

Use FMC and FTD Smart License Registration and Common Issues to Troubleshoot

Contents

- [Introduction](#)
- [Prerequisites](#)
- [Requirements](#)
- [Components Used](#)
- [Background Information](#)
- [FMC Smart License Registration](#)
- [Prerequisites](#)
- [FMC Smart License Registration](#)
- [Confirmation in Smart Software Manager \(SSM\) Side](#)
- [FMC Smart License De-Registration](#)
- [RMA](#)
- [Troubleshoot](#)
- [Common Issues](#)
- [Case Study 1. Invalid Token](#)
- [Case Study 2. Invalid DNS](#)
- [Case Study 3. Invalid Time Values](#)
- [Case study 4. No Subscription](#)
- [Case study 5. Out-of-Compliance \(OOC\)](#)
- [Case study 6. No Strong Encryption](#)
- [Additional Notes](#)
- [Set Notification of Smart License State](#)
- [Get Health Alert Notifications from the FMC](#)
- [Multiple FMCs on the Same Smart Account](#)
- [FMC Must Maintain Internet Connectivity](#)
- [Deploy Multiple FMCv](#)
- [Frequently Asked Questions \(FAQs\)](#)
- [Related Information](#)

Introduction

This document describes the Smart License registration configuration of Firepower Management Center on Firepower Threat Defense-managed devices.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

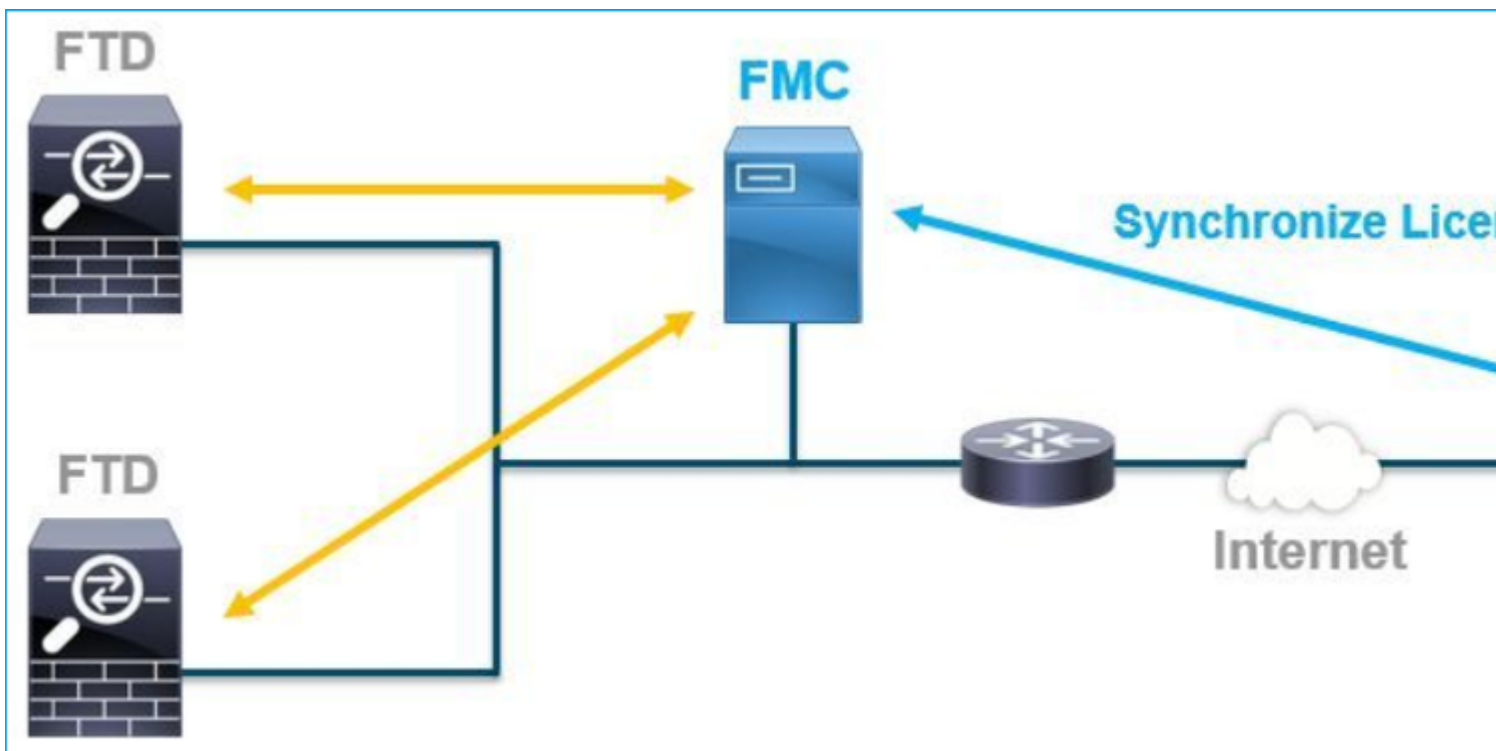
The information in this document was created from the devices in a specific lab environment. All of the

devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

FMC, FTD, and Smart License registration.

Smart License registration is performed on the Firepower Management Center (FMC). The FMC communicates with the Cisco Smart Software Manager (CSSM) portal over the internet. In the CSSM, the firewall administrator manages the Smart Account and its licenses. The FMC can freely assign and delete licenses to the managed Firepower Threat Defense (FTD) devices. In other words, the FMC centrally manages licenses for FTD devices.



An additional license is required to use certain features of FTD devices. The Smart License types customers can assign to an FTD device are documented in [FTD License Types and Restrictions](#).

The Base license is included in the FTD device. This license is automatically registered in your Smart Account when the FMC is registered to CSSM.

