Configure and Troubleshoot Cisco XDR with Secure Firewall Release 7.2

Contents

Introduction
Prerequisites
Requirements
Components Used
Background
Configure
Verify

Introduction

This document describes how to integrate and troubleshoot Cisco XDR with Cisco Secure Firewall integration on Secure Firewall 7.2.

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Firepower Management Center (FMC)
- Cisco Secure Firewall
- Optional Virtualization of images
- Secure Firewall and FMC must be licensed

Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background

Release 7.2 includes changes on the way that Secure Firewall integrates with Cisco XDR and Cisco XDR Orchestration:

Feature	**Description**
Improved Cisco XDR integration, Cisco XDR orchestration.	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.

Consult 7.2 complete **Release Notes** to check all the features included within this release.

Configure

Prior to start the integration, ensure these URLs are allowed on your environment:

US Region

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

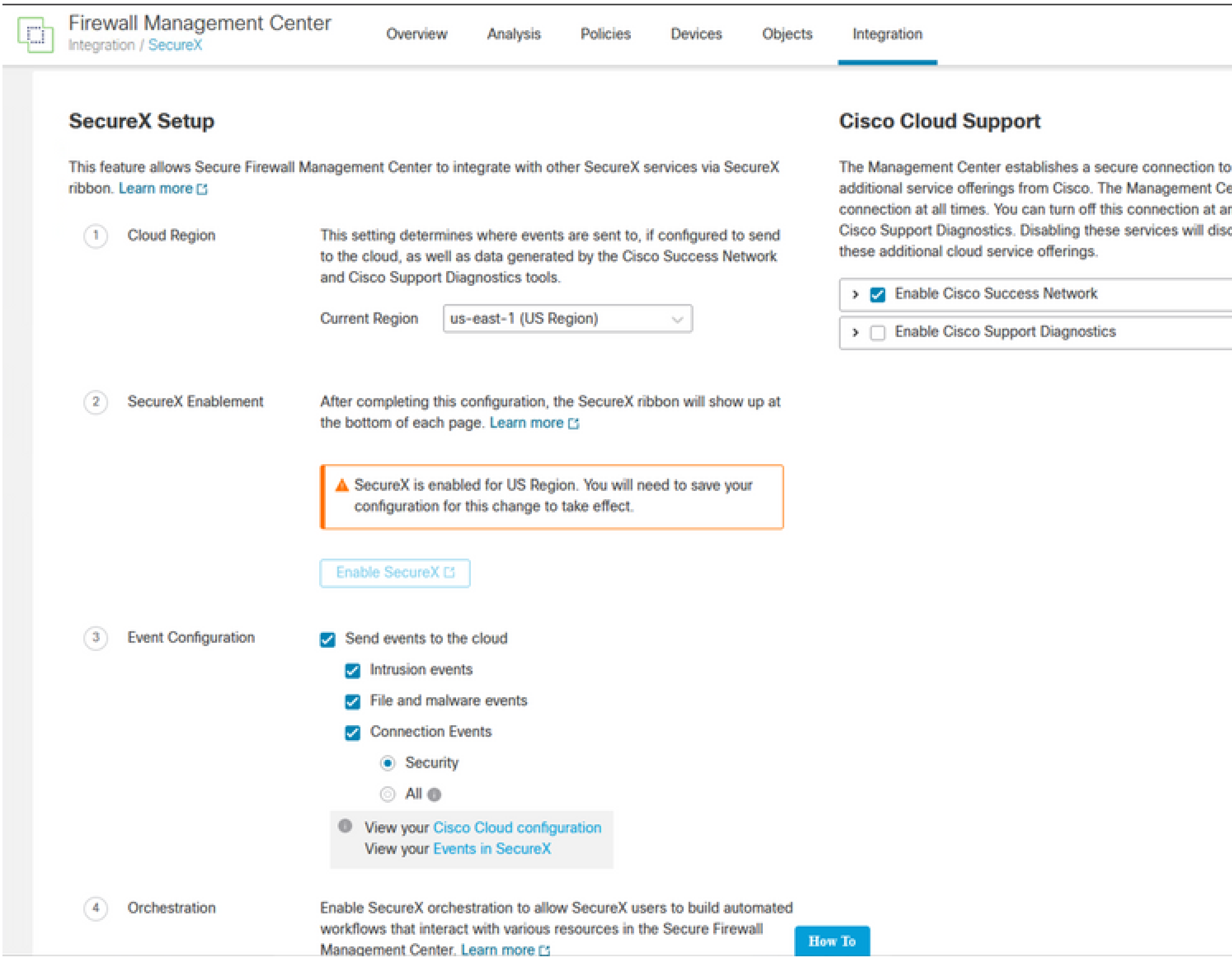
EU Region

- 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

Step 1. To start the integration log into the FMC. Go to **Integration>Cisco XDR,** select the region where you want to connect (US, EU or APJC), select the type of events you want to forward to Cisco XDR, and then select **Enable Cisco XDR:**



Firewall Management Center

Integration / SecureX

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: us-east-1 (US 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.

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

Cisco Cloud Support

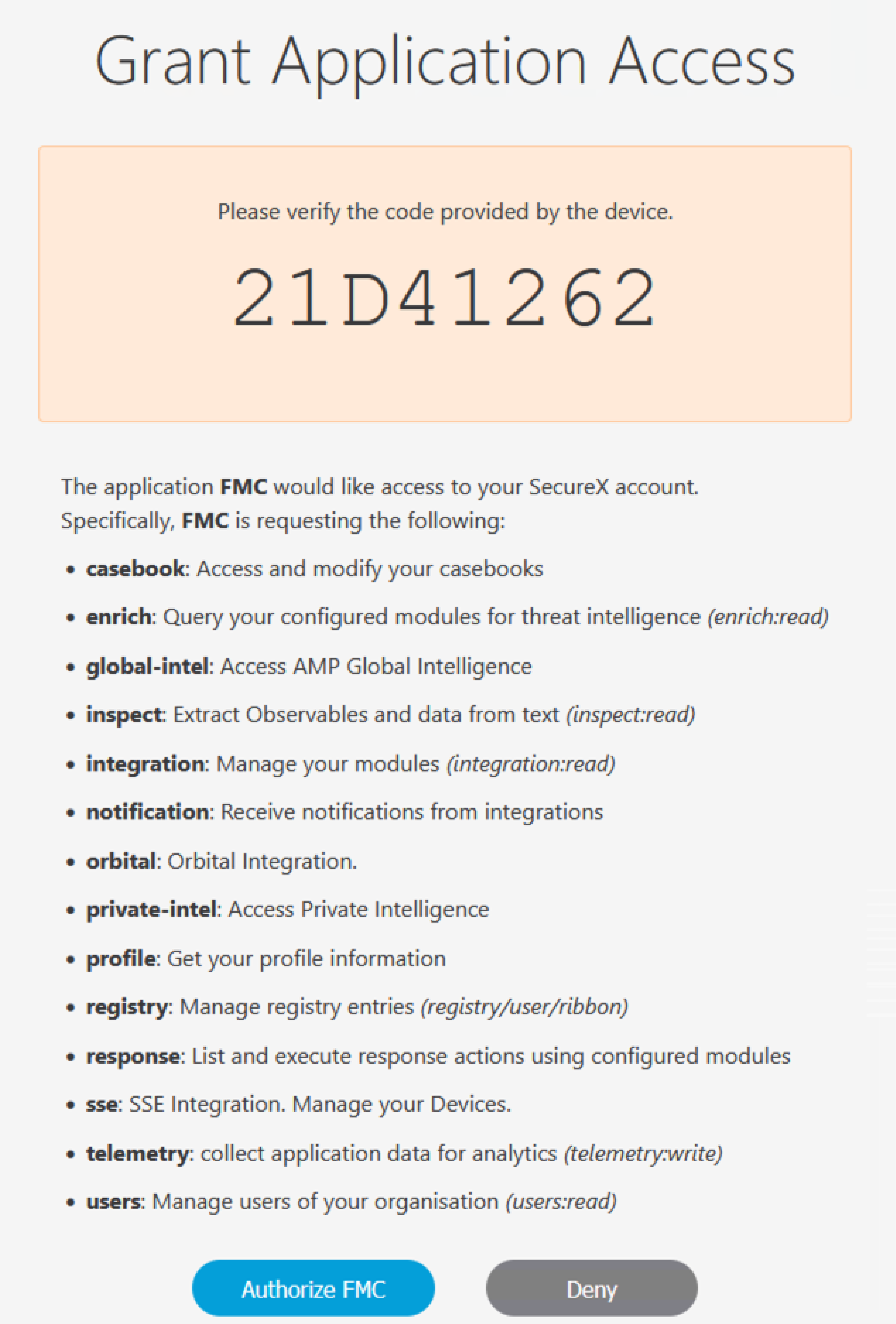
The Management Center establishes a secure connection to additional service offerings from Cisco. The Management Ce connection at all times. You can turn off this connection at ar Cisco Support Diagnostics. Disabling these services will disc these additional cloud service offerings.

