Intégration et dépannage de Cisco XDR avec Firepower Threat Defense (FTD)

Table des matières

[Introduction](#)
[Conditions préalables](#)
[Exigences](#)
[Composants utilisés](#)
[Configurer](#)
[Licences](#)
[Liez vos comptes à SSE et enregistrez les périphériques.](#)
[Enregistrement des périphériques auprès de SSE](#)

Introduction

Ce document décrit les étapes requises pour intégrer, vérifier et dépanner Cisco XDR avec Firepower Firepower Firepower Threat Defense (FTD).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)
- Virtualisation facultative des images

Composants utilisés

- Défense contre les menaces Firepower (FTD) - 6,5
- Centre de gestion Firepower (FMC) - 6,5
- Échange de services de sécurité (SSE)
- Cisco XDR
- Portail de licences Smart

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

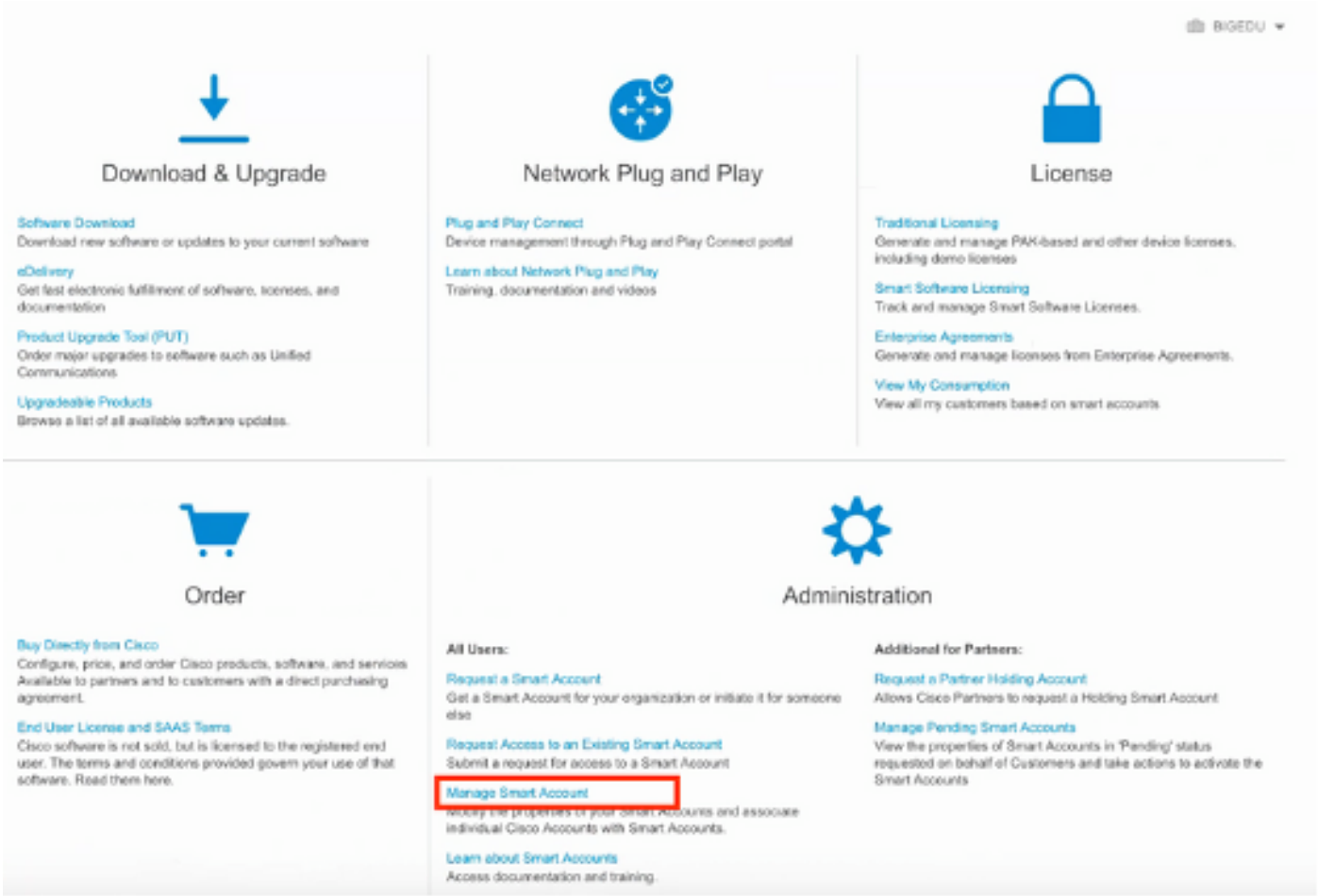
Configurer

Licences

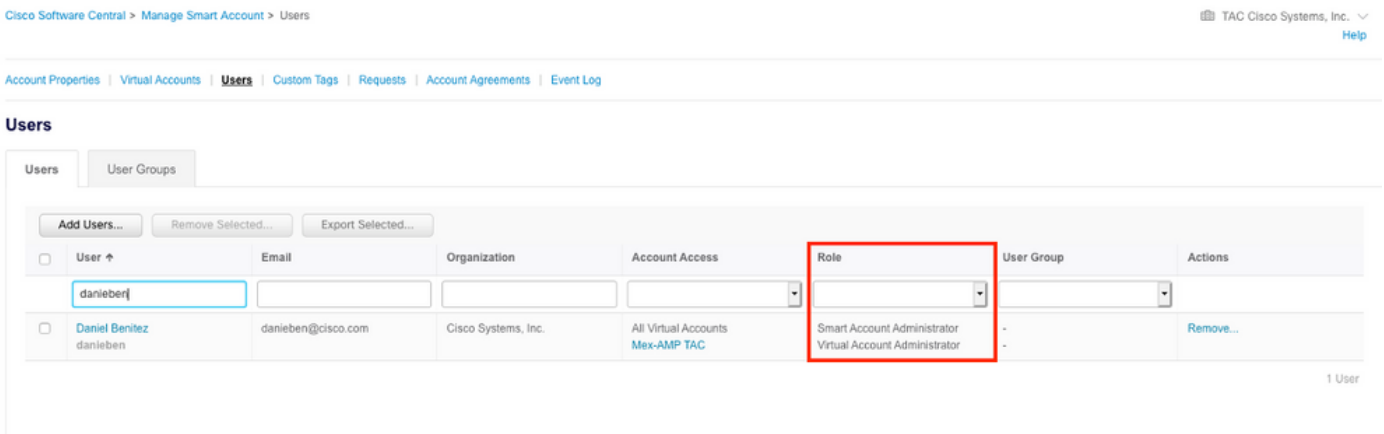
Rôles de compte virtuel :

Seul l'administrateur du compte virtuel ou l'administrateur du compte Smart a le privilège de lier le compte Smart au compte SSE.

