

Integrate and Troubleshoot Cisco XDR with Firepower Threat Defense (FTD)

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Licensing](#)

[Link your accounts to SSE and register the devices.](#)

[Register the devices to SSE](#)

Introduction

This document describes the steps required to integrate, verify, and troubleshoot Cisco XDR with Firepower Threat Defense (FTD).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)
- Optional Virtualization of images

Components Used

- Firepower Threat Defense (FTD) - 6.5
- Firepower Management Center (FMC) - 6.5
- Security Services exchange (SSE)
- Cisco XDR
- 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. If your network is live, ensure that you understand the potential impact of any command.

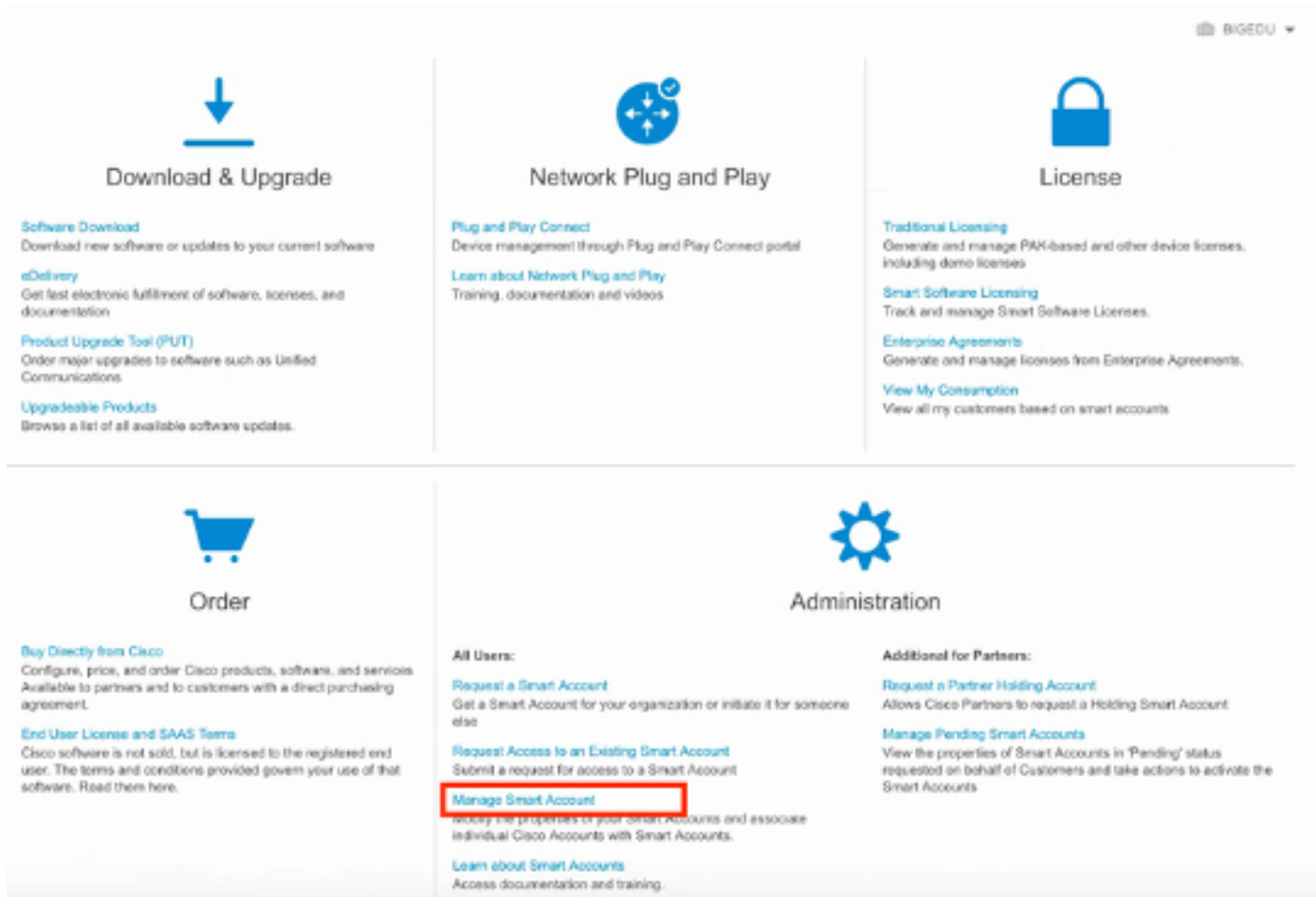
Configure

Licensing

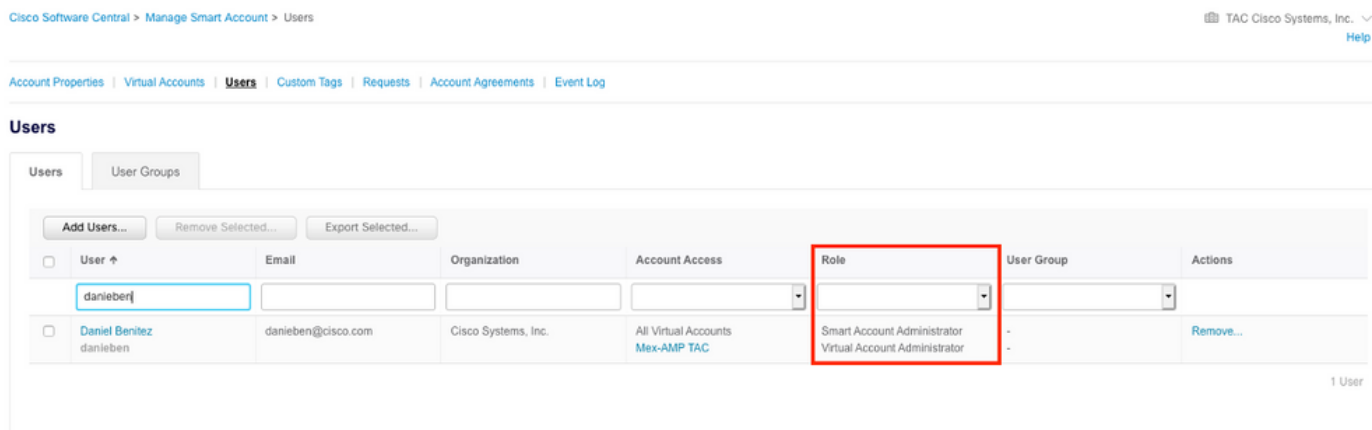
Virtual Account Roles:

Only the Virtual Account Admin or the Smart Account Admin has the privilege to link the smart account with the SSE account.

Step 1. In order to validate the smart account role, navigate to **software.cisco.com** and under the **Administration Menu**, select **Manage Smart Account**.



Step 2. In order to validate the user role, navigate to **Users**, and validate that under Roles the accounts are set to have Virtual Account Administrator, as shown in the image.



Step 3. Ensure the Virtual Account that is selected to link on SSE contains the license for the security devices if an account that does not contain the security license is linked on SSE, the security devices and the event does not appear on the SSE portal.

Cisco Software Central > Smart Software Licensing TAC Cisco Systems, Inc. ▾

Smart Software Licensing

[Feedback](#) [Support](#) [Help](#)

[Alerts](#) | [Inventory](#) | [Convert to Smart Licensing](#) | [Reports](#) | [Preferences](#) | [On-Prem Accounts](#) | [Activity](#)

