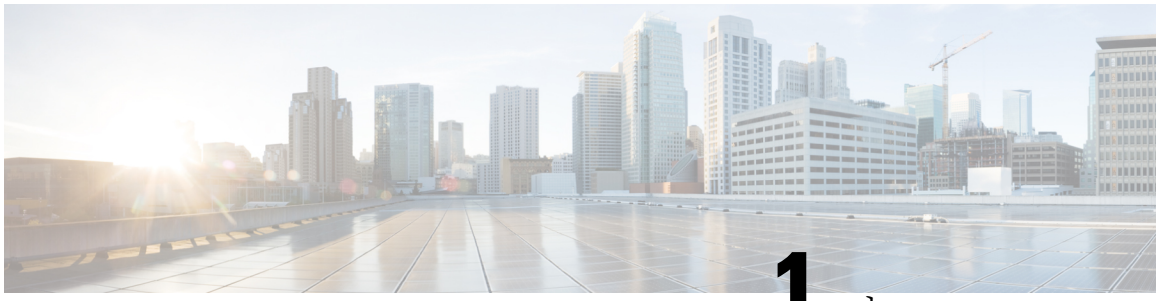
Cisco Secure Firewall Threat Defense 및 Cisco XDR 통합 가이드

최종 변경: 2024년 12월 16일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



1 장

Secure Firewall Threat Defense와 Cisco XDR 통합 소개

Secure Firewall Threat Defense 및Cisco XDR 통합에 관한 정보

Secure Firewall Threat Defense를 Cisco Extended Detection and Response(Cisco XDR)와 통합하여 Cisco의 통합 보안 포트폴리오와 방화벽 구축을 연결하여 가시성을 통합하고 자동화를 가능하게 하며 네트워크 전반에서 보안을 강화하는 일관된 환경을 구축합니다.

Cisco XDR 정보

Cisco XDR는 여러 텔레메트리 소스에서 탐지를 상호 연결하여 가시성을 통합하는 클라우드 기반 솔루션 으로, 보안 팀이 가장 정교한 위협을 탐지하고 우선 순위를 정하고 이에 대응합니다.

방화벽 구축을 Cisco XDR와 통합하여 다음을 수행할 수 있습니다.

- 방화벽 이벤트를 상호 연결하고 분석하여 엔드 투 엔드 인시던트를 확인하고 위험을 기반으로 인시던트를 승격하므로 분석가가 시급하게 해결해야 하는 사항에 집중할 수 있습니다.
- 알림의 우선순위를 명확하게 지정하고 탐지부터 대응까지 최단 경로를 제공하여 위협 탐지 및 대응 기능을 향상합니다.
- 자동화와 가이드형 대응 권장 사항을 사용하여 자신 있게 위협을 해소합니다.

Cisco XDR에 대한 자세한 내용은 Cisco XDR 도움말 센터를 참조하십시오.

참고 Cisco XDR는 별도 라이선스 제품입니다. Cisco Secure Firewall 제품에 필요한 라이선스 외에 추가 구독이 필요합니다. 자세한 정보는 Cisco XDR 라이선스를 참고하십시오.

지역 클라우드

표 *1:* 지역 클라우드의 ***URL***

지역	클라우드에 연결	지원되는 통합 방법 및 **Threat Defense** 디바이스 버전
북미	• api-sse.cisco.com • mx*.sse.itd.cisco.com • eventing-ingest.sse.itd.cisco.com • defenseorchestrator.com • edge.us.cdo.cisco.com	• 직접 통합: 버전 6.4 이상 • 시스템 로그를 이용한 통합: 버전 6.3 이상
유럽	• api.eu.sse.itd.cisco.com • mx*.eu.sse.itd.cisco.com • eventing-ingest.eu.sse.itd.cisco.com • defenseorchestrator.eu • edge.eu.cdo.cisco.com	• 직접 통합: 버전 6.5 이상 • 시스템 로그를 이용한 통합: 버전 6.3 이상
아시아(APJC)	• api.apj.sse.itd.cisco.com • mx*.apj.sse.itd.cisco.com • eventing-ingest.apj.sse.itd.cisco.com • apj.cdo.cisco.com • edge.apj.cdo.cisco.com	• 직접 통합: 버전 6.5 이상 • 시스템 로그를 이용한 통합: 버전 6.3 이상
호주	• api.aus.sse.itd.cisco.com • mx*.aus.sse.itd.cisco.com • eventing-ingest.aus.sse.itd.cisco.com • aus.cdo.cisco.com	• 직접 통합: 버전 6.5 이상 • 시스템 로그를 이용한 통합: 버전 6.3 이상

지역	클라우드에 연결	지원되는 통합 방법 및 **Threat Defense** 디바이스 버전
인도	• api.in.sse.itd.cisco.com • mx*.in.sse.itd.cisco.com • eventing-ingest.in.sse.itd.cisco.com • in.cdo.cisco.com	• 직접 통합: 버전 6.5 이상 • 시스템 로그를 이용한 통합: 버전 6.3 이상

지역 클라우드 선택 지침 및 제한 사항

지역 클라우드를 선택할 때는 다음 사항을 염두에 두십시오.

- 지역 클라우드 선택은 Threat Defense 디바이스 버전 및 통합 방법(시스템 로그 또는 직접)에 따라 다릅니다.

  지역 클라우드 및 해당 URL의 목록은 지역 클라우드를 참조하십시오.

- 가능하다면 구축한 곳에서 가장 가까운 지역 클라우드를 사용하십시오.
- 다른 지역 클라우드에서는 데이터를 병합하거나 집계할 수 없습니다. 여러 지역의 데이터를 집계하려면 모든 지역의 디바이스가 동일한 지역 클라우드로 데이터를 전송해야 합니다.
- 각 지역 클라우드에서 어카운트를 만들 수 있으며 각 클라우드의 데이터는 별도로 유지됩니다.
- 선택한 지역 클라우드는 Cisco 지원 진단 및 Cisco 지원 네트워크 기능에도 사용됩니다. 이 설정은 Security Analytics and Logging(SaaS)를 사용하는 Secure Network Analytics 클라우드의 클라우드 영역에도 적용됩니다.

지원되는 이벤트 유형

Threat Defense 및 Cisco XDR 통합은 다음 이벤트 유형을 지원합니다.

표 ***2: Cisco Security Cloud***로 이벤트를 전송하기 위해 지원되는 이벤트 유형

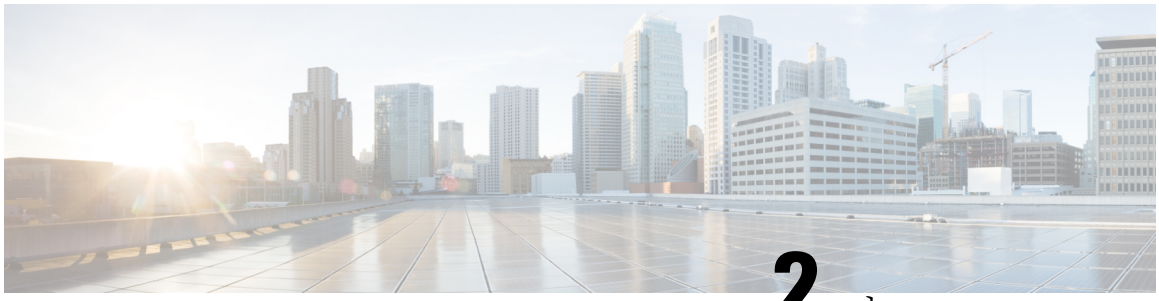
이벤트 유형	직접 통합을 위한 지원되는 **Threat Defense** 디바이스 버전	시스템 로그 통합을 위한 지원되는 **Threat Defense** 디바이스 버전
침입 이벤트	6.4 이상	6.3 이상

이벤트 유형	직접 통합을 위한 지원되는 **Threat Defense** 디바이스 버전	시스템 로그 통합을 위한 지원되는 **Threat Defense** 디바이스 버전
높은 우선순위 연결 이벤트 수행: • 보안 관련 연결 이벤트. • 파일 및 악성코드 이벤트와 관련된 연결 이벤트. • 침입 이벤트와 관련된 연결 이벤트.	6.5 이상	지원되지 않음
파일 및 악성코드 이벤트	6.5 이상	지원되지 않음

이벤트를 클라우드로 전송하는 방법 비교

Threat Defense 디바이스는 시스템 로그를 이용하거나 직접 보안 서비스 익스체인지 포털을 통해 이벤트를 클라우드에 전송합니다.