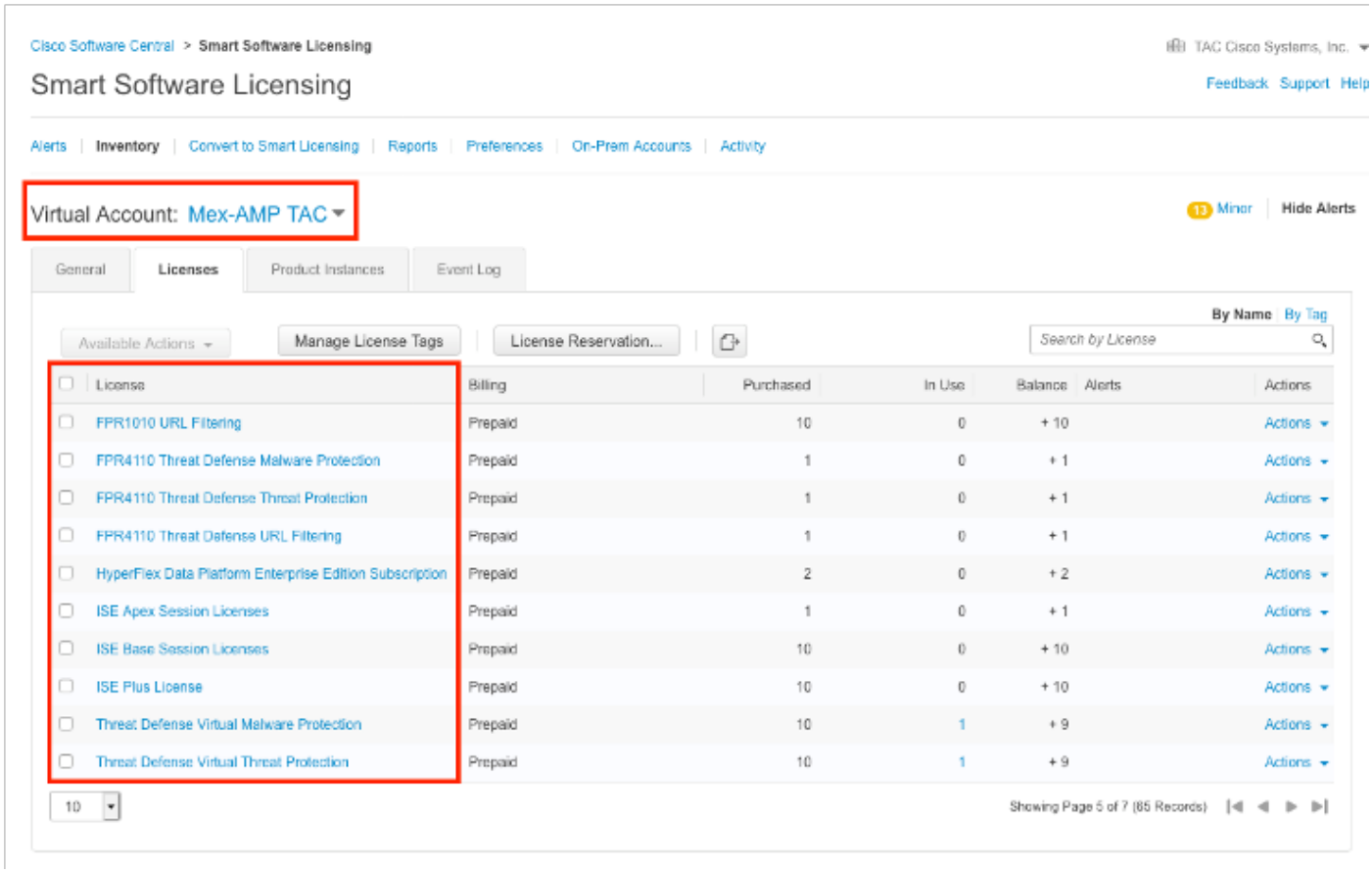
Étape 1. Afin de valider le rôle de compte Smart, accédez à software.cisco.com et sous le menu Administration, sélectionnez Manage Smart Account.



