Integrazione e risoluzione dei problemi di Cisco XDR con Secure Firewall

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati

Configurazione

- Licenze
- Collega i tuoi account a SSX e registra i dispositivi.

Metodo 1 (integrazione parziale): Arricchisci indagini

- Registrare i dispositivi su SSX

Introduzione

In questo documento viene descritto come integrare, verificare e risolvere i problemi relativi a Cisco XDR con Secure Firewall.

Esistono due metodi per integrare Secure Firewall e XDR e ogni integrazione fornisce risultati diversi.

Il primo metodo descrive come integrare Secure Firewall, Security Services Exchange (SSX), Security Cloud Control, XDR-Analytics e XDR per arricchire le indagini.

Il secondo metodo descrive come integrare Secure Firewall, SSX, Security Cloud Control, XDR-A, SAL Cloud e XDR, per arricchire Incident.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense
- Virtualizzazione delle immagini opzionale
- Cisco Defense Orchestrator
- Security Services Exchange
- Security Cloud Control

Componenti usati

- Secure Firewall - 7.2
- Firepower Management Center (FMC) - 7.2
- SSX (Security Services Exchange)
- Cisco XDR
- Portale delle licenze Smart
- Cisco Defense Orchestrator
- Security Cloud Control

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.

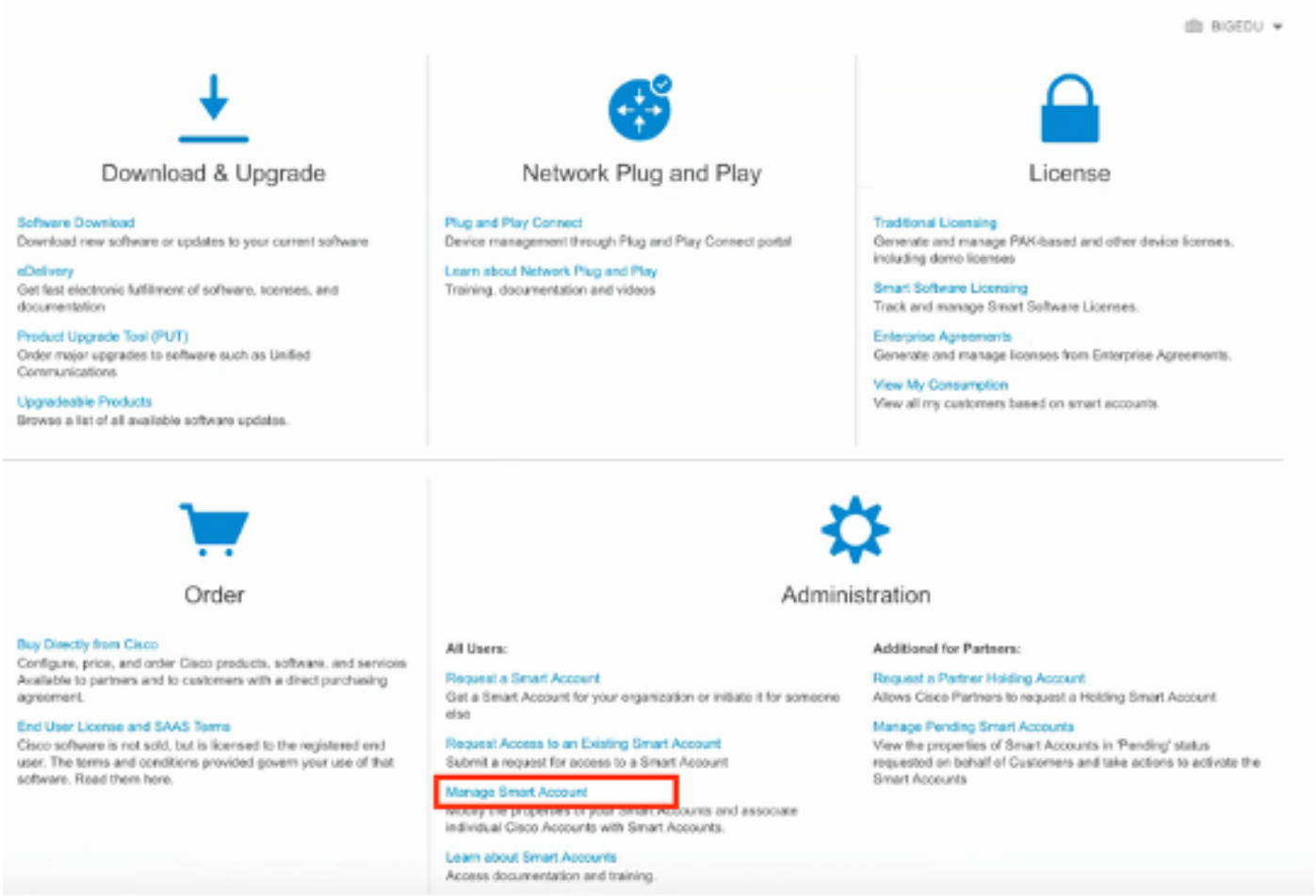
Configurazione

Licenze

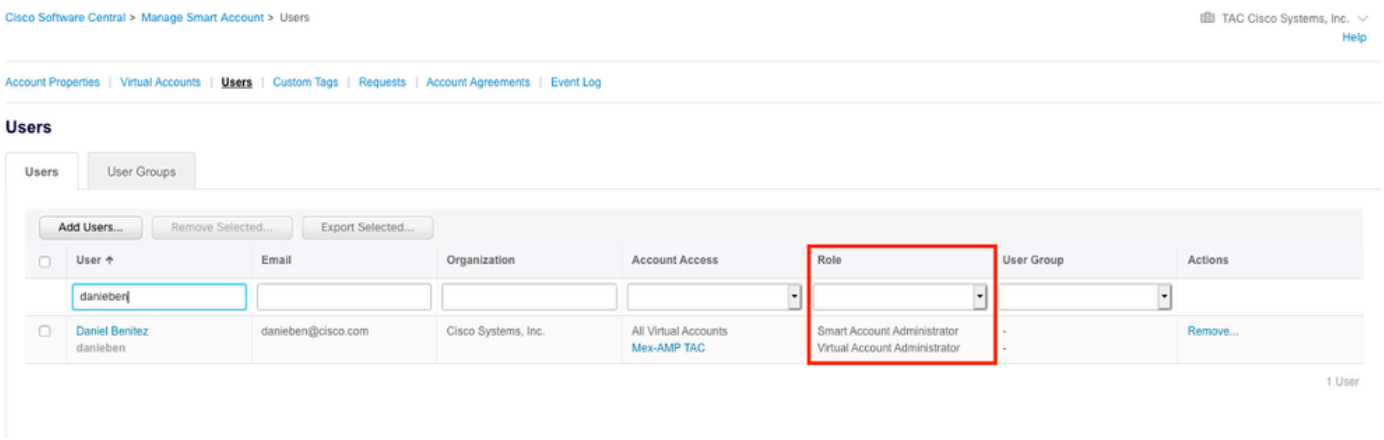
Ruoli account virtuale:

Solo l'amministratore dell'account virtuale o l'amministratore dello Smart Account ha il privilegio di collegare lo Smart Account con l'account SSX.

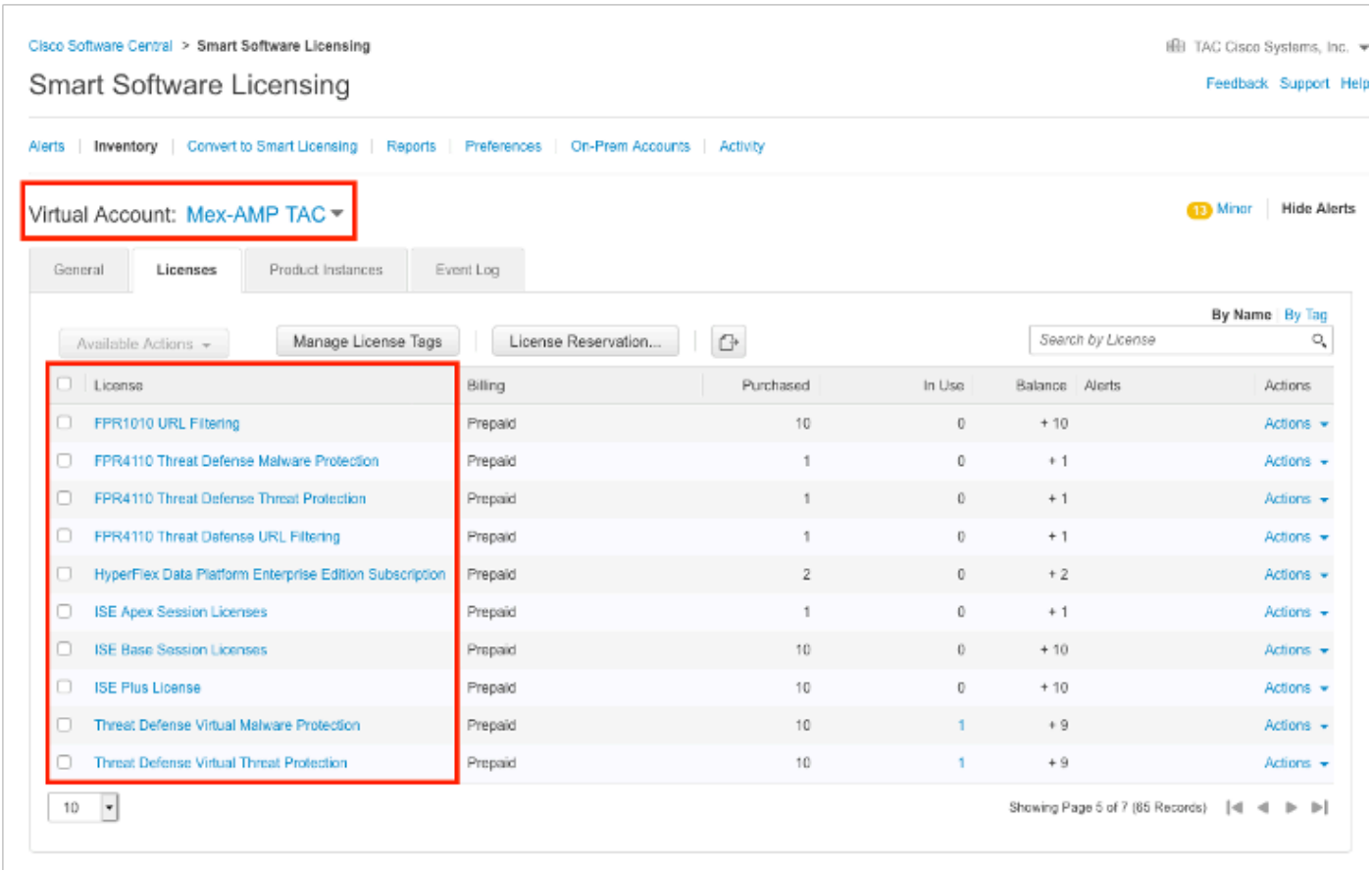
Passaggio 1. Per convalidare il ruolo dello smart account, accedere al sito software.cisco.com e nel menu Amministrazione, selezionare Gestisci smart account.



