Cisco XDR mit Secure Firewall Version 7.2 konfigurieren und Fehlerbehebung dafür durchführen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Cisco XDR in die Cisco Secure Firewall 7.2 integriert wird, um Probleme mit dieser zu beheben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Firepower Management Center (FMC)
- Sichere Firewall von Cisco
- Optionale Bildvirtualisierung
- Secure Firewall und FMC müssen lizenziert werden

Verwendete Komponenten

- Cisco Secure Firewall - 7.2
- FirePOWER Management Center (FMC) - 7.2
- Security Services Exchange (SSE)
- Cisco XDR
- Smart License-Portal
- Cisco Threat Response (CTR)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrund

Version 7.2 enthält Änderungen hinsichtlich der Integration der sicheren Firewall mit Cisco XDR und Cisco

XDR Orchestration:

Funktion	Beschreibung
Verbesserte Cisco XDR-Integration, Cisco XDR-Orchestrierung.	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.

In den vollständigen **Versionshinweisen** von 7.2 finden Sie alle in dieser Version enthaltenen Funktionen.

Konfigurieren

Stellen Sie vor Beginn der Integration sicher, dass die folgenden URLs in Ihrer Umgebung zulässig sind:

Region USA

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

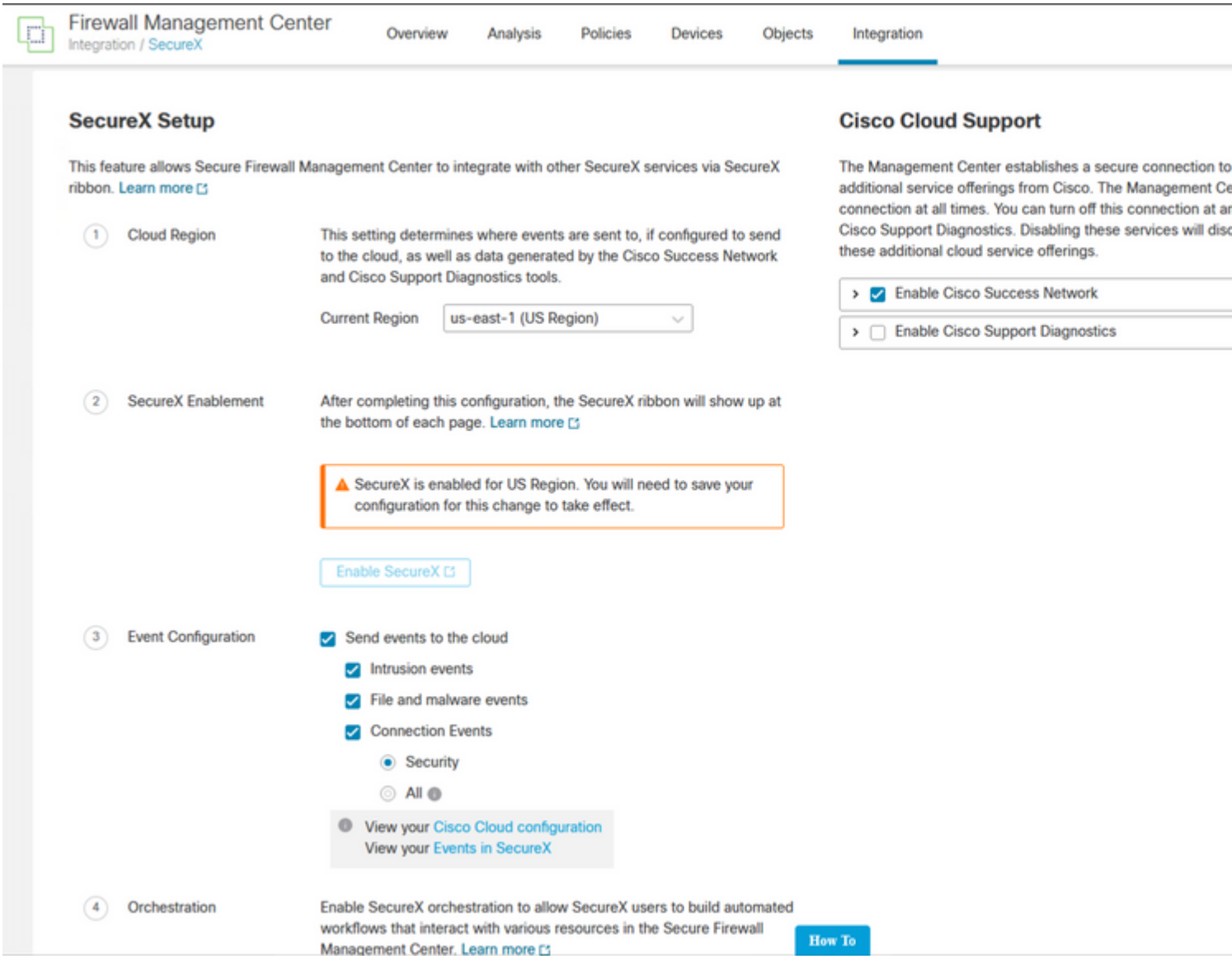
EU-Region

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

APJ-Region

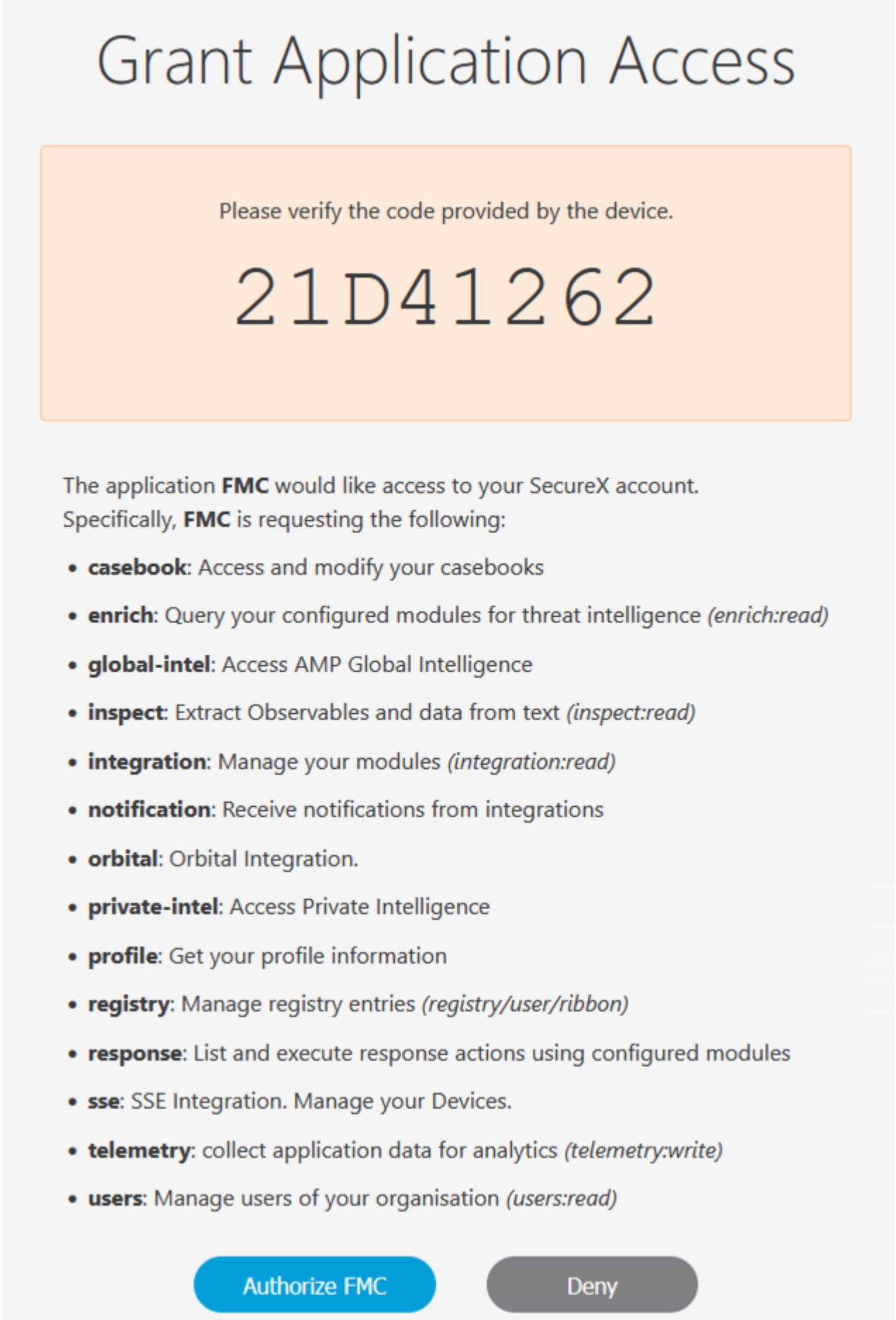
- api.apj.sse.itd.cisco.com
- eventing-ingest.apj.sse.itd.cisco.com

