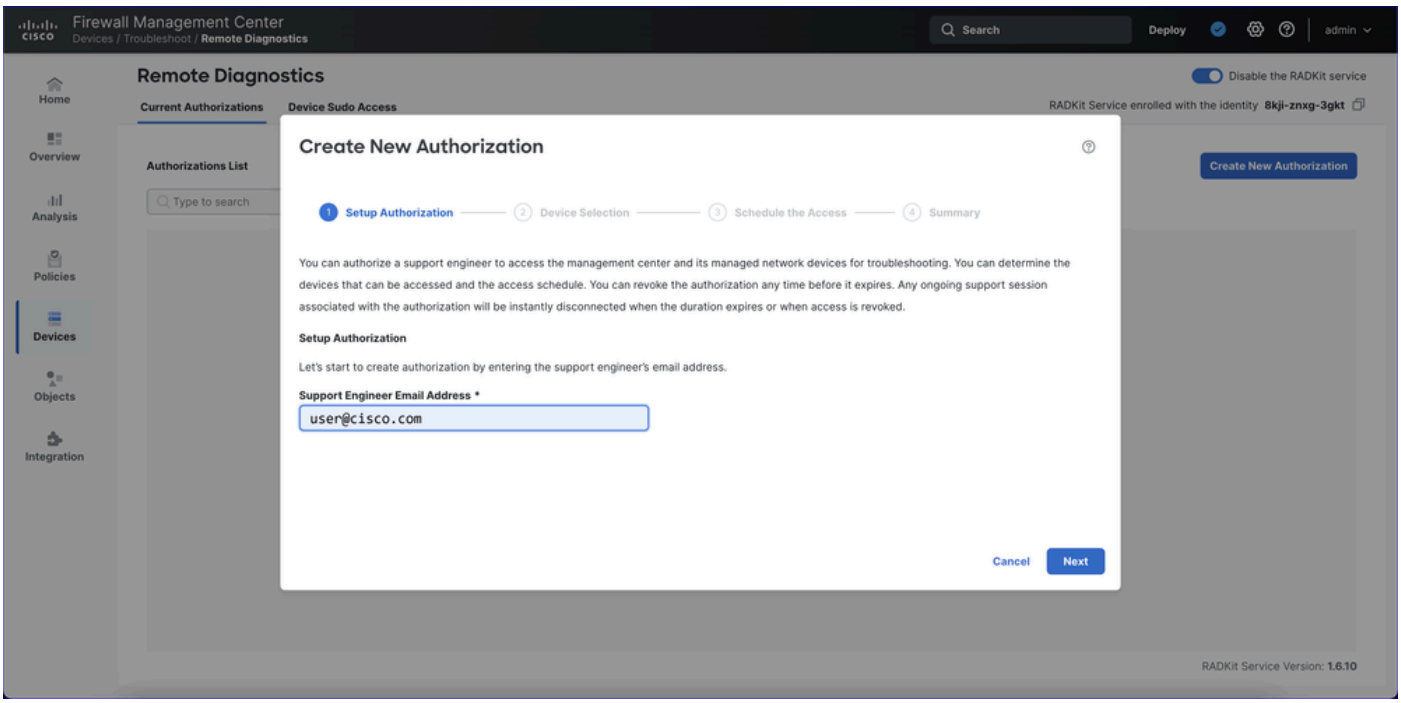


Crea nuova autorizzazione: Passaggio 1

- Per creare una nuova autorizzazione, il primo passaggio consiste nell'aggiungere l'indirizzo

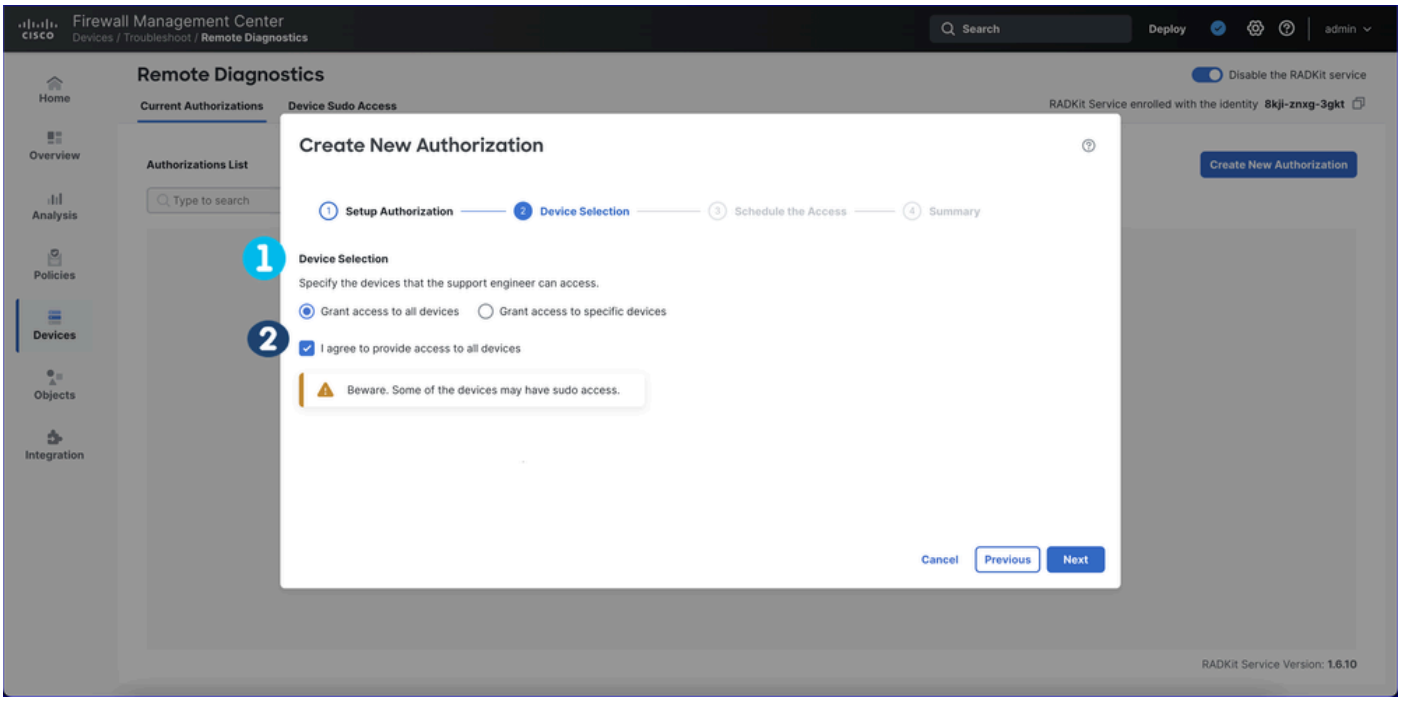
e-mail del tecnico di assistenza.

- Per creare una nuova autorizzazione, è necessario eseguire quattro passaggi. Lo stato di avanzamento dei passi viene visualizzato nella parte superiore.



Crea nuova autorizzazione: Passaggio 2

- Passaggio 1: Specificare i dispositivi a cui può accedere il tecnico dell'assistenza. Oppure, come nell'esempio, concedere l'accesso a tutti i dispositivi.
- Passaggio 2: Selezionare il pulsante di opzione per tutte le periferiche o per quelle specifiche. Per dispositivi specifici, è possibile scegliere i CCP e/o i FTD. Si noti l'avviso che l'accesso sudo può fornire ad alcune periferiche nella scheda Accesso sudo periferica. Il pulsante Avanti non viene abilitato finché la casella di controllo non viene selezionata.
- L'accesso Sudo viene fornito per dispositivo nella scheda Accesso Sudo dispositivo in seguito (non durante la creazione di un'autorizzazione).

