

# RADKit voor externe probleemoplossing instellen op HyperFlex

## Inhoud

---

[Inleiding](#)

[Achtergrondinformatie](#)

[Wat is RADKit?](#)

[Waarom RADKit voor HX?](#)

[RADKit vs. Intersight](#)

[Overzicht op hoog niveau](#)

[Connectiviteitsdiagram](#)

[Componenten](#)

[Vorbereiding](#)

[Overzicht van te volgen stappen](#)

[Stap 1. De RADKit-service downloaden en installeren](#)

[Stap 2. Start de RADKit-service en voer de Initial Setup \(Bootstrap\) uit](#)

[Stap 3. Meld je RADKit Service aan bij RADKit Cloud](#)

[Stap 4. Apparaten en endpoints toevoegen](#)

[RADKit gebruiken op een TAC SR](#)

[1. Geef RADKit-service-id op](#)

[2. Externe gebruiker toevoegen](#)

[Gerelateerde informatie](#)

---

## Inleiding

Dit document beschrijft hoe u een RADKit-omgeving kunt starten en voorbereiden voor het oplossen van problemen op afstand in een Cisco HyperFlex-omgeving.

## Achtergrondinformatie

Het belangrijkste doel van dit document is om uit te leggen hoe u uw omgeving kunt voorbereiden voor gebruik door TAC om RADKit te gebruiken voor probleemoplossing.

### Wat is RADKit?

RADKit is een netwerkbrede orkestrator. Ontdek een innovatieve nieuwe aanpak voor uw apparatuur, verbeter uw Cisco-services en breid uw mogelijkheden uit.

Meer informatie over RADKit vindt u hier: <https://radkit.cisco.com/>

## Waarom RADKit voor HX?

Cisco HyperFlex bestaat uit verschillende componenten: Fabric Interconnects, UCS Servers, ESXi, vCenter en SCVM's. In veel gevallen moet informatie uit verschillende apparaten worden verzameld en gecorreleerd. Terwijl het oplossen van problemen, kan nieuwe informatie in tijd worden vereist en het doen van dit over een (lange) zitting Webex of door (grote) steunbundels door Intersight te halen is niet altijd de meest efficiënte manier. Met behulp van RADKit kan een TAC engineer tijdens het probleemoplossingsproces op een veilige en gecontroleerde manier de benodigde informatie opvragen bij de verschillende apparaten en services.

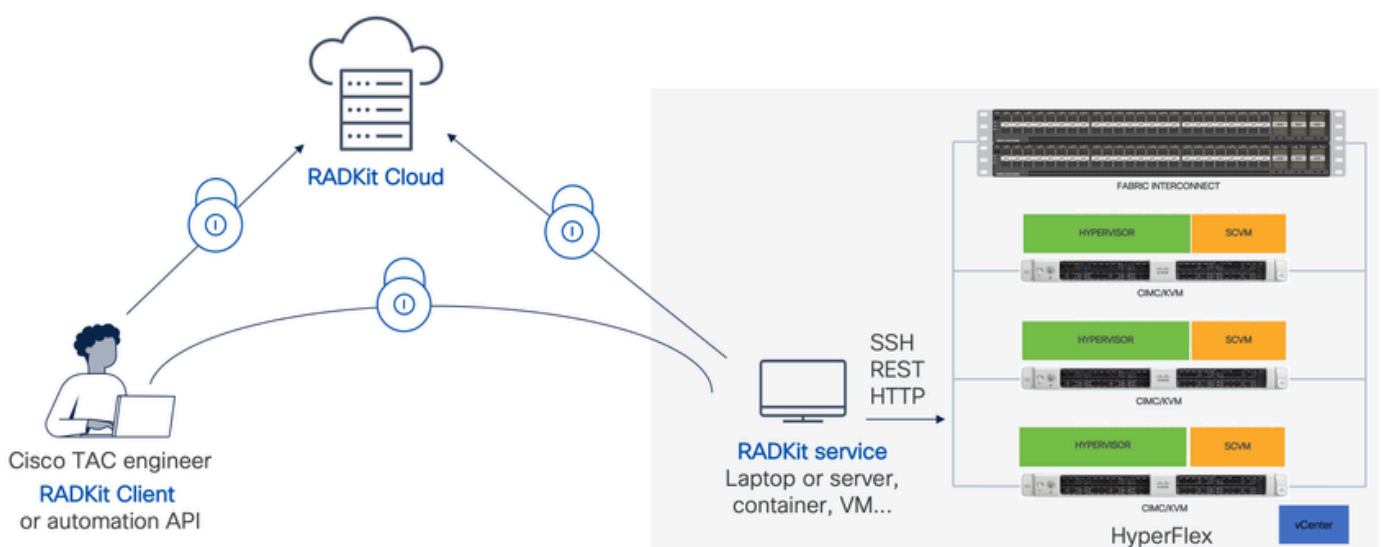
## RADKit vs. Intersight

Intersight blijft de primaire connectiviteitsmethode voor HyperFlex-clusters, die talrijke voordelen biedt zoals automatische logboekverzameling, telemetrie en proactieve bewaking van uw omgeving voor hardware en andere bekende waarschuwingen.

