使用安全防火墙7.2版配置思科XDR并对其进行故障排除

目录

简介

本文档介绍如何将Cisco XDR与Secure Firewall 7.2上的Cisco Secure Firewall集成进行集成和故障排除。

先决条件

要求

建议掌握下列主题的相关知识：

- Firepower Management Center (FMC)
- 思科安全防火墙
- 映像的可选虚拟化
- 安全防火墙和FMC必须获得许可

使用的组件

- 思科安全防火墙 — 7.2
- Firepower管理中心(FMC)- 7.2
- 安全服务交换(SSE)
- 思科XDR
- 智能许可证门户
- 思科威胁响应(CTR)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景

版本7.2包括安全防火墙与Cisco XDR和Cisco XDR协调集成的方式更改：

功能	描述
改进了Cisco XDR集成和Cisco XDR协调。	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 orchestration—a powerful drag-and-drop interface you can use to automate workflows across security tools. After you enable SecureX, you can enable orchestration.

请参阅7.2完整发行说明以检查此版本中包含的所有功能。

配置

在开始集成之前，请确保在您的环境中允许这些URL:

美国地区

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

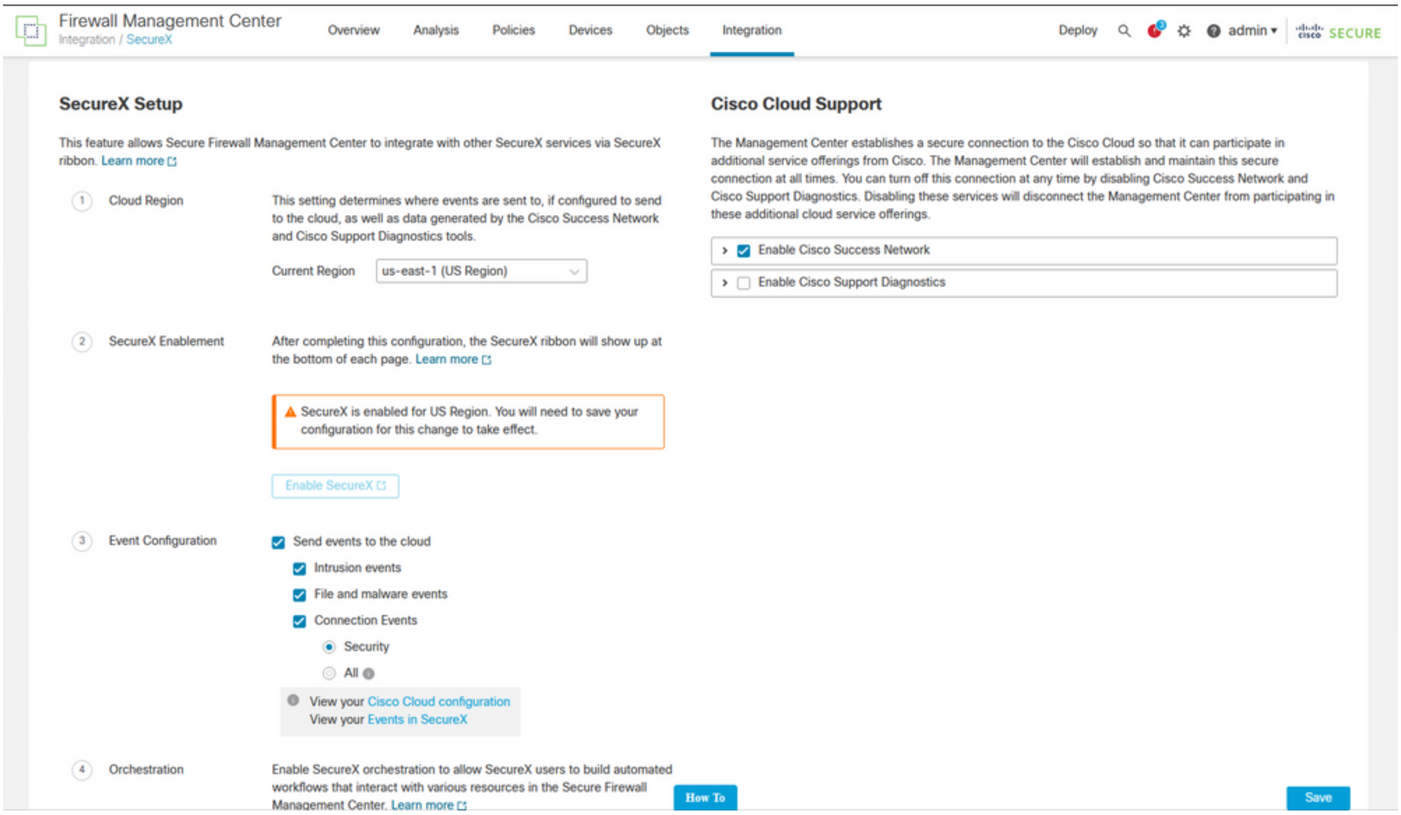
欧盟地区

- api.eu.ss e.itd.cisco.com
- eventing-ingest.eu.ss e.itd.cisco.com

APJ地区

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

步骤1.启动集成日志到FMC。转至Integration>Cisco XDR，选择要连接的区域（美国、欧盟或APJC），选择要转发到Cisco XDR的事件类型，然后选择Enable 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: 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.

