

# Integrazione e risoluzione dei problemi di Cisco XDR con Firepower Threat Defense (FTD)

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Licenze](#)

[Collega gli account all'SSE e registra i dispositivi.](#)

[Registrare i dispositivi per l'SSE](#)

## Introduzione

In questo documento viene descritto come integrare, verificare e risolvere i problemi relativi a Cisco XDR con Firepower Threat Defense (FTD).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)
- Virtualizzazione delle immagini opzionale

### Componenti usati

- Firepower Threat Defense (FTD) - 6.5
- Firepower Management Center (FMC) - 6.5
- SSE (Security Services Exchange)
- Cisco XDR
- Portale delle licenze Smart

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

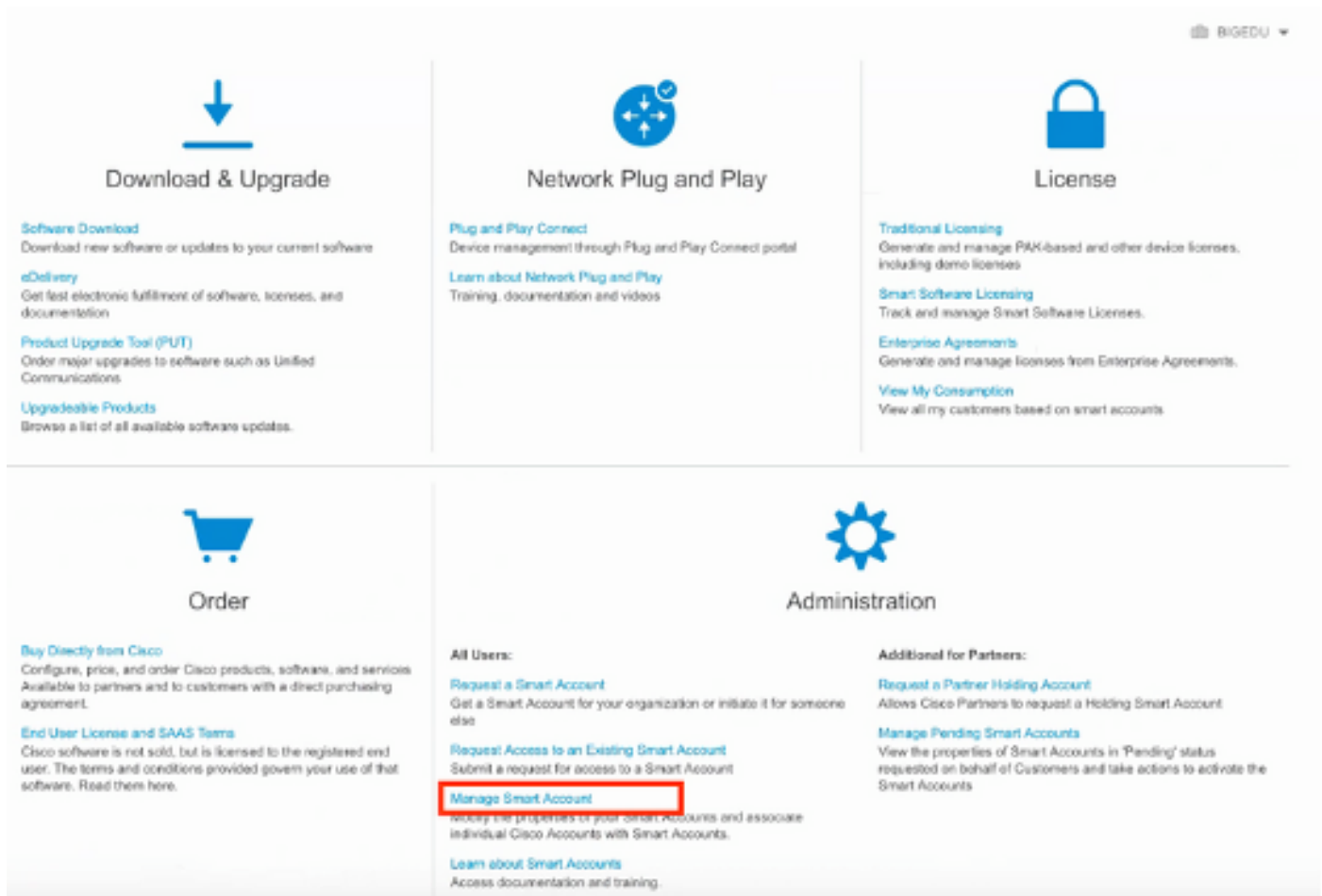
## Configurazione

## Licenze

Ruoli account virtuale:

Solo l'amministratore dell'account virtuale o l'amministratore dello Smart Account dispone del privilegio per collegare lo Smart Account all'account SSE.

