

Utilice FMC y FTD Registro de licencia inteligente y problemas comunes para resolver problemas

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Registro de licencia inteligente FMC](#)

[Prerequisites](#)

[Registro de licencia inteligente FMC](#)

[Confirmación en el lado de Smart Software Manager \(SSM\)](#)

[Cancelación del registro de la licencia inteligente FMC](#)

[RMA](#)

[Troubleshoot](#)

[Problemas comunes](#)

[Caso Práctico 1. Token no válido](#)

[Caso Práctico 2. DNS no válido](#)

[Caso Práctico 3. Valores de tiempo no válidos](#)

[Caso Práctico 4. Sin suscripción](#)

[Caso Práctico 5. Incumplimiento \(OOC\).](#)

[Caso Práctico 6. Sin cifrado seguro](#)

[Notas complementarias](#)

[Establecer la notificación del estado de la licencia inteligente](#)

[Obtener notificaciones de alertas de estado del FMC](#)

[Varios CSP en la misma cuenta inteligente](#)

[FMC debe mantener la conectividad a Internet](#)

[Implementación de varios FMCv](#)

[Preguntas más frecuentes \(FAQ\)](#)

[Información Relacionada](#)

Introducción

Este documento describe la configuración de registro de licencia inteligente de Firepower Management Center en dispositivos administrados con Firepower Threat Defence.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

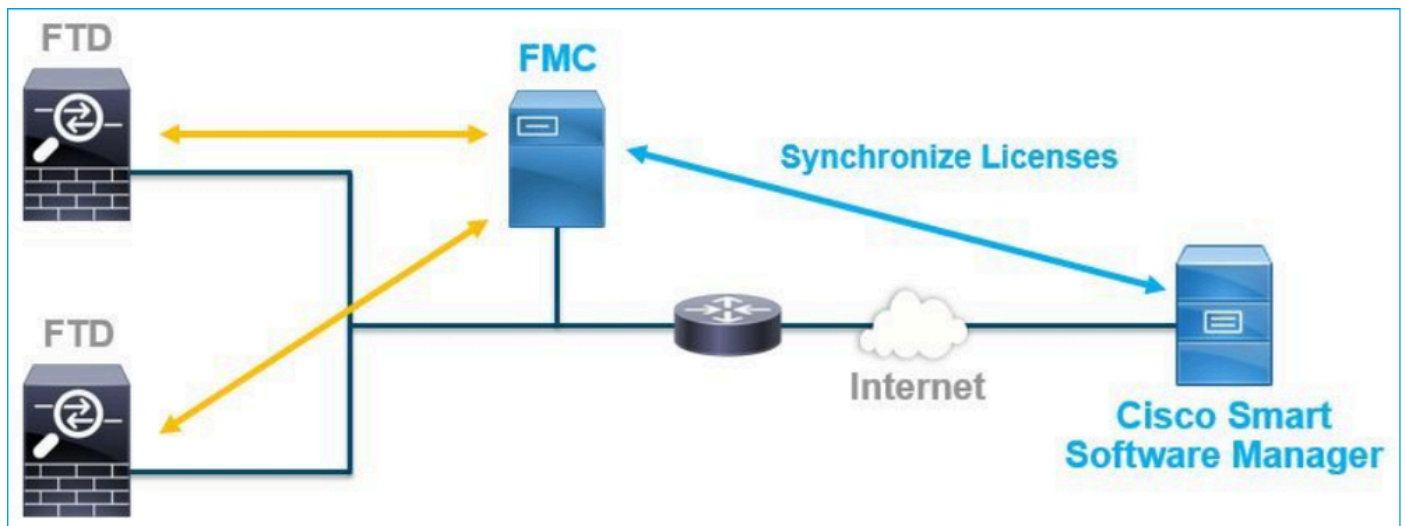
Componentes Utilizados

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Registro en FMC, FTD y Smart License.

El registro de Smart License se realiza en Firepower Management Center (FMC). El FMC se comunica con el portal Cisco Smart Software Manager (CSSM) a través de Internet. En el CSSM, el administrador del firewall administra la cuenta inteligente y sus licencias. El FMC puede asignar y eliminar licencias libremente a los dispositivos Firepower Threat Defence (FTD) administrados. En otras palabras, el FMC gestiona de forma centralizada las licencias de los dispositivos FTD.



Se necesita una licencia adicional para utilizar ciertas funciones de los dispositivos FTD. Los tipos de licencia inteligente que los clientes pueden asignar a un dispositivo FTD se documentan en [Tipos y restricciones de licencia FTD](#).

La licencia básica se incluye en el dispositivo FTD. Esta licencia se registra automáticamente en su cuenta Smart Account cuando el CSM está registrado en CSSM.

Las licencias basadas en plazos: Amenazas, malware y filtrado de URL son opcionales. Para utilizar funciones relacionadas con una licencia, es necesario asignar una licencia al dispositivo FTD.

Para utilizar Firepower Management Center Virtual (FMCv) para la gestión de FTD, también se necesita una licencia de dispositivo Firepower MCv en CSSM para FMCv.

La licencia de FMCv se incluye en el software y es perpetua.

Además, en este documento se proporcionan escenarios para ayudar a resolver los errores comunes de registro de licencias que pueden ocurrir.

