Intégration et dépannage de Cisco XDR avec Secure Firewall

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Configurer

- Licences
- Liez vos comptes à SSX et enregistrez les périphériques.

Méthode 1 (demi-intégration) : Enrichir les investigations

- Enregistrement des périphériques sur SSX

Introduction

Ce document décrit les étapes requises pour intégrer, vérifier et dépanner Cisco XDR avec Secure Firewall.

Il existe deux méthodes d'intégration de Secure Firewall et de XDR, et chaque intégration donne des résultats différents.

La première méthode décrit comment intégrer Secure Firewall, Security Services Exchange (SSX), Security Cloud Control, XDR-Analytics et XDR pour enrichir les investigations.

La deuxième méthode décrit comment intégrer Secure Firewall, SSX, Security Cloud Control, XDR-A, SAL Cloud et XDR, pour enrichir les incidents.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense
- Virtualisation facultative des images
- Cisco Defense Orchestrator
- échange de services de sécurité
- Contrôle du cloud de sécurité

Composants utilisés

- Pare-feu sécurisé - 7.2
- Centre de gestion Firepower (FMC) - 7.2
- Échange de services de sécurité (SSX)
- Cisco XDR
- Portail de licences Smart
- Cisco Defense Orchestrator
- Contrôle du cloud de sécurité

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.

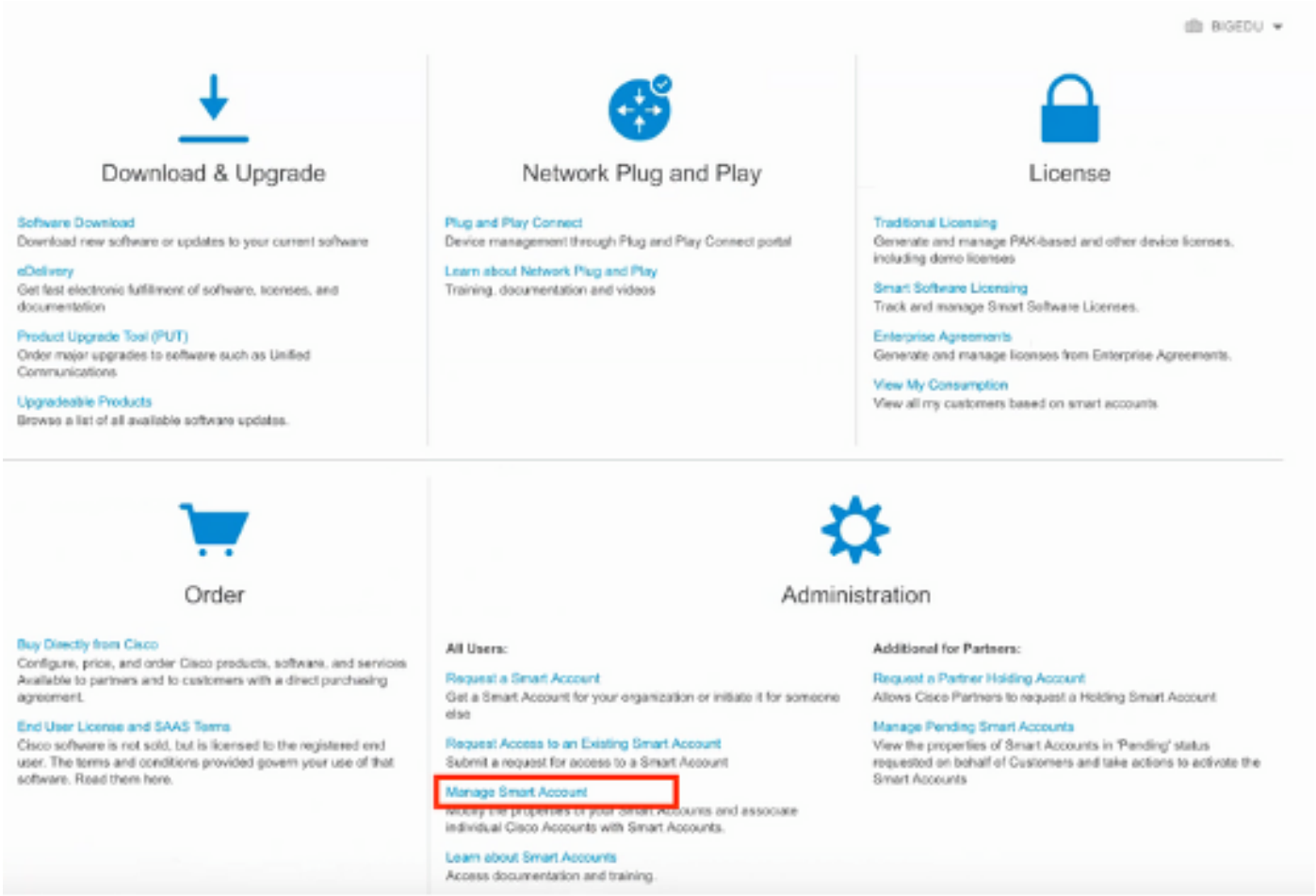
Configurer

Licences

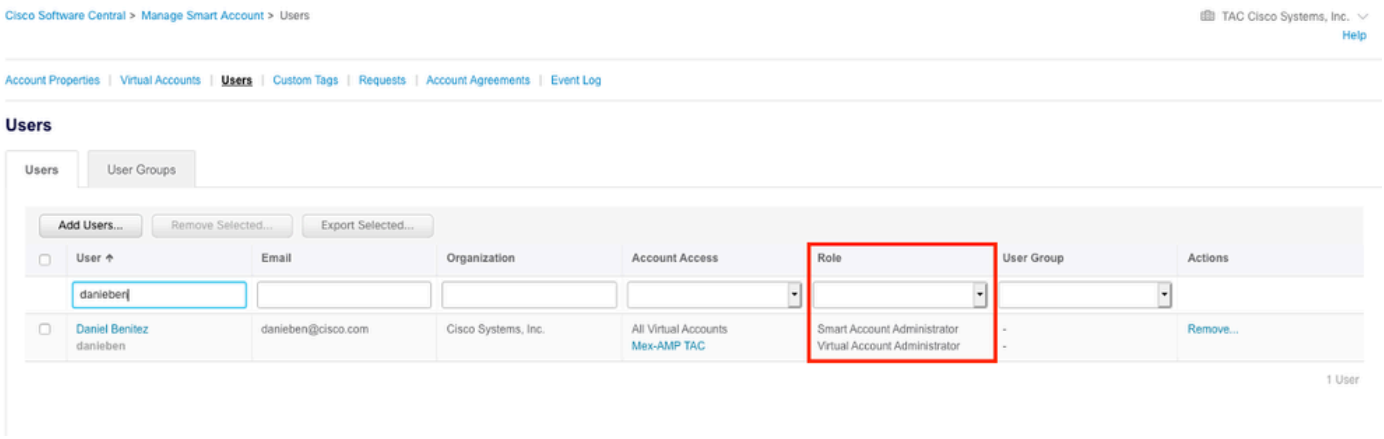
Rôles de compte virtuel :

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

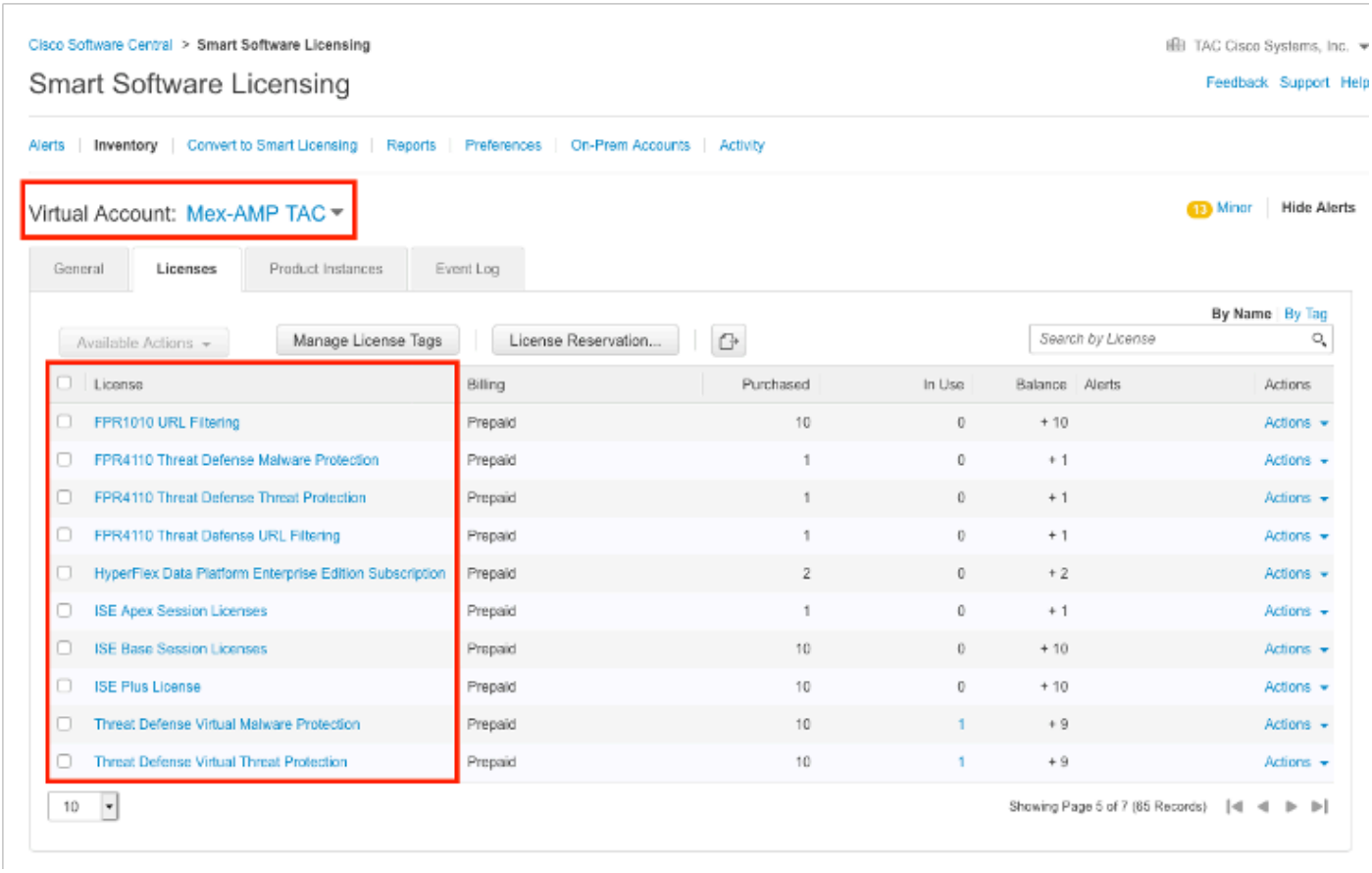
Étape 1. Afin de valider le rôle de compte Smart, accédez à software.cisco.com et sous le menu Administration, sélectionnez Manage Smart Account.



