Integre e solucione problemas do Cisco XDR com o firewall seguro

Contents

Introdução

Pré-requisitos

- Requisitos
- Componentes Utilizados

Configurar

- Licenciamento
- Vincule suas contas ao SSX e registre os dispositivos.

Método 1 (meia integração): Enriquecer as investigações

- Registrar os dispositivos no SSX

Introdução

Este documento descreve as etapas necessárias para integrar, verificar e solucionar problemas do Cisco XDR com Secure Firewall.

Há dois métodos para integrar o Secure Firewall e o XDR, e cada integração fornece resultados diferentes.

O primeiro método descreve como integrar Secure Firewall, Security Services Exchange (SSX), Security Cloud Control, XDR-Analytics e XDR para enriquecer as investigações.

O segundo método descreve como integrar Secure Firewall, SSX, Security Cloud Control, XDR-A, SAL Cloud e XDR, para enriquecer incidentes.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Firewall Management Center (FMC)
- Defesa contra ameaças do Cisco Secure Firewall
- Virtualização opcional de imagens
- Cisco Defense Orchestrator
- Security Services Exchange (Troca de serviços de segurança)
- Controle de nuvem de segurança

Componentes Utilizados

- Firewall seguro - 7.2
- Firepower Management Center (FMC) - 7.2
- Troca de serviços de segurança (SSX)
- Cisco XDR
- Portal Smart License
- Cisco Defense Orchestrator
- Controle de nuvem de segurança

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

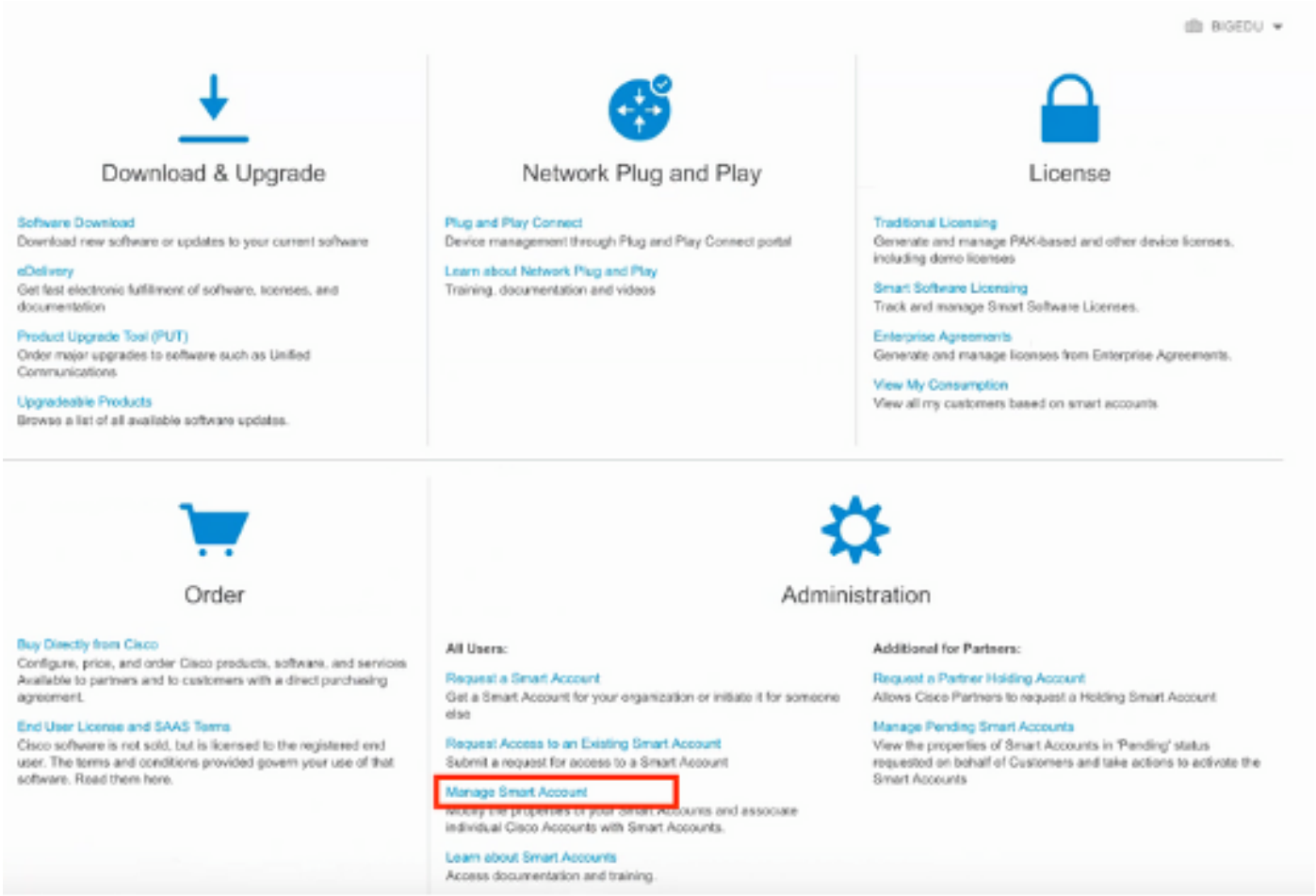
Configurar

Licenciamento

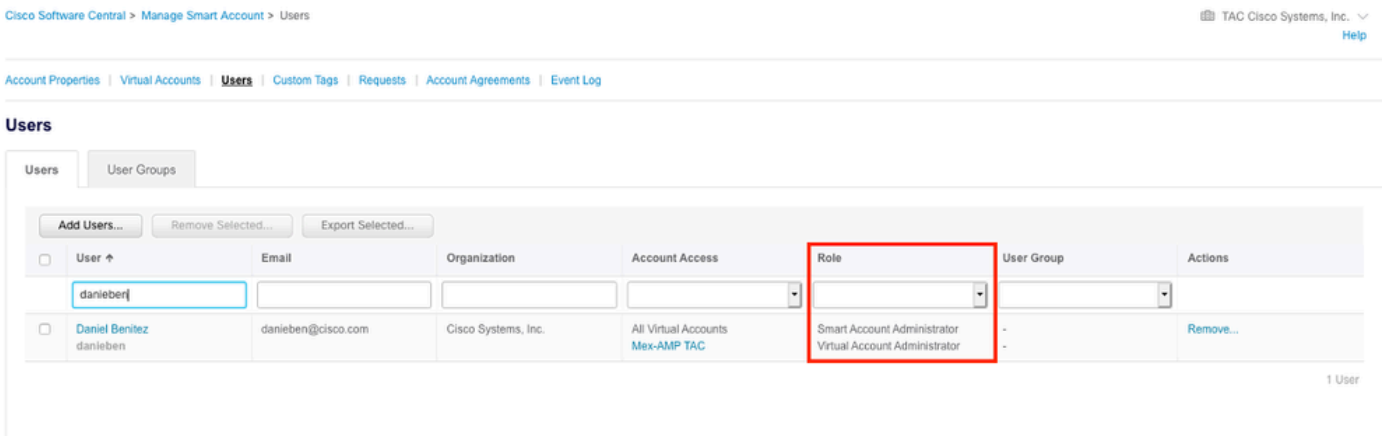
Funções da Virtual Account:

Somente o administrador da Virtual Account ou o administrador da Smart Account têm o privilégio de vincular a Smart Account à conta SSX.

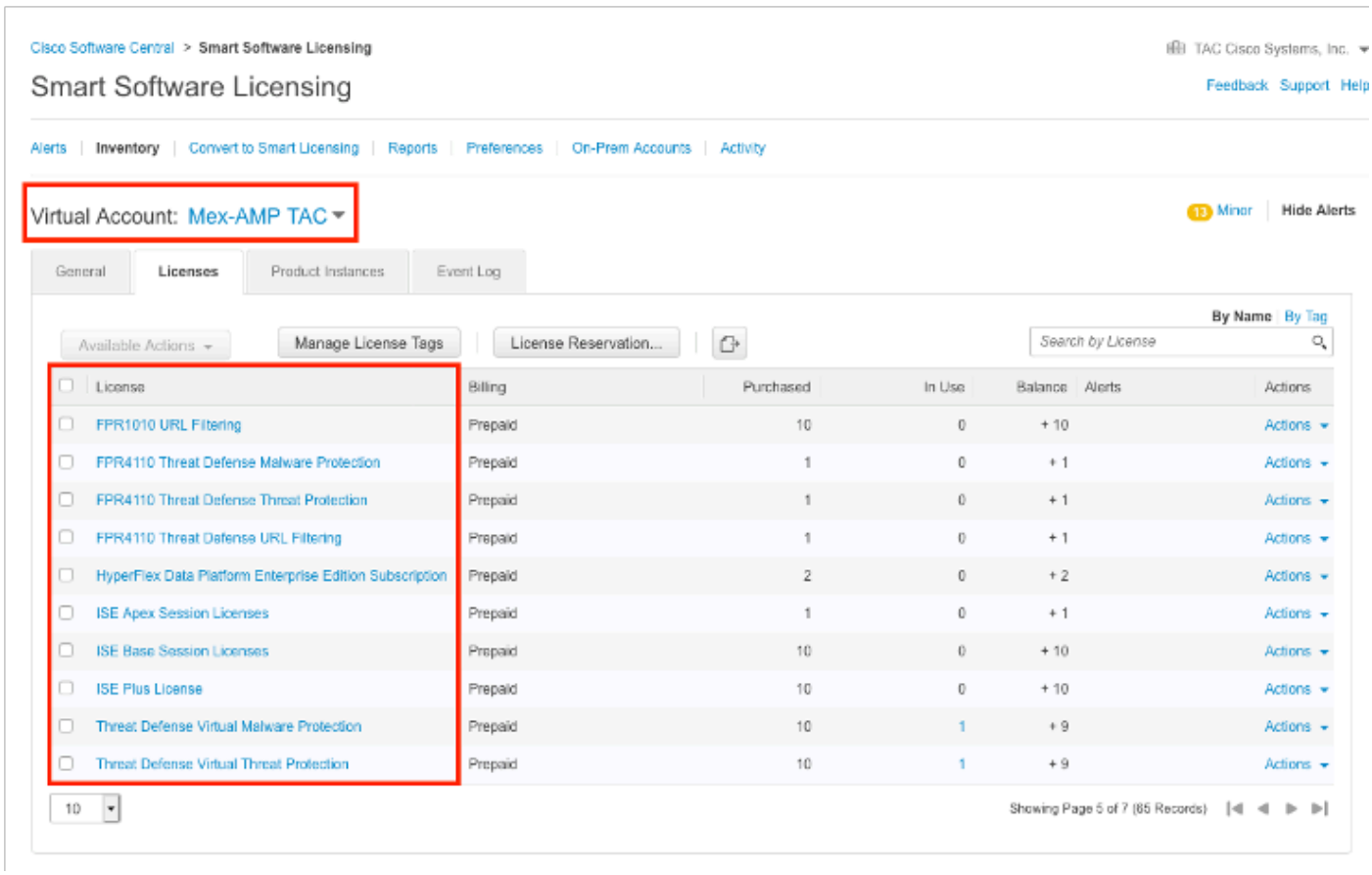
Etapa 1. Para validar a função da Smart Account, navegue até software.cisco.com e, no menu Administração, selecione Gerenciar Smart Account.



