دمج Cisco XDR واستكشاف أخطائه وإصلاحها باستخدام برنامج الدفاع عن تهديد الطاقة النارية (FTD)

المحتويات

المقدمة

يصف هذا المستند الخطوات المطلوبة لدمج Cisco XDR والتحقق من صحته واستكشاف أخطائه وإصلاحها باستخدام برنامج الدفاع عن تهديد الطاقة النارية (FTD).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- مركز إدارة Firepower (FMC)
- Firepower Threat Defense (FTD)
- المحاكاة الافتراضية الاختيارية للصور

المكونات المستخدمة

- الدفاع ضد تهديد الطاقة النارية (FTD) - 6.5
- مركز إدارة Firepower (FMC) - 6.5
- تبادل خدمات الأمان (SSE)
- XDR من Cisco
- بوابة الترخيص Smart

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.

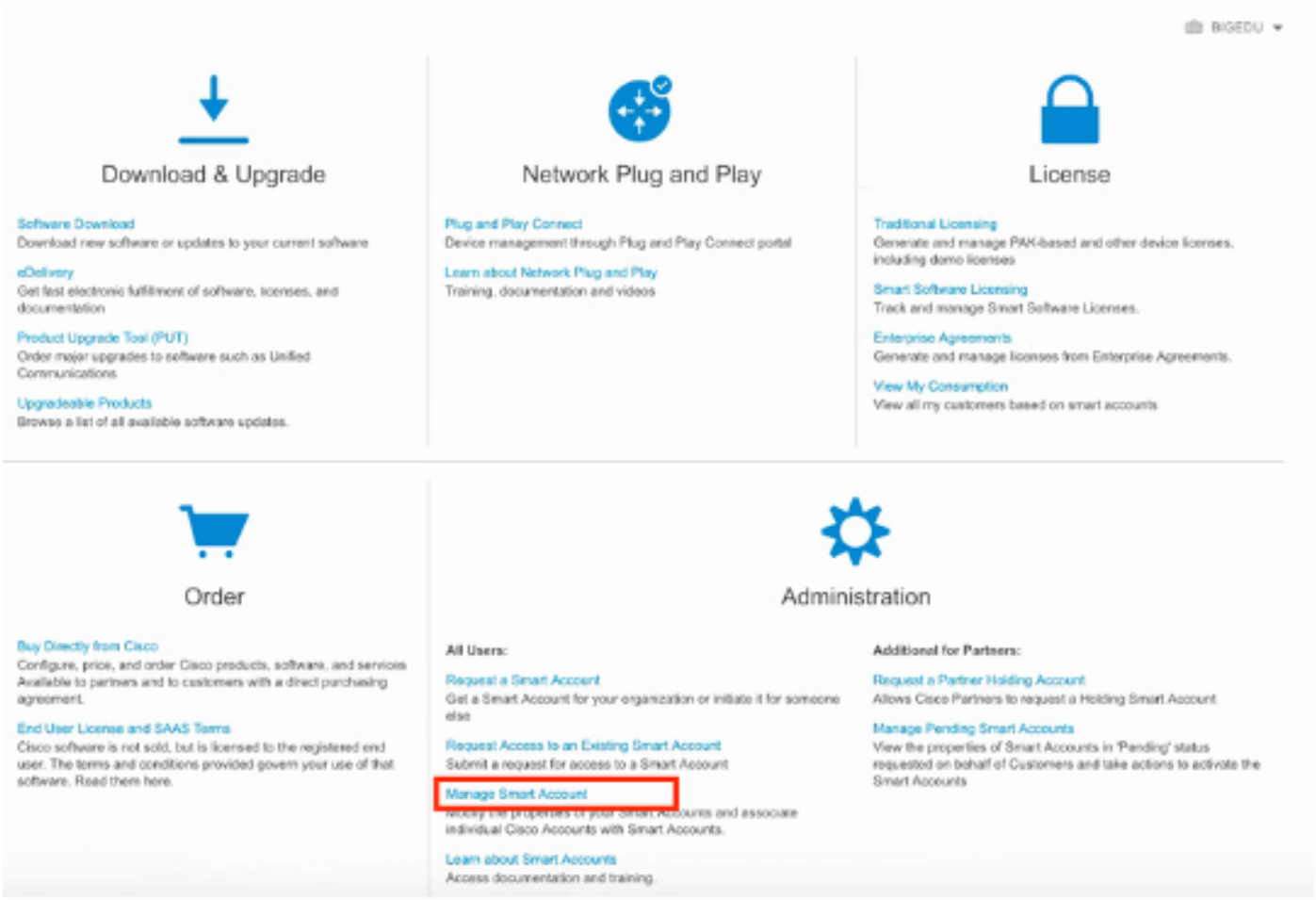
التكوين

الترخيص

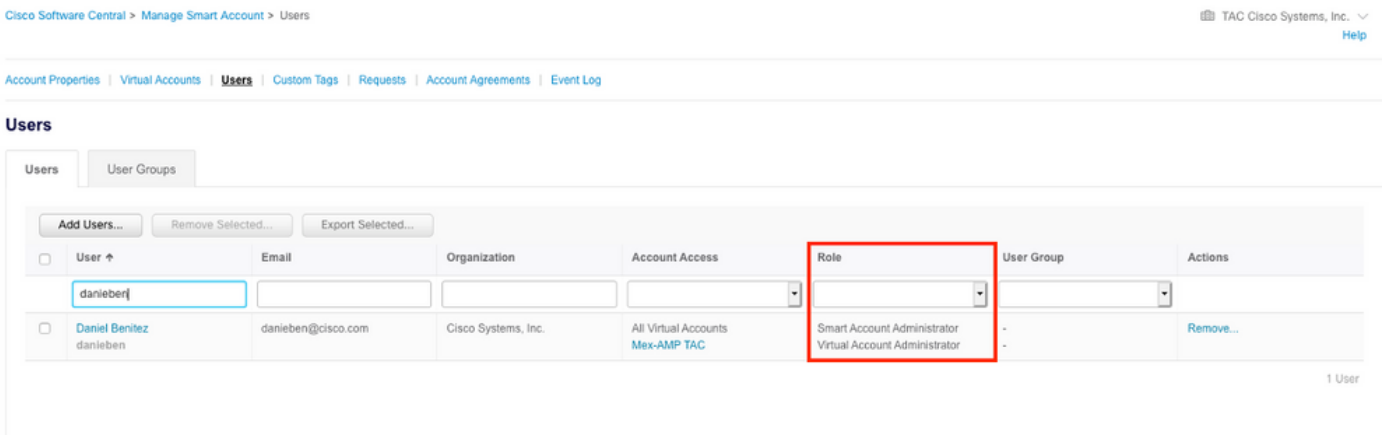
أدوار الحساب الظاهري:

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

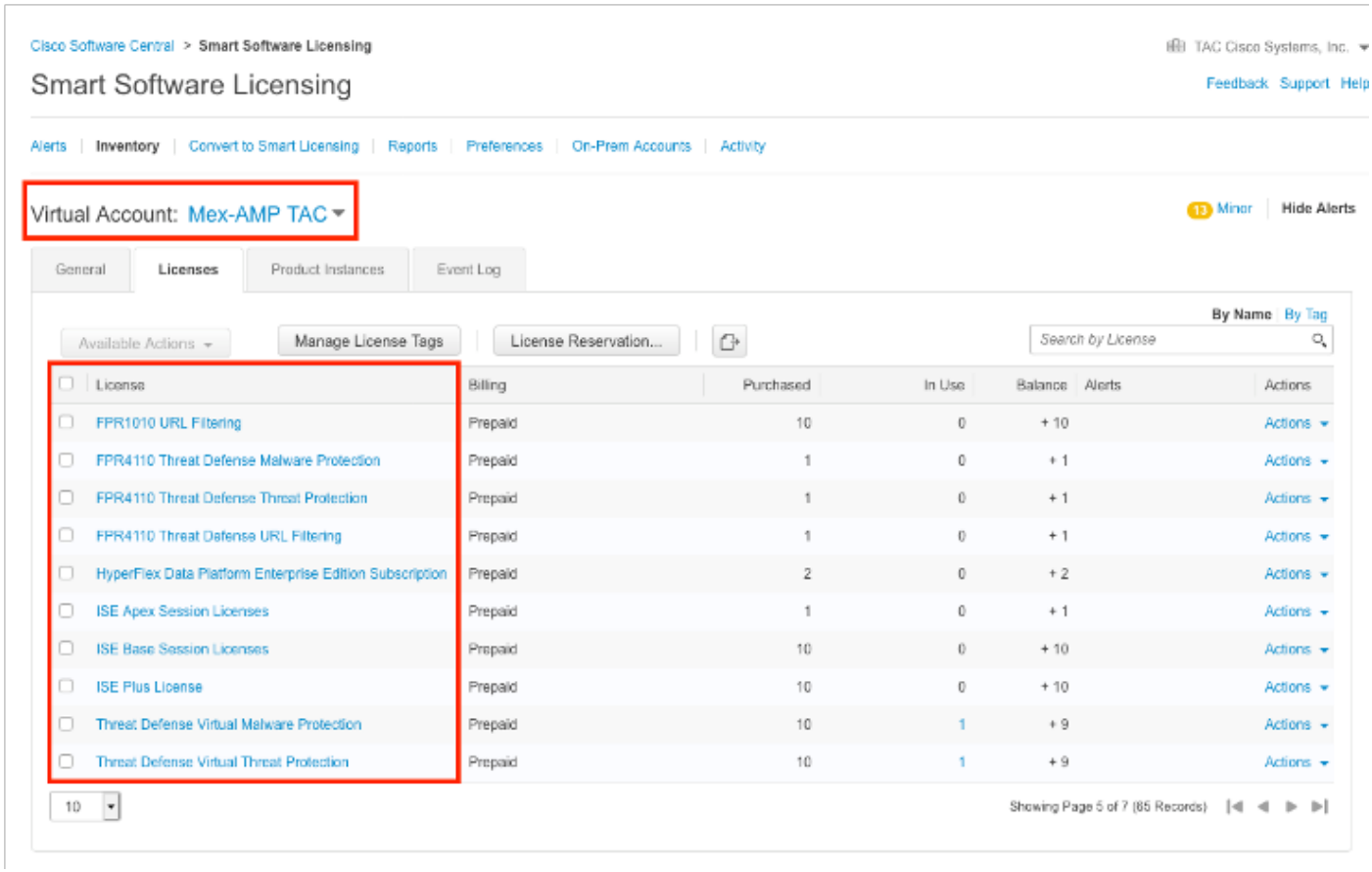
الخطوة 1. للتحقق من صحة دور الحساب الذكي، انتقل إلى software.cisco.com وتحت قائمة الإدارة، حدد إدارة الحساب الذكي.