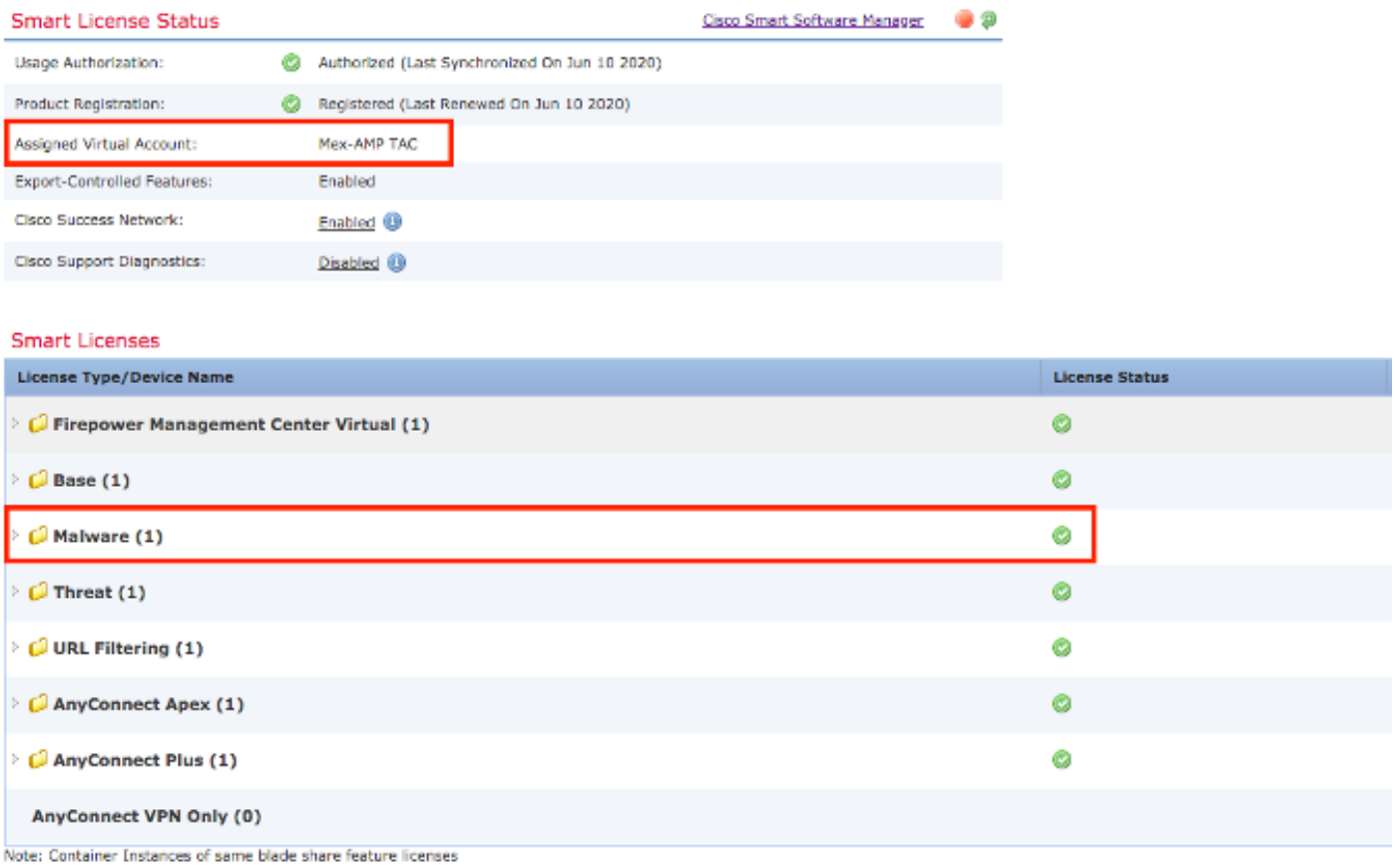
Étape 2. Afin de valider le rôle d'utilisateur, naviguez jusqu'à Users, et vérifiez que sous Roles les comptes sont configurés pour avoir Virtual Account Administrator, comme indiqué dans l'image.



Étape 3. Assurez-vous que le compte virtuel sélectionné pour la liaison sur SSE contient la licence pour les périphériques de sécurité si un compte qui ne contient pas la licence de sécurité est lié sur SSE, les périphériques de sécurité et l'événement n'apparaissent pas sur le portail SSE.

