將SecureX與Firepower威脅防禦(FTD)整合並進行故障排除

目錄

簡介
必要條件
需求
採用元件
設定
授權
將您的帳戶連結到SSE並註冊裝置。
向SSE註冊裝置
在SecureX上配置自定義儀表板
驗證
疑難排解
檢測連線問題
DNS解析引起的連線問題
SSE門戶的註冊問題
驗證SSEConnector狀態
驗證傳送到SSE門戶和CTR的資料
影片

簡介

SecureXFirepower Firepower(FTD)

必要條件

需求

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)
-

採用元件

- Firepower(FTD)- 6.5
- Firepower(FMC)- 6.5
- (SSE)
- SecureX

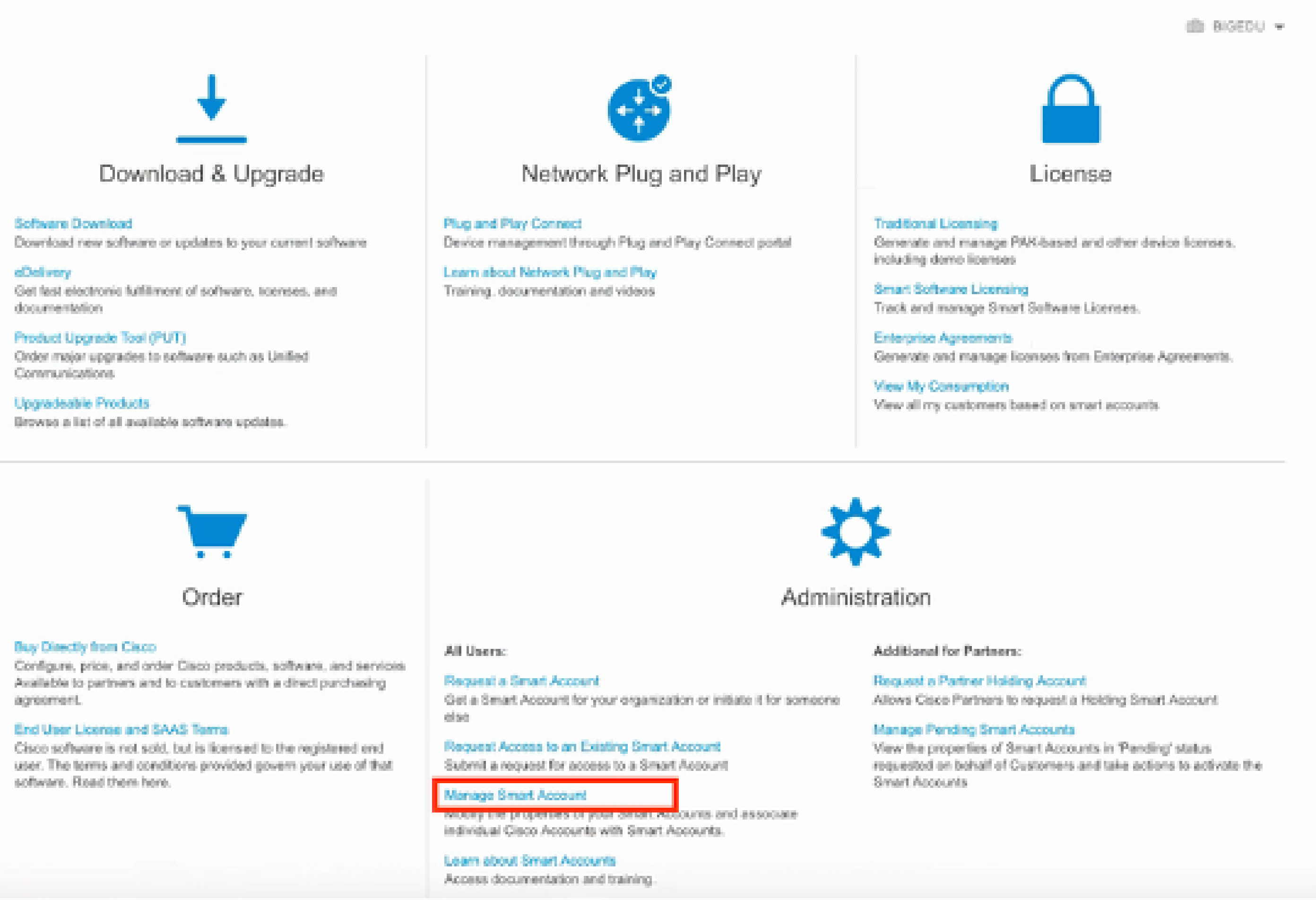
設定

授權

虛擬帳戶角色：

只有虛擬帳戶管理員或智慧帳戶管理員有權將智慧帳戶與SSE帳戶連結。

步驟1。若要驗證智慧帳戶角色，請導覽至**software.cisco.com**，然後在**Administration Menu**下選擇**Manage Smart Account**。



BIGEDU

Download & Upgrade

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

Plug and Play Connect
Device management through Plug and Play Connect portal

Learn about Network Plug and Play
Training, documentation and videos

License

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

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

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.

