

FMC- und FTD Smart License-Registrierung und allgemeine Probleme zur Fehlerbehebung verwenden

Inhalt

[Einleitung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Hintergrundinformationen](#)
[FMC Smart-Lizenzregistrierung](#)
[Voraussetzungen](#)
[FMC Smart-Lizenzregistrierung](#)
[Bestätigung auf Seite von Smart Software Manager \(SSM\)](#)
[Aufhebung der Registrierung von FMC Smart-Lizenzen](#)
[RMA](#)
[Fehlerbehebung](#)
[Häufige Probleme](#)
[Anwenderbericht 1. Ungültiges Token](#)
[Anwenderbericht 2. Ungültiger DNS](#)
[Anwenderbericht 3. Ungültige Zeitwerte](#)
[Fallstudie 4. Kein Abonnement](#)
[Anwenderbericht 5. Out-of-Compliance \(OOC\)](#)
[Fallstudie 6. Keine starke Verschlüsselung](#)
[Zusätzliche Hinweise](#)
[Benachrichtigung über Smart-Lizenzstatus festlegen](#)
[Statusbenachrichtigungen vom FMC abrufen](#)
[Mehrere FMCs auf demselben Smart Account](#)
[FMC muss Internetverbindung aufrechterhalten](#)
[Bereitstellung mehrerer FMCs](#)
[Häufig gestellte Fragen \(FAQ\)](#)
[Zugehörige Informationen](#)

Einleitung

Dieses Dokument beschreibt die Konfiguration der Smart License-Registrierung von Firepower Management Center auf Firepower Threat Defense-verwalteten Geräten.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

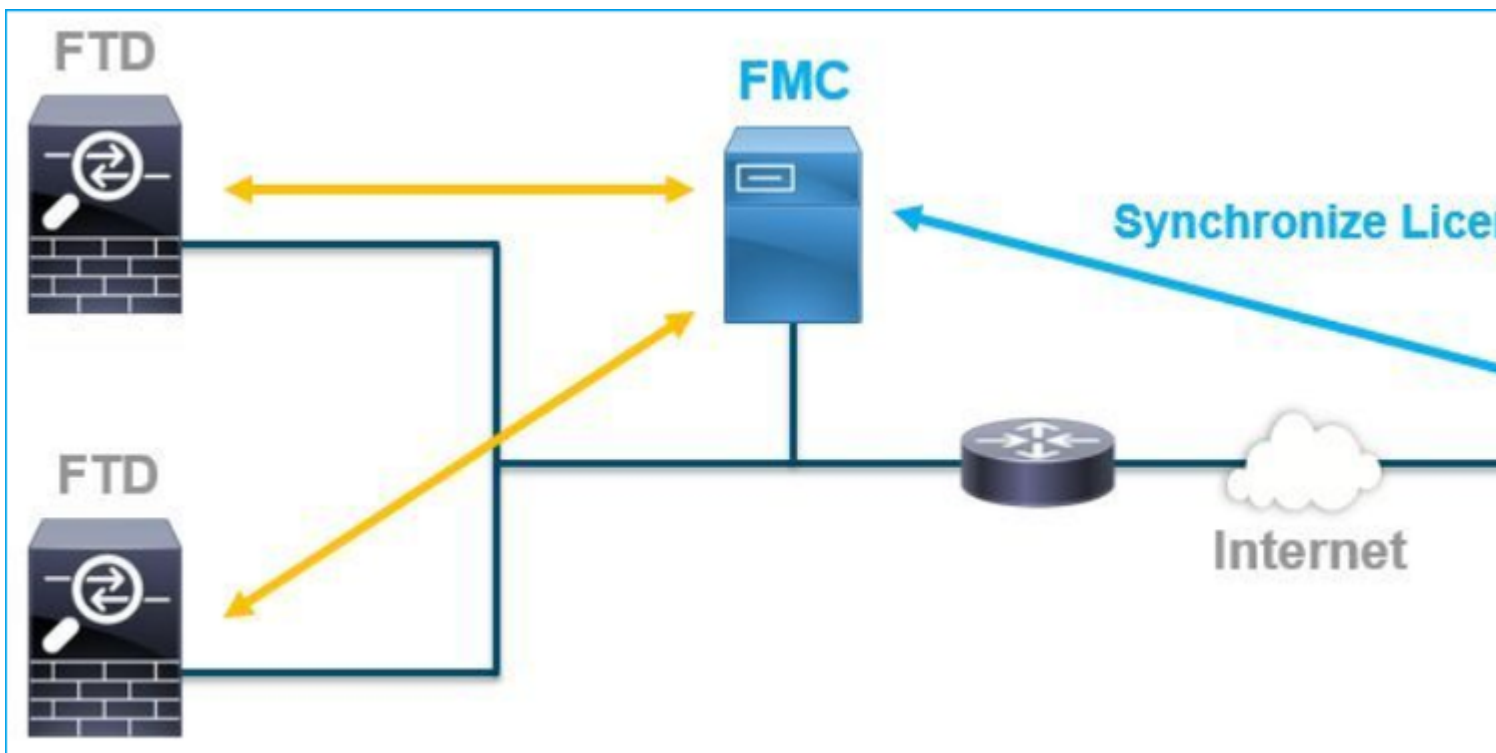
Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

FMC-, FTD- und Smart License-Registrierung.

Die Smart License-Registrierung erfolgt im FirePOWER Management Center (FMC). Das FMC kommuniziert über das Internet mit dem Cisco Smart Software Manager (CSSM) Portal. Im CSSM verwaltet der Firewall-Administrator den Smart Account und die zugehörigen Lizenzen. Das FMC kann Lizenzen für verwaltete Firepower Threat Defense (FTD)-Geräte frei zuweisen und löschen. Mit anderen Worten: Das FMC verwaltet Lizenzen für FTD-Geräte zentral.



Für die Verwendung bestimmter Funktionen von FTD-Geräten ist eine zusätzliche Lizenz erforderlich. Die Smart License-Typen, die Kunden einem FTD-Gerät zuweisen können, sind in [FTD-Lizenztypen und -beschränkungen](#) dokumentiert.

Die Base-Lizenz ist im FTD-Gerät enthalten. Diese Lizenz wird automatisch in Ihrem Smart Account registriert, wenn das FMC bei CSSM registriert ist.

