Configuration et dépannage de Cisco XDR avec Secure Firewall version 7.2

Table des matières

Introduction

Ce document décrit comment intégrer et dépanner Cisco XDR avec l'intégration de Cisco Secure Firewall sur Secure Firewall 7.2.

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Firepower Management Center (FMC)
- Pare-feu sécurisé Cisco
- Virtualisation facultative des images
- Secure Firewall et FMC doivent être sous licence

Composants utilisés

- Pare-feu sécurisé Cisco - 7.2
- Centre de gestion Firepower (FMC) - 7.2
- Échange de services de sécurité (SSE)
- Cisco XDR
- Portail de licences Smart
- Cisco Threat Response (CTR)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Fond

La version 7.2 inclut des modifications sur la façon dont Secure Firewall s'intègre à Cisco XDR et à Cisco XDR Orchestration :

Fonctionnalité	Description
Intégration améliorée de Cisco XDR, orchestration de Cisco XDR.	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.

Consultez les Notes de version complètes de 7.2 pour vérifier toutes les fonctionnalités incluses dans cette version.

Configurer

Avant de commencer l'intégration, assurez-vous que les URL suivantes sont autorisées dans votre environnement :

Région des États-Unis

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

Région de l'UE

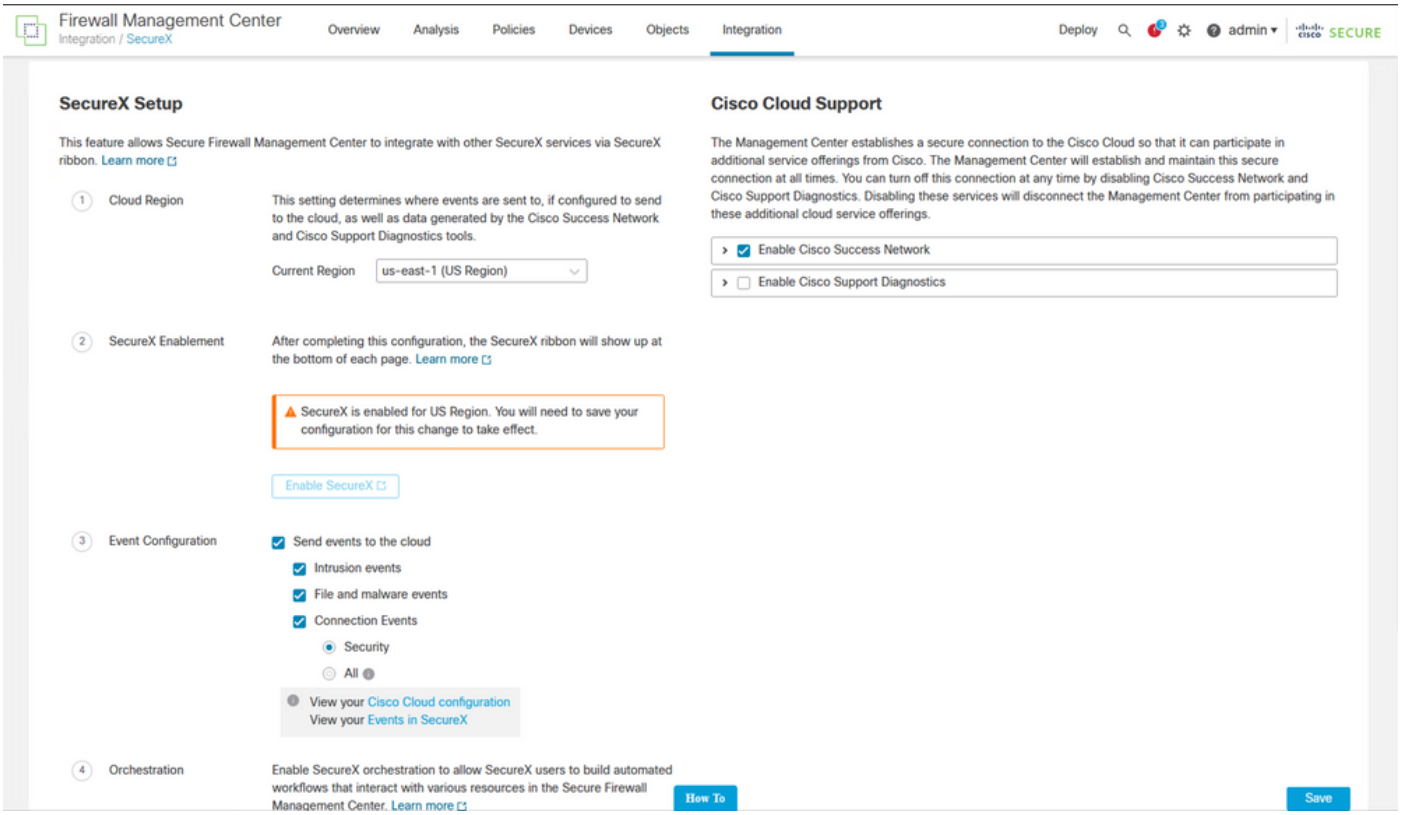
- api.eu.sse.itd.cisco.com

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

Région APJ

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

Étape 1. Pour démarrer le journal d'intégration dans le FMC Accédez à Integration>Cisco XDR, sélectionnez la région où vous souhaitez vous connecter (US, EU ou APJC), sélectionnez le type d'événements que vous souhaitez transférer à Cisco XDR, puis sélectionnez Enable Cisco XDR:



Notez que les modifications ne sont pas appliquées tant que vous ne sélectionnez pas Save .

Étape 2. Une fois l'option Enregistrer sélectionnée, vous êtes redirigé vers votre FMC autorisé dans votre compte Cisco XDR (vous devez vous connecter au compte Cisco XDR avant cette étape), sélectionnez Autoriser FMC :

Grant Application Access

Please verify the code provided by the device.