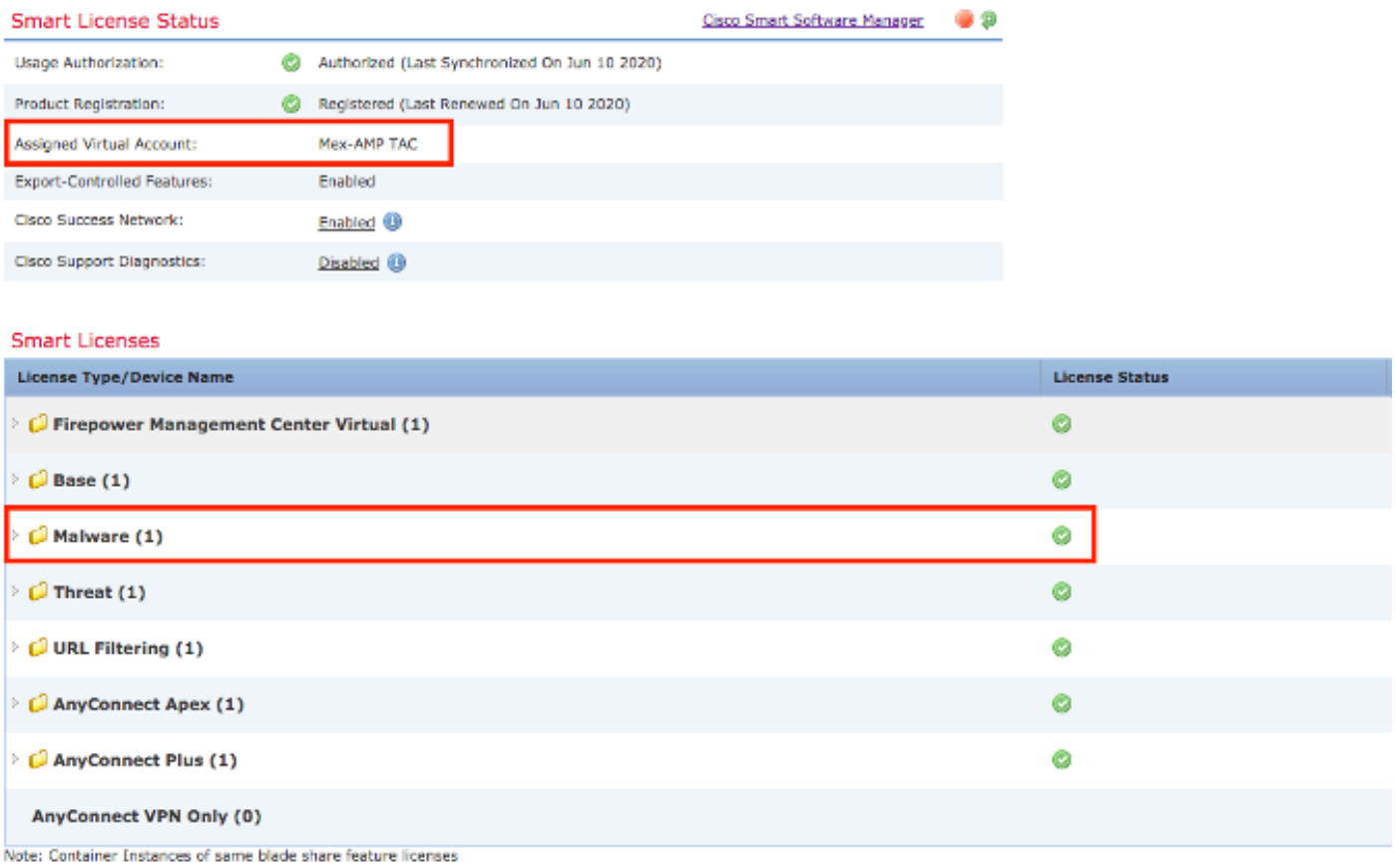
Passaggio 2. Per convalidare il ruolo utente, passare a Utenti e verificare che in Ruoli gli account siano impostati per disporre di un account con account di amministratore virtuale, come mostrato nell'immagine.



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

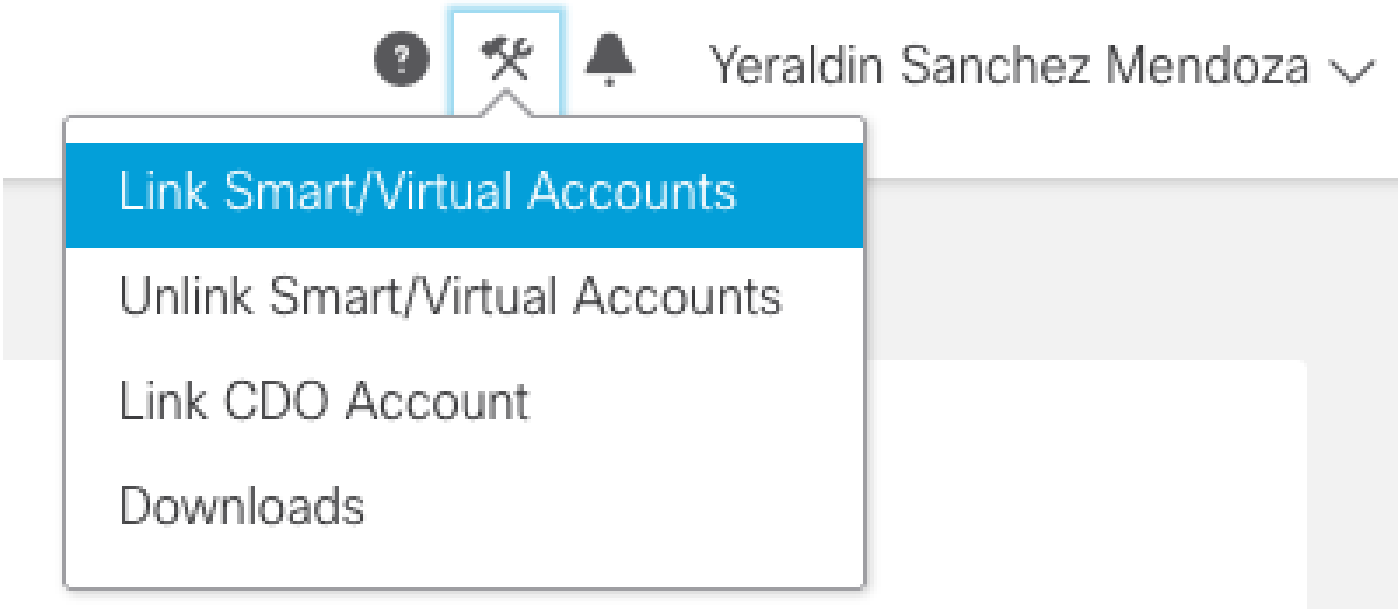


Passaggio 4. Per verificare che il CCP sia stato registrato nell'account virtuale corretto, selezionare Sistema > Licenze > Smart License:



Collega i tuoi account a SSX e registra i dispositivi.

Passaggio 1. Quando si accede al proprio account SSX, è necessario collegare lo smart account al proprio account SSX. A tale scopo, è necessario fare clic sull'icona Strumenti e selezionare Collega smart/account virtuali.



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

Metodo 1 (integrazione parziale): Arricchisci indagini

Registrare i dispositivi su SSX

Passaggio 1. Verificare che gli URL seguenti siano consentiti nell'ambiente in uso:

Regione USA

- api-sse.cisco.com
- mx*.sse.itd.cisco.com
- dex.sse.itd.cisco.com
- eventing-ingest.sse.itd.cisco.com
- registration.us.sse.itd.cisco.com
- defenseorchestrator.com
- edge.us.cdo.cisco.com

Regione UE

- api.eu.sse.itd.cisco.com
- mx*.eu.sse.itd.cisco.com
- dex.eu.sse.itd.cisco.com
- eventing-ingest.eu.sse.itd.cisco.com
- registration.eu.sse.itd.cisco.com
- defenseorchestrator.eu
- edge.eu.cdo.cisco.com

Area APJC

- api.apj.sse.itd.cisco.com
- mx*.apj.sse.itd.cisco.com
- dex.apj.sse.itd.cisco.com
- eventing-ingest.apj.sse.itd.cisco.com
- registration.apj.sse.itd.cisco.com
- apj.cdo.cisco.com
- edge.apj.cdo.cisco.com

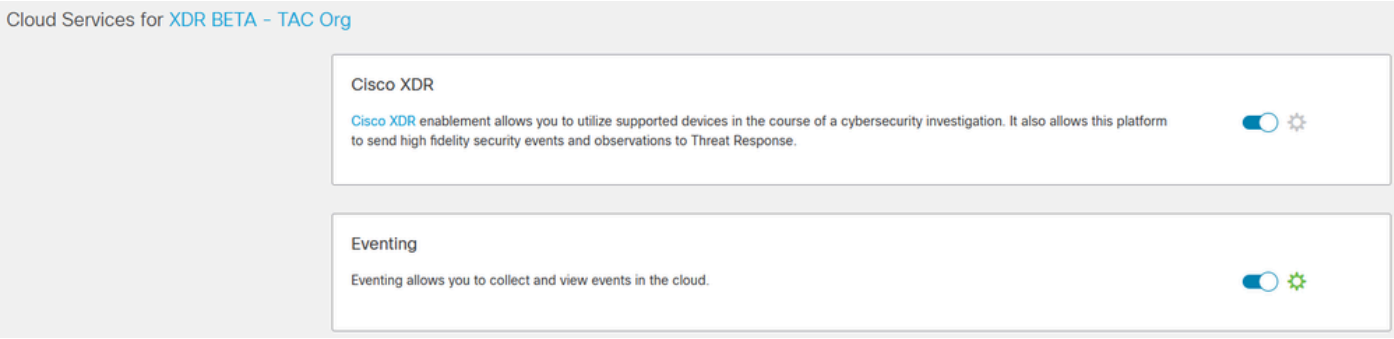
Regione Australia:

- api.aus.sse.itd.cisco.com
- mx*.aus.sse.itd.cisco.com
- dex.au.sse.itd.cisco.com
- eventing-ingest.aus.sse.itd.cisco.com
- registration.au.sse.itd.cisco.com
- aus.cdo.cisco.com

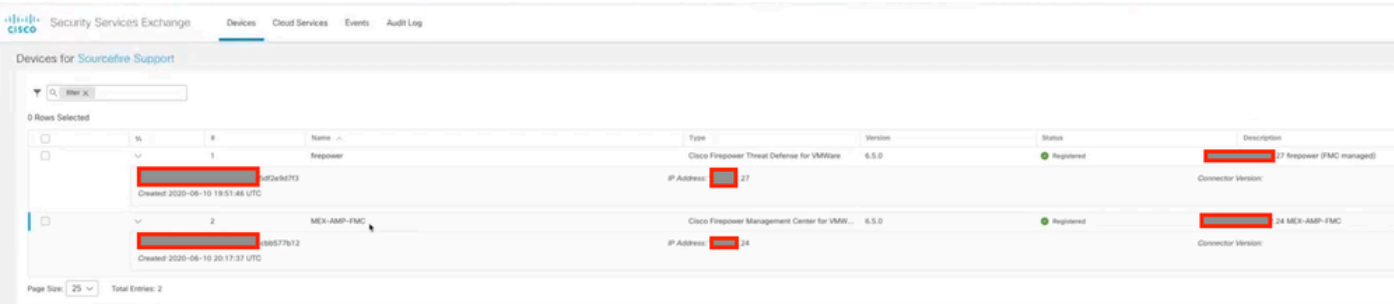
Regione India:

- api.in.sse.itd.cisco.com
- mx*.in.sse.itd.cisco.com
- dex.in.sse.itd.cisco.com
- eventing-ingest.in.sse.itd.cisco.com
- registration.in.sse.itd.cisco.com
- in.cdo.cisco.com

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

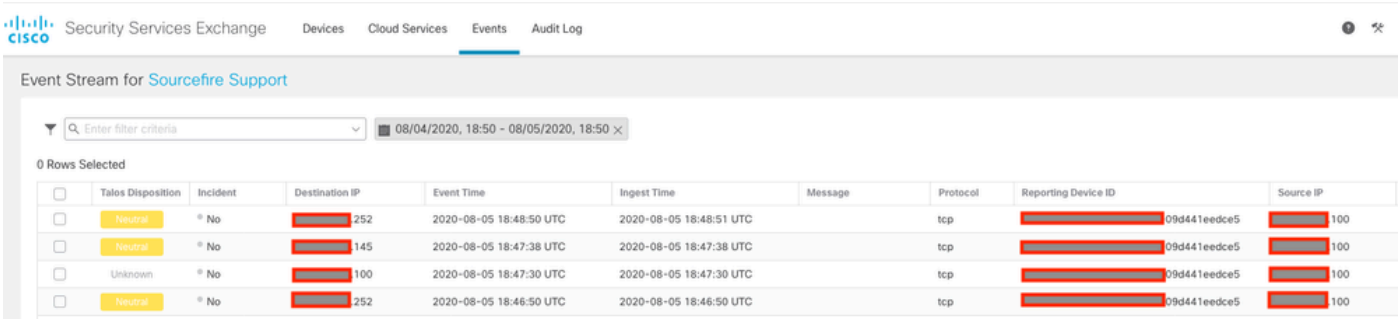


Passaggio 3. È possibile verificare che ora sia possibile visualizzare i dispositivi registrati su SSX:



Gli eventi vengono inviati dai dispositivi Secure Firewall, passare a Events sul portale SSX per

verificare gli eventi inviati dai dispositivi a SSX, come mostrato nell'immagine.



Registra i dispositivi su Security Cloud Control (SCC/CDO)

Passaggio 1. Verificare che questi URL siano consentiti nell'ambiente in uso

Regione USA:

- defenseorchestrator.com
- edge.us.cdo.cisco.com

Regione UE

- defenseorchestrator.eu
- edge.eu.cdo.cisco.com

Area APJC

- apjc.cdo.cisco.com
- edge.apjc.cdo.cisco.com

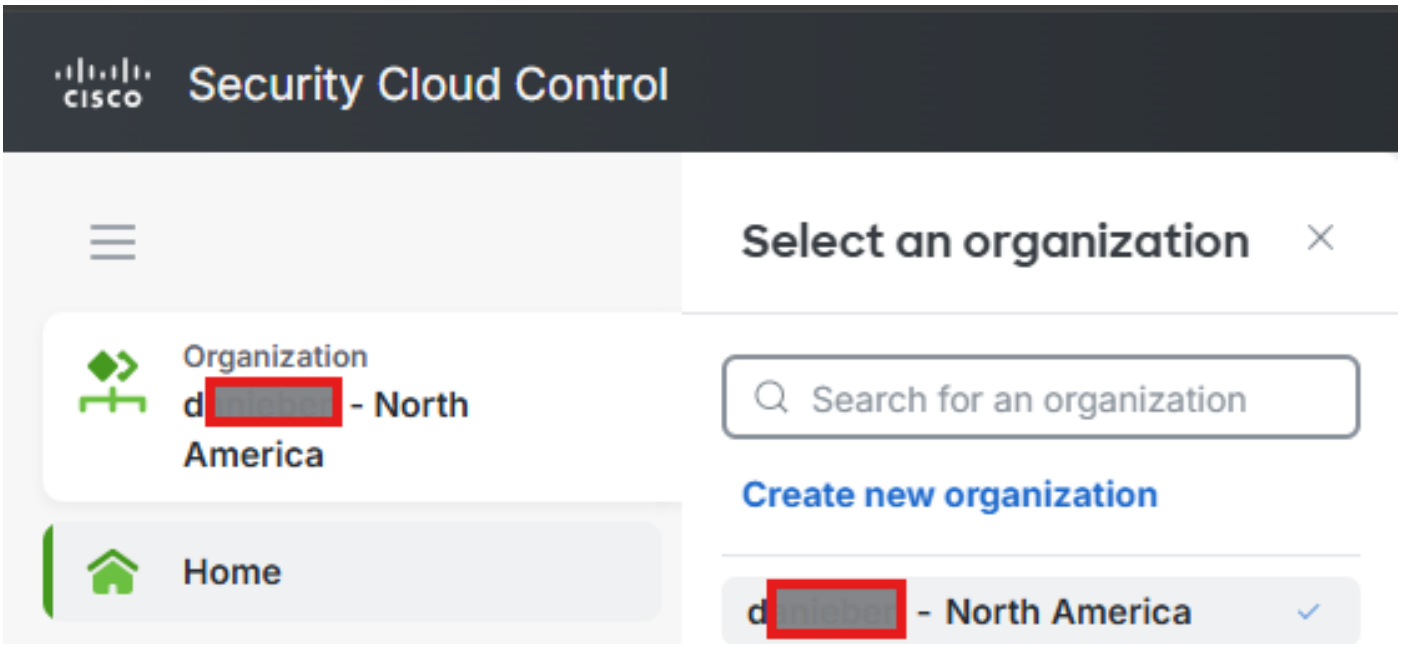
Regione Australia:

- aus.cdo.cisco.com

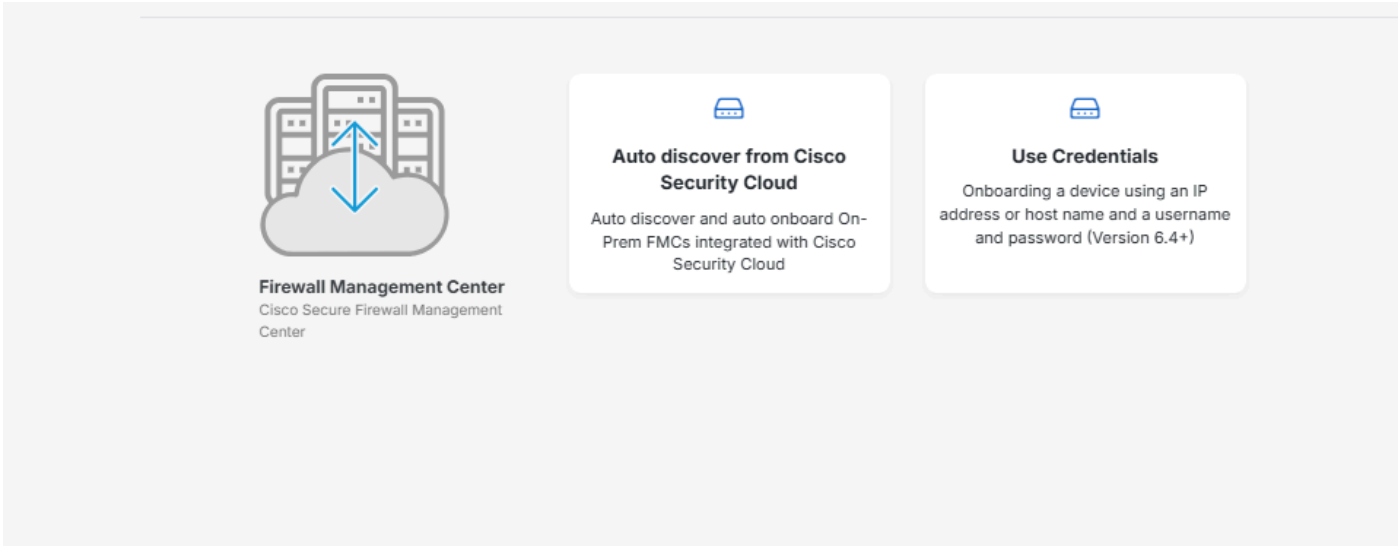
Regione India:

- in.cdo.cisco.com

Passaggio 2. Passare a Security Cloud Control (il collegamento può variare in base alla propria area geografica). Questo indica di selezionare la propria organizzazione di Security Cloud Control.