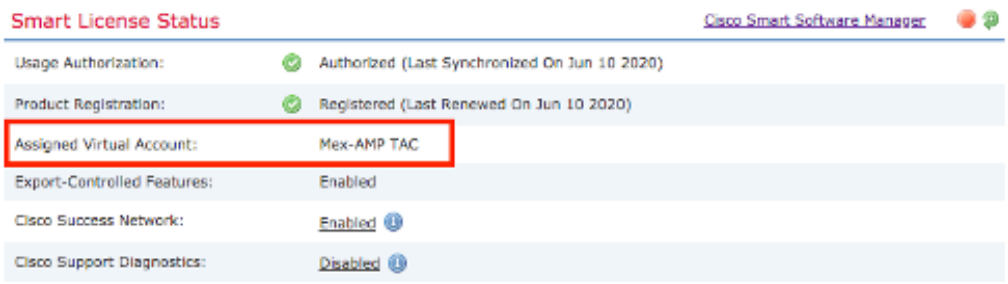
Étape 2. Afin de valider le rôle d'utilisateur, naviguez jusqu'à Users, et vérifiez que sous Roles les comptes sont configurés pour avoir Virtual Account Administrator, comme indiqué dans l'image.

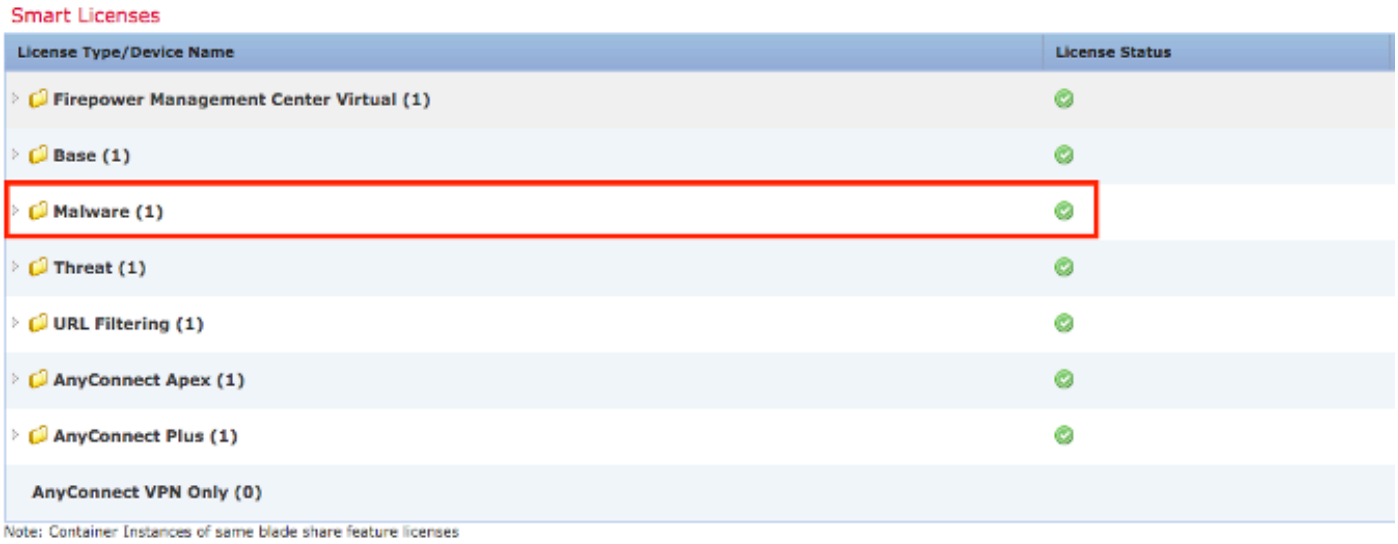


Étape 3. Assurez-vous que le compte virtuel sélectionné pour la liaison sur SSX contient la licence pour les périphériques de sécurité si un compte qui ne contient pas la licence de sécurité est lié sur SSX, les périphériques de sécurité et l'événement n'apparaissent pas sur le portail SSX.



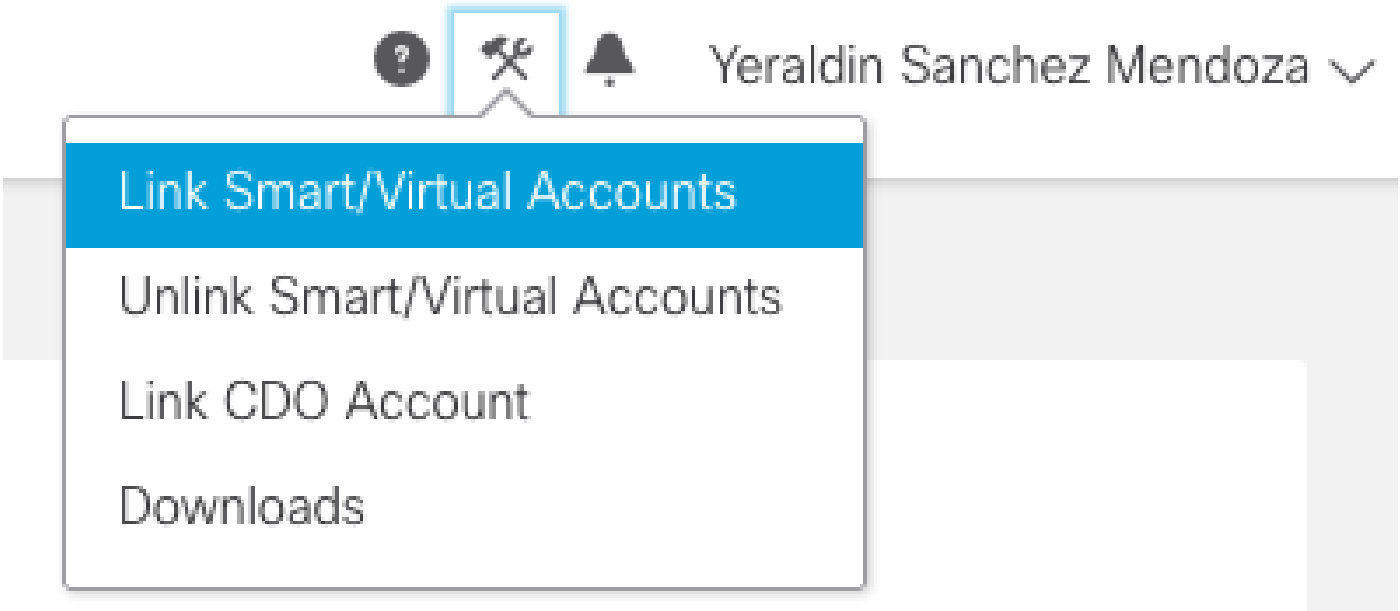
Étape 4. Afin de valider que le FMC a été enregistré sur le compte virtuel correct, accédez à System > Licenses > Smart License :





Liez vos comptes à SSX et enregistrez les périphériques.

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



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

Méthode 1 (demi-intégration) : Enrichir les investigations

Enregistrement des périphériques sur SSX

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

Région des États-Unis

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

Région de l'UE

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

Région APJC

- 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

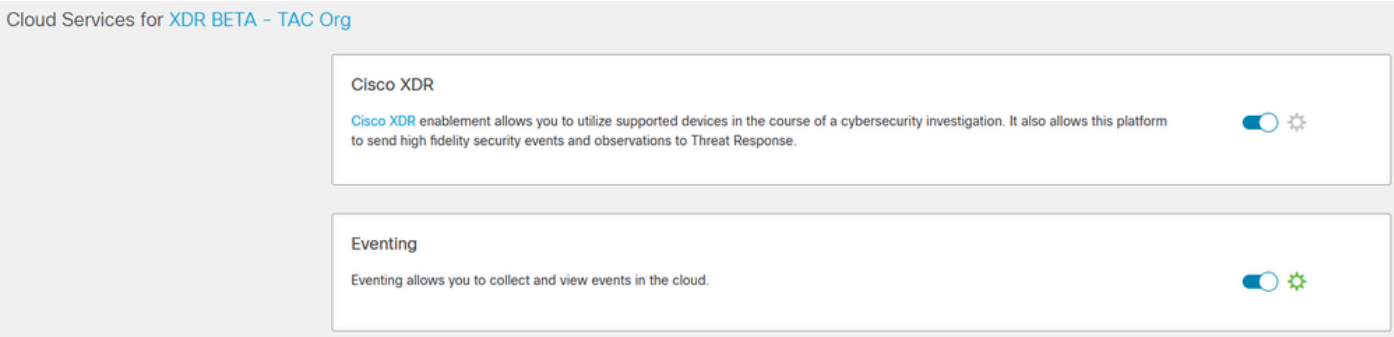
Région Australie :

