

# Registratie van slimme licenties voor FMC en FTD gebruiken voor probleemoplossing

## Inhoud

[Inleiding](#)  
[Voorwaarden](#)  
[Vereisten](#)  
[Gebruikte componenten](#)  
[Achtergrondinformatie](#)  
[Registratie van Slimme FMC-licenties](#)  
[Voorwaarden](#)  
[Registratie van Slimme FMC-licenties](#)  
[Bevestiging in Smart Software Manager \(SSM\)-kant](#)  
[Registratie van FMC Smart License](#)  
[RMA](#)  
[Problemen oplossen](#)  
[Veelvoorkomende problemen](#)  
[Casestudy 1. Ongeldige token](#)  
[Casestudy 2. Ongeldige DNS](#)  
[Case Study 3. Ongeldige tijdwaarden](#)  
[Case study 4. Geen abonnement](#)  
[Case study 5. Out-of-Compliance \(OSC\)](#)  
[Case study 6. Geen sterke encryptie](#)  
[Aanvullende opmerkingen](#)  
[Melding van slimme licentiestatus instellen](#)  
[Ontvang meldingen van gezondheidmeldingen van het VCC](#)  
[Meervoudige VCC's op dezelfde slimme account](#)  
[FMC moet internetconnectiviteit behouden](#)  
[Meervoudige FMCv implementeren](#)  
[Veelgestelde vragen](#)  
[Gerelateerde informatie](#)

## Inleiding

In dit document wordt de configuratie voor de registratie van slimme licenties beschreven van Firepower Management Center op door Firepower Threat Defence beheerde apparaten.

## Voorwaarden

### Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

### Gebruikte componenten

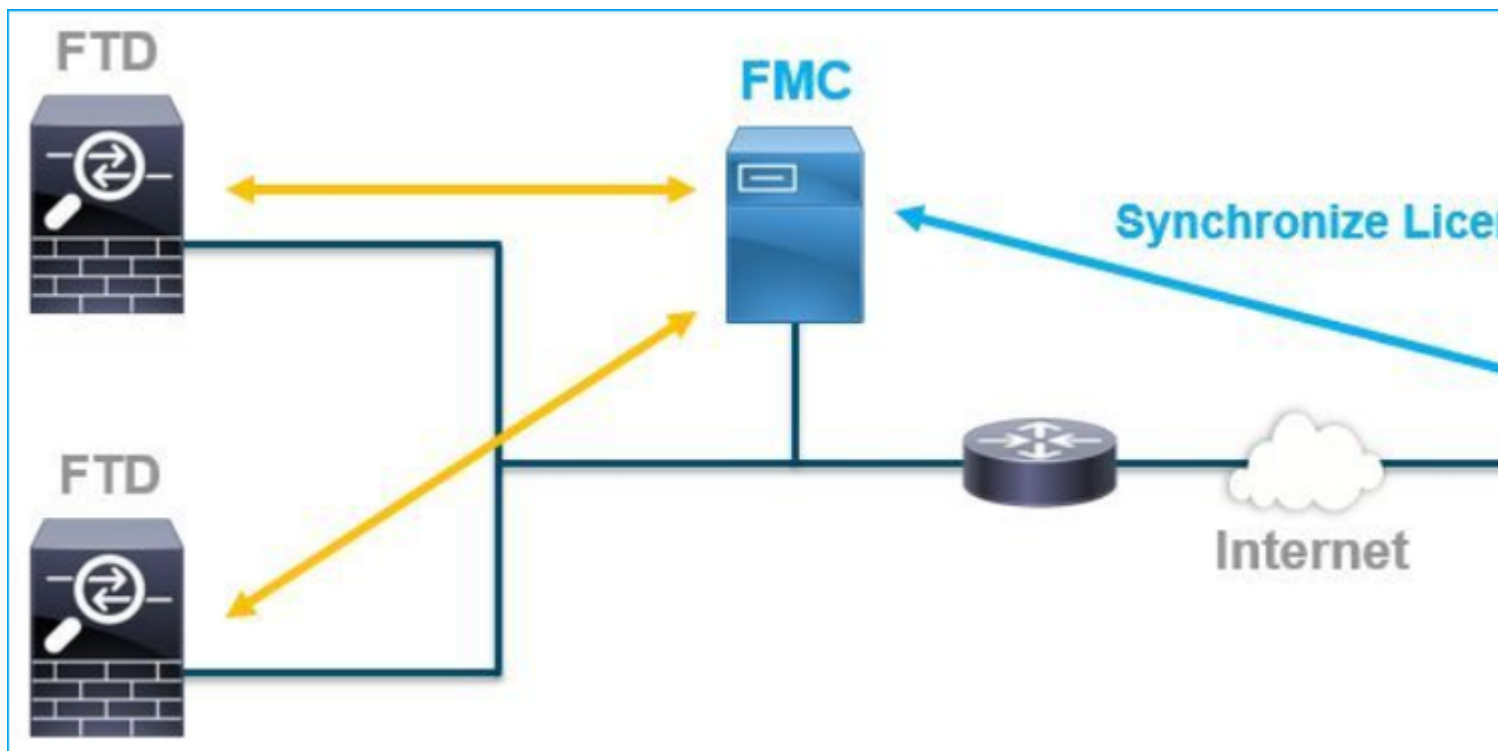
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle

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

registratie van FMC-, FTD- en slimme licenties.

Smart License-registratie wordt uitgevoerd op het Firepower Management Center (FMC). Het VCC communiceert via het internet met de Cisco Smart Software Manager (CSSM)-portal. In CSSM beheert de firewallbeheerder de Smart Account en de bijbehorende licenties. Het FMC kan vrijelijk licenties toewijzen en verwijderen aan de beheerde Firepower Threat Defence (FTD)-apparaten. Met andere woorden, het FMC beheert centraal de vergunningen voor FTD-apparatuur.



Voor het gebruik van bepaalde eigenschappen van FTD-apparaten is een aanvullende licentie vereist. De slimme licentietypen die klanten aan een FTD-apparaat kunnen toewijzen, worden gedocumenteerd in [FTD-licentietypen en -beperkingen](#).

De basislicentie is opgenomen in het FTD-apparaat. Deze licentie wordt automatisch geregistreerd in uw Smart Account wanneer het VCC is geregistreerd bij CSSM.

De op termijn gebaseerde licenties: Threat, Malware en URL-filtering zijn optioneel. Om functies te gebruiken die betrekking hebben op een licentie, moet een licentie worden toegewezen aan het FTD-apparaat.

Om een Firepower Management Center Virtual (FMCv) te kunnen gebruiken voor het FTD-beheer, is ook een **Firepower MCv Device License** in CSSM nodig voor het FMCv.

De FMCv licentie is opgenomen in de software en het is eeuwigdurend.

Daarnaast worden in dit document scenario's geboden om te helpen bij het oplossen van vaak voorkomende fouten in de licentieregistratie.

Kijk voor meer informatie over licenties op [Cisco Firepower System functielicenties](#) en [veelgestelde vragen](#)

[over FirePOWER Licensing.](#)

## Registratie van Slimme FMC-licenties

### Voorwaarden

1. Om een slimme vergunning te kunnen registreren, moet het VCC toegang hebben tot het internet. Aangezien het certificaat wordt uitgewisseld tussen het VCC en de Smart License Cloud met HTTPS, moet u ervoor zorgen dat er geen apparaat in het pad is dat de communicatie kan beïnvloeden of wijzigen. (bijvoorbeeld Firewall, Proxy, SSL-decryptie apparaat, enzovoort).
2. Open de CSSM en geef een Token ID uit vanuit **Inventaris > Algemeen > Nieuwe Token**-knop, zoals in deze afbeelding.

