Secure Firewall Release 7.2로 Cisco XDR 구성 및 문제 해결

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[배경](#)
[구성](#)
[다음을 확인합니다.](#)

소개

이 문서에서는 Cisco XDR과 Secure Firewall 7.2의 Cisco Secure Firewall 통합을 통합하고 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- FMC(Firepower Management Center)
- Cisco 보안 방화벽
- 이미지 가상화 옵션
- Secure Firewall 및 FMC는 라이센스가 있어야 합니다.

사용되는 구성 요소

- Cisco Secure Firewall - 7.2
- FMC(firepower 관리 센터) - 7.2
- SSE(Security Services Exchange)
- Cisco XDR
- Smart License 포털
- Cisco CTR(Threat Response)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경

릴리스 7.2에는 보안 방화벽과 Cisco XDR 및 Cisco XDR 오케스트레이션의 통합 방식에 대한 변경 사항이 포함되어 있습니다.

기능	설명
Cisco XDR 통합, Cisco XDR 오케스트레이션 개선.	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.

이 릴리스에 포함된 모든 기능을 확인하려면 7.2 릴리스 정보를 참조하십시오.

구성

통합을 시작하기 전에 사용자 환경에서 다음 URL이 허용되는지 확인합니다.

미국 지역

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

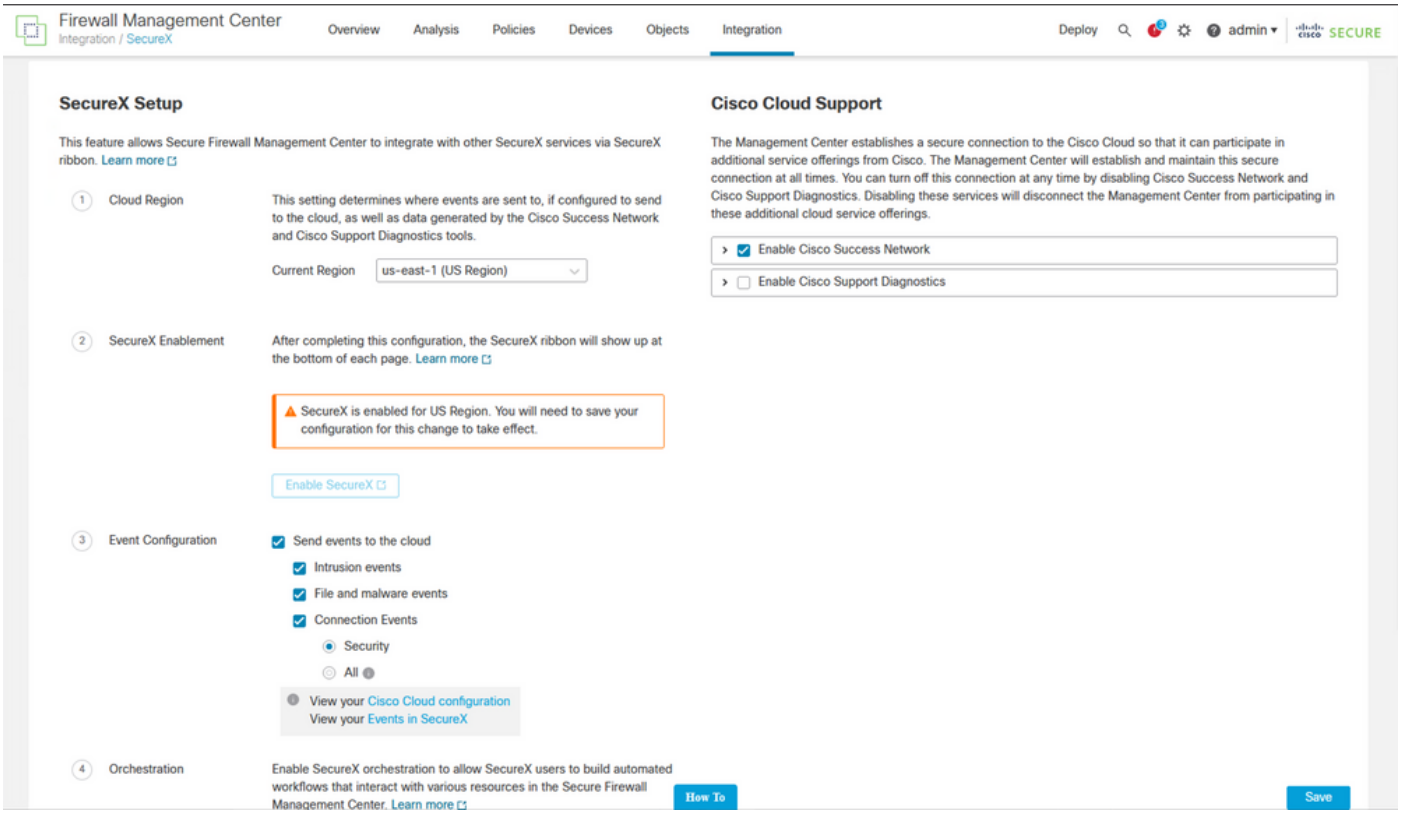
EU 지역

- api.eu.sse.itd.cisco.com을 참조하십시오.
- eventing-ingest.eu.sse.itd.cisco.com을 참조하십시오.

APJ 지역

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

1단계. FMC에 대한 통합 로그를 시작합니다. 통합>Cisco XDR로 이동하여 연결할 지역(미국, EU 또는 APJC)을 선택하고 Cisco XDR로 전달할 이벤트 유형을 선택한 다음 Cisco XDR 사용을 선택합니다.



를 선택할 때까지 변경 사항이 적용되지 않습니다 Save .

2단계. [저장]을 선택하면 Cisco XDR 계정에서 FMC를 인증하도록 리디렉션됩니다(이 단계를 수행하기 전에 Cisco XDR 계정에 로그인해야 함). 다음과 같이 FMC 권한 부여를 선택합니다.

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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.