☑ Enable Cisco Success Network

□ Enable Cisco Support Diagnostics

Notice that the changes are not applied, until you select Save .

Step 2. Once Save was selected, you are redirected to authorized your FMC in your Cisco XDR account (you need to login to the Cisco XDR account prior to this step), select **Authorize FMC**:



Grant Application Access

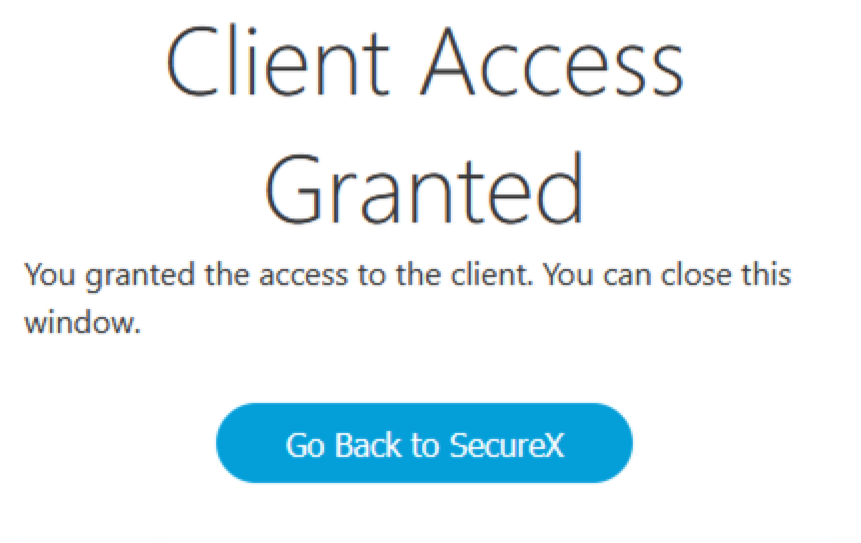
Please verify the code provided by the device.