Die laufzeitbasierten Lizenzen: Threat, Malware und URL-Filterung sind optional. Um lizenzbezogene Funktionen nutzen zu können, muss dem FTD-Gerät eine Lizenz zugewiesen werden.

Um eine FirePOWER Management Center Virtual (FMCv) für die FTD-Verwaltung zu verwenden, ist für die FMCv-**Gerätelizenz** ebenfalls eine **FirePOWER MCv-Gerätelizenz** in CSSM erforderlich.

Die FMCv-Lizenz ist in der Software enthalten und unbefristet.

Darüber hinaus enthält dieses Dokument Szenarien, die bei der Behebung von häufigen Registrierungsfehlern für Lizenzen helfen.

Weitere Informationen zu den Lizenzen finden Sie unter [Cisco FirePOWER System Feature Licenses](#) und [Frequently Asked Questions \(FAQ\) zu FirePOWER Licensing](#).

FMC Smart-Lizenzregistrierung

Voraussetzungen

1. Für die Smart License-Registrierung muss das FMC auf das Internet zugreifen. Da das Zertifikat zwischen dem FMC und der Smart License Cloud mit HTTPS ausgetauscht wird, stellen Sie sicher, dass sich kein Gerät im Pfad befindet, das die Kommunikation beeinflussen/verändern kann. (Firewall, Proxy, SSL-Verschlüsselungsgerät usw.).
2. Greifen Sie auf den CSSM zu, und geben Sie eine Token-ID aus **Inventory > General > New Token** (**Inventar > Allgemein > Neue Token**-Schaltfläche) aus, wie in diesem Bild dargestellt.

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
M2RmMWWkYmItZmRI...	2020-Jun-30 19:34:48 (in 16 ...)		Allowed	[Redacted]
ZmJjODEzYjEtOTJjZi0...	2021-May-22 00:54:03 (in 34...)		Allowed	

Wenn Sie eine starke Verschlüsselung verwenden möchten, aktivieren Sie die Option **Exportgesteuerte Nutzung zulassen für die mit diesem Token registrierten Produkte**. Wenn diese Option aktiviert ist, wird im Kontrollkästchen ein Häkchen angezeigt.

3. Wählen Sie **Token erstellen**.

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 [i](#)

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

FMC Smart-Lizenzregistrierung

Navigieren Sie zu **System > Licenses > Smart Licenses** (System > Lizenzen > Smart Licenses) auf dem FMC, und wählen Sie die Schaltfläche **Register** (Registrieren) aus, wie in diesem Bild dargestellt.

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:	--

Geben Sie die Token-ID in das Fenster für die Smart Licensing-Produktregistrierung ein, und wählen Sie **Apply Changes** (**Änderungen anwenden**) aus, wie in diesem Bild dargestellt.

Smart Licensing Product Registration

Product Instance Registration Token:

OWI4Mzc5MTAtNzQwYi00YTlVLTkyNTktMGMxNGJlYmRmNDUwLTE1OTQ3OTQ5%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.

Cancel

Apply Changes

Wenn die Smart License-Registrierung erfolgreich war, wird im Status der Produktregistrierung **"Registriert"** angezeigt, wie in dieser Abbildung dargestellt.

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:

Export-Controlled Features: Enabled

Cisco Success Network: Enabled

Cisco Support Diagnostics: Disabled

Smart Licenses

Filter Devices...

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

Um dem FTD-Gerät eine zeitlich begrenzte Lizenz zuzuweisen, wählen Sie **Lizenzen bearbeiten**. Wählen Sie dann ein verwaltetes Gerät aus, und fügen Sie es dem Abschnitt Geräte mit Lizenz hinzu. Wählen Sie anschließend die Schaltfläche **Apply (Anwenden)**, wie in diesem Bild dargestellt.

Edit Licenses

Malware

Threat

URL Filtering

AnyConnect Apex

AnyConnect Plus

AnyConnect VPN Only

Devices without license

Search

FTD

1

Add

2

Devices with license (1)

FTD

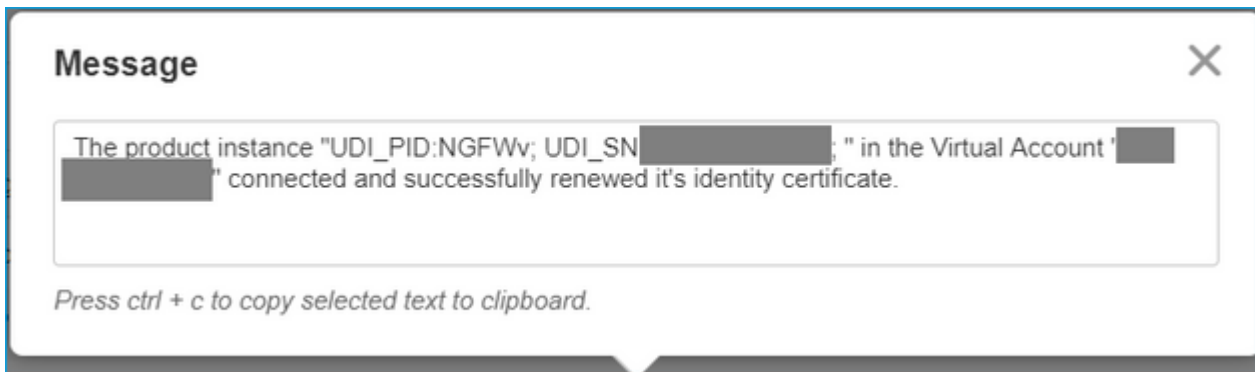
3

Cancel

Apply

Bestätigung auf Seite von Smart Software Manager (SSM)

Der Erfolg der FMC Smart License-Registrierung kann aus **Inventory > Event Log** in CSSM bestätigt werden, wie in diesem Bild gezeigt.

