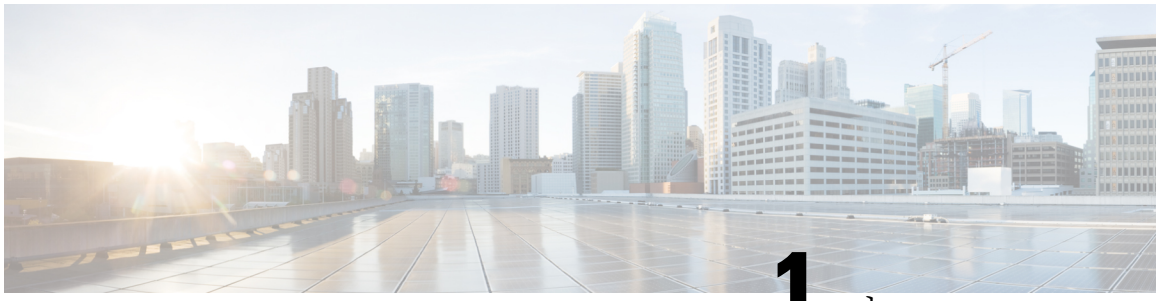
Cisco Firepower 및 SecureX 통합 가이드

초판: 2020년 6월 24일

최종 변경: 2021년 1월 8일

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

Firepower 및 통합에 대한 중요 정보 SecureX

Firepower 정보 및 SecureX

Cisco 보안 제품 구매에 포함된 통합 포털인 SecureX을(를) 통해 모든 Cisco 보안 제품의 데이터를 볼 수 있습니다.

SecureX 는 Cisco의 통합 보안 포트폴리오를 기존 인프라와 연결하여 가시성을 통합하고 자동화를 지원하며 네트워크, 엔드포인트, 클라우드 및 애플리케이션 전반에서 보안을 강화하는 단순화된 플랫폼 환경입니다.

SecureX에 관한 자세한 내용은 https://www.cisco.com/c/en/us/products/security/securex/index.html의 내용을 참조하십시오.

SecureX 포털에서 Firepower 데이터를 보고 작업하려면 이 문서의 지침을 따르십시오.

SecureX 지역 클라우드

지역	클라우드에 연결	지원되는 **Firepower** 통합 방법
북미	https://securex.us.security.cisco.com	• 직접 통합: Firepower 릴리스 6.4 이상 • 시스템 로그를 통한 통합: Firepower 릴리스 6.3 이상

지역	클라우드에 연결	지원되는 Firepower 통합 방법
유럽	https://securex.eu.security.cisco.com	• 직접 통합: Firepower 릴리스 6.5 이상 • 시스템 로그를 통한 통합: Firepower 릴리스 6.3 이상
아시아(APJC)	https://securex.apjc.security.cisco.com	• 직접 통합: Firepower 릴리스 6.5 이상 • 시스템 로그를 통한 통합: Firepower 릴리스 6.3 이상

지역 클라우드 선택 지침 및 제한 사항

지역 클라우드를 선택하기 전에 다음 사항을 고려하십시오.

- Firepower 버전 및 통합 방법(syslog 또는 직접)이 선택에 영향을 미칩니다.

  자세한 내용은 SecureX 지역 클라우드, 1 페이지의 내용을 참조하십시오.

- 가능하다면 Firepower를 구축한 곳에서 가장 가까운 지역 클라우드를 사용하십시오.
- 다른 클라우드에 있는 데이터는 집계하거나 병합할 수 없습니다.
- 여러 지역의 데이터를 집계해야 한다면, 모든 지역의 디바이스는 동일한 지역 클라우드로 데이터를 전송해야 합니다.
- 각 지역별 클라우드에서 계정을 생성할 수 있습니다. 각 클라우드의 데이터는 분리됩니다.
- Firepower 제품에서 선택하는 지역은 Cisco Support Diagnostics 및 Cisco Support Network 기능(적용 가능하며 활성화된 경우)에도 사용됩니다. 자세한 내용은 Firepower 제품의 온라인 도움말을 참조하십시오.
- Firepower 구축이 Cisco Security Analytics and Logging(SaaS) / CDO 및 SecureX/Cisco SecureX Threat Response 모두와 직접 통합되는 경우 이러한 모든 통합은 동일한 지역 클라우드를 사용해야 합니다.

지원되는 이벤트 유형

Firepower 및 SecureX 통합은 다음 이벤트 유형을 지원합니다.

표 *1: Cisco Cloud*로의 이벤트 전송을 위한 *Firepower* 버전 지원

기능	**FMC** 버전에서 관리하는 디바이스 **(**직접 통합**)**	**FDM** 버전에서 관리하는 **FTD** 디바이스 **(**직접 통합**)**	시스템 로그
침입(IPS) 이벤트	6.3 이상(시스템 로그 이용) 6.4 이상(직접 연결 이용)	6.3 이상(시스템 로그 이용) 6.4 이상(직접 연결 이용)	지원
보안 인텔리전스 연결 이벤트	6.5 이상	6.5 이상	지원되지 않음
파일 및 악성코드 이벤트	6.5 이상	6.5 이상	지원되지 않음

이벤트를 클라우드로 전송하는 방법 비교

Firepower 디바이스는 이벤트를 보안 서비스 익스체인지 포털을 통해 SecureX에서 사용할 수 있도록 합니다(시스템 로그나 직접 연결 이용).

직접 전송	프록시를 사용하여 시스템 로그를 통해 전송
지원되는 Firepower 소프트웨어 버전을 실행하는 Firepower Threat Defense(NGFW) 장치만 지원	지원되는 Firepower 소프트웨어 버전을 실행하는 모든 디바이스 지원
Firepower 6.4 이상 지원	Firepower 6.3 이상 지원
지원되는 이벤트 유형, 2 페이지에 나열된 모든 이벤트 유형을 지원합니다.	침입 이벤트만 지원합니다.
Firepower Threat Defense 디바이스는 반드시 인터넷에 연결해야 합니다.	Firepower 디바이스는 인터넷에 연결하지 않아도 됩니다.
Firepower 구축에서는 Smart Software Manager 온프레미스 서버(이전 명칭은 Smart Software Satellite Server)를 사용할 수 없습니다.	구축시 Smart Software Manager 온 프레미스 서버를 사용할 수 있습니다.

직접 전송	프록시를 사용하여 시스템 로그를 통해 전송
사내 프록시 서버를 설정하고 유지 관리하지 않아도 됩니다.	사내 가상 Cisco Security Services Proxy(CSSP) 서버가 필요합니다. 이 프록시 서버에 대 한 자세한 내용은 SSE 보안 서비스 익스체인지(온라인 도움말)에서 확인할 수 있습니다. SSE에 액세스하는 방법은 Access(액세스) 보안 서비스 익스체인지, 26 페이지의 내용을 참조하십시오.