Cisco Software Central > Smart Software Licensing

### Smart Software Licensing

Alerts | **Inventory** | Convert to Smart Licensing | Reports | Preferences | On-Prem Accounts | Activity

Virtual Account: [Redacted] ▼

**General** | Licenses | Product Instances | Event Log

#### Virtual Account

Description: [Redacted]

Default Virtual Account: No

#### Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

**New Token...**

Token	Expiration Date	Uses	Export-Controlled	Description
M2RmMWVkymltZmRI. [Icon]	2020-Jun-30 19:34:48 (in 16 ...)		Allowed	[Redacted]
ZmJjODEzYjEtOTJjZi0. [Icon]	2021-May-22 00:54:03 (in 34...)		Allowed	

Om sterke encryptie te gebruiken, laat de **Allow uitvoer-gecontroleerde functionaliteit op de producten toe die met deze symbolische** optie worden **geregistreerd**. Als deze optie is ingeschakeld, wordt het selectieteken weergegeven in het aankruisvakje.

3. Selecteer **Token maken**.

## Create Registration Token

This will create a token that is used to register product instances, so that they can use licenses from this virtual account. Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account:

Description:

\* Expire After:  Days  
*Between 1 - 365, 30 days recommended*

Max. Number of Uses:

*The token will be expired when either the expiration or the maximum uses is reached*

Allow export-controlled functionality on the products registered with this token ?

[Create Token](#) [Cancel](#)

## Registratie van Slimme FMC-licenties

Ga naar het **stelsel** > **Licenties** > **Slimme Licenties** op het VCC en selecteer de knop **Registreren**, zoals in deze afbeelding.

Firepower Management Center  
 System / Licenses / Smart Licenses

Overview Analysis Policies Devices Objects AMP

Welcome to Smart Licenses

Before you use Smart Licenses, obtain a registration token from [Cisco Smart Software Manager](#), then click Register

[Register](#)

Smart License Status

Usage Authorization:	--
Product Registration:	Unregistered
Assigned Virtual Account:	--
Export-Controlled Features:	--
Cisco Success Network:	--
Cisco Support Diagnostics:	--

Voer de Token ID in het venster voor registratie van slimme licenties in en selecteer **Wijzigingen toepassen**, zoals in deze afbeelding.

### Smart Licensing Product Registration

Product Instance Registration Token:

OWI4Mzc5MTAtNzQwYi00YTVILTkyNTktMGMxNGJIYmRmNDUwLTE1OTQ3OTQ5%  
0ANzc3ODB8SnVXc2tPaks4SE5Jc25xTDkySnFYempTZnJEWVdVQU1SU1NiOWFM

If you do not have your ID token, you may copy it from your Smart Software manager The under the assigned virtual account. [Cisco Smart Software Manager](#)

Management Center establishes a secure connection to the Cisco Cloud so that it can participate in additional service offerings from Cisco. Management Center will establish and maintain this secure connection at all times. You can turn off this connection at any time by disabling Cisco Success Network and Cisco Support Diagnostics. Disabling these services will disconnect the device from the cloud.

Cisco Success Network

The Cisco Success Network provides usage information and statistics to Cisco. This information allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network. Check out the [sample data](#) that will be sent to Cisco.

Enable Cisco Success Network

Cisco Support Diagnostics

The Cisco Support Diagnostics capability provides entitled customers with an enhanced support experience by allowing Cisco TAC to collect essential information from your devices during the course of a TAC case. Additionally, Cisco will periodically collect configuration and operational health data from your devices and process that data through our automated problem detection system, and proactively notify you of issues detected. To view a sample

Internet connection is required.

Als de registratie van de slimme licentie succesvol was, wordt de productregistratiestatus **geregistreerd**, zoals in deze afbeelding wordt weergegeven.

**FMC Smart Licenses** Overview Analysis Policies Devices Objects AMP Intelligence Dep

### Smart License Status

Cisco Smart Software Manager ✖ ↺

Usage Authorization:	✔	Authorized (Last Synchronized On Jun 15 2020)
Product Registration:	✔	Registered (Last Renewed On Jun 15 2020)
Assigned Virtual Account:		[REDACTED]
Export-Controlled Features:		Enabled
Cisco Success Network:		<a href="#">Enabled</a> ⓘ
Cisco Support Diagnostics:		<a href="#">Disabled</a> ⓘ

### Smart Licenses

Filter Devices...

License Type/Device Name	License Status	Device Type
> Base (5)	✔	
Malware (0)		
Threat (0)		
URL Filtering (0)		

Als u een licentie op basis van de voorwaarden aan het FTD-apparaat wilt toewijzen, selecteert u **Licenties bewerken**. Selecteer en voeg vervolgens een beheerd apparaat toe aan het gedeelte Apparaten met licentie. Selecteer tot slot de knop **Toepassen** zoals in deze afbeelding.

### Edit Licenses

Malware Threat URL Filtering AnyConnect Apex AnyConnect Plus AnyConnect VPN Only

Devices without license ↺

Q Search

**FTD**

**1**

Add **2**

Devices with license (1)

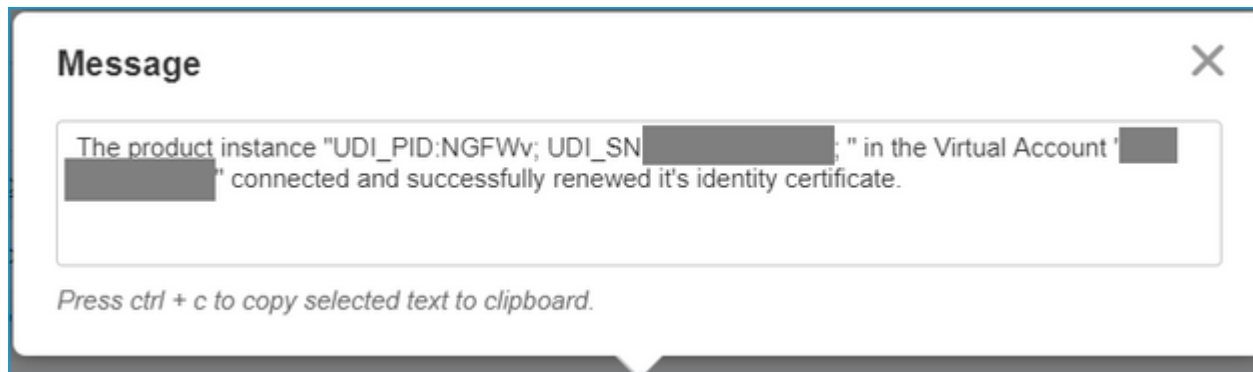
**FTD**

**3**

Cancel **Apply**

## Bevestiging in Smart Software Manager (SSM)-kant

Het succes van de registratie van de Slimme Licentie van het VCC kan worden bevestigd door **Inventory > Event Log** in CSSM, zoals in deze afbeelding wordt getoond.

