Cisco XDR configureren en problemen oplossen met Secure Firewall release 7.2

Inhoud

Inleiding

Dit document beschrijft hoe u Cisco XDR kunt integreren en problemen kunt oplossen met de integratie van Cisco Secure Firewall in Secure Firewall 7.2.

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- Firepower Management Center (FMC)
- Cisco Secure-firewall
- Optionele virtualisatie van afbeeldingen
- Secure Firewall en VCC moeten zijn gelicentieerd

Gebruikte componenten

- Cisco Secure-firewall - 7.2
- Firepower Management Center (FMC) - 7.2
- Security Services exchange (SSE)
- Cisco XDR router
- Smart License Portal
- Cisco Threat Response (CTR)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrond

Release 7.2 omvat wijzigingen in de manier waarop Secure Firewall in Cisco XDR en Cisco XDR Orchestration wordt geïntegreerd:

Feature	Beschrijving
Verbeterde Cisco XDR integratie, Cisco XDR orkestratie.	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.

Raadpleeg 7.2 volledige **Releaseopmerkingen** om alle functies in deze release te controleren.

Configureren

Zorg ervoor dat deze URLâ€™s zijn toegestaan op uw omgeving, voordat u de integratie start:

Amerikaanse regio

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

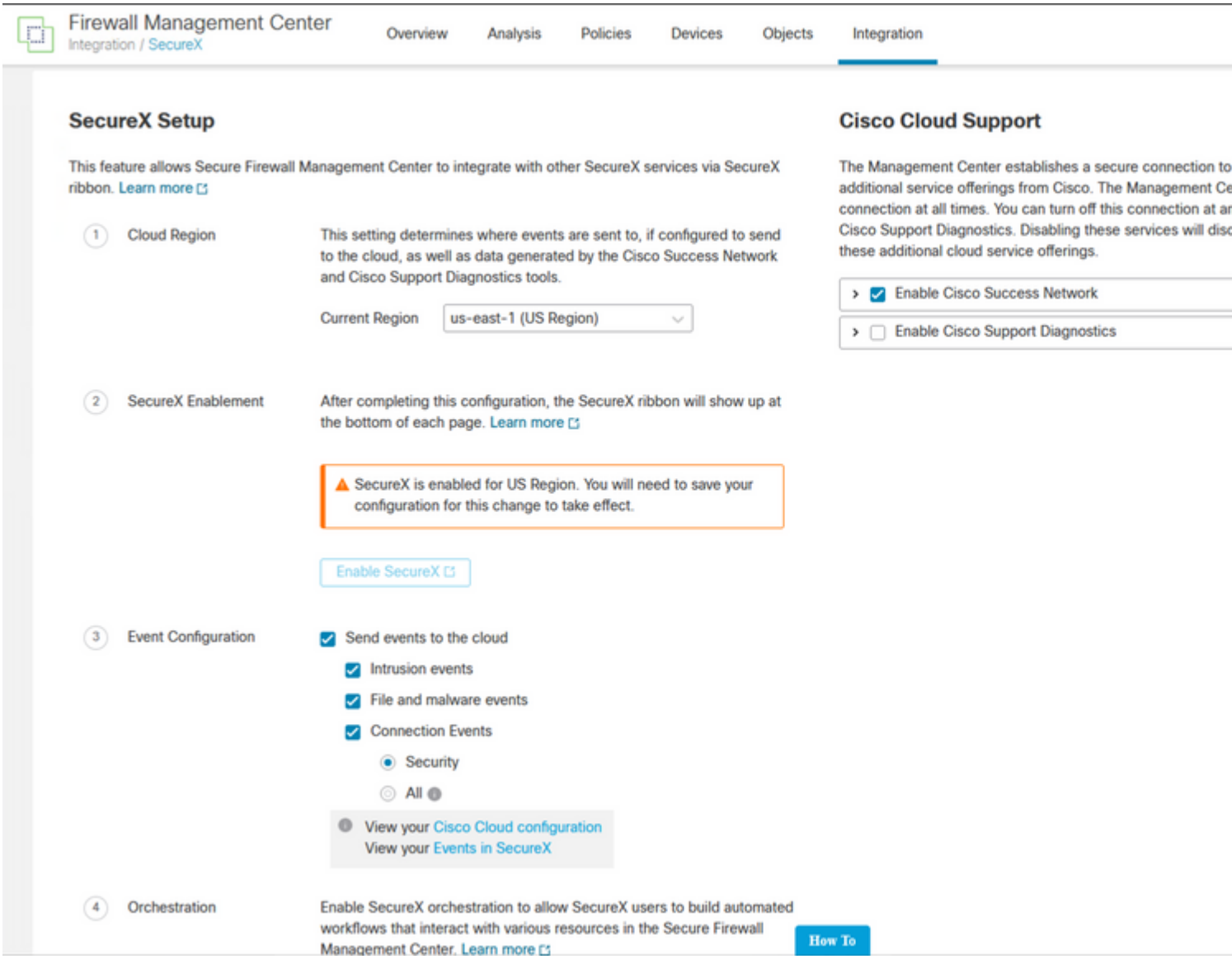
EU-regio

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

APJ-regio

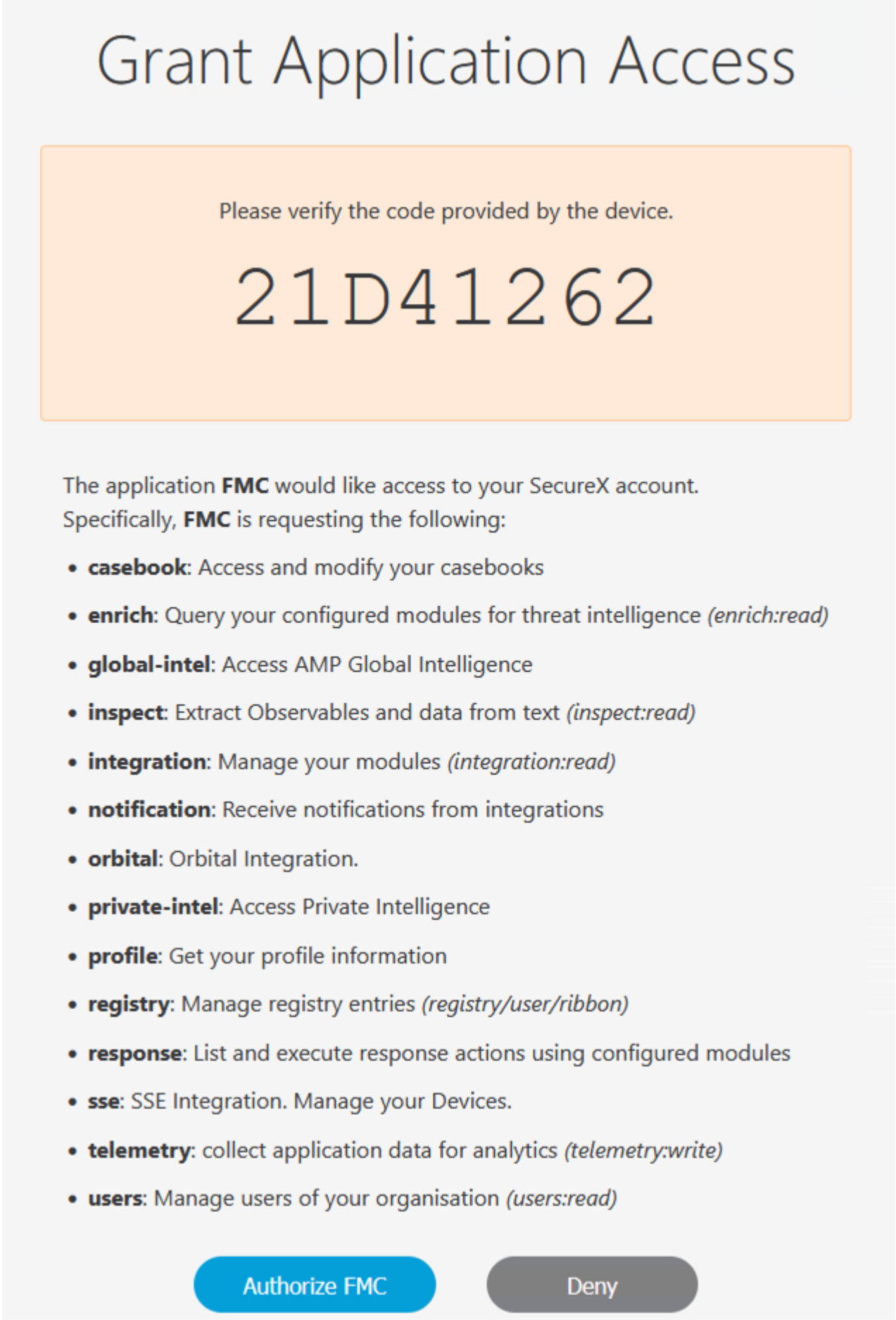
- api.apj.sse.itd.cisco.com
- eventing-ingest.apj.sse.itd.cisco.com