Hoewel veel HX-clusters zijn verbonden met Intersight, is Intersight momenteel voornamelijk bedoeld voor de implementatie, het onderhoud en de bewaking van uw HyperFlex-clusters. Intersight staat de capaciteit toe om steunbundels en telemetrie-informatie te verzamelen, die typisch een goed uitgangspunt voor het oplossen van problemen is. Voor live probleemoplossing, waarbij een TAC engineer in een klassiek scenario een Webex-sessie zou gebruiken, komt RADKit op zijn plaats. Het vervangt Intersight niet, maar voegt een andere benadering van probleemoplossing toe, door gebruik te maken van een interactieve sessie of door gebruik te maken van programmatische request-response sequenties.

## Overzicht op hoog niveau

### Connectiviteitsdiagram



### Componenten

- RADKit Service: RADkit-servicecomponent op locatie, die wordt gebruikt als een veilige gateway naar uw HX-omgeving. Als klant behoudt u de volledige controle over welke apparaten toegankelijk zijn en wie ze op welk moment kan gebruiken. Deze service kan worden gehost op elke Linux, MacOS of Windows machine.
- RADKit client: front-end gebruikt door de TAC engineer om toegang te krijgen tot uw omgeving, met behulp van programmatische probleemoplossing en bewaking, geautomatiseerde ophalen en analyse van apparaatuitgangen met behulp van Cisco-interne tools of directe interactie met de apparaten via CLI.
- RADKit Cloud: Biedt veilig transport tussen de klant en de service.

## Vorbereiding

### Overzicht van te volgen stappen

Deze stappen zijn vereist voordat een TAC engineer RADKit kan gebruiken om verbinding te maken met uw HX-omgeving en problemen op te lossen:

1. Download en installeer de RADkit service. Het kan worden geïnstalleerd op elke Linux, MacOS of Windows machine.
2. Start de RADKit-service en voer de eerste configuratie uit (bootstrap). Maak een super admin-account aan om de RADKit-service verder te beheren via een webinterface.
3. Meld je RADKit aan bij de RADKit cloud. Registreer uw RADKit-service met de RADKit-cloud en genereer een service-ID om uw omgeving te identificeren.
4. Voeg apparaten en endpoints toe. Geef een lijst op van apparaten en sla referenties op voor apparaten die mogelijk toegankelijk moeten worden gemaakt.

Een meer gedetailleerde/algemene uitleg van deze stappen vindt u hier:

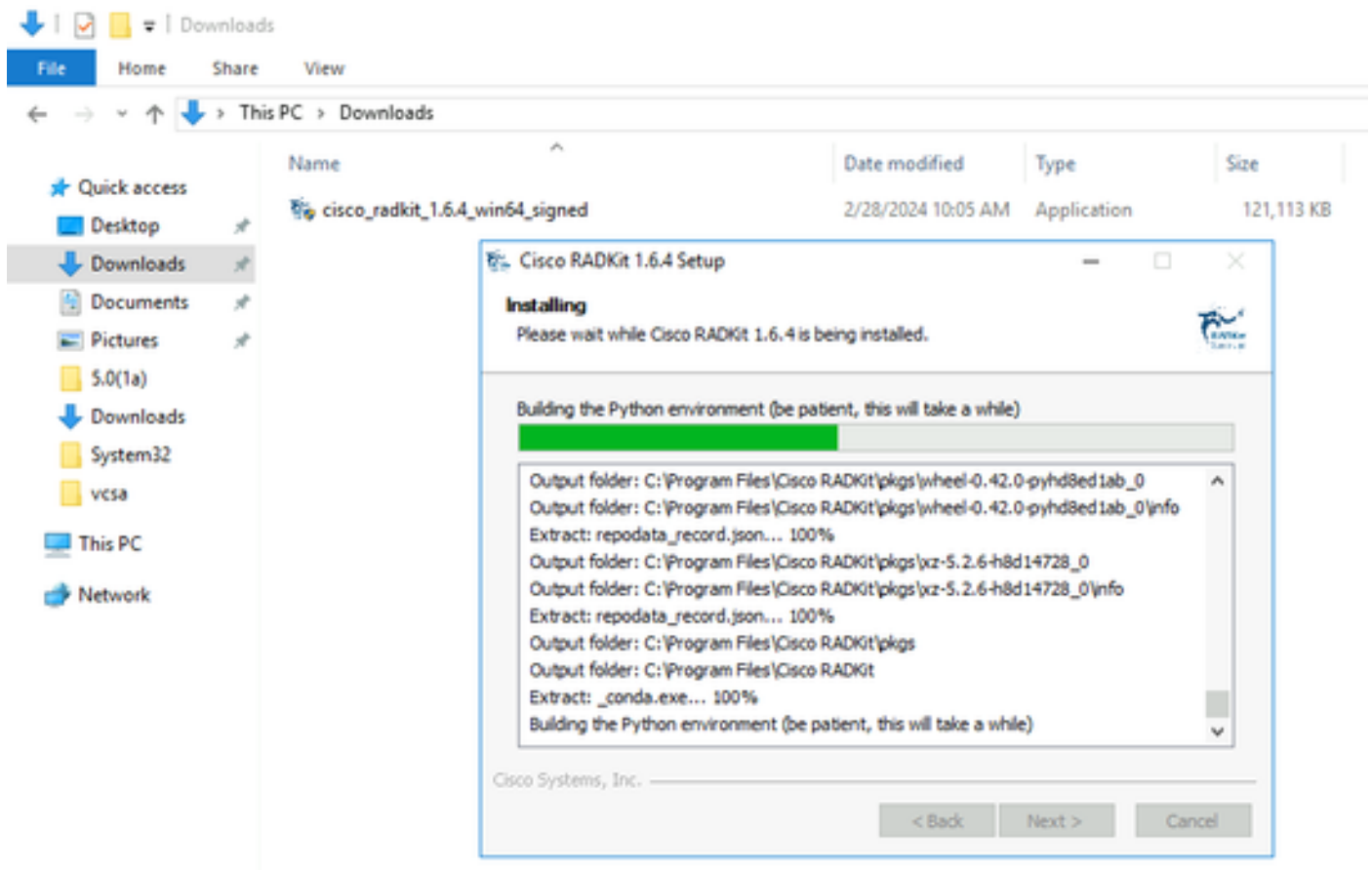
[https://radkit.cisco.com/docs/pages/one\\_page\\_setup.html](https://radkit.cisco.com/docs/pages/one_page_setup.html)

