

Integre y solucione problemas de Cisco XDR con Firepower Threat Defence (FTD)

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Licencias](#)

[Vincule sus cuentas a SSE y registre los dispositivos.](#)

[Registre los dispositivos en SSE](#)

Introducción

Este documento describe los pasos necesarios para integrar, verificar y solucionar problemas de Cisco XDR con Firepower Firepower Threat Defense (FTD).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Centro de administración Firepower (FMC)
- Firepower Threat Defense (FTD)
- Virtualización opcional de imágenes

Componentes Utilizados

- Firepower Threat Defense (FTD): 6,5
- FirePOWER Management Center (FMC): 6,5
- Security Services Exchange (SSE)
- Cisco XDR
- Portal de licencias inteligentes

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.

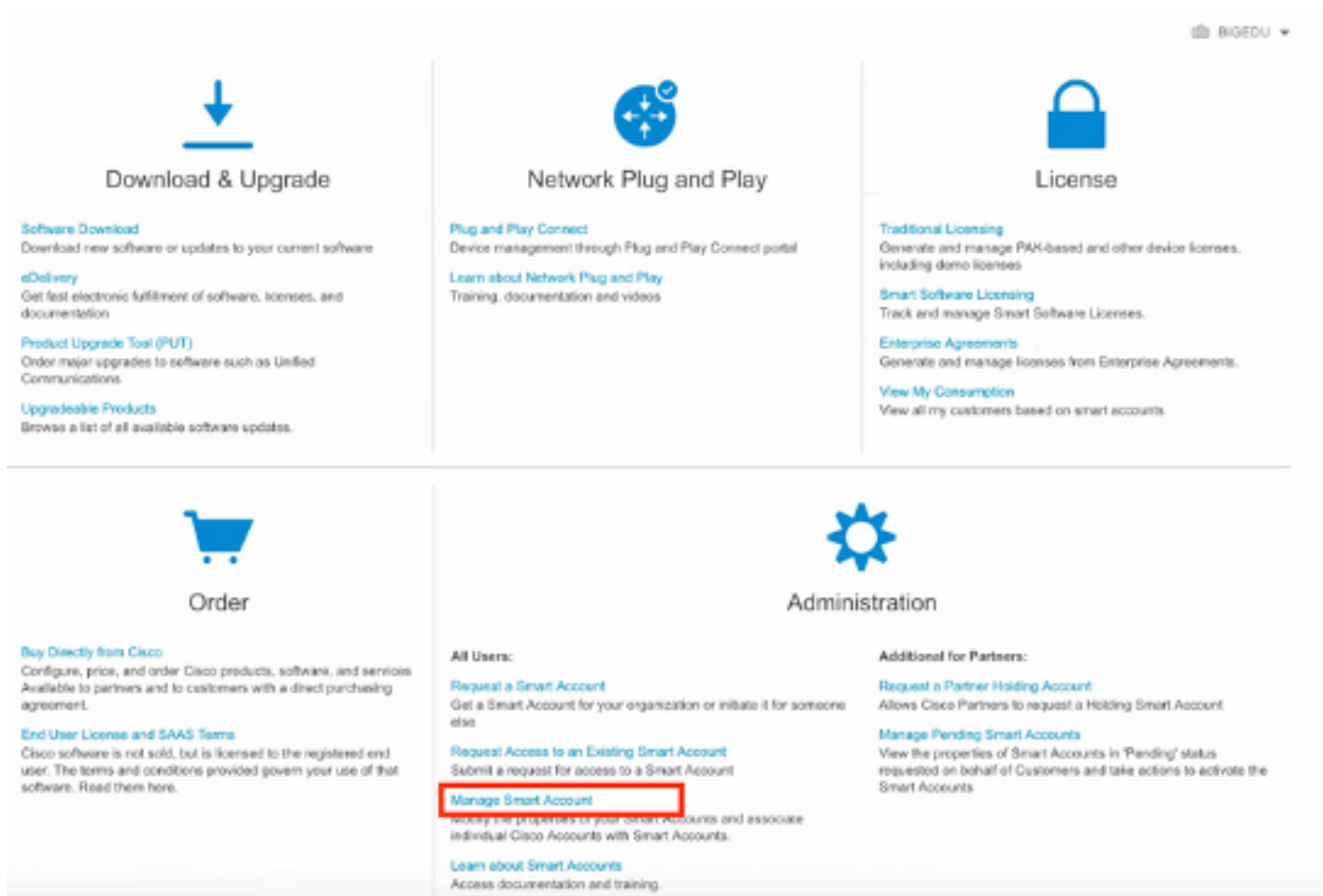
Configurar

Licencias

Funciones de cuenta virtual:

Solo el administrador de la cuenta virtual o el administrador de la cuenta inteligente tiene el privilegio de vincular la cuenta inteligente con la cuenta SSE.

Paso 1. Para validar el rol de cuenta inteligente, navegue hasta software.cisco.com y en el Menú de administración, seleccione Administrar cuenta inteligente.



The screenshot shows the Cisco software.cisco.com administration interface. The top right corner displays the user name 'BIGEDU'. The main content is organized into a grid of six categories, each with an icon and a list of links:

- Download & Upgrade** (Download icon):
 - [Software Download](#): Download new software or updates to your current software
 - [eDelivery](#): Get fast electronic fulfillment of software, licenses, and documentation
 - [Product Upgrade Tool \(PUT\)](#): Order major upgrades to software such as Unified Communications
 - [Upgradeable Products](#): Browse a list of all available software updates.
- Network Plug and Play** (Network icon):
 - [Plug and Play Connect](#): Device management through Plug and Play Connect portal
 - [Learn about Network Plug and Play](#): Training, documentation and videos
- License** (Lock icon):
 - [Traditional Licensing](#): Generate and manage PAK-based and other device licenses, including demo licenses
 - [Smart Software Licensing](#): Track and manage Smart Software Licenses.
 - [Enterprise Agreements](#): Generate and manage licenses from Enterprise Agreements.
 - [View My Consumption](#): View all my customers based on smart accounts
- Order** (Shopping cart icon):
 - [Buy Directly from Cisco](#): Configure, price, and order Cisco products, software, and services Available to partners and to customers with a direct purchasing agreement.
 - [End User License and SAAS Terms](#): Cisco software is not sold, but is licensed to the registered end user. The terms and conditions provided govern your use of that software. Read them here.
- Administration** (Gear icon):
 - All Users:**
 - [Request a Smart Account](#): Get a Smart Account for your organization or initiate it for someone else
 - [Request Access to an Existing Smart Account](#): Submit a request for access to a Smart Account
 - [Manage Smart Account](#): Modify the properties of your Smart Accounts and associate individual Cisco Accounts with Smart Accounts. (This link is circled in red in the image)
 - [Learn about Smart Accounts](#): Access documentation and training.
 - Additional for Partners:**
 - [Request a Partner Holding Account](#): Allows Cisco Partners to request a Holding Smart Account
 - [Manage Pending Smart Accounts](#): View the properties of Smart Accounts in 'Pending' status requested on behalf of Customers and take actions to activate the Smart Accounts

Paso 2. Para validar la función de usuario, navegue hasta Usuarios, y valide que bajo Roles las cuentas están configuradas para tener Virtual Account Administrator, como se muestra en la imagen.

Users

Users | User Groups

[Add Users...](#) [Remove Selected...](#) [Export Selected...](#)

User	Email	Organization	Account Access	Role	User Group	Actions
<input type="checkbox"/> danieber						
<input type="checkbox"/> Daniel Benitez danieben	danieben@cisco.com	Cisco Systems, Inc.	All Virtual Accounts Mex-AMP TAC	Smart Account Administrator Virtual Account Administrator		Remove...

1 User

Paso 3. Asegúrese de que la cuenta virtual que se selecciona para vincular en SSE contenga la licencia para los dispositivos de seguridad si una cuenta que no contiene la licencia de seguridad está vinculada en SSE, los dispositivos de seguridad y el evento no aparecen en el portal de SSE.

