

# Firepower Management Center 및 Cisco SaaS(Security Analytics and Logging) 통합 가이드

초판: 2020년 7월 21일

최종 변경: 2020년 7월 21일

## Firepower 및 SaaS(Cisco Security Analytics and Logging) 통합 Cisco Security Analytics and Logging(SaaS)

Firepower 이벤트를 저장하는 데 추가 공간이 필요한 경우 Cisco Security Analytics and Logging(SaaS)를 사용하여 Firepower 이벤트를 스토리지용 Stealthwatch 클라우드에 전송하고, 필요에 따라 Stealthwatch 클라우드를 사용하여 보안 애널리틱스에 Firepower 이벤트 데이터를 제공할 수 있습니다.

이 통합은 FMC(Firepower Management Center)에서 관리하는 FTD(Firepower Threat Defense) 디바이스와 관련이 있습니다. 이 문서는 Firepower 소프트웨어를 실행하지 않는 디바이스, FDM(Firepower Device Manager)에서 관리하는 디바이스 또는 FMC에서 관리하는 비 FTD 디바이스에는 적용되지 않습니다.

Cisco Security Analytics and Logging(SaaS)에 관한 자세한 내용은 <https://www.cisco.com/c/en/us/products/security/security-analytics-logging/index.html>의 내용을 참조하십시오.

## Cisco Security Analytics and Logging 원격 이벤트 스토리지 옵션 비교

다음은 이벤트 데이터를 외부(Firepower Management Center)에 저장하는 비슷하지만 다른 옵션입니다.

온프레미스	SaaS
방화벽 뒤에서 스토리지 시스템을 구매, 라이선싱, 설정합니다.	라이선스 및 데이터 스토리지 요금제를 구매하고 Cisco 클라우드에 데이터를 전송합니다.
지원되는 이벤트 유형: <ul style="list-style-type: none"> <li>• 연결</li> <li>• 보안 인텔리전스</li> <li>• 침입</li> <li>• 파일 및 악성코드</li> </ul>	지원되는 이벤트 유형: <ul style="list-style-type: none"> <li>• 연결</li> <li>• 보안 인텔리전스</li> <li>• 침입</li> <li>• 파일 및 악성코드</li> </ul>

온프레미스	<b>SaaS</b>
시스템 로그를 통해 이벤트를 스토리지로 전송합니다.	시스템 로그를 통해 이벤트를 스토리지로 전송합니다.
Stealthwatch Management Console 어플라이언스를 사용하여 이벤트를 확인합니다. FMC 이벤트 뷰어에서 교차 실행합니다.	라이선스에 따라 CDO 또는 Stealthwatch의 이벤트를 확인합니다. FMC 이벤트 뷰어에서 교차 실행합니다.
자세한 내용은 <i>Firepower Management Center</i> 설정 가이드 또는 온라인 도움말의 데이터 스토리지 장에 있는 링크를 참조하십시오.	

## SAL(SaaS) 통합을 위한 요구 사항 및 사전 요건

요구 사항 또는 사전 조건 유형	요건
Firepower	Firepower Threat Defense 디바이스를 관리하는 Firepower Management Center Firepower 릴리스 6.4 이상 필수 버전은 FMC 및 모든 관리되는 FTD 디바이스에 적용됩니다. Firepower 시스템을 구축하고 이벤트를 성공적으로 생성해야 합니다.
지역 클라우드	이벤트를 전송할 지역 클라우드를 결정합니다. 이벤트는 다른 지역 클라우드에서 보거나 이동할 수 없습니다.
데이터 요금제	시스템에 필요한 클라우드 스토리지의 양을 결정합니다. <a href="#">스토리지 요구 사항 계산 및 데이터 계획 구매, 4 페이지</a> 의 내용을 참조하십시오.
라이선싱	<ul style="list-style-type: none"> <li>• Cisco Security Analytics and Logging 라이선스: 임의 라이선싱 옵션 및 설명은 <a href="#">SAL(SaaS) 라이선스, 3 페이지</a>의 내용을 참조하십시오.</li> <li>• CDO 라이선스: 추가 CDO 라이선싱이 필요하지 않습니다.</li> <li>• Stealthwatch Cloud 라이선스: 추가 라이선싱이 필요하지 않습니다.</li> <li>• Firepower 라이선스: 추가 Firepower 라이선싱이 필요하지 않습니다.</li> </ul>
어카운트	이 통합을 위한 라이선스를 구매하면 이 기능을 지원하기 위한 CDO 테넌트 계정이 제공됩니다.
지원되는 Firepower 이벤트 유형	침입, 연결, 보안 인텔리전스, 파일 및 악성코드 이벤트

