Verwenden Sie die FMC- und FTD Smart License Registration sowie häufige Probleme zur Fehlerbehebung.

Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
Registrierung der FMC Smart-Lizenz
Voraussetzungen
Registrierung der FMC Smart-Lizenz
Bestätigung auf der Seite von Smart Software Manager (SSM)
FMC Smart-Lizenzderegistrierung
Fehlerbehebung
Häufige Probleme
Anwenderbericht 1. Ungültiges Token
Anwenderbericht 2. Ungültiger DNS
Anwenderbericht 3. Ungültige Zeitwerte
Anwenderbericht 4. Kein Abonnement
Anwenderbericht 5. Out-of-Compliance (OOC)
Anwenderbericht 6. Keine zuverlässige Verschlüsselung
Zusätzliche Hinweise
Smart License State-Benachrichtigung festlegen
Abrufen von Gesundheitsbenachrichtigungen vom FMC
Mehrere FMCs auf demselben Smart Account
FMC muss Internetverbindungen aufrechterhalten
Bereitstellung mehrerer FMCv
Häufig gestellte Fragen (FAQs)
Zugehörige Informationen

Einleitung

Dieses Dokument beschreibt die Konfiguration der Smart-Lizenzregistrierung des FirePOWER Management Center auf Firepower Threat Defense-verwalteten Geräten.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

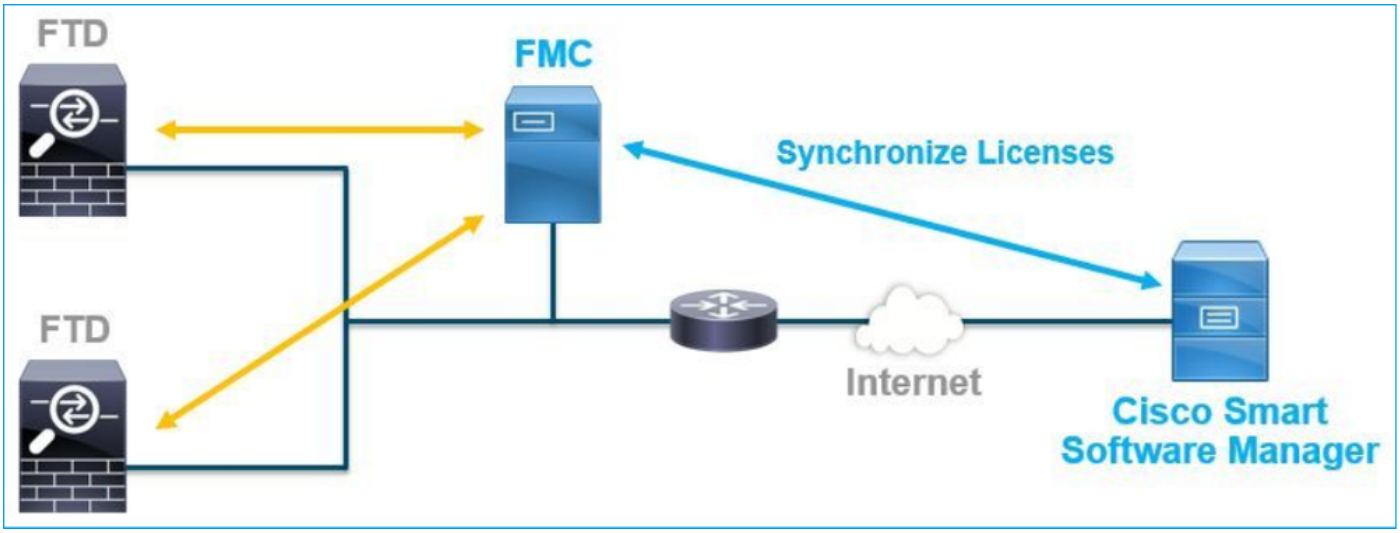
Verwendete Komponenten

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 verstehen.

Hintergrundinformationen

FMC-, FTD- und Smart License-Registrierung.

Die Smart-Lizenzregistrierung wird im FirePOWER Management Center (FMC) durchgeführt. Das FMC kommuniziert über das Internet mit dem Cisco Smart Software Manager-Portal (CSSM). Im CSSM verwaltet der Firewall-Administrator das Smart Account und dessen Lizenzen. Das FMC kann den verwalteten FirePOWER Threat Defense-Geräten (FTD) Lizenzen kostenlos zuweisen und löschen. Das heißt, der FMC verwaltet Lizenzen für FTD-Geräte zentral.



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

Die Basislizenz ist im FTD-Gerät enthalten. Diese Lizenz wird automatisch in Ihrem Smart Account registriert, wenn das FMC bei CSSM registriert ist.
Laufzeitbasierte Lizenzen: Bedrohungen, Malware und URL-Filterung sind optional. Um Funktionen im Zusammenhang mit einer Lizenz zu verwenden, muss dem FTD-Gerät eine Lizenz zugewiesen werden.

Zur Verwendung eines FirePOWER Management Center Virtual (FMCv) für die FTD-Verwaltung wird auch eine **FirePOWER MCv-Gerätelizenz** in CSSM für das FMCv benötigt.

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

Darüber hinaus enthält dieses Dokument Szenarien, die bei der Fehlerbehebung für häufige Fehler bei der Lizenzregistrierung helfen.

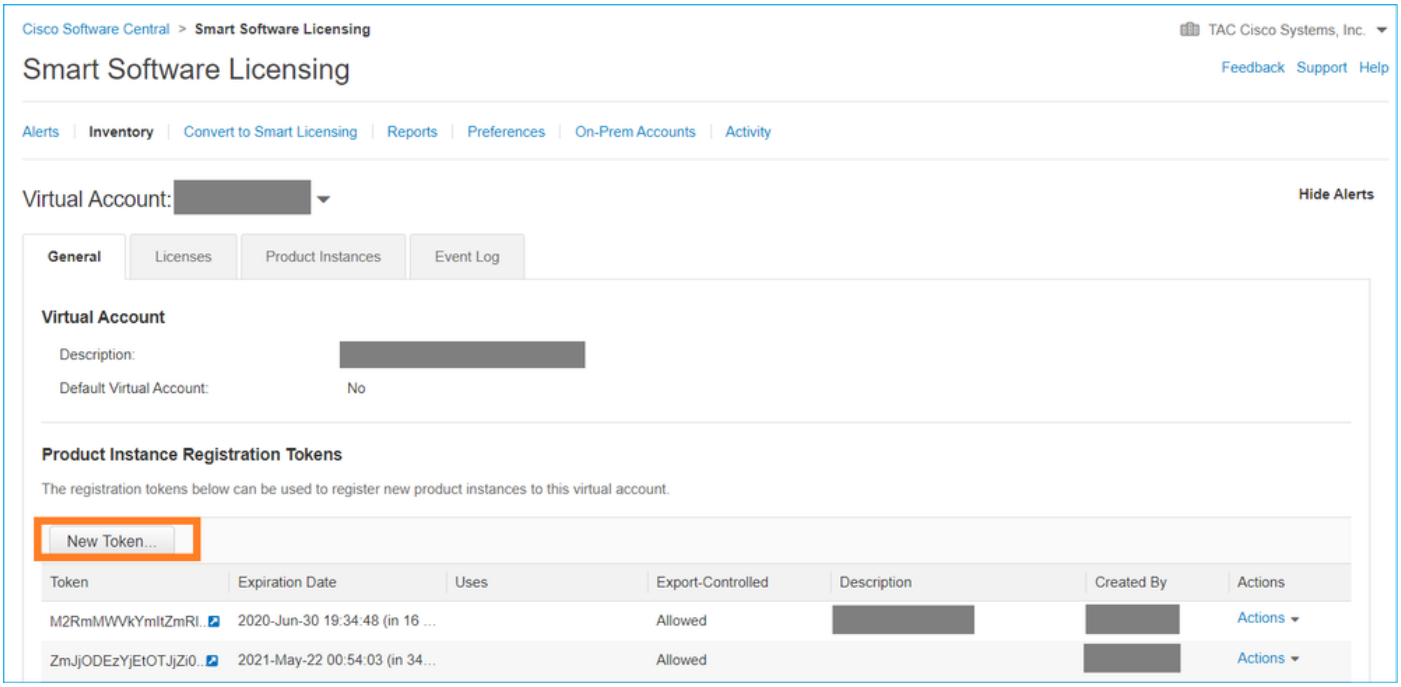
Weitere Einzelheiten zu Lizenzen finden Sie in den Cisco FirePOWER System Feature Licenses und Frequently Asked Questions (FAQs) über FirePOWER Licensing (FAQ) (Cisco FirePOWER-Systemfunktionslizenzen und Häufig gestellte Fragen (FAQs)).