모범 사례

참조하는 절차 항목의 요구 사항(Requirements) 항목 및 시작하기 전에(Before You Begin) 항목을 포함한, 다음 항목에 있는 가이드라인 및 설정 지침을 정확하게 따르십시오.

- 모든 통합의 경우:

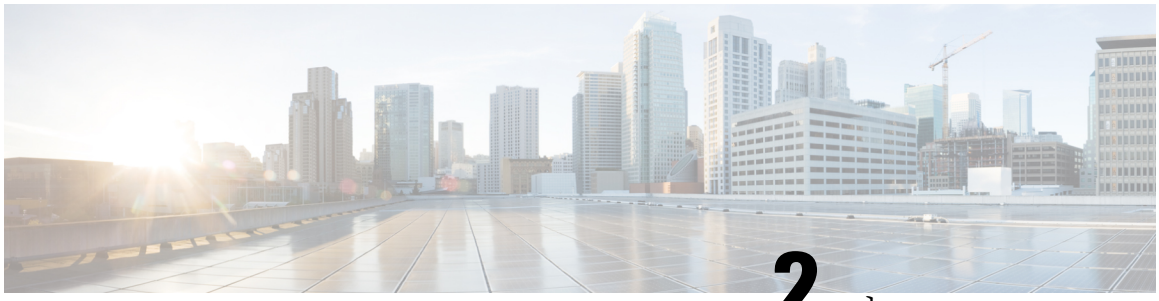
  지역 클라우드 선택 지침 및 제한 사항, 2 페이지의 내용을 참조하십시오.

- 직접 통합:

  Cisco Cloud에 이벤트를 직접 전송하고 SecureX와 통합하는 방법, 11 페이지의 내용을 참조하십시오.

- 시스템 로그를 이용한 통합:

  시스템 로그를 이용해 Cisco Cloud에 이벤트를 전송하는 방법, 24 페이지의 내용을 참조하십시오.



2 장

Cisco Cloud 계정

SecureX 액세스에 필요한 필수 계정

SecureX 및 관련 도구(SSE 포함)를 사용하려면, 사용할 지역 클라우드에서 다음 계정 중 하나가 있어야 합니다.

- Cisco 보안 계정
- AMP for Endpoints 계정
- Cisco Threat Grid 계정
- SecureX 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 액세스할 계정 받기 SecureX, 5 페이지의 내용을 참조하십시오.

액세스할 계정 받기 SecureX

중요 사용자나 사용자의 조직이 대상 지역 클라우드에서 계정을 이미 이용하고 있다면, 기존 계정을 사용하십시오. 새 어카운트를 생성하지 마십시오.

프로시저

단계 **1** 사용할 SecureX 지역 클라우드를 결정합니다.

지역 클라우드 선택 지침 및 제한 사항, 2 페이지의 내용을 참조하십시오.

단계 **2** 사용할 지역 클라우드에 아직 계정이 없다면, 관리자에게 조직이 해당 클라우드에 대해 지원되는 계정이 있는지 물어 보십시오.

지원되는 계정 유형에 대해서는 SecureX 액세스에 필요한 필수 계정, 5 페이지의 내용을 참조하십시오.

단계 **3** 조직 구성원이 해당 지역 클라우드에 대한 계정을 만들었다면,

관련 계정 관리자에게 클라우드 계정에 대한 액세스 관리, 6 페이지의 지침에 따라 사용자 계정을 추가해달라고 요청하십시오.

단계 **4** 아니면 조직의 계정을 새로 만들어야 합니다. (사용자가 계정 관리자가 됩니다).

a) 브라우저에서, 선택한 지역 클라우드로 이동합니다.

링크 관련 사항은 SecureX 지역 클라우드, 1 페이지의 내용을 참조하십시오.

b) **Create an Account(**계정 생성**)**를 클릭합니다.

c) 계정 생성과 관련하여 질문이 있는 경우 https://www.cisco.com/c/en/us/support/security/securex/series.html 페이지에서 링크된 *Cisco SecureX Sign-On* 설명서를 참조하십시오.

클라우드 계정에 대한 액세스 관리

사용자 계정 관리는 보유한 클라우드 계정의 유형에 따라 달라집니다.

참고 Threat Grid 또는 AMP for Endpoints 계정을 사용하여 클라우드에 액세스하는 경우 해당 제품의 설명서를 참조하십시오.

SecureX 계정에 대한 사용자 액세스 관리

조직에서 클라우드에 액세스하기 위해 SecureX 계정을 사용하는 경우 이 절차를 사용하여 사용자를 관리합니다.

시작하기 전에

SecureX 계정에 관리자 레벨 권한이 있어야 합니다.

프로시저

단계 1 SecureX 지역 클라우드에 로그인합니다.

단계 2 **Administration(**관리**)**을 클릭합니다.

단계 3 질문이있는 경우 SecureX의 온라인 도움말을 참조하십시오.

조직의 **Cisco** 보안 계정에 대한 액세스 관리

Cisco 보안 계정 소유자나 관리자라면, 조직의 Cisco 보안 계정에 추가 사용자 액세스를 부여하고 기존 사용자를 관리할 수 있습니다(계정 활성화 이메일 재전송 포함).

프로시저

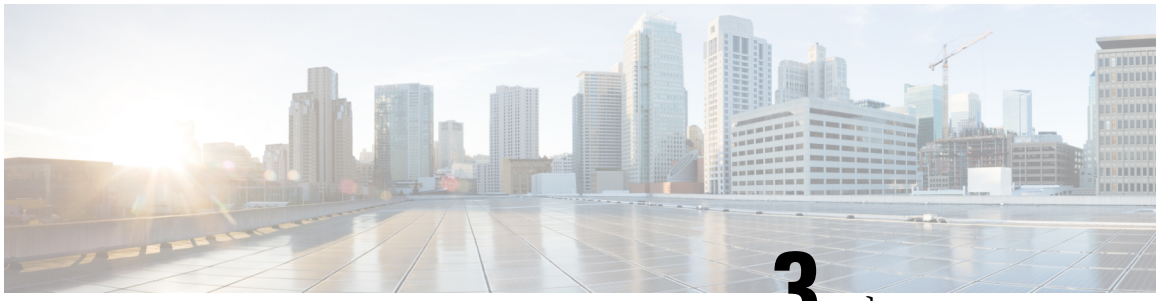
단계 1 지역 클라우드의 해당 URL로 이동합니다.

- 북미: https://castle.amp.cisco.com
- 유럽: https://castle.eu.amp.cisco.com
- 아시아(APJC): https://castle.apjc.cisco.com

단계 2 **Users(**사용자**)**를 클릭합니다.