Passaggio 1. Per convalidare il ruolo dello smart account, accedere al sito [software.cisco.com](https://software.cisco.com) e nel menu Administration (Amministrazione), selezionare Manage Smart Account (Gestisci smart account).



The screenshot shows the Cisco Software Center Administration menu. The 'Administration' section is expanded, and the 'Manage Smart Account' option is highlighted with a red box. The menu items are as follows:

- Download & Upgrade**
  - [Software Download](#): Download new software or updates to your current software
  - [eDelivery](#): Get fast electronic fulfillment of software, licenses, and documentation
  - [Product Upgrade Tool \(PUT\)](#): Order major upgrades to software such as Unified Communications
  - [Upgradeable Products](#): Browse a list of all available software updates.
- Network Plug and Play**
  - [Plug and Play Connect](#): Device management through Plug and Play Connect portal
  - [Learn about Network Plug and Play](#): Training, documentation and videos
- License**
  - [Traditional Licensing](#): Generate and manage PAK-based and other device licenses, including demo licenses
  - [Smart Software Licensing](#): Track and manage Smart Software Licenses.
  - [Enterprise Agreements](#): Generate and manage licenses from Enterprise Agreements.
  - [View My Consumption](#): View all my customers based on smart accounts
- Order**
  - [Buy Directly from Cisco](#): Configure, price, and order Cisco products, software, and services Available to partners and to customers with a direct purchasing agreement.
  - [End User License and SAAS Terms](#): Cisco software is not sold, but is licensed to the registered end user. The terms and conditions provided govern your use of that software. Read them here.
- Administration**
  - All Users:**
    - [Request a Smart Account](#): Get a Smart Account for your organization or initiate it for someone else
    - [Request Access to an Existing Smart Account](#): Submit a request for access to a Smart Account
    - [Manage Smart Account](#)**: Modify the properties of your Smart Accounts and associate individual Cisco Accounts with Smart Accounts.
    - [Learn about Smart Accounts](#): Access documentation and training.
  - Additional for Partners:**
    - [Request a Partner Holding Account](#): Allows Cisco Partners to request a Holding Smart Account
    - [Manage Pending Smart Accounts](#): View the properties of Smart Accounts in 'Pending' status requested on behalf of Customers and take actions to activate the Smart Accounts

Passaggio 2. Per convalidare il ruolo utente, passare a Utenti e verificare che in Ruoli gli account siano impostati in modo da disporre di un account con account di amministratore virtuale, come mostrato nell'immagine.

**Users**

User	Email	Organization	Account Access	Role	User Group	Actions
<input type="checkbox"/> danieber						
<input type="checkbox"/> Daniel Benitez danieben	danieben@cisco.com	Cisco Systems, Inc.	All Virtual Accounts Mex-AMP TAC	Smart Account Administrator Virtual Account Administrator		Remove...

1 User

Passaggio 3. Verificare che l'account virtuale selezionato per il collegamento in SSE contenga la licenza per i dispositivi di sicurezza se un account che non contiene la licenza di sicurezza è collegato in SSE, nei dispositivi di sicurezza e l'evento non viene visualizzato sul portale SSE.

Cisco Software Central > Smart Software Licensing

Smart Software Licensing

[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... | Search by License





License	Billing	Purchased	In Use	Balance	Alerts	Actions
<input type="checkbox"/> License						
<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

Showing Page 5 of 7 (85 Records)















Passaggio 4. Per verificare che il CCP sia stato registrato nell'account virtuale corretto, passare a Sistema>Licenze>Smart License (Licenze Smart):

## 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:	<a href="#">Enabled</a> 
Cisco Support Diagnostics:	<a href="#">Disabled</a> 

