

FMC 및 FTD Smart License 등록 및 일반 문제를 사용하여 트러블슈팅

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[FMC Smart 라이선스 등록](#)

[사전 요구 사항](#)

[FMC Smart 라이선스 등록](#)

[SSM\(Smart Software Manager\)측 확인](#)

[FMC Smart 라이선스 등록 취소](#)

[RMA](#)

[문제 해결](#)

[일반적인 문제](#)

[사례 연구 1. 잘못된 토큰](#)

[사례 연구 2. 잘못된 DNS](#)

[사례 연구 3. 잘못된 시간 값](#)

[사례 연구 4. 구독 없음](#)

[사례 연구 5. 규정 위반\(OOC\)](#)

[사례 연구 6. 강력한 암호화 없음](#)

[추가 참고 사항](#)

[Smart License 상태 알림 설정](#)

[FMC에서 상태 알림 알림 받기](#)

[동일한 Smart Account의 여러 FMC](#)

[FMC는 인터넷 연결을 유지해야 함](#)

[여러 FMCv 구축](#)

[자주 묻는 질문\(FAQ\)](#)

[관련 정보](#)

소개

이 문서에서는 Firepower Threat Defense 관리 디바이스에서 Firepower Management Center의 Smart License 등록 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

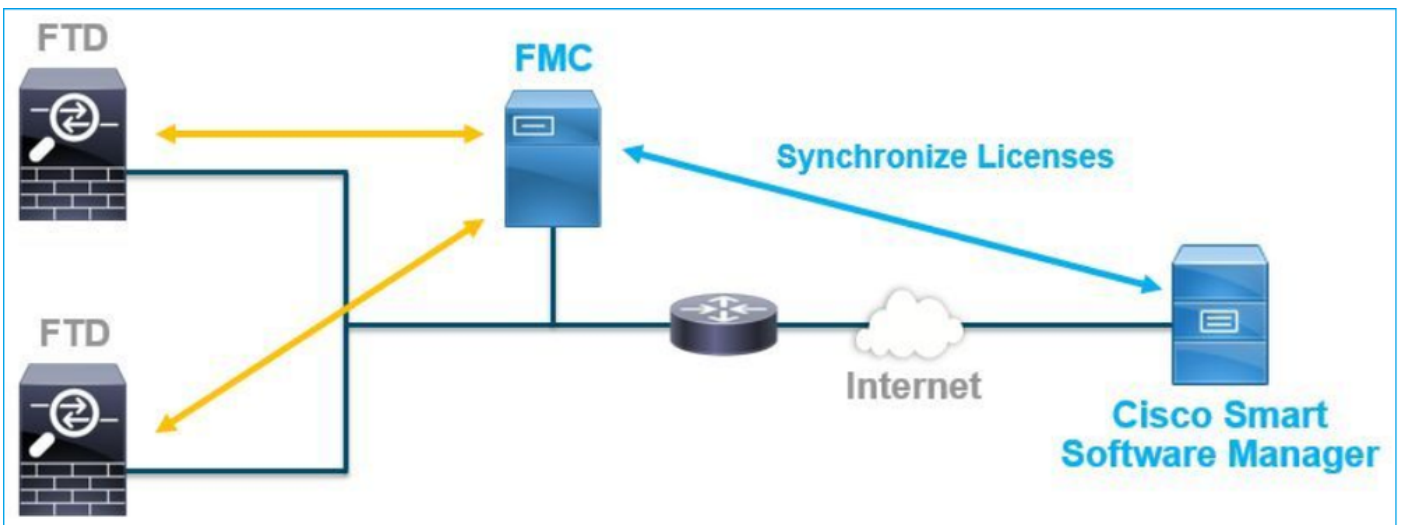
사용되는 구성 요소

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

FMC, FTD 및 Smart License 등록

Smart License 등록은 FMC(Firepower 관리 센터)에서 수행됩니다. FMC는 인터넷을 통해 CSSM(Cisco Smart Software Manager) 포털과 통신합니다. CSSM에서 방화벽 관리자는 Smart Account 및 해당 라이선스를 관리합니다. FMC는 관리되는 FTD(Firepower Threat Defense) 디바이스에 자유롭게 라이선스를 할당 및 삭제할 수 있습니다. 즉, FMC는 FTD 디바이스의 라이선스를 중앙에서 관리합니다.



FTD 디바이스의 특정 기능을 사용하려면 추가 라이선스가 필요합니다. 고객이 FTD 디바이스에 할당할 수 있는 Smart License 유형은 FTD License [Types and Restrictions\(FTD 라이선스 유형 및 제한\)](#)에 설명되어 있습니다.

Base 라이선스는 FTD 디바이스에 포함됩니다. 이 라이선스는 FMC가 CSSM에 등록될 때 Smart Account에 자동으로 등록됩니다.

기간별 라이선스: 위협, 악성코드, URL 필터링은 선택 사항입니다. 라이선스와 관련된 기능을 사용하려면 라이선스를 FTD 디바이스에 할당해야 합니다.

FTD 관리에 FMCv(Firepower Management Center Virtual)를 사용하려면 CSSM의 Firepower MCv 디바이스 라이선스도 FMCv에 필요합니다.

FMCv 라이선스는 소프트웨어에 포함되어 있으며 영구적입니다.

또한 이 문서에서는 발생할 수 있는 일반적인 라이선스 등록 오류를 해결하는 데 도움이 되는 시나리오를 제공합니다.