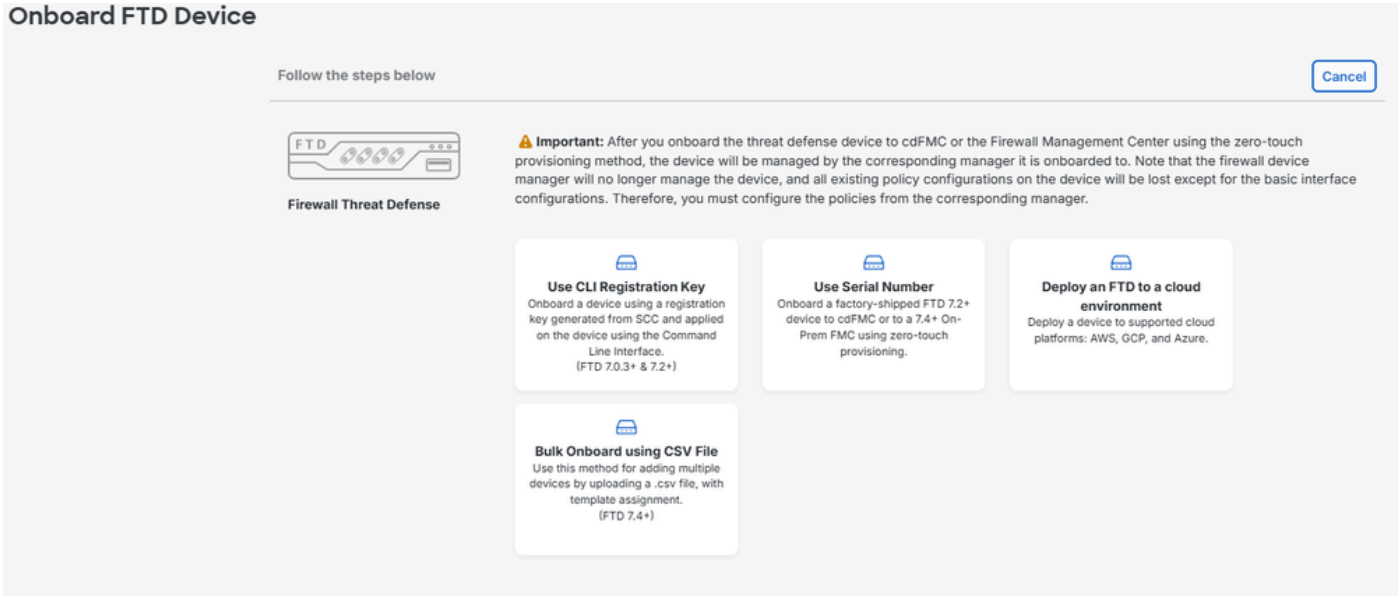
Passaggio 3. Dopo aver selezionato l'organizzazione appropriata, passare a Products > Firewall, verificare se il dispositivo è già presente. In caso contrario, è possibile includerlo in Security Cloud Control (Cisco Defense Orchestrator). A tale scopo, in Overall Inventory, fare clic su Visualizza tutti i dispositivi.



Passaggio 4. Passare a Amministrazione > Centro gestione firewall, viene visualizzato un elenco dei CCP integrati in SCC. Se il Centro gestione firewall non è visibile, fare clic sull'icona con il segno più.

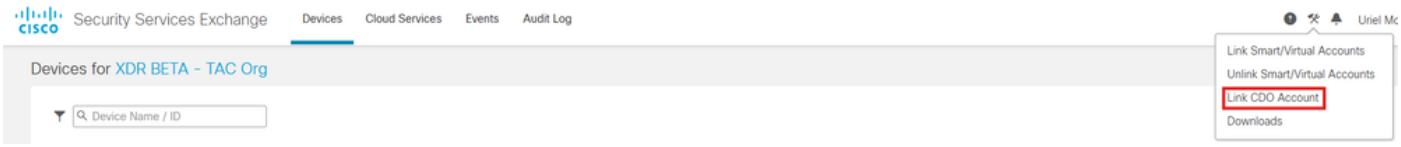
Passaggio 4.1. Normalmente, i firewall sicuri vengono caricati automaticamente; in caso contrario, selezionare il dispositivo che si desidera caricare (FTD) e il metodo di caricamento preferito.

Passaggio 4.2. Sotto la sezione Security Devices (Dispositivi di sicurezza), fare clic sul segno più (+), selezionare Onboard Secure Firewall Device (Dispositivo di sicurezza integrato) e la



Passaggio 5. Una volta caricati i dispositivi in Security Cloud Control, è possibile visualizzarli nell'inventario.

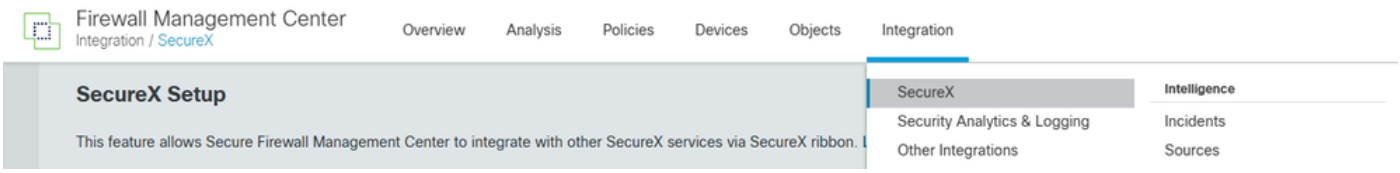
Passaggio 6. Verificare che l'organizzazione CDO sia collegata all'organizzazione SSX. A tale scopo, passare a Security Services Exchange, fare clic sull'icona del menu Strumenti, quindi su Collega account CDO.