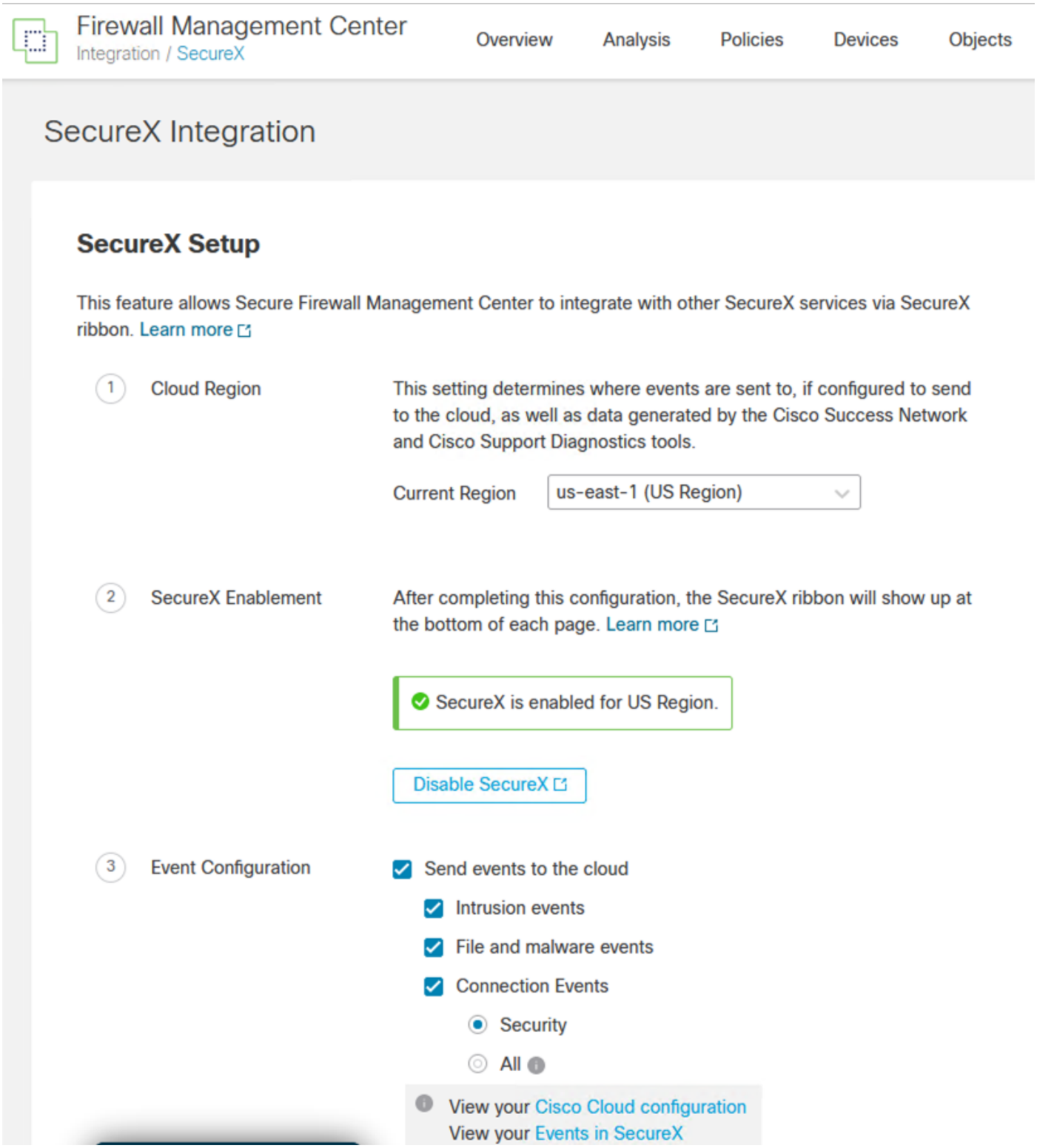
21D41262

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)*

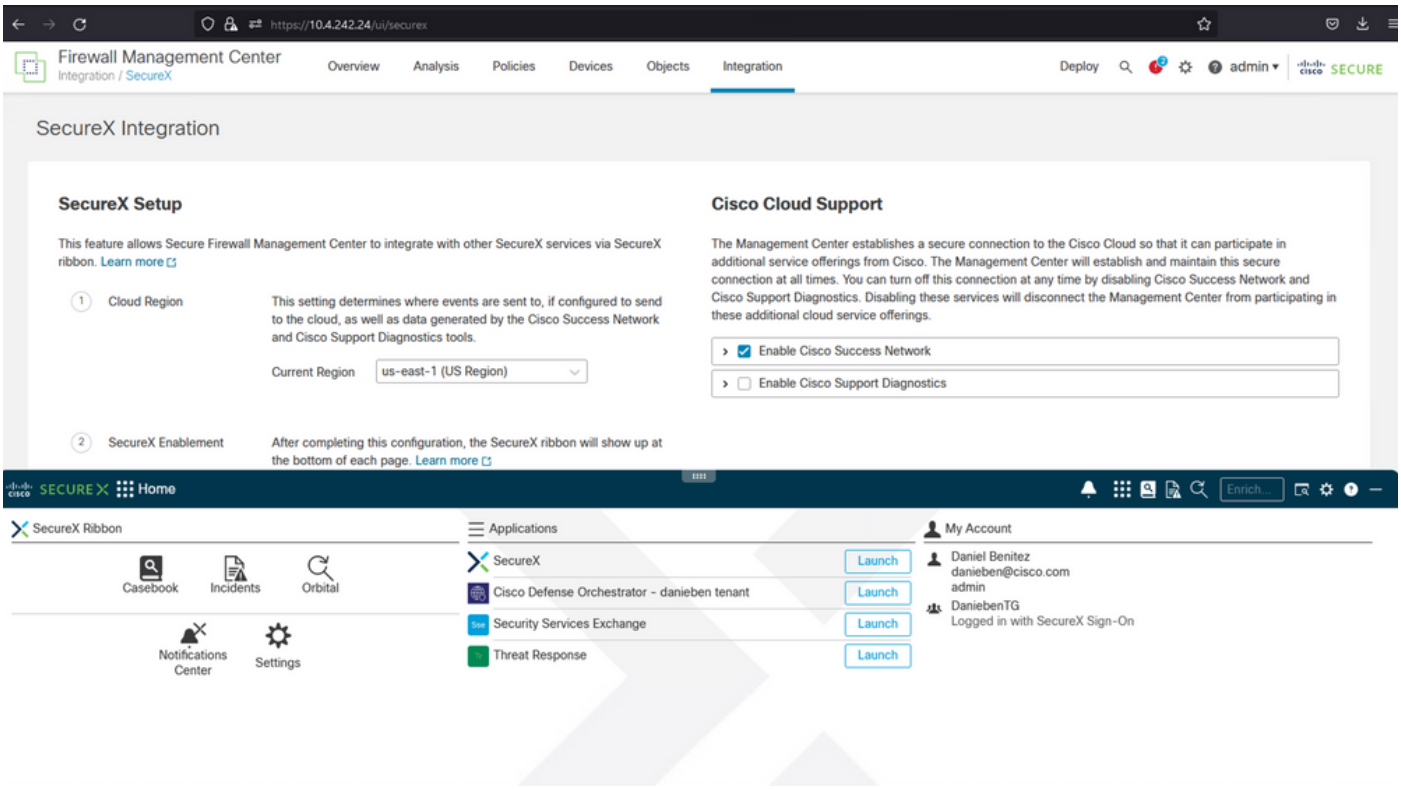
Authorize FMC Deny

Une fois l'organisation Cisco XDR sélectionnée, vous êtes redirigé, une fois de plus vers le FMC et vous devez recevoir le message indiquant que l'intégration a réussi :