직접 이벤트 전송	시스템 로그를 사용하여 이벤트 전송
지원되는 소프트웨어 버전을 실행하는 Threat Defense 디바이스만 지원합니다.	지원되는 소프트웨어 버전을 실행하는 모든 디바이스를 지원합니다.
버전 6.4 이상을 지원합니다.	버전 6.3 이상을 지원합니다.
나열된 모든 이벤트 유형을 지원합니다.	침입 이벤트만 지원합니다.
Threat defense 디바이스가 인터넷에 연결되어 있어야 합니다.	디바이스는 인터넷에 연결하지 않아도 됩니다.
구축에서는 Smart Software Manager 온 프레미스 서버(이전 명칭은 Smart Software Satellite Server)를 사용할 수 없습니다.	구축시 Smart Software Manager 온 프레미스 서버를 사용할 수 있습니다.
사내 프록시 서버를 설정하고 유지 관리하지 않아도 됩니다.	온프레미스 가상 Cisco Security Services 프록시 서버가 필요합니다. 이 프록시 서버에 대한 자세한 내용은 Cisco Security Services 프록시를 참조하십시오. 보안 서비스 익스체인지에 액세스하려면 보안 서비스 익스체인지 액세스를 참조하십시오.



2 장

Cisco Security Cloud 어카운트

Cisco XDR 통합을 활성화하는 데 필요한 계정

Management Center를 Cisco Security Cloud과 통합하고 분석 및 위협 조사를 위해 Cisco XDR에 이벤트를 전송하려면 지역 클라우드 에 다음 계정 중 하나가 있어야 합니다.

- Cisco Security Cloud 로그인 계정.
- Secure Endpoint 계정
- Secure Malware Analytics 계정
- Cisco 보안 계정.

중요 사용자나 사용자의 조직이 대상 지역 클라우드에서 상기 계정 중 하나를 이미 이용하고 있다면, 기존 계정을 사용하십시오. 새 계정을 생성하지 마십시오. 계정과 연결된 데이터는 해당 계정에만 사용할 수 있습니다.

계정이 없다면 Cisco XDR 통합 활성화를 위한 계정 얻기, 6 페이지의 내용을 참조하십시오.

직접 통합을 위해서는 관리 센터 및 매니지드 디바이스를 등록하는 CDO 테넌트가 필요합니다. 아직 CDO 테넌트가 없는 경우 테넌트를 요청합니다. 자세한 내용은 CDO 테넌트 요청을 참조하십시오.

Cisco XDR 통합 활성화를 위한 계정 얻기

시작하기 전에

사용할 지역 클라우드에서 사용자가 사용자의 조직이 이미 계정을 만들었다면, 새 계정을 만들지 마십시오. 기존 계정을 사용하여 Cisco XDR에 방화벽 이벤트 데이터 전송을 활성화합니다. 조직에 이미 해당 클라우드에 대해 지원되는 계정이 있는지 확인합니다. 지원되는 계정 유형에 대해서는 Cisco XDR 통합을 활성화하는 데 필요한 계정, 5 페이지의 내용을 참조하십시오. 조직 내 누군가가 해당 지역 클라우드의 계정을 이미 만들었다면 해당 계정 관리자에게 대신 계정을 추가해달라고 요청해야 합니다. 자세한 내용은 사용자 CDO 계정에 대한 액세스 관리, 6 페이지를 참조하십시오.

프로시저

단계 **1** 사용할 지역 클라우드를 결정합니다. 자세한 내용은 지역 클라우드 선택 지침 및 제한 사항, 3 페이지를 참고하십시오.

단계 **2** 보안 클라우드 로그인 어카운트가 없지만 하나를 만들려면 선택한 지역 클라우드로 이동합니다.

지역 클라우드 및 해당 URL의 목록은 지역 클라우드, 2 페이지의 내용을 참조하십시오.

단계 **3** **Sign Up Now(**지금 등록하기**)**를 클릭합니다.

보안 클라우드 로그인 계정을 생성하는 방법에 대한 자세한 내용은 새 Cisco Security Cloud 로그인 계정 생성을 참조하십시오.

클라우드 계정에 대한 액세스 관리

사용자 계정 관리는 보유한 클라우드 계정의 유형에 따라 달라집니다.

참고 Secure Malware Analytics 또는 Secure Endpoint 계정을 사용하여 클라우드에 액세스하는 경우 해당 제품에 대한 설명서를 참조하십시오.

사용자 CDO 계정에 대한 액세스 관리

Cisco Security Cloud에 액세스하기 위해 CDO 계정을 사용하는 경우 이 절차를 사용하여 사용자를 관리합니다.

시작하기 전에

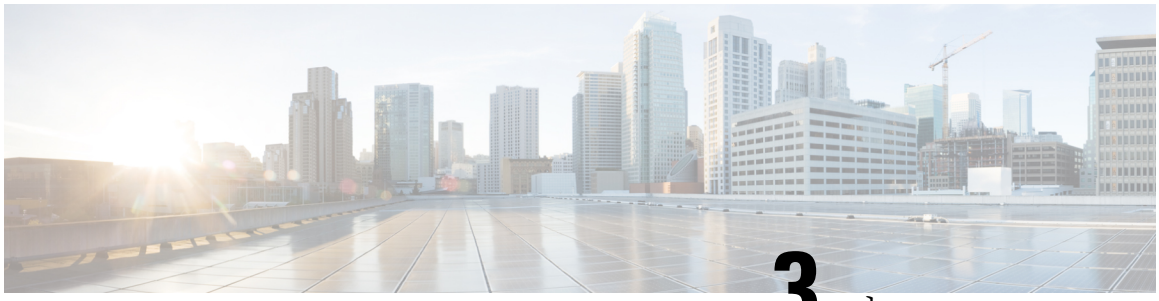
이 작업을 수행하려면 CDO에 슈퍼 관리자 권한이 있어야 합니다.

프로시저

단계 1 CDO에 로그인합니다.

단계 2 CDO 내비게이션 바에서 **Settings(**설정**)** > **User Management(**사용자 관리**)**를 클릭합니다.

CDO의 사용자 관리에 대한 자세한 내용은 CDO 온라인 도움말을 참조하십시오.



3 장

클라우드로 이벤트 바로 전송

직접 통합 관련 정보

Threat Defense 릴리스 6.4부터는 지원되는 방화벽 이벤트를 Cisco Security Cloud로 직접 전송하도록 Threat Defense 디바이스를 구성할 수 있습니다. 디바이스는 이벤트를 보안 서비스 익스체인지로 전송하며, 여기서 Cisco XDR를 비롯한 다양한 클라우드 서비스로 이벤트를 승격하여 이벤트 분석 및 조사를 개선할 수 있습니다.

직접 통합 요구사항

요구 사항 유형	요건
Secure Firewall 버전	• 미국 클라우드의 경우 Threat Defense 버전 6.4 이상. • 유럽, APJC, 인도, 호주 클라우드의 경우 Threat Defense 버전 6.5 이상. • SecureX 통합 또는 Cisco Security Cloud 통합을 활성화하여 이벤트를 직접 전송하는 경우, Management Center 버전 7.0.2에서 7.0.x 또는 버전 7.2.0 이상까지.

요구 사항 유형	요건
라이선싱	• Cisco Cloud에 전송할 이벤트를 생성하려면 시스템에 라이선스가 있어야 합니다. 자세한 내용은 Cisco Secure Firewall 라이선싱 정보를 참조하십시오. • 사용자의 환경에서는 Cisco Smart Software Manager 온 프레미스 서버(이전 Cisco Smart Software Satellite 서버)를 사용하거나 에어 갭 환경에 구축할 수 없습니다. • Cisco XDR는 별도 라이선스 제품입니다. Cisco Secure Firewall 제품에 라이선스 외에 추가 구독이 필요합니다. 자세한 정보는 Cisco XDR 라이선스를 참고하십시오. • 이미 SecureX 구독을 사용하여 Cisco Security Cloud로 이벤트를 전송하고 있었다면 계속해서 Cisco XDR로 이벤트를 전송할 수 있습니다. 하지만 이제 CDO 계정을 사용하여 클라우드 테넌시에 Management Center를 등록하는 경우 CDO 계정에 Cisco XDR로 이벤트를 전달할 수 있는 Security Analytics and Logging 라이선스가 있어야 합니다.

