

Use o registro de licença inteligente FMC e FTD e problemas comuns para solucionar problemas

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Registro de licença inteligente do FMC](#)

[Pré-requisitos](#)

[Registro de licença inteligente do FMC](#)

[Confirmação no lado do Smart Software Manager \(SSM\)](#)

[Cancelamento de registro da licença inteligente do FMC](#)

[RMA](#)

[Troubleshooting](#)

[Problemas comuns](#)

[Casos Práticos 1. Token inválido](#)

[Casos Práticos 2. DNS inválido](#)

[Casos Práticos 3. Valores de tempo inválidos](#)

[Casos Práticos 4. Sem Assinatura](#)

[Casos Práticos 5. Fora de conformidade \(OOC\)](#)

[Casos Práticos 6. Sem criptografia forte](#)

[Notas adicionais](#)

[Definir Notificação de Estado de Licença Inteligente](#)

[Obter Notificações de Alerta de Integridade do FMC](#)

[Vários FMCs na mesma Conta inteligente](#)

[O FMC deve manter a conectividade com a Internet](#)

[Implantar vários FMCs](#)

[Perguntas frequentes \(FAQs\)](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve a configuração de registro da Licença inteligente do Firepower Management Center em dispositivos gerenciados pelo Firepower Threat Defense.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

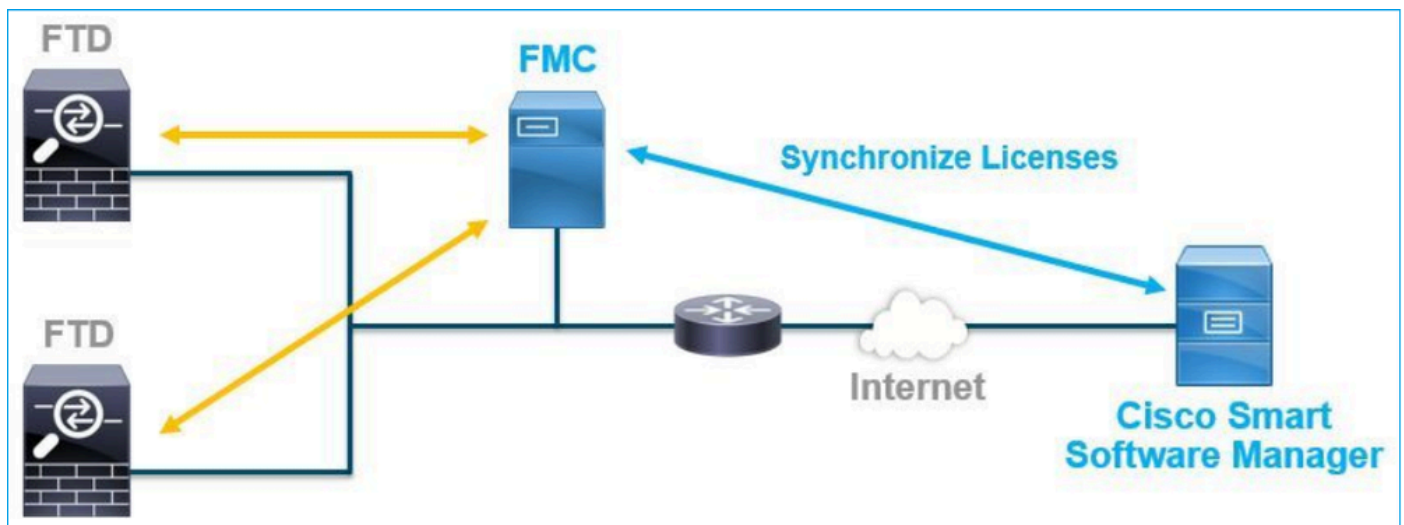
Componentes Utilizados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

FMC, FTD e registro de Licença inteligente.

O registro da Smart License é realizado no Firepower Management Center (FMC). O FMC se comunica com o portal do Cisco Smart Software Manager (CSSM) pela Internet. No CSSM, o administrador do firewall gerencia a Conta inteligente e suas licenças. O FMC pode atribuir e excluir licenças livremente para os dispositivos Firepower Threat Defense (FTD) gerenciados. Por outras palavras, o CVP gere centralmente as licenças dos dispositivos de DTF.



É necessária uma licença adicional para usar determinados recursos dos dispositivos de FTD. Os tipos de Smart License que os clientes podem atribuir a um dispositivo FTD são documentados em [Tipos de Licença e Restrições FTD](#).

A licença Básica está incluída no dispositivo FTD. Essa licença é registrada automaticamente em sua Smart Account quando o FMC é registrado no CSSM.

As licenças baseadas em termos: Ameaças, Malware e Filtragem de URL são opcionais. Para usar recursos relacionados a uma licença, uma licença precisa ser atribuída ao dispositivo FTD.

Para usar um Firepower Management Center Virtual (FMCv) para o gerenciamento de FTD, uma licença de dispositivo Firepower MCv no CSSM também é necessária para o FMCv.

A licença FMCv está incluída no software e é perpétua.

Além disso, cenários são fornecidos neste documento para ajudar a solucionar erros comuns de registro de licença que possam ocorrer.

