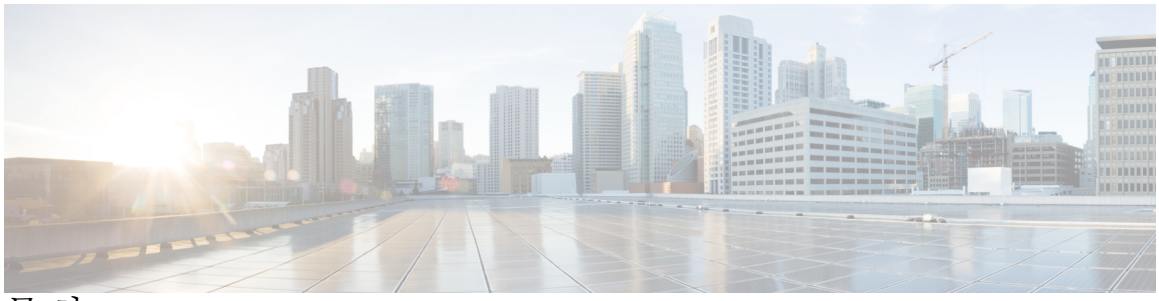
# Cisco Defense Orchestrator를 사용한 ASA 관리

초판: 2021년 3월 10일

최종 변경: 2022년 5월 12일

**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



# 목 차

# Cisco Defense Orchestrator를 사용한 ASA 관리



# Cisco Defense Orchestrator를 사용한 ASA 관리

CDO(Cisco Defense Orchestrator)는 모든 ASA 디바이스에서 간단하고 일관되며 안전한 보안 정책 관리 방법을 제공하는 클라우드 기반의 다중 디바이스 관리자입니다.

이 문서의 목표는 CDO(Cisco Defense Orchestrator)를 처음 사용하는 고객에게 개체 및 정책을 표준화하고, 매니지드 디바이스를 업그레이드하고, VPN 정책을 관리하고, 원격 작업자를 모니터링하는 데 사용할 수 있는 활동의 개요를 제공하는 것입니다. 이 문서에서는 다음 사항을 가정합니다.

- 30일 평가판 계정을 개설했거나 CDO를 구매했으며 Cisco에서 CDO 테넌트를 생성했습니다.
- Cisco Defense Orchestrator의 사용자 역할 사용자에 대한 새 CDO 테넌트에 대한 초기 로그인, 34 페이지을(를) 설정했습니다.
- ASA가 이미 구성되어 있으며 엔터프라이즈에서 사용 중입니다.
- CDO에서 관리하려는 ASA를 인터넷에서 직접 액세스할 수 없는 경우 네트워크에서 SDC(Secure Device Connector)를 구축해야 합니다. SDC는 CDO와 ASA 간의 통신을 관리합니다. 자세한 내용은 CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축, 8 페이지 또는 자체 VM에 보안 디바이스 커넥터 구축, 12 페이지를 참고하십시오.

디바이스 오케스트레이션 활동의 개요에 따라 이 문서에서는 CDO의 CLI 인터페이스, 변경 로그, 공용 REST API를 소개하고 CDO가 디바이스에서 관리할 수 있는 기타 기능에 대한 요약을 제공합니다.

시작하기

### Secure Device Connectors

디바이스 자격 증명을 사용하여 CDO 를 ASA에 연결하는 경우, 네트워크에서 SDC(Secure Device Connector)를 다운로드하고 구축하여 CDO와 ASA 간의 통신을 관리하는 것이 모범 사례입니다. ASA는 모두 디바이스 자격 증명을 사용하여 CDO에 온보딩할 수 있습니다. SDC가 ASA와 CDO 간의 통신을 관리하는 것을 원치 않고 인터넷에서 직접 디바이스에 액세스할 수 있는 경우, 네트워크에 SDC를 설치할 필요가 없습니다. Cloud Connector를 사용하여 ASA를 CDO에 온보딩할 수 있습니다.

Cisco Defense Orchestrator를 사용한 ASA 관리

테넌트에 대해 둘 이상의 SDC를 구축하면 성능 저하 없이 CDO 테넌트를 사용하여 더 많은 디바이스를 관리할 수 있습니다. 단일 SDC에서 관리할 수 있는 디바이스의 수는 해당 디바이스에 구현된 기능 및 해당 구성 파일의 크기에 따라 달라집니다. 그러나 구축을 계획할 때는 1개의 SDC가 약 500개의 디바이스를 지원할 것으로 예상합니다.

SDC를 보려면 다음을 수행합니다.

1. CDO에 로그인합니다.
2. CDO 메뉴에서 **Admin(관리)** > **Secure Connector(보안 커넥터)**를 선택합니다.

### 디바이스 온보딩

대량 ASA 온보딩으로 또는 ASA 디바이스 온보딩 ASA를 CDO에 온보딩할 수 있습니다. CDO에서 지원하는 ASA 소프트웨어 및 하드웨어에 대한 자세한 내용은 ASA 지원 세부 사항, 37 페이지의 내용을 참조하십시오.

### 테넌트에서 추가 **CDO** 사용자 생성

CDO(Cisco Defense Orchestrator)에는 읽기 전용, 편집 전용, 구축 전용, 관리자, 슈퍼 관리자 등 다양한 사용자 역할이 있습니다. 사용자 역할은 각 테넌트의 각 사용자에 대해 구성됩니다. CDO 사용자가 둘 이상의 테넌트에 액세스할 수 있는 경우, 사용자 ID는 동일하지만 테넌트마다 역할이 다를 수 있습니다. 인터페이스 또는 설명서에서 읽기 전용 사용자, Admin 사용자 또는 Super Admin 사용자를 언급하는 경우 특정 테넌트에 대한 사용자의 권한 수준을 의미합니다. 다양한 유형의 사용자에게 부여되는 권한에 대한 자세한 내용은 Cisco Defense Orchestrator의 사용자 역할, 70 페이지의 내용을 참조하십시오.

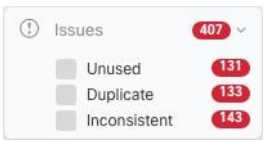
테넌트가 생성될 때 슈퍼 관리자 사용자가 자동으로 할당되었습니다. 슈퍼 관리자는 테넌트에서 다른 사용자를 생성할 수 있습니다. 이러한 새 사용자가 테넌트에 연결하려면 CDO의 사용자 레코드와 동일한 이메일 주소를 사용하는 Cisco Secure Sign-On 계정이 있거나 해당 계정을 생성해야 합니다. CDO에서 사용자 레코드를 생성하려면 사용자 역할에 대한 사용자 레코드 생성, 75 페이지의 내용을 참조하십시오.

### 정책 오케스트레이션

정책 오케스트레이션에는 개체 및 정책 검토가 포함됩니다. ASA 정책으로 작업할 때는 CDO에서 "액세스 그룹"을 "액세스 정책"이라고 합니다. ASA 액세스 정책은 CDO 메뉴 바 Policies(정책) > ASA Access Policies(ASA 액세스 정책)에서 찾을 수 있습니다.

### 네트워크 개체 문제 해결

시간이 지남에 따라 보안 디바이스에 더 이상 사용되지 않거나, 다른 개체와 중복되거나, 디바이스 간에 값이 일치하지 않는 개체가 있을 수 있습니다. 이러한 개체 문제를 해결 하 여 오케스트레이션 작업을 시작 합니다.



Cisco Defense Orchestrator를 사용한 ASA 관리

아래의 순서대로 개체 문제를 해결합니다. 초기 단계에서 수행하는 작업을 통해 이후 단계에서 해결해야 하는 문제를 해결할 수 있습니다.

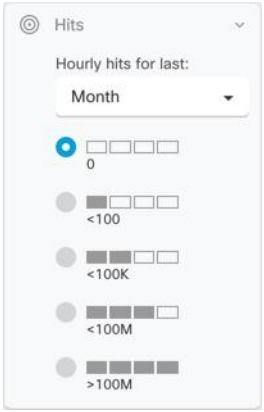
1. 사용되지 않은 개체 문제 해결 Unused objects(미사용 개체) 는 디바이스에 존재하지만 다른 개체, 액세스 목록 또는 NAT 규칙에서 참조하지 않는 개체입니다.
2. 중복 개체 문제 해결 중복 개체 는 이름은 다르지만 값은 동일한 디바이스에 있는 두 개 이상의 개체입니다. 이러한 개체는 대개 실수로 생성되고 유사한 용도로 사용되며 다른 정책에서 사용됩니다. 중복 개체 문제를 해결한 후 CDO는 유지된 개체 이름으로 영향을 받는 모든 개체 참조를 업데이트합니다.
3. 불일치 개체 문제 해결. 불일치 개체 는 두 개 이상의 디바이스에서 이름은 같지만 값이 다른 개체입니다. 사용자가 동일한 이름 및 콘텐츠를 사용하여 서로 다른 구성에서 개체를 생성하지만 시간이 지남에 따라 이러한 개체의 값이 달라지므로 불일치가 발생하는 경우가 있습니다. 이러한 현상은 보안 문제입니다. 오래된 리소스를 보호하는 규칙이 있을 수 있습니다.

### 섀도우 규칙 수정

네트워크 개체 문제를 해결했으므로 이제 섀도우 규칙에 대한 네트워크 정책을 검토하고 해결합니다. 섀도우 규칙은 ASA 액세스 정책 페이지에서 반달 모양의 배지 로 표시됩니다. 액세스 정책의 규칙은 목록에서 구성되며 위에서 아래로 한 번에 하나씩 평가됩니다. 네트워크 트래픽이 정책에서 섀도우 규칙 위의 규칙과 일치하므로 정책의 섀도우 규칙은 일치하지 않습니다. 적중되지 않는 섀도우 규칙이 있는 경우 해당 규칙을 제거하거나 ASA 네트워크 정책 편집하여 규칙을 적용합니다.

### 정책 적중률 평가

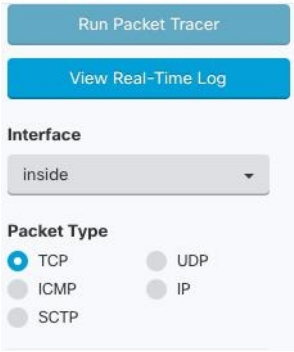
정책의 규칙이 실제로 네트워크 트래픽을 평가하는지 확인합니다. CDO는 1시간마다 정책의 규칙에 대한 적중률 데이터를 수집합니다. CDO에서 디바이스를 오래 관리할수록 특정 규칙의 적중률 데이터가 더 의미가 있습니다. 관심 있는 기간의 적중 횟수를 기준으로 ASA 액세스 정책을 필터링하여 적중 여부를 확인합니다. 그렇지 않은 경우 정책을 다시 작성하거나 삭제하는 것이 좋습니다.




### 정책 문제 해결

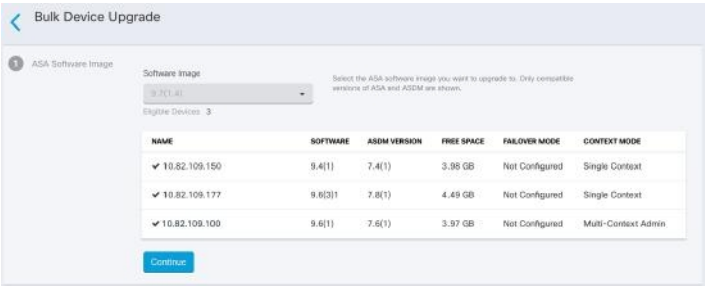
AT 패킷 트레이서를 사용하여 정책을 통해 가상 패킷의 경로를 테스트하고 규칙이 실수로 액세스를 차단하거나 허용하는지 확인할 수 있습니다.

Cisco Defense Orchestrator를 사용한 ASA 관리




### ASA 및 ASDM 업그레이드

그런 다음 최신 버전의 ASA 및 ASDM으로 업그레이드합니다. 고객은 CDO를 사용하여 ASA를 업그레이드할 때 75%~90%의 시간 절약을 보고했습니다.




CDO는 단일 상황 또는 다중 상황 모드에서 개별 ASA 또는 여러 ASA에 설치된 ASA 및 ASDM 이미지를 업그레이드할 수 있는 마법사를 제공합니다. CDO는 ASA 및 ASDM 이미지의 데이터베이스를 유지 관리합니다.

CDO는 백그라운드에서 필요한 업그레이드 호환성 검사를 수행합니다. 마법사는 호환되는 ASA 및 ASDM 이미지를 선택하고 설치하고 디바이스를 재부팅하여 업그레이드를 완료하는 프로세스를 안내합니다. CDO는 CDO에서 선택한 이미지가 ASA에 복사되고 설치된 이미지인지 확인하여 업그레이드 프로세스를 보호합니다.

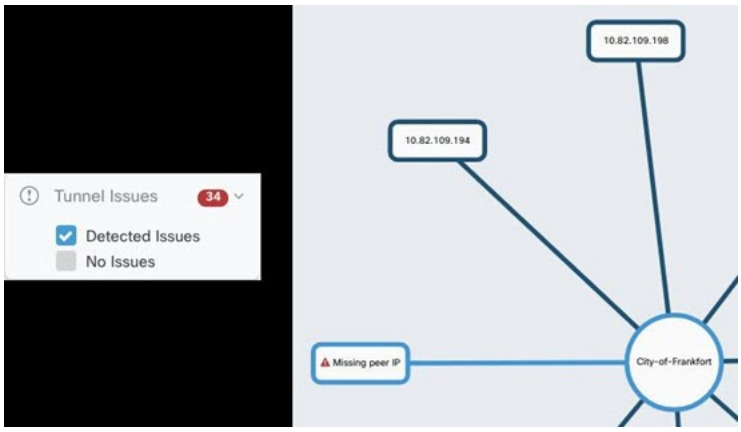
CDO는 주기적으로 데이터베이스를 검토하고 최신 ASA 및 ASDM 이미지를 추가합니다. CDO는 일반적으로 사용 가능한(GA) 이미지만 지원하며 데이터베이스에 맞춤형 이미지를 추가하지 않습니다. 목록에 특정 GA 이미지가 표시되지 않으면 지원 문의 페이지에서 Cisco TAC에 문의하십시오. 설정된 지원 티켓 SLA를 사용하여 요청을 처리하고 누락된 GA 이미지를 업로드합니다.

단일 ASA에서 ASA 및 ASDM 이미지 업그레이드, 161 페이지을 검토한 다음 자체 저장소의 이미지를 사용하여 여러 ASA 업그레이드, 160 페이지에서 ASA 업그레이드에 대해 자세히 알아보십시오.

### VPN 연결 모니터링 및 관리

#### 사이트 간 VPN 문제 검토

CDO는 네트워크의 ASA 디바이스에 존재하는 VPN 문제를 보고합니다. VPN 피어 목록을 표시 하는 테이블 또는 허브 및 스포크 토폴로지의 VPN 연결을 표시 하는 맵 등 두 가지 방법으로 환경을 볼 수 있습니다. 필터 사이드바를 사용하여 주의가 필요한 VPN 터널을 검색합니다.




CDO를 사용하여 VPN 터널 평가:

- 사이트 투 사이트 VPN 터널 연결 확인
- 누락된 피어가 있는 VPN 터널 찾기
- 암호화 키 문제가 있는 VPN 피어 찾기
- 터널에 대해 정의된 불완전하거나 잘못 구성된 액세스 목록 찾기
- 터널 구성에서 문제 찾기

### 관리되지 않는 사이트 간 **VPN** 피어 온보딩

CDO는 관리되지 않는 VPN 피어도 식별합니다. 이러한 디바이스를 식별하면 관리되지 않는 디바이스 온보딩, 262 페이지에서 디바이스를 온보딩하고 CDO를 통해 관리합니다.

### **ASA** 원격 액세스 **VPN** 지원

CDO를 사용하면 ASA를 통해 연결할 때 사용자가 엔터프라이즈 리소스에 안전하게 액세스할 수 있도록 RA VPN(Remote Access Virtual Private Network) 구성을 생성할 수 있습니다. ASA가 CDO에 온보딩된 경우 CDO는 ASDM 또는 CSM(Cisco Security Manager)을 사용하여 이미 구성된 RA VPN 설정을 인식하므로 CDO로 관리할 수 있습니다.

AnyConnect는 RA VPN 연결을 제공하는 엔드포인트 디바이스에서만 지원되는 클라이언트입니다.

CDO는 ASA 디바이스에서 RA VPN 기능의 다음 측면을 지원합니다.

- SSL 클라이언트 기반 원격 액세스
- IPv4 and IPv6 addressing
- 여러 ASA 디바이스에서 공유 RA VPN 구성

자세한 내용은 ASA에 대한 원격 액세스 VPN 구성, 270 페이지을 참조하십시오.

Cisco Defense Orchestrator를 사용한 ASA 관리

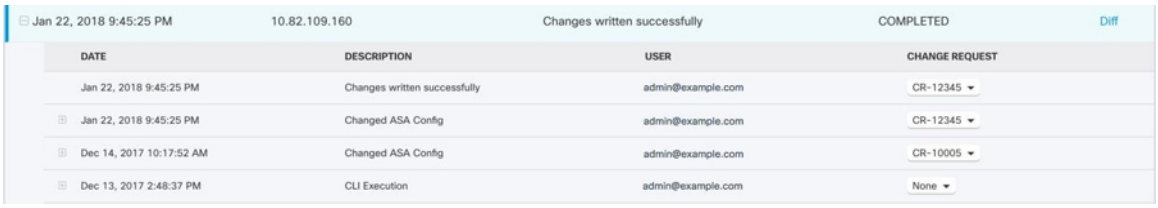
### 디바이스 구성 동기화 모니터링

CDO는 데이터베이스에 저장한 디바이스 구성을 ASA에 설치된 디바이스 구성과 주기적으로 비교합니다. CDO에 등록한 ASA는 여전히 디바이스의 ASDM(Adaptive Security Device Manager)에서 관리할 수 있으므로 CDO의 구성이 디바이스의 구성과 동일한지 확인하고 차이점을 알려줍니다. Synced(동기화됨), Not Synced(동기화되지 않음) 또는 Conflict Detected(충돌 탐지됨) 디바이스 상태에 대한 자세한 내용은 충돌 탐지, 363 페이지의 내용을 참조하십시오.

### 변경 로그에서 변경 사항 추적

디바이스의 구성에 대한 변경 사항은 변경 로그, 369 페이지에 기록됩니다. 변경 로그에는 CDO에서 디바이스로 구축된 변경 사항, 디바이스에서 CDO로 가져온 변경 사항, 해당 변경 사항의 "차이"를 볼 수 있는 기능, 변경된 내용, 발생한 시간, 수행한 사람 등의 정보가 표시됩니다.

회사의 추적 번호를 사용하는 변경 요청 관리할 수도 있습니다. 변경 로그에서 해당 맞춤형 라벨, 날짜 범위, 특정 사용자 또는 변경 유형별로 변경 목록을 필터링하여 원하는 항목을 찾을 수 있습니다.




### 이전 구성 복원

"실행 취소"하려는 ASA를 변경하는 경우 CDO를 사용하여 디바이스를 이전 구성으로 복원할 수 있습니다. 자세한 내용은 Secure Firewall ASA 구성 복원 정보, 106 페이지을 참조하십시오.

### 명령줄 인터페이스 및 명령 매크로를 사용하여 디바이스 관리

CDO는 그래픽 사용자 인터페이스(GUI)와 CDO 명령줄 인터페이스(CLI)를 모두 제공하는 웹 기반 관리 제품으로, 디바이스를 한 번에 하나씩 관리하거나 여러 디바이스를 동시에 관리할 수 있습니다.

ASA CLI 사용자는 CLI 툴의 추가 기능을 높이 평가할 것입니다. 다음은 SSH 세션으로 디바이스에 연결하는 대신 CDO의 CLI 툴을 사용하는 몇 가지 이유입니다.

- CDO는 명령에 필요한 사용자 모드를 알고 있습니다. 명령을 실행하기 위해 권한 수준을 높이거나 낮출 필요가 없으며, 명령을 실행하기 위해 특정 명령 컨텍스트를 입력할 필요도 없습니다.
- CDO는 하므로 목록에서 명령을 선택하여 쉽게 다시 실행할 수 있습니다.
- CLI 작업은 변경 로그에 기록되므로 전송된 명령과 수행한 작업을 읽을 수 있습니다.
- 명령을 대량 모드에서 실행할 수 있으며, 이를 통해 여러 디바이스에 개체 또는 정책을 동시에 구축할 수 있습니다.
- CDO는 한 CLI 매크로를 제공합니다.. CLI 매크로는 있는 그대로 실행할 수 있는 즉시 사용 가능한 명령 또는 완료하고 실행할 수 있는 "공란 채우기" CLI 명령입니다. 하나의 디바이스에서 이러한 명령을 실행하거나 동시에 여러 ASA에 명령을 전송할 수 있습니다.

- CLI는 전체 ASA 구성 파일을 제공합니다. 이를 보거나 고급 사용자인 경우 CLI 명령을 실행하여 변경하지 않고 직접 편집하고 변경 사항을 저장할 수 있습니다.

### 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.

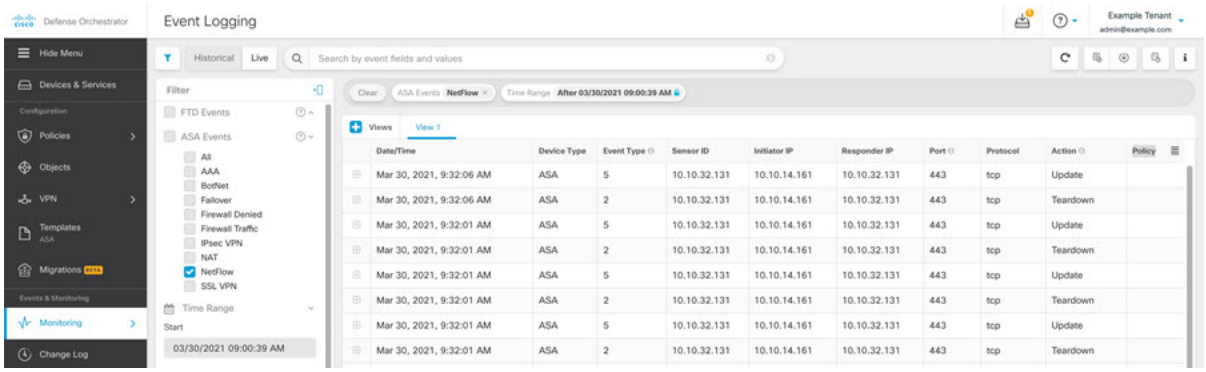
CDO Public API는 이 링크에서 실행하거나 사용자 메뉴에서 **</>CDO API**를 선택하여 실행할 수 있습니다.

### CDO와 SecureX 통합

Cisco SecureX 플랫폼은 가시성을 통합하고 자동화를 가능하게 하며 네트워크, 엔드포인트, 클라우드 및 애플리케이션 전반에서 보안을 강화하는 일관된 경험을 위해 Cisco의 광범위한 통합 보안 포트폴리오와 고객의 인프라를 연결합니다. 통합 플랫폼에서 기술을 연결함으로써 SecureX는 측정 가능한 통찰력, 바람직한 결과 및 더할 나위 없는 팀 간 협업을 제공합니다. SecureX 및 CDO, 535 페이지 및 CDO을 SecureX에 추가, 536 페이지 방법에 대해 자세히 알아볼 수 있습니다.

### Cisco Security Analytics and Logging

Cisco Security Analytics and Logging, 383 페이지은 추가 라이센싱을 통해 시스템 로그 이벤트 및 Netflow Secure Event Logging(NSEL) 이벤트를 ASA에서 보안 이벤트 커넥터, 437 페이지(SEC)로 전송한 다음 Cisco Cloud로 전달할 수 있습니다. 클라우드에 있으면 CDO의 Event Logging(이벤트 로깅) 페이지에서 해당 이벤트를 볼 수 있습니다. 여기서 이벤트를 필터링하고 검토하여 네트워크에서 트리거하는 보안 규칙을 명확하게 이해할 수 있습니다.




이벤트 모니터링 외에도 CDO에서 Secure Cloud Analytics 포털을 실행하여 로깅된 이벤트에 대한 행동 분석을 수행할 수 있습니다.

Cisco Defense Orchestrator를 사용한 ASA 관리

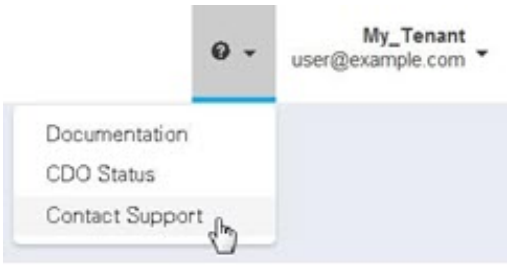
Cisco Security Analytics and Logging을 구현하는 방법에 대한 자세한 설명은 ASA 디바이스에 대한 SaaS(Secure Logging Analytics) 구현, 389 페이지의 내용을 참조하십시오.

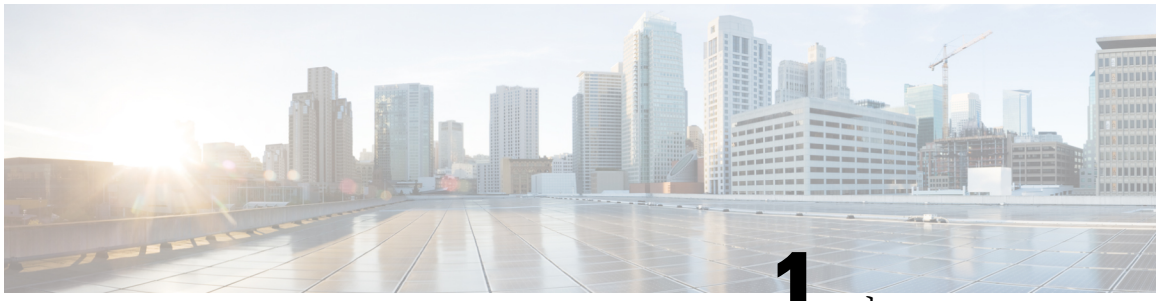
### 향후 작업

이제 ASA의 온보딩 및 정책 조정을 시작할 수 있습니다.

### 도움이 필요한 경우

CDO GUI에서 지원 메뉴를 클릭하여 Cisco Defense Orchestrator 지원팀에 문의, 제품 설명서를 읽을 수 있습니다.





1 장

# Cisco Defense Orchestrator의 기본 사항

Cisco Defense Orchestrator (CDO)는 명확하고 간결한 인터페이스를 통해 정책 관리에 대한 고유한 보기를 제공합니다. 다음은 CDO를 처음 사용할 때 기본 사항을 다루는 항목입니다.

# CDO 테넌트 요청

CDO 테넌트의 30일 무료 평가판을 요청하여 디바이스를 온보딩하고 관리할 수 있습니다. 그런 다음 Cisco 계정 팀에 연락하여 테넌트를 라이선스가 있는 테넌트로 업그레이드할 수 있습니다.

시작하기 전에

SecureX계정을 아직 생성하지 않았으면 생성하십시오. 새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성을 참조하십시오.

절차

1. https://www.defenseorchestrator.com/new로 진행합니다.
2. CDO 테넌트를 프로비저닝하려는 지역을 선택합니다.
3. **Sign Up with SecureX(SecureX**로 가입**)**를 클릭합니다.
4. SecureX 계정으로 로그인합니다.

   성공적으로 로그인하면 등록된 이메일 ID로 테넌트 세부 정보가 포함된 이메일을 받게 됩니다. 선택한 지역에 새 CDO 테넌트가 생성됩니다. 이메일의 지침에 따라 새 CDO 테넌트에 액세스합니다.

   CDO 테넌트에 처음으로 로그인하는 방법에 대한 자세한 내용은 새 CDO 테넌트에 대한 초기 로그인을 참조하십시오.

   CDO 테넌트 및 다양한 테넌트 설정 관리에 대한 자세한 내용은 새 CDO 테넌트에 대한 초기 로그인를 참조하십시오.

추가 **CDO** 테넌트 요청

기존 테넌트를 추가로 생성하려면 어카운트 매니저에게 문의하십시오.

# 라이선스

Cisco Defense Orchestrator에서 디바이스를 온보딩하고 관리하려면, 관리하려는 디바이스에 따라 기본 구독 및 디바이스별 기간 기반 구독을 구매해야 합니다.

# 라이선스 정보

CDO는 테넌트 자격에 대한 기본 구독과 디바이스 관리를 위한 디바이스 라이선스가 필요합니다. 필요한 테넌트 수에 따라 하나 이상의 CDO 기본 구독을 구입하고 디바이스 모델 번호 및 수량에 따라 디바이스 라이선스를 구입할 수 있습니다. 즉, 기본 구독을 구매하면 CDO 테넌트가 제공되며 CDO를 사용하여 관리하기로 선택한 모든 디바이스에 대해 별도의 디바이스 라이선스가 필요합니다. 배포 계획을 위해 각 CDO 테넌트는 SDC(보안 디바이스 커넥터)를 통해 약 500개의 디바이스를 관리하고 클라우드 커넥터를 사용하는 원하는 수의 디바이스를 관리할 수 있습니다. 자세한 내용은 Secure Device Connector(SDC)를 참조하십시오.

서브스크립션

Cisco Defense Orchestrator 구독은 기간 기반입니다.

- 기본- 1년, 3년 및 5년 동안의 구독을 제공하고 CDO 테넌트에 액세스하고 적절하게 라이선스가 부여된 디바이스를 온보딩할 수 있는 권한을 제공합니다.
- 디바이스 라이선스 - 관리하기로 선택한 모든 지원 디바이스에 대해 1년, 3년 및 5년 구독을 제공합니다. 예를 들어 Cisco Firepower 1010 디바이스에 대한 3년 소프트웨어 구독을 구매한 경우, 3년 동안 CDO에서 클라우드 사용 Firewall Management Center를 사용하여 Cisco Firepower 1010 디바이스를 관리하도록 선택할 수 있습니다.

CDO가 지원하는 Cisco 보안 디바이스에 대한 자세한 내용은 CDO에서 지원하는 소프트웨어 및 하드웨어를 참조하십시오.

중요 CDO에서 고가용성 디바이스 쌍을 관리하기 위해 두 개의 별도 디바이스 라이선스가 필요하지 않습니다. ASA(Secure Firewall ASA) 또는 FTD(Secure Firewall Threat Defense) 고가용성 쌍이 있는 경우, CDO는 고가용성 디바이스 쌍을 하나의 단일 디바이스로 간주하므로 하나의 ASA 또는 FTD 디바이스 라이선스를 구입하는 것으로 충분합니다.

참고 Cisco 스마트 라이선스 포털을 통해 CDO 라이선스를 관리할 수 없습니다.

소프트웨어 서브스크립션 지원

CDO 기본 구독에는 구독 기간 동안 유효한 소프트웨어 구독 지원이 포함되며 추가 비용 없이 소프트웨어 업데이트, 주요 업그레이드 및 Cisco TAC(Technical Assistance Center)에 대한 액세스를 제공합니다. 소프트웨어 지원이 기본적으로 선택되어 있지만 요구 사항에 따라 CDO 솔루션 지원을 활용할 수도 있습니다.

# 평가판 라이선스

**Cisco Defense Orchestrator** 평가판 라이선스

SecureX 계정에서 30일 Cisco Defense Orchestrator 평가판을 요청할 수 있습니다. 자세한 내용은 CDO 테넌트 요청을 참조하십시오.

클라우드 사용 **Firewall Management Center** 평가 라이선스

클라우드 사용 Firewall Management Center에 90일 평가판 라이선스가 제공되며 그 이후에는 위협 방어 서비스가 차단됩니다.

CDO 테넌트에서 프로비저닝된 클라우드 사용 Firewall Management Center를 가져오는 방법을 알아보려면 CDO 테넌트용 클라우드 사용 Firewall Management Center 요청을 참조하십시오.

# 클라우드 제공 **Firewall Management Center** 및 **Threat Defense** 라이선스

CDO에서 클라우드 사용 Firewall Management Center를 사용하기 위해 별도의 라이선스를 구입할 필요가 없습니다. CDO 테넌트의 기본 구독에는 클라우드 사용 Firewall Management Center에 대한 비용이 포함됩니다.

참고 클라우드 사용 Firewall Management Center는 에어갭 네트워크의 디바이스에 대한 특정 라이선스 예약(SLR)을 지원하지 않습니다.

클라우드 제공 **Firewall Management Center**용 **Threat Defense** 라이선스

클라우드 사용 Firewall Management Center에서 관리하는 각 Secure Firewall Threat Defense 디바이스에 대해 개별 라이선스가 필요합니다. 자세한 내용은 *Cisco Defense Orchestrator*에서 클라우드 사용 *Firewall Management Center*로 *Firewall Threat Defense* 관리에서 라이센싱을 참조하십시오.

CDO가 클라우드 사용 Firewall Management Center으로 마이그레이션된 디바이스에 대한 라이선스를 처리하는 방법을 알아보려면 Management Center에서 Cloud로 Threat Defense 마이그레이션을 참조하십시오.

# 추가 지원 디바이스 및 라이선스

클라우드 사용 Firewall Management Center, CDO를 통해 Secure Firewall Threat Defense 디바이스를 지원하는 것 외에도 다음 디바이스도 관리합니다.

- Cisco Secure Firewall ASA
- Cisco Secure Firewall Cloud Native
- 온프레미스 Cisco Secure Firewall Management Center
- Cisco Meraki 보안 어플라이언스
- Cisco IOS 디바이스
- SSH를 사용하여 액세스할 수 있는 디바이스
- Amazon Web Services(AWS) 가상 프라이빗 클라우드(VPC)
- Duo 관리자 패널
- Umbrella 조직

CDO 기본 인타이틀먼트 라이선스와 관리하려는 디바이스에 특정한 라이선스가 필요합니다.

# SDC(Secure Device Connector)

디바이스 자격 증명을 사용하여 CDO에 디바이스를 온보딩할 때 CDO는 디바이스와 CDO 간의 프록시 통신을 위해 네트워크에서 SDC(Secure Device Connector)를 다운로드하고 구축하는 것이 모범 사례라고 간주합니다. 그러나 원하는 경우 CDO에서 외부 인터페이스를 통해 직접 통신을 수신하도록 디바이스를 활성화할 수 있습니다. ASA(Adaptive Security Appliance), FDM 관리 디바이스, FMC(Firepower Management Center), Secure Firewall Cloud Native 디바이스, SSH 및 IOS 디바이스는 모두 SDC를 사용하여 CDO에 온보딩할 수 있습니다.

SDC는 매니지드 디바이스에서 실행해야 하는 명령과 매니지드 디바이스로 전송해야 하는 메시지에 대해 CDO를 모니터링합니다. SDC는 CDO를 대신하여 명령을 실행하고, 매니지드 디바이스를 대신하여 CDO에 메시지를 전송하고, 매니지드 디바이스에서 CDO로 응답을 반환합니다.

SDC는 AES-128-GCM over HTTPS(TLS 1.2)를 사용하여 서명 및 암호화된 보안 통신 메시지를 사용하여 CDO와 통신합니다. 온보딩된 디바이스 및 서비스에 대한 모든 자격 증명은 브라우저에서 SDC로 직접 암호화되며, AES-128-GCM을 사용하여 저장 상태에서도 암호화됩니다. SDC만 디바이스 자격 증명에 액세스할 수 있습니다. 다른 CDO 서비스는 자격 증명에 액세스할 수 없습니다. SDC와 CDO 간의 통신을 허용하는 방법에 대한 자세한 내용은 매니지드 디바이스에 Cisco Defense Orchestrator 연결, 6 페이지의 내용을 참조하십시오.

SDC는 하이퍼바이저의 가상 머신으로 어플라이언스에 설치하거나 AWS 또는 Azure와 같은 클라우드 환경에 설치할 수 있습니다. CDO에서 제공하는 통합된 가상 머신 및 SDC 이미지를 사용하여 SDC를 설치하거나, 고유한 가상 머신을 생성하고 여기에 SDC를 설치할 수 있습니다. SDC 가상 어플라이언스는 CentOS 운영 체제를 포함하며 Docker 컨테이너 내에서 실행됩니다.

각 CDO 테넌트에는 무제한의 SDC가 있을 수 있습니다. 이러한 SDC는 테넌트 간에 공유되지 않으며 단일 테넌트 전용입니다. 단일 SDC에서 관리할 수 있는 디바이스의 수는 해당 디바이스에 구현된 기능 및 해당 구성 파일의 크기에 따라 달라집니다. 그러나 구축을 계획할 때는 1개의 SDC가 약 500개의 디바이스를 지원할 것으로 예상합니다.

테넌트에 대해 둘 이상의 SDC를 구축하면 다음과 같은 이점도 제공됩니다.

- 성능 저하 없이 CDO 테넌트로 더 많은 디바이스를 관리할 수 있습니다.
- 네트워크 내의 격리된 네트워크 세그먼트에 SDC를 구축하고 동일한 CDO 테넌트로 해당 세그먼트의 디바이스를 계속 관리할 수 있습니다. 여러 SDC가 없으면 서로 다른 CDO 테넌트를 사용하여 격리된 네트워크 세그먼트에서 디바이스를 관리해야 합니다.

두 번째 또는 후속 SDC를 구축하는 절차는 첫 번째 SDC를 구축할 때와 동일합니다. 테넌트의 초기 SDC는 테넌트의 이름과 숫자 1을 통합하며 CDO의 페이지의 Secure Connectors(보안 커넥터) 탭에 표시됩니다. 각 추가 SDC는 순서대로 번호가 매겨집니다. CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축, 8 페이지 및 자체 VM에 보안 디바이스 커넥터 구축, 12 페이지 참조

관련 정보:

- 매니지드 디바이스에 Cisco Defense Orchestrator 연결
- 보안 디바이스 커넥터 문제 해결, 553 페이지
- 보안 디바이스 커넥터 업데이트, 23 페이지
- 보안 디바이스 커넥터 제거, 20 페이지

# 매니지드 디바이스에 Cisco Defense Orchestrator 연결

CDO는 클라우드 커넥터 또는 SDC(Secure Device Connector)를 통해 관리하는 디바이스에 연결합니다.

인터넷에서 디바이스에 직접 액세스할 수 있는 경우 클라우드 커넥터를 사용하여 디바이스에 연결해야 합니다. 디바이스를 구성할 수 있는 경우 클라우드 지역의 CDO IP 주소에서 포트 443에 대한 인바운드 액세스를 허용합니다.

인터넷에서 디바이스에 액세스할 수 없는 경우 CDO가 디바이스와 통신할 수 있도록 네트워크에 온프레미스 SDC를 구축할 수 있습니다. 디바이스를 구성할 수 있는 경우 포트 443(또는 디바이스 관리를 위해 설정한 포트)에서 전체 인바운드 액세스를 허용해야 합니다.

다음을 온보딩하려면 네트워크에 온프레미스 SDC가 필요합니다.

- 클라우드에서 액세스할 수 없는 ASA 디바이스.
- 클라우드에서 액세스할 수 없는 FDM 관리 디바이스 및 "자격 증명 온보딩" 방법이 사용됩니다.
- Cisco IOS 디바이스.
- SSH 액세스가 가능한 디바이스.

다른 모든 디바이스 및 서비스에는 온프레미스 SDC가 필요하지 않습니다. CDO는 "Cloud Connector"를 사용하여 연결합니다. 인바운드 액세스를 허용해야 하는 IP 주소를 확인하려면 다음 섹션을 참조하십시오.

### 클라우드 커넥터를 통해 디바이스를 CDO에 연결

클라우드 커넥터를 통해 CDO를 디바이스에 직접 연결할 때는 EMEA, 미국 또는 APJC 지역의 다양한 IP 주소에 대해 포트 443(또는 디바이스 관리를 위해 구성한 모든 포트)에서 인바운드 액세스를 허용해야 합니다.

유럽, 중동 또는 아프리카(EMEA) 지역의 고객이 https://defenseorchestrator.eu/에서 CDO에 연결하는 경우 다음 IP 주소에서의 인바운드 액세스를 허용합니다.

- 35.157.12.126
- 35.157.12.15

미국 지역의 고객이 https://defenseorchestrator.com에서 CDO에 연결하는 경우 다음 IP 주소에서의 인바운드 액세스를 허용합니다.

- 52.34.234.2
- 52.36.70.147

APJC(아시아-태평양-일본-중국) 지역의 고객이 https://www.apj.cdo.cisco.com/에서 CDO에 연결하는 경우 다음 IP 주소에서의 인바운드 액세스를 허용합니다.

- 54.199.195.111
- 52.199.243.0

### SDC를 사용하여 CDO에 디바이스 연결

SDC를 통해 CDO를 디바이스에 연결할 때 CDO에서 관리하려는 디바이스는 포트 443(또는 디바이스 관리를 위해 구성한 모든 포트)에서 전체 인바운드 액세스를 허용해야 합니다. 이는 관리 액세스 제어 규칙을 사용하여 구성됩니다.

또한 SDC가 구축된 가상 머신이 매니지드 디바이스의 관리 인터페이스에 네트워크로 연결되어 있는지 확인해야 합니다.

### SDC에 ASA 또는 Secure Firewall Cloud Native를 연결하기 위한 특별 고려 사항

특히 ASA 또는 Secure Firewall Cloud Native의 경우 SDC는 ASDM에서 사용하는 것과 동일한 보안 통신 채널을 사용합니다.

관리 중인 ASA 또는 Secure Firewall Cloud Native도 AnyConnect VPN 클라이언트 연결을 허용하도록 구성된 경우 ASDM HTTP 서버 포트를 1024 이상의 값으로 변경해야 합니다. 이 포트 번호는 디바이스를 ASA 또는 Secure Firewall Cloud Native 디바이스에 온보딩할 때 사용되는 포트 번호와 동일합니다.

### ASA 또는 Secure Firewall Cloud Native 명령 예

다음 예에서는 ASA 또는 Secure Firewall Cloud Native 외부 인터페이스의 이름이 'outside'이고 AnyConnect 클라이언트가 ASA 또는 Secure Firewall Cloud Native에 구성되어 있으므로, ASDM HTTP 서버가 포트 8443에서 수신 대기 중이라고 가정합니다.

외부 인터페이스를 활성화하려면 다음 명령을 입력합니다.

EMEA:

**http 35.157.12.126 255.255.255.255 outside**

**http 35.157.12.15 255.255.255.255 outside**

미국:

**http 52.34.234.2 255.255.255.255 outside**

**http 52.36.70.147 255.255.255.255 outside**

아시아 태평양 일본 중국 지역:

**http 54.199.195.111 255.255.255.255 outside**

**http 52.199.243.0 255.255.255.255 outside**

AnyConnect VPN 클라이언트를 사용 중인 경우 ASDM HTTP 서버 포트를 활성화하려면 다음 명령을 입력합니다.

**http server enable 8443**

# CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축

디바이스 자격 증명을 사용하여 CDO를 디바이스에 연결하는 경우 네트워크에 SDC를 다운로드하고 배포하여 CDO와 디바이스 간의 통신을 관리하는 것이 가장 좋습니다. 일반적으로 이러한 디바이스는 경계를 기반으로 하지 않으며 공용 IP 주소가 없거나 외부 인터페이스에 대한 개방형 포트가 있습니다. ASA(Adaptive Security Appliance), FDM 관리 디바이스, FMC(Firepower Management Center), Secure Firewall Cloud Native 디바이스, SSH 및 IOS 디바이스는 모두 SDC를 사용하여 CDO에 온보딩할 수 있습니다.

SDC는 매니지드 디바이스에서 실행해야 하는 명령과 매니지드 디바이스로 전송해야 하는 메시지에 대해 CDO를 모니터링합니다. SDC는 CDO를 대신하여 명령을 실행하고, 매니지드 디바이스를 대신하여 CDO에 메시지를 전송하고, 매니지드 디바이스에서 CDO로 응답을 반환합니다.

단일 SDC에서 관리할 수 있는 디바이스의 수는 해당 디바이스에 구현된 기능 및 해당 구성 파일의 크기에 따라 달라집니다. 그러나 구축을 계획할 때는 1개의 SDC가 약 500개의 디바이스를 지원할 것으로 예상합니다. 자세한 내용은 단일 CDO 테넌트에서 여러 SDC 사용, 23 페이지를 참조하십시오.

이 절차에서는 CDO의 VM 이미지를 사용하여 네트워크에 SDC를 설치하는 방법을 설명합니다. 이는 SDC를 생성하는 가장 쉽고 신뢰할 수 있는 방법입니다. 생성한 VM을 사용하여 SDC를 생성해야 하는 경우 자체 VM에 보안 디바이스 커넥터 구축, 12 페이지을 수행합니다.

### 시작하기 전에

SDC를 구축하기 전에 다음 사전 요건을 검토합니다.

- CDO는 엄격한 인증서 확인이 필요하며 SDC와 인터넷 간의 웹/콘텐츠 프록시 검사를 지원하지 않습니다. 프록시 서버를 사용하는 경우 SDC(보안 디바이스 커넥터)와 CDO 간의 트래픽 검사를 비활성화합니다.

- SDC는 TCP 포트 443 또는 디바이스 관리를 위해 구성한 포트에서 인터넷에 대한 전체 아웃바운드 액세스 권한을 가져야 합니다. CDO에서 관리하는 디바이스는 이 포트의 인바운드 트래픽도 허용해야 합니다.
- 매니지드 디바이스에 Cisco Defense Orchestrator 연결를 검토하여 적절한 네트워크 액세스를 확인합니다.
- CDO는 vSphere 웹 클라이언트 또는 ESXi 웹 클라이언트를 사용하여 SDC VM OVF 이미지 설치를 지원합니다.
- CDO는 vSphere 데스크톱 클라이언트를 사용한 SDC VM OVF 이미지 설치를 지원하지 않습니다.
- ESXi 5.1 하이퍼바이저.
- Cent OS 7 게스트 운영체제.
- SDC가 하나만 있는 VMware ESXi 호스트의 시스템 요구 사항:
  - VMware ESXi 호스트에는 vCPU 2개가 필요합니다.
  - VMware ESXi 호스트에는 최소 2GB의 메모리가 필요합니다.
  - VMware ESXi에는 프로비저닝 선택에 따라 가상 머신을 지원하기 위해 64GB의 디스크 공간이 필요합니다.
- 테넌트용 SDC 및 단일 SEC(Secure Event Connector)가 있는 VM의 시스템 요구 사항. (SEC는 Security Analytics and Logging(SaaS) 정보에서 사용되는 구성 요소입니다.)

  VMware ESXi 호스트에 추가하는 각 SEC에는 4개의 CPU와 8GB의 추가 메모리가 필요합니다.

  따라서 하나의 SDC와 하나의 SEC가 있는 VMware ESXi 호스트에 대한 요구 사항은 다음과 같습니다.
  - VMware ESXi 호스트에는 vCPU 6개가 필요합니다.
  - VMware ESXi 호스트에는 최소 10GB의 메모리가 필요합니다.
  - VMware ESXi에는 프로비저닝 선택에 따라 가상 머신을 지원하기 위해 64GB의 디스크 공간이 필요합니다.
- docker IP는 SDC의 IP 범위 및 디바이스 IP 범위와 다른 서브넷에 있어야 합니다.
- 설치를 시작하기 전에 다음 정보를 수집하십시오.
  - SDC에 사용할 고정 IP 주소
  - 설치 프로세스 중 생성하는 `root` 및 `cdo` 사용자의 비밀번호.
  - 조직에서 사용하는 DNS 서버의 IP 주소
  - SDC 주소가 있는 네트워크의 게이트웨이 IP 주소
  - 시간 서버의 FQDN 또는 IP 주소.

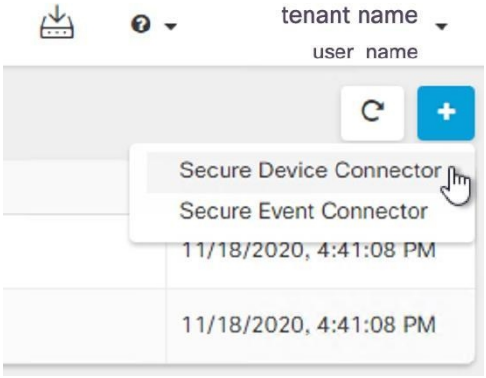
- SDC 가상 머신은 보안 패치를 정기적으로 설치하도록 구성되며, 이를 위해서는 포트 80 아웃바운드를 열어야 합니다.

---

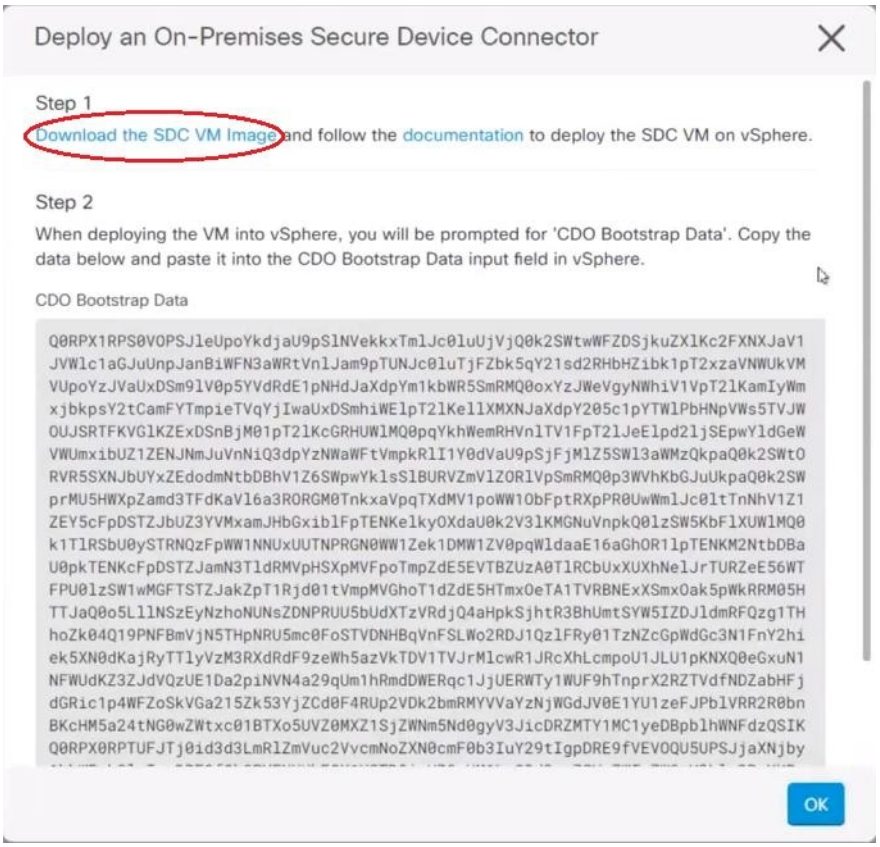
단계 **1** SDC를 생성할 CDO 테넌트에 로그온합니다.

단계 **2** CDO 메뉴에서 **Tools & Services(**툴 및 서비스**)** > **Secure Connectors(**보안 커넥터**)**를 선택합니다.

단계 **3** Secure Connectors(보안 커넥터) 페이지에서 파란색 더하기 버튼을 클릭하고 **Secure Device Connector(**보안 디바이스 커넥터**)**를 클릭합니다.




단계 **4** 1단계에서 **Download the SDC VM image(SDC VM** 이미지 다운로드**)**를 클릭합니다. 별도의 탭에서 열립니다.



단계 **5** .zip 파일의 모든 파일을 추출합니다. 다음과 같이 표시됩니다.

- CDO-SDC-VM-ddd50fa.ovf
- CDO-SDC-VM-ddd50fa.mf
- CDO-SDC-VM-ddd50fa-disk1.vmdk

단계 **6** vSphere 웹 클라이언트를 사용하여 VMware 서버에 관리자로 로그인합니다.

참고 ESXi 웹 클라이언트를 사용하지 마십시오.

단계 **7** 지시에 따라 OVF 템플릿에서 보안 디바이스 커넥터 가상 머신을 구축합니다.

단계 **8** 설정이 완료되면 SDC VM의 전원을 켭니다.

단계 **9** 새 SDC VM의 콘솔을 엽니다.

단계 **10** 사용자 이름 **cdo**로 로그인합니다. 기본 암호는 **adm123**입니다.

단계 **11** 프롬프트에 `sudo sdc-onboard setup`을 입력합니다.

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

단계 **12** 비밀번호를 물으면 `adm123`을 입력합니다.

단계 **13** 지시에 따라 `root` 사용자의 새 비밀번호를 생성합니다. 루트 사용자의 비밀번호를 입력합니다.

단계 **14** 지시에 따라 **cdo** 사용자의 새 암호를 생성합니다. cdo 사용자의 비밀번호를 입력합니다.

단계 **15** **Please choose the CDO domain you connect to(**연결할 **CDO** 도메인을 선택하십시오**)** 메시지가 표시되면 Cisco Defense Orchestrator 도메인 정보를 입력합니다.

단계 **16** 메시지가 표시되면 SDC VM의 다음 도메인 정보를 입력합니다.

a) IP 주소/CIDR
b) 게이트웨이
c) DNS 서버
d) NTP 서버 또는 FQDN
e) Docker 브리지

또는 docker 브리지가 적용되지 않는 경우 Enter 키를 누릅니다.

단계 **17** **Are these values valid(**이 값이 올바릅니까**?) (y/n)** 메시지가 나타나면 **y**를 사용하여 입력을 확인합니다**.**

단계 **18** 입력을 확인합니다.

단계 **19** **"Would you like to setup the SDC now?(**지금 **SDC**를 설정하시겠습니까**?) (y/n)** 메시지가 나타나면 `n`을 입력합니다.

단계 **20** VM 콘솔에서 자동으로 로그아웃됩니다.

단계 **21** SDC에 대한 SSH 연결을 생성합니다. **cdo**로 로그인하고 비밀번호를 입력합니다.

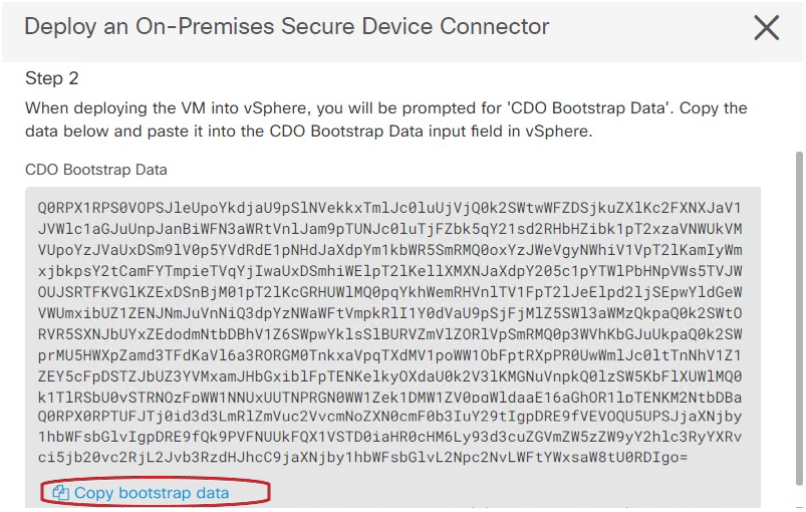
단계 **22** 프롬프트에 `sudo sdc-onboard bootstrap`을 입력합니다.

```
[cdo@localhost ~]$ sudo sdc-onboard bootstrap
```

단계 **23** **[sudo]** 비밀번호를 묻는 메시지가 표시되면 단계 14에서 생성한 cdo 비밀번호를 입력합니다.

단계 **24** **Please copy the bootstrap data form the Secure Connector Page of CDO(CDO**의 보안 커넥터 페이지에서 부트스트랩 데이터를 복사하십시오**.)** 메시지가 표시되면 다음 절차를 수행합니다.

1. CDO에 로그인합니다.
2. CDO 메뉴에서 **Admin(**관리**)** > **Secure Connector(**보안 커넥터**)**를 선택합니다.
3. Actions(작업) 창에서 **Deploy an On-Premises Secure Device Connector(**온프레미스 보안 디바이스 커넥터 구축**)**를 클릭합니다.
4. 대화 상자의 2단계에서 **Copy the bootstrap data(**부트스트랩 데이터 복사**)**를 클릭하고 SSH 창에 붙여넣습니다.




단계 **25** **Do you want to update these setting(**이 설정을 업데이트하시겠습니까**?) (y/n)** 메시지가 나타나면 `n`을 입력합니다.

단계 **26** Secure Device Connector(보안 디바이스 커넥터) 페이지로 돌아갑니다. 새 SDC의 상태가 **Active(**활성**)**로 변경될 때까지 화면을 새로 고칩니다.

---

관련 정보**:**

- 보안 디바이스 커넥터 문제 해결, 553 페이지
- SDC와의 디바이스 연결 문제 해결, 554 페이지

# 자체 **VM**에 보안 디바이스 커넥터 구축

디바이스 자격 증명을 사용하여 CDO 를 디바이스에 연결하는 경우, 네트워크에서 SDC(Secure Device Connector)를 다운로드하고 구축하여 CDO와 디바이스 간의 통신을 관리하는 것이 모범 사례입니다. 일반적으로 이러한 디바이스는 경계를 기반으로 하지 않으며 공용 IP 주소가 없거나 외부 인터페이스에 대한 개방형 포트가 있습니다. ASA(Adaptive Security Appliance), FDM 관리 장치, FMC(Firepower Management Center) 및 Secure Firewall Cloud Native 디바이스는 모두 디바이스 자격 증명을 사용하여 CDO에 온보딩할 수 있습니다.

SDC는 매니지드 디바이스에서 실행해야 하는 명령과 매니지드 디바이스로 전송해야 하는 메시지에 대해 CDO를 모니터링합니다. SDC는 CDO를 대신하여 명령을 실행하고, 매니지드 디바이스를 대신하여 CDO에 메시지를 전송하고, 매니지드 디바이스에서 CDO로 응답을 반환합니다.

단일 SDC에서 관리할 수 있는 디바이스의 수는 해당 디바이스에 구현된 기능 및 해당 구성 파일의 크기에 따라 달라집니다. 그러나 구축을 계획할 때는 1개의 SDC가 약 500개의 디바이스를 지원할 것으로 예상합니다. 자세한 내용은 단일 CDO 테넌트에서 여러 SDC 사용, 23 페이지를 참조하십시오.

이 절차에서는 자체 가상 머신 이미지를 사용하여 네트워크에 SDC를 설치하는 방법을 설명합니다.

참고 SDC를 설치하는 가장 쉽고 신뢰할 수 있는 방법은 CDO의 SDC OVA 이미지를 다운로드하여 설치하는 것입니다. 해당 지침은 CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축, 8 페이지의 내용을 참조하십시오.

시작하기 전에

- CDO는 엄격한 인증서 확인이 필요하며 SDC와 인터넷 간의 웹/콘텐츠 프록시를 지원하지 않습니다.
- SDC는 TCP 포트 443에서 인터넷에 대한 전체 아웃바운드 액세스 권한을 가져야 합니다.
- 네트워킹 지침은 매니지드 디바이스에 Cisco Defense Orchestrator 연결을 검토하십시오.
- vCenter 웹 클라이언트 또는 ESXi 웹 클라이언트와 함께 설치된 VMware ESXi 호스트

참고 vSphere 데스크톱 클라이언트를 사용한 설치는 지원되지 않습니다.

- ESXi 5.1 하이퍼바이저.
- Cent OS 7 게스트 운영체제.
- SDC만 있는 VM의 시스템 요구 사항:
  - VMware ESXi 호스트에는 CPU 2개가 필요합니다.
  - VMware ESXi 호스트에는 최소 2GB의 메모리가 필요합니다.
  - VMware ESXi에는 프로비저닝 선택에 따라 가상 머신을 지원하기 위해 64GB의 디스크 공간이 필요합니다. 이 값은 필요에 따라 필요한 디스크 공간을 확장할 수 있도록 파티션과 함께 LVM(논리적 볼륨 관리)을 사용한다고 가정합니다.
- 테넌트용 SDC 및 단일 SEC(Secure Event Connector)가 있는 VM의 시스템 요구 사항. (SEC는 Security Analytics and Logging(SaaS) 정보에서 사용되는 구성 요소입니다.)

  VMware ESXi 호스트에 추가하는 각 SEC에는 4개의 CPU와 8GB의 추가 메모리가 필요합니다.

  따라서 하나의 SDC와 하나의 SEC가 있는 VMware ESXi 호스트에 대한 요구 사항은 다음과 같습니다.

- VMware ESXi 호스트에는 vCPU 6개가 필요합니다.
- VMware ESXi 호스트에는 최소 10GB의 메모리가 필요합니다.
- VMware ESXi에는 프로비저닝 선택에 따라 가상 머신을 지원하기 위해 64GB의 디스크 공간이 필요합니다.

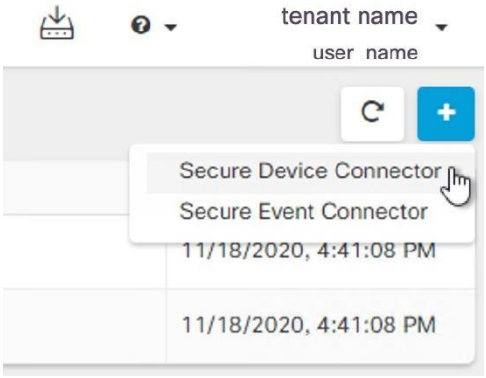
- VM의 CPU와 메모리를 업데이트한 후 VM의 전원을 켜고 Secure Connector(보안 커넥터) 페이지에 SDC가 "Active(활성)" 상태로 표시되는지 확인합니다.
- 이 절차를 수행하는 사용자는 Linux 환경에서 작업하고 파일 편집을 위해 vi 시각적 편집기를 사용하는 데 익숙해야 합니다.
- CentOS 가상 머신에 온프레미스 SDC를 설치하는 경우 정기적으로 Yum 보안 패치를 설치하는 것이 좋습니다. Yum 구성에 따라 Yum 업데이트를 가져오려면 포트 80 및 443에서 아웃바운드 액세스를 열어야 할 수 있습니다. 또한 업데이트를 예약하려면 yum-cron 또는 crontab을 구성해야 합니다. 보안 운영 팀과 함께 Yum 업데이트를 받기 위해 변경해야 하는 보안 정책이 있는지 확인합니다.

참고 시작하기 전에: 절차의 명령을 복사하여 터미널 창에 붙여넣지 말고 대신 입력하십시오. 일부 명령에는 "n-대시"가 포함되며, 잘라내기 및 붙여넣기 프로세스에서 이러한 명령은 "m-대시"로 적용되어 명령이 실패할 수 있습니다.

단계 **1** SDC를 생성할 CDO 테넌트에 로그온합니다.

단계 **2** CDO 메뉴에서 **Tools & Services(**툴 및 서비스**)** > **Secure Connectors(**보안 커넥터**)**를 선택합니다.

단계 **3** Secure Connectors(보안 커넥터) 페이지에서 파란색 더하기 버튼을 클릭하고 **Secure Device Connector(**보안 디바이스 커넥터**)**를 클릭합니다.




단계 **4** 창의 2단계에서 부트스트랩 데이터를 메모장에 복사합니다.

단계 **5** 최소 SDC에 할당된 다음 RAM 및 디스크 공간을 사용하여 **CentOS 7** 가상 머신을 설치합니다.

- 8GB RAM

- 10GB 디스크 공간

단계 **6** 설치가 완료되면 SDC의 IP 주소, 서브넷 마스크 및 게이트웨이를 지정하는 등의 기본 네트워킹을 구성합니다.

단계 **7** DNS(Domain Name Server) 서버를 구성합니다.

단계 **8** NTP(Network Time Protocol) 서버를 구성합니다.

단계 **9** SDC의 CLI와의 손쉬운 상호 작용을 위해 CentOS에 SSH 서버를 설치합니다.

단계 **10** Yum 업데이트를 실행한 후 **open-vm-tools**, **nettools** 및 **bind-utils** 패키지를 설치합니다.

```
[root@sdc-vm ~]# yum update -y
                 [root@sdc-vm ~]# yum install -y open-vm-tools net-tools bind-utils
```

단계 **11** AWS CLI 패키지를 설치합니다. https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html의 내용을 참조하십시오.

참고 **--user** 플래그를 사용하지 마십시오.

단계 **12** Docker CE 패키지를 설치합니다. https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ce의 내용을 참조하십시오.

참고 "저장소를 사용하여 설치" 방법을 사용합니다.

단계 **13** Docker 서비스를 시작하고 부팅 시 시작되도록 활성화합니다.

```
[root@sdc-vm ~]# systemctl start docker
[root@sdc-vm ~]# systemctl enable docker
Created symlink from /etc/systemd/system/multiuser.target.wants/docker.service to
    /usr/lib/systemd/system/docker.service.
```

단계 **14** 두 사용자("cdo" 및 "sdc")를 생성합니다. cdo 사용자는 관리 기능을 실행하기 위해 로그인하는 사용자이며(루트 사용자를 직접 사용할 필요가 없음), sdc 사용자는 SDC 도커 컨테이너를 실행하는 사용자입니다.

```
[root@sdc-vm ~]# useradd cdo
[root@sdc-vm ~]# useradd sdc –d /usr/local/cdo
```

단계 **15** cdo 사용자의 비밀번호를 생성합니다.

```
[root@sdc-vm ~]# passwd cdo
Changing password for user cdo.
New password: <type password>
Retype new password: <type password>
passwd: all authentication tokens updated successfully.
```

단계 **16** cdo 사용자를 "Wheel" 그룹에 추가하여 관리(sudo) 권한을 부여합니다.

```
[root@sdc-vm ~]# usermod -aG wheel cdo
[root@sdc-vm ~]#
```

단계 **17** Docker가 설치되면 사용자 그룹이 생성됩니다. CentOS/Docker 버전에 따라 "docker" 또는 "dockerroot"라고 부를 수 있습니다. /etc/group 파일을 확인하여 어떤 그룹이 생성되었는지 확인한 다음 sdc 사용자를 이 그룹에 추가합니다.

```
[root@sdc-vm ~]# grep docker /etc/group
 docker:x:993:
[root@sdc-vm ~]#
[root@sdc-vm ~]# usermod -aG docker sdc
[root@sdc-vm ~]#
```

단계 **18** /etc/docker/daemon.json 파일이 없는 경우 파일을 생성하고 아래 내용을 입력합니다. 생성되면 docker 데몬을 다시 시작합니다.

참고 "group" 키에 입력한 그룹 이름이 이전 단계의 /etc/group 파일에서 찾은 그룹과 일치하는지 확인합니다.

```
[root@sdc-vm ~]# cat /etc/docker/daemon.json
        {
           "live-restore": true,
           "group": "docker"
        }
        [root@sdc-vm ~]# systemctl restart docker
        [root@sdc-vm ~]#
```

단계 **19** 현재 vSphere 콘솔 세션을 사용 중인 경우 SSH로 전환하고 "cdo" 사용자로 로그인합니다. 로그인한 후에는 "sdc" 사용자로 변경합니다. 암호를 묻는 메시지가 표시되면 "cdo" 사용자의 암호를 입력합니다.

```
[cdo@sdc-vm ~]$ sudo su sdc
              [sudo] password for cdo: <type password for cdo user>
              [sdc@sdc-vm ~]$
```

단계 **20** 디렉터리를 **/usr/local/cdo**로 변경합니다.

단계 **21** `bootstrapdata`라는 새 파일을 생성하고 온프레미스 보안 디바이스 커넥터 구축 마법사의 2단계에서 가져온 부트스트랩 데이터를 이 파일에 붙여넣습니다. 파일을 **Save(**저장**)**합니다. `vi` 또는 `nano`를 사용하여 파일을 생성할 수 있습니다.

단계 **22** 부트스트랩 데이터는 base64로 인코딩됩니다. 이를 디코딩하고 `extractedbootstrapdata`라는 파일로 내보냅니다.

```
[sdc@sdc-vm ~]$ base64 -d /usr/local/cdo/bootstrapdata > /usr/local/cdo/extractedbootstrapdata
             [sdc@sdc-vm ~]$
```

cat 명령을 실행하여 디코딩된 데이터를 확인합니다. 명령 및 디코딩된 데이터는 다음과 같이 표시됩니다.

```
[sdc@sdc-vm ~]$ cat /usr/local/cdo/extractedbootstrapdata
              CDO_TOKEN="<token string>"
              CDO_DOMAIN="www.defenseorchestrator.com"
              CDO_TENANT="<tenant-name>"

CDO_BOOTSTRAP_URL="https://www.defenseorchestrator.com/sdc/bootstrap/tenant-name/<tenant-name-SDC>"
```

단계 **23** 다음 명령을 실행하여 디코딩된 부트스트랩 데이터의 섹션을 환경 변수로 내보냅니다.

```
[sdc@sdc-vm ~]$ sed -e 's/^/export /g' extractedbootstrapdata > sdcenv && source sdcenv
             [sdc@sdc-vm ~]$
```

단계 **24** CDO에서 부트스트랩 번들을 다운로드합니다.

```
[sdc@sdc-vm ~]$ curl -O -H "Authorization: Bearer $CDO_TOKEN" "$CDO_BOOTSTRAP_URL"
              100 10314 100 10314 0 0 10656 0 --:--:-- --:--:-- --:--:-- 10654
              [sdc@sdc-vm ~]$ ls -l /usr/local/cdo/*SDC
              -rw-rw-r--. 1 sdc sdc 10314 Jul 23 13:48 /usr/local/cdo/tenant-name-SDC
```

단계 **25** SDC tarball의 압축을 풀고 `bootstrap.sh` 파일을 실행하여 SDC 패키지를 설치합니다.

```
[sdc@sdc-vm ~]$ tar xzvf /usr/local/cdo/tenant-name-SDC
                <snipped – extracted files>
                [sdc@sdc-vm ~]$
                [sdc@sdc-vm ~]$ /usr/local/cdo/bootstrap/bootstrap.sh
                [2018-07-23 13:54:02] environment properly configured
                download: s3://onprem-sdc/toolkit/prod/toolkit.tar to toolkit/toolkit.tar
                toolkit.sh
                common.sh
                [2018-07-23 13:54:04] startup new container
                Unable to find image 'ciscodefenseorchestrator/sdc_prod:latest' locally
                sha256:d98f17101db10e66db5b5d6afda1c95c29ea0004d9e4315508fd30579b275458: Pulling from
                ciscodefenseorchestrator/sdc_prod
                08d48e6f1cff: Pull complete
                ebbd10b629b1: Pull complete
                d14d580ef2ed: Pull complete
                45421d451ab8: Pull complete
                <snipped – downloads>
                no crontab for sdc
```

이제 SDC가 CDO에서 "Active(활성)"로 표시됩니다.

---

다음에 수행할 작업

- 디바이스 및 서비스 온보딩로 이동하여 CDO로 관리하려는 디바이스를 온보딩합니다.
- 보안 이벤트 커넥터를 설치하는 경우 SDC 가상 머신에 SEC(Secure Event Connector) 설치, 438 페이지로 돌아갑니다.
- 테넌트에 두 번째 이상의 보안 이벤트 커넥터를 설치하는 경우, CDO 이미지를 사용하여 SEC 설치로 돌아갑니다.

# Terraform 모듈을 사용하여 AWS VPC에 보안 디바이스 커넥터 구축

시작하기 전에

AWS VPC에서 SDC를 구축하기 전에 다음 사전 요건을 검토하십시오.

- CDO는 엄격한 인증서 확인이 필요하며 SDC와 인터넷 간의 웹/콘텐츠 프록시 검사를 지원하지 않습니다. 프록시 서버를 사용하는 경우 SDC(보안 디바이스 커넥터)와 CDO 간의 트래픽 검사를 비활성화합니다.
- 매니지드 디바이스에 Cisco Defense Orchestrator 연결를 검토하여 적절한 네트워크 액세스를 확인합니다.
- 이 경우 AWS 계정, 하나 이상의 서브넷이 있는 AWS VPC 및 AWS Route53 호스팅 영역이 필요합니다.
- CDO 부트스트랩 데이터, AWS VPC ID 및 해당 서브넷 ID가 있는지 확인합니다.
- SDC를 구축하는 프라이빗 서브넷에 NAT 게이트웨이가 연결되어 있는지 확인합니다.

- 방화벽 관리 HTTP 인터페이스가 실행 중인 포트에서 NAT 게이트웨이에 연결된 탄력적 IP로 이동하는 트래픽을 엽니다.

---

단계 1 Terraform 파일에 다음 코드 줄을 추가합니다. 변수에 대한 입력을 수동으로 입력해야 합니다.

```
module "example-sdc" {
  source              = "git::https://github.com/cisco-lockhart/terraform-aws-cdo-sdc.git?ref=v0.0.1"
  env                 = "example-env-ci"
  instance_name       = "example-instance-name"
  instance_size       = "r5a.xlarge"
  cdo_bootstrap_data = "<replace-with-cdo-bootstrap-data>"
  vpc_id              = <replace-with-vpc-id>
  subnet_id           = <replace-with-private-subnet-id>
}
```

입력 변수 및 설명 목록은 Secure Device Connector Terraform 모듈을 참조하십시오.

단계 2 Terraform 코드에서 `instance_id`를 출력으로 등록합니다.

```
output "example_sdc_instance_id" {
  value = module. example-sdc.instance_id
}
```

`instance_id`를 사용하여 AWS Systems Manager 세션 관리자(SSM)를 통한 문제 해결을 위해 SDC 인스턴스에 연결할 수 있습니다. 사용 가능한 출력 목록은 Secure Device Connector Terraform 모듈의 출력을 참조하십시오.

---

다음에 수행할 작업

모든 SDC 문제 해결의 경우, AWS SSM을 사용하여 SDC 인스턴스에 연결해야 합니다. 인스턴스에 연결하는 방법에 대한 자세한 내용은 AWS Systems Manager 세션 관리자를 참조하십시오. SSH를 사용하여 SDC 인스턴스에 연결하는 포트는 보안상의 이유로 노출되지 않습니다.

# 보안 디바이스 커넥터의 IP 주소 변경

시작하기 전에

- 이 작업을 수행하려면 관리자여야 합니다.
- SDC는 TCP 포트 443 또는 디바이스 관리를 위해 구성한 포트에서 인터넷에 대한 전체 아웃바운드 액세스 권한을 가져야 합니다.

참고 SDC의 IP 주소를 변경한 후 디바이스를 CDO에 다시 등록할 필요가 없습니다.

---

단계 1 SDC에 대한 SSH 연결을 생성하거나 가상 머신의 콘솔을 열고 CDO 사용자로 로그인합니다.

단계 2 IP 주소를 변경하기 전에 SDC VM의 네트워크 인터페이스 구성 정보를 보려면 `ifconfig` 명령을 사용합니다.

```
[cdo@localhost ~]$ ifconfig
```

단계 **3** 인터페이스의 IP 주소를 변경하려면 `sudo sdc-onboard setup` 명령을 입력합니다.

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

단계 **4** 프롬프트에 비밀번호를 입력합니다.

```
[sudo] password for cdo:
```

단계 **5** 루트 및 CDO 비밀번호를 재설정하라는 프롬프트에 `n`을 입력합니다.

```
Would you like to reset the root and cdo passwords? (y/n):
```

단계 **6** 네트워크 재구성 프롬프트에 `y`를 입력합니다.

```
Would you like to re-configure the network? (y/n):
```

단계 **7** 메시지가 표시되면 SDC에 할당하려는 새 IP 주소와 SDC VM의 다른 도메인 정보를 입력합니다.

a) IP Address(IP 주소)
b) 게이트웨이
c) DNS 서버
d) NTP 서버 또는 FQDN

   또는 NTP 서버 또는 FQDN이 적용되지 않는 경우 Enter 키를 누릅니다.

e) Docker 브리지

   또는 docker 브리지가 적용되지 않는 경우 Enter 키를 누릅니다.

단계 **8** 값의 정확성을 묻는 메시지가 표시되면 `y`로 항목을 확인합니다.

```
Are these values correct? (y/n):
```

참고 이 명령을 실행하면 이전 IP 주소에 대한 SSH 연결이 끊어지므로, `y`를 입력하기 전에 값이 정확한지 확인합니다.

단계 **9** SDC에 할당한 새 IP 주소를 사용하여 SSH 연결을 만들고 로그인합니다.

단계 **10** 연결 상태 테스트 명령을 실행하여 SDC가 실행 중인지 확인할 수 있습니다.

```
[cdo@localhost ~]$ sudo sdc-onboard status
```

모든 확인 항목은 녹색으로 `[ OK(확인) ]`이라고 표시되어야 합니다.

참고 VM의 콘솔에서 이 절차를 수행하는 경우 값이 올바른지 확인하면 연결 상태 테스트가 자동으로 실행되고 상태가 표시됩니다.

단계 **11** CDO 사용자 인터페이스를 통해 SDC의 연결을 확인할 수도 있습니다. 이렇게 하려면 CDO 애플리케이션을 열고 **Tools & Services(**도구 및 서비스**)** > **Secure Connectors** 페이지로 이동합니다.

단계 **12** 페이지를 한 번 새로 고치고 IP 주소를 변경한 보안 커넥터를 선택합니다.

단계 **13** **Actions(**작업**)** 창에서 **Request Heartbeat(**하트비트 요청**)**를 클릭합니다.

하트비트 요청 성공 메시지가 표시되고, 마지막 하트비트에 현재 날짜와 시간이 표시되어야 합니다.

중요 변경한 IP 주소는 GMT 오전 3시 이후에만 SDC의 세부 정보 창에 반영됩니다.

VM에 SDC를 배포하는 방법에 대한 자세한 내용은 자체 VM에 보안 디바이스 커넥터 구축, 12 페이지를 참조하세요.

# 보안 디바이스 커넥터 제거

**Warning** 이 절차에서는 SDC(보안 디바이스 커넥터)를 삭제합니다. 이는 되돌릴 수 없습니다. 이 작업을 수행한 후에는 새 SDC를 설치하고 디바이스를 다시 연결할 때까지 해당 SDC에 연결된 디바이스를 관리할 수 없습니다. 디바이스를 다시 연결하려면 다시 연결해야 하는 각 디바이스에 대한 관리자 자격 증명을 다시 입력해야 할 수 있습니다.

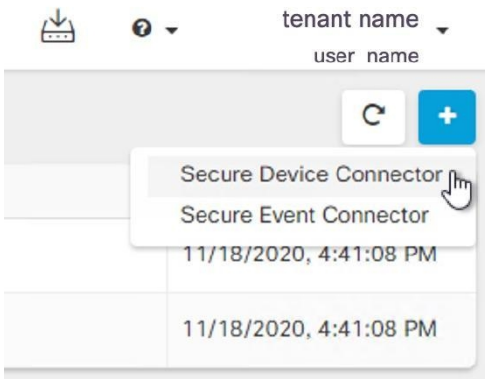
테넌트에서 SDC를 제거하려면 다음 절차를 수행합니다.

단계 **1** 삭제할 SDC에 연결된 모든 디바이스를 제거합니다. 다음 두 가지 방법 중 하나로 하면 됩니다.

- 일부 디바이스를 다른 SDC로 이동하거나 SDC에서 완전히 벗어나십시오. 자세한 내용은 아래를 참조하십시오.
- 삭제할 SDC에 연결된 모든 디바이스를 CDO에서 제거합니다.
  a. SDC에서 사용하는 모든 디바이스를 식별하려면 동일한 SDC를 사용하여 CDO에 연결하는 모든 디바이스 찾기를 참조하십시오.
  b. **Inventory(**재고 목록**)** 페이지에서 식별한 모든 디바이스를 선택합니다.
  c. Device Actions(디바이스 작업) 창에서 **Remove(**제거**)**를 클릭하고 **OK(**확인**)**를 클릭하여 작업을 확인합니다.

단계 **2** CDO 메뉴에서 **Tools & Services(**툴 및 서비스**)** > **Secure Connectors(**보안 커넥터**)**를 선택합니다.

단계 **3** Secure Connectors(보안 커넥터) 페이지에서 파란색 더하기 버튼을 클릭하고 **Secure Device Connector(**보안 디바이스 커넥터**)**를 선택합니다.



단계 **4** Secure Connector(보안 커넥터) 테이블에서 제거할 SDC를 선택합니다. 이제 디바이스 수가 0이어야 합니다.

단계 **5** 작업 창에서 **Remove(**제거**)**를 클릭합니다. 다음 경고가 표시됩니다.

**Warning** <sdc_name>을 삭제하려고 합니다. SDC 삭제는 되돌릴 수 없습니다. SDC를 삭제하면 디바이스를 온보딩하거나 다시 온보딩하기 전에 새 SDC를 생성하고 온보딩해야 합니다.

현재 온보딩된 디바이스가 있으므로 SDC를 제거하려면 새 SDC를 설정한 후 해당 디바이스를 다시 연결하고 자격 증명을 다시 제공해야 합니다.

- 질문이나 우려 사항이 있는 경우 **Cancel(**취소**)**을 클릭하고 CDO 지원에 문의하십시오.
- 계속하려면 <sdc_name>을 입력란에 입력하고 **OK(**확인**)**를 클릭합니다.

단계 **6** 확인 대화 상자에서 계속 진행하려면 경고 메시지에 나와 있는 SDC의 이름을 입력합니다.

단계 **7** **OK(**확인**)**를 클릭하여 SDC 제거를 확인합니다.

# SDC 간에 ASA 이동

CDO는 단일 CDO 테넌트에서 여러 SDC 사용 다음 절차를 사용하여 한 SDC에서 다른 SDC로 관리형 ASA를 이동할 수 있습니다.

단계 **1** 탐색 모음에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭한 다음 **ASA** 탭을 클릭합니다.

단계 **3** 다른 SDC로 이동하려는 ASA를 선택합니다.

단계 **4** **Device Actions(**디바이스 작업**)** 창에서 **Update Credentials(**자격 증명 업데이트**)**를 클릭합니다.

단계 **5** 보안 디바이스 커넥터 버튼을 클릭하고 디바이스를 이동하려는 SDC를 선택합니다.

단계 **6** CDO가 디바이스에 로그인하는 데 사용하는 관리자 사용자 이름과 암호를 입력하고 **Update(**업데이트**)**를 클릭합니다. 변경되지 않은 경우 관리자 사용자 이름과 암호는 ASA 온보딩에 사용한 것과 동일한 자격 증명입니다. 이러한 변경 사항을 디바이스에 배포할 필요는 없습니다.

참고 모든 ASA가 동일한 자격 증명을 사용하는 경우 한 SDC에서 다른 SDC로 ASA를 대량으로 이동할 수 있습니다. ASA에 다른 자격 증명이 있는 경우 한 번에 하나의 SDC에서 다른 하나로 이동해야 합니다.

# Meraki MX 연결 자격 증명 업데이트

Meraki 대시보드에서 새 API 키를 생성하는 경우 CDO에서 연결 자격 증명을 업데이트해야 합니다. 새 키를 생성하려면 Meraki API 키 생성 및 검색에서 자세한 내용을 확인하십시오. CDO에서는 디바이스 자체에 대한 연결 자격 증명을 업데이트할 수 없습니다. 필요한 경우 Meraki 대시보드에서 API 키를 수동으로 새로 고칠 수 있습니다. 자격 증명을 업데이트하고 통신을 다시 설정하려면 CDO UI에서 API 키를 수동으로 업데이트해야 합니다.

**Note** CDO가 디바이스를 동기화하지 못하면 CDO의 연결 상태에 "Invalid Credentials(유효하지 않은 자격 증명)"가 표시될 수 있습니다. 이 경우 API 키를 사용하려고 시도했을 수 있습니다. 선택한 Meraki MX의 API 키가 올바른지 확인합니다.

Meraki MX 디바이스에 대한 자격 증명을 업데이트하려면 다음 절차를 사용합니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭한 다음 **Meraki** 탭을 클릭합니다.

단계 **3** 연결 자격 증명을 업데이트할 Meraki MX를 선택합니다.

단계 **4** **Device Actions(**디바이스 작업**)** 창에서 **Update Credentials(**자격 증명 업데이트**)**를 클릭합니다.

단계 **5** CDO가 디바이스에 로그인하는 데 사용하는 **API** 키를 입력하고 **Update(**업데이트**)**를 클릭합니다. 변경하지 않는 한 이 API 키는 Meraki MX를 온보딩하는 데 사용한 것과 동일한 자격 증명입니다. 이러한 변경 사항을 디바이스에 구축할 필요는 없습니다.

# 보안 디바이스 커넥터 이름 변경

단계 **1** CDO 메뉴에서 **Tools & Services(**툴 및 서비스**)** > **Secure Connectors(**보안 커넥터**)**를 선택합니다.

단계 **2** 이름을 바꾸려는 SDC를 선택합니다.

단계 **3** 세부 정보 창에서 SDC 이름 옆에 있는 편집 아이콘 를 클릭합니다.

단계 **4** SDC의 이름을 바꿉니다.

**Inventory(**인벤토리**)** 창의 보안 디바이스 커넥터 필터를 포함하여 CDO 인터페이스에 SDC 이름이 나타날 때마다 이 새 이름이 나타납니다.

# 기본 보안 디바이스 커넥터 지정

전부는 아니지만 CDO에서 관리하는 많은 디바이스가 SDC를 통해 CDO에 연결됩니다. SDC를 통해 CDO에 연결하는 디바이스를 온보딩하는 경우 온보딩 중에 달리 지정하지 않는 한 테넌트의 기본 SDC와 연결됩니다.

보안 커넥터 페이지에서 기본적으로 선택되는 SDC를 지정할 수 있습니다.

단계 **1** CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.

단계 **2** 기본값으로 사용할 SDC를 선택합니다.

단계 **3** 작업 창에서 **Make Default(**기본값으로 설정**)**를 클릭합니다. Make Default(기본값으로 설정) 작업이 표시되지 않으면 SDC가 이미 기본 SDC인 것입니다.

# 보안 디바이스 커넥터 업데이트

이 절차를 문제 해결 툴로 사용합니다. 일반적으로 SDC는 자동으로 업데이트되므로 이 절차를 사용할 필요가 없습니다. 그러나 VM의 시간 구성이 잘못된 경우 SDC는 업데이트를 수신하기 위해 AWS에 연결할 수 없습니다. 이 절차는 SDC의 업데이트를 시작하며 시간 동기화 문제로 인한 오류를 해결합니다.

단계 **1** SDC에 연결합니다. SSH를 사용하여 연결하거나 VMware 하이퍼바이저에서 콘솔 보기를 사용할 수 있습니다.)

단계 **2** **cdo** 사용자로 SDC에 로그인합니다.

단계 **3** SDC 도커 컨테이너를 업데이트하려면 SDC 사용자로 전환합니다.

```
[cdo@sdc-vm ~]$ sudo su sdc
                [sudo] password for cdo: <type password for cdo user>
                [sdc@sdc-vm ~]$
```

단계 **4** SDC 툴킷을 업그레이드합니다.

```
[cdo@sdc-vm ~]$ /usr/local/cdo/toolkit/toolkit.sh upgradeToolkit
                [sdc@sdc-vm ~]$
```

단계 **5** SDC를 업그레이드합니다.

```
[cdo@sdc-vm ~]$ /usr/local/cdo/toolkit/toolkit.sh upgradeSDC
                [sdc@sdc-vm ~]$
```

# 단일 **CDO** 테넌트에서 여러 **SDC** 사용

테넌트에 대해 둘 이상의 SDC를 구축하면 성능 저하 없이 더 많은 디바이스를 관리할 수 있습니다. 단일 SDC에서 관리할 수 있는 디바이스의 수는 해당 디바이스에 구현된 기능 및 해당 구성 파일의 크기에 따라 달라집니다.

테넌트에 SDC를 무제한으로 설치할 수 있습니다. 각 SDC는 하나의 네트워크 세그먼트를 관리할 수 있습니다. 이러한 SDC는 해당 네트워크 세그먼트의 디바이스를 동일한 CDO 테넌트에 연결합니다. 여러 SDC가 없으면 서로 다른 CDO 테넌트를 사용하여 격리된 네트워크 세그먼트에서 디바이스를 관리해야 합니다.

두 번째 또는 후속 SDC를 구축하는 절차는 첫 번째 SDC를 구축할 때와 동일합니다. CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축하거나 자체 VM에 보안 디바이스 커넥터 구축할 수 있습니다. 테넌트의 초기 SDC는 테넌트의 이름과 숫자 1을 통합합니다. 각 추가 SDC는 순서대로 번호가 매겨집니다.

# 동일한 SDC를 사용하여 CDO에 연결하는 모든 디바이스 찾기

동일한 SDC를 사용하여 CDO에 연결하는 모든 디바이스를 식별하려면 다음 절차를 수행합니다.

단계 1 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 2 **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 필터 기준이 이미 지정된 경우 Inventory(재고 목록) 테이블 상단에 있는 **clear(**지우기**)** 버튼을 클릭하여 CDO로 관리하는 모든 디바이스 및 서비스를 표시합니다.

단계 5 필터 버튼 을 클릭하여 필터 메뉴를 확장합니다.

단계 6 필터의 Secure Device Connectors(보안 디바이스 커넥터) 섹션에서 원하는 SDC의 이름을 확인합니다. Inventory(재고 목록) 테이블에는 필터에서 선택한 SDC를 통해 CDO에 연결하는 디바이스만 표시됩니다.

단계 7 (선택 사항) 필터 메뉴에서 추가 필터를 선택하여 검색을 더욱 구체화합니다.

단계 8 (선택 사항) 작업이 완료되면 Inventory(재고 목록) 테이블 상단에 있는 **clear(**지우기**)** 버튼을 클릭하여 CDO로 관리하는 모든 디바이스 및 서비스를 표시합니다.

# 보안 디바이스 커넥터 오픈 소스 및 서드파티 라이선스 특성

========== ==========

*** amqplib ***

**amqplib copyright (c) 2013, 2014**

**Michael Bridgen <mikeb@squaremobius.net>**

이 패키지 **"amqplib"**는 **MIT** 라이선스에 따라 라이선스가 부여됩니다**.** 사본은 이 디렉토리의 **LICENSE-MIT** 파일에서 찾거나 다음에서 다운로드할 수 있습니다**.**

http://opensource.org/licenses/MIT

==========

*** async ***

**Copyright (c) 2010-2016 Caolan McMahon**

본 소프트웨어와 관련 문서 파일**(**이하 "소프트웨어"**)**의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며**,** 이에 대한 비용은 부담하지 않습니다**.** 이는 소프트웨어의 사용**,** 복제**,** 수정**,** 통합**,** 게시**,** 배포**,** 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다**.** 또한**,** 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다**.**

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다**.**

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 취급과 관련하여 계약 행위, 불법 행위 또는 기타 행위 등의 클레임, 손해, 또는 기타 책임에 대해 책임을 지지 않습니다.

==========

*** bluebird ***

**The MIT License (MIT)**

**Copyright (c) 2013-2015 Petka Antonov**

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 취급과 관련하여 계약 행위, 불법 행위 또는 기타 행위 등의 클레임, 손해, 또는 기타 책임에 대해 책임을 지지 않습니다.

==========

*** cheerio ***

**Copyright (c) 2012 Matt Mueller <mattmuelle@gmail.com>**

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 취급과 관련하여 계약 행위, 불법 행위 또는 기타 행위 등의 클레임, 손해, 또는 기타 책임에 대해 책임을 지지 않습니다.

==========

*** command-line-args ***

**MIT** 라이선스**(MIT)**

**Copyright (c) 2015 Lloyd Brookes <75pound@gmail.com>**

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 취급과 관련하여 계약 행위, 불법 행위 또는 기타 행위 등의 클레임, 손해, 또는 기타 책임에 대해 책임을 지지 않습니다.

==========

*** ip ***

이 소프트웨어는 **MIT** 라이센스에 따라 라이센스가 부여됩니다.

**Copyright Fedor Indutny, 2012.**

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 취급과 관련하여 계약 행위, 불법 행위 또는 기타 행위 등의 클레임, 손해, 또는 기타 책임에 대해 책임을 지지 않습니다.

==========

*** json-buffer ***

**Copyright (c) 2013 Dominic Tarr**

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다.어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 거래와 관련하여 계약, 불법 행위 등으로 인해 발생한 어떠한 클레임, 손해, 또는 기타 책임에 대해서도 책임을 지지 않습니다.

==========

*** json-stable-stringify ***

이 소프트웨어는 **MIT** 라이선스에 따라 배포됩니다.

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 취급과 관련하여 계약 행위, 불법 행위 또는 기타 행위 등의 클레임, 손해, 또는 기타 책임에 대해 책임을 지지 않습니다.

==========

*** json-stringify-safe ***

**ISC** 라이선스

**Copyright (c) Isaac Z. Schlueter and Contributors**

위의 저작권 고지와 이 허가 고지가 모든 사본에 포함되어 있는 한, 본 소프트웨어를 비용 여부에 상관없이 어떤 목적으로든 사용, 복사, 수정 및/또는 배포할 수 있는 권한이 여기에 부여됩니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자는 본 소프트웨어의 사용 또는 성능과 관련하여 계약, 과실 또는 기타 불법 행위로 인해 발생한 어떠한 직접적, 간접적, 부수적, 특별, 징벌적 또는 결과적 손해(대체 상품 또는 서비스의 조달, 사용, 데이터 또는 이익의 손실, 사업 중단을 포함하되 이에 국한되지 않음)에 대해 책임을 지지 않습니다.

==========

*** lodash ***

**Copyright JS Foundation and other contributors** <https://js.foundation/>

**Underscore.js, copyright Jeremy Ashkenas** 기반

**DocumentCloud** 및 조사 리포터 및 편집자<http://underscorejs.org/>

이 소프트웨어는 많은 개인의 자발적 기여로 구성됩니다. 정확한 기여 내역은 다음에서 제공되는 https://github.com/lodash/lodash 개정 내역을 참조하십시오.

다음 라이센스는 다음을 제외하고 이 소프트웨어의 모든 부분에 적용됩니다.

아래에 문서화:

====

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 본 소프트웨어의 사용 또는 성능과 관련하여 계약, 불법 행위 등으로 인해 발생한 어떠한 직접적, 간접적, 부수적, 특별, 우발적 또는 결과적 손해(대체 상품 또는 서비스의 조달, 사용, 데이터 또는 이익의 손실, 사업 중단을 포함하되 이에 국한되지 않음)에 대해 책임을 지지 않습니다.

====

샘플 코드에 대한 저작권 및 관련 권리는 **CC0**을 통해 포기됩니다. 샘플 코드는 문서의 산문 내에 표시되는 모든 소스 코드로 정의됩니다.

CC0: http://creativecommons.org/publicdomain/zero/1.0/

====

**node_modules** 및 공급업체 디렉토리에 있는 파일은 자체 라이선스가 있는 이 소프트웨어에서 사용하는 외부에서 유지 관리되는 라이브러리입니다. 용어가 위의 용어와 다를 수 있으므로 해당 용어를 읽어보는 것이 좋습니다.

==========

*** log4js ***

**Copyright 2015 Gareth Jones (**다른 많은 사람들의 기여 포함**)**

**Apache** 라이선스 버전 **2.0("**라이선스**")**에 따라 라이선스가 부여됩니다. 라이센스를 준수하지 않는 한 이 파일을 사용할 수 없습니다. 다음에서 라이센스 사본을 얻을 수 있습니다.

http://www.apache.org/licenses/LICENSE-2.0

해당 법률에서 요구하거나 서면으로 동의하지 않는 한 라이선스에 따라 배포된 소프트웨어는 명시적이든 묵시적이든 어떠한 종류의 보증이나 조건 없이 "있는 그대로" 배포됩니다.라이선스에 따른 권한 및 제한 사항을 관리하는 특정 언어는 라이선스를 참조하십시오.

==========

*** mkdirp ***

**Copyright 2010 James Halliday(mail@substack.net)**

이 프로젝트는 **MIT/X11** 라이선스에 따라 배포되는 무료 소프트웨어입니다.

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 취급과 관련하여 계약 행위, 불법 행위 또는 기타 행위 등의 클레임, 손해, 또는 기타 책임에 대해 책임을 지지 않습니다.

==========

*** node-forge ***

새로운 **BSD** 라이선스(**3**개 조항)

**Copyright (c) 2010, Digital Bazar, Inc.**

**All rights reserved.**

다음 조건을 충족하는 경우 수정 여부에 관계없이 소스 및 바이너리 형식으로 재배포 및 사용이 허용됩니다.

***** 소스 코드의 재배포는 위의 저작권 표시, 이 조건 목록 및 다음 면책 조항을 유지해야 합니다.

***** 바이너리 형식의 재배포는 배포와 함께 제공된 설명서 및/또는 기타 자료에 위의 저작권 고지, 이 조건 목록 및 다음 면책 조항을 복제해야 합니다.

*** Digital Bazaar, Inc.**의 이름이나 기여자의 이름은 특정 사전 서면 허가 없이 이 소프트웨어에서 파생된 제품을 보증하거나 홍보하는 데 사용할 수 없습니다.

이 소프트웨어는 저작권자와 기여자에 의해 "있는 그대로" 제공되며, 명시적 또는 묵시적으로 상품성 및 특정 목적에의 적합성을 포함한 모든 보증이 거부됩니다. 어떠한 경우에도 **DIGITAL BAZAAR**는 어떠한 직접적, 간접적, 부수적, 특별, 징벌적 또는 결과적 손해(대체 상품 또는 서비스의 조달, 사용, 데이터 또는 이익의 손실, 사업 중단을 포함하되 이에 국한되지 않음)에 대해 책임을 지지 않습니다. 이러한 손해가 계약, 엄격한 책임, 불법행위(과실 또는 기타 포함)에 대한 어떠한 책임 이론에 의거하여 발생하였는지 여부와 상관없이, 해당 손해의 가능성이 있음을 사전에 고지받았더라도, 이 소프트웨어의 사용으로 인해 발생하는 어떠한 방식의 책임도 지지 않습니다.

==========

*** request ***

**Apache License**

버전 **2.0, January 2004**

http://www.apache.org/licenses/

사용, 복제 및 배포에 대한 약관

**1.** 정의.

"라이선스"는 이 문서의 섹션 **1**에서 **9**까지 정의된 사용, 복제 및 배포에 대한 조건을 의미합니다.

"라이선스 제공자"는 라이센스를 부여하는 저작권 소유자 또는 저작권 소유자가 승인한 법인을 의미합니다.

"법적 실체"는 행위 실체와 해당 실체를 통제하거나 통제받거나 공통 통제하에 있는 다른 모든 실체의 조합을 의미합니다. 이 정의의 목적상 "통제"는 **(i)** 계약 또는 기타 방식으로 해당 법인의 지시 또는 관리를 유발하는 직간접적인 권한 또는 **(ii) 50%(50%)** 또는 더 많은 발행주식, 또는 **(iii)** 해당 법인의 수익적 소유권.

"귀하"(또는 "귀하의")는 계약 또는 기타 방식으로 본 라이센스에 의해 부여된 권한을 행사하는 개인 또는 법인을 의미하거나 **(ii)** 다음 중 **50%** 이상을 소유합니다. 발행주식, 또는 **(iii)** 그러한 법인의 수익적 소유권.

"소스" 형식은 소프트웨어 소스 코드, 문서 소스 및 구성 파일을 포함하되 이에 국한되지 않는 수정을 위한 기본 형식을 의미합니다.

"개체" 형식은 컴파일된 개체 코드, 생성된 문서 및 다른 미디어 유형으로의 변환을 포함하되 이에 국한되지 않는 소스 형식의 기계적 변환 또는 변환으로 인해 발생하는 모든 형식을 의미합니다.

"저작물"은 저작물에 포함되거나 첨부된 저작권 표시(예는 아래 부록에 제공됨)에 표시된 대로 라이센스에 따라 사용 가능한 소스 또는 개체 형식의 저작물을 의미합니다.

"파생 저작물"은 저작물을 기반으로 하는(또는 저작물에서 파생된) 원본 또는 개체 형식의 모든 저작물을 의미하며 편집 편집, 주석, 정교화 또는 기타 편집이 전체적으로 저자의 원본 저작물을 나타냅니다. 본 라이선스에서 파생물은 저작물 및 그 파생물과 분리된 상태를 유지하거나 인터페이스에 단순히 링크(또는 이름으로 연결)되는 저작물은 포함하지 않습니다.

"기여"는 원본 저작물과 저작물에 포함하기 위해 저작권 소유자 또는 저작권 소유자를 대신하여 제출할 권한이 있는 개인 또는 법인이 라이선스 허가자에게 의도적으로 제출된 저작물 또는 파생물에 대한 편집 또는 추가를 포함한 저작물을 의미합니다. 이 정의에서 \"제출\"은 저작물에 대해 논의하고 개선하기 위해 라이선스 허가자 또는 그 대리인에게 전송되는 모든 형태의 전자, 구두 또는 서면 제출을 의미합니다. 여기에는 저작물을 논의하고 개선할 목적으로 라이선스 허가자 또는 그 대리인이 관리하는 전자 메일 목록, 소스 코드 제어 시스템, 문제 추적 시스템을 통한 커뮤니케이션이 포함되며 이에 국한되지 않습니다. 단, 저작권 소유자가 "기고문이 아님"을 명시적으로 표시하거나 서면으로 지정한 커뮤니케이션은 제외됩니다.

"기여자"는 라이선스 제공자 및 라이선스 제공자가 대신하여 기여물을 받아 작업물에 통합한 모든 개인 또는 법인을 의미합니다.

**2.** 저작권 라이선스 부여. 이 라이선스의 조건에 따라 각 기여자는 이로써 귀하에게 영구적이고 전 세계적이며 비독점적이고 무료이며 로열티가 없고 취소할 수 없는 저작권 라이선스를 부여합니다. 저작물 및 그러한 파생 저작물을 소스 또는 개체 형태로 재라이선스하고 배포합니다.

**3.** 특허 라이선스 부여. 본 라이선스의 약관에 따라 각 기여자는 귀하에게 저작물의 제작, 사용, 판매 제안, 판매, 가져오기, 기타 방식의 이전을 위한 영구적, 세계적, 비독점적, 요금 및 로열티 무료, 철회 불가능한(본 섹션에 명시된 경우 제외) 특허 라이선스를 부여합니다. 이러한 라이선스는 기여자가 부

여할 수 있는 특허권에만 적용되며, 이는 기여물 단독으로 또는 기여물이 제출된 저작물과의 조합으로 인해 침해될 수 있습니다. 귀하가 저작물 또는 저작물에 통합된 기여가 직접적 또는 기여적 특허 침해를 구성한다고 주장하는 어떤 법인에 대해 특허 소송(소송에서 교차 청구 또는 반소 포함)을 제기하는 경우, 본 라이선스에 따라 귀하에게 부여된 모든 특허 라이선스는 작업은 그러한 소송이 제기된 날짜에 종료됩니다.

**4.** 재배포. 귀하는 다음 조건을 충족하는 경우 편집 여부에 관계없이 모든 매체와 소스 또는 개체 형식으로 저작물 또는 그 파생 저작물의 사본을 재생산 및 배포할 수 있습니다.

귀하는 저작물 또는 파생 저작물의 다른 수령인에게 본 라이센스의 사본을 제공해야 합니다. 그리고

귀하는 수정된 파일에 귀하가 파일을 변경했음을 알리는 눈에 띄는 통지를 전달해야 합니다. 그리고

파생 저작물의 일부와 관련되지 않은 통지를 제외하고 저작물의 소스 형식에서 가져온 모든 저작권, 특허, 상표 및 귀속 고지를 귀하가 배포하는 파생 저작물의 소스 형식으로 유지해야 합니다. 그리고

저작물이 배포의 일부로 "**NOTICE**" 텍스트 파일을 포함하는 경우 귀하가 배포하는 모든 파생 저작물에는 그러한 **NOTICE** 파일에 포함된 귀속 고지의 읽을 수 있는 사본이 포함되어야 합니다. 다음 위치 중 적어도 하나에 있는 **2**차 저작물**: 2**차 저작물의 일부로 배포되는 **NOTICE** 텍스트 파일 내에서 파생 저작물과 함께 제공되는 경우 소스 양식 또는 문서 내에서; 또는 파생 저작물에 의해 생성된 디스플레이 내에서 그러한 제**3**자 고지가 일반적으로 표시되는 경우**. NOTICE** 파일의 내용은 정보 제공의 목적으로만 사용되며 이에 따라 라이선스가 편집되지 않습니다. 저작물의 **NOTICE** 텍스트와 함께 또는 그 부록으로 배포하는 파생물 내 속성 고지로 인해 라이선스가 변경되지 않는 경우, 이러한 추가적인 속성 고지를 추가할 수 있습니다. 귀하는 귀하의 편집 사항에 자신의 저작권 진술을 추가할 수 있으며 편집 사항의 사용, 복제 또는 배포 또는 그러한 파생 저작물 전체에 대한 추가 또는 다른 라이선스 조건을 제공할 수 있습니다. 그렇지 않으면 저작물은 본 라이선스에 명시된 조건을 준수합니다.

**5.** 기여물 제출. 귀하가 달리 명시하지 않는 한, 귀하가 저작물에 포함하기 위해 라이선스 허가자에게 의도적으로 제출한 모든 기여물은 추가 약관 없이 본 라이선스의 약관에 따라야 합니다. 위의 내용에도 불구하고 여기의 어떠한 내용도 그러한 기여와 관련하여 귀하가 라이선스 제공자와 체결한 별도의 라이선스 계약 조건을 대체하거나 편집하지 않습니다.

**6.** 상표. 본 라이선스는 저작물의 출처를 설명하고 **NOTICE** 파일의 내용을 재생산하는 데 합당하고 관례적인 사용에 필요한 경우를 제외하고 라이선스 제공자의 상표명, 상표, 서비스 마크 또는 제품 이름을 사용할 수 있는 권한을 부여하지 않습니다.

**7.** 보증의 면책조항. 해당 법률에 의해 요구되는 경우나 서면으로 합의된 경우를 제외하고, 라이선서는 작업물(및 각 기여자는 자신의 기여물)을 "있는 그대로" 제공하며, 명시적이거나 묵시적으로 어떠한 종류의 보증이나 조건도 포함하지 않습니다. 이는 제목, 비침해성, 상품성 또는 특정 목적에 대한 적합성에 대한 어떠한 보증이나 조건을 포함합니다. 귀하는 저작물 사용 또는 재배포의 적합성을 판단할 전적인 책임이 있으며 본 라이선스에 따른 귀하의 권한 행사와 관련된 모든 위험을 감수합니다.

**8.** 책임의 제한. 어떠한 경우에도, 과실(비롯하여 과실포함 책임), 계약 또는 기타 이론에 의한, 해당 법에 의해 요구되는 경우(예: 고의적이고 중대한 과실 행위)나 서면으로 합의된 경우를 제외하고, 어떤 기여자도 본 라이선스로 인한 손해에 대해 법적으로 책임을지지 않습니다. 이는 작업물의 사용 또는 사용 불능으로 인해 발생하는 어떠한 종류의 직접적, 간접적, 특수적, 우발적 또는 결과적 손해(예: 선의의 상실, 작업 중단, 컴퓨터 고장 또는 장애, 그 외 모든 상업적 손해나 손실을 포함)에 대해서도

책임을지지 않습니다. 심지어 해당 기여자에게 그러한 손해의 가능성이 알려져 있더라도 마찬가지입니다.

**9.** 보증 또는 추가 책임 수락. 저작물 또는 그 파생물을 재배포하는 경우 귀하는 지원, 보증, 면책 또는 본 라이선스와 일치하는 기타 책임 의무 및/또는 권리의 수락을 제공하고 요금을 청구할 수 있습니다. 그러나 이러한 의무를 수락할 때에는 다른 기여자를 대신하여 행동하지 않고 오로지 자신의 명의로, 자신의 책임하에만 행동해야 하며, 해당 보증이나 추가적인 책임을 수락함으로써 발생하는 어떠한 책임에 대해서도 각 기여자를 면책시키고 방어하며 보호하기 위해 보증을 제공하는 경우에만 그렇게 행동할 수 있습니다.

이용 약관의 끝

==========

*** rimraf ***

**ISC** 라이선스

**Copyright (c) Isaac Z. Schlueter and Contributors**

위의 저작권 고지와 이 허가 고지가 모든 사본에 포함되어 있는 한, 본 소프트웨어를 비용 여부에 상관없이 어떤 목적으로든 사용, 복사, 수정 및/또는 배포할 수 있는 권한이 여기에 부여됩니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태**("**있는 그대로**")**로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자는 본 소프트웨어의 사용 또는 성능과 관련하여 계약, 과실 또는 기타 불법 행위로 인해 발생한 어떠한 직접적, 간접적, 부수적, 특별, 징벌적 또는 결과적 손해(대체 상품 또는 서비스의 조달, 사용, 데이터 또는 이익의 손실, 사업 중단을 포함하되 이에 국한되지 않음)에 대해 책임을 지지 않습니다.

==========

*** uuid ***

**Copyright (c) 2010-2012 Robert Kieffer**

**MIT** 라이선스- http://opensource.org/licenses/mit-license.php

==========

*** validator ***

**Copyright (c) 2016 Chris O'Hara <cohara87@gmail.com>**

본 소프트웨어와 관련 문서 파일**(**이하 "소프트웨어"**)**의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태**("**있는 그대로**")**로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 본 소프트웨어

의 사용 또는 성능과 관련하여 계약, 불법 행위 등으로 인해 발생한 어떠한 직접적, 간접적, 부수적, 특별, 우발적 또는 결과적 손해(대체 상품 또는 서비스의 조달, 사용, 데이터 또는 이익의 손실, 사업 중단을 포함하되 이에 국한되지 않음)에 대해 책임을 지지 않습니다.

==========

*** when ***

오픈 소스 이니셔티브 **OSI - MIT** 라이선스

http://www.opensource.org/licenses/mit-license.php

**Copyright (c) 2011 Brian Cavalier**

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 본 소프트웨어의 사용 또는 성능과 관련하여 계약, 불법 행위 등으로 인해 발생한 어떠한 직접적, 간접적, 부수적, 특별, 우발적 또는 결과적 손해(대체 상품 또는 서비스의 조달, 사용, 데이터 또는 이익의 손실, 사업 중단을 포함하되 이에 국한되지 않음)에 대해 책임을 지지 않습니다.==========

# CDO에 로그인

Cisco Defense Orchestrator(CDO)에 로그인하려면 고객에게 SAML 2.0 호환 IdP(Identity Provider), 다단계 인증 제공자 및 사용자 관리가 있는 계정이 필요합니다.

IdP 어카운트에는 사용자의 자격 증명이 포함되며 IdP는 이러한 자격 증명을 기반으로 사용자를 인증합니다. 다단계 인증은 ID 보안의 추가 레이어를 제공합니다. CDO 사용자 레코드에는 주로 사용자 이름, 연결된 CDO 테넌트 및 사용자의 역할이 포함됩니다. 사용자가 로그인하면 CDO는 IdP의 사용자 ID를 CDO의 테넌트에 있는 기존 사용자 레코드에 매핑하려고 시도합니다. CDO가 일치 항목을 찾으면 사용자는 해당 테넌트에 로그인됩니다.

엔터프라이즈에 자체 SSO(Single Sign-On) ID 제공자가 없는 경우 ID 제공자는 Cisco Secure Cloud Sign-on입니다. Cisco Secure Cloud Sign-On은 다단계 인증에 Duo를 사용합니다. 고객은 원하는 경우 SAML SSO(Single Sign-On)를 Cisco Defense Orchestrator와 통합할 수 있습니다.

CDO에 로그인하려면 먼저 Cisco Secure Cloud Sign-On에서 계정을 생성하고 Duo Security를 사용하여 MFA(Multi-Factor Authentication)를 구성하고 테넌트 최고 관리자가 CDO 레코드를 생성하도록 해야 합니다.

2019년 10월 14일에 CDO는 Cisco Secure Cloud Sign-On을 ID 제공자 및 MFA용 Duo로 사용하도록 기존의 모든 테넌트를 변환했습니다.

참고

- 자체 SSO(Single Sign-On) ID 제공자를 사용하여 CDO에 로그인하는 경우 Cisco Secure Cloud Sign-On 및 Duo로의 전환이 영향을 미치지 않습니다. 고유한 로그인 솔루션을 계속 사용합니다.
- CDO 무료 평가판을 사용 중인 경우 이 전환이 영향을 미쳤습니다.

CDO 테넌트가 2019년 10월 14일 이후에 생성된 경우 새 CDO 테넌트에 대한 초기 로그인, 34 페이지를 참조하십시오.

2019년 10월 14일 이전에 CDO 테넌트가 존재했다면 Cisco Secure Cloud Sign On ID 제공자로 마이그레이션, 35 페이지를 참조하십시오.

# 새 CDO 테넌트에 대한 초기 로그인

Cisco Defense Orchestrator(CDO)는 Cisco Secure Cloud Sign-On을 ID 제공자로 사용하며, MFA(multi-factor authentication)에는 Duo를 사용합니다. **CDO**에 로그인하려면 먼저 **Cisco Secure Sign-On**에서 계정을 생성하고 **Duo**를 사용하여 **MFA**를 구성해야 합니다.

v에는 사용자 ID를 보호하기 위해 추가 보안 레이어를 제공하는 MFA가 필요합니다. MFA 유형인 이중 인증에서는 CDO에 로그인하는 사용자의 ID를 확인하기 위해 두 가지 구성 요소 또는 요소가 필요합니다. 첫 번째 요소는 사용자 이름과 비밀번호이고, 두 번째 요소는 요청 시 생성되는 일회용 비밀번호(OTP)입니다.

중요

**2019**년 **10**월 **14**일 이전에 **CDO** 테넌트가 존재했다면 이 문서 대신 Cisco Secure Cloud Sign On ID 제공자로 마이그레이션, 35 페이지를 사용하여 로그인 지침을 사용합니다.

시작하기 전에

**DUO Security** 설치**.** 휴대전화에 Duo Security 앱을 설치하는 것이 좋습니다. Duo 설치에 대한 질문은 Duo 이중 인증 가이드: 등록 가이드를 참고하십시오.

시간 동기화. 모바일 디바이스를 사용하여 일회용 비밀번호를 생성합니다. OTP는 시간을 기반으로 하므로 디바이스 시계를 실시간으로 동기화하는 것이 중요합니다. 디바이스 시계가 자동으로 또는 수동으로 올바른 시간으로 설정되었는지 확인합니다.

다음 작업**?**

새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성, 63 페이지를 계속합니다. 이는 4단계 프로세스입니다. 4단계를 모두 완료해야 합니다.

## 로그인 실패 문제 해결

실수로 잘못된 **CDO** 지역에 로그인했기 때문에 로그인에 실패함

적절한 CDO 지역에 로그인했는지 확인합니다. https://sign-on.security.cisco.com에 로그인하면 액세스할 지역을 선택할 수 있습니다. **CDO**타일을 클릭하여 defenceorchestrator.com에 액세스하거나 **CDO(EU)**를 클릭하여 defenceorchestrator.eu에 액세스합니다.

# Cisco Secure Cloud Sign On ID 제공자로 마이그레이션

2019년 10월 14일, Cisco Defense Orchestrator(CDO)는 모든 테넌트를 MFA(multi-factor authentication)를 위한 ID 제공자 및 Duo로 Cisco Secure Cloud Sign-On으로 변환했습니다. **CDO**에 로그인하려면 먼저 **Cisco Secure Sign-On**에서 계정을 활성화하고 **Duo**를 사용하여 **MFA**를 구성해야 합니다.

CDO에는 사용자 ID를 보호하기 위해 추가 보안 레이어를 제공하는 MFA가 필요합니다. MFA 유형인 이중 인증에서는 CDO에 로그인하는 사용자의 ID를 확인하기 위해 두 가지 구성 요소 또는 요소가 필요합니다. 첫 번째 요소는 사용자 이름과 비밀번호이고, 두 번째 요소는 요청 시 생성되는 일회용 비밀번호(OTP)입니다.

참고

- 자체 SSO(Single Sign-On) ID 제공자를 사용하여 CDO에 로그인하는 경우 Cisco Secure Cloud Sign-On 및 Duo로의 전환이 영향을 미치지 않습니다. 고유한 로그인 솔루션을 계속 사용합니다.
- CDO 무료 평가판을 사용 중인 경우 이 전환이 적용됩니다.
- **CDO** 테넌트가 **2019**년 **10**월 **14**일 이후에 생성된 경우 이 문서 대신 새 CDO 테넌트에 대한 초기 로그인, 34 페이지에서 로그인 지침을 참조하십시오.

시작하기 전에

마이그레이션하기 전에 다음 단계를 수행하는 것이 좋습니다.

- **DUO Security** 설치**.** 휴대전화에 Duo Security 앱을 설치하는 것이 좋습니다. Duo 설치에 대한 질문은 Duo 이중 인증 가이드: 등록 가이드를 참고하십시오.
- 시간 동기화. 모바일 디바이스를 사용하여 일회용 비밀번호를 생성합니다. OTP는 시간을 기반으로 하므로 디바이스 시계를 실시간으로 동기화하는 것이 중요합니다. 디바이스 시계가 자동으로 또는 수동으로 올바른 시간으로 설정되었는지 확인합니다.
- 새 Cisco Secure Sign-On 어카운트 생성 및 Duo 다단계 인증 구성. 이는 4 단계 프로세스입니다. 4 단계를 모두 완료해야 합니다.

## 마이그레이션 후 로그인 실패 문제 해결

잘못된 사용자 이름 또는 암호로 인해 **CDO**에 로그인하지 못함

해결 방법 CDO에 로그인하려고 할 때 사용자 이름 및 비밀번호가 올바른 데도 로그인이 실패하는 것을 알고 있거나, "비밀번호를 잊음"를 시도하여 사용 가능한 비밀번호를 복원할 수 없는 경우, 새 Cisco Secure Cloud Sign-On 계정을 사용하려면 새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성, 63 페이지의 지침에 따라 새 Cisco Secure Cloud Sign-On 계정에 등록해야 합니다.

**Cisco Secure Cloud Sign-On** 대시보드 로그인에 성공했지만 **CDO**를 실행할 수 없음

해결 방법 CDO 테넌트와 다른 사용자 이름으로 Cisco Secure Cloud Sign-On 계정을 만들었을 수 있습니다. CDO와 Cisco Secure Sign-On 간의 사용자 정보를 표준화하려면 Cisco TAC(Technical Assistance Center)에 문의하십시오.

저장된 북마크를 사용한 로그인 실패

해결 방법 브라우저에 저장한 이전 북마크를 사용하여 로그인을 시도했을 수 있습니다. 북마크는 https://cdo.onelogin.com을 가리킬 수 있습니다.

해결 방법 https://sign-on.security.cisco.com에 로그인합니다.

- 해결 방법 아직 Cisco Secure Sign-On 계정을 생성하지 않은 경우 새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성
- 해결 방법 새 계정을 생성한 경우 대시보드에서 Cisco Defense Orchestrator(US), Cisco Defense Orchestrator(EU) 또는 Cisco Defense Orchestrator(APJC)에 해당하는 CDO 타일을 클릭합니다.
- 해결 방법 https://sign-on.security.cisco.com을 가리키도록 북마크를 업데이트합니다.

# Cisco Secure Cloud Sign On 대시보드에서 CDO 실행

단계 **1** Cisco Secure Cloud Sign-on 대시보드에서 해당 CDO 버튼을 클릭합니다. CDO 타일은 https://defenseorchestrator.com으로 안내하고 CDO(EU) 타일은 https://defenseorchestrator.eu로 안내합니다.

단계 **2** 두 인증자를 모두 설정한 경우 인증자 로고를 클릭하여 Duo Security 또는 Google Authenticator를 선택합니다.

- 기존 테넌트에 사용자 레코드가 이미 있는 경우 해당 테넌트에 로그인됩니다.
- 이미 여러 포털에 사용자 레코드가 있는 경우 연결할 포털을 선택할 수 있습니다.
- 여러 테넌트에 대한 사용자 레코드가 이미 있는 경우 연결할 CDO 테넌트를 선택할 수 있습니다.
- 기존 테넌트에 대한 사용자 레코드가 아직 없는 경우 CDO에 대해 자세히 알아보거나 평가판 테넌트를 요청할 수 있습니다.

포털 보기는 여러 테넌트에서 통합된 정보를 검색하고 표시합니다. 자세한 내용은 멀티 테넌트 포털 관리, on page 53을 참조하십시오.

테넌트 보기에는 사용자 레코드가 있는 여러 테넌트가 표시됩니다.


# 테넌트에서 슈퍼 관리자 관리

테넌트의 슈퍼 관리자 수를 제한하는 것이 가장 좋습니다. 슈퍼 관리자 권한을 가져야 하는 사용자를 결정하고 사용자 관리를 검토한 다음 다른 사용자의 역할을 "Admin(관리자)"으로 변경합니다.

# CDO에서 지원하는 소프트웨어 및 하드웨어

CDO 설명서에서는 CDO가 지원하는 소프트웨어 및 디바이스에 대해 설명합니다. CDO가 지원하지 않는 소프트웨어 및 디바이스는 지적하지 않습니다. 소프트웨어 버전 또는 디바이스 유형에 대한 지원을 명시적으로 요청하지 않는 경우 지원되지 않습니다.

관련 정보:

- ASA 지원 세부 사항, 37 페이지
- 브라우저 지원, 38 페이지

## ASA 지원 세부 사항

CDO는 CDO에서 지원하지 않는 ASASM(ASA Services Module)을 제외하고 ASAv 인스턴스를 포함하여 ASA 8.4 이상을 실행하는 모든 플랫폼(모델별 ASA 및 ASDM호환성 참조)을 관리할 수 있습니다.

CDO는 ASA 8.3을 실행하는 ASA를 온보딩할 수 있지만 변경 사항을 배포하거나 다른 방식으로 관리할 수는 없습니다. 지원은 "읽기 전용"입니다.

9.12 이전 버전에서 ASA 및 ASDM 업그레이드 사전 요건하는 등 ASA의 모든 버전을 지원하지 않는 CDO 기능이 있을 수 있습니다. 이러한 경우 CDO 설명서에 해당 기능에 대한 사전 요건과 함께 모든 버전 예외가 나열됩니다.

CDO는 ASA와 다른 운영 체제를 실행하는 ASA FirePOWER 모듈을 관리하지 않습니다. Firepower Management Center 또는 ASDM을 사용하여 ASA Firepower 모듈을 별도로 관리해야 합니다.

ASA 5508-X 및 5516-X를 최신 ROMMON 이미지로 업그레이드하는 것이 좋습니다. Cisco ASA 및 Firepower Threat Defense 이미지 재설치 가이드의 지침을 참조하십시오. 그렇지 않은 경우 다음 ASA 소프트웨어 버전을 사용합니다.

- ASA 9.6(x)~9.15(x)
- ASA 9.5(2), 9.5(3)

ASA, ASDM 및 하드웨어 호환성에 대한 자세한 내용은 Cisco Secure Firewall ASA 호환성 가이드를 참조하십시오.

# 클라우드 디바이스 지원 정보

다음 표에서는 클라우드 기반 디바이스에 대한 소프트웨어 및 디바이스 유형 지원에 대해 설명합니다. 아래 표의 디바이스 유형에 대한 온보딩 및 기능에 대한 자세한 내용은 관련 링크를 참조하십시오.

| 디바이스 유형 | 메모 |
|---|---|
| **Google Cloud Platform** | Google Cloud Platform(GCP)은 GCP 콘솔을 통해 업데이트를 수신합니다. 플랫폼 및 사용 가능한 서비스에 대한 자세한 내용은 Google Cloud 설명서를 참조하십시오. 확인 |
| **Microsoft Azure** | Azure는 Azure 콘솔을 통해 업데이트를 수신합니다. 플랫폼 및 사용 가능한 서비스에 대한 자세한 내용은 Azure 설명서를 참조하십시오. |

# 브라우저 지원

CDO는 다음 브라우저의 최신 버전을 지원합니다.

- Google Chrome
- Mozilla Firefox

# Cisco Defense Orchestrator 플랫폼 유지 관리 일정

### Cisco Defense Orchestrator 유지 관리 일정

CDO은 새로운 기능과 품질 개선으로 매주 플랫폼을 업데이트합니다. 이 일정에 따라 업데이트가 3시간 동안 이루어질 수 있습니다.

대부분의 경우 업데이트는 목요일에 완료되지만 필요한 경우 금요일 및 일요일의 유지 관리 시간이 사용됩니다.

표 *1: CDO* 유지 관리 일정

| 요일 | 시간<br>**(24**시간제**)** |
|---|---|
| 목요일 | 09:00 UTC - 12:00 UTC |
| 금요일 | 09:00 UTC - 12:00 UTC |
| 일요일 | 09:00 UTC - 12:00 UTC |

이 유지 관리 기간 동안 테넌트에 계속 액세스할 수 있으며 클라우드 사용 Firewall Management Center가 있는 경우, 해당 플랫폼에도 액세스할 수 있습니다. 또한 CDO에 온보딩한 디바이스가 보안 정책을 계속 적용합니다.

참고 유지 관리 기간 동안 관리하는 디바이스에 구성 변경 사항을 배포하는 데 CDO을 사용하지 않는 것이 좋습니다.

CDO를 중지하거나 클라우드 사용 Firewall Management Center과 통신을 중단되는 오류가 있는 경우, 해당 오류는 유지 관리 기간을 벗어나더라도 영향을 받는 모든 테넌트에서 가능한 한 빨리 해결됩니다.

### 클라우드 제공 Firewall Management Center 유지 관리 일정

테넌트에 배포된 클라우드 사용 Firewall Management Center을 보유한 고객은 CDO가 클라우드 사용 Firewall Management Center 환경을 업데이트하기 약 1주일 전에 알림을 받습니다. 테넌트의 슈퍼 관리자 및 관리 사용자는 이메일로 알림을 받습니다. CDO는 또한 모든 사용자에게 예정된 업데이트를 알리는 배너를 홈페이지에 표시합니다.

테넌트에 대한 업데이트는 최대 1시간이 걸릴 수 있으며 테넌트 지역에 할당된 유지 관리 날짜의 3시간 유지 관리 시간 내에 이루어집니다. 테넌트가 업데이트되는 동안에는 클라우드 사용 Firewall Management Center 환경에 액세스할 수 없지만, CDO의 나머지 부분에 계속 액세스할 수 있습니다.

표 2: 클라우드 제공 *Firewall Management Center* 유지 관리 일정

| 요일 | 시간<br>(24시간제) | 지역 |
|---|---|---|
| 수요일 | 04:00 UTC - 07:00 UTC | 유럽, 중동 또는 아프리카 (EMEA) |
| 수요일 | 17:00 UTC - 20:00 UTC | 아시아-태평양-일본(APJ) |
| 목요일 | 09:00 UTC - 12:00 UTC | 아메리카 |

# 테넌트 관리

Cisco Defense Orchestrator(CDO)는 설정 페이지에서 테넌트 및 개별 사용자 계정의 특정 측면을 사용자 지정할 수 있는 기능을 제공합니다. CDO 메뉴의 왼쪽 탐색 패널에서 **Settings**(설정)를 클릭합니다.

관련 정보:

- 일반 설정, 40 페이지
- 사용자 관리
- 로깅 설정
- 알림 설정, 44 페이지

## 일반 설정

오른쪽 상단의 관리자 드롭다운에서 **Settings**(설정)를 클릭합니다.

일반 CDO 설정에 관한 다음 항목을 참조하십시오.

- 사용자 설정, on page 41
- 내 토큰은 API 토큰, on page 49를 참조하십시오.
- **Tenant Settings**(테넌트 설정)은 다음을 참조하십시오.
  - 변경 요청 추적 활성화, on page 41
  - Cisco 지원에서 테넌트를 볼 수 없도록 설정, on page 41
  - 자동 구축 예약 옵션 활성화, on page 42
  - 기본 충돌 탐지 간격, on page 42
  - 웹 분석, on page 43
  - 테넌트 ID, on page 44

• 테넌트 이름, on page 44

## 사용자 설정

CDO UI를 표시할 언어를 선택합니다. 이 선택은 이 변경을 수행하는 사용자에게만 영향을 미칩니다.

## 내 토큰

자세한 내용은 API 토큰을 참조하십시오.

## 테넌트 설정

### 변경 요청 추적 활성화

변경 요청 추적을 활성화하면 테넌트의 모든 사용자에게 영향을 미칩니다. 변경 요청 추적을 활성화하려면 다음 절차를 따르십시오.

단계 **1** 오른쪽 상단의 관리자 드롭다운에서 **Settings(**설정**)**를 클릭합니다.

단계 **2** **General(**일반**)** 탭을 클릭합니다.

단계 **3** 변경 요청 추적 아래의 슬라이더를 클릭합니다.

확인되면 인터페이스의 왼쪽 하단 모서리에 변경 요청 도구 모음이 나타나고 변경 로그의 변경 요청 드롭다운 메뉴가 나타납니다.

### **Cisco** 지원에서 테넌트를 볼 수 없도록 설정

Cisco 지원에서는 지원 티켓을 해결하거나 두 개 이상의 고객에게 영향을 미치는 문제를 사전에 해결하기 위해 사용자를 테넌트와 연결합니다. 그러나 원하는 경우 계정 설정을 변경하여 Cisco 지원이 테넌트에 액세스하지 못하도록 할 수 있습니다. 이렇게 하려면 "Cisco 지원에서 이 테넌트를 볼 수 없도록 방지" 아래의 버튼을 밀어서 녹색 확인 표시를 표시합니다.

Cisco 지원에서 테넌트를 볼 수 없도록 하려면 다음 절차를 따르십시오.

단계 **1** 오른쪽 상단의 관리자 드롭다운에서 **Settings(**설정**)**를 클릭합니다.

단계 **2** **General(**일반**)** 탭을 클릭합니다.

단계 **3** **Cisco** 지원팀에서 이 테넌트를 볼 수 없도록 방지 아래의 슬라이더를 클릭합니다.

### 디바이스 변경 사항 자동 수락 옵션 활성화

디바이스 변경에 대한 자동 수락을 활성화하면 Defense Orchestrator가 디바이스에서 직접 수행된 모든 변경 사항을 자동으로 수락할 수 있습니다. 이 옵션을 비활성화된 상태로 두거나 나중에 비활성화하는 경우 수락하기 전에 각 디바이스 충돌을 검토해야 합니다.

디바이스 변경 사항에 대한 자동 수락을 활성화하려면 다음 절차를 따르십시오.

단계 **1** 오른쪽 상단의 관리자 드롭다운에서 **Settings(**설정**)**를 클릭합니다.

단계 **2** **General(**일반**)** 탭을 클릭합니다.

단계 **3** **Enable the option to auto-accept device changes(**디바이스 변경 사항을 자동으로 수락하는 옵션 활성화**)** 아래의 슬라이더를 클릭합니다.

## 기본 충돌 탐지 간격

이 간격은 CDO가 변경 사항을 위해 온보딩된 디바이스를 폴링하는 빈도를 결정합니다. 이 선택은 이 테넌트로 관리되는 모든 디바이스에 영향을 주며 언제든지 변경할 수 있습니다.

**Note** 하나 이상의 디바이스를 선택한 후 **Inventory(**재고 목록**)** 페이지에서 사용 가능한 **Conflict Detection(**충돌 탐지**)** 옵션을 통해 이 선택 항목을 오버라이드할 수 있습니다.

이 옵션을 구성하고 충돌 탐지를 위한 새 간격을 선택하려면 다음 절차를 수행합니다.

단계 **1** 오른쪽 상단의 관리자 드롭다운에서 **Settings(**설정**)**를 클릭합니다.

단계 **2** **General Settings(**일반 설정**)** 탭을 클릭합니다.

단계 **3** **Default Conflict Detection Interval(**기본 충돌 탐지 간격**)**의 드롭다운 메뉴를 클릭하고 시간 값을 선택합니다.

## 자동 구축 예약 옵션 활성화

자동 구축을 예약하는 옵션을 활성화하면 편리한 날짜와 시간에 향후 구축을 예약할 수 있습니다. 활성화되면 단일 또는 반복 자동 구축을 예약할 수 있습니다. 자동 구축을 예약하려면 자동 구축 예약을 참조하십시오.

전용 의 보류 중인 변경 사항이 있는 경우 디바이스에 대한 CDO의 변경 사항은 디바이스에 자동으로 구축되지 않습니다. 디바이스가 **Conflict Detected(**충돌 탐지됨**)** 또는 **Not Synced(**동기화되지 않음**)**와 같이 **Synced(**동기화됨**)** 상태가 아닌 경우 예약된 구축이 실행되지 않습니다. 예약된 구축이 실패한 모든 인스턴스가 작업 페이지에 나열됩니다.

**Enable the Option to Schedule Automatic Deployments(**자동 구축 예약 옵션 활성화**)**가 해제된 경우 예약된 모든 구축이 삭제됩니다.

**Important** CDO를 사용하여 디바이스에 대해 둘 이상의 예약된 구축을 생성하는 경우 새 구축이 기존 구축을 덮어씁니다. API를 사용하여 디바이스에서 둘 이상의 예약된 구축을 생성하는 경우, 새 구축을 예약하기 전에 기존 구축을 삭제해야 합니다.

자동 구축을 예약하는 옵션을 활성화하려면 다음 절차를 따르십시오.

단계 **1** 오른쪽 상단의 관리자 드롭다운에서 **Settings(**설정**)**를 클릭합니다.

단계 **2** **General Settings(**일반 설정**)** 탭을 클릭합니다.

단계 **3** **Enable the option to schedule automatic deployment(**자동 구축을 예약하는 옵션 활성화**)** 아래의 슬라이더를 클릭합니다.

## 웹 분석

웹 분석은 페이지 히트를 기반으로 익명의 제품 사용 정보를 Cisco에 제공합니다. 이 정보에는 확인한 페이지, 특정 페이지를 사용한 시간, 브라우저 버전, 제품 버전, 디바이스 호스트 이름 등이 포함됩니다. Cisco는 이 정보를 활용해 기능 사용 패턴을 확인하고 제품을 개선할 수 있습니다. 모든 사용량 데이터는 익명으로 전송되며 민감한 데이터는 전송되지 않습니다.

웹 분석은 기본적으로 활성화됩니다. 웹 분석을 비활성화하거나 나중에 활성화하려면 다음 절차를 따르십시오.

단계 **1** 오른쪽 상단의 관리자 드롭다운에서 **Settings(**설정**)**를 클릭합니다.

단계 **2** **General Settings(**일반 설정**)** 탭을 클릭합니다.

단계 **3** 웹 분석 아래의 슬라이더를 클릭합니다.

## 기본 반복 백업 일정 구성

여러 디바이스에서 백업 일정을 일관되게 하려면 이 설정을 사용하여 기본 반복 백업 일정을 구성하십시오. 특정 디바이스에 대한 백업을 예약할 때 기본 설정을 사용하거나 변경할 수 있습니다. 기본 반복 백업 일정을 변경해도 기존의 예약된 백업이나 반복 백업 일정은 변경되지 않습니다.

단계 **1** **Frequency(**빈도**)** 필드에서 매일, 매주 또는 매월을 선택합니다.

단계 **2** 백업을 수행할 시간을 24시간 단위로 선택합니다. UTC(Coordinated Universal Time)로 시간을 예약합니다.

- 매주 백업하는 경우: 백업을 수행할 요일을 확인합니다.
- 매월 백업하는 경우: **Days of Month(**날짜**)** 필드를 클릭하고 백업을 예약할 날짜를 추가합니다. 참고: 31일을 입력했지만 해당 월에 31일이 없는 경우 백업이 수행되지 않습니다. 예약된 백업 시간에 이름과 설명을 지정합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

테넌트 **ID**

테넌트 ID는 테넌트를 식별합니다. 이 정보는Cisco TAC(Technical Assistance Center)에 문의해야 하는 경우에 유용합니다.

테넌트 이름

테넌트 이름도 테넌트를 식별합니다. 테넌트 이름은 조직 이름이 아닙니다. 이 정보는Cisco TAC(Technical Assistance Center)에 문의해야 하는 경우에 유용합니다.

# 알림 설정

테넌트와 연결된 디바이스가 특정 작업을 수행할 때마다 CDO에서 이메일 알림을 받도록 구독할 수 있습니다. 이러한 알림은 테넌트와 연결된 모든 디바이스에 적용되지만, 모든 디바이스 유형이 사용 가능한 모든 옵션을 지원하는 것은 아닙니다. 또한 아래에 나열된 CDO 알림에 대한 변경 사항은 실시간으로 자동 업데이트되며 구축이 필요하지 않습니다.

CDO의 이메일 알림은 작업 유형 및 영향을 받는 디바이스를 나타냅니다. 디바이스의 현재 상태 및 작업 내용에 대한 자세한 정보를 알아보려면 CDO에 로그인하여 영향을 받는 디바이스의 변경 로그를 검토하는 것이 좋습니다.

왼쪽 탐색 모음에서 **Settings(**설정**)** > **Notification Settings(**알림 설정**)**를 클릭합니다.

디바이스 워크플로우에 대한 알림 전송

**Note** 이러한 설정을 변경하거나 알림을 수동으로 구독하려면 최고 관리자 사용자 역할이 있어야 합니다. 자세한 내용은 Cisco Defense Orchestrator의 사용자 역할을 참조하십시오.

알림을 받을 디바이스 워크플로우 시나리오를 모두 선택해야 합니다. 다음 작업을 수동으로 확인합니다.

- 구축 - 이 작업은 하며, SSH 또는 IOS 디바이스에 대한 통합 인스턴스는 포함하지 않습니다.
- 백업 - 이 작업은 FDM 관리 디바이스에만 적용됩니다.
- 업그레이드 - 이 작업은 ASA 및 FDM 관리 디바이스에만 적용됩니다.
- **FTD**를 클라우드로 마이그레이션 - 이 작업은 FTD

  Device Manager를 FMC에서 CDO로 변경할 때 적용됩니다.

디바이스 이벤트에 대한 알림 전송

**Note** 이러한 설정을 변경하거나 알림을 수동으로 구독하려면 최고 관리자 사용자 역할이 있어야 합니다. 자세한 내용은 Cisco Defense Orchestrator의 사용자 역할을 참조하십시오.

알림을 받을 디바이스 워크플로우 시나리오를 모두 선택해야 합니다. 다음 작업을 수동으로 확인합니다.

- 오프라인 상태 - 이 작업은 테넌트와 연결된 모든 디바이스에 적용됩니다.
- 온라인 재전환 - 이 작업은 테넌트와 연결된 모든 디바이스에 적용됩니다.
- 충돌 탐지됨 - 이 작업은 테넌트와 연결된 모든 디바이스에 적용됩니다.
- **HA** 상태 변경됨 - 이 작업은 HA 또는 페일오버 쌍 내의 디바이스, 현재 상태 및 변경된 상태를 나타냅니다. 이 작업은 테넌트와 연결된 모든 HA 및 페일오버 구성에 적용됩니다.
- 사이트 간 세션 연결 끊김 - 이 작업은 테넌트에 구성된 모든 사이트 간 VPN 구성에 적용됩니다.

백그라운드 로그 검색을 위해 알림 전송

이러한 설정을 변경하거나 알림을 수동으로 구독하려면 최고 관리자 사용자 역할이 있어야 합니다. 자세한 내용은 Cisco Defense Orchestrator의 사용자 역할을 참조하십시오.

테넌트에 로그인한 사용자가 백그라운드 검색을 생성하면 알림을 받습니다. 알림을 받을 디바이스 워크플로우 시나리오를 모두 선택해야 합니다. 다음 작업을 수동으로 확인합니다.

- 검색 시작 - 검색이 시작되면 알림을 받습니다. 이는 즉시 검색 및 예약된 검색에 모두 적용됩니다.
- 검색 완료 - 검색이 종료되면 알림을 받습니다. 이는 즉시 검색 및 예약된 검색에 모두 적용됩니다.
- 검색 실패 - 검색이 실패하면 알림을 받습니다. 이는 즉시 검색 및 예약된 검색에 모두 적용됩니다. 매개변수 또는 쿼리를 확인하고 다시 시도하십시오.

가입자

**Subscribe to receive alerts(**알림 수신 구독**)** 토글을 활성화하여 테넌트 로그인과 연결된 이메일을 알림 목록에 추가합니다. 메일링 리스트에서 이메일을 제거하려면 토글을 선택 취소하여 회색으로 표시합니다.

특정 사용자 역할은 이 설정 페이지의 구독 작업에 제한적으로 액세스할 수 있습니다. 최고 관리자 사용자 역할의 사용자는 이메일 항목을 추가하거나 제거할 수 있습니다. 자신이 아닌 다른 사람 또는 대체 이메일 연락처를 구독 중인 사용자 목록에 추가하려면  을 클릭하고 이메일을 수동으로 입력합니다.

**Warning** 사용자를 수동으로 추가하는 경우 올바른 이메일을 입력해야 합니다. CDO는 테넌트와 연결된 알려진 사용자에 대한 이메일 주소를 확인하지 않습니다.

### CDO 알림 보기

알림  아이콘을 클릭하여 테넌트에서 발생한 최신 알림을 확인합니다. CDO의 알림은 30일 후에 알림 목록에서 제거됩니다.

**Note** **Send Alerts When(**알림 전송 시기**)** 섹션에서 선택한 사항은 CDO에 표시되는 알림 유형에 영향을 미칩니다.

서비스 통합

메시징 앱에서 수신 Webhook를 활성화하고 앱 대시보드에서 직접 CDO 알림을 수신합니다. CDO에서 이 옵션을 활성화하려면 선택한 앱에서 수신 Webhook를 수동으로 허용하고 Webhook URL을 검색해야 합니다. 자세한 내용은 CDO 알림을 위한 서비스 통합 활성화를 참조하십시오.

## CDO 알림을 위한 서비스 통합 활성화

서비스 통합을 활성화하여 지정된 메시징 애플리케이션 또는 서비스를 통해 CDO 알림을 전달합니다. 알림을 받으려면 메시지 프로그램에서 웹후크 URL을 생성하고 CDO의 **Notification Settings(**알림 설정**)** 페이지에서 해당 웹후크를 CDO에 지정해야 합니다.

CDO는 기본적으로 Cisco Webex 및 Slack을 서비스 통합으로 지원합니다. 이러한 서비스로 전송되는 메시지는 채널 및 자동화된 봇용으로 특별히 형식이 지정됩니다.

참고 알림 설정 페이지에서 선택한 **Notification Settings(**알림 설정**)**은 메시지 프로그램으로 전달되는 이벤트입니다.

### Webex Teams에 대해 수신 Webhook

시작하기 전에

CDO 알림은 지정된 작업 공간에 표시되거나 비공개 메시지에 자동 봇으로 표시됩니다. Webex Teams이 웹후크를 처리하는 방법에 대한 자세한 정보는 개발자용 Webex를 참조하십시오.

Webex Teams에 대해 수신 웹후크를 허용하려면 다음 절차를 따르십시오.

단계 **1** Webex Teams 응용프로그램을 엽니다.

단계 **2** 창의 왼쪽 하단에서 **Apps(**앱**)** 아이콘을 클릭합니다. 이 작업은 기본 브라우저의 새 탭에서 Cisco Webex App Hub를 엽니다.

단계 **3** 수신 웹후크를 찾으려면 검색창을 사용하세요.

단계 **4** **Connect(**연결**)**을 선택합니다. 이 작업은 새 탭에서 애플리케이션을 허용하는 OAuth 인증을 엽니다.

