Configurazione e risoluzione dei problemi di Cisco XDR con Secure Firewall release 7.2

Sommario

Introduzione

In questo documento viene descritto come integrare e risolvere i problemi di Cisco XDR con l'integrazione di Cisco Secure Firewall su Secure Firewall 7.2.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firepower Management Center (FMC)
- Cisco Secure Firewall
- Virtualizzazione delle immagini opzionale
- È necessario disporre della licenza per Secure Firewall e FMC

Componenti usati

- Cisco Secure Firewall - 7.2
- Firepower Management Center (FMC) - 7.2
- SSE (Security Services Exchange)
- Cisco XDR
- Portale delle licenze Smart
- Cisco Threat Response (CTR)

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.

Introduzione

La versione 7.2 include modifiche al modo in cui Secure Firewall si integra con Cisco XDR e Cisco XDR Orchestration:

Funzionalità	Descrizione
Miglioramento dell'integrazione Cisco XDR, orchestrazione Cisco XDR.	We have streamlined the SecureX integration process. Now, as long as you already have a SecureX account, you just choose your cloud region on the new Integration > SecureX page, click Enable SecureX, and authenticate to SecureX. The option to send events to the cloud, as well as to enable Cisco Success Network and Cisco Support Diagnostics, are also moved to this new page. When you enable SecureX integration on this new page, licensing and management for the systems's cloud connection switches from Cisco Smart Licensing to SecureX. If you already enabled SecureX the "old" way, you must disable and re-enable to get the benefits of this cloud connection management. Note that this page also governs the cloud region for and event types sent to the Secure Network Analytics (Stealthwatch) cloud using Security Analytics and Logging (SaaS), even though the web interface does not indicate this. Previously, these options were on System > Integration > Cloud Services. Enabling SecureX does not affect communications with the Secure Network Analytics cloud; you can send events to both. The management center also now supports SecureX orchestrationâ€”a powerful drag-and-drop interface you can use to automate workflows across security tools. After you enable SecureX, you can enable orchestration.

Consultare la sezione 7.2 **Note** di **rilascio** complete per controllare tutte le funzioni incluse in questa release.

Configurazione

Prima di avviare l'integrazione, verificare che nell'ambiente siano consentiti i seguenti URL:

Regione USA

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

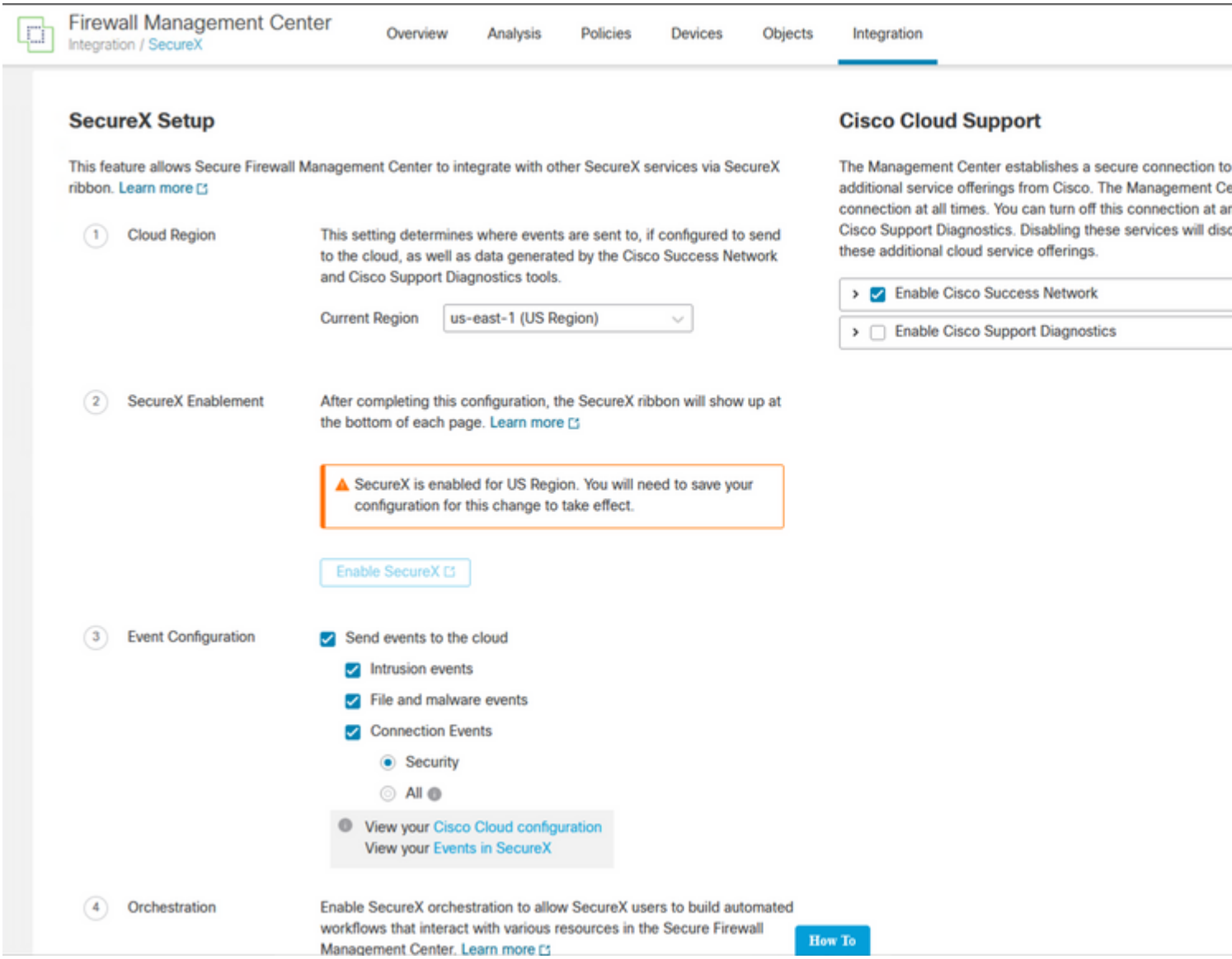
Regione UE

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

Area APJ

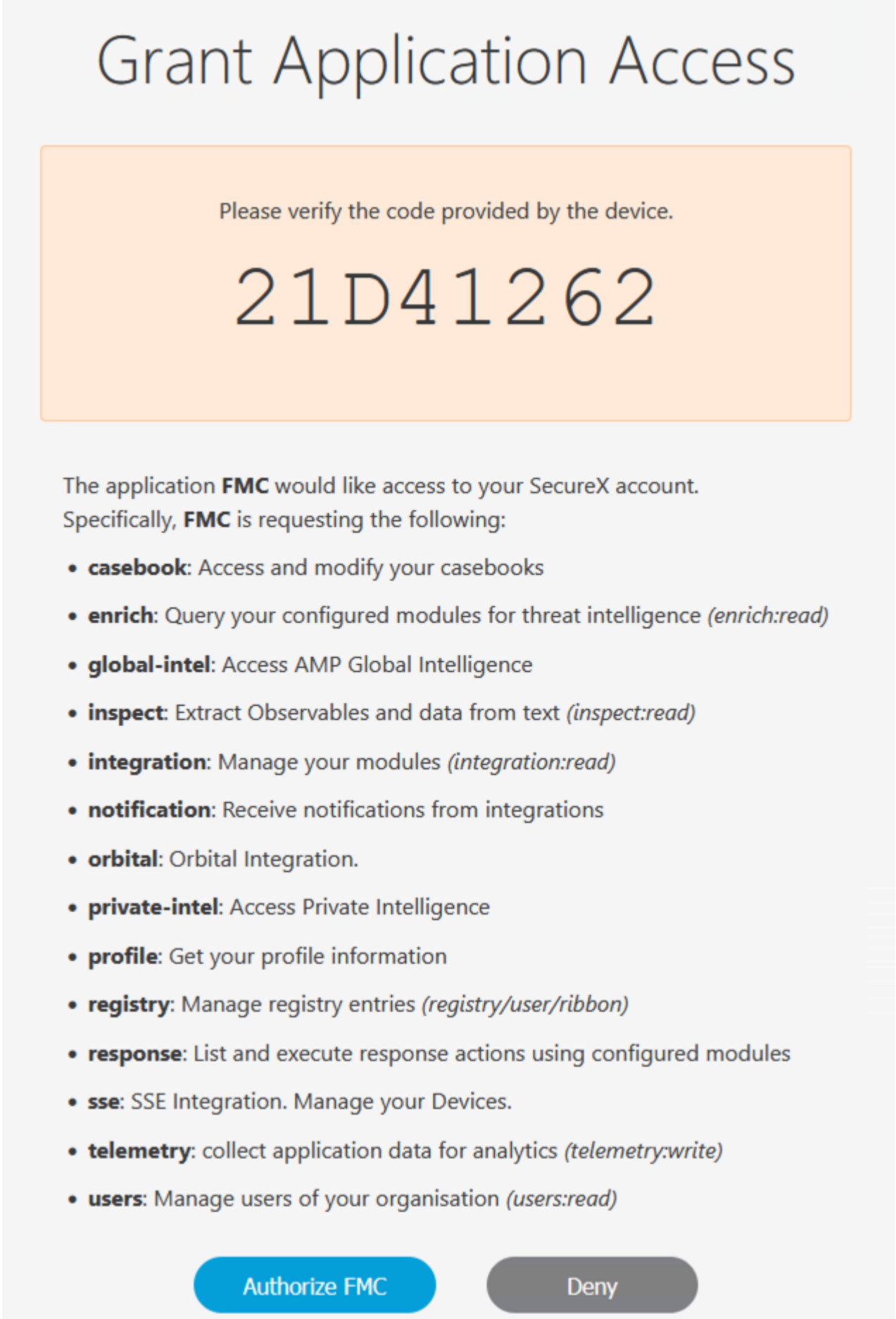
- api.apj.sse.itd.cisco.com
- eventing-ingest.apj.sse.itd.cisco.com