요구 사항 또는 사전 조건 유형	요건
추가 사전 요건	각 절차의 시작하기 전에 또는 사전 요건 섹션을 참조하십시오.

## SAL(SaaS) 라이선스

라이선스	세부 사항
무료 평가판	30일 무료 평가판 라이선스를 받으려면 <a href="https://info.securexanalytics.com/sal-trial.html">https://info.securexanalytics.com/sal-trial.html</a> 을(를) 방문하십시오.
로깅 및 문제 해결	Cisco 클라우드에 이벤트를 저장하고 CDO 웹 인터페이스를 사용하여 저장된 이벤트를 보고 필터링합니다.
(선택 사항) 로깅 분석 및 탐지	<p>시스템은 FTD 이벤트에 Stealthwatch Cloud 동적 엔터티 모델링을 적용하고, 행동 모델링 분석을 사용하여 Stealthwatch Cloud 관찰 및 알림을 생성할 수 있습니다. Cisco SSO(Single Sign-On)를 사용하여 CDO에서 사용자에게 프로비저닝된 Stealthwatch Cloud 포털로 교차 실행할 수 있습니다.</p> <p>SAL용 라이선스를 구매하면 로그 보기용 CDO 테넌트 및 위협 탐지용 SWC 인스턴스에 대한 액세스 권한이 제공됩니다. SAL 사용자는 SAL이 제공하는 결과를 위해 이 두 포털에 액세스하기 위해 별도의 CDO 또는 SWC 라이선스가 필요하지 않습니다.</p>
(선택 사항) 전체 네트워크 분석 및 탐지	<p>시스템은 FTD 이벤트와 네트워크 트래픽 모두에 동적 엔터티 모델링을 적용하고 관찰 및 알림을 생성합니다. Cisco SSO(Single Sign-On)를 사용하여 CDO에서 사용자에게 프로비저닝된 Stealthwatch Cloud 포털로 교차 실행할 수 있습니다.</p> <p>SAL용 라이선스를 구매하면 로그 보기용 CDO 테넌트 및 위협 탐지용 SWC 인스턴스에 대한 액세스 권한이 제공됩니다. SAL 사용자는 SAL이 제공하는 결과를 위해 이 두 포털에 액세스하기 위해 별도의 CDO 또는 SWC 라이선스가 필요하지 않습니다.</p>

SAL(SaaS) 라이선싱 옵션에 대한 자세한 내용은 *Cisco Security Analytics and Logging* 주문 가이드 (<https://www.cisco.com/c/en/us/products/collateral/security/security-analytics-logging/guide-c07-742707.html>)를 참조하십시오.

SAL(SaaS) 라이선스는 이러한 제품 중 하나에 대한 별도의 라이선스를 보유하지 않고도 Cisco Defense Orchestrator 테넌트를 사용하여 분석을 위해 방화벽 로그 및 SWC(Stealthwatch Cloud) 인스턴스를 볼 수 있는 권한을 제공합니다.

SAL(SaaS) 라이선스를 구매하려면 공인 Cisco 영업 담당자에게 문의하거나 주문 가이드(위의 링크)를 참조하여 **SAL-SUB**로 시작하는 PID를 찾아보십시오.

