Integre e solucione problemas do SecureX com o Firepower Threat Defense (FTD)

Contents

Introduction

Este documento descreve as etapas necessárias para integrar, verificar e solucionar problemas do SecureX com o Firepower Firepower Firepower Threat Defense (FTD).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)
- Virtualização opcional de imagens

Componentes Utilizados

- Firepower Threat Defense (FTD) - 6,5
- Firepower Management Center (FMC) - 6,5
- Troca de serviços de segurança (SSE)
- SecureX

- Smart License Portal

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

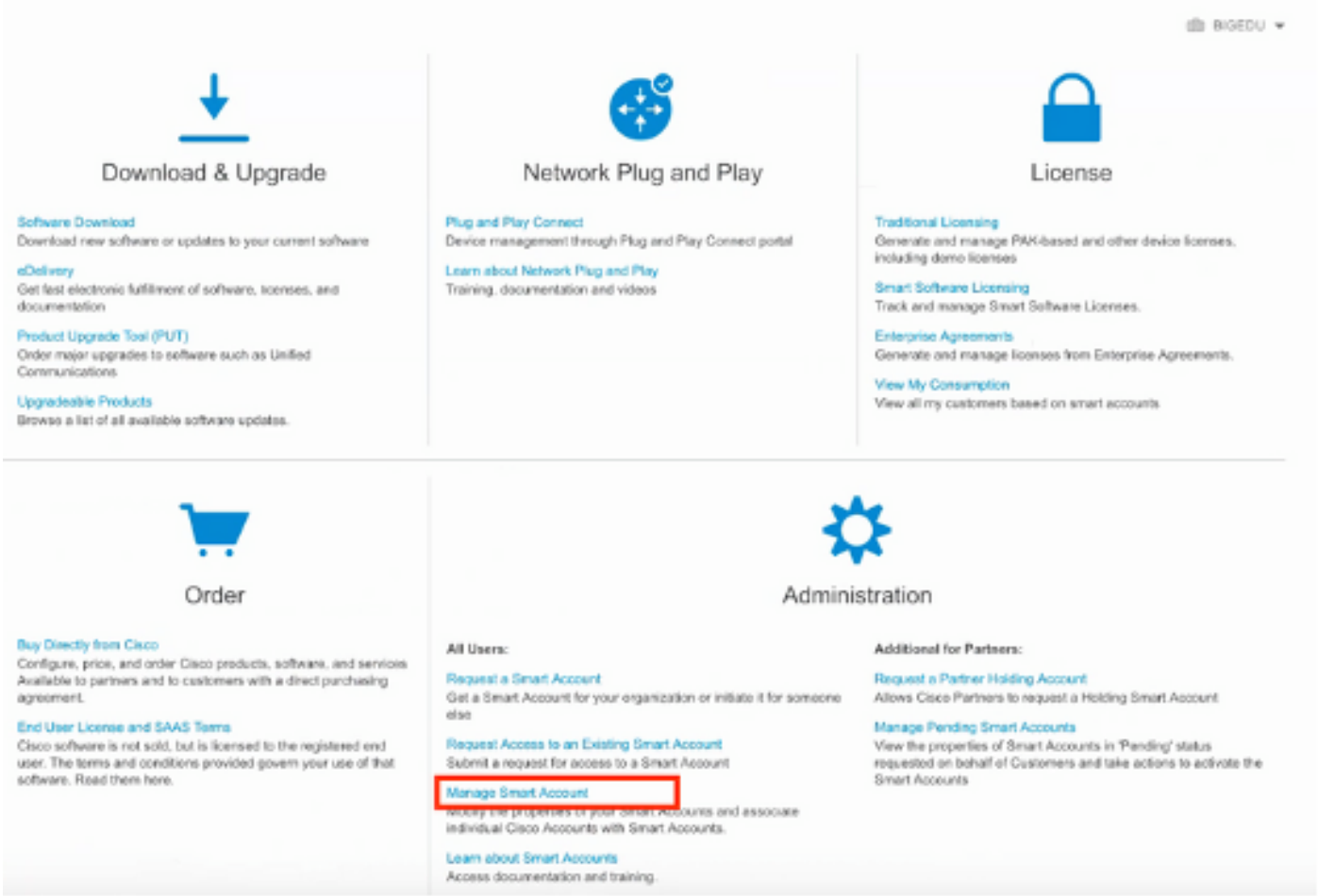
Configurar

Licenciamento

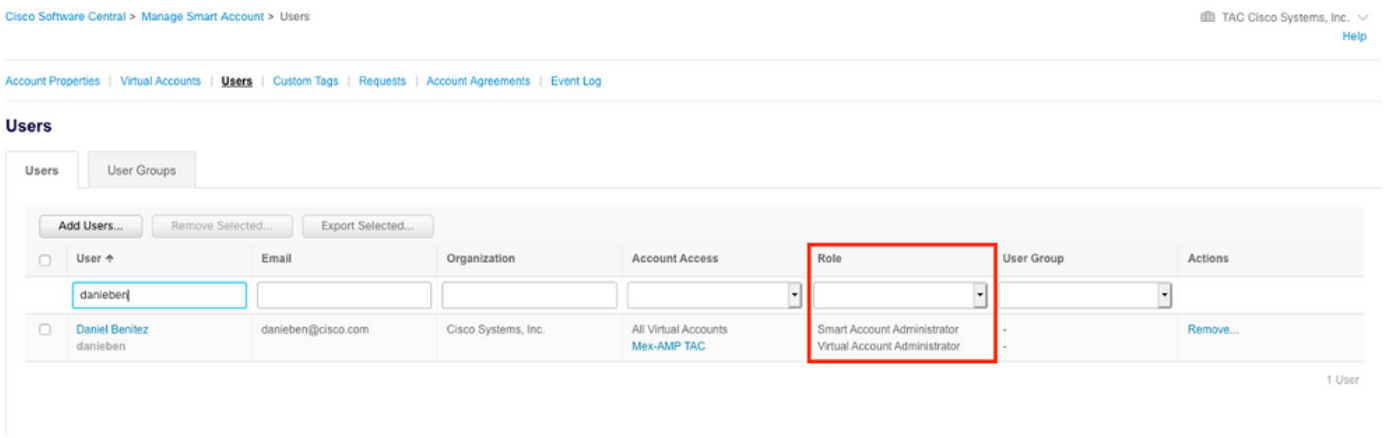
Funções da Virtual Account:

Somente o administrador da Virtual Account ou o administrador da Smart Account tem o privilégio de vincular a Smart Account à conta SSE.

