# Geïntegreerde en probleemoplossing met Secure Power Threat Defense (FTD)

## Inhoud



## Inleiding

Dit document beschrijft de stappen die vereist zijn om SecureX met Firepower Firepower Threat Defense (FTD) te integreren, controleren en oplossen.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- FireSIGHT Management Center (FMC)
- Firepower Threat Defense (FTD)
- Optioneel virtualisatie van afbeeldingen

### Gebruikte componenten

- Firepower Threat Defense (FTD) - 6.5
- Firepower Management Center (FMC) - 6.5
- Security Services exchange (SSE)
- SecureX

- Smart License Portal

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

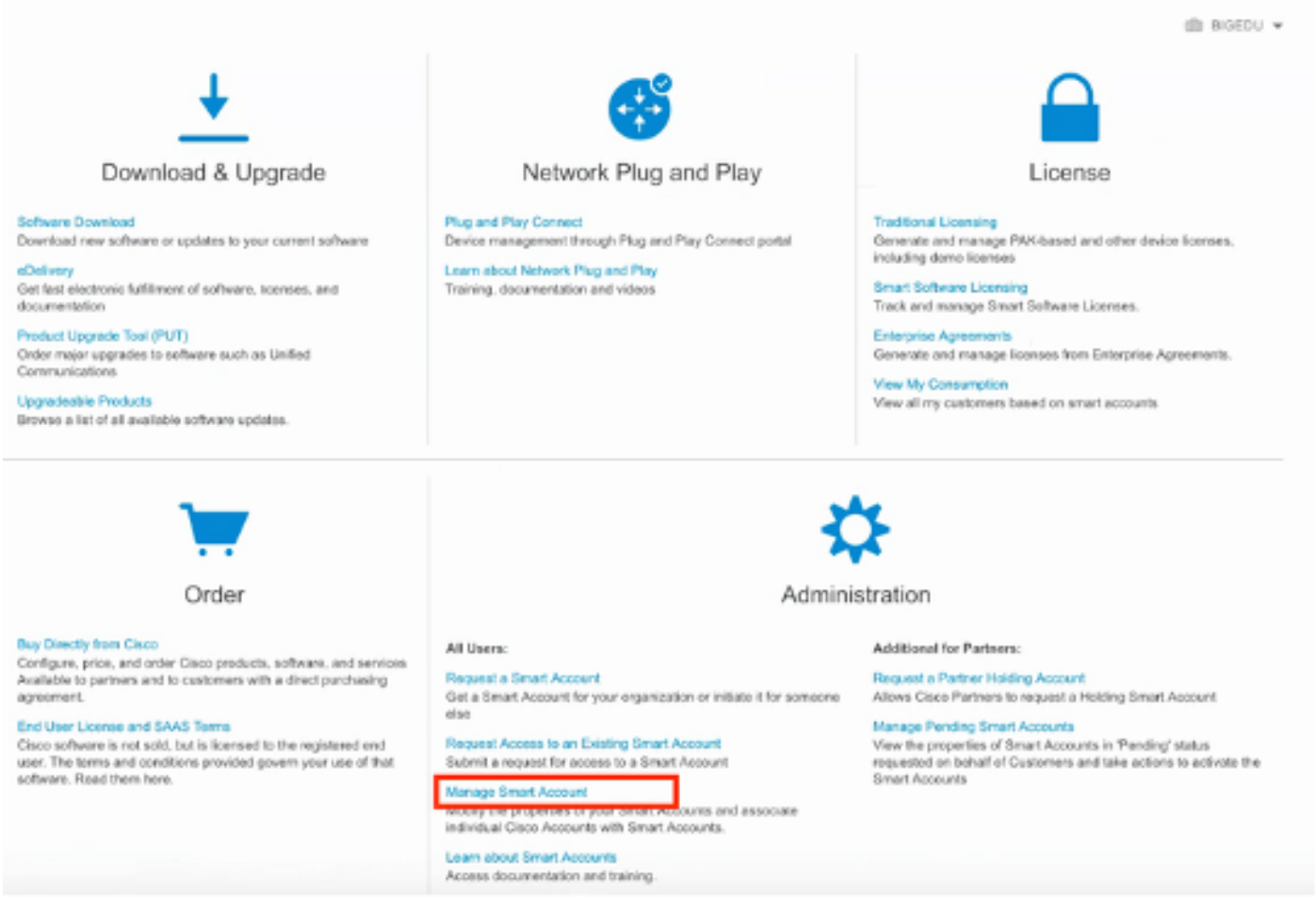
# Configureren

## Licentie

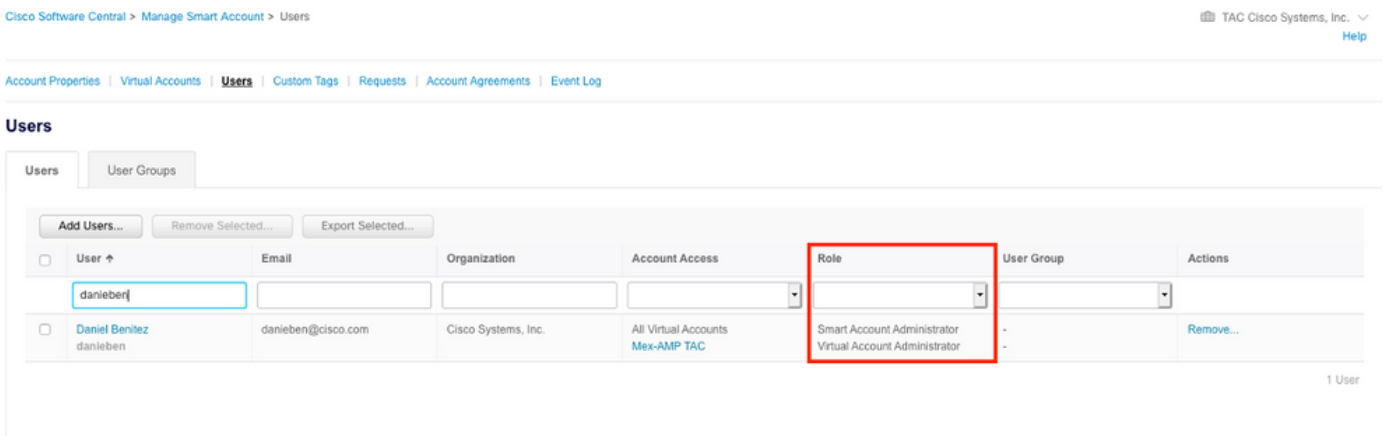
Virtuele accountrollen:

Alleen de Virtual Account Admin of de Smart Account Admin heeft het voorrecht om de slimme account met de SSE-account te verbinden.