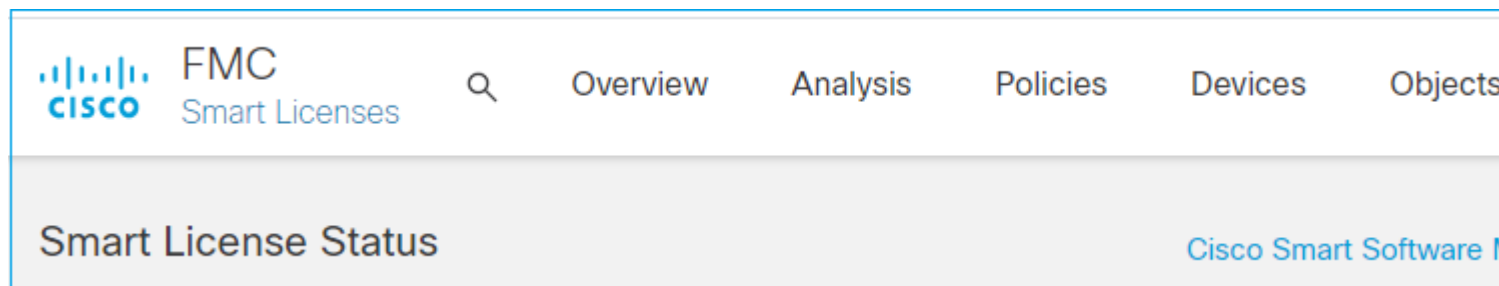


De registratiestatus van het VCC kan worden bevestigd op basis van de **inventaris > Product Instanties**. Controleer het gebeurtenissenlogboek van het tabblad **Gebeurtenislogboek**. De Smart License-registratie en de gebruiksstatus kunnen worden gecontroleerd via het tabblad **Inventaris > Licenties**. Controleer of de op voorwaarden gebaseerde licentie die u hebt aangeschaft, correct wordt gebruikt en er geen meldingen zijn die op onvoldoende licenties wijzen.

## Registratie van FMC Smart License

### De-registratie van het VCC uit Cisco SSM opheffen

Als u de licentie om de een of andere reden wilt vrijgeven of een ander token wilt gebruiken, navigeert u naar **System > Licenties > Slimme licenties** en selecteert u de knop Registreren verwijderen, zoals in deze afbeelding wordt weergegeven.



### Registratie uit SSM-kant verwijderen

Open Smart Software Manager ([Cisco Smart Software Manager](#)) en selecteer in de **lijst > Product-instanties** de optie **Verwijderen** op het gewenste VCC. Selecteer vervolgens **Product Instance verwijderen** om het VCC te verwijderen en de toegewezen licenties vrij te geven, zoals in deze afbeelding.

Cisco Software Central > Smart Software Licensing

## Smart Software Licensing


Alerts **Inventory** Convert to Smart Licensing | Reports | Preferences | On-Prem Accounts | Activity

Virtual Account: [REDACTED]

General Licenses **Product Instances** Event Log

Authorize License-Enforced Features... [Icon] fmcv

Name	Product Type	Last Contact
fmcv-rabc1	FP	2022-Sep-13 09:28:40
<b>fmcvxyz1</b>	FP	2022-Sep-12 14:01:45

 **Confirm Remove Product Instance** [Close]

If you continue, the product instance "fmcvxyz1" will no longer appear in the Smart Software Manager and will no longer be consuming any licenses. In order to bring it back, you will need to re-register the product instance.

**Remove Product Instance** Cancel

## RMA

Als het VCC RMA's is, deregistreert u het VCC bij Cisco Smart Software Manager (CSSM) met de stappen in het vak **FMC Smart License Deregistration > Registratie uit SSM verwijderen** en registreert u het VCC opnieuw bij CSSM met de stappen in het vak **FMC Smart License Registration**.

## Problemen oplossen

### Verificatie van tijdsynchronisatie

Open de FMC CLI (bijvoorbeeld SSH) en controleer of de tijd juist is en gesynchroniseerd is met een vertrouwde NTP-server. Omdat het certificaat wordt gebruikt voor de authenticatie van slimme licenties, is het belangrijk dat het VCC over de juiste tijdsinformatie beschikt:

<#root>



```
admin@FMC:~$
```

```
date  
Thu
```

```
Jun 14 09:18:47 UTC 2020
```

```
admin@FMC:~$
```

```
admin@FMC:~$
```

```
ntpq -pn
```

```
remote          refid          st t when poll reach  delay  offset jitter  
=====
```

*10.0.0.2	171.68.xx.xx	2 u	387	1024	377	0.977	0.469	0.916
127.127.1.1	.SFCL.	13 l	-	64	0	0.000	0.000	0.000

Controleer vanuit de FMC UI de NTP-serverwaarden vanuit **System > Configuration > Time Synchronization**.

### Naamresolutie inschakelen en bereikbaarheid controleren op tools.cisco.com

Zorg ervoor dat het VCC een FQDN kan oplossen en bereikbaar is via tools.cisco.com:

```
<#root>
```

```
>
```

```
expert
```

```
admin@FMC2000-2:~$
```

```
sudo su
```

```
Password:
```

```
root@FMC2000-2:/Volume/home/admin# ping tools.cisco.com
```

```
PING tools.cisco.com (173.37.145.8) 56(84) bytes of data.
```

```
64 bytes from tools2.cisco.com (173.37.145.8): icmp_req=1 ttl=237 time=163 ms
```

```
64 bytes from tools2.cisco.com (173.37.145.8): icmp_req=2 ttl=237 time=163 ms
```

Controleer vanuit de FMC UI het IP-beheer en de DNS-server via **System > Configuration > Management Interfaces**.

### Controleer de toegang tot HTTPS (TCP 443) van het VCC tot tools.cisco.com

Gebruik de opdracht Telnet of curl om ervoor te zorgen dat het VCC HTTPS-toegang heeft tot tools.cisco.com. Als de TCP 443-communicatie is verbroken, controleert u of deze niet is geblokkeerd door een firewall en of er geen SSL-decryptie-apparaat in het pad is.

```
<#root>
```

```
root@FMC2000-2:/Volume/home/admin#
```

```
telnet tools.cisco.com 443
```

```
Trying 72.163.4.38...
```

```
Connected to tools.cisco.com.
```

Escape character is '^]'.  
^CConnection closed by foreign host.

<--- Press Ctrl+C

Curl test:

<#root>

root@FMC2000-2:/Volume/home/admin#

curl -vvk https://tools.cisco.com

\*

Trying 72.163.4.38...

\* TCP\_NODELAY set

\* Connected to tools.cisco.com (72.163.4.38) port 443 (#0)

\* ALPN, offering http/1.1

\* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH

\* successfully set certificate verify locations:

\* CAfile: /etc/ssl/certs/ca-certificates.crt

CApath: none

\* TLSv1.2 (OUT), TLS header, Certificate Status (22):

\* TLSv1.2 (OUT), TLS handshake, Client hello (1):

\* TLSv1.2 (IN), TLS handshake, Server hello (2):

\* TLSv1.2 (IN), TLS handshake, Certificate (11):

\* TLSv1.2 (IN), TLS handshake, Server finished (14):

\* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):

\* TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):

\* TLSv1.2 (OUT), TLS handshake, Finished (20):

\* TLSv1.2 (IN), TLS change cipher, Change cipher spec (1):

\* TLSv1.2 (IN), TLS handshake, Finished (20):

\* SSL connection using TLSv1.2 / AES128-GCM-SHA256

\* ALPN, server accepted to use http/1.1

\* Server certificate:

\* subject: C=US; ST=CA; L=San Jose; O=Cisco Systems, Inc.; CN=tools.cisco.com

\* start date: Sep 17 04:00:58 2018 GMT

\* expire date: Sep 17 04:10:00 2020 GMT

\* issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID SSL ICA G2

\* SSL certificate verify ok.