### Stap 1. De RADKit-service downloaden en installeren

De details in deze stap kunnen een beetje anders zijn, afhankelijk van welk besturingssysteem u gebruikt om de RADKit-service te installeren, maar in het algemeen is het proces zeer vergelijkbaar. Download hier de nieuwste release voor uw besturingssysteem:

<https://radkit.cisco.com/downloads/release/>.

Voer het installatieprogramma voor uw systeem uit en volg de aanwijzingen totdat de installatie is voltooid:

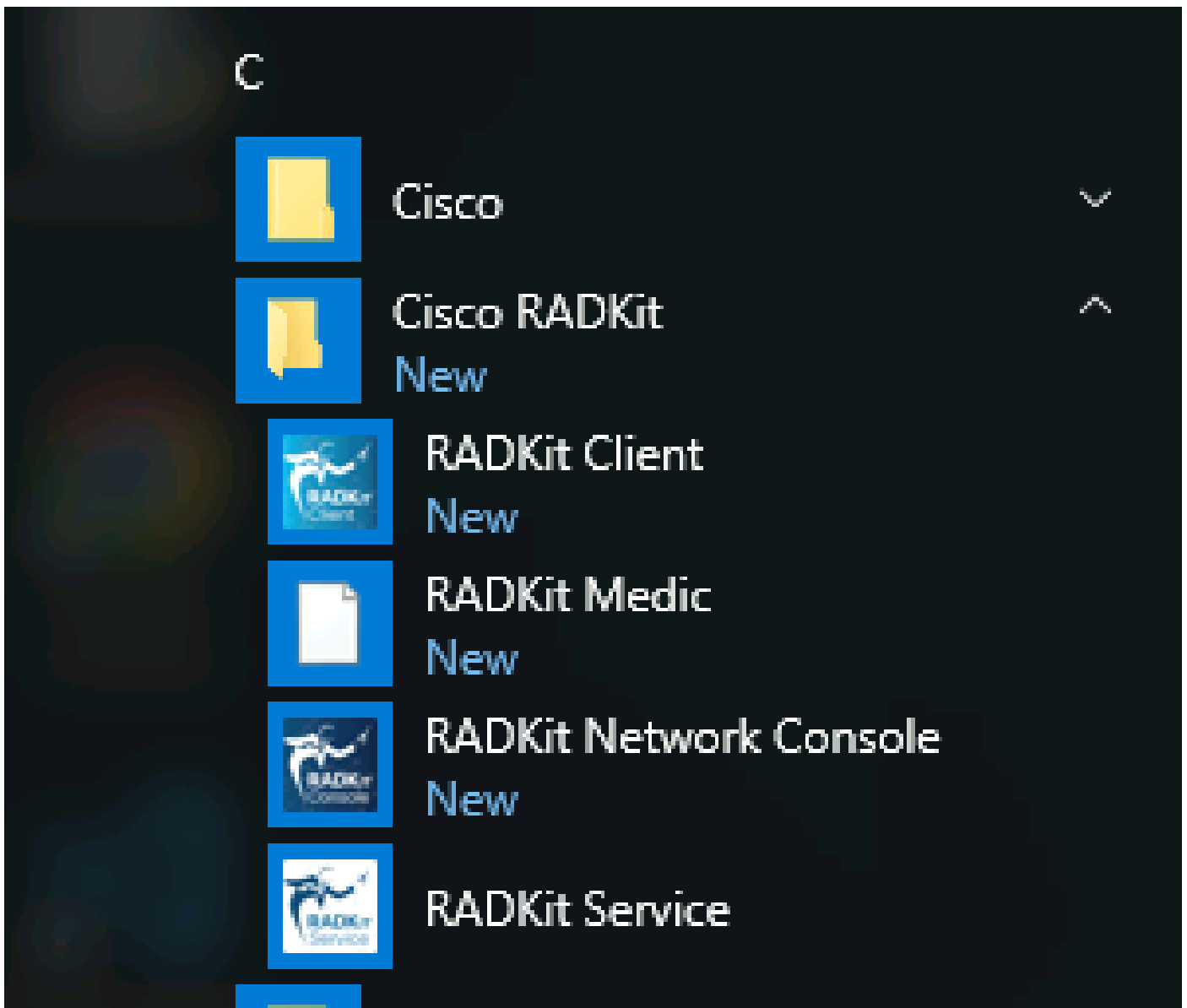


Nadat alle RADKit-componenten zijn geïnstalleerd, kunt u doorgaan naar de volgende stap waar u door de eerste setup gaat.

## Stap 2. Start de RADKit-service en voer de Initial Setup (Bootstrap) uit

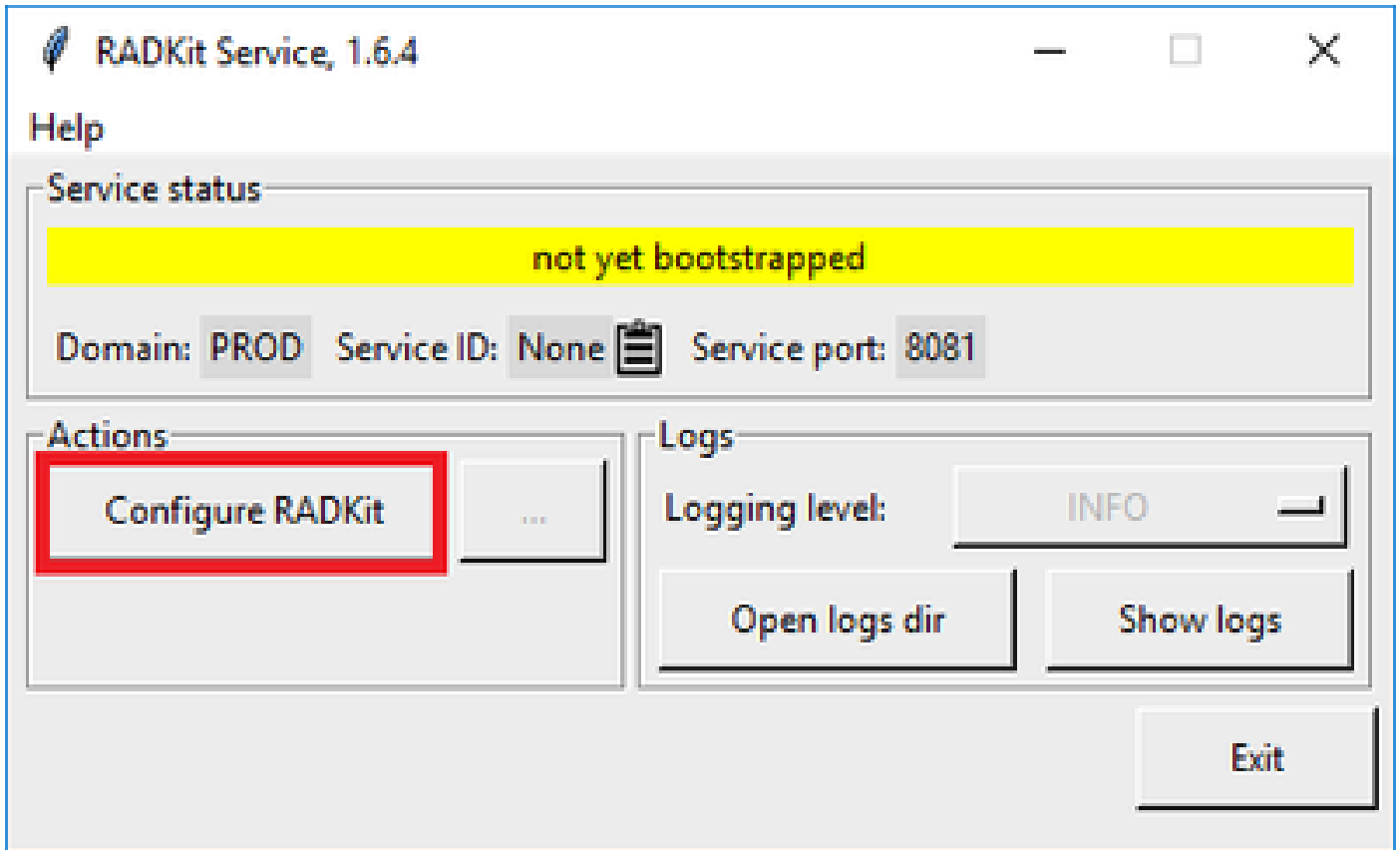
Maak in deze stap een superadmin-account aan om de RADKit-service verder te beheren via een webinterface.

