

Configuración y solución de problemas de SecureX con Secure Firewall versión 7.2

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Background](#)

[Configurar](#)

[Verificación](#)

Introducción

Este documento describe cómo integrar y resolver problemas de SecureX con la integración de Cisco Secure Firewall en Secure Firewall 7.2.

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- Centro de administración Firepower (FMC)
- Firewall seguro de Cisco
- Virtualización opcional de imágenes
- Secure Firewall y FMC deben tener licencia

Componentes Utilizados

- Firewall seguro de Cisco - 7.2
- FirePOWER Management Center (FMC): 7,2
- Security Services Exchange (SSE)
- SecureX
- Portal de licencias inteligentes
- Cisco Threat Response (CTR)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Background

La versión 7.2 incluye cambios en la forma en que Secure Firewall se integra con SecureX y SecureX Orchestration:

Función	Descripción
Integración de SecureX mejorada, orquestación de SecureX.	<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 > 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.</p>

Consulte las [Release Notes](#) completas de 7.2 para verificar todas las funciones incluidas en esta versión.

Configurar

Antes de iniciar la integración, asegúrese de que se permiten estas URL en su entorno:

Región de Estados Unidos

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

Región UE

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

Región APJ

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

Paso 1. Iniciar el registro de integración en el FMC. Vaya a **Integration>SecureX**, seleccione la región a la que desea conectarse (EE.UU., UE o APJC), seleccione el tipo de eventos que desea reenviar a SecureX y, a continuación, seleccione **Enable 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

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 additional service offerings from Cisco. The Management Center connection at all times. You can turn off this connection at any time. Disabling these services will disconnect the Management Center from these additional cloud service offerings.

Enable Cisco Success Network

Enable Cisco Support Diagnostics

Observe que los cambios no se aplican hasta que seleccione Save .

Paso 2. Una vez que haya seleccionado Save (Guardar), se le redirigirá a authorized your FMC (autorizado) en su cuenta SecureX (debe iniciar sesión en la cuenta SecureX antes de este paso), seleccione 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

Paso 3. Una vez concedida la autorización, se le redirige a SecureX:

Client Access Granted

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

[Go Back to SecureX](#)

En caso de que tenga varias organizaciones, se le mostrará la página de inicio de SecureX para seleccionar la organización en la que desea integrar los dispositivos FMC y Secure Firewall:



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.

[Create Organization >](#)

Paso 4. Una vez seleccionada la organización SecureX, se le redirige de nuevo al FMC y debe aparecer el mensaje que indica que la integración se ha realizado correctamente:



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

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.

[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](#)

Verificación

Una vez finalizada la integración, puede expandir la **cinta** de opciones desde la parte inferior de la página:

Firewall Management Center
Integration / SecureX

Overview Analysis Policies Devices Objects Integration

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:

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 Center maintains this connection at all times. You can turn off this connection at any time through the Cisco Support Diagnostics. Disabling these services will disable these additional cloud service offerings.

Enable Cisco Success Network

Enable Cisco Support Diagnostics

SECURE X Home

SecureX Ribbon

Casebook Incidents Orbital

Notifications Center Settings

Applications

SecureX Launch

Cisco Defense Orchestrator - danieben tenant Launch

Security Services Exchange Launch

Threat Response Launch

My Account

Daniel Benitez danieben@cisco.com admin

DaniebenTG Logged in with S...

En la **cinta**, inicie **Security Services Exchange** y en **Devices** debe ver tanto el FMC como el Secure Firewall que acaba de integrar:

Security Services Exchange

Devices Cloud Services Events Audit Log

Devices for [DaniebenTG](#)

Device Name / ID

0 Rows Selected

<input type="checkbox"/>	%	#	Name ^	Type	Version	Status	Cloud Connectiv...	Description
<input type="checkbox"/>	>	1	MexAmp-FTD	Cisco Firepower...	7.2.0	Registered	2022-08-31 02:35	10.4.242.25 MexAmp-FTD
<input type="checkbox"/>	>	2	mexMEX-AMP-FMcmex	Secure Firewall ...	7.2.0	Registered	2022-08-31 02:34	10.4.242.24 mexMEX-AM

Page Size: Total Entries: 2

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).