# Problemen oplossen met de verbindingsstatus van Talos

## Inhoud



## Inleiding

In dit document wordt beschreven hoe u problemen met de TALOS-connectiviteit kunt oplossen met Secure Firewall FMC en FDM.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Firewall Management Center (FMC)

- Cisco Secure Firewall Device Manager (FDM)

- Cisco Secure Firewall Threat Defense (FTD)

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

FMC versie 7.6.0 of 7.7.0
FDM versie 7.6.0 of 7.7.0
FTD versie 7.6.0 of 7.7.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

Het Cisco Secure Firewall Management Center (FMC) vertrouwt op een certificaat aan de clientzijde om een veilige verbinding tot stand te brengen met de bedreigingsinlichtingendiensten van Cisco Talos. Deze verificatie is essentieel voor de FMC om met succes kritieke updates te downloaden, waaronder URL Reputation Databases (URLDB's), Lightweight Security Packages (LSP's) en andere verrijkingsgegevens.

Onder normale bedrijfsomstandigheden wordt dit certificaat vooraf geleverd tijdens de installatie van de software en is het ontworpen om automatisch te worden verlengd wanneer de vervaldatum nadert. Een bekend probleem in bepaalde versies van de Cisco Secure Firewall FMC-software verhindert echter dat het proces voor automatische verlenging na 30 maart 2025 met succes wordt voltooid. Wanneer dit gebeurt, kan de FMC niet authenticeren met Talos, wat leidt tot connectiviteitsfouten en het onvermogen om bijgewerkte bedreigingsinformatie op te halen.

#### Certificaatstatus controleren

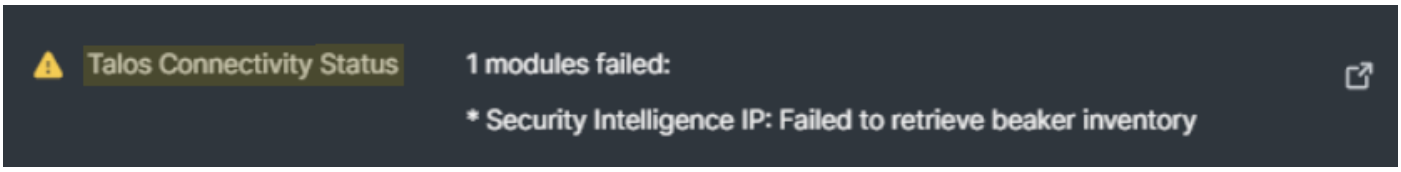
### FMC GUI

Wanneer het certificaat aan de clientzijde niet kan worden verlengd, activeert de Cisco FMC gezondheidswaarschuwingen om beheerders op de hoogte te stellen van de onderbreking in de communicatie met Cisco Talos. U kunt deze meldingen controleren door naar Systeem > Gezondheid te gaan en het gedeelte Connectiviteitsstatus van talos te bekijken.

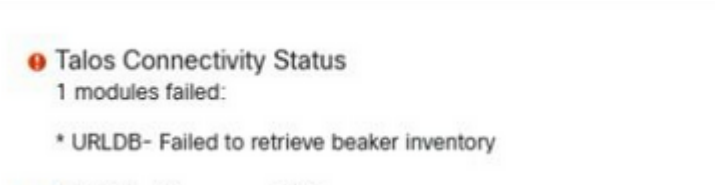
Als uw systeem wordt beïnvloed door het probleem met de vervaldatum van het certificaat, ziet u

meestal een van deze foutmeldingen:

