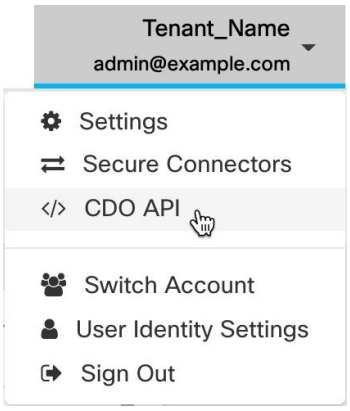
2020의 주요 기능

2020년 12월

2020년 12월 17일

CDO 공용 API

CDO는 공용 API를 게시하고 문서, 예시 및 테스트를 위한 플레이그라운드를 제공했습니다. 공용 API의 목표는 CDO UI에서 일반적으로 수행할 수 있는 많은 작업을 코드에서 간단하고 효과적으로 수행할 수 있는 방법을 제공하는 것입니다.



이 API를 사용하려면 GraphQL을 알아야 합니다. 이는 매우 배우기 쉬우며, 공식 가이드(https://graphql.org/learn/)를 통해 쉽고 간단하게 읽을 수 있습니다. GraphQL은 유연하고 강력한 유형이며 자동 문서화되기 때문에 선택했습니다.

전체 스키마 설명서를 찾으려면 GraphQL 플레이그라운드로 이동하여 페이지 오른쪽에 있는 docs(문서) 탭을 클릭합니다.

사용자 메뉴에서 CDO 공용 API를 선택하여 시작할 수 있습니다.

2020년 12월 10일

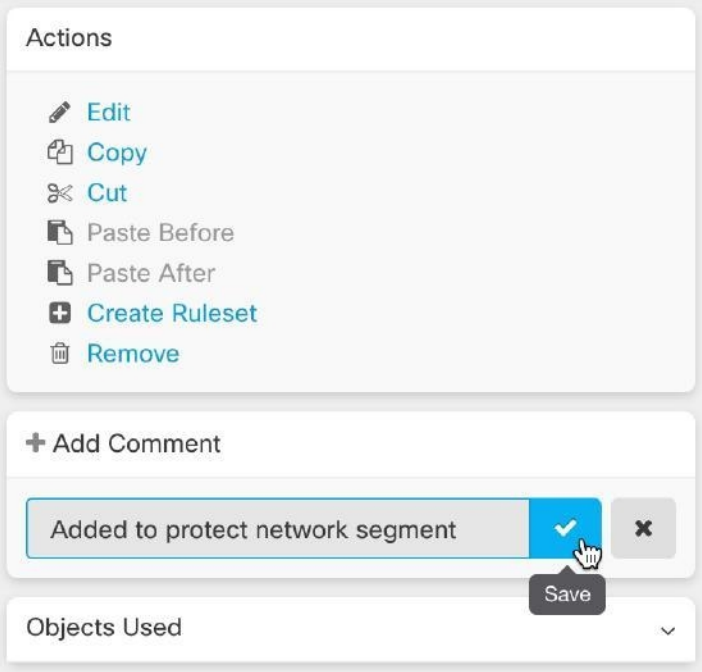
FTD 구성 내보내기

이제 FTD 디바이스의 전체 구성을 CDO가 읽을 수 있는 JSON 파일로 내보낼 수 있습니다. 관리하는 모든 CDO 테넌트에서 이 파일을 FTD 모델(FTD 템플릿)로 가져올 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD 구성 내보내기"를 참조하십시오.

FTD 규칙에 코멘트 추가

이제 FTD 정책 및 규칙 집합의 규칙에 코멘트를 추가할 수 있습니다. 규칙 코멘트는 CDO에만 표시됩니다. 이는 FTD에 기록되지 않으며 FDM에 표시되지도 않습니다.



자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD 정책 및 규칙 집합의 규칙에 코멘트 추가"를 참조하십시오.

2020년 11월

2020년 11월 13일

로우 터치**(Low-Touch)** 프로비저닝 및 일련 번호 온보딩

로우 터치 프로비저닝은 FTD 소프트웨어 버전 6.7 이상을 실행하는 새로운 Firepower 1000 또는 2100 Series 디바이스를 공장에서 배송하거나 이미지 재설치한 후 네트워크에 연결하고 CDO에 자동으로 온보딩한 다음 원격으로 구성할 수 있는 기능입니다. 이렇게 하면 CDO에 디바이스를 온보딩하는 것과 관련된 많은 수동 작업이 필요하지 않습니다. 로우 터치 프로비저닝 프로세스는 물리적 디바이스에 로그인해야 하는 필요성을 최소화합니다. 직원이 네트워킹 디바이스를 사용한 경험이 적은 원격 사무실 또는 기타 위치를 위한 것입니다.

FTD 6.7 이미지가 공장에서 설치된 Firepower 1000 및 2100 Series 디바이스는 2020년 말 또는 2021년 초에 Cisco에서 주문할 수 있습니다.

디바이스의 일련 번호를 사용하여 구성된 FTD(Firepower Threat Defense) 버전 6.7 이상 디바이스를 FTD 6.7에 온보딩하고 CDO에 온보딩할 수도 있습니다.

자세한 내용은 다음 문서를 참조하십시오.