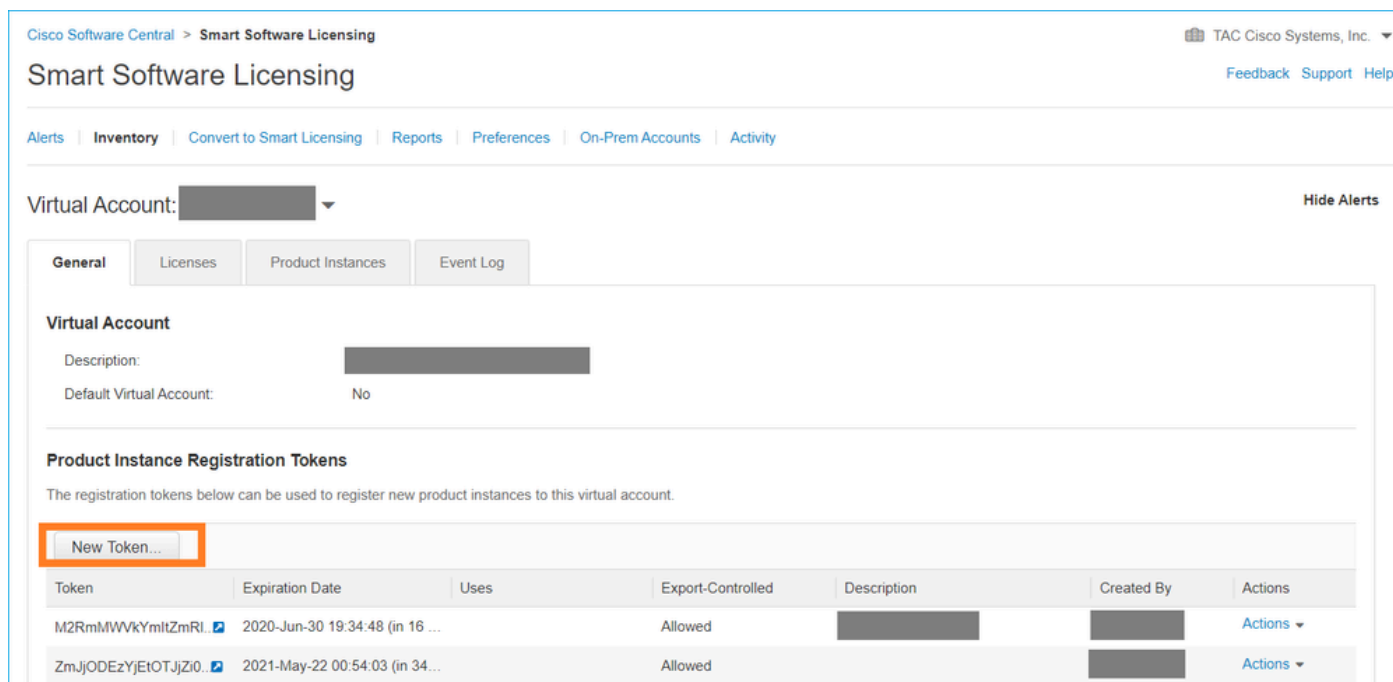
Para obter mais detalhes sobre licenças, consulte [Licenças de recursos do Cisco Firepower System](#) e [Perguntas frequentes \(FAQ\) sobre o licenciamento do Firepower](#).

Registro de licença inteligente do FMC

Pré-requisitos

1. Para o registro de uma licença inteligente, o CVP deve ter acesso à Internet. Como o certificado é trocado entre o FMC e a Smart License Cloud com HTTPS, verifique se não há nenhum dispositivo no caminho que possa afetar/modificar a comunicação. (por exemplo, Firewall, Proxy, dispositivo de Criptografia SSL e assim por diante).

2. Acesse o CSSM e emita um ID de token no botão Inventory > General > New Token, como mostrado nesta imagem.



The screenshot shows the Cisco Software Central interface for Smart Software Licensing. The breadcrumb trail is "Cisco Software Central > Smart Software Licensing". The page title is "Smart Software Licensing" with links for "Feedback", "Support", and "Help". A navigation bar includes "Alerts", "Inventory", "Convert to Smart Licensing", "Reports", "Preferences", "On-Prem Accounts", and "Activity". A "Virtual Account" dropdown menu is visible, along with a "Hide Alerts" button. Below the navigation, there are tabs for "General", "Licenses", "Product Instances", and "Event Log". The "General" tab is active, showing "Virtual Account" details (Description, Default Virtual Account: No) and "Product Instance Registration Tokens". A note states: "The registration tokens below can be used to register new product instances to this virtual account." A "New Token..." button is highlighted with a red box. Below it is a table of registration tokens.

Token	Expiration Date	Uses	Export-Controlled	Description	Created By	Actions
M2RmMWVkymltZmRI...	2020-Jun-30 19:34:48 (in 16 ...)		Allowed			Actions ▾
ZmJjODEzYjEtOTJjZi0...	2021-May-22 00:54:03 (in 34...)		Allowed			Actions ▾

Para usar criptografia forte, habilite a opção Permitir funcionalidade de exportação controlada nos produtos registrados com este token. Quando ativada, uma marca de seleção é exibida na caixa de seleção.

3. Selecione Criar 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 ?

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

Registro de licença inteligente do FMC

Navegue até System > Licenses > Smart Licenses no FMC e selecione o botão Register, como mostrado nesta imagem.

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

[Register](#)

Smart License Status

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

Insira a ID do token na janela Registro do produto Smart Licensing e selecione Aplicar alterações, como mostrado nesta imagem.

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

Se o registro da Smart License tiver sido bem-sucedido, o status do registro do produto mostrará Registered, como mostrado nesta imagem.

The screenshot shows the Cisco Smart License Status page. At the top, there is a navigation bar with tabs for Overview, Analysis, Policies, Devices, Objects, AMP, Intelligence, and Deploy. The main content area is titled "Smart License Status" and includes a "Cisco Smart Software Manager" link. Below this, there is a table with the following rows:

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 ⓘ

Below the status table is the "Smart Licenses" section, which includes a "Filter Devices..." search box and an "Edit Licenses" button. The main table lists license types and their counts:

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

Para atribuir uma licença com base no período ao dispositivo FTD, selecione Editar licenças. Em seguida, selecione e adicione um dispositivo gerenciado à seção Dispositivos com licença. Finalmente, selecione o botão Apply como mostrado nesta imagem.

The screenshot shows the "Edit Licenses" dialog box. At the top, there are tabs for Malware, Threat, URL Filtering, AnyConnect Apex, AnyConnect Plus, and AnyConnect VPN Only. The "Malware" tab is selected. Below the tabs, there are two sections: "Devices without license" and "Devices with license (1)".

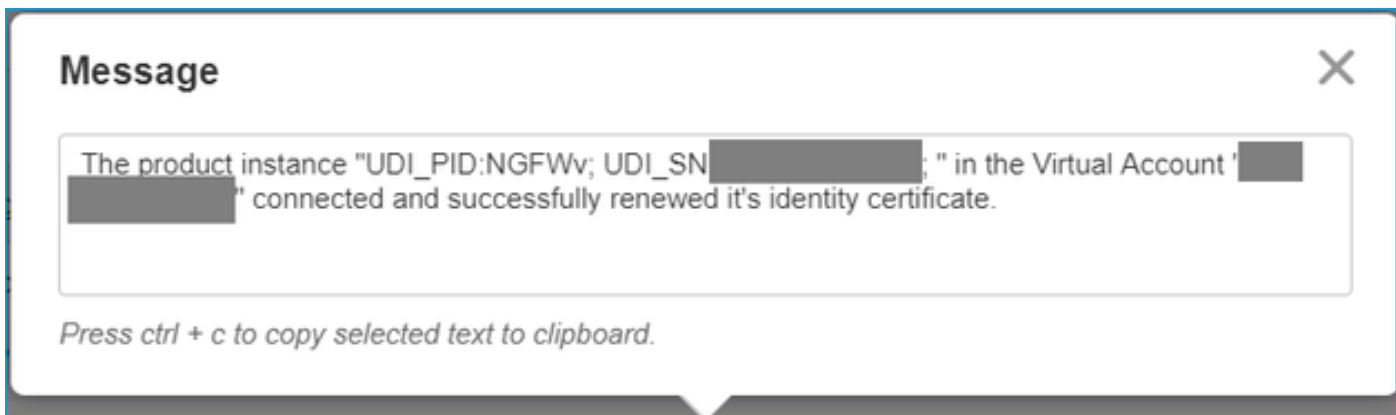
In the "Devices without license" section, there is a search box and a list of devices. The device "FTD" is highlighted with an orange box and labeled with the number "1".