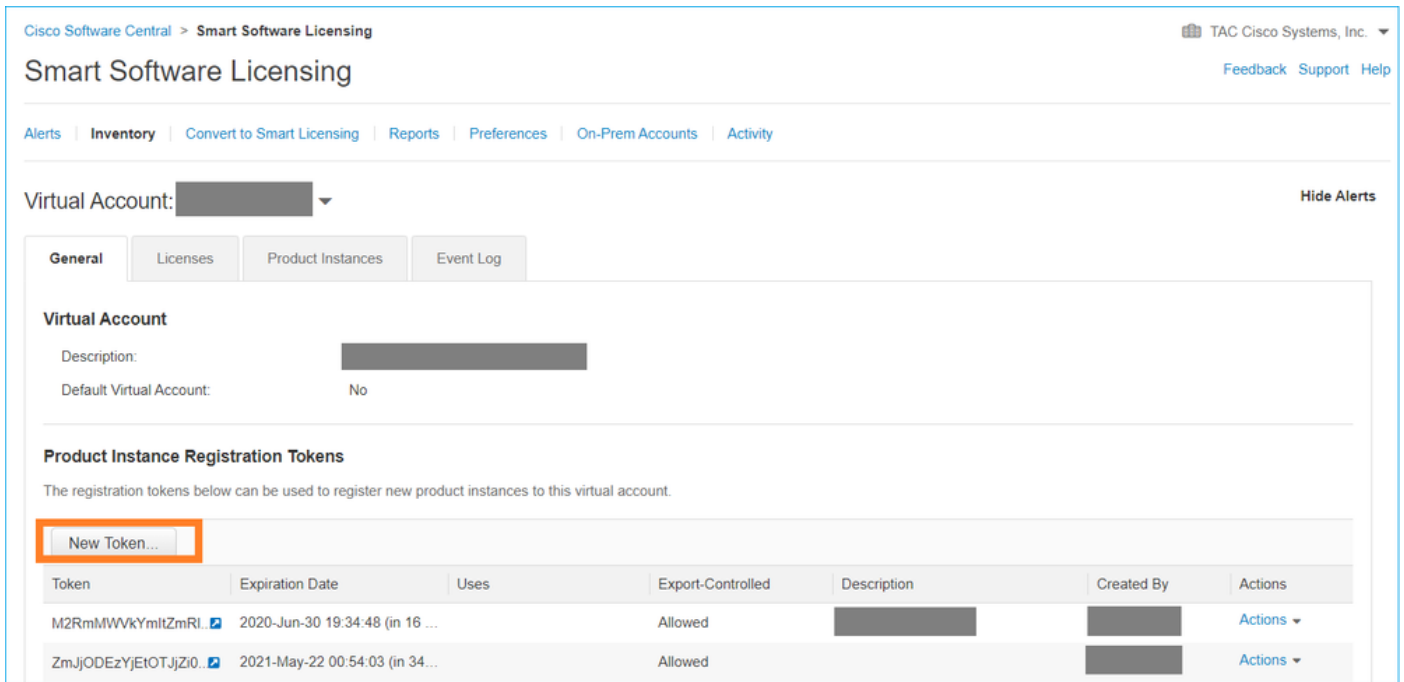
라이선스에 대한 자세한 내용은 [Cisco Firepower 시스템 기능 라이선스](#) 및 [Firepower 라이선싱에 대한 FAQ를 참조하십시오](#).

FMC Smart 라이선스 등록

사전 요구 사항

1. Smart License를 등록하려면 FMC가 인터넷에 액세스해야 합니다. 인증서가 HTTPS를 통해 FMC와 Smart License Cloud 간에 교환되므로, 경로에 통신에 영향을 줄 수 있는 디바이스가 없는지 확인합니다. (예: 방화벽, 프록시, SSL 암호 해독 디바이스 등)

2. CSSM에 액세스하여 이 이미지에 표시된 대로 Inventory(인벤토리) > General(일반) > New Token(새 토큰) 버튼에서 토큰 ID를 발급합니다.



강력한 암호화를 사용하려면 이 토큰 옵션으로 등록된 제품에 대해 Allow export-controlled(내보내기 제어 기능 허용)을 활성화합니다. 활성화하면 확인란에 확인 표시가 나타납니다.

3. 토큰 생성을 선택합니다.

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

FMC Smart 라이선스 등록

FMC에서 System(시스템) > Licenses(라이선스) > Smart Licenses(Smart 라이선스)로 이동하고 이 이미지에 표시된 대로 Register(등록) 버튼을 선택합니다.

Firepower Management Center
 System / Licenses / Smart Licenses

Overview Analysis Policies Devices Objects AMP Intelligence

Welcome to Smart Licenses

Before you use Smart Licenses, obtain a registration token from Cisco Smart Software Manager, then click Register

Smart License Status

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

Smart Licensing Product Registration(Smart Licensing 제품 등록) 창에 토큰 ID를 입력하고 이 이미지에 표시된 대로 Apply Changes(변경 사항 적용)를 선택합니다.

Smart Licensing Product Registration

Product Instance Registration Token:

OWI4Mzc5MTAtNzQwYi00YTVILTkyNTktMGMxNGJlYmRmNDUwLTE1OTQ3OTQ5%
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

Smart License 등록이 성공하면, 이 이미지에 표시된 것처럼 Product Registration(제품 등록) 상태에 Registered(등록됨)가 표시됩니다.

The screenshot shows the Cisco FMC Smart Licenses management page. At the top, there are navigation tabs: Overview, Analysis, Policies, Devices, Objects, AMP, Intelligence, and Deploy. The main content area is divided into two sections:

- Smart License Status:** A summary table showing the following status:

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:	Enabled ⓘ
Cisco Support Diagnostics:	Disabled ⓘ
- Smart Licenses:** A table with columns: License Type/Device Name, License Status, Device Type, Domain, and Group. The table shows a summary for 'Base (5)' with a green status icon, and sub-sections for Malware (0), Threat (0), and URL Filtering (0). There is a 'Filter Devices...' search box and an 'Edit Licenses' button at the top right of this section.

FTD 디바이스에 기간별 라이선스를 할당하려면 Edit Licenses(라이선스 수정)를 선택합니다. 그런 다음 관리되는 디바이스를 선택하여 Devices with license(라이선스가 있는 디바이스) 섹션에 추가합니다. 마지막으로, 이 이미지에 표시된 대로 Apply 버튼을 선택합니다.

