將Cisco XDR與Firepower威脅防禦(FTD)整合並排除故障

目錄

簡介

本檔案介紹將Cisco XDR與Firepower Firepower威脅防禦(FTD)整合、驗證和故障排除所需的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)
- 映像的可選虛擬化

採用元件

- Firepower威脅防禦(FTD)- 6.5
- Firepower管理中心(FMC)- 6.5
- 安全服務交換(SSE)
- Cisco XDR
- 智慧授權入口網站

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

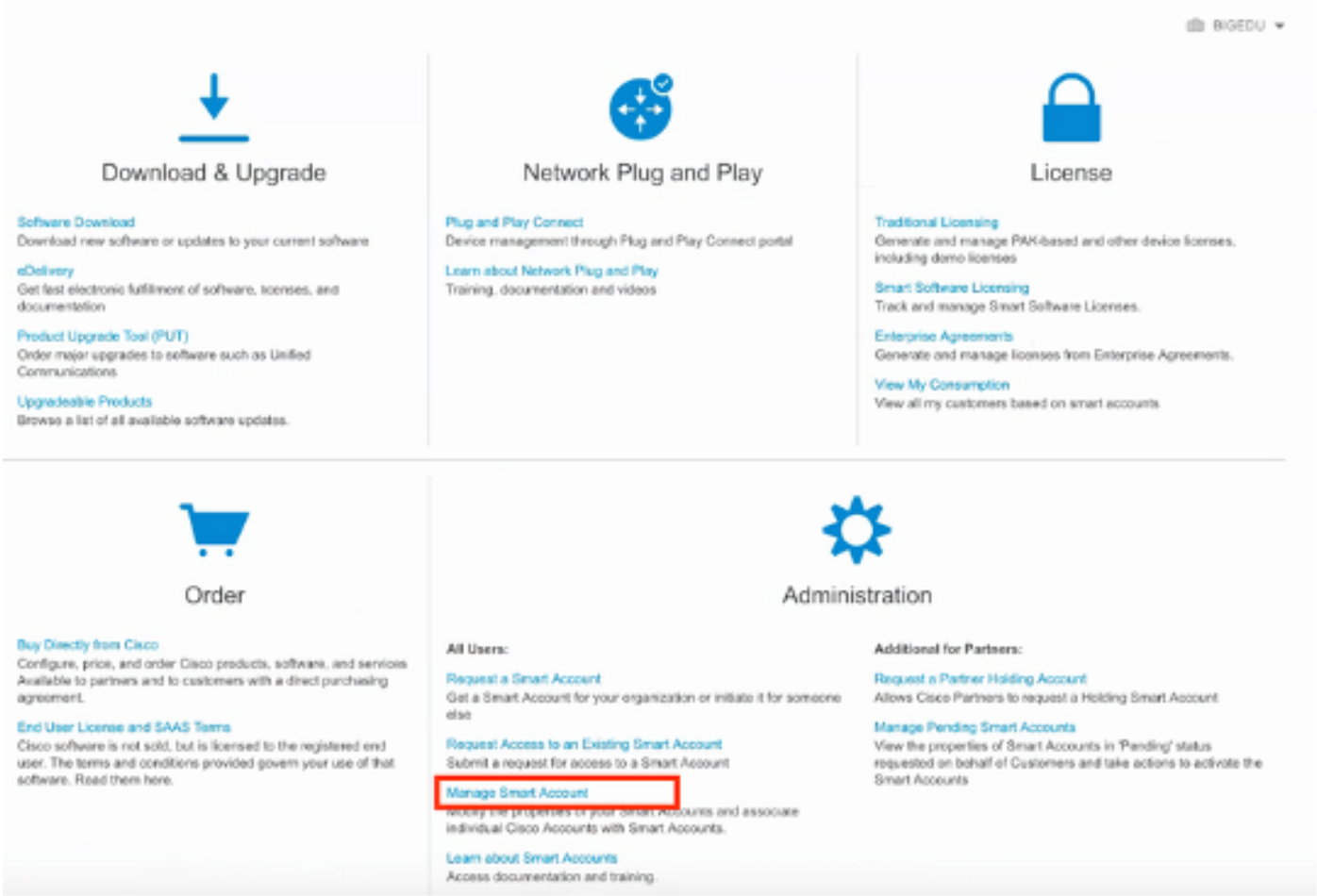
設定

授權

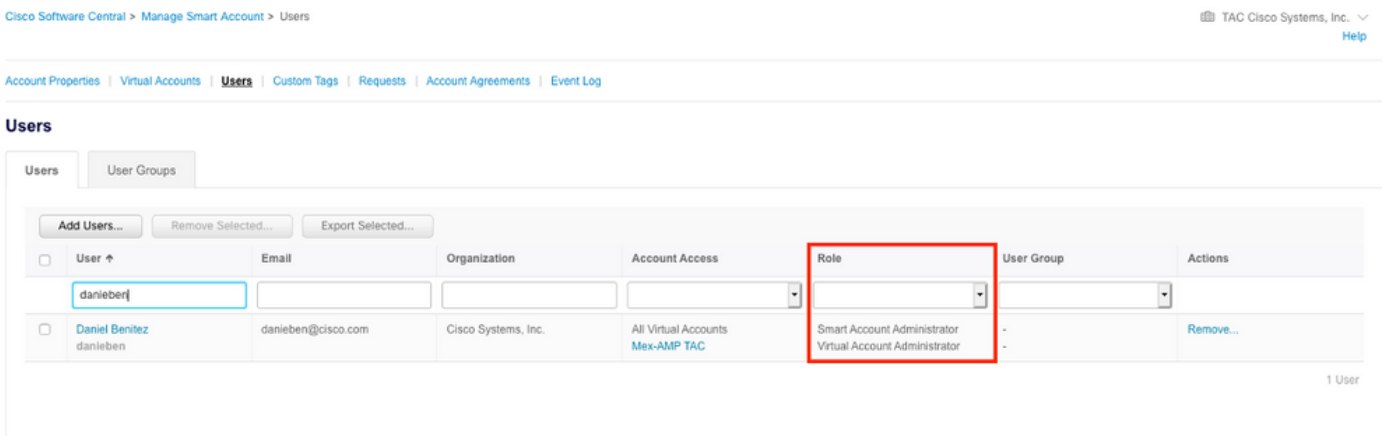