**Zoek** RADKit Service in het menu Start (op Windows) of in de map Toepassingen (op macOS) en start het:



De allereerste keer dat u het start, kan het een beetje duren voordat RADKit Service start (ongeveer 10 tot 30 seconden afhankelijk van de snelheid van uw systeem). Daaropvolgend zullen de runs veel sneller gaan.

Nadat het opstarten is voltooid, in het dialoogvenster RADKit Service, zodra de status verandert in not yet bootstrapped de druk op Configure RADKit :



Hiermee opent u uw webbrowser en neemt u mee naar de RADKit Service WebUI, een web-based managementinterface waarmee u RADKit Service kunt beheren.

Er wordt verwacht dat het een certificaatwaarschuwing krijgt, die u kunt overslaan, wanneer u verbinding maakt met deze URL omdat het een zelfondertekend certificaat gebruikt.

Aangezien een superadmin gebruiker nog niet bestaat, zal WebUI u vragen om een wachtwoord voor deze gebruiker te creëren:

# Register superadmin user

No superadmin user was found.  
Please fill in this form to create a superadmin account.



A superadmin user must be created. Please enter a strong password for this user. This password will be requested in the future to (re)start or manage RADKit Service.

Username \*

Password \*

Repeat Password \*

PASSWORD REQUIREMENTS:

- Minimum **8** characters
- Minimum **1** lowercase letter
- Minimum **1** uppercase letter
- Minimum **1** digit
- Minimum **1** symbol

Selecteer een wachtwoord dat voldoet aan de eisen voor de wachtwoordsterkte die rechts worden weergegeven.

Het wachtwoord voor deze account zal worden gebruikt om geheimen zoals priv sleutels en apparaatreferenties te beschermen; als je het verliest, zullen alle geheimen verloren gaan en zal RADKit Service opnieuw moeten worden ge initialiseerd, dus kies het zorgvuldig en schrijf het op een veilige locatie. Deze kan zo nodig later worden gewijzigd.

Na het cre ren van de superadmin-account, gebruik het om in te loggen op de WebUI:



# Log in

Username \*

superadmin

Password \*

.....



Login

Nadat de superadmin-account is aangemaakt en u met succes bent aangemeld bij de WebUI, kunt u doorgaan naar de volgende stap waar uw RADKit-service is geregistreerd bij de RADKit cloudcomponent.

Stap 3. Meld je RADKit Service aan bij RADKit Cloud

Registreer in deze stap uw RADKit-service met RADKit cloud en genereer een service-ID om uw omgeving te identificeren.

Na het inloggen op de WebUI met de superadmin-gebruiker (zie stap 2), navigeer naar het connectiviteitsscherm:

Remote Automation Development Kit  
Cisco RADKit Service

Domain: PROD Service ID: none

Connectivity

+ Add Device

o Edit Cart

<input type="checkbox"/>	Active	Device Name	Hostname or IP Address	Device Type
⚠ No devices available				

Showing 0 to 0 of 0 entries. | Selected: 0.



Als u een proxy nodig hebt voor verbinding met internet, raadpleegt u de gedetailleerde installatie-instructies die hier beschikbaar zijn:

[https://radkit.cisco.com/docs/pages/one\\_page\\_setup.html](https://radkit.cisco.com/docs/pages/one_page_setup.html)

Nu moet u de Service inschrijven om het te laten verbinden met RADKit Cloud. Dit wordt gedaan door in te loggen via Service WebUI met behulp van uw Cisco.com (CCO) account. Klik op Enroll with SSO om verder te gaan

## Cloud Connectivity

DOMAIN: PROD

BASE URL: <https://prod.radkit-cloud.cisco.com>

Forwarder Endpoint	Status	Latency [ms]
 No forwarder endpoints connected		

## Service Identity Certificate



This RADKit Service needs to be enrolled to become functional. Please select an enrollment method by clicking one of the buttons below.