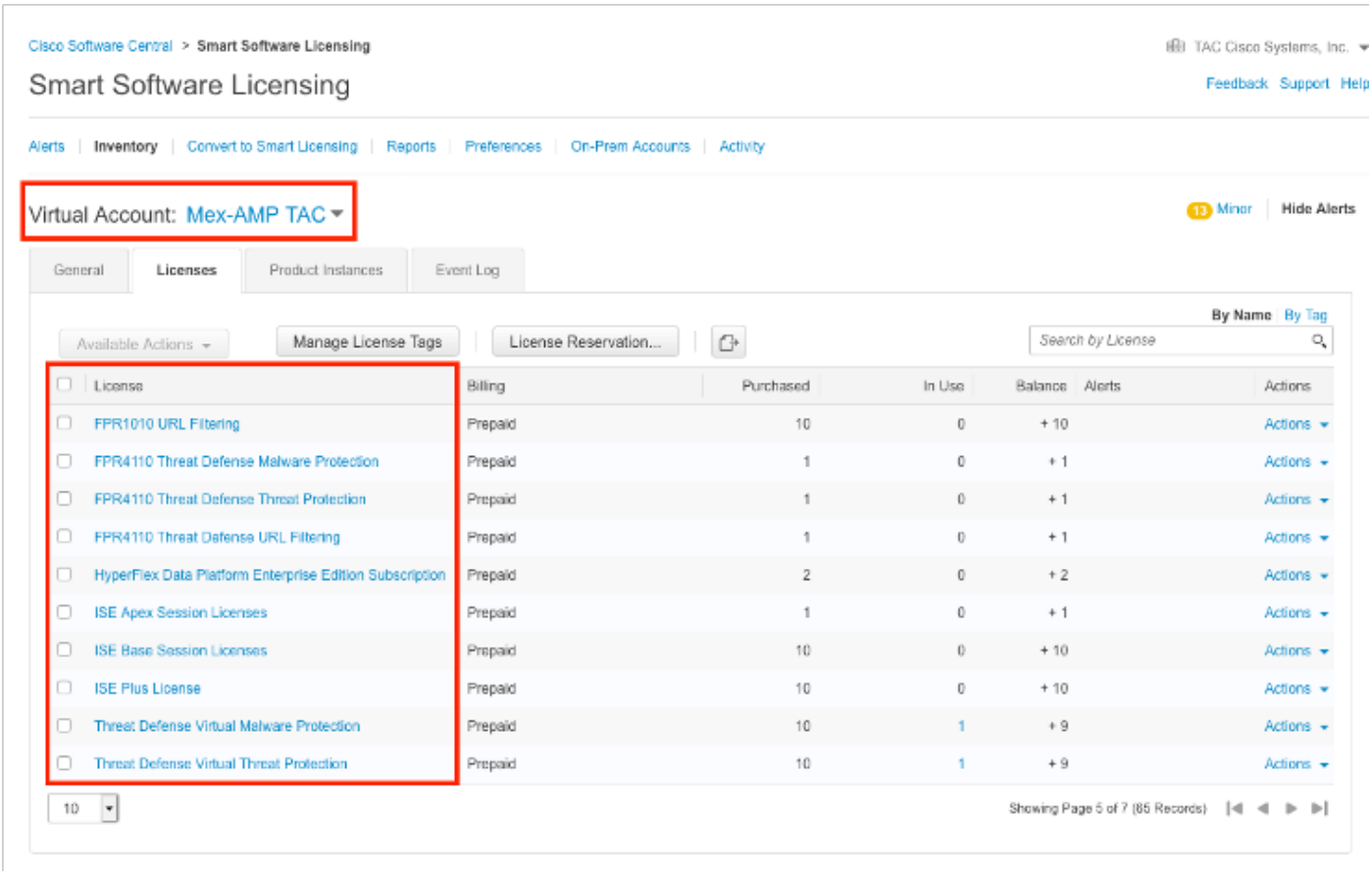
Etapa 1. Para validar a função de Smart Account, navegue até **software.cisco.com** e, no **menu Administração**, selecione **Gerenciar Smart Account**.



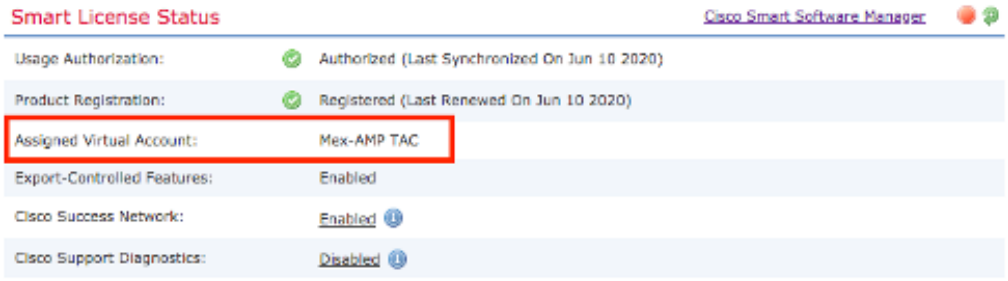
Etapa 2. Para validar a função de usuário, navegue até **Usuários** e valide se, em Funções, as contas estão definidas para ter o Administrador de Virtual Account, como mostrado na imagem.