요구 사항 유형	요건
연결성	

요구 사항 유형	요건
	Management Center 및 매니지드 디바이스는 다음 주소의 Cisco Security Cloud로의 아웃바운드 연결을 포트 443에서 지원해야 합니다. • 미국 지역: • api-sse.cisco.com • mx*.sse.itd.cisco.com • dex.sse.itd.cisco.com • eventing-ingest.sse.itd.cisco.com • registration.us.sse.itd.cisco.com • defenseorchestrator.com • edge.us.cdo.cisco.com • EU 지역: • api.eu.sse.itd.cisco.com • mx*.eu.sse.itd.cisco.com • dex.eu.sse.itd.cisco.com • eventing-ingest.eu.sse.itd.cisco.com • registration.eu.sse.itd.cisco.com • defenseorchestrator.eu • edge.eu.cdo.cisco.com • 아시아(APJC) 지역: • api.apj.sse.itd.cisco.com • mx*.apj.sse.itd.cisco.com • dex.apj.sse.itd.cisco.com • eventing-ingest.apj.sse.itd.cisco.com • registration.apj.sse.itd.cisco.com • apj.cdo.cisco.com • edge.apj.cdo.cisco.com • 호주 지역: • api.aus.sse.itd.cisco.com

요구 사항 유형	요건
	• mx*.aus.sse.itd.cisco.com • dex.au.sse.itd.cisco.com • eventing-ingest.aus.sse.itd.cisco.com • registration.au.sse.itd.cisco.com • aus.cdo.cisco.com • 인도 지역: • api.in.sse.itd.cisco.com • mx*.in.sse.itd.cisco.com • dex.in.sse.itd.cisco.com • eventing-ingest.in.sse.itd.cisco.com • registration.in.sse.itd.cisco.com • in.cdo.cisco.com
일반	방화벽 구축에서 예상대로 이벤트가 생성되고 있습니다.

고가용성 구축 및 **Cisco Security Cloud** 통합

다음에서는 방화벽 고가용성 구축을 Cisco Security Cloud와 통합하기 위한 지침에 대해 설명합니다.

- Threat Defense 고가용성 또는 클러스터 구축을 Cisco Security Cloud와 통합하려면 모든 피어를 보안 서비스 익스체인지와 통합해야 합니다.
- 보안 서비스 익스체인지 통합을 수행하려면 고가용성 구축의 모든 Threat Defense 디바이스가 인터넷에 연결할 수 있어야 합니다.
- Management Center 고가용성 구축을 Cisco Security Cloud와 통합할 때는 액티브 피어에서 Cisco Security Cloud 통합을 활성화해야 합니다.
- 스탠바이 Management Center 피어를 액티브 역할로 승격하는 경우, 액티브 및 스탠바이 피어 간에 Cisco Security Cloud 통합이 전송됩니다.
- Management Center의 고가용성 구축을 해제하는 경우에도 두 피어는 모두 Cisco Security Cloud와 통합된 상태로 유지됩니다.

고가용성 구축 구성 및 관리에 관한 자세한 내용은 Cisco Secure Firewall Management Center 관리 가이드의 고가용성 섹션을 참조하십시오.

이벤트를 **Cisco Security Cloud**에 직접 전송하고 **Cisco XDR**와 통합하는 방법

	수행해야 할 작업	추가 정보
1단계	다음을 결정합니다. • 클라우드로 전송하려는 이벤트 유형. • 이벤트를 전송하는 방법. • 이벤트 전송에 사용할 지역 클라우드.	Secure Firewall Threat Defense 및Cisco XDR 통합에 관한 정보, 1 페이지를 참조하십시오.
2단계	직접 통합 요구사항을 충족합니다.	직접 통합 요구사항, 9 페이지의 내용을 참조하십시오.
3단계	Cisco XDR 통합을 위해 디바이스를 관리하고 이벤트를 필터링하는 데 사용할 클라우드 포털인 보안 서비스 익스체인지에 액세스합니다.	보안 서비스 익스체인지 액세스, 25 페이지를 참조하십시오.
4단계	보안 서비스 익스체인지에서 이벤팅 서비스를 활성화합니다.	**Cloud Services(**클라우드 서비스**)**를 클릭하고 다음 옵션을 활성화합니다. • **Cisco SecureX Threat Response** 또는 **Cisco XDR** • 이벤트
5단계	CDO를 사용하여 Threat Defense 디바이스에서 구성을 관리하거나 Cisco Security Cloud에 디바이스를 등록하는 경우, CDO 계정을 이 통합에 사용할 보안 서비스 익스체인지 계정과 병합합니다.	Link Your Cisco Defense Orchestrator 및 보안 서비스 익스체인지 계정 연결, 15 페이지의 내용을 참조하십시오.
6단계	스마트 라이선싱 어카운트를 사용하여 Cisco Security Cloud에 디바이스를 등록하는 경우, 이 통합에 사용할 보안 서비스 익스체인지 계정과 스마트 라이선싱 어카운트를 연결합니다.	스마트 라이선스 어카운트를 보안 서비스 익스체인지에 연결, 17 페이지의 내용을 참조하십시오.

	수행해야 할 작업	추가 정보
7단계	방화벽 관리자에서 Cisco Security Cloud와의 통합을 활성화합니다.	• device manager에서 관리하는 디바이스에 대해서는 이벤트를 직접 전송하도록 Device Manager 구성, 17 페이지의 내용을 참조하십시오. • Management Center에서 관리하는 디바이스에 대해서는 이벤트를 직접 전송하도록 Management Center 구성, 18 페이지의 내용을 참조하십시오.
8단계	보안 서비스 익스체인지에서 중요한 이벤트를 자동으로 승격하도록 시스템을 구성합니다.	중요 이벤트 승격을 자동화하지 않는 경우 보안 서비스 익스체인지에서 이벤트를 보려면 수동으로 검토하고 승격해야 할 수 있습니다. 자세한 내용은 보안 서비스 익스체인지 온라인 도움말의 인시던트에 이벤트 승격 정보를 참조하십시오.
9단계	(선택 사항) 보안 서비스 익스체인지에서 중요하지 않은 특정 이벤트의 자동 삭제를 구성합니다.	자세한 내용은 보안 서비스 익스체인지 온라인 도움말의 이벤트를 참조하십시오.
10단계	통합이 올바르게 설정되었는지 확인합니다. 필요하다면 문제를 해결합니다.	참조: • 직접 연결을 사용하여 이벤트가 보안 서비스 익스체인지에 도달하는지 확인, 26 페이지 • 직접 통합 문제 해결, 26 페이지
11단계	Cisco XDR에서 승격한 이벤트가 인시던트 관리자에 예상대로 표시되는지 확인합니다.	자세한 지침은 Cisco XDR 도움말 센터를 참조하십시오.

Link Your Cisco Defense Orchestrator 및 보안 서비스 익스체인지 계정 연결

CDO 계정을 사용하여 Threat Defense 디바이스를 Cisco Security Cloud에 등록하고 이벤트를 보안 서비스 익스체인지로 전송하려는 경우, CDO 계정을 보안 서비스 익스체인지 계정과 연결해야 합니다.

하나의 CDO 계정만 하나의 보안 서비스 익스체인지 계정과 연결할 수 있습니다. 둘 이상의 지역 클라우드에 테넌트 계정이 있는 경우 각 지역 클라우드에 대해 별도로 테넌트 계정을 연결해야 합니다.

참고 이 작업은 되돌릴 수 없습니다.

시작하기 전에

- Cisco Security Cloud 로그인 계정을 사용하여 CDO 및 해당 지역 클라우드에 로그인할 수 있어야 합니다.
- CDO 계정에는 관리자 또는 슈퍼 관리자 권한이 있어야 합니다.
- 보안 서비스 익스체인지 계정에 관리자 권한이 있어야 합니다.

프로시저

단계 **1** 보안 서비스 익스체인지와 연결할 테넌트가 포함된 CDO 계정에 로그인합니다.

단계 **2** 보안 서비스 익스체인지와 연결할 테넌트를 선택합니다.