> GET / HTTP/1.1

> Host: tools.cisco.com

> User-Agent: curl/7.62.0

> Accept: \*/\*

>

< HTTP/1.1 200 OK

< Date: Wed, 17 Jun 2020 10:28:31 GMT

< Last-Modified: Thu, 20 Dec 2012 23:46:09 GMT

< ETag: "39b01e46-151-4d15155dd459d"

< Accept-Ranges: bytes

< Content-Length: 337

< Access-Control-Allow-Credentials: true

< Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS

< Access-Control-Allow-Headers: Content-type, fromPartyID, inputFormat, outputFormat, Authorization, Cor

< Content-Type: text/html

< Set-Cookie: CP\_GUTC=10.163.4.54.1592389711389899; path=/; expires=Mon, 16-Jun-25 10:28:31 GMT; domain=

< Set-Cookie: CP\_GUTC=10.163.44.92.1592389711391532; path=/; expires=Mon, 16-Jun-25 10:28:31 GMT; domain=

```
< Cache-Control: max-age=0
< Expires: Wed, 17 Jun 2020 10:28:31 GMT
<
<html>
<head>
<script language="JavaScript">

var input = document.URL.indexOf('intellishield');
if(input != -1) {
  window.location="https://intellishield.cisco.com/security/alertmanager/";
}
else {
  window.location="http://www.cisco.com";
};

</script>
</head>

<body>
<a href="http://www.cisco.com">www.cisco.com</a>
</body>
</html>
* Connection #0 to host tools.cisco.com left intact
root@FMC2000-2:/Volume/home/admin#
```

## DNS-verificatie

Controleer een geslaagde oplossing op tools.cisco.com:

```
<#root>

root@FMC2000-2:/Volume/home/admin#

nslookup tools.cisco.com

Server:          192.0.2.100
Address:         192.0.2.100#53

Non-authoritative answer:

Name:   tools.cisco.com
Address: 72.163.4.38
```

## Proxy-verificatie

Als apProxy wordt gebruikt, controleer dan de waarden op zowel het VCC als de proxyserver-side. Controleer in het VCC of het VCC de juiste proxyserver IP en poort gebruikt.

```
<#root>

root@FMC2000-2:/Volume/home/admin#

cat /etc/sf/smart_callhome.conf

KEEP_SYNC_ACTIVE:1
PROXY_DST_URL:https://tools.cisco.com/its/service/oddce/services/DDCEService
```

PROXY\_SRV:192.0.xx.xx

PROXY\_PORT:80

In de FMC UI kunnen de proxywaarden worden bevestigd via **System > Configuration > Management Interfaces**.

Indien de waarden van de FMC-zijde juist zijn, controleer dan de waarden van de proxy-serverzijde (bijvoorbeeld, indien de proxy-server toegang verleent vanuit het FMC en naar tools.cisco.com. Bovendien, laat verkeer en certificaatuitwisseling door de volmacht toe. Het VCC gebruikt een certificaat voor de registratie van slimme vergunningen).

## Verlopen Token ID

Controleer of de afgegeven token-id niet is verlopen. Als deze is verlopen, vraagt u de Smart Software Manager-beheerder een nieuwe token op te geven en de slimme licentie opnieuw te registreren met de nieuwe Token ID.

## De FMC-gateway wijzigen

Er kunnen gevallen zijn waarin Smart License authenticatie niet correct kan worden uitgevoerd vanwege de effecten van een relay proxy of SSL decryptie apparaat. Indien mogelijk de route voor de internettoegang van het VCC wijzigen om deze apparaten te vermijden en de registratie van de slimme vergunning opnieuw proberen.

## Bekijk de Health Events op FMC

Ga in het VCC naar **Systeem > Gezondheid > Evenementen** en controleer de status van de Smart License Monitor module op fouten. Bijvoorbeeld, als de verbinding mislukt vanwege een verlopen certificaat; een fout, zoals **id gecertificeerd verlopen** wordt gegenereerd, zoals in deze afbeelding.

No Search Constraints (Edit Search)						
Health Monitor Table View of Health Events						
	Module Name ×	Test Name ×	Time ×	Description ×	Value ×	Un
▼	Smart License Monitor	Smart License Monitor	2020-06-17 13:48:55	Smart License usage is out of compliance.	0	Lic
▼	Appliance Heartbeat	Appliance Heartbeat	2020-06-17 13:48:55	Appliance mzafeiro_FP2110-2 is not sending heartbe...	0	

## Controleer het gebeurtenissenlogboek aan de SSM-kant

Als het VCC verbinding kan maken met de CSSM, controleert u het gebeurtenissenlogboek van de connectiviteit in **Inventory > Event Log**. Controleer of er dergelijke gebeurtenislogbestanden of foutlogbestanden in de CSM zijn. Indien er geen probleem is met de waarden/exploitatie van de VCC-locatie en er geen gebeurtenislogboek aan de zijde van de CSSM is, bestaat de mogelijkheid dat er een probleem is met de route tussen het VCC en de CSSM.

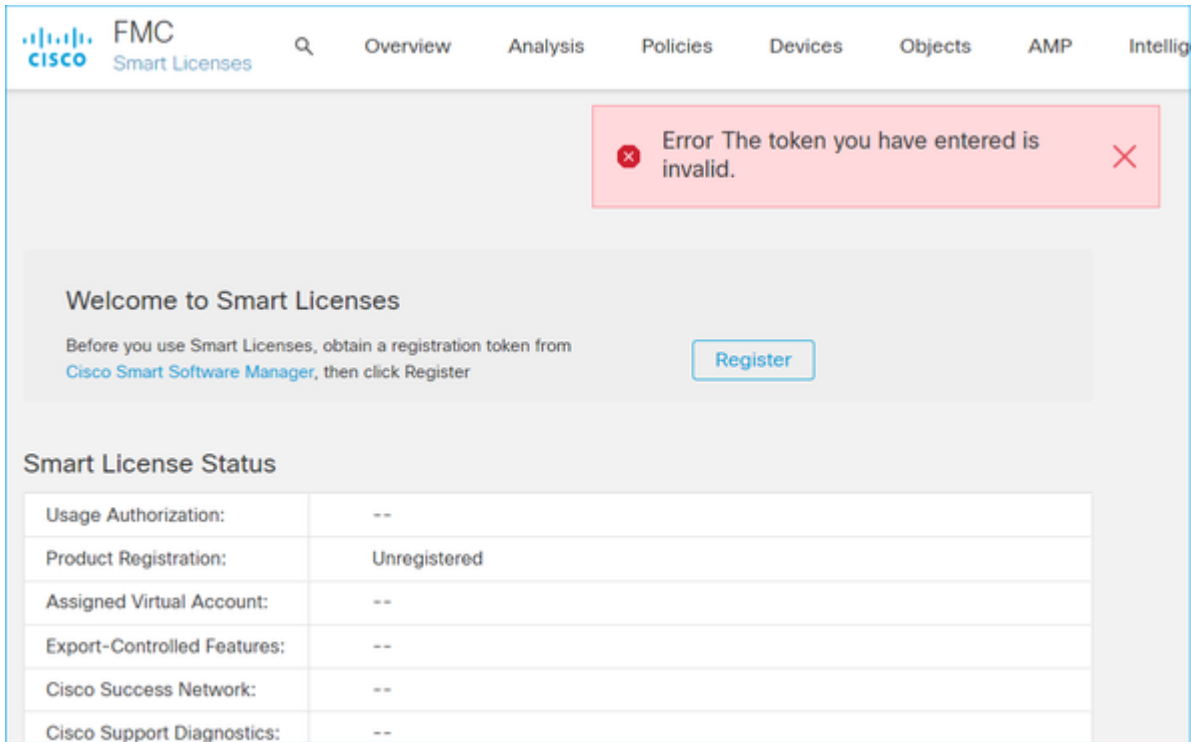
## Veelvoorkomende problemen

Samenvatting van de registratie- en toelatingsstaten:

<b>Registratiestatus van product</b>	<b>Toepassingsstatus</b>	<b>Opmerkingen</b>
NIET GEREGISTREERD	â€”	Het VCC staat niet geregistreerd of wordt niet geëvalueerd. Dit is de begintoestand na de installatie van het VCC of na het verstrijken van de evaluatievergunning voor 90 dagen.
Geregistreerd	geautoriseerd	Het FMC is geregistreerd bij Cisco Smart Software Manager (CSSM) en er zijn FTD-apparaten geregistreerd met een geldig abonnement.
Geregistreerd	Vergunning verlopen	Het VCC heeft niet meer dan 90 dagen gecommuniceerd met het Cisco-licentiestuknummer.
Geregistreerd	NIET GEREGISTREERD	Het FMC is geregistreerd bij Cisco Smart Software Manager (CSSM), maar er zijn geen FTD-apparaten geregistreerd in het FMC.
Geregistreerd	Out-of-Compliance	Het FMC is geregistreerd bij Cisco Smart Software Manager (CSSM), maar er zijn FTD-apparaten geregistreerd met een ongeldig abonnement(en). Een FTD (FP4112)-apparaat maakt bijvoorbeeld gebruik van THREAT-abonnement, maar met Cisco Smart Software Manager (CSSM) zijn er geen THREAT-abonnementen beschikbaar voor FP4112.
Evaluatie (90 dagen)	N.v.t.	De evaluatieperiode is in gebruik, maar er zijn geen FTD-apparaten geregistreerd in het VCC.

