将Cisco XDR与安全防火墙集成并进行故障排除

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SSX并注册设备。

方法1（半集成）：丰富调查内容

- 将设备注册到SSX

简介

本文档介绍集成、验证带有安全防火墙的Cisco XDR并对其进行故障排除所需的步骤。

集成安全防火墙和XDR有两种方法，每种集成都会提供不同的结果。

第一种方法介绍如何集成安全防火墙、安全服务交换(SSX)、安全云控制、XDR-Analytics和XDR，以丰富调查内容。

第二种方法描述如何集成安全防火墙、SSX、安全云控制、XDR-A、SAL云和XDR以丰富突发事件。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科防火墙管理中心(FMC)
- 思科安全防火墙威胁防御
- 映像的可选虚拟化
- 思科防御协调器
- 安全服务交换
- 安全云控制

使用的组件

- 安全防火墙 — 7.2
- Firepower管理中心(FMC)- 7.2
- 安全服务交换(SSX)
- 思科XDR

- 智能许可证门户
- 思科防御协调器
- 安全云控制

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。

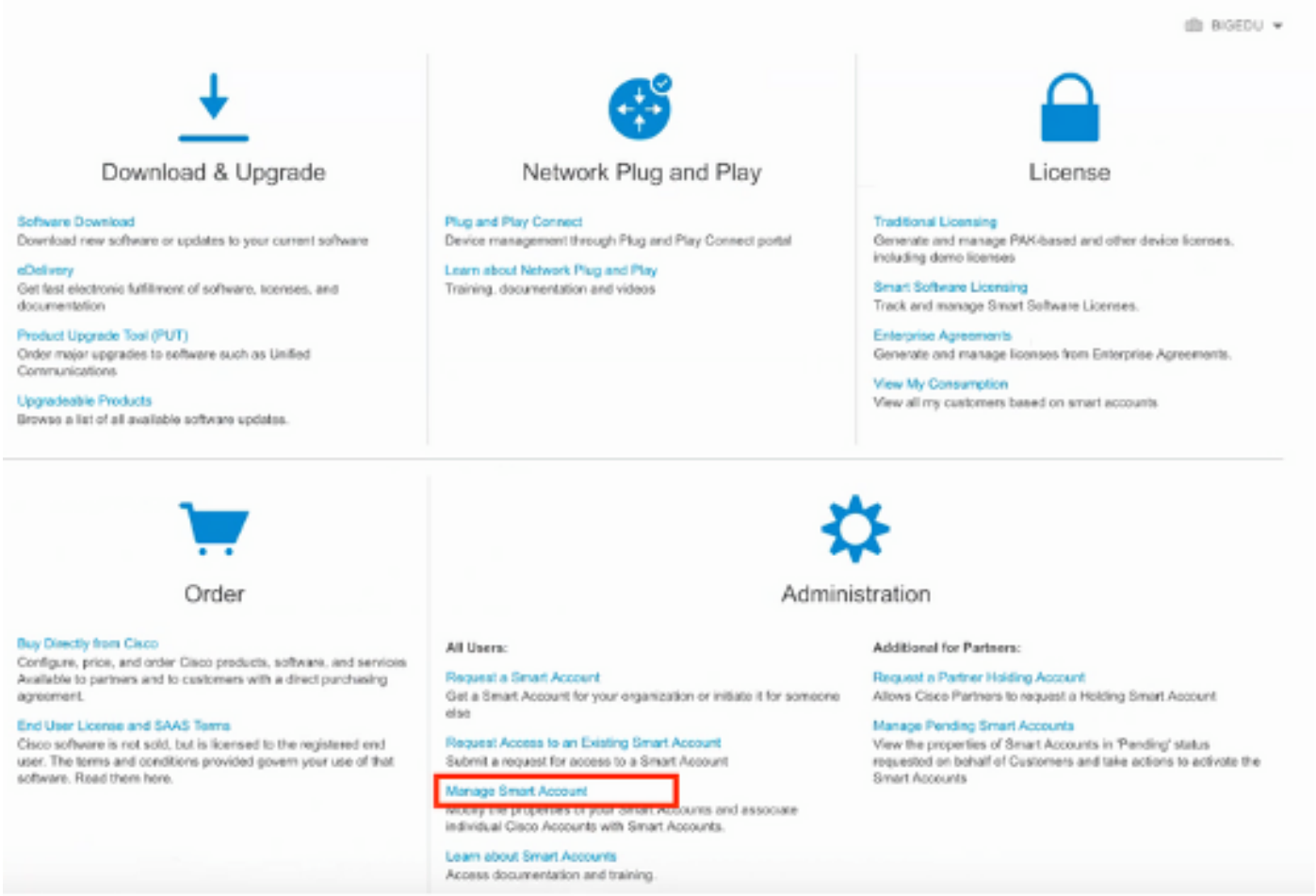
配置

许可

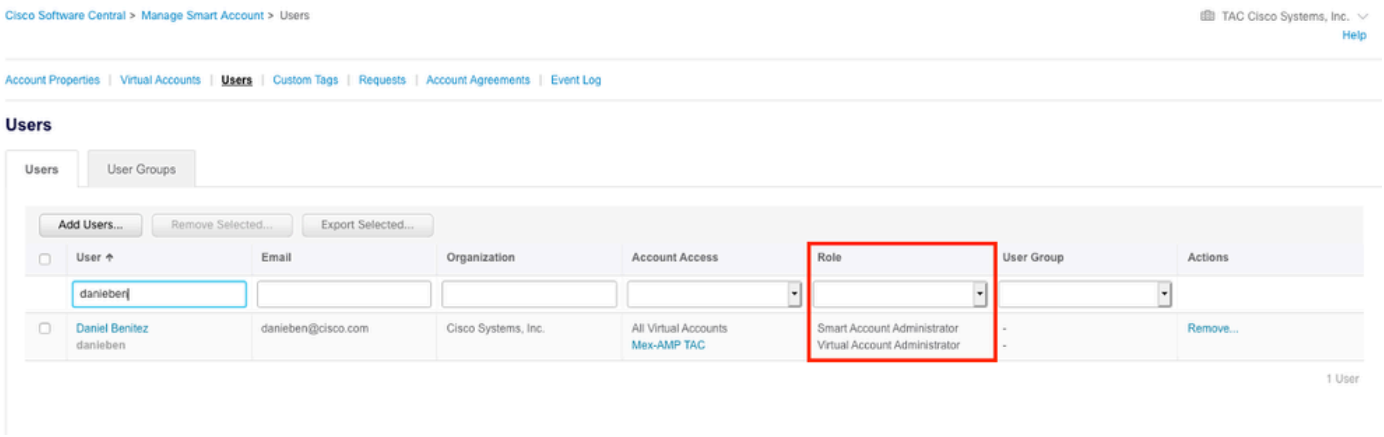
虚拟帐户角色：

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SSX帐户关联。

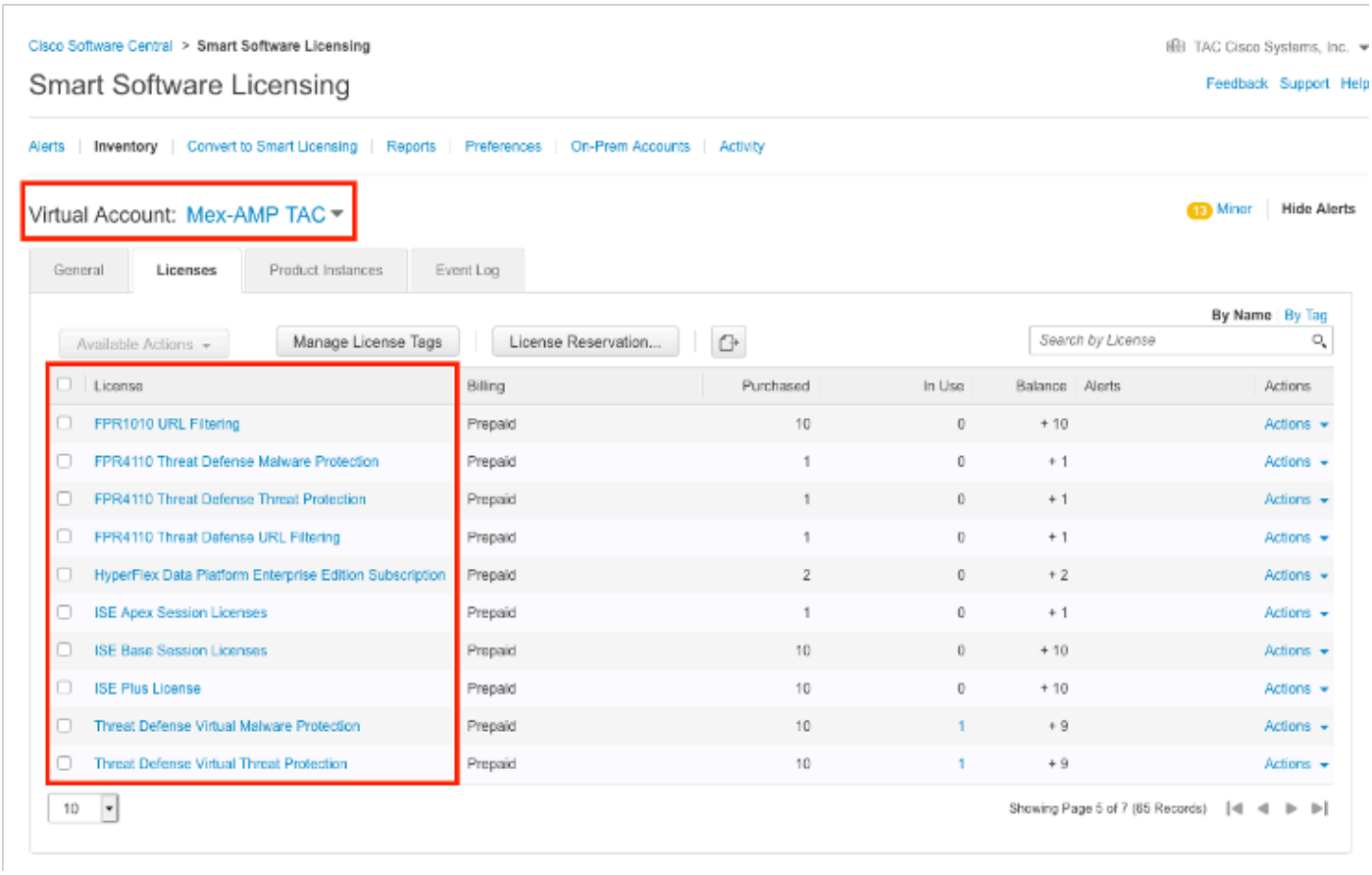
第1步：要验证智能帐户角色，请导航到software.cisco.com，在Administration Menu下，选择Manage Smart Account。