Schritt 1: Um die Integration zu starten, melden Sie sich beim FMC an. Gehen Sie zu **Integration>Cisco XDR,** wählen Sie die Region aus, mit der Sie eine Verbindung herstellen möchten (USA, EU oder APJC), wählen Sie die Art der Ereignisse aus, die Sie an Cisco XDR weiterleiten möchten, und wählen Sie dann **Cisco XDR aktivieren aus:**

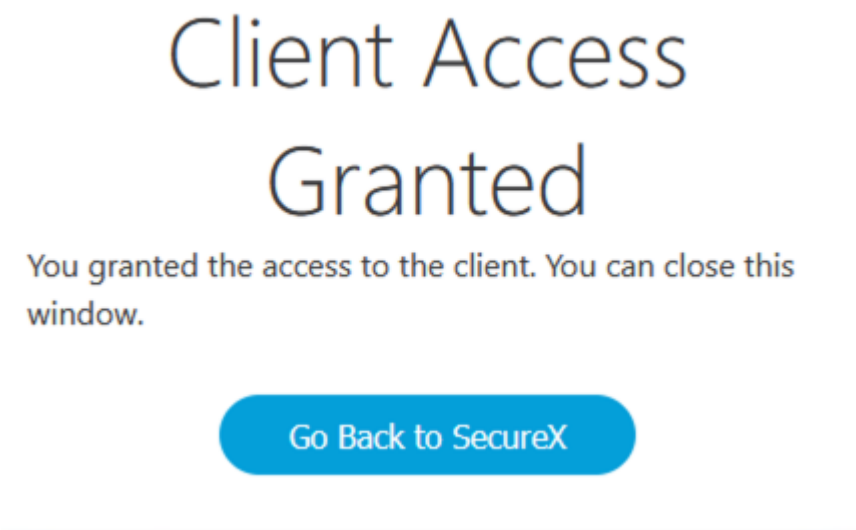


Beachten Sie, dass die Änderungen erst angewendet werden, wenn Sie Save .