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

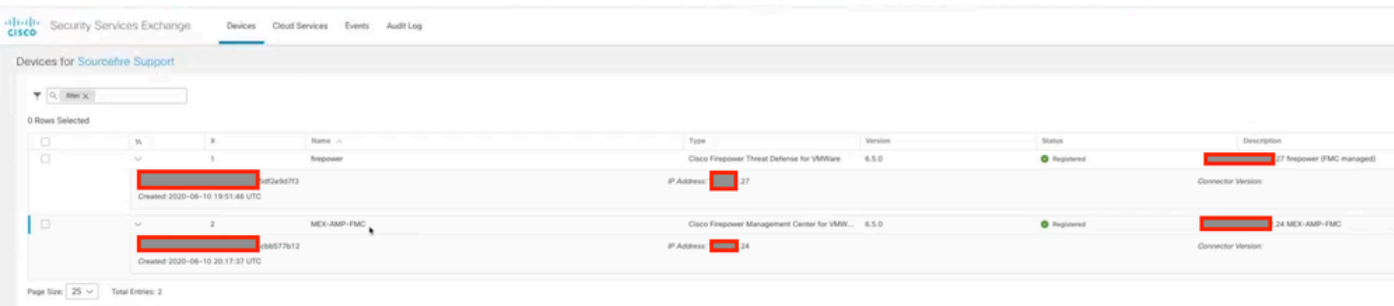
Région Inde :

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

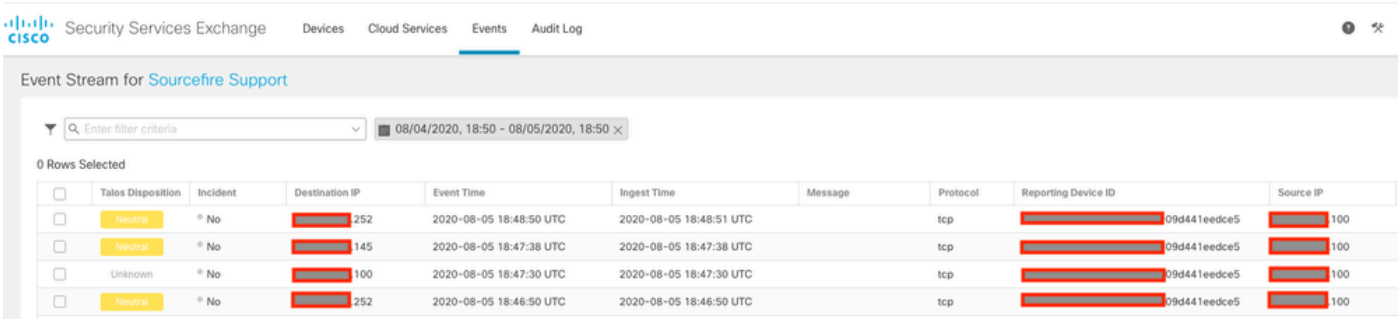
Étape 2. Connectez-vous au portail SSX à l'aide de l'URL suivante : https://admin.sse.itd.cisco.com, accédez à Services cloud et activez les deux options Cisco XDR et Evénement, comme illustré dans l'image.



Étape 3. Vous pouvez valider que vous pouvez maintenant voir les périphériques inscrits sur SSX :



Les Événements sont envoyés par les périphériques Secure Firewall, naviguez jusqu'aux Événements sur le portail SSX pour vérifier les événements envoyés par les périphériques à SSX, comme indiqué dans l'image.



Enregistrement des périphériques dans Security Cloud Control (SCC/CDO)

Étape 1. Assurez-vous que ces URL sont autorisées dans votre environnement

Région US :

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

Région de l'UE

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

Région APJC

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

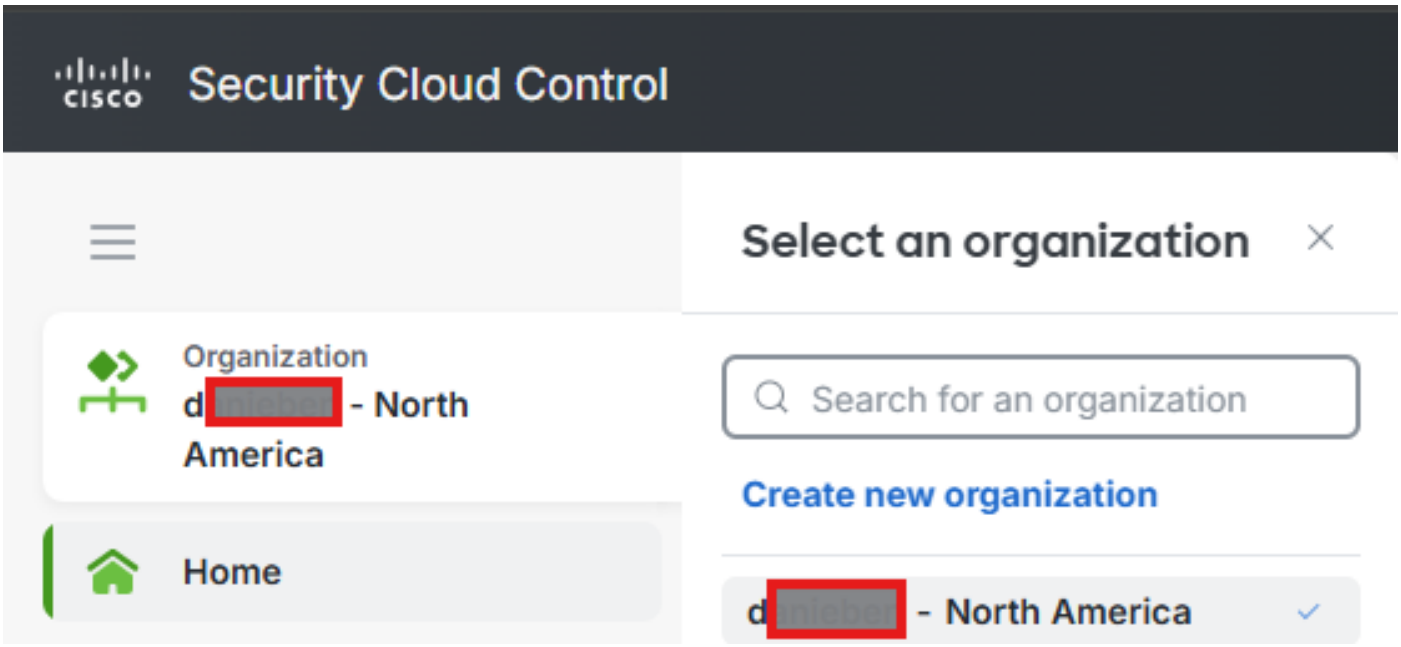
Région Australie :

- aus.cdo.cisco.com

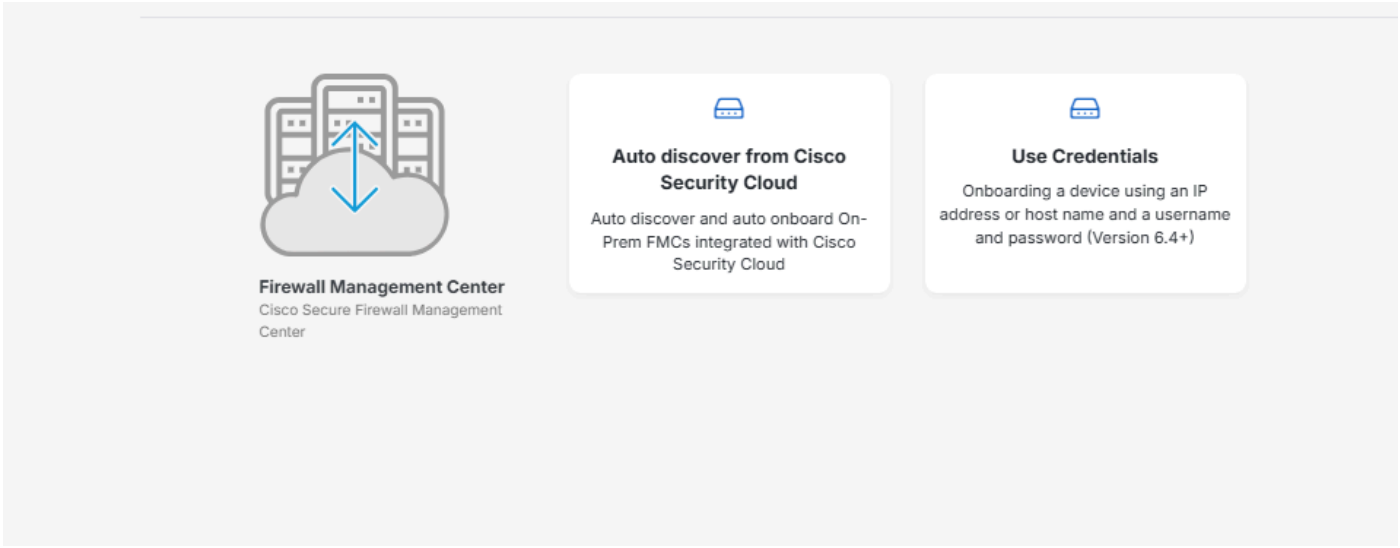
Région Inde :

- in.cdo.cisco.com

Étape 2. Accédez à Security Cloud Control (le lien peut varier selon votre région) et sélectionnez votre organisation Security Cloud Control.