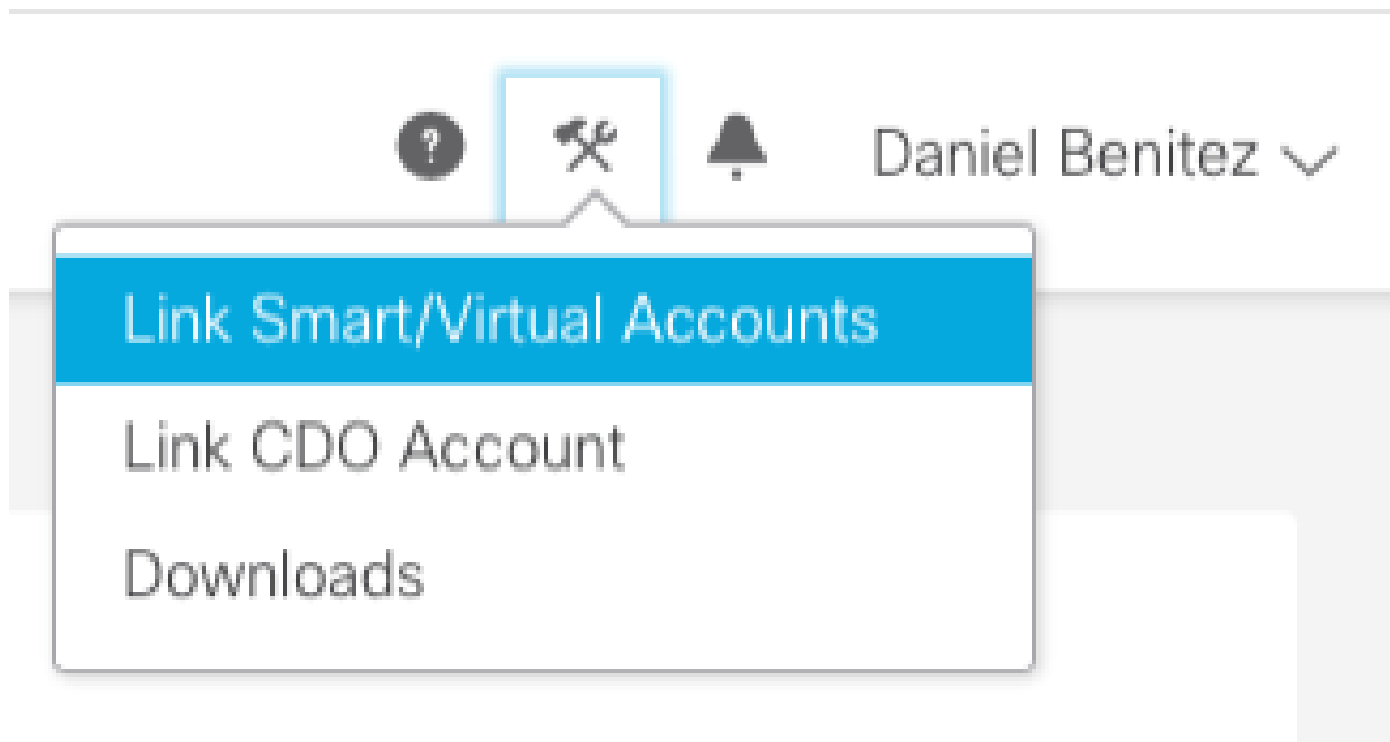
## Smart Licenses

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

Collega gli account all'SSE e registra i dispositivi.

Passaggio 1. Quando si accede al proprio account SSE, è necessario collegare lo smart account al proprio account SSE. A tale scopo, è necessario fare clic sull'icona degli strumenti e selezionare Collega account.



Una volta collegato l'account, viene visualizzato lo Smart Account con tutti gli account virtuali.

## Registrare i dispositivi per l'SSE

Passaggio 1. Assicurarsi che nell'ambiente siano consentiti i seguenti URL:

### Regione USA

- [api-sse.cisco.com](https://api-sse.cisco.com)
- [eventing-ingest.sse.itd.cisco.com](https://eventing-ingest.sse.itd.cisco.com)

