# Cisco XDRとFirepower Threat Defense(FTD)の統合およびトラブルシューティング

## 内容



## 概要

このドキュメントでは、Cisco XDRとFirepowerFirepower脅威対策(FTD)を統合、検証、およびトラブルシューティングするために必要な手順について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Firepower Management Center（ FMC ）
- Firepower Threat Defense（ FTD ）
- イメージの仮想化（ オプション ）

### 使用するコンポーネント

- Firepower脅威対策(FTD) - 6.5
- Firepower Management Center(FMC) - 6.5
- セキュリティサービスエクスチェンジ(SSE)
- Cisco XDR
- スマートライセンスポータル

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

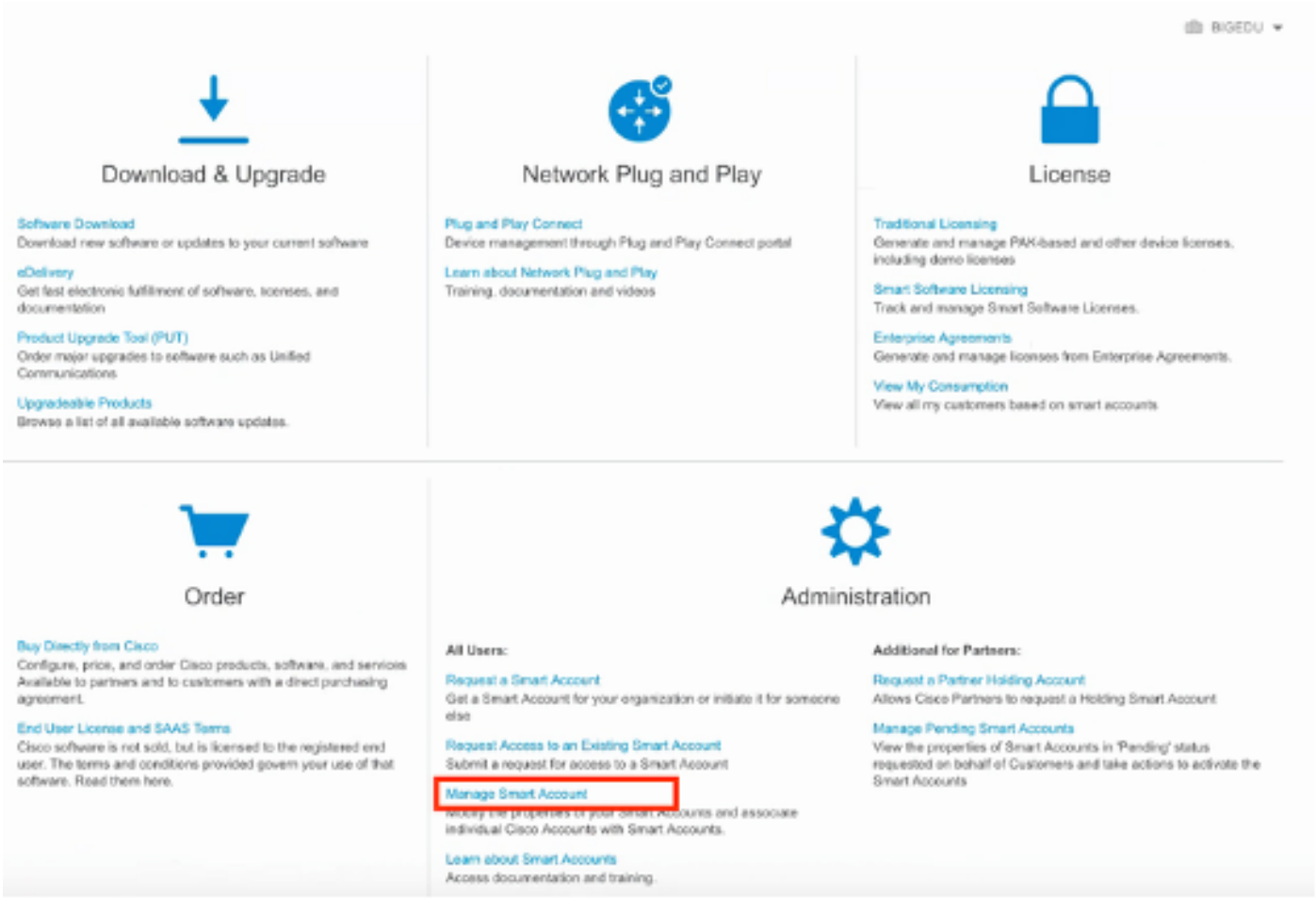
# 設定

## ライセンス

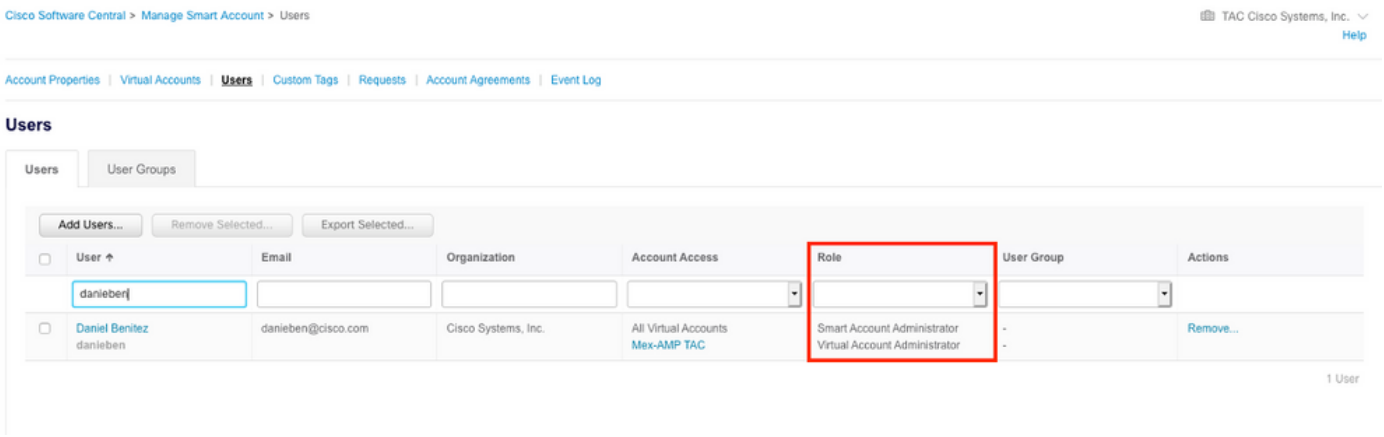
仮想アカウントロール：

スマートアカウントをSSEアカウントにリンクする権限を持つのは、仮想アカウント管理者またはスマートアカウント管理者のみです。

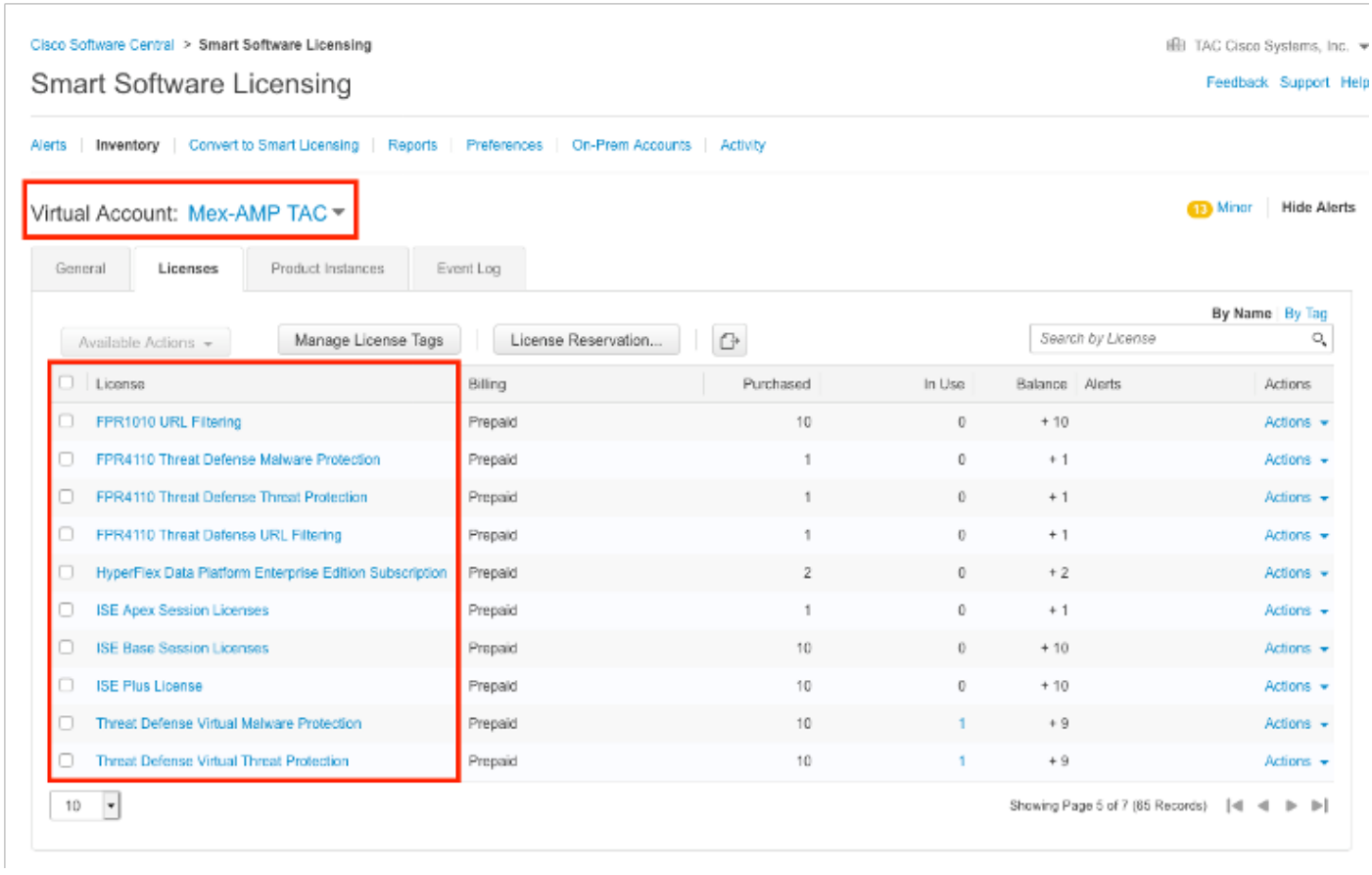
ステップ 1：スマートアカウントの役割を検証するには、software.cisco.comに移動し、Administration MenuでManage Smart Accountを選択します。




ステップ 2：ユーザロールを検証するには、Usersに移動し、次の図に示すように、Rolesの下でアカウントがVirtual Account Administratorに設定されていることを検証します。




ステップ 3：セキュリティライセンスを含まないアカウントがSSEでリンクされている場合、SSEでリンクするように選択された仮想アカウントにセキュリティデバイスのライセンスが含まれていることを確認します。セキュリティデバイスおよびイベントはSSEポータルに表示されません。




