Intégration et dépannage de SecureX avec Firepower Threat Defense (FTD)

Contenu

Introduction

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

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Components Used

- Firepower Threat Defense (FTD) - 6,5
- Firepower Management Center (FMC) - 6,5
- Échange de services de sécurité (SSE)
- SecureX

- Portail des licences Smart

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. 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.

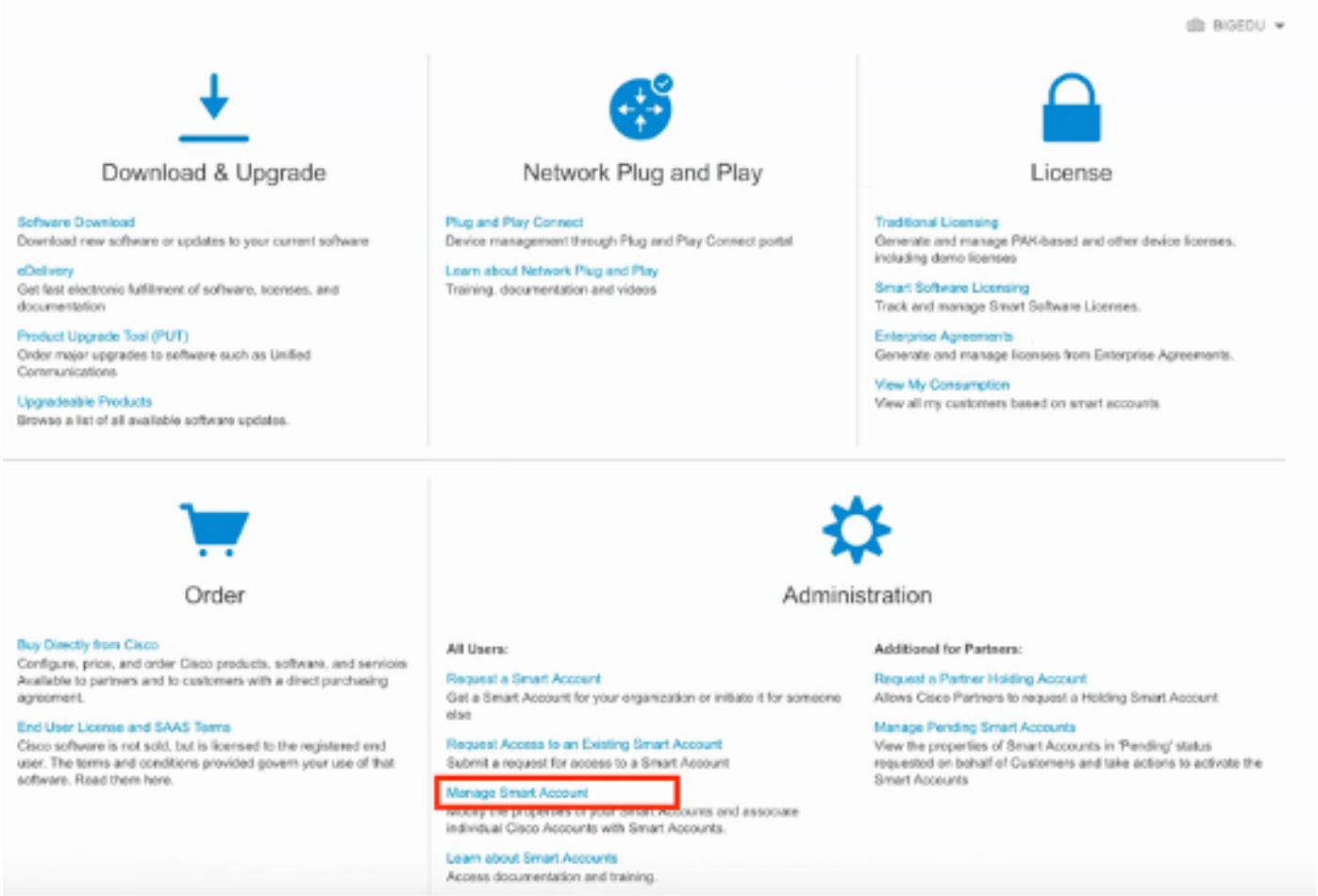
Configuration

Licence

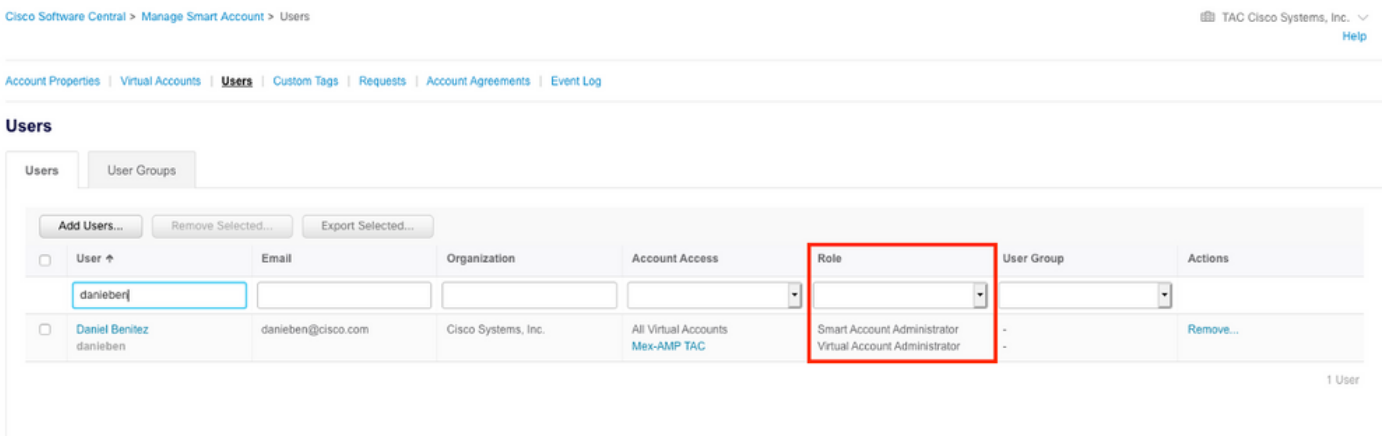
Rôles de compte virtuel :

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

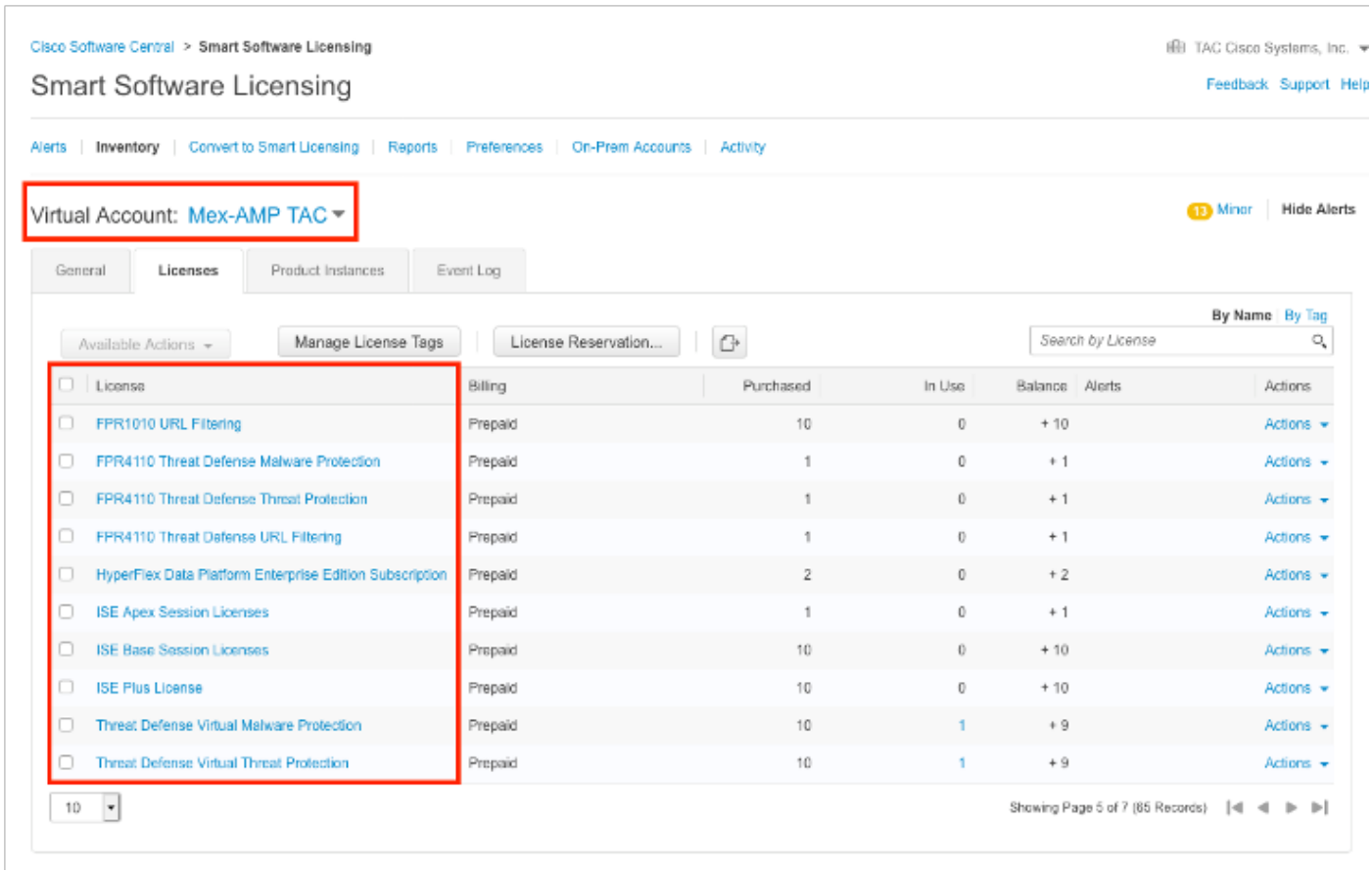
Étape 1. Afin de valider le rôle de compte Smart, accédez à **software.cisco.com** et sous le **menu Administration**, sélectionnez **Gérer le compte Smart**.