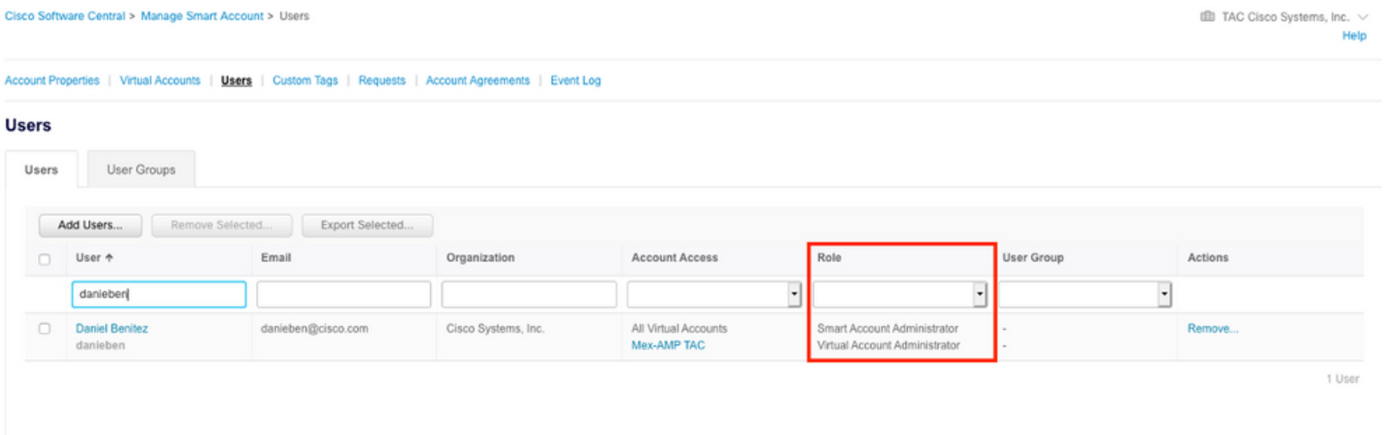
Learn about Smart Accounts
Access documentation and training.

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

步驟2。若要驗證使用者角色，請導覽至**Users**，並驗證在「Roles」下，帳戶是否設為虛擬帳戶管理員，如下圖所示。



Cisco Software Central > Manage Smart Account > Users

TAC Cisco Systems, Inc.
Help

Account Properties | Virtual Accounts | **Users** | Custom Tags | Requests | Account Agreements | Event Log

Users

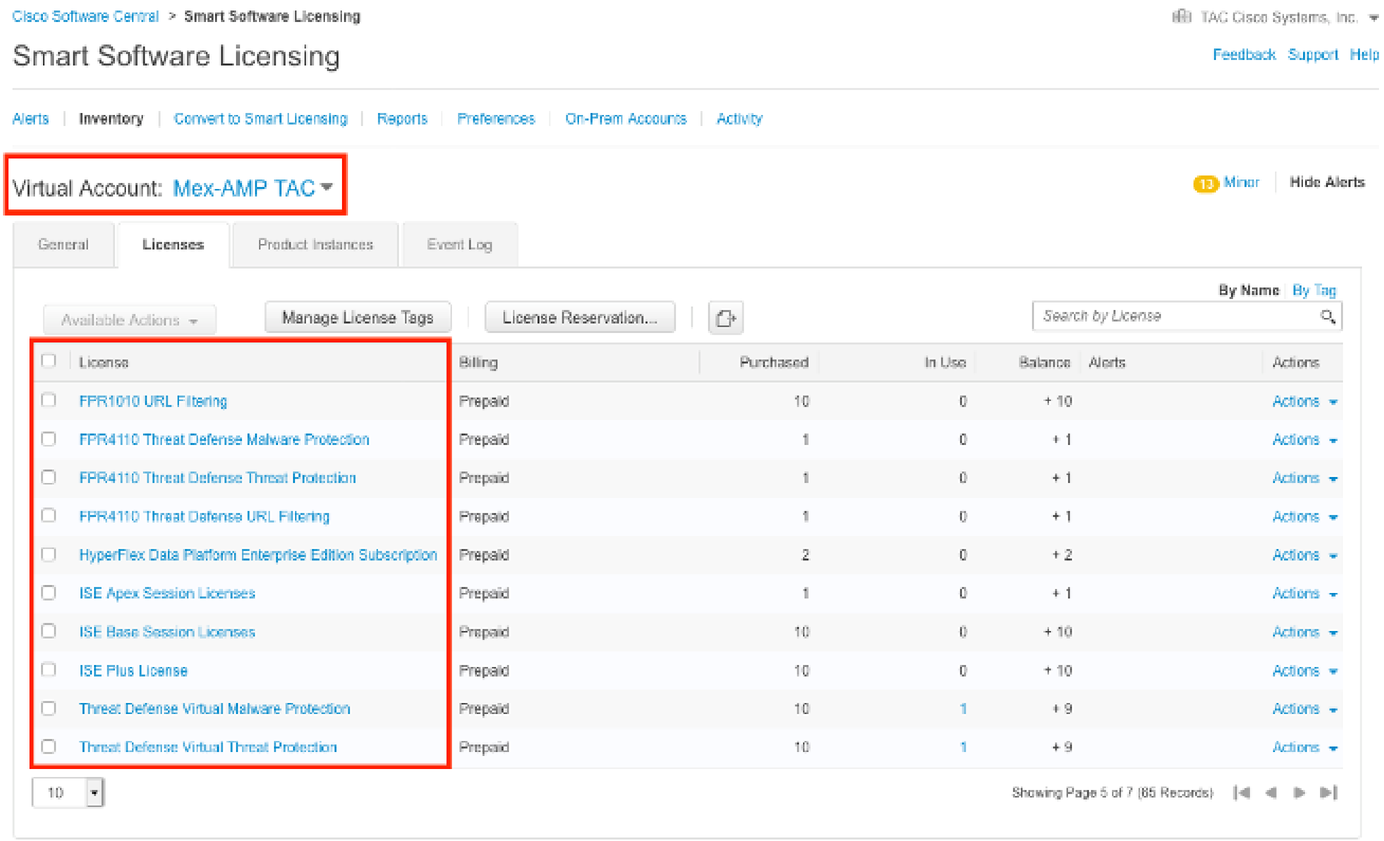
Users | User Groups

Add Users... | Remove Selected... | Export Selected...