단계 **3** 계정에 대한 새 API 토큰을 생성합니다.

a) 창의 오른쪽 상단에 있는 사용자 메뉴에서 **Settings(**설정**)**를 선택합니다.

b) **My Tokens(**내 토큰**)** 섹션에서 **Generate API Token(API** 토큰 생성**)** 또는 **Refresh(**새로 고침**)**를 클릭합니다.

c) 토큰을 복사합니다.

API 토큰에 대한 자세한 내용은 API 토큰을 참조하십시오.

단계 **4** 보안 서비스 익스체인지에서 오른쪽 상단의 **Tools(**툴**)**( ) 아이콘을 클릭하고 **Link Cisco Defense Orchestrator Account(Cisco Defense Orchestrator** 계정 연결**)**를 선택합니다.

단계 **5** CDO에서 복사한 토큰을 붙여 넣습니다.

단계 **6** 연결하려는 테넌트를 연결하고 있는지 확인합니다.

단계 **7** **Link Cisco Defense Orchestrator Account(Cisco Defense Orchestrator** 계정 연결**)**을 클릭합니다.

단계 **8** CDO 계정에서 로그아웃했다가 다시 로그인합니다.

다음에 수행할 작업

- 테넌트 연결 전에 디바이스에서 생성된 이벤트는 테넌트 연결 후 동일한 디바이스에서 생성한 이벤트와 다른 디바이스 ID를 갖습니다.
- 이벤트를 생성한 디바이스에 이벤트를 매핑할 필요가 없는 경우 이제 연결된 테넌트와 연결된 디바이스에 대해 "등록되지 않음" 디바이스 항목을 삭제할 수 있습니다.

스마트 라이선스 어카운트를 보안 서비스 익스체인지에 연결

서로 다른 스마트 라이선싱 어카운트에 등록된 제품을 클라우드의 단일 보기에 통합하려면 해당 스마트 라이선싱 어카운트를 보안 서비스 익스체인지 테넌트에 연결해야 합니다.

시작하기 전에

스마트 라이선싱 어카운트를 연결하려면 이 통합에 사용 중인 모든 스마트 라이선싱 어카운트 및 보안 서비스 익스체인지 테넌트에 대해 관리자 레벨 권한이 있어야 합니다.

프로시저

단계 **1** 보안 서비스 익스체인지의 아무 페이지 오른쪽 상단에서 **Tools(**도구**)** 버튼()을 클릭하고 **Link Smart/Virtual Accounts(**스마트/가상 어카운트 연결**)**를 선택합니다.

단계 **2** **Link more account(**추가 계정 연결**)**를 클릭합니다.

단계 **3** 이 클라우드 계정과 통합할 계정을 선택합니다.

단계 **4** **Link Smart/Virtual Accounts(**스마트/가상 어카운트 연결**)**를 클릭합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

이벤트를 직접 전송하도록 **Device Manager** 구성

참고 사용 가능한 옵션은 **device manager** 버전에 따라 다릅니다. 사용 중인 버전에 해당하지 않는 단계는 건너 뜁니다. 예를 들어 지역 및 이벤트 유형을 선택하는 기능은 버전에 따라 다릅니다.

시작하기 전에

- 이 절차를 계속 진행하기 전에 클라우드 서비스에 디바이스를 등록하십시오. 자세한 내용은 Cisco Secure Firewall Device Manager 구성 가이드의 클라우드 서비스 구성 섹션을 참조하십시오.
- 클라우드 서비스에 디바이스를 등록하는 데 CDO를 사용하는 경우, CDO 계정을 보안 서비스 익스체인지 테넌트와 연결합니다. 자세한 내용은 Link Your Cisco Defense Orchestrator 및 보안 서비스 익스체인지 계정 연결, 15 페이지를 참고하십시오.
- 스마트 라이선스를 사용하여 클라우드 서비스에 디바이스를 등록하는 경우, 스마트 라이선싱 어카운트를 보안 서비스 익스체인지 테넌트에 연결합니다. 자세한 내용은 스마트 라이선스 어카운트를 보안 서비스 익스체인지에 연결, 17 페이지을 참조하십시오.
- device manager에서 다음을 수행합니다.
  - 디바이스의 이름이 고유한지 확인합니다. 그렇지 않은 경우 **Devices(**디바이스**)** > **System Settings(**시스템 설정**)** > **Hostname(**호스트 이름**)**을 클릭하고 이름을 할당합니다.

- Threat Defense 디바이스가 이벤트를 성공적으로 생성하고 있는지 확인합니다.
- Cisco Security Cloud Sign On 인증서가 있는지 확인하고 계정이 생성된 지역 클라우드에 로그인할 수 있는지 확인합니다.

프로시저

단계 **1** device manager에서 **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)** 링크를 클릭합니다.

단계 **2** **Cisco Cloud**로 이벤트 전송 옵션에 대해 **Enable(**활성화**)**를 클릭합니다.

단계 **3** 클라우드로 전송할 이벤트 유형을 선택하고 **OK(**확인**)**를 클릭합니다. 나중에 선택한 이벤트 목록 옆에 있는 **Edit(**편집**)**를 클릭하여 이벤트 선택 사항을 변경할 수 있습니다.

연결 이벤트를 전송하도록 선택하면 이 통합에서 보안 관련 연결 이벤트만 사용됩니다.

단계 **4** 디바이스가 보안 서비스 익스체인지에 등록되었는지 확인합니다.

a) 브라우저 창에서 device manager이(가) 열리지 않는다면 보안 서비스 익스체인지 액세스, 25 페이지의 내용을 참조하십시오.

b) 보안 서비스 익스체인지에서 **Devices(**디바이스**)**를 클릭합니다.

c) Threat Defense 디바이스가 목록에 나타나는지 확인합니다.

참고

Devices(디바이스**)** 목록에서 Threat Defense 디바이스에 대해 표시되는 설명은 일련번호로, 디바이스의 커맨드라인 인터페이스에서 **show running-config** 명령을 실행하는 표시되는 일련번호와 같습니다.

이벤트를 직접 전송하도록 **Management Center** 구성

방화벽 이벤트를 클라우드로 전송하면 외부 툴을 사용하여 방화벽 인시던트를 조사할 수 있습니다. 디바이스는 방화벽 이벤트를 보안 서비스 익스체인지에 전송하며, 여기서 다양한 클라우드 서비스로 전달하여 가시성을 통합하고 위협 조사를 개선할 수 있습니다.

디바이스가 Cisco Security Cloud에 방화벽 이벤트를 전송하도록 허용하려면 Management Center를 스마트 라이선스(시스템(⚙) > 스마트 라이선스)에 등록하거나 **SecureX** 통합 또는 **Cisco Security Cloud** 통합을 활성화하여 Cisco Security Cloud와 통합해야 합니다. Cisco Security Cloud과 통합하면 Management Center를 CDO 계정과 연결하고 Secure Firewall 구축을 Cisco Cloud 테넌시에 온보딩하여 Cisco의 통합 보안 클라우드 서비스에 연결하도록 합니다.

참고 **SecureX** 통합 또는 **Cisco Security Cloud** 통합을 활성화하여 Cisco Security Cloud를 Management Center와 통합하려면 Management Center가 버전 7.0.2와 7.0.x, 또는 버전 7.2 이상이어야 합니다.

Management Center과 Cisco Security Cloud의 통합에 대한 자세한 내용은 Cisco Security Cloud를 사용하여 Management Center 활성화, 19 페이지의 내용을 참조하십시오.

Cisco Security Cloud를 사용하여 Management Center 활성화

이 절차를 사용하여 Management Center와 Cisco Security Cloud를 통합합니다. Cisco Security Cloud 통합을 활성화하면 관리 센터가 Cisco 클라우드 테넌시에 등록됩니다. 이를 통해 방화벽 이벤트를 Cisco Cloud로 전송할 수 있고 다양한 클라우드 서비스(예: Cisco XDR)를 사용하여 이벤트를 보고 분석할 수 있습니다.