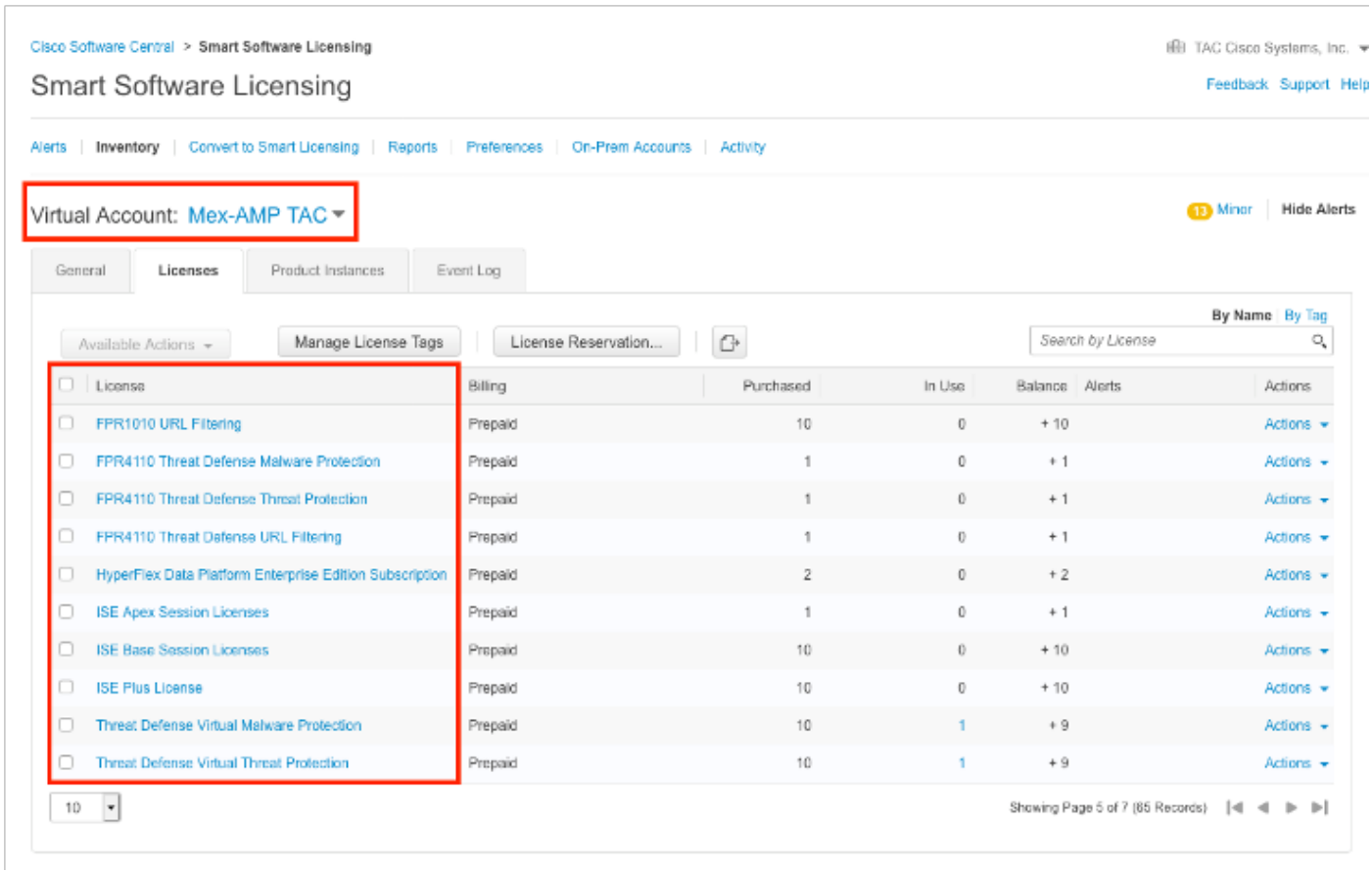
Stap 1. Om de slimme accountrol te valideren, navigeer dan naar **software.cisco.com** en **selecteer Smart Account** beheren **in** het **menu** Beheer.




Stap 2. Om de gebruikersrol te valideren, moet u naar **gebruikers** navigeren en valideren dat onder Roles de rekeningen worden ingesteld op een virtuele accountbeheerder, zoals in de afbeelding wordt weergegeven.




Stap 3. Zorg ervoor dat de virtuele account die op SSE is geselecteerd voor koppeling, de licentie voor de beveiligingsapparaten bevat als een account dat de beveiligingslicentie niet bevat, op SSE is gekoppeld, de beveiligingsapparaten en de gebeurtenis niet op het SSE-portaal verschijnt.




Stap 4. Om te bevestigen dat het FMC is geregistreerd op de juiste virtuele account, navigeer dan naar **Systeem>Licenties>Smart Licentie:**

Smart License Status — Cisco Smart Software Manager

| | |
|---|---|
| Usage Authorization: | Authorized (Last Synchronized On Jun 10 2020) |
| Product Registration: | Registered (Last Renewed On Jun 10 2020) |
| Assigned Virtual Account: | Mex-AMP TAC |
| Export-Controlled Features: | Enabled |
| Cisco Success Network: | Enabled |
| Cisco Support Diagnostics: | Disabled |