☐	User ↑	Email	Organization	Account Access	Role	User Group	Actions
	danieben						
☐	Daniel Benitez danieben	danieben@cisco.com	Cisco Systems, Inc.	All Virtual Accounts Mex-AMP TAC	Smart Account Administrator Virtual Account Administrator	- -	Remove...

1 User

步驟3.確保選擇在SSE上鍊接的虛擬帳戶包含安全裝置的許可證，前提是不包含安全許可證的帳戶連結在SSE上，安全裝置和事件沒有顯示在SSE門戶上。



Cisco Software Central > Smart Software Licensing

TAC Cisco Systems, Inc.

Smart Software Licensing

Feedback Support Help

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

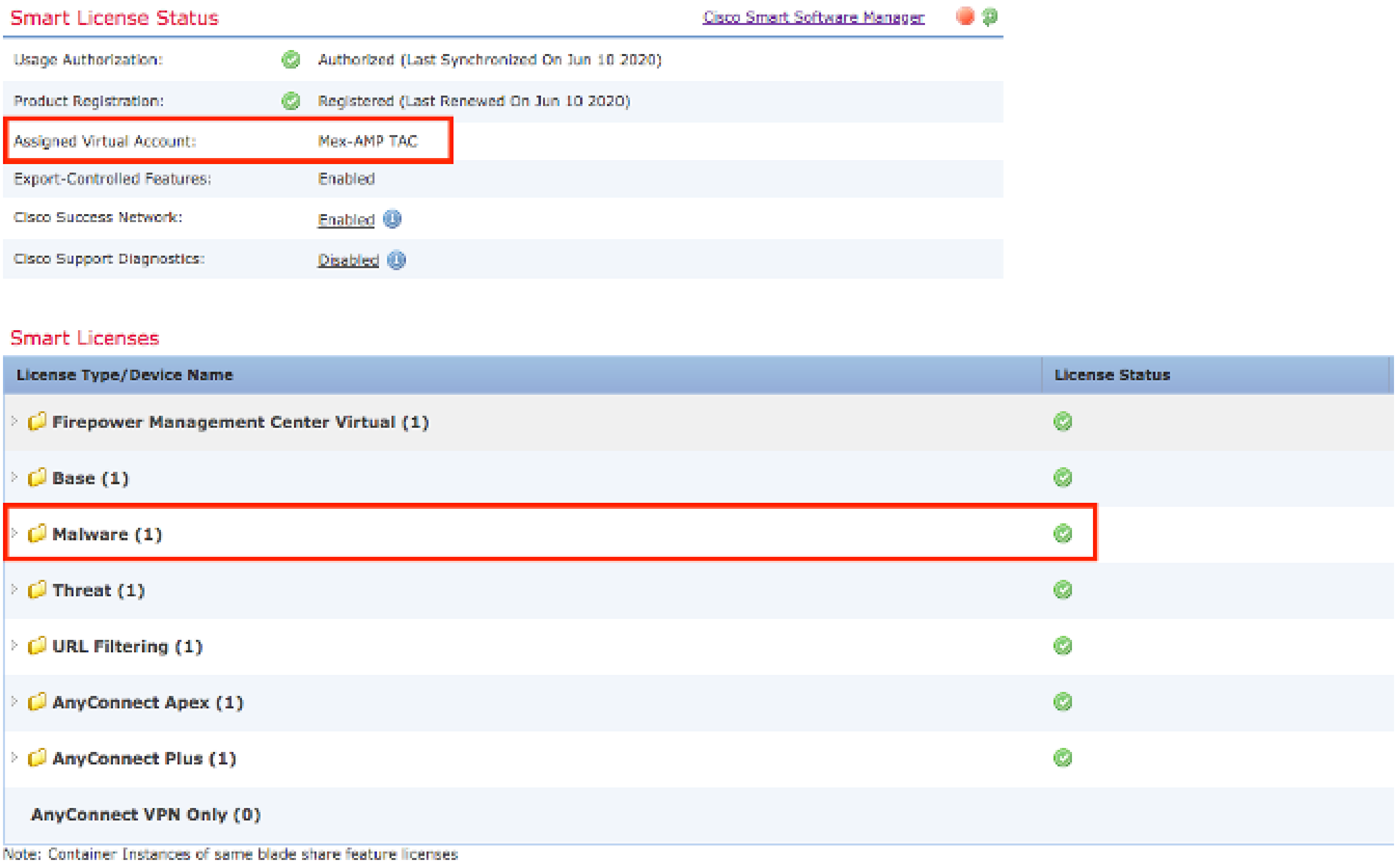
Search by License

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

10

Showing Page 5 of 7 (65 Records)

