

# 使用安全防火墙版本7.2配置SecureX并对其进行故障排除

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景](#)

[配置](#)

[验证](#)

## 简介

本文档介绍如何将SecureX与安全防火墙7.2上的思科安全防火墙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)
- SecureX
- 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包括对Secure Firewall与SecureX和SecureX Orchestration集成的方式所做的更改：

功能	描述
改进了SecureX集成和SecureX协调。	<p>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 &gt; 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 &gt; Integration &gt; 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.</p>

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.sse.e.itd.cisco.com
- eventing-ingest.eu.sse.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>SecureX，选择要连接的区域（美国、欧盟或APJC），选择要转发到SecureX的事件类型，然后选择Enable SecureX:

Firewall Management Center  
Integration / SecureX

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin | cisco SECURE

### SecureX Setup

This feature allows Secure Firewall Management Center to integrate with other SecureX services via SecureX ribbon. [Learn more](#)

- 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:
- 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](#)
- 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](#)
- 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](#) [Save](#)

### 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

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SecureX帐户中授权您的FMC（您需要在此步骤之前登录SecureX帐户），选择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*)

Authorize FMC

Deny

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。