

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

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Introduzione](#)

[Configurazione](#)

[Verifica](#)

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
<p>Miglioramento dell'integrazione Cisco XDR, orchestrazione Cisco XDR.</p>	<p>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.</p>

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**:



SecureX Setup

This feature allows Secure Firewall Management Center to integrate with other SecureX services via SecureX ribbon. [Learn more](#)

1 Cloud Region

This setting determines where events are sent to, if configured to send to the cloud, as well as data generated by the Cisco Success Network and Cisco Support Diagnostics tools.

Current Region

2 SecureX Enablement

After completing this configuration, the SecureX ribbon will show up at the bottom of each page. [Learn more](#)

▲ SecureX is enabled for US Region. You will need to save your configuration for this change to take effect.

[Enable 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](#)

4 Orchestration

Enable SecureX orchestration to allow SecureX users to build automated workflows that interact with various resources in the Secure Firewall Management Center. [Learn more](#)

[How To](#)

Cisco Cloud Support

The Management Center establishes a secure connection to additional service offerings from Cisco. The Management Center connection at all times. You can turn off this connection at any time. Disabling these services will disconnect the Management Center from these additional cloud service offerings.

Enable Cisco Success Network

Enable Cisco Support Diagnostics

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):

Grant Application Access

Please verify the code provided by the device.

21D41262

The application **FMC** would like access to your SecureX account. Specifically, **FMC** is requesting the following:

- **casebook:** Access and modify your casebooks
- **enrich:** Query your configured modules for threat intelligence (*enrich:read*)
- **global-intel:** Access AMP Global Intelligence
- **inspect:** Extract Observables and data from text (*inspect:read*)
- **integration:** Manage your modules (*integration:read*)
- **notification:** Receive notifications from integrations
- **orbital:** Orbital Integration.
- **private-intel:** Access Private Intelligence
- **profile:** Get your profile information
- **registry:** Manage registry entries (*registry/user/ribbon*)
- **response:** List and execute response actions using configured modules
- **sse:** SSE Integration. Manage your Devices.
- **telemetry:** collect application data for analytics (*telemetry:write*)
- **users:** Manage users of your organisation (*users:read*)

Authorize FMC

Deny

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

Client Access Granted

You granted the access to the client. You can close this window.

[Go Back to SecureX](#)

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:



Select Organization

You are a member of 7 organizations.

- DaniebenTG**
Last login: 42 seconds ago
- Cisco Demo**
Last login: 1 day ago
- CX Technical Leaders**
Last login: 1 day ago

Pending Invitations

You have 0 pending invitations.

Matched Organizations

There are no suggested matched organizations for your email domain. We recommend that you contact a SecureX Admin user to send you an invitation to the appropriate organization in SecureX.

[Create Organization >](#)

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:



SecureX Integration

SecureX Setup

This feature allows Secure Firewall Management Center to integrate with other SecureX services via SecureX ribbon. [Learn more](#)

1 Cloud Region

This setting determines where events are sent to, if configured to send to the cloud, as well as data generated by the Cisco Success Network and Cisco Support Diagnostics tools.

Current Region

2 SecureX Enablement

After completing this configuration, the SecureX ribbon will show up at 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

