



## 2016의 주요 기능

---

이 문서에서는 2016년에 Cisco Defense Orchestrator에 추가된 몇 가지 기능에 대해 설명합니다.

- [2016년 12월, on page 1](#)
- [2016년 11월, on page 2](#)
- [2016년 9월, on page 2](#)
- [2016년 8월, on page 4](#)

### 2016년 12월

#### 2016년 12월 22일

##### **NAT** 정책 관리

이제 Cisco Defense Orchestrator에서는 사용하기 쉬운 탐색 마법사 및 고급 인터페이스 기반 다이어그램을 통해 NAT 정책 읽기, 수정, 검색 및 생성을 지원하여 ASA 디바이스에 정의된 NAT 정책(및 해당 순서)의 전체 목록을 표시합니다.

#### 2016년 12월 15일

##### 사용되지 않는 이름(개체) 변환

디바이스의 구성에 레거시(사용되지 않는) 이름이 포함되어 있습니까? 이제 Cisco Defense Orchestrator에서는 개체 문제를 해결하는 동안 개체, 개체 그룹 및 이름 전체를 조사하여 정책에 사용되는 모든 개체의 일관성을 제공하고 이름을 개체로 변환하는 작업을 지원합니다.

## 2016년 11월

### 2016년 11월 18일

완전하게 새도입된 규칙 지원

모든 트래픽은 규칙 집합 순서대로 규칙에 의해 처리되므로, 이제 의도된 트래픽을 처리하지 않는 불필요한 네트워크 정책을 필터링하고 식별할 수 있습니다. 네트워크 정책을 변경하면 CDO는 편집되거나 추가된 규칙이 다른 규칙에 의해 새도입되는 경우 경고를 보냅니다.

### 2016년 11월 8일

온프레미스 보안 디바이스 커넥터

Cisco Defense Orchestrator는 CDO와 지원되는 디바이스 및 서비스 간의 직접 통신을 활성화합니다. 이 통신은 원격 위치와 CDO 클라우드 서비스 간의 프록시 역할을 하는 CDO SDC(Secure Device Connector)에 의해 활성화됩니다. 이 서비스는 이제 다음과 같은 두 가지 구축 모델에서 사용할 수 있습니다.

**On-Prem Secure Device Connector** - On-Prem Secure Device Connector는 요청된 계정 전용으로 사전 구성된 가상 어플라이언스입니다.

클라우드 보안 디바이스 커넥터 - 모든 클라우드 보안 디바이스 커넥터는 Cisco Defense Orchestrator 팀에서 자동으로 프로비저닝되고 관리됩니다.

## 2016년 9월

### 2016년 9월 29일

변경 로그

온보딩된 디바이스 및 서비스 전체에서 단일 보기 내에서 Cisco Defense Orchestrator를 통해 수행되는 애플리케이션(layer7) 및 네트워크(layer3) 정책 변경 사항을 지속적으로 캡처합니다. 새로운 변경 로그는 최신 변경 사항을 한눈에 볼 수 있도록 나열하며, 디바이스, 변경 상태, 사용자 등을 기준으로 추가 수정을 정렬하고 필터링할 수 있습니다. 새로운 변경 로그 기능을 통해 조직은 다음을 수행할 수 있습니다.

- 네트워크 및 애플리케이션 정책 변경(신규, 수정 및 삭제된 규칙, 온보딩 또는 삭제된 디바이스 및 서비스 등)의 인라인 증분 보기(diff) 전과 후
- 정책 변경 충돌(Cisco Defense Orchestrator 외부에서 발생) 및 디바이스 또는 서비스에 대한 덮어쓰기 탐지

- 사고 조사 또는 트러블슈팅 중에 사용자, 대상 및 시기에 대한 답변 가능
- 공통 형식 또는 서드파티 모니터링 시스템으로 내보내기



**Note** 현재 Cisco Defense Orchestrator에서 관리하는 디바이스 및 서비스는 처음 구축하거나 읽은 후에만 변경 로그 이벤트 수집을 시작합니다. 자세한 내용은 [Cisco Defense Orchestrator를 사용하여 FTD 관리](#)의 "FTD 디바이스에 대한 보안 로깅 분석"을 참조하십시오.