步驟4.要驗證FMC是否已註冊到正確的虛擬帳戶，請導航到**System>Licenses>Smart License:**



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

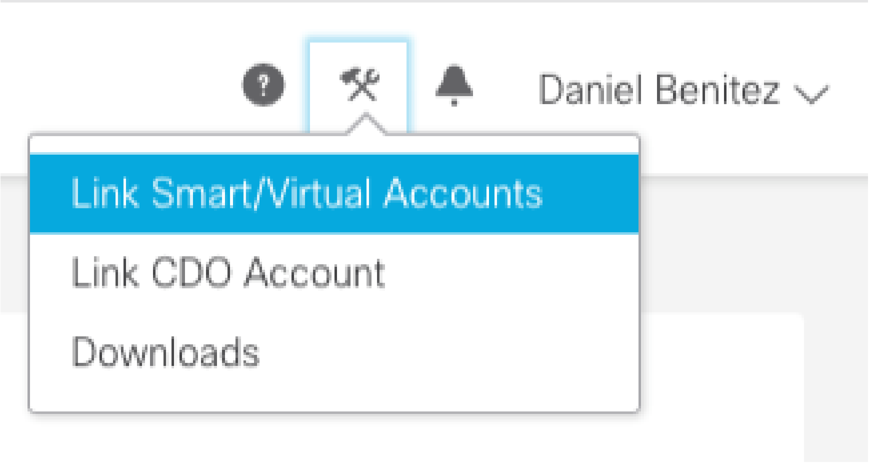
Smart Licenses

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

將您的帳戶連結到SSE並註冊裝置。

步驟1。當您登入您的SSE帳戶時，您必須將您的智慧帳戶連結到SSE帳戶，為此，您需要按一下工具圖示並選擇**連結帳戶**。



帳戶連結後，您會看到智慧帳戶及其上的所有虛擬帳戶。

向SSE註冊裝置

步驟1.確保您的環境中允許這些URL:

美國地區

- api-sse.cisco.com

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

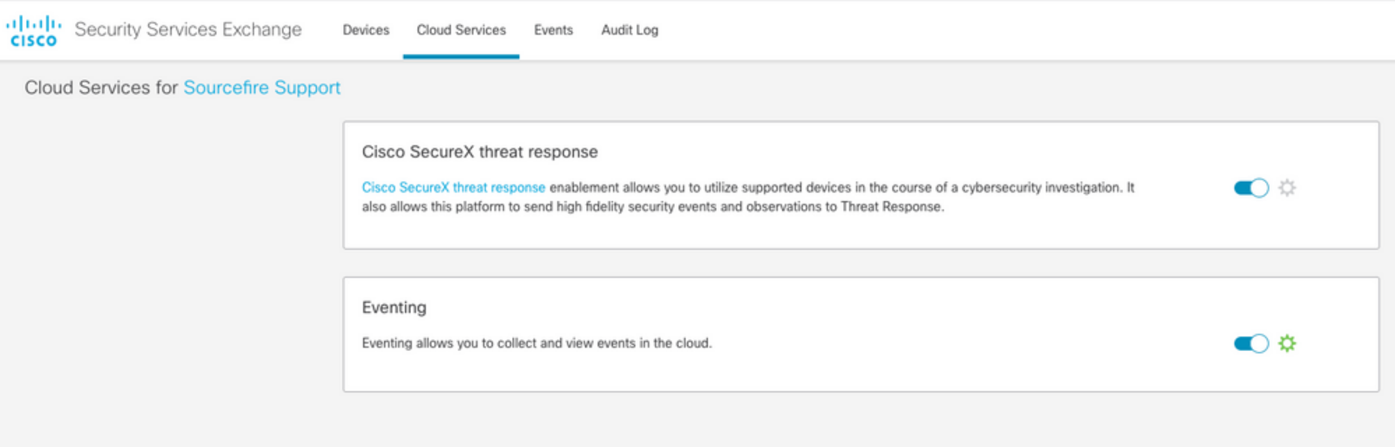
歐盟地區

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

亞太及日本地區

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

步驟2.使用此URL https://admin.sse.itd.cisco.com登入SSE入口網站，導覽至**Cloud Services**，並啟用**Eventing**和**Cisco SecureX威脅響應**選項，如下圖所示：