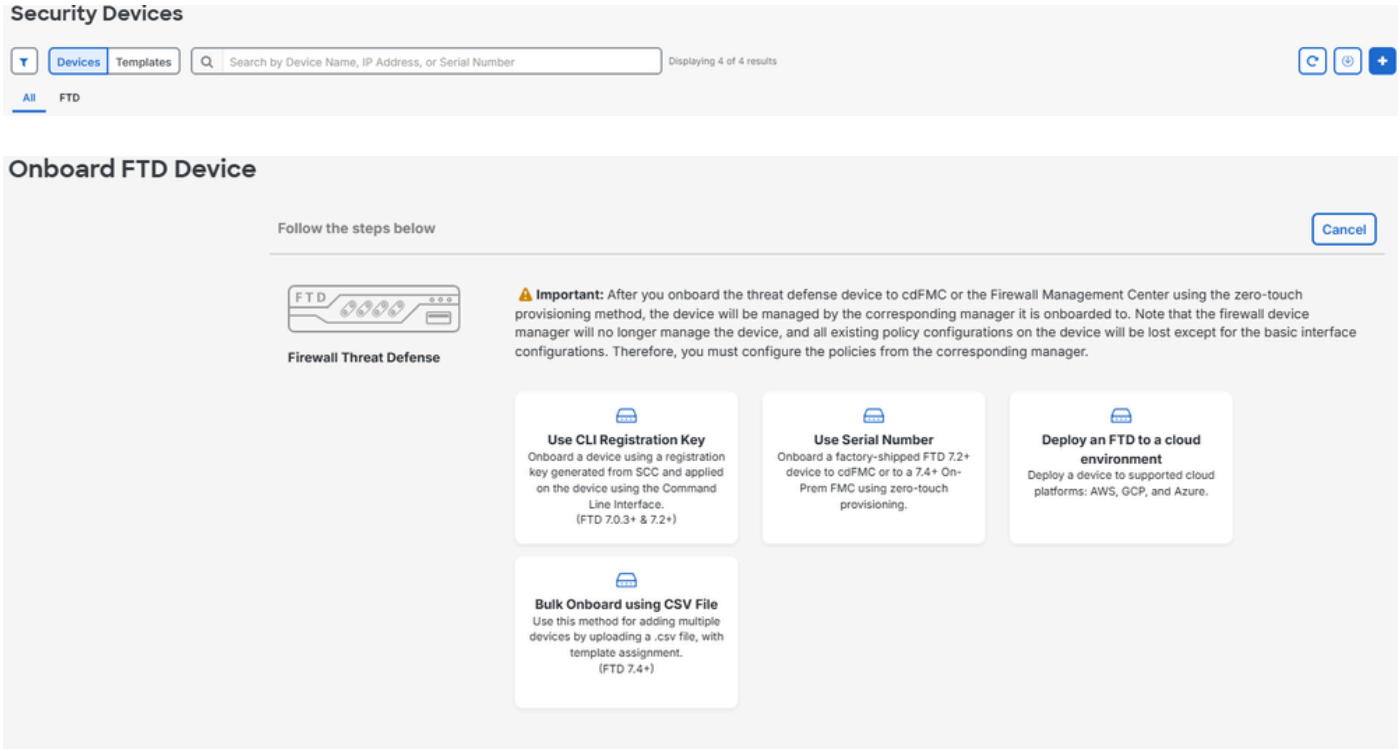
Étape 3. Une fois que vous avez sélectionné l'organisation appropriée, naviguez vers Products > Firewall, vérifiez si votre périphérique est déjà là, sinon, vous pouvez l'intégrer à Security Cloud Control (Cisco Defense Orchestrator), pour cela, sous Overall Inventory, cliquez sur View all Devices.



Étape 4. Accédez à Administration > Firewall Management Center, une liste de vos FMC intégrés dans SCC est présentée, si vous ne voyez pas votre Firewall Management Center, cliquez sur l'icône plus.

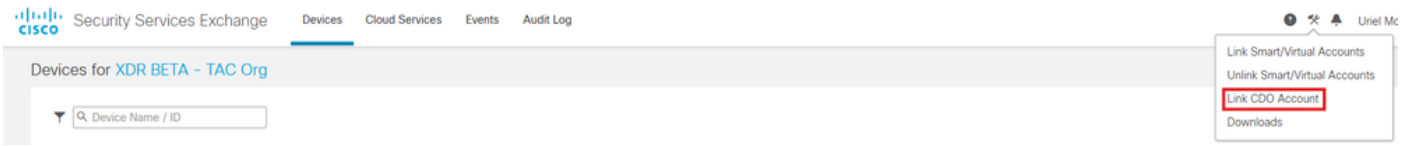
Étape 4.1. Normalement, les pare-feu sécurisés sont automatiquement intégrés. Sinon, sélectionnez le périphérique que vous souhaitez intégrer (FTD) et la méthode d'intégration que vous préférez.

Étape 4.2. Dans la section Security Devices (Périphériques de sécurité), cliquez sur l'icône plus, sélectionnez Onboard Secure Firewall Device (Périphérique de pare-feu sécurisé intégré) et sélectionnez



Étape 5. Une fois que vous avez intégré vos périphériques dans Security Cloud Control, vous pouvez le visualiser dans l'inventaire.

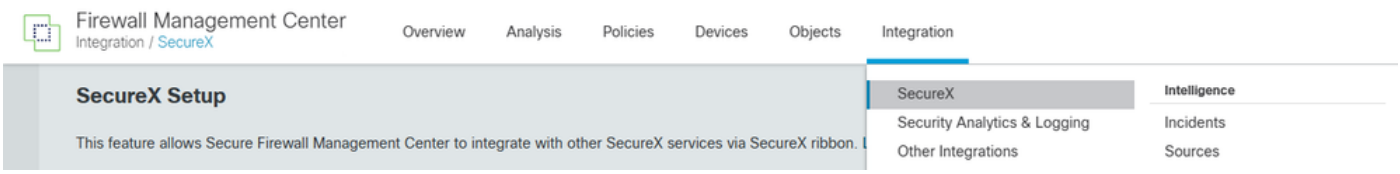
Étape 6. Assurez-vous que votre organisation CDO est liée à votre organisation SSX. Pour cela, accédez à Security Services Exchange, cliquez sur l'icône du menu Outils, puis cliquez sur Lier un compte CDO.