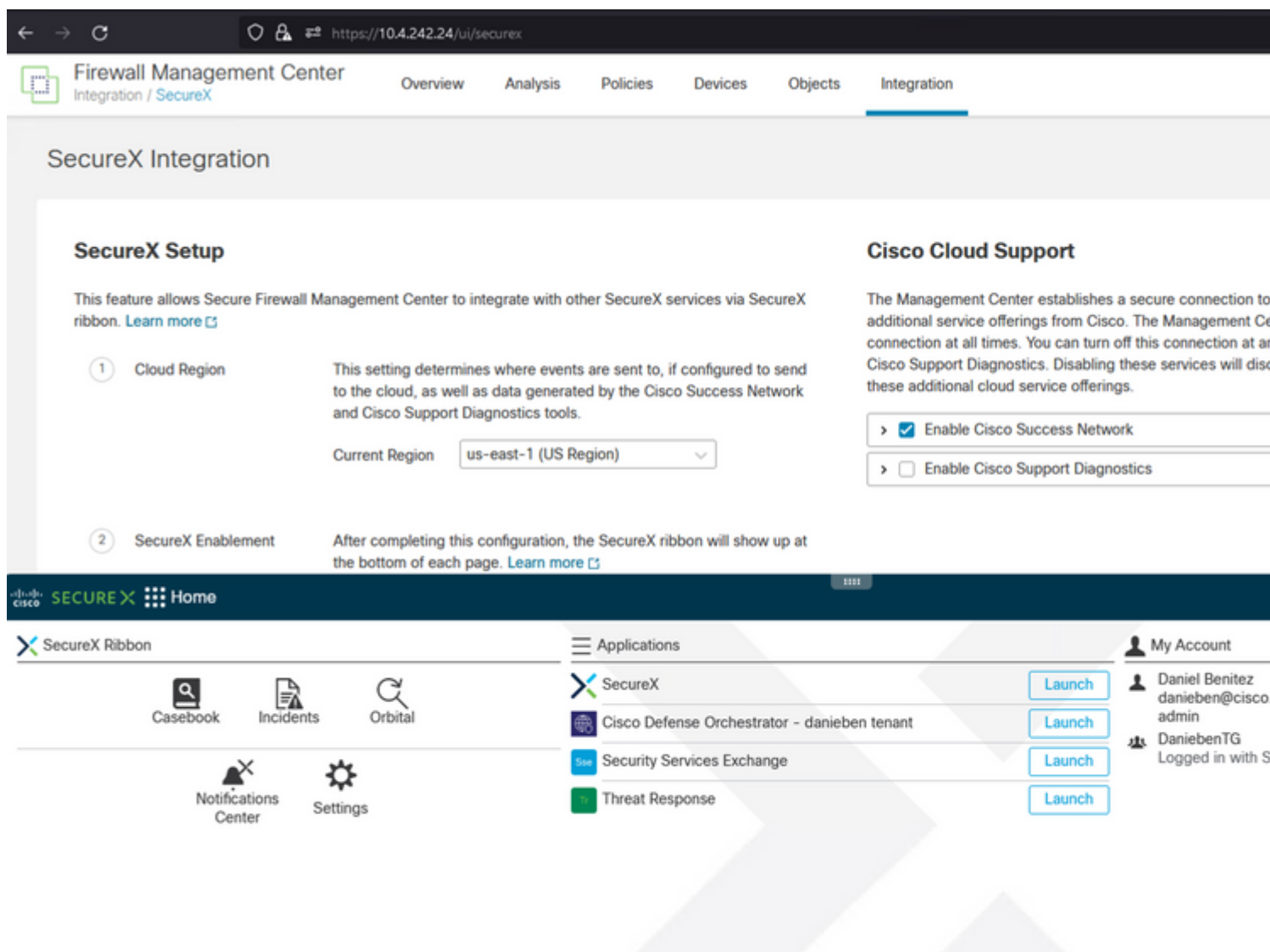
Security

All ⓘ

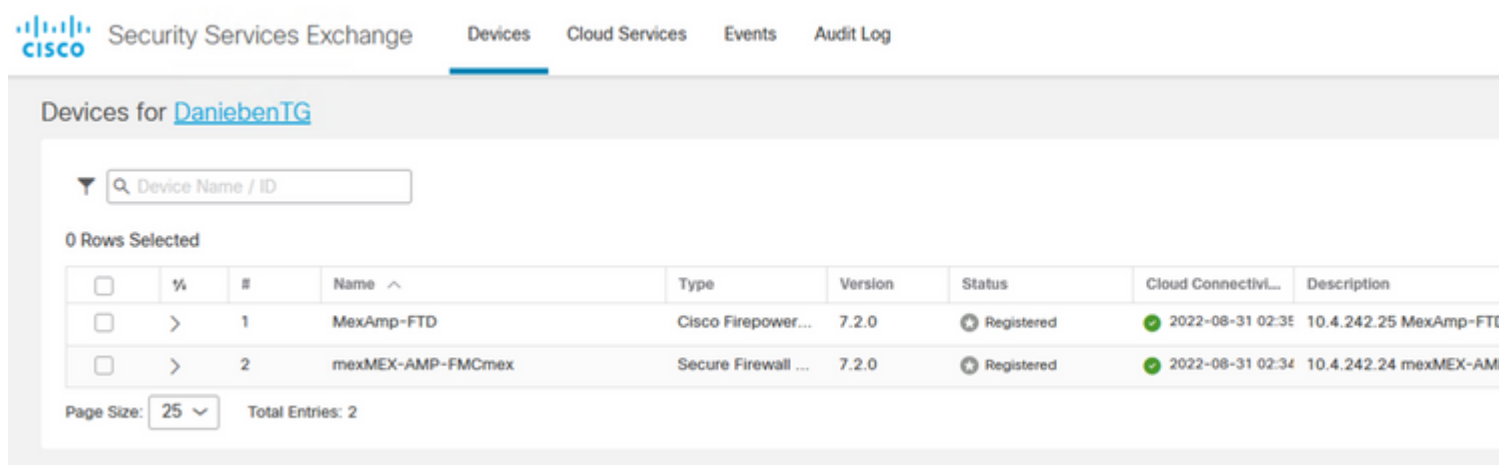
ⓘ View your [Cisco Cloud configuration](#)
View your [Events in SecureX](#)

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).