Integración y solución de problemas de Cisco XDR con firewall seguro

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Configurar

- Licencias
- Vincule sus cuentas a SSX y registre los dispositivos.

Método 1 (integración a medias): Mejore las investigaciones

- Registre los dispositivos en SSX

Introducción

Este documento describe los pasos necesarios para integrar, verificar y solucionar problemas de Cisco XDR con Secure Firewall.

Hay dos métodos para integrar Secure Firewall y XDR, y cada integración proporciona resultados diferentes.

El primer método describe cómo integrar Secure Firewall, Security Services Exchange (SSX), Security Cloud Control, XDR-Analytics y XDR para enriquecer las investigaciones.

El segundo método describe cómo integrar Secure Firewall, SSX, Security Cloud Control, XDR-A, SAL Cloud y XDR para enriquecer los incidentes.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defence
- Virtualización opcional de imágenes
- Orquestador de defensa de Cisco
- Intercambio de servicios de seguridad
- Seguridad Control en la nube

Componentes Utilizados

- Firewall seguro: 7.2
- FirePOWER Management Center (FMC): 7,2
- Intercambio de servicios de seguridad (SSX)
- Cisco XDR
- Portal de licencias inteligentes
- Orquestador de defensa de Cisco
- Seguridad Control en la nube

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

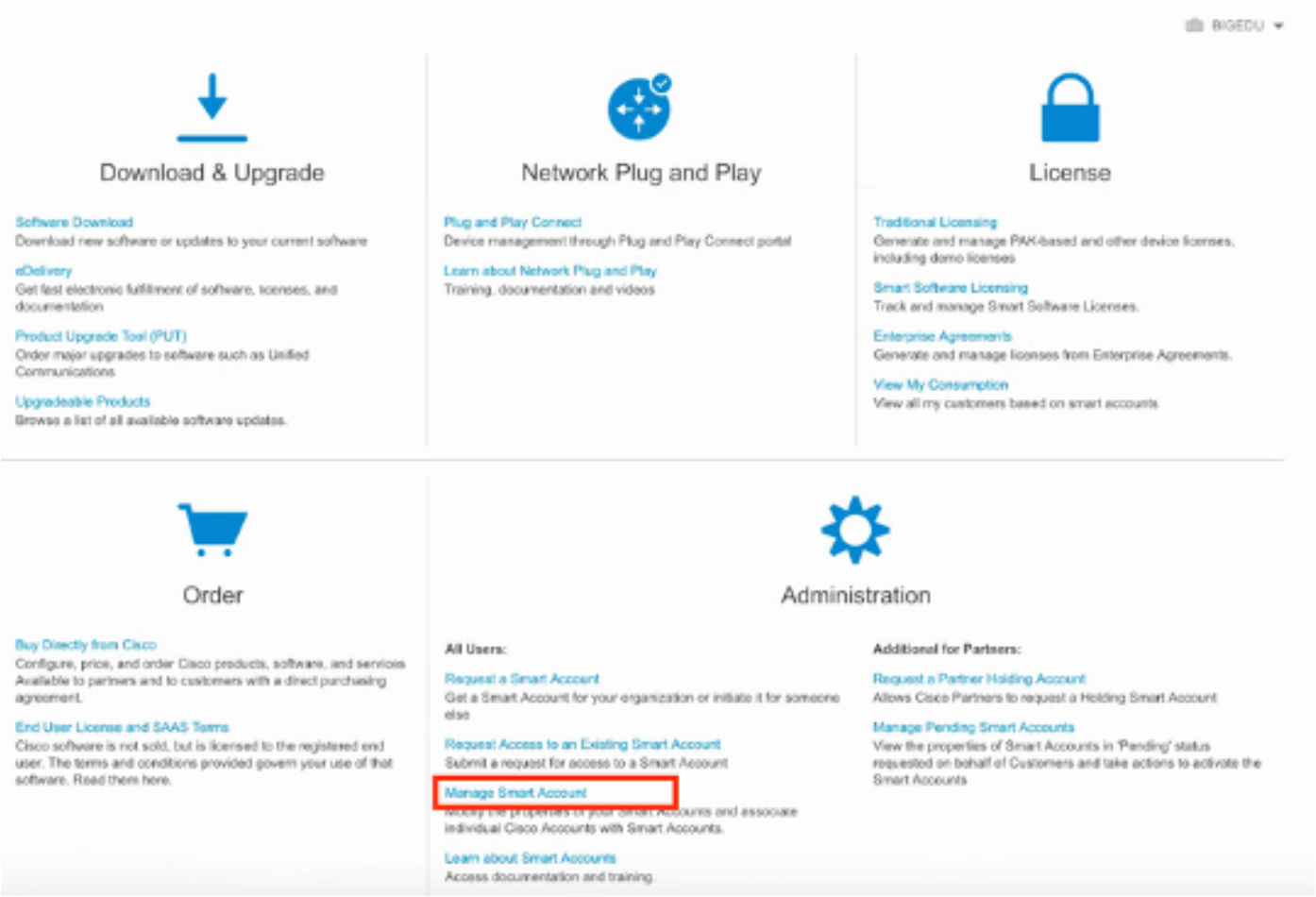
Configurar

Licencias

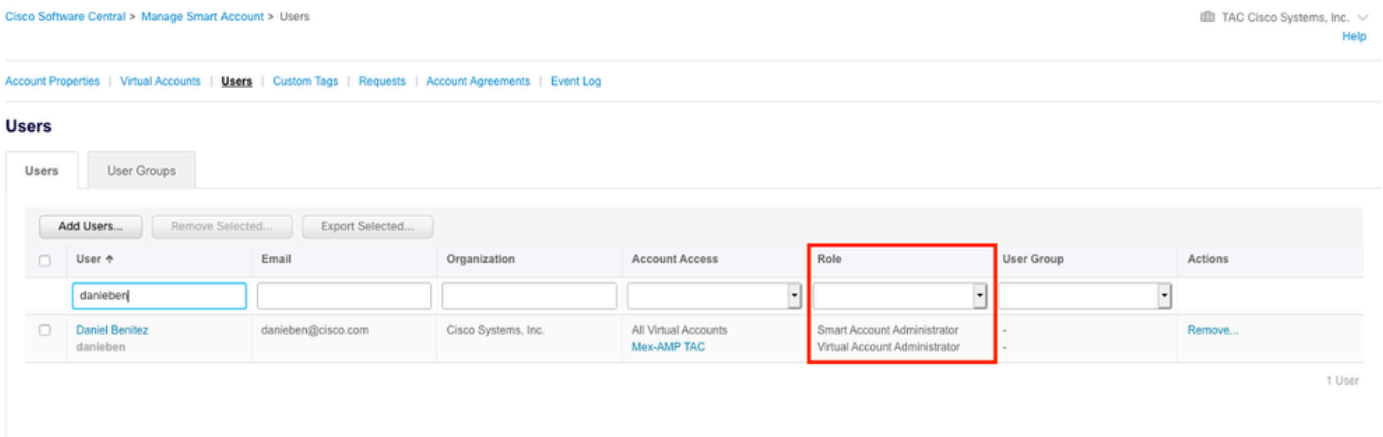
Funciones de cuenta virtual:

Solo el administrador de la cuenta virtual o el administrador de la cuenta inteligente tiene el privilegio de vincular la cuenta inteligente con la cuenta SSX.

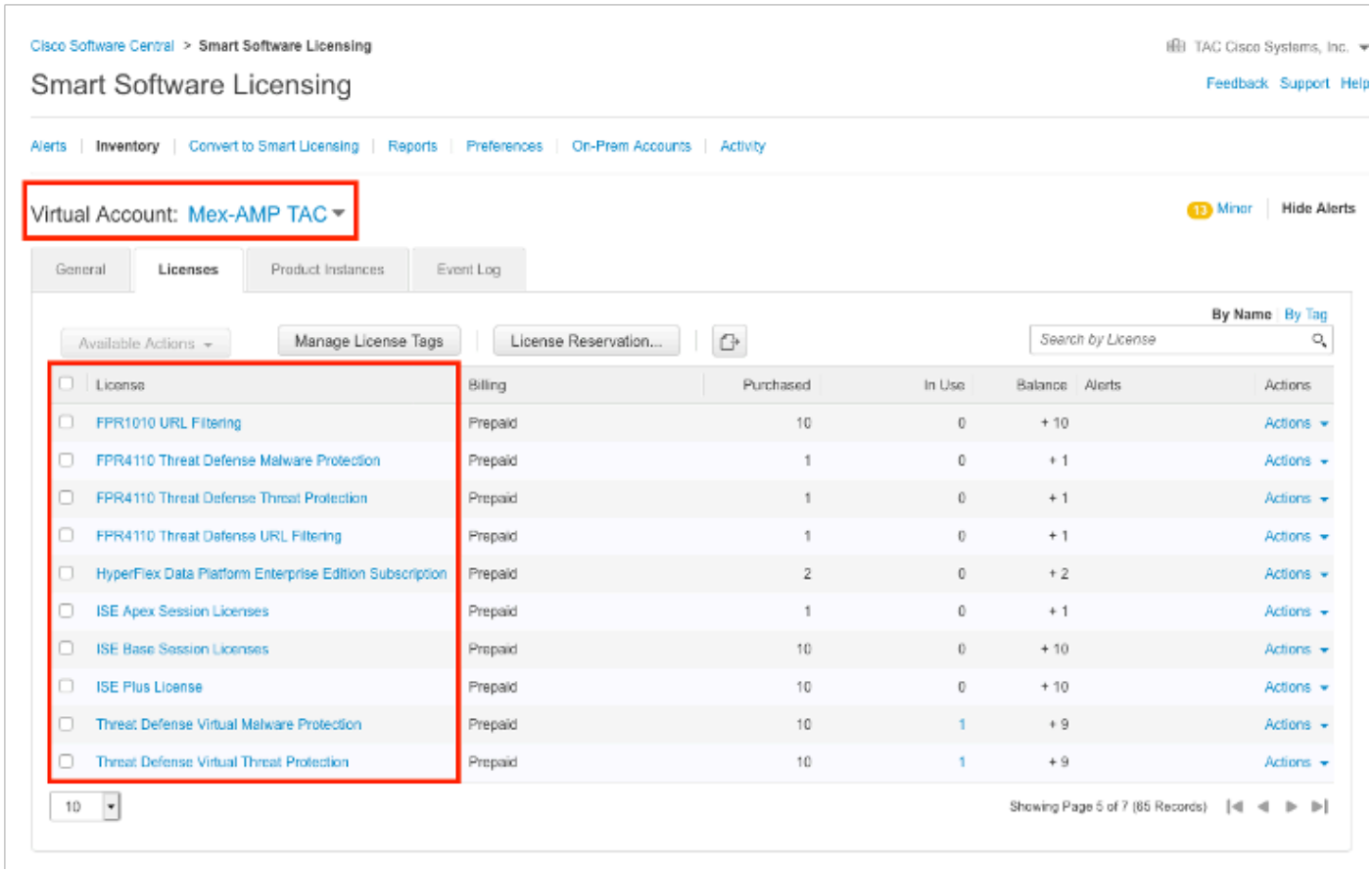
Paso 1. Para validar el rol de cuenta inteligente, navegue hasta software.cisco.com y en el Menú de administración, seleccione Administrar cuenta inteligente.