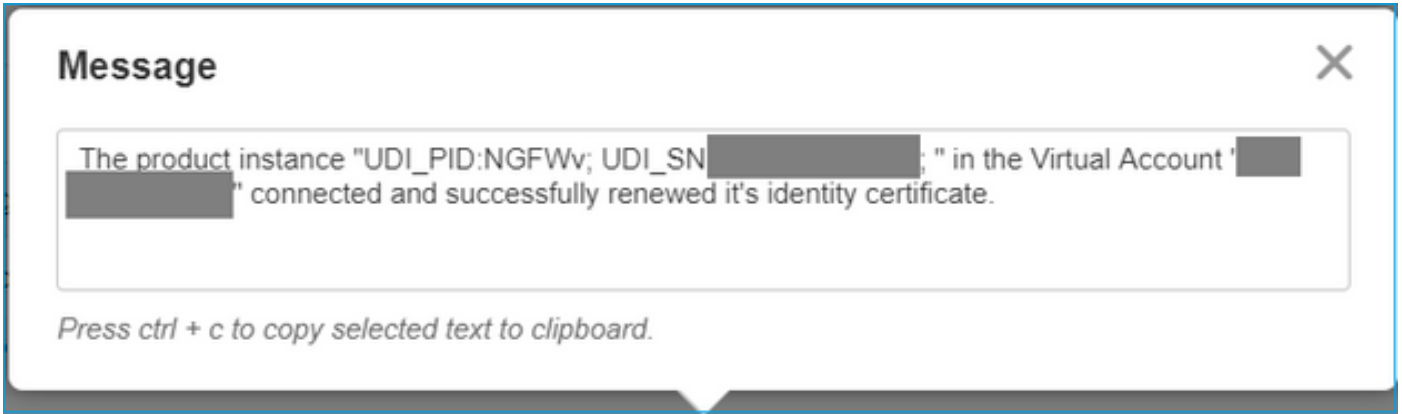
The screenshot shows the 'Edit Licenses' dialog box. It has tabs for Malware, Threat, URL Filtering, AnyConnect Apex, AnyConnect Plus, and AnyConnect VPN Only. The 'Malware' tab is selected. The dialog is split into two panes:

- Devices without license:** Contains a search box and a list with one item, 'FTD', which is highlighted with an orange box and labeled '1'.
- Devices with license (1):** Contains a list with one item, 'FTD', which is highlighted with an orange box.

An 'Add' button is located between the two panes and is labeled '2'. At the bottom right, there are 'Cancel' and 'Apply' buttons, with the 'Apply' button highlighted with an orange box and labeled '3'.

SSM(Smart Software Manager)측 확인

FMC Smart License 등록의 성공은 이 그림과 같이 CSSM의 Inventory(인벤토리) > Event Log(이벤트 로그)에서 확인할 수 있습니다.

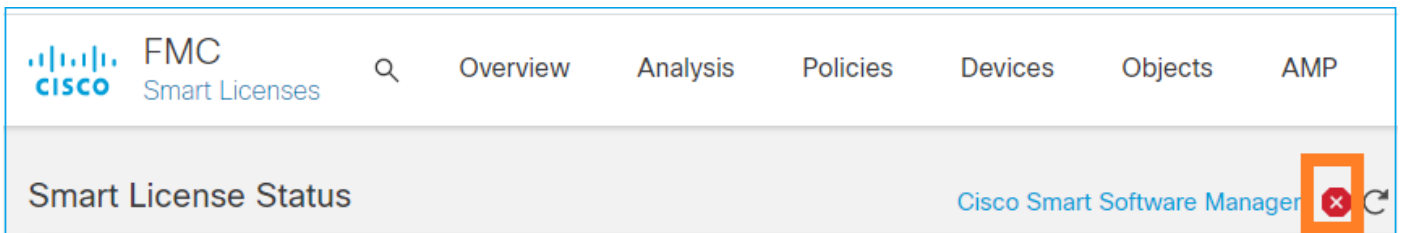


FMC의 등록 상태는 Inventory(인벤토리) > Product Instances(제품 인스턴스)에서 확인할 수 있습니다. Event Log(이벤트 로그) 탭에서 이벤트 로그를 확인합니다. Smart License 등록 및 사용 상태는 Inventory(인벤토리) > Licenses(라이선스) 탭에서 확인할 수 있습니다. 구매한 기간별 라이선스가 올바르게 사용되고 라이선스 부족을 나타내는 경고가 없는지 확인합니다.

FMC Smart 라이선스 등록 취소

Cisco SSM에서 FMC 등록 취소

어떤 이유로 라이선스를 릴리스하거나 다른 토큰을 사용하려면 이 이미지에 표시된 대로 System > Licenses > Smart Licenses로 이동하여 등록 취소 버튼을 선택합니다.



SSM 측에서 등록 제거

Smart Software Manager([Cisco Smart Software Manager](#))에 액세스하고 Inventory(인벤토리) > Product Instances(제품 인스턴스)에서 대상 FMC에서 Remove(제거)를 선택합니다. 그런 다음 Remove Product Instance(제품 인스턴스 제거)를 선택하여 이 이미지에 표시된 대로 FMC를 제거하고 할당된 라이선스를 해제합니다.

Cisco Software Central > Smart Software Licensing

Smart Software Licensing

Support Help


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

Virtual Account: [Redacted] 3 Major 171 Minor Hide Alerts

General Licenses **Product Instances** Event Log

Authorize License-Enforced Features... [fmcv]

Name	Product Type	Last Contact	Alerts	Actions
fmcv-rabc1	FP	2022-Sep-13 09:28:40		Actions ▾
fmcvxyz1	FP	2022-Sep-12 14:01:45		Actions ▾ Transfer... Remove...