## **Casestudy 1. Ongeldige token**

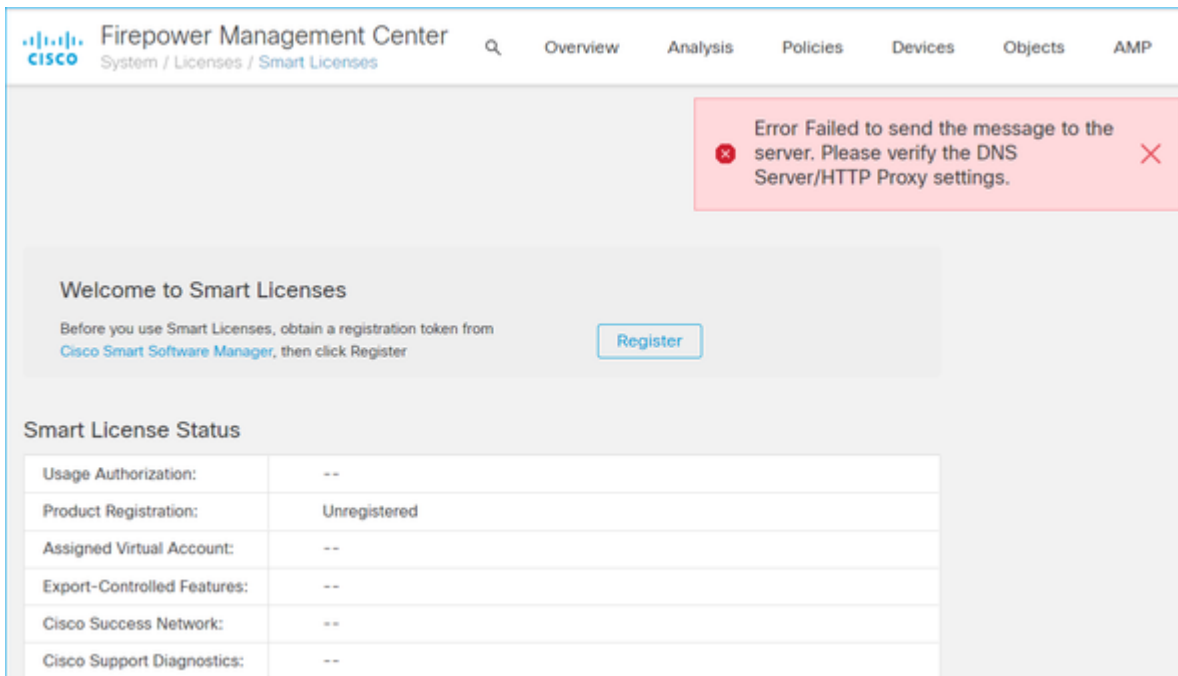
Symptoom: registratie op de CSSM mislukt snel (~10) vanwege een ongeldig token, zoals in deze afbeelding.



Resolutie: gebruik een geldige token.

## Casestudy 2. Ongeldige DNS

Symptoom: na enige tijd is registratie op de CSSM mislukt (~25 seconden), zoals in deze afbeelding wordt weergegeven.



Controleer het /var/log/process\_stdout.log bestand. De DNS kwestie wordt gezien:

```
<#root>
```

```
root@FMC2000-2: /Volume/home/admin#
```

```
cat /var/log/process_stdout.log
```

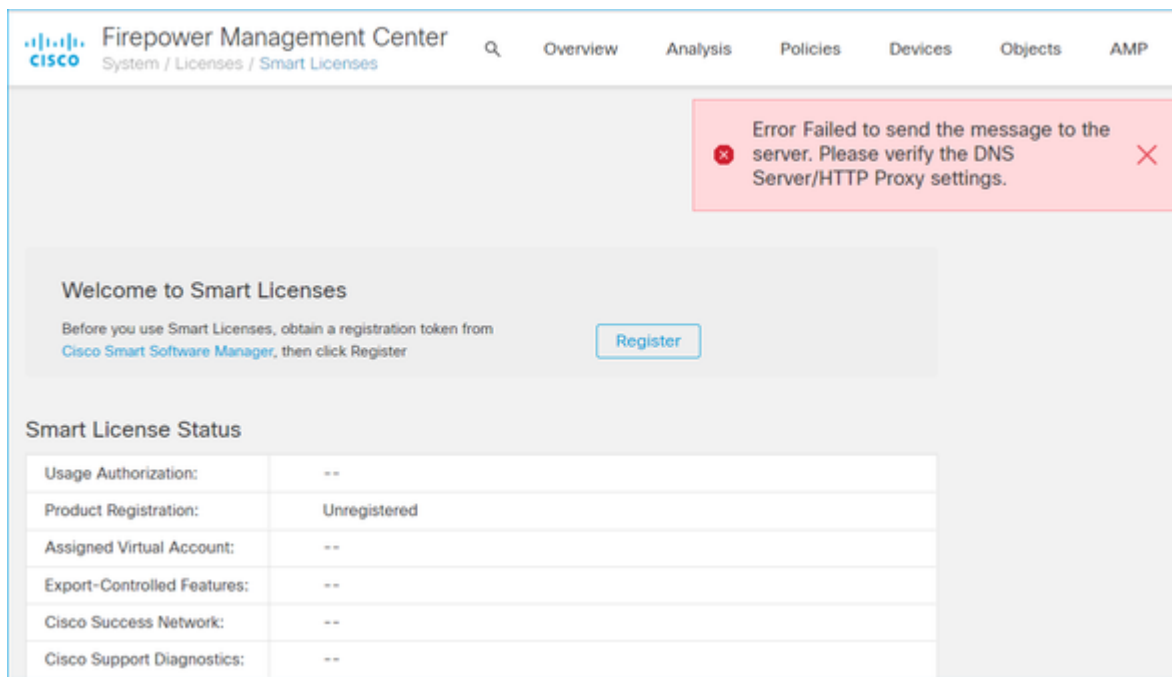
```
2020-06-25 09:05:21 sla[24043]: *Thu Jun 25 09:05:10.989 UTC: CH-LIB-ERROR: ch_pf_curl_send_msg[494], failed to perform, err code 6, err string
```

```
"Couldn't resolve host name"
```

Resolutie: CSSM fout in hostname-resolutie. De resolutie is om DNS te configureren, indien niet geconfigureerd, of de DNS problemen op te lossen.

### Case Study 3. Ongeldige tijdwaarden

Symptoom: na enige tijd is registratie op de CSSM mislukt (~25 seconden), zoals in deze afbeelding wordt weergegeven.