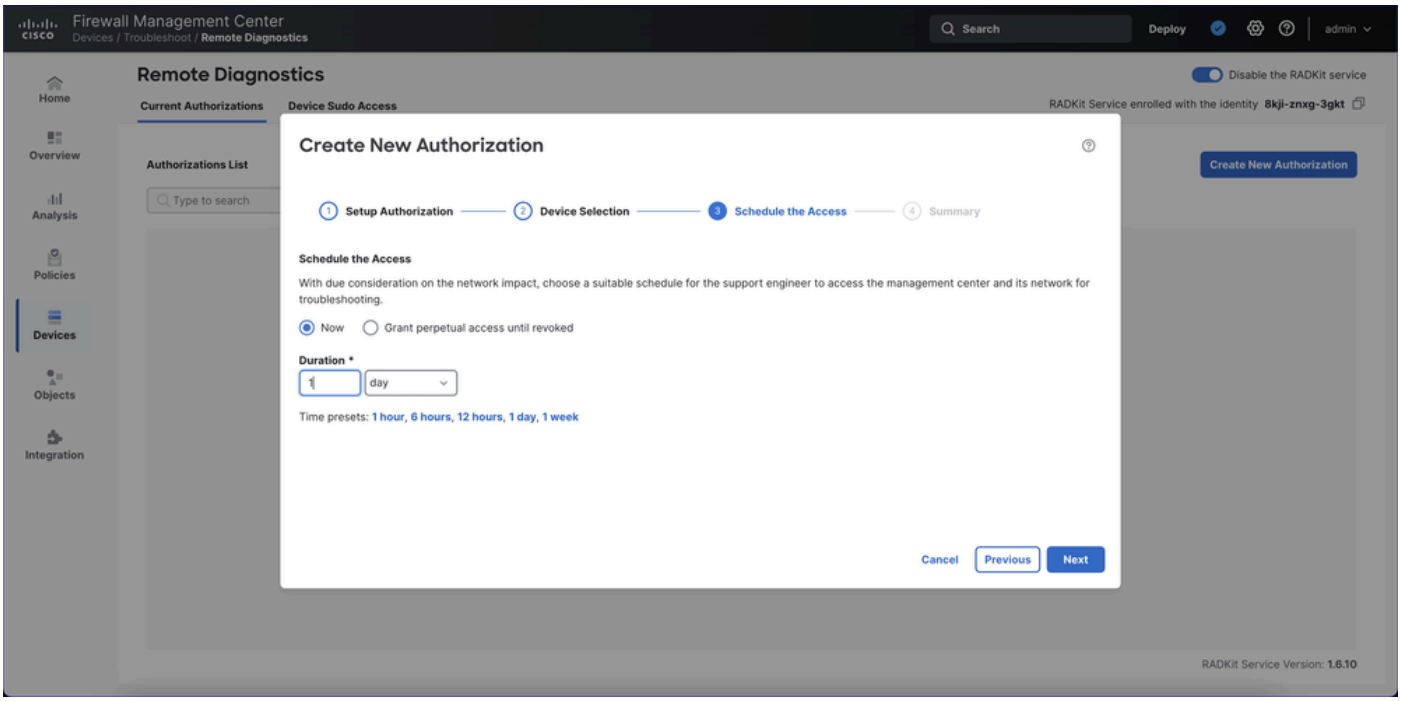


Note sul prelievo di dispositivi

- È possibile selezionare solo i dispositivi su una build supportata (ad esempio, nella versione iniziale, solo i dispositivi 7.7.0).
- I dispositivi disattivati e non raggiungibili non sono selezionabili. RADKit si basa su sftunnel (TCP 8305) per accedere ai dispositivi.
  - Se si verifica un problema di connettività del tunnel protetto, non funziona, ma viene comunque visualizzato nell'inventario RADKit.
  - Se un dispositivo è spento, non viene rilevato affatto.
- Se in una coppia HA sono presenti CCP, è possibile aggiungere solo i CCP attivi/primari.
- I dispositivi vengono aggiunti all'inventario RADKit quando si crea/modifica un'autorizzazione. Quando i dispositivi vengono cancellati dal FMC, vengono rimossi dall'"inventario" dei dispositivi.

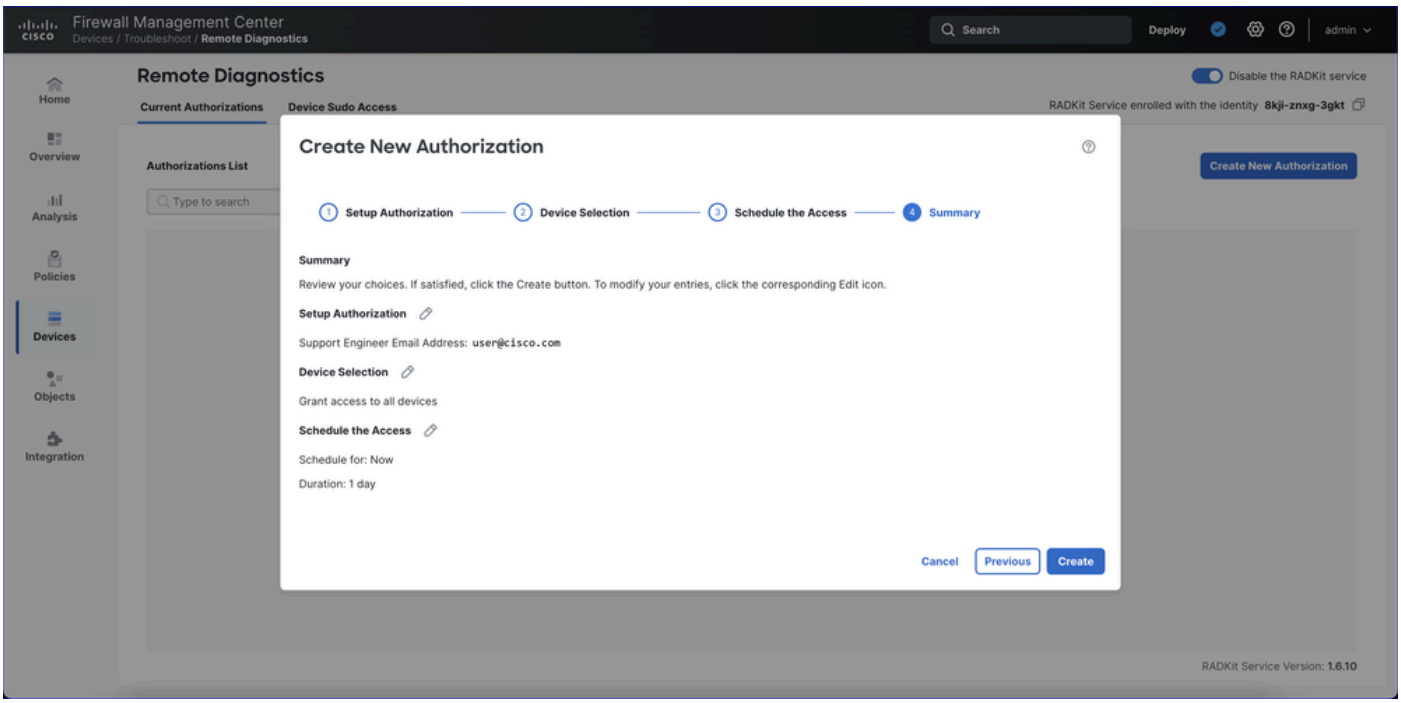
Crea nuova autorizzazione: Passaggio 3

- Passaggio 3: Specificare la durata per l'accesso ai dispositivi da parte del tecnico di supporto.
- Selezionare "Ora" e specificare una durata oppure
- Selezionare "Concedi accesso perpetuo fino alla revoca".
- La durata predefinita è 1 giorno. È possibile impostare qualsiasi durata; sono inoltre disponibili alcuni valori di durata predefiniti.