Cloud Services for Sourcefire Support

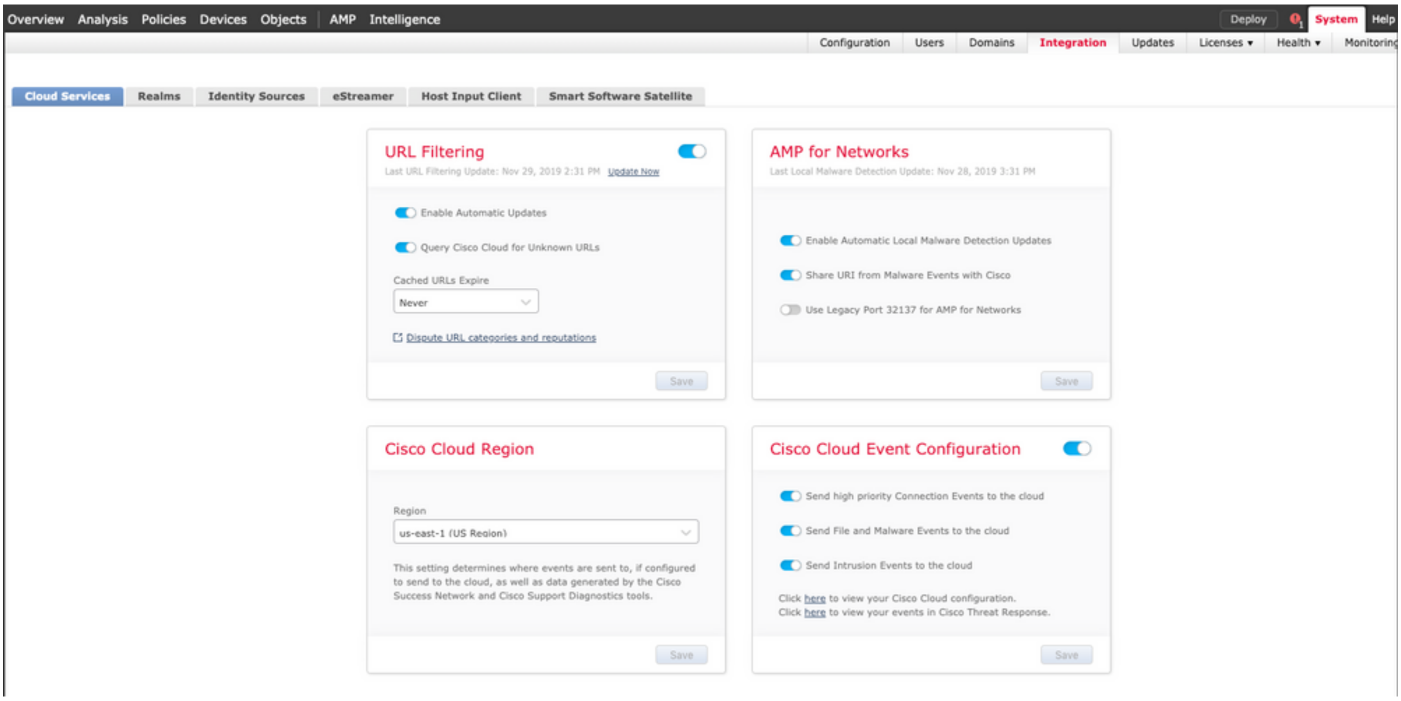
Cisco SecureX threat response

Cisco SecureX threat response enablement allows you to utilize supported devices in the course of a cybersecurity investigation. It also allows this platform to send high fidelity security events and observations to Threat Response.

Eventing

Eventing allows you to collect and view events in the cloud.

步驟3.登入到Firepower管理中心並導航到**System>Integration>Cloud Services**，啟用**Cisco Cloud Event Configuration**，然後選擇要傳送到雲的事件：



URL Filtering

Last URL Filtering Update: Nov 29, 2019 2:31 PM Update Now

Enable Automatic Updates

Query Cisco Cloud for Unknown URLs

Cached URLs Expire: Never

Dispute URL categories and reputations

AMP for Networks

Last Local Malware Detection Update: Nov 28, 2019 3:31 PM

Enable Automatic Local Malware Detection Updates

Share URI from Malware Events with Cisco

Use Legacy Port 32137 for AMP for Networks

Cisco Cloud Region

Region: us-east-1 (US Region)

This setting determines where events are sent to, if configured to send to the cloud, as well as data generated by the Cisco Success Network and Cisco Support Diagnostics tools.

Cisco Cloud Event Configuration

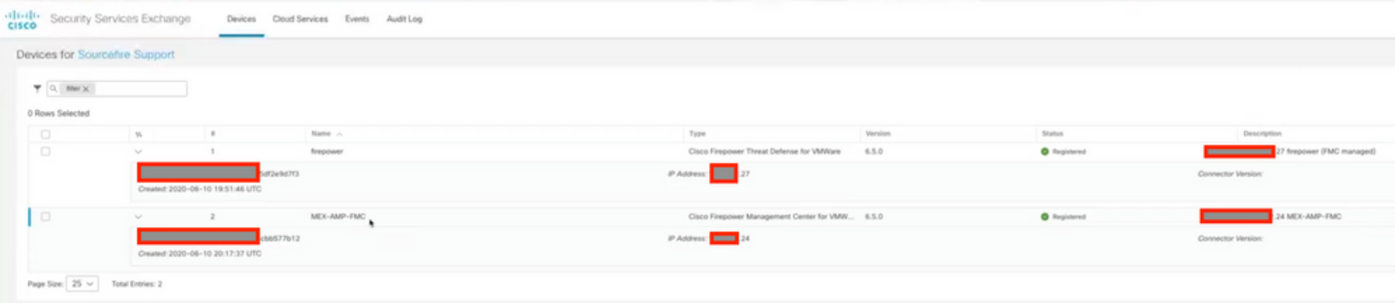
Send high priority Connection Events to the cloud

Send File and Malware Events to the cloud

Send Intrusion Events to the cloud

Click here to view your Cisco Cloud configuration.
Click here to view your events in Cisco Threat Response.