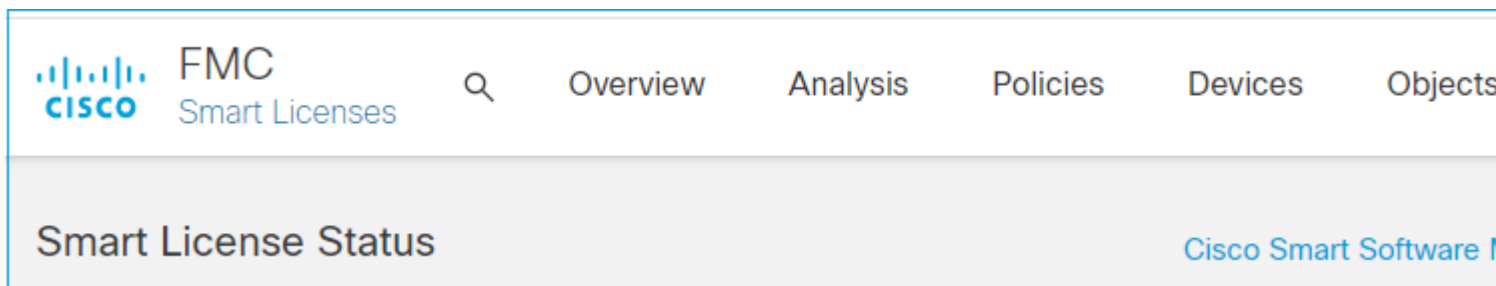


Der Registrierungsstatus des FMC kann unter **Inventar > Produktinstanzen** bestätigt werden. Überprüfen Sie das Ereignisprotokoll auf der Registerkarte **Ereignisprotokoll**. Die Smart License-Registrierung und der Nutzungsstatus können auf der Registerkarte **Inventory > Licenses (Inventar > Lizenzen)** überprüft werden. Vergewissern Sie sich, dass die erworbene laufzeitbasierte Lizenz korrekt verwendet wird, und es gibt keine Warnmeldungen, die auf unzureichende Lizenzen hinweisen.

Aufhebung der Registrierung von FMC Smart-Lizenzen

Registrierung des FMC vom Cisco SSM aufheben

Um die Lizenz aus irgendeinem Grund freizugeben oder ein anderes Token zu verwenden, navigieren Sie zu **System > Licenses > Smart Licenses**, und wählen Sie die Schaltfläche "De-Register" (Registrierung aufheben), wie in diesem Bild dargestellt.



Registrierung von SSM-Seite entfernen

Greifen Sie auf den Smart Software Manager ([Cisco Smart Software Manager](#)) zu, und wählen Sie unter **Inventar > Produktinstanzen** die Option **Entfernen** auf dem Ziel-FMC aus. Wählen Sie dann **Produktinstanz entfernen**, um das FMC zu entfernen und die zugewiesenen Lizenzen freizugeben, wie in diesem Bild dargestellt.

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
fmcvxyz1	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

Wenn das FMC ein RMA-FMC ist, heben Sie die Registrierung des FMC vom Cisco Smart Software Manager (CSSM) auf. Gehen Sie dazu wie im Abschnitt **FMC Smart License De-Registration > Remove Registration from SSM Side** beschrieben vor, und registrieren Sie das FMC dann erneut beim CSSM, wie im Abschnitt **FMC Smart License Registration** beschrieben.

Fehlerbehebung

Überprüfung der Zeitsynchronisierung

Greifen Sie auf die FMC-CLI (z. B. SSH) zu, und stellen Sie sicher, dass die Uhrzeit korrekt und mit einem vertrauenswürdigen NTP-Server synchronisiert ist. Da das Zertifikat für die Smart License-Authentifizierung verwendet wird, ist es wichtig, dass das FMC über die richtigen Zeitinformationen verfügt:

<#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

Überprüfen Sie in der FMC-Benutzeroberfläche die NTP-Serverwerte unter **System > Configuration > Time Synchronization (System > Konfiguration > Zeitsynchronisierung)**.

Namensauflösung aktivieren und Erreichbarkeit prüfen: tools.cisco.com

Stellen Sie sicher, dass das FMC einen FQDN auflösen kann und über folgende Adresse erreichbar ist: 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

Überprüfen Sie in der FMC-Benutzeroberfläche die IP-Adresse für die Verwaltung und die IP des DNS-Servers unter **System > Configuration > Management Interfaces (System > Konfiguration > Verwaltungsschnittstellen)**.

Überprüfen des HTTPS-Zugriffs (TCP 443) von FMC zu tools.cisco.com

Verwenden Sie den Telnet- oder Curl-Befehl, um sicherzustellen, dass das FMC HTTPS-Zugriff auf tools.cisco.com hat. Wenn die TCP 443-Kommunikation unterbrochen ist, stellen Sie sicher, dass sie nicht durch eine Firewall blockiert wird und sich kein SSL-Verschlüsselungsgerät im Pfad befindet.

<#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
```

Rolltest:

```
<#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-Überprüfung

Überprüfen Sie die erfolgreiche Auflösung in 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-Verifizierung