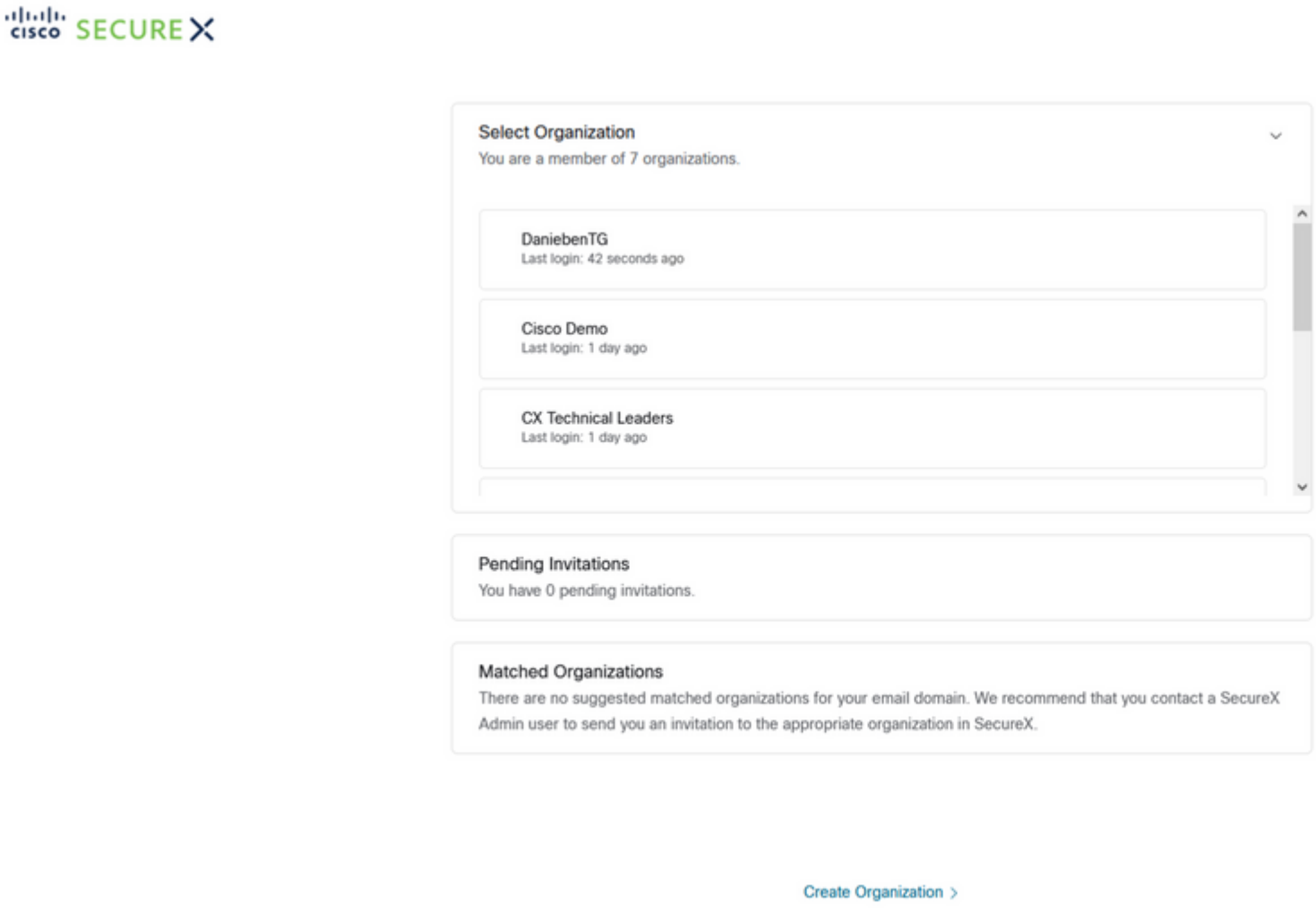
Schritt 2: Nachdem Sie "Speichern" ausgewählt haben, werden Sie an das autorisierte FMC Ihres Cisco XDR-Kontos weitergeleitet (Sie müssen sich vor diesem Schritt