단계 **5** **Accept(**수락**)**을 선택합니다. 탭은 자동으로 애플리케이션의 구성 페이지로 리디렉션됩니다.

단계 **6** 다음을 구성합니다.

- **Webhook** 이름 - 이 애플리케이션에서 제공하는 메시지를 식별하기 위한 이름을 입력합니다.
- 공간 선택 - 드롭다운 메뉴를 사용하여 **Space(**공간**)**를 선택합니다. 공간이 이미 Webex 팀에 존재해야 합니다. 공간이 존재하지 않는 경우 Webex Teams에서 새 공간을 만들고 애플리케이션의 구성 페이지를 새로 고쳐 새 공간을 표시할 수 있습니다.

단계 **7** **Add(**추가**)**를 선택합니다. 선택한 Webex Space는 애플리케이션이 추가되었다는 알림을 받게 됩니다.

단계 **8** 웹후크 URL을 복사합니다.

단계 **9** CDO에 로그인합니다.

단계 **10** 왼쪽 탐색 모음에서 **Settings(**설정**)** > **Notification Settings(**알림 설정**)**를 클릭합니다.

단계 **11** **Service Integrations(**서비스 통합**)**으로 스크롤합니다.

단계 **12** 파란색 플러스 버튼을 클릭합니다.

단계 **13** **Name(**이름**)**을 입력합니다. 이 이름은 구성된 서비스 통합으로 CDO에 나타납니다. 구성된 서비스로 전달되는 이벤트에는 나타나지 않습니다.

단계 **14** 드롭다운 메뉴를 확장하고 **Webex**를 서비스 유형으로 선택합니다.

단계 **15** 서비스에서 생성한 웹후크 URL을 붙여넣습니다.

단계 **16** OK(확인)를 클릭합니다.

## Slack용 수신 Webhook

CDO 알림은 지정된 채널에 표시되거나 비공개 메시지에 자동 봇으로 표시됩니다. Slack이 수신 웹후크를 처리하는 방법에 대한 자세한 내용은 Slack 앱을 참조하십시오.

Slack에 대해 수신 웹후크를 허용하려면 다음 절차를 따르십시오.

단계 **1** Slack계정에 로그인합니다.

단계 **2** 왼쪽 패널에서 아래로 스크롤하여 **Add Apps(**앱 추가**)**를 선택합니다.

단계 **3** **Incoming Webhooks(**수신 웹후크**)**에 대한 애플리케이션 디렉토리를 검색하고 앱을 찾습니다. **Add(**추가**)**를 선택합니다.

단계 **4** Slack 워크스페이스의 관리자가 아닌 경우, 조직의 관리자에게 요청을 보내고 앱이 계정에 추가될 때까지 기다려야 합니다. **Request Configuration(**요청 구성**)**을 선택합니다. 선택적 메시지를 입력하고 **Submit Request(**요청 제출**)**을 선택합니다.

단계 **5** 워크스페이스에 수신 웹후크 앱이 활성화되면 Slack 설정 페이지를 새로고침하고 **Add New Webhook to Workspace(**워크스페이스에 새 웹후크 추가**)**를 선택합니다.

단계 **6** 드롭다운 메뉴를 사용하여 CDO 알림을 표시할 Slack 채널을 선택합니다. **Authorize(**승인**)**을 선택합니다. 요청이 활성화되기를 기다리는 동안 이 페이지에서 다른 곳으로 이동하려면 Slack에 로그인하고 왼쪽 상단 모서리에서 작업 공간 이름을 선택하기만 하면 됩니다. 드롭다운 메뉴에서 **Customize Workspace(**작업 공간 사용자 지정**)**을 선택하고 **Configure Apps(**앱 구성**)**을 선택합니다. **Custom Integrations(**사용자 지정 통합**)** > **Manage (**관리**)**로 이동합니다. **Incoming Webhooks(**수신 웹후크**)**를 선택하여 앱의 랜딩 페이지를 연 다음 탭에서 **Configuration(**구성**)**

을 선택합니다. 그러면 이 앱이 활성화된 작업 공간 내의 모든 사용자가 나열됩니다. 계정 구성만 보고 편집할 수 있습니다. 작업 공간 이름을 선택하여 구성을 편집하고 계속 진행합니다.

단계 **7** Slack 설정 페이지는 앱의 구성 페이지로 리디렉션됩니다. 웹후크 URL을 찾아 복사합니다.

단계 **8** CDO에 로그인합니다.

단계 **9** 왼쪽 탐색 모음에서 **Settings(**설정**)** > **Notification Settings(**알림 설정**)**를 클릭합니다.

단계 **10** **Service Integrations(**서비스 통합**)**으로 스크롤합니다.

단계 **11** 파란색 플러스 버튼을 클릭합니다.

단계 **12** **Name(**이름**)**을 입력합니다. 이 이름은 구성된 서비스 통합으로 CDO에 나타납니다. 구성된 서비스로 전달되는 이벤트에는 나타나지 않습니다.

단계 **13** 드롭다운 메뉴를 확장하고 서비스 유형으로 **Slack**을 선택합니다.

단계 **14** 서비스에서 생성한 웹후크 URL을 붙여넣습니다.

단계 **15** OK(확인)를 클릭합니다.

---

사용자 지정 통합을 위한 수신 웹후크

시작하기 전에

CDO는 사용자 지정 통합을 위한 메시지 형식을 지정하지 않습니다. 사용자 지정 서비스 또는 애플리케이션을 통합하기로 선택한 경우 CDO는 JSON 메시지를 보냅니다.

수신 웹후크를 활성화하고 웹후크 URL을 생성하는 방법에 대한 서비스 설명서를 참조하십시오. 웹후크 URL이 있으면 아래 절차를 사용하여 웹후크를 활성화합니다.

---

단계 **1** 선택한 사용자 지정 서비스 또는 애플리케이션에서 웹후크 URL을 생성하고 복사합니다.

단계 **2** CDO에 로그인합니다.

단계 **3** 왼쪽 탐색 모음에서 **Settings(**설정**)** > **Notification Settings(**알림 설정**)**를 클릭합니다.

단계 **4** **Service Integrations(**서비스 통합**)**으로 스크롤합니다.

단계 **5** 파란색 플러스 버튼을 클릭합니다.

단계 **6** **Name(**이름**)**을 입력합니다. 이 이름은 구성된 서비스 통합으로 CDO에 나타납니다. 구성된 서비스로 전달되는 이벤트에는 나타나지 않습니다.

단계 **7** 드롭다운 메뉴를 확장하고 서비스 유형으로 **Custom(**사용자 지정**)**을 선택합니다.

단계 **8** 서비스에서 생성한 웹후크 URL을 붙여넣습니다.

단계 **9** OK(확인)를 클릭합니다.

---

# 로깅 설정

월별 이벤트 로깅 한도와 한도가 재설정될 때까지 남은 일수를 확인합니다. 저장된 로깅은 Cisco cloud가 수신한 압축된 이벤트 데이터를 나타냅니다.

지난 12개월 동안 테넌트가 받은 모든 로깅을 보려면 **View Historical Usage(**기록 히스토리 보기**)** 를 클릭합니다.

추가 스토리지를 요청하는 데 사용할 수 있는 링크도 있습니다.

# SAML SSO(Single Sign-On)를 Cisco Defense Orchestrator와 통합

Cisco Defense Orchestrator(CDO)는 Cisco Secure Sign-On을 SAML Single Sign-On Identity Provider(IdP) 및 MFA(다단계 인증)용 Duo Security로 사용합니다. 이는 CDO의 기본 인증 방법입니다.

그러나 고객이 자신의 SAML SSO(Single Sign-On) IdP 솔루션을 CDO와 통합하려는 경우 IdP가 SAML 2.0 및 IdP(Identity Provider) 시작 워크플로를 지원하는 경우라면 가능합니다.

자체 SAML 솔루션을 CDO와 통합하려면 지원 부서에 문의하여 케이스를 생성해야 합니다. 지침은 Cisco Secure Cloud Sign-On ID 제공자 통합 가이드를 참조하십시오.

**Attention** 케이스를 열 때 요청이 올바른 팀에 전달되도록 **Manually Select A Technology(**수동으로 **A** 기술 선택**)**를 선택하고 **SecureX - Sign-on and Administration(SecureX -** 로그인 및 관리**)**을 선택했는지 확인합니다.

# SSO 인증서 갱신

ID 공급자(IdP)는 일반적으로 SecureX SSO와 통합됩니다. Cisco TAC 사례를 열고 metadata.xml 파일을 제공하십시오. 자세한 내용은 Cisco SecureX Sign-On 타사 ID 제공자 통합 가이드를 참조하십시오.

주의 사례를 열 때 기술 수동 선택을 선택하고 요청이 올바른 팀에 전달되도록 **SecureX -** 로그온 및 관리를 선택했는지 확인합니다.

(레거시만 해당) IdP(Identity Provider) 통합이 CDO와 직접 통합된 경우 CDO 고객이 TAC로 지원 티켓을 여는 방법을 열고 metadata.xml 파일을 제공하십시오.

참고 IdP를 CDO와 직접 통합하는 대신 SecureX SSO와 통합하는 것이 매우 좋습니다.

# API 토큰

개발자는 CDO REST API 호출을 할 때 CDO API 토큰을 사용합니다. 호출이 성공하려면 REST API 인증 헤더에 API 토큰을 삽입해야 합니다. API 토큰은 만료되지 않는 "장기" 액세스 토큰입니다. 그러나 이를 갱신하고 취소할 수 있습니다.

CDO 내에서 API 토큰을 생성할 수 있습니다. 이러한 토큰은 생성 직후 일반 설정 페이지가 열려 있는 동안에만 표시됩니다. CDO에서 다른 페이지를 열고 일반 설정페이지로 돌아가면, 토큰이 분명히 발급었지만 토큰이 더 이상 표시되지 않습니다.

개별 사용자는 특정 테넌트에 대한 자체 토큰을 생성할 수 있습니다. 사용자는 다른 사용자를 대신하여 토큰을 생성할 수 없습니다. 토큰은 계정-테넌트 쌍에 고유하며 다른 사용자-테넌트 조합에 사용할 수 없습니다.

## API 토큰 형식 및 클레임

API 토큰은 JSON 웹 토큰(JWT)입니다. JWT 토큰 형식에 대해 자세히 알아보려면 JSON 웹 토큰 소개를 읽어보십시오.

CDO API 토큰은 다음과 같은 클레임 집합을 제공합니다.

- **id** - 사용자/디바이스 uid
- **parentId** - 테넌트 uid
- **ver** - 공개 키의 버전(초기 버전은 0, 예, **cdo_jwt_sig_pub_key.0**)
- **subscriptions** - 보안 서비스 익스체인지 구독 (선택 사항)
- **client_id** - "**api-client**"
- **jti** - 토큰 ID

## 토큰 관리

### API 토큰 생성

단계 **1** 왼쪽 내비게이션 바에서 **Settings(**설정**)** > **General Settings(**일반 설정**)**를 클릭합니다.
단계 **2** 내 토큰에서 **Generate API Token(API** 토큰 생성**)**를 클릭합니다.
단계 **3** 민감한 데이터를 유지하기 위한 기업의 모범 사례에 따라 안전한 위치에 토큰을 저장하십시오.

### API 토큰 갱신

API 토큰은 만료되지 않습니다. 그러나 사용자는 토큰이 분실되거나 손상된 경우 또는 기업의 보안 지침을 준수하기 위해 API 토큰을 갱신하도록 선택할 수 있습니다.

단계 **1** 왼쪽 탐색 모음에서 **Settings(**설정**)** > **General Settings(**일반 설정**)**를 클릭합니다.
단계 **2** 내 토큰에서 **Renew(**갱신**)**을 클릭합니다. CDO에서 새 토큰을 생성합니다.
단계 **3** 민감한 데이터를 유지하기 위한 기업의 모범 사례에 따라 안전한 위치에 새 토큰을 저장하십시오.

### API 토큰 취소

단계 1 왼쪽 내비게이션 바에서 **Settings(설정)** > **General Settings(일반 설정)**를 클릭합니다.

단계 2 내 토큰에서 **Revoke(취소)**를 클릭합니다. CDO는 토큰을 취소합니다.

# ID 제공자 계정과 Cisco Defense Orchestrator 사용자 레코드 간의 관계

Cisco Defense Orchestrator(CDO)에 로그인하려면 고객에게 SAML 2.0 호환 IdP(Identity Provider), 다단계 인증 제공자 및 CDO의 사용자 레코드가 있는 계정이 필요합니다. IdP 어카운트에는 사용자의 자격 증명이 포함되며 IdP는 이러한 자격 증명을 기반으로 사용자를 인증합니다. 다단계 인증은 ID 보안의 추가 레이어를 제공합니다. CDO 사용자 레코드에는 주로 사용자 이름, 연결된 CDO 테넌트 및 사용자의 역할이 포함됩니다. 사용자가 로그인하면 CDO는 IdP의 사용자 ID를 CDO의 테넌트에 있는 기존 사용자 레코드에 매핑하려고 시도합니다. CDO가 일치하는 항목을 찾으면 사용자는 해당 테넌트에 로그인됩니다.

엔터프라이즈에 자체 SSO(Single Sign-On) ID 제공자가 없는 경우 ID 제공자는 Cisco Secure Cloud Sign-on입니다. Cisco Secure Cloud Sign-On은 다단계 인증에 Duo를 사용합니다. 고객은 원하는 경우 SAML SSO(Single Sign-On)를 Cisco Defense Orchestrator와 통합할 수 있습니다.

## 로그인 워크플로우

다음은 IdP 계정이 CDO 사용자 레코드와 상호 작용하여 CDO 사용자에 로그인하는 방법에 대한 간략한 설명입니다.

단계 1 사용자는 인증을 위해 Cisco Secure Cloud Sign-On(https://sign-on.security.cisco.com)과 같은 SAML 2.0 호환 ID 공급자(IdP)에 로그인하여 CDO에 대한 액세스를 요청합니다.

단계 2 IdP는 사용자가 인증되었다는 SAML 어설션을 발행하고 포털은 https://defenseorchestrator.com 또는 https://defenseorchestrator.eu 또는 https://www.apj.cdo.cisco.com/를 나타내는 타일과 같이 사용자가 액세스할 수 있는 애플리케이션을 표시합니다.

단계 3 CDO는 SAML 어설션의 유효성을 검사하고 사용자 이름을 추출한 다음 테넌트 중에서 해당 사용자 이름에 해당하는 사용자 레코드를 찾으려고 시도합니다.

- 사용자가 CDO의 단일 테넌트에 대한 사용자 레코드를 가지고 있는 경우 CDO는 사용자에게 테넌트에 대한 액세스 권한을 부여하고 사용자의 역할에 따라 수행할 수 있는 작업이 결정됩니다.
- 사용자가 두 개 이상의 테넌트에 대한 사용자 레코드를 가지고 있는 경우 CDO는 인증된 사용자에게 선택할 수 있는 테넌트 목록을 제공합니다. 사용자는 테넌트를 선택하고 해당 테넌트에 액세스할 수 있습니다. 특정 테넌트에 대한 사용자의 역할에 따라 수행할 수 있는 작업이 결정됩니다.
- CDO에 인증된 사용자와 테넌트의 사용자 레코드에 대한 매핑이 없는 경우 CDO는 사용자에게 CDO에 대해 자세히 알아보거나 무료 평가판을 요청할 수 있는 기회를 제공하는 랜딩 페이지를 표시합니다.

CDO에 사용자 레코드를 생성해도 IdP에 계정이 생성되지 않고 IdP에 계정을 생성해도 CDO에 사용자 레코드가 생성되지 않습니다.

마찬가지로 IdP에서 계정을 삭제한다고 해서 CDO에서 사용자 기록을 삭제한 것은 아닙니다. 그러나 IdP 계정이 없는 경우 사용자를 CDO에 인증할 방법이 없습니다. CDO 사용자 기록을 삭제한다고 해서 IdP 계정이 삭제된 것은 아닙니다. 그러나 CDO 사용자 레코드가 없는 경우 인증된 사용자가 CDO 테넌트에 액세스할 수 있는 방법이 없습니다.

## 이 아키텍처의 의미

**Cisco Security Cloud** 로그인을 사용하는 고객

CDO의 Cisco Secure Cloud Sign-On ID 공급자를 사용하는 고객의 경우 슈퍼 관리자는 CDO에 사용자 레코드를 생성할 수 있으며 사용자는 CDO에 자체 등록할 수 있습니다. 두 사용자 이름이 일치하고 사용자가 올바르게 인증된 경우 사용자는 CDO에 로그인할 수 있습니다.

슈퍼 관리자가 사용자가 CDO에 액세스하지 못하도록 해야 하는 경우 CDO 사용자의 사용자 레코드를 간단히 삭제할 수 있습니다. Cisco Secure Cloud Sign-On 계정은 여전히 존재하며 슈퍼 관리자가 사용자를 복원하려는 경우 Cisco Secure Cloud Sign-On에 사용된 것과 동일한 사용자 이름으로 새 CDO 사용자 레코드를 생성하면 됩니다.

고객이 기술 지원 센터(TAC)에 전화해야 하는 CDO 문제에 직면한 경우 고객은 TAC 엔지니어를 위한 사용자 레코드를 생성하여 테넌트를 조사하고 정보와 제안을 고객에게 다시 보고할 수 있습니다.
.

자체 **ID** 제공자가 있는 고객

SAML SSO(Single Sign-On)를 Cisco Defense Orchestrator와 통합의 경우 ID 공급자 계정과 CDO 테넌트를 모두 제어합니다. 이러한 고객은 CDO에서 ID 공급자 계정 및 사용자 레코드를 만들고 관리할 수 있습니다.

사용자가 CDO에 액세스하지 못하도록 해야 하는 경우, IdP 계정, CDO 사용자 레코드 또는 둘 다를 삭제할 수 있습니다.

Cisco TAC의 도움이 필요한 경우, TAC 엔지니어를 위해 읽기 전용 역할이 있는 ID 공급자 계정과 CDO 사용자 레코드를 모두 생성할 수 있습니다. 그런 다음 TAC 엔지니어는 고객의 CDO 테넌트에 액세스하여 조사하고 고객에게 정보와 제안을 보고할 수 있습니다.3

**Cisco Managed Service** 제공자

Cisco MSP(Managed Service Provider)가 CDO의 Cisco Secure Cloud Sign-On IdP를 사용하는 경우 Cisco Secure Cloud Sign-On에 자체 등록할 수 있으며 고객은 MSP가 고객의 테넌트를 관리할 수 있도록 CDO에 사용자 레코드를 생성할 수 있습니다. 물론 고객은 원할 때 MSP의 레코드를 삭제할 수 있는 모든 권한을 가집니다.

관련 주제

- 일반 설정
- 사용자 관리
- Cisco Defense Orchestrator의 사용자 역할

# 멀티 테넌트 포털 관리

CDO 다중 테넌트 포털 보기는 여러 테넌트의 모든 디바이스에서 정보를 검색하고 표시합니다. 이 다중 테넌트 포털은 디바이스 상태, 디바이스에서 실행 중인 소프트웨어 버전 등을 보여줍니다.

**Note** 다중 테넌트 포털에서 여러 지역에 걸쳐 테넌트를 추가하고 해당 테넌트가 관리하는 디바이스를 볼 수 있습니다. 다중 테넌트 포털에서 테넌트를 편집하거나 디바이스를 구성할 수 없습니다.

시작하기 전에

다중 테넌트 포털은 해당 기능이 테넌트에서 활성화된 경우에만 사용할 수 있습니다. 테넌트에 대해 다중 테넌트 포털을 활성화하려면 Cisco TAC에서 지원 티켓을 여십시오. 지원 티켓이 해결되고 포털이 생성되면 포털에서 최고 관리자 역할을 가진 사용자는 여기에 테넌트를 추가할 수 있습니다.

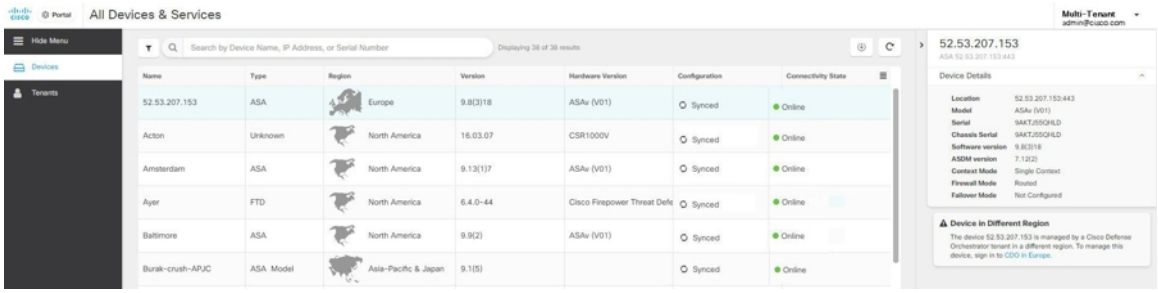
발생할 수 있는 특정 브라우저 관련 문제를 방지하려면 웹 브라우저에서 캐시와 쿠키를 지우는 것이 좋습니다.

멀티 테넌트 포털

포털은 다음 메뉴를 제공합니다.

- 디바이스:
  - 포털에 추가된 테넌트에 있는 모든 디바이스를 표시합니다. 필터 및 검색 필드를 사용하여 보려는 디바이스를 검색합니다. 디바이스를 클릭하여 상태, 온보딩 방법, 방화벽 모드, 페일오버 모드, 소프트웨어 버전 등을 볼 수 있습니다.
  - 인터페이스는 테이블에서 볼 디바이스 속성을 선택하거나 지울 수 있는 열 선택기 ≡ 를 제공합니다. 'AnyConnect 원격 액세스 VPN'을 제외하고 다른 모든 디바이스 속성은 기본으로 선택됩니다. 테이블을 사용자 정의하면 CDO는 다음에 CDO에 로그인할 때 선택 사항을 기억합니다.
  - 디바이스를 클릭하면 오른쪽에서 세부 정보를 볼 수 있습니다.
  - 포털 정보를 쉼표로 구분된 값(.csv) 파일로 내보낼 수 있습니다. 이 정보는 디바이스를 분석하거나 액세스 권한이 없는 사람에게 보내는 데 도움이 됩니다. 데이터를 내보낼 때마다 CDO는 새 .csv 파일을 생성합니다. 생성된 파일에는 이름에 날짜와 시간이 포함되어 있습니다.
  - 디바이스를 관리하는 CDO 테넌트에서만 디바이스를 관리할 수 있습니다. 다중 테넌트 포털은 CDO 테넌트 페이지로 연결되는 장치 관리 링크를 제공합니다. 해당 테넌트에 대한 계정이 있고 테넌트가 포털과 동일한 지역에 있는 경우 디바이스에 이 링크가 표시됩니다. 테넌트에 액세스할 수 있는 권한이 없는 경우 디바이스 관리 링크가 표시되지 않습니다. 권한을 얻기 위해 조직의 슈퍼 관리자에게 문의할 수 있습니다.

**Note** 디바이스를 관리하는 테넌트가 다른 지역에 있는 경우 해당 지역의 CDO에 로그인할 수 있는 링크가 표시됩니다. 해당 지역의 CDO 또는 해당 지역의 테넌트에 액세스할 수 없는 경우 디바이스를 관리할 수 없습니다.




- 테넌트:
  - 포털에 추가된 테넌트를 표시합니다.
  - 이를 통해 슈퍼 관리자는 포털에 테넌트를 추가할 수 있습니다.
  - 를 클릭하면 CDO 테넌트의 메인 페이지를 볼 수 있습니다.

## 멀티 테넌트 포털에 테넌트 추가

슈퍼 관리자 역할이 있는 사용자는 포털에 테넌트를 추가할 수 있습니다. 여러 지역에 걸쳐 테넌트를 추가할 수 있습니다. 예를 들어 유럽 지역의 테넌트를 미국 지역에 추가하거나 그 반대로 추가할 수 있습니다.

**Important** 테넌트에 대한 API 전용 사용자 생성하고 CDO 인증을 위한 API 토큰을 생성하는 것이 좋습니다.

**Note** 포털에 여러 테넌트를 추가하려면 각 테넌트에서 API 토큰을 생성하고 텍스트 파일에 붙여넣습니다. 그런 다음 토큰을 생성하기 위해 매번 테넌트로 전환하지 않고도 포털에 테넌트를 차례로 쉽게 추가할 수 있습니다.

단계 **1** 왼쪽 내비게이션 바에서 **Settings(**설정**)** > **General Settings(**일반 설정**)** > **My Tokens(**내 토큰**)**를 클릭합니다.

단계 **2** **Generate API Token(API** 토큰 생성**)**을 클릭한 다음 복사합니다.

단계 **3** 포털로 이동하여 **Tenants(**테넌트**)** 탭을 클릭합니다.

단계 **4** 오른쪽에 테넌트 추가 버튼을 클릭합니다.

단계 **5** 토큰을 붙여넣고 **Save(**저장**)**를 클릭합니다.

## 멀티 테넌트 포털에서 테넌트 삭제

단계 **1** 포털로 이동하여 **Tenants(**테넌트**)** 탭을 클릭합니다.

단계 **2** 오른쪽에 나타나는 해당 삭제 아이콘을 클릭하여 원하는 테넌트를 제거합니다.

단계 **3** **Remove(**제거**)**를 클릭합니다. 연결된 디바이스도 포털에서 제거됩니다.

## 관리-테넌트 포털 설정

Cisco Defense Orchestrator(Defense Orchestrator)는 설정 페이지에서 다중 테넌트 포털 및 개별 사용자 계정의 특정 측면을 사용자 지정할 수 있는 기능을 제공합니다. 왼쪽 탐색 모음에서 **Settings(**설정**)**를 클릭하여 설정 페이지에 액세스합니다.

설정

**General Settings(**일반 설정**)**

웹 분석은 페이지 히트를 기반으로 익명의 제품 사용 정보를 Cisco에 제공합니다. 이 정보에는 확인한 페이지, 특정 페이지를 사용한 시간, 브라우저 버전, 제품 버전, 디바이스 호스트 이름 등이 포함됩니다. Cisco는 이 정보를 활용해 기능 사용 패턴을 확인하고 제품을 개선할 수 있습니다. 모든 사용량 데이터는 익명으로 전송되며 민감한 데이터는 전송되지 않습니다.

웹 분석은 기본적으로 활성화됩니다. 웹 분석을 비활성화하거나 나중에 활성화하려면 다음 절차를 따르십시오.

1. CDO 대시보드 왼쪽의 내비게이션 바에서 **Settings(**설정**)**를 클릭합니다.
2. **General Settings(**일반 설정**)**를 클릭합니다.
3. 웹 분석 아래의 슬라이더를 클릭합니다.

사용자 관리

**User Management(**사용자 관리**)** 화면에서 다중 테넌트 포털과 연결된 모든 사용자 레코드를 볼 수 있습니다. 사용자 계정을 추가, 편집 또는 삭제할 수 있습니다. 자세한 내용은 User 사용자 관리를 참조하십시오.

테넌트 전환

포털 테넌트가 둘 이상인 경우 CDO에서 로그아웃하지 않고 다른 포털 또는 테넌트 간에 전환할 수 있습니다.

단계 **1** 다중 테넌트 포털에서 오른쪽 상단 모서리에 나타나는 테넌트 메뉴를 클릭합니다.

단계 **2** **Switch tenant(**테넌트 전환**)**를 클릭합니다.

단계 **3** 보려는 포털 또는 테넌트를 선택합니다.

## Cisco Success Network

Cisco Success Network는 사용자가 활성화하는 클라우드 서비스입니다. Cisco Success Network를 활성화하면 디바이스와 Cisco cloud간에 보안 연결이 설정되어 사용 정보 및 통계를 스트리밍합니다. 스트리밍 원격 측정은 디바이스에서 관심 있는 데이터를 선택하고 구조화된 형식으로 원격 관리 스테이션에 전송하는 메커니즘을 제공하여 다음과 같은 이점을 제공합니다.

- 네트워크에서 제품의 효율성을 향상시킬 수있는 활용 가능한 미사용 기능을 알려줍니다.
- 제품에 사용할 수 있는 추가 기술 지원 서비스 및 모니터링에 대해 알려줍니다.
- Cisco가 제품을 개선할 수 있습니다.

디바이스는 항상 보안 연결을 설정하고 유지하며 Cisco Success Network에 등록할 수 있습니다. 디바이스를 등록하고 나면 Cisco Success Network 설정을 변경할 수 있습니다.

참고

- 위협 방어 고가용성 쌍의 경우 활성 디바이스 선택이 대기 디바이스의 Cisco Success Network 설정을 오버라이드합니다.
- CDO는 Cisco Success Network 설정을 관리하지 않습니다. Firewall Device Manager 사용자 인터페이스를 통해 관리되는 설정 및 원격 분석 정보가 제공됩니다.

### Cisco Success Network 활성화 또는 비활성화

초기 시스템 설정 중에 Cisco Smart Software Manager에 디바이스를 등록하라는 메시지가 표시됩니다. 90일 평가 라이선스를 대신 선택한 경우에는 평가 기간이 종료되기 전에 디바이스를 등록해야 합니다. 디바이스를 등록하려면 Cisco Smart Software Manager(Smart Licensing 페이지)에 디바이스를 등록하거나 등록 키를 입력하여 CDO에 등록합니다.

디바이스를 등록할 때는 가상 어카운트가 디바이스에 라이선스를 할당합니다. 디바이스를 등록하면 활성화한 선택 가능한 라이선스도 등록됩니다.

Firewall Device Manager UI를 통해서만 이 옵션을 비활성화할 수 있지만 Cisco Success Network를 비활성화하여 언제든지 이 연결을 끌 수 있습니다. 비활성화하면 클라우드에서 디바이스의 연결이 끊어집니다. 연결 해제는 업데이트 수신 또는 스마트 라이선싱 기능 작동에 영향을 주지 않으므로 이러한 기능은 계속 정상적으로 작동됩니다. 자세한 내용은 Firepower 디바이스 매니저 구성 가이드, 버전 6.4.0+에서 시스템 관리 창의 **Cisco Success Network**에 연결 섹션을 참조하십시오.

# 사용자 관리

CDO에서 사용자 레코드를 생성하거나 수정하기 전에 ID 제공자 계정과 Cisco Defense Orchestrator 사용자 레코드 간의 관계를 읽고 IdP(Identity Provider) 계정과 사용자 레코드의 상호 작용 방식을 확

인하십시오. CDO사용자는 인증을 받고 CDO테넌트에 액세스할 수 있도록 CDO레코드 및 해당 IdP 계정이 필요합니다.

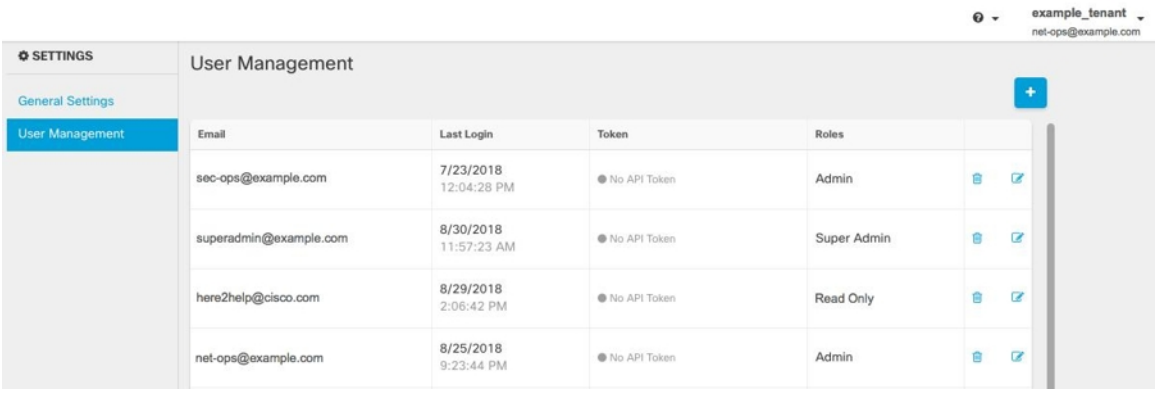
엔터프라이즈에 자체 IdP가 없는 경우 Cisco Secure Sign-On은 모든 CDO 테넌트에 대한 ID 제공자입니다. 이 문서의 나머지 부분에서는 Cisco Secure Sign-On을 ID 제공자로 사용한다고 가정합니다.

**User Management(**사용자 관리**)** 화면에서 테넌트와 연결된 모든 사용자 레코드를 볼 수 있습니다. 여기에는 지원 티켓을 해결하기 위해 사용자 어카운트와 일시적으로 연결된 모든 Cisco 지원 엔지니어가 포함됩니다.

# 테넌트와 연결된 사용자 기록 보기

단계 **1** 오른쪽 상단의 관리자 드롭다운에서 **Settings(**설정**)**를 클릭합니다.

단계 **2** **User Management(**사용자 관리**)**를 클릭합니다.




참고 Cisco 지원이 테넌트에 액세스하지 못하도록 하려면, 일반 설정 페이지에서 계정 설정을 구성합니다.

# 사용자 관리의 **Active Directory** 그룹

대량의 사용자에 대해 회전율이 높은 테넌트의 경우 개별 사용자를 CDO에 추가하는 대신 CDO를 AD(Active Directory) 그룹에 매핑하여 사용자 목록 및 사용자 역할을 더 쉽게 관리할 수 있습니다. 새 사용자 추가 또는 기존 사용자 제거와 같은 모든 사용자 변경은 이제 Active Directory에서 수행할 수 있으며 더 이상 CDO에서 수행할 필요가 없습니다.

사용자 관리 페이지에서 AD 그룹을 추가, 편집 또는 삭제하려면 **SuperAdmin** 사용자 역할이 있어야 합니다. 자세한 내용은 Cisco Defense Orchestrator의 사용자 역할을 참조하십시오.

**Active Directory** 그룹 탭

**Settings(**설정**)** 페이지의 사용자 관리 섹션에는 현재 CDO에 매핑된 Active Directory 그룹에 대한 탭이 있습니다. 가장 중요한 것은 이 페이지에 AD 관리자에서 할당된 AD 그룹의 역할이 표시된다는 것입니다.

AD 그룹 내의 사용자는 Active Directory 그룹 탭이나 사용자 탭에 개별적으로 나열되지 않습니다.

감사 로그 탭

**Settings(**설정**)** 페이지의 User Management(사용자 관리) 섹션에는 Audit Logs(감사 로그) 탭이 있습니다. 이 새 섹션에는 CDO 테넌트에 액세스한 모든 사용자의 마지막 로그인 시간과 마지막 로그인 시간에 각 사용자가 보유한 역할이 표시됩니다. 여기에는 명시적 사용자 로그인과 AD 그룹 로그인이 모두 포함됩니다.

다중 역할 사용자

CDO의 IAM 기능에 따른 확장으로 이제 사용자가 여러 역할을 가질 수 있습니다.

사용자는 AD에서 여러 그룹의 일부가 될 수 있으며 각 그룹은 서로 다른 CDO 역할로 CDO에서 정의될 수 있습니다. 로그인 시 사용자가 얻는 최종 권한은 사용자가 속한 CDO에 정의된 모든 AD 그룹의 역할 조합입니다. 예를 들어 사용자가 두 개의 AD 그룹에 속해 있고 두 그룹이 편집 전용 및 배포 전용과 같은 두 가지 다른 역할로 CDO에 추가된 경우, 사용자는 편집 전용 및 배포 전용 권한을 모두 보유하게 됩니다. 이는 여러 그룹 및 역할에 적용됩니다.

AD 그룹 매핑은 CDO에서 한 번만 정의하면 되며, 이후에 다른 그룹 간에 사용자를 추가, 제거 또는 이동하여 사용자에 대한 액세스 및 권한 관리를 AD에서만 독점적으로 수행할 수 있습니다.

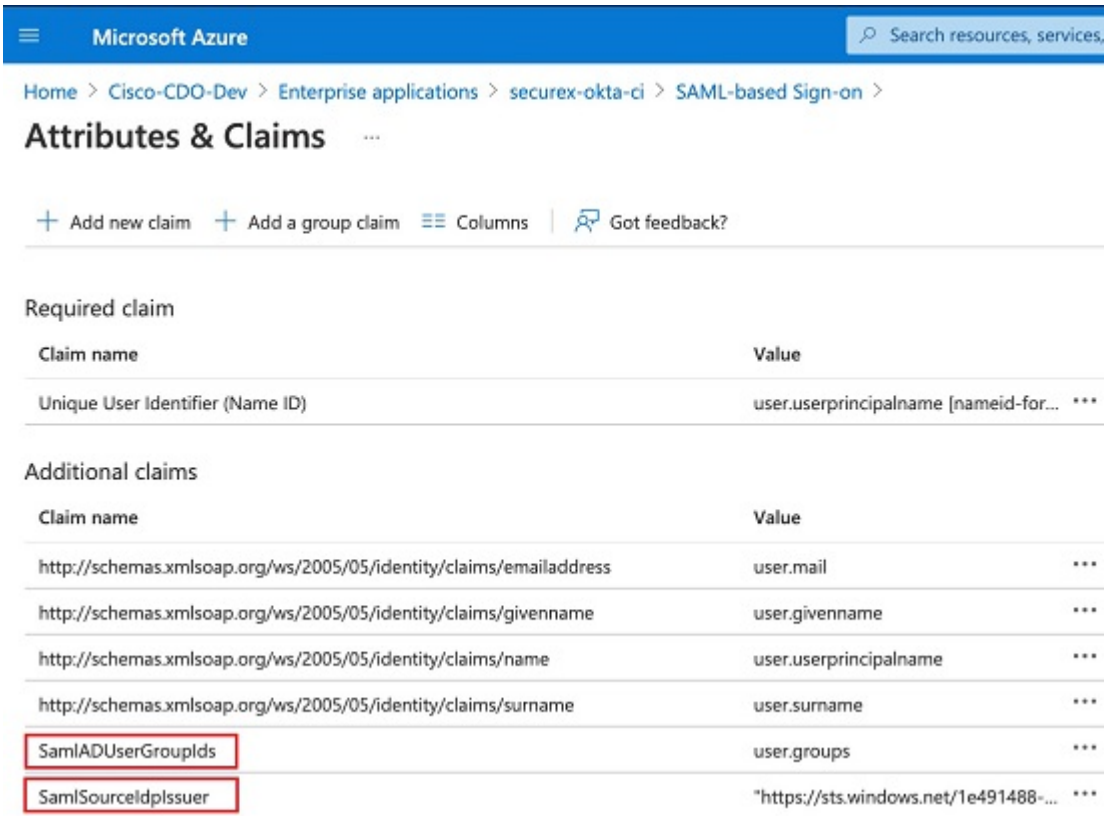
참고 사용자가 개별 사용자이자 동일한 테넌트에 있는 AD 그룹의 일부인 경우 개별 사용자의 사용자 역할이 AD 그룹의 사용자 역할을 오버라이드합니다.

# 시작하기 전에

사용자 관리의 형태로 CDO에 AD 그룹 매핑을 추가하기 전에 AD가 SecureX와 통합되어 있어야 합니다. AD ID 공급자(IdP)가 아직 통합되지 않은 경우 다음 작업을 수행해야 합니다.

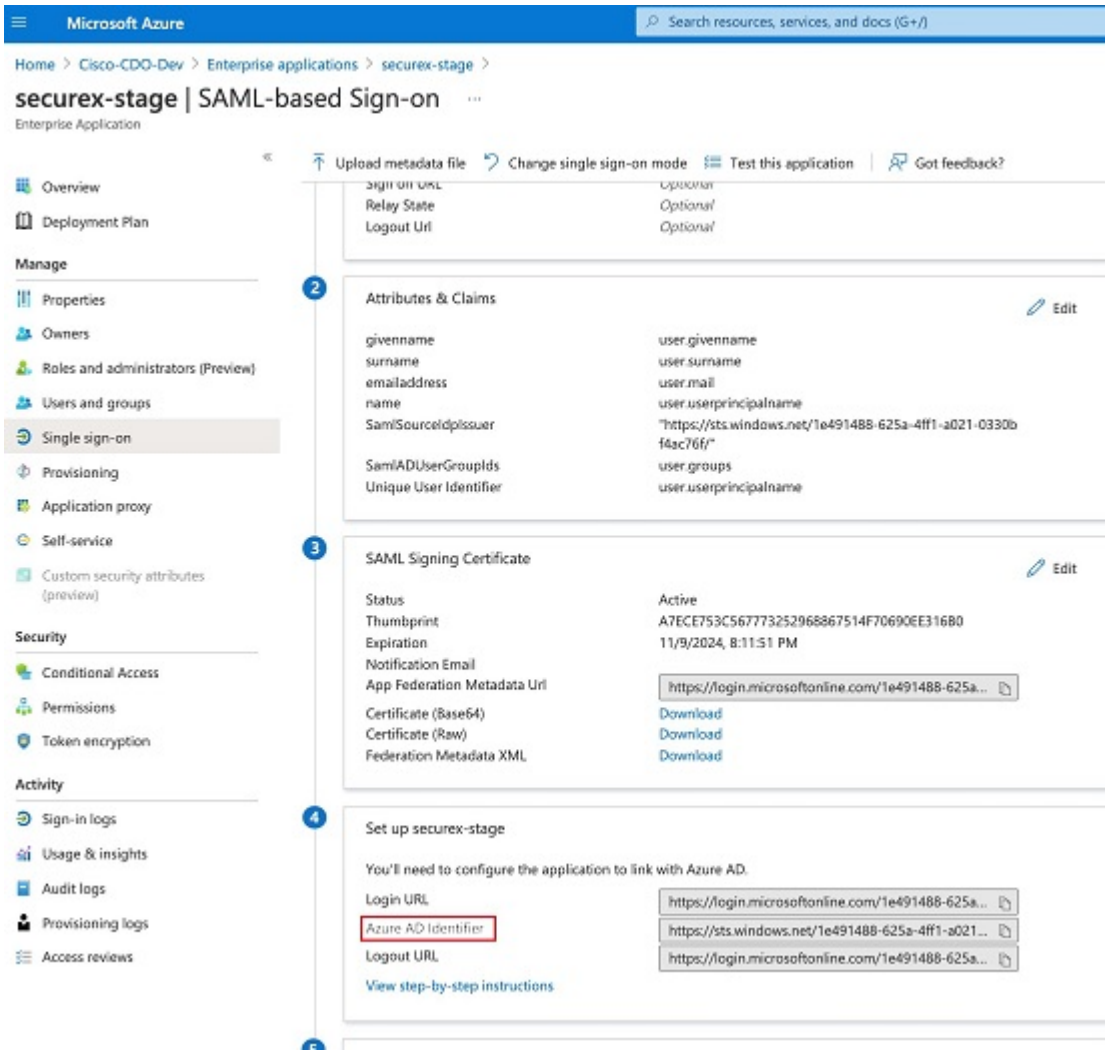
1. Cisco TAC로 지원 사례를 열고 다음 정보와 함께 사용자 지정 AD IdP 통합을 요청하십시오.
   - CDO 테넌트 이름 및 지역.
   - 사용자 지정 라우팅을 정의할 도메인(예: @cisco.com, @myenterprise.com).
   - .XML 형식의 인증서 및 페더레이션 메타데이터.
2. AD에 다음 사용자 지정 SAML 클레임을 추가합니다. 이 값은 대소문자를 구분합니다.
   - **SamlADUserGroupIds** - 이 속성은 사용자가 AD에 가지고 있는 모든 그룹 연결을 설명합니다. 예를 들어 Azure에서 아래 스크린샷과 같이 **+ Add a group claim(+** 그룹 클레임 추가**)**를 선택합니다.

그림 ***1: Active Directory***에 정의된 사용자 지정 클레임




- **SamlSourceIdpIssuer** - 이 특성은 AD 인스턴스를 고유하게 식별합니다. 예를 들어 Azure에서 **+ Add a group claim(+** 그룹 클레임 추가**)**를 선택하고 스크롤하여 아래 스크린샷과 같이 Azure AD 식별자를 찾습니다.

그림 *2: Azure Active Directory* 식별자 찾기




# 사용자 관리를 위한 **Active Directory** 그룹 추가

단계 **1** CDO에 로그인합니다.

단계 **2** 오른쪽 상단의 관리자 드롭다운에서 **Settings(**설정**)**를 클릭합니다.

단계 **3** **User Management(**사용자 관리**)** 탭을 클릭합니다.

단계 **4** 테이블 상단에서 **Active Directory Groups(**활동 디렉토리 그룹**)** 탭을 선택합니다.

단계 **5** 현재 AD 그룹이 없는 경우 **Add AD group(AD** 그룹 추가**)**를 클릭합니다. 기존 항목이 있으면 Add(추가) 버튼을 클릭합니다.

단계 **6** 다음 정보를 입력합니다.

- 그룹 이름 - 고유한 이름을 입력합니다. 이 이름은 AD의 그룹 이름과 일치하지 않아도 됩니다. CDO에서는 이 필드에 대한 특수 문자를 지원하지 않습니다.
- 그룹 **ID** - AD에서 그룹 ID를 수동으로 입력합니다. 그룹 ID의 값은 사용자 지정 클레임 정의의 그룹 ID와 동일해야 합니다. 그룹의 고유 ID에 해당하는 모든 값(예: my-favorite-group, 12345 등)이 될 수 있습니다.
- **AD** 발급자 - AD에서 AD 발급자 값을 수동으로 입력합니다.
- 역할 - 이 AD 그룹에 포함된 모든 사용자의 역할을 결정합니다. 자세한 내용은 사용자 역할을 참조하십시오.
- (선택 사항) 참고 - 이 AD 그룹에 적용 가능한 참고를 추가합니다.

단계 **7** **OK(**확인**)**를 선택합니다.

# 사용자 관리를 위한 **Active Directory** 그룹 편집

시작하기 전에

CDO에서 AD 그룹의 사용자 관리를 편집하면 CDO가 AD 그룹을 제한하는 방식만 편집할 수 있습니다. CDO에서 AD 그룹 자체를 편집할 수 없습니다. AD 그룹 내의 사용자 목록을 편집하려면 AD를 사용해야 합니다.

단계 **1** CDO에 로그인합니다.

단계 **2** 오른쪽 상단의 관리자 드롭다운에서 **Settings(**설정**)**를 클릭합니다.

단계 **3** **User Management(**사용자 관리**)** 탭을 클릭합니다.

단계 **4** 테이블 상단에서 **Active Directory Groups(**활동 디렉토리 그룹**)** 탭을 선택합니다.

단계 **5** 편집할 AD 그룹을 식별하고 **Edit(**편집**)** 아이콘을 선택합니다.

단계 **6** 다음 값을 편집합니다.

- 그룹 이름 - 고유한 이름을 입력합니다. CDO에서는 이 필드에 대한 특수 문자를 지원하지 않습니다.
- 그룹 **ID** - AD에서 그룹 ID를 수동으로 입력합니다. 그룹 ID의 값은 사용자 지정 클레임 정의의 그룹 ID와 동일해야 합니다. 그룹의 고유 ID에 해당하는 모든 값(예: my-favorite-group, 12345 등)이 될 수 있습니다.
- **AD** 발급자 - AD에서 AD 발급자 값을 수동으로 입력합니다.
- 역할 - 이 AD 그룹에 포함된 모든 사용자의 역할을 결정합니다. 자세한 내용은 사용자 역할을 참조하십시오.
- 참고 - 이 AD 그룹에 적용 가능한 참고를 추가합니다.

# 사용자 관리를 위한 Active Directory 그룹 삭제

단계 1 CDO에 로그인합니다.
단계 2 오른쪽 상단의 관리자 드롭다운에서 **Settings(**설정**)**를 클릭합니다.
단계 3 **User Management(**사용자 관리**)** 탭을 클릭합니다.
단계 4 테이블 상단에서 **Active Directory Groups(**활동 디렉토리 그룹**)** 탭을 선택합니다.
단계 5 삭제할 AD 그룹을 식별합니다.
단계 6 **Delete(**삭제**)** 아이콘을 선택합니다.
단계 7 **OK(**확인**)**를 클릭하여 AD 그룹 삭제를 확인합니다.

# 새 CDO 사용자 생성

새 CDO 사용자를 생성하려면 이 두 가지 작업이 필요합니다. 순차적으로 수행할 필요는 없습니다.

- 새 사용자를 위해 Cisco Secure Cloud Sign On 계정 생성
- CDO 사용자 이름으로 CDO 사용자 레코드 생성

이러한 작업이 완료되면 사용자는 새 사용자가 Cisco Secure Sign-On 대시보드에서 CDO 열기

# 새 사용자를 위해 Cisco Secure Cloud Sign On 계정 생성

Cisco Secure Cloud Sign-on 계정 생성은 새 사용자가 언제든지 수행할 수 있습니다. 사용자는 할당될 테넌트의 이름을 알 필요가 없습니다.

## CDO에 로그인 정보

Cisco Defense Orchestrator(CDO)는 Cisco Secure Sign-On을 ID 제공자로 사용하며, MFA(multi-factor authentication)에는 Duo를 사용합니다. **CDO**에 로그인하려면 먼저 **Cisco Security Cloud Sign On**에서 계정을 생성하고 **Duo**를 사용하여 **MFA**를 구성해야 합니다.

CDO에는 사용자 ID를 보호하기 위해 추가 보안 레이어를 제공하는 MFA가 필요합니다. MFA 유형인 이중 인증에서는 CDO에 로그인하는 사용자의 ID를 확인하기 위해 두 가지 구성 요소 또는 요소가 필요합니다. 첫 번째 요소는 사용자 이름과 비밀번호이고, 두 번째 요소는 요청 시 생성되는 일회용 비밀번호(OTP)입니다.

**Important** **2019**년 **10**월 **14**일 이전에 **CDO** 테넌트가 존재했다면 이 문서 대신 Cisco Secure Cloud Sign On ID 제공자로 마이그레이션, on page 35를 사용하여 로그인 지침을 사용합니다.

# 로그인하기 전에

**DUO Security** 설치**.** 휴대전화에 Duo Security 앱을 설치하는 것이 좋습니다. Duo 설치에 대한 질문은 Duo 이중 인증 가이드: 등록 가이드를 참고하십시오.

시간 동기화. 모바일 디바이스를 사용하여 일회용 비밀번호를 생성합니다. OTP는 시간을 기반으로 하므로 디바이스 시계를 실시간으로 동기화하는 것이 중요합니다. 디바이스 시계가 자동으로 또는 수동으로 올바른 시간으로 설정되었는지 확인합니다.

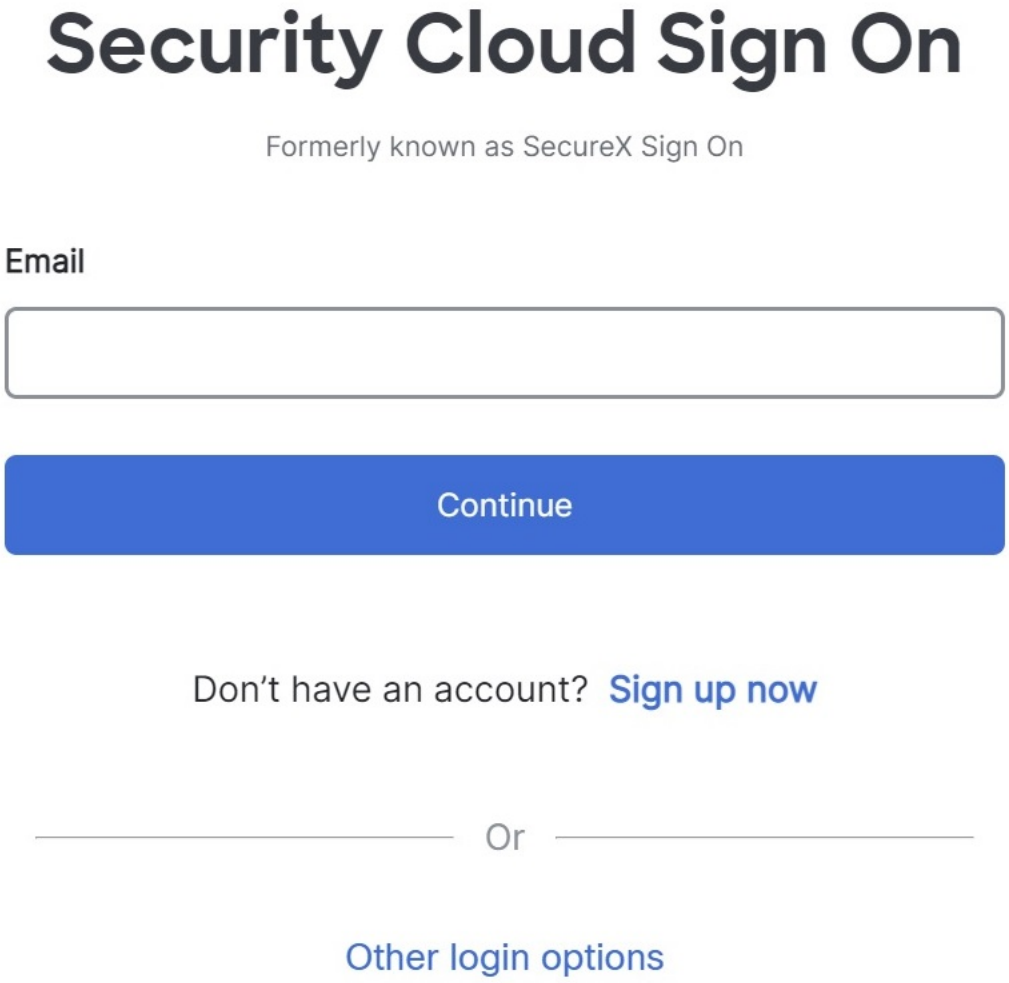
## 새 **Cisco Secure Cloud Sign On** 계정 생성 및 **Duo** 다단계 인증 구성

초기 로그인 워크플로우는 4단계 프로세스입니다. 4단계를 모두 완료해야 합니다.

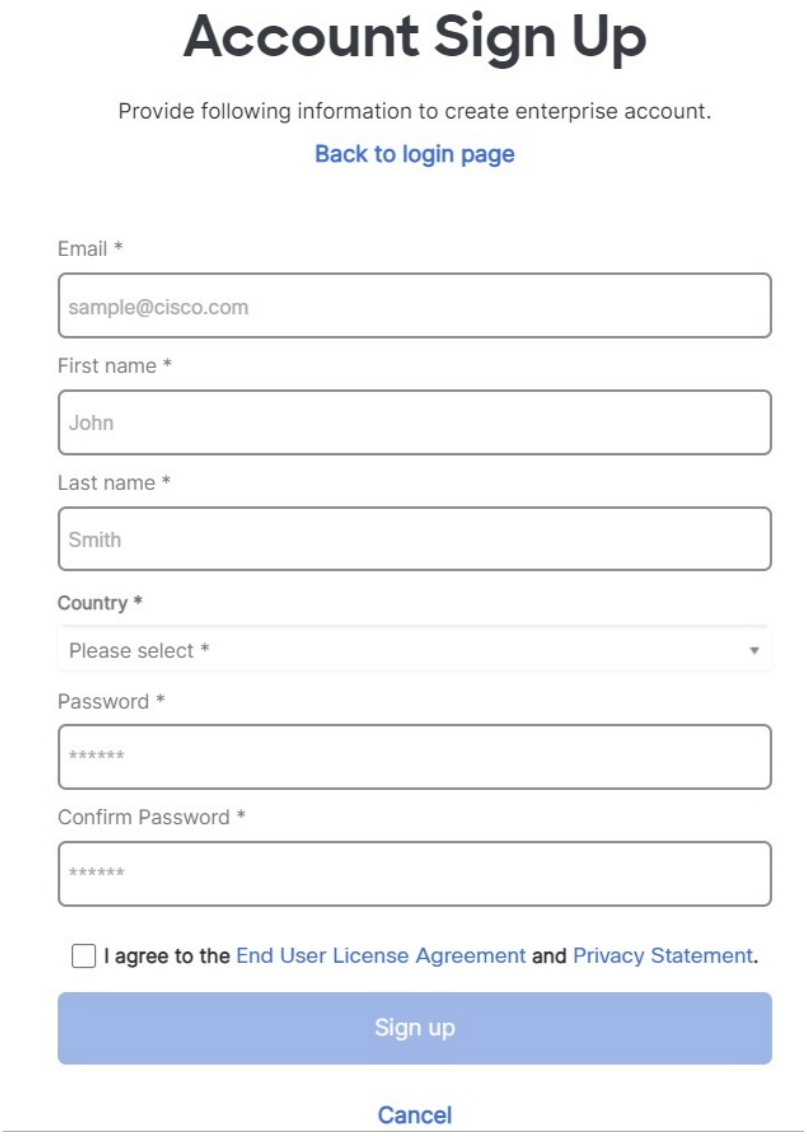
단계 **1** 새 **Cisco Secure Cloud Sign-On** 계정 등록

**a.** https://sign-on.security.cisco.com으로 이동합니다.

**b.** Sign In(로그인) 화면 하단에서 **Sign up(**등록**)**를 클릭합니다.




c. 계정 생성 상자의 필드를 채우십시오.




다음은 몇 가지 팁입니다.

- **Email(**이메일**)** - CDO에 로그인하는 데 사용할 이메일 주소를 입력합니다.
- 암호 - 강력한 암호를 입력하십시오.

**d.** **Create Account(**계정 생성**)**를 클릭한 후.

Cisco는 등록한 주소로 확인 이메일을 보냅니다. 이메일을 열고 어카운트 활성화를 클릭합니다.

단계 **2** **Duo**를 통한 다단계 인증 설정

다단계 인증을 설정할 때는 모바일 디바이스를 사용하는 것이 좋습니다.

**a.** **Set up multi-factor authentication(**다단계 인증 설정**)** 화면에서 **Configure factor(**요인 구성**)**를 클릭합니다.

**b.** **Start setup(**설정 시작**)**을 클릭하고 프롬프트에 따라 모바일 디바이스를 선택하고 해당 모바일 디바이스와 어카운트의 페어링을 확인합니다.

자세한 내용은 Duo Guide to Two Factor Authentication: Enrollment Guide를 참조하십시오. 디바이스에 이미 Duo 앱이 있는 경우 이 어카운트에 대한 활성화 코드를 받게 됩니다. Duo는 하나의 디바이스에서 여러 계정을 지원합니다.

**c.** 마법사가 끝나면 **Continue to Login(**계속 로그인**)**를 클릭합니다.

**d.** 2단계 인증을 사용하여 Cisco Secure Cloud Sign-On에 로그인합니다.

단계 **3** **(**선택 사항**) Google OTP**를 추가 인증자로 설정

**a.** Google Authenticator와 페어링할 모바일 디바이스를 선택하고 **Next(**다음**)**를 클릭합니다.

**b.** 설정 마법사의 프롬프트에 따라 Google 인증기를 설정합니다.

단계 **4** **Cisco Secure Sign-On** 어카운트에 대한 어카운트 복구 옵션 구성

**a.** SMS를 사용하여 계정을 재설정하려면 복원 전화번호를 선택합니다.

**b.** 보안 이미지를 선택합니다.

**c.** **Create My Account(**내 계정 생성**)**를 클릭합니다. 이제 CDO 앱 타일이 있는 Cisco Security Sign-On 대시보드가 표시됩니다. 다른 앱 타일도 표시될 수 있습니다.

**Tip**

대시보드에서 타일을 끌어 원하는 대로 정렬하고, 탭을 생성하여 타일을 그룹화하고, 탭의 이름을 바꿀 수 있습

# CDO 사용자 이름으로 CDO 사용자 레코드 생성

"슈퍼 관리자" 권한이 있는 CDO 사용자만 CDO 사용자 레코드를 생성할 수 있습니다. 슈퍼 관리자는 위의 **Create Your CDO Username(CDO** 사용자 이름 생성**)** 작업에서 지정한 것과 동일한 이메일 주소로 사용자 레코드를 만들어야 합니다.

적절한 사용자 역할이 있는 사용자 레코드를 생성하려면 다음 절차를 수행합니다.

단계 **1** CDO에 로그인합니다.

단계 **2** 오른쪽 상단의 관리자 드롭다운에서 **Settings(**설정**)**를 클릭합니다.

단계 **3** **User Management(**사용자 관리**)** 탭을 클릭합니다.

단계 **4** 파란색 더하기  버튼을 클릭하여 새 사용자를 테넌트에 추가합니다.

단계 **5** 사용자의 이메일 주소를 입력합니다.

**Note** 사용자의 이메일 주소는 Cisco Secure Log-On 계정의 이메일 주소와 일치해야 합니다.

단계 **6** 드롭다운 메뉴에서 사용자 Cisco Defense Orchestrator의 사용자 역할을 선택합니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

# 새 사용자가 Cisco Secure Sign-On 대시보드에서 CDO 열기

단계 **1** Cisco Secure Sign-on 대시보드에서 적절한 **CDO** 타일을 클릭합니다. **CDO** 타일은 https://defenseorchestrator.com으로 안내하고 **CDO(EU)** 타일은 https://defenseorchestrator.eu로 안내합니다.

단계 **2** 두 인증자를 모두 설정한 경우 인증자 로고를 클릭하여 Duo Security 또는 Google Authenticator를 선택합니다.

- 기존 테넌트에 사용자 레코드가 이미 있는 경우 해당 테넌트에 로그인됩니다.
- 이미 여러 포털에 사용자 레코드가 있는 경우 연결할 포털을 선택할 수 있습니다.
- 여러 테넌트에 대한 사용자 레코드가 이미 있는 경우 연결할 CDO 테넌트를 선택할 수 있습니다.
- 기존 테넌트에 대한 사용자 레코드가 아직 없는 경우 CDO에 대해 자세히 알아보거나 평가판 테넌트를 요청할 수 있습니다.

포털 보기는 여러 테넌트에서 통합된 정보를 검색하고 표시합니다. 자세한 내용은 멀티 테넌트 포털 관리를 참조하십시오.

테넌트 보기에는 사용자 레코드가 있는 여러 테넌트가 표시됩니다.


# Cisco Defense Orchestrator의 사용자 역할

Cisco Defense Orchestrator(CDO)에는 읽기 전용, 편집 전용, 구축 전용, 관리자, 슈퍼 관리자 등 다양한 사용자 역할이 있습니다. 사용자 역할은 각 테넌트의 각 사용자에 대해 구성됩니다. CDO 사용자가 둘 이상의 테넌트에 액세스할 수 있는 경우, 사용자 ID는 동일하지만 테넌트마다 역할이 다를 수 있습니다. 사용자는 한 테넌트에 대해서는 읽기 전용 역할을, 다른 테넌트에서는 슈퍼 관리자 역할을 가질 수 있습니다. 인터페이스 또는 설명서에서 읽기 전용 사용자, Admin 사용자 또는 Super Admin 사용자를 언급하는 경우 특정 테넌트에 대한 사용자의 권한 수준을 의미합니다.

## 읽기 전용 역할

읽기 전용 역할이 할당된 사용자는 모든 페이지에서 이 파란색 배너를 볼 수 있습니다.

Read Only User. You cannot make configuration changes.

.

읽기 전용 역할의 사용자는 다음을 수행할 수 있습니다.

- CDO의 모든 페이지 또는 설정을 봅니다.
- 모든 페이지의 콘텐츠를 검색하고 필터링합니다.
- 디바이스 구성을 비교하고 변경 로그를 보고 VPN 매핑을 확인합니다.
- 모든 페이지의 모든 설정 또는 개체에 관한 모든 경고를 봅니다.

- 자체 API 토큰을 생성, 새로 고침 및 취소합니다. 읽기 전용 사용자가 자신의 토큰을 취소하면 다시 생성할 수 없습니다.
- 인터페이스를 통해 지원팀에 문의하고 변경 로그를 내보낼 수 있습니다.

읽기 전용 사용자는 다음을 수행할 수 없습니다.

- 모든 페이지에서 무엇이든 생성, 업데이트, 구성 또는 삭제합니다.
- 디바이스를 온보딩합니다.
- 개체 또는 정책과 같은 항목을 만드는 데 필요한 작업을 단계별로 진행하지만 저장할 수는 없습니다.
- CDO 사용자 레코드를 생성합니다.
- 사용자 역할을 변경합니다.
- 액세스 규칙을 정책에 연결하거나 분리합니다.

# 편집 전용 역할

편집 전용 역할이 있는 사용자는 다음을 수행할 수 있습니다.

- 개체, 정책, 규칙 세트, 인터페이스, VPN 등을 포함하되 이에 국한되지 않는 디바이스 구성을 편집하고 저장합니다.
- **Read Configuration(**구성 읽기**)** 작업을 통해 이루어진 구성 변경을 허용합니다.
- 변경 요청 관리 작업을 활용합니다.

편집 전용 사용자는 다음을 수행할 수 없습니다**.**

- 디바이스 또는 여러 디바이스에 변경 사항을 배포합니다.
- 단계적 변경 또는 OOB를 통해 감지된 변경을 폐기합니다.
- AnyConnect 패키지를 업로드하거나 이러한 설정을 구성합니다.
- 디바이스에 대한 이미지 업그레이드를 예약하거나 수동으로 시작합니다.
- 보안 데이터베이스 업그레이드를 예약하거나 수동으로 시작합니다.
- Snort 2와 Snort 3 버전 사이를 수동으로 전환합니다.
- 템플릿을 생성합니다.
- 기존 OOB 변경 설정을 변경합니다.
- 시스템 관리 설정을 편집합니다.
- 디바이스를 온보딩합니다.
- 디바이스를 삭제합니다.

- VPN 세션 또는 사용자 세션을 삭제합니다.
- CDO 사용자 레코드를 생성합니다.
- 사용자 역할을 변경합니다.

# 배포 전용 역할

배포 전용 역할이 있는 사용자는 다음을 수행할 수 있습니다.

- 디바이스 또는 여러 디바이스에 단계적 변경 사항을 배포합니다.
- ASA 디바이스에 대한 구성 변경 사항을 되돌리거나 복원합니다.
- 디바이스에 대한 이미지 업그레이드를 예약하거나 수동으로 시작합니다.
- 보안 데이터베이스 업그레이드를 예약하거나 수동으로 시작합니다.
- 변경 요청 관리 작업을 활용합니다.

배포 전용 사용자는 다음을 수행할 수 없습니다**.**

- Snort 2와 Snort 3 버전 사이를 수동으로 전환합니다.
- 템플릿을 생성합니다.
- 기존 OOB 변경 설정을 변경합니다.
- 시스템 관리 설정을 편집합니다.
- 디바이스를 온보딩합니다.
- 디바이스를 삭제합니다.
- VPN 세션 또는 사용자 세션을 삭제합니다.
- 모든 페이지에서 무엇이든 생성, 업데이트, 구성 또는 삭제합니다.
- 디바이스를 온보딩합니다.
- 개체 또는 정책과 같은 항목을 만드는 데 필요한 작업을 단계별로 진행하지만 저장할 수는 없습니다.
- CDO 사용자 레코드를 생성합니다.
- 사용자 역할을 변경합니다.
- 액세스 규칙을 정책에 연결하거나 분리합니다.

# **VPN** 세션 관리자 역할

VPN 세션 관리자 역할은 사이트 투 사이트 VPN 연결이 아닌 원격 액세스 VPN 연결을 모니터링하는 관리자를 위해 설계되었습니다.

VPN 세션 관리자 역할이 있는 사용자는 다음을 수행할 수 있습니다.

- CDO의 모든 페이지 또는 설정을 봅니다.
- 모든 페이지의 콘텐츠를 검색하고 필터링합니다.
- 디바이스 구성을 비교하고 변경 로그를 보고 RA VPN 매핑을 확인합니다.
- 모든 페이지의 모든 설정 또는 개체에 관한 모든 경고를 봅니다.
- 자체 API 토큰을 생성, 새로 고침 및 취소합니다. 참고로 VPN 세션 관리자 사용자가 자신의 토큰을 취소하면 토큰을 다시 만들 수 없습니다.
- 인터페이스를 통해 지원팀에 문의하고 변경 로그를 내보냅니다.
- 기존 RA VPN 세션을 종료합니다.

VPN 세션 관리자 사용자는 다음을 수행할 수 없습니다**.**

- 모든 페이지에서 무엇이든 생성, 업데이트, 구성 또는 삭제합니다.
- 디바이스를 온보딩합니다.
- 개체 또는 정책과 같은 항목을 만드는 데 필요한 작업을 단계별로 진행하지만 저장할 수는 없습니다.
- CDO 사용자 레코드를 생성합니다.
- 사용자 역할을 변경합니다.
- 액세스 규칙을 정책에 연결하거나 분리합니다.

# 관리자 역할

관리 사용자는 대부분의 CDO 측면에 대한 완전한 액세스 권한을 가집니다. 관리 사용자는 다음을 수행할 수 있습니다.

- CDO에서 개체 또는 정책을 생성, 읽기, 업데이트 및 삭제하고 설정을 구성합니다.
- 디바이스를 온보딩합니다.
- CDO의 모든 페이지 또는 설정을 봅니다.
- 모든 페이지의 콘텐츠를 검색하고 필터링합니다.
- 디바이스 구성을 비교하고 변경 로그를 보고 VPN 매핑을 확인합니다.
- 모든 페이지의 모든 설정 또는 개체에 관한 모든 경고를 봅니다.
- 자체 API 토큰을 생성, 새로 고침 및 취소합니다. 토큰이 취소되면 인터페이스를 통해 지원팀에 문의하고 변경 로그를 내보낼 수 있습니다.

관리 사용자는 다음을 수행할 수 없습니다**.**

- CDO 사용자 레코드를 생성합니다.
- 사용자 역할을 변경합니다.

# 슈퍼 관리자

슈퍼 관리자는 CDO의 모든 측면에 대한 완전한 액세스 권한을 갖습니다. 슈퍼 관리자는 다음을 수행할 수 있습니다.

- 사용자 역할을 변경합니다.
- 사용자 레코드를 생성합니다.

**Note** 최고 관리자는 CDO 사용자 레코드를 생성할 수 있지만 사용자가 테넌트에 로그인하는 데 필요한 모든 사용자 레코드는 아닙니다. 사용자는 테넌트에서 사용하는 ID 제공자의 계정도 필요합니다. 엔터프라이즈에 자체 SSO(Single Sign-On) ID 제공자가 없는 경우 ID 제공자는 Cisco Secure Cloud Sign-on입니다. 사용자는 Cisco Secure Cloud Sign-On 계정에 자가 등록할 수 있습니다. 자세한 내용은 새 CDO 테넌트에 대한 초기 로그인, on page 34를 참조하십시오.

- CDO에서 개체 또는 정책을 생성, 읽기, 업데이트 및 삭제하고 설정을 구성합니다.
- 디바이스를 온보딩합니다.
- CDO의 모든 페이지 또는 설정을 봅니다.
- 모든 페이지의 콘텐츠를 검색하고 필터링합니다.
- 디바이스 구성을 비교하고 변경 로그를 보고 VPN 매핑을 확인합니다.
- 모든 페이지의 모든 설정 또는 개체에 관한 모든 경고를 봅니다.
- 자체 API 토큰을 생성, 새로 고침 및 취소합니다. 토큰이 취소되면 다음을 수행할 수 있습니다.
- 인터페이스를 통해 지원팀에 문의하고 변경 로그를 내보낼 수 있습니다.

# 사용자 역할의 기록 변경

사용자 레코드는 사용자의 현재 역할이 기록된 것입니다. 테넌트와 연결된 사용자를 보면 레코드별로 각 사용자의 역할을 확인할 수 있습니다. 사용자 역할을 변경하면 사용자 레코드가 변경됩니다. 사용자의 역할은 사용자 관리 테이블에서 해당 역할로 식별됩니다. 자세한 내용은 사용자 관리를 참조하십시오.

사용자 레코드를 변경하려면 슈퍼 관리자여야 합니다. 테넌트에 슈퍼 관리자가 없는 경우 CDO 고객이 TAC로 지원 티켓을 여는 방법에 문의하십시오.

# 사용자 역할에 대한 사용자 레코드 생성

CDO 사용자는 인증을 받고 CDO 테넌트에 액세스할 수 있도록 CDO 레코드 및 해당 IdP 계정이 필요합니다. 이 절차는 Cisco Secure Cloud Sign-On의 사용자 계정이 아니라 사용자의 CDO 사용자 레코드를 생성합니다. 사용자가 Cisco Security Cloud Sign On에 계정이 없는 경우, https://sign-on.security.cisco.com으로 이동하고 로그인 화면 하단에서 **Sign up(**등록**)**을 클릭하여 자가 등록할 수 있습니다. .

**Note** 이 작업을 수행하려면 CDO에서 슈퍼 관리자 역할이 있어야 합니다.

## 사용자 레코드 생성

적절한 사용자 역할이 있는 사용자 레코드를 생성하려면 다음 절차를 수행합니다.

단계 **1** CDO에 로그인합니다.

단계 **2** 오른쪽 상단의 관리자 드롭다운에서 **Settings(**설정**)**를 클릭합니다.

단계 **3** **User Management(**사용자 관리**)** 탭을 클릭합니다.

단계 **4** 파란색 더하기 버튼을 클릭하여 새 사용자를 테넌트에 추가합니다.

단계 **5** 사용자의 이메일 주소를 입력합니다.

**Note** 사용자의 이메일 주소는 Cisco Secure Log-On 계정의 이메일 주소와 일치해야 합니다.

단계 **6** 드롭다운 메뉴에서 사용자 Cisco Defense Orchestrator의 사용자 역할을 선택합니다.

단계 **7** **v**를 클릭합니다.

**Note** 최고 관리자는 CDO 사용자 레코드를 생성할 수 있지만 사용자가 테넌트에 로그인하는 데 필요한 모든 사용자 레코드는 아닙니다. 사용자는 테넌트에서 사용하는 ID 제공자의 계정도 필요합니다. 엔터프라이즈에 자체 SSO(Single Sign-On) ID 제공자가 없는 경우 ID 제공자는 Cisco Secure Sign-on입니다. 사용자는 Cisco Secure Sign-On 계정에 자가 등록할 수 있습니다. 자세한 내용은 새 CDO 테넌트에 대한 초기 로그인, on page 34를 참조하십시오.

## API 전용 사용자 생성

단계 **1** CDO에 로그인합니다.

단계 **2** 오른쪽 상단의 관리자 드롭다운에서 **Settings(**설정**)**를 클릭합니다.

단계 **3** **User Management(**사용자 관리**)** 탭을 클릭합니다.

단계 **4** 테넌트에 새 사용자를 추가하려면 파란색 플러스 버튼  를 클릭합니다.

단계 **5** **API Only User(API** 전용 사용자**)** 확인란을 선택합니다.

단계 **6** **Username(**사용자 이름**)** 필드에 사용자 이름을 입력하고 **OK(**확인**)**를 클릭합니다.

중요 사용자 이름은 이메일 주소이거나 '@yourtenant' 접미사가 사용자 이름에 자동으로 추가되므로 '@' 문자를 포함할 수 없습니다.

단계 **7** 드롭다운 메뉴에서 사용자 Cisco Defense Orchestrator의 사용자 역할을 선택합니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

단계 **9** **User Management(**사용자 관리**)** 탭을 클릭합니다.

단계 **10** 새 API 전용 사용자의 토큰 열에서 **Generate API Token(API** 토큰 생성**)**을 클릭하여 API 토큰을 얻습니다.

# 사용자 역할에 대한 사용자 레코드 편집

이 작업을 수행하려면 슈퍼 관리자 역할이 있어야 합니다. 슈퍼 관리자가 로그인한 CDO 사용자의 역할을 변경할 경우 역할이 변경되면 해당 사용자는 자동으로 세션에서 로그아웃됩니다. 사용자가 다시 로그인하면 새 역할을 맡게 됩니다.

**Note** 이 작업을 수행하려면 CDO에서 슈퍼 관리자 역할이 있어야 합니다.

**Caution** 사용자 레코드의 역할을 변경하면 사용자 레코드와 연결된 API 토큰이 있는 경우 해당 토큰이 삭제됩니다. 사용자 역할이 변경되면 사용자는 새 API 토큰을 생성해야 합니다.

## 사용자 역할 편집

**Note** CDO 사용자가 로그인되어 있고 슈퍼 관리자가 역할을 변경하는 경우, 변경 사항을 적용하려면 사용자가 로그아웃했다가 다시 로그인해야 합니다.

사용자 레코드에 정의된 역할을 편집하려면 다음 절차를 따르십시오.

단계 **1** CDO에 로그인합니다.

단계 **2** 오른쪽 상단의 관리자 드롭다운에서 **Settings(**설정**)**를 클릭합니다.

단계 **3** **User Management(**사용자 관리**)** 탭을 클릭합니다.

단계 **4** 사용자 행에서 편집 아이콘을 클릭합니다.

단계 **5** 역할 드롭다운 메뉴에서 사용자의 새 Cisco Defense Orchestrator의 사용자 역할을 선택합니다.

단계 **6** 사용자 레코드에 사용자와 연결된 API 토큰이 있는 것으로 표시되면 사용자의 역할을 변경하고 결과적으로 API 토큰을 삭제할 것임을 확인해야 합니다.

단계 **7** **v**를 클릭합니다.

단계 **8** CDO가 API 토큰을 삭제한 경우 사용자에게 연락하여 새 API 토큰을 생성합니다.

# 사용자 역할에 대한 사용자 레코드 삭제

CDO에서 사용자 레코드를 삭제하면 Cisco Secure Cloud Sign-On 계정과 사용자 레코드의 매핑이 끊어져 연결된 사용자가 CDO에 로그인할 수 없습니다. 사용자 레코드를 삭제하면 해당 사용자 레코드와 연결된 API 토큰도 삭제됩니다. CDO에서 사용자 레코드를 삭제해도 Cisco Secure Cloud Sign-On에서 사용자의 IdP 계정은 삭제되지 않습니다.

**Note** 이 작업을 수행하려면 CDO에서 슈퍼 관리자 역할이 있어야 합니다.

## 사용자 레코드 삭제

사용자 레코드에 정의된 역할을 삭제하려면 다음 절차를 참조하십시오.

단계 **1** CDO에 로그인합니다.

단계 **2** 오른쪽 상단의 관리자 드롭다운에서 **Settings(**설정**)**를 클릭합니다.

단계 **3** **User Management(**사용자 관리**)** 탭을 클릭합니다.

단계 **4** 삭제할 사용자 행에서 휴지통 아이콘를 클릭합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** 확인을 클릭하여 테넌트에서 계정을 제거할 것임을 확인합니다.

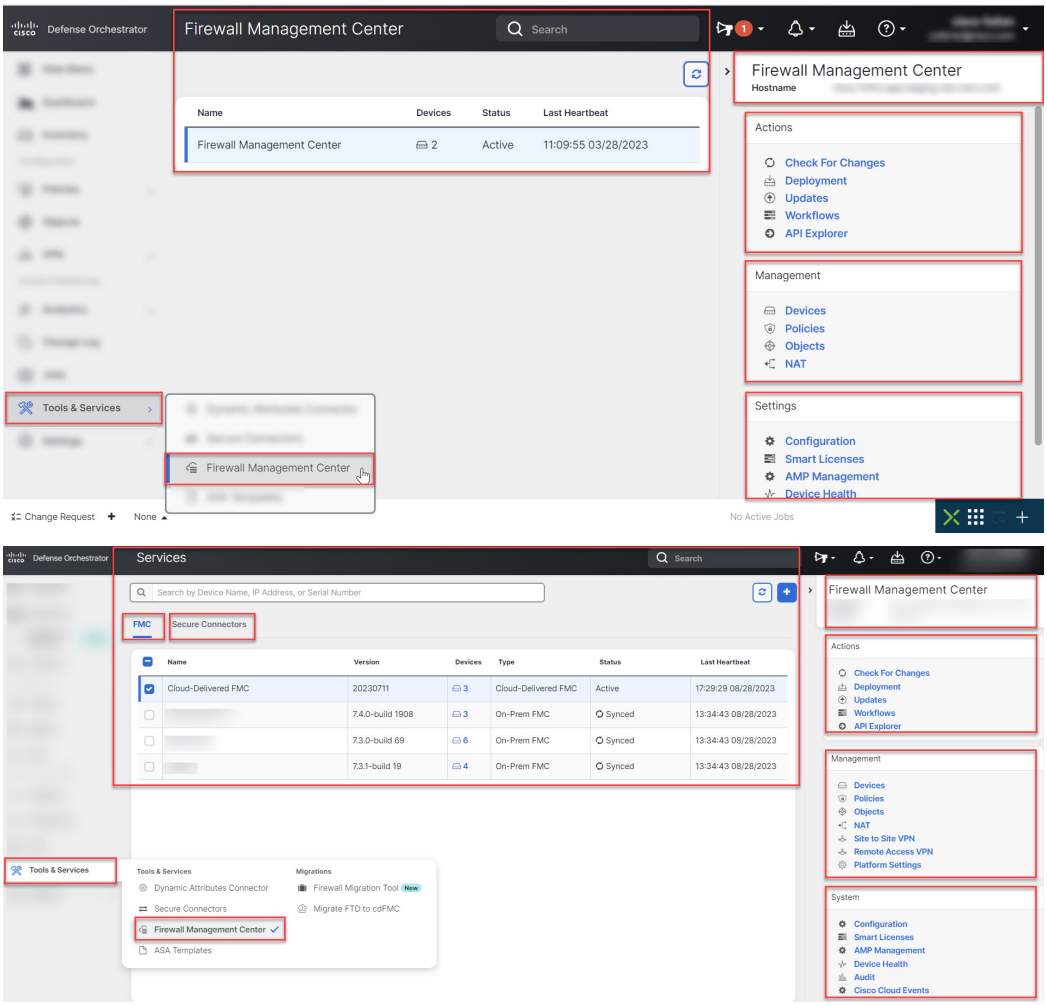
# 서비스 페이지 정보 보기

**Services(**서비스**)** 페이지에 CDO가 제공하는 서비스 목록이 표시됩니다. **FMC** 탭을 선택하면 CDO 계정에 연결된 클라우드 사용 Firewall Management Center 및 CDO에 온보딩된 모든 온프레미스 Management Center가 나열됩니다. 이러한 온프레미스 Management Center에서 관리하는 디바이스는 **Inventory(**인벤토리**)** 페이지에 나열됩니다. **Services(**서비스**)** 페이지의 **Secure Connector(**보안 커넥터**)** 탭 아래에도 보안 커넥터가 나열됩니다.

파란색 더하기 아이콘( )을 클릭하여 **FMC** 탭을 선택하고 온프레미스 Management Center를 온보딩한 후 오른쪽 창의 옵션을 사용하여 디바이스 작업을 수행할 수 있습니다. 디바이스의 버전, Management Center에서 관리하는 디바이스의 수, 디바이스 유형, 디바이스 동기화 상태 등의 디바이스 정보도 확인할 수 있습니다. 매니지드 디바이스 아이콘을 클릭하면 **Inventory(**인벤토리**)** 페이지로 이동하며, 이 페이지에는 선택된 온프레미스 Management Center에서 관리하는 디바이스가 자동으로 필터링되어 표시됩니다. **Services(**서비스**)** 페이지에서는 하나 이상의 온프레미스 Management Center를 동시에 선택하여 Management Center 그룹에 대한 작업을 한 번에 수행할 수 있습니다. 클라우드 사용 Firewall Management Center가 선택된 상태에서는 어떤 온프레미스 Management Center도 선택할 수 없습니다. 새 보안 커넥터를 추가하거나 기존 보안 커넥터에 대해 작업을 수행하려면 **Secure Connector(**보안 커넥터**)** 탭을 선택하고 를 클릭합니다.

CDO의 메인 메뉴에서 클라우드 사용 Firewall Management Center 애플리케이션 페이지를 엽니다.

**Tools & Services(**툴 및 서비스**)** > **Firewall Management Center**로 이동합니다.




클라우드 사용 Firewall Management Center의 경우 Services(서비스) 페이지에 다음 정보가 표시됩니다.

- 클라우드 사용 Firewall Management Center가 테넌트에 구축되지 않은 경우, **Request FMC(FMC 요청)**를 클릭합니다.
- 클라우드 사용 Firewall Management Center에 구축된 Secure Firewall Threat Defense 디바이스 수.
- CDO 및 클라우드 사용 Firewall Management Center 페이지 간의 연결 상태.
- 클라우드 사용 Firewall Management Center의 마지막 하트비트. 이는 클라우드 사용 Firewall Management Center 자체의 상태와 여기에서 관리하는 디바이스 수가 이 페이지의 테이블과 마지막으로 동기화된 것을 나타냅니다.
- 선택한 클라우드 사용 Firewall Management Center의 호스트 이름.

**Cloud-Delivered FMC(**클라우드 제공 **FMC)**를 선택하고 **Actions(**작업**)**, **Management(**관리**)** 또는 **Settings**(설정) 창의 링크를 사용하여 클릭한 링크와 연결된 구성 작업을 수행할 수 있는 클라우드 사용 Firewall Management Center사용자 인터페이스를 엽니다.

클라우드 사용 Firewall Management Center 페이지가 열리면 파란색 물음표 버튼을 클릭하고 **Page-level Help(**페이지 수준 도움말**)**를 선택하여 현재 페이지와 수행 가능한 추가 작업에 대해 자세히 알아볼 수 있습니다.

클라우드 사용 **Firewall Management Center** 디바이스 수 및 상태 업데이트

**Cloud-Delivered FMC(**클라우드 제공 **FMC)**를 선택하고 **Actions(**작업**)** 창에서 **Check for Changes(**변경 사항 확인**)**를 클릭합니다. 테이블의 디바이스 수 및 상태 정보가 이 페이지와 클라우드 사용 Firewall Management Center가 마지막으로 동기화되었을 때 사용 가능한 정보로 업데이트됩니다. 동기화는 10분마다 이루어집니다.

다른 탭에서 **CDO** 및 클라우드 사용 **Firewall Management Center** 애플리케이션 열기 지원

클라우드 사용 Firewall Management Center에서 위협 방어 디바이스 또는 개체를 구성할 때 추가 브라우저 탭에서 해당 구성 페이지를 열면 로그아웃하지 않고도 CDO 및 클라우드 사용 Firewall Management Center 포털에서 동시에 작업할 수 있습니다. 예를 들어, 클라우드 사용 Firewall Management Center에서 개체를 생성하고 동시에 보안 정책에서 생성된 CDO의 이벤트 로그를 모니터링할 수 있습니다.

이 기능은 클라우드 사용 Firewall Management Center 포털로 이동하는 모든 CDO 링크에서 사용할 수 있습니다. 새 탭에서 클라우드 사용 Firewall Management Center 포털을 여는 방법:

CDO 포털에서 **Ctrl**(Windows) 또는 **Command**(Mac) 버튼을 누른 상태로 해당 링크를 클릭합니다.

참고 한 번 클릭하면 동일한 탭에서 클라우드 사용 Firewall Management Center 페이지가 열립니다.

다음은 새 탭에서 클라우드 사용 Firewall Management Center 포털 페이지를 여는 몇 가지 예입니다.

- **Tools & Services(**툴 및 서비스**)** > **Firewall Management Center**를 선택하고 **Cloud-Delivered FMC(**클라우드 제공 **FMC)**를 선택합니다.

  오른쪽 창에서 **Ctrl**(Windows) 또는 **Command**(Mac) 버튼을 누른 상태로 액세스하려는 페이지를 클릭합니다.

- **Objects(**개체**)** > **Other FTD Objects(**기타 **FTD** 개체**)**를 선택합니다.
- CDO 페이지 오른쪽 상단 모서리에 있는 검색 아이콘을 클릭하고 표시되는 검색 필드에 검색 문자열을 입력합니다.

  검색 결과에서 **Ctrl**(Windows) 또는 **Command**(Mac) 버튼을 누른 상태로 화살표 아이콘을 클릭합니다.
- **Dashboard(**대시보드**)** > **Quick Actions(**빠른 작업**)**를 선택합니다.

  **Ctrl**(Windows) 또는 **Command**(Mac) 버튼을 누른 상태에서 **Manage FTD Policies(FTD** 정책 관리**)** 또는 **Manage FTD Objects(FTD** 개체 관리**)**를 클릭합니다.

참고 새 CDO 테넌트로 전환하면 새 탭에서 이미 열린 해당 클라우드 사용 Firewall Management Center 포털이 로그아웃됩니다.

# 디바이스 및 서비스 관리

Cisco CDO(Defense Orchestrator)는 지원되는 디바이스 및 서비스를 보고, 관리하고, 필터링하고, 평가하는 기능을 제공합니다. **Inventory(**인벤토리**)** 페이지에서 다음을 수행할 수 있습니다.

- CDO 관리를 위한 디바이스 및 서비스를 온보딩합니다.
- 관리 디바이스 및 서비스의 구성 상태 및 연결 상태를 봅니다.
- 별도의 탭으로 분류된 온보딩된 디바이스 및 템플릿을 봅니다. 재고 목록 페이지 정보 보기, 87 페이지을 참조하십시오.
- 개별 디바이스 및 서비스를 평가하고 조치를 취합니다.
- 디바이스 및 서비스별 정보를 보고 문제를 해결합니다.
- 다음에서 관리하는 위협 방어 디바이스의 디바이스 상태를 확인합니다.
  - 클라우드 사용 Firewall Management Center
  - 온프레미스 Management Center

  클라우드 사용 Firewall Management Center에서 관리하는 위협 방어 디바이스의 경우, 클러스터에 있는 디바이스의 노드 상태도 볼 수 있습니다.
- 이름, 유형, IP 주소, 모델 이름, 일련 번호 또는 레이블로 디바이스 또는 템플릿을 검색합니다. 검색은 대/소문자를 구분하지 않습니다. 여러 검색어를 제공하면 검색어 중 하나 이상과 일치하는 디바이스 및 서비스가 나타납니다. 검색, 90 페이지을 참조하십시오.
- 디바이스 유형, 하드웨어 및 소프트웨어 버전, snort 버전, 구성 상태, 연결 상태, 충돌 감지, 보안 디바이스 커넥터 및 레이블을 기준으로 디바이스 또는 템플릿 필터를 필터링합니다. 필터를 참조하십시오.

# CDO에서 디바이스의 IP 주소 변경

IP 주소를 사용하여 CDO(Cisco Defense Orchestrator)에 디바이스를 온보딩하면 CDO는 해당 IP 주소를 데이터베이스에 저장하고 해당 IP 주소를 사용하여 디바이스와 통신합니다. 디바이스의 IP 주소가 변경되면 새 주소와 일치하도록 CDO에 저장된 IP 주소를 업데이트할 수 있습니다. CDO에서 디바이스의 IP 주소를 변경해도 디바이스의 구성은 변경되지 않습니다.

CDO가 디바이스와 통신하는 데 사용하는 IP 주소를 변경하려면 다음 절차를 수행합니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 **4** IP 주소를 변경할 디바이스를 선택합니다.

단계 **5** **Device Details(**디바이스 세부 정보**)** 창 위에서 디바이스의 IP 주소 옆에 있는 편집 버튼을 클릭합니다.


단계 **6** 필드에 새 IP 주소를 입력하고 파란색 확인 버튼을 클릭합니다.

디바이스 자체는 변경되지 않으므로 디바이스의 Configuration Status(구성 상태)는 계속해서 Synced(동기화됨)로 표시됩니다.

관련 정보**:**

- 테넌트 간 디바이스 이동, on page 86
- CDO에 디바이스 대량 다시 연결, on page 86

# CDO에서 디바이스의 이름 변경

모든 디바이스, 모델, 템플릿 및 서비스는 온보딩되거나 CDO에서 생성될 때 이름이 지정됩니다. 디바이스 자체의 구성을 변경하지 않고 해당 이름을 변경할 수 있습니다.

단계 **1** 탐색 모음에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 **3** 이름을 변경하려는 디바이스를 선택합니다.

단계 **4** **Device Details(**디바이스 세부 정보**)** 창 위에서 디바이스의 이름 옆에 있는 편집 버튼을 클릭합니다.


단계 **5** 필드에 새 이름을 입력하고 파란색 확인 버튼을 클릭합니다.

디바이스 자체는 변경되지 않으므로 디바이스의 Configuration Status(구성 상태)는 계속해서 Synced(동기화됨)로 표시됩니다.

# 디바이스 및 서비스 목록 내보내기

이 문서에서는 디바이스 및 서비스 목록을 쉼표로 구분된 값(.csv) 파일로 내보내는 방법을 설명합니다. 이 형식이 되면 Microsoft Excel과 같은 스프레드시트 애플리케이션에서 파일을 열어 목록의 항목을 정렬하고 필터링할 수 있습니다.

내보내기 버튼은 디바이스 및 템플릿 탭에서 사용할 수 있습니다. 또한 선택한 디바이스 유형 탭의 디바이스에서 세부 정보를 내보낼 수 있습니다.

디바이스 및 서비스 목록을 내보내기 전에 필터 창을 살펴보고 재고 목록 테이블에 내보내려는 정보가 표시되는지 확인합니다. 모든 필터를 지워 모든 매니지드 디바이스 및 서비스를 확인하거나 정보를 필터링하여 모든 디바이스 및 서비스의 하위 집합을 표시합니다. 내보내기 기능은 Inventory(재고 목록) 테이블에서 확인할 수 있는 내용을 내보냅니다.

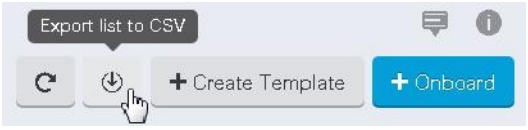
단계 **1** CDO 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 유형 탭을 클릭하여 해당 탭 아래의 디바이스에서 세부 정보를 내보내거나 **All(**모두**)**을 클릭하여 모든 디바이스에서 세부 정보를 내보냅니다.

필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 **4** **Export list to CSV(CSV**로 목록 내보내기**)**를 클릭합니다.




단계 **5** 메시지가 표시되면 .csv 파일을 저장합니다.

단계 **6** 스프레드시트 애플리케이션에서 .csv 파일을 열어 결과를 정렬하고 필터링합니다.

# 디바이스 구성 내보내기

한 번에 하나의 디바이스 구성만 내보낼 수 있습니다. 다음 절차를 사용하여 디바이스의 구성을 JSON 파일로 내보냅니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

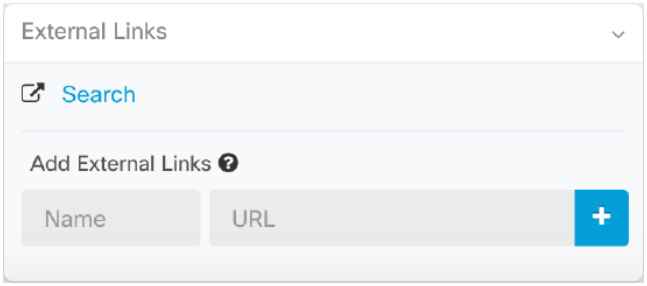
단계 **4** 원하는 디바이스를 선택하여 강조 표시하십시오.

단계 **5** **Actions(**작업**)** 창에서 **Export Configuration(**구성 내보내기**)**를 선택합니다.

단계 **6** **Confirm(**확인**)**을 선택하여 구성을 JSON 파일로 저장합니다.

# 디바이스의 외부 링크

외부 리소스에 대한 하이퍼링크를 생성하여 CDO로 관리하는 디바이스와 연결할 수 있습니다. 이 기능을 사용하여 디바이스 중 하나의 로컬 관리자에 대한 편리한 링크를 생성할 수 있습니다(ASA의 경우 ASDM(Adaptive Security Device Manager), FTD의 경우 ). 또한 이를 사용하여 검색 엔진, 설명서 리소스, 회사 Wiki 또는 선택한 다른 URL에 연결할 수 있습니다. 외부 링크를 원하는 만큼 디바이스에 연결할 수 있습니다. 동일한 링크를 여러 디바이스와 동시에 연결할 수도 있습니다.




생성한 링크는 어디에나 연결할 수 있지만 회사의 보안 요구 사항은 변경되지 않습니다. 예를 들어 특정 URL에 도달하기 위해 온프레미스 또는 VPN 연결을 통해 일반적으로 기업 네트워크에 연결해야 하는 경우 이러한 요구 사항은 그대로 유지됩니다. 회사에서 특정 URL을 차단하는 경우 해당 URL은 계속 차단됩니다. 제한되지 않은 URL은 계속해서 제한되지 않습니다.

위치 변수

URL에 통합할 수 있는 {location} 변수를 생성했습니다. 이 변수는 디바이스의 IP 주소로 채워집니다. 예를 들면 다음과 같습니다.

```
https://{location}
```

ASA의 ASDM에 도달 또는

관련 정보**:**

- 디바이스 메모 작성, on page 86
- 디바이스 및 서비스 목록 내보내기, on page 82

## 장치에서 외부 링크 생성

단계 **1** 탐색 모음에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 2 **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.
단계 3 해당 디바이스 탭을 클릭합니다.
단계 4 장치 또는 모델을 선택합니다.

필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 5 세부 정보 창의 오른쪽에서, **External Links(**외부 링크**)** 섹션으로 이동합니다.
단계 6 링크 이름을 입력합니다.
단계 7 URL 필드에 링크의 URL을 입력합니다. 예를 들어 Cisco의 경우 http://www.cisco.com을 입력하는 것과 같이 전체 URL을 지정해야 합니다.
단계 8 +를 클릭하여 링크를 디바이스와 연결합니다.

## ASDM 에 대한 외부 링크 생성

다음은 CDO에서 직접 ASA의 ASDM(Adaptive Security Device Manager)과 을 여는 편리한 방법입니다.

단계 1 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.
단계 2 **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.
단계 3 해당 디바이스 탭을 클릭합니다.

필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 4 디바이스 또는 모델을 선택합니다.
단계 5 세부 정보 창의 오른쪽에서, **External Links(**외부 링크**)** 섹션으로 이동합니다.
단계 6 ASDM 과 같은 링크 이름을 입력합니다.
단계 7 URL 필드에 https://{location}을 입력합니다. {location} 변수는 디바이스의 IP 주소로 채워집니다.
단계 8 + 상자를 클릭합니다.

## 여러 디바이스에 대한 외부 링크 생성

단계 1 탐색 모음에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.
단계 2 **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.
단계 3 해당 디바이스 탭을 클릭합니다.

필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 4 여러 디바이스 또는 모델을 선택합니다.
단계 5 세부 정보 창의 오른쪽에서, **External Links(**외부 링크**)** 섹션으로 이동합니다.
단계 6 링크 이름을 입력합니다.

단계 **7** 다음 방법 중 하나를 사용하여 도달하려는 URL을 입력하십시오.

- 입력

  ```
  https://{location}
  ```

  URL 필드에. {location} 변수는 디바이스의 IP 주소로 채워집니다. 이렇게 하면 디바이스의 ASDM에 대한 자동 링크가 생성됩니다.

- URL 필드에 링크의 URL을 입력합니다. 예를 들어 Cisco의 경우 http://www.cisco.com을 입력하는 것과 같이 전체 URL을 지정해야 합니다.

단계 **8** +를 클릭하여 링크를 디바이스와 연결합니다.

## 외부 링크 편집 또는 삭제

단계 **1** 탐색 모음에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.
단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.
단계 **3** 해당 디바이스 탭을 클릭합니다.

필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 **4** 디바이스 또는 모델을 선택합니다.
단계 **5** 세부 정보 창의 오른쪽에서, **External Links(**외부 링크**)** 섹션으로 이동합니다.
단계 **6** 편집 및 삭제 아이콘을 표시하려면 링크 이름에 마우스를 올려놓습니다.
단계 **7** 해당 아이콘을 클릭하여 외부 링크를 편집하거나 삭제하고 작업을 확인합니다.

## 여러 디바이스에 대한 외부 링크 편집 또는 삭제

단계 **1** 탐색 모음에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.
단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.
단계 **3** 해당 디바이스 탭을 클릭합니다.

필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 **4** 여러 디바이스 또는 모델을 선택합니다.
단계 **5** 세부 정보 창의 오른쪽에서, **External Links(**외부 링크**)** 섹션으로 이동합니다.
단계 **6** 편집 및 삭제 아이콘을 표시하려면 링크 이름에 마우스를 올려놓습니다.
단계 **7** 해당 아이콘을 클릭하여 외부 링크를 편집하거나 삭제하고 작업을 확인합니다.

# CDO에 디바이스 대량 다시 연결

관리자는 CDO를 통해 둘 이상의 매니지드 디바이스를 CDO에 동시에 다시 연결할 수 있습니다. CDO가 관리하는 디바이스가 "unreachable(연결할 수 없음)"로 표시되면 CDO는 더 이상 대역 외 구성 변경 사항을 탐지하거나 디바이스를 관리할 수 없습니다. 연결이 끊어지는 데에는 여러 가지 이유가 있을 수 있습니다. 디바이스에 대한 CDO 관리를 복원하는 첫 번째 단계는 디바이스를 다시 연결하는 것입니다.

**Note** 새 인증서가 있는 디바이스를 다시 연결하는 경우 CDO는 디바이스에서 새 인증서를 자동으로 검토 및 수락하고 계속해서 다시 연결합니다. 그러나 하나의 디바이스에만 다시 연결하는 경우 CDO는 계속해서 다시 연결하려면 인증서를 수동으로 검토하고 수락하라는 메시지를 표시합니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** 디바이스를 찾으려면 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

필터를 사용하여 연결 상태가 "unreachable(연결할 수 없음)"인 디바이스를 찾습니다.

단계 **4** 필터링된 결과에서 다시 연결을 시도할 디바이스를 선택합니다.

단계 **5** **Reconnect(**다시 연결**)** 을 클릭합니다. CDO는 선택한 모든 디바이스에 적용할 수 있는 작업에 대해서만 명령 버튼을 제공합니다.

단계 **6** 알림 탭에서 대량 디바이스 다시 연결 작업의 진행 상황을 확인합니다. 대량 디바이스 다시 연결 작업의 성공 또는 실패에 대한 자세한 내용을 보려면 파란색 Review(검토) 링크를 클릭합니다. 그러면 작업 페이지, on page 379로 이동합니다.

**Tip** 디바이스의 인증서 또는 자격 증명이 변경되어 재연결 실패가 발생한 경우, 해당 디바이스에 개별적으로 다시 연결하여 새 자격 증명을 추가하고 새 인증서를 수락해야 합니다.

# 테넌트 간 디바이스 이동

디바이스를 CDO 테넌트에 온보딩하면 한 CDO 테넌트 간에 디바이스를 마이그레이션할 수 없습니다. 디바이스를 새 테넌트로 이동하려면 이전 테넌트에서 디바이스를 제거하고 새 테넌트에 다시 온보딩해야 합니다.

# 디바이스 메모 작성

이 절차를 사용하여 디바이스에 대한 단일 일반 텍스트 메모 파일을 생성합니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 메모를 작성할 디바이스 또는 모델을 선택합니다.

단계 **5** 오른쪽의 **Management(**관리**)** 창에서 **Notes(**메모**)**를 클릭합니다. Notes.

단계 **6** 오른쪽의 편집기 버튼을 클릭하고 기본 텍스트 편집기, Vim 또는 Emacs 텍스트 편집기를 선택합니다.

단계 **7** 메모 페이지를 편집합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.
메모가 탭에 저장됩니다.

# 재고 목록 페이지 정보 보기

**Inventory(**재고 관리**)** 페이지에는 모든 물리적 및 가상 온보딩된 디바이스와 온보딩된 디바이스에서 생성된 템플릿이 표시됩니다. 이 페이지는 유형에 따라 디바이스 및 템플릿을 분류하고 각 디바이스 유형 전용 해당 탭에 표시합니다. 검색 기능을 사용하거나 필터를 적용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다.

이 페이지에서 다음 세부 정보를 볼 수 있습니다.

- **Device(**디바이스**)** 탭에는 CDO에 온보딩된 모든 라이브 디바이스가 표시됩니다.
- **Templates(**템플릿**(**에는 CDO로 가져온 라이브 디바이스 또는 구성 파일에서 생성된 모든 템플릿 디바이스가 표시됩니다.

# 레이블 및 필터링

레이블은 디바이스 또는 개체를 그룹화하는 데 사용됩니다. 온보딩 중에 또는 온보딩 후에 언제든지 하나 이상의 디바이스에 레이블을 적용할 수 있습니다. 개체를 생성한 후 개체에 레이블을 적용할 수 있습니다. 디바이스 또는 개체에 레이블을 적용한 후에는 해당 레이블을 기준으로 디바이스 테이블 또는 개체 테이블의 내용을 필터링할 수 있습니다.

참고 디바이스에 적용된 레이블은 연결된 개체로 확장되지 않으며, 공유 개체에 적용된 레이블은 연결된 개체로 확장되지 않습니다.

"group name:label" 구문을 사용하여 레이블 그룹을 생성할 수 있습니다. 예를 들어 Region:East 또는 Region:West입니다. 이 두 레이블을 생성하는 경우 그룹 레이블은 Region(지역)이 되며 해당 그룹의 East(동부) 또는 West(서부) 중에서 선택할 수 있습니다.

# 디바이스 및 개체에 레이블 적용

디바이스에 레이블을 적용하려면 다음 단계를 수행하십시오.

단계 **1** 디바이스에 레이블을 추가하려면 왼쪽 탐색 창에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다. 개체에 레이블을 추가하려면 왼쪽 탐색 창에서 **Objects(**개체**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 생성된 테이블에서 하나 이상의 디바이스 또는 모델을 선택합니다.

단계 **5** 오른쪽의 **Add Groups and Labels(**그룹 및 레이블 추가**)** 필드에서 디바이스의 레이블을 지정합니다.

단계 **6** 파란색 + 아이콘을 클릭합니다.

# 필터

**Inventory(**재고 목록**)** 및 **Objects(**개체**)** 페이지에서 다양한 필터를 사용하여 원하는 디바이스 및 개체를 찾을 수 있습니다.

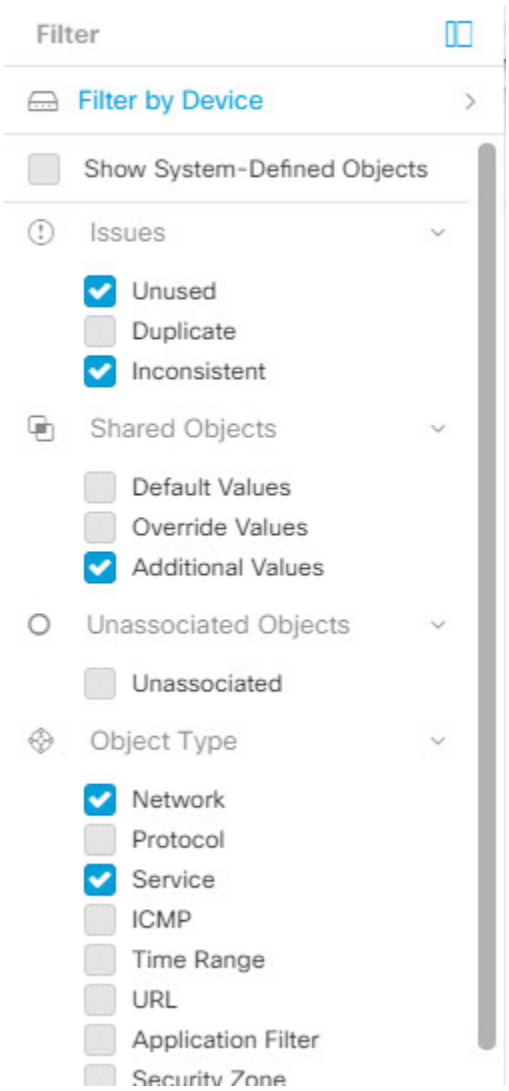
필터링하려면 Devices and Services(디바이스 및 서비스), Policies(정책) 및 Objects(개체) 탭의 왼쪽 창에서 을 클릭합니다.

Inventory(재고 목록) 필터를 사용하면 디바이스 유형, 하드웨어 및 소프트웨어 버전, snort 버전, 구성 상태, 연결 상태, 충돌 탐지, 보안 디바이스 커넥터 및 레이블을 기준으로 필터링할 수 있습니다. 필터를 적용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다. 필터를 사용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다.

개체 필터를 사용하면 디바이스, 문제 유형, 공유 개체, 연결되지 않은 개체 및 개체 유형을 기준으로 필터링할 수 있습니다. 결과에 시스템 개체를 포함하거나 포함하지 않을 수 있습니다. 또한 검색 필드를 사용하여 필터 결과에서 특정 이름, IP 주소 또는 포트 번호를 포함하는 개체를 검색할 수 있습니다.

디바이스 및 개체를 필터링할 때 검색 용어를 결합하여 몇 가지 잠재적 검색 전략을 생성하여 관련 결과를 찾을 수 있습니다.

다음 예제에서는 "문제(사용되었거나 일관성 없음)" 및 추가 값이 있는 공유 개체 및 네트워크 또는 서비스 유형의 개체 검색에 필터를 적용합니다.




# 동일한 SDC를 사용하여 CDO에 연결하는 모든 디바이스 찾기

동일한 SDC를 사용하여 CDO에 연결하는 모든 디바이스를 식별하려면 다음 절차를 수행합니다.

단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 필터 기준이 이미 지정된 경우 Inventory(재고 목록) 테이블 상단에 있는 **clear(**지우기**)** 버튼을 클릭하여 CDO로 관리하는 모든 디바이스 및 서비스를 표시합니다.

단계 **5** 필터 버튼 을 클릭하여 필터 메뉴를 확장합니다.

단계 **6** 필터의 Secure Device Connectors(보안 디바이스 커넥터) 섹션에서 원하는 SDC의 이름을 확인합니다. Inventory(재고 목록) 테이블에는 필터에서 선택한 SDC를 통해 CDO에 연결하는 디바이스만 표시됩니다.

단계 **7** (선택 사항) 필터 메뉴에서 추가 필터를 선택하여 검색을 더욱 구체화합니다.

단계 **8** (선택 사항) 작업이 완료되면 Inventory(재고 목록) 테이블 상단에 있는 **clear(**지우기**)** 버튼을 클릭하여 CDO로 관리하는 모든 디바이스 및 서비스를 표시합니다.

# 검색

CDO는 디바이스, 개체 및 액세스 그룹을 쉽게 찾을 수 있는 강력한 검색 기능을 제공합니다. **Devices & Service(**디바이스 및 서비스**)** 공간에서 검색 창에 입력을 시작하면 검색 기준에 맞는 디바이스가 표시됩니다. 디바이스의 일부 부분 이름, IP 주소 또는 물리적 디바이스의 일련 번호를 입력하여 디바이스를 찾을 수 있습니다.

마찬가지로 **Objects(**개체**)** 공간의 검색 창을 사용하여 개체 이름의 일부를 입력하거나 IP 주소, 포트, 명명된 주소, 프로토콜의 일부를 입력하여 개체를 찾을 수 있습니다.

단계 **1** 인터페이스 상단 근처의 검색 창으로 이동합니다.

단계 **2** 검색 표시줄에 검색 기준을 입력하면 해당 결과가 표시됩니다.

# 글로벌 검색

전체 검색 기능을 사용하면 CDO에서 관리하는 장치를 빠르게 찾고 탐색할 수 있습니다.

모든 검색 결과는 선택한 인덱싱 옵션을 기반으로 합니다. 인덱싱 옵션은 다음과 같습니다.

- 전체 인덱싱 - 전체 인덱싱 프로세스를 호출해야 합니다. 이 프로세스는 시스템의 모든 장치와 개체를 검색하고 인덱싱을 호출한 후에만 검색 인덱스에 표시합니다. 전체 인덱싱을 호출하려면 관리 권한이 있어야 합니다.

  자세한 내용은 전체 인덱싱 시작, 91 페이지을 참고하십시오.

- 증분 인덱싱 - 장치 또는 개체가 추가, 수정 또는 삭제될 때마다 검색 인덱스가 자동으로 업데이트되는 이벤트 기반 인덱싱 프로세스입니다.

검색 필드에 입력하는 정보는 대소문자를 구분하지 않습니다. 다음 엔터티를 사용하여 전역 검색을 수행할 수 있습니다.

- 장치 이름 - 부분 장치 이름, URL, IP 주소 또는 범위를 지원합니다.
- 개체 유형 - 개체 이름, 개체 설명 및 구성된 값을 지원합니다.

- 정책 유형 - 정책 이름, 정책 설명, 규칙 이름 및 규칙 설명을 지원합니다.

  CDO에서 관리되는 클라우드 제공 방화벽 관리 센터 및 온프레미스 FMC는 다음 정책 유형을 지원합니다.

  - 액세스 제어 정책
  - 사전 필터 정책
  - 위협 방어 NAT 정책

검색식을 입력하면 인터페이스에 검색 결과가 표시되기 시작하므로 검색을 실행하기 위해 *Enter* 키를 누를 필요가 없습니다.

검색 결과에는 검색 문자열과 일치하는 모든 장치 및 개체가 표시됩니다. 검색 문자열이 디바이스 또는 개체보다 더 많이 일치하면 결과가 범주(디바이스, 개체 및 connected_fmc) 아래에 나타납니다.

기본적으로 검색 결과의 첫 번째 항목이 강조 표시되고 해당 항목에 대한 관련 정보가 오른쪽 창에 나타납니다. 검색 결과를 스크롤하고 항목을 클릭하면 해당 정보를 볼 수 있습니다. 항목 옆의 화살표 아이콘을 클릭하여 해당 페이지로 이동할 수 있습니다.

참고

- 전역 검색은 중복 검색 결과를 표시하지 않습니다. 개체의 경우 공유 개체의 UID는 개체 보기로 이동하는 데 사용됩니다.
- CDO에서 장치를 삭제하면, 연결된 모든 개체가 전역 검색 인덱스에서 제거됩니다.
- 정책에서 개체를 삭제하고 전체 인덱싱을 시작하기 전에 장치를 유지하면, 개체가 장치와 연결되어 있기 때문에 전역 검색 인덱스에 남아 있습니다.

# 전체 인덱싱 시작

단계 **1** 관리자 또는 슈퍼 관리자 권한이 있는 계정을 사용하여 CDO에 로그인합니다.

단계 **2** CDO 메뉴 표시줄에서 **Settings(**설정**)** > **General Settings(**일반 설정**)**를 탐색합니다.

단계 **3** 전역 검색에서 **Initiate Full Indexing(**전체 인덱싱 시작**)**을 클릭하여 인덱싱을 트리거합니다.

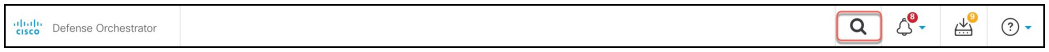

참고 전체 인덱싱을 시작하면 CDO 테넌트의 기존 인덱싱이 지워집니다.

단계 **4** 글로벌 검색 워크플로우를 보려면 **here(**여기**)**를 클릭합니다.

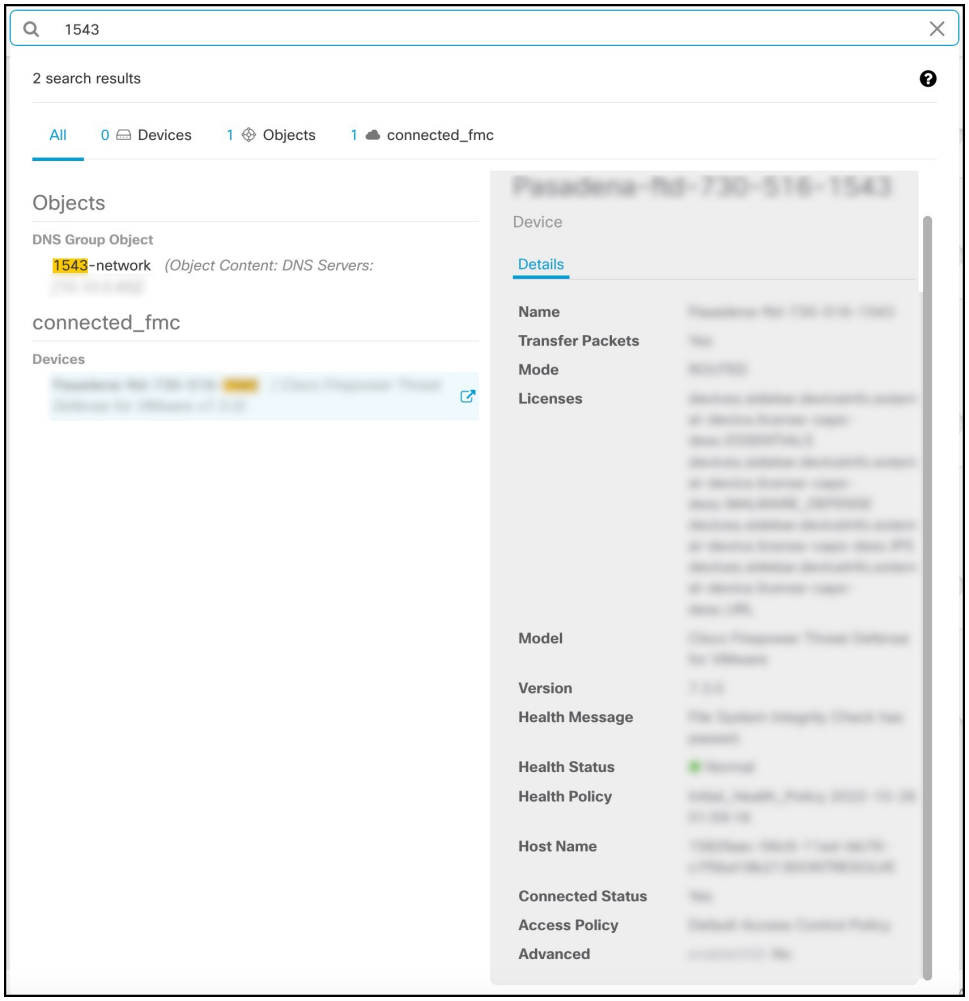
# 전역 검색 수행

단계 **1** CDO에 로그인합니다.

단계 **2** CDO 페이지 오른쪽 상단 모서리에 있는 검색 아이콘을 클릭하고 표시되는 검색 필드에 검색 문자열을 입력합니다.




검색 문자열을 입력하기 시작하면 검색 결과에 가능한 항목 목록이 표시됩니다. 검색 결과는 All, Devices, Objects 및 connected_fmc의 네 가지 범주 아래에 나타납니다. 오른쪽 창에는 선택한 검색 결과에 대한 정보가 표시됩니다.




단계 **3** 검색 결과에서 디바이스 또는 개체를 선택하고 화살표 아이콘을 클릭하여 검색 결과에서 해당 디바이스 및 개체 페이지로 이동합니다. 검색 결과에서 항목을 선택하고 화살표 아이콘을 클릭하여 검색 결과에서 해당 페이지로 이동합니다.

참고 클라우드 사용 Firewall Management Center에서 디바이스 검색 결과를 선택하면, CDO에서 클라우드 사용 Firewall Management Center 사용자 인터페이스로 이동할 수 있습니다.

클라우드 사용 Firewall Management Center에 대한 자세한 내용은 Cisco Defense Orchestrator에서 Cloud-Delivered Firewall Management Center로 Firewall Threat Defense 관리를 참조하십시오.

단계 **4** **X**를 클릭하여 검색 표시줄을 닫습니다.

# CDO 명령줄 인터페이스

CDO는 사용자에게 ASA 디바이스를 관리하기 위한 CLI(명령줄 인터페이스)를 제공합니다. 사용자는 단일 디바이스 또는 여러 디바이스에 동시에 명령을 전송할 수 있습니다.

관련 정보**:**

- 자세한 ASA CLI 설명서는 ASA 명령줄 인터페이스 설명서, on page 108의 내용을 참조하십시오.

## 명령줄 인터페이스 사용

단계 **1** **Inventory(**재고 목록**)** 페이지를 엽니다.

단계 **2** 재고 목록 테이블 위에 있는 디바이스 버튼을 클릭합니다.

단계 **3** 명령줄 인터페이스(CLI)를 사용하여 관리하려는 디바이스를 찾으려면 디바이스 탭과 필터 버튼을 사용합니다.

단계 **4** 디바이스를 선택합니다.

단계 **5** **Device Actions(**장치 작업**)** 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **6** **Command Line Interface(**명령줄 인터페이스**)** 탭을 클릭합니다.

단계 **7** 명령 창에 명령을 입력하고 **Send(**보내기**)**를 클릭합니다. 명령에 대한 디바이스의 응답은 "응답 창" 아래에 표시됩니다.

**Note** 실행할 수 있는 명령에 제한 사항이 있는 경우 해당 제한 사항은 명령 창 위에 나열됩니다.

**Related Topics**

명령줄 인터페이스에 명령 입력, 93 페이지

## 명령줄 인터페이스에 명령 입력

한 줄에 하나의 명령을 입력하거나 여러 줄에 여러 명령을 순차적으로 입력할 수 있으며 CDO는 명령을 순서대로 실행합니다. 다음 ASA 예에서는 세 개의 네트워크 개체와 해당 네트워크 개체를 포함하는 네트워크 개체 그룹을 생성하는 명령 배치를 전송합니다.


ASA장치 명령 입력: CDO는 ASA의 전역 구성 모드에서 명령을 실행합니다.

긴 명령: 매우 긴 명령을 입력하면 CDO는 API에 대해 모두 실행할 수 있도록 명령을 여러 명령으로 분할하려고 시도합니다. CDO가 명령을 적절하게 분리할 수 없는 경우 명령 목록을 구분할 위치에 대한 힌트를 묻는 메시지가 표시됩니다. 예를 들면 다음과 같습니다.

오류: CDO가 600자를 초과하는 이 명령의 일부를 실행하려고 시도했습니다. 적절한 명령 구분 지점이 어디인지에 대한 힌트를 CDO에 제공할 수 있습니다. 명령 목록 사이에 빈 행을 추가하면 됩니다.

이 오류가 표시되는 경우:

단계 **1** CLI 기록 창에서 오류를 일으킨 명령을 클릭합니다. CDO는 긴 명령 목록으로 명령 상자를 채웁니다.

단계 **2** 관련 명령 그룹 뒤에 빈 줄을 입력하여 긴 명령 목록을 편집합니다. 예를 들어 네트워크 개체 목록을 정의한 후 빈 줄을 추가하고 위의 예와 같이 그룹에 추가합니다. 명령 목록의 다양한 지점에서 이 작업을 수행할 수 있습니다.

단계 **3** **Send(**보내기**)**를 클릭합니다.

# 명령 기록 작업

CLI 명령을 보낸 후 CDO는 **Command Line Interface(**명령줄 인터페이스**)** 페이지의 기록 창에 해당 명령을 기록합니다. 기록 창에 저장된 명령을 다시 실행하거나 명령을 템플릿으로 사용할 수 있습니다.

단계 **1** **Inventory(**인벤토리**)** 페이지에서 구성할 디바이스를 선택합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **5** 아직 확장되지 않은 경우 시계 아이콘을 클릭하여 기록 창을 확장합니다.

단계 **6** 편집하거나 다시 보내려는 히스토리 창에서 명령을 Select(선택)합니다.

단계 **7** 명령 창에서 명령을 그대로 재사용하거나 편집하고 **Send(**보내기**)**를 클릭합니다. CDO는 응답 창에 명령 결과를 표시합니다.

**Note** CDO는 다음 두 가지 상황에서 응답창에 `Done!(완료!)` 메시지를 표시합니다.

- 명령이 성공적으로 실행된 후.
- 명령에 반환할 결과가 없는 경우. 예를 들어 특정 구성 항목을 검색하는 정규식과 함께 show 명령을 실행할 수 있습니다. 정규식 기준을 충족하는 구성 항목이 없는 경우 CDO는 `완료!`를 반환합니다.

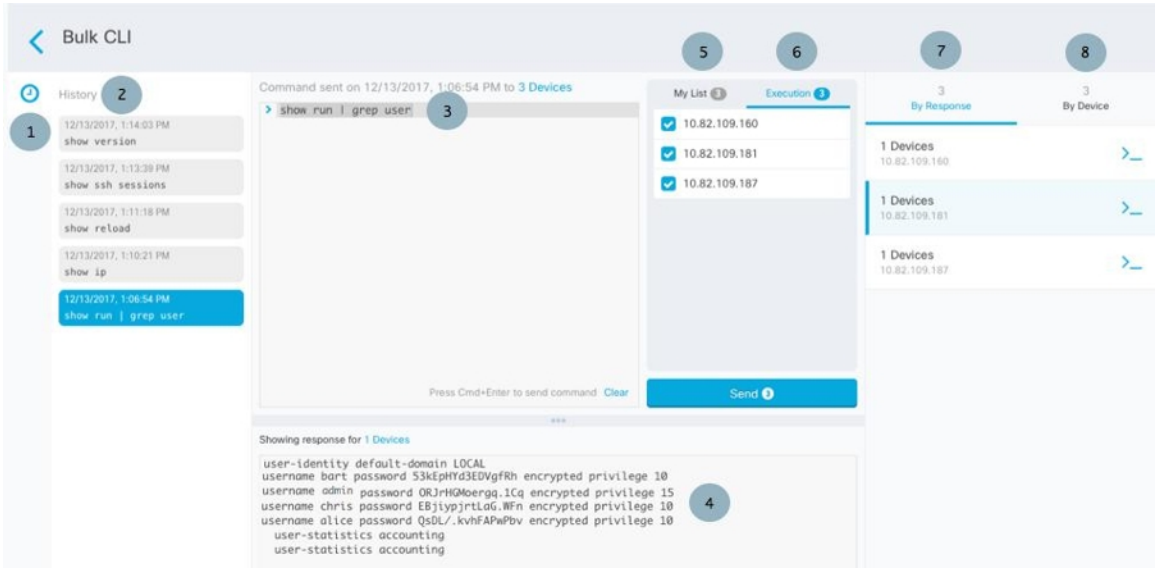
# 대량 명령줄 인터페이스

CDO는 CLI(command line interface)를 사용하여 Secure Firewall ASA, FDM 관리, 위협 방어, SSH 및 Cisco IOSSecure Firewall Cloud Native 디바이스를 관리할 수 있는 기능을 사용자에게 제공합니다. 사용자는 단일 디바이스 또는 같은 종류의 여러 디바이스에 동시에 명령을 보낼 수 있습니다. 이 섹션에서는 한 번에 여러 디바이스에 CLI 명령을 보내는 방법을 설명합니다.

관련 정보:

- ASA CLI 설명서에 대한 자세한 설명서는 ASA 명령줄 인터페이스 설명서, on page 108를 참조하십시오.

## 대량 **CLI** 인터페이스



**Note** CDO는 다음 두 가지 상황에서 **Done!(**완료**!)** 메시지를 표시합니다.

- 명령이 오류 없이 성공적으로 실행된 후.
- 명령에 반환할 결과가 없는 경우. 예를 들어 특정 구성 항목을 검색하는 정규식과 함께 show 명령을 실행할 수 있습니다. 정규식 기준을 충족하는 구성 항목이 없는 경우 CDO는 완료**!**를 반환합니다.

| 숫자 | 설명 |
|---|---|
| 1 | 시계를 클릭하여 명령 기록 창을 확장하거나 축소합니다. |
| 2 | 명령 기록. 명령을 보낸 후 CDO는 이 히스토리 창에 명령을 기록하므로 돌아가서 선택하고 다시 실행할 수 있습니다. |
| 3 | 명령 창. 이 창의 프롬프트에 명령을 입력합니다. |
| 4 | 응답 창. CDO는 명령에 대한 디바이스의 응답과 CDO 메시지를 표시합니다. 두 개 이상의 디바이스에 대한 응답이 동일한 경우 응답 창에 "X 디바이스에 대한 응답 표시"라는 메시지가 표시됩니다. X 디바이스를 클릭하면 CDO가 명령에 동일한 응답을 반환한 모든 디바이스를 표시합니다.<br>**Note** CDO는 다음 두 가지 상황에서 **Done!(**완료**!)** 메시지를 표시합니다.<br>• 명령이 오류 없이 성공적으로 실행된 후.<br>• 명령에 반환할 결과가 없는 경우. 예를 들어 특정 구성 항목을 검색하는 정규식과 함께 show 명령을 실행할 수 있습니다. 정규식 기준을 충족하는 구성 항목이 없는 경우 CDO는 완료**!**를 반환합니다. |
| 5 | **My List(**내 목록**)** 탭에는 **Inventory(**인벤토리**)** 테이블에서 선택한 디바이스가 표시되며 명령을 보낼 디바이스를 포함하거나 제외할 수 있습니다. |
| 6 | 위 그림에서 강조 표시된 **Execution(**실행**)** 탭은 히스토리 창에서 선택한 명령의 디바이스를 표시합니다. 이 예에서 show run \| grep user 명령이 기록 창에서 선택되고 실행 탭에 10.82.109.160, 10.82.109.181 및 10.82.10.9.187로 전송된 것으로 표시됩니다. |
| 7 | **By Response(**응답별**)** 탭을 클릭하면 명령에 의해 생성된 응답 목록이 표시됩니다. 동일한 응답은 한 행에 함께 그룹화됩니다. By Response(응답별) 탭에서 행을 선택하면 CDO는 응답 창에 해당 명령에 대한 응답을 표시합니다. |
| 8 | **By Device(**디바이스별**)** 탭을 클릭하면 각 디바이스의 개별 응답이 표시됩니다. 목록에서 디바이스 중 하나를 클릭하면 특정 디바이스에서 명령에 대한 응답을 볼 수 있습니다. |

# 대량 명령 전송

단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** 디바이스를 찾으려면 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 적절한 디바이스 탭을 선택하고 필터 버튼을 사용하여 명령줄 인터페이스를 사용하여 구성할 디바이스를 찾습니다.

단계 **4** 디바이스를 선택합니다.

단계 **5** **Device Actions(**장치 작업**)** 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **6** 내 목록 필드에서 명령을 보낼 디바이스를 선택하거나 선택 취소할 수 있습니다.

단계 **7** 명령 창에 명령을 입력하고 **Send(**보내기**)**를 클릭합니다. 명령 출력은 응답 창에 표시되고 명령은 변경 로그에 기록되며 CDO 명령은 대량 CLI 창의 기록 창에 명령을 기록합니다.

**Note** 명령은 동기화된 선택된 ASA 디바이스에서 성공하고 동기화되지 않은 디바이스에서는 실패할 수 있습니다. 선택한 ASA 디바이스 중 하나라도 동기화되지 않은 경우 `show`, `ping`, `traceroute`, `vpn-sessiondb`, `changeto`, `dir`, `write` 및 `copy` 명령만 허용됩니다.

# 대량 명령 기록 작업

대량 CLI 명령을 보낸 후, CDO는 대량 CLI 인터페이스 기록에 해당 명령을 기록합니다. 기록 창에 저장된 명령을 다시 실행하거나 명령을 템플릿으로 사용할 수 있습니다. 기록 창의 명령은 명령이 실행된 원래 디바이스와 연결됩니다.

단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** 디바이스를 찾으려면 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 적절한 디바이스 유형 탭을 클릭하고 필터 아이콘을 클릭하여 구성하려는 디바이스를 찾습니다.

단계 **4** 디바이스를 선택합니다.

단계 **5** **Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **6** 편집하거나 다시 보내려는 히스토리 창에서 명령을 **Select(**선택**)**합니다. 선택하는 명령은 특정 디바이스와 연결되며 반드시 첫 번째 단계에서 선택한 디바이스와 연결되지는 않습니다.

단계 **7** 내 목록 탭을 보고 전송하려는 명령이 예상하는 디바이스로 전송되는지 확인합니다.

단계 **8** 명령 창에서 명령을 편집하고 **Send(**보내기**)**를 클릭합니다. CDO는 응답 창에 명령 결과를 표시합니다.

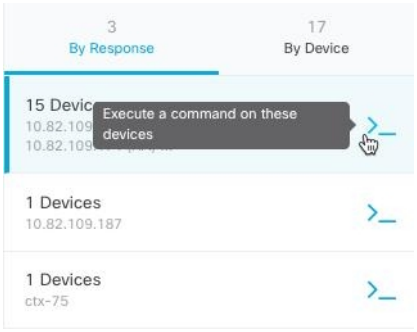
**Note** 명령은 동기화된 선택된 ASA 디바이스에서 성공하고 동기화되지 않은 디바이스에서는 실패할 수 있습니다. 선택한 ASA 디바이스 중 하나라도 동기화되지 않은 경우 `show`, `ping`, `traceroute`, `vpn-sessiondb`, `changeto`, `dir`, `write` 및 `copy` 명령만 허용됩니다.

# 대량 명령 필터 작업

대량 CLI 명령을 실행한 후 **By Resonse(**응답별**)** 필터 및 **By Device(**디바이스별**)** 필터를 사용하여 계속해서 디바이스를 구성할 수 있습니다.

## 응답 기준 필터

대량 명령을 실행한 후 CDO는 명령을 보낸 디바이스에서 반환된 응답 목록으로 **By Response(**응답별**)** 탭을 채웁니다. 응답이 동일한 디바이스는 단일 행에 통합됩니다. **By Response(**응답별**)** 탭에서 행을 클릭하면 응답 창에 디바이스의 응답이 표시됩니다. 응답 창에 두 개 이상의 디바이스에 대한 응답이 표시되면 "X 디바이스에 대한 응답 표시"라는 메시지가 표시됩니다. **X devices(X** 디바이스**)**를 클릭하면 CDO가 명령에 동일한 응답을 반환한 모든 디바이스를 표시합니다.




명령 응답과 관련된 디바이스 목록에 명령을 보내려면 다음 절차를 따르십시오.

단계 **1** **By Response(**응답별**)** 탭에서 행의 명령 기호를 클릭합니다.

단계 **2** 명령 창에서 명령을 검토하고 **Send(**보내기**)**를 클릭하여 명령을 다시 보내거나 **Clear(**지우기**)**를 클릭하여 명령 창을 지우고 디바이스로 보낼 새 명령을 입력한 다음 **Send(**보내기**)**를 클릭합니다.

단계 **3** 명령에서 받은 응답을 검토하십시오.

단계 **4** 선택한 디바이스에서 실행 중인 구성 파일이 변경 사항을 반영한다고 확신하는 경우 명령 창에 `write memory`를 입력하고 **Send(**보내기**)**를 클릭합니다. 이렇게 하면 실행 중인 구성이 시작 구성에 저장됩니다.

## 디바이스 기준 필터

대량 명령을 실행한 후 CDO는 실행 탭과 디바이스별 탭을 명령을 보낸 디바이스 목록으로 채웁니다. 디바이스별 탭에서 행을 클릭하면 각 디바이스에 대한 응답이 표시됩니다.

동일한 디바이스 목록에서 명령을 실행하려면 다음 절차를 따르십시오.

단계 **1** **By Device(**디바이스 별**)** 탭을 클릭합니다.

단계 **2** **>_Execute a command on these devices(**이 디바이스에서 명령 실행**)**를 클릭합니다.

단계 **3** **Clear(**지우기**)**를 클릭하여 명령 창을 지우고 새 명령을 입력합니다.

단계 **4** 내 목록 창에서 목록의 개별 디바이스를 선택하거나 선택 취소하여 명령을 보낼 디바이스 목록을 지정합니다.

단계 **5** **Send(**보내기**)**를 클릭합니다. 명령에 대한 응답이 응답 창에 표시됩니다. 응답 창에 두 개 이상의 디바이스에 대한 응답이 표시되면 "X 디바이스에 대한 응답 표시"라는 메시지가 표시됩니다. X 디바이스를 클릭하면 CDO가 명령에 동일한 응답을 반환한 모든 디바이스를 표시합니다.

단계 **6** 선택한 디바이스에서 실행 중인 구성 파일이 변경 사항을 반영한다고 확신하는 경우 명령 창에 `write memory`를 입력하고 **Send(**보내기**)**를 클릭합니다.

# 디바이스 관리를 위한 CLI 매크로

CLI 매크로는 즉시 사용할 수 있는 완전한 형식의 CLI 명령이거나 실행 전에 수정할 수 있는 CLI 명령의 템플릿입니다. 모든 매크로는 하나 이상의 ASA 디바이스에서 동시에 실행할 수 있습니다.

여러 디바이스에서 동일한 명령을 동시에 실행하려면 템플릿과 유사한 CLI 매크로를 사용합니다. CLI 매크로는 디바이스 구성 및 관리의 일관성을 유지합니다. 완전한 형식의 CLI 매크로를 사용하여 디바이스에 대한 정보를 가져옵니다. ASA 디바이스에서 즉시 사용할 수 있는 다양한 CLI 매크로가 있습니다.

자주 수행하는 작업을 모니터링하기 위해 CLI 매크로를 생성할 수 있습니다. 자세한 내용은 새 명령에서 CLI 매크로 생성을 참조하십시오.

CLI 매크로는 시스템 정의 또는 사용자 정의입니다. 시스템 정의 매크로는 CDO에서 제공하며 편집하거나 삭제할 수 없습니다. 사용자 정의 매크로는 사용자가 생성하며 편집하거나 삭제할 수 있습니다.

**Note** 디바이스가 CDO에 온보딩된 후에만 디바이스에 대한 매크로를 생성할 수 있습니다.

ASA를 예로 들어 ASA 중 하나에서 특정 사용자를 찾으려면 다음 명령을 실행할 수 있습니다.

```
show running-config | grep username
```

명령을 실행할 때 사용자 이름을 검색할 사용자의 사용자 이름으로 대체합니다. 이 명령으로 매크로를 만들려면 동일한 명령을 사용하고 사용자 이름을 중괄호로 묶습니다.

```
> show running-config | grep {{username}}
```

매개변수의 이름은 원하는 대로 지정할 수 있습니다. 이 매개변수 이름을 사용하여 동일한 매크로를 생성할 수도 있습니다.

```
> show running-config | grep {{username_of_local_user_stored_on_asa}}
```

매개변수 이름은 설명적일 수 있으며 영숫자 문자와 밑줄을 사용해야 합니다. 이 경우 명령 구문은

```
show running-config | grep
```

명령의 일부이며 명령을 전송하는 디바이스에 대해 적절한 CLI 구문을 사용해야 합니다.

# 새 명령에서 CLI 매크로 생성

단계 1 CLI 매크로를 생성하기 전에 CDO의 명령줄 인터페이스에서 명령을 테스트하여 명령 구문이 올바른지, 그리고 신뢰할 수 있는 결과를 반환하는지 확인합니다.

**Note**
- 자세한 ASA CLI 설명서는 ASA 명령줄 인터페이스 설명서, on page 108의 내용을 참조하십시오.

단계 2 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 3 **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 4 적절한 디바이스 유형 탭을 클릭하고 온라인 및 동기화된 디바이스를 선택합니다.

단계 5 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 6 CLI 매크로 즐겨찾기 스타 ★를 클릭하여 이미 존재하는 매크로를 확인합니다.

단계 7 더하기 버튼  을 클릭합니다.

단계 8 매크로에 고유한 이름을 지정합니다. 원하는 경우 CLI 매크로에 대한 설명 및 참고 사항을 제공합니다.

단계 9 **Command(**명령**)** 필드에 전체 명령을 입력합니다.

단계 10 명령을 실행할 때 수정하려는 명령 부분을 중괄호로 묶인 매개변수 이름으로 교체합니다.

단계 11 **Create(**생성**)**를 클릭합니다. 생성한 매크로는 처음에 지정한 디바이스뿐만 아니라 해당 유형의 모든 디바이스에서 사용할 수 있습니다.

명령을 실행하려면 CLI 매크로 실행을 참조하십시오.

# CLI 기록 또는 기존 CLI 매크로에서 CLI 매크로 생성

이 절차에서는 이미 실행한 명령, 다른 사용자 정의 매크로 또는 시스템 정의 매크로에서 사용자 정의 매크로를 생성합니다.

단계 1 탐색 모음에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

참고 CLI 기록에서 사용자 정의 매크로를 생성하려면 명령을 실행한 디바이스를 선택합니다. CLI 매크로는 동일한 계정의 디바이스 간에 공유되지만 CLI 기록은 공유되지 않습니다.

단계 2 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 3 적절한 디바이스 유형 탭을 클릭하고 온라인 및 동기화된 디바이스를 선택합니다.

단계 4 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 5 CLI 매크로를 만들려는 명령을 찾아 선택합니다. 다음 방법 중 하나를 사용합니다.

- 해당 디바이스에서 실행한 명령을 보려면 시계  를 클릭합니다. 매크로로 전환할 항목을 선택하면 명령 창에 명령이 나타납니다.

- CLI 매크로 즐겨찾기 스타 ★를 클릭하여 이미 존재하는 매크로를 확인합니다. 변경할 사용자 정의 또는 시스템 정의 CLI 매크로를 선택합니다. 명령 창에 명령이 나타납니다.

단계 **6** 명령 창의 명령을 사용하여 CLI 매크로 금색 별 ☆를 클릭합니다. 이 명령은 이제 새 CLI 매크로의 기본이 됩니다.

단계 **7** 매크로에 고유한 이름을 지정합니다. 원하는 경우 CLI 매크로에 대한 설명 및 참고 사항을 제공합니다.

단계 **8** 명령 필드에서 명령을 검토하고 원하는 대로 변경합니다.

단계 **9** 명령을 실행할 때 수정하려는 명령 부분을 중괄호로 묶인 매개변수 이름으로 교체합니다.

단계 **10** **Create(**생성**)**를 클릭합니다. 생성한 매크로는 처음에 지정한 디바이스뿐만 아니라 해당 유형의 모든 디바이스에서 사용할 수 있습니다.

명령을 실행하려면 CLI 매크로 실행을 참조하십시오.

# CLI 매크로 실행

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 적절한 디바이스 유형 탭을 클릭하고 하나 이상의 디바이스를 선택합니다.

단계 **4** **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

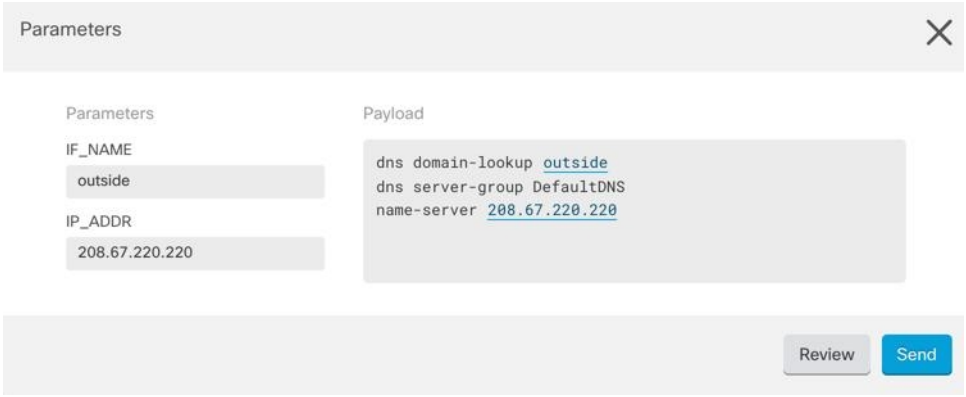
단계 **5** 명령 패널에서 별표 ★를 클릭합니다.

단계 **6** 명령 패널에서 CLI 매크로를 선택합니다.

단계 **7** 다음 두 가지 방법 중 하나로 매크로를 실행합니다.

- 매크로에 정의할 매개변수가 없는 경우 **Send(**전송**)**를 클릭합니다. 명령에 대한 응답이 응답 창에 나타납니다. 다 됐습니다.
- 아래의 Configure DNS 매크로와 같은 매개변수가 매크로에 포함된 경우 **>_ View Parameters(**매개변수 보기**)**를 클릭합니다.