Wenn apProxy verwendet wird, überprüfen Sie die Werte sowohl auf dem FMC als auch auf dem Proxy-Server. Überprüfen Sie auf dem FMC, ob das FMC die richtige IP und den richtigen Port für den Proxyserver verwendet.

```

<#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 der FMC-UI können die Proxywerte unter **System > Configuration > Management Interfaces (System > Konfiguration > Verwaltungsschnittstellen)** bestätigt werden.

Wenn die FMC-seitigen Werte korrekt sind, überprüfen Sie die Proxy-Server-seitigen Werte (z. B. wenn der Proxy-Server den Zugriff vom FMC und auf tools.cisco.com zulässt). Datenverkehr und Zertifikataustausch über den Proxy zulassen. Das FMC verwendet ein Zertifikat für die Smart License (Registrierung).

Abgelaufene Token-ID

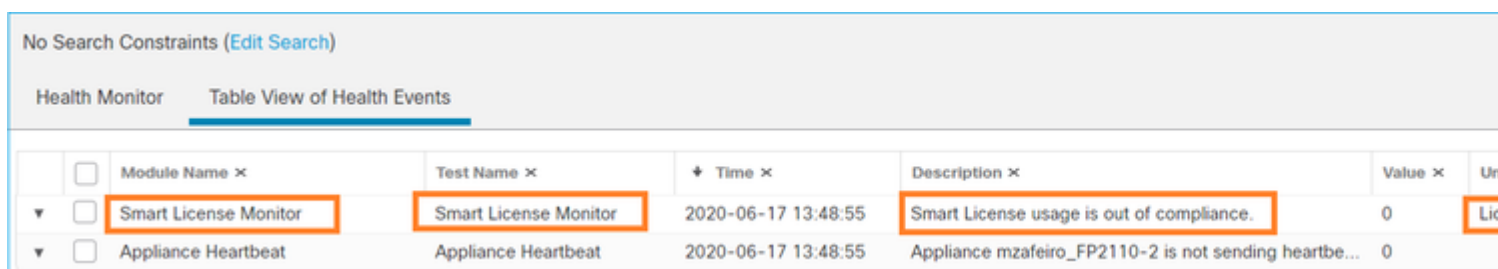
Vergewissern Sie sich, dass die ausgestellte Token-ID nicht abgelaufen ist. Wenn sie abgelaufen ist, bitten Sie den Smart Software Manager-Administrator, ein neues Token auszustellen und die Smart-Lizenz mit der neuen Token-ID erneut zu registrieren.

Ändern des FMC-Gateways

Es kann Fälle geben, in denen die Smart License-Authentifizierung aufgrund der Auswirkungen eines Relay-Proxys oder eines SSL-Verschlüsselungsgeräts nicht ordnungsgemäß durchgeführt werden kann. Ändern Sie nach Möglichkeit die Route für den FMC-Internetzugang, um diese Geräte zu vermeiden, und wiederholen Sie die Smart License-Registrierung.

Überprüfen Sie die Systemereignisse auf FMC.

Navigieren Sie auf dem FMC zu **System > Health > Events** (System > Zustand > Ereignisse), und überprüfen Sie den Status des Smart License Monitor-Moduls auf Fehler. Wenn die Verbindung beispielsweise aufgrund eines abgelaufenen Zertifikats fehlschlägt, wird ein Fehler generiert, z. B. "**id certificated** abgelaufen" (**abgelaufene ID**), wie in diesem Bild dargestellt.



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

Überprüfen Sie das Ereignisprotokoll auf SSM-Seite.

Wenn das FMC eine Verbindung zum CSSM herstellen kann, überprüfen Sie das Ereignisprotokoll der Verbindung unter **Inventory > Event Log (Bestand > Ereignisprotokoll)**. Überprüfen Sie, ob solche Ereignis- oder Fehlerprotokolle im CSSM vorhanden sind. Wenn es kein Problem mit den Werten/dem Betrieb des FMC-Standorts gibt und es kein Ereignisprotokoll auf der CSSM-Seite gibt, besteht die Möglichkeit, dass es ein Problem mit der Route zwischen dem FMC und dem CSSM gibt.

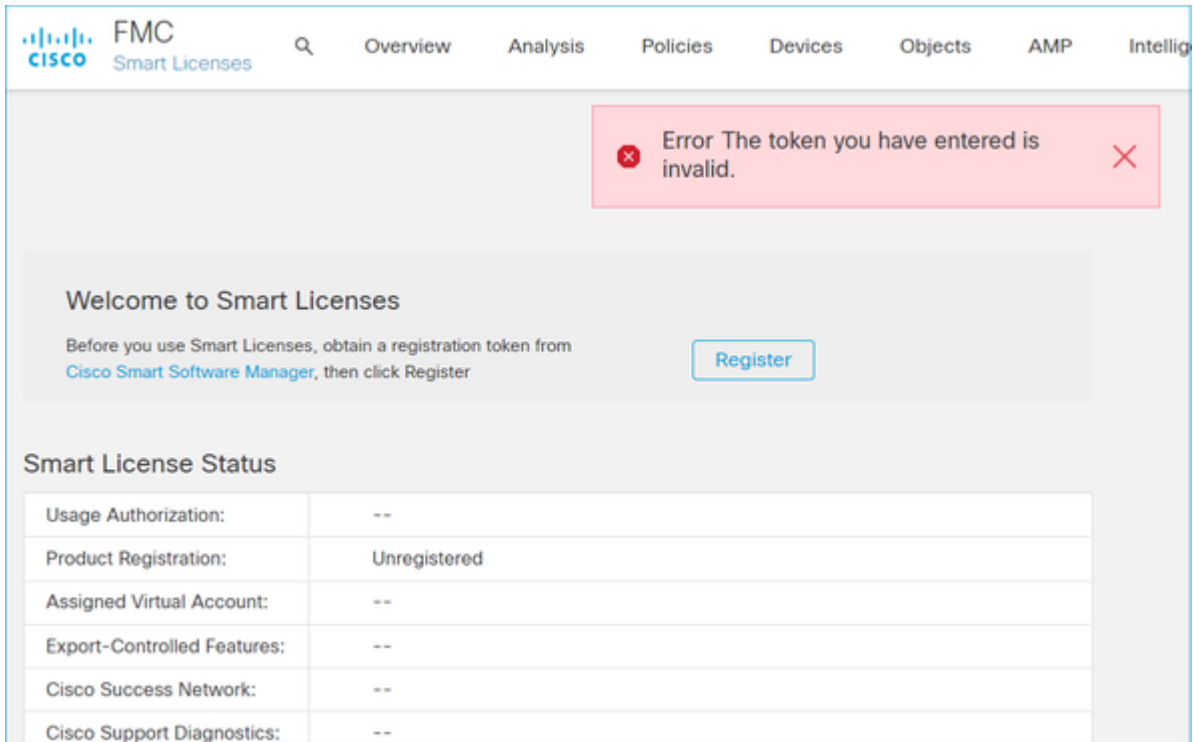
Häufige Probleme

Zusammenfassung der Registrierungs- und Autorisierungsstatus:

Status der Produktregistrierung	Autorisierungsstatus der Nutzung	Kommentare
UNREGISTERED (Nicht registriert)	â€”	Das FMC befindet sich weder im Registrierungs- noch im Evaluierungsmodus. Dies ist der ursprüngliche Status nach der FMC-Installation oder nach Ablauf der 90-tägigen Testlizenz.
Registriert	Autorisiert	Das FMC ist beim Cisco Smart Software Manager (CSSM) registriert, und es gibt FTD-Geräte, die mit einem gültigen Abonnement registriert sind.
Registriert	Autorisierung abgelaufen	Das FMC kommunizierte mehr als 90 Tage lang nicht mit dem Cisco Lizenz-Backend.
Registriert	UNREGISTERED (Nicht registriert)	Das FMC ist beim Cisco Smart Software Manager (CSSM) registriert, es sind jedoch keine FTD-Geräte am FMC registriert.
Registriert	Out-of-Compliance	<p>Das FMC ist beim Cisco Smart Software Manager (CSSM) registriert, aber es gibt FTD-Geräte, die mit ungültigen Abonnements registriert sind.</p> <p>Ein FTD-Gerät (FP4112) verwendet beispielsweise ein THREAT-Abonnement, aber mit dem Cisco Smart Software Manager (CSSM) sind für FP4112 keine THREAT-Abonnements verfügbar.</p>
Evaluierung (90 Tage)	â€”	Der Evaluierungszeitraum wird genutzt, es sind jedoch keine FTD-Geräte am FMC registriert.

Anwenderbericht 1. Ungültiges Token

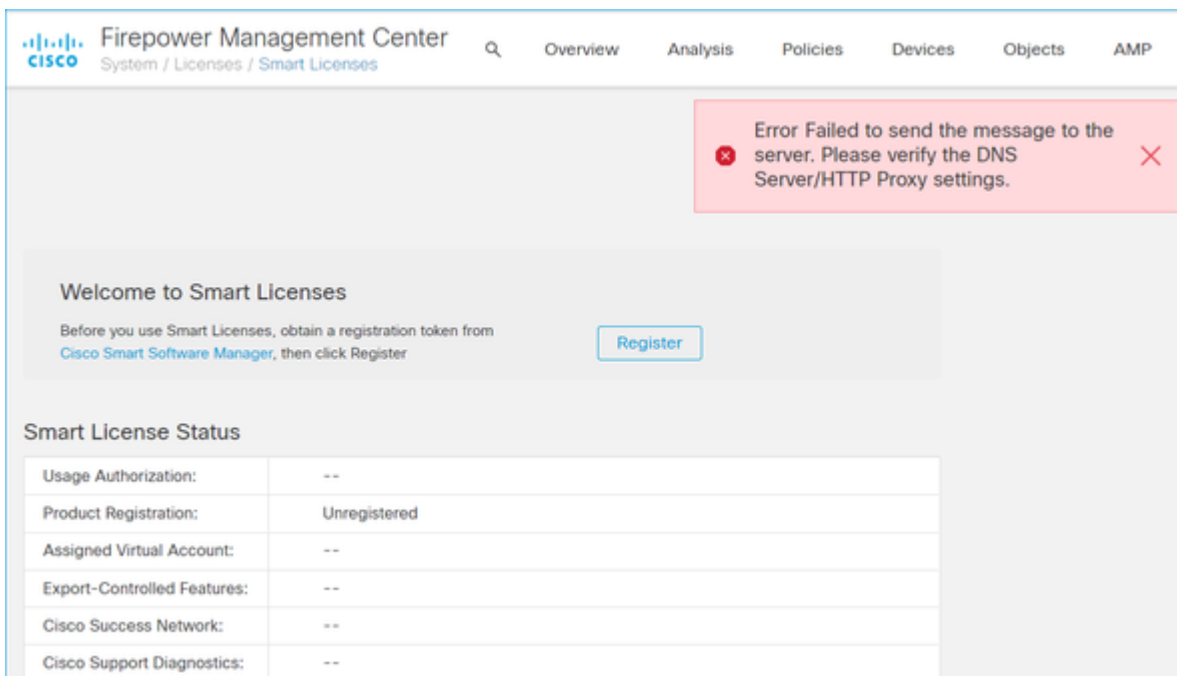
Symptom: Die Registrierung beim CSSM schlägt schnell fehl (~10 s), da das Token ungültig ist, wie in diesem Bild gezeigt.



Auflösung: Verwenden Sie ein gültiges Token.

Anwenderbericht 2. Ungültiger DNS

Symptom: Die Registrierung beim CSSM ist nach einer Weile (~25 s) fehlgeschlagen, wie in diesem Bild gezeigt.



Überprüfen Sie die Datei /var/log/process_stdout.log. Das DNS-Problem tritt auf:

```
<#root>
```

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

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

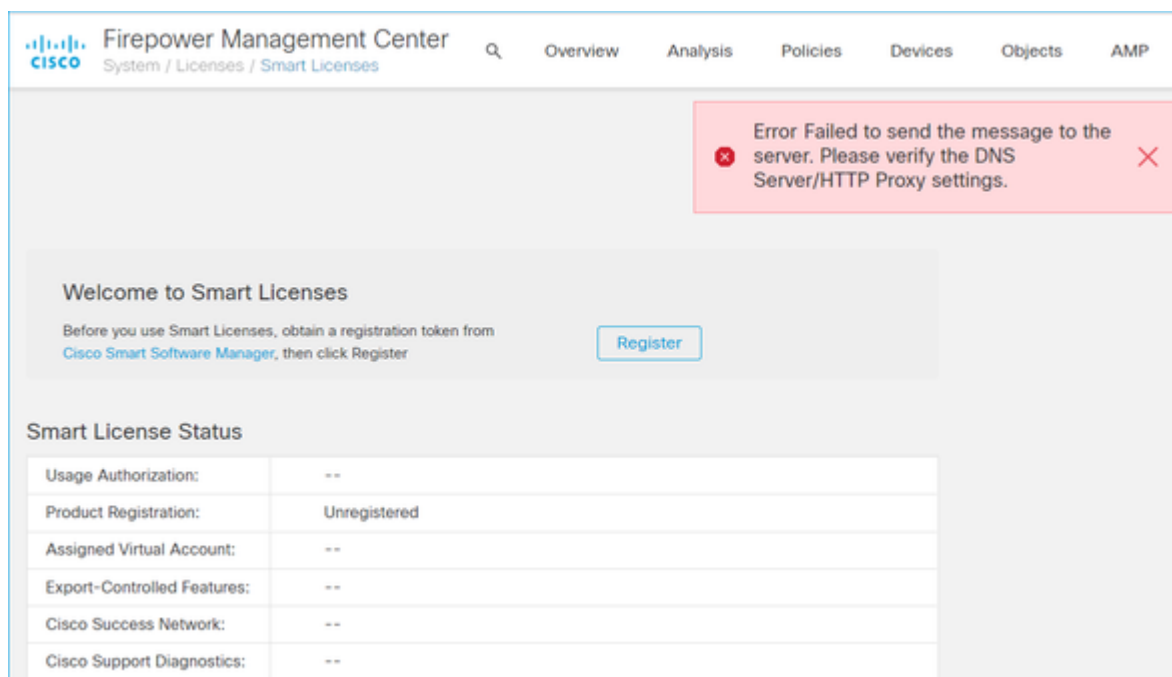
```
2020-06-25 09:05:21 sla[24043]: *Thu Jun 25 09:05:10.989 UTC: CH-LIB-ERROR: ch_pf_curl_send_msg[494], failed to perform, err code 6, err string
```

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

Auflösung: Fehler bei der Auflösung des CSSM-Hostnamens. Die Lösung besteht darin, DNS zu konfigurieren (falls nicht konfiguriert) oder die DNS-Probleme zu beheben.

Anwenderbericht 3. Ungültige Zeitwerte

Symptom: Die Registrierung beim CSSM ist nach einer Weile (~25 s) fehlgeschlagen, wie in diesem Bild gezeigt.



Überprüfen Sie die **Datei /var/log/process_stdout.log**. Es treten folgende Zertifikatsprobleme auf:

```
<#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/oddce/services/DDCEService
```

Überprüfen Sie den FMC-Zeitwert:

<#root>

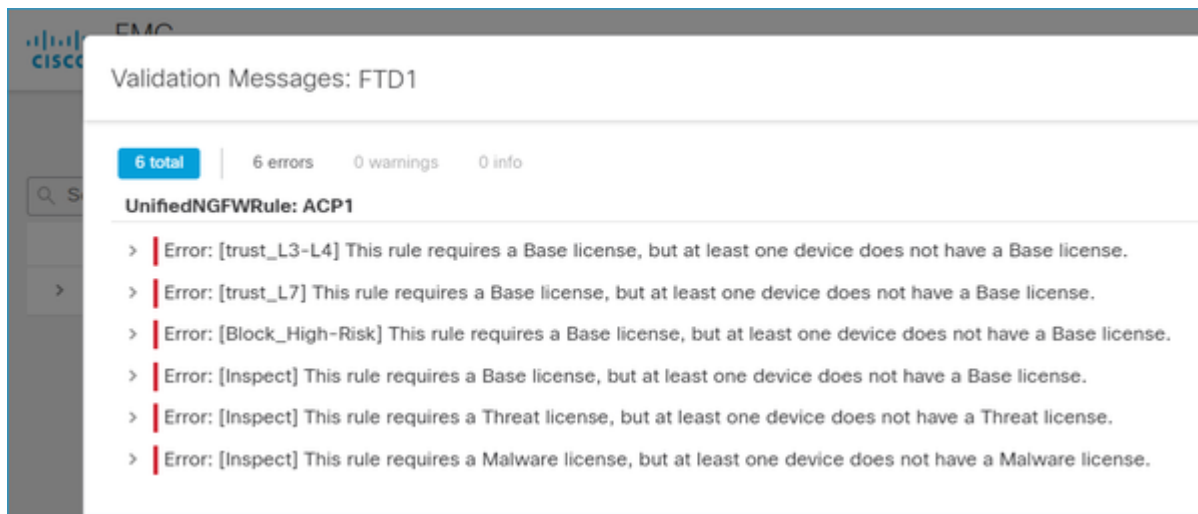
root@FMC2000-2:/Volume/home/admin#

date

Fri Jun 25 09:27:22 UTC 2021

Fallstudie 4. Kein Abonnement

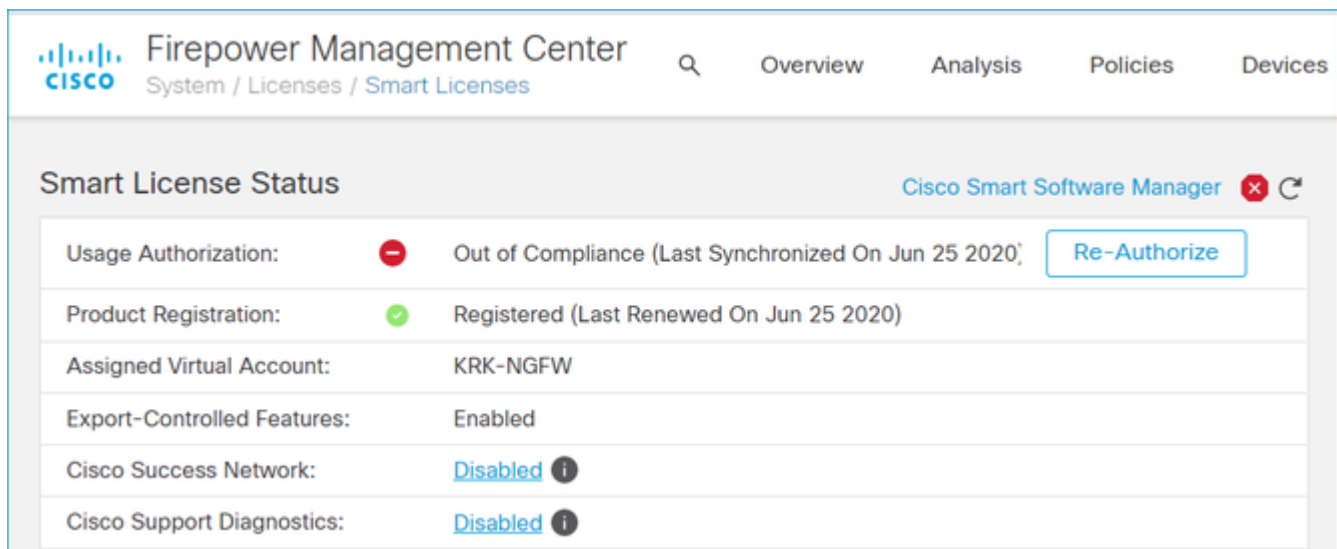
Wenn für eine bestimmte Funktion kein Lizenzabonnement vorhanden ist, ist die FMC-Bereitstellung nicht möglich:



Lösung: Es ist erforderlich, das erforderliche Abonnement zu erwerben und auf das Gerät anzuwenden.

Anwenderbericht 5. Out-of-Compliance (OOC)

Wenn keine Berechtigung für FTD-Abonnements besteht, wird die FMC Smart License in den Status "Out-of-compliance" (OOC) versetzt:



Überprüfen Sie im CSSM die Warnmeldungen auf Fehler:

General Licenses Product Instances Event Log							
Available Actions		Manage License Tags		License Reservation...		Search by License	
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	

Fallstudie 6. Keine starke Verschlüsselung

Wenn nur die Basislizenz verwendet wird, ist die DES-Verschlüsselung (Data Encryption Standard) in der FTD LINA-Engine aktiviert. In diesem Fall schlagen Bereitstellungen wie L2L Virtual Private Network (VPN) mit stärkeren Algorithmen fehl:

Validation Messages

Device

FTD1

2 total 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

Cisco Firepower Management Center
System / Licenses / Smart Licenses
Overview Analysis Policies Devices

Smart License Status
Cisco Smart Software Manager

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
Cisco Success Network:	Enabled
Cisco Support Diagnostics:	Disabled

Auflösung: Registrieren Sie das FMC beim CSSM, und aktivieren Sie das Strong Encryption-Attribut.

Zusätzliche Hinweise

Benachrichtigung über Smart-Lizenzstatus festlegen

E-Mail-Benachrichtigung von SSM

SSM-seitig ermöglicht SSM E-Mail-Benachrichtigung den Empfang von zusammenfassenden E-Mails für verschiedene Ereignisse. Beispielsweise Benachrichtigung bei Lizenzmangel oder bei Lizenzen, die bald ablaufen. Es können Benachrichtigungen über eine Produktinstanzverbindung oder einen Fehler bei der Aktualisierung empfangen werden.

Diese Funktion ist sehr nützlich, um Funktionseinschränkungen aufgrund des Lizenzablaufs zu erkennen und zu verhindern.

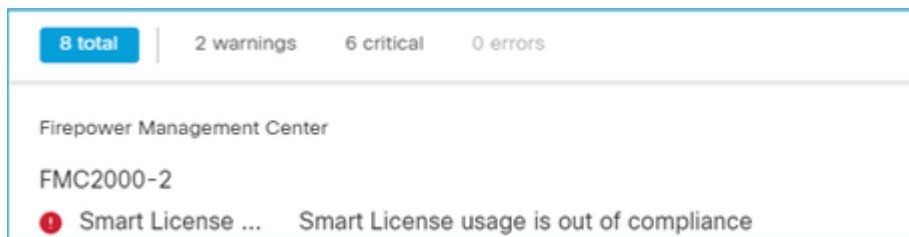
Statusbenachrichtigungen vom FMC abrufen

Auf der FMC-Seite ist es möglich, eine Warnmeldung des Zustandsmonitors zu konfigurieren und eine Warnmeldung zu einem Zustandsereignis zu erhalten. Der Modul Smart License Monitor ist verfügbar, um den Smart License-Status zu überprüfen. Die Monitorwarnung unterstützt Syslog-, E-Mail- und SNMP-Traps.

Dies ist ein Konfigurationsbeispiel zum Abrufen einer Syslog-Meldung, wenn ein Smart License-Überwachungsereignis auftritt:

The screenshot displays the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes the Cisco logo, the title 'Firepower Management Center', and a breadcrumb trail 'System / Health / Monitor Alerts'. Navigation tabs for 'Overview', 'Analysis', 'Policies', 'Devices', and 'Other' are visible. The main content area is titled 'Active Health Alerts' and contains a 'Configure Health Alerts' section. In this section, the 'Health Alert Name' is set to 'Smart-License-Syslog-Alert'. The 'Severity' is configured as 'Critical' from a list that also includes 'Warning', 'Normal', 'Error', and 'Recovered'. The 'Module' dropdown menu is open, showing a list of modules: 'Realm', 'Reconfiguring Detection', 'Security Intelligence', 'Smart License Monitor' (which is highlighted), 'Snort Identity Memory Usage', 'Threat Data Updates on Device...', 'Time Series Data Monitor', 'Time Synchronization Status', 'URL Filtering Monitor', 'User Agent Status Monitor', and 'VPN Status'.

Dies ist ein Beispiel für eine Statusmeldung:



Die vom FMC generierte Syslog-Meldung lautet:

<#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

Weitere Informationen zu den Systemmonitor-Warnmeldungen finden Sie unter [Systemüberwachung](#).

Mehrere FMCs auf demselben Smart Account

Wenn mehrere FMCs für dasselbe Smart Account verwendet werden, muss jeder FMC-Hostname eindeutig sein. Wenn mehrere FMCs in CSSM verwaltet werden, muss der Hostname jedes FMC eindeutig sein, um jedes FMC zu unterscheiden. Dies ist nützlich für die Wartung der FMC Smart License, die in Betrieb ist.

FMC muss Internetverbindung aufrechterhalten

Nach der Registrierung überprüft das FMC die Smart License Cloud und den Lizenzstatus alle 30 Tage. Wenn das FMC 90 Tage lang nicht kommunizieren kann, wird die lizenzierte Funktion beibehalten. Sie behält jedoch den Status **Autorisierung abgelaufen bei**. Selbst in diesem Zustand versucht das FMC kontinuierlich, eine Verbindung zur Smart License Cloud herzustellen.

Bereitstellung mehrerer FMCv

Wenn das FirePOWER-System in einer virtuellen Umgebung verwendet wird, wird Clone (warm oder kalt) nicht offiziell unterstützt. Jedes virtuelle FirePOWER Management Center (FMCv) ist einzigartig, da es Authentifizierungsinformationen enthält. Um mehrere FMCv bereitzustellen, muss die FMCv aus der OVF-Datei (Open Virtualization Format) erstellt werden. Weitere Informationen zu dieser Einschränkung finden Sie im [Cisco FirePOWER Management Center Virtual for VMware Deployment Quick Start Guide](#).

Häufig gestellte Fragen (FAQ)

Wie viele Gerätelizenzen sind in FTD HA erforderlich?

Wenn zwei FTDs für Hochverfügbarkeit verwendet werden, ist für jedes Gerät eine Lizenz erforderlich. Wenn das Intrusive Protection System (IPS) und die Advanced Malware Protection (AMP)-Funktion für das FTD HA-Paar verwendet werden, sind beispielsweise zwei Lizenzen für Bedrohungen und Malware erforderlich.

Warum werden von FTD keine AnyConnect-Lizenzen verwendet?

Stellen Sie nach der FMC-Registrierung beim Smart Account sicher, dass die AnyConnect-Lizenz aktiviert ist. Um die Lizenz zu aktivieren, navigieren Sie zu **FMC > Geräte**, wählen Sie Ihr Gerät und dann **Lizenz**. Wählen Sie das **Bleistiftsymbol** aus, wählen Sie die Lizenz aus, die im Smart Account hinterlegt ist, und wählen Sie **Speichern**.

Warum wird nur eine AnyConnect-Lizenz im Smart Account "In Gebrauch" verwendet, wenn 100 Benutzer verbunden sind?

Dies ist ein erwartetes Verhalten, da Smart Account die Anzahl der Geräte verfolgt, auf denen diese Lizenz aktiviert ist, ohne dass aktive Benutzer verbunden sind.

Warum liegt der Fehler vor? Device does not have the AnyConnect License **nach der Konfiguration und Bereitstellung eines Remote Access VPN durch das FMC?**

Stellen Sie sicher, dass das FMC bei der Smart License Cloud registriert ist. Das erwartete Verhalten ist, dass die Konfiguration des Remote-Zugriffs nicht bereitgestellt werden kann, wenn das FMC nicht registriert ist oder sich im Testmodus befindet. Wenn das FMC registriert ist, stellen Sie sicher, dass die AnyConnect-Lizenz in Ihrem Smart Account vorhanden und dem Gerät zugewiesen ist.

Um eine Lizenz zuzuweisen, navigieren zu **FMC Geräte**, wählen Sie Ihr Gerät, **Lizenz** (Bleistiftsymbol). Wählen Sie die Lizenz im Smart Account aus, und wählen Sie **Speichern**.

Warum liegt der Fehler vor? Remote Access VPN with SSL cannot be deployed when Export-Controlled Features (Strong-crypto) are disabled **Wann findet eine Bereitstellung einer Remote Access-VPN-Konfiguration statt?**

Für das auf dem FTD bereitgestellte Remote Access-VPN muss eine Strong Encryption-Lizenz aktiviert sein. DEStellen Sie sicher, dass auf dem FMC eine Strong Encryption-Lizenz aktiviert ist. Um den Status der Strong Encryption-Lizenz zu überprüfen, navigieren an die **FMC-System > Lizenzen > Smart Licensing**, und prüfen Sie, ob die exportgesteuerten Features aktiviert sind.