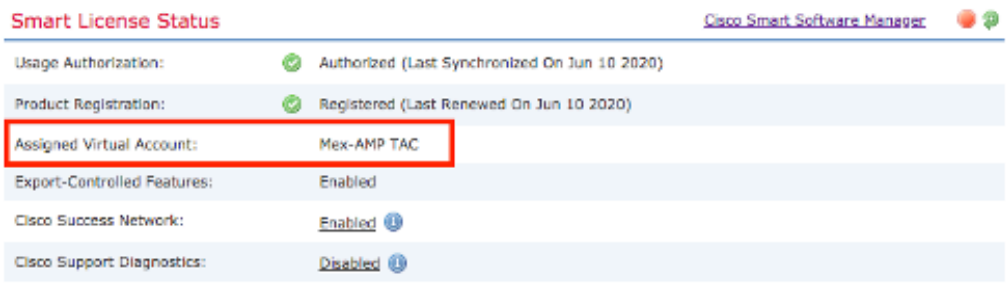
步骤2.要验证用户角色，请导航到用户，并验证在“角色”下帐户是否设置为具有虚拟帐户管理员，如图所示。

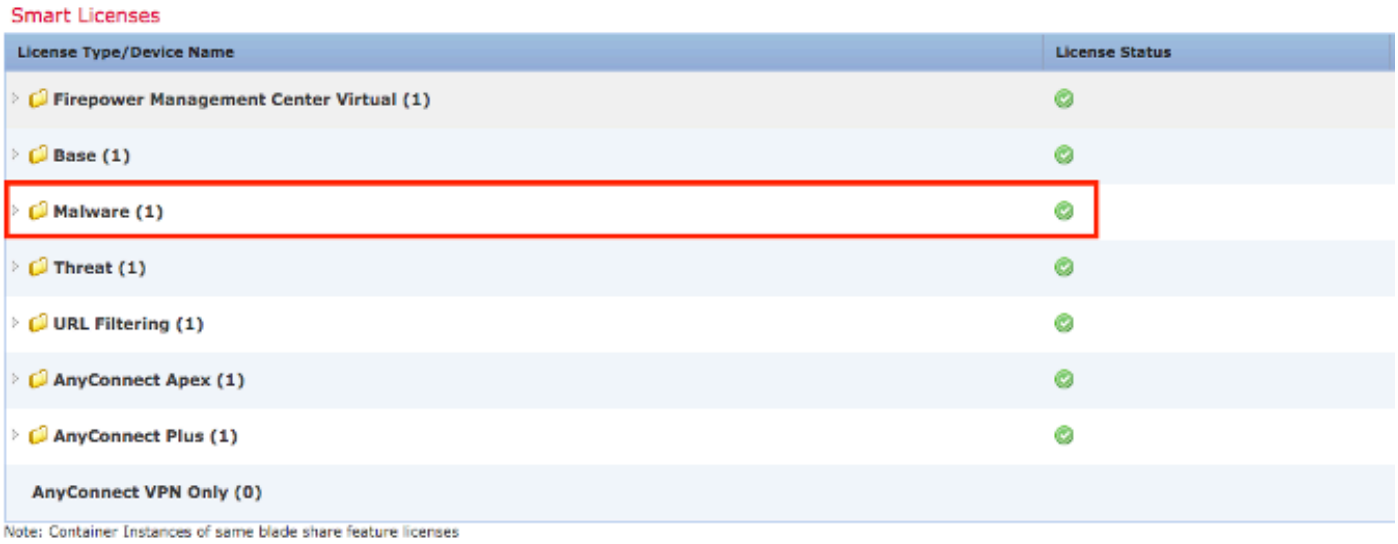


第3步：确保选择在SSX上链接的虚拟帐户包含安全设备的许可证，如果不包含安全许可证的帐户在SSX上链接，则安全设备和事件不会显示在SSX门户上。



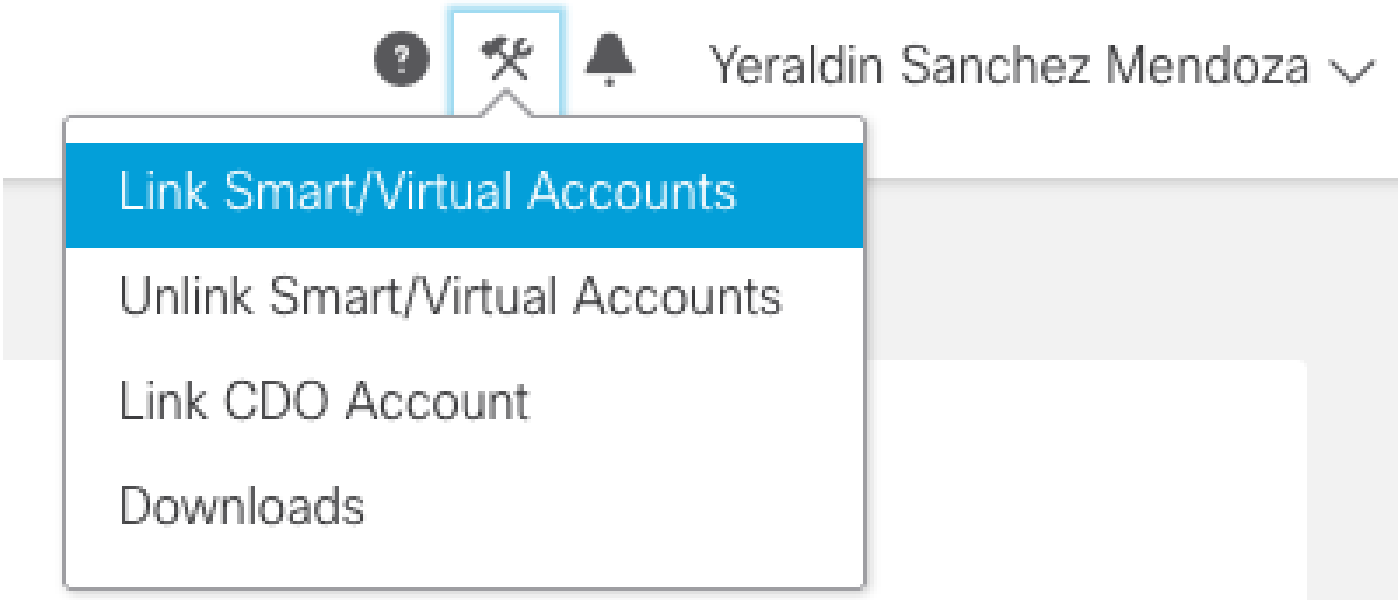
第4步：要验证FMC是否已注册到正确的虚拟帐户，请导航到系统>许可证>智能许可证：





将您的帐户链接到SSX并注册设备。

步骤1.登录到SSX帐户时，必须将智能帐户链接到SSX帐户，为此，您需要点击工具图标并选择链接智能/虚拟帐户。



帐户链接后，您会看到智能帐户及其上的所有虚拟帐户。

方法1（半集成）：丰富调查内容

将设备注册到SSX

步骤1.确保在您的环境中允许这些URL:

美国地区

- api-sse.cisco.com
- mx*.sse.itd.cisco.com
- dex.sse.itd.cisco.com
- eventing-ingest.sse.itd.cisco.com
- registration.us.ss e.itd.cisco.com
- defenseorchestrator.com
- edge.us.cd o.cisco.com

欧盟地区

- api.eu.ss e.itd.cisco.com
- mx*.eu.sse.itd.cisco.com
- dex.eu.ss e.itd.cisco.com
- eventing-ingest.eu.ss e.itd.cisco.com
- registration.eu.ss e.itd.cisco.com
- defenseorchestrator.eu
- edge.eu.cd o.cisco.com

亚太地区

- api.apj.sse.itd.cisco.com
- mx*.apj.sse.itd.cisco.com
- dex.apj.sse.itd.cisco.com
- eventing-ingest.apj.sse.itd.cisco.com
- registration.apj.sse.itd.cisco.com
- apj.cdo.cisco.com
- edge.apj.cdo.cisco.com

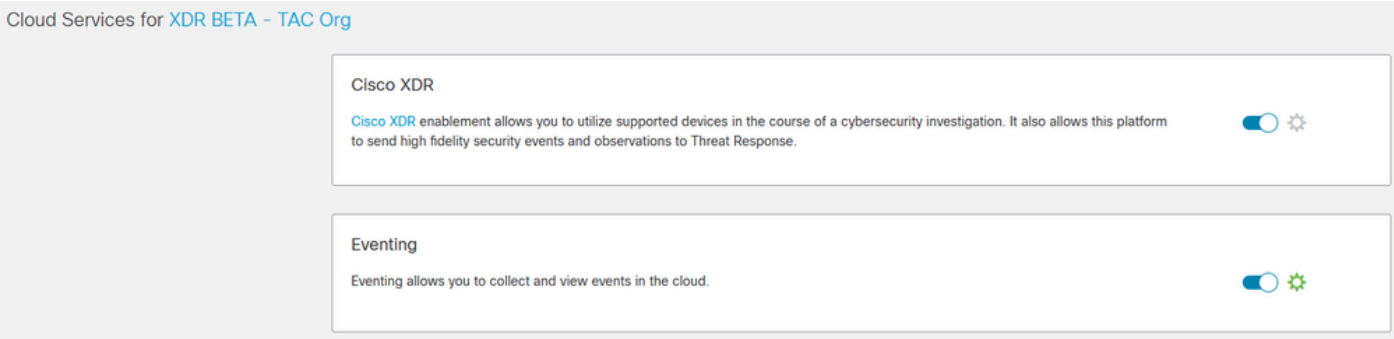
澳大利亚地区：

- api.aus.sse.itd.cisco.com
- mx*.aus.sse.itd.cisco.com
- dex.au.ss e.itd.cisco.com
- eventing-ingest.aus.sse.itd.cisco.com
- registration.au.ss e.itd.cisco.com
- aus.cdo.cisco.com