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

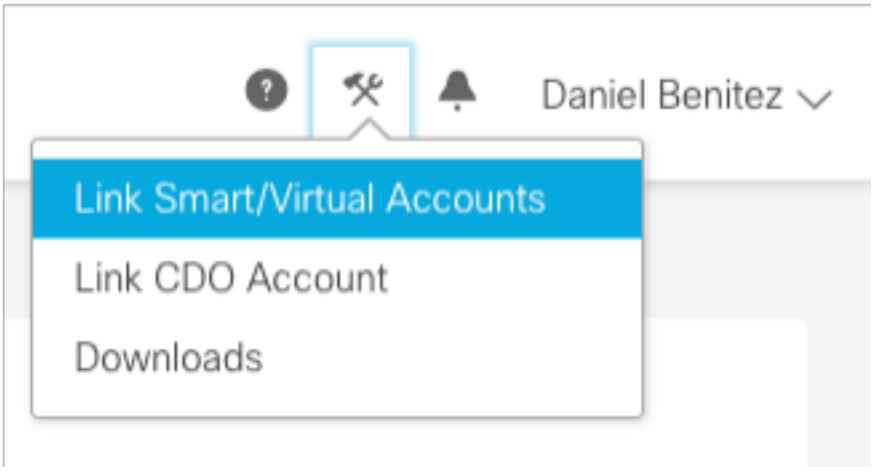


Etapa 4. Para validar que o FMC foi registrado na Virtual Account correta, navegue para **System>Licenses>Smart License:**



Vincule suas contas ao SSE e registre os dispositivos.

Etapa 1. Ao fazer logon na sua conta SSE, você precisa vincular sua Smart Account à sua conta SSE, pois você precisa clicar no ícone de ferramentas e selecionar **Vincular contas**.