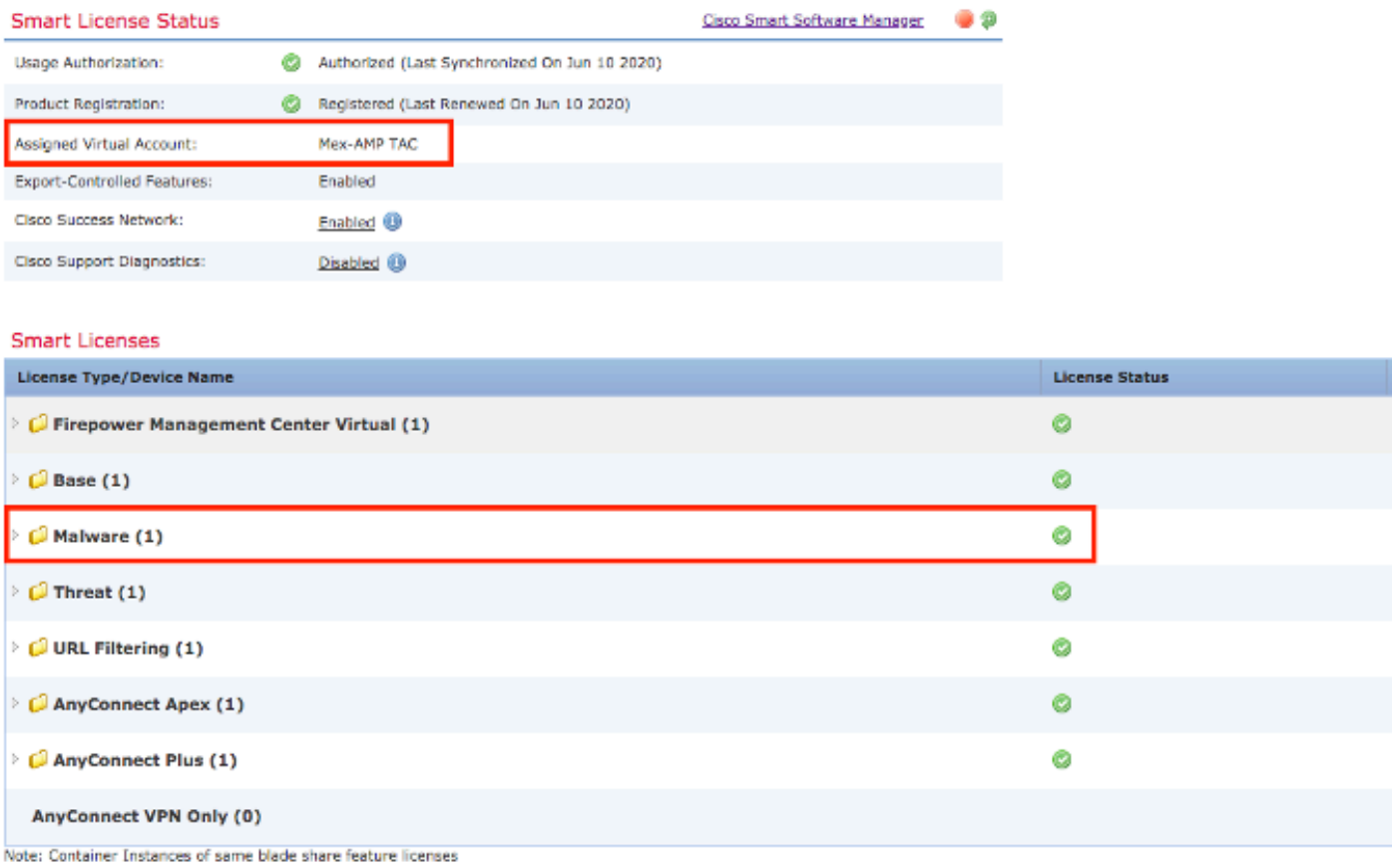
Paso 2. Para validar el rol de usuario, navegue hasta Usuarios, y valide que bajo Roles las cuentas están configuradas para tener Virtual Account Administrator, como se muestra en la imagen.



Paso 3. Asegúrese de que la cuenta virtual que se ha seleccionado para vincular en SSX contiene la licencia para los dispositivos de seguridad si una cuenta que no contiene la licencia de seguridad está vinculada en SSX, los dispositivos de seguridad y el evento no aparecen en el portal de SSX.

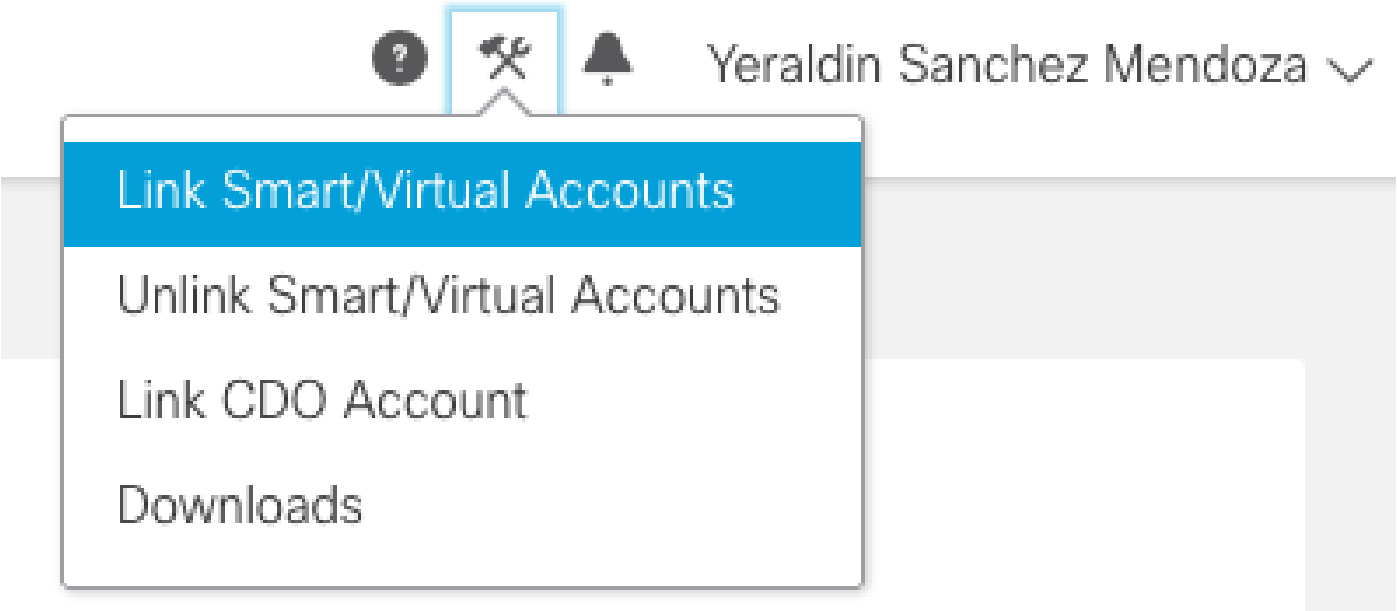


Paso 4. Para validar que el FMC se registró en la cuenta virtual correcta, navegue hasta Sistema > Licencias > Licencia inteligente:



Vincule sus cuentas a SSX y registre los dispositivos.

Paso 1. Cuando inicie sesión en su cuenta de SSX, tiene que vincular su cuenta inteligente a su cuenta de SSX, para eso debe hacer clic en el icono de herramientas y seleccionar Vincular cuentas inteligentes / virtuales.



Una vez vinculada la cuenta, verá la cuenta inteligente con todas las cuentas virtuales.

Método 1 (integración a medias): Mejore las investigaciones

Registre los dispositivos en SSX

Paso 1. Asegúrese de que estas URL estén permitidas en su entorno:

Región de Estados Unidos

- 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

Región 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

Región 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

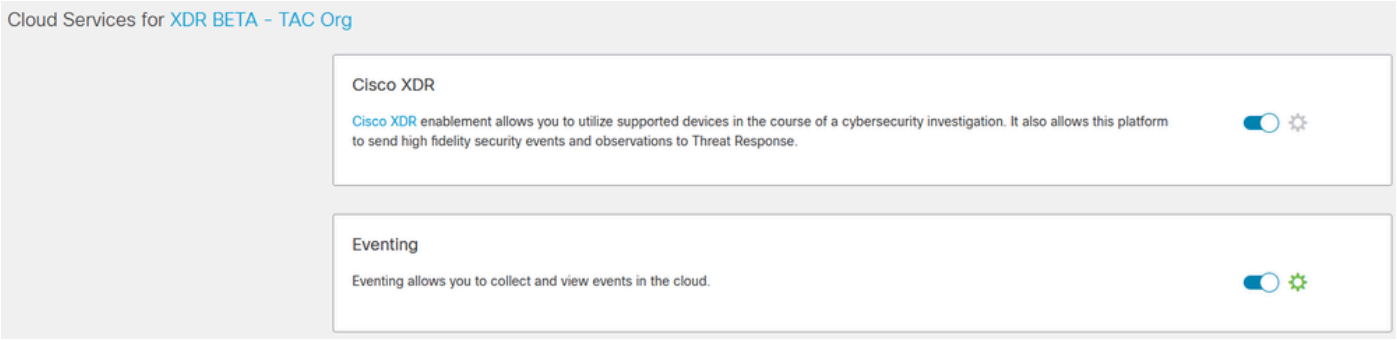
Región de Australia:

- 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

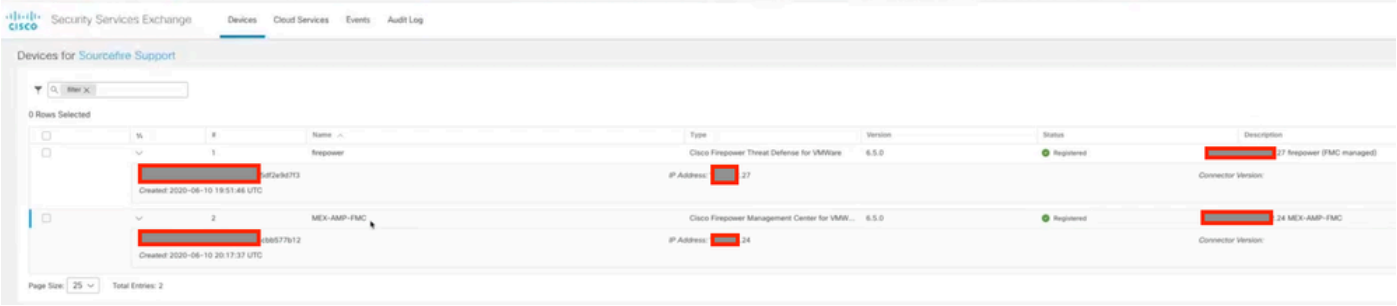
Región de la India:

- 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

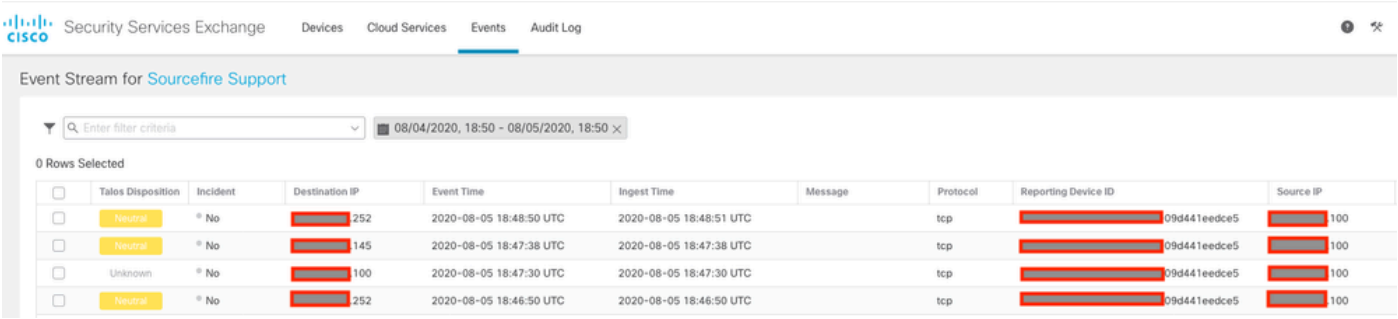
Paso 2. Inicie sesión en el portal de SSX con esta URL https://admin.sse.itd.cisco.com, navegue hasta Cloud Services y habilite ambas opciones Cisco XDR y Eventing, como se muestra en la imagen.



Paso 3. Puede validar que ahora puede ver los dispositivos inscritos en SSX:



Los eventos son enviados por los dispositivos Secure Firewall, navegue hasta Events en el portal SSX para verificar los eventos enviados por los dispositivos a SSX, como se muestra en la imagen.



Registre los dispositivos en Security Cloud Control (SCC/CDO)

Paso 1. Asegúrese de que estas URL estén permitidas en su entorno

Región de EE. UU.

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

Región UE

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

Región APJC

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

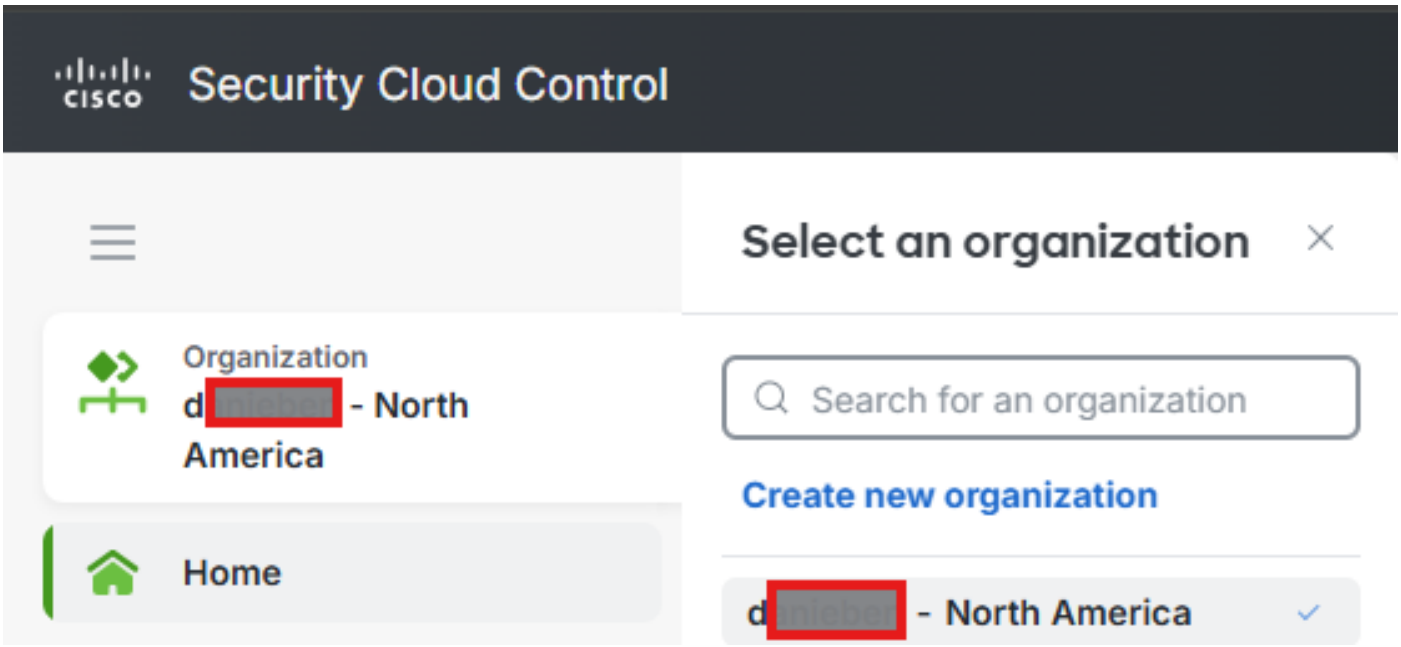
Región de Australia:

- aus.cdo.cisco.com

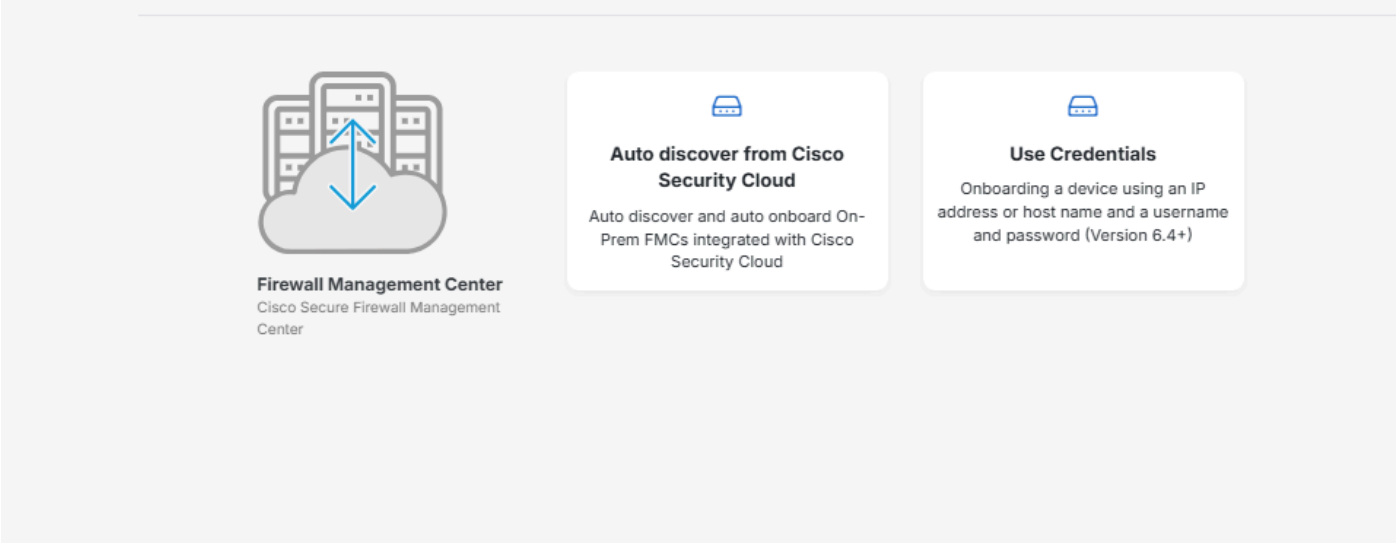
Región de la India:

- in.cdo.cisco.com

Paso 2. Navegue hasta Security Cloud Control (el enlace puede variar según su región). Esto le indica que seleccione su organización de control de la nube de seguridad.