虛擬帳戶角色：

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。

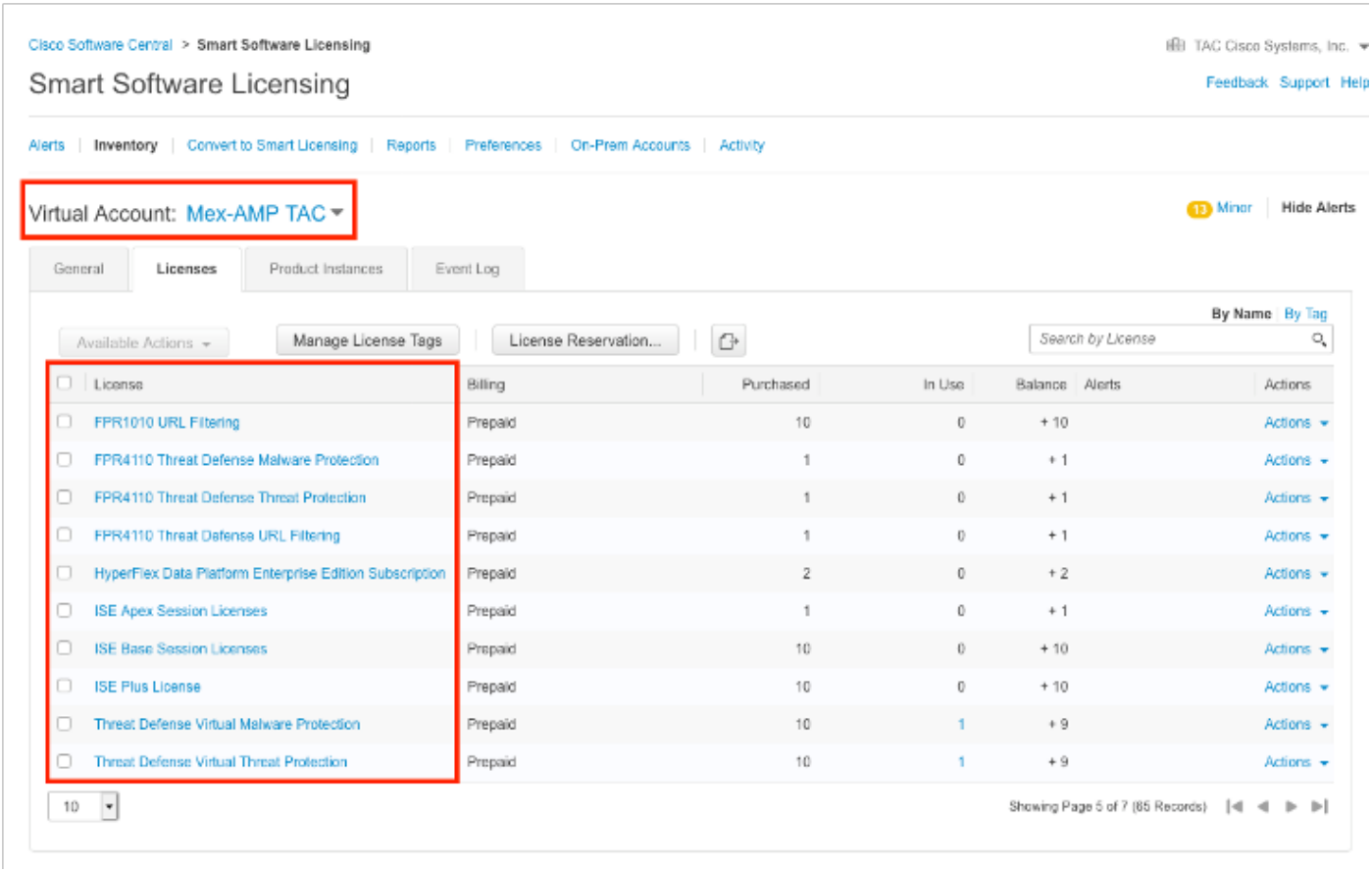
步驟1.若要驗證智慧帳戶角色，請導航到software.cisco.com，然後在Administration Menu下選擇Manage Smart Account。