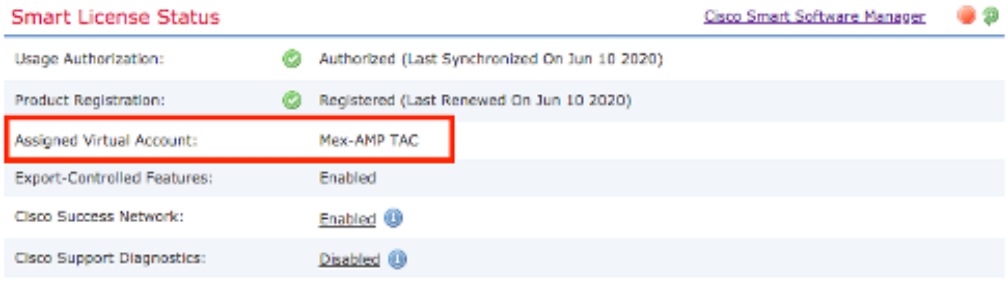
Étape 2. Afin de valider le rôle d'utilisateur, accédez à **Utilisateurs**, et validez que sous Rôles, les comptes sont configurés pour avoir un administrateur de compte virtuel, comme illustré dans l'image.



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, que les périphériques de sécurité et l'événement n'apparaît pas sur le portail SSE.

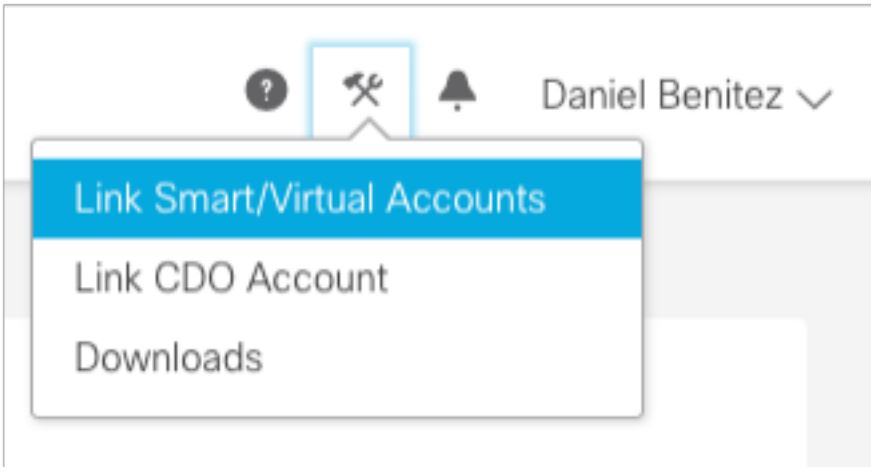


Étape 4. Pour vérifier que le FMC a été enregistré sur le compte virtuel approprié, accédez à **System>Licenses>Smart License:**



Liez vos comptes à SSE et enregistrez les périphériques.