ステップ 4：FMCが正しい仮想アカウントに登録されたことを確認するには、System > Licenses > Smart Licenseの順に移動します。

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 |

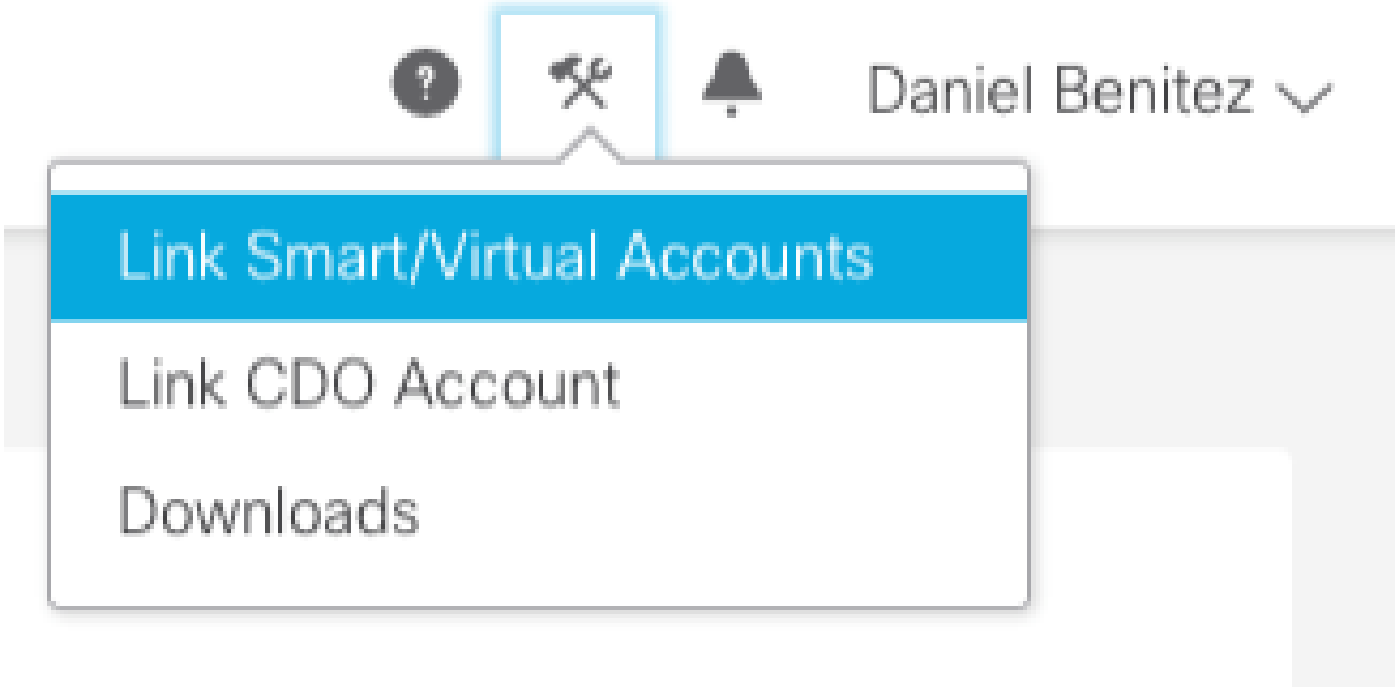
Smart Licenses

| 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

アカウントをSSEにリンクし、デバイスを登録します。

ステップ 1：SSEアカウントにログインする際は、スマートアカウントをSSEアカウントにリンクする必要があります。そのためには、ツールアイコンをクリックして、Link Accountsを選択する必要があります。