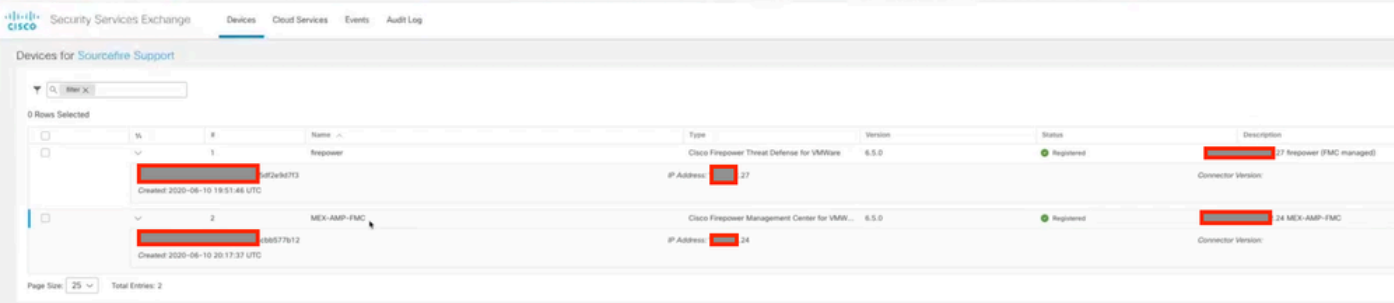
印度地区：

- api.in.ss e.itd.cisco.com
- mx*.in.sse.itd.cisco.com
- dex.in.ss e.itd.cisco.com
- eventing-ingest.in.ss e.itd.cisco.com
- registration.in.ss e.itd.cisco.com
- in.cdo.cisco.com

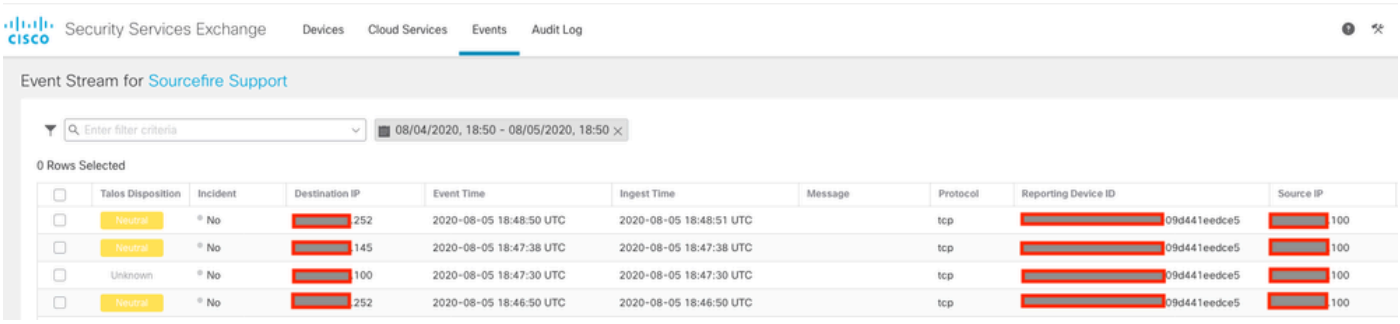
第2步：使用此URL https://admin.sse.itd.cisco.com登录SSX门户，导航到云服务，然后启用Cisco XDR和Eventing这两个选项，如图所示。



第3步：您可以验证现在是否可以看到在SSX上注册的设备：



Events由Secure Firewall设备发送，导航到SSX门户上的Events，以验证设备发送到SSX的事件，如图所示。



将设备注册到安全云控制(SCC/CDO)

步骤1.确保在您的环境中允许这些URL

美国地区：

- defenseorchestrator.com
- edge.us.cd o.cisco.com

欧盟地区

- defenseorchestrator.eu
- edge.eu.cd o.cisco.com

亚太地区

- apjc.cdo.cisco.com
- edge.apjc.cdo.cisco.com

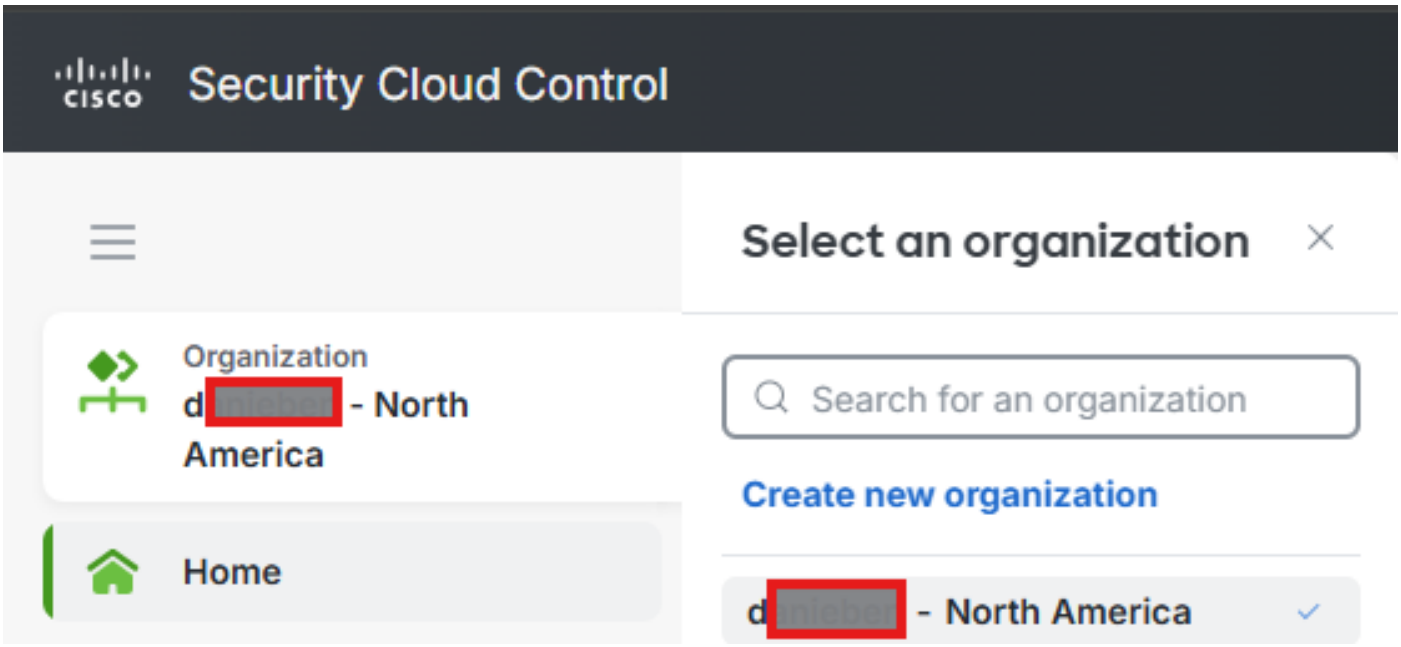
澳大利亚地区：

- aus.cdo.cisco.com

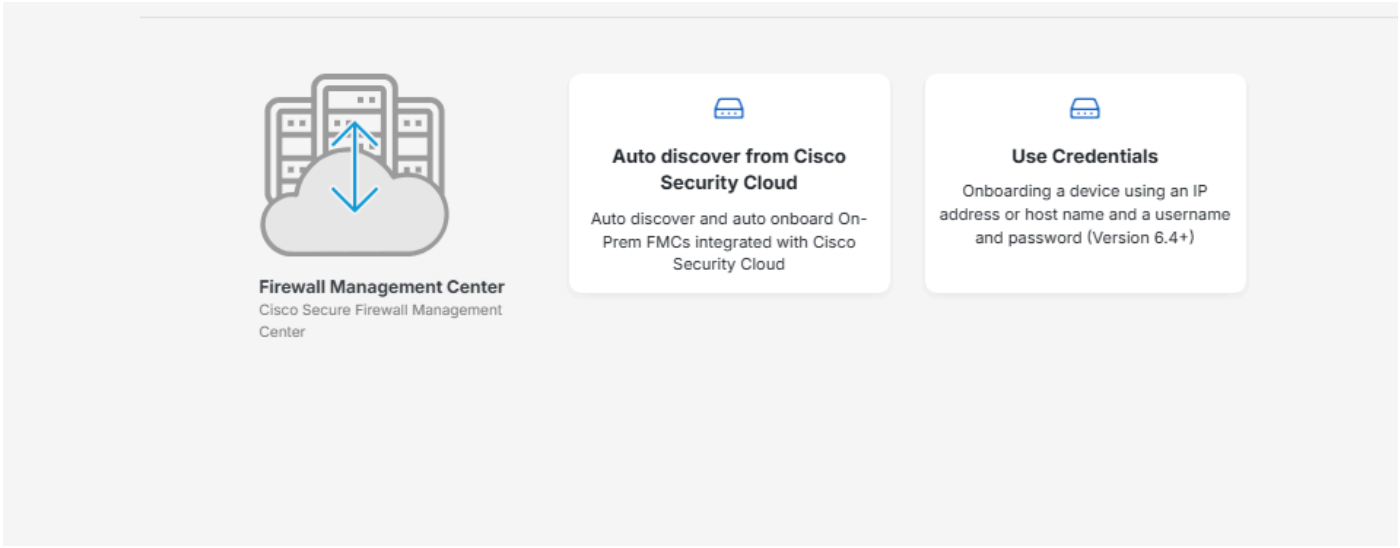
印度地区：

- in.cdo.cisco.com

第2步：导航到安全云控制（链接可能因您所在的区域而异），这会引导您选择安全云控制组织。



步骤3.选择适当的组织后，导航到产品>防火墙，验证您的设备是否已经存在，如果没有，您可以将其加入安全云控制(Cisco Defense Orchestrator)，为此，在“整体库存”下，单击“查看所有设备”。