Controleer het `/var/log/process_stdout.log` bestand. De certificaatkwesties worden gezien:

```
<#root>
```

```
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_curl_request_init[59],
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_curl_post_prepare[299],
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_curl_post_prepare[302],
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_curl_head_init[110],
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-ERROR: ch_pf_curl_send_msg[494],
```

```
failed to perform, err code 60, err string "SSL peer certificate or SSH remote key was not OK"
```

```
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-TRACE: ch_pf_http_unlock[330], unlc
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-TRACE: ch_pf_send_http[365], send h
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-TRACE: ch_pf_curl_is_cert_issue[514],
```

```
cert issue checking, ret 60, url https://tools.cisco.com/its/service/odcce/services/DDCEService
```

Controleer de VCC-tijdwaarde:

<#root>

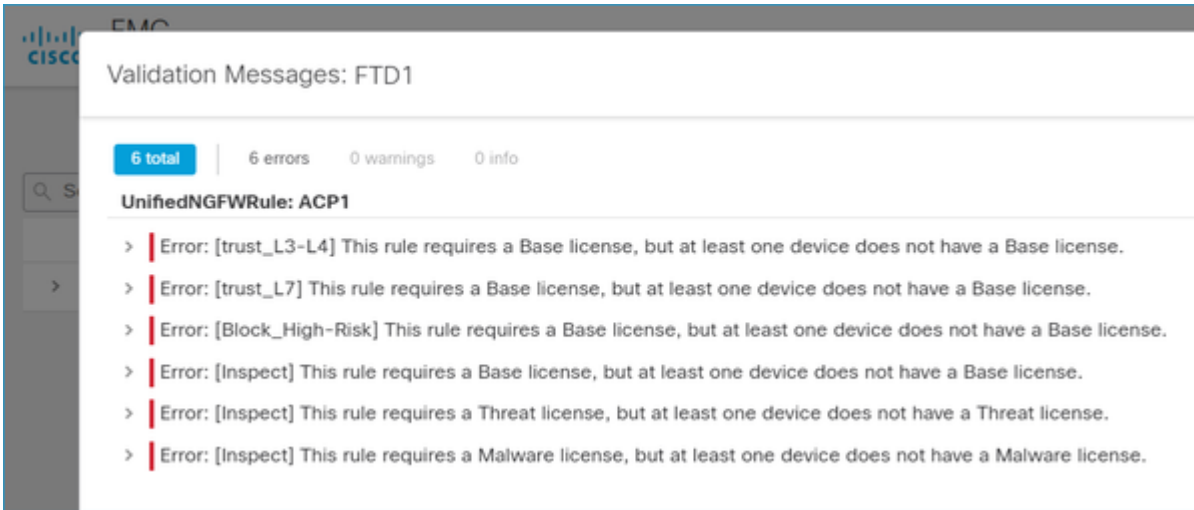
root@FMC2000-2: /Volume/home/admin#

date

Fri Jun 25 09:27:22 UTC 2021

## Case study 4. Geen abonnement

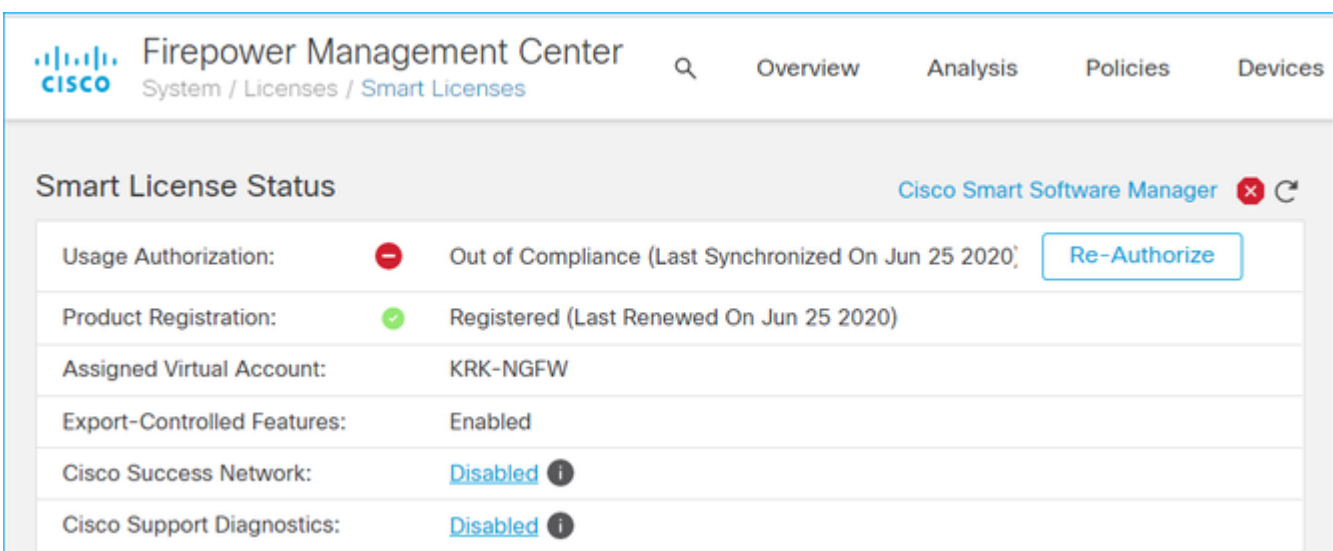
Als er geen licentieabonnement voor een specifieke functie is, kan het VCC niet worden ingezet:



Resolutie: Het is nodig om het vereiste abonnement op het apparaat te kopen en toe te passen.

## Case study 5. Out-of-Compliance (OSC)

Als er geen recht op FTD-abonnementen bestaat, gaat de slimme FMC-licentie naar de staat van de niet-naleving (OSC):



Controleer in de CSM de meldingen op fouten:



License	Billing	Purchased	In Use	Balance	Alerts	Actions
<input type="checkbox"/> FPR4110 Threat Defense Threat Protection	Prepaid	75	2	+ 73		Actions
<input type="checkbox"/> FPR4110 Threat Defense URL Filtering	Prepaid	75	0	+ 75		Actions
<input type="checkbox"/> FPR4115 Threat Defense Malware Protection	Prepaid	0	1	-1	Insufficient Licenses	Actions
<input type="checkbox"/> FPR4115 Threat Defense Threat Protection	Prepaid	0	1	-1	Insufficient Licenses	Actions
<input type="checkbox"/> FPR4115 Threat Defense URL Filtering	Prepaid	0	1	-1	Insufficient Licenses	Actions
<input type="checkbox"/> FPR4120 Threat Defense Malware Protection	Prepaid	75	0	+ 75		Actions
<input type="checkbox"/> FPR4120 Threat Defense Threat Protection	Prepaid	75	0	+ 75		Actions

## Case study 6. Geen sterke encryptie

Als alleen de basislicentie wordt gebruikt, is Data Encryption Standard (DES)-codering ingeschakeld in de FTD LINA-engine. In dat geval mislukken implementaties zoals L2L Virtual Private Network (VPN) met sterkere algoritmen:

Validation Messages

Device: **FTD1** (1 error, 1 warning, 0 info)

Site To Site VPN: FTD\_VPN

Error: Strong crypto (i.e encryption algorithm greater than DES ) for VPN topology FTD\_VPN is not supported. This may be because FMC is running in evaluation mode or smart license account is not entitled for strong crypto. MSG\_SEPARATOR IKEv2 PolicyTITLE\_SEPARATORAES-GCM-NUL-SHA MSG\_SEPARATORMSG\_SEPARATOR

Firepower Management Center

System / Licenses / Smart Licenses

Smart License Status

Usage Authorization: ✔ Authorized (Last Synchronized On Jun 25 2020)

Product Registration: ✔ Registered (Last Renewed On Jun 25 2020)

Assigned Virtual Account: KRK-NGFW

**Export-Controlled Features: Disabled** [Request Export Key](#)

Cisco Success Network: Enabled ⓘ

Cisco Support Diagnostics: Disabled ⓘ

Resolutie: registreer het VCC bij de CSSM en laat een sterk encryptie-kenmerk inschakelen.