Registrierung der FMC Smart-Lizenz

Voraussetzungen

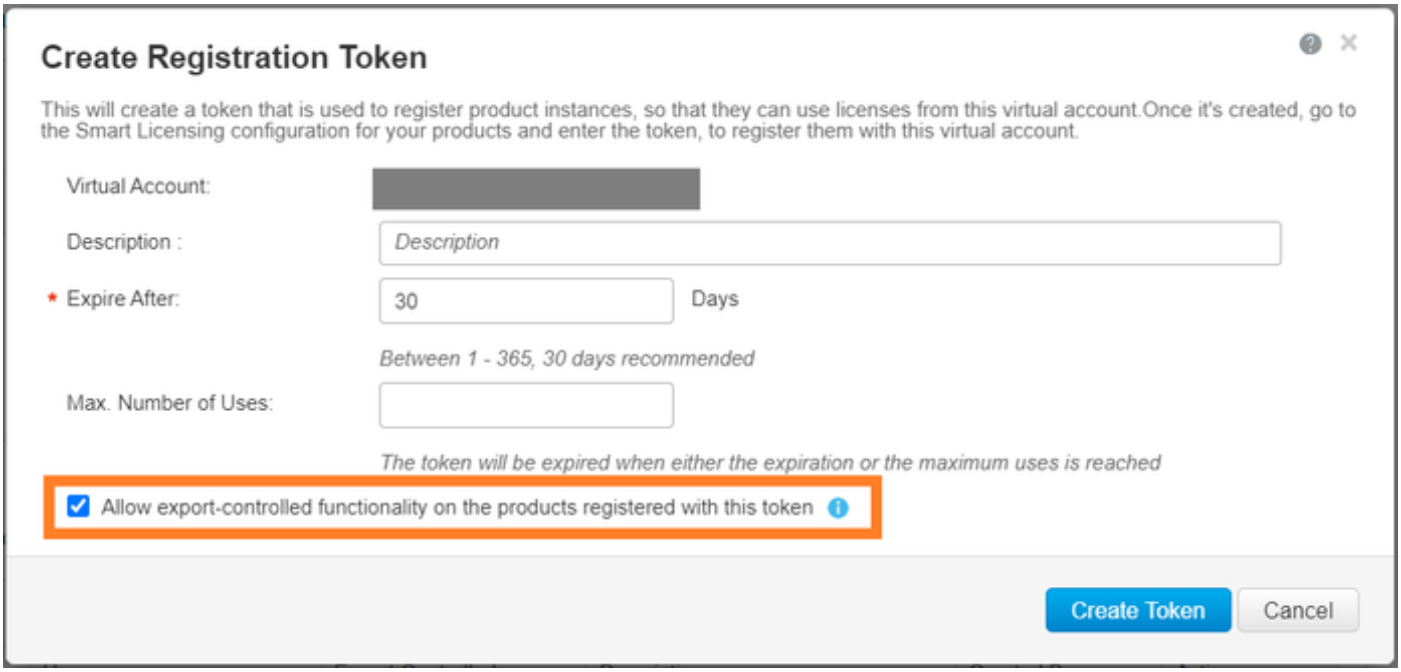
1. Für die Smart License-Registrierung muss das FMC auf das Internet zugreifen. Da das Zertifikat zwischen dem FMC und der Smart License Cloud mit HTTPS ausgetauscht wird, stellen Sie sicher, dass sich im Pfad kein Gerät befindet, das die Kommunikation beeinflussen/ändern kann. (z. B. Firewall, Proxy, SSL-Entschlüsselungsgerät usw.).

2. Rufen Sie das CSSM auf, und geben Sie eine Token-ID von **Inventory > General > New Token** (**Bestand > Allgemein > Neue Token**) aus, wie in diesem Bild gezeigt.



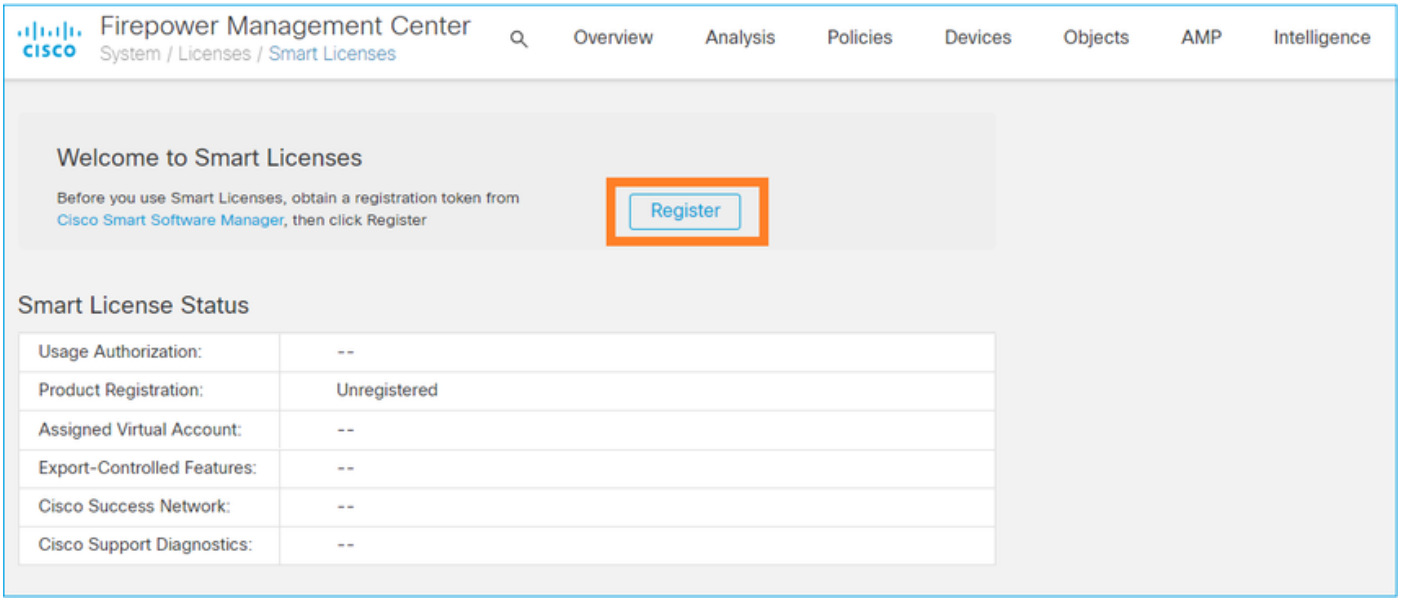
Um eine starke Verschlüsselung zu verwenden, aktivieren Sie die **Funktion Exportkontrolle zulassen für die mit dieser Tokenoption registrierten Produkte**. Wenn diese Option aktiviert ist, wird ein Häkchen im Kontrollkästchen angezeigt.