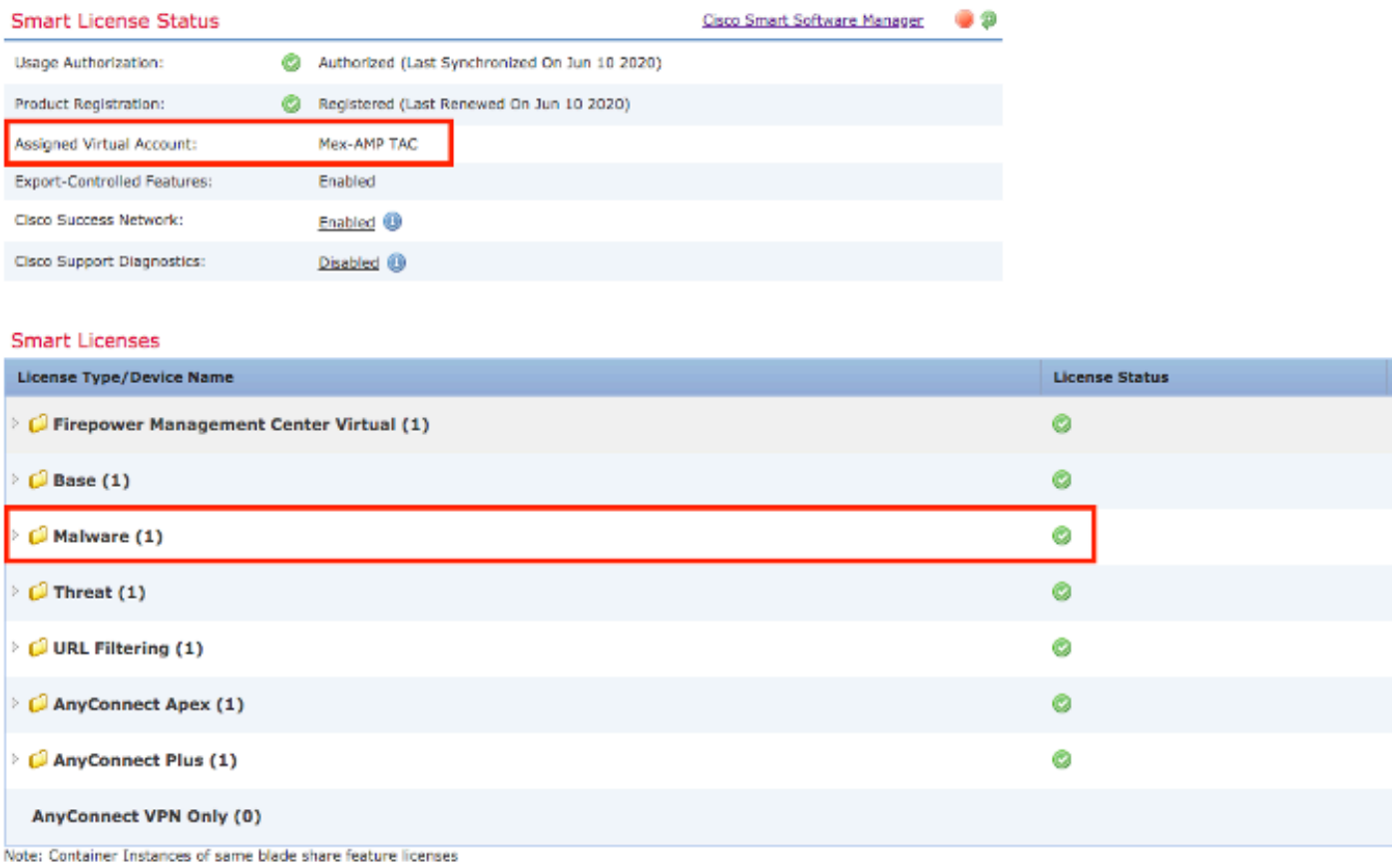
Etapa 2. Para validar a função de usuário, navegue até Usuários e confirme se, em Funções, as contas estão definidas para ter o Administrador da Virtual Account, como mostrado na imagem.



Etapa 3. Verifique se a Virtual Account selecionada para vincular no SSX contém a licença para os dispositivos de segurança se uma conta que não contém a licença de segurança estiver vinculada no SSX, se os dispositivos de segurança e o evento não aparecerem no portal SSX.

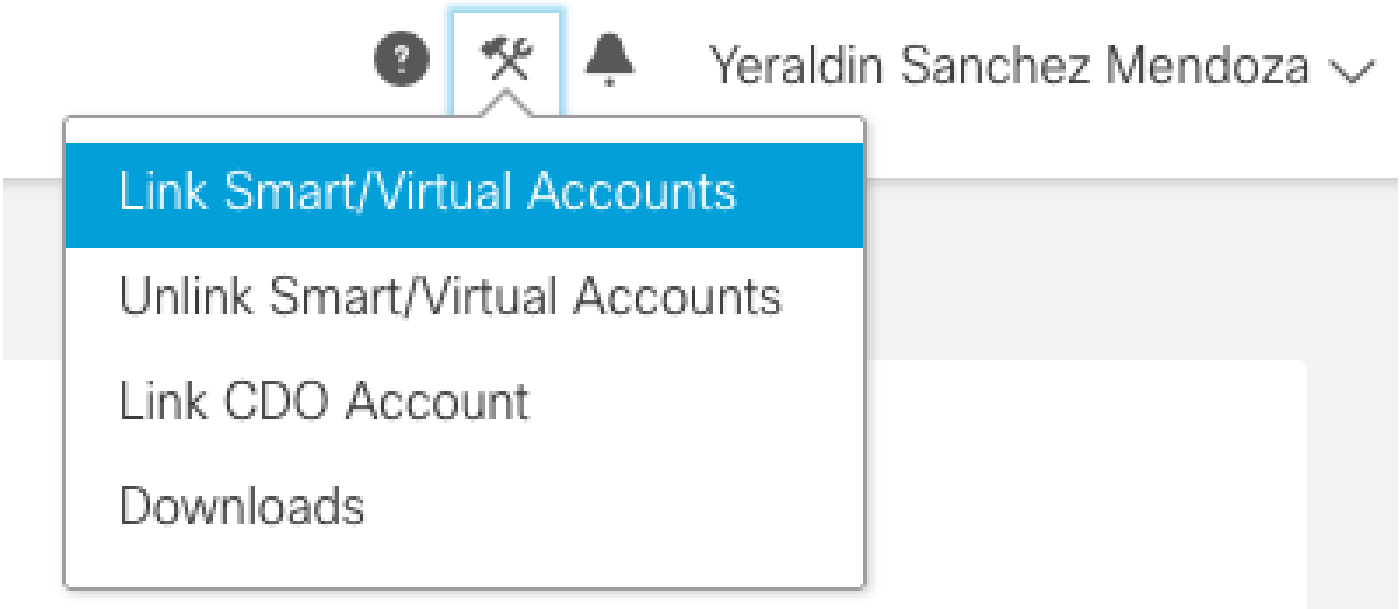


Etapa 4. Para validar que o FMC foi registrado na Virtual Account correta, navegue até System > Licenses > Smart License:



Vincule suas contas ao SSX e registre os dispositivos.

Etapa 1. Ao fazer logon em sua conta SSX, você precisa vincular sua Smart Account à sua conta SSX, para isso, você precisa clicar no ícone Ferramentas e selecionar Vincular Smart/Virtual Accounts.



Quando a conta estiver vinculada, você verá a Smart Account com todas as Virtual Accounts nela.

Método 1 (meia integração): Enriquecer as investigações

Registrar os dispositivos no SSX

Etapa 1. Certifique-se de que estes URLs sejam permitidos em seu ambiente:

Região dos EUA

- 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

Região da 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

Região da 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

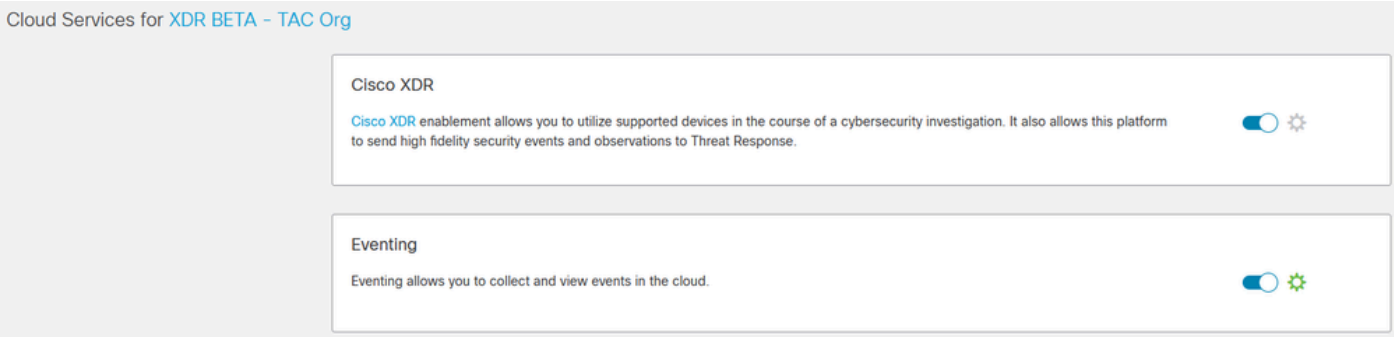
Região da Austrália:

- 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

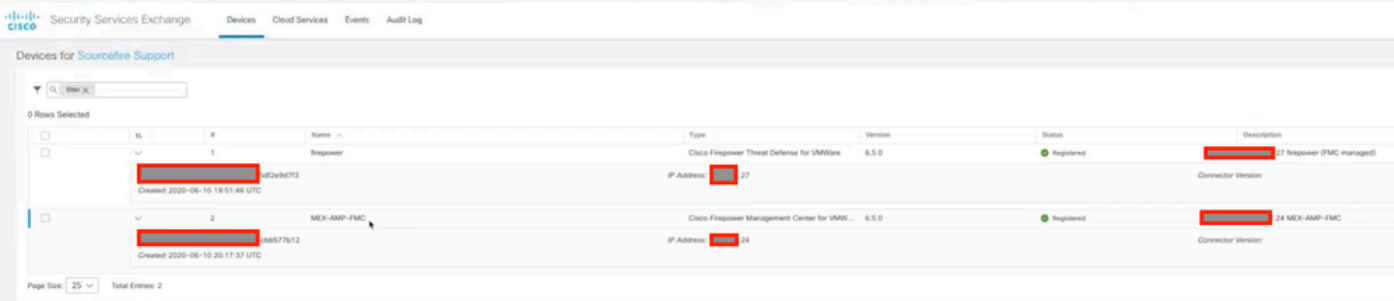
Região da Índia:

- 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

Etapa 2. Faça login no portal SSX com este URL https://admin.sse.itd.cisco.com, navegue até Cloud Services e habilite ambas as opções Cisco XDR e Eventing, como mostrado na imagem.