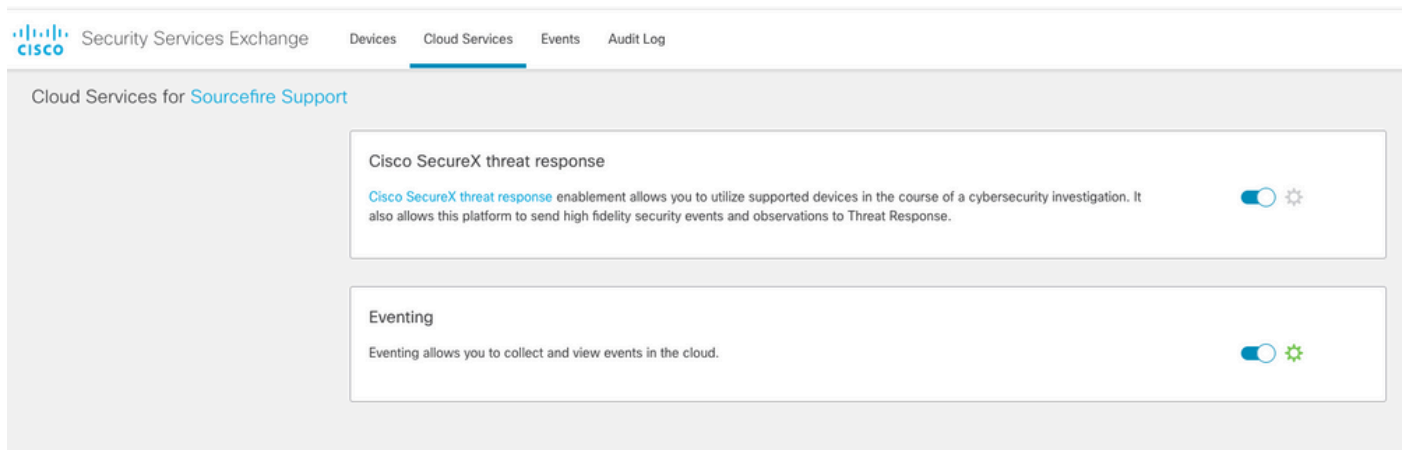
### Regione UE

- [api.eu.sse.itd.cisco.com](https://api.eu.sse.itd.cisco.com)
- [eventing-ingest.eu.sse.itd.cisco.com](https://eventing-ingest.eu.sse.itd.cisco.com)