The term-based licenses: Threat, Malware, and URL Filtering are optional. To use features related to a license, a license needs to be assigned to the FTD device.

To use a Firepower Management Center Virtual (FMCv) for the FTD management, a **Firepower MCv Device License** in CSSM is also needed for the FMCv.

The FMCv license is included in the software, and it is perpetual.

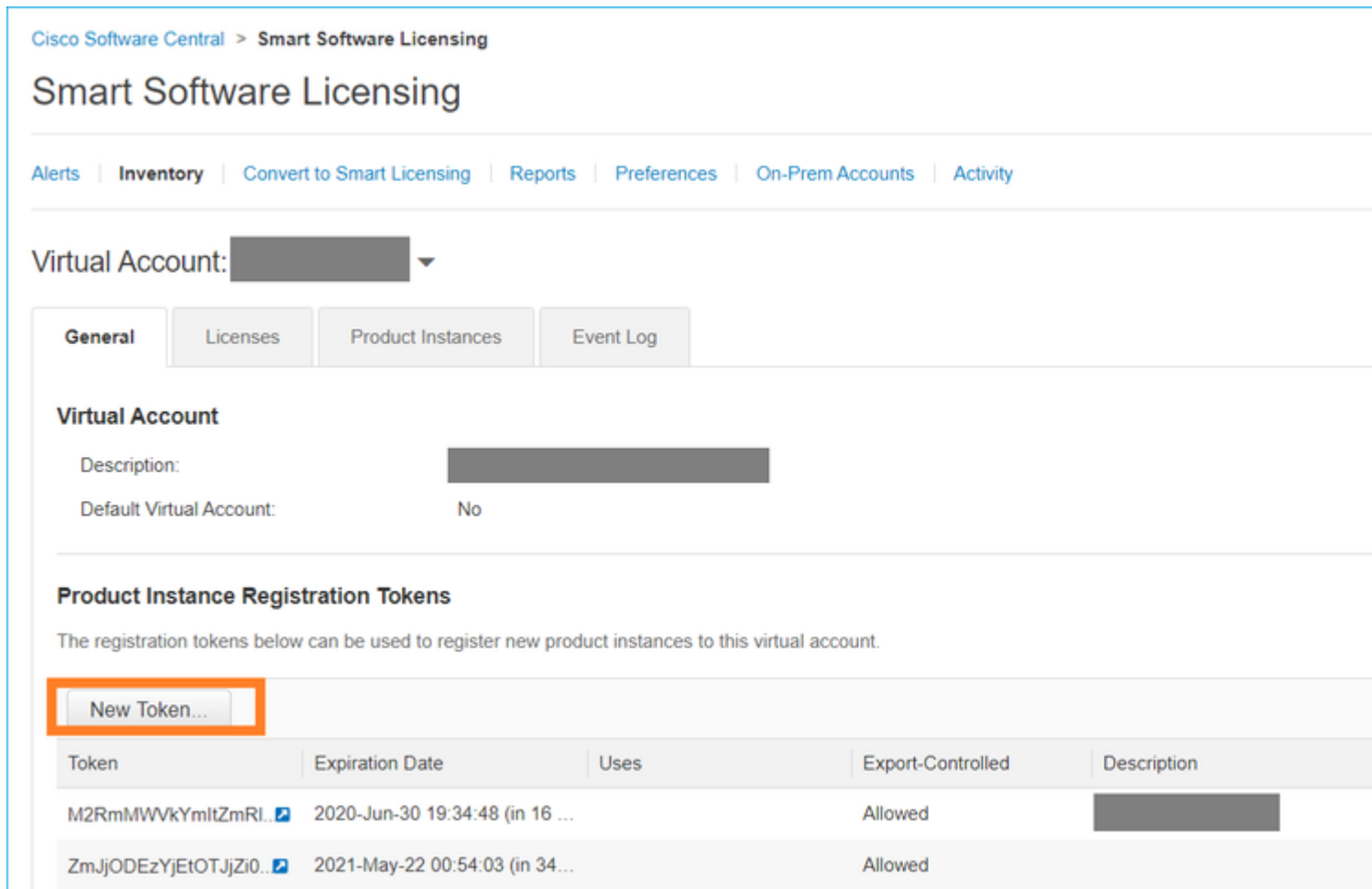
Additionally, scenarios are provided in this document to help troubleshoot common license registration errors that can occur.

For more details about licenses check [Cisco Firepower System Feature Licenses](#) and [Frequently Asked Questions \(FAQ\) about Firepower Licensing](#).

FMC Smart License Registration

Prerequisites

1. For Smart License registration, the FMC must access the internet. Because the certificate is exchanged between the FMC and the Smart License Cloud with HTTPS, ensure there is no device in the path that can affect/modify the communication. (for example, Firewall, Proxy, SSL Decryption device, and so on).
2. Access the CSSM and issue a Token ID from **Inventory > General > New Token** button, as shown in this image.



To use strong encryption, enable the **Allow export-controlled functionality on the products registered with this token** option. When enabled, a checkmark displays in the check box.

3. Select **Create Token**.

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 License Registration

Navigate to the **System > Licenses > Smart Licenses** on the FMC, and select the **Register** button, as shown in this image.

**Firepower Management Center**

System / Licenses / Smart Licenses

OverviewAnalysisPoliciesDevicesObjectsAMP

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:	--

Enter the Token ID in the Smart Licensing Product Registration window and select **Apply Changes**, as shown in this image.

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

If the Smart License registration was successful, the Product Registration status shows **Registered**, as shown in this image.

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)		

To assign a term-based license to the FTD device, select **Edit Licenses**. Then select and add a managed device to the Devices with license section. Finally, select the **Apply** button as shown in this image.