단계 3 사용자 액세스를 추가하거나 수정합니다.

Account Administrator(계정 관리자**)**를 선택하면 해당 사용자는 사용자 액세르를 부여 및 관리할 수 있게 됩니다.



3 장

클라우드로 이벤트 바로 전송

직접 통합 관련 정보

Firepower 릴리스 6.4부터는 지원되는 이벤트를 Firepower Threat Defense(FTD) 디바이스에서 Cisco Cloud로 바로 전송하도록 Firepower 시스템을 구성할 수 있습니다.

특히 Firepower 디바이스는 이벤트를 보안 서비스 익스체인지(SSE)로 전송하는 데, 여기서는 이벤트를 SecureX에 표시되는 인시던트로 자동 또는 수동으로 승격할 수 있습니다.

직접 통합 요구사항

요구 사항 유형	요건
Firepower 디바이스	Firepower Threat Defense 디바이스 • 관리 주체 Firepower Management Center • Firepower Device Manager에서 관리
Firepower 버전	US 클라우드: 6.4 이상 EU 클라우드: 6.5 이상 APJC 클라우드: 6.5 이상 버전 요구 사항은 디바이스 및 FMC에 모두 적용됩니다(해당되는 경우).

요구 사항 유형	요건
라이선싱	이 통합에는 특별한 라이선스가 필요하지 않습니다. 하지만 다음 경우를 고려하십시오. • SecureX에서 확인하려는 이벤트를 생성하려면 Firepower 시스템에 라이선스가 있어야 합니다. 자세한 내용은 https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-licensing-information-listing.html 섹션을 참조해 주십시오. • 이 기능은 Firepower 평가판 라이선스에서는 지원되지 않습니다. • 사용자의 환경에서는 Cisco Smart Software Manager 온 프레미스 서버(이전 Cisco Smart Software Satellite 서버)를 사용하거나 에어 갭 환경에 구축할 수 없습니다.
계정	직접 통합을 위한 계정 요구 사항, 11 페이지의 내용을 참조하십시오. FDM을 CDO와 함께 사용하는 경우 (FDM에서 관리하는 FTD 전용) CDO 및 SecureX 계정 병합, 14 페이지도 참조하십시오.
연결성	FMC 및 매니지드 디바이스는 다음 주소의 Cisco Cloud로의 아웃바운드 연결을 포트 443에서 지원해야 합니다. • 북미 클라우드: • api-sse.cisco.com • https://eventing-ingest.sse.itd.cisco.com • https://mx01.sse.itd.cisco.com • EU 클라우드(Firepower 6.5 이상): • api-sse.cisco.com • api.eu.sse.itd.cisco.com • https://eventing-ingest.eu.sse.itd.cisco.com • https://mx01.eu.sse.itd.cisco.com • 아시아(APJC) 클라우드(Firepower 6.5 이상): • api.apj.sse.itd.cisco.com • mx01.apj.sse.itd.cisco.com • eventing-ingest.apj.sse.itd.cisco.com
일반	Firepower 시스템이 이벤트를 예상대로 생성하고 있습니다.

직접 통합을 위한 계정 요구 사항

- Firepower 이벤트 데이터를 전송할 지역 클라우드에 대한 계정이 있어야 합니다.

  지원되는 계정 유형에 대해서는 SecureX 액세스에 필요한 필수 계정, 5 페이지의 내용을 참조하십시오.

  사용할 지역 클라우드에서 사용자가 사용자의 조직이 이미 계정을 만들었다면, 새 계정을 만들지 마십시오. 다른 계정의 데이터를 집계하거나 병합할 수 없습니다.

  계정을 얻으려면 액세스할 계정 받기 SecureX, 5 페이지의 내용을 참조하십시오.

  클라우드 계정에는 관리자 레벨 권한이 있어야 합니다.

- 제품을 라이선싱하는 Cisco 스마트 계정에 대한 관리자 권한이 있어야 합니다.

  Smart 계정 관리자 역할을 결정하려면 https://software.cisco.com(으)로 이동해 **Manage Smart Account(**스마트 계정 관리**)**를 클릭하고, 페이지 오른쪽 상단에서 Smart Account(스마트 계정)을 선택하고, **Users(**사용자**)** 탭을 클릭한 다음 사용자 ID를 검색해야 합니다.

- 라이선싱 스마트 계정과 클라우드에 액세스하는 데 사용할 계정은 같은 Cisco CCO 계정에 연결돼 있어야 합니다.

- Firepower 계정에는 다음 사용자 역할 중 하나가 있어야 합니다.
  - Admin(관리자)
  - 액세스 관리자
  - Network Admin(네트워크 관리자)
  - 보안 승인자

Cisco Cloud에 이벤트를 직접 전송하고 SecureX와 통합하는 방법

참고 디바이스가 이미 클라우드에 이벤트를 전송 중인 경우, 다시 전송하도록 구성할 필요가 없습니다. SecureX 및 Cisco SecureX Threat Response (이전에는 Cisco Threat Response)는 동일한 이벤트 데이터 집합을 사용합니다.

	수행해야 할 작업	추가 정보
단계	전송할 이벤트, 해당 이벤트를 전송하는 방법, 사용할 지역 클라우드 등에 대해 결정합니다.	다음 항목을 참조하십시오. Firepower 및 통합에 대한 중요 정보 SecureX, 1 페이지

	수행해야 할 작업	추가 정보
단계	요구 사항	직접 통합 요구사항, 9 페이지 및 하위 항목을 충족합니다.
단계	브라우저에서, 디바이스 및 이벤트 필터링을 관리하는 데 사용할 SecureX용 클라우드 포털인 보안 서비스 익스체인지에 액세스합니다.	Access(액세스) 보안 서비스 익스체인지, 13 페이지의 내용을 참조하십시오.
단계	(FDM 전용) CDO를 사용하여 FTD 디바이스의 설정을 관리하는 경우 CDO 계정을 이 문서에 설명된 서비스에 사용하는 계정과 병합해야 합니다.	(FDM에서 관리하는 FTD 전용) CDO 및 SecureX 계정 병합, 14 페이지의 내용을 참조하십시오.
단계	보안 서비스 익스체인지에서 라이선싱 계정을 연결해, 조직 내 다양한 계정에 등록한 디바이스가 제공하는 이벤트 데이터를 보고 처리할 수 있게 합니다.	Link Smart 라이선스 계정, 16 페이지의 내용을 참조하십시오.
단계	보안 서비스 익스체인지에서 이벤팅 서비스를 활성화합니다.	**Cloud Services(**클라우드 서비스**)**를 클릭하고 다음 옵션을 활성화합니다. • **Cisco SecureX Threat Response** • 이벤트
단계	Firepower 제품에서 Cisco Cloud와의 통합을 활성화합니다.	팁**:** 이 항목에 있는 전제 조건을 건너뛰지 마십시오. • FDM(Firepower Device Manager)에서 관리하는 디바이스에 대해서는 다음을 참조하십시오. Cisco Cloud에 이벤트를 전송하도록 FDM 구성, 16 페이지 • Firepower Management Center(FMC)에서 관리하는 디바이스에 대해서는 다음을 참조하십시오. 디바이스가 이벤트를 Cisco Cloud로 전송하도록 FMC 구성, 18 페이지
단계	Firepower 시스템에서 이벤트를 생성할 때까지 기다립니다.	--