アカウントがリンクされると、すべての仮想アカウントを含むスマートアカウントが表示されます。

## SSEへのデバイスの登録

ステップ 1：ご使用の環境で次のURLが許可されていることを確認してください。

米国地域

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

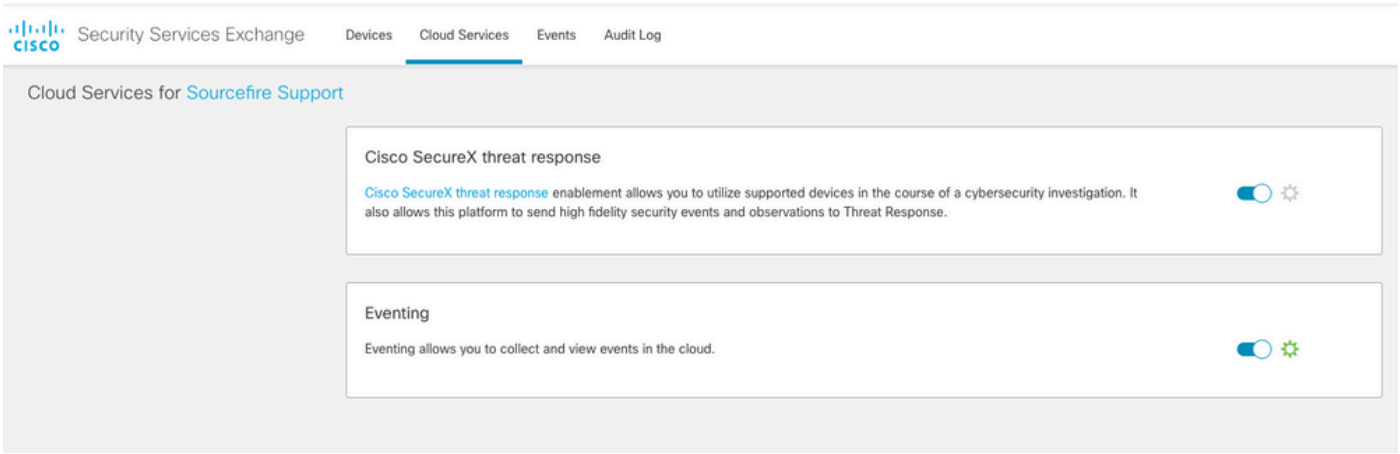
EU地域

- api.eu.ss e.itd.cisco.com
- eventing-ingest.eu.ss e.itd.cisco.com

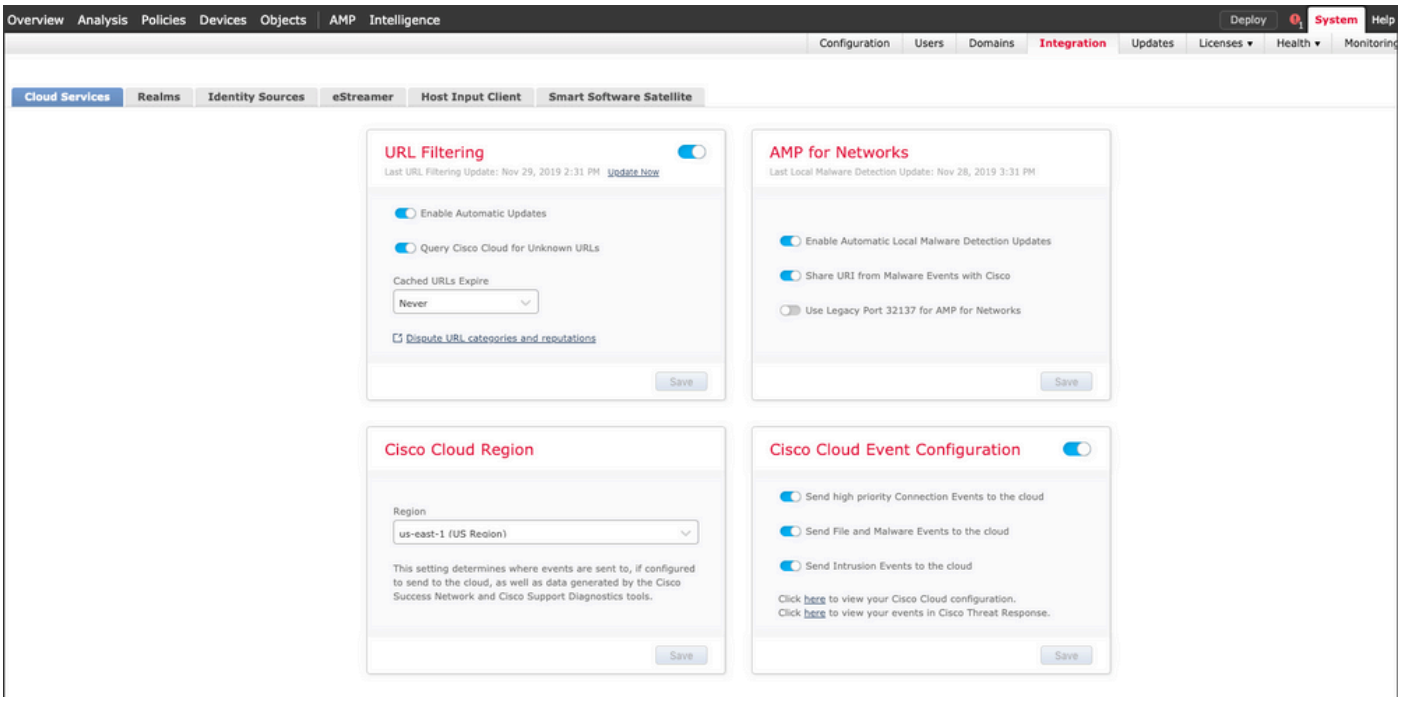
APJ地域

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