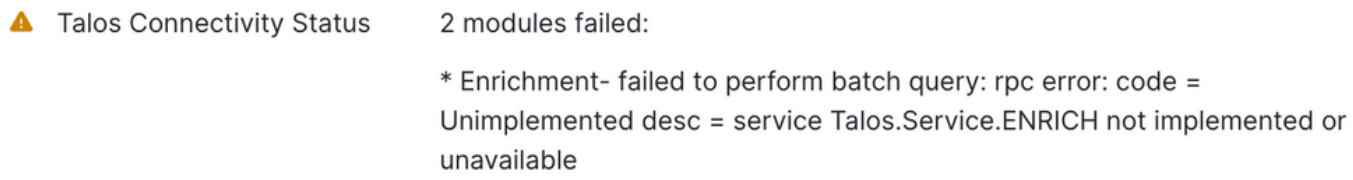
- "LSP - Kan bekerinventaris niet ophalen":




- "URLDB - Kan de bekerinventaris niet ophalen":




- "Verrijking - Batchquery is niet uitgevoerd":




## FMC-CLI

Ga naar de expertmodus en voer de opdracht uit om te controleren of de huidige vervaldatum van het certificaat aan de clientzijde is verlopen om te bepalen of dit probleem gevolgen heeft voor uw FMC-toestel:

<#root>

```
expert
sudo su
//type the 'FMC CLI admin password'

sudo openssl x509 --in /var/sf/beaker3/securefirewall-dev-prod-01_prod.pem --text
```

Zoek in de opdrachtuitvoer het gedeelte Validiteit. Het veld Niet na geeft de huidige vervaldatum van het certificaat aan. Als deze datum al is verstreken of nadert, is het verlengingsproces mislukt

en is een handmatige herstart van de service nodig om de certificaatvernieuwing te starten.

Voorbeeld:

<#root>

```
> expert
>sudo su
//type the 'FMC CLI admin password'
openssl x509 --in /var/sf/beaker3/securefirewall-dev-prod-01_prod.pem --text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 46240369 (0x2c19271)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = California, L = San Jose, O = Cisco Systems Inc., OU = Security, CN = Keym
```

**Validity**

```
Not Before: Jan 30 22:32:39 2024 GMT
```

**Not After :**

```
 Mar 30 22:32:39 2025 GMT
        Subject: CN = SFW76EVAL-prod-01, C = US, ST = California, L = San Jose, O = Cisco, OU = Securit
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
```

# Problemen oplossen

## 1. Identificeer uw scenario

| Softwareversie | Bijbehorende bug-ID | hoofdoorzaak |
|---|---|---|
| 7.6.0 of 7.7.0 | Cisco bug ID CSCwo63951 | Fout bij verlopen certificaat/connectiviteit |
| 7.6.1+ of 7.7.10+ | Cisco bug ID CSCwr23982 | Registratie- / licentieconfiguratie (bijvoorbeeld air-gapped). |

## 2. Problemen oplossen voor versie 7.6.0 en 7.7.0

Symptomen

Naast de eerder genoemde gezondheidswaarschuwingen, observeer je deze gedragingen:

- FDM Task Manager Fouten: "Snort 3 cloud update mislukt: Geen reactie van de update server of verbinding time-out."
- Logboekvermeldingen: fouten in /ngfw/var/log/berichten die aangeven: er is geen verbinding gemaakt met tunnel (UUID), fout: er is geen verbinding gemaakt.
- Status: Stagnerende updates in het scherm UI: Voorkeuren voor URL-filtering worden weergegeven met "Nog niet bijgewerkt".

Tijdelijke tijdelijke tijdelijke tijdelijke tijdelijke oplossing

Om de services onmiddellijk te herstellen, start u de vereiste processen opnieuw op via de expertmodus:

Stap 1. Open de CLI en ga naar de expertmodus.

Stap 2. Voer de volgende opdrachten uit:

```
expert
sudo su
//type the 'FMC CLI admin password'
pmtool restartbyid talosAgent
pmtool restartbyid beaker3
```

---

Opmerking: met deze tijdelijke oplossing wordt een certificaat geactiveerd dat slechts vijf dagen geldig is. U moet dit proces elke vijf dagen herhalen totdat een permanente oplossing wordt toegepast.

