Configurar e solucionar problemas do Cisco XDR com o Secure Firewall versão 7.2

Contents

Introdução

Este documento descreve como integrar e solucionar problemas do Cisco XDR com a integração do Cisco Secure Firewall no Secure Firewall 7.2.

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Firepower Management Center (FMC)
- Firewall seguro da Cisco
- Virtualização opcional de imagens
- O firewall e o FMC seguros devem ser licenciados

Componentes Utilizados

- Cisco Secure Firewall - 7.2
- Firepower Management Center (FMC) - 7.2
- Troca de serviços de segurança (SSE)
- Cisco XDR
- Portal Smart License
- Cisco Threat Response (CTR)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Background

A versão 7.2 inclui alterações na forma como o Secure Firewall se integra com a Orquestração Cisco XDR e Cisco XDR:

Recurso	Descrição
Integração aprimorada com o Cisco XDR e orquestração do 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.

Consulte as **Notas de versão** completas da versão 7.2 para verificar todos os recursos incluídos nesta versão.

Configurar

Antes de iniciar a integração, verifique se estes URLs são permitidos em seu ambiente:

Região dos EUA

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

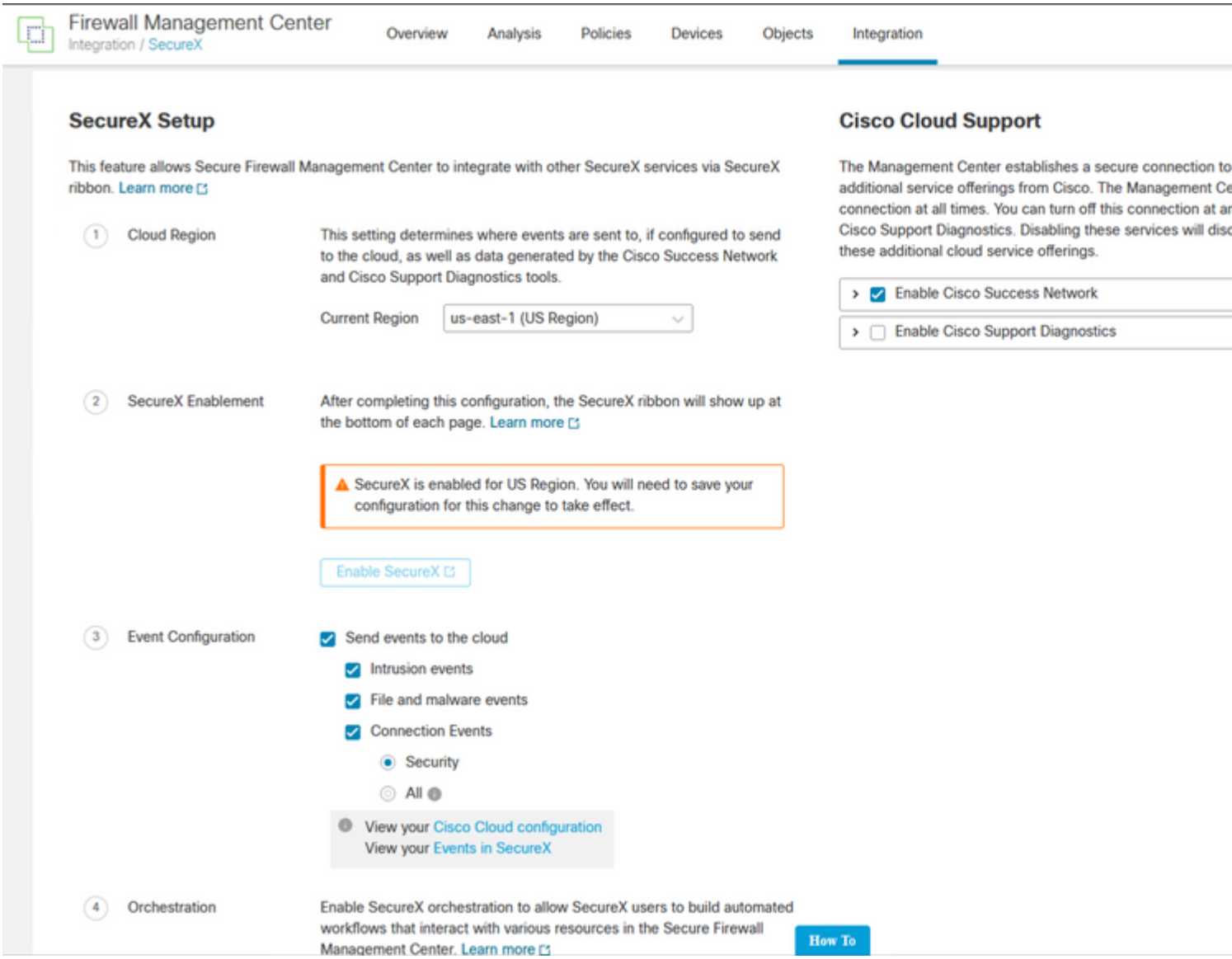
Região da UE

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

Região APJ

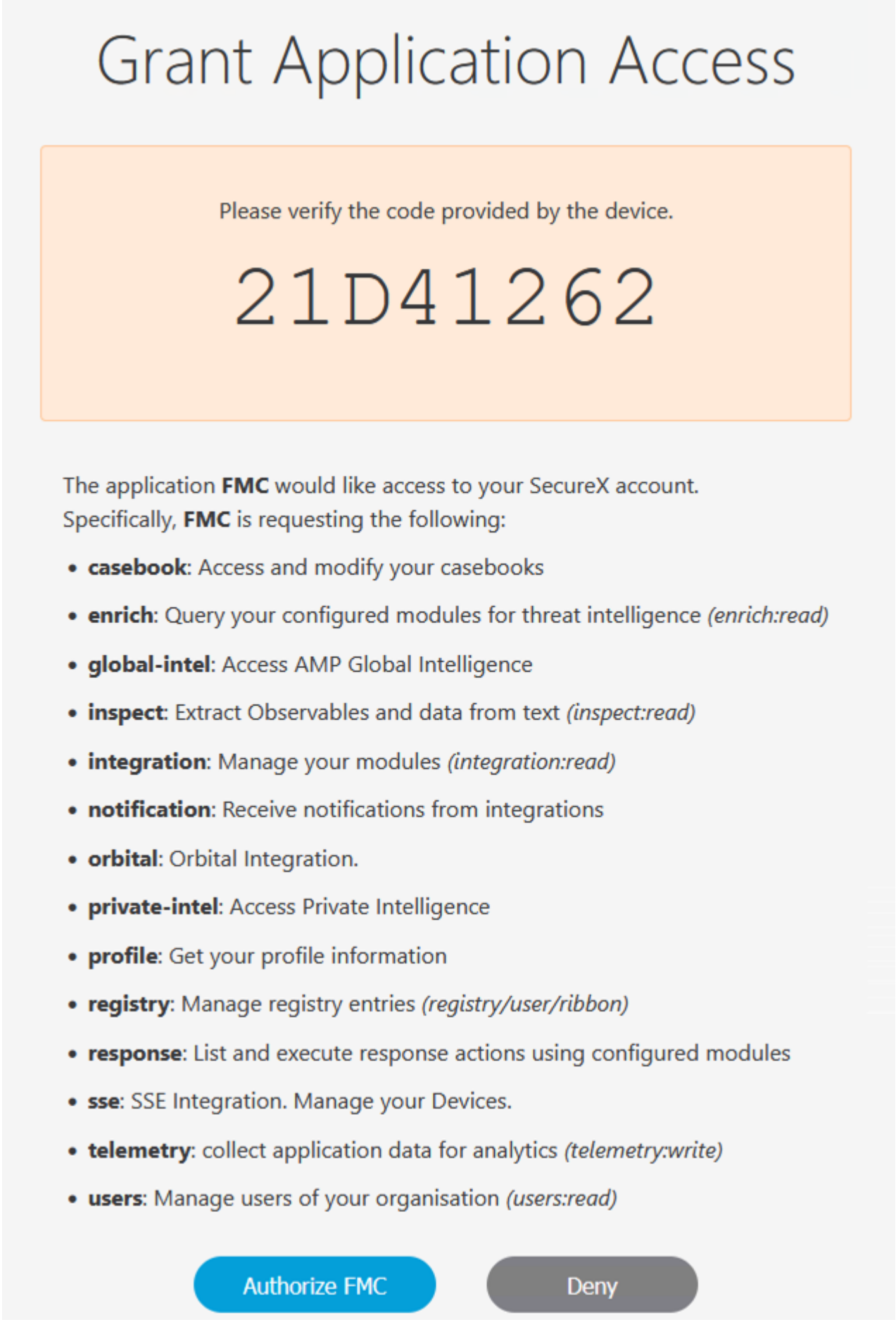
- api.apj.sse.itd.cisco.com
- eventing-ingest.apj.sse.itd.cisco.com