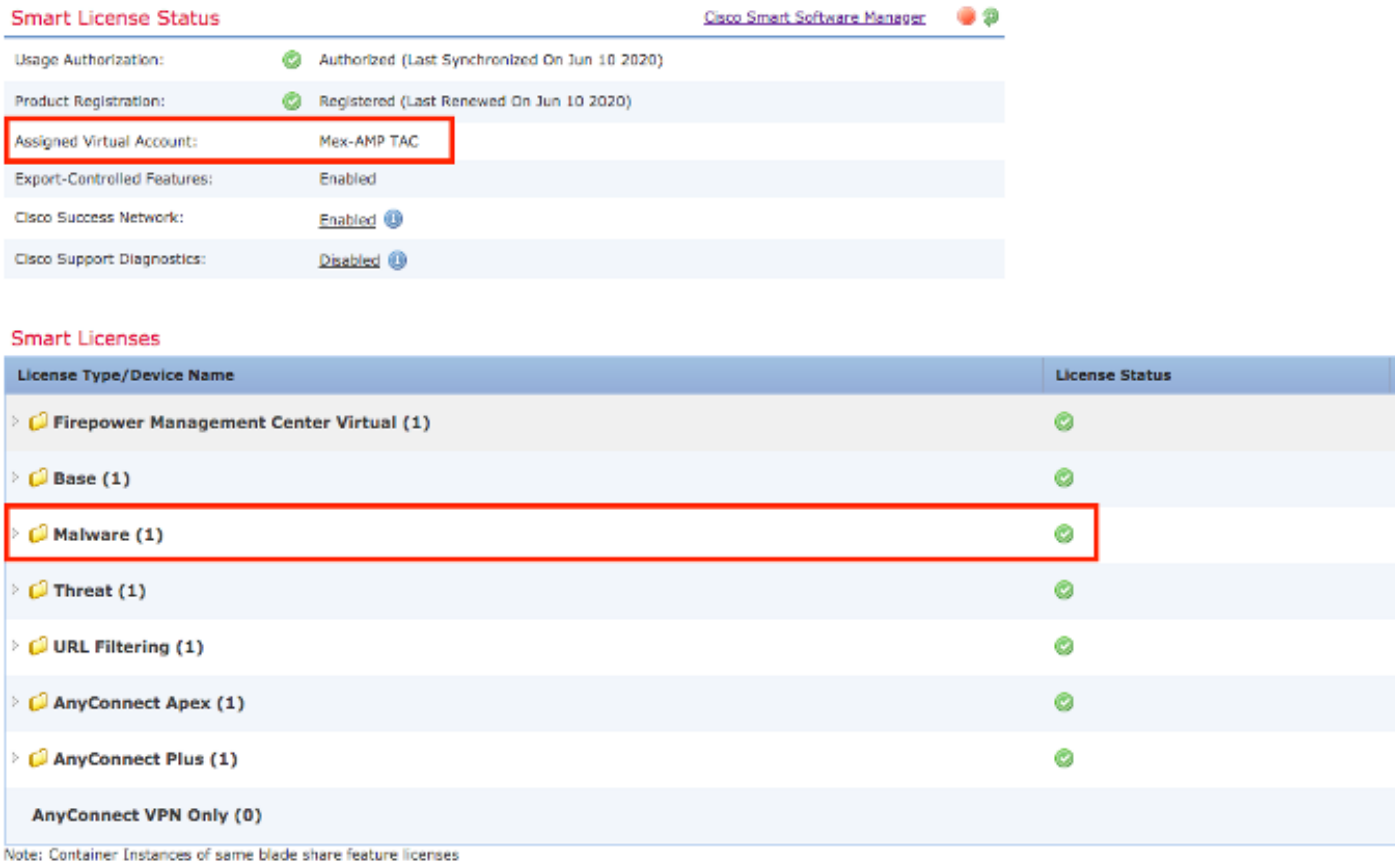
步驟2.若要驗證使用者角色，請導航到使用者，並驗證在「角色」下，帳戶是否設定為具有虛擬帳戶管理員，如下圖所示。



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，如果不包含安全許可證的帳戶在SSE上鍊接，則安全裝置和事件不會顯示在SSE門戶上。