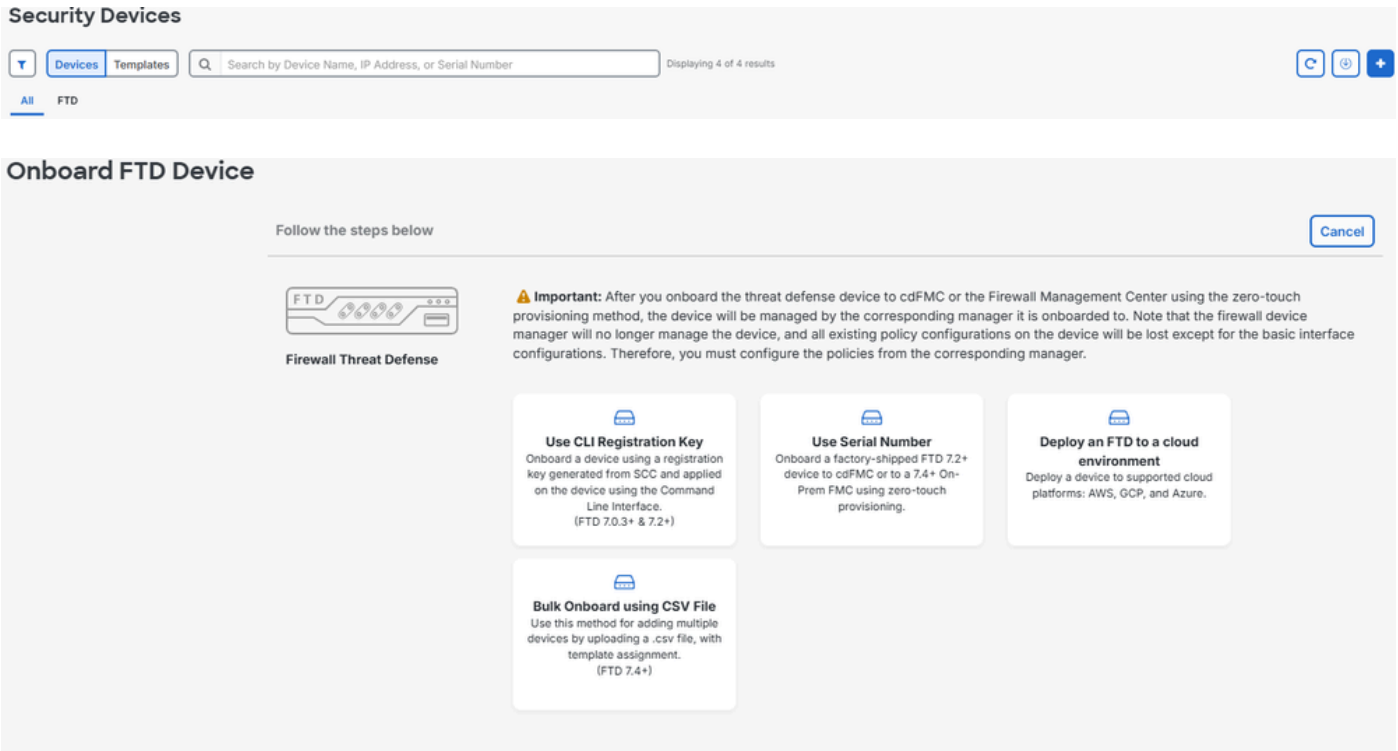
Paso 3. Una vez que haya seleccionado la organización adecuada, navegue hasta Productos > Firewall, verifique si su dispositivo ya está allí, si no, puede Incorporarlo a Control de nube de seguridad (Cisco Defense Orchestrator), para esto, en Inventario general, haga clic en Ver todos los dispositivos.



Paso 4. Navegue hasta Administration > Firewall Management Center, se presenta una lista de sus FMCs integrados en SCC, si no ve su Firewall Management Center, haga clic en el icono más.

Paso 4.1. Normalmente, los firewalls seguros se incorporan automáticamente; de lo contrario, seleccione el dispositivo que desea incorporar (FTD) y el método de incorporación que prefiera.

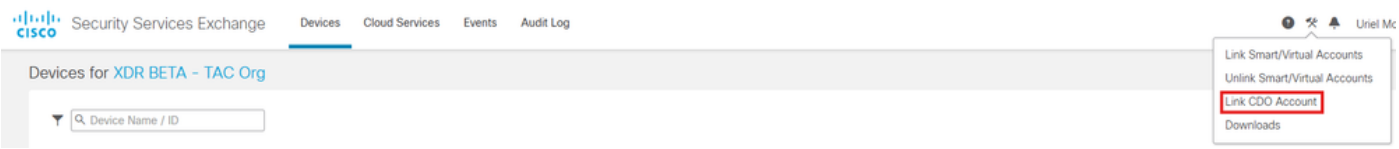
Paso 4.2. En la sección Security Devices (Dispositivos de seguridad), haga clic en el icono más, seleccione Onboard Secure Firewall Device y su



Paso 5. Una vez que haya incorporado sus dispositivos en Security Cloud Control, puede visualizarlos en el inventario.

Paso 6. Asegúrese de que su organización CDO está vinculada a su organización SSX. Para ello, navegue hasta Intercambio de servicios de seguridad, haga clic en el icono del menú

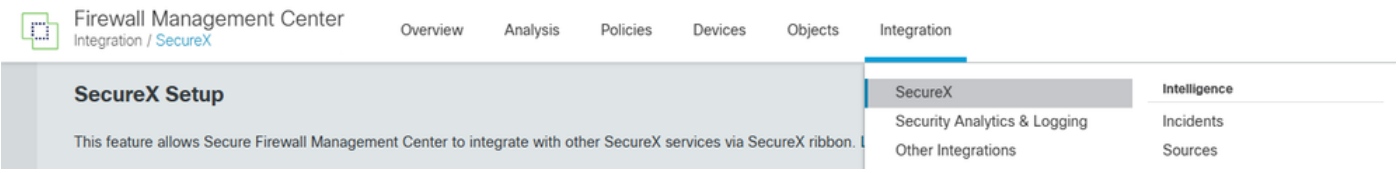
Herramientas y, a continuación, haga clic en Vincular cuenta CDO.



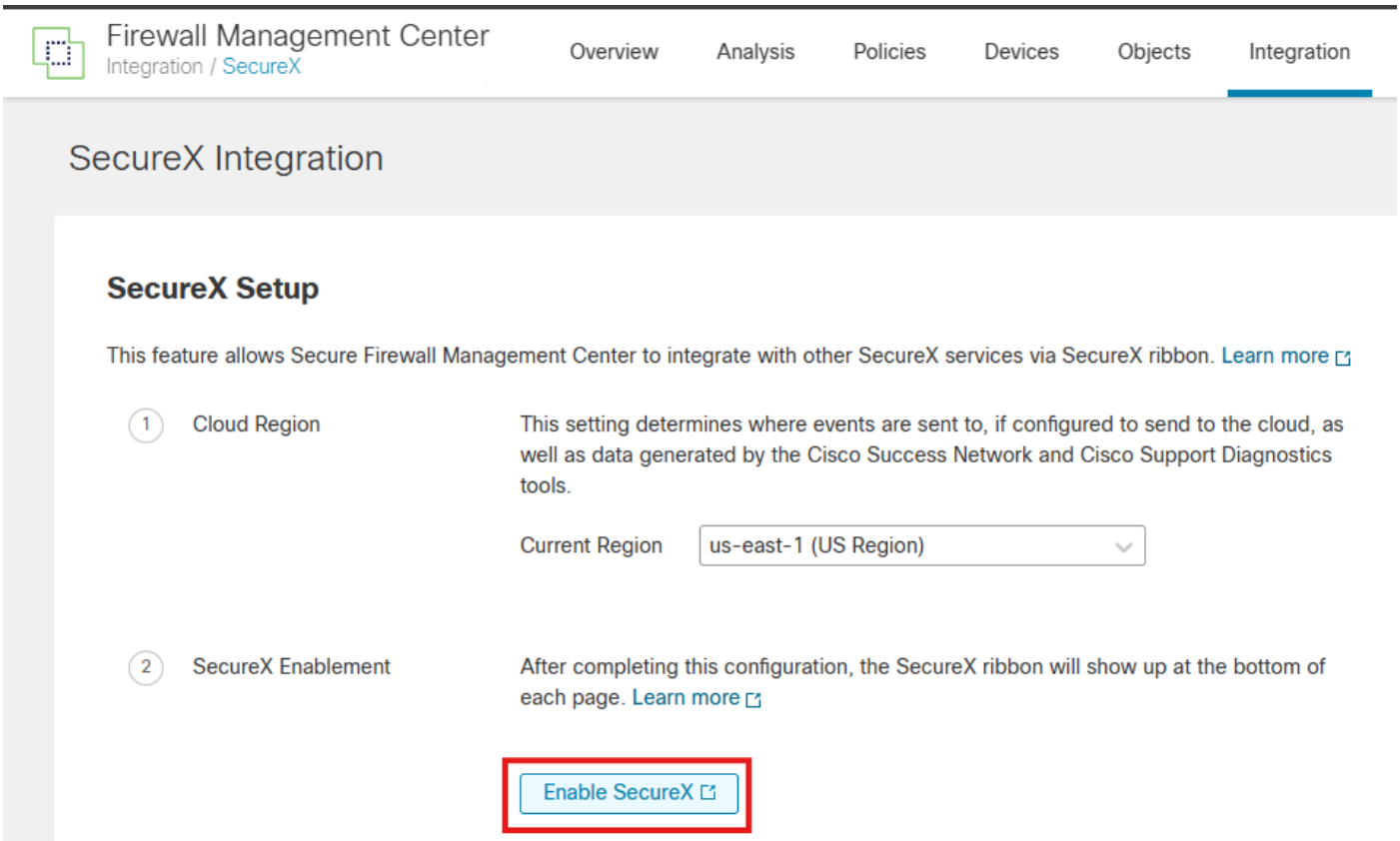
Integre un firewall seguro

De 7.2.x a 7.4.x con Cisco XDR

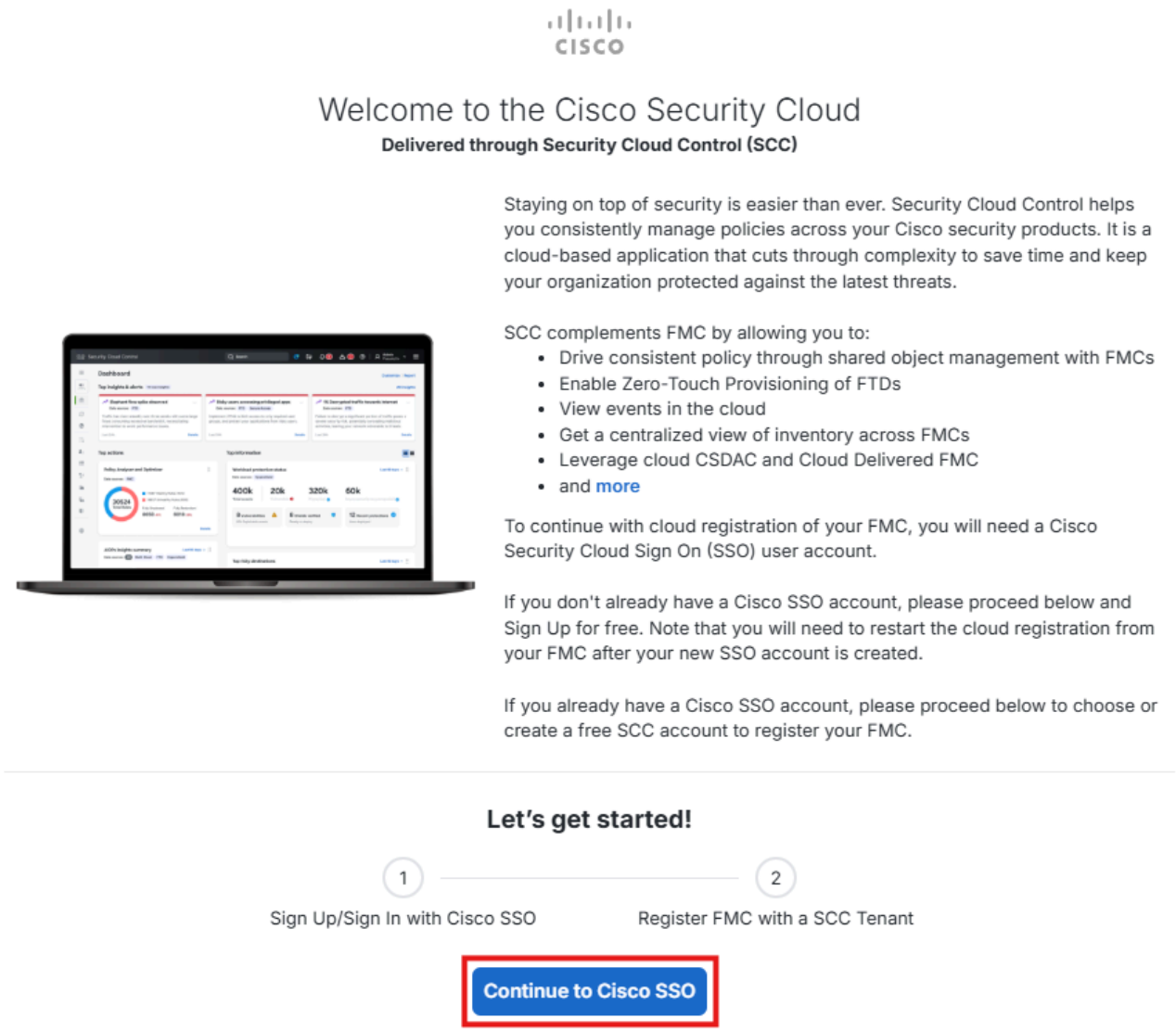
Paso 1. En Secure Firewall Management Center, navegue hasta Integración > SecureX