Cisco Software Central > Smart Software Licensing

Smart Software Licensing

[Alerts](#) | [Inventory](#) | [Convert to Smart Licensing](#) | [Reports](#) | [Preferences](#) | [On-Prem Accounts](#) | [Activity](#)

Virtual Account: **Mex-AMP TAC** 13 Minor | [Hide Alerts](#)

General | **Licenses** | Product Instances | Event Log

Available Actions [Manage License Tags](#) [License Reservation...](#)

By Name | By Tag


Search by License





<input type="checkbox"/> License	Billing	Purchased	In Use	Balance	Alerts	Actions
<input type="checkbox"/> FPR1010 URL Filtering	Prepaid	10	0	+ 10		Actions
<input type="checkbox"/> FPR4110 Threat Defense Malware Protection	Prepaid	1	0	+ 1		Actions
<input type="checkbox"/> FPR4110 Threat Defense Threat Protection	Prepaid	1	0	+ 1		Actions
<input type="checkbox"/> FPR4110 Threat Defense URL Filtering	Prepaid	1	0	+ 1		Actions
<input type="checkbox"/> HyperFlex Data Platform Enterprise Edition Subscription	Prepaid	2	0	+ 2		Actions
<input type="checkbox"/> ISE Apex Session Licenses	Prepaid	1	0	+ 1		Actions
<input type="checkbox"/> ISE Base Session Licenses	Prepaid	10	0	+ 10		Actions
<input type="checkbox"/> ISE Plus License	Prepaid	10	0	+ 10		Actions
<input type="checkbox"/> Threat Defense Virtual Malware Protection	Prepaid	10	1	+ 9		Actions
<input type="checkbox"/> Threat Defense Virtual Threat Protection	Prepaid	10	1	+ 9		Actions

10 Showing Page 5 of 7 (85 Records) [◀](#) [▶](#)















Paso 4. Para validar que el FMC se registró en la cuenta virtual correcta, vaya a Sistema>Licencias>Licencia inteligente:

Smart License Status

Cisco Smart Software Manager 

Usage Authorization:	 Authorized (Last Synchronized On Jun 10 2020)
Product Registration:	 Registered (Last Renewed On Jun 10 2020)
Assigned Virtual Account:	Mex-AMP TAC
Export-Controlled Features:	Enabled
Cisco Success Network:	Enabled 
Cisco Support Diagnostics:	Disabled 