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

Registrar os dispositivos no SSE

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

Região dos EUA

- api-sse.cisco.com

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

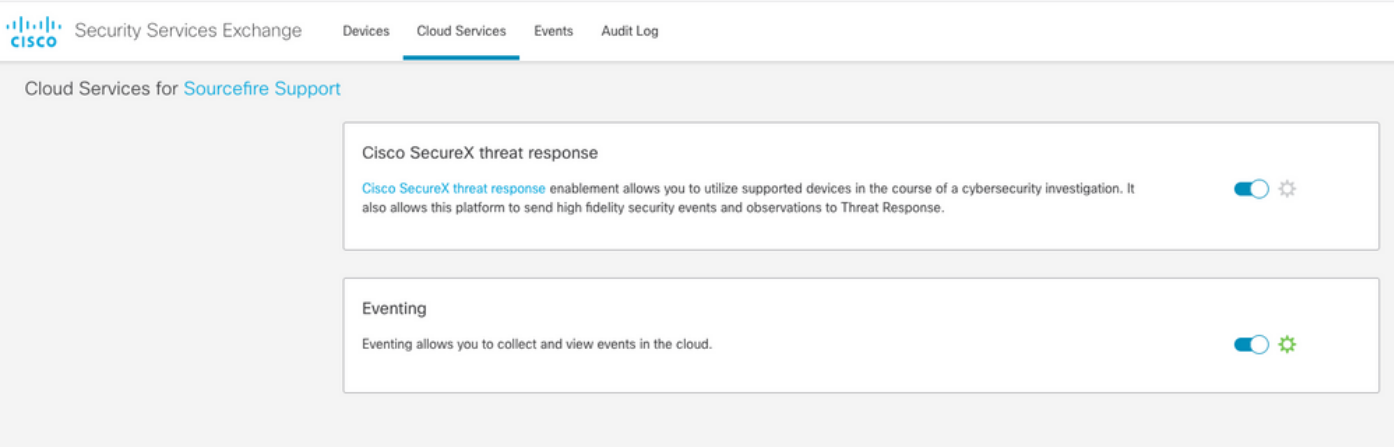
Região da UE

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

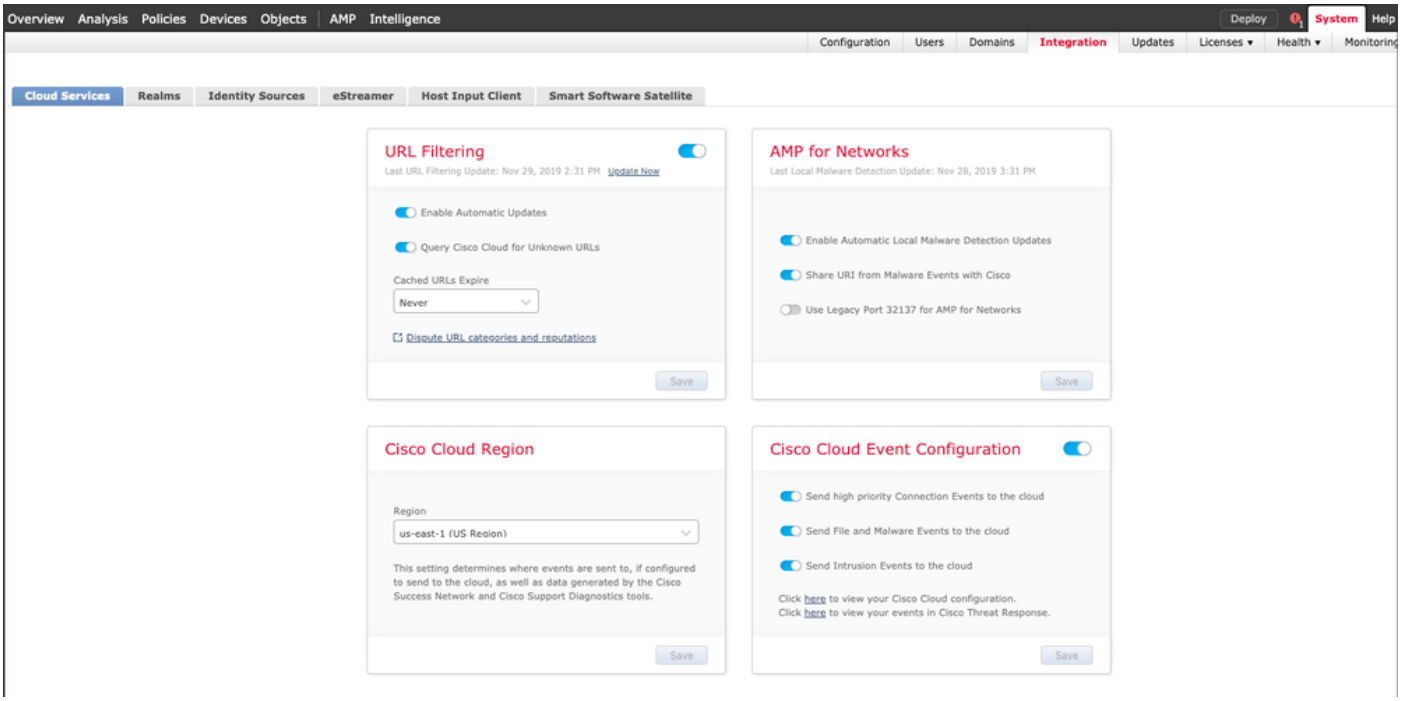
Região APJ

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