In the "Devices with license (1)" section, the device "FTD" is listed and highlighted with an orange box. An "Add" button is located between the two sections and is labeled with the number "2".

At the bottom right of the dialog box, there are "Cancel" and "Apply" buttons. The "Apply" button is highlighted with an orange box and labeled with the number "3".

Confirmação no lado do Smart Software Manager (SSM)

O sucesso do registro da FMC Smart License pode ser confirmado em Inventory > Event Log no CSSM, como mostrado nesta imagem.

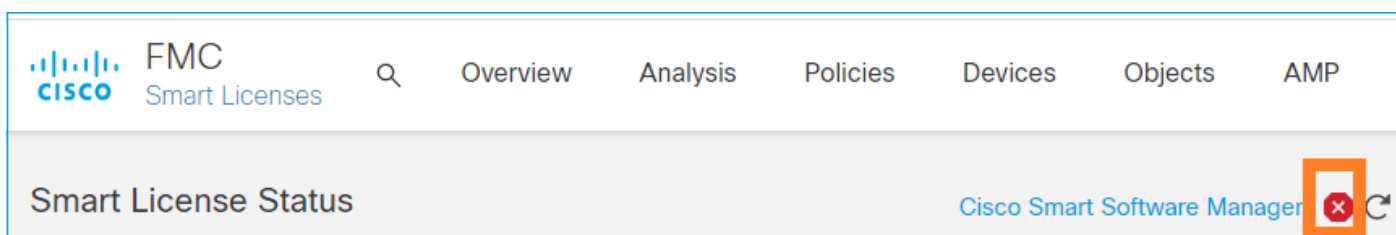


O status de registro do FMC pode ser confirmado em Inventário > Instâncias do produto. Verifique o registro de eventos na guia Event Log. O registro e o status de uso da Licença inteligente podem ser verificados na guia Inventário > Licenças. Verifique se a licença baseada em prazo adquirida está sendo usada corretamente e se não há alertas que indiquem licenças insuficientes.

Cancelamento de registro da licença inteligente do FMC

Cancele o registro do FMC no Cisco SSM

Para liberar a licença por algum motivo ou usar um token diferente, navegue para System > Licenses > Smart Licenses e selecione o botão de cancelamento de registro, como mostrado nesta imagem.



Remover Registro do Lado SSM

Acesse o Smart Software Manager ([Cisco Smart Software Manager](#)) e, em Inventory > Product Instances, selecione Remove no FMC de destino. Em seguida, selecione Remove Product Instance para remover o FMC e liberar as licenças alocadas, como mostrado nesta imagem.

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

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

Se o FMC for devolvido, cancele o registro do FMC no Cisco Smart Software Manager (CSSM) usando as etapas da seção Cancelamento de registro da licença inteligente do FMC > Remover registro do lado do SSM e registre novamente o FMC no CSSM usando as etapas da seção Registro da licença inteligente do FMC.

Troubleshooting

Verificação de Sincronização de Tempo

Acesse a CLI do FMC (por exemplo, SSH) e verifique se a hora está correta e se está sincronizada com um servidor NTP confiável. Como o certificado é usado para autenticação de Licença inteligente, é importante que o FMC tenha as informações de hora corretas:

```
<#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

Na interface do usuário do FMC, verifique os valores do servidor NTP em System > Configuration > Time Synchronization.

Habilite a resolução de nomes e verifique a acessibilidade para tools.cisco.com (smartreceiver.cisco.com do FMC 7.3+)

Garantir que o FMC possa resolver um FQDN e esteja acessível para tools.cisco.com (smartreceiver.cisco.com do FMC 7.3 em diante, conforme a [ID de bug da 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
```

Na interface do usuário do FMC, verifique o IP de gerenciamento e o IP do servidor DNS em System > Configuration > Management Interfaces.

Verifique o acesso HTTPS (TCP 443) do FMC para tools.cisco.com (smartreceiver.cisco.com do FMC 7.3+)

Use Telnet ou curl para garantir que o FMC tenha acesso HTTPS a tools.cisco.com (smartreceiver.cisco.com do FMC 7.3+). Se a comunicação TCP 443 estiver interrompida, verifique se ela não está bloqueada por um firewall e se não há nenhum dispositivo de criptografia SSL no caminho.

<#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
```

Ensaio em curva:

<#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#

```

Verificação DNS

Verifique se a resolução foi bem-sucedida em tools.cisco.com (smartreceiver.cisco.com do 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

Verificação de proxy

Se apProxy for usado, verifique os valores no FMC e no servidor proxy. No FMC, verifique se o FMC usa o IP e a porta corretos do servidor proxy.