Confirm Remove Product Instance

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

FMC가 RMA인 경우 FMC Smart License De-Registration(FMC 스마트 라이선스 등록 취소) > Remove Registration from SSM Side(SSM 측에서 등록 제거)의 단계에 따라 CSSM(Cisco Smart Software Manager)에서 FMC를 등록 취소한 다음 FMC Smart License Registration(FMC 스마트 라이선스 등록) 섹션의 단계에 따라 CSSM에 FMC를 다시 등록합니다.

문제 해결

시간 동기화 확인

FMC CLI(예: SSH)에 액세스하여 시간이 올바르게 신뢰할 수 있는 NTP 서버와 동기화되었는지 확인합니다. 인증서는 Smart License 인증에 사용되므로 FMC에 올바른 시간 정보가 있어야 합니다.

```
<#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

FMC UI에서 System > Configuration > Time Synchronization의 NTP 서버 값을 확인합니다.

이름 확인 사용 및 tools.cisco.com에 대한 연결 가능성 확인

FMC에서 FQDN을 확인할 수 있고 tools.cisco.com에 연결할 수 있는지 확인합니다.

```
<#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
```

FMC UI의 System(시스템) > Configuration(컨피그레이션) > Management Interfaces(관리 인터페이스)에서 관리 IP 및 DNS 서버 IP를 확인합니다.

FMC에서 tools.cisco.com으로 HTTPS(TCP 443) 액세스 확인

Telnet 또는 curl 명령을 사용하여 FMC가 tools.cisco.com에 대한 HTTPS 액세스 권한을 갖는지 확인합니다. TCP 443 통신이 끊긴 경우 방화벽에 의해 차단되지 않고 경로에 SSL 암호 해독 장치가 없는지 확인합니다.

<#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

컬 테스트:

<#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, Co
< 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; domai
< 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 확인

tools.cisco.com에 대한 확인이 성공했는지 확인합니다.

```
<#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
```

프록시 확인

apProxy가 사용되는 경우 FMC 및 프록시 서버 측 모두에서 값을 확인합니다. FMC에서 FMC가 올

바른 프록시 서버 IP 및 포트를 사용하는지 확인합니다.

<#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
```

FMC UI에서 프록시 값은 System > Configuration > Management Interfaces에서 확인할 수 있습니다.

FMC측 값이 정확하면 프록시 서버측 값을 확인합니다(예: 프록시 서버가 FMC 및 tools.cisco.com에 대한 액세스를 허용하는 경우). 또한 프록시를 통한 트래픽 및 인증서 교환을 허용합니다. FMC는 Smart License 등록을 위해 인증서를 사용합니다.

만료된 토큰 ID

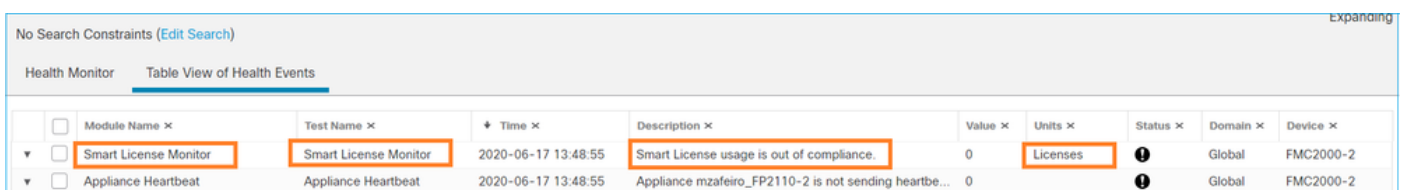
발급된 토큰 ID가 만료되지 않았는지 확인합니다. 만료되면 Smart Software Manager 관리자에게 새 토큰을 발급하고 새 토큰 ID로 Smart 라이선스를 다시 등록하도록 요청합니다.

FMC 게이트웨이 변경

릴레이 프록시 또는 SSL 암호 해독 장치의 영향으로 스마트 라이선스 인증을 올바르게 수행할 수 없는 경우가 있을 수 있습니다. 가능하면 이러한 디바이스를 피하도록 FMC 인터넷 액세스에 대한 경로를 변경하고 Smart License 등록을 다시 시도하십시오.

FMC에서 상태 이벤트 확인

FMC에서 System > Health > Events로 이동하고 Smart License Monitor 모듈의 상태에서 오류를 확인합니다. 예를 들어 만료된 인증서로 인해 연결이 실패하는 경우 이 이미지에 표시된 대로 id 인증서 만료와 같은 오류가 생성됩니다.



Module Name	Test Name	Time	Description	Value	Units	Status	Domain	Device
Smart License Monitor	Smart License Monitor	2020-06-17 13:48:55	Smart License usage is out of compliance.	0	Licenses	!	Global	FMC2000-2
Appliance Heartbeat	Appliance Heartbeat	2020-06-17 13:48:55	Appliance mzafeiro_FP2110-2 is not sending heartbe...	0		!	Global	FMC2000-2

SSM 측의 이벤트 로그 확인

FMC가 CSSM에 연결할 수 있는 경우 Inventory(인벤토리) > Event Log(이벤트 로그)에서 연결의 이벤트 로그를 확인합니다. CSSM에 이러한 이벤트 로그 또는 오류 로그가 있는지 확인합니다.

FMC 사이트의 값/운영에 문제가 없고 CSSM 측에 이벤트 로그가 없는 경우 FMC와 CSSM 간의 경로에 문제가 있을 가능성이 있습니다.