3. Wählen Sie **Token erstellen aus**.

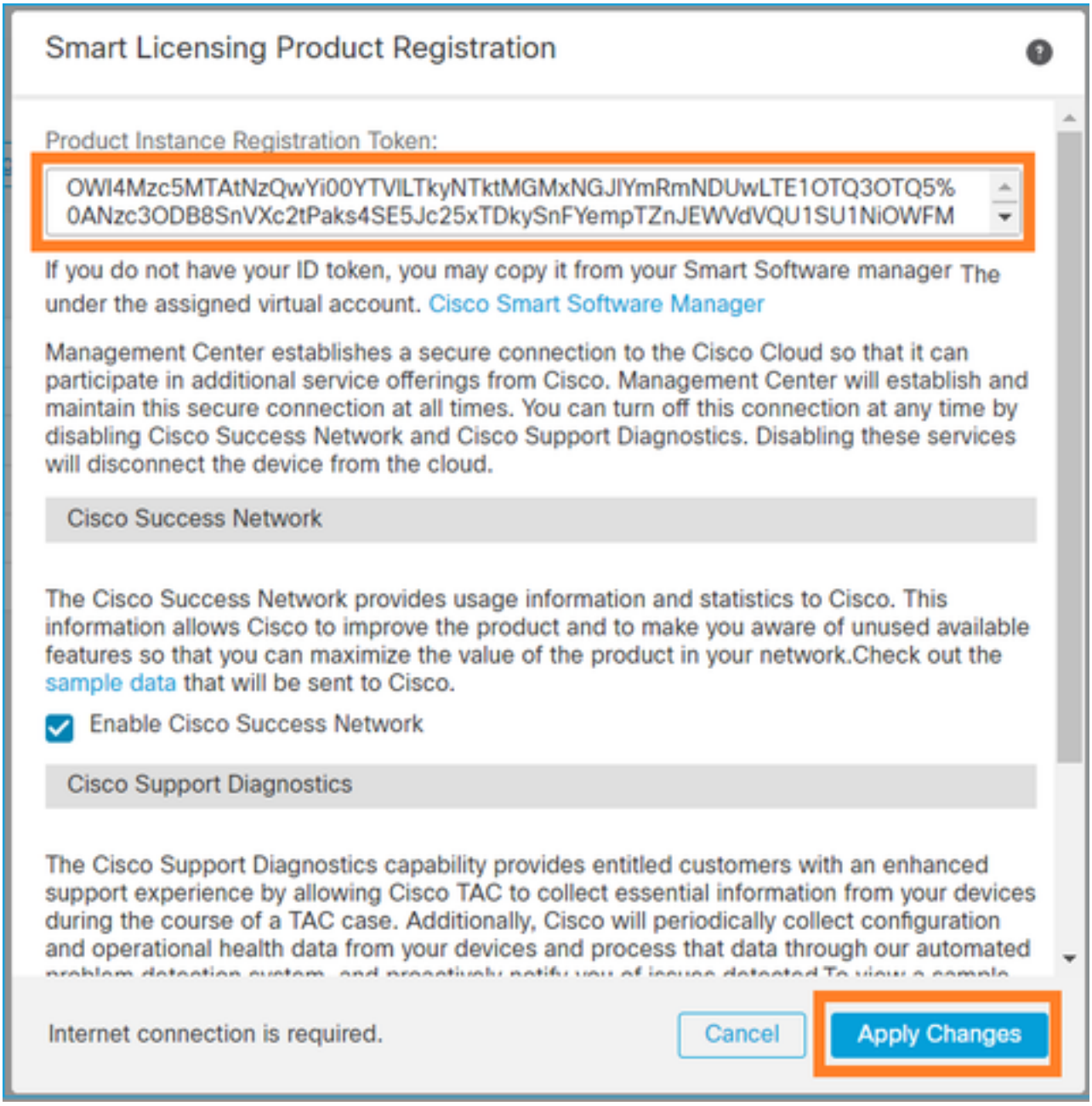


Registrierung der FMC Smart-Lizenz

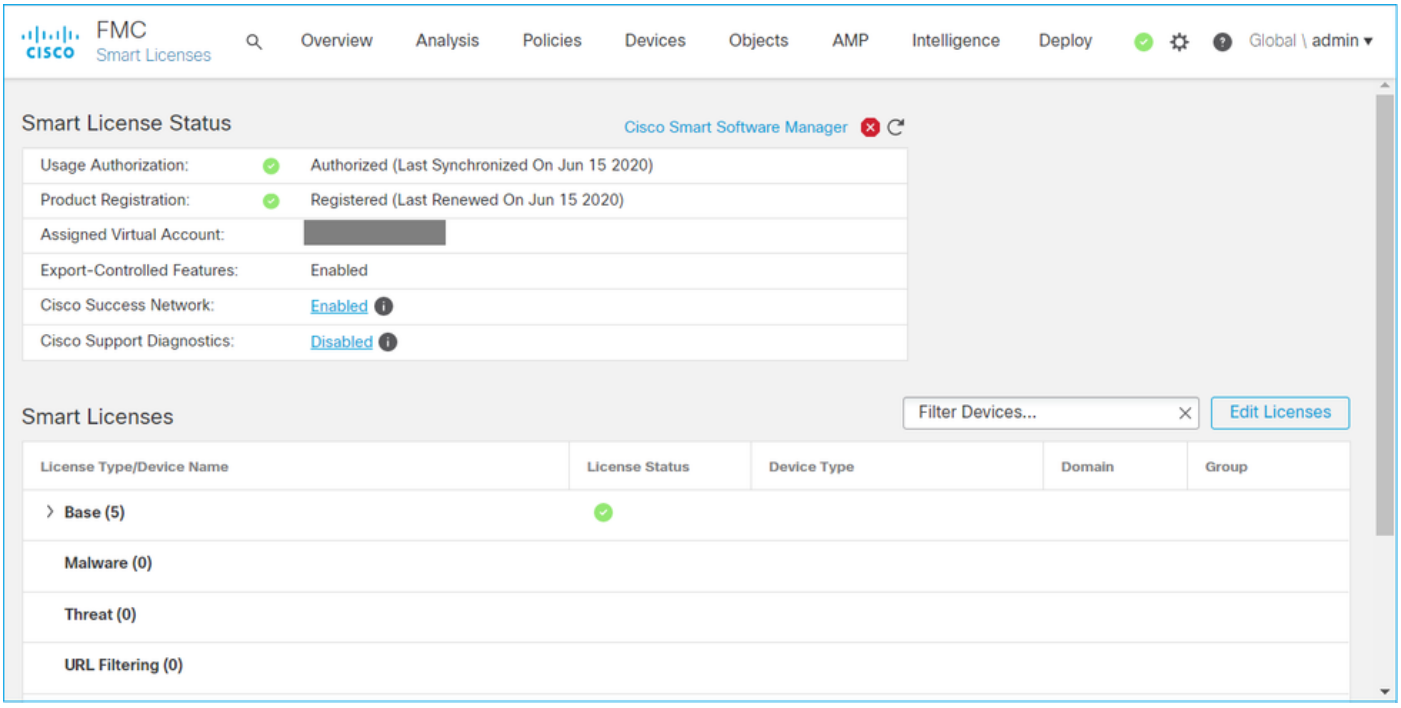
Navigieren Sie zu **System > Licenses (System > Lizenzen > Smart Licenses)** im FMC, und wählen Sie die Schaltfläche **Registrieren** aus, wie in diesem Bild gezeigt.



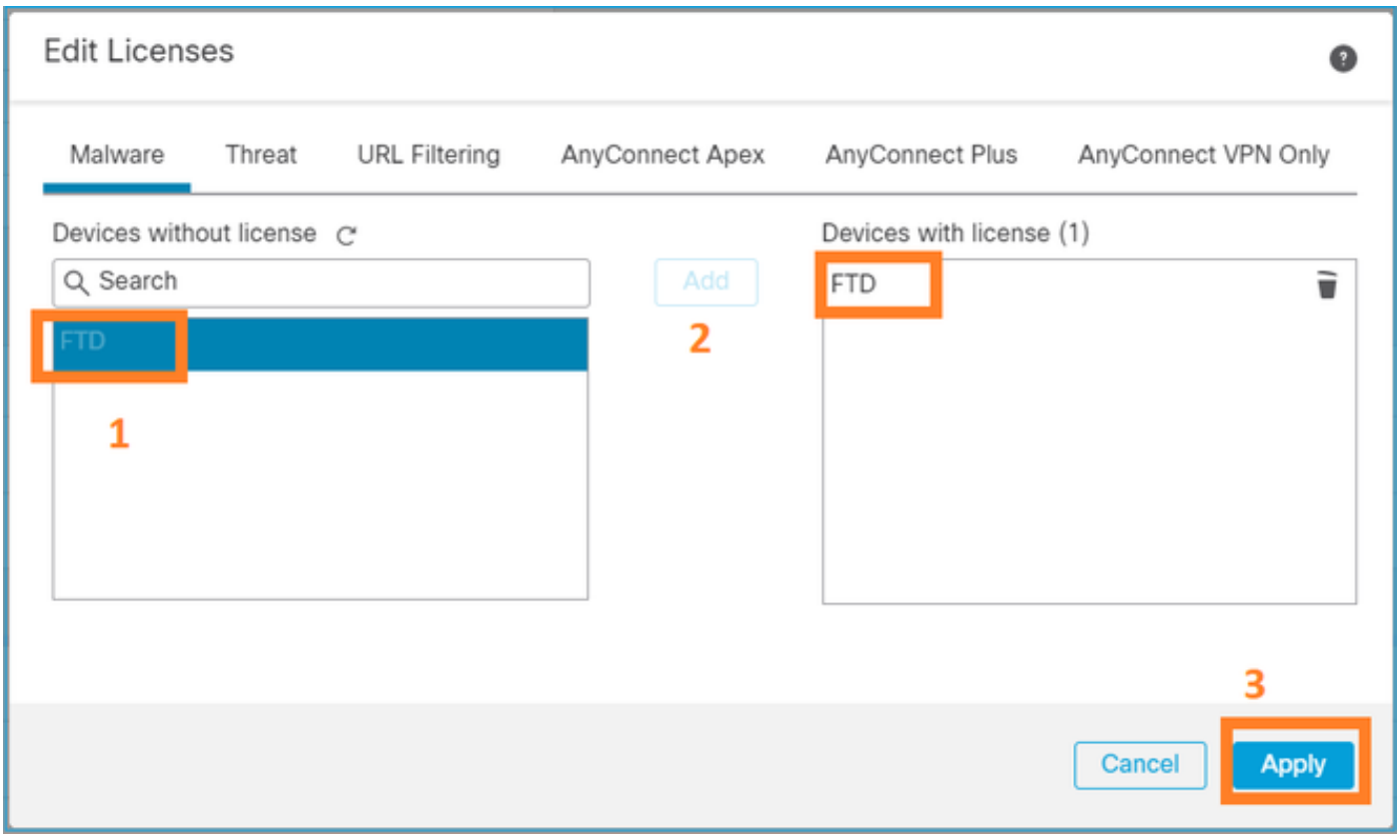
Geben Sie die Token-ID im Fenster Smart Licensing Product Registration (Produktregistrierung für Smart Licensing) ein, und wählen Sie **Apply Changes (Änderungen anwenden)** aus, wie in diesem Bild gezeigt.



Wenn die Smart License-Registrierung erfolgreich war, wird als Produktregistrierungsstatus **Registriert** angezeigt, wie in diesem Bild gezeigt.

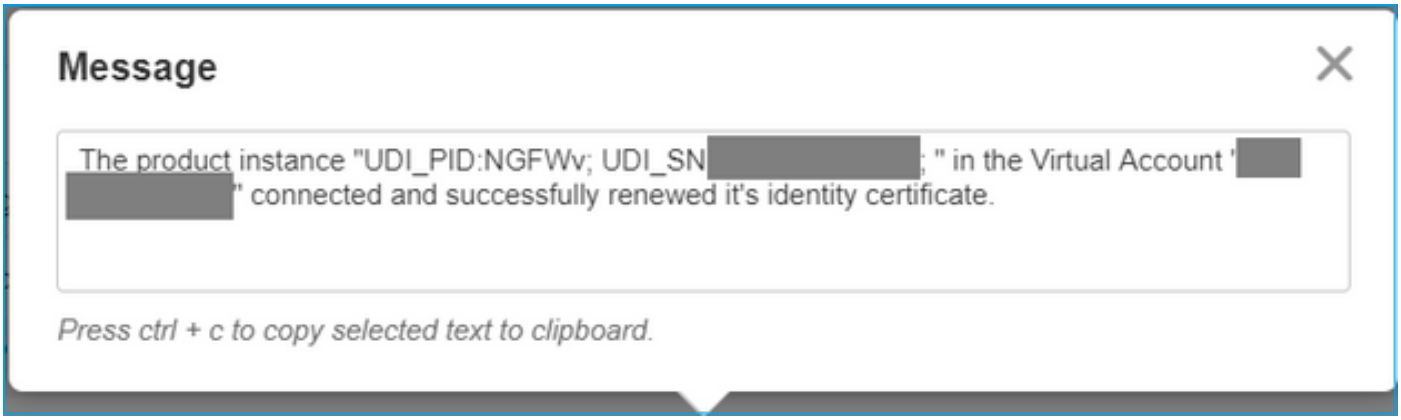


Um dem FTD-Gerät eine zeitlich begrenzte Lizenz zuzuweisen, wählen Sie **Edit Licenses (Lizenzen bearbeiten)** aus. Wählen Sie anschließend ein verwaltetes Gerät aus, und fügen Sie es dem Abschnitt Geräte mit Lizenz hinzu. Wählen Sie zum Schluss die Schaltfläche **Übernehmen**, wie in diesem Bild gezeigt.