<#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
```

Na interface do usuário do FMC, os valores de proxy podem ser confirmados em System > Configuration > Management Interfaces.

Se os valores do lado do FMC estiverem corretos, verifique os valores do lado do servidor proxy (por exemplo, se o servidor proxy permitir o acesso do FMC e de tools.cisco.com). Além disso, permita a troca de tráfego e certificados através do proxy. O FMC utiliza um certificado para o registro da Smart License).

ID do token expirado

Verifique se a ID do token emitido não expirou. Se ele tiver expirado, peça ao administrador do Smart Software Manager para emitir um novo token e registrar novamente a Smart License com a nova ID de token.

Alterar o gateway do FMC

Pode haver casos em que a autenticação da Licença inteligente não pode ser executada corretamente devido aos efeitos de um proxy de retransmissão ou dispositivo de descryptografia SSL. Se possível, altere a rota de acesso à Internet do FMC para evitar esses dispositivos e repita o registro da Licença inteligente.

Verificar os eventos de integridade no FMC

No FMC, navegue para System > Health > Events e verifique o status do módulo do Smart

License Monitor em busca de erros. Por exemplo, se a conexão falhar devido a um certificado expirado; um erro, como id certificated expirou, é gerado, como mostrado nesta imagem.

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 o registro de eventos no lado do SSM

Se o FMC puder se conectar ao CSSM, verifique o registro de eventos da conectividade em Inventory > Event Log. Verifique se há registros de eventos ou registros de erros no CSSM. Se não houver qualquer problema com os valores/funcionamento do local do CVP e se não existir um registro de eventos no lado do CSSM, é possível que se trate de um problema com a rota entre o CVP e o CSSM.

Problemas comuns

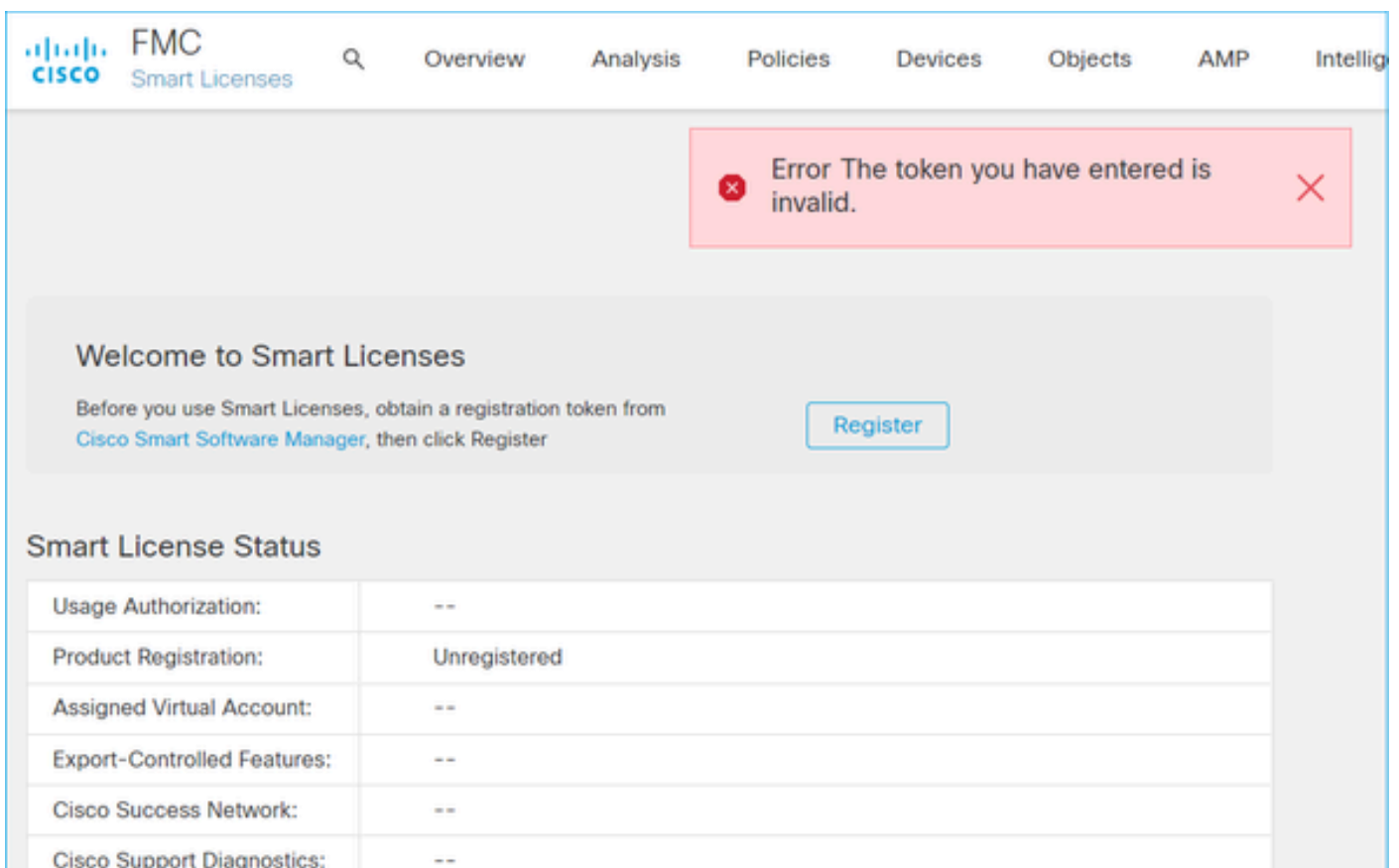
Resumo dos Estados de registro e autorização:

Estado de registro do produto	Estado de Autorização de Uso	Comentários
Não registrado	—	O FMC não está no modo Registrado nem no modo Avaliação. Este é o estado inicial após a instalação do FMC ou após o vencimento da licença de avaliação de 90 dias.
Registrado	Autorizado	O FMC está registrado no Cisco Smart Software Manager (CSSM) e há dispositivos FTD registrados com uma assinatura válida.
Registrado	Autorização expirada	O FMC não conseguiu se comunicar com o back-end de licenças da Cisco por mais de 90 dias.
Registrado	Não registrado	O FMC está registrado no Cisco Smart Software Manager (CSSM), mas não há dispositivos FTD registrados no FMC.
Registrado	Fora de conformidade	O FMC está registrado com o Cisco Smart Software Manager (CSSM), mas há dispositivos FTD

		<p>registrados com uma assinatura inválida.</p> <p>Por exemplo, um dispositivo FTD (FP4112) usa a assinatura THREAT, mas com o Cisco Smart Software Manager (CSSM) não há assinaturas THREAT disponíveis para FP4112.</p>
Avaliação (90 dias)	N/A	O período de avaliação está em uso, mas não há dispositivos FTD registrados no FMC.

Casos Práticos 1. Token inválido

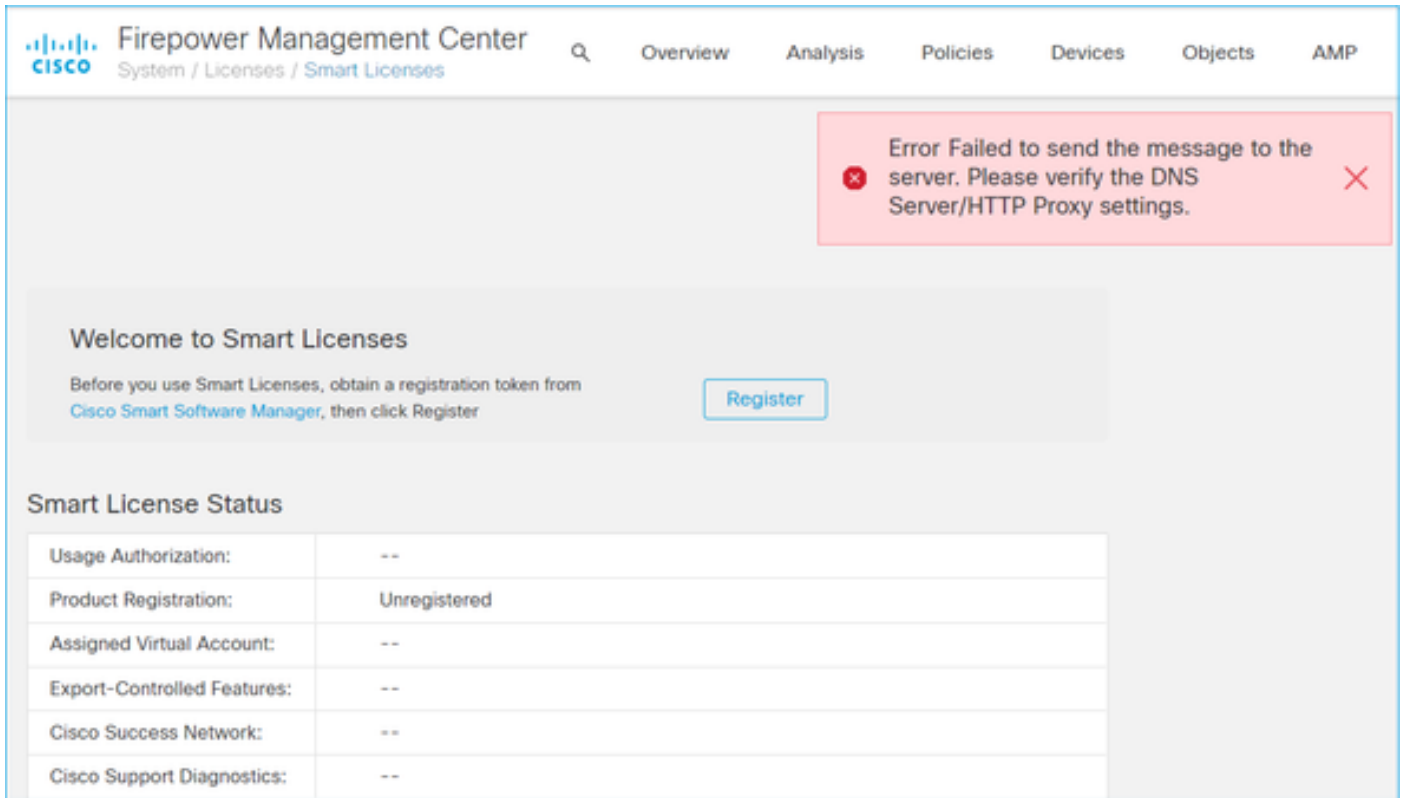
Sintoma: o registro no CSSM falha rapidamente (~10s) devido a token inválido, como mostrado nesta imagem.



Resolução: use um token válido.

Casos Práticos 2. DNS inválido

Sintoma: o registro no CSSM falhou após um tempo (~25s), como mostrado nesta imagem.



Verifique o arquivo `/var/log/process_stdout.log`. O problema de DNS é visto:

```
<#root>
```

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

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

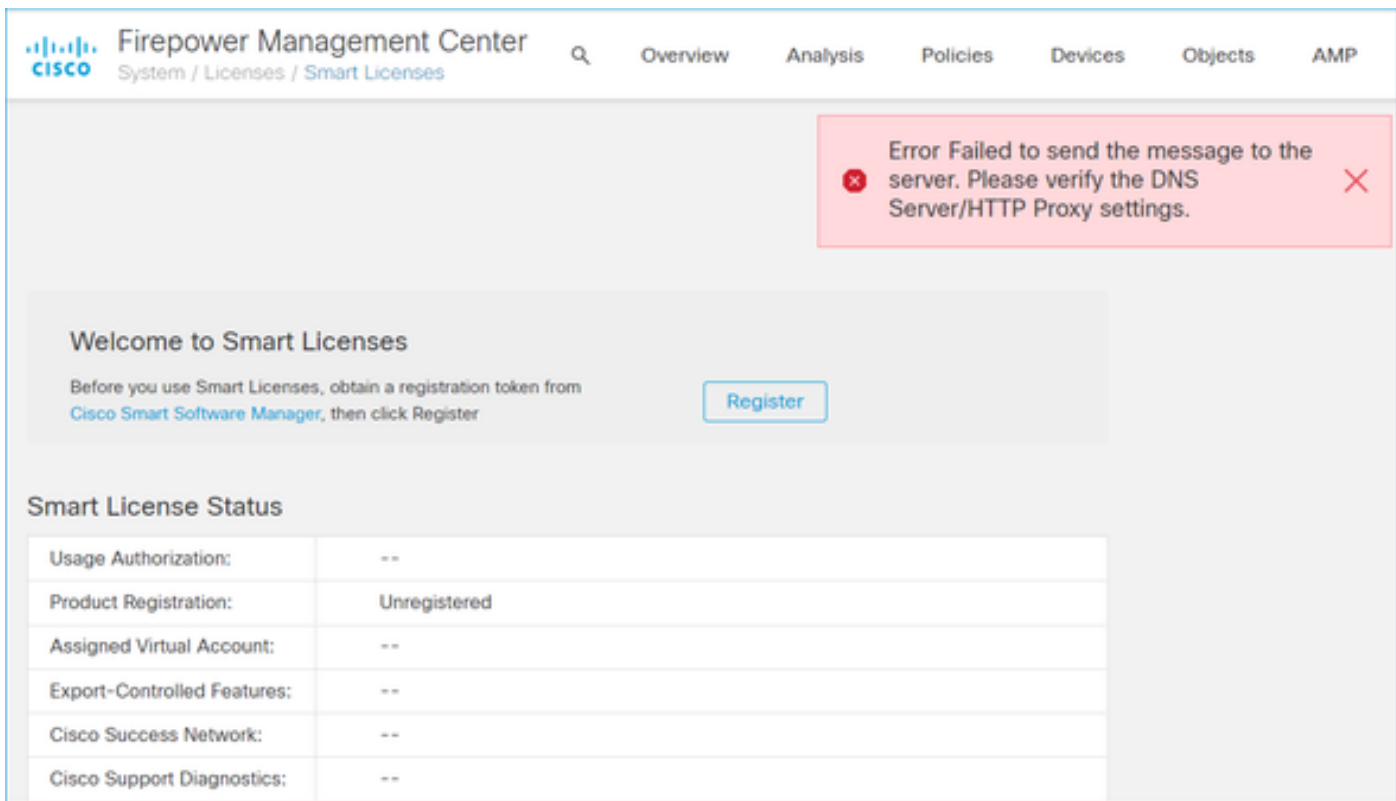
```
2020-06-25 09:05:21 sla[24043]: *Thu Jun 25 09:05:10.989 UTC: CH-LIB-ERROR: ch_pf_cur1_send_msg[494], failed to perform, err code 6, err string
```

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

Resolução: falha na resolução do nome de host CSSM. A solução é configurar o DNS, se não estiver configurado, ou corrigir os problemas do DNS.

Casos Práticos 3. Valores de tempo inválidos

Sintoma: o registro no CSSM falhou após um tempo (~25s), como mostrado nesta imagem.



Verifique o arquivo /var/log/process_stdout.log. Os problemas de certificado são vistos:

<#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
```