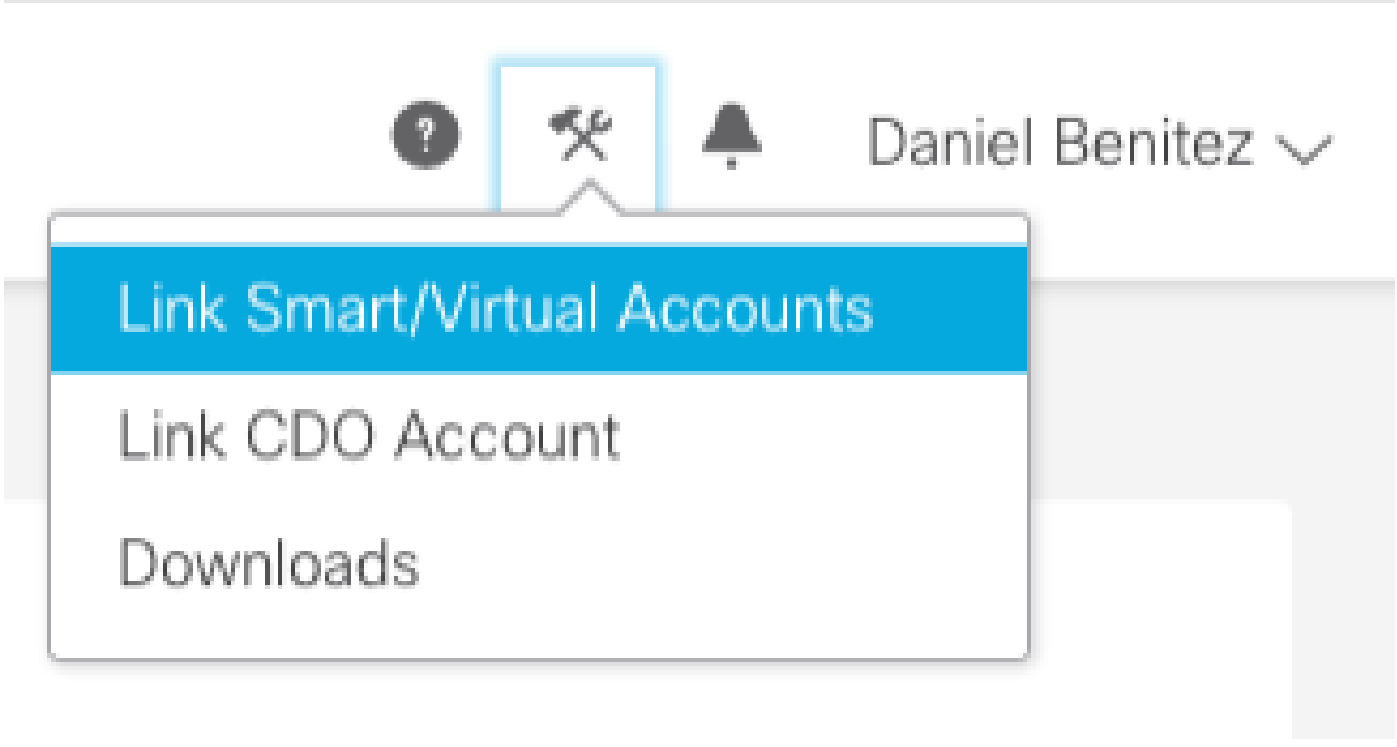


Étape 4. Pour vérifier que le FMC a été enregistré sur le compte virtuel approprié, accédez à System>Licenses>Smart License :



Liez vos comptes à SSE et enregistrez les périphériques.

Étape 1. Lorsque vous vous connectez à votre compte SSE, vous devez lier votre compte Smart à votre compte SSE, pour cela, vous devez cliquer sur l'icône des outils et sélectionner Lier des comptes.



Une fois le compte lié, vous voyez le compte Smart avec tous les comptes virtuels.

Enregistrement des périphériques auprès de SSE

Étape 1. Assurez-vous que les URL suivantes sont autorisées dans votre environnement :

