دمج Cisco XDR واستكشاف أخطائه وإصلاحها باستخدام جدار الحماية الآمن

المحتويات

المقدمة

يصف هذا المستند الخطوات المطلوبة لدمج Cisco XDR مع جدار الحماية الآمن والتحقق من صحته واستكشاف أخطائه وإصلاحها.

هناك طريقتان لدمج Secure Firewall و XDR، وكل دمج يوفر نتائج مختلفة.

تصف الطريقة الأولى كيفية دمج جدار الحماية الآمن، وتبادل خدمات الأمان (SSX)، والتحكم في سحابة الأمان، وتحليلات XDR و XDR لإثراء التحقيقات.

تصف الطريقة الثانية كيفية دمج جدار الحماية الآمن و SSX والتحكم في سحابة الأمان و XDR-A و SAL Cloud و XDR لإثراء الحوادث.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- مركز إدارة Firepower (FMC)
- جدار الحماية الآمن
- المحاكاة الافتراضية الاختيارية للصور
- Cisco Defense Orchestrator
- تبادل خدمات الأمان
- التحكم في سحابة الأمان

المكونات المستخدمة

- جدار الحماية الآمن - 7.2
- مركز إدارة Firepower (FMC) - 7.2
- تبادل خدمات الأمان (SSX)
- XDR من Cisco
- بوابة الترخيص Smart
- Cisco Defense Orchestrator
- التحكم في سحابة الأمان

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

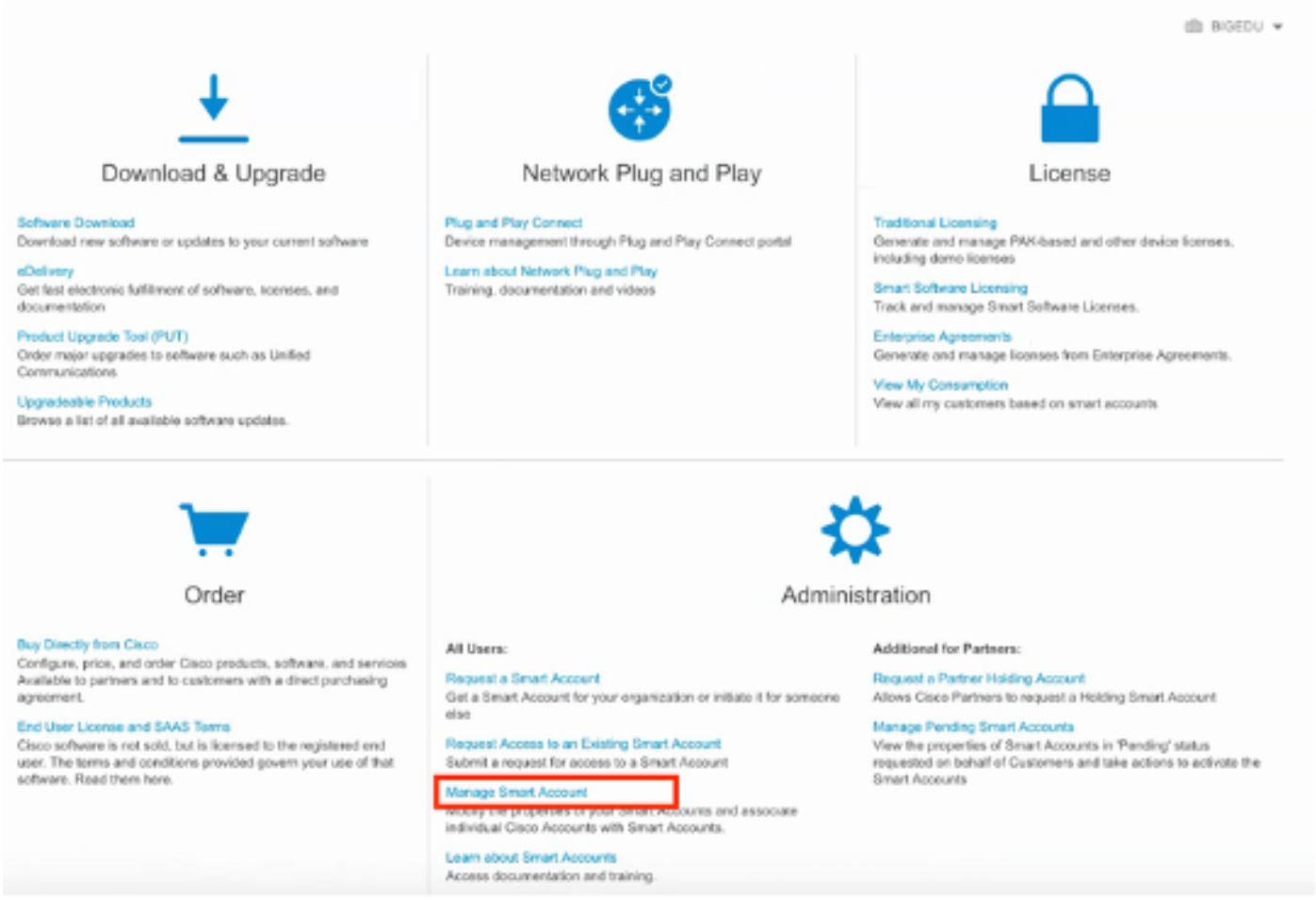
التكوين

الترخيص

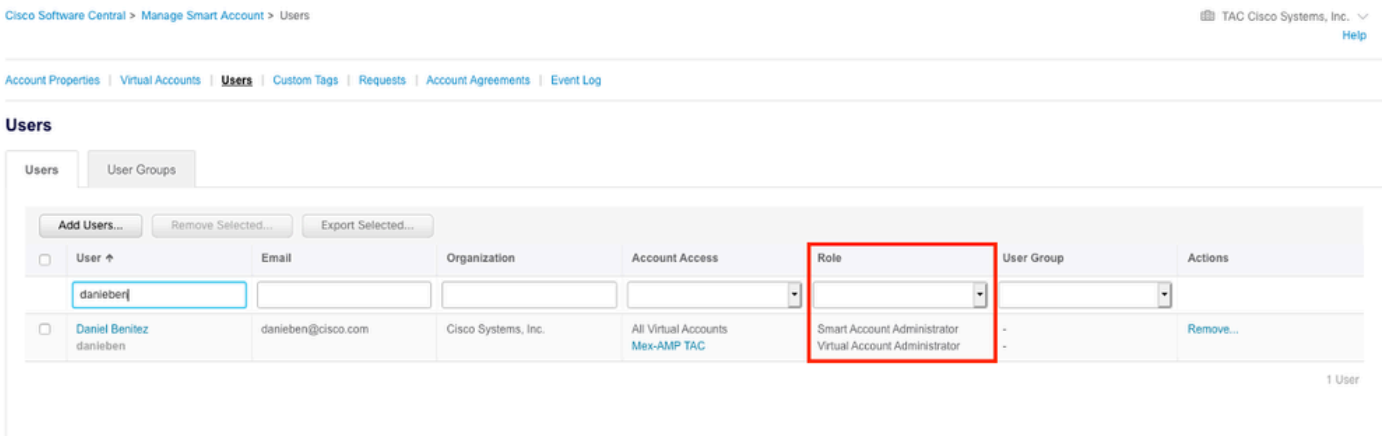
أدوار الحساب الظاهري:

يتمتع فقط مسؤول الحساب الظاهري أو مسؤول الحساب الذكي بامتياز ربط الحساب الذكي بحساب SSE.

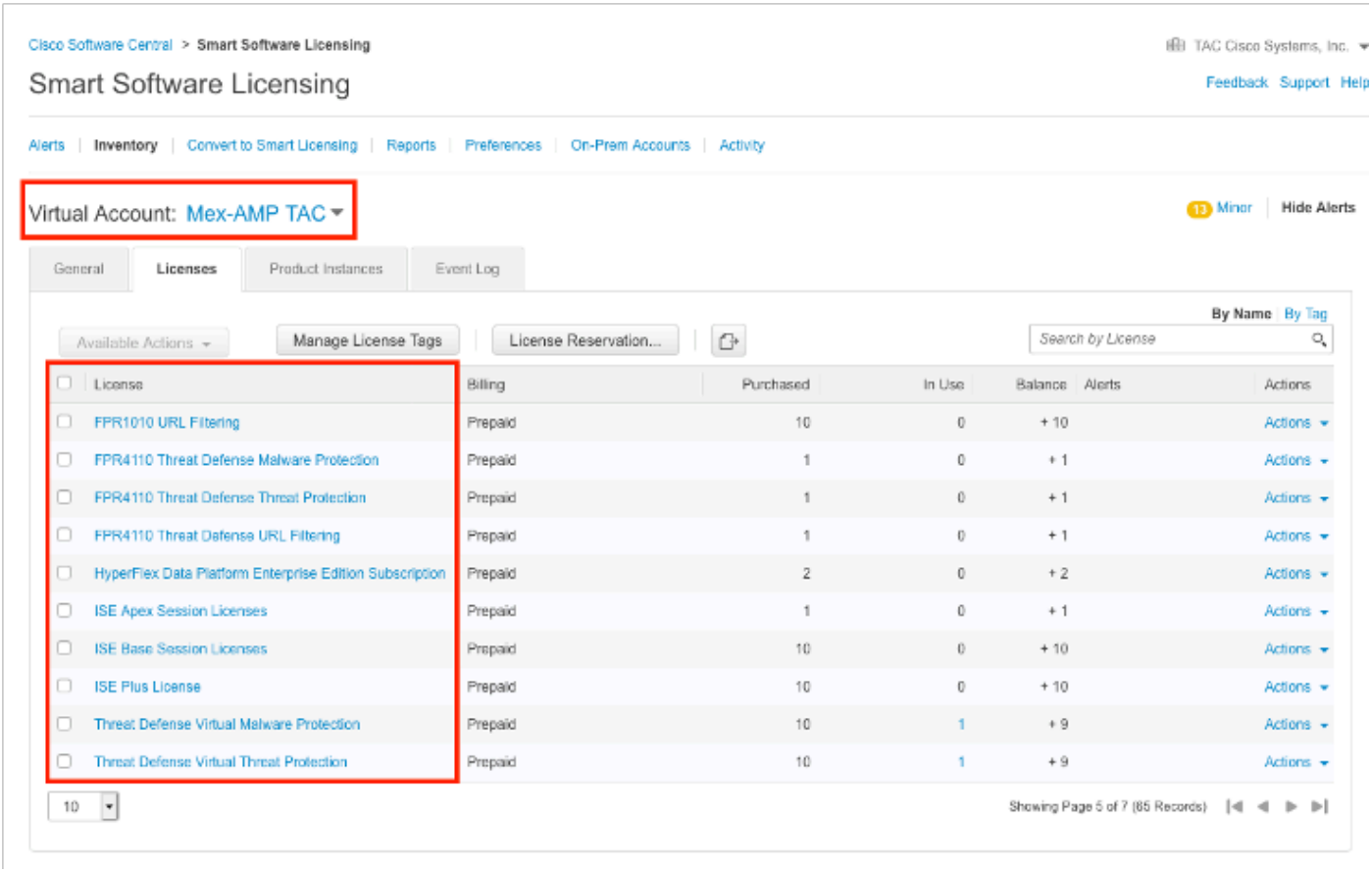
الخطوة 1. للتحقق من صحة دور الحساب الذكي، انتقل إلى software.cisco.com وتحت قائمة الإدارة، حدد إدارة الحساب الذكي.