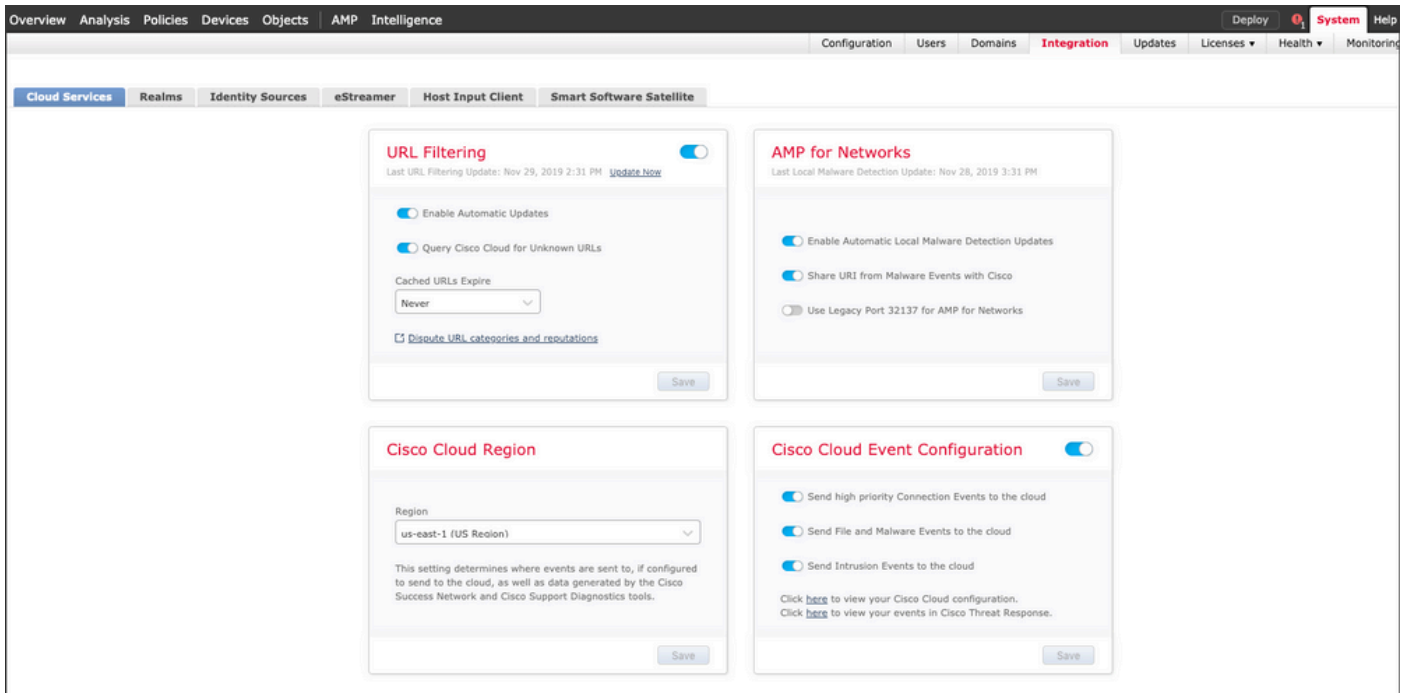
### Area APJ

- [api.apj.sse.itd.cisco.com](https://api.apj.sse.itd.cisco.com)
- [eventing-ingest.apj.sse.itd.cisco.com](https://eventing-ingest.apj.sse.itd.cisco.com)

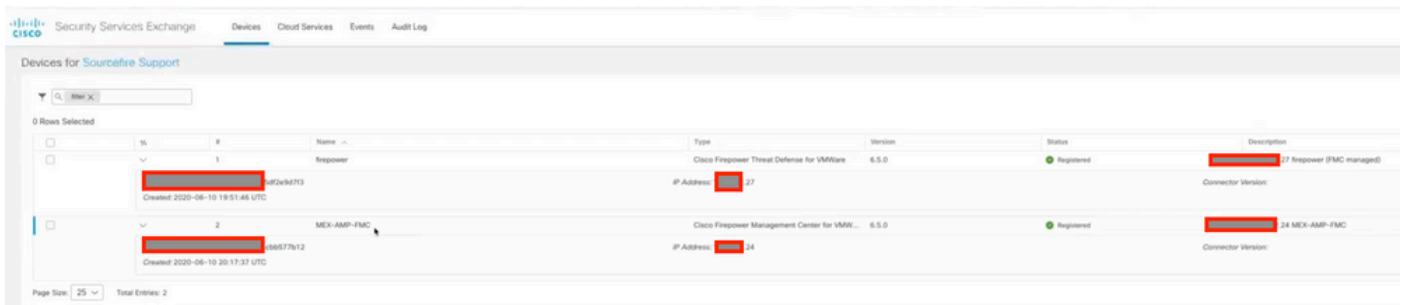
Passaggio 2. Accedere al portale SSE con questo URL <https://admin.sse.itd.cisco.com>, passare a Cloud Services e abilitare entrambe le opzioni Eventing e Cisco CDR XDR threat response, come mostrato nell'immagine seguente:



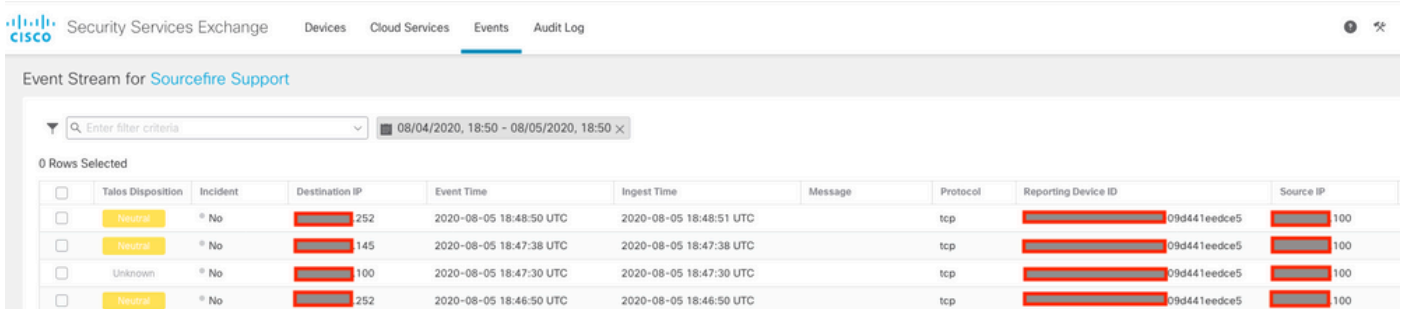
Passaggio 3. Accedere a Firepower Management Center e selezionare System>Integration>Cloud Services, abilitare Cisco Cloud Event Configuration (Configurazione eventi cloud Cisco) e selezionare gli eventi che si desidera inviare al cloud:



Passaggio 4. È possibile tornare al portale SSE e verificare che sia ora possibile visualizzare i dispositivi registrati su SSE:



Gli eventi vengono inviati dai dispositivi FTD, passare a Events sul portale SSE per verificare gli eventi inviati dai dispositivi a SSE, come mostrato nell'immagine:



## Verifica

Convalida che gli FTD generano eventi (malware o intrusione), per gli eventi di intrusione passare a Analisi>File>Eventi malware, per gli eventi di intrusione passare ad Analisi>Intrusione>Eventi.