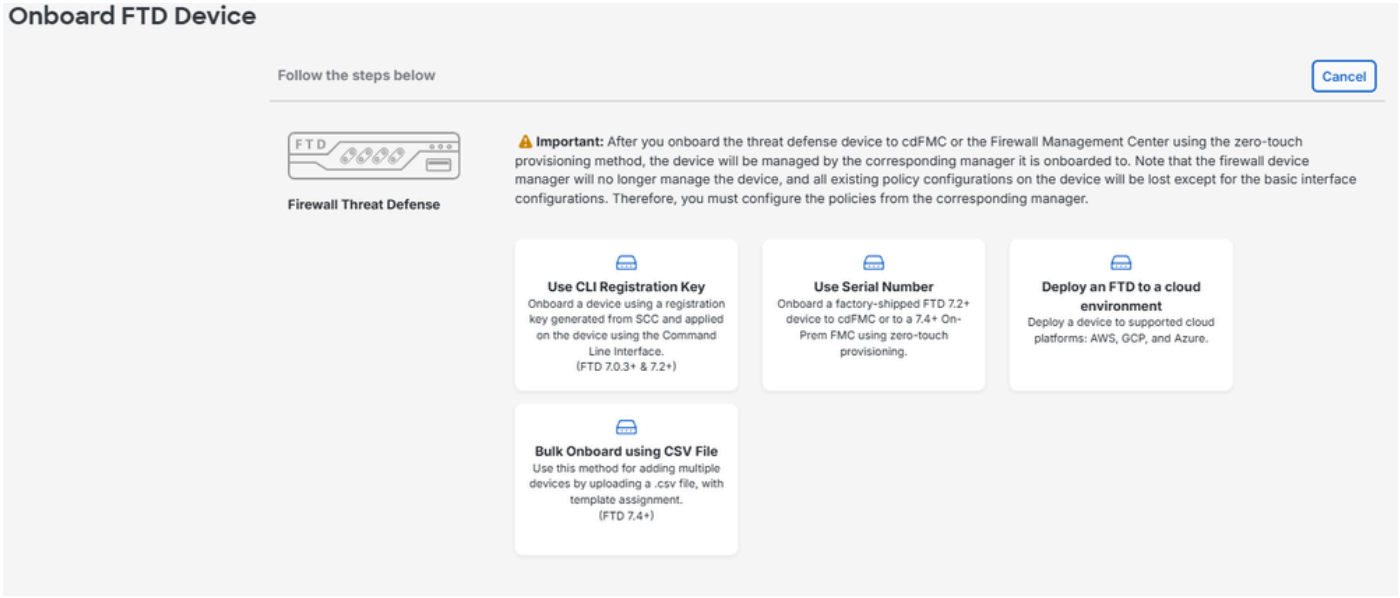


第4步：导航到管理>防火墙管理中心，系统将显示集成到SCC的FMC列表；如果未看到防火墙管理中心，请单击加号图标。

第4.1步：通常，Secure防火墙将自动登录，如果不自动登录，请选择您要登录的设备(FTD)和您的首选登录方法。

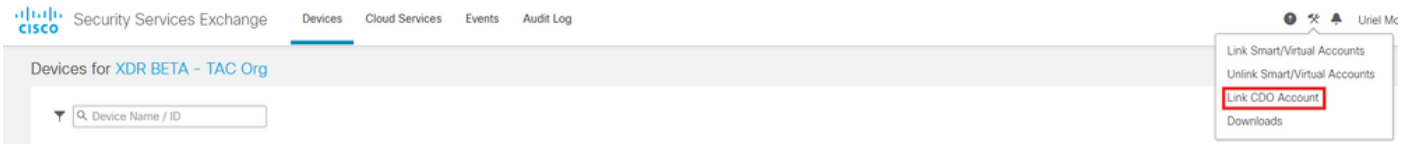
第4.2步：在安全设备(Security Devices)部分下，点击加号图标，选择板载安全防火墙设备和您的首选





步骤5.在Security Cloud Control中登录设备后，您可以在资产中看到设备。

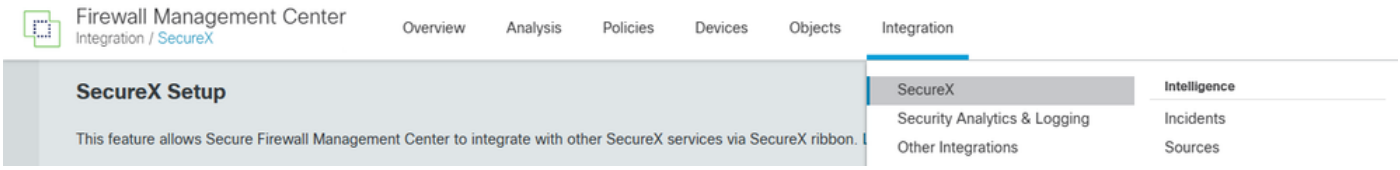
第6步：确保您的CDO组织已链接到您的SSX组织，为此，请导航到安全服务Exchange，单击工具菜单图标，然后单击链接CDO帐户。