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)*

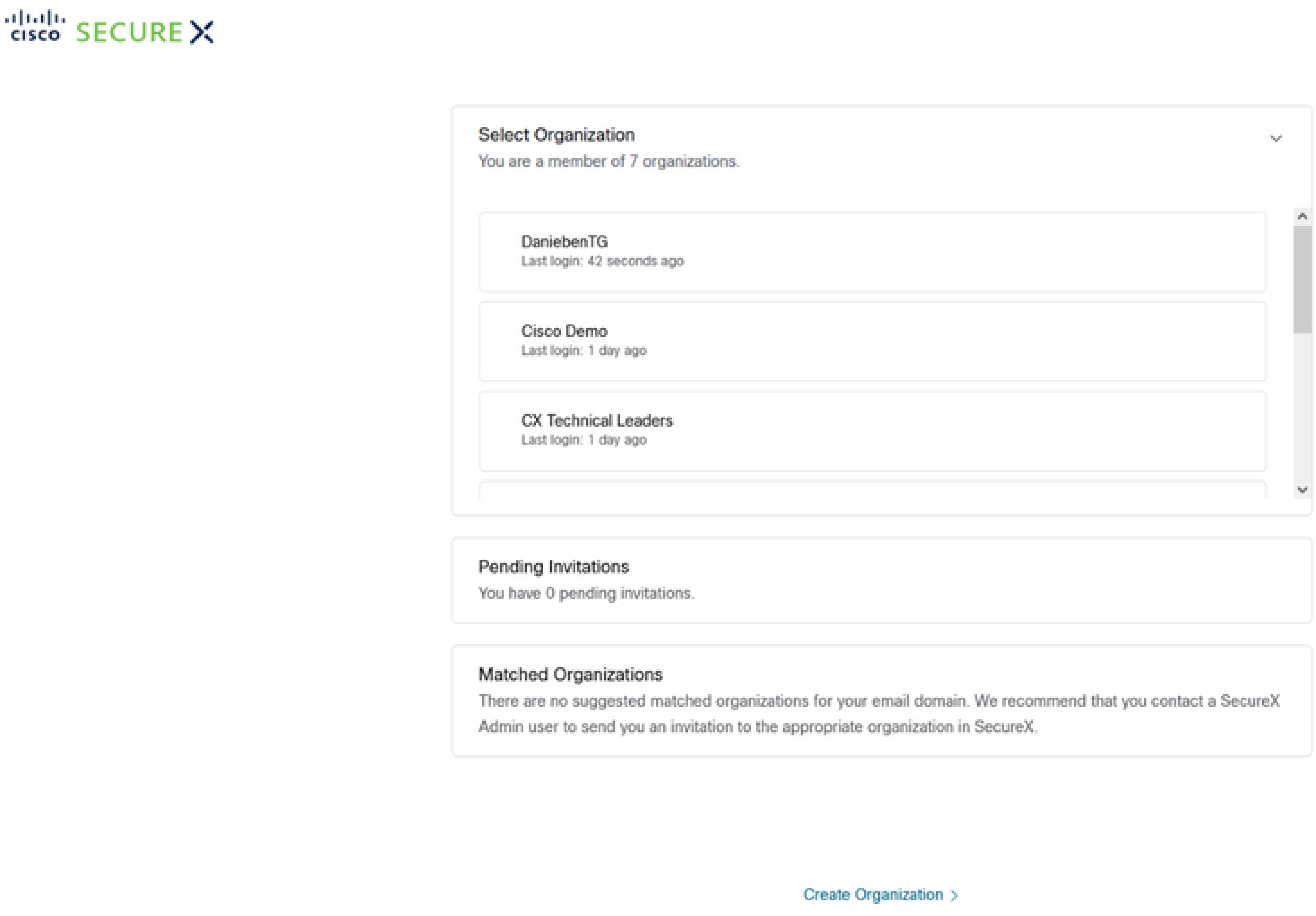
Step 3. Once the authorization is granted, you are redirected to Cisco XDR:



Client Access Granted

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

In case you have multiple Orgs, you are presented with the Cisco XDR landing page to select the Organization where you want to integrate your FMC and Secure Firewall devices:



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

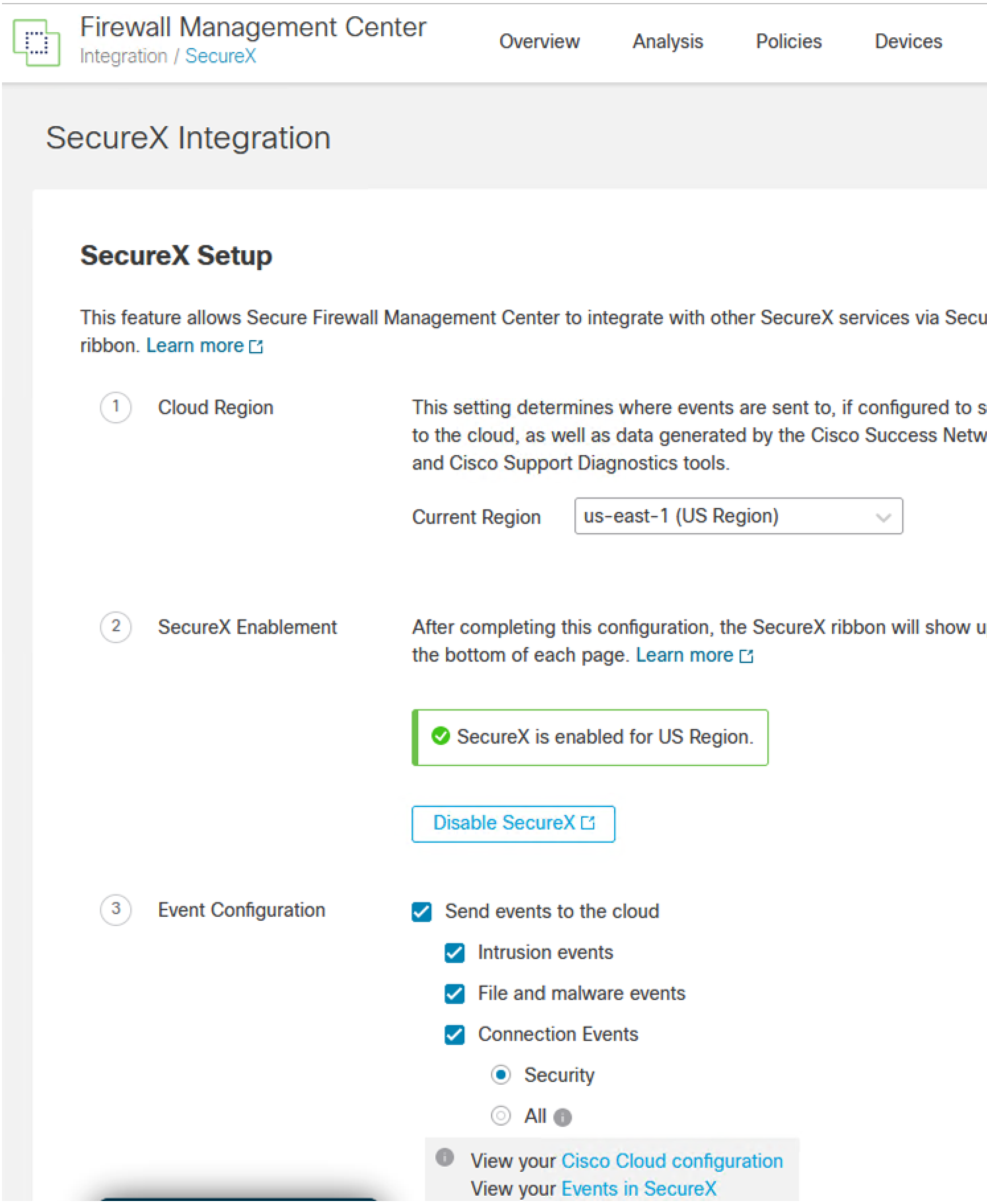
Pending Invitations

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.

Step 4. After the Cisco XDR Organization was selected, you are redirected, once again to the FMC and you must get the message that shows the integration was successful:



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.