	수행해야 할 작업	추가 정보
단계	통합이 올바르게 설정되었는지 확인합니다. 필요하다면 문제를 해결합니다.	참조: • 이벤트가 (직접 연결을 통해) 보안 서비스 익스체인지에 도달하는지 확인합니다., 19 페이지 • 직접 통합 문제 해결, 20 페이지
단계	보안 서비스 익스체인지에서 중요한 이벤트를 자동으로 승격하도록 시스템을 구성합니다.	중요 이벤트 승격을 자동화하지 않는 경우 SecureX에서 이벤트를 보려면 수동으로 검토하고 승격해야 할 수 있습니다. 이벤트 승격에 관한 정보는 보안 서비스 익스체인지에서 온라인 도움말의 정보를 참조하십시오. SSE에 액세스하는 방법은 Access(액세스) 보안 서비스 익스체인지, 13 페이지의 내용을 참조하십시오.
단계	(선택 사항) 보안 서비스 익스체인지에서 중요하지 않은 특정 이벤트의 자동 삭제를 구성합니다.	이벤트 필터링에 관한 정보는 보안 서비스 익스체인지에서 온라인 도움말의 정보를 참조하십시오. SSE에 액세스하는 방법은 Access(액세스) 보안 서비스 익스체인지, 13 페이지의 내용을 참조하십시오.
단계	SecureX에서 Firepower 모듈을 추가합니다.	SecureX에서 **Integration Modules(**통합 모듈**) > Available Integration Modules(**사용 가능한 통합 모듈**)**로 이동하여 Firepower 모듈을 추가합니다. 이 모듈에 관한 자세한 내용은 SecureX의 온라인 도움말을 참조하십시오.

Access(액세스) 보안 서비스 익스체인지

시작하기 전에

브라우저에서 팝업 차단을 비활성화합니다.

프로시저

단계 **1** 브라우저 창에서 사용자의SecureX 클라우드로 이동합니다.

- 북미 클라우드: https://securex.us.security.cisco.com
- 유럽 클라우드: https://securex.eu.security.cisco.com
- 아시아 클라우드: https://securex.apjc.security.cisco.com

단계 **2** SecureX, AMP for Endpoints, Cisco Threat Grid 또는 Cisco Security 계정 관련 자격 증명을 사용하여 로그인합니다.

계정 자격 증명은 지역 클라우드마다 다릅니다.

단계 **3** 보안 서비스 익스체인지(으)로 이동합니다.

Integrations(통합**) > Devices(**디바이스**) > Manage Devices(**디바이스 관리**)**를 선택합니다.

보안 서비스 익스체인지 가 새 브라우저 창에서 열립니다.

(FDM에서 관리하는 FTD 전용) CDO 및 SecureX 계정 병합

이 작업을 수행해야 할 수도 있고 필요하지 않을 수도 있습니다.

FDM 관리Firepower Threat Defense(FTD) 디바이스를 Cisco Defense Orchestrator(CDO) 또는 Cisco Security Analytics and Logging(SaaS) 및 SecureX 또는 Cisco SecureX Threat Response와 함께 사용할 경우 CDO 계정을 SecureX 또는 Cisco SecureX Threat Response에 대한 디바이스와 연결된 계정과 병합해야 합니다. (이전에는 Cisco SecureX Threat Response가 Cisco Threat Response 또는 CTR로 알려짐)

하나의 CDO 테넌트만 하나의 SecureX/Cisco SecureX Threat Response 계정과 병합할 수 있습니다.

둘 이상의 지역 클라우드에 계정이 있는 경우 각 지역 클라우드에 대해 별도로 계정을 병합해야 합니다.

SecureX 클라우드의 계정을 병합하는 경우 동일한 클라우드의 Cisco SecureX Threat Response에 대해 다시 수행할 필요가 없으며 그 반대도 마찬가지입니다.

이 작업은 되돌릴 수 없습니다.

시작하기 전에

병합해야 하는 계정의 인증서를 사용하여 CDO 및 해당 지역 SecureX 또는 Cisco SecureX Threat Response 클라우드에 로그인할 수 있어야 합니다.

CDO 사용자 계정에는 관리자 또는 슈퍼 관리자 권한이 있어야 합니다.

사용자 SecureX 또는 Cisco SecureX Threat Response 계정에 관리자 권한이 있어야 합니다.

프로시저

단계 **1** 병합할 계정의 인증서를 사용하여 적절한 지역 CDO 사이트에 로그인합니다.

예를 들어 미국 클라우드는 https://defenseorchestrator.com이고 EU 클라우드는 https://defenseorchestrator.eu입니다.

단계 **2** 병합할 테넌트 계정을 선택합니다.

단계 **3** CDO에서 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 CDO의 온라인 도움말을 참조하십시오.
https://docs.defenseorchestrator.com/Configuration_Guides/Devices_and_Services/API_Tokens

단계 **4** 보안 서비스 익스체인지(SSE)를 아직 보고 있지 않은 경우:

a) 병합할 계정을 사용하여 해당 SecureX 지역 클라우드에 로그인합니다.
b) 보안 서비스 익스체인지(으)로 이동합니다.

SecureX에서: **Administration(**관리**) > Devices(**디바이스**) > Manage Devices(**디바이스 관리**)**를 선택합니다.

보안 서비스 익스체인지 가 새 브라우저 창에서 열립니다.

단계 **5** SSE에서 페이지 오른쪽 상단의 > **Link CDO Account(CDO** 계정 연결**)**를 클릭합니다.

단계 **6** CDO에서 복사한 토큰을 붙여 넣습니다.

단계 **7** 연결하려는 계정을 연결하고 있는지 확인합니다.

단계 **8** **Link CDO Accounts(CDO** 계정 연결**)**를 클릭합니다.

다음에 수행할 작업

- 이 절차를 수행해도 계정 인증서는 변경되지 않습니다. 병합 후에는 계정 병합 전에 사용했던 각 제품(CDO, Cisco Security Analytics and Logging(SaaS) , SecureX, CTR 등)에 계속해서 동일한 인증서를 사용합니다.
- SSE에 디바이스를 등록하기 전에 이 절차를 완료한 경우:

  Cisco Cloud에 이벤트를 직접 전송하고 SecureX와 통합하는 방법, 11 페이지에서 단계를 계속 진행합니다.