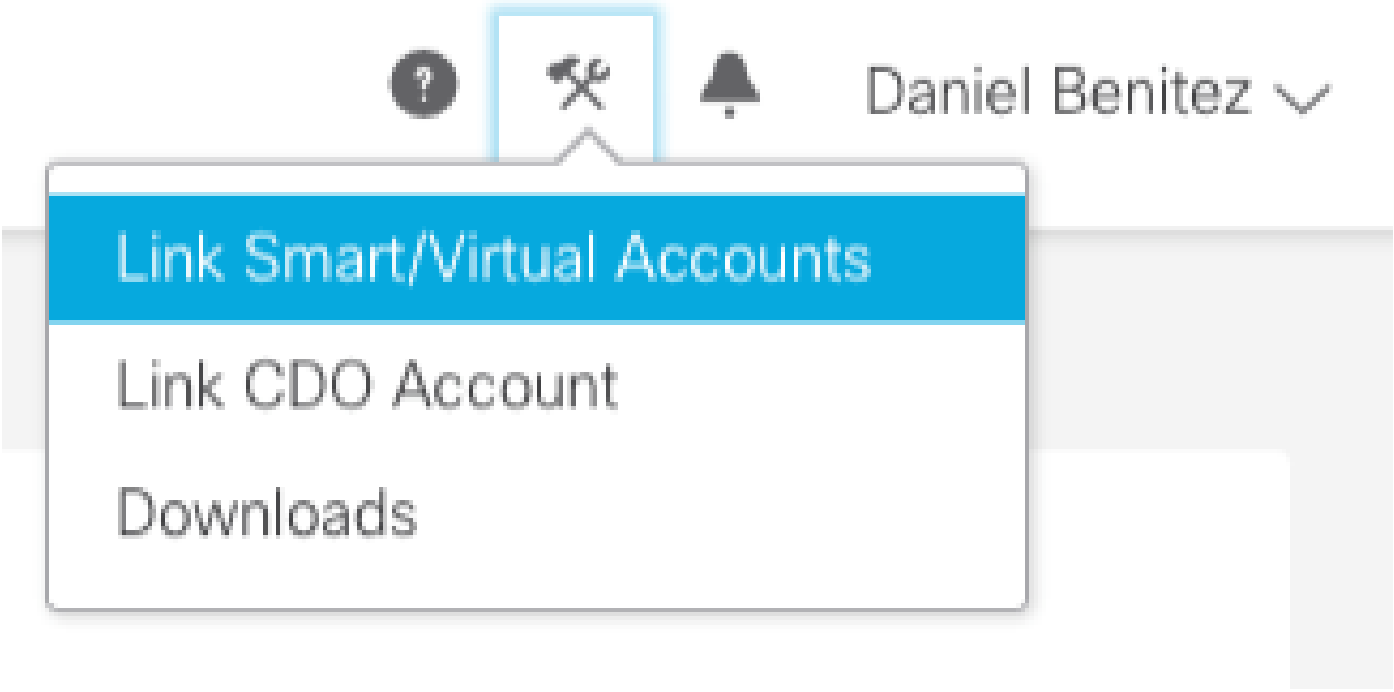


步驟4.要驗證FMC是否已註冊到正確的虛擬帳戶，請導航到System>Licenses>Smart License:



將您的帳戶連結到SSE並註冊裝置。

步驟1.登入SSE帳戶時，必須將智慧帳戶連結到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

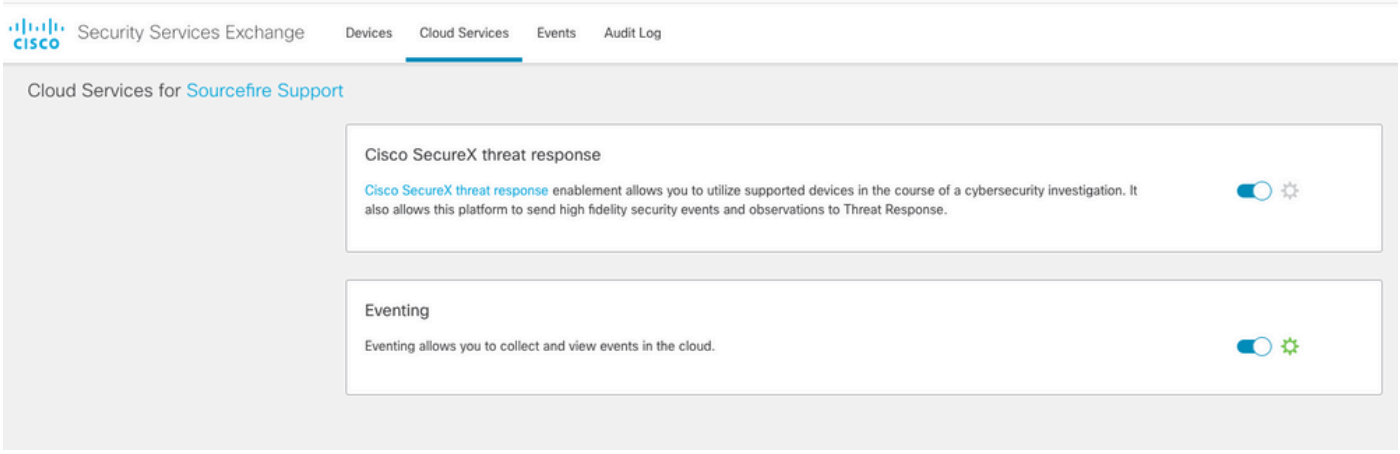
歐盟地區

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

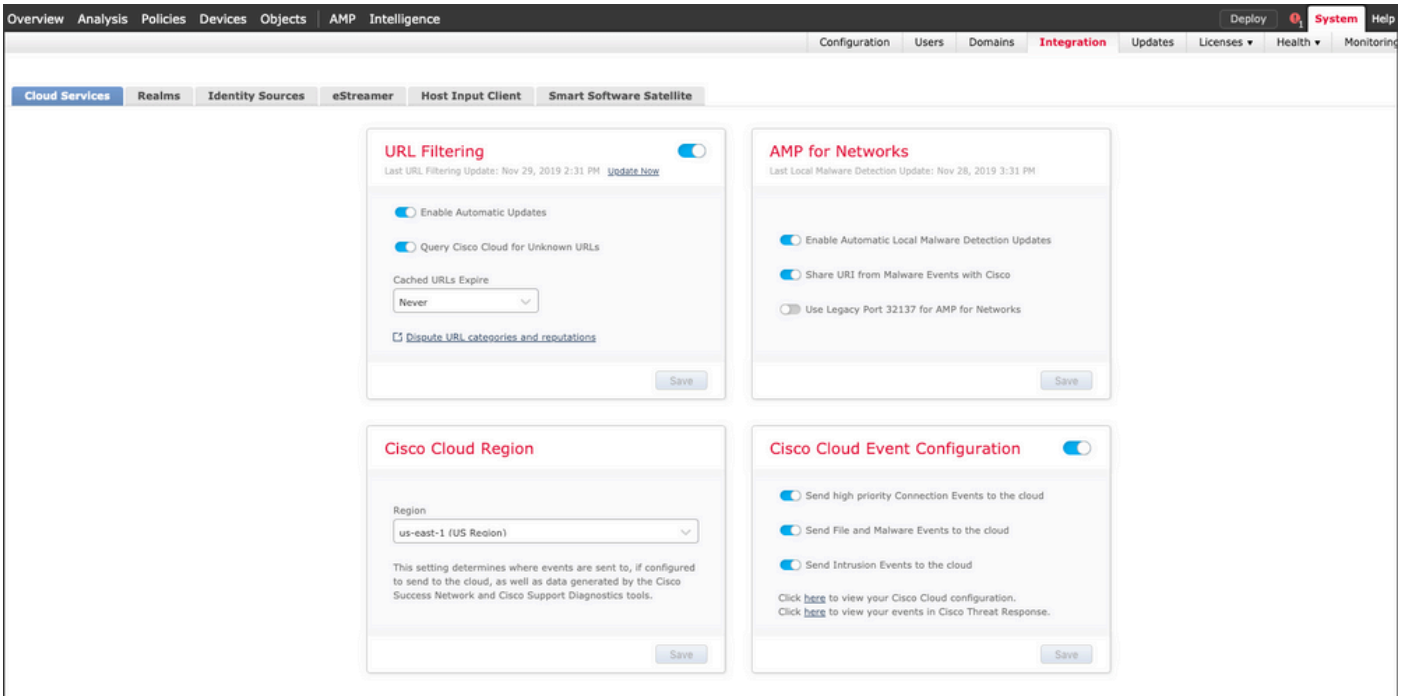
亞太及日本地區

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

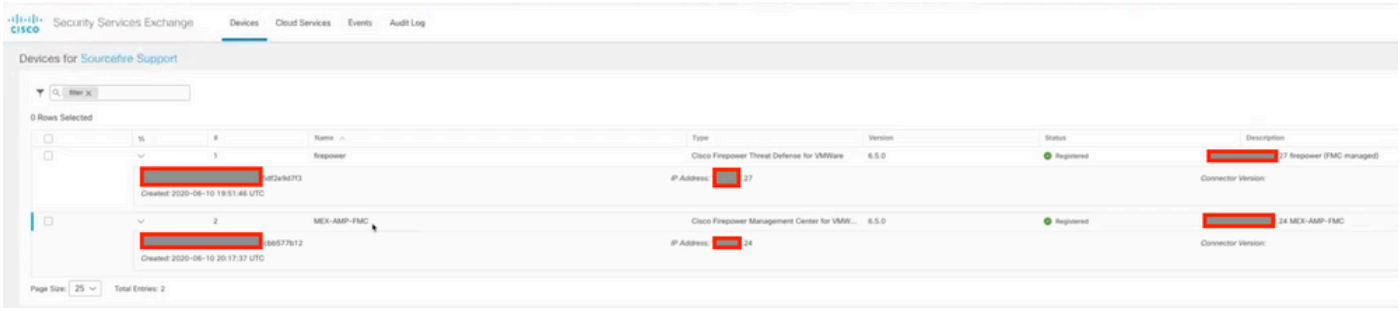
步驟2.使用此URL https://admin.sse.itd.cisco.com登入到SSE門戶，導航到Cloud Services，然後啟用Eventing和Cisco XDR威脅響應選項，如下圖所示：



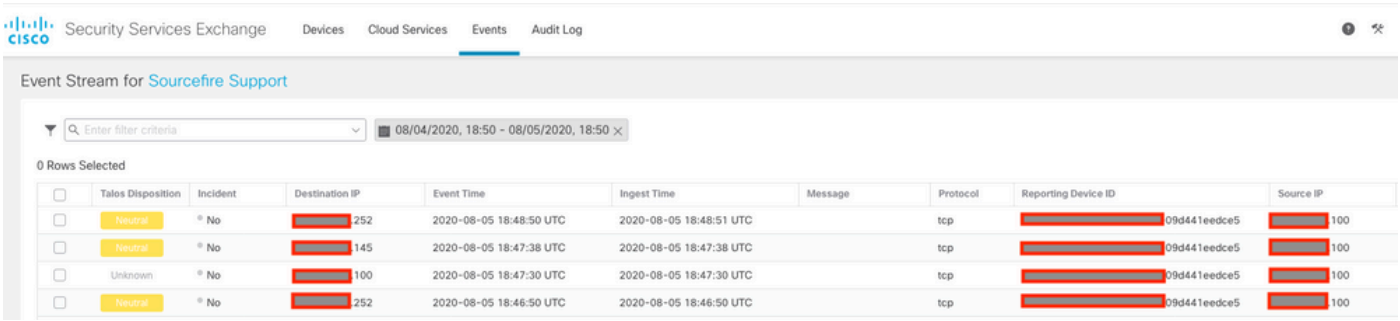
步驟3.登入到Firepower管理中心並導航到System>Integration>Cloud Services，啟用Cisco Cloud Event Configuration，然後選擇要傳送到雲的事件：



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：



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：



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Cisco XDR控制面板上，或者檢查API日誌，以便檢視可能的API故障原因。

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-timeo
```

在這種情況下，退出代碼28表示操作超時，我們必須檢查與Internet的連線。您還必須看到退出代碼6，這意味著存在DNS解析問題

由於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'
```

此輸出顯示，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
```

此輸出顯示未到達已配置的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
```

在可以再次測試此連線之後，這次連線成功。

```
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：

<#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

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;
```

注意：您會收到403 Forbidden消息，因為從測試傳送的引數不是SSE期望的，但證明這足以驗證連線。

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_SSEConnecto
```

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.soc
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.a
```

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:co
time="2020-04-13T14:38:18.244707779-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:c
```

```
time="2020-04-13T14:42:42.564695622-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:c
time="2020-04-13T14:47:48.484762429-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:c
time="2020-04-13T14:52:38.404700083-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:c
```

> 注意：注意，必須更改顯示的x.x.x.246和1x.x.x.246屬於https://eventing-ingest.sse.itd.cisco.com的IP地址，因此建議允許基於URL而不是IP地址的SSE門戶流量。

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.
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。