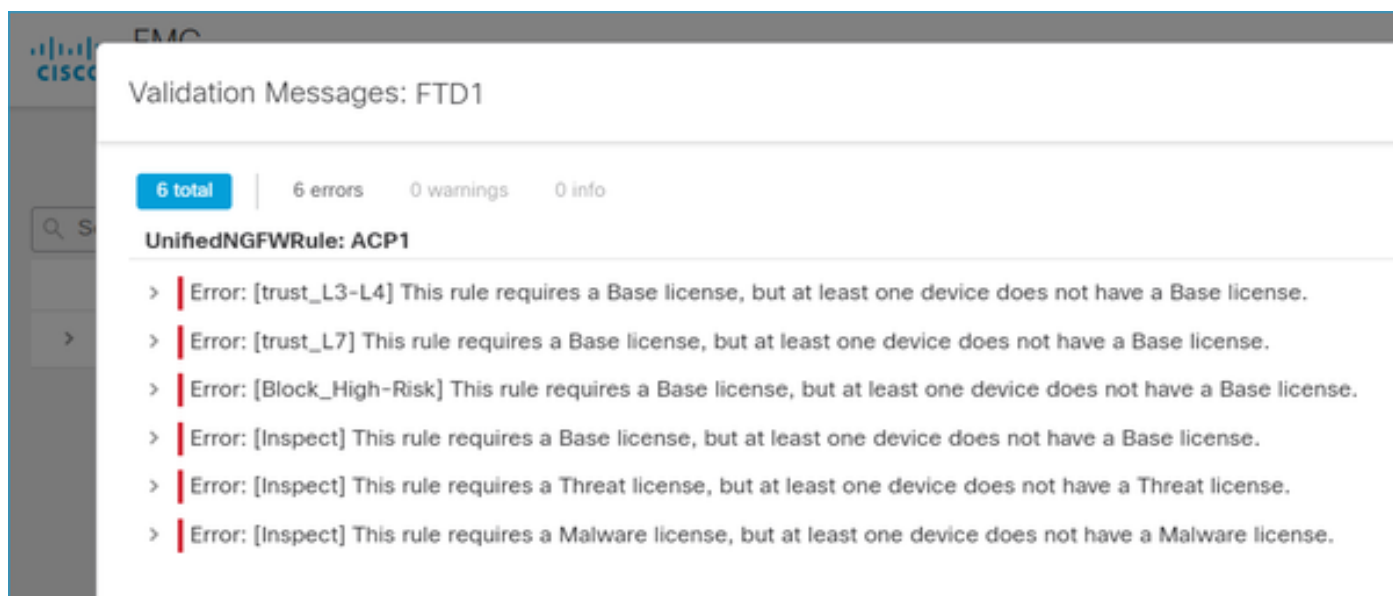
Verifique o valor de hora do FMC:

<#root>

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


Casos Práticos 4. Sem Assinatura

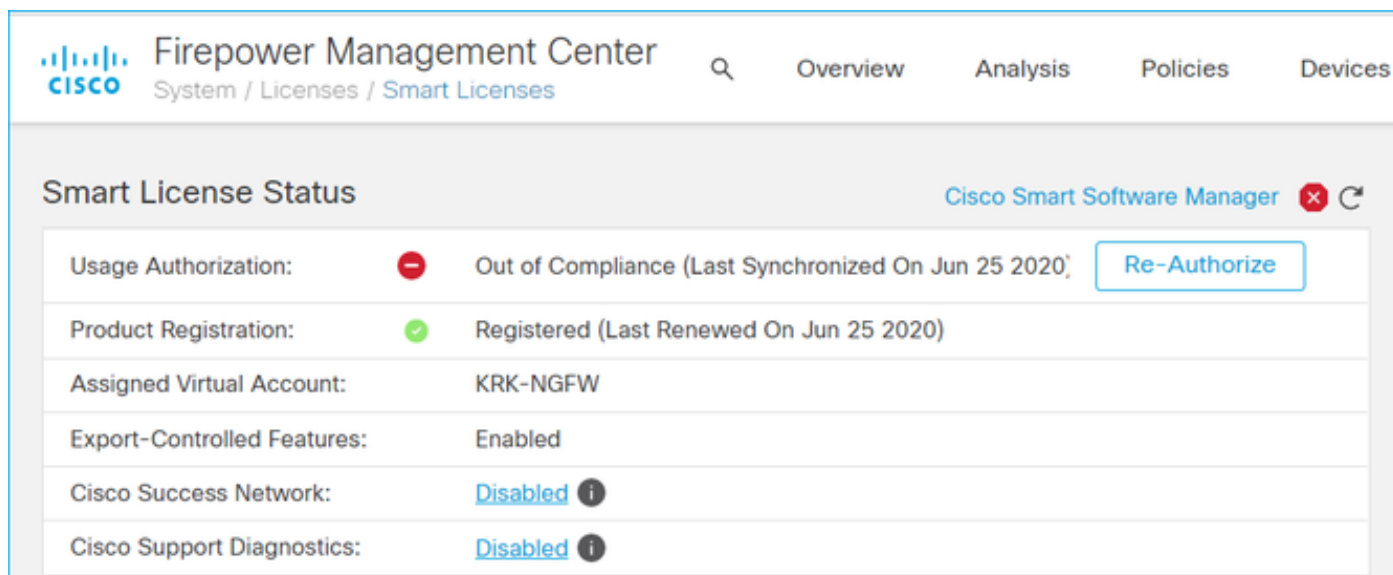
Se não houver assinatura de licença para um recurso específico, a implantação do FMC não será possível:



Resolução: é necessário comprar e aplicar a assinatura necessária ao dispositivo.

Casos Práticos 5. Fora de conformidade (OOC)

Se não houver direito a assinaturas de FTD, a Licença inteligente do FMC entrará no estado fora de conformidade (OOC):



No CSSM, verifique se há erros nos Alertas:

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

Casos Práticos 6. Sem criptografia forte

Se apenas a Licença básica for usada, a criptografia DES (Data Encryption Standard) será habilitada no mecanismo LINA do FTD. Nesse caso, as implantações como a rede virtual privada (VPN) L2L com algoritmos mais fortes falham:

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

Smart License Status

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 ⓘ

Resolução: registre o FMC no CSSM e tenha um atributo de criptografia forte habilitado.