- CDO 및 SecureX 또는 Cisco SecureX Threat Response 통합을 위해 디바이스를 등록한 후 이 절차를 수행한 경우 SSE의 디바이스 페이지에 디바이스 인스턴스가 중복될 수 있습니다.

  이 경우 이전에 CDO 등록과 연결되었던 디바이스의 인스턴스가 이제 SecureX 또는 Cisco SecureX Threat Response 통합에 사용된 계정과 연결됩니다.

  병합 전에 디바이스에서 생성된 이벤트는 병합 후 동일한 디바이스에서 생성한 이벤트와 다른 디바이스 ID를 갖습니다.

  이벤트를 생성한 디바이스에 이벤트를 매핑할 필요가 없는 경우 이제 병합된 계정과 연결된 디바이스에 대해 "등록되지 않음" 디바이스 항목을 삭제할 수 있습니다.

Link Smart 라이선스 계정

다른 라이선싱 스마트 계정(또는 가상 계정)으로 등록한 제품을 클라우드의 단일 보기로 통합하려면, 관련 라이선싱 계정을 SecureX 및 Cisco SecureX Threat Response에 액세스하는 데 사용할 계정에 연결해야 합니다.

시작하기 전에

- 라이선싱 계정을 연결하려면 모든 라이선싱 계정 및 SecureX 또는 Cisco SecureX Threat Response에 액세스하는 데 사용하는 계정에 대해 관리자 레벨의 스마트 계정 또는 가상 계정 권한이 있어야 합니다. (후자는 Cisco Threat Response 또는 CTR로 알려져 있습니다.)
- 연결된 계정 보기는 사용자 레벨 계정에서도 가능합니다.
- 이미 Cisco SecureX Threat Response에 사용하기 위해 어카운트를 연결한 경우, SecureX에 대해 어카운트를 다시 연결할 필요가 없으며, 그 반대의 경우도 마찬가지입니다.
- 이 절차를 완료하려면 Cisco.com(CCO) 자격 증명이 필요합니다.

프로시저

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

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

단계 **3** 메시지가 나타나면 Cisco.com(CCO) 자격 증명을 사용하여 로그인합니다.

단계 **4** 이 클라우드 계정과 통합할 계정을 선택합니다.

단계 **5** **Link Accounts(**계정 연결**)**를 클릭합니다.

Link Smart 라이선스 계정

현재 연결된 스마트 라이선싱 계정의 연결을 해제해야 하는 경우 보안 서비스 익스체인지(SSE)의 온라인 도움말에 있는 지침을 참조하십시오.

Cisco Cloud에 이벤트를 전송하도록 FDM 구성

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

시작하기 전에

- Cisco Cloud에 이벤트를 직접 전송하고 SecureX와 통합하는 방법, 11 페이지에서 지금까지의 단계를 수행합니다.
- CDO를 사용하는 경우 이 절차를 시작하기 전에 계정을 병합해야 합니다. (FDM에서 관리하는 FTD 전용) CDO 및 SecureX 계정 병합, 14 페이지의 내용을 참조하십시오.
- FDM에서 디바이스의 이름이 고유한지 확인합니다. 그렇지 않다면 **Device(**디바이스**) > System Settings(**시스템 설정**) > Hostname(**호스트 이름**)**에서 고유한 이름을 할당합니다.
- FDM에서 하나 이상의 액세스 제어 규칙에 침입 및 기타 적용 가능한 정책을 적용하고 디바이스가 이벤트를 제대로 생성하는지 확인합니다.
- 클라우드 인증서가 있는지 확인하고 계정이 생성된 SecureX 지역 클라우드에 로그인할 수 있는지 확인합니다.

  URL은 SecureX 지역 클라우드, 1 페이지의 내용을 참조하십시오.
- 브라우저에서 다음을 수행합니다.
  - 팝업 차단 비활성화
  - 타사 쿠키 허용

프로시저

단계 **1** Firepower Device Manager에서 **Device(**디바이스**)**를 클릭하고 **System Settings(**시스템 설정**) > Cloud Services(**클라우드 서비스**)** 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Cloud Services(**클라우드 서비스**)**를 클릭하면 됩니다.

단계 **2** 아직 지역 클라우드를 선택하지 않았다면 지역을 선택합니다.

단계 **3** 클라우드로 전송할 이벤트 유형을 선택합니다.

연결 이벤트를 전송하도록 선택하면 이 통합에서 보안 인텔리전스 연결 이벤트만 사용됩니다. 다른 모든 연결 이벤트는 이 통합에서 사용되지 않습니다.

단계 **4** **Cisco Threat Response** 기능의 제어 **Enable(**활성화**)**을 클릭합니다.

메시지가 표시된다면, 공개된 내용을 읽고 **Accept(**수락**)**를 클릭합니다.

단계 **5** 디바이스가 보안 서비스 익스체인지에 등록되었는지 확인합니다.

a) 브라우저 창에서 보안 서비스 익스체인지이(가) 열리지 않는다면 Access(액세스) 보안 서비스 익스체인지, 13 페이지의 내용을 참조하십시오.
b) 보안 서비스 익스체인지에서 **Devices(**디바이스**)**를 클릭합니다.
c) Firepower Threat Defense 디바이스가 목록에 나타나는지 확인합니다.

참고: 디바이스 목록에서 FTD 디바이스에 대해 표시되는 설명은 일련번호로, 디바이스의 커맨드 라인 인터페이스에서 **show running-config** 명령을 실행하는 표시되는 일련번호와 같습니다.

다음에 수행할 작업

- 고가용성 구성을 구축한다면, FDM의 온라인 도움말에서 추가 지침을 확인하십시오.
- Cisco Cloud에 이벤트를 직접 전송하고 SecureX와 통합하는 방법, 11 페이지에서 남은 단계를 계속 진행합니다.

중요 이를 구성한 후 Cisco Defense Orchestrator와의 통합을 활성화하면 디바이스가 SSE에서 등록 취소될 수 있습니다. SSE의 Devices(디바이스) 탭에 이 문제가 표시되면 (FDM에서 관리하는 FTD 전용) CDO 및 SecureX 계정 병합, 14 페이지의 내용을 참조하십시오.

디바이스가 이벤트를 **Cisco Cloud**로 전송하도록 **FMC** 구성

관리되는 Firepower Threat Defense 디바이스가 이벤트를 클라우드로 직접 전송하도록 Firepower Management Center을(를) 구성합니다.

참고 사용 가능한 옵션은 FMC 버전에 따라 다릅니다. 사용 중인 버전에 적용되지 않는 단계는 건너뜁니다.