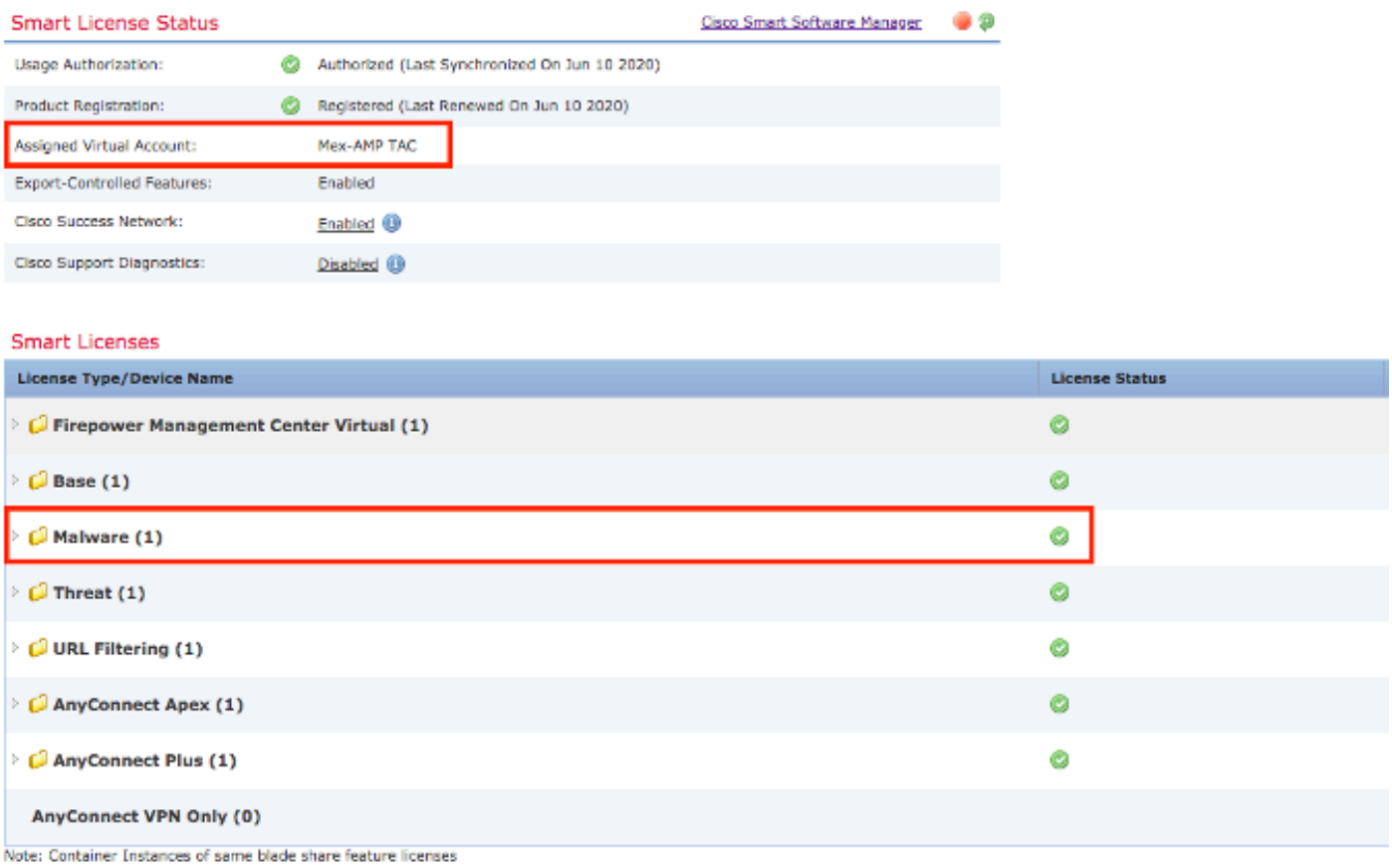
الخطوة 2. للتحقق من صحة دور المستخدم، انتقل إلى المستخدمين، وتحقق من تعيين الحسابات تحت الأدوار إلى مسؤول حساب ظاهري، كما هو موضح في الصورة.



الخطوة 3. تأكد من أن "الحساب الظاهري" المحدد للارتباط على SSE يحتوي على ترخيص لأجهزة الأمان في حالة إرتباط حساب ال يحتوي على ترخيص الأمان على SSE وأجهزة الأمان والحدث ال يظهر على وابة SSE.

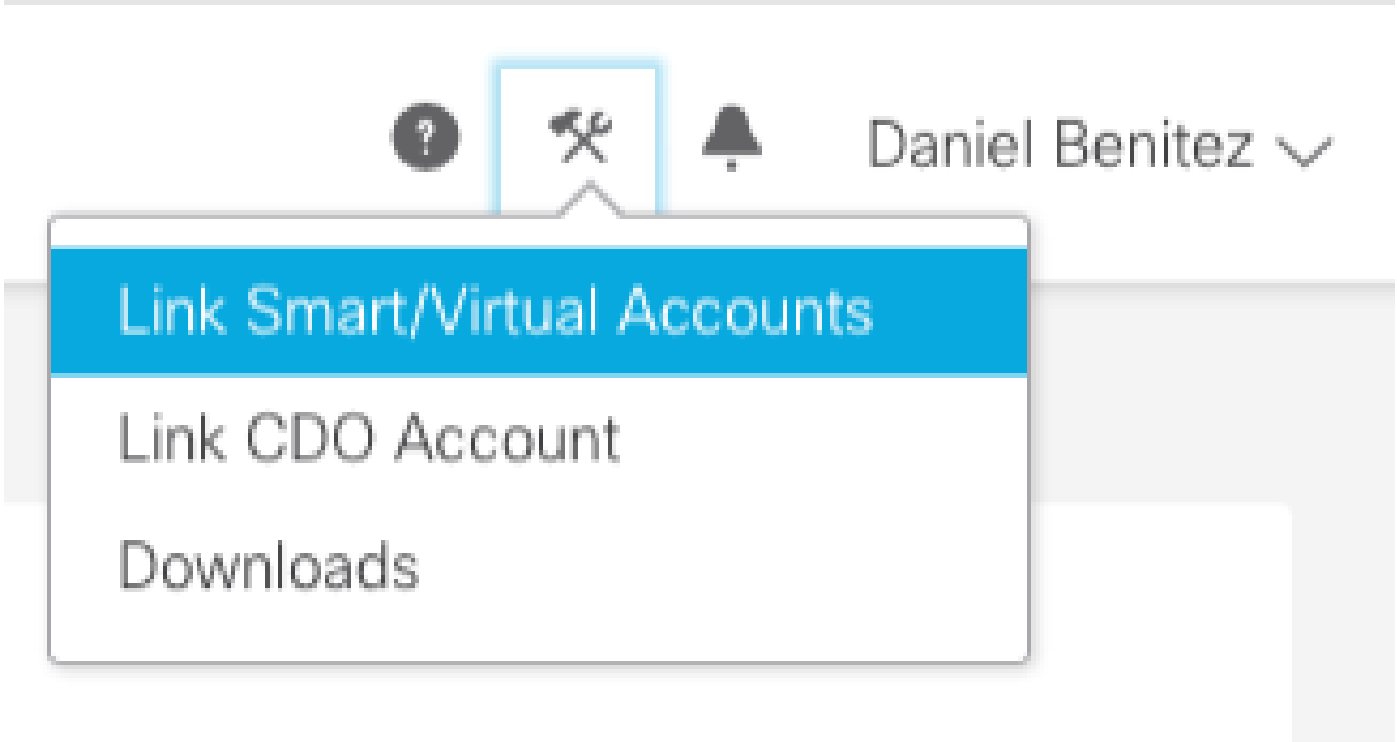


الخطوة 4. للتحقق من تسجيل FMC في الحساب الظاهري الصحيح، انتقل إلى تراخيص النظام>الترخيص الذكي:



أربط حساباتك ب SSE وسجل الأجهزة.

الخطوة 1. عند تسجيل الدخول إلى حساب SSE، يجب عليك ربط حسابك الذكي بحساب SSE، لذلك تحتاج إلى النقر فوق رمز الأدوات وتحديد ربط الحسابات.



بمجرد ربط الحساب، سترى الحساب الذكي الذي يحتوي على كافة الحسابات الظاهرية الموجودة عليه.