Edit Licenses

Malware

Threat

URL Filtering

AnyConnect Apex

AnyConnect Plus

AnyConnect VPN Only

Devices without license

Search

FTD

Add

Devices with license (1)

FTD

1

2

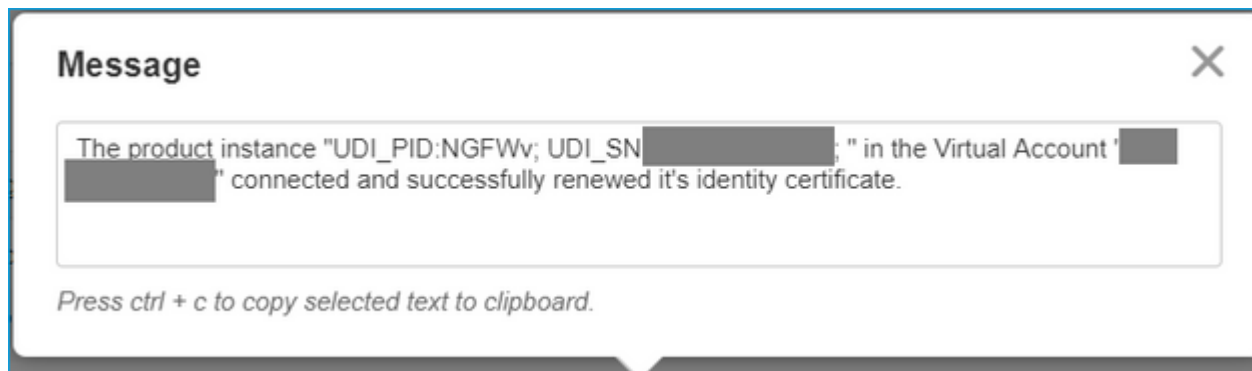
3

Cancel

Apply

Confirmation in Smart Software Manager (SSM) Side

The success of the FMC Smart License registration can be confirmed from **Inventory > Event Log** in CSSM, as shown in this image.

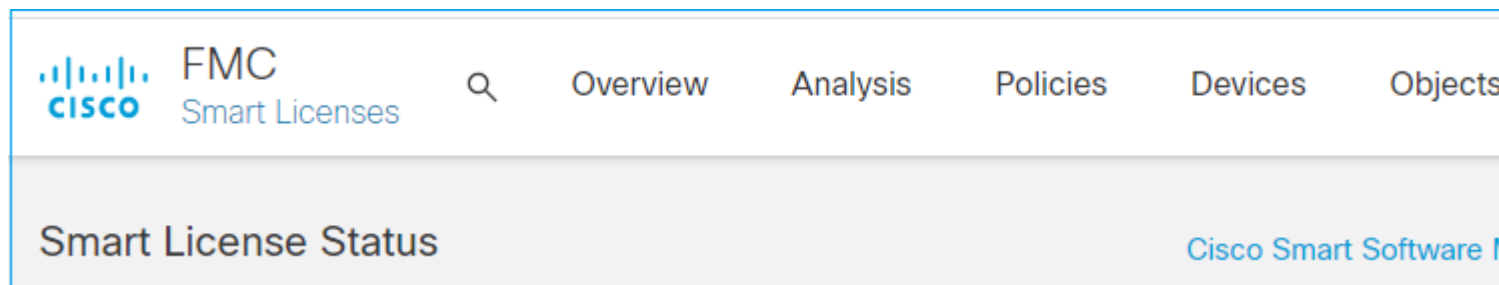


The registration status of the FMC can be confirmed from **Inventory > Product Instances**. Check the event log from the **Event Log** tab. Smart License registration and use status can be checked from the **Inventory > Licenses** tab. Verify the term-based license purchased is used correctly and there are no Alerts that indicate insufficient licenses.

FMC Smart License De-Registration

De-register the FMC from the Cisco SSM

To release the license for some reason or use a different token, navigate to **System > Licenses > Smart Licenses** and select the de-register button, as shown in this image.



Remove Registration from SSM Side

Access the Smart Software Manager ([Cisco Smart Software Manager](#)) and from the **Inventory > Product Instances**, select **Remove** on the target FMC. Then select **Remove Product Instance** to remove the FMC and release the allocated licenses, as shown in this image.


Cisco Software Central > Smart Software Licensing

Smart Software Licensing


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

Virtual Account: XXXXXXXXXX

General Licenses **Product Instances** Event Log

Authorize License-Enforced Features...  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

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

If the FMC is RMA'd, de-register the FMC from Cisco Smart Software Manager (CSSM) using the steps in section **FMC Smart License De-Registration > Remove Registration from SSM Side** and then re-register the FMC with CSSM using the steps in section **FMC Smart License Registration**.

Troubleshoot

Time Synchronization Verification

Access the FMC CLI (for example, SSH) and ensure the time is correct and it is synchronized with a trusted NTP server. Because the certificate is used for Smart License authentication, it is important that the FMC has the correct time information:

<#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

From the FMC UI, verify the NTP server values from **System > Configuration > Time Synchronization**.

Enable Name Resolution and Check Reachability to tools.cisco.com

Ensure the FMC can resolve an FQDN and has reachability to 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
```

From the FMC UI, verify the management IP and DNS server IP from **System > Configuration > Management Interfaces**.

Verify HTTPS (TCP 443) access from FMC to tools.cisco.com

Use Telnet or curl command to ensure the FMC has HTTPS access to tools.cisco.com. If the TCP 443 communication is broken, verify it is not blocked by a firewall and there is no SSL decryption device in the path.