시작하기 전에

- Firepower Management Center에서 다음을 수행합니다.
  - **System(**시스템**) > Configuration(**구성**)** 페이지로 이동한 다음, 클라우드의 디바이스 목록에서 명확하게 확인할 수 있도록 FMC에 고유한 이름을 지정합니다.
  - FMC에 FTD 디바이스를 추가하고, 디바이스에 라이선스를 할당하고, 시스템이 올바르게 작동하는지 확인합니다. (필요한 정책을 생성했고, 이벤트가 생성되어 Analysis(분석) 탭의 Firepower Management Center 웹 인터페이스에 정상적으로 표시된다는 뜻입니다.)
- Cisco Cloud에 이벤트를 직접 전송하고 SecureX와 통합하는 방법, 11 페이지에서 지금까지의 단계를 수행합니다.
- 클라우드 인증서가 있는지 확인하고 계정이 생성된 SecureX 지역 클라우드에 로그인할 수 있는지 확인합니다.

  URL은 SecureX 지역 클라우드, 1 페이지의 내용을 참조하십시오.

- 현재 시스템 로그를 사용하여 클라우드로 이벤트를 전송하는 경우 중복을 방지하기 위해 이러한 전송을 비활성화합니다.

프로시저

단계 **1** Firepower Management Center에서 **System(**시스템**) > Integration(**통합**)**을 선택합니다.

단계 **2** **Cloud Services(**클라우드 서비스**)**를 클릭합니다.

단계 **3** **Cisco Cloud Event Configuration(Cisco Cloud** 이벤트 설정**)** 또는 **Cisco Cloud**(사용 중인 FMC 버전에 따라 다름)에 대한 슬라이더를 활성화합니다.

단계 **4** 아직 수행하지 않았고 FMC에서 **Cisco Cloud Region(Cisco** 클라우드 영역**)** 옵션을 제공하는 경우 계정을 생성 한 Cisco Cloud Region(Cisco 클라우드 영역)을 선택합니다.

단계 **5** 클라우드로 전송할 이벤트 유형을 활성화합니다.

연결 이벤트를 전송하는 경우 이 통합에서 보안 인텔리전스 연결 이벤트만 사용됩니다. 다른 모든 연결 이벤트는 이 통합에서 사용되지 않습니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

Save(저장**)** 버튼을 누를 수 없다면, 선택된 지역 클라우드에 FMC가 이미 등록되어 있다는 뜻입니다.

단계 **7** 기능이 올바르게 활성화되어 있는지 확인합니다.

a) 시스템을 동기화할 수 있도록 몇 분 정도 기다립니다.

b) 기능을 활성화한 페이지에서 링크를 클릭해 Cisco Cloud 구성을 확인합니다. (링크는 같은 **Cisco Cloud** 상자에 있습니다.)

보안 서비스 익스체인지 새 브라우저 창에서 열립니다.

c) SecureX 계정에 액세스하는 데 사용하는 자격 증명으로 로그인합니다.

d) **Devices(**디바이스**)**를 클릭합니다.

e) Firepower Management Center 및 해당 매니지드 디바이스가 목록에 나타나는지 확인합니다.

다음에 수행할 작업

Cisco Cloud에 이벤트를 직접 전송하고 SecureX와 통합하는 방법, 11 페이지에서 남은 단계를 계속 진행합니다.

이벤트가 (직접 연결을 통해) 보안 서비스 익스체인지에 도달하는지 확인합니다.

시작하기 전에

예상한 이벤트가 Firepower에 정상적으로 표시되는지 확인합니다.

프로시저

단계 **1** 보안 서비스 익스체인지에서 작업하고 있지 않다면 Access(액세스) 보안 서비스 익스체인지, 13 페이지이(가) 됩니다.

단계 **2** **Events(**이벤트**)**를 클릭합니다.

단계 **3** 디바이스에서 이벤트를 찾습니다.

예상한 이벤트가 표시되지 않는다면 직접 통합 문제 해결, 20 페이지의 팁을 참조하고 Cisco Cloud에 이벤트를 직접 전송하고 SecureX와 통합하는 방법, 11 페이지에서 다시 확인해 보십시오.

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.

디바이스 인터페이스에는 통합이 활성화되었다고 표시되면 클라우드의 **Devices(**디바이스**)** 페이지에 디바이스가 표시되지 않습니다.

- 클라우드 계정에 연결되지 않은 스마트 계정이나 가상 계정으로 디바이스에 라이선스를 부여했을 것입니다. 다음 중 하나를 수행합니다.
  - SSE에서 디바이스가 라이선스를 받은 계정을 링크합니다.

    Link Smart 라이선스 계정, 16 페이지의 내용을 참조하십시오.
  - 연결된 계정에서 디바이스에 라이선스를 부여합니다.

    FMC 또는 FDM에서 통합을 비활성화하고, 현재 라이선스를 디바이스에서 등록 최소하고, 연결된 계정에서 디바이스에 다시 라이선스를 부여한 다음 FDM 또는 FMC에서 통합을 재활성화합니다.
- Firepower 설정에서 선택한 지역과 동일한 지역 클라우드가 표시되는지 확인합니다. 클라우드에 이벤트를 전송하기 시작할 때 지역을 선택하지 않았다면, 먼저 북미 클라우드를 사용해보십시오.

FMC에서 매니지드 디바이스가 **SSE** 디바이스 페이지에 올바르게 나열되지 않음

(6.4.0.4 이전 릴리스) 수동으로 디바이스에 고유한 이름을 지정 합니다. Devices(디바이스) 목록에서 각 행에 대 한 연필 아이콘을 클릭 합니다. 추천: 설명에 있는 IP 주소를 복사하십시오.

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

(6.4.0.4 ~ 6.6 릴리스) 디바이스 이름은 FMC에서 SSE로 처음 등록될 때만 SSE로 전송되며, FMC에서 디바이스 이름이 변경되면 SSE에서 업데이트되지 않습니다.

SSE의 Devices(디바이스) 페이지에서 이전에 등록한 디바이스가 예기치 않게 Unregistered(등록되지 않음)로 표시됩니다.