So aktivieren Sie eine Strong Encryption-Lizenz, wenn Export-Controlled Features ist deaktiviert?

Diese Funktion wird automatisch aktiviert, wenn für das Token, das bei der Registrierung des FMC in der Smart Account Cloud verwendet wird, die Option **Ausfuhrkontrollierte Funktionen für die mit diesem Token registrierten Produkte zulassen** aktiviert ist. Wenn diese Option für das Token nicht aktiviert ist, heben Sie die Registrierung des FMC auf, und registrieren Sie es erneut, wenn diese Option aktiviert ist.

Was kann getan werden, wenn die Option "Exportgesteuerte Funktionalität für die mit diesem Token registrierten Produkte zulassen" beim Generieren des Tokens nicht verfügbar ist?

Wenden Sie sich an Ihr Cisco Account Team.

Warum wird die Fehlermeldung "Strong crypto (d. h., der Verschlüsselungsalgorithmus ist größer als DES) für die VPN-Topologie s2s wird nicht unterstützt" empfangen?

Dieser Fehler wird angezeigt, wenn das FMC den Evaluierungsmodus verwendet oder das Smart License-Konto nicht über eine Strong Encryption-Lizenz verfügt. VÜberprüfen Sie, ob das FMC bei der Lizenzbehörde registriert ist, und **lassen Sie die exportgesteuerte Funktion für die mit diesem Token registrierten Produkte** zu. Wenn der Smart Account keine Strong Encryption-Lizenz verwenden darf, ist die Bereitstellung einer Site-to-Site-VPN-Konfiguration mit Chiffren, die sicherer als DES sind, nicht zulässig.

Warum wird der Status "Nicht konform" im FMC empfangen?

Das Gerät kann die Compliance verlieren, wenn eines der verwalteten Geräte nicht verfügbare Lizenzen verwendet.

Wie kann der Status "Nicht konform" korrigiert werden?

Befolgen Sie die Schritte im FirePOWER Konfigurationsleitfaden:

1. Im Abschnitt "Smart Licenses" am unteren Seitenrand können Sie sehen, welche Lizenzen benötigt werden.
2. Erwerben Sie die erforderlichen Lizenzen über Ihre üblichen Kanäle.
3. Im Cisco Smart Software Manager (<https://software.cisco.com/#SmartLicensing-Inventory>), überprüfen Sie, ob die Lizenzen in Ihrem Virtual Account angezeigt werden.
4. Wählen Sie im FMC System > Licenses > Smart Licenses aus.
5. Wählen Sie **Erneut autorisieren**.

Das vollständige Verfahren finden Sie unter [Lizenzierung des FirePOWER-Systems](#).

Was sind die Funktionen der Firepower Threat Defense Base?

Die Base-Lizenz ermöglicht:

- Konfiguration von FTD-Geräten für das Switching und Routing (einschließlich DHCP Relay und NAT).
- Konfiguration von FTD-Geräten in einem Hochverfügbarkeitsmodus (HA).
- Konfiguration von Sicherheitsmodulen als Cluster innerhalb eines Firepower 9300-Chassis (Intra-Chassis-Cluster).
- Konfiguration von Firepower 9300- oder Firepower 4100-Geräten (FTD) als Cluster (Interchassis-Cluster).
- Konfiguration der Benutzer- und Anwendungskontrolle und Hinzufügen von Benutzer- und Anwendungsbedingungen zu Zugriffskontrollregeln.

Wie kann die Firepower Threat Defense Base Feature-Lizenz bezogen werden?

Beim Kauf eines virtuellen Firepower Threat Defense- oder Firepower Threat Defense-Geräts wird automatisch eine Base-Lizenz erworben. Sie wird automatisch Ihrem Smart Account hinzugefügt, wenn FTD sich beim FMC registriert.

Welche IP-Adressen müssen im Pfad zwischen dem FMC und der Smart License Cloud zulässig sein?

Das FMC verwendet die IP-Adresse Port 443 zur Kommunikation mit der Smart License Cloud.

Diese IP-Adresse (<https://tools.cisco.com>) in folgende IP-Adressen aufgelöst:

- 72.163.4.38
- 173.37.145.8

Zugehörige Informationen

- [Konfigurationsleitfäden für FirePOWER Management Center](#)
- [Cisco Live Smart Licensing - Überblick: BRKARC-2034](#)
- [Funktionslizenzen für Cisco Secure Firewall Management Center](#)
- [Häufig gestellte Fragen \(FAQs\) zur Cisco Smart Software-Lizenzierung](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.