Région des États-Unis

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

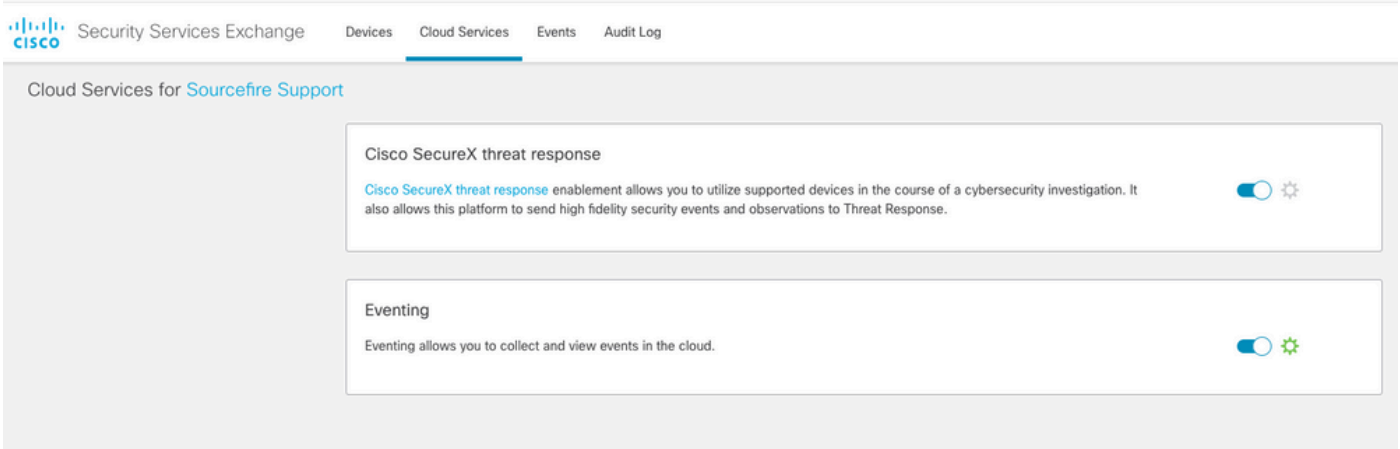
Région de l'UE

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

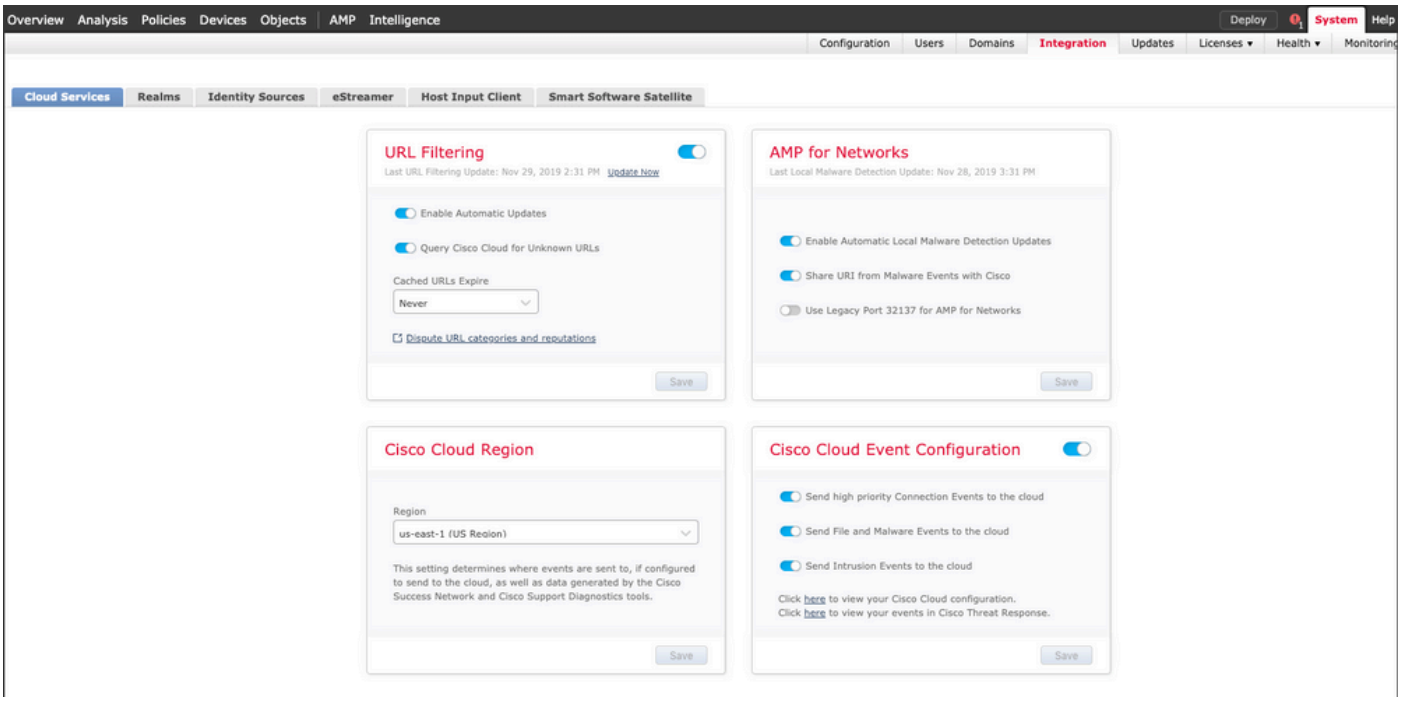
Région APJ

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

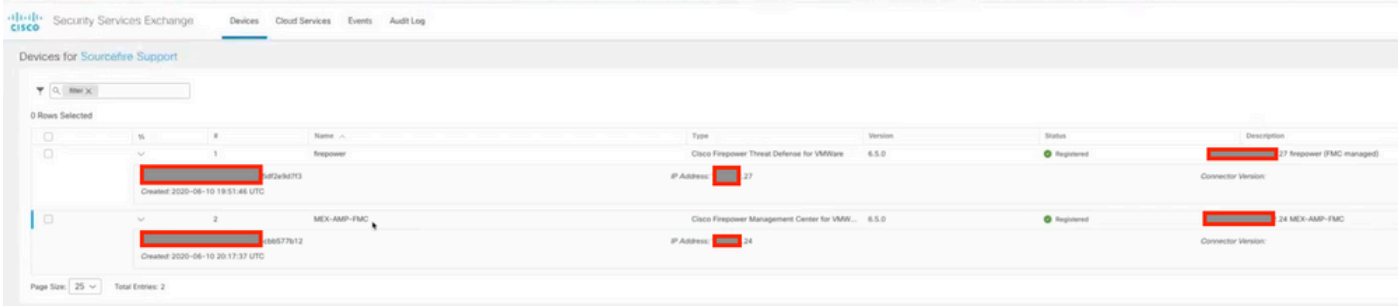
Étape 2. Connectez-vous au portail SSE à l'adresse