الطريقة 1 (نصف التكامل): إثارة التحقيقات

تسجيل الأجهزة في SSE

الخطوة 1. تأكد من أن عناوين URL هذه مسموح بها على بيئتك:

المنطقة الامريكية

- api-sse.cisco.com
- eventing-ingest.sse.itd.cisco.com
- mx*.sse.itd.cisco.com
- dex.sse.itd.cisco.com
- eventing-ingest.sse.itd.cisco.com
- registration.us.sse.itd.cisco.com

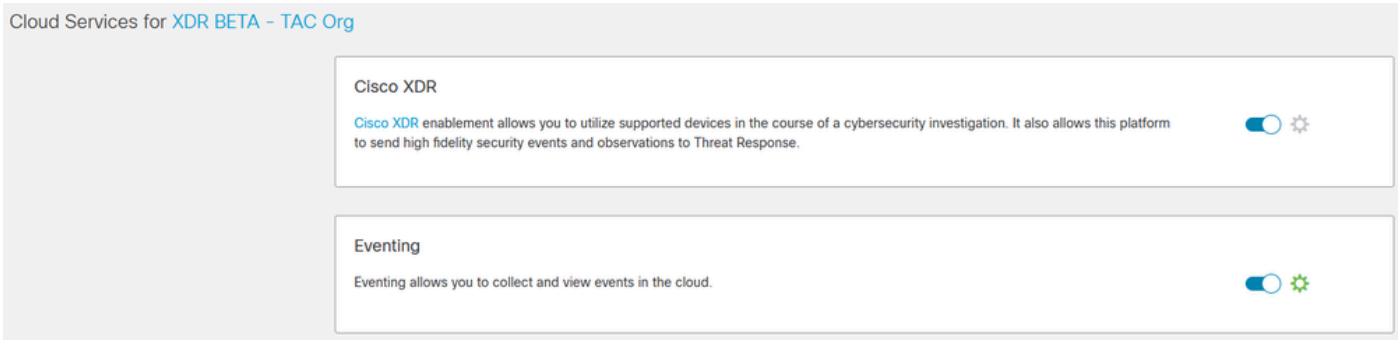
منطقة الاتحاد الأوروبي

- api.eu.sse.itd.cisco.com
- mx*.eu.sse.itd.cisco.com
- dex.eu.sse.itd.cisco.com
- eventing-ingest.eu.sse.itd.cisco.com
- registration.eu.sse.itd.cisco.com

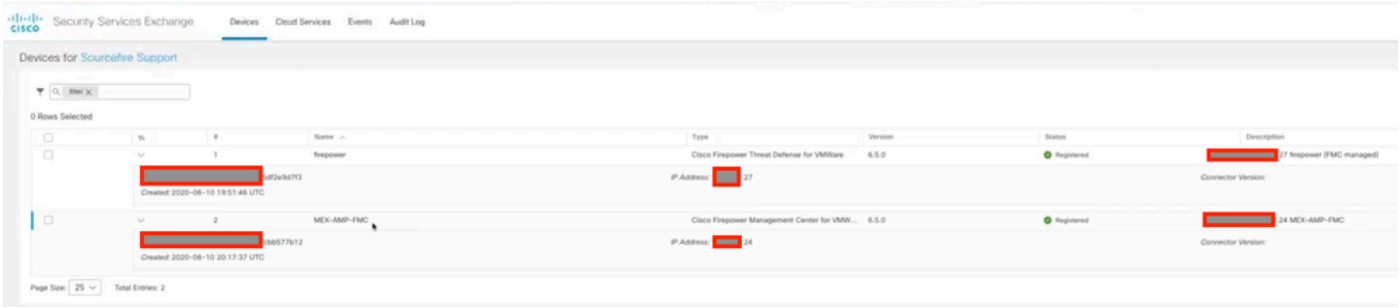
إقليم أبكان

- 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

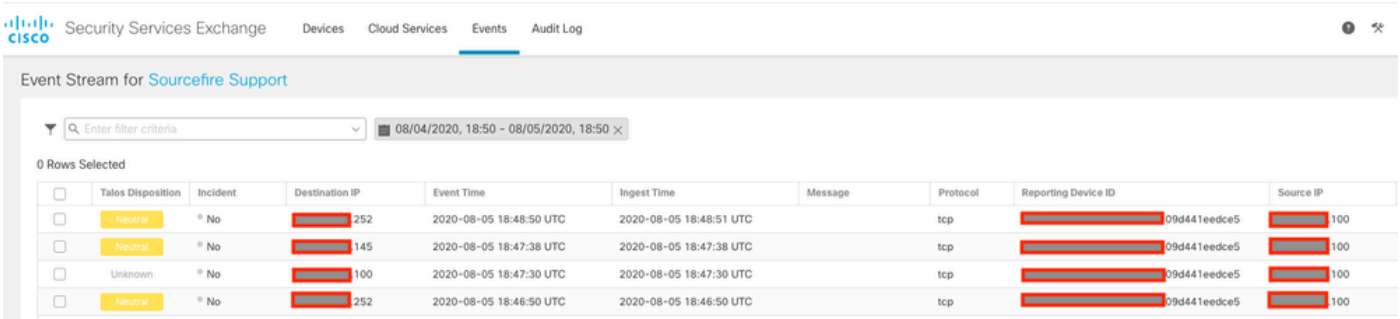
الخطوة 2. سجل الدخول إلى بوابة SSE باستخدام عنوان URL هذا https://admin.sse.itd.cisco.com، انتقل إلى خدمات السحابة، وقم بتمكين الخياري Eventing وCisco XDR response، كما هو موضح في الصورة التالية:



الخطوة 3. يمكنك التحقق من أنه يمكنك الآن رؤية الأجهزة المسجلة في SSE:



يتم إرسال الأحداث بواسطة أجهزة جدار الحماية الآمنة، انتقل إلى الأحداث الموجودة على بوابة SSX للتحقق من الأحداث التي تم إرسالها بواسطة الأجهزة إلى SSX، كما هو موضح في الصورة:



تسجيل الأجهزة في التحكم في سحابة الأمان (SCC/CDO)

الخطوة 1. تأكد من أن عناوين URL هذه مسموح بها على بيئتك

المنطقة الأمريكية:

- defenseorchestrator.com
- edge.us.cdo.cisco.com

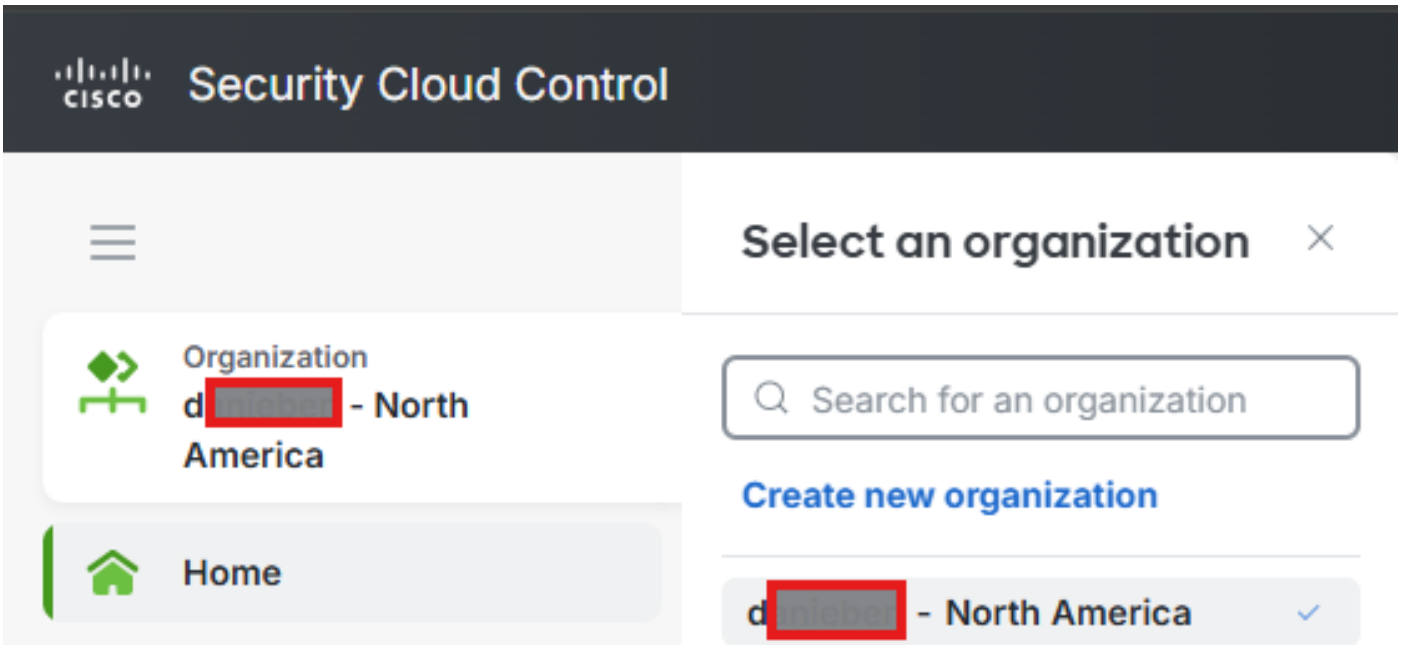
منطقة الاتحاد الأوروبي

- defenseorchestrator.eu
- edge.eu.cdo.cisco.com

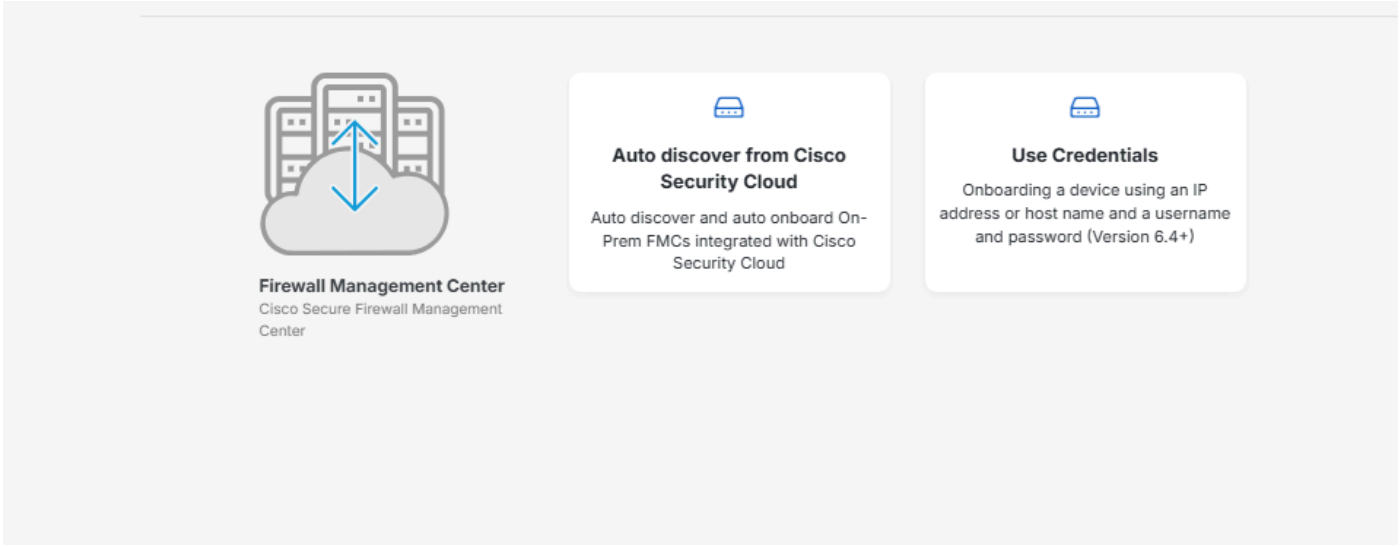
إقليم أبكان

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

الخطوة 2. انتقل إلى التحكم في شبكة الأمان (يمكن أن يختلف الارتباط حسب منطقتك) وهذا يوجهك لتحديد مؤسسة التحكم في سحابة الأمان.