## Aanvullende opmerkingen

### Melding van slimme licentiestatus instellen

## E-mailmelding via SSM

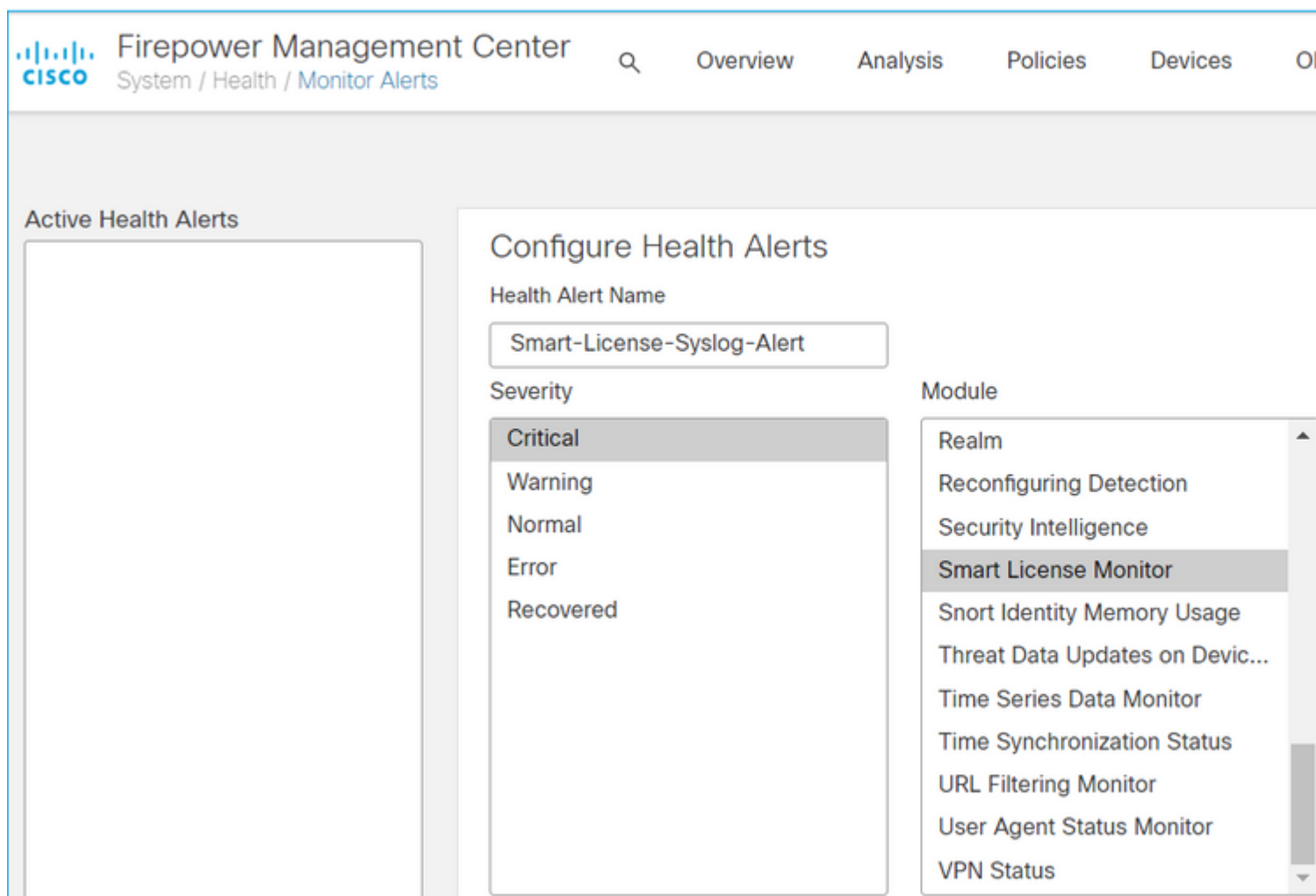
Aan de SSM-kant maakt SSM Email Notification de ontvangst van samenvattende e-mails voor verschillende gebeurtenissen mogelijk. Bijvoorbeeld een melding bij gebrek aan licentie of bij verlopen licenties. Er kunnen meldingen van een verbinding met een productexemplaar of een update van een storing worden ontvangen.

Deze functie is zeer nuttig om het optreden van functionele beperkingen als gevolg van het verlopen van de licentie op te merken en te voorkomen.

## Ontvang meldingen van gezondheidsmeldingen van het VCC

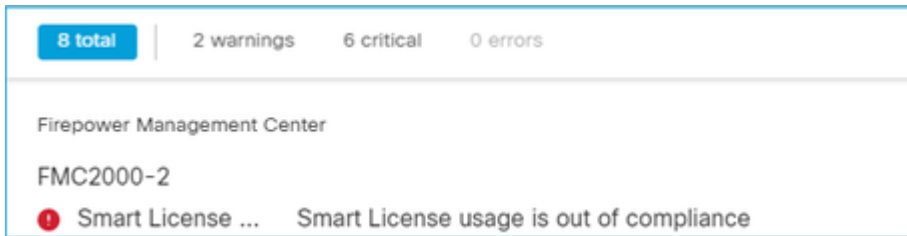
Van de kant van het VCC is het mogelijk om een Health Monitor Alert te configureren en een waarschuwingsbericht te ontvangen van een gezondheidsgebeurtenis. De Module Smart License Monitor is beschikbaar om de status van de Smart License te controleren. De monitorwaarschuwing ondersteunt Syslog, Email en SNMP-trap.

Dit is een configuratievoorbeeld om een Syslog-bericht te krijgen wanneer een Smart License monitor-gebeurtenis plaatsvindt:



The screenshot displays the Cisco Firepower Management Center interface. The top navigation bar includes the Cisco logo, the title "Firepower Management Center", and a search icon. Below the title, the breadcrumb "System / Health / Monitor Alerts" is visible. The main content area is divided into two sections: "Active Health Alerts" on the left, which is currently empty, and "Configure Health Alerts" on the right. In the "Configure Health Alerts" section, the "Health Alert Name" field is set to "Smart-License-Syslog-Alert". The "Severity" dropdown menu is open, showing options: "Critical" (selected), "Warning", "Normal", "Error", and "Recovered". The "Module" dropdown menu is also open, showing a list of modules: "Realm", "Reconfiguring Detection", "Security Intelligence", "Smart License Monitor" (selected), "Snort Identity Memory Usage", "Threat Data Updates on Devic...", "Time Series Data Monitor", "Time Synchronization Status", "URL Filtering Monitor", "User Agent Status Monitor", and "VPN Status".

Dit is een voorbeeld van een gezondheidswaarschuwing:



Het door het VCC gegenereerde Syslog-bericht is:

<#root>

Mar 13 18:47:10 xx.xx.xx.xx Mar 13 09:47:10 FMC :

HMNOTIFY: Smart License Monitor (Sensor FMC)

: Severity: critical: Smart License usage is out of compliance

Raadpleeg de [gezondheidsbewaking](#) voor aanvullende informatie over de meldingen voor de gezondheidsmonitor.

## Meervoudige VCC's op dezelfde slimme account

Wanneer meerdere VCC's op dezelfde slimme rekening worden gebruikt, moet elke VCC-hostnaam uniek zijn. Wanneer meerdere VCC's in CSSM's worden beheerd, moet, om elk VCC van elkaar te onderscheiden, de hostnaam van elk VCC uniek zijn. Dit is handig voor het onderhoud van de Slimme Licentie van het FMC.