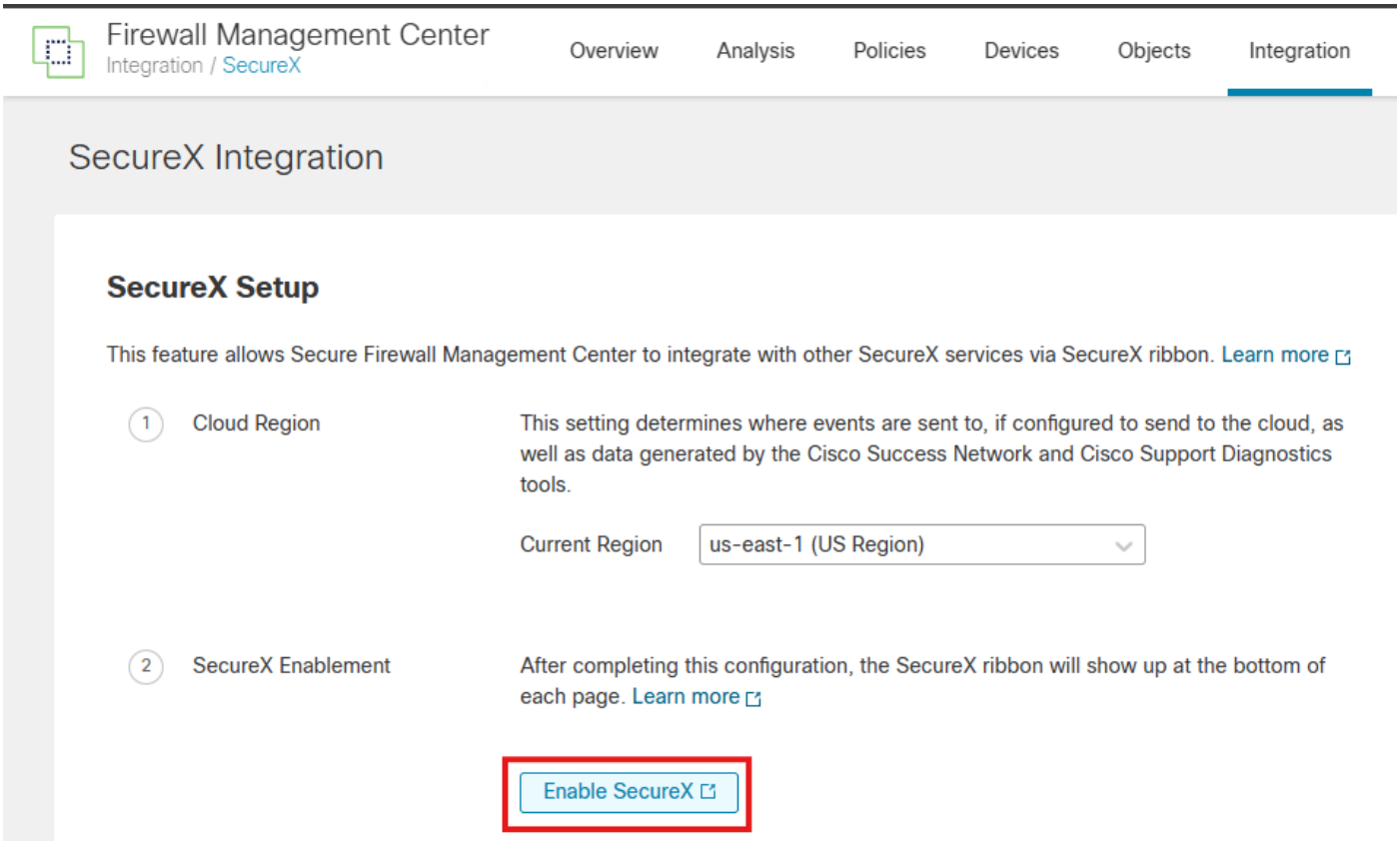
集成安全防火墙

从7.2.x到7.4.x（使用Cisco XDR）

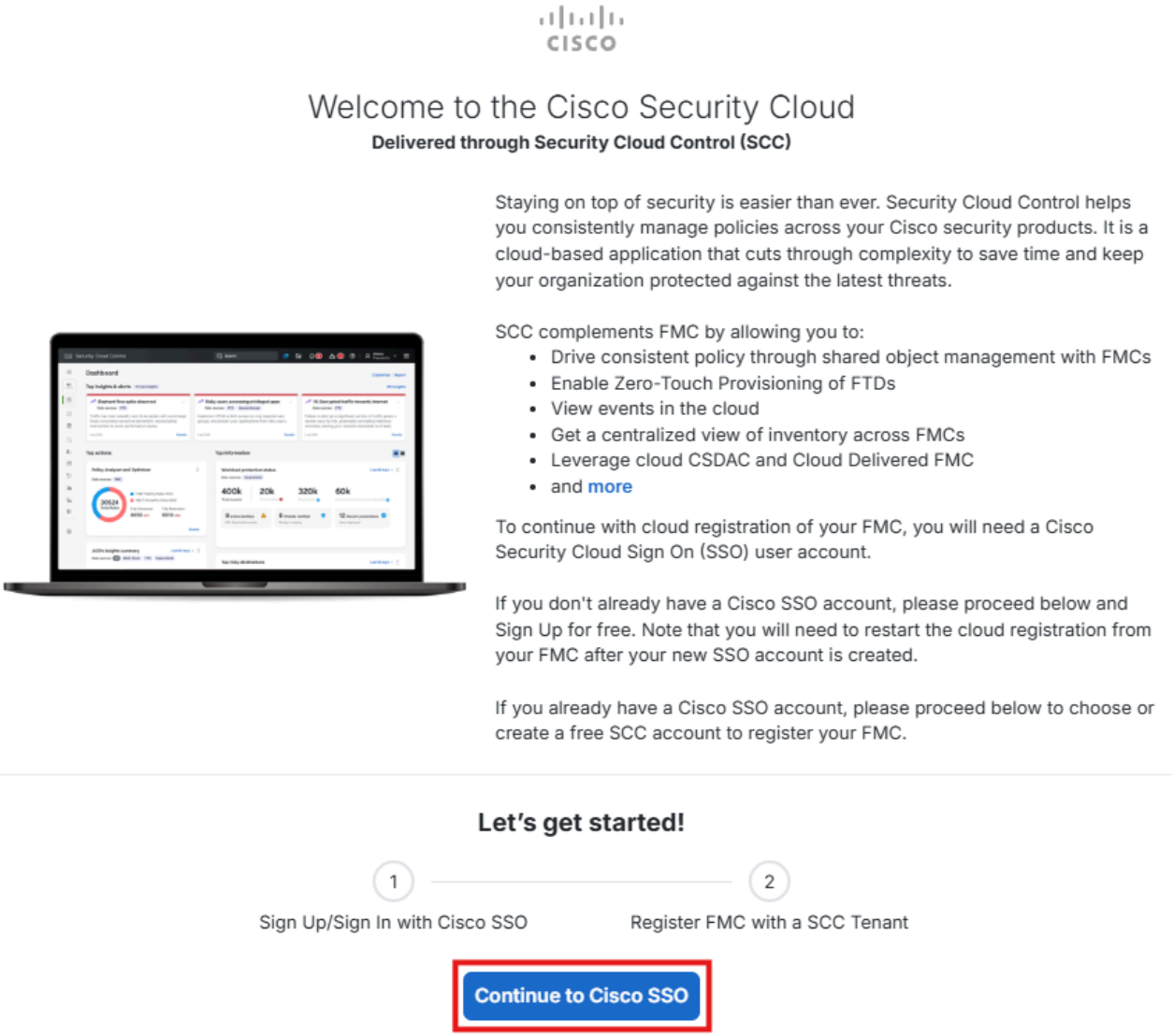
步骤1.在安全防火墙管理中心中，导航到集成> SecureX



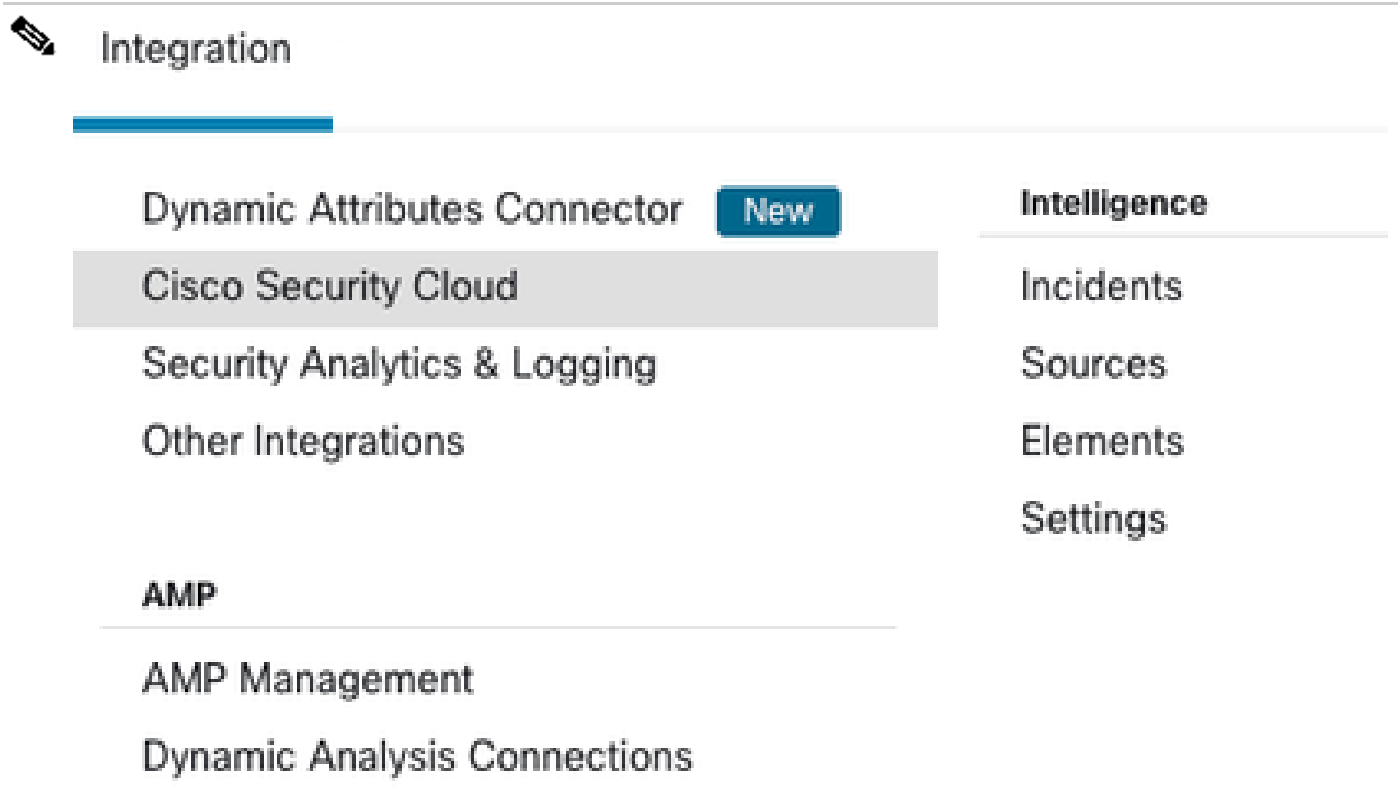
步骤2.选择正确的区域，然后点击Enable SecureX。



第 3 步： 点击Enable SecureX后，它将您重定向到Cisco Defense Orchestrator Authentication Page（利用安全云登录），然后点击Continue to Cisco SSO。



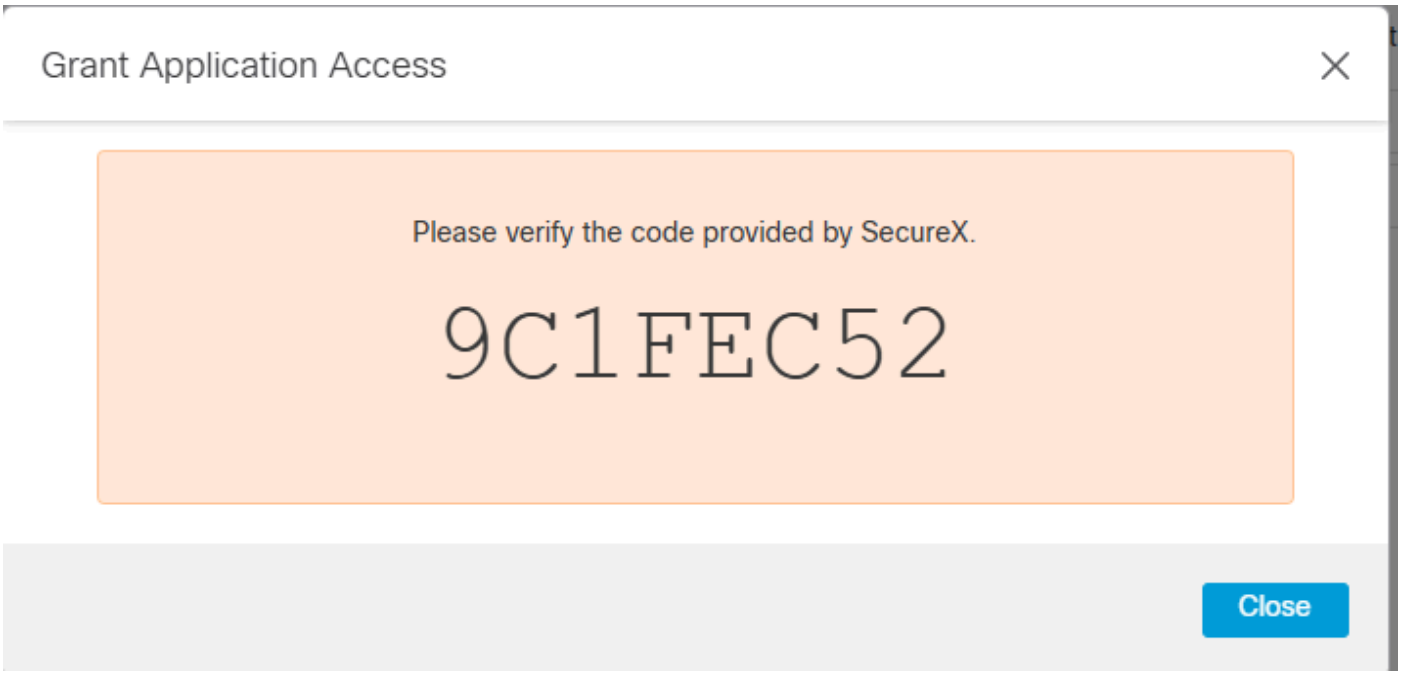
注意：
从7.6.x及更高版本通过Cisco XDR
步骤1.在您的安全防火墙管理中心中，导航到集成 > 思科安全云

