Integration und Fehlerbehebung von Cisco XDR mit FirePOWER Threat Defense (FTD)

Inhalt

Einleitung

In diesem Dokument werden die erforderlichen Schritte zur Integration, Überprüfung und Fehlerbehebung von Cisco XDR mit Firepower Firepower Threat Defense (FTD) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)
- Optionale Bildvirtualisierung

Verwendete Komponenten

- Firepower Threat Defense (FTD) - 6.5
- FirePOWER Management Center (FMC) - 6.5
- Security Services Exchange (SSE)
- Cisco XDR
- Smart License-Portal

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

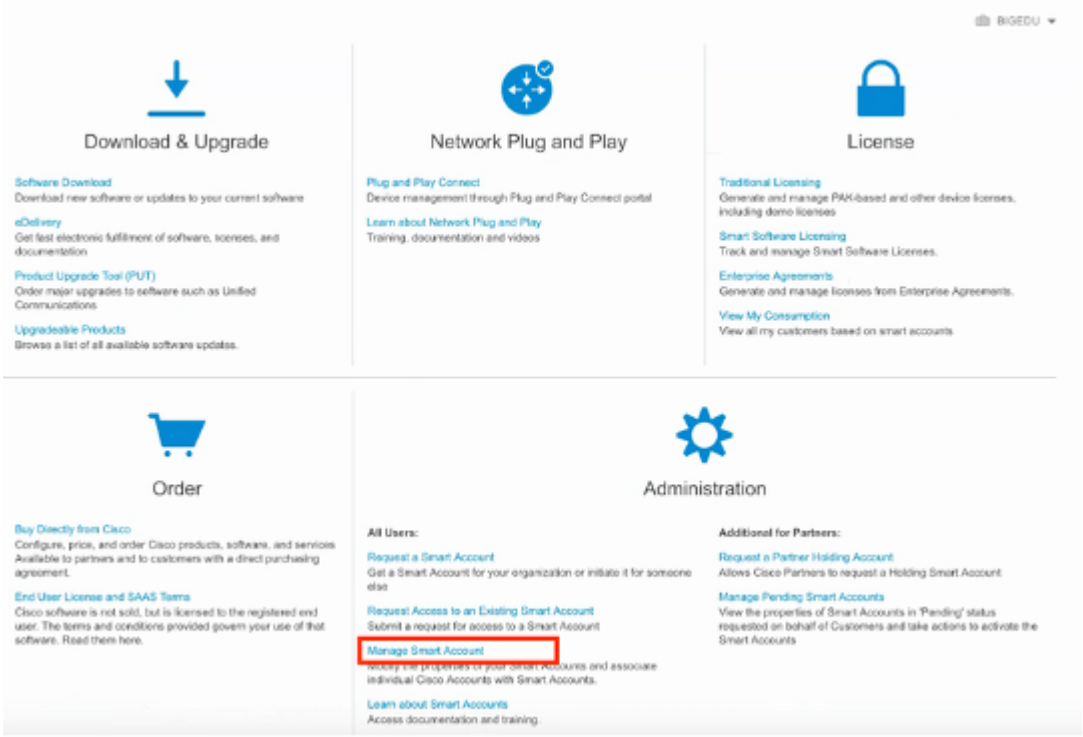
Konfigurieren

Lizenzierung

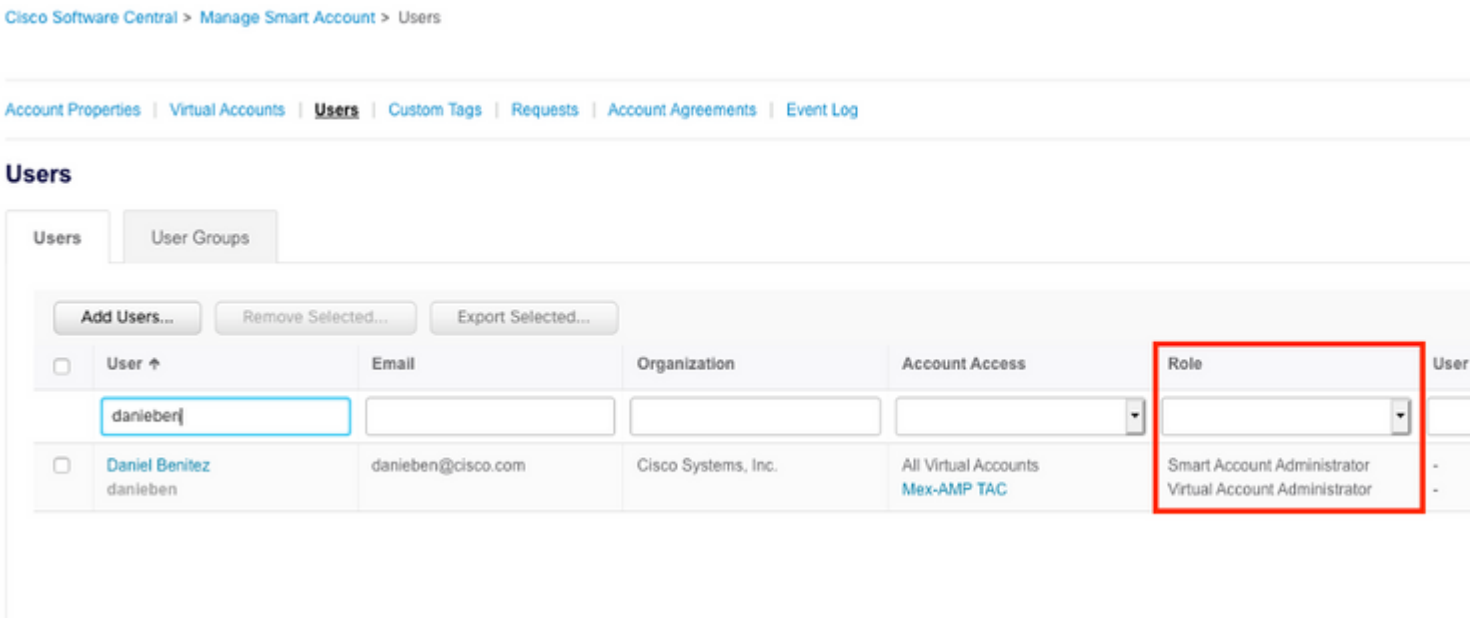
Virtuelle Kontorollen:

Nur der Virtual Account Admin oder der Smart Account Admin sind berechtigt, das Smart Account mit dem SSE-Konto zu verknüpfen.