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



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

Enregistrer les périphériques sur SSE

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

Région des États-Unis

- api-sse.cisco.com

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

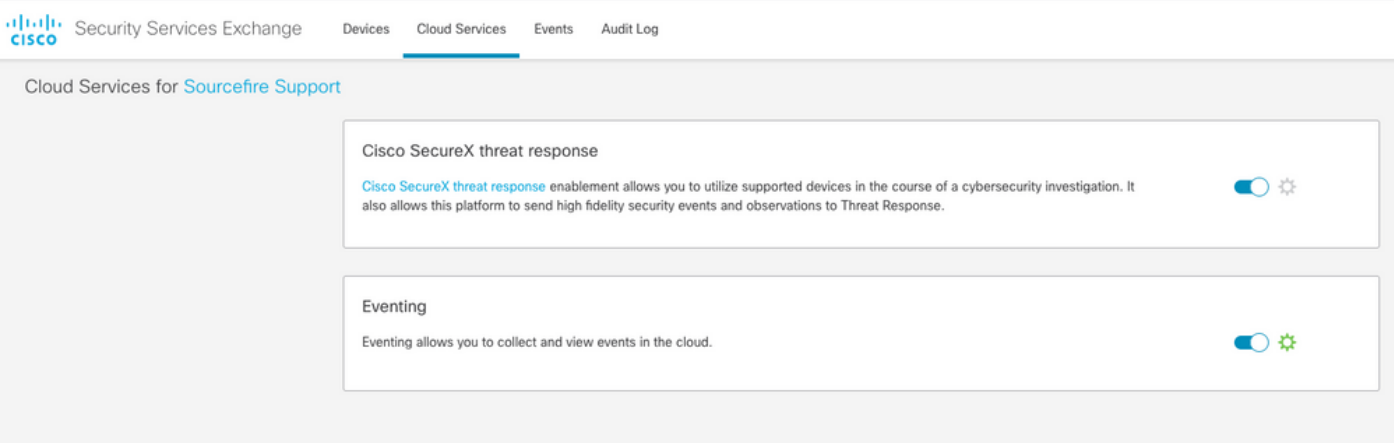
Région UE

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

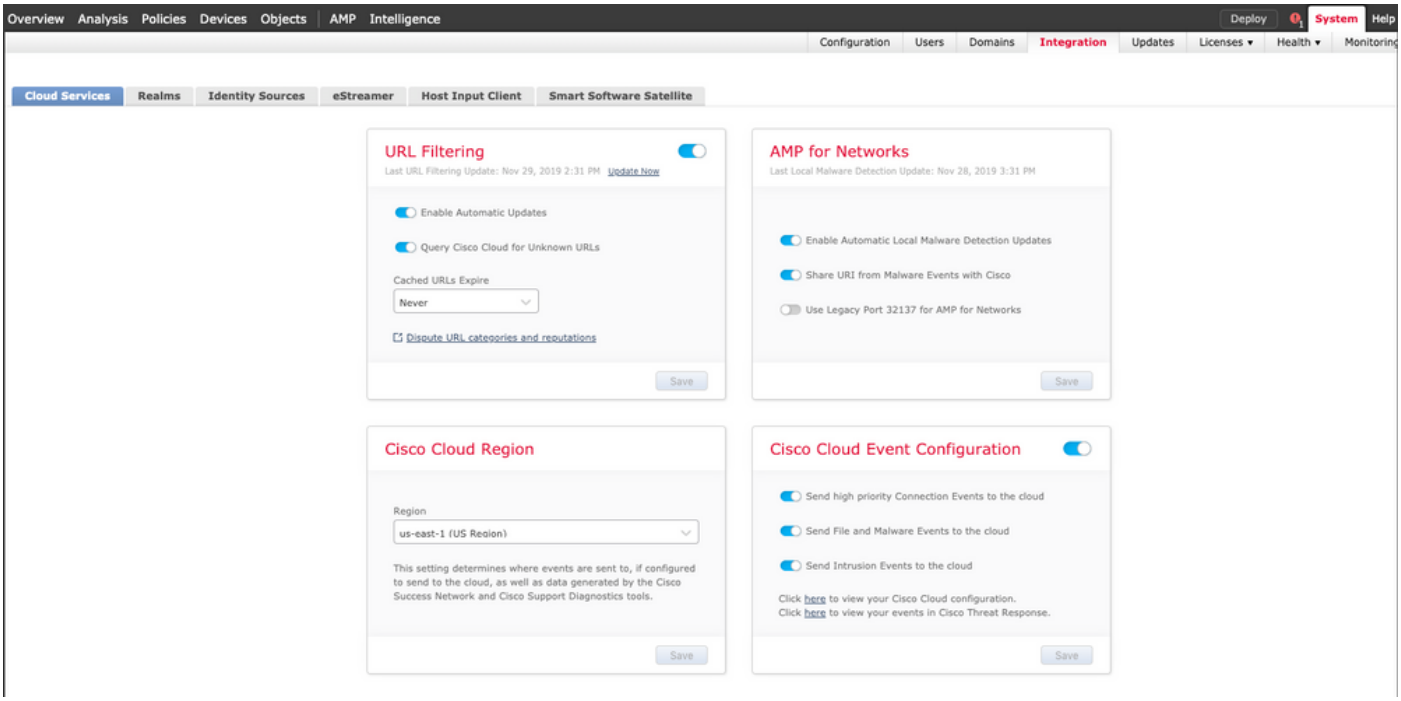
Région APJ

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