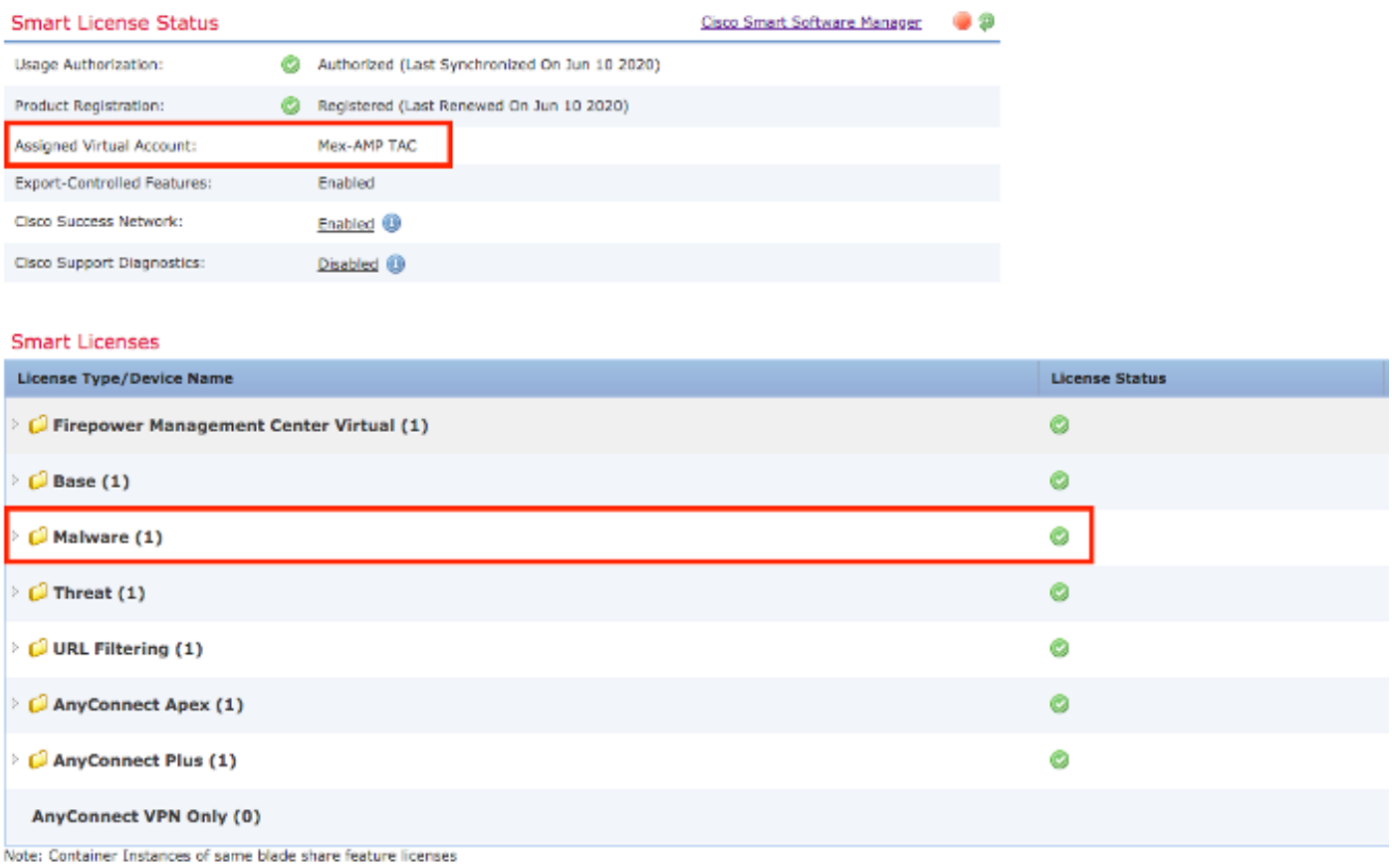
الخطوة 2. للتحقق من صحة دور المستخدم، انتقل إلى المستخدمين، وتحقق من أنه تحت الأدوار يتم تعيين الحسابات على مسؤول حساب ظاهري، كما هو موضح في الصورة.