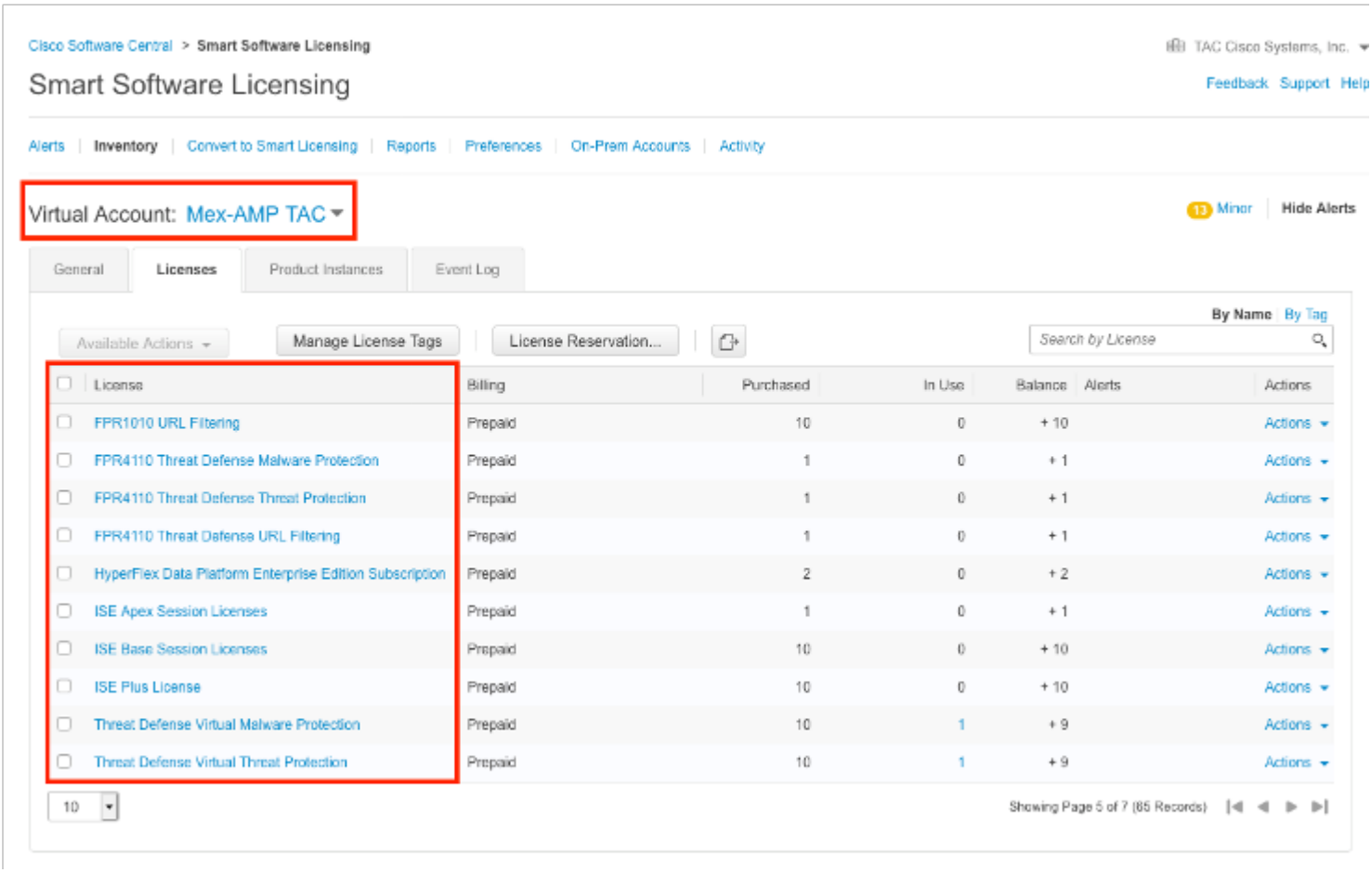
Schritt 1: Um die Smart Account-Rolle zu überprüfen, navigieren Sie zu **software.cisco.com**, und wählen Sie im **Administrationsmenü** die Option **Smart Account verwalten aus**.