단계 **8** Parameters(매개변수) 창의 Parameters(매개변수) 필드에 매개변수 값을 입력합니다.




단계 **9** **Send(**보내기**)**를 클릭합니다. CDO가 성공적으로 명령을 전송하고 디바이스의 구성을 업데이트하면 완료됩니다!

- ASA의 경우 실행 중인 구성이 업데이트됩니다.

단계 **10** 명령을 전송한 후 "일부 명령이 실행 중인 구성을 변경했을 수 있습니다."라는 메시지와 함께 두 개의 링크가 표시될 수 있습니다.


- **Write to Disk(**디스크에 쓰기**)**를 클릭하면 이 명령의 변경 사항과 실행 중인 구성의 다른 모든 변경 사항이 디바이스의 시작 구성에 저장됩니다.
- **Dismiss(**해제**)**를 클릭하면 메시지가 사라집니다.

# CLI 매크로 편집

사용자 정의 CLI 매크로는 편집할 수 있지만 시스템 정의 매크로는 편집할 수 없습니다. CLI 매크로를 수정하면 모든 ASA 디바이스에 대해 변경됩니다. 매크로는 특정 디바이스에 한정되지 않습니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.
단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.
단계 **3** 해당 디바이스 탭을 클릭합니다.
단계 **4** 디바이스를 선택합니다.
단계 **5** **Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.
단계 **6** 편집할 사용자 정의 매크로를 선택합니다.
단계 **7** 매크로 레이블에서 편집 아이콘을 클릭합니다.
단계 **8** Edit Macro(매크로 편집) 대화 상자에서 CLI 매크로를 편집합니다.
단계 **9** **Save(**저장**)**를 클릭합니다.

CLI 매크로를 실행하는 방법에 대한 지침은 CLI 매크로 실행를 참조하십시오.

## CLI 매크로 삭제

사용자 정의 CLI 매크로는 삭제할 수 있지만 시스템 정의 매크로는 삭제할 수 없습니다. CLI 매크로를 삭제하면 모든 디바이스에서 삭제됩니다. 매크로는 특정 디바이스에 한정되지 않습니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.
단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.
단계 **3** 해당 디바이스 탭을 클릭합니다.
단계 **4** 디바이스를 선택합니다.
단계 **5** **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.
단계 **6** 삭제할 사용자 정의 CLI 매크로를 선택합니다.
단계 **7** CLI 매크로 레이블에서 휴지통 아이콘를 클릭합니다.
단계 **8** CLI 매크로를 제거할지 확인합니다.

# CLI를 사용한 ASA 구성

CDO에서 제공하는 CLI 인터페이스에서 CLI 명령을 실행하여 ASA 디바이스를 구성할 수 있습니다. 인터페이스를 사용하려면 **Devices & Services(**디바이스 및 서비스**)** 메뉴에서 디바이스를 선택하고 **Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다. 자세한 내용은 CDO 명령줄 인터페이스 사용을 참조하십시오.

### 새 로깅 서버 추가

시스템 로깅은 디바이스의 메시지를 syslog 데몬을 실행 중인 서버로 수집하는 방식입니다. 중앙 syslog 서버에 로깅하면 로그와 경고를 종합하는 데 도움이 됩니다.

자세한 내용은 실행 중인 ASA 버전의 CLI 책 1: Cisco ASA 시리즈 일반 작업 CLI 구성 가이드에서 '로깅' 장의 '모니터링' 섹션을 참조하십시오.

### DNS 서버 구성

ASA에서 호스트 이름의 IP 주소를 확인할 수 있도록 DNS 서버를 구성해야 합니다. 또한 액세스 규칙에서 FQDN(Fully Qualified Domain Name) 네트워크 개체를 사용하려면 DNS 서버를 구성해야 합니다.

자세한 내용은 실행 중인 ASA 버전의 CLI 책 1: Cisco ASA 시리즈 일반 작업 CLI 구성 가이드에서 'DNS 서버 구성' 섹션의 '기본 설정' 장을 참조하십시오.

정적 및 기본 경로 추가

비연결 호스트 또는 네트워크에 트래픽을 라우팅하려면 정적 또는 동적 라우팅을 사용하여 해당 호스트 또는 네트워크로 가는 경로를 정의해야 합니다.

자세한 내용은 CLI 책 1: Cisco ASA 시리즈 일반 작업 CLI 구성 가이드의 '정적 및 기본 경로' 장을 참조하십시오.

인터페이스 구성

CLI 명령을 사용하여 관리 및 데이터 인터페이스를 구성할 수 있습니다. 자세한 내용은 CLI 책 1: Cisco ASA 시리즈 일반 작업 CLI 구성 가이드의 '기본 인터페이스 구성' 장을 참조하십시오.

# ASA 구성 비교

이 절차를 사용하여 두 ASA의 구성을 비교합니다.

단계 1 탐색 메뉴에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 2 **Devices(**장치**)** 탭을 클릭하여 ASA 디바이스를 찾거나 **Templates(**템플릿**)**탭을 클릭하여 ASA 모델 디바이스를 찾습니다.

단계 3 **ASA** 탭을 클릭합니다.

단계 4 비교하려는 디바이스에 대한 디바이스 목록을 필터링합니다.

단계 5 두 개의 ASA를 선택합니다. 상태는 중요하지 않습니다. Defense Orchestrator에 저장된 ASA의 구성을 비교하고 있습니다.

단계 6 오른쪽의 디바이스 작업 창에서 **Compare(**비교**)**를 클릭합니다.

단계 7 구성 비교 대화 상자에서 **Next(**다음**)** 및 **Previous(**이전**)**를 클릭하여 구성 파일에서 파란색으로 강조 표시된 차이점을 건너뜁니다.

# ASA 대량 CLI 사용 사례

ASA 디바이스에 CDO의 대량 CLI 기능을 사용할 때 발생할 수 있는 워크플로우는 다음과 같습니다.

## ASA의 실행 중인 구성에 있는 모든 사용자를 표시한 다음 사용자 중 한 명 삭제

단계 1 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 2 **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 3 **ASA** 탭을 클릭합니다.

단계 **4** 사용자를 삭제하려는 디바이스의 디바이스 목록을 검색 및 필터링하고 선택합니다.

**Note** 선택한 디바이스가 동기화되었는지 확인합니다. 디바이스가 동기화되지 않은 경우 `show`, `ping`, `traceroute`, `vpn-sessiondb`, `changeto`, `dir`, `copy` 및 `write` 명령만 허용됩니다.

단계 **5** 세부 정보 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다. CDO는 내 목록 창에서 선택한 디바이스를 나열합니다. 더 적은 수의 디바이스에 명령을 보내기로 결정한 경우 해당 목록에서 디바이스를 선택 취소하십시오.

단계 **6** 명령 창에서 `show run | grep user`를 입력하고 **Send(**보내기**)**를 클릭합니다. 사용자 문자열을 포함하는 실행 중인 구성 파일의 모든 줄이 응답 창에 표시됩니다. 실행 탭이 열리고 명령이 실행된 디바이스가 표시됩니다.

단계 **7** By Response(응답별) 탭을 클릭하고 응답을 검토하여 삭제할 사용자가 있는 디바이스를 결정합니다.

단계 **8** 내 목록 탭을 클릭하고 사용자를 삭제할 디바이스 목록을 선택합니다.

단계 **9** 명령 창에서 no 형식의 user 명령을 입력하여 user2를 삭제한 다음 **Send(**보내기**)**를 클릭합니다. 이 예에서는 user2를 삭제합니다.

```
no user user2 password reallyhardpassword privilege 10
```

단계 **10** 사용자 이름을 검색하는 데 사용한 `show run | grep user` 명령 인스턴스에 대한 히스토리 패널을 찾습니다. 해당 명령을 선택하고 실행 목록에서 디바이스 목록을 확인한 다음 **Send(**보내기**)**를 선택합니다. 지정한 디바이스에서 사용자 이름이 삭제된 것을 볼 수 있습니다.

단계 **11** 실행 중인 구성에서 올바른 사용자를 삭제했고 올바른 사용자가 실행 중인 구성에 남아 있는 것에 만족하는 경우 다음을 수행합니다.

**a.** 히스토리 창에서 `no user user2 password reallyhardpassword privilege 10` 명령을 선택합니다.

**b.** **By Device(**디바이스 별**)** 탭을 클릭하고 이 디바이스에서 명령 실행를 클릭합니다.

**c.** 명령 창에서 **Clear(**지우기**)**를 클릭하여 명령 창을 지웁니다.

**d.** `배포 메모리` 명령을 입력하고 **Send(**보내기**)**를 클릭합니다.

# 선택한 ASA에서 모든 SNMP 구성 찾기

이 절차는 ASA의 실행 중인 구성에 있는 모든 SNMP 구성 항목을 보여줍니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 **3** **ASA** 탭을 클릭합니다.

단계 **4** 실행 중인 구성에서 SNMP 구성을 분석하려는 디바이스를 필터링 및 검색하고 선택합니다.

**Note** 선택한 디바이스가 동기화되었는지 확인합니다. 디바이스가 동기화되지 않은 경우 `show`, `ping`, `traceroute`, `vpn-sessiondb`, `changeto`, 및 `dir` 명령만 허용됩니다.

단계 **5** 세부 정보 창에서 **Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다. 디바이스는 내 목록 창에서 선택한 디바이스를 나열합니다. 더 적은 수의 디바이스에 명령을 보내기로 결정한 경우 해당 목록에서 디바이스를 선택 취소하십시오.

단계 **6** 명령 창에서 `show run | grep snmp`를 입력하고 **Send(**보내기**)**를 클릭합니다. snmp 문자열을 포함하는 실행 중인 구성 파일의 모든 줄이 응답 창에 표시됩니다. 실행 탭이 열리고 명령이 실행된 디바이스가 표시됩니다.

단계 **7** 응답 창에서 명령 출력을 검토합니다.

# Secure Firewall ASA 구성 복원 정보

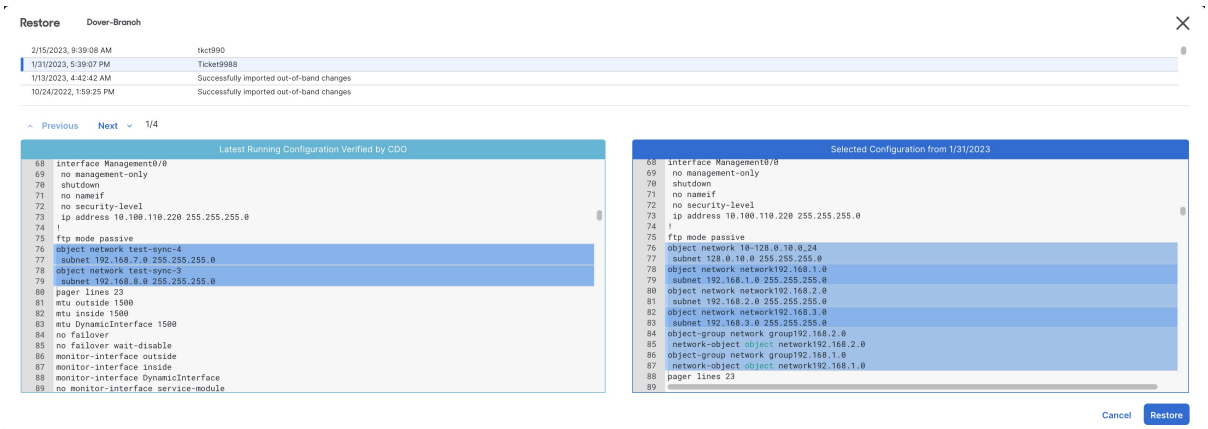
ASA의 구성을 변경하고, 변경 사항을 되돌리고자 하는 경우ASA의 과거 구성을 복원할 수 있습니다. 이는 예기치 않거나 원치 않는 결과를 초래한 구성 변경 사항을 편리하게 제거할 수 있는 방법입니다.

## ASA 구성 복원 정보

구성을 복원하기 전에 다음 참고 사항을 검토합니다.

- CDO는 복원하도록 선택한 구성을 ASA에 배포된 마지막으로 알려진 구성과 비교하지만, 복원하도록 선택한 구성을 준비되었지만 ASA에 배포되지 않은 구성과 비교하지 않습니다. ASA에 배포되지 않은 변경 사항이 있고 과거 구성을 복원하는 경우, 복원 프로세스는 배포되지 않은 변경 사항을 덮어쓰게 되며 해당 변경 사항은 손실됩니다.
- 과거 구성을 복원하기 전에, ASA이 동기화됨 또는 동기화되지 않음 상태일 수 있지만 디바이스가 충돌 감지됨 상태인 경우 과거 구성을 복원하기 전에 충돌을 해결해야 합니다.
- 과거 구성을 복원하면 배포된 모든 중간 구성 변경 사항을 덮어씁니다. 예를 들어 아래 목록에서 2023년 1월 31일의 구성을 복원하면 2023년 2월 15일에 이루어진 구성 변경 사항을 덮어씁니다.
- 다음 및 이전 버튼을 클릭하면 구성 파일을 통해 이동하고 구성 파일 변경 사항을 강조 표시합니다.
- 원래 구성 변경에 변경 요청 레이블을 적용한 경우 해당 레이블이 구성 복원 목록에 나타납니다.

***Figure 3: ASA*** 복원 구성 화면



구성 변경 사항은 얼마 동안 유지됩니까?

1년 이하의 ASA 구성을 복원할 수 있습니다. CDO는 변경 로그에 기록된 구성 변경 사항을 복원합니다. 변경 로그는 ASA에 구성 변경 사항을 쓰거나 읽을 때마다 변경 사항을 기록합니다. CDO는 1년치 변경 로그를 저장하며, 이전 연도 내에 수행된 백업 수에는 제한이 없습니다.

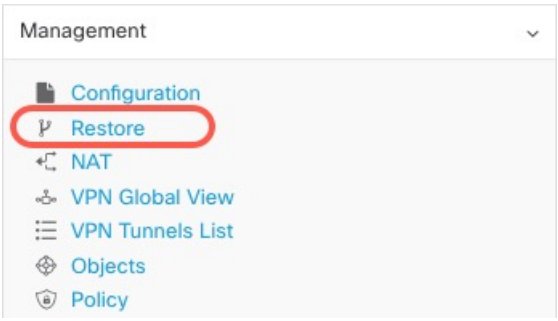
# Secure Firewall ASA 구성 복원

단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

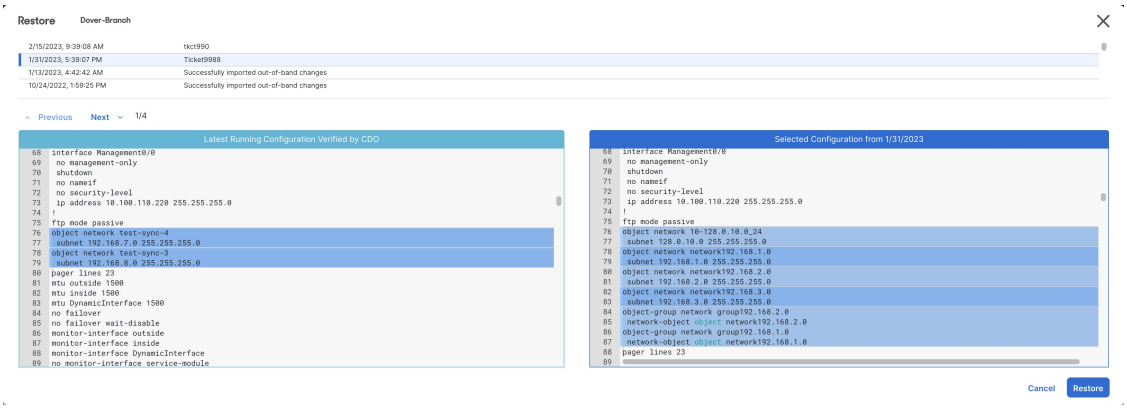
단계 **2** ASA 탭을 클릭합니다.

단계 **3** 복원하려는 ASA 구성을 선택합니다.

단계 **4** **Management(**관리**)** 창에서, **Restore(**복원**)**를 클릭합니다.




단계 **5** **Restore(**복원**)** 페이지에서 되돌리려는 구성을 선택합니다.




예를 들어 위 그림에서 2023년 1월 31일의 구성이 선택되었습니다.

단계 **6** "CDO에서 확인한 최신 실행 구성"과 "<날짜>에서 선택한 구성"을 비교하여 <날짜>에서 선택한 구성 창에 표시된 구성을 복원할 것인지 확인합니다. 이전 및 다음을 사용하여 모든 변경 사항을 비교합니다.

단계 **7** **Restore(**복원**)**을 클릭하면 CDO에서 구성이 준비됩니다. **Inventory(**재고 관리**)** 페이지에서 디바이스의 구성 상태가 이제 "동기화되지 않음"임을 알 수 있습니다.

단계 **8** 우측 창에서 **Deploy Changes...(**변경 사항 배포...**)**를 클릭하여 변경 사항을 배포하고 ASA를 동기화합니다.

## 문제 해결

잃어버렸지만 유지하고 싶었던 변경 사항을 복원하려면 어떻게 해야 합니까?

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.
단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.
단계 **3** ASA 탭을 클릭합니다.
단계 **4** 필요한 디바이스를 선택합니다.
단계 **5** 오른쪽 창에서 **Change Log(**로그 변경**)**를 클릭합니다.
단계 **6** 변경 로그에서 변경 사항을 검토합니다. 해당 레코드에서 손실된 구성을 재구성할 수 있습니다.

# ASA 명령줄 인터페이스 설명서

CDO는 ASA 명령줄 인터페이스를 완벽하게 지원합니다. Cisco에서는 사용자가 단일 디바이스 및 여러 디바이스에 ASA 명령을 동시에 전송할 수 있도록 CDO 내에서 터미널과 유사한 인터페이스를 제공합니다. ASA 명령줄 인터페이스 설명서는 광범위합니다. CDO 설명서의 일부를 다시 작성하는 대신 Cisco.com의 ASA CLI 설명서에 대한 포인터를 제공합니다.

### ASA 명령줄 인터페이스 구성 가이드

ASA 버전 9.1부터는 ASA CLI 구성 가이드가 3개의 별도 책으로 구성됩니다.

- CLI Book 1: Cisco ASA Series 일반 운영 CLI 환경 설정 가이드
- CLI Book 2: Cisco ASA Series Firewall CLI 환경 설정 가이드
- CLI Book 3: Cisco ASA Series VPN CLI 구성 가이드

Cisco.com에서 Support(지원) > Products by Category(제품) > Security(보안) > Firewalls(방화벽) > ASA 5500(구성) > Configuration Guides(구성 가이드)로 이동하여 ASA CLI 구성 가이드에 도달할 수 있습니다.

### 몇 가지 특정 ASA 명령줄 인터페이스 구성 가이드 섹션

**show** 및 **more** 명령 출력 필터링 정규식을 사용하여 show 명령 출력을 필터링하는 자세한 내용은 CLI 설명서 1: Cisco ASA 시리즈 일반 운영 CLI 구성 가이드의 show 및 more 명령 출력 필터링에서 확인할 수 있습니다.

### ASA 명령 참조

ASA 명령 참조 가이드에는 모든 ASA 명령 및 해당 옵션이 알파벳순으로 나열되어 있습니다. ASA 명령 참조는 버전과 관련이 없습니다. 다음의 네 가지 책으로 게시됩니다.

- Cisco ASA Series 명령 참조, A - H 명령

- Cisco ASA Series 명령 참조, I - R 명령
- Cisco ASA Series 명령 참조, S 명령
- Cisco ASA Series 명령 참조, T - Z 명령 및 ASASM에 대한 IOS 명령

Cisco.com에서 Support(지원) > Products by Category(범주별 제품) > Security(보안) > Firewalls(방화벽) > ASA 5500(ASA 5500) > Reference Guides(참조 가이드) > Command References(명령 참조) > ASA Command References(ASA 명령 참조)로 이동하여 ASA 명령 참조 가이드로 이동할 수 있습니다.

# ASA, Cisco Secure Firewall Cloud Native, 및 Cisco IOS 장치 구성 파일

ASA, Secure Firewall Cloud Native및 Cisco IOS디바이스와 같은 일부 유형의 디바이스는 해당 구성을 단일 파일에 저장합니다. 이러한 디바이스의 경우 Cisco Defense Orchestrator에서 구성 파일을 보고 다양한 작업을 수행할 수 있습니다.

## 디바이스의 구성 파일 보기

ASA, Secure Firewall Cloud Native, SSH 관리 디바이스 및 Cisco IOS를 실행하는 디바이스와 같이 단일 구성 파일에 전체 구성을 저장하는 디바이스의 경우 CDO를 사용하여 구성 파일을 볼 수 있습니다.

참고 SSH 관리 디바이스 및 Cisco IOS 디바이스에는 읽기 전용 구성이 있습니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 보려는 구성이 있는 디바이스 또는 모델을 선택합니다.

단계 **5** 오른쪽의 관리 창에서 **Configuration(**구성**)**를 클릭합니다.
전체 구성 파일이 표시됩니다.

관련 정보**:**

- 전체 디바이스 구성 파일 편집

# 전체 디바이스 구성 파일 편집

일부 디바이스 유형은 ASA와 같은 단일 구성 파일에 구성을 저장합니다. 이러한 디바이스의 경우 CDO에서 디바이스 구성 파일을 보고 디바이스에 따라 다양한 작업을 수행할 수 있습니다.

현재 ASA 구성 파일만 CDO를 사용하여 직접 편집할 수 있습니다.

⚠

**Caution** 이 절차는 디바이스 구성 파일의 구문에 익숙한 고급 사용자를 위한 것입니다. 이 방법은 Defense Orchestrator에 저장된 구성 파일의 복사본을 직접 변경합니다.

## 절차

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** **ASA** 탭을 클릭합니다.

단계 **4** 구성을 편집하려는 디바이스를 선택합니다.

단계 **5** 오른쪽의 관리 창에서 **Configuration(**구성**)**를 클릭합니다.

단계 **6** **Device Configuration(**디바이스 구성**)** 페이지에서 **Edit(**편집**)**를 클릭합니다.

단계 **7** 오른쪽의 편집기 버튼을 클릭하고 기본 텍스트 편집기, **Vim** 또는 **Emacs** 텍스트 편집기를 선택합니다.

단계 **8** 파일을 편집하고 변경 사항을 저장합니다.

단계 **9** **Devices & Services(**디바이스 및 서비스**)** 페이지로 돌아가 변경 사항을 미리 보고 배포합니다.

# CLI 명령 결과 내보내기

독립형 디바이스 또는 여러 디바이스에 실행된 CLI 명령의 결과를 쉼표로 구분된 값(.csv) 파일로 내보내 원하는 대로 정보를 필터링하고 정렬할 수 있습니다. 단일 디바이스 또는 여러 디바이스의 CLI 결과를 한 번에 내보낼 수 있습니다. 내보낸 정보에는 다음이 포함됩니다.

- 디바이스
- 날짜
- 사용자
- 명령
- 출력

# CLI 명령 결과 내보내기

명령 창에서 방금 실행한 명령의 결과를 .csv 파일로 내보낼 수 있습니다.

단계 1 탐색 모음에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 2 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 디바이스를 선택하여 강조 표시하십시오.

단계 5 디바이스에 대한 **Device Actions(**디바이스 작업**)** 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 6 명령줄 인터페이스 창에서 명령을 입력하고 **Send(**보내기**)**를 클릭하여 디바이스에 명령을 실행합니다.

단계 7 입력된 명령 창 오른쪽에서 내보내기 아이콘 를 클릭합니다.

단계 8 .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다. .csv 파일에서 명령 출력을 읽을 때 모든 셀을 확장하여 명령의 모든 결과를 확인합니다.

# CLI 매크로의 결과 내보내기

명령 창에서 실행된 매크로의 결과를 내보낼 수 있습니다. 하나 이상의 디바이스에서 실행된 CLI 매크로의 결과를 .csv 파일로 내보내려면 다음 절차를 따르십시오.

단계 1 **Devices & Services(**디바이스 및 서비스**)** 페이지를 엽니다.

단계 2 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 디바이스를 선택하여 강조 표시하십시오.

단계 5 디바이스에 대한 **Device Actions(**디바이스 작업**)** 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 6 CLI 창의 왼쪽 창에서 CLI 매크로 즐겨찾기 별표 를 선택합니다.

단계 7 내보낼 매크로 명령을 클릭합니다. 적절한 매개변수를 입력하고 **Send(**보내기**)**를 클릭합니다.

단계 8 입력된 명령 창 오른쪽에서 내보내기 아이콘 를 클릭합니다.

단계 9 .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다. .csv 파일에서 명령 출력을 읽을 때 모든 셀을 확장하여 명령의 모든 결과를 확인합니다.

# CLI 명령 기록 내보내기

다음 절차를 사용하여 하나 또는 여러 디바이스의 CLI 기록을 .csv 파일로 내보냅니다.

단계 1 탐색 창에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.
단계 2 **Devices(**디바이스**)** 탭을 클릭합니다.
단계 3 해당 디바이스 탭을 클릭합니다.
단계 4 디바이스를 선택하여 강조 표시하십시오.
단계 5 디바이스에 대한 디바이스 작업 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.
단계 6 아직 확장되지 않은 경우 시계 아이콘을 클릭하여 기록 창을 확장합니다.
단계 7 입력된 명령 창 오른쪽에서 내보내기 아이콘 를 클릭합니다.
단계 8 .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다. .csv 파일에서 명령 출력을 읽을 때 모든 셀을 확장하여 명령의 모든 결과를 확인합니다.

관련 정보**:**

- CDO 명령줄 인터페이스, on page 93
- 새 명령에서 CLI 매크로 생성
- CLI 매크로 삭제
- CLI 매크로 편집
- CLI 매크로 실행
- ASA 대량 CLI 사용 사례
- ASA 명령줄 인터페이스 설명서
- 대량 명령줄 인터페이스

# CLI 매크로 목록 내보내기

명령 창에서 실행된 매크로만 내보낼 수 있습니다. 다음 절차를 사용하여 하나 이상의 디바이스의 CLI 매크로를 .csv 파일로 내보냅니다.

단계 1 탐색 창에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.
단계 2 **Devices(**디바이스**)** 탭을 클릭합니다.
단계 3 해당 디바이스 탭을 클릭합니다.
단계 4 디바이스를 선택하여 강조 표시하십시오.
단계 5 디바이스에 대한 디바이스 작업 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.
단계 6 CLI 창의 왼쪽 창에서 CLI 매크로 즐겨찾기 별표를 선택합니다.
단계 7 내보낼 매크로 명령을 클릭합니다. 적절한 매개변수를 입력하고 **Send(**보내기**)**를 클릭합니다.
단계 8 입력된 명령 창 오른쪽에서 내보내기 아이콘 를 클릭합니다.

단계 **9** .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다.

# 개체

개체는 하나 이상의 보안 정책에서 사용할 수 있는 정보의 컨테이너입니다. 개체를 사용하면 정책 일관성을 쉽게 유지할 수 있습니다. 단일 개체를 만들고 다른 정책을 사용하고 개체를 편집할 수 있으며 해당 변경 사항은 개체를 사용하는 모든 정책에 전파됩니다. 개체가 없는 경우 동일한 변경이 필요한 모든 정책을 개별적으로 편집해야 합니다.

디바이스를 온보딩하면, CDO는 해당 디바이스에서 사용하는 모든 개체를 인식하고, 저장한 다음, **Objects(**개체**)** 페이지에 나열합니다. **Objects(**개체**)** 페이지에서 기존 개체를 편집하고 보안 정책에 사용할 새 개체를 생성할 수 있습니다.

CDO은 여러 디바이스에서 사용되는 개체를 **shared object(**공유 개체**)**라고 부르고 **Objects(**개체**)** 페이지에서 이 배지로 식별합니다.

때때로 공유 개체는 일부 "문제"를 발생시키고 더 이상 여러 정책 또는 디바이스에서 완벽하게 공유되지 않습니다.

- **Duplicate objects(**중복 개체**)**는 이름은 다르지만 값은 같은 동일한 디바이스에 있는 두 개 이상의 개체입니다. 이러한 개체는 일반적으로 비슷한 용도로 사용되며 다른 정책에서 사용됩니다. 중복 개체는 다음 문제 아이콘로 식별됩니다.
- **Inconsistent objects(**일관성 없는 개체**)** 는 이름은 같지만 값이 다른 두 개 이상의 디바이스에 있는 개체입니다. 때로는 사용자가 동일한 이름과 콘텐츠로 다른 구성으로 개체를 생성하지만 시간이 지남에 따라 이러한 개체의 값이 달라져 불일치가 발생합니다. 일관성 없는 개체는 다음 문제 아이콘로 식별됩니다.
- 사용되지 않는 개체는 디바이스 구성에 존재하지만 다른 개체, 액세스 목록 또는 NAT 규칙에서 참조하지 않는 개체입니다. 사용되지 않는 개체는 다음 문제 아이콘로 식별됩니다.

규칙 또는 정책에서 즉시 사용할 개체를 생성할 수도 있습니다. 규칙 또는 정책과 연결되지 않은 개체를 생성할 수 있습니다. 규칙이나 정책에서 연결되지 않은 개체를 사용하는 경우, CDO는 해당 개체의 복사본을 생성하고 해당 복사본을 사용합니다.

**Objects(**개체**)** 메뉴로 이동하거나 네트워크 정책의 세부 정보에서 확인하여 CDO에 의해 관리되는 개체를 볼 수 있습니다.

CDO은 한 위치에서 지원되는 디바이스 전체에 걸쳐 네트워크 및 서비스 개체를 관리할 수 있습니다. CDO에서는 다음과 같은 방법으로 개체를 관리할 수 있습니다.

- 다양한 기준에 따라 모든 개체를 검색하고 개체 필터합니다.
- 디바이스에서 중복되거나, 사용되지 않거나, 일관성이 없는 개체를 찾고 이러한 개체 문제를 통합, 삭제 또는 해결하십시오.
- 연결되지 않은 개체를 찾아 사용하지 않는 경우 삭제합니다.
- 여러 디바이스에서 공통적인 공유 개체를 검색합니다.

- 변경 사항을 커밋하기 전에 일련의 정책 및 디바이스에 대한 개체 변경 사항의 영향을 평가합니다.
- 다양한 정책 및 디바이스와 개체 및 개체의 관계 집합을 비교합니다.
- CDO에 온보딩된 후 디바이스에서 사용 중인 개체를 캡처합니다.

온보딩된 디바이스에서 개체를 생성, 편집 또는 읽는 데 문제가 있는 경우 자세한 내용은 문제 해결 Cisco Defense Orchestrator, on page 569를 참조하십시오.

# 개체 유형

다음 표에서는 CDO를 사용하여 디바이스에 대해 생성하고 관리할 수 있는 개체에 대해 설명합니다.

***Table 3: ASA(Adaptive Security Appliance)*** 개체 유형

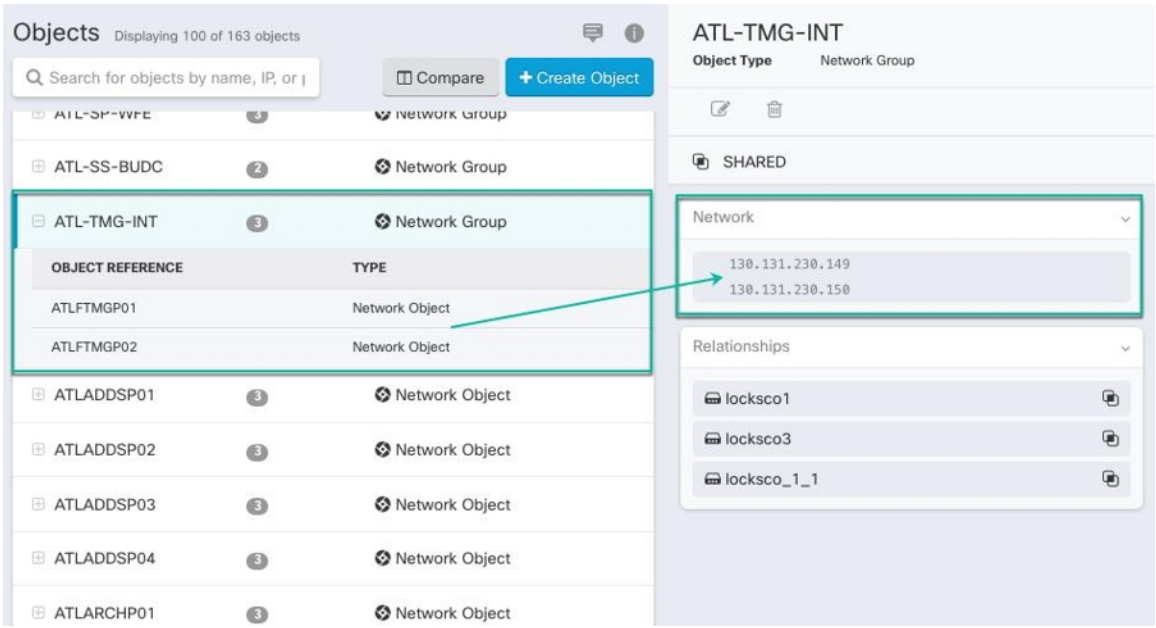
| 개체 | 설명 |
|---|---|
| IP 주소 풀 생성 | 개별 IPv4 또는 IPv6 주소 또는 IP 주소 범위와 일치하도록 주소 풀 개체를 구성할 수 있습니다. |
| RA VPN AnyConnect 클라이언트 프로파일 업로드 | AnyConnect 클라이언트 프로파일 개체는 파일 개체이며 구성(일반적으로 원격 액세스 VPN 정책)에서 사용되는 파일을 나타냅니다. AnyConnect 클라이언트 프로파일 및 AnyConnect 클라이언트 이미지 파일을 포함할 수 있습니다. |
| 네트워크 개체 | 네트워크 그룹과 네트워크 개체(네트워크 개체로 총칭함)는 호스트 또는 네트워크의 주소를 정의합니다. |
| 서비스 개체 | 서비스 개체, 서비스 그룹 및 포트 그룹은 TCP/IP 프로토콜 제품군의 일부로 간주되는 프로토콜 또는 포트를 포함하는 재사용 가능한 구성 요소입니다. |
| ASA 시간 범위 개체 | 시간 범위 개체는 특정 시간을 정의하며 시작 시간, 종료 시간, 선택 사항인 반복 항목으로 구성됩니다. 네트워크 정책에서 이 개체를 사용하여 특정 기능 또는 자산에 대한 시간 기반 액세스를 제공합니다. |
| 트러스트 포인트 개체 | 신뢰 지점을 사용하여 ASA에서 디지털 인증서를 관리하고 추적할 수 있습니다. |

# 공유 개체

CDO(Cisco Defense Orchestrator)는 이름과 콘텐츠가 동일한 여러 디바이스의 개체인 공유 개체를 호출합니다. 공유 개체는 이 아이콘으로 식별됩니다.

**Objects(**개체**)** 페이지에서 공유 개체를 사용하면 한 곳에서 개체를 수정할 수 있으며 변경 사항은 해당 개체를 사용하는 다른 모든 정책에 영향을 미치므로 정책을 쉽게 유지 관리할 수 있습니다. 공유 개체가 없으면 동일한 변경이 필요한 모든 정책을 개별적으로 수정해야 합니다.

공유 개체를 볼 때 CDO는 개체 테이블에 있는 개체의 내용을 표시합니다. 공유 개체는 정확히 동일한 내용을 갖습니다. CDO는 세부 정보 창에서 개체 요소의 결합된 보기 또는 "평평한" 보기를 보여줍니다. 세부 정보 창에서 네트워크 요소는 간단한 목록으로 병합되며 명명된 개체와 직접 연결되지 않습니다.

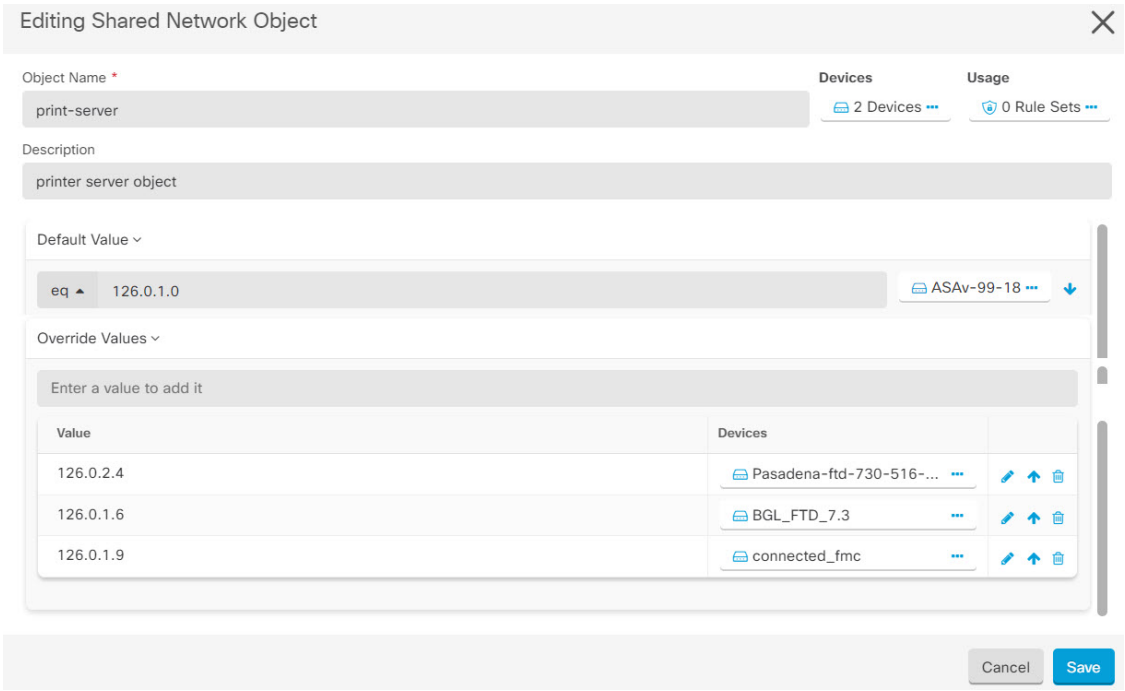



# 개체 재정의

개체 오버라이드를 사용하면 특정 디바이스에서 공유 네트워크 개체의 값을 오버라이드할 수 있습니다. CDO는 오버라이드를 구성할 때 지정한 디바이스에 해당하는 값을 사용합니다. 이름은 같지만 값이 다른 두 개 이상의 디바이스에 있는 개체에 대하여 CDO는 이러한 값이 오버라이드 되기 때문에 **Inconsistent objects(**일관성 없는 개체**)**로 식별하지 않습니다.

대부분의 디바이스에 대한 정의가 해당하는 개체를 생성하고 다른 정의가 필요한 일부 디바이스의 개체에 대한 특정 변경 사항을 지정하는 오버라이드를 사용할 수 있습니다. 모든 디바이스에 오버라이드가 필요한 개체를 생성할 수도 있습니다. 하지만 이 경우 모든 디바이스에 단일 정책을 생성할 수 있습니다. 개체 오버라이드는 필요한 경우 개별 디바이스의 정책을 바꾸지 않고도 디바이스 전반에 걸쳐 사용이 가능한 작은 공유 정책 집합을 생성하도록 합니다.

예를 들어 각 사무실에 .프린터 서버가 있고, 프린터 서버 개체인 `print-server`를 만든 시나리오를 생각해 보십시오. ACL에는 프린터 서버가 인터넷에 액세스하는 것을 거부하는 규칙이 있습니다. 프린터 서버 개체에는 한 사무실에서 다른 사무실로 변경하려는 기본값이 있습니다. 값이 다를 수 있지만 개체 오버라이드를 사용하고 규칙과 "프린터-서버" 개체를 모든 위치에서 일관되게 유지함으로써 이 작업을 수행할 수 있습니다.



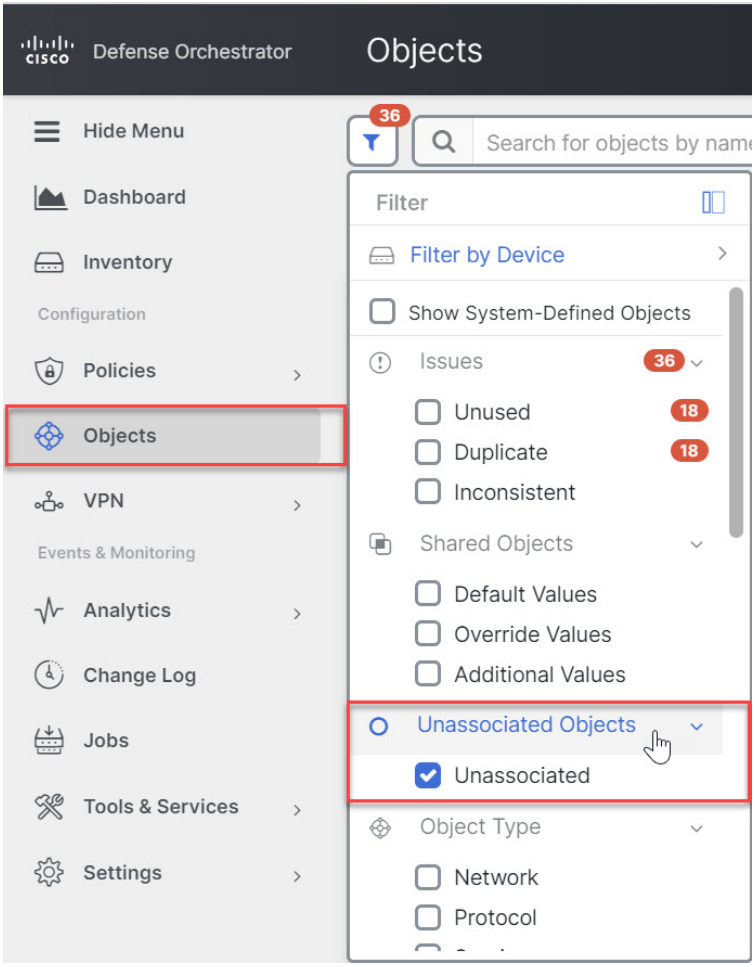

**Note** 일관되지 않은 개체가 있는 경우 오버라이드를 통해 개체를 단일 공유 개체로 결합할 수 있습니다. 자세한 내용은 불일치 개체 문제 해결, on page 575를 참조하십시오.

# 연결 해제된 개체

규칙 또는 정책에서 즉시 사용할 개체를 생성할 수 있습니다. 규칙이나 정책과 연결되지 않은 개체를 생성할 수도 있습니다. 규칙이나 정책에서 연결되지 않은 개체를 사용할 때, CDO는 해당 개체의 사본을 생성하고 해당 사본을 사용합니다. 연결되지 않은 원래 개체는 야간 유지 관리 작업에 의해 삭제되거나 사용자가 삭제할 때까지 사용 가능한 개체 목록에 남아 있습니다.

개체와 연결된 규칙 또는 정책이 실수로 삭제된 경우 모든 구성이 손실되지 않도록 연결되지 않은 개체는 사본으로 CDO에 남아 있습니다.

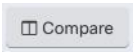
연결되지 않은 개체를 보려면 개체 탭의 왼쪽 창에서 를 클릭하고 **Unassociated (연결되지 않음)** 확인란을 선택합니다.




# 개체 비교

단계 **1** 왼쪽의 CDO 탐색 바에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 페이지에서 개체를 필터링하여 비교하려는 개체를 찾습니다.

단계 **3** **Compare(**비교**)** 버튼 

를 클릭합니다.

단계 **4** 비교할 개체를 최대 3개까지 선택합니다.

단계 **5** 화면 하단에서 개체를 나란히 봅니다.

- 개체 세부 정보 제목 표시줄에서 위쪽 및 아래쪽 화살표를 클릭하면 개체 세부 정보를 더 많이 또는 더 적게 볼 수 있습니다.
- 세부 정보 및 관계 상자를 확장하거나 축소하여 더 많거나 적은 정보를 확인합니다.

단계 **6** (선택 사항) 관계 상자는 개체가 사용되는 방식을 보여줍니다. 디바이스 또는 정책과 연결될 수 있습니다. 개체가 디바이스와 연결된 경우 디바이스 이름을 클릭한 다음 **View Configuration(**구성 보기**)**을 클릭하여 디바이스 구성을 볼 수 있습니다. CDO는 디바이스의 구성 파일을 표시하고 해당 개체에 대한 항목을 강조 표시합니다.

# 필터

**Inventory(**재고 목록**)** 및 **Objects(**개체**)** 페이지에서 다양한 필터를 사용하여 원하는 디바이스 및 개체를 찾을 수 있습니다.

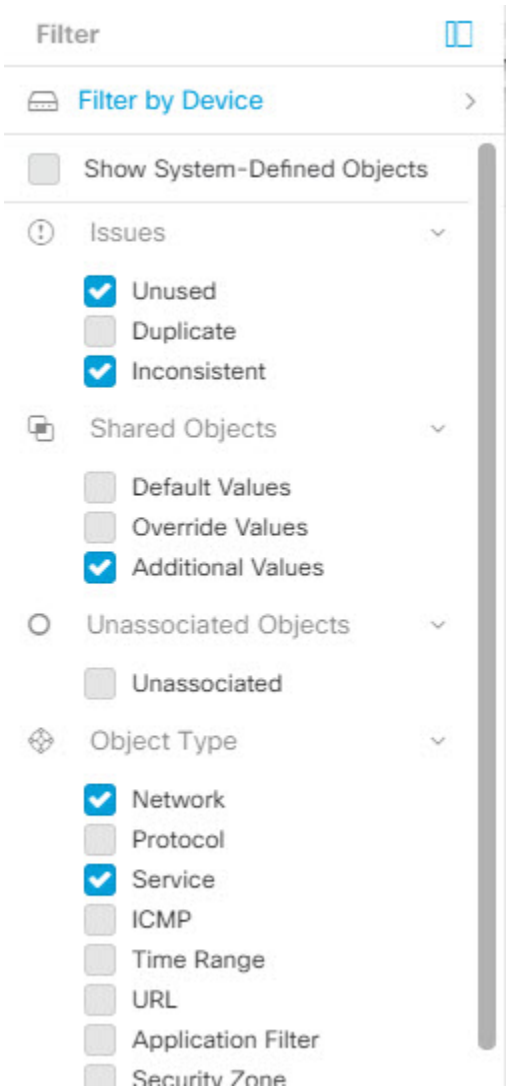
필터링하려면 Devices and Services(디바이스 및 서비스), Policies(정책) 및 Objects(개체) 탭의 왼쪽 창에서 을 클릭합니다.

Inventory(재고 목록) 필터를 사용하면 디바이스 유형, 하드웨어 및 소프트웨어 버전, snort 버전, 구성 상태, 연결 상태, 충돌 탐지, 보안 디바이스 커넥터 및 레이블을 기준으로 필터링할 수 있습니다. 필터를 적용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다. 필터를 사용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다.

개체 필터를 사용하면 디바이스, 문제 유형, 공유 개체, 연결되지 않은 개체 및 개체 유형을 기준으로 필터링할 수 있습니다. 결과에 시스템 개체를 포함하거나 포함하지 않을 수 있습니다. 또한 검색 필드를 사용하여 필터 결과에서 특정 이름, IP 주소 또는 포트 번호를 포함하는 개체를 검색할 수 있습니다.

디바이스 및 개체를 필터링할 때 검색 용어를 결합하여 몇 가지 잠재적 검색 전략을 생성하여 관련 결과를 찾을 수 있습니다.

다음 예제에서는 "문제(사용되었거나 일관성 없음)" 및 추가 값이 있는 공유 개체 및 네트워크 또는 서비스 유형의 개체 검색에 필터를 적용합니다.




# 개체 필터

필터링하려면 Objects(개체) 탭의 왼쪽 창에서 을(를) 클릭합니다.

- **All Objects(**모든 개체**)** - 이 필터는 CDO에 온보딩된 모든 디바이스에서 사용 가능한 모든 개체를 제공합니다. 이 필터는 모든 개체를 찾아보거나 하위 필터를 검색하거나 추가로 적용하기 위한 시작점으로 유용합니다.
- **Shared Objects(**공유 개체**)** - 이 빠른 필터는 CDO가 두 개 이상의 디바이스에서 공유하는 것으로 확인한 모든 개체를 표시합니다.
- **Objects By Device(**디바이스별 개체**)** - 선택한 디바이스에 있는 개체를 볼 수 있도록 특정 디바이스를 선택할 수 있습니다.

하위 필터 – 각 기본 필터에는 선택 범위를 좁히기 위해 적용할 수 있는 하위 필터가 있습니다. 이러한 하위 필터는 네트워크, 서비스, 프로토콜 등의 개체 유형을 기반으로 합니다.

이 필터 표시줄에서 선택한 필터는 다음 기준과 일치하는 개체를 반환합니다.

***** 두 디바이스 중 하나에 있는 개체. (디바이스를 지정하려면 **Filter by Device(**디바이스별 필터링**)**를 클릭합니다.) AND는

***** 일치하지 않는 개체 AND는

***** 네트워크 개체 또는 서비스 개체 AND

***** 개체 명명 규칙에 "**group**"이라는 단어가 있습니다.

**Show System Objects(**시스템 개체 표시**)**를 선택했으므로 결과에 시스템 개체와 사용자 정의 개체가 모두 포함됩니다.

시스템 개체 필터 표시

일부 디바이스는 공통 서비스에 대해 사전 정의된 개체가 함께 제공됩니다. 이러한 시스템 개체는 이미 생성되어 규칙 및 정책에서 사용할 수 있으므로 편리합니다. 개체 테이블에는 여러 시스템 개체가 있을 수 있습니다. 시스템 개체는 편집하거나 삭제할 수 없습니다.

**Show System Objects(**시스템 개체 표시**)**는 기본적으로 꺼져 있습니다. 개체 테이블에 시스템 개체를 표시하려면 필터 표시줄에서 **Show System Objects(**시스템 개체 표시**)**를 선택합니다. 개체 테이블에서 시스템 개체를 숨기려면 필터 표시줄에서 Show System Objects(시스템 개체 표시)를 선택하지 않은 상태로 둡니다.

시스템 개체를 숨기면 검색 및 필터링 결과에 포함되지 않습니다. 시스템 개체를 표시하면 개체 검색 및 필터링 결과에 포함됩니다.

## 개체 필터 구성

원하는 만큼 기준을 필터링할 수 있습니다. 더 많은 범주를 필터링할수록 예상되는 결과는 줄어듭니다.

단계 **1** 왼쪽의 CDO 탐색 바에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 페이지 상단의 필터 아이콘 을 클릭하여 필터 패널을 엽니다. 선택한 필터를 선택 취소하여 실수로 필터링된 개체가 없는지 확인합니다. 또한 검색 필드를 살펴보고 검색 필드에 입력되었을 수 있는 텍스트를 삭제합니다.

단계 **3** 특정 디바이스에 있는 것으로 결과를 제한하려면 다음을 수행합니다.

**a.** **Filter By Device(**디바이스별 필터링**)**를 클릭합니다.

**b.** 모든 디바이스를 검색하거나 디바이스 탭을 클릭하여 특정 종류의 디바이스만 검색합니다.

**c.** 필터 기준에 포함할 디바이스를 선택합니다.

**d.** **OK(**확인**)**를 클릭합니다.

단계 **4** 검색 결과에 시스템 개체를 포함하려면 **Show System Objects(**시스템 개체 표시**)**를 선택합니다. 검색 결과에서 시스템 개체를 제외하려면 **Show System Objects(**시스템 개체 표시**)**의 선택을 취소합니다.

단계 **5** 필터링할 개체 **Issues(**문제**)**를 선택합니다. 두 개 이상의 문제를 선택하면 선택한 범주의 개체가 필터 결과에 포함됩니다.

단계 **6** 문제가 있었지만 관리자가 무시한 개체를 확인하려면 **Ignored(**무시됨**)** 문제를 선택합니다.

단계 **7** 두 개 이상의 디바이스 간에 공유되는 개체를 필터링하는 경우 **Shared Objects(**공유 개체**)**에서 필수 필터를 선택합니다.

- **Default Values(**기본값**)**: 기본값만 있는 개체를 필터링합니다.
- **Override Values(**값 재정의**)**: 오버라이드된 값이 있는 개체를 필터링합니다.
- **Additional Values(**추가 값**)**: 추가 값이 있는 개체를 필터링합니다.

단계 **8** 규칙 또는 정책의 일부가 아닌 개체를 필터링하는 경우 **Unassociated(**연결되지 않음**)**를 선택합니다.

단계 **9** 필터링할 개체 유형을 선택합니다.

단계 **10** Objects(개체) 검색 필드에 개체 이름, IP 주소 또는 포트 번호를 추가하여 필터링된 결과 중에서 검색 기준으로 개체를 찾을 수도 있습니다.

### 필터 기준에서 디바이스를 제외해야 하는 경우

필터링 기준에 디바이스를 추가하면 결과에 디바이스의 개체가 표시되지만 해당 개체와 다른 디바이스의 관계는 표시되지 않습니다. 예를 들어 **ObjectA**가 ASA1과 ASA2 간에 공유된다고 가정합니다. ASA1에서 공유 개체를 찾기 위해 개체를 필터링하는 경우 **ObjectA**를 찾을 수 있지만 **Relationships(**관계**)** 창에는 해당 개체가 ASA1에 있다는 것만 표시됩니다.

개체와 관련된 모든 디바이스를 보려면 검색 기준에 디바이스를 지정하지 마십시오. 다른 기준으로 필터링하고 원하는 경우 검색 기준을 추가하십시오. CDO가 식별하는 개체를 선택한 다음 관계 창을 살펴봅니다. 개체와 관련된 모든 디바이스 및 정책이 표시됩니다.

## 개체 무시

사용되지 않거나 중복되거나 일관성이 없는 개체를 해결하는 한 가지 방법은 해당 개체를 무시하는 것입니다. 사용되지 않은 개체 문제 해결 중복 개체 문제 해결 불일치 개체 문제 해결 해당 상태에 대한 타당한 이유가 있다고 판단하고 개체 문제를 해결되지 않은 상태로 두도록 선택할 수 있습니다. 나중에 무시된 개체를 해결해야 할 수도 있습니다. CDO는 개체 문제를 검색할 때 무시된 개체를 표시하지 않으므로 무시된 개체에 대한 개체 목록을 필터링한 다음 결과에 따라 조치를 취해야 합니다.

단계 **1** 왼쪽의 CDO 탐색 바에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 개체 필터

단계 **3** **Object(**개체**)** 테이블에서 무시를 취소할 개체를 선택합니다. 한 번에 하나의 개체를 무시 취소할 수 있습니다.

단계 **4** 세부 정보 창에서 **Unignore(**무시**)**를 클릭합니다.

단계 **5** 요청을 확인합니다. 이제 문제별로 개체를 필터링하면 이전에 무시되었던 개체를 찾아야 합니다.

# 개체 삭제

단일 개체 또는 여러 개체를 삭제할 수 있습니다.

## 단일 개체 삭제

**Caution** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(**개체**) > ASA Objects(ASA** 개체**)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

단계 **1** 왼쪽의 CDO 탐색 모음에서 **Objects(**개체**)**를 선택하고 옵션을 선택합니다.

단계 **2** 개체 필터와 검색 필드를 사용하여 삭제하려는 개체를 찾아 선택합니다.

단계 **3** **Relationships(**관계**)** 창을 검토합니다. 개체가 정책 또는 개체 그룹에서 사용되는 경우 해당 정책 또는 그룹에서 개체를 제거할 때까지 개체를 삭제할 수 없습니다.

단계 **4** 작업 창에서 **Remove(**제거**)** 아이콘를 클릭합니다.

단계 **5** **OK(**확인**)**을 클릭하여 개체 삭제를 확인합니다.

단계 **6** 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나, 한 번에 여러 변경 사항을 기다렸다가 배포합니다.

## 사용되지 않는 개체 그룹 삭제

디바이스를 온보딩하고 개체 문제를 해결하기 시작하면 사용하지 않는 개체를 많이 찾습니다. 한 번에 최대 50개의 사용하지 않는 개체를 삭제할 수 있습니다.

단계 **1** **Issues(**문제**)** 필터를 사용하여 미사용 개체를 찾습니다. 디바이스 필터를 사용하여 디바이스 없음을 선택하여 디바이스와 연결되지 않은 개체를 찾을 수도 있습니다. 개체 목록을 필터링하면 개체 확인란이 나타납니다.

단계 **2** 개체 테이블 머리글에서 **Select all(**모두 선택**)** 확인란을 선택하여 개체 테이블에 나타나는 필터에 의해 발견된 모든 개체를 선택합니다. 또는 삭제할 개별 개체에 대한 개별 확인란을 선택합니다.

단계 **3** 작업 창에서 **Remove(**제거**)** 아이콘를 클릭합니다.

단계 **4** 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

# 네트워크 개체

네트워크 개체는 호스트 이름, 네트워크 IP 주소, IP 주소의 범위, FQDN(인증된 도메인 이름) 또는 CIDR 표기법으로 표현된 서브 네트워크를 포함할 수 있습니다. 네트워크 그룹은 그룹에 추가하는 네트워크 개체 및 기타 개별 주소 또는 서브 네트워크의 모음입니다. 네트워크 개체 및 네트워크 그룹은 액세스 규칙, 네트워크 정책 및 NAT 규칙에서 사용됩니다. CDO를 사용하여 네트워크 개체 및 네트워크 그룹을 생성, 업데이트 및 삭제할 수 있습니다.

***Table 4:*** 네트워크 개체의 허용되는 값

| 디바이스 유형 | **IPv4 / IPv6** | 단일 주소 | 주소 범위 | 전체**(Fully Qualified)** 도메인 이름 | **CIDR** 표기법의 서브넷 |
|---|---|---|---|---|---|
| ASA | IPv4 및 IPv6 | 예 | 예 | 예 | 예 |

***Table 5:*** 네트워크 그룹의 허용되는 콘텐츠

| 디바이스 유형 | **IP** 값 | 네트워크 개체 | 네트워크 그룹 |
|---|---|---|---|
| ASA | 예 | 예 | 예 |

제품 간 네트워크 개체 재사용

클라우드 사용 Firewall Management Center가 포함된 Cisco Defense Orchestrator 테넌트가 있는 경우:

Secure Firewall Threat Defense, FDM 관리 위협 방어, ASA 또는 Meraki 네트워크 개체 또는 그룹을 생성하면 클라우드 사용 Firewall Management Center를 구성할 때 사용되는 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지의 개체 목록에도 개체의 복사본이 추가되며, 그 반대의 경우도 마찬가지입니다.

한 페이지에서 네트워크 개체 또는 그룹에 대한 변경 사항은 두 페이지의 개체 또는 그룹 인스턴스에 적용됩니다. 한 페이지에서 개체를 삭제하면 다른 페이지에서도 개체의 해당 복사본이 삭제됩니다.

예외:

- 클라우드 사용 Firewall Management Center에 대해 동일한 이름의 네트워크 개체가 이미 있는 경우 Secure Firewall Threat Defense, FDM 관리 위협 방어, ASA 또는 Meraki 네트워크 개체는 Cisco Defense Orchestrator의 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지에서 복제되지 않습니다.
- 온프레미스 Secure Firewall Management Center에서 관리하는 온보딩된 위협 방어 디바이스의 네트워크 개체 및 그룹은 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지에 복제되지 않으며, 클라우드 사용 Firewall Management Center에서 사용할 수 없습니다.

  클라우드 사용 Firewall Management Center로 마이그레이션된 온프레미스 Secure Firewall Management Center 인스턴스의 경우, 네트워크 개체 및 그룹이 FTD 디바이스에 구축된 정책에서 사용되었다면 네트워크 개체 및 그룹이 CDO 개체 페이지에 복제됩니다.

- CDO와 클라우드 사용 Firewall Management Center 간에 네트워크 개체 공유 는 새로운 테넌트에서 자동으로 활성화되지만 기존 테넌트에 대해서는 요청해야 합니다. 네트워크 개체를 클라우드 사용 Firewall Management Center와 공유하지 않는 경우 CDO 고객이 TAC로 지원 티켓을 여는 방법하여 테넌트에서 기능을 활성화하십시오.

네트워크 개체 보기

CDO를 사용하여 생성한 네트워크 개체와 온보딩된 디바이스 구성에서 인식되는 CDO가 Objects(개체) 페이지에 표시됩니다. 개체 유형으로 레이블이 지정됩니다. 이렇게 하면 개체 유형으로 필터링하여 원하는 개체를 빠르게 찾을 수 있습니다.

Objects(개체) 페이지에서 네트워크 개체를 선택하면 Details(세부 정보) 창에 개체의 값이 표시됩니다. Relationships(관계) 창에는 개체가 정책에서 사용되는지 여부와 개체가 저장된 디바이스가 표시됩니다.

네트워크 그룹을 클릭하면 해당 그룹의 콘텐츠가 표시됩니다. 네트워크 그룹은 네트워크 개체에 의해 제공되는 모든 값의 복합물입니다.

# ASA 네트워크 개체 및 네트워크 그룹 생성 또는 편집

**ASA** 네트워크 개체는 CIDR 표기법으로 표시된 호스트 이름, IP 주소 또는 서브넷 주소를 포함할 수 있습니다. 네트워크 그룹은 액세스 규칙, 네트워크 정책 및 NAT 규칙에 사용되는 네트워크 개체, 네트워크 그룹 및 IP 주소의 복합 그룹입니다. CDO를 사용하여 네트워크 개체 및 네트워크 그룹을 생성, 읽기, 업데이트 및 삭제할 수 있습니다.

***Table 6: ASA*** 네트워크 개체 및 그룹의 허용 값

| 디바이스 유형 | **IPv4 / IPv6** | 단일 주소 | 주소 범위 | **FQDN(Partially Qualified Domain Name)** | **CIDR** 표기법의 서브넷 |
|---|---|---|---|---|---|
| ASA | IPv4 / IPv6 | 예 | 예 | 예 | 예 |

**Note** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(**개체**) > ASA Objects(ASA** 개체**)** 페이지에서 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다.

**Caution** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(**개체**) > ASA Objects(ASA** 개체**)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

## 새 네트워크 개체 생성

네트워크 개체는 호스트 이름, 네트워크 IP 주소, IP 주소의 범위, FQDN(인증된 도메인 이름) 또는 CIDR 표기법으로 표현된 서브 네트워크를 포함할 수 있습니다. 네트워크 개체는 액세스 규칙, 네트워크 정책 및 NAT 규칙에서 사용됩니다. CDO를 사용하여 네트워크 개체 및 네트워크 그룹을 생성, 업데이트 및 삭제할 수 있습니다.

**Note** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(**개체**) > ASA Objects(ASA** 개체**)** 페이지에서 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다.

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2** 파란색 더하기 버튼 을 클릭하여 개체를 생성합니다.

단계 **3** **ASA** > **Network(ASA** 네트워크**)**를 클릭합니다.

단계 **4** 개체 이름을 입력합니다.

단계 **5** **Create a network object(**네트워크 개체 생성**)**를 선택합니다.

단계 **6** (선택 사항) 개체 설명을 입력합니다.

단계 **7** **Value(**값**)** 섹션에서 다음 방법 중 하나로 IP 주소 정보를 추가합니다.

- **eq**를 선택한 다음 단일 IP 주소, CIDR 표기법을 사용한 서브넷 주소 또는 PQDN(Partially Qualified Domain Name)을 입력합니다.
- 범위를 선택한 다음 IP 주소의 범위를 입력합니다. 시작 주소와 끝 주소를 공백으로 구분하여 범위를 입력합니다. 예: 10.1.1.1 10.1.1.255 또는 2001:DB8:1::1 2001:DB8:1::3

단계 **8** **Add(**추가**)**를 클릭합니다.

**Important** 새로 생성된 네트워크 개체는 규칙 또는 정책의 일부가 아니므로 ASA 디바이스와 연결되지 않습니다. 이러한 개체를 보려면 개체 필터에서 **Unassociated(**연결되지 않음**)** 개체 범주를 선택합니다. 자세한 내용은 개체 필터를 참고하십시오. 디바이스의 규칙 또는 정책에서 연결되지 않은 개체를 사용하면 이러한 개체는 해당 디바이스와 연결됩니다.

## ASA 네트워크 그룹 생성

네트워크 그룹은 IP 주소 값, 네트워크 개체 및 네트워크 그룹을 포함할 수 있습니다. 새 네트워크 그룹을 만들 때 이름, IP 주소, IP 주소 범위 또는 FQDN으로 기존 개체를 검색하고 네트워크 그룹에 추가할 수 있습니다. 개체가 없는 경우 동일한 인터페이스에서 해당 개체를 즉시 생성하고 네트워크 그룹에 추가할 수 있습니다. 네트워크 그룹은 IPv4 및 IPv6 주소를 모두 포함할 수 있습니다.

**Note** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(**개체**) > ASA Objects(ASA** 개체**)** 페이지에서 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다.

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2** 파란색 더하기 버튼 을 클릭하여 개체를 생성합니다.

단계 **3** **ASA** > **Network(ASA** 네트워크**)**를 클릭합니다.

단계 **4** 개체 이름을 입력합니다.

단계 **5** **Create a network group(**네트워크 그룹 생성**)**을 선택합니다.

단계 **6** (선택 사항) 개체 설명을 입력합니다.

단계 **7** **Values(**값**)** 필드에 값 또는 개체 이름을 입력합니다. 입력을 시작하면 CDO에서 항목과 일치하는 개체 이름 또는 값을 제공합니다.

단계 **8** 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.

단계 **9** CDO가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add(**추가**)**를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.

단계 **10** 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.

- 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name(**이 이름의 새 개체로 추가**)**을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.
- 새 개체를 생성하려면 **Add as New Object(**새 개체로 추가**)**를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.
- 개체를 사용하지 않고 인라인 값을 만들려면 **Add Value(**값 추가**)**를 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.

값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.

**Note** 편집 아이콘을 클릭하여 세부 정보를 편집할 수 있습니다. 삭제 버튼을 클릭해도 개체 자체는 삭제되지 않습니다. 대신 네트워크 그룹에서 제거됩니다.

단계 **11** 필요한 개체를 추가한 후 **Add(**추가**)**를 클릭하여 새 네트워크 그룹을 생성합니다.

단계 **12** 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, on page 352.

## ASA 네트워크 개체 편집

**Caution** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(**개체**) > ASA Objects(ASA** 개체**)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.

단계 **3** 네트워크 개체를 선택하고 **Actions(**작업**)** 창에서 편집 아이콘 을 클릭합니다.

단계 **4** 위의 절차에서 만든 것과 같은 방식으로 대화 상자에서 값을 편집합니다.

**Note** 네트워크 그룹에서 개체를 제거하려면 옆에 있는 삭제 아이콘을 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭합니다. CDO에 변경의 영향을 받을 디바이스가 표시됩니다.

단계 **6** **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

## ASA 네트워크 그룹 편집

**Caution** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(**개체**) > ASA Objects(ASA** 개체**)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

단계 **1** 좌측의 CDO 탐색 모음에서 **Objects(**개체**) > ASA Objects(ASA** 개체**)**를 클릭합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 편집하려는 네트워크 그룹을 찾습니다.

단계 **3** SGT 그룹을 선택하고 **Actions(**작업**)** 창에서 편집 아이콘 를 클릭합니다.

단계 **4** 이 네트워크 그룹에 새 네트워크 개체 또는 네트워크 그룹을 추가하려면 다음 단계를 수행합니다.

**a.** 개체 이름 또는 네트워크 그룹 옆에 나타나는 편집 아이콘 을 클릭하여 편집합니다.

**b.** 확인 표시를 클릭하여 변경 사항을 저장합니다.

**Note** 네트워크 그룹에서 값을 제거하려면 삭제 아이콘을 클릭합니다.

단계 **5** 이 네트워크 그룹에 새 네트워크 개체 또는 네트워크 그룹을 추가하려면 다음 단계를 수행합니다.

**a.** **Values(**값**)** 필드에 새 값이나 기존 네트워크 개체의 이름을 입력합니다. 입력을 시작하면 CDO에서 항목과 일치하는 개체 이름 또는 값을 제공합니다. 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.

**b.** CDO가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add(**추가**)**를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.

**c.** 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.

- 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name(**이 이름의 새 개체로 추가**)**을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.
- 새 개체를 생성하려면 **Add as New Object(**새 개체로 추가**)**를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.
- 개체를 사용하지 않고 인라인 값을 만들려면 **Add Value(**값 추가**)**를 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.

값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.

단계 **6** **Save(**저장**)**를 클릭합니다. CDO에 변경의 영향을 받을 정책이 표시됩니다.

단계 **7** **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

단계 **8** 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, on page 352.

## 공유 네트워크 그룹에 값 추가

연결된 모든 디바이스에 있는 공유 네트워크 그룹의 값을 "기본값"이라고 합니다. CDO를 사용하면 공유 네트워크 그룹에 "추가 값"을 추가하고 해당 공유 네트워크 그룹과 연결된 일부 디바이스에 해당 값을 할당할 수 있습니다. CDO는 변경 사항을 디바이스에 구축할 때 콘텐츠를 확인하고 공유 네트워크 그룹과 연결된 모든 디바이스에 "기본값"을 푸시하고 지정된 디바이스에만 "추가 값"을 푸시합니다.

모든 사이트에서 액세스할 수 있어야 하는 본사에 4개의 AD 기본 서버가 있는 시나리오를 예로 들어 보겠습니다. 따라서 모든 사이트에서 사용할 "Active-Directory"라는 개체 그룹을 생성했습니다. 이제 지사 중 하나에 두 개의 AD 서버를 추가하려고 합니다. 개체 그룹 "Active-Directory"에서 해당 지사에 특정한 추가 값으로 세부 정보를 추가하여 이 작업을 수행할 수 있습니다. 이 두 서버는 "Active-Directory" 개체가 일관성이 있는지 또는 공유되는지를 확인하는 데 참여하지 않습니다. 따라서 모든 사이트에서 4개의 AD 기본 서버에 액세스할 수 있지만 지사(2개의 추가 서버 포함)는 2개의 AD 서버와 4개의 AD 기본 서버에 액세스할 수 있습니다.

**Note** 일치하지 않는 공유 네트워크 그룹이 있는 경우 추가 값을 사용하여 단일 공유 네트워크 그룹으로 결합할 수 있습니다. 자세한 내용은 불일치 개체 문제 해결을 참조하십시오.

**Caution** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(**개체**) > ASA Objects(ASA** 개체**)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 편집할 공유 네트워크 그룹을 찾습니다.

단계 **3** **Actions(**작업**)** 창에서 편집 아이콘 을 클릭합니다.

- **Devices(**디바이스**)** 필드에는 공유 네트워크 그룹이 있는 디바이스가 표시됩니다.
- **Usage(**사용**)** 필드에는 공유 네트워크 그룹과 연결된 규칙 집합이 표시됩니다.
- **Default Values(**기본값**)** 필드는 생성 중에 제공된 공유 네트워크 그룹과 연결된 기본 네트워크 개체 및 해당 값을 지정합니다. 이 필드 옆에서 이 기본값이 포함된 디바이스의 수를 볼 수 있으며, 클릭하여 해당 이름 및 디바이스 유형을 볼 수 있습니다. 이 값과 연결된 규칙 집합도 확인할 수 있습니다.

단계 **4** 추가 값 필드에 값 또는 이름을 입력합니다. 입력을 시작하면 CDO에서 항목과 일치하는 개체 이름 또는 값을 제공합니다.

단계 **5** 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.

단계 **6** CDO가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add(**추가**)**를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.

단계 **7** 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.

- 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name(**이 이름의 새 개체로 추가**)**을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.

- 새 개체를 생성하려면 **Add as New Object(**새 개체로 추가**)**를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.
- 개체를 사용하지 않고 인라인 값을 만들려면 **Add Value(**값 추가**)**를 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.

값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.

단계 **8** **Devices(**디바이스**)** 열에서 새로 추가된 개체와 연결된 셀을 클릭하고 **Add Devices(**디바이스 추가**)**를 클릭합니다.

단계 **9** 원하는 디바이스를 선택하고 **OK(**확인**)**를 클릭합니다.

단계 **10** **Save(**저장**)**를 클릭합니다. CDO에 변경의 영향을 받을 디바이스가 표시됩니다.

단계 **11** **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

단계 **12** 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, on page 352.

## 공유 네트워크 그룹의 추가 값 편집

**Caution** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(**개체**) > ASA Objects(ASA** 개체**)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

단계 **1** 좌측의 CDO 탐색 모음에서 **Objects(**개체**) > ASA Objects(ASA** 개체**)**를 클릭합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 편집하려는 오버라이드가 있는 개체를 찾습니다.

단계 **3** **Actions(**작업**)** 창에서 편집 아이콘 를 클릭합니다.

단계 **4** 오버라이드 값을 편집합니다.

- 값을 편집하려면 편집 아이콘을 클릭합니다.
- **Devices(**디바이스**)** 열의 셀을 클릭하여 새 디바이스를 할당합니다. 이미 할당된 디바이스를 선택하고 **Remove Overrides(**오버라이드 제거**)**를 클릭하여 해당 디바이스에서 오버라이드를 제거할 수 있습니다.
- **Default Values(**기본값**)**의 화살표를 클릭하여 푸시하고 공유 네트워크 그룹의 추가 값으로 설정합니다. 공유 네트워크 그룹과 연결된 모든 디바이스가 자동으로 할당됩니다.
- **Override Values(**값 재정의**)**에서 화살표를 클릭하여 공유 네트워크 그룹의 기본 개체로 푸시하고 설정합니다.
- 네트워크 그룹에서 개체를 제거하려면 옆에 있는 삭제 아이콘을 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭합니다. CDO에 변경의 영향을 받을 디바이스가 표시됩니다.

단계 **6** **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

단계 **7** 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, on page 352.

## 네트워크 개체 및 그룹 삭제

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(**개체**) > ASA Objects(ASA** 개체**)** 페이지에서 네트워크 개체나 그룹을 삭제하면 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지에서 복제된 네트워크 개체 또는 그룹이 삭제되며, 그 반대의 경우도 마찬가지입니다.

# 트러스트 포인트 개체

CDO를 사용하면 디지털 인증서를 트러스트 포인트 개체로 추가한 다음 하나 이상의 관리 ASA 디바이스에 설치할 수 있습니다. 단일 트러스트 포인트 개체는 ID 쌍(ID 인증서 및 발급자의 CA 인증서), ID 인증서만 또는 CA 인증서만 포함하는 컨테이너입니다.

ASA 디바이스에서 여러 트러스트 포인트를 구성할 수 있습니다. 지원되는 인증서 형식은 PKCS12, PEM 및 DER입니다.

## PKCS12를 사용하여 ID 인증서 개체 추가

이 절차에서는 인증서 파일을 업로드하거나 기존 인증서 텍스트를 텍스트 상자에 붙여넣어 내부 인증서 ID 또는 내부 ID 인증서를 생성합니다. ID 인증서는 원하는 만큼 생성할 수 있습니다.

**PKCS12** 형식으로 인코딩된 파일을 업로드할 수 있습니다. PKCS12는 하나의 암호화된 파일에 서버 인증서, 중간 인증서 및 개인 키를 보관하는 단일 파일입니다. PKCS#12 또는 PFX에서 파일은 하나의 암호화된 파일에 서버 인증서, 중간 인증서 및 개인 키를 보관합니다. 암호 해독을 위해 **Passphrase(**암호 문구**)** 값을 입력합니다.

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2**  아이콘을 클릭하고 **ASA** > **Trustpoints(**트러스트 포인트**)**를 선택합니다.

단계 **3** 인증서의 **Object Name(**개체 이름**)**을 입력합니다. 이름은 컨피그레이션에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 **4** **Certificate Type(**인증서 유형**)** 단계에서 **Identity Certificate(ID** 인증서**)**를 선택합니다.

단계 **5** **Import Type(**가져오기 유형**)** 단계에서 **Upload(**업로드**)**를 선택하여 인증서 파일을 업로드합니다.

**Enrollment(**등록**)** 단계가 Terminal(터미널)로 설정되어 있습니다.

단계 **6** **Certificate Contents(**인증서 콘텐츠**)** 단계에서 PKCS12 형식 세부 정보를 입력합니다.

PKCS#12 또는 PFX에서 파일은 하나의 암호화된 파일에 서버 인증서, 중간 인증서 및 개인 키를 보관합니다. 암호 해독을 위해 **Passphrase(**암호 문구**)** 값을 입력합니다.

단계 **7** **Continue(**계속**)**를 클릭합니다.

단계 **8** **Advanced Options(**고급 옵션**)** 단계에서 다음을 구성할 수 있습니다.

**Revocation(**해지**)** 탭에서 다음을 구성할 수 있습니다.

- **CRL(Certificate Revocation List)** 활성화 - CRL 확인 활성화 여부를 확인합니다.

  기본적으로 **Use CRL distribution point from the certificate(**인증서에서 **CRL** 배포 지점 사용**)** 확인란이 선택되어 인증서에서 해지 목록 배포 URL을 가져옵니다.

  **Cache Refresh Time (in minutes)(**캐시 새로 고침 시간**(**분**))** - 캐시 새로 고침 간격(분)을 입력합니다. 기본값은 60분입니다. 범위는 1분 ~ 1440분입니다. 동일한 CRL을 CA에서 반복적으로 검색할 필요 없이 ASA에서 검색된 CRL을 로컬에 저장할 수 있는데, 이를 CRL 캐싱이라고 합니다. CRL 캐시 용량은 플랫폼에 따라 다르며 모든 상황을 포괄하여 누적됩니다. 새로 검색된 CRL을 캐시에 저장하려는데 저장 한도를 초과할 경우, ASA에서는 가장 오래전에 사용된 CRL을 제거하면서 사용 가능한 공간을 늘립니다.

- **OCSP(Online Certificate Status Protocol)** 활성화 - OCSP 확인 활성화 여부를 확인합니다.

  **OCSP** 서버 **URL** - OCSP 확인이 필요한 경우 폐기를 위한 OCSP 서버 확인 URL입니다. 이 URL은 **`http://`**로 시작해야 합니다.

  **Disable Nonce Extension(Nonce** 확장 비활성화**)** - 암호 기술을 사용하여 요청과 응답을 바인딩함으로써 반복 공격을 방지하는 확인란을 활성화합니다. 이 프로세스에서는 요청의 확장을 응답의 확장과 일치하는지 비교하면서 동일함을 보장합니다. 사용 중인 OCSP 서버가 이와 같이 일치하는 nonce 확장을 포함하지 않는 미리 생성된 응답을 보내는 경우, **Disable Nonce Extension(Nonce** 확장 비활성화**)** 확인란을 선택 취소합니다.

  **Evaluation Priority(**평가 우선순위**)** - 인증서의 해지 상태를 CRL에서 먼저 평가할지 OSCP에서 먼저 평가할지를 지정합니다.

- **Consider the certificate valid if revocation information cannot be reached(**해지 정보에 연결할 수 없는 경우 인증서를 유효한 것으로 간주**)** - 해지 정보에 연결할 수 없는 경우 인증서를 유효한 인증서로 간주하려면 이 확인란을 선택합니다.

  해지 확인에 대한 자세한 내용은 Cisco ASA Series 일반 운영 ASDM 설정의 "기본 설정" 책, XY 문서에서 "디지털 인증서" 장을 참조하십시오.

**Others(**기타**)** 탭을 클릭합니다.

- **Use CA Certificate for the Validation of(**다음을 위한 **CA** 인증서 사용**)** - 이 CA가 검증할 수 있는 연결 유형을 지정합니다.
  - **IPSec Client(IPSec** 클라이언트**)** - 원격 SSL 서버에서 제공하는 인증서를 검증합니다.
  - **SSL Client(SSL** 클라이언트**)** - 수신 SSL 연결에서 제공하는 인증서를 검증합니다.
  - **SSL Server(SSL** 서버**)** - 수신 IPSec 연결에서 제공하는 인증서를 검증합니다.
- **Use Identity Certificate for(ID** 인증서 사용**)** - 등록된 ID 인증서의 사용 방법을 지정합니다.
  - **SSL & IPSec** - SSL 및 IPSec 연결 인증에 사용합니다.

- **Code Signer(**코드 서명자**)** — 코드 서명자 인증서는 해당 개인 키가 디지털 서명 생성에 사용되는 특수한 인증서입니다. 코드 서명에 사용되는 인증서는 CA에서 가져온 것으로, 서명된 코드 자체가 인증서 원본을 나타냅니다.

- 기타 옵션:
  - **Enable CA flag in basic constraints extension(**기본 제약 조건 확장에서 **CA** 플래그 활성화**)** - 이 인증서에서 다른 인증서에 서명할 수 있어야 하는 경우 이 옵션을 선택합니다. 기본 제약 조건 확장은 인증서의 주체가 CA(Certificate Authority)인지 여부를 식별하며 이 경우 인증서를 사용하여 다른 인증서에 서명할 수 있습니다. CA 플래그는 이 확장의 일부입니다. 인증서에 이러한 항목이 있는지 여부
  - **Accept certificates issued by this CA(CA**에서 발급된 인증서 허용**)** - ASA에서 지정된 CA의 인증서를 허용해야 하는 경우 이 옵션을 선택합니다.
  - **Ignore IPsec Key Usage(IPsec** 키 사용 무시**)** - IPsec 원격 클라이언트 인증서의 키 사용 및 확장 키 사용 확장 값을 검증하지 않으려는 경우 이 옵션을 선택합니다. IPsec 클라이언트 인증서를 확인하는 키 사용을 억제할 수 있습니다. 기본적으로 이 옵션은 활성화되어 있지 않습니다.

단계 **9** **Add(**추가**)**를 클릭합니다.

# 자체 서명 인증서 개체 생성

이 절차에서는 마법사에서 적절한 인증서 필드 값을 입력하여 ASA에 대한 자체 서명 인증서를 생성하는 단계를 설명합니다. 자체 서명 인증서는 원하는 만큼 생성할 수 있습니다.

자체 서명 ID 인증서 개체를 생성하려면 다음 단계를 수행합니다.

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2**  아이콘을 클릭하고 **ASA** > **Trustpoints(**트러스트 포인트**)**를 선택합니다.

단계 **3** 인증서의 **Object Name(**개체 이름**)**을 입력합니다. 이름은 컨피그레이션에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 **4** **Identity Certificate(ID** 인증서**)** 단계에서 **Identity Certificate(ID** 인증서**)**를 선택합니다.

단계 **5** **Import Type(**가져오기 유형**)** 단계에서 **New(**새로 만들기**)**를 선택하여 인증서 파일을 업로드하고 **Continue(**계속**)**를 클릭합니다.

단계 **6** **Enrollment(**등록**)** 단계에서 **Self-Signed(**자체 서명**)**를 선택하고 **Continue(**계속**)**를 클릭합니다.

**Certificates Content(**인증서 콘텐츠**)** 단계가 나타납니다. 생성 중인 자체 서명 인증서의 CN 및 SANS 콘텐츠를 이해하려면 인증서 내용을 기반으로 하는 자체 서명 및 CSR 인증서 생성을 읽어보십시오.

단계 **7** **Certificate Contents(**인증서 콘텐츠**)** 단계에서 다음을 구성합니다.

- 국가**(C)**— 드롭다운 목록에서 국가 코드를 선택합니다.
- **State or Province(**주/도**) (ST)** — 인증서에 포함할 주/도입니다.

- **Locality or City(**구/군/시**) (L)** — 인증서에 포함할 구/군/시(예: 도시 이름)입니다.
- 조직**(O)** - 인증서에 포함될 조직 또는 회사 이름입니다.
- **Organizational Unit(Department)(**조직 단위**(**부서**)) (OU)** — 인증서에 포함할 조직 단위의 이름(예: 부서 이름)입니다.
- 일반 이름**(CN)** - 인증서에 포함할 X.500 일반 이름입니다. 이는 디바이스, 웹사이트 또는 다른 문자열의 이름일 수 있습니다. 일반적으로 연결에 성공하려면 이 요소가 필요합니다. 예를 들어 원격 액세스 VPN에 사용되는 내부 인증서에는 CN을 포함해야 합니다.
- **Email Address(**이메일 주소**) (EA)**— ID 인증서와 연결된 이메일 주소입니다.
- **IP Address(IP** 주소**)**— 점으로 구분된 4개의 십진수로 표기되는 네트워크상의 ASA IP 주소입니다.
- **Device's FQDN(**디바이스의 **FQDN)**— DNS 트리 계층 구조에서 노드의 위치를 나타내는 명확한 도메인 이름입니다.
- **Include Device's Serial Number(**디바이스의 일련 번호 포함**)**— 인증서 매개 변수에 ASA 일련 번호를 추가하려면 확인란을 선택합니다.

a) **Key(**키**)** 탭을 클릭합니다.

- **RSA** 또는 **ECDSA** 키 유형을 선택합니다.
- **Key Size(**키 크기**)** - 키 페어가 존재하지 않는 경우 비트 단위로 원하는 키 크기(모듈러스)를 지정합니다. RSA의 권장 키 크기는 1024이고 ECDSA의 경우 348입니다. 모듈러스 크기가 클수록 키가 안전합니다. 그러나 모듈러스 크기가 큰 키는 생성 및 교환 프로세스에 더 오랜 시간이 걸립니다.(512비트보다 큰 경우 1분 이상)
- **Continue(**계속**)**를 클릭합니다.

단계 **8** **Advanced Options(**고급 옵션**)** 단계에서 다음을 구성할 수 있습니다.

**Revocation(**해지**)** 탭에서 다음을 구성할 수 있습니다.

- **CRL(Certificate Revocation List)** 활성화 - CRL 확인 활성화 여부를 확인합니다.

  기본적으로 **Use CRL distribution point from the certificate(**인증서에서 **CRL** 배포 지점 사용**)** 확인란이 선택되어 인증서에서 해지 목록 배포 URL을 가져옵니다.

  **Cache Refresh Time (in minutes)(**캐시 새로 고침 시간**(**분**))** - 캐시 새로 고침 간격(분)을 입력합니다. 기본값은 60분입니다. 범위는 1분 ~ 1440분입니다. 동일한 CRL을 CA에서 반복적으로 검색할 필요 없이 ASA에서 검색된 CRL을 로컬에 저장할 수 있는데, 이를 CRL 캐싱이라고 합니다. CRL 캐시 용량은 플랫폼에 따라 다르며 모든 상황을 포괄하여 누적됩니다. 새로 검색된 CRL을 캐시에 저장하려는데 저장 한도를 초과할 경우, ASA에서는 가장 오래전에 사용된 CRL을 제거하면서 사용 가능한 공간을 늘립니다.

- **OCSP(Online Certificate Status Protocol)** 활성화 - OCSP 확인 활성화 여부를 확인합니다.

  **OCSP** 서버 **URL** - OCSP 확인이 필요한 경우 폐기를 위한 OCSP 서버 확인 URL입니다. 이 URL은 **`http://`**로 시작해야 합니다.

**Disable Nonce Extension(Nonce** 확장 비활성화**)** - 암호 기술을 사용하여 요청과 응답을 바인딩함으로써 반복 공격을 방지하는 확인란을 활성화합니다. 이 프로세스에서는 요청의 확장을 응답의 확장과 일치하는지 비교하면서 동일함을 보장합니다. 사용 중인 OCSP 서버가 이와 같이 일치하는 nonce 확장을 포함하지 않는 미리 생성된 응답을 보내는 경우, **Disable Nonce Extension(Nonce** 확장 비활성화**)** 확인란을 선택 취소합니다.

**Evaluation Priority(**평가 우선순위**)** - 인증서의 해지 상태를 CRL에서 먼저 평가할지 OSCP에서 먼저 평가할지를 지정합니다.

- **Consider the certificate valid if revocation information cannot be reached(**해지 정보에 연결할 수 없는 경우 인증서를 유효한 것으로 간주**)** - 해지 정보에 연결할 수 없는 경우 인증서를 유효한 인증서로 간주하려면 이 확인란을 선택합니다.

  해지 확인에 대한 자세한 내용은 Cisco ASA Series 일반 운영 ASDM 설정의 "기본 설정" 책, XY 문서에서 "디지털 인증서" 장을 참조하십시오.

**Others(**기타**)** 탭을 클릭합니다.

- **Use CA Certificate for the Validation of(**다음을 위한 **CA** 인증서 사용**)** - 이 CA가 검증할 수 있는 연결 유형을 지정합니다.
  - **IPSec Client(IPSec** 클라이언트**)** - 원격 SSL 서버에서 제공하는 인증서를 검증합니다.
  - **SSL Client(SSL** 클라이언트**)** - 수신 SSL 연결에서 제공하는 인증서를 검증합니다.
  - **SSL Server(SSL** 서버**)** - 수신 IPSec 연결에서 제공하는 인증서를 검증합니다.
- **Use Identity Certificate for(ID** 인증서 사용**)** - 등록된 ID 인증서의 사용 방법을 지정합니다.
  - **SSL & IPSec** - SSL 및 IPSec 연결 인증에 사용합니다.
  - **Code Signer(**코드 서명자**)** — 코드 서명자 인증서는 해당 개인 키가 디지털 서명 생성에 사용되는 특수한 인증서입니다. 코드 서명에 사용되는 인증서는 CA에서 가져온 것으로, 서명된 코드 자체가 인증서 원본을 나타냅니다.
- 기타 옵션:
  - **Enable CA flag in basic constraints extension(**기본 제약 조건 확장에서 **CA** 플래그 활성화**)** - 이 인증서에서 다른 인증서에 서명할 수 있어야 하는 경우 이 옵션을 선택합니다. 기본 제약 조건 확장은 인증서의 주체가 CA(Certificate Authority)인지 여부를 식별하며 이 경우 인증서를 사용하여 다른 인증서에 서명할 수 있습니다. CA 플래그는 이 확장의 일부입니다. 인증서에 이러한 항목이 있는지 여부
  - **Accept certificates issued by this CA(CA**에서 발급된 인증서 허용**)** - ASA에서 지정된 CA의 인증서를 허용해야 하는 경우 이 옵션을 선택합니다.
  - **Ignore IPsec Key Usage(IPsec** 키 사용 무시**)** - IPsec 원격 클라이언트 인증서의 키 사용 및 확장 키 사용 확장 값을 검증하지 않으려는 경우 이 옵션을 선택합니다. IPsec 클라이언트 인증서를 확인하는 키 사용을 억제할 수 있습니다. 기본적으로 이 옵션은 활성화되어 있지 않습니다.

단계 **9** **Add(**추가**)**를 클릭합니다.

# CSR(Certificate Signing Request)을 위한 ID 인증서 개체 추가

CSR(Certificate Signing Requests)을 생성하고 지정된 CA에서 ID 인증서를 얻으려면 CA(Certification Authority) 서버 정보 및 등록 매개변수가 필요합니다. 요청을 생성하려면 RSA(Rivest-Shamir-Adleman) 또는 ECDSA(Elliptic Curve Digital Signature Algorithm) 키 유형을 선택해야 합니다.

식별 정보를 제공하고 선택적으로 CA에서 얻은 CA 인증서를 업로드하여 트러스트 포인트 개체를 생성합니다.

---

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2**  아이콘을 클릭하고 **ASA** > **Trustpoints(**트러스트 포인트**)**를 선택합니다.

단계 **3** 인증서의 **Object Name(**개체 이름**)**을 입력합니다. 이름은 컨피그레이션에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 **4** **Identity Certificate(ID** 인증서**)** 단계에서 **Identity Certificate(ID** 인증서**)**를 선택합니다.

단계 **5** **Import Type(**가져오기 유형**)** 단계에서 **New(**새로 만들기**)**를 선택하여 인증서 파일을 업로드하고 **Continue(**계속**)**를 클릭합니다.

단계 **6** **Enrollment(**등록**)** 단계에서 **Manual(**수동**)**을 선택합니다.

단계 **7** (선택 사항) CA에서 가져온 CA 인증서를 붙여넣거나 업로드할 수 있습니다. 필드를 비워둘 수 있습니다.

단계 **8** Continue(계속)를 클릭합니다.

Certificates Content(인증서 콘텐츠) 단계가 나타납니다. 생성 중인 서명 인증서의 CN 및 SANS 콘텐츠를 이해하려면 인증서 내용을 기반으로 하는 자체 서명 및 CSR 인증서 생성을 읽어보십시오.

단계 **9** **Certificate Contents(**인증서 콘텐츠**)** 단계에서 다음을 구성합니다.

- 국가**(C)**— 드롭다운 목록에서 국가 코드를 선택합니다.
- **State or Province(**주/도**) (ST)** — 인증서에 포함할 주/도입니다.
- **Locality or City(**구/군/시**) (L)** — 인증서에 포함할 구/군/시(예: 도시 이름)입니다.
- 조직**(O)** - 인증서에 포함될 조직 또는 회사 이름입니다.
- **Organizational Unit(Department)(**조직 단위**(**부서**)) (OU)** — 인증서에 포함할 조직 단위의 이름(예: 부서 이름)입니다.
- 일반 이름**(CN)** - 인증서에 포함할 X.500 일반 이름입니다. 이는 디바이스, 웹사이트 또는 다른 문자열의 이름일 수 있습니다. 일반적으로 연결에 성공하려면 이 요소가 필요합니다. 예를 들어 원격 액세스 VPN에 사용되는 내부 인증서에는 CN을 포함해야 합니다.
- **Email Address(**이메일 주소**) (EA)**— ID 인증서와 연결된 이메일 주소입니다.
- **IP Address(IP** 주소**)**— 점으로 구분된 4개의 십진수로 표기되는 네트워크상의 ASA IP 주소입니다.
- **SAN(Subject Alternative Name)** - 이 필드는 'unstructuredName'으로도 인증서 주체 DN의 일부가 됩니다. 인증서가 여러 도메인 또는 IP 주소에 사용되는 경우, 이 필드를 활용하는 것이 좋습니다.
  - **Use Device Host Name(**디바이스 호스트 이름 사용**)**: 디바이스의 호스트 이름이 사용됩니다.

- **Custom: Device's FQDN(**사용자 지정 디바이스의 **FQDN)**— DNS 트리 계층 구조에서 노드의 위치를 나타내는 명확한 도메인 이름입니다.

  참고 CN 및 사용자 지정 **FQDN**에 지정된 값은 동일한 것이 좋습니다.

- **Include Device's Serial Number(**디바이스의 일련 번호 포함**)**— 인증서에 ASA의 일련 번호를 추가하려면 확인란을 선택합니다. CA는 인증서 인증 또는 추후 특정 디바이스와 인증서를 연결하기 위해 일련 번호를 사용합니다. 확실하지 않은 경우 일련 번호를 포함하면 디버깅 시 유용합니다.

a) **Key(**키**)** 탭을 클릭합니다.

- **RSA** 또는 **ECDSA** 키 유형을 선택합니다.
- **Key Size(**키 크기**)** - 키 페어가 존재하지 않는 경우 비트 단위로 원하는 키 크기(모듈러스)를 지정합니다. RSA의 권장 키 크기는 1024이고 ECDSA의 경우 348입니다. 모듈러스 크기가 클수록 키가 안전합니다. 그러나 모듈러스 크기가 큰 키는 생성 및 교환 프로세스에 더 오랜 시간이 걸립니다.(512비트보다 큰 경우 1분 이상)
- **Continue(**계속**)**를 클릭합니다.

단계 **10** **Advanced Options(**고급 옵션**)** 단계에서 다음을 구성할 수 있습니다.

**Revocation(**해지**)** 탭에서 다음을 구성할 수 있습니다.

- **CRL(Certificate Revocation List)** 활성화 - CRL 확인 활성화 여부를 확인합니다.

  기본적으로 **Use CRL distribution point from the certificate(**인증서에서 **CRL** 배포 지점 사용**)** 확인란이 선택되어 인증서에서 해지 목록 배포 URL을 가져옵니다.

  **Cache Refresh Time (in minutes)(**캐시 새로 고침 시간**(**분**))** - 캐시 새로 고침 간격(분)을 입력합니다. 기본값은 60분입니다. 범위는 1분 ~ 1440분입니다. 동일한 CRL을 CA에서 반복적으로 검색할 필요 없이 ASA에서 검색된 CRL을 로컬에 저장할 수 있는데, 이를 CRL 캐싱이라고 합니다. CRL 캐시 용량은 플랫폼에 따라 다르며 모든 상황을 포괄하여 누적됩니다. 새로 검색된 CRL을 캐시에 저장하려는데 저장 한도를 초과할 경우, ASA에서는 가장 오래전에 사용된 CRL을 제거하면서 사용 가능한 공간을 늘립니다.

- **OCSP(Online Certificate Status Protocol)** 활성화 - OCSP 확인 활성화 여부를 확인합니다.

  **OCSP** 서버 **URL** - OCSP 확인이 필요한 경우 폐기를 위한 OCSP 서버 확인 URL입니다. 이 URL은 **`http://`** 로 시작해야 합니다.

  **Disable Nonce Extension(Nonce** 확장 비활성화**)** - 암호 기술을 사용하여 요청과 응답을 바인딩함으로써 반복 공격을 방지하는 확인란을 활성화합니다. 이 프로세스에서는 요청의 확장을 응답의 확장과 일치하는지 비교하면서 동일함을 보장합니다. 사용 중인 OCSP 서버가 이와 같이 일치하는 nonce 확장을 포함하지 않는 미리 생성된 응답을 보내는 경우, **Disable Nonce Extension(Nonce** 확장 비활성화**)** 확인란을 선택 취소합니다.

  **Evaluation Priority(**평가 우선순위**)** - 인증서의 해지 상태를 CRL에서 먼저 평가할지 OSCP에서 먼저 평가할지를 지정합니다.

- **Consider the certificate valid if revocation information cannot be reached(**해지 정보에 연결할 수 없는 경우 인증서를 유효한 것으로 간주**)** - 해지 정보에 연결할 수 없는 경우 인증서를 유효한 인증서로 간주하려면 이 확인란을 선택합니다.

해지 확인에 대한 자세한 내용은 Cisco ASA Series 일반 운영 ASDM 설정의 "기본 설정" 책, XY 문서에서 "디지털 인증서" 장을 참조하십시오.

**Others(**기타**)** 탭을 클릭합니다.

- **Use CA Certificate for the Validation of(**다음을 위한 **CA** 인증서 사용**)** - 이 CA가 검증할 수 있는 연결 유형을 지정합니다.
  - **IPSec Client(IPSec** 클라이언트**)** - 원격 SSL 서버에서 제공하는 인증서를 검증합니다.
  - **SSL Client(SSL** 클라이언트**)** - 수신 SSL 연결에서 제공하는 인증서를 검증합니다.
  - **SSL Server(SSL** 서버**)** - 수신 IPSec 연결에서 제공하는 인증서를 검증합니다.
- **Use Identity Certificate for(ID** 인증서 사용**)** - 등록된 ID 인증서의 사용 방법을 지정합니다.
  - **SSL & IPSec** - SSL 및 IPSec 연결 인증에 사용합니다.
  - **Code Signer(**코드 서명자**)** — 코드 서명자 인증서는 해당 개인 키가 디지털 서명 생성에 사용되는 특수한 인증서입니다. 코드 서명에 사용되는 인증서는 CA에서 가져온 것으로, 서명된 코드 자체가 인증서 원본을 나타냅니다.
- 기타 옵션:
  - **Enable CA flag in basic constraints extension(**기본 제약 조건 확장에서 **CA** 플래그 활성화**)** - 이 인증서에서 다른 인증서에 서명할 수 있어야 하는 경우 이 옵션을 선택합니다. 기본 제약 조건 확장은 인증서의 주체가 CA(Certificate Authority)인지 여부를 식별하며 이 경우 인증서를 사용하여 다른 인증서에 서명할 수 있습니다. CA 플래그는 이 확장의 일부입니다. 인증서에 이러한 항목이 있는지 여부
  - **Accept certificates issued by this CA(CA**에서 발급된 인증서 허용**)** - ASA에서 지정된 CA의 인증서를 허용해야 하는 경우 이 옵션을 선택합니다.
  - **Ignore IPsec Key Usage(IPsec** 키 사용 무시**)** - IPsec 원격 클라이언트 인증서의 키 사용 및 확장 키 사용 확장 값을 검증하지 않으려는 경우 이 옵션을 선택합니다. IPsec 클라이언트 인증서를 확인하는 키 사용을 억제할 수 있습니다. 기본적으로 이 옵션은 활성화되어 있지 않습니다.

단계 **11** **Add(**추가**)**를 클릭합니다.

이렇게 하면 트러스트 포인트 인증서 개체가 생성됩니다.

# 신뢰할 수 있는 CA 인증서 개체 추가

외부 인증 기관으로부터 신뢰할 수 있는 CA 인증을 획득하거나, OpenSSL 도구 등 자체 내부 CA를 사용하여 CA 인증을 생성하십시오. 다음의 지원되는 형식 중 하나로 인코딩된 파일을 업로드할 수 있습니다.

- DER(Distinguished Encoding Rules)
- PEM(Privacy-enhanced Electronic Mail)

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2**  아이콘을 클릭하고 **ASA** > **Trustpoints(**트러스트 포인트**)**를 선택합니다.

단계 **3** 인증서의 **Object Name(**개체 이름**)**을 입력합니다. 이름은 컨피그레이션에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 **4** **Certificate Type(**인증서 유형**)** 단계에서 **Trusted CA Certificate(**신뢰할 수 있는 **CA** 인증서**)**를 선택합니다.

단계 **5** **Certificate Contents(**인증서 콘텐츠**)** 단계에서 텍스트 상자에 인증서 콘텐츠를 붙여넣거나 마법사의 설명에 따라 CA 인증서 파일을 업로드합니다.

단계 **6** **Continue(**계속**)**를 클릭합니다. 마법사가 4단계로 진행합니다.

인증서는 다음 지침을 따라야 합니다.

- 인증서의 서버 이름이 서버 호스트 이름/IP 주소와 일치해야 합니다. 예를 들어 IP 주소로 10.10.10.250을 사용하는데 인증서의 주소는 ad.example.com이면 연결은 실패합니다.
- 인증서는 PEM 또는 DER 형식의 X509 인증서여야 합니다.
- 붙여넣는 인증서는 BEGIN CERTIFICATE 및 END CERTIFICATE 줄을 포함해야 합니다. 예를 들면 다음과 같습니다.

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAsx
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxDzAN
BgNVBAcMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjExFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6HOgKlOwXbRvOdksTzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

단계 **7** **Advanced Options(**고급 옵션**)** 단계에서 다음을 구성할 수 있습니다.

**Revocation(**해지**)** 탭에서 다음을 구성할 수 있습니다.

- **CRL(Certificate Revocation List)** 활성화 - CRL 확인 활성화 여부를 확인합니다.

  기본적으로 **Use CRL distribution point from the certificate(**인증서에서 **CRL** 배포 지점 사용**)** 확인란이 선택되어 인증서에서 해지 목록 배포 URL을 가져옵니다.

  **Cache Refresh Time (in minutes)(**캐시 새로 고침 시간**(**분**))** - 캐시 새로 고침 간격(분)을 입력합니다. 기본값은 60분입니다. 범위는 1분 ~ 1440분입니다. 동일한 CRL을 CA에서 반복적으로 검색할 필요 없이 ASA에서 검색된 CRL을 로컬에 저장할 수 있는데, 이를 CRL 캐싱이라고 합니다. CRL 캐시 용량은 플랫폼에 따라 다르며 모든 상황을 포괄하여 누적됩니다. 새로 검색된 CRL을 캐시에 저장하려는데 저장 한도를 초과할 경우, ASA에서는 가장 오래전에 사용된 CRL을 제거하면서 사용 가능한 공간을 늘립니다.

- **OCSP(Online Certificate Status Protocol)** 활성화 - OCSP 확인 활성화 여부를 확인합니다.

  **OCSP** 서버 **URL** - OCSP 확인이 필요한 경우 폐기를 위한 OCSP 서버 확인 URL입니다. 이 URL은 **`http://`**로 시작해야 합니다.

**Disable Nonce Extension(Nonce** 확장 비활성화**)** - 암호 기술을 사용하여 요청과 응답을 바인딩함으로써 반복 공격을 방지하는 확인란을 활성화합니다. 이 프로세스에서는 요청의 확장을 응답의 확장과 일치하는지 비교하면서 동일함을 보장합니다. 사용 중인 OCSP 서버가 이와 같이 일치하는 nonce 확장을 포함하지 않는 미리 생성된 응답을 보내는 경우, **Disable Nonce Extension(Nonce** 확장 비활성화**)** 확인란을 선택 취소합니다.

**Evaluation Priority(**평가 우선순위**)** - 인증서의 해지 상태를 CRL에서 먼저 평가할지 OSCP에서 먼저 평가할지를 지정합니다.

- **Consider the certificate valid if revocation information cannot be reached(**해지 정보에 연결할 수 없는 경우 인증서를 유효한 것으로 간주**)** - 해지 정보에 연결할 수 없는 경우 인증서를 유효한 인증서로 간주하려면 이 확인란을 선택합니다.

  해지 확인에 대한 자세한 내용은 Cisco ASA Series 일반 운영 ASDM 설정의 "기본 설정" 책, XY 문서에서 "디지털 인증서" 장을 참조하십시오.

**Others(**기타**)** 탭을 클릭합니다.

- **Use CA Certificate for the Validation of(**다음을 위한 **CA** 인증서 사용**)** - 이 CA가 검증할 수 있는 연결 유형을 지정합니다.
  - **IPSec Client(IPSec** 클라이언트**)** - 원격 SSL 서버에서 제공하는 인증서를 검증합니다.
  - **SSL Client(SSL** 클라이언트**)** - 수신 SSL 연결에서 제공하는 인증서를 검증합니다.
  - **SSL Server(SSL** 서버**)** - 수신 IPSec 연결에서 제공하는 인증서를 검증합니다.
- 기타 옵션:
  - **Enable CA flag in basic constraints extension(**기본 제약 확장에서 **CA** 플래그 활성화**)** - 기본 제약 확장을 사용하는 인증서의 주체가 CA인지 검증하려면 이 옵션을 선택합니다.
  - **Accept certificates issued by this CA(CA**에서 발급된 인증서 허용**)** - ASA에서 지정된 CA의 인증서를 허용해야 하는 경우 이 옵션을 선택합니다.
  - **Accept certificates issued by the subordinates CAs of this CA(**이 **CA**의 하위 **CA**에서 발급한 인증서 수락**)** - ASA에서 하위 CA의 인증서를 허용해야 하는 경우 이 옵션을 선택합니다.
  - **Ignore IPsec Key Usage(IPsec** 키 사용 무시**)** - IPsec 원격 클라이언트 인증서의 키 사용 및 확장 키 사용 확장 값을 검증하지 않으려는 경우 이 옵션을 선택합니다. IPsec 클라이언트 인증서를 확인하는 키 사용을 억제할 수 있습니다. 기본적으로 이 옵션은 활성화되어 있지 않습니다.

단계 **8** **Add(**추가**)**를 클릭합니다.

이렇게 하면 트러스트 포인트 인증서 개체가 생성됩니다.

# 인증서 내용을 기반으로 하는 자체 서명 및 CSR 인증서 생성

자체 서명 및 CSR 인증서의 CN 및 SANS 콘텐츠에 대한 아이디어가 필요합니다. 콘텐츠는 생성 과정에서 지정한 매개변수를 기반으로 합니다. AnyConnect 클라이언트가 조직의 원하는 VPN 헤드엔드에 연결하려면 매개변수를 정확하게 구성해야 합니다.

이 섹션에서는 지정된 매개변수를 기반으로 자체 서명 및 CSR 인증서의 내용에 대한 아이디어를 제공하는 다양한 사용 사례를 예시와 함께 제공합니다.

사용 사례 **1:** 다른 **CN** 및 **FQDN** 값

예:

- Common Name(공용 이름)(CN): mywebsite.com
- FQDN: mysan.com

표 *7:* 예*:* 다른 ***CN*** 및 ***FQDN*** 값

| | 공용 이름**(CN)** | **unstructuredName** | **SANS** |
|---|---|---|---|
| 자체 서명 | mywebsite.com | mysan.com | mysan.com |
| CSR | mywebsite.com | mysan.com | - |

사용 사례 **2:** 없음으로 설정된 **FQDN** 필드

예:

- Common Name(공용 이름)(CN): mywebsite.com
- FQDN: 없음

표 *8:* 예*:* 없음으로 설정된 ***FQDN*** 필드

| | 공용 이름**(CN)** | **SANS** |
|---|---|---|
| 자체 서명 | Host Name(호스트 이름) | - |
| CSR | mywebsite.com | - |

사용 사례 **3: FQDN** 없음**(**기본 **FQDN)**

예:

- Common Name(공용 이름)(CN): mywebsite.com

표 *9:* 예*: FQDN* 없음*(*기본 *FQDN)*

| | 공용 이름**(CN)** | **unstructuredName** | **SANS** |
|---|---|---|---|
| 자체 서명 | mywebsite.com | 호스트 이름 | - |
| CSR | mywebsite.com | 호스트 이름 | Host Name(호스트 이름) |

사용 사례 **4: FQDN**에 **IP** 주소가 지정됨

예:

- Common Name(공용 이름)(CN): mywebsite.com
- FQDN: 4.5.6.7

표 *10:* 예*: FQDN*에 *IP* 주소가 지정됨

| | 공용 이름**(CN)** | **unstructuredName** | **SANS** |
|---|---|---|---|
| 자체 서명 | mywebsite.com | 4.5.6.7 | - |
| CSR | mywebsite.com | 4.5.6.7 | 4.5.6.7 |

사용 사례 **5: IP** 주소가 지정됨

예:

- IP 주소: 4.5.6.7
- Common Name(공용 이름)(CN): mywebsite.com
- FQDN: fqdn.com

표 *11:* 예*: IP* 주소가 지정됨

| | 공용 이름**(CN)** | **unstructuredAddress** | **unstructuredName** | **SANS** |
|---|---|---|---|---|
| 자체 서명 | mywebsite.com | 4.5.6.7 | fqdn.com | - |
| CSR | mywebsite.com | 4.5.6.7 | fqdn.com | fqdn.com |

사용 사례 **6:** 일련 번호 확인란이 선택됨

예:

- 일련 번호: 9AQXMWOKDT9

표 *12:* 예*: IP* 일련 번호 확인란이 선택됨

| | serialNumber | SANS |
|---|---|---|
| 자체 서명 | 9AQXMWOKDT9 | - |
| CSR | 9AQXMWOKDT9 | fqdn.com |

활용 사례 **7:** 이메일 주소가 지정됨

예:

- EA: abc@xyz.com

표 *13:* 예*:* 이메일 주소가 지정됨

| | unstructredName | emailAddress | SANS |
|---|---|---|---|
| 자체 서명 | Host Name(호스트 이름) | abc@xyz.com | Host Name(호스트 이름) |
| CSR | Host Name(호스트 이름) | abc@xyz.com | - |

# RA VPN 개체

# 서비스 개체

## ASA 서비스 개체

ASA 서비스 개체, 서비스 그룹 및 포트 그룹은 IP 프로토콜 제품군의 일부로 간주되는 프로토콜 또는 포트를 포함하는 재사용 가능한 구성 요소입니다. 서비스 개체에서 단일 프로토콜을 지정하고 이를 소스 포트, 목적지 포트 또는 소스 및 목적지 포트 모두에 할당할 수 있습니다. 서비스 그룹은 여러 서비스 개체를 포함하며 여러 프로토콜을 포함할 수 있습니다.

포트 그룹은 일종의 ASA 서비스 개체입니다. 포트 그룹은 서비스 유형(예: TCP 또는 UDP)과 포트 번호 또는 포트 번호 범위를 페어링하는 포트 개체를 포함합니다. 그 다음 트래픽 일치 기준을 정의하는 목적으로 보안 정책의 개체를 사용할 수 있습니다. 예를 들어 액세스 제어 규칙에서 이를 사용하여 특정 TCP 포트 범위에 대한 트래픽을 허용할 수 있습니다.

자세한 내용은 ASA 서비스 개체 생성 및 편집을 참조하십시오.

### 프로토콜 개체

프로토콜 개체는 덜 일반적으로 사용되는 또는 레거시 프로토콜을 포함하는 서비스 개체 유형입니다. 프로토콜 개체는 이름 및 프로토콜 번호로 식별됩니다. CDO는 ASA 및 Firepower(FDM 관리) 구성에서 이러한 개체를 인식하고 사용자가 쉽게 찾을 수 있도록 자체 필터인 "프로토콜"을 제공합니다.

### ICMP 개체

ICMP(Internet Control Message Protocol) 개체는 ICMP 및 IPv6-ICMP 메시지를 위한 서비스 개체입니다. CDO는 ASA 및 Firepower 구성에서 해당 디바이스가 온보딩되고 사용자가 개체를 쉽게 찾을 수 있도록 해당 디바이스에 "ICMP" 필터를 제공할 때 이러한 개체를 인식합니다.

CDO를 사용하면 ASA 구성에서 ICMP 개체를 제거하거나 이름을 바꿀 수 있습니다. CDO를 사용하여 Firepower 구성에서 ICMP 및 ICMPv6 개체를 생성, 업데이트 및 삭제할 수 있습니다.

**Note** ICMPv6 프로토콜의 경우 AWS는 특정 인수 선택을 지원하지 않습니다. 모든 ICMPv6 메시지를 허용하는 규칙만 지원됩니다.

관련 정보:

- 개체 삭제, on page 122

# ASA 서비스 개체 생성 및 편집

서비스 개체에서 단일 프로토콜을 지정하고 이를 소스 포트, 목적지 포트 또는 소스 및 목적지 포트 모두에 할당할 수 있습니다.

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2** **Create Object(**개체 생성**)** > **ASA** > **Service(**서비스**)**를 클릭합니다.

단계 **3** 개체 이름을 입력합니다.

단계 **4** 서비스 개체 생성을 선택합니다.

단계 **5** **Service Type(**서비스 유형**)** 버튼을 클릭하고 개체를 만들 프로토콜을 선택합니다.

- **TCP, UDP** 및 **TCP-UDP** 서비스 유형의 경우 소스 포트, 목적지 포트 또는 둘 다를 입력합니다.
  - 소스 포트 식별자를 사용하면 번호가 지정된 특정 포트에서 시작되는 트래픽을 일치시킬 수 있습니다. 소스 포트 식별자에서 같음, 범위, 보다 작음, 보다 큼 또는 같지 않음 연산자를 선택하고 적절한 포트 번호 또는 범위를 제공합니다.
  - 목적지 포트 식별자를 사용하면 번호가 지정된 특정 포트에 도착하는 트래픽을 일치시킬 수 있습니다. 목적지 포트 식별자에서 같음, 범위, 보다 작음, 보다 큼 또는 같지 않음 연산자를 선택하고 적절한 포트 번호 또는 범위를 제공합니다.
- 프로토콜 서비스 유형에 대해, 0-255 사이의 프로토콜 번호 또는 ip, tcp, udp, gre 등과 같이 잘 알려진 이름을 입력합니다.

단계 **6** **Add(**추가**)**를 클릭합니다.

예

- 수신 FTP 트래픽을 식별하는 서비스 개체는 TCP 서비스 유형 및 대상 포트 범위가 21인 개체입니다.
- 발신 DNS 및 TCP 트래픽을 통한 DNS를 식별하는 서비스 개체는 tcp-udb 서비스 유형 및 소스 포트가 53인 개체입니다.

## ASA 서비스 그룹 생성

서비스 그룹은 하나 이상의 프로토콜을 나타내는 하나 이상의 서비스 개체로 구성될 수 있습니다.

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2** **Create Object(**개체 생성**) > ASA > Service(**서비스**)**를 클릭합니다.

단계 **3** 개체 이름을 입력합니다.

단계 **4** **Create a service group(**서비스 그룹 생성**)**를 선택합니다.

단계 **5** **Add Object(**개체 추가**)**를 클릭하고, 개체를 선택하고, **Select(**선택**)**을 클릭하여 기존 개체를 추가합니다. 개체를 더 추가하려면 이 단계를 반복합니다.

단계 **6** 필요한 경우 서비스 그룹에 별도의 개별 서비스 유형 값을 추가합니다.

- **TCP, UDP** 및 **TCP-UDP** 서비스 유형의 경우 소스 포트, 목적지 포트 또는 둘 다를 입력합니다.
  - 소스 포트 식별자를 사용하면 번호가 지정된 특정 포트에서 시작되는 트래픽을 일치시킬 수 있습니다. 소스 포트 식별자에서 같음, 범위, 보다 작음, 보다 큼 또는 같지 않음 연산자를 선택하고 적절한 포트 번호 또는 범위를 제공합니다.
  - 목적지 포트 식별자를 사용하면 번호가 지정된 특정 포트에 도착하는 트래픽을 일치시킬 수 있습니다. 목적지 포트 식별자에서 같음, 범위, 보다 작음, 보다 큼 또는 같지 않음 연산자를 선택하고 적절한 포트 번호 또는 범위를 제공합니다.
- 프로토콜 서비스 유형에 대해, 0-255 사이의 프로토콜 번호 또는 ip, tcp, udp, gre 등과 같이 잘 알려진 이름을 입력합니다.

단계 **7** 개별 포트 값을 더 추가하려면 **Add Another Value(**다른 값 추가**)**를 클릭하고 단계 6을 반복합니다.

단계 **8** 서비스 그룹에 서비스 개체 및 서비스 값 추가를 완료하면 **Add(**추가**)**를 클릭합니다.

## ASA 서비스 개체 또는 서비스 그룹 편집

단계 **1** 좌측의 CDO 탐색 모음에서 **Objects(**개체**) > ASA Objects(ASA** 개체**)**를 클릭합니다.

단계 **2** 개체를 필터링하여 편집할 개체를 찾은 다음 개체 테이블에서 개체를 선택합니다.

단계 **3** 세부 정보 창에서 Edit(편집)  를 클릭합니다.

단계 **4** 위의 절차에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 수정합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

단계 **6** CDO에 변경의 영향을 받을 정책이 표시됩니다. **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

# ASA 시간 범위 개체

시간 범위 개체란 무엇입니까**?**

시간 범위 개체는 특정 시간을 정의하며 시작 시간, 종료 시간, 선택 사항인 반복 항목으로 구성됩니다. 네트워크 정책에서 이 개체를 사용하여 특정 기능 또는 자산에 대한 시간 기반 액세스를 제공합니다. 예를 들어, 업무 시간에만 특정 서버에 대한 액세스를 허용하는 액세스 규칙을 만들 수 있습니다. 시간 범위 생성은 디바이스에 대한 액세스를 제한하지 않습니다. 이러한 개체에 대해 구성된 시간은 디바이스에 대해 로컬입니다.

이 개체에 절대 또는 반복 시간 범위를 추가할 수 있습니다. 반복 범위는 주기적인 시간 범위로 간주됩니다.

**Note** 시간 범위에 절대값과 기간 값이 모두 지정된 경우, 절대 시작 시간에 도달해야 기간 값의 평가가 이루어지며 절대 종료 시간에 도달하면 더 이상 평가되지 않습니다.

# ASA 시간 범위 개체 생성

다음 절차에 따라 ASA 디바이스에 대한 시간 범위 개체를 생성합니다.

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2** 파란색 더하기 버튼  을 클릭하여 개체를 생성합니다.

단계 **3** **ASA** > 시간범위**(Time Range)**를 클릭합니다.

단계 **4** 개체 이름을 입력합니다.

단계 **5** 시간 범위를 정의합니다.

- 절대 시간 범위 - 원하는 시간 범위에 대한 시작 시각과 종료 시각을 입력합니다. 몇 분, 몇 시간, 며칠 또는 몇 주에 걸쳐 이 개체를 실행하도록 선택할 수 있습니다. 시간 범위 개체는 하나의 절대 시간 범위만 가질 수 있습니다.

- 반복 시간 범위 -  를 클릭하여 일주일 내내 반복되는 주기적 시간 범위를 추가합니다. 드롭다운 메뉴에서 **Frequency(**빈도**)**, 시간 범위가 적용될 **Days(**요일**)** 및 **Start(**시작**)** 및 **End(**종료**)** 시각을 선택합니다. 시간 범위 개체는 여러 주기 범위를 가질 수 있습니다.

**Note** 시간 범위 개체에 대한 시작 및 종료 시각은 옵션입니다. 개체에 설정된 시작 시각이 없는 경우 시간 범위가 즉시 적용됩니다. 개체에 설정된 종료 시각이 없는 경우 시간 범위는 무기한 지속됩니다.

단계 6 **Add(**추가**)**를 클릭하여 개체를 생성합니다.

# ASA 시간 범위 개체 편집

다음 절차를 사용하여 ASA 디바이스에 대한 시간 범위 개체를 편집합니다.

단계 1 좌측의 CDO 탐색 모음에서 **Objects(**개체**) > ASA Objects(ASA** 개체**)**를 클릭합니다.

단계 2 개체를 필터링하여 편집할 개체를 찾은 다음 개체 테이블에서 개체를 선택합니다.

단계 3 세부 정보 창에서 Edit(편집)  를 클릭합니다.

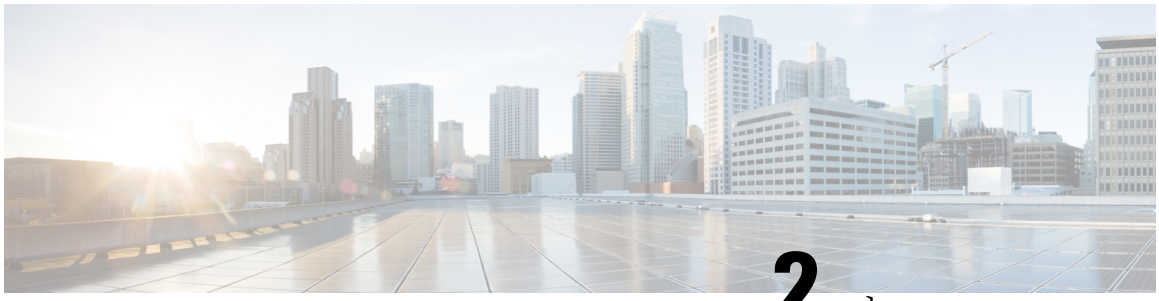
단계 4 필요에 따라 값을 편집하고 **Save(**저장**)**를 클릭합니다.

단계 5 개체가 현재 정책에서 사용 중인 경우 CDO는 변경의 영향을 받는 정책을 표시합니다. **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

단계 6 개체가 디바이스의 정책에서 사용되는 경우 변경 사항을 지금 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 여러 변경 사항을 여러 변경 사항을 한 번에 배포합니다.

관련 정보**:**

- 개체 삭제
- ASA 레거시 네트워크 정책



2 장

# 디바이스 및 서비스 온보딩

라이브 디바이스와 모델 디바이스를 모두 CDO에 온보딩할 수 있습니다. 모델 디바이스는 CDO를 사용하여 보고 편집할 수 있는 업로드된 구성 파일입니다.

대부분의 라이브 디바이스 및 서비스는 보안 디바이스 커넥터가 CDO를 디바이스 또는 서비스에 연결할 수 있도록 개방형 HTTPS 연결을 필요로 합니다.

SDC 및 해당 상태에 대한 자세한 내용은 SDC(Secure Device Connector), 5 페이지의 내용을 참조하십시오.

이 장에는 다음 섹션이 포함되어 있습니다.



# ASA 디바이스 온보딩

이 절차를 사용하여 ASA 모델이 아닌 단일 라이브 ASA 디바이스를 CDO에 온보딩합니다. 여러 ASA를 한 번에 온보딩하려면 대량 ASA 온보딩을 참조하십시오.

### Before you begin

디바이스 사전 요건

- 매니지드 디바이스에 Cisco Defense Orchestrator 연결, on page 6를 검토합니다.

- ASA의 실행 중인 구성 파일은 4.5MB 미만이어야 합니다. 실행 중인 구성 파일의 크기를 확인하려면 ASA 실행 구성 크기 확인을 참조하십시오.
- IP 주소 지정: 각 ASA, ASAv 또는 ASA 보안 상황에는 고유한 IP 주소가 있어야 하며 SDC는 관리 트래픽을 수신하도록 구성된 인터페이스에서 해당 상황에 연결해야 합니다.

인증서 사전 요건

ASA 디바이스에 호환되는 인증서가 없는 경우 디바이스 온보딩이 실패할 수 있습니다. 다음 요구 사항이 충족되었는지 확인하십시오.

- 디바이스에서 1.0 이상의 TLS 버전을 사용합니다.
- 디바이스에서 제시한 인증서가 만료되지 않았으며 발급 날짜가 과거입니다(즉, 이미 유효하며 나중에 유효해질 예정이 아님).
- 인증서는 SHA-256 인증서여야 합니다. SHA1 인증서는 허용되지 않습니다.
- 다음 조건 중 하나가 참입니다.
  - 디바이스가 자체 서명 인증서를 사용하며, 인증된 사용자가 신뢰하는 최신 인증서와 동일합니다.
  - 디바이스는 신뢰할 수 있는 CA(Certificate Authority)에서 서명한 인증서를 사용하며, 제공된 리프 인증서를 관련 CA에 연결하는 인증서 체인을 제공합니다.

온보딩 프로세스 중에 인증서 오류가 발생하는 경우 인증서 오류로 인해 ASA를 온보딩할 수 없음, on page 541에서 자세한 내용을 참조하십시오.

개방형 **SSL** 암호 사전 요건

디바이스에 호환되는 SSL 암호 그룹이 없으면 디바이스는 SDC(Secure Device Connector)와 성공적으로 통신할 수 없습니다. 다음 암호 그룹 중 하나를 사용합니다.

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA256
- DHE-RSA-AES256-SHA256

ASA에서 사용하는 암호 그룹이 이 목록에 없는 경우 SDC가 이를 지원하지 않으므로 ASA의 암호 그룹 업데이트해야 합니다.

단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** 파란색 더하기 버튼을  클릭하여 ASA를 온보딩합니다.

단계 **3** **ASA** 타일을 클릭합니다.

단계 **4** 디바이스 찾기 단계에서 다음을 수행합니다.

**a.** **Secure Device Connector(**보안 디바이스 커넥터**)** 버튼을 클릭하고 네트워크에 설치된 보안 디바이스 커넥터를 선택합니다. SDC를 사용하지 않으려는 경우 CDO는 클라우드 커넥터를 사용하여 ASA에 연결할 수 있습니다. 선택은 매니지드 디바이스에 Cisco Defense Orchestrator 연결하는 방법에 따라 달라집니다.

**b.** 디바이스에 이름을 지정합니다.

**c.** 디바이스 또는 서비스의 위치(IP 주소, FQDN 또는 URL)를 입력합니다. 기본 포트는 443입니다.

**d.** **Next(**다음**)**를 클릭합니다.

단계 **5** **Credentials(**자격 증명**)** 단계에서 CDO가 디바이스에 연결하는 데 사용할 ASA 관리자 또는 이와 유사한 최고 권한의 ASA 사용자의 사용자 이름 및 비밀번호를 입력하고 **Next(**다음**)**를 클릭합니다.

단계 **6** (선택 사항) 완료 단계에서 디바이스의 레이블을 입력합니다. 이 레이블을 기준으로 디바이스 목록을 필터링할 수 있습니다. 자세한 내용은 레이블 및 필터링을 참조하십시오.

단계 **7** 디바이스 또는 서비스에 레이블을 지정한 후에는 **Inventory(**재고 목록**)** 목록에서 볼 수 있습니다.

**Note** 구성의 크기 및 다른 디바이스 또는 서비스의 수에 따라 구성을 분석하는 데 시간이 걸릴 수 있습니다.

# 고가용성 쌍의 일부인 **ASA** 온보딩

고가용성 쌍의 일부인 ASA를 온보딩하는 경우 쌍의 기본 디바이스만 온보딩하는 데 ASA 디바이스 온보딩, on page 149를 사용합니다.

# 다중 상황 모드에서 **ASA** 온보딩

멀티컨텍스트 모드 정보

물리적 어플라이언스에 설치된 단일 ASA를 상황이라고 하는 여러 논리적 디바이스로 분할할 수 있습니다. 다중 상황 모드에서 구성된 ASA에는 다음과 같은 세 가지 구성이 사용됩니다.

- 보안 상황
- 관리 상황

- 시스템 구성

### 보안 상황 정보

각 보안 상황은 각자 보안 정책, 인터페이스, 관리자가 있는 독립적인 디바이스의 역할을 합니다. 다중 보안 상황은 여러 대의 독립형 디바이스가 있는 것과 비슷합니다. 보안 상황은 프라이빗 클라우드 인프라에 설치된 가상 머신 이미지와 같은 가상 ASA가 아닙니다. 보안 상황은 하드웨어 어플라이언스에 설치된 ASA에 구성됩니다. 각 상황은 해당 어플라이언스의 물리적 인터페이스에 구성됩니다.

다중 상황 모드에 대한 자세한 내용은 ASA CLI 및 ASDM 구성 가이드를 참조하십시오.

CDO는 각 보안 상황을 별도의 ASA로 온보딩하고 별도의 ASA인 것처럼 관리합니다.

### 관리 상황 정보

관리 상황은 보안 상황과 비슷하지만, 사용자가 관리 상황에 로그인하면 시스템 관리자 권한을 갖게 되어 시스템 및 그 밖의 모든 상황에 액세스할 수 있다는 점이 다릅니다. 관리 상황은 어떠한 제한도 받지 않으며, 일반 컨텍스트로 사용될 수 있습니다. 그러나 관리 상황에 로그인하면 모든 컨텍스트에 대한 관리자 권한이 부여되므로, 관리 상황 액세스 권한을 적합한 사용자로 한정할 필요가 있습니다.

CDO는 각 관리 상황을 별도의 ASA로 온보딩하고 별도의 ASA인 것처럼 관리합니다. 또한 CDO는 어플라이언스에서 ASA 및 ASDM 소프트웨어를 업그레이드할 때 관리 상황을 사용합니다.

### 시스템 구성 관련 정보

시스템 관리자는 시스템 구성에서 각 상황 컨피그레이션 위치, 할당된 인터페이스, 기타 상황 운영 매개 변수를 컨피그레이션함으로써 상황을 추가하고 관리합니다. 이는 단일 모드 컨피그레이션처럼 시작 컨피그레이션이 됩니다. 시스템 구성은 ASA를 위한 기본적인 설정을 나타냅니다. 시스템 구성은 자체 네트워크 인터페이스나 네트워크 설정을 포함하지 않습니다. 그보다는 시스템에서 네트워크 리소스에 액세스해야 할 때(예: 서버로부터 상황 다운로드) 관리 상황으로 지정된 상황 중 하나를 사용합니다.

CDO는 시스템 구성을 온보딩하지 않습니다.

### 보안 및 관리 상황에 대한 온보딩 사전 요건

보안 및 관리 상황 온보딩에 대한 사전 요건은 다른 ASA의 온보딩에서도 동일합니다. 사전 요건 목록은 ASA 디바이스 온보딩, 149 페이지의 내용을 참조하십시오.

다중 상황 모드에서 ASA를 지원하는 Cisco 어플라이언스를 알아보려면 실행 중인 ASA 소프트웨어 버전에 대한 *CLI 설명서 1: Cisco ASA 시리즈 일반 운영 CLI 구성 가이드*의 "다중 상황 모드" 장을 참조하십시오.

단일 상황 방화벽으로 실행되는 ASA와 다중 상황 방화벽의 관리 상황에서는 ASDM 및 CDO 액세스에 여러 포트 번호를 사용할 수 있습니다. 그러나 보안 상황의 경우 ASDM 및 CDO 액세스 포트는 포트 443으로 고정됩니다. 이는 ASA의 제한 사항입니다.

온보딩 **ASA** 보안 및 관리 상황

보안 상황 또는 관리 상황을 온보딩하는 방법은 다른 ASA를 온보딩하는 방법과 동일합니다. 온보딩 지침은 ASA 디바이스 온보딩, 149 페이지 또는 대량 ASA 온보딩, 153 페이지의 내용을 참조하십시오.

보안 상황 업그레이드

CDO는 다중 상황 ASA의 각 보안 및 관리 상황을 별도의 ASA로 취급하며, 각각은 개별적으로 온보딩됩니다. 그러나 다중 상황 ASA의 모든 보안 및 관리 상황은 어플라이언스에 설치된 동일한 버전의 ASA 소프트웨어를 실행합니다.

ASA의 보안 상황에서 사용하는 ASA 및 ASDM 버전을 업그레이드하려면 관리 상황을 온보딩하고 해당 상황에서 업그레이드를 수행합니다. 자세한 내용은 단일 ASA에서 ASA 및 ASDM 이미지 업그레이드, 161 페이지 또는 ASA 및 ASDM 대량 업그레이드, 158 페이지 ASA 및 ASDM 대량 업그레이드, 158 페이지의 내용을 참조하십시오.

# 대량 **ASA** 온보딩

CDO(Cisco Defense Orchestrator)를 사용하면 a.csv 파일에서 모든 ASA에 필요한 정보를 제공하여 ASA를 대량 온보딩할 수 있습니다. ASA가 온보딩되는 동안 필터 창을 사용하여 대기열에 있는 온보딩 시도, 로드 중, 완료 또는 실패한 온보딩 시도를 표시할 수 있습니다.

### Before you begin

- 매니지드 디바이스에 Cisco Defense Orchestrator 연결, on page 6를 검토합니다.
- 온보딩하려는 ASA의 연결 정보가 포함된 .csv 파일을 준비합니다. 한 줄의 ASA에 대한 정보를 추가합니다. 줄의 시작 부분에 #을 사용하여 코멘트를 나타낼 수 있습니다.
  - ASA 위치(IP 주소 또는 FQDN)
  - ASA 관리자 사용자 이름
  - ASA 관리자 비밀번호
  - (선택 사항) CDO의 디바이스 이름
  - SDCName 필드에 CDO를 ASA에 연결하는 데 사용할 네트워크의 SDC(Secure Device Connector) 이름을 지정합니다. SDC를 사용하여 ASA를 CDO에 연결하지 않으려는 경우에도 "none"을 입력할 수 있습니다. 디바이스를 온보딩할 때 SDCName 필드에 "none"을 지정하면 클라우드 커넥터를 사용하여 ASA를 온보딩합니다. 클라우드 커넥터를 사용하면 SDC를 설치하지 않고도 디바이스를 CDO에 연결할 수 있습니다. 선택은 매니지드 디바이스에 Cisco Defense Orchestrator 연결하는 방법에 따라 달라집니다.
  - (선택 사항) CDO용 디바이스 레이블
  - 하나의 레이블을 추가하려면 마지막 CSV 필드에 레이블 이름을 추가합니다.
  - 디바이스에 둘 이상의 레이블을 추가하려면 값을 따옴표로 묶습니다. 예: 알파, 베타, 감마.

- 범주 및 선택 항목 레이블을 추가하려면 콜론(:)으로 두 값을 구분합니다. 예를 들면 `Rack:50` 입니다.

구성 파일의 샘플:

```
#Location,Username,Password,DeviceName,SDCName,DeviceLabel
192.168.3.2,admin,CDO123!,ASA3,sdc1,"HA-1,Rack:50"
192.168.4.2,admin,CDO123!,ASA4,sdc1,"HA-1,Rack:50"
ASA2.example.com,admin,CDO123!,ASA2,none,Rack:51
asav.virtual.io,admin,CDO123!,ASA-virtual,sdc3,Test
```

**Caution** CDO는 .csv 파일의 데이터를 검증하지 않습니다. 항목의 정확성을 확인해야 합니다.

단계 **1** 내비게이션 바에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** 파란색 더하기 버튼 을 클릭하여 ASA를 온보딩합니다.

단계 **3** Onboarding(온보딩) 페이지에서 **Multiple ASAs(**여러 **ASA)** 타일을 클릭합니다.

단계 **4** **Browse(**찾아보기**)**를 클릭하여 ASA 항목이 포함된 .csv 파일을 찾습니다. 지정한 디바이스가 이제 ASA 대량 온보딩 테이블에 대기되어 온보딩할 준비가 되었습니다.

**Caution** 온보딩 프로세스가 완료될 때까지 ASA 대량 온보딩 페이지에서 다른 곳으로 이동하지 마십시오. 다른 곳으로 이동하면 온보딩 프로세스가 중지됩니다.

단계 **5** **Start(**시작**)**를 클릭합니다. ASA 대량 온보딩 테이블의 상태 열에서 온보딩 프로세스의 진행 상황을 확인할 수 있습니다. 디바이스가 성공적으로 온보딩되면 상태가 "Complete(완료)"로 변경됩니다.

### What to do next

대량 온보딩을 일시 중지하고 나중에 다시 시작해야 하는 경우 대량 온보딩 일시 중지 및 다시 시작, on page 154의 내용을 참조하십시오.

.

# 대량 온보딩 일시 중지 및 다시 시작

온보딩 프로세스를 일시 중지해야 하는 경우 **Pause(**일시 중지**)**를 클릭합니다. CDO가 온보딩을 시작한 모든 디바이스의 온보딩을 완료합니다. 벌크 온보딩 프로세스를 재개하려면 **Start(**시작**)**를 클릭합니다. CDO가 대기 중인 다음 디바이스의 온보딩을 시작합니다.

**Pause(**일시 중지**)**를 클릭하고 이 페이지에서 나가면 페이지로 돌아가 처음부터 대량 온보딩 절차를 다시 수행해야 합니다. 그러나 CDO는 이미 온보딩한 디바이스를 인식하고, 이 새 온보딩 시도의 디바이스를 중복으로 표시하며, 목록을 빠르게 이동하여 대기열에 있는 디바이스를 온보딩합니다.

# ASA 모델 생성 및 가져오기

단계 1 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.
단계 2 **Devices(**디바이스**)** 탭을 클릭합니다.
단계 3 **ASA** 탭을 클릭합니다.
단계 4 ASA 디바이스를 선택하고 왼쪽 창의 **Management(**관리**)**에서 **Configuration(**구성**)**을 클릭합니다.
단계 5 **Download(**다운로드**)**를 클릭하여 디바이스 컨피그레이션을 로컬 컴퓨터에 다운로드합니다.

# ASA 구성 가져오기

주의: ASA의 실행 중인 구성 파일은 4.5MB 미만이어야 합니다. 온보딩하기 전에 구성 파일의 크기를 확인합니다.

단계 1 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.
단계 2 파란색 더하기( ) 버튼을 클릭하여 구성을 가져옵니다.
단계 3 오프라인 관리를 위해 구성 가져오기를 클릭합니다.
단계 4 **Device Type(**장치 유형**)**을 **ASA**로 선택합니다.
단계 5 **Browse(**찾아보기**)**를 클릭하고 업로드할 구성 파일(텍스트 형식)을 선택합니다.
단계 6 구성이 확인되면 디바이스 또는 서비스에 레이블을 지정하라는 메시지가 표시됩니다. 자세한 내용은 레이블 및 필터링을 참조하십시오.
단계 7 모델 디바이스에 레이블을 지정한 후에는 **Devices & Services(**디바이스 및 서비스**)** 목록에서 볼 수 있습니다.

**Note** 구성의 크기 및 다른 디바이스 또는 서비스의 수에 따라 구성을 분석하는 데 시간이 걸릴 수 있습니다.

# CDO에서 디바이스 삭제

CDO에서 디바이스를 삭제하려면 다음 절차를 따르십시오.

단계 1 CDO에 로그인합니다.
단계 2 **Inventory(**인벤토리**)** 페이지로 이동합니다.
단계 3 삭제할 디바이스를 찾아 디바이스 행에서 디바이스를 확인하고 선택합니다.
단계 4 오른쪽에 있는 디바이스 작업 패널에서 **Remove(**제거**)**를 선택합니다.

단계 **5** 메시지가 표시되면 **OK(**확인**)**를 선택하여 선택한 디바이스 제거를 확인합니다. 디바이스를 온보딩 상태로 유지하려면 **Cancel(**취소**)**을 선택합니다.

# 오프라인 관리를 위한 디바이스 컨피그레이션 가져오기

오프라인 관리를 위해 디바이스의 구성을 가져오면 네트워크의 라이브 디바이스에서 작업하지 않고도 디바이스의 구성을 검토하고 최적화할 수 있습니다. CDO는 이러한 업로드된 구성 파일을 "모델"이라고도 합니다.

이러한 디바이스의 구성을 CDO로 가져올 수 있습니다.

- ASA(Adaptive Security Appliance) ASA 모델 생성 및 가져오기를 참조하십시오.
- FTD(Firepower Threat Defense)
- ASR(Aggregation Services Router) 및 ISR(Integrated Services Router)과 같은 Cisco IOS 디바이스

# ASA 및 ASDM 업그레이드 사전 요건

CDO(Cisco Defense Orchestrator)는 개별 ASA, 여러 ASA, 액티브-스탠바이 구성의 ASA, 단일 상황 또는 다중 상황 모드에서 실행 중인 ASA에 설치된 ASA 및 ASDM 이미지를 업그레이드하는 데 도움이 되는 마법사를 제공합니다.

CDO는 업그레이드할 수 있는 ASA 및 ASDM 이미지의 저장소를 유지 관리합니다. CDO의 이미지 저장소에서 업그레이드 이미지를 선택하면 CDO는 백그라운드에서 필요한 모든 업그레이드 단계를 수행합니다. 마법사는 호환 가능한 ASA 소프트웨어 및 ASDM 이미지를 선택하고 설치하고 디바이스를 재부팅하여 업그레이드를 완료하는 프로세스를 안내합니다. Cisco에서는 CDO에서 선택한 이미지가 ASA에 복사되고 설치된 이미지인지 확인하여 업그레이드 프로세스를 보호합니다. CDO는 주기적으로 ASA 이진 파일의 재고 목록을 검토하고 최신 ASA 및 ASDM 이미지가 있으면 해당 이미지를 저장소에 추가합니다. 이는 ASA에서 인터넷에 대한 아웃바운드 액세스 권한이 있는 고객에게 가장 적합한 옵션입니다.

CDO의 이미지 저장소에는 일반적으로 사용 가능한(GA) 이미지만 포함됩니다. 목록에 특정 GA 이미지가 표시되지 않으면 Cisco TAC에 문의하거나 지원 문의 페이지에서 지원팀에 이메일을 보내십시오. 설정된 지원 티켓 SLA를 사용하여 요청을 처리하고 누락된 GA 이미지를 업로드합니다.

ASA에서 인터넷에 대한 아웃바운드 액세스 권한이 없는 경우 Cisco.com에서 원하는 ASA 및 ASDM 이미지를 다운로드하여 자체 저장소에 저장하고 업그레이드 마법사에 해당 이미지에 대한 맞춤형 URL을 제공하면 CDO가 이러한 이미지를 사용하여 업그레이드를 수행합니다. 그러나 이 경우 업그레이드 대상 이미지를 결정합니다. CDO는 이미지 무결성 검사 또는 디스크 공간 검사를 수행하지 않습니다. FTP, TFTP, HTTP, HTTPS, SCP 및 SMB 프로토콜 중 하나를 사용하여 저장소에서 이미지를 검색할 수 있습니다.

