使用Firepower威胁防御(FTD)集成思科XDR并进行故障排除

目录

简介

先决条件

- 要求
- 使用的组件

配置

- 许可
- 将您的帐户链接到SSE并注册设备。
- 将设备注册到SSE

简介

本文档介绍使用Firepower Firepower威胁防御(FTD)集成、验证和排除Cisco XDR故障所需的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)
- 映像的可选虚拟化

使用的组件

- Firepower威胁防御(FTD)- 6.5
- Firepower管理中心(FMC)- 6.5
- 安全服务交换(SSE)
- 思科XDR
- 智能许可证门户

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

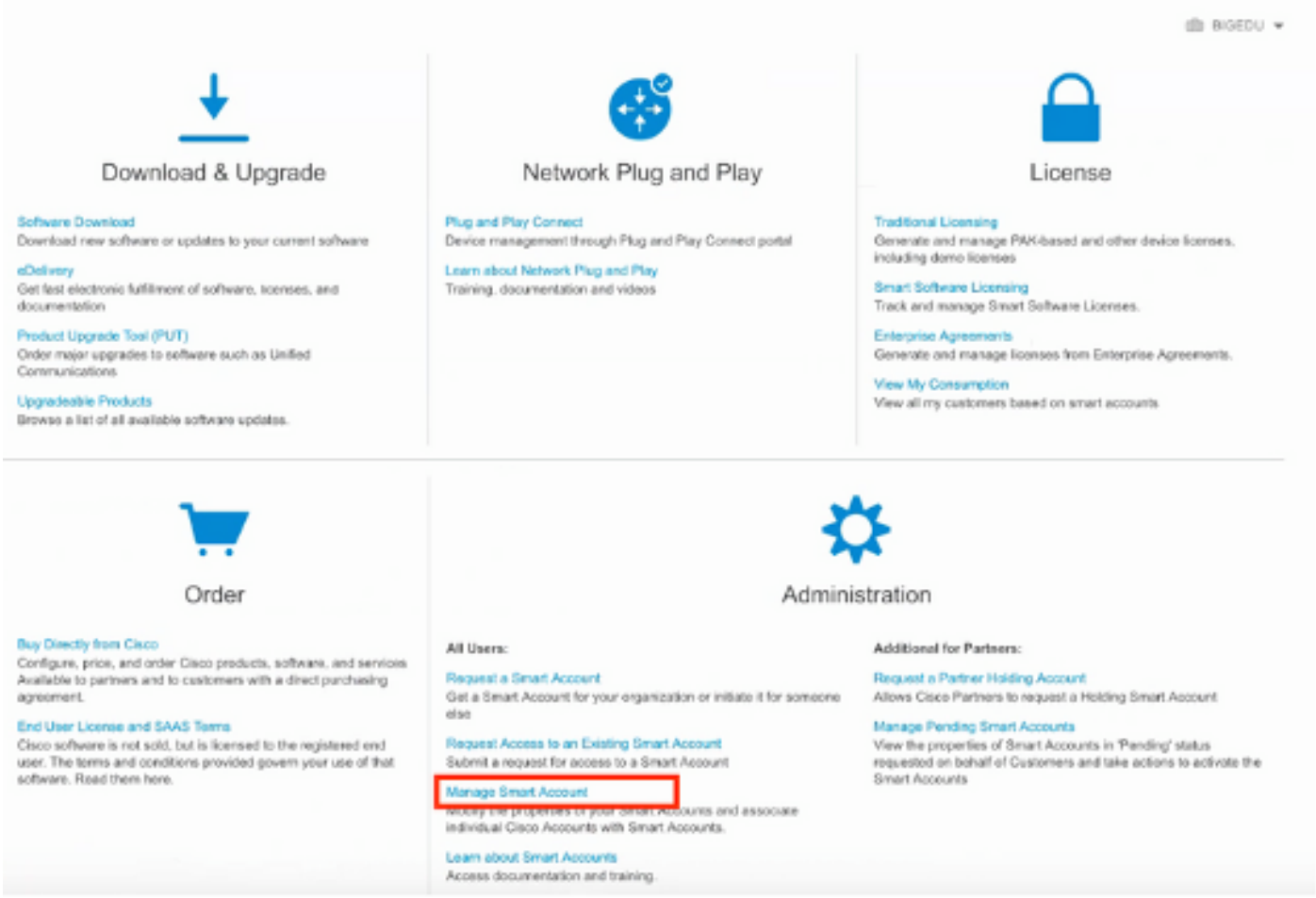
配置

许可

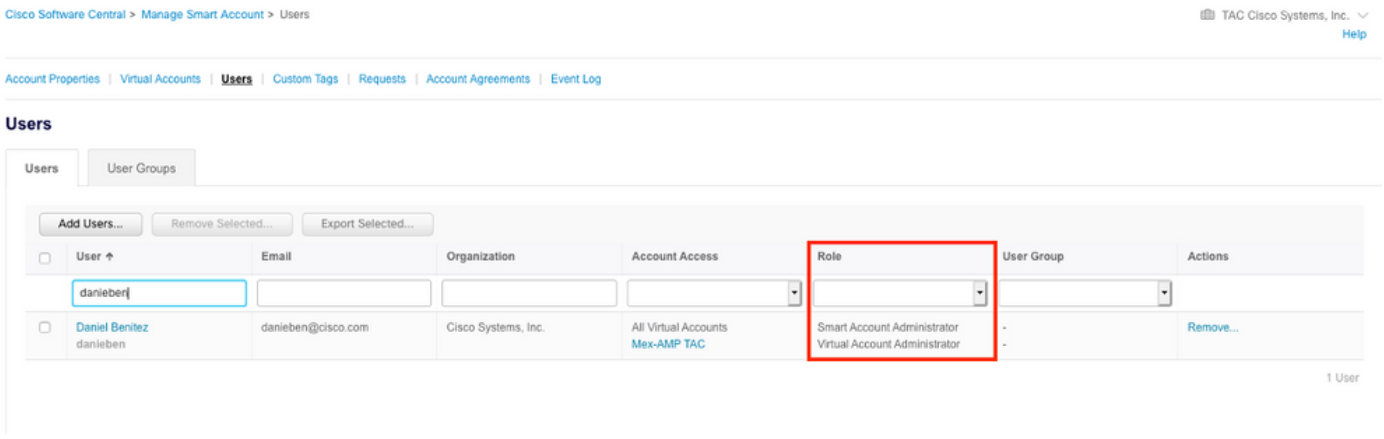
虚拟帐户角色：