步驟4.您可以返回SSE門戶並驗證現在是否可以看到在SSE上註冊的裝置：



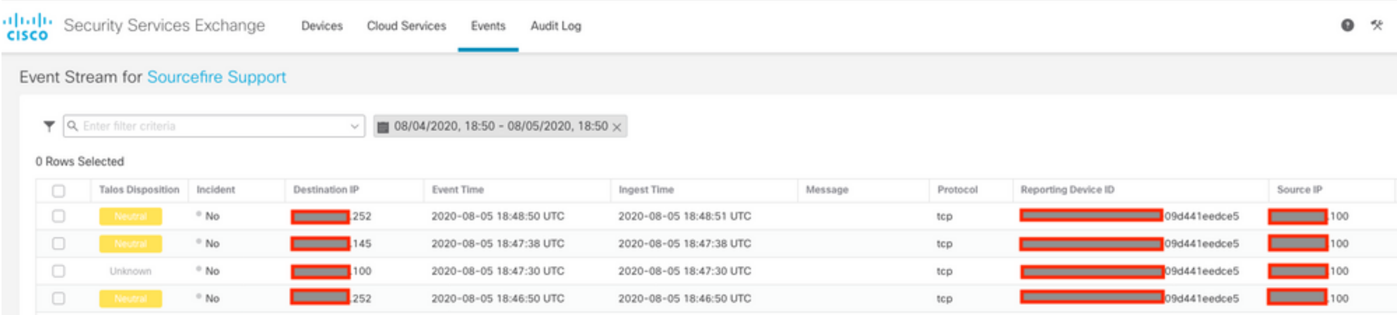
Devices for Sourcefire Support

0 Rows Selected

□	%	#	Name	Type	Version	Status	Description
□	⌄	1	firepower	Cisco Firepower Threat Defense for VMWare	6.5.0	● Registered	[redacted].27 firepower (FMC managed)
	[redacted]5df2e9d7f3 Created: 2020-06-10 19:51:46 UTC			IP Address: [redacted].27			Connector Version:
□	⌄	2	MEX-AMP-FMC	Cisco Firepower Management Center for VMW...	6.5.0	● Registered	[redacted].24 MEX-AMP-FMC
	[redacted]cbb577b12 Created: 2020-06-10 20:17:37 UTC			IP Address: [redacted].24			Connector Version:

Page Size: 25 Total Entries: 2

Events由FTD裝置傳送，請導覽至SSE入口網站上的**Events**，以驗證裝置傳送至SSE的事件，如下圖所示：



Event Stream for Sourcefire Support

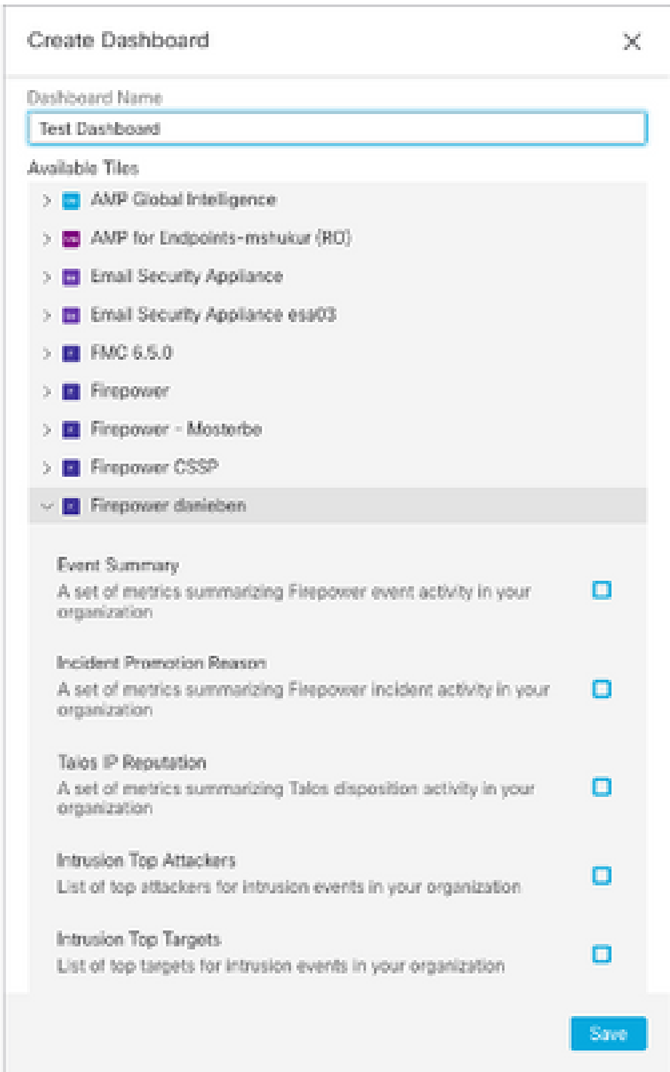
08/04/2020, 18:50 - 08/05/2020, 18:50

0 Rows Selected

□	Talos Disposition	Incident	Destination IP	Event Time	Ingest Time	Message	Protocol	Reporting Device ID	Source IP
□	Neutral	No	[redacted].252	2020-08-05 18:48:50 UTC	2020-08-05 18:48:51 UTC		tcp	[redacted]09d441eedce5	[redacted].100
□	Neutral	No	[redacted].145	2020-08-05 18:47:38 UTC	2020-08-05 18:47:38 UTC		tcp	[redacted]09d441eedce5	[redacted].100
□	Unknown	No	[redacted].100	2020-08-05 18:47:30 UTC	2020-08-05 18:47:30 UTC		tcp	[redacted]09d441eedce5	[redacted].100
□	Neutral	No	[redacted].252	2020-08-05 18:46:50 UTC	2020-08-05 18:46:50 UTC		tcp	[redacted]09d441eedce5	[redacted].100