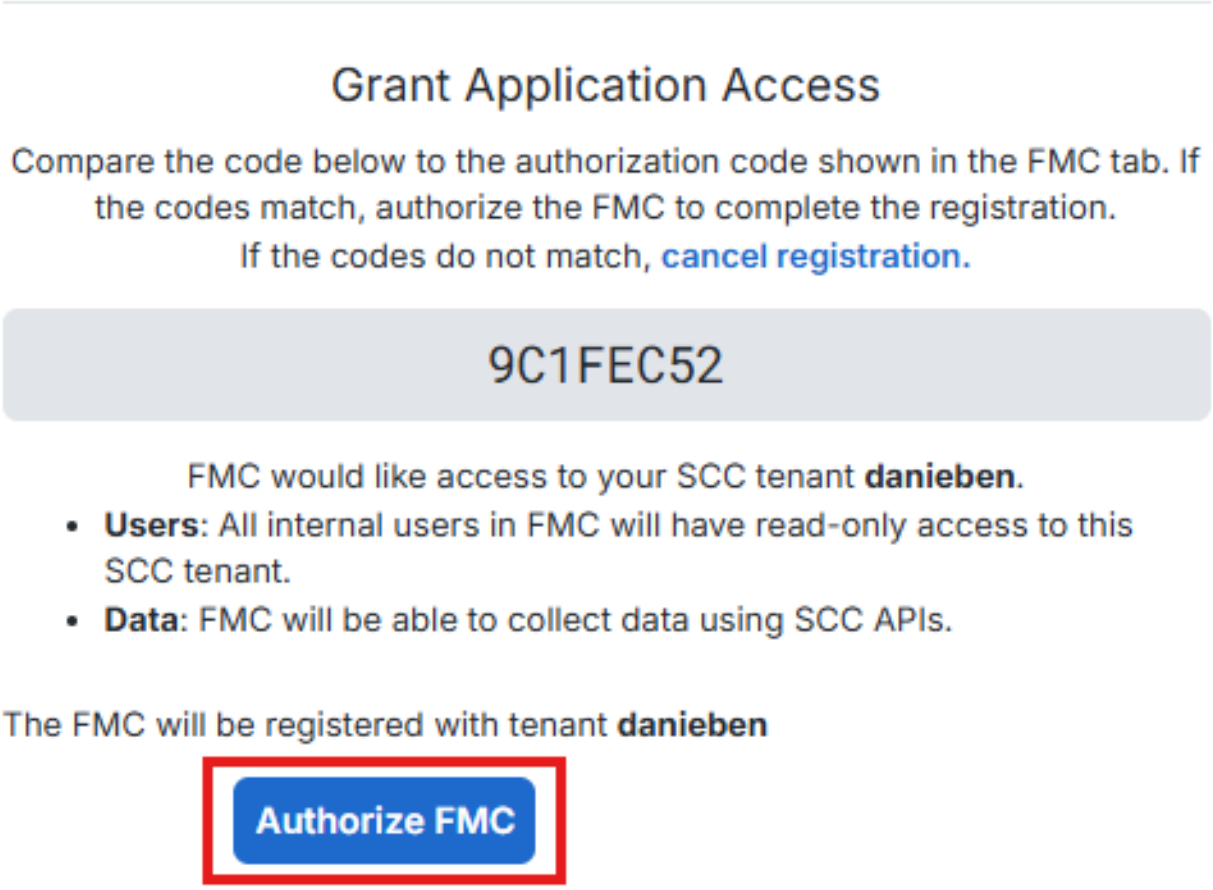


步骤2.选择正确的区域，然后单击启用思科安全云。
第 3 步： 点击Enable Cisco Security Cloud后，它将您重定向到Cisco Defense Orchestrator Authentication Page（利用安全云登录），然后点击Continue to Cisco SSO。

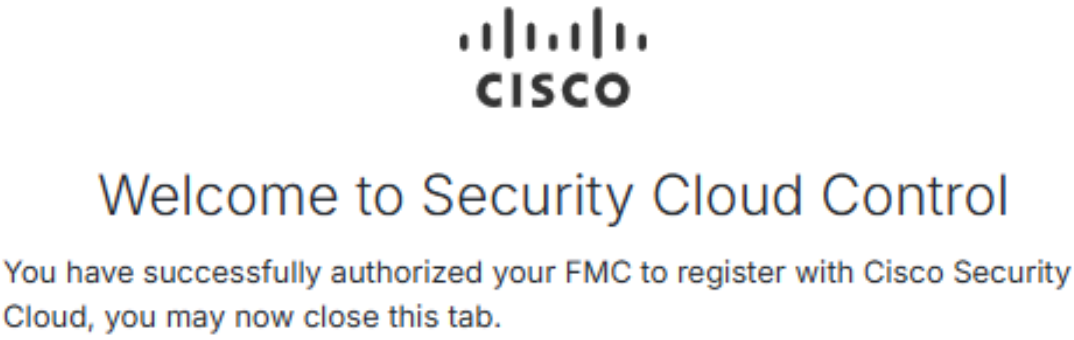
步骤4.您可以选择现有安全云控制租户或创建新租户。

第5步：选择适当的租户，并确保您在此页面中收到的代码与您在FMC中收到的代码匹配，如果匹配，请点击授权FMC。



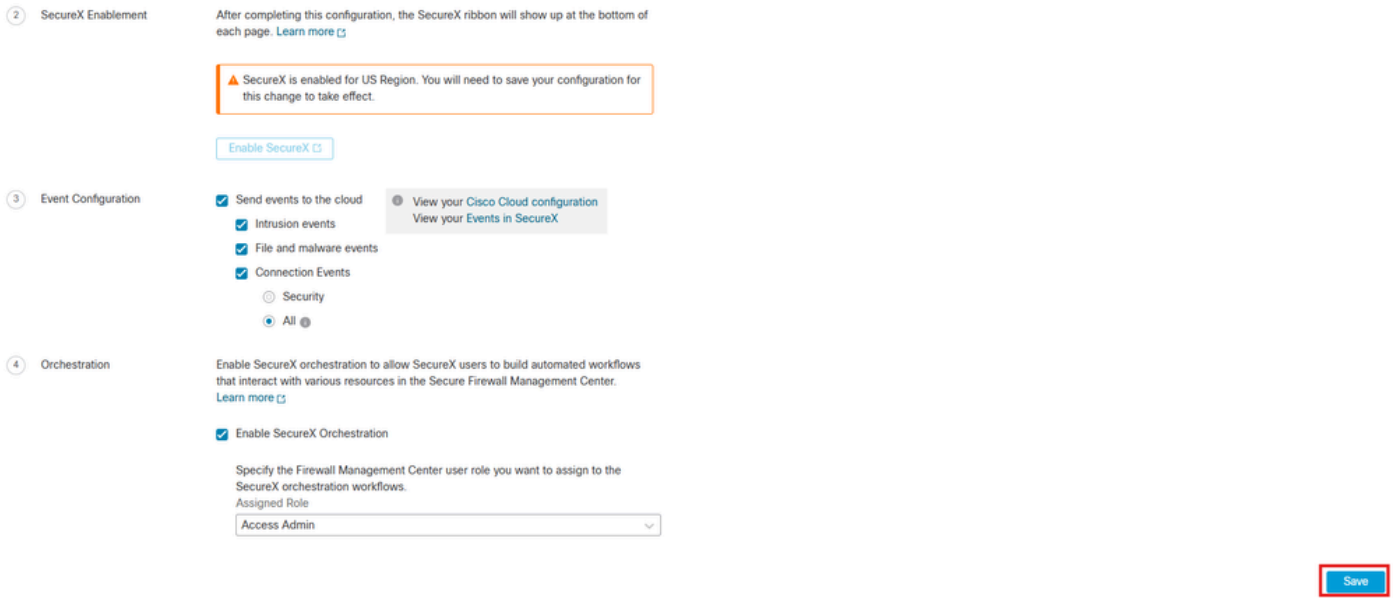


第6步：输入您的安全云登录凭证并授权集成，一旦完成，系统将显示确认FMC已获授权注册到思科安全云。



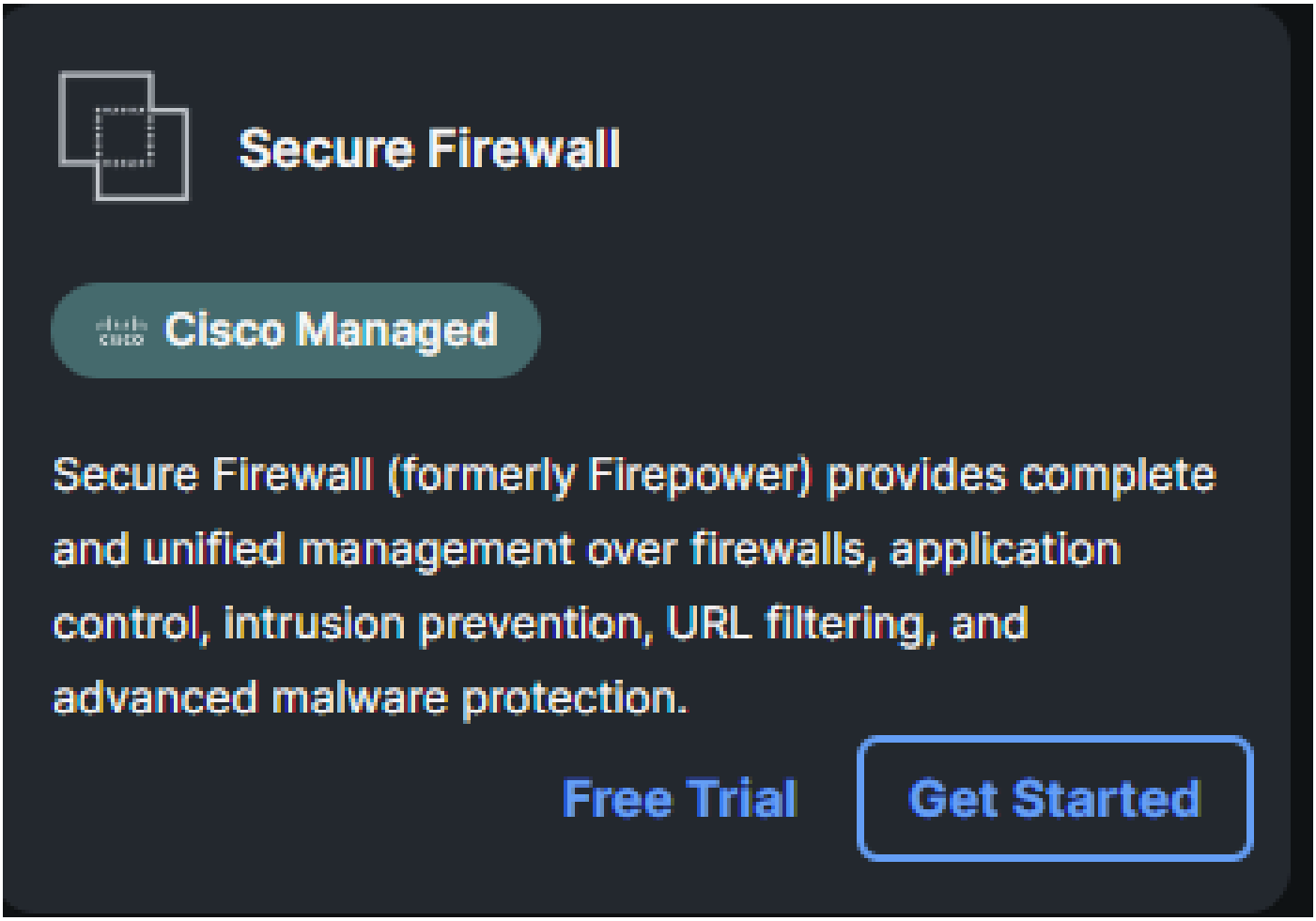
第7步：完成授权后，您可以导航回您的FMC，选择要发送到云的事件，并在完成此操作后，点击保存。