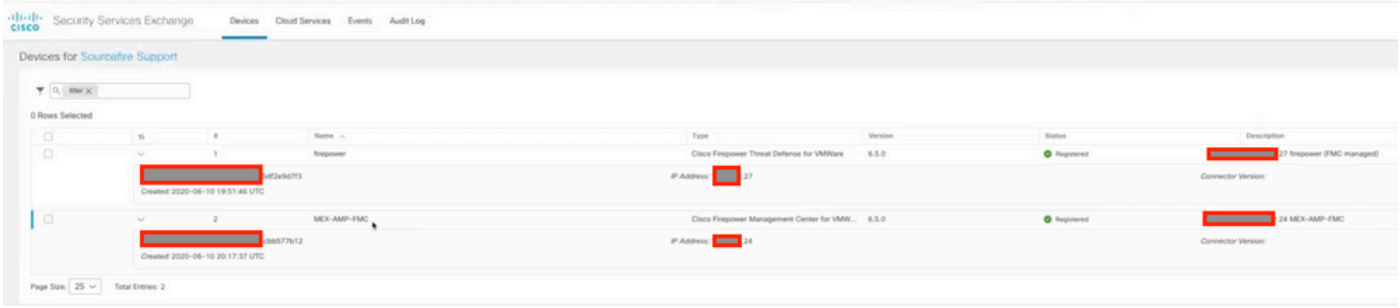
ステップ 2：次の図に示すように、次のURL https://admin.sse.itd.cisco.comでSSEポータルにログインし、クラウドサービスに移動して、両方のオプションイベント処理とCisco XDR Threat Responseを有効にします。



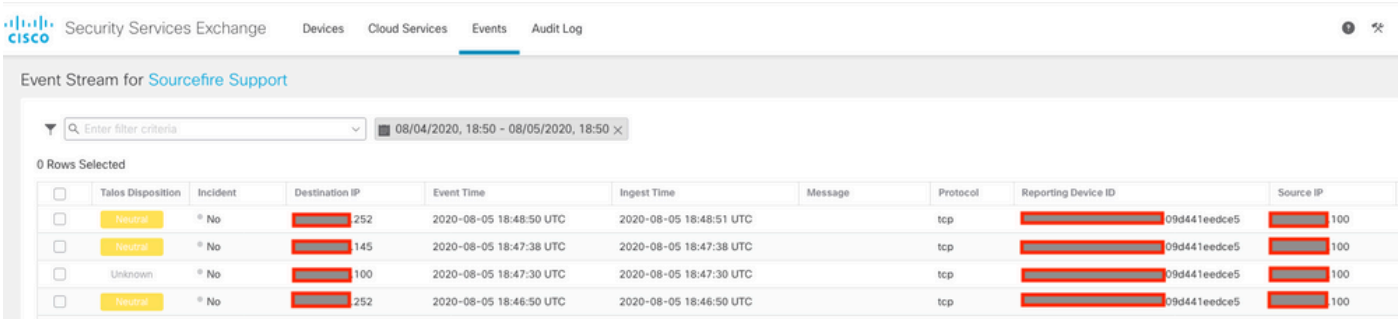

ステップ 3：firepower Management Centerにログインし、System > Integration > Cloud Servicesの順に選択して、Cisco Cloud Event Configurationを有効にし、クラウドに送信するイベントを選択します。