3 Event Configuration

☑ Send events to the cloud

☑ Intrusion events

☑ File and malware events

☑ Connection Events

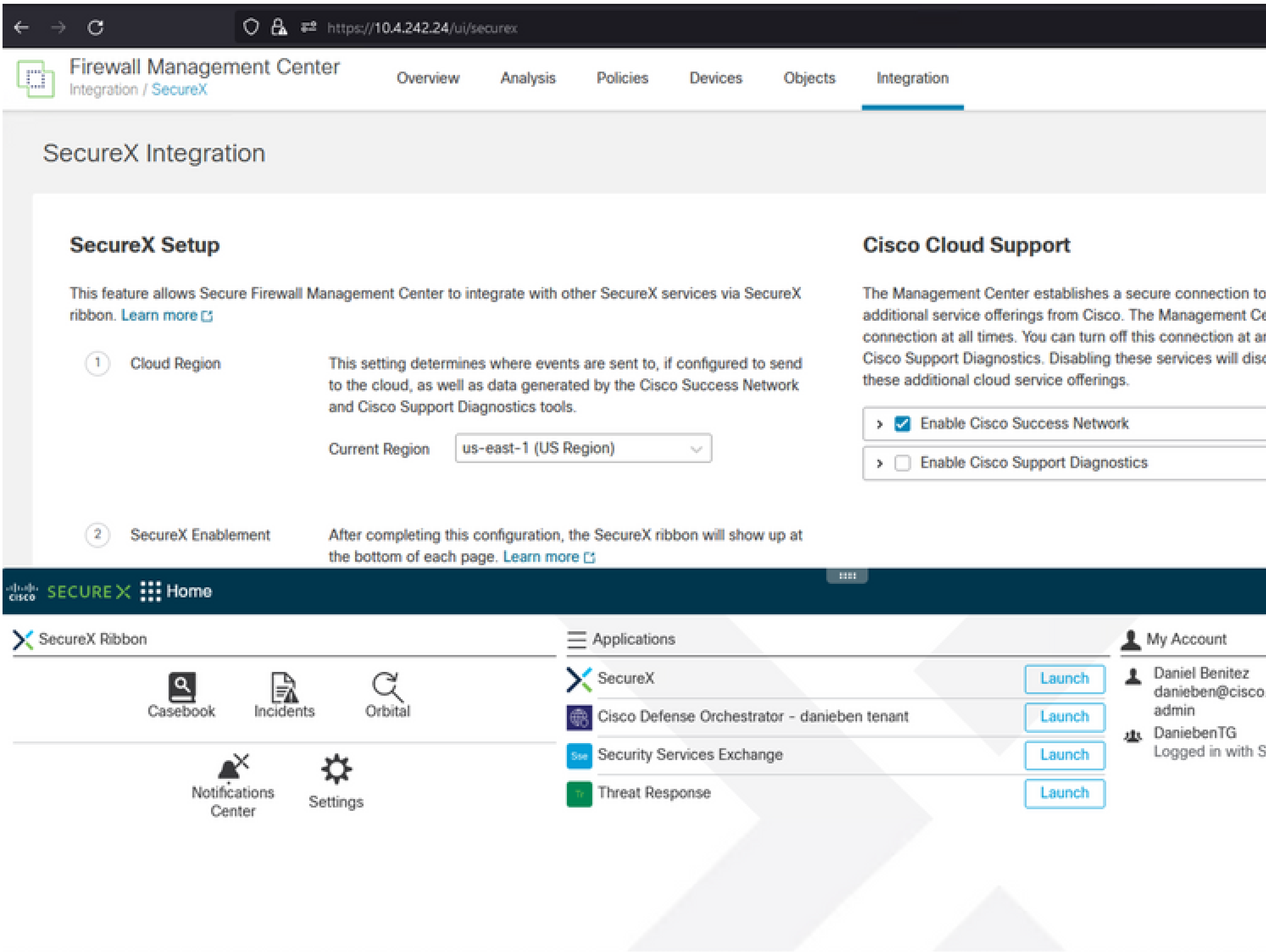
● Security

○ All

View your Cisco Cloud configuration
View your Events in SecureX

Verify

Once the integration is done, you can expand the **Ribbon** from the bottom of the page:



https://10.4.242.24/ui/securex

Firewall Management Center
Integration / SecureX

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: us-east-1 (US Region)

2 SecureX Enablement

After completing this configuration, the SecureX ribbon will show up at the bottom of each page. Learn more

Cisco Cloud Support

The Management Center establishes a secure connection to
additional service offerings from Cisco. The Management Ce
connection at all times. You can turn off this connection at a
Cisco Support Diagnostics. Disabling these services will dis
these additional cloud service offerings.