- 로우 터치 프로비저닝

- 일련 번호가 있는 FTD 6.7 디바이스 온보딩
- Cisco Firepower 1000 또는 2100 방화벽용 Firepower Easy 구축 가이드

보안 영역에 **Firepower Threat Defense** 인터페이스 할당

이제 FTD 인터페이스를 보안 영역에 할당하여 트래픽을 추가로 분류하고 관리할 수 있습니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "보안 영역에 Firepower 인터페이스 할당"을 참조하십시오.

2020년 11월 6일

Firepower Threat Defense, 버전 **6.6.1** 및 **6.7**에 대한 **CDO** 지원

CDO는 이제 FTD(Firepower Threat Defense) 버전 6.6.1 및 6.7을 지원합니다. FTD 6.6.1 또는 6.7을 실행하는 새 FTD 디바이스를 온보딩하거나 CDO를 사용하여 해당 버전으로 업그레이드할 수 있습니다. CDO는 기존 FTD 기능과 다음과 같은 새로운 FTD 6.7 기능을 계속 지원합니다.

- 보안 그룹 태그 및 SGT 그룹
- Active Directory 영역 개체

CDO가 현재 지원하는 FTD 기능에 대한 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리를 참조하십시오.

버전 **6.7**의 **CDO TLS** 서버 **ID** 검색 및 **TLS 1.3**

이제 서버 인증서의 정보를 사용하여 TLS 1.3으로 암호화된 트래픽에서 URL 필터링 및 애플리케이션 제어를 수행할 수 있습니다. 이 기능이 작동하기 위해 트래픽 암호를 해독할 필요는 없습니다. 애플리케이션 또는 URL 필터링을 사용하는 액세스 규칙과 일치하도록 TLS 1.3으로 암호화된 트래픽의 경우 시스템은 TLS 1.3 인증서를 암호 해독해야 합니다. 암호화된 연결이 올바른 액세스 제어 규칙과 일치하는지 확인하려면 FDM(Firepower Device Manager)이든 FMC(Firepower Management Center)이든 관리 UI에서 **TLS** 서버 **ID** 검색을 활성화하는 것이 좋습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "Firepower Threat Defense의 TLS 서버 ID 검색"을 참조하십시오.

2020년 10월

2020년 10월 15일

새 사용자 역할

이제 CDO는 정책 수정과 정책 구축의 책임을 나누는 두 가지 추가 사용자 역할을 제공합니다. 새로운 **Edit-Only(**편집 전용**)** 역할을 통해 사용자는 디바이스의 구성을 변경할 수 있지만 이러한 변경 사

항을 구축할 수는 없습니다. 새로운 **Deploy-Only(**구축 전용**)** 역할을 통해 사용자는 보류 중인 구성 변경 사항을 구축할 수 있지만 구성을 변경할 수는 없습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FMC* 관리의 "사용자 역할"을 참조하십시오.

2020년 10월 2일

FTD API 지원

CDO는 이제 FTD 디바이스에서 고급 작업을 수행하기 위해 REST(Representational State Transfer) API(애플리케이션 프로그래밍 인터페이스) 요청을 실행할 수 있는 API 툴 인터페이스를 제공합니다. 또한 이 인터페이스는 다음 기능을 제공합니다.

- 이미 실행된 API 명령의 이력을 기록합니다.
- 재사용할 수 있는 시스템 정의 API 매크로를 제공합니다.
- 이미 실행한 명령 또는 다른 사용자 정의 매크로에서 표준 API 매크로를 사용하여 사용자 정의 API 매크로를 생성할 수 있습니다.

FTD API 툴에 대한 자세한 내용은 *Cisco Defense Orchestrator*로 *FTD* 관리의 "FTD API 툴 사용"을 참조하십시오.

2020년 9월

2020년 9월 25일

멀티 테넌트 포털 지원

이제 CDO에는 다양한 지역의 테넌트에서 디바이스의 통합 보기를 제공하는 다중 테넌트 포털이 도입되었습니다. 이 보기는 단일 창에서 테넌트의 정보를 수집하는 데 도움이 됩니다. CDO 지원 팀이 요구 사항에 따라 하나 이상의 포털을 생성하도록 할 수 있습니다.

- 다음 정보를 제공하는 Device Details(디바이스 세부 정보) 보기를 제공합니다.
  - 각 디바이스에 대한 디바이스 위치, 소프트웨어 버전, 온보딩 방법 및 기타 세부 정보를 표시합니다.
  - 해당 디바이스를 소유하는 CDO 테넌트 페이지에서 디바이스를 관리할 수 있습니다.
  - 다른 지역의 CDO 테넌트에 로그인하고 해당 디바이스를 관리할 수 있는 링크를 제공합니다.
- 포털의 정보를 쉼표로 구분된 값(.csv) 파일로 내보내 분석하거나 액세스 권한이 없는 사용자에게 전송합니다.
- API 토큰을 사용하여 새 테넌트를 원활하게 추가할 수 있습니다.

- CDO에서 로그아웃하지 않고 포털 간 전환을 허용합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "멀티 테넌트 포털 관리"를 참조하십시오.

클라우드 기반 보안 디바이스 커넥터에 대한 보안 이벤트 커넥터 지원

이제 Cisco Security Analytics and Logging(SAL SaaS) 고객은 보안 디바이스 커넥터가 Cisco Cloud에 설치된 경우 보안 이벤트 커넥터를 설치할 수 있습니다. Cisco Security Analytics and Logging을 구성하기 위해 더 이상 온프레미스 Secure Device Connector로 전환할 필요가 없습니다.