모든 **ASA**에 대한 구성 사전 요건

- ASA에서 DNS를 활성화해야 합니다.
- CDO의 이미지 저장소에서 업그레이드 이미지를 사용하는 경우 ASA에서 인터넷에 연결할 수 있어야 합니다.
- ASA와 저장소 FQDN 간의 HTTPS 연결을 확인합니다.
- ASA가 CDO에 성공적으로 온보딩되었습니다.
- ASA가 CDO에 동기화됩니다.
- ASA가 온라인 상태입니다.
- 맞춤형 URL 업그레이드의 경우:
  - Cisco ASA 업그레이드 가이드를 사용하여 ASA와 호환되는 ASA 및 ASDM 버전을 확인합니다.
  - 이미지 저장소에 ASA 및 ASDM 이미지를 다운로드합니다.
  - ASA에서 이미지 저장소에 액세스할 수 있는지 확인합니다.
  - ASA 및 ASDM 이미지를 저장할 충분한 디스크 공간이 ASA에 있는지 확인합니다.
  - URL 구문 정보는 맞춤형 URL 업그레이드를 참조하십시오.

**Firepower 1000** 및 **Firepower 2100 Series** 디바이스에 대한 구성 사전 요건

- Firepower 2100 Series 디바이스의 FXOS 모드는 어플라이언스 모드로 구성되어야 합니다. 자세한 내용은 Firepower 2100을 어플라이언스 또는 플랫폼 모드로 설정을 참조하십시오.
- 디바이스에서 ASA 버전 9.13(1) 이상을 실행해야 합니다.
- ASA 소프트웨어를 업그레이드하기 전에 FXOS 번들을 업그레이드해야 합니다. 자세한 내용은 Firepower 2100 ASA 및 FXOS 호환성을 참조하십시오.

**ASA**를 실행하는 **Firepower 4100** 및 **Firepower 9300 Series** 디바이스

CDO는 Firepower 4100또는 Firepower 9300 Series 디바이스에 대한 업그레이드를 지원하지 않습니다. 이러한 디바이스는 CDO 외부에서 업그레이드해야 합니다.

업그레이드 지침

- CDO는 액티브/스탠바이 "페일오버" 쌍으로 구성된 ASA를 업그레이드할 수 있습니다. CDO는 액티브/액티브 "클러스터링된" 쌍으로 구성된 ASA를 업그레이드할 수 없습니다.

소프트웨어 및 하드웨어 사전 요건

업그레이드할 수 있는 최소 ASA 및 ASDM 버전:

- ASA: ASA 9.1.2
- ASDM: 최소 버전이 없습니다.

지원되는 하드웨어 버전

- CDO에서 지원하는 소프트웨어 및 하드웨어을 참조하십시오.

# ASA 및 ASDM 대량 업그레이드

단계 **1** ASA 및 ASDM 이미지 업그레이드에 대한 업그레이드 요구 사항 및 중요 정보는 ASA 및 ASDM 업그레이드 사전 요건을 검토하십시오.

**Note** ASA 1000 또는 2000 Series 디바이스를 업그레이드하는 경우 ASA 및 ASDM 업그레이드 사전 요건을 읽어보십시오.

단계 **2** (선택 사항) 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭하고 변경 로그에서 이 작업에 의해 업그레이드된 디바이스를 식별하는 변경 요청 관리을 생성합니다.

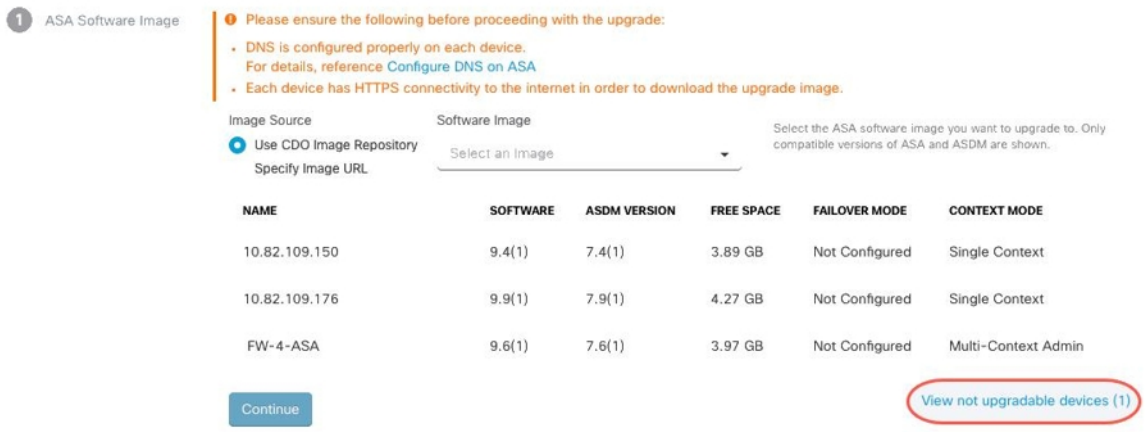
단계 **3** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **4** 필터를 사용하여 대량 업그레이드에 포함할 디바이스 목록을 좁힐 수 있습니다.

단계 **5** 필터링된 디바이스 목록에서 업그레이드할 디바이스를 선택합니다.

단계 **6** **Device Actions(**디바이스 작업**)** 창에서 **Upgrade(**업그레이드**)**를 클릭합니다.

단계 **7** Bulk Device Upgrade(대량 디바이스 업그레이드) 페이지에 업그레이드할 수 있는 디바이스가 표시됩니다. 선택한 디바이스 중 업그레이드할 수 없는 디바이스가 있으면 CDO에서 업그레이드할 수 없는 디바이스를 볼 수 있는 링크를 제공합니다.




단계 **8** 1단계에서 **Use CDO Image Repository(CDO** 이미지 저장소 사용**)**를 클릭하여 업그레이드할 ASA 소프트웨어 이미지를 선택하고 **Continue(**계속**)**를 클릭합니다.

이 목록에는 선택한 소프트웨어 버전으로 업그레이드할 수 있는 ASA의 수가 표시됩니다. 아래 예에서는 모든 디바이스를 버전 9.9(1.2)로 업그레이드할 수 있으며, 두 개의 디바이스를 9.8(2)로 업그레이드할 수 있으며, 디바이스 중 하나를 9.6(1)으로 업그레이드할 수 있습니다.


선택한 소프트웨어 버전이 선택한 디바이스와 호환되지 않는 경우 CDO에서 알림을 보냅니다. 아래 예에서 CDO는 10.82.109.176 디바이스를 이미 실행 중인 것보다 이전 버전으로 업그레이드할 수 없습니다.

| NAME | SOFTWARE | ASDM VERSION | FREE SPACE | FAILOVER MODE | CONTEXT MODE |
|---|---|---|---|---|---|
| ✔ 10.82.109.150 | 9.4(1) | 7.4(1) | 3.89 GB | Not Configured | Single Context |
| ✔ FW-4-ASA | 9.6(1) | 7.6(1) | 3.97 GB | Not Configured | Multi-Context Admin |
| ✖ 10.82.109.176 | 9.9(1) | 7.9(1) | 4.27 GB | Not Configured | Single Context |

단계 **9** 2단계에서 업그레이드할 ASDM 이미지를 선택합니다. 업그레이드할 수 있는 ASA와 호환되는 ASDM 선택 항목만 표시됩니다.

단계 **10** 3단계에서는 선택 사항을 확인하고 ASA에 이미지를 다운로드할지 아니면 이미지를 복사하여 설치하고 디바이스를 재부팅할지를 결정합니다.

단계 **11** 준비가 되면 **Perform Upgrade(**업그레이드 수행**)**를 클릭합니다.

**Note** 업그레이드가 실패하면 CDO에 메시지가 표시됩니다. 업그레이드 실패의 원인은 ASA 및 ASDM 이미지를 ASA로 전송하지 못하는 네트워크 문제인 경우가 많습니다.

단계 **12** 또는 CDO가 나중에 업그레이드를 수행하도록 하려면 Schedule Upgrade(업그레이드 예약) 확인란을 선택합니다. 미래의 날짜 및 시간을 선택하려면 필드를 클릭합니다. 완료되면 Schedule Upgrade(업그레이드 예약) 버튼을 클릭합니다.

단계 **13** (다중 상황 모드의 경우) 관리자 상황 및 보안 상황이 부팅된 후 보안 상황에 "새 인증서가 탐지되었습니다."라는 메시지가 표시될 수 있습니다. 이 메시지가 표시되면 모든 보안 상황에 대한 인증서를 수락합니다. 업그레이드로 인한 기타 변경 사항을 수락합니다.

단계 **14** 작업 페이지에서 대량 업그레이드 작업의 진행 상황을 확인합니다. 대량 업그레이드 작업의 성공 또는 실패에 대한 자세한 내용을 보려면 파란색 Review(검토) 링크를 클릭합니다. 그러면 작업 페이지로 이동합니다.

단계 **15** 변경 요청 레이블을 생성하고 활성화한 경우 실수로 다른 구성 변경 사항을 이 이벤트와 연결하지 않도록 레이블을 지워야 합니다.

# 자체 저장소의 이미지를 사용하여 여러 **ASA** 업그레이드

단계 **1** ASA 및 ASDM 이미지 업그레이드에 대한 업그레이드 요구 사항 및 중요 정보는 ASA 및 ASDM 업그레이드 사전 요건을 검토하십시오.

단계 **2** (선택 사항) 탐색 모음에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭하고 변경 로그에서 이 작업에 의해 업그레이드된 디바이스를 식별하는 변경 요청 관리을 생성합니다.

단계 **3** **Devices(**디바이스**)** 탭을 클릭합니다.

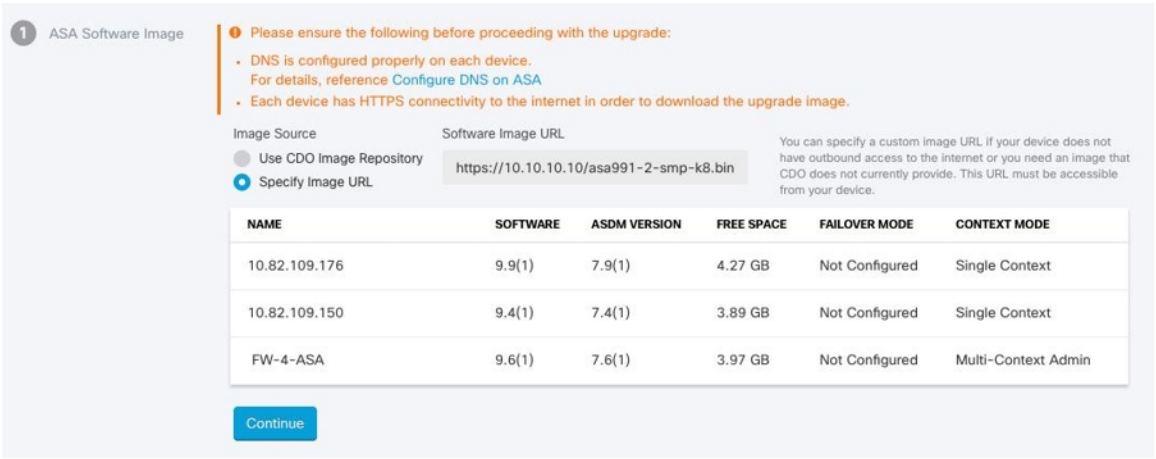
단계 **4** 필터, on page 88를 사용하여 대량 업그레이드에 포함할 디바이스 목록을 좁힐 수 있습니다.

단계 **5** 필터링된 디바이스 목록에서 업그레이드할 디바이스를 선택합니다.

단계 **6** **Device Actions(**디바이스 작업**)** 창에서 **Upgrade(**업그레이드**)**를 클릭합니다.

단계 **7** 1단계에서 **Specify Image URL(**이미지 **URL** 지정**)**을 클릭하고 **Software Image URL(**소프트웨어 이미지 **URL)** 필드에 업그레이드할 ASA 이미지의 URL을 입력한 후 **Continue(**계속**)**를 클릭합니다. URL 구문 정보는 맞춤형 URL 업그레이드를 참조하십시오.

**Note** 아래 그림은 소프트웨어 이미지 URL 필드의 HTTPS URL을 보여줍니다. FTP, TFTP, HTTP, HTTPS, SCP 및 SMB 프로토콜 중 하나를 사용하여 저장소에서 이미지를 검색할 수 있습니다. URL 구문 정보는 맞춤형 URL 업그레이드를 참조하십시오.




단계 **8** 2단계에서 **Specify Image URL(**이미지 **URL** 지정**)**을 클릭하고 **Software Image URL(**소프트웨어 이미지 **URL)** 필드에 업그레이드할 ASDM 이미지의 URL을 입력한 후 **Continue(**계속**)**를 클릭합니다.

단계 **9** 3단계에서는 선택 사항을 확인하고 ASA에 이미지를 다운로드할지 아니면 이미지를 복사하여 설치하고 디바이스를 재부팅할지를 결정합니다.

단계 **10** 준비가 되면 **Perform Upgrade(**업그레이드 수행**)**를 클릭합니다.

**Note** 업그레이드가 실패하면 CDO에 메시지가 표시됩니다. 업그레이드 실패의 원인은 ASA 및 ASDM 이미지를 ASA로 전송하지 못하는 네트워크 문제인 경우가 많습니다.

단계 **11** 또는 CDO가 나중에 업그레이드를 수행하도록 하려면 Schedule Upgrade(업그레이드 예약) 확인란을 선택합니다. 미래의 날짜 및 시간을 선택하려면 필드를 클릭합니다. 완료되면 Schedule Upgrade(업그레이드 예약) 버튼을 클릭합니다.

단계 **12** (다중 상황 모드의 경우) 관리자 상황 및 보안 상황이 부팅된 후 보안 상황에 "새 인증서가 탐지되었습니다."라는 메시지가 표시될 수 있습니다. 이 메시지가 표시되면 모든 보안 상황에 대한 인증서를 수락합니다. 업그레이드로 인한 기타 변경 사항을 수락합니다.

단계 **13** 작업 페이지에서 대량 업그레이드 작업의 진행 상황을 확인합니다. 대량 업그레이드 작업의 성공 또는 실패에 대한 자세한 내용을 보려면 파란색 Review(검토) 링크를 클릭합니다. 그러면 작업 페이지로 이동합니다.

단계 **14** 변경 요청 레이블을 생성하고 활성화한 경우 실수로 다른 구성 변경 사항을 이 이벤트와 연결하지 않도록 레이블을 지워야 합니다.

### What to do next

업그레이드 참고 사항

- Devices & Services(디바이스 및 서비스) 페이지를 열고 테이블의 Configuration Status(구성 상태) 열을 확인하여 업그레이드 배치의 진행 상황을 모니터링할 수도 있습니다.
- Devices & Services(디바이스 및 서비스) 페이지에서 해당 디바이스를 선택하고 업그레이드 버튼을 클릭하여 대량 업그레이드에 포함된 단일 디바이스의 진행 상황을 볼 수 있습니다. CDO에서 해당 디바이스의 Device Upgrade(디바이스 업그레이드) 페이지로 이동합니다.

# 단일 ASA에서 ASA 및 ASDM 이미지 업그레이드

단일 ASA에서 ASA 및 ASDM 이미지를 업그레이드하려면 다음 절차를 따르십시오.

단계 **1** ASA 및 ASDM 이미지 업그레이드에 대한 업그레이드 요구 사항 및 중요 정보는 ASA 및 ASDM 업그레이드 사전 요건을 검토하십시오.

**Note** ASA 1000 또는 2000 Series 디바이스를 업그레이드하는 경우 ASA 및 ASDM 업그레이드 사전 요건을 읽어보십시오.

단계 **2** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **3** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **4** (선택 사항) 변경 로그에서 이 작업에 의해 업그레이드된 디바이스를 식별하는 변경 요청 관리을 생성합니다.

단계 **5** 업그레이드할 디바이스를 선택합니다.

단계 **6** **Device Actions(**디바이스 작업**)** 창에서 **Upgrade(**업그레이드**)**를 클릭합니다.

단계 **7** Device Upgrade(디바이스 업그레이드) 페이지에서 마법사가 제공하는 지침을 따릅니다.

**a.** 1단계에서 **Use CDO Image Repository(CDO** 이미지 저장소 사용**)**를 클릭하여 업그레이드할 ASA 소프트웨어 이미지를 선택하고 **Continue(**계속**)**를 클릭합니다.

**Note** ASA 및 ASDM을 자체 저장소에 저장된 이미지로 업그레이드하는 경우 **Specify Image URL(**이미지 **URL** 지정**)**을 선택하고 Software Image URL(소프트웨어 이미지 URL) 필드에 ASA 또는 ASDM 이미지의 URL을 입력합니다. FTP, TFTP, HTTP, HTTPS, SCP 및 SMB 프로토콜 중 하나를 사용하여 저장소에서 이미지를 검색할 수 있습니다. URL 구문 정보는 맞춤형 URL 업그레이드를 참조하십시오.

(선택 사항) CDO가 나중에 업그레이드를 수행하도록 하려면 Schedule Upgrade(업그레이드 예약) 확인란을 선택합니다. 미래의 날짜 및 시간을 선택하려면 필드를 클릭합니다. 완료되면 **Schedule Upgrade(**업그레이드 예약**)**를 클릭합니다.

**b.** 2단계에서 업그레이드할 ASDM 이미지를 선택합니다. 업그레이드할 수 있는 ASA와 호환되는 ASDM 선택 항목만 표시됩니다.

**c.** 3단계에서는 선택 사항을 확인하고 ASA에 이미지를 다운로드할지 아니면 이미지를 복사하여 설치하고 디바이스를 재부팅할지를 결정합니다.

단계 **8** 준비가 되면 **Perform Upgrade(**업그레이드 수행**)**를 클릭합니다.

단계 **9** (다중 상황 모드의 경우) 관리자 상황 및 보안 상황이 부팅된 후 보안 상황에 "새 인증서가 탐지되었습니다."라는 메시지가 표시될 수 있습니다. 이 메시지가 표시되면 모든 보안 상황에 대한 인증서를 수락합니다. 업그레이드로 인한 기타 변경 사항을 수락합니다. 데모를 보고 싶으십니까? 이 절차의 스크린캐스트를 시청하십시오!

---

### What to do next

업그레이드 참고 사항

- 업그레이드할 이미지를 선택하고 마음이 바뀌면 소프트웨어 이미지와 연결된 **Skip Upgrade(**업그레이드 건너뛰기**)** 확인란을 선택합니다. 이미지가 디바이스에 복사되지 않으며 디바이스가 이미지와 함께 업그레이드되지도 않습니다.
- **Perform Upgrade(**업그레이드 수행**)** 단계에서 ASA에 이미지를 복사하기만 하려는 경우 나중에 Device Upgrade(디바이스 업그레이드) 페이지로 돌아가 "Upgrade Now(지금 업그레이드)"를 클릭하여 업그레이드를 수행할 수 있습니다. 복사 작업이 완료되면 Devices & Services(디바이스 및 서비스) 페이지에 해당 디바이스에 대한 "Ready to Upgrade(업그레이드 준비 완료)" 메시지가 표시됩니다.
- 이미지를 복사하고 설치하고 디바이스를 재부팅하는 동안에는 디바이스에서 작업을 수행할 수 없습니다. 이미지를 설치한 다음 재부팅하는 디바이스는 Devices & Services(디바이스 및 서비스) 페이지에 "Upgrading(업그레이드)"으로 표시됩니다.
- 업그레이드 프로세스 중에는 디바이스에서 작업을 수행할 수 없습니다. 즉, 이미지를 설치하고 디바이스를 재부팅합니다.
- 이미지를 디바이스에 복사하기만 선택한 경우 디바이스에서 작업을 수행할 수 있습니다. 이미지를 복사하는 디바이스는 Devices & Services(디바이스 및 서비스) 페이지에 "Copying Images(이미지 복사 중)"로 표시됩니다.
- 자체 서명 인증서가 있는 디바이스를 업그레이드하면 문제가 발생할 수 있습니다. 자세한 내용은 새 인증서 문제 트러블슈팅를 참조하십시오.

# 액티브/스탠바이 쌍의 **ASA** 및 **ASDM** 이미지 업그레이드

액티브/스탠바이 페일오버 모드에서 ASA 쌍을 업그레이드하기 전에 아래의 사전 요건을 검토하십시오. ASA를 구성하고 페일오버 모드에서 작동하는 방법에 대한 자세한 내용은 ASA 설명서에서 고가용성을 위한 페일오버를 참조하십시오.

데모를 보고 싶으십니까? 이 절차의 스크린캐스트를 시청하십시오.

사전 요건

- ASA 및 ASDM 이미지 업그레이드에 대한 요구 사항 및 중요 정보는 ASA 및 ASDM 업그레이드 사전 요건을 검토하십시오.
- 기본(액티브) 및 보조(스탠바이) ASA는 액티브/스탠바이 페일오버 모드에서 구성됩니다.
- 기본 ASA는 액티브/스탠바이 쌍의 액티브 디바이스입니다. 기본 ASA가 비활성 상태인 경우 CDO는 업그레이드를 수행하지 않습니다.
- 기본 및 보조 ASA 소프트웨어 버전은 동일합니다.

## 워크플로

이 프로세스에서는 CDO가 ASA의 활성/대기 쌍을 업그레이드합니다.

단계 **1** CDO는 ASA 및 ASDM 이미지를 두 ASA에 모두 다운로드합니다.

**Note** 사용자는 ASA 및 ASDM 이미지를 다운로드할 수 있지만, 바로 업그레이드할 수는 없습니다. ASA 및 ASDM 이미지를 이전에 다운로드한 경우 CDO는 해당 이미지를 다시 다운로드하지 않습니다. CDO는 이 다음 단계로 업그레이드 워크플로를 계속 진행합니다.

단계 **2** CDO는 보조 ASA를 먼저 업그레이드합니다.

단계 **3** 업그레이드가 완료되고 보조 ASA가 "Standby-Ready(대기 준비)" 상태로 돌아가면 CDO에서 페일오버를 시작하여 보조 ASA가 활성 ASA가 되도록 합니다.

단계 **4** CDO는 현재 대기 ASA인 기본 ASA를 업그레이드합니다.

단계 **5** 기본 ASA가 "Standby-Ready(대기 준비)" 상태로 돌아가면 CDO가 페일오버를 시작하여 기본 ASA가 활성 ASA가 되도록 합니다.

**Warning** 자체 서명 인증서가 있는 디바이스를 업그레이드하면 문제가 발생할 수 있습니다. 자세한 내용은 새 인증서 문제 트러블슈팅를 참조하십시오.

# 액티브/스탠바이 쌍의 **ASA** 및 **ASDM** 이미지 업그레이드

단계 **1** CDO에 로그인합니다.

단계 **2** **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **3** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **4** 업그레이드할 디바이스를 선택합니다.

단계 **5** **Device Actions(**디바이스 작업**)** 창에서 **Upgrade(**업그레이드**)**를 클릭합니다.

디바이스의 장애 조치 모드는 Active/Standby(활성/대기)입니다.


단계 **6** Device Upgrade(디바이스 업그레이드) 페이지에서 마법사가 제공하는 지침을 따릅니다.

**Note** ASA 및 ASDM을 자체 저장소에 저장된 이미지로 업그레이드하는 경우 **Specify Image URL(**이미지 **URL** 지정**)**을 선택하고 Software Image URL(소프트웨어 이미지 URL) 필드에 ASA 또는 ASDM 이미지의 URL을 입력합니다. FTP, TFTP, HTTP, HTTPS, SCP 및 SMB 프로토콜 중 하나를 사용하여 저장소에서 이미지를 검색할 수 있습니다. URL 구문 정보는 맞춤형 URL 업그레이드를 참조하십시오.

# 맞춤형 **URL** 업그레이드

새 ASA 소프트웨어 및 ASDM 이미지로 ASA를 업그레이드하는 경우 CDO(Cisco Defense Orchestrator)에서 이미지 저장소에 저장한 이미지를 사용하거나 자체 이미지 저장소에 저장한 이미지를 사용할 수 있습니다. ASA에 인터넷에 대한 아웃바운드 액세스가 없는 경우, CDO를 사용하여 ASA를 업그레이드하는 가장 좋은 방법은 자체 이미지 저장소를 유지하는 것입니다.

CDO는 ASA의 copy 명령을 사용하여 이미지를 검색하고 ASA의 플래시 드라이브(disk0:/)에 복사합니다. Specify Image URL(이미지 URL 지정) 필드에서 copy 명령의 URL 부분을 제공합니다. 예를 들어 전체 copy 명령은 다음과 같습니다.

```
ciscoasa# copy ftp://admin:adminpass@10.10.10.10/asa991-smp-k8.bin disk:/0
```

다음을 제공합니다.

```
ftp://admin:adminpass@10.10.10.10/asa991-smp-k8.bin
```

Specify Image URL(이미지 URL 지정) 필드에 입력합니다.

CDO는 업그레이드 이미지를 검색하는 http, https, ftp, tftp, smb 및 scp 방법을 지원합니다.

### URL 구문 예

다음은 ASA copy 명령에 대한 URL 구문의 예입니다. 이러한 URL 예에서는 다음을 가정합니다.

- 이미지 저장소 주소: 10.10.10.10
- 이미지 저장소에 액세스하기 위한 사용자 이름: admin
- 비밀번호: adminpass
- 경로: images/asa
- 이미지 파일 이름: asa991-smp-k8.bin

**http**[**s**]**://** [[ *user* [ **:** *password* ] **@** ] *server* [ **:** *port* ] **/** [ *path* **/** ] *filename* ]

https://admin:adminpass@10.10.10.10:8080/images/asa/asa991-smp-k8.bin
**HTTP[s] example without a username and password:**
https://10.10.10.10:8080/images/asa/asa991-smp-k8.bin

**ftp://** [[ *user* [ **:** *password* ] **@** ] *server* [**:** *port* ] **/** [ *path* **/** ] *filename* [ **;type=** *xx* ]]â€"The **type** 은 **ap**(ASCII 패시브 모드),**an**(ASCII 일반 모드), **ip**(기본 바이너리 패시브 모드), **in**(바이너리 일반 모드)과 같은 키워드 중 하나일 수 있습니다.

ftp://admin:adminpass@10.10.10.10:20/images/asa/asa991-smp-k8.bin
**FTP example without a username and password:**
ftp://10.10.10.10:20/images/asa/asa991-smp-k8.bin

**tftp://** [[ *user* [ **:** *password* ] **@** ] *server* [ **:** *port* ] **/** [ *path* **/** ] *filename* [ **;int=** *interface_name* ]]

tftp://admin:adminpass@10.10.10.10/images/asa/asa991-smp-k8.bin outside
**TFTP example without a username and password:**
tftp://10.10.10.10/images/asa/asa991-smp-k8.bin outside

**Note** 경로 이름은 공백을 포함할 수 없습니다. 경로 이름에 공백이 있으면 **copy tftp** 명령 대신 **tftp-server** 명령에서 경로를 설정합니다. **;int=** *interface* 옵션은 경로 조회를 건너뛰고 항상 지정된 인터페이스를 사용하여 TFTP 서버에 연결합니다.

**smb:**/[[ *path* **/** ] *filename* ] - UNIX 서버 로컬 파일 시스템을 표시합니다.

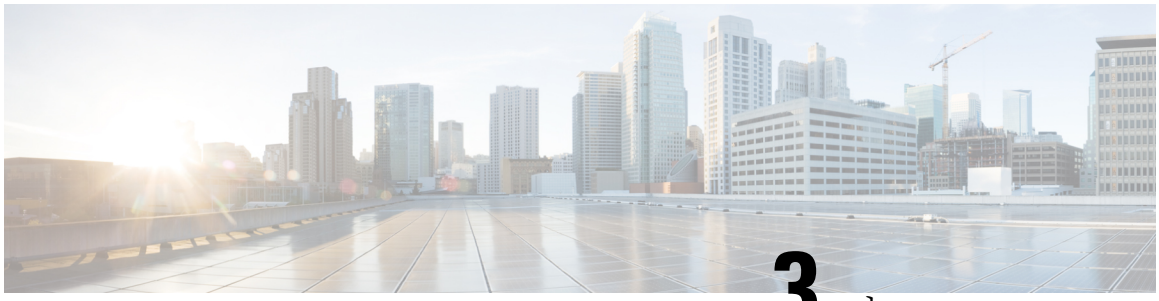
smb:/images/asa/asa991-smp-k8.bin

**scp://** [[ *user* [ **:** *password* ] **@** ] *server* [ **/** *path* ] **/** *filename* [ **;int=** *interface_name* ]]â€"The**;int=** *interface* 옵션은 경로 조회를 건너뛰고 항상 지정된 인터페이스를 사용하여 SCP(Secure Copy) 서버에 연결합니다.

scp://admin:adminpass@10.10.10.10:8080/images/asa/asa991-smp-k8.bin outside
**SCP example without a username and password:**
scp://10.10.10.10:8080/images/asa/asa991-smp-k8.bin outside

Cisco ASA Series 명령 참조, A~H 명령 가이드의 URL 구문이 포함된 전체 copy 명령.

맞춤형 URL을 사용하여 ASA 및 ASDM 이미지를 업그레이드하는 방법에 대한 자세한 내용은 ASA 및 ASDM 업그레이드 사전 요건을 참조하십시오.



3 장

# ASA 디바이스 구성

이 장에는 다음 섹션이 포함되어 있습니다.

# ASA 연결 자격 증명 업데이트

ASA를 온보딩하는 과정에서 CDO가 디바이스에 연결하는 데 사용해야 하는 사용자 이름 및 비밀번호를 입력했습니다. 디바이스에서 해당 자격 증명이 변경된 경우 **Update Credentials(**자격 증명 업데이트**)** 디바이스 작업을 사용하여 CDO에서도 해당 자격 증명을 업데이트하십시오. 이 기능을 사용하면 디바이스를 다시 등록하지 않고도 CDO에서 자격 증명을 업데이트할 수 있습니다. 전환할 사용자 이름과 암호 조합은 해당 사용자의 ASA 또는 AAA(Authentication, Authorization, and Accounting) 서버에 이미 존재해야 합니다. 이 프로세스는 Cisco Defense Orchestrator 데이터베이스에만 영향을 미칩니다. 자격 증명 업데이트 기능을 사용할 때 ASA 구성이 변경되지 않습니다.

단계 **1** 탐색 모음에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**장치**)** 탭을 클릭한 다음 **ASA**를 클릭합니다.

단계 **3** 업데이트할 연결 자격 증명이 있는 ASA를 선택합니다. 한 번에 하나 이상의 ASA에서 자격 증명을 업데이트할 수 있습니다.

단계 **4** **Device Actions(**장치 작업**)** 창에서 **Update Credentials(**자격 증명 업데이트**)**를 클릭합니다.

단계 **5** ASA를 CDO에 연결하는 데 사용하는 Cloud Connector 또는 SDC(보안 디바이스 커넥터)를 선택합니다.

단계 **6** ASA에 연결하는 데 사용할 새 사용자 이름 및 비밀번호를 입력합니다.

단계 **7** 자격 증명이 변경된 후 CDO는 디바이스를 동기화합니다.

참고 CDO가 디바이스를 동기화하지 못하면 CDO의 연결 상태에 "Invalid Credentials(유효하지 않은 자격 증명)"가 표시될 수 있습니다. 이 경우 유효하지 않은 사용자 이름과 비밀번호 조합을 사용하려고 시도했을 수 있습니다. 사용하려는 자격 증명이 ASA 또는 AAA 서버에 저장되어 있는지 확인하고 다시 시도하십시오.

# SDC 간에 ASA 이동

CDO는 단일 CDO 테넌트에서 여러 SDC 사용 다음 절차를 사용하여 한 SDC에서 다른 SDC로 관리형 ASA를 이동할 수 있습니다.

단계 **1** CDO 메뉴 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** 다른 SDC로 이동하려는 ASA를 선택합니다.

단계 **3** Device Actions(디바이스 작업) 창에서 **Update Credentials(**자격 증명 업데이트**)**를 클릭합니다.

단계 **4** 보안 디바이스 커넥터 버튼을 클릭하고 디바이스를 이동하려는 SDC를 선택합니다.

단계 **5** ASA를 온보딩하는 데 사용한 관리자 사용자 이름 및 비밀번호를 입력하고 Update(업데이트)를 클릭합니다. 이러한 변경 사항을 디바이스에 구축할 필요는 없습니다.

# 개체

개체는 하나 이상의 보안 정책에서 사용할 수 있는 정보의 컨테이너입니다. 개체를 사용하면 정책 일관성을 쉽게 유지할 수 있습니다. 단일 개체를 만들고 다른 정책을 사용하고 개체를 편집할 수 있으며 해당 변경 사항은 개체를 사용하는 모든 정책에 전파됩니다. 개체가 없는 경우 동일한 변경이 필요한 모든 정책을 개별적으로 편집해야 합니다.

디바이스를 온보딩하면, CDO는 해당 디바이스에서 사용하는 모든 개체를 인식하고, 저장한 다음, **Objects(**개체**)** 페이지에 나열합니다. **Objects(**개체**)** 페이지에서 기존 개체를 편집하고 보안 정책에 사용할 새 개체를 생성할 수 있습니다.

CDO은 여러 디바이스에서 사용되는 개체를 **shared object(**공유 개체**)**라고 부르고 **Objects(**개체**)** 페이지에서 이 배지 로 식별합니다.

때때로 공유 개체는 일부 "문제"를 발생시키고 더 이상 여러 정책 또는 디바이스에서 완벽하게 공유되지 않습니다.

- **Duplicate objects(**중복 개체**)**는 이름은 다르지만 값은 같은 동일한 디바이스에 있는 두 개 이상의 개체입니다. 이러한 개체는 일반적으로 비슷한 용도로 사용되며 다른 정책에서 사용됩니다. 중복 개체는 다음 문제 아이콘로 식별됩니다.
- **Inconsistent objects(**일관성 없는 개체**)** 는 이름은 같지만 값이 다른 두 개 이상의 디바이스에 있는 개체입니다. 때로는 사용자가 동일한 이름과 콘텐츠로 다른 구성으로 개체를 생성하지만 시간이 지남에 따라 이러한 개체의 값이 달라져 불일치가 발생합니다. 일관성 없는 개체는 다음 문제 아이콘로 식별됩니다.
- 사용되지 않는 개체는 디바이스 구성에 존재하지만 다른 개체, 액세스 목록 또는 NAT 규칙에서 참조하지 않는 개체입니다. 사용되지 않는 개체는 다음 문제 아이콘로 식별됩니다.

규칙 또는 정책에서 즉시 사용할 개체를 생성할 수도 있습니다. 규칙 또는 정책과 연결되지 않은 개체를 생성할 수 있습니다. 규칙이나 정책에서 연결되지 않은 개체를 사용하는 경우, CDO는 해당 개체의 복사본을 생성하고 해당 복사본을 사용합니다.

**Objects(**개체**)** 메뉴로 이동하거나 네트워크 정책의 세부 정보에서 확인하여 CDO에 의해 관리되는 개체를 볼 수 있습니다.

CDO은 한 위치에서 지원되는 디바이스 전체에 걸쳐 네트워크 및 서비스 개체를 관리할 수 있습니다. CDO에서는 다음과 같은 방법으로 개체를 관리할 수 있습니다.

- 다양한 기준에 따라 모든 개체를 검색하고 개체 필터합니다.
- 디바이스에서 중복되거나, 사용되지 않거나, 일관성이 없는 개체를 찾고 이러한 개체 문제를 통합, 삭제 또는 해결하십시오.
- 연결되지 않은 개체를 찾아 사용하지 않는 경우 삭제합니다.
- 여러 디바이스에서 공통적인 공유 개체를 검색합니다.
- 변경 사항을 커밋하기 전에 일련의 정책 및 디바이스에 대한 개체 변경 사항의 영향을 평가합니다.
- 다양한 정책 및 디바이스와 개체 및 개체의 관계 집합을 비교합니다.
- CDO에 온보딩된 후 디바이스에서 사용 중인 개체를 캡처합니다.

온보딩된 디바이스에서 개체를 생성, 편집 또는 읽는 데 문제가 있는 경우 자세한 내용은 문제 해결 Cisco Defense Orchestrator, on page 569를 참조하십시오.

# 개체 유형

다음 표에서는 CDO를 사용하여 디바이스에 대해 생성하고 관리할 수 있는 개체에 대해 설명합니다.

***Table 14: ASA(Adaptive Security Appliance)*** 개체 유형

| 개체 | 설명 |
|---|---|
| IP 주소 풀 생성 | 개별 IPv4 또는 IPv6 주소 또는 IP 주소 범위와 일치하도록 주소 풀 개체를 구성할 수 있습니다. |

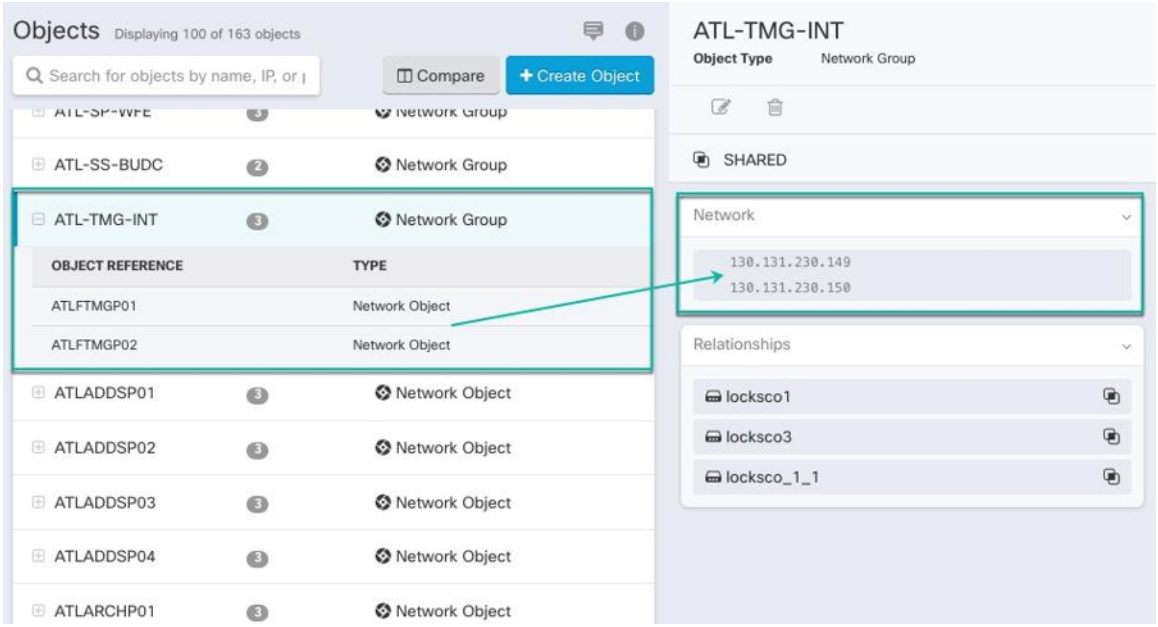
| 개체 | 설명 |
| --- | --- |
| RA VPN AnyConnect 클라이언트 프로파일 업로드 | AnyConnect 클라이언트 프로파일 개체는 파일 개체이며 구성(일반적으로 원격 액세스 VPN 정책)에서 사용되는 파일을 나타냅니다. AnyConnect 클라이언트 프로파일 및 AnyConnect 클라이언트 이미지 파일을 포함할 수 있습니다. |
| 네트워크 개체 | 네트워크 그룹과 네트워크 개체(네트워크 개체로 총칭함)는 호스트 또는 네트워크의 주소를 정의합니다. |
| 서비스 개체 | 서비스 개체, 서비스 그룹 및 포트 그룹은 TCP/IP 프로토콜 제품군의 일부로 간주되는 프로토콜 또는 포트를 포함하는 재사용 가능한 구성 요소입니다. |
| ASA 시간 범위 개체 | 시간 범위 개체는 특정 시간을 정의하며 시작 시간, 종료 시간, 선택 사항인 반복 항목으로 구성됩니다. 네트워크 정책에서 이 개체를 사용하여 특정 기능 또는 자산에 대한 시간 기반 액세스를 제공합니다. |
| 트러스트 포인트 개체 | 신뢰 지점을 사용하여 ASA에서 디지털 인증서를 관리하고 추적할 수 있습니다. |

# 공유 개체

CDO(Cisco Defense Orchestrator)는 이름과 콘텐츠가 동일한 여러 디바이스의 개체인 공유 개체를 호출합니다. 공유 개체는 이 아이콘으로 식별됩니다.

**Objects(**개체**)** 페이지에서 공유 개체를 사용하면 한 곳에서 개체를 수정할 수 있으며 변경 사항은 해당 개체를 사용하는 다른 모든 정책에 영향을 미치므로 정책을 쉽게 유지 관리할 수 있습니다. 공유 개체가 없으면 동일한 변경이 필요한 모든 정책을 개별적으로 수정해야 합니다.

공유 개체를 볼 때 CDO는 개체 테이블에 있는 개체의 내용을 표시합니다. 공유 개체는 정확히 동일한 내용을 갖습니다. CDO는 세부 정보 창에서 개체 요소의 결합된 보기 또는 "평평한" 보기를 보여줍니다. 세부 정보 창에서 네트워크 요소는 간단한 목록으로 병합되며 명명된 개체와 직접 연결되지 않습니다.

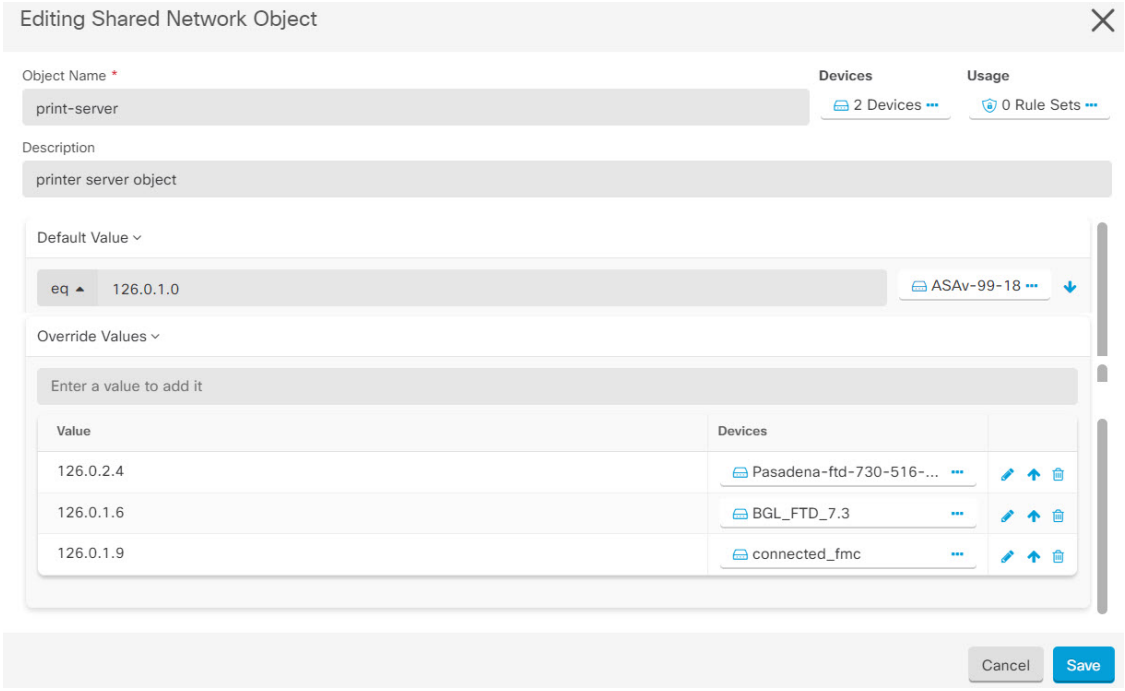



# 개체 재정의

개체 오버라이드를 사용하면 특정 디바이스에서 공유 네트워크 개체의 값을 오버라이드할 수 있습니다. CDO는 오버라이드를 구성할 때 지정한 디바이스에 해당하는 값을 사용합니다. 이름은 같지만 값이 다른 두 개 이상의 디바이스에 있는 개체에 대하여 CDO는 이러한 값이 오버라이드 되기 때문에 **Inconsistent objects(**일관성 없는 개체**)**로 식별하지 않습니다.

대부분의 디바이스에 대한 정의가 해당하는 개체를 생성하고 다른 정의가 필요한 일부 디바이스의 개체에 대한 특정 변경 사항을 지정하는 오버라이드를 사용할 수 있습니다. 모든 디바이스에 오버라이드가 필요한 개체를 생성할 수도 있습니다. 하지만 이 경우 모든 디바이스에 단일 정책을 생성할 수 있습니다. 개체 오버라이드는 필요한 경우 개별 디바이스의 정책을 바꾸지 않고도 디바이스 전반에 걸쳐 사용이 가능한 작은 공유 정책 집합을 생성하도록 합니다.

예를 들어 각 사무실에 .프린터 서버가 있고, 프린터 서버 개체인 `print-server`를 만든 시나리오를 생각해 보십시오. ACL에는 프린터 서버가 인터넷에 액세스하는 것을 거부하는 규칙이 있습니다. 프린터 서버 개체에는 한 사무실에서 다른 사무실로 변경하려는 기본값이 있습니다. 값이 다를 수 있지만 개체 오버라이드를 사용하고 규칙과 "프린터-서버" 개체를 모든 위치에서 일관되게 유지함으로써 이 작업을 수행할 수 있습니다.



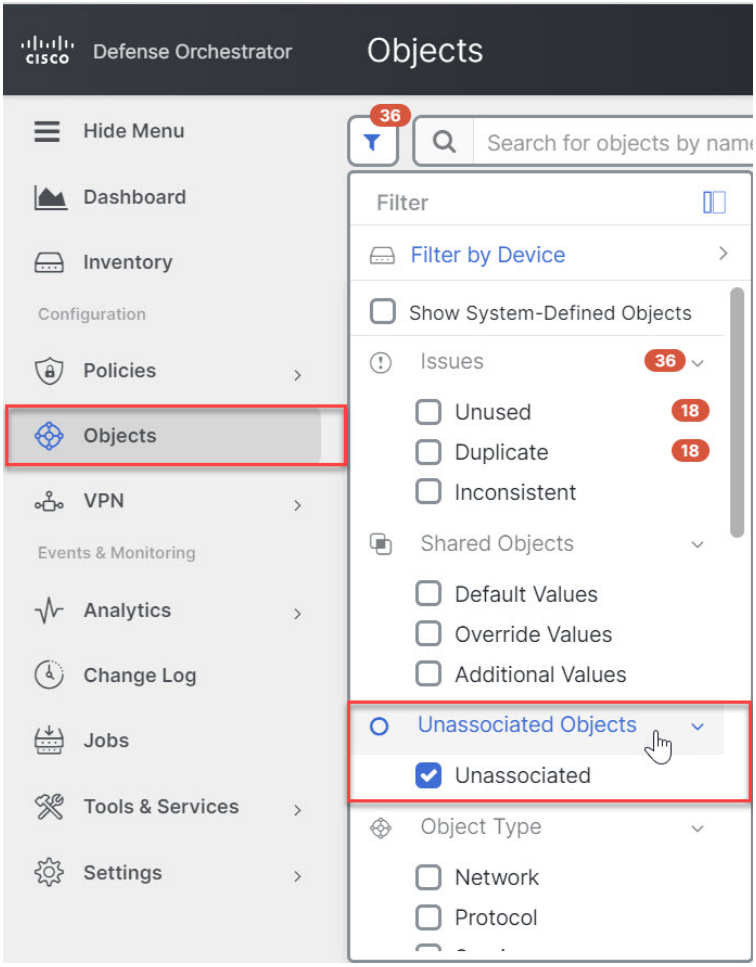

**Note** 일관되지 않은 개체가 있는 경우 오버라이드를 통해 개체를 단일 공유 개체로 결합할 수 있습니다. 자세한 내용은 불일치 개체 문제 해결, on page 575를 참조하십시오.

# 연결 해제된 개체

규칙 또는 정책에서 즉시 사용할 개체를 생성할 수 있습니다. 규칙이나 정책과 연결되지 않은 개체를 생성할 수도 있습니다. 규칙이나 정책에서 연결되지 않은 개체를 사용할 때, CDO는 해당 개체의 사본을 생성하고 해당 사본을 사용합니다. 연결되지 않은 원래 개체는 야간 유지 관리 작업에 의해 삭제되거나 사용자가 삭제할 때까지 사용 가능한 개체 목록에 남아 있습니다.

개체와 연결된 규칙 또는 정책이 실수로 삭제된 경우 모든 구성이 손실되지 않도록 연결되지 않은 개체는 사본으로 CDO에 남아 있습니다.

연결되지 않은 개체를 보려면 개체 탭의 왼쪽 창에서 를 클릭하고 **Unassociated (**연결되지 않음**)** 확인란을 선택합니다.




# 개체 비교

단계 **1** 왼쪽의 CDO 탐색 바에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 페이지에서 개체를 필터링하여 비교하려는 개체를 찾습니다.

단계 **3** **Compare(**비교**)** 버튼 Compare를 클릭합니다.

단계 **4** 비교할 개체를 최대 3개까지 선택합니다.

단계 **5** 화면 하단에서 개체를 나란히 봅니다.

- 개체 세부 정보 제목 표시줄에서 위쪽 및 아래쪽 화살표를 클릭하면 개체 세부 정보를 더 많이 또는 더 적게 볼 수 있습니다.
- 세부 정보 및 관계 상자를 확장하거나 축소하여 더 많거나 적은 정보를 확인합니다.

단계 **6** (선택 사항) 관계 상자는 개체가 사용되는 방식을 보여줍니다. 디바이스 또는 정책과 연결될 수 있습니다. 개체가 디바이스와 연결된 경우 디바이스 이름을 클릭한 다음 **View Configuration(**구성 보기**)**을 클릭하여 디바이스 구성을 볼 수 있습니다. CDO는 디바이스의 구성 파일을 표시하고 해당 개체에 대한 항목을 강조 표시합니다.

# 필터

**Inventory(**재고 목록**)** 및 **Objects(**개체**)** 페이지에서 다양한 필터를 사용하여 원하는 디바이스 및 개체를 찾을 수 있습니다.

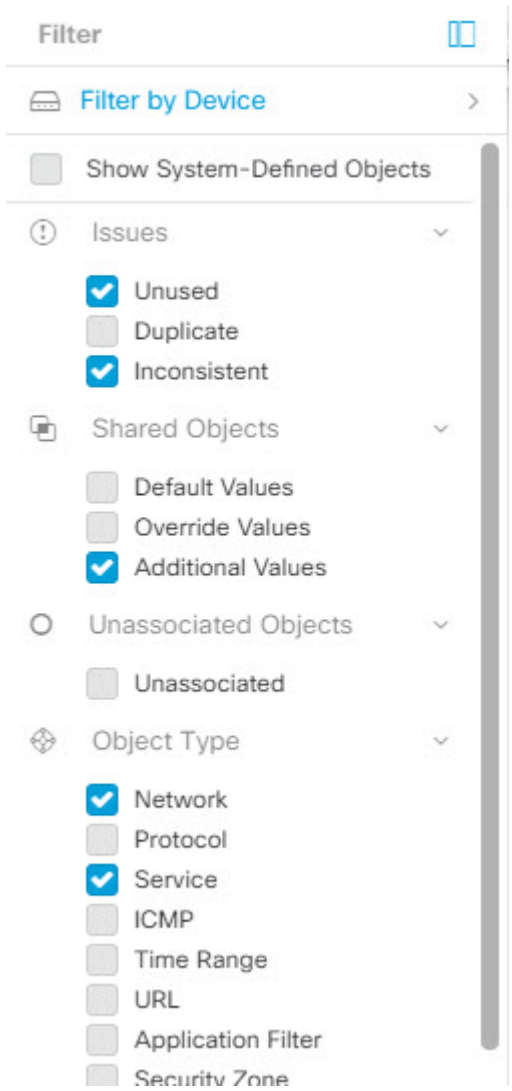
필터링하려면 Devices and Services(디바이스 및 서비스), Policies(정책) 및 Objects(개체) 탭의 왼쪽 창에서 을 클릭합니다.

Inventory(재고 목록) 필터를 사용하면 디바이스 유형, 하드웨어 및 소프트웨어 버전, snort 버전, 구성 상태, 연결 상태, 충돌 탐지, 보안 디바이스 커넥터 및 레이블을 기준으로 필터링할 수 있습니다. 필터를 적용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다. 필터를 사용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다.

개체 필터를 사용하면 디바이스, 문제 유형, 공유 개체, 연결되지 않은 개체 및 개체 유형을 기준으로 필터링할 수 있습니다. 결과에 시스템 개체를 포함하거나 포함하지 않을 수 있습니다. 또한 검색 필드를 사용하여 필터 결과에서 특정 이름, IP 주소 또는 포트 번호를 포함하는 개체를 검색할 수 있습니다.

디바이스 및 개체를 필터링할 때 검색 용어를 결합하여 몇 가지 잠재적 검색 전략을 생성하여 관련 결과를 찾을 수 있습니다.

다음 예제에서는 "문제(사용되었거나 일관성 없음)" 및 추가 값이 있는 공유 개체 및 네트워크 또는 서비스 유형의 개체 검색에 필터를 적용합니다.




# 개체 필터

필터링하려면 Objects(개체) 탭의 왼쪽 창에서 을(를) 클릭합니다.

- **All Objects(**모든 개체**)** - 이 필터는 CDO에 온보딩된 모든 디바이스에서 사용 가능한 모든 개체를 제공합니다. 이 필터는 모든 개체를 찾아보거나 하위 필터를 검색하거나 추가로 적용하기 위한 시작점으로 유용합니다.
- **Shared Objects(**공유 개체**)** - 이 빠른 필터는 CDO가 두 개 이상의 디바이스에서 공유하는 것으로 확인한 모든 개체를 표시합니다.
- **Objects By Device(**디바이스별 개체**)** - 선택한 디바이스에 있는 개체를 볼 수 있도록 특정 디바이스를 선택할 수 있습니다.

하위 필터 – 각 기본 필터에는 선택 범위를 좁히기 위해 적용할 수 있는 하위 필터가 있습니다. 이러한 하위 필터는 네트워크, 서비스, 프로토콜 등의 개체 유형을 기반으로 합니다.

이 필터 표시줄에서 선택한 필터는 다음 기준과 일치하는 개체를 반환합니다.

* 두 디바이스 중 하나에 있는 개체. (디바이스를 지정하려면 **Filter by Device(**디바이스별 필터링**)**를 클릭합니다.) AND는

* 일치하지 않는 개체 AND는

* 네트워크 개체 또는 서비스 개체 AND

* 개체 명명 규칙에 "**group**"이라는 단어가 있습니다.

**Show System Objects(**시스템 개체 표시**)**를 선택했으므로 결과에 시스템 개체와 사용자 정의 개체가 모두 포함됩니다.

시스템 개체 필터 표시

일부 디바이스는 공통 서비스에 대해 사전 정의된 개체가 함께 제공됩니다. 이러한 시스템 개체는 이미 생성되어 규칙 및 정책에서 사용할 수 있으므로 편리합니다. 개체 테이블에는 여러 시스템 개체가 있을 수 있습니다. 시스템 개체는 편집하거나 삭제할 수 없습니다.

**Show System Objects(**시스템 개체 표시**)**는 기본적으로 꺼져 있습니다. 개체 테이블에 시스템 개체를 표시하려면 필터 표시줄에서 **Show System Objects(**시스템 개체 표시**)**를 선택합니다. 개체 테이블에서 시스템 개체를 숨기려면 필터 표시줄에서 Show System Objects(시스템 개체 표시)를 선택하지 않은 상태로 둡니다.

시스템 개체를 숨기면 검색 및 필터링 결과에 포함되지 않습니다. 시스템 개체를 표시하면 개체 검색 및 필터링 결과에 포함됩니다.

## 개체 필터 구성

원하는 만큼 기준을 필터링할 수 있습니다. 더 많은 범주를 필터링할수록 예상되는 결과는 줄어듭니다.

단계 **1** 왼쪽의 CDO 탐색 바에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 페이지 상단의 필터 아이콘 을 클릭하여 필터 패널을 엽니다. 선택한 필터를 선택 취소하여 실수로 필터링된 개체가 없는지 확인합니다. 또한 검색 필드를 살펴보고 검색 필드에 입력되었을 수 있는 텍스트를 삭제합니다.

단계 **3** 특정 디바이스에 있는 것으로 결과를 제한하려면 다음을 수행합니다.

**a.** **Filter By Device(**디바이스별 필터링**)**를 클릭합니다.

**b.** 모든 디바이스를 검색하거나 디바이스 탭을 클릭하여 특정 종류의 디바이스만 검색합니다.

**c.** 필터 기준에 포함할 디바이스를 선택합니다.

**d.** **OK(**확인**)**를 클릭합니다.

단계 **4** 검색 결과에 시스템 개체를 포함하려면 **Show System Objects(**시스템 개체 표시**)**를 선택합니다. 검색 결과에서 시스템 개체를 제외하려면 **Show System Objects(**시스템 개체 표시**)**의 선택을 취소합니다.

단계 **5** 필터링할 개체 **Issues(**문제**)**를 선택합니다. 두 개 이상의 문제를 선택하면 선택한 범주의 개체가 필터 결과에 포함됩니다.

단계 **6** 문제가 있었지만 관리자가 무시한 개체를 확인하려면 **Ignored(**무시됨**)** 문제를 선택합니다.

단계 **7** 두 개 이상의 디바이스 간에 공유되는 개체를 필터링하는 경우 **Shared Objects(**공유 개체**)**에서 필수 필터를 선택합니다.

- **Default Values(**기본값**)**: 기본값만 있는 개체를 필터링합니다.
- **Override Values(**값 재정의**)**: 오버라이드된 값이 있는 개체를 필터링합니다.
- **Additional Values(**추가 값**)**: 추가 값이 있는 개체를 필터링합니다.

단계 **8** 규칙 또는 정책의 일부가 아닌 개체를 필터링하는 경우 **Unassociated(**연결되지 않음**)**를 선택합니다.

단계 **9** 필터링할 개체 유형을 선택합니다.

단계 **10** Objects(개체) 검색 필드에 개체 이름, IP 주소 또는 포트 번호를 추가하여 필터링된 결과 중에서 검색 기준으로 개체를 찾을 수도 있습니다.

---

필터 기준에서 디바이스를 제외해야 하는 경우

필터링 기준에 디바이스를 추가하면 결과에 디바이스의 개체가 표시되지만 해당 개체와 다른 디바이스의 관계는 표시되지 않습니다. 예를 들어 **ObjectA**가 ASA1과 ASA2 간에 공유된다고 가정합니다. ASA1에서 공유 개체를 찾기 위해 개체를 필터링하는 경우 **ObjectA**를 찾을 수 있지만 **Relationships(**관계**)** 창에는 해당 개체가 ASA1에 있다는 것만 표시됩니다.

개체와 관련된 모든 디바이스를 보려면 검색 기준에 디바이스를 지정하지 마십시오. 다른 기준으로 필터링하고 원하는 경우 검색 기준을 추가하십시오. CDO가 식별하는 개체를 선택한 다음 관계 창을 살펴봅니다. 개체와 관련된 모든 디바이스 및 정책이 표시됩니다.

# 개체 무시

사용되지 않거나 중복되거나 일관성이 없는 개체를 해결하는 한 가지 방법은 해당 개체를 무시하는 것입니다. 사용되지 않은 개체 문제 해결 중복 개체 문제 해결 불일치 개체 문제 해결 해당 상태에 대한 타당한 이유가 있다고 판단하고 개체 문제를 해결되지 않은 상태로 두도록 선택할 수 있습니다. 나중에 무시된 개체를 해결해야 할 수도 있습니다. CDO는 개체 문제를 검색할 때 무시된 개체를 표시하지 않으므로 무시된 개체에 대한 개체 목록을 필터링한 다음 결과에 따라 조치를 취해야 합니다.

---

단계 **1** 왼쪽의 CDO 탐색 바에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 개체 필터

단계 **3** **Object(**개체**)** 테이블에서 무시를 취소할 개체를 선택합니다. 한 번에 하나의 개체를 무시 취소할 수 있습니다.

단계 **4** 세부 정보 창에서 **Unignore(**무시**)**를 클릭합니다.

단계 **5** 요청을 확인합니다. 이제 문제별로 개체를 필터링하면 이전에 무시되었던 개체를 찾아야 합니다.

---

# 개체 삭제

단일 개체 또는 여러 개체를 삭제할 수 있습니다.

## 단일 개체 삭제

**Caution** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(**개체**) > ASA Objects(ASA** 개체**)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

단계 **1** 왼쪽의 CDO 탐색 모음에서 **Objects(**개체**)**를 선택하고 옵션을 선택합니다.

단계 **2** 개체 필터와 검색 필드를 사용하여 삭제하려는 개체를 찾아 선택합니다.

단계 **3** **Relationships(**관계**)** 창을 검토합니다. 개체가 정책 또는 개체 그룹에서 사용되는 경우 해당 정책 또는 그룹에서 개체를 제거할 때까지 개체를 삭제할 수 없습니다.

단계 **4** 작업 창에서 **Remove(**제거**)** 아이콘를 클릭합니다.

단계 **5** **OK(**확인**)**을 클릭하여 개체 삭제를 확인합니다.

단계 **6** 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나, 한 번에 여러 변경 사항을 기다렸다가 배포합니다.

## 사용되지 않는 개체 그룹 삭제

디바이스를 온보딩하고 개체 문제를 해결하기 시작하면 사용하지 않는 개체를 많이 찾습니다. 한 번에 최대 50개의 사용하지 않는 개체를 삭제할 수 있습니다.

단계 **1** **Issues(**문제**)** 필터를 사용하여 미사용 개체를 찾습니다. 디바이스 필터를 사용하여 디바이스 없음을 선택하여 디바이스와 연결되지 않은 개체를 찾을 수도 있습니다. 개체 목록을 필터링하면 개체 확인란이 나타납니다.

단계 **2** 개체 테이블 머리글에서 **Select all(**모두 선택**)** 확인란을 선택하여 개체 테이블에 나타나는 필터에 의해 발견된 모든 개체를 선택합니다. 또는 삭제할 개별 개체에 대한 개별 확인란을 선택합니다.

단계 **3** 작업 창에서 **Remove(**제거**)** 아이콘를 클릭합니다.

단계 **4** 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

# 네트워크 개체

네트워크 개체는 호스트 이름, 네트워크 IP 주소, IP 주소의 범위, FQDN(인증된 도메인 이름) 또는 CIDR 표기법으로 표현된 서브 네트워크를 포함할 수 있습니다. 네트워크 그룹은 그룹에 추가하는 네트워크 개체 및 기타 개별 주소 또는 서브 네트워크의 모음입니다. 네트워크 개체 및 네트워크 그룹은 액세스 규칙, 네트워크 정책 및 NAT 규칙에서 사용됩니다. CDO를 사용하여 네트워크 개체 및 네트워크 그룹을 생성, 업데이트 및 삭제할 수 있습니다.

***Table 15:*** 네트워크 개체의 허용되는 값

| 디바이스 유형 | **IPv4 / IPv6** | 단일 주소 | 주소 범위 | 전체**(Fully Qualified)** 도메인 이름 | **CIDR** 표기법의 서브넷 |
|---|---|---|---|---|---|
| ASA | IPv4 및 IPv6 | 예 | 예 | 예 | 예 |

***Table 16:*** 네트워크 그룹의 허용되는 콘텐츠

| 디바이스 유형 | **IP** 값 | 네트워크 개체 | 네트워크 그룹 |
|---|---|---|---|
| ASA | 예 | 예 | 예 |

제품 간 네트워크 개체 재사용

클라우드 사용 Firewall Management Center가 포함된 Cisco Defense Orchestrator 테넌트가 있는 경우:

Secure Firewall Threat Defense, FDM 관리 위협 방어, ASA 또는 Meraki 네트워크 개체 또는 그룹을 생성하면 클라우드 사용 Firewall Management Center를 구성할 때 사용되는 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지의 개체 목록에도 개체의 복사본이 추가되며, 그 반대의 경우도 마찬가지입니다.

한 페이지에서 네트워크 개체 또는 그룹에 대한 변경 사항은 두 페이지의 개체 또는 그룹 인스턴스에 적용됩니다. 한 페이지에서 개체를 삭제하면 다른 페이지에서도 개체의 해당 복사본이 삭제됩니다.

예외:

- 클라우드 사용 Firewall Management Center에 대해 동일한 이름의 네트워크 개체가 이미 있는 경우 Secure Firewall Threat Defense, FDM 관리 위협 방어, ASA 또는 Meraki 네트워크 개체는 Cisco Defense Orchestrator의 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지에서 복제되지 않습니다.
- 온프레미스 Secure Firewall Management Center에서 관리하는 온보딩된 위협 방어 디바이스의 네트워크 개체 및 그룹은 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지에 복제되지 않으며, 클라우드 사용 Firewall Management Center에서 사용할 수 없습니다.

  클라우드 사용 Firewall Management Center로 마이그레이션된 온프레미스 Secure Firewall Management Center 인스턴스의 경우, 네트워크 개체 및 그룹이 FTD 디바이스에 구축된 정책에서 사용되었다면 네트워크 개체 및 그룹이 CDO 개체 페이지에 복제됩니다.

- CDO와 클라우드 사용 Firewall Management Center 간에 네트워크 개체 공유 는 새로운 테넌트에서 자동으로 활성화되지만 기존 테넌트에 대해서는 요청해야 합니다. 네트워크 개체를 클라우드 사용 Firewall Management Center와 공유하지 않는 경우 CDO 고객이 TAC로 지원 티켓을 여는 방법하여 테넌트에서 기능을 활성화하십시오.

네트워크 개체 보기

CDO를 사용하여 생성한 네트워크 개체와 온보딩된 디바이스 구성에서 인식되는 CDO가 Objects(개체) 페이지에 표시됩니다. 개체 유형으로 레이블이 지정됩니다. 이렇게 하면 개체 유형으로 필터링하여 원하는 개체를 빠르게 찾을 수 있습니다.

Objects(개체) 페이지에서 네트워크 개체를 선택하면 Details(세부 정보) 창에 개체의 값이 표시됩니다. Relationships(관계) 창에는 개체가 정책에서 사용되는지 여부와 개체가 저장된 디바이스가 표시됩니다.

네트워크 그룹을 클릭하면 해당 그룹의 콘텐츠가 표시됩니다. 네트워크 그룹은 네트워크 개체에 의해 제공되는 모든 값의 복합물입니다.

# ASA 네트워크 개체 및 네트워크 그룹 생성 또는 편집

**ASA** 네트워크 개체는 CIDR 표기법으로 표시된 호스트 이름, IP 주소 또는 서브넷 주소를 포함할 수 있습니다. 네트워크 그룹은 액세스 규칙, 네트워크 정책 및 NAT 규칙에 사용되는 네트워크 개체, 네트워크 그룹 및 IP 주소의 복합 그룹입니다. CDO를 사용하여 네트워크 개체 및 네트워크 그룹을 생성, 읽기, 업데이트 및 삭제할 수 있습니다.

***Table 17: ASA*** 네트워크 개체 및 그룹의 허용 값

| 디바이스 유형 | **IPv4 / IPv6** | 단일 주소 | 주소 범위 | **PQDN(Partially Qualified Domain Name)** | **CIDR** 표기법의 서브넷 |
|---|---|---|---|---|---|
| ASA | IPv4 / IPv6 | 예 | 예 | 예 | 예 |

**Note** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(**개체**) > ASA Objects(ASA** 개체**)** 페이지에서 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다.

**Caution** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(**개체**) > ASA Objects(ASA** 개체**)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

## 새 네트워크 개체 생성

네트워크 개체는 호스트 이름, 네트워크 IP 주소, IP 주소의 범위, FQDN(인증된 도메인 이름) 또는 CIDR 표기법으로 표현된 서브 네트워크를 포함할 수 있습니다. 네트워크 개체는 액세스 규칙, 네트워크 정책 및 NAT 규칙에서 사용됩니다. CDO를 사용하여 네트워크 개체 및 네트워크 그룹을 생성, 업데이트 및 삭제할 수 있습니다.

**Note** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(**개체**) > ASA Objects(ASA** 개체**)** 페이지에서 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다.

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2** 파란색 더하기 버튼  을 클릭하여 개체를 생성합니다.

단계 **3** **ASA** > **Network(ASA** 네트워크**)**를 클릭합니다.

단계 **4** 개체 이름을 입력합니다.

단계 **5** **Create a network object(**네트워크 개체 생성**)**를 선택합니다.

단계 **6** (선택 사항) 개체 설명을 입력합니다.

단계 **7** **Value(**값**)** 섹션에서 다음 방법 중 하나로 IP 주소 정보를 추가합니다.

- **eq**를 선택한 다음 단일 IP 주소, CIDR 표기법을 사용한 서브넷 주소 또는 PQDN(Partially Qualified Domain Name)을 입력합니다.
- 범위를 선택한 다음 IP 주소의 범위를 입력합니다. 시작 주소와 끝 주소를 공백으로 구분하여 범위를 입력합니다. 예: 10.1.1.1 10.1.1.255 또는 2001:DB8:1::1 2001:DB8:1::3

단계 **8** **Add(**추가**)**를 클릭합니다.

**Important** 새로 생성된 네트워크 개체는 규칙 또는 정책의 일부가 아니므로 ASA 디바이스와 연결되지 않습니다. 이러한 개체를 보려면 개체 필터에서 **Unassociated(**연결되지 않음**)** 개체 범주를 선택합니다. 자세한 내용은 개체 필터를 참고하십시오. 디바이스의 규칙 또는 정책에서 연결되지 않은 개체를 사용하면 이러한 개체는 해당 디바이스와 연결됩니다.

## ASA 네트워크 그룹 생성

네트워크 그룹은 IP 주소 값, 네트워크 개체 및 네트워크 그룹을 포함할 수 있습니다. 새 네트워크 그룹을 만들 때 이름, IP 주소, IP 주소 범위 또는 FQDN으로 기존 개체를 검색하고 네트워크 그룹에 추가할 수 있습니다. 개체가 없는 경우 동일한 인터페이스에서 해당 개체를 즉시 생성하고 네트워크 그룹에 추가할 수 있습니다. 네트워크 그룹은 IPv4 및 IPv6 주소를 모두 포함할 수 있습니다.

**Note** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(**개체**) > ASA Objects(ASA** 개체**)** 페이지에서 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다.

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2** 파란색 더하기 버튼 을 클릭하여 개체를 생성합니다.

단계 **3** **ASA** > **Network(ASA** 네트워크**)**를 클릭합니다.

단계 **4** 개체 이름을 입력합니다.

단계 **5** **Create a network group(**네트워크 그룹 생성**)**을 선택합니다.

단계 **6** (선택 사항) 개체 설명을 입력합니다.

단계 **7** **Values(**값**)** 필드에 값 또는 개체 이름을 입력합니다. 입력을 시작하면 CDO에서 항목과 일치하는 개체 이름 또는 값을 제공합니다.

단계 **8** 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.

단계 **9** CDO가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add(**추가**)**를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.

단계 **10** 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.

- 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name(**이 이름의 새 개체로 추가**)**을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.
- 새 개체를 생성하려면 **Add as New Object(**새 개체로 추가**)**를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.
- 개체를 사용하지 않고 인라인 값을 만들려면 **Add Value(**값 추가**)**를 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.

값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.

**Note** 편집 아이콘을 클릭하여 세부 정보를 편집할 수 있습니다. 삭제 버튼을 클릭해도 개체 자체는 삭제되지 않습니다. 대신 네트워크 그룹에서 제거됩니다.

단계 **11** 필요한 개체를 추가한 후 **Add(**추가**)**를 클릭하여 새 네트워크 그룹을 생성합니다.

단계 **12** 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, on page 352.

## ASA 네트워크 개체 편집

**Caution** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(**개체**) > ASA Objects(ASA** 개체**)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.

단계 **3** 네트워크 개체를 선택하고 **Actions(**작업**)** 창에서 편집 아이콘 을 클릭합니다.

단계 **4** 위의 절차에서 만든 것과 같은 방식으로 대화 상자에서 값을 편집합니다.

**Note** 네트워크 그룹에서 개체를 제거하려면 옆에 있는 삭제 아이콘을 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭합니다. CDO에 변경의 영향을 받을 디바이스가 표시됩니다.

단계 **6** **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

## ASA 네트워크 그룹 편집

**Caution** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(**개체**) > ASA Objects(ASA** 개체**)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

단계 **1** 좌측의 CDO 탐색 모음에서 **Objects(**개체**) > ASA Objects(ASA** 개체**)**를 클릭합니다.
단계 **2** 개체 필터 및 검색 필드를 사용하여 편집하려는 네트워크 그룹을 찾습니다.

단계 **3** SGT 그룹을 선택하고 **Actions(**작업**)** 창에서 편집 아이콘 를 클릭합니다.
단계 **4** 이 네트워크 그룹에 새 네트워크 개체 또는 네트워크 그룹을 추가하려면 다음 단계를 수행합니다.

**a.** 개체 이름 또는 네트워크 그룹 옆에 나타나는 편집 아이콘 을 클릭하여 편집합니다.

**b.** 확인 표시를 클릭하여 변경 사항을 저장합니다.

**Note** 네트워크 그룹에서 값을 제거하려면 삭제 아이콘을 클릭합니다.

단계 **5** 이 네트워크 그룹에 새 네트워크 개체 또는 네트워크 그룹을 추가하려면 다음 단계를 수행합니다.

**a.** **Values(**값**)** 필드에 새 값이나 기존 네트워크 개체의 이름을 입력합니다. 입력을 시작하면 CDO에서 항목과 일치하는 개체 이름 또는 값을 제공합니다. 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.

**b.** CDO가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add(**추가**)**를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.

**c.** 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.

- 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name(**이 이름의 새 개체로 추가**)**을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.
- 새 개체를 생성하려면 **Add as New Object(**새 개체로 추가**)**를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.
- 개체를 사용하지 않고 인라인 값을 만들려면 **Add Value(**값 추가**)**를 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.

값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.

단계 **6** **Save(**저장**)**를 클릭합니다. CDO에 변경의 영향을 받을 정책이 표시됩니다.
단계 **7** **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.
단계 **8** 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, on page 352.

## 공유 네트워크 그룹에 값 추가

연결된 모든 디바이스에 있는 공유 네트워크 그룹의 값을 "기본값"이라고 합니다. CDO를 사용하면 공유 네트워크 그룹에 "추가 값"을 추가하고 해당 공유 네트워크 그룹과 연결된 일부 디바이스에 해당 값을 할당할 수 있습니다. CDO는 변경 사항을 디바이스에 구축할 때 콘텐츠를 확인하고 공유 네트워크 그룹과 연결된 모든 디바이스에 "기본값"을 푸시하고 지정된 디바이스에만 "추가 값"을 푸시합니다.

모든 사이트에서 액세스할 수 있어야 하는 본사에 4개의 AD 기본 서버가 있는 시나리오를 예로 들어 보겠습니다. 따라서 모든 사이트에서 사용할 "Active-Directory"라는 개체 그룹을 생성했습니다. 이제 지사 중 하나에 두 개의 AD 서버를 추가하려고 합니다. 개체 그룹 "Active-Directory"에서 해당 지사에 특정한 추가 값으로 세부 정보를 추가하여 이 작업을 수행할 수 있습니다. 이 두 서버는 "Active-Directory" 개체가 일관성이 있는지 또는 공유되는지를 확인하는 데 참여하지 않습니다. 따라서 모든 사이트에서 4개의 AD 기본 서버에 액세스할 수 있지만 지사(2개의 추가 서버 포함)는 2개의 AD 서버와 4개의 AD 기본 서버에 액세스할 수 있습니다.

**Note** 일치하지 않는 공유 네트워크 그룹이 있는 경우 추가 값을 사용하여 단일 공유 네트워크 그룹으로 결합할 수 있습니다. 자세한 내용은 불일치 개체 문제 해결을 참조하십시오.

**Caution** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(**개체**) > ASA Objects(ASA** 개체**)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 편집할 공유 네트워크 그룹을 찾습니다.

단계 **3** **Actions(**작업**)** 창에서 편집 아이콘 을 클릭합니다.

- **Devices(**디바이스**)** 필드에는 공유 네트워크 그룹이 있는 디바이스가 표시됩니다.
- **Usage(**사용**)** 필드에는 공유 네트워크 그룹과 연결된 규칙 집합이 표시됩니다.
- **Default Values(**기본값**)** 필드는 생성 중에 제공된 공유 네트워크 그룹과 연결된 기본 네트워크 개체 및 해당 값을 지정합니다. 이 필드 옆에서 이 기본값이 포함된 디바이스의 수를 볼 수 있으며, 클릭하여 해당 이름 및 디바이스 유형을 볼 수 있습니다. 이 값과 연결된 규칙 집합도 확인할 수 있습니다.

단계 **4** 추가 값 필드에 값 또는 이름을 입력합니다. 입력을 시작하면 CDO에서 항목과 일치하는 개체 이름 또는 값을 제공합니다.

단계 **5** 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.

단계 **6** CDO가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add(**추가**)**를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.

단계 **7** 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.

- 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name(**이 이름의 새 개체로 추가**)**을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.

- 새 개체를 생성하려면 **Add as New Object(**새 개체로 추가**)**를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.
- 개체를 사용하지 않고 인라인 값을 만들려면 **Add Value(**값 추가**)**를 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.

값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.

단계 **8** **Devices(**디바이스**)** 열에서 새로 추가된 개체와 연결된 셀을 클릭하고 **Add Devices(**디바이스 추가**)**를 클릭합니다.

단계 **9** 원하는 디바이스를 선택하고 **OK(**확인**)**를 클릭합니다.

단계 **10** **Save(**저장**)**를 클릭합니다. CDO에 변경의 영향을 받을 디바이스가 표시됩니다.

단계 **11** **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

단계 **12** 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, on page 352.

## 공유 네트워크 그룹의 추가 값 편집

**Caution**

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(**개체**) > ASA Objects(ASA** 개체**)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

단계 **1** 좌측의 CDO 탐색 모음에서 **Objects(**개체**) > ASA Objects(ASA** 개체**)**를 클릭합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 편집하려는 오버라이드가 있는 개체를 찾습니다.

단계 **3** **Actions(**작업**)** 창에서 편집 아이콘 를 클릭합니다.

단계 **4** 오버라이드 값을 편집합니다.

- 값을 편집하려면 편집 아이콘을 클릭합니다.
- **Devices(**디바이스**)** 열의 셀을 클릭하여 새 디바이스를 할당합니다. 이미 할당된 디바이스를 선택하고 **Remove Overrides(**오버라이드 제거**)**를 클릭하여 해당 디바이스에서 오버라이드를 제거할 수 있습니다.
- **Default Values(**기본값**)**의 화살표를 클릭하여 푸시하고 공유 네트워크 그룹의 추가 값으로 설정합니다. 공유 네트워크 그룹과 연결된 모든 디바이스가 자동으로 할당됩니다.
- **Override Values(**값 재정의**)**에서 화살표를 클릭하여 공유 네트워크 그룹의 기본 개체로 푸시하고 설정합니다.
- 네트워크 그룹에서 개체를 제거하려면 옆에 있는 삭제 아이콘을 클릭합니다.

단계 5 **Save(**저장**)**를 클릭합니다. CDO에 변경의 영향을 받을 디바이스가 표시됩니다.

단계 6 **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

단계 7 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, on page 352.

## 네트워크 개체 및 그룹 삭제

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(**개체**) > ASA Objects(ASA** 개체**)** 페이지에서 네트워크 개체나 그룹을 삭제하면 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지에서 복제된 네트워크 개체 또는 그룹이 삭제되며, 그 반대의 경우도 마찬가지입니다.

# 트러스트 포인트 개체

CDO를 사용하면 디지털 인증서를 트러스트 포인트 개체로 추가한 다음 하나 이상의 관리 ASA 디바이스에 설치할 수 있습니다. 단일 트러스트 포인트 개체는 ID 쌍(ID 인증서 및 발급자의 CA 인증서), ID 인증서만 또는 CA 인증서만 포함하는 컨테이너입니다.

ASA 디바이스에서 여러 트러스트 포인트를 구성할 수 있습니다. 지원되는 인증서 형식은 PKCS12, PEM 및 DER입니다.

## PKCS12를 사용하여 ID 인증서 개체 추가

이 절차에서는 인증서 파일을 업로드하거나 기존 인증서 텍스트를 텍스트 상자에 붙여넣어 내부 인증서 ID 또는 내부 ID 인증서를 생성합니다. ID 인증서는 원하는 만큼 생성할 수 있습니다.

**PKCS12** 형식으로 인코딩된 파일을 업로드할 수 있습니다. PKCS12는 하나의 암호화된 파일에 서버 인증서, 중간 인증서 및 개인 키를 보관하는 단일 파일입니다. PKCS#12 또는 PFX에서 파일은 하나의 암호화된 파일에 서버 인증서, 중간 인증서 및 개인 키를 보관합니다. 암호 해독을 위해 **Passphrase(**암호 문구**)** 값을 입력합니다.

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 2  아이콘을 클릭하고 **ASA** > **Trustpoints(**트러스트 포인트**)**를 선택합니다.

단계 3 인증서의 **Object Name(**개체 이름**)**을 입력합니다. 이름은 컨피그레이션에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 4 **Certificate Type(**인증서 유형**)** 단계에서 **Identity Certificate(ID** 인증서**)**를 선택합니다.

단계 5 **Import Type(**가져오기 유형**)** 단계에서 **Upload(**업로드**)**를 선택하여 인증서 파일을 업로드합니다.

**Enrollment(**등록**)** 단계가 Terminal(터미널)로 설정되어 있습니다.

단계 6 **Certificate Contents(**인증서 콘텐츠**)** 단계에서 PKCS12 형식 세부 정보를 입력합니다.

PKCS#12 또는 PFX에서 파일은 하나의 암호화된 파일에 서버 인증서, 중간 인증서 및 개인 키를 보관합니다. 암호 해독을 위해 **Passphrase(**암호 문구**)** 값을 입력합니다.

단계 **7** **Continue(**계속**)**를 클릭합니다.

단계 **8** **Advanced Options(**고급 옵션**)** 단계에서 다음을 구성할 수 있습니다.

**Revocation(**해지**)** 탭에서 다음을 구성할 수 있습니다.

- **CRL(Certificate Revocation List)** 활성화 - CRL 확인 활성화 여부를 확인합니다.

  기본적으로 **Use CRL distribution point from the certificate(**인증서에서 **CRL** 배포 지점 사용**)** 확인란이 선택되어 인증서에서 해지 목록 배포 URL을 가져옵니다.

  **Cache Refresh Time (in minutes)(**캐시 새로 고침 시간**(**분**))** - 캐시 새로 고침 간격(분)을 입력합니다. 기본값은 60분입니다. 범위는 1분 ~ 1440분입니다. 동일한 CRL을 CA에서 반복적으로 검색할 필요 없이 ASA에서 검색된 CRL을 로컬에 저장할 수 있는데, 이를 CRL 캐싱이라고 합니다. CRL 캐시 용량은 플랫폼에 따라 다르며 모든 상황을 포괄하여 누적됩니다. 새로 검색된 CRL을 캐시에 저장하려는데 저장 한도를 초과할 경우, ASA에서는 가장 오래전에 사용된 CRL을 제거하면서 사용 가능한 공간을 늘립니다.

- **OCSP(Online Certificate Status Protocol)** 활성화 - OCSP 확인 활성화 여부를 확인합니다.

  **OCSP** 서버 **URL** - OCSP 확인이 필요한 경우 폐기를 위한 OCSP 서버 확인 URL입니다. 이 URL은 **`http://`**로 시작해야 합니다.

  **Disable Nonce Extension(Nonce** 확장 비활성화**)** - 암호 기술을 사용하여 요청과 응답을 바인딩함으로써 반복 공격을 방지하는 확인란을 활성화합니다. 이 프로세스에서는 요청의 확장을 응답의 확장과 일치하는지 비교하면서 동일함을 보장합니다. 사용 중인 OCSP 서버가 이와 같이 일치하는 nonce 확장을 포함하지 않는 미리 생성된 응답을 보내는 경우, **Disable Nonce Extension(Nonce** 확장 비활성화**)** 확인란을 선택 취소합니다.

  **Evaluation Priority(**평가 우선순위**)** - 인증서의 해지 상태를 CRL에서 먼저 평가할지 OSCP에서 먼저 평가할지를 지정합니다.

- **Consider the certificate valid if revocation information cannot be reached(**해지 정보에 연결할 수 없는 경우 인증서를 유효한 것으로 간주**)** - 해지 정보에 연결할 수 없는 경우 인증서를 유효한 인증서로 간주하려면 이 확인란을 선택합니다.

  해지 확인에 대한 자세한 내용은 Cisco ASA Series 일반 운영 ASDM 설정의 "기본 설정" 책, XY 문서에서 "디지털 인증서" 장을 참조하십시오.

**Others(**기타**)** 탭을 클릭합니다.

- **Use CA Certificate for the Validation of(**다음을 위한 **CA** 인증서 사용**)** - 이 CA가 검증할 수 있는 연결 유형을 지정합니다.
  - **IPSec Client(IPSec** 클라이언트**)** - 원격 SSL 서버에서 제공하는 인증서를 검증합니다.
  - **SSL Client(SSL** 클라이언트**)** - 수신 SSL 연결에서 제공하는 인증서를 검증합니다.
  - **SSL Server(SSL** 서버**)** - 수신 IPSec 연결에서 제공하는 인증서를 검증합니다.
- **Use Identity Certificate for(ID** 인증서 사용**)** - 등록된 ID 인증서의 사용 방법을 지정합니다.
  - **SSL & IPSec** - SSL 및 IPSec 연결 인증에 사용합니다.

- **Code Signer(**코드 서명자**)** — 코드 서명자 인증서는 해당 개인 키가 디지털 서명 생성에 사용되는 특수한 인증서입니다. 코드 서명에 사용되는 인증서는 CA에서 가져온 것으로, 서명된 코드 자체가 인증서 원본을 나타냅니다.

- 기타 옵션:
  - **Enable CA flag in basic constraints extension(**기본 제약 조건 확장에서 **CA** 플래그 활성화**)** - 이 인증서에서 다른 인증서에 서명할 수 있어야 하는 경우 이 옵션을 선택합니다. 기본 제약 조건 확장은 인증서의 주체가 CA(Certificate Authority)인지 여부를 식별하며 이 경우 인증서를 사용하여 다른 인증서에 서명할 수 있습니다. CA 플래그는 이 확장의 일부입니다. 인증서에 이러한 항목이 있는지 여부
  - **Accept certificates issued by this CA(CA**에서 발급된 인증서 허용**)** - ASA에서 지정된 CA의 인증서를 허용해야 하는 경우 이 옵션을 선택합니다.
  - **Ignore IPsec Key Usage(IPsec** 키 사용 무시**)** - IPsec 원격 클라이언트 인증서의 키 사용 및 확장 키 사용 확장 값을 검증하지 않으려는 경우 이 옵션을 선택합니다. IPsec 클라이언트 인증서를 확인하는 키 사용을 억제할 수 있습니다. 기본적으로 이 옵션은 활성화되어 있지 않습니다.

단계 **9** **Add(**추가**)**를 클릭합니다.

# 자체 서명 인증서 개체 생성

이 절차에서는 마법사에서 적절한 인증서 필드 값을 입력하여 ASA에 대한 자체 서명 인증서를 생성하는 단계를 설명합니다. 자체 서명 인증서는 원하는 만큼 생성할 수 있습니다.

자체 서명 ID 인증서 개체를 생성하려면 다음 단계를 수행합니다.

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2**  아이콘을 클릭하고 **ASA** > **Trustpoints(**트러스트 포인트**)**를 선택합니다.

단계 **3** 인증서의 **Object Name(**개체 이름**)**을 입력합니다. 이름은 컨피그레이션에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 **4** **Identity Certificate(ID** 인증서**)** 단계에서 **Identity Certificate(ID** 인증서**)**를 선택합니다.

단계 **5** **Import Type(**가져오기 유형**)** 단계에서 **New(**새로 만들기**)**를 선택하여 인증서 파일을 업로드하고 **Continue(**계속**)**를 클릭합니다.

단계 **6** **Enrollment(**등록**)** 단계에서 **Self-Signed(**자체 서명**)**를 선택하고 **Continue(**계속**)**를 클릭합니다.

**Certificates Content(**인증서 콘텐츠**)** 단계가 나타납니다. 생성 중인 자체 서명 인증서의 CN 및 SANS 콘텐츠를 이해하려면 인증서 내용을 기반으로 하는 자체 서명 및 CSR 인증서 생성을 읽어보십시오.

단계 **7** **Certificate Contents(**인증서 콘텐츠**)** 단계에서 다음을 구성합니다.

- 국가**(C)**— 드롭다운 목록에서 국가 코드를 선택합니다.
- **State or Province(**주/도**) (ST)** — 인증서에 포함할 주/도입니다.

- **Locality or City(**구/군/시**) (L)** — 인증서에 포함할 구/군/시(예: 도시 이름)입니다.
- 조직**(O)** - 인증서에 포함될 조직 또는 회사 이름입니다.
- **Organizational Unit(Department)(**조직 단위**(**부서**)) (OU)** — 인증서에 포함할 조직 단위의 이름(예: 부서 이름)입니다.
- 일반 이름**(CN)** - 인증서에 포함할 X.500 일반 이름입니다. 이는 디바이스, 웹사이트 또는 다른 문자열의 이름일 수 있습니다. 일반적으로 연결에 성공하려면 이 요소가 필요합니다. 예를 들어 원격 액세스 VPN에 사용되는 내부 인증서에는 CN을 포함해야 합니다.
- **Email Address(**이메일 주소**) (EA)**— ID 인증서와 연결된 이메일 주소입니다.
- **IP Address(IP** 주소**)**— 점으로 구분된 4개의 십진수로 표기되는 네트워크상의 ASA IP 주소입니다.
- **Device's FQDN(**디바이스의 **FQDN)**— DNS 트리 계층 구조에서 노드의 위치를 나타내는 명확한 도메인 이름입니다.
- **Include Device's Serial Number(**디바이스의 일련 번호 포함**)**— 인증서 매개 변수에 ASA 일련 번호를 추가하려면 확인란을 선택합니다.

a) **Key(**키**)** 탭을 클릭합니다.

- **RSA** 또는 **ECDSA** 키 유형을 선택합니다.
- **Key Size(**키 크기**)** - 키 페어가 존재하지 않는 경우 비트 단위로 원하는 키 크기(모듈러스)를 지정합니다. RSA의 권장 키 크기는 1024이고 ECDSA의 경우 348입니다. 모듈러스 크기가 클수록 키가 안전합니다. 그러나 모듈러스 크기가 큰 키는 생성 및 교환 프로세스에 더 오랜 시간이 걸립니다.(512비트보다 큰 경우 1분 이상)
- **Continue(**계속**)**를 클릭합니다.

단계 **8** **Advanced Options(**고급 옵션**)** 단계에서 다음을 구성할 수 있습니다.

**Revocation(**해지**)** 탭에서 다음을 구성할 수 있습니다.

- **CRL(Certificate Revocation List)** 활성화 - CRL 확인 활성화 여부를 확인합니다.

  기본적으로 **Use CRL distribution point from the certificate(**인증서에서 **CRL** 배포 지점 사용**)** 확인란이 선택되어 인증서에서 해지 목록 배포 URL을 가져옵니다.

  **Cache Refresh Time (in minutes)(**캐시 새로 고침 시간**(**분**))** - 캐시 새로 고침 간격(분)을 입력합니다. 기본값은 60분입니다. 범위는 1분 ~ 1440분입니다. 동일한 CRL을 CA에서 반복적으로 검색할 필요 없이 ASA에서 검색된 CRL을 로컬에 저장할 수 있는데, 이를 CRL 캐싱이라고 합니다. CRL 캐시 용량은 플랫폼에 따라 다르며 모든 상황을 포괄하여 누적됩니다. 새로 검색된 CRL을 캐시에 저장하려는데 저장 한도를 초과할 경우, ASA에서는 가장 오래전에 사용된 CRL을 제거하면서 사용 가능한 공간을 늘립니다.

- **OCSP(Online Certificate Status Protocol)** 활성화 - OCSP 확인 활성화 여부를 확인합니다.

  **OCSP** 서버 **URL** - OCSP 확인이 필요한 경우 폐기를 위한 OCSP 서버 확인 URL입니다. 이 URL은 **`http://`**로 시작해야 합니다.

**Disable Nonce Extension(Nonce** 확장 비활성화**)** - 암호 기술을 사용하여 요청과 응답을 바인딩함으로써 반복 공격을 방지하는 확인란을 활성화합니다. 이 프로세스에서는 요청의 확장을 응답의 확장과 일치하는지 비교하면서 동일함을 보장합니다. 사용 중인 OCSP 서버가 이와 같이 일치하는 nonce 확장을 포함하지 않는 미리 생성된 응답을 보내는 경우, **Disable Nonce Extension(Nonce** 확장 비활성화**)** 확인란을 선택 취소합니다.

**Evaluation Priority(**평가 우선순위**)** - 인증서의 해지 상태를 CRL에서 먼저 평가할지 OSCP에서 먼저 평가할지를 지정합니다.

- **Consider the certificate valid if revocation information cannot be reached(**해지 정보에 연결할 수 없는 경우 인증서를 유효한 것으로 간주**)** - 해지 정보에 연결할 수 없는 경우 인증서를 유효한 인증서로 간주하려면 이 확인란을 선택합니다.

  해지 확인에 대한 자세한 내용은 Cisco ASA Series 일반 운영 ASDM 설정의 "기본 설정" 책, XY 문서에서 "디지털 인증서" 장을 참조하십시오.

**Others(**기타**)** 탭을 클릭합니다.

- **Use CA Certificate for the Validation of(**다음을 위한 **CA** 인증서 사용**)** - 이 CA가 검증할 수 있는 연결 유형을 지정합니다.
  - **IPSec Client(IPSec** 클라이언트**)** - 원격 SSL 서버에서 제공하는 인증서를 검증합니다.
  - **SSL Client(SSL** 클라이언트**)** - 수신 SSL 연결에서 제공하는 인증서를 검증합니다.
  - **SSL Server(SSL** 서버**)** - 수신 IPSec 연결에서 제공하는 인증서를 검증합니다.
- **Use Identity Certificate for(ID** 인증서 사용**)** - 등록된 ID 인증서의 사용 방법을 지정합니다.
  - **SSL & IPSec** - SSL 및 IPSec 연결 인증에 사용합니다.
  - **Code Signer(**코드 서명자**)** — 코드 서명자 인증서는 해당 개인 키가 디지털 서명 생성에 사용되는 특수한 인증서입니다. 코드 서명에 사용되는 인증서는 CA에서 가져온 것으로, 서명된 코드 자체가 인증서 원본을 나타냅니다.
- 기타 옵션:
  - **Enable CA flag in basic constraints extension(**기본 제약 조건 확장에서 **CA** 플래그 활성화**)** - 이 인증서에서 다른 인증서에 서명할 수 있어야 하는 경우 이 옵션을 선택합니다. 기본 제약 조건 확장은 인증서의 주체가 CA(Certificate Authority)인지 여부를 식별하며 이 경우 인증서를 사용하여 다른 인증서에 서명할 수 있습니다. CA 플래그는 이 확장의 일부입니다. 인증서에 이러한 항목이 있는지 여부
  - **Accept certificates issued by this CA(CA**에서 발급된 인증서 허용**)** - ASA에서 지정된 CA의 인증서를 허용해야 하는 경우 이 옵션을 선택합니다.
  - **Ignore IPsec Key Usage(IPsec** 키 사용 무시**)** - IPsec 원격 클라이언트 인증서의 키 사용 및 확장 키 사용 확장 값을 검증하지 않으려는 경우 이 옵션을 선택합니다. IPsec 클라이언트 인증서를 확인하는 키 사용을 억제할 수 있습니다. 기본적으로 이 옵션은 활성화되어 있지 않습니다.

단계 **9** **Add(**추가**)**를 클릭합니다.

# CSR(Certificate Signing Request)을 위한 ID 인증서 개체 추가

CSR(Certificate Signing Requests)을 생성하고 지정된 CA에서 ID 인증서를 얻으려면 CA(Certification Authority) 서버 정보 및 등록 매개변수가 필요합니다. 요청을 생성하려면 RSA(Rivest-Shamir-Adleman) 또는 ECDSA(Elliptic Curve Digital Signature Algorithm) 키 유형을 선택해야 합니다.

식별 정보를 제공하고 선택적으로 CA에서 얻은 CA 인증서를 업로드하여 트러스트 포인트 개체를 생성합니다.

---

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2** + 아이콘을 클릭하고 **ASA** > **Trustpoints(**트러스트 포인트**)**를 선택합니다.

단계 **3** 인증서의 **Object Name(**개체 이름**)**을 입력합니다. 이름은 컨피그레이션에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 **4** **Identity Certificate(ID** 인증서**)** 단계에서 **Identity Certificate(ID** 인증서**)**를 선택합니다.

단계 **5** **Import Type(**가져오기 유형**)** 단계에서 **New(**새로 만들기**)**를 선택하여 인증서 파일을 업로드하고 **Continue(**계속**)**를 클릭합니다.

단계 **6** **Enrollment(**등록**)** 단계에서 **Manual(**수동**)**을 선택합니다.

단계 **7** (선택 사항) CA에서 가져온 CA 인증서를 붙여넣거나 업로드할 수 있습니다. 필드를 비워둘 수 있습니다.

단계 **8** Continue(계속)를 클릭합니다.

Certificates Content(인증서 콘텐츠) 단계가 나타납니다. 생성 중인 서명 인증서의 CN 및 SANS 콘텐츠를 이해하려면 인증서 내용을 기반으로 하는 자체 서명 및 CSR 인증서 생성을 읽어보십시오.

단계 **9** **Certificate Contents(**인증서 콘텐츠**)** 단계에서 다음을 구성합니다.

- 국가**(C)**— 드롭다운 목록에서 국가 코드를 선택합니다.
- **State or Province(**주/도**) (ST)** — 인증서에 포함할 주/도입니다.
- **Locality or City(**구/군/시**) (L)** — 인증서에 포함할 구/군/시(예: 도시 이름)입니다.
- 조직**(O)** - 인증서에 포함될 조직 또는 회사 이름입니다.
- **Organizational Unit(Department)(**조직 단위**(**부서**)) (OU)** — 인증서에 포함할 조직 단위의 이름(예: 부서 이름)입니다.
- 일반 이름**(CN)** - 인증서에 포함할 X.500 일반 이름입니다. 이는 디바이스, 웹사이트 또는 다른 문자열의 이름일 수 있습니다. 일반적으로 연결에 성공하려면 이 요소가 필요합니다. 예를 들어 원격 액세스 VPN에 사용되는 내부 인증서에는 CN을 포함해야 합니다.
- **Email Address(**이메일 주소**) (EA)**— ID 인증서와 연결된 이메일 주소입니다.
- **IP Address(IP** 주소**)**— 점으로 구분된 4개의 십진수로 표기되는 네트워크상의 ASA IP 주소입니다.
- **SAN(Subject Alternative Name)** - 이 필드는 'unstructuredName'으로도 인증서 주체 DN의 일부가 됩니다. 인증서가 여러 도메인 또는 IP 주소에 사용되는 경우, 이 필드를 활용하는 것이 좋습니다.
  - **Use Device Host Name(**디바이스 호스트 이름 사용**)**: 디바이스의 호스트 이름이 사용됩니다.

- **Custom: Device's FQDN(**사용자 지정 디바이스의 **FQDN)**— DNS 트리 계층 구조에서 노드의 위치를 나타내는 명확한 도메인 이름입니다.

  참고 CN 및 사용자 지정 **FQDN**에 지정된 값은 동일한 것이 좋습니다.

- **Include Device's Serial Number(**디바이스의 일련 번호 포함**)**— 인증서에 ASA의 일련 번호를 추가하려면 확인란을 선택합니다. CA는 인증서 인증 또는 추후 특정 디바이스와 인증서를 연결하기 위해 일련 번호를 사용합니다. 확실하지 않은 경우 일련 번호를 포함하면 디버깅 시 유용합니다.

a) **Key(**키**)** 탭을 클릭합니다.

- **RSA** 또는 **ECDSA** 키 유형을 선택합니다.
- **Key Size(**키 크기**)** - 키 페어가 존재하지 않는 경우 비트 단위로 원하는 키 크기(모듈러스)를 지정합니다. RSA의 권장 키 크기는 1024이고 ECDSA의 경우 348입니다. 모듈러스 크기가 클수록 키가 안전합니다. 그러나 모듈러스 크기가 큰 키는 생성 및 교환 프로세스에 더 오랜 시간이 걸립니다.(512비트보다 큰 경우 1분 이상)
- **Continue(**계속**)**를 클릭합니다.

단계 **10** **Advanced Options(**고급 옵션**)** 단계에서 다음을 구성할 수 있습니다.

**Revocation(**해지**)** 탭에서 다음을 구성할 수 있습니다.

- **CRL(Certificate Revocation List)** 활성화 - CRL 확인 활성화 여부를 확인합니다.

  기본적으로 **Use CRL distribution point from the certificate(**인증서에서 **CRL** 배포 지점 사용**)** 확인란이 선택되어 인증서에서 해지 목록 배포 URL을 가져옵니다.

  **Cache Refresh Time (in minutes)(**캐시 새로 고침 시간**(**분**))** - 캐시 새로 고침 간격(분)을 입력합니다. 기본값은 60분입니다. 범위는 1분 ~ 1440분입니다. 동일한 CRL을 CA에서 반복적으로 검색할 필요 없이 ASA에서 검색된 CRL을 로컬에 저장할 수 있는데, 이를 CRL 캐싱이라고 합니다. CRL 캐시 용량은 플랫폼에 따라 다르며 모든 상황을 포괄하여 누적됩니다. 새로 검색된 CRL을 캐시에 저장하려는데 저장 한도를 초과할 경우, ASA에서는 가장 오래전에 사용된 CRL을 제거하면서 사용 가능한 공간을 늘립니다.

- **OCSP(Online Certificate Status Protocol)** 활성화 - OCSP 확인 활성화 여부를 확인합니다.

  **OCSP** 서버 **URL** - OCSP 확인이 필요한 경우 폐기를 위한 OCSP 서버 확인 URL입니다. 이 URL은 **`http://`**로 시작해야 합니다.

  **Disable Nonce Extension(Nonce** 확장 비활성화**)** - 암호 기술을 사용하여 요청과 응답을 바인딩함으로써 반복 공격을 방지하는 확인란을 활성화합니다. 이 프로세스에서는 요청의 확장을 응답의 확장과 일치하는지 비교하면서 동일함을 보장합니다. 사용 중인 OCSP 서버가 이와 같이 일치하는 nonce 확장을 포함하지 않는 미리 생성된 응답을 보내는 경우, **Disable Nonce Extension(Nonce** 확장 비활성화**)** 확인란을 선택 취소합니다.

  **Evaluation Priority(**평가 우선순위**)** - 인증서의 해지 상태를 CRL에서 먼저 평가할지 OSCP에서 먼저 평가할지를 지정합니다.

- **Consider the certificate valid if revocation information cannot be reached(**해지 정보에 연결할 수 없는 경우 인증서를 유효한 것으로 간주**)** - 해지 정보에 연결할 수 없는 경우 인증서를 유효한 인증서로 간주하려면 이 확인란을 선택합니다.

해지 확인에 대한 자세한 내용은 Cisco ASA Series 일반 운영 ASDM 설정의 "기본 설정" 책, XY 문서에서 "디지털 인증서" 장을 참조하십시오.

**Others(**기타**)** 탭을 클릭합니다.

- **Use CA Certificate for the Validation of(**다음을 위한 **CA** 인증서 사용**)** - 이 CA가 검증할 수 있는 연결 유형을 지정합니다.
  - **IPSec Client(IPSec** 클라이언트**)** - 원격 SSL 서버에서 제공하는 인증서를 검증합니다.
  - **SSL Client(SSL** 클라이언트**)** - 수신 SSL 연결에서 제공하는 인증서를 검증합니다.
  - **SSL Server(SSL** 서버**)** - 수신 IPSec 연결에서 제공하는 인증서를 검증합니다.
- **Use Identity Certificate for(ID** 인증서 사용**)** - 등록된 ID 인증서의 사용 방법을 지정합니다.
  - **SSL & IPSec** - SSL 및 IPSec 연결 인증에 사용합니다.
  - **Code Signer(**코드 서명자**)** — 코드 서명자 인증서는 해당 개인 키가 디지털 서명 생성에 사용되는 특수한 인증서입니다. 코드 서명에 사용되는 인증서는 CA에서 가져온 것으로, 서명된 코드 자체가 인증서 원본을 나타냅니다.
- 기타 옵션:
  - **Enable CA flag in basic constraints extension(**기본 제약 조건 확장에서 **CA** 플래그 활성화**)** - 이 인증서에서 다른 인증서에 서명할 수 있어야 하는 경우 이 옵션을 선택합니다. 기본 제약 조건 확장은 인증서의 주체가 CA(Certificate Authority)인지 여부를 식별하며 이 경우 인증서를 사용하여 다른 인증서에 서명할 수 있습니다. CA 플래그는 이 확장의 일부입니다. 인증서에 이러한 항목이 있는지 여부
  - **Accept certificates issued by this CA(CA**에서 발급된 인증서 허용**)** - ASA에서 지정된 CA의 인증서를 허용해야 하는 경우 이 옵션을 선택합니다.
  - **Ignore IPsec Key Usage(IPsec** 키 사용 무시**)** - IPsec 원격 클라이언트 인증서의 키 사용 및 확장 키 사용 확장 값을 검증하지 않으려는 경우 이 옵션을 선택합니다. IPsec 클라이언트 인증서를 확인하는 키 사용을 억제할 수 있습니다. 기본적으로 이 옵션은 활성화되어 있지 않습니다.

단계 **11** **Add(**추가**)**를 클릭합니다.

이렇게 하면 트러스트 포인트 인증서 개체가 생성됩니다.

# 신뢰할 수 있는 CA 인증서 개체 추가

외부 인증 기관으로부터 신뢰할 수 있는 CA 인증을 획득하거나, OpenSSL 도구 등 자체 내부 CA를 사용하여 CA 인증을 생성하십시오. 다음의 지원되는 형식 중 하나로 인코딩된 파일을 업로드할 수 있습니다.

- DER(Distinguished Encoding Rules)
- PEM(Privacy-enhanced Electronic Mail)

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 2  아이콘을 클릭하고 **ASA** > **Trustpoints(**트러스트 포인트**)**를 선택합니다.

단계 3 인증서의 **Object Name(**개체 이름**)**을 입력합니다. 이름은 컨피그레이션에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 4 **Certificate Type(**인증서 유형**)** 단계에서 **Trusted CA Certificate(**신뢰할 수 있는 **CA** 인증서**)**를 선택합니다.

단계 5 **Certificate Contents(**인증서 콘텐츠**)** 단계에서 텍스트 상자에 인증서 콘텐츠를 붙여넣거나 마법사의 설명에 따라 CA 인증서 파일을 업로드합니다.

단계 6 **Continue(**계속**)**를 클릭합니다. 마법사가 4단계로 진행합니다.

인증서는 다음 지침을 따라야 합니다.

- 인증서의 서버 이름이 서버 호스트 이름/IP 주소와 일치해야 합니다. 예를 들어 IP 주소로 10.10.10.250을 사용하는데 인증서의 주소는 ad.example.com이면 연결은 실패합니다.
- 인증서는 PEM 또는 DER 형식의 X509 인증서여야 합니다.
- 붙여넣는 인증서는 BEGIN CERTIFICATE 및 END CERTIFICATE 줄을 포함해야 합니다. 예를 들면 다음과 같습니다.

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAsx
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxDzAN
BgNVBAcMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjExFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6HOgKlOwXbRvOdksTzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

단계 7 **Advanced Options(**고급 옵션**)** 단계에서 다음을 구성할 수 있습니다.

**Revocation(**해지**)** 탭에서 다음을 구성할 수 있습니다.

- **CRL(Certificate Revocation List)** 활성화 - CRL 확인 활성화 여부를 확인합니다.

  기본적으로 **Use CRL distribution point from the certificate(**인증서에서 **CRL** 배포 지점 사용**)** 확인란이 선택되어 인증서에서 해지 목록 배포 URL을 가져옵니다.

  **Cache Refresh Time (in minutes)(**캐시 새로 고침 시간**(**분**))** - 캐시 새로 고침 간격(분)을 입력합니다. 기본값은 60분입니다. 범위는 1분 ~ 1440분입니다. 동일한 CRL을 CA에서 반복적으로 검색할 필요 없이 ASA에서 검색된 CRL을 로컬에 저장할 수 있는데, 이를 CRL 캐싱이라고 합니다. CRL 캐시 용량은 플랫폼에 따라 다르며 모든 상황을 포괄하여 누적됩니다. 새로 검색된 CRL을 캐시에 저장하려는데 저장 한도를 초과할 경우, ASA에서는 가장 오래전에 사용된 CRL을 제거하면서 사용 가능한 공간을 늘립니다.

- **OCSP(Online Certificate Status Protocol)** 활성화 - OCSP 확인 활성화 여부를 확인합니다.

  **OCSP** 서버 **URL** - OCSP 확인이 필요한 경우 폐기를 위한 OCSP 서버 확인 URL입니다. 이 URL은 **`http://`**로 시작해야 합니다.

**Disable Nonce Extension(Nonce** 확장 비활성화**)** - 암호 기술을 사용하여 요청과 응답을 바인딩함으로써 반복 공격을 방지하는 확인란을 활성화합니다. 이 프로세스에서는 요청의 확장을 응답의 확장과 일치하는지 비교하면서 동일함을 보장합니다. 사용 중인 OCSP 서버가 이와 같이 일치하는 nonce 확장을 포함하지 않는 미리 생성된 응답을 보내는 경우, **Disable Nonce Extension(Nonce** 확장 비활성화**)** 확인란을 선택 취소합니다.

**Evaluation Priority(**평가 우선순위**)** - 인증서의 해지 상태를 CRL에서 먼저 평가할지 OSCP에서 먼저 평가할지를 지정합니다.

- **Consider the certificate valid if revocation information cannot be reached(**해지 정보에 연결할 수 없는 경우 인증서를 유효한 것으로 간주**)** - 해지 정보에 연결할 수 없는 경우 인증서를 유효한 인증서로 간주하려면 이 확인란을 선택합니다.

  해지 확인에 대한 자세한 내용은 Cisco ASA Series 일반 운영 ASDM 설정의 "기본 설정" 책, XY 문서에서 "디지털 인증서" 장을 참조하십시오.

**Others(**기타**)** 탭을 클릭합니다.

- **Use CA Certificate for the Validation of(**다음을 위한 **CA** 인증서 사용**)** - 이 CA가 검증할 수 있는 연결 유형을 지정합니다.
  - **IPSec Client(IPSec** 클라이언트**)** - 원격 SSL 서버에서 제공하는 인증서를 검증합니다.
  - **SSL Client(SSL** 클라이언트**)** - 수신 SSL 연결에서 제공하는 인증서를 검증합니다.
  - **SSL Server(SSL** 서버**)** - 수신 IPSec 연결에서 제공하는 인증서를 검증합니다.
- 기타 옵션:
  - **Enable CA flag in basic constraints extension(**기본 제약 확장에서 **CA** 플래그 활성화**)** - 기본 제약 확장을 사용하는 인증서의 주체가 CA인지 검증하려면 이 옵션을 선택합니다.
  - **Accept certificates issued by this CA(CA**에서 발급된 인증서 허용**)** - ASA에서 지정된 CA의 인증서를 허용해야 하는 경우 이 옵션을 선택합니다.
  - **Accept certificates issued by the subordinates CAs of this CA(**이 **CA**의 하위 **CA**에서 발급한 인증서 수락**)** - ASA에서 하위 CA의 인증서를 허용해야 하는 경우 이 옵션을 선택합니다.
  - **Ignore IPsec Key Usage(IPsec** 키 사용 무시**)** - IPsec 원격 클라이언트 인증서의 키 사용 및 확장 키 사용 확장 값을 검증하지 않으려는 경우 이 옵션을 선택합니다. IPsec 클라이언트 인증서를 확인하는 키 사용을 억제할 수 있습니다. 기본적으로 이 옵션은 활성화되어 있지 않습니다.

단계 **8** **Add(**추가**)**를 클릭합니다.

이렇게 하면 트러스트 포인트 인증서 개체가 생성됩니다.

# 인증서 내용을 기반으로 하는 자체 서명 및 CSR 인증서 생성

자체 서명 및 CSR 인증서의 CN 및 SANS 콘텐츠에 대한 아이디어가 필요합니다. 콘텐츠는 생성 과정에서 지정한 매개변수를 기반으로 합니다. AnyConnect 클라이언트가 조직의 원하는 VPN 헤드엔드에 연결하려면 매개변수를 정확하게 구성해야 합니다.

이 섹션에서는 지정된 매개변수를 기반으로 자체 서명 및 CSR 인증서의 내용에 대한 아이디어를 제공하는 다양한 사용 사례를 예시와 함께 제공합니다.

사용 사례 **1:** 다른 **CN** 및 **FQDN** 값

예:

- Common Name(공용 이름)(CN): mywebsite.com
- FQDN: mysan.com

표 ***18:*** 예***:*** 다른 ***CN*** 및 ***FQDN*** 값

| | 공용 이름**(CN)** | **unstructuredName** | **SANS** |
|---|---|---|---|
| 자체 서명 | mywebsite.com | mysan.com | mysan.com |
| CSR | mywebsite.com | mysan.com | - |

사용 사례 **2:** 없음으로 설정된 **FQDN** 필드

예:

- Common Name(공용 이름)(CN): mywebsite.com
- FQDN: 없음

표 ***19:*** 예***:*** 없음으로 설정된 ***FQDN*** 필드

| | 공용 이름**(CN)** | **SANS** |
|---|---|---|
| 자체 서명 | Host Name(호스트 이름) | - |
| CSR | mywebsite.com | - |

사용 사례 **3: FQDN** 없음**(**기본 **FQDN)**

예:

- Common Name(공용 이름)(CN): mywebsite.com

표 *20:* 예*: FQDN* 없음*(*기본 *FQDN)*

| | 공용 이름**(CN)** | **unstructuredName** | **SANS** |
|---|---|---|---|
| 자체 서명 | mywebsite.com | 호스트 이름 | - |
| CSR | mywebsite.com | 호스트 이름 | Host Name(호스트 이름) |

사용 사례 **4: FQDN**에 **IP** 주소가 지정됨

예:

- Common Name(공용 이름)(CN): mywebsite.com
- FQDN: 4.5.6.7

표 *21:* 예*: FQDN*에 *IP* 주소가 지정됨

| | 공용 이름**(CN)** | **unstructuredName** | **SANS** |
|---|---|---|---|
| 자체 서명 | mywebsite.com | 4.5.6.7 | - |
| CSR | mywebsite.com | 4.5.6.7 | 4.5.6.7 |

사용 사례 **5: IP** 주소가 지정됨

예:

- IP 주소: 4.5.6.7
- Common Name(공용 이름)(CN): mywebsite.com
- FQDN: fqdn.com

표 *22:* 예*: IP* 주소가 지정됨

| | 공용 이름**(CN)** | **unstructuredAddress** | **unstructuredName** | **SANS** |
|---|---|---|---|---|
| 자체 서명 | mywebsite.com | 4.5.6.7 | fqdn.com | - |
| CSR | mywebsite.com | 4.5.6.7 | fqdn.com | fqdn.com |

사용 사례 **6:** 일련 번호 확인란이 선택됨

예:

- 일련 번호: 9AQXMWOKDT9

표 *23:* 예*: IP* 일련 번호 확인란이 선택됨

| | serialNumber | SANS |
|---|---|---|
| 자체 서명 | 9AQXMWOKDT9 | - |
| CSR | 9AQXMWOKDT9 | fqdn.com |

활용 사례 **7:** 이메일 주소가 지정됨

예:

- EA: abc@xyz.com

표 *24:* 예*:* 이메일 주소가 지정됨

| | unstructredName | emailAddress | SANS |
|---|---|---|---|
| 자체 서명 | Host Name(호스트 이름) | abc@xyz.com | Host Name(호스트 이름) |
| CSR | Host Name(호스트 이름) | abc@xyz.com | - |

# RA VPN 개체

# 서비스 개체

## ASA 서비스 개체

ASA 서비스 개체, 서비스 그룹 및 포트 그룹은 IP 프로토콜 제품군의 일부로 간주되는 프로토콜 또는 포트를 포함하는 재사용 가능한 구성 요소입니다. 서비스 개체에서 단일 프로토콜을 지정하고 이를 소스 포트, 목적지 포트 또는 소스 및 목적지 포트 모두에 할당할 수 있습니다. 서비스 그룹은 여러 서비스 개체를 포함하며 여러 프로토콜을 포함할 수 있습니다.

포트 그룹은 일종의 ASA 서비스 개체입니다. 포트 그룹은 서비스 유형(예: TCP 또는 UDP)과 포트 번호 또는 포트 번호 범위를 페어링하는 포트 개체를 포함합니다. 그 다음 트래픽 일치 기준을 정의하는 목적으로 보안 정책의 개체를 사용할 수 있습니다. 예를 들어 액세스 제어 규칙에서 이를 사용하여 특정 TCP 포트 범위에 대한 트래픽을 허용할 수 있습니다.

자세한 내용은 ASA 서비스 개체 생성 및 편집을 참조하십시오.

### 프로토콜 개체

프로토콜 개체는 덜 일반적으로 사용되는 또는 레거시 프로토콜을 포함하는 서비스 개체 유형입니다. 프로토콜 개체는 이름 및 프로토콜 번호로 식별됩니다. CDO는 ASA 및 Firepower(FDM 관리) 구성에서 이러한 개체를 인식하고 사용자가 쉽게 찾을 수 있도록 자체 필터인 "프로토콜"을 제공합니다.

### ICMP 개체

ICMP(Internet Control Message Protocol) 개체는 ICMP 및 IPv6-ICMP 메시지를 위한 서비스 개체입니다. CDO는 ASA 및 Firepower 구성에서 해당 디바이스가 온보딩되고 사용자가 개체를 쉽게 찾을 수 있도록 해당 디바이스에 "ICMP" 필터를 제공할 때 이러한 개체를 인식합니다.

CDO를 사용하면 ASA 구성에서 ICMP 개체를 제거하거나 이름을 바꿀 수 있습니다. CDO를 사용하여 Firepower 구성에서 ICMP 및 ICMPv6 개체를 생성, 업데이트 및 삭제할 수 있습니다.

**Note** ICMPv6 프로토콜의 경우 AWS는 특정 인수 선택을 지원하지 않습니다. 모든 ICMPv6 메시지를 허용하는 규칙만 지원됩니다.

관련 정보:

- 개체 삭제, on page 122

# ASA 서비스 개체 생성 및 편집

서비스 개체에서 단일 프로토콜을 지정하고 이를 소스 포트, 목적지 포트 또는 소스 및 목적지 포트 모두에 할당할 수 있습니다.

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2** **Create Object(**개체 생성**)** > **ASA** > **Service(**서비스**)**를 클릭합니다.

단계 **3** 개체 이름을 입력합니다.

단계 **4** 서비스 개체 생성을 선택합니다.

단계 **5** **Service Type(**서비스 유형**)** 버튼을 클릭하고 개체를 만들 프로토콜을 선택합니다.

- **TCP, UDP** 및 **TCP-UDP** 서비스 유형의 경우 소스 포트, 목적지 포트 또는 둘 다를 입력합니다.
  - 소스 포트 식별자를 사용하면 번호가 지정된 특정 포트에서 시작되는 트래픽을 일치시킬 수 있습니다. 소스 포트 식별자에서 같음, 범위, 보다 작음, 보다 큼 또는 같지 않음 연산자를 선택하고 적절한 포트 번호 또는 범위를 제공합니다.
  - 목적지 포트 식별자를 사용하면 번호가 지정된 특정 포트에 도착하는 트래픽을 일치시킬 수 있습니다. 목적지 포트 식별자에서 같음, 범위, 보다 작음, 보다 큼 또는 같지 않음 연산자를 선택하고 적절한 포트 번호 또는 범위를 제공합니다.
- 프로토콜 서비스 유형에 대해, 0-255 사이의 프로토콜 번호 또는 ip, tcp, udp, gre 등과 같이 잘 알려진 이름을 입력합니다.

단계 **6** **Add(**추가**)**를 클릭합니다.

예

- 수신 FTP 트래픽을 식별하는 서비스 개체는 TCP 서비스 유형 및 대상 포트 범위가 21인 개체입니다.
- 발신 DNS 및 TCP 트래픽을 통한 DNS를 식별하는 서비스 개체는 tcp-udb 서비스 유형 및 소스 포트가 53인 개체입니다.

## ASA 서비스 그룹 생성

서비스 그룹은 하나 이상의 프로토콜을 나타내는 하나 이상의 서비스 개체로 구성될 수 있습니다.

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2** **Create Object(**개체 생성**) > ASA > Service(**서비스**)**를 클릭합니다.

단계 **3** 개체 이름을 입력합니다.

단계 **4** **Create a service group(**서비스 그룹 생성**)**를 선택합니다.

단계 **5** **Add Object(**개체 추가**)**를 클릭하고, 개체를 선택하고, **Select(**선택**)**을 클릭하여 기존 개체를 추가합니다. 개체를 더 추가하려면 이 단계를 반복합니다.

단계 **6** 필요한 경우 서비스 그룹에 별도의 개별 서비스 유형 값을 추가합니다.

- **TCP, UDP** 및 **TCP-UDP** 서비스 유형의 경우 소스 포트, 목적지 포트 또는 둘 다를 입력합니다.
  - 소스 포트 식별자를 사용하면 번호가 지정된 특정 포트에서 시작되는 트래픽을 일치시킬 수 있습니다. 소스 포트 식별자에서 같음, 범위, 보다 작음, 보다 큼 또는 같지 않음 연산자를 선택하고 적절한 포트 번호 또는 범위를 제공합니다.
  - 목적지 포트 식별자를 사용하면 번호가 지정된 특정 포트에 도착하는 트래픽을 일치시킬 수 있습니다. 목적지 포트 식별자에서 같음, 범위, 보다 작음, 보다 큼 또는 같지 않음 연산자를 선택하고 적절한 포트 번호 또는 범위를 제공합니다.
- 프로토콜 서비스 유형에 대해, 0-255 사이의 프로토콜 번호 또는 ip, tcp, udp, gre 등과 같이 잘 알려진 이름을 입력합니다.

단계 **7** 개별 포트 값을 더 추가하려면 **Add Another Value(**다른 값 추가**)**를 클릭하고 단계 6을 반복합니다.

단계 **8** 서비스 그룹에 서비스 개체 및 서비스 값 추가를 완료하면 **Add(**추가**)**를 클릭합니다.

## ASA 서비스 개체 또는 서비스 그룹 편집

단계 **1** 좌측의 CDO 탐색 모음에서 **Objects(**개체**) > ASA Objects(ASA** 개체**)**를 클릭합니다.

단계 **2** 개체를 필터링하여 편집할 개체를 찾은 다음 개체 테이블에서 개체를 선택합니다.

단계 **3** 세부 정보 창에서 Edit(편집) 를 클릭합니다.

단계 **4** 위의 절차에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 수정합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

단계 **6** CDO에 변경의 영향을 받을 정책이 표시됩니다. **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

# ASA 시간 범위 개체

시간 범위 개체란 무엇입니까**?**

시간 범위 개체는 특정 시간을 정의하며 시작 시간, 종료 시간, 선택 사항인 반복 항목으로 구성됩니다. 네트워크 정책에서 이 개체를 사용하여 특정 기능 또는 자산에 대한 시간 기반 액세스를 제공합니다. 예를 들어, 업무 시간에만 특정 서버에 대한 액세스를 허용하는 액세스 규칙을 만들 수 있습니다. 시간 범위 생성은 디바이스에 대한 액세스를 제한하지 않습니다. 이러한 개체에 대해 구성된 시간은 디바이스에 대해 로컬입니다.

이 개체에 절대 또는 반복 시간 범위를 추가할 수 있습니다. 반복 범위는 주기적인 시간 범위로 간주됩니다.

**Note** 시간 범위에 절대값과 기간 값이 모두 지정된 경우, 절대 시작 시간에 도달해야 기간 값의 평가가 이루어지며 절대 종료 시간에 도달하면 더 이상 평가되지 않습니다.

# ASA 시간 범위 개체 생성

다음 절차에 따라 ASA 디바이스에 대한 시간 범위 개체를 생성합니다.

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2** 파란색 더하기 버튼 을 클릭하여 개체를 생성합니다.

단계 **3** **ASA** > 시간범위**(Time Range)**를 클릭합니다.

단계 **4** 개체 이름을 입력합니다.

단계 **5** 시간 범위를 정의합니다.

- 절대 시간 범위 - 원하는 시간 범위에 대한 시작 시각과 종료 시각을 입력합니다. 몇 분, 몇 시간, 며칠 또는 몇 주에 걸쳐 이 개체를 실행하도록 선택할 수 있습니다. 시간 범위 개체는 하나의 절대 시간 범위만 가질 수 있습니다.

- 반복 시간 범위 - 를 클릭하여 일주일 내내 반복되는 주기적 시간 범위를 추가합니다. 드롭다운 메뉴에서 **Frequency(**빈도**)**, 시간 범위가 적용될 **Days(**요일**)** 및 **Start(**시작**)** 및 **End(**종료**)** 시각을 선택합니다. 시간 범위 개체는 여러 주기 범위를 가질 수 있습니다.

**Note** 시간 범위 개체에 대한 시작 및 종료 시각은 옵션입니다. 개체에 설정된 시작 시각이 없는 경우 시간 범위가 즉시 적용됩니다. 개체에 설정된 종료 시각이 없는 경우 시간 범위는 무기한 지속됩니다.

단계 6 **Add(**추가**)**를 클릭하여 개체를 생성합니다.

# ASA 시간 범위 개체 편집

다음 절차를 사용하여 ASA 디바이스에 대한 시간 범위 개체를 편집합니다.

단계 1 좌측의 CDO 탐색 모음에서 **Objects(**개체**) > ASA Objects(ASA** 개체**)**를 클릭합니다.

단계 2 개체를 필터링하여 편집할 개체를 찾은 다음 개체 테이블에서 개체를 선택합니다.

단계 3 세부 정보 창에서 Edit(편집)  를 클릭합니다.

단계 4 필요에 따라 값을 편집하고 **Save(**저장**)**를 클릭합니다.

단계 5 개체가 현재 정책에서 사용 중인 경우 CDO는 변경의 영향을 받는 정책을 표시합니다. **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

단계 6 개체가 디바이스의 정책에서 사용되는 경우 변경 사항을 지금 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 여러 변경 사항을 여러 변경 사항을 한 번에 배포합니다.

관련 정보**:**

- 개체 삭제
- ASA 레거시 네트워크 정책

# 보안 정책 관리

보안 정책에서 네트워크 트래픽을 검사하는 궁극적인 목표는 트래픽을 의도한 대상으로 허용하거나 보안 위협이 식별된 경우 트래픽을 삭제하는 것입니다. CDO를 사용하여 다양한 유형의 디바이스에서 보안 정책을 구성할 수 있습니다.

- ASA 정책(확장 액세스 목록), 215 페이지
- 네트워크 주소 변환, 222 페이지

# ASA 레거시 네트워크 정책

이 섹션에서는 Cisco CDO(Defense Orchestrator)에서 관리하는 모든 디바이스에서 사용 중인 모든 네트워크 정책 목록을 표시하는 레거시 네트워크 정책 페이지에 대한 정보를 제공합니다. **Policies(**정책**) > ASA Policies(ASA** 정책**)**을 탐색하여 네트워크 정책 페이지로 이동합니다.

네트워크 정책은 네트워크 규칙의 모음입니다. 각 네트워크 규칙은 원본 및 대상 IP 주소, IP 프로토콜, 포트 번호, EtherType 등과 같은 특성을 기반으로 네트워크 트래픽이 네트워크 대상에 도달하는 것을 허용하거나 방지합니다.

CDO는 네트워크 정책을 생성할 때 이를 ASA 인터페이스와 연결하고 정책에 하나의 기본 규칙을 생성합니다. 네트워크 정책은 인터페이스와 연결될 때 ASA에서 "액세스 그룹"이라고 합니다. 정책 이름은 ASA의 ACL(액세스 제어 목록) 이름과 동일합니다. CDO가 만든 기본 규칙과 이 네트워크 정책에 추가하는 후속 규칙을 ASA에서는 ACE(액세스 제어 항목)이라고 합니다.

관련 정보:

- 레거시 보기에서 ASA 네트워크 정책 생성
- ASA 네트워크 정책 편집
- ASA 네트워크 정책 복사
- ASA 네트워크 정책 비교
- ASA 네트워크 정책 삭제
- ASA 네트워크 정책 및 규칙 검색 및 필터링
- 공유 ASA 네트워크 정책
- ACE(액세스 제어 항목)

# 레거시 보기에서 ASA 네트워크 정책 생성

이 절차를 사용하여 ASA 네트워크 정책을 생성합니다.

단계 1 **Policies(**정책**)** > **ASA Policies(ASA** 정책**)**를 선택합니다.

단계 2 **Create Policy(**정책 생성**)**를 클릭합니다.

단계 3 디바이스 필터를 클릭하여 정책을 저장할 디바이스를 검색하십시오.

단계 4 정책의 이름을 입력합니다. 참고로 디바이스에 이름이 같은 두 개의 네트워크 정책이 있을 수 없습니다.

단계 5 이 정책을 적용하려는 인터페이스를 선택합니다.

단계 6 정책이 아웃바운드 또는 인바운드 트래픽용인지 지정합니다. 참고로 동일한 디바이스에서 동일한 방향으로 동일한 인터페이스에 대해 두 개의 정책을 가질 수 없습니다.

단계 7 **Save(**저장**)**를 클릭합니다. CDO는 네트워크 정책 및 해당 정책에 대한 단일 "permit IP any any" 규칙을 생성합니다.

단계 8 필요에 따라 ASA 네트워크 정책 편집합니다.

단계 9 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

# ASA 네트워크 정책 편집

Defense Orchestrator를 사용하면 정책 세부 정보 페이지에서 네트워크 정책 및 정책 규칙을 편집할 수 있습니다. 다음과 같은 방법으로 ASA 정책을 편집할 수 있습니다.

- 정책 이름 변경

## 정책 이름 변경

단계 **1** **Policies(**정책**)** > **ASA Policies(ASA** 정책**)**를 선택합니다.

단계 **2** 이름을 바꾸려는 네트워크 정책을 선택합니다.

단계 **3** 세부 정보 창에서 이름 변경 아이콘 를 클릭합니다.

단계 **4** 정책 이름을 편집한 다음 파란색 확인란을 클릭하여 변경 사항을 저장합니다.

## 정책에 규칙 추가

단계 **1** **Policies(**정책**)** > **ASA Policies(ASA** 정책**)**을 선택합니다.

단계 **2** 편집하려는 네트워크 정책을 선택합니다.

단계 **3** **Edit Policy(**정책 편집**)**를 클릭합니다.

단계 **4** 세부 정보 창에서 도구 편집 도구 모음의 을 클릭하여 네트워크 정책에 규칙을 추가합니다. 정책에서 강조 표시된 규칙 위에 새 규칙이 추가됩니다. 규칙은 규칙 목록의 위치에 따라 1부터 "마지막"까지 우선 순위가 지정됩니다.

**Note** 새 규칙에는 기본적으로 **Permit(**허용**)** 작업이 할당됩니다.

단계 **5** **Save(**저장**)**를 클릭합니다. Defense Orchestrator는 변경의 영향을 받는 디바이스를 식별합니다.

단계 **6** 정책 세부 정보 창에서 디바이스 필드를 검토합니다. 최적의 항목 수를 초과한 경우 ASA가 설치된 ASA 하드웨어 모델에 따라 "ACE 수 초과, 최대 항목 500개, 1000개 발견"과 같은 경고가 표시됩니다.

단계 **7** 지금 변경한 내용을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 정책 내에서 규칙 이동

단계 **1** **Policies(**정책**)** > **ASA Policies(ASA** 정책**)**을 선택합니다.

단계 **2** 네트워크 정책을 선택합니다.

단계 **3** 세부 정보 창에서 **Edit Policy(**정책 편집**)**를 클릭합니다.

단계 4 규칙 테이블에서 규칙을 선택하고 편집 도구 모음에서 **cut(**잘라내기**)** 를 클릭합니다.

단계 5 방금 잘라낸 규칙이 앞에 오도록 할 규칙을 선택합니다. 규칙은 규칙 목록에서 위치별로 우선 순위가 지정됩니다. 규칙이 높을수록 우선 순위가 높아집니다.

단계 6 Paste(붙여넣기) 를 클릭합니다.

단계 7 **Save(**저장**)**를 클릭합니다. Defense Orchestrator는 변경의 영향을 받는 디바이스를 식별합니다.

단계 8 지금 변경한 내용을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 정책 간 규칙 이동

한 정책에서 규칙을 복사하여 다른 정책에 붙여넣을 수 있습니다.

단계 1 **Policies(**정책**) > ASA Policies(ASA** 정책**)**를 선택합니다.

단계 2 복사할 규칙이 있는 네트워크 정책을 선택합니다.

단계 3 세부 정보 창에서 **Edit Policy(**정책 편집**)**를 클릭합니다.

단계 4 규칙 테이블에서 규칙을 선택하고 편집 도구 모음에서 **copy(**복사**)** 를 클릭합니다.

단계 5 **Policies(**정책**) > ASA Policies(ASA** 정책**)**을 선택합니다.

단계 6 규칙을 복사할 네트워크 정책을 선택합니다.

단계 7 세부 정보 창에서 **Edit Policy(**정책 편집**)**를 클릭합니다.

단계 8 방금 복사한 규칙 뒤에 올 규칙을 선택합니다. 규칙은 규칙 목록에서 위치별로 우선 순위가 지정됩니다. 규칙이 높을수록 우선 순위가 높아집니다.

단계 9 Paste(붙여넣기) 를 클릭합니다.

단계 10 **Save(**저장**)**를 클릭합니다. Defense Orchestrator는 변경의 영향을 받는 디바이스를 식별합니다.

단계 11 지금 변경한 내용을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 정책에서 규칙 비활성화

규칙은 기본적으로 활성화되어 있습니다. 정책 내에서 개별 규칙을 비활성화할 수 있습니다.

단계 1 **Policies(**정책**) > ASA Policies(ASA** 정책**)**을 선택합니다.

단계 2 비활성화하려는 규칙이 있는 네트워크 정책을 선택합니다.

단계 3 세부 정보 창에서 **Edit Policy(**정책 편집**)**를 클릭합니다.

단계 4 비활성화하려는 규칙을 선택합니다.

단계 5 활성 설정을 끕니다. 


단계 6 **Save(**저장**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다. Defense Orchestrator는 변경의 영향을 받는 디바이스를 식별합니다.

단계 **8** 지금 변경한 내용을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 로그 규칙 활동

네트워크 정책 규칙으로 인한 활동은 기본적으로 로깅되지 않습니다. 개별 규칙에 대한 로깅을 활성화할 수 있습니다.

단계 **1** **Policies(**정책**)** > **ASA Policies(ASA** 정책**)**를 선택합니다.

단계 **2** 활성화하려는 규칙이 있는 네트워크 정책을 선택합니다.

단계 **3** 세부 정보 창에서 **Edit Policy(**정책 편집**)**를 클릭합니다.

단계 **4** 활동을 로깅하려는 규칙을 선택합니다.

단계 **5** 로깅을 활성화하려면 슬라이더를 클릭합니다. 

단계 **6** **Edit(**편집**)**를 클릭합니다.

단계 **7** 해당 규칙의 활동이 수집되는 로깅 수준과 빈도를 선택합니다. 다음 표는 Syslog 메시지 심각도 수준을 나열합니다.

| 심각도 레벨 | 설명 |
|---|---|
| **emergencies(**비상**)** | 시스템을 사용할 수 없습니다. |
| **Alert(**긴급 경고**)** | 즉각적인 행동이 필요합니다. |
| **critical(**심각**)** | 심각한 상태입니다. |
| **error(**오류**)** | 오류 상태입니다. |
| **warning(**경고**)** | 경고 상태입니다. |
| **notification(**알림**)** | 일반적이지만 중요한 상태입니다. |
| **informational(**정보**)** | 정보 메시지만 해당됩니다. |
| **debugging(**디버깅**)** | 디버깅 메시지만 해당됩니다. |
| **Note** | ASA는 심각도 레벨이 0(응급)인 Syslog 메시지를 생성하지 않습니다. |

단계 **8** 로깅 간격을 변경할 수도 있습니다. 로깅 간격은 해당 간격 동안 로그에 도달한 횟수를 보여줍니다. 로깅 간격은 1~600초 범위에서 정의됩니다. 기본값은 300입니다. 이 값은 삭제 통계 수집에 쓰이는 캐시에서 비활성 플로우을 삭제하기 위한 시간 초과 값으로도 사용됩니다.

단계 **9** **Save(**저장**)**를 클릭합니다. Defense Orchestrator는 변경의 영향을 받는 디바이스를 식별합니다.

단계 **10** 지금 변경한 내용을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 정책의 시간 범위 정의

시간 기반 ASA 네트워크 정책은 시간을 기준으로 네트워크 및 리소스에 대한 액세스를 허용합니다. 시간은 시간 범위 개체로 정의됩니다. 시간 범위 개체에는 시작 시간과 종료 시각이 있으며 반복 이벤트로 정의할 수도 있습니다.

시간 범위 개체가 ASA에 이미 정의되어 있는 경우 이를 네트워크 정책과 연결할 수 있습니다. 시간 범위 개체가 ASA에 아직 존재하지 않는 경우 Defense Orchestrator의 CLI 도구를 사용하여 생성하거나 ASA에서 직접 생성해야 합니다.

네트워크 정책에 대한 시간 범위를 추가하려면 다음 절차를 따르십시오.

단계 **1** **Policies(**정책**)** > **ASA Policies(ASA** 정책**)**를 선택합니다.

단계 **2** 편집하려는 네트워크 정책을 선택합니다.

단계 **3** **Edit Policy(**정책 편집**)**를 클릭합니다.

단계 **4** 네트워크 정책 상자에서 슬라이더를 클릭하여 시간 범위를 활성화합니다.

단계 **5** 시간 범위 개체를 생성하거나 드롭다운 목록에서 기존 시간 범위 개체를 **Choose(**선택**)**합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

단계 **7** **Devices & Services(**디바이스 및 서비스**)** 페이지로 돌아가 방금 정책을 편집한 디바이스를 선택합니다. 디바이스가 동기화되지 않았는지 확인해야 합니다.

단계 **8** 미리보기 및 배포**...**를 클릭합니다.

단계 **9** 디바이스 동기화 상자에서 정책을 생성할 명령과 정책의 규칙을 검토합니다.

단계 **10** 제안된 변경 사항에 만족하면 **Apply Changes to Device(**디바이스에 변경 사항 적용**)**를 클릭합니다.

단계 **11** 지금 변경한 내용을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

# ASA 네트워크 정책 복사

이 절차를 사용하여 한 ASA에서 다른 ASA로 네트워크 정책을 복사합니다.

단계 **1** **Policies(**정책**)** > **ASA Policies(ASA** 정책**)**를 선택합니다.

단계 **2** 복사하려는 정책을 검색하고 필터링합니다.

단계 **3** 복사할 네트워크 정책 행에서 **copy icon(**복사 아이콘**)**를 클릭합니다.

단계 **4** 디바이스에 정책을 추가합니다.

- 단일 인터페이스에 할당된 네트워크 정책의 경우: **Add Policy to Device(**디바이스에 정책 추가**)** 대화 상자에서 정책을 복사할 디바이스, 인터페이스 및 트래픽 방향을 선택합니다. 전역 액세스 정책을 다른 디바이스에 복사하는 경우
- 전역 정책의 경우: **Add Policy to Device(**디바이스에 정책 추가**)** 대화 상자에서 정책을 복사할 디바이스를 선택하고 전역 정책으로 만들기를 선택합니다. 정책에 대한 인터페이스나 방향을 선택할 수 없음을 알 수 있습니다. 전역 정책은 항상 디바이스의 모든 인터페이스에 할당되며 항상 인바운드 트래픽을 평가합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

단계 **6** 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

# ASA 네트워크 정책 비교

단계 **1** 탐색 창에서 **Policies(**정책**) > ASA Policies(ASA** 정책**)**을 선택합니다.

단계 **2** 뷰어의 오른쪽 상단에서 **Compare(**비교**)**를 클릭합니다.

단계 **3** 비교할 최대 2개의 정책을 선택합니다.

단계 **4** 뷰어 하단에서 **View Comparison(**비교 보기**)**를 클릭합니다. 그러면 비교 뷰어가 나타납니다. 마치면 **Done(**완료**)**를 클릭한 다음 **Done Comparing(**비교 완료**)**를 클릭합니다.

# ASA 네트워크 정책 삭제

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 **3** **ASA** 탭을 클릭하고 정책을 삭제할 ASA를 검색하여 선택합니다.

단계 **4** 관리 창에서 **Configuration(**구성**)**를 클릭합니다.

단계 **5** **Edit(**편집**)**를 클릭합니다.

단계 **6** 디바이스 구성에서 네트워크 정책 및 규칙을 찾습니다.

네트워크 정책은 ASA 구성 파일에서 액세스 그룹이라고 하며 형식은 다음과 같습니다.

```
access-group <policy name> <direction of traffic> interface <interface name>
```

다음은 액세스 그룹 항목의 예입니다.

```
access-group abc-75-1-out out interface interface-1
```

네트워크 규칙은 ASA 구성 파일에서 액세스 목록이라고 하며 형식은 다음과 같습니다.

```
access-list <policy name> extended permit ip any any
```

다음은 액세스 목록 항목의 예입니다.

```
access-list abc-75-1-out extended permit ip any any
```

단계 **7** 네트워크 정책이 포함된 행과 네트워크 규칙이 포함된 행을 강조 표시하고 삭제합니다.

단계 **8** 변경 사항을 **Save(**저장**)**합니다.

단계 **9** 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

# ASA 네트워크 정책 및 규칙 검색 및 필터링

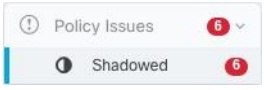
검색 표시줄을 사용하여 네트워크 정책의 이름과 정책 내의 규칙에서 이름, 키워드 또는 구를 검색합니다. 검색은 대/소문자를 구분하지 않습니다.

### 필터

필터 사이드바를 사용하여 네트워크 정책 문제, 공유 정책 및 특정 디바이스에 대한 정책을 찾으십시오. 필터링은 추가되지 않으며 각 필터 설정은 서로 독립적으로 작동합니다.

### 정책 문제

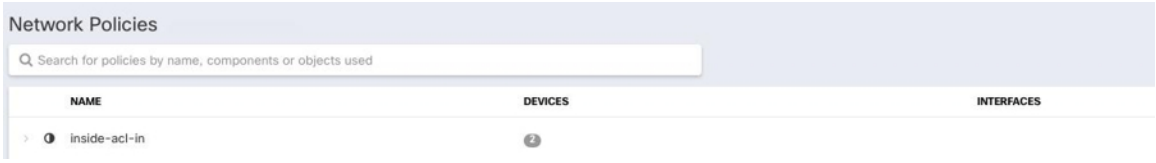
CDO는 섀도우 규칙이 포함된 네트워크 정책을 식별합니다. 섀도우 규칙을 포함하는 정책의 수는 정책 문제 필터에 표시됩니다.