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

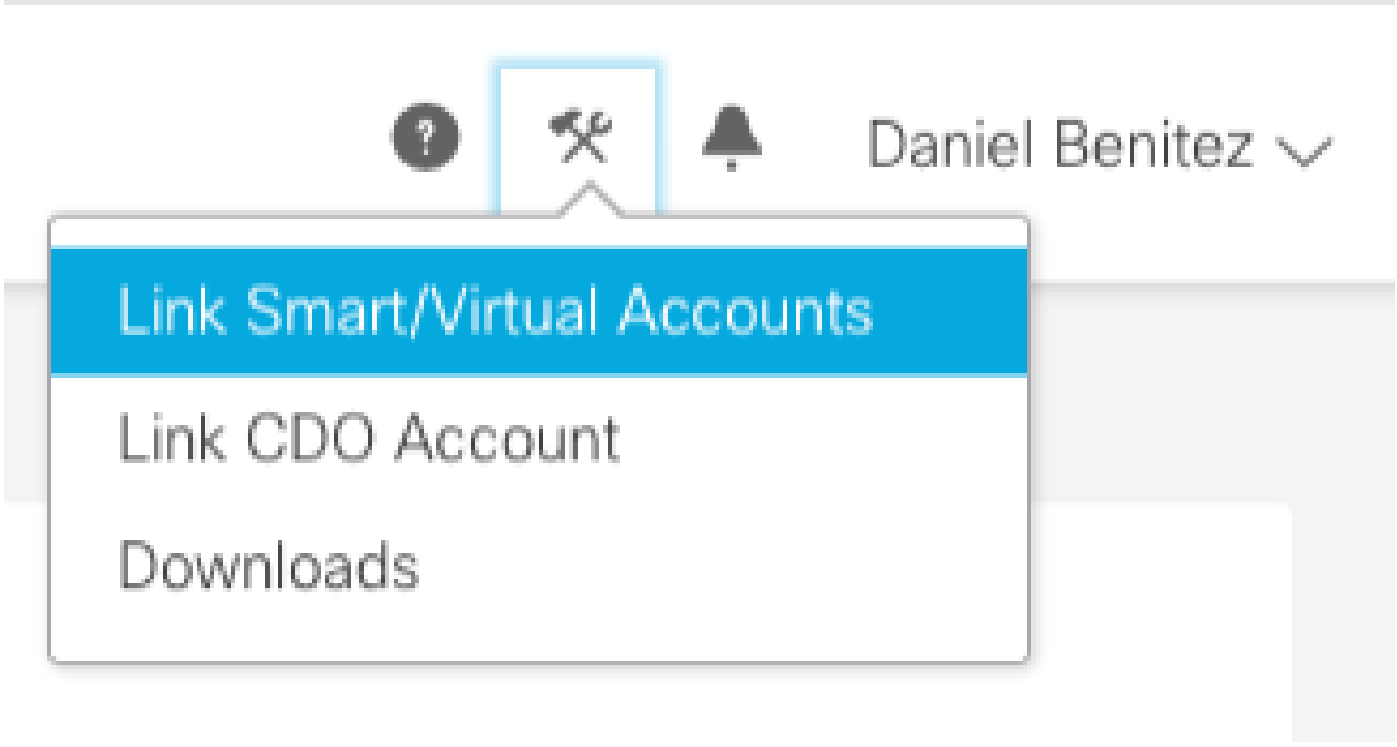


الخطوة 4. للتحقق من تسجيل FMC في الحساب الظاهري الصحيح، انتقل إلى تراخيص النظام>الترخيص الذكي:



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 "أدوات" وتحديد ربط الحسابات.