일반적인 문제

등록 및 권한 부여 상태 요약:

제품 등록 상태	사용 권한 부여 상태	의견
등록되지 않음	—	FMC가 Registered(등록됨) 또는 Evaluation(평가) 모드가 아닙니다. 이는 FMC 설치 후 또는 90일 평가 라이선스 만료 후의 초기 상태입니다.
등록됨	승인	FMC는 CSSM(Cisco Smart Software Manager)에 등록되며 유효한 서브스크립션으로 등록된 FTD 디바이스가 있습니다.
등록됨	권한 부여 만료됨	FMC가 90일 이상 Cisco 라이선스 백엔드와 통신하지 못했습니다.
등록됨	등록되지 않음	FMC가 CSSM(Cisco Smart Software Manager)에 등록되었지만 FMC에 등록된 FTD 디바이스는 없습니다.
등록됨	규정 위반	FMC가 CSSM(Cisco Smart Software Manager)에 등록되었지만 잘못된 서브스크립션으로 등록된 FTD 디바이스가 있습니다. 예를 들어 FTD(FP4112) 디바이스에서 THREAT 서브스크립션을 사용하지만, CSSM(Cisco Smart Software Manager)을 사용하는 경우 FP4112에 사용할 수 있는 위협 서브스크립션은 없습니다.
평가(90일)	해당 없음	평가 기간이 사용 중이지만 FMC에 등록된 FTD 디바이스는 없습니다.

사례 연구 1. 잘못된 토큰

증상: 이 그림에서 볼 수 있듯이 잘못된 토큰으로 인해 CSSM에 대한 등록이 빠르게(~10s) 실패합니다.

FMC Smart Licenses

Overview Analysis Policies Devices Objects AMP Intellig

Error The token you have entered is invalid.

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:	--

해결 방법: 올바른 토큰을 사용하십시오.

사례 연구 2. 잘못된 DNS

증상: 이 그림과 같이 잠시 후(25초) CSSM에 등록하지 못했습니다.

Firepower Management Center System / Licenses / Smart Licenses

Overview Analysis Policies Devices Objects AMP

Error Failed to send the message to the server. Please verify the DNS Server/HTTP Proxy settings.

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:	--

/var/log/process_stdout.log 파일을 확인합니다. DNS 문제가 나타납니다.

<#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_cur1_send_msg[494], failed to perform, err code 6, err string
```

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

해결 방법: CSSM 호스트 이름 확인 오류입니다. 해결책은 구성되지 않은 경우 DNS를 구성하거나 DNS 문제를 수정하는 것입니다.

사례 연구 3. 잘못된 시간 값

증상: 이 그림과 같이 잠시 후(25초) CSSM에 등록하지 못했습니다.

Firepower Management Center
System / Licenses / Smart Licenses

Overview Analysis Policies Devices Objects AMP

Error Failed to send the message to the server. Please verify the DNS Server/HTTP Proxy settings.

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:	--

/var/log/process_stdout.log 파일을 확인합니다. 인증서 문제가 나타납니다.

<#root>

```
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_cur1_request_init[59]  
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_cur1_post_prepare[299]  
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_cur1_post_prepare[302]  
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_cur1_head_init[110],  
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-ERROR: ch_pf_cur1_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], unl
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
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[51
cert issue checking, ret 60, url https://tools.cisco.com/its/service/oddce/services/DDCEService
```

FMC 시간 값을 확인합니다.

```
<#root>
```

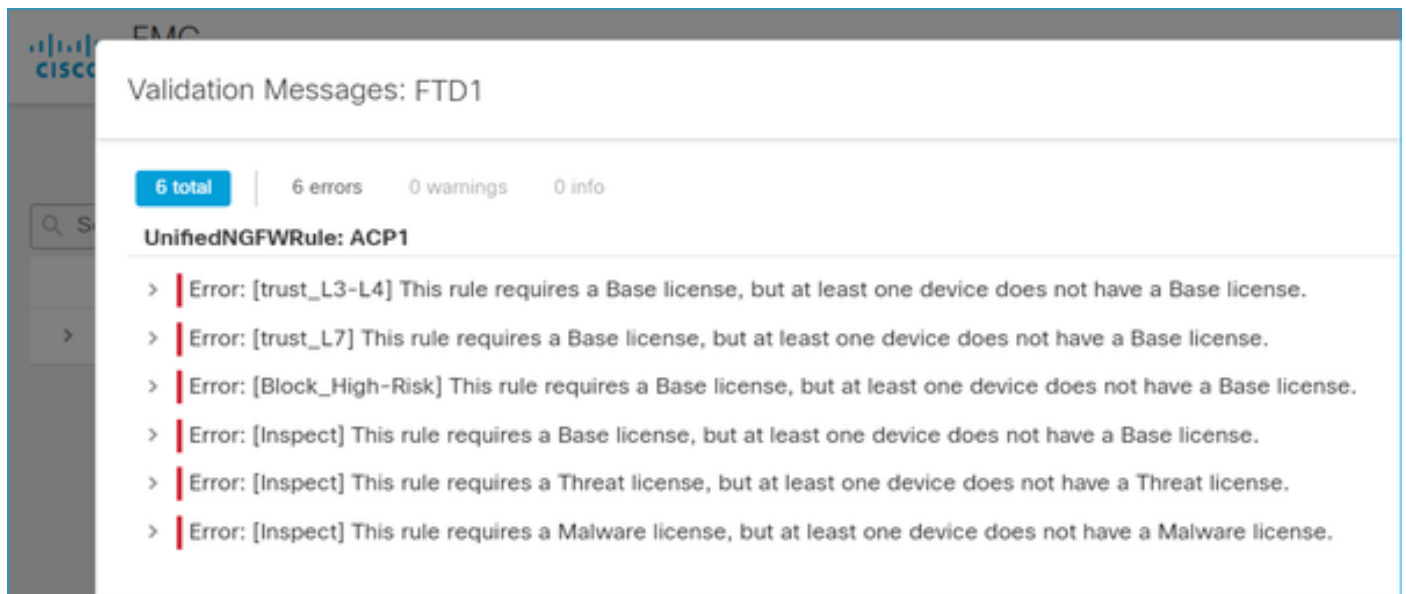
```
root@FMC2000-2:/Volume/home/admin#
```