---

permanente resolutie

Om dit probleem permanent op te lossen, moet u ervoor zorgen dat aan deze voorwaarden wordt voldaan:

Stap 1. Connectiviteit verifiëren: Zorg ervoor dat het toestel uitgaande toegang heeft tot https://api-

sse.cisco.com. Ga hiervoor naar de FMC CLI, voer de expertmodus in en voer de volgende opdrachten uit:

Stap 1.1. DNS-resolutie testen:

<#root>

```
expert
sudo su
//type the 'FMC CLI admin password'
```

**nslookup api-sse.cisco.com**

Stap 1.2. TCP-poorttoegang testen:

<#root>

```
 expert
sudo su
//type the 'FMC CLI admin password'
```

**telnet api-sse.cisco.com 443**

---

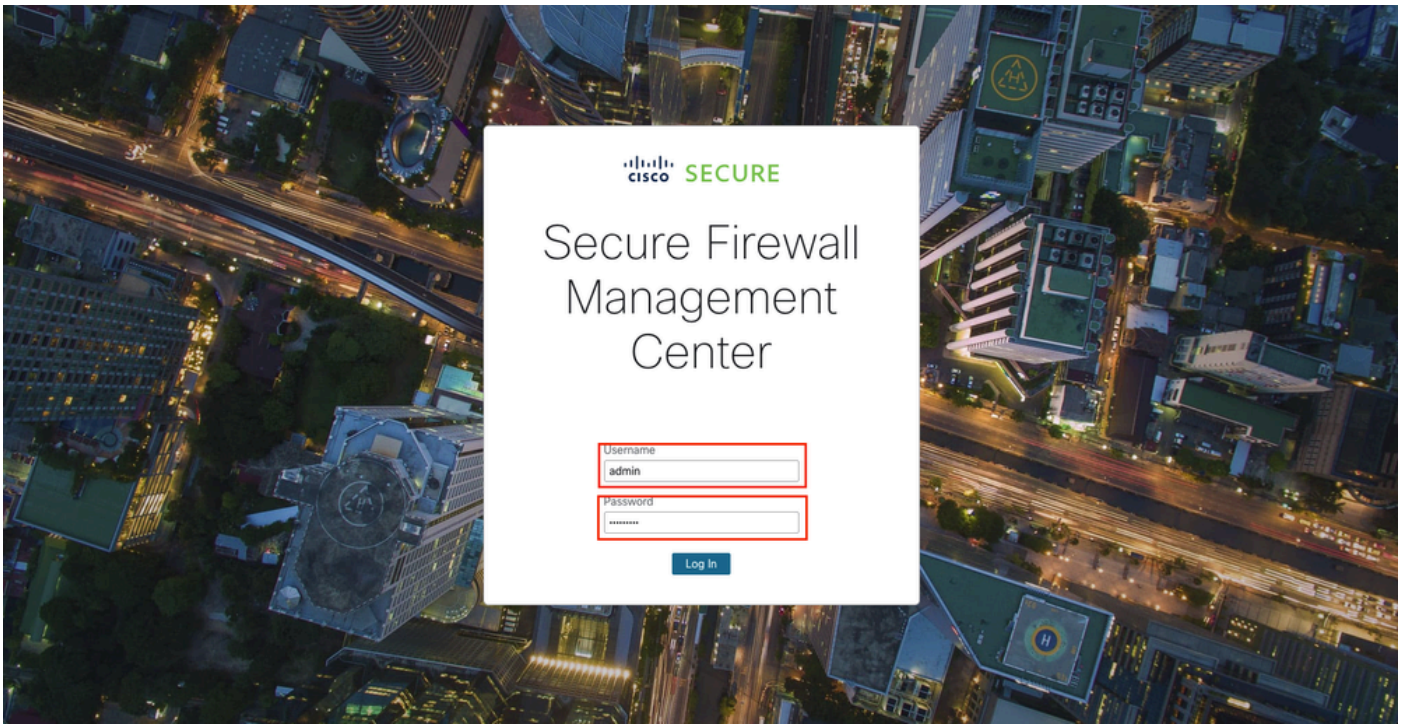
Opmerking: Controleer of uitgaande HTTPS (TCP 443)-toegang tot https://api-sse.cisco.com is toegestaan via alle upstream firewalls, proxy's of beveiligingsapparaten.