只有虚拟帐户管理员或智能帐户管理员有权将智能帐户与SSE帐户关联。

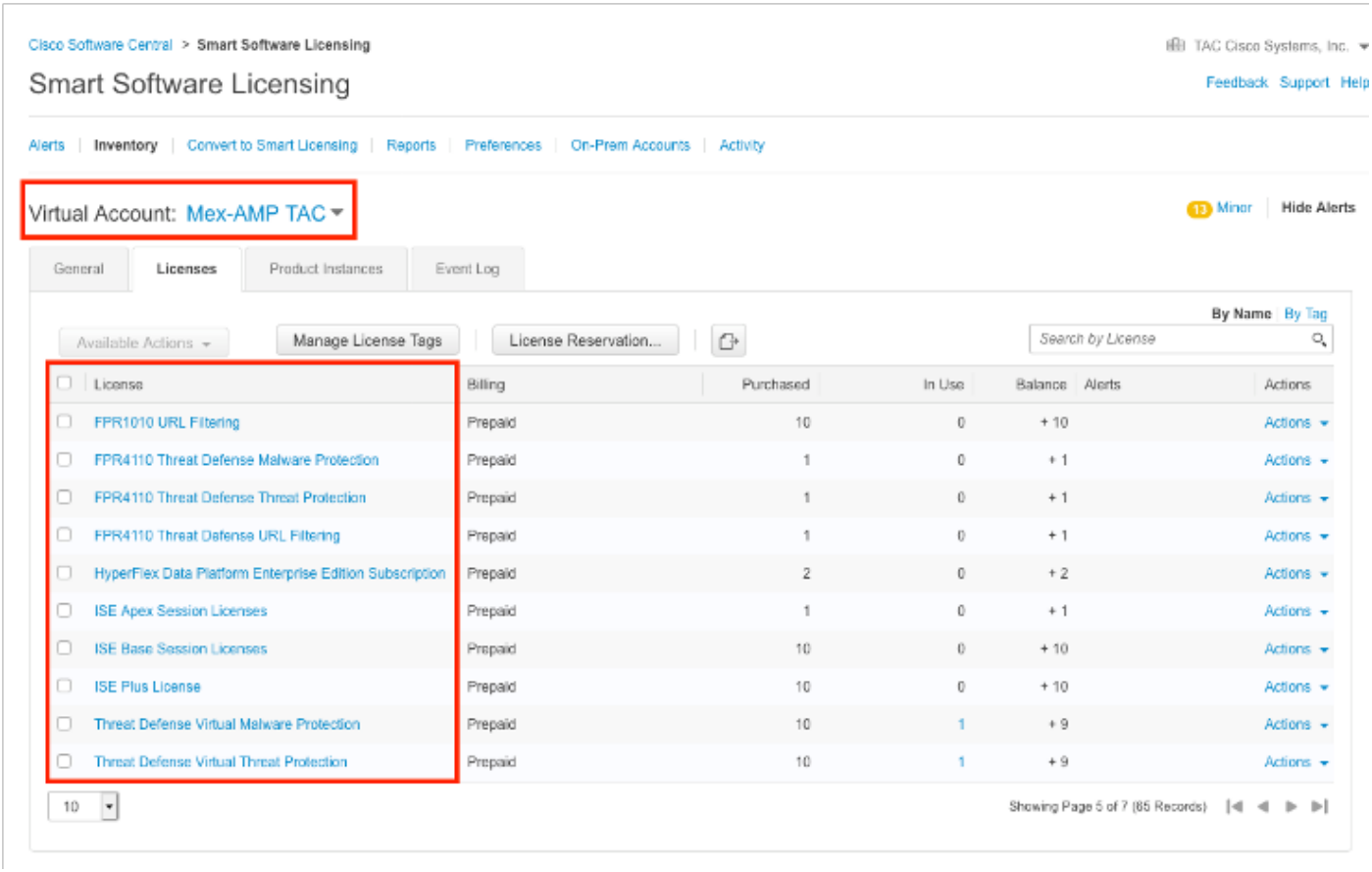
步骤1:要验证智能帐户角色，请导航至software.cisco.com，然后在Administration Menu下选择Manage Smart Account。



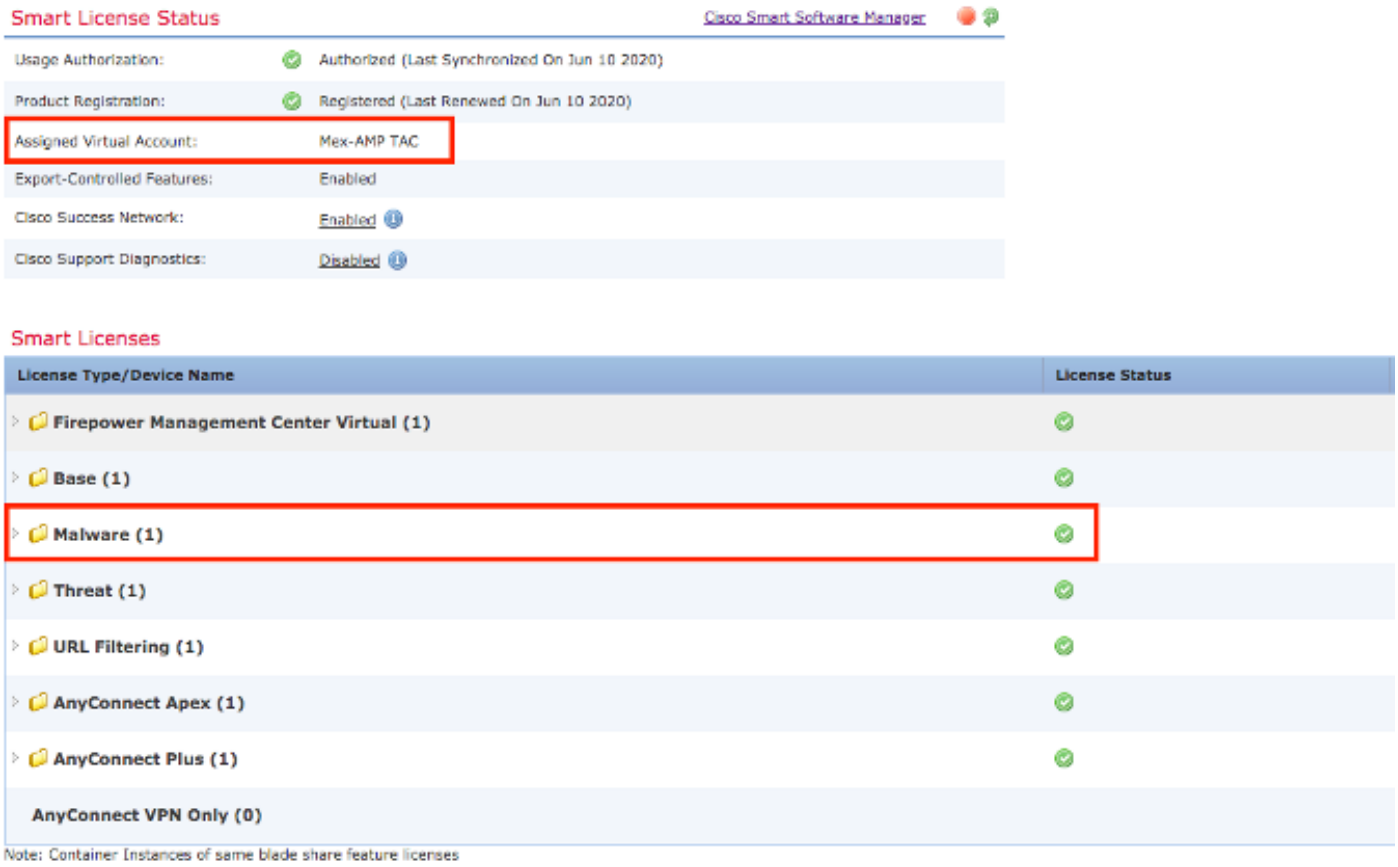
第二步：要验证用户角色，请导航到Users，并验证在Roles下，帐户设置为具有虚拟帐户管理员，如图所示。