## FMC moet internetconnectiviteit behouden

Na registratie controleert het FMC elke 30 dagen de Smart License Cloud en de licentiestatus. Indien het VCC gedurende 90 dagen niet kan communiceren, blijft de erkende functie behouden, maar blijft de status **Verlopen vergunning behouden**. Zelfs in deze staat probeert het FMC voortdurend verbinding te maken met de Smart License Cloud.

## Meervoudige FMCv implementeren

Als het Firepower System wordt gebruikt in een virtuele omgeving, wordt kloon (warm of koud) niet officieel ondersteund. Elk Firepower Management Center Virtual (FMCv) is uniek omdat het authenticatie informatie in heeft. Om meerdere FMCv te kunnen gebruiken, moet de FMCv worden gemaakt uit het OVF-bestand (Open Virtualization Format). Raadpleeg voor meer informatie over deze beperking de [Cisco Firepower Management Center Virtual for VMware Implementation Quick Start Guide](#).

## Veelgestelde vragen

### Hoeveel apparaatlicenties zijn er in FTD HA vereist?

Wanneer twee FTD's worden gebruikt in High Availability is voor elk apparaat een licentie vereist. Er zijn bijvoorbeeld twee Threat- en Malware-licenties nodig als het Intrusive Protection System (IPS) en Advanced Malware Protection (AMP) op het FTD HA-paar worden gebruikt.

### Waarom worden er geen AnyConnect-licenties gebruikt door FTD?

Zorg ervoor dat de AnyConnect-licentie is ingeschakeld nadat de FMC-account is geregistreerd bij de Smart Account. Als u de licentie wilt inschakelen, navigeert u naar **FMC > Apparaten**, kies uw apparaat en selecteer **Licentie**. Selecteer het pictogram **Potlood**, kies de licentie die wordt gedeponerd in de Smart Account en selecteer **Opslaan**.

### **Waarom is slechts één AnyConnect-licentie 'in gebruik' in de Smart Account als 100 gebruikers zijn verbonden?**

Dit is verwacht gedrag, aangezien Smart Account het aantal apparaten bijhoudt die deze licentie ingeschakeld hebben, niet actieve gebruikers verbonden.

### **Waarom is er de fout? Device does not have the AnyConnect License na configuratie en implementatie van een Remote Access VPN door het VCC?**

Zorg ervoor dat het VCC is geregistreerd in de Smart License Cloud. Het verwachte gedrag is dat de configuratie voor toegang op afstand niet kan worden ingezet wanneer het VCC niet is geregistreerd of in de evaluatiemodus. Als het VCC is geregistreerd, controleert u of de AnyConnect-licentie in uw Smart Account aanwezig is en aan het apparaat is toegewezen.

Om een licentie toe te wijzen, bevaan in **FMC Devices**, selecteer uw apparaat, **Licentie** (potlood pictogram). Kies de licentie in de slimme account en selecteer **Opslaan**.

### **Waarom is er de fout? Remote Access VPN with SSL cannot be deployed when Export-Controlled Features (Strong-crypto) are disabled wanneer er een plaatsing van een configuratie van Remote Access VPN is?**

De Remote Access VPN die op de FTD wordt geïmplementeerd, vereist dat een Strong Encryption-licentie is ingeschakeld. NLZorg ervoor dat een Strong Encryption-licentie op het VCC is ingeschakeld. Om de status van de Strong Encryption-licentie te controleren, bevaan aan de **FMC-systeem > Licenties > Slimme licenties** controleer of door export gecontroleerde functies zijn ingeschakeld.

### **Hoe kunt u een sterke encryptie-licentie inschakelen als Export-Controlled Features gehandicapt is?**

Deze functionaliteit wordt automatisch ingeschakeld als het token dat wordt gebruikt tijdens de registratie van het VCC in de Smart Account Cloud de optie **Export-Controlled functionaliteit toestaan op de producten die met dit token zijn** ingeschakeld. Als deze optie niet is ingeschakeld voor het token, verwijdert u de registratie van het VCC en registreert u het opnieuw met deze optie ingeschakeld.

### **Wat kan er worden gedaan als de optie 'Export-Controlled functionaliteit op de met dit token geregistreerde producten toestaan' niet beschikbaar is als het token wordt gegenereerd?**

Neem contact op met uw Cisco-accountteam.

### **Waarom wordt de fout 'Strong crypto (dat wil zeggen, encryptie algoritme groter dan DES) voor VPN topologie s2s niet ondersteund' ontvangen?**

Deze fout wordt weergegeven wanneer het VCC de evaluatiemodus gebruikt of wanneer de Smart License Account geen recht heeft op een Strong Encryption-licentie. VControleer of het VCC is geregistreerd bij de Licentieautoriteit en **of de functionaliteit voor exportcontrole van de met deze token geregistreerde producten** is ingeschakeld. Als de slimme account geen sterke encryptie-licentie mag gebruiken, is de implementatie van VPN Site-to-Site-configuratie met algoritmen die sterker zijn dan DES, niet toegestaan.

### **Waarom wordt een "out of compliance"-status bij het VCC ontvangen?**

Het apparaat kan niet meer aan de regels voldoen wanneer een van de beheerde apparaten gebruik maakt van niet-beschikbare licenties.

### **Hoe kan de "Out of Compliance"-status worden gecorrigeerd?**

Volg de stappen die worden beschreven in de Firepower Configuration Guide:

1. Bekijk de sectie Smart Licences onderaan de pagina om te bepalen welke licenties nodig zijn.
2. Schaf de vereiste licenties aan via uw gebruikelijke kanalen.
3. In Cisco Smart Software Manager (<https://software.cisco.com/#SmartLicensing-Inventory>) Controleer of de licenties in uw virtuele account worden weergegeven.
4. Selecteer in het VCC Systeem > Licenties > Slimme licenties.
5. Selecteer **Opnieuw autoriseren**.

De volledige procedure vindt u in [Licensing the Firepower System](#).

### **Wat zijn de functies van Firepower Threat Defense Base?**

De basislicentie maakt het mogelijk:

- Configuratie van FTD-apparaten naar switch en route (inclusief DHCP Relay en NAT).
- Configuratie van FTD-apparaten in een High Availability (HA)-modus.
- Configuratie van beveiligingsmodules als een cluster binnen een Firepower 9300 chassis (intra-chassis cluster).
- Configuratie van Firepower 9300 of Firepower 4100 Series apparaten (FTD) als een cluster (inter-chassis cluster).
- Configuratie van gebruikers- en toepassingscontrole en toevoeging van gebruikers- en toepassingsvoorwaarden aan toegangscontroleregels.

### **Hoe kan de Firepower Threat Defence Base Features Licentie worden verkregen?**

Een basislicentie wordt automatisch meegeleverd bij elke aankoop van een Firepower Threat Defence of Firepower Threat Defence Virtuele apparaat. Het wordt automatisch toegevoegd aan je Smart Account wanneer FTD zich registreert bij het FMC.

### **Welke IP-adressen moeten worden toegestaan op het pad tussen het VCC en de Smart License Cloud?**

Het VCC gebruikt het IP-adres op poort 443 om te communiceren met de Smart License Cloud.

Dat IP-adres (<https://tools.cisco.com>) is opgelost aan deze IP-adressen:

- 72.163.4.38
- 173.37.145.8

## **Gerelateerde informatie**

- [Configuratiehandleidingen voor Firepower Management Center](#)
- [Cisco Live Smart Licensing - Overzicht: BRKARC-2034](#)
- [Licenties voor Cisco Secure Firewall Management Center](#)
- [Veelgestelde vragen over Cisco Smart Software Licensing](#)

## 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.