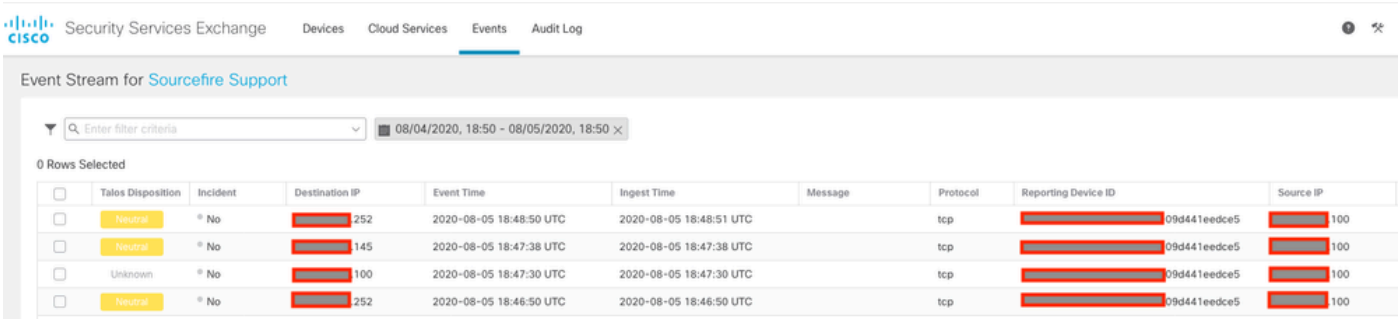


Etapa 3. Você pode confirmar que agora pode ver os dispositivos registrados no SSX:



Os eventos são enviados pelos dispositivos do Secure Firewall, navegue para os Eventos no portal SSX para verificar os eventos enviados pelos dispositivos para o SSX, como mostrado na

imagem.



Registre os dispositivos no Security Cloud Control (SCC/CDO)

Etapa 1. Certifique-se de que esses URLS sejam permitidos em seu ambiente

Região dos EUA:

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

Região da UE

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

Região da APJC

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

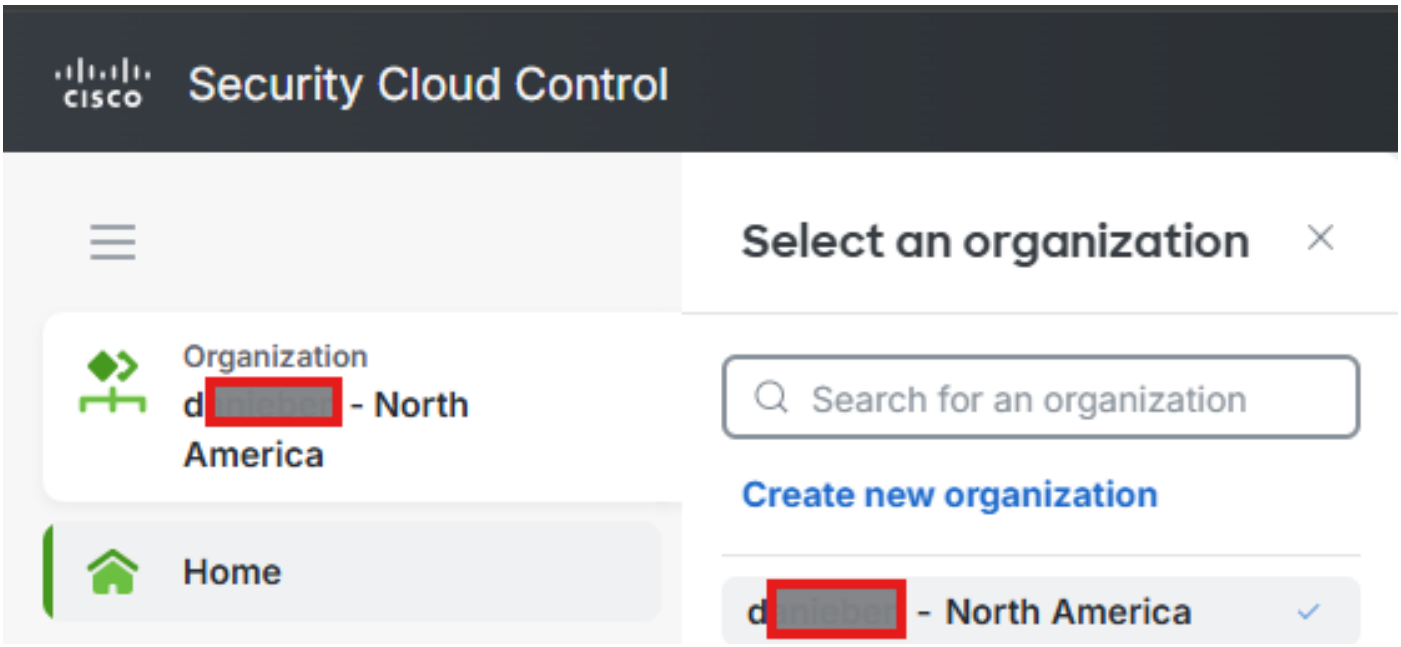
Região da Austrália:

- aus.cdo.cisco.com

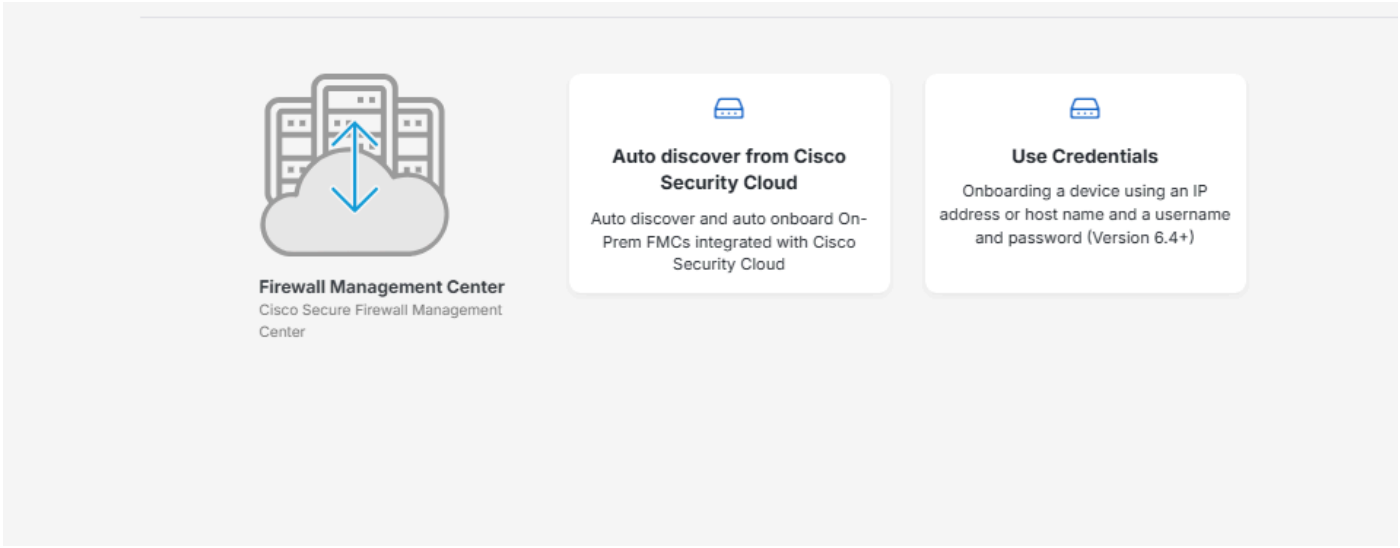
Região da Índia:

- in.cdo.cisco.com

Etapa 2. Navegue até Security Cloud Control (o link pode variar dependendo da sua região). Isso o direciona para selecionar sua Security Cloud Control Organization.