CDO는 네트워크 정책 페이지에서 섀도우 배지 ◑로 섀도우 규칙과 이를 포함하는 네트워크 정책을 표시합니다. 섀도우 규칙을 포함하는 모든 정책을 보려면 **Shadowed(**숨겨짐**)**를 클릭합니다. 자세한 내용은 섀도우 규칙을 참조하십시오.

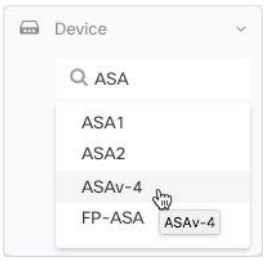
### 공유 정책

공유 정책은 두 개 이상의 디바이스에서 발견되는 정책입니다. 공유 정책에 대한 변경 사항은 해당 정책이 있는 모든 디바이스에 영향을 미칩니다. 아래 예에서 **inside-acl-in** 정책은 두 디바이스에서 공유됩니다. 자세한 내용은 공유 ASA 네트워크 정책을 참조하십시오.



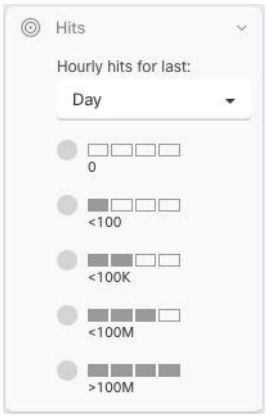

### 디바이스

**Device(**디바이스**)** 필터를 확장하고 **Search devices(**디바이스 검색**)** 필드에 이름 또는 IP 주소를 입력한 다음 결과에서 찾은 디바이스를 선택하여 디바이스별로 네트워크 정책 목록을 필터링합니다.




**Hits(**히트**)**

이 필터를 사용하여 지정된 기간 동안 여러 번 트리거된 디바이스 전체의 정책을 찾으십시오.




## 적중 횟수가 0인 모든 네트워크 정책 찾기

적중되지 않은 네트워크 정책이 있는 경우 정책을 수정하여 더 효과적으로 만들거나 간단히 삭제할 수 있습니다.

단계 **1** **Policies(**정책**)** > **ASA Policies(**정책**)**을 탐색합니다.
단계 **2** 필터 창에서 **Show All(**모두 표시**)**을 클릭하여 기존 필터를 지웁니다.
단계 **3** Hits(적중) 필터를 확장합니다.
단계 **4** 기간을 선택합니다.
단계 **5** 0의 적중 횟수를 선택합니다.

## 적중 횟수가 0인 디바이스의 모든 네트워크 정책 찾기

단계 **1** **Policies(**정책**)** > **ASA Policies(**정책**)**을 탐색합니다.
단계 **2** 필터 창에서 **Show All(**모두 표시**)**을 클릭하여 기존 필터를 지웁니다.
단계 **3** 디바이스 필터를 확장하고 필터링할 디바이스를 선택합니다.
단계 **4** Hits(적중) 필터를 확장합니다.

단계 **5** 기간을 선택합니다.
단계 **6** 0의 적중 횟수를 선택합니다.

## 네트워크 정책의 규칙이 적중되는 빈도 찾기

단계 **1** **Policies(**정책**)** > **ASA Policies(**정책**)**을 탐색합니다.
단계 **2** 필터 창에서 **Show All(**모두 표시**)**을 클릭하여 기존 필터를 지웁니다.
단계 **3** 하나의 디바이스에서 사용되는 네트워크 정책을 선택합니다.
단계 **4** 네트워크 정책의 각 규칙이 적중되는 빈도를 알아보려면 규칙 테이블의 **Hits(**적중**)** 열을 살펴보십시오.
단계 **5** 네트워크 정책에 규칙이 너무 많아 결과를 한 눈에 볼 수 없는 경우 적중 필터를 확장합니다.
단계 **6** 기간을 선택합니다.
단계 **7** 다른 적중 필터를 선택하여 다른 규칙이 어떤 범주에 속하는지 확인합니다.

## 공유 네트워크 정책이 적중되는 빈도 찾기

네트워크 정책에 대한 적중은 개별 디바이스에 대해 계산됩니다. 필터에서 디바이스를 지정하지 않으면 두 개 이상의 디바이스에서 공유되는 단일 네트워크 정책에 대한 적중률을 확인할 수 없습니다.

단계 **1** **Policies(**정책**)** > **ASA Access Policies(ASA** 액세스 정책**)**를 탐색합니다.
단계 **2** 기존 정책을 지우려면 정책 테이블 위에서 **Clear(**지우기**)**를 클릭합니다.
단계 **3** Shared Policies(공유 정책) 필터를 확장하고 **Shared(**공유**)**를 클릭합니다.
단계 **4** 공유 네트워크 정책을 선택합니다.
단계 **5** 해당 정책의 세부 정보 창에서 해당 네트워크 정책을 사용하는 디바이스를 기록한 다음 네트워크 정책 테이블로 돌아갑니다.
단계 **6** 검색 필드에 공유 정책의 이름을 입력합니다.
단계 **7** Devices(디바이스) 필터를 확장하고 공유 정책을 사용하는 디바이스 중 하나로 필터링합니다.
단계 **8** Hits(적중) 필터를 확장합니다.
단계 **9** 기간을 선택합니다.
단계 **10** 다른 적중 필터를 선택하여 어떤 범주에 속하는지 결정합니다.

## 적중률을 기준으로 네트워크 정책 필터링

단계 **1** **Policies(**정책**)** > **ASA Access Policies(ASA** 액세스 정책**)**를 탐색합니다.
단계 **2** 기존 필터를 지우려면 정책 테이블 위에서 **Clear(**지우기**)**를 클릭합니다.
단계 **3** Hits(적중) 필터를 확장합니다.

단계 4 기간을 선택합니다.

단계 5 다른 적중률 범주를 선택합니다. CDO는 지정한 적중률만큼 적중되는 정책을 표시합니다. 적중률 기준과 일치하는 공유 네트워크 정책이 있는 경우 CDO는 공유 정책을 사용하는 모든 디바이스에 대한 행을 표시합니다.

# 공유 ASA 네트워크 정책

CDO(Cisco Defense Orchestrator)는 여러 ASA에서 사용하는 동일한 네트워크 정책을 찾아 네트워크 정책 페이지에서 식별합니다. 공유 네트워크 정책이 있는 경우 정책을 한 번 변경하고 공유되는 다른 디바이스에 변경 사항을 배포할 수 있습니다. 이렇게 하면 디바이스 간에 네트워크 정책이 일관되게 유지됩니다.

## 공유 네트워크 정책 속성

네트워크 정책 테이블은 네트워크 정책을 사용하는 디바이스 수를 식별합니다. 둘 이상의 디바이스에서 사용 중임을 나타내는 모든 네트워크 정책은 공유 정책입니다. 공유 네트워크 정책 찾기:

단계 1 **Policies(**정책**)** > **ASA Policies(**정책**)**을 탐색합니다.

단계 2 페이지에서 이전 필터링 또는 검색 기준을 지우려면 필터 창에서 **Show All(**모두 표시**)**을 클릭합니다.

단계 3 필터 표시줄에서 Shared Policies(공유 정책)를 확장하고 Shared(공유)를 선택합니다.

단계 4 검색을 더욱 구체화하려면 검색 창에 키워드를 입력합니다.

단계 5 네트워크 정책 테이블에서 공유 네트워크 정책을 선택합니다.

**Note** 필터 및 검색 기준은 조합하여 사용되지 않으며 한 번에 하나만 사용할 수 있습니다. 예를 들어 "Shared Policies(공유 정책)"로 필터링하면 모든 공유 정책이 표시됩니다. 디바이스 이름을 검색에 추가하면 정책 공유 여부와 상관없이 해당 디바이스 이름에서 사용하는 모든 네트워크 정책이 표시됩니다.

## 공유 네트워크 정책 편집

단계 1 편집할 공유 ASA 네트워크 정책.

단계 2 공유 정책을 선택합니다. CDO는 CDO에서 관리하는 디바이스가 해당 네트워크 정책을 사용하는지 식별합니다.

단계 3 세부 정보 창에서 **Edit Policy(**정책 편집**)**을 클릭합니다.

단계 4 정책에서 규칙을 수정합니다.

단계 5 **Save(**저장**)**를 클릭합니다.

단계 6 변경의 영향을 받을 디바이스를 확인합니다.

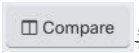
단계 7 Devices & Service(디바이스 및 서비스) 페이지를 열고 디바이스가 더 이상 동기화되지 않는지 확인합니다.

단계 **8** **Deploy Changes Manually(**수동으로 변경 사항 구축**)...**를 클릭하고 표시되는 지침에 따라 ASA에 저장된 구성을 변경 사항으로 업데이트합니다.

## 공유 네트워크 정책 비교

공유 네트워크 정책을 비교하는 목적은 약간 분기된 정책을 찾아 재정렬하는 것입니다. 거의 동일한 정책이 여러 개 있는 경우, 해당 정책이 분기되어 실제로는 동일해야 합니다. 네트워크 정책을 재정렬하면 CDO가 정책을 공유된 것으로 인식하며, 정책을 변경하면 해당 정책을 사용하여 다른 디바이스에 변경 사항을 배포할 수 있습니다.

단계 **1** 비교할 공유 ASA 네트워크 정책.

단계 **2** 비교 

를 클릭합니다.

단계 **3** 비교할 두 네트워크 정책을 선택하고 **View Comparison(**비교 보기**)**을 클릭합니다.

단계 **4** 차이점을 확인하고 **Done Comparing(**비교 완료**)**을 클릭합니다.

단계 **5** 정책 중 하나를 변경하여 다른 정책과 일치시키려면 네트워크 정책 테이블에서 해당 정책을 선택하고 세부 정보 창에서 **Edit Policy(**정책 편집**)**를 클릭하여 수정합니다.

# ASA 정책(확장 액세스 목록)

CDO(Cisco Defense Orchestrator)는 사용자에게 모든 디바이스에서 네트워크 및 애플리케이션 보안 정책을 일관되게 유지할 수 있는 기능을 제공합니다. 이 고유한 기능을 사용하면 여러 디바이스에서 동시에 정책을 간단하고 쉽게 변경할 수 있습니다.

# ACE(액세스 제어 항목)

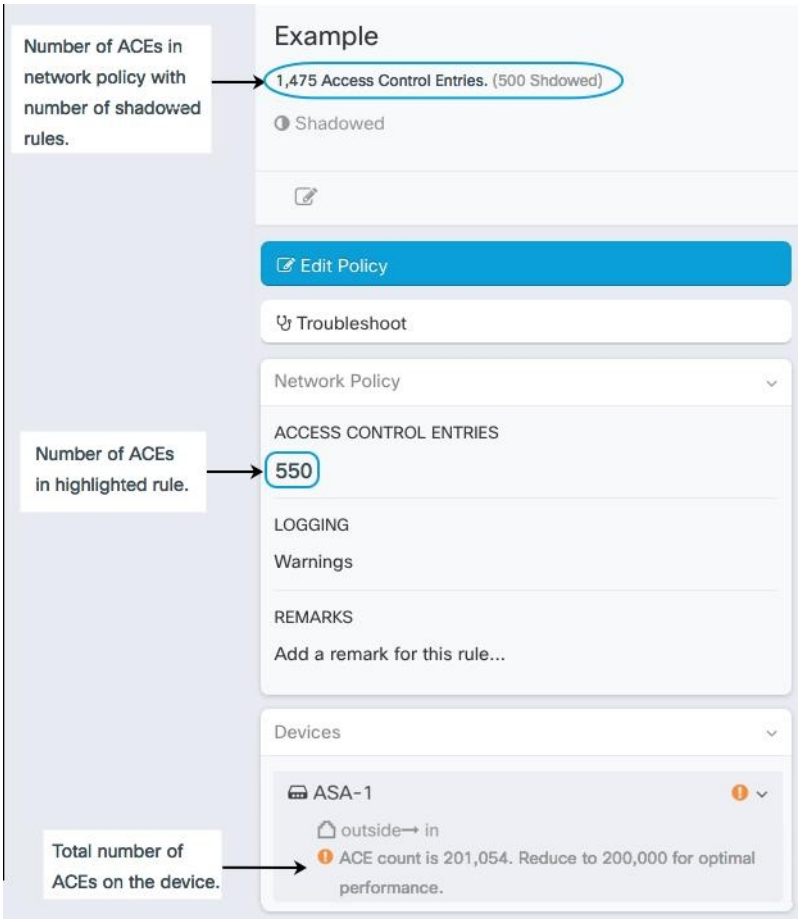
볼 수 있는 항목과 볼 수 없는 항목의 관점에서 액세스 제어 항목에 대해 생각해 보십시오.

여러분은 다음과 같은 것을 볼 수 있습니다. CDO의 사용자 인터페이스 측면에서 네트워크 정책에 추가하는 규칙은 ASA의 액세스 제어 항목입니다. 이 규칙은 소스와 대상 주소 또는 한 주소 그룹과 다른 주소 그룹 간에 허용되는 네트워크 트래픽을 정의합니다.

여러분은 다음과 같은 것을 볼 수 없습니다. ASA는 네트워크 규칙이 암시하는 소스 IP 주소와 대상 IP 주소의 가능한 모든 조합을 설명하기 위해 생성한 네트워크 규칙을 확장합니다. 예를 들어 한 네트워크 개체에 있는 3개의 IP 주소가 다른 개체에 있는 3개의 IP 주소에 액세스하는 것이 거부되는 규칙이 있는 경우 ASA가 메모리에 저장하는 가능한 액세스 제어 항목은 9개입니다.

ASA에서 처리할 수 있는 ACE 수에는 하드 코딩된 제한이 없지만 ACE 수가 너무 많으면 ASA 성능이 저하됩니다. 표 4를 참조하십시오. 특정 ASA 디바이스에 대해 예상되는 최대 ACE 항목 수에 대한 이 적응형 보안 어플라이언스 FAQ에서 "Cisco ASA 모델에 대한 최대 액세스 제어 항목".

CDO는 모든 네트워크 정책에서 파생된 총 ACE 수를 유지하고 해당 ACE 수가 어플라이언스에서 예상되는 최대 ACE 제한을 초과할 때 알려줍니다. CDO가 제공하는 정보는 다음과 같습니다.




디바이스의 **ACE** 수 줄이기

다음은 예상되는 최대 ACE 수를 초과한 디바이스에서 ACE 수를 줄이는 몇 가지 방법입니다.

- 부분적으로 그리고 완전히 섀도우 규칙 규칙이 있는 정책을 찾습니다. 적절한 경우 이러한 규칙을 삭제하십시오.
- 적중 횟수가 0인 디바이스의 모든 네트워크 정책 찾기 적중률이 0인 네트워크 정책의 규칙이 적중되는 빈도 찾기 적절한 경우 히트가 0인 정책 또는 규칙을 삭제합니다.
- 액세스 제어 항목의 예상 수를 초과한 ASA 네트워크 정책 및 규칙 검색 및 필터링 해당 정책을 검토합니다. 해당 정책의 소스 및 대상 주소가 원래 계획한 만큼 광범위해야 하는지 고려하십시오.

# ASA 글로벌 액세스 정책 구성

전역 액세스 정책은 ASA의 모든 인터페이스에 적용되는 네트워크 정책입니다. 이러한 정책은 인바운드 네트워크 트래픽에만 적용됩니다. 규칙 집합을 모든 ASA 인터페이스에 균일하게 적용하려면 전역 액세스 정책을 생성합니다.

ASA에는 하나의 전역 액세스 정책만 구성할 수 있습니다. 다른 정책과 마찬가지로 전역 액세스 정책에도 둘 이상의 규칙이 할당될 수 있습니다.

ASA 전역 액세스 정책은 특정 인터페이스에 대한 네트워크 정책 이후, 그리고 모든 트래픽에 대한 암시적 거부 규칙 이전에 처리됩니다. ASA에서 규칙을 처리하는 순서는 다음과 같습니다.

1. 인터페이스 액세스 규칙.
2. 브리지 그룹 멤버 인터페이스의 경우, BVI(Bridge Virtual Interface) 액세스 규칙입니다.
3. 전역 액세스 규칙
4. 암시적 거부

**ASA** 글로벌 액세스 정책 구성에 대한 제한 사항

CDO를 사용하면 ASA에 대한 전역 액세스 정책을 생성하고 수정할 수 있습니다. 그러나 CDO에 온보딩할 때 ASA에 전역 액세스 정책이 있었다면 다음과 같은 제한 사항이 적용됩니다.

- 정책을 수정할 수는 있지만 디바이스당 하나의 전역 액세스 정책만 허용되므로 새 정책을 생성할 수는 없습니다.
- ASA의 전역 액세스 정책에 CDO가 지원하지 않는 규칙이 포함된 경우 정책을 수정할 수 없습니다.
- CLI 인터페이스를 사용하거나 디바이스 구성 파일을 수정하는 방법으로만 정책을 삭제할 수 있습니다.

## 글로벌 액세스 정책 생성

단계 **1** **Policies(**정책**)** > **ASA Policies(ASA** 정책**)**를 클릭합니다.

단계 **2** 필터 패널에서 정책 목록을 필터링하여 전역 정책을 추가할 디바이스를 찾습니다.

단계 **3** Network Policies(네트워크 정책) 테이블의 Interfaces(인터페이스) 열에 "global(전역)"이라는 레이블이 붙은 정책이 없는지 확인합니다.

단계 **4** **Create Policy(**정책 생성**)**를 클릭합니다.

단계 **5** Device(디바이스) 버튼을 클릭하고 전역 정책을 추가할 ASA를 선택합니다. **Select(**선택**)**를 클릭합니다.

단계 **6** 정책에 이름을 지정하고 **Create as global policy(**전역 정책으로 생성**)**를 선택합니다. 정책에 대한 인터페이스나 방향을 선택할 수 없음을 알 수 있습니다. 전역 정책은 항상 디바이스의 모든 인터페이스에 할당되며 항상 인바운드 트래픽을 평가합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

단계 **8** 새 정책에 규칙을 추가하려면 ASA 네트워크 정책 편집을 사용합니다.

# 글로벌 액세스 정책 편집

위에서 설명한 구성 제한 사항을 염두에 두고 ASA 네트워크 정책 편집를 사용하여 전역 액세스 정책을 편집합니다.

**Note** Edit Policy(정책 편집) 버튼이 비활성화되어 글로벌 정책을 편집할 수 없다면, 정책이 ASA에서 생성되었고 CDO에서 지원하지 않는 개체가 포함된 규칙이 포함되어 있기 때문일 수 있습니다. 이러한 규칙은 전역 액세스 정책 테이블에서 볼 수 없습니다. 이 경우 CDO의 CLI 툴을 사용하여 구성 파일을 편집하거나 CDO를 사용하여 ASA의 구성 파일을 편집하거나 ASA에서 직접 전역 정책을 편집해야 합니다.

다른 디바이스에 전역 액세스 정책 복사

ASA 네트워크 정책 복사를 사용하여 한 디바이스에서 다른 디바이스로 전역 액세스 정책을 복사하거나 한 디바이스에서 다른 디바이스의 단일 인터페이스로 전역 액세스 정책을 복사합니다.

전역 액세스 정책 삭제

CDO의 사용자 인터페이스를 사용하여 전역 액세스 정책을 삭제할 수 없습니다. 전역 액세스 정책을 삭제하려면 CDO의 CLI 툴을 사용하거나 CDO를 사용하여 ASA의 구성 파일을 편집하거나 ASA에서 직접 전역 액세스 정책을 편집하여 명령줄에서 전역 액세스 정책을 삭제해야 합니다.

# 적중률

CDO를 사용하면 클라우드의 단일 창에서 보다 정확한 정책 분석 및 근본 원인에 대한 즉각적인 조치 가능한 피벗을 위한 간단한 시각화를 제공하여 정책 규칙의 결과를 평가할 수 있습니다. 적중률 기능을 사용하면 다음을 수행할 수 있습니다.

- 보안 상태를 증가하는 사용되지 않는 정책 규칙을 제거합니다.
- 병목 현상을 즉시 식별하여 방화벽 성능을 최적화하고 정확하고 효율적인 우선순위를 적용합니다(예: 가장 많이 트리거되는 정책 규칙이 우선순위가 높음).
- 구성된 데이터 보존 기간(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 평가합니다.

# ASA 정책의 적중률 보기

단계 **1** CDO 메뉴 모음에서 **Policies(**정책**)** > **ASA Access Policies(ASA** 액세스 정책**)**를 선택합니다.

단계 **2** 필터 아이콘을 클릭하고 필터를 열린 상태로 고정합니다.

단계 **3** Hits(적중) 영역에서 다양한 적중 횟수 필터를 클릭하여 다른 정책보다 적중 빈도가 높거나 낮은 정책을 표시합니다.

# 네트워크 정책 규칙 내보내기

각 Access-Group 또는 Crypto-Map의 콘텐츠를 .csv 파일로 내보낼 수 있습니다. 이 .csv는 각 ACL(Access Control List) 및 CDO가 각 ACL에 대해 보유한 데이터를 표시합니다.

단계 **1** 탐색 창에서 **Policies(**정책**)** > **ASA Policies(ASA** 정책**)**를 클릭합니다.

단계 **2** (선택 사항) ASA 네트워크 정책 및 규칙 검색 및 필터링를 사용하여 결과를 필터링합니다.

단계 **3** 결과에서 네트워크 정책을 선택합니다.

단계 **4** **Export to CSV(CSV**로 내보내기**)** 

를 클릭합니다.

단계 **5** CDO는 화면에 표시되는 규칙을 .csv 파일로 내보냅니다.

# 디바이스에 ASA 정책 변경 사항 적용

CDO(Cisco Defense Orchestrator)에서 보안 정책을 수정하면 영향을 받는 디바이스 또는 서비스에 변경 사항이 적용됩니다. 그 결과 구성이 동기화되지 않습니다. 현재 동기화되지 않은 모든 디바이스 또는 서비스에서 **Deploy to Device...(**디바이스에 구축**...)**를 클릭하여 정책 변경 사항을 검토하고 적용할 수 있습니다.

## 스크립트로 디바이스에 구축

ASA 디바이스 정책 구성 변경이 완료되면 변경 사항을 검토하고 디바이스에 적용해야 합니다.

단계 **1** **Devices(**디바이스**)** 탭으로 이동하여 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **2** 적절한 디바이스 유형 탭을 클릭하고 테이블에서 수정된 디바이스를 선택합니다. 구성 상태가 **Not Synced(**동기화되지 않음**)**로 표시되어야 하며, 이는 디바이스에 아직 적용되지 않은 변경 사항이 있음을 나타냅니다.

단계 **3** 오른쪽 사이드바에서 **Sync(**동기화**)**를 클릭하여 디바이스에 적용할 명령을 생성하여 CDO 구성과 동기화된 상태로 전환합니다.

단계 **4** 메시지가 표시되면 **Download Commands(**명령 다운로드**)**를 클릭하여 명령의 복사본을 로컬로 다운로드합니다. 이러한 명령은 텍스트 파일에 포함되며 적용하기 전에 검토할 수 있습니다. 원하는 경우 변경 사항을 되돌리는 명령도 생성됩니다.

단계 **5** CDO 외부에서 표준 프로토콜을 사용하여 디바이스에 로그온하고 다운로드한 명령을 적용합니다.

단계 **6** 모든 명령을 입력한 후 CDO로 돌아가서 **Devices(**디바이스**)** 탭에서 수정된 디바이스를 다시 선택합니다.

단계 **7** **Refresh(**새로 고침**)**를 클릭하여 CDO와의 동기화를 확인합니다.

---

명령의 하위 집합이 실행되었거나 추가 명령이 대역 외에서 실행된 경우 CDO는 차이점을 표시하는 창을 열고 사용자에게 *Conflict Detected(*충돌 감지됨*)*라는 업데이트된 상태를 제공하여 차이점을 나타냅니다.

# ASA 정책의 보안 그룹 태그

액세스 제어 규칙에서 보안 그룹 개체 그룹(이후 "SGT 그룹"이라고 함)의 보안 그룹 태그를 사용하는 ASA를 온보드하는 경우 Cisco Defense Orchestrator를 사용하여 SGT 그룹을 사용하는 규칙을 편집하고 해당 규칙이 있는 정책을 관리할 수 있습니다. 그러나 CDO GUI를 사용하여 SGT 그룹을 생성하거나 편집할 수는 없습니다. SGT 그룹을 생성하거나 수정하려면 ASA의 ASDM(Adaptive Security Device Manager) 또는 CDO에서 사용 가능한 명령줄 인터페이스를 사용해야 합니다.

CDO의 개체 페이지에서 SGT 그룹의 세부 정보를 읽을 때 해당 개체가 편집 불가한 시스템 제공 개체로 식별되는 것을 확인할 수 있습니다.

CDO 관리자는 SGT 그룹을 포함하는 ACL 및 ASA 정책에서 다음 작업을 수행할 수 있습니다.

- CDO 관리자는 소스 및 대상 보안 그룹을 제외한 ACL의 모든 측면을 편집할 수 있습니다.
- 한 ASA에서 다른 ASA로 SGT 그룹을 포함하는 정책을 복사합니다.

명령줄 인터페이스를 사용하여 Cisco TrustSec을 구성하는 방법에 대한 자세한 지침은 해당 ASA 릴리스의 ASA CLI 제2권: Cisco ASA Series 방화벽 CLI 구성 가이드의 "ASA 및 Cisco TrustSec" 장을 참조하십시오.

# 섀도우 규칙

섀도우 규칙이 있는 네트워크 정책은 정책에 있는 하나 이상의 규칙이 선행하는 규칙이 섀도우 규칙에 의해 패킷이 평가되는 것을 방지하기 때문에 절대 트리거되지 않는 정책입니다.

예를 들어 "예제" 네트워크 정책에서 다음과 같은 네트워크 개체 및 네트워크 규칙을 고려하십시오.

```
object network 02-50
range 10.10.10.2 10.10.10.50
```

```
object network 02-100
range 10.10.10.2 10.10.10.100

access-list example extended deny ip any4 object 02-50
access-list example extended permit ip host 10.10.10.35 object 02-50
access-list example extended permit ip any4 object 02-100
```

이 규칙에 의해 트래픽이 평가되지 않습니다.

```
access-list example extended permit ip host 10.10.10.35 object 02-50
```

이전 규칙 때문에,

```
access-list example extended deny ip any4 object 02-50
```

**ipv4** 주소가 **10.10.10.2 - 10.10.10.50** 범위의 주소에 도달하는 것을 거부합니다.

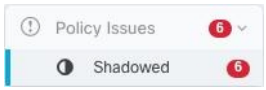
# 섀도우 규칙이 있는 네트워크 정책 찾기

섀도우 규칙이 있는 네트워크 정책을 찾으려면 네트워크 정책 필터를 사용합니다.

단계 **1** 탐색 창에서 **Policies(**정책**)** > **ASA Policies(ASA** 정책**)**를 클릭합니다.

단계 **2** ASA Access Policies(ASA 액세스 정책) 테이블 상단에 있는 필터 아이콘을 클릭합니다.

단계 **3** 정책 문제 필터에서 **Shadowed(**섀도우**)**를 선택하여 섀도우 규칙이 있는 모든 정책을 확인합니다.




# 섀도우 규칙 문제 해결

위의 "예제" 네트워크 정책에 설명된 규칙은 다음과 같이 표시됩니다.


1행의 규칙은 정책의 다른 규칙을 섀도잉하므로 섀도우 경고 배지 ▲로 표시됩니다.우 라인 2의 규칙은 정책의 다른 규칙에 의해 섀도우된 ◑로 표시됩니다. 2행의 규칙에 대한 작업은 정책의 다른 규칙에 의해 섀도우되어 있으므로 회색으로 표시됩니다. CDO는 정책의 어떤 규칙이 2행의 규칙을 섀도잉하는지 알려줄 수 있습니다.

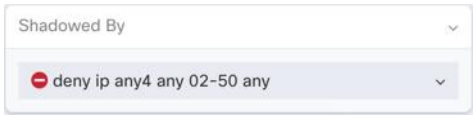
라인 3의 규칙은 일부 시간에만 트리거될 수 있습니다. 이것은 부분적으로 섀도우 규칙입니다. 10.10.10.2-10.10.10.50 범위의 IP 주소에 도달하려는 모든 IPv4 주소의 네트워크 트래픽은 첫 번째 규

칙에 의해 이미 거부되었기 때문에 평가되지 않습니다. 그러나 10.10.10.51-10.10.10.100 범위의 주소에 도달하려는 모든 IPv4 주소는 마지막 규칙에 의해 평가되고 허용됩니다.

**Caution** CDO는 부분적으로 음영 처리된 규칙에 섀도우 경고 배지 ⚠를 적용하지 않습니다.

단계 **1** 정책에서 섀도우 규칙을 선택합니다. 위의 예에서는 줄 2를 클릭하는 것을 의미합니다.

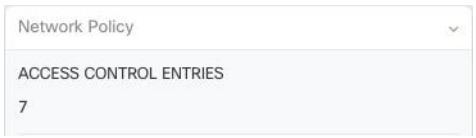
단계 **2** 규칙 세부 정보 창에서 **Shadowed By** 영역을 찾습니다. 이 예에서 2행의 규칙에 대한 **Shadowed By** 영역은 1행의 규칙에 의해 섀도우 처리되고 있음을 보여줍니다.




단계 **3** 섀도우 처리 중인 규칙을 검토합니다. 너무 광범위합니까? 섀도우 처리된 규칙을 검토합니다. 정말로 필요하십니까? 섀도잉 처리 중인 규칙을 수정하거나 섀도잉 처리된 규칙을 삭제합니다.

**Note** 섀도우 규칙을 삭제하면 ASA의 ACE(Access Control Entry) 수가 줄어듭니다. 이렇게 하면 다른 ACE를 사용하여 다른 규칙을 생성할 수 있는 공간이 확보됩니다. CDO는 네트워크 정책의 모든 규칙에서 파생된 ACE 수를 계산하고 네트워크 정책 세부 정보 창 상단에 총계를 표시합니다. 네트워크 정책의 규칙 중 섀도우 규칙이 있으면 해당 번호도 나열됩니다.


또한 CDO는 네트워크 정책의 단일 규칙에서 파생된 ACE의 수를 표시하고 네트워크 정책 세부 정보 창에 해당 정보를 표시합니다. 다음은 해당 목록의 예입니다.




단계 **4** 네트워크 정책 세부 정보 창의 Devices(디바이스) 영역에서 정책을 사용하는 디바이스를 확인합니다.

단계 **5** Devices & Service(디바이스 및 서비스) 페이지를 열고 정책 변경의 영향을 받는 디바이스에 다시 변경사항을 배포합니다.

# 네트워크 주소 변환

IP 네트워크 내의 각 컴퓨터와 디바이스에는 호스트를 식별하는 고유한 IP 주소가 할당됩니다. 공용 IPv4 주소의 부족 때문에 이러한 IP 주소는 대부분 사설이며, 사설 회사 네트워크 외부로 라우팅되지

않습니다. RFC 1918의 정의에 따르면 사설 IP 주소는 내부적으로 사용할 수 있지만 외부에 알려서는 안 되는 주소입니다.

- 10.0.0.0~10.255.255.255
- 172.16.0.0 ~ 172.31.255.255
- 192.168.0.0~192.168.255.255

NAT의 주요 기능 중 하나는 사설 IP 네트워크가 인터넷에 연결되도록 하는 것입니다. NAT는 사설 IP 주소를 공용 IP 주소로 교체하여, 내부 사설 네트워크의 사설 주소를 공용 인터넷에서 사용할 수 있는 합법적이고 라우팅 가능한 주소로 전환합니다. 이렇게 하여 NAT는 공용 주소를 절약합니다. 전체 네트워크에 대해 최소 하나의 공용 주소만 외부에 알리도록 구성할 수 있기 때문입니다.

NAT의 기타 기능은 다음과 같습니다.

- 보안 - 직접 공격을 피할 수 있도록 내부 IP 주소를 숨깁니다.
- IP 라우팅 솔루션 - NAT를 사용하는 경우 중첩 IP 주소 문제가 발생하지 않습니다.
- 유연성 - 외부적으로 사용 가능한 공용 주소에 영향을 주지 않고 내부 IP 주소 지정 방식을 변경할 수 있습니다. 예를 들어 인터넷에 액세스할 수 있는 서버의 경우, 인터넷용으로는 고정 IP 주소를 유지하고 내부적으로는 서버 주소를 변경할 수 있습니다.
- IPv4와 IPv6 간 변환(라우팅된 방식 전용) - IPv6 네트워크를 IPv4 네트워크에 연결하려는 경우 NAT를 이용하면 두 가지 주소 유형 간에 변환할 수 있습니다.

Cisco Defense Orchestrator를 사용하여 다양한 활용 사례에 대한 NAT 규칙을 생성할 수 있습니다. NAT 규칙 마법사 또는 다음 항목을 사용하여 다른 NAT 규칙을 생성합니다.

# NAT 규칙 처리 순서

네트워크 개체 NAT 규칙과 2회 NAT 규칙은 세 개의 섹션으로 구분되는 단일 테이블에 저장됩니다. 섹션 1 규칙이 먼저 적용된 다음, 일치가 발견될 때까지 섹션 2, 마지막으로 섹션 3이 적용됩니다. 예를 들어 섹션 1에서 일치가 발견되면 섹션 2와 3은 평가되지 않습니다. 다음 표는 각 섹션 내의 규칙 순서를 보여줍니다.

***Table 25: NAT*** 규칙 테이블

| 테이블 섹션 | 규칙 유형 | 섹션 내 규칙의 순서 |
|---|---|---|
| 섹션 1 | 2회 NAT(ASA)<br>수동 NAT(FTD) | 첫 번째 일치부터 컨피그레이션에 나타나는 순서대로 적용됩니다. 첫 번째 일치가 적용되므로, 일반 규칙 앞에 특수 규칙이 오도록 해야 합니다. 그렇지 않으면 특수 규칙이 원하는 대로 적용되지 않을 수 있습니다. 기본적으로 2회 NAT 규칙은 섹션 1에 추가됩니다. |

| 테이블 섹션 | 규칙 유형 | 섹션 내 규칙의 순서 |
|---|---|---|
| 섹션 2 | 네트워크 개체 NAT(ASA)<br>자동 NAT(FTD) | 섹션 1에서 일치하는 항목을 찾을 수 없으면 섹션 2 규칙이 다음 순서로 적용됩니다.<br>**1.** 고정 규칙<br>**2.** 동적 규칙<br>각 규칙 유형 내에서는 다음의 순서 지침이 사용됩니다.<br>**1.** 실제 IP 주소의 수량 - 가장 적은 것에서 가장 많은 것. 예를 들면 주소가 1개인 개체가 주소가 10개인 개체보다 먼저 평가됩니다.<br>**2.** 수량이 동일한 경우 IP 주소 번호가 낮은 것에서 높은 것 순으로 사용됩니다. 예를 들면, 10.1.1.0이 11.1.1.0보다 먼저 평가됩니다.<br>**3.** IP 주소가 동일한 경우 네트워크 개체의 이름이 알파벳순으로 사용됩니다. 예를 들어 "Arlington" 개체는 "Detroit" 개체보다 먼저 평가됩니다. |
| 섹션 3 | 2회 NAT(ASA)<br>수동 NAT(FTD) | 아직도 일치가 발견되지 않으면 섹션 3 규칙이 첫 번째부터 컨피그레이션에 나타나는 순서대로 적용됩니다. 이 섹션에는 가장 일반적인 규칙을 포함해야 합니다. 또한 이 섹션에서는 특정 규칙이 일반 규칙보다 먼저 적용되도록 해야 합니다. |

예를 들어 섹션 2 규칙의 경우 네트워크 개체 내에서 다음 IP 주소를 정의합니다.

- 192.168.1.0/24(고정)
- 192.168.1.0/24(동적)
- 10.1.1.0/24(고정)
- 192.168.1.1/32(고정)
- 172.16.1.0/24(동적) (개체 Detroit)
- 172.16.1.0/24(동적)(개체 Arlington)

결과 순서는 다음과 같습니다.

- 192.168.1.1/32(고정)
- 10.1.1.0/24(고정)

- 192.168.1.0/24(고정)
- 172.16.1.0/24(동적)(개체 Arlington)
- 172.16.1.0/24(동적) (개체 Detroit)
- 192.168.1.0/24(동적)

# 네트워크 주소 변환 마법사

NAT(Network Address Translation) 마법사는 다음 유형의 액세스에 대해 디바이스에서 NAT 규칙을 만드는 데 도움이 됩니다.

- 내부 사용자의 인터넷 액세스를 활성화합니다. 이 NAT 규칙을 사용하여 내부 네트워크의 사용자가 인터넷에 연결할 수 있습니다.
- 내부 서버를 인터넷에 노출합니다. 이 NAT 규칙을 사용하여 네트워크 외부의 사람들이 내부 웹 또는 이메일 서버에 도달하도록 허용할 수 있습니다.

**"내부 사용자를 위한 인터넷 액세스 활성화"**의 전제 조건

NAT 규칙을 생성하기 전에 다음 정보를 수집하십시오.

- 사용자에게 가장 가까운 인터페이스 이것은 일반적으로 "내부" 인터페이스라고 합니다.
- 인터넷 연결에 가장 가까운 인터페이스 이것은 일반적으로 "외부" 인터페이스라고 합니다.
- 특정 사용자만 인터넷에 연결할 수 있도록 하려면 해당 사용자의 서브넷 주소가 필요합니다.

**"내부 서버를 인터넷에 노출"**하기 위한 전제 조건

NAT 규칙을 생성하기 전에 다음 정보를 수집하십시오.

- 사용자에게 가장 가까운 인터페이스 이것은 일반적으로 "내부" 인터페이스라고 합니다.
- 인터넷 연결에 가장 가까운 인터페이스 이것은 일반적으로 "외부" 인터페이스라고 합니다.
- 인터넷 연결 IP 주소로 변환하려는 네트워크 내부 서버의 IP 주소입니다.
- 서버에서 사용할 공용 IP 주소입니다.

다음 작업

NAT 마법사를 사용하여 NAT 규칙 생성, on page 226의 내용을 참조하십시오.

# NAT 마법사를 사용하여 NAT 규칙 생성

**Before you begin**

NAT 마법사를 사용하여 NAT 규칙을 만드는 데 필요한 사전 요구 사항은 네트워크 주소 변환 마법사, on page 225를 참조하십시오.

단계 **1** CDO 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 필터 및 검색 필드를 사용하여 NAT 규칙을 생성하려는 디바이스를 찾으십시오.

단계 **5** 상세정보 패널의 **Management(**관리**)** 영역에서 **NAT** NAT를 클릭합니다.

단계 **6** + > **NAT Wizard(NAT** 마법사**)**를 클릭합니다.

단계 **7** NAT 마법사 질문에 응답하고 화면의 지시를 따르십시오.

- NAT 마법사는 네트워크 개체, on page 123를 사용하여 규칙을 생성합니다. 드롭다운 메뉴에서 기존 개체를 선택하거나 만들기 버튼 + Create... 를 사용하여 새 개체를 생성합니다.
- NAT 규칙을 저장하려면 먼저 모든 IP 주소를 네트워크 개체로 정의해야 합니다.

단계 **8** 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

# NAT의 일반적인 사용 사례

**2**회 **NAT** 및 수동 **NAT**

다음은 "자동 NAT"라고도 하는 "네트워크 개체 NAT"를 사용하여 수행할 수 있는 몇 가지 일반적인 작업입니다.

- 공용 IP 주소를 사용하여 인터넷에 연결하도록 내부 네트워크의 서버 활성화, 227 페이지
- 내부 네트워크의 사용자가 외부 인터페이스의 공용 IP 주소를 사용하여 인터넷에 액세스하도록 활성화, 228 페이지
- 공용 IP 주소의 특정 포트에서 내부 네트워크의 서버를 사용할 수 있도록 설정, 229 페이지
- 사설 IP 주소 범위를 공용 IP 주소 범위로 변환, 233 페이지

네트워크 개체 및 **NAT**자동 **NAT**

다음은 "수동 NAT"라고도 하는 "Twice NAT"를 사용하여 수행할 수 있는 일반적인 작업입니다.

• 외부 인터페이스를 통과할 때 IP 주소 범위가 변환되지 않도록 방지, 235 페이지

# 공용 IP 주소를 사용하여 인터넷에 연결하도록 내부 네트워크의 서버 활성화

활용 사례

인터넷에서 액세스해야 하는 사설 IP 주소가 있는 서버가 있고 사설 IP 주소에 대해 하나의 공용 IP 주소를 NAT하기에 충분한 공용 IP 주소가 있는 경우 이 NAT 전략을 사용합니다. 공용 IP 주소가 제한된 경우 공용 IP 주소의 특정 포트에서 내부 네트워크의 서버를 사용할 수 있도록 설정를 참조하세요(해당 솔루션이 더 적합할 수 있음).

전략

서버에는 정적 사설 IP 주소가 있으며 네트워크 외부의 사용자는 서버에 연결할 수 있어야 합니다. 고정 사설 IP 주소를 고정 공용 IP 주소로 변환하는 네트워크 개체 NAT 규칙을 생성합니다. 그런 다음 해당 공용 IP 주소에서 사설 IP 주소에 도달하는 트래픽을 허용하는 액세스 정책을 생성합니다. 마지막으로 이러한 변경 사항을 디바이스에 배포합니다.

### Before you begin

시작하기 전에 두 개의 네트워크 개체를 생성합니다. 하나의 개체는 *servername_inside*로 이름을 지정하고 다른 개체는 *servername_outside*로 이름을 지정합니다. *servername*_inside 네트워크 개체는 서버의 사설 IP 주소를 포함해야 합니다. *servername*_outside 네트워크 개체에는 서버의 공용 IP 주소가 포함되어야 합니다. 지침은 네트워크 개체을 참조하십시오.

---

단계 **1** CDO 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** NAT 규칙을 생성하려는 디바이스를 선택합니다.

단계 **5** 오른쪽의 **Management(**관리**)** 창에서 **NAT**를 클릭합니다.

단계 **6**  **> Network Object NAT**를 클릭합니다.

단계 **7** 섹션 1, **Type(**유형**)**에서 **Static(**정적**)**을 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **8** 섹션 2, **Interfaces(**인터페이스**)**에서 소스 인터페이스로 **inside(**내부**)**를 선택하고 대상 인터페이스로 **outside(**외부**)**를 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **9** 섹션 3, **Packets(**패킷**)**에서 , 다음 작업을 수행합니다.

**a.** 원본 주소 메뉴를 확장하고 **Choose(**선택**)**을 클릭한 다음 **servername_inside** 개체를 선택합니다.

**b.** 변환된 주소 메뉴를 확장하고 **Choose(**선택**)**을 클릭한 다음 **servername_outside** 개체를 선택합니다.

단계 **10** 섹션 4, **Advanced(**고급**)**을 건너뜁니다.

단계 **11** FDM 관리 디바이스의 경우 섹션 5, 이름에서 NAT 규칙에 이름을 지정합니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

단계 **13** ASA의 경우 네트워크 정책 규칙을 배포하거나 기다렸다가, FDM 관리 디바이스의 경우 액세스 제어 정책 규칙을 배포하여 트래픽이 *servername*_inside에서 *servername*_outside로 흐를 수 있도록 합니다.

단계 **14** 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

---

**ASA**의 저장된 구성 파일 항목

다음은 이 절차의 결과로 생성되어 ASA의 저장된 구성 파일에 나타나는 항목입니다.

**Note** 이것은 FDM 관리 디바이스에 적용되지 않습니다.

이 절차에 의해 생성된 개체

```
object network servername_outside
host 209.165.1.29
object network servername_inside
host 10.1.2.29
```

이 절차에 의해 생성된 ***NAT*** 규칙

```
object network servername_inside
 nat (inside,outside) static servername_outside
```

# 내부 네트워크의 사용자가 외부 인터페이스의 공용 **IP** 주소를 사용하여 인터넷에 액세스하도록 활성화

활용 사례

외부 인터페이스의 공용 주소를 공유하여 개인 네트워크의 사용자와 컴퓨터가 인터넷에 연결할 수 있도록 합니다.

전략

사설 네트워크의 모든 사용자가 디바이스의 외부 인터페이스 공용 IP 주소를 공유할 수 있도록 허용하는 포트 주소 변환(PAT) 규칙을 생성합니다.

사설 주소가 공용 주소 및 포트 번호에 매핑된 후 디바이스는 해당 매핑을 기록합니다. 해당 공용 IP 주소 및 포트로 향하는 들어오는 트래픽이 수신되면 디바이스는 이를 요청한 사설 IP 주소로 다시 보냅니다.

---

단계 **1** CDO 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** NAT 규칙을 생성하려는 디바이스를 선택합니다.

단계 **5** 오른쪽의 **Management(관리)** 창에서 **NAT**를 클릭합니다.

단계 **6** + > **Network Object NAT**를 클릭합니다.

단계 **7** 섹션 1, 유형 에서 **Dynamic(동적)**을 선택합니다. **Continue(계속)**를 클릭합니다.

단계 **8** 섹션 2, 인터페이스에서, 소스 인터페이스로 **any(아무거나)**를 선택하고 대상 인터페이스로 **outside(외부)**를 선택합니다. **Continue(계속)**를 클릭합니다.

단계 **9** 섹션 3, **Packets(패킷)**에서, 다음 작업을 수행합니다.

**a.** 원래 주소 메뉴를 확장하고, **Choose(선택)**을 클릭한 다음 네트워크 구성에 따라 **any-ipv4** 또는 **any-ipv6** 개체를 선택합니다.

**b.** 변환된 주소 메뉴를 확장하고 사용 가능한 목록에서 인터페이스를 선택합니다. 인터페이스는 외부 인터페이스의 공용 주소를 사용하도록 나타냅니다.

단계 **10** FTD(Firepower Threat Defense)의 경우 섹션 5, **Name(이름)**에서 NAT 규칙에 이름을 지정합니다.

단계 **11** **Save(저장)**를 클릭합니다.

단계 **12** 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

**ASA**의 저장된 구성 파일 항목

다음은 이 절차의 결과로 생성되어 ASA의 저장된 구성 파일에 나타나는 항목입니다.

**Note** 이것은 FDM 관리 디바이스에 적용되지 않습니다.

이 절차에 의해 생성된 개체

```
object network any_network
subnet 0.0.0.0 0.0.0.0
```

이 절차에 의해 생성된 ***NAT*** 규칙

```
object network any_network
nat (any,outside) dynamic interface
```

# 공용 IP 주소의 특정 포트에서 내부 네트워크의 서버를 사용할 수 있도록 설정

활용 사례

공용 IP 주소가 하나만 있거나 매우 제한된 수인 경우, 정적 IP 주소 및 포트에 바인딩된 인바운드 트래픽을 내부 주소로 변환하는 네트워크 개체 NAT 규칙을 만들 수 있습니다. 특정 사례에 대한 절차를 제공했지만 지원되는 다른 애플리케이션의 모델로 사용할 수 있습니다.

사전 요구 사항

시작하기 전에 FTP, HTTP 및 SMTP 서버에 각각 하나씩 세 개의 개별 네트워크 개체를 생성합니다. 다음 절차를 위해 이러한 개체를 **ftp-server-object**, **http-server-object** 및 **smtp-server-object**라고 합니다. 지침은 ASA 네트워크 개체 및 네트워크 그룹 생성 또는 편집을 참조하십시오.

# FTP 서버에 대한 NAT 수신 FTP 트래픽

단계 **1** CDO 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** NAT 규칙을 생성하려는 디바이스를 선택합니다.

단계 **5** 오른쪽의 **Management(**관리**)** 창에서 **NAT**를 클릭합니다.

단계 **6**  **> Network Object NAT**를 클릭합니다.

단계 **7** 섹션 1, **Type(**유형**)**에서 **Static(**정적**)**을 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **8** 섹션 2, **Interfaces(**인터페이스**)**에서 소스 인터페이스로 **inside(**내부**)**를 선택하고 대상 인터페이스로 **outside(**외부**)**를 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **9** 섹션 3, **Packets(**패킷**)**에서 , 다음 작업을 수행합니다.

- 원본 주소 메뉴를 확장하고, **Choose(**선택**)**를 클릭한 다음**ftp**-server-object를 선택합니다.
- 변환된 주소 메뉴를 확장하고, **Choose(**선택**)**를 클릭한 다음 **Interface(**인터페이스**)**를 선택합니다.
- **Use Port Translation(**포트 변환 사용**)**을 선택합니다.
- **tcp**, **ftp, ftp**를 선택합니다.


단계 **10** 섹션 4, **Advanced(**고급**)**을 건너뜁니다.

단계 **11** FTD(Firepower Threat Defense)의 경우 섹션 5, **Name(**이름**)**에서 NAT 규칙에 이름을 지정합니다.

단계 **12** **Save(**저장**)**를 클릭합니다. NAT 테이블의 NAT 규칙 처리 순서에 새 규칙이 생성됩니다.

단계 **13** 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

**ASA**의 저장된 구성 파일 항목

다음은 이 절차의 결과로 생성되어 ASA의 저장된 구성 파일에 나타나는 항목입니다.

**Note** 이것은 FDM 관리 디바이스에 적용되지 않습니다.

이 절차에 의해 생성된 개체

```
object network ftp-object
host 10.1.2.27
```

이 절차에 의해 생성된 ***NAT*** 규칙

```
object network ftp-object
nat (inside,outside) static interface service tcp ftp ftp
```

## HTTP 서버에 대한 NAT 수신 HTTP 트래픽

공용 IP 주소가 하나만 있거나 매우 제한된 수인 경우, 정적 IP 주소 및 포트에 바인딩된 인바운드 트래픽을 내부 주소로 변환하는 네트워크 개체 NAT 규칙을 만들 수 있습니다. 특정 사례에 대한 절차를 제공했지만 지원되는 다른 애플리케이션의 모델로 사용할 수 있습니다.

### Before you begin

시작하기 전에 http 서버에 대한 네트워크 개체를 생성합니다. 이 절차에서는개체를 **http-object**라고 합니다. 지침은 ASA 네트워크 개체 및 네트워크 그룹 생성 또는 편집을 참조하십시오.

단계 **1** CDO 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** NAT 규칙을 생성하려는 디바이스를 선택합니다.

단계 **5** 오른쪽의 **Management(**관리**)** 창에서 **NAT**를 클릭합니다.

단계 **6** + > **Network Object NAT**를 클릭합니다.

단계 **7** 섹션 1, **Type(**유형**)**에서 **Static(**정적**)**을 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **8** 섹션 2, **Interfaces(**인터페이스**)**에서 소스 인터페이스로 **inside(**내부**)**를 선택하고 대상 인터페이스로 **outside(**외부**)**를 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **9** 섹션 3, **Packets(**패킷**)**에서 , 다음 작업을 수행합니다.

- 원본 주소 메뉴를 확장하고 **Choose(**선택**)**을 클릭한 다음 **http**-object를 선택합니다.
- 변환된 주소 메뉴를 확장하고, **Choose(**선택**)**를 클릭한 다음 **Interface(**인터페이스**)**를 선택합니다.
- **Use Port Translation(**포트 변환 사용**)**을 선택합니다.
- **tcp**, **http**, http를 선택합니다.

단계 **10** 섹션 4, **Advanced(**고급**)**을 건너뜁니다.

단계 **11** FTD(Firepower Threat Defense)의 경우 섹션 5, **Name(**이름**)**에서 NAT 규칙에 이름을 지정합니다.

단계 **12** **Save(**저장**)**를 클릭합니다. NAT 테이블의 NAT 규칙 처리 순서에 새 규칙이 생성됩니다.

단계 **13** 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

**ASA**의 저장된 구성 파일 항목

다음은 이 절차의 결과로 생성되어 ASA의 저장된 구성 파일에 나타나는 항목입니다.

**Note** 이것은 FDM 관리 디바이스에 적용되지 않습니다.

이 절차에 의해 생성된 개체

```
object network http-object
host 10.1.2.28
```

이 절차에 의해 생성된 ***NAT*** 규칙

```
object network http-object
nat (inside,outside) static interface service tcp www www
```

# SMTP 서버에 대한 NAT 수신 SMTP 트래픽

공용 IP 주소가 하나만 있거나 매우 제한된 수인 경우, 정적 IP 주소 및 포트에 바인딩된 인바운드 트래픽을 내부 주소로 변환하는 네트워크 개체 NAT 규칙을 만들 수 있습니다. 특정 사례에 대한 절차를 제공했지만 지원되는 다른 애플리케이션의 모델로 사용할 수 있습니다.

### Before you begin

시작하기 전에 smtp 서버에 대한 네트워크 개체를 생성합니다. 이 절차에서는개체를 **smtp-**개체라고 합니다. 지침은 ASA 네트워크 개체 및 네트워크 그룹 생성 또는 편집을 참조하십시오.

단계 **1** CDO 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** NAT 규칙을 생성하려는 디바이스를 선택합니다.

단계 **5** 오른쪽의 **Management(**관리**)** 창에서 **NAT**를 클릭합니다.

단계 **6** + > **Network Object NAT**를 클릭합니다.

단계 **7** 섹션 1, **Type(**유형**)**에서 **Static(**정적**)**을 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **8** 섹션 2, **Interfaces(**인터페이스**)**에서 소스 인터페이스로 **inside(**내부**)**를 선택하고 대상 인터페이스로 **outside(**외부**)**를 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **9** 섹션 3, **Packets(**패킷**)**에서 , 다음 작업을 수행합니다.

- 원본 주소 메뉴를 확장하고, **Choose(**선택**)**를 클릭한 다음 smtp-server-object를 선택합니다.
- 변환된 주소 메뉴를 확장하고, **Choose(**선택**)**를 클릭한 다음 **Interface(**인터페이스**)**를 선택합니다.
- **Use Port Translation(**포트 변환 사용**)**을 선택합니다.
- **tcp**, **smtp**, **smtp**를 선택합니다.


단계 **10** 섹션 4, **Advanced(**고급**)**을 건너뜁니다.

단계 **11** FTD(Firepower Threat Defense)의 경우 섹션 5, **Name(**이름**)**에서 NAT 규칙에 이름을 지정합니다.

단계 **12** **Save(**저장**)**를 클릭합니다. NAT 테이블의 NAT 규칙 처리 순서에 새 규칙이 생성됩니다.

단계 **13** 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

**ASA**의 저장된 구성 파일 항목

다음은 이 절차의 결과로 생성되어 ASA의 저장된 구성 파일에 나타나는 항목입니다.

**Note** 이것은 FDM 관리 디바이스에 적용되지 않습니다.

이 절차에 의해 생성된 개체

```
object network smtp-object
host 10.1.2.29
```

이 절차에 의해 생성된 ***NAT*** 규칙

```
object network smtp-object
nat (inside,outside) static interface service tcp smtp smtp
```

# 사설 IP 주소 범위를 공용 IP 주소 범위로 변환

활용 사례

수신 디바이스(트랜잭션의 다른 끝에 있는 디바이스)가 트래픽을 허용하도록 IP 주소를 특정 범위로 변환해야 하는 특정 디바이스 유형 또는 사용자 유형 그룹이 있는 경우 이 접근 방식을 사용합니다.

# 내부 주소 풀을 외부 주소 풀로 변환

**Before you begin**

변환하려는 사설 IP 주소 풀에 대한 네트워크 개체를 생성하고 해당 사설 IP 주소를 변환하려는 공용 주소 풀에 대한 네트워크 개체를 생성합니다.

ASA의 경우 "원래 주소" 풀(변환하려는 개인 IP 주소 풀)은 주소 범위가 있는 네트워크 개체, 서브넷을 정의하는 네트워크 개체 또는 풀의 모든 주소를 포함하는 네트워크 그룹일 수 있습니다. FTD의 경우 "원래 주소" 풀은 풀의 모든 주소를 포함하는 네트워크 그룹 또는 서브넷을 정의하는 네트워크 개체일 수 있습니다.

**Note** ASA 의 경우 "변환된 주소" 풀을 정의하는 네트워크 그룹은 서브넷을 정의하는 네트워크 개체일 수 없습니다.

이러한 주소 풀을 생성할 때 지침을 보려면 ASA 네트워크 개체 및 네트워크 그룹 생성 또는 편집을 사용하고 하십시오.

다음 절차를 위해 개인 주소 풀의 이름을 **inside_pool**로 지정하고 공용 주소 풀의 이름을 **outside_pool**로 지정했습니다.

단계 **1** CDO 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** NAT 규칙을 생성하려는 디바이스를 선택합니다.

단계 **5** 오른쪽의 **Management(**관리**)** 창에서 **NAT**를 클릭합니다.

단계 **6** + > **Network Object NAT**를 클릭합니다.

단계 **7** 섹션 1 **Type(**유형**)**에서 **Dynamic(**동적**)**을 선택하고 **Continue(**계속**)**를 클릭합니다.

단계 **8** 섹션 2, 인터페이스에서 소스 인터페이스를 내부로, 대상 인터페이스를 외부로 설정합니다. **Continue(**계속**)**를 클릭합니다.

단계 **9** 섹션 3, **Packets(**패킷**)**에서, 다음 작업을 수행합니다.

- 원본 주소의 경우 **Choose(**선택**)**을 클릭한 다음 위의 전제 조건 섹션에서 만든 **inside_pool** 네트워크 개체(또는 네트워크 그룹)를 선택합니다.
- 변환된 주소의 경우 **Choose(**선택**)**을 클릭한 다음 위의 전제 조건 섹션에서 만든 **outside_pool** 네트워크 개체(또는 네트워크 그룹)를 선택합니다.

단계 **10** 섹션 4, **Advanced(**고급**)**을 건너뜁니다.

단계 **11** FTD(Firepower Threat Defense)의 경우 섹션 5, **Name(**이름**)**에서 NAT 규칙에 이름을 지정합니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

단계 **13** 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

**ASA**의 저장된 구성 파일 항목

이러한 절차의 결과로 ASA의 저장된 구성 파일에 나타나는 항목입니다.

**Note** 이것은 FDM 관리 디바이스에 적용되지 않습니다.

이 절차에 의해 생성된 개체

```
object network outside_pool
    range 209.165.1.1 209.165.1.255
object network inside_pool
    range 10.1.1.1 10.1.1.255
```

이 절차에 의해 생성된 ***NAT*** 규칙

```
object network inside_pool
nat (inside,outside) dynamic outside_pool
```

# 외부 인터페이스를 통과할 때 **IP** 주소 범위가 변환되지 않도록 방지

활용 사례

이 Twice NAT 사용 사례를 사용하여 사이트 투 사이트 VPN을 활성화합니다.

전략

네트워크의 한 위치에 있는 IP 주소가 다른 위치에 변경되지 않고 도착하도록 IP 주소 풀을 자체적으로 변환하고 있습니다.

## **2**회 **NAT** 규칙 생성

**Before you begin**

변환할 IP 주소 풀을 정의하는 네트워크 개체 또는 네트워크 그룹을 생성합니다. ASA의 경우 주소 범위는 IP 주소 범위를 사용하는 네트워크 개체, 서브넷을 정의하는 네트워크 개체 또는 범위의 모든 주소를 포함하는 네트워크 그룹 개체로 정의할 수 있습니다.

네트워크 개체 또는 네트워크 그룹을 생성할 때 지침을 보려면 ASA 네트워크 개체 및 네트워크 그룹 생성 또는 편집 을 사용합니다.

다음 절차를 위해 네트워크 개체 또는 네트워크 그룹인 Site-to-Site-PC-Pool을 호출합니다.

단계 **1** CDO 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 2 **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 NAT 규칙을 생성하려는 디바이스를 선택합니다.

단계 5 오른쪽의 **Management(**관리**)** 창에서 **NAT**를 클릭합니다.

단계 6  > **Twice NAT(2**회 **NAT)**를 클릭합니다..

단계 7 섹션 1, **Type(**유형**)**에서 **Static(**정적**)**을 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 8 섹션 2, **Interfaces(**인터페이스**)**에서 소스 인터페이스로 **inside(**내부**)**를 선택하고 대상 인터페이스로 **outside(**외부**)**를 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 9 섹션 3, 패킷에서 다음과 같이 변경합니다.

- 원래 주소 메뉴를 확장하고 **Choose(**선택**)**를 클릭한 다음 전제 조건 섹션에서 생성한 사이트 투 사이트 PC 풀 개체를 선택합니다.
- 변환된 주소 메뉴를 펼치고 **Choose(**선택**)**를 클릭한 후 전제 조건 섹션에서 생성한 Site-to-Site-PC-Pool 개체를 선택합니다.

단계 10 섹션 4, **Advanced(**고급**)**을 건너뜁니다.

단계 11 FTD(Firepower Threat Defense)의 경우 섹션 5, **Name(**이름**)**에서 NAT 규칙에 이름을 지정합니다.

단계 12 **Save(**저장**)**를 클릭합니다.

단계 13 ASA의 경우 암호화 맵을 생성합니다. 암호화 맵 생성에 대한 자세한 내용은 CLI 책 3: Cisco ASA Series VPN CLI 구성 가이드를 참조하고 LAN-to-LAN IPsec VPN에 대한 장을 검토하십시오.

단계 14 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

---

**ASA**의 저장된 구성 파일 항목

이러한 절차의 결과로 ASA의 저장된 구성 파일에 나타나는 항목입니다.

**Note** 이것은 FDM 관리 디바이스에 적용되지 않습니다.

이 절차에 의해 생성된 개체

```
object network Site-to-Site-PC-Pool
range 10.10.2.0 10.10.2.255
```

이 절차에 의해 생성된 ***NAT*** 규칙

```
nat (inside,outside) source static Site-to-Site-PC-Pool Site-to-Site-PC-Pool
```

# 가상 프라이빗 네트워크 관리

VPN(Virtual Private Network)은 인터넷과 같은 공용 네트워크를 통해 엔드포인트 간에 보안 터널을 설정합니다.

이 섹션은 ASA(Adaptive Security Appliance) 디바이스의 원격 액세스 및 사이트 투 사이트 VPN에 적용됩니다. 또한 ASA에서 VPN 연결을 배포하고 원격 액세스하는 데 사용되는 SSL 표준에 대해서도 설명합니다.

CDO 에서는 다음과 같은 유형의 VPN 연결을 지원합니다.

- 사이트 간 가상 프라이빗 네트워크, 237 페이지
- 원격 액세스 가상 프라이빗 네트워크

# 사이트 간 가상 프라이빗 네트워크

사이트간 VPN 터널은 다양한 위치에 있는 네트워크를 연결합니다. 관리형 디바이스 및 관리형 디바이스와 모든 관련 표준을 준수하는 다른 Cisco 또는 타사 피어 간에 Site-to-Site IPsec 연결을 만들 수 있습니다. 이러한 피어는 IPv4와 IPv6 주소를 사용하여 내부 주소와 외부 주소를 함께 포함할 수 있습니다 . Site-to-Site 터널은 IPsec(Internet Protocol Security) 프로토콜 제품군 및 인터넷 키 교환 버전 2(IKEv2)를 사용하여 구축됩니다. VPN 연결이 설정되면 로컬 게이트웨이의 뒤에 있는 호스트는 보안 VPN 터널을 통해 원격 게이트의 뒤에 있는 호스트와 연결할 수 있습니다.

### **VPN** 토폴로지

새로운 Site-to-Site VPN 토폴로지를 생성하려면 고유한 이름을 부여하거나 토폴로지 유형을 지정하거나 IPsec IKEv1 또는 IKEv2에 사용되는 IKE 버전 또는 둘 다 및 인증 방법을 선택해야 합니다. 구성된 후 토폴로지를 ASA에 구축합니다.

### **IPsec** 및 **IKE**

CDO에서 Site-to-Site VPN은 IKE 정책과 VPN 토폴로지에 할당된 IPsec 제안을 기반으로 구성됩니다. 정책 및 제안은 IPsec 터널에서 트래픽을 보호하는 데 사용되는 보안 프로토콜 및 알고리즘과 같은 Site-to-Site VPN의 특성을 정의하는 파라미터 집합입니다. VPN 토폴로지에 할당할 수 있는 전체 구성 이미지를 정의하려면 몇 가지 정책 유형이 필요할 수 있습니다.

#### 인증

VPN 연결을 인증하려면 각 디바이스의 토폴로지에서 사전 공유 키를 구성합니다. 사전 공유 키를 사용하면 IKE 인증 단계에서 사용되는 보안 키를 두 피어 간에 공유할 수 있습니다.

### **VPN** 암호화 도메인

VPN의 암호화 도메인은 경로 기반 또는 정책 기반 트래픽 선택기라는 두 가지 방법으로 정의할 수 있습니다.

- 정책 기반: 암호화 도메인은 IPSec 터널에 들어오는 모든 트래픽을 허용하도록 설정됩니다. IPSec 로컬 및 원격 트래픽 선택기는 0.0.0.0으로 설정됩니다. 즉, IPSec 터널로 라우팅되는 모든 트래픽은 소스/대상 서브넷에 관계없이 암호화됩니다. ASA는 암호화 맵을 사용하는 정책 기반 VPN을 지원합니다.
- 경로 기반: 암호화 도메인은 소스와 대상 모두에 대해 특정 IP 범위만 암호화하도록 설정됩니다. 이는 가상 IPsec 인터페이스를 생성하며, 해당 인터페이스에 들어오는 모든 트래픽은 암호화 및 암호 해독됩니다. ASA는 VTI(Virtual Tunnel Interface)를 사용하여 경로 기반 VPN을 지원합니다.

관련 정보:

- ASA에 대한 사이트 간 VPN 구성, on page 238
- ASA 사이트 간 가상 사설망 모니터링

# ASA에 대한 사이트 간 VPN 구성

CDO(Cisco Defense Orchestrator)는 ASA(Adaptive Security Appliance) 디바이스에서 사이트 간 VPN 기능의 다음 측면을 지원합니다.

- IPsec IKEv1 및 IKEv2 프로토콜이 모두 지원됩니다.
- 인증을 위한 자동 또는 수동 사전 공유 키.
- IPv4 및 IPv6. 내부와 외부의 모든 조합이 지원됩니다.
- IPsec IKEv2 사이트 간 VPN 토폴로지는 보안 인증을 준수하기 위한 구성 설정을 제공합니다.
- 정적 및 동적 인터페이스.
- 엔드포인트로 작동하는 엑스트라넷 디바이스의 정적 또는 동적 IP 주소 지원.

### 엑스트라넷 디바이스

각 토폴로지 유형에는 CDO에서 관리되지 않는 엑스트라넷 디바이스가 포함될 수 있습니다. 예를 들면 다음과 같습니다.

- CDO에서 지원하지만 조직에는 책임이 부여되지 않는 Cisco 디바이스. 회사 내의 다른 조직에서 관리하는 네트워크의 스포크 또는 서비스 제공자나 파트너의 네트워크에 대한 연결 등이 포함됩니다.
- 관리되지 않는 디바이스. CDO를 사용하여 관리되지 않는 디바이스에 구성을 생성하거나 구축할 수 없습니다. 관리되지 않는 디바이스를 VPN 토폴로지에 "엑스트라넷" 디바이스로 추가합니다.

### 동적 주소 지정 피어로 사이트 간 VPN 연결 구성

CDO를 사용하면 피어의 VPN 인터페이스 IP 주소 중 하나를 알 수 없거나 인터페이스가 DHCP 서버에서 주소를 가져올 때 피어 간에 사이트 간 VPN 연결을 생성할 수 있습니다. 사전 공유 키, IKE 설정 및 IPsec 구성이 다른 피어와 일치하는 모든 동적 피어는 사이트 간 VPN 연결을 설정할 수 있습니다.

피어 A와 B를 고려하십시오. 고정 피어는 VPN 인터페이스의 IP 주소가 고정되어 있는 디바이스이고 동적 피어는 VPN 인터페이스의 IP 주소를 알 수 없거나 임시 IP 주소가 있는 디바이스입니다.

다음 사용 사례에서는 동적으로 주소가 지정된 피어를 사용하여 안전한 사이트 간 VPN 연결을 설정하는 다양한 시나리오를 설명합니다.

- A는 정적 피어이고 B는 동적 피어이거나 그 반대입니다.
- A는 고정 피어이고 B는 DHCP 서버에서 확인된 IP 주소를 사용하거나 그 반대로 하는 동적 피어입니다.
- A는 동적 피어이고, B는 고정 또는 동적 IP 주소를 사용하는 엑스트라넷 디바이스입니다.
- A는 DHCP 서버에서 확인된 IP 주소를 사용하는 동적 피어이고, B는 고정 또는 동적 IP 주소를 사용하는 엑스트라넷 디바이스입니다.

참고 ASDM(Adaptive Security Device Manager)과 같은 로컬 관리자를 사용하여 인터페이스의 IP 주소를 변경하면 CDO에서 해당 피어의 **Configuration Status(**구성 상태**)**에 "Conflict Detected(충돌 탐지됨)"가 표시됩니다. "충돌 탐지됨" 상태 해결하면 다른 피어의 **Configuration Status(**구성 상태**)**가 "Not Synced(동기화되지 않음)" 상태로 변경됩니다. "Not Synced(동기화되지 않음)" 상태인 디바이스에 CDO 구성을 구축해야 합니다.

일반적으로 동적 피어는 연결을 시작하는 피어여야 합니다. 다른 피어는 동적 피어의 IP 주소를 알지 못하기 때문입니다. 원격 피어가 연결을 설정하려고 시도하면 다른 피어가 사전 공유 키, IKE 설정 및 IPsec 구성을 사용하여 연결을 검증합니다.

원격 피어에서 연결을 시작한 후에만 VPN 연결이 설정되므로 VPN 터널에서 트래픽을 허용하는 액세스 제어 규칙과 일치하는 모든 아웃바운드 트래픽은 연결이 설정될 때까지 중단됩니다. 이를 통해 데이터가 적절한 암호화 및 VPN 보호 없이 네트워크를 벗어나지 않게 합니다.

참고 다음 시나리오에서는 사이트 간 VPN 연결을 구성할 수 없습니다.

디바이스에 둘 이상의 동적 피어 연결이 있는 경우

- 3개의 디바이스 A, B 및 C를 고려하십시오.
- A(고정 피어)와 B(동적 피어) 간에 사이트 간 VPN 연결을 구성합니다.
- 엑스트라넷 디바이스를 생성하여 A와 C(동적 피어) 간에 사이트 간 VPN 연결을 구성합니다. A의 고정 VPN 인터페이스 IP 주소를 엑스트라넷 디바이스에 할당하고 C와의 연결을 설정합니다.

### ASA 사이트 간 VPN 지침 및 제한 사항

- CDO는 S2S VPN에 대한 흥미로운 트래픽을 설계하기 위해 crypto-acl을 지원하지 않습니다. 이는 보호된 네트워크만 지원합니다.

- IKE 포트 500/4500이 사용 중이거나 활성화된 일부 PAT 변환이 있을 때마다 사이트 간 VPN을 동일한 포트에서 구성할 수 없으므로 해당 포트에서 서비스를 시작하는 데 실패합니다.
- 전송 모드는 지원되지 않으며 터널 모드만 지원됩니다. IPsec 터널 모드는 새 IP 패킷에서 페이로드가 되는 원래 IP 데이터그램 전체를 암호화합니다. 방화벽 뒤에 배치되어 있는 호스트와 주고받는 트래픽을 방화벽이 보호하는 경우 터널 모드를 사용합니다. 터널 모드는 인터넷 등의 신뢰할 수 없는 네트워크를 통해 연결하는 두 방화벽 또는 기타 보안 게이트웨이 간에 일반 IPSec이 구현되는 통상적인 방식입니다.
- 이 릴리스에서는 하나 이상의 VPN 터널을 포함하는 PTP 토폴로지만 지원됩니다. Point-to-Point 구축에서는 두 엔드포인트 간에 VPN 터널을 설정합니다.

### Virtual Tunnel Interface에 대한 지침

- VTI는 IPsec 모드에서만 구성할 수 있습니다. ASA에서의 GRE 터널 종료는 지원되지 않습니다.
- 터널 인터페이스를 사용하여 트래픽에 대한 동적 또는 정적 경로를 사용할 수 있습니다.
- 기본 물리적 인터페이스에 따라 VTI에 대한 MTU가 자동으로 설정됩니다. 그러나 VTI가 활성화된 후 물리적 인터페이스 MTU를 변경하는 경우, 새 MTU 설정을 사용하려면 VTI를 비활성화했다가 다시 활성화해야 합니다.
- 네트워크 주소 변환을 적용해야 할 경우, IKE 및 ESP 패킷이 UDP 헤더에서 캡슐화됩니다.
- IKE 및 IPsec 보안 연계는 터널에서 데이터 트래픽에 관계없이 지속적으로 다시 입력됩니다. 이렇게 하면 VTI 터널은 항상 작동합니다.
- 터널 그룹 이름은 피어가 IKEv1 또는 IKEv2 id로 전송하는 항목과 일치해야 합니다.
- LAN-to-LAN 터널 그룹에서 IKEv1의 경우, 터널 인증 방법이 디지털 인증서 및/또는 적극적인 모드를 사용하도록 구성된 피어인 경우, IP 주소가 아닌 이름을 사용할 수 있습니다.
- VTI 및 암호화 맵 구성은 동일한 물리적 인터페이스에서 공존할 수 있으며 암호화 맵에 구성된 피어 주소를 제공하며 VTI에 대한 터널 대상은 서로 다릅니다.
- 기본적으로 VTI를 통과하는 모든 트래픽이 암호화됩니다.
- 기본적으로 VTI 인터페이스의 보안 레벨은 0입니다.
- 액세스 목록은 VTI를 통과하는 트래픽을 제어하기 위해 VTI 인터페이스에 적용될 수 있습니다.
- VTI에서는 BGP만 지원됩니다.
- ASA가 IOS IKEv2 VTI 클라이언트를 종료하는 경우, IOS에서 config-exchange 요청을 비활성화합니다. ASA는 IOS VTI 클라이언트에서 시작한 이 L2L 세션에 대한 mode-CFG 속성을 검색할 수 없기 때문입니다.
- IPv6은 지원되지 않습니다.

관련 정보:

- 사이트 간 VPN 터널 생성, 241 페이지

- VPN에서 사용되는 암호화 및 해시 알고리즘
- NAT에서 원격 액세스 트래픽 제외, 305 페이지

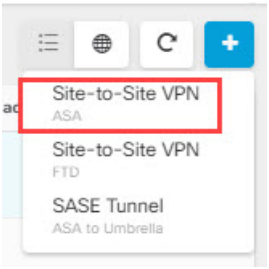
## 사이트 간 VPN 터널 생성

두 ASA 또는 엑스트라넷 디바이스를 사용하는 ASA 간에 사이트 간 VPN 터널을 생성하려면 다음 절차를 수행합니다.

---

단계 1 탐색 창에서 **VPN** > **Site-to-Site ASA/FDM (**사이트 간 **ASA/FDM )**을 선택합니다.

단계 2 오른쪽 상단 모서리에 있는 파란색 더하기 를 클릭하고 ASA 레이블이 있는 **Site-to-Site VPN(**사이트 간 **VPN)**을 클릭합니다.




단계 3 **Configuration Name(**구성 이름**)** 필드에 생성한 사이트 간 VPN 구성의 이름을 입력합니다.

단계 4 새 정책 기반 또는 경로 기반 사이트 간 VPN을 생성하는 옵션 중 하나를 선택합니다.

단계 5 **Peer Devices(**피어 디바이스**)** 섹션에서 다음을 수행합니다.

a) 피어 **1**: ASA 디바이스를 선택하고 **Select(**선택**)**를 클릭합니다.

b) 피어 **2**: 다른 ASA 디바이스를 선택한 다음 **Select(**선택**)**를 클릭합니다.

엑스트라넷: 피어 2에서 엑스트라넷 디바이스를 선택하려면 엑스트라넷 슬라이더를 클릭하여 활성화합니다.

**Static(**고정**)**을 선택하고 IP 주소를 지정하거나, DHCP 할당 IP가 있는 엑스트라넷 디바이스의 경우 **Dynamic(**동적**)**을 선택합니다. **IP Address(IP** 주소**)**는 정적 인터페이스의 IP 주소 또는 동적 인터페이스의 **DHCP Assigned(DHCP** 할당됨**)**를 표시합니다.

c) 엔드포인트 디바이스에 대한 **VPN** 액세스 인터페이스를 선택합니다.

d) (경로 기반 VPN에 적용 가능) LAN 서브넷을 제어하는 **LAN** 인터페이스를 선택합니다. 여러 인터페이스를 선택할 수 있습니다.

선택한 LAN 인터페이스에 연결된 네트워크가 라우팅 정책 액세스 목록에 추가됩니다. 라우팅 정책 액세스 목록과 일치하는 트래픽은 VPN 터널에 의해 암호화/암호 해독됩니다.

e) (정책 기반에 적용 가능) 참여 디바이스에 대해 보호된 네트워크를 추가하려면 **Add Network(**네트워크 추가**)**를 클릭합니다.

f) (선택 사항이며 정책 기반에 적용 가능) 로컬 VPN 액세스 인터페이스의 NAT 정책에서 VPN 트래픽을 제외하려면 **NAT Exempt(NAT** 면제**)**를 선택합니다. 개별 피어에 대해 수동으로 구성해야 합니다. NAT 규칙을 로컬 네트워크에 적용하지 않으려는 경우 로컬 네트워크를 호스팅하는 인터페이스를 선택합니다. 이 옵션은 로컬 네트워크가 단일 라우팅 인터페이스(브리지 그룹 멤버 아님) 뒤에 있는 경우에만 작동합니다. 로컬 네트워크가 둘

이상의 라우팅 인터페이스 또는 하나 이상의 브리지 그룹 멤버 뒤에 있는 경우에는 NAT 제외 규칙을 수동으로 생성해야 합니다. 필요한 규칙을 수동으로 생성하는 방법에 대한 자세한 내용은 NAT에서 ASA 사이트 간 VPN 트래픽 제외를 참조하십시오.

g) **Next(**다음**)**를 클릭합니다.

단계 **6** (라우트 기반에 적용 가능) 이전 단계에서 피어 디바이스가 구성되면 터널 세부 정보에서 **VTI** 주소 필드가 자동으로 채워집니다. 필요한 경우 새 VTI로 사용할 IP 주소를 수동으로 입력할 수 있습니다.

단계 **7** **IKE Settings(IKE** 설정**)** 섹션에서 IKE(Internet Key Exchange) 협상 중에 사용할 IKE 버전을 선택하고 프라이버시 구성을 지정합니다. IKE 정책에 대한 자세한 내용은 글로벌 IKE 정책 구성을 참조하십시오.

CDO는 사용자가 수행한 구성에 따라 IKE 설정을 제안합니다. 권장 IKE 구성 설정을 계속 사용하거나 새로 정의할 수 있습니다.

참고 IKE 정책은 디바이스에 전역적이며 연결된 모든 VPN 터널에 적용됩니다. 따라서 정책을 추가하거나 삭제하면 이 디바이스가 참여하는 모든 VPN 터널에 영향을 미칩니다.

a) 적절하게 IKE 버전 중 하나 또는 둘 다를 선택합니다.

기본적으로 **IKEV** 버전 **2**가 활성화되어 있습니다.

참고 경로 기반 VPN에는 두 IKE 버전을 모두 활성화할 수 없습니다.

b) **Add IKEv2 Policy(IKEv2** 정책 추가**)**를 클릭하고 IKEv2 정책을 선택합니다.

참고 **Create New IKEv2 Policy(**새 **IKEv2** 정책 생성**)**를 클릭하여 새 IKEv2 정책을 생성합니다. 새 IKEv2 정책 생성에 대한 자세한 내용은 IKEv2 정책 관리을 참고하십시오. 기존 IKEv2 정책을 삭제하려면 선택한 정책 위에 마우스를 놓고 x 아이콘을 클릭합니다.

c) 참여 디바이스에 대한 사전 공유 키를 입력합니다. 사전 공유 키는 연결에서 각 피어에 컨피그레이션된 암호 키 문자열입니다. IKE는 인증 단계 중에 이러한 키를 사용합니다.

(IKEv2) 피어 **1** 사전 공유 키, 피어 **2** 사전 공유 키: IKEv2의 경우 각 피어에서 고유한 키를 구성할 수 있습니다. 사전 공유 키를 입력합니다. show(표시) 버튼을 클릭하고 피어에 대해 적절한 사전 공유를 입력할 수 있습니다. 키는 영숫자 1~127자가 될 수 있습니다. 다음 표에서는 두 피어에 대한 사전 공유 키의 용도에 대해 설명합니다.

| | 로컬 사전 공유 키 | 원격 피어 사전 공유 키 |
|---|---|---|
| 피어 **1** | 피어 1 사전 공유 키 | 피어 2 사전 공유 키 |
| 피어 **2** | 피어 2 사전 공유 키 | 피어 1 사전 공유 키 |

d) **IKE Version 1(IKE** 버전 **1)**을 클릭하여 활성화합니다.

e) **Add IKEv1 Policy(IKEv1** 정책 추가**)**를 클릭하고 IKEv1 정책을 선택합니다. **Create New IKEv1 Policy(**새 **IKEv1** 정책 생성**)**를 클릭하여 새 IKEv1 정책을 생성합니다. 새 IKEv1 정책 생성에 대한 자세한 내용은 IKEv1 정책 관리을 참고하십시오. 기존 IKEv1 정책을 삭제하려면 선택한 정책 위에 마우스 커서를 올리고 x 아이콘을 클릭합니다.

f) (IKEv1) 사전 공유 키: IKEv1의 경우, 각 피어에서 동일한 사전 공유 키를 컨피그레이션해야 합니다. 키는 영숫자 1~127자가 될 수 있습니다. 이 시나리오에서 피어 1과 피어 2는 동일한 사전 공유 키를 사용하여 데이터를 암호화하고 해독합니다.

g) **Next(**다음**)**를 클릭합니다.

단계 **8** **IPSec Settings(IPSec** 설정**)** 섹션에서 CDO는 사용자가 수행한 구성을 기반으로 IKEv2 제안을 제안합니다. 권장 IKE 구성 설정을 계속 사용하거나 새로 정의할 수 있습니다. IPSec 설정에 대한 자세한 내용은 IPsec 제안 구성을 참고하십시오.

a) **+ IKEv2 Proposals(+ IKEv2** 제안**)**를 클릭하여 IPSec 구성을 선택합니다. **IKE Settings(IKE** 설정**)** 단계에서 선택한 항목에 따라 해당 IKEV 제안을 사용할 수 있습니다. 기존 IKEv2 제안을 삭제하려면 선택한 제안 위에 마우스를 올려 놓고 x 아이콘을 클릭합니다.

참고 **Create New IKEv2 Proposals(**새 **IKEv2** 제안 생성**)**를 클릭하여 새 IKEv2 제안을 생성합니다. 새 IKEv2 정책 생성에 대한 자세한 내용은 IPsec 제안 구성을 참고하십시오.

b) **Perfect Forward Secrecy**용 **Diffie-Hellman** 그룹을 선택합니다. 자세한 내용은 VPN에서 사용되는 암호화 및 해시 알고리즘, 243 페이지를 참조하십시오.

c) **Next(**다음**)**를 클릭합니다.

단계 **9** **Finish(**완료**)** 섹션에서 구성을 읽고 구성에 만족하는 경우에만 계속 진행하고 **Submit(**제출**)**을 클릭하십시오.

새로 구성된 사이트 간 VPN 터널을 표시하는 VPN Tunnels(VPN 터널) 페이지로 이동합니다. 변경 사항이 준비되며 수동으로 구축해야 합니다. VTI 터널을 통해 디바이스 간에 VTI 트래픽을 자동으로 라우팅하도록 라우팅 정책이 생성됩니다. 이 정책을 보려면 **Inventory(**인벤토리**)** 페이지에서 디바이스를 선택하고 **Configuration(**구성**)** > **Diff(**차이**)**를 선택하십시오.

새 터널과 연결된 디바이스에 사이트 간 VPN 구성을 구축하려면 CDO GUI를 사용하여 구성 변경 사항 구축 섹션을 참조하십시오.

## 기존 CDO 사이트 투 사이트 VPN 삭제

단계 **1** 탐색 모음에서 **VPN**> **ASA/FDM Site-to-Site VPN(ASA/FDM** 사이트 간 **VPN)**을 선택합니다.

단계 **2** 삭제할 원하는 사이트 투 사이트 VPN 터널을 선택합니다.

단계 **3** **Actions(**작업**)** 창에서 **Delete(**삭제**)**를 클릭합니다.

선택한 사이트 투 사이트 VPN 터널이 삭제됩니다.

## VPN에서 사용되는 암호화 및 해시 알고리즘

VPN 터널은 일반적으로 공용 네트워크(대개 인터넷)를 통과하므로 연결을 암호화하여 트래픽을 보호해야 합니다. IKE 정책 및 IPsec 제안을 사용하여 적용할 암호화 및 기타 보안 기술을 정의합니다.

디바이스 라이선스에서 강력한 암호화 적용이 허용되는 경우에는 광범위한 암호화 및 해시 알고리즘과 Diffie-Hellman 그룹 중에서 선택할 수 있습니다. 그러나 일반적으로는 터널에 적용하는 암호화가 강력할수록 시스템 성능은 더 나빠집니다. 따라서 효율성을 저하하지 않으면서 충분한 보호 기능을 제공하는 보안과 성능 간의 적절한 균형 지점을 찾아야 합니다.

Cisco는 선택할 수 있는 옵션에 대한 구체적인 지침을 제공하지는 않습니다. 대규모 기업이나 기타 조직 내에서 보안을 담당하는 경우 충족해야 하는 표준이 이미 정의되어 있을 수 있습니다. 그렇지 않은 경우, 선택할 수 있는 옵션에 대해 조사해야 합니다.

다음 주제에서는 사용 가능한 옵션에 대해 설명합니다.

### 사용할 암호화 알고리즘 결정

IKE 정책 또는 IPsec 제안에 사용할 암호화 알고리즘을 결정할 때는 VPN의 디바이스가 지원하는 알고리즘으로 선택이 제한됩니다.

IKEv2의 경우 여러 암호화 알고리즘을 구성할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 해당 순서를 사용하여 피어와 협상합니다. IKEv1의 경우 단일 옵션만 선택할 수 있습니다.

IPsec 제안의 경우 알고리즘은 인증, 암호화 및 재생 방지 서비스를 제공하는 ESP(Encapsulating Security Protocol)에서 사용됩니다. ESP는 IP 프로토콜 유형 50입니다. IKEv1 IPsec 제안에서 알고리즘 이름에는 ESP- 접두사가 붙습니다.

디바이스 라이선스에 따라 강력한 암호화를 사용할 수 있는 경우 다음 암호화 알고리즘 중에서 선택할 수 있습니다. 강력한 암호화를 사용할 수 없으면 DES만 선택할 수 있습니다.

- AES-GCM - (IKEv2만 해당) 기밀 유지 및 데이터 원본 인증 기능을 제공하는 블록 암호화 작동 모드인 AES-GCM(Advanced Encryption Standard in Galois/Counter Mode)은 AES보다 보안성이 뛰어납니다. AES-GCM은 세 가지 키 강도(128비트, 192비트 및 256비트 키)를 제공합니다. 키 길이가 길수록 보안성은 더 높지만 성능은 낮습니다. GCM은 NSA Suite B를 지원하는 데 필요한 AES의 모드입니다. NSA Suite B는 암호화 강도에 대한 연방 기준을 충족시키기 위해 디바이스가 지원해야 하는 암호화 알고리즘 세트입니다.
- AES-GMAC - (IKEv2 IPsec 제안만 해당) AES-GMAC(Advanced Encryption Standard Galois Message Authentication Code)는 데이터 원본 인증 기능만 제공하는 블록 암호화 작동 모드입니다. 이 모드는 데이터를 암호화하지 않고 데이터 인증을 허용하는 AES-GCM의 변형입니다. AES-GMAC는 세 가지 키 강도(128비트, 192비트 및 256비트 키)를 제공합니다.
- AES - AES(Advanced Encryption Standard)는 DES보다 보안성이 뛰어나며 3DES보다 계산 효율성이 높은 대칭 암호화 알고리즘입니다. AES는 세 가지 키 강도(128비트, 192비트 및 256비트 키)를 제공합니다. 키 길이가 길수록 보안성은 더 높지만 성능은 낮습니다.
- DES - 56비트 키를 사용하여 암호화를 수행하는 DES(Data Encryption Standard)는 대칭 보안 키 블록 알고리즘입니다. 라이선스 어카운트가 내보내기 제어에 대한 요건을 충족하지 않는 경우에는 이 옵션이 유일한 옵션입니다. 3DES보다 속도가 빠르며 시스템 리소스를 더 적게 사용하지만 보안성은 더 낮습니다. 강력한 데이터 기밀 유지 기능이 필요하지 않으며 시스템 리소스나 속도가 중요한 경우에는 DES를 선택하십시오.
- 3DES - 56비트 키를 사용하여 암호화를 3회 수행하는 3DES(Triple DES)는 서로 다른 키를 사용하여 각 데이터 블록을 3회 처리하므로 DES보다 안전합니다. 그러나 시스템 리소스를 더 많이 사용하며 DES보다 속도가 느립니다.
- NULL - null 암호화 알고리즘은 암호화를 수행하지 않는 인증 기능을 제공합니다. 이 알고리즘은 대개 테스트용으로만 사용됩니다.

### 사용할 해시 알고리즘 결정

IKE 정책에서 해시 알고리즘은 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성합니다. IKEv2에서 해시 알고리즘은 두 가지 옵션으로 구분됩니다. 그중 하나는 무결성 알고리즘 옵션이고 다른 하나는 PRF(Pseudo-Random Function: 의사 난수 함수) 옵션입니다.

IPsec 제안에서 해시 알고리즘은 인증을 위한 ESP(Encapsulating Security Protocol)에서 사용됩니다. IKEv2 IPsec 제안에서는 이러한 알고리즘을 무결성 해시라고 합니다. IKEv1 IPsec 제안에서는 알고리즘 이름에 ESP- 접두사가 붙으며 -HMAC(Hash Method Authentication Code) 접미사도 붙습니다.

IKEv2의 경우 여러 해시 알고리즘을 구성할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 해당 순서를 사용하여 피어와 협상합니다. IKEv1의 경우 단일 옵션만 선택할 수 있습니다.

다음 해시 알고리즘 중에서 선택할 수 있습니다.

- SHA(Secure Hash Algorithm) - 표준 SHA(SHA-1)에서는 160비트 다이제스트를 생성합니다. SHA는 MD5보다 무차별 암호 대입 공격에 대한 방어력이 뛰어납니다. 그러나 MD5 보다 리소스를 더 많이 사용 합니다. 최고 보안 레벨이 필요한 구현의 경우 SHA 해시 알고리즘을 사용합니다.
- IKEv2 컨피그레이션에는 다음과 같은 더욱 안전한 SHA-2 옵션을 사용할 수 있습니다. NSA Suite B 암호화 사양을 구현하려는 경우 이러한 옵션 중 하나를 선택합니다.
  - SHA-256 - 256비트 다이제스트를 생성하는 Secure Hash Algorithm SHA-2를 지정합니다.
  - SHA-384 - 384비트 다이제스트를 생성하는 Secure Hash Algorithm SHA-2를 지정합니다.
  - SHA-512 - 512비트 다이제스트를 생성하는 Secure Hash Algorithm SHA-2를 지정합니다.
- MD5(Message Digest 5) - 128비트 다이제스트를 생성합니다. MD5는 SHA보다 전반적으로 성능이 우수하여 처리 시간이 짧지만 SHA보다 취약한 것으로 간주됩니다.
- null 또는 None(NULL, ESP-NONE) - (IPsec 제안에만 해당됨) null 해시 알고리즘으로, 대개 테스트용으로만 사용됩니다. 그러나 암호화 알고리즘으로 AES-GCM/GMAC 옵션 중 하나를 선택하는 경우에는 null 무결성 알고리즘을 선택해야 합니다. null 이외의 옵션을 선택하더라도 이러한 암호화 표준에 대해서는 무결성 해시가 무시됩니다.

### 사용할 **Diffie-Hellman** 모듈러스 그룹 결정

다음 Diffie-Hellman 키 파생 알고리즘을 사용하여 IPsec 보안 연계(SA) 키를 생성할 수 있습니다. 각 그룹의 크기 모듈러스는 서로 다릅니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어에 일치하는 모듈러스 그룹이 있어야 합니다.

AES 암호화를 선택하는 경우 AES에 필요한 큰 키를 지원하려면 DH(Diffie-Hellman) 그룹 5 이상을 사용해야 합니다. IKEv1 정책에서는 아래에 나열된 그룹을 모두 지원하지는 않습니다.

NSA Suite B 암호화 사양을 구현하려면 IKEv2를 사용하고 ECDH(Elliptic Curve Diffie-Hellman) 옵션 19, 20, 21 중 하나를 선택합니다. 2048비트 모듈러스를 사용하는 엘립틱 커브 옵션과 그룹은 Logjam과 같은 공격에 노출될 가능성이 작습니다.

IKEv2의 경우에는 여러 그룹을 구성할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 해당 순서를 사용하여 피어와 협상합니다. IKEv1의 경우 단일 옵션만 선택할 수 있습니다.

- 2 - Diffie-Hellman 그룹 2: 1024비트 MODP(모듈식 지수) 그룹. 이 옵션은 더 이상 좋은 보호 방법으로 간주되지 않습니다.

- 5 - Diffie-Hellman 그룹 5: 1536비트 MODP 그룹. 전에는 이 옵션이 128비트 키에 대해 좋은 보호 방법으로 간주되었지만 이제는 더 이상 좋은 보호 방법으로 간주되지 않습니다.
- 14 - Diffie-Hellman 그룹 14: 2048비트 MODP(모듈식 지수) 그룹. 192비트 키에 적합한 보호를 제공합니다.
- 19 - Diffie-Hellman 그룹 19: NIST(국내 표준 및 기술) 256비트 ECP(elliptic curve modulo a prime) 그룹
- 20 - Diffie-Hellman 그룹 20: NIST 384비트 ECP 그룹
- 21 - Diffie-Hellman 그룹 21: NIST 521비트 ECP 그룹
- 24 - Diffie-Hellman 그룹 24: 2048비트 MODP 그룹 및 256비트 소수 위수 하위 그룹. 이 옵션은 더 이상 권장되지 않습니다.

사용할 인증 방법 결정

다음과 같은 방법을 사용하여 사이트 간 VPN 연결에서 피어를 인증할 수 있습니다.

사전 공유 키

사전 공유 키는 연결에서 각 피어에 컨피그레이션된 암호 키 문자열입니다. 이 키는 인증 단계 중에 IKE에서 사용합니다. IKEv1의 경우, 각 피어에서 동일한 사전 공유 키를 컨피그레이션해야 합니다. IKEv2의 경우, 각 피어에 고유 키를 컨피그레이션할 수 있습니다.

사전 공유 키는 인증서에 비해 확장성이 떨어집니다. 다수의 Site-to-Site VPN 연결을 컨피그레이션해야 하는 경우, 사전 공유 키 방법 대신 인증서 방법을 사용하십시오.

## NAT에서 사이트 간 VPN 트래픽 제외

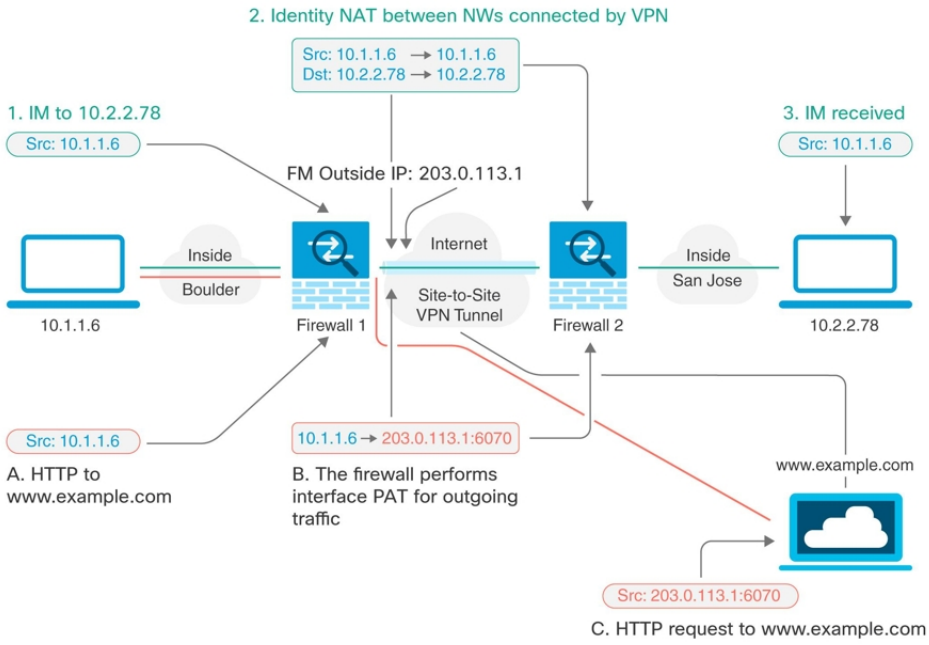
인터페이스에 사이트 대 사이트 VPN 연결이 정의되어 있고 해당 인터페이스에 대한 NAT 규칙도 있는 경우 NAT 규칙에서 VPN의 트래픽을 선택적으로 제외할 수 있습니다. VPN 연결의 원격 쪽에서 내부 주소를 처리할 수 있는 경우 이러한 VPN 트래픽을 제외할 수 있습니다.

VPN 연결을 생성할 때 **NAT Exempt(NAT** 제외**)** 옵션을 선택하여 규칙을 자동으로 생성할 수 있습니다. 그러나 브리지 그룹 멤버가 아닌 단일 라우팅 인터페이스를 통해 보호된 로컬 네트워크에 연결하는 경우에만 이 방법을 사용할 수 있습니다. 그렇지 않고 연결의 로컬 네트워크가 둘 이상의 라우팅 인터페이스 또는 하나 이상의 브리지 그룹 멤버에 있는 경우에는 NAT 제외 규칙을 수동으로 구성해야 합니다.

NAT 규칙에서 VPN 트래픽을 제외하려면 대상이 원격 네트워크일 때 로컬 트래픽에 대한 ID 수동 NAT 규칙을 생성합니다. 그런 다음 대상이 인터넷 등의 다른 항목일 때 트래픽에 NAT를 적용합니다. 로컬 네트워크의 인터페이스가 여러 개인 경우 각 인터페이스에 대해 규칙을 생성합니다. 또한 다음과 같은 제안 사항을 고려합니다.

- 연결에 로컬 네트워크가 여러 개 있으면 네트워크를 정의하는 개체를 포함할 네트워크 개체 그룹을 생성합니다.
- VPN에 IPv4 및 IPv6 네트워크를 둘 다 포함하는 경우 각 네트워크에 대해 별도의 ID NAT 규칙을 생성합니다.

볼더 사무실과 산호세 사무실을 연결하는 사이트 대 사이트 터널을 보여주는 다음 예를 살펴보십시오. 인터넷으로 이동할 트래픽(예: 볼더의 10.1.1.6에서 www.example.com으로)의 경우 인터넷 액세스를 위해 NAT에서 제공하는 공용 IP 주소가 필요합니다. 아래 예에서는 인터페이스 PAT(Port Address Translation) 규칙을 사용합니다. 그러나 VPN 터널을 지나갈 트래픽(예: 볼더의 10.1.1.6에서 산호세의 10.2.2.78로)에 대해서는 NAT를 수행하지 않으려고 합니다. 그렇게 하려면 ID NAT 규칙을 만들어 해당 트래픽을 제외해야 합니다. ID NAT는 주소를 동일한 주소로 변환합니다.




다음 예에서는 방화벽1(볼더)의 컨피그레이션에 대해 설명합니다. 이 예에서는 내부 인터페이스가 브리지 그룹이라고 가정하므로 각 멤버 인터페이스에 대해 규칙을 작성해야 합니다. 라우팅 내부 인터페이스가 하나이든 여러 개이든 프로세스는 동일합니다.

**Note** 이 예에서는 IPv4만 사용한다고 가정합니다. VPN에 IPv6 네트워크도 포함되어 있으면 IPv6용 병렬 규칙을 생성합니다. IPv6 인터페이스 PAT를 구현할 수는 없으므로 PAT에 사용할 고유 IPv6 주소가 포함된 호스트 개체를 생성해야 합니다.

단계 **1** 여러 네트워크를 정의하기 위한 개체를 생성합니다.

**a.** 좌측의 CDO 내비게이션 바에서 **Objects(**개체**) > FDM Objects(FDM** 개체**)**를 클릭합니다.

**b.** 파란색 더하기 버튼 을 클릭하여 개체를 생성합니다.

**c.** **ASA** > **Network(ASA** 네트워크**)**를 클릭합니다.

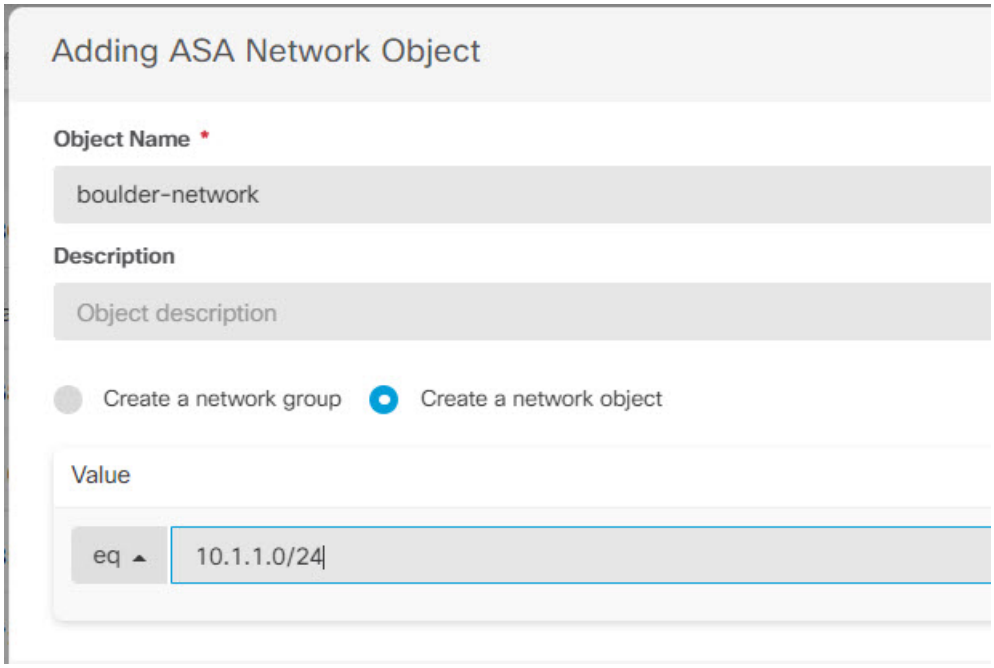
**d.** 볼더 내부 네트워크를 확인합니다.

e. 개체 이름을 입력합니다(예: boulder-network).

f. **Create a network object(**네트워크 개체 생성**)**를 선택합니다.

g. Value(값) 섹션에서 다음을 수행합니다.

- **eq**를 선택하고 단일 IP 주소 또는 CIDR 표기법으로 표시된 서브넷 주소를 입력합니다.
- 범위를 선택하고 IP 주소 범위를 입력합니다. 예를 들어 네트워크 주소를 10.1.1.0/24로 입력합니다.




h. **Add(**추가**)**를 클릭합니다.

i. 파란색 더하기 버튼 을 클릭하여 개체를 생성합니다.

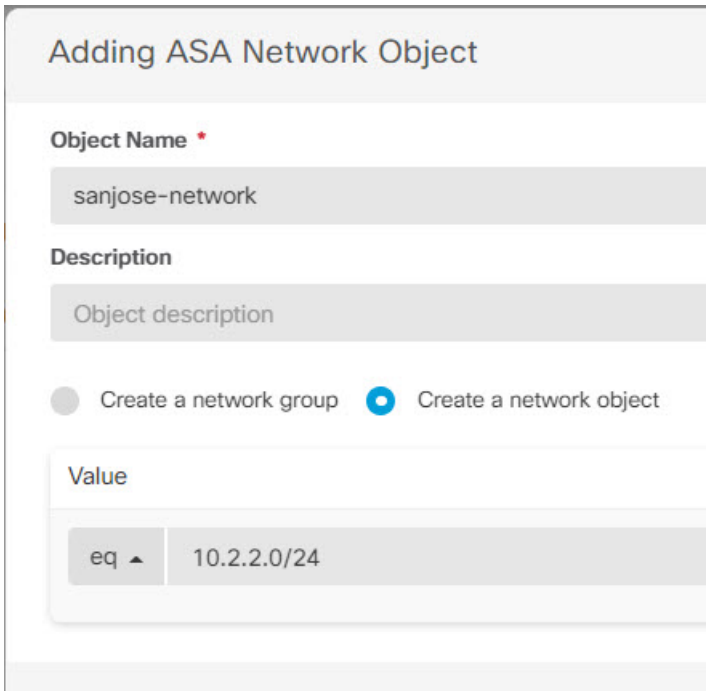
j. 내부 산호세 네트워크를 정의합니다.

k. 개체 이름(예: san-jose)을 입력합니다.

l. **Create a network object(**네트워크 개체 생성**)**를 선택합니다.

m. Value(값) 섹션에서 다음을 수행합니다.

- **eq**를 선택하고 단일 IP 주소 또는 CIDR 표기법으로 표시된 서브넷 주소를 입력합니다.
- 범위를 선택하고 IP 주소 범위를 입력합니다. 예를 들어 네트워크 주소를 10.1.1.0/24로 입력합니다.




**n.** **Add(**추가**)**를 클릭합니다.

단계 **2** 방화벽1(볼더)에서 VPN을 통해 산호세로 이동할 때 볼더 네트워크용 수동 ID NAT를 구성합니다.

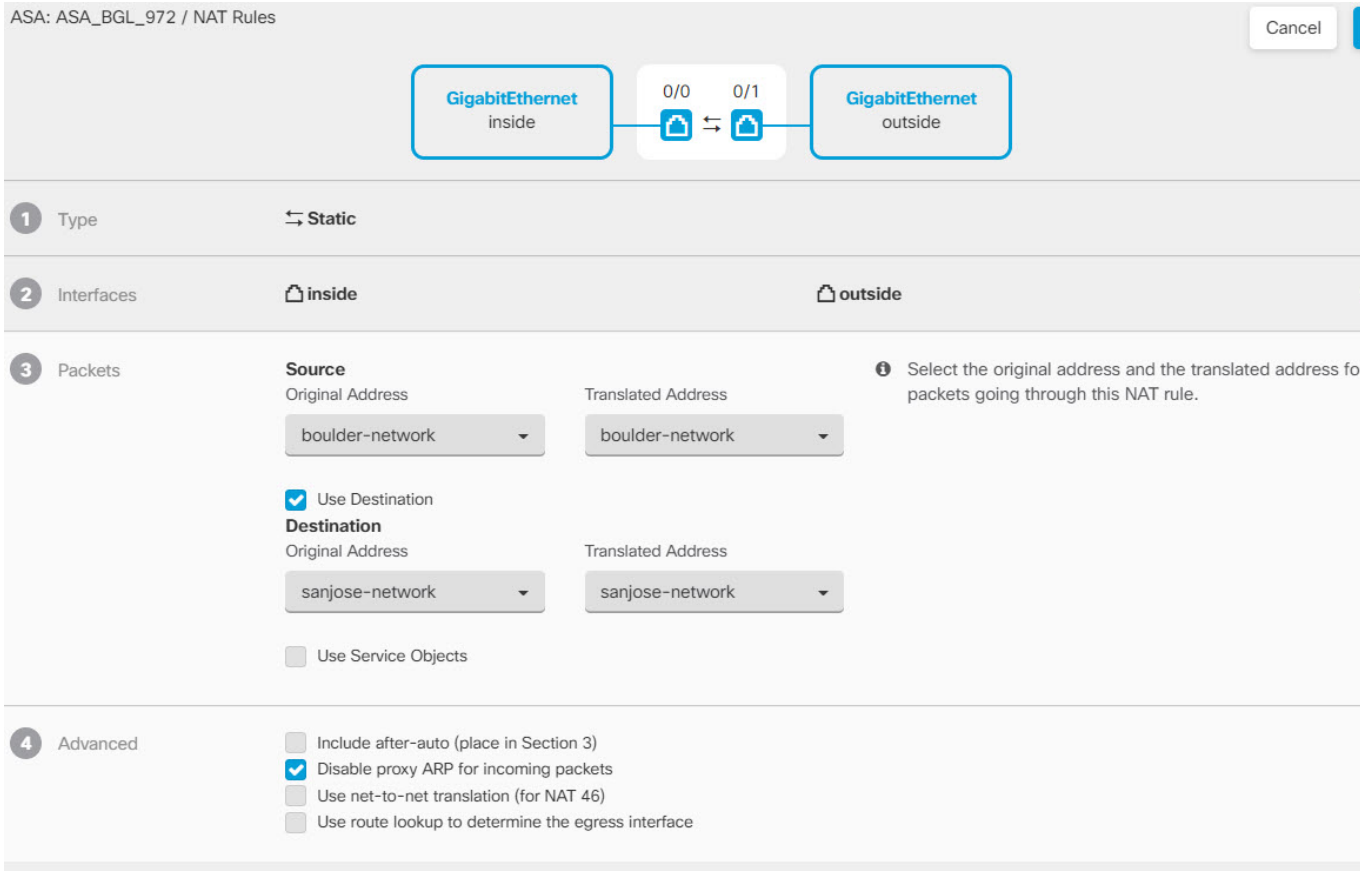
**a.** CDO 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

**b.** 필터를 사용하여 NAT 규칙을 생성할 디바이스를 찾습니다.

**c.** 상세정보 패널의 Management(관리) 영역에서 **NAT** NAT를 클릭합니다.

**d.** + > **2**회 **NAT**를 클릭합니다.

- 섹션 1에서 **Static(**정적**)**을 선택합니다. **Continue(**계속**)**를 클릭합니다.
- 섹션 2에서 **Source Interface(**소스 인터페이스**)** = **inside(**내부**)** 및 **Destination Interface(**대상 인터페이스**)** = **outside(**외부**)**를 선택합니다. **Continue(**계속**)**를 클릭합니다.
- 섹션 3에서 **Source Original Address(**소스 원본 주소**)** = 'boulder-network' 및 **Source Translated Address(**소스 변환 주소**)** = 'boulder-network'를 선택합니다.
- **Use Destination(**대상 사용**)**을 선택합니다.
- **Destination Original Address(**대상 원본 주소**)** = 'sanjose-network' 및 **Source Translated Address(**소스 변환 주소**)** = 'sanjose-network'를 선택합니다. 참고: 대상 주소를 변환하지 않을 것이기 때문에 원본 주소 및 변환된 대상 주소에 대해 동일한 주소를 지정하여 대상 주소에 대한 ID NAT를 구성해야 합니다. 포트 필드는 모두 비워 둡니다. 이 규칙은 소스 및 대상 둘 다에 대해 ID NAT를 구성합니다.




- **Disable proxy ARP for Incoming packet(**수신 패킷에 대해 프록시 **ARP** 비활성화**)**을 선택합니다.
- **Save(**저장**)**를 클릭합니다.
- 이 프로세스를 반복하여 각각의 기타 내부 인터페이스에 대해 동일 규칙을 생성합니다.

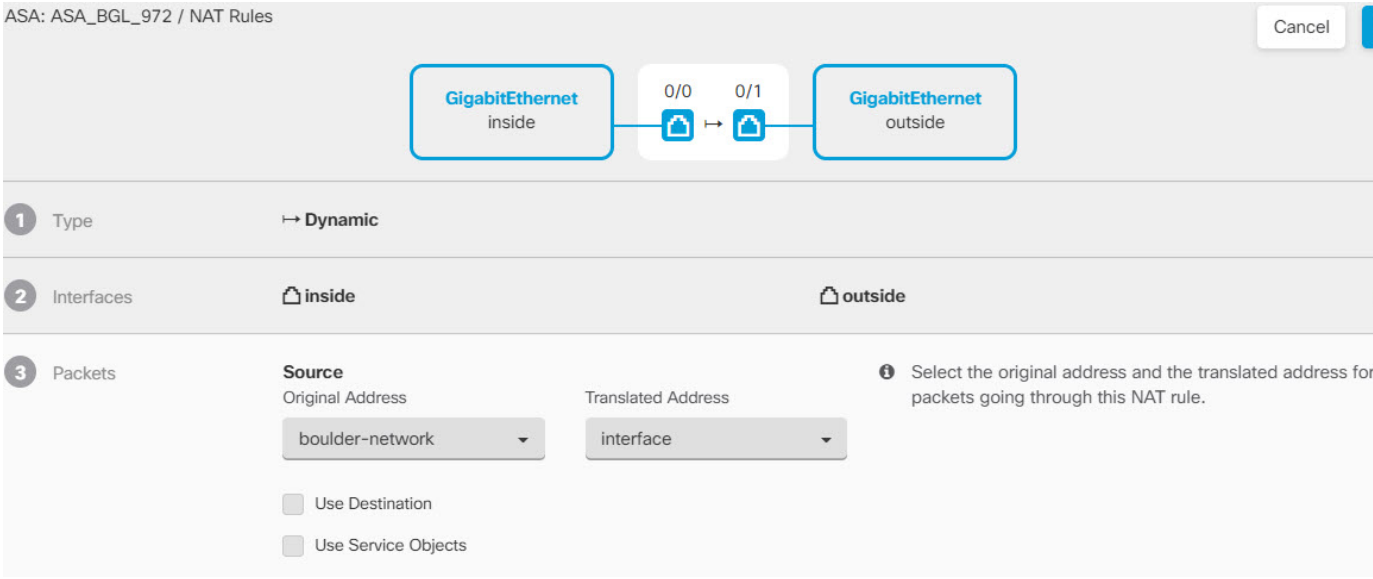
단계 **3** 방화벽1(볼더)에서 내부 볼더 네트워크에 대해 인터넷으로 이동할 때 수동 동적 인터페이스 PAT를 구성합니다. 참고: 모든 IPv4 트래픽에 적용되는 내부 인터페이스용 동적 인터페이스 PAT 규칙은 이미 있을 수 있습니다. 이러한 규칙은 초기 구성 중에 기본적으로 생성되기 때문입니다. 그러나 여기서는 완전한 설명을 위해 컨피그레이션을 제공합니다. 이러한 단계를 완료하기 전에 내부 인터페이스와 네트워크에 적용되는 규칙이 이미 있는지 확인하고 해당 규칙이 있으면 이 단계를 건너뜁니다.

**a.**  > **2**회 **NAT**를 클릭합니다.

**b.** 섹션 1에서 **Dynamic(**동적**)**을 선택합니다. **Continue(**계속**)**를 클릭합니다.

**c.** 섹션 2에서 **Source Interface(**소스 인터페이스**)** = **inside(**내부**)** 및 **Destination Interface(**대상 인터페이스**)** = **outside(**외부**)**를 선택합니다. **Continue(**계속**)**를 클릭합니다.

**d.** 섹션 3에서 **Source Original Address(**소스 원본 주소**)** = 'boulder-network' 및 **Source Translated Address(**소스 변환 주소**)** = 'interface'를 선택합니다.




e. **Save(**저장**)**를 클릭합니다.

f. 이 프로세스를 반복하여 각각의 기타 내부 인터페이스에 대해 동일 규칙을 생성합니다.

단계 **4** CDO에 구성 변경 사항을 구축합니다. 자세한 내용은 CDO GUI를 사용하여 구성 변경 사항 구축, on page 355를 참고하십시오.

단계 **5** 방화벽2(산호세)도 관리하는 경우 해당 디바이스에 대해 비슷한 규칙을 구성할 수 있습니다.

- 대상이 boulder-network일 때는 sanjose-network용 수동 ID NAT 규칙을 구성합니다. 방화벽2 내부 및 외부 네트워크용으로 새 인터페이스 개체를 생성합니다.
- 대상이 "임의"일 때는 sanjose-network용 수동 동적 인터페이스 PAT 규칙을 생성합니다.

## 글로벌 **IKE** 정책 구성

IKE(Internet Key Exchange)는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용되는 키 관리 프로토콜입니다.

IKE 협상은 2단계로 구성됩니다. 1단계에서는 두 IKE 피어 간의 보안 연계를 협상합니다. 그러면 피어가 2단계에서 안전하게 통신할 수 있습니다. 2단계 협상 중에는 IKE가 IPsec 등의 기타 애플리케이션에 대해 SA를 설정합니다. 두 단계에서는 모두 연결을 협상할 때 제안을 사용합니다. IKE 제안은 두 피어가 상호 간의 IKE 협상을 보호하는 데 사용하는 알고리즘 집합입니다. IKE 협상에서는 두 피어가 먼저 공통(공유) IKE 정책을 합의합니다. 이 정책은 후속 IKE 협상을 보호하는 데 사용되는 보안 파라미터를 제시합니다.

IKE 정책 개체는 이러한 협상을 위한 IKE 제안을 정의합니다. 활성화하는 개체는 피어가 VPN 연결을 협상할 때 사용됩니다. 연결당 서로 다른 IKE 정책을 지정할 수는 없습니다. 각 개체의 상대 우선순위에 따라 이러한 정책 중 먼저 사용을 시도할 정책이 결정되며, 숫자가 작을수록 우선 순위는 높

습니다. 협상에서 장애가 발생하여 두 피어가 모두 지원할 수 있는 정책을 찾지 못하면 연결이 설정되지 않습니다.

글로벌 IKE 정책을 정의하려면 각 IKE 버전에 대해 활성화할 개체를 선택합니다. 사전 정의된 개체가 요건을 충족하지 않는 경우 새 정책을 생성하여 보안 정책을 적용합니다.

다음 절차에서는 개체 페이지를 통해 글로벌 정책을 구성하는 방법을 설명합니다. IKE 정책 설정에서 Edit(수정)을 클릭하여 VPN 연결을 수정할 때 정책을 활성화, 비활성화 및 생성할 수도 있습니다.

다음 항목에서는 각 버전에 대해 IKE 정책을 구성하는 방법에 대해 설명합니다.

- IKEv1 정책 관리
- IKEv2 정책 관리

## IKEv1 정책 관리

IKEv1 정책을 생성하고 편집하는 방법을 설명합니다.

### IKEv1 정책 정보

IKE(Internet Key Exchange) 버전 1 정책 개체에는 VPN 연결을 정의할 때 IKEv1 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv1 정책이 있습니다. 필요에 맞는 정책이 있으면 State(상태) 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

**Related Topics**

IKEv1 정책 생성 또는 편집, 252 페이지

### *IKEv1* 정책 생성 또는 편집

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKE Policy(**새 **IKE** 정책 생성**)** 링크를 클릭하여 사이트 간 VPN 연결에서 IKE 설정을 편집하면서 IKEv1 정책을 생성할 수도 있습니다.

---

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > FDM Objects(FDM** 개체**)**을 클릭합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 파란색 더하기  버튼을 클릭하고 **FDM** > **IKEv1 Policy(IKEv1** 정책**)**를 선택하여 새 IKEv1 정책을 생성합니다.
- 개체 페이지에서 편집할 IKEv1 정책을 선택하고 오른쪽의 Actions(작업) 창에서 **Edit(**편집**)**를 클릭합니다.

단계 **3** 개체 이름을 최대 128자로 입력합니다.

단계 **4** IKEv1 속성을 구성합니다.

- **Priority(**우선순위**)**—IKE 정책의 상대 우선 순위는 1~65,535입니다. 우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다. 원격 IPsec 피어는 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그 다음 우선 순위에 정의된 파라미터 사용을 시도합니다. 번호가 낮을수록 우선 순위가 높습니다.
- **Encryption(**암호화**)** - 2단계 협상 보호를 위한 1단계 SA(보안 연계)를 설정하는 데 사용되는 암호화 알고리즘입니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정을 참조하십시오.
- **Diffie-Hellman Group(Diffie-Hellman** 그룹**)** - 공유 암호를 각 IPsec 피어에 전송하지 않고 두 IPsec 피어 간에 파생하는 데 사용할 Diffie Hellman 그룹입니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. 옵션에 대한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정을 참조하십시오.
- **Lifetime(**라이프타임**)**—SA(보안 연결)의 라이프타임(초)으로, 120~2147483647의 값이거나 비어 있습니다. 라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 특정 지점까지는 라이프타임이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연계를 더 빠르게 설정할 수 있습니다. 기본값은 86400입니다. 무제한 라이프타임을 지정하려면 아무 값도 입력하지 않고 필드를 비워 둡니다.
- **Authentication(**인증**)** - 두 피어 간에 사용할 인증 방법입니다. 자세한 내용은 사용할 인증 방법 결정을 참조하십시오.
  - **Preshared Key(**사전 공유 키**)** - 각 디바이스에 정의된 사전 공유 키를 사용합니다. 이 키를 사용하면 보안 키를 두 피어 간에 공유할 수 있으며 인증 단계 수행 시 IKE에서 보안 키를 사용할 수 있습니다. 동일한 사전 공유 키를 사용하여 피어를 구성하지 않으면 IKE SA를 설정할 수 없습니다.
  - **Certificate(**인증서**)** - 서로 식별할 피어에 대해 디바이스 ID 인증서를 사용합니다. Certificate Authority에서 각 피어를 등록하여 이 인증서를 가져와야 합니다. 또한 각 피어에서 ID 인증서 서명에 사용되는 신뢰할 수 있는 CA 루트 및 중간 CA 인증서를 업로드해야 합니다. 피어는 동일한 또는 다른 CA에 등록할 수 있습니다. 어느 피어든 간에 SSC(자가서명 인증서)를 사용할 수 없습니다.
- **Hash(**해시**)** - 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하기 위한 해시 알고리즘입니다. 옵션에 대한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정을 참조하십시오.

단계 **5** **Add(**추가**)**를 클릭합니다.

## IKEv2 정책 관리

IKEv2 정책을 생성하고 편집하는 방법을 설명합니다.

### IKEv2 정책 정보

IKE(Internet Key Exchange) 버전 2 정책 개체에는 VPN 연결을 정의할 때 IKEv2 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv2 정책이 있습니다. 필요에 맞는 정책이 있으면 State(상태) 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

**Related Topics**

IKEv2 정책 생성 또는 편집, 254 페이지

## *IKEv2* 정책 생성 또는 편집

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKEv2 Policy(새 IKEv2 정책 생성)** 링크를 클릭하여 사이트 간 VPN 연결에서 IKE 설정을 편집하면서 IKEv2 정책을 생성할 수도 있습니다.

---

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 파란색 더하기  버튼을 클릭하고 **FTD > IKEv2 Policy(IKEv2 정책)**를 선택하여 새 IKEv2 정책을 생성합니다.
- 개체 페이지에서 수정할 IKEv2 정책을 선택하고 오른쪽의 Actions(작업) 창에서 **Edit(편집)**를 클릭합니다.

단계 **3** 개체 이름을 최대 128자로 입력합니다.

단계 **4** IKEv2 속성을 구성합니다.

- **Priority(우선순위)**—IKE 정책의 상대 우선 순위는 1~65,535입니다. 우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다. 원격 IPsec 피어는 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그 다음 우선 순위에 정의된 파라미터 사용을 시도합니다. 번호가 낮을수록 우선 순위가 높습니다.
- **State(상태)** - IKE 정책이 활성화되어 있는지 여부입니다. 토글을 클릭하여 상태를 변경합니다. IKE 협상 중에는 활성화된 정책만 사용됩니다.
- **Encryption(암호화)** - 2단계 협상 보호를 위한 1단계 SA(보안 연계)를 설정하는 데 사용되는 암호화 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 단, 같은 정책에 혼합 모드(AES-GCM) 및 일반 모드 옵션을 둘 다 포함할 수는 없습니다. 일반 모드에서는 무결성 해시를 선택해야 하는 반면 혼합 모드에서는 개별 무결성 해시 선택이 금지됩니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정을 참조하십시오.
- **Diffie-Hellman Group(Diffie-Hellman 그룹)** - 공유 암호를 각 IPsec 피어에 전송하지 않고 두 IPsec 피어 간에 파생하는 데 사용할 Diffie Hellman 그룹입니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 그룹에서 가장 취약한 그룹 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정을 참조하십시오.
- **Integrity Hash(무결성 해시)** - 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하기 위한 해시 알고리즘의 무결성 부분입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. AES-GCM 암호

화 옵션에서는 무결성 해시가 사용되지 않습니다. 옵션에 대한 설명은 사용할 해시 알고리즘 결정을 참조하십시오.

- **PRF(Pseudo-Random Function)** 해시 - 해시 알고리즘의 PRF(Pseudo Random Function) 부분으로, IKEv2 터널 암호화에 필요한 키 요소 및 해싱 작업을 파생시키기 위해 알고리즘으로 사용됩니다. IKEv1에서는 무결성 및 PRF 알고리즘이 구분되지 않지만 IKEv2에서는 이러한 요소에 대해 서로 다른 알고리즘을 지정할 수 있습니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 해시 알고리즘 결정을 참조하십시오.
- **Lifetime(**라이프타임**)**—SA(보안 연결)의 라이프타임(초)으로, 120~2147483647의 값이거나 비어 있습니다. 라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 특정 지점까지는 라이프타임이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연계를 더 빠르게 설정할 수 있습니다. 기본값은 86400입니다. 무제한 라이프타임을 지정하려면 아무 값도 입력하지 않고 필드를 비워 둡니다.

단계 **5** **Add(**추가**)**를 클릭합니다.

## IPsec 제안 구성

IPsec는 가장 안전하게 VPN 설정을 하는 방법 중 하나입니다. IPsec는 IP 패킷 레벨에서 데이터 암호화 기능을 제공하는 강력한 표준 기반 솔루션입니다. IPsec를 사용하는 경우 데이터는 터널을 통해 공용 네트워크를 사용하여 전송됩니다. 터널은 두 피어 간의 안전한 논리적 통신 경로입니다. IPsec 터널로 진입하는 트래픽은 보안 프로토콜 및 알고리즘이 조합된 변환 집합에 의해 보호됩니다. IPsec 보안 연계(SA) 협상 중에 피어는 두 피어에서 동일한 변환 집합을 검색합니다.

IKE 버전(IKEv1 또는 IKEv2)에 따라 각기 다른 IPsec 제안 개체가 있습니다.

- IKEv1 IPsec 제안을 생성할 때는 IPsec가 동작하는 모드를 선택하고 필요한 암호화 및 인증 유형을 정의합니다. 알고리즘에 대해서는 단일 옵션을 선택할 수 있습니다. VPN에서 여러 조합을 지원하려면 여러 IKEv1 IPsec 제안 개체를 생성하여 선택합니다.
- IKEv2 IPsec 제안을 생성할 때는 VPN에서 허용되는 모든 암호화 및 해시 알고리즘을 선택할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 일치하는 항목을 찾을 때까지 피어와 협상합니다. 이를 통해 IKEv1과 마찬가지로 허용된 각 조합을 개별적으로 전송하는 대신 모든 허용된 조합을 전달하는 단일 제안서를 보낼 수 있습니다.

IKEv1 및 IKEv2 IPsec 제안에는 모두 ESP(Encapsulating Security Protocol)가 사용됩니다. ESP는 인증, 암호화 및 재생 방지 서비스를 제공합니다. ESP는 IP 프로토콜 유형 50입니다.

**Note** IPsec 터널에서는 암호화 및 인증을 모두 사용하는 것이 좋습니다.

다음 항목에서는 각 IKE 버전에 대해 IPsec 제안을 구성하는 방법을 설명합니다.

- IKEv1 IPsec 제안 개체 관리

- IKEv2 IPsec 제안 개체 관리

## IKEv1 IPsec 제안 개체 관리

IPsec 제안 개체는 IKE 2단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다. IKEv1과 IKEv2용으로 별도의 개체가 있습니다. 현재 CDO(Cisco Defense Orchestrator)는 IKEv1 IPsec 제안 개체를 지원합니다.

IKEv1 및 IKEv2 IPsec 제안에는 모두 ESP(Encapsulating Security Protocol)가 사용됩니다. ESP는 인증, 암호화 및 재생 방지 서비스를 제공합니다. ESP는 IP 프로토콜 유형 50입니다.

**Note** IPsec 터널에서는 암호화 및 인증을 모두 사용하는 것이 좋습니다.

**Related Topics**

IKEv1 IPsec 제안 개체 생성 또는 편집, 256 페이지

### *IKEv1 IPsec* 제안 개체 생성 또는 편집

여러 가지 사전 정의된 IKEv1 IPsec 제안이 있습니다. 새 제안을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 편집하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 편집할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKEv1 Proposal(**새 **IKEv1** 제안 생성**)** 링크를 클릭하여 사이트 투 사이트 VPN 연결에서 IKEv1 IPsec 설정을 편집하면서 IKEv1 IPsec 제안 개체를 생성할 수도 있습니다.

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > FDM Objects(FDM** 개체**)**을 클릭합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 파란색 플러스 버튼  을 클릭하고 **FDM** > **IKEv1 IPsec Proposal(IKEv1 IPsec** 제안**)**을 선택하여 새 개체를 생성합니다.
- 개체 페이지에서 편집할 IPsec 제안을 선택하고 오른쪽의 작업 창에서 **Edit(**편집**)**를 클릭합니다.

단계 **3** 새 개체의 개체 이름을 입력합니다.

단계 **4** IKEv1 IPsec 제안 개체가 작동하는 모드를 선택합니다.

- 터널 모드에서는 전체 IP 패킷이 캡슐화됩니다. IPSec 헤더는 원본 IP 헤더와 새 IP 헤더 사이에 추가됩니다. 이는 기본값입니다. 방화벽 뒤에 배치되어 있는 호스트와 주고받는 트래픽을 방화벽이 보호하는 경우 터널 모드를 사용합니다. 터널 모드는 인터넷 등의 신뢰할 수 없는 네트워크를 통해 연결하는 두 방화벽 또는 기타 보안 게이트웨이 간에 일반 IPsec이 구현되는 통상적인 방식입니다.
- 전송 모드에서는 IP 패킷의 상위 레이어 프로토콜만 캡슐화됩니다. IPSec 헤더는 TCP 등의 상위 계층 프로토콜 헤더와 IP 헤더 사이에 삽입됩니다. 전송 모드에서는 소스 호스트와 대상 호스트가 모두 IPsec를 지원해야 합니다. 터널의 대상 피어가 IP 패킷의 최종 대상인 경우에만 전송 모드를 사용할 수 있습니다. 전송 모드는 대개 GRE, L2TP, DLSW 등의 레이어 2 또는 레이어 3 터널링 프로토콜을 보호할 때만 사용됩니다.

단계 **5** 이 제안에 대한 **ESP Encryption(ESP** 암호화**)**(Encapsulating Security Protocol) 알고리즘을 선택합니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정을 참조하십시오.

단계 **6** 인증에 사용할 **ESP Hash(ESP** 해시**)** 또는 무결성 알고리즘을 선택합니다. 옵션에 대한 설명은 사용할 해시 알고리즘 결정을 참조하십시오.

단계 **7** **Add(**추가**)**를 클릭합니다.

## IKEv2 IPsec 제안 개체 관리

IPsec 제안 개체는 IKE 2단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다.

IKEv2 IPsec 제안을 생성할 때는 VPN에서 허용되는 모든 암호화 및 해시 알고리즘을 선택할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 일치하는 항목을 찾을 때까지 피어와 협상합니다. 이를 통해 IKEv1과 마찬가지로 허용된 각 조합을 개별적으로 전송하는 대신 모든 허용된 조합을 전달하는 단일 제안서를 보낼 수 있습니다.

### Related Topics

IKEv2 IPsec 제안 개체 생성 또는 편집, 257 페이지

### *IKEv2 IPsec* 제안 개체 생성 또는 편집

여러 가지 사전 정의된 IKEv2 IPsec 제안이 있습니다. 새 제안을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 편집하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 편집할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 Create New IPsec Proposal(새 IPsec 제안 생성) 링크를 클릭하여 VPN 연결에서 IKEv2 IPsec 설정을 편집하면서 IKEv2 IPsec 제안 개체를 생성할 수도 있습니다.

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > FDM Objects(FDM** 개체**)**을 클릭합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 파란색 플러스 버튼  을 클릭하고 **FDM** > **IKEv2 IPsec Proposal(IKEv2 IPsec** 제안**)**을 선택하여 새 개체를 생성합니다.
- 개체 페이지에서 편집할 IPsec 제안을 선택하고 오른쪽의 작업 창에서 **Edit(**편집**)**를 클릭합니다.

단계 **3** 새 개체의 개체 이름을 입력합니다.

단계 **4** IKE2 IPsec 제안 개체 구성:

- **Encryption(**암호화**)** - 이 제안에 대한 ESP(Encapsulating Security Protocol) 암호화 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정을 참조하십시오.

- **Integrity Hash(무결성 해시)** - 인증에 사용할 해시 또는 무결성 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 해시 알고리즘 결정을 참조하십시오.

단계 **5** **Add(추가)**를 클릭합니다.

## ASA 사이트 간 가상 사설망 모니터링

CDO를 사용하면 온보딩된 ASA 디바이스에서 이미 존재하는 사이트 간 VPN 구성을 모니터링할 수 있습니다. 사이트 간 구성을 수정하거나 삭제할 수 없습니다.

### 사이트 투 사이트 VPN 터널 연결 확인

**Check Connectivity(연결 확인)** 버튼을 사용하여 터널에 대한 실시간 연결 확인을 트리거하여 터널이 현재 사이트 간 VPN 터널 검색 및 필터링인지를 식별합니다. 온디맨드 연결 확인 버튼을 클릭하지 않으면 온보딩된 모든 디바이스에서 사용 가능한 모든 터널의 확인이 1시간에 한 번 수행됩니다.

**Note**

- CDO는 ASA에서 이 연결성 검사 명령을 실행하여 터널이 활성 상태인지 유휴 상태인지를 확인합니다.

  ```
  show vpn-sessiondb l2l sort ipaddress
  ```

- 모델 ASA 디바이스 터널은 항상 유휴로 표시됩니다.

VPN 페이지에서 터널 연결을 확인하려면 다음을 수행합니다.

단계 **1** 기본 탐색 모음에서 VPN > ASA/FDM Site-to-Site VPN를 클릭합니다.

단계 **2** 사이트 투 사이트 VPN 터널에 대한 터널 목록을 사이트 간 VPN 터널 검색 및 필터링하고 선택합니다.

단계 **3** 오른쪽의 작업 창에서 **Check Connectivity(연결 확인)**를 클릭합니다.

### VPN 문제 식별

CDO는 ASA에서 VPN 문제를 식별할 수 있습니다. (이 기능은 아직 AWS VPC 사이트 투 사이트 VPN 터널에 사용할 수 없습니다.) 이 문서에서는 다음을 설명합니다.

- 누락된 피어가 있는 VPN 터널 찾기
- 암호화 키 문제가 있는 VPN 피어 찾기
- 터널에 대해 정의된 불완전하거나 잘못 구성된 액세스 목록 찾기
- 터널 구성에서 문제 찾기

터널 구성 문제 해결, on page 260

## 누락된 피어가 있는 *VPN* 터널 찾기

"Missing IP Peer" 상태는 FDM 관리 디바이스보다 ASA 디바이스에서 발생할 가능성이 높습니다.

단계 **1** CDO 탐색 창에서 **VPN** > **ASA/FDM Site-to-Site VPN(ASA/FDM** 사이트 간 **VPN)**을 클릭하여 VPN 페이지를 엽니다.

단계 **2** **Table View(**테이블 보기**)**를 선택합니다.

단계 **3** 필터 아이콘 을 클릭하여 필터 패널을 엽니다.

단계 **4** 감지된 문제를 확인합니다.

단계 **5** 문제 를 보고하는 각 디바이스를 선택하고 오른쪽의 Peers(피어) 창을 확인합니다. 하나의 피어 이름이 나열됩니다. CDO는 다른 피어 이름을 "[Missing peer IP.]"로 보고합니다.

## 암호화 키 문제가 있는 *VPN* 피어 찾기

이 접근 방식을 사용하여 다음과 같은 암호화 키 문제가 있는 VPN 피어를 찾습니다.

- IKEv1 또는 IKEv2 키가 잘못되었거나 누락되었거나 일치하지 않습니다.
- 사용되지 않거나 낮은 암호화 터널

단계 **1** CDO 탐색 모음에서 **VPN** > **ASA/FDM Site-to-Site VPN(ASA/FDM** 사이트 간 **VPN)**을 클릭하여 VPN 페이지를 엽니다.

단계 **2** **Table View(**테이블 보기**)**를 선택합니다.

단계 **3** 필터 아이콘 을 클릭하여 필터 패널을 엽니다.

단계 **4** 문제 를 보고하는 각 디바이스를 선택하고 오른쪽의 Peers(피어) 창을 확인합니다. 피어 정보에는 두 피어가 모두 표시됩니다.

단계 **5** 디바이스 중 하나에 대해 **View Peers(**피어 보기**)**를 클릭합니다.

단계 **6** Diagram View(다이어그램 보기)에서 문제를 보고하는 디바이스를 두 번 클릭합니다.

단계 **7** 하단의 Tunnel Details(터널 세부 정보) 창에서 **Key Exchange(**키 교환**)**를 클릭합니다. 두 디바이스를 모두 보고 해당 지점에서 주요 문제를 진단할 수 있습니다.

## 터널에 대해 정의된 불완전하거나 잘못 구성된 액세스 목록 찾기

"불완전하거나 잘못 구성된 액세스 목록" 상태는 ASA 디바이스에서만 발생할 수 있습니다.

단계 **1** CDO 탐색 모음에서 **VPN** > **ASA/FDM Site-to-Site VPN(ASA/FDM** 사이트 간 **VPN)**을 클릭하여 VPN 페이지를 엽니다.

단계 **2** **Table View(**테이블 보기**)**를 선택합니다.

단계 **3** 필터 아이콘 을 클릭하여 필터 패널을 엽니다.

단계 4 문제 ⚠를 보고하는 각 디바이스를 선택하고 오른쪽의 Peers(피어) 창을 확인합니다. 피어 정보에는 두 피어가 모두 표시됩니다.

단계 5 디바이스 중 하나에 대해 **View Peers(**피어 보기**)**를 클릭합니다.

단계 6 Diagram View(다이어그램 보기)에서 문제를 보고하는 디바이스를 두 번 클릭합니다.

단계 7 하단의 Tunnel Details(터널 세부 정보) 패널에서 **Tunnel Details(**터널 세부 정보**)**를 클릭합니다. "Network Policy: Incomplete(네트워크 정책: 완료되지 않음)" 메시지가 표시됩니다.

---

터널 구성에서 문제 찾기

터널 구성 오류는 다음 시나리오에서 발생할 수 있습니다.

- 사이트 투 사이트 VPN 인터페이스의 IP 주소가 변경되면 "피어 IP 주소 값이 변경되었습니다."
- VPN 터널의 IKE 값이 다른 VPN 터널과 일치하지 않으면 "IKE 값 불일치" 메시지가 나타납니다.

---

단계 1 CDO 탐색 모음에서 **VPN** > **ASA/FDM Site-to-Site VPN(ASA/FDM** 사이트 간 **VPN)**을 클릭하여 VPN 페이지를 엽니다.

단계 2 **Table View(**테이블 보기**)**를 선택합니다.

단계 3 필터 아이콘을 클릭하여 필터 패널을 엽니다.

단계 4 터널 문제에서 탐지된 문제를 클릭하여 오류를 보고하는 VPN 구성을 봅니다. 구성 보고 문제 ⚠를 볼 수 있습니다.

단계 5 VPN 구성 보고 문제를 선택합니다.

단계 6 오른쪽의 피어 창에 문제가 있는 피어에 대한 ⚠ 아이콘이 나타납니다. ⚠ 아이콘 위로 마우스를 가져가면 문제와 해결 방법을 볼 수 있습니다.

다음 단계: 터널 구성 문제 해결.

---

터널 구성 문제 해결

이 절차는 다음과 같은 터널 구성 문제를 해결하려고 시도합니다.

- 사이트 투 사이트 VPN 인터페이스의 IP 주소가 변경되면 "피어 IP 주소 값이 변경되었습니다."
- VPN 터널의 IKE 값이 다른 VPN 터널과 일치하지 않으면 "IKE 값 불일치" 메시지가 나타납니다.

자세한 내용은 터널 구성에서 문제 찾기를 참조하십시오.

---

단계 1 CDO 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 2 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 3 적절한 디바이스 유형 탭을 클릭하고 문제를 보고하는 VPN 구성과 연결된 디바이스를 선택합니다.

단계 4 "충돌 탐지됨" 상태 해결

단계 **5** CDO 탐색 창에서 **VPN** > **ASA/FDM Site-to-Site VPN(ASA/FDM** 사이트 간 **VPN)**을 클릭하여 VPN 페이지를 엽니다.

단계 **6** 이 문제를 보고하는 VPN 구성을 선택합니다.

단계 **7** **Actions(**작업**)**창에서 **Edit**(편집) 아이콘을 클릭합니다.

단계 **8** 4단계에서 **Finish(**마침**)** 버튼을 클릭할 때까지 각 단계에서 **Next(**다음**)**를 클릭합니다.

단계 **9** 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, 352 페이지.

---

## 사이트 간 **VPN** 터널 검색 및 필터링

필터 사이드바를 검색 필드와 함께 사용하여 VPN 터널 다이어그램에 표시된 VPN 터널 검색에 집중할 수 있습니다.

---

단계 **1** 기본 내비게이션 바에서 **VPN > ASA/FDM Site-to-Site VPN(ASA/FDM** 사이트 간 **VPN)**으로 이동합니다.

단계 **2** 필터 아이콘을 클릭하여 필터 창을 엽니다.

단계 **3** 다음 필터를 사용하여 검색을 구체화합니다.

- **Filter by Device(**디바이스별 필터링**) - Filter by Device(**디바이스별 필터링**)**를 클릭하고 디바이스 유형 탭을 선택한 후 필터링을 통해 찾으려는 디바이스를 선택합니다.
- **Tunnel Issues(**터널 문제**)** - 터널의 양쪽에 문제가 있음을 탐지했는지 여부입니다. 디바이스에 문제가 있는 몇 가지 예로는 연결된 인터페이스 또는 피어 IP 주소 또는 액세스 목록 누락, IKEv1 제안 불일치 등이 있습니다(AWS VPC VPN 터널에서는 터널 문제 탐지를 아직 사용할 수 없음).
- **Devices/Services(**디바이스/서비스**)** -디바이스 유형을 기준으로 필터링합니다.
- **Status(**상태**)** – 터널 상태는 활성 또는 유휴 상태일 수 있습니다.
  - **Active(**활성**)** - 네트워크 패킷이 VPN 터널을 통과하는 열린 세션이 있거나 성공적인 세션이 설정되었고 아직 시간 초과되지 않았습니다. Active(활성)는 터널이 활성 상태이고 관련성이 있음을 나타내는 데 도움이 될 수 있습니다.
  - **Idle(**유휴**)** - CDO가 이 터널에 대한 열린 세션을 검색할 수 없습니다. 터널이 사용 중이 아니거나 이 터널에 문제가 있을 수 있습니다.
- **Onboarded(**온보딩됨**)** - CDO에서 디바이스를 관리하거나 CDO에서 관리하지 않을 수 있습니다(관리되지 않음).
  - 관리됨 – CDO가 관리하는 디바이스별로 필터링합니다.
  - 관리되지 않음 - CDO가 관리하지 않는 디바이스로 필터링합니다.
- **Device Types(**디바이스 유형**)** - 터널의 한쪽이 라이브(연결된 디바이스) 디바이스인지 아니면 모델 디바이스인지 여부입니다.