Virtual Account: **Mex-AMP TAC** 13 Minor | Hide Alerts

General | **Licenses** | Product Instances | Event Log

Available Actions ▾ | Manage License Tags | License Reservation... | 📄

By Name | By Tag

Search by License

<input type="checkbox"/> License	Billing	Purchased	In Use	Balance	Alerts	Actions
<input type="checkbox"/> FPR1010 URL Filtering	Prepaid	10	0	+ 10		Actions ▾
<input type="checkbox"/> FPR4110 Threat Defense Malware Protection	Prepaid	1	0	+ 1		Actions ▾
<input type="checkbox"/> FPR4110 Threat Defense Threat Protection	Prepaid	1	0	+ 1		Actions ▾
<input type="checkbox"/> FPR4110 Threat Defense URL Filtering	Prepaid	1	0	+ 1		Actions ▾
<input type="checkbox"/> HyperFlex Data Platform Enterprise Edition Subscription	Prepaid	2	0	+ 2		Actions ▾
<input type="checkbox"/> ISE Apex Session Licenses	Prepaid	1	0	+ 1		Actions ▾
<input type="checkbox"/> ISE Base Session Licenses	Prepaid	10	0	+ 10		Actions ▾
<input type="checkbox"/> ISE Plus License	Prepaid	10	0	+ 10		Actions ▾
<input type="checkbox"/> Threat Defense Virtual Malware Protection	Prepaid	10	1	+ 9		Actions ▾
<input type="checkbox"/> Threat Defense Virtual Threat Protection	Prepaid	10	1	+ 9		Actions ▾

10 ▾ Showing Page 5 of 7 (85 Records) |◀◀ ▶▶▶

Step 4. To validate that the FMC was registered to the correct Virtual Account, Navigate to **System>Licenses>Smart License**:

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](#) ⓘ

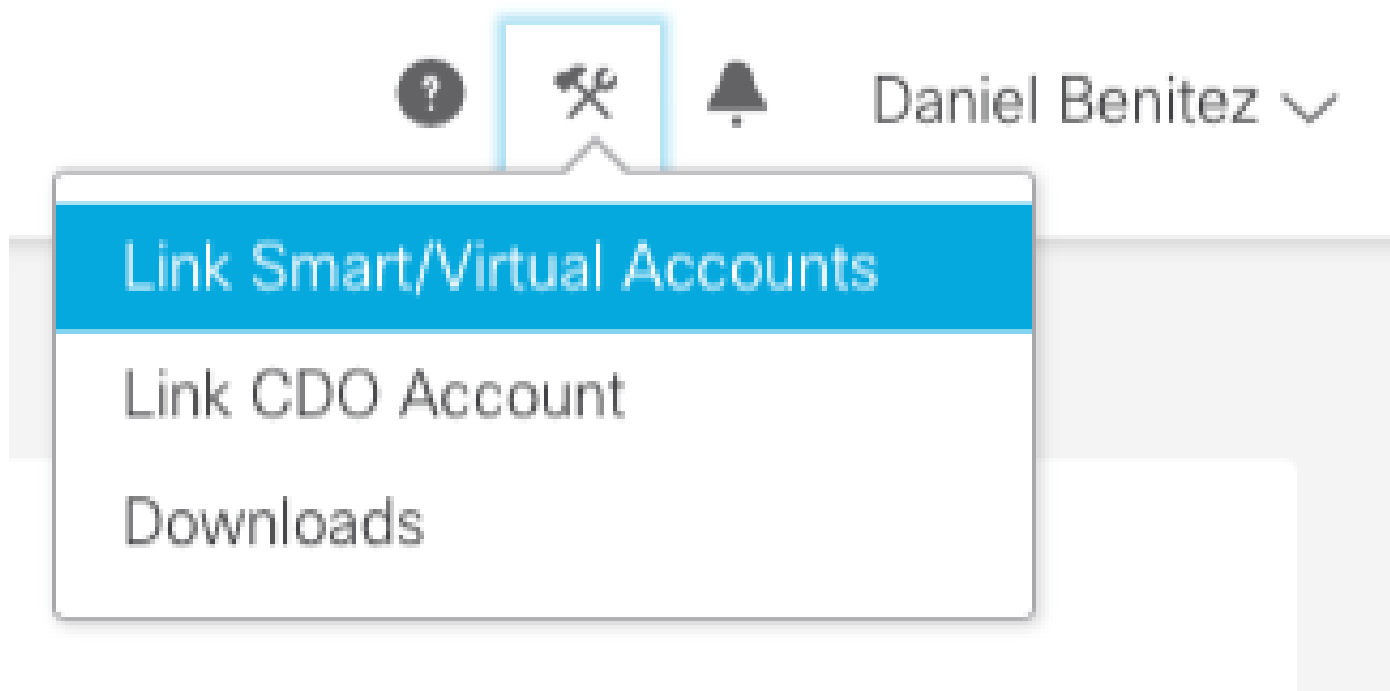
Smart Licenses

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

Link your accounts to SSE and register the devices.