Recommended:

Enroll with SSO

Advanced:

Enroll with OTP

Voer het e-mailadres in dat overeenkomt met uw Cisco.com (CCO)-account in het veld e-mailadres bij Stap 2. klik vervolgens op Submit as shown in the image:

# Single Sign-On Enrollment



✓ Checking prerequisites

2 Email address

Provide email address for SSO login:

Submit

3 Connecting to the Access Service

Nadat RADKit Service verbinding maakt met RADKit Cloud voor autorisatie, wordt u een [CLICK HERE] link getoond die u naar de Cisco SSO-server brengt voor verificatie. Klik op de link om verder te gaan; het wordt geopend in een nieuw browsertabblad/venster. Zorg ervoor dat u hetzelfde e-mailadres gebruikt om u aan te melden bij SSO, zoals u hebt ingevoerd in de stap die u eerder hebt genoemd:

✓ OAuth connect

5 Waiting for SSO

Follow the SSO login link to continue: [\[CLICK HERE\]](#)

6 Requesting service certificate OTP

Nadat de SSO-verificatie is voltooid (of meteen, als u al geauthenticeerd was) wordt u naar een RADKit Access bevestigingspagina gebracht. Lees de informatie op de pagina en klik op Accept om RADKit Service te machtigen om zich aan te melden bij uw CCO-account als eigenaar.

## Do you accept this authorization request?

Environment: PROD

Endpoint IP Address: 208.1.4.28:2049-1800-1800

Endpoint Hostname: 208.1.4.28:2049-1800-1800

This page means that a RADKit instance is attempting to connect to the RADKit Cloud with your SSO credentials.

If you *did not* initiate this request, please click "Deny" now. If you are certain that this request is legitimate, click "Accept".

If you suspect that an illegitimate session may have been granted access in the past, click the "Log out all sessions" button below to immediately log out all RADKit SSO sessions associated with your user ID. This will not log out your SSO sessions in other applications.

Accept

Deny

Log out all sessions

Dan kom je bij een scherm dat zegt: Authentication result: Success .

Klik niet op de knop Log out all sessions; in plaats daarvan sluit u het tabblad/venster SSO en keert u terug naar de RADKit Service WebUI.

Dit laat zien Service enrolled with the identity: .... De unieke identificatie die volgt is uw RADKit Service ID, ook bekend als het Service Serial Number. In het voorbeeld screenshot is de Service-ID axT9-kplb-5dwc van u anders.

- ✓ Requesting service certificate
- ✓ Saving the identity
- ✓ Starting/Restarting the service

✓ Service enrolled with the identity: axt9-kplb-5dwc

Close

Klik op Close om het dialogvenster te sluiten en naar het Connectivity scherm terug te keren.

Na het verfrissen van de WebUI, wordt uw service-ID weergegeven bovenop de RADKit GUI, samen met de connectiviteitsstatus zoals hier te zien:



Wanneer een TAC engineer toegang moet krijgen tot een van de apparaten in uw omgeving, hebben ze deze service-ID nodig om uw RADKit-service te identificeren.

Nu een verbinding tot stand is gebracht met de RADKit Cloud-component en een service-ID heeft gegenereerd terwijl u dit doet, voegt u in de volgende stap de apparaten toe die via RADKit kunnen worden bereikt.

#### Stap 4. Apparaten en endpoints toevoegen

In deze stap, voeg de apparaten en hun geloofsbriefjes voor de apparaten toe die door RADKit kunnen worden betreden. Voor HyperFlex betekent dit dat deze apparaten en hun referenties idealiter moeten worden toegevoegd:

Apparaat	Apparaattype	Beheerprotocollen	referenties	Doorsturen van TCP-poorten	Opmerkingen
Hypervisor (ESXi-hosts)	Linux	Terminal (SSH)	wortel		

Opslagcontroller (SCVM)	HyperFlex HX	Terminalschakelaar (SSH)	beheerder wortel (inschakelen)	443	Voer in het veld Wachtwoord inschakelen het hoofdwachtwoord in. Dit wordt gebruikt wanneer een toestemmingstoken vereist is. Voor Swagger: vink "verify-TLS-certificaat" uit en laat het veld basis-URL leeg
vCenter	Linux	Terminal (SSH)	wortel		
UCSM	generiek	Terminal (SSH)	beheerder		
Installateur (optioneel)	Linux	Terminal (SSH)	wortel	443	
CIMC (alleen voor randclusters)	generiek	Terminal (SSH)	beheerder		
Getuige (alleen voor uitgerekte clusters)	Linux	Terminal (SSH)	wortel		
Intersight CVA/PCA (facultatief)	Linux	Terminal (SSH)	beheerder	443	

Het is belangrijk om de apparaten alleen toe te voegen met behulp van hun IP-adres en niet hun hostname, omdat dit nodig is om de apparaten die in hetzelfde cluster horen te correleren.

Om deze apparaten toe te voegen, in de RADKit WebUI, navigeer aan het scherm Apparaten:

Remote Automation Development Kit  
Cisco RADKit Service

Domain: PROD Service ID: axt9-kplb-5dwc

Connectivity

+ Add Device

Active Device Name Hostname or IP Address Device Type In

Devices

Remote Users

No devices available

Showing 0 to 0 of 0 entries. | Selected: 0.

Voer voor elk van de hierboven genoemde apparaten een nieuw item in door op Add Device te klikken . Voer het IP-adres in, selecteer het apparaattype en geef details afhankelijk van elk apparaattype voor alle knooppunten in uw cluster. Als u klaar bent, klikt u op Add & closeom terug te gaan naar het scherm Apparaten of Add & continue om een ander apparaat toe te voegen.