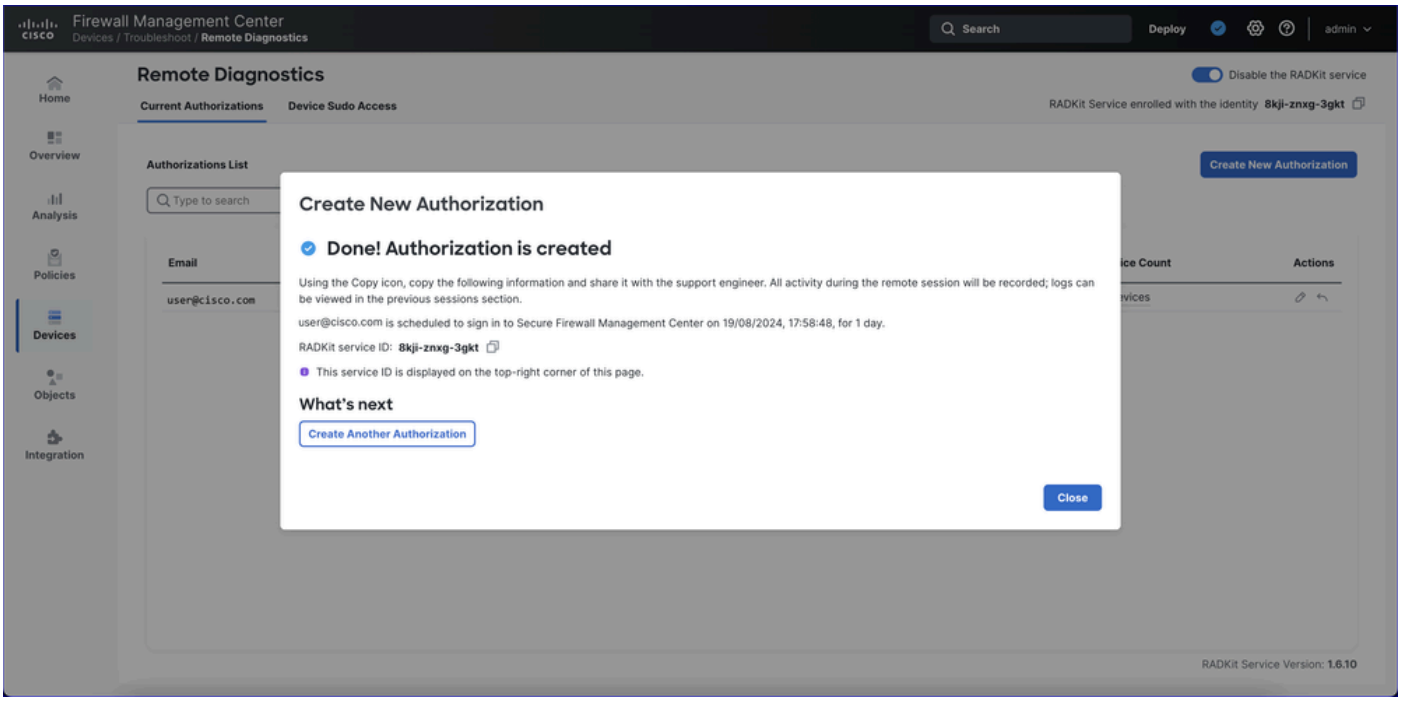
Crea riepilogo nuove autorizzazioni

La fase finale è il riepilogo dell'autorizzazione. L'utente può rivedere e modificare la configurazione.



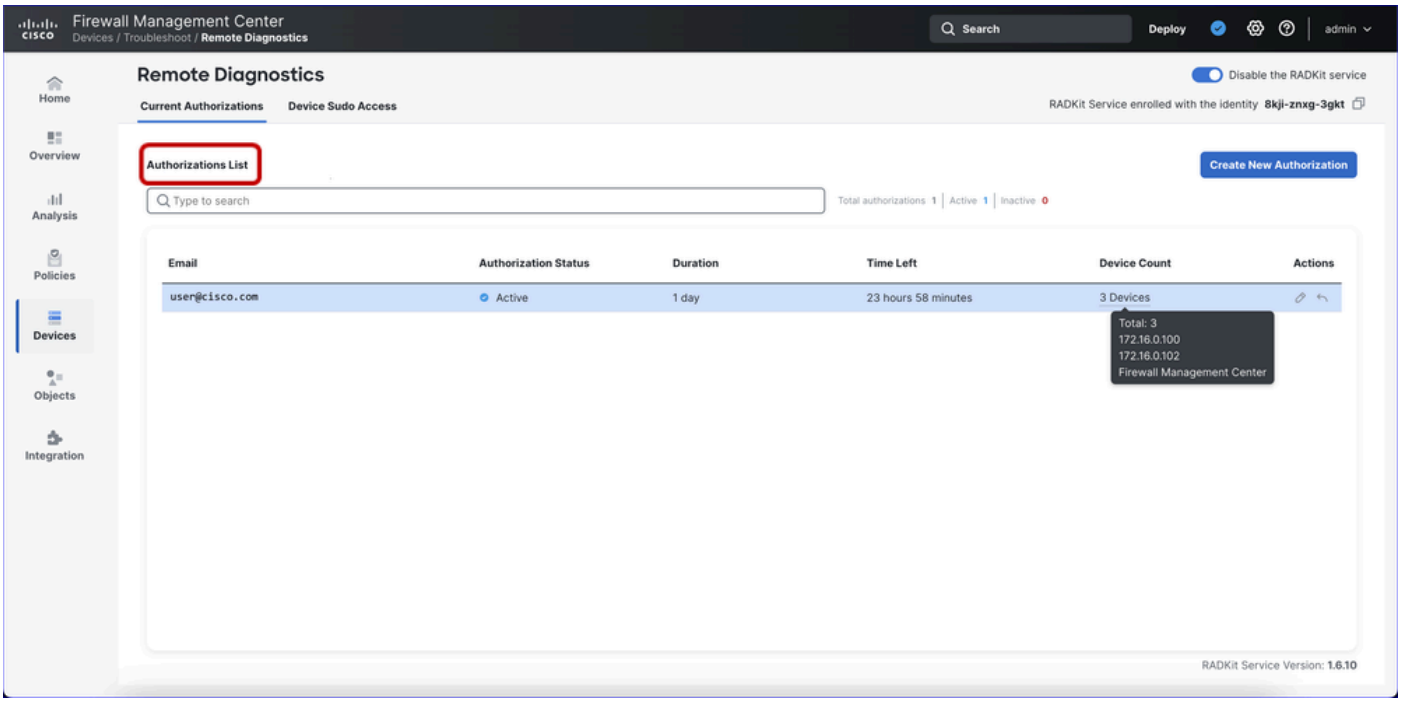
Creazione nuova autorizzazione completata

Al termine della creazione dell'autorizzazione viene visualizzata una schermata di conferma:



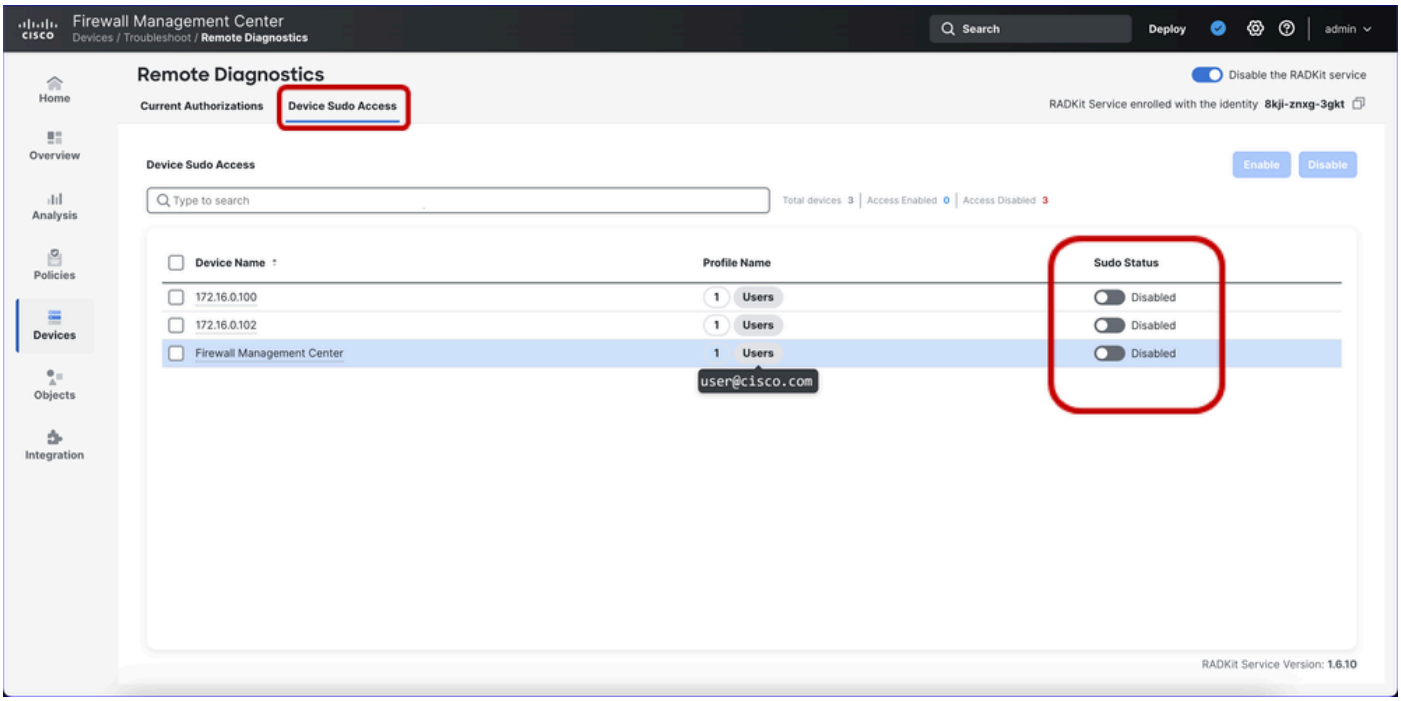
Elenco Autorizzazioni Correnti, Compresa La Revoca