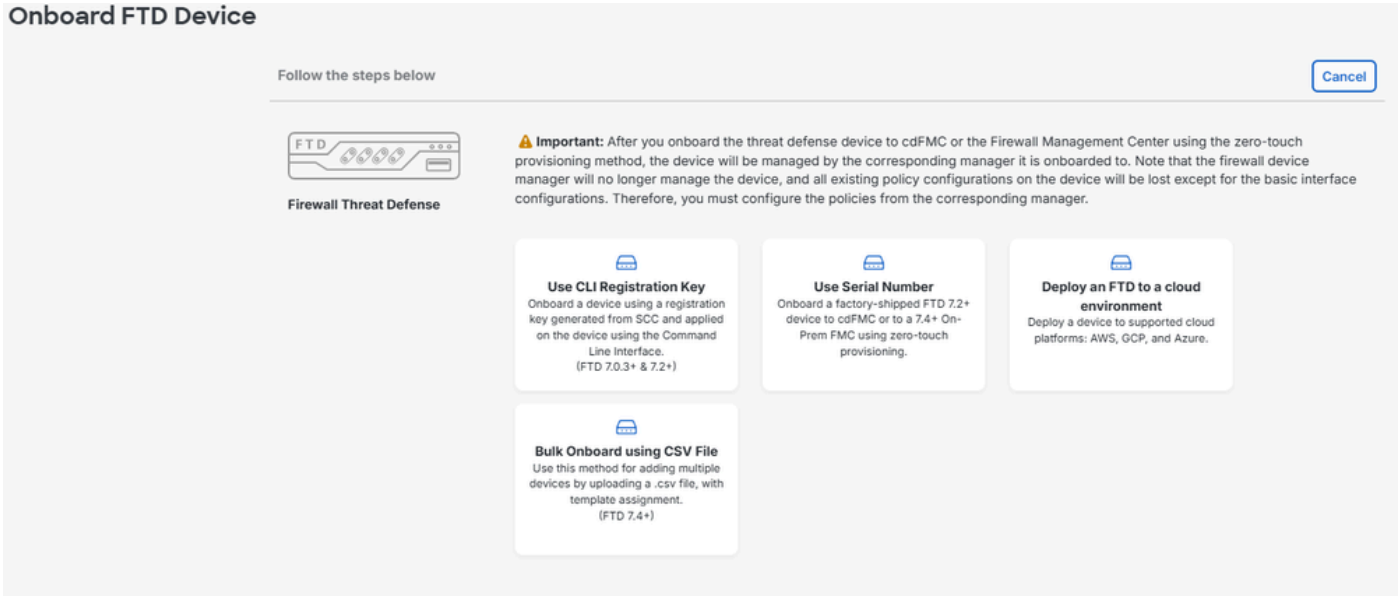
Etapa 3. Depois de selecionar a organização apropriada, navegue para Products > Firewall, verifique se o dispositivo já está lá, caso contrário, você pode Onboard it to Security Cloud Control (Cisco Defense Orchestrator), para isso, em Inventário geral, clique em Visualizar todos os dispositivos.



Etapa 4. Navegue até Administration > Firewall Management Center, uma lista de seus FMCs integrados ao SCC é apresentada. Se você não vir seu Firewall Management Center, clique no ícone de mais.

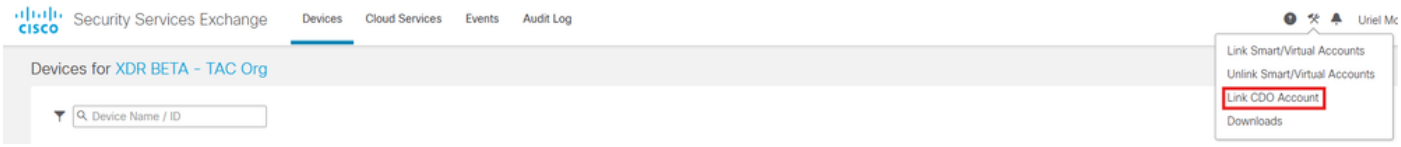
Etapa 4.1. Normalmente, os firewalls seguros são integrados automaticamente. Caso contrário, selecione o dispositivo que deseja integrar (FTD) e o método de integração de sua preferência.

Etapa 4.2. Na seção Security Devices (Dispositivos de segurança), clique no ícone de mais, selecione Onboard Secure Firewall Device e seu dispositivo



Etapa 5. Depois de integrar seus dispositivos no Security Cloud Control, você poderá visualizá-lo no inventário.

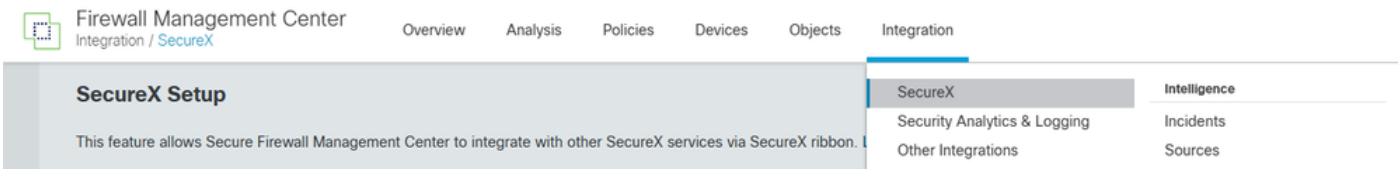
Etapa 6. Certifique-se de que sua organização CDO está vinculada à sua organização SSX, para isso, navegue para Security Services Exchange, clique no ícone do menu Ferramentas, clique em Vincular conta CDO.



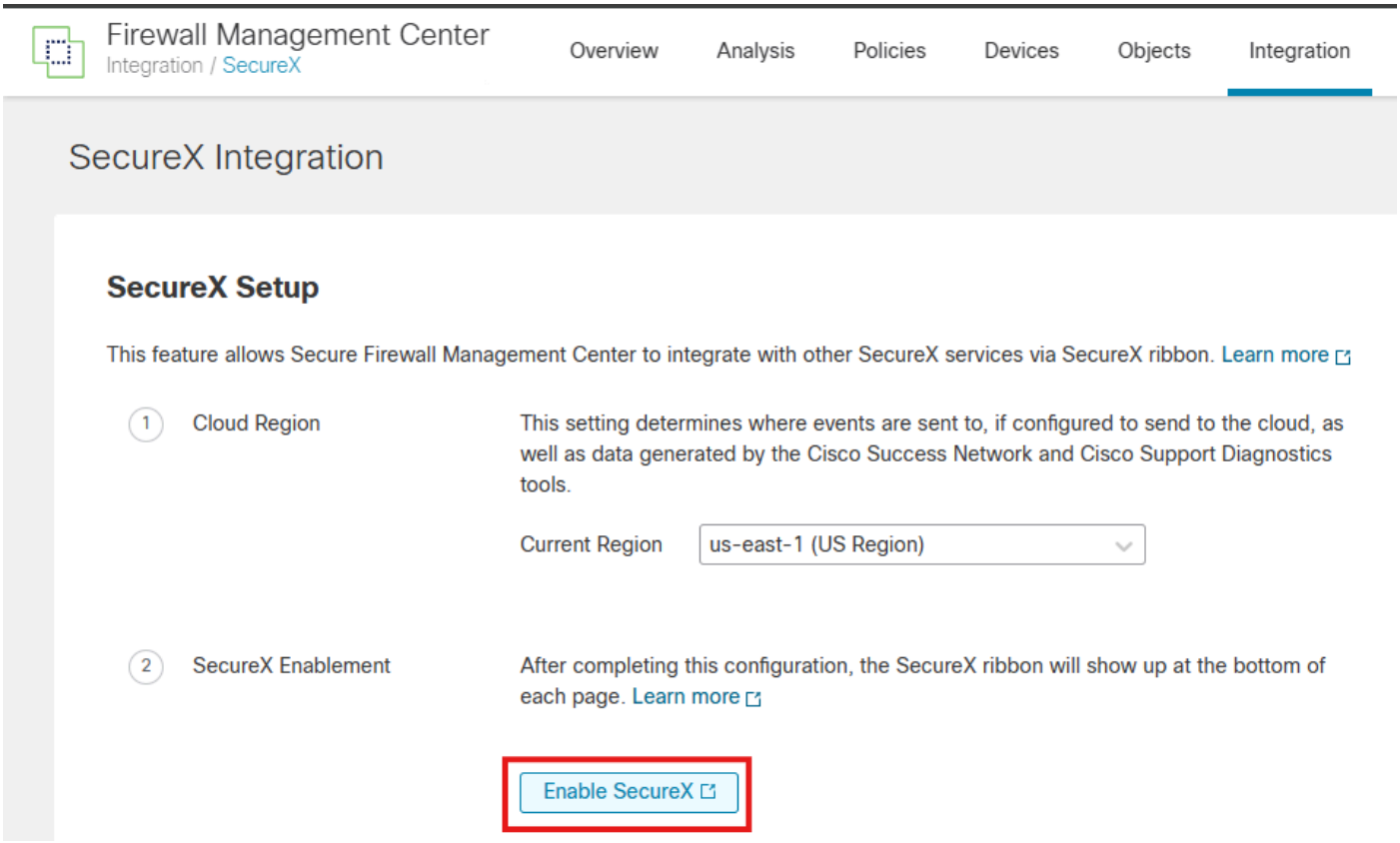
Integre o firewall seguro

De 7.2.x a 7.4.x com Cisco XDR

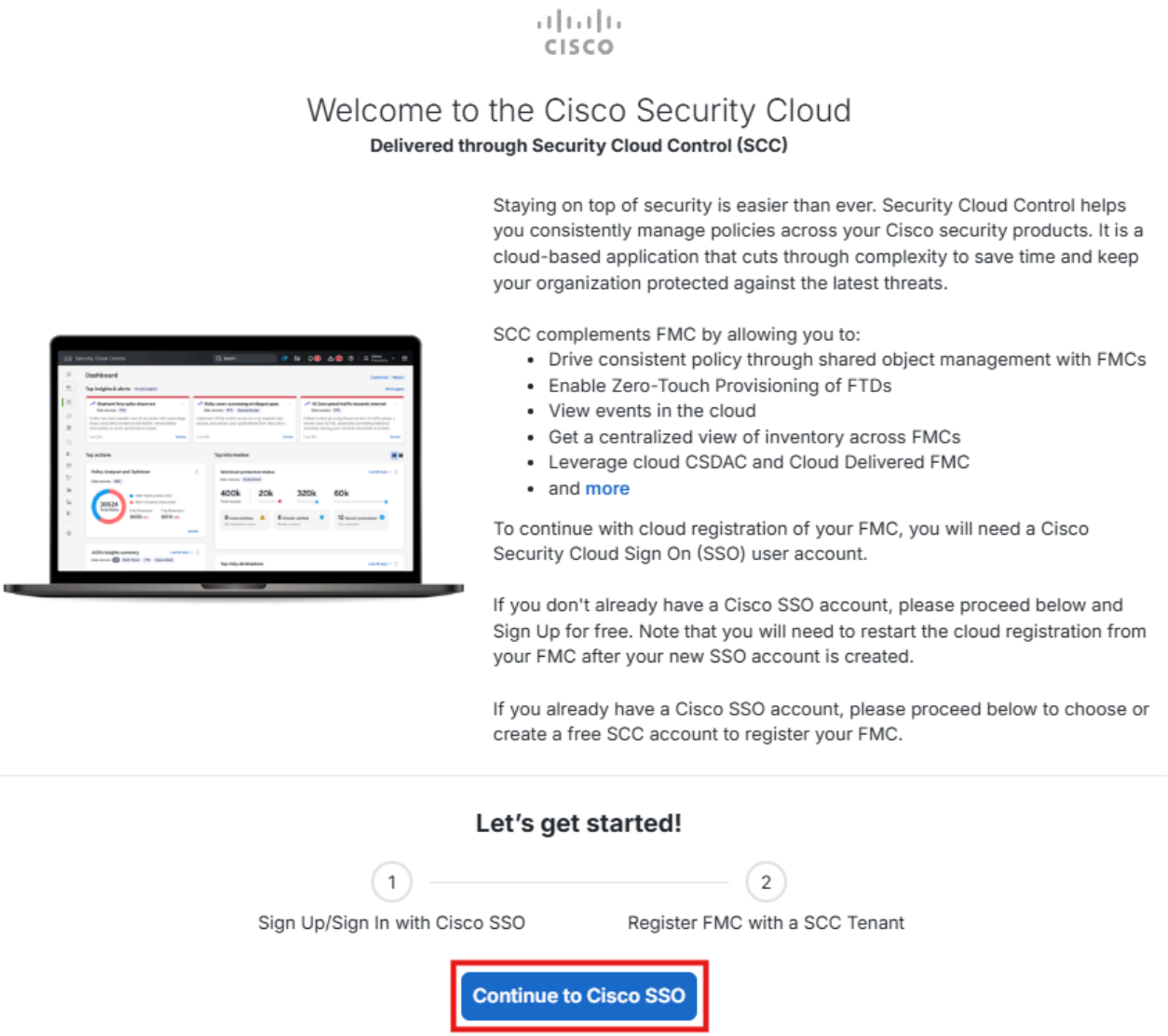
Etapa 1. No Secure Firewall Management Center, navegue até Integração > SecureX