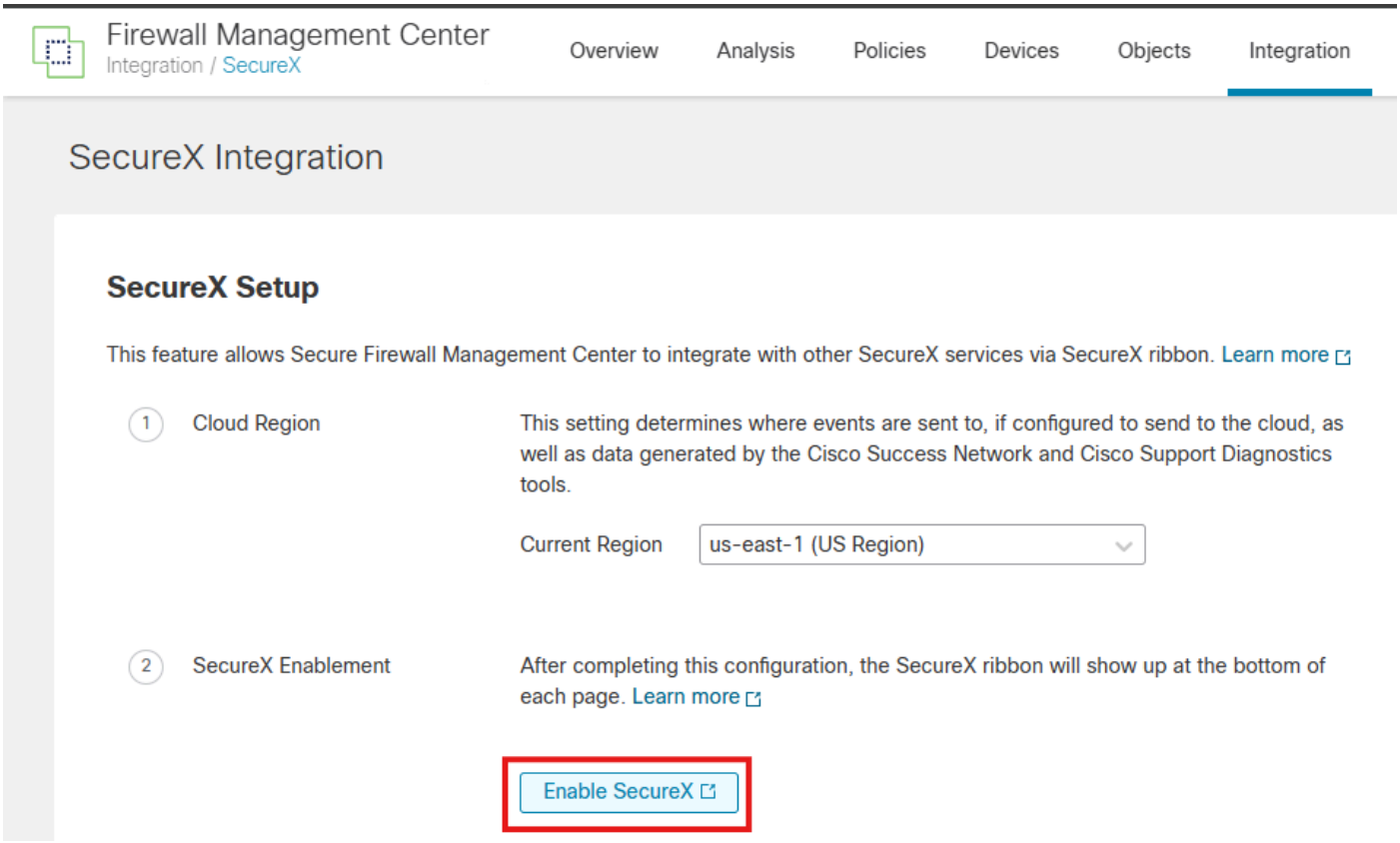
Integrazione di Secure Firewall

Da 7.2.x a 7.4.x con Cisco XDR

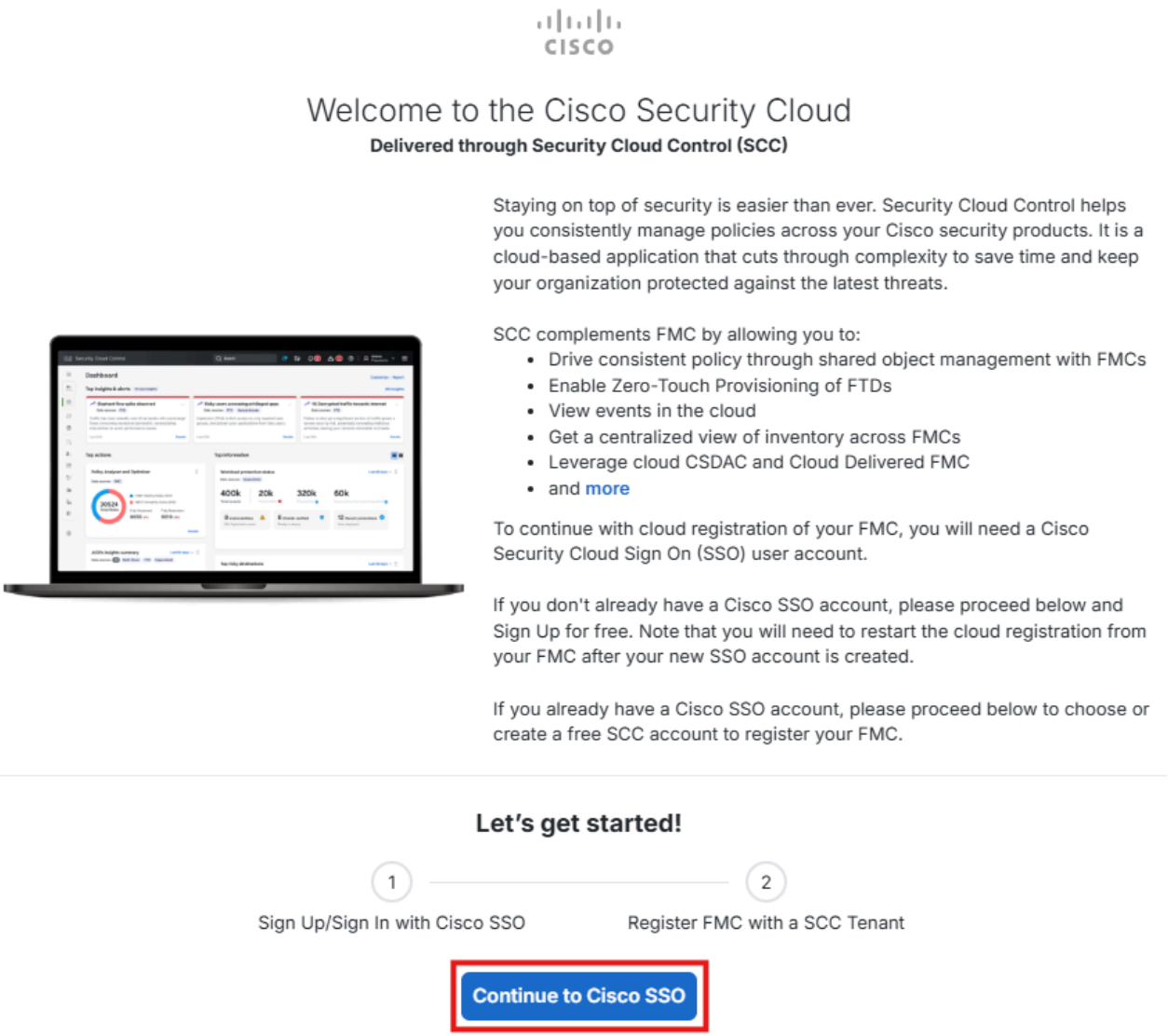
Passaggio 1. In Centro gestione firewall sicuro passare a Integrazione > SecureX



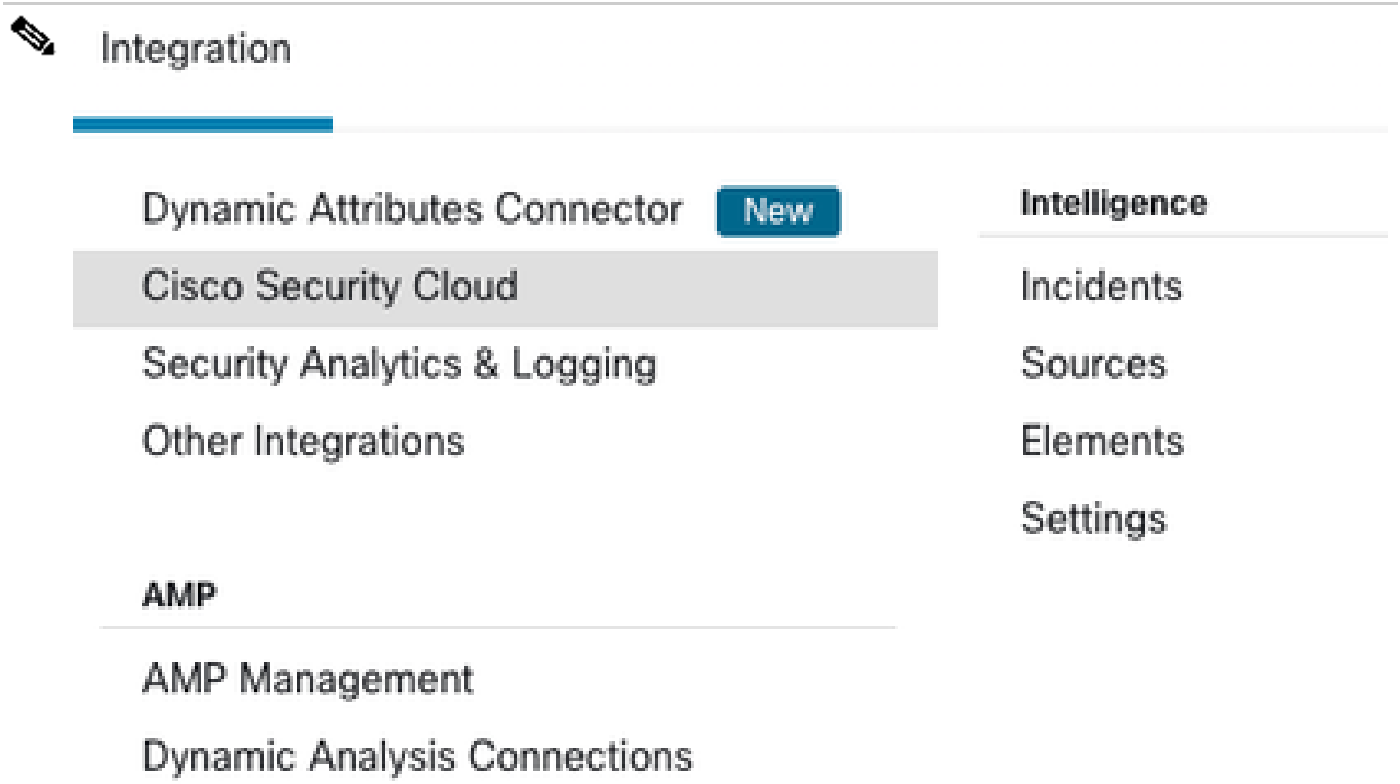
Passaggio 2. Scegliere l'area destra e fare clic su Abilita SecureX.



Passaggio 3. Dopo aver fatto clic su Abilita SecureX, viene eseguito il reindirizzamento alla pagina di autenticazione di Cisco Defense Orchestrator (che sfrutta la funzionalità di accesso al cloud di sicurezza). Fare clic su Continua per Cisco SSO.



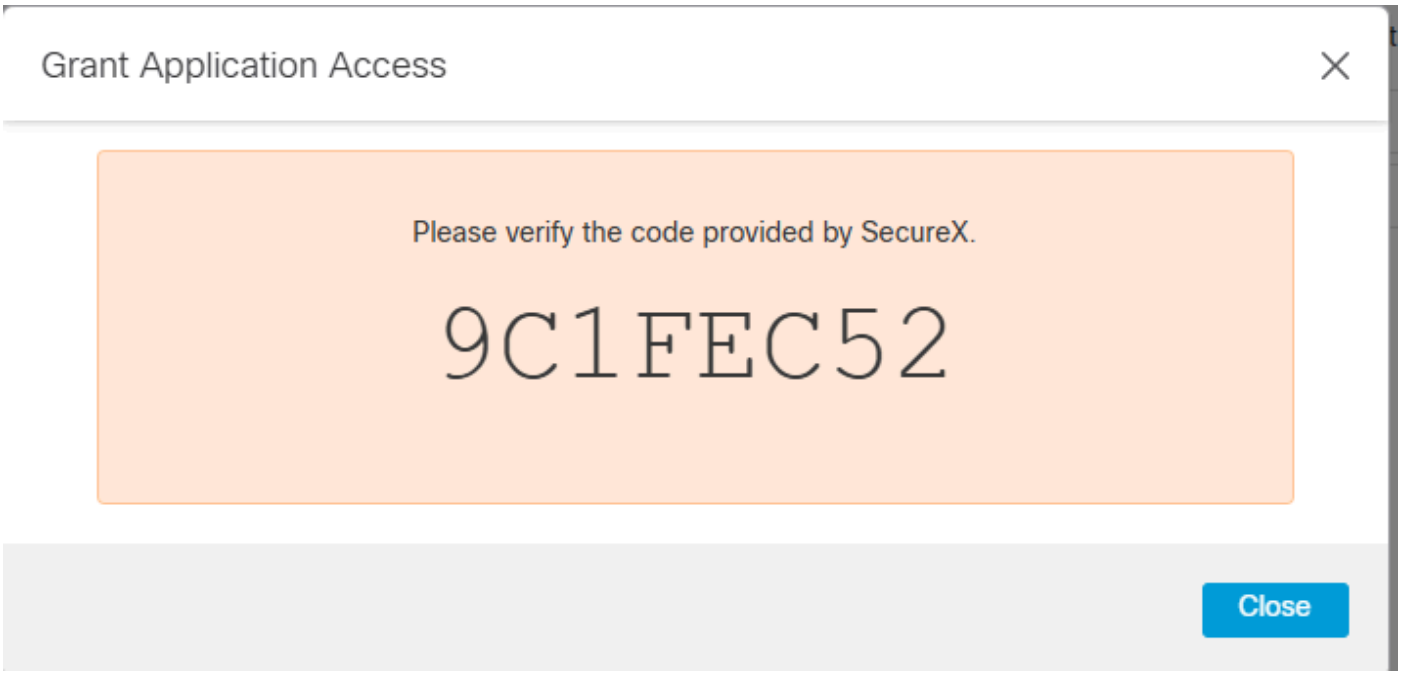
Nota:
A partire dalla versione 7.6.x con Cisco XDR
Passaggio 1. In Secure Firewall Management Center, passare a Integrazione > Cisco Security Cloud

