

Cisco XDR configureren en problemen oplossen met Secure Firewall release 7.2

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrond](#)

[Configureren](#)

[Verifiëren](#)

Inleiding

Dit document beschrijft hoe u Cisco XDR kunt integreren en problemen kunt oplossen met de integratie van Cisco Secure Firewall in Secure Firewall 7.2.

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- Firepower Management Center (FMC)
- Cisco Secure-firewall
- Optionele virtualisatie van afbeeldingen
- Secure Firewall en VCC moeten zijn gelicentieerd

Gebruikte componenten

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrond

Release 7.2 omvat wijzigingen in de manier waarop Secure Firewall in Cisco XDR en Cisco XDR Orchestration wordt geïntegreerd:

Feature	Beschrijving
<p>Verbeterde Cisco XDR integratie, Cisco XDR orkestratie.</p>	<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 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>

Raadpleeg 7.2 volledige [Releaseopmerkingen](#) om alle functies in deze release te controleren.

Configureren

Zorg ervoor dat deze URLâ€™s zijn toegestaan op uw omgeving, voordat u de integratie start:

Amerikaanse regio

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

EU-regio

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

APJ-regio

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

Stap 1. Het integratielogboek in het VCC starten. Ga naar **Integratie>Cisco XDR**, selecteer de regio waar u verbinding wilt maken (VS, EU of APJC), selecteer het type gebeurtenissen dat u wilt doorsturen naar Cisco XDR en selecteer vervolgens **Cisco XDR inschakelen**:



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

Bericht dat de veranderingen niet worden toegepast, tot uitgezocht u Save .

Stap 2. Nadat Save is geselecteerd, wordt u doorgestuurd naar de geautoriseerde locatie van uw VCC in uw Cisco XDR-account (u moet vóór deze stap inloggen op de Cisco XDR-account). Selecteer **FMC autoriseren**:

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

Stap 3. Nadat de autorisatie is verleend, wordt u doorgestuurd naar Cisco XDR:

Client Access Granted

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

[Go Back to SecureX](#)

Als u meerdere Orgs hebt, krijgt u de landingspagina van Cisco XDR om de organisatie te selecteren waar u uw FMC en Secure Firewall-apparaten wilt integreren:



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 >](#)

Stap 4. Nadat de Cisco XDR-organisatie is geselecteerd, wordt u opnieuw doorgestuurd naar het VCC en krijgt u het bericht dat aangeeft dat de integratie is geslaagd:



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](#)

Verifiieren

Zodra de integratie is voltooid, kunt u het **lint** uitvouwen onder aan de pagina:

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. Disabling these services will disconnect the Management Center from these additional cloud service offerings.

Enable Cisco Success Network

Enable Cisco Support Diagnostics

Navigation bar: Home, SecureX Ribbon (Casebook, Incidents, Orbital, Notifications Center, Settings), Applications (SecureX, Cisco Defense Orchestrator - danieben tenant, Security Services Exchange, Threat Response), My Account (Daniel Benitez, danieben@cisco.com, admin, DaniebenTG, Logged in with S...)

Op het **lint**, lanceer **Security Services Exchange** en onder **Apparaten** moet u zowel de FMC en Secure Firewall zien die u zojuist hebt geïntegreerd:

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.