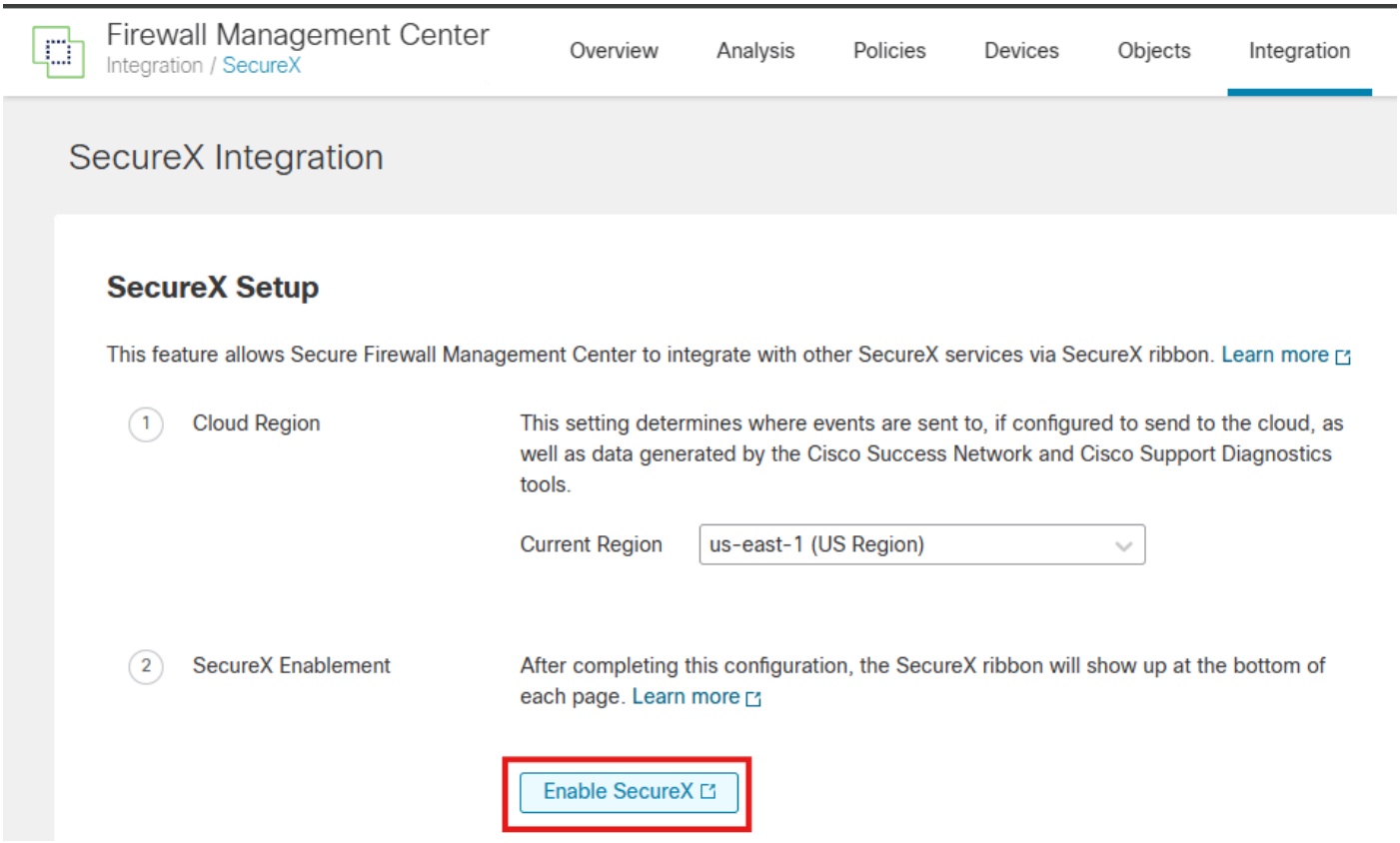
Intégrer un pare-feu sécurisé

De 7.2.x à 7.4.x avec Cisco XDR

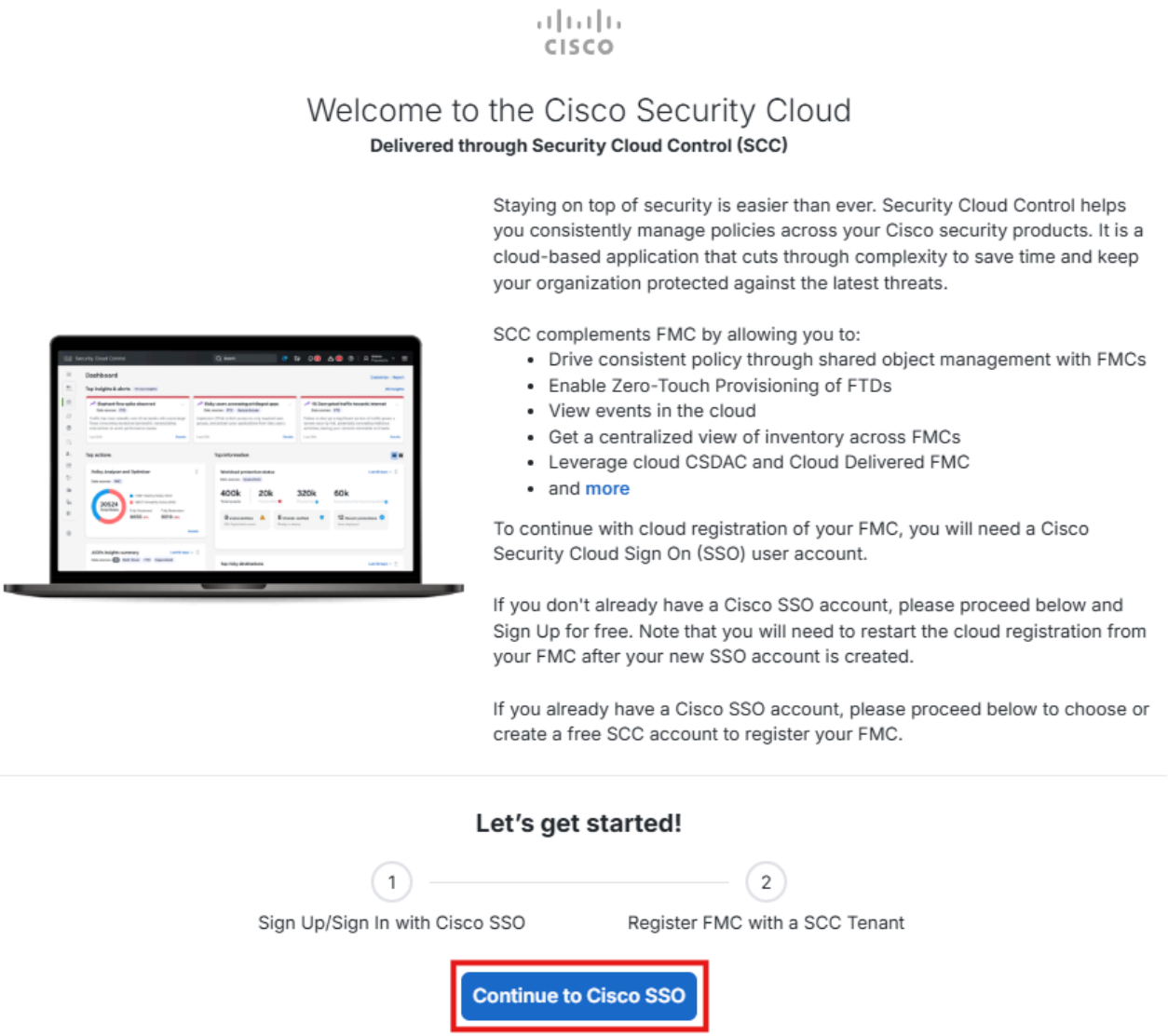
Étape 1. Dans votre Centre de gestion du pare-feu sécurisé, accédez à Intégration > SecureX



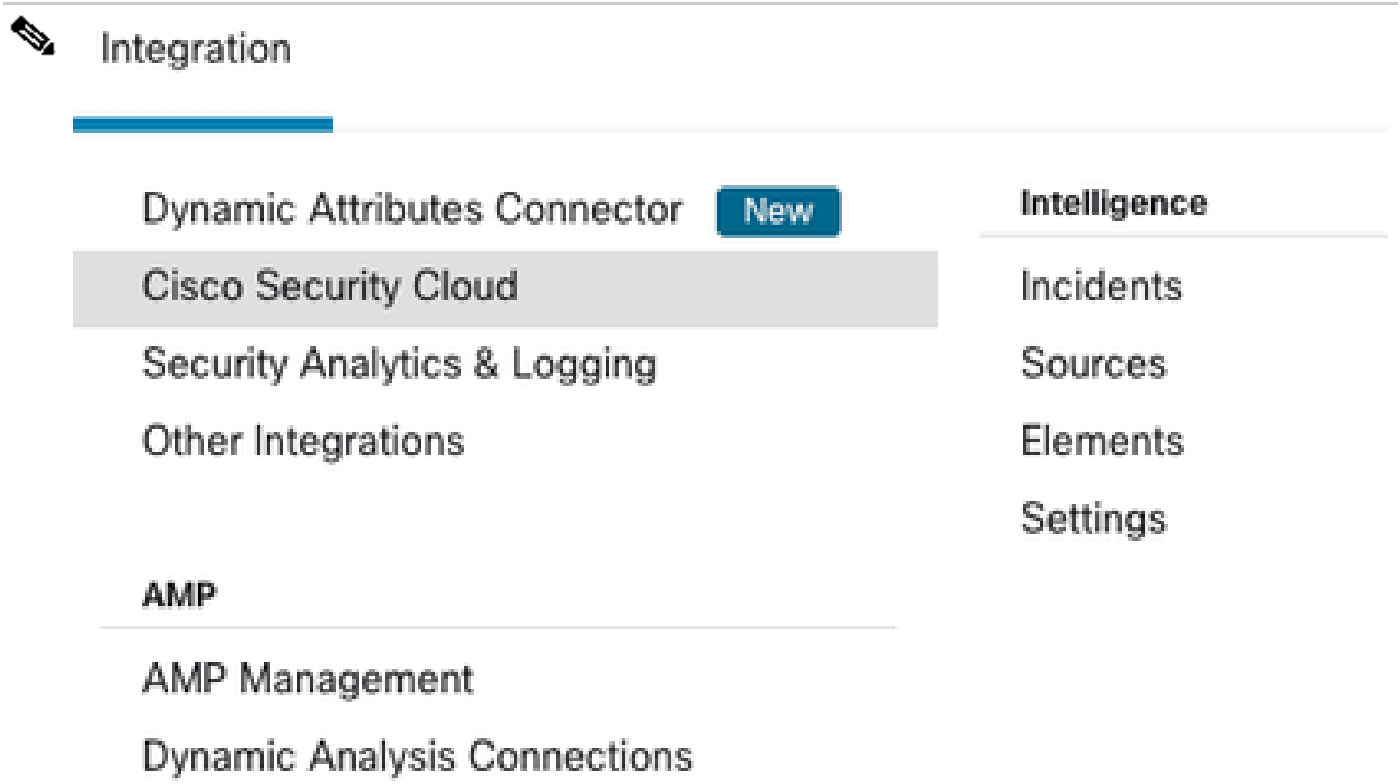
Étape 2. Choisissez la région appropriée, puis cliquez sur Enable SecureX.



Étape 3. Après avoir cliqué sur Activer SecureX, il vous redirige vers la page d'authentification de Cisco Defense Orchestrator (qui tire parti de la connexion au cloud de sécurité), cliquez sur Continuer vers Cisco SSO.



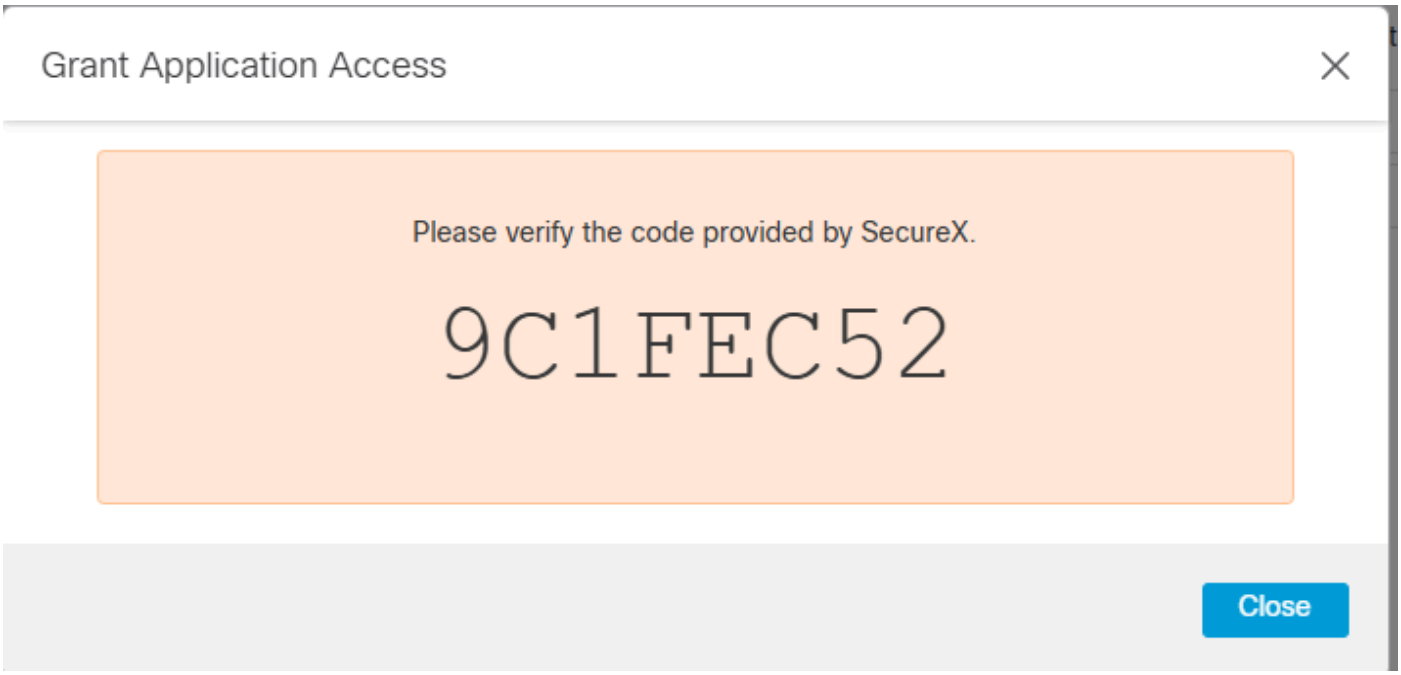
Remarque :
À partir de la version 7.6.x et ultérieure avec Cisco XDR
Étape 1. Dans votre Secure Firewall Management Center, accédez à Integration > Cisco Security Cloud