Etapa 2. Efetue login no portal SSE com este URL https://admin.sse.itd.cisco.com, navegue para **serviços em nuvem** e habilite as duas opções **Eventos** e **resposta a ameaças do Cisco SecureX**, como mostrado na próxima imagem:

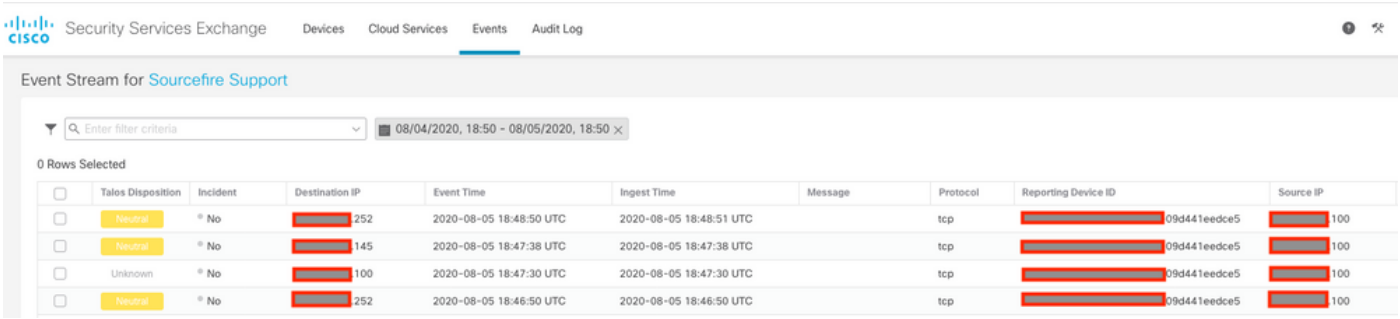


Etapa 3. Faça login no Firepower Management Center e navegue até **System>Integration>Cloud Services**, ative **Cisco Cloud Event Configuration** e selecione os eventos que deseja enviar para a nuvem:



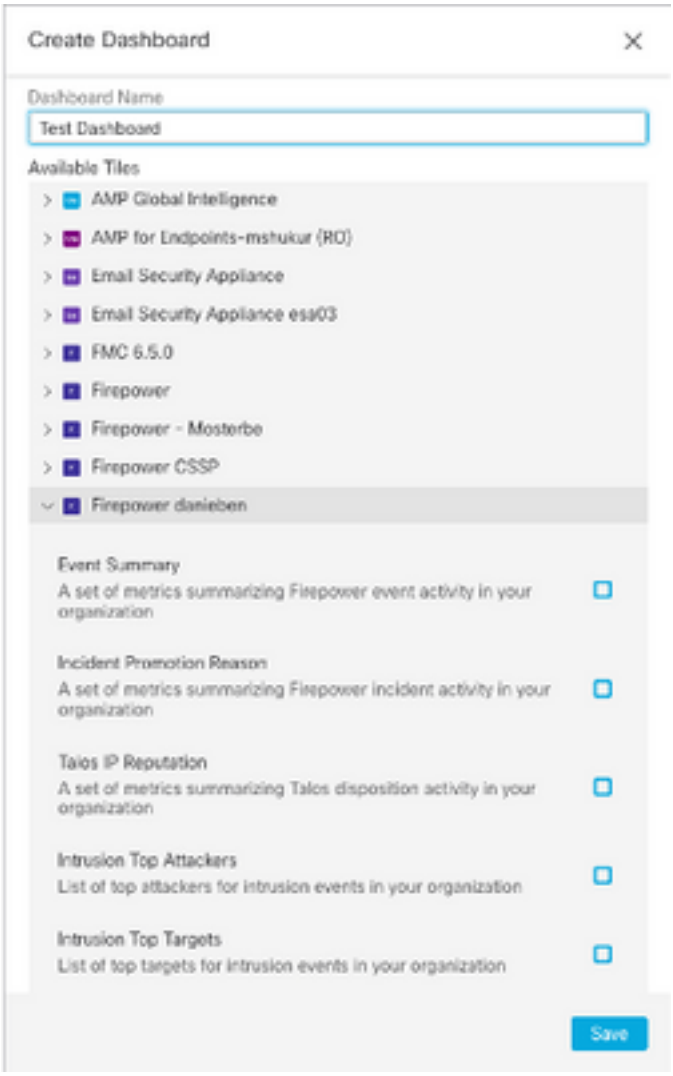
Etapa 4. Você pode voltar ao portal SSE e confirmar que agora você pode ver os dispositivos registrados no SSE:

Os eventos são enviados pelos dispositivos FTD, navegue até os **eventos** no portal SSE para verificar os eventos enviados pelos dispositivos ao SSE, como mostrado na imagem:

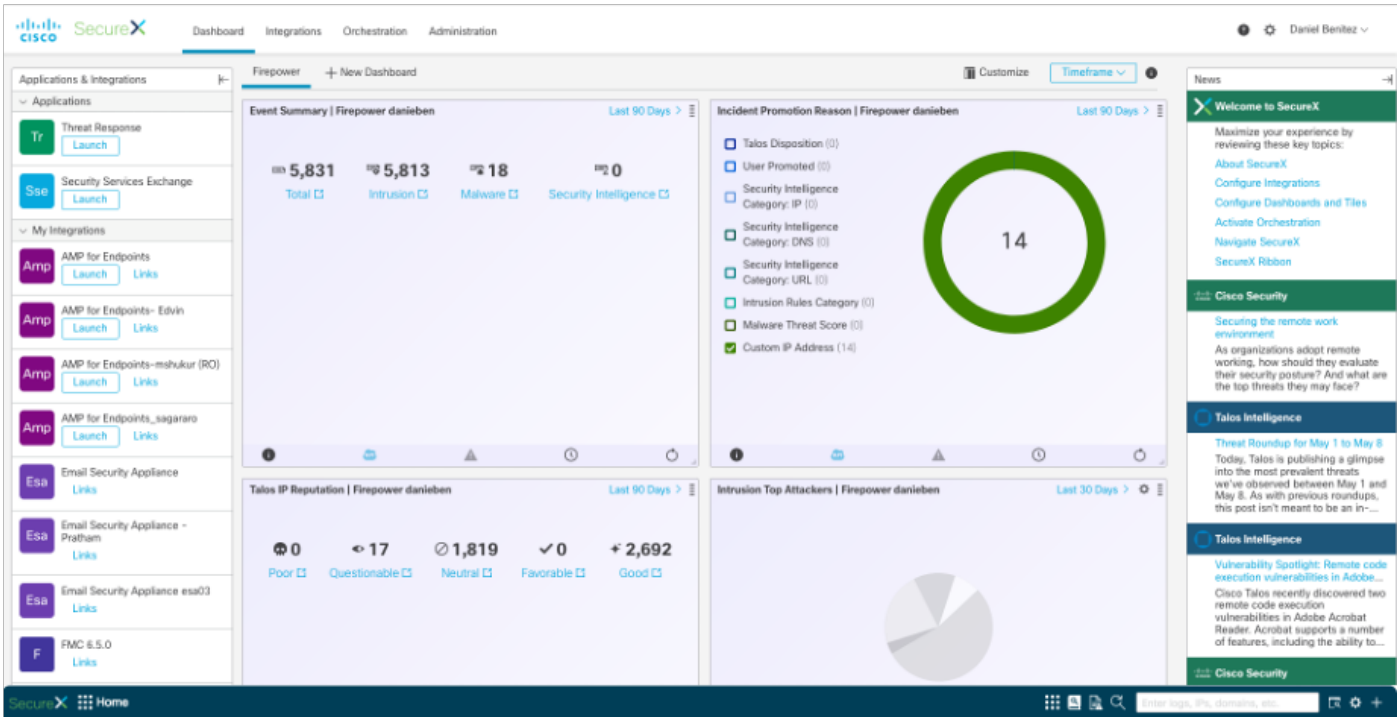


Configurar Painéis Personalizados No SecureX

Etapa 1. Para criar seu Painel, clique no ícone **+ Novo Painel**, Selecione um nome e um Mosaico que deseja usar para o Painel, como mostrado na imagem:



Etapa 2. Depois disso, você poderá ver as informações do painel preenchidas a partir do SSE, poderá selecionar qualquer uma das ameaças detectadas e o portal SSE será iniciado com o filtro de Tipo de evento:



Verificar

Valide se os FTDs geram eventos (malware ou invasão); para eventos de invasão, navegue para **Analysis >Files>Eventos de malware, para eventos de invasão, navegue até Analysis>Intrusion>Events.**

Valide se os eventos estão registrados no portal SSE conforme mencionado na seção **Registrar os dispositivos no SSE**, etapa 4**.**

Confirme se as informações são exibidas no painel do SecureX ou verifique os registros da API para que você possa ver o motivo de uma possível falha da API.

Troubleshoot

Detectar problemas de conectividade

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

```
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.
```

Nesse caso, o código de saída 28 significa que a operação expirou e devemos verificar a conectividade com a Internet. Você também pode ver o código de saída 6, o que significa problemas com a resolução DNS

Problemas de conectividade devido à resolução de DNS

Etapa 1. Verifique se a conectividade funciona 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'
```

A saída acima mostra que o dispositivo não consegue resolver o URL https://api-sse.cisco.com, nesse 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
```

A saída acima mostra que o DNS configurado não foi alcançado, para confirmar as configurações de 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 desta 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 portal SSE

O FMC e o FTD precisam de uma conexão com os URLs SSE em sua interface de gerenciamento, para testar a conexão, insira estes comandos na CLI do Firepower com acesso raiz:

```
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
```

A verificação de 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 proibido, pois os parâmetros enviados do teste não são o que o SSE espera, mas isso prova o suficiente para validar a conectividade.

Verificar o estado do SSEConnector

Você pode verificar as propriedades do conector como 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 este comando, este é um exemplo de uma conexão incorreta:

```
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
```

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

Verificar os dados enviados ao portal SSE e CTR

Para enviar eventos do dispositivo FTD para VER, 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 SSE e o 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)
```

Nos registros 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"
```

> **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 podem mudar, é por isso que a recomendação é permitir o tráfego ao portal SSE com base em URL em vez de endereços IP.

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

Vídeo