이 제품에 대한 추가 정보는 여기(<https://apps.cisco.com/Commerce/guest>)에 있습니다.

## 스토리지 요구 사항 계산 및 데이터 계획 구매

Cisco 클라우드가 FTD 에서 매일 수신하는 이벤트 수를 반영하는 데이터 플랜을 구매해야 합니다. 이를 "일일 수집 속도"라고 합니다.

데이터 스토리지 요구 사항을 추정하려면 다음을 수행합니다.

- (권장 사항) 구매하기 전에 Cisco Security Analytics and Logging(SaaS) 무료 평가판에 참여해 주십시오. [SAL\(SaaS\) 라이선스, 3 페이지](#)의 내용을 참조하십시오.
- <https://ngfwpe.cisco.com/ftd-logging-estimator>의 로깅 볼륨 견적 도구를 사용하십시오.

데이터 플랜은 다양한 일일 볼륨으로, 연간 단위로 제공됩니다. 데이터 플랜에 대한 자세한 내용은 <https://www.cisco.com/c/en/us/products/collateral/security/security-analytics-logging/guide-c07-742707.html>에서 *Cisco Security Analytics* 및 로깅 주문 가이드를 참조하십시오.



**참고** SAL(SaaS) 라이선스 및 데이터 플랜을 보유하고 있는 경우 나중에 다른 라이선스를 취득할 수 있으며, 이것만 있으면 다른 데이터 플랜을 구매할 필요가 없습니다. 네트워크 트래픽 처리량이 변경되어 다른 데이터 플랜을 취득하는 경우에는 다른 SAL(SaaS) 라이선스를 구입하지 않아도 됩니다.

## SAL(SaaS)에서 시스템 로그를 사용하여 이벤트 데이터 스토리지를 설정하는 방법

	수행해야 할 작업	추가 정보
단계	요구 사항 및 사전 요건 검토	<a href="#">SAL(SaaS) 통합을 위한 요구 사항 및 사전 요건, 2 페이지</a> 의 내용을 참조하십시오.
단계	필요한 라이선스, 계정 및 데이터 스토리지 요금제 받기	승인된 Cisco 영업 담당자에게 문의하십시오.
단계	다단계 인증을 사용하여 CDO 액세스 설정	<a href="#">CDO에 로그인</a> 에 대한 내용은 CDO 온라인 도움말의 지침을 참조하십시오. 선택합니다.