---

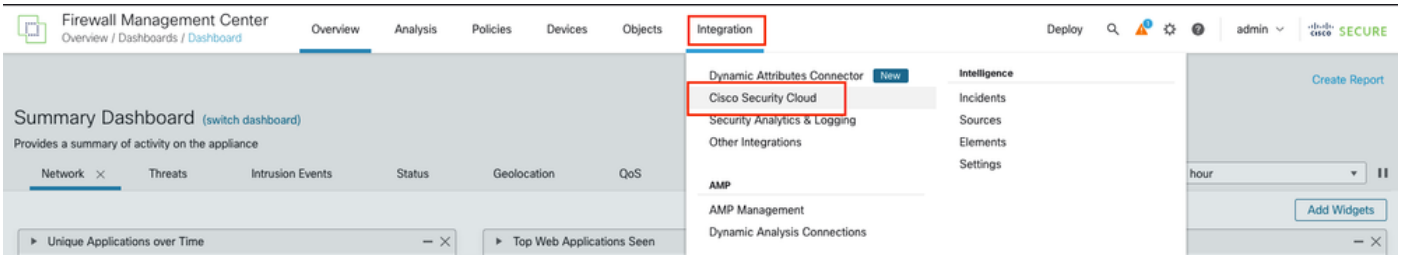
Stap 2. Telemetrie inschakelen: Zorg ervoor dat Customer Success Network (CSN) telemetrie is ingeschakeld, zodat de SSEConnector een nieuw certificaat kan krijgen. Om CSN in te schakelen op de FMC, zijn dit de stappen:

Stap 2.1. Log in op de FMC GUI door een webbrowser te openen en naar de FMC URL te navigeren (bijvoorbeeld: https://<FMC_IP_or_Hostname>). Voer uw gebruikersnaam en wachtwoord in om toegang te krijgen tot de