시작하기 전에

- CDO는 ID 공급자로 Cisco Security Cloud Sign On을 사용하고 다단계 인증에는 Duo를 사용합니다. Cisco Security Cloud Sign On 자격 증명이 있고 어카운트를 생성한 Cisco 지역 클라우드에 로그인할 수 있는지 확인합니다. 지역 클라우드 URL은 지역 클라우드, 2 페이지의 내용을 참조하십시오.
- CDO 테넌트는 Management Center를 Cisco Security Cloud와 통합해야 합니다. 아직 CDO 테넌트가 없는 경우 테넌트를 요청합니다. 자세한 내용은 CDO 테넌트 요청을 참조하십시오.
- Management Center 온보딩에 사용하려는 CDO 테넌트를 보안 서비스 익스체인지 어카운트에 연결합니다. 자세한 내용은 CDO와 SecureX 또는 Cisco XDR 테넌트 어카운트 연결을 참조하십시오.
- 글로벌 도메인에서 구성을 수정해야 합니다.
- **Cisco SecureX Threat Response** 또는 **Cisco XDR** 및 **Eventing** 서비스가 보안 서비스 익스체인지에서 활성화되었는지 확인합니다. > **Cloud Services(**클라우드 서비스**)**에서 이 설정을 확인합니다.
- 이 절차를 수행하려면 Management Center가 버전 7.0.2~7.0.x 또는 버전 7.2 이상이어야 합니다.

프로시저

단계 **1** Management Center의 버전에 따라:

- Management Center가 7.0.2 및 7.0.x 버전 또는 7.2.0~7.4.x 버전인 경우 **Integration(**통합**)** > **SecureX**를 클릭합니다.
- Management Center 버전 이 7.6.0 이상인 경우 **Integration(**통합**)** > **Cisco Security Cloud**를 클릭합니다.

단계 **2** (선택 사항) **Current Region(**현재 지역**)** 드롭다운 목록에서 Cisco 지역 클라우드를 선택합니다.

참고

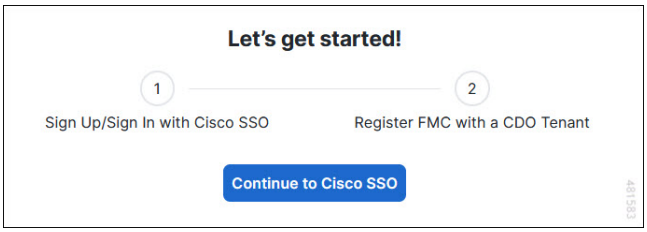
- 여기서 선택한 지역 클라우드는 Cisco Success Network 및 Cisco Support Diagnostics 기능에도 사용됩니다. 이 설정은 Security Analytics and Logging(SaaS)를 사용하는 Secure Network Analytics 클라우드의 클라우드 영역에도 적용됩니다.
- 이미 스마트 라이선스로 Management Center을 등록한 경우 기본적으로 선택한 지역이 스마트 라이선스 지역에 해당합니다. 이러한 시나리오에서는 지역을 변경할 필요가 없습니다.

단계 **3** 7.0.2~7.0.x 버전 또는 7.2.0~7.4.x 버전의 Management Center 버전에 대해 **Enable SecureX(SecureX** 활성화**)**를 클릭합니다. Management Center 버전 7.6.0 이상에 대해 **Enable Cisco Security Cloud(Cisco Security Cloud** 활성화**)**를 클릭합니다.

CDO 어카운트에 로그인할 수 있는 별도의 브라우저 탭이 열립니다. 이 페이지가 팝업 차단기로 차단되지 않았는지 확인하십시오.

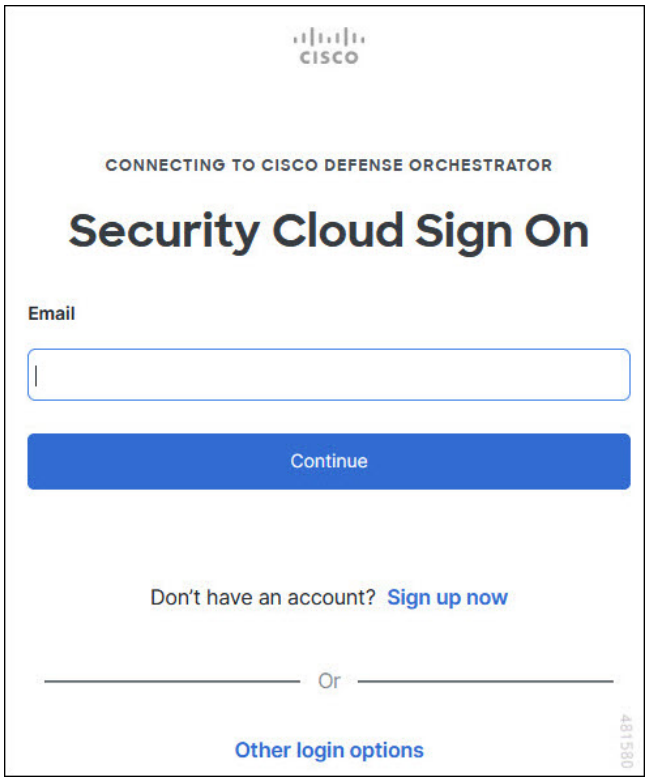
단계 **4** **Continue to Cisco SSO(Cisco SSO**로 계속 진행**)**을 클릭합니다.

그림 ***1: Cisco Security Cloud*** 시작 페이지



단계 **5** CDO 어카운트에 로그인합니다.

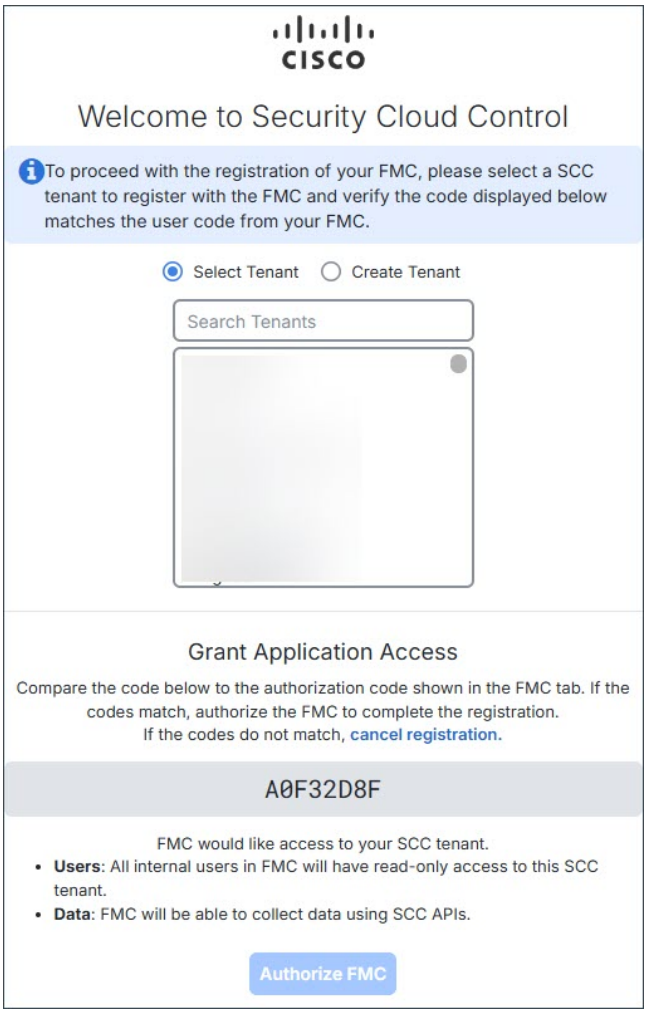
그림 *2: Cisco Security Cloud Sign On*



CDO에 로그인할 Security Cloud 로그인 계정이 없고 계정을 생성하려면 **Security Cloud** 로그인 페이지에서 **Sign up now(**지금 가입**)**을 클릭합니다. 새 Cisco Secure Cloud Sign-On 계정 생성을 참조하십시오.

단계 **6** 이 통합에 사용할 CDO 테넌트를 선택합니다. Management Center 및 매니지드 디바이스는 여기에서 선택한 CDO 테넌트에 온보딩됩니다.