단계 4 검색 창에 디바이스 이름 또는 IP 주소를 입력하여 필터링된 결과를 검색할 수도 있습니다. 검색은 대/소문자를 구분하지 않습니다.

---

관리되지 않는 디바이스 온보딩

CDO는 피어 중 하나가 온보딩될 때 사이트 간 VPN 터널을 검색 합니다. 두 번째 피어가 CDO에서 관리되지 않는 경우 VPN 터널 목록을 필터링하여 관리되지 않는 디바이스를 찾아 온보딩할 수 있습니다.

---

단계 1 기본 내비게이션 바에서 **VPN** > **ASA/FDM Site-to-Site VPN(ASA/FDM** 사이트 간 **VPN)**을 선택하여 VPN 페이지를 엽니다.

단계 2 **Table View(**테이블 보기**)**를 선택합니다.

단계 3 를 클릭하여 필터 패널을 엽니다.

단계 4 **Unmanaged(**관리되지 않음**)**를 선택합니다.

단계 5 결과의 테이블에서 터널을 선택합니다.

단계 6 오른쪽의 **Peers(**피어**)** 창에서 **Onboard Device(**온보드 디바이스**)**를 클릭하고 화면의 지침을 따릅니다.

---

관련 정보**:**

- 디바이스 및 서비스 온보딩, on page 149
- ASA 디바이스 온보딩, on page 149

사이트 투 사이트 **VPN** 터널의 **IKE** 개체 세부 정보 보기

선택한 터널의 피어/디바이스에 구성된 IKE 개체의 세부 정보를 볼 수 있습니다. 이러한 세부 정보는 IKE 정책 개체의 우선 순위에 따라 계층 구조의 트리 구조로 나타납니다.

**Note** 엑스트라넷 디바이스는 IKE 개체 세부 정보를 표시하지 않습니다.

---

단계 1 왼쪽의 CDO 탐색 모음에서 **VPN > ASA/FDM Site-to-Site VPN(ASA/FDM** 사이트 간 **VPN)**를 클릭합니다.

단계 2 **VPN Tunnels(VPN** 터널**)** 페이지에서 피어를 연결하는 VPN 터널의 이름을 클릭합니다.

단계 3 오른쪽의 **Relationships(**관계**)** 아래에 세부 정보를 보려는 개체를 확장합니다.

---

마지막으로 성공한 사이트 투 사이트 **VPN** 터널 설정 날짜 보기

---

단계 1 사이트 간 VPN 터널 정보 보기.

단계 2 **Tunnel Details(**터널 세부 정보**)** 창를 클릭합니다.

단계 3 **Last Seen Active(**마지막 확인한 활성**)** 필드를 확인합니다.

## 사이트 간 VPN 터널 정보 보기

사이트 간 VPN 테이블 보기는 CDO에 온보딩된 모든 디바이스에서 사용 가능한 모든 사이트 간 VPN 터널의 전체 목록입니다. 터널은 이 목록에 한 번만 존재합니다. 테이블에 나열된 터널을 클릭하면 추가 조사를 위해 터널의 피어로 직접 이동할 수 있는 옵션이 오른쪽 사이드바에 제공됩니다.

CDO가 터널의 양쪽을 모두 관리하지 않는 경우 관리되지 않는 디바이스 온보딩를 클릭하여 언매니지드 피어의 온보드 기본 온보딩 페이지를 열 수 있습니다. CDO가 터널의 양쪽을 모두 관리하는 경우 Peer 2(피어 2) 열에 매니지드 디바이스의 이름이 포함됩니다. 그러나 AWS VPC의 경우 Peer 2 열에 VPN 게이트웨이의 IP 주소가 포함됩니다.

테이블 보기에서 사이트 간 VPN 연결을 보려면 다음을 수행합니다.

단계 1 기본 탐색 모음에서 **VPN > ASA/FDM Site-to-Site VPN**를 클릭합니다.

단계 2 **Table view(**테이블 보기**)** 버튼을 클릭합니다.

단계 3 사이트 간 VPN 터널 검색 및 필터링를 사용하여 특정 터널을 찾거나 전역 보기 그래픽을 확대하여 원하는 VPN 게이트웨이 및 해당 피어를 찾습니다.

## 사이트 투 사이트 *VPN* 전역 보기

단계 1 기본 탐색 모음에서 **VPN > ASA/FDM Site-to-Site VPN**를 클릭합니다.

단계 2 **Global view(**전역 보기**)** 버튼을 클릭합니다.

단계 3 사이트 간 VPN 터널 검색 및 필터링를 사용하여 특정 터널을 찾거나 전역 보기 그래픽을 확대하여 원하는 VPN 게이트웨이 및 해당 피어를 찾습니다.

단계 4 전역 보기에 표시된 피어 중 하나를 선택합니다.

단계 5 **View Details(**세부사항 보기**)**를 클릭합니다.

단계 6 VPN 터널의 다른 쪽 끝을 클릭하면 CDO에 해당 연결에 대한 Tunnel Details(터널 세부 정보), NAT Information(NAT 정보) 및 Key Exchange(키 교환) 정보가 표시됩니다.

- **Tunnel Details(**터널 세부 정보**)** - 터널에 대한 이름 및 연결 정보를 표시합니다. Refresh(새로 고침) 아이콘을 클릭하면 터널에 대한 연결 정보가 업데이트됩니다.
- **Tunnel Details specific to AWS connections(AWS** 연결 관련 터널 세부 정보**)** -AWS 사이트 투 사이트 연결에 대한 터널 세부 정보는 다른 연결과 약간 다릅니다. AWS VPC에서 VPN 게이트웨이로의 각 연결에 대해 AWS는 2개의 VPN 터널을 생성합니다. 이는 고가용성을 위한 것입니다.
  - 터널의 이름은 VPN 게이트웨이가 연결된 VPC의 이름을 나타냅니다. 터널에 이름이 지정된 IP 주소는 VPN 게이트웨이가 VPC로 인식하는 IP 주소입니다.
  - CDO 연결 상태가 "active(활성)"로 표시되면 AWS 터널 상태가 "Up(가동 중)"입니다. CDO 연결 상태가 "inactive(비활성)"인 경우 AWS 터널 상태는 "Down(중단)"입니다.

- **NAT Information(NAT** 정보**)** - 사용 중인 NAT 규칙의 유형, 원래 및 변환된 패킷 정보를 표시하고, 해당 터널에 대한 NAT 규칙을 볼 수 있는 NAT 테이블에 대한 링크를 제공합니다. (AWS VPC 사이트 투 사이트 VPN에는 아직 사용할 수 없습니다.)
- **Key Exchange(**키 교환**)** - 터널 및 키 교환 문제에서 사용 중인 암호화 키를 표시합니다. (AWS VPC 사이트 투 사이트 VPN에는 아직 사용할 수 없습니다.)

터널 창

Tunnels(터널) 창에는 특정 VPN 게이트웨이와 연결된 모든 터널의 목록이 표시됩니다. VPN 게이트웨이와 AWS VPC 간의 사이트 간 VPN 연결의 경우, tunnels(터널) 창에는 VPN 게이트웨이에서 VPC로의 모든 터널이 표시됩니다. VPN 게이트웨이와 AWS VPC 간의 각 사이트 간 VPN 연결에는 2개의 터널이 있으므로 다른 디바이스에 대해 일반적으로 표시되는 터널 수가 두 배입니다.

**VPN** 게이트웨이 세부 정보

VPN 게이트웨이에 연결된 피어의 수 및 VPN 게이트웨이의 IP 주소를 표시합니다. 이는 VPN Tunnels(VPN 터널) 페이지에만 표시됩니다.

피어 창

사이트 간 VPN 피어 쌍을 선택하면 Peers(피어) 창에 쌍의 두 디바이스가 나열되며 디바이스 중 하나에 대해 **View Peers(**피어 보기**)**를 클릭할 수 있습니다. **View Peers(**피어 보기**)**를 클릭하면 디바이스가 연결된 다른 사이트 간 피어가 표시됩니다. 이는 Table(테이블) 보기 및 Global(전역) 보기에 표시됩니다.

# 원격 액세스 가상 프라이빗 네트워크

RA VPN(원격 액세스 VPN)을 사용하면 개별 사용자가 인터넷에 연결된 컴퓨터 또는 기타 지원되는 iOS 또는 Android 디바이스를 사용하여 원격 위치에서 네트워크에 연결할 수 있습니다. 따라서 모바일 근무자가 홈 네트워크 또는 공개 Wi-Fi 네트워크 등에서 연결할 수 있습니다.

RA VPN 구성은 다음 구성 요소로 구성됩니다.

- 연결 프로파일: 홈 네트워크 등의 외부 네트워크에 있는 사용자가 내부 네트워크에 연결할 수 있도록 원격 액세스 VPN 연결 프로파일을 생성할 수 있습니다. 다른 인증 방법을 수용하기 위해 별도 프로파일을 생성합니다. 연결 프로파일은 ID 소스와 그룹 정책으로 구성됩니다.

관련 정보**:**

- ASA에 대한 원격 액세스 VPN 구성, on page 270

## 원격 액세스 가상 프라이빗 네트워크 세션

RA VPN(Remote Access Virtual Private Network)은 모바일 사용자 또는 재택 근무자와 같은 원격 사용자에게 보안 연결을 제공합니다. 이러한 연결을 모니터링하면 연결 및 사용자 세션 성능에 대한 중요

한 지표를 얻을 수 있습니다. Cisco Defense Orchestrator (CDO) RA VPN 모니터링 기능을 통해 원격 액세스 VPN 문제가 있는지 여부와 존재 여부를 신속하게 확인할 수 있습니다. 그런 다음 이 정보를 적용하고 네트워크 관리 도구를 사용하여 네트워크 및 사용자의 문제를 줄이거나 없앨 수 있습니다. 필요에 따라 원격 액세스 VPN 세션의 연결을 끊을 수도 있습니다.

Remote Access Virtual Private Monitoring(원격 액세스 가상 프라이빗 모니터링) 페이지는 다음 정보를 제공합니다.

- 지난 90일 동안의 활성 세션 및 기록 세션 목록입니다.
- CDO에서 관리하는 모든 활성 VPN 헤드엔드의 보기를 한눈에 볼 수 있도록 직관적인 그래픽 시각적 개체를 표시합니다.
- 라이브 세션 화면에는 CDO 테넌트에서 가장 많이 사용되는 운영 체제 및 VPN 연결 프로파일이 표시됩니다. 또한 평균 세션 기간과 업로드 및 다운로드한 데이터도 표시됩니다.
- 디바이스 유형, 디바이스 이름, 세션 길이, 전송 및 수신된 데이터의 양과 같은 기준을 기반으로 검색 범위를 좁힐 수 있는 필터링 기능입니다.

관련 정보:

- 라이브 AnyConnect 원격 액세스 VPN 세션 모니터링, on page 265
- 기록 AnyConnect RA VPN 세션 모니터링, on page 267
- RA VPN 세션 검색 및 필터링
- RA VPN 모니터링 보기 사용자 지정
- RA VPN 세션을 CSV 파일로 내보내기
- 사용자의 모든 활성 RA VPN 세션 연결 끊기

## 라이브 AnyConnect 원격 액세스 VPN 세션 모니터링

디바이스의 활성 AnyConnect RA VPN 세션에서 실시간 데이터를 모니터링할 수 있습니다. 이 데이터는 10분마다 자동으로 새로 고쳐집니다. 언제든지 최신 세션 목록을 검색하려면 화면 오른쪽 모서리에 나타나는 다시 로드 아이콘 을 클릭하십시오.

시작하기 전에

- RA VPN 헤드 엔드를 CDO에 온보딩합니다.
- 라이브 데이터를 모니터링하려는 디바이스의 연결 상태는 **Inventory(**인벤토리**)** 페이지에서 "Online(온라인)"인지 확인합니다.

---

단계 **1** CDO 탐색 창에서 **VPN** > **Remote Access VPN Monitoring(VPN** 원격 액세스 **VPN** 모니터링**)**을 클릭합니다.

또는 CDO 홈 페이지에서 **View Active Remote Access VPN Sessions(**활성 원격 액세스 **VPN** 세션 보기**)**를 클릭하거나 **VPN** > **Remote Access VPN(**원격 액세스 **VPN)**으로 이동하여 화면 오른쪽 상단 모서리에 있는 아이콘을 클릭할 수 있습니다.

단계 **2** **RA VPN**을 클릭합니다.

단계 **3** **Live(**라이브**)**를 클릭합니다.

RA VPN 세션 검색 및 필터링하여 디바이스 유형, 세션 길이, 업로드 및 다운로드 데이터 범위와 같은 기준에 따라 검색 범위를 좁힐 수 있습니다.

참고 데이터 **TX** 및 데이터 **RX** 정보는 FTD에서 사용할 수 없습니다.

---

## 라이브 데이터 보기

라이브 데이터는 대시보드 및 테이블 형식으로 표시됩니다.

### **Dashboard(**대시보드**)** 보기

대시보드를 보려면 화면의 오른쪽 상단 모서리에 나타나는 **Show Charts View(**차트 보기 표시**)** 아이콘을 클릭해야 합니다.

대시보드는 CDO에서 관리하는 모든 활성 VPN 헤드엔드의 보기를 한눈에 확인할 수 있도록 제공합니다.

- **Breakdown (All Devices)(**애널리틱스 데이터**(**모든 디바이스**))**: 총 라이브 세션 수를 표시합니다. 4개의 호 길이로 구분된 원도표도 표시됩니다. 세션 수가 가장 많은 상위 3개 디바이스의 VPN 세션 비율을 보여줍니다. 나머지 호 길이는 다른 디바이스의 어그리게이션를 나타냅니다.
- CDO 테넌트에서 가장 많이 사용되는 운영 체제 및 연결 프로파일이 표시됩니다.
- 평균 세션 기간과 업로드 및 다운로드한 데이터도 표시됩니다.
- **Active Sessions by Country(**국가별 활성 세션**)**: RA VPN 헤드엔드에 연결된 사용자 위치의 인터랙티브 히트맵을 표시합니다.
  - 사용자가 연결한 국가는 해당 국가에서 설정된 세션의 상대적 비율에 따라 점점 더 짙은 파란색 음영으로 표시됩니다. 파란색이 어두울수록 해당 국가에서 더 많은 세션이 설정되었음을 의미합니다.
  - 맵의 맨 아래에 있는 범례는 국가의 세션 수와 국가를 표시하는 데 사용되는 파란색 음영 간의 상관관계를 나타내는 척도를 제공합니다.
  - 맵에 마우스 포인터를 올려놓으면 해당 국가의 이름 및 해당 국가에서 설정된 총 활성 사용자 세션 수를 확인할 수 있습니다.
  - 테이블 위에 마우스 포인터를 올려놓으면 해당 국가의 위치와 맵의 총 활성 사용자 세션 수를 확인할 수 있습니다.

### 테이블 형식 보기

데이터를 테이블 형식으로 보려면 화면의 오른쪽 상단 모서리에 있는 **Show Tabular View(**테이블 형식 보기 표시**)** 아이콘을 클릭합니다.

테이블 형식은 현재 연결된 VPN 사용자의 전체 목록을 제공합니다.

- **Location(**위치**)** 열에는 공용 IP 주소를 지리위치 지정하여 VPN 헤드엔드에 연결된 모든 사용자의 위치가 표시됩니다. 사용자 상세정보를 보려면 행을 클릭합니다. 왼쪽 창의 위치 링크를 클릭하면 사용자의 위치가 Google 맵에 표시됩니다.

중요 CDO는 라이브 데이터에 표준 필터를 적용하고 대시보드에 표시합니다. 사용자 지정 필터는 시각적 대시보드 보기에서 지원되지 않으므로, 테이블 형식 데이터가 표시되는 경우에만 새 필터를 적용할 수 있습니다. 적용한 모든 필터를 제거하려면 **Clear(**지우기**)**를 클릭합니다. 표준 필터는 제거할 수 없습니다.

RA VPN 세션 검색 및 필터링 기능을 사용하여 디바이스 유형, 세션 길이, 업로드 및 다운로드 데이터 범위와 같은 기준에 따라 검색 범위를 좁힐 수 있습니다. 한 번에 최대 10,000개의 결과를 표시할 수 있습니다.

Status(상태) 열에 **Active(**활성**)** 레이블이 있는 녹색 점은 활성 VPN 사용자의 세션을 나타냅니다.

## 기록 AnyConnect RA VPN 세션 모니터링

지난 3개월 동안 기록된 AnyConnect RA VPN 세션의 기록 데이터를 모니터링할 수 있습니다.

시작하기 전에

- RA VPN 헤드 엔드를 CDO에 온보딩합니다.

단계 **1** CDO 탐색 창에서 **VPN** > **Remote Access VPN Monitoring(VPN** 원격 액세스 **VPN** 모니터링**)**을 클릭합니다.

또는 CDO 홈 페이지에서 **View Active Remote Access VPN Sessions(**활성 원격 액세스 **VPN** 세션 보기**)**를 클릭하거나 **VPN** > **Remote Access VPN(VPN** 원격 액세스 **VPN)**으로 이동하여 오른쪽 상단 모서리에 있는 아이콘 을 클릭할 수 있습니다.

단계 **2** **RA VPN**을 클릭합니다.

단계 **3** **Historical(**기록**)**을 클릭합니다.

CDO는 지난 3개월 동안 기록된 RA VPN 세션의 기록 데이터를 표시합니다.

RA VPN 세션 검색 및 필터링 기능을 사용하여 디바이스 유형, 세션 길이, 업로드 및 다운로드 데이터 범위와 같은 기준에 따라 검색 범위를 좁힐 수 있습니다.

데이터 **TX** 및 데이터 **RX** 정보는 FTD에서 사용할 수 없습니다.

## 이력 데이터 보기

이력 데이터는 대시보드 및 표 형식으로 표시됩니다.

**Dashboard(**대시보드**)** 보기

대시보드를 보려면 화면의 오른쪽 상단에 나타나는 **Show Charts View(**차트 보기 표시**)** 아이콘을 클릭해야 합니다. 테이블 보기와 함께 대시보드 보기가 표시됩니다.

대시보드는 CDO에서 관리하는 모든 활성 VPN 헤드엔드의 보기를 한눈에 볼 수 있도록 제공합니다. 지난 24시간, 7일 및 30일 동안 모든 디바이스에 대해 기록된 VPN 세션을 보여주는 막대 그래프를 제공합니다. 드롭다운에서 기간을 선택할 수 있습니다. 개별 막대에 마우스 커서를 대면 해당 날짜의 총 세션 수와 날짜를 확인할 수 있습니다.

테이블 형식 보기

대시보드를 보려면 화면의 오른쪽 상단에 나타나는 **Show Tabular View(**테이블 형식 보기 표시**)** 아이콘을 클릭하여 테이블 형식 보기만 표시해야 합니다. 테이블 형식은 지난 3개월 동안 연결된 VPN 사용자의 전체 목록을 제공합니다.

**Location(**위치**)** 열에는 공용 IP 주소를 지리위치 지정하여 VPN 헤드엔드에 연결된 모든 사용자의 위치가 표시됩니다. 사용자 상세정보를 보려면 행을 클릭합니다. 왼쪽 창의 위치 링크를 클릭하면 사용자의 위치가 Google 맵에 표시됩니다.

중요 CDO는 기록 데이터에 표준 필터를 적용하고 대시보드에 표시합니다. 대시보드는 맞춤형 필터를 지원하지 않으므로 테이블 형식 데이터가 표시되는 경우에만 새 필터를 적용할 수 있습니다. 새로 적용된 필터를 지우면 대시보드가 다시 실행됩니다. 화면에서 **Clear(**지우기**)**를 클릭하여 수동으로 적용된 필터를 제거합니다. 표준 필터는 제거할 수 없습니다.

RA VPN 세션 검색 및 필터링 기능을 사용하여 세션 날짜와 시간 범위, 세션 길이, 업로드 및 다운로드 데이터 범위와 같은 기준에 따라 검색 범위를 좁힐 수 있습니다. 한 번에 최대 10,000개의 결과를 표시할 수 있습니다.

Status(상태) 열에 **Active(**활성**)** 레이블이 있는 녹색 점은 활성 VPN 사용자의 세션을 나타냅니다.

## RA VPN 세션 검색 및 필터링

검색

검색 창 기능을 사용하여 RA VPN 세션을 찾습니다. 검색 창에 디바이스 이름, IP 주소 또는 일련 번호를 입력하기 시작합니다. 그러면 검색 기준에 맞는 RA VPN 세션이 표시됩니다. 검색은 대/소문자를 구분하지 않습니다.

필터

필터 사이드바를 사용하여 세션 시간 범위, 세션 길이, 업로드 및 다운로드 데이터 범위 등의 기준에 따라 RA VPN 세션을 찾습니다. 필터 기능은 라이브 보기와 기록 보기 모두에서 사용할 수 있습니다.

- **Filter by Devices(**디바이스별 필터링**)**: **All Types(**모든 유형**)** 탭에서 하나 또는 모든 디바이스를 선택하여 선택한 디바이스의 세션을 봅니다. 창은 또한 유형에 따라 디바이스를 분류하고 해당 탭 아래에 표시합니다.

- **Sessions Time Range(**세션 시간 범위**)**(기록 데이터에만 적용 가능): 지정된 날짜 및 시간 범위의 기록 세션을 표시합니다. 지난 3개월 동안 기록된 데이터를 볼 수 있습니다.
- **Sessions Length(**세션 길이**)**: 지정된 세션의 기간 길이를 기준으로 세션을 표시합니다. 시간 단위(시간, 분 또는 초)를 설정하고 슬라이더를 이동하여 최소 및 최대 기간 길이를 지정합니다. 제공된 필드에 길이를 지정할 수도 있습니다.
- **Upload (TX)(**업로드**(TX))**: 보안 네트워크에 업로드되거나 전송된 데이터의 지정된 양을 기준으로 세션을 표시합니다. 단위(GB, MB 또는 KB)를 설정하고 그에 따라 슬라이더를 이동하여 범위를 선택합니다. 사용 가능한 필드에 값을 지정할 수도 있습니다.
- **Download (RX)(**다운로드**(RX))**: 보안 네트워크에서 다운로드하거나 수신한 지정된 데이터 양을 기준으로 세션을 표시합니다. 단위(GB, MB 또는 KB)를 설정하고 그에 따라 슬라이더를 이동하여 범위를 선택합니다. 사용 가능한 필드에 값을 지정할 수도 있습니다.

### **RA VPN** 모니터링 보기 사용자 지정

원하는 보기에 적용되는 열 헤더만 포함하도록 라이브 및 기록 모드에서 RA VPN 모니터링 보기를 편집할 수 있습니다. 열 오른쪽에 있는 열 필터 아이콘 ≡ 을 클릭하고 원하는 열을 선택하거나 선택 취소합니다.

CDO는 다음에 CDO에 로그인할 때 선택 항목을 기억합니다.

### **RA VPN** 세션을 **CSV** 파일로 내보내기

하나 이상의 디바이스의 RA VPN 세션을 쉼표로 구분된 값(.csv) 파일로 내보낼 수 있습니다. Microsoft Excel과 같은 스프레드시트 애플리케이션에서 .csv 파일을 열어 목록의 항목을 정렬하고 필터링할 수 있습니다. 이 정보는 RA VPN 세션을 분석하는 데 도움이 됩니다. 세션을 내보낼 때마다 CDO는 새 .csv 파일을 생성합니다. 생성된 파일에는 이름에 날짜와 시간이 포함되어 있습니다.

CDO는 최대 100,000개의 활성 세션을 CSV 파일로 내보낼 수 있습니다. 모든 디바이스의 총 세션 수가 최대 제한을 초과하는 경우 **View By Device(**디바이스별 보기**)** 필터를 사용하여 개별 디바이스에 대한 보고서를 생성할 수 있습니다.

---

단계 **1** CDO 탐색 창에서 **VPN** > **Remote Access VPN Monitoring(VPN** 원격 액세스 **VPN** 모니터링**)**을 클릭합니다.

단계 **2** **View By Devices(**디바이스별 보기**)** 영역에서 다음 중 하나를 선택합니다.

- **All Devices(**모든 디바이스**)** - 그 아래에 나열된 모든 디바이스에서 활성 세션을 내보냅니다.
- 해당 디바이스의 세션을 내보낼 디바이스를 클릭합니다.

단계 **3** 오른쪽 상단 모서리에 있는 ⏻ 아이콘을 클릭합니다. CDO는 화면에 표시되는 규칙을 .csv 파일로 내보냅니다.

단계 **4** 스프레드시트 애플리케이션에서 .csv 파일을 열어 결과를 정렬하고 필터링합니다.

---

### ASA 사용자의 활성 RA VPN 세션 연결 끊기

ASA 디바이스에서 모든 사용자의 모든 활성 RA VPN 세션을 종료할 수 있습니다. 라이브 모드와 기록 모드 모두에서 이 작업을 수행할 수 있습니다.

CDO는 사용자가 VPN 세션을 보고 종료할 수 있도록 VPN 세션 관리자 사용자 역할을 제공합니다. 자세한 내용은 Cisco Defense Orchestrator의 사용자 역할을 참조하십시오.

---

단계 1 CDO 탐색 창에서 **VPN** > **Remote Access VPN Monitoring(VPN** 원격 액세스 **VPN** 모니터링**)**을 클릭합니다.

단계 2 디바이스별 보기 영역에서 해당 디바이스의 모든 활성 세션을 종료하려는 ASA 디바이스를 클릭합니다.

단계 3 오른쪽 상단에 나타나는 **Terminate All Sessions(**모든 세션 종료**)**를 클릭합니다.

단계 4 **Yes, Terminate All Sessions(**예**,** 모든 세션을 종료합니다**)**를 클릭하여 선택을 확인합니다.

---

### 사용자의 모든 활성 *RA VPN* 세션 연결 끊기

사용자의 연결을 끊으면 CDO는 해당 ASA 디바이스에서 사용자의 모든 활성 RA VPN 세션을 종료합니다. 라이브 모드와 기록 모드 모두에서 이 작업을 수행할 수 있습니다.

---

단계 1 CDO 탐색 창에서 **VPN** > **Remote Access VPN Monitoring(VPN** 원격 액세스 **VPN** 모니터링**)**을 클릭합니다.

단계 2 세션의 연결을 끊을 사용자를 검색합니다. **Search(**검색**)** 막대에 검색 기준을 입력할 수 있습니다.

단계 3 활성 세션을 클릭하고 오른쪽의 **Actions(**작업**)** 창에서 **Terminate all RA VPN sessions for this user(**이 사용자에 대한 모든 **RA VPN** 세션 종료**)** 링크를 클릭합니다.

---

## ASA에 대한 원격 액세스 VPN 구성

ASASecure Firewall Cloud Native에서는 사용자에게 비공개 연결로 표시되는 TCP/IP 네트워크(예를 들어 인터넷)를 통해 보안 연결을 생성하여 VPN(Virtual Private Network)을 생성합니다. 단일 사용자-LAN(single-user-to-LAN) 연결 및 LAN-to-LAN 연결을 만들 수 있습니다.

보안 연결을 터널이라고 하며, ASA에서는 터널링 프로토콜을 사용하여 보안 파라미터를 협상하고, 터널을 생성하고 관리하며, 패킷을 캡슐화하고, 터널을 통해 패킷을 전송하거나 수신하고, 패킷의 캡슐화를 해제합니다. ASA에서는 양방향 터널 엔드포인트로서의 기능을 수행합니다. 플레인 패킷을 수신하고, 이를 캡슐화한 다음, 해당 패킷의 캡슐화가 해제되고 최종 대상으로 전송되는 터널의 다른 쪽 끝에 패킷을 전송합니다. ASA에서는 캡슐화된 패킷을 수신하고 해당 패킷의 캡슐화를 해제한 후 이를 최종 대상으로 전송할 수도 있습니다.

CDO는 새로운 RA VPN(Remote Access Virtual Private Network)을 구성하기 위한 직관적인 사용자 인터페이스를 제공합니다. 또한 CDO에 온보딩된 여러 ASA(Adaptive Security Appliance) 디바이스에 대한 RA VPN 연결을 쉽고 빠르게 구성할 수 있습니다.

CDO를 사용하면 ASA 디바이스에서 RA VPN 구성을 처음부터 구성할 수 있습니다. 또한 ASDM(Adaptive Security Defense Manager) 또는 CSM(Cisco Security Manager)과 같은 다른 ASA 관리 도구를 사용하여 이미 구성된 RA VPN 설정을 관리할 수 있습니다. 이미 RA VPN 설정이 있는 ASA 디바이스를 온보딩하는 경우 CDO는 자동으로 "기본 RA VPN 구성"을 생성하고 ASA 디바이스를 이

구성과 연결합니다. 이 기본 구성은 디바이스에 정의된 모든 연결 프로파일 개체를 포함할 수 있습니다. CDO로 읽히는 RAVPN 속성을 이해하려면 온보딩된 ASA 디바이스의 RA VPN 구성 읽기 섹션을 참조하십시오. 그렇지 않으면 "ASA에 대한 엔드 투 엔드 원격 액세스 VPN 구성 프로세스" 섹션에 설명된 단계를 수행할 수 있습니다.

관련 정보:

- ASA에 대한 엔드 투 엔드 원격 액세스 VPN 구성 프로세스
  - ASA에 대한 ID 소스 구성
    - ASA Active Directory 영역 개체 생성 또는 편집
    - ASA RADIUS 서버 개체 또는 그룹 생성 또는 편집
  - 새 ASA RA VPN 그룹 정책 생성, on page 277
  - ASA RA VPN 구성 생성, on page 285
  - ASA RA VPN 연결 프로파일 구성, on page 289
- 온보딩된 ASA 디바이스의 RA VPN 구성 읽기
- IP 주소 풀 생성
- NAT에서 원격 액세스 트래픽 제외, on page 305
- ASA의 원격 액세스 VPN 구성 확인
- ASA의 원격 액세스 VPN 구성 세부 정보 보기

## ASA에 대한 엔드 투 엔드 원격 액세스 VPN 구성 프로세스

이 섹션에서는 CDO에 온보딩된 ASA 디바이스에서 RA VPN(Remote Access Virtual Private Network)을 구성하는 엔드 투 엔드 절차를 제공합니다.

클라이언트에 대한 원격 액세스 VPN을 활성화하려면 여러 개의 개별 항목을 구성해야 합니다. 다음 절차에서는 이러한 엔드 투 엔드 프로세스를 제공합니다.

---

단계 **1** 원격 사용자 인증에 사용되는 ID 소스를 구성합니다. 자세한 내용은 ASA에 대한 ID 소스 구성을 참조하십시오.

다음 소스를 사용하여 RA VPN을 사용하여 네트워크에 연결을 시도하는 사용자를 인증할 수 있습니다. 또한 인증을 위해 클라이언트 인증서를 단독으로 또는 ID 소스와 함께 사용할 수 있습니다.

- AD(Active Directory) ID 영역: 기본 인증 소스로 사용됩니다. AD(Active Directory) 서버에서 사용자 어카운트가 정의됩니다. AD ID 영역 구성을 참조하십시오. ASA Active Directory 영역 개체 생성 또는 편집을 참조하십시오.
- RADIUS 서버 그룹: 기본 또는 보조 인증 소스로서, 권한 부여 및 계정 관리를 위한 것입니다. ASA RADIUS 서버 개체 또는 그룹 생성 또는 편집을 참조하십시오.
- Local Identity Source(로컬 사용자 데이터베이스): 기본 또는 대체 소스로 사용됩니다. 외부 서버를 사용하지 않고 디바이스에서 직접 사용자를 정의할 수 있습니다. 로컬 데이터베이스를 대체 소스로 사용하는 경우 외부 서

버에 설명한 것과 같은 사용자 이름/비밀번호를 정의해야 합니다. 참고: ASDM(Adaptive Security Device Manager)에서만 ASA 디바이스에서 직접 사용자 계정을 생성할 수 있습니다. Cisco ASA Series Firewall ASDM 구성 가이드, XY의 개체 액세스 제어" 장에서 "로컬 사용자 그룹 구성" 섹션을 참조하십시오.

단계 **2** (선택 사항) 새 ASA RA VPN 그룹 정책 생성, on page 277. 그룹 정책에서는 사용자와 관련된 속성을 정의합니다. 그룹 멤버십에 근거하여 리소스에 차등 액세스를 제공하도록 그룹 정책을 구성할 수 있습니다. 또는 모든 연결에 기본 정책을 사용합니다.

단계 **3** ASA RA VPN 구성 생성, on page 285.

단계 **4** ASA RA VPN 연결 프로파일 구성, on page 289.

단계 **5** (선택 사항) NAT에서 원격 액세스 트래픽 제외, on page 305.

단계 **6** CDO에서 ASA로 구성 변경 사항 구축.

**Important** ASDM(Adaptive Security Device Manager)과 같은 로컬 관리자를 사용하여 원격 액세스 VPN 구성을 변경하면 CDO에서 해당 디바이스의 구성 상태가 "Conflict Detected(충돌 탐지됨)"로 표시됩니다. 디바이스의 대역 외 변경 사항을 참조하십시오. 이 ASA에서 구성 충돌 해결할 수 있습니다.

---

### What to do next

다음 단계

RA VPN 구성이 ASA 디바이스에 다운로드되면 사용자는 인터넷에 연결된 컴퓨터 또는 기타 지원되는 iOS 또는 Android 디바이스를 사용하여 원격 위치에서 네트워크에 연결할 수 있습니다. 테넌트의 모든 온보딩된 ASA RA VPN 헤드엔드에서 라이브 AnyConnect RA VPN(Remote Access RA VPN) 세션을 모니터링할 수 있습니다. 원격 액세스 가상 프라이빗 네트워크 세션을 참조하십시오.

## *ASA*에 대한 *ID* 소스 구성

Microsoft Active Directory(AD) 영역 및 RADIUS 서버와 같은 ID 소스는 조직 내 사용자의 사용자 계정을 정의하는 AAA 서버 및 데이터베이스입니다. IP 주소와 연결된 사용자 ID를 제공하거나 원격 액세스 VPN 연결 또는 CDO에 대한 액세스를 인증하는 등 다양한 방법으로 이 정보를 사용할 수 있습니다.

**Objects(**개체**) > FTD Network Objects(FTD** 네트워크 개체**)**를 클릭한 다음 (  )>**Identity Source(ID** 소스**)**를클릭하여 소스를 생성합니다. 그런 다음, ID 소스가 필요한 서비스를 구성할 때 이러한 개체를 사용할 수 있습니다. 적절한 필터를 적용하여 기존 소스를 검색하고 관리할 수 있습니다.

### 디렉터리 기본 DN 결정

디렉터리 속성을 구성할 때는 사용자와 그룹에 대한 공통 기본 DN(고유 이름)을 지정해야 합니다. 이 기준은 디렉터리 서버에서 정의되며 네트워크마다 다릅니다. 올바른 기준을 입력해야 ID 정책이 실행됩니다. 기준이 잘못된 경우 시스템이 사용자 또는 그룹 이름을 확인할 수 없으므로 ID 기반 정책이 실행될 수 없습니다.

**Note** 올바른 기준을 가져오려면 디렉터리 서버 담당 관리자에게 문의하십시오.

Active Directory의 경우 도메인 관리자로 Active Directory 서버에 로그인하여 다음과 같이 명령 프롬프트에 **dsquery** 명령을 사용해 기준을 확인하여 올바른 기준을 확인할 수 있습니다.

사용자 검색 기준

알려진 사용자 이름(부분 또는 전체)을 포함한 **dsquery user** 명령을 입력하여 기본 고유 이름을 확인합니다. 예를 들어 다음 명령은 부분 이름 "John*"를 사용하여 "John"으로 시작되는 모든 사용자에 대한 정보를 반환합니다.

**C:\Users\Administrator>dsquery user -name "John*"**

**"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"**

이 경우 기본 DN은 "DC=csc-lab,DC=example,DC=com"이 됩니다.

그룹 검색 기준

알려진 그룹 이름을 포함한 **dsquery group** 명령을 입력하여 기본 고유 이름을 확인합니다. 예를 들어 다음 명령은 그룹 이름 Employees를 사용하여 고유 이름을 반환합니다.

**C:\>dsquery group -name "Employees"**

**"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"**

이 경우 그룹 기본 DN은 “DC=csc-lab,DC=example,DC=com”이 됩니다.

ADSI 편집 프로그램을 사용하여 Active Directory 구조를 찾을 수도 있습니다(**Start(**시작**)** > **Run(**실행**)** > **adsiedit.msc**). ADSI 편집에서 조직 단위(OU), 그룹, 사용자 등의 개체를 마우스 오른쪽 단추로 클릭하고 **Properties(**속성**)**를 선택하여 고유 이름을 확인합니다. 그러면 DC 값 문자열을 기준으로 복사할 수 있습니다.

기준이 올바른지를 확인하려면 다음 단계를 수행합니다.

단계 **1** 디렉터리 속성의 Test Connection(연결 테스트) 버튼을 클릭하여 연결을 확인합니다. 모든 문제를 해결하고 디렉터리 속성을 저장합니다.

단계 **2** 디바이스에 변경 사항을 커밋합니다.

단계 **3** 액세스 규칙을 생성하고 **Users(**사용자**)** 탭을 선택한 다음 디렉터리에서 알려진 사용자 및 그룹 이름을 추가해 봅니다. 디렉터리가 포함된 영역에서 일치하는 사용자 및 그룹을 입력하면 자동 완성 제안 사항이 표시됩니다. 이러한 제안 사항이 드롭다운 목록에 표시되는 경우 시스템이 디렉터리를 정상적으로 쿼리한 것입니다. 입력한 문자열이 사용자 또는 그룹 이름에 포함되어 있는데 제안 사항이 표시되지 않으면 해당하는 검색 기준을 편집해야 합니다.

### What to do next

자세한 내용은 ASA Active Directory 영역 개체 생성 또는 편집을 참조하십시오.

RADIUS 서버 및 그룹

RADIUS 서버를 사용하여 관리 사용자를 인증하고 권한을 부여할 수 있습니다. RADIUS 서버를 사용하도록 기능을 구성할 때는 개별 서버 대신 RADIUS 그룹을 선택합니다. RADIUS 그룹은 서로의 복사본인 RADIUS 서버가 모인 컬렉션입니다. 그룹에 서버가 여러 개 포함된 경우 이러한 서버는 백업 서버 체인을 형성하여 한 서버를 사용할 수 없는 경우 이중화를 제공합니다. 하지만 서버가 하나뿐이더라도 멤버가 하나인 그룹을 생성하여 기능에 대한 RADIUS 지원을 구성해야 합니다.

이 소스는 다음과 같은 목적으로 사용할 수 있습니다.

- 인증용 ID 소스이자 권한 부여 및 과금 용도의 원격 액세스 VPN. AD를 RADIUS 서버와 함께 사용할 수 있습니다.
- ID 정책(원격 액세스 VPN 로그인에서 사용자 ID를 수집하기 위한 패시브 ID 소스로 사용)

자세한 내용은 ASA RADIUS 서버 개체 또는 그룹 생성 또는 편집을 참조하십시오.

## ASA Active Directory 영역 개체 생성 또는 편집

AD 영역 개체와 같은 ID 소스 개체를 생성하거나 편집할 때 CDO는 SDC를 통해 ASA 디바이스에 구성 요청을 보냅니다. 그런 다음 ASA는 구성된 AD 영역과 통신합니다.

개체를 생성하려면 다음 절차를 따르십시오.

---

단계 **1** 좌측의 CDO 탐색 모음에서 **Objects(**개체**) > ASA Objects(ASA** 개체**)**를 클릭합니다.

단계 **2** **Create Object(**개체 생성**)** (+) **RA VPN Objects(**개체**) (ASA & FDM) > Identity Source(ID** 소스**)**를 클릭합니다.

단계 **3** 개체의 **Object name(**개체 이름**)**을 입력합니다.

단계 **4** **Device Type(**장치 유형**)**을 **ASA**로 선택합니다.

단계 **5** 마법사의 첫 번째 부분에서 **ID** 소스 유형으로 **Active Directory** 영역을 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **6** 기본 영역 속성을 구성합니다.

- 디렉터리 사용자 이름**,** 디렉터리 암호- 검색하려는 사용자 정보에 대한 적절한 권한이 있는 사용자의 고유한 사용자 이름과 암호입니다. Active Directory의 경우에는 사용자에게 상승된 권한이 필요하지 않습니다. 도메인에 어떤 사용자라도 지정할 수 있습니다. 사용자 이름은 정규화되어야 합니다. 예를 들어 Administrator@example.com(단순히 Administrator가 아님)입니다.

  참고 시스템은 이 정보에서 ldap-login-dn 및 ldap-login-password를 생성합니다. 예를 들어 Administrator@example.com은 cn=administrator,cn=users,dc=example,dc=com으로 변환됩니다. cn=users는 항상 이 변환의 일부이므로 여기에서 일반 이름 "users" 폴더 아래에 지정하는 사용자를 구성해야 합니다.

- **Base Distinguished Name(**기본 고유 이름**)** - 사용자 및 그룹 정보를 검색하거나 조회하기 위한 디렉토리 트리, 즉 사용자 및 그룹의 공통 상위. cn=users,dc=example,dc=com을 예로 들 수 있습니다.

단계 **7** 디렉터리 서버 속성을 구성합니다.

- **Hostname/IP Address(**호스트 이름**/IP** 주소**)** - 디렉터리 서버의 호스트 이름 또는 IP 주소입니다. 서버에 대한 암호화된 연결을 사용하는 경우에는 IP 주소가 아닌 FQDN(Fully-Qualified Domain Name)을 입력해야 합니다.

- **Port(포트)** - 서버와의 통신에 사용되는 포트 번호입니다. 기본값은 389입니다. 암호화 방법으로 LDAPS를 선택하는 경우에는 포트 636을 사용합니다.
- 암호화- 사용자 및 그룹 정보를 다운로드하기 위해 암호화된 연결을 사용하려면 **LDAPS**를 선택하여 SSL을 사용하여 ASA와 LDAP 서버 간의 통신을 보호합니다. SSL을 통한 LDAP가 필요합니다. 이 옵션은 포트 636을 사용합니다.

  기본값은 **None(없음)**입니다. 이 옵션은 사용자 및 그룹 정보를 일반 텍스트로 다운로드함을 의미합니다.

단계 **8** (선택 사항) **Test(테스트)** 버튼을 사용하여 구성을 확인합니다.

단계 **9** (선택 사항) AD(Active Directory) 영역에 여러 AD 서버를 추가하려면 **Add another configuration(다른 구성 추가)**를 클릭합니다. 이 AD 서버들은 서로의 중복이어야 하고 동일한 AD 도메인을 지원해야 합니다. 따라서 디렉터리 이름, 디렉터리 암호 및 기본 고유 이름과 같은 기본 영역 속성은 해당 AD 영역과 연결된 모든 AD 서버에서 동일해야 합니다.

단계 **10** **Add(추가)**를 클릭합니다.

---

ASA Active Directory 영역 개체 편집

ID 소스 개체를 편집할 때는 ID 소스 유형을 변경할 수 없습니다. 올바른 유형으로 새 개체를 생성해야 합니다.

---

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(개체) > ASA Objects(ASA 개체)**을 클릭합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.

단계 **3** 편집할 개체를 선택합니다.

단계 **4** 세부정보 패널의 **Actions(작업)** 창에서 편집 아이콘  를 클릭합니다.

단계 **5** 위의 절차에서 만든 것과 같은 방식으로 대화 상자에서 값을 편집합니다. 아래 나열된 구성 표시줄을 확장하여 호스트 이름/IP 주소 또는 암호화 정보를 편집하거나 테스트합니다.

단계 **6** **Save(저장)**를 클릭합니다.

단계 **7** CDO에 변경의 영향을 받을 정책이 표시됩니다. **Confirm(확인)**을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

단계 **8** 지금 변경 사항을 CDO에서 ASA로 구성 변경 사항 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

---

ASA RADIUS 서버 개체 또는 그룹 생성 또는 편집

RADIUS 서버 개체 또는 RADIUS 서버 개체 그룹과 같은 ID 소스 개체를 생성하거나 편집할 때 CDO는 SDC를 통해 구성 요청을 ASA 디바이스로 보냅니다.

RADIUS 서버 개체 생성

RADIUS 서버는 AAA(인증, 권한 부여 및 계정 관리) 서비스를 제공합니다.

개체를 생성하려면 다음 절차를 따르십시오.

단계 1 좌측의 CDO 탐색 모음에서 **Objects(**개체**) > ASA Objects(ASA** 개체**)**를 클릭합니다.

단계 2 **Create Object(**개체 생성**)** (  )**> RA VPN Objects(**개체**) (ASA & FDM) > Identity Source(ID** 소스**)**를 클릭합니다.

단계 3 개체의 **Object name(**개체 이름**)**을 입력합니다.

단계 4 **Device Type(**장치 유형**)**을 **ASA**로 선택합니다.

단계 5 **ID** 소스 유형으로 **RADIUS Server Group(RADIUS** 서버 그룹**)** 을 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 6 다음 속성을 사용하여 ID 소스 구성을 편집합니다.

- **Server Name or IP Address(**서버 이름 또는 **IP** 주소**)** - 서버의 정규화된 호스트 이름(FQDN) 또는 IP 주소입니다.
- **Authentication Port(**인증 포트**)**(선택 사항) - RADIUS 인증 및 권한 부여가 수행되는 포트입니다. 기본값은 1,812입니다.
- **Timeout(**시간 제한**)** - 시스템이 다음 서버로 요청을 보내기 전까지 서버의 응답을 기다리는 시간(1~300초)입니다. 기본값은 10초입니다.
- **Server Secret Key(**서버 비밀 키**)**입력(선택 사항) - ASA 디바이스와 RADIUS 서버 간에 데이터를 암호화하는 데 사용되는 공유 비밀입니다. 이 키는 대/소문자를 구분하며 공백은 포함하지 않는 영숫자 문자열(최대 64자)입니다. 또한 영숫자 문자 또는 밑줄로 시작해야 하며 특수 문자 $ & - _ . + @는 포함할 수 없습니다. 문자열은 RADIUS 서버에 구성된 것과 일치해야 합니다. 비밀 키를 구성하지 않으면 연결이 암호화되지 않습니다.

단계 7 **Add(**추가**)**를 클릭합니다.

단계 8 지금 변경 사항을 CDO에서 ASA로 구성 변경 사항 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

RADIUS 서버 그룹 생성

RADIUS 서버 그룹은 하나 이상의 RADIUS 서버 개체를 포함합니다. 그룹 내의 서버는 서로의 복사본이어야 합니다. 이러한 서버는 백업 서버 체인을 형성하므로 첫 번째 서버를 사용할 수 없는 경우 시스템이 목록의 다음 서버 사용을 시도할 수 있습니다.

개체 그룹을 생성하려면 다음 절차를 따르십시오.

단계 1 좌측의 CDO 탐색 모음에서 **Objects(**개체**) > ASA Objects(ASA** 개체**)**를 클릭합니다.

단계 2 **Create Object(**개체 생성**)** (  ) **RA VPN Objects(**개체**) (ASA & FDM)Identity Source(ID** 소스**)**를 클릭합니다.

단계 3 개체의 **Object name(**개체 이름**)**을 입력합니다.

단계 4 **Device Type(**장치 유형**)**을 **ASA**로 선택합니다.

단계 5 ID 소스 유형으로 **RADIUS Server (RADIUS** 서버**) Group(**그룹**)**을 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 6 다음 속성을 사용하여 ID 소스 구성을 편집합니다.

- 데드 타임 - 실패한 서버는 모든 서버가 실패한 후에만 재활성화됩니다. 데드 시간은 모든 서버를 다시 활성화하기 전에 마지막 서버가 실패한 후 대기하는 시간입니다.

- **Maximum Failed Attempts(**최대 실패 시도 횟수**)** - 다음 서버 사용을 시도하기 전에 그룹의 RADIUS 서버로 전송되었으나 실패한 요청(즉, 응답을 받지 못한 요청)의 수입니다. 최대 실패 시도 횟수가 초과되면 시스템에서 해당 서버를 Failed(장애 발생)로 표시합니다. 특정 기능에 대해 로컬 데이터베이스를 사용하여 대체 방법을 구성했는데 그룹의 모든 서버가 응답하지 않으면 해당 그룹은 응답이 없는 것으로 간주되고 대체 방법을 시도합니다. 서버 그룹은 데드 타임 동안 응답하지 않는 것으로 표시된 상태를 유지하므로 해당 기간 내의 추가 AAA 요청은 서버 그룹에 연결을 시도하지 않으며 폴백 방법이 즉시 사용됩니다.
- **Dynamic Authorization/Port(**동적 인증/포트**) (**선택사항**) -** RADIUS 동적 인증 또는 이 RADIUS 서버 그룹에 대한 CoA(Change of Authorization) 서비스를 활성화할 경우, 해당 그룹은 CoA 알림이 등록되며 Cisco ISE(Identity Services Engine)의 CoA 정책 업데이트를 위해 지정된 포트를 수신합니다. ISE와 함께 원격 액세스 VPN에서 이 서버 그룹을 사용하는 경우에만 동적 인증을 활성화합니다.

단계 **7** 드롭다운 메뉴에서 RADIUS 서버를 지원하는 AD 영역을 선택합니다. AD 영역을 아직 생성하지 않은 경우 드롭다운 메뉴에서 **Create(**생성**)**를 클릭합니다.

단계 **8** 기존 RADIUS 서버 개체를 추가하려면 **RADIUS SERVER Add(RADIUS** 서버 추가**)**  버튼을 클릭합니다. 선택 사항으로 이 창에서 새 RADIUS 서버 개체를 만들 수 있습니다.

**Note** 목록의 첫 번째 서버가 응답하지 않을 때까지 사용되므로 이러한 개체를 우선 순위에 추가하십시오. 그런 다음 ASA는 목록의 다음 서버로 기본 설정됩니다.

단계 **9** 지금 변경 사항을 CDO에서 ASA로 구성 변경 사항 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

---

RADIUS 서버 개체 또는 그룹 편집

Radius 서버 개체 또는 Radius 서버 그룹을 편집하려면 다음 절차를 따르십시오.

---

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.

단계 **3** 편집할 개체를 선택합니다.

단계 **4** 세부정보 패널의 **Actions(**작업**)** 창에서 편집 아이콘  를 클릭합니다.

단계 **5** 위의 절차에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 편집합니다. 호스트 이름/IP 주소 또는 암호화 정보를 편집하거나 테스트하려면 구성 표시줄을 확장합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

단계 **7** CDO에 변경의 영향을 받을 정책이 표시됩니다. **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

단계 **8** 지금 변경 사항을 CDO에서 ASA로 구성 변경 사항 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

---

새 *ASA RA VPN* 그룹 정책 생성

그룹 정책은 원격 액세스 VPN 연결을 위한 사용자 중심 속성/값 쌍의 집합입니다. 연결 프로파일은 터널이 설정된 이후에 사용자 연결을 위한 조건을 설정하는 그룹 정책을 사용합니다. 그룹 정책을 사

용하면 각 사용자에 대해 개별적으로 각 특성을 지정할 필요 없이 사용자 또는 사용자 그룹에 전체 특성 집합을 적용할 수 있습니다.

시스템에는 "DfltGrpPolicy"라는 이름의 기본 그룹 정책이 포함되어 있습니다. 필요한 서비스를 제공하는 추가 그룹 정책을 만들 수 있습니다.

참고 일치하지 않는 그룹 정책 개체를 RA VPN 구성에 추가할 수 없습니다. RA VPN 구성 그룹 정책을 추가하기 전에 모든 불일치를 해결하십시오.

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > FTD Network Objects(FTD** 네트워크 개체**)**을 클릭합니다.

단계 **2** 파란색 더하기 버튼을 클릭합니다.

단계 **3** **RA VPN Objects (ASA & FTD)(RA VPN** 개체 **(ASA** 및 **FDM) ) > RA VPN Group Policy(RA VPN** 그룹 정책**)**를 클릭합니다.

단계 **4** 그룹 정책의 이름을 입력합니다. 이름은 최대 64자까지 입력할 수 있고 공백이 허용됩니다.

단계 **5** **Device Type(**디바이스 유형**)** 드롭다운에서 **ASA**를 선택합니다.

단계 **6** 다음 중 하나를 수행합니다.

- 필요한 탭을 클릭하고 페이지에서 속성을 구성합니다.
  - ASA RA VPN 그룹 정책 속성
  - AnyConnect 클라이언트 프로파일, 279 페이지
  - 세션 설정 속성, 280 페이지
  - 주소 할당 속성, 280 페이지
  - 스플릿 터널링 속성, 281 페이지
  - AnyConnect 속성, 282 페이지
  - 트래픽 필터 속성, 284 페이지
  - Windows 브라우저 프록시 속성, 284 페이지

단계 **7** **Save(**저장**)**를 클릭하여 그룹 정책을 생성합니다.

## ASA RA VPN 그룹 정책 속성

이 섹션에서는 ASA RA VPN 그룹 정책과 관련된 속성에 대해 설명합니다.

### 일반 속성

그룹 정책의 일반 속성에서는 그룹의 이름 및 기타 기본 설정을 정의합니다.

- **DNS Server(DNS 서버)**: VPN에 연결된 경우 도메인 이름 확인을 위한 DNS 서버의 IP 주소를 입력합니다. 쉼표를 사용하여 주소를 구분할 수 있습니다.
- **Banner(배너)**: 로그인 시 사용자에게 표시할 배너 텍스트 또는 환영 메시지입니다. 기본값은 배너 없음입니다. 길이는 최대 496자까지 가능합니다. AnyConnect 클라이언트에서는 부분 HTML을 지원합니다. 원격 사용자에게 배너가 적절히 표시되게 하려면 <BR> 태그를 사용하여 줄 바꿈을 나타냅니다.
- **Default Domain(기본 도메인)**: RA VPN의 사용자에 대한 기본 도메인 이름입니다. example.com 등을 예로 들 수 있습니다. 이 도메인은 정규화되지 않은 호스트 이름(예: serverA.example.com이 아닌 serverA)에 추가됩니다.

### AnyConnect 클라이언트 프로파일

이 기능은 소프트웨어 버전 6.7 이상을 실행하는 FTD에서 지원됩니다.

Cisco AnyConnect VPN 클라이언트는 다양한 내장 모듈을 통해 향상된 보안을 제공합니다. 이러한 모듈은 웹 보안, 엔드 포인트 플로우에 대한 네트워크 가시성, 네트워크 외부 로밍 보호와 같은 서비스를 제공합니다. 각 클라이언트 모듈에는 요구 사항에 따라 사용자 지정 구성 그룹이 포함된 클라이언트 프로파일이 포함되어 있습니다.

VPN 사용자가 VPN AnyConnect 클라이언트 소프트웨어를 다운로드할 때 클라이언트에 다운로드할 AnyConnect VPN 프로파일 개체 및 AnyConnect 모듈을 선택할 수 있습니다.

1. AnyConnect VPN 프로파일 개체를 선택하거나 생성합니다. RA VPN AnyConnect 클라이언트 프로파일 업로드, on page 308의 내용을 참조하십시오. DART 및 Start Before Login(로그인 전 시작) 모듈을 제외하고 AnyConnect VPN 프로파일 개체를 선택해야 합니다.
2. **Add Any Connect Client Module(모든 연결 클라이언트 모듈 추가)**을 클릭합니다.

   다음 AnyConnect 모듈은 선택 사항이며 이러한 모듈을 VPN AnyConnect 클라이언트 소프트웨어와 함께 다운로드하도록 구성할 수 있습니다.

   - **AMP Enabler** — 엔드포인트용 AMP(Advanced Malware Protection)를 구축합니다.
   - **DART** — 시스템 로그 및 기타 진단 정보를 캡처하여 데스크톱에 .zip 파일을 만듭니다. 따라서 편리하게 Cisco TAC로 문제 해결 정보를 보낼 수 있습니다.
   - **Feedback(피드백)** - 고객이 활성화하고 사용한 기능 및 모듈에 대한 정보를 제공합니다.
   - **ISE Posture**: OPSWAT v3 라이브러리를 사용하여 엔드포인트의 컴플라이언스를 평가하기 위한 상태 확인을 수행합니다.
   - **Network Access Manager** - 802.1X(계층 2)와 유선 및 무선 네트워크에 액세스하기 위한 디바이스 인증을 제공합니다.
   - **Network Visibility(네트워크 가시성)** — 용량 및 서비스 계획, 감사, 컴플라이언스 및 보안 분석을 수행하기 위한 엔터프라이즈 관리자의 역량을 개선합니다.
   - **Start Before Login(로그인 전 시작)** - Windows 로그인 대화 상자가 나타나기 전에 AnyConnect를 시작하여 Windows에 로그온하기 전에 VPN 연결을 통하여 사용자를 엔터프라이즈 인프라에 연결시킵니다.

- **Umbrella** 로밍 보안 — 활성 VPN이 없을 때 DNS 레이어 보안을 제공합니다.
- 웹 보안 - 정의된 보안 정책에 따라 웹 페이지의 요소를 분석하고 허용되는 콘텐츠를 허용하며 악성 또는 허용되지 않는 콘텐츠를 차단합니다.

3. 클라이언트 모듈 목록에서 **AnyConnect** 모듈을 선택합니다.
4. **Profile(**프로파일**)** 목록에서 AnyConnect 클라이언트 프로파일을 포함하는 프로파일 개체를 선택하거나 생성합니다.
5. 프로파일과 함께 클라이언트 모듈을 다운로드하려면 **Enable Module Download(**모듈 다운로드 활성화**)**를 선택하여 엔드포인트를 활성화합니다. 선택하지 않으면 엔드포인트는 클라이언트 프로파일만 다운로드할 수 있습니다.

세션 설정 속성

그룹 정책의 세션 설정에서는 사용자가 VPN을 통해 연결할 수 있는 시간과 설정할 수 있는 별도 연결의 개수를 제어합니다.

- **Maximum Connection Time(**최대 연결 시간**)**: 사용자가 로그아웃했다가 다시 연결하지 않고 VPN에 연결된 상태를 유지할 수 있는 최대 시간을 1~4473924(분)로 입력하거나 비워 둡니다. 기본값은 무제한(비워 둠)이지만 유휴 시간 제한은 계속 적용됩니다.
- **Connection Time Alert Interval(**연결 시간 알림 간격**)**: 최대 연결 시간을 지정하는 경우, 알림 간격에서는 사용자에게 앞으로 다가올 자동 연결 해제에 관해 경고를 표시하기까지 지나야 할 최대 시간을 정의합니다. 사용자는 연결 종료를 선택하고 다시 접속해 타이머를 다시 시작할 수 있습니다. 기본값은 1분입니다. 1분에서 30분까지 지정할 수 있습니다.
- **Idle Time(**유휴 시간**)**: VPN 연결이 자동으로 종료될 때까지 유휴 상태일 수 있는 시간을 1~35791394(분) 범위 내로 입력합니다. 이 연속되는 분 단위 시간 동안 연결에서 통신 활동이 없는 경우, 시스템에서는 연결을 중지합니다. 기본값은 30분입니다.
- **Idle Time Alert Interval(**유휴 시간 알림 간격**)**: 유휴 세션으로 인해 사용자에게 앞으로 다가올 자동 연결 해제에 관해 경고를 표시하기까지 지나야 할 유휴 시간입니다. 어떤 활동에서도 타이머를 재설정할 수 있습니다. 기본값은 1분입니다. 1분에서 30분까지 지정할 수 있습니다.
- **Simultaneous Login Per User(**사용자당 동시 로그인 수**)**: 한 사용자에게 허용되는 동시 연결의 최대 개수입니다. 기본값은 3입니다. 1~2147483647개의 연결을 지정할 수 있습니다. 다수의 동시 연결을 허용하면 보안이 취약해지고 성능이 저하될 수 있습니다.

주소 할당 속성

그룹 정책의 주소 할당 속성에서는 그룹에 대해 IP 주소 풀을 정의합니다. 여기에 정의된 풀은 이 그룹을 사용하는 모든 연결 프로파일에 정의된 풀을 재정의합니다. 연결 프로파일에 정의된 풀을 사용하려면 이러한 설정을 비워둡니다.

- **IPv4 Address Pool(IPv4** 주소 풀**), IPv6 Address Pool(IPv6** 주소 풀**)**: 이 옵션에서는 원격 엔드포인트의 주소 풀을 정의합니다. 클라이언트가 VPN 연결을 설정하는 데 사용하는 IP 버전에 따라 이러한 풀의 주소가 클라이언트에 할당됩니다. 지원하려는 각 IP 유형에 대한 서브넷을 정의하

는 IP 주소 풀을 선택합니다. 해당 IP 버전을 지원하고 싶지 않은 경우, 목록을 비워두십시오. 예를 들어 IPv4 풀을 10.100.10.0/24로 정의할 수 있습니다. 주소 풀은 외부 인터페이스의 IP 주소와 동일한 서브넷에 있을 수 없습니다. 새 IP 주소 풀 생성을 생성합니다. 로컬 주소 할당에 사용할 최대 6개의 주소 풀로 구성된 목록을 지정할 수 있습니다. 풀을 지정하는 순서는 중요합니다. 시스템에서는 풀이 표시되는 순서에 따라 이 풀에서 주소를 할당합니다. 참고: 동일한 그룹 정책에 대해 IPv4 주소 풀과 IPv6 주소 풀을 둘 다 구성할 수 있습니다. 동일한 그룹 정책에 두 버전의 IP 주소가 모두 구성된 경우 IPv4에 대해 구성된 클라이언트는 IPv4 주소를 가져오고 IPv6에 대해 구성된 클라이언트는 IPv6 주소를 가져오며 IPv4 주소와 IPv6 주소 둘 다에 대해 구성된 클라이언트는 IPv4 주소와 IPv6 주소를 둘 다 가져옵니다.

- **DHCP Scope(DHCP 범위)**: 연결 프로파일에서 주소 풀에 대한 DHCP 서버를 컨피그레이션하는 경우, DHCP 범위에서는 이 그룹에 대한 풀에 사용할 서브넷을 식별합니다. 또한 DHCP 서버 주소에는 해당 범위에서 식별하는 동일한 풀에 주소가 있어야 합니다. 이 범위를 통해 사용자는 DHCP 서버에 정의된 주소 풀의 하위 집합을 선택하여 이 특정 그룹에 사용할 수 있습니다. 네트워크 범위를 정의하지 않으면 DHCP 서버에서 구성된 주소 풀 순으로 IP 주소를 할당합니다. 할당되지 않은 주소를 식별할 때까지 풀을 검색합니다. 범위를 지정하려면 네트워크 번호 호스트 주소를 포함하는 네트워크 개체를 입력합니다. 예를 들어 192.168.5.0/24 서브넷 풀에서 주소를 사용하도록 DHCP 서버에 지시하려면 192.168.5.0을 호스트 주소로 지정하는 네트워크 개체를 입력하십시오. IPv4 주소 지정에만 DHCP를 사용할 수 있습니다.

### 스플릿 터널링 속성

그룹 정책의 스플릿 터널링 속성에서는 내부 네트워크로 가는 트래픽과 외부로 가는 트래픽을 시스템에서 각각 분별하여 처리하는 방식을 정의합니다. 스플릿 터널링은 일부 네트워크 트래픽이 VPN 터널(암호화됨)을 통과하도록 유도하고 나머지 네트워크 트래픽은 VPN 터널 외부(암호화되지 않음 또는 일반 텍스트 형식)로 보냅니다.

일반적으로 원격 액세스 VPN에서는 VPN 사용자가 디바이스를 통해 인터넷에 액세스하도록 할 수 있습니다. 그러나 VPN 사용자가 RA VPN에 연결되어 있는 동안 외부 네트워크에 액세스하도록 허용할 수 있습니다. 이 기술을 스플릿 터널링 또는 헤어피닝이라고도 합니다. 스플릿 터널을 이용하면 보안 터널을 통한 원격 네트워크 VPN 연결이 가능하며, VPN 터널 외부의 네트워크에도 연결할 수 있습니다. 스플릿 터널링은 FTD 디바이스의 네트워크 부하를 줄이고 외부 인터페이스의 대역폭을 늘립니다.

#### 시작하기 전에

IPv4 네트워크에 대해 스플릿 터널 정책을 생성하고 IPv6 네트워크에 대해 다른 스플릿 터널 정책을 생성하는 경우, 지정한 액세스 목록이 두 가지 프로토콜 모두에 사용됩니다. 따라서 액세스 목록은 IPv4 및 IPv6 트래픽에 대한 ACE(Access Control Entries: 액세스 제어 항목)를 포함해야 합니다.

ASA 디바이스가 CDO에 온보딩되면 디바이스와 연결된 확장 ACL을 읽습니다. 자세한 내용은 그룹 정책 을 참조하십시오. 새 ACL을 생성하려면 ASA 정책(확장 액세스 목록)을 참조하십시오.

**Note** 생성 중인 ACL에서 스플릿 터널링을 위한 네트워크를 소스 네트워크로 지정해야 합니다.

- **IPv4 Split Tunneling(IPv4** 스플릿 터널링**)**, **IPv6 Split Tunneling(IPv6** 스플릿 터널링**)**: 트래픽에서 IPv4와 IPv6 중 어떤 주소 지정을 사용하는지에 따라 다른 옵션을 지정할 수 있지만, 각각의 경우 옵션은 동일합니다. 스플릿 터널링을 활성화하려는 경우, 네트워크 개체를 선택해야 하는 옵션 중 하나를 지정합니다.
  - **Allow all traffic over tunnel(**터널을 지나는 모든 트래픽 허용**)**: 스플릿 터널링은 실행하지 마십시오. 사용자가 RA VPN 연결을 하면 사용자의 모든 트래픽은 보호된 터널을 통과합니다. 이는 기본값입니다. 또한 이 기본값은 가장 안전한 옵션으로 간주됩니다.
  - **Allow specified traffic over the tunnel(**터널을 통해 지정된 트래픽 허용**)**: 소스 네트워크를 정의하는 확장 액세스 목록을 선택합니다. 이러한 소스의 모든 트래픽은 보호된 터널을 통과합니다. 클라이언트는 다른 소스의 트래픽을 터널 외부의 연결(예: 로컬 Wi-Fi 또는 네트워크 연결)로 라우팅합니다.
  - **Exclude networks specified below(**아래에 지정된 네트워크 제외**)**: 소스 네트워크를 정의하는 네트워크 개체를 선택합니다. 클라이언트는 이러한 소스의 모든 트래픽을 터널 외부의 연결로 라우팅합니다. 다른 소스의 트래픽은 터널을 통과합니다.
  - **Network List(**네트워크 목록**)**: IPv4 및 IPv6 네트워크를 모두 포함할 수 있는 확장 ACL 네트워크를 선택합니다.

- **Split DNS(**스플릿 **DNS)**: 보안 연결을 통해 일부 DNS 요청을 전송하도록 시스템을 구성함과 동시에 클라이언트가 클라이언트에 구성된 DNS 서버로 다른 DNS 요청을 전송하도록 허용할 수 있습니다. 다음 DNS 동작을 컨피그레이션할 수 있습니다.
  - **Send DNS Request as per split tunnel policy(**스플릿 터널 정책에 따라 **DNS** 요청 전송**)**: 이 옵션을 사용하면 스플릿 터널 옵션을 정의하는 것과 동일한 방식으로 DNS 요청이 처리됩니다. 스플릿 터널링을 활성화하는 경우, DNS 요청은 대상 주소에 근거하여 전송됩니다. 스플릿 터널링을 활성화하지 않는 경우, 모든 DNS 요청은 보호된 연결을 경유해 전송됩니다.
  - **Always send DNS requests over tunnel(**항상 터널을 통해 **DNS** 요청 전송**)**: 스플릿 터널링을 활성화하되 모든 DNS 요청을 보호된 연결을 경유해 그룹에 정의된 DNS 서버로 전송하려는 경우, 이 옵션을 선택합니다.
  - **Send only specified domains over tunnel(**지정된 도메인만 터널을 통해 전송**)**: 보호된 DNS 서버에서 특정 도메인에 대해서만 주소를 확인하게 하고 싶은 경우, 이 옵션을 선택합니다. 그런 다음, 도메인 이름을 쉼표로 구분하여 해당 도메인을 지정합니다. example.com, example1.com을 예로 들 수 있습니다. 내부 DNS 서버에서는 내부 도메인의 이름을 확인하고 외부 DNS 서버에서는 다른 모든 인터넷 트래픽을 처리하게 하려는 경우, 이 옵션을 사용합니다.

### AnyConnect 속성

그룹 정책의 AnyConnect 속성에서는 원격 액세스 VPN 연결에 대해 AnyConnect 클라이언트에서 사용하는 일부 SSL 및 연결 설정을 정의합니다.

- **SSL** 설정

- **Enable Datagram Transport Layer Security (DTLS)(DTLS(Datagram Transport Layer Security)** 활성화**)**: AnyConnect 클라이언트에서 2개의 터널(SSL 터널 및 DTLS 터널)을 동시에 사용하도록 허용할지 여부를 선택합니다. DTLS를 사용하면 일부 SSL 연결에서 발생하는 레이턴시 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성능을 개선할 수 있습니다. DTLS를 활성화하지 않은 경우에는 SSL VPN 연결을 설정하는 AnyConnect 클라이언트 사용자가 SSL 터널만 사용하여 연결합니다.
- **DTLS Compression(DTLS** 압축**)**: LZS를 사용하여 이 그룹에 대한 DTLS(Datagram Transport Layer Security) 연결을 압축할지 여부를 선택합니다. DTLS 압축은 기본적으로 비활성화되어 있습니다.
- **SSL** 압축: 데이터 압축 활성화 여부를 선택하고, 활성화하는 경우 압축 해제 또는 **LZS** 중 사용할 데이터 압축 방법을 선택합니다. SSL 압축은 기본적으로 **Disabled(**비활성화**)** 상태입니다. 데이터를 압축하면 전송 속도가 빨라지지만 각 사용자 세션에 대한 메모리 요건 및 CPU 사용량이 증가합니다. 따라서 SSL 압축으로 인해 디바이스의 전체 처리량은 줄어듭니다.
- **SSL Rekey Method(SSL** 키 재입력 방법**)**, **SSL Rekey Interval(SSL** 키 재입력 간격**)**: 클라이언트는 VPN 연결에 키를 재입력하여 암호화 키 및 초기화 벡터를 재협상할 수 있어 연결 보안이 강화됩니다. **None(**없음**)**을 선택하여 키 재입력을 비활성화합니다. 키 재입력을 활성화하려면 **New Tunnel(**새 터널**)**을 선택하여 매번 새 터널을 생성합니다. (**Existing Tunnel(**기존 터널**)** 옵션을 선택하면 **New Tunnle(**새 터널**)**과 동일한 조치가 수행됩니다.) 키 재입력을 활성화하는 경우, 키 재입력 간격도 설정하십시오. 기본값은 4분입니다. 4~10080분(일주일) 범위 내에서 간격을 설정할 수 있습니다.

• 연결 설정

- **Ignore the DF (Don't Fragment) bit(DF(Don't Fragment)** 비트 무시**)**: 단편화해야 하는 패킷에서 DF(Don't Fragment) 비트를 무시할지 여부를 선택합니다. 이 옵션을 선택하면 DF 비트가 설정된 패킷의 강제 단편화가 허용되므로 이 패킷이 터널을 통과할 수 있습니다.
- **Client Bypass Protocol(**클라이언트 우회 프로토콜**)**: 이 옵션을 선택하면 보안 게이트웨이에서 IPv6 트래픽만 예상할 때 IPv4 트래픽을 관리하는 방법 또는 IPv4 트래픽만 예상할 때 IPv6 트래픽을 관리하는 방법을 구성할 수 있습니다.

  AnyConnect 클라이언트에서 헤드엔드와의 VPN 연결을 수행할 때 헤드엔드에서는 IPv4 주소나 IPv6 주소 또는 IPv4 및 IPv6 주소 모두를 지정합니다. 헤드엔드에서 AnyConnect 연결에 IPv4 주소만 또는 IPv6 주소만 지정할 경우, 헤드엔드에서 IP 주소를 지정하지 않은 네트워크 트래픽을 삭제하거나 이 트래픽이 헤드엔드를 우회하여 암호화되지 않은 또는 "일반 텍스트" 형태(활성화 및 확인된 상태)로 클라이언트에서 전송되는 것을 허용하도록 Client Bypass Protocol(클라이언트 우회 프로토콜)을 컨피그레이션할 수 있습니다.

  예를 들어 보안 게이트웨이에서 AnyConnect 연결에 IPv4 주소만 지정하고 엔드포인트는 이중 스택이라고 가정합시다. 엔드포인트가 IPv6 주소에 연결하려고 시도할 때 클라이언트 우회 프로토콜이 비활성화된 경우 IPv6 트래픽이 끊기지만 클라이언트 우회 프로토콜이 활성화된 경우, IPv6 트래픽은 클라이언트에서 암호화되지 않은 상태로 전송됩니다.
- **MTU**: Cisco AnyConnect VPN 클라이언트에서 설정한 SSL VPN 연결의 MTU(Maximum Transmission Unit)입니다. 기본값은 1406바이트입니다. 범위는 576~1462바이트입니다.

- **Keepalive Messages Between AnyConnect and VPN Gateway(AnyConnect**와 **VPN** 게이트웨이 간의 연결 유지 메시지**)**: 피어 간에 연결 유지 메시지를 교환하여 터널에서 데이터를 송수신하는 데 사용할 수 있다는 것을 시연할지 여부를 선택합니다. 연결 유지 메시지는 설정된 간격에 따라 전송됩니다. 기본 간격은 20초, 유효 범위는 15~600초입니다.
- **DPD on Gateway Side Interval(**게이트웨이 측 간격의 **DPD)**, **DPD on Client Side Interval(**클라이언트 측 간격의 **DPD)**: DPD(Dead Peer Detection)를 활성화하면 피어가 더 이상 응답하지 않을 경우 VPN 게이트웨이 또는 VPN 클라이언트를 신속하게 탐지할 수 있습니다. 게이트웨이 또는 클라이언트 DPD를 별도로 활성화할 수 있습니다. DPD 메시지 전송의 기본 간격은 30초입니다. 간격은 5-3600초 사이일 수 있습니다.

### 트래픽 필터 속성

그룹 정책의 트래픽 필터 속성에서는 그룹에 할당된 사용자에게 부과하고 싶은 제한 사항을 정의합니다. 액세스 제어 정책 규칙을 생성하는 대신 이 속성을 사용해 RA VPN 사용자를 호스트 또는 서브넷 주소 및 프로토콜, VLAN에 따라 특정 리소스로 제한할 수 있습니다. 기본적으로 그룹 정책에 따라 RA VPN 사용자는 보호된 네트워크의 어떤 대상에 액세스하는 것도 제한되지 않습니다.

- **Access List Filter(**액세스 목록 필터**)**: 확장된 ACL(액세스 제어 목록)을 사용하여 액세스를 제한합니다. Smart CLI 확장 ACL 개체를 선택합니다. 확장 ACL을 통해 소스 주소, 대상 주소 및 프로토콜(예: IP 또는 TCP)을 기준으로 필터링할 수 있습니다. ACL은 하향식, 최초 일치 방식에 따라 평가되므로 특정 규칙이 다수의 일반 규칙보다 먼저 배치되도록 보장합니다. ACL의 끝에는 암묵적 "deny any(모두 거부)"가 있으므로 서브넷 몇 개에 대한 액세스만 거부하고 다른 모든 액세스는 허용하려면 ACL의 끝에 "permit any(모두 허용)" 규칙을 포함하십시오. 확장 ACL 스마트 CLI 개체를 수정하는 중에는 네트워크 개체를 생성할 수 없으므로 그룹 정책을 수정하기 전에 ACL을 생성해야 합니다. 그러지 않는 경우, 개체만 생성할 수 있습니다. 그런 다음 다시 돌아가 네트워크 개체를 생성한 후 필요한 모든 액세스 제어 항목을 생성하면 됩니다. ACL을 생성하려면 FDM에 로그인하고 **Device(**디바이스**)** > **Advanced Configuration(**고급 구성**)** > **Smart CLI(**스마트 **CLI)** > **Objects(**개체**)**로 이동하여 개체를 생성하고 **Extended Access List(**확장 액세스 목록**)**를 개체 유형으로 선택합니다.
- **Restrict VPN to VLAN(VPN**을 **VLAN**으로 제한**)**: “VLAN 매핑”이라고도 하는 이 속성에서는 이 그룹 정책이 적용되는 세션에 이그레스(egress) VLAN 인터페이스를 지정합니다. 시스템에서는 이 그룹에서 나오는 모든 트래픽을 선택한 VLAN으로 전달합니다. 이 특성을 사용하여 그룹 정책에 VLAN을 할당하면 액세스 제어를 간소화할 수 있습니다. ACL을 사용하여 세션의 트래픽을 필터링하는 방법 대신 이 속성에 값을 할당하는 방법도 가능합니다. 디바이스에서 하위 인터페이스에 정의된 VLAN 번호를 반드시 지정하십시오. 값의 범위는 1에서 4094까지입니다.

### **Windows** 브라우저 프록시 속성

그룹 정책의 Windows 브라우저 프록시 속성에서는 사용자의 브라우저에 정의된 프록시의 작동 방식과 작동 여부를 결정합니다.

**Browser Proxy During VPN Session(VPN** 세션 중 브라우저 프록시**)**에 대해 다음 값 중 하나를 선택할 수 있습니다.

- **No change in endpoint settings(**엔드포인트 설정에 변경 사항 없음**)**: 이 옵션을 통해 사용자는 HTTP에 대해 브라우저 프록시를 컨피그레이션하거나 컨피그레이션하지 않을 수 있으며 컨피그레이션되어 있는 경우 프록시를 사용할 수 있습니다.
- **Disable browser proxy(**브라우저 프록시 비활성화**)**: 브라우저에 대해 정의된 프록시(있는 경우)를 사용하지 않습니다. 이 경우 프록시를 통해 브라우저 연결이 설정되지 않습니다.
- **Auto detect settings(**설정 자동 탐지**)**: 클라이언트 디바이스에 대해 브라우저에서 자동 프록시 서버 감지를 사용하도록 활성화합니다.
- **Use custom settings(**사용자 정의 설정 사용**)**: HTTP 트래픽에 대해 모든 클라이언트 디바이스에서 사용해야 하는 프록시를 정의합니다. 다음 설정을 구성합니다.
  - **Proxy Server IP or Hostname(**프록시 서버 **IP** 또는 호스트네임**)**, **Port(**포트**)**: 프록시 서버의 IP 주소 또는 호스트네임, 프록시 서버에서 프록시 연결에 사용하는 포트입니다. 호스트와 포트를 합해 100자를 초과할 수 없습니다.
  - **Browser Exemption List(**브라우저 면제 목록**)**: 면제 목록의 호스트/포트에 대한 연결은 프록시를 통과하지 않습니다. 프록시를 사용해서는 안 되는 대상에 대해 모든 호스트/포트 값을 추가합니다. www.example.com port 80을 예로 들 수 있습니다. 목록에 항목을 추가하려면 **Add Proxy Exemption(**프록시 예외 추가**)**을 클릭합니다. 항목을 삭제하려면 휴지통 아이콘을 클릭합니다. 모든 주소와 포트를 합한 전체 프록시 예외 목록은 255자를 초과할 수 없습니다.

## *ASA RA VPN* 구성 생성

CDO를 사용하면 하나 이상의 ASA(Adaptive Security Appliance) 디바이스를 RA VPN 구성 마법사에 추가하고 디바이스와 연결된 VPN 인터페이스, 액세스 제어 및 NAT 면제 설정을 구성할 수 있습니다. 따라서 각 RA VPN 구성에는 RA VPN 구성과 연결된 여러 ASA 디바이스에서 공유되는 연결 프로파일 및 그룹 정책이 있을 수 있습니다. 또한 연결 프로파일 및 그룹 정책을 생성하여 구성을 개선할 수 있습니다.

RA VPN 설정으로 이미 구성된 ASA 디바이스 또는 RA VPN 설정이 없는 새 디바이스를 온보딩할 수 있습니다. ASA 디바이스 온보딩, 149 페이지을 참조하십시오. 이미 RA VPN 설정이 있는 ASA 디바이스를 온보딩하는 경우 CDO는 자동으로 "기본 RA VPN 구성"을 생성하고 ASA 디바이스를 이 구성과 연결합니다. 또한 이 기본 구성은 디바이스에 정의된 모든 연결 프로파일 개체를 포함할 수 있습니다. 온보딩된 ASA 디바이스의 RA VPN 구성 읽기를 참조하십시오. CDO를 사용하면 기본 구성을 삭제할 수 있습니다.

중요

- 동일한 원격 액세스 VPN 구성에서 ASA 및 FTD 를 추가할 수 없습니다.
- ASA 디바이스는 두 개 이상의 RA VPN 구성을 가질 수 없습니다.

시작하기 전에

RA VPN 구성에 ASA 디바이스를 추가하려면 먼저 다음 사전 요구 사항을 충족해야 합니다.

- 라이선스 요구 사항

  수출 통제 기능을 사용하려면 디바이스를 활성화해야 합니다.

  ASA 디바이스의 라이선스 요약을 보려면 ASA 명령줄 인터페이스에서 show license summary 명령을 실행합니다. CDO ASA CLI 인터페이스를 사용하려면 CDO 명령줄 인터페이스을 참조하십시오.

  - 라이선스 요약에서 활성화된 수출 통제 기능의 예:

```
등록: 상태: REGISTERED 스마트 어카운트: Cisco SVS temp-request access licensing@cisco.com
내보내기 제어 기능: ALLOWED

마지막 갱신 시도: 없음

다음 갱신 시도: 2021년 6월 8일 09:46:22 UTC
```

  VPN 구성을 생성하거나 편집하려면 '내보내기 제어 기능' 속성이 '허용됨' 상태여야 합니다.

  이 속성이 '허용되지 않음' 상태인 경우 CDO는 VPN 구성을 생성하거나 편집하고 디바이스에서 RA VPN 구성을 허용하지 않을 때 오류 메시지('RA VPN은 수출 규격이 아닌 디바이스에 대해 구성할 수 없습니다.')를 표시합니다.

- 디바이스 ID 인증서

  클라이언트와 ASA 디바이스 간의 SSL 연결을 인증하려면 인증서가 필요합니다. VPN 구성을 시작하려면 먼저 ASA 디바이스에 ID 인증서가 이미 있는지 확인합니다.

  디바이스에 인증서가 있는지 여부를 확인하려면 ASA 명령줄 인터페이스에서 **show crypto CA Certificates** 명령을 실행합니다. CDO ASA CLI 인터페이스를 사용하려면 CDO 명령줄 인터페이스을 참조하십시오.

  ID 인증서가 없거나 새 인증서를 등록하려는 경우 CDO를 사용하여 ASA에 설치합니다. ASA 인증서 관리를 참조하십시오.

  원격 액세스 VPN 컨텍스트에서 디지털 인증서의 사용은 원격 액세스 VPN 인증서 기반 인증, 304 페이지에 설명되어 있습니다.

- 외부 인터페이스.

  외부 인터페이스는 ASA 디바이스에 이미 구성되어 있어야 합니다. 인터페이스를 구성하려면 **ASDM** 또는 **ASA CLI**를 사용해야 합니다. ASDM을 사용한 인터페이스 구성에 대해 알아보려면 Cisco ASA Series General Operations CLI Configuration Guide, X.Y의 "Interfaces" 책을 참조하십시오.

- AnyConnect 패키지를 다운로드하고 원격 서버에 업로드하십시오. 나중에 RA VPN 마법사 또는 ASA 파일 관리 마법사를 사용하여 서버에서 ASA로 AnyConnect 소프트웨어 패키지를 업로드하십시오. ASA 디바이스에서 AnyConnect 소프트웨어 패키지 관리를 참조하십시오.

- 보류 중인 구성 배포이 없습니다.

- 인증에 로컬 데이터베이스를 사용하는 경우 ASDM 또는 ASA CLI를 사용하여 로컬 데이터베이스에 사용자 계정을 추가합니다.

ASDM을 사용하여 사용자 계정을 추가하려면 Cisco ASA Series VPN CLI 구성 가이드, X.Y의 "AAA 서버 및 로컬 데이터베이스" 책에서 "로컬 데이터베이스에 사용자 계정 추가" 섹션을 참조하십시오.

ASA CLI를 사용하여 사용자 계정을 추가하려면, **username[***username***] password [***password***] privilege [***priv_level]*** command.usernamepasswordpriv_level] 명령을 실행합니다.

- ASA 변경 사항은 CDO에 동기화됩니다.
  1. 왼쪽의 CDO 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭하고 동기화할 하나 이상의 ASA 디바이스를 검색합니다.
  2. 하나 이상의 디바이스를 선택한 다음 **Check for changes(**변경 사항 확인**)**를 클릭합니다. CDO는 하나 이상의 FTD 디바이스와 통신하여 변경 사항을 동기화합니다.
- RA VPN 구성 그룹 정책 개체가 일치합니다.
  - 일치하지 않는 모든 그룹 정책 개체는 RA VPN 구성에 추가할 수 없으므로 확인해야 합니다. 문제를 해결하거나 **Objects(**개체**)** 페이지에서 일치하지 않는 그룹 정책 개체를 제거합니다. 자세한 내용은 중복 개체 문제 해결 및 불일치 개체 문제 해결을 참조하십시오.

---

단계 **1** ASA 디바이스 온보딩, 149 페이지.

단계 **2** 왼쪽의 CDO 탐색 모음에서 **VPN** > **ASA/FDM** 원격 액세스 **VPN** 구성를 클릭합니다.

단계 **3** 파란색 더하기  버튼을 클릭하여새 RA VPN 구성을 생성합니다.

단계 **4** 원격 액세스 VPN 구성의 이름을 입력합니다.

단계 **5** 파란색 더하기  버튼을 클릭하여 ASA 디바이스를 구성에 추가합니다.

디바이스 세부 정보를 추가하고 디바이스와 연결된 네트워크 트래픽 관련 권한을 구성할 수 있습니다.

1. 다음 디바이스 세부 사항을 입력합니다.
   - 디바이스: 추가할 ASA 디바이스를 선택하고 **Select(**선택**)**를 클릭합니다. 중효동일한 원격 액세스 VPN 구성에서 ASA 및 FTD를 추가할 수 없습니다.
   - **Certificate of Device Identity(**디바이스 **ID**의 인증서**)**: 디바이스의 ID를 설정하는 데 사용되는 내부 인증서를 선택합니다. 그러면 AnyConnect 클라이언트가 디바이스에 연결할 때 디바이스 ID를 설정합니다. 보안 VPN 연결을 완료하려면 클라이언트가 이 인증서를 허용해야 합니다.
   - **Outside Interface(**외부 인터페이스**)**: 원격 액세스 VPN 연결 시 사용자가 연결할 인터페이스를 선택합니다. 이 인터페이스는 대개 외부(인터넷 연결) 인터페이스이지만, 이 연결 프로파일을 사용하여 지원하려는 디바이스와 엔드 유저 간의 인터페이스를 선택하면 됩니다.

     주의 수출 규격이 아닌 디바이스에 대한 RA VPN 구성을 생성하거나 편집할 수 없습니다. 수출 통제 기능이 활성화된 ASA 디바이스에 라이선스를 부여하고 다시 시도해야 합니다.

2. **Continue(**계속**)**를 클릭하여 트래픽 권한을 구성합니다.

- **Bypass Access Control policy for decrypted traffic(**암호 해독된 트래픽에 대해 액세스 제어 정책 우회**)(sysopt permit-vpn)**: 암호 해독된 트래픽은 기본적으로 액세스 제어 정책 검사를 받습니다. 이 옵션을 활성화하면 암호 해독된 트래픽 옵션이 액세스 제어 정책 검사를 무시하지만, VPN 필터 ACL과 AAA 서버에서 다운로드한 인증 ACL이 VPN 트래픽에 계속 적용됩니다.

  이 옵션을 선택하는 경우, 시스템에서는 전역 설정인 sysopt connection permit-vpn 명령을 구성한다는 점에 유의하십시오. 이로 인해 Site-to-Site VPN 연결의 동작도 영향을 받습니다.

  이 옵션을 선택하지 않는 경우, 외부 사용자가 원격 액세스 VPN 주소 풀의 IP 주소를 스푸핑할 수 있고, 따라서 네트워크에 액세스할 수 있습니다. 이것이 가능한 이유는 주소 풀에서 내부 리소스에 액세스할 수 있게 허용하는 액세스 제어 규칙을 생성해야 하기 때문입니다. 액세스 제어 규칙을 사용하는 경우, 소스 IP 주소만 사용하기보다 사용자 사양을 이용해 액세스를 제어하는 것이 좋습니다.

  이 옵션을 선택할 경우의 단점은 VPN 트래픽이 검사되지 않는다는 것입니다. 즉 침입 및 파일 보호, URL 필터링 또는 기타 고급 기능이 트래픽에 적용되지 않습니다. 즉 트래픽에 대해 연결 이벤트가 생성되지 않고, 따라서 통계 대시보드에 VPN 연결이 반영되지 않는다는 의미이기도 합니다.

- **NAT** 제외**(Exempt)**: NAT NAT 제외는 주소 변환을 제외하고 변환된 호스트와 원격 호스트가 모두 보호되는 호스트와의 연결을 시작할 수 있도록 허용합니다. NAT 제외를 구성하여 NAT 변환에서 원격 액세스 VPN 엔드포인트로 오가는 트래픽을 제외합니다. NAT에서 원격 액세스 트래픽 제외, 305 페이지의 내용을 참조하십시오.

3. 확인를 클릭합니다.

   **AnyConnect Packages Detected(**감지된 **AnyConnect** 패키지**)**는 디바이스에서 이미 사용 가능한 AnyConnect 패키지를 표시합니다.

   RA VPN 마법사에서 AnyConnect 패키지를 ASA에 업로드하는 두 가지 옵션이 있습니다.

   - (방법 1): CDO 저장소에서 패키지를 선택합니다. ASA는 인터넷에 액세스할 수 있어야 합니다.
   - (방법 2): AnyConnect 패키지가 사전 로드된 ftp/http/https/scp/smb/tftp URL 위치를 지정합니다.

   지침은 ASA 디바이스에서 AnyConnect 소프트웨어 패키지 관리를 참조하십시오.

   참고 참고: 기존 패키지를 교체하려면 ASA 디바이스에서 AnyConnect 소프트웨어 패키지 관리를 참조하십시오.

단계 **6** **OK(**확인**)**를 클릭합니다.

ASA VPN 구성이 생성됩니다.

---

ASA RA VPN 구성 수정

기존 RA VPN 구성의 이름 및 디바이스 세부 정보를 수정할 수 있습니다.

---

단계 **1** 수정할 구성을 선택하고 **Actions(**작업**)** 아래에서 **Edit(**편집**)**를 클릭합니다.

- 필요한 경우 이름을 수정합니다.

- 디바이스를 추가하려면 파란색 더하기 버튼  을 클릭합니다.
- 을 클릭하여 ASA 디바이스에서 다음을 수행합니다.
  - **Edit(편집)**를 클릭하여 기존 RA VPN 구성을 수정합니다.
  - **Remove(제거)**를 클릭하여 RA VPN 구성에서 ASA 디바이스를 제거합니다. 그룹 정책을 제외하고 해당 디바이스와 연결된 모든 연결 프로파일 및 RA VPN 설정이 삭제됩니다. 개체 페이지에서 그룹 정책을 명시적으로 제거할 수 있습니다.

    **Note** ASA가 구성을 사용하는 유일한 디바이스인 경우 ASA를 제거할 수 없습니다. 또는 RA VPN 구성을 제거할 수 있습니다.

단계 **2** CDO에서 ASA로 구성 변경 사항 구축.

---

**What to do next**

구성 또는 디바이스의 이름을 입력하여 Remote Access VPN 구성을 검색할 수도 있습니다.
관련 정보**:**

- ASA RA VPN 연결 프로파일 구성, on page 289.

## *ASA RA VPN* 연결 프로파일 구성

원격 액세스 VPN 연결 프로파일에서는 외부 사용자가 AnyConnect 클라이언트를 사용하여 시스템에 VPN 연결을 할 수 있게 허용하는 특성을 정의합니다. 각 프로파일에서 정의하는 것은 사용자를 인증하는 데 사용되는 AAA 서버 및 인증서, 사용자에게 IP 주소를 할당하기 위한 주소 풀, 다양한 사용자 중심 속성을 정의하는 그룹 정책입니다.

여러 사용자 그룹에 가변적인 서비스를 제공해야 하는 경우 또는 다양한 인증 소스가 있는 경우, RA VPN구성 내에 프로파일을 여러 개 생성합니다. 예를 들어 조직이 다른 인증 서버를 사용하는 다른 조직과 병합하는 경우, 해당 인증 서버를 사용하는 새 그룹에 대해 프로파일을 만들 수 있습니다.

RA VPN 연결 프로파일을 사용하면 홈 네트워크 등의 외부 네트워크에 있는 사용자가 내부 네트워크에 연결할 수 있습니다. 다른 인증 방법을 수용하기 위해 별도 프로파일을 생성합니다.

시작하기 전에

ASA RA VPN 구성 생성, 285 페이지.

---

단계 **1** CDO 탐색 창에서 **VPN** > **ASA/FDM Remote Access VPN Configuration(ASA/FDM** 원격 액세스 **VPN** 구성**)**를 클릭합니다. VPN 구성을 클릭하여 현재 얼마나 많은 연결 프로파일 및 그룹 정책이 구성되어 있는지에 대한 요약 정보를 볼 수 있습니다.

참고 디바이스에 할당된 그룹 정책을 확인하려면 **Actions(**작업**)**에서 **Group Policies(**그룹 정책**)**를 클릭합니다. 연결 프로파일에 할당된 그룹 정책은 목록에 자동으로 추가되며 제거할 수 없습니다.

필요한 그룹 정책이 아직 없는 경우  을 클릭하고 목록에서 선택합니다. 필요한 서비스를 제공하는 추가 그룹 정책을 만들 수 있습니다. 새 ASA RA VPN 그룹 정책 생성, 277 페이지을 참조하십시오.

단계 **2** 연결 프로파일을 클릭하고 오른쪽 사이드바의 **Actions(**작업**)** 아래에서 **Add Connection Profile(**연결 프로파일 추가**)**를 클릭합니다.

단계 **3** 기본 연결 속성을 구성합니다.

- **Connection Profile Name(**연결 프로파일 이름**)**: 이 연결의 이름을 공백 없이 50자까지 입력합니다. 예를 들면 MainOffice를 입력합니다.

  참고 여기서 입력하는 이름이 AnyConnect 클라이언트에서 사용자에게 표시되는 연결 목록에 나타납니다. 따라서 사용자가 쉽게 이해할 수 있는 이름을 선택해야 합니다.

- **Group Alias(**그룹 별칭**), Group URL(**그룹 **URL)**: 별칭에는 특정 연결 프로파일에 대한 대체 이름 또는 URL이 포함되어 있습니다. ASA 디바이스에 연결하는 경우, VPN 사용자는 연결 목록의 AnyConnect 클라이언트에서 별칭 이름을 선택할 수 있습니다. 연결 프로파일 이름이 그룹 별칭으로 자동 추가됩니다. 또한 원격 액세스 VPN 연결을 시작하는 동안 엔드포인트에서 선택할 수 있는 그룹 URL의 목록을 구성할 수 있습니다. 사용자가 그룹 URL을 사용하여 연결하는 경우, 시스템에서는 URL과 일치하는 연결 프로파일을 자동으로 사용합니다. 이 URL은 설치된 AnyConnect 클라이언트가 아직 없는 클라이언트에서 사용됩니다. 그룹 별칭 및 URL을 필요한 만큼 추가하십시오. 이러한 별칭 및 URL은 디바이스에 정의된 모든 연결 프로파일 전반에 걸쳐 고유한 것이어야 합니다. 그룹 URL은 **https://**로 시작해야 합니다.

- 예를 들어 별칭 계약자 및 그룹 URL https://ravpn.example.com/contractor가 있을 수 있습니다. AnyConnect 클라이언트가 설치된 후 사용자는 연결의 AnyConnect VPN 드롭다운 목록에서 그룹 별칭을 선택하기만 하면 됩니다.

단계 **4** 기본 ID 소스를 구성하고, 선택적으로 보조 ID 소스를 구성합니다. 이 옵션을 통해 원격 사용자가 원격 액세스 VPN 연결을 활성화하기 위해 디바이스에 인증하는 방식을 결정합니다. 가장 간단한 방식은 AAA만 사용하여 AD 영역을 선택하거나 LocalIdentitySource를 사용하는 것입니다. **Authentication Type(**인증 유형**)**에는 다음과 같은 방식을 사용할 수 있습니다.

- **AAA Only(AAA**만**)**: 사용자 이름 및 암호에 근거하여 사용자를 인증하고 사용자에게 권한을 부여합니다. 자세한 내용은 연결 프로파일에 대해 AAA 구성 , 291 페이지 섹션을 참조하십시오.

- **Client Certificate Only(**클라이언트 인증서만**)**: 클라이언트 디바이스 ID 인증서에 근거하여 사용자를 인증합니다. 자세한 내용은 연결 프로파일에 대한 인증서 인증 구성을 참조하십시오.

- **AAA and ClientCertificate(AAA** 및 **ClientCertificate)**: 사용자 이름/암호와 클라이언트 디바이스 ID 인증서를 모두 사용합니다.

단계 **5** 클라이언트에 대해 주소 풀을 구성합니다. 주소 풀에서는 원격 클라이언트가 VPN 연결을 설정할 때 시스템에서 원격 클라이언트에 할당할 수 있는 IP 주소를 정의합니다. 자세한 내용은 클라이언트 주소 풀 할당 구성을 참조하십시오.

단계 **6** **Continue(**계속**)**를 클릭합니다.

단계 **7** 목록에서 이 프로파일에 사용할 **Group Policy(**그룹 정책**)**를 선택하고 **Select(**선택**)**를 클릭합니다.

그룹 정책에서는 터널이 설정된 후에 사용자 연결에 대한 조건을 설정합니다. 시스템에는 'DfltGrpPolicy'라는 이름의 기본 그룹 정책이 포함되어 있습니다. 필요한 서비스를 제공하는 추가 그룹 정책을 만들 수 있습니다. 새 ASA RA VPN 그룹 정책 생성, 277 페이지을 참조하십시오.

단계 **8** **Continue(**계속**)**를 클릭합니다.

단계 **9** 요약을 검토합니다. 먼저 요약이 정확한지 확인합니다. AnyConnect 소프트웨어를 처음으로 설치하고 VPN 연결을 완료할 수 있는지를 테스트하기 위해 엔드 유저가 수행해야 하는 작업을 파악할 수 있습니다.  를 클릭하여 지침을 클립보드에 복사한 다음 사용자에게 배포합니다.

단계 **10** **Done(**완료**)**를 클릭합니다.

단계 **11** ASA에 대한 엔드 투 엔드 원격 액세스 VPN 구성 프로세스의 5단계를 수행합니다.

## 연결 프로파일에 대해 AAA 구성

인증, 권한 부여, 계정 관리 (AAA) 서버에서는 사용자 이름과 암호를 사용하여 사용자에게 원격 액세스 VPN에 대한 액세스가 허용되어 있는지 확인합니다. RADIUS 서버를 사용하는 경우, 인증된 사용자들 사이에서 권한 부여 수준을 구별하여 보호받는 리소스에 대한 차등 액세스를 제공할 수 있습니다. 또한 RADIUS 계정 관리 서비스를 사용하여 사용량을 추적할 수 있습니다.

AAA를 구성하는 경우, 기본 ID 소스를 구성해야 합니다. 보조 및 대체 소스는 선택 사항입니다. 2단계 인증을 구현하려면 RSA 토큰 또는 듀오와 같은 보조 소스를 사용합니다.

### 기본 **ID** 소스 옵션

- 사용자 인증을 위한 기본 **ID** 소스: 인증은 일반적으로 액세스 권한이 부여되기 전에 사용자가 유효한 사용자 이름과 유효한 암호를 입력하도록 하여 사용자를 식별하는 방법을 제공합니다. 원격 사용자를 인증하는 데 사용되는 기본 ID 소스입니다. VPN 연결을 완료하려면 이 소스 또는 대체 소스(선택 사항)에서 최종 사용자를 정의해야 합니다. 다음 중 하나를 선택합니다.
  - AD(Active Directory) ID 영역.
  - Radius 서버 그룹.
  - LocalIdentitySource(로컬 사용자 데이터베이스): 외부 서버를 사용하지 않고 디바이스에서 직접 사용자를 정의할 수 있습니다.

    ASA에 대한 ID 소스 구성를 클릭하여 새 ID 소스를 생성할 수 있습니다.

- **Fallback Local Identity Source(**대체 로컬 **ID** 소스**)**: 기본 소스가 외부 서버인데 기본 서버를 사용할 수 없는 경우, 대체 소스로 LocalIdentitySource를 선택할 수 있습니다. 로컬 데이터베이스를 대체 소스로 사용하는 경우 외부 서버에 정의한 것과 같은 로컬 사용자 이름/비밀번호를 정의해야 합니다.
- **Strip options(**제거 옵션**)**: 영역은 관리 도메인입니다. 다음 옵션을 활성화하면 사용자 이름에만 근거하여 인증할 수 있습니다. 이러한 옵션의 조합을 활성화할 수 있습니다. 그러나 서버에서 구분 기호를 구문 분석할 수 없는 경우, 두 확인란을 모두 선택해야 합니다.
  - **Strip Identity Source Server from Username(**사용자 이름에서 **ID** 소스 서버 제거**)**: AAA 서버로 사용자 이름을 전달하기 전에 사용자 이름에서 ID 소스 이름을 제거할지 여부. 예를 들

어 이 옵션을 선택하고 사용자가 사용자 이름으로 domain\username을 입력하면 도메인이 사용자 이름에서 제거되고 인증을 위해 AAA 서버로 전송됩니다. 기본적으로 이 옵션은 선택되어 있지 않습니다.

- **Strip Group from Username(**사용자 이름에서 그룹 제거**)**: AAA 서버로 사용자 이름을 전달하기 전에 사용자 이름에서 그룹 이름을 제거할지 여부. 이 옵션은 username@domain 형식에서 지정된 이름에 적용되며, 도메인 및 @ 기호를 제거합니다. 기본적으로 이 옵션은 선택되어 있지 않습니다.

보조 **ID** 소스

- **Secondary Identity Source for User Authorization(**사용자 권한 부여를 위한 보조 **ID** 소스**)**: 두 번째 ID 소스로서 선택 사항입니다. 사용자가 기본 소스로 인증에 성공하는 경우, 사용자에게 보조 소스를 사용해 인증하라는 메시지가 표시됩니다. AD 영역, RADIUS 서버 그룹 또는 로컬 ID 소스를 선택할 수 있습니다.
- **Advanced options(**고급 옵션**)**: **Advanced(**고급**)** 링크를 클릭하고 다음 옵션을 구성합니다.
  - **Fallback Local Identity Source for Secondary(**보조용 대체 시스템 로컬 **ID** 소스**)**: 보조 소스가 외부 서버인데 보조 서버를 사용할 수 없는 경우, LocalIdentitySource를 대체 소스로 선택할 수 있습니다. 로컬 데이터베이스를 대체 소스로 사용하는 경우, 보조 외부 서버에 정의한 것과 같은 로컬 사용자 이름/암호를 정의해야 합니다.
  - **Use Primary Username for Secondary Login(**보조 로그인에 기본 사용자 이름 사용**)**: 보조 ID 소스를 사용하는 경우, 시스템에서는 기본적으로 보조 소스에 대한 사용자 이름 및 암호를 모두 입력하라는 메시지를 표시합니다. 이 옵션을 선택하는 경우, 시스템에서는 보조 암호만 입력하라는 메시지를 표시하고 기본 ID 소스에 대해 인증된 보조 소스에 동일한 사용자 이름을 사용합니다. 기본 및 보조 ID 소스 모두에서 동일한 사용자 이름을 구성하는 경우, 이 옵션을 선택합니다.
    - **Username for Session Server(**세션 서버의 사용자 이름**)**: 인증에 성공하면 사용자 이름이 이벤트 및 통계 대시보드에 표시되고, 이 이름은 사용자 또는 그룹 기반 SSL 암호 해독 및 액세스 제어 규칙에 대한 일치 여부를 확인하고 계정을 관리하는 데 사용됩니다. 두 가지 인증 소스를 사용하고 있기 때문에 기본 또는 보조 사용자 이름을 사용자 ID로 사용할지 여부를 시스템에 알려주어야 합니다. 기본적으로 기본 이름을 사용합니다.
    - **Password Type(**암호 유형**)**: 보조 서버의 암호를 가져오는 방법. 기본값은 **Prompt(**프롬프트**)**입니다. 이는 사용자에게 암호를 입력하라는 메시지가 표시됨을 뜻합니다. 사용자가 기본 서버에 인증할 때 입력한 암호를 자동으로 사용하려면 **Primary Identity Source Password(**기본 **ID** 소스 암호**)**를 선택합니다. 모든 사용자에 대해 동일한 암호를 사용하려면 **Common Password(**공통 암호**)**를 선택한 다음, **Common Password(**공통 암호**)** 필드에 해당 암호를 입력합니다.
  - **Authorization Server(**권한 부여 서버**)**: 원격 액세스 VPN 사용자를 인증하도록 구성된 RADIUS 서버 그룹. 인증이 완료되면 권한 부여 기능에서 인증된 각 사용자에게 사용할 수 있는 서비스 및 명령을 제어합니다. 권한 부여 기능은 사용자가 수행할 수 있도록 인가를 받은 것이 무엇인지, 즉 사용자의 실제 능력 및 제한 사항을 설명하는 일련의 속성을 결합함으로써 작

동합니다. 권한 부여 기능을 사용하지 않는 경우, 인증 기능에서만 인증된 모든 사용자에게 동일한 액세스 권한을 제공합니다.

시스템이 그룹 정책에 정의된 것과 중복되는 권한 부여 속성을 RADIUS 서버에서 가져오는 경우, RADIUS 속성은 그룹 정책 속성을 오버라이드한다는 점에 유의하십시오.

ASA RADIUS 서버 개체 또는 그룹 생성 또는 편집을 클릭하여 새 서버 그룹을 생성할 수 있습니다.

- **Accounting Server(**과금 서버**)**: (선택 사항) 원격 액세스 VPN 세션에 대한 계정 관리에 사용할 RADIUS 서버 그룹입니다. 계정 관리 기능에서는 사용자가 액세스 중인 서비스뿐 아니라 사용 중인 네트워크 리소스의 수까지도 추적합니다. ASA 디바이스에서는 RADIUS 서버에 사용자 활동을 보고합니다. 계정 관리 정보에는 세션 시작 및 중지 시각, 사용자 이름, 각 세션의 디바이스를 통과한 바이트 수, 사용한 서비스, 각 세션의 지속시간이 포함됩니다. 네트워크 관리, 클라이언트 요금 청구 또는 감사에 대한 데이터를 분석할 수 있습니다. 관리 계정 기능을 단독으로 사용하거나 인증 및 권한 부여 기능과 함께 사용할 수 있습니다.

  ASA RADIUS 서버 개체 또는 그룹 생성 또는 편집을 클릭하여 새 서버 그룹을 생성할 수 있습니다.

### 연결 프로파일에 대한 인증서 인증 구성

**Note** 이 섹션은 **Authentication Type(**인증 유형**)**이 **AAA Only(AAA**만**)**인 경우에는 적용되지 않습니다.

클라이언트 디바이스에 설치된 인증서를 사용해 원격 액세스 VPN 연결을 인증할 수 있습니다.

클라이언트 인증서를 사용하는 경우에도 보조 ID 소스, 대체 소스, 권한 부여 및 과금 서버를 구성할 수 있습니다. 이 옵션은 AAA 옵션입니다. 자세한 내용은 ASA RA VPN 연결 프로파일 구성, on page 289을 참조하십시오.

다음은 인증서별 속성입니다. 기본 및 보조 ID 소스에 대해 개별적으로 이러한 속성을 구성할 수 있습니다. 보조 소스 구성은 선택 사항입니다.

- **Username from Certificate(**인증서의 사용자 이름**)**: 다음 중 하나를 선택합니다.
  - **Map Specific Field(**특정 필드 매핑**)**: **Primary Field(**기본 필드**)** 및 **Secondary Field(**보조 필드**)**의 순서대로 인증서 요소를 사용합니다. 기본값은 CN(Common Name) 및 OU(Organizational Unit)입니다. 조직에 대해 작동하는 옵션을 선택합니다. 필드는 서로 결합하여 사용자 이름을 제공하고, 이 이름은 이벤트, 대시보드에서 사용되며 SSL 암호 해독 및 액세스 제어 규칙에서 일치 목적으로 사용됩니다.
  - **Use entire DN (distinguished name) as username(**전체 **DN(**고유 이름**)**을 사용자 이름으로 사용**)**: 시스템은 DN 필드에서 사용자 이름을 자동으로 파생합니다.
- 고급 옵션(**Authentication Type(**인증 유형**)**이 **Client Certificate Only(**클라이언트 인증서 전용**)**인 경우에는 해당되지 않음): **Advanced(**고급**)** 링크를 클릭하고 다음 옵션을 구성합니다.

- **Prefill username from certificate on user login window(**인증서의 사용자 이름을 사용자 로그인 창에 미리 채우기**)**: 사용자에게 인증하라는 메시지를 표시할 때 사용자 이름 필드에 검색된 사용자 이름을 입력할지 여부.
- **Hide username in login window(**로그인 창에서 사용자 이름 숨기기**)**: **Prefill(**미리 채우기**)** 옵션을 선택하면 사용자 이름을 숨길 수 있습니다. 따라서 사용자는 암호 프롬프트에서 사용자 이름을 편집할 수 없습니다.

클라이언트 주소 풀 할당 구성

원격 액세스 VPN에 연결하는 엔드포인트에 대한 IP 주소를 시스템에서 제공할 방법이 있어야 합니다. AAA 서버는 이러한 주소, DHCP 서버, 그룹 정책에 구성된 IP 주소 풀 또는 연결 프로파일에 구성된 IP 주소 풀을 제공할 수 있습니다. 시스템은 순서대로 이 리소스를 시도하고 사용 가능한 주소를 가져올 때 중지했다가 이 주소를 클라이언트에 할당합니다. 따라서 동시 연결 수가 비정상적인 경우에 페일세이프를 생성할 수 있는 여러 가지 옵션을 구성할 수 있습니다.

연결 프로파일에 대한 주소 풀을 구성하려면 다음 방법 중 한 가지 이상을 사용합니다.

- **IPv4 Address Pool(IPv4** 주소 풀**)** 및 **IPv4 Address Pool(IPv4** 주소 풀**)**: 먼저 서브넷을 지정하는 최대 6개의 네트워크 개체를 생성합니다. IPv4 및 IPv6에 대해 별도 풀을 구성할 수 있습니다. 그런 다음, 그룹 정책 또는 연결 프로파일의 **IPv4 Address Pool(IPv4** 주소 풀**)** 및 **IPv6 Address Pool(IPv6** 주소 풀**)** 옵션에서 이러한 개체를 선택합니다. IPv4 및 IPv6 모두 구성할 필요는 없고 지원하려는 주소 체계를 구성하면 됩니다. 또한 그룹 정책 및 연결 프로파일 모두에서 풀을 구성할 필요는 없습니다. 그룹 정책에서는 연결 프로파일 설정을 오버라이드하므로 그룹 정책에서 풀을 구성하는 경우, 연결 프로파일에서 옵션을 비워두십시오. 풀은 나열한 순서대로 사용된다는 점에 유의하십시오. 새 IPv4 또는 IPv6 주소 풀을 생성하려면, IP 주소 풀 생성을 참조하십시오.
- **DHCP Servers(DHCP** 서버**)**: 먼저 RA VPN에 대한 IPv4 주소 범위를 하나 이상 사용하여 DHCP 서버를 구성합니다(DHCP를 사용하여 IPv6 풀을 구성할 수는 없음). 그런 다음, DHCP 서버의 IP 주소로 호스트 네트워크 개체를 생성합니다. 그러면 연결 프로파일의 **DHCP Servers(DHCP** 서버**)** 속성에서 이 개체를 선택할 수 있습니다. 두 개 이상의 DHCP 서버를 구성할 수 있습니다. DHCP 서버에 주소 풀이 여러 개인 경우, 연결 프로파일에 연결하는 새 ASA RA VPN 그룹 정책 생성에서 **DHCP Scope(DHCP** 범위**)** 속성을 사용해 어떤 풀을 사용할지 선택할 수 있습니다. 풀의 네트워크 주소로 호스트 네트워크 개체를 생성합니다. 예를 들어 DHCP 풀에 192.168.15.0/24 및 192.168.16.0/24가 포함된 경우, DHCP 범위를 192.168.16.0으로 설정하면 192.168.16.0/24 서브넷에서 주소가 선택됩니다.

관련 정보**:**

ASA에 대한 엔드 투 엔드 원격 액세스 VPN 구성 프로세스

## *ASA* 디바이스에서 *AnyConnect* 소프트웨어 패키지 관리

원격 액세스 VPN 마법사를 사용하여 AnyConnect 패키지를 업로드하려면 다음 단계 중 하나를 수행할 수 있습니다.

- CDO 저장소에서 패키지를 업로드합니다.

- HTTP, HTTPS, TFTP, FTP, SMB 또는 SCP 프로토콜을 사용하여 서버에서 패키지를 업로드합니다.

CDO 저장소에서 AnyConnect 패키지 업로드

원격 액세스 VPN 구성 마법사는 CDO 저장소에서 운영 체제별로 AnyConnect 패키지를 제공하며, 이러한 패키지를 선택하여 디바이스에 업로드할 수 있습니다. 디바이스가 인터넷 및 적절한 DNS 구성에 액세스할 수 있는지 확인합니다.

참고 표시된 목록에서 원하는 패키지를 사용할 수 없거나 디바이스에서 인터넷에 액세스할 수 없는 경우 AnyConnect 패키지가 미리 로드된 서버를 사용하여 패키지를 업로드할 수 있습니다.

단계 **1** 운영 체제에 해당하는 필드를 클릭하고 AnyConnect 패키지를 선택합니다.

단계 **2** 를 클릭하여 패키지를 업로드합니다. 체크섬이 일치하지 않으면 AnyConnect 패키지 업로드가 실패합니다. 장애에 대한 자세한 내용은 디바이스의 워크플로우 탭을 참조하십시오.

서버에서 ASA로 AnyConnect 패키지 업로드

AnyConnect 클라이언트 소프트웨어 패키지를 컴퓨터에 다운로드하고 ASA에서 액세스할 수 있는 원격 서버에 업로드합니다. 나중에 RA VPN 마법사 또는 ASA 파일 관리 마법사를 사용하여 서버에서 ASA로 AnyConnect 소프트웨어 패키지를 업로드하십시오. 도메인 이름을 사용하는 URL의 경우 디바이스에서 DNS를 올바르게 구성해야 합니다.

ASA RA VPN 마법사는 HTTP, HTTPS, TFTP, FTP, SMB 또는 SCP 프로토콜을 사용한 패키지 업로드를 지원합니다.

파일 업로드에 지원되는 프로토콜의 syntax(명령문):

| 프로토콜 | 구문 | 예 |
|---|---|---|
| HTTP | http://[[path/ ]filename] | http://www.geonames.org/data-sources.html |
| HTTPS | https://[[path/ ]filename] | https://docs.aws.amazon.com/amazov/tagging.html |
| TFTP | tftp://[[path/ ]filename] | tftp://10.10.16.6/ftd/components.html |
| FTP | ftp://[[user[:password]@]server[:port]/[path/ ]filename] | [illegible] |
| SMB | smb://[[path/ ]filename] | smb://10.10.32.145//sambashare/hello.txt |
| SCP | scp://[[user[:password]@]server[/path]/ filename] | scp://rootcisco123@10.10.16.6//root/events_send.py |

### Before you begin

원하는 운영 체제에 대한 "AnyConnect 헤드엔드 배포 패키지"를 다운로드했는지 확인하십시오. 항상 최신 AnyConnect 버전을 다운로드하여 최신 기능, 버그 수정 및 보안 패치가 있는지 확인하십시오. 디바이스에서 패키지를 정기적으로 업데이트합니다.

**Important** ASA 파일 관리 마법사를 사용하여 패키지를 업로드하려는 경우, 다운로드한 후 패키지의 이름을 수정하지 마십시오.

**Note** 운영 체제(Windows, Mac, Linux)별로 AnyConnect 패키지를 하나씩 업로드할 수 있습니다. 지정된 OS 유형의 여러 버전을 업로드할 수는 없습니다.

단계 **1** https://software.cisco.com/download/home/283000185에서 AnyConnect 패키지를 다운로드합니다.

- EULA에 동의하고 K9(암호화된 이미지) 권한이 있는지 확인합니다.
- 운영 체제에 맞는 "AnyConnect Headend Deployment Package" 패키지를 선택합니다. 패키지 이름은 "anyconnect-win-4.7.04056-webdeploy-k9.pkg"와 유사합니다. Windows, macOS 및 Linux용 별도의 헤드엔드 패키지가 있습니다.

단계 **2** AnyConnect 패키지를 원격 서버에 업로드합니다. ASA 디바이스 및 서버에서 네트워크 경로가 있는지 확인합니다.

ASA RA VPN 마법사는 HTTP, HTTPS, TFTP, FTP, SMB 또는 SCP 프로토콜로 패키지 업로드를 지원합니다.

**Important** AnyConnect 패키지를 HTTPS 서버에 업로드하는 경우 다음 단계를 수행해야 합니다.

- ASA 디바이스에서 해당 서버의 신뢰할 수 있는 CA 인증서를 업로드합니다.
- HTTPS 서버에 신뢰할 수 있는 CA 인증서를 설치합니다.

단계 **3** 원격 서버의 URL은 인증 프롬프트가 표시되지 않는 직접 링크여야 합니다. URL이 사전 인증된 경우 RA VPN 마법사의 URL을 지정하여 파일을 다운로드할 수 있습니다.

단계 **4** 원격 서버 IP 주소가 NAT된 경우 원격 서버 위치의 NAT된 공용 IP 주소를 제공해야 합니다.

## ASA에 새 AnyConnect 패키지 업로드

RA VPN 마법사 또는 ASA 파일 관리 마법사를 사용하여 AnyConnect 소프트웨어 패키지를 ASA에 업로드할 수 있습니다.

다음 절차를 사용하여 HTTP 또는 HTTPS 서버에서 ASA 디바이스에 새 AnyConnect 패키지를 업로드합니다.

단계 1 **AnyConnect Package Detected(AnyConnect** 패키지 감지됨**)**에서 Windows, Mac 및 Linux 엔드포인트용 개별 패키지를 업로드할 수 있습니다.

단계 2 해당하는 Platform(플랫폼) 필드에서 Windows, Mac 및 Linux와 호환되는 AnyConnect 패키지가 사전 업로드되는 서버의 경로를 지정합니다. 서버 경로의 예:
'http://<ip_address>:port_number/<folder_name>/anyconnect-win-4.8.01090-webdeploy-k9.pkg',
'https://<ip_address>:port_number/<folder_name>/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg'.

단계 3 를 클릭하여 패키지를 업로드합니다. CDO는 경로에 연결할 수 있고 지정된 파일 이름이 유효한 패키지인지 확인합니다. 검증에 성공하면 AnyConnect 패키지의 이름이 나타납니다. RA VPN 구성에 ASA 디바이스를 추가하면 AnyConnect 패키지를 여기에 업로드할 수 있습니다.

단계 4 **OK(**확인**)**를 클릭합니다. AnyConnect 패키지가 RA VPN 구성에 추가됩니다.

단계 5 5단계부터 ASA RA VPN 구성 생성을 계속 진행합니다.

### What to do next

VPN 연결을 완료하려면 사용자가 해당 워크스테이션에 AnyConnect 클라이언트 소프트웨어를 설치해야 합니다. 자세한 내용은 ASA에서 사용자가 AnyConnect 클라이언트 소프트웨어를 설치할 수 있는 방법 을 참조하십시오.

## 파일 관리 마법사를 사용하여 AnyConnect 패키지 업로드

HTTP, HTTPS, TFTP, FTP, SMB 또는 SCP 서버에서 단일 또는 여러 ASA 디바이스로 AnyConnect 패키지를 업로드하려면 파일 관리 마법사를 사용합니다. AnyConnect 패키지를 여러 ASA 디바이스에 동시에 푸시하려는 경우 대량 업로드가 유용합니다. 자세한 내용은 ASA 파일 관리를 참조하십시오.

**Important** ASA 파일 관리 마법사를 사용하여 패키지를 업로드하려는 경우, 다운로드한 후 패키지의 이름을 수정하지 마십시오.

업로드가 완료되면 ASA RA VPN 구성 마법사를 열고 패키지가 자동으로 탐지되는지 확인합니다. OS 버전에 대해 여러 패키지를 업로드하는 경우 마법사의 드롭다운 목록에 해당 패키지가 나열되어 그중 하나를 선택할 수 있습니다. 그런 다음 RA VPN 구성을 생성하여 디바이스에 구축할 수 있습니다.

## 기존 AnyConnect 패키지 교체

AnyConnect 패키지가 디바이스에 이미 있는 경우 RA VPN 마법사에서 확인할 수 있습니다. 드롭다운 목록에서 운영 체제에 대해 사용 가능한 모든 AnyConnect 패키지를 볼 수 있습니다. 목록에서 기존 패키지를 선택하고 새 패키지로 교체할 수 있지만 새 패키지를 목록에 추가할 수는 없습니다.

**Note** 기존 패키지를 새 패키지로 교체하려면 ASA 디바이스가 연결할 수 있는 네트워크의 서버에 새 AnyConnect 패키지가 이미 업로드되어 있는지 확인합니다.

단계 1 왼쪽의 CDO 내비게이션 바에서 **VPN** > **ASA/FDM** 원격 액세스 **VPN**을 클릭합니다.

단계 2 수정할 RA VPN 구성을 선택하고 **Actions(**작업**)** 아래에서 **Edit(**편집**)**를 클릭합니다.

단계 3 **AnyConnect Packages Detected(AnyConnect** 패키지 탐지됨**)**에서 기존 AnyConnect 패키지 옆에 나타나는 아이콘을 클릭합니다. 운영 체제에 여러 버전의 AnyConnect 패키지가 있는 경우 목록에서 교체할 패키지를 선택하고 **Edit(**편집**)**를 클릭합니다. 해당 필드에서 기존 패키지가 사라집니다.

단계 4 새 AnyConnect 패키지가 사전 로드되는 서버의 경로를 지정하고 을 클릭하여 패키지를 업로드합니다.

단계 5 **OK(**확인**)**를 클릭합니다. 새 AnyConnect 패키지가 RA VPN 구성에 추가됩니다.

단계 6 6단계부터 ASA RA VPN 구성 생성, on page 285로 계속 진행합니다.

## AnyConnect 패키지 삭제

단계 1 왼쪽의 CDO 내비게이션 바에서 **VPN** > **ASA/FDM** 원격 액세스 **VPN**을 클릭합니다.

단계 2 수정할 RA VPN 구성을 선택하고 **Actions(**작업**)** 아래에서 **Edit(**편집**)**를 클릭합니다.

단계 3 **AnyConnect Packages Detected(**탐지된 **AnyConnect** 패키지**)**에서 삭제할 AnyConnect 패키지 옆에 표시되는 아이콘을 클릭합니다. 운영 체제에 여러 버전의 AnyConnect 패키지가 있는 경우 목록에서 삭제할 패키지를 선택합니다. 해당 필드에서 기존 패키지가 사라집니다.

**Note** 삭제 작업을 중지하고 기존 패키지를 유지하려면 **Cancel(**취소**)**을 클릭합니다.

단계 4 **OK(**확인**)**를 클릭합니다.디바이스의 구성 상태가 '동기화되지 않음' 상태입니다.

**Note** 이 단계에서 삭제 작업을 실행 취소하려면 **Inventory(**인벤토리**)** 페이지로 이동하여 **Discard Changes(**변경 사항 취소**)**를 클릭하여 기존 AnyConnect 패키지를 유지합니다.

단계 5 CDO에서 ASA로 구성 변경 사항 구축.

## 온보딩된 **ASA** 디바이스의 **RA VPN** 구성 읽기

이미 RA VPN 설정이 있는 ASDM 관리형 ASA 디바이스를 온보딩하면 기존 원격 액세스 VPN 구성을 검색하고 표시합니다. CDO는 "기본 RA VPN 구성"을 자동으로 생성하고 ASA 디바이스를 이 구성과 연결합니다. CDO에서 읽히지 않거나 지원되지 않지만 CDO 명령줄 인터페이스에서 구성할 수 있는 일부 RA VPN 구성이 있습니다.

**Note** 이 섹션에서는 CDO에서 지원되거나 지원되지 않는 모든 구성을 다루지는 않습니다. 대신 가장 일반적으로 사용되는 항목만 설명합니다.

온보딩된 ASA에서 RA VPN 구성을 보려면, 다음 단계를 수행합니다.

단계 **1** CDO 인터페이스에서 **VPN** > **ASA/FDM Remote Access VPN Configuration(ASA/FDM** 원격 액세스 **VPN** 구성**)**으로 이동합니다.

단계 **2** 온보딩된 ASA 디바이스에 해당하는 RA VPN 구성을 클릭합니다. CDO는 "기본 **RA VPN** 구성"을 자동으로 생성하고 ASA 디바이스를 이 구성과 연결합니다. 기본 구성을 삭제할 수 있습니다. CDO에서 읽는 ASA RA VPN 구성은 다음과 같이 분류됩니다.

- 디바이스 설정
- 연결 프로파일
- 그룹 정책

디바이스 설정

온보딩된 ASA 디바이스와 연결된 RA VPN 구성이 **Default_RA_VPN_Configuration**에 나타납니다. 해당 구성과 연결된 ASA 디바이스(오른쪽의 **Devices(**디바이스**)** 창에서)의 이름을 보려면 이 구성을 클릭해야 합니다. 편집 버튼을 클릭하여 ASA 디바이스에 있는 AnyConnect 패키지를 확인할 수도 있습니다.

연결 프로파일

CDO는 ASA 디바이스의 "AnyConnect 클라이언트 VPN 액세스"에 정의된 연결 프로파일을 지원하고 읽습니다. "클라이언트리스 SSL VPN 액세스" 구성은 지원되지 않습니다.

연결 프로파일 속성을 보려면 다음을 수행합니다.

단계 **1** **Default_RA_VPN_Configuration**을 확장합니다.

단계 **2** 원하는 연결 프로파일 중 하나를 클릭하고 **Edit(**편집**)**를 클릭합니다.

모든 기본 및 고급 ASA RA VPN 속성은 CDO RA VPN 구성 페이지의 연결 프로파일 이름 및 세부 정보에서 확인할 수 있습니다.

**Note** 기본 구성을 삭제할 수 있습니다(기본 RA VPN 구성을 선택하고 오른쪽의 **Actions(**작업**)** 창에서 **Remove(**제거**)** 클릭).

기본 *ID* 소스

- CDO는 **Connection Aliases(**연결 별칭**)** 및 **Group URLs(**그룹 **URL)** 속성을 **Group Alias(**그룹 별칭**)** 및 **Group URL(**그룹 **URL)**로 읽습니다.

**Note**

- SAML, 다중 인증서 및 AAA, 다중 인증서로 구성된 연결 프로파일은 읽을 수 없습니다.
- 인터페이스 및 서버 그룹이 있는 인증 서버 그룹은 지원되지 않습니다.

- CDO는 기본 **ID** 소스에서 "AAA", "AAA 및 인증서" 및 "인증서 전용" 인증 방법으로 구성된 AnyConnect 연결 프로파일을 지원합니다.
- **AAA** 서버 그룹은 CDO에서 기본 **ID** 소스의 사용자 인증을 위한 기본 **ID** 소스로 읽힙니다(인증 유형으로 **AAA** 또는 **AAA** 및 클라이언트 인증서를 선택하여 이 속성을 확인할 수 있음).
  - **AAA** 서버 그룹이 로컬이 아닌 다른 항목으로 구성된 경우 CDO는 이 특성을 읽고 **Primary Identity Source(**기본 **ID** 소스**)** 아래의 **Fallback Local Identity Source(**대체 로컬 **ID** 소스**)** 필드에 이 속성을 표시합니다. (인증 유형으로 **AAA**를 선택하여 이 속성을 확인할 수 있습니다.)

    CDO에서 읽은 서버 그룹 특성에 대한 자세한 내용은 AAA 서버 그룹을 참조하십시오.

보조 **ID** 소스

**Secondary Identity Source(**보조 **ID** 소스**)**에는 ASA 디바이스의 보조 인증 속성이 표시됩니다. 이러한 속성을 보려면 인증 유형으로 **AAA** 또는 **AAA and Client Certificate(**클라이언트 인증서**)**를 선택하고 **View Secondary Identity Source(**보조 **ID** 소스 보기**)**를 클릭합니다.

- **Secondary Identity Source for User Authentication(**사용자 인증을 위한 보조 **ID** 소스**)**에 보조 인증 **Server Group(**서버 그룹**)** 속성이 표시됩니다.
  - 서버 그룹이 LOCAL(로컬) 이외의 항목으로 구성된 경우 CDO는 이 특성을 읽고 **Secondary Identity Source(**보조 **ID** 소스**)** 아래의 **Fallback Local Identity Source for Secondary(**보조 **ID** 소스에 대한 대체 로컬 **ID** 소스**)** 필드에 이 속성을 표시합니다.
- CDO는 **Attribute Server(**속성 서버**)** 및 **Interface-Specific Authorization Server Groups(**인터페이스별 권한 부여 서버 그룹**)** 속성을 지원하지 않습니다.

CDO에서 읽은 서버 그룹 특성에 대한 자세한 내용은 AAA 서버 그룹을 참조하십시오.

권한 부여 서버

- **Authorization Server(**권한 부여 서버**)**에 권한 부여 **Server Group(**서버 그룹**)** 속성이 표시됩니다.
- CDO는 인터페이스 및 서버 그룹이 있는 권한 부여 서버 그룹을 지원하지 않습니다.

CDO에서 읽은 RADIUS 서버 그룹 특성에 대한 자세한 내용은 RADIUS 서버 그룹을 참조하십시오.

계정 관리 서버

**Accounting Server(**과금 서버**)**에 과금 서버 그룹 속성이 표시됩니다. CDO에서 읽은 서버 그룹 특성에 대한 자세한 내용은 RADIUS 서버 그룹을 참조하십시오.

클라이언트 주소 풀 할당

CDO는 **Client Address Assignment(**클라이언트 주소 할당**)** 속성(**DHCP** 서버, 클라이언트 주소 풀 및 클라이언트 **IPv6** 주소 풀)을 개체로 읽습니다. (이러한 속성은 **Client Address Pool Assignment(**클라이언트 주소 풀 할당**)**에서 확인할 수 있습니다.) DHCP 서버 세부 정보는 리터럴로 읽힙니다.

**Note** CDO는 특정 인터페이스에 할당된 IP 주소 풀을 지원하지 않습니다. 그러나 이러한 속성은 ASA CLI(명령줄 인터페이스)에서 확인할 수 있습니다.

### *AAA* 서버 그룹

CDO는 LDAP 서버 그룹 및 연결된 LDAP 서버를 **Active Directory** 영역 개체로 나타냅니다. AD(Active Directory)의 경우 영역은 Active Directory 도메인과 동일합니다. CDO는 이미 존재하는 AD 영역 개체의 AD 비밀번호를 읽습니다.

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2** 이 개체를 보려면 **Active Directory Realms(Active Directory** 영역**)** 필터를 적용합니다.

단계 **3** 원하는 Active Directory 영역 개체를 선택하고 **Edit(**편집**)**를 클릭하여 세부 정보를 확인합니다.

#### What to do next

AD 영역에 연결된 AD 서버 및 해당 구성이 포함되어 있음을 확인할 수 있습니다. AD 영역에 대해 여러 AD(Active Directory) 서버가 있는 경우 AD 서버는 서로 중복되어야 하며 동일한 AD 도메인을 지원해야 합니다. 따라서 **Directory Name(**디렉터리 이름**)**, **Directory Password(**디렉터리 비밀번호**)**, **Base Distinguished Name(**기본 고유 이름**)**과 같은 기본 영역 속성은 해당 AD 영역과 연결된 모든 AD 서버에서 동일해야 합니다. 이러한 속성이 동일하지 않은 경우 CDO는 Active Directory 영역 개체에 경고 메시지를 표시합니다. AD 서버 전체에서 일관성을 유지하려면 이러한 속성을 수정해야 합니다. 이 경고를 해결하지 않고 계속 진행하면 CDO는 AD 서버 속성 중 하나를 사용하여 해당 영역 개체의 다른 서버에 적용합니다.

### *RADIUS* 서버 그룹

ASA 디바이스의 AAA RADIUS 서버 그룹 속성은 CDO에서 RADIUS 서버 그룹 개체로 읽힙니다.

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2** 이 개체를 보려면 **RADIUS** 서버 그룹필터를 적용합니다.

단계 **3** 원하는 개체를 선택한 다음 **Edit(**편집**)**를 클릭하여 세부 정보를 확인합니다.

- ASA에서 **Enable dynamic authorization(**동적 권한 부여 활성화**)**는 CDO에서 **Dynamic Authorization(**동적 권한 부여**)(RA VPN**에만 해당**)**으로 읽힙니다.
- **Reactivation Mode(**재활성화 모드**)**의 **Depletion(**감소**)** 옵션은 CDO에서 읽히므로, 감소 시간과 관련된 **Dead Time(**데드 타임**)** 값은 CDO에서 읽힙니다. 그러나 **Timed(**시간 제한**)** 속성은 CDO에서 읽히지 않습니다.
- CDO **Accounting Mode(**계정 관리 모드**)**, **Timed(**시간 제한**)**, **Enable interim accounting update(**임시 계정 업데이트 활성화**)**, **Enable interim accounting update(**임시 계정 업데이트 활성화**)** 및 **Use authorization only mode(**권한 부여 전용 모드 사용**)**을 지원하지 않습니다.

---

*RADIUS* 서버

CDO는 ASA에서 Radius 서버를 읽을 때 이름을 "Radius 서버 group_server 이름 또는 IP 주소의 이름"으로 지정하는 Radius 서버 개체를 생성합니다.

---

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2** 이 개체를 보려면 **RADIUS Server(RADIUS** 서버**)** 필터를 적용합니다.

단계 **3** 원하는 개체를 선택한 다음 **Edit(**편집**)**를 클릭하여 세부 정보를 확인합니다.

---

그룹 정책

**Group Policy(**그룹 정책**)** 섹션에서 드롭다운을 클릭하여 디바이스와 연결된 그룹 정책을 확인합니다.

**Attention** CDO는 터널링 프로토콜로 구성된 그룹 정책을 **SSL VPN** 클라이언트로 읽습니다.

CDO는 ASA에 구성된 대부분의 그룹 정책 속성을 읽습니다. 이 정보는 RA VPN 그룹 정책 마법사의 여러 탭에 표시됩니다. ASA 디바이스에서 읽은 그룹 정책의 세부 정보를 보려면 다음을 수행해야 합니다.

---

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**) > FTD Network Objects(FTD** 네트워크 개체**)**을 클릭합니다.

단계 **2** **RA VPN Group Policy(RA VPN** 그룹 정책**)**를 기준으로 필터링합니다.

단계 **3** 해당 디바이스와 연결된 그룹 정책을 선택하고 **Edit(**편집**)**를 클릭합니다.

---

### What to do next

**Note** CDO는 ASA 디바이스의 스플릿 터널링에 정의된 표준 ACL(Access Control List)을 지원하지 않습니다. ACL(Extended Access Control List)을 지원하며 ASA 정책에서 ACL로 읽습니다. 자세한 내용은 ASA RA VPN 그룹 정책 속성을 참조하십시오. 정책을 보려면 내비게이션 바에서 **Policies(**정책**)** > **ASA Access Policies(ASA** 액세스 정책**)**를 클릭합니다.

확장 ACL을 선택하려면 다음을 수행합니다.

- **Split Tunneling(**스플릿 터널링**)** 탭을 클릭합니다.
- ASA의 트래픽이 IPv4 주소를 사용하는지 IPv6 주소를 사용하는지에 따라 해당 드롭다운 목록에서 "Allow specified traffic over tunnel(터널을 통한 지정된 트래픽 허용)" 또는 "Exclude networks specified below(아래에 지정된 네트워크 제외)"를 선택합니다. ASA에서 가져온 확장 ACL을 선택합니다.

## IP 주소 풀 생성

VPN 연결을 사용하여 네트워크에 원격으로 연결하는 클라이언트에 할당하도록 ASA에 대한 IPv4 및 IPv6 IP 주소 풀을 구성할 수 있습니다. 풀을 지정하는 순서는 중요합니다. 연결 프로파일 또는 그룹 정책에 대해 둘 이상의 주소 풀을 구성한 경우 ASA에서는 ASA에 추가된 순서대로 주소 풀을 사용합니다.

IPv4 주소 풀을 정의하려면 IP 주소 범위를 제공합니다. IPv4 주소 풀의 예는 10.10.147.100 - 10.10.147.177입니다.

IPv6 주소 풀을 정의하려면 시작 IP 주소 범위, 주소 접두사 및 풀에 구성할 수 있는 주소 수를 지정합니다. IPv6 주소 풀의 예는 2001:DB8:1::1입니다.

로컬이 아닌 서브넷에서 주소를 할당할 경우 이러한 네트워크에 대한 경로를 보다 쉽게 추가할 수 있도록 서브넷 경계에 속하는 풀을 추가하는 것이 좋습니다.

IP 주소 풀을 생성하려면 다음을 수행합니다.

단계 **1** 좌측의 CDO 내비게이션 바에서, **Objects(**개체**)** > **ASA Objects(ASA** 개체**)**을 클릭합니다.

단계 **2** 파란색 더하기 버튼  을 클릭하고 **ASA** > **Address Pool(ASA** 주소 풀**)**을 선택합니다.

단계 **3** **Create IP Address Pool(IP** 주소 풀 생성**)** 대화 상자에서 다음 정보를 입력합니다.

- **Object Name(**개체 이름**)** - 주소 풀의 이름을 입력합니다. 최대 64자까지 입력할 수 있습니다.
- **IPv4 address pool(IPv4** 주소 풀**)**: IPv4 주소 풀을 구성하려면 이 라디오 버튼을 선택합니다.
  - **IPv4 Address Range(IPv4** 주소 범위**)**: 구성된 각 풀에서 사용 가능한 첫 번째 IP 주소와 마지막 IP 주소를 입력합니다. 예: 10.10.147.100 - 10.10.147.177.
  - **Mask(**마스크**)** - 이 IP 주소 풀이 있는 서브넷을 식별합니다.

- **IPv6 address pool(IPv6** 주소 풀**)**: IPv6 주소 풀을 구성하려면 이 라디오 버튼을 선택합니다.
  - **IPv6** 주소: 구성된 풀에서 사용한 첫 번째 IP 주소 및 접두어 길이를 비트로 입력합니다. <address>/<prefix> 형식. 예: 2001:DB8:1::1/3.
  - **Number of Addresses(**주소 수**)** - 풀에 있는 IP 주소부터 시작하여 IPv6 주소의 수를 식별합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

---

원격 액세스 **VPN** 인증서 기반 인증

원격 액세스 VPN은 다음 시나리오에서 보안 게이트웨이 및 AnyConnect 클라이언트(종단)를 인증하기 위해 디지털 인증서를 사용합니다.

중요 CDO는 VPN 헤드엔드(ASA )에서 디지털 인증서 설치를 처리합니다. AnyConnect 클라이언트 디바이스에 대한 인증서 설치는 처리하지 않습니다. 조직의 관리자가 이를 처리해야 합니다.

- VPN 헤드엔드 디바이스(ASA ) 식별 및 인증:

  VPN 헤드엔드는 AnyConnect 클라이언트가 VPN 연결을 요청할 때 자신을 식별하고 인증하기 위해 ID 인증서가 필요합니다. CDO를 사용하여 디바이스에 ID 인증서를 설치해야 합니다. PKCS12 또는 인증서 및 키를 사용하여 ID 인증서 설치를 참조하십시오. AnyConnect 클라이언트에 발급자의 CA 인증서를 반드시 설치해야 하는 것은 아닙니다.

  CDO에서 원격 액세스 VPN 구성을 생성하는 동안 등록된 ID 인증서를 디바이스의 외부 인터페이스에 할당하고 구성을 디바이스로 다운로드합니다. ID 인증서는 디바이스의 외부 인터페이스에서 완전히 작동합니다.

  AnyConnect 클라이언트가 VPN에 연결을 시도하면 디바이스는 AnyConnect 클라이언트에 ID 인증서를 제공하여 자체적으로 인증합니다. AnyConnect 클라이언트는 신뢰할 수 있는 CA 인증서로 이 ID 인증서를 확인하고 인증서와 디바이스를 신뢰합니다. CA 인증서가 AnyConnect 클라이언트에 설치되어 있지 않은 경우 메시지가 표시되면 사용자는 디바이스를 수동으로 신뢰해야 합니다.

- AnyConnect 클라이언트 식별 및 인증:

참고 이는 RA VPN 구성의 연결 프로파일에서 인증 방법으로 "클라이언트 인증서 전용" 또는 "AAA 및 클라이언트 인증서"를 사용하는 경우에 적용됩니다. "AAA 전용"에는 적용되지 않습니다.

  디바이스가 신뢰되면 AnyConnect 클라이언트는 VPN 연결을 완료하기 위해 스스로를 인증해야 합니다. AnyConnect 클라이언트에 ID 인증서를 설치하고 CDO를 사용하여 디바이스에 신뢰할 수 있는 CA 인증서를 설치해야 합니다. 동일한 인증 기관이 이러한 인증서를 발급해야 합니다. ASA에서 신뢰할 수 있는 CA 인증서 설치를 참조하십시오.

AnyConnect 클라이언트는 ID 인증서를 제시하고 디바이스는 신뢰할 수 있는 CA 인증서로 이 인증서를 확인하고 VPN 연결을 설정합니다.