Verificare che gli eventi siano registrati sul portale SSE come indicato nella sezione Registrazione

dei dispositivi per l'SSE, passaggio 4.

Verificare che le informazioni siano visualizzate nel dashboard Cisco XDR o controllare i registri API in modo da poter visualizzare il motivo di un possibile errore API.

## Risoluzione dei problemi

### Rileva problemi di connettività

È possibile rilevare problemi di connettività generici dal file `action_queue.log`. In caso di errore, è possibile visualizzare tali registri nel file:

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

In questo caso, il codice di uscita 28 indica che l'operazione è scaduta ed è necessario verificare la connettività a Internet. È inoltre necessario visualizzare il codice di uscita 6 che indica problemi con la risoluzione DNS

### Problemi di connettività dovuti alla risoluzione DNS

Passaggio 1. Verificare che la connettività funzioni correttamente.

```
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'
```

Questo output mostra che il dispositivo non è in grado di risolvere l'URL <https://api-sse.cisco.com>. In questo caso, è necessario verificare che sia configurato il server DNS corretto, che possa essere convalidato con `nslookup` dalla CLI degli esperti:

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

Questo output mostra che il DNS configurato non è raggiunto. Per confermare le impostazioni DNS, utilizzare il 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

```

In questo esempio è stato utilizzato il server DNS errato. È possibile modificare le impostazioni DNS con questo comando:

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

Una volta verificata la connettività, la connessione viene stabilita correttamente.

```

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 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;

```

## Problemi di registrazione nel portale SSE

Sia FMC che FTD necessitano di una connessione agli URL SSE sull'interfaccia di gestione. Per testare la connessione, immettere questi comandi sulla CLI di Firepower con accesso root:

```
<#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
```

Il controllo del certificato può essere ignorato con questo 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
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;
```

---

Nota: viene visualizzato il messaggio 403 Proibito poiché i parametri inviati dal test non sono quelli previsti da SSE, ma questo è sufficiente per convalidare la connettività.

---

## Verifica stato SSEConnector

È possibile verificare le proprietà del connettore come illustrato.

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

Per controllare la connettività tra SSConnector e EventHandler, è possibile utilizzare questo comando, ad esempio una connessione non valida:

```
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
```

Nell'esempio di una connessione stabilita, è possibile vedere che lo stato del flusso è connected (connesso):

```
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
```

## Verifica dei dati inviati al portale SSE e al CTR

Per inviare eventi dal dispositivo FTD a SEE una connessione TCP deve essere stabilita con <https://eventing-ingest.sse.ftd.cisco.com> Questo è un esempio di connessione non stabilita tra il portale SSE e 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
```

Nei log di connector.log:

```
time="2020-04-13T14:34:02.88472046-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to https://eventing-ingest.sse.ftd.cisco.com:443"
time="2020-04-13T14:38:18.244707779-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to https://eventing-ingest.sse.ftd.cisco.com:443"
time="2020-04-13T14:42:42.564695622-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to https://eventing-ingest.sse.ftd.cisco.com:443"
time="2020-04-13T14:47:48.484762429-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to https://eventing-ingest.sse.ftd.cisco.com:443"
time="2020-04-13T14:52:38.404700083-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:connect] failed to connect to https://eventing-ingest.sse.ftd.cisco.com:443"
```

---

Nota: si noti che gli indirizzi IP visualizzati x.x.x.246 e 1x.x.x.246 appartengono a

---

---

<https://eventing-ingest.sse.itd.cisco.com> devono essere modificati. Per questo motivo si consiglia di consentire il traffico verso il portale SSE in base all'URL anziché agli indirizzi IP.

---

Se la connessione non viene stabilita, gli eventi non vengono inviati al portale SSE. Questo è un esempio di connessione stabilita tra l'FTD e il portale 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.
```

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).