```
date
```

```
Fri Jun 25 09:27:22 UTC 2021
```

사례 연구 4. 구독 없음

특정 기능에 대한 라이선스 서브스크립션이 없으면 FMC 구축이 불가능합니다.



해결 방법: 필요한 서브스크립션을 구매하여 디바이스에 적용해야 합니다.

사례 연구 5. 규정 위반(OOC)

FTD 서브스크립션에 대한 자격이 없는 경우 FMC Smart License는 OOC(Out-of-Compliance) 상태로 전환됩니다.

Firepower Management Center
System / Licenses / Smart Licenses

Overview Analysis Policies Devices

Smart License Status

Cisco Smart Software Manager ✖ ↻

Usage Authorization:	✖	Out of Compliance (Last Synchronized On Jun 25 2020)	Re-Authorize
Product Registration:	✔	Registered (Last Renewed On Jun 25 2020)	
Assigned Virtual Account:		KRK-NGFW	
Export-Controlled Features:		Enabled	
Cisco Success Network:		Disabled ℹ	
Cisco Support Diagnostics:		Disabled ℹ	

CSSM에서 Alerts for errors를 확인합니다.

General Licenses Product Instances Event Log

Available Actions Manage License Tags License Reservation... 🔍

Search by License 🔍 By Name By Tag

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

사례 연구 6. 강력한 암호화 없음

Base 라이선스만 사용할 경우 FTD LINA 엔진에서 DES(Data Encryption Standard) 암호화가 활성화됩니다. 이 경우, L2L VPN(Virtual Private Network)과 같이 강력한 알고리즘을 사용하는 구축은 실패합니다.

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 can 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
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	Request Export Key
Cisco Success Network:		Enabled i	
Cisco Support Diagnostics:		Disabled i	

해결 방법: FMC를 CSSM에 등록하고 Strong Encryption 특성이 활성화되었습니다.

추가 참고 사항

Smart License 상태 알림 설정

SSM의 이메일 알림

SSM 측에서 SSM Email Notification을 사용하면 다양한 이벤트에 대한 요약 이메일을 수신할 수 있습니다. 예를 들어, 라이선스 부족 또는 곧 만료될 라이선스에 대한 알림입니다. 제품 인스턴스 연결 또는 업데이트 실패 알림을 수신할 수 있습니다.

이 기능은 라이선스 만료로 인한 기능 제한의 발생을 알리고 방지하는데 매우 유용하다.

Smart Software Licensing

[Alerts](#) | [Inventory](#) | [License Conversion](#) | [Reports](#) | [Email Notification](#) | [Satellites](#) | [Activity](#)