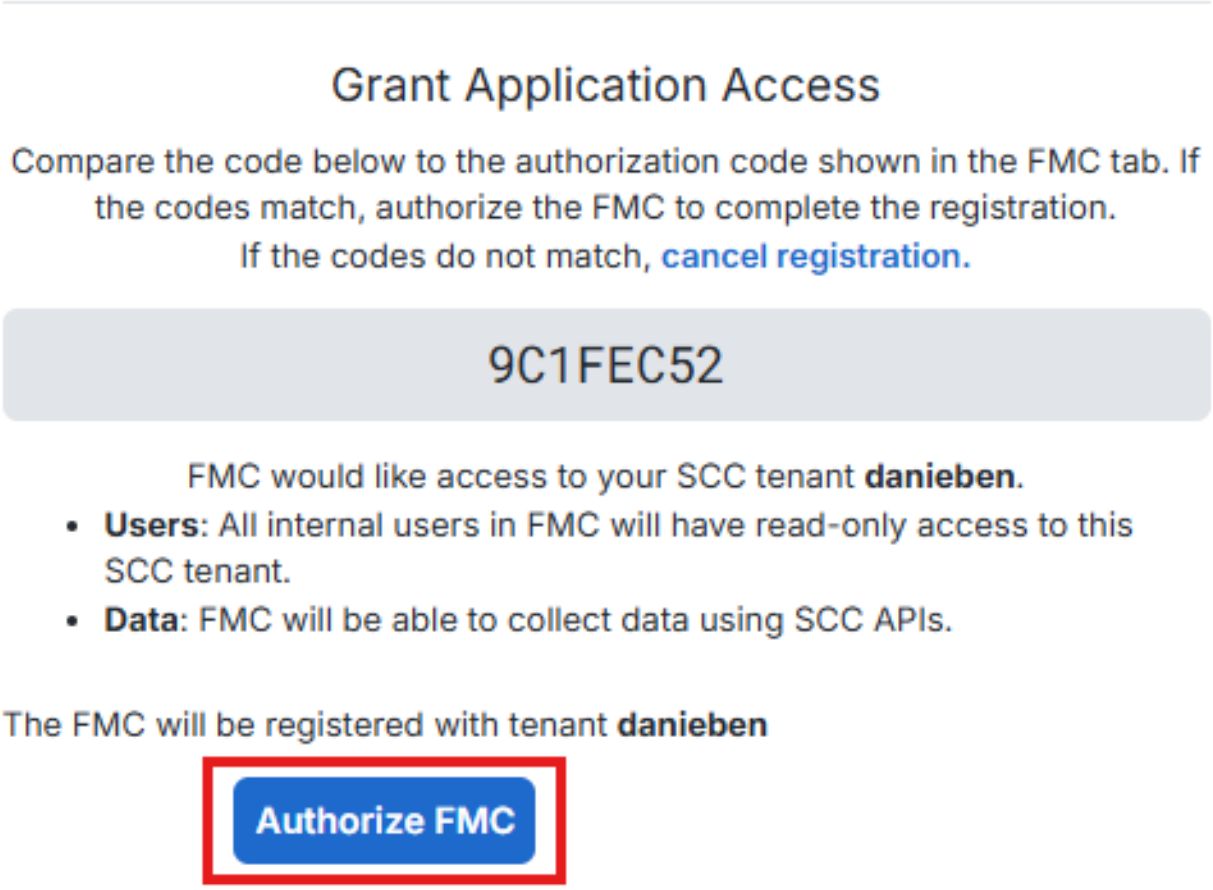


Passaggio 2. Scegliere l'area destra e fare clic su Abilita Cisco Security Cloud.
Passaggio 3. Dopo aver fatto clic su Abilita Cisco Security Cloud, viene eseguito il reindirizzamento alla pagina di autenticazione di Cisco Defense Orchestrator (che sfrutta l'accesso a Security Cloud), fare clic su Continua per Cisco SSO.

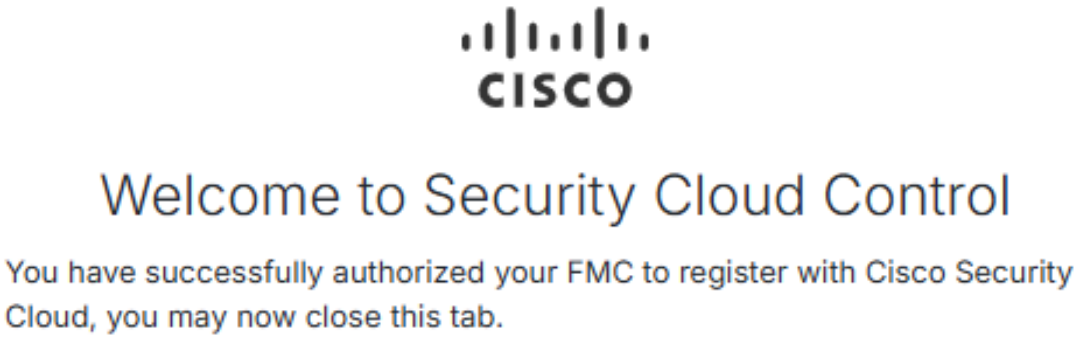
Passaggio 4. È possibile selezionare un tenant di Security Cloud Control preesistente o crearne uno nuovo.

Passaggio 5. Selezionare il tenant appropriato e verificare che il codice ricevuto in questa pagina corrisponda al codice ricevuto in FMC. Se corrispondono, fare clic su Autorizza FMC.



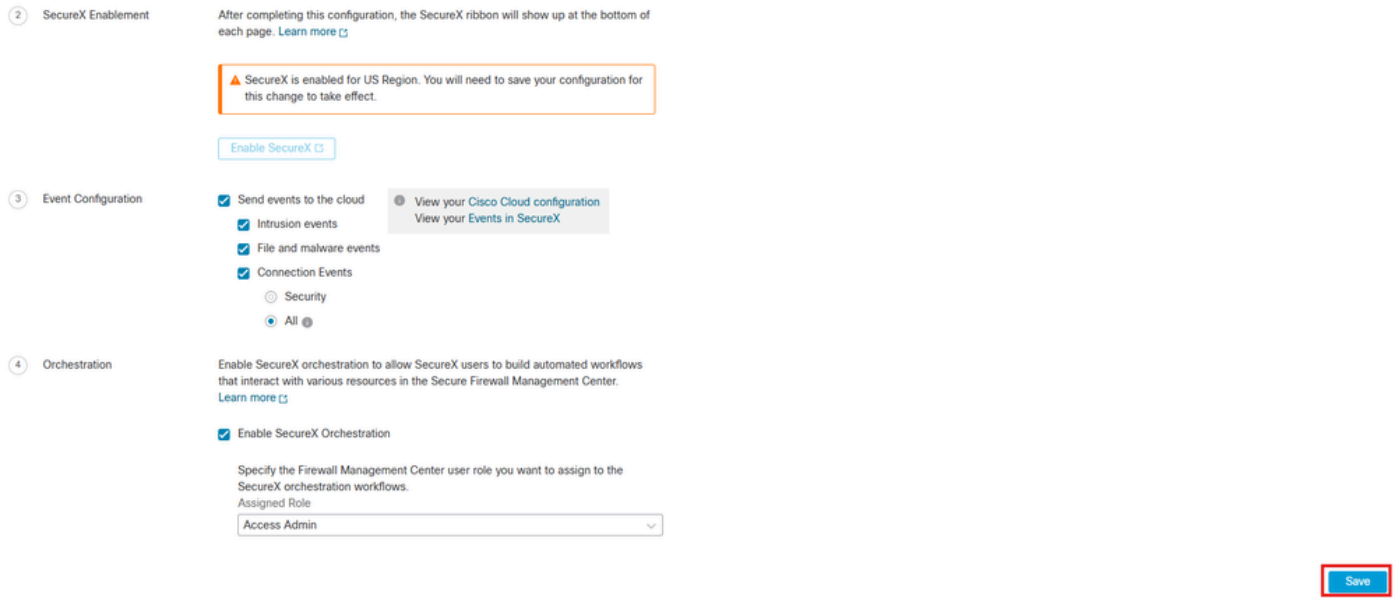


Passaggio 6. Inserire le credenziali di accesso a Security Cloud e autorizzare l'integrazione. Al termine, viene presentata una conferma che FMC è stato autorizzato a registrare con Cisco Security Cloud.



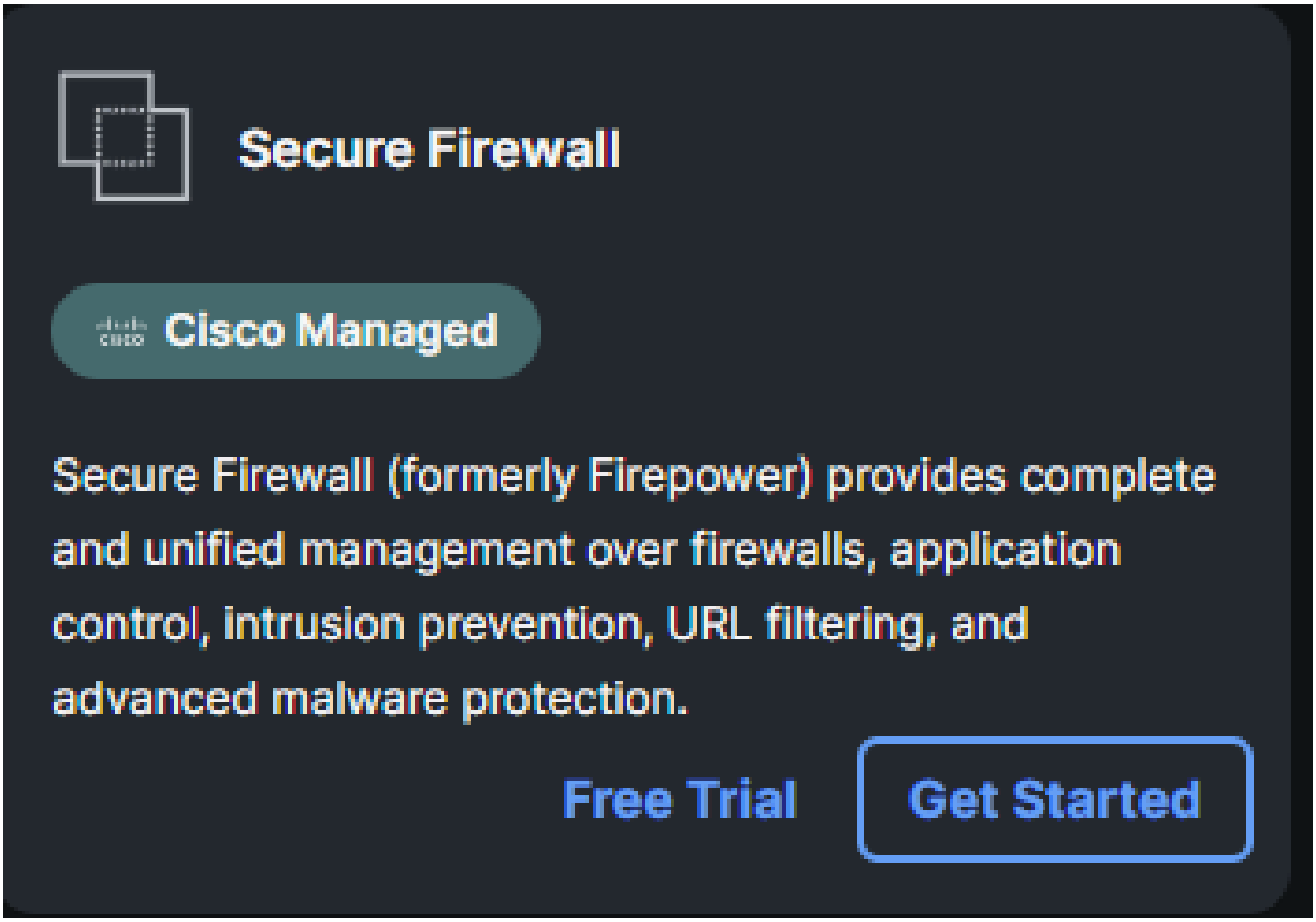
Passaggio 7. Dopo aver completato l'autorizzazione, è possibile tornare al FMC e selezionare gli eventi da inviare al cloud. Al termine, fare clic su Salva.