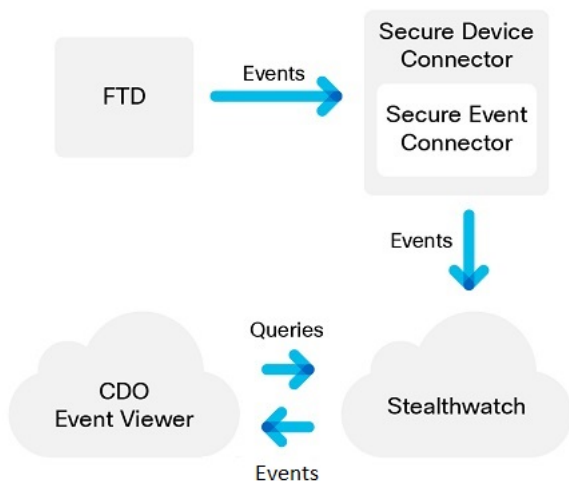
	수행해야 할 작업	추가 정보
단계	VMWare 가상 머신에 온프레미스 SDC(Secure Device Connector) 설정	<p>이 구성 요소는 Firepower 디바이스에서 이벤트를 전송할 구성 요소인 SEC의 설치를 활성화할 때만 필요합니다.</p> <p>CDO 온라인 도움말에 설명된 대로 다음 중 하나를 사용합니다.</p> <ul style="list-style-type: none"> <li>• (기본 설정) CDO 제공 VM 이미지를 사용합니다.</li> <li>• CDO 제공 이미지를 사용하지 않고 SDC를 생성합니다.</li> </ul> <p>중요! 절차 사전 요건을 건너뛰지 마십시오. 그러나 이 통합에 적용되지 않는 온보딩에 대한 정보는 무시하십시오.</p>
단계	방금 생성한 SDC 가상 머신에 SEC(Secure Event Connector)를 설치합니다.	<p>이는 Firepower 디바이스에서 이벤트를 전송할 구성 요소입니다.</p> <p><a href="#">보안 이벤트 커넥터 설치</a>에 대한 지침은 CDO 온라인 도움말을 참조하십시오.</p> <p>중요! 절차 사전 요건을 건너뛰지 마십시오. 그러나 이 통합에 적용되지 않는 온보딩에 대한 정보는 무시하십시오.</p>
단계	관리되는 디바이스에서 시스템 로그 이벤트를 SEC로 전송하도록 FMC를 설정합니다.	<a href="#">FTD 디바이스에서 보안 이벤트 시스템 로그 메시지 보내기, 6 페이지</a>
단계	이벤트가 성공적으로 전송되고 있는지 확인	<a href="#">이벤트 보기 및 작업, 9 페이지</a> 의 내용을 참조하십시오.
단계	(선택 사항) 클라우드로 연결 이벤트를 전송하는 경우 FMC에 저장하지 않으려면 FMC에서 해당 스토리지를 비활성화합니다.	FMC 온라인 도움말의 데이터베이스 이벤트 제한 항목에서 연결 이벤트에 대한 정보를 참조하십시오.
단계	(선택 사항) FMC에 표시되는 이벤트에서 클라우드의 관련 이벤트로 쉽게 피봇할 수 있도록 FMC에서 CDO로 교차 실행을 설정합니다.	FMC의 온라인 도움말을 참조하십시오.
단계	(선택 사항) CDO에서 일반 설정 구성	<p>예를 들어 Cisco 지원 담당자가 데이터를 사용할 수 없게 할 수 있습니다.</p> <p>CDO 온라인 도움말에서 <a href="#">General Settings(일반 설정)</a>를 참조하십시오.</p>

시스템 로그를 사용하여 SAL(SaaS)에 Firepower 이벤트 보내기 개요

	수행해야 할 작업	추가 정보
단계	(선택 사항) 동료가 이벤트를 보고 작업할 수 있도록 CDO 사용자 계정을 생성합니다.	CDO 온라인 도움말에서 새 CDO 사용자 생성을 참고하십시오.
단계		

## 시스템 로그를 사용하여 SAL(SaaS)에 Firepower 이벤트 보내기 개요

SAL(SaaS)(Cisco Security Analytics and Logging(SaaS))를 사용하면 Firepower 디바이스에서 이벤트를 네트워크상의 가상 머신에 설치된 SEC(Security Event Connector)에 시스템 로그 메시지로 전송하고 이 SEC는 스토리지용 Stealthwatch 클라우드에 이벤트를 전달합니다. 사용자는 웹 기반 CDO(Cisco Defense Orchestrator) 포털을 사용하여 이벤트를 보고 작업할 수 있습니다. 구매한 SAL 라이선스에 따라 Stealthwatch 클라우드 포털을 사용하여 해당 제품의 분석 기능에 액세스할 수도 있습니다.



참고 CDO 포털에 있는 대부분의 기능은 이 통합에 적용되지 않습니다. 예를 들어 CDO는 디바이스를 관리하지 않으므로 디바이스가 CDO에 온보딩되지 않습니다.

## FTD 디바이스에서 보안 이벤트 시스템 로그 메시지 보내기

이 절차에서는 에서 관리하는 Firepower Management Center FTD 디바이스에서 보안 이벤트(연결, 보안 인텔리전스, 침입, 파일 및 악성코드 이벤트)에 대한 시스템 로그 메시지를 전송하기 위한 모범 사례 설정을 설명합니다.