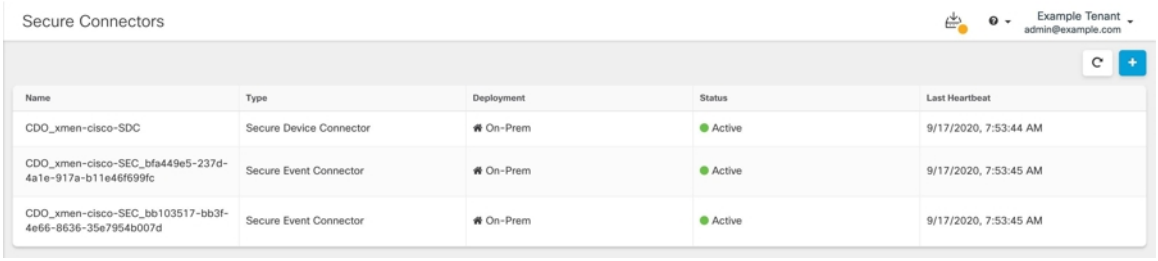
자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *Cisco Secure Firewall Cloud Native* 관리의 다음 항목을 참조하십시오.

- 보안 이벤트 커넥터 설치
- 클라우드 SDC가 있는 테넌트에 CDO 이미지를 사용하여 SEC 설치
- 클라우드 SDC가 있는 테넌트에 VM 이미지를 사용하여 SEC 설치

2020년 9월 17일

다중 보안 이벤트 커넥터 지원

SEC(Secure Event Connector)는 ASA 및 FTD에서 Cisco Cloud로 이벤트를 전달하므로 Cisco SAL SaaS(Security Analytics and Logging) 라이선싱에 따라 Event Logging(이벤트 로깅) 페이지에서 이벤트를 보고 Secure Cloud Analytics로 조사할 수 있습니다. 둘 이상의 SEC를 사용하면 서로 다른 위치에 설치하고 Cisco Cloud에 이벤트를 전송하는 작업을 배포할 수 있습니다.



테넌트에 추가 SEC를 설치하는 방법을 알아보려면 다음 문서를 참조하십시오.

- 온프레미스 SDC가 있는 테넌트에 CDO 이미지를 사용하여 여러 SEC 설치
- VM 이미지를 사용하여 여러 SEC 설치

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *Cisco Secure Firewall Cloud Native* 관리의 "Cisco Security Analytics 및 로깅"을 참조하십시오.

2020년 8월

2020년 8월 20일

Firepower Management Center 지원

이제 CDO는 버전 6.4 이상을 실행하는 FMC(Firepower Management Center) 및 모든 매니지드 디바이스를 온보딩할 수 있습니다. FMC 지원은 FMC 온보딩, FMC에서 관리하는 디바이스 보기, FMC UI 교차 실행으로 제한됩니다.

CDO가 FMC 어플라이언스를 관리하는 방법을 검토하려면 *Cisco Defense Orchestrator를 사용하여 FMC 관리*를 참조하십시오.

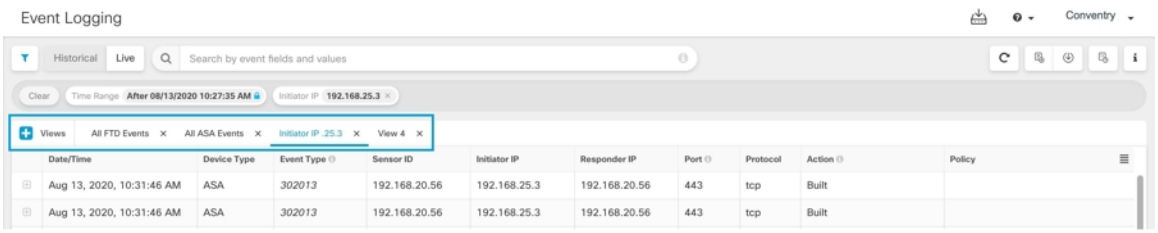
FMC 온보딩에 대한 자세한 내용은 *Cisco Defense Orchestrator를 사용하여 FMC 관리*의 "FMC 온보딩"을 참조하십시오.

지원되는 FMC 하드웨어 및 소프트웨어 버전을 검토하려면 *Cisco Defense Orchestrator를 사용하여 FMC 관리*에서 "CDO의 소프트웨어 및 하드웨어 지원"을 참조하십시오.

사용자 지정 가능한 이벤트 필터

Cisco SAL SaaS(Security Analytics and Logging) 고객은 반복 사용을 위해 Event Logging(이벤트 로깅) 페이지에서 맞춤형 이벤트 필터를 생성하고 저장할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator를 사용하여 Cisco Secure Firewall Cloud Native 관리*의 "맞춤형 이벤트 필터"를 참조하십시오.



이벤트 로깅 페이지의 향상된 검색 기능

Cisco Security Analytics and Logging(SAL SaaS) 고객은 이제 Event Logging(이벤트 로깅) 페이지의 검색 기능에 대한 다음과 같은 개선 사항을 활용할 수 있습니다.

- 요소 속성을 클릭하여 검색 필드에 추가합니다.