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 the Cisco Cloud so that it can participate in additional service offerings from Cisco. The Management Center will establish and maintain this secure connection at all times. You can turn off this connection at any time by disabling Cisco Success Network and Cisco Support Diagnostics. Disabling these services will disconnect the Management Center from participating in these additional cloud service offerings.

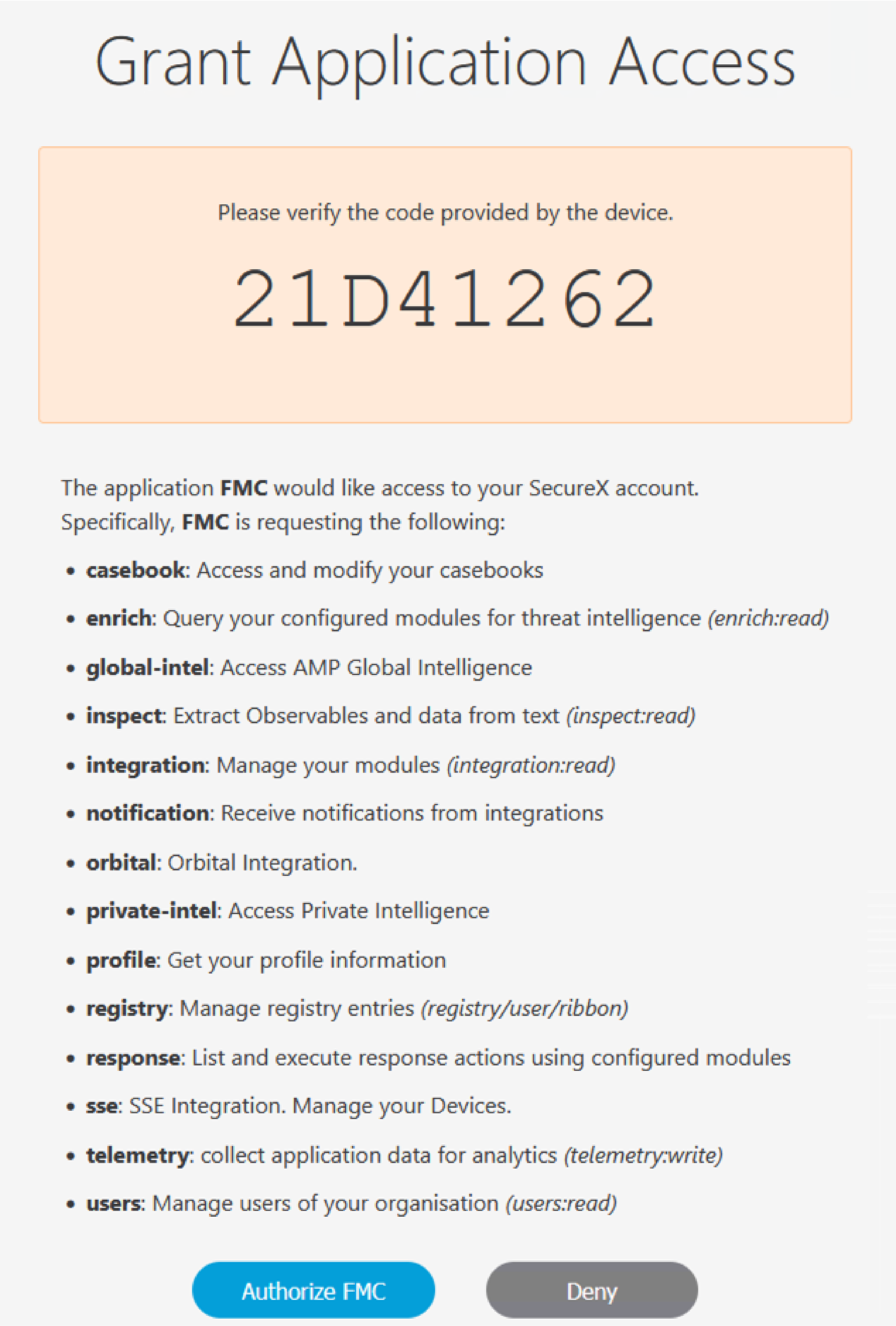
☑ Enable Cisco Success Network

□ Enable Cisco Support Diagnostics

Save

请注意，在您选择之前，不会应用更改 Save .

第二步：选择“保存”后，系统会将您重定向到在Cisco XDR帐户中授权FMC（您需要在此步骤之前登录Cisco XDR帐户），选择授权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)*

第三步，授权授予后，您将被重定向到Cisco XDR