步骤8.您可以选择启用SecureX Orchestration（XDR自动化）

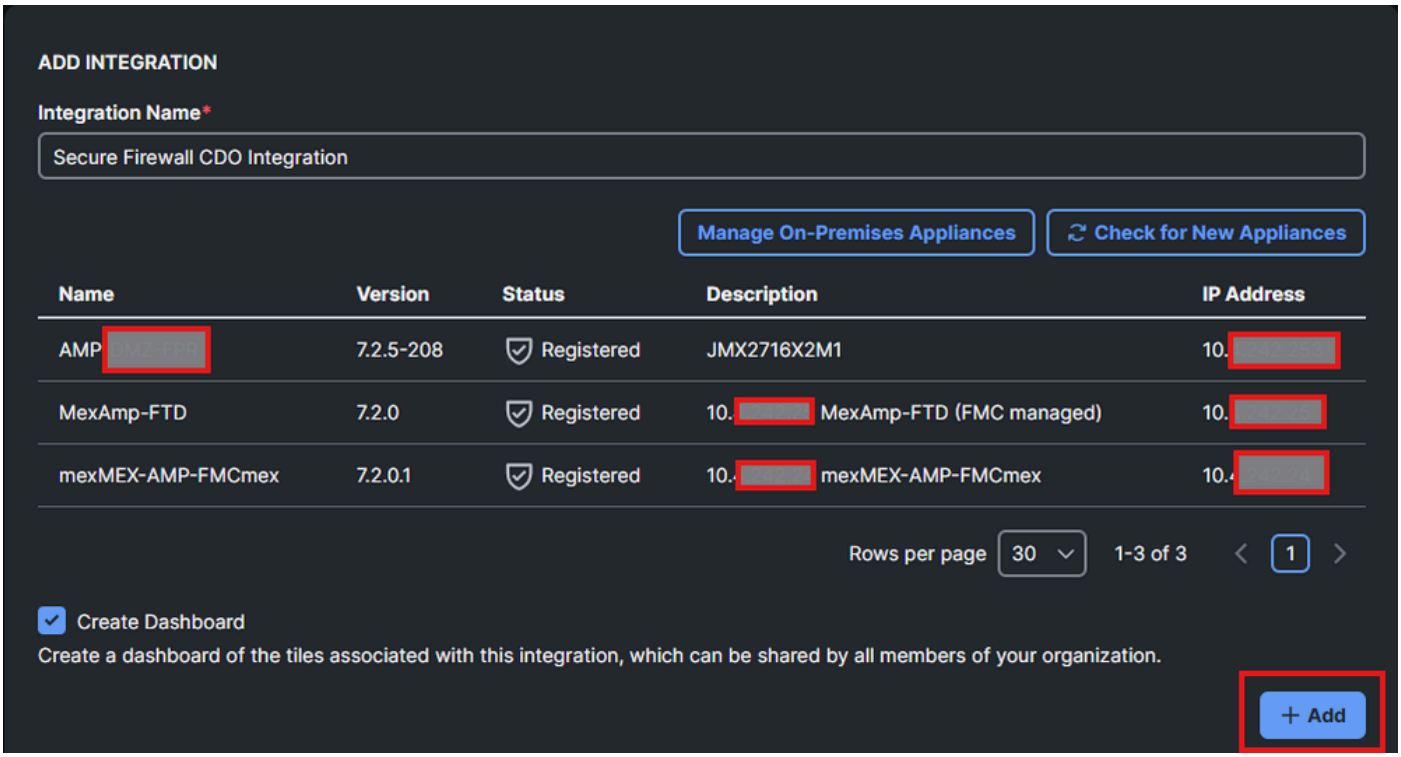


第9步：导航到XDR>管理>本地设备，搜索您的设备，这些设备必须自动注册。

步骤10.导航到XDR > Administration > Integrations，然后启用Secure Firewall Integration。



第10.1步：为您的集成分配名称，点击+Add。



通过这种集成，您可以在XDR中丰富调查工作。

方法2（完全集成）：丰富XDR中的事件

注意：为了确保安全防火墙、XDR、思科防御协调器(CDO)、安全服务交换(SSX)和安全分析和记录(SAL)之间的无缝集成，需要手动映射。此过程涉及联系思科TAC以执行必要的配置和映射。