Étape 2. Connectez-vous au portail SSE à l'aide de cette URL https://admin.sse.itd.cisco.com, accédez aux **services cloud** et activez les deux options **Evant** et **Cisco SecureX pour contrer les menaces**, comme indiqué dans l'image suivante :

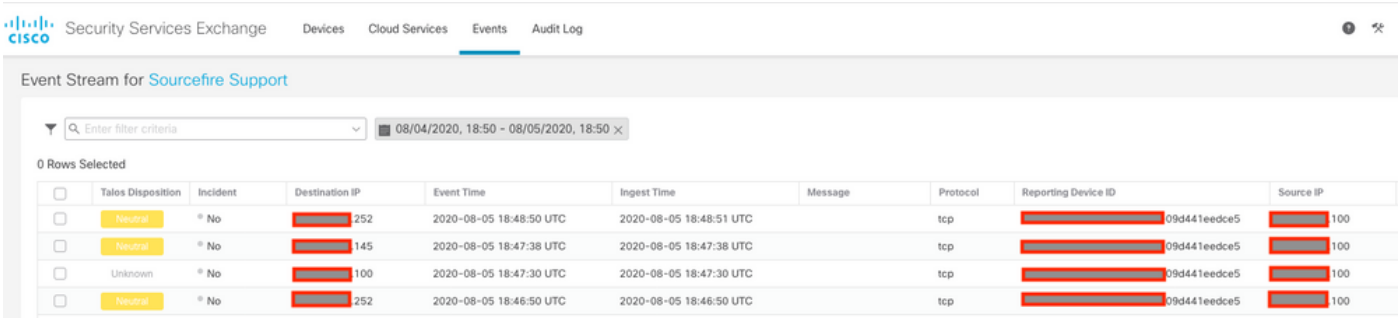


Étape 3. Connectez-vous à Firepower Management Center et accédez à **System>Integration>Cloud Services**, activez **Cisco Cloud Event Configuration** et sélectionnez les événements que vous souhaitez envoyer au cloud :