- Event Logging(이벤트 로깅) 페이지의 열을 끌어 놓아 원하는 방식으로 이벤트 정보를 확인합니다.
- Event Logging(이벤트 로깅) 페이지의 새로운 AND NOT 및 OR NOT 검색 연산자는 더욱 세분화된 이벤트 검색 기능을 제공합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *Cisco Secure Firewall Cloud Native* 관리의 "이벤트 로깅에서 이벤트 검색 및 필터링"을 참조하십시오.

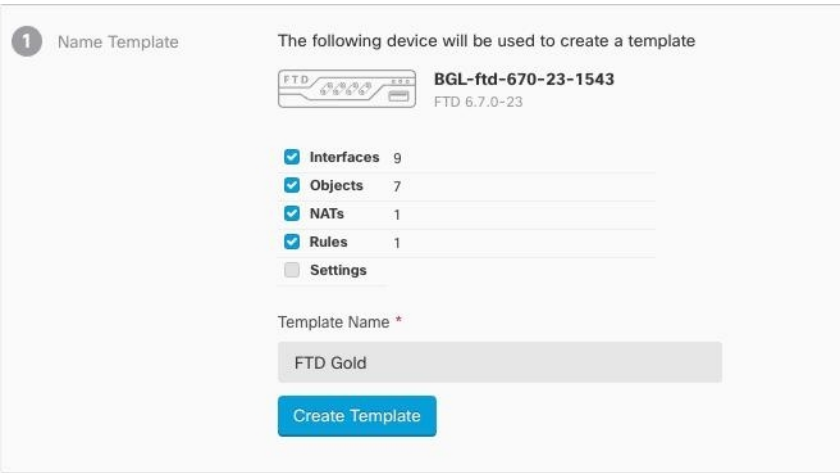
2020년 8월 13일

사용자 지정 충돌 탐지 폴링 간격

이제 디바이스 유형 또는 이전에 구성한 폴링 간격과 상관없이 디바이스별로 맞춤형 폴링 간격을 구성할 수 있습니다. 여기에는 디바이스 상태 또는 탐지된 대역 외 변경 사항에 대한 탐지가 포함됩니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "디바이스 변경에 대한 폴링 예약"을 참조하십시오.

맞춤형 **FTD** 템플릿

이제 온보딩된 FTD 디바이스 구성에서 하나 이상의 부분(액세스 규칙, NAT 규칙, 설정, 인터페이스 및 개체)을 선택하여 맞춤형 FTD 템플릿을 생성할 수 있습니다. 다른 FTD에 맞춤형 템플릿을 적용하면 포함된 부분을 기반으로 기존 구성이 유지, 업데이트 또는 제거됩니다. 그러나 CDO에서는 모든 부분을 선택하여 완전한 템플릿을 생성하고 다른 FTD에 적용할 수 있습니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD 템플릿"을 참조하십시오.



2020년 7월

2020년 7월 30일

개체 재정의

CDO는 사용자가 지정한 장치에 사용하는 공유 네트워크 개체에 대한 대체 값을 제공할 수 있는 "개체 재정의"를 도입합니다. 필요한 경우 개별 디바이스의 정책을 바꾸지 않고도 디바이스 전반에 걸쳐 사용이 가능한 작은 공유 정책 집합을 생성할 수 있습니다. 개체 재정의를 사용하면 공유 정책 또는 규칙 집합에서 사용하는 일부 또는 모든 디바이스에서 재정의할 수 있는 개체를 생성할 수 있습니다.

개체를 재정의하려면 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "개체 재정의"를 참조하십시오.

향상된 네트워크 그룹 마법사

새 네트워크 개체를 즉시 생성하고 기존 개체를 수정할 수 있도록 네트워크 그룹 편집 마법사가 개선되었습니다. 또한 공유 네트워크 그룹이 정의된 디바이스에 디바이스별 추가 값을 추가할 수 있습니다.

네트워크 그룹 마법사의 개선 사항에 대한 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "Firepower 네트워크 개체 또는 네트워크 그룹 생성 또는 수정" 및 ASA 네트워크 개체 및 네트워크 그룹 생성 또는 수정"을 참조하십시오.

2020년 7월 9일

RA VPN 및 이벤트 보기 사용자 지정

이제 RA VPN(Remote Access Virtual Private Network)에 대해 생성된 테이블과 라이브 및 기록 이벤트 보기를 모두 사용자 지정할 수 있습니다. 요구 사항에 가장 적합하고 포트폴리오에 중요한 방식으로 테이블을 구성하고 저장합니다.

사용자 지정과 관련된 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 다음 섹션을 참조하십시오.

- 원격 액세스 VPN 모니터링 보기 사용자 지정
- CDO의 기록 이벤트 보기

2020년 7월 2일

SecureX

이제 CDO를 SecureX에 통합하여 디바이스, 정책 및 테넌트당 적용된 개체의 요약을 제공하여 보안 포트폴리오 전반에서 가시성 및 자동화를 강화할 수 있습니다. CDO 및 SecureX를 통합하는 방법에 대한 자세한 내용은 SecureX를 참조하십시오.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *Cisco Secure Firewall Cloud Native* 관리의 다음 항목을 참조하십시오.

- SecureX 및 CDO
- CDO에서 SecureX 연결

Cisco Security Analytics and Logging(SAL SaaS) 이벤트 다운로드

Event Logging(이벤트 로깅) 페이지에서 ASA 및 FTD 이벤트를 필터링한 후 이제 압축된 .CSV 파일로 결과를 다운로드할 수 있습니다.