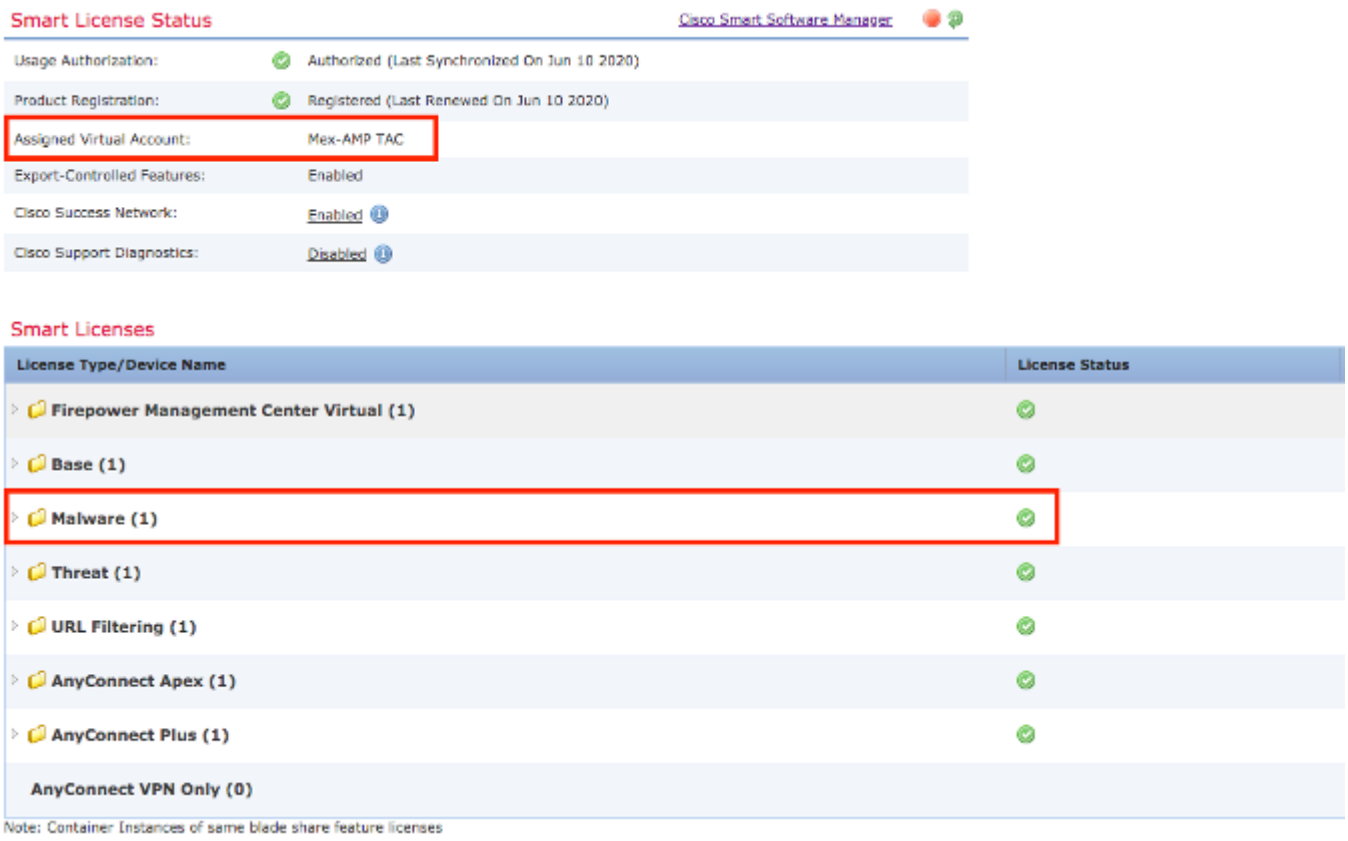
Schritt 2: Um die Benutzerrolle zu validieren, navigieren Sie zu **Benutzer**, und überprüfen Sie, ob die Konten unter Rollen als Virtual Account Administrator konfiguriert sind, wie im Bild gezeigt.