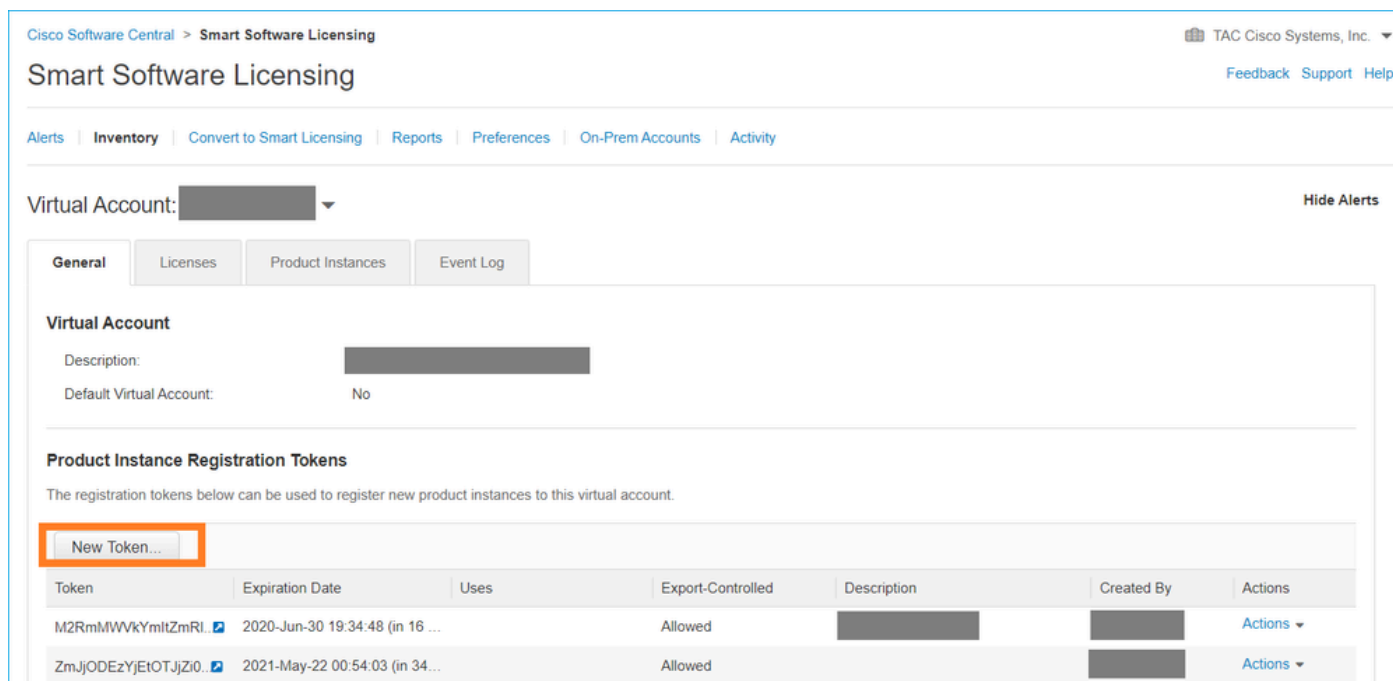
Para obtener más información sobre las licencias, consulte [Cisco Firepower System Feature Licenses](#) y [Preguntas frecuentes \(FAQ\) sobre Firepower Licensing](#).

Registro de licencia inteligente FMC

Prerequisites

1. Para el registro de la licencia inteligente, el CSP debe acceder a Internet. Dado que el certificado se intercambia entre el FMC y la nube de licencias inteligentes con HTTPS, asegúrese de que no haya ningún dispositivo en la ruta que pueda afectar/modificar la comunicación. (por ejemplo, Firewall, Proxy, dispositivo de descifrado SSL, etc.).

2. Acceda al CSSM y emita un ID de token desde el botón Inventory > General > New Token, como se muestra en esta imagen.



The screenshot shows the Cisco Software Central interface for Smart Software Licensing. The page title is "Smart Software Licensing" and it includes navigation tabs for Alerts, Inventory, Convert to Smart Licensing, Reports, Preferences, On-Prem Accounts, and Activity. A "Virtual Account" dropdown is visible. Below the tabs, there are sections for "Virtual Account" (Description, Default Virtual Account) and "Product Instance Registration Tokens". A "New Token..." button is highlighted with a red box. Below this button is a table of existing tokens.

Token	Expiration Date	Uses	Export-Controlled	Description	Created By	Actions
M2RmMWVkymltZmRI...	2020-Jun-30 19:34:48 (in 16 ...)		Allowed			Actions
ZmJjODEzYjEOTjJzO...	2021-May-22 00:54:03 (in 34...)		Allowed			Actions

Para utilizar un cifrado avanzado, habilite la función Permitir control de exportación en los productos registrados con esta opción de token. Cuando está activada, aparece una marca de verificación en la casilla de verificación.

3. Seleccione Crear 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

Registro de licencia inteligente FMC

Navegue hasta System > Licenses > Smart Licenses en el FMC y seleccione el botón Register, como se muestra en esta imagen.

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:	--

Ingrese el ID de token en la ventana Registro de productos de Smart Licensing y seleccione Aplicar cambios, como se muestra en esta imagen.

Smart Licensing Product Registration

Product Instance Registration Token:

OWI4Mzc5MTAtNzQwYi00YTVILTkyNTktMGMxNGJIYmRmNDUwLTE1OTQ3OTQ5%
0ANzc3ODB8SnVXc2tPaks4SE5Jc25xTDkySnFYempTZnJEWVdVQU1SU1NiOWFM

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

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

Cisco Success Network

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

Enable Cisco Success Network

Cisco Support Diagnostics

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

Internet connection is required.

Cancel

Apply Changes

Si el registro de Smart License se realizó correctamente, el estado de registro del producto muestra Registered, como se muestra en esta imagen.

Smart License 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

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

Para asignar una licencia basada en plazos al dispositivo FTD, seleccione Edit Licenses. A continuación, seleccione y agregue un dispositivo administrado a la sección Dispositivos con licencia. Finalmente, seleccione el botón Apply como se muestra en esta imagen.

Edit Licenses

Malware Threat URL Filtering AnyConnect Apex AnyConnect Plus AnyConnect VPN Only

Devices without license

Search

FTD

Add

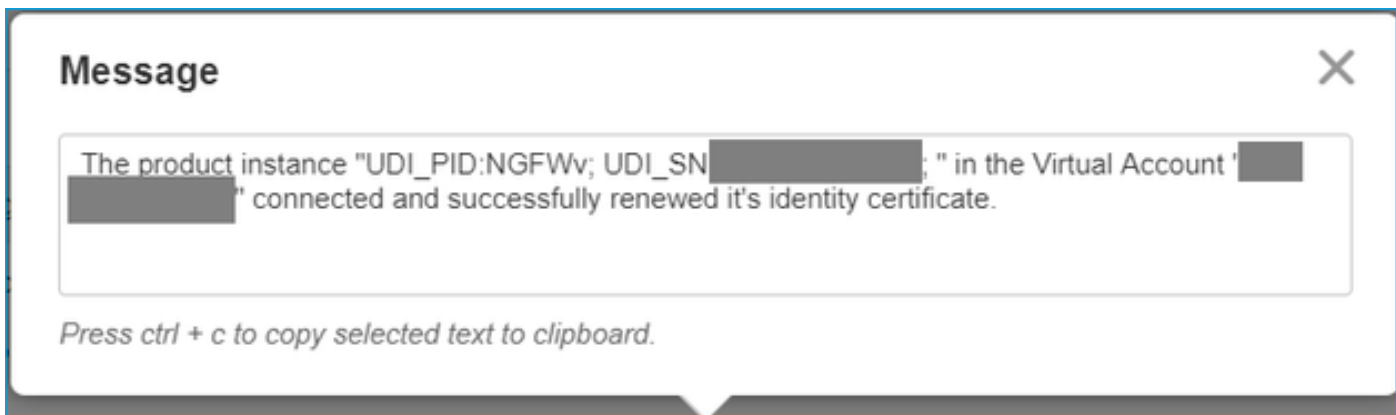
Devices with license (1)

FTD

Cancel Apply

Confirmación en el lado de Smart Software Manager (SSM)

El éxito del registro de FMC Smart License se puede confirmar en Inventory > Event Log en CSSM, como se muestra en esta imagen.