Passaggio 1. Avviare il log di integrazione nel CCP. Andare a **Integrazione>Cisco XDR,** selezionare la regione a cui ci si desidera connettere (Stati Uniti, UE o APJC), selezionare il tipo di eventi che si desidera inoltrare a Cisco XDR, quindi selezionare **Abilita Cisco XDR:**

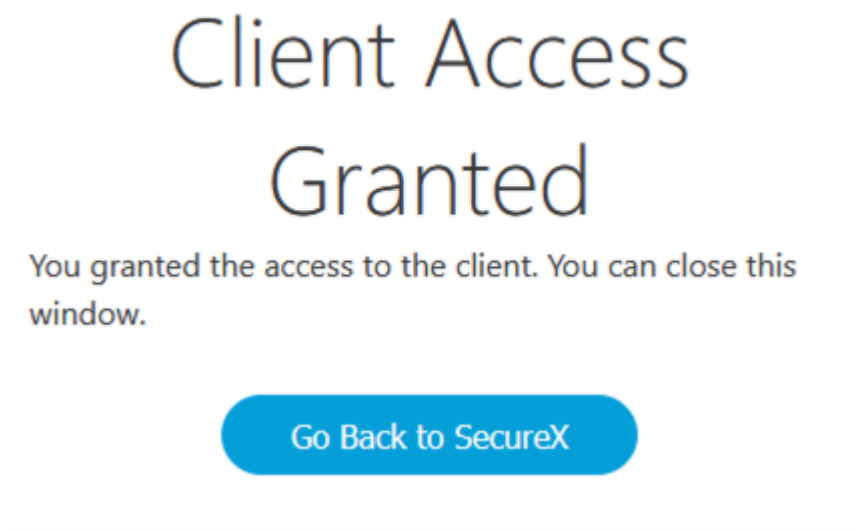


Le modifiche non vengono applicate finché non si seleziona Save .