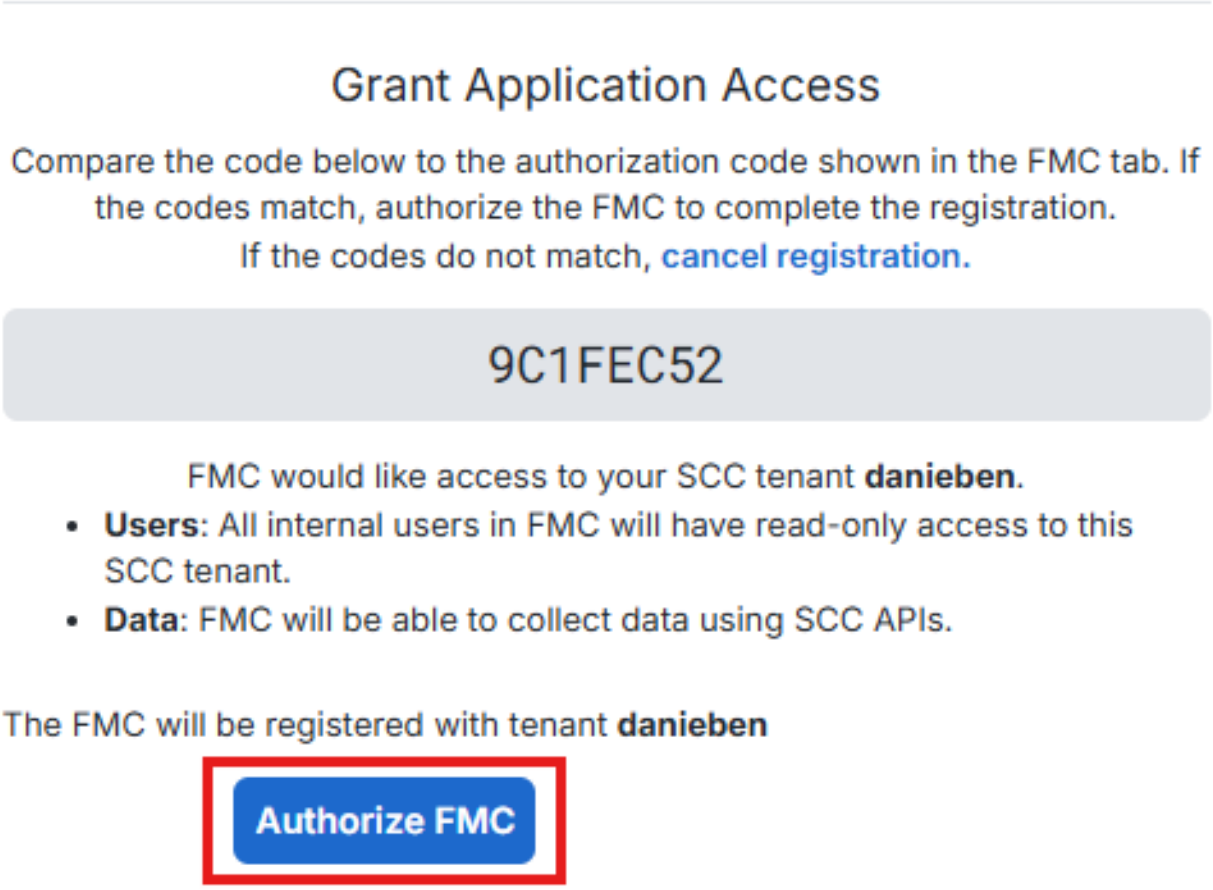


Étape 2. Choisissez la région appropriée, puis cliquez sur Enable Cisco Security Cloud.
Étape 3. Après avoir cliqué sur Enable Cisco Security Cloud, il vous redirige vers la page d'authentification de Cisco Defense Orchestrator (qui tire parti de Security Cloud Sign On), cliquez sur Continue to Cisco SSO.

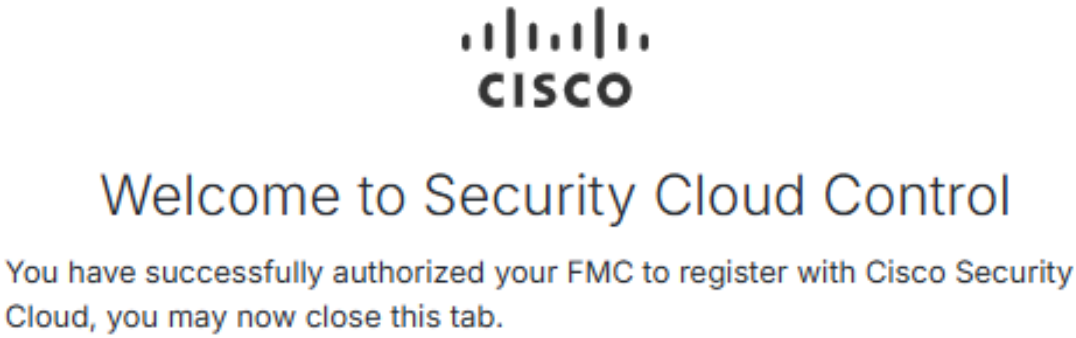
Étape 4. Vous pouvez sélectionner un locataire de contrôle cloud de sécurité préexistant ou en créer un nouveau.

Étape 5. Sélectionnez le locataire approprié et assurez-vous que le code que vous recevez dans cette page correspond au code que vous recevez dans FMC. S'ils correspondent, cliquez sur Autoriser FMC.



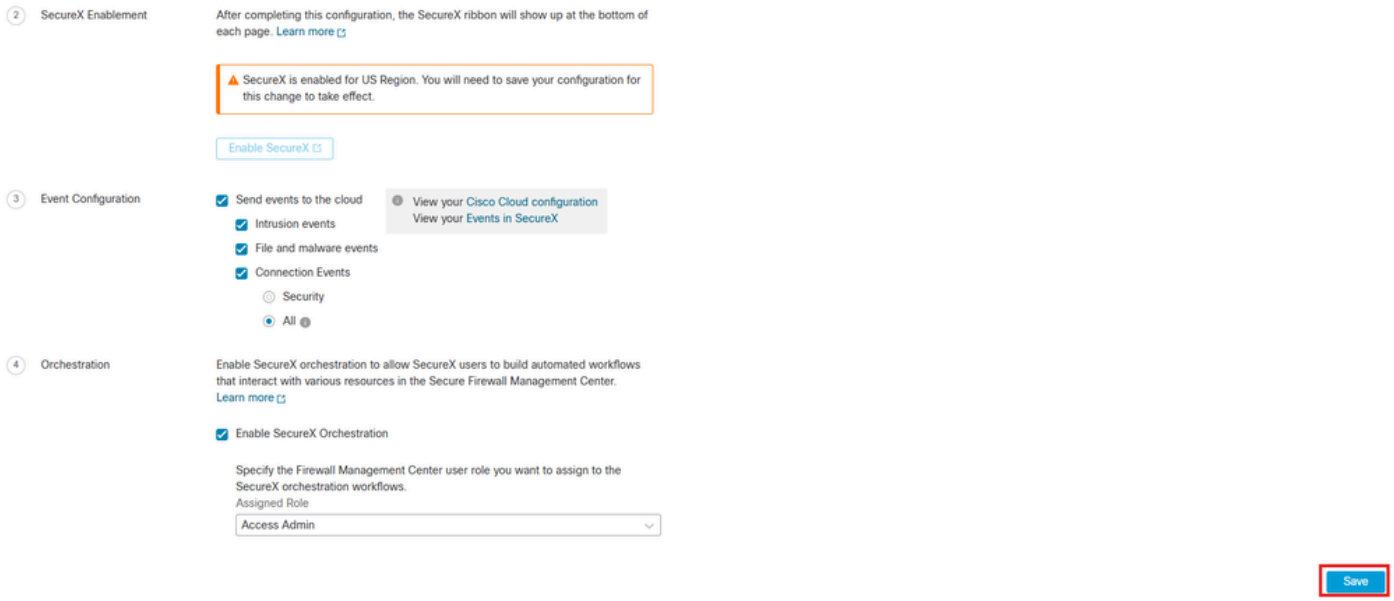


Étape 6. Entrez vos informations d'identification de connexion au cloud de sécurité et autorisez l'intégration. Une fois l'intégration terminée, une confirmation indiquant que FMC a été autorisé à s'enregistrer auprès de Cisco Security Cloud s'affiche.



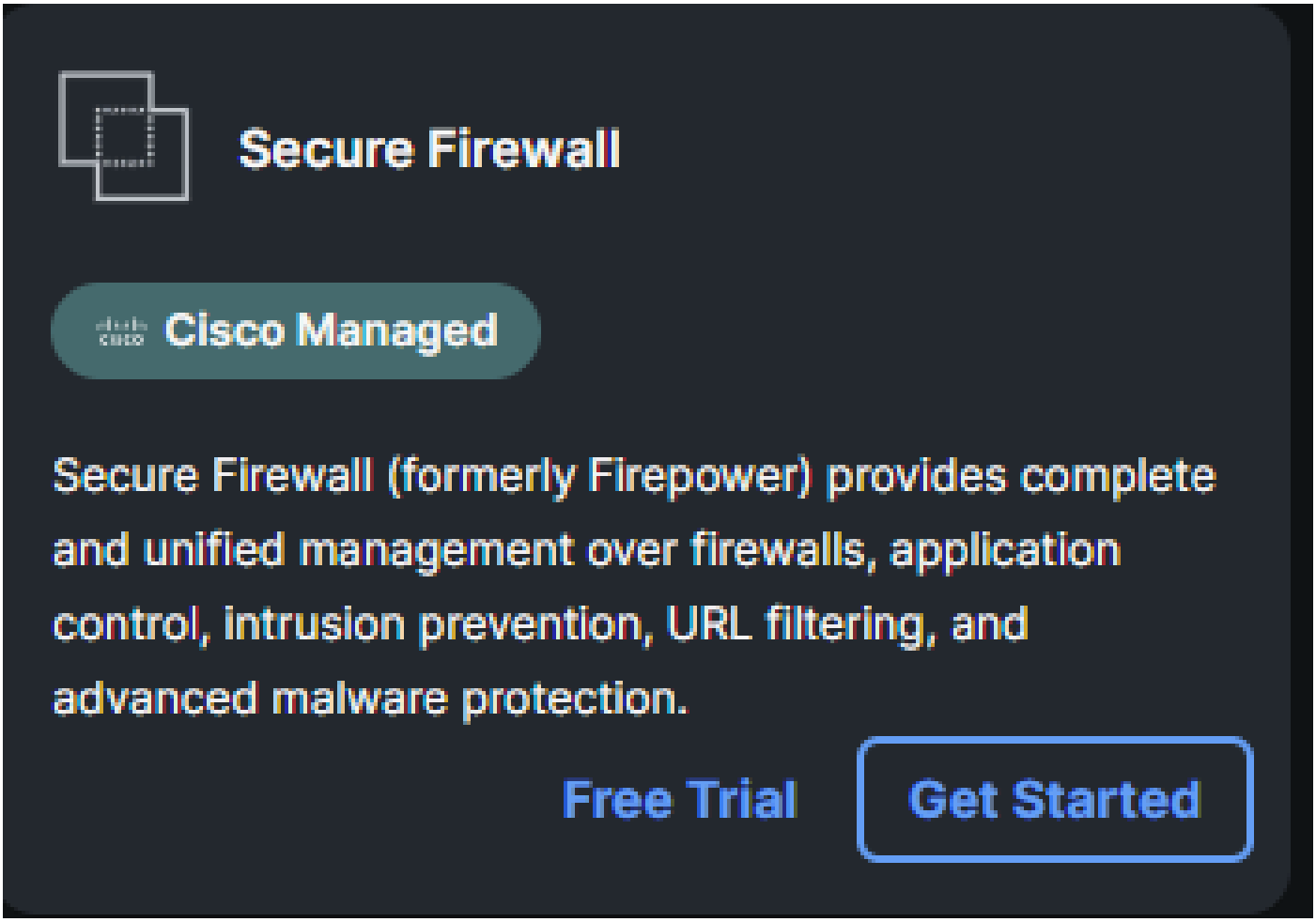
Étape 7. Une fois l'autorisation terminée, vous pouvez revenir à votre FMC et sélectionner les événements que vous souhaitez envoyer vers le cloud. Une fois que vous avez terminé, cliquez sur Enregistrer.