步骤1.您的CDO帐户必须具有安全分析和记录许可证，才能将事件转发到Cisco XDR。

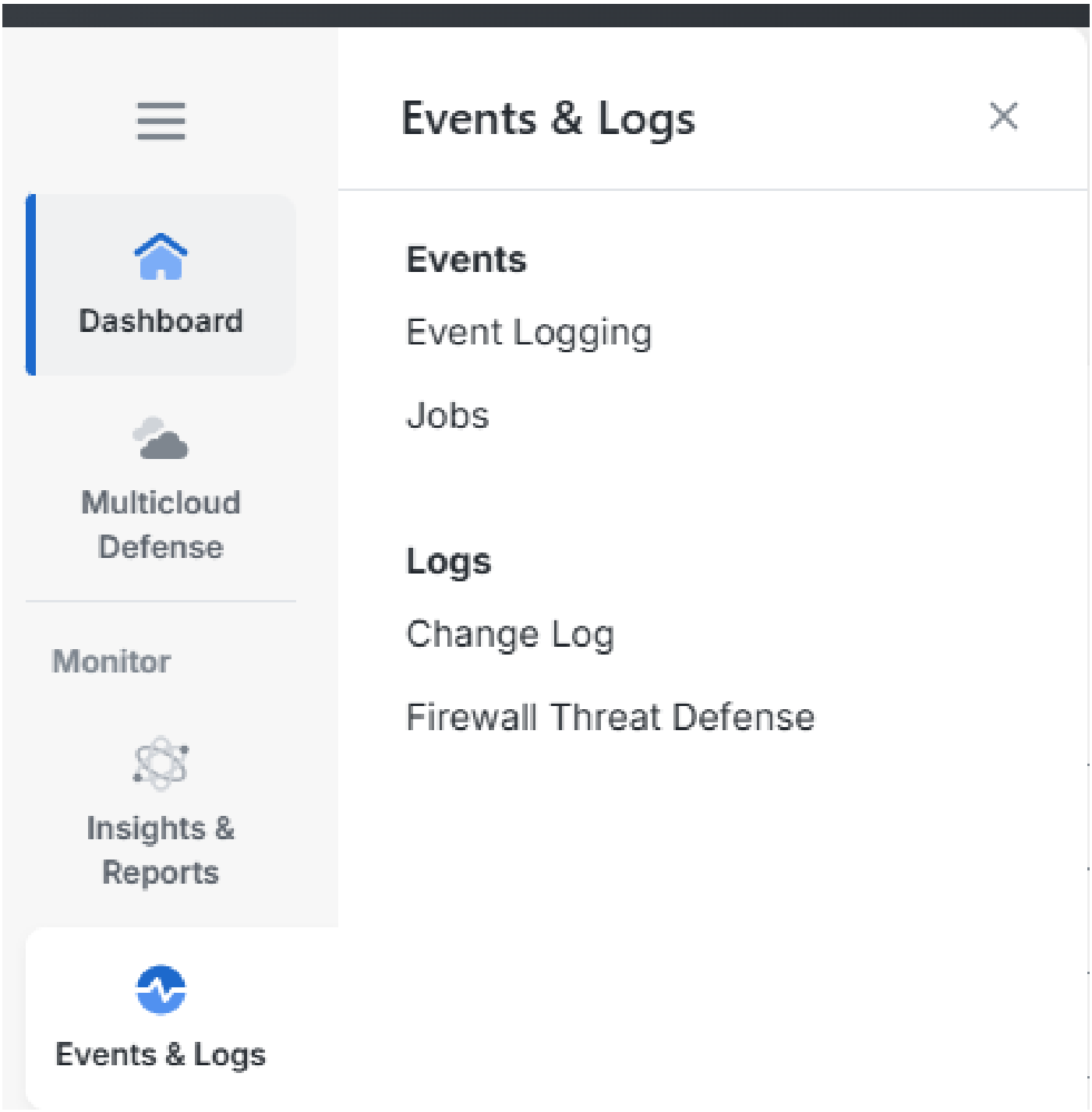
步骤2.请使用前面介绍的步骤在SSX和安全云控制中注册设备。

第3步：完成后，请联系TAC以了解这些详细信息，并请求将安全云控制/SAL链接到XDR分析。

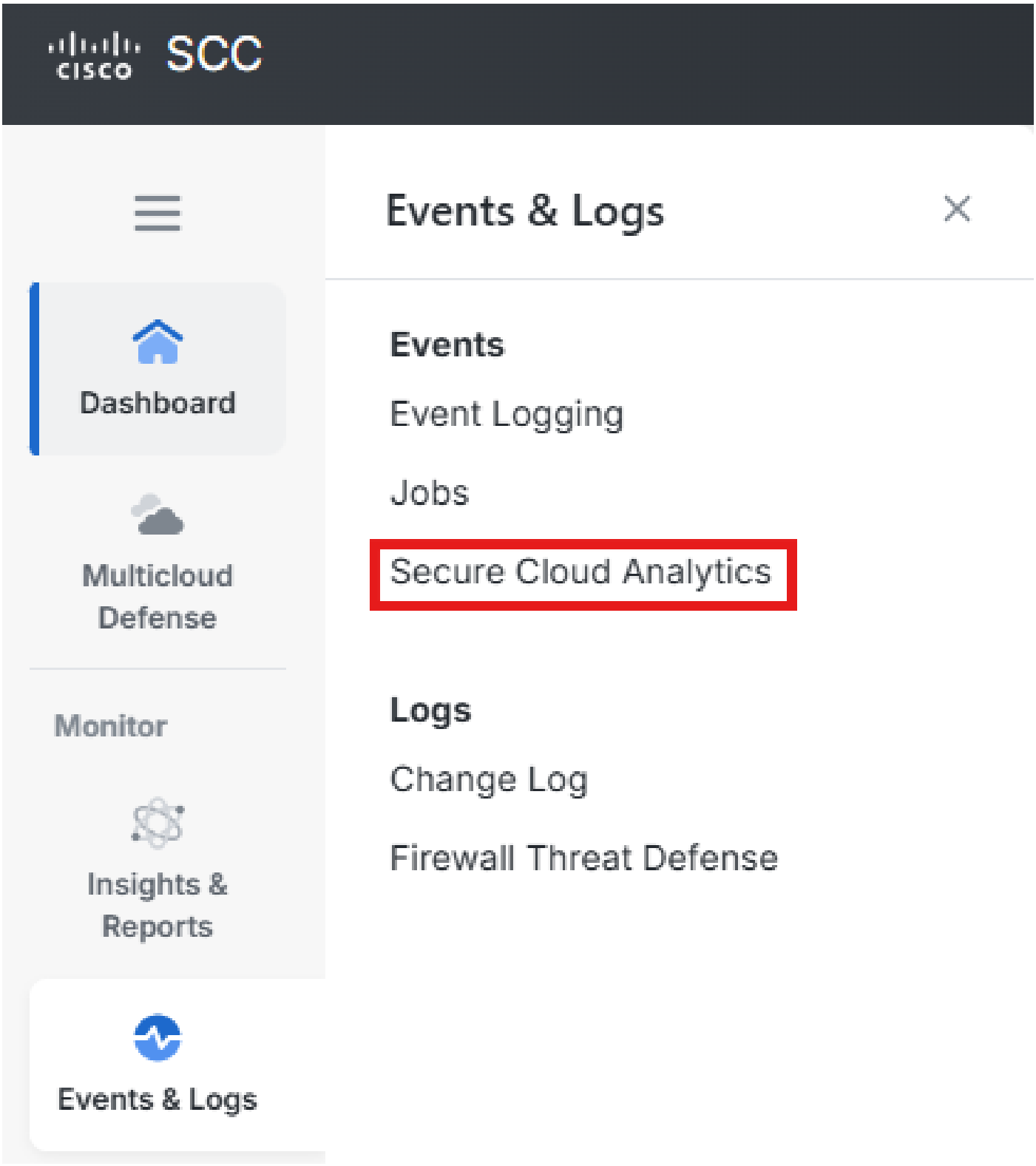
- CDO租户ID
- CDO名称
- XDR组织ID
- SSX租户ID
- SSX名称
- SCA组织ID

步骤4.确保您的CDO帐户已链接到XDR分析门户。

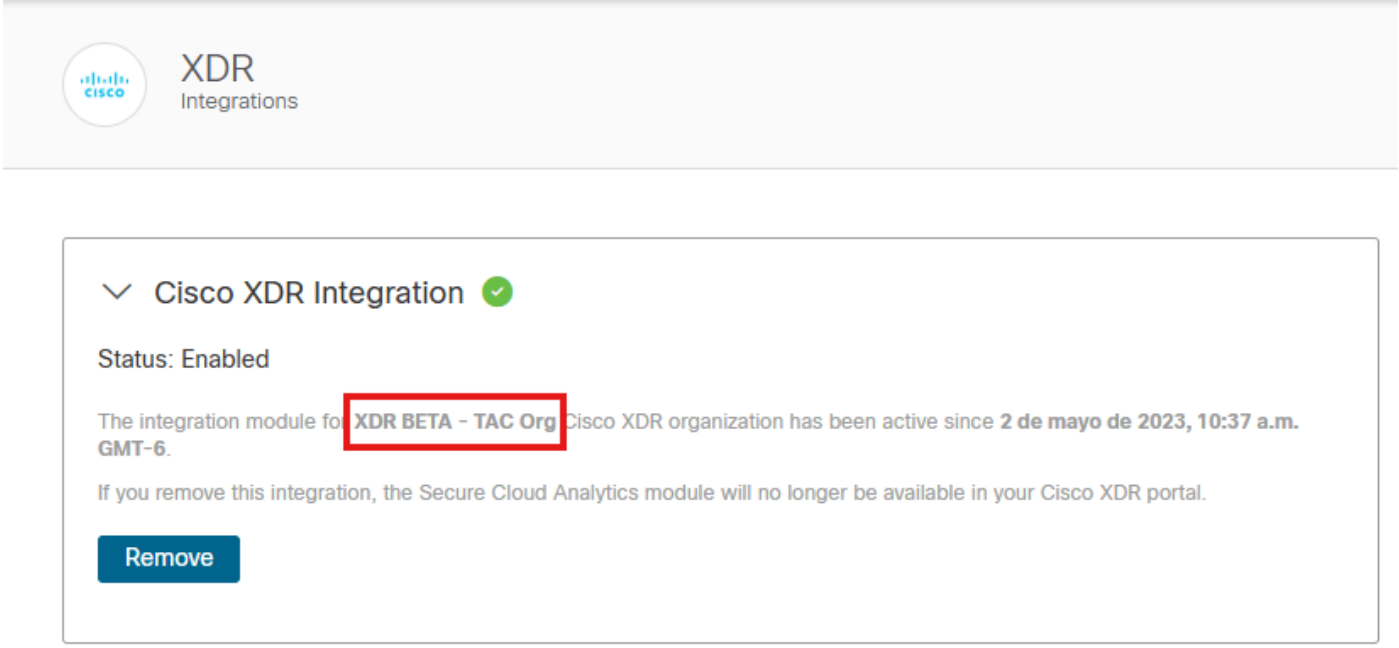
在将CDO门户链接到XDR分析之前，它如下所示：



链接完成后，您可以看到导航到XDR分析门户的选项。



第5步：在将XDR分析帐户链接到安全云控制门户(CDO)后，您需要确保XDR分析与XDR集成，为此，在XDR分析中，导航到设置>集成> XDR，查找XDR集成，并确保进行绿色检查，同时集成模块指向正确的XDR组织。



验证

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

按照将设备注册到SSX部分第4步所述，验证在SSX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。

验证所有租户是否正确链接在一起，如果存在问题，请打开TAC案例并提供以下详细信息：

- CDO租户ID
- CDO名称
- XDR组织ID
- SSX租户ID
- SSX名称
- SCA组织ID

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.检查连通性是否正常工作。

```
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;
```

SSX门户的注册问题

FMC和安全防火墙都需要连接到其管理接口上的SSX 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，因为从测试中发送的参数不是SSX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SSX门户和CTR的数据

要从安全防火墙设备向SSX发送事件，需要使用https://eventing-ingest.sse.itd.cisco.com建立TCP连接。以下是SSX门户和安全防火墙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
```

> 注意：请注意，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，因此建议允许基于URL而不是IP地址的数据流进入SSX门户。

如果此连接未建立，则事件不会发送到SSX门户。下面是安全防火墙和SSX门户之间已建立的连接的示例：

```
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.
```

设备(FTD)无法注册到安全云控制

如果您的设备无法注册到安全云控制，请确保它已连接到相应的CDO租户。

要验证正确的URL，请导航到Administration > Firewall Management Center，选择Cloud Delivered FMC，在屏幕右上角可以看到主机名。

```
admin@MexAmpFTD:~$ nc -vz xxxxxxxx.app.us.cdo.cisco.com 443
Connection to xxxxxxxx.app.us.cdo.cisco.com 443 port [tcp/https] succeeded!
```

如果您仍然面临连接到CDO的问题，请确保端口8305已打开，这是连接问题的一个示例。

```
admin@AMP-DMZ-FPR:~$ sudo tail /ngfw/var/log/messages
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneld:sf_peers [INFO] Peer xxxxxxxx.app.us.cdo.ci
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneld:sf_ssl [INFO] Connect to xxxxxxxx.app.us.cd
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneld:sf_ssl [INFO] Initiate connection using res
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneld:sf_ssl [INFO] Initiate IPv6 type connection
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneld:sf_ssl [INFO] Initiate IPv4 type connection
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneld:sf_ssl [INFO] Initiate IPv4 connection from
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneld:sf_ssl [INFO] Initiating IPv4 connection to
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneld:sf_ssl [INFO] Wait to connect to 8305 (IPv4
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneld:sf_ssl [INFO] Connect to x.x.x.51 failed on
```

设备注册到错误的SSX租户

您可以验证您的FMC注册到哪个SSX租户。

```
admin@fmc01:~$ curl localhost:8989/v1/contexts/default/tenant

{"registeredTenantInfo":{"companyId":"689xxxxx-eaxx-5bxx-b1xx-a7662axxxxx","companyName":"XDR BETA - TA
```

如果SSX租户不正确，您需要重新执行在SSX中注册设备的步骤

如果SSX租户正确，但CDO租户未链接到相应的SSX组织，请联系TAC以了解以下详细信息：

- SSX租户ID
- CDO租户ID

相关信息

- 思科安全防火墙威胁防御和思科XDR集成指南
- 思科技术支持和下载

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）。