- L'elenco delle autorizzazioni correnti viene visualizzato nella scheda Autorizzazioni correnti.
- Le Azioni (colonna a destra) sono Revoca accesso e Modifica autorizzazione.



Elenco accessi sudo dispositivo

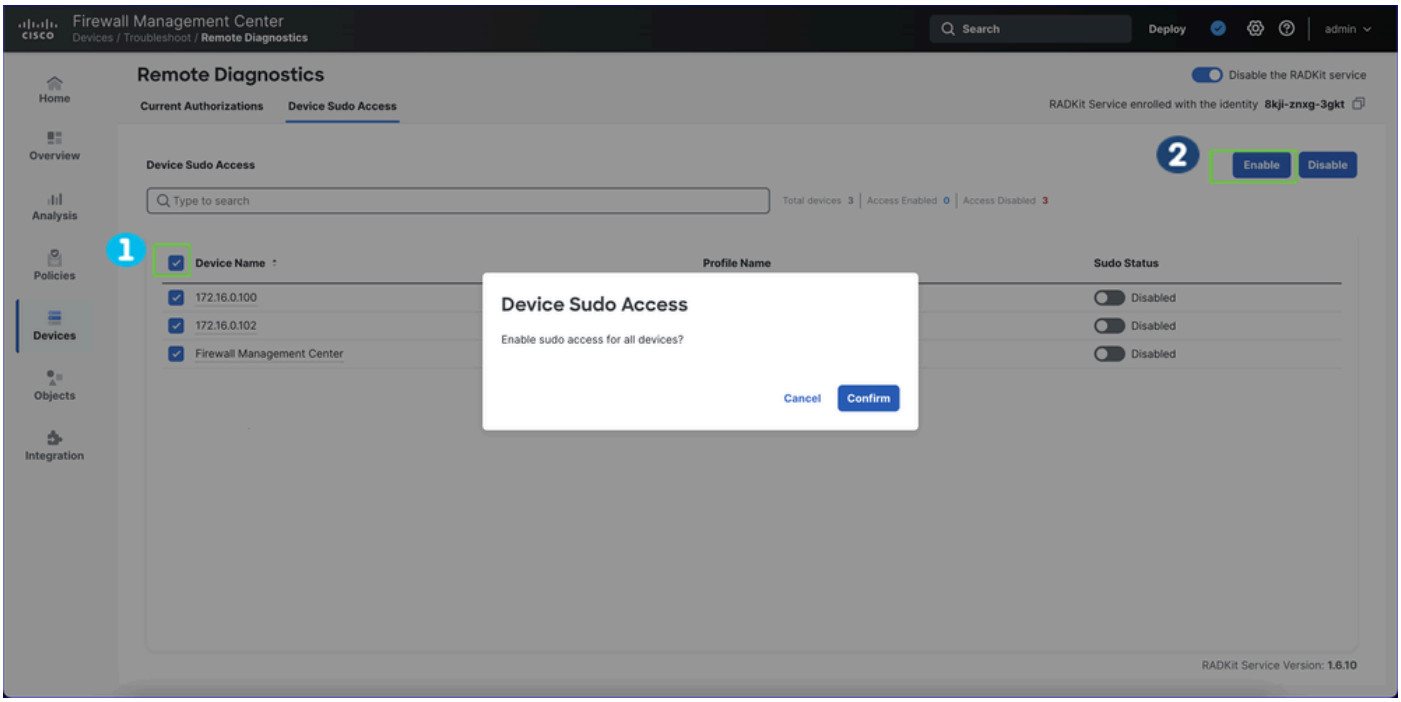
- L'elenco delle periferiche con impostazioni di accesso sudo è disponibile nella scheda Accesso sudo periferica.
- Utilizzare l'interruttore nella colonna a destra per attivare o disattivare l'accesso sudo. È disattivata per impostazione predefinita.
- Inoltre, è possibile abilitare o disabilitare in blocco l'accesso sudo.



Conferma abilitazione accesso sudo dispositivi

1. L'accesso sudo può essere abilitato per tutti o solo per alcuni dispositivi specifici selezionando i dispositivi e facendo clic sul pulsante "Abilita".

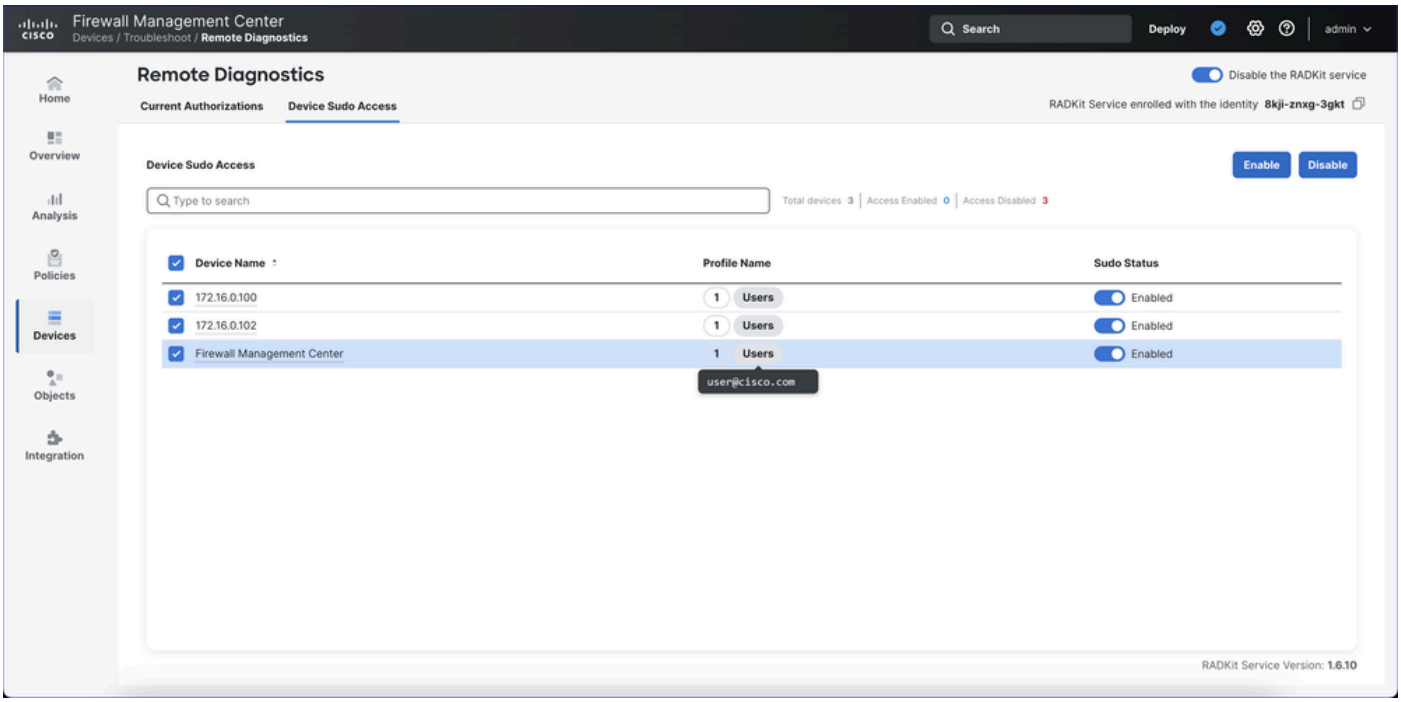
2. Quando si abilita, viene visualizzata una finestra di dialogo di conferma ed è necessario fare clic su Conferma.