Étape 8. Vous pouvez sélectionner Activer l'orchestration SecureX (XDR Automate)

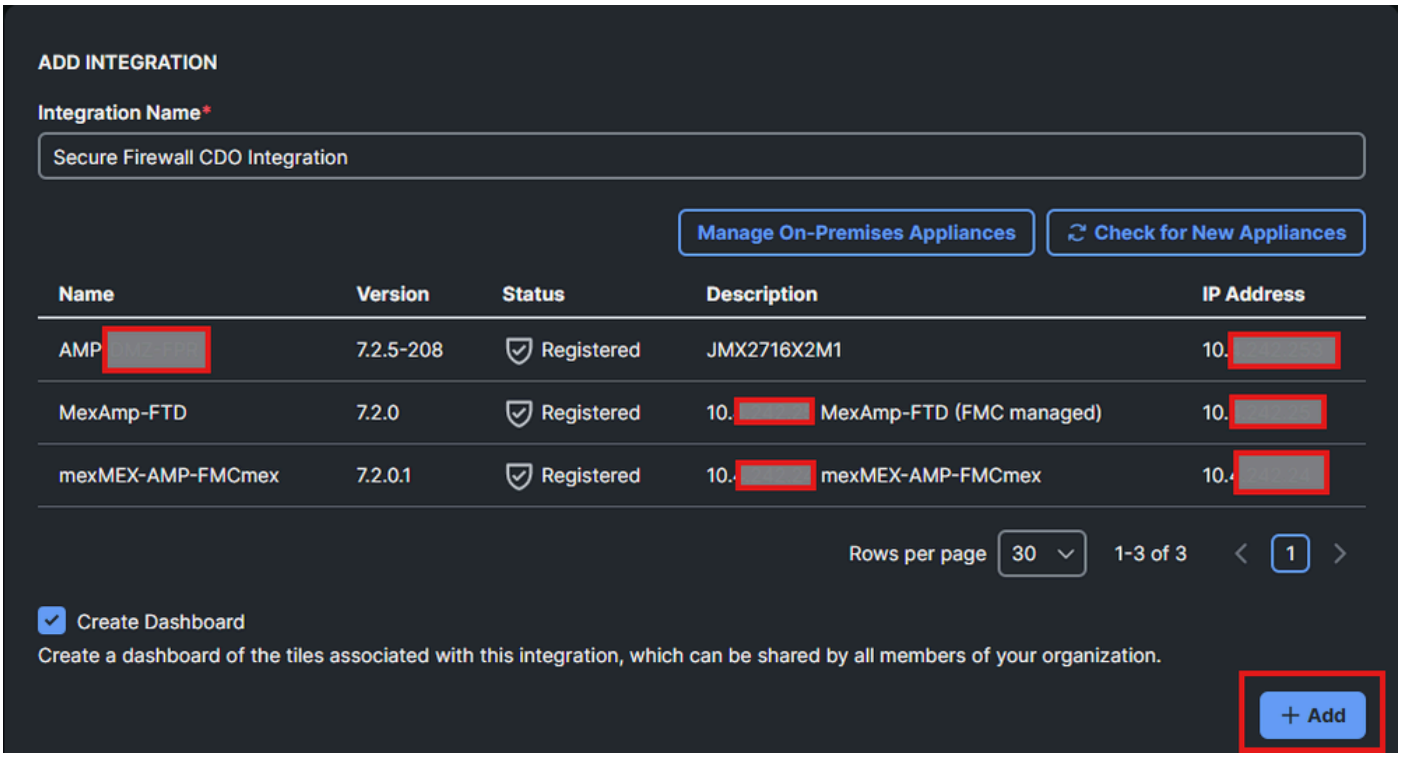


Étape 9. Accédez à XDR > Administration > On Premises Appliance et recherchez vos appliances, elles doivent être enregistrées automatiquement.

Étape 10. Accédez à XDR > Administration > Integrations et activez l'intégration du pare-feu sécurisé.



Étape 10.1. Attribuez un nom à votre intégration, cliquez sur +Ajouter.



Cette intégration vous permet d'enrichir les investigations dans XDR.

Méthode 2 (intégration complète) : Enrichir les incidents en XDR

Remarque : Afin d'assurer une intégration transparente entre Secure Firewall, XDR, Cisco Defense Orchestrator (CDO), Security Services Exchange (SSX) et Security Analytics and Logging (SAL), le mappage manuel est nécessaire. Ce processus implique de contacter le TAC Cisco pour effectuer les configurations et mappages nécessaires.

Étape 1. Votre compte CDO doit disposer d'une licence Security Analytics and Logging pour transférer les événements à Cisco XDR.

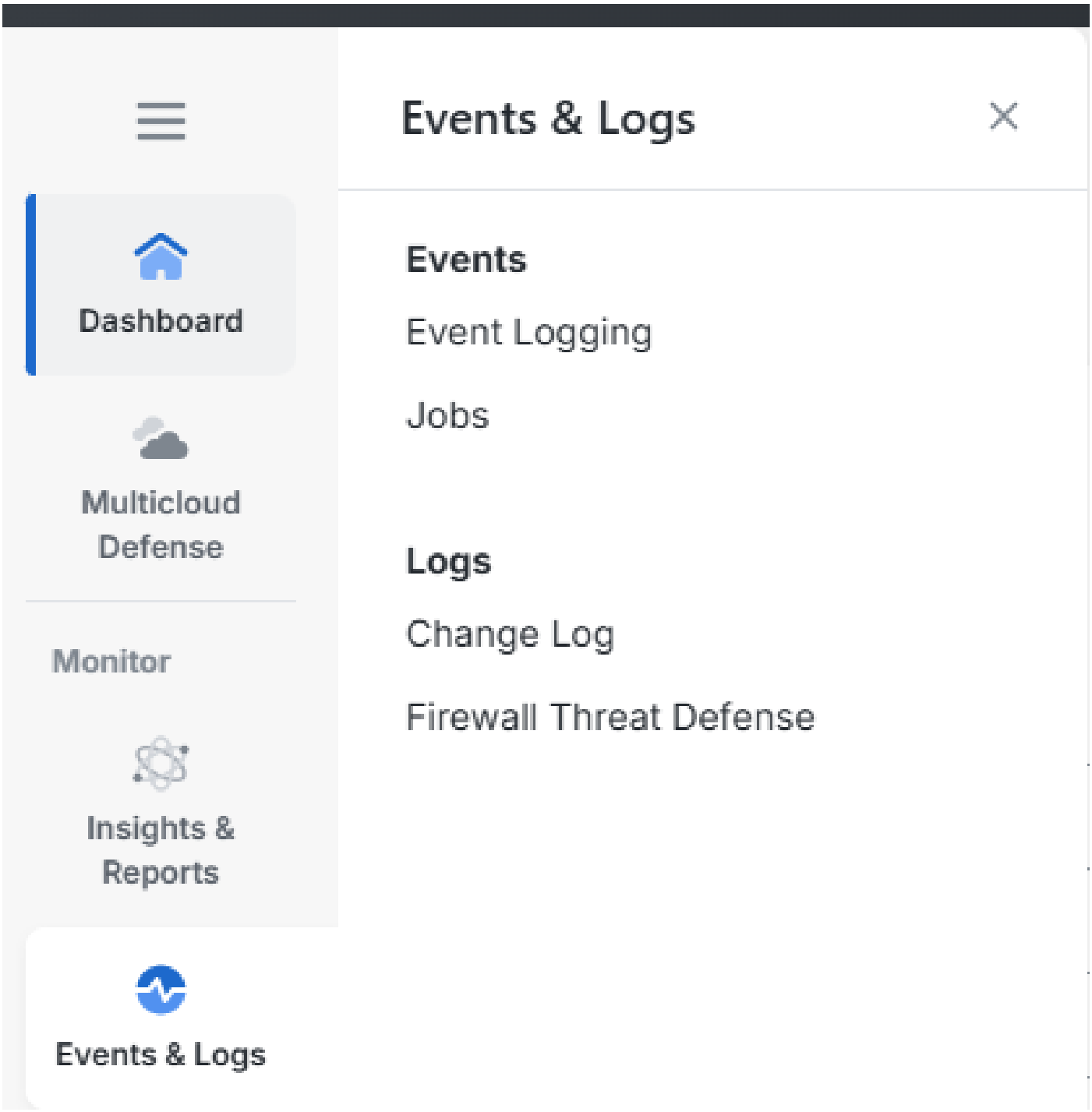
Étape 2. Suivez les étapes décrites précédemment pour enregistrer vos appliances dans SSX et Security Cloud Control.

Étape 3. Une fois que vous avez terminé, contactez le TAC avec ces détails et demandez à lier Security Cloud Control/SAL à XDR Analytics.