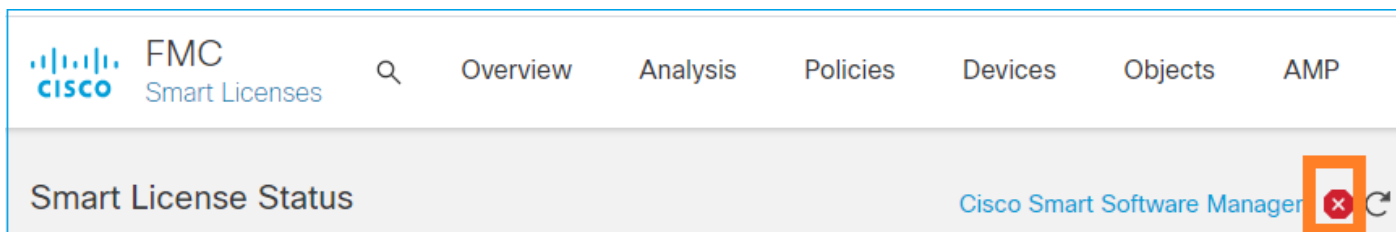


El estado de registro del CSP se puede confirmar en Inventario > Instancias de productos. Compruebe el registro de eventos en la ficha Registro de eventos. El registro de Smart License y el estado de uso se pueden comprobar en la pestaña Inventory > Licenses. Verifique que la licencia basada en plazos adquirida se utilice correctamente y que no haya alertas que indiquen licencias insuficientes.

Cancelación del registro de la licencia inteligente FMC

Anulación del registro del FMC del Cisco SSM

Para liberar la licencia por algún motivo o utilizar un token diferente, navegue hasta System > Licenses > Smart Licenses y seleccione el botón de anular registro, como se muestra en esta imagen.



Eliminar registro del lado SSM

Acceda a Smart Software Manager ([Cisco Smart Software Manager](#)) y en Inventario > Instancias de productos, seleccione Eliminar en el FMC de destino. A continuación, seleccione Remove Product Instance para eliminar el FMC y liberar las licencias asignadas, como se muestra en esta imagen.

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... [Icon] fmcv [X] [Q]

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

Si se devuelve el FMC, anule su registro en Cisco Smart Software Manager (CSSM) siguiendo los pasos de la sección Anulación del registro de licencia inteligente de FMC > Eliminar registro del lado de SSM y, a continuación, vuelva a registrar el FMC con CSSM siguiendo los pasos de la sección Registro de licencia inteligente de FMC.

Troubleshoot

Verificación de sincronización horaria

Acceda a la CLI de FMC (por ejemplo, SSH) y asegúrese de que la hora es correcta y de que está sincronizada con un servidor NTP de confianza. Dado que el certificado se utiliza para la autenticación de Smart License, es importante que el FMC tenga la información horaria correcta:

```
<#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

Desde la interfaz de usuario de FMC, verifique los valores del servidor NTP desde System > Configuration > Time Synchronization .

Habilite la resolución de nombres y compruebe la disponibilidad en tools.cisco.com (smartreceiver.cisco.com de FMC 7.3+)

Asegúrese de que el FMC puede resolver un FQDN y de que puede acceder a tools.cisco.com (smartreceiver.cisco.com) a partir de FMC 7.3 según la [ID de error de Cisco CSCwj95397](#)

```
<#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
```

Desde la interfaz de usuario de FMC, verifique la IP de administración y la IP del servidor DNS desde System > Configuration > Management Interfaces .

Verifique el acceso HTTPS (TCP 443) desde FMC a tools.cisco.com (smartreceiver.cisco.com)

desde FMC 7.3+)

Utilice el comando Telnet o curl para asegurarse de que el FMC dispone de acceso HTTPS a tools.cisco.com (smartreceiver.cisco.com desde FMC 7.3+). Si se interrumpe la comunicación TCP 443, compruebe que no está bloqueada por un firewall y que no hay ningún dispositivo de descifrado SSL en la ruta.

<#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
```

Ensayo de rizo:

<#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#

```

Verificación de DNS

Verifique que la resolución se haya realizado correctamente en tools.cisco.com (smartreceiver.cisco.com desde FMC 7.3+):

```
<#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

Verificación de proxy

Si se utiliza apProxy, verifique los valores tanto en el FMC como en el servidor proxy. En el FMC, compruebe si el FMC utiliza la IP y el puerto del servidor proxy correctos.

```
<#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
```

En la interfaz de usuario de FMC, los valores de proxy se pueden confirmar desde System > Configuration > Management Interfaces.

Si los valores del lado del CSP son correctos, compruebe los valores del lado del servidor proxy (por ejemplo, si el servidor proxy permite el acceso desde el CSP y a tools.cisco.com. Además, permita el intercambio de tráfico y certificados a través del proxy. El CSP utiliza un certificado para el registro de la licencia inteligente).

ID de token caducado

Verifique que el ID de token emitido no haya caducado. Si ha caducado, solicite al administrador de Smart Software Manager que emita un nuevo token y vuelva a registrar la licencia inteligente con el nuevo ID de token.

Cambio del gateway FMC

Puede haber casos en los que la autenticación de Smart License no se pueda realizar correctamente debido a los efectos de un proxy de retransmisión o un dispositivo de descifrado SSL. Si es posible, cambie la ruta para el acceso a Internet de FMC para evitar estos dispositivos y vuelva a intentar el registro de la licencia inteligente.