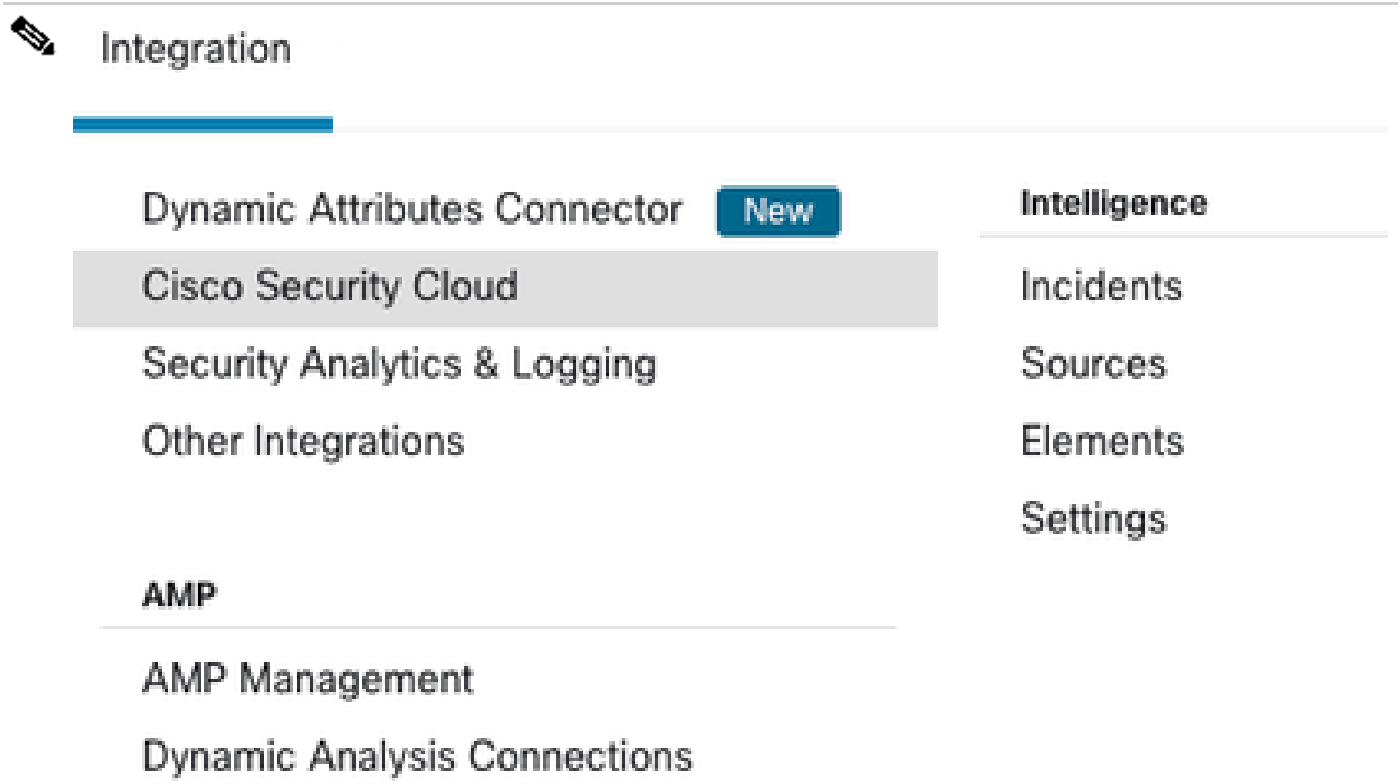
Etapa 2. Escolha a região direita e clique em Enable SecureX.



Etapa 3. Depois de clicar em Enable SecureX (Habilitar SecureX), você será redirecionado para a página de autenticação do Cisco Defense Orchestrator (que aproveita o Security Cloud Sign On), depois clique em Continue to Cisco SSO (Continuar para o Cisco SSO).



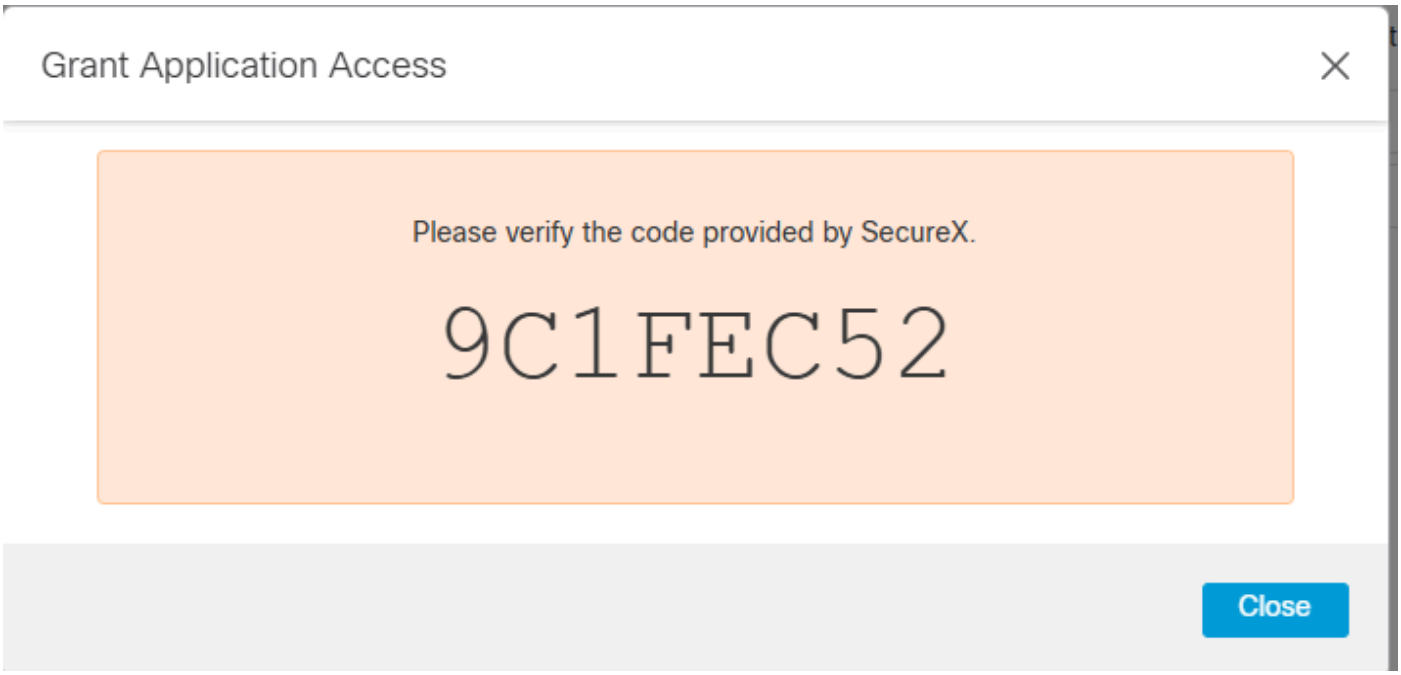
Note:
A partir do 7.6.x e posterior com o Cisco XDR
Etapa 1. Em seu Secure Firewall Management Center, navegue até Integração > Cisco Security Cloud