在SecureX上配置自定義儀表板

步驟1。若要建立儀表板，請按一下**+新建儀表板**圖示，選擇要用於儀表板的名稱和磁貼，如下圖所示：



Create Dashboard ✕

Dashboard Name

Test Dashboard

Available Tiles

- › AMP Global Intelligence
- › AMP for Endpoints-mshukur (RO)
- › Email Security Appliance
- › Email Security Appliance esa03
- › FMC 6.5.0
- › Firepower
- › Firepower - Mosterbe
- › Firepower CSSP
- ⌄ Firepower danieben

Event Summary
A set of metrics summarizing Firepower event activity in your organization ☐

Incident Promotion Reason
A set of metrics summarizing Firepower incident activity in your organization ☐

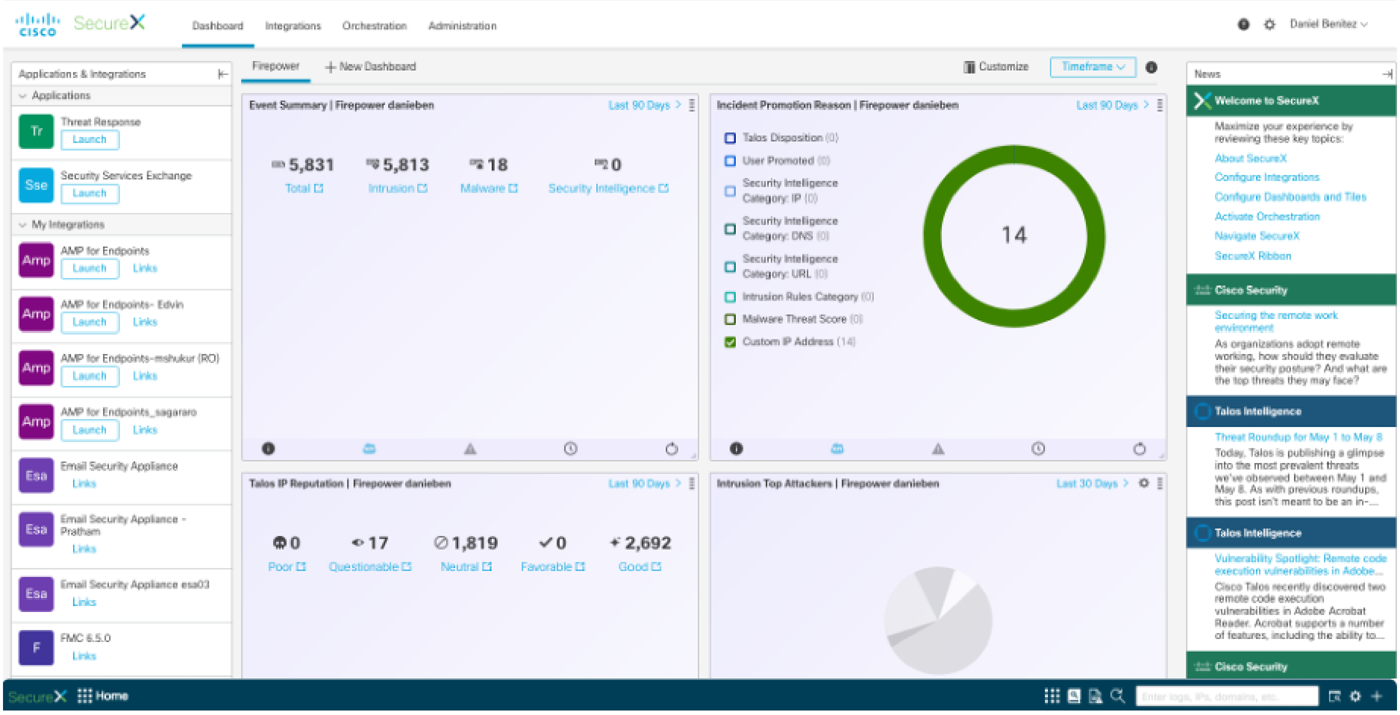
Talos IP Reputation
A set of metrics summarizing Talos disposition activity in your organization ☐

Intrusion Top Attackers
List of top attackers for intrusion events in your organization ☐

Intrusion Top Targets
List of top targets for intrusion events in your organization ☐

Save

第2步：在此之後，您可以看到從SSE填充的儀表板資訊，您可以選擇任何檢測到的威脅，然後啟動SSE門戶，並在其上使用事件型別篩選器：



Applications & Integrations

Applications
- Threat Response — Launch
- Security Services Exchange — Launch

My Integrations
- AMP for Endpoints — Launch Links
- AMP for Endpoints- Edvin — Launch Links
- AMP for Endpoints-mshukur (RO) — Launch Links
- AMP for Endpoints_sagararo — Launch Links
- Email Security Appliance — Links
- Email Security Appliance - Pratham — Links
- Email Security Appliance esa03 — Links
- FMC 6.5.0 — Links