- downloadable.CSV 파일에 추가하는 이벤트는 시간 범위로 정의됩니다.
- 단일 .CSV 파일은 최대 약 50GB의 압축 정보를 수용할 수 있습니다.
- 다운로드 가능한 파일의 생성은 병렬로 수행할 수 있습니다.
- 생성된 .CSV 파일은 Cisco Cloud에 저장되며 여기에서 직접 다운로드됩니다. 이러한 파일은 CDO/Secure Cloud Analytics 서버 리소스를 사용하지 않습니다.
- 완료된 downloadable.CSV 파일은 7일 동안 저장된 후 삭제됩니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *Cisco Secure Firewall Cloud Native* 관리의 "이벤트 다운로드"를 참조하십시오.

2020년 6월

2020년 6월 18일

Firepower Threat Defense 개요 보고서

이제 온보딩된 일부 또는 모든 Firepower Threat Defense(FTD) 디바이스에서 맞춤형 개요 보고서를 생성할 수 있습니다. 이 보고서는 암호화된 트래픽, 인터셉트된 위협, 탐지된 웹 범주 등의 운영 통계 모음을 표시합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 다음 항목을참조하십시오.

- FTD 개요 보고서
- 보고서 관리

Cisco Security Analytics and Logging 개선 사항

ASA 시스템 로그 및 **NSEL** 이벤트 지원

ASA의 이벤트 로깅을 지원하도록 Cisco Security Analytics and Logging(Cisco Security Analytics 및 로깅)이 크게 확장되었습니다.

- **ASA** 로깅: SAL SaaS(Security Analytics and Logging)는 이제 관리 방법에 관계없이 모든 Cisco ASA 방화벽에서의 로깅을 지원합니다. 사용자는 ASA 로그를 시스템 로그 형식, NSEL(NetFlow Security Event Logs) 형식 또는 둘 다로 전송할 수 있습니다. 로깅 분석을 활성화하려는 고객은 상위 계층 SAL 라이선스에 필요한 텔레메트리를 제공하기 위해 NSEL 로그를 활성화해야 합니다.

  기존 FTD 로깅 외에도 CDO는 Cisco 보안 포트폴리오의 첫 번째 제품으로 Cisco의 전체 방화벽 플릿에 대한 로깅을 집계하고 통합합니다.

  자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리에서 다음 항목을 참조하십시오.

  - ASA 디바이스에 대한 Cisco Security Analytics and Logging
  - ASA 디바이스에 대한 Cisco Security Analytics and Logging 구현

- 장기 저장 및 다운로드: 사용자는 이제 SAL을 처음 주문할 때 또는 나중에 애드온으로 1년, 2년 또는 3년 동안 로그를 저장하도록 선택할 수 있습니다. 방화벽 로깅의 기본 보존 기간은 90일로 유지됩니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "보안 애널리틱스 및 로깅 이벤트 스토리지"를 참조하십시오.

- 트래픽 분석: FTD 연결 레벨 로그 및 ASA(NSEL) 로그는 모두 SAL의 트래픽 분석을 통해 실행할 수 있으며, 관찰 및 알림은 SecureX 로그인을 사용하여 Secure Cloud Analytics에 교차 실행하여 검토할 수 있습니다. 시스템 로그를 기록하는 ASA 고객만 트래픽 분석을 활성화하기 위해 NSEL 로그로 전환해야 합니다. Logging Analytics and Detection 및 Total Network Analytics and Detection 라이선스를 취득한 고객은 추가 비용 없이 분석을 위해 Secure Cloud Analytics 포털을

프로비저닝하고 사용할 수 있습니다. Secure Cloud Analytics 탐지 항목에는 SAL 사용자가 Secure Cloud Analytics 핵심 기능의 일부로 사용할 수 있는 기타 탐지 항목 외에도 방화벽 로깅 데이터를 사용하여 특별히 활성화된 관찰 및 알림이 포함됩니다. 기존 기록 및 트러블슈팅 라이선스 보유자는 30일 동안 약정 없이 상위 라이선스의 탐지 기능을 테스트할 수 있습니다.

- 무료 평가판: 이 양식을 작성하여 모든 라이선스에 대해 약정 없는 30일 SAL 평가판을 시작할 수 있습니다. 이 로우 터치 평가판에는 클라우드로 데이터를 내보내는 데 필요한 최소 온프레미스 커넥터 집합만 필요합니다. 이 평가판을 사용하여 SAL 기능을 평가하고 프로덕션 환경을 지원하는 데 필요한 데이터 볼륨을 예측할 수 있습니다. 이는 SAL 라이선스에 대한 적절한 일일 볼륨을 구매하기 위한 선행 단계입니다. 이를 위해 SAL 평가판은 대부분의 사용자 볼륨에 대한 데이터를 조절하지 않습니다. 또한 예상 툴을 사용하면 SAL 일일 볼륨을 예측할 수 있습니다.