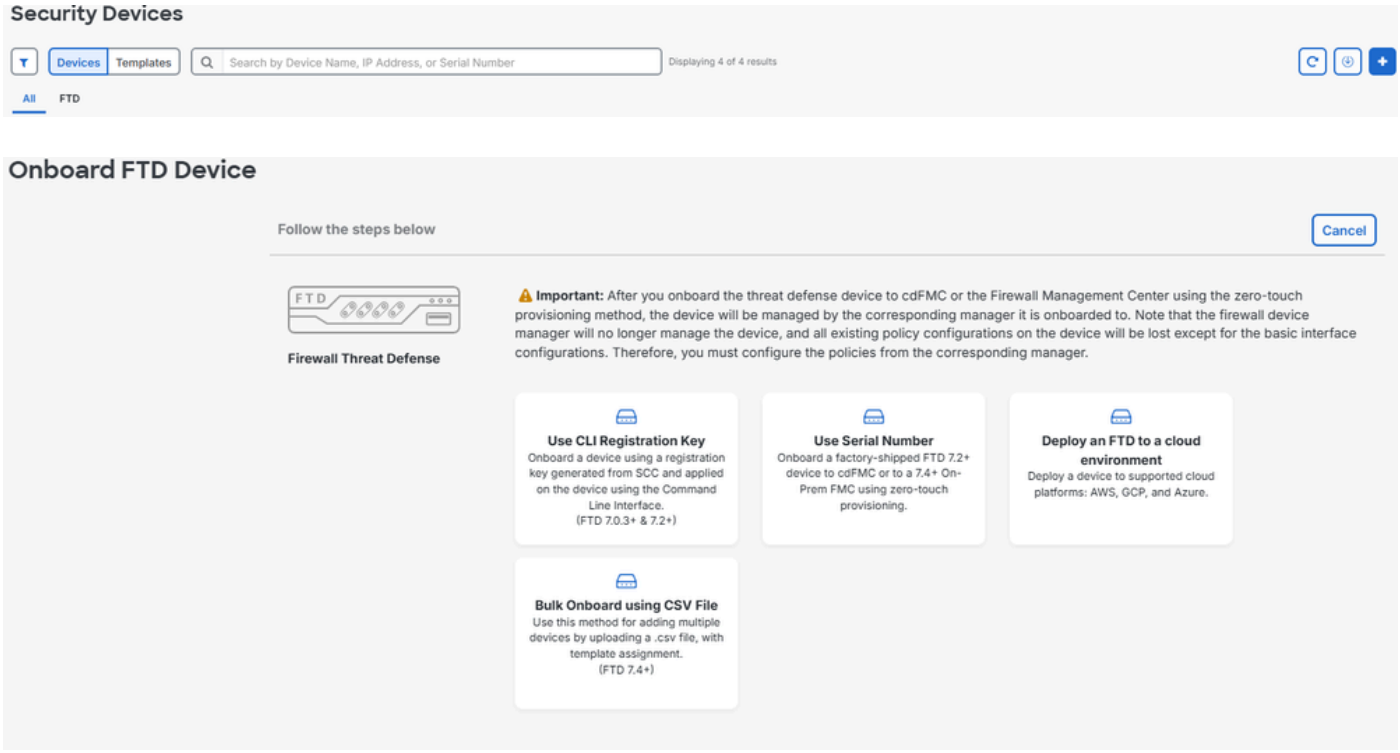
الخطوة 3. بمجرد تحديد المؤسسة المناسبة، انتقل إلى Products>Firewall، تحقق مما إذا كان الجهاز لديك موجودا بالفعل، إن لم يكن موجودا، فيمكنك تضمينه إلى التحكم في سحابة الأمان (Cisco Defense Orchestrator)، لهذا، ضمن قائمة الجرد العامة، انقر فوق تحديد جميع الأجهزة.



الخطوة 4. انتقل إلى Administration>مركز إدارة جدار الحماية، يتم تقديم قائمة بأنظمة FMC المدمجة في SCC، إذا لم ترى مركز إدارة جدار الحماية، انقر على رمز Plus.

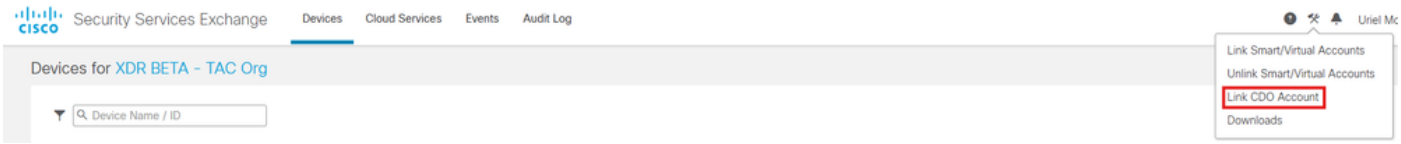
الخطوة 4.1. عادة، يتم إدراج جدران الحماية الآمنة لقائي على الوحة، إذا لم يكن الأمر كذلك، فحدد الجهاز الذي تريد إستخدامه على الوحة (في وضع FTD) وأسلوب تسجيل الدخول المفضل لديك.

الخطوة 4.2. تحت قسم أجهزة الأمان النقر فوق أيقونة زائد، حدد جهاز جدار الحماية الآمن على اللوحة



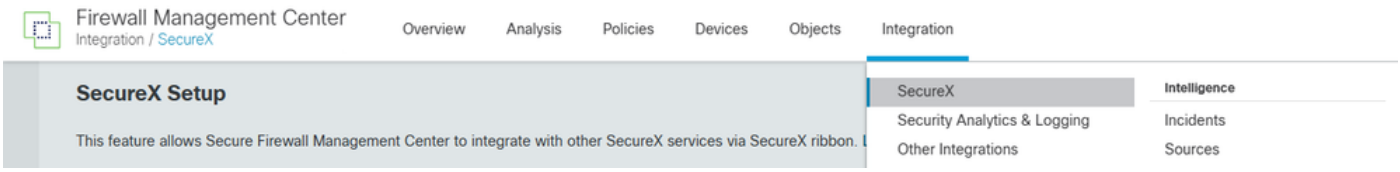
الخطوة 5. بمجرد تسجيل الوصول إلى أجهزتك في "التحكم في سحابة الأمان"، يمكنك تصورها في المخزون.

الخطوة 6. تأكد من أن مؤسسة CDO مرتبطة بمؤسسة SSX الخاصة بك، لهذا السبب، انتقل إلى "تبادل خدمات الأمان"، وانقر فوق رمز القائمة "أدوات"، وانقر فوق إرتباط حساب CDO.

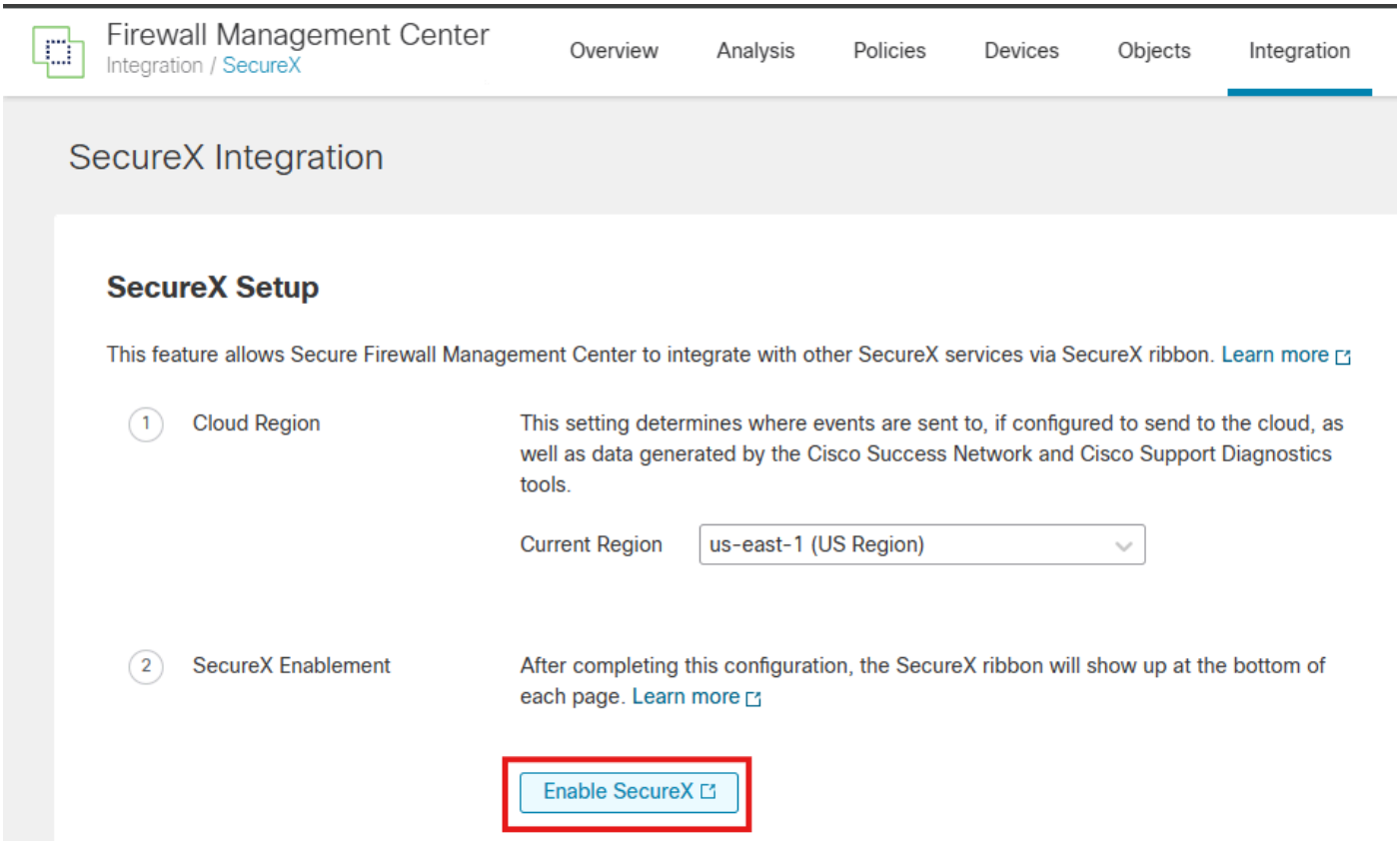


دمج جدار الحماية الآمن 7.2.x مع Cisco XDR.