```
<#root>
```

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

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

```
Trying 72.163.4.38...
```

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

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

<--- Press Ctrl+C

Curl test:

<#root>

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

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

*

Trying 72.163.4.38...

* TCP_NODELAY set

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

* ALPN, offering http/1.1

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

* successfully set certificate verify locations:

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

CAPath: none

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

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

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

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

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

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

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

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

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

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

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

* ALPN, server accepted to use http/1.1

* Server certificate:

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

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

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

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

* SSL certificate verify ok.

> GET / HTTP/1.1

> Host: tools.cisco.com

> User-Agent: curl/7.62.0

> Accept: */*

>

< HTTP/1.1 200 OK

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

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

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

< Accept-Ranges: bytes

< Content-Length: 337

< Access-Control-Allow-Credentials: true

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

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

< Content-Type: text/html

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

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

```

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

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

</script>
</head>

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

```

DNS Verification

Verify successful resolve to 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 Verification

If apProxy is used, check the values on both the FMC and the proxy server-side. On the FMC, check if the FMC uses the correct proxy server IP and port.

```

<#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 the FMC UI, the proxy values can be confirmed from **System > Configuration > Management Interfaces**.

If the FMC-side values are correct, check the proxy server-side values (for example, if the proxy server permits access from the FMC and to tools.cisco.com. Additionally, permit traffic and certificate exchange through the proxy. The FMC uses a certificate for the Smart License registration).

Expired Token ID

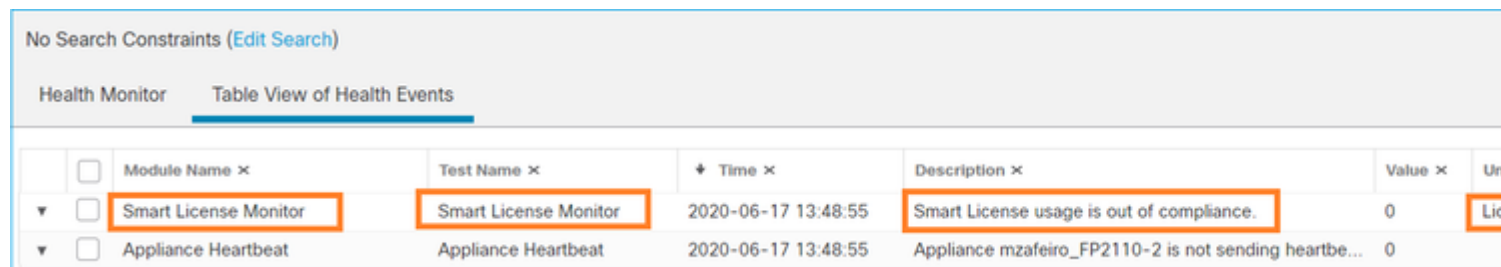
Verify the issued token ID is not expired. If it is expired, ask the Smart Software Manager administrator to issue a new token and re-register the Smart License with the new Token ID.

Change the FMC Gateway

There can be cases where Smart License authentication cannot be performed correctly due to the effects of a relay proxy or SSL decryption device. If possible, change the route for the FMC internet access to avoid these devices, and retry the Smart License registration.

Check the Health Events on FMC

On the FMC, navigate to **System > Health > Events** and check the status of the Smart License Monitor module for errors. For example, if the connection fails due to an expired certificate; an error, such as **id certificated expired** is generated, as shown in this image.



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

Check the Event Log on the SSM Side

If the FMC can connect to the CSSM, check the event log of the connectivity in **Inventory > Event Log**. Check if there are such event logs or error logs in the CSSM. If there is no problem with the values/operation of the FMC site, and there is no event log on the CSSM side, there is a possibility it is a problem with the route between the FMC and the CSSM.

Common Issues

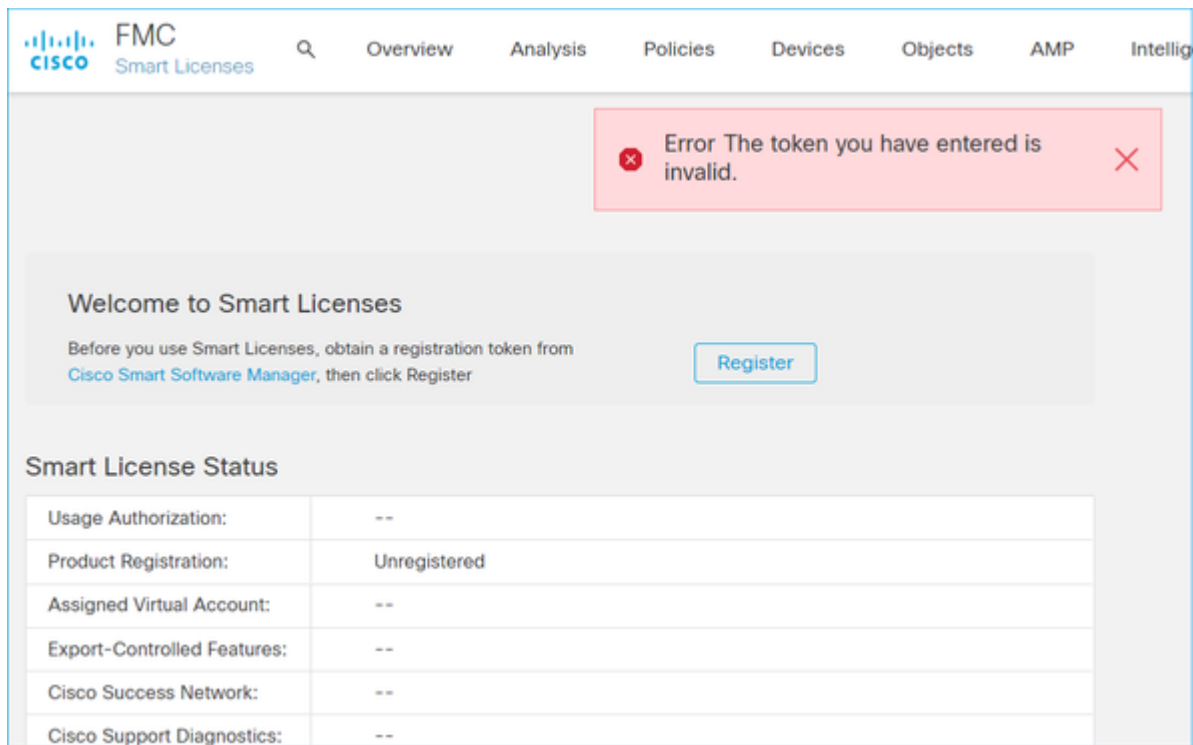
Summary of Registration and Authorization States:

Product Registration State	Usage Authorization State	Comments

Unregistered	--	The FMC is in neither Registered nor Evaluation mode. This is the initial state after FMC installation or after 90-day Evaluation License Expiration.
Registered	Authorized	The FMC is registered with the Cisco Smart Software Manager (CSSM) and there are FTD devices registered with a valid subscription.
Registered	Authorization Expired	The FMC failed to communicate with the Cisco License backend for more than 90 days.
Registered	Unregistered	The FMC is registered with the Cisco Smart Software Manager (CSSM), but there are no FTD devices registered on the FMC.
Registered	Out-of-Compliance	<p>The FMC is registered with the Cisco Smart Software Manager (CSSM), but there are FTD devices registered with an invalid subscription(s).</p> <p>For example, an FTD (FP4112) device uses THREAT subscription, but with the Cisco Smart Software Manager (CSSM) there are no THREAT subscriptions available for FP4112.</p>
Evaluation (90 days)	N/A	The evaluation period is in use, but there are no FTD devices registered on the FMC.

Case Study 1. Invalid Token

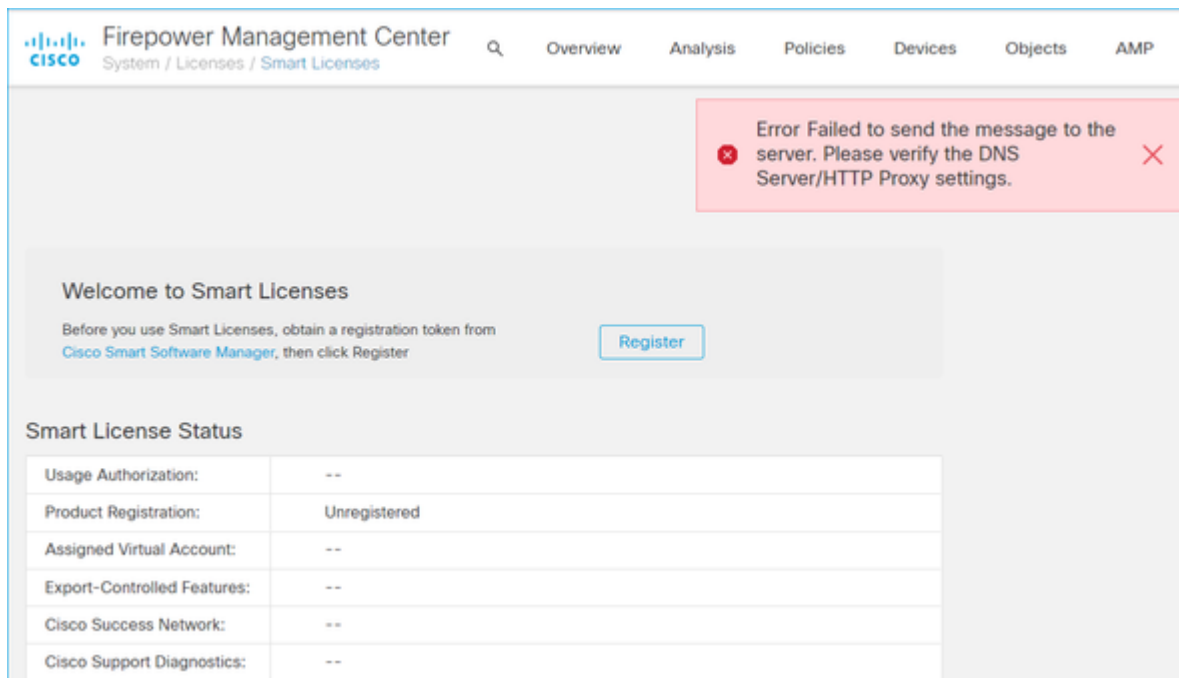
Symptom: Registration to the CSSM fails quickly (~10s) due to invalid token, as shown in this image.



Resolution: Use a valid token.

Case Study 2. Invalid DNS

Symptom: Registration to the CSSM failed after a while (~25s), as shown in this image.



Check the /var/log/process_stdout.log file. The DNS issue is seen:

```
<#root>
```