Accesso sudo dispositivi abilitato

- Dopo aver attivato o disattivato l'accesso sudo per un dispositivo, la colonna Stato sudo sulla destra della pagina viene aggiornata.

- Il tecnico di supporto è in grado di eseguire sudo su sul dispositivo; questa è senza password. Il tecnico dell'assistenza non deve disporre della password di root.



Altre note

- Solo i dispositivi del dominio a cui l'utente FMC ha accesso sono visibili e possono essere autorizzati per l'accesso remoto.
- Se i CCP sono in HA:
  - Il servizio RADKit può essere abilitato solo su Active/Primary.
  - Impossibile aggiungere il CCP secondario attualmente come dispositivo a cui accedere dal client RADKit.
- L'autorizzazione può essere concessa a un solo tecnico di supporto alla volta.
  - Se è necessario l'accesso di un altro tecnico, creare un'altra autorizzazione per il tecnico aggiuntivo. L'ID servizio sarà lo stesso.

API REST FMC

API REST del servizio RADKit

Per supportare le operazioni di creazione e lettura sul servizio RADKit, sono stati introdotti i seguenti nuovi URL:

- SCARICA: /api/fmc_troubleshoot/v1/domain/{domainUUID}/radkit/services
  - Recupera tutti i dati del servizio RADKit da FMC.
- SCARICA: /api/fmc_troubleshoot/v1/domain/{domainUUID}/radkit/services/{id}
  - Recupera/recupera i dati del servizio RADKit dall'ID specificato.
- POST: /api/fmc_troubleshoot/v1/domain/{domainUUID}/radkit/services
  - Crea il servizio RADKit nel FMC (attiva/disattiva il servizio).

Modello di servizio RADKit

Il modello di servizio RADKit è costituito da:

- tipo
- ID
- stato
- èRegistrato
- ID servizio
- version


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


Supporto Cisco: Utilizzo client RADKit

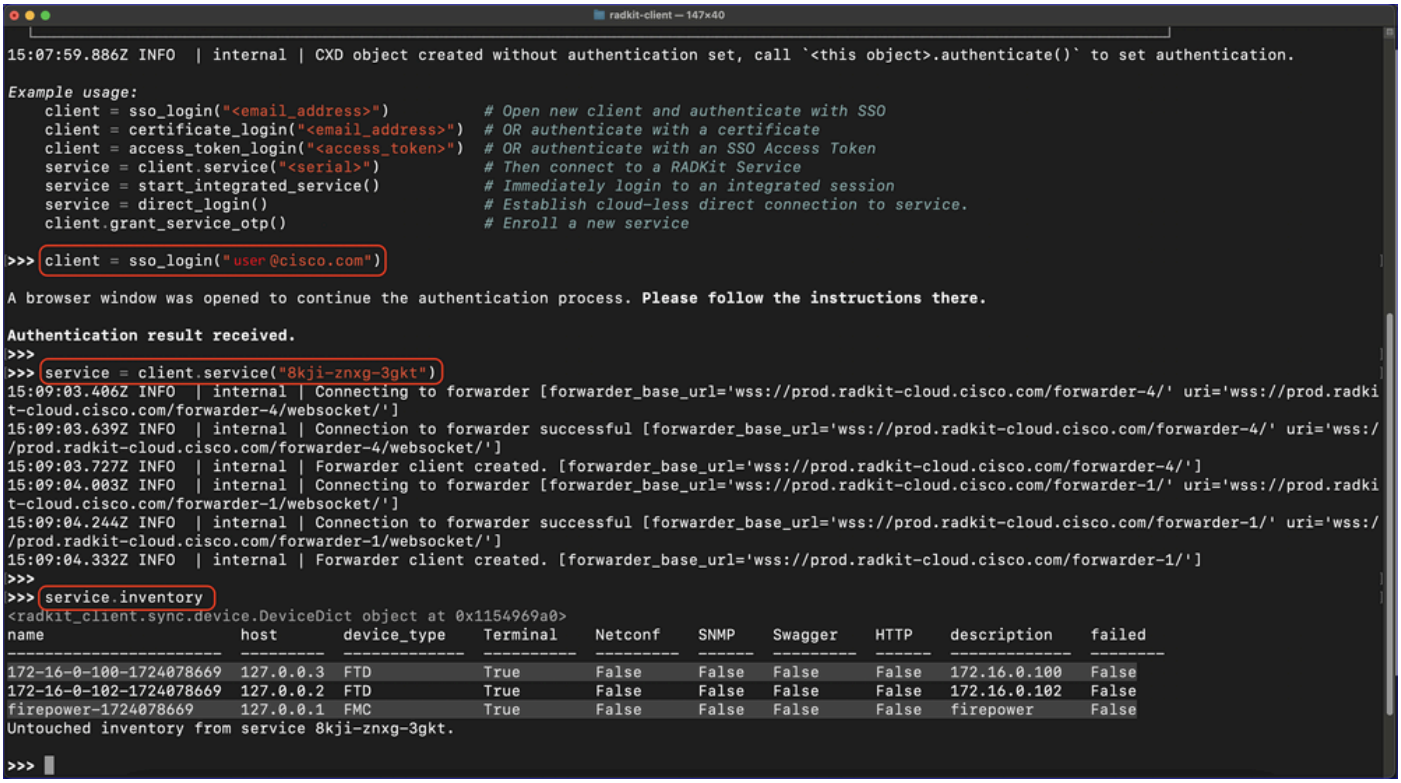
Lato supporto: Installare il client RADKit

- Per accedere al FMC/FTD, è necessario che il supporto disponga del client RADKit installato.
  - Il client funziona su sistemi operativi Windows, Mac e Linux.
- Il supporto può accedere a più dispositivi da più utenti. Ogni autorizzazione RADKit ha il proprio "inventario" di dispositivi.
  - Per ogni inventario di dispositivi utente che il supporto desidera accedere, è necessario l'ID servizio RADKit.
  - Per un singolo inventario, l'accesso è possibile sia per il CCP che per i relativi FTD gestiti dal client RADKit, come specificato dall'utente al momento dell'autorizzazione dell'accesso.

Ottenere e installare il client RADKit

Il client RADKit può essere installato localmente da https://radkit.cisco.com/downloads/release/ e quindi avviato dal terminale con il comando: radkit-client

Sono disponibili programmi di installazione per Windows, MacOS e Linux.



Schermata del client RADKit con i comandi di login (dettagli nella sezione successiva).

Comandi di login per il client RADKit

- Utilizzare l'indirizzo di posta elettronica immesso dall'utente durante l'autorizzazione in FMC.
- Accesso del client RADKit e connessione ai comandi ID servizio specificati. L'ID del servizio RADKit, in questo esempio 8abc-znxg-3abc, deve corrispondere a quello rilevato dall'amministratore del firewall 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
```

Comando di inventario servizio client RADKit

Comando per la creazione di un elenco dell'inventario a cui l'utente remoto (Cisco TAC engineer) è autorizzato ad accedere:

```
<#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.
```

È disponibile un comando di filtro per i dispositivi nell'inventario (sezione successiva). Utilizzare il nome nella colonna a sinistra per avviare una sessione interattiva con il dispositivo (comando nella sezione successiva).

Suggerimento: Se l'inventario è obsoleto, è possibile aggiornarlo utilizzando il comando: **>>>** service.update_inventory()

Client RADKit: Filtra dispositivi

Comando per filtrare i dispositivi nell'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 sessione interattiva dispositivo client RADKit

Avvio di una sessione interattiva per un dispositivo (in questo caso un FMC) denominato "firepower-1724078669", tratto dal precedente comando "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)
```

Comandi di esecuzione client RADKit sui dispositivi

Eseguire i comandi sui dispositivi.