Notas adicionais

Definir Notificação de Estado de Licença Inteligente

Notificação de e-mail por SSM

No lado do SSM, a Notificação por e-mail do SSM permite a recepção de e-mails de resumo para vários eventos. Por exemplo, notificação por falta de licença ou para licenças prestes a expirar. Notificações de conexão da instância do produto ou de falha na atualização podem ser recebidas.

Essa função é muito útil para observar e evitar a ocorrência de restrições funcionais devido à expiração da licença.

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

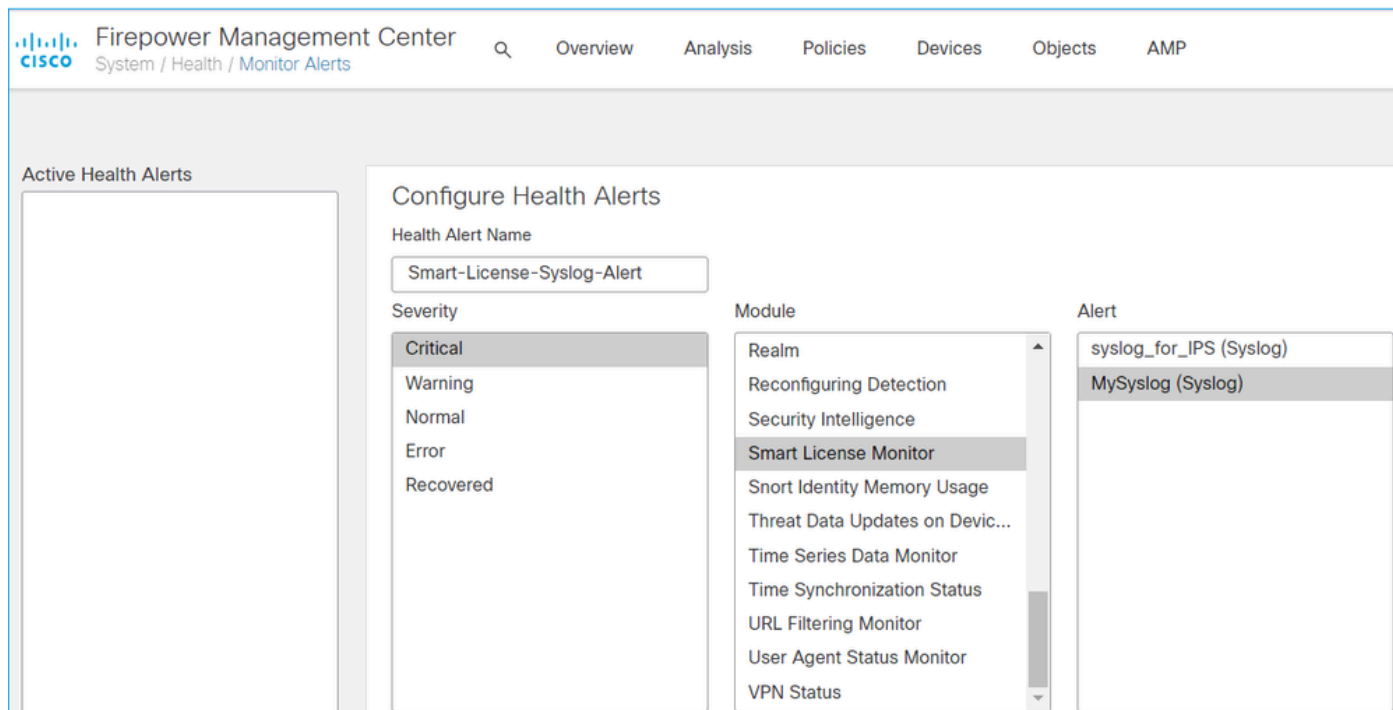
Receive an email when a Satellite synchronization file has finished processing by Smart Software Manager

Obter Notificações de Alerta de Integridade do FMC

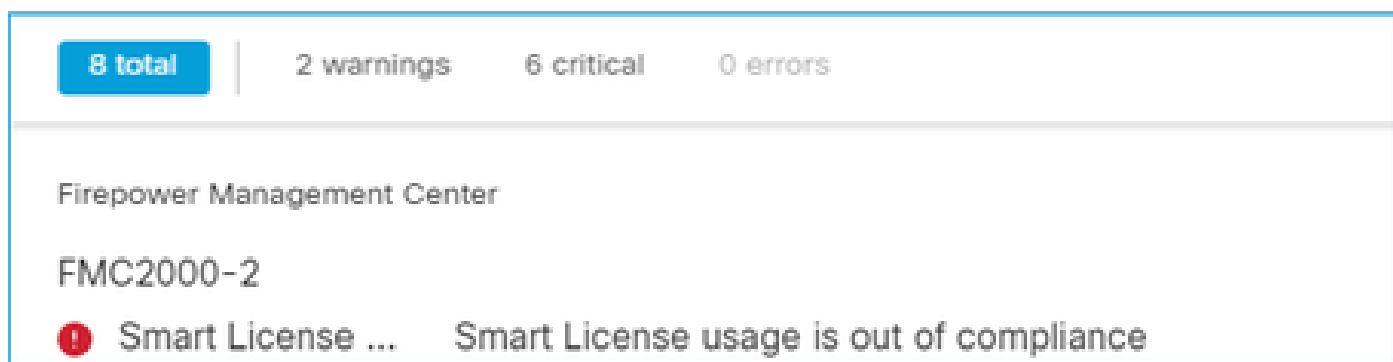
No lado do FMC, é possível configurar um alerta do monitor de saúde e receber uma notificação

de alerta de um evento de saúde. O Monitor de Licença Inteligente do Módulo está disponível para verificar o status da Licença Inteligente. O alerta do monitor oferece suporte a Syslog, Email e interceptação SNMP.

Este é um exemplo de configuração para obter uma mensagem de Syslog quando ocorrer um evento do monitor de Smart License:



Este é um exemplo de um Alerta de Integridade:



A mensagem Syslog gerada pelo FMC é:

<#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 [Monitoramento de Integridade](#) para obter detalhes adicionais sobre os Alertas do Monitor de Integridade.

Vários FMCs na mesma Conta inteligente

Quando vários FMCs são utilizados na mesma Conta inteligente, cada nome de host do FMC deve ser único. Quando são geridos vários CVP no CSSM, para distinguir cada CVP, o nome de host de cada CVP deve ser único. Isso é útil para a manutenção da licença inteligente do FMC em operação.

O FMC deve manter a conectividade com a Internet

Após o registro, o FMC verifica o status da Smart License Cloud e da licença a cada 30 dias. Se o CVP não puder comunicar durante 90 dias, a função licenciada é mantida, mas permanece no estado Autorização expirada. Mesmo nesse estado, o FMC tenta se conectar continuamente à nuvem de licença inteligente.