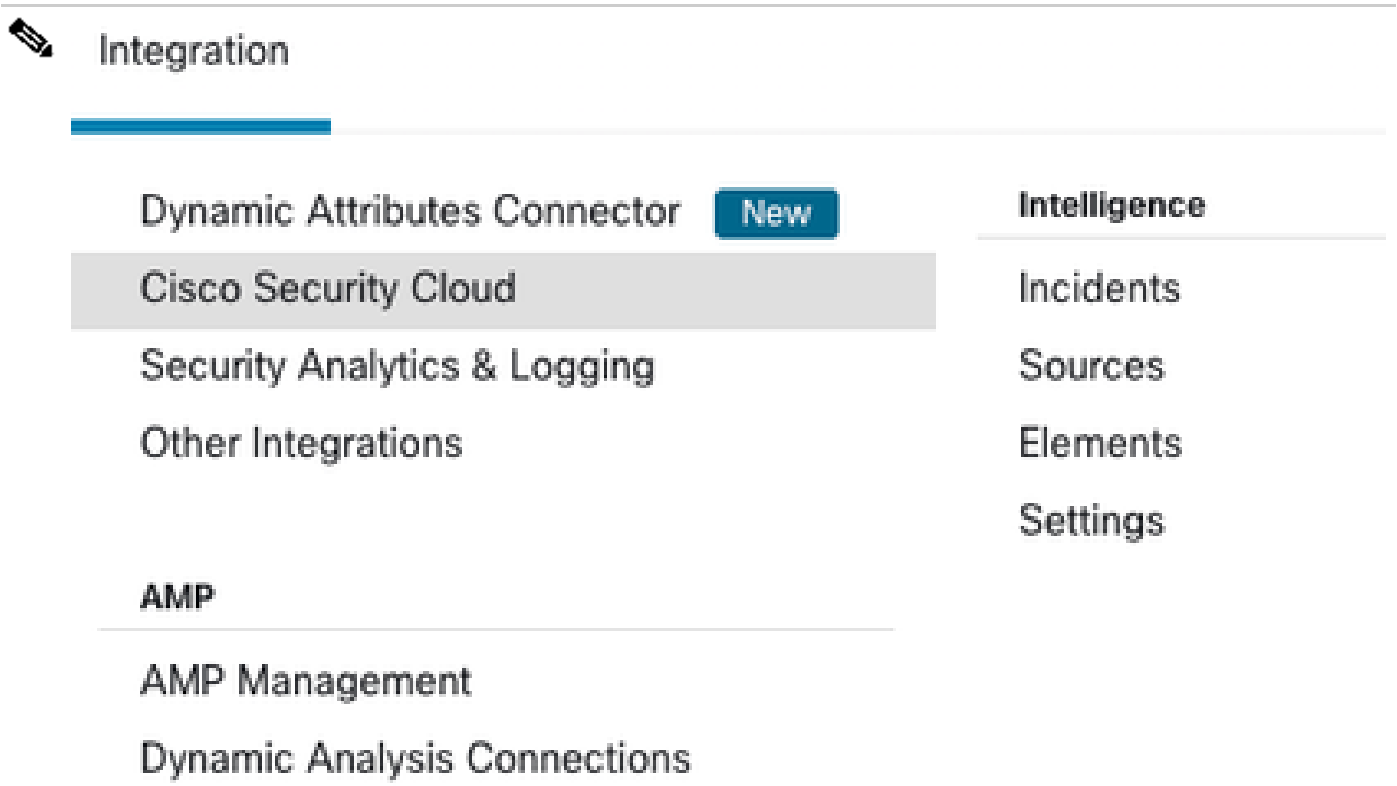
Paso 2. Elija la región correcta y haga clic en Habilitar SecureX.



Paso 3. Después de hacer clic en Activar SecureX, se le redirige a la página de autenticación de Cisco Defense Orchestrator (que aprovecha el inicio de sesión en la nube de seguridad), haga clic en Continuar con Cisco SSO.



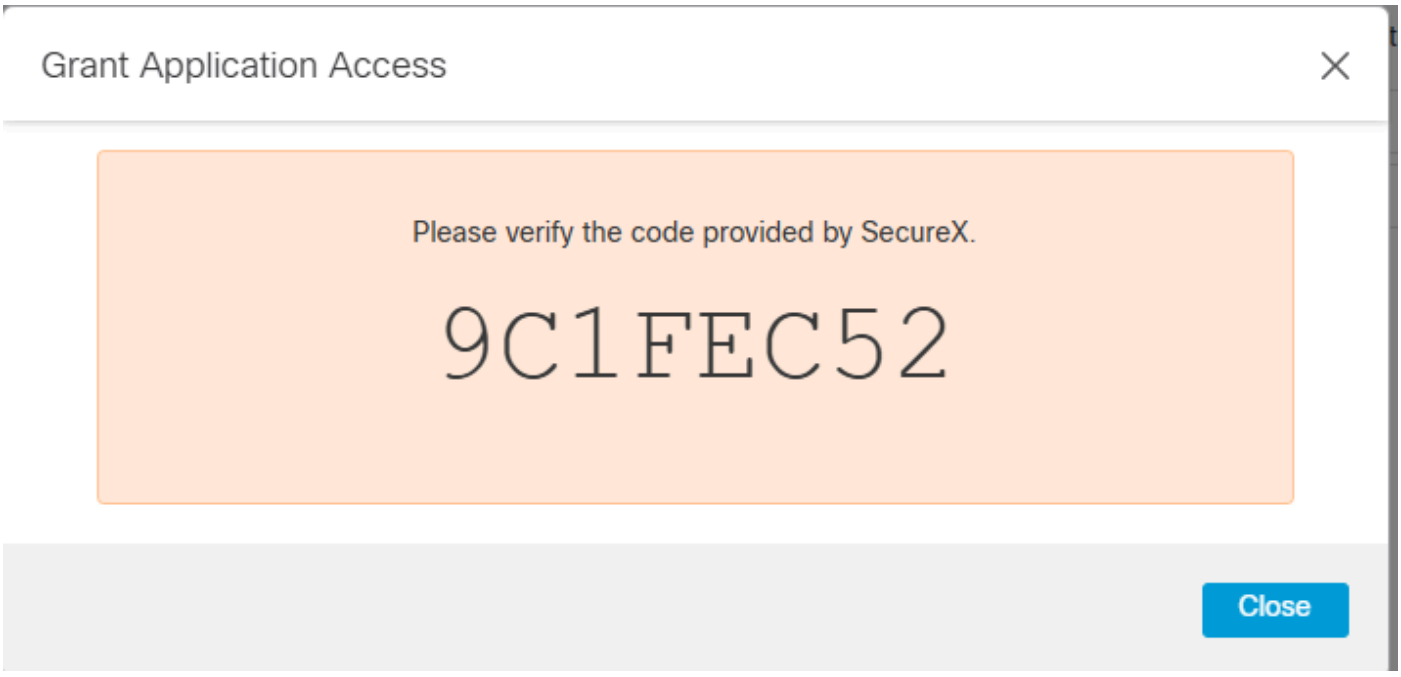
Nota:
A partir de la versión 7.6.x y posteriores con Cisco XDR
Paso 1. En el Secure Firewall Management Center, navegue hasta Integración > Cisco Security Cloud