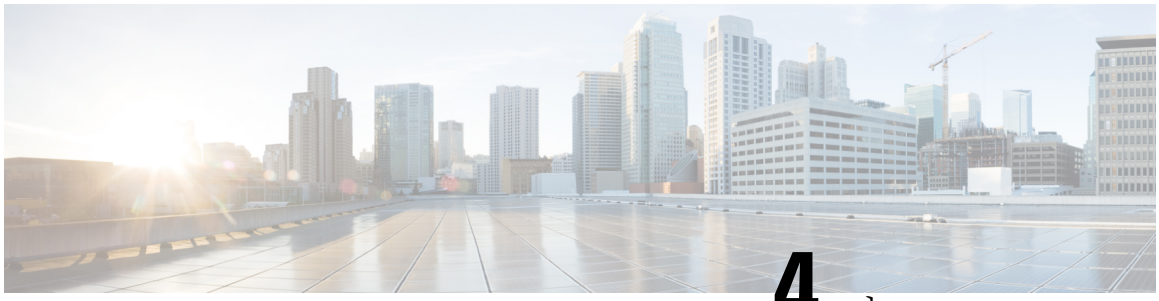
이러한 디바이스가 FDM에서 관리되는 FTD 디바이스이고 SecureX 또는 와의 통합을 위해 SSE에 디바이스를 등록한 후 CDO와의 통합을 활성화했고 아직 계정을 병합하지 않은 경우, (FDM에서 관리하는 FTD 전용) CDO 및 SecureX 계정 병합, 14 페이지의 절차를 완료합니다.

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 새로고칩니다.
- 예상한 이벤트가 Firepower에 표시되는지 확인합니다.
- FDM을 사용한다면 액세스 규칙 로깅 설정을 확인하십시오.
- SSE의 **Cloud Services(클라우드 서비스)** 페이지에 있는 **Eventing(이벤팅)** 설정에서 자동 삭제(필터링을 통한 이벤트 제거) 구성을 확인합니다.
- 다른 문제 해결 팁은 SSE의 온라인 도움말에서 확인할 수 있습니다.

일부 이벤트가 누락되었음

- 연결 이벤트를 전송하는 경우 보안 인텔리전스 연결 이벤트만 사용됩니다. 다른 모든 연결 이벤트는 무시됩니다.
- 전역 차단 또는 허용 목록 및 Cisco Threat Intelligence Director(TID)을 포함하여 FMC에서 맞춤형 보안 인텔리전스 개체를 사용하는 경우 해당 개체를 사용하여 처리되는 이벤트를 자동으로 승격하도록 SSE를 구성해야 합니다. 이벤트를 인시던트로 승격하는 정보는 SSE의 온라인 도움말을 참조하십시오. .



4 장

시스템 로그를 사용하여 클라우드로 이벤트 전송

시스템 로그를 통한 통합 관련 정보

Firepower 릴리스 6.3부터는 시스템 로그를 사용하여, 지원되는 이벤트를 Firepower 디바이스에서 Cisco Cloud로 전송할 수 있습니다. 사내 Cisco Security Services Proxy(CSSP) 서버를 설정하고 시스템 로그 메시지가 이 프록시로 전송되도록 디바이스를 구성해야 합니다.

10분마다 프록시가 수집된 이벤트를 보안 서비스 익스체인지(SSE)로 포워딩하며, 여기서는 이벤트를 SecureX에 표시되는 인시던트로 자동 또는 수동으로 승격할 수 있습니다.

시스템 로그를 이용한 통합 요구사항

요구 사항 유형	요건
Firepower 디바이스	지원되는 Firepower 소프트웨어 버전을 실행하는 모든 디바이스
Firepower 버전	6.3 이상
사용할 SecureX 클라우드에서의 계정	SecureX 액세스에 필요한 필수 계정, 5 페이지의 내용을 참조하십시오.

요구 사항 유형	요건
라이선싱	이 통합에는 특별한 라이선스가 필요하지 않습니다. 하지만 다음 경우를 고려하십시오. • SecureX에 전송할 이벤트를 생성하려면 Firepower 시스템에 라이선스가 있어야 합니다. 자세한 내용은 https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-licensing-information-listing.html 섹션을 참조해 주십시오. • 이 기능은 Firepower 평가판 라이선스에서는 지원되지 않습니다. • 사용자의 환경에서는 에어갭 환경에 구축할 수 없습니다.
일반	Firepower 시스템이 이벤트를 예상대로 생성하고 있습니다.

시스템 로그를 이용해 **Cisco Cloud**에 이벤트를 전송하는 방법

참고 디바이스가 이미 클라우드에 이벤트를 전송 중인 경우, 다시 전송하도록 구성할 필요가 없습니다. SecureX 및 Cisco SecureX Threat Response (이전에는 Cisco Threat Response)는 동일한 이벤트 데이터 집합을 사용합니다.

	수행해야 할 작업	추가 정보
단계	전송할 이벤트, 해당 이벤트를 전송하는 방법, 사용할 지역 클라우드 등에 대해 결정합니다.	다음 항목을 참조하십시오. Firepower 및 통합에 대한 중요 정보 SecureX, 1 페이지
단계	요구 사항을 충족합니다.	시스템 로그를 이용한 통합 요구사항, 23 페이지의 내용을 참조하십시오.
단계	디바이스 관리 및 이벤트 필터링에 사용할, SecureX용 플랫폼인 보안 서비스 익스체인지(SSE)에 액세스합니다.	Access(액세스) 보안 서비스 익스체인지, 26 페이지의 내용을 참조하십시오.
단계	Cisco Security Services Proxy(CSSP) 서버를 설치하고 구성합니다.	보안 서비스 익스체인지에서 무료 설치 프로그램과 지침을 다운로드합니다. SSE의 브라우저 창 오른쪽 상단에 있는 Tools 버튼(🛠)에서 **Downloads(**다운로드**)**를 선택합니다.

	수행해야 할 작업	추가 정보
단계	보안 서비스 익스체인지에서 기능을 활성화합니다.	**Cloud Services(**클라우드 서비스**)**를 클릭하고 다음 옵션을 활성화합니다. • **Cisco SecureX Threat Response** • 이벤팅 서비스
단계	지원되는 이벤트에 대한 시스템 로그 메시지를 프록시 서버로 전송하도록 Firepower 디바이스를 구성합니다.	• FDM(Firepower Device Manager)에서 관리하는 디바이스의 경우: FDM 온라인 도움말의 '침입 이벤트에 대한 시스템 로그 구성'에서 관련 정보를 참조하십시오. • Firepower Management Center(FMC)에서 관리하는 디바이스의 경우: FMC 온라인 도움말의 '외부 도구를 이용한 이벤트 분석' 장에 있는 시스템 로그 관련 정보를 참조하십시오.
단계	Firepower 제품에서 메시지가 각 이벤트를 생성한 디바이스를 식별하는지 확인합니다.	• Firepower Device Manager에서 다음을 수행합니다. **Device(**디바이스**) > Hostname(**호스트 이름**)**에서 호스트 이름을 지정합니다. • Firepower Management Center에서 다음을 수행합니다. Platform Settings(플랫폼 설정)의 시스템 로그 **Settings(**시스템 로그 설정**)** 탭에서 시스템 로그 디바이스 **ID**를 활성화하고 식별자를 지정합니다.
단계	Firepower 시스템에서 지원되는 이벤트를 생성할 때까지 기다립니다.	--
단계	보안 서비스 익스체인지에 이벤트가 예상대로 표시되는지 확인하고 필요하다면 문제 해결을 진행합니다.	참조: • 이벤트가 (시스템 로그를 통해) 보안 서비스 익스체인지에 도달하는지 확인합니다., 27 페이지 • 시스템 로그 통합 문제 해결, 27 페이지