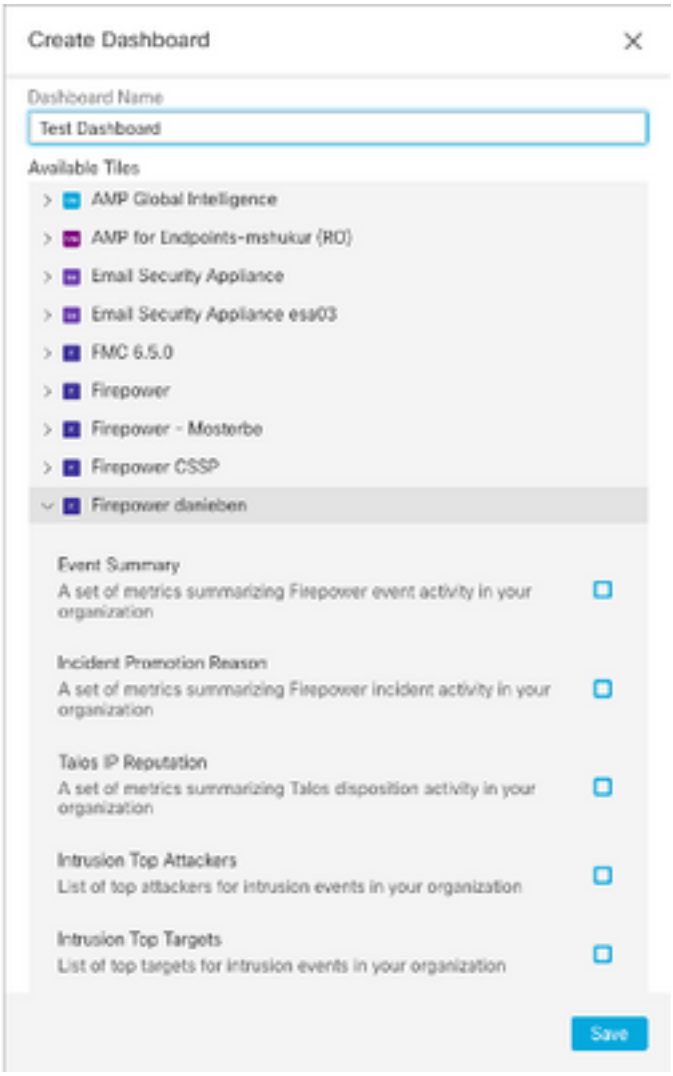
Étape 4. Vous pouvez revenir au portail SSE et valider que vous pouvez maintenant voir les périphériques inscrits sur SSE :

Les événements sont envoyés par les périphériques FTD, accédez aux **événements** sur le portail SSE pour vérifier les événements envoyés par les périphériques à SSE, comme l'illustre l'image :