beim Cisco XDR-Konto anmelden). Wählen Sie **FMC autorisieren aus**:



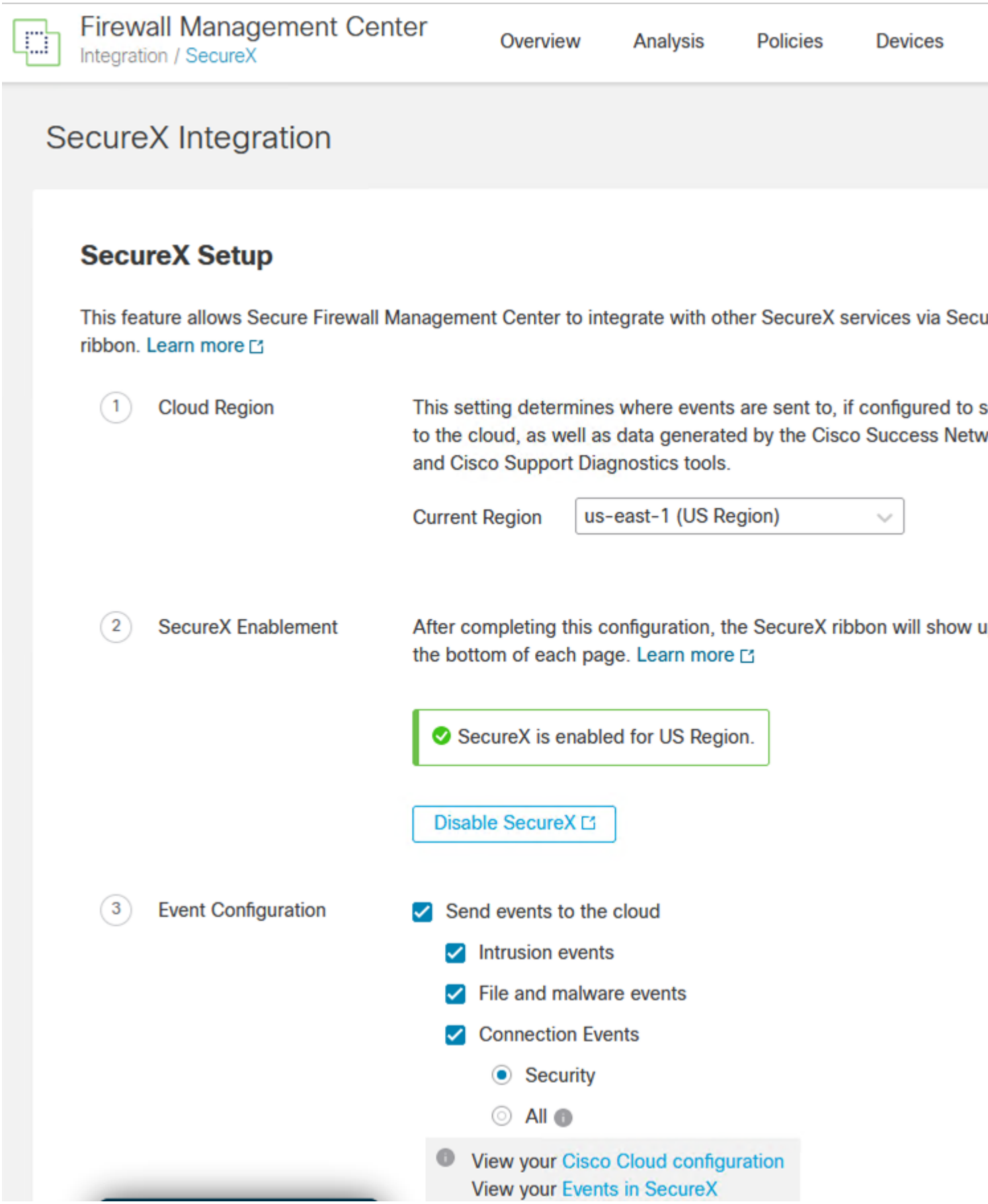
Schritt 3: Sobald die Autorisierung erteilt wurde, werden Sie zu Cisco XDR umgeleitet:



Wenn Sie mehrere Organisationen betreiben, wird Ihnen die Cisco XDR-Startseite angezeigt, auf der Sie die Organisation auswählen können, in die Sie Ihre FMC- und Secure Firewall-Geräte integrieren möchten:

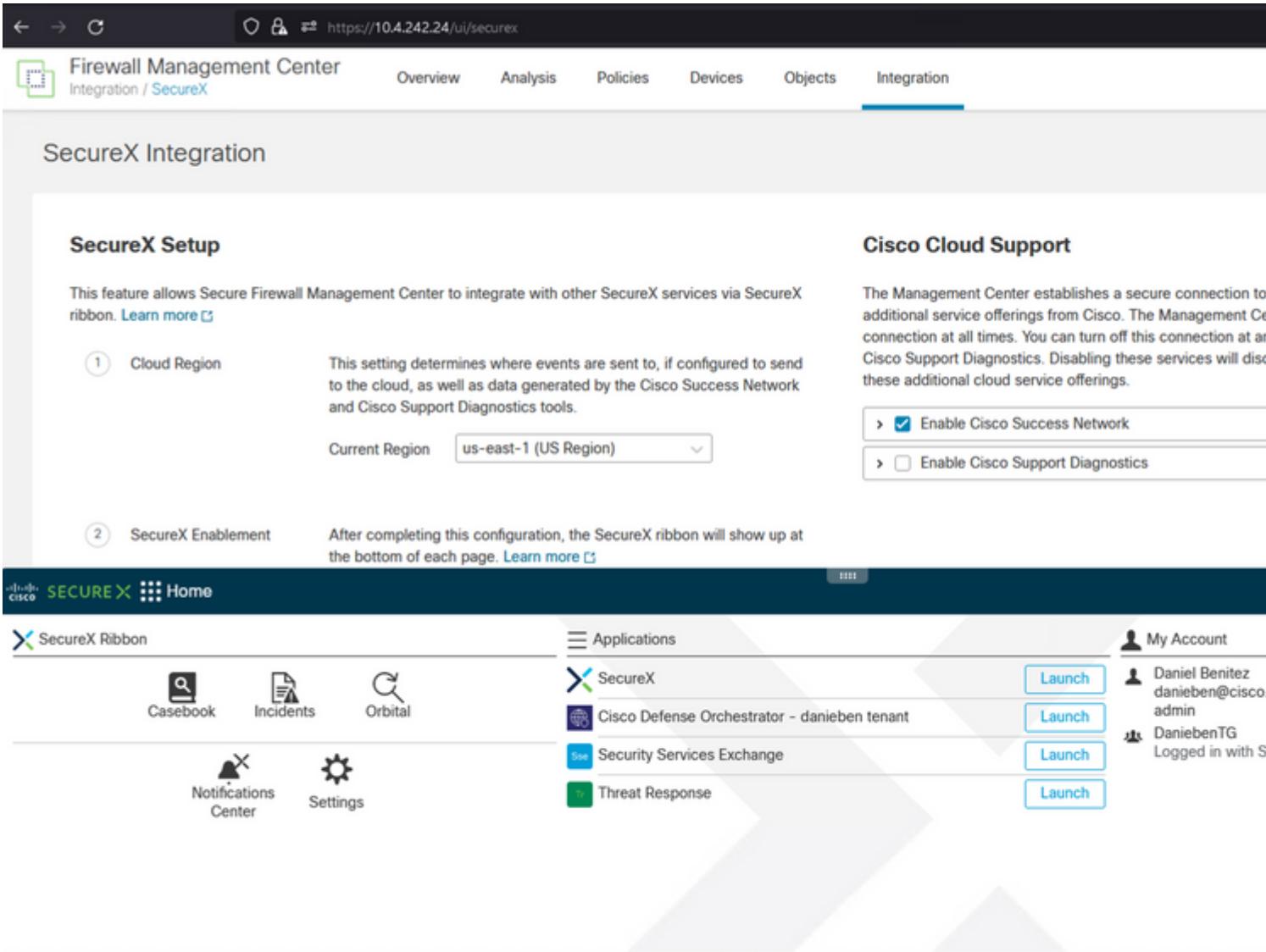


Schritt 4: Nachdem die Cisco XDR-Organisation ausgewählt wurde, werden Sie erneut an das FMC weitergeleitet, und es muss eine Meldung angezeigt werden, dass die Integration erfolgreich war:

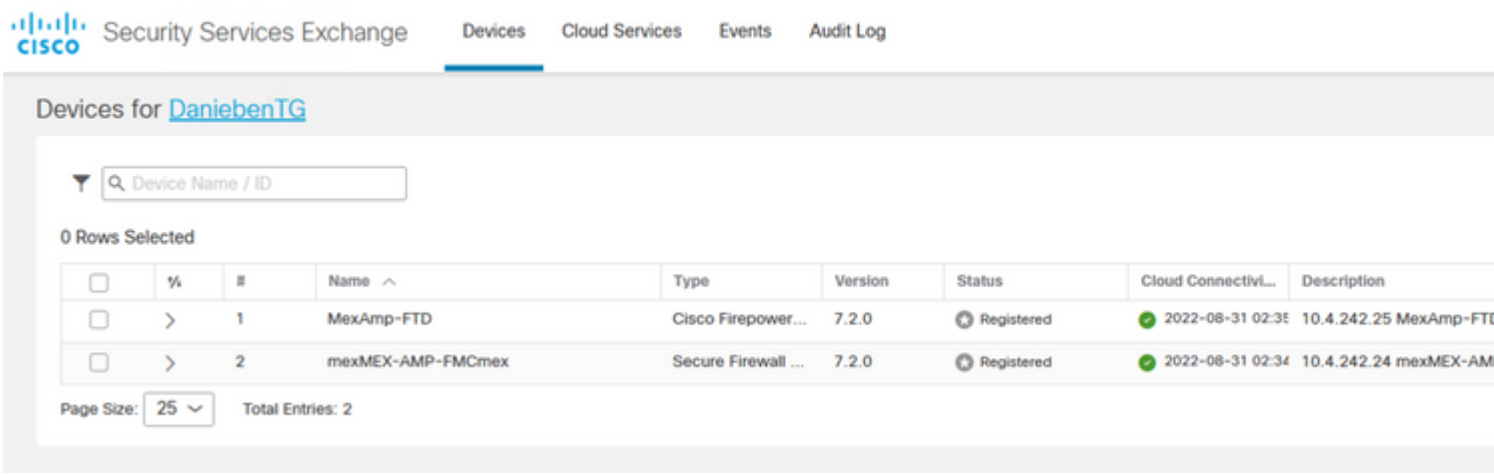


Überprüfung

Nach Abschluss der Integration können Sie die **Multifunktionsleiste** unten auf der Seite erweitern:



Starten Sie auf dem **Menüband Security Services Exchange**, und sehen Sie unter **Devices** (Geräte) sowohl das FMC als auch die Secure Firewall, die Sie gerade integriert haben:



Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.