참고 대부분의 FTD 시스템 로그 설정은 보안 이벤트에 적용되지 않습니다. 이 절차에 설명된 옵션만 설정하십시오.

## 시작하기 전에

- Firepower Management Center에서 보안 이벤트를 생성하도록 정책을 설정하고 표시될 것으로 예상되는 이벤트가 Analysis(분석) 메뉴의 해당 테이블에 나타나는지 확인합니다.
- 시스템 로그 서버 IP 주소, 포트 및 프로토콜(UDP 또는 TCP)을 수집합니다.  
CDO에 로그인합니다. 그런 다음 CDO 브라우저 창의 오른쪽 상단에 있는 사용자 메뉴에서 **Secure Connector**(보안 커넥터)를 선택합니다. **Secure Event Connector**(보안 이벤트 커넥터)를 클릭하면 오른쪽에 필요한 정보가 표시됩니다.
- 디바이스가 시스템 로그 서버에 연결할 수 있는지 확인합니다.
- FMC 온라인 도움말의 "연결 로깅" 장에서 추가 정보를 참조하십시오.

## 프로시저

**단계 1** Firepower Management Center 웹 인터페이스에 로그인합니다.

**단계 2** FTD 디바이스에 대한 시스템 로그 설정을 구성합니다.

- Devices**(디바이스) > **Platform Settings**(플랫폼 설정)를 클릭합니다.
- FTD 디바이스와 연결된 플랫폼 설정 정책을 편집합니다.
- 왼쪽 탐색 창에서 시스템 로그를 클릭합니다.
- Syslog Servers**(시스템 로그 서버)를 클릭하고 **Add**(추가)를 클릭하여 서버, 프로토콜, 인터페이스 및 관련 정보를 입력합니다.

위의 CDO에서 수집한 IP 주소, 포트 및 프로토콜을 사용합니다.

EMBLEM 형식 및 보안 시스템 로그는 이 통합에서 지원되지 않습니다.

이 페이지의 옵션에 대한 질문이 있는 경우 FMC 온라인 도움말의 "시스템 로그 서버 설정" 항목을 참조하십시오.


- Syslog Settings**(시스템 로그 설정)를 클릭하고 다음 설정을 구성합니다.
  - **Syslog** 메시지에서 타임스탬프 활성화
  - 타임스탬프 형식
  - **Syslog** 디바이스 ID 활성화
- Logging Setup**(로깅 설정)을 클릭합니다.
- Send syslog in EMBLEM format**(EMBLEM 형식으로 시스템 로그 전송)이 선택되지 않았는지 확인합니다.
- 설정을 **Save**(저장)합니다.

**단계 3** 액세스 제어 정책(파일 및 악성코드 로깅 포함)에 대한 일반 로깅 설정을 구성합니다.

- Policies**(정책) > **Access Control**(액세스 제어)을 클릭합니다.
- 해당 액세스 제어 정책을 편집합니다.
- Logging**(로깅)을 클릭합니다.

- d) **FTD 6.3 이상:** 디바이스에 구축된 **FTD** 플랫폼 설정 정책에 설정된 시스템 로그 설정을 사용합니다.를 선택합니다.
- e) (선택 사항) **Syslog Severity**(시스템 로그 심각도)를 선택합니다.
- f) 파일 및 악성코드 이벤트를 전송하려면 **Send Syslog messages for File and Malware**(파일 및 악성코드 이벤트에 대해 시스템 로그 메시지 전송)를 선택합니다.
- g) **Save**(저장)를 클릭합니다.

단계 4 액세스 제어 정책에 대한 보안 인텔리전스 이벤트에 대한 로깅을 활성화합니다.

- a) 동일한 액세스 제어 정책에서 **Security Intelligence**(보안 인텔리전스) 탭을 클릭합니다.
- b) 다음 각 위치에서 로깅( )를 클릭하여 연결의 시작과 끝 및 시스템 로그 서버를 활성화합니다.
  - **DNS Policy**(DNS 정책) 옆.
  - **Block List**(차단 목록) 상자에서 **Networks**(네트워크) 및 **URL**에 대해.