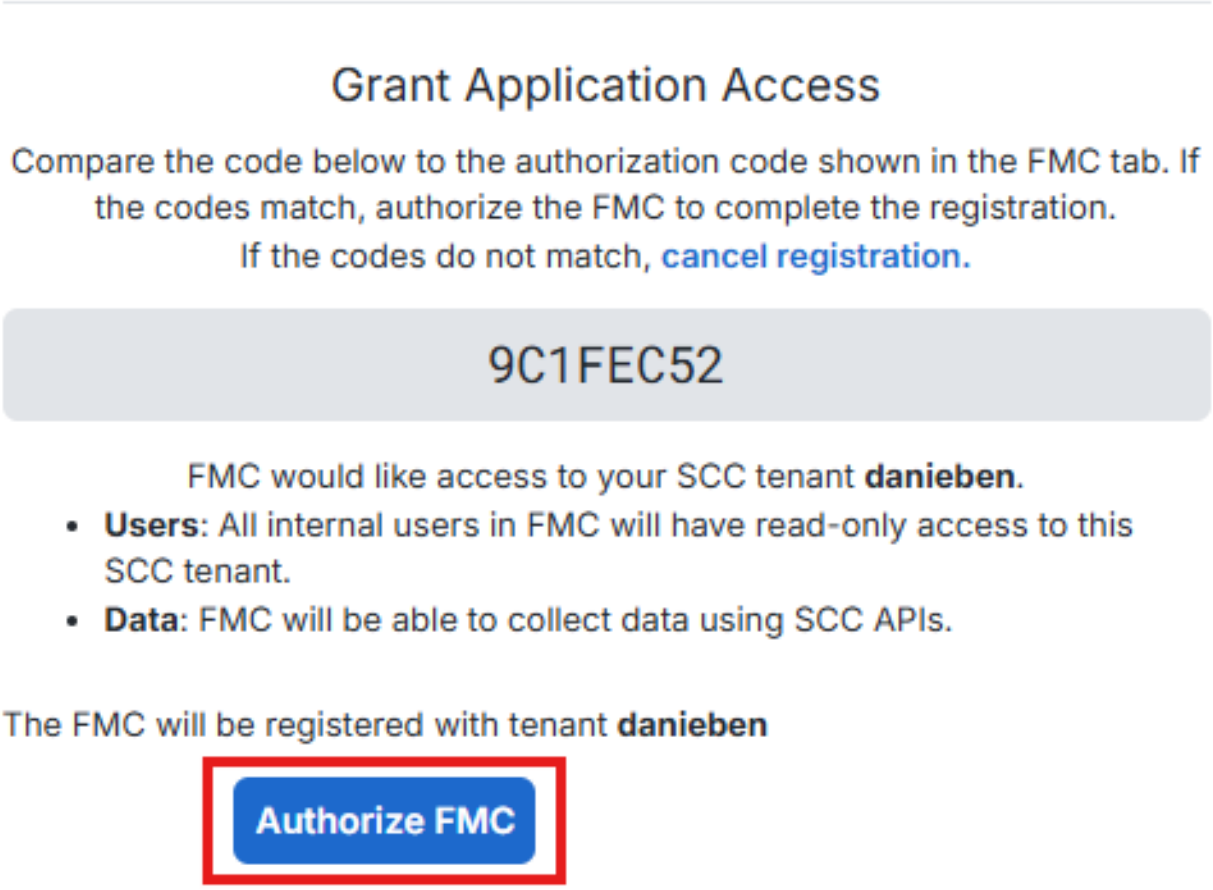


Etapa 2. Escolha a região certa e clique em Enable Cisco Security Cloud.
Etapa 3. Depois de clicar em Enable Cisco Security Cloud, você será redirecionado para a página de autenticação do Cisco Defense Orchestrator (que aproveita o Security Cloud Sign On), clique em Continue to Cisco SSO.

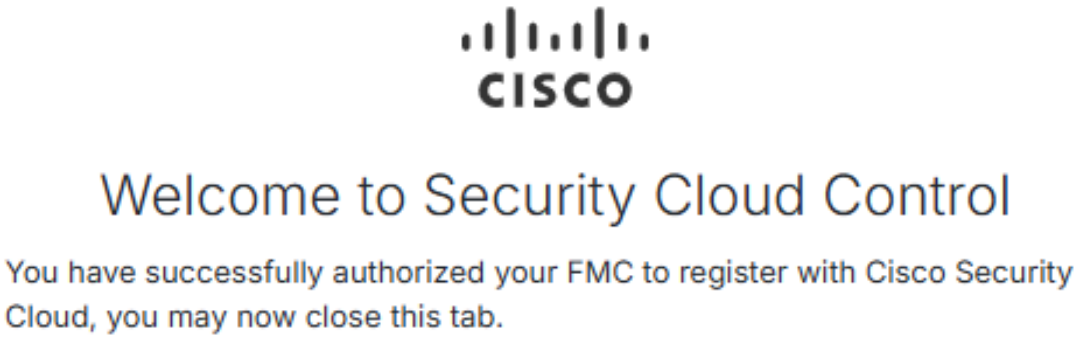
Etapa 4. Você pode selecionar um Locatário do Security Cloud Control preexistente ou criar um novo.

Etapa 5. Selecione o Locatário apropriado e verifique se o código que você está recebendo nesta página corresponde ao código que você está recebendo no FMC. Se eles corresponderem, clique em Autorizar FMC.



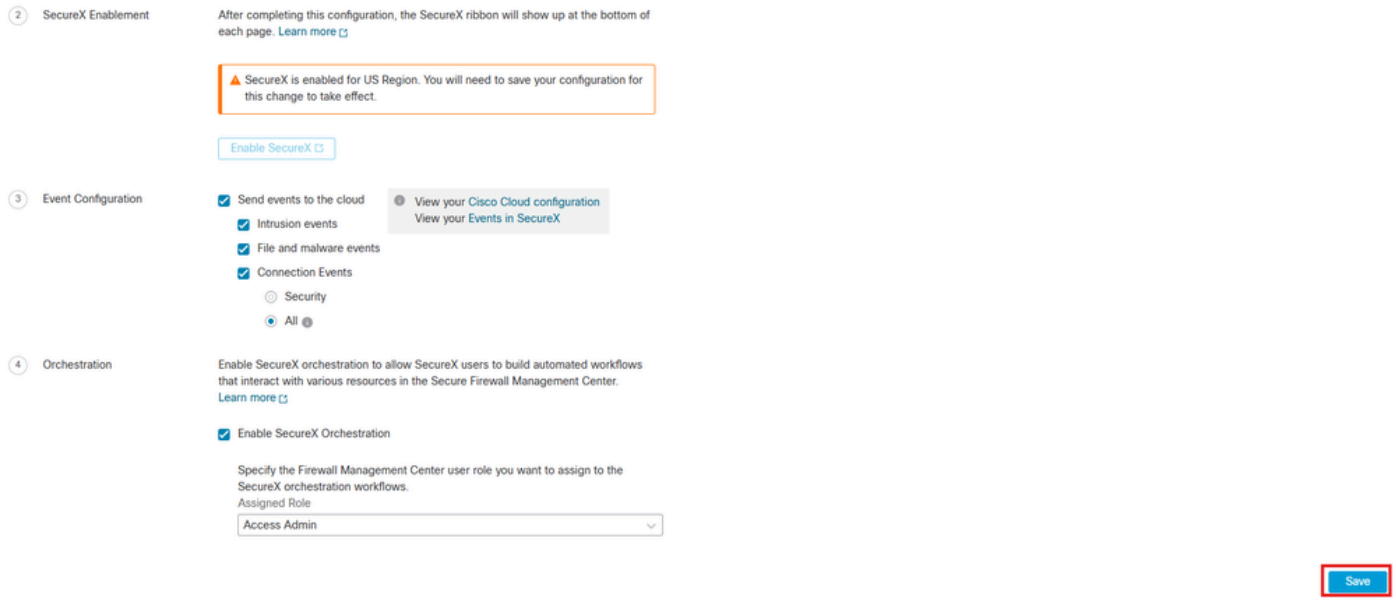


Etapa 6. Insira suas credenciais de Logon do Security Cloud e autorize a integração. Após a conclusão, uma confirmação de que o FMC foi autorizado a se registrar no Cisco Security Cloud é apresentada.



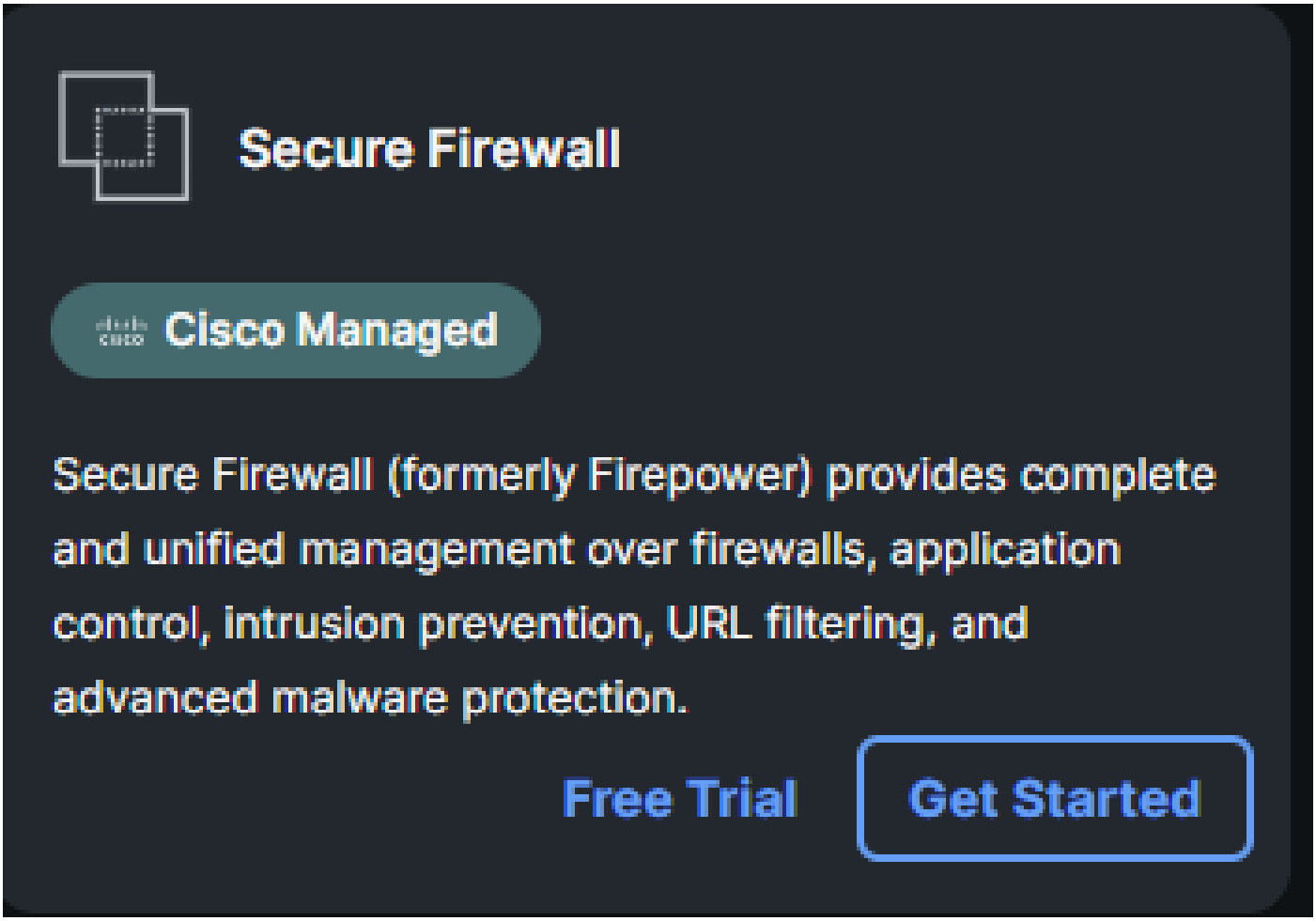
Etapa 7. Após a autorização ser concluída, você pode navegar de volta para o FMC e selecionar quais eventos deseja enviar para a nuvem. Depois de concluir essa etapa, clique em Salvar.