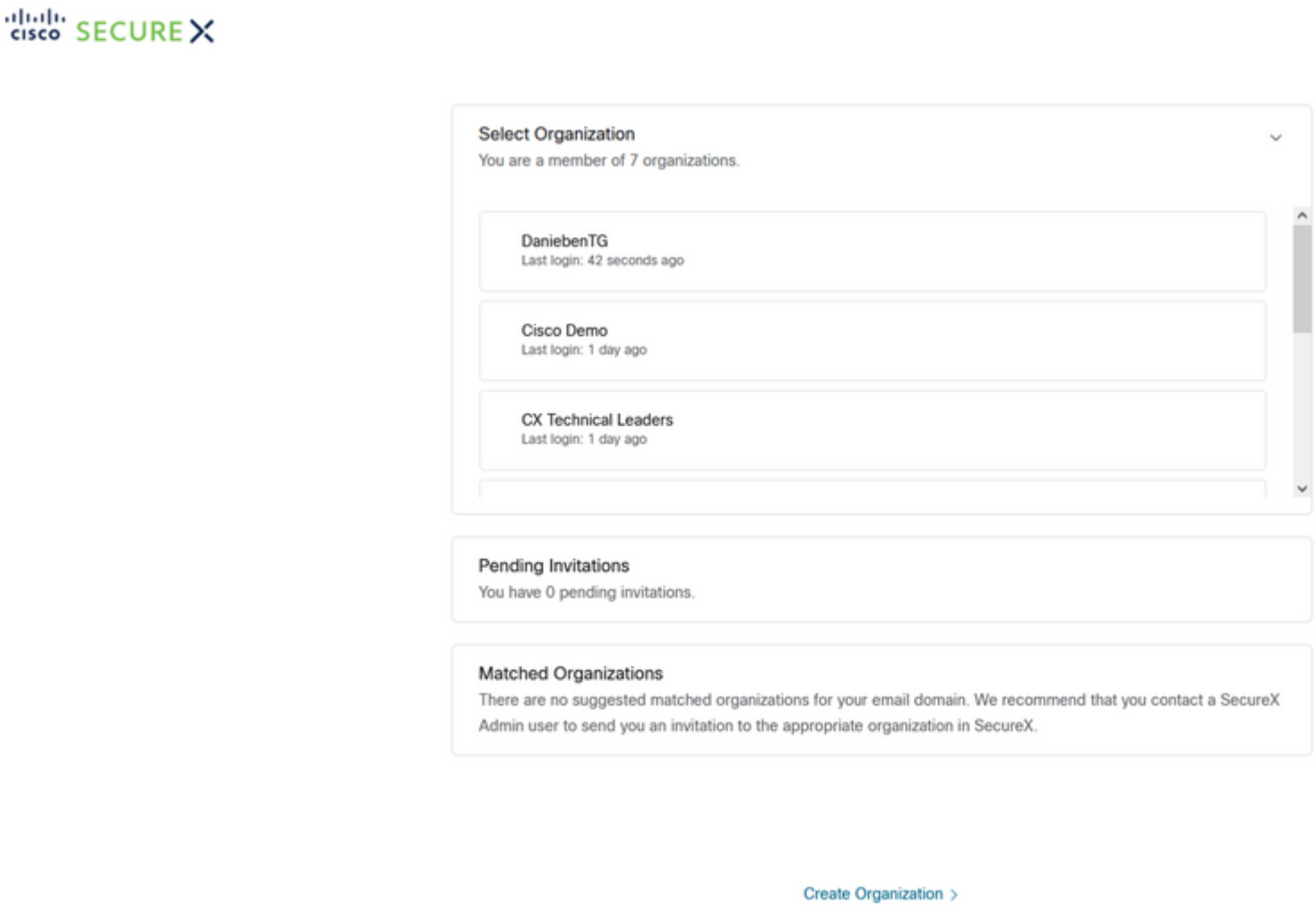
Passaggio 2. Dopo aver selezionato Save (Salva), si viene reindirizzati all'account FMC autorizzato nell'account Cisco XDR (è necessario accedere all'account Cisco XDR prima di questo passaggio). Selezionare Authorize FMC (Autorizza FMC):