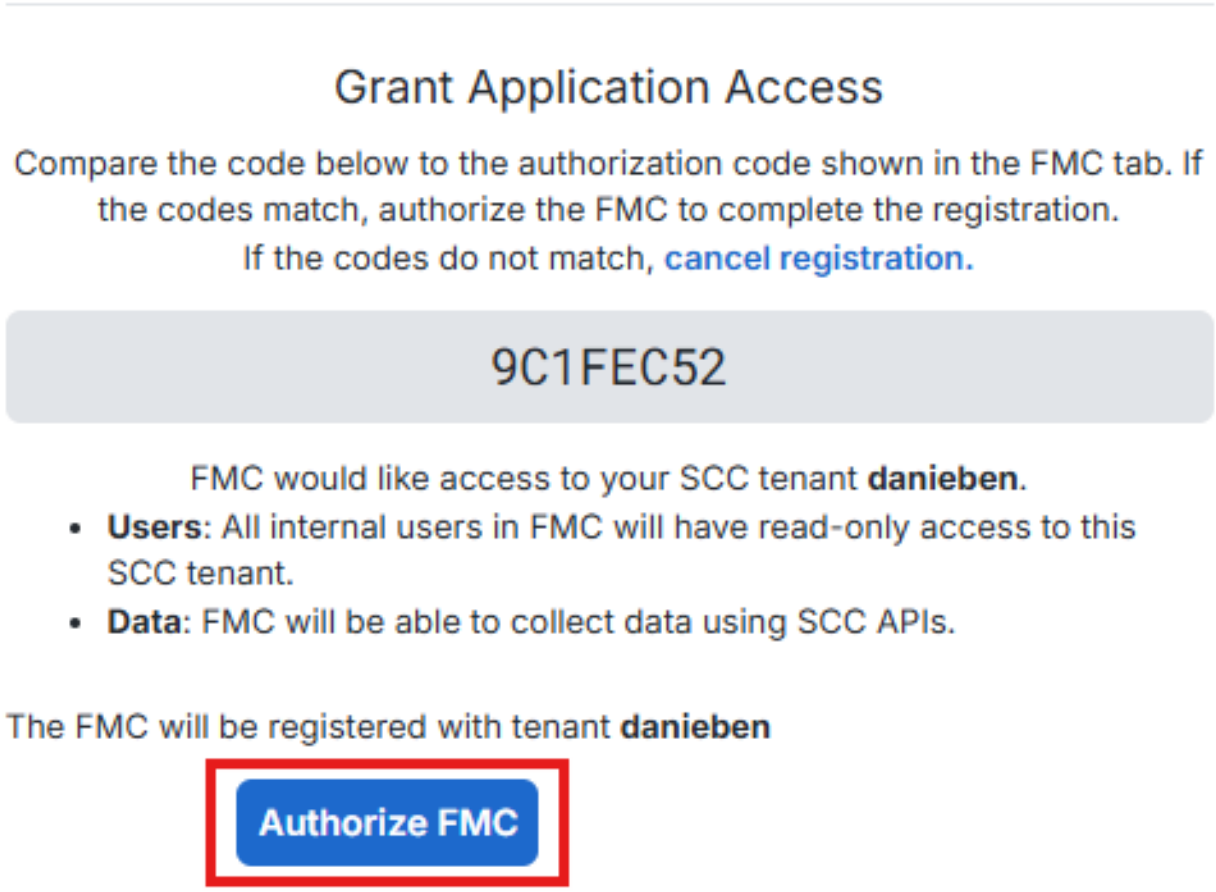


Paso 2. Elija la región correcta y haga clic en Habilitar Cisco Security Cloud.
Paso 3. Después de hacer clic en Activar Cisco Security Cloud, le redirige a la página de autenticación de Cisco Defense Orchestrator (que aprovecha el inicio de sesión de Security Cloud), haga clic en Continuar con Cisco SSO.

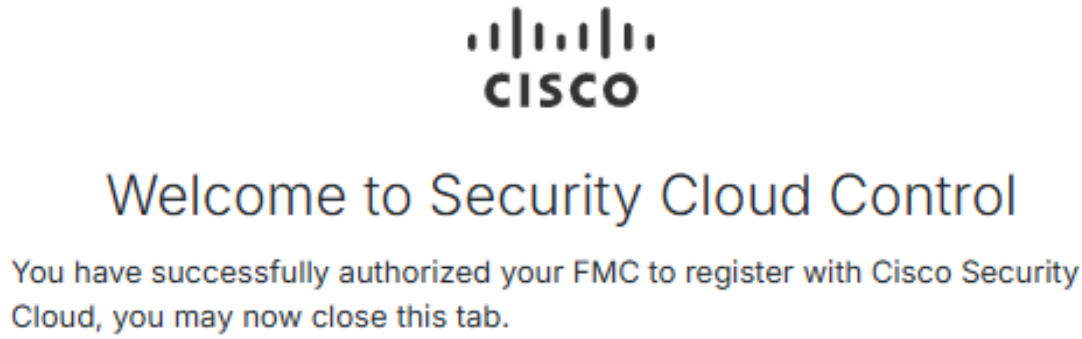
Paso 4. Puede seleccionar un arrendatario de control de la nube de seguridad existente o crear uno nuevo.

Paso 5. Seleccione el arrendatario adecuado y asegúrese de que el código que recibe en esta página coincide con el código que recibe en FMC. Si coinciden, haga clic en Autorizar FMC.



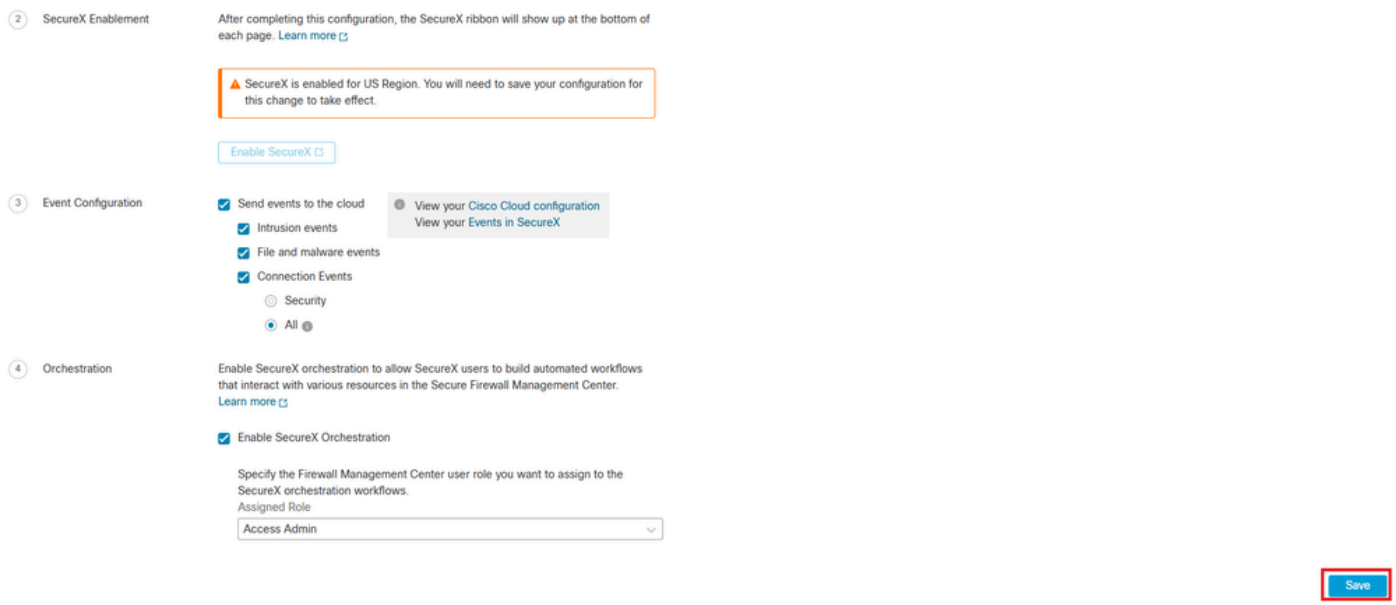


Paso 6. Introduzca sus credenciales de inicio de sesión en la nube de seguridad y autorice la integración. Una vez completada, se presenta una confirmación de que FMC está autorizado a registrarse en Cisco Security Cloud.



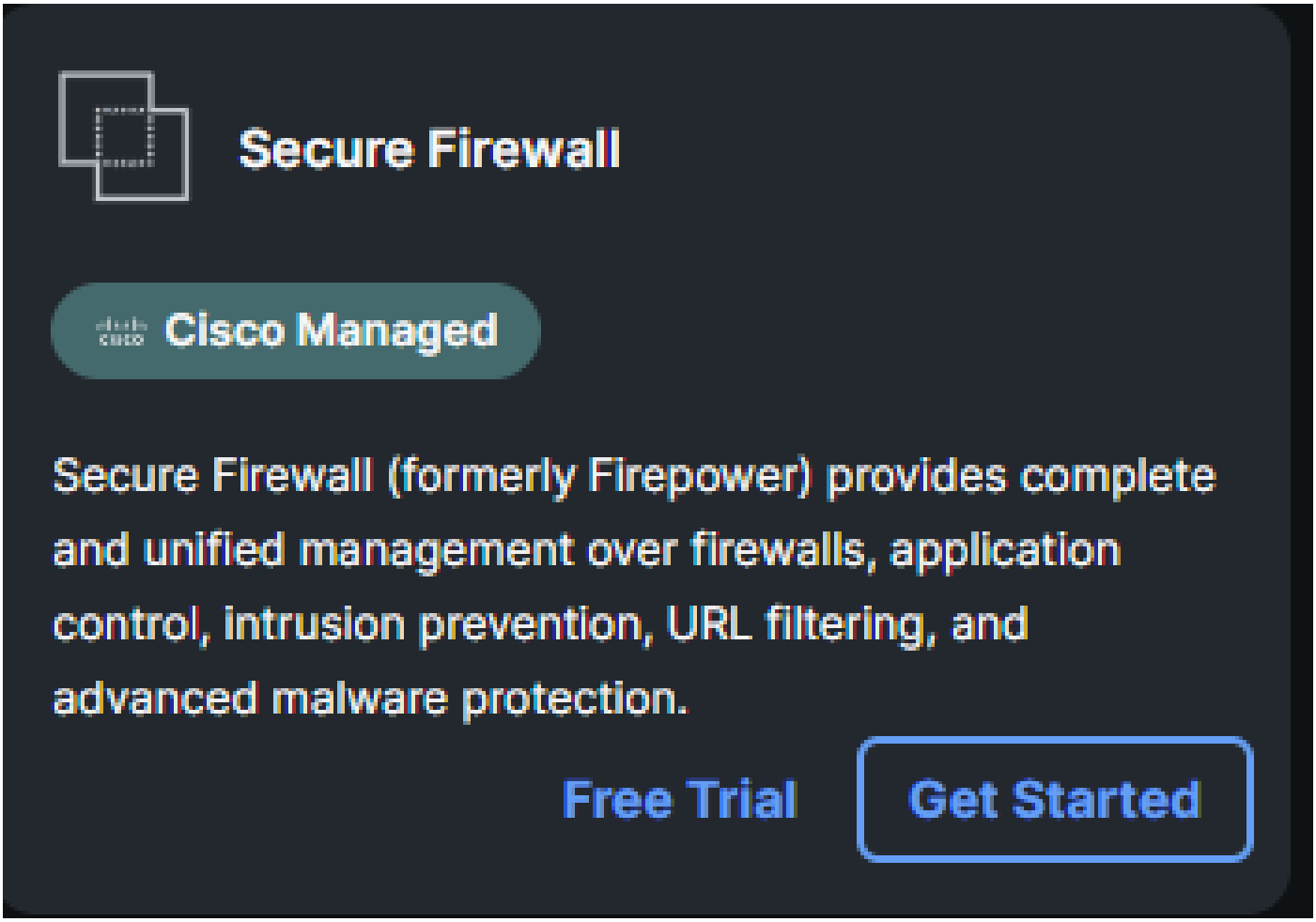
Paso 7. Una vez completada la autorización, puede volver a su FMC, seleccionar los eventos que desea enviar a la nube y, una vez finalizado, hacer clic en Guardar.