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

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

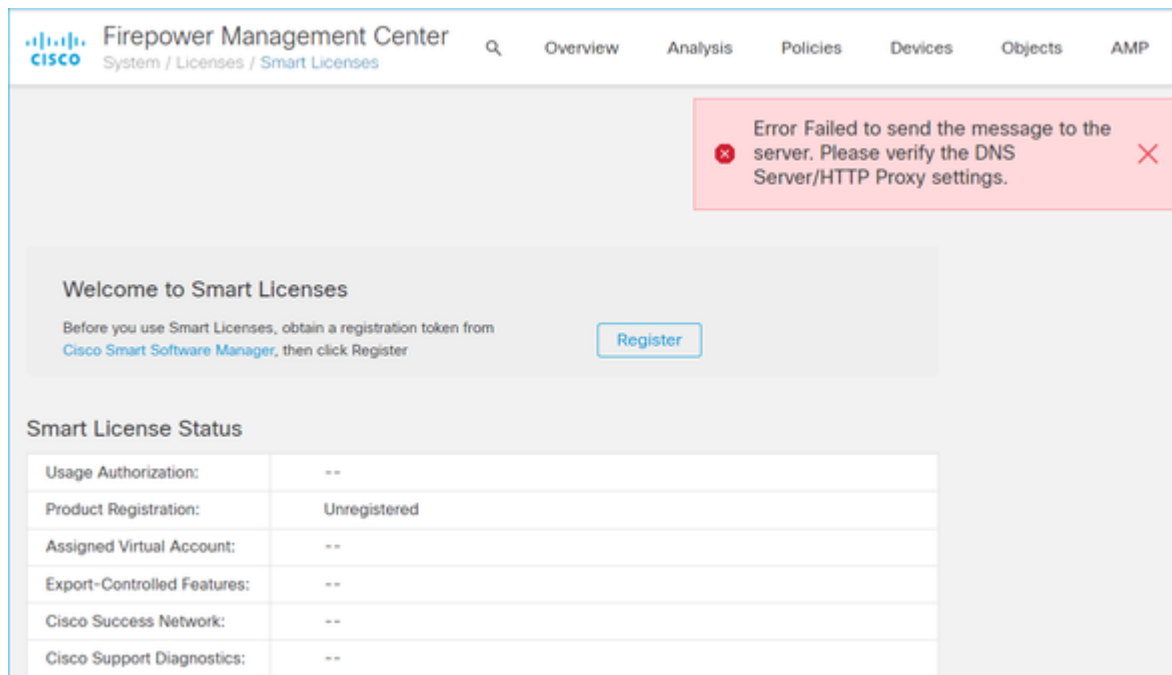
```
2020-06-25 09:05:21 sla[24043]: *Thu Jun 25 09:05:10.989 UTC: CH-LIB-ERROR: ch_pf_curl_send_msg[494],
failed to perform, err code 6, err string

"Couldn't resolve host name"
```

Resolution: CSSM hostname resolution failure. The resolution is to configure DNS, if not configured, or fix the DNS issues.

Case Study 3. Invalid Time Values

Symptom: Registration to the CSSM failed after a while (~25s), as shown in this image.



Check the `/var/log/process_stdout.log` file. The certificate issues are seen:

<#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
```

Check the FMC time value:

<#root>

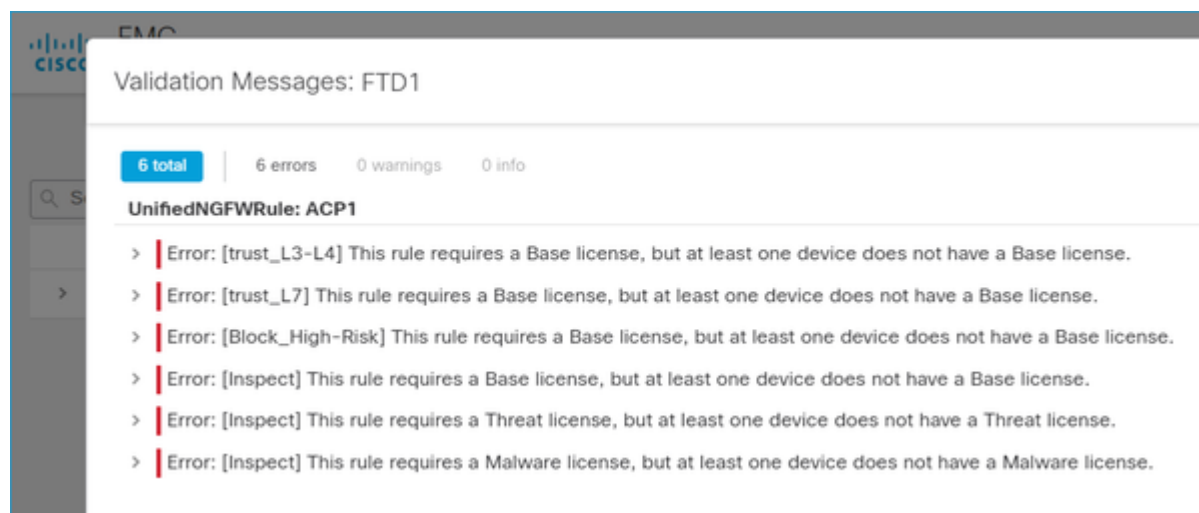
```
root@FMC2000-2:/Volume/home/admin#
```