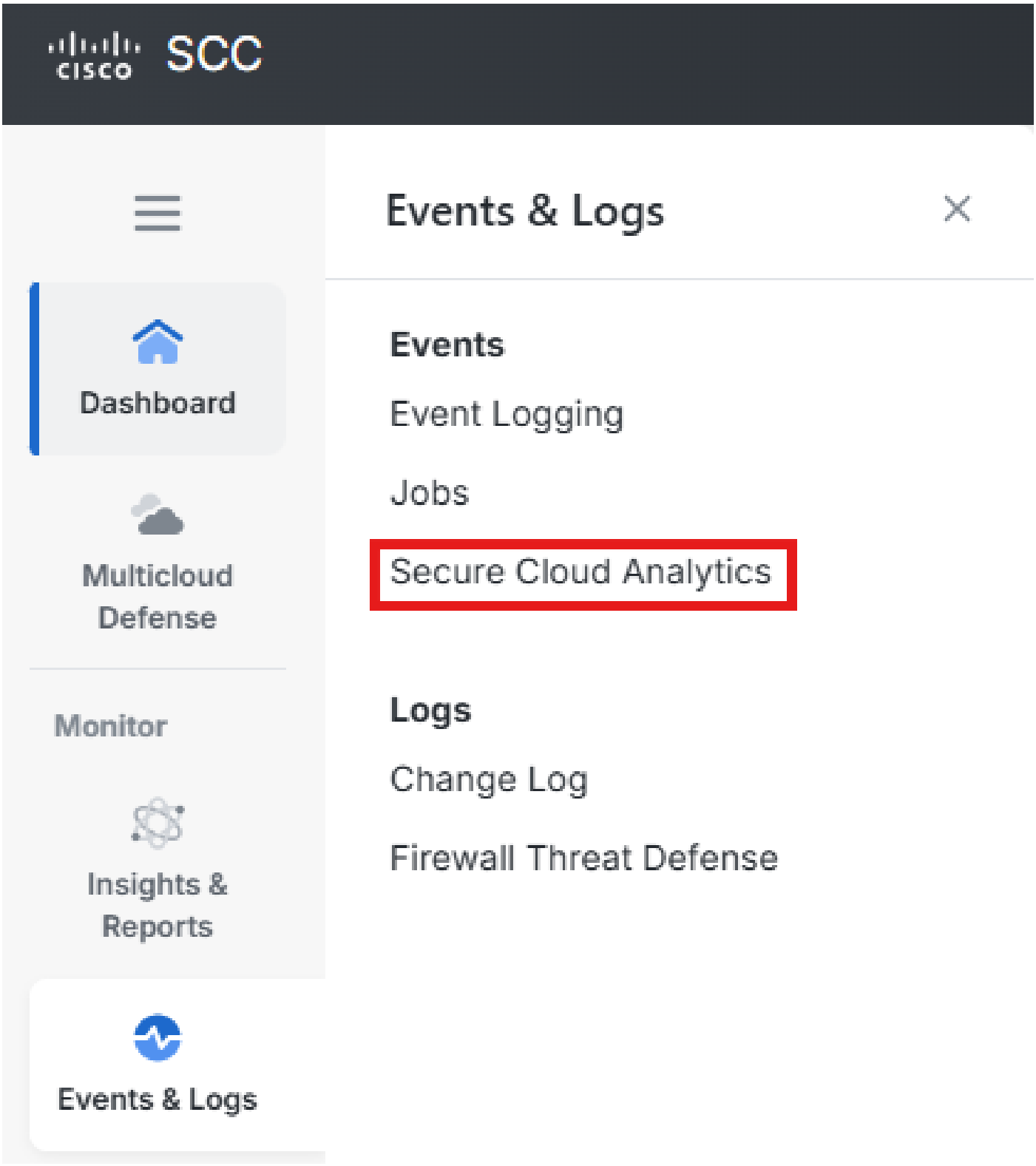
- ID du locataire CDO
- Nom CDO
- ID d'organisation XDR
- ID du locataire SSX
- Nom SSX
- ID d'organisation SCA

Étape 4. Assurez-vous que votre compte CDO est lié au portail XDR Analytics.

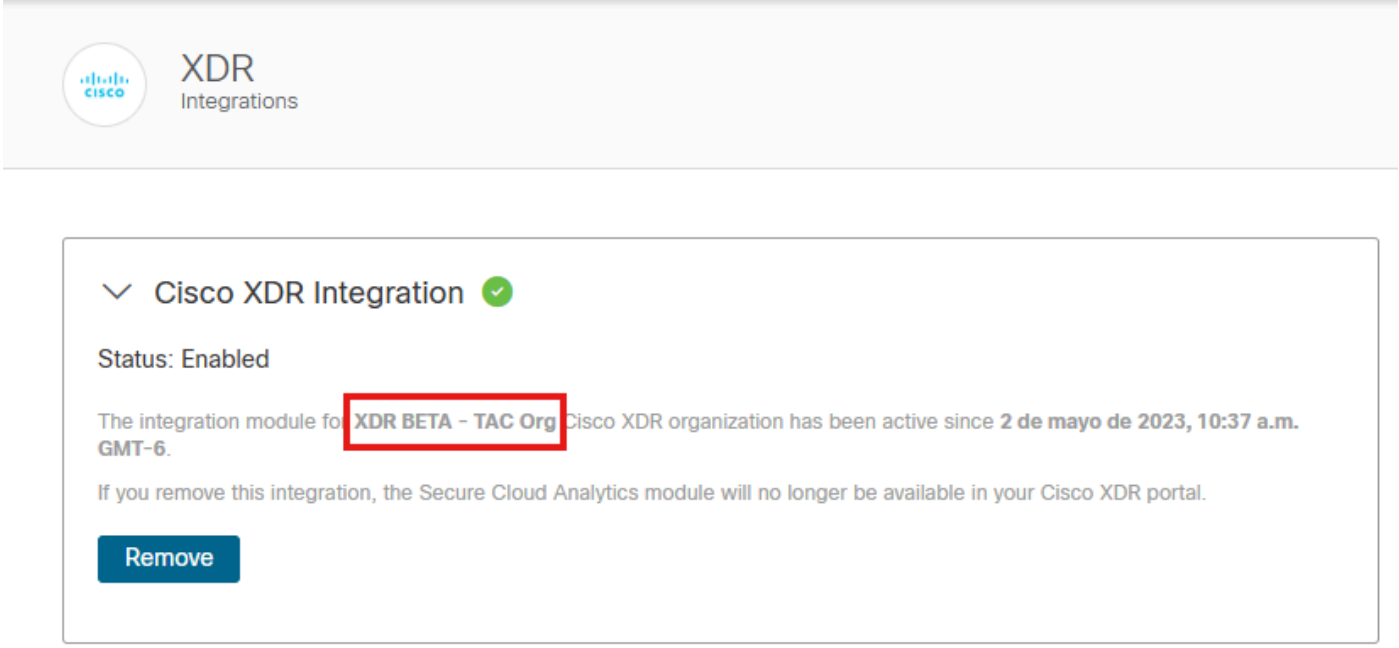
Avant de lier votre portail CDO à XDR Analytics, il ressemble à ceci :



Une fois le lien terminé, vous pouvez voir l'option permettant d'accéder à votre portail XDR Analytics.



Étape 5. Une fois que votre compte XDR Analytics est lié à votre portail de contrôle du cloud de sécurité (CDO), vous devez vous assurer que votre XDR Analytics est intégré à XDR. Pour cela, dans XDR Analytics, accédez à Paramètres > Intégrations > XDR, recherchez l'intégration de XDR et assurez-vous qu'il y a une coche verte et que le module d'intégration pointe vers votre organisation XDR correcte.



Vérifier

Vérifiez que les pare-feu sécurisés génèrent des événements (malware ou intrusion), pour les événements d'intrusion, accédez à Analyse >Fichiers >Malware Events, pour les événements d'intrusion, accédez à Analysis > Intrusion > Events.

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

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.

Vérifiez que tous les locataires sont correctement reliés entre eux. Si vous rencontrez des problèmes, ouvrez un dossier TAC et fournissez les informations suivantes :

- ID du locataire CDO
- Nom CDO
- ID d'organisation XDR
- ID du locataire SSX
- Nom SSX
- ID d'organisation SCA

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 : vérification du bon fonctionnement de la connectivité

```
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 SSX

FMC et Secure Firewall ont tous deux besoin d'une connexion aux URL SSX 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 à ce que SSX attend, mais cela s'avère suffisant pour 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 SSX et au CTR

Pour envoyer des événements du périphérique Secure Firewall à SSX, une connexion TCP doit être établie avec https://eventing-ingest.sse.itd.cisco.com Ceci est un exemple de connexion non établie entre le portail SSX et le Secure Firewall :

```
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 SSX basé sur l'URL au lieu des adresses IP.

Si cette connexion n'est pas établie, les événements ne sont pas envoyés au portail SSX. Voici un exemple d'une connexion établie entre le pare-feu sécurisé et le portail SSX :

```
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.
```

Le périphérique (FTD) ne peut pas être inscrit au contrôle du cloud de sécurité

Si votre périphérique ne peut pas être inscrit dans le contrôle du cloud de sécurité, assurez-vous qu'il est connecté au locataire CDO approprié.

Pour vérifier l'URL correcte, accédez à Administration > Firewall Management Center, sélectionnez Cloud Delivered FMC, en haut à droite de votre écran, vous pouvez voir le nom d'hôte.

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

Si vous rencontrez toujours des problèmes pour vous connecter à CDO, assurez-vous que le port 8305 est ouvert, ceci est un exemple de problème de connexion.

```
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
```

Périphérique inscrit à un client SSX incorrect

Vous pouvez vérifier à quel client SSX votre FMC est inscrit.

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

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

Si le locataire SSX est incorrect, vous devez recommencer les étapes pour inscrire vos appliances dans SSX

Si le locataire SSX est correct, mais que le locataire CDO n'est pas lié à l'organisation SSX appropriée, veuillez contacter le TAC avec ces détails :

- ID du locataire SSX
- ID du locataire CDO

Informations connexes

- Guide d'intégration de Cisco Secure Firewall Threat Defense et de Cisco XDR
- Assistance technique de Cisco et téléchargements

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.