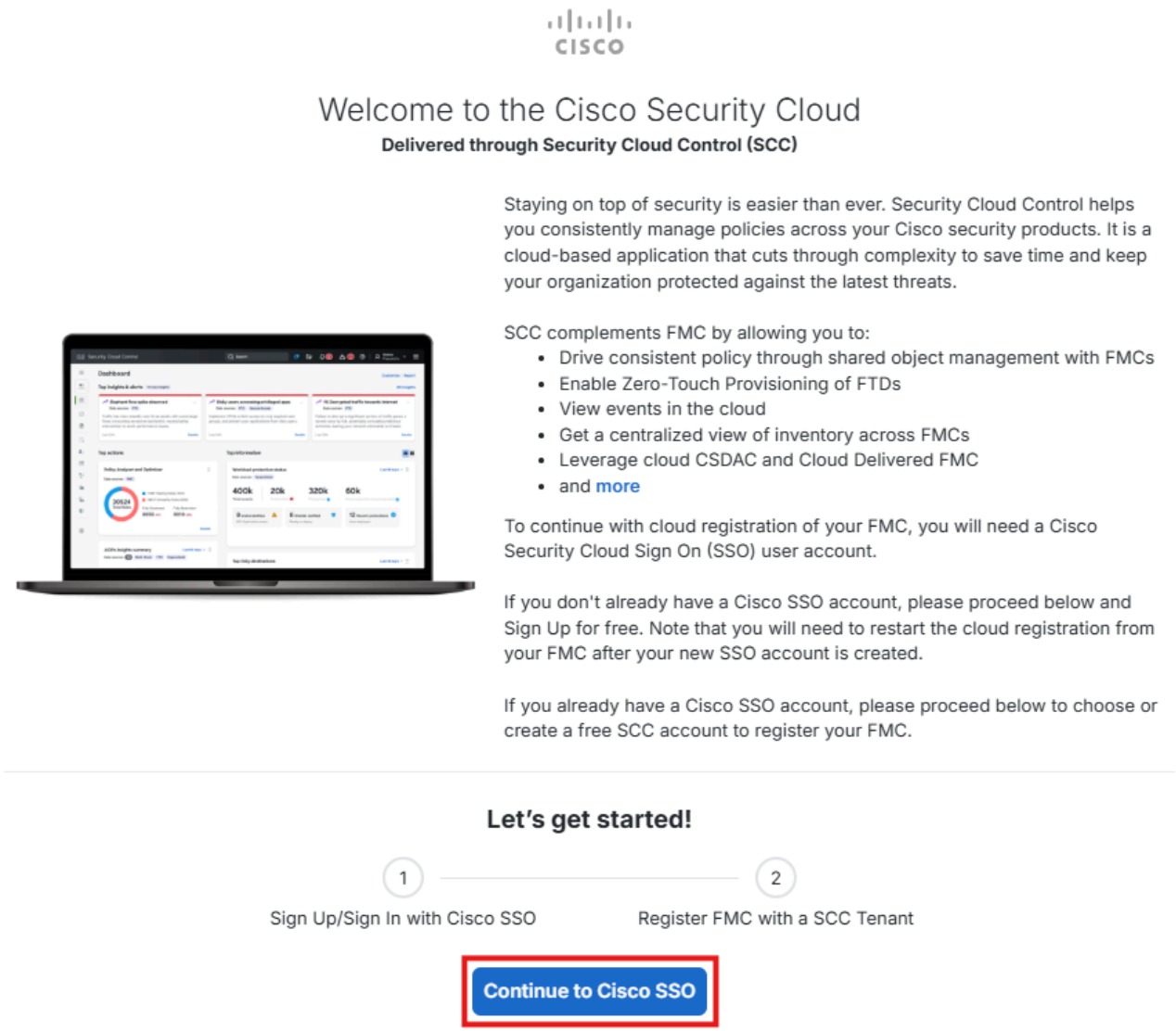
الخطوة 1. في مركز إدارة جدار الحماية الآمن، انتقل إلى الدمج>SecureX



الخطوة 2. أختر المنطقة المناسبة، وانقر فوق تمكين SecureX.

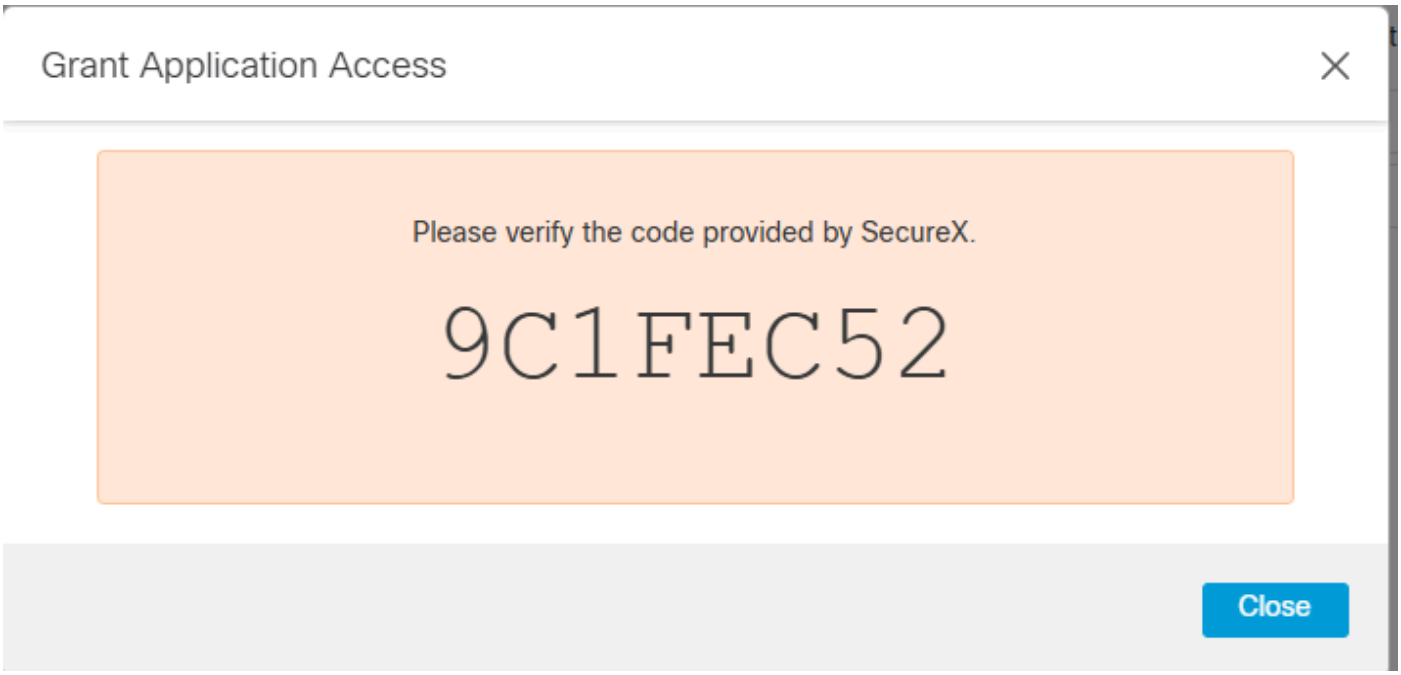


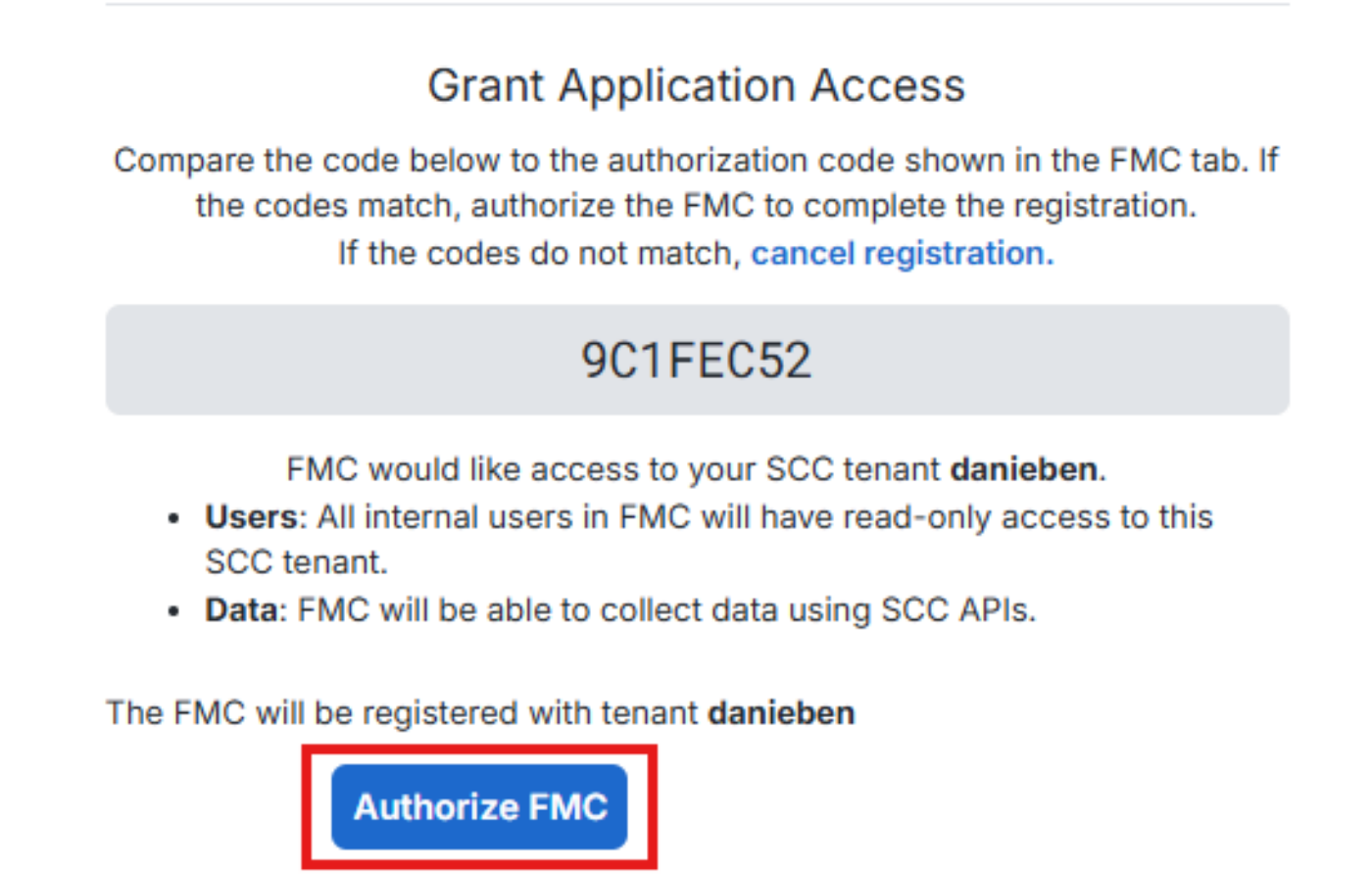
الخطوة 3. بعد النقر فوق تمكين SecureX، فإنه يعيد توجيهك إلى صفحة مصادقة Cisco Defense Orchestrator (التي تستفيد من تسجيل دخول سحابة الأمان)، انقر فوق متابعة إلى Cisco SSO.