보안 분석 및 로깅을 위한 향상된 이벤트 모니터링

- 이제 CDO의 Event Logging(이벤트 로깅) 페이지에서 ASA 이벤트를 유형별로 필터링할 수 있습니다. 모든 시스템 로그 이벤트 또는 NSEL 이벤트를 개별적으로 또는 함께 볼 수 있습니다.
- 대부분의 ASA 시스템 로그 이벤트는 구문 분석되어 이벤트에 대한 자세한 정보를 제공합니다. 이 세부 정보는 Secure Cloud Analytics에서 이벤트를 분석하는 데 사용할 수 있습니다.
- 보려는 정보 열만 표시하고 나머지는 숨김으로써 Event Logging(이벤트 로깅) 페이지의 보기를 맞춤화할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "이벤트 로깅에서 이벤트 필터링"을 참조하십시오.

2020년 6월 4일

원격 액세스 **VPN** 세션 모니터링 및 종료

이제 CDO를 사용하여 테넌트의 모든 ASA(Adaptive Security Appliance) 및 FTD(Firepower Threat Defense) VPN 헤드엔드 전반에서 라이브 AnyConnect Remote Access VPN 세션을 모니터링할 수 있습니다. 총 활성 VPN 세션 수, 현재 연결된 사용자 및 세션 수, 수신 및 전송된 데이터의 양에 대한 정보를 수집합니다.

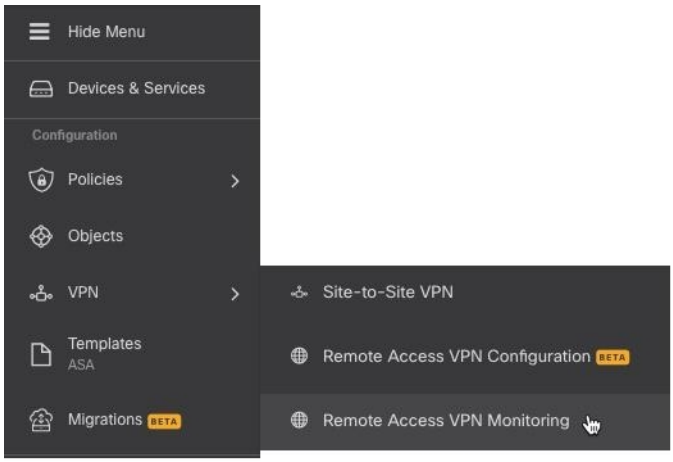
테넌트에서 각 RA VPN 헤드엔드의 성능을 보고, 헤드엔드별로 세션을 필터링하고, VPN 모니터링 테이블에서 보려는 세션 속성을 선택할 수 있습니다. 또한 하나 이상의 디바이스의 RA VPN 세션을 쉼표로 구분된 값(.csv) 파일로 내보낼 수 있습니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *Cisco Secure Firewall Cloud Native* 관리의 "CSV 파일로 RA VPN 세션 내보내기"를 참고하십시오.

ASA에서 단일 사용자의 모든 활성 RA VPN 세션을 종료하고 ASA에서 모든 사용자의 모든 활성 RA VPN 세션을 종료할 수 있습니다.

자세한 내용은 다음 주제를 참고하십시오.

- *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 ASA에서 활성 RA VPN 세션 연결 끊기
- *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 FTD에서 활성 RA VPN 세션 연결 끊기

VPN > Remote Access VPN Monitoring(원격 액세스 **VPN** 모니터링**)**을 클릭하여 탐색 모음에서 Remote Access VPN Monitoring(원격 액세스 VPN 모니터링) 화면을 엽니다.



AWS Virtual Private Cloud Management - 무료 평가판

CDO에서 90일 동안 무료로 AWS VPC를 관리해 보십시오. CDO에서 Devices & Services(디바이스 및 서비스) 페이지를 열고 AWS VPC를 온보딩하여 시작합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *AWS* 관리의 "AWS VPC 온보딩"을 참조하십시오.

새로운 기능 타일

이제 CDO 랜딩 페이지에 최신 기능과 CDO가 해당 기능을 구현한 시기를 보여주는 새로운 기능 타일이 있습니다. 관심 있는 기능이 있는 경우 기능의 제목을 클릭하여 해당 기능에 대한 설명서를 읽어보십시오.

2020년 5월

2020년 5월 20일

새 **API** 전용 사용자

이제 CDO를 통해 슈퍼 관리자는 CDO REST API 호출 시 CDO에 인증하기 위한 API 토큰을 생성하는 데 사용할 수 있는 "API 전용 사용자"를 생성할 수 있습니다. 이 사용자 어카운트 및 해당 API 토큰은 원래 슈퍼 관리자가 조직을 떠난 후에도 계속 작동합니다.

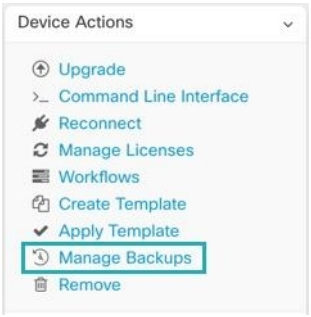
자세한 내용은 Cisco Defense Orchestrator를 사용하여 FTD 관리의 "API 전용 사용자 생성"을 참조하십시오.

2020년 5월 7일

Firepower Threat Defense 디바이스 백업

이제 CDO를 사용하여 FTD(Firepower Threat Defense)의 시스템 구성을 백업할 수 있습니다. CDO를 사용하여 다음을 수행할 수 있습니다.