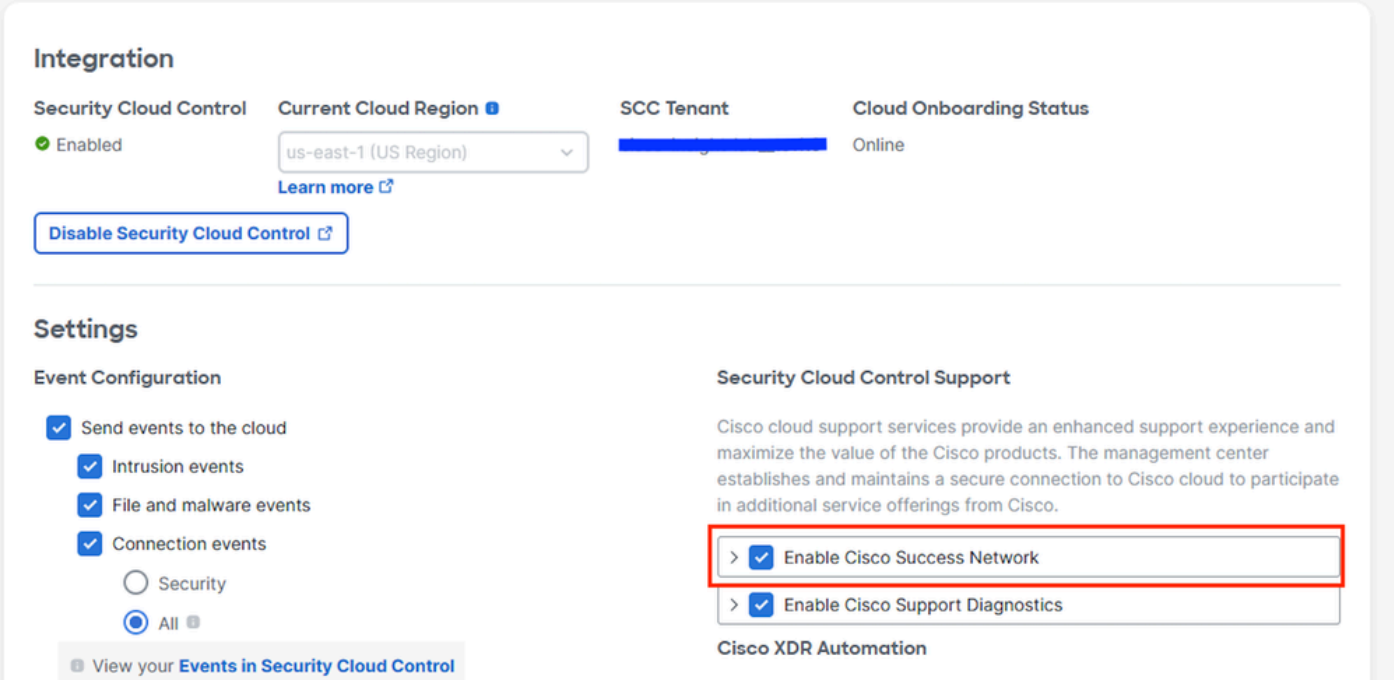
FMC GUI-interface.




Stap 2.2. Navigeer naar Cisco Success Network Settings: Selecteer Integratie > Cisco Security Cloud in het hoofdmenu.




Stap 2.3. Zoek en schakel de optie met het label Cisco Success Network in: Schakel hiervoor het selectievakje Cisco Success Network inschakelen in om de telemetrie te activeren.




Stap 3. Updates installeren: installeer GeoDB 2025-04-03-094 of VDB 406 (of hoger). Dit leidt tot de installatie van een nieuw 365-dagen certificaat.

---

Opmerking: hoge beschikbaarheid (HA). In een HA-paar wordt het SSEConnector-proces niet uitgevoerd op de standby-eenheid. Als u de stand-by FMC wilt bijwerken, voert u een switch uit zodat de stand-by actief wordt en installeert u vervolgens de vereiste VDB- of GeoDB-update.

---

## 3. Problemen oplossen voor de versies 7.6.1+ en 7.7.10+

Dit probleem doet zich meestal voor in omgevingen zonder standaard Cisco Security Cloud (CSC)-registratie, zoals die met behulp van Evaluatielicenties, SSM On-Prem, PLR of SLR.

Geïmpacteerde kenmerken

- Automatische/handmatige LSP-updates (Lightweight Security Package).
- URL-filtering database-inhoud updates en cloud lookups.
- Talos verrijking van verbindingsevenementen.

Aanbevolen acties

1. Standaardomgeving: registreer de FMC via Integratie > Cisco Security Cloud. Registratie activeert automatisch een nieuw certificaat downloaden binnen 30 minuten.

2. Handmatige updates: als automatische updates mislukken, download de nieuwste LSP handmatig van software.cisco.com en installeer deze rechtstreeks op de FMC.

3. Air-Gapped Omgevingen: Als uw netwerk geen internettoegang heeft, wordt de gezondheidsmodule Talos Connectivity Status irrelevant. Schakel in dit scenario deze specifieke module uit binnen uw toegepaste gezondheidsbeleid.

## Gerelateerde informatie

- Neem voor meer hulp contact op met het Cisco Technical Assistance Centre (TAC). Een geldig supportcontract is vereist: Cisco Worldwide Support Contacts.

- Cisco Support & Downloads: Cisco Technical Support & 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.