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

Ottieni ulteriori dettagli dai dispositivi

Considerando questo 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
```

Per ottenere i dettagli di 'show version' dai dispositivi 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
```

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

>
```

Metodo 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
----------------------------------------------------
```

Recupero di file dai dispositivi

- Tramite il client RADKit, un tecnico Cisco TAC può eseguire il protocollo SSH sui dispositivi ed eseguire diverse operazioni, tra cui la generazione di file per la risoluzione dei problemi.

Supporto Cisco: Console RADKit

Utilizzo della console di rete RADKit

- In alternativa all'uso del client RADKit, un tecnico di assistenza Cisco TAC potrebbe usare la console di rete RADKit. Network Console fa parte del client RADKit.
- La console di rete RADKit è una funzione che fornisce una semplice interfaccia a riga di comando (CLI) per le funzioni di base del client RADKit. È destinato a essere utilizzato per una connettività rapida a un'istanza del servizio RADKit, stabilendo sessioni interattive e scaricando/caricando file senza problemi e con una formazione minima.
- Avviare Network Console dalla riga di comando: radkit-network-console
- Per ulteriori informazioni, consultare la documentazione di RADKit.

Compatibilità con aggiornamenti e versioni precedenti

Aggiornamento a 7.7 e da 7.7 in su

- Il servizio RADKit è stato aggiunto in Secure Firewall 7.7.0.
    - I dispositivi aggiornati alla versione 7.7.0+ dispongono della configurazione necessaria per il servizio RADKit.

Esperienza con FTD non supportati

- Affinché questa funzione funzioni, i CCP e i FTD devono avere la versione minima 7.7.0 (i FTD con versione inferiore alla 7.7 non possono essere aggiunti a un'autorizzazione RADKit del CCP 7.7).
- Gli FTD registrati non disponibili in 7.7.0 non possono essere prelevati per l'abilitazione dell'autorizzazione.