Passaggio 8. È possibile selezionare Abilita orchestrazione SecureX (XDR Automate)

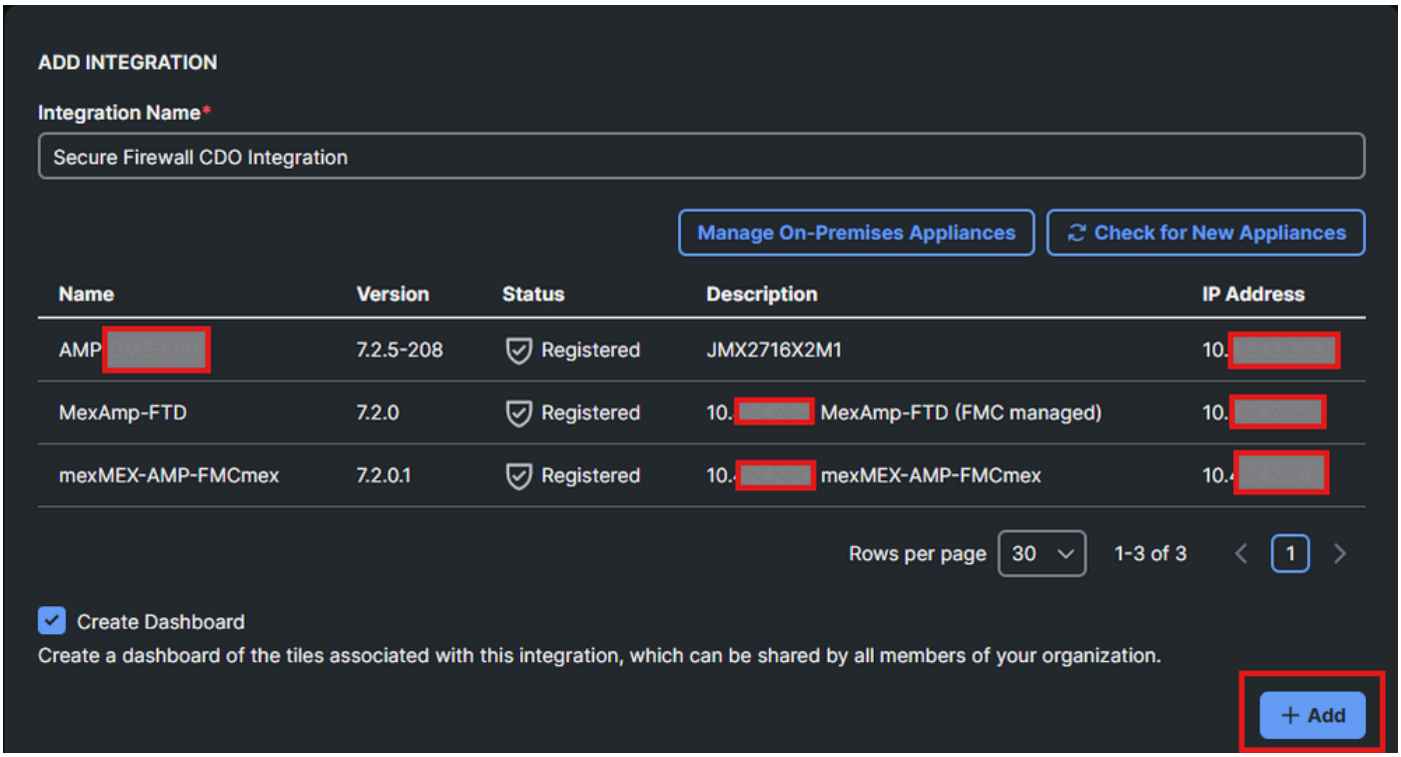


Passaggio 9. Passare a XDR > Amministrazione >Accessorio locale e cercare gli accessori, che devono essere registrati automaticamente.

Passaggio 10. Passare a XDR > Amministrazione > Integrazioni e abilitare l'integrazione Secure Firewall.



Passaggio 10.1. Assegnare un nome all'integrazione, fare clic su +Aggiungi.



Questa integrazione consente di arricchire le ricerche all'interno di XDR.

Metodo 2 (Integrazione completa): Arricchimento dei casi in XDR

Nota: Per garantire l'integrazione completa tra Secure Firewall, XDR, Cisco Defense Orchestrator (CDO), Security Services Exchange (SSX) e Security Analytics and Logging (SAL), è necessario il mapping manuale. Questo processo comporta la connessione a Cisco TAC per eseguire le configurazioni e le mappature necessarie.

Passaggio 1. L'account CDO deve disporre di una licenza Security Analytics and Logging per inoltrare gli eventi a Cisco XDR.

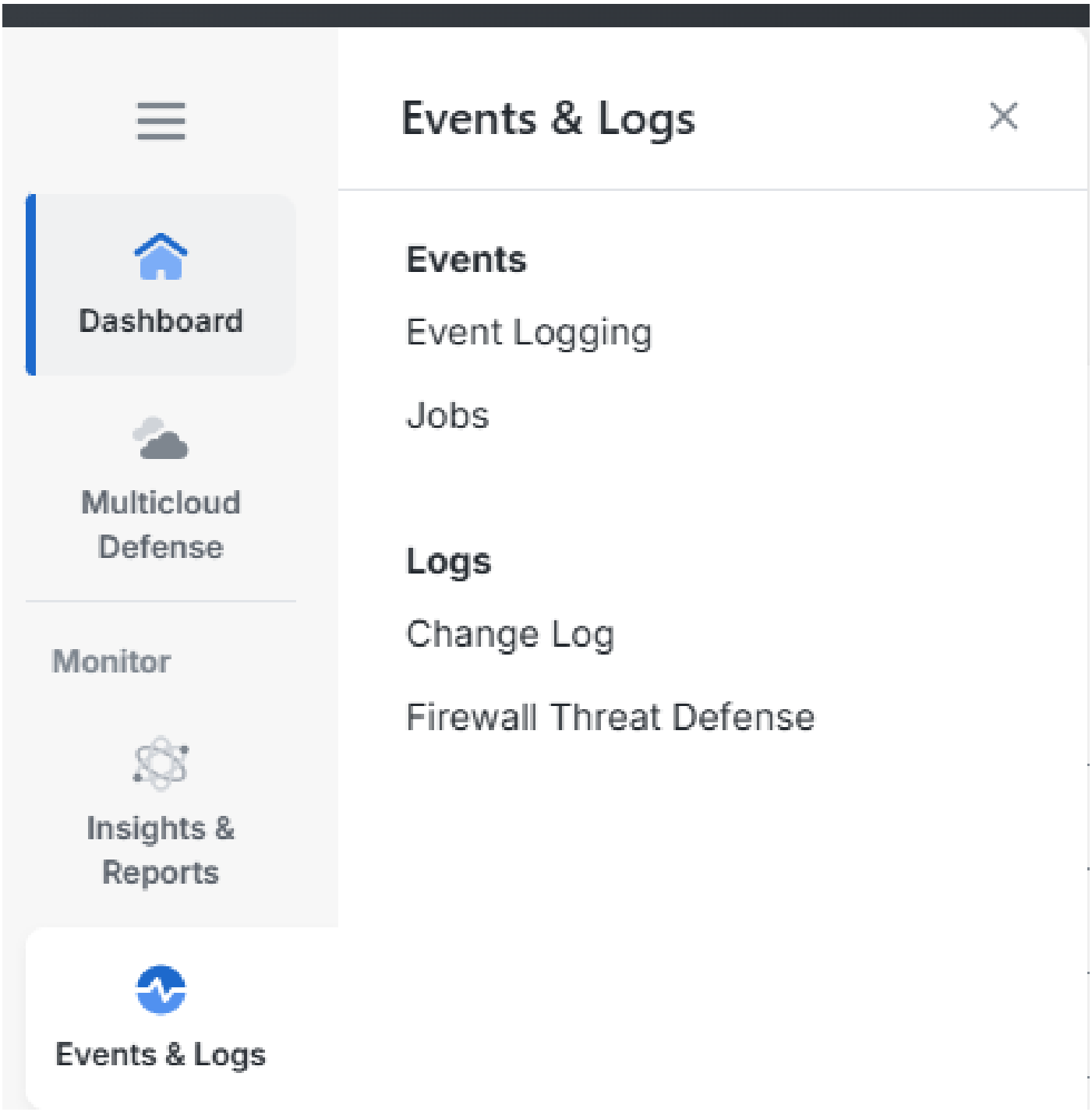
Passaggio 2. Per registrare gli accessori in SSX e Security Cloud Control, attenersi alla procedura descritta in precedenza.

Passaggio 3. Una volta terminato, contatta TAC con questi dettagli e richiedi di collegare Security Cloud Control/SAL a XDR Analytics.