Comprobar los eventos de estado en FMC

En el FMC, navegue hasta System > Health > Events y verifique el estado del módulo Smart License Monitor para ver si hay errores. Por ejemplo, si la conexión falla debido a un certificado

caducado; se genera un error, como id certificated expired, como se muestra en esta imagen.

The screenshot shows a table titled 'Table View of Health Events'. The table has columns for Module Name, Test Name, Time, Description, Value, Units, Status, Domain, and Device. Two rows are visible. The first row is for 'Smart License Monitor' with a test name 'Smart License Monitor', a time of '2020-06-17 13:48:55', a description 'Smart License usage is out of compliance.', a value of '0', units of 'Licenses', and a status icon indicating an error. The second row is for 'Appliance Heartbeat' with a test name 'Appliance Heartbeat', a time of '2020-06-17 13:48:55', a description 'Appliance mzafeiro_FP2110-2 is not sending heartbe...', a value of '0', and a status icon indicating an error.

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

Verifique el Registro de Eventos en el Lado SSM

Si el FMC puede conectarse al CSSM, verifique el registro de eventos de la conectividad en Inventario > Registro de eventos. Verifique si existen tales registros de eventos o de errores en el CSSM. Si no hay ningún problema con los valores o el funcionamiento del sitio del CSM, y no hay ningún registro de eventos en el lado del CSSM, existe la posibilidad de que exista un problema con la ruta entre el CSSM y el CSSM.

Problemas comunes

Resumen de los Estados de registro y autorización:

Estado de registro del producto	Estado de autorización de uso	Comentarios
NO REGISTRADO	—	El CSP no se encuentra en modo de registro ni de evaluación. Este es el estado inicial tras la instalación de FMC o tras el vencimiento de la licencia de evaluación de 90 días.
Registrado	Autorizado	El FMC está registrado con Cisco Smart Software Manager (CSSM) y hay dispositivos FTD registrados con una suscripción válida.
Registrado	Autorización caducada	El FMC no pudo comunicarse con el servidor de licencias de Cisco durante más de 90 días.
Registrado	NO REGISTRADO	El FMC está registrado con Cisco Smart Software Manager (CSSM), pero no hay dispositivos FTD registrados en el FMC.
Registrado	Incumplimiento	El FMC está registrado con Cisco Smart Software Manager (CSSM), pero hay dispositivos FTD registrados con una suscripción no válida.

		Por ejemplo, un dispositivo FTD (FP4112) utiliza una suscripción THREAT, pero con Cisco Smart Software Manager (CSSM) no hay suscripciones THREAT disponibles para FP4112.
Evaluación (90 días)	N/A	El período de evaluación está en uso, pero no hay dispositivos FTD registrados en el FMC.

Caso Práctico 1. Token no válido

Síntoma: el registro en el CSSM falla rápidamente (~10 s) debido a un token no válido, como se muestra en esta imagen.

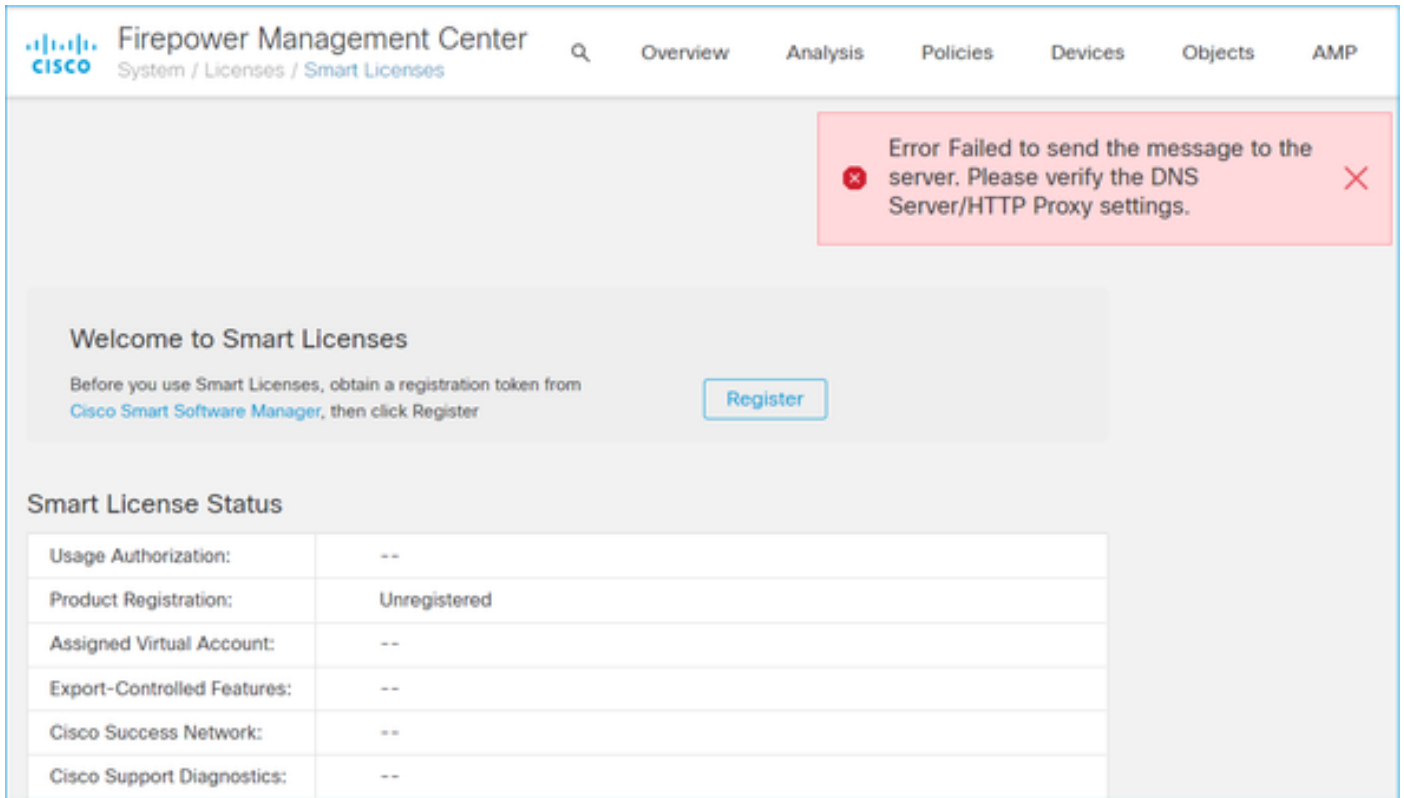
The screenshot shows the Cisco FMC Smart Licenses interface. At the top, there is a navigation menu with the following items: Overview, Analysis, Policies, Devices, Objects, AMP, and Intellig. Below the navigation menu, there is a red error message box that reads: "Error The token you have entered is invalid." Below the error message, there is a "Welcome to Smart Licenses" section with a "Register" button. Below the "Register" button, there is a "Smart License Status" table with the following data:

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

Resolución: utilice un token válido.