Paso 8. Puede seleccionar Habilitar SecureX Orchestration (XDR Automate)

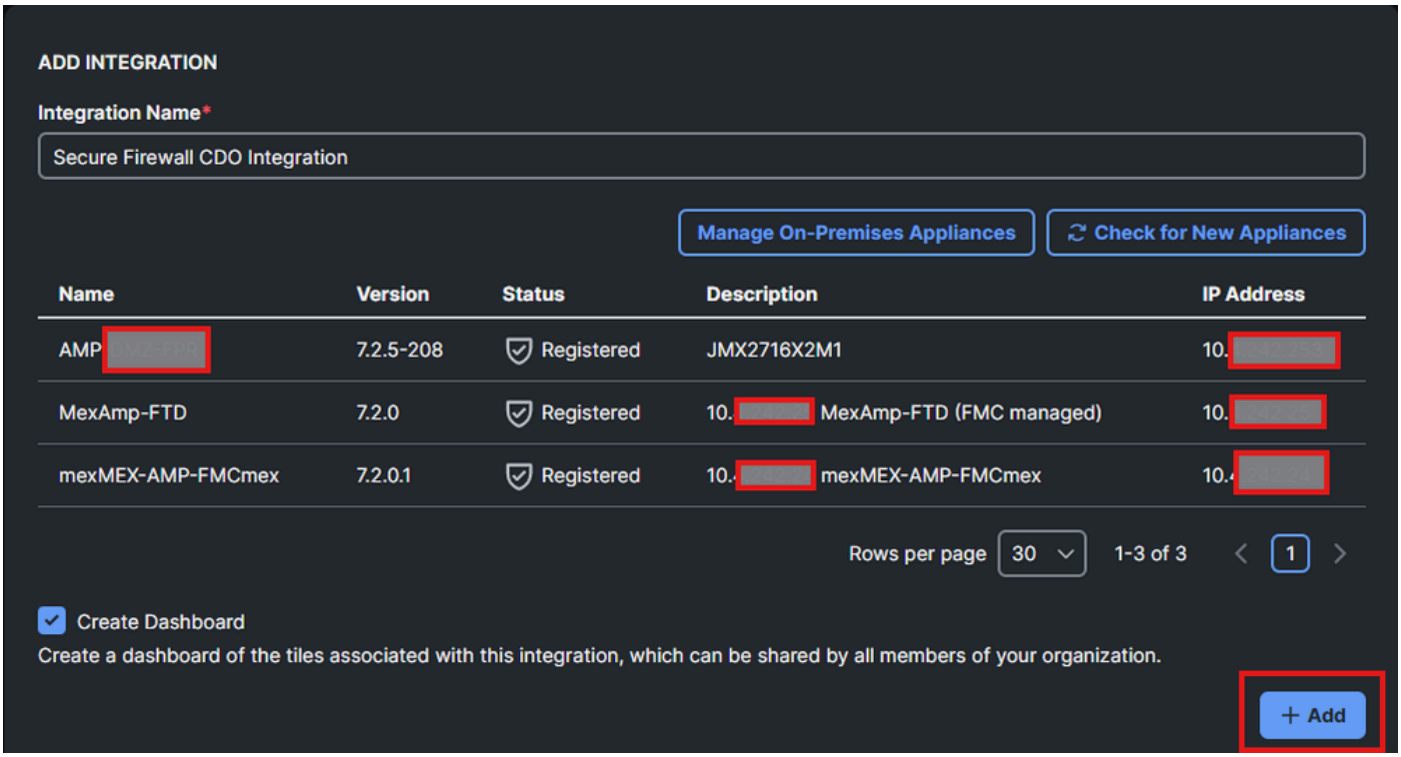


Paso 9. Navegue hasta XDR > Administration > On Premises Appliance y busque sus dispositivos, los cuales deben registrarse automáticamente.

Paso 10. Navegue hasta XDR > Administración > Integraciones y habilite la integración de firewall seguro.



Paso 10.1. Asigne un nombre a su integración, haga clic en +Agregar.



Esta integración permite enriquecer las investigaciones en XDR.

Método 2 (integración completa): Enriquecer los incidentes en XDR

Nota: Para garantizar una integración perfecta entre Secure Firewall, XDR, Cisco Defense Orchestrator (CDO), Security Services Exchange (SSX) y Security Analytics and Logging (SAL), se requiere la asignación manual. Este proceso implica ponerse en contacto con el TAC de Cisco para realizar las configuraciones y asignaciones necesarias.

Paso 1. Su cuenta de CDO debe tener una licencia de Security Analytics and Logging para reenviar eventos a Cisco XDR.

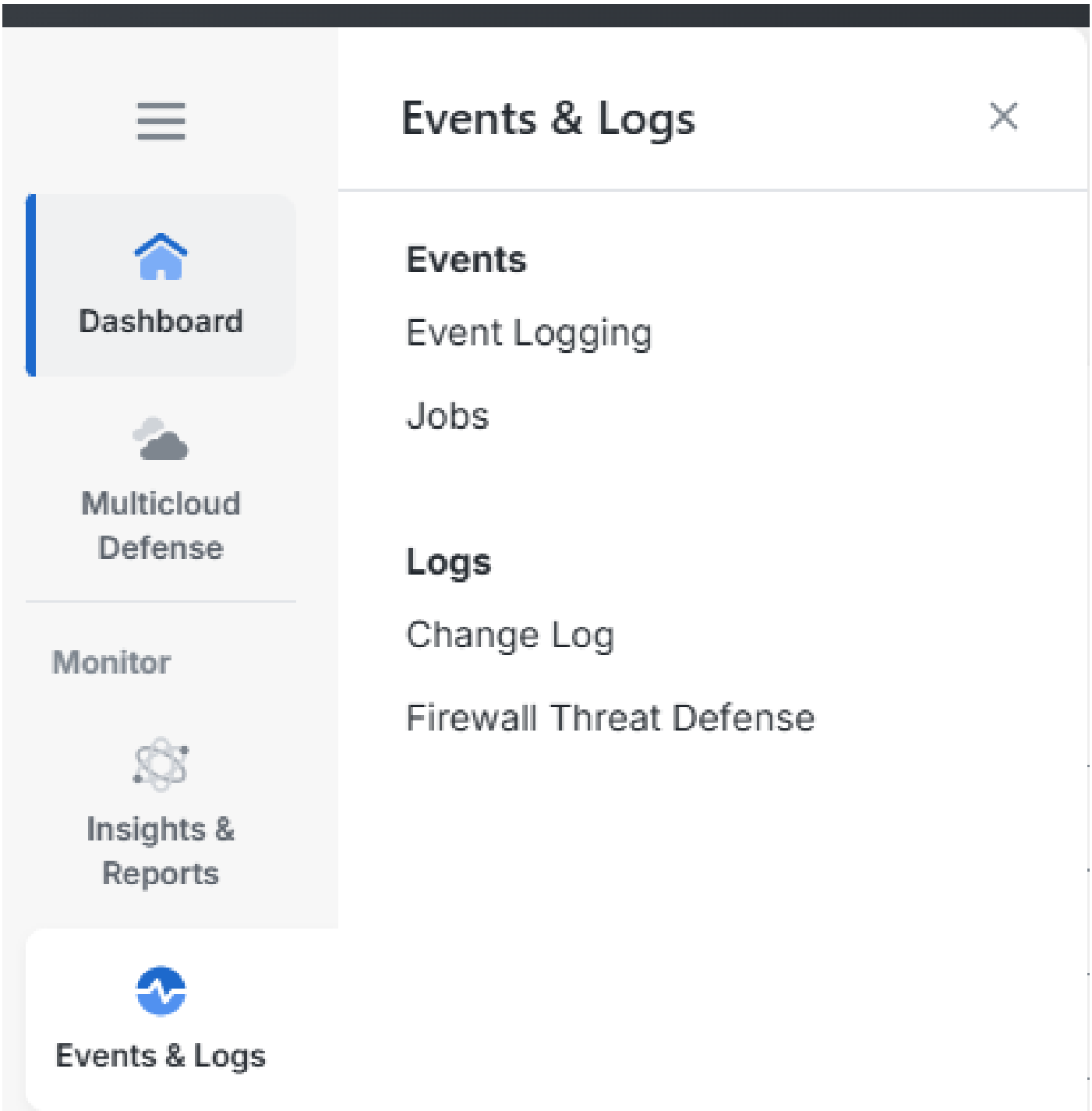
Paso 2. Siga los pasos descritos anteriormente para registrar sus dispositivos en SSX y Security Cloud Control.

Paso 3. Una vez que haya terminado, póngase en contacto con el TAC con estos detalles y solicite vincular Security Cloud Control/SAL a XDR Analytics.

