Secure Firewallリリース7.2を使用したCisco XDRの設定とトラブルシューティング

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[バックグラウンド](#)
[設定](#)
[確認](#)

概要

このドキュメントでは、Cisco XDRとSecure Firewall 7.2上のCisco Secure Firewallの統合を統合し、トラブルシューティングする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Firepower Management Center（FMC）
- Cisco Secureファイアウォール
- イメージの仮想化（オプション）
- セキュアファイアウォールとFMCのライセンスが必要

使用するコンポーネント

- Cisco Secure Firewall:7.2
- Firepower Management Center(FMC) - 7.2
- セキュリティサービスエクスチェンジ(SSE)
- Cisco XDR
- スマートライセンスポータル
- Cisco Threat Response（CTR）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

バックグラウンド

リリース7.2では、Secure FirewallがCisco XDRおよびCisco XDR Orchestrationと統合される方法が変更されています。

機能	説明
Cisco XDR統合、Cisco XDRオーケストレーションの改善	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.

このリリースに含まれるすべての機能を確認するには、7.2の完全な『リリースノート』を参照してください。

設定

統合を開始する前に、ご使用の環境で次のURLが許可されていることを確認してください。

米国地域

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

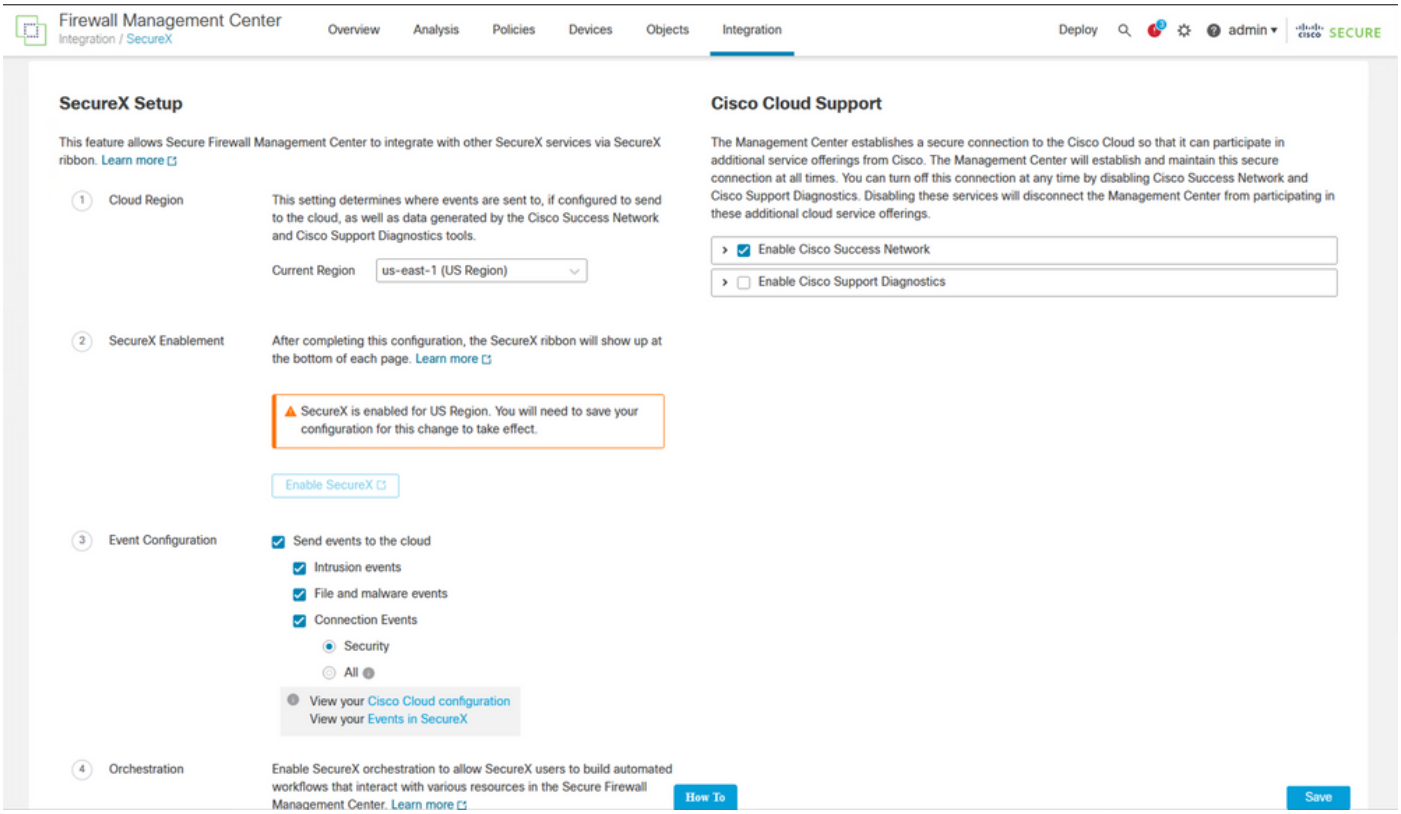
EU地域

- api.eu.ss e.itd.cisco.com
- eventing-ingest.eu.ss e.itd.cisco.com

APJ地域

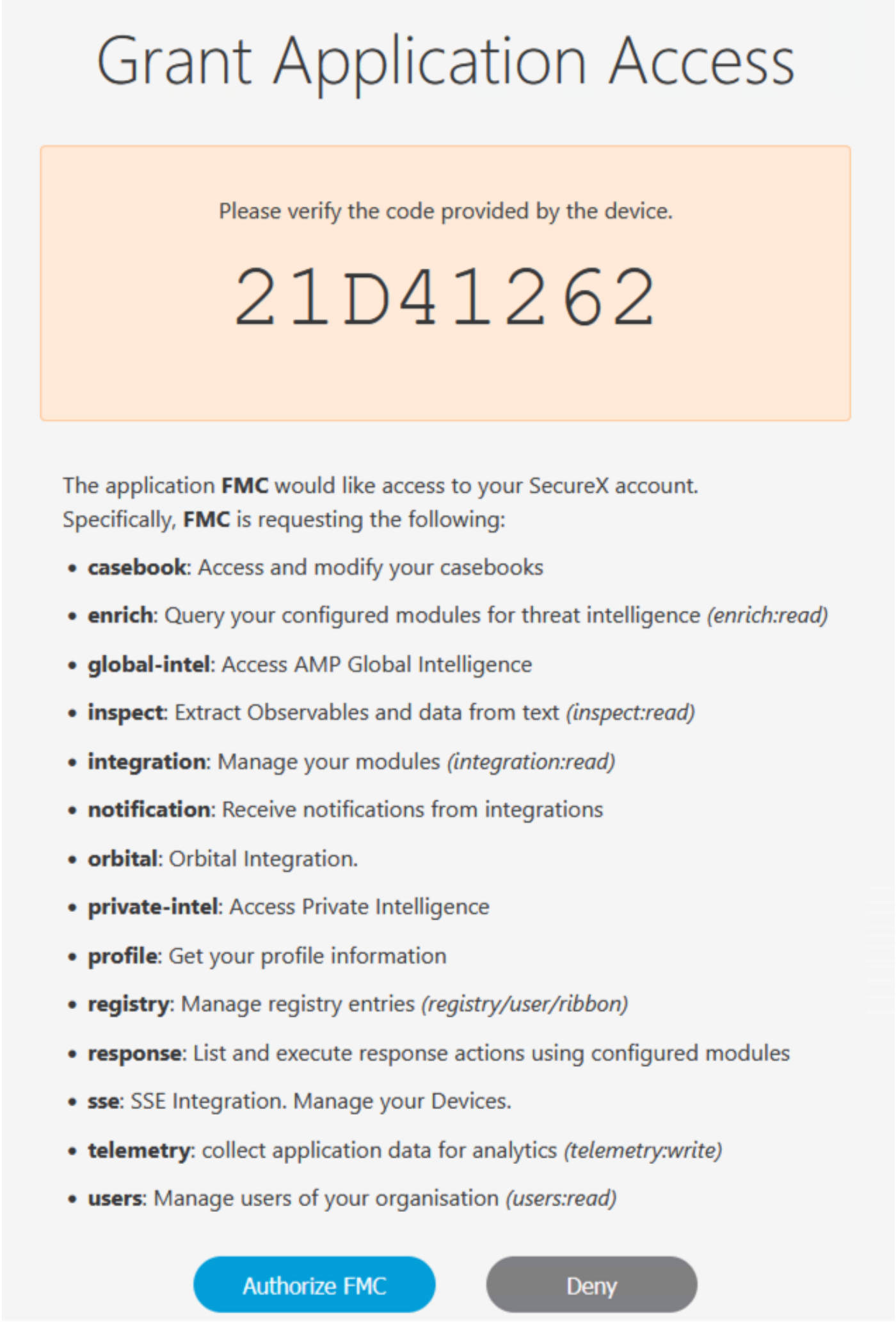
- api.apj.sse.itd.cisco.com
- eventing-ingest.apj.sse.itd.cisco.com

ステップ1:統合を開始するには、FMCにログインします。Integration > Cisco XDRの順に移動し、接続する地域（米国、EU、またはAPJC）を選択し、Cisco XDRに転送するイベントのタイプを選択してから、Enable Cisco XDR:



を選択するまで、変更は適用されません Save を参照。

ステップ 2：保存を選択すると、Cisco XDRアカウントでFMCが承認されるようにリダイレクトされます（この手順の前にCisco XDRアカウントにログインする必要があります）。Authorize FMCを選択します。


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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。