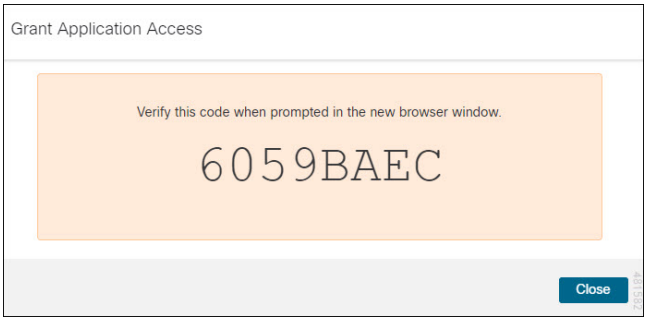
그림 *3: CDO* 테넌트 선택



아직 CDO 테넌트가 없거나 이 통합에 새 테넌트를 사용하려는 경우 새 테넌트를 생성합니다. 자세한 내용은 CDO 테넌트 요청을 참조하십시오.

단계 **7** CDO 로그인 페이지에 표시된 코드가 Management Center에서 제공한 코드와 일치하는지 확인합니다.

그림 *4: Management Center*에서 확인 코드



단계 **8** **Authorize FMC(FMC** 권한 부여**)**를 클릭합니다.

단계 **9** Management Center UI에서 구성을 저장하려면 **Save(**저장**)**를 클릭합니다.

Notifications(알림**)** > **Tasks(**작업**)**에서 작업 진행 상황을 볼 수 있습니다.

등록 작업을 완료하는 데 최대 90초가 소요될 수 있습니다. 등록 작업이 진행되는 동안 Management Center를 사용해야 하는 경우 새 창에서 Management Center를 엽니다.

클라우드로 이벤트 전송 활성화

매니지드 디바이스가 이벤트를 직접 Cisco Security Cloud에 전송하도록 Management Center을 구성합니다. 이 페이지에서 구성하는 클라우드 지역 및 이벤트 유형은 적용 가능하고 활성화된 경우 여러 통합에 사용할 수 있습니다.

시작하기 전에

- Management Center에서 다음을 수행합니다.
  - **System(**시스템**)** > **Configuration(**구성**)** 페이지로 이동하여 클라우드의 디바이스 목록에서 명확하게 식별할 수 있도록 Management Center에 고유한 이름을 지정합니다.
  - Management Center에 Threat Defense 디바이스를 추가하고, 디바이스에 라이선스를 할당하고, 시스템이 올바르게 작동하는지 확인합니다. 필요한 정책을 생성했는지, 생성된 이벤트가 **Analysis(**분석**)** 메뉴의 Management Center UI에 예상대로 표시되는지 확인합니다.
  - Management Center를 스마트 라이선스에 등록하거나 Cisco Security Cloud 통합을 활성화합니다.
- 방화벽 이벤트 전송에 사용할 Cisco 지역 클라우드를 결정합니다. 자세한 내용은 지역 클라우드 선택 지침 및 제한 사항, 3 페이지를 참고하십시오.
- Cisco Security Cloud 통합을 사용하여 클라우드 서비스에 디바이스를 등록하는 경우 CDO 계정을 보안 서비스 익스체인지 테넌트와 연결해야 합니다. 자세한 내용은 Link Your Cisco Defense Orchestrator 및 보안 서비스 익스체인지 계정 연결, 15 페이지를 참고하십시오.

중요 이미 SecureX 구독을 사용하여 Cisco Security Cloud로 이벤트를 전송하고 있었다면 계속해서 Cisco XDR로 이벤트를 전송할 수 있습니다. 하지만 이제 CDO 계정을 사용하여 클라우드 테넌시에 Management Center를 등록하는 경우 CDO 계정에 Cisco XDR로 이벤트를 전달할 수 있는 Security Analytics and Logging 라이선스가 있어야 합니다.

- 스마트 라이선스를 사용하여 클라우드 서비스에 디바이스를 등록하는 경우, 스마트 라이선싱 어카운트를 보안 서비스 익스체인지 테넌트에 연결해야 합니다. 자세한 내용은 스마트 라이선스 어카운트를 보안 서비스 익스체인지에 연결, 17 페이지를 참고하십시오.

- Cisco Security Cloud Sign On 인증서가 있는지 확인하고 계정이 생성된 지역 클라우드에 로그인할 수 있는지 확인합니다.
- 스마트 어카운트 또는 CDO 테넌트를 보안 서비스 익스체인지 계정에 연결했는지 확인합니다.
- 현재 시스템 로그를 사용하여 클라우드로 이벤트를 전송하는 경우 중복을 방지하기 위해 이 기능을 비활성화합니다.

프로시저

단계 **1** Management Center의 버전에 따라:

- Management Center가 7.0.2 및 7.0.x 버전 또는 7.2.0~7.4.x 버전인 경우 **Integration(통합)** > **SecureX**를 클릭합니다.
- Management Center 버전 이 7.6.0 이상인 경우 **Integration(통합)** > **Cisco Security Cloud**를 클릭합니다.

단계 **2** (선택 사항) **Current Region(현재 지역)** 드롭다운 목록에서 지역 클라우드를 선택합니다.

단계 **3** **Send events to the cloud(이벤트를 클라우드로 전송)** 체크 박스를 선택합니다.

단계 **4** 클라우드로 보낼 이벤트 유형을 선택합니다.

참고
클라우드로 보내는 이벤트는 다음 표에 표시된 것처럼 여러 통합에 사용할 수 있습니다.

통합	지원되는 이벤트 옵션	참고
Security Analytics and Logging(SaaS)	모두	높은 우선순위 연결 이벤트는 다음과 같습니다. • 보안 관련 연결 이벤트. • 파일 및 악성코드 이벤트와 관련된 연결 이벤트. • 침입 이벤트와 관련된 연결 이벤트.
Cisco XDR	버전에 따라 다름: • 보안 관련 연결 이벤트. • 침입 이벤트. • 파일 및 악성코드 이벤트.	모든 연결 이벤트를 보내더라도 Cisco XDR는 보안 관련 연결 이벤트만 지원합니다. 참고 Cisco XDR는 별도 라이선스 제품입니다. Cisco Secure Firewall 제품에 필요한 라이선스 외에 추가 구독이 필요합니다. 자세한 정보는 Cisco XDR 라이선스를 참고하십시오.

참고

- **Intrusion Events(**침입 이벤트**)**를 활성화하면 Management Center 디바이스는 영향 플래그와 함께 이벤트를 전송합니다.
- **File and Malware Events(**파일 및 악성코드 이벤트**)**를 활성화하면 Threat Defense 디바이스에서 전송된 이벤트 외에도 Management Center은 소급 이벤트를 전송합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

Cisco XDR 자동화를 사용하여 위협 분석 및 대응

이 설정을 활성화하면 Cisco XDR 사용자가 생성한 자동화된 워크플로우가 Management Center 리소스와 상호 작용할 수 있습니다.

Cisco XDR 자동화는 자동화된 워크플로를 구축하기 위한 코드가 필요 없는 접근 방식을 제공하며, 다양한 일정 및 이벤트에 응답하여 실행되도록 설정할 수 있습니다. Cisco XDR 자동화는 데이터 수집 및 인시던트 생성을 자동화하는 데 도움이 됩니다. 모든 관련 제어 지점에서 자동화와 가이드형 대응 권장 사항을 사용하여 위협을 해소할 수 있습니다.

Cisco XDR 자동화 기능에 대한 자세한 내용은 Cisco XDR 설명서를 참조하십시오.

프로시저

단계 **1** **Integration(**통합**)** > **Cisco Security Cloud**를 클릭합니다.

단계 **2** **Enable Cisco XDR Automation** 체크 박스를 선택합니다.

단계 **3** Cisco XDR 자동화 워크플로우에 할당할 Management Center 사용자 역할을 선택합니다.

Access Admin(액세스 관리자**)** 역할이 기본값으로 설정되어 있어 **Policies(**정책**)** 메뉴에서 액세스 제어 정책 및 관련 기능에 액세스할 수 있습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

보안 서비스 익스체인지 액세스

시작하기 전에

브라우저에서 팝업 차단을 비활성화합니다.

프로시저

단계 **1** 브라우저 창에서 URL https://admin.sse.itd.cisco.com을 사용하여 보안 서비스 익스체인지 관리 포털로 이동합니다.

단계 **2** Cisco 보안 클라우드 로그인 Secure Endpoint , Secure Malware Analytics 또는 Cisco Security 계정 관련 자격 증명을 사용하여 로그인합니다.

계정 자격 증명은 지역 클라우드마다 다릅니다.

직접 연결을 사용하여 이벤트가 보안 서비스 익스체인지에 도달하는지 확인

시작하기 전에

예상한 이벤트가 디바이스에 정상적으로 표시되는지 확인합니다.