- 온디맨드 방식으로 디바이스를 백업합니다.
- 매일부터 매달 선택한 시간에 주기로 반복 백업을 예약합니다.
- 백업을 다운로드하고 FDM(Firepower Device Manager)을 사용하여 복원합니다.



자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD 백업"을 참조하십시오.

2020년 4월

2020년 4월 16일

Firepower Threat Defense 6.6.0을 실행하는 디바이스에 대한 **CDO** 지원

이제 CDO에서 FTD 6.6.0 디바이스를 관리합니다. 다음은 CDO가 제공하는 새로운 지원 측면입니다.

- Firepower Threat Defense(FTD) 6.6.0을 실행하는 디바이스 온보딩
- FTD 6.4.x 이상 디바이스를 FTD 6.6.0 디바이스로 업그레이드 디바이스는 개별 FTD 또는 고가용성 쌍으로 구성된 FTD일 수 있습니다. 다음 주의 사항은 업그레이드 지원에 적용됩니다.
  - Firepower 4100 및 Firepower 9300 디바이스에 대한 업그레이드는 현재 지원되지 않습니다.
  - 고객은 CDO의 업그레이드 페이지에 있는 드롭다운을 사용하여 FTD 6.6.0으로 업그레이드할 수 있습니다.
- CDO는 FTD 기능에 대한 지원을 지속적으로 개발하고 새로운 기능 지원이 준비되는 대로 릴리스합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "Firepower Threat Defense 지원 세부 사항"을 참조하십시오.

2020년 4월 9일

Firepower Threat Defense 명령줄 인터페이스

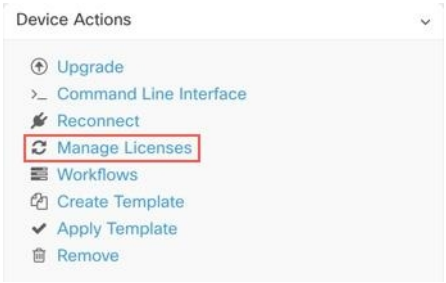
이제 CDO에서 직접 FTD 디바이스에 CLI 요청을 실행할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*로 *FTD* 관리의 "CDO 명령줄 인터페이스 사용"을 참조하십시오.

2020년 4월 2일

Firepower Threat Defense 디바이스용 라이선스 관리 개선

이제 FTD 디바이스 라이선스 정보 보기, 라이선스 활성화 및 비활성화, 라이선스 새로 고침을 모두 Devices & Services(디바이스 및 서비스) 페이지의 Device Actions(디바이스 작업) 창에서 단일 버튼으로 관리할 수 있습니다.



2020년 3월

2020년 3월 26일

FTD 보안 데이터베이스 업데이트

CDO를 사용하면 FTD 디바이스를 온보딩할 때 보안 데이터베이스를 즉시 업데이트하는 동시에 향후 업데이트를 예약할 수 있습니다. 이 기능은 SRU, SI(보안 인텔리전스), VDB(취약성) 및 지리위치 데이터베이스를 업데이트합니다. 향후 업데이트는 온보딩 프로세스의 일부로만 예약할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD 보안 데이터베이스 업데이트"를 참조하십시오.

FTD 서비스 개체의 포트 범위 지원

이제 CDO는 다양한 포트 번호를 포함하는 서비스 개체(FTD에서는 포트 개체라고도 함) 생성을 지원합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "Firepower 서비스 개체 생성 및 편집"을 참조하십시오.

2020년 3월 24일

Cisco Secure 로그인 도메인 마이그레이션

2020년 3월 24일 화요일 오후 5시(태평양 일광 절약 시간)에 Cisco Security Single Sign-on 솔루션의 공식 도메인이 https://security.cisco.com에서 https://sign-on.security.cisco.com(으)로 이동되었습니다.

저장된 링크를 업데이트하고 비밀번호 관리자가 새 URL을 참조하도록 업데이트하는 것이 좋습니다.

이렇게 하면 짧은 기간 동안 CDO에 대한 액세스가 제한되지만, 로컬 디바이스 관리자 또는 SSH 연결을 사용하여 업데이트를 수행하는 기능은 제한되지 않습니다.

문제가 발생하는 경우 기술 지원을 제공할 수 있는 Cisco TAC에 문의하십시오.

2020년 3월 12일

FTD 규칙 집합

CDO에 Firepower Threat Defense 디바이스용 규칙 집합이 도입되었습니다. 규칙 집합은 여러 FTD 디바이스에서 공유할 수 있는 액세스 제어 규칙의 모음입니다. 규칙 집합의 규칙에 대한 모든 변경 사항은 해당 규칙 집합을 사용하는 다른 FTD 디바이스에 영향을 미칩니다. FTD 정책은 디바이스별(로컬) 규칙과 공유(규칙 집합) 규칙을 모두 포함할 수 있습니다. FTD 디바이스의 기존 규칙에서 규칙 집합을 생성할 수도 있습니다.

이 기능은 현재 Firepower Threat Defense 6.5 이상 릴리스를 실행하는 디바이스에서 사용할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD 규칙 집합"을 참조하십시오.

2020년 3월 5일

FTD 정책 내에서 또는 다른 **FTD** 정책으로 규칙 복사 또는 이동

이제 한 FTD의 정책에서 다른 FTD의 정책으로 규칙을 복사하거나 이동할 수 있습니다. 또한 규칙이 네트워크 트래픽을 평가하는 순서를 세부적으로 조정할 수 있도록 FTD 정책 내에서 규칙을 더 쉽게 이동할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD 액세스 제어 규칙 복사" 및 "FTD 액세스 제어 규칙 이동"을 참조하십시오.