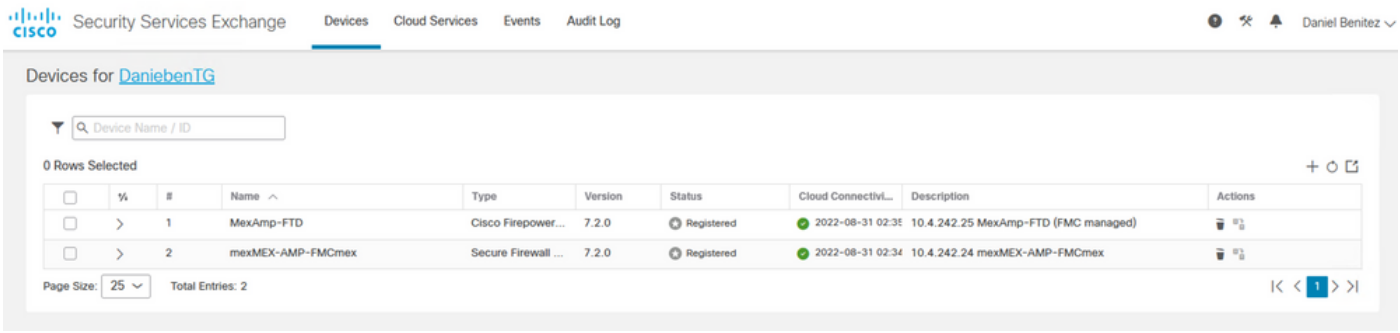


Vérifier

Une fois l'intégration terminée, vous pouvez développer le Ruban à partir du bas de la page :



Sur le Ruban, lancez Security Services Exchange et sous Devices vous devez voir à la fois le FMC et le pare-feu sécurisé que vous venez d'intégrer :



À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.