Firepower | + New Dashboard | Customize | Timeframe

Event Summary | Firepower danieben — Last 90 Days

5,831	5,813	18	0
Total	Intrusion	Malware	Security Intelligence

Incident Promotion Reason | Firepower danieben — Last 90 Days

- ☐ Talos Disposition (0)
- ☐ User Promoted (0)
- ☐ Security Intelligence Category: IP (0)
- ☐ Security Intelligence Category: DNS (0)
- ☐ Security Intelligence Category: URL (0)
- ☐ Intrusion Rules Category (0)
- ☐ Malware Threat Score (0)
- ☑ Custom IP Address (14)

14

Talos IP Reputation | Firepower danieben — Last 90 Days

0	17	1,819	0	2,692
Poor	Questionable	Neutral	Favorable	Good

Intrusion Top Attackers | Firepower danieben — Last 30 Days

News

Welcome to SecureX
Maximize your experience by reviewing these key topics:
About SecureX
Configure Integrations
Configure Dashboards and Tiles
Activate Orchestration
Navigate SecureX
SecureX Ribbon

Cisco Security
Securing the remote work environment
As organizations adopt remote working, how should they evaluate their security posture? And what are the top threats they may face?

Talos Intelligence
Threat Roundup for May 1 to May 8
Today, Talos is publishing a glimpse into the most prevalent threats we've observed between May 1 and May 8. As with previous roundups, this post isn't meant to be an in-...

Talos Intelligence
Vulnerability Spotlight: Remote code execution vulnerabilities in Adobe...
Cisco Talos recently discovered two remote code execution vulnerabilities in Adobe Acrobat Reader. Acrobat supports a number of features, including the ability to...

Cisco Security

驗證

驗證FTD是否生成事件（惡意軟體或入侵），對於入侵事件，請導航至 **Analysis>Files>Malware Events，對於入侵事件，請導覽至Analysis>Intrusion>Events。**

驗證在**將裝置註冊到SSE** 部分第4步中提到的在SSE門戶上註冊的事件.

驗證資訊是否顯示在SecureX控制面板上，或者檢查API日誌，以便檢視可能的API失敗的原因。

疑難排解

檢測連線問題

可以從action_queue.log檔案中檢測一般連線問題。在出現故障時，您可以看到檔案中存在以下日誌：

```
ActionQueueScrape.pl[19094]: [SF::SSE::Enrollment] canConnect: System (/usr/bin/curl -s --
connect-timeout 10 -m 20 -L --max-redirs 5 --max-filesize 104857600 --capath
/ngfw/etc/sf/keys/fireamp/thawte_roots -f
https://api.eu.sse.itd.cisco.com/providers/sse/api/v1/regions) Failed, curl returned 28 at
/ngfw/usr/local/sf/lib/perl/5.10.1/SF/System.pmline 10477.
```

在這種情況下，退出代碼28表示操作超時，我們應該檢查與Internet的連線。您還可能看到退出代碼6，這意味著存在DNS解析問題

DNS解析引起的連線問題

步驟1.檢查連線是否正常工作。

```
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'
```

上面的輸出顯示，裝置無法解析URL https://api-sse.cisco.com，在這種情況下，我們需要驗證是否配置了正確的DNS伺服器，它可以通過專家CLI中的nslookup進行驗證：

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

上面的輸出顯示未到達配置的DNS，為了確認DNS設定，請使用**show network**命令：

```
> 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
```

在此示例中，使用了錯誤的DNS伺服器，您可以使用以下命令更改DNS設定：

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

重新測試此連線後，連線成功。

```
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
CApath: /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 c hain (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;
```

SSE門戶的註冊問題

FMC和FTD都需要連線到其管理介面上的SSE URL，要測試連線，請在具有根訪問許可權的Firepower CLI上輸入以下命令：

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

可以使用以下命令繞過證書檢查：

```
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
CApath: /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 c hain (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;
```

> **附註**：您會收到403 Forbidden報文，因為從測試傳送的引數不是SSE期望的，但這一點足以驗證連通性。

驗證SSEConnector狀態

您可以驗證聯結器屬性，如圖所示。

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

為了檢查SSConnector和EventHandler之間的連線，可以使用此命令，以下是連線錯誤的示例：

```
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
```

在已建立的連線的範例中，可以看到串流狀態為已連線：

```
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.soc
```

驗證傳送到SSE門戶和CTR的資料

若要從FTD裝置傳送事件以瞭解TCP連線需要使用https://eventing-ingest.sse.itd.cisco.com建立，以下是SSE入口和FTD之間未建立連線的範例：

```
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:https (SYN_SENT)
```

在connector.log日誌中：

```
time="2020-04-13T14:34:02.88472046-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp x.x.x.246:443: getsockopt: connection timed out"
time="2020-04-13T14:38:18.244707779-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp x.x.x.234:443: getsockopt: connection timed out"
```

```
time="2020-04-13T14:42:42.564695622-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp x.x.x.246:443: getsockopt: connection timed out"
time="2020-04-13T14:47:48.484762429-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp x.x.x.234:443: getsockopt: connection timed out"
time="2020-04-13T14:52:38.404700083-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp x.x.x.234:443: getsockopt: connection timed out"
```

> **附註**：請注意，顯示的x.x.x.246和1x.x.x.246屬於https://eventing-ingest.sse.itd.cisco.com的IP地址可能會更改，因此建議允許基於URL而非IP地址的流量進入SSE門戶。

如果此連線未建立，則事件不會傳送到SSE門戶。以下是FTD和SSE輸入網站之間已建立的連線的範例：

```
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.amazonaws.com:https (ESTABLISHED)
```

影片