https://admin.sse.itd.cisco.com, accédez à Services cloud et activez les deux options Événement et Réponse aux menaces Cisco XDR, comme indiqué dans l'image suivante :



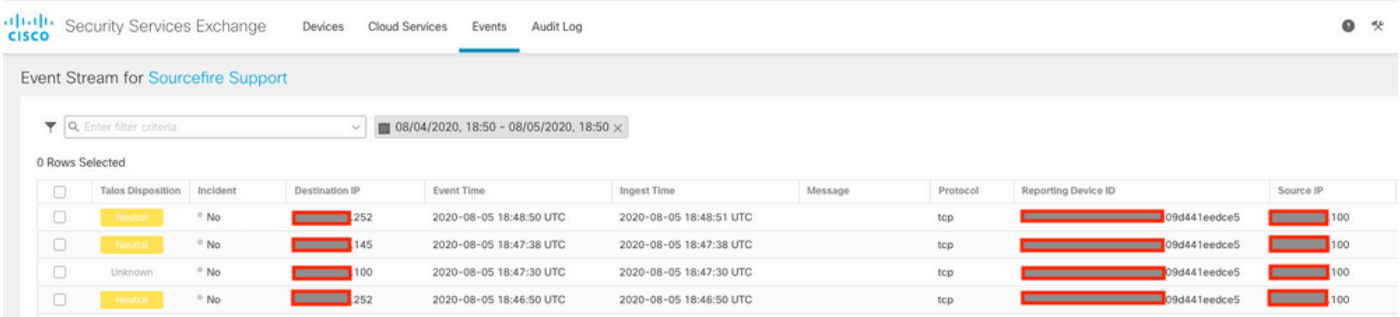
Étape 3. Connectez-vous à Firepower Management Center et accédez à System>Integration>Cloud Services, activez Cisco Cloud Event Configuration et sélectionnez les événements que vous souhaitez envoyer au cloud :