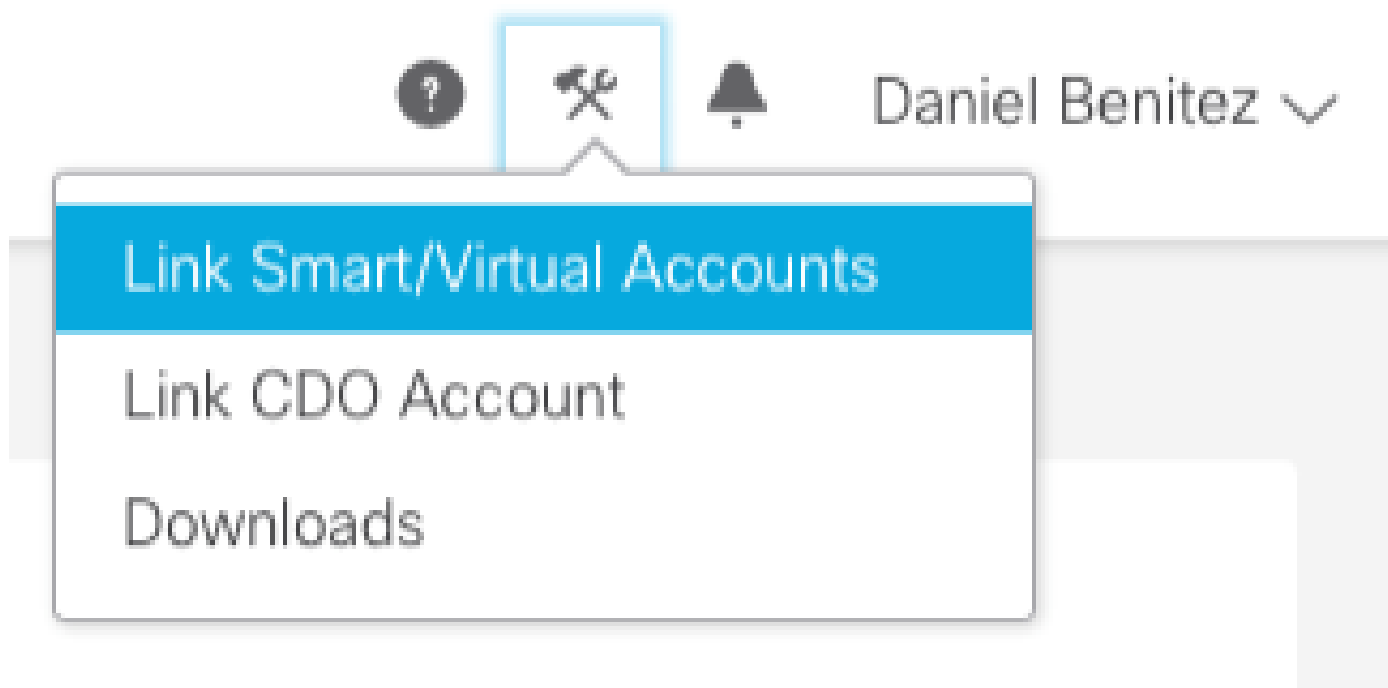
Smart Licenses

License Type/Device Name	License Status
>  Firepower Management Center Virtual (1)	
>  Base (1)	
>  Malware (1)	
>  Threat (1)	
>  URL Filtering (1)	
>  AnyConnect Apex (1)	
>  AnyConnect Plus (1)	
AnyConnect VPN Only (0)	

Note: Container Instances of same blade share feature licenses

Vincule sus cuentas a SSE y registre los dispositivos.

Paso 1. Cuando inicia sesión en su cuenta SSE, debe vincular su cuenta inteligente a su cuenta SSE, para lo cual debe hacer clic en el icono de herramientas y seleccionar Vincular cuentas.



Una vez vinculada la cuenta, verá la cuenta inteligente con todas las cuentas virtuales.

Registre los dispositivos en SSE

Paso 1. Asegúrese de que estas URL están permitidas en su entorno:

Región de Estados Unidos

- api-sse.cisco.com
- eventing-ingest.sse.itd.cisco.com

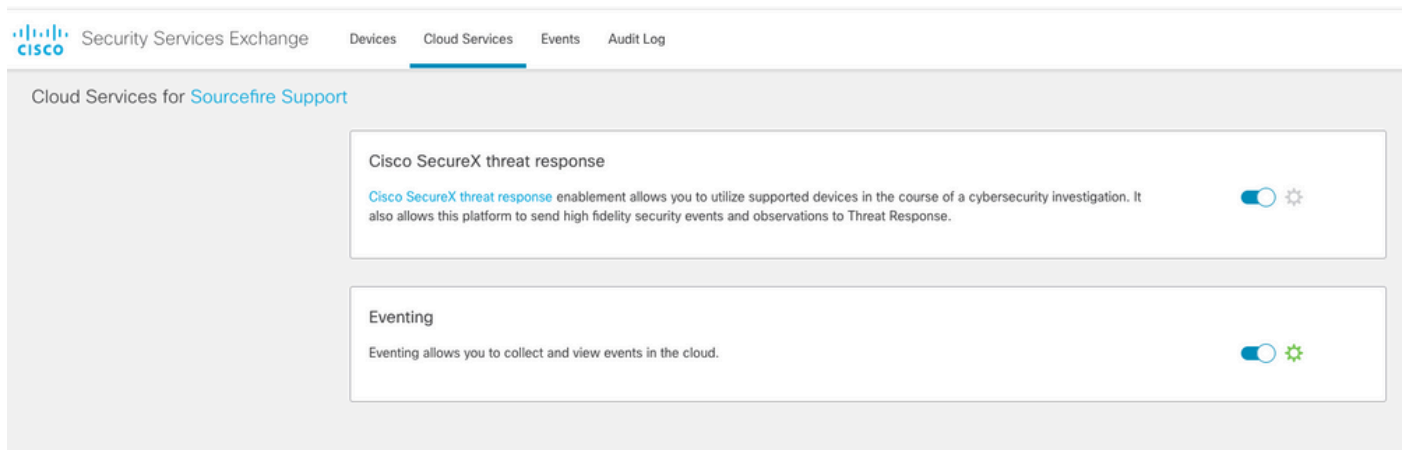
Región UE

- api.eu.sse.itd.cisco.com
- eventing-ingest.eu.sse.itd.cisco.com

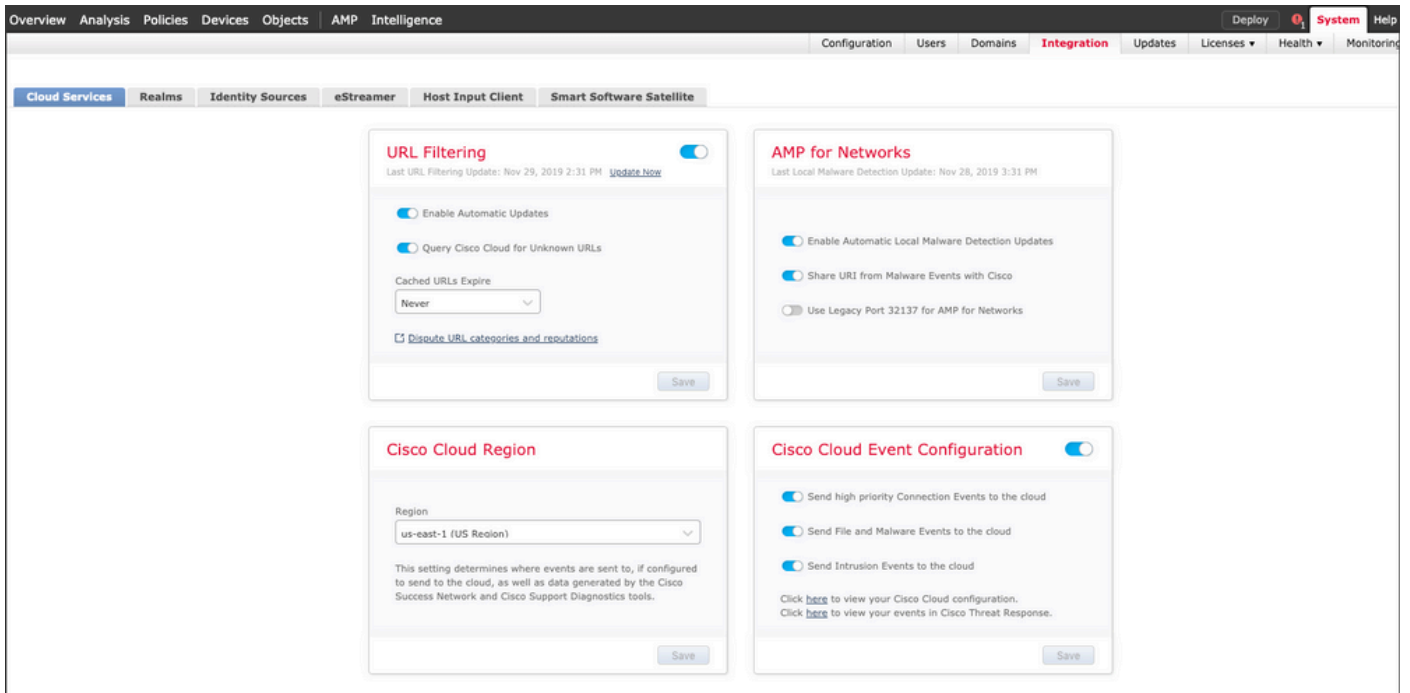
Región APJ

- api.apj.sse.itd.cisco.com
- eventing-ingest.apj.sse.itd.cisco.com

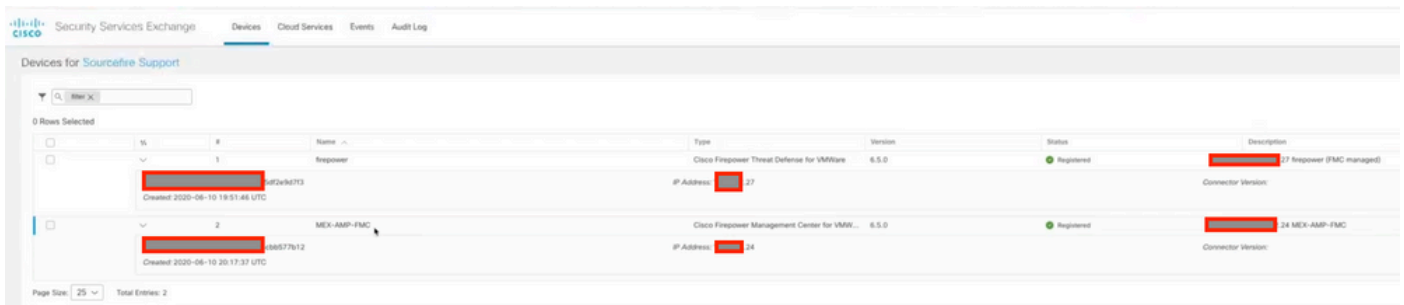
Paso 2. Inicie sesión en el portal de SSE con esta URL <https://admin.sse.itd.cisco.com>, vaya a Cloud Services y habilite las opciones Eventing y Cisco XDR threat response, como se muestra en la siguiente imagen:



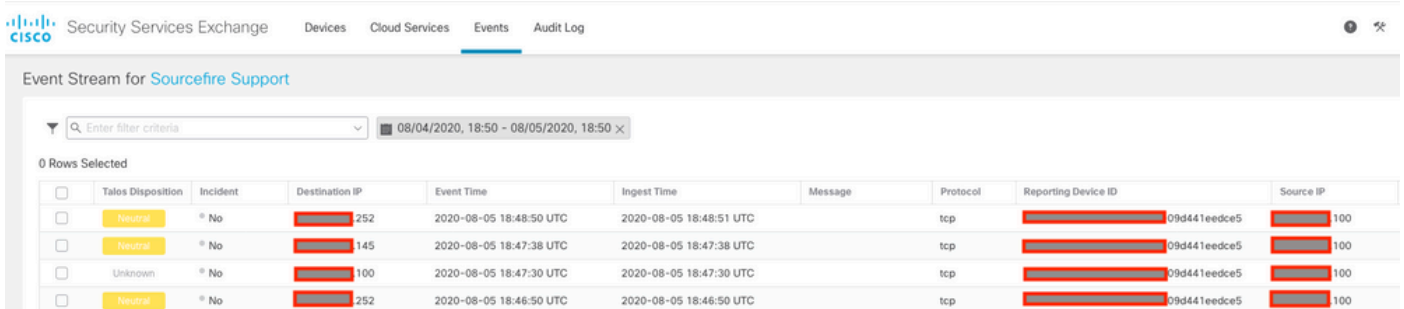
Paso 3. Inicie sesión en Firepower Management Center y navegue hasta System>Integration>Cloud Services, habilite Cisco Cloud Event Configuration y seleccione los eventos que desea enviar a la nube:



Paso 4. Puede volver al portal de SSE y comprobar que ahora puede ver los dispositivos inscritos en SSE:



Los eventos son enviados por los dispositivos FTD, navegue hasta Eventos en el portal SSE para verificar los eventos enviados por los dispositivos a SSE, como se muestra en la imagen:



Verificación

Valide que los FTD generan eventos (malware o intrusiones) para que los eventos de intrusión accedan a Análisis>Archivos>Eventos de malware; para eventos de intrusión, vaya a Análisis>Intrusión>Eventos.

Valide que los eventos estén registrados en el portal SSE como se menciona en el paso 4 de la sección Registro de los dispositivos en SSE.

Valide que se muestre la información en el panel de Cisco XDR o compruebe los registros de la API para ver el motivo de un posible fallo de la API.

Troubleshoot

Detectar problemas de conectividad

Puede detectar problemas de conectividad genéricos desde el archivo `action_queue.log`. En caso de fallo, podrá ver los registros presentes en el archivo:

```
ActionQueueScrape.pl[19094]: [SF::SSE::Enrollment] canConnect: System (/usr/bin/curl -s --connect-timeo
```

En este caso, el código de salida 28 significa que la operación ha agotado el tiempo de espera y debemos verificar la conectividad a Internet. También debe ver el código de salida 6, que significa problemas con la resolución de DNS