Etapa 8. Você pode optar por ativar a orquestração SecureX (XDR Automate)

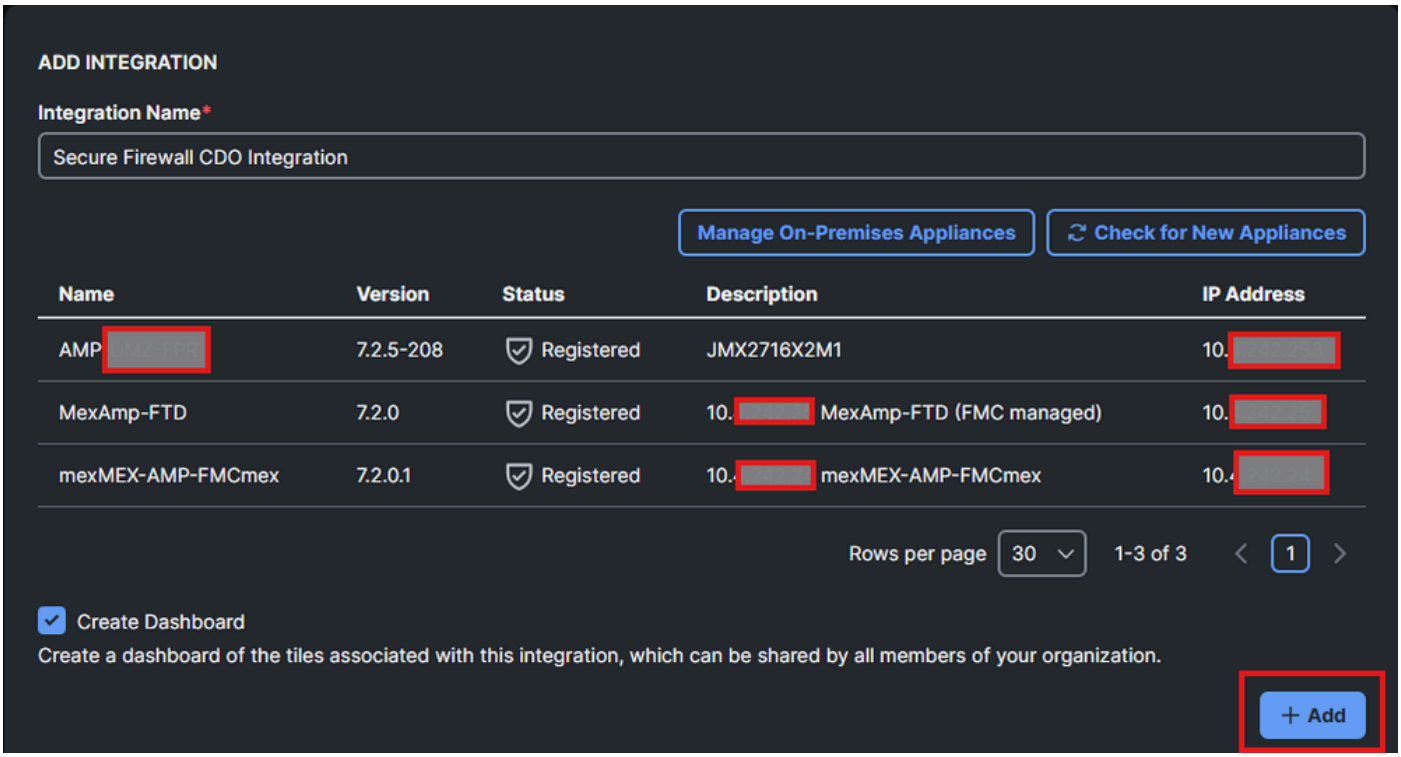


Etapa 9. Navegue até XDR > Administration > On Premises Appliance e procure seus equipamentos, eles devem ser registrados automaticamente.

Etapa 10. Navegue até XDR > Administration > Integrations e ative a Secure Firewall Integration.



Etapa 10.1. Atribua um nome à sua integração, clique em +Adicionar.



Essa integração permite enriquecer as Investigações no XDR.

Método 2 (Integração total): Enriquecer Incidentes no XDR

Note: Para garantir a integração perfeita entre o Secure Firewall, o XDR, o Cisco Defense Orchestrator (CDO), o Security Services Exchange (SSX) e o Security Analytics and Logging (SAL), é necessário o mapeamento manual. Esse processo envolve entrar em contato com o Cisco TAC para executar as configurações e os mapeamentos necessários.

Etapa 1. Sua conta CDO deve ter uma licença Security Analytics and Logging para encaminhar eventos para o Cisco XDR.

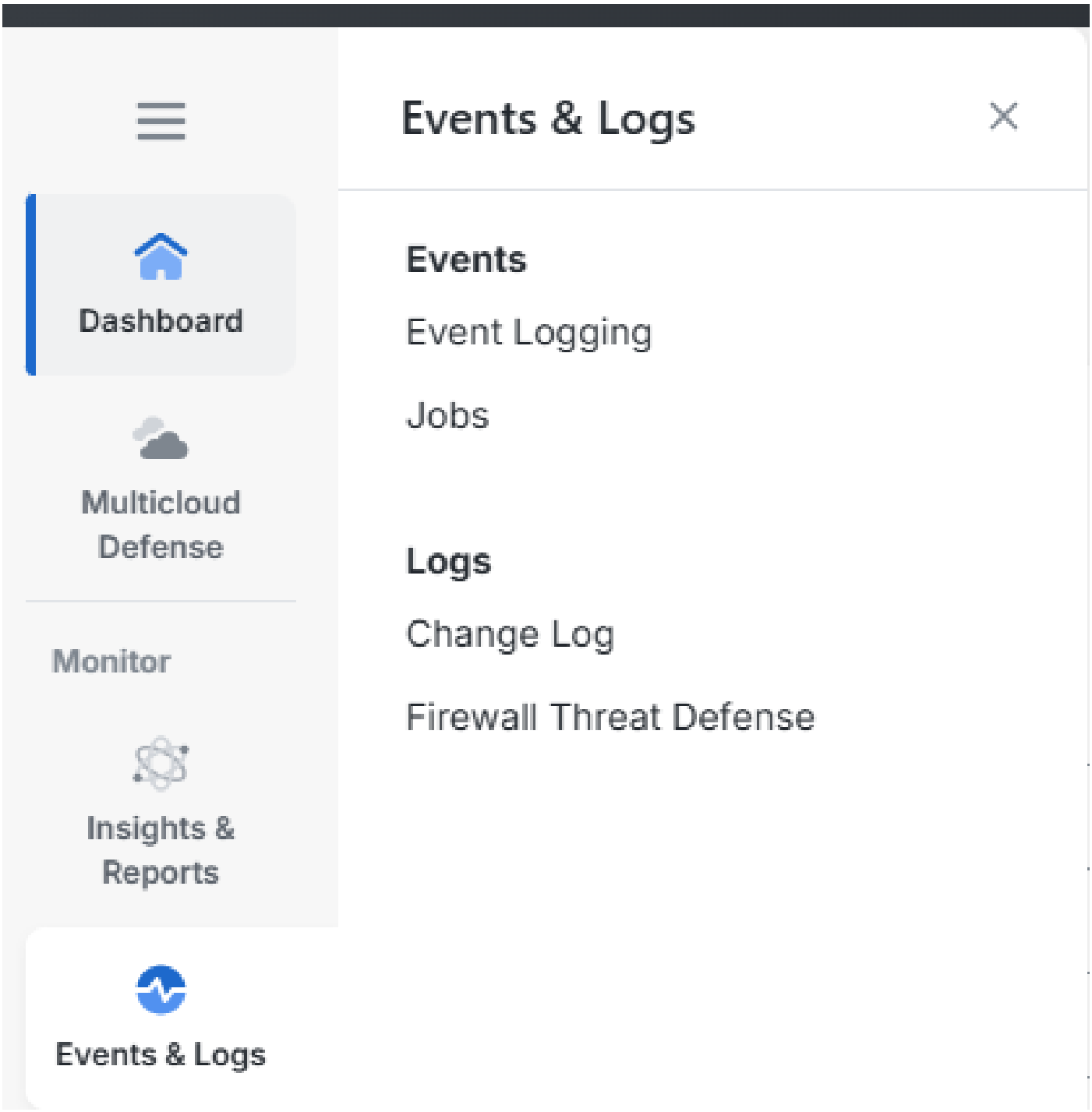
Etapa 2. Use as etapas descritas anteriormente para registrar seus dispositivos no SSX e no Security Cloud Control.

Etapa 3. Quando terminar, entre em contato com o TAC e solicite o link Security Cloud Control/SAL (Controle de nuvem de segurança/SAL) para XDR Analytics.