Bestätigung auf der Seite von Smart Software Manager (SSM)

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

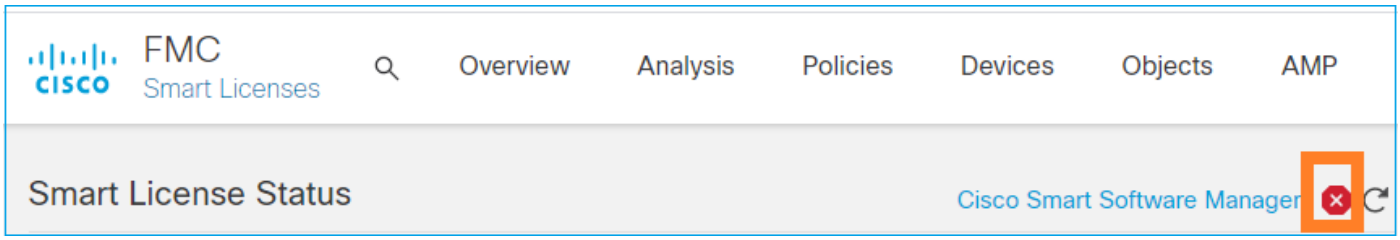


Der Registrierungsstatus des FMC kann über **Inventory > Product Instances** bestätigt werden. Überprüfen Sie das Ereignisprotokoll von der Registerkarte **Ereignisprotokoll**. Der Registrierungs- und Verwendungsstatus für Smart-Lizenzen kann auf der Registerkarte **Bestand > Lizenzen** überprüft werden. Überprüfen Sie, ob die erworbene Lizenz auf Dauer korrekt verwendet wird, und es gibt keine Warnmeldungen, die auf unzureichende Lizenzen hinweisen.

FMC Smart-Lizenzderegistrierung

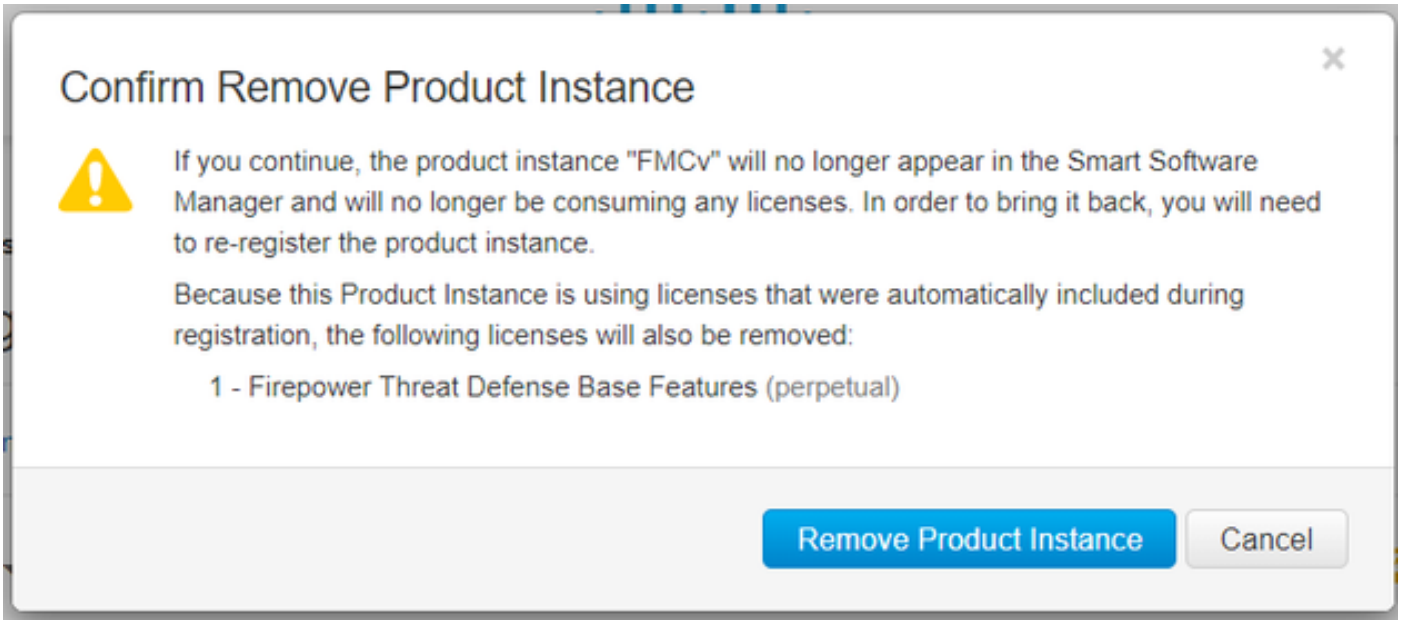
Registrierung des FMC vom Cisco SSM entfernen

Um die Lizenz aus irgendeinem Grund freizugeben oder ein anderes Token zu verwenden, navigieren Sie zu **System > Licenses > Smart Licenses (System > Lizenzen > Smart Licenses),** und wählen Sie die Schaltfläche zum Entfernen der Registrierung aus, wie in diesem Bild gezeigt.



Entfernen Sie die Registrierung von der SSM-Seite.

Wählen Sie im **Bestand > Produktinstanzen** die Option **Entfernen** im Ziel-FMC aus. Wählen Sie anschließend **Produktinstanz entfernen**, um das FMC zu entfernen und die zugeordneten Lizenzen freizugeben, wie in diesem Bild gezeigt.



Fehlerbehebung

Überprüfung der Zeitsynchronisierung

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

```
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 von **System > Configuration > Time Synchronization.**

Aktivieren der Namensauflösung und Überprüfung der Erreichbarkeit unter tools.cisco.com

Stellen Sie sicher, dass das FMC einen FQDN auflösen kann und erreichbar ist unter tools.cisco.com:

```
> 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 Verwaltungs-IP und die DNS-Server-IP von **System > Configuration > Management Interfaces (System > Konfiguration > Verwaltungsschnittstellen).**

Überprüfen des HTTPS-Zugriffs (TCP 443) vom FMC auf tools.cisco.com

Stellen Sie mithilfe des Befehls Telnet oder curl sicher, dass das FMC HTTPS-Zugriff auf tools.cisco.com hat. Wenn die TCP-443-Kommunikation unterbrochen ist, stellen Sie sicher, dass sie nicht von einer Firewall blockiert wird und sich kein SSL-Entschlüsselungsgerät im Pfad befindet.

```
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@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, Content-Length, Accept, Origin
< Content-Type: text/html
< Set-Cookie: CP_GUTC=10.163.4.54.1592389711389899; path=/; expires=Mon, 16-Jun-25 10:28:31 GMT;
domain=.cisco.com
< Set-Cookie: CP_GUTC=10.163.44.92.1592389711391532; path=/; expires=Mon, 16-Jun-25 10:28:31
GMT; domain=.cisco.com
< 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

Erfolgreiche Auflösung auf tools.cisco.com überprüfen:

```
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-Überprüfung

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

```
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-Benutzeroberfläche können die Proxywerte über **System > Configuration > Management Interfaces** bestätigt werden.

Wenn die FMC-seitigen Werte korrekt sind, überprüfen Sie die serverseitigen Proxywerte (z. B., wenn der Proxyserver den Zugriff vom FMC und auf tools.cisco.com zulässt. Darüber hinaus lassen Sie Datenverkehr und Zertifikatsaustausch über den Proxy zu. Das FMC verwendet ein Zertifikat für die Smart License-Registrierung).

Abgelaufene Token-ID

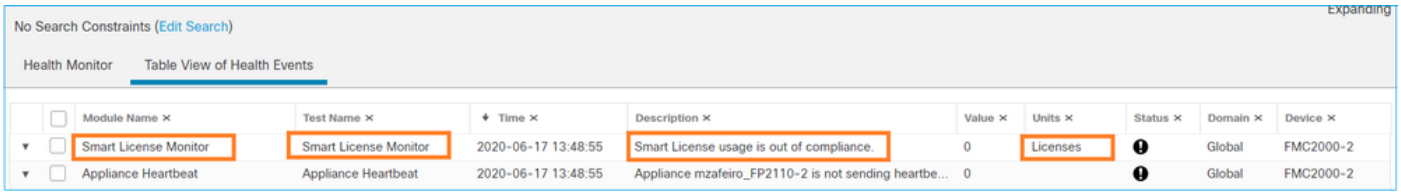
Überprüfen Sie, ob die ausgegebene Token-ID nicht abgelaufen ist. Wenn der Vorgang abgelaufen ist, bitten Sie den Smart Software Manager-Administrator, ein neues Token auszugeben und die Smart License mit der neuen Token-ID erneut zu registrieren.

Ändern des FMC Gateway

Es kann vorkommen, dass die Smart License-Authentifizierung aufgrund der Auswirkungen eines Relay-Proxys oder SSL-Entschlüsselungsgeräts nicht ordnungsgemäß durchgeführt werden kann. Wenn möglich, ändern Sie die Route für den FMC-Internetzugang, um diese Geräte zu vermeiden, und wiederholen Sie die Smart License-Registrierung.

Überprüfen Sie die Systemereignisse auf dem FMC.

Navigieren Sie im FMC zu **System > Health > Events (System > Status > Ereignisse)**, und überprüfen Sie den Status des Smart License Monitor-Moduls auf Fehler. Wenn die Verbindung beispielsweise aufgrund eines abgelaufenen Zertifikats fehlschlägt, Ein Fehler, wie z. B. **ID zertifiziert abgelaufen**, wird generiert, wie in diesem Bild gezeigt.



Überprüfen Sie das Ereignisprotokoll auf der SSM-Seite.

Wenn das FMC eine Verbindung zum CSSM herstellen kann, überprüfen Sie das Ereignisprotokoll der Verbindung unter **Bestand > Ereignisprotokoll**. Überprüfen Sie, ob solche Ereignisprotokolle oder Fehlerprotokolle im CSSM vorhanden sind. Wenn keine Probleme mit den Werten/dem Betrieb der FMC-Site auftreten und kein Ereignisprotokoll auf der CSSM-Seite vorhanden ist, besteht die Möglichkeit, dass es ein Problem mit der Route zwischen dem FMC und dem CSSM gibt.

Häufige Probleme

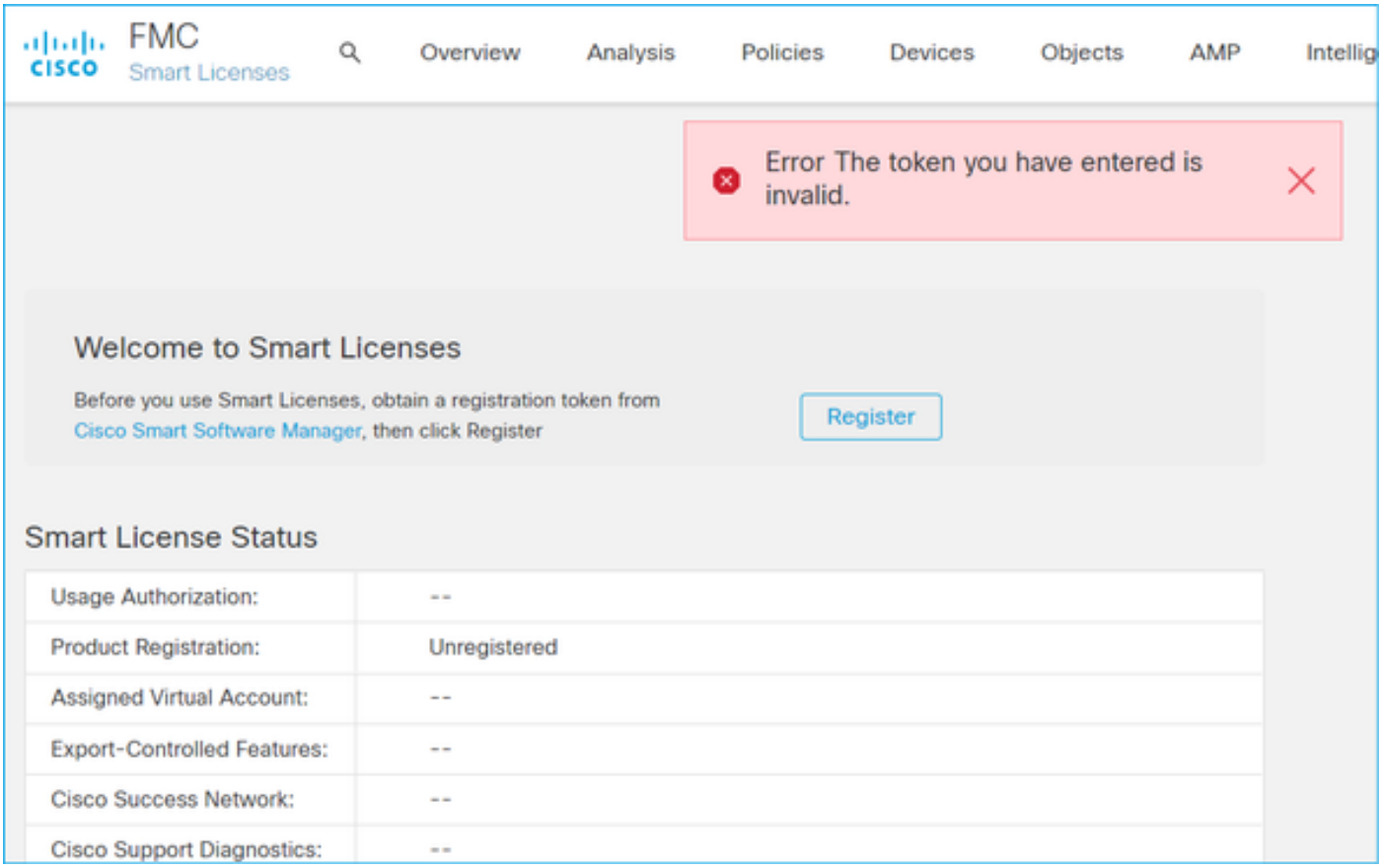
Zusammenfassung der Registrierungs- und Zulassungsstaaten:

Status der Produktregistrierung	Nutzungsautorisierungszustand	Kommentare
Nicht registriert	—	Das FMC befindet sich weder im registrierten noch im Evaluierungsmodus. Dies ist der Anfangsstatus nach der FMC-Installation oder nach Ablauf der Testlizenz für 90 Tage.
Registriert	Autorisiert	Das FMC ist beim Cisco Smart Software

		Manager (CSSM) registriert, und es sind FTD-Geräte registriert, für die ein gültiges Abonnement besteht.
Registriert	Autorisierung abgelaufen	Das FMC konnte seit mehr als 90 Tagen nicht mehr mit dem Cisco Lizenz-Backend kommunizieren.
Registriert	Nicht registriert	Das FMC ist beim Cisco Smart Software Manager (CSSM) registriert, es sind jedoch keine FTD-Geräte im FMC registriert.
Registriert	Out-of-Compliance	Das FMC ist beim Cisco Smart Software Manager (CSSM) registriert. Es gibt jedoch FTD-Geräte, die für ungültige Abonnements registriert sind. Beispielsweise verwendet ein FTD-Gerät (FP4112) ein THREAT-Abonnement, aber mit dem Cisco Smart Software Manager (CSSM) sind für FP4112 keine THREAT-Abonnements verfügbar.
Auswertung (90 Tage)	_	Der Evaluierungszeitraum ist in Gebrauch, es sind jedoch keine FTD-Geräte im FMC registriert.

Anwenderbericht 1. Ungültiges Token

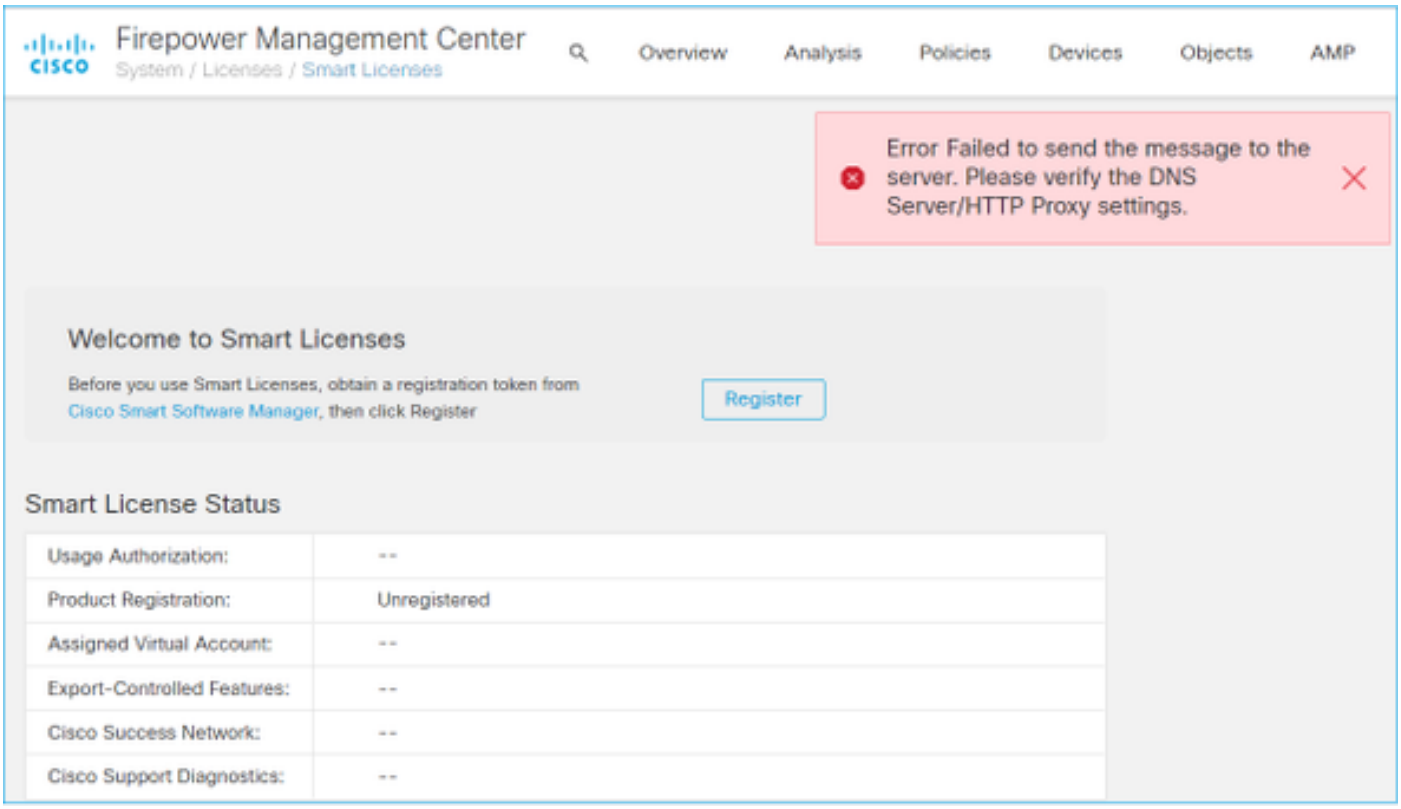
Symptom: Die Registrierung beim CSSM schlägt aufgrund eines ungültigen Tokens schnell fehl (~10 s), wie in diesem Bild gezeigt.



Auflösung: Verwenden Sie ein gültiges Token.

Anwenderbericht 2. Ungültiger DNS

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



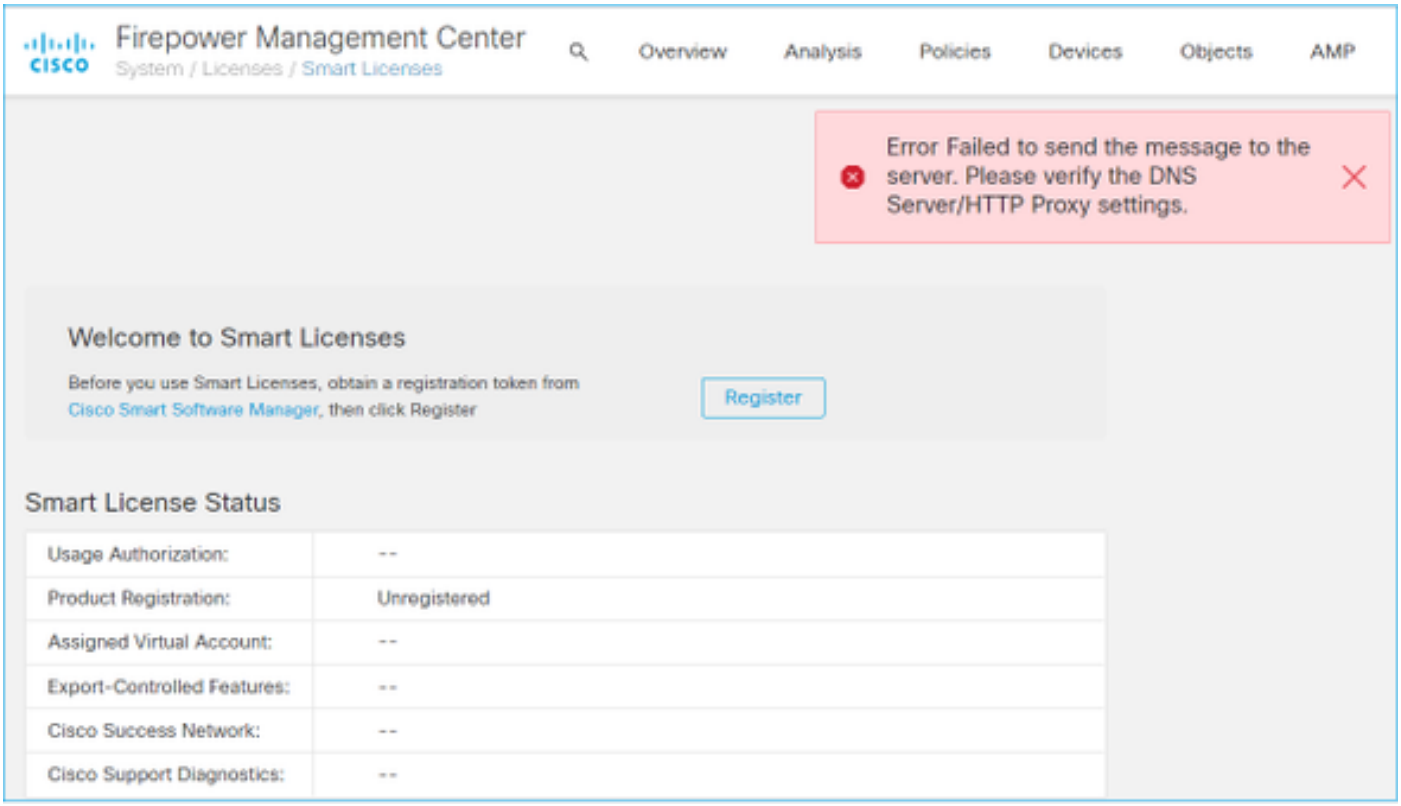
Überprüfen Sie die Datei /var/log/process_stdout.log. Das DNS-Problem wird angezeigt:

```
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, wenn es nicht konfiguriert ist, oder die DNS-Probleme zu beheben.

Anwenderbericht 3. Ungültige Zeitwerte

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



Überprüfen Sie die **Datei /var/log/process_stdout.log**. Die Zertifikatprobleme werden angezeigt:

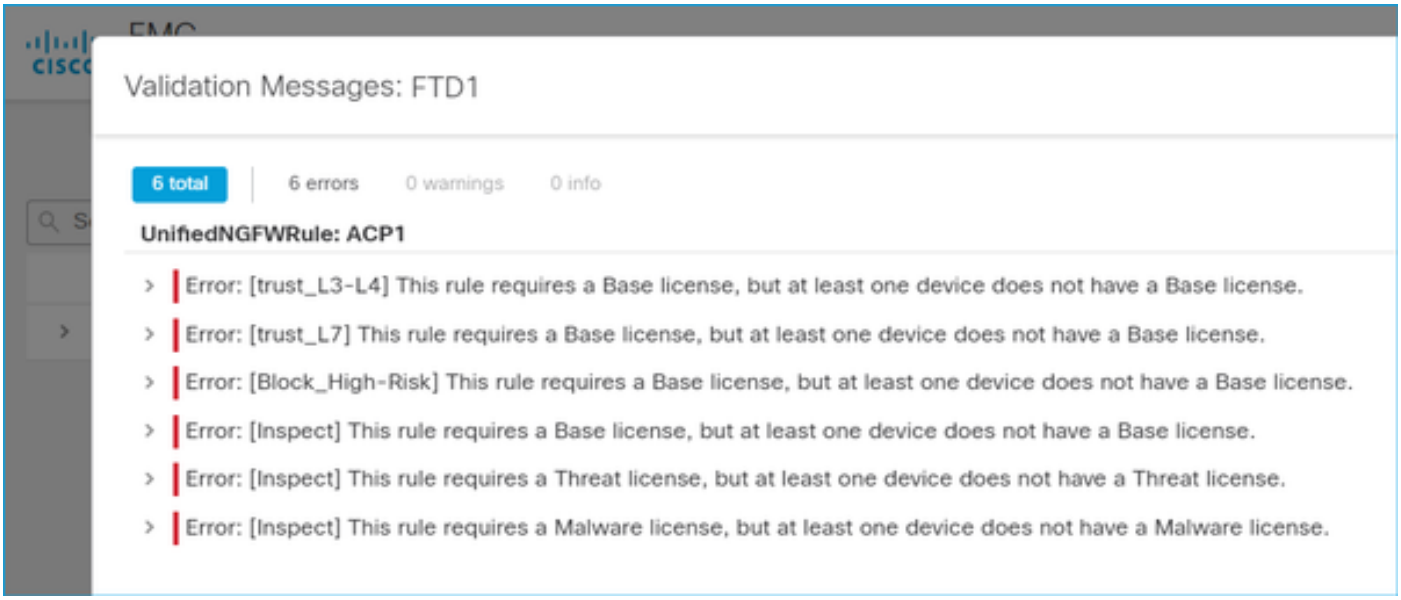
```
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE:
ch_pf_curl_request_init[59], request "POST", url
"https://tools.cisco.com/its/service/oddce/services/DDCEService"
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE:
ch_pf_curl_post_prepare[299], https related setting
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], set ca info
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], init msg header
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], unlock http mutex.
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 http msg, result 30
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@FMC2000-2:/Volume/home/admin# date
Fri Jun 25 09:27:22 UTC 2021
```