Étape 4. Vous pouvez revenir au portail SSE et confirmer que vous pouvez désormais voir les périphériques inscrits sur SSE :



Les événements sont envoyés par les périphériques FTD, naviguez jusqu'aux événements sur le portail SSE pour vérifier les événements envoyés par les périphériques à SSE, comme indiqué dans l'image :



Vérifier

Vérifiez que les FTD génèrent des événements (malware ou intrusion), pour les événements d'intrusion, accédez à Analyse>Fichiers>Événements de programmes malveillants, pour les événements d'intrusion, accédez à Analyse>Intrusion>Événements.

Vérifiez que les événements sont enregistrés sur le portail SSE comme indiqué à l'étape 4 de la section Register the devices to SSE.

Vérifiez que les informations s'affichent sur le tableau de bord Cisco XDR ou consultez les journaux d'API afin de connaître la raison d'une éventuelle défaillance de l'API.

Dépannage

Détecter les problèmes de connectivité

Vous pouvez détecter des problèmes de connectivité génériques à partir du fichier action_queue.log. En cas d'échec, vous pouvez voir ces journaux présents dans le fichier :

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

Dans ce cas, le code de sortie 28 signifie que l'opération a expiré et que nous devons vérifier la connectivité à Internet. Vous devez également voir le code de sortie 6, ce qui signifie des problèmes avec la résolution DNS

Problèmes de connectivité dus à la résolution DNS

Étape 1. Vérifiez que la connectivité fonctionne correctement.

```
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'
```

Ce résultat montre que le périphérique n'est pas en mesure de résoudre l'URL https://api-sse.cisco.com, dans ce cas, nous devons valider que le serveur DNS approprié est configuré, il peut être validé avec une nslookup de l'expert CLI :

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

Ce résultat montre que le DNS configuré n'est pas atteint. Afin de confirmer les paramètres DNS, utilisez la commande 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
```

Dans cet exemple, un serveur DNS incorrect a été utilisé. Vous pouvez modifier les paramètres DNS à l'aide de cette commande :

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

Une fois cette connectivité testée à nouveau et cette fois, la connexion est établie.

```
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;
```

Problèmes d'inscription au portail SSE

FMC et FTD ont tous deux besoin d'une connexion aux URL SSE sur leur interface de gestion. Pour tester la connexion, entrez ces commandes sur l'interface de ligne de commande Firepower avec accès racine :

<#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

La vérification du certificat peut être contournée avec cette commande :

```
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;
```

> Remarque : vous obtenez le message 403 Forbidden car les paramètres envoyés à partir du test ne correspondent pas aux attentes de SSE, mais cela suffit à valider la connectivité.

Vérifier l'état SSEConnector

Vous pouvez vérifier les propriétés du connecteur comme indiqué.

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

Afin de vérifier la connectivité entre le SSConnector et le EventHandler, vous pouvez utiliser cette commande, ceci est un exemple d'une mauvaise connexion :

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

Dans l'exemple d'une connexion établie, vous pouvez voir que l'état du flux est connecté :

```
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
```

Vérifier les données envoyées au portail SSE et CTR

Afin d'envoyer des événements du périphérique FTD à SEE, une connexion TCP doit être établie avec https://eventing-ingest.sse.itd.cisco.com Ceci est un exemple d'une connexion non établie entre le portail SSE et le 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
```

Dans les journaux connector.log :

```
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
```

> Remarque : notez que les adresses IP affichées x.x.x.246 et 1x.x.x.246 appartiennent à https://eventing-ingest.sse.itd.cisco.com doivent changer, c'est pourquoi la recommandation est d'autoriser le trafic vers le portail SSE basé sur l'URL au lieu des adresses IP.

Si cette connexion n'est pas établie, les événements ne sont pas envoyés au portail SSE. Voici un exemple de connexion établie entre le FTD et le portail 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.
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.