FTD 버전 **6.5** 이상으로의 **AnyConnect** 소프트웨어 패키지 업로드

이제 CDO의 원격 액세스 VPN 마법사를 사용하여 원격 서버에서 FTD 6.5 이상을 실행하는 FTD(Firepower Threat Defense) 디바이스로 AnyConnect 패키지를 업로드할 수 있습니다. 원격 서버가 HTTP 또는 HTTPS 프로토콜을 지원하는지 확인합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD 버전 6.5 이상을 실행하는 FTD 디바이스에 AnyConnect 소프트웨어 패키지 업로드"를 참조하십시오.

2020년 3월 3일

CDO 인터페이스의 용어 업데이트

디바이스를 관리하려면 CDO(Cisco Defense Orchestrator)의 자체 데이터베이스에 디바이스 구성 복사본이 저장되어 있어야 합니다. CDO는 구성을 "읽을 때" 디바이스에 저장된 구성의 복사본을 만들어 CDO의 데이터베이스에 저장합니다. 읽기 작업을 수행할 때 수행 중인 작업을 더 잘 설명하기 위해 일부 인터페이스 옵션의 이름을 변경했습니다.

새로운 용어는 다음과 같습니다.

- 변경 사항 확인. 디바이스의 구성 상태가 Synced(동기화됨)인 경우 Check for Changes(변경 사항 확인) 링크를 사용할 수 있습니다. Check for Changes(변경 사항 확인)를 클릭하면 CDO가 디바이스 구성의 복사본을 디바이스 구성의 복사본과 비교하도록 지시합니다. 차이가 있는 경우 CDO는 디바이스에 저장된 복사본으로 디바이스 구성의 복사본을 즉시 덮어씁니다.
- 변경 사항 취소. 디바이스의 구성이 Not Synced(동기화되지 않음)인 경우 Discard Changes(변경 사항 취소)를 클릭하면 CDO가 디바이스 구성 복사본에 적용한 모든 변경 사항이 삭제되고 디바이스에 있는 구성의 복사본으로 덮어씁니다.
- 검토 없이 수락.이 작업은 CDO의 디바이스 구성 복사본을 디바이스에 저장된 구성의 복사본으로 덮어씁니다. CDO는 작업을 확인하라는 메시지를 표시하지 않습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "구성 변경 사항 읽기, 삭제, 확인 및 구축"을 참조하십시오.

2020년 2월

2020년 2월 6일

Firepower 1010에 대한 스위치 포트 모드 지원

이제 CDO는 Firepower 1010 디바이스에 대한 스위치 포트 모드 기능을 완벽하게 지원합니다.

구성 지침 및 제한 사항에 대한 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD에 대한 스위치 포트 모드 인터페이스" 및 "스위치 포트 모드에 대한 FTD VLAN 구성"을 참조하십시오.

2020년 1월

2020년 1월 22일

사이트 대 사이트 연결을 위한 동적 피어 지원

이제 피어의 VPN 인터페이스 중 하나에 동적 IP 주소가 있는 경우 두 피어 간에 사이트 간 VPN 터널을 구성할 수 있습니다. 이 동적 피어는 매니지드 FTD 디바이스 또는 엑스트라넷 디바이스일 수 있습니다.

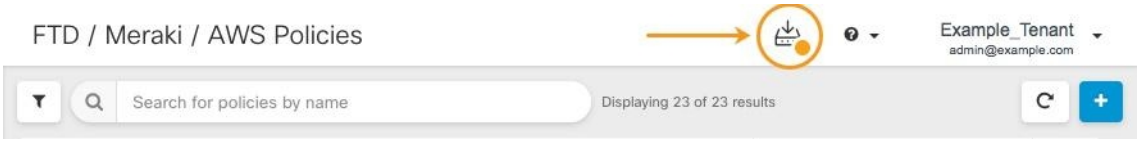
자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "동적으로 주소가 지정된 피어를 사용하여 사이트 간 VPN 연결 구성"을 참조하십시오.

2020년 1월 16일

향상된 구축 경험

CDO는 구축 워크플로를 개선했습니다. 이제 추가 구축 아이콘이 CDO 전체에서 표시됩니다. 더 이상 구성 변경 사항을 구축하기 위해 Devices & Services(디바이스 및 서비스) 페이지로 돌아갈 필요가 없습니다.

구축 아이콘에 주황색 점이 포함되어 있으면 CDO로 관리하는 디바이스 중 하나 이상(구축 준비가 된 디바이스)이 하나 이상 변경되었음을 나타냅니다.



자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축"을 참조하십시오.

대량 작업 취소

이제 여러 디바이스에서 수행한 활성 대량 작업을 취소할 수 있습니다. 예를 들어 4개의 매니지드 디바이스를 다시 연결하려고 시도했는데 그 중 3개의 디바이스가 성공적으로 다시 연결되었지만 네 번째 디바이스는 다시 연결에 성공하거나 실패하지 않았습니다. 이제 **Jobs(**작업**)** 페이지로 이동하여 진행 중인 대량 작업을 찾은 다음 Cancel(취소)을 클릭하여 작업을 중지할 수 있습니다.