Hier vindt u voorbeelditems en hun configuratie voor elk apparaattype:

Voorbeeld voor ESXi-hosts:

## Edit Device ✕

**Device Name\*** (as it will appear in RADIC8) ?

**Device Type\***

**Management IP Address or Hostname\*** ?

**Jumphost Name**

**Forwarded TCP ports** ?

**Description**

?

**PSAC status: DISABLED**

**Available Labels - 0 of 0** (click to add)

NO LABELS AVAILABLE

**Selected Labels - 0** (click to delete)

+ Create new + None added

**Active** (remotely manageable)

**Available Management Protocols:**

Terminal
  Netconf
  Swagger
  HTTP
  SNMP

---

**Terminal**

Connection method:

SSH (Password)
  SSH (Public key)
  Telnet

**Username**

**Password**

if left blank, will be set to "" as default ?

**Port**

**Enable Password** ?

**Update**

Voorbeeld voor opslagcontrollers:

# Edit Device



Device Name (as it will appear in RedBox)

cluster2-node1-rcvm

Device Type

HyperFlex

Management IP Address or Hostname

172.16.2.14

Jumpshot Name

- Optional jumpshot -

Forwarded TCP ports

443

Description

Label search

RBAC status: **DISABLED**

Available Labels - 0 of 0 (click to add)

NO LABELS AVAILABLE

Selected Labels - 0 (click to delete)

Create New

None added

Active (remotely manageable)

Available Management Protocols:

Terminal  Netconf  Swagger  HTTP  SNMP

## Terminal

Connection method

SSH (Password)  SSH (Public key)  Telnet

Allow connecting using obsolete/insecure SSH algorithms

Use SSH tunneling when using this device as a jumpshot

Username

admin

Password

\*\*\*\*\*

If left blank, will be set to "" as default

Port

22

Enable Password

\*\*\*\*\*

If left blank, will be set to "" as default

## Swagger

Verify TLS certificate

\* Leave unchecked if the device presents a self-signed certificate

Allow connecting using obsolete/insecure TLS algorithms

Username

admin

Password

\*\*\*\*\*

If left blank, will be set to "" as default

Base URL

\* Leave blank if unused

Update



Voorbeeld voor vCenter:

## Edit Device ✕

Device Name\* (as it will appear in RADIUS) [?](#)

Device Type\*

Management IP Address or Hostname\* [?](#)

Jumphost Name

Forwarded TCP ports [?](#)

Description

[?](#) RBAC status: **DISABLED**

Available Labels - 0 of 0 (click to add)  

NO LABELS AVAILABLE

Selected Labels - 0 (click to delete)

Active (remotely manageable)

Available Management Protocols:  
 Terminal  Netconf  Swagger  HTTP  SNMP

---

### Terminal

Connection method:  
 SSH (Password)  SSH (Public key)  Telnet

Allow connecting using obsolete/insecure SSH algorithms  
 Use SSH Tunneling when using this device as a jumphost

Username

Password  
  
If left blank, will be set to "" as default [?](#)

Port

Enable Password [?](#)

Voorbeeld van UCSM:

## Edit Device ✕

**Device Name\*** (as it will appear in RADKit) [?](#)

**Device Type\***

**Management IP Address or Hostname\*** [?](#)

**Jumphost Name**

**Forwarded TCP ports** [?](#)

**Description**

[?](#)

**RBAC status: DISABLED**

Available Labels - 0 of 0 (click to add)

NO LABELS AVAILABLE

Selected Labels - 0 (click to delete)

[Create new](#) [None added](#)

**Active** (remotely manageable)

Available Management Protocols:

Terminal  Netconf  Swagger  HTTP  SNMP

---

### Terminal

Connection method:

SSH (Password)  SSH (Public key)  Telnet

Allow connecting using obsolete/insecure SSH algorithms

Use SSH Tunneling when using this device as a jumphost

**Username**

**Password**

If left blank, will be set to "" as default [?](#)

**Port**

**Enable Password** [?](#)

[Update](#)

RADKit gebruiken op een TAC SR

Als alle voorbereiding is gedaan en u toegang tot uw apparaten aan een TAC engineer wilt geven, kunt u deze stappen doorlopen.

Een ingenieur heeft uw RADKit service-ID en toegang tot uw omgeving of geselecteerde apparaten (bij gebruik van RBAC) nodig voor de tijd die nodig is.