第三步：确保选择在SSE上链接的虚拟帐户包含安全设备的许可证，如果不包含安全许可证的帐户在SSE上链接，则安全设备和事件不会显示在SSE门户上。

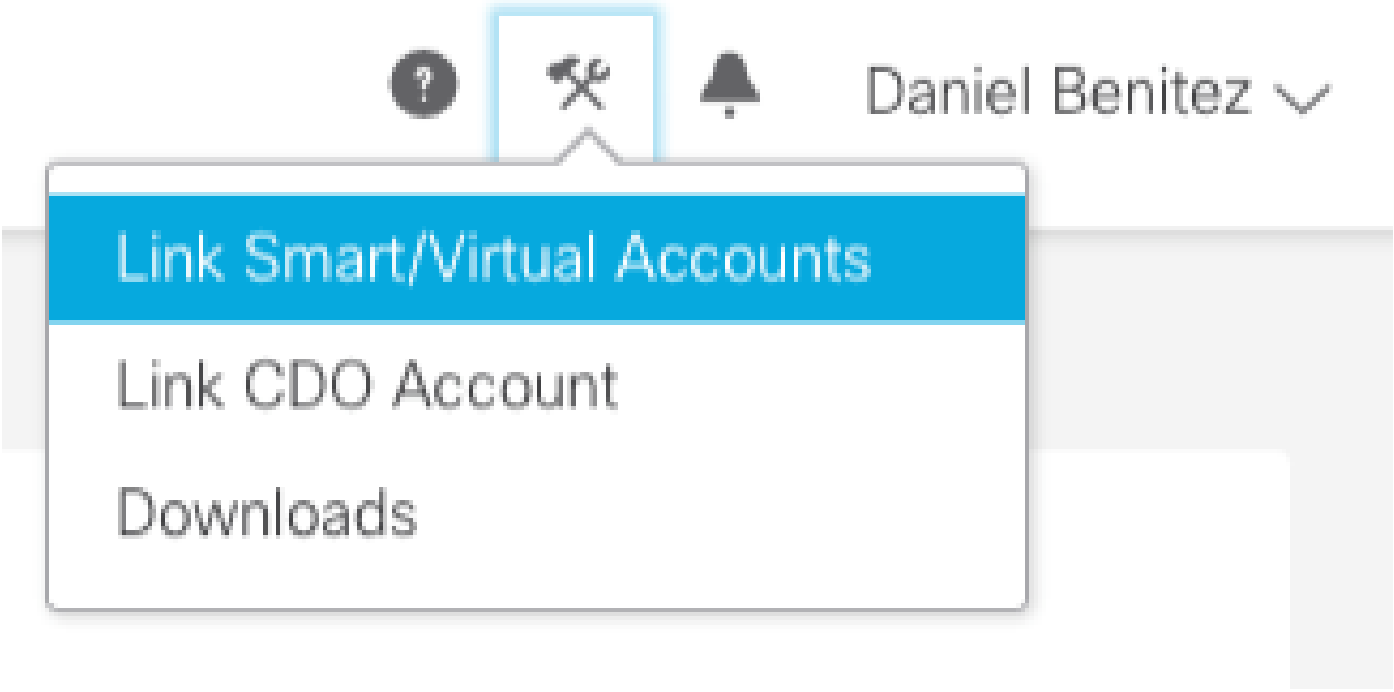


第四步：要验证FMC是否已注册到正确的虚拟帐户，请导航到系统>许可证>智能许可证：



将您的帐户链接到SSE并注册设备。

步骤1:登录SSE帐户时，必须将智能帐户链接到SSE帐户，为此，您需要点击工具图标并选择Link Accounts。



帐户链接后，您会看到智能帐户及其上的所有虚拟帐户。

将设备注册到SSE

步骤1:确保您的环境中允许以下URL:

美国地区

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

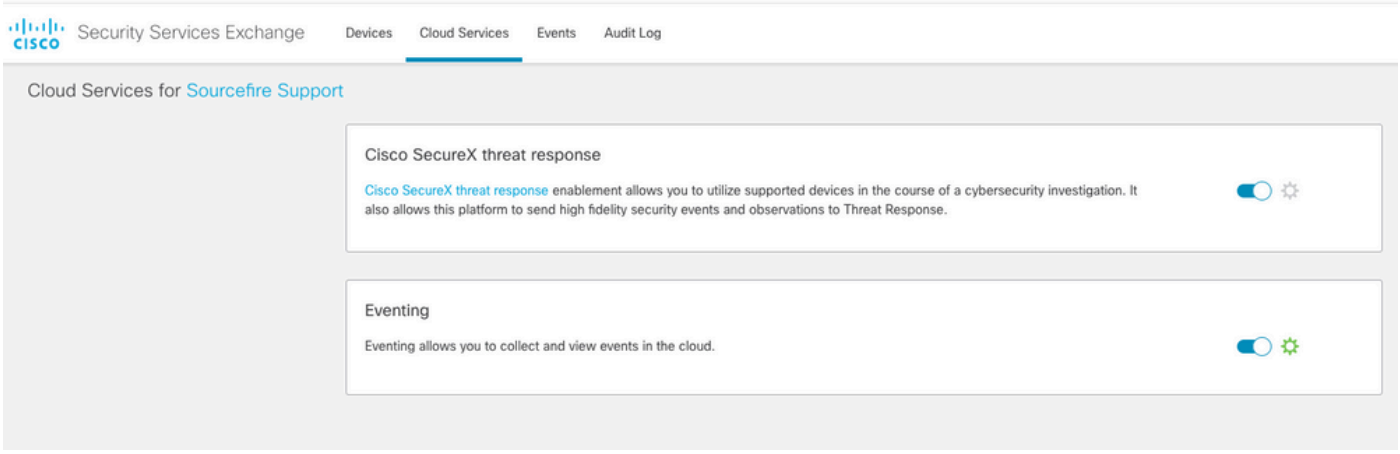
欧盟地区

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

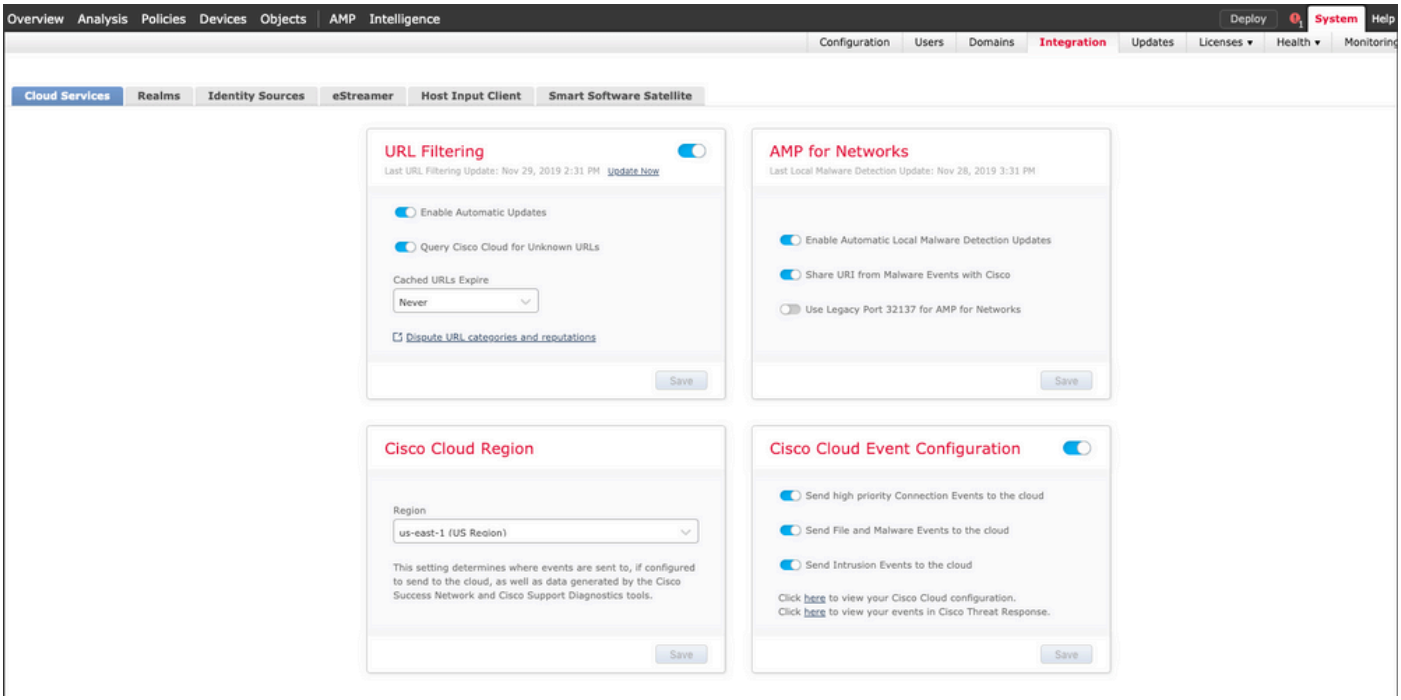