Caso Práctico 2. DNS no válido

Síntoma: el registro en el CSSM falló después de un tiempo (~25 s), como se muestra en esta imagen.



Compruebe el archivo `/var/log/process_stdout.log`. Se observa el problema de DNS:

```
<#root>
```

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

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

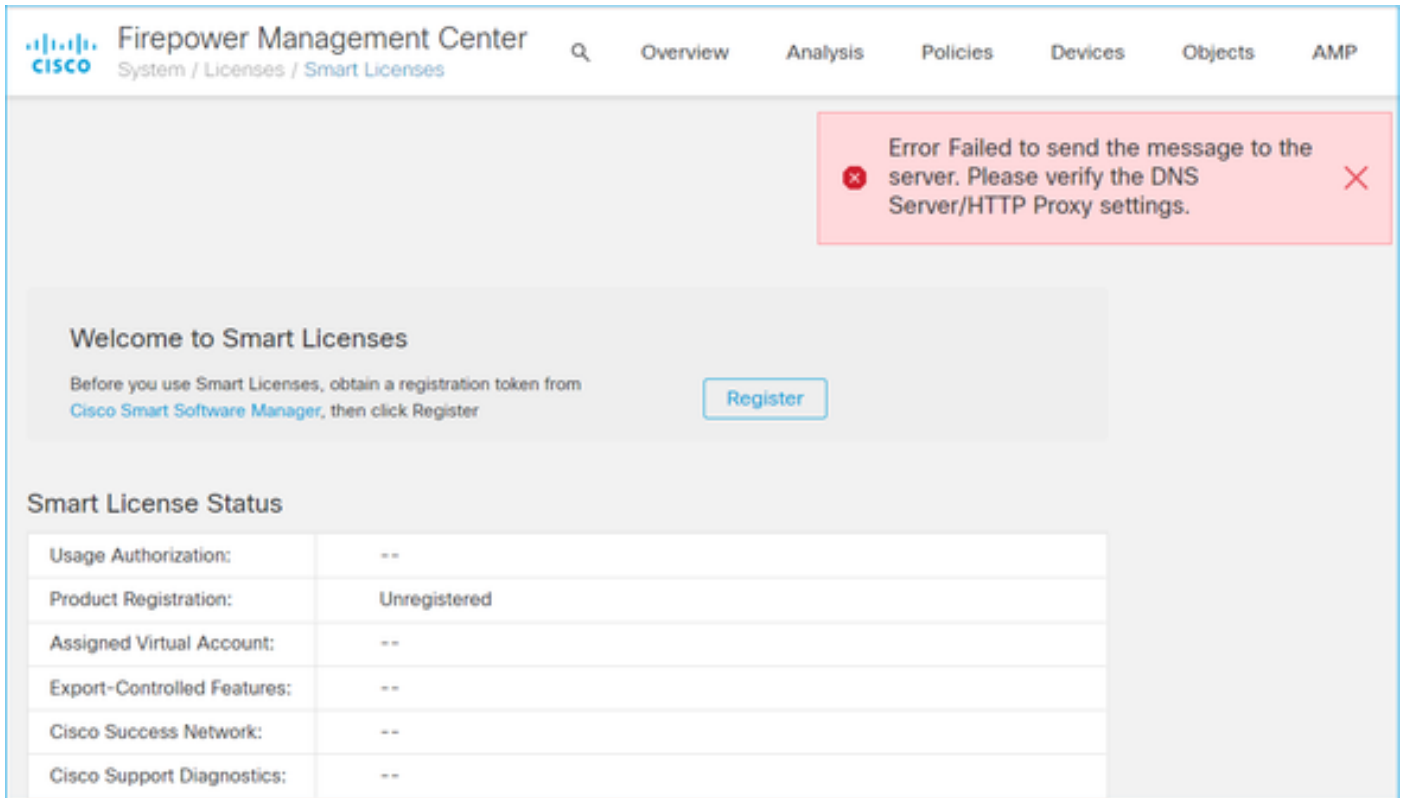
```
2020-06-25 09:05:21 sla[24043]: *Thu Jun 25 09:05:10.989 UTC: CH-LIB-ERROR: ch_pf_cur1_send_msg[494], failed to perform, err code 6, err string
```

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

Resolución: error de resolución del nombre de host CSSM. La resolución es configurar DNS, si no está configurado, o solucionar los problemas de DNS.

Caso Práctico 3. Valores de tiempo no válidos

Síntoma: el registro en el CSSM falló después de un tiempo (~25 s), como se muestra en esta imagen.



Verifique el archivo `/var/log/process_stdout.log`. Se ven los problemas de certificado:

<#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], 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/odce/services/DDCEService
```

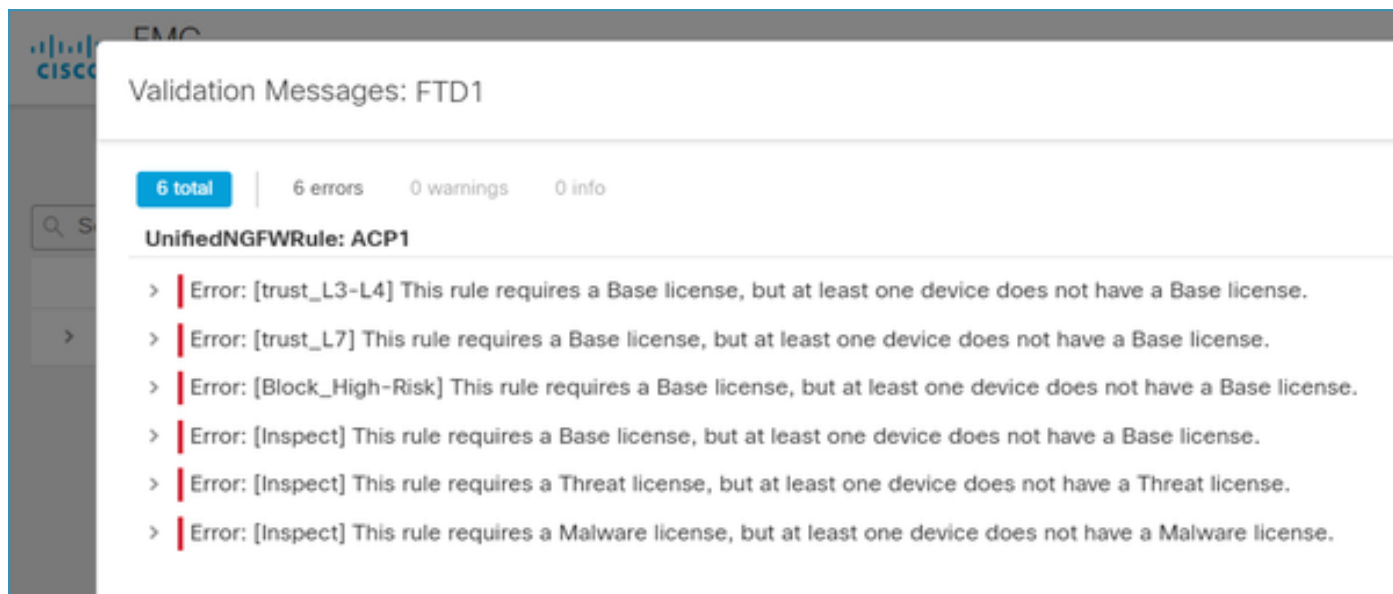
Compruebe el valor de tiempo del CSP:

<#root>