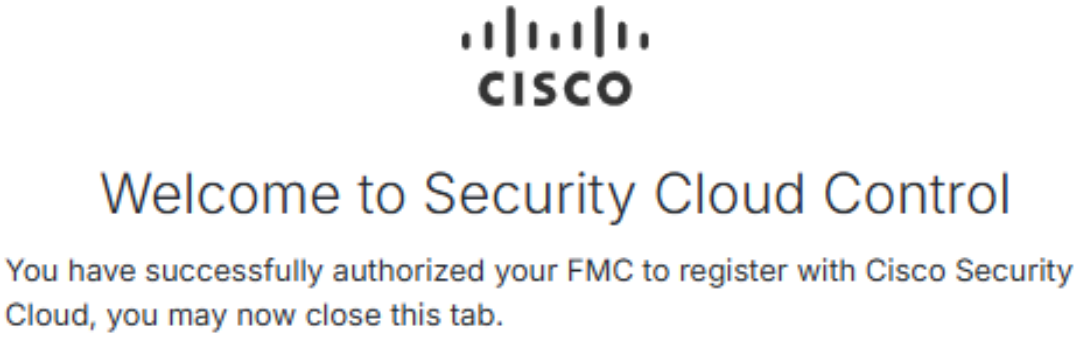
الخطوة 4. يمكنك إما تحديد مستأجر عنصر تحكم في سحابة أمان موجود مسبقا أو إنشاء مستأجر جديد.

الخطوة 5. حدد المستأجر المناسب وتأكد من أن الرمز الذي تتلقاه في هذه الصفحة يطابق الرمز الذي تتلقاه في FMC، إذا كان مطابق، انقر فوق تخويل FMC.



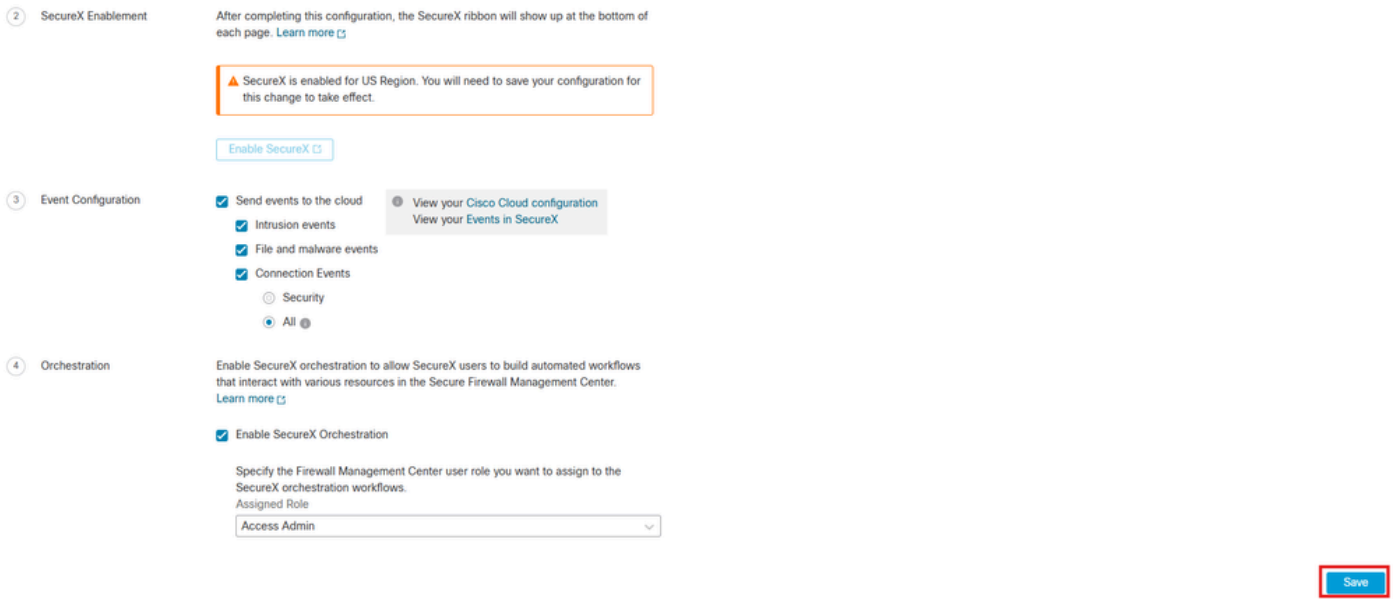


الخطوة 6. أدخل بيانات اعتماد تسجيل الدخول إلى سحابة الأمان وتخويل الدمج، بمجرد اكتماله، يتم تقديم تأكيد على أن FMC قد تم تخويلها للتسجيل مع سحابة أمان Cisco.



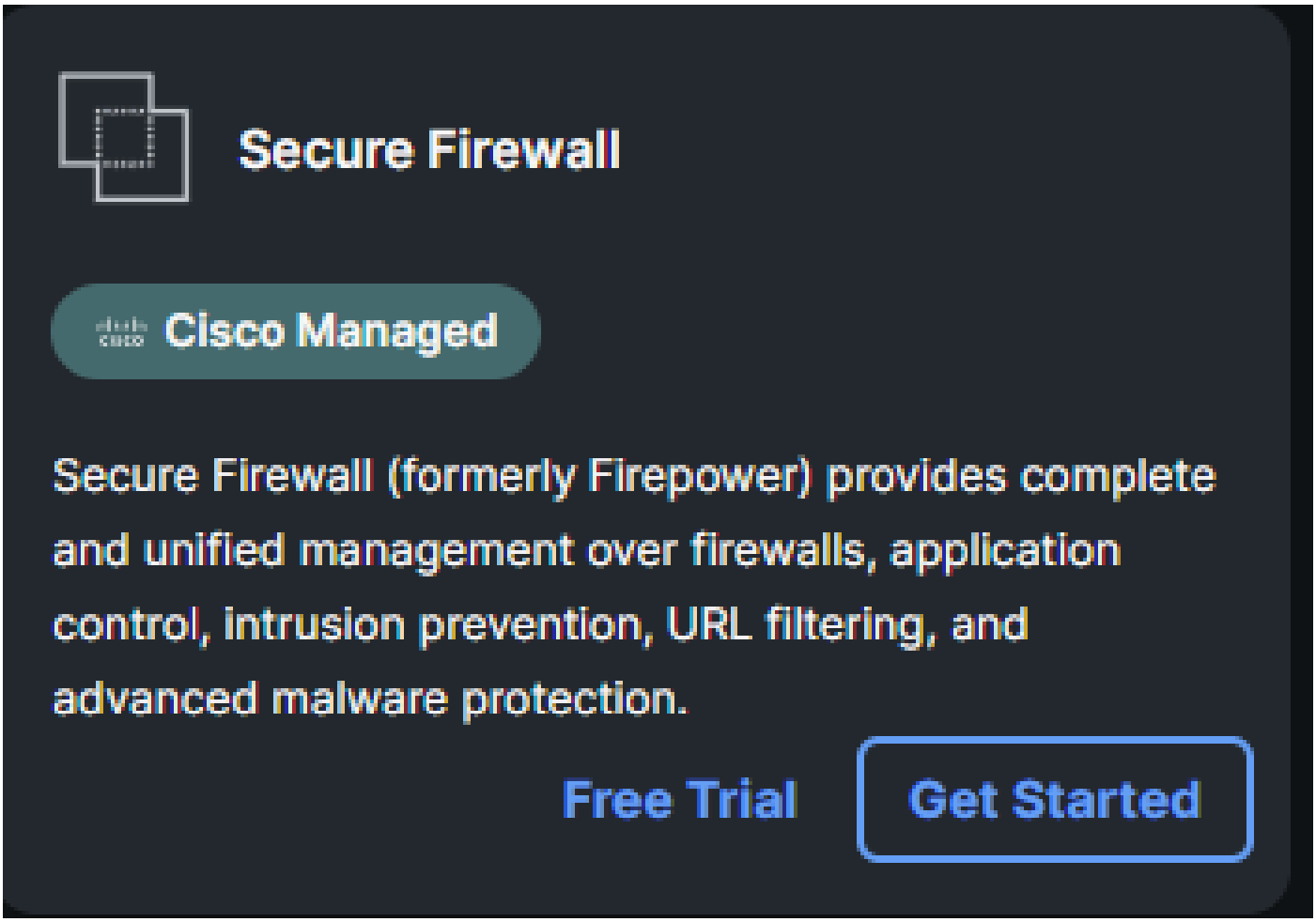
الخطوة 7. بعد اكتمال التفويض، يمكنك إعادة الاتصال ب FMC، وتحديد الأحداث التي تريد إرسالها إلى مجموعة النظراء وبمجرد الانتهاء من ذلك، انقر فوق حفظ.