```
date
```

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

Case study 4. No Subscription

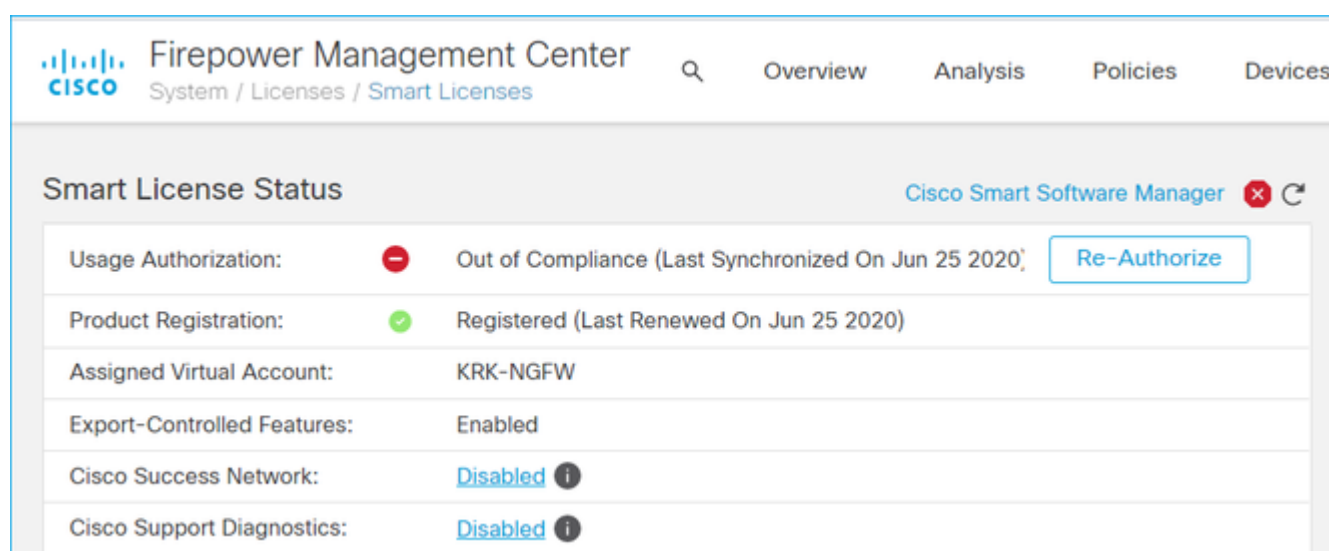
If there is no license subscription for a specific feature, the FMC deployment is not possible:



Resolution: There is a need to purchase and apply the required subscription to the device.

Case study 5. Out-of-Compliance (OOC)

If there is no entitlement for FTD subscriptions, the FMC Smart License goes to the out-of-compliance (OOC) state:



In the CSSM, check the Alerts for errors:

<div>General</div> <div>Licenses</div> <div>Product Instances</div> <div>Event Log</div>							
Available Actions ▾		Manage License Tags		License Reservation...		<div>By Name</div> <div>By T</div>	
						Search by License	
<input type="checkbox"/>	License	Billing	Purchased	In Use	Balance	Alerts	Actions
<input type="checkbox"/>	FPR4110 Threat Defense Threat Protection	Prepaid	75	2	+ 73		Actions
<input type="checkbox"/>	FPR4110 Threat Defense URL Filtering	Prepaid	75	0	+ 75		Actions
<input type="checkbox"/>	FPR4115 Threat Defense Malware Protection	Prepaid	0	1	-1	✖ Insufficient Licenses	Actions
<input type="checkbox"/>	FPR4115 Threat Defense Threat Protection	Prepaid	0	1	-1	✖ Insufficient Licenses	Actions
<input type="checkbox"/>	FPR4115 Threat Defense URL Filtering	Prepaid	0	1	-1	✖ Insufficient Licenses	Actions
<input type="checkbox"/>	FPR4120 Threat Defense Malware Protection	Prepaid	75	0	+ 75		Actions
<input type="checkbox"/>	FPR4120 Threat Defense Threat Protection	Prepaid	75	0	+ 75		Actions

Case study 6. No Strong Encryption

If only the Base License is used, Data Encryption Standard (DES) encryption is enabled in the FTD LINA engine. In that case, deployments like L2L Virtual Private network (VPN) with stronger algorithms fail:

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.

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	ⓘ
Cisco Support Diagnostics:	Disabled	ⓘ

Resolution: Register the FMC to the CSSM and have a Strong Encryption attribute enabled.

Additional Notes

Set Notification of Smart License State

Email Notification by SSM

On the SSM side, SSM Email Notification allows reception of summary emails for various events. For example, notification for a lack of license or for licenses that are about to expire. Notifications of product instance connection or of update failure can be received.

This function is very useful to notice and prevent the occurrence of functional restrictions due to license expiration.

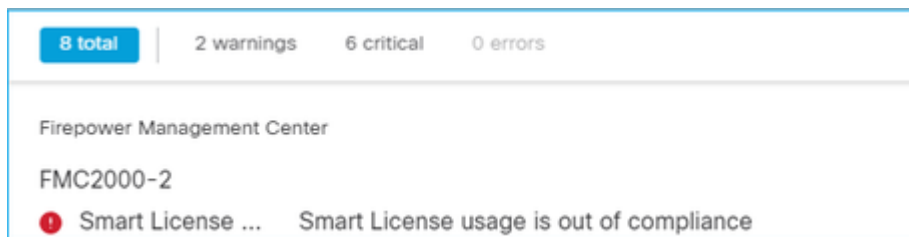
Get Health Alert Notifications from the FMC

On the FMC side, it is possible to configure a Health Monitor Alert and receive an alert notification of a health event. The Module Smart License Monitor is available to check the Smart License status. The monitor alert supports Syslog, Email, and SNMP trap.

This is a configuration example to get a Syslog message when a Smart License monitor event occurs:

The screenshot shows 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', and 'Devices' are visible. The main content area is titled 'Configure Health Alerts' and is divided into two sections. On the left, under 'Active Health Alerts', there is an empty box. On the right, the configuration fields are: 'Health Alert Name' with the value 'Smart-License-Syslog-Alert'; 'Severity' with a dropdown menu showing 'Critical' (selected), 'Warning', 'Normal', 'Error', and 'Recovered'; and 'Module' with a dropdown menu showing 'Realm', 'Reconfiguring Detection', 'Security Intelligence', 'Smart License Monitor' (selected), 'Snort Identity Memory Usage', 'Threat Data Updates on Devic...', 'Time Series Data Monitor', 'Time Synchronization Status', 'URL Filtering Monitor', 'User Agent Status Monitor', and 'VPN Status'.

This is an example of a Health Alert:



The Syslog message generated by the FMC is:

<#root>

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

HMNOTIFY: Smart License Monitor (Sensor FMC)

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

Refer to the [Health Monitoring](#) for additional details about the Health Monitor Alerts.

Multiple FMCs on the Same Smart Account

When multiple FMCs are used on the same Smart Account, each FMC hostname must be unique. When multiple FMCs in CSSM are managed, to distinguish each FMC, the hostname of the each FMC must be unique. This is useful for FMC Smart License maintenance in operation.

FMC Must Maintain Internet Connectivity

After registration, the FMC checks the Smart License Cloud and license status every 30 days. If the FMC cannot communicate for 90 days, the licensed function is maintained, but it remains in **Authorization Expired** status. Even in this state, the FMC tries continuously to connect to the Smart License Cloud.

Deploy Multiple FMCv

When the Firepower System is used in a virtual environment, clone (hot or cold) is not officially supported. Each Firepower Management Center virtual (FMCv) is unique because it has authentication information inside. To deploy multiple FMCv, the FMCv must be created from the Open Virtualization Format (OVF) file one at a time. For more information about this limitation, refer to the [Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide](#).

Frequently Asked Questions (FAQs)

In FTD HA, how many device licenses are required?

