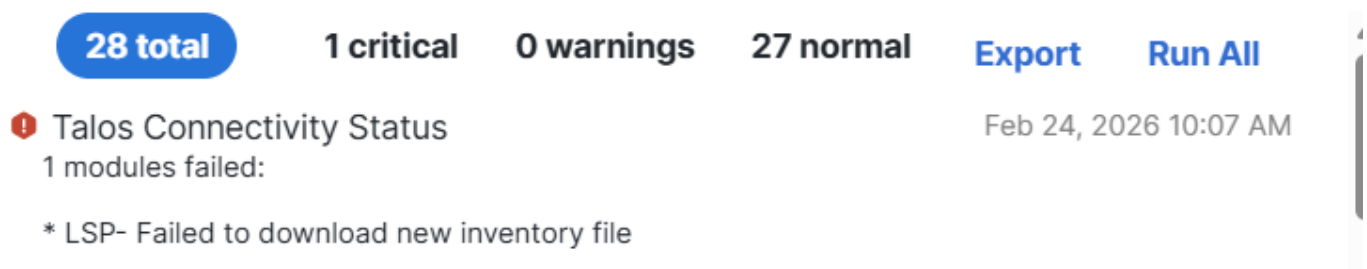


FMC Automatische LSP-updates " Nieuwe inventaris" is niet gedownload;

uitgeven

Automatische LSP-updates (Lightweight Security Package) mislukken bij Cisco FMC. LSP-updates worden niet meer automatisch geïnstalleerd, terwijl de handmatige LSP-installatie goed blijft werken. VDB-updates en updates van de Snort-regel werken nog steeds normaal via automatische processen.

Voorbeeldwaarschuwing



28 total **1 critical** **0 warnings** **27 normal** [Export](#) [Run All](#)

Talos Connectivity Status Feb 24, 2026 10:07 AM
1 modules failed:

- * LSP- Failed to download new inventory file

inline_image_0.png

milieu

- Cisco Secure Firewall Firepower Management Center 7.6.x On-Prem (van toepassing op alle FMC-modellen en versies 7.6+)

resolutie

Als u het probleem met de automatische LSP-update wilt oplossen, controleert u of de vereiste netwerkconnectiviteit correct is geconfigureerd op upstream firewalls of netwerkapparaten die het

updateproces kunnen blokkeren.

1: Controleer de huidige LSP-versiestatus

Controleer de huidige LSP-versie die is geïnstalleerd op het Firepower Threat Defense-apparaat:

```
show version
```

Voorbeeld van uitvoer met de huidige LSP-versie:

```
-----[ apparaat ]-----
```

```
Model: Cisco Secure Firewall 3140 Threat Defense (80) versie 7.6.2.1 (Build 3)
```

```
UUID: 5fb22700-68c8-11ee-b5a0-d2e6638aec56
```

```
LSP versie: lsp-rel-20260121-2008
```

```
VDB-versie: 421
```

```
-----
```

2: Vereisten voor netwerkconnectiviteit controleren

Zorg ervoor dat uitgaande toegang via poort 80 is toegestaan op elke upstream firewall of netwerkbeveiligingsapparaat voor deze bestemmingen:

- updates-dyn-talos.sco.cisco.com - Vereist voor LSP-updates
- updates.ironport.com - Vereist voor updates van beveiligingsinhoud

Deze bestemmingen zijn essentieel voor het goed functioneren van het automatische updateproces. Elke blokkering van deze verbindingen voorkomt automatische LSP-updates, terwijl handmatige updates nog steeds kunnen werken.

Voorbeeld verbindingstest van FMC met fout

```
root@fmc:/Volume/home/user# curl -v -k http://updates.ironport.com
```

```
<h1>Webpagina geblokkeerd</h1>
```

```
<p>De webpagina die u probeert te bezoeken, is geblokkeerd in overeenstemming met het bedrijfsbeleid. Neem contact op met de systeembeheerder als u denkt dat dit een fout is.</p>
```

Voorbeelden van foutenlogboeken van /var/log/sf/talos_agent.log

```
sf/talos_agent.log:TalosAgent:ERROR:
```

```
updater.go:talosagent.cisco.com/pkg/updater.UpdateService:475 2026/02/13 04:11:05 Nieuw inventarisbestand niet gedownload: bestand niet gedownload:
```

```
204cf9af41f70cb30cfd3a7d41ab2f7366219cbfa805b4ec7443bb957f373b87630d8e4027491747102d060e
```

```
rpc-fout: code = interne desc = http-fout 50
```

```
204CF9AF41F70CB30CFD3A7D41AB2F7366219CBFA805B4EC7443BB957F373B87630D8E4027491747102D060ED5E238AB
```

```
sf/talos_agent.log:TalosAgent:ERROR:
```

```
updater.go:talosagent.cisco.com/pkg/updater.UpdateService:475 2026/02/24 19:18:08 Nieuw inventarisbestand niet gedownload: bestand niet gedownload:
```

```
3b1e29d5b30bd9dc79f15fad7726e616d73e93ec473e383bb08086b41d3bb571b7e08d3f0fb3fc5e839415c
```

```
rpc-fout: code = interne desc = downloaden van
```

```
http://updates.ironport.com:80/lsp/1/lsp/default/20260223001: verbindingfout: Verbinding herstellen door peer0
```