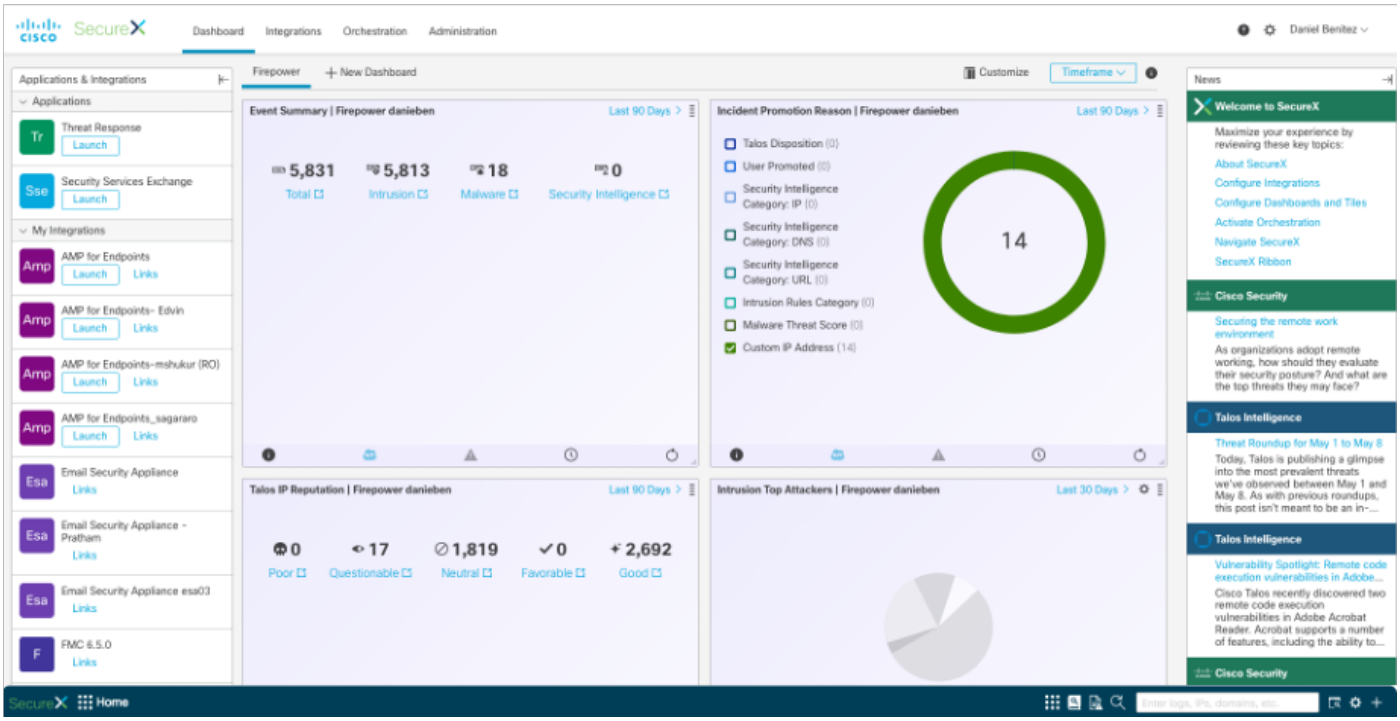


Configurer des tableaux de bord personnalisés sur SecureX

Étape 1. Pour créer votre tableau de bord, cliquez sur l'icône **+ Nouveau tableau de bord**, sélectionnez un nom et une vignette à utiliser pour le tableau de bord, comme illustré dans l'image :



Étape 2. Après cela, vous pouvez voir les informations du tableau de bord renseignées à partir de SSE, vous pouvez sélectionner l'une des menaces détectées et le portail SSE démarre avec le filtre Type d'événement :



Vérification

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

Valider les événements sont enregistrés sur le portail SSE, comme indiqué dans la section **Enregistrer les périphériques sur SSE** étape 4**.**

Vérifiez que ces informations sont affichées sur le tableau de bord SecureX ou consultez les journaux de l'API pour voir 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 de tels journaux présents dans le fichier :

```
ActionQueueScrape.pl[19094]: [SF::SSE::Enrollment] canConnect: System (/usr/bin/curl -s --
connect-timeout 10 -m 20 -L --max-redirs 5 --max-filesize 104857600 --capath
/ngfw/etc/sf/keys/fireamp/thawte_roots -f
https://api.eu.sse.itd.cisco.com/providers/sse/api/v1/regions) Failed, curl returned 28 at
/ngfw/usr/local/sf/lib/perl/5.10.1/SF/System.pmline 10477.
```

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

La sortie ci-dessus montre que le périphérique ne peut pas 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
```

La sortie ci-dessus 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, le mauvais serveur DNS a été utilisé, vous pouvez modifier les paramètres DNS à l'aide de la commande suivante :

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

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

```
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 :

curl -v https://api-sse.cisco.com/providers/sse/services/registration/api/v2/clients --cacert /ngfw/etc/ssl/connectorCA.pem
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 ignorée 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 recevez le message 403 Interdit, car les paramètres envoyés à partir du test ne correspondent pas aux attentes de SSE, mais cela se révèle suffisant pour valider la connectivité.

Vérifier l'état de 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 SSConnector et EventHandler, vous pouvez utiliser cette commande, voici un exemple de 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_SSEConnector.sock
```

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.sock
unix 3 [ ] STREAM CONNECTED 378537 7741/EventHandler
/ngfw/var/sf/run/EventHandler_SSEConnector.soc
```

Vérifier les données envoyées au portail SSE et au CTR

Pour envoyer des événements du périphérique FTD à SEE, une connexion TCP doit être établie

avec https://eventing-ingest.sse.itd.cisco.com Voici un exemple de 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.amazonaws.com:https (SYN_SENT)
```

Dans les journaux connector.log :

```
time="2020-04-13T14:34:02.88472046-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp x.x.x.246:443: getsockopt: connection timed out"
time="2020-04-13T14:38:18.244707779-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp x.x.x.234:443: getsockopt: connection timed out"
time="2020-04-13T14:42:42.564695622-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp x.x.x.246:443: getsockopt: connection timed out"
time="2020-04-13T14:47:48.484762429-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp x.x.x.234:443: getsockopt: connection timed out"
time="2020-04-13T14:52:38.404700083-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp x.x.x.234:443: getsockopt: connection timed out"
```

> **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 peuvent changer, c'est pourquoi la recommandation est d'autoriser le trafic vers le portail SSE en fonction de 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.amazonaws.com:https (ESTABLISHED)
```

Vidéo