Etapa 1. Para iniciar o registro de integração no FMC. Vá para **Integration>Cisco XDR,** selecione a região onde deseja se conectar (US, EU ou APJC), selecione o tipo de evento que deseja encaminhar para o Cisco XDR e, em seguida, selecione **Enable Cisco XDR:**

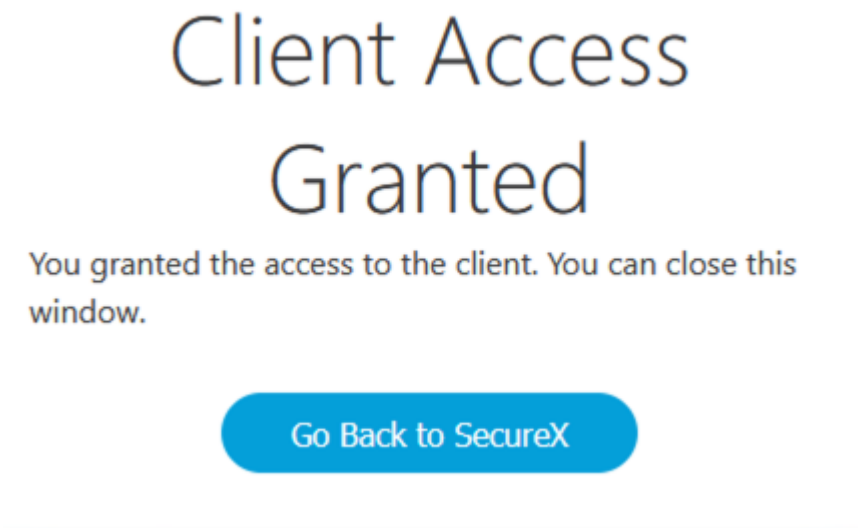


Observe que as alterações não são aplicadas, até que você selecione Save .

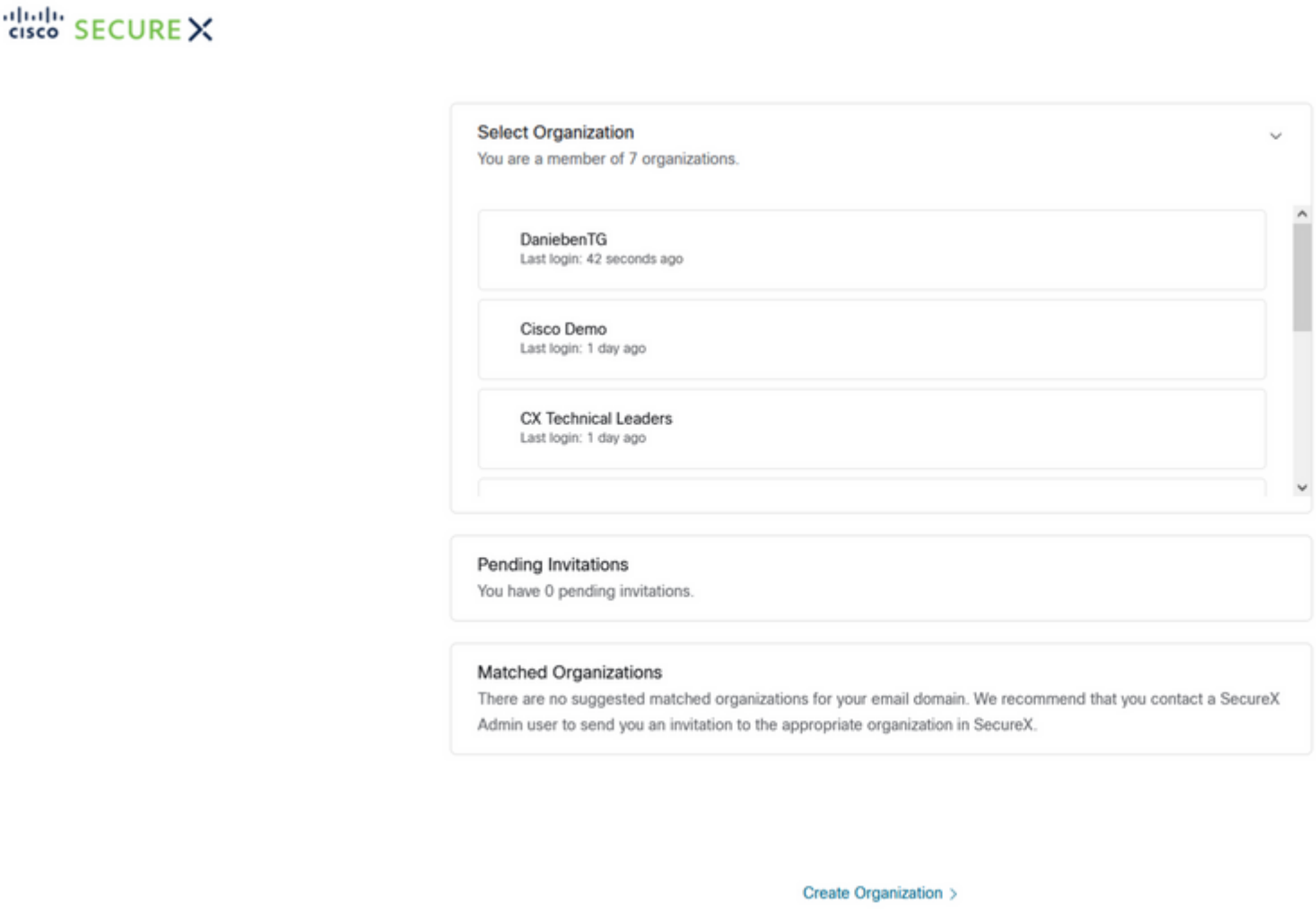
Etapa 2. Depois de selecionar Save (Salvar), você será redirecionado para o FMC autorizado em sua conta Cisco XDR (você precisa fazer login na conta Cisco XDR antes desta etapa), selecione Authorize FMC:



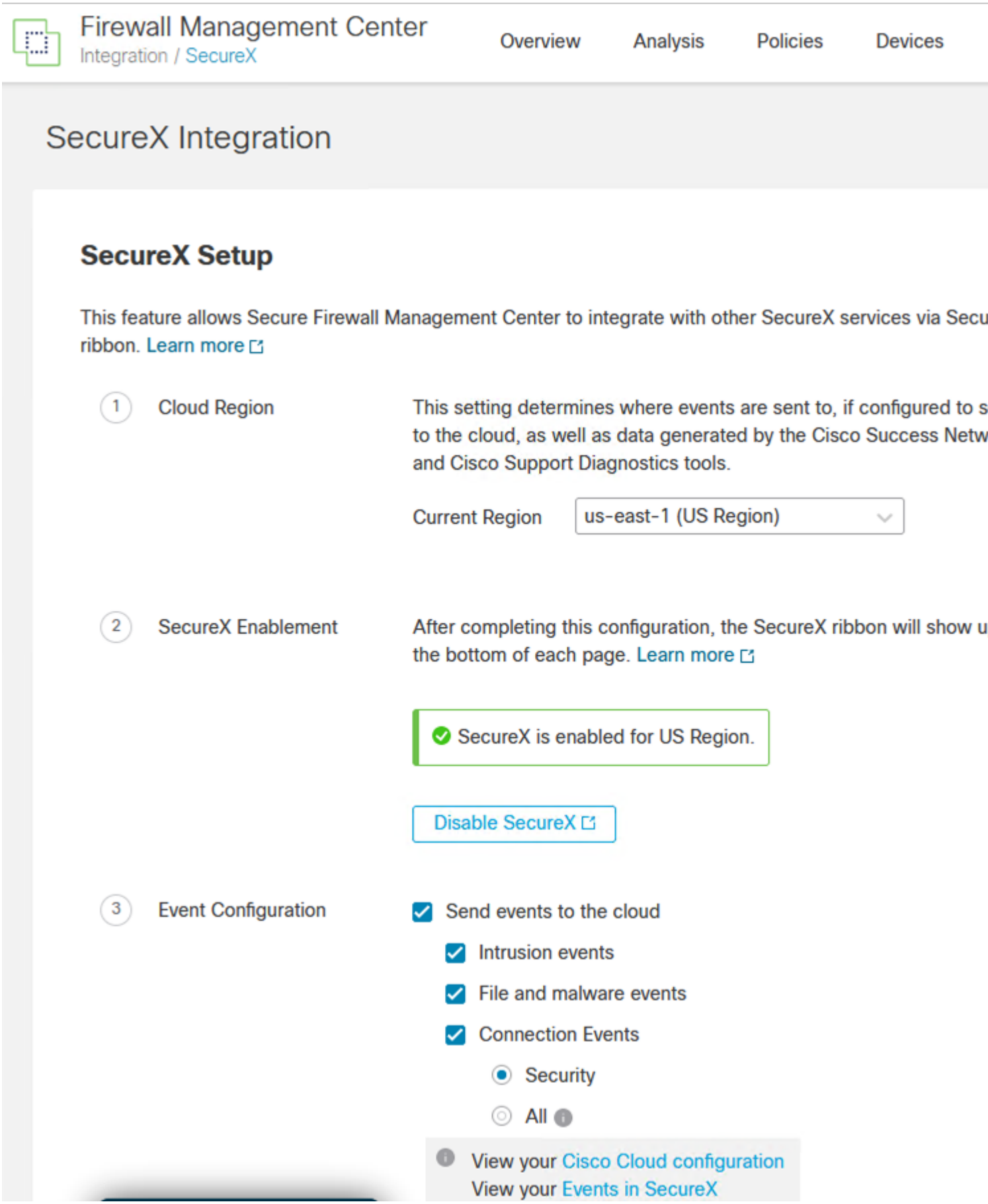
Etapa 3. Quando a autorização for concedida, você será redirecionado para o Cisco XDR:



Caso você tenha várias organizações, será exibida a página inicial do Cisco XDR para selecionar a organização em que deseja integrar seus dispositivos FMC e de firewall seguro:

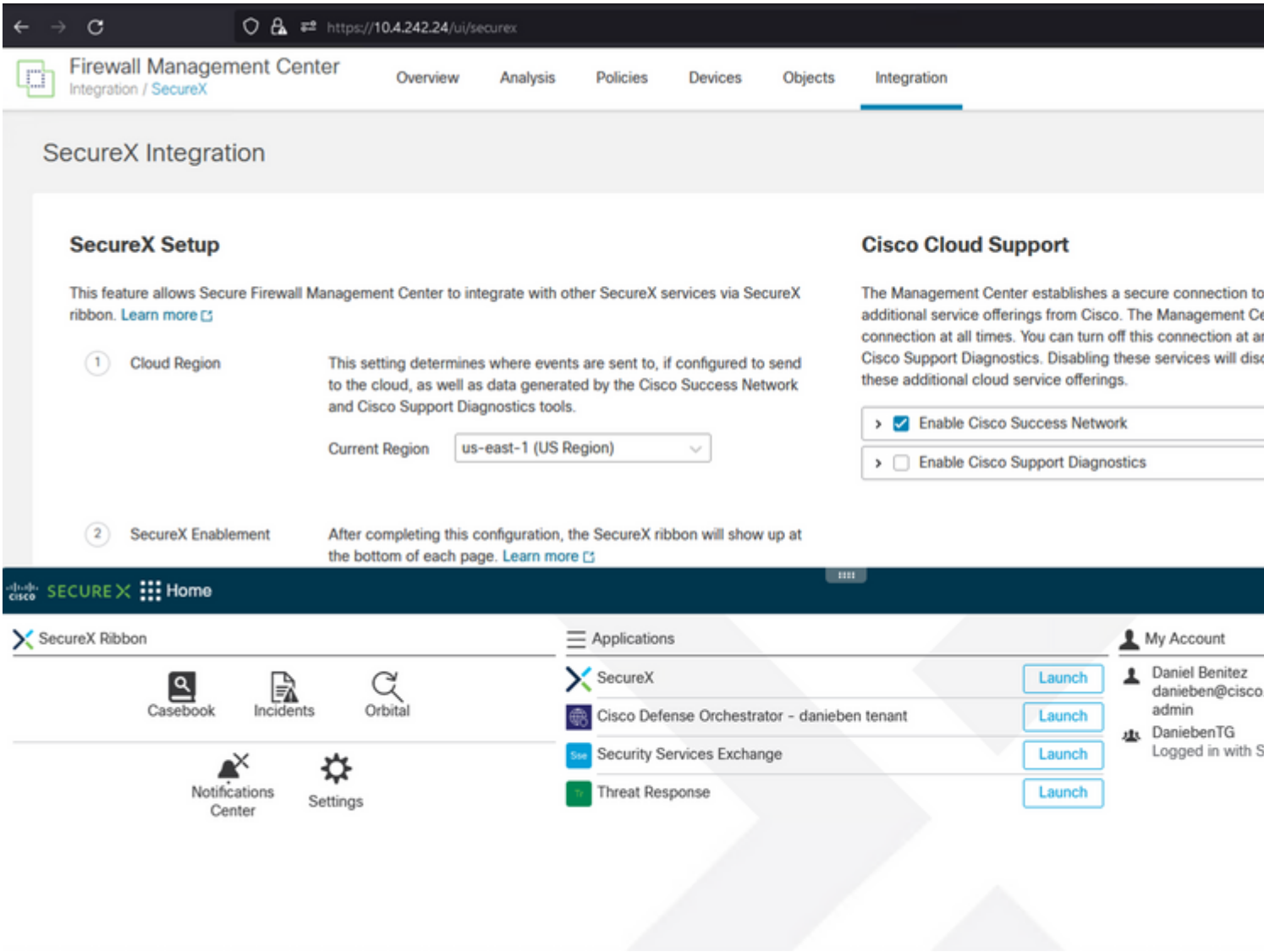


Etapa 4. Depois que a organização Cisco XDR for selecionada, você será redirecionado, mais uma vez, para o FMC e receberá a mensagem que mostra que a integração foi bem-sucedida:

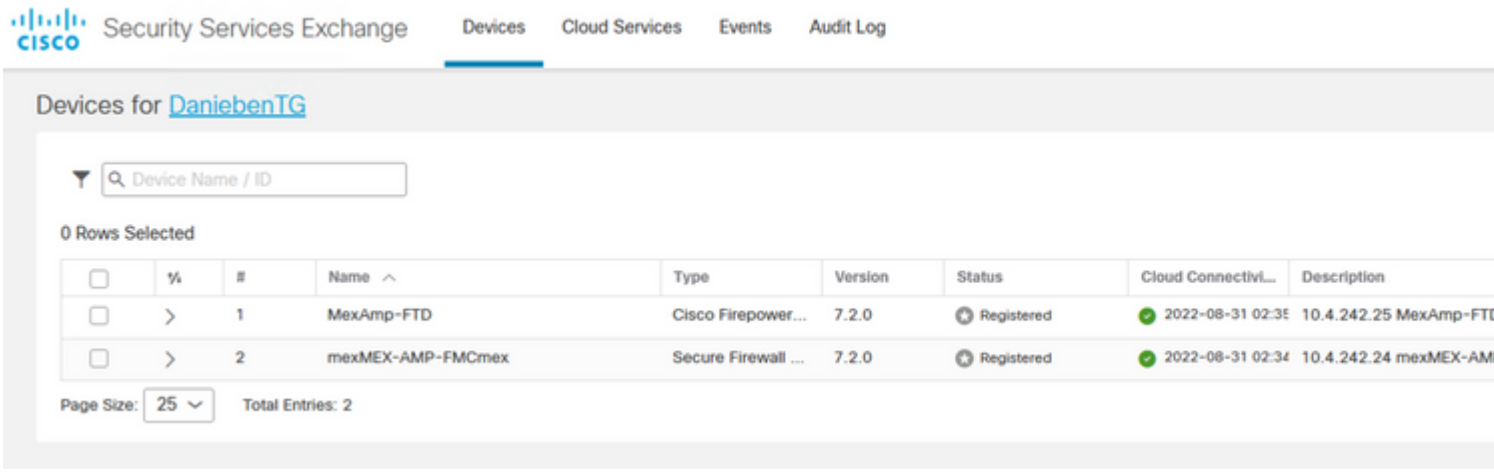

Firewall Management Center
Integration / SecureX
Overview
Analysis
Policies
Devices
SecureX Integration
SecureX Setup
This feature allows Secure Firewall Management Center to integrate with other SecureX services via Secu
ribbon. Learn more
1
Cloud Region
This setting determines where events are sent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

Verificar

Depois que a integração estiver concluída, você poderá expandir a **Faixa de Opções** na parte inferior da página:



Na **Faixa de opções**, inicie o **Security Services Exchange** e, em **Devices**, você deverá ver o FMC e o Firewall Seguro que acabou de integrar:



Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.