Schritt 3: Stellen Sie sicher, dass das virtuelle Konto, das auf SSE verknüpft werden soll, die Lizenz für die Sicherheitsgeräte enthält, wenn ein Konto, das die Sicherheitslizenz nicht enthält, auf SSE, den Sicherheitsgeräten und dem Ereignis im SSE-Portal nicht angezeigt wird.

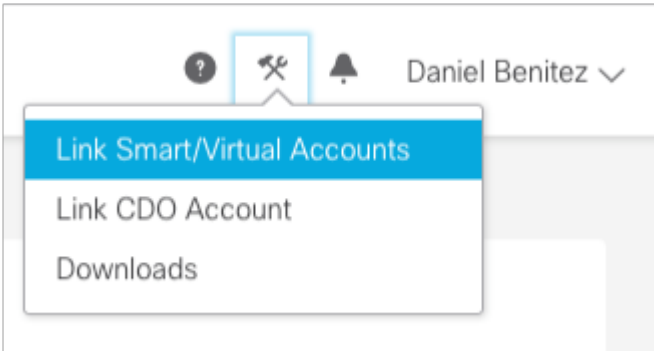


Schritt 4: Um zu überprüfen, ob das FMC beim richtigen Virtual Account registriert wurde, navigieren Sie zu **System>Licenses>Smart License:**



Verknüpfen Sie Ihre Konten mit SSE, und registrieren Sie die Geräte.

Schritt 1: Wenn Sie sich bei Ihrem SSE-Konto anmelden, müssen Sie Ihr Smart Account mit Ihrem SSE-Konto verknüpfen. Dazu müssen Sie auf das Symbol "Tools" klicken und "**Konten verknüpfen**" auswählen.



Sobald das Konto verknüpft ist, wird das Smart Account mit allen virtuellen Konten angezeigt.

Registrieren Sie die Geräte bei SSE.