When two FTDs are used in High Availability, a license is required for each device. For example, two Threat and Malware licenses are needed if the Intrusive Protection System (IPS) and Advanced Malware Protection (AMP) feature are used on the FTD HA pair.

Why are no AnyConnect licenses used by FTD?

After FMC registration to the Smart Account, ensure the AnyConnect License is enabled. To enable the license, navigate to **FMC > Devices**, choose your device, and select **License**. Select the **Pencil** icon, choose

the license that is deposited in the Smart Account, and select **Save**.

Why is only one AnyConnect license 'In Use' in the Smart Account when 100 users are connected?

This is expected behavior, as Smart Account tracks the number of devices that have this license enabled, not active users connected.

Why is there the error Device does not have the AnyConnect License after configuration and deployment of a Remote Access VPN by the FMC?

Ensure the FMC is registered to the Smart License Cloud. The expected behavior is Remote Access configuration cannot be deployed when the FMC is unregistered or in Evaluation mode. If the FMC is registered, ensure the AnyConnect License exists in your Smart Account and it is assigned to the device.

To assign a license, navigate to **FMC Devices**, select your device, **License** (Pencil icon). Choose the license in the Smart Account and select **Save**.

Why is there the error Remote Access VPN with SSL cannot be deployed when Export-Controlled Features (Strong-crypto) are disabled when there is a deployment of a Remote Access VPN configuration?

The Remote Access VPN deployed on the FTD requires a Strong Encryption license to be enabled. Ensure a Strong Encryption license is enabled on the FMC. To check the status of the Strong Encryption license, navigate to the FMC **System > Licenses > Smart Licensing** and verify Export-Controlled Features are enabled.

How to enable a Strong Encryption License if Export-Controlled Features is disabled?

This functionality is enabled automatically if the token used during the registration of the FMC to the Smart Account Cloud has the option **Allow export-controlled functionality on the products registered with this token** enabled. If the token does not have this option enabled, de-register the FMC and register it again with this option enabled.

What can be done if the option 'Allow export-controlled functionality on the products registered with this token' is not available when the token is generated?

Contact your Cisco Account team.

Why is the error 'Strong crypto (that is, encryption algorithm greater than DES) for VPN topology s2s is not supported' received?

This error is displayed when the FMC uses Evaluation mode or the Smart License Account is not entitled to a Strong Encryption license. Verify the FMC is registered to the License Authority and **Allow export-controlled functionality on the products registered with this token** is enabled. If the Smart Account is not allowed to use a Strong Encryption license, deployment of VPN Site-to-Site configuration with ciphers stronger than DES is not allowed.

Why is an 'Out of Compliance' status on the FMC received?

The device can become out of compliance when one of the managed devices uses unavailable licenses.

How can the 'Out of Compliance' status be corrected?

Follow the steps described in the Firepower Configuration Guide:

1. Look at the Smart Licenses section at the bottom of the page to determine which licenses are needed.
2. Purchase the required licenses through your usual channels.
3. In Cisco Smart Software Manager (<https://software.cisco.com/#SmartLicensing-Inventory>), verify the licenses appear in your virtual account.
4. In the FMC, select **System > Licenses > Smart Licenses**.
5. Select **Re-Authorize**.

The full procedure can be found in [Licensing the Firepower System](#).

What are the Firepower Threat Defense Base features?

The Base license allows:

- Configuration of FTD devices to switch and route (which includes DHCP Relay and NAT).
- Configuration of FTD devices in a high availability (HA) mode.
- Configuration of security modules as a cluster within a Firepower 9300 chassis (intra-chassis cluster).
- Configuration of Firepower 9300 or Firepower 4100 series devices (FTD) as a cluster (inter-chassis cluster).
- Configuration of user and application control and addition of user and application conditions to access control rules.

How can the Firepower Threat Defense Base Features License be obtained?

A Base license is automatically included with every purchase of a Firepower Threat Defense or Firepower Threat Defense Virtual device. It is automatically added to your Smart Account when FTD registers to the FMC.

Which IP addresses must be allowed in the path between the FMC and the Smart License Cloud?

The FMC uses the IP address on port 443 to communicate with the Smart License Cloud.

That IP address (<https://tools.cisco.com>) is resolved to these IP addresses:

- 72.163.4.38
- 173.37.145.8

Related Information

- [Firepower Management Center Configuration Guides](#)
- [Cisco Live Smart Licensing Overview: BRKARC-2034](#)
- [Cisco Secure Firewall Management Center Feature Licenses](#)
- [Cisco Smart Software Licensing Frequently Asked Questions \(FAQs\)](#)