Risoluzione dei problemi

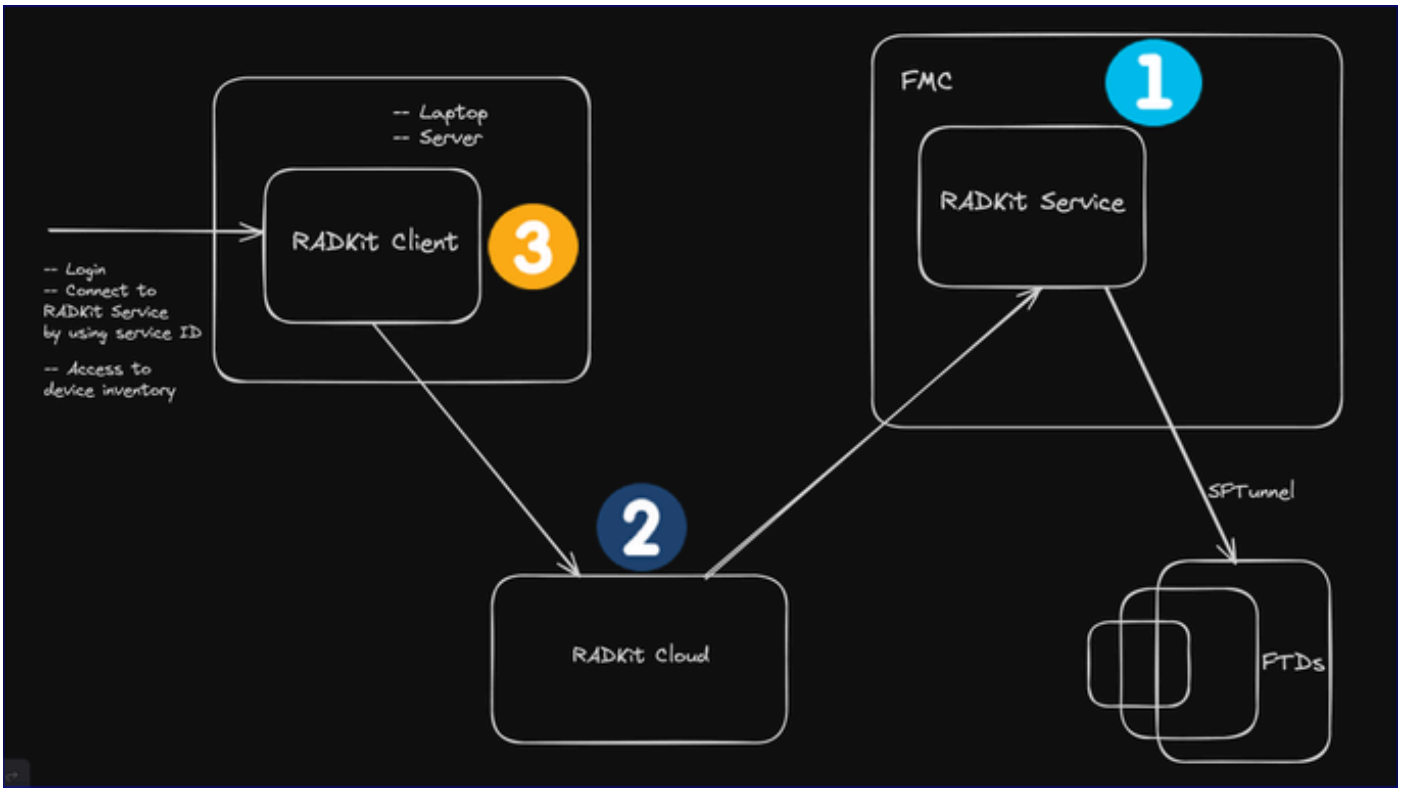
Panoramica sulla diagnostica

Punti di risoluzione dei problemi

1. Utilizzare gli strumenti di sviluppo del browser e i registri FMC per visualizzare gli eventi in corso in FMC.

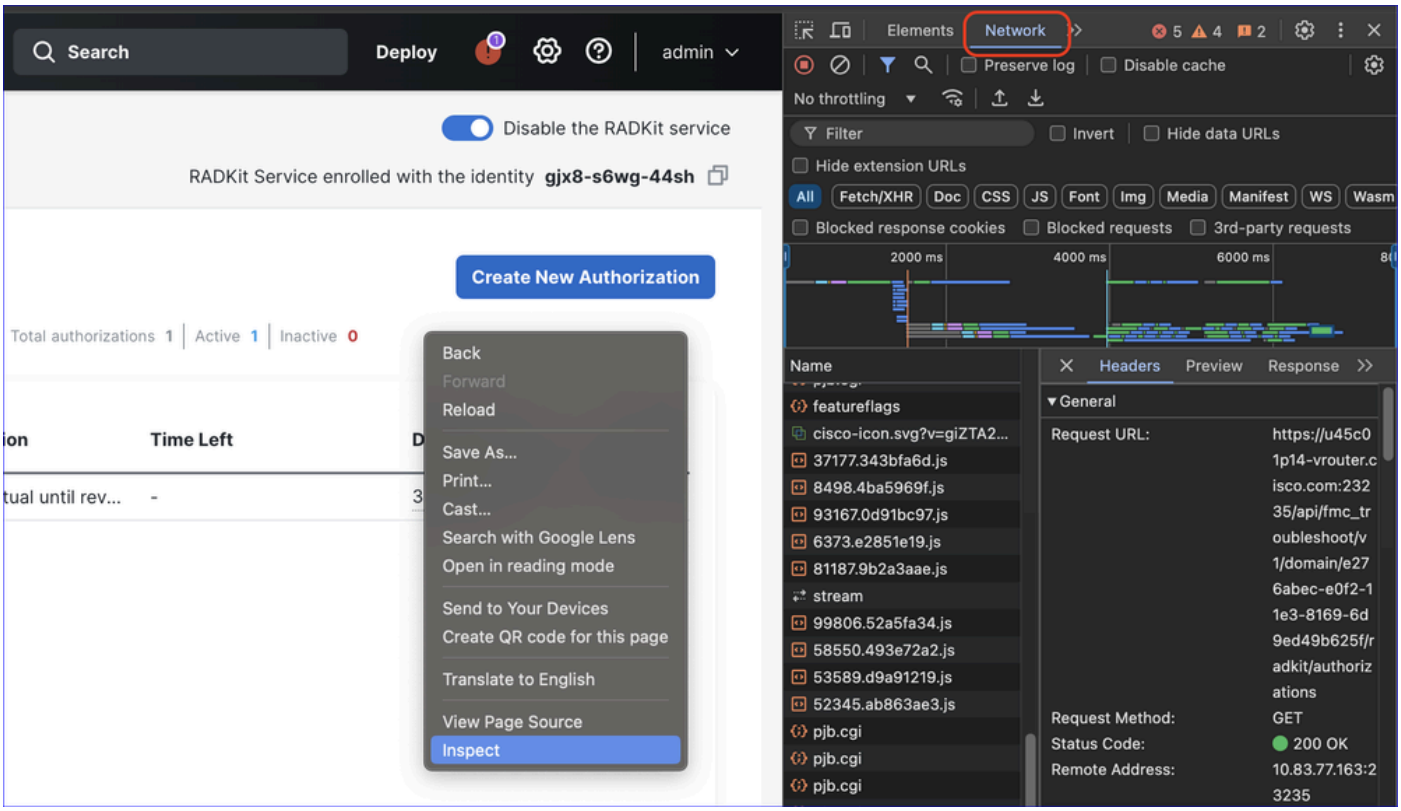
2. Per i problemi di comunicazione tra il servizio RADKit su FMC, RADkit Cloud e il client RADKit, consultare la registrazione del client RADKit.

3. Client RADKit.



Come risolvere i problemi: Strumenti di sviluppo del browser

- La scheda Strumenti di sviluppo del browser, Rete, mostra le chiamate API eseguite nella pagina, che possono essere utilizzate per la risoluzione dei problemi in FMC. Per avviare questa procedura, fare clic con il pulsante destro del mouse sulla pagina, quindi fare clic su Ispeziona.
- Controllare il codice di stato della chiamata API e l'anteprima della risposta nella scheda Rete.



API Go Middleware del servizio RADKit

Go Middleware per l'integrazione RADKit utilizza chiamate API non disponibili pubblicamente tramite FMC API explorer. Il registro API Go Middleware è disponibile in /var/log/auth-daemon.log. Funzionalità Le prestazioni di Go Middleware includono:

- Registrare il servizio RADKit nel cloud RADKit con il processo Single Sign-On.
- Recuperare un elenco di tutte le autorizzazioni degli utenti RADKit remoti e dei dispositivi associati.
- Recupera un'autorizzazione utente RADKit remota specifica e i dispositivi associati tramite un messaggio di posta elettronica.
- Creare un'autorizzazione utente RADKit remota e concedere le autorizzazioni per accedere ai dispositivi (tutti i dispositivi o un elenco di dispositivi selezionati) per un intervallo di tempo specificato.
- Modifica un'autorizzazione utente RADKit remota.
- Elimina un'autorizzazione utente RADKit remota.

Registri per la risoluzione dei problemi del servizio RADKit

- Registri FMC generali: comando pigtail da una sessione ssh del CCP.
- API Go Middleware: /var/log/auth-daemon.log
- I registri contenenti RADKit e il daemon di autenticazione elaborano i dati:

/var/log/process_stdout.log

/var/log/process_stderr.log

Tutti questi registri sono inclusi nella risoluzione dei problemi FMC/FTD.

- Registri del servizio RADKit interno: /var/lib/radkit/logs/service/
- Registri delle operazioni eseguite dal client RADKit sui dispositivi (FMC e FTD): /var/lib/radkit/session_logs/service

Log da inviare a Cisco TAC

- Screenshot degli errori.
- Descrizione del problema.
- Passi da riprodurre.
- Pigtail e /var/log/auth-daemon.log log estratti contenenti gli errori.

Monitoraggio dell'accesso

Nei registri di verifica del CCP è riportata la registrazione di chi ha ottenuto l'accesso per quanto tempo e di chi l'ha concesso.

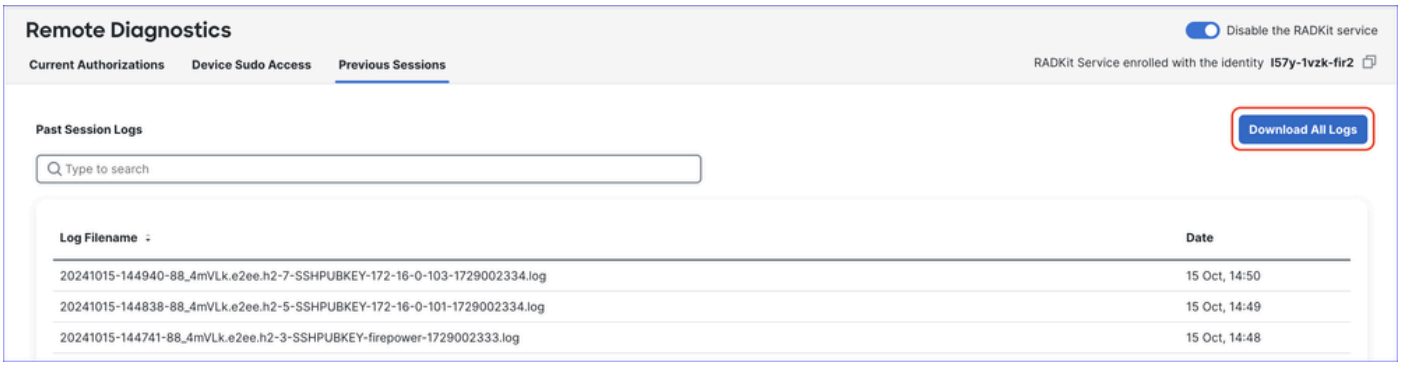
Registri sessione RADKit

I registri di sessione RADKit per le operazioni eseguite dal client RADKit sui dispositivi (FMC e FTD) sono presenti sul FMC all'indirizzo /var/lib/radkit/session_logs/service:

- I registri provengono dal servizio RADKit stesso.
- Questi registri sono inclusi in un pacchetto di risoluzione dei problemi.
- I registri sono accessibili anche dall'interfaccia utente (vedere la sezione successiva).
- Sono presenti più file di log della sessione. uno per sessione.

Radkit log sessioni precedenti

I log delle sessioni RADKit per le operazioni sui dispositivi eseguite dal client RADKit sono disponibili per il download come archivio contenente tutti i log nella scheda Sessioni precedenti facendo clic sul pulsante "Scarica tutti i log".