Schritt 1: Stellen Sie sicher, dass die folgenden URLs in Ihrer Umgebung zulässig sind:

Region USA

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

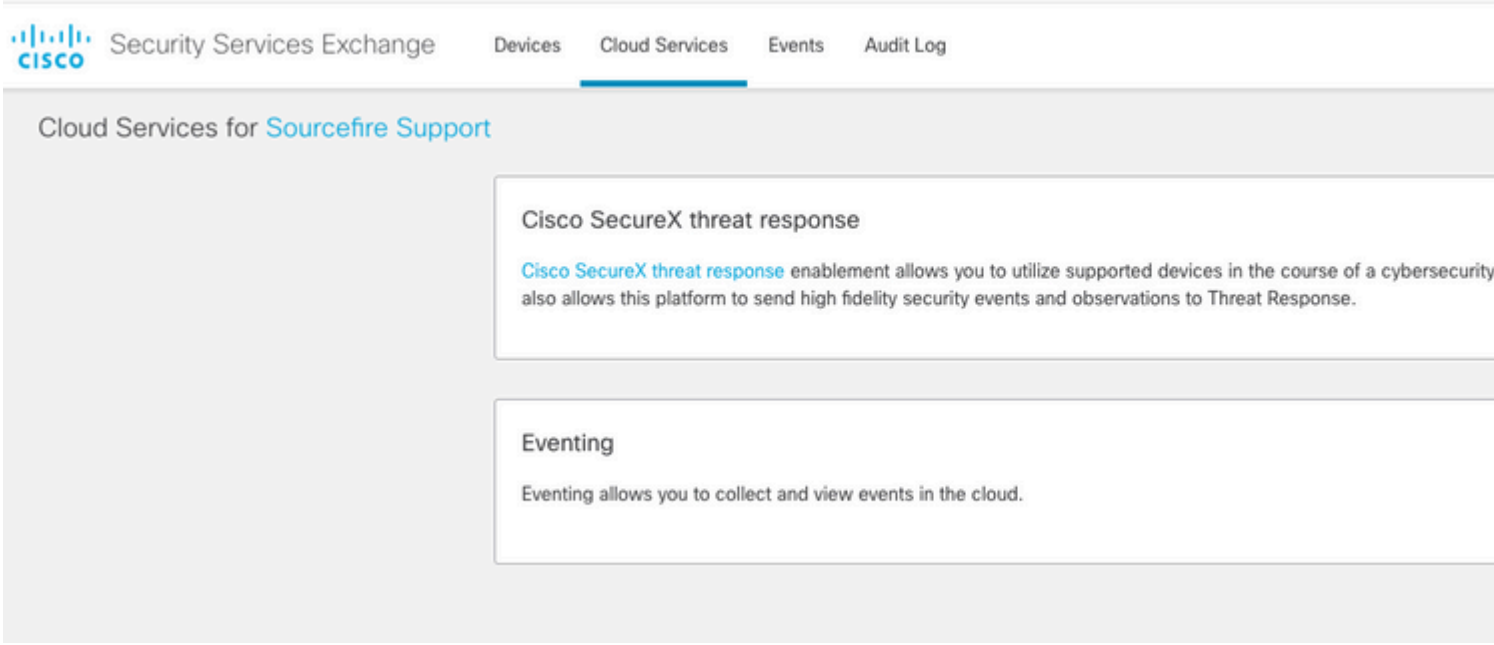
EU-Region

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

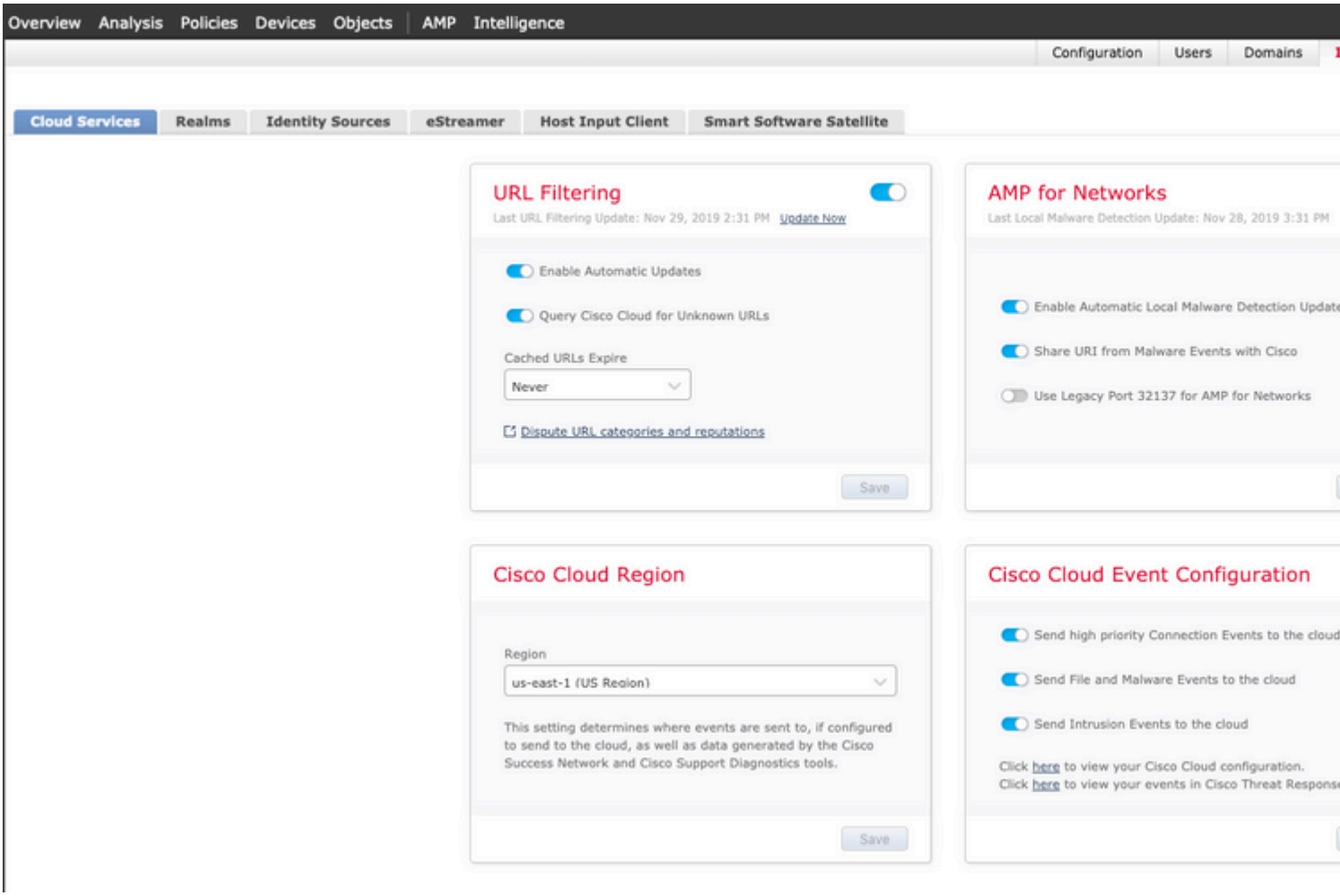
APJ-Region