- c) **Save**(저장)를 클릭합니다.

단계 5 액세스 제어 정책에서 각 규칙에 대해 시스템 로그 로깅을 활성화합니다.

- a) 동일한 액세스 제어 정책에서 **Rules**(규칙) 탭을 클릭합니다.
- b) 편집할 규칙을 클릭합니다.
- c) 규칙에서 **Logging**(로깅) 탭을 클릭합니다.
- d) 연결의 시작 및 끝을 모두 활성화합니다.
- e) 파일 이벤트를 로깅할 경우 **Log Files**(로그 파일)를 선택합니다.
- f) **Syslog Server**(시스템 로그 서버)를 활성화합니다.
- g) 규칙이 "**Using default syslog configuration in Access Control Logging**(세스 제어 기록에서 기본 시스템 로그 컨피그레이션 사용)"인지 확인합니다.

재정의 설정하지 마십시오.

- h) **Add**(추가)를 클릭합니다.
- i) 정책의 각 규칙에 대해 반복합니다.

단계 6 침입 이벤트를 전송할 경우:

- a) 액세스 제어 정책과 연결된 침입 정책으로 이동합니다.
- b) 침입 정책에서 **Advanced Settings**(고급 설정) > **Syslog Alerting**(시스템 로그 알림)을 선택합니다.  
정책이 액세스 제어 로깅에 대해 설정된 기본 설정을 사용하고 있는지 확인합니다.
- c) **Back**(뒤로)을 클릭합니다.
- d) 왼쪽 탐색창에서 **Policy Information**(정책 정보)을 클릭합니다.
- e) **Commit Changes**(변경 커밋)를 클릭합니다.

다음에 수행할 작업

- 변경을 완료한 경우, 매니지드 디바이스에 변경 사항을 구축합니다.



## 이벤트 보기 및 작업

클라우드에서 이벤트를 보고 검색하려면:

### 프로시저

단계 1 브라우저를 사용하여 이벤트를 전송한 지역 CDO 클라우드로 이동합니다.

- 북미:  
<http://www.defenseorchestrator.com>
- 유럽:  
<http://www.defenseorchestrator.eu>

단계 2 CDO에 로그인합니다.

단계 3 탐색 막대에서 **Monitoring**(모니터링) > **Event Logging**(이벤트 로깅)을 선택합니다.

단계 4 **Historical**(기록) 탭을 사용하여 기록 이벤트 데이터를 볼 수 있습니다. 기본적으로 뷰어에는 이 탭이 표시됩니다.

단계 5 라이브 이벤트를 보려면 **Live**(라이브) 탭을 클릭합니다.

이 페이지에서 수행할 수 있는 작업에 대한 자세한 내용은 CDO 온라인 도움말에서 [이벤트 보기](#)에 대한 지침을 참조하십시오.

다음에 수행할 작업

**Logging Analytics and Detection**(로깅 분석 및 탐지) 또는 **Total Network Analytics and Detection**(총 네트워크 분석 및 탐지) 라이선스가 있는 경우 [CDO 온라인 도움말](#)의 지침을 참조하여 Stealthwatch Cloud 포털로 교차 실행하십시오.

## FAQ

**SAL**에 대한 자세한 정보는 어디에서 확인할 수 있습니까?

[SAL 시작하기 및 자주 묻는 질문\(FAQ\)](#)도 참조하십시오.

**Firepower** 디바이스를 **CDO**에 온보딩해야 하나요?

아니요. CDO에 디바이스를 온보딩하지 마십시오.

**SecureX** 또는 **Cisco Threat Response**를 사용하는 경우 내 **CDO** 계정을 병합해야 하나요?

아니요. CDO 계정을 SecureX 및 Cisco Threat Response에 사용하는 계정과 병합하지 마십시오.