Problemas de conectividad debido a la resolución de DNS

Paso 1. Compruebe que la conectividad funciona correctamente.

```
root@ftd01:~# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* getaddrinfo(3) failed for api-sse.cisco.com:443
* Couldn't resolve host 'api-sse.cisco.com'
* Closing connection 0
curl: (6) Couldn't resolve host 'api-sse.cisco.com'
```

Este resultado muestra que el dispositivo no puede resolver la URL <https://api-sse.cisco.com>, en este caso, necesitamos validar que el servidor DNS correcto está configurado, se puede validar con una `nslookup` de la CLI experta:

```
root@ftd01:~# nslookup api-sse.cisco.com
;; connection timed out; no servers could be reached
```

Este resultado muestra que no se alcanza el DNS configurado, para confirmar la configuración de DNS, utilice el comando `show network`:

```

> show network
===== [ System Information ] =====
Hostname           : ftd01
DNS Servers        : x.x.x.10
Management port    : 8305
IPv4 Default route
Gateway            : x.x.x.1

===== [ eth0 ] =====
State              : Enabled
Link               : Up
Channels           : Management & Events
Mode               : Non-Autonegotiation
MDI/MDIX           : Auto/MDIX
MTU                : 1500
MAC Address        : x:x:x:x:9D:A5
----- [ IPv4 ] -----
Configuration      : Manual
Address            : x.x.x.27
Netmask            : 255.255.255.0
Broadcast          : x.x.x.255
----- [ IPv6 ] -----
Configuration      : Disabled

===== [ Proxy Information ] =====
State              : Disabled
Authentication     : Disabled

```

En este ejemplo se utilizó un servidor DNS incorrecto, puede cambiar la configuración DNS con este comando:

```
> configure network dns x.x.x.11
```

Después de que esta conectividad se pueda probar de nuevo y esta vez, la conexión se realiza correctamente.

```

root@ftd01:~# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* Trying x.x.x.66...
* Connected to api-sse.cisco.com (x.x.x.66) port 443 (#0)
* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
* CAfile: none
Cpath: /etc/ssl/certs
* 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 key exchange (12):
* TLSv1.2 (IN), TLS handshake, Request CERT (13):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Certificate (11):

```



```

* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Client hello (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256
* ALPN, server accepted to use http/1.1
* Server certificate:
* subject: C=US; ST=California; L=San Jose; O=Cisco Systems, Inc.; CN=api -sse.cisco.com
* start date: 2019-12-03 20:57:56 GMT
* expire date: 2021-12-03 21:07:00 GMT
* issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID S SL ICA G2
* SSL certificate verify result: self signed certificate in certificate chain (19), continuing anyway.
> GET / HTTP/1.1
> Host: api-sse.cisco.com
> User-Agent: curl/7.44.0
> Accept: */*
>
< HTTP/1.1 403 Forbidden
< Date: Wed, 08 Apr 2020 01:27:55 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 9
< Connection: keep-alive
< Keep-Alive: timeout=5
< ETag: "5e17b3f8-9"
< Cache-Control: no-store
< Pragma: no-cache
< Content-Security-Policy: default-src 'self'
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block
< Strict-Transport-Security: max-age=31536000; includeSubdomains;

```

Problemas de registro en el portal SSE

Tanto FMC como FTD necesitan una conexión a las URL de SSE en su interfaz de gestión. Para probar la conexión, introduzca estos comandos en la CLI de Firepower con acceso raíz:

```
<#root>
```

```
curl -v https://api-sse.cisco.com/providers/sse/services/registration/api/v2/clients --cacert /ngfw/etc/
```

```
curl -v https://est.sco.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
```

```
curl -v https://eventing-ingest.sse.itd.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
```

```
curl -v https://mx01.sse.itd.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
```