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

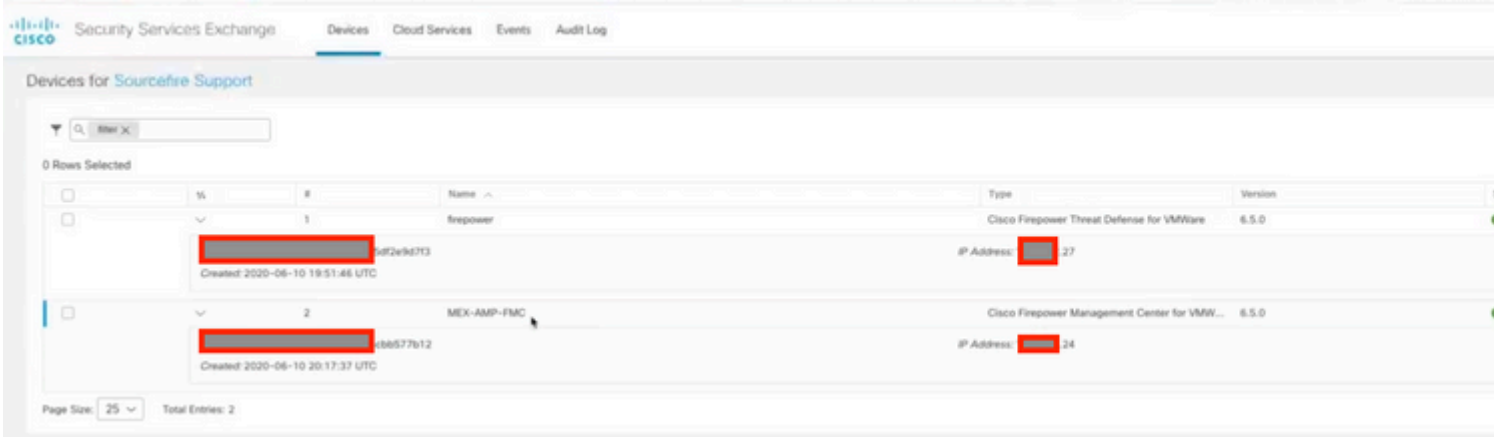
Schritt 2: Melden Sie sich mit folgender URL beim SSE-Portal an: https://admin.sse.itd.cisco.com, navigieren Sie zu **Cloud Services,** und aktivieren Sie die beiden Optionen **Eventing** und **Cisco XDR Threat Response, wie im folgenden Bild gezeigt:**