Anwenderbericht 4. Kein Abonnement

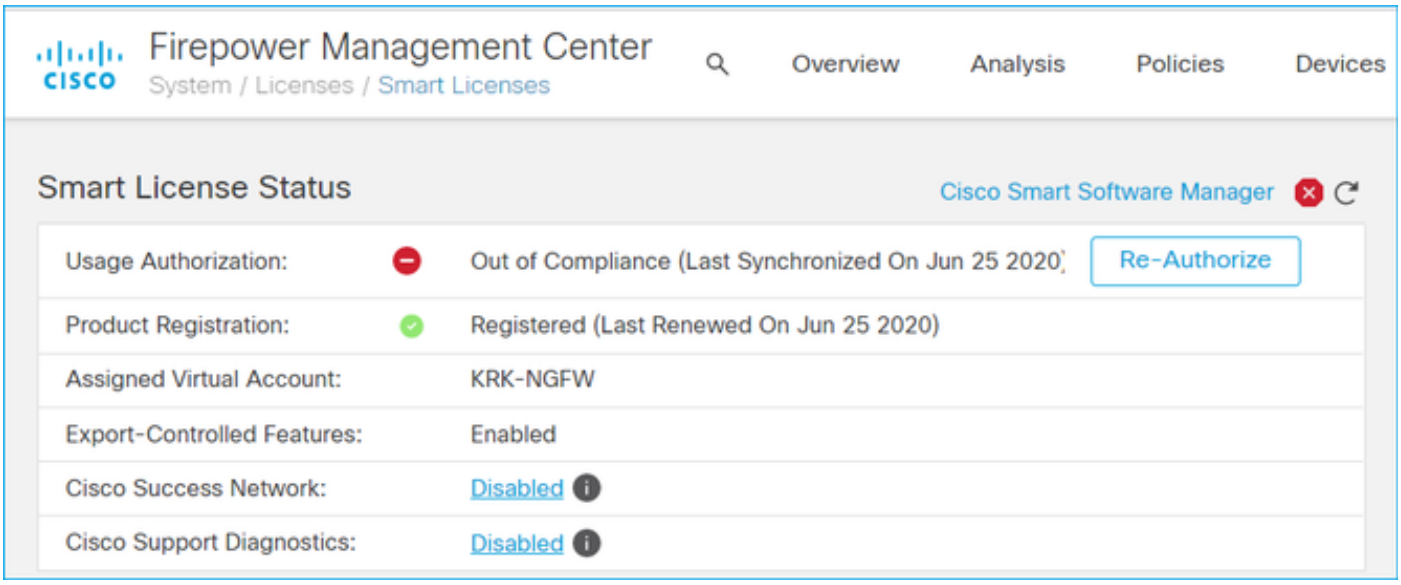
Wenn für eine bestimmte Funktion kein Lizenzabonnement vorhanden ist, ist die FMC-Bereitstellung nicht möglich:



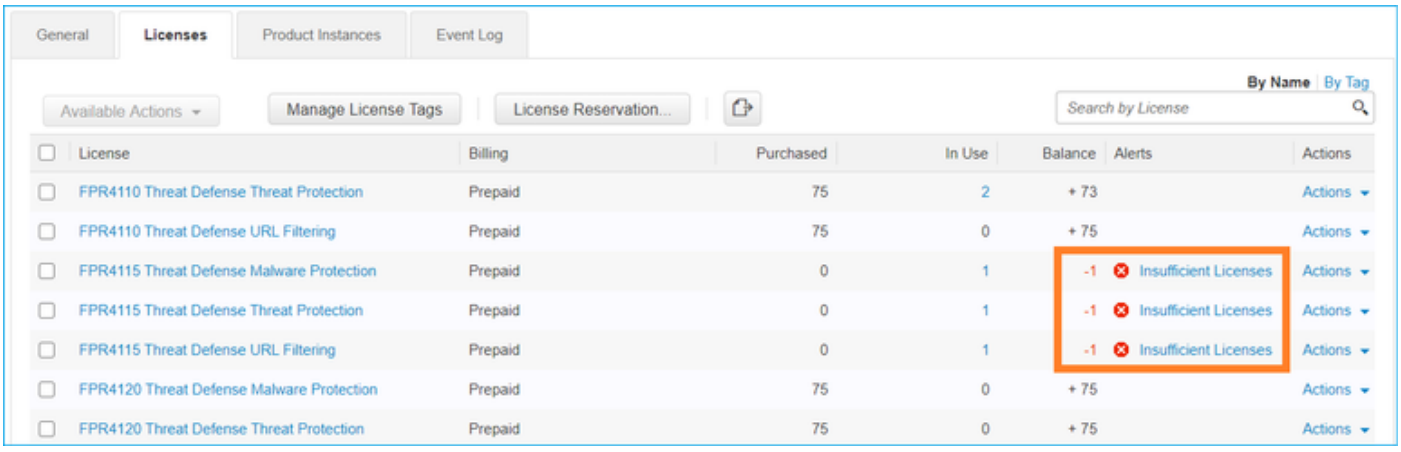
Auflösung: Sie müssen das erforderliche Abonnement erwerben und auf das Gerät anwenden.

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) geändert:

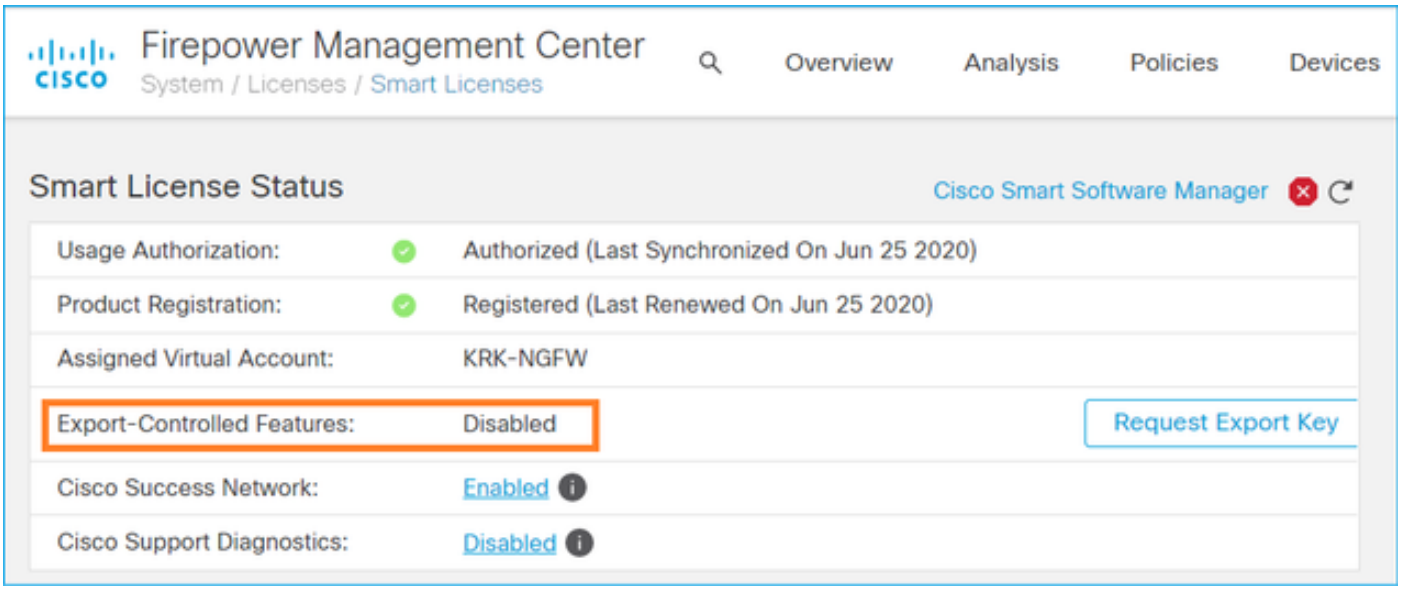


Überprüfen Sie im CSSM die Warnmeldungen auf Fehler:



Anwenderbericht 6. Keine zuverlässige Verschlüsselung

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



Auflösung: Registrieren Sie das FMC beim CSSM, und haben Sie ein Strong Encryption-Attribut aktiviert.

Zusätzliche Hinweise

Smart License State-Benachrichtigung festlegen

E-Mail-Benachrichtigung durch SSM

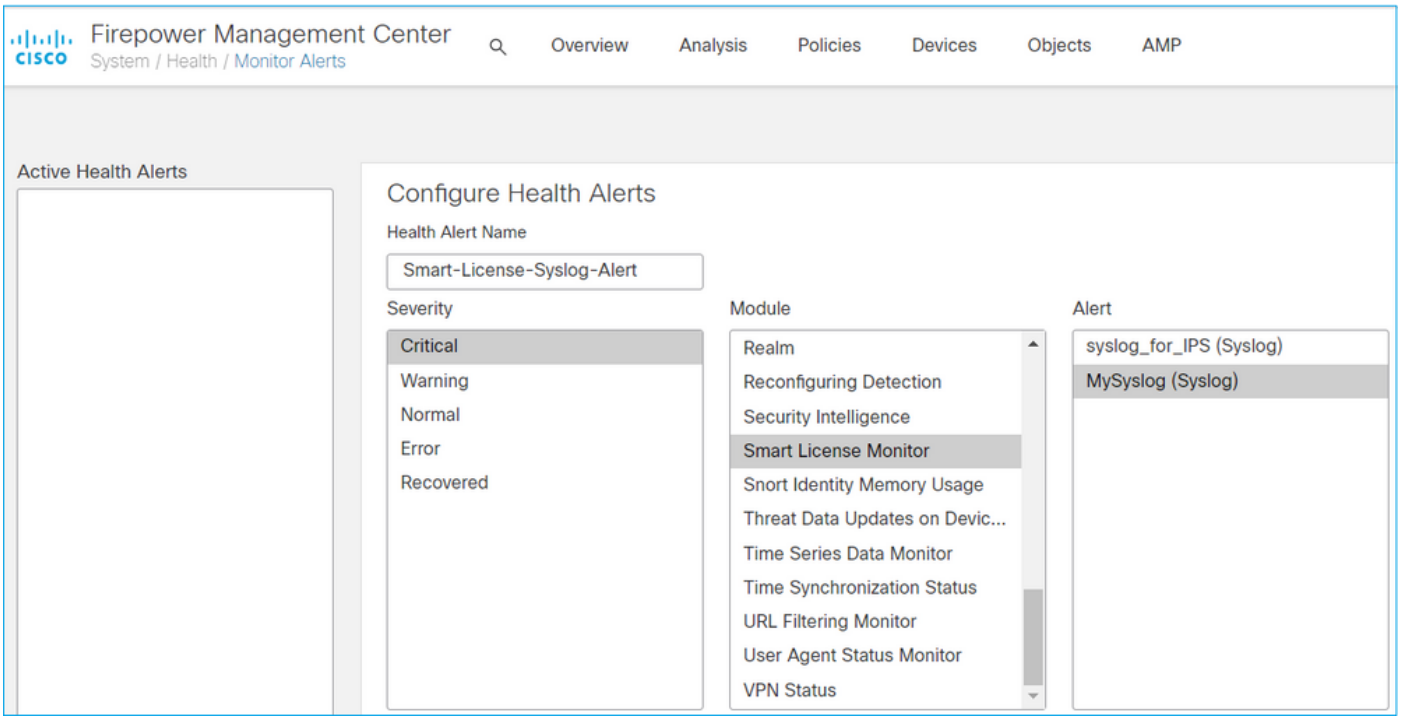
Auf der SSM-Seite ermöglicht die SSM-E-Mail-Benachrichtigung den Empfang zusammengefasster E-Mails für verschiedene Ereignisse. Beispielsweise Benachrichtigung bei fehlender Lizenz oder bei Lizenzen, die bald ablaufen. Benachrichtigungen über die Verbindung der Produktinstanz oder einen Update-Fehler können empfangen werden.