프로시저

단계 **1** 보안 서비스 익스체인지 계정에 로그인합니다. 자세한 내용은 보안 서비스 익스체인지 액세스, 25 페이지를 참고하십시오.

단계 **2** 보안 서비스 익스체인지에서 **Events(**이벤트**)**를 클릭합니다.

단계 **3** 디바이스에서 이벤트를 찾습니다.

예상한 이벤트가 표시되지 않을 경우 직접 통합 문제 해결, 26 페이지의 내용을 참조하십시오.

직접 통합 문제 해결

클라우드에 액세스하는 데 문제가 있습니다.

- 클라우드 계정을 활성화한 직후 이 통합 구성을 시도했는데 통합 구현에서 문제가 발생했다면, 1~2시간 기다린 다음 클라우드 계정에 로그인하십시오.
- 계정에 연결된 지역 클라우드의 URL에 액세스하는지 확인합니다.

Management Center에서 관리하는 디바이스가 보안 서비스 익스체인지 디바이스 페이지에 올바르게 나열되지 않음

(6.4.0.4 이전 릴리스) 수동으로 디바이스에 고유한 이름을 지정합니다. Devices(디바이스) 목록에서 각 행에 대한 **Edit(**편집**)** 아이콘을 클릭합니다. 추천: 설명에 있는 IP 주소를 복사하십시오.

이 변경사항은 Devices(디바이스) 목록에서만 유효합니다. 구축의 다른 곳에서는 표시되지 않습니다.

(6.4.0.4 ~ 6.6 릴리스) 디바이스 이름은 Management Center에서 보안 서비스 익스체인지로 처음 등록될 때만 보안 서비스 익스체인지으로 전송되며, Management Center에서 디바이스 이름이 변경되면 보안 서비스 익스체인지에서 업데이트되지 않습니다.

예상 이벤트가 이벤트 목록에 없습니다.

- 올바른 지역 클라우드 및 계정을 확인하십시오.
- 디바이스가 클라우드에 도달할 수 있고 방화벽을 통과하는 모든 필수 주소로의 트래픽을 허용했는지 확인합니다.
- **Events(**이벤트**)** 페이지에서 **Refresh(**새로고침**)** 버튼을 눌러 목록을 새로 고치고 예상되는 이벤트가 나타나는지 확인합니다.
- 보안 서비스 익스체인지의 **Cloud Services(**클라우드 서비스**)** 페이지에 있는 **Eventing(**이벤팅**)** 설정에서 자동 삭제(필터링을 통한 이벤트 제거) 구성을 확인합니다.
- 자세한 문제 해결 팁은 보안 서비스 익스체인지의 온라인 도움말에서 확인할 수 있습니다.

일부 이벤트가 누락되었음

- 모든 연결 이벤트를 클라우드로 전송하는 경우 Cisco XDR는 보안 연결 이벤트만 사용합니다.
- 전역 차단 또는 허용 목록 및 Threat Intelligence Director을 포함하여 Management Center에서 맞춤형 보안 인텔리전스 개체를 사용하는 경우 해당 개체를 사용하여 처리되는 이벤트를 자동으로 승격하도록 보안 서비스 익스체인지를 구성해야 합니다. 자세한 내용은 보안 서비스 익스체인지 온라인 도움말을 참고하십시오.

Cisco Security Cloud 구성을 저장하지 못했습니다.

Management Center 페이지에서 Cisco Security Cloud 설정을 저장하지 못한 경우

- Management Center이 클라우드에 연결되어 있는지 확인합니다.
- 글로벌 도메인에서 Cisco Security Cloud 구성을 수정해야 합니다.

시간 초과로 인해 **Cisco Security Cloud** 통합 실패

구성을 시작한 후 Management Center 페이지가 시간이 초과되기 전에 권한 부여 수신을 위해 15분 동안 대기합니다. 15분 내에 권한 부여를 완료해야 합니다. **Enable Cisco Security Cloud(Cisco Security Cloud** 활성화**)**를 클릭하여 시간 초과 후 새 권한 부여 요청을 시작합니다.

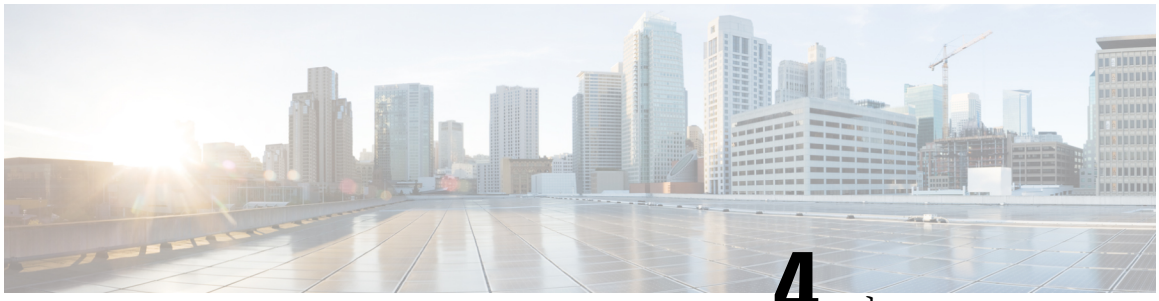
CDO 어카운트를 사용하여 방화벽 디바이스를 보안 서비스 익스체인지에 등록하지 못했습니다.

Management Center가 CDO 어카운트를 사용해 보안 서비스 익스체인지에 매니지드 디바이스를 등록하지 못하면 **Notification(**알림**)** > **Tasks(**작업**)** 아래에 메시지가 나타납니다. Management Center는 원래 구성을 복원합니다. 디바이스 등록에 실패하는 경우 다음을 확인합니다.

- CDO 계정에 관리자 권한이 있습니다.

- Management Center가 보안 서비스 익스체인지에 연결되어 있습니다.

방화벽 디바이스를 보안 서비스 익스체인지에 다시 등록하려면 Cisco Security Cloud 구성을 비활성화했다가 활성화합니다.



4 장

시스템 로그를 사용하여 클라우드로 이벤트 전송

시스템 로그를 통한 통합 관련 정보

Threat Defense 릴리스 6.3부터는 시스템 로그를 사용하여, 지원되는 이벤트를 디바이스에서 Cisco Cloud로 전송할 수 있습니다. 온프레미스 Cisco Security Services Proxy(CSSP) 서버를 설정하고 시스템 로그 메시지가 이 프록시로 전송되도록 디바이스를 구성할 수 있습니다.

프록시는 10분마다 수집된 이벤트를 보안 서비스 익스체인지에 전달합니다. 여기서 이벤트는 Cisco XDR를 비롯한 다양한 Cisco Security Cloud 서비스로 승격되어 이벤트 분석 및 조사를 개선할 수 있습니다.

시스템 로그를 이용한 통합 요구사항

요구 사항 유형	요건
Threat Defense 디바이스 버전	6.3 이상
사용할 지역 클라우드의 계정	Cisco XDR 통합을 활성화하는 데 필요한 계정, 5 페이지의 내용을 참조하십시오.

요구 사항 유형	요건
라이선싱	• Cisco Cloud에 전송할 이벤트를 생성하려면 Secure Firewall 구축에 라이선스가 있어야 합니다. 자세한 내용은 라이선싱 정보를 참조하십시오. • 이 통합은 평가판 라이선스에서는 지원되지 않습니다. • 사용자의 환경에서는 에어갭 환경에 구축할 수 없습니다. • Cisco XDR는 별도 라이선스 제품입니다. Cisco Secure Firewall 제품에 라이선스 외에 추가 구독이 필요합니다. 자세한 정보는 Cisco XDR 라이선스를 참고하십시오.
일반	Threat Defense 디바이스에서 예상대로 이벤트가 생성되고 있습니다.

시스템 로그를 사용하여 **Cisco Security Cloud**로 이벤트를 전송하고 **Cisco XDR**와 통합하는 방법

참고 디바이스에서 이미 Cisco Security Cloud로 이벤트를 전송하고 있는 경우에는 이벤트 전송을 다시 구성할 필요가 없습니다.