Email Notification

Daily Event Summary

Receive a daily email summary containing the events selected below

Email Address:

Alert Events:

- Insufficient Licenses - Usage in account exceeds available licenses
- Licenses Expiring - Warning that term-limited licenses will be expiring. Sent 90, 60, 30, 14, 7, 3 and 1 day prior to expiration.
- Licenses Expired - Term-limited licenses have expired. Only displayed if Licenses Expiring warning have not been dismissed.
- Product Instance Failed to Connect - Product has not successfully connected during its renewal period
- Product Instance Failed to Renew - Product did not successfully connect within its maximum allowed renewal period.
- Satellite Synchronization Overdue - Satellite has not synchronized within the expected time period.
- Satellite Unregistered and Removed - Satellite failed to synchronize in 90 days and has been removed.
- Licenses Not Converted - One or more traditional licenses were not automatically converted to Smart during Product Instance Registration.

Informational Events:

- New Licenses - An order has been processed and new licenses have been added to the account
- New Product Instance - A new product instance has successfully registered with the account
- Licenses Reserved - A product instance has reserved licenses in the account

Status Notification

Receive an email when a Satellite synchronization file has finished processing by Smart Software Manager

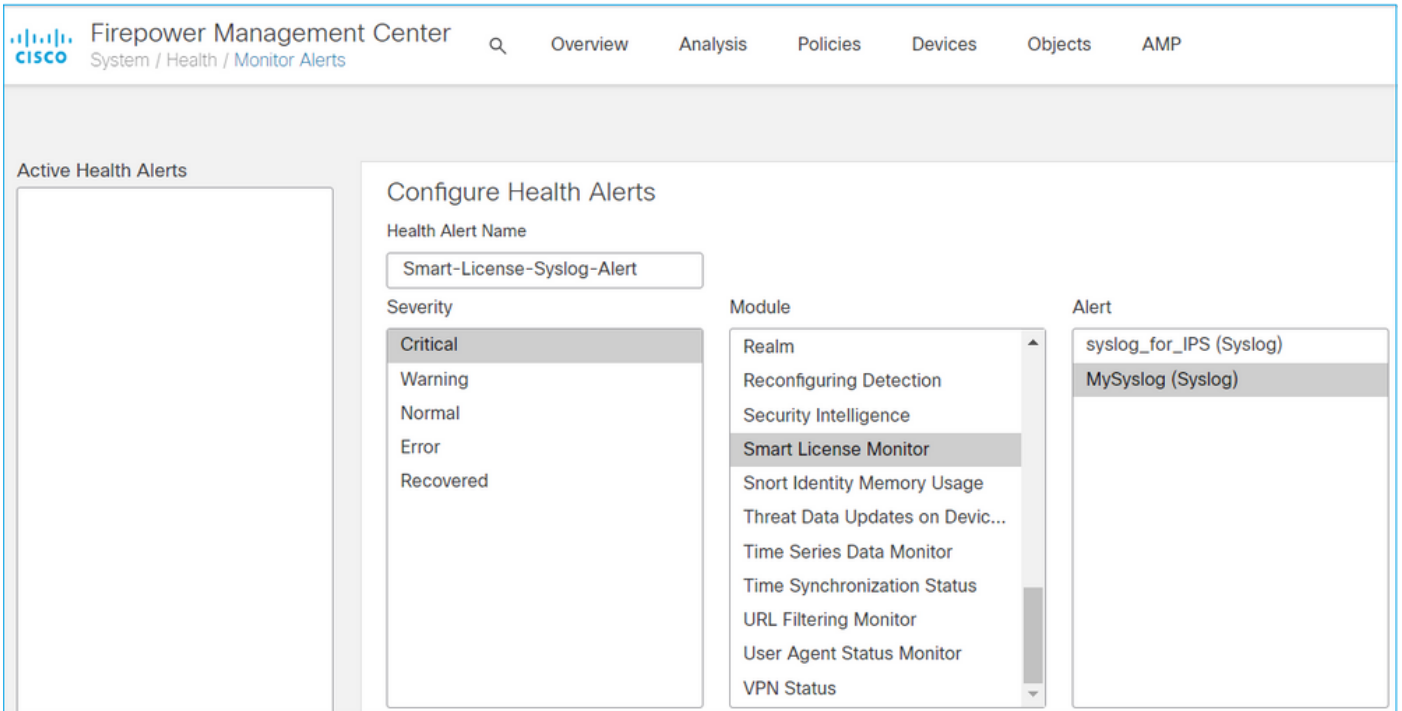
Save

Reset

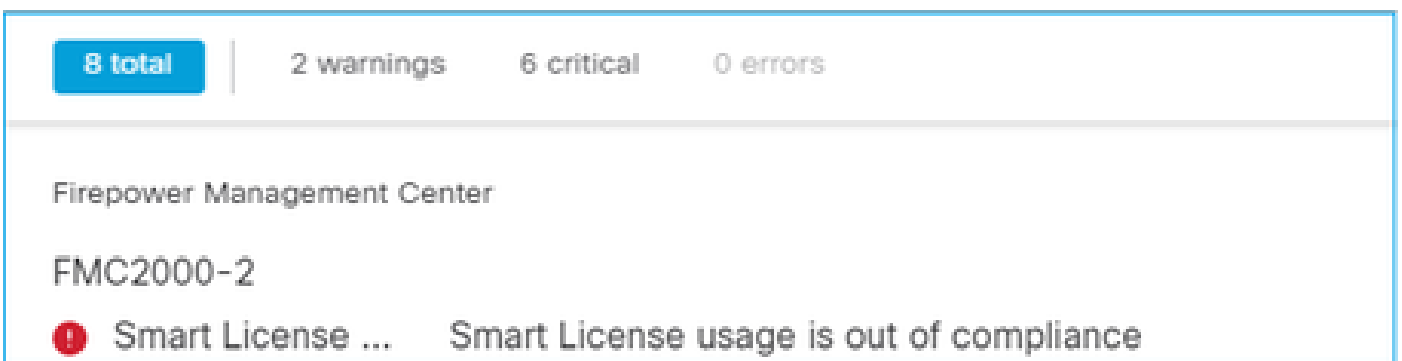
FMC에서 상태 알림 알림 받기

FMC 측에서 Health Monitor Alert를 구성하고 상태 이벤트에 대한 경고 알림을 수신할 수 있습니다. Module Smart License Monitor를 사용하여 Smart License 상태를 확인할 수 있습니다. 모니터 알림은 Syslog, 이메일 및 SNMP 트랩을 지원합니다.

다음은 Smart License 모니터 이벤트가 발생할 때 Syslog 메시지를 가져오기 위한 컨피그레이션 예입니다.



다음은 상태 알림의 예입니다.



FMC에서 생성되는 Syslog 메시지는 다음과 같습니다.