3: Controleer de updateconfiguratie

Bevestig dat automatische updates correct zijn geconfigureerd in het Firewall Management Center voor LSP-updates. Het feit dat VDB- en Snort-regelupdates automatisch blijven werken, suggereert dat het basisupdatemechanisme functioneel is, maar LSP-specifieke connectiviteit kan worden geblokkeerd.

4: Connectiviteit testen

Nadat u hebt bevestigd dat de vereiste bestemmingen toegankelijk zijn via upstream-beveiligingsapparaten, controleert u het automatische updateproces om te controleren of LSP-updates de normale werking hervatten.

Voorbeeld van werkoutput

```
root@echo-ngfw-fmfv3:/Volume/home/admin# curl -v -k http://updates.ironport.com
```

```
* 208.90.58.25:80 geprobeerd...
```

```
* Verbonden met updates.ironport.com (208.90.58.25) poort 80 (#0)
```

```
> GET / HTTP/1.1
```

```
> Host: updates.ironport.com
```

```
> User-Agent: curl/7.79.1
```

```
> Accepteren: */*
```

```
>
```

```
* Bundle markeren als niet-ondersteunend voor multigebruik
```

```
< HTTP/1.1 200 OK
```

```
< Server: nginx/1.20.1
```

```
< Datum: ma, 16 mrt 2026 20:22:35 GMT
```

```
< Content-Type: tekst/html
```

```
< Lengte inhoud: 689
```

```
< Laatst gewijzigd: wo, 06 sep 2006 17:26:12 GMT
```

```
< Verbinding: keep-alive
```

```
< ETag: "44ff04b4-2b1"
```

```
< Verloopt: di, 17 mrt 2026 20:22:35 GMT
```

```
< Cache-Control: max-age=86400
```

< Accepteren-bereiken: bytes

<

<HTML>

<!-- \$Header: /usr/local/cvsroot/godspeed/upgrade_server/http/html/root.html,v 1.1 2004/06/25 22:43:59 brie Exp \$ -->

<HOOFD>

</HOOFD>

<BODY>

<IMG SRC="<http://ironport.com/media/logo.gif>">

<P>

Dit is de IronPort-updateserver. Als u probeert om nieuwe verkeerscontrole-, merlin- of WBRS-pakketten hebt u deze pagina per ongeluk bereikt.

Raadpleeg de Release Notes van Update Manager voor instructies om te downloaden de nieuwe software.

</P>

<P>

Als u vragen heeft, neem dan gerust contact op met de klantenservice van IronPort

op (877)641-4766 of support@ironport.com.

</P>

</BODY>

</HTML>

* Verbinding #0 naar host updates.ironport.com intact gelaten

Zorg ervoor dat het apparaat voldoet aan de vereisten voor poort- en domeinconnectiviteit voor andere verschillende update- en downloadtypen zoals vermeld in openbare documentatie van Cisco:

- [Beheerdershandleiding voor het Cisco Secure Firewall Management Center, 7.6: beveiliging, internettoegang en communicatiepoorten](#)

Oorzaak

De automatische LSP-updatefout wordt veroorzaakt door een geblokkeerde netwerkverbinding met de vereiste updateservers. In het bijzonder wordt uitgaande toegang via poort 80 naar updates-dyn-talos.sco.cisco.com en updates.ironport.com beperkt door upstream firewallregels of netwerkbeveiligingsbeleid. Dit voorkomt dat de FMC automatisch LSP-updates downloadt en installeert, terwijl handmatige updates nog steeds kunnen worden uitgevoerd omdat ze verschillende downloadmethoden of inhoud in de cache kunnen gebruiken.

Het probleem kan echter ook worden beïnvloed door de mogelijkheid van de FMC om grote bestanden te downloaden van de Cisco-cloudsite. Door de FMC-bandbreedte af te knijpen, in combinatie met andere meerdere software-updates (bijv. SRU en VDB) binnen hetzelfde tijdsbestek, kan concurrentie voor bandbreedte worden ingesteld, wat leidt tot downloadfouten. In dergelijke gevallen moet u de downloadtijden van de software scheiden om ze voldoende bandbreedte voor downloads te bieden of eventuele problemen met de upstream-bandbreedte op te lossen.

Verwante inhoud

- [Cisco Technical Support en downloads](#)
- [Beheerdershandleiding voor het Cisco Secure Firewall Management Center, 7.6: beveiliging, internettoegang en communicatiepoorten](#)

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.