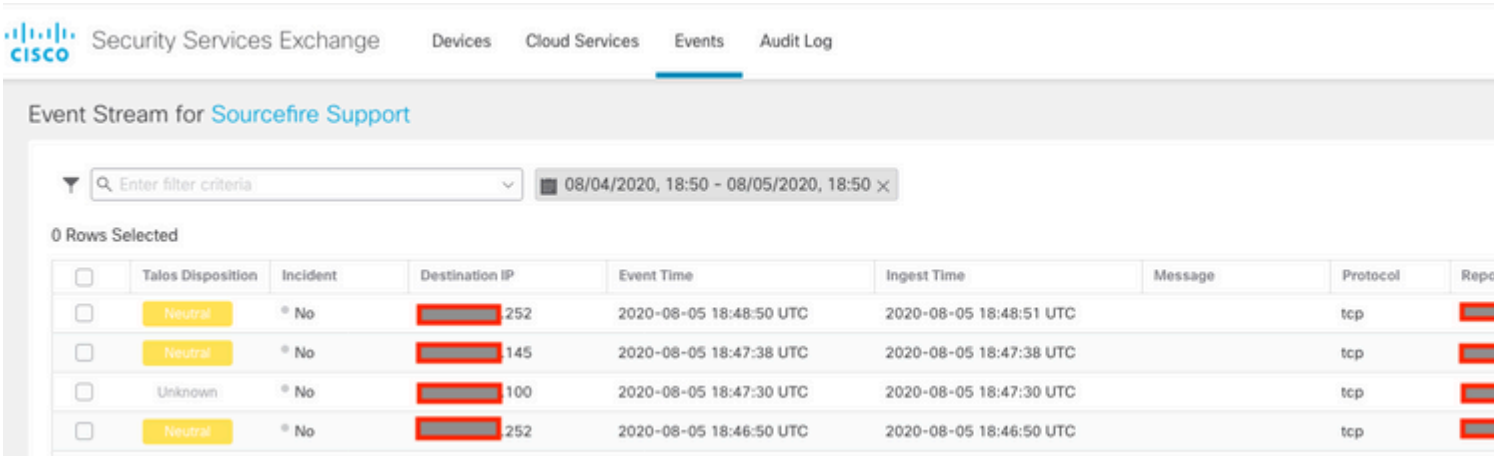
Schritt 3: Melden Sie sich beim FirePOWER Management Center an, navigieren Sie zu **System>Integration>Cloud-Services,** aktivieren Sie die **Cisco Cloud Event Configuration,** und wählen Sie die Ereignisse aus, die Sie an die Cloud senden möchten:



Schritt 4: Sie können zum SSE-Portal zurückkehren und überprüfen, ob die bei SSE registrierten Geräte jetzt angezeigt werden:



Die Ereignisse werden von den FTD-Geräten gesendet. Navigieren Sie zu den **Ereignissen** auf dem SSE-Portal, um die Ereignisse zu überprüfen, die von den Geräten an SSE gesendet werden, wie in der Abbildung dargestellt:



Überprüfung

Überprüfen Sie, ob FTDs Ereignisse generieren (Malware oder unbefugter Zugriff), und navigieren Sie zu **Analyse>Dateien>Malware-Ereignisse**; für Angriffsversuche navigieren Sie zu **Analyse > Angriffsversuche > Ereignisse.**

Validieren Sie, dass die Ereignisse im SSE-Portal registriert werden, wie im Abschnitt **Registrieren der Geräte für SSE** in Schritt 4 erwähnt**..**

Überprüfen Sie, ob die Informationen im Cisco XDR-Dashboard angezeigt werden, oder überprüfen Sie die API-Protokolle, um den Grund für einen möglichen API-Fehler zu ermitteln.