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

تسجيل الأجهزة في SSE

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

المنطقة الأمريكية

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

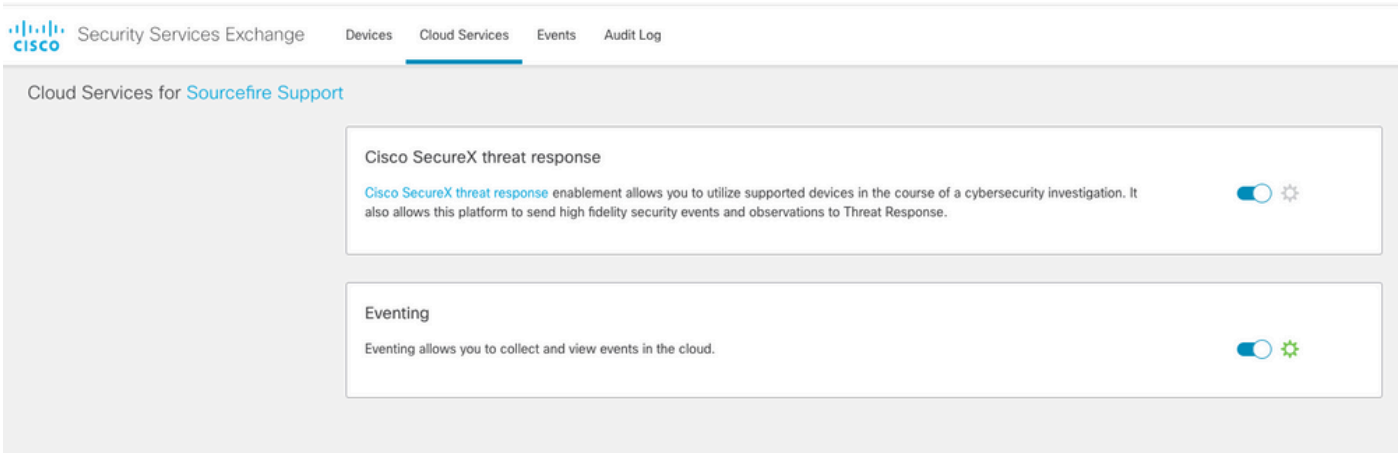
منطقة الاتحاد الأوروبي

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

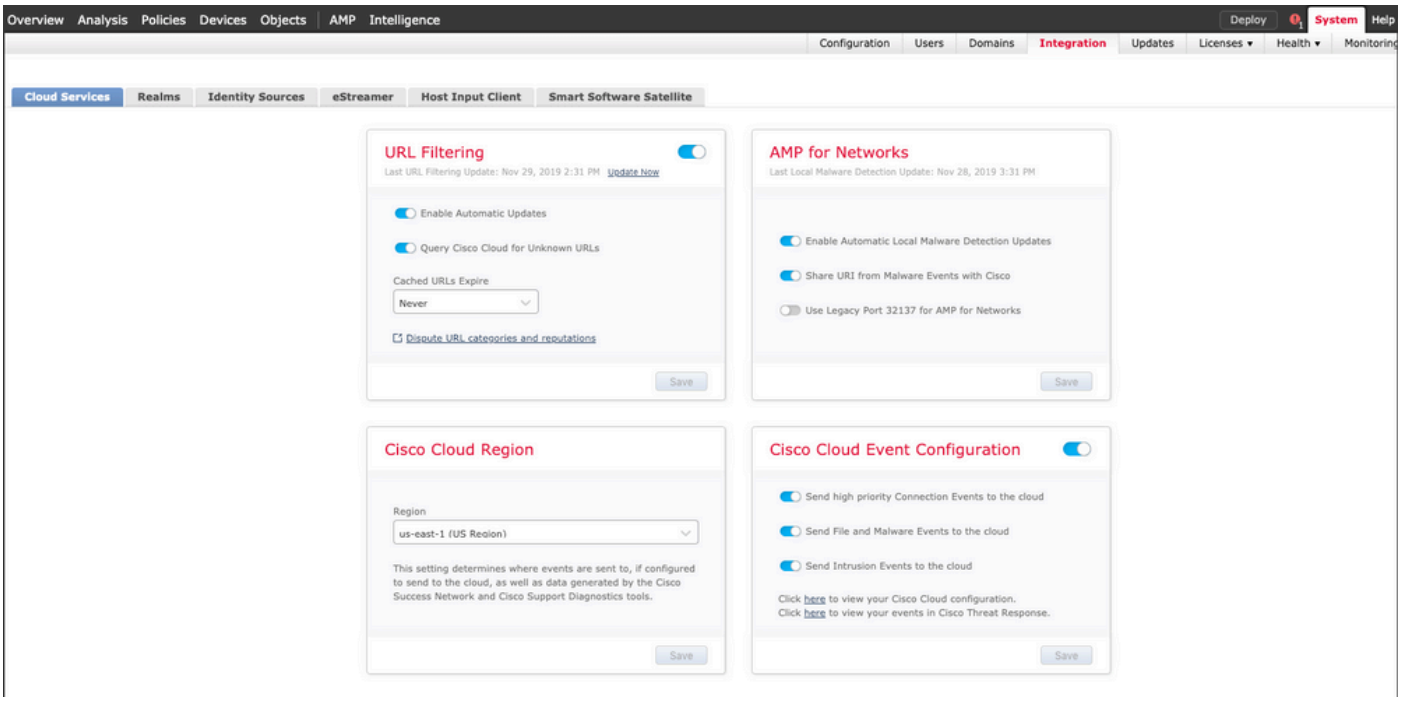