Diese Funktion ist sehr nützlich, um festzustellen und zu verhindern, dass funktionale Einschränkungen aufgrund des Lizenzablaufs auftreten.

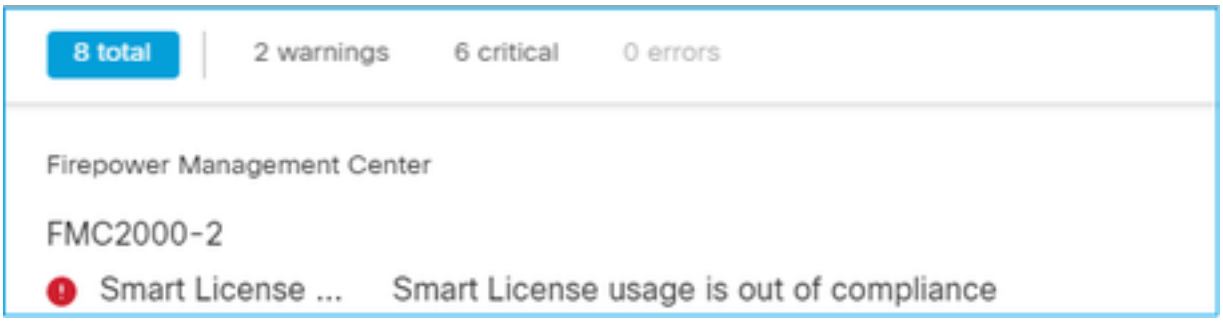
Abrufen von Gesundheitsbenachrichtigungen vom FMC

Auf der FMC-Seite ist es möglich, eine Health Monitor-Warnung zu konfigurieren und eine Warnmeldung über ein Systemereignis zu erhalten. Der Modul Smart License Monitor ist zur Überprüfung des Smart License-Status verfügbar. Die Überwachungswarnung unterstützt Syslog, E-Mail und SNMP-Trap.

Dies ist ein Konfigurationsbeispiel, um eine Syslog-Meldung abzurufen, wenn ein Smart License Monitor-Ereignis auftritt:



Dies ist ein Beispiel für eine Gesundheitswarnung:



Die vom FMC generierte Syslog-Meldung lautet:

```
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 Systemüberwachungswarnungen finden Sie unter Systemüberwachung.

Mehrere FMCs auf demselben Smart Account

Wenn im gleichen Smart Account mehrere FMCs verwendet werden, muss jeder FMC-Hostname eindeutig sein. Wenn mehrere FMCs im CSSM verwaltet werden, muss zur Unterscheidung jedes FMC der Hostname jedes FMC eindeutig sein. Dies ist nützlich für die laufende FMC Smart

License Wartung.

FMC muss Internetverbindungen aufrechterhalten

Nach der Registrierung prüft das FMC alle 30 Tage den Status der Smart License Cloud und der Lizenz. Wenn das FMC 90 Tage nicht kommunizieren kann, wird die lizenzierte Funktion beibehalten, aber der Status **Autorisierung abgelaufen** bleibt. Sogar 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 Klon (warm oder kalt) nicht offiziell unterstützt. Jede FirePOWER Management Center Virtual (FMCv) ist einzigartig, da sie über Authentifizierungsinformationen verfügt. Um mehrere FMCv bereitzustellen, muss die FMCv jeweils 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 (FAQs)

Wie viele Gerätelizenzen sind in FTD HA erforderlich?

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

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, Gerät auswählen und Lizenz auswählen. Wählen Sie das Bleistiftsymbol aus.**, wählen Sie die im Smart Account hinterlegte Lizenz aus, und wählen Sie **Speichern aus.**

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

Dieses Verhalten wird erwartet, da Smart Account die Anzahl der Geräte verfolgt, auf denen diese Lizenz aktiviert ist, nicht jedoch die Anzahl der aktiven Benutzer, die mit dem Netzwerk 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 für die Smart License Cloud registriert ist. Das erwartete Verhalten ist, dass die Remote-Zugriffskonfiguration nicht bereitgestellt werden kann, wenn das FMC nicht registriert ist oder sich im Evaluierungsmodus befindet. Wenn das FMC registriert ist, stellen Sie sicher, dass die AnyConnect-Lizenz in Ihrem Smart Account vorhanden ist und dem Gerät zugewiesen ist.

So weisen Sie eine Lizenz zu: navigieren zuFMC-**Geräte**, Gerät auswählen, **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 wenn eine Remote Access VPN-Konfiguration implementiert wird?

Für das im FTD bereitgestellte Remote Access VPN muss eine Strong Encryption-Lizenz aktiviert sein. EnStellen Sie sicher, dass eine Strong Encryption-Lizenz auf dem FMC aktiviert ist. So überprüfen Sie den Status der Lizenz für starke Verschlüsselung: navigieren an die FMC-**System > Lizenzen > Smart Licensing**und überprüfen Sie, ob die Exportfunktionen aktiviert sind.

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

Diese Funktion wird automatisch aktiviert, wenn das Token, das bei der Registrierung des FMC in die Smart Account Cloud verwendet wird, die Option **Exportgesteuerte Funktionen für die Produkte zulassen** bietet, **die mit diesem Token** aktiviert **sind**. Wenn diese Option für das Token nicht aktiviert ist, entfernen Sie die Registrierung des FMC, 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' nicht verfügbar ist, wenn das Token generiert wird?

Wenden Sie sich an Ihr Cisco Account Team.

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

Dieser Fehler wird angezeigt, wenn das FMC den Evaluierungsmodus verwendet oder das Smart License Account nicht auf eine Strong Encryption-Lizenz Anspruch hat. VÜberprüfen Sie, ob das FMC bei der License Authority registriert ist und **die exportgesteuerte Funktion für die mit diesem Token registrierten Produkte zulassen** aktiviert ist. Wenn dem Smart Account die Verwendung einer Lizenz für starke Verschlüsselung nicht gestattet ist, ist die Bereitstellung einer Site-to-Site-VPN-Konfiguration mit Chiffern, die stärker als DES sind, nicht zulässig.

Warum wird der Status "Out of Compliance" auf dem FMC empfangen?

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

Wie kann der Status "Out of Compliance" korrigiert werden?

Befolgen Sie die Schritte, die im Firepower-Konfigurationshandbuch beschrieben sind:

1. Im Abschnitt "Smart Licenses" unten auf der Seite können Sie ermitteln, welche Lizenzen erforderlich sind.

2. Erwerben Sie die erforderlichen Lizenzen über Ihre üblichen Kanäle.

3. Cisco Smart Software Manager (https://software.cisco.com/#SmartLicensing-Inventory)überprüfen, überprüfen Sie, ob die Lizenzen in Ihrem virtuellen Konto angezeigt werden.

4. Wählen Sie im FMC **System > Licenses > Smart Licenses (System > Lizenzen > Smart Licenses)** aus.

5. Wählen Sie **Erneute Autorisierung aus**.

Das vollständige Verfahren finden Sie unter Lizenzierung des FirePOWER-Systems.

Welche Funktionen bietet Firepower Threat Defense Base?

Die Basislizenz ermöglicht:

- Konfiguration von FTD-Geräten zum Umschalten und Weiterleiten (einschließlich DHCP Relay und NAT).
- Konfiguration von FTD-Geräten im HA-Modus (High Availability)
- Konfiguration von Sicherheitsmodulen als Cluster innerhalb eines Firepower 9300-Chassis (Intra-Chassis-Cluster).
- Konfiguration von FirePOWER Geräten der Serie 9300 oder FirePOWER der Serie 4100 (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?

Bei jedem Kauf eines FirePOWER Threat Defense- oder FirePOWER Threat Defense Virtual-Geräts ist automatisch eine Base-Lizenz enthalten. Sie wird automatisch zu Ihrem Smart Account hinzugefügt, wenn sich FTD beim FMC registriert.

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

Der FMC verwendet die IP-Adresse. auf Port 443, um mit der Smart License Cloud zu kommunizieren.

Diese IP-Adresse (https://tools.cisco.com)wird auf diese IP-Adressen aufgelöst:

- 72.163.4.38
- 173.37.145.8

Zugehörige Informationen

- Konfigurationsanleitungen für das FirePOWER Management Center
- Überblick über Cisco Live Smart Licensing: BRKARC-2034
- Funktionslizenzen für Cisco Secure Firewall Management Center
- Cisco Smart Software Licensing - Häufig gestellte Fragen (FAQs)