ステップ 4：SSEポータルに戻り、SSEに登録されているデバイスが表示されることを確認します。




イベントはFTDデバイスによって送信されます。次の図に示すように、SSEポータルでEventsに移動し、デバイスからSSEに送信されたイベントを確認します。




## 確認

FTDがイベント（マルウェアまたは侵入）を生成していることを検証します。侵入イベントについては、次の場所に移動します。 分析>ファイル>マルウェアイベント：侵入イベントの場合は、[分析] > [侵入] > [イベント]に移動します。

「SSEへのデバイスの登録」セクションのステップ4で説明されているように、イベントがSSEポータルに登録されていることを検証しますを参照。

Cisco XDRダッシュボードに情報が表示されていることを確認するか、API口グを確認してAPI障害の原因を調べます。

# トラブルシュート

## 接続の問題の検出

action_queue.logファイルから一般的な接続の問題を検出できます。障害が発生した場合は、次のような口グがファイルに存在することを確認できます。

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

この場合、終了コード28は動作がタイムアウトしたことを意味し、インターネットへの接続を確認する必要があります。終了コード6も表示される必要があります。これは、DNS解決の問題を意味します

## DNS解決による接続の問題

ステップ 1：接続が正常に機能していることを確認します。

```
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'
```

次の出力は、デバイスがURL https://api-sse.cisco.comを解決できないことを示しています。この場合、適切なDNSサーバが設定されていることを検証する必要があります。このサーバは、エキスパートCLIからnslookupを使用して検証できます。

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

次の出力は、設定されているDNSに到達していないことを示しています。DNS設定を確認するには、show networkコマンドを使用します。

```
> 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
```

この例では、誤ったDNSサーバが使用されています。次のコマンドを使用してDNS設定を変更できます。

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

この接続を再度テストし、今度は接続が成功します。

```
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ポータルへの登録に関する問題

FMCとFTDの両方で、管理インターフェイスのSSE URLへの接続が必要です。接続をテストするには、rootアクセス権を持つFirepowerCLIで次のコマンドを入力します。

<#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**

次のコマンドを使用すると、証明書チェックをバイパスできます。

```
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：テストから送信されたパラメータはSSEが期待したものではないため、403 Forbiddenメッセージが表示されますが、これは接続を検証するのに十分であることを示しています。

---

## SSEConnectorの状態の確認

次に示すように、コネクタのプロパティを確認できます。

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

SSConnectorとEventHandlerの間の接続を確認するには、次のコマンドを使用できます。接続が正しくない場合の例を次に示します。

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

確立された接続の例では、ストリームステータスがconnectedであることを確認できます。

```
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
```

## SSEポータルとCTRに送信されるデータを確認する

FTDデバイスからイベントを送信して、TCP接続がhttps://eventing-ingest.sse.itd.cisco.comで確立される必要があることを確認します。次に、SSEポータルとFTDの間で確立されない接続の例を示します。

```
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
```

connector.logログで、次の操作を行います。

```
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：表示されるx.x.x.246および1x.x.x.246がhttps://eventing-ingest.sse.itd.cisco.comに属するIPアドレスは変更する必要があることに注意してください。これが、IPアドレスではなくURLに基づいてSSEポータルへのトラフィックを許可することが推奨される理由です。

この接続が確立されない場合、イベントはSSEポータルに送信されません。次に、FTDとSSEポータルの間に確立された接続の例を示します。

```
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.
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。