```
<#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
```

Health Monitor Alerts에 대한 자세한 내용은 [Health Monitoring](#)을 참조하십시오.

동일한 Smart Account의 여러 FMC

동일한 Smart Account에서 여러 FMC를 사용하는 경우 각 FMC 호스트 이름은 고유해야 합니다. CSSM에서 여러 FMC를 관리할 경우 각 FMC를 구분하려면 각 FMC의 호스트 이름이 고유해야 합

니다. 이 기능은 작동 중인 FMC Smart License 유지 보수에 유용합니다.

FMC는 인터넷 연결을 유지해야 함

등록 후 FMC는 30일마다 Smart License 클라우드 및 라이선스 상태를 확인합니다. FMC가 90일 동안 통신할 수 없는 경우, 라이선스 기능은 유지되지만 Authorization Expired(권한 부여 만료됨) 상태로 유지됩니다. 이 상태에서도 FMC는 Smart License Cloud에 계속 연결하려고 시도합니다.

여러 FMCv 구축

가상 환경에서 Firepower 시스템을 사용할 경우 클론(핫 또는 콜드)이 공식적으로 지원되지 않습니다. 각 FMCv(Firepower Management Center virtual)는 내부에 인증 정보가 있으므로 고유합니다. 여러 FMCv를 구축하려면 OVF(Open Virtualization Format) 파일에서 한 번에 하나씩 FMCv를 만들어야 합니다. 이 제한 사항에 대한 자세한 내용은 [Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide](#)를 참조하십시오.

자주 묻는 질문(FAQ)

FTD HA에서 필요한 디바이스 라이선스는 몇 개입니까?

High Availability에서 2개의 FTD를 사용하는 경우 각 디바이스에 라이선스가 필요합니다. 예를 들어, FTD HA 쌍에서 IPS(Intrusive Protection System) 및 AMP(Advanced Malware Protection) 기능을 사용하는 경우 두 개의 위협 및 악성코드 라이선스가 필요합니다.

FTD에서 AnyConnect 라이선스를 사용하지 않는 이유는 무엇입니까?

Smart Account에 FMC를 등록한 후 AnyConnect 라이선스가 활성화되었는지 확인합니다. 라이선스를 활성화하려면 FMC > Devices(디바이스)에서 디바이스를 선택하고 License(라이선스)를 선택합니다. 연필 아이콘을 선택합니다. Smart Account에 저장된 라이선스를 선택하고 저장을 선택합니다.

100명의 사용자가 연결되어 있을 때 Smart Account에서 AnyConnect 라이선스가 '사용 중'인 이유는 무엇입니까?

이는 Smart Account가 연결된 활성 사용자가 아니라 이 라이선스가 활성화된 디바이스 수를 추적하므로 예상되는 동작입니다.

오류가 발생한 이유 Device does not have the AnyConnect License FMC에서 원격 액세스 VPN을 구성하고 구축한 후에는 어떻게 됩니까?

FMC가 Smart License Cloud에 등록되어 있는지 확인합니다. 예상되는 동작은 FMC가 등록 취소되었거나 평가 모드인 경우 원격 액세스 컨피그레이션을 구축할 수 없다는 것입니다. FMC가 등록된 경우 AnyConnect 라이선스가 Smart Account에 있으며 디바이스에 할당되어 있는지 확인합니다.

라이선스를 할당하려면 탐색 수신 FMC Devices, 디바이스 선택, 라이선스(연필 아이콘). Smart Account에서 라이선스를 선택하고 저장.

오류가 발생한 이유 Remote Access VPN with SSL cannot be deployed when Export-Controlled Features (Strong-crypto) are disabled
원격 액세스 VPN 컨피그레이션을 구축하는 경우

FTD에 구축된 원격 액세스 VPN을 사용하려면 Strong Encryption 라이선스가 활성화되어야 합니다. EnFMC에서 Strong Encryption 라이선스가 활성화되어 있는지 확인합니다. Strong Encryption 라이선스의 상태를 확인하려면 탐색 에 대한 FMC System(FMC 시스템) > Licenses(라이선스) > Smart Licensing(스마트 라이선싱) 및 Export-Controlled Features가 활성화되어 있는지 확인합니다.

다음과 같은 경우 Strong Encryption 라이선스를 활성화하는 방법 Export-Controlled Features 비활성화되었습니까?

FMC를 Smart Account 클라우드에 등록하는 동안 사용되는 토큰에 이 토큰으로 등록된 제품에서 Allow export-controlled functionality(내보내기 제어 기능 허용) 옵션이 활성화된 경우 이 기능이 자동으로 활성화됩니다. 토큰에 이 옵션이 활성화되지 않은 경우 FMC를 등록 취소하고 이 옵션이 활성화된 상태로 다시 등록합니다.

토큰이 생성될 때 '이 토큰으로 등록된 제품에 대한 수출 통제 기능 허용' 옵션을 사용할 수 없는 경우 어떻게 할 수 있는가?

Cisco 어카운트 팀에 문의하십시오.

VPN 토폴로지 s2에 대한 Strong crypto(즉, DES보다 큰 암호화 알고리즘)가 지원되지 않음' 오류가 수신된 이유는 무엇입니까?

이 오류는 FMC에서 평가 모드를 사용하거나 Smart License Account에 Strong Encryption 라이선스가 없는 경우에 표시됩니다. VFMC가 License Authority에 등록되었는지 확인하고 이 토큰에 등록된 제품에 대한 수출 통제 기능 허용이 활성화됩니다. Smart Account에서 Strong Encryption 라이선스를 사용할 수 없는 경우, DES보다 강력한 암호를 사용하는 VPN Site-to-Site 컨피그레이션을 구축할 수 없습니다.

FMC에서 '컴플라이언스 위반' 상태가 수신된 이유는 무엇입니까?

관리되는 디바이스 중 하나가 사용할 수 없는 라이선스를 사용할 경우 디바이스가 규정 위반이 될 수 있습니다.

'규정 준수 위반' 상태를 수정하려면 어떻게 해야 합니까?

firepower 컨피그레이션 가이드에 설명된 단계를 수행합니다.

1. 페이지 하단의 Smart License 섹션을 참조하여 필요한 라이선스를 확인합니다.
2. 일반적인 채널을 통해 필요한 라이선스를 구매합니다.
3. Cisco Smart Software Manager(<https://software.cisco.com/#SmartLicensing-Inventory>), 라이선스가 가상 어카운트에 나타나는지 확인합니다.
4. FMC에서 System > Licenses > Smart Licenses를 선택합니다.

5. 재승인을 선택합니다.

전체 절차는 [Firepower 시스템](#) 라이선싱에서 [확인할 수 있습니다](#).

firepower Threat Defense Base의 기능은 무엇입니까?

Base 라이선스에서는 다음을 수행할 수 있습니다.

- 전환 및 라우팅할 FTD 디바이스 컨피그레이션(DHCP 릴레이 및 NAT 포함).
- HA(고가용성) 모드에서 FTD 디바이스 컨피그레이션.
- firepower 9300 쉐시 내 클러스터로 보안 모듈 구성(인트라 쉐시 클러스터).
- firepower 9300 또는 Firepower 4100 Series 장치(FTD)를 클러스터(쉐시 간 클러스터)로 구성합니다.
- 사용자 및 애플리케이션 제어 구성 및 액세스 제어 규칙에 사용자 및 애플리케이션 조건 추가

firepower Threat Defense 기본 기능 라이선스를 받으려면 어떻게 해야 합니까?

Base 라이선스는 Firepower Threat Defense 또는 Firepower Threat Defense 가상 디바이스를 구매할 때마다 자동으로 포함됩니다. FTD가 FMC에 등록되면 자동으로 Smart Account에 추가됩니다.

FMC와 Smart License Cloud 사이의 경로에서 어떤 IP 주소를 허용해야 합니까?

FMC는 IP 주소를 사용합니다 포트 443에서 Smart License Cloud와 통신할 수 있습니다.

해당 IP 주소(<https://tools.cisco.com>)이(가) 다음 IP 주소로 확인됩니다.

- 72.163.4.38
- 173.37.145.8

관련 정보

- [Firepower Management Center 컨피그레이션 가이드](#)
- [Cisco Live Smart Licensing 개요: BRKARC-2034](#)
- [Cisco Secure Firewall Management Center 기능 라이선스](#)
- [Cisco Smart Software Licensing 자주 묻는 질문\(FAQ\)](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.