☑ Enable Cisco Success Network

□ Enable Cisco Support Diagnostics

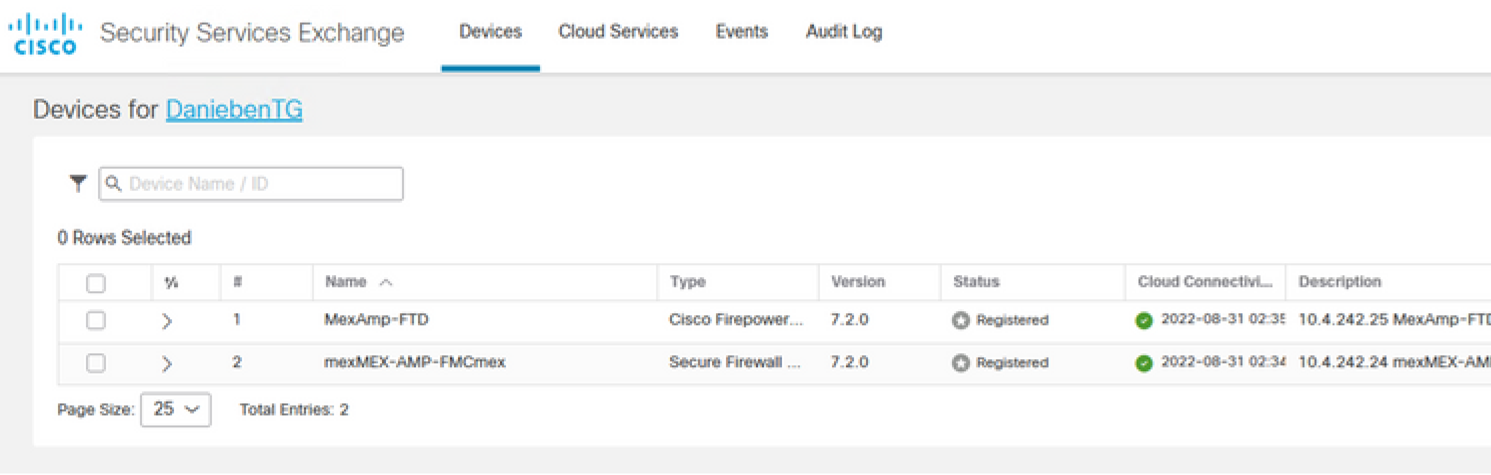
Applications	
SecureX	Launch
Cisco Defense Orchestrator - danieben tenant	Launch
Security Services Exchange	Launch
Threat Response	Launch

My Account

Daniel Benitez
danieben@cisco
admin

DaniebenTG
Logged in with S

On the **Ribbon**, launch **Security Services Exchange** and under **Devices** you must see both the FMC and Secure Firewall you just integrated:



Devices for DaniebenTG

Device Name / ID

0 Rows Selected

□	⅟	#	Name	Type	Version	Status	Cloud Connectivi...	Description
□	>	1	MexAmp-FTD	Cisco Firepower...	7.2.0	Registered	✓ 2022-08-31 02:35	10.4.242.25 MexAmp-FTI
□	>	2	mexMEX-AMP-FMCmex	Secure Firewall ...	7.2.0	Registered	✓ 2022-08-31 02:34	10.4.242.24 mexMEX-AM

Page Size: 25   Total Entries: 2