منطقة آسيا والمحاذ واليابان

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

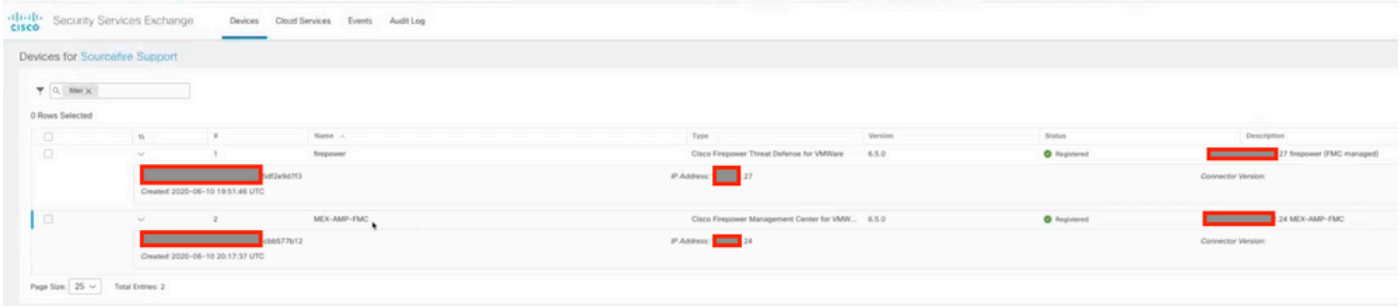
الخطوة 2. قم بتسجيل الدخول إلى بوابة SSE باستخدام عنوان URL هذا https://admin.sse.itd.cisco.com، وتصفح إلى خدمات السحابة، وتمكين كل الخيارين تصحيح وإستجابة تهديدات Cisco XDR، كما هو موضح في الصورة التالية:



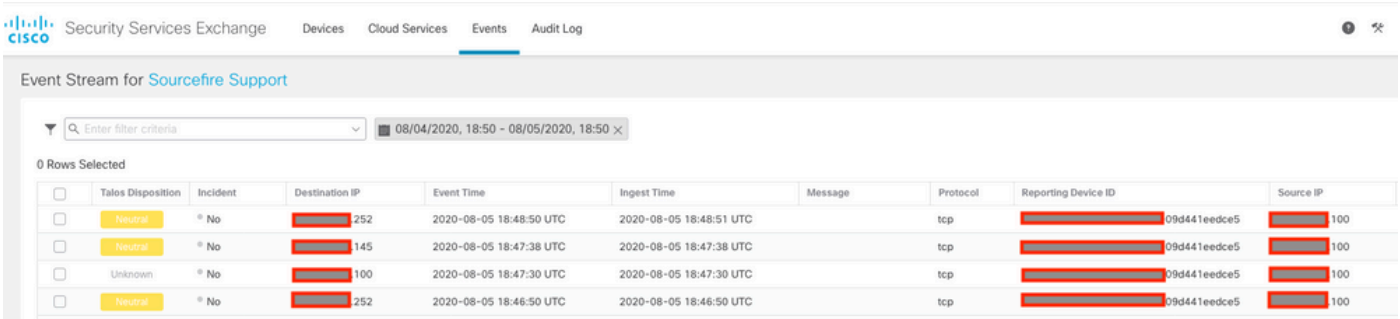
الخطوة 3. سجل الدخول إلى مركز إدارة Firepower وانتقل إلى System>Integration>خدمات السحابة، وقم بتمكين تكوين حدث Cisco Cloud وحدد الأحداث التي تريد إرسالها إلى السحابة:



الخطوة 4. يمكنك الرجوع إلى بوابة SSE والتحقق من أنه يمكنك الآن رؤية الأجهزة المسجلة في SSE:



يتم إرسال الأحداث بواسطة أجهزة FTD، انتقل إلى الأحداث الموجودة على بوابة SSE للتحقق من الأحداث التي تم إرسالها بواسطة الأجهزة إلى SSE، كما هو موضح في الصورة:



التحقق من الصحة

تحقق من أن أنظمة FTD تقوم بإنشاء أحداث (برامج ضارة أو أختراق)، وتنتقل أحداث التسلل إلى التحليلالملفاتأحداث البرامج الضارة، وأحداث التسلل، انتقل إلى التحليلأحداث الاختراق.

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

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. تحقق 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 المنسب، 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
```

ف ي اذه الم ث ال، ت م إس ت خ دام خ اد م DNS الخ أط، ي م ك ن ت غ ي ي ر إ ع داد ات DNS ب اس ت خ دام اذه الأ م ر:

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

ب ع د إ خ ت اب ر اذه الا ت ص ال م ر ة أ خ ر ى و ه ذه الم ر ة، ي ك ون الا ت ص ال ن اج ح ا.

```
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 و FTD إلى اتصال بعناوين SSE URLs 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: يمكنك الحصول على الرسالة 403 الممحوظة لأن المعلومات التي تم إرسالها من الاختبار ليست ما يتوقعه SSE ولكن هذا يثبت بما يكفي 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 هذه الأمر، هذه 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 أحداث من جهاز FTD للاطلاع على حاجة إنشاء اتصال TCP مع https://eventing-ingest.sse.itd.cisco.com هذه مثال على اتصال لم يتم إنشاؤه بين مدخل SSE و FTD:

```
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 1x.x.x.246 و x.x.x.246 تنتمي إلى https://eventing-ingest.sse.itd.cisco.com وهذا هو السبب في أن التوصية هي السماح بدلا من عناوين IP. يجب تغييرها، استنادا إلى URL لحركة مرور البيانات إلى بوابة SSE.

إذا لم يتم إنشاء هذا الاتصال، فلن يتم إرسال الأحداث إلى بوابة SSE. هذا مثال على اتصال ثابت بين FTD وبوابة 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.
```

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).