APJ地区

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

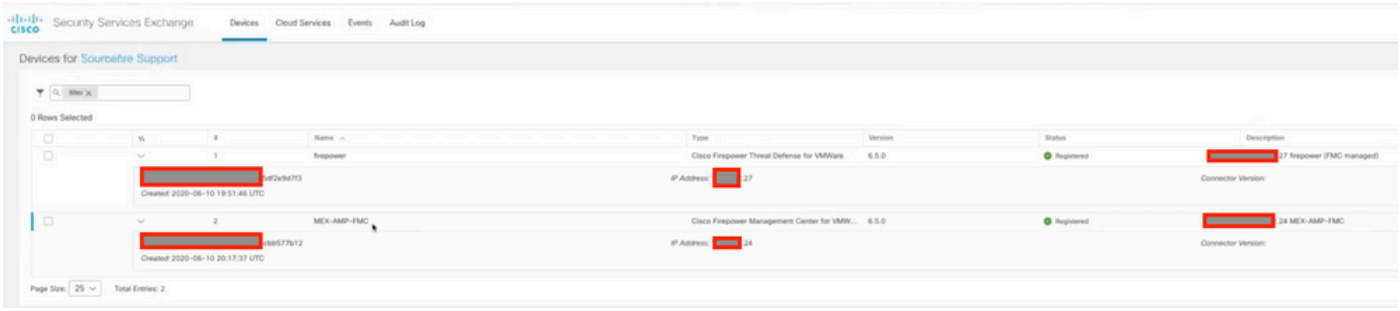
第二步：使用此URL https://admin.sse.itd.cisco.com登录SSE门户，导航到云服务，并启用事件和思科XDR威胁响应这两个选项，如下图所示：