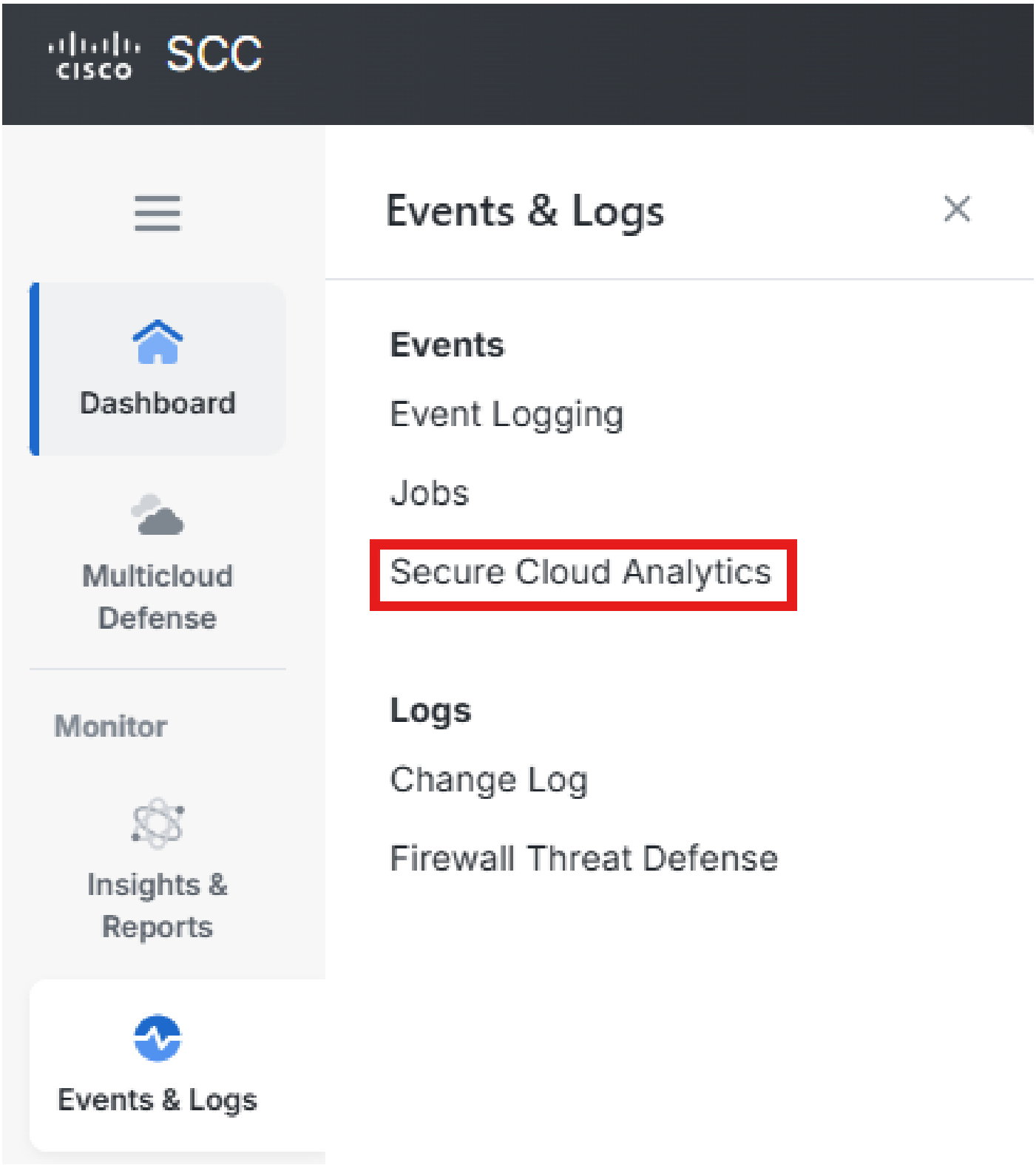
- ID de arrendatario de CDO
- Nombre de CDO
- ID de organización XDR
- ID de arrendatario de SSX
- Nombre de SSX
- ID de organización de SCA

Paso 4. Asegúrese de que su cuenta de CDO está vinculada al portal de análisis XDR.

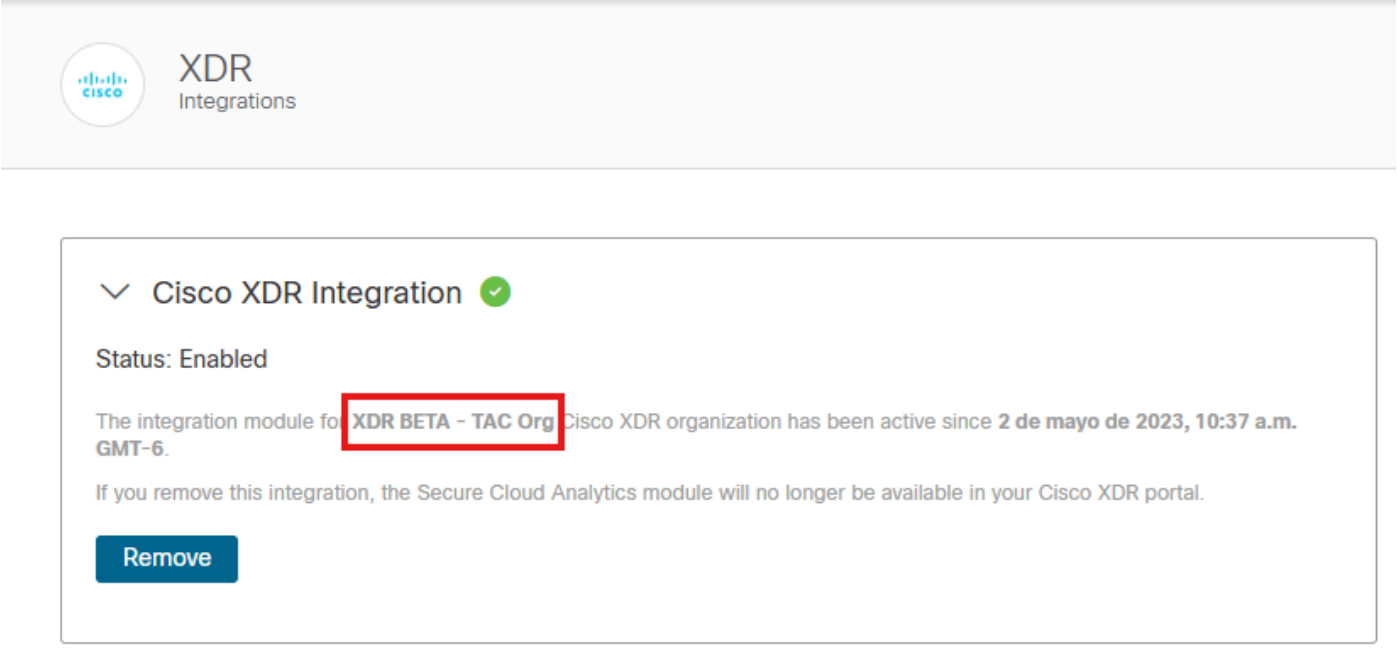
Antes de vincular el portal de CDO a XDR Analytics, el aspecto es el siguiente:



Una vez finalizado el enlace, puede ver la opción para desplazarse hasta el portal de análisis de XDR.



Paso 5. Una vez que su cuenta de XDR Analytics esté vinculada a su Security Cloud Control Portal (CDO), debe asegurarse de que el análisis de XDR está integrado con XDR. Para ello, en Análisis de XDR, vaya a Configuración > Integraciones > XDR, busque Integración de XDR y asegúrese de que haya una marca de verificación verde y de que el módulo de integración apunte a su organización XDR correcta.



Verificación

Valide que los firewalls seguros generan eventos (malware o intrusión) para que los eventos de intrusión accedan a Análisis >Archivos >Eventos de malware; para eventos de intrusión, vaya a Análisis > Intrusión > Eventos.

Valide que los eventos están registrados en el portal SSX como se menciona en el paso 4 de la sección Registro de los dispositivos en SSX.

Valide que se muestre la información en el panel de Cisco XDR o compruebe los registros de la API para ver el motivo de un posible fallo de la API.

Valide que todos los arrendatarios estén correctamente vinculados entre sí. Si tiene problemas, abra un caso TAC y proporcione estos detalles:

- ID de arrendatario de CDO
- Nombre de CDO
- ID de organización XDR
- ID de arrendatario de SSX
- Nombre de SSX
- ID de organización de SCA

Troubleshoot

Detectar problemas de conectividad

Puede detectar problemas de conectividad genéricos desde el archivo action_queue.log. En caso de fallo, podrá ver los registros presentes en el archivo:

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

En este caso, el código de salida 28 significa que la operación ha agotado el tiempo de espera y debemos verificar la conectividad a Internet. También debe ver el código de salida 6, que significa problemas con la resolución de DNS

Problemas de conectividad debido a la resolución de DNS

Paso 1. Compruebe que la conectividad funciona correctamente.

```
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'
```

Este resultado muestra que el dispositivo no puede resolver la URL https://api-sse.cisco.com, en este caso, necesitamos validar que el servidor DNS correcto está configurado, se puede validar con una nslookup de la CLI experta:

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

Este resultado muestra que no se alcanza el DNS configurado, para confirmar la configuración de DNS, utilice el comando 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
```

En este ejemplo se utilizó un servidor DNS incorrecto, puede cambiar la configuración DNS con este comando:

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

Después de que esta conectividad se pueda probar de nuevo y esta vez, la conexión se realiza correctamente.

```
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;
```

Problemas de registro en el portal SSX

Tanto FMC como Secure Firewall necesitan una conexión a las URL SSX en su interfaz de administración. Para probar la conexión, introduzca estos comandos en la CLI de Firepower con acceso raíz:

<#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 verificación de certificados se puede omitir con este comando:

```
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;
```

Nota: Recibirá el mensaje 403 Forbidden ya que los parámetros enviados desde la prueba no son los que SSX espera, pero esto demuestra ser suficiente para validar la conectividad.

Verificar el estado del conector

Puede comprobar las propiedades del conector tal y como se muestra.

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

Para verificar la conectividad entre SSConnector y EventHandler puede utilizar este comando, este es un ejemplo de una conexión defectuosa:

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

En el ejemplo de una conexión establecida, puede ver que el estado de la secuencia es conectado:

```
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
```

Verificar los datos enviados al portal SSX y al CTR

Para enviar eventos desde el dispositivo Secure Firewall a SSX, es necesario establecer una conexión TCP con https://eventing-ingest.sse.itd.cisco.com Este es un ejemplo de una conexión no establecida entre el portal SSX y el 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
```

En los registros de 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
```

Nota: Se ha observado que las direcciones IP mostradas x.x.x.246 y 1x.x.x.246 pertenecen a https://eventing-ingest.sse.itd.cisco.com deben cambiar, por lo que se recomienda permitir el tráfico al portal SSX basado en URL en lugar de direcciones IP.

Si no se establece esta conexión, los eventos no se envían al portal SSX. Este es un ejemplo de una conexión establecida entre el Secure Firewall y el portal 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.
```

El dispositivo (FTD) no se puede inscribir en el control de seguridad en la nube

Si su dispositivo no se puede inscribir en el control de la nube de seguridad, asegúrese de que tiene conectividad con el arrendatario CDO adecuado.

Para verificar la URL correcta, navegue hasta Administration > Firewall Management Center, seleccione Cloud Delivered FMC, en la parte superior derecha de la pantalla puede ver el nombre de host.

```
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 todavía tiene problemas para conectarse a CDO, asegúrese de que el puerto 8305 esté abierto, este es un ejemplo de un problema de conexión.

```
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
```

Dispositivo inscrito en un arrendatario SSX incorrecto

Puede comprobar a qué arrendatario de SSX está inscrito su FMC.

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

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

Si el arrendatario de SSX no es correcto, debe volver a realizar los pasos para inscribir los dispositivos en SSX

Si el arrendatario de SSX es correcto, pero el arrendatario de CDO no está vinculado a la organización de SSX adecuada, póngase en contacto con el TAC con estos detalles:

- ID de arrendatario de SSX

- ID de arrendatario de CDO

Información Relacionada

- Guía de integración de Cisco Secure Firewall Threat Defence y Cisco XDR
- Soporte técnico y descargas de Cisco

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).