

# Cisco XDR mit Secure Firewall Version 7.2 konfigurieren und Fehlerbehebung dafür durchführen

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrund](#)

[Konfigurieren](#)

[Überprüfung](#)

## Einleitung

In diesem Dokument wird beschrieben, wie Cisco XDR in die Cisco Secure Firewall 7.2 integriert wird, um Probleme mit dieser zu beheben.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Firepower Management Center (FMC)
- Sichere Firewall von Cisco
- Optionale Bildvirtualisierung
- Secure Firewall und FMC müssen lizenziert werden

### Verwendete Komponenten

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Hintergrund

Version 7.2 enthält Änderungen hinsichtlich der Integration der sicheren Firewall mit Cisco XDR und Cisco

## XDR Orchestration:

Funktion	Beschreibung
Verbesserte Cisco XDR-Integration, Cisco XDR-Orchestrierung.	<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 orchestrationâ€™a powerful drag-and-drop interface you can use to automate workflows across security tools. After you enable SecureX, you can enable orchestration.</p>

In den vollständigen [Versionshinweisen](#) von 7.2 finden Sie alle in dieser Version enthaltenen Funktionen.

## Konfigurieren

Stellen Sie vor Beginn der Integration sicher, dass die folgenden URLs in Ihrer Umgebung zulässig sind:

### Region USA

- [api-sse.cisco.com](https://api-sse.cisco.com)
- [eventing-ingest.sse.itd.cisco.com](https://eventing-ingest.sse.itd.cisco.com)

### EU-Region

- [api.eu.sse.itd.cisco.com](https://api.eu.sse.itd.cisco.com)
- [eventing-ingest.eu.sse.itd.cisco.com](https://eventing-ingest.eu.sse.itd.cisco.com)

### APJ-Region

- [api.apj.sse.itd.cisco.com](https://api.apj.sse.itd.cisco.com)
- [eventing-ingest.apj.sse.itd.cisco.com](https://eventing-ingest.apj.sse.itd.cisco.com)

**Schritt 1:** Um die Integration zu starten, melden Sie sich beim FMC an. Gehen Sie zu **Integration>Cisco XDR**, wählen Sie die Region aus, mit der Sie eine Verbindung herstellen möchten (USA, EU oder APJC), wählen Sie die Art der Ereignisse aus, die Sie an Cisco XDR weiterleiten möchten, und wählen Sie dann **Cisco XDR aktivieren aus:**



## 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

Beachten Sie, dass die Änderungen erst angewendet werden, wenn Sie **Save** .

**Schritt 2:** Nachdem Sie "Speichern" ausgewählt haben, werden Sie an das autorisierte FMC Ihres Cisco XDR-Kontos weitergeleitet (Sie müssen sich vor diesem Schritt beim Cisco XDR-Konto anmelden). Wählen Sie **FMC autorisieren aus**:

# 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

**Schritt 3:** Sobald die Autorisierung erteilt wurde, werden Sie zu Cisco XDR umgeleitet:

# Client Access Granted

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

[Go Back to SecureX](#)

Wenn Sie mehrere Organisationen betreiben, wird Ihnen die Cisco XDR-Startseite angezeigt, auf der Sie die Organisation auswählen können, in die Sie Ihre FMC- und Secure Firewall-Geräte integrieren möchten:



### 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 >](#)

**Schritt 4:** Nachdem die Cisco XDR-Organisation ausgewählt wurde, werden Sie erneut an das FMC weitergeleitet, und es muss eine Meldung angezeigt werden, dass die Integration erfolgreich war:



## 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](#)

## Überprüfung

Nach Abschluss der Integration können Sie die **Multifunktionsleiste** unten auf der Seite erweitern:

The screenshot displays the 'SecureX Integration' page in the Firewall Management Center. The 'SecureX Setup' section includes a 'Cloud Region' dropdown set to 'us-east-1 (US Region)' and a 'SecureX Enablement' section. The 'Cisco Cloud Support' section has two checkboxes: 'Enable Cisco Success Network' (checked) and 'Enable Cisco Support Diagnostics' (unchecked). Below the configuration is a navigation bar with 'SecureX Ribbon' (Casebook, Incidents, Orbital, Notifications Center, Settings), 'Applications' (SecureX, Cisco Defense Orchestrator, Security Services Exchange, Threat Response), and 'My Account' (Daniel Benitez, DaniebenTG).

Starten Sie auf dem **Menüband Security Services Exchange**, und sehen Sie unter **Devices** (Geräte) sowohl das FMC als auch die Secure Firewall, die Sie gerade integriert haben:

The screenshot shows the 'Security Services Exchange' page with the 'Devices' tab selected. The page title is 'Devices for DaniebenTG'. There is a search bar for 'Device Name / ID'. Below the search bar, it says '0 Rows Selected'. A table lists the devices:

	%	#	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: 25 Total Entries: 2

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.