الخطوة 8. يمكنك تحديد تمكين تزامن SecureX (أتمتة XDR)

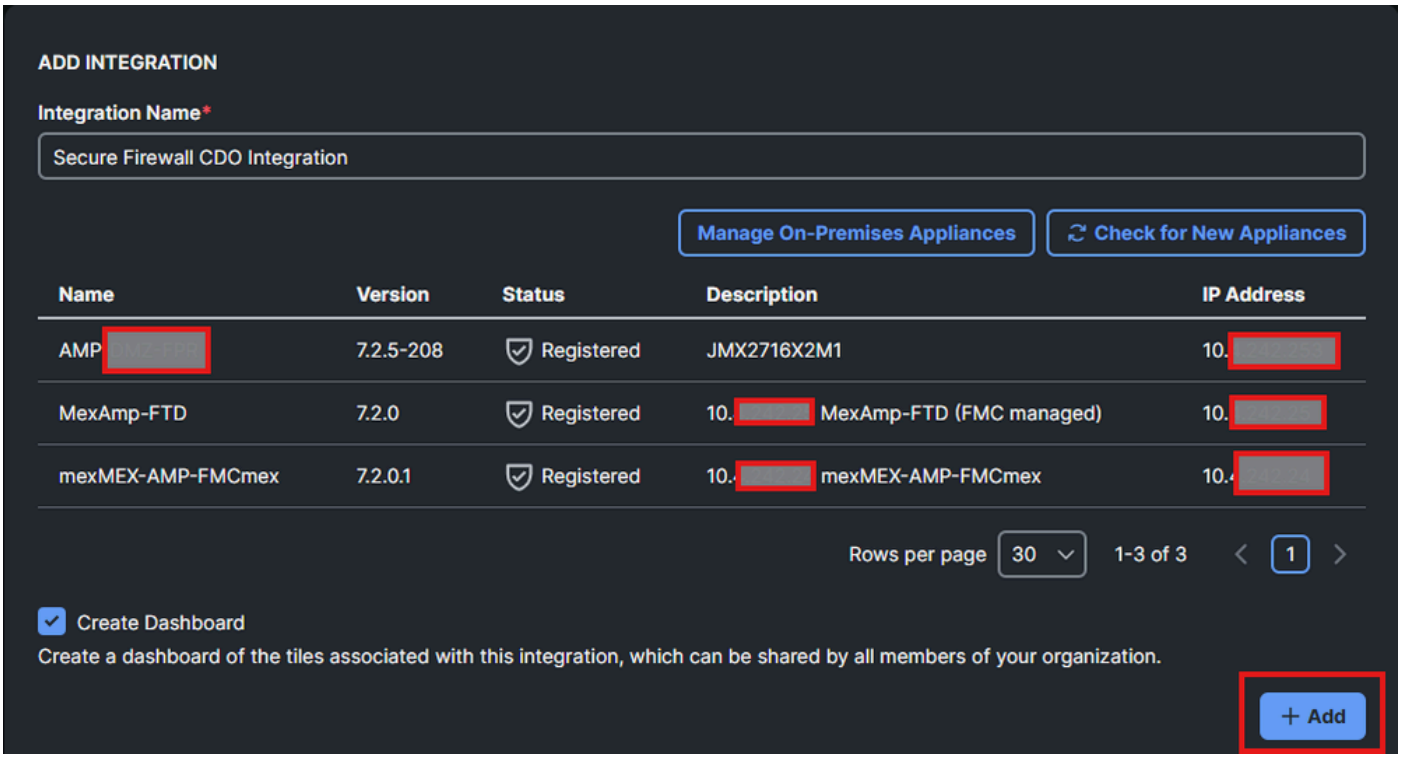


الخطوة 9. انتقل إلى XDR>Administration (إدارة XDR)>الجهاز On Premises وابحث عن أجهزتك، يجب أن يتم تسجيلها تلقائيا.

الخطوة 10. انتقل إلى إدارة XDR>عمليات التكامل وتمكين تكامل جدار الحماية الآمن.



الخطوة 10.1. قم بتعيين اسم للتكامل الخاص بك، انقر فوق +إضافة.



يتيح لك هذا الدمج إثراء التحقيقات داخل XDR.

الطريقة 2 (التكامل الكامل): إثراء الأحداث في XDR

الخطوة 1. يجب أن يحتوي حساب CDO لديك على ترخيص تحليلات الأمان والتسجيل لإعادة توجيه الأحداث إلى Cisco XDR.

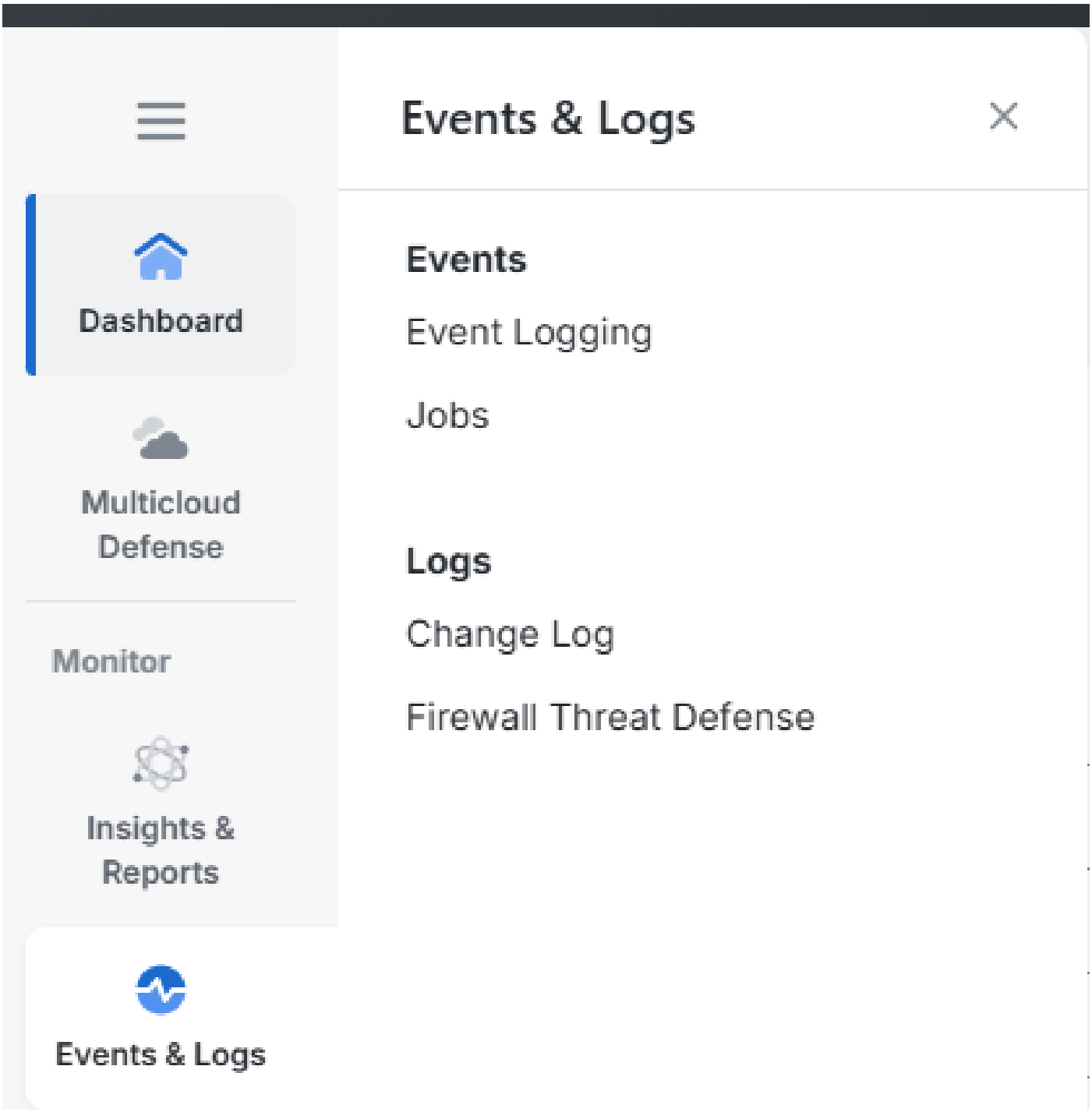
الخطوة 2. يجري إستخدام الخطوات الموضحة سابقا لتسجيل أجهزتك في SSX والتحكم في سحابة الأمان.

الخطوة 3. بمجرد الانتهاء، يجري الوصول إلى TAC باستخدام هذه التفاصيل وطلب ربط التحكم في سحابة الأمان/SAL بتحليلات XDR.

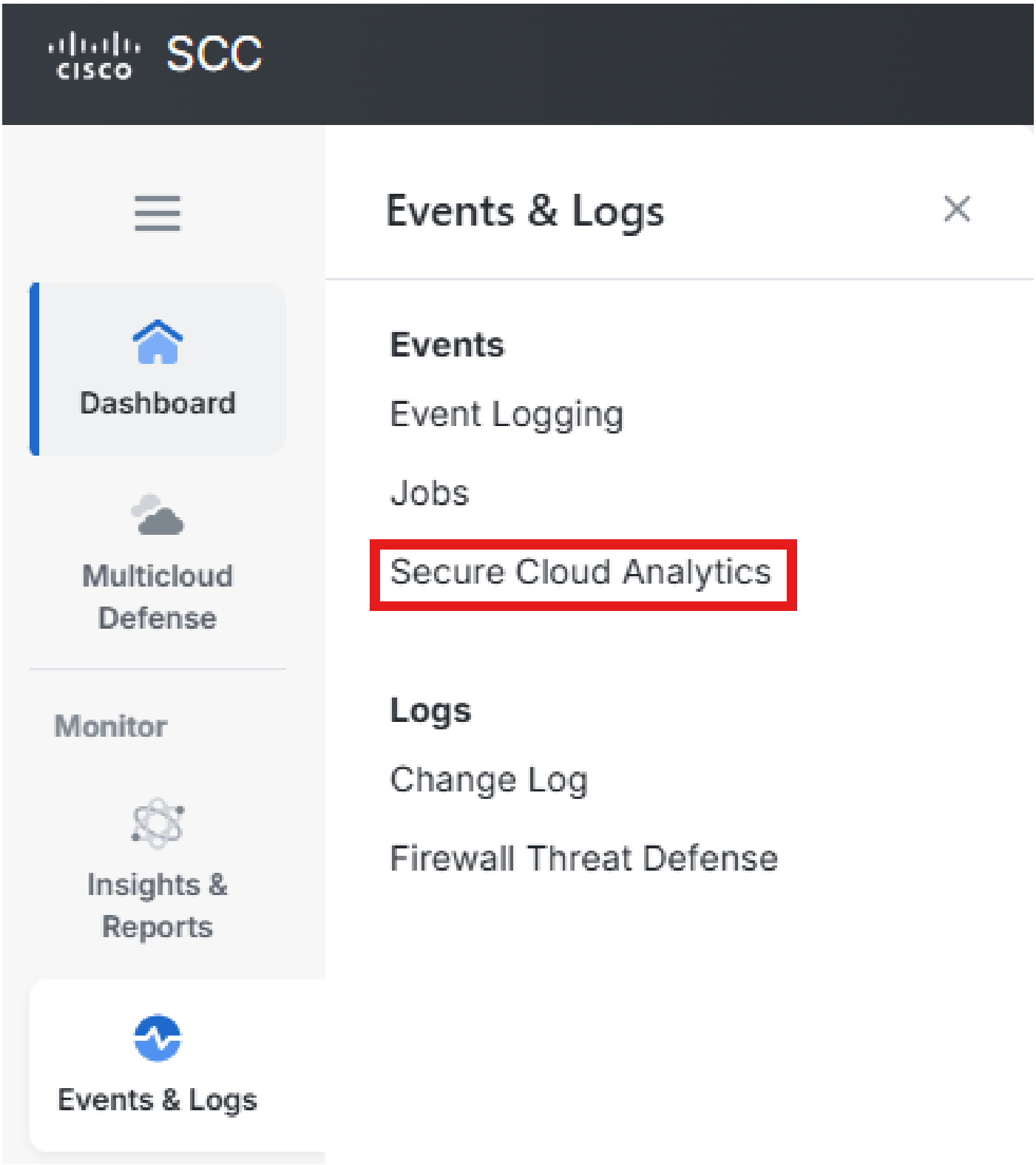
- معرف مستأجر CDO
- اسم CDO
- XDR Org ID
- معرف مستأجر SSE
- اسم SSE
- معرف مؤسسة SCA

الخطوة 4. تأكد من إرتباط حساب CDO الخاص بك ببوابة تحليلات XDR.