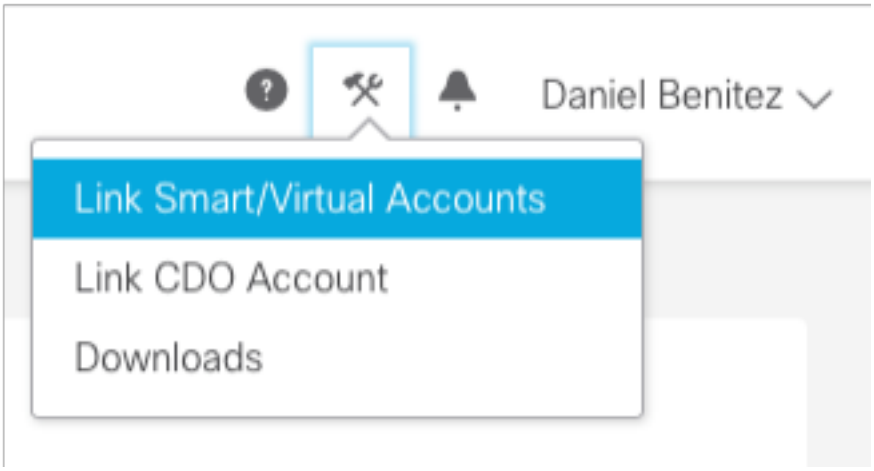
Smart Licenses

| License Type/Device Name | License Status |
|---|---|
| Firepower Management Center Virtual (1) | |
| Base (1) | |
| Malware (1) | |
| Threat (1) | |
| URL Filtering (1) | |
| AnyConnect Apex (1) | |
| AnyConnect Plus (1) | |
| AnyConnect VPN Only (0) | |

Note: Container Instances of same blade share feature licenses

## Koppel uw rekeningen aan SSE en registreer de apparaten.

Stap 1. Wanneer u zich aanmeldt bij uw SSE-account, moet u uw slimme account aan uw SSE-account koppelen, zodat u op het pictogram Gereedschappen moet klikken en **Link Account** kunt selecteren.




Zodra de account is gekoppeld, ziet u het Smart Account met alle virtuele accounts.

## Registreer de apparaten in SSE

Stap 1. Zorg ervoor dat deze URL's op uw omgeving zijn toegestaan:

Amerikaanse regio

- api-sse.cisco.com

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

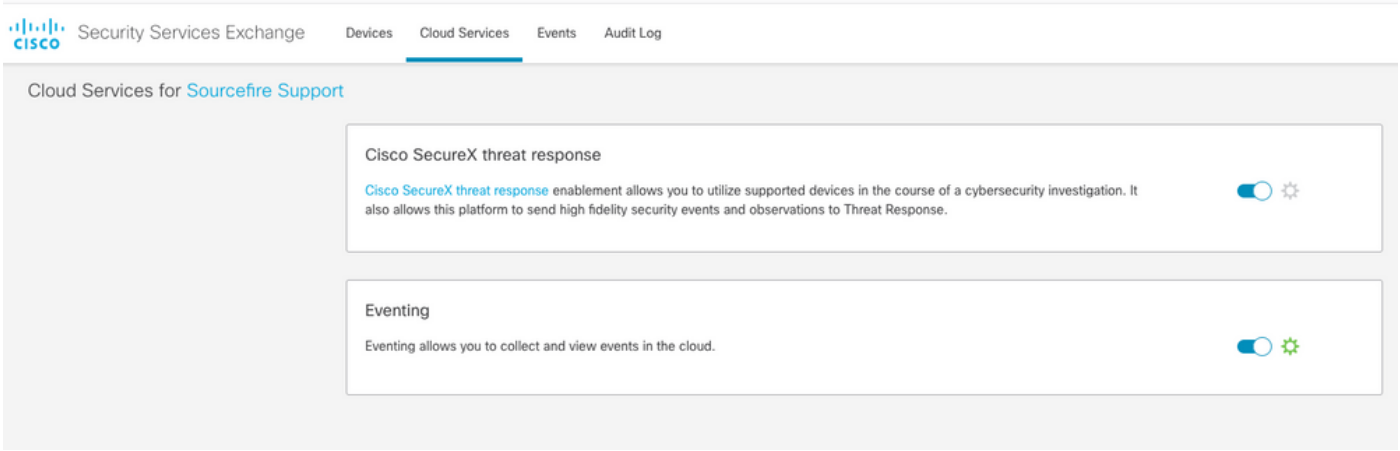
EU-regio

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

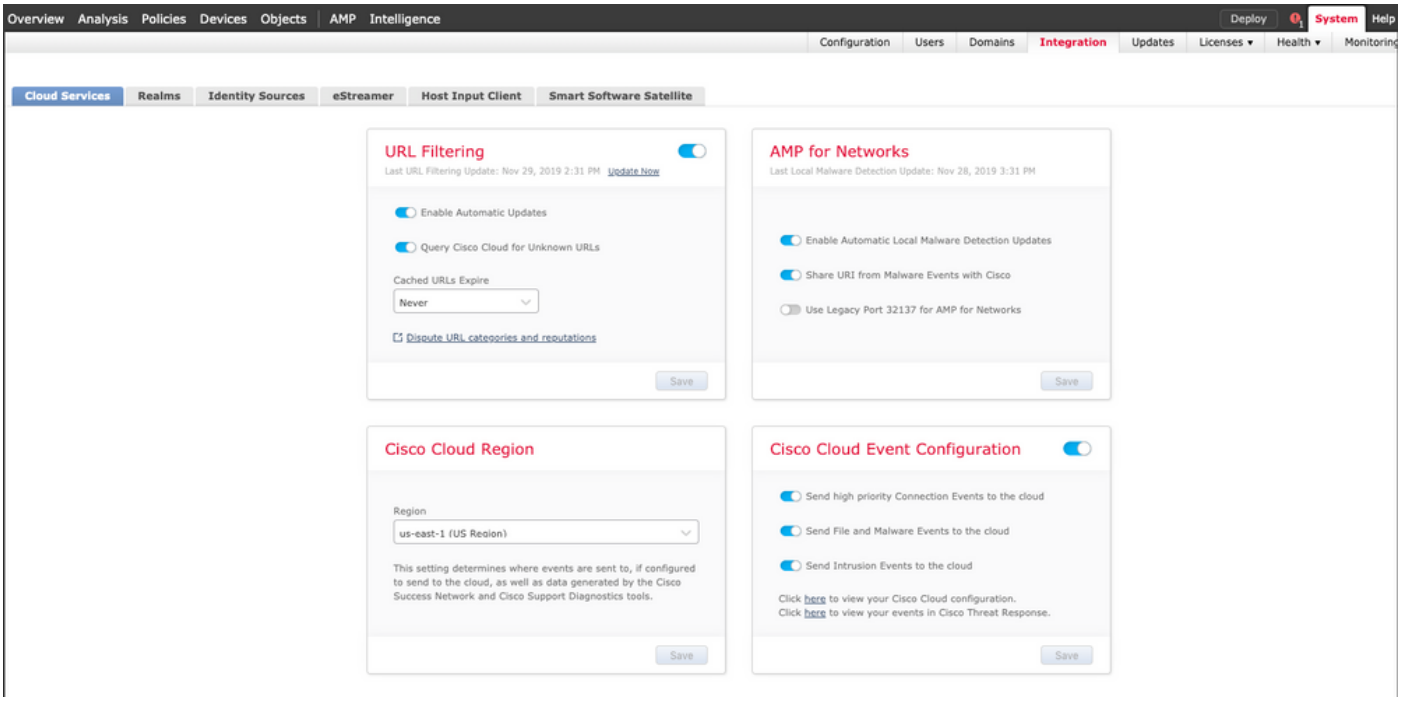
APJ-regio

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

Stap 2. Meld u aan bij het SSE-portal met deze URL https://admin.sse.itd.cisco.com, navigeer naar **cloudservices** en stel beide opties in en **Cisco SecureX-bedreigingsrespons** zoals in de volgende afbeelding:

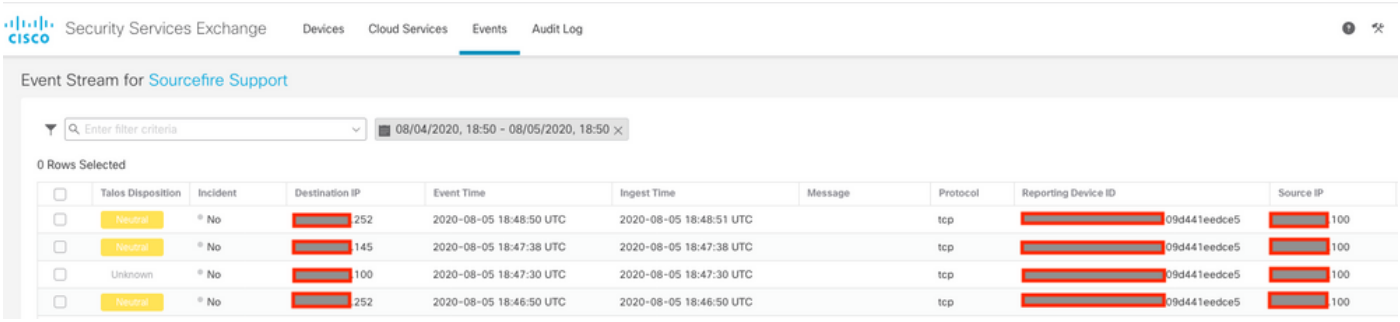



Stap 3. Meld u aan bij het FireSIGHT Management Center en navigeer naar **Systeem>Integratie>Cloudservices**, stelt **Cisco Cloud Event Configuration in** en selecteert u de gebeurtenissen die u naar de cloud wilt verzenden:



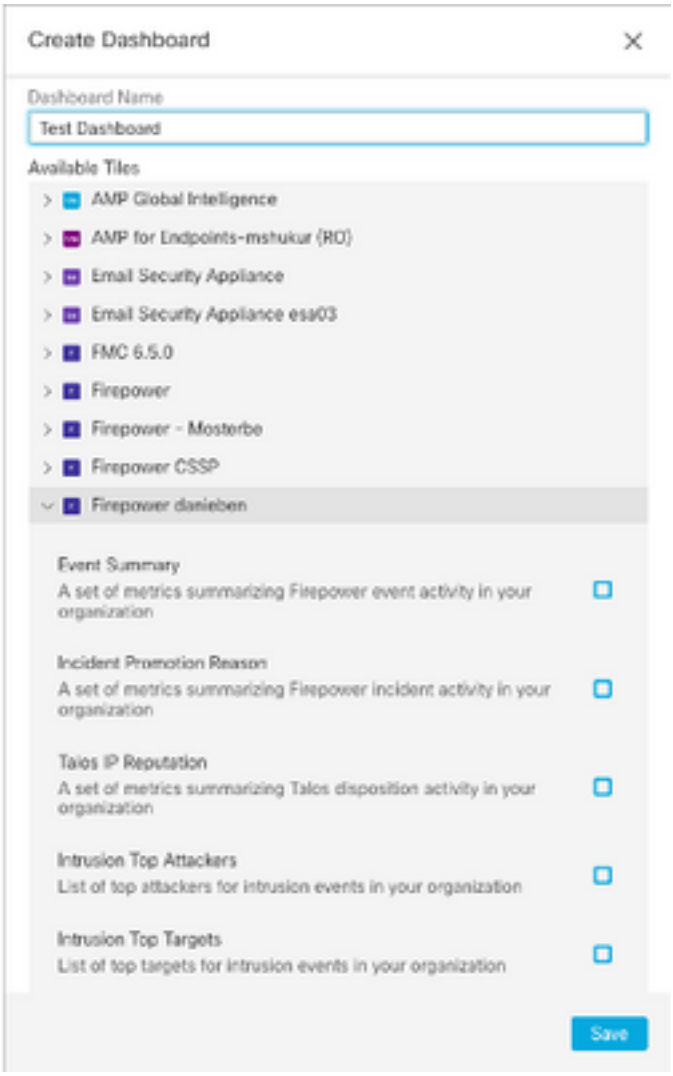

Stap 4. U kunt teruggaan naar het SSE-portal en valideren dat u nu de apparaten kunt zien die in SSE zijn ingevoerd:


De gebeurtenissen worden door de FTD apparaten verstuurd, navigeer naar de **gebeurtenissen** in het SSE portal om de gebeurtenissen te controleren die door de apparaten naar SSE worden verstuurd, zoals in de afbeelding:

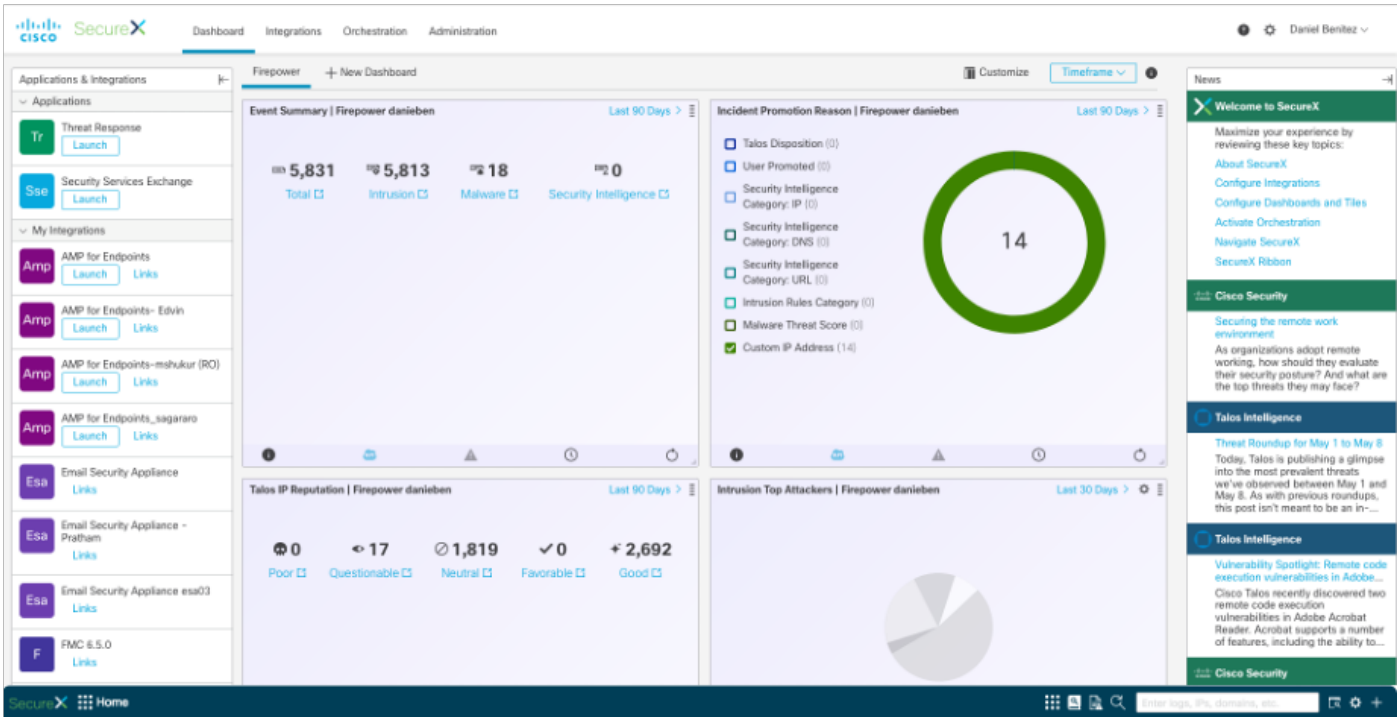



## Aangepaste dashboards op SecureX configureren

Stap 1. Als u uw Dashboard wilt maken, klikt u op in het pictogram **+ New Dashboard**, selecteert u een naam en een bestand dat u voor het Dashboard wilt gebruiken, zoals in de afbeelding:




Stap 2. Nadat u de Dashboard-informatie kunt zien die met SSE gevuld is, kunt u een van de gedetecteerde bedreigingen selecteren en het SSE-portal start met het filter Event Type op deze pagina:



# Verifiëren

Bevestig dat de FTD's gebeurtenissen genereren (malware of inbraakverschijnselen), voor inbraakgebeurtenissen navielen om **Analyse>Bestanden>Malware Event, voor inbraakgebeurtenissen, navigeer naar Analyse>Inbraakgebeurtenissen.**

Bevestig de gebeurtenissen die op het SSE-portaal zijn geregistreerd zoals vermeld in het **Registreer de apparaten aan SSE** sectie stap 4**.**

Bevestig dat informatie op het SecureX-dashboard wordt weergegeven of controleer de API-logbestanden zodat u de reden voor een mogelijke API-fout kunt zien.

# Problemen oplossen

## Connectiviteitsproblemen detecteren

U kunt generieke aansluitingsproblemen detecteren in het action_wachtrij.log bestand. In gevallen van falen kunt u dergelijke logs in het bestand zien:

```
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.
```

In dit geval betekent exit code 28 een time-out voor de bewerking en moeten we de connectiviteit op het internet controleren. Mogelijk ziet u ook exit code 6, wat problemen met DNS-oplossing betekent

## Connectiviteitsproblemen door DNS-resolutie

Stap 1. Controleer of de connectiviteit correct werkt.

```
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'
```

Bovenstaande uitvoer toont aan dat het apparaat niet in staat is om de URL op te lossen https://api-sse.cisco.com, in dit geval moeten we valideren dat de juiste DNS server is geconfigureerd, het kan worden gevalideerd met een upgrade van de deskundige CLI:

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

De bovenstaande uitvoer toont aan dat de DNS-instelling niet is bereikt en gebruik de opdracht **Netwerk** om de DNS-instellingen te bevestigen:

```
> 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
```

In dit voorbeeld werd de verkeerde DNS-server gebruikt, u kunt de DNS-instellingen met deze opdracht wijzigen:

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

Nadat deze verbinding opnieuw kan worden getest en deze keer is de verbinding succesvol.

```
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;
```

## Registratieproblemen bij SSE-portal

Zowel FMC als FTD hebben een verbinding nodig met de SSE URL's op hun beheerinterface om de verbinding te testen, om deze opdrachten in te voeren in de Firepower CLI met worteltoegang:

**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**

De certificaatcontrole kan met deze opdracht worden omzeild:

```
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;
```

**Opmerking:** Je krijgt het 403 Verboden bericht omdat de parameters die uit de test worden verstuurd niet zijn wat SSE verwacht, maar dit bewijst genoeg om connectiviteit te valideren.

## Controleer de SSECconnector-status

U kunt de verbindingseigenschappen zoals getoond verifiëren.

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

Om de connectiviteit tussen de SSCconnector en de EventHandler te controleren kunt u deze opdracht gebruiken, is dit een voorbeeld van een slechte verbinding:

```
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
```

In het voorbeeld van een gevestigde verbinding kunt u zien dat de stream status verbonden is:

```
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
```

## Controleer gegevens die naar het SSE-portaal en de CTR zijn verzonden

Om gebeurtenissen van het FTD-apparaat naar SEE te kunnen versturen moet een TCP-verbinding tot stand worden gebracht met https://eventing-ingest.sse.itd.cisco.com Dit is een voorbeeld van een verbinding die niet tot stand is gebracht tussen het SSE-portaal en de 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)
```

In de blog 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"
```

> **Opmerking:** Merkte op dat de IP-adressen die x.x.x.246 en 1x.x.x.246 worden weergegeven, tot https://eventing-ingest.sse.itd.cisco.com behoren, wat de reden is dat de aanbeveling het verkeer naar SSE Portal op basis van URL in plaats van IP-adressen toestaat.

Als deze verbinding niet tot stand is gebracht, worden de gebeurtenissen niet naar het SSE-portaal verzonden. Dit is een voorbeeld van een gevestigde verbinding tussen het FTD en het SSE-portaal:

```
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)
```

# Video