적중률. 이제 Cisco Defense Orchestrator를 사용하면 네트워크 운영 사용자가 안전하고 확장 가능한 정책 오케스트레이션 외에 정책 규칙 결과를 평가할 수 있으므로, 클라우드의 단일 창에서 보다 정확한 정책 분석 및 근본 원인에 대한 즉각적인 조치 가능한 피벗을 위한 간단한 시각화를 제공할 수 있습니다. 새로운 적중률 기능을 통해 조직은 다음을 수행할 수 있습니다.

- 보안 상태를 증가하는 사용되지 않는 정책 규칙을 제거합니다.
- 병목 현상을 즉시 식별하여 방화벽 성능을 최적화하고 정확하고 효율적인 우선순위를 적용합니다(가장 많이 트리거되는 정책 규칙이 우선순위가 높음).
- 구성된 데이터 보존(1년)에 대한 디바이스 또는 정책 규칙 재설정 시에도 적중률 기록 정보 유지
- 실행 가능한 정보를 기반으로 의심스러운 새도우 및 사용되지 않는 규칙에 대한 검증을 강화합니다. 업데이트 또는 삭제에 대한 의심 제거
- 사전 정의된 시간 간격(일, 주, 월, 연도) 및 실제 적중 횟수(0, >100, >100k 등)를 활용하여 전체 정책에 대한 컨텍스트에서 정책 규칙 사용을 시각화하여 네트워크를 통과하는 패킷에 대한 영향을 평가

## 2016년 9월 23일

사용자 인터페이스 재설계: 밝은 테마로 변경

Cisco Defense Orchestrator 사용자 경험을 보다 직관적이고 쉽게 설명할 수 있는 Cisco 스타일로 조정된 새로운 사용자 경험 테마로 재설계합니다. 사용해 보십시오!

다중 개체 지원

이제 Cisco Defense Orchestrator 개체 관리를 사용하면 개체 및 개체 그룹 값을 인라인으로 편집할 수 있을 뿐만 아니라 단일 액세스 목록 매개변수에서 여러 개체를 참조할 수 있습니다. 사용자 정의 개체 그룹에 자동으로 할당합니다(dm\_inline\_\* 개체 생성 필요 없음).

대역외 정책 수정 승인 또는 거부

수행된 원격 변경 사항 또는 변경 사항(디바이스 또는 서비스에서)을 식별할 뿐만 아니라 식별된 대역 외 변경 사항을 실시간으로 승인하거나 거부하는 기능을 통해 정책 오케스트레이션 적용을 개선합니다.

## 2016년 8월

### 2016년 8월 18일

#### 위임 관리자 지원

위임 관리자 지원. Cisco Defense Orchestrator를 사용하면 할당된 계정 간에 더 쉽고 빠르게 피벗할 수 있도록 사용자당 둘 이상의 단일 계정(테넌트)을 관리할 수 있으며, 계정 보안을 유지하고 계정(테넌트) 간에 완전한 데이터를 분리할 수 있습니다.

#### 사전 정의 템플릿 가져오기 및 내보내기

사전 정의된 템플릿 가져오기를 활성화합니다. 조직에서 사용하거나 서드파티에서 제공하는 사전 정의된 디바이스 구성 템플릿을 활용하여 조직의 모든 디바이스 및 서비스를 온보딩하는 확장 가능한 오케스트레이션을 활성화합니다.

#### 디바이스 및 서비스 연결 상태 관리

디바이스 연결 상태 평가. 디바이스 및 서비스 가용성 상태를 지속적으로 모니터링할 수 있도록 새로운 "Reconnect(다시 연결)" 버튼이 추가되었으며, 모든 변경 또는 작업에 대한 알림은 자동으로 또는 온디맨드 방식으로 수행되어야 합니다(예: 디바이스 자격 증명 업데이트, 디바이스 인증서 갱신).

### 2016년 8월 11일

#### 향상된 템플릿 관리

템플릿 개선 사항을 관리합니다. 새 디바이스 템플릿 구성 파일을 생성하거나 기존 디바이스 템플릿 구성 파일을 업데이트할 때, Cisco Defense Orchestrator 사용자는 이제 디바이스 구성 파일 전체에서 쉽게 검색할 수 있으며, 어카운트의 디바이스 전체에서 사용할 수 있도록 새 매개변수 또는 기존 매개변수에 여러 값을 할당할 수 있습니다.

. 템플릿 생성 및 관리에 대한 자세한 내용은 [Cisco Defense Orchestrator를 사용하여 FTD 관리의 "템플릿"](#)을 참조하십시오.

## 번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.