Esempio di problema con la risoluzione dei problemi Procedura dettagliata

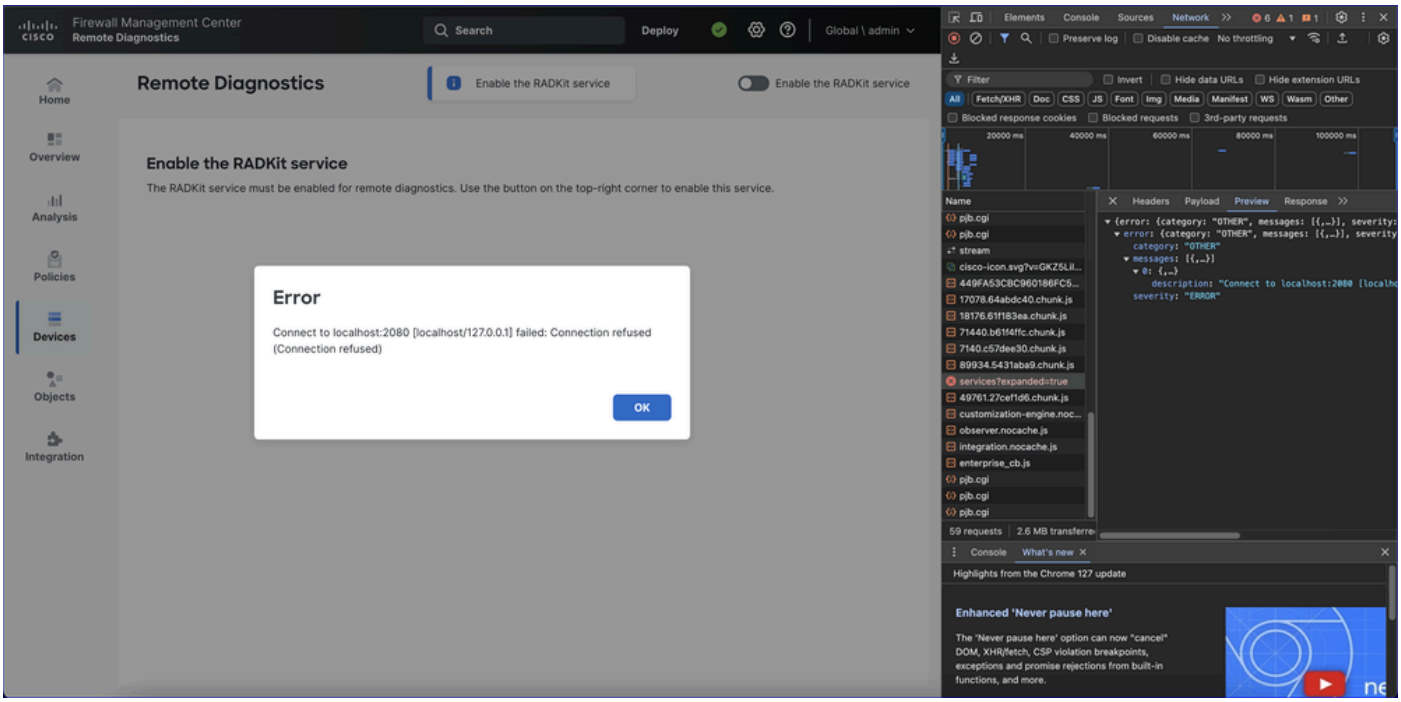
Esempio di risoluzione dei problemi

In caso di errore come "Connect to localhost:2080 [localhost/127.0.0.1] failed: Connessione rifiutata (connessione rifiutata)", provare a riavviare il daemon di autenticazione da una sessione SSH del FMC:

<#root>

root@firepower:~$

sudo pmtool restartbyid auth-daemon



Telemetria

L'output di telemetria è stato aggiunto per questa funzionalità:

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

Domande frequenti

Domande frequenti: Accesso e registrazione

D. L'iscrizione funziona con il proxy se FMC non dispone di accesso diretto a Internet?

R. Sì, se il proxy ha accesso a prod.radkit-cloud.cisco.com, utilizzato per il processo di iscrizione.

D. Un utente può utilizzare il proprio IdP per questo servizio?

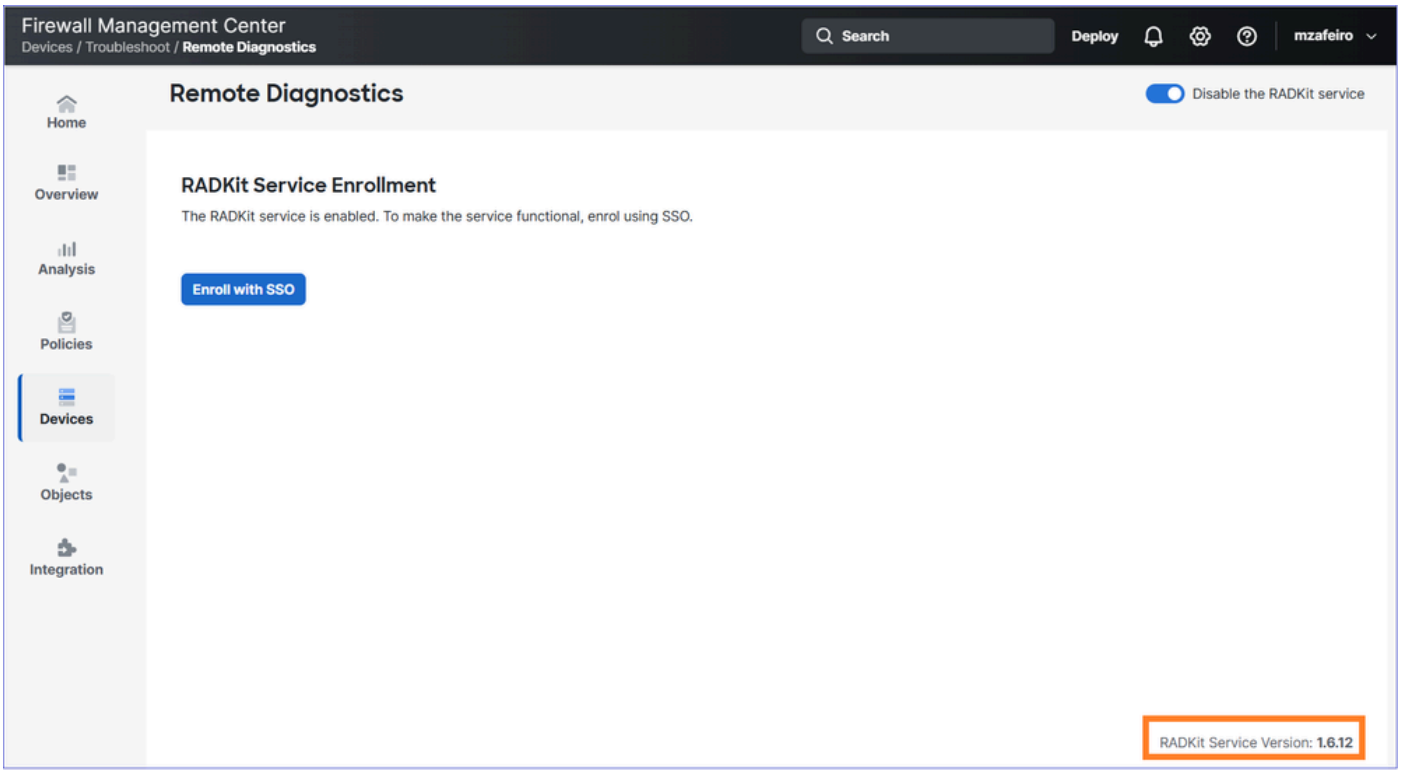
R. Solo Cisco SSO è accettato sul cloud RADKit. È possibile associare l'account della società a un account Cisco, in modo che la registrazione al servizio RADKit sia possibile con un'e-mail di terze parti.

Domande frequenti: Versioni RADKit

D. Quale versione di RADkit è inclusa in FMC nella versione 7.7? Come possiamo sapere quale versione di RADKit è inclusa nel FMC? Può essere aggiornato senza l'aggiornamento del FMC?

R.

- La versione di RADKit fornita con 7.7.0 è 1.6.12.
- La versione del servizio RADKit è visualizzata nella parte inferiore della pagina Diagnostica remota FMC: "Versione servizio RADKit: 1.6.12."



- RADKit è fornito con pacchetti/aggiornamenti rapidi di FMC. L'aggiornamento del servizio RADKit in FMC separatamente non è supportato.

Domande frequenti: Other (Altro)

D. È possibile includere dispositivi esterni non gestiti dal CCP?

R. Solo i dispositivi gestiti dal FMC possono essere aggiunti all'inventario RADKit e quindi essere accessibili tramite un'autorizzazione.

D. La configurazione RADKit viene sottoposta a backup come parte del backup FMC?

R.

- Il backup della configurazione non viene eseguito come parte del backup di FMC.
- Non viene sostenuta in quanto prevediamo che, in generale, l'accesso perpetuo non sarà garantito; l'accesso è in genere limitato nel tempo.

Riferimenti

Collegamenti utili:

- Guida alla configurazione di 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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).