1. Geef RADKit-service-id op

Als u nog geen TAC-case hebt geopend, hebt u de mogelijkheid om in Support Case Manager op Cisco.com te vermelden Use RADKit for data collection:

Use RADKit for data collection

RADKit Service ID 

axt9-kplb-5dwc

Als u al een open-serviceaanvraag hebt, kunt u de RADKit Service ID toevoegen in Support Case Manager met de sectie Contactinformatie van de klant:

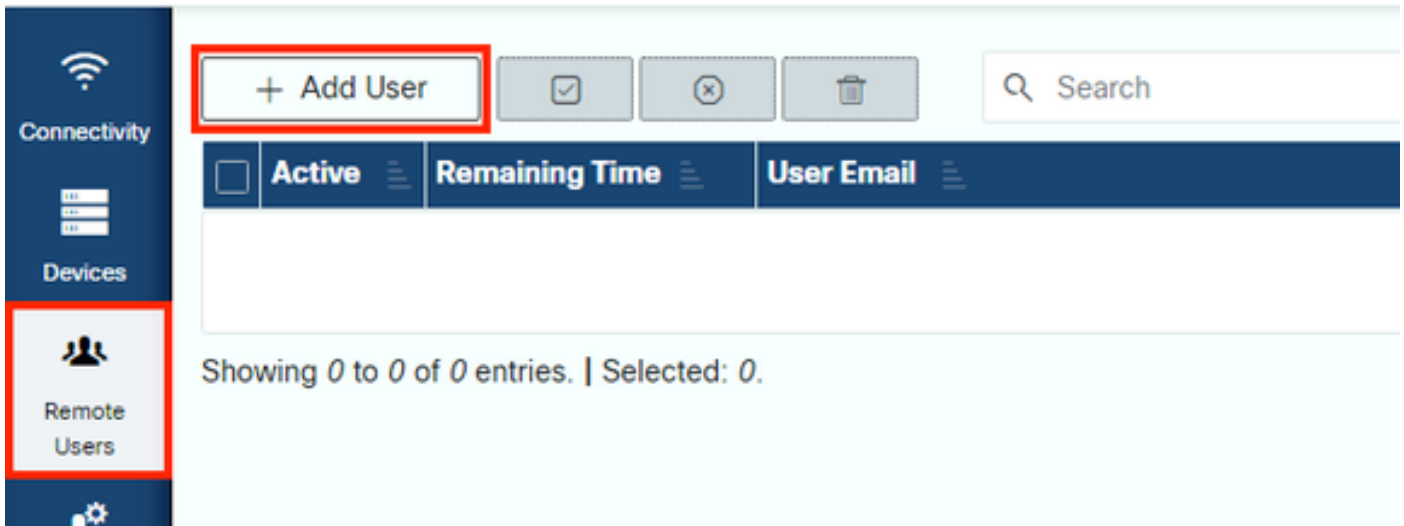


The screenshot shows the 'CUSTOMER CONTACT INFORMATION' section in the Support Case Manager interface. It includes fields for Customer Name (Jens Depuydt), Business Phone (+322...), Email (j.depuydt@cisico.com), Preferred Contact Method (Email), Change Notifications (Off for Contact and CC list, Off for this SR), Customer Email (j.depuydt@cisico.com), and Customer Company (Cisco). A red box highlights the 'RADKIT SERVICE ID' field, which contains the text 'axt9-kplb-5dwc' and a link to 'Add/Edit RADKit Service ID'. To the right, there is a section for 'Edit RADKit Service ID' with a checked box for 'Use RADKit for data collection' and 'Save' and 'Cancel' buttons.

Of vermeld gewoon uw ID aan de TAC engineer die aan uw case werkt.

## 2. Externe gebruiker toevoegen

Alvorens om het even welke gebruiker met uw apparaten kan werken, moet u expliciete toegang verlenen en een tijds kader vormen waarvoor deze toegang geldig blijft. Om dit te doen, in de RADKit WebUI, navigeer naar het Remote Users scherm en maak een nieuwe externe gebruiker door te klikken Add User.



Voer het @cisco.com e-mailadres van de TAC Engineer in (let op typos). Let op het Activate this user aanvinkvakje en de Time slice of Manual instellingen.

Terwijl de gebruiker actief is, hebben ze toegang tot de geconfigureerde apparaten via RADKit Service, op voorwaarde dat die apparaten zijn ingeschakeld en dat het RBAC-beleid hen toestaat.

De tijdsegment geeft de tijd aan waarna de gebruiker automatisch wordt gedeactiveerd; met andere woorden, een tijdsegment vertegenwoordigt een tijdgebonden probleemoplossingssessie. De gebruikerssessie kan worden uitgebreid tot de duur van het tijdsegment voor die gebruiker. Als u gebruikers handmatig wilt in- of uitschakelen, selecteert u in plaats daarvan de optieManual.

Gebruikers kunnen altijd handmatig worden geactiveerd/gedeactiveerd, ongeacht of ze een tijdsegment geconfigureerd hebben of niet. Wanneer een gebruiker wordt gedeactiveerd, worden al zijn sessies via RADKit Service direct losgekoppeld.

Als u klaar bent, klikt u op Add & close om terug te gaan naar het scherm Externe gebruikers.

Gerelateerde informatie

- Meer informatie en antwoorden op veelgestelde vragen kunt u vinden op de website van RADKit: <https://radkit.cisco.com/>
- [Cisco Technical Support en downloads](#)

## Over deze vertaling

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