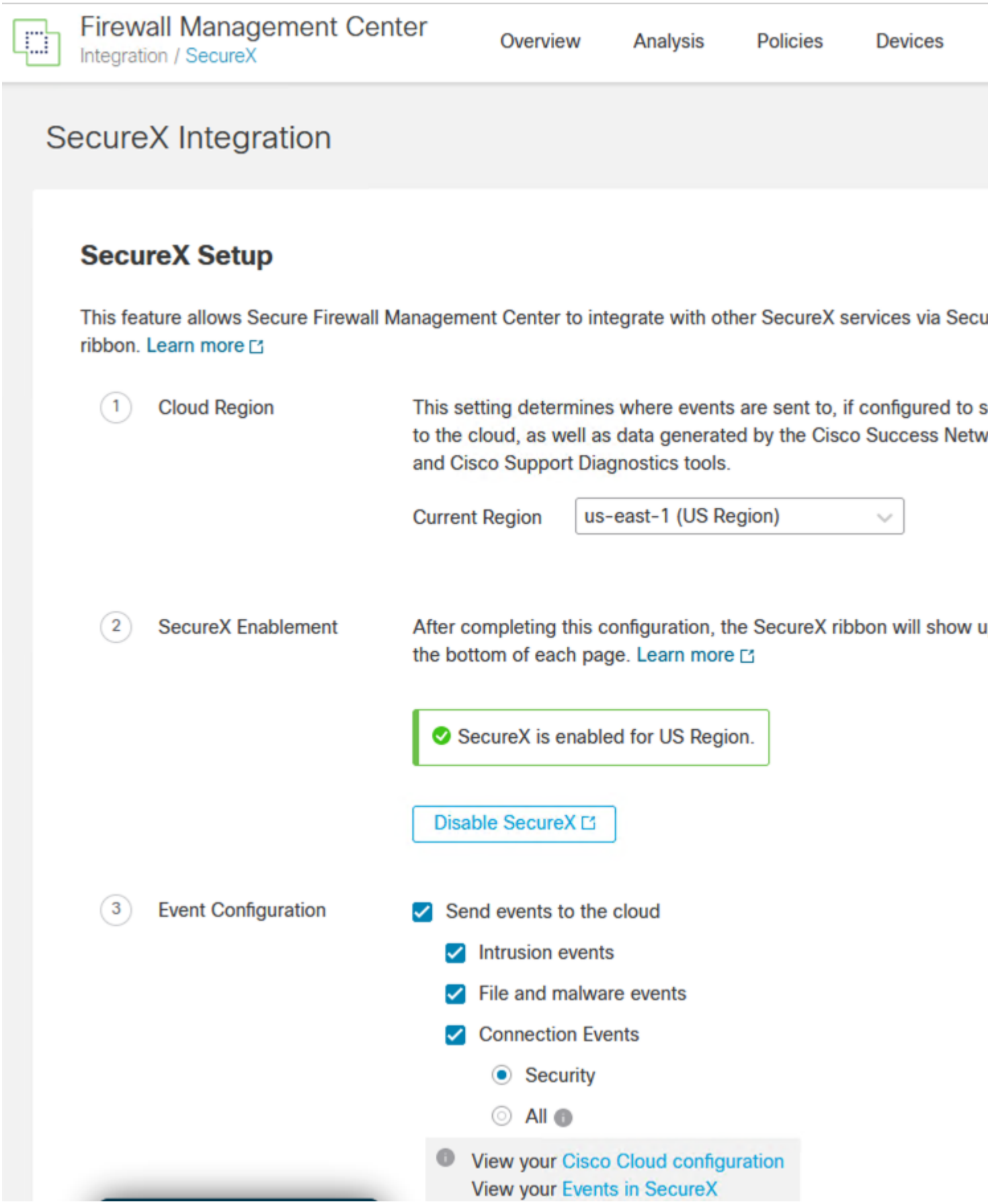
Passaggio 3. Dopo aver concesso l'autorizzazione, si viene reindirizzati a Cisco XDR:



Se si hanno più organizzazioni, viene visualizzata la pagina iniziale Cisco XDR in cui è possibile selezionare l'organizzazione in cui si desidera integrare il FMC e i dispositivi Secure Firewall:

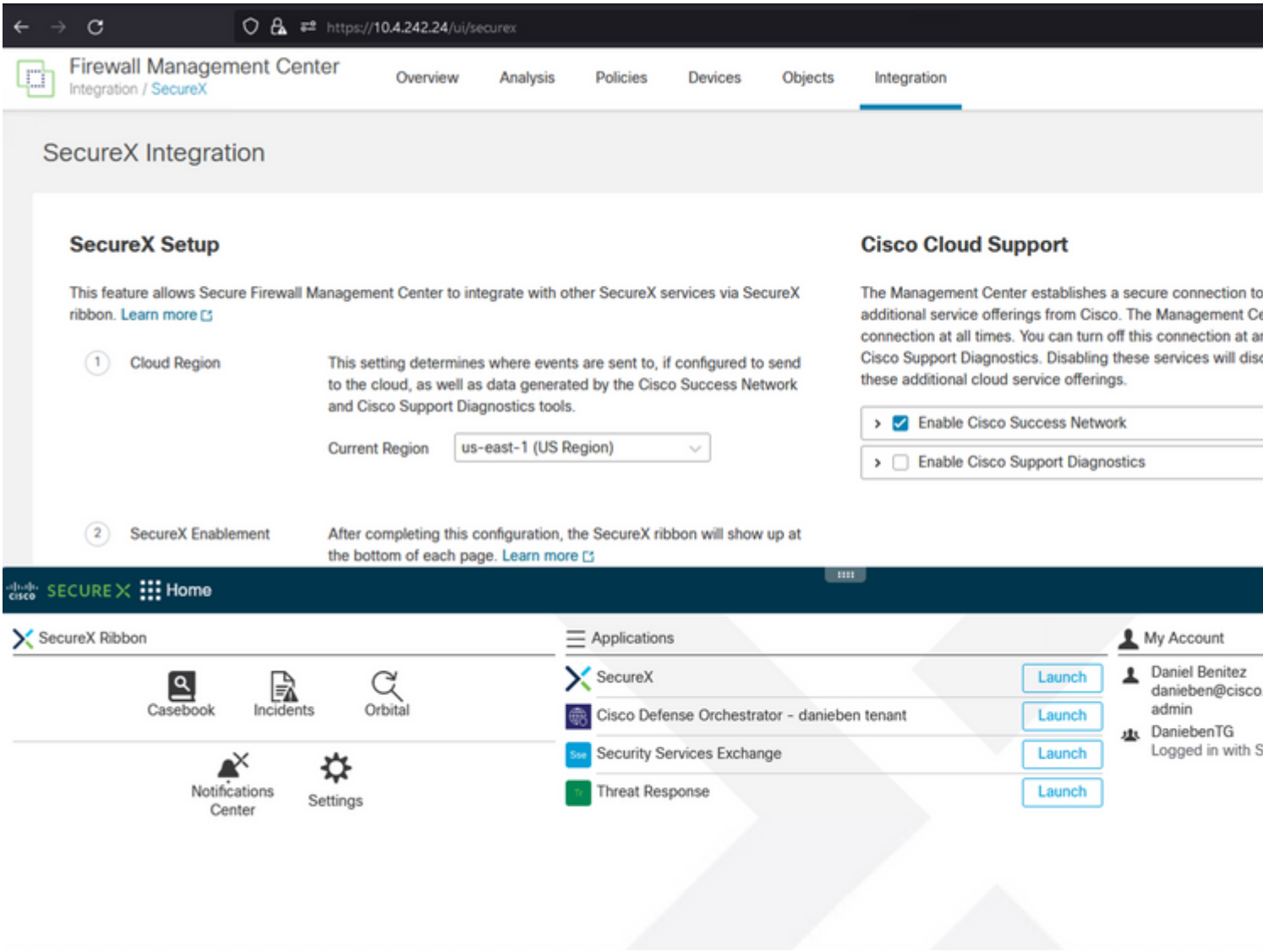


Passaggio 4. Dopo aver selezionato l'organizzazione Cisco XDR, si viene nuovamente reindirizzati al FMC e viene visualizzato il messaggio indicante che l'integrazione è riuscita:

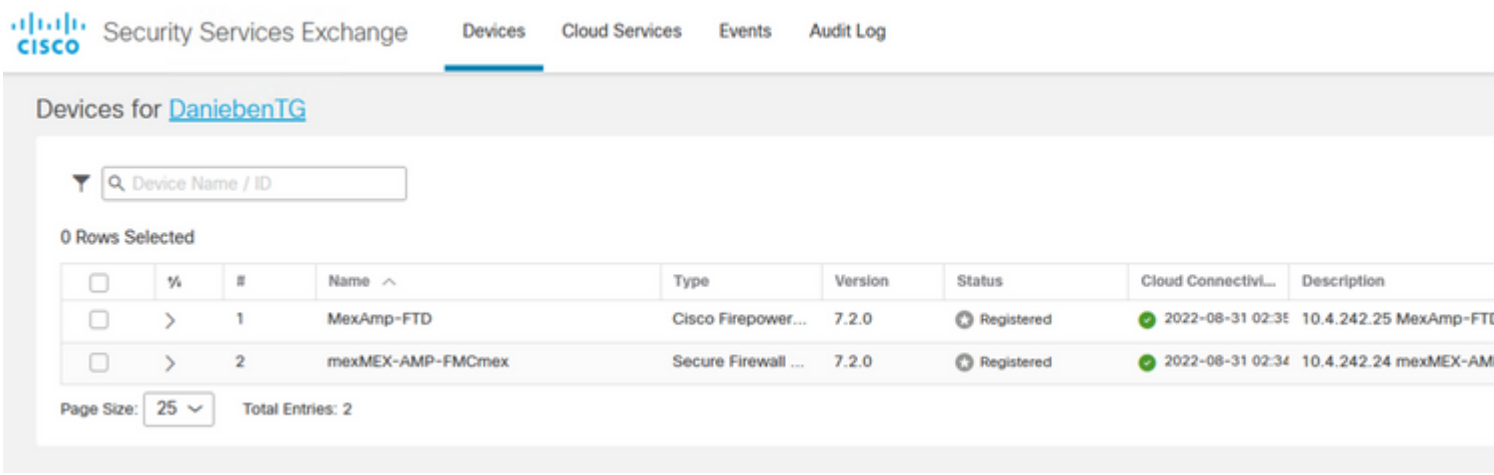

Firewall Management Center
Integration / SecureX
Overview
Analysis
Policies
Devices
SecureX Integration
SecureX Setup
This feature allows Secure Firewall Management Center to integrate with other SecureX services via Secu
ribbon. Learn more
1
Cloud Region
This setting determines where events are sent to, if configured to s
to the cloud, as well as data generated by the Cisco Success Netw
and Cisco Support Diagnostics tools.
Current Region
us-east-1 (US Region)
2
SecureX Enablement
After completing this configuration, the SecureX ribbon will show u
the bottom of each page. Learn more
SecureX is enabled for US Region.
Disable SecureX
3
Event Configuration
Send events to the cloud
Intrusion events
File and malware events
Connection Events
Security
All
View your Cisco Cloud configuration
View your Events in SecureX

Verifica

Al termine dell'integrazione, è possibile espandere la **barra multifunzione** dalla parte inferiore della pagina:



Sulla **barra multifunzione**, avviare **Security Services Exchange** e sotto **Devices** è necessario visualizzare sia FMC che Secure Firewall appena integrati:



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).