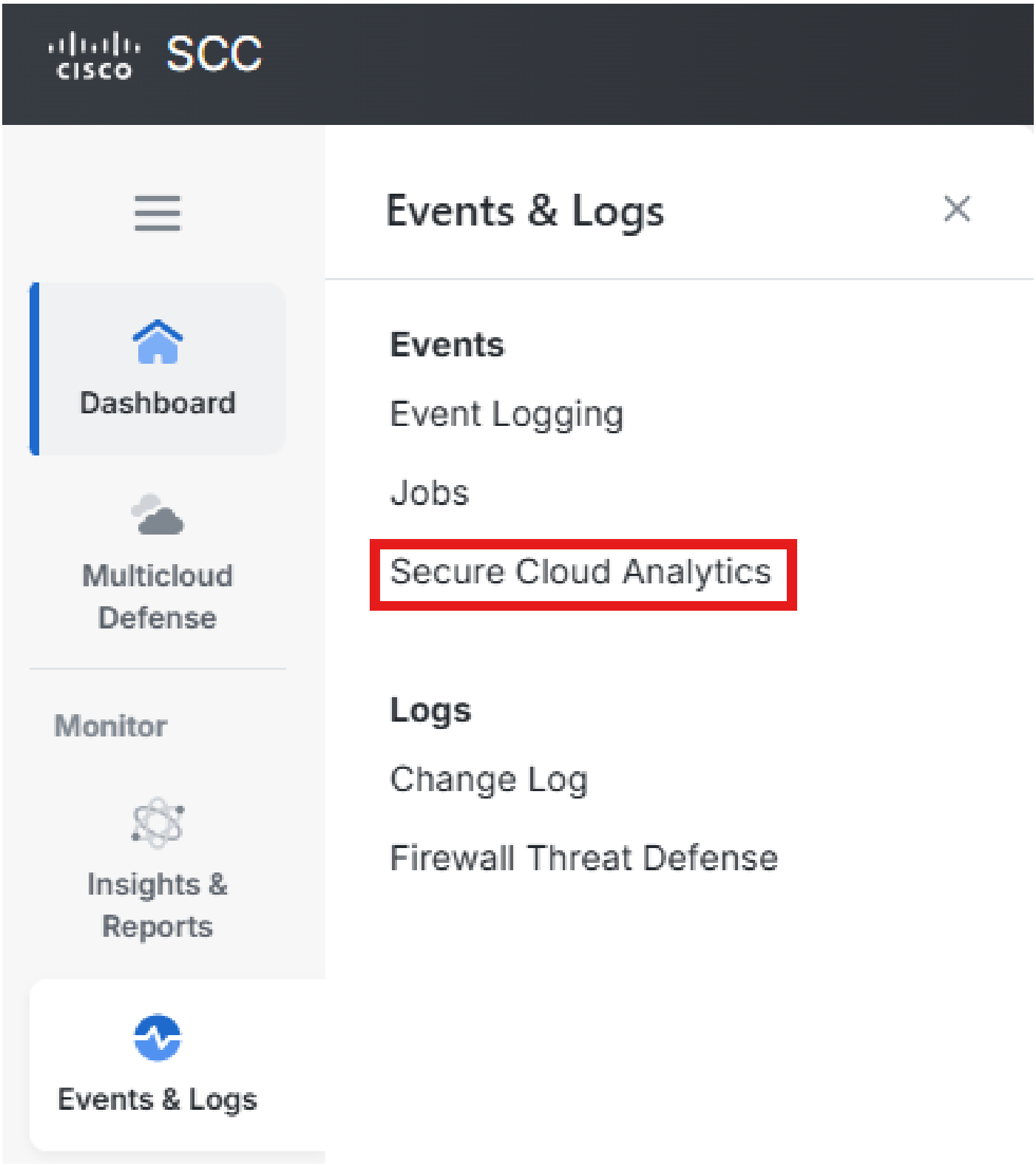
- ID do locatário CDO
- Nome do CDO
- ID da Org XDR
- ID do locatário SSX
- Nome SSX
- ID da Org. SCA

Etapa 4. Verifique se sua conta CDO está vinculada ao Portal de análise XDR.

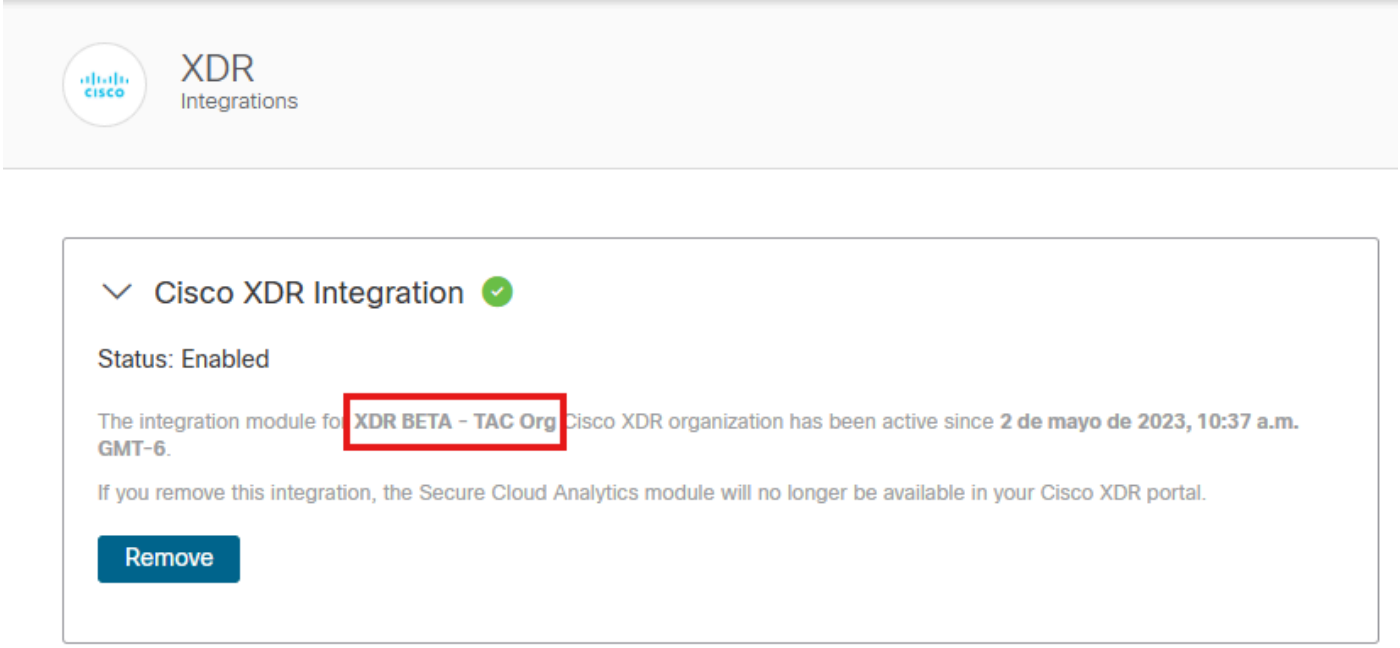
Antes de vincular seu portal CDO ao XDR Analytics, ele se parece com o seguinte:



Depois que o link for concluído, você poderá ver a opção para navegar para o Portal de análise XDR.



Etapa 5. Depois que sua conta do XDR Analytics estiver vinculada ao Security Cloud Control Portal (CDO), você precisará verificar se o XDR Analytics está integrado ao XDR. Para isso, no XDR Analytics, navegue até Settings > Integrations > XDR, procure XDR Integration e verifique se há uma verificação verde e se o módulo Integration aponta para a organização XDR correta.



Verificar

Valide se os Secure Firewalls geram eventos (malware ou invasão), para eventos de invasão, navegue até Análise >Arquivos >Eventos de malware, para eventos de intrusão, navegue para Análise > Intrusão > Eventos.

Verifique se os eventos estão registrados no portal SSX conforme mencionado na seção Registrar os dispositivos no SSX, etapa 4.

Verifique se as informações são exibidas no painel do Cisco XDR ou verifique os logs de API para que você possa ver o motivo de uma possível falha de API.

Verifique se todos os locatários estão corretamente vinculados, se você tiver problemas, abra um caso TAC e forneça estes detalhes:

- ID do locatário CDO
- Nome do CDO
- ID da Org XDR
- ID do locatário SSX
- Nome SSX
- ID da Org. SCA

Troubleshooting

Detectar problemas de conectividade

Você pode detectar problemas de conectividade genéricos a partir do arquivo action_queue.log. Em caso de falha, você pode ver esses logs presentes no arquivo:

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

Nesse caso, o código de saída 28 significa que a operação atingiu o tempo limite e precisamos verificar a conectividade com a Internet. Você também deve ver o código de saída 6, que significa problemas com a resolução DNS

Problemas de conectividade devido à resolução DNS

Etapa 1. Verifique se a conectividade está funcionando corretamente.

```
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'
```

Esta saída mostra que o dispositivo não pode resolver o URL https://api-sse.cisco.com; neste caso, precisamos validar se o servidor DNS apropriado está configurado, ele pode ser validado com um nslookup da CLI do especialista:

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

Esta saída mostra que o DNS configurado não foi alcançado. Para confirmar as configurações DNS, use o 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
```

Neste exemplo, o servidor DNS errado foi usado. Você pode alterar as configurações DNS com este comando:

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

Depois que essa conectividade puder ser testada novamente e dessa vez, a conexão será bem-sucedida.

```
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 no SSX Portal

O FMC e o Secure Firewall precisam de uma conexão com os URLs SSX em sua interface de gerenciamento. Para testar a conexão, insira estes comandos na CLI do Firepower com acesso raiz:

<#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

A verificação do certificado pode ser ignorada com 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;
```

Note: Você recebe a mensagem 403 Forbidden, pois os parâmetros enviados do teste não são o que o SSX espera, mas isso prova o suficiente para validar a conectividade.

Verificar o estado do SSEConnector

Você pode verificar as propriedades do conector conforme mostrado.

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

Para verificar a conectividade entre o SSConnector e o EventHandler, você pode usar esse comando, este é um exemplo de conexão inválida:

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

No exemplo de uma conexão estabelecida, você pode ver que o status do fluxo está 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 os dados enviados ao portal SSX e ao CTR

Para enviar eventos do dispositivo Secure Firewall para SSX, uma conexão TCP precisa ser estabelecida com https://eventing-ingest.sse.itd.cisco.com Este é um exemplo de uma conexão não estabelecida entre o portal SSX e o 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
```

Nos logs 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
```

Note: Observado que os endereços IP exibidos x.x.x.246 e 1x.x.x.246 pertencem a https://eventing-ingest.sse.itd.cisco.com devem ser alterados, é por isso que a recomendação é permitir o tráfego para o SSX Portal com base na URL em vez de endereços IP.

Se essa conexão não for estabelecida, os eventos não serão enviados ao portal SSX. Este é um exemplo de uma conexão estabelecida entre o Secure Firewall e o 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.
```

O dispositivo (FTD) não pode ser inscrito no Security Cloud Control

Se seu dispositivo não puder ser inscrito no Security Cloud Control, verifique se ele tem conectividade com o locatário de CDO apropriado.

Para verificar o URL correto, navegue para Administração > Centro de gerenciamento de firewall, selecione FMC fornecido pela nuvem, na parte superior direita da tela, você pode ver o nome do 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!
```

Se você ainda estiver enfrentando problemas para se conectar ao CDO, verifique se a porta 8305 está aberta, este é um exemplo de um problema de conexão.

```
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 no locatário SSX incorreto

Você pode verificar em qual locatário SSX seu FMC está inscrito.

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

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

Se o locatário do SSX estiver incorreto, você precisará refazer as etapas para inscrever seus dispositivos no SSX

Se o locatário do SSX estiver correto, mas o locatário do CDO não estiver vinculado à organização do SSX apropriada, entre em contato com o TAC com estes detalhes:

- ID do locatário SSX

- ID do locatário CDO

Informações Relacionadas

- Guia de integração do Cisco Secure Firewall Threat Defense e do Cisco XDR
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.