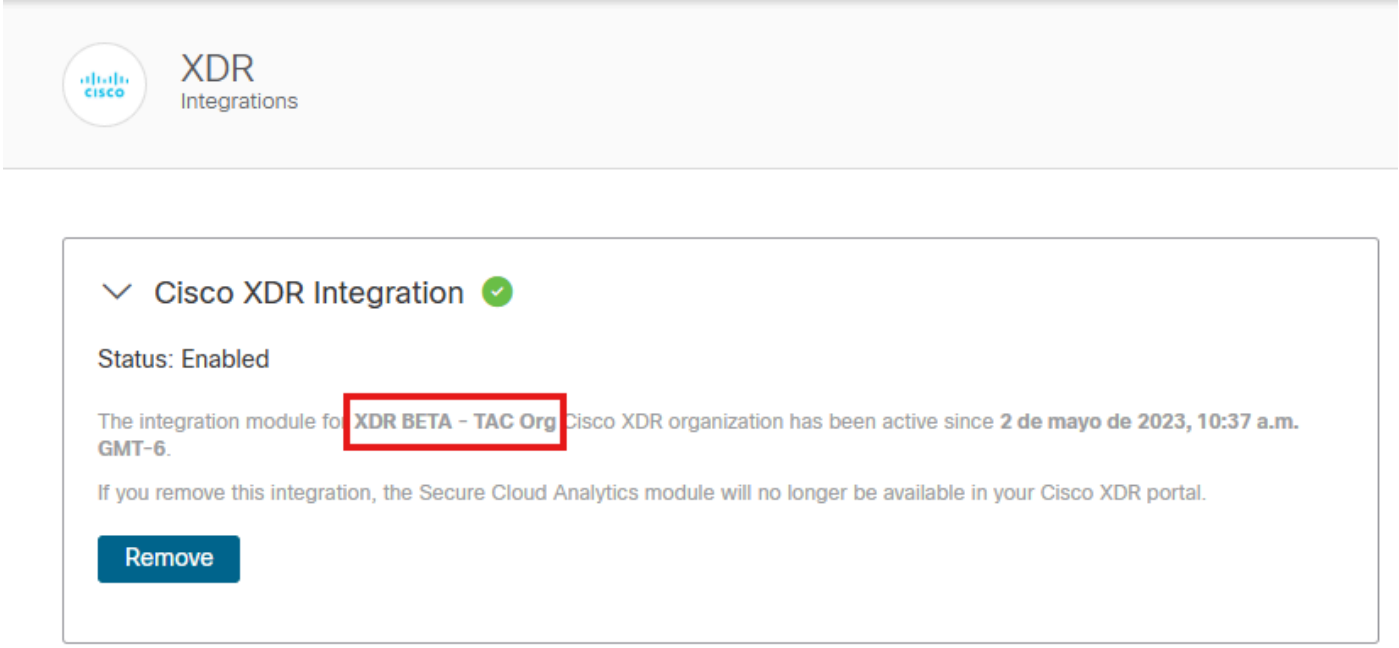
قبل ربط بوابة CDO بتحليلات XDR، يجب أن يكون ما يلي:



بعد اكتمال الارتباط، يمكنك رؤية الخيار للانتقال إلى مدخل تحليلات XDR.



الخطوة 5. ما إن يتم ربط حساب تحليلات XDR الخاص بك بـ Security Cloud Control Portal (CDO)، تحتاج إلى التأكد من أن تحليلات XDR مدمجة مع XDR، لهذا، في تحليلات XDR، انتقل إلى Settings>Integration>XDR، ابحث عن تكامل XDR وتأكد من وجود تحقق أخضر ومن أن وحدة التكامل تشير إلى مؤسسة XDR الصحيحة.



التحقق من الصحة

تحقق من أن جدران الحماية الآمنة تقوم بإنشاء أحداث (برامج ضارة أو أختراق)، ولأحداث التسلل انتقل إلى التحليل>الملفات>أحداث البرامج الضارة، لأحداث التطفل، انتقل إلى Analysis>أحداث التطفل.

تحقق من صحة الأحداث المسجلة على بوابة SSE كما هو مذكور في الخطوة 4 تسجيل الأجهزة على قسم SSE.

تحقق من صحة عرض هذه المعلومات على لوحة معلومات Cisco XDR أو تحقق من سجلات واجهة برمجة التطبيقات (API) حتى يمكنك الاطلاع على سبب فشل واجهة برمجة التطبيقات (API) المحتمل.

تحقق من أن جميع المستأجرين مرتبطون معا بشكل صحيح، إذا كانت لديك مشاكل، افتح حالة مركز المساعدة الفنية وقم بتوفير التفاصيل التالية:

- معرف مستأجر CDO
- اسم CDO
- XDR Org ID
- معرف مستأجر SSE
- اسم SSE
- معرف مؤسسة SCA

استكشاف الأخطاء وإصلاحها

اكتشاف مشاكل الاتصال

يمكنك الكشف عن مشاكل الاتصال العامة من ملف action_queue.log. في حالات الفشل،

يمكنك رؤية هذه السجلات الموجودة في الملف:

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

في هذه الحالة، يعني رمز الخروج 28 انتهاء مهلة العملية ويجب التحقق من الاتصال بالإنترنت. يجب أن ترى أيضا رمز الخروج 6 الذي يعني مشاكل في دقة DNS

مشكلات الاتصال بسبب دقة DNS

الخطوة 1. تأكد من أن الاتصال يعمل بشكل صحيح.

```
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'
```

يوضح هذا الإخراج أن الجهاز غير قادر على حل عنوان URL https://api-sse.cisco.com، وفي هذه الحالة، نحتاج إلى التحقق من تكوين خادم DNS المناسب، ويمكن التحقق من صحته باستخدام NSLOOKUP من واجهة سطر الأوامر (CLI) الخبير:

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

يوضح هذا الإخراج أنه لم يتم الوصول إلى DNS الذي تم تكوينه، لتأكيد إعدادات DNS، أستخدم الأمر show network:

```
> 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
```

في هذا المثال، تم إستخدام خادم DNS الخطأ، يمكنك تغيير إعدادات DNS باستخدام هذا الأمر:

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

بعد إختبار هذا الاتصال مرة أخرى وهذه المرة، يكون الاتصال ناجحا.

```
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;
```

مشاكل التسجيل إلى بوابة SSE

يحتاج كل من FMC وجدار الحماية الآمن إلى اتصال بعنوان SSE URL على واجهة الإدارة الخاصة بهم، لاختبار الاتصال، أدخل هذه الأوامر على Firepower CLI مع الوصول الجذر:

<#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

يمكن تجاوز التحقق من الشهادة بهذا الأمر:

```
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;
```

ملاحظة: تحصل على الرسالة 403 الممنوعة لأن المعلومات المرسلة من الاختبار ليست ما يتوقعه SSE ولكن هذا يثبت بما فيه الكفاية للتحقق من الاتصال.

التحقق من حالة SsecConnector

يمكنك التحقق من خصائص الموصل كما هو موضح.

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

للتحقق من الاتصال بين SSContor و EventHandler الذي يمكنك إستخدام هذا الأمر، هذا مثال على اتصال سيئ:

```
root@firepower:/etc/sf# netstat -anlp | grep EventHandler_SSEConnector.sock
```

```
unix 2 [ ACC ] STREAM LISTENING 3022791165 11204/EventHandler /ngfw/var/sf/run/EventHandler_SSEConnecto
```

في مثال على اتصال ثابت، يمكنك أن ترى أن حالة الدفق متصلة:

```
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
```

التحقق من البيانات المرسلة إلى بوابة SSE و CTR

للإرسال الأحداث من جهاز جدار الحماية الآمن للاطلاع على حاجة إنشاء اتصال TCP مع https://eventing-ingest.sse.itd.cisco.com هذا مثال على اتصال لم يتم إنشاؤه بين مدخل SSE وجدار الحماية الآمن:

```
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
```

في الموصل.السجلات:

```
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
```

> ملاحظة: لاحظ أن عناوين IP المعروضة x.x.x.246 و 1x.x.246 تنتمي إلى https://eventing-ingest.sse.itd.cisco.com وبجب أن تتغير، ولهذا السبب فإن التوصية هي السماح لحركة مرور البيانات بوابة SSE استنادا إلى URL بدلا من عناوين IP.

إذا لم يتم إنشاء هذا الاتصال، فلن يتم إرسال الأحداث إلى بوابة SSE. هذا مثال على اتصال ثابت بين جدار الحماية الآمن ومدخل SSE:

```
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.
```

لا يمكن تسجيل الجهاز (FTD) في عنصر التحكم في سحابة الأمان

إذا تعذر تسجيل جهازك في "التحكم في سحابة الأمان"، فتأكد من توفر اتصال به لمستأجر CDO المناسب.

للتحقق من عنوان URL الصحيح، انتقل إلى Administration>مركز إدارة جدار الحماية، حدد Cloud Delivered FMC، في الجانب الأيسر العلوي من شاشتك، يمكنك رؤية اسم المضيف.

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

إذا كنت لا تزال تواجه مشاكل للاتصال بـ CDO، فتأكد من فتح المنفذ 8305، هذا مثال على مشكلة اتصال.

```
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
```

تم تسجيل الجهاز إلى مستأجر SSX خاطئ

يمكنك التحقق من أي مستأجر SSX مسجل في FMC الخاص بك.

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

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

إذا كان مستأجر SSX غير صحيح، تحتاج إلى إعادة تنفيذ الخطوات لتسجيل الأجهزة في SSX

إذا كان مستأجر SSX صحيحا، ولكن مستأجر CDO غير مرتبط بمؤسسة SSX المناسبة، الرجاء الاتصال بـ TAC مع هذه التفاصيل:

- معرف مستأجر SSX
- معرف مستأجر CDO

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).