Step 1. When you logon to your SSE account, you have to link your smart account to your SSE account, for that you need to click tools icon and select **Link Accounts**.



Once the account is linked you see the Smart Account with all the Virtual Accounts on it.

Register the devices to SSE

Step 1. Ensure these URLs are allowed on your environment:

US Region

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

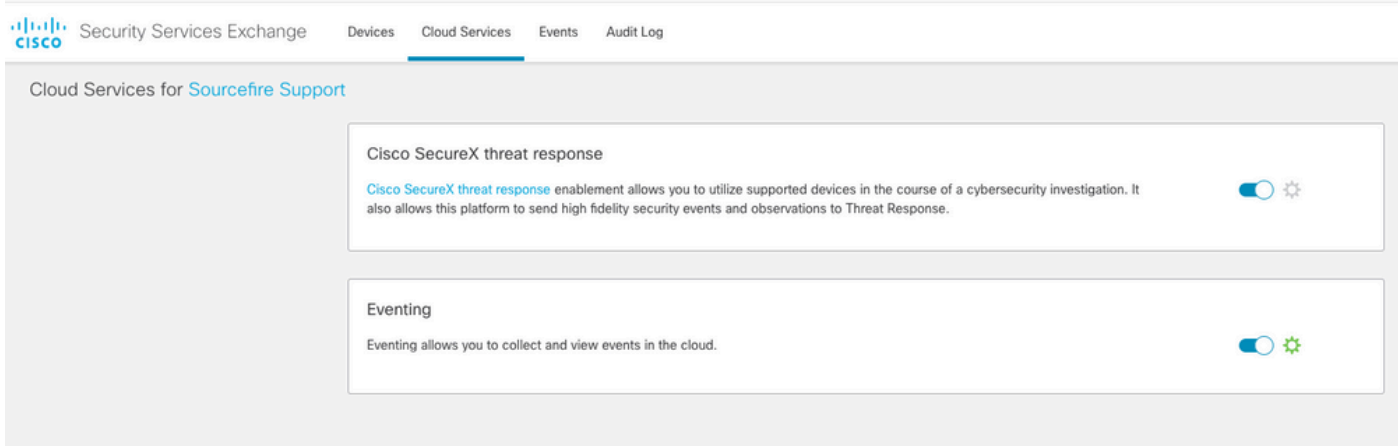
EU Region

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

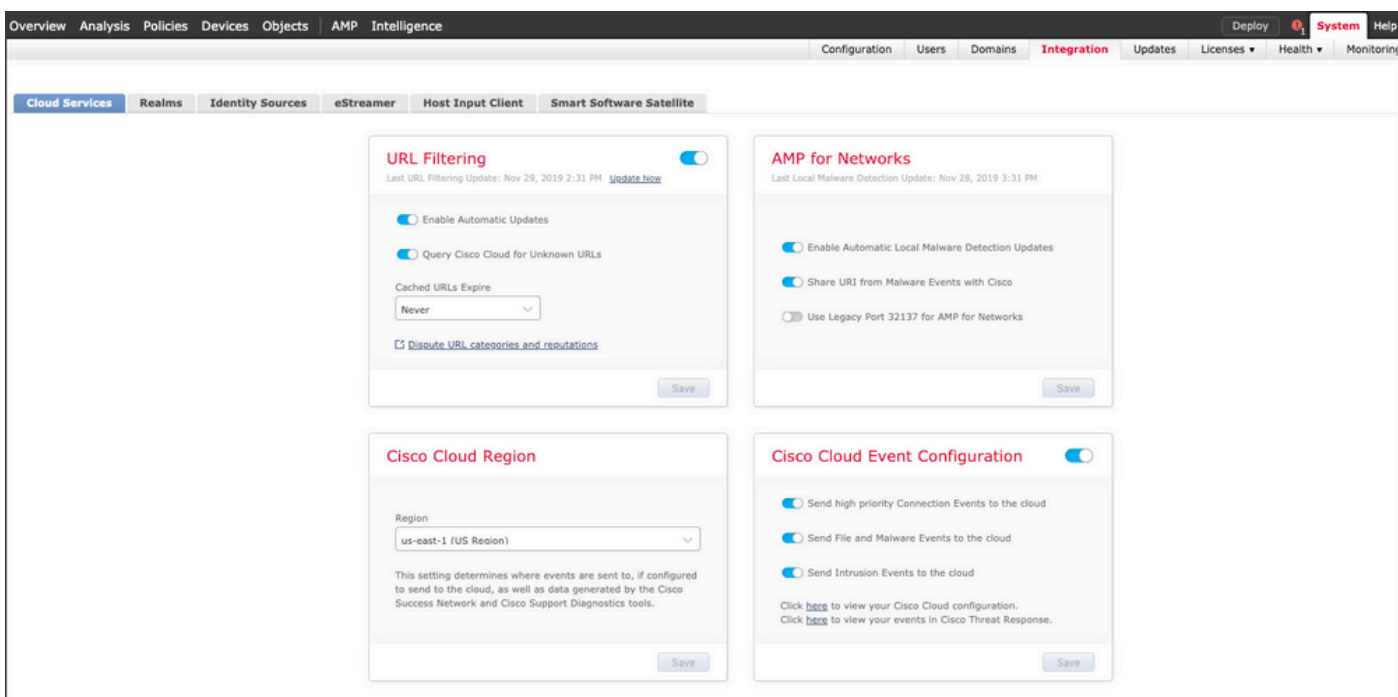
APJ Region

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

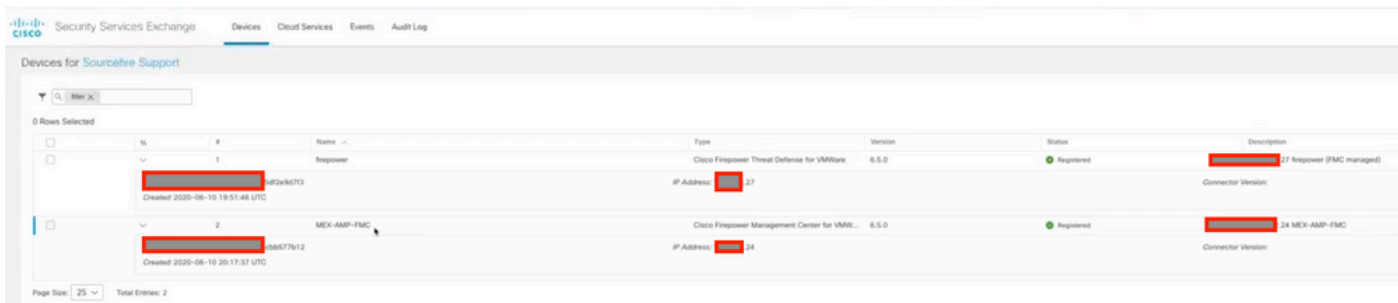
Step 2. Log in to the SSE portal with this URL <https://admin.sse.itd.cisco.com>. Navigate to **Cloud Services**, and enable both options **Eventing** and **Cisco Cisco XDR threat response**, as shown in the next image:



Step 3. Log in to the Firepower Management Center and navigate to **System>Integration>Cloud Services**, enable **Cisco Cloud Event Configuration** and select the events you want to send to the cloud:



Step 4. You can go back to the SSE portal and validate that now you can see the devices enrolled on SSE:



The Events are sent by the FTD devices, navigate to the **Events** on the SSE portal to verify the events sent by the devices to SSE, as shown in the image:

Security Services Exchange Devices Cloud Services **Events** Audit Log

Event Stream for Sourcefire Support

Enter filter criteria 08/04/2020, 18:50 - 08/05/2020, 18:50

0 Rows Selected

<input type="checkbox"/>	Talos Disposition	Incident	Destination IP	Event Time	Ingest Time	Message	Protocol	Reporting Device ID	Source IP
<input type="checkbox"/>	Neutral	* No	[REDACTED] 252	2020-08-05 18:48:50 UTC	2020-08-05 18:48:51 UTC		tcp	[REDACTED] 09d441eedce5	[REDACTED] 100
<input type="checkbox"/>	Neutral	* No	[REDACTED] 145	2020-08-05 18:47:38 UTC	2020-08-05 18:47:38 UTC		tcp	[REDACTED] 09d441eedce5	[REDACTED] 100
<input type="checkbox"/>	Unknown	* No	[REDACTED] 100	2020-08-05 18:47:30 UTC	2020-08-05 18:47:30 UTC		tcp	[REDACTED] 09d441eedce5	[REDACTED] 100
<input type="checkbox"/>	Neutral	* No	[REDACTED] 252	2020-08-05 18:46:50 UTC	2020-08-05 18:46:50 UTC		tcp	[REDACTED] 09d441eedce5	[REDACTED] 100

Verify

Validate that the FTDs generate events (malware or intrusion), for intrusion events navigate to **Analysis>Files>Malware Events**, for intrusion events navigate to **Analysis>Intrusion>Events**.

Validate the events are registered on the SSE portal as mentioned on the **Register the devices to SSE** section step 4.

Validate that information is displayed on the Cisco XDR dashboard or check the API logs so you can see the reason for a possible API failure.

Troubleshoot

Detect Connectivity Problems

You can detect generic connectivity problems from the action_queue.log file. In cases of failure you can see such logs present in the file:

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

In this case exit code 28 means operation timed out and we must check connectivity to the Internet. You must also see exit code 6 which means problems with DNS resolution

Connectivity Problems due to DNS Resolution

Step 1. Check that the connectivity works properly.

```
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'
```

This output shows that the device is unable to resolve the URL <https://api-sse.cisco.com>, in this case, we need to validate that the proper DNS server is configured, it can be validated with a nslookup from the expert CLI:

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

This output shows that the DNS configured is not reached, in order to confirm the DNS settings, use the **show network** command:

```
> 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 this example the wrong DNS server was used, you can change the DNS settings with this command:

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

After this connectivity can be tested again and this time, the connection is successful.

```
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
Cpath: /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 chain (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;

```

Registration issues to SSE Portal

Both FMC and FTD need a connection to the SSE URLs on their management interface, to test the connection, enter these commands on the Firepower CLI with root access:

```
<#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
```

The certificate check can be bypassed with this command:

```
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
Cpath: /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 chain (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: You get the 403 Forbidden message as the parameters sent from the test is not what SSE

 expects but this proves enough to validate connectivity.

Verify SSEConnector state

You can verify the connector properties as shown.

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

In order to check the connectivity between the SSEConnector and the EventHandler you can use this command, this is an example of a bad connection:

```
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 the example of an established connection you can see that the stream status is connected:

```
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.sock
```


Verify data sent to the SSE portal and CTR

In order to send events from the FTD device to SEE a TCP connection needs to be established with <https://eventing-ingest.sse.itd.cisco.com> This is an example of a connection not established between the SSE portal and the 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:443 (ESTABLISHED)
```

In the connector.log logs:

```
time="2020-04-13T14:34:02.88472046-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to SSE portal: dial tcp 100.25.93.234:443: connect: connection refused"
time="2020-04-13T14:38:18.244707779-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to SSE portal: dial tcp 100.25.93.234:443: connect: connection refused"
time="2020-04-13T14:42:42.564695622-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to SSE portal: dial tcp 100.25.93.234:443: connect: connection refused"
time="2020-04-13T14:47:48.484762429-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to SSE portal: dial tcp 100.25.93.234:443: connect: connection refused"
time="2020-04-13T14:52:38.404700083-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to SSE portal: dial tcp 100.25.93.234:443: connect: connection refused"
```

 **Note:** Noticed that the IP addresses displayed x.x.x.246 and 1x.x.x.246 belong to <https://eventing-ingest.sse.itd.cisco.com> must change, this is why the recommendation is to allow the traffic to SSE Portal based on URL instead of IP addresses.

If this connection is not established, the events are not sent to the SSE portal. This is an example of an established connection between the FTD and the 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.
```