Fehlerbehebung

Erkennen von Verbindungsproblemen

Sie können generische Verbindungsprobleme aus der Datei action_queue.log erkennen. Bei einem Fehler werden die Protokolle in der Datei angezeigt:

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

In diesem Fall bedeutet Exitcode 28, dass der Vorgang abgelaufen ist, und wir müssen die Verbindung zum Internet überprüfen. Sie müssen auch Code 6 zum Beenden sehen, was bedeutet, dass Probleme mit der DNS-Auflösung auftreten.

Verbindungsprobleme aufgrund von DNS-Auflösung

Schritt 1: Überprüfen Sie, ob die Verbindung ordnungsgemäß funktioniert.

```
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'
```

Diese Ausgabe zeigt, dass das Gerät nicht in der Lage ist, die URL https://api-sse.cisco.com aufzulösen. In diesem Fall müssen wir überprüfen, ob der richtige DNS-Server konfiguriert ist. Er kann mit einem nslookup aus der CLI des Experten validiert werden:

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

Diese Ausgabe zeigt an, dass der konfigurierte DNS nicht erreicht wurde. Verwenden Sie zum Bestätigen der DNS-Einstellungen den Befehl **show network (Netzwerk anzeigen**):

```
> 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 diesem Beispiel wurde der falsche DNS-Server verwendet. Sie können die DNS-Einstellungen mit dem folgenden Befehl ändern:

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

Nachdem diese Verbindung erneut getestet werden kann, ist die Verbindung dieses Mal erfolgreich.

```
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;
```

Registrierungsprobleme beim SSE-Portal

Sowohl FMC als auch FTD benötigen eine Verbindung zu den SSE-URLs auf ihrer Verwaltungsschnittstelle. Zum Testen der Verbindung geben Sie die folgenden Befehle in die Firepower-CLI mit Root-Zugriff ein:

<#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

Die Zertifikatsüberprüfung kann mit dem folgenden Befehl umgangen werden:

```
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;
```

Hinweis: Sie erhalten die Meldung 403 Forbidden (403 Verboten), da die vom Test gesendeten Parameter nicht den Erwartungen des SSE entsprechen. Dies ist jedoch ausreichend, um die Verbindung zu validieren.

Überprüfen des SSEConnector-Status

Sie können die Verbindungseigenschaften wie abgebildet überprüfen.

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

Um die Verbindung zwischen SSConnector und EventHandler zu überprüfen, können Sie diesen Befehl verwenden. Dies ist ein Beispiel für eine fehlerhafte Verbindung:

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

Im Beispiel einer bestehenden Verbindung sehen Sie, dass der Stream-Status verbunden ist:

```
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
```

Überprüfen der an das SSE-Portal und den CTR gesendeten Daten

Um Ereignisse vom FTD-Gerät an SEE zu senden, muss eine TCP-Verbindung mit https://eventing-ingest.sse.itd.cisco.com aufgebaut werden. Dies ist ein Beispiel für eine Verbindung, die nicht zwischen dem SSE-Portal und dem FTD hergestellt wurde:

```
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.am
```

In connector.log logs:

```
time="2020-04-13T14:34:02.88472046-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:cor
time="2020-04-13T14:38:18.244707779-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:co
time="2020-04-13T14:42:42.564695622-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:co
time="2020-04-13T14:47:48.484762429-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:co
time="2020-04-13T14:52:38.404700083-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:co
```

> **Hinweis:** Beachten Sie, dass die angezeigten IP-Adressen x.x.x.246 und 1x.x.x.246 zu **https://eventing-ingest.sse.itd.cisco.com** gehören. Daher wird empfohlen, den Datenverkehr zum SSE-Portal basierend auf URL anstelle von IP-Adressen zuzulassen.

Wenn diese Verbindung nicht hergestellt wird, werden die Ereignisse nicht an das SSE-Portal gesendet. Dies ist ein Beispiel für eine bestehende Verbindung zwischen dem FTD und dem SSE-Portal:

```
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.a
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.