```
root@FMC2000-2:/Volume/home/admin#
date
Fri Jun 25 09:27:22 UTC 2021
```


Caso Práctico 4. Sin suscripción

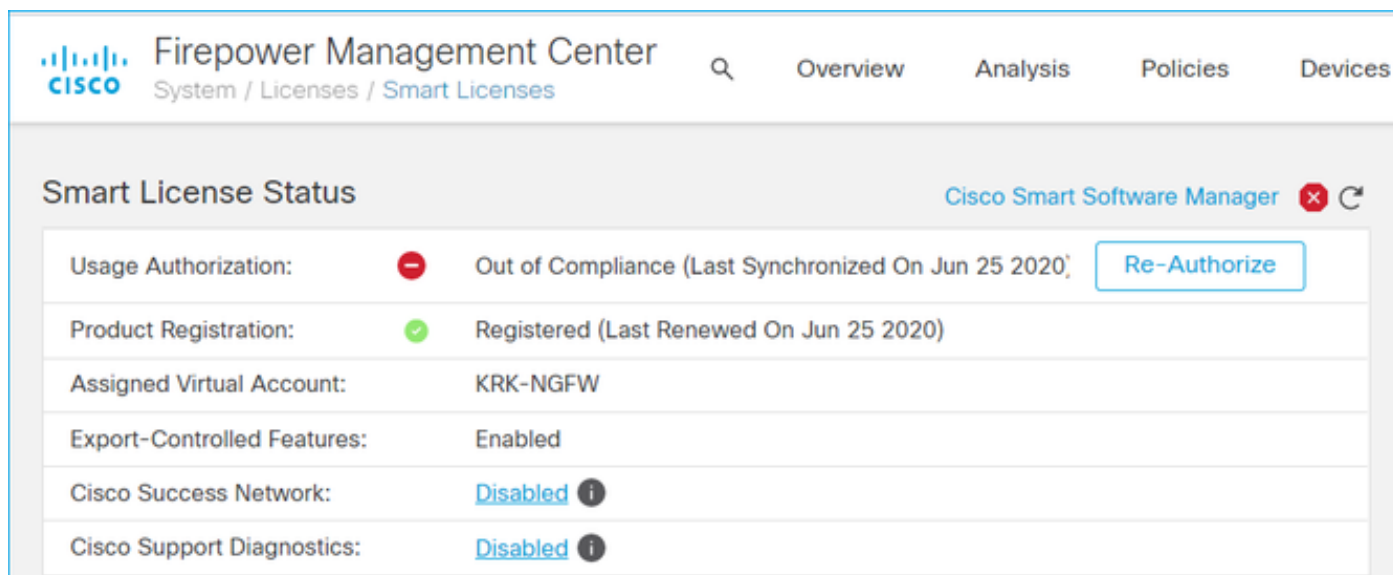
Si no hay ninguna suscripción de licencia para una función específica, la implementación de FMC no es posible:



Resolución: es necesario comprar y aplicar la suscripción necesaria al dispositivo.

Caso Práctico 5. Incumplimiento (OOC).

Si no existe ningún derecho para las suscripciones a FTD, la licencia inteligente de FMC pasa al estado de incumplimiento (OOC):



En el CSSM, verifique las Alertas en busca de errores:

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

Caso Práctico 6. Sin cifrado seguro

Si sólo se utiliza la licencia básica, se habilita el cifrado del estándar de cifrado de datos (DES) en el motor LINA de FTD. En ese caso, las implementaciones como la red privada virtual (VPN) L2L con algoritmos más potentes fallan:

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-NULL-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
Cisco Support Diagnostics:	Disabled

Resolución: registre el FMC en el CSSM y tenga activado un atributo de cifrado avanzado.

Notas complementarias

Establecer la notificación del estado de la licencia inteligente

Notificación de correo electrónico por SSM

En el lado SSM, SSM Email Notification permite la recepción de correos electrónicos de resumen para diversos eventos. Por ejemplo, notificación de falta de licencia o de licencias que están a punto de caducar. Se pueden recibir notificaciones de conexión de instancia de producto o de error de actualización.

Esta función es muy útil para advertir y evitar la aparición de restricciones funcionales debido a la expiración de la licencia.

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

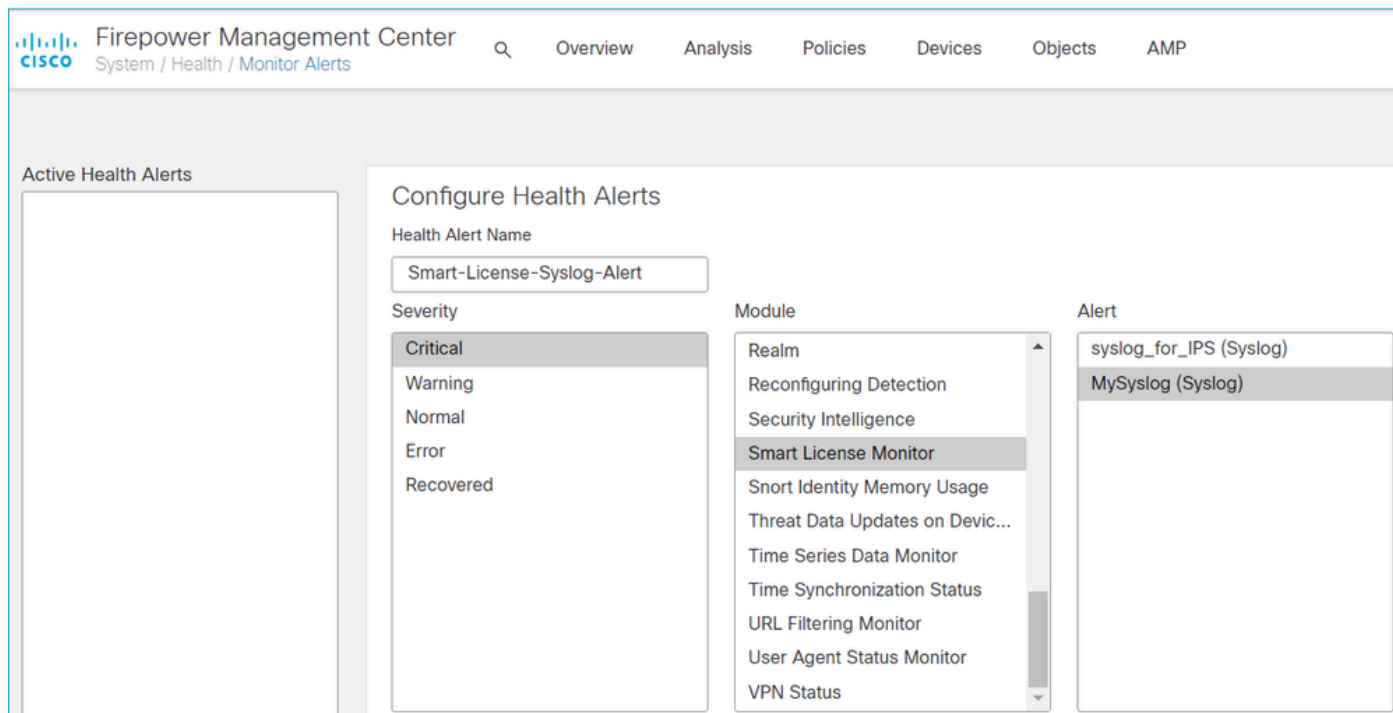
Status Notification

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

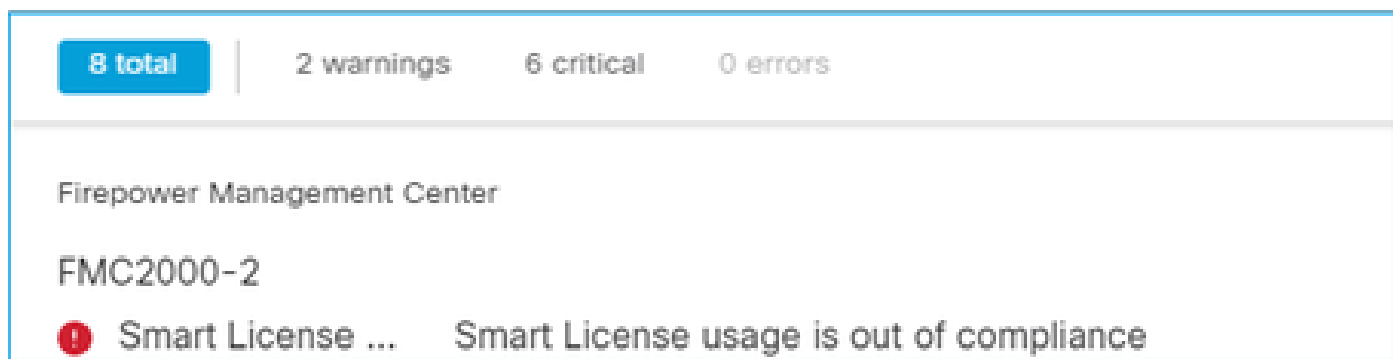
Obtener notificaciones de alertas de estado del FMC

En el lado de FMC, es posible configurar una alerta de monitor de estado y recibir una notificación de alerta de un evento de estado. Module Smart License Monitor está disponible para comprobar el estado de Smart License. La alerta de monitor admite Syslog, correo electrónico y capturas SNMP.

Este es un ejemplo de configuración para obtener un mensaje de Syslog cuando ocurre un evento del monitor de Smart License:



Este es un ejemplo de una alerta de estado:



El mensaje Syslog generado por el CSP es:

```
<#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
```

Consulte [Supervisión de estado](#) para obtener detalles adicionales sobre las alertas de supervisión de estado.

Varios CSP en la misma cuenta inteligente

Cuando se utilizan varios CSP en la misma cuenta inteligente, cada nombre de host de CSP debe ser único. Cuando se gestionen varios CSM, para distinguir cada CSM, el nombre de host de cada CSM debe ser único. Esto es útil para el mantenimiento de FMC Smart License en funcionamiento.

FMC debe mantener la conectividad a Internet

Después del registro, el FMC comprueba el estado de la licencia y la nube de Smart License cada 30 días. Si el CSP no puede comunicarse durante 90 días, la función con licencia se mantiene, pero permanece en el estado Autorización caducada. Incluso en este estado, FMC intenta conectarse continuamente a la nube de licencias inteligentes.

Implementación de varios FMCv

Cuando se utiliza el sistema Firepower en un entorno virtual, no se admite oficialmente la clonación (en caliente o en frío). Cada FirePOWER Management Center virtual (FMCv) es único porque contiene información de autenticación. Para implementar varios FMCv, estos deben crearse a partir del archivo Open Virtualization Format (OVF) de uno en uno. Para obtener más información sobre esta limitación, consulte la [Guía de inicio rápido de implementación de Cisco Firepower Management Center Virtual para VMware](#).

Preguntas más frecuentes (FAQ)

En FTD HA, ¿cuántas licencias de dispositivos se necesitan?

Cuando se utilizan dos FTD en alta disponibilidad, se necesita una licencia para cada dispositivo. Por ejemplo, se necesitan dos licencias de amenazas y malware si se utilizan las funciones Sistema de protección intrusiva (IPS) y Protección frente a malware avanzado (AMP) en el par FTD HA.

¿Por qué no utiliza FTD ninguna licencia de AnyConnect?

Después de registrarse en el FMC en la cuenta Smart Account, asegúrese de que la licencia de AnyConnect esté habilitada. Para activar la licencia, vaya a FMC > Dispositivos, elija su dispositivo y seleccione Licencia. Seleccione el icono Lápiz., elija la licencia que se deposita en la cuenta inteligente y seleccione Guardar.

¿Por qué solo se utiliza una licencia de AnyConnect en la cuenta inteligente cuando hay 100 usuarios conectados?

Este es el comportamiento esperado, ya que Smart Account realiza un seguimiento del número de dispositivos que tienen esta licencia habilitada, no de los usuarios activos conectados.

¿Por qué se produce el error `Device does not have the AnyConnect License` tras la configuración e implementación de una VPN de acceso remoto por parte del FMC?

Asegúrese de que el FMC esté registrado en Smart License Cloud. El comportamiento esperado es que la configuración de acceso remoto no se puede implementar cuando el FMC no está registrado o está en modo de evaluación. Si el FMC está registrado, asegúrese de que la licencia de AnyConnect exista en su cuenta Smart Account y de que esté asignada al dispositivo.

Para asignar una licencia, navegar a FMC Devices, seleccione su dispositivo, Licencia (icono de lápiz). Elija la licencia en Smart Account y seleccione Guardar.

¿Por qué se produce el error `Remote Access VPN with SSL cannot be deployed when Export-Controlled Features (Strong-crypto) are disabled` cuando hay una implementación de una configuración VPN de acceso remoto?

La VPN de acceso remoto implementada en el FTD requiere que se habilite una licencia de cifrado seguro. EsAsegúrese de que la licencia de cifrado seguro está activada en el FMC. Para comprobar el estado de la licencia de cifrado seguro, navegar a la FMC System > Licenses > Smart Licensing y verifique que las funciones controladas por exportación estén habilitadas.

¿Cómo se habilita una licencia de cifrado seguro si `Export-Controlled Features` está deshabilitada?

Esta funcionalidad se habilita automáticamente si el token utilizado durante el registro del FMC en la nube de Smart Account tiene la opción Permitir la funcionalidad de exportación controlada en los productos registrados con este token habilitado. Si el testigo no tiene activada esta opción, anule el registro del CSP y vuelva a registrarlo con esta opción activada.

¿Qué se puede hacer si la opción 'Permitir funcionalidad de exportación controlada en los productos registrados con este token' no está disponible cuando se genera el token?

Póngase en contacto con su equipo de cuentas de Cisco.

¿Por qué no se recibe el error "Cifrado seguro (es decir, algoritmo de cifrado mayor que DES) para la topología VPN s2s"?

Este error aparece cuando el FMC utiliza el modo de evaluación o la cuenta de Smart License no tiene derecho a una licencia de cifrado seguro. Verifique que el FMC esté registrado ante la autoridad de licencias y que esté habilitada la función de permitir exportación controlada en los productos registrados con este token. Si no se permite a la cuenta inteligente utilizar una licencia de cifrado avanzado, no se permite la implementación de la configuración VPN de sitio a sitio con cifrados más seguros que DES.

¿Por qué se recibe un estado de 'Incumplimiento' en el FMC?

El dispositivo puede quedar fuera de conformidad cuando uno de los dispositivos administrados utiliza licencias no disponibles.

¿Cómo se puede corregir el estado "Incumplimiento"?

Siga los pasos descritos en la Guía de configuración de Firepower:

1. Consulte la sección Smart Licenses (Licencias inteligentes) en la parte inferior de la página para determinar qué licencias se necesitan.
2. Adquiera las licencias necesarias a través de sus canales habituales.
3. En Cisco Smart Software Manager (<https://software.cisco.com/#SmartLicensing-Inventory>), verifique que las licencias aparezcan en su cuenta virtual.
4. En el FMC, seleccione System > Licenses > Smart Licenses.
5. Seleccione Volver a Autorizar.

El procedimiento completo se puede encontrar en [Licencias del sistema Firepower](#).

¿Cuáles son las funciones de Firepower Threat Defence Base?

La licencia básica permite:

- Configuración de los dispositivos FTD para el switch y la ruta (que incluye DHCP Relay y NAT).
- Configuración de dispositivos FTD en modo de alta disponibilidad (HA).
- Configuración de módulos de seguridad como un clúster dentro de un chasis Firepower 9300 (clúster dentro del chasis).
- Configuración de los dispositivos Firepower serie 9300 o Firepower serie 4100 (FTD) como un clúster (clúster entre chasis).
- Configuración del control de usuarios y aplicaciones y adición de condiciones de usuarios y aplicaciones a las reglas de control de acceso.

¿Cómo se puede obtener la licencia de las funciones de base de Firepower Threat Defence?

Con cada compra de un dispositivo Firepower Threat Defense o Firepower Threat Defence Virtual se incluye automáticamente una licencia Base. Se añade automáticamente a su cuenta Smart Account cuando el FTD se registra en el FMC.

¿Qué direcciones IP se deben permitir en la ruta entre el FMC y la nube de licencias inteligentes?

El CSP utiliza la dirección IP en el puerto 443 para comunicarse con Smart License Cloud.

Esa dirección IP (<https://tools.cisco.com>) se resuelve en estas direcciones IP:

- 72.163.4.38
- 173.37.145.8

Para las versiones FMC superiores a 7.3, se conecta a <https://smartreceiver.cisco.com>, que

resuelve estas direcciones IP:

- 146 112 59 81

Información Relacionada

- [Guías de configuración de Firepower Management Center](#)
- [Descripción general de Cisco Live Smart Licensing: BRKARC-2034](#)
- [Licencias de funciones de Cisco Secure Firewall Management Center](#)
- [Preguntas frecuentes \(FAQ\) sobre licencias de software inteligente de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).