Stap 1. Het integratielogboek in het VCC starten. Ga naar **Integratie>Cisco XDR,** selecteer de regio waar u verbinding wilt maken (VS, EU of APJC), selecteer het type gebeurtenissen dat u wilt doorsturen naar Cisco XDR en selecteer vervolgens **Cisco XDR inschakelen:**

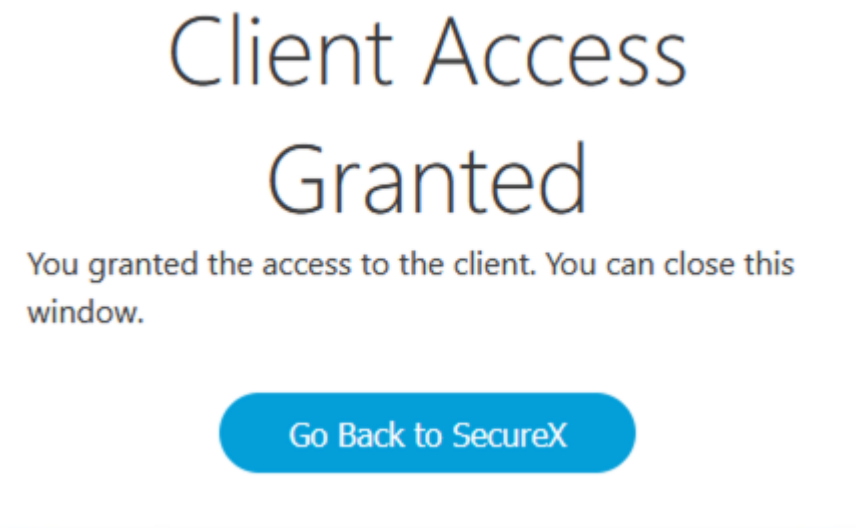


Bericht dat de veranderingen niet worden toegepast, tot uitgezocht u Save .

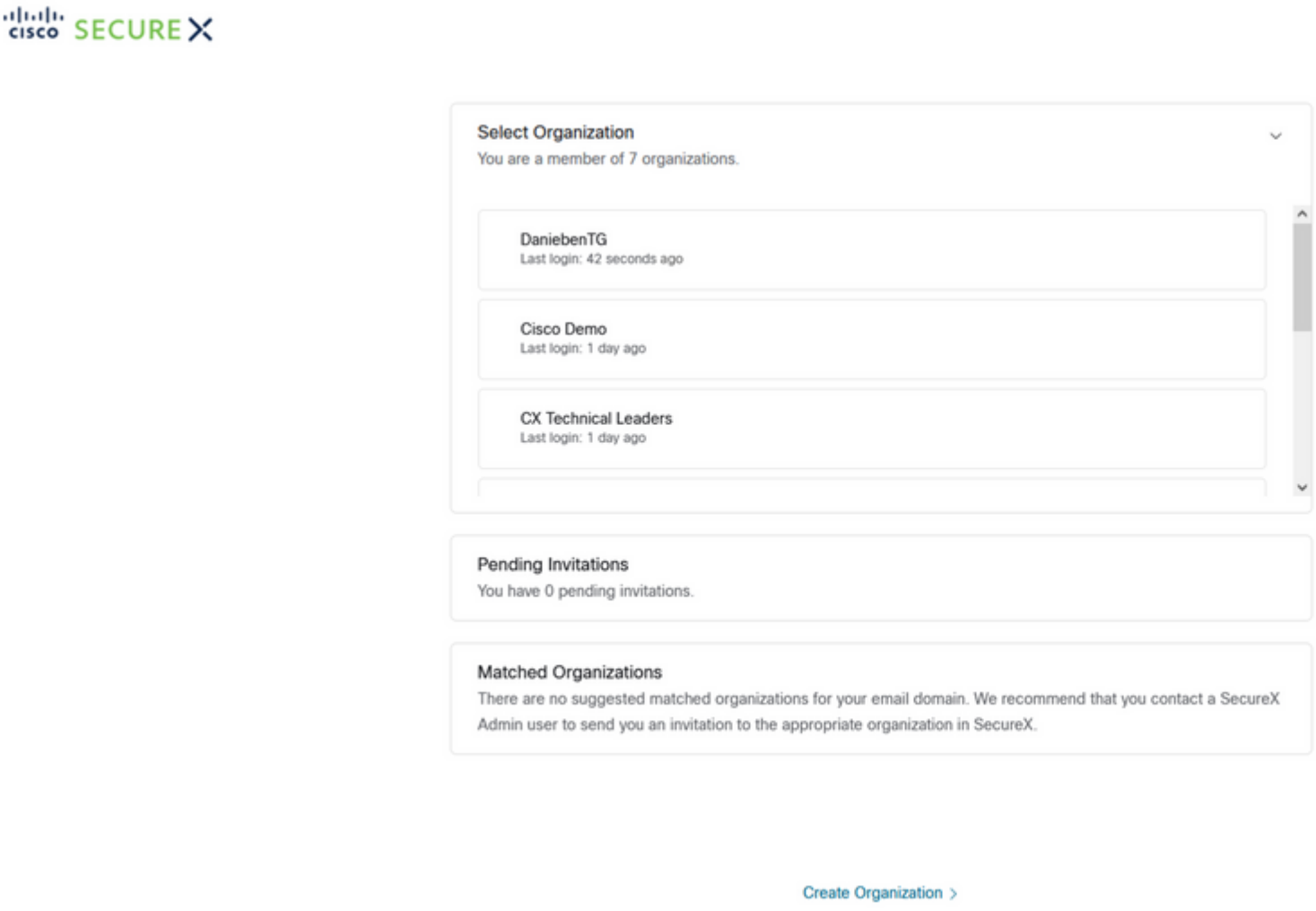
Stap 2. Nadat Save is geselecteerd, wordt u doorgestuurd naar de geautoriseerde locatie van uw VCC in uw Cisco XDR-account (u moet vóór deze stap inloggen op de Cisco XDR-account). Selecteer **FMC autoriseren**:



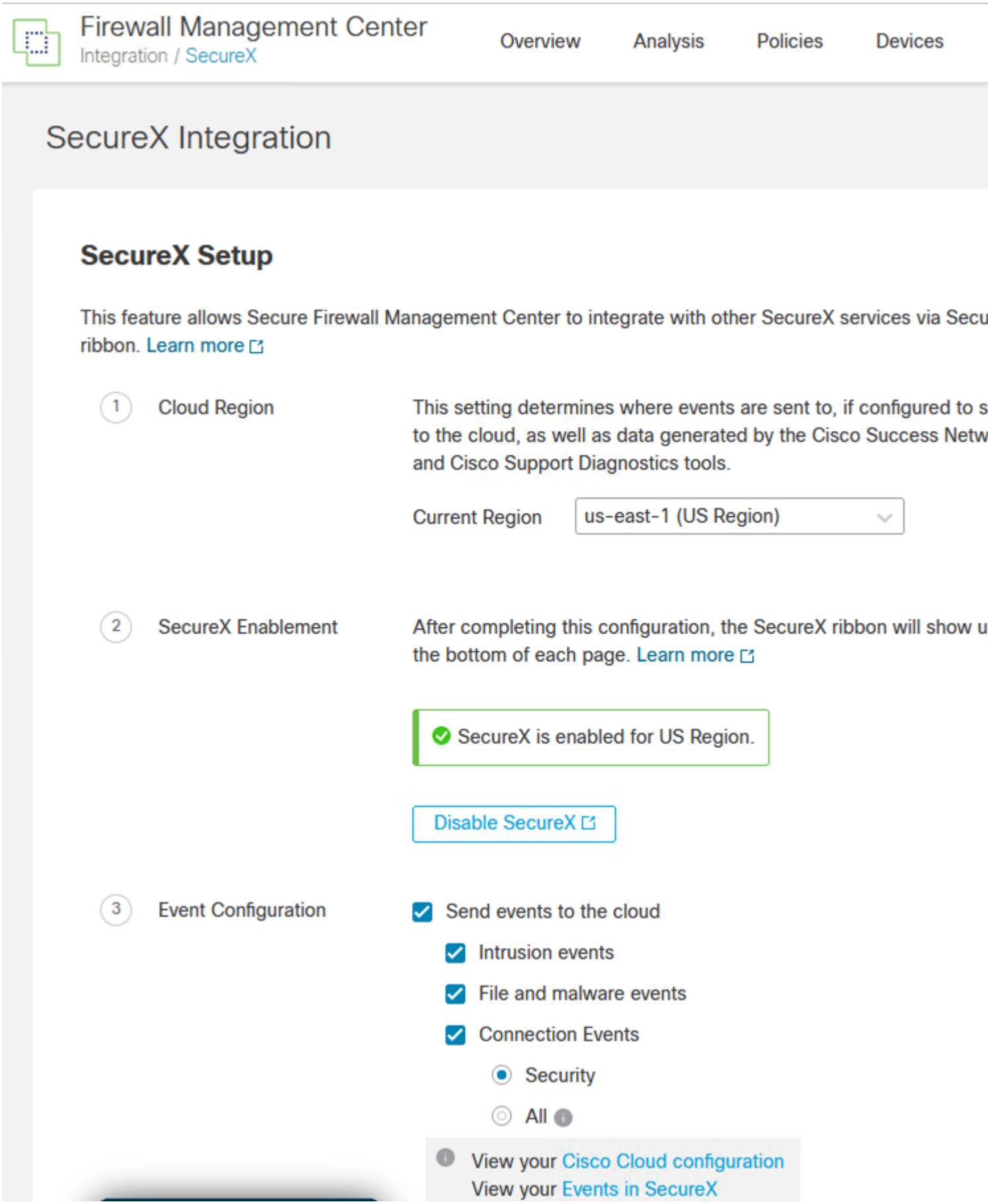
Stap 3. Nadat de autorisatie is verleend, wordt u doorgestuurd naar Cisco XDR:



Als u meerdere Orgs hebt, krijgt u de landingspagina van Cisco XDR om de organisatie te selecteren waar u uw FMC en Secure Firewall-apparaten wilt integreren:

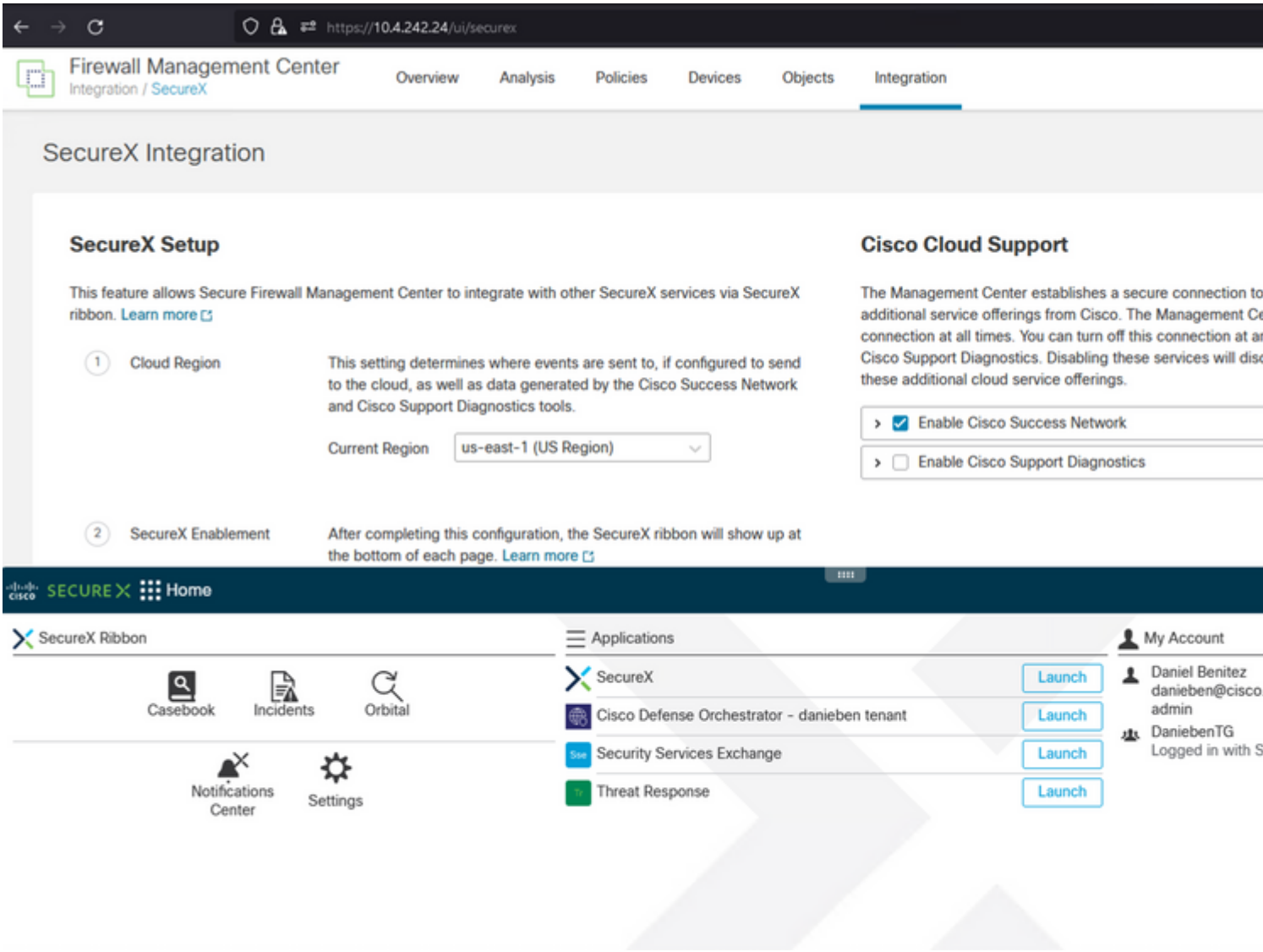


Stap 4. Nadat de Cisco XDR-organisatie is geselecteerd, wordt u opnieuw doorgestuurd naar het VCC en krijgt u het bericht dat aangeeft dat de integratie is geslaagd:

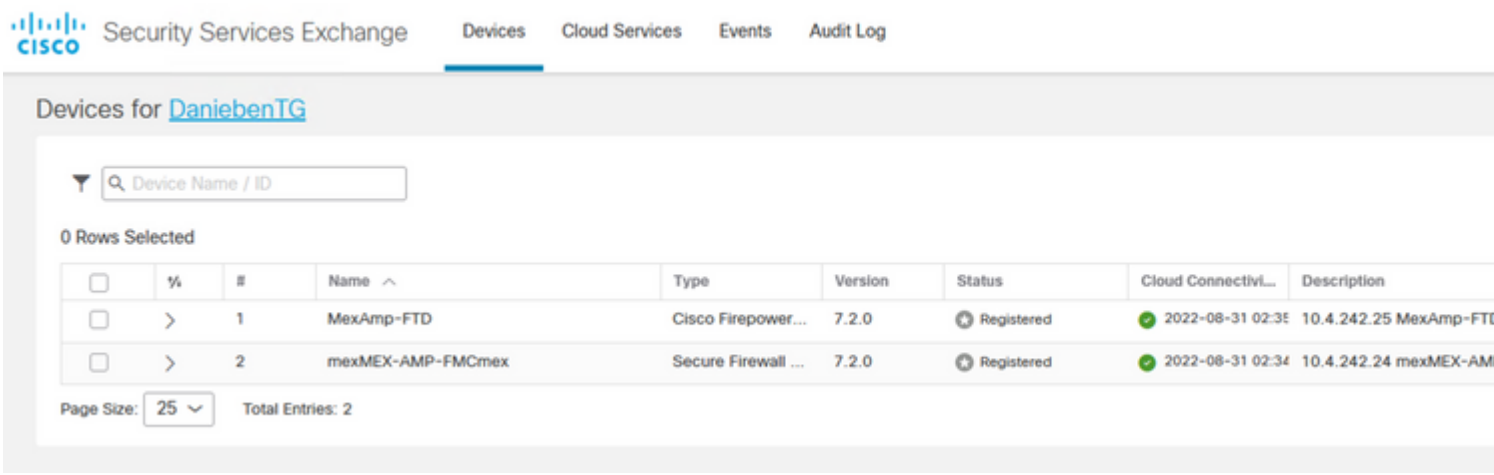

Firewall Management Center
Integration / SecureX
Overview
Analysis
Policies
Devices
SecureX Integration
SecureX Setup
This feature allows Secure Firewall Management Center to integrate with other SecureX services via Secu
ribbon. Learn more
1
Cloud Region
This setting determines where events are sent 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

Verifiëren

Zodra de integratie is voltooid, kunt u het **lint** uitvouwen onder aan de pagina:



Op het **lint**, lanceer **Security Services Exchange** en onder **Apparaten** moet u zowel de FMC en Secure Firewall zien die u zojuist hebt geïntegreerd:



Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.