단계	수행해야 할 작업	추가 정보
1단계	다음을 결정합니다. • 클라우드로 전송하려는 이벤트 유형. • 이벤트를 전송하는 방법. • 이벤트 전송에 사용할 지역 클라우드.	Secure Firewall Threat Defense 및Cisco XDR 통합에 관한 정보, 1 페이지를 참조하십시오.
2단계	시스템 로그 통합에 대한 요구 사항을 충족합니다.	시스템 로그를 이용한 통합 요구사항, 29 페이지의 내용을 참조하십시오.
3단계	Cisco XDR 통합을 위해 디바이스를 관리하고 이벤트를 필터링하는 데 사용할 클라우드 포털인 보안 서비스 익스체인지에 액세스합니다.	보안 서비스 익스체인지 액세스, 25 페이지를 참조하십시오.

단계	수행해야 할 작업	추가 정보
4단계	Cisco Security Services 프록시 서버를 설치하고 구성합니다.	보안 서비스 익스체인지에서 무료 설치 프로그램과 지침을 다운로드합니다. 보안 서비스 익스체인지에서 브라우저 창의 오른쪽 상단 근처에 있는 **Tools(**도구**)** 아이콘에서 **Downloads(**다운로드**)**를 선택합니다.
5단계	보안 서비스 익스체인지에서 기능을 활성화합니다.	**Cloud Services(**클라우드 서비스**)**를 클릭하고 다음 옵션을 활성화합니다. • **Cisco SecureX Threat Response** 또는 **Cisco XDR** • 이벤트
6단계	지원되는 이벤트에 대한 시스템 로그 메시지를 프록시 서버로 전송하도록 디바이스를 구성합니다.	• device manager에서 관리하는 디바이스에 대해서는 Cisco Secure Firewall Device Manager 구성 가이드에서 침입 이벤트를 위한 시스템 로그 구성 섹션을 참조하십시오. • Management Center에서 관리하는 디바이스에 대해서는 Cisco Secure Firewall Management Center 관리 가이드에서 외부 툴을 사용한 이벤트 분석 섹션을 참조하십시오.
7단계	제품에서 메시지가 각 이벤트를 생성한 디바이스를 식별하는지 확인합니다.	• device manager에서 다음을 수행합니다. **Device(**디바이스**) > Hostname(**호스트 이름**)**에서 호스트 이름을 지정합니다. • Management Center에서 다음을 수행합니다. Platform Settings(플랫폼 설정)의 **Syslog Settings(**시스템 로그 설정**)** 탭에서 **Enable Syslog Device ID(**시스템 로그 디바이스 **ID** 활성화**)**를 클릭하고 식별자를 지정합니다.
8단계	보안 서비스 익스체인지에서 중요한 이벤트를 자동으로 승격하도록 시스템을 구성합니다.	중요 이벤트 승격을 자동화하지 않는 경우 Cisco XDR에서 이벤트를 보려면 수동으로 검토하고 승격해야 합니다. 이벤트 승격에 관한 정보는 보안 서비스 익스체인지에서 온라인 도움말의 정보를 참조하십시오. 보안 서비스 익스체인지에 액세스하려면 보안 서비스 익스체인지 액세스, 25 페이지의 내용을 참조하십시오.

단계	수행해야 할 작업	추가 정보
9단계	(선택 사항) 보안 서비스 익스체인지에서 중요하지 않은 특정 이벤트의 자동 삭제를 구성합니다.	이벤트 필터링에 대한 자세한 내용은 보안 서비스 익스체인지 온라인 도움말을 참조하십시오. 보안 서비스 익스체인지에 액세스하려면 보안 서비스 익스체인지 액세스, 25 페이지의 내용을 참조하십시오.
10단계	보안 서비스 익스체인지에 이벤트가 예상대로 표시되는지 확인하고 필요하다면 문제 해결을 진행합니다.	참조: • 보안 서비스 익스체인지시스템 로그를 사용하여 이벤트가 도달하는지 확인, 32 페이지. • 시스템 로그 통합 문제 해결, 33 페이지.

보안 서비스 익스체인지 액세스

시작하기 전에

브라우저에서 팝업 차단을 비활성화합니다.

프로시저

단계 **1** 브라우저 창에서 URL https://admin.sse.itd.cisco.com을 사용하여 보안 서비스 익스체인지 관리 포털로 이동합니다.

단계 **2** Cisco 보안 클라우드 로그인 Secure Endpoint , Secure Malware Analytics 또는 Cisco Security 계정 관련 자격 증명을 사용하여 로그인합니다.

계정 자격 증명은 지역 클라우드마다 다릅니다.

보안 서비스 익스체인지시스템 로그를 사용하여 이벤트가 도달하는지 확인

시작하기 전에

이벤트가 디바이스에 정상적으로 표시되는지 확인합니다.

프로시저

단계 **1** 메시지가 프록시에서 보안 서비스 익스체인지(으)로 포워딩될 수 있도록, 디바이스가 지원되는 이벤트를 탐지한 후 약 15분 동안 기다립니다.

단계 **2** 보안 서비스 익스체인지 계정에 로그인합니다. 자세한 내용은 보안 서비스 익스체인지 액세스, 25 페이지를 참고하십시오.

단계 **3** 보안 서비스 익스체인지에서 **Events(**이벤트**)**를 클릭합니다.

단계 **4** 디바이스에서 이벤트를 찾습니다.

예상한 이벤트가 표시되지 않을 경우 시스템 로그 통합 문제 해결, 33 페이지의 내용을 참조하십시오.

시스템 로그 통합 문제 해결

이벤트가 **Cisco Security Services** 프록시에 도달하지 않습니다**.**

디바이스가 네트워크의 Cisco Security Services에 연결할 수 있는지 확인합니다.

클라우드에 액세스하는 데 문제가 있습니다**.**

- 클라우드 계정을 활성화한 직후 이 통합 구성을 시도했는데 통합 구현에서 문제가 발생했다면, 1~2시간 기다린 다음 클라우드 계정에 로그인하십시오.
- 계정에 연결된 지역 클라우드의 URL에 액세스하는지 확인합니다.

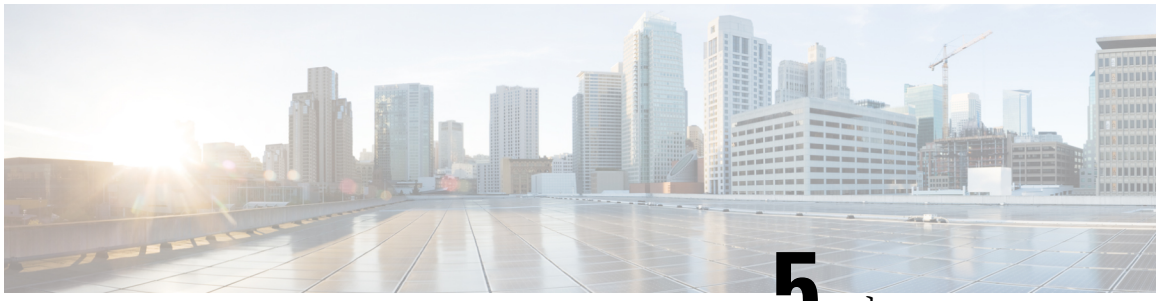
예상 이벤트가 이벤트 목록에 없습니다**.**

다음을 확인합니다.

- 예상한 이벤트가 디바이스에 표시되는지 확인합니다.
- 보안 서비스 익스체인지에서 **Cloud Services(**클라우드 서비스**)** 페이지에 있는 **Eventing(**이벤팅**)** 설정에서 자동 삭제(필터링을 통한 이벤트 제거) 구성을 확인합니다.
- 이벤트를 전송하는 지역 클라우드를 보고 있는지 확인합니다.

시스템 로그 필드 관련 질문

시스템 로그 필드 및 설명에 관한 내용은 Threat Defense 시스템 로그 메시지를 참조하십시오.



5 장

추가 참조 자료

Cisco XDR 사용에 대한 추가 정보

Cisco XDR 사용과 문제 해결에 대한 자세한 내용은 Cisco XDR 도움말 센터를 참조하십시오. Cisco XDR 제품에 대한 자세한 내용은 Cisco XDR 제품 페이지를 참조하십시오.

Cisco XDR FAQ는 자주 묻는 질문을 참조하십시오.

보안 서비스 익스체인지 사용 정보

보안 서비스 익스체인지 또는 Cisco Security Services 프록시 사용에 대한 자세한 내용은

보안 서비스 익스체인지의 온라인 도움말을 참조하십시오.