La verificación de certificados se puede omitir con este comando:

```
root@ftd01:~# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* Trying x.x.x.66...
* Connected to api-sse.cisco.com (x.x.x.66) port 443 (#0)
* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
* CAfile: none
Cpath: /etc/ssl/certs
* 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 key exchange (12):
* TLSv1.2 (IN), TLS handshake, Request CERT (13):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Certificate (11):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Client hello (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256
* ALPN, server accepted to use http/1.1
* Server certificate:
* subject: C=US; ST=California; L=San Jose; O=Cisco Systems, Inc.; CN=api -sse.cisco.com
* start date: 2019-12-03 20:57:56 GMT
* expire date: 2021-12-03 21:07:00 GMT
* issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID S SL ICA G2
* SSL certificate verify result: self signed certificate in certificate chain (19), continuing anyway.
> GET / HTTP/1.1
> Host: api-sse.cisco.com
> User-Agent: curl/7.44.0
> Accept: */*
>
< HTTP/1.1 403 Forbidden
< Date: Wed, 08 Apr 2020 01:27:55 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 9
< Connection: keep-alive
< Keep-Alive: timeout=5
< ETag: "5e17b3f8-9"
< Cache-Control: no-store
< Pragma: no-cache
< Content-Security-Policy: default-src 'self'
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block
< Strict-Transport-Security: max-age=31536000; includeSubdomains;
```

Nota: Recibe el mensaje 403 Forbidden ya que los parámetros enviados desde la prueba no son los que SSE espera, pero esto demuestra ser suficiente para validar la conectividad.

Verificar el estado del conector

Puede comprobar las propiedades del conector tal y como se muestra.

```
# more /ngfw/etc/sf/connector.properties
registration_interval=180
connector_port=8989
connector_fqdn=api-sse.cisco.com
```

Para verificar la conectividad entre SSConnector y EventHandler puede utilizar este comando, este es un ejemplo de una conexión defectuosa:

```
root@firepower:/etc/sf# netstat -anlp | grep EventHandler_SSEConnector.sock
unix 2 [ ACC ] STREAM LISTENING 3022791165 11204/EventHandler /ngfw/var/sf/run/EventHandler_SSEConnector.sock
```

En el ejemplo de una conexión establecida, puede ver que el estado de la secuencia es conectado:

```
root@firepower:/etc/sf# netstat -anlp | grep EventHandler_SSEConnector.sock
unix 2 [ ACC ] STREAM LISTENING 382276 7741/EventHandler /ngfw/var/sf/run/EventHandler_SSEConnector.sock
unix 3 [ ] STREAM CONNECTED 378537 7741/EventHandler /ngfw/var/sf/run/EventHandler_SSEConnector.sock
```

Verificar los datos enviados al portal SSE y al CTR

Para enviar eventos desde el dispositivo FTD a SEE, debe establecerse una conexión TCP con <https://eventing-ingest.sse.ftd.cisco.com>. Este es un ejemplo de una conexión no establecida entre el portal SSE y el FTD:

```
root@firepower:/ngfw/var/log/connector# lsof -i | grep conn
connector 60815 www 10u IPv4 3022789647 0t0 TCP localhost:8989 (LISTEN)
connector 60815 www 12u IPv4 110237499 0t0 TCP firepower.cisco.com:53426->ec2-100-25-93-234.compute-1.amazonaws.com:443
```

En los registros de connector.log:

```
time="2020-04-13T14:34:02.88472046-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to https://eventing-ingest.sse.ftd.cisco.com:443"
time="2020-04-13T14:38:18.244707779-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to https://eventing-ingest.sse.ftd.cisco.com:443"
time="2020-04-13T14:42:42.564695622-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to https://eventing-ingest.sse.ftd.cisco.com:443"
time="2020-04-13T14:47:48.484762429-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to https://eventing-ingest.sse.ftd.cisco.com:443"
time="2020-04-13T14:52:38.404700083-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to https://eventing-ingest.sse.ftd.cisco.com:443"
```

Nota: Se ha observado que las direcciones IP mostradas x.x.x.246 y 1x.x.x.246 pertenecen

a <https://eventing-ingest.sse.itd.cisco.com> deben cambiar; por este motivo, se recomienda permitir el tráfico al portal SSE en función de la URL en lugar de las direcciones IP.

Si no se establece esta conexión, los eventos no se envían al portal SSE. Este es un ejemplo de una conexión establecida entre el FTD y el portal SSE:

```
root@firepower:# lsof -i | grep conn
connector 13277  www  10u  IPv4 26077573      0t0  TCP localhost:8989 (LISTEN)
connector 13277  www  19u  IPv4 26077679      0t0  TCP x.x.x.200:56495->ec2-35-172-147-246.compute-1.
```

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).