Implantar vários FMCv

Quando o sistema Firepower é usado em um ambiente virtual, o clone (quente ou frio) não é oficialmente suportado. Cada FMCv (Firepower Management Center virtual) é exclusivo porque contém informações de autenticação. Para implantar vários FMCv, o FMCv deve ser criado no arquivo OVF (Open Virtualization Format), um de cada vez. Para obter mais informações sobre essa limitação, consulte o [Guia de início rápido de implantação do Cisco Firepower Management Center Virtual for VMware](#).

Perguntas frequentes (FAQs)

No FTD HA, quantas licenças de dispositivo são necessárias?

Quando dois FTDs são usados em alta disponibilidade, uma licença é necessária para cada dispositivo. Por exemplo, duas licenças de ameaça e malware são necessárias se o sistema de proteção contra intrusão (IPS) e o recurso de proteção avançada contra malware (AMP) forem usados no par HA do FTD.

Por que nenhuma licença do AnyConnect é usada pelo FTD?

Após o registro do FMC na Smart Account, verifique se a licença do AnyConnect está habilitada. Para habilitar a licença, navegue até FMC > Devices, escolha seu dispositivo e selecione License. Selecione o ícone Lápis escolha a licença depositada na Smart Account e selecione Salvar.

Por que apenas uma licença do AnyConnect está em uso na Smart Account quando 100 usuários estão conectados?

Esse é o comportamento esperado, pois a Conta inteligente controla o número de dispositivos que têm essa licença habilitada, e não usuários ativos conectados.

Por que ocorre o erro `Device does not have the AnyConnect License` após a configuração e a implantação de uma VPN de acesso remoto pelo FMC?

Verifique se o FMC está registrado na Smart License Cloud. O comportamento esperado é a configuração de Acesso Remoto, que não pode ser implantada quando o FMC não está registrado ou está no modo de Avaliação. Se o FMC estiver registrado, verifique se a licença do AnyConnect existe em sua Conta inteligente e se ela está atribuída ao dispositivo.

Para atribuir uma licença, navegar para FMC Devices, selecione seu dispositivo, License (ícone do lápis). Escolha a licença na Smart Account e selecione Save.

Por que há o erro `Remote Access VPN with SSL cannot be deployed when Export-Controlled Features (Strong-crypto) are disabled` quando há uma implantação de uma configuração de VPN de acesso remoto?

A VPN de acesso remoto implantada no FTD requer uma licença de criptografia forte para ser habilitada. Verifique se uma licença de criptografia forte está habilitada no FMC. Para verificar o status da licença com criptografia forte, navegar para o Sistema FMC > Licenças > Smart Licensing e verifique se Export-Controlled Features (Recursos controlados por exportação) está ativado.

Como habilitar uma Licença de Criptografia Forte se o `Export-Controlled Features` estiver desabilitado?

Essa funcionalidade será habilitada automaticamente se o token usado durante o registro do FMC na Nuvem da Conta Inteligente tiver a opção Permitir funcionalidade de exportação controlada nos produtos registrados com esse token habilitada. Se o token não tiver essa opção habilitada, cancele o registro do FMC e registre-o novamente com essa opção habilitada.

O que pode ser feito se a opção 'Permitir funcionalidade de exportação controlada nos produtos registrados com este token' não estiver disponível quando o token for gerado?

Entre em contato com sua equipe de contas da Cisco.

Por que o erro 'Não há suporte para criptografia forte (ou seja, algoritmo de criptografia maior que DES) para s2s da topologia de VPN' foi recebido?

Este erro é exibido quando o FMC usa o modo de Avaliação ou a Smart License Account não tem direito a uma licença de criptografia forte. Verifique se o FMC está registrado para a autoridade de licença e se Permitir funcionalidade de exportação controlada nos produtos registrados com este token está habilitado. Se a Conta inteligente não tiver permissão para usar uma licença de Criptografia Forte, a implantação da configuração site a site da VPN com cifras mais fortes que DES não será permitida.

Por que é recebido um status de "Fora de conformidade" no FMC?

O dispositivo pode ficar fora de conformidade quando um dos dispositivos gerenciados usar licenças indisponíveis.

Como o status 'Fora de conformidade' pode ser corrigido?

Siga as etapas descritas no Guia de configuração do Firepower:

1. Consulte a seção Smart Licenses na parte inferior da página para determinar quais licenças são necessárias.
2. Compre as licenças necessárias pelos canais normais.
3. No Cisco Smart Software Manager (<https://software.cisco.com/#SmartLicensing-Inventory>), verifique se as licenças aparecem em sua Virtual Account.
4. No FMC, selecione System > Licenses > Smart Licenses.
5. Selecione Autorizar Novamente.

O procedimento completo pode ser encontrado em [Licenciamento do sistema Firepower](#).

Quais são os recursos da base do Firepower Threat Defense?

A licença Básica permite:

- Configuração de dispositivos FTD para comutação e roteamento (o que inclui Retransmissão DHCP e NAT).
- Configuração de dispositivos FTD em um modo de alta disponibilidade (HA).
- Configuração de módulos de segurança como um cluster em um chassi Firepower 9300 (cluster interno do chassi).
- Configuração de dispositivos Firepower 9300 ou Firepower 4100 Series (FTD) como um cluster (cluster entre chassis).
- Configuração de controle de usuário e aplicativo e adição de condições de usuário e aplicativo às regras de controle de acesso.

Como a licença dos recursos básicos do Firepower Threat Defense pode ser obtida?

Uma licença básica é incluída automaticamente em cada compra de um dispositivo virtual Firepower Threat Defense ou Firepower Threat Defense. Ele é automaticamente adicionado à sua Conta inteligente quando o FTD se registra no FMC.

Quais endereços IP devem ser permitidos no caminho entre o FMC e a Smart License Cloud?

O FMC usa o endereço IP na porta 443 para se comunicar com a Smart License Cloud.

Esse endereço IP (<https://tools.cisco.com>) é resolvido para estes endereços IP:

- 72.163.4.38
- 173.37.145.8

Para versões do FMC superiores a 7.3, ele se conecta a <https://smartreceiver.cisco.com> que resolve para estes endereços IP:

- 146.112.59. 81

Informações Relacionadas

- [Guias de configuração do Firepower Management Center](#)
- [Visão geral do Cisco Live Smart Licensing: BRKARC-2034](#)
- [Licenças de recursos do Cisco Secure Firewall Management Center](#)
- [Perguntas frequentes \(FAQs\) sobre o Cisco Smart Software Licensing](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.