	수행해야 할 작업	추가 정보
단계	보안 서비스 익스체인지에서 중요한 이벤트를 자동으로 승격하도록 시스템을 구성합니다.	중요 이벤트 승격을 자동화하지 않는 경우 SecureX에서 이벤트를 보려면 수동으로 검토하고 승격해야 할 수 있습니다. 이벤트 승격에 관한 정보는 보안 서비스 익스체인지에서 온라인 도움말의 정보를 참조하십시오. SSE에 액세스하는 방법은 Access(액세스) 보안 서비스 익스체인지, 13 페이지의 내용을 참조하십시오.
단계	(선택 사항) 보안 서비스 익스체인지에서 중요하지 않은 특정 이벤트의 자동 삭제를 구성합니다.	이벤트 필터링에 관한 정보는 보안 서비스 익스체인지에서 온라인 도움말의 정보를 참조하십시오. SSE에 액세스하는 방법은 Access(액세스) 보안 서비스 익스체인지, 13 페이지의 내용을 참조하십시오.
단계	SecureX에서 Firepower 모듈을 추가합니다.	SecureX에서 **Integration Modules(통합 모듈) > Available Integration Modules(사용 가능한 통합 모듈)**로 이동하여 Firepower 모듈을 추가합니다. 이 모듈에 관한 자세한 내용은 SecureX의 온라인 도움말을 참조하십시오.

Access(액세스) 보안 서비스 익스체인지

시작하기 전에

브라우저에서 팝업 차단을 비활성화합니다.

프로시저

단계 **1** 브라우저 창에서 사용자의SecureX 클라우드로 이동합니다.

- 북미 클라우드: https://securex.us.security.cisco.com
- 유럽 클라우드: https://securex.eu.security.cisco.com
- 아시아 클라우드: https://securex.apjc.security.cisco.com

단계 **2** SecureX, AMP for Endpoints, Cisco Threat Grid 또는 Cisco Security 계정 관련 자격 증명을 사용하여 로그인합니다.

계정 자격 증명은 지역 클라우드마다 다릅니다.

단계 **3** 보안 서비스 익스체인지(으)로 이동합니다.

Integrations(통합) > Devices(디바이스) > Manage Devices(디바이스 관리)를 선택합니다.

보안 서비스 익스체인지 가 새 브라우저 창에서 열립니다.

이벤트가(시스템 로그를 통해) 보안 서비스 익스체인지에 도달하는지 확인합니다.

시작하기 전에

예상한 이벤트가 Firepower에 정상적으로 표시되는지 확인합니다.

프로시저

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

단계 **2** Access(액세스) 보안 서비스 익스체인지, 26 페이지.

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

단계 **4** 디바이스에서 이벤트를 찾습니다.

예상한 이벤트가 표시되지 않는다면 시스템 로그 통합 문제 해결, 27 페이지의 팁을 참조하고 시스템 로그를 이용해 Cisco Cloud에 이벤트를 전송하는 방법, 24 페이지에서 다시 확인해 보십시오.

시스템 로그 통합 문제 해결

이벤트가 CSSP에 도달하지 않습니다.

디바이스가 네트워크의 CSSP에 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.

- Events(이벤트) 페이지에서 **Refresh(**새로고침**)** 버튼을 눌러 목록을 새로고칩니다.
- 예상한 이벤트가 Firepower에 표시되는지 확인합니다.

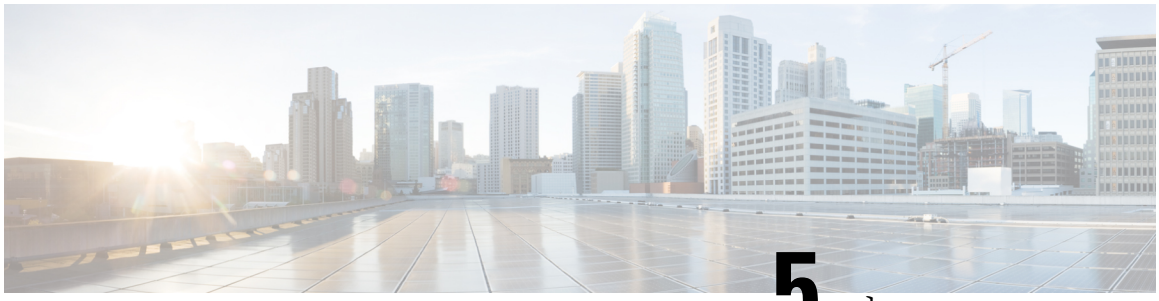
- SSE의 **Cloud Services(**클라우드 서비스**)** 페이지에 있는 **Eventing(**이벤팅**)** 설정에서 자동 삭제(필터링을 통한 이벤트 제거) 구성을 확인합니다.
- 이벤트를 전송하는 지역 클라우드를 보고 있는지 확인합니다.

시스템 로그 필드 관련 질문

시스템 로그 필드 및 설명에 관한 내용은 https://www.cisco.com/c/en/us/support/security/defense-center/products-system-message-guides-list.html에 있는 *Cisco Firepower Threat Defense* 시스템 로그 메시지 가이드를 참조하십시오.

일부 이벤트가 **SecureX** 타일에서 누락됨

전역 차단 또는 허용 목록을 포함하여 FMC에서 맞춤형 보안 인텔리전스 개체를 사용하는 경우 해당 개체를 사용하여 처리되는 이벤트를 자동으로 승격하도록 SSE를 구성해야 합니다. 이벤트를 인시던트로 승격하는 정보는 SSE의 온라인 도움말을 참조하십시오. .



5 장

다음 단계

사용에 대한 추가 정보: SecureX

SecureX 사용

SecureX 사용에 대한 모든 정보는 SecureX의 온라인 도움말을 참조하십시오.

추가 정보: http://cs.co/SecureX_faq

SecureX 대시보드의 **Firepower** 타일

Firepower 타일을 포함하여 SecureX 대시보드의 타일에 대한 자세한 내용은 https://www.cisco.com/c/en/us/td/docs/security/securex/tiles/securex-tiles-list.html의 내용을 참조하십시오.

작업 중 보안 서비스 익스체인지

보안 서비스 익스체인지 또는 Cisco Security Services Proxy 사용 관련 정보는 보안 서비스 익스체인지의 온라인 도움말을 참조하십시오.