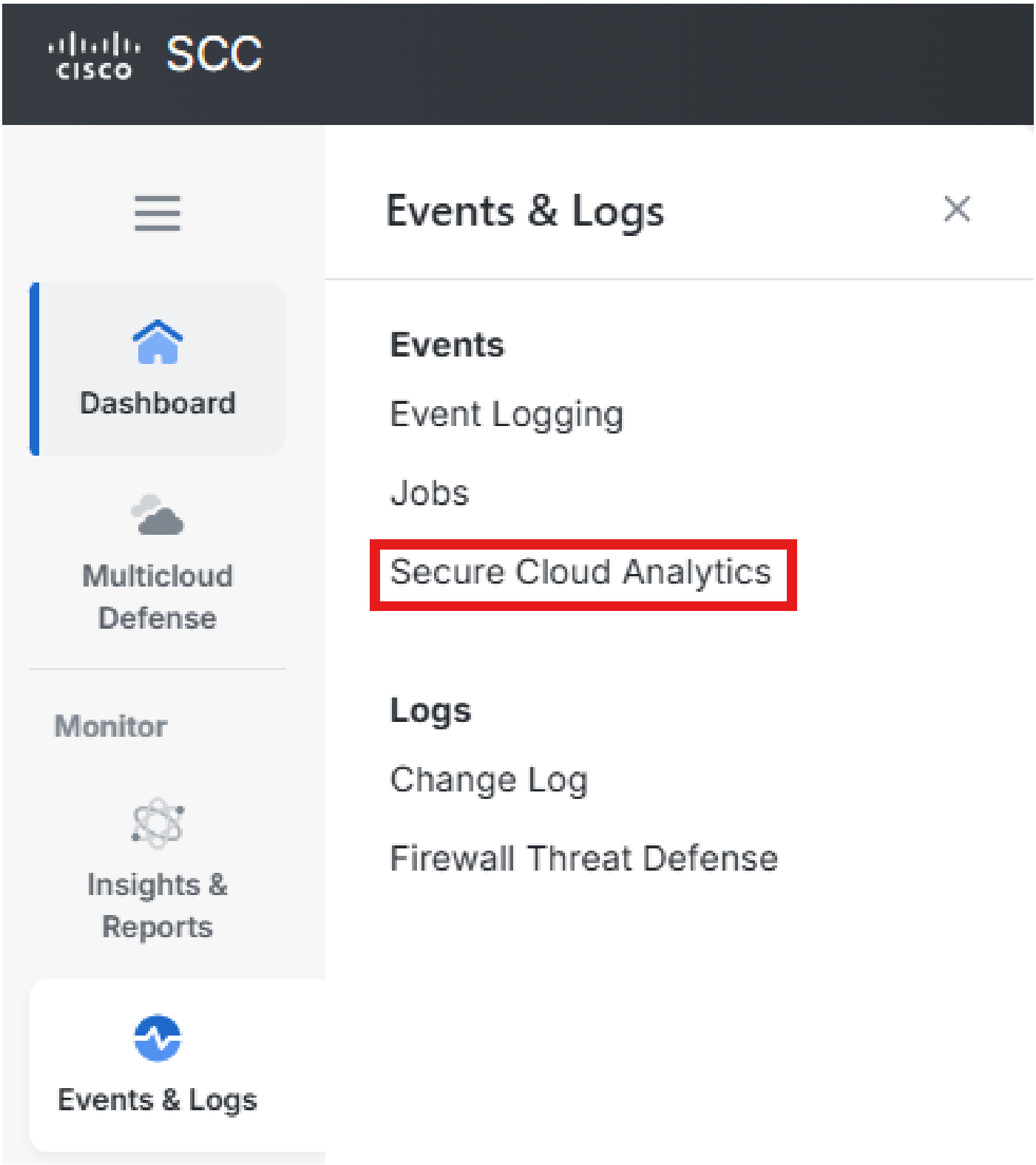
- ID tenant CDO
- Nome CDO
- ID organizzazione XDR
- ID tenant SSX
- Nome SSX
- ID organizzazione SCA

Passaggio 4. Verificare che l'account CDO sia collegato al portale XDR Analytics.

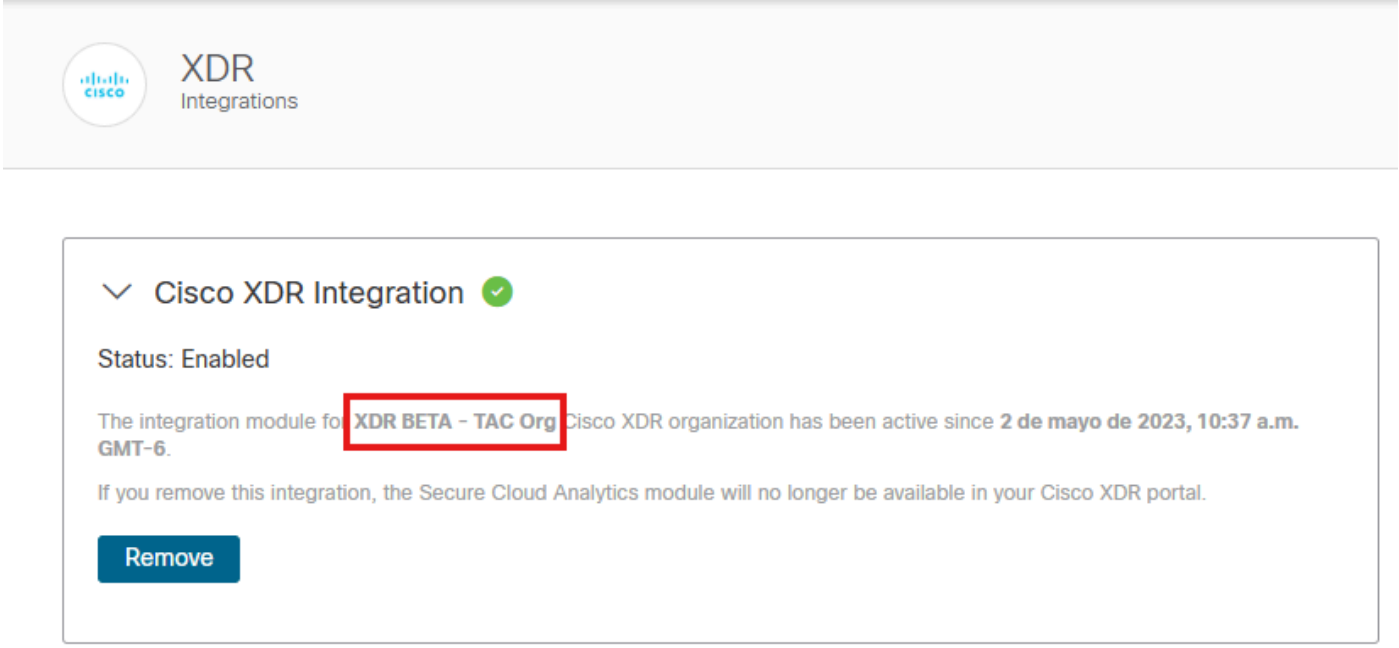
Prima di collegare il portale CDO a XDR Analytics, è possibile ottenere il seguente aspetto:



Al termine del collegamento, sarà possibile visualizzare l'opzione per passare al portale XDR Analytics.



Passaggio 5. Dopo aver collegato l'account XDR Analytics al portale di controllo di Security Cloud (CDO), è necessario verificare che l'account XDR Analytics sia integrato con XDR. A tale scopo, in XDR Analytics, passare a Impostazioni >Integrazioni >XDR, cercare Integrazione XDR e verificare che sia presente un controllo verde e che il modulo Integrazione punti all'organizzazione XDR corretta.



Verifica

Verificare che i firewall sicuri generino 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 SSX come indicato nella sezione Registrazione dei dispositivi su SSX al 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.

Verificare che tutti i tenant siano collegati correttamente. In caso di problemi, aprire una richiesta TAC e fornire i seguenti dettagli:

- ID tenant CDO
- Nome CDO
- ID organizzazione XDR
- ID tenant SSX
- Nome SSX
- ID organizzazione SCA

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-timeo
```

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 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;
```

Problemi di registrazione su SSX Portal

Sia FMC che Secure Firewall necessitano di una connessione agli URL SSX 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
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;
```

Nota: Viene visualizzato il messaggio 403 Forbidden poiché i parametri inviati dal test non sono quelli previsti da SSX, 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_SSEConnecto
```

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

Verifica dei dati inviati al portale SSX e al CTR

Per inviare eventi dal dispositivo Secure Firewall a SSX, è necessario stabilire una connessione TCP con https://eventing-ingest.sse.itd.cisco.com Questo è un esempio di connessione non stabilita tra il portale SSX e Secure Firewall:

```
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.a
```

Nei log di connector.log:

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

Nota: Notato che gli indirizzi IP visualizzati 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 SSX in base a URL anziché a indirizzi IP.

Se la connessione non viene stabilita, gli eventi non vengono inviati al portale SSX. Questo è un esempio di connessione stabilita tra il Secure Firewall e il portale SSX:

```
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.
```

Impossibile registrare il dispositivo (FTD) in Security Cloud Control

Se non è possibile registrare il dispositivo in Security Cloud Control, verificare che disponga della connettività al tenant CDO appropriato.

Per verificare l'URL corretto, passare ad Amministrazione> Centro gestione firewall, selezionare Cloud Delivered FMC, in alto a destra dello schermo è possibile visualizzare il nome host.

```
admin@MexAmpFTD:~$ nc -vz xxxxxxxx.app.us.cdo.cisco.com 443
Connection to xxxxxxxx.app.us.cdo.cisco.com 443 port [tcp/https] succeeded!
```

Se si verificano ancora problemi di connessione a CDO, verificare che la porta 8305 sia aperta, ad esempio un problema di connessione.

```
admin@AMP-DMZ-FPR:~$ sudo tail /ngfw/var/log/messages
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneld:sf_peers [INFO] Peer xxxxxxxx.app.us.cdo.ci
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneld:sf_ssl [INFO] Connect to xxxxxxxx.app.us.cd
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneld:sf_ssl [INFO] Initiate connection using res
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneld:sf_ssl [INFO] Initiate IPv6 type connection
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneld:sf_ssl [INFO] Initiate IPv4 type connection
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneld:sf_ssl [INFO] Initiate IPv4 connection from
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneld:sf_ssl [INFO] Initiating IPv4 connection to
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneld:sf_ssl [INFO] Wait to connect to 8305 (IPv4)
Jan 25 18:48:56 AMP-DMZ-FPR SF-IMS[20448]: [1465] sftunneld:sf_ssl [INFO] Connect to x.x.x.51 failed on
```

Registrazione del dispositivo al tenant SSX errato

È possibile verificare a quale tenant SSX è registrato il CCP.

```
admin@fmc01:~$ curl localhost:8989/v1/contexts/default/tenant

{"registeredTenantInfo":{"companyId":"689xxxxx-eaxx-5bxx-b1xx-a7662axxxxx","companyName":"XDR BETA - TA
```

Se il tenant SSX non è corretto, è necessario ripetere i passaggi per registrare gli accessori in SSX

Se il tenant SSX è corretto, ma il tenant CDO non è collegato all'organizzazione SSX appropriata, contattare TAC con questi dettagli:

- ID tenant SSX
- ID tenant CDO

Informazioni correlate

- Guida all'integrazione di Cisco Secure Firewall Threat Defense e Cisco XDR
- Supporto tecnico Cisco e download

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).