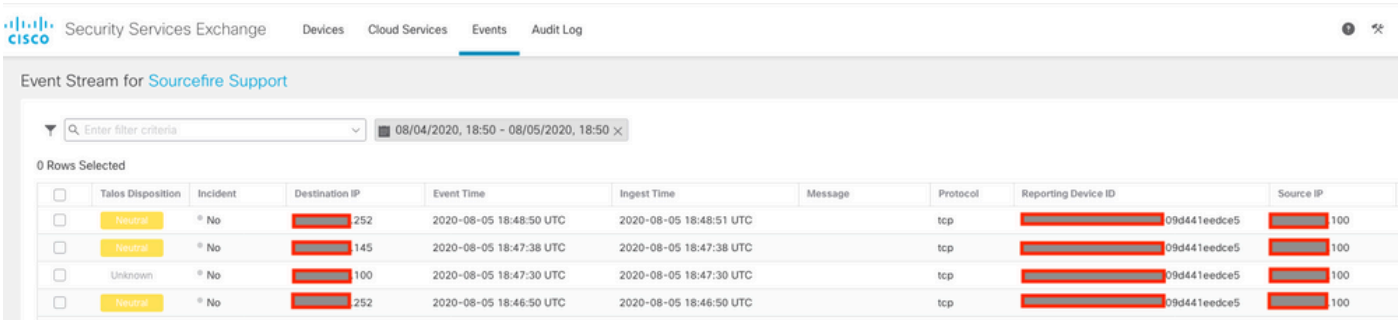
第三步：登录到Firepower管理中心并导航到System>Integration>Cloud Services，启用Cisco Cloud Event Configuration，然后选择要发送到云的事件：



第四步：您可以返回到SSE门户并验证现在是否可以看到在SSE上注册的设备：



Events由FTD设备发送，导航至SSE门户上的Events以验证设备发送到SSE的事件，如图所示：



验证

验证FTD是否生成事件（恶意软件或入侵），对于入侵事件，请导航到Analysis>Files>Malware Events，对于入侵事件，请导航到Analysis>Intrusion>Events。

按照向SSE注册设备第4部分所述，验证在SSE门户上注册的事件。

验证信息是否显示在Cisco XDR控制面板上，或者检查API日志，以便查看可能的API故障原因。

故障排除

检测连接问题

您可以从action_queue.log文件中检测一般连接问题。如果发生故障，您可以在文件中看到此类日志：

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

在这种情况下，退出代码28表示操作超时，我们必须检查与Internet的连接。您还必须看到退出代码6，这意味着存在DNS解析问题

DNS解析引起的连接问题

步骤1:检查连接是否工作正常。

```
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'
```

此输出显示设备无法解析URL https://api-sse.cisco.com，在这种情况下，我们需要验证是否配置了

正确的DNS服务器，它可以通过专家CLI中的nslookup进行验证：

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

此输出显示未到达配置的DNS，为了确认DNS设置，请使用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
```

在本示例中，使用了错误的DNS服务器，您可以使用以下命令更改DNS设置：

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

在可以再次测试此连接之后，这次连接成功。

```
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门户的注册问题

FMC和FTD都需要在其管理接口上连接到SSE URL，要测试连接，请在具有根访问权限的Firepower CLI上输入以下命令：

<#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

可以使用以下命令绕过证书检查：

```
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：您将收到403 Forbidden消息，因为从测试发送的参数不是SSE期望的值，但是这足以验证连接。

检验SSEConnector状态

可以验证连接器属性，如下所示。

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

为了检查SSConnector和EventHandler之间的连接，可以使用此命令，以下是连接错误的示例：

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

在已建立的连接示例中，您可以看到流状态为connected:

```
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
```

验证发送到SSE门户和CTR的数据

要从FTD设备发送事件以查看TCP连接需要与https://eventing-ingest.sse.itd.cisco.com建立。以下是SSE门户和FTD之间未建立连接的示例：

```
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日志中：

```
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：注意，显示的IP地址x.x.x.246和1x.x.x.246属于https://eventing-ingest.sse.itd.cisco.com必须更改，因此建议根据URL而不是IP地址允许流量进入SSE门户。

如果此连接未建立，则事件不会发送到SSE门户。以下是FTD和SSE门户之间已建立连接的示例：

```
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.
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。