## NAT에서 원격 액세스 트래픽 제외

NAT 제외를 구성하여 NAT 변환에서 원격 액세스 VPN 엔드포인트로 오가는 트래픽을 제외합니다. NAT에서 VPN 트래픽을 제외하지 않는 경우 내부 인터페이스와 외부 인터페이스에 대한 기존 NAT 규칙이 주소의 RA VPN 풀에 적용되지 않는지 확인합니다. NAT 제외 규칙은 지정된 소스/대상 인터페이스 및 네트워크 조합에 대한 수동 고정 ID NAT 규칙이며 NAT 정책에서는 반영되지 않고 숨겨집니다. NAT 제외를 활성화하는 경우에는 다음 항목도 구성해야 합니다.

- 내부 인터페이스: 원격 사용자가 액세스할 내부 네트워크의 인터페이스를 선택합니다. NAT 규칙은 이러한 인터페이스에 대해 생성됩니다.
- 내부 네트워크: 원격 사용자가 액세스할 내부 네트워크를 나타내는 네트워크 개체를 선택합니다. 네트워크 목록에는 지원할 주소 풀과 동일한 IP 유형이 포함되어 있어야 합니다.

### 시작하기 전에

해당 디바이스의 연결 프로파일 및 그룹 정책에서 사용되는 로컬 IP 주소 풀의 구성과 일치하는 ASA 네트워크 개체를 생성합니다. 이러한 네트워크 개체는 NAT 규칙을 구성할 때 대상 주소 및 변환된 주소로 할당되어야 합니다. 새 네트워크 개체 생성, 125 페이지의 내용을 참조하십시오.

---

단계 **1** CDO 탐색 모음에서 **Inventory(재고 목록)**를 클릭합니다.

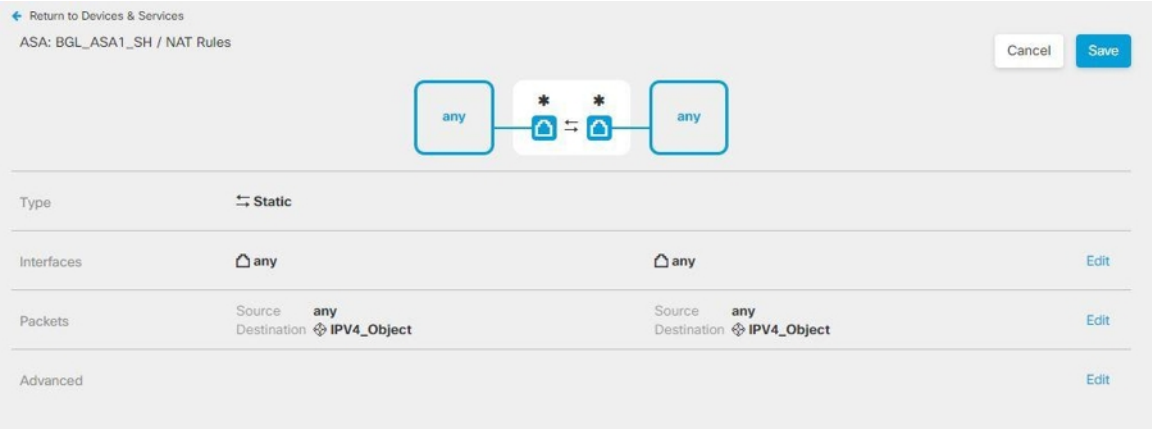
단계 **2** **Inventory(재고 목록)** 필터 및 검색 필드를 사용하여 NAT 규칙을 생성하려는 ASA 디바이스를 찾습니다.

단계 **3** 상세정보 패널의 **Management(관리)** 영역에서 **NAT** NAT를 클릭합니다.

단계 **4**  > **Twice NAT(2회 NAT)**를 클릭합니다.

1. 섹션 1에서 **Static(정적)**을 선택합니다. **Continue(계속)**를 클릭합니다.
2. 섹션 2에서 **Source Interface(소스 인터페이스)** = 'any' 및 **Destination Interface(대상 인터페이스)** = 'any'를 선택합니다. **Continue(계속)**를 클릭합니다.
3. 섹션 3에서 **Source Original Address(소스 원본 주소)** = 'any' 및 **Source Translated Address(소스 변환 주소)** = 'any'를 선택합니다.
4. **Use Destination(대상 사용)**을 선택합니다.
    1. **Destination Original Address(대상 원본 주소)** 및 **Source Translated Address(소스 변환 주소)**: 드롭다운에서 **Choose(선택)**를 클릭하고 로컬 IP 주소 풀의 구성과 일치하는 네트워크 개체를 선택합니다. 아래 예에서 'IPV4_Object'는 ASA(BGL_ASA1_SH) 디바이스의 연결 프로파일 및 그룹 정책 설정에서 사용되는 IPv4 주

소 풀 개체와 동일한 구성을 가진 네트워크 개체입니다.




2. **Disable proxy ARP for Incoming packet(**수신 패킷에 대해 프록시 **ARP** 비활성화**)**을 선택합니다.
3. **Save(**저장**)**를 클릭합니다.
4. 4단계부터 프로세스를 반복하여 IP 주소 풀에 해당하는 다른 각 네트워크 개체에 대해 동일한 규칙을 생성합니다.

단계 **5** CDO에서 ASA로 구성 변경 사항 구축.

---

**ASA**에서 사용자가 **AnyConnect** 클라이언트 소프트웨어를 설치할 수 있는 방법

VPN 연결을 완료하려면 사용자가 AnyConnect 클라이언트 소프트웨어를 설치해야 합니다. 기존 소프트웨어 배포 방법을 사용하여 소프트웨어를 직접 설치할 수 있습니다. 또는 사용자가 ASA 디바이스에서 AnyConnect 클라이언트를 직접 설치하게 할 수도 있습니다.

**Note** 소프트웨어를 설치하려면 사용자에게 워크스테이션에 대한 관리자 권한이 있어야 합니다.

사용자가 ASA 디바이스에서 소프트웨어를 처음 설치하도록 하려면 사용자에게 다음 단계를 수행하도록 하십시오.

**Note** Android 및 iOS 사용자는 해당 앱 스토어에서 AnyConnect를 다운로드해야 합니다.

---

단계 **1** 웹 브라우저를 사용하여 **https://** *ravpn-address*를 엽니다. 여기서 *ravpn-address*는 VPN 연결을 허용할 외부 인터페이스의 IP 주소 또는 호스트 이름입니다. 원격 액세스 VPN을 구성할 때 이 인터페이스를 식별합니다. 시스템에서 사용자에게 로그인하라는 메시지를 표시합니다.

단계 **2** 사이트에 로그인합니다. 사용자는 원격 액세스 VPN용으로 구성된 디렉터리 서버를 사용하여 인증을 합니다. 로그인이 성공해야 설치를 계속할 수 있습니다. 로그인이 성공하면 시스템은 사용자에게 필요한 AnyConnect 클라이언

트 버전이 이미 있는지를 확인합니다. 사용자 컴퓨터에 AnyConnect 클라이언트가 없거나 클라이언트가 하위 레벨인 경우에는 시스템에서 AnyConnect 소프트웨어 설치를 자동으로 시작합니다. 설치가 완료되면, AnyConnect에서 원격 액세스 VPN 연결을 완료합니다.

## 온보딩된 ASA의 원격 액세스 VPN 구성 수정

ASA 디바이스가 CDO에 온보딩되면 온보딩된 ASA 디바이스에서 기존 원격 액세스 VPN 구성을 검색하고 표시합니다. 자세한 내용은 온보딩된 ASA 디바이스의 RA VPN 구성 읽기, 298 페이지을 참고하십시오.

이러한 구성을 수정하고 새 구성을 디바이스에 다운로드할 수 있습니다.

- ASA RA VPN 구성 수정
- ASA 연결 프로파일 수정

### 원격 액세스 *VPN* 구성 수정

단계 **1** 왼쪽의 CDO 내비게이션 바에서 **VPN** > **Remote Access VPN Configuration(**원격 액세스 **VPN** 구성**)**을 클릭합니다.

단계 **2** VPN 구성에 그룹 정책을 추가하거나 제거하려면 온보딩된 ASA 디바이스와 연결된 VPN 구성을 클릭합니다. 왼쪽의 Actions(작업) 창에서 **Group Policies(**그룹 정책**)**를 클릭합니다.

a) 파란색 + 아이콘을 클릭하고 선택 항목을 구성한 다음 Select(선택)를 클릭합니다.

b) Save(저장)를 클릭합니다. 새 ASA RA VPN 그룹 정책 생성할 수도 있습니다.

단계 **3** VPN 구성을 클릭하고 왼쪽의 **Actions(**작업**)** 창에서 **Edit(**편집**)**를 클릭합니다.

마법사는 구성과 연결된 ASA 디바이스를 나열합니다.

a) 생성된 것과 동일한 방식으로 다음 세부 정보를 수정할 수 있습니다.

- RA VPN 구성의 이름을 변경합니다.
- 디바이스 세부 정보를 표시하는 행에 나타나는 점 3개를 클릭하고 **Edit(**편집**)**를 클릭합니다.

자세한 내용은 ASA RA VPN 구성 생성, 285 페이지 항목을 참조하십시오.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, 352 페이지

### *ASA* 연결 프로파일 수정

단계 **1** 왼쪽의 CDO 내비게이션 바에서 **VPN** > **Remote Access VPN Configuration(**원격 액세스 **VPN** 구성**)**을 클릭합니다.

단계 **2** 온보딩된 ASA 디바이스와 연결된 VPN 구성을 확장하고 연결 프로파일을 선택합니다.

단계 **3** 왼쪽의 **Actions(**작업**)** 창에서 **Edit(**편집**)**를 클릭합니다.

단계 **4** 생성된 것과 동일한 방식으로 값을 편집하고 **Done(**완료**)**을 클릭합니다.

자세한 내용은 ASA RA VPN 연결 프로파일 구성, 289 페이지을 참조해 주십시오.

단계 **5** 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, 352 페이지

## RA VPN AnyConnect 클라이언트 프로파일 업로드

원격 액세스 VPN AnyConnect 클라이언트 프로파일은 파일에 저장된 구성 매개변수의 그룹입니다. 핵심 클라이언트 VPN 기능과 선택적 클라이언트 모듈인 Network Access Manager, AMP Enabler, ISE Posture, 네트워크 가시성, 고객 피드백 경험 프로파일, Umbrella 로밍 보안 및 웹 보안에 대한 구성 설정을 포함하는 다양한 AnyConnect 클라이언트 프로파일이 있습니다.

CDO는 이러한 프로파일을 나중에 그룹 정책에서 사용할 수 있는 개체로 업로드할 수 있습니다.

- **AnyConnect VPN** 프로파일 — AnyConnect 클라이언트 프로파일은 AnyConnect 클라이언트 소프트웨어와 함께 클라이언트에 다운로드됩니다. 이러한 프로파일은 시작 시의 자동 연결 및 자동 다시 연결, 그리고 엔드 유저가 AnyConnect 클라이언트 환경 설정 및 고급 설정에서 옵션을 변경할 수 있는지 여부와 같은 여러 클라이언트 관련 옵션을 정의합니다. CDO는 XML 파일 형식을 지원합니다.
- **AMP Enabler** 서비스 프로파일 - 이 프로파일은 AnyConnect AMP Enabler에 사용됩니다. 원격 액세스 VPN 사용자가 VPN에 연결하면 AMP Enabler 및 이 프로파일이 FDM 관리 디바이스에서 엔드 포인트로 푸시됩니다. CDO는 XML 및 ASP 파일 형식을 지원합니다.
- 피드백 프로파일 - 고객 경험 피드백 프로파일을 추가하고 이 유형을 선택하여 고객이 활성화하고 사용하는 기능 및 모듈에 대한 정보를 수신할 수 있습니다. CDO는 FSP 파일 형식을 지원합니다.
- **ISE Posture** 프로파일 - AnyConnect ISE Posture 모듈용 프로파일 파일을 추가하는 경우 이 옵션을 선택합니다. CDO는 XML 및 ISP 파일 형식을 지원합니다.
- **Network Access Manager** 서비스 프로파일 - Network Access Manager 프로파일 편집기를 사용하여 NAM 프로파일 파일을 설정하고 추가합니다. CDO는 XML 및 NSP 파일 형식을 지원합니다.
- 네트워크 가시성 서비스 프로파일 - AnyConnect 네트워크 가시성 모듈의 프로파일 파일입니다. NVM 프로파일 편집기를 사용하여 프로파일을 생성할 수 있습니다. CDO는 XML 및 NVMSP 파일 형식을 지원합니다.
- **Umbrella** 로밍 보안 프로파일 - Umbrella 로밍 보안 모듈을 구축하는 경우 이 파일 유형을 선택해야 합니다. CDO는 XML 및 JSON 파일 형식을 지원합니다.
- 웹 보안 서비스 프로파일 - 웹 보안 모듈용 프로파일 파일을 추가할 때 이 파일 유형을 선택합니다. CDO는 XML, WSO 및 WSP 파일 형식을 지원합니다.

### Before you begin

적합한 GUI 기반 AnyConnect 프로필 편집기를 사용하여 필요한 프로파일을 생성합니다. AnyConnect Secure Mobility Client 범주의 Cisco 소프트웨어 다운로드 센터에서 프로파일 편집기를 다운로드하고 AnyConnect "프로파일 편집기 - Windows/독립형 설치 프로그램(MSI)"을 설치할 수 있습니다. 프로파일 편집기 설치 프로그램에는 독립형 버전의 프로파일 편집기가 포함되어 있습니다. 설치 파일은

Windows 전용이며 파일 이름은 anyconnect-profileeditor-win-<version>-k9.msi입니다. 여기서 <version>은 AnyConnect 버전입니다. 예를 들면 anyconnect-profileeditor-win-4.3.04027-k9.msi와 같습니다. 또한 프로파일 편집기를 설치하기 전에 Java JRE 1.6 이상도 설치해야 합니다.

Umbrella 로밍 보안 프로파일 편집기를 제외하고 이 패키지에는 모듈을 생성하는 데 필요한 모든 프로파일 편집기가 포함되어 있습니다. 자세한 내용은 Cisco AnyConnect Secure Mobility Client 관리자 가이드에서 해당 릴리스의 *AnyConnect* 프로파일 편집기 장을 참조하십시오. Umbrella 대시보드와 별도로 Umbrella 로밍 보안 프로파일을 다운로드합니다. 자세한 내용은 Cisco Umbrella 사용 설명서의 "Umbrella 로밍 보안" 장에서 "Umbrella 대시보드에서 AnyConnect 로밍 보안 프로필 다운로드" 섹션을 참고하십시오.

단계 **1** 좌측의 CDO 내비게이션 바에서 **Objects(**개체**) > FDM Objects(FDM** 개체**)**를 클릭합니다.

단계 **2** 파란색 더하기  버튼을 클릭합니다.

단계 **3** **RA VPN Objects (ASA & FDM)(RA VPN** 개체**(ASA** 및 **FDM)) > AnyConnect Client Profile(AnyConnect** 클라이언트 프로파일**)**를 클릭합니다.

단계 **4** **Object Name(**개체 이름**)** 필드에 AnyConnect 클라이언트 프로파일의 이름을 입력합니다.

단계 **5** **Browse(**찾아보기**)**를 클릭하고 프로파일 편집기를 사용하여 생성한 파일을 선택합니다.

단계 **6** **Open(**열기**)**을 클릭하여 프로파일을 업로드합니다.

단계 **7** **Add(**추가**)**를 클릭하여 개체를 추가합니다.

관련 정보**:**

- RA VPN 그룹 정책 창에서 클라이언트 모듈을 AnyConnect VPN 프로파일과 연결합니다. 새 ASA RA VPN 그룹 정책 생성 을 참조하십시오.

**Note** 클라이언트 모듈 연결은 소프트웨어 버전 6.7 이상을 실행하는 모든 ASA 버전 및 FDM에서 지원됩니다.

## ASA의 원격 액세스 VPN 구성 확인

원격 액세스 VPN을 구성하고 디바이스에 구성을 배포한 후에는 원격 연결을 수행할 수 있는지 확인합니다.

단계 **1** 외부 네트워크에서 AnyConnect 클라이언트를 사용하여 VPN 연결을 설정합니다. 웹 브라우저를 사용하여 **https://** *ravpn-address*를 엽니다. 여기서 *ravpn-address*는 VPN 연결을 허용할 외부 인터페이스의 IP 주소 또는 호스트 이름입니다. 필요한 경우, 클라이언트 소프트웨어를 설치하여 연결을 완료합니다. ASA에서 사용자가 AnyConnect 클라이언트 소프트웨어를 설치할 수 있는 방법 을 참조하십시오. 그룹 URL을 구성한 경우, 그룹 URL도 시도해 보십시오.

단계 **2** **Devices & Services(**디바이스 및 서비스**)** 페이지에서, 확인하려는 디바이스(FTD 또는 ASA)를 선택하고 디바이스 작업**(Device Actions)** 아래의 **Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **3** **show vpn-sessiondb** 명령을 사용하여 현재 VPN 세션에 대한 요약 정보를 봅니다.

단계 **4** 통계에는 활성 AnyConnect 클라이언트 세션, 누적 세션에 대한 정보, 최대 동시 세션 수, 비활성 세션이 표시되어야 합니다. 다음은 명령의 샘플 출력입니다.

```
> show vpn-sessiondb
----------------------------------------------------------------------------
VPN Session Summary
----------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ----------------------------------------------
AnyConnect Client          :      1 :         49 :          3 :        0
  SSL/TLS/DTLS             :      1 :         49 :          3 :        0
Clientless VPN             :      0 :          1 :          1
  Browser                  :      0 :          1 :          1
----------------------------------------------------------------------------


  Total Active and Inactive    :      1            Total Cumulative :     50
  Device Total VPN Capacity    :  10000
  Device Load                  :     0%
  ----------------------------------------------------------------------------

  ----------------------------------------------------------------------------
  Tunnels Summary
  ----------------------------------------------------------------------------
                               Active : Cumulative : Peak Concurrent
                              ----------------------------------------
  Clientless                  :      0 :          1 :               1
  AnyConnect-Parent           :      1 :         49 :               3
  SSL-Tunnel                  :      1 :         46 :               3
  DTLS-Tunnel                 :      1 :         46 :               3
  ----------------------------------------------------------------------------
  Totals                      :      3 :        142
  ----------------------------------------------------------------------------

  ----------------------------------------------------------------------------
  IPv6 Usage Summary
  ----------------------------------------------------------------------------
                               Active : Cumulative : Peak Concurrent
                              ----------------------------------------
  AnyConnect SSL/TLS/DTLS     :      :            :
    Tunneled IPv6             :      1 :         20 :               2
  ----------------------------------------------------------------------------
```

단계 **5** **show vpn-sessiondb anyconnect** 명령을 사용하여 현재 AnyConnect VPN 세션에 대한 세부 정보를 봅니다. 세부 정보에는 사용된 암호화, 전송 및 수신한 바이트 수, 기타 통계 정보가 포함됩니다. VPN 연결을 사용하면 이 명령을 다시 호출할 경우 전송/수신한 바이트 수 변경 사항이 표시되어야 합니다.

단계 **6** **show vpn-sessiondb anyconnect** 명령을 사용하여 현재 AnyConnect VPN 세션에 대한 세부 정보를 봅니다. 세부 정보에는 사용된 암호화, 전송 및 수신한 바이트 수, 기타 통계 정보가 포함됩니다. VPN 연결을 사용하면 이 명령을 다

시 호출할 경우 전송/수신한 바이트 수 변경 사항이 표시되어야 합니다.

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : User1                  Index        : 4820
Assigned IP  : 172.18.0.1             Public IP    : 192.168.2.20
Assigned IPv6: 2009::1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 27731                  Bytes Rx     : 14427
Group Policy : MyRaVpn|Policy         Tunnel Group : MyRaVpn
Login Time   : 21:58:10 UTC Mon Apr 10 2017
Duration     : 0h:51m:13s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a800fd012d400058ebfff2
Security Grp : none                   Tunnel Zone : 0
```

## ASA의 원격 액세스 VPN 구성 세부 정보 보기

단계 **1** 왼쪽의 CDO 탐색 모음에서 **VPN** > **ASA/FDM** 원격 액세스 **VPN** 구성를 클릭합니다.

단계 **2** 존재하는 VPN 구성 개체를 클릭합니다. 현재 얼마나 많은 연결 프로파일 및 그룹 정책이 구성되어 있는지 나타내는 요약 정보를 그룹에서 표시합니다.

- RA VPN 구성을 확장하여 연결된 모든 연결 프로파일을 확인합니다.
  - 추가 + 버튼을 클릭하여 새 연결 프로파일을 추가합니다.
  - 보기 버튼( )을 클릭하여 연결 프로파일 및 연결 지침에 관한 요약 정보를 엽니다. **Actions(**작업**)** 아래에서 **Edit(**편집**)**를 클릭하여 변경 사항을 편집할 수 있습니다.
- **Actions(**작업**)** 아래의 다음 옵션 중 하나를 클릭하여 추가 작업을 수행할 수 있습니다.
  - 그룹 정책을 할당/추가하려면 **Group Policies(**그룹 정책**)**를 클릭합니다.
  - 더 이상 필요하지 않은 구성 개체 또는 연결 프로파일을 클릭하고 **Remove(**제거**)**를 클릭하여 삭제합니다.

# ASA 템플릿

템플릿을 사용하면 사용자가 디바이스/서비스 구성을 일반적으로 구성하여 함께 그룹화된 다른 구성에 적용할 수 있습니다. 이러한 템플릿은 함께 그룹화되는 여러 구현에 영향을 주기 위해 변경을 수행할 수 있는 단일 위치를 제공합니다.

# ARM 템플릿 매개변수

새 템플릿을 생성할 때 특정 디바이스를 모델로 삼을 수 있습니다. CDO는 템플릿이 모델링되는 디바이스의 구성 내에서 선택한 텍스트 필드를 기반으로 템플릿 매개변수를 설정할 수 있는 기능을 제공합니다. 템플릿 매개변수 보기 내에서 매개변수를 생성하고 기존 매개변수에서 설정하고 검색할 수 있습니다.

**Note** ASA 템플릿에 대한 구성을 가져오도록 선택하는 경우 구성은 JSON 형식이어야 합니다.

## 새 매개변수 생성

단계 **1** 온보딩된 기존 디바이스를 사용하여 CDO 상단에 있는 Templates(템플릿) 탭으로 이동합니다.
단계 **2** **New Template(**새 템플릿**)** 또는 **Manage Templates(**템플릿 관리**)**를 선택합니다.
단계 **3** 원하는 구성을 선택하여 매개변수를 생성합니다.
단계 **4** 화면 상단의 Name(이름) 필드에 템플릿 이름을 입력합니다.
단계 **5** 매개변수를 추가할 텍스트 필드를 선택합니다.
단계 **6** 매개 변수에 설명을 제공하고 값을 추가하고 필요한 메모를 추가합니다.
단계 **7** Name(이름) 필드 옆에 있는 **Save(**저장**)**를 클릭하여 매개변수를 저장합니다.
단계 **8** 그런 다음 **Review Template(**템플릿 검토**)**를 클릭하여 템플릿을 검토할 수 있습니다.

이제 이 템플릿을 사용하여 온보딩되는 모든 향후 디바이스에 적용되는 저장된 파라미터가 있습니다.

# 새 ASA, ISR 또는 ASR 템플릿 생성

기본 설정

알려진 ASA, ISR 또는 ASR 기본 구성으로 시작합니다. 템플릿의 매개 변수화를 시작하려면 원하는 구성을 선택합니다. 매개 변수화에는 구성 파일 내에서 필드 또는 특성을 선택하고 구성 파일 인스턴스화에서 선택될 값 목록을 식별하는 작업이 포함됩니다.

**Note** ASA 템플릿에 대한 구성을 가져오도록 선택하는 경우 구성은 JSON 형식이어야 합니다.

매개변수 추가

기본 구성을 선택하여 매개 변수화 프로세스를 시작할 수 있습니다. 구성 편집기에서 매개 변수화를 위해 원하는 필드를 선택합니다. 선택한 문자열은 이중 괄호로 묶여 있습니다. 왼쪽 창에서 매개 변수의 이름을 변경하고, 설명을 추가하고, 여러 값을 추가할 수 있습니다. **Allow Custom Value(**맞춤형

값 허용)를 선택하면 인스턴스화 시 맞춤형 값을 설정할 수 있습니다. 그렇지 않으면 식별된 값만 선택할 수 있습니다.

매개변수화가 완료되면 템플릿의 이름을 지정하고 **Save(**저장**)**를 클릭합니다.

매개변수화에 대한 자세한 내용은 ARM 템플릿 매개변수를 참조하십시오.

검토

템플릿이 저장되면 **Review(**검토**)**를 클릭하여 검토 프로세스로 이동합니다. 검토에서 템플릿은 매개변수가 있는 값을 포함하여 있는 그대로 내보낼 수 있습니다. 이는 반드시 유효한 구성은 아니지만 CDO에 저장된 템플릿을 검토할 수 있는 수단을 제공한다는 점에 유의하십시오. 필요한 경우 **Edit(**편집**)**를 클릭하여 템플릿을 편집할 수도 있습니다. **Diff(**차이**)** 버튼은 저장된 템플릿과 가장 최근 수정 사항 간의 차이점을 보여줍니다.

# 템플릿에서 ASA 구성 생성

템플릿에서 구성 생성

템플릿에서 사용자 지정 구성을 생성하는 프로세스를 시작하려면 **Config from Template(**템플릿에서 구성**)** 버튼을 선택합니다. 사용 가능한 템플릿이 나열됩니다. 고른 템플릿을 선택하고 **Choose Template(**템플릿 선택**)**을 클릭합니다.

대부분의 경우 템플릿에는 사용자 지정 구성을 제공하기 위해 **Export(**내보내기**)**에서 설정해야 하는 매개변수화된 값이 포함됩니다. 왼쪽 창에서 이 구성에 대해 원하는 대로 각 매개변수와 값을 선택합니다. 값이 편집기에 표시됩니다. 이는 내보낼 때 매개변수를 대체하는 값입니다. 모든 매개변수 값이 설정되면 **Export(**내보내기**)** 버튼을 클릭하여 구성을 내보내고 다운로드합니다. 템플릿에 매개변수화된 값이 포함되어 있지 않으면 **Export(**내보내기**)** 버튼을 클릭하여 구성을 있는 그대로 내보냅니다.

# ASA 템플릿 관리

Manage Templates(템플릿 관리) 보기에서는 모든 기존 템플릿을 시각화하고 수정 및 삭제할 수 있습니다. 템플릿을 편집하는 동안 매개변수 설정 및 값 구성을 수정할 수 있습니다. 기존 템플릿 위에 마우스를 놓고 **Edit(**수정**)**를 선택하면 됩니다.

템플릿 수정

편집 보기에서 다음 작업을 수행합니다.

- 편집기에서 텍스트를 두 번 클릭하거나 강조 표시하여 매개변수를 추가합니다.
- Description(설명) 텍스트 상자에 입력하여 매개변수를 설명합니다. 그런 다음 **Add Value(**값 추가**)**를 클릭합니다.
- 값을 제공하고 메모를 작성합니다. **Add(**추가**)**를 클릭합니다.
- 작업이 완료되면 **Save(**저장**)**를 클릭합니다.

- 이제 **Review Template(**템플릿 검토**)**을 클릭하여 템플릿을 검토할 수 있습니다.
  - **Diff(**차이**)**를 클릭하여 파일을 비교할 수 있습니다.
  - 템플릿을 내보내려면 **Export(**내보내기**)**를 클릭합니다.

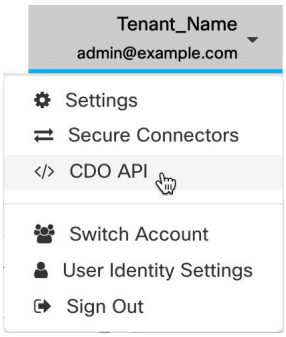
# CDO 공용 API

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. 공식 가이드(https://graphql.org/learn/)를 통해 쉽고 간단하게 읽을 수 있습니다.

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

사용자 메뉴에서 CDO 공용 API를 선택하여 시작할 수 있습니다.




# API 토큰

개발자는 CDO REST API 호출을 할 때 CDO API 토큰을 사용합니다. 호출이 성공하려면 REST API 인증 헤더에 API 토큰을 삽입해야 합니다. API 토큰은 만료되지 않는 "장기" 액세스 토큰입니다. 그러나 이를 갱신하고 취소할 수 있습니다.

CDO 내에서 API 토큰을 생성할 수 있습니다. 이러한 토큰은 생성 직후 일반 설정 페이지가 열려 있는 동안에만 표시됩니다. CDO에서 다른 페이지를 열고 일반 설정 페이지로 돌아가면, 토큰이 분명히 발급었지만 토큰이 더 이상 표시되지 않습니다.

개별 사용자는 특정 테넌트에 대한 자체 토큰을 생성할 수 있습니다. 사용자는 다른 사용자를 대신하여 토큰을 생성할 수 없습니다. 토큰은 계정-테넌트 쌍에 고유하며 다른 사용자-테넌트 조합에 사용할 수 없습니다.

### API 토큰 형식 및 클레임

API 토큰은 JSON 웹 토큰(JWT)입니다. JWT 토큰 형식에 대해 자세히 알아보려면 JSON 웹 토큰 소개를 읽어보십시오.

CDO API 토큰은 다음과 같은 클레임 집합을 제공합니다.

- **id** - 사용자/디바이스 uid
- **parentId** - 테넌트 uid
- **ver** - 공개 키의 버전(초기 버전은 0, 예, **cdo_jwt_sig_pub_key.0**)
- **subscriptions** - 보안 서비스 익스체인지 구독 (선택 사항)
- **client_id** - "**api-client**"
- **jti** - 토큰 ID

# FDM-관리 디바이스 템플릿으로 ASA 구성 마이그레이션

**Attention** Firepower Device Manager(FDM) 지원 및 기능은 요청 시에만 제공됩니다. 테넌트에서 Firewall Device Manager 지원을 아직 활성화하지 않은 경우 디바이스를 관리하거나 FDM 관리 디바이스에 구축할 수 없습니다. TAC를 사용하여 지원 티켓 열기에 요청을 보냅니다.

Cisco Defense Orchestrator는 ASA를 FDM 관리 디바이스로 마이그레이션하는 데 도움이 됩니다. CDO는 ASA에서 실행 중인 구성의 이러한 요소를 FDM 관리 디바이스 템플릿으로 마이그레이션하는 데 도움이 되는 마법사를 제공합니다.

- 액세스 제어 규칙(ACL)
- 인터페이스
- NAT(네트워크 주소 변환) 규칙
- 네트워크 개체 및 네트워크 그룹 개체
- 경로
- 서비스 개체 및 서비스 그룹 개체
- 사이트 간 VPN

ASA 실행 구성의 이러한 요소가 FDM 관리 디바이스 템플릿으로 마이그레이션되면 FDM 템플릿을 CDO에서 관리하는 새 FDM 관리 디바이스에 적용할 수 있습니다. FDM 관리 디바이스는 템플릿에 정의된 구성을 채택하므로, 이제 FDM 관리 디바이스는 ASA 실행 구성의 일부 측면으로 구성됩니다.

구성을 실행하는 ASA의 다른 요소는 이 프로세스를 사용하여 마이그레이션되지 않습니다. 이러한 다른 요소는 FDM 관리 디바이스 템플릿에서 빈 값으로 표시됩니다. 템플릿이 FDM 관리 디바이스에 적용되면 마이그레이션한 값을 새 FDM 관리 디바이스에 적용하고 빈 값은 무시합니다. 새 FDM 관

리 디바이스의 다른 기본값은 그대로 유지됩니다. 마이그레이션하지 않은 구성을 실행하는 ASA의 다른 요소는 마이그레이션 프로세스 외부의 FDM 관리 디바이스에서 다시 생성해야 합니다.

CDO를 사용하여 ASA를 FDM 관리 디바이스로 마이그레이션하는 프로세스에 대한 전체 설명은 Cisco Defense Orchestrator를 사용하여 ASA를 FDM 매니지드 디바이스로 마이그레이션을 참조하십시오.

# ASA 인증서 관리

디지털 인증서는 인증 디바이스 및 개별 사용자를 위한 디지털 ID를 제공합니다. 디지털 인증서에는 어떤 디바이스나 사용자를 식별하는 정보, 이를테면 이름, 일련 번호, 회사, 부서 또는 IP 주소가 들어 있습니다. 디지털 인증서는 사용자 또는 디바이스의 공개 키 사본 하나도 포함합니다. "디지털 인증서"에 대한 자세한 내용은 Cisco ASA 시리즈 일반 운영 ASDM 구성, X.Y 문서에서 "디지털 인증서" 장을 참조하십시오.

CA(인증 증명)는 인증서에 "서명"하여 그 진위를 확인함으로써 해당 디바이스 또는 사용자의 ID를 보장하는 신뢰받는 기관입니다. CA는 ID 인증서도 발급합니다.

- **ID** 인증서 — ID 인증서는 특정 시스템 또는 호스트용 인증서입니다. 이러한 인증서는 OpenSSL 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명 인증서를 생성할 수도 있습니다. CA는 ID 인증서를 발급하는데, 이는 특정 시스템이나 호스트를 위한 인증서입니다.
- 신뢰할 수 있는 **CA** 인증서 인증서 — 신뢰할 수 있는 CA 인증서는 다른 인증서에 서명하는 데 사용됩니다. 이러한 인증서는 CA 인증서에는 활성화되지만 ID 인증서에는 비활성화되는 기본 제약 조건 확장 및 CA 플래그와 관련된 내부 ID 인증서와 다릅니다. 신뢰할 수 있는 CA 인증서는 자체 서명되며 루트 인증서라고도 합니다.

원격 액세스 VPN은 VPN 연결을 안전하게 설정하기 위해 보안 게이트웨이 및 AnyConnect 클라이언트(종단) 인증에 디지털 인증서를 사용합니다. 자세한 내용은 원격 액세스 VPN 인증서 기반 인증을 참고하십시오.

### 인증서 설치 가이드

ASA에서의 인증서 설치에 대한 다음 가이드를 읽어보십시오.

- 인증서는 단일 또는 여러 ASA 디바이스에 동시에 설치할 수 있습니다.
- 한 번에 하나의 인증서만 설치할 수 있습니다.
- 인증서는 라이브 ASA 디바이스에만 설치할 수 있으며 모달 디바이스에는 설치할 수 없습니다.
- Secure Firewall Cloud Native 디바이스에 인증서를 설치할 수 없습니다.

# ASA 인증서 설치

디지털 인증서를 트러스트 포인트 개체로 업로드하고 CDO에서 관리하는 ASA 디바이스에 설치해야 합니다.

참고 ASA 디바이스에 대역 외 변경 사항이 없으며 모든 단계적 변경 사항이 구축되었는지 확인합니다.

다음에는 CDO에서 지원하는 디지털 인증서 및 형식이 나와 있습니다.

- ID 인증서는 다음 방법을 사용하여 설치할 수 있습니다.
  - PKCS12 파일 가져오기.
  - 자체 서명 인증서
  - CSR(Certificate Signing Request) 가져오기.
- 신뢰할 수 있는 CA 인증서는 PEM 또는 DER 형식을 사용하여 설치할 수 있습니다.

CDO를 사용하여 ASA에 인증서를 설치하는 단계를 보여주는 스크린캐스트를 시청하십시오. 또한 설치된 인증서를 수정, 내보내기 및 삭제하는 단계를 보여줍니다.

지원되는 인증서 형식

- PKCS12: PKCS#12, P12 또는 PFX 형식은 서버 인증서, 중간 인증서 및 개인 키를 하나의 암호화 가능한 파일에 저장하기 위한 이진 형식입니다. PFX 파일은 일반적으로 **.pfx** 및 **.p12**와 같은 확장자를 갖습니다.
- PEM: PEM(원래 "Privacy Enhanced Mail") 파일은 ASCII(또는 Base64) 인코딩 데이터를 포함하며 인증서 파일은 .pem, .crt, .cer 또는 .key 형식일 수 있습니다. 이는 Base64 인코딩 ASCII 파일이며 "-----BEGIN CERTIFICATE-----" 및 "-----END CERTIFICATE-----" 명령문을 포함합니다.
- DER: DER(Distinguished Encoding Rules) 형식은 ASCII PEM 형식이 아닌 인증서의 이진 형식입니다. 파일 확장자가 **.der**인 경우도 있지만 파일 확장자가 **.cer**인 경우도 많습니다. 따라서 DER.cer 파일과 PEM.cer 파일의 차이점을 구분하는 유일한 방법은 텍스트 편집기에서 파일을 열고 BEGIN/END 문을 찾는 것입니다. PEM과 달리 DER 인코딩 파일은 -----BEGIN CERTIFICATE-----와 같은 일반 텍스트 명령문을 포함하지 않습니다.

트러스트 포인트 화면

ASA 디바이스를 CDO에 온보딩한 후 **Devices & Services(**디바이스 및 서비스**)** 탭에서 ASA 디바이스를 선택하고 왼쪽의 **Management(**관리**)** 창에서 **Trustpoints(**트러스트 포인트**)**를 클릭합니다.

**Trustpoints(**트러스트 포인트**)** 탭에 디바이스에 이미 설치된 인증서가 표시됩니다.

- "Installed(설치됨)" 상태는 해당 인증서가 디바이스에 성공적으로 설치되었음을 나타냅니다.
- "Unknown(알 수 없음)" 상태는 해당 인증서에 어떤 정보도 포함되어 있지 않음을 나타냅니다. 이를 제거하고 올바른 세부 정보를 사용하여 다시 업로드해야 합니다. CDO는 모든 알 수 없는 인증서를 신뢰할 수 있는 CA 인증서로 검색합니다.
- "Installed(설치됨)"가 표시된 행을 클릭하여 오른쪽 창에서 인증서 세부 정보를 확인합니다. 선택한 인증서의 추가 세부 정보를 보려면 **more(**더 보기**)**를 클릭합니다.

- 설치된 ID 인증서는 PKCS12 또는 PEM 형식으로 내보내고 다른 ASA 디바이스로 가져올 수 있습니다. ID 인증서 내보내기를 참조하십시오.
- 설치된 인증서에서는 고급 설정만 수정할 수 있습니다.
  - 고급 설정을 수정하려면 **Edit(편집)**를 클릭합니다.
  - 변경한 후 **Send(전송)**를 클릭하여 업데이트된 인증서를 설치합니다.

# PKCS12를 사용하여 ID 인증서 설치

PKCS12 형식으로 생성된 기존 트러스트 포인트 개체를 선택하여 ASA 디바이스에 설치할 수 있습니다. 설치 마법사에서 새 트러스트 포인트 개체를 생성하고 ASA 디바이스에 인증서를 설치할 수도 있습니다.

시작하기 전에

- 인증서 설치 가이드을 읽어보십시오.
- ASA는 "Synced(동기화됨)" 및 "Online(온라인)" 상태여야 합니다.

---

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** 단일 ASA 디바이스에 ID 인증서를 설치하려면 다음을 수행합니다.

a) **Devices(**디바이스**)** 탭을 클릭합니다.
b) **ASA** 탭을 클릭하고 ASA 디바이스를 선택합니다.
c) 오른쪽의 **Management(**관리**)** 창에서 **Trustpoints(**트러스트 포인트**)**를 클릭합니다.
d) **Install(**설치**)**을 클릭합니다.

참고 여러 ASA 디바이스에 인증서를 설치할 수도 있습니다. 여러 ASA 디바이스를 선택하고 오른쪽의 **Devices Action(**디바이스 작업**)**에서 **Install Certificate(**인증서 설치**)**를 클릭합니다.

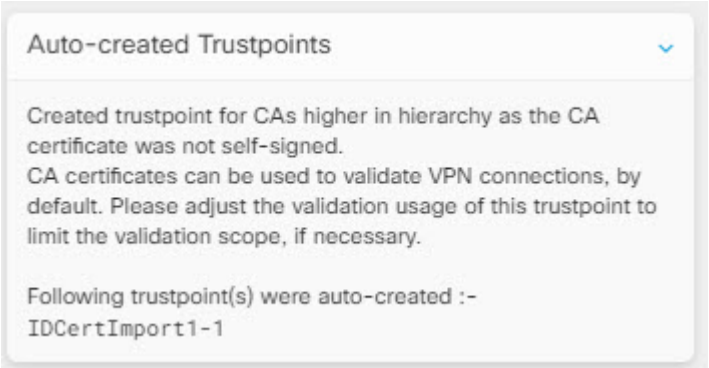
단계 **3** **Select Trustpoint Certificate to Install(**설치할 트러스트 포인트 인증서 선택**)**에서 다음 중 하나를 클릭합니다.

- **Create(**생성**)**를 클릭하여 새 트러스트 포인트 개체를 추가합니다. 자세한 내용은 PKCS12를 사용하여 ID 인증서 개체 추가를 참조하십시오.
- **Choose(**선택**)**를 클릭하여 PKCS 유형의 인증서 등록 개체를 선택합니다.

단계 **4** **Send(**보내기**)**를 클릭합니다.

이렇게 하면 ASA 디바이스에 인증서가 설치됩니다.

참고 중간 CA가 설치된 PKCS12 인증서를 가져오는 경우, ASA에서는 아직 설치되지 않은 모든 중간 CA 인증서에 대해 트러스트 포인트 개체를 자동으로 생성하여 디바이스에 설치합니다. ID 인증서를 클릭하면 다음 예와 같이 오른쪽 창에 메시지가 표시됩니다.




# 자체 서명 등록을 사용한 인증서 설치

자체 서명 인증서에 대해 생성된 기존 트러스트 포인트 개체를 선택하여 ASA 디바이스에 설치할 수 있습니다. 설치 마법사에서 새 트러스트 포인트 개체를 생성하고 ASA 디바이스에 인증서를 설치할 수도 있습니다.

시작하기 전에

- 인증서 설치 가이드을 읽어보십시오.
- ASA는 "Synced(동기화됨)" 및 "Online(온라인)" 상태여야 합니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** 단일 ASA 디바이스에 ID 인증서를 설치하려면 다음을 수행합니다.

a) **Devices(**디바이스**)** 탭을 클릭합니다.
b) **ASA** 탭을 클릭하고 ASA 디바이스를 선택합니다.
c) 오른쪽의 **Management(**관리**)** 창에서 **Trustpoints(**트러스트 포인트**)**를 클릭합니다.
d) **Install(**설치**)**을 클릭합니다.

참고 여러 ASA 디바이스에 서명된 인증서를 설치할 수도 있습니다. 여러 ASA 디바이스를 선택하고 오른쪽의 **Devices Action(**디바이스 작업**)**에서 **Install Certificate(**인증서 설치**)**를 클릭합니다.

단계 **3** **Select Trustpoint Certificate to Install(**설치할 트러스트 포인트 인증서 선택**)**에서 다음 중 하나를 클릭합니다.

- **Create(**생성**)**를 클릭하여 새 트러스트 포인트 개체를 추가합니다. 자세한 내용은 PKCS12를 사용하여 ID 인증서 개체 추가를 참조하십시오.
- **Choose(**선택**)**를 클릭하여 자체 서명 인증서 유형의 인증서 등록 개체를 선택합니다.

단계 **4** **Send(**보내기**)**를 클릭합니다.

자체 서명된 등록 유형의 트러스트 포인트의 경우 발급자 공통 이름 상태는 항상 ASA 디바이스이며 관리되는 디바이스는 자체 CA로 작동하여 자체 ID를 생성하는 CA 인증서가 필요하지 않습니다.

# 인증서 서명 요청(CSR) 관리

먼저 CSR 요청을 생성한 다음 신뢰할 수 있는 CA(Certificate Authority)에서 이 요청에 서명을 받아야 합니다. 그런 다음 CA에서 발급한 서명된 ID 인증서를 ASA 디바이스에 설치할 수 있습니다.

- 인증서 설치 가이드을 읽어보십시오.
- ASA는 "Synced(동기화됨)" 및 "Online(온라인)" 상태여야 합니다.

다음 다이어그램은 ASA에서 CSR을 생성하고 인증된 발급 인증서를 설치하는 워크플로우를 보여줍니다.

## CSR 요청 생성

단계 1 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 2 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 3 **ASA** 탭을 클릭하고 ASA 디바이스를 선택합니다.

단계 4 단일 ASA 디바이스에 ID 인증서를 설치하려면 다음을 수행합니다.

단계 5 **Install(**설치**)**을 클릭합니다.

단계 6 **Select Trustpoint Certificate to Install(**설치할 트러스트 포인트 인증서 선택**)**에서 다음 중 하나를 클릭합니다.

- **Create(**생성**)**를 클릭하여 새 트러스트 CSR 개체를 추가합니다. 자세한 내용은 CSR(Certificate Signing Request)을 위한 ID 인증서 개체 추가, 136 페이지을 참고하십시오.
- 이미 생성된 CSR 요청 신뢰 지점을 선택하려면 를 **Choose(**선택**)**합니다.

단계 7 **Send(**보내기**)**를 클릭합니다.

이렇게 하면 서명되지 않은 CSR(인증서 서명 요청)이 생성됩니다.

단계 8 복사 아이콘 copy_icon.png를 클릭하여 CSR 세부 정보를 복사합니다. CSR 요청을 ".csr" 파일 형식으로 다운로드할 수도 있습니다.

단계 9 **OK(**확인**)**를 클릭합니다.

단계 10 인증서에 서명하려면 인증서 서명 요청(CSR)을 인증 기관에 제출합니다.

## 인증 기관에서 발급한 서명된 ID 인증서 설치

CA가 서명된 인증서를 발급하면 ASA 디바이스에 인증서를 설치합니다.

단계 1 **Trustpoint(**트러스트 포인트**)** 화면에서 **Status(**상태**)**가 "Awaiting Signed Certificate Install(서명된 인증서 설치 대기 중)"인 CSR 요청을 클릭하고 오른쪽의 **Actions(**작업**)** 창에서 **Install Certified ID Certificate(**인증된 **ID** 인증서 설치**)**를 클릭합니다.

단계 2 CA에서 수신한 서명된 인증서를 업로드합니다. 파일을 끌어다 놓거나 제공된 필드에 내용을 붙여넣을 수 있습니다. 트러스트 포인트 명령은 선택한 트러스트 포인트를 기반으로 생성됩니다.

단계 3 **Send(**보내기**)**를 클릭합니다.

이렇게 하면 서명된 ID 인증서가 ASA 디바이스에 설치됩니다. 인증서를 설치하면 디바이스에 변경 사항이 즉시 구축됩니다.

참고 여러 ASA 디바이스에 인증서를 설치할 수도 있습니다. 여러 ASA 디바이스를 선택하고 오른쪽의 **Devices Action(**디바이스 작업**)**에서 **Install Certificate(**인증서 설치**)**를 클릭합니다.

# ASA에 신뢰할 수 있는 CA 인증서 설치

시작하기 전에

- 인증서 설치 가이드을 읽어보십시오.
- ASA는 "Synced(동기화됨)" 및 "Online(온라인)" 상태여야 합니다.

---

단계 **1** 탐색 메뉴에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** **ASA** 탭을 클릭하고 ASA 디바이스를 선택합니다.

단계 **4** 단일 ASA 디바이스에 ID 인증서를 설치하려면 다음을 수행합니다.

a) ASA 디바이스를 선택하고 오른쪽의 **Management(**관리**)** 창에서 **Trustpoints(**트러스트 포인트**)**를 클릭합니다.

b) **Install(**설치**)**을 클릭합니다.

참고 여러 ASA 디바이스에 인증서를 설치할 수도 있습니다. 여러 ASA 디바이스를 선택하고 오른쪽의 **Devices Action(**디바이스 작업**)**에서 **Install Certificate(**인증서 설치**)**를 클릭합니다.

단계 **5** **Select Trustpoint Certificate to Install(**설치할 트러스트 포인트 인증서 선택**)**에서 다음 중 하나를 클릭합니다.

- **Create(**생성**)**를 클릭하여 새 트러스트 포인트 개체를 추가합니다. 자세한 내용은 신뢰할 수 있는 CA 인증서 개체 추가, 138 페이지을 참고하십시오.
- 신뢰할 수 있는 인증 기관 개체 선태을 **Choose(**선택**)**합니다.

단계 **6** **Send(**보내기**)**를 클릭합니다.

그러면 ASA 디바이스에 신뢰할 수 있는 CA 파일이 설치됩니다.

---

# ID 인증서 내보내기

신뢰 지점과 연결된 키 쌍 및 발급된 인증서를 PKCS12 또는 PEM 형식으로 내보내고 가져올 수 있습니다. 이 형식은 신뢰 지점 구성을 다른 ASA에서 수동으로 복제하는 데 유용합니다.

### SUMMARY STEPS

1. 탐색 메뉴에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.
2. **Devices(**디바이스**)** 탭을 클릭합니다.
3. **ASA**를 클릭합니다.
4. ASA 디바이스를 선택하고 오른쪽의 **Management(**관리**)**에서 **Trustpoints(**트러스트 포인트**)**를 클릭합니다.
5. ID 인증서를 클릭하여 인증서 구성을 내보냅니다. 또는 검색 필드에 이름을 입력하여 인증서를 검색할 수 있습니다.

6. 오른쪽의 **Actions(**작업**)** 창에서 **Export Certificate(**인증서 내보내기**)**를 클릭합니다.
7. **PKCS12 Format(PKCS12** 형식**)** 또는 **PEM Format(PEM** 형식**)**을 클릭하여 인증서 형식을 선택합니다.
8. 내보낼 PKCS12 파일을 암호화하는 데 사용한 암호화 패스프레이즈를 입력합니다.
9. 암호화 패스프레이즈를 확인합니다.
10. **Export(**내보내기**)**를 클릭하여 인증서 구성을 내보냅니다.

**DETAILED STEPS**

| | 명령 또는 동작 | 목적 |
|---|---|---|
| 단계 **1** | 탐색 메뉴에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다. | |
| 단계 **2** | **Devices(**디바이스**)** 탭을 클릭합니다. | |
| 단계 **3** | **ASA**를 클릭합니다. | |
| 단계 **4** | ASA 디바이스를 선택하고 오른쪽의 **Management(**관리**)**에서 **Trustpoints(**트러스트 포인트**)**를 클릭합니다. | |
| 단계 **5** | ID 인증서를 클릭하여 인증서 구성을 내보냅니다. 또는 검색 필드에 이름을 입력하여 인증서를 검색할 수 있습니다. | |
| 단계 **6** | 오른쪽의 **Actions(**작업**)** 창에서 **Export Certificate(**인증서 내보내기**)**를 클릭합니다. | |
| 단계 **7** | **PKCS12 Format(PKCS12** 형식**)** 또는 **PEM Format(PEM** 형식**)**을 클릭하여 인증서 형식을 선택합니다. | |
| 단계 **8** | 내보낼 PKCS12 파일을 암호화하는 데 사용한 암호화 패스프레이즈를 입력합니다. | |
| 단계 **9** | 암호화 패스프레이즈를 확인합니다. | |
| 단계 **10** | **Export(**내보내기**)**를 클릭하여 인증서 구성을 내보냅니다. | 정보 대화 상자가 나타나 인증서 컨피그레이션 파일을 지정된 위치에 성공적으로 내보냈음을 알립니다. |

# 설치된 인증서 편집

설치된 인증서의 고급 옵션만 수정할 수 있습니다.

단계 **1** 탐색 메뉴에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** **ASA** 탭을 클릭합니다.

단계 **4** ASA 디바이스를 선택하고 오른쪽의 **Management(**관리**)**에서 **Trustpoints(**트러스트 포인트**)**를 클릭합니다.

단계 **5** 수정할 인증서를 클릭하고 오른쪽의 **Actions(**작업**)** 창에서 **Edit(**편집**)**를 클릭합니다.

단계 **6** 필수 매개변수를 수정하고 **Save(**저장**)**를 클릭합니다.

# ASA에서 기존 인증서 삭제

인증서를 하나씩 삭제할 수 있습니다. 삭제한 인증서 컨피그레이션은 복원할 수 없습니다.

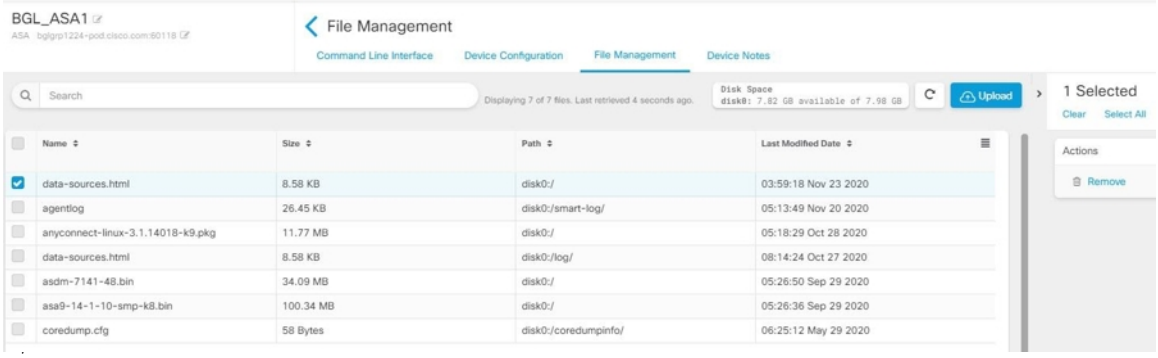
단계 **1** 탐색 메뉴에서 **Devices & Services(**장치 및 서비스**)**를 클릭합니다.
단계 **2** ASA 디바이스를 선택하고 오른쪽의 **Management(**관리**)**에서 **Trustpoints(**트러스트 포인트**)**를 클릭합니다.
단계 **3** 삭제할 인증서를 클릭하고 오른쪽의 **Actions(**작업**)** 창에서 **Remove(**제거**)**를 클릭합니다.
단계 **4** **OK(**확인**)**를 클릭하여 선택한 인증서를 제거합니다.

# ASA 파일 관리

CDO는 ASA 디바이스의 플래시(disk0) 공간에 있는 파일 보기, 업로드 또는 삭제와 같은 기본 파일 관리 작업을 수행하기 위한 파일 관리 툴을 제공합니다.

**Note** disk1에 있는 파일은 관리할 수 없습니다.

File Management(파일 관리) 화면에는 디바이스의 플래시(disk0)에 있는 모든 파일이 나열됩니다. 파일 업로드에 성공하면 새로 고침 아이콘을 클릭하여 파일을 볼 수 있습니다. 기본적으로 이 화면은 10분마다 자동으로 새로 고쳐집니다. **Disk Space(**디스크 공간**)** 필드에는 disk0 디렉터리의 디스크 공간이 표시됩니




AnyConnect 이미지를 단일 또는 여러 ASA 디바이스에 업로드할 수 있습니다. 업로드에 성공하면 AnyConnect 이미지가 선택한 ASA 디바이스의 RA VPN 구성과 연결됩니다. 이렇게 하면 새로 릴리스된 AnyConnect 패키지를 여러 ASA 디바이스에 동시에 업로드할 수 있습니다.

플래시 시스템에 파일 업로드

CDO는 원격 서버에서의 URL 기반 파일 업로드만 지원합니다. 파일 업로드에 지원되는 프로토콜은 HTTP, HTTPS, TFTP, FTP, SMB 또는 SCP입니다. AnyConnect 소프트웨어 이미지, DAP.xml, data.xml, 호스트 스캔 이미지 파일 등의 파일을 단일 또는 여러 ASA 디바이스에 업로드할 수 있습니다.

**Note** 원격 서버의 URL 경로가 유효하지 않거나 발생할 수 있는 문제로 인해 CDO는 선택한 ASA 디바이스에 파일을 업로드하지 않습니다. 자세한 내용은 디바이스 워크플로우로 이동하여 알아보십시오.

디바이스가 고가용성으로 구성되어 있고 CDO가 먼저 스탠바이 디바이스에 파일을 업로드하고 업로드에 성공한 후에만 파일이 액티브 디바이스에 업로드된다고 가정합니다. 파일 제거 프로세스 중에도 동일한 동작이 적용됩니다.

파일 업로드에 지원되는 프로토콜의 syntax(명령문):

| 프로토콜 | 구문 | 예 |
|---|---|---|
| HTTP | http://[[path/ ]filename] | http://www.geonames.org/data-sources.html |
| HTTPS | https://[[path/ ]filename] | https://docs.aws.amazon.com/amazon/tagging.html |
| TFTP | tftp://[[path/ ]filename] | tftp://10.10.16.6/ftd/components.html |
| FTP | ftp://[[user[:password]@]server[:port]/[path/ ]filename] | [illegible] |
| SMB | smb://[[path/ ]filename] | smb://10.10.32.145//sambashare/hello.txt |
| SCP | scp://[[user[:password]@]server[/path]/filename] | scp://root:cisco123@10.10.16.6//root/events_send.py |

시작하기 전에

- ASA 디바이스에서 원격 서버에 액세스할 수 있는지 확인합니다.
- 파일이 이미 원격 서버에 업로드되었는지 확인합니다.
- ASA 디바이스에서 해당 서버로 연결되는 네트워크 경로가 있는지 확인합니다.
- FQDN이 URL에 사용되는 경우 DNS가 구성되어 있는지 확인합니다.
- 원격 서버의 URL은 인증 프롬프트가 표시되지 않는 직접 링크여야 합니다.
- 원격 서버 IP 주소가 NAT된 경우 원격 서버 위치의 NAT된 공용 IP 주소를 제공해야 합니다.

**Note** 페일오버에서 피어로 구성된 ASA에 파일을 업로드하는 경우 CDO는 페일오버 쌍의 다른 피어에 대한 새 파일을 승인하지 않으며 디바이스 상태가 **Not Synced(**동기화되지 않음**)**로 변경됩니다. CDO가 두 디바이스에서 파일을 인식하도록 하려면 두 디바이스 모두에 변경 사항을 수동으로 구축해야 합니다.

# 단일 ASA 디바이스에 파일 업로드

이 절차를 사용하여 파일을 단일 ASA 디바이스에 업로드합니다.

단계 1 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 2 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 3 **ASA** 탭을 클릭하고 ASA 디바이스를 선택합니다.

단계 4 오른쪽의 **Management(**관리**)** 창에서 **File Management(**파일 관리**)**를 클릭합니다. 사용 가능한 디스크 공간 및 ASA 디바이스에 있는 파일을 볼 수 있습니다.

단계 5 오른쪽의 **Upload(**업로드**)** 버튼을 클릭합니다.

단계 6 **URL** 링크에서 파일이 사전 업로드된 서버의 경로를 지정합니다. **Destination Path(**대상 경로**)** 필드에는 **disk0** 디렉터리에 업로드되는 파일의 이름이 표시됩니다. disk0 내의 특정 디렉터리에 파일을 업로드하려면 이 필드에 파일 이름을 지정합니다. 예를 들어 dap.xml 파일을 "DAPFiles" 디렉터리에 업로드하려면 필드에 " **disk0:/** DAPFiles/dap.xml"을 지정합니다.

**Note** CDO ASA CLI 인터페이스에서 **dir** 명령을 실행하여 disk0 폴더에 있는 디렉터리를 볼 수 있습니다.

단계 7 지정된 서버 경로가 AnyConnect 파일을 가리키는 경우 **Associate file with RA VPN Configuration(RA VPN** 구성과 파일 연결**)** 확인란이 활성화됩니다. 참고: 이 확인란은 올바른 명명 규칙을 따르는 AnyConnect 파일 이름(예: 'anyconnect-win-xxx.pkg', 'anyconnect-linux-xxx.pkg' 또는 'anyconnect-mac-xxx.pkg' 형식)에 대해서만 활성화됩니다. 이 확인란을 선택하면 CDO는 업로드에 성공한 후 AnyConnect 파일을 선택한 ASA 디바이스의 RA VPN 구성에 연결합니다.

단계 8 **Upload(**업로드**)**를 클릭합니다. CDO가 디바이스에 파일을 업로드합니다.

단계 9 5단계에서 AnyConnect 패키지를 RA VPN 구성과 연결하도록 선택한 경우 CDO에서 ASA로 구성 변경 사항 구축.

### What to do next

디바이스에 구성 변경 사항을 구축할 필요가 없습니다.

# 여러 ASA 디바이스에 파일 업로드

이 절차를 사용하여 동시에 여러 ASA 디바이스에 파일을 업로드합니다.

단계 1 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 2 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 3 대량 업로드를 수행하려면 **ASA** 탭을 클릭하고 여러 ASA 디바이스를 선택합니다.

단계 4 오른쪽의 **Device Actions(**디바이스 작업**)**에서 **Upload File(**파일 업로드**)**를 클릭합니다. 참고: ASA 디바이스가 온라인이어야 **Upload File(**파일 업로드**)** 링크가 나타납니다.

단계 5 **URL** 링크에서 파일이 사전 업로드된 서버의 경로를 지정합니다. **Destination Path(**대상 경로**)** 필드에는 **disk0** 디렉터리에 업로드되는 파일의 이름이 표시됩니다. disk0 내의 특정 디렉터리에 파일을 업로드하려면 이 필드에 파일

이름을 지정합니다. 예를 들어 dap.xml 파일을 "DAPFiles" 디렉터리에 업로드하려면 필드에 " **disk0:/** DAPFiles/dap.xml"을 지정합니다.

**Note** CDO ASA CLI 인터페이스에서 **dir** 명령을 실행하여 disk0 폴더에 있는 디렉터리를 볼 수 있습니다.

단계 **6** 지정된 서버 경로가 AnyConnect 파일을 가리키는 경우 **Associate file with RA VPN Configuration(RA VPN** 구성과 파일 연결**)** 확인란이 활성화됩니다.

**Note** 이 확인란은 올바른 명명 규칙을 따르는 AnyConnect 파일 이름(예: 'anyconnect-win-xxx.pkg', 'anyconnect-linux-xxx.pkg' 또는 'anyconnect-mac-xxx.pkg' 형식)에 대해서만 활성화됩니다. 이 확인란을 선택하면 CDO는 업로드에 성공한 후 AnyConnect 파일을 선택한 ASA 디바이스의 RA VPN 구성에 연결합니다.

단계 **7** **Upload(**업로드**)**를 클릭합니다.

단계 **8** 4단계에서 AnyConnect 패키지를 RA VPN 구성과 연결하도록 선택한 경우, CDO에서 ASA로 구성 변경 사항 구축.

### What to do next

개별 디바이스에서 파일을 업로드하는 진행 상황을 볼 수 있습니다. ASA 디바이스를 선택하고 오른쪽의 **Management(**관리**)** 창에서 **File Management(**파일 관리**)**를 클릭합니다. 파일 업로드가 진행 중인 경우 작업이 완료될 때까지 기다립니다.

디바이스에 구성 변경 사항을 구축할 필요가 없습니다.

# ASA에서 파일 제거

RA VPN 구성과 연결된 AnyConnect 파일은 제거할 수 없습니다. 해당 RA VPN 구성에서 AnyConnect 파일의 연결을 해제한 다음 파일 관리 툴에서 파일을 제거해야 합니다.

**Note** 페일오버에서 피어로 구성된 ASA에 파일을 업로드하는 경우 CDO는 페일오버 쌍의 다른 피어에 대한 새 파일을 승인하지 않으며 디바이스 상태가 **Not Synced(**동기화되지 않음**)**로 변경됩니다. CDO가 두 디바이스에서 파일을 인식하도록 하려면 두 디바이스 모두에 변경 사항을 수동으로 구축해야 합니다.

제거 작업은 선택한 파일을 플래시 메모리에서 영구적으로 삭제합니다. 파일을 삭제할 때 확인을 요청하는 메시지가 나타납니다. 선택한 ASA 디바이스에서 파일을 제거하려면 다음 절차를 수행합니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** **ASA** 탭을 클릭하고 ASA 디바이스를 선택합니다.

단계 **4** 오른쪽의 **Management(**관리**)** 창에서 **File Management(**파일 관리**)**를 클릭합니다.

단계 **5** 제거할 파일을 선택하고 오른쪽의 **Actions(**작업**)** 아래에서 **Remove(**제거**)**를 클릭합니다. 최대 25개의 파일을 선택할 수 있습니다. CDO가 일부 파일을 제거하지 못한 경우 디바이스 워크플로우를 확인하여 제거된 파일과 보존된 파일을 확인할 수 있습니다.

단계 **6** AnyConnect 패키지를 제거하도록 선택한 경우 CDO에서 ASA로 구성 변경 사항 구축합니다.

# ASA 고가용성 관리

## 액티브-액티브 페일오버 모드에서 ASA에 적용된 구성 변경 사항

CDO(Cisco Defense Orchestrator)는 CDO에 준비된 ASA의 실행 구성을 변경하거나 CDO에 저장된 구성을 변경할 때 구성의 해당 측면을 CDO GUI로 관리할 수 있으면 구성 파일의 관련 행만 변경하려고 시도합니다. CDO GUI를 사용하여 원하는 구성을 변경할 수 없는 경우, CDO는 변경을 위해 전체 구성 파일을 덮어쓰려고 시도합니다.

다음은 두 가지 예입니다.

- CDO GUI를 사용하여 네트워크 개체를 생성하거나 변경할 수 있습니다. CDO가 해당 변경 사항을 ASA의 구성에 배포해야 하는 경우, 변경이 발생할 때 ASA에서 실행 중인 구성 파일의 관련 줄을 덮어씁니다.
- CDO GUI를 사용하여 새 ASA 사용자를 생성할 수 없습니다. ASA의 ASDM 또는 CLI를 사용하여 새 사용자를 ASA에 추가한 경우, 해당 대역 외 변경 사항이 수락되고 CDO가 저장된 구성 파일을 업데이트하면 CDO는 CDO에 준비된 ASA의 전체 구성 파일을 덮어쓰려고 시도합니다.

ASA가 액티브-액티브 페일오버 모드에서 구성된 경우 이러한 규칙은 준수되지 않습니다. CDO가 액티브-액티브 페일오버 모드에서 구성된 ASA를 관리하는 경우 CDO가 항상 자신의 모든 구성 변경 사항을 ASA로 구축하거나 ASA의 모든 구성 변경 사항을 자신으로 읽을 수는 없습니다. 다음은 두 가지 경우입니다.

- **CDO**에서 수행한 **ASA** 구성 파일의 변경 사항**(CDO GUI**에서 지원하지 않는 경우**)**은 **ASA**에 구축할 수 없습니다. 또한 CDO가 지원하지 않는 구성 파일에 대한 변경 사항과 CDO가 지원하는 구성 파일에 대한 변경 사항의 조합은 ASA에 구축할 수 없습니다. 두 경우 모두 "CDO는 현재 페일오버 모드의 디바이스에 대한 전체 구성 교체를 지원하지 않습니다. Cancel(취소)을 클릭하고 디바이스에 변경 사항을 수동으로 적용하십시오." CDO 인터페이스의 메시지와 함께 Replace Configuration(구성 교체) 버튼이 비활성화되어 있습니다.
- 액티브-액티브 페일오버 모드에서 구성된 **ASA**에 대한 대역 외 변경 사항은 **CDO**에 의해 거부되지 않습니다. ASA의 실행 중인 구성을 대역 외 변경을 수행하는 경우, ASA는 Devices & Services(디바이스 및 서비스) 페이지에서 "Conflict Detected(충돌 탐지됨)"로 표시됩니다. 충돌을 검토하고 충돌을 거부하려고 하면 CDO가 해당 작업을 차단합니다. "CDO는 이 디바이스에 대한 대역 외 변경 거부를 지원하지 않습니다. 이 디바이스는 지원되지 않는 소프트웨어 버전을 실행하거나 액티브/액티브 페일오버 쌍의 멤버입니다. Continue(계속)를 클릭하여 대역 외 변경 사항을 수락하십시오."

⚠

**Caution** ASA에서 대역 외 변경 사항을 수락해야 하는 경우 CDO에 준비되었지만 아직 ASA에 구축되지 않은 모든 구성 변경 사항이 덮어쓰기되고 손실됩니다.

CDO는 페일오버 모드에서 ASA에 대한 구성 변경 사항이 CDO GUI에서 지원되는 경우 해당 구성 변경 사항을 지원합니다.

관련 정보**:**

# ASA에서 DNS 구성

이 절차를 사용하여 각 ASA에서 도메인 이름 서버(DNS)를 구성합니다.

사전 요구 사항

- ASA는 인터넷에 연결되어야 합니다.
- 시작하기 전에 다음 정보를 수집합니다.
  - DNS 서버에 연결할 수 있는 ASA 인터페이스의 이름(예: 내부, 외부 또는 dmz).
  - 조직에서 사용하는 DNS 서버의 IP 주소 자체 DNS 서버를 유지 관리하지 않는 경우 Cisco Umbrella를 사용할 수 있습니다. Cisco Umbrella의 IP 주소는 208.67.220.220입니다.

## 절차

단계 **1** 탐색 모음에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** **ASA** 탭을 클릭하고 DNS를 구성할 모든 ASA를 선택합니다.

단계 **4** 오른쪽의 Actions(작업) 창에서 **Command Line Interface(**명령줄 인터페이스**)**를 선택합니다.

단계 **5** CLI 매크로 즐겨찾기 별을 클릭합니다.

단계 **6** **Configure DNS Macro(DNS** 매크로 구성**)**를 선택합니다.

단계 **7** **>_View Parameters(**매개변수 보기**)**를 선택하고 Parameters(매개변수) 열에서 다음 매개변수의 값을 입력합니다.

- IF_Name - DNS 서버에 연결할 수 있는 ASA 인터페이스의 이름입니다.
- IP_ADDR - 조직에서 사용하는 DNS 서버의 IP 주소

단계 **8** **Send to devices(**디바이스로 전송**)**를 클릭합니다.

# CDO 명령줄 인터페이스

CDO는 사용자에게 ASA 디바이스를 관리하기 위한 CLI(명령줄 인터페이스)를 제공합니다. 사용자는 단일 디바이스 또는 여러 디바이스에 동시에 명령을 전송할 수 있습니다.

관련 정보:

- 자세한 ASA CLI 설명서는 ASA 명령줄 인터페이스 설명서, on page 108의 내용을 참조하십시오.

## 명령줄 인터페이스 사용

단계 1 **Inventory(**재고 목록**)** 페이지를 엽니다.

단계 2 재고 목록 테이블 위에 있는 디바이스 버튼을 클릭합니다.

단계 3 명령줄 인터페이스(CLI)를 사용하여 관리하려는 디바이스를 찾으려면 디바이스 탭과 필터 버튼을 사용합니다.

단계 4 디바이스를 선택합니다.

단계 5 **Device Actions(**장치 작업**)** 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 6 **Command Line Interface(**명령줄 인터페이스**)** 탭을 클릭합니다.

단계 7 명령 창에 명령을 입력하고 **Send(**보내기**)**를 클릭합니다. 명령에 대한 디바이스의 응답은 "응답 창" 아래에 표시됩니다.

**Note** 실행할 수 있는 명령에 제한 사항이 있는 경우 해당 제한 사항은 명령 창 위에 나열됩니다.

**Related Topics**

명령줄 인터페이스에 명령 입력, 93 페이지

## 명령줄 인터페이스에 명령 입력

한 줄에 하나의 명령을 입력하거나 여러 줄에 여러 명령을 순차적으로 입력할 수 있으며 CDO는 명령을 순서대로 실행합니다. 다음 ASA 예에서는 세 개의 네트워크 개체와 해당 네트워크 개체를 포함하는 네트워크 개체 그룹을 생성하는 명령 배치를 전송합니다.

ASA장치 명령 입력: CDO는 ASA의 전역 구성 모드에서 명령을 실행합니다.

긴 명령: 매우 긴 명령을 입력하면 CDO는 API에 대해 모두 실행할 수 있도록 명령을 여러 명령으로 분할하려고 시도합니다. CDO가 명령을 적절하게 분리할 수 없는 경우 명령 목록을 구분할 위치에 대한 힌트를 묻는 메시지가 표시됩니다. 예를 들면 다음과 같습니다.

```
오류: CDO가 600자를 초과하는 이 명령의 일부를 실행하려고 시도했습니다. 적절한 명령 구분 지점이 어디인지에 대한 힌트를 CDO에 제공할 수 있습니다. 명령 목록 사이에 빈 행을 추가하면 됩니다.
```

이 오류가 표시되는 경우:

단계 **1** CLI 기록 창에서 오류를 일으킨 명령을 클릭합니다. CDO는 긴 명령 목록으로 명령 상자를 채웁니다.

단계 **2** 관련 명령 그룹 뒤에 빈 줄을 입력하여 긴 명령 목록을 편집합니다. 예를 들어 네트워크 개체 목록을 정의한 후 빈 줄을 추가하고 위의 예와 같이 그룹에 추가합니다. 명령 목록의 다양한 지점에서 이 작업을 수행할 수 있습니다.

단계 **3** **Send(**보내기**)**를 클릭합니다.

# 명령 기록 작업

CLI 명령을 보낸 후 CDO는 **Command Line Interface(**명령줄 인터페이스**)** 페이지의 기록 창에 해당 명령을 기록합니다. 기록 창에 저장된 명령을 다시 실행하거나 명령을 템플릿으로 사용할 수 있습니다.

단계 **1** **Inventory(**인벤토리**)** 페이지에서 구성할 디바이스를 선택합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **5** 아직 확장되지 않은 경우 시계 아이콘 을 클릭하여 기록 창을 확장합니다.

단계 **6** 편집하거나 다시 보내려는 히스토리 창에서 명령을 Select(선택)합니다.

단계 **7** 명령 창에서 명령을 그대로 재사용하거나 편집하고 **Send(**보내기**)**를 클릭합니다. CDO는 응답 창에 명령 결과를 표시합니다.

**Note** CDO는 다음 두 가지 상황에서 응답창에 `Done!(완료!)` 메시지를 표시합니다.

- 명령이 성공적으로 실행된 후.
- 명령에 반환할 결과가 없는 경우. 예를 들어 특정 구성 항목을 검색하는 정규식과 함께 show 명령을 실행할 수 있습니다. 정규식 기준을 충족하는 구성 항목이 없는 경우 CDO는 `완료!`를 반환합니다.

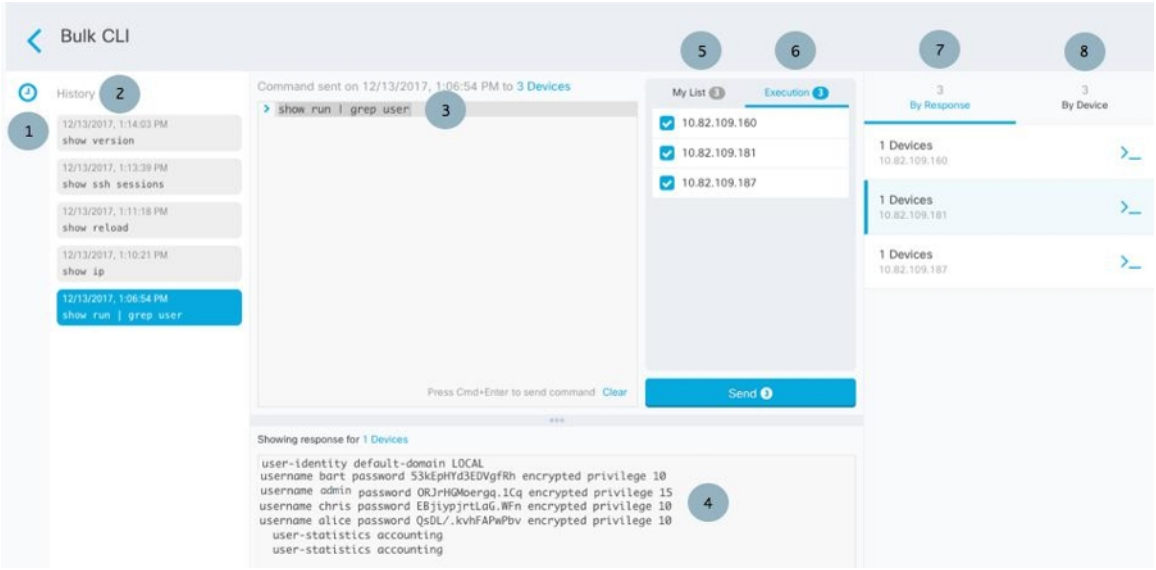
# 대량 명령줄 인터페이스

CDO는 CLI(command line interface)를 사용하여 Secure Firewall ASA, FDM 관리, 위협 방어, SSH 및 Cisco IOSSecure Firewall Cloud Native 디바이스를 관리할 수 있는 기능을 사용자에게 제공합니다. 사용자는 단일 디바이스 또는 같은 종류의 여러 디바이스에 동시에 명령을 보낼 수 있습니다. 이 섹션에서는 한 번에 여러 디바이스에 CLI 명령을 보내는 방법을 설명합니다.

관련 정보:

- ASA CLI 설명서에 대한 자세한 설명서는 ASA 명령줄 인터페이스 설명서, on page 108를 참조하십시오.

## 대량 **CLI** 인터페이스




**Note** CDO는 다음 두 가지 상황에서 **Done!(**완료**!)** 메시지를 표시합니다.

- 명령이 오류 없이 성공적으로 실행된 후.
- 명령에 반환할 결과가 없는 경우. 예를 들어 특정 구성 항목을 검색하는 정규식과 함께 show 명령을 실행할 수 있습니다. 정규식 기준을 충족하는 구성 항목이 없는 경우 CDO는 완료**!**를 반환합니다.

| 숫자 | 설명 |
|---|---|
| 1 | 시계를 클릭하여 명령 기록 창을 확장하거나 축소합니다. |

| 숫자 | 설명 |
|---|---|
| 2 | 명령 기록. 명령을 보낸 후 CDO는 이 히스토리 창에 명령을 기록하므로 돌아가서 선택하고 다시 실행할 수 있습니다. |
| 3 | 명령 창. 이 창의 프롬프트에 명령을 입력합니다. |
| 4 | 응답 창. CDO는 명령에 대한 디바이스의 응답과 CDO 메시지를 표시합니다. 두 개 이상의 디바이스에 대한 응답이 동일한 경우 응답 창에 "X 디바이스에 대한 응답 표시"라는 메시지가 표시됩니다. X 디바이스를 클릭하면 CDO가 명령에 동일한 응답을 반환한 모든 디바이스를 표시합니다.<br>**Note** CDO는 다음 두 가지 상황에서 **Done!(**완료**!)** 메시지를 표시합니다.<br>• 명령이 오류 없이 성공적으로 실행된 후.<br>• 명령에 반환할 결과가 없는 경우. 예를 들어 특정 구성 항목을 검색하는 정규식과 함께 show 명령을 실행할 수 있습니다. 정규식 기준을 충족하는 구성 항목이 없는 경우 CDO는 완료**!**를 반환합니다. |
| 5 | **My List(**내 목록**)** 탭에는 **Inventory(**인벤토리**)** 테이블에서 선택한 디바이스가 표시되며 명령을 보낼 디바이스를 포함하거나 제외할 수 있습니다. |
| 6 | 위 그림에서 강조 표시된 **Execution(**실행**)** 탭은 히스토리 창에서 선택한 명령의 디바이스를 표시합니다. 이 예에서 show run \| grep user 명령이 기록 창에서 선택되고 실행 탭에 10.82.109.160, 10.82.109.181 및 10.82.10.9.187로 전송된 것으로 표시됩니다. |
| 7 | **By Response(**응답별**)** 탭을 클릭하면 명령에 의해 생성된 응답 목록이 표시됩니다. 동일한 응답은 한 행에 함께 그룹화됩니다. By Response(응답별) 탭에서 행을 선택하면 CDO는 응답 창에 해당 명령에 대한 응답을 표시합니다. |
| 8 | **By Device(**디바이스별**)** 탭을 클릭하면 각 디바이스의 개별 응답이 표시됩니다. 목록에서 디바이스 중 하나를 클릭하면 특정 디바이스에서 명령에 대한 응답을 볼 수 있습니다. |

# 대량 명령 전송

단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** 디바이스를 찾으려면 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 적절한 디바이스 탭을 선택하고 필터 버튼을 사용하여 명령줄 인터페이스를 사용하여 구성할 디바이스를 찾습니다.

단계 **4** 디바이스를 선택합니다.

단계 **5** **Device Actions(**장치 작업**)** 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 6 내 목록 필드에서 명령을 보낼 디바이스를 선택하거나 선택 취소할 수 있습니다.

단계 7 명령 창에 명령을 입력하고 **Send(**보내기**)**를 클릭합니다. 명령 출력은 응답 창에 표시되고 명령은 변경 로그에 기록되며 CDO 명령은 대량 CLI 창의 기록 창에 명령을 기록합니다.

**Note** 명령은 동기화된 선택된 ASA 디바이스에서 성공하고 동기화되지 않은 디바이스에서는 실패할 수 있습니다. 선택한 ASA 디바이스 중 하나라도 동기화되지 않은 경우 `show`, `ping`, `traceroute`, `vpn-sessiondb`, `changeto`, `dir`, `write` 및 `copy` 명령만 허용됩니다.

# 대량 명령 기록 작업

대량 CLI 명령을 보낸 후, CDO는 대량 CLI 인터페이스 기록에 해당 명령을 기록합니다. 기록 창에 저장된 명령을 다시 실행하거나 명령을 템플릿으로 사용할 수 있습니다. 기록 창의 명령은 명령이 실행된 원래 디바이스와 연결됩니다.

단계 1 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 2 디바이스를 찾으려면 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 3 적절한 디바이스 유형 탭을 클릭하고 필터 아이콘을 클릭하여 구성하려는 디바이스를 찾습니다.

단계 4 디바이스를 선택합니다.

단계 5 **Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 6 편집하거나 다시 보내려는 히스토리 창에서 명령을 **Select(**선택**)**합니다. 선택하는 명령은 특정 디바이스와 연결되며 반드시 첫 번째 단계에서 선택한 디바이스와 연결되지는 않습니다.

단계 7 내 목록 탭을 보고 전송하려는 명령이 예상하는 디바이스로 전송되는지 확인합니다.

단계 8 명령 창에서 명령을 편집하고 **Send(**보내기**)**를 클릭합니다. CDO는 응답 창에 명령 결과를 표시합니다.

**Note** 명령은 동기화된 선택된 ASA 디바이스에서 성공하고 동기화되지 않은 디바이스에서는 실패할 수 있습니다. 선택한 ASA 디바이스 중 하나라도 동기화되지 않은 경우 `show`, `ping`, `traceroute`, `vpn-sessiondb`, `changeto`, `dir`, `write` 및 `copy` 명령만 허용됩니다.

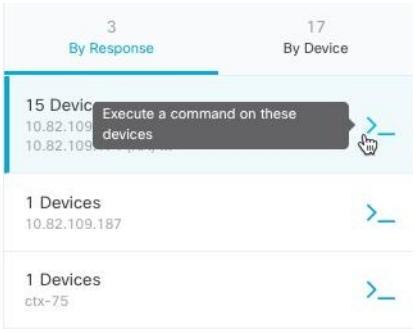
# 대량 명령 필터 작업

대량 CLI 명령을 실행한 후 **By Resonse(**응답별**)** 필터 및 **By Device(**디바이스별**)** 필터를 사용하여 계속해서 디바이스를 구성할 수 있습니다.

## 응답 기준 필터

대량 명령을 실행한 후 CDO는 명령을 보낸 디바이스에서 반환된 응답 목록으로 **By Response(**응답별**)** 탭을 채웁니다. 응답이 동일한 디바이스는 단일 행에 통합됩니다. **By Response(**응답별**)** 탭에서 행을 클릭하면 응답 창에 디바이스의 응답이 표시됩니다. 응답 창에 두 개 이상의 디바이스에 대한 응답이

표시되면 "X 디바이스에 대한 응답 표시"라는 메시지가 표시됩니다. **X devices(X** 디바이스**)**를 클릭하면 CDO가 명령에 동일한 응답을 반환한 모든 디바이스를 표시합니다.




명령 응답과 관련된 디바이스 목록에 명령을 보내려면 다음 절차를 따르십시오.

단계 **1** **By Response(**응답별**)** 탭에서 행의 명령 기호를 클릭합니다.

단계 **2** 명령 창에서 명령을 검토하고 **Send(**보내기**)**를 클릭하여 명령을 다시 보내거나 **Clear(**지우기**)**를 클릭하여 명령 창을 지우고 디바이스로 보낼 새 명령을 입력한 다음 **Send(**보내기**)**를 클릭합니다.

단계 **3** 명령에서 받은 응답을 검토하십시오.

단계 **4** 선택한 디바이스에서 실행 중인 구성 파일이 변경 사항을 반영한다고 확신하는 경우 명령 창에 `write memory`를 입력하고 **Send(**보내기**)**를 클릭합니다. 이렇게 하면 실행 중인 구성이 시작 구성에 저장됩니다.

## 디바이스 기준 필터

대량 명령을 실행한 후 CDO는 실행 탭과 디바이스별 탭을 명령을 보낸 디바이스 목록으로 채웁니다. 디바이스별 탭에서 행을 클릭하면 각 디바이스에 대한 응답이 표시됩니다.

동일한 디바이스 목록에서 명령을 실행하려면 다음 절차를 따르십시오.

단계 **1** **By Device(**디바이스 별**)** 탭을 클릭합니다.

단계 **2** **>_Execute a command on these devices(**이 디바이스에서 명령 실행**)**를 클릭합니다.

단계 **3** **Clear(**지우기**)**를 클릭하여 명령 창을 지우고 새 명령을 입력합니다.

단계 **4** 내 목록 창에서 목록의 개별 디바이스를 선택하거나 선택 취소하여 명령을 보낼 디바이스 목록을 지정합니다.

단계 **5** **Send(**보내기**)**를 클릭합니다. 명령에 대한 응답이 응답 창에 표시됩니다. 응답 창에 두 개 이상의 디바이스에 대한 응답이 표시되면 "X 디바이스에 대한 응답 표시"라는 메시지가 표시됩니다. X 디바이스를 클릭하면 CDO가 명령에 동일한 응답을 반환한 모든 디바이스를 표시합니다.

단계 **6** 선택한 디바이스에서 실행 중인 구성 파일이 변경 사항을 반영한다고 확신하는 경우 명령 창에 `write memory`를 입력하고 **Send(**보내기**)**를 클릭합니다.

# 디바이스 관리를 위한 CLI 매크로

CLI 매크로는 즉시 사용할 수 있는 완전한 형식의 CLI 명령이거나 실행 전에 수정할 수 있는 CLI 명령의 템플릿입니다. 모든 매크로는 하나 이상의 ASA 디바이스에서 동시에 실행할 수 있습니다.

여러 디바이스에서 동일한 명령을 동시에 실행하려면 템플릿과 유사한 CLI 매크로를 사용합니다. CLI 매크로는 디바이스 구성 및 관리의 일관성을 유지합니다. 완전한 형식의 CLI 매크로를 사용하여 디바이스에 대한 정보를 가져옵니다. ASA 디바이스에서 즉시 사용할 수 있는 다양한 CLI 매크로가 있습니다.

자주 수행하는 작업을 모니터링하기 위해 CLI 매크로를 생성할 수 있습니다. 자세한 내용은 새 명령에서 CLI 매크로 생성을 참조하십시오.

CLI 매크로는 시스템 정의 또는 사용자 정의입니다. 시스템 정의 매크로는 CDO에서 제공하며 편집하거나 삭제할 수 없습니다. 사용자 정의 매크로는 사용자가 생성하며 편집하거나 삭제할 수 있습니다.

**Note** 디바이스가 CDO에 온보딩된 후에만 디바이스에 대한 매크로를 생성할 수 있습니다.

ASA를 예로 들어 ASA 중 하나에서 특정 사용자를 찾으려면 다음 명령을 실행할 수 있습니다.

```
show running-config | grep username
```

명령을 실행할 때 사용자 이름을 검색할 사용자의 사용자 이름으로 대체합니다. 이 명령으로 매크로를 만들려면 동일한 명령을 사용하고 사용자 이름을 중괄호로 묶습니다.

```
> show running-config | grep {{username}}
```

매개변수의 이름은 원하는 대로 지정할 수 있습니다. 이 매개변수 이름을 사용하여 동일한 매크로를 생성할 수도 있습니다.

```
> show running-config | grep {{username_of_local_user_stored_on_asa}}
```

매개변수 이름은 설명적일 수 있으며 영숫자 문자와 밑줄을 사용해야 합니다. 이 경우 명령 구문은

```
show running-config | grep
```

명령의 일부이며 명령을 전송하는 디바이스에 대해 적절한 CLI 구문을 사용해야 합니다.

## 새 명령에서 CLI 매크로 생성

단계 **1** CLI 매크로를 생성하기 전에 CDO의 명령줄 인터페이스에서 명령을 테스트하여 명령 구문이 올바른지, 그리고 신뢰할 수 있는 결과를 반환하는지 확인합니다.

**Note**
- 자세한 ASA CLI 설명서는 ASA 명령줄 인터페이스 설명서, on page 108의 내용을 참조하십시오.

단계 **2** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 3 **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 4 적절한 디바이스 유형 탭을 클릭하고 온라인 및 동기화된 디바이스를 선택합니다.

단계 5 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 6 CLI 매크로 즐겨찾기 스타 ★를 클릭하여 이미 존재하는 매크로를 확인합니다.

단계 7 더하기 버튼  을 클릭합니다.

단계 8 매크로에 고유한 이름을 지정합니다. 원하는 경우 CLI 매크로에 대한 설명 및 참고 사항을 제공합니다.

단계 9 **Command(**명령**)** 필드에 전체 명령을 입력합니다.

단계 10 명령을 실행할 때 수정하려는 명령 부분을 중괄호로 묶인 매개변수 이름으로 교체합니다.

단계 11 **Create(**생성**)**를 클릭합니다. 생성한 매크로는 처음에 지정한 디바이스뿐만 아니라 해당 유형의 모든 디바이스에서 사용할 수 있습니다.

명령을 실행하려면 CLI 매크로 실행을 참조하십시오.

# CLI 기록 또는 기존 CLI 매크로에서 CLI 매크로 생성

이 절차에서는 이미 실행한 명령, 다른 사용자 정의 매크로 또는 시스템 정의 매크로에서 사용자 정의 매크로를 생성합니다.

단계 1 탐색 모음에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

참고 CLI 기록에서 사용자 정의 매크로를 생성하려면 명령을 실행한 디바이스를 선택합니다. CLI 매크로는 동일한 계정의 디바이스 간에 공유되지만 CLI 기록은 공유되지 않습니다.

단계 2 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 3 적절한 디바이스 유형 탭을 클릭하고 온라인 및 동기화된 디바이스를 선택합니다.

단계 4 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 5 CLI 매크로를 만들려는 명령을 찾아 선택합니다. 다음 방법 중 하나를 사용합니다.

- 해당 디바이스에서 실행한 명령을 보려면 시계  를 클릭합니다. 매크로로 전환할 항목을 선택하면 명령 창에 명령이 나타납니다.
- CLI 매크로 즐겨찾기 스타 ★를 클릭하여 이미 존재하는 매크로를 확인합니다. 변경할 사용자 정의 또는 시스템 정의 CLI 매크로를 선택합니다. 명령 창에 명령이 나타납니다.

단계 6 명령 창의 명령을 사용하여 CLI 매크로 금색 별 를 클릭합니다. 이 명령은 이제 새 CLI 매크로의 기본이 됩니다.

단계 7 매크로에 고유한 이름을 지정합니다. 원하는 경우 CLI 매크로에 대한 설명 및 참고 사항을 제공합니다.

단계 8 명령 필드에서 명령을 검토하고 원하는 대로 변경합니다.

단계 9 명령을 실행할 때 수정하려는 명령 부분을 중괄호로 묶인 매개변수 이름으로 교체합니다.

단계 **10** **Create(**생성**)**를 클릭합니다. 생성한 매크로는 처음에 지정한 디바이스뿐만 아니라 해당 유형의 모든 디바이스에서 사용할 수 있습니다.

명령을 실행하려면 CLI 매크로 실행을 참조하십시오.

# CLI 매크로 실행

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 적절한 디바이스 유형 탭을 클릭하고 하나 이상의 디바이스를 선택합니다.

단계 **4** **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **5** 명령 패널에서 별표 ★를 클릭합니다.

단계 **6** 명령 패널에서 CLI 매크로를 선택합니다.

단계 **7** 다음 두 가지 방법 중 하나로 매크로를 실행합니다.

- 매크로에 정의할 매개변수가 없는 경우 **Send(**전송**)**를 클릭합니다. 명령에 대한 응답이 응답 창에 나타납니다. 다 됐습니다.
- 아래의 Configure DNS 매크로와 같은 매개변수가 매크로에 포함된 경우 **>_ View Parameters(**매개변수 보기**)**를 클릭합니다.


단계 **8** Parameters(매개변수) 창의 Parameters(매개변수) 필드에 매개변수 값을 입력합니다.


단계 **9** **Send(**보내기**)**를 클릭합니다. CDO가 성공적으로 명령을 전송하고 디바이스의 구성을 업데이트하면 완료됩니다!

- ASA의 경우 실행 중인 구성이 업데이트됩니다.

단계 **10** 명령을 전송한 후 "일부 명령이 실행 중인 구성을 변경했을 수 있습니다."라는 메시지와 함께 두 개의 링크가 표시될 수 있습니다.


- **Write to Disk(**디스크에 쓰기**)**를 클릭하면 이 명령의 변경 사항과 실행 중인 구성의 다른 모든 변경 사항이 디바이스의 시작 구성에 저장됩니다.
- **Dismiss(**해제**)**를 클릭하면 메시지가 사라집니다.

# CLI 매크로 편집

사용자 정의 CLI 매크로는 편집할 수 있지만 시스템 정의 매크로는 편집할 수 없습니다. CLI 매크로를 수정하면 모든 ASA 디바이스에 대해 변경됩니다. 매크로는 특정 디바이스에 한정되지 않습니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 디바이스를 선택합니다.

단계 **5** **Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **6** 편집할 사용자 정의 매크로를 선택합니다.

단계 **7** 매크로 레이블에서 편집 아이콘을 클릭합니다.

단계 **8** Edit Macro(매크로 편집) 대화 상자에서 CLI 매크로를 편집합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

CLI 매크로를 실행하는 방법에 대한 지침은 CLI 매크로 실행를 참조하십시오.

# CLI 매크로 삭제

사용자 정의 CLI 매크로는 삭제할 수 있지만 시스템 정의 매크로는 삭제할 수 없습니다. CLI 매크로를 삭제하면 모든 디바이스에서 삭제됩니다. 매크로는 특정 디바이스에 한정되지 않습니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 디바이스를 선택합니다.

단계 **5** **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **6** 삭제할 사용자 정의 CLI 매크로를 선택합니다.

단계 **7** CLI 매크로 레이블에서 휴지통 아이콘를 클릭합니다.
단계 **8** CLI 매크로를 제거할지 확인합니다.

# CLI를 사용한 ASA 구성

CDO에서 제공하는 CLI 인터페이스에서 CLI 명령을 실행하여 ASA 디바이스를 구성할 수 있습니다. 인터페이스를 사용하려면 **Devices & Services(**디바이스 및 서비스**)** 메뉴에서 디바이스를 선택하고 **Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다. 자세한 내용은 CDO 명령줄 인터페이스 사용을 참조하십시오.

### 새 로깅 서버 추가

시스템 로깅은 디바이스의 메시지를 syslog 데몬을 실행 중인 서버로 수집하는 방식입니다. 중앙 syslog 서버에 로깅하면 로그와 경고를 종합하는 데 도움이 됩니다.

자세한 내용은 실행 중인 ASA 버전의 CLI 책 1: Cisco ASA 시리즈 일반 작업 CLI 구성 가이드에서 '로깅' 장의 '모니터링' 섹션을 참조하십시오.

### **DNS** 서버 구성

ASA에서 호스트 이름의 IP 주소를 확인할 수 있도록 DNS 서버를 구성해야 합니다. 또한 액세스 규칙에서 FQDN(Fully Qualified Domain Name) 네트워크 개체를 사용하려면 DNS 서버를 구성해야 합니다.

자세한 내용은 실행 중인 ASA 버전의 CLI 책 1: Cisco ASA 시리즈 일반 작업 CLI 구성 가이드에서 'DNS 서버 구성' 섹션의 '기본 설정' 장을 참조하십시오.

### 정적 및 기본 경로 추가

비연결 호스트 또는 네트워크에 트래픽을 라우팅하려면 정적 또는 동적 라우팅을 사용하여 해당 호스트 또는 네트워크로 가는 경로를 정의해야 합니다.

자세한 내용은 CLI 책 1: Cisco ASA 시리즈 일반 작업 CLI 구성 가이드의 '정적 및 기본 경로' 장을 참조하십시오.

### 인터페이스 구성

CLI 명령을 사용하여 관리 및 데이터 인터페이스를 구성할 수 있습니다. 자세한 내용은 CLI 책 1: Cisco ASA 시리즈 일반 작업 CLI 구성 가이드의 '기본 인터페이스 구성' 장을 참조하십시오.

# ASA 구성 비교

이 절차를 사용하여 두 ASA의 구성을 비교합니다.

단계 1 탐색 메뉴에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 2 **Devices(**장치**)** 탭을 클릭하여 ASA 디바이스를 찾거나 **Templates(**템플릿**)**탭을 클릭하여 ASA 모델 디바이스를 찾습니다.

단계 3 **ASA** 탭을 클릭합니다.

단계 4 비교하려는 디바이스에 대한 디바이스 목록을 필터링합니다.

단계 5 두 개의 ASA를 선택합니다. 상태는 중요하지 않습니다. Defense Orchestrator에 저장된 ASA의 구성을 비교하고 있습니다.

단계 6 오른쪽의 디바이스 작업 창에서 **Compare(**비교**)**를 클릭합니다.

단계 7 구성 비교 대화 상자에서 **Next(**다음**)** 및 **Previous(**이전**)**를 클릭하여 구성 파일에서 파란색으로 강조 표시된 차이점을 건너뜁니다.

# ASA 대량 CLI 사용 사례

ASA 디바이스에 CDO의 대량 CLI 기능을 사용할 때 발생할 수 있는 워크플로우는 다음과 같습니다.

## ASA의 실행 중인 구성에 있는 모든 사용자를 표시한 다음 사용자 중 한 명 삭제

단계 1 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 2 **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 3 **ASA** 탭을 클릭합니다.

단계 4 사용자를 삭제하려는 디바이스의 디바이스 목록을 검색 및 필터링하고 선택합니다.

**Note** 선택한 디바이스가 동기화되었는지 확인합니다. 디바이스가 동기화되지 않은 경우 `show`, `ping`, `traceroute`, `vpn-sessiondb`, `changeto`, `dir`, `copy` 및 `write` 명령만 허용됩니다.

단계 5 세부 정보 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다. CDO는 내 목록 창에서 선택한 디바이스를 나열합니다. 더 적은 수의 디바이스에 명령을 보내기로 결정한 경우 해당 목록에서 디바이스를 선택 취소하십시오.

단계 6 명령 창에서 `show run | grep user`를 입력하고 **Send(**보내기**)**를 클릭합니다. 사용자 문자열을 포함하는 실행 중인 구성 파일의 모든 줄이 응답 창에 표시됩니다. 실행 탭이 열리고 명령이 실행된 디바이스가 표시됩니다.

단계 7 By Response(응답별) 탭을 클릭하고 응답을 검토하여 삭제할 사용자가 있는 디바이스를 결정합니다.

단계 8 내 목록 탭을 클릭하고 사용자를 삭제할 디바이스 목록을 선택합니다.

단계 9 명령 창에서 no 형식의 user 명령을 입력하여 user2를 삭제한 다음 **Send(**보내기**)**를 클릭합니다. 이 예에서는 user2를 삭제합니다.

```
no user user2 password reallyhardpassword privilege 10
```

단계 **10** 사용자 이름을 검색하는 데 사용한 `show run | grep user` 명령 인스턴스에 대한 히스토리 패널을 찾습니다. 해당 명령을 선택하고 실행 목록에서 디바이스 목록을 확인한 다음 **Send(**보내기**)**를 선택합니다. 지정한 디바이스에서 사용자 이름이 삭제된 것을 볼 수 있습니다.

단계 **11** 실행 중인 구성에서 올바른 사용자를 삭제했고 올바른 사용자가 실행 중인 구성에 남아 있는 것에 만족하는 경우 다음을 수행합니다.

**a.** 히스토리 창에서 `no user user2 password reallyhardpassword privilege 10` 명령을 선택합니다.

**b.** **By Device(**디바이스 별**)** 탭을 클릭하고 이 디바이스에서 명령 실행를 클릭합니다.

**c.** 명령 창에서 **Clear(**지우기**)**를 클릭하여 명령 창을 지웁니다.

**d.** `배포 메모리` 명령을 입력하고 **Send(**보내기**)**를 클릭합니다.

## 선택한 ASA에서 모든 SNMP 구성 찾기

이 절차는 ASA의 실행 중인 구성에 있는 모든 SNMP 구성 항목을 보여줍니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 **3** **ASA** 탭을 클릭합니다.

단계 **4** 실행 중인 구성에서 SNMP 구성을 분석하려는 디바이스를 필터링 및 검색하고 선택합니다.

**Note** 선택한 디바이스가 동기화되었는지 확인합니다. 디바이스가 동기화되지 않은 경우 `show, ping, traceroute, vpn-sessiondb, changeto,` 및 `dir` 명령만 허용됩니다.

단계 **5** 세부 정보 창에서 **Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다. 디바이스는 내 목록 창에서 선택한 디바이스를 나열합니다. 더 적은 수의 디바이스에 명령을 보내기로 결정한 경우 해당 목록에서 디바이스를 선택 취소하십시오.

단계 **6** 명령 창에서 `show run | grep snmp`를 입력하고 **Send(**보내기**)**를 클릭합니다. snmp 문자열을 포함하는 실행 중인 구성 파일의 모든 줄이 응답 창에 표시됩니다. 실행 탭이 열리고 명령이 실행된 디바이스가 표시됩니다.

단계 **7** 응답 창에서 명령 출력을 검토합니다.

# Secure Firewall ASA 구성 복원 정보

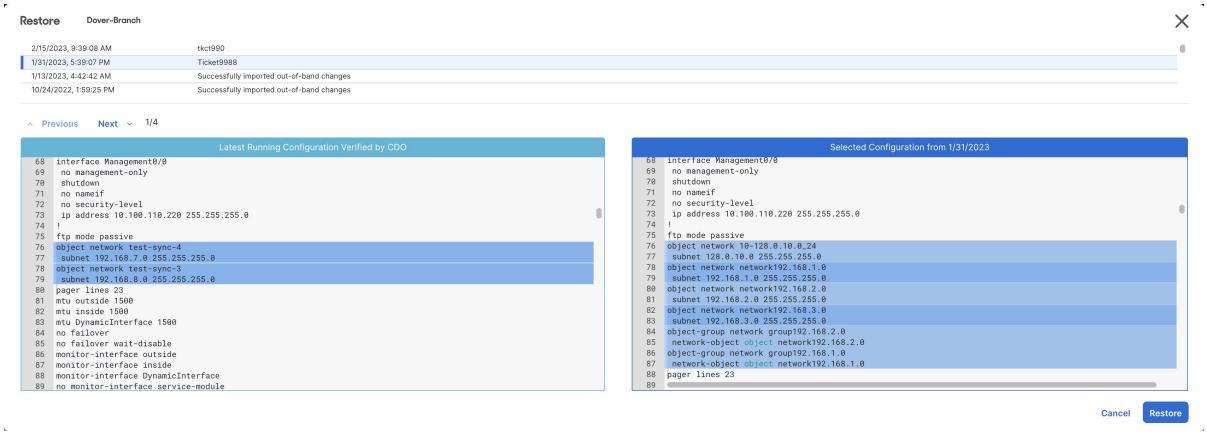
ASA의 구성을 변경하고, 변경 사항을 되돌리고자 하는 경우ASA의 과거 구성을 복원할 수 있습니다. 이는 예기치 않거나 원치 않는 결과를 초래한 구성 변경 사항을 편리하게 제거할 수 있는 방법입니다.

### ASA 구성 복원 정보

구성을 복원하기 전에 다음 참고 사항을 검토합니다.

- CDO는 복원하도록 선택한 구성을 ASA에 배포된 마지막으로 알려진 구성과 비교하지만, 복원하도록 선택한 구성을 준비되었지만 ASA에 배포되지 않은 구성과 비교하지 않습니다. ASA에 배포되지 않은 변경 사항이 있고 과거 구성을 복원하는 경우, 복원 프로세스는 배포되지 않은 변경 사항을 덮어쓰게 되며 해당 변경 사항은 손실됩니다.
- 과거 구성을 복원하기 전에, ASA이 동기화됨 또는 동기화되지 않음 상태일 수 있지만 디바이스가 충돌 감지됨 상태인 경우 과거 구성을 복원하기 전에 충돌을 해결해야 합니다.
- 과거 구성을 복원하면 배포된 모든 중간 구성 변경 사항을 덮어씁니다. 예를 들어 아래 목록에서 2023년 1월 31일의 구성을 복원하면 2023년 2월 15일에 이루어진 구성 변경 사항을 덮어씁니다.
- 다음 및 이전 버튼을 클릭하면 구성 파일을 통해 이동하고 구성 파일 변경 사항을 강조 표시합니다.
- 원래 구성 변경에 변경 요청 레이블을 적용한 경우 해당 레이블이 구성 복원 목록에 나타납니다.

***Figure 4: ASA*** 복원 구성 화면




구성 변경 사항은 얼마 동안 유지됩니까**?**

1년 이하의 ASA 구성을 복원할 수 있습니다. CDO는 변경 로그에 기록된 구성 변경 사항을 복원합니다. 변경 로그는 ASA에 구성 변경 사항을 쓰거나 읽을 때마다 변경 사항을 기록합니다. CDO는 1년치 변경 로그를 저장하며, 이전 연도 내에 수행된 백업 수에는 제한이 없습니다.

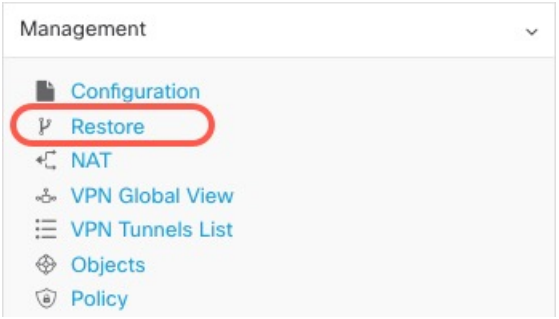
# Secure Firewall ASA 구성 복원

단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

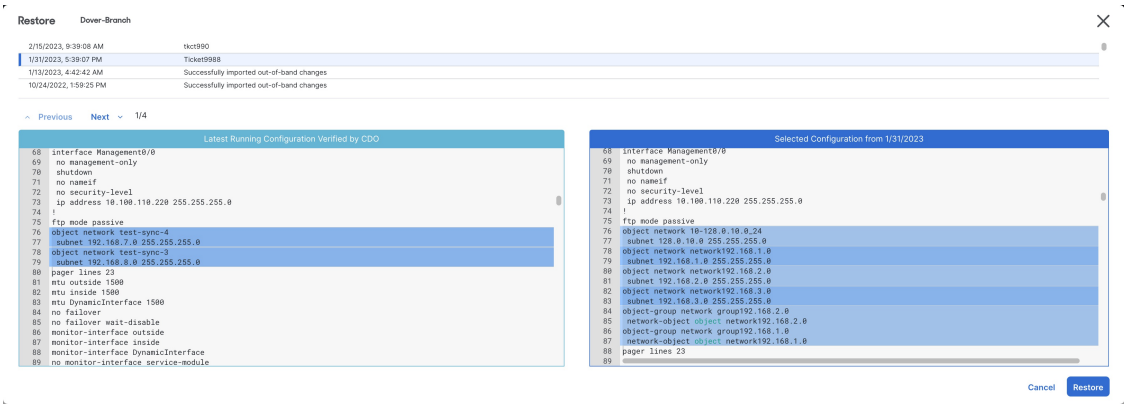
단계 **2** ASA 탭을 클릭합니다.

단계 **3** 복원하려는 ASA 구성을 선택합니다.

단계 **4** **Management(**관리**)** 창에서, **Restore(**복원**)**를 클릭합니다.




단계 **5** **Restore(**복원**)** 페이지에서 되돌리려는 구성을 선택합니다.




예를 들어 위 그림에서 2023년 1월 31일의 구성이 선택되었습니다.

단계 **6** "CDO에서 확인한 최신 실행 구성"과 "<날짜>에서 선택한 구성"을 비교하여 <날짜>에서 선택한 구성 창에 표시된 구성을 복원할 것인지 확인합니다. 이전 및 다음을 사용하여 모든 변경 사항을 비교합니다.

단계 **7** **Restore(**복원**)**을 클릭하면 CDO에서 구성이 준비됩니다. **Inventory(**재고 관리**)** 페이지에서 디바이스의 구성 상태가 이제 "동기화되지 않음"임을 알 수 있습니다.

단계 **8** 우측 창에서 **Deploy Changes...(**변경 사항 배포...**)**를 클릭하여 변경 사항을 배포하고 ASA를 동기화합니다.

# 문제 해결

잃어버렸지만 유지하고 싶었던 변경 사항을 복원하려면 어떻게 해야 합니까?

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** ASA 탭을 클릭합니다.

단계 **4** 필요한 디바이스를 선택합니다.

단계 **5** 오른쪽 창에서 **Change Log(**로그 변경**)**를 클릭합니다.

단계 **6** 변경 로그에서 변경 사항을 검토합니다. 해당 레코드에서 손실된 구성을 재구성할 수 있습니다.

# ASA 명령줄 인터페이스 설명서

CDO는 ASA 명령줄 인터페이스를 완벽하게 지원합니다. Cisco에서는 사용자가 단일 디바이스 및 여러 디바이스에 ASA 명령을 동시에 전송할 수 있도록 CDO 내에서 터미널과 유사한 인터페이스를 제공합니다. ASA 명령줄 인터페이스 설명서는 광범위합니다. CDO 설명서의 일부를 다시 작성하는 대신 Cisco.com의 ASA CLI 설명서에 대한 포인터를 제공합니다.

### ASA 명령줄 인터페이스 구성 가이드

ASA 버전 9.1부터는 ASA CLI 구성 가이드가 3개의 별도 책으로 구성됩니다.

- CLI Book 1: Cisco ASA Series 일반 운영 CLI 환경 설정 가이드
- CLI Book 2: Cisco ASA Series Firewall CLI 환경 설정 가이드
- CLI Book 3: Cisco ASA Series VPN CLI 구성 가이드

Cisco.com에서 Support(지원) > Products by Category(제품) > Security(보안) > Firewalls(방화벽) > ASA 5500(구성) > Configuration Guides(구성 가이드)로 이동하여 ASA CLI 구성 가이드에 도달할 수 있습니다.

### 몇 가지 특정 ASA 명령줄 인터페이스 구성 가이드 섹션

**show** 및 **more** 명령 출력 필터링 정규식을 사용하여 show 명령 출력을 필터링하는 자세한 내용은 CLI 설명서 1: Cisco ASA 시리즈 일반 운영 CLI 구성 가이드의 show 및 more 명령 출력 필터링에서 확인할 수 있습니다.

### ASA 명령 참조

ASA 명령 참조 가이드에는 모든 ASA 명령 및 해당 옵션이 알파벳순으로 나열되어 있습니다. ASA 명령 참조는 버전과 관련이 없습니다. 다음의 네 가지 책으로 게시됩니다.

- Cisco ASA Series 명령 참조, A - H 명령
- Cisco ASA Series 명령 참조, I - R 명령
- Cisco ASA Series 명령 참조, S 명령
- Cisco ASA Series 명령 참조, T - Z 명령 및 ASASM에 대한 IOS 명령

Cisco.com에서 Support(지원) > Products by Category(범주별 제품) > Security(보안) > Firewalls(방화벽) > ASA 5500(ASA 5500) > Reference Guides(참조 가이드) > Command References(명령 참조) > ASA Command References(ASA 명령 참조)로 이동하여 ASA 명령 참조 가이드로 이동할 수 있습니다.

# ASA, Cisco Secure Firewall Cloud Native, 및 Cisco IOS 장치 구성 파일

ASA, Secure Firewall Cloud Native및 Cisco IOS디바이스와 같은 일부 유형의 디바이스는 해당 구성을 단일 파일에 저장합니다. 이러한 디바이스의 경우 Cisco Defense Orchestrator에서 구성 파일을 보고 다양한 작업을 수행할 수 있습니다.

## 디바이스의 구성 파일 보기

ASA, Secure Firewall Cloud Native, SSH 관리 디바이스 및 Cisco IOS를 실행하는 디바이스와 같이 단일 구성 파일에 전체 구성을 저장하는 디바이스의 경우 CDO를 사용하여 구성 파일을 볼 수 있습니다.

참고 SSH 관리 디바이스 및 Cisco IOS 디바이스에는 읽기 전용 구성이 있습니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 보려는 구성이 있는 디바이스 또는 모델을 선택합니다.

단계 **5** 오른쪽의 관리 창에서 **Configuration(**구성**)**를 클릭합니다.
전체 구성 파일이 표시됩니다.

관련 정보**:**

- 전체 디바이스 구성 파일 편집

## 전체 디바이스 구성 파일 편집

일부 디바이스 유형은 ASA와 같은 단일 구성 파일에 구성을 저장합니다. 이러한 디바이스의 경우 CDO에서 디바이스 구성 파일을 보고 디바이스에 따라 다양한 작업을 수행할 수 있습니다.

현재 ASA 구성 파일만 CDO를 사용하여 직접 편집할 수 있습니다.

**Caution** 이 절차는 디바이스 구성 파일의 구문에 익숙한 고급 사용자를 위한 것입니다. 이 방법은 Defense Orchestrator에 저장된 구성 파일의 복사본을 직접 변경합니다.

### 절차

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** **ASA** 탭을 클릭합니다.

단계 **4** 구성을 편집하려는 디바이스를 선택합니다.

단계 **5** 오른쪽의 관리 창에서 **Configuration(**구성**)**를 클릭합니다.

단계 **6** **Device Configuration(**디바이스 구성**)** 페이지에서 **Edit(**편집**)**를 클릭합니다.

단계 **7** 오른쪽의 편집기 버튼을 클릭하고 기본 텍스트 편집기, **Vim** 또는 **Emacs** 텍스트 편집기를 선택합니다.

단계 **8** 파일을 편집하고 변경 사항을 저장합니다.

단계 **9** **Devices & Services(**디바이스 및 서비스**)** 페이지로 돌아가 변경 사항을 미리 보고 배포합니다.

# CLI 명령 결과 내보내기

독립형 디바이스 또는 여러 디바이스에 실행된 CLI 명령의 결과를 쉼표로 구분된 값(.csv) 파일로 내보내 원하는 대로 정보를 필터링하고 정렬할 수 있습니다. 단일 디바이스 또는 여러 디바이스의 CLI 결과를 한 번에 내보낼 수 있습니다. 내보낸 정보에는 다음이 포함됩니다.

- 디바이스
- 날짜
- 사용자
- 명령
- 출력

# CLI 명령 결과 내보내기

명령 창에서 방금 실행한 명령의 결과를 .csv 파일로 내보낼 수 있습니다.

### 절차

단계 **1** 탐색 모음에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 디바이스를 선택하여 강조 표시하십시오.

단계 **5** 디바이스에 대한 **Device Actions(**디바이스 작업**)** 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **6** 명령줄 인터페이스 창에서 명령을 입력하고 **Send(**보내기**)**를 클릭하여 디바이스에 명령을 실행합니다.

단계 7 입력된 명령 창 오른쪽에서 내보내기 아이콘 를 클릭합니다.

단계 8 .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다. .csv 파일에서 명령 출력을 읽을 때 모든 셀을 확장하여 명령의 모든 결과를 확인합니다.

# CLI 매크로의 결과 내보내기

명령 창에서 실행된 매크로의 결과를 내보낼 수 있습니다. 하나 이상의 디바이스에서 실행된 CLI 매크로의 결과를 .csv 파일로 내보내려면 다음 절차를 따르십시오.

단계 1 **Devices & Services(**디바이스 및 서비스**)** 페이지를 엽니다.

단계 2 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 디바이스를 선택하여 강조 표시하십시오.

단계 5 디바이스에 대한 **Device Actions(**디바이스 작업**)** 창에서 >_**Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 6 CLI 창의 왼쪽 창에서 CLI 매크로 즐겨찾기 별표 를 선택합니다.

단계 7 내보낼 매크로 명령을 클릭합니다. 적절한 매개변수를 입력하고 **Send(**보내기**)**를 클릭합니다.

단계 8 입력된 명령 창 오른쪽에서 내보내기 아이콘 를 클릭합니다.

단계 9 .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다. .csv 파일에서 명령 출력을 읽을 때 모든 셀을 확장하여 명령의 모든 결과를 확인합니다.

# CLI 명령 기록 내보내기

다음 절차를 사용하여 하나 또는 여러 디바이스의 CLI 기록을 .csv 파일로 내보냅니다.

단계 1 탐색 창에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 2 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 디바이스를 선택하여 강조 표시하십시오.

단계 5 디바이스에 대한 디바이스 작업 창에서 >_**Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 6 아직 확장되지 않은 경우 시계 아이콘 을 클릭하여 기록 창을 확장합니다.

단계 7 입력된 명령 창 오른쪽에서 내보내기 아이콘 를 클릭합니다.

단계 8 .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다. .csv 파일에서 명령 출력을 읽을 때 모든 셀을 확장하여 명령의 모든 결과를 확인합니다.

관련 정보:

- CDO 명령줄 인터페이스, on page 93
- 새 명령에서 CLI 매크로 생성
- CLI 매크로 삭제
- CLI 매크로 편집
- CLI 매크로 실행
- ASA 대량 CLI 사용 사례
- ASA 명령줄 인터페이스 설명서
- 대량 명령줄 인터페이스

## CLI 매크로 목록 내보내기

명령 창에서 실행된 매크로만 내보낼 수 있습니다. 다음 절차를 사용하여 하나 이상의 디바이스의 CLI 매크로를 .csv 파일로 내보냅니다.

단계 1 탐색 창에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.
단계 2 **Devices(**디바이스**)** 탭을 클릭합니다.
단계 3 해당 디바이스 탭을 클릭합니다.
단계 4 디바이스를 선택하여 강조 표시하십시오.
단계 5 디바이스에 대한 디바이스 작업 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.
단계 6 CLI 창의 왼쪽 창에서 CLI 매크로 즐겨찾기 별표 ★를 선택합니다.
단계 7 내보낼 매크로 명령을 클릭합니다. 적절한 매개변수를 입력하고 **Send(**보내기**)**를 클릭합니다.
단계 8 입력된 명령 창 오른쪽에서 내보내기 아이콘  를 클릭합니다.
단계 9 .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다.

# 변경 사항 읽기, 삭제, 확인 및 구축

디바이스를 관리하려면 CDO의 로컬 데이터베이스에 저장된 디바이스 구성의 자체 복사본이 있어야 합니다. CDO는 관리하는 디바이스에서 구성을 "읽을 때" 디바이스 구성의 복사본을 가져와 저장합니다. CDO가 디바이스 구성의 복사본을 처음 읽고 저장하는 경우는 디바이스가 온보딩될 때입니다. 이러한 선택 항목은 다양한 목적으로 구성을 읽는 것을 설명합니다.

- **Discard Changes(**변경 사항 취소**)**는 디바이스의 구성 상태가 "Not Synced(동기화되지 않음)"인 경우에 사용할 수 있습니다. Not Synced(동기화되지 않음) 상태에서는 CDO에서 보류 중인 디바이스의 구성에 대한 변경 사항이 있습니다. 이 옵션을 사용하면 보류 중인 모든 변경 사항을 취소할 수 있습니다. 보류 중인 변경 사항이 삭제되고 CDO가 디바이스에 저장된 구성의 복사본으로 구성의 복사본을 덮어씁니다.
- 변경 사항을 확인합니다. 이 작업은 디바이스의 구성 상태가 동기화됨인 경우에 사용할 수 있습니다. Checking for Changes(변경 사항 확인)를 클릭하면 CDO가 디바이스의 구성 복사본을 디바이스에 저장된 구성의 복사본과 비교하게 됩니다. 차이가 있는 경우 CDO는 디바이스에 저장된 복사본으로 디바이스 구성의 복사본을 즉시 덮어씁니다.
- 충돌을 검토하고 검토 없이 수락합니다. . 디바이스에서 Conflict Detection(충돌 탐지)을 활성화한 경우 CDO는 10분마다 디바이스의 구성 변경 사항을 확인합니다. 디바이스에 저장된 구성의 복사본이 변경된 경우 CDO는 "Conflict Detected(충돌 탐지됨)" 구성 상태를 표시하여 사용자에게 알립니다.
  - 충돌을 검토합니다. Review Conflict(충돌 검토)를 클릭하면 디바이스에서 직접 변경 사항을 검토하고 이를 수락하거나 거부할 수 있습니다.
  - 검토 없이 수락합니다**.** 이 작업은 CDO의 디바이스 구성 복사본을 디바이스에 저장된 구성의 최신 복사본으로 덮어씁니다. CDO에서는 덮어쓰기 작업을 수행하기 전에 구성의 두 복사본에서 차이점을 확인하라는 메시지를 표시하지 않습니다.

모두 읽기는 대량 작업입니다. 상태에 상관없이 둘 이상의 디바이스를 선택하고 **Read All(**모두 읽기**)**을 클릭하여 CDO에 저장된 모든 디바이스의 구성을 디바이스에 저장된 구성으로 덮어쓸 수 있습니다.

### 변경 사항 구축

디바이스의 구성을 변경하면 CDO는 변경 사항을 구성의 자체 복사본에 저장합니다. 이러한 변경 사항은 디바이스에 구축될 때까지 CDO에서 "보류 중"입니다. 디바이스에 구축되지 않은 설정 변경 사항이 있는 경우 디바이스는 동기화되지 않음 설정 상태가 됩니다.

보류 중인 구성 변경 사항은 디바이스를 통해 실행되는 네트워크 트래픽에 영향을 주지 않습니다. CDO가 디바이스에 변경 사항을 구축한 후에야 적용됩니다. CDO는 디바이스의 구성에 변경 사항을 구축할 때 변경된 구성의 요소만 덮어씁니다. 디바이스에 저장된 전체 구성 파일을 덮어쓰지 않습니다. 구축은 단일 디바이스 또는 둘 이상의 디바이스에서 동시에 시작할 수 있습니다.

참고 구축 또는 반복 구축을 예약할 수 있습니다. 자세한 내용은 자동 구축 예약, 359 페이지를 참조하십시오.

**Discard All(**모두 취소**)**은 **Preview and Deploy(**미리보기 및 구축**)...**를 클릭한 후에만 사용할 수 있는 옵션입니다.. Preview and Deploy(미리보기 및 구축)를 클릭하면 CDO는 CDO에 보류 중인 변경 사항의 미리보기를 표시합니다. **Discard All(**모두 취소**)**을 클릭하면 CDO에서 보류 중인 모든 변경 사항이 삭제되며 선택한 디바이스에 어떤 것도 구축되지 않습니다. 위의 "변경 사항 취소"와 달리 보류 중인 변경 사항을 삭제하면 작업이 종료됩니다.

# 모든 디바이스 구성 읽기

CDO(Cisco Defense Orchestrator) 외부의 디바이스에 대한 구성이 변경되면 CDO에 저장된 디바이스의 구성과 디바이스 구성의 로컬 복사본은 더 이상 동일하지 않습니다. 구성을 다시 동일하게 만들기 위해 디바이스에 저장된 구성으로 CDO의 디바이스 구성 복사본을 덮어쓰려는 경우가 많습니다. **Read All(**모두 읽기**)** 링크를 사용하여 여러 디바이스에서 동시에 이 작업을 수행할 수 있습니다.

CDO에서 디바이스 구성의 두 복사본을 관리하는 방법에 대한 자세한 내용은 변경 사항 읽기, 삭제, 확인 및 구축을 참조하십시오.

다음은 **Read All(**모두 읽기**)**을 클릭하면 CDO의 디바이스 구성 복사본을 디바이스의 구성 복사본으로 덮어쓰는 세 가지 구성 상태입니다.

- 충돌 탐지 -충돌 탐지가 활성화된 경우 CDO는 구성 변경 사항에 대해 10분마다 관리하는 디바이스를 폴링합니다. CDO는 디바이스의 구성이 변경된 것을 발견하면 디바이스에 대한 구성 상태를 "충돌 탐지됨"으로 표시합니다.
- 동기화됨 -디바이스가 동기화된 상태인 경우 **Read All(**모두 읽기**)**을 클릭하면 CDO는 즉시 디바이스를 확인하여 구성이 직접 변경되었는지 확인합니다. **Read All(**모두 읽기**)**을 클릭하면 CDO가 디바이스 구성의 복사본을 덮어쓸 것임을 확인한 다음 덮어쓰기를 수행합니다.
- 동기화되지 않음 - 디바이스가 Not Synced(동기화되지 않음) 상태인 경우 **Read All(**모두 읽기**)**을 클릭하면 CDO는 CDO를 사용하는 디바이스의 구성에 대해 보류 중인 변경 사항이 있으며 Read All(모두 읽기) 작업을 진행하면 해당 변경 사항이 삭제되고 디바이스의 구성이 포함된 CDO의 구성 복사본입니다. 이 Read All(모두 읽기)은 변경 사항 취소와 같은 기능을 합니다.

---

단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** (선택 사항) 변경 로그에서 이 대량 작업의 결과를 쉽게 식별할 수 있도록 변경 요청 관리을 생성합니다.

단계 **5** CDO를 저장할 디바이스를 선택합니다. CDO는 선택한 모든 디바이스에 적용할 수 있는 작업에 대해서만 명령 버튼을 제공합니다.

단계 **6** **Read All(**모두 읽기**)**을 클릭합니다.

단계 **7** CDO는 CDO에 준비된 구성 변경 사항이 있는 경우 선택한 디바이스에 대해 경고하고, 구성 대량 읽기 작업을 계속할 것인지 묻습니다. 계속하려면 **Read All(**모두 읽기**)**을 클릭합니다.

단계 **8** Read All(모두 읽기) 구성 작업의 진행 상황은 작업 페이지에서 확인합니다. 대량 작업의 개별 작업이 성공하거나 실패한 방식에 대한 자세한 내용을 보려면 파란색 Review(검토) 링크를 클릭합니다. 그러면 작업 페이지 페이지로 이동합니다.

단계 **9** 변경 요청 레이블을 생성하고 활성화한 경우 실수로 다른 구성 변경 사항을 이 이벤트와 연결하지 않도록 레이블을 지워야 합니다.

---

관련 정보

- 변경 사항 읽기, 삭제, 확인 및 구축

# ASA에서 CDO로 구성 변경 읽기

**Cisco Defense Orchestrator가 ASA 디바이스 구성을 "읽는" 이유는 무엇입니까?**

ASA를 관리하려면, CDO에 ASA의 실행 중인 구성 파일의 자체 저장된 복사본이 있어야 합니다. CDO가 디바이스 구성 파일의 복사본을 처음 읽고 저장하는 경우는 디바이스가 온보딩될 때입니다. 이후에 CDO가 ASA에서 구성을 읽을 때, 변경 사항 확인, 검토 없이 수락 또는 구성 읽기를 선택하게 됩니다. 자세한 내용은 변경 사항 읽기, 삭제, 확인 및 구축를 참조하십시오.

CDO는 또한 다음과 같은 상황에서 ASA 구성을 읽어야 합니다.

- 구성 변경 사항을 ASA에 배포하지 못했고 디바이스 상태가 목록에 없거나 동기화되지 않음입니다.
- 디바이스 온보딩에 실패했으며 디바이스 상태가 구성 없음입니다.
- CDO 외부에서 디바이스 구성을 변경했으며 변경 사항이 폴링되거나 감지되지 않았습니다. 디바이스 상태는 동기화됨 또는 충돌 감지됨입니다.

이러한 경우 CDO는 디바이스에 저장된 마지막으로 알려진 구성의 복사본이 필요합니다.

## ASA에서 구성 변경 사항 읽기

ASA에서 구성 변경 사항을 읽으라는 메시지가 표시되는 경우:

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.
단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.
단계 **3** 해당 디바이스 탭을 클릭합니다.
단계 **4** CDO가 최근 온보딩에 실패한 디바이스 또는 CDO가 변경 사항을 배포하지 못한 디바이스를 선택합니다.
단계 **5** 오른쪽의 동기화됨 창에서 **Read Configuration(**구성 읽기**)**를 클릭합니다. 이 옵션은 현재 CDO에 저장된 구성을 덮어씁니다.

# 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축

테넌트의 디바이스에 대한 구성을 변경했지만 해당 변경 사항을 구축하지 않은 경우 Deploy(구축) 아이콘

. 이러한 변경의 영향을 받는 디바이스는 **Devices and Services(**디바이스 및 서비스**)** 페이지에서 "Not Synced(동기화되지 않음)" 상태로 표시됩니다. **Deploy(**구축**)**를 클릭하면 보류 중인 변경 사항이 있는 디바이스를 검토하고 해당 디바이스에 변경 사항을 구축할 수 있습니다.

이 구축 방법은 지원되는 모든 디바이스에서 사용할 수 있습니다.

단일 구성 변경 사항에 이 구축 방법을 사용하거나, 기다렸다가 여러 변경 사항을 한 번에 구축할 수 있습니다.

## SUMMARY STEPS

1. 화면의 오른쪽 상단에서 **Deploy(**구축**)** 아이콘  을 클릭합니다**.**
2. 구축하려는 변경 사항이 있는 디바이스를 선택합니다. 디바이스에 노란색 주의 삼각형이 있는 경우 해당 디바이스에 변경 사항을 구축할 수 없습니다. 노란색 주의 삼각형 위에 마우스를 올려놓으면 해당 디바이스에 변경 사항을 구축할 수 없는 이유를 확인할 수 있습니다.
3. 디바이스를 선택한 후 오른쪽 패널에서 디바이스를 확장하고 특정 변경 사항을 미리 볼 수 있습니다.
4. (선택 사항) 보류 중인 변경 사항에 대한 자세한 정보를 보려면 **View Detailed Changelog(**자세한 변경 로그 보기**)** 링크를 클릭하여 해당 변경과 관련된 변경 로그를 엽니다. **Deploy(**구축**)** 아이콘을 클릭하여 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지로 돌아갑니다.
5. (선택 사항) **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에서 나가지 않고 변경 사항을 추적하려면 변경 요청 관리합니다.
6. 선택한 디바이스에 변경 사항을 즉시 구축하려면 **Deploy Now(**지금 구축**)**를 클릭합니다. 작업 트레이의 활성 작업 표시기에 진행 상황이 표시됩니다.
7. (선택 사항) 구축이 완료되면 CDO 탐색 모음에서 **Jobs(**작업**)**를 클릭합니다. 구축 결과를 보여주는 최근 "Deploy Changes(변경 사항 구축)" 작업이 표시됩니다.
8. 변경 요청 레이블을 생성했으며 더 이상 연결할 구성 변경 사항이 없는 경우 해당 레이블을 지웁니다.

## DETAILED STEPS

단계 **1** 화면의 오른쪽 상단에서 **Deploy(**구축**)** 아이콘  을 클릭합니다**.**

단계 **2** 구축하려는 변경 사항이 있는 디바이스를 선택합니다. 디바이스에 노란색 주의 삼각형이 있는 경우 해당 디바이스에 변경 사항을 구축할 수 없습니다. 노란색 주의 삼각형 위에 마우스를 올려놓으면 해당 디바이스에 변경 사항을 구축할 수 없는 이유를 확인할 수 있습니다.

단계 **3** 디바이스를 선택한 후 오른쪽 패널에서 디바이스를 확장하고 특정 변경 사항을 미리 볼 수 있습니다.

단계 **4** (선택 사항) 보류 중인 변경 사항에 대한 자세한 정보를 보려면 **View Detailed Changelog(**자세한 변경 로그 보기**)** 링크를 클릭하여 해당 변경과 관련된 변경 로그를 엽니다. **Deploy(**구축**)** 아이콘을 클릭하여 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지로 돌아갑니다.

단계 **5** (선택 사항) **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에서 나가지 않고 변경 사항을 추적하려면 변경 요청 관리합니다.

단계 6 선택한 디바이스에 변경 사항을 즉시 구축하려면 **Deploy Now(**지금 구축**)**를 클릭합니다. 작업 트레이의 활성 작업 표시기에 진행 상황이 표시됩니다.

단계 7 (선택 사항) 구축이 완료되면 CDO 탐색 모음에서 **Jobs(**작업**)**를 클릭합니다. 구축 결과를 보여주는 최근 "Deploy Changes(변경 사항 구축)" 작업이 표시됩니다.

단계 8 변경 요청 레이블을 생성했으며 더 이상 연결할 구성 변경 사항이 없는 경우 해당 레이블을 지웁니다.

---

다음에 수행할 작업

- 예약된 자동 배포
- CDO에서 ASA로 구성 변경 사항 구축, 354 페이지
- ASA에 구축한 후 로그 항목 변경, 371 페이지

# CDO에서 ASA로 구성 변경 사항 구축

**CDO**가 **ASA**에 변경 사항을 구축하는 이유

CDO(Cisco Defense Orchestrator)를 사용하여 디바이스의 구성을 관리하고 변경하면 CDO는 변경 사항을 구성 파일의 자체 복사본에 저장합니다. 이러한 변경 사항은 디바이스에 "구축"될 때까지 CDO에서 "준비된" 것으로 간주됩니다. 준비된 구성 변경은 디바이스를 통해 실행되는 네트워크 트래픽에 영향을 주지 않습니다. CDO가 디바이스에 변경 사항을 "구축"한 후에야 디바이스를 통해 실행되는 트래픽에 영향을 미칩니다. CDO는 디바이스의 구성에 변경 사항을 구축할 때 변경된 구성의 요소만 덮어씁니다. 디바이스에 저장된 전체 구성 파일을 덮어쓰지 않습니다.

ASA에는 "실행 중인" 구성 파일("실행 중인 구성"이라고도 함)과 "시작" 구성 파일("시작 구성"이라고도 함)이 있습니다. 실행 중인 구성 파일에 저장된 구성은 ASA를 통과하는 트래픽에 적용됩니다. 실행 중인 구성을 변경하고 해당 변경 사항이 생성하는 동작에 만족하면 시작 구성에 구축할 수 있습니다. ASA가 재부팅된 경우 시작 구성을 구성 시작점으로 사용합니다. 시작 구성에 저장되지 않은 실행 중인 구성에 대한 변경 사항은 ASA가 리부팅된 후 손실됩니다.

CDO에서 ASA로 변경 사항을 구축할 때는 실행 중인 구성 파일에 해당 변경 사항을 기록합니다. 이러한 변경 사항으로 인해 생성되는 동작에 만족하면 해당 변경 사항을 시작 구성 파일에 구축할 수 있습니다.

구축은 단일 디바이스 또는 둘 이상의 디바이스에서 동시에 시작할 수 있습니다. 단일 디바이스에 대해 개별 구축 또는 반복 구축을 예약할 수 있습니다.

일부 변경 사항은 **ASA**에 직접 구축됩니다**.**

CDO에서 CDO 명령줄 인터페이스 디바이스 관리를 위한 CLI 매크로 인터페이스를 사용하여 ASA를 변경하는 경우 이러한 변경 사항은 CDO에서 "스테이징"되지 않습니다. ASA의 실행 중인 구성에 직접 구축됩니다. 이러한 방식으로 변경하면 디바이스는 CDO와 "동기화"된 상태로 유지됩니다.

# 구성 변경 사항 배포 정보

이 섹션에서는 CDO의 GUI를 사용하거나 CDO의 CLI 인터페이스 또는 CLI 매크로 인터페이스를 사용하지 않고 디바이스 구성 페이지를 편집하여 ASA 구성 파일을 변경한다고 가정합니다.

ASA 구성 업데이트는 2단계 프로세스입니다.

단계 **1** 다음 방법 중 하나를 사용하여 CDO를 변경합니다.

- CDO GUI
- 디바이스 구성 페이지의 디바이스 구성

단계 **2** 변경한 후 Devices & Services(디바이스 및 서비스) 페이지로 돌아간 다음 디바이스에 대한 변경 사항을 미리 보고 배포**...**합니다.

다음에 수행할 작업

CDO가 ASA의 실행 구성을 CDO에 준비된 구성으로 업데이트하거나 ASA에 저장된 실행 구성으로 CDO의 구성을 변경할 때 구성의 해당 측면을 CDO GUI로 관리할 수 있으면 구성 파일의 관련 행만 변경하려고 시도합니다. CDO GUI를 사용하여 원하는 구성을 변경할 수 없는 경우, CDO는 변경을 위해 전체 구성 파일을 덮어쓰려고 시도합니다.

다음은 두 가지 예입니다.

- CDO GUI를 사용하여 네트워크 개체를 생성하거나 변경할 수 있습니다. CDO가 해당 변경 사항을 ASA의 구성에 배포해야 하는 경우, 변경이 발생할 때 ASA에서 실행 중인 구성 파일의 관련 줄을 덮어씁니다.
- CDO GUI를 사용하여 새 로컬 ASA 사용자를 생성 할 수 없지만, 디바이스 구성 페이지에서 ASA의 구성을 편집하여 생성할 수 있습니다. 디바이스 구성 페이지에서 사용자를 추가하고 해당 변경 사항을 ASA에 배포하는 경우, CDO는 실행 중인 전체 구성 파일을 덮어써 해당 변경 사항을 ASA에서 실행 중인 구성 파일에 저장하려고 합니다.

# **CDO GUI**를 사용하여 구성 변경 사항 구축

단계 **1** CDO GUI를 사용하여 구성을 변경하고 변경 사항을 저장하면 해당 변경 사항은 ASA의 실행 중인 구성 파일의 CDO에 저장된 버전에 저장됩니다.

단계 **2** **Inventory(**재고 목록**)** 페이지의 디바이스로 돌아갑니다.

단계 **3** Devices(디바이스) 탭을 클릭합니다. 이제 디바이스가 "동기화되지 않음"으로 표시됩니다.

단계 **4** 다음 방법 중 하나를 사용하여 변경 사항을 구축합니다.

- 화면의 오른쪽 상단에 있는 **Deploy(**구축**)** 아이콘 을 클릭합니다. 이렇게 하면 디바이스에 대한 변경 사항을 구축하기 전에 검토할 수 있습니다. 변경한 디바이스를 확인하고 디바이스를 확장하여 변경 사항을 검토한 후 **Deploy Now(**지금 구축**)**를 클릭하여 변경 사항을 구축합니다.

  참고 Devices with Pending Changes(보류 중인 변경 사항이 있는 디바이스) 화면에서 디바이스 옆에 노란색 경고 삼각형이 표시되면 변경 사항을 구축할 수 없습니다. 디바이스에 변경 사항을 구축할 수 없는 이유를 알아보려면 경고 삼각형 위에 마우스를 올려놓습니다.

- Not Synced(동기화되지 않음) 창에서 **Preview and Deploy(**미리보기 및 구축**)...**를 클릭합니다.

  1. ASA 구성 파일을 변경하는 명령을 검토합니다.
  2. 명령에 만족하는 경우 Configuration Recovery Preference(구성 복구 기본 설정)를 선택합니다.

     참고 "알려주시면 구성을 수동으로 복원하겠습니다."를 선택합니다. 계속하기 전에 **View Manual Synchronization Instructions(**수동 동기화 지침 보기**)**를 클릭합니다.

  3. **Apply Changes to Device(**변경 사항 적용**)**를 클릭합니다.
  4. 성공 메시지에서 확인하려면 **OK(**확인**)**를 클릭합니다.

# 자동 배포 예약

또한 자동 구축 예약하여 단일 디바이스 또는 보류 중인 변경 사항이 있는 모든 디바이스에 대한 배포를 예약하도록 테넌트를 구성할 수 있습니다.

# CDO의 CLI 인터페이스를 사용하여 구성 변경 사항 배포

단계 **1** 탐색 창에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 구성을 변경하려는 디바이스를 선택합니다.

단계 **5** **Actions(**작업**)** 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **6** 명령줄 인터페이스 테이블에 명령이 있으면 **Clear(**지우기**)**를 클릭하여 제거합니다.

단계 **7** 명령줄 인터페이스 테이블의 상단 상자에 명령 프롬프트에 명령을 입력합니다. 각 명령을 해당 줄에 입력하거나 구성 파일의 섹션을 명령으로 입력하여 단일 명령 또는 여러 명령을 일괄적으로 실행할 수 있습니다. 다음은 명령줄 인터페이스 테이블에 입력할 수 있는 몇 가지 명령의 예입니다.

네트워크 개체 "albany"를 생성하는 단일 명령

```
object network albany
host 209.165.30.2
```

여러 명령이 함께 전송됨:

```
object network albany
host 209.165.30.2
object network boston
host 209.165.40.2
object network cambridge
host 209.165.50.2
```

명령으로 입력된 실행 중인 구성 파일의 섹션:

```
interface GigabitEthernet0/5
 nameif guest
 security-level 0
 no ip address
```

참고 CDO는 EXEC 모드, Privileged EXEC 모드 및 전역 구성 모드 사이를 이동할 필요가 없습니다. 적절한 맥락에서 입력한 명령을 해석합니다.

단계 **8** 명령을 입력한 후 **Send(**보내기**)**를 클릭합니다. CDO가 ASA에서 실행 중인 구성 파일에 대한 변경 사항을 성공적으로 배포한 후 Done!(완료!)를 수신합니다.

단계 **9** 명령을 전송한 후 "일부 명령이 실행 중인 구성을 변경했을 수 있습니다."라는 메시지와 함께 두 개의 링크가 표시될 수 있습니다.

- **Deploy to Disk(**디스크에 배포**)**를 클릭하면 이 명령에 의해 변경된 사항과 실행 중인 구성의 다른 모든 변경 사항이 ASA의 시작 구성에 저장됩니다.
- **Dismiss(**해제**)**를 클릭하면 메시지가 사라집니다.

# 디바이스 구성을 편집하여 구성 변경 사항 배포

⚠

주의 이 절차는 ASA 구성 파일의 구문에 익숙한 고급 사용자를 위한 것입니다. 이 방법은 CDO에 저장된 실행 중인 구성 파일을 직접 변경합니다.

단계 **1** 탐색 창에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 구성을 변경하려는 디바이스를 선택합니다.

단계 **5** 작업 창에서 **View Configuration(**구성 보기**)**를 클릭합니다.

단계 **6** **Edit(**편집**)**를 클릭합니다.

단계 **7** 실행 중인 구성을 변경하고 **Save(**저장**)**합니다.

단계 **8** Devices & Services(디바이스 및 서비스) 페이지로 돌아갑니다. 동기화되지 않음 창에서 **Preview and Deploy...(**미리보기 및 배포**...)**를 클릭합니다.

단계 **9** 디바이스 동기화 창에서 변경 사항을 검토합니다.

단계 **10** 변경 종류에 따라 **Replace Configuration(**구성 대체**)** 또는 **Apply Changes to Device(**디바이스에 변경 적용**)**를 클릭합니다.

# 여러 디바이스에서 공유 개체에 대한 구성 변경 사항 배포

두 개 이상의 디바이스에서 공유하는 정책 또는 개체를 변경할 때 이 절차를 사용합니다. 그러나 많은 디바이스에서 공통 정책을 사용하는 경우 공통 정책을 변경할 수 있습니다.

단계 **1** 편집할 공유 개체가 포함된 정책 페이지 또는 개체 페이지를 열고 편집합니다.

단계 **2** 공유 디바이스 목록을 검토하고 언급된 모든 디바이스에서 변경할 것인지 확인합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

단계 **5** **Deploy(**배포**)** 아이콘을 클릭하고 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.

# 디바이스 구성 대량 구축

예를 들어 공유 개체를 수정하여 여러 디바이스를 변경한 경우 해당 변경 사항을 영향을 받는 모든 디바이스에 한 번에 적용할 수 있습니다.

단계 **1** 탐색 창에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** CDO에서 구성을 변경한 모든 디바이스를 선택합니다. 이러한 디바이스는 "동기화되지 않음" 상태로 표시되어야 합니다.

단계 **5** 다음 방법 중 하나를 사용하여 변경 사항을 구축합니다.

- 화면의 오른쪽 상단에 있는 **Deploy(**구축**)** 버튼을 클릭합니다. 이렇게 하면 구축하기 전에 선택한 디바이스에서 보류 중인 변경 사항을 검토할 수 있습니다. **Deploy Now(**지금 구축**)**를 클릭하여 변경 사항을 구축합니다.

  **Note** **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 화면에서 디바이스 옆에 노란색 경고 삼각형이 표시되면 해당 디바이스에 변경 사항을 구축할 수 없습니다. 변경 사항을 해당 디바이스에 구축할 수 없는 이유에 대한 정보를 보려면 경고 삼각형 위에 마우스를 올려놓습니다.

- 세부 정보 창에서 **Deploy All(**모두 구축**)**을 클릭합니다. 경고를 검토하고 **OK(**확인**)**를 클릭합니다. 대량 구축은 변경 사항을 검토하지 않고 즉시 시작됩니다.

단계 **6** (선택 사항) 탐색 모음에서 Jobs(작업) 아이콘  을 클릭하여 대량 구축의 결과를 확인합니다.

관련 정보:

- 자동 구축 예약, on page 359

# 예약된 자동 배포

CDO를 사용하면 CDO에서 관리하는 하나 이상의 디바이스에 대한 구성을 변경한 다음 편리한 시간에 해당 디바이스에 변경 사항을 배포하도록 예약할 수 있습니다.

Settings(설정) 페이지의 **Tenant Settings(**테넌트 설정**)** 탭에 자동 구축 예약 옵션 활성화, on page 42 있는 경우에만 배포을 예약할 수 있습니다. 이 옵션이 활성화되면 예약된 배포을 생성, 편집 또는 삭제할 수 있습니다. 예약된 배포은 CDO에 저장된 모든 단계적 변경 사항을 설정된 날짜 및 시간에 배포합니다. Jobs(작업) 페이지에서 예약된 배포을 보고 삭제할 수도 있습니다.

CDO에서 변경 사항 읽기, 삭제, 확인 및 구축 않은 디바이스 변경 사항이 있는 경우 충돌이 해결될 때까지 예약된 배포을 건너뜁니다. 예약된 배포이 실패한 인스턴스가 Jobs(작업) 페이지에 나열됩니다. **Enable the Option to Schedule Automatic Deployments(**자동 구축 예약 옵션 활성화**)**가 해제된 경우 예약된 모든 배포이 삭제됩니다.

**Caution** 여러 디바이스에 대해 새 배포을 예약하는 경우 해당 디바이스 중 일부가 이미 배포을 예약한 경우, 새로 예약된 배포이 기존의 예약된 배포을 덮어씁니다.

**Note** 예약된 배포을 생성하면 디바이스의 표준 시간대가 아닌 현지 시간으로 일정이 생성됩니다. 예약된 배포은 일광 절약 시간에 맞게 자동으로 조정되지 않습니다.

# 자동 구축 예약

구축 일정은 단일 이벤트 또는 반복 이벤트일 수 있습니다. 반복 자동 구축을 사용하면 유지 보수 기간에 맞춰 반복 구축을 편리하게 이용할 수 있습니다. 단일 디바이스에 대해 일회성 또는 반복 구축을 예약하려면 다음 절차를 따르십시오.

**Note** 기존 구축이 예약된 디바이스에 대한 구축을 예약하는 경우 새로 예약된 구축이 기존 구축을 덮어씁니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 하나 이상의 디바이스를 선택합니다.

단계 **5** Device Details(디바이스 세부 정보) 창에서 Scheduled Deployments(예약된 구축) 탭을 찾아 **Schedule(**예약**)**을 클릭합니다.

단계 **6** 구축을 수행해야 하는 시기를 선택합니다.

- 일회성 구축의 경우 **Once on(**한 번**)** 옵션을 클릭하여 달력에서 날짜와 시간을 선택합니다.
- 반복 구축의 경우 **Every(**마다**)** 옵션을 클릭합니다. 매일 또는 일주일에 한 번 구축을 선택할 수 있습니다. 구축을 수행해야 하는 날짜와 시간을 선택합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

# 예약된 배포 편집

예약된 배포를 편집하려면 다음 절차를 따르십시오.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 하나 이상의 디바이스를 선택합니다.

단계 **5** **Device Details(**디바이스 세부 정보**)** 창에서 예약된 배포 탭을 찾아 **Edit(**편집**)**를 클릭합니다.

단계 **6** 예약된 배포의 반복, 날짜 또는 시간을 편집합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

# 예약된 배포 삭제

예약된 배포를 삭제하려면 다음 절차를 따르십시오.

**Note** 여러 디바이스에 대한 배포를 예약한 다음 일부 디바이스에 대한 일정을 변경하거나 삭제하면 나머지 디바이스에 대한 원래 예약된 배포가 유지됩니다.

단계 **1** 탐색 모음에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 2 **Devices(**디바이스**)** 탭을 클릭합니다.
단계 3 해당 디바이스 탭을 클릭합니다.
단계 4 하나 이상의 디바이스를 선택합니다.
단계 5 **Device Details(**장치 세부 정보**)**창에서 예약된 배포 탭을 찾아 **Delete(**삭제**)**를 클릭합니다.

**What to do next**

- 변경 사항 읽기, 삭제, 확인 및 구축
- 모든 디바이스 구성 읽기, on page 351
- CDO에서 ASA로 구성 변경 사항 구축, on page 354
- 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, on page 352

# 구성 변경 사항 확인

디바이스의 구성이 디바이스에서 직접 변경되었으며 CDO에 저장된 구성의 복사본과 더 이상 동일하지 않은지 확인하려면 변경 사항을 확인합니다. 디바이스가 "Synced(동기화됨)" 상태일 때 이 옵션이 표시됩니다.

변경 사항을 확인하려면 다음을 수행합니다.

단계 1 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.
단계 2 **Devices(**디바이스**)** 탭을 클릭합니다.
단계 3 해당 디바이스 탭을 클릭합니다.
단계 4 구성이 디바이스에서 직접 변경되었을 가능성이 있는 디바이스를 선택합니다.
단계 5 오른쪽의 Synced(동기화) 창에서 **Check for Changes(**변경 사항 확인**)**를 클릭합니다.
단계 6 다음 동작은 디바이스에 따라 약간 다릅니다.

- 디바이스의 경우 디바이스의 구성이 변경된 경우 다음 메시지가 표시됩니다.

  디바이스에서 정책을 읽는 중입니다. 디바이스에 활성 구축이 있는 경우 완료 후 읽기가 시작됩니다.

  - 계속하려면 **OK(**확인**)**를 클릭하십시오. 디바이스의 구성이 CDO에 저장된 구성을 덮어씁니다.
  - 작업을 취소하려면 **Cancel(**취소**)**을 클릭합니다.

- ASA 디바이스의 경우:

a. 표시되는 두 가지 구성을 비교합니다. **Continue(**계속**)**를 클릭합니다. **Last Known Device Configuration(**마지막으로 알려진 디바이스 구성**)** 레이블이 지정된 구성은 CDO에 저장된 구성입니다. **Found on Device(**디바이스에서 발견**)** 레이블이 지정된 구성은 ASA에 저장된 구성입니다.

b. 다음 중 하나를 선택합니다.

1. "마지막으로 알려진 디바이스 구성"을 유지하려면 대역 외 변경 사항을 거부합니다.
2. 대역 외 변경 사항을 수락하여 CDO에 저장된 디바이스의 구성을 디바이스에 있는 구성으로 덮어씁니다.

c. **Continue(**계속**)**를 클릭합니다.

# 변경 사항 취소

CDO를 사용하여 디바이스의 구성에 적용한 구축 해제된 구성 변경 사항을 모두 "실행 취소"하려면 **Discard Changes(**변경 사항 취소**)**를 클릭합니다. **Discard Changes(**변경 사항 취소**)**를 클릭하면 CDO는 디바이스 구성의 로컬 복사본을 디바이스에 저장된 구성으로 완전히 덮어씁니다.

**Discard Changes(**변경 사항 취소**)**를 클릭하면 디바이스의 구성 상태가 **Not Synced(**동기화되지 않음**)** 상태가 됩니다. 변경 사항을 취소하면 CDO의 구성 복사본이 디바이스의 구성 복사본과 동일하게 되며 CDO의 구성 상태는 Synced(동기화)로 돌아갑니다.

디바이스에 대해 구축되지 않은 모든 구성 변경 사항을 취소하거나 "실행 취소"하려면 다음을 수행합니다.

단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 구성을 변경한 디바이스를 선택합니다.

단계 **5** 오른쪽의 Not Synced(동기화되지 않음) 창에서 **Discard Changes(**변경 사항 취소**)**를 클릭합니다.

- FDM 관리 디바이스의 경우 CDO는 "CDO에서 보류 중인 변경 사항이 취소되고 이 디바이스에 대한 CDO 구성이 디바이스에서 현재 실행 중인 구성으로 교체됩니다."라고 경고합니다. 변경 사항을 취소하려면 **Continue(**계속**)**를 클릭합니다.
- Meraki 디바이스의 경우 CDO가 변경 사항을 즉시 삭제합니다.
- AWS 디바이스의 경우 CDO는 삭제하려는 항목을 표시합니다. **Accept(**수락**)** 또는 **Cancel(**취소**)**을 클릭합니다.

# 디바이스의 대역 외 변경 사항

대역 외 변경 사항은 CDO를 사용하지 않고 디바이스에서 직접 변경한 사항을 의미합니다. 이러한 변경은 SSH 연결을 통해 디바이스의 명령줄 인터페이스를 사용하거나 ASA용 ASDM(Adaptive Security Device Manager) 또는 FDM 관리 디바이스용 FDM과 같은 로컬 관리자를 사용하여 수행할 수 있습니다. 대역 외 변경은 CDO에 저장된 디바이스의 구성과 디바이스 자체에 저장된 구성 간에 충돌을 일으킵니다.

디바이스에서 대역외 변경 탐지

ASA, FDM 관리 디바이스 또는 Cisco IOS 디바이스에 대해 Conflict Detection(충돌 탐지)이 활성화된 경우 CDO는 10분마다 디바이스를 확인하여 CDO 외부에서 디바이스의 구성에 직접 적용된 새로운 변경 사항을 검색합니다.

CDO에 저장되지 않은 디바이스 구성 변경 사항이 있음을 발견하면 CDO는 해당 디바이스의 구성 상태를 "충돌 탐지됨" 상태로 변경합니다.

Defense Orchestrator에서 충돌을 탐지하는 경우 다음 두 가지 조건 중 하나가 발생할 수 있습니다.

- CDO의 데이터베이스에 저장되지 않은 디바이스에 직접 적용된 구성 변경 사항이 있습니다.
- FDM 관리 디바이스의 경우 구축되지 않은 FDM 관리 디바이스에 "보류 중인" 구성 변경 사항이 있을 수 있습니다.

# Defense Orchestrator와 디바이스 간 구성 동기화

구성 충돌 정보

디바이스 및 서비스 페이지에서 디바이스 또는 서비스의 상태가 "Synced(동기화됨)", "Not Synced(동기화되지 않음)" 또는 "Conflict Detected(충돌 탐지됨)"인 것을 확인할 수 있습니다.

- 디바이스가 동기화되면 CDO(Cisco Defense Orchestrator)의 구성과 디바이스에 로컬로 저장된 구성이 동일합니다.
- 디바이스가 동기화되지 않은 경우 CDO에 저장된 구성이 변경되었으며 이제 디바이스에 로컬로 저장된 구성이 다릅니다. CDO에서 디바이스로 변경 사항을 구축하면 CDO의 버전과 일치하도록 디바이스의 구성이 변경됩니다.
- CDO 외부에서 디바이스에 적용된 변경 사항을 대역 외 변경 사항이라고 합니다. 대역 외 변경이 수행되면 디바이스에 대해 충돌 탐지가 활성화된 경우 디바이스 상태가 "Conflict Detected(충돌 탐지됨)"로 변경됩니다. 대역 외 변경 사항을 수락하면 는 CDO의 구성을 디바이스의 구성과 일치하도록 변경합니다.

# 충돌 탐지

충돌 탐지가 활성화된 경우 CDO(Cisco Defense Orchestrator)는 기본 간격 동안 디바이스를 폴링하여 CDO 외부에서 디바이스의 구성이 변경되었는지 확인합니다. CDO는 변경 사항을 탐지하면 디바이스의 구성 상태를 **Conflict Detected(**충돌 탐지됨**)**로 변경합니다. CDO 외부에서 디바이스에 적용된 변경 사항을 "대역 외" 변경 사항이라고 합니다.

이 옵션이 활성화되면 디바이스별로 충돌 또는 OOB 변경 사항이 탐지되는 빈도를 구성할 수 있습니다. 자세한 내용은 디바이스 변경 사항에 대한 폴링 예약, on page 367를 참조하십시오.

# 충돌 탐지 활성화

충돌 감지를 활성화하면 Defense Orchestrator 외부의 디바이스가 변경된 인스턴스에 대해 경고합니다.

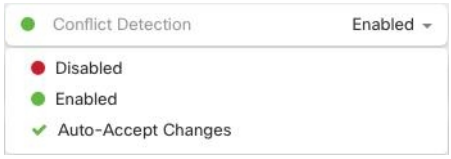
단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 선택합니다.

단계 **4** 충돌 탐지를 활성화할 디바이스를 선택합니다.

단계 **5** 디바이스 테이블 오른쪽에 있는 충돌 감지 상자의 목록에서 **Enabled(**활성화됨**)**을 선택합니다.




# 디바이스에서 대역외 변경 사항 자동 수락

변경 사항 자동 수락을 활성화하여 매니지드 디바이스에 대한 직접 변경 사항을 자동으로 수락하도록 CDO(Cisco Defense Orchestrator)를 구성할 수 있습니다. CDO를 사용하지 않고 디바이스에 직접 적용된 변경 사항을 대역 외 변경 사항이라고 합니다. 대역 외 변경은 CDO에 저장된 디바이스의 구성과 디바이스 자체에 저장된 구성 간에 충돌을 일으킵니다.

자동 수락 변경 기능은 충돌 탐지를 개선한 것입니다. 디바이스에서 변경 사항 자동 수락이 활성화된 경우 CDO는 10분마다 변경 사항을 확인하여 디바이스의 구성에 대한 대역 외 변경 사항이 있는지 확인합니다. 구성이 변경된 경우 CDO는 사용자에게 확인 상자를 표시하지 않고 디바이스 구성의 로컬 버전을 자동으로 업데이트합니다.

CDO에서 아직 디바이스에 구축되지 않은 구성 변경 사항이 있는 경우 CDO는 구성 변경을 자동으로 수락하지 않습니다. 화면의 프롬프트에 따라 다음 작업을 결정합니다.

자동 수락 변경 사항을 사용하려면 먼저 테넌트가 **Inventory(**재고 목록**)** 페이지의 Conflict Detection(충돌 탐지) 메뉴에서 auto-accept(자동 수락) 옵션을 표시하도록 활성화합니다. 그런 다음 개별 디바이스에 대한 변경 사항 자동 수락을 활성화합니다.

CDO가 대역 외 변경 사항을 탐지하지만 수동으로 수락하거나 거부할 수 있는 옵션을 제공하도록 하려면 대신 충돌 탐지, on page 363를 활성화합니다.

# 변경 사항 자동 수락 구성

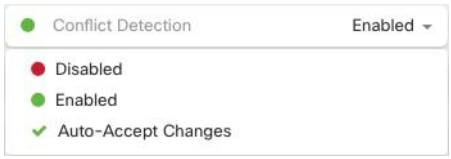
단계 **1** 관리자 또는 슈퍼 관리자 권한이 있는 계정을 사용하여 CDO에 로그인합니다.

단계 **2** CDO 메뉴에서 **Settings(**설정**)** > **General Settings(**일반 설정**)**를 탐색합니다.

단계 **3** **Tenant Settings(**테넌트 설정**)** 영역에서, 토글을 클릭하여 "디바이스 변경 사항을 자동으로 수락하는 옵션 활성화"로 전환합니다. 이렇게 하면 변경 사항 자동 수락 메뉴 옵션이 **Inventory(**인벤토리**)** 페이지의 충돌 감지 메뉴에 표시됩니다.

단계 **4** **Inventory(**인벤토리**)** 페이지를 열고 대역 외 변경을 자동으로 수락할 디바이스를 선택합니다.

단계 **5** **Conflict Detection(**충돌 감지**)** 메뉴의 드롭다운 메뉴에서 **Auto-Accept Changes(**변경 사항 자동 수락**)**을 선택합니다.




# 테넌트의 모든 디바이스에 대한 변경 사항 자동 수락 비활성화

단계 **1** 관리자 또는 슈퍼 관리자 권한이 있는 계정을 사용하여 CDO에 로그인합니다.

단계 **2** CDO 메뉴에서 **Settings(**설정**)** > **General Settings(**일반 설정**)**를 탐색합니다.

단계 **3** **Tenant Settings(**테넌트 설정**)** 영역에서 회색 X가 표시되도록 토글을 왼쪽으로 밀어 "디바이스 변경 사항을 자동으로 수락하는 옵션 활성화"를 비활성화합니다. 이렇게 하면 충돌 감지 메뉴에서 변경 사항 자동 수락 옵션이 비활성화되고 테넌트의 모든 디바이스에 대한 기능이 비활성화 됩니다.

**Note** "자동 수락"을 비활성화하면 CDO에 수락하기 전에 각 디바이스 충돌을 검토해야 합니다. 여기에는 이전에 변경 사항을 자동으로 수락하도록 구성된 디바이스가 포함됩니다.

# 구성 충돌 해결

이 섹션에서는 디바이스에서 발생하는 구성 충돌을 해결하는 방법에 대한 정보를 제공합니다.

## "동기화되지 않음" 상태 해결

다음 절차를 사용하여 구성 상태가 "동기화되지 않음"인 디바이스를 확인합니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 동기화되지 않은 것으로 보고된 디바이스를 선택합니다.

단계 **5** 오른쪽의 동기화되지 않음 패널에서 다음 중 하나를 선택합니다.

- 미리보기 및 배포... - CDO에서 디바이스로 구성 변경 사항을 푸시하려면 지금 수행한 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 한 번에 여러 변경 사항을 기다렸다가 배포하십시오.
- 변경 사항 취소 - CDO에서 디바이스로 구성 변경을 푸시하지 않으려는 경우, 또는 CDO에서 시작한 구성 변경을 "취소"하려는 경우. 이 옵션은 CDO에 저장된 구성을 디바이스에 저장된 실행 중인 구성으로 덮어씁니다.

# "충돌 탐지됨" 상태 해결

CDO를 사용하면 각 라이브 디바이스에서 충돌 탐지를 활성화하거나 비활성화할 수 있습니다. 충돌 탐지, on page 363이 활성화되어 있고 CDO를 사용하지 않고 디바이스의 구성을 변경한 경우, 디바이스의 구성 상태는 **Conflict Detected(**충돌 탐지됨**)**로 표시됩니다.

"충돌 탐지됨" 상태를 해결하려면 다음 절차를 수행합니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 충돌을 보고하는 디바이스를 선택하고 오른쪽의 세부 정보 창에서 **Review Conflict(**충돌 검토**)**를 클릭합니다.

단계 **5** **Device Sync(**디바이스 동기화**)** 페이지에서 강조 표시된 차이점을 검토하여 두 구성을 비교합니다.

- "Last Known Device Configuration(마지막으로 알려진 디바이스 구성)" 패널은 CDO에 저장된 디바이스 구성입니다.
- "Found on Device(디바이스에서 발견됨)" 패널은 ASA에서 실행 중인 구성에 저장된 구성입니다.

단계 **6** 다음 중 하나를 선택하여 충돌을 해결합니다.

- **Accept Device changes(**디바이스 변경 사항 수락**)**: 구성 및 **CDO**에 저장된 보류 중인 변경 사항을 디바이스의 실행 중인 구성으로 덮어씁니다.

  **Note** CDO는 명령줄 인터페이스 외부에서 Cisco IOS 디바이스에 변경 사항을 배포하는 것을 지원하지 않으므로, 충돌을 해결할 때 Cisco IOS 디바이스에 대한 유일한 선택은 **Accept Without Review(**검토 없이 수락**)**를 선택하는 것입니다.

- **Reject Device Changes(**디바이스 변경 거부**)**: 디바이스에 저장된 구성을 CDO에 저장된 구성으로 덮어씁니다.

**Note** 거부되거나 수락된 모든 구성 변경 사항은 변경 로그에 기록됩니다.

# 디바이스 변경 사항에 대한 폴링 예약

충돌 탐지, on page 363를 활성화했거나 Settings(설정) 페이지에서 **Enable device changes to auto-accept device changes(**디바이스 변경 자동 수락 옵션 활성화**)**를 선택한 경우 CDO는 기본 간격 동안 디바이스를 폴링하여 CDO 외부에서 디바이스의 구성이 변경되었는지 확인합니다. CDO가 디바이스별로 변경 사항을 폴링하는 빈도를 맞춤화할 수 있습니다. 이러한 변경 사항은 둘 이상의 디바이스에 적용할 수 있습니다.

디바이스에 대해 구성된 선택 항목이 없으면 "테넌트 기본값"에 대한 간격이 자동으로 구성됩니다.

**Note** **Devices & Services(**디바이스 및 서비스**)** 페이지에서 디바이스별 간격을 맞춤 설정하면 **General Settings(**일반 설정**)** 페이지에서 기본 충돌 탐지 간격로 선택한 폴링 간격이 재정의됩니다.

**Devices & Services(**디바이스 및 서비스**)** 페이지에서 **Conflict Detection(**충돌 탐지**)**을 활성화하거나 Settings(설정) 페이지에서 디바이스 변경 사항을 자동 수락하는 옵션을 활성화한 후 다음 절차를 사용하여 CDO가 디바이스를 폴링할 빈도를 예약합니다.

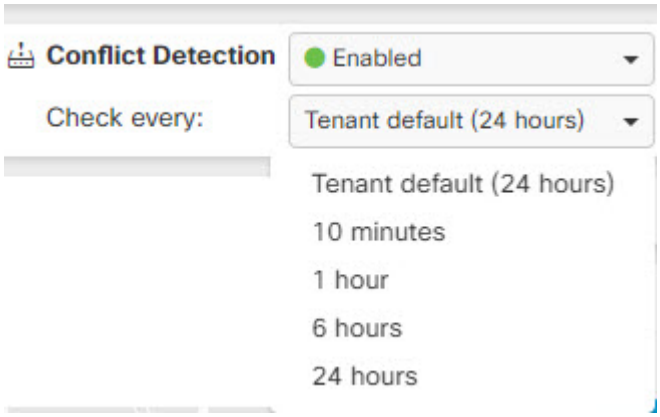
단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

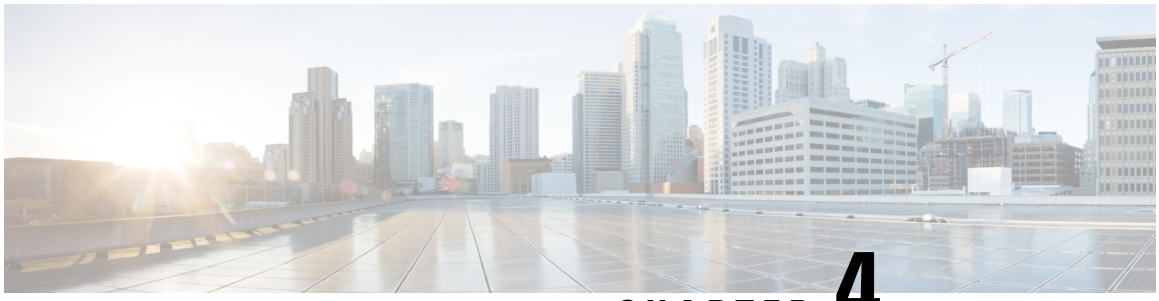
단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 충돌 탐지를 활성화할 디바이스를 선택합니다.

단계 **5** **Conflict Detection(**충돌 탐지**)**과 동일한 영역에서 **Check every(**확인 간격**)**의 드롭다운 메뉴를 클릭하고 원하는 폴링 간격을 선택합니다.





CHAPTER 4

# 모니터링 및 보고

CDO의 모니터링 및 보고 기능은 기존 정책 및 그로 인한 보안 태세의 영향에 대한 유용한 정보를 제공합니다.



## 변경 로그

### 변경 로그 정보

변경 로그는 CDO에서 수행되는 구성 변경 사항을 지속적으로 캡처합니다. 이 단일 보기에는 지원되는 모든 디바이스 및 서비스에 대한 변경 사항이 포함됩니다. 다음은 변경 로그의 몇 가지 기능입니다.

- 디바이스 구성에 대한 변경 사항을 나란히 비교합니다.
- 모든 변경 로그 항목에 대한 일반 영어 레이블입니다.
- 디바이스의 온보딩 및 제거를 기록합니다.
- CDO 외부에서 발생하는 정책 변경 충돌 탐지.
- 인시던트 조사 또는 문제 해결 중에 누가, 무엇을, 언제 하는지에 대한 답변을 제공합니다.
- 전체 변경 로그 또는 일부만 CSV 파일로 다운로드할 수 있습니다.

### 로그 용량 변경

CDO는 1년 동안 변경 로그에 정보를 보관합니다. 1년이 지난 정보는 삭제됩니다.

CDO가 데이터베이스에 저장하는 변경 로그 정보와 변경 로그를 내보낼 때 표시되는 정보는 다릅니다. 자세한 내용은 변경 로그를 CSV 파일로 내보내기, on page 374를 참조하십시오.

### 변경 로그 페이지의 변경 로그 항목

변경 로그 항목은 단일 디바이스 구성의 변경 사항, 디바이스에서 수행된 작업 또는 CDO 외부에서 디바이스가 변경된 경우를 반영합니다.

- 구성에 대한 변경 사항이 포함된 변경 로그 항목의 경우, 행의 아무 곳이나 클릭하여 변경 사항을 확장할 수 있습니다.
- 충돌로 탐지된 CDO 외부의 대역 외 변경 사항의 경우, 시스템 사용자는 마지막 사용자로 보고됩니다.
- CDO의 디바이스 구성이 디바이스의 구성과 동기화된 후 또는 디바이스가 CDO에서 제거되면 CDO는 변경 로그 항목을 닫습니다. 디바이스에서 CDO로 구성을 "읽은" 후 또는 CDO에서 디바이스로 구성을 배포하면 구성이 동기화됩니다.
- CDO는 기존 항목을 닫은 직후 새 변경 로그 항목을 생성합니다. 추가 구성 변경 사항이 열린 변경 로그 항목에 추가됩니다.
- 디바이스에 대한 읽기, 배포 및 삭제 작업에 대한 이벤트가 표시됩니다. 이러한 작업은 디바이스의 변경 로그를 닫습니다.
- CDO가 디바이스의 구성과 동기화되거나(읽기 또는 배포을 통해) CDO가 더 이상 디바이스를 관리하지 않는 경우 변경 로그가 닫힙니다.
- CDO 외부에서 디바이스가 변경되면 변경 로그에 "충돌 탐지됨" 항목이 기록됩니다.

### 활성 및 완료된 변경 로그 항목

변경 로그는 활성 또는 완료 상태입니다. CDO를 사용하여 디바이스의 구성을 변경하면 해당 변경 사항이 활성 변경 로그 항목에 기록됩니다. 디바이스에서 CDO로 구성을 읽고, CDO에서 디바이스로 변경 사항을 배포하거나, CDO에서 디바이스를 삭제하거나, 실행 중인 구성 파일을 업데이트하는 CLI 명령을 실행하면 활성 변경 로그가 완성되고 향후 변경을 위해 새 로그가 생성됩니다.

다음 이미지는 ASA의 활성 변경 로그 항목입니다. 왼쪽의 타임스탬프 옆에 있는 열린 원을 확인합니다.

변경 로그에서 항목 찾기

변경 로그 이벤트는 검색 및 필터링이 가능합니다. 검색 창을 사용하여 키워드와 일치하는 이벤트를 찾습니다. 필터 를 사용하여 지정한 모든 기준을 충족하는 항목을 찾습니다. 변경 로그를 필터링하고 검색 필드에 키워드를 추가하여 필터링된 결과 내에서 항목을 찾는 방식으로 작업을 결합할 수도 있습니다.

# ASA 변경 로그 세부 사항

ASA 변경 로그 항목에 대한 설명은 다음 문서를 참조하십시오.

- ASA에 구축한 후 로그 항목 변경, on page 371
- ASA에서 변경 사항을 읽은 후 로그 항목 변경, on page 372
- 변경 로그 차이 보기, on page 373

# ASA에 구축한 후 로그 항목 변경

다음은 변경 로그 항목에 대한 설명입니다. 항목의 왼쪽 상단에 확인 표시가 있는 녹색 원은 변경 로그가 완료되었음을 나타냅니다. 변경 로그는 항목을 최신 항목에서 가장 오래된 항목 순으로 표시하고 변경 사항을 최신 항목순으로 정렬합니다.

변경 로그 항목 행에서 파란색 변경 로그 차이 보기 링크를 클릭하면 실행 중인 구성 파일의 컨텍스트에서 변경 사항을 나란히 비교하여 표시합니다.

아래의 여러 변경 사항에 대한 설명을 참조하십시오.

| 그림의 번호 | 설명 |
|---|---|
| 1 | 다음은 2018년 9월 11일 오전 10:03:59에 admin@example.com이 변경한 내용입니다.<br>**1.** "HR_network" 개체가 추가되었습니다.<br>**2.** 초기 네트워크 주소(10.10.11.0) 및 서브넷 마스크(255.255.255.0)가 HR_network 개체에 추<br>니다.<br>**3.** "engineering" 네트워크의 주소가 "HR_network"에 도달하는 것을 거부하는 "engineering_acc<br>워크 정책에 규칙이 추가되었습니다. |
| 2 | 실행 중인 구성 파일의 체크섬이 ASA에 의해 재계산되고 변경되었습니다. 이전 값이 제거되고<br>추가되었습니다. |
| 3 | ASA는 개체를 Defense Orchestrator에서 배치한 위치와 실행 중인 구성 파일의 다른 위치로 이<br>**Note** 이런 종류의 항목이 항상 표시되는 것은 아닙니다. |
| 4 | 실행 중인 구성 파일이 마지막으로 업데이트된 시간의 레코드입니다. 이전 타임스탬프가 제거<br>타임스탬프가 추가됩니다. 이 변경 사항은 ASA에 의해 수행되었습니다. |
| 5 | 이는 구성을 변경하기 위해 Defense Orchestrator에서 ASA로 전송하는 명령입니다. |

# ASA에서 변경 사항을 읽은 후 로그 항목 변경

CDO(Cisco Defense Orchestrator)는 관리하는 ASA에서 변경 사항을 감지하면 변경 로그 항목을 열고 구성 충돌이 감지된 시간을 기록합니다. 이것은 CDO가 충돌을 감지했을 때 볼 수 있는 변경 로그 항목의 종류입니다.


변경 사항을 수락하거나 변경 사항을 검토하고 수락하면 해당 변경 사항이 변경 로그 항목에 추가되고 항목이 완료됩니다.

이 항목은 엔지니어링 네트워크의 주소가 HR_network에 도달하지 못하도록 하는 충돌 감지 변경 및 규칙 삭제를 보여줍니다. 변경 로그 항목에는 "대역 외 변경 사항을 성공적으로 가져왔습니다."라는 메시지와 함께 변경 사항도 표시됩니다. 관리자가 대역 외 변경을 거부하도록 선택한 경우 변경 로그에는 거부된 내용과 함께 "디바이스에서 대역 외 변경을 성공적으로 거부했습니다."라는 메시지가 표시되었을 것입니다. 대역 외 변경은 CDO를 사용하지 않고 ASA 디바이스에 직접 적용되는 변경을 의미합니다.

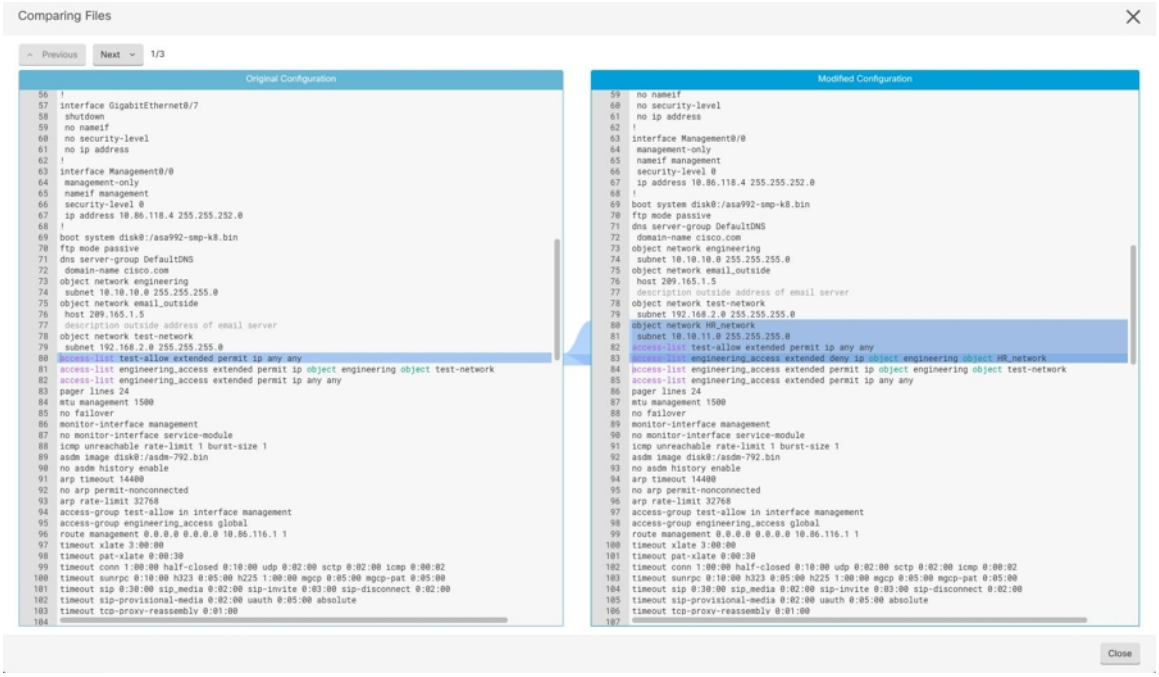
관련 주제

- 변경 로그, on page 369
- ASA에 구축한 후 로그 항목 변경, on page 371
- 변경 로그 차이 보기, on page 373
- 변경 사항 읽기, 삭제, 확인 및 구축

# 변경 로그 차이 보기

변경 로그에서 파란색 "Diff" 링크를 클릭하면 디바이스의 실행 중인 구성 파일에서 변경 사항을 나란히 비교할 수 있습니다. 두 버전의 차이점을 확인할 수 있습니다.

아래 그림에서 "Original Configuration(원본 구성)"은 변경 사항이 ASA에 기록되기 전에 실행 중인 구성 파일이며, "Modified Configuration(수정된 구성)" 열은 변경 사항이 기록된 후 실행 중인 구성 파일을 보여줍니다. 이 경우 Original Configuration(원본 구성) 열은 실행 중인 구성 파일에서 실제로 변경되지 않은 행을 강조 표시하지만 Modified Configuration(수정된 구성) 열에서 참조 지점을 제공합니다. 왼쪽에서 오른쪽 열로 이어지는 선을 따라가면 "engineering" 네트워크의 주소가 "HR_network" 네트워크의 주소에 도달하지 못하도록 하는 HR_network 개체 및 액세스 규칙이 추가된 것을 확인할 수 있습니다. **Previous(**이전**)** 및 **Next(**다음**)** 버튼을 사용하여 파일의 변경 사항을 클릭합니다.




관련 주제

- 변경 로그, on page 369

# 변경 로그를 CSV 파일로 내보내기

CDO 변경 로그 전체 또는 하위 집합을 쉼표로 구분된 값(.csv) 파일로 내보내 원하는 대로 정보를 필터링하고 정렬할 수 있습니다.

변경 로그를 .csv 파일로 내보내려면 다음 절차를 수행합니다.

단계 **1** 탐색창에서 **Change Log(**변경 로그**)**를 클릭합니다.

단계 **2** 다음 작업 중 하나를 수행하여 내보낼 변경 사항을 찾습니다.

- 필터 필드 및 검색 필드를 사용하여 내보낼 항목을 정확하게 찾습니다. 예를 들어 디바이스를 기준으로 필터링하면 선택한 디바이스에 대한 변경 사항만 표시됩니다.
- 변경 로그에서 모든 필터 및 검색 기준을 지웁니다. 이렇게 하면 전체 변경 로그를 내보낼 수 있습니다.

**Note** CDO는 1년간의 변경 로그 데이터를 저장합니다. 최대 1년의 변경 로그 기록을 다운로드하는 것보다 변경 로그 내용을 필터링하고 .csv 파일로 결과를 다운로드하는 것이 더 나을 수 있습니다.

단계 **3** 변경 로그 의 오른쪽 상단에 있는 파란색 내보내기 버튼을 클릭합니다.

단계 **4** .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다.

## CDO의 변경 로그 용량과 내보낸 변경 로그 크기의 차이

CDO의 변경 로그 페이지에서 내보내는 정보는 CDO가 데이터베이스에 저장하는 변경 로그 정보와 다릅니다.

모든 변경 로그에 대해 CDO는 디바이스 구성의 두 사본을 저장합니다. 하나는 "시작" 구성이고, 다른 하나는 닫힌 변경 로그의 경우 "종료" 구성 또는 열린 변경 로그의 경우 "현재" 구성입니다. 이를 통해 CDO는 구성 차이를 나란히 표시할 수 있습니다. 또한 CDO는 변경한 사용자 이름, 변경한 시간 및 기타 세부 정보와 함께 모든 단계 "변경 이벤트"를 추적하고 저장합니다.

그러나 변경 로그를 내보낼 때 구성의 전체 사본 2개가 내보내기에 포함되지 않습니다. 여기에는 내보내기 파일이 변경 로그 CDO가 저장하는 것보다 훨씬 작은 "변경 이벤트"만 포함됩니다.

CDO는 최대 1년의 변경 로그 정보를 저장하며 여기에는 두 개의 구성 사본이 포함됩니다.

# 변경 요청 관리

변경 요청 관리를 사용하면 서드파티 티켓팅 시스템에서 연 변경 요청 및 해당 비즈니스 근거를 변경 로그의 이벤트와 연결할 수 있습니다. CDO에서 변경 요청을 생성하고, 이를 고유한 이름으로 식별하고, 변경에 대한 설명을 입력하고, 변경 요청을 변경 로그 이벤트와 연결하려면 변경 요청 관리를 사용합니다. 나중에 변경 로그에서 변경 요청 이름을 검색할 수 있습니다.

**Note** CDO에서 변경 요청 추적에 대한 참조를 확인할 수도 있습니다. 변경 요청 추적 및 변경 요청 관리는 동일한 기능을 나타냅니다.

## 변화 요청 관리 활성화

변경 요청 추적을 활성화하면 테넌트의 모든 사용자에게 영향을 미칩니다. 변경 요청 추적을 활성화하려면 다음 절차를 따르십시오.

단계 **1** 사용자 메뉴에서 Settings(설정)를 선택합니다.

단계 **2** 사용자 메뉴에서 **General Settings(**일반 설정**)**를 클릭합니다.

단계 **3** "변경 요청 추적" 아래의 슬라이더를 클릭합니다.

확인되면 Defense Orchestrator 인터페이스의 왼쪽 하단 모서리에 변경 요청 도구 모음이 나타나고 변경 로그의 변경 요청 드롭다운 메뉴가 나타납니다.

# 변경 요청 생성

단계 **1** CDO 페이지에서 페이지 왼쪽 하단 모서리에 있는 변경 요청 도구 모음의 파란색 **+** 버튼을 클릭합니다.

단계 **2** 변경 요청에 이름과 설명을 지정합니다. 조직에서 구현하려는 변경 요청 식별자를 변경 요청 이름에 반영하십시오. 설명 필드를 사용하여 변경 목적을 설명하십시오.

**Note** 변경 요청을 생성한 후에는 변경 요청의 이름을 변경할 수 없습니다.

단계 **3** 변경 요청을 저장합니다.

**Note** CDO는 변경 요청을 비활성화하거나 변경 요청 도구 모음에서 변경 요청 정보를 지울 때까지 모든 새 변경을 해당 변경 요청 이름과 연결하여 변경 요청을 저장합니다.

# 변경 요청을 변경 로그 이벤트와 연결

단계 **1** 탐색 창에서 **Change Log(**로그 변경**)**를 클릭합니다.

단계 **2** 변경 로그를 확장하여 변경 요청과 연결하려는 이벤트를 표시합니다.

단계 **3** 변경 요청 열에서 이벤트의 드롭다운 메뉴를 클릭합니다. 최신 변경 요청이 변경 요청 목록의 맨 위에 나열됩니다.

단계 **4** 변경 요청의 이름을 클릭하고 **Select(**선택**)**를 클릭합니다.

# 변경 요청으로 변경 로그 이벤트 검색

단계 **1** 탐색 창에서 **Change Log(**로그 변경**)**를 클릭합니다.

단계 **2** 해당 변경 요청과 연관된 변경 로그 이벤트를 찾기 위해 변경 로그 검색 필드에 변경 요청의 정확한 이름을 입력합니다. CDO는 정확히 일치하는 변경 로그 이벤트를 강조 표시합니다.

# 변경 요청 검색

단계 **1** 변경 요청 도구 모음에서 변경 요청 메뉴를 클릭합니다.

단계 **2** 변경 요청 이름 또는 검색 중인 키워드 입력을 시작합니다. 변경 요청 목록의 이름 필드와 설명 필드 모두에서 부분 일치에 대한 결과가 표시되기 시작합니다.

# 변경 요청 필터링

필터 트레이에는 로그 변경 이벤트를 찾는 데 사용할 수 있는 변경 요청 필터가 있습니다.

단계 **1** **Change Log(**로그 변경**)** 페이지 왼쪽의 필터 트레이에서 변경 요청 영역을 찾습니다.

단계 **2** 필터를 확장하고 검색 필드에 변경 요청 이름을 입력하기 시작합니다. 부분 일치 항목이 검색 필드 아래에 나타나기 시작합니다.

단계 **3** 변경 요청 이름을 선택하고 해당 확인란을 선택하면 변경 로그 테이블에 일치 항목이 나타납니다. CDO는 정확히 일치하는 변경 로그 이벤트를 강조 표시합니다.

# 변경 요청 툴바 지우기

변경 요청 도구 모음을 지우면 변경 로그 이벤트가 기존 변경 요청과 자동으로 연결되지 않습니다.

단계 **1** 변경 요청 도구 모음에서 변경 요청 메뉴를 선택합니다.

단계 **2** **Clear(**지우기**)**를 클릭합니다. 변경 요청 메뉴가 **None(**없음**)**으로 변경됩니다.

# 변경 로그 이벤트와 관련된 변경 요청 지우기

단계 **1** 탐색창에서 **Change Log(**변경 로그**)**를 클릭합니다.

단계 **2** 변경 로그를 확장하여 변경 요청에서 연결 해제하려는 이벤트를 표시합니다.

단계 **3** 변경 요청 열에서 이벤트의 드롭다운 메뉴를 클릭합니다.

단계 **4** **Clear(**지우기**)**를 클릭합니다.

# 변경 요청 삭제

변경 요청을 삭제하면 변경 로그가 아닌 변경 요청 목록에서 삭제됩니다.

단계 **1** 변경 요청 도구 모음에서 변경 요청 메뉴를 클릭합니다.

단계 **2** 변경 요청 이름을 클릭합니다.

단계 **3** 해당 행에서 삭제 아이콘을 클릭합니다.

단계 **4** 녹색 확인 표시를 클릭하여 변경 요청 삭제를 확인합니다.

# 변화 요청 관리 비활성화

변경 요청 관리를 비활성화하면 계정의 모든 사용자에게 영향을 미칩니다. 변경 요청 관리를 비활성화하려면 다음 절차를 따르십시오.

단계 **1** 사용자이름 메뉴에서 **Settings(**설정**)**를 선택합니다.

단계 **2** 변경 요청 추적 아래의 버튼을 밀어 회색 X를 표시합니다.

# 활용 사례

이러한 사용 사례는 이전에 위의 지침에 따라 변경 요청 관리를 활성화했다고 가정합니다.

외부 시스템에서 유지 관리되는 티켓을 해결하기 위해 수행된 방화벽 변경 사항 추적

이 사용 사례에서 사용자는 외부 시스템에서 유지 관리되는 티켓을 해결하기 위해 방화벽을 변경하고 있습니다. 사용자는 이러한 방화벽 변경으로 인한 변경 로그 이벤트를 변경 요청과 연결하려고 합니다. 이 절차에 따라 변경 요청을 생성하고 변경 로그 이벤트를 연결합니다.

1. 변경 요청 생성, on page 376. 외부 시스템의 티켓 이름 또는 번호를 변경 요청 이름으로 사용합니다. 설명 필드를 사용하여 변경 또는 기타 관련 정보에 대한 근거를 추가합니다.
2. 변경 요청 도구 모음에 새 변경 요청이 표시되는지 확인합니다.
3. 방화벽을 변경하십시오.
4. 탐색 창에서 변경 로그를 클릭하고 새 변경 요청과 연결된 변경 로그 이벤트를 찾습니다.
5. 완료되면 변경 요청 툴바 지우기, on page 377.

방화벽을 변경한 후 개별 변경 로그 이벤트를 수동으로 업데이트합니다.

이 사용 사례에서 사용자는 외부 시스템에 유지 관리되는 티켓을 해결하기 위해 방화벽을 변경했지만 변경 요청 관리 기능을 사용하여 변경 요청을 변경 로그 이벤트와 연결하는 것을 잊었습니다. 사용자는 티켓 번호로 변경 로그 이벤트를 업데이트하기 위해 변경 로그로 돌아가려고 합니다. 변경 요청을 변경 로그 이벤트와 연결하려면 이 절차를 따르십시오.

1. 변경 요청 생성, on page 376. 외부 시스템의 티켓 이름 또는 번호를 변경 요청 이름으로 사용합니다. 설명 필드를 사용하여 변경 또는 기타 관련 정보에 대한 근거를 추가합니다.
2. 탐색 창에서 **Change Log(**로그 변경**)**를 클릭하고 방화벽 변경 사항과 관련된 변경 로그 이벤트를 검색합니다.
3. 변경 요청을 변경 로그 이벤트와 연결, on page 376.
4. 완료되면 변경 요청 도구 모음을 지웁니다.

변경 요청과 관련된 변경 로그 이벤트 검색

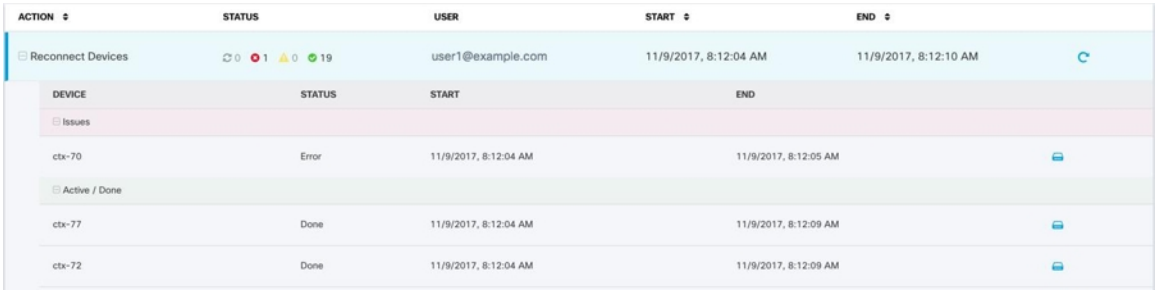
이 사용 사례에서 사용자는 외부 시스템에서 유지 관리되는 티켓을 해결하기 위해 수행한 작업의 결과로 변경 로그에 기록된 변경 로그 이벤트를 확인하려고 합니다. 변경 요청과 관련된 변경 로그 이벤트를 검색하려면 다음 절차를 따르십시오.

1. 탐색 창에서 **Change Log(**로그 변경**)**를 클릭합니다**.**
2. 다음 방법 중 하나를 사용하여 변경 요청과 관련된 변경 로그 이벤트를 검색합니다.
   - 해당 변경 요청과 연관된 변경 로그 이벤트를 찾기 위해 변경 로그 검색 필드에 변경 요청의 정확한 이름을 입력합니다. CDO는 정확히 일치하는 변경 로그 이벤트를 강조 표시합니다.
   - 변경 로그 이벤트를 찾기 위한 변경 요청 필터링, on page 377
3. 관련된 변경 요청을 보여주는 강조 표시된 변경 로그 이벤트를 찾으려면 각 변경 로그를 봅니다.

# 작업 페이지

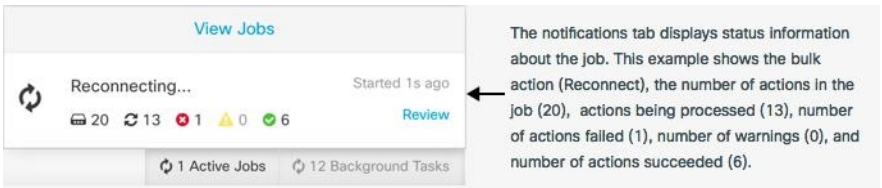
Jobs(작업) 페이지에는 벌크 작업의 상태에 대한 정보가 표시됩니다. 대량 작업은 여러 디바이스를 다시 연결하거나, 여러 디바이스에서 구성을 읽거나, 여러 디바이스를 동시에 업그레이드하는 것일 수 있습니다. 작업 테이블에서 색상으로 구분된 행은 성공하거나 실패한 개별 작업을 나타냅니다.

테이블의 한 행은 단일 대량 작업을 나타냅니다. 예를 들어 1개의 대량 작업이 20개의 디바이스를 다시 연결하려는 시도일 수 있습니다. Jobs(작업) 페이지에서 행을 확장하면 대량 작업의 영향을 받는 각 디바이스에 대한 결과가 표시됩니다.




Jobs(작업) 페이지는 다음과 같은 세 가지 방법으로 액세스할 수 있습니다.

- 알림 탭에서 알림 행의 **Review(**검토**)** 링크를 클릭합니다. Jobs(작업) 페이지로 리디렉션되고 해당 알림이 나타내는 특정 작업이 표시됩니다.



- Notifications(알림) 탭 상단에서 "Viewjobs(작업 보기)" 링크를 클릭하면 Jobs(작업) 페이지로 이동합니다.
- CDO의 메뉴에서 **Monitoring(**모니터링**)** > **Jobs(**작업**)**를 선택합니다. 이 표에는 CDO에서 수행되는 대량 작업의 전체 목록이 나와 있습니다.

필터링 및 검색

Jobs(작업) 페이지에서 작업 유형, 해당 작업을 수행한 사용자 및 작업 상태별로 필터링하고 검색할 수 있습니다.

# 작업이 실패한 대량 작업 다시 시작

작업 페이지를 검토할 때 대량 작업에서 하나 이상의 작업이 실패한 경우 필요한 편집을 수행한 후 대량 작업을 다시 실행할 수 있습니다. CDO는 실패한 작업에 대해서만 작업을 다시 실행합니다. 대량 작업을 다시 실행하려면 다음을 실행합니다.

단계 **1** 작업 페이지에서 실패한 작업을 나타내는 행을 선택합니다.

단계 **2** 다시 시작 아이콘을 클릭합니다.

# 대량 작업 취소

이제 여러 디바이스에서 수행한 활성 대량 작업을 취소할 수 있습니다. 예를 들어 4개의 관리 디바이스를 다시 연결하려고 시도했는데 그 중 3개의 디바이스가 성공적으로 다시 연결되었지만 네 번째 디바이스는 다시 연결에 성공하거나 실패하지 않았습니다.

대량 작업을 취소하려면 다음을 수행합니다.

단계 **1** CDO 탐색 메뉴에서 **Jobs(**작업**)**를 클릭합니다.

단계 **2** 아직 실행 중인 대량 작업을 찾아 작업 행 오른쪽에 있는 **Cancel(**취소**)** 링크를 클릭합니다.

대량 작업의 일부가 성공한 경우 해당 작업은 취소되지 않습니다. 아직 실행 중이던 모든 작업이 취소됩니다.

# 워크플로우 페이지

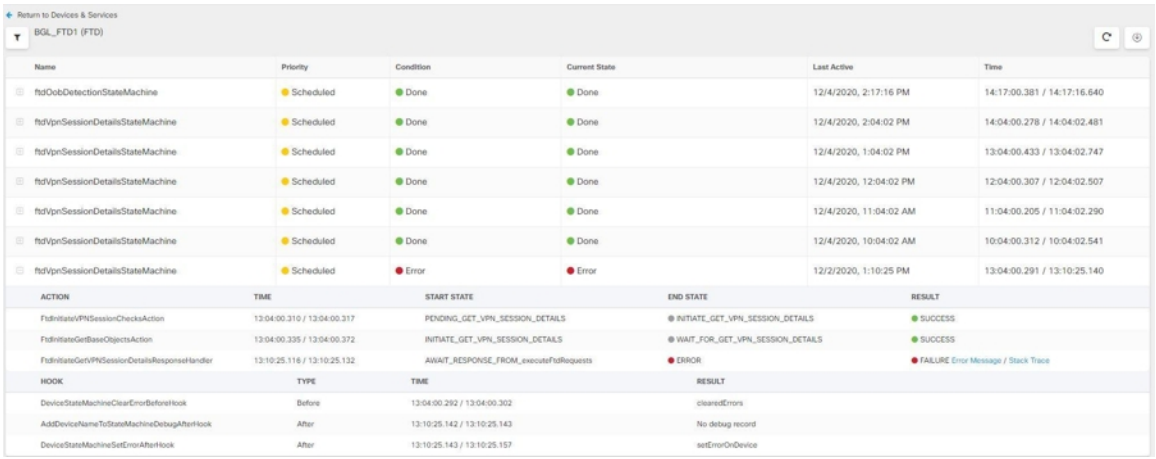
워크플로우 페이지에서는 디바이스, SDC(보안 디바이스 커넥터) 또는 SEC(보안 이벤트 커넥터)와 통신할 때와 디바이스에 규칙 세트 변경 사항을 적용할 때 CDO가 실행하는 모든 프로세스를 모니터링할 수 있습니다. CDO는 모든 단계에 대해 워크플로우 테이블에 항목을 만들고 이 페이지에 그 결

과를 표시합니다. 이 항목에는 상호 작용하는 디바이스가 아니라 CDO가 수행하는 작업에만 관련된 정보가 포함되어 있습니다.

CDO는 디바이스에서 작업을 수행하지 못할 때 오류를 보고하며 자세한 내용은 오류가 발생한 단계를 보기 위해 워크플로우 페이지로 이동할 수 있습니다.

이 페이지를 방문하여 오류를 확인 및 해결하거나 TAC가 요구할 때 정보를 공유할 수 있습니다.

워크플로우 페이지로 이동하려면 **Inventory(**인벤토리**)** 페이지에서 디바이스 탭을 클릭합니다. 적절한 디바이스 유형 탭을 클릭하여 디바이스를 찾고 원하는 디바이스를 선택합니다. 오른쪽 창의 장치 및 작업에서 워크플로를 클릭합니다. 다음 그림은 워크플로우 테이블의 항목이 있는 워크플로우 페이지를 보여줍니다.

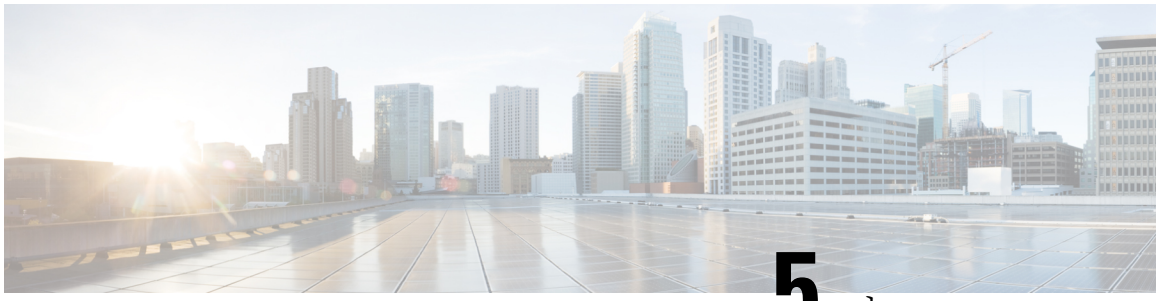



### 워크플로우 정보 다운로드

전체 워크플로우 정보를 JSON 파일로 다운로드하고 TAC 팀에서 추가 분석을 요청할 때 제공할 수 있습니다. 이 정보를 다운로드하려면 디바이스를 선택하고 해당 워크플로우 페이지로 이동한 다음 오른쪽 상단 모서리에 나타나는 내보내기 버튼 를 클릭합니다.

### 스택 추적 생성

해결할 수 없는 오류가 있는 경우 TAC에서 스택 추적 사본을 요청할 수 있습니다. 오류에 대한 스택 추적을 수집하려면 **Stack Trace(**스택 추적**)** 링크를 클릭하고 **Copy Stacktrace(**스택 추적 복사**)**를 클릭하여 화면에 나타나는 스택을 클립보드로 복사합니다.



5 장

# Cisco Security Analytics and Logging

# Security Analytics and Logging(SaaS) 정보

Cisco SAL(Security Analytics and Logging)을 사용하면 모든 FDM 관리 디바이스에서 연결, 침입, 파일, 맬웨어 및 보안 인텔리전스 이벤트와 ASA에서 모든 syslog 이벤트 및 NSEL(Netflow Secure Event Logging) 이벤트를 캡처하고 CDO(Cisco Defense Orchestrator)의 한 곳에서 볼 수 있습니다. 이벤트는 Cisco 클라우드에 저장되며 CDO의 Event Logging(이벤트 로깅) 페이지에서 볼 수 있습니다. 이 페이지에서 이벤트를 필터링하고 검토하여 네트워크에서 트리거되는 보안 규칙을 명확하게 파악할 수 있습니다.

추가 라이선싱을 사용하면 이러한 이벤트를 캡처한 후 CDO에서 프로비저닝된 Secure Cloud Analytics 포털로 교차 실행할 수 있습니다. Secure Cloud Analytics는 이벤트 및 네트워크 플로우 데이터에 대한 행동 분석을 수행하여 네트워크의 상태를 추적하는 SaaS(Software as a Service) 솔루션입니다. 방화벽 이벤트 및 네트워크 플로우 데이터를 비롯한 소스에서 네트워크 트래픽에 대한 정보를 수집하여 트래픽에 대한 관찰을 생성하고 트래픽 패턴을 기반으로 네트워크 엔티티의 역할을 자동으로 식별합니다. Secure Cloud Analytics는 Talos와 같은 위협 인텔리전스의 다른 소스와 결합된 이 정보를 사용하여 본질적으로 악의적인 행동이 있음을 나타내는 경고를 생성합니다. 알림과 함께 Secure Cloud Analytics는 알림을 조사하고 악의적인 동작의 소스를 찾기 위한 더 나은 기반을 제공하기 위해 수집한 네트워크 및 호스트 가시성 및 상황 정보를 제공합니다.

용어 참고: 이 설명서에서는 Cisco Security Analytics and Logging을 Secure Cloud Analytics 포털(Software as a Service 제품)과 함께 사용하는 경우 이러한 통합을 Cisco Security Analytics and Logging(SaaS) 또는 SAL(SaaS)이라고 합니다.

# ASA에 대한 SAL SaaS(Security Analytics and Logging) 정보

SaaS(Security Analytics and Logging)를 사용하면 ASA에서 모든 시스템 로그 이벤트 및 NSEL(Netflow Secure Event Logging)을 캡처하여 CDO(Cisco Defense Orchestrator)에서 한 곳에서 볼 수 있습니다.

이벤트는 Cisco 클라우드에 저장되며 CDO의 Event Logging(이벤트 로깅) 페이지에서 볼 수 있습니다. 이 페이지에서 이벤트를 필터링하고 검토하여 네트워크에서 트리거되는 보안 규칙을 명확하게 파악할 수 있습니다. **Logging and Troubleshooting(**기록 및 문제 해결**)** 패키지는 이러한 기능을 제공합니다.

시스템은 로깅 분석 및 탐지 패키지(이전 방화벽 분석 및 로깅 패키지)를 사용하여 FTD 이벤트에 Secure Cloud Analytics 동적 엔티티 모델링을 적용하고 행동 모델링 분석을 사용하여 Secure Cloud Analytics 관찰 및 알림을 생성할 수 있습니다. 전체 네트워크 분석 및 모니터링 패키지를 구입하는 경우 시스템은 FTD 이벤트와 네트워크 트래픽 모두에 동적 엔터티 모델링을 적용하고 관찰 및 알림을 생성합니다. Cisco SSO(Single Sign-On, 단일 인증)를 사용하여 CDO에서 사용자에게 프로비저닝된 Secure Cloud Analytics 포털로 교차 실행할 수 있습니다.

### CDO 이벤트 뷰어에 ASA 이벤트가 표시되는 방법

ASA에서 로깅이 활성화되고 네트워크 트래픽이 액세스 제어 규칙 기준과 일치하면 시스템 로그 이벤트 및 NSEL 이벤트가 생성됩니다. 이벤트가 Cisco Cloud에 저장되면 CDO에서 볼 수 있습니다.

모든 디바이스에서 여러 SEC(Secure Event Connector)를 설치하고 규칙에 의해 생성된 이벤트를 마치 시스템 로그 서버인 것처럼 SEC로 전송할 수 있습니다. 그런 다음 SEC는 Cisco Cloud에 이벤트를 전달합니다. 모든 SEC에 동일한 이벤트를 전달하지 마십시오. Cisco Cloud로 전송되는 이벤트를 복제하고 일일 수집 속도를 불필요하게 부풀릴 수 있습니다.

보안 이벤트 커넥터를 통해 **ASA**에서 **Cisco Cloud**로 시스템 로그 및 **NSEL** 이벤트를 전송하는 방법

기본 로깅 및 문제 해결 라이선스를 사용하는 경우 ASA 이벤트가 Cisco Cloud에 도달하는 방법은 다음과 같습니다.

1. 사용자 이름 및 비밀번호를 사용하여 CDO에 ASA를 온보딩합니다.
2. 시스템 로그 및 NSEL 이벤트를 시스템 로그 서버인 것처럼 SEC 중 하나에 전달하고 디바이스에서 로깅을 활성화하도록 ASA를 구성합니다.
3. SEC는 이벤트가 저장된 Cisco Cloud로 이벤트를 전달합니다.
4. CDO는 설정한 필터에 따라 Cisco Cloud의 이벤트를 이벤트 뷰어에 표시합니다.

**Logging Analytics and Detection(**로깅 분석 및 탐지**)** 또는 **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스를 사용하면 다음 작업도 수행됩니다.

1. Cisco Secure Cloud Analytics는 Cisco 클라우드에 저장된 ASA 시스템 로그 이벤트에 분석을 적용합니다.
2. 생성된 관찰 및 알림은 CDO 포털과 연결된 Secure Cloud Analytics 포털에서 액세스할 수 있습니다.
3. CDO 포털에서 Secure Cloud Analytics 포털을 교차 실행하여 이러한 관찰 및 알림을 검토할 수 있습니다.

솔루션에 사용된 구성 요소

**SDC(Secure Device Connector)** - SDC는 CDO를 ASA에 연결합니다. ASA에 대한 로그인 자격 증명은 SDC에 저장되지 않습니다. 자세한 내용은 SDC(Secure Device Connector), on page 5를 참조하십시오.

**SEC(Secure Event Connector)** - SEC는 ASA에서 이벤트를 수신하여 Cisco Cloud로 전달하는 애플리케이션입니다. Cisco Cloud에 있으면 CDO의 Event Logging(이벤트 로깅) 페이지에서 이벤트를 보거나 Secure Cloud Analytics를 사용하여 분석할 수 있습니다. 환경에 따라 SEC는 보안 디바이스 커넥터(있는 경우)에 설치됩니다. 또는 네트워크에서 유지 관리하는 자체 CDO 커넥터 가상 머신에서 수행할 수 있습니다. 자세한 내용은 보안 이벤트 커넥터, on page 437를 참조하십시오.

**Adaptive Security Appliance (ASA)**-ASA에서는 고급 스테이트풀 방화벽 및 VPN 집선 장치 기능을 제공하며 애드온 모듈과 통합된 서비스를 제공합니다. ASA에는 다중 보안 상황(가상 방화벽과 유사), 클러스터링(다중 방화벽을 단일 방화벽으로 통합), 투명(Layer 2) 방화벽 또는 라우팅(Layer 3) 방화벽 가동, 고급 검사 엔진, IPsec VPN, SSL VPN 및 클라이언트리스 SSL VPN 지원 등의 다양한 기능이 포함되어 있습니다.

**Secure Cloud Analytics**는 ASA 이벤트에 동적 엔티티 모델링을 적용하여 이 정보를 기반으로 탐지를 생성합니다. 이렇게 하면 네트워크에서 수집한 텔레메트리를 심층적으로 분석하여 추세를 식별하고

네트워크 트래픽의 이상 동작을 검사할 수 있습니다. **Logging Analytics and Detection(**로깅 분석 및 탐지**)** 또는 **Total Network Analytics and Monitoring(**총 네트워크 분석 및 모니터링**)** 라이선스가 있는 경우 이 서비스를 사용할 수 있습니다.

라이선싱

이 솔루션을 구성하려면 다음 계정 및 라이선스가 필요합니다.

- **Cisco Defense Orchestrator**. CDO 테넌트가 있어야 합니다.
- **Secure Device Connector**. 보안 디바이스 커넥터에 대한 별도의 라이선스는 없습니다.
- **Secure Event Connector**. 보안 이벤트 커넥터에 대한 별도의 라이선스는 없습니다.
- **Secure Logging Analytics(SaaS)**. Security Analytics and Logging 라이선스 테이블을 참조하십시오.
- **ASA(Adaptive Security Appliance)**. 기본 라이선스 이상

### **Security Analytics and Logging** 라이선싱

SaaS(Security Analytics and Logging)를 구현하려면 다음 라이선스 중 하나를 구매해야 합니다.

| 라이선스 이름 | 제공된 기능 | 사용가능한라이선스기간 | 기능 사전 요건 |
|---|---|---|---|
| 로깅 및 문제 해결 | • 라이브 피드 및 기록 보기로 CDO 내의 ASA 이벤트 및 이벤트 세부 정보 보기 | • 1년<br>• 3년<br>• 5년 | • CDO<br>• 소프트웨어 버전 9.6 이상을 실행하는 온프레미스 ASA 구축<br>• Cisco Cloud에 ASA 이벤트를 전달하기 위한 하나 이상의 SEC 구축 |

| 라이선스 이름 | 제공된 기능 | 사용 가능한 라이선스 기간 | 기능 사전 요건 |
|---|---|---|---|
| 로깅 분석 및 탐지(이전 이름 방화벽 분석 및 모니터링) | 로깅 및 문제 해결 기능 추가:<br>• 이벤트에 동적 엔터티 모델링 및 행동 분석을 적용합니다.<br>• 이벤트 데이터를 기반으로 Secure Cloud Analytics에서 알림 열기, CDO 이벤트 뷰어에서 교차 실행 | • 1년<br>• 3년<br>• 5년 | • CDO<br>• 소프트웨어 버전 9.6 이상을 실행하는 온프레미스 ASA 구축<br>• Cisco Cloud에 ASA 이벤트를 전달하기 위한 하나 이상의 SEC 구축<br>• 새로 프로비저닝된 또는 기존의 Cisco Secure Cloud Analytics 포털. |

| 라이선스 이름 | 제공된 기능 | 사용가능한라이선스기간 | 기능 사전 요건 |
|---|---|---|---|
| 총 네트워크 분석 및 모니터링 | 로깅 분석 및 탐지, 추가:<br>• ASA 이벤트, 온프레미스 네트워크 트래픽 및 클라우드 기반 네트워크 트래픽에 동적 엔티티 모델링 및 행동 분석을 적용합니다.<br>• ASA 이벤트 데이터, Cisco Secure Cloud Analytics 센서에서 수집한 온프레미스 네트워크 트래픽 플로우 데이터 및 CDO 이벤트 뷰어에서 교차 실행되는 Cisco Secure Cloud Analytics에 전달된 클라우드 기반 네트워크 트래픽의 조합을 기반으로 하는 Cisco Secure Cloud Analytics의 공개 알림 | • 1년<br>• 3년<br>• 5년 | • CDO<br>• 소프트웨어 버전 9.6 이상을 실행하는 온프레미스 ASA 구축<br>• Cisco Cloud에 이벤트를 전달하기 위한 하나 이상의 SEC 구축<br>• 네트워크 트래픽 플로우 데이터를 클라우드에 전달하기 위해 하나 이상의 Cisco Secure Cloud Analytics 센서 버전 4.1 이상을 구축하거나, 네트워크 트래픽 플로우 데이터를 Cisco Secure Cloud Analytics로 전달하기 위해 Cisco Secure Cloud Analytics를 클라우드 기반 구축과 통합합니다.<br>• 새로 프로비저닝된 또는 기존의 Cisco Secure Cloud Analytics 포털. |

데이터 요금제

Cisco Cloud가 온보딩된 ASA에서 매일 수신하는 이벤트 수를 반영하는 데이터 요금제를 구매해야 합니다. 이를 "일일 수집 속도"라고 합니다. Logging Volume Estimator 도구를 사용하여 일일 수집 속도를 예측할 수 있으며, 속도가 변경되면 데이터 요금제를 업데이트할 수 있습니다.

데이터 요금제는 일별 볼륨 1GB 단위로 제공되며 1년, 3년 또는 5년 단위로 제공됩니다. 데이터 요금제에 대한 자세한 내용은 Secure Logging Analytics(SaaS) 주문 가이드를 참조하십시오.

**Note** Security Analytics and Logging 라이선스 및 데이터 요금제를 보유하고 있는 경우 나중에 다른 라이선스를 취득할 수 있으며, 이것만 있으면 다른 데이터 요금제를 구매할 필요가 없습니다. 네트워크 트래픽 처리량이 변경되어 다른 데이터 플랜을 취득하는 경우에는 다른 Security Analytics and Logging 라이선스를 구입하지 않아도 됩니다.

**30**일 무료 평가판

CDO에 로그인하고 **Monitoring(**모니터링**)** > **Event Logging(**이벤트 로깅**)** 탭으로 이동하여 30일 무료 평가판을 요청할 수 있습니다. 30일 평가판이 끝나면 SaaS(Secure Logging Analytics) 주문 가이드의 지침에 따라 CCW(Cisco Commerce Workspace)에서 서비스를 계속하기 위해 원하는 이벤트 데이터 볼륨을 주문할 수 있습니다.

다음 단계

ASA 디바이스에 대한 SaaS(Secure Logging Analytics) 구현으로 이동

# ASA 디바이스에 대한 SaaS(Secure Logging Analytics) 구현

시작하기 전에

- ASA에 대한 SAL SaaS(Security Analytics and Logging) 정보를 검토하여 다음에 대해 알아보십시오.
  - Cisco Cloud로 이벤트를 전송하는 방법
  - 솔루션의 애플리케이션
  - 필요한 라이선스
  - 필요한 데이터 요금제
- CDO 테넌트를 생성하기 위해 매니지드 서비스 제공자 또는 CDO 영업 담당자에게 문의했습니다.
- SDC(Secure Device Connector), 5 페이지를 검토합니다. SDC를 사용하여 CDO를 ASA에 연결하는 것은 "모범 사례"로 간주되지만 필수 사항은 아닙니다.
- 네트워크에서 SDC를 구축하려는 경우 다음 방법 중 하나를 사용하여 설치할 수 있습니다.
  - CDO의 준비된 VM 이미지를 사용하여 SDC를 설치하려면 CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축를 사용합니다. 이는 SDC를 구축하는 가장 쉬운 방법입니다.
  - 자체 VM에 보안 디바이스 커넥터 구축을 사용합니다.
- 보안 이벤트 커넥터 설치했으며 모든 ASA에서 테넌트에 온보딩된 SEC로 이벤트를 전송할 수 있습니다.

- 어카운트 사용자에 대한 새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성했습니다.

**Cisco SaaS(Security Analytics and Logging)**를 구현하고 보안 이벤트 커넥터를 통해 **Cisco Cloud**로 이벤트를 전송하는 워크플로우

1. 위의 "시작하기 전에"를 검토하여 환경이 올바르게 구성되었는지 확인하십시오.
2. 사용자 이름 및 비밀번호를 사용하는 ASA 디바이스 온보딩, 149 페이지
3. 명령줄 인터페이스를 사용하여 ASA Syslog 이벤트를 Cisco Cloud로 전송.
4. CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성.
5. 이벤트가CDO에 표시되는지 확인합니다. 탐색 막대에서 **Monitoring(**모니터링**) > Event Logging(**이벤트 로깅**)**을 선택합니다. 라이브 이벤트를 보려면 Live(라이브) 탭을 클릭합니다.
6. **Firewall Analytics and Monitoring(**방화벽 분석 및 모니터링**)** 또는 **Total Network Analytics and Monitoring(**총 네트워크 분석 및 모니터링**)** 라이선스가 있는 경우 다음 섹션인 **Cisco Secure Cloud Analytics**를 사용하여 이벤트 분석을 계속 진행합니다.

### Cisco Secure Cloud Analytics를 사용하여 이벤트 분석

**Firewall Analytics and Monitoring(**방화벽 분석 및 모니터링**)** 또는 **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스가 있는 경우 이전 단계와 함께 다음을 수행합니다.

1. Cisco Secure Cloud Analytics 포털 프로비저닝, 458 페이지.
2. **Total Network Analytics and Monitoring** 라이선스를 구매한 경우 하나 이상의 Secure Cloud Analytics 센서를 내부 네트워크에 구축합니다. 전체 네트워크 분석 및 보고를 위한 Cisco Secure Cloud Analytics 센서 구축, 460 페이지의 내용을 참조하십시오.
3. Cisco SSO(Single Sign-On) 자격 증명에 연결된 Secure Cloud Analytics 사용자 어카운트를 생성하도록 사용자를 초대합니다. CDO에서 Cisco Secure Cloud Analytics 알림 보기, 461 페이지의 내용을 참조하십시오.
4. FTD 이벤트에서 생성된 Secure Cloud Analytics 알림을 모니터링하려면 CDO에서 Secure Cloud Analytics로 교차 실행합니다. CDO에서 Cisco Secure Cloud Analytics 알림 보기, 461 페이지의 내용을 참조하십시오.

### CDO에서 교차 실행하여 Cisco Secure Cloud Analytics 알림 검토

**Firewall Analytics and Monitoring(**방화벽 분석 및 모니터링**)** 또는 **Total Network Analytics and Monitoring(**총 네트워크 분석 및 모니터링**)** 라이선스를 사용하면 CDO에서 Secure Cloud Analytics로 교차 실행하여 FTD 이벤트에 의해 생성된 알림을 검토할 수 있습니다.

자세한 내용은 다음 문서를 참조하십시오.

- CDO에 로그인

- CDO에서 Cisco Secure Cloud Analytics 알림 보기, 461 페이지
- Cisco Secure Cloud Analytics 및 동적 엔티티 모델링
- 방화벽 이벤트 기반 알림 작업

보안 이벤트 커넥터 문제 트러블슈팅

다음 문제 해결 항목을 사용하여 다음에 대한 상태 및 로깅 정보를 수집합니다.

- SEC 온보딩 실패 문제 해결
- 문제 해결 로그 파일 이벤트 로깅
- 상태 확인을 사용하여 보안 이벤트 커넥터의 상태 학습

워크플로

보안 및 분석 로깅 이벤트를 사용하여 네트워크 문제 해결에서는 Cisco Security Analytics 및 로깅에서 생성된 이벤트를 사용하여 사용자가 네트워크 리소스에 액세스할 수 없는 이유를 확인하는 방법을 설명합니다.

방화벽 이벤트 기반 알림 작업도 참조하십시오.

# CDO 매크로를 사용하여 Cisco Cloud로 ASA 시스템 로그 이벤트 전송

명령줄 인터페이스를 사용하여 ASA Syslog 이벤트를 Cisco Cloud로 전송에 설명된 모든 명령을 사용하는 CDO 매크로를 생성하고 동일한 배치의 모든 ASA에서 해당 매크로를 실행하여 Cisco Cloud에 이벤트를 전송하도록 모든 ASA를 구성할 수 있습니다.

CDO의 매크로 툴을 사용하면 CLI 명령 목록을 어셈블하고, 명령 syntax(명령문)의 요소를 매개변수로 변환한 다음, 두 번 이상 사용 가능하게끔 명령 목록을 저장할 수 있습니다. 매크로는 한 번에 둘 이상의 디바이스에서 실행할 수도 있습니다.

검증된 매크로를 사용하면 디바이스 간의 컨피그레이션 일관성이 향상되고, 명령줄 인터페이스를 사용할 때 발생할 수 있는 syntax(명령문) 오류가 방지됩니다.

자세한 내용을 읽기 전에 이러한 항목을 검토하여 매크로 사용 메커니즘을 이해하십시오. 이 문서에서는 최종 매크로 어셈블에 대해서만 설명합니다.

- 디바이스 관리를 위한 CLI 매크로
- 새 명령에서 CLI 매크로 생성
- CLI 매크로 실행
- CLI 매크로 편집
- CLI 매크로 삭제

# ASA Security Analytics and Logging (SaaS) 매크로 생성

다음 절차에서 볼 수 있는 서식에는 ASA CLI 명령과 매크로 형식의 두 가지 유형이 있습니다. ASA CLI 명령은 ASA 구문 규칙을 따르도록 작성되었습니다. 매크로 규칙은 새 명령에서 CLI 매크로 생성에 설명되어 있습니다.

시작하기 전에 별도의 창에서 명령줄 인터페이스를 사용하여 ASA Syslog 이벤트를 Cisco Cloud로 전송를 열고 이 절차와 동시에 읽어보십시오. 그러면 매크로를 생성할 때 명령 설명을 읽을 수 있습니다.

**Note** 로깅 구성이 이미 ASA에 있는 경우 CDO에서 매크로를 실행해도 기존 로깅 구성이 모두 지워지지는 않습니다. 대신, CDO 매크로에 정의된 설정이 이미 있는 것과 병합됩니다.

단계 **1** 일반 텍스트 편집기를 열고 아래의 지침 및 옵션에 따라 매크로로 변환할 명령 목록을 생성합니다. CDO는 매크로에 기록된 순서대로 명령을 실행합니다. 일부 명령에는 매크로를 실행할 때 입력하는 {{parameters}} 값이 있습니다.

단계 **2** ASA가 syslog 서버인 것처럼 **SEC**에 메시지를 보내도록 구성합니다**.**

메시지를 전송할 syslog 서버로 SEC를 지정하려면 **logging host** 명령을 사용합니다. 테넌트에 온보딩한 SEC 중 하나에 이벤트를 보낼 수 있습니다.

**logging host** 명령은 이벤트를 보낼 TCP 또는 UDP 포트를 지정합니다. 어떤 포트를 사용해야 하는지 확인하려면 SaaS(Secure Logging Analytics)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기를 참조하십시오.

**logging host***interface_nameSEC_IP_address* { **tcp/port** | **udp/port** }

시스템 로그 이벤트를 SEC로 전송하는 데 사용하는 프로토콜에 따라 이 명령을 두 개의 서로 다른 매크로 중 하나로 설정합니다.

logging host {{interface_name}} {{SEC_ip_address}} tcp/{{port_number}}

logging host {{interface_name}} {{SEC_ip_address}} udp/{{port)_number}}

(선택 사항) TCP를 사용하는 경우 매크로의 명령 목록에 이 명령을 추가할 수 있습니다. 매개변수가 필요하지 않습니다.

**logging permit-hostdown**

단계 **3** 어떤 **syslog** 메시지를 **syslog** 서버에 전송할지 지정합니다**.**

**logging trap** 명령을 사용하여 syslog 서버로 보내야 하는 syslog 메시지를 지정합니다.

**logging trap** { *severity_level* | *message_list* }

심각도 수준별로 SEC로 전송되는 이벤트를 정의하려면 명령을 다음 매크로로 전환합니다.

logging trap {{severity_level}}

메시지 목록의 일부인 SEC에 이벤트만 보내려면 명령을 다음 매크로로 변환합니다.

logging trap {{message_list_name}}

이전 단계에서 **logging trap message_list** 명령을 선택한 경우 메시지 목록에서 syslog를 정의해야 합니다. 매크로를 생성할 때 명령 설명을 읽을 수 있도록 사용자 지정 이벤트 목록 생성를 엽니다. 다음 명령으로 시작합니다.

**logging list***name* { **level***level* [ **class***message_class* ] | **message***start_id* [ *-end_id* ] }

이를 다음과 같이 분류합니다.

logging list {{message_list_name}} level {{security_level}}

logging list {{message_list_name}} level {{security_level}} class {{message_class}}

logging list {{message_list_name}} message {{syslog_range_or_number}}

마지막 변형에서는 메시지 파라미터 {{syslog_range_or_number}}를 단일 syslog ID(106023) 또는 범위(302013-302018)로 입력할 수 있습니다. 메시지 목록을 만들려면 원하는 만큼의 줄에서 하나 이상의 명령 변형을 사용합니다. 단일 매크로에서 동일한 이름의 모든 매개변수는 사용자가 입력한 것과 동일한 값을 사용한다는 점에 유의하십시오. CDO는 매개변수가 비어 있는 매크로를 실행하지 않습니다.

**Important** **logging list** 명령은 매크로에서 **logging trap** 명령 앞에 와야 합니다. 먼저 목록을 정의하면 **logging trap** 명령에서 사용할 수 있습니다. 아래의 샘플 매크로를 참조하십시오.

단계 **4** (선택 사항) syslog 타임스탬프를 추가합니다**.** ASA에서 발생한 syslog 메시지에 날짜와 시간을 추가하려면 이 명령을 추가합니다. 타임스탬프 값은 **SyslogTimestamp** 필드에 표시됩니다. 이 명령을 명령 목록에 추가합니다. 매개변수는 필요하지 않습니다.

**logging timestamp**

**Note** 버전 9.10(1)부터 ASA는 이벤트 시스템 로그에서 RFC 5424에 따라 타임스탬프를 활성화하는 옵션을 제공합니다. 이 옵션을 활성화하면 syslog 메시지의 모든 타임스탬프가 RFC 5424 형식에 따라 시간을 표시합니다. 다음은 RFC 5424 형식의 샘플 출력입니다.

```
 <166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol from
src interface :src IP/src port to dest IP/dest port
```

.

단계 **5** (선택 사항) EMBLEM 형식이 아닌 syslog 메시지에 디바이스 **ID**를 포함합니다**.** 매크로를 생성할 때 명령 설명을 읽을 수 있도록 디바이스 ID를 EMBLEM 이외 형식 Syslog 메시지에 포함를 엽니다. 이는 매크로의 기반이 되는 CLI 명령입니다.

**logging device-id** { **cluster-id** | **context-name** | **hostname** | **ipaddress** *interface_name* [ **system** ] | **string***text* }

이를 다음과 같이 분류합니다.

**logging device-id cluster-id**

**logging device-id context-name**

**logging device-id hostname**

**logging device-id ipaddress** {{interface_name}} **system**

**logging device-id string** {{text_16_char_or_less}}

단계 **6** 로깅을 활성화합니다**.** 이 명령을 그대로 매크로에 추가합니다. 매개변수가 없습니다.

**logging enable**

단계 **7** 매크로의 마지막 줄에 쓰기 **write memory**를 추가하지 마십시오**.** 대신 **show running-config logging** 명령을 추가하여 ASA의 시작 구성에 커밋하기 전에 입력한 로깅 명령의 결과를 검토합니다.

**show running-config logging**

단계 **8** 구성이 변경되었다고 확신하는 경우 **write memory** 명령에 대한 별도의 매크로를 생성하거나 CDO의 대량 CLI 인터페이스 기능을 사용하여 매크로를 사용하여 구성한 모든 디바이스에 명령을 실행할 수 있습니다.

**write memory**

단계 **9** (선택 사항) 액세스 제어 규칙 "permit" 이벤트에 대한 로깅을 활성화합니다**.** 이 단계는 명령줄 인터페이스를 사용하여 ASA Syslog 이벤트를 Cisco Cloud로 전송 절차에 설명되어 있지만 이 매크로에는 포함되어 있지 않습니다. 대신 CDO GUI에서 수행됩니다.

단계 **10** 매크로를 저장합니다.

### Example

다음은 단일 매크로로 결합된 명령 목록의 샘플입니다.

```
logging host {{interface_name}} {{SEC_ip_address}} {{tcp_or_udp}}/{{port_number}}
logging permit-hostdown
logging list {{message_list_name}} level {{security_level}}
logging list {{message_list_name}} message {{syslog_range_or_number_1}}
logging list {{message_list_name}} message {{syslog_range_or_number_2}}
logging trap {{message_list_name}}
logging device-id cluster-id
logging enable
show running-config logging
```

**Note** 서로 다른 특정 syslog ID 또는 범위를 추가하는 몇 가지 logging list 명령이 있습니다. {{syslog_range_or_number_X}} 매개변수에는 숫자 또는 기타 구분자가 필요합니다. 그렇지 않으면 매크로가 채워질 때 값이 모두 동일하게 됩니다. 또한 모든 매개변수에 값이 지정되지 않은 경우 CDO는 매크로를 실행하지 않으므로 실행하려는 명령만 매크로에 포함해야 한다는 점에 유의하십시오. 모든 syslog ID가 동일한 목록에 포함되므로 event_list_name이 각 줄에서 동일하게 유지됩니다.

### What to do next

매크로 실행

ASA Security Analytics and Logging Macro(보안 분석 및 로깅 매크로)를 생성하고 저장한 후 매크로를 실행하여 ASA syslog 이벤트를 Cisco Cloud로 전송합니다.

# 명령줄 인터페이스를 사용하여 ASA Syslog 이벤트를 Cisco Cloud로 전송

이 절차에서는 ASA Syslog 이벤트를 SEC(보안 이벤트 커넥터)에 전달한 다음 로깅을 활성화하는 방법을 설명합니다. 이러한 절차에서는 해당 워크플로우를 완료하는 데 필요한 사항만 설명합니다. ASA에서 로깅을 구성할 수 있는 모든 방법에 대한 자세한 내용은 ASDM1: Cisco ASA 시리즈 일반 운영 ASDM 구성 가이드 또는 CLI 1권: Cisco ASA 시리즈 일반 운영 CLI 구성 가이드의 모니터링 장을 참조하십시오.

지원되는 **ASA** 명령에 대한 제한 사항

CDO는 아직 다음 Syslog 명령 또는 메시지 형식을 지원하지 않습니다.

- Syslog의 EMBLEM 형식
- 보안 Syslog

## ASA용 CDO 명령줄 인터페이스

이 절차의 모든 작업은 ASA용 CDO의 명령줄 인터페이스에서 진행하게 됩니다. 명령줄 인터페이스 페이지를 열려면 다음을 수행합니다.

---

단계 **1** 탐색 모음에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 적절한 디바이스 유형 탭을 클릭하고 로깅을 활성화할 ASA를 선택합니다.

단계 **4** 오른쪽의 Device Actions(디바이스 작업) 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **5** **Command Line Interface(**명령줄 인터페이스**)** 탭을 클릭합니다. 이제 프롬프트에서 아래에 설명된 명령을 입력할 준비가 되었습니다.

모든 명령을 입력한 후 **Send(**전송**)**를 클릭합니다. CDO의 CLI 인터페이스는 ASA에 직접 연결되므로 명령은 디바이스의 실행 중인 구성에 즉시 기록됩니다. ASA의 시작 구성에 변경 사항을 기록하려면 `write memory` 명령을 추가로 실행해야 합니다.

---

## 보안 이벤트 커넥터에 ASA 시스템 로그 이벤트 전달

ASA 시스템 로그 이벤트를 온보딩한 SEC(Secure Event Connector) 중 하나로 전달한 다음 로깅을 활성화하려면 다음 절차에서 작업을 완료해야 합니다.

---

단계 **1** ASA이 시스템 로그 서버인 것처럼 SEC에 메시지를 보내도록 구성합니다.

단계 **2** SEC에 전송할 모든 로그의 심각도 레벨 또는 시스템 로그 이벤트 목록을 결정합니다.

단계 **3** 로깅을 활성화합니다.

단계 **4** 변경 사항을 ASA의 시작 구성에 저장합니다.

# CLI를 사용하여 ASA Syslog 이벤트를 Cisco 클라우드로 전송

단계 **1** ASA이 **syslog** 서버인 것처럼 **SEC**에 메시지를 보내도록 구성합니다**.**

ASA에서 Cisco cloud로 시스템 로그 이벤트를 전송할 때 외부 시스템 로그 서버인 것처럼 SEC로 전달하면 SEC에서 Cisco cloud로 메시지를 전달합니다.

syslog 메시지를 SEC에 보내려면 다음 단계를 수행합니다.

**a.** TCP 또는 UDP를 사용하여 ASA이 syslog 서버인 것처럼 SEC에 메시지를 전송하도록 를 구성합니다. SEC는 IPv4 또는 IPv6 주소를 사용할 수 있습니다. TCP 또는 UDP 포트로 이벤트를 전송합니다. 어떤 포트를 사용해야 하는지 확인하려면 SaaS(Secure Logging Analytics)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기를 참조하십시오.

다음은 **logging host** 명령 구문의 예입니다.

**logging host** *interface_name SEC_IP_address* [ [ **tcp/port** ] | [ **udp/port** ] ]

예:

```
 > logging host mgmt 192.168.1.5 tcp/10125
> logging host mgmt 192.168.1.5 udp/10025
> logging host mgmt 2002::1:1 tcp/10125
> logging host mgmt 2002::1:1 udp/10025
```

- **interface_name** 인수는 메시지가 syslog 서버로 전송되는 ASA 인터페이스를 지정합니다. SDC와의 통신에 이미 사용 중인 동일한 ASA 인터페이스를 통해 SDC에 syslog 메시지를 보내는 것이 "모범 사례"입니다.
- **SEC_IP_address** 인수는 SEC가 설치된 VM의 IP 주소를 포함해야 합니다.
- **tcp/port** 또는 **udp/port** 키워드-인수 쌍은 시스템 로그 메시지가 TCP 프로토콜 및 관련 포트 또는 UDP 프로토콜 및 관련 포트를 사용하여 전송되도록 지정합니다. UDP 또는 TCP를 사용하여 syslog 서버에 데이터를 전송하도록 ASA를 구성할 수 있지만 둘 다 사용할 수는 없습니다. 프로토콜을 지정하지 않으면 기본 프로토콜은 UDP입니다.

  TCP를 지정한 경우 ASA은 syslog 서버의 장애를 감지하고 보호 조치로서 ASA를 통한 새로운 연결을 차단합니다. TCP syslog 서버에 대한 연결에 관계없이 새 연결을 허용하려면 b 단계를 참조하십시오. UDP를 지정한 경우 ASA는 syslog 서버의 작동 여부에 관계없이 새 연결을 계속 허용합니다. 유효한  값

  **Note** 두 개의 개별 syslog 서버로 ASA 메시지를 전송하려는 경우, 다른 syslog 서버의 적절한 인터페이스, IP 주소, 프로토콜 및 포트를 사용하여 두 번째 logging host 명령을 실행할 수 있습니다.

**b.** (선택 사항) TCP를 통해 이벤트를 SEC로 전송하는 경우 SEC가 중단되었거나 ASA의 로그 대기열이 꽉 차면 새 연결이 차단됩니다. syslog 서버가 백업되고 로그 대기열이 비워지면 새로운 연결이 다시 허용됩니다. TCP 시스

템 로그 서버에 대한 연결에 관계없이 새 연결을 허용하려면 이 명령을 사용하여 TCP 연결 시스템 로그 서버가 다운될 때 새 연결을 차단하는 기능을 비활성화합니다.

**logging permit-hostdown**

예:

```
> logging permit-hostdown
```

단계 **2** 다음 명령으로 어떤 시스템 로그 메시지를 시스템 로그 서버에 전송할지 지정합니다**.**

**logging trap** { severity_level | message_list }

예:

```
> logging trap 3
> logging trap asa_syslogs_to_cloud
```

심각도 레벨 숫자(1~7) 또는 이름을 지정할 수 있습니다. 예를 들어 심각도를 3으로 설정한 경우 ASA는 심각도 수준 3, 2, 1에 대해 syslog 메시지를 보냅니다.

message_list 인수는 사용자 지정 이벤트 목록을 생성한 경우 해당 목록의 이름으로 교체됩니다. 사용자 지정 이벤트 목록을 지정할 때는 해당 목록에 있는 시스템 로그 메시지만 보안 이벤트 커넥터로 전송합니다. 위의 예에서 asa_syslogs_to_cloud는 이벤트 목록의 이름입니다.

message_list를 사용하면 Cisco Cloud로 전송되는 syslog 메시지를 엄격하게 정의하여 비용을 절약할 수 있습니다.

message_list를 생성하려면 사용자 지정 이벤트 목록 생성를 참조하십시오. 데이터 수집 및 스토리지 비용에 대한 자세한 내용은 데이터 스토리지 요금제를 참조하십시오.

단계 **3** **(**선택 사항**) syslog** 타임스탬프 추가

logging timestamp 명령을 사용하여 syslog 메시지가 ASA에서 생성된 날짜 및 시간을 메시지에 추가합니다. 타임스탬프 값은 **SyslogTimestamp** 필드에 표시됩니다.

예:

```
> logging timestamp
```

**Note** 버전 9.10(1)부터 ASA는 이벤트 시스템 로그에서 RFC 5424에 따라 타임스탬프를 활성화하는 옵션을 제공합니다. 이 옵션을 활성화하면 syslog 메시지의 모든 타임스탬프가 RFC 5424 형식에 따라 시간을 표시합니다. 다음은 RFC 5424 형식의 샘플 출력입니다.

```
<166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol from src
interface :src IP/src port to dest IP/dest port.
```

단계 **4** **(**선택 사항**) EMBLEM** 형식이 아닌 **syslog** 메시지에 디바이스 **ID** 포함

디바이스 ID는 특정 ASA에서 전송된 모든 syslog 메시지를 쉽게 구분하는 데 도움이 되는 syslog 메시지에 삽입할 수 있는 ID입니다. 지침은 디바이스 ID를 EMBLEM 이외 형식 Syslog 메시지에 포함을 참조하십시오.

단계 **5** **(**선택 사항**)** 액세스 제어 규칙 **"permit"** 이벤트에 대한 로깅 활성화

액세스 제어 규칙이 리소스에 대한 액세스를 거부하면 이벤트가 자동으로 로깅됩니다. 액세스 제어 규칙이 리소스에 대한 액세스를 허용할 때 생성되는 이벤트도 로깅하려면, 액세스 제어 규칙에 대한 로깅을 켜고 심각도 유형을 구성해야 합니다. 개별 네트워크 액세스 제어 규칙에 대한 로깅을 설정하는 방법에 대한 지침은 로그 규칙 활동를 참조하십시오.

**Note** 액세스 제어 규칙 "permit" 이벤트에 대한 로깅을 활성화하면 일일 이벤트 수집 속도를 기반으로 하므로 구매한 데이터 플랜을 더 많이 사용하게 됩니다.

단계 **6** 로깅 활성화

명령 프롬프트에서 logging enable을 입력합니다. ASA에서 로깅은 개별 규칙이 아니라 전체 디바이스에 대해 활성화됩니다.

예:

```
> logging enable
```

**Note** 현재 CDO는 보안 로깅 활성화를 지원하지 않습니다.

단계 **7** 시작 구성에 변경 사항 저장

명령 프롬프트에서 write memory를 입력합니다. ASA에서 로깅은 개별 규칙이 아니라 전체 디바이스에 대해 활성화됩니다.

예:

```
> write memory
```

관련 정보**:**

- SDC 가상 머신에 SEC(Secure Event Connector) 설치, on page 438
- CDO 이미지를 사용하여 SEC 설치

# 사용자 지정 이벤트 목록 생성

다음 방법 중 하나를 사용하여 Cisco Cloud에 ASA syslog 이벤트를 전송할 때 맞춤형 이벤트 목록을 생성합니다.

- 명령줄 인터페이스를 사용하여 ASA Syslog 이벤트를 Cisco Cloud로 전송
- CDO 매크로를 사용하여 Cisco Cloud로 ASA 시스템 로그 이벤트 전송

다음 세 가지 기준에 따라 message_list라고도 하는 이벤트 목록을 생성할 수 있습니다.

- 이벤트 클래스
- 심각도
- 메시지 ID

특정 로깅 대상(예: syslog 서버 또는 Secure Event Connector)으로 보낼 사용자 지정 이벤트 목록을 생성하려면 다음 단계를 수행하십시오.

단계 **1** **Devices & Services(**디바이스 및 서비스**)** 페이지에서 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **2** 해당 탭을 클릭하고 맞춤형 이벤트 목록에 포함할 syslog 메시지가 있는 ASA를 선택합니다.

단계 **3** **Device Actions(**디바이스 작업**)** 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **4** ASA에 **logging list** 명령을 실행하려면 이 명령 구문을 사용합니다.

**logging list** *name* { **level** *level* [ **class** *message_class* ] | **message** *start_id* [ *-end_id* ] }

*name* 인수는 목록의 이름을 지정합니다. **level** *level* 키워드 및 인수 쌍은 심각도 레벨을 지정합니다. **class** *message_class* 키워드-인수 쌍은 특정 메시지 클래스를 지정합니다. **message** *start_id* [*-end_id*] 키워드-인수 쌍은 개별 시스템 로그 메시지 숫자 또는 숫자 범위를 지정합니다.

**Note** 심각도 레벨 이름을 syslog 메시지 목록의 이름으로 사용하지 마십시오. 금지된 이름에는 긴급, 경고, 중요 , 오류, 알림, 정보 및 디버깅이 포함됩니다. 마찬가지로 이벤트 목록 이름의 맨 앞에 이러한 단어의 처음 3개 글자를 사용하지 마십시오. 예를 들어 "err"로 시작하는 이벤트 목록 이름을 사용하지 마십시오.

- 심각도에 따라 이벤트 목록에 **syslog** 메시지를 추가합니다**.** 예를 들어 심각도를 3으로 설정한 경우 ASA는 심각도 수준 3, 2, 1에 대해 syslog 메시지를 보냅니다.

  예:

  ```
  > logging list asa_syslogs_to_cloud level 3
  ```

- 다른 기준에 따라 시스템 로그 메시지를 이벤트 목록에 추가합니다**.**

  이전 단계와 동일한 명령을 입력하여 기존 메시지 목록의 이름과 추가 기준을 지정합니다. 목록에 추가할 각 기준에 대한 새로운 명령을 입력합니다. 예를 들어 다음과 같이 목록에 포함할 syslog 메시지에 대한 기준을 지정할 수 있습니다.

  - 302013~302018 범위에 해당하는 시스템 로그 메시지 ID.
  - 심각도 레벨이 중요 이상인 모든 syslog 메시지(긴급, 경고 또는 중요).
  - 심각도 레벨이 경고 이상인 모든 HA 클래스 시스템 로그 메시지(긴급, 알림, 심각, 오류 또는 경고).

    예:

    ```
    > logging list asa_syslogs_to_cloud message 302013-302018
    > logging list asa_syslogs_to_cloud level critical
    > logging list asa_syslogs_to_cloud level warning class ha
    ```

    **Note** 다음 조건을 하나라도 충족하면 syslog 메시지가 로깅됩니다. syslog 메시지가 조건을 둘 이상 충족하는 경우 메시지는 한 번만 로깅됩니다.

단계 **5** 시작 구성에 변경 사항 저장

명령 프롬프트에 **write memory**를 입력합니다.

예:

```
> write memory
```

# 디바이스 ID를 EMBLEM 이외 형식 Syslog 메시지에 포함

EMBLEM 형식이 아닌 시스템 로그 메시지에 디바이스 ID를 포함하도록 ASA를 구성할 수 있습니다. syslog 메시지에 대해 1가지 디바이스 ID 유형만 지정할 수 있습니다. 다음 절차에서 이 절차를 참조합니다.

- 명령줄 인터페이스를 사용하여 ASA Syslog 이벤트를 Cisco Cloud로 전송
- CDO 매크로를 사용하여 Cisco Cloud로 ASA 시스템 로그 이벤트 전송

이 디바이스 식별자는 Event Logging(이벤트 로깅) 페이지에 표시되는 시스템 로그 이벤트의 SensorID 필드에 반영됩니다.

---

단계 **1** 디바이스 ID를 할당하려는 시스템 로그 메시지가 있는 ASA를 선택합니다.

단계 **2** Device Actions(디바이스 작업) 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **3** 디바이스에 **logging device-id** 명령을 실행하려면 이 명령 syntax(명령문)를 사용합니다.

**logging device-id** { **cluster-id** | **context-name** | **hostname** | **ipaddress***interface_name* [ **system** ] | **string***text* }

예:

```
> logging device-id hostname
> logging device-id context-name
> logging device-id string Cambridge
```

**context-name** 키워드는 현재 컨텍스트의 이름을 디바이스 ID로 사용하도록 지정합니다(다중 컨텍스트 모드에만 적용). 다중 컨텍스트 모드에서 관리자 컨텍스트 모드를 위해 디바이스 ID 로깅을 활성화하는 경우 시스템 실행 공간에서 발생하는 메시지는 시스템의 디바이스 ID를 사용하고 관리자 컨텍스트에서 발생하는 메시지는 관리자 컨텍스트의 이름을 디바이스 ID로 사용합니다.

**Note** ASA 클러스터에서는 항상 선택된 인터페이스에 대해 기본 유닛 IP 주소를 사용합니다.

**cluster-id** 키워드는 클러스터에서 개별 ASA 유닛의 부트 구성 고유 이름을 디바이스 ID로 지정합니다.

**hostname** 키워드는 ASA의 호스트 이름을 디바이스 ID로 사용하도록 지정합니다.

**ipaddress** *interface_name* 키워드-인수 쌍은 *interface_name*으로 지정된 인터페이스 IP 주소를 디바이스 ID로 사용하도록 지정합니다. **ipaddress** 키워드를 사용하는 경우 시스템 로그 메시지가 전송되는 인터페이스에 관계없이 디바이스 ID가 지정된 ASA 인터페이스 IP 주소가 됩니다. 클러스터 환경에서 **system** 키워드는 디바이스 ID가 인터페이스의 시스템 IP 주소가 되도록 만듭니다. 이 키워드는 디바이스에서 전송되는 모든 syslog 메시지에 대해 하나의 일관된 디바이스 ID를 제공합니다.

**string** *text* 키워드-인수 쌍은 문자열이 디바이스 ID로 사용되도록 지정합니다. 문자열은 최대 16자를 포함할 수 있습니다.

공백 또는 다음 문자를 사용할 수 없습니다.

- &(앰퍼샌드)
- `(작은따옴표)
- "(큰따옴표)

- <(보다 작음)
- >(보다 큼)
- ? (물음표)

단계 **4** 시작 구성에 변경 사항 저장

명령 프롬프트에 **write memory**를 입력합니다.

예:

```
> write memory
```

# ASA 디바이스용 NetFlow Secure Event Logging(NSEL)

ASA의 기본 Syslog 메시지에는 ASA에서 보고하는 이벤트가 위협을 나타내는지 여부를 확인하는 데 필요한 데이터가 많이 부족합니다. NSEL(Netflow Secure Event Logging)은 해당 데이터와 함께 Secure Cloud Analytics를 제공합니다.

"플로우는 네트워크 디바이스를 통과하는 몇 가지 공통 속성이 있는 패킷의 단방향 시퀀스로 정의됩니다. 이렇게 수집된 플로우는 외부 디바이스인 NetFlow 컬렉터로 내보내집니다. 네트워크 플로우는 매우 세분화됩니다. 예를 들어 플로우 레코드에는 IP 주소, 패킷 및 바이트 수, 타임스탬프, ToS(서비스 유형), 애플리케이션 포트, 입력 및 출력 인터페이스 등의 세부 정보가 포함됩니다."[1]

Cisco ASA는 NetFlow 버전 9 서비스를 지원합니다. NSEL의 ASA 구현은 플로우에서 중요한 이벤트를 나타내는 레코드만 내보내는 상태 저장 IP 플로우 추적 방법을 제공합니다. 스테이트풀 플로우 추적에서 추적된 플로우는 일련의 상태 변경을 거칩니다.

이 문서에서는 CDO 매크로를 사용하여 ASA에 대해 NetFlow를 구성하는 간단한 방법을 설명합니다. Cisco ASA NetFlow 구현 가이드는 ASA에서 NetFlow를 구성하는 방법에 대한 매우 자세한 설명을 제공하며, 이 콘텐츠와 함께 유용한 리소스를 찾을 수 있습니다.

향후 작업

CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성으로 이동합니다.

관련 문서

- CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성
- ASA에서 NSEL(NetFlow Secure Event Logging) 구성 삭제
- ASA 전역 정책의 이름 확인

1. ("Cisco Systems NetFlow 서비스 내보내기 버전 9." 인터넷 엔지니어링 태스크 포스, 네트워크 워킹 그룹, 코멘트 요청: 3954, 2004년 10월, B. Claise, Ed. https://www.ietf.org/rfc/rfc3954.txt)

# CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성

ASA는 NSEL(NetFlow Secure Event Logging)을 사용하여 세부 연결 이벤트 데이터를 보고합니다. 양방향 플로우 통계를 포함하는 Stealthwatch Cloud 분석을 이 연결 이벤트 데이터에 적용할 수 있습니다. 이 절차에서는 ASA 디바이스에서 NSEL을 구성하고 이러한 NSEL 이벤트를 플로우 컬렉터로 전송하는 방법을 설명합니다. 이 경우 플로우 컬렉터는 SEC(Secure Event Connector)입니다.

이 절차는 **NSEL** 구성 매크로를 참조합니다.

```
 flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
flow-export template timeout-rate {{timeout_rate_in_mins}}
flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
flow-export active refresh-interval {{refresh_interval_in_mins}}
class-map {{flow_export_class_name}}
     match {{add_this_traffic_to_class_map}}
policy-map {{global_policy_map_name}}
     class {{flow_export_class_name}}
          flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}
service-policy {{global_policy_map_name}} global
logging flow-export-syslogs disable
show run flow-export
show run policy-map {{global_policy_map_name}}
show run class-map {{flow_export_class_name}}
```

다음은 모든 기본값, 클래스 맵의 일반 이름 및 global_policy에 추가된 클래스 맵이 포함된 Configure NSEL 매크로의 예입니다. 이러한 절차를 완료하면 매크로는 다음과 유사합니다.

```
 flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
flow-export template timeout-rate 60
flow-export delay flow-create 55
flow-export active refresh-interval 1
class-map flow_export_class_map
     match any
policy-map global_policy
     class flow_export_class_map
          flow-export event-type all destination {{SEC_IPv4_address}}
logging flow-export-syslogs disable
show run flow-export
show run policy-map global_policy
show run class-map flow_export_class_map
```

시작하기 전에

다음 정보를 수집합니다.

- 이전에 CDO 매크로로 작업한 적이 없는 경우 다음 항목을 읽어보십시오.
  - 디바이스 관리를 위한 CLI 매크로, on page 99
    - CLI 매크로 편집, on page 102
    - CLI 매크로 실행, on page 101
- ASA에서 데이터를 수신할 SEC의 IPv4 주소
- SEC에 데이터를 보낼 asa의 인터페이스

- NetFlow 이벤트 전송에 사용되는 UDP 포트 번호 SaaS(Secure Logging Analytics)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기, on page 436의 내용을 참조하십시오.
- ASA 전역 정책의 이름 확인, on page 409

워크플로

이 워크플로에 따라 CDO 매크로를 사용하여 ASA 디바이스에 대한 NSEL을 구성합니다. 각 단계를 수행해야 합니다.

1. NSEL 매크로 구성 열기 , on page 403.
2. NSEL 메시지의 대상 및 SEC로 전송되는 간격 정의, on page 404.
3. SEC로 전송될 NSEL 이벤트를 정의하는 클래스 맵 생성, on page 405.
4. NSEL 이벤트에 대한 정책 맵 정의, on page 405.
5. 중복된 시스템 로그 메시지 비활성화, on page 406.
6. 매크로 검토 및 전송, on page 408.

향후 작업

NSEL 매크로 구성 열기 , on page 403로 이동하여 위의 워크플로를 시작합니다.

# NSEL 매크로 구성 열기

### Before you begin

이는 더 긴 워크플로의 첫 번째 부분입니다. 시작하기 전에 CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성, on page 402의 내용을 참조하십시오.

---

단계 **1** **Devices & Services(**디바이스 및 서비스**)** 페이지에서 **Devices(**디바이스**)** 탭을 클릭합니다.
단계 **2** 적절한 디바이스 유형 탭을 클릭하고 NSEL(NetFlow Secure Event Logging)을 구성할 ASA을 선택합니다.
단계 **3** **Device Actions(**디바이스 작업**)** 창에서 **Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.
단계 **4** Macro(매크로) 별   을 클릭하여 사용 가능한 매크로 목록을 표시합니다.
단계 **5** 매크로 목록에서 **Configuring NSEL(NSEL** 구성**)**을 선택합니다.
단계 **6** Macro(매크로) 상자에서 **View Parameters(**매개변수 보기**)**를 클릭합니다.

---

### What to do next

NSEL 메시지의 대상 및 SEC로 전송되는 간격 정의, on page 404를 진행합니다.

# NSEL 메시지의 대상 및 SEC로 전송되는 간격 정의

NSEL 메시지는 테넌트에 온보딩한 SEC 중 하나로 전송할 수 있습니다. 이 지침은 매크로의 다음 섹션을 참조합니다.

flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}

flow-export template timeout-rate {{timeout_rate_in_mins}}

flow-export delay flow-create {{delay_flow_create_rate_in_secs}}

flow-export active refresh-interval {{refresh_interval_in_mins}}

### Before you begin

이는 더 큰 워크플로우의 일부입니다. 시작하기 전에 CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성, on page 402의 내용을 참조하십시오.

단계 **1** **flow-export destination** 명령은 NetFlow 패킷이 전송되는 컬렉터를 정의합니다. 이 경우 SEC로 전송됩니다. 다음 매개변수에 대한 필드를 입력합니다.

- **{{interface}}** - NetFlow 이벤트가 전송되는 ASA의 인터페이스 이름을 입력합니다.
- **{{SEC_IPv4_address}}** - SEC의 IPv4 주소를 입력합니다. SEC는 플로우 컬렉터 역할을 합니다.
- **{{SEC_NetFlow_port}}** - NetFlow 패킷이 전송되는 SEC의 UDP 포트 번호를 입력합니다.

단계 **2** **flow-export template timeout-rate** 명령은 템플릿 레코드가 구성된 모든 출력 대상으로 전송되는 간격을 지정합니다.

- **{{timeout_rate_in_mins}}** - 템플릿을 재전송할 때까지의 시간(분)을 입력합니다. **60**분 값을 사용하는 것이 좋습니다. SEC는 템플릿을 처리하지 않습니다. 숫자가 크면 SEC에 대한 트래픽이 줄어듭니다.

단계 **3** **flow-export delay flow-create** 명령은 flow-create 이벤트의 전송을 지정된 시간(초)만큼 지연시킵니다. 이 값은 권장 Active Timeout(활성 시간 제한) 값과 일치하며 ASA에서 내보낸 플로우 이벤트 수를 줄입니다. 이 속도에서 NSEL 이벤트는 연결 종료 시 또는 연결 생성 후 55초 중 더 빠른 시점에 CDO에 처음 표시됩니다. 이 명령이 구성되지 않은 경우 지연이 없으며 플로우가 생성되는 즉시 flow-create 이벤트가 내보내집니다.

- **{{delay_flow_create_rate_in_secs}}** - 플로우 생성 이벤트 전송 간의 지연 시간(초)을 입력합니다. **55**초 값을 사용하는 것이 좋습니다.

단계 **4** **flow-export active refresh-interval** 명령은 수명이 긴 플로우에 대한 상태 업데이트가 ASA에서 전송되는 빈도를 정의합니다. 유효한 값은 1분~60분입니다. Flow Update Interval(플로우 업데이트 간격) 필드에서 **flow-export active refresh-interval**을 **flow-export delay flow-create** 간격보다 5초 이상 크게 구성하면 flow-update 이벤트가 flow-creation 이벤트보다 먼저 표시되지 않습니다.

- **{{refresh_interval_in_mins}}-1**분 값을 사용하는 것이 좋습니다. 유효한 값은 1분~60분입니다.

### What to do next

SEC로 전송될 NSEL 이벤트를 정의하는 클래스 맵 생성, on page 405를 진행합니다.

## SEC로 전송될 NSEL 이벤트를 정의하는 클래스 맵 생성

매크로의 다음 명령은 클래스의 모든 NSEL 이벤트를 그룹화한 다음 해당 클래스를 SEC(Secure Event Connector)로 내보냅니다. 이 지침은 매크로의 다음 섹션을 참조합니다.

class-map {{flow_export_class_name}}

match {{add_this_traffic_to_class_map}}

### Before you begin

이는 더 큰 워크플로우의 일부입니다. 시작하기 전에 CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성, on page 402의 내용을 참조하십시오.

---

단계 **1** **class-map** 명령은 SEC로 내보낼 NSEL 트래픽을 식별하는 클래스 맵의 이름을 지정합니다.

- **{{flow-export-class-name}}**- 클래스 맵의 이름을 입력합니다. 이름의 길이는 최대 40자입니다. "class-default"라는 이름 그리고 "_internal" 또는 "_default"로 시작하는 모든 이름은 예약되어 있습니다. 모든 유형의 클래스 맵은 동일한 네임스페이스를 사용하므로, 다른 클래스 맵 유형에서 사용된 이름을 재사용할 수 없습니다.

단계 **2** 클래스 맵과 연결될(일치하는) 트래픽을 식별합니다. **{{add_this_traffic_to_class_map}}**의 값에 대해 다음 옵션 중 하나를 선택합니다.

- **{{add_this_traffic_to_class_map}}** 필드에 **any**를 입력합니다. NSEL 트래픽에 대한 모든 트래픽 유형을 모니터링합니다. **"any"** 값을 사용하는 것이 좋습니다**.**
- **{{add_this_traffic_to_class_map}}** 필드에 **access-list *name-of-access-list***를 입력합니다. 이렇게 하면 생성한 액세스 목록과 연결된 모든 트래픽이 연결됩니다. 자세한 내용은 Cisco ASA NetFlow 구현 가이드에서 모듈러 정책 프레임워크를 통한 플로우 내보내기 구성을 참조하십시오.

---

### What to do next

NSEL 이벤트에 대한 정책 맵 정의, on page 405를 계속합니다.

## NSEL 이벤트에 대한 정책 맵 정의

이 작업은 이전 작업에서 생성한 클래스에 NetFlow 내보내기 작업을 할당하고 새 정책 맵에 클래스를 할당합니다. 이 지침은 매크로의 다음 섹션을 참조합니다.

policy-map {{global_policy_map_name}}

class {{flow_export_class_name}}

flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}

**Before you begin**

이는 더 큰 워크플로우의 일부입니다. 시작하기 전에 CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성, on page 402의 내용을 참조하십시오.

---

단계 **1** **policy-map** 명령은 policy-map을 생성합니다. 다음 작업에서는 이 정책 맵을 전역 정책과 연결합니다.

- **{{global_policy_map_name}}** - 정책 맵의 이름을 입력합니다. 방화벽의 기존 전역 정책 이름(있는 경우)을 사용하는 것이 좋습니다. 전역 정책의 기본 이름은 **global_policy**입니다. ASA 전역 정책의 이름 확인을 참조하십시오. Cisco ASA NetFlow 구현 가이드의 Configure Flow-Export Actions Through Modular Policy Framework(모듈형 정책 프레임워크를 통한 플로우 내보내기 작업 구성)에 따라 새 정책 맵을 생성하고 전역적으로 적용하는 경우 나머지 검사 정책은 비활성화됩니다.

단계 **2** **class** 명령은 SEC로 전송될 NSEL 이벤트를 정의하는 클래스 맵 생성, on page 405에서 생성한 클래스 맵의 이름을 상속합니다.

단계 **3** **flow-export event-type** {{event-type}} **destination** {{IPv4_address}} 명령은 플로우 컬렉터(이 경우 SEC)로 전송해야 하는 이벤트 유형을 정의합니다.

- **{{event-type}}** - event_type 키워드는 필터링되는 지원 이벤트의 이름입니다. **"all"** 값을 사용하는 것이 좋습니다.
- **{{SEC_IPv4_address}}** -SEC의 IPv4 주소입니다. 해당 값은 NSEL 메시지의 대상 및 SEC로 전송되는 간격 정의, on page 404에 입력한 값에서 상속됩니다.

---

**What to do next**

중복된 시스템 로그 메시지 비활성화, on page 406를 계속합니다.

## 중복된 시스템 로그 메시지 비활성화

이 지침은 매크로의 이 섹션을 참조합니다. 명령을 수정할 필요가 없습니다.

logging flow-export-syslogs disable

NetFlow를 활성화하여 플로우 정보를 내보내면 다음 표의 시스템 로그 메시지가 중복됩니다. 동일한 정보를 NetFlow를 통해 내보내므로 성능을 위해 중복 시스템 로그 메시지를 비활성화하는 것이 좋습니다.

**Note** NSEL 및 시스템 로그 메시지가 모두 활성화된 경우 두 로깅 유형 간에 시간순으로 정렬되지 않습니다.

| **Syslog** 메시지 | 설명 | **NSEL** 이벤트 **ID** | **NSEL** 확장 이벤트 **ID** |
|---|---|---|---|
| 106100 | ACL(액세스 제어 규칙)이 발생할 때마다 생성됨 | 1 — 플로우가 생성됨(ACL에서 플로우를 허용한 경우)<br>3 — 플로우가 거부됨(ACL에서 플로우를 거부한 경우) | 0 — ACL이 플로우를 허용한 경우<br>1001 — 인그레스 ACL에서 플로우를 거부함<br>1002 — 이그레스 ACL에서 플로우를 거부함 |
| 106015 | 첫 번째 패킷이 SYN 패킷이 아니므로 TCP 플로우가 거부됨 | 3 — 플로우가 거부됨 | 1004 — 첫 번째 패킷이 TCP SYN 패킷이 아니므로 플로우가 거부됨 |
| 106023 | **access-group** 명령을 통해 인터페이스에 연결된 ACL에서 플로우를 거부한 경우 | 3 — 플로우가 거부됨 | 1001 — 인그레스 ACL에서 플로우를 거부함<br>1002 — 이그레스 ACL에서 플로우를 거부함 |
| 302013, 302015, 302017, 302020 | TCP, UDP, GRE, ICMP 연결 생성 | 1 — 플로우가 생성됨 | 0 — 무시함 |
| 302014, 302016, 302018, 302021 | TCP, UDP, GRE, ICMP 연결 해체 | 2 — 플로우가 삭제됨 | 0 — 무시함<br>>2000 — 플로우가 해체됨 |
| 313001 | 디바이스에 대한 ICMP 패킷이 거부됨 | 3 — 플로우가 거부됨 | 1003 — 구성으로 인해 To-the-box 플로우가 거부됨 |
| 313008 | 디바이스에 대한 ICMP v6 패킷이 거부됨 | 3 — 플로우가 거부됨 | 1003 — 구성으로 인해 To-the-box 플로우가 거부됨 |
| 710003 | 디바이스 인터페이스에 대한 연결 시도가 거부됨 | 3 — 플로우가 거부됨 | 1003 — 구성으로 인해 To-the-box 플로우가 거부됨 |

중복 시스템 로그 메시지를 비활성화하지 않으려면 이 매크로를 편집하고 이 줄만 삭제할 수 있습니다.

**logging flow-export-syslogs disable**

NetFlow 관련 시스템 로그 메시지 비활성화 및 다시 활성화의 절차에 따라 나중에 개별 시스템 로그 메시지를 활성화하거나 비활성화할 수 있습니다.

## 매크로 검토 및 전송

**Before you begin**

이는 더 큰 워크플로우의 일부입니다. 시작하기 전에 CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성, on page 402의 내용을 참조하십시오.

단계 **1** 매크로의 필드를 입력한 후 **Review(**검토**)**를 클릭하여 ASA로 전송되기 전에 명령을 검토합니다.

단계 **2** 명령에 대한 응답이 만족스러우면 **Send(**전송**)**를 클릭합니다.

단계 **3** 명령을 전송한 후 "일부 명령이 실행 중인 구성을 변경했을 수 있습니다."라는 메시지와 함께 두 개의 링크가 표시될 수 있습니다.


- **Write to Disk(**디스크에 쓰기**)**를 클릭하면 이 명령으로 수행한 변경 사항과 실행 중인 구성의 다른 모든 변경 사항이 디바이스의 시작 구성에 저장됩니다.
- **Dismiss(**해제**)**를 클릭하면 메시지가 사라집니다.

CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성, on page 402에 설명된 워크플로우를 완료했습니다.

# ASA에서 NSEL(NetFlow Secure Event Logging) 구성 삭제

이 절차에서는 SEC(Secure Event Connector)를 NSEL 플로우 컬렉터로 지정하는 ASA에서 NetFlow NSEL(Secure Event Logging) 을 삭제하는 방법을 설명합니다. 이 절차에서는 CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성에 설명된 매크로를 반대로 수행합니다.

이 절차는 **DELETE NSEL** 매크로를 참조합니다.

```
policy-map {{flow_export_policy_name}}
no class {{flow_export_class_name}}
no class-map {{flow_export_class_name}}
no flow-export destination {{interface}} {{IPv4_address}} {{NetFlow_port}}
no flow-export template timeout-rate {{timeout_rate_in_mins}}
no flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
no flow-export active refresh-interval {{refresh_interval_in_mins}}
logging flow-export-syslogs enable
show run flow-export
show run policy-map {{flow_export_policy_name}}
show run class-map {{flow_export_class_name}}
```

## DELETE-NSEL 매크로 열기

단계 **1** **Devices & Services(**디바이스 및 서비스**)** 페이지에서 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **2** 적절한 디바이스 유형 탭을 클릭하고 NSEL(NetFlow Secure Event Logging) 구성을 삭제할 ASA을 선택합니다.

단계 **3** **Device Actions(**디바이스 작업**)** 창에서 **Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **4** 매크로 별표(  Macros )를 클릭하여 사용 가능한 매크로 목록을 표시합니다.

단계 **5** 매크로 목록에서 **DELETE-NSEL**을 선택합니다.

단계 **6** Macro(매크로) 상자에서 **View Parameters(**매개변수 보기**)**를 클릭합니다.

## 매크로에 값을 입력하여 **No** 명령 완료

ASA CLI는 명령의 "no" 형식을 사용하여 삭제합니다. 매크로의 필드를 입력하여 명령의 "no" 형식을 완성합니다.

단계 **1** policy-map {{flow_export_policy_name}}

- **{{flow_export_policy_name}}** - 정책 맵 이름의 값을 입력합니다.

단계 **2** no class {{flow_export_class_name}}

- **{{flow_export_class_name}}** - 클래스 맵 이름의 값을 입력합니다.

단계 **3** no class-map {{flow_export_class_name}}

- **{{flow_export_class_name}}** - 클래스 맵 이름의 값이 위의 단계에서 상속됩니다.

단계 **4** no flow-export destination {{interface}} {{IPv4_address}} {{NetFlow_port}}

- **{{interface}}** - NetFlow 이벤트가 전송된 ASA의 인터페이스 이름을 입력합니다.
- **{{IPv4_address}}** - SEC의 IPv4 주소를 입력합니다. SEC는 플로우 컬렉터 역할을 합니다.
- **{{NetFlow_port}}** - NetFlow 패킷이 전송되는 SEC의 UDP 포트 번호를 입력합니다.

단계 **5** no flow-export template timeout-rate {{timeout_rate_in_mins}}

- **{{timeout_rate_in_mins}}** - flow-export 템플릿 제한 시간을 입력합니다.

단계 **6** no flow-export delay flow-create {{delay_flow_create_rate_in_secs}}

- **{{delay_flow_create_rate_in_secs}}** - flow-export 지연 흐름 생성 속도를 입력합니다.

단계 **7** no flow-export active refresh-interval {{refresh_interval_in_mins}}

- **{{refresh_interval_in_mins}}** - flow-export 활성 새로 고침 간격을 입력합니다.

# **ASA** 전역 정책의 이름 확인

ASA의 전역 정책 이름을 확인하려면 다음 절차를 수행합니다.

단계 **1** Devices & Services(디바이스 및 서비스) 페이지에서 전역 정책의 이름을 찾을 디바이스를 선택합니다.

단계 **2** Device Actions(디바이스 작업) 창에서 **>_Command Reference(**명령 참조**)**를 선택합니다.

단계 **3** Command Line Interface(명령줄 인터페이스) 창의 프롬프트에 다음을 입력합니다.

**show running-config service-policy**

아래 예의 출력에서 global_policy는 전역 정책의 이름입니다.

예:

> **show running-config service-policy**

**service-policy global_policy global**

# NSEL 데이터 플로우 문제 해결

CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성 및 을 했으면 다음 절차를 사용하여 NSEL 이벤트가 사용자 ASA에서 Cisco Cloud로 전송되고 Cisco Cloud가 이를 수신하는지 확인합니다.

ASA가 NSEL 이벤트를 SEC(보안 이벤트 커넥터)로 보낸 다음 Cisco Cloud로 보내도록 구성된 후에는 데이터가 즉시 흐르지 않습니다. NET에서 생성되는 NSEL 관련 트래픽이 있다고 가정하면 첫 번째 NSEL 패킷이 ASA에 도착하는 데 몇 분 정도 걸릴 수 있습니다.

**Note** 이 워크플로우는 "flow-export counters" 명령 및 "capture" 명령을 사용하여 NSEL 데이터 플로우 문제를 해결하는 방법을 보여줍니다. 이러한 명령 사용에 대한 자세한 내용은CLI Book 1: Cisco ASA 시리즈 일반 운영 CLI 구성 가이드의 "패킷 캡처" 및 Cisco ASA NetFlow 구현 가이드의 "NSEL 모니터링"을 참조하십시오.

다음 세 가지 작업을 수행합니다.

- NetFlow 패킷이 SEC로 전송되고 있는지 확인
- Cisco Cloud에서 NetFlow 패킷을 수신하고 있는지 확인

## NSEL 이벤트가 SEC로 전송되고 있는지 확인

두 명령 중 하나를 사용하여 NSEL 패킷이 SEC로 전송되고 있는지 확인합니다.

- flow-export counters
- capture

**"flow-export counters"** 명령을 사용하여 전송되는 **flow-export** 패킷 및 **NSEL** 오류 확인

- NSEL 이벤트를 SEC로 전송하도록 ASA를 구성했는지 확인합니다 CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성을 참조하십시오.

- SEC IP 주소는 NSEL 이벤트의 플로우 컬렉터 주소입니다. 테넌트에 둘 이상의 SEC를 온보딩한 경우 올바른 IP 주소를 사용하고 있는지 확인합니다.
- NetFlow 이벤트를 전달하는 데 사용되는 UDP 포트 번호를 찾습니다. SaaS(Secure Logging Analytics)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기를 참조하십시오.
- NSEL 이벤트를 전송하는 ASA에서 권장되는 인터페이스는 관리 인터페이스입니다. 인터페이스가 다를 수 있습니다.

CDO의 대량 명령줄 인터페이스를 사용하여 NSEL에 대해 구성한 ASA에 이러한 명령을 전송합니다.

---

단계 **1** 탐색 창에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 적절한 디바이스 탭을 클릭하고 NSEL 이벤트를 SEC로 전송하도록 구성한 ASA를 선택합니다.

단계 **4** **Device Actions(**장치 작업**)** 창에서 **Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **5** `clear flow-export counters` 명령을 실행하여 플로우 내보내기 카운터를 재설정합니다. 이렇게 하면 새 이벤트가 수신되는지 쉽게 확인할 수 있도록 clear export flow 카운터가 0으로 재설정됩니다.

예시:

```
> clear flow-export counters
Done!
```

단계 **6** NSEL 패킷의 대상, 전송된 패킷 수 및 오류를 확인하려면 show flow-export counters 명령을 실행합니다.

예시:

```
>show flow-export counters
대상: management 209.165.200.225 10425
Statistics:
packets sent 25000
오류:
block allocation errors 0
invalid interface 0
template send failure 0
no route to collector 0
source port allocation 0
```

위의 출력에서 목적지 줄은 NSEL 이벤트가 전송 된 인터페이스, SEC의 IP 주소, SEC의 포트 10425를 보여줍니다.ASA 또한 25000의 전송된 패킷도 표시 됩니다.

오류가 없고 패킷이 전송되는 경우 아래의 Cisco Cloud에서 NetFlow 패킷을 수신하고 있는지 확인으로 건너뛰십시오.

---

오류 설명:

- **block allocation errors(**블록 할당 오류**)** -블록 할당 오류가 수신되면 ASA가 플로우 엑스포터에 메모리를 할당하지 않은 것입니다.
  - 복구 작업: Cisco TAC(Technical Assistance Center)에 문의합니다.
- **invalid interface(**잘못된 인터페이스**)** - NSEL 이벤트를 SEC로 전송하려고 하지만 플로우 내보내기에 대해 정의한 인터페이스가 전송하도록 구성되지 않았음을 나타냅니다.
  - 복구 작업: NSEL을 구성할 때 선택한 인터페이스를 검토합니다. 관리 인터페이스를 사용하는 것이 좋습니다. 사용자의 인터페이스는 다를 수 있습니다.
- **template send failure(**템플릿 전송 실패**)** - NSEL을 정의해야 하는 템플릿이 올바르게 구문 분석되지 않았습니다.
  - 복구 작업: Cisco Defense Orchestrator 지원팀에 문의
- no route to collector - 에서 SEC로의 네트워크 경로가 없음을 나타냅니다.ASA
  - 복구 작업:
    - NSEL을 구성할 때 SEC에 사용한 IP 주소가 올바른지 확인합니다.
    - SEC의 상태가 Active(활성)이고 최근 하트비트를 전송했는지 확인합니다. SDC에 연결할 수 없음, on page 553을 참조하십시오.
    - 보안 디바이스 커넥터의 상태가 Active(활성)이고 최근 하트비트를 전송했는지 확인합니다.
- **source port allocation(**소스 포트 할당**)** -ASA 에 잘못된 포트가 있음을 나타낼 수 있습니다.

## "capture" 명령을 사용하여 ASA에서 SEC로 전송된 NSEL 패킷 캡처

- NSEL 이벤트를 SEC로 전송하도록 ASA를 구성했는지 확인합니다 CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성을 참조하십시오.
- SEC IP 주소는 NSEL 이벤트의 플로우 컬렉터 주소입니다. 테넌트에 둘 이상의 SEC를 온보딩한 경우 올바른 IP 주소를 사용하고 있는지 확인합니다.
- NetFlow 이벤트를 전달하는 데 사용되는 UDP 포트 번호를 찾습니다. SaaS(Secure Logging Analytics)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기를 참조하십시오.
- NSEL 이벤트를 전송하는 ASA에서 권장되는 인터페이스는 관리 인터페이스입니다. 인터페이스가 다를 수 있습니다.

CDO의 CDO 명령줄 인터페이스를 사용하여 NSEL에 대해 구성한 ASA에 이러한 명령을 전송합니다.

---

단계 **1** 탐색 창에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 적절한 디바이스 유형 탭을 클릭하고 NSEL 이벤트를 SEC로 전송하도록 구성한 ASA를 선택합니다.

단계 **4** **Device Actions(**디바이스 작업**)** 창에서 **Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **5** 명령 창에서 이 **capture** 명령을 실행합니다.

>**capture***capture_name***interface***interface_name* **match udp any host** *IP_of_SEC***eq***NetFlow_port*

어디에서

- *capture_name*은 패킷 캡처의 이름입니다.
- *interface_name*은 NSEL 패킷이 ASA를 나가는 인터페이스의 이름입니다.
- *IP_of_SEC*는 SEC VM의 IP 주소입니다.
- *NetFlow_port*는 NSEL 이벤트가 전송되는 포트입니다.

이렇게 하면 패킷 캡처가 시작됩니다.

단계 **6** 캡처된 패킷을 보려면 **show capture** 명령을 실행합니다.

**> show capture***capture_name*

여기서 *capture_name*은 이전 단계에서 정의한 패킷 캡처의 이름입니다.

다음은 캡처 시간, 패킷이 전송된 IP 주소, IP 주소 및 패킷이 전송된 포트를 표시하는 출력의 예입니다. 이 예에서 192.168.25.4는 SEC의 IP 주소이고 포트 10425는 NSEL 이벤트를 수신하는 SEC의 포트입니다.

캡처된 6개의 패킷

```
1: 14:23:51.706308 192.168.0.169.16431 > 192.168.25.4.10425: udp 476
2: 14:23:53.923017 192.168.0.169.16431 > 192.168.25.4.10425: udp 248
3: 14:24:07.411904 192.168.0.169.16431 > 192.168.25.4.10425: udp 1436
4: 14:24:07.411920 192.168.0.169.16431 > 192.168.25.4.10425: udp 1276
5: 14:24:21.021208 192.168.0.169.16431 > 192.168.25.4.10425: udp 112
6: 14:24:27.444755 192.168.0.169.16431 > 192.168.25.4.10425: udp 196
```

단계 **7** 패킷 캡처를 수동으로 중지하려면 **capture stop** 명령을 실행합니다.

**> capture** *capture_name***stop**

여기서 *capture_name*은 이전 단계에서 정의한 패킷 캡처의 이름입니다.

## **Cisco Cloud**에서 **NetFlow** 패킷을 수신하고 있는지 확인

시작하기 전에

NSEL 이벤트가 ASA에서 전송되고 있는지 확인합니다.

## 라이브 NSEL 이벤트 확인

라이브 이벤트와 기록 이벤트를 모두 확인합니다.

이 절차에서는 Cisco Cloud가 지난 1시간 내에 수신한 NSEL 이벤트를 필터링합니다.

단계 1 CDO 메뉴에서 분석 > 이벤트 로깅를 선택합니다.
단계 2 **Live(**라이브**)** 탭을 클릭합니다.
단계 3 이벤트 필터를 고정으로 엽니다.
단계 4 ASA Events(이벤트) 섹션에서 NetFlow가 선택되어 있는지 확인합니다.
단계 5 NSEL 이벤트를 전송하도록 구성한 ASA의 IP 주소를 Sensor ID(센서 ID) 필드에 입력합니다.
단계 6 필터의 맨 아래에서 "Include NetFlow Events(NetFlow 이벤트 포함)"가 선택되어 있는지 확인합니다.

## 이전 NSEL 이벤트 확인

이 절차는 Cisco 클라우드가 지정한 기간 내에 수신한 NSEL 이벤트를 필터링합니다.

단계 1 CDO 메뉴에서 분석 > 이벤트 로깅를 선택합니다.
단계 2 기록 탭을 클릭합니다.
단계 3 이벤트 필터를 고정으로 엽니다.
단계 4 ASA Events(이벤트) 섹션에서 NetFlow가 선택되어 있는지 확인합니다.
단계 5 CDO가 NSEL 이벤트를 수신한 적이 있는지 확인할 수 있도록 시작 시간을 충분히 이전으로 설정합니다.
단계 6 NSEL 이벤트를 전송하도록 구성한 ASA의 IP 주소를 Sensor ID(센서 ID) 필드에 입력합니다.
단계 7 필터의 맨 아래에서 "Include NetFlow Events(NetFlow 이벤트 포함)"가 선택되어 있는지 확인합니다.

# ASA 이벤트 유형

이벤트 로깅 페이지에서 이벤트 검색 및 필터링할 때 이벤트 유형 목록에서 선택할 수 있습니다. 이러한 이벤트 유형은 시스템 로그 ID의 그룹을 나타냅니다. 아래 표는 어떤 시스템 로그 ID가 어떤 ASA 이벤트 유형에 포함되어 있는지 보여줍니다. 특정 시스템 로그 ID에 대해 자세히 알아보려면 Cisco ASA 시리즈 시스템 로그 메시지 가이드에서 검색할 수 있습니다.

일부 시스템 로그 이벤트에는 추가 속성 "EventName"이 있습니다. attribute:value 쌍을 기준으로 필터링하여 EventName 특성을 사용하여 이벤트 테이블을 필터링하여 찾을 수 있습니다. Syslog 이벤트에 대한 이벤트 이름 속성을 참조하십시오.

일부 시스템 로그 이벤트에는 추가 속성 "EventGroup" 및 "EventGroupDefinition"이 있습니다. attribute:value 쌍을 기준으로 필터링하여 이러한 추가 속성을 사용하여 이벤트 테이블을 필터링할 수 있습니다. 일부 시스템 로그 메시지에 대한 EventGroup 및 EventGroupDefinition 속성을 참조하십시오.

ASA 디바이스용 NetFlow Secure Event Logging(NSEL)는 시스템 로그 이벤트와 다릅니다. NetFlow 필터는 NSEL 레코드를 생성한 모든 NetFlow 이벤트 ID를 검색합니다. 이러한 NetFlow 이벤트 ID는 Cisco ASA NetFlow 구현 가이드에 정의되어 있습니다.

| 필터 이름 | 해당 시스템 로그 이벤트 또는 **NetFlow** 이벤트 |
|---|---|
| AAA | 109001-109035<br>113001-113027 |
| 봇넷 | 338001-338310 |
| 장애 조치 | 101001-101005, 102001, 103001-103007, 104001-104004, 105001-105048<br>210001-210022<br>311001-311004<br>709001-709007 |
| 방화벽 거부됨 | 106001, 106007, 106012, 106013, 106015, 106016, 106017, 106020, 106021, 106022, 106023, 106025, 106027<br>방화벽 거부됨 이벤트는 NetFlow에 포함될 수 있으며 NetFlow 이벤트 ID 및 시스템 로그 ID와 함께 보고될 수 있습니다. |
| 방화벽 트래픽 | 106001-106100, 108001-108007, 110002-110003<br>201002-201013, 209003-209005, 215001<br>302002-302304, 302022-302027, 303002-303005, 313001-313008, 317001-317006, 324000-324301, 337001-337009<br>400001-400050, 401001-401005, 406001-406003, 407001-407003, 408001-408003, 415001-415020, 416001, 418001-418002, 419001-419003, 424001-424002, 431001-431002, 450001<br>500001-500005, 508001-508002<br>607001-607003, 608001-608005, 609001-609002, 616001<br>703001-703003, 726001<br>방화벽 트래픽 이벤트는 NetFlow에 포함될 수 있으며 NetFlow 이벤트 ID 및 시스템 로그 ID와 함께 보고될 수 있습니다. |
| IPsec VPN | 402001-402148, 602102-602305, 702304-702307 |
| NAT | 201002-201013, 202001-202011, 305005-305012 |

| 필터 이름 | 해당 시스템 로그 이벤트 또는 NetFlow 이벤트 |
|---|---|
| SSL VPN | 716001-716060, 722001-722053, 723001-723014, 724001-724004, 725001-725015 |
| NetFlow | 0, 1, 2, 3, 5 |

관련 정보:

- 일부 시스템 로그 메시지에 대한 EventGroup 및 EventGroupDefinition 속성, 479 페이지
- Syslog 이벤트에 대한 이벤트 이름 속성

# 구문 분석된 ASA 시스템 로그 이벤트

구문 분석된 시스템 로그 이벤트는 다른 시스템 로그 이벤트보다 더 많은 이벤트 속성을 포함하며, 구문 분석된 특정 필드에서 검색할 수 있습니다. SEC는 지정한 모든 ASA 이벤트를 Cisco Cloud로 전달하지만, 아래 테이블의 시스템 로그 메시지만 구문 애널리틱스됩니다. 구문 분석된 모든 시스템 로그 이벤트는 식별을 돕기 위해 이탤릭체로 표시됩니다.

시스템 로그에 대한 자세한 설명은 Cisco ASA Series 시스템 로그 메시지를 참조하십시오.

| 시스템 로그 ID | 시스템 로그 범주 | 시스템 로그 메시지의 목적 |
|---|---|---|
| 106015 | 방화벽 | 상태가 잘못된 TCP 거부를 나타냅니다. |
| 106023 | 방화벽 | 실제 IP 패킷이 ACL에 의해 거부되었습니다. 이 메시지는 ACL에 대해 로그 옵션을 활성화하지 않은 경우에도 나타납니다. |
| 106100 | 액세스 목록/사용자 세션 | 패킷이 ACL에 의해 허용되거나 거부되었습니다. |
| 113019 | 사용자 인증 | 중요 AnyConnect |
| 302013, 302015, 302017, 302020 | 사용자 세션 | TCP, UDP, GRE 및 ICMP 연결 생성을 위한 연결 시작 및 종료 Syslog. |
| 302014, 302016, 302018, 302021 | 사용자 세션 | TCP, UDP, GRE 및 ICMP 연결 생성을 위한 연결 시작 및 종료 Syslog. |
| 302020 - 302021 | 사용자 세션 | ICMP 세션 설정 및 해제. |
| 305006 | 사용자 세션/NAT 및 PAT | NAT 연결 실패 |

| 시스템 로그 **ID** | 시스템 로그 범주 | 시스템 로그 메시지의 목적 |
|---|---|---|
| 305011-305014 | 사용자 세션/NAT 및 PAT | NAT 빌드/해체 관련 |
| 313001, 313008 | IP 스택 | 상자에 거부된 연결을 나타냅니다. |
| 414004 | 시스템 | 중요 AnyConnect |
| 609001 - 609002 | 방화벽 | 영역에 연결된 호스트 **ip-address**에 대해 네트워크 상태 컨테이너가 예약/제거되었습니다. |
| 710002,710004 710005 | 사용자 세션 | 상자 연결 실패 |
| 710003 | 사용자 세션 | 상자에 거부된 연결을 나타냅니다. |
| 746012, 746013 | 사용자 세션 | 중요 AnyConnect |

관련 정보**:**

- 명령줄 인터페이스를 사용하여 ASA Syslog 이벤트를 Cisco Cloud로 전송
- 이벤트 로깅 페이지에서 이벤트 검색 및 필터링

# Secure Firewall Cloud Native용 SaaS(Secure Analytics and Logging)

이벤트는 Cisco 클라우드에 저장되며 CDO의 Event Logging(이벤트 로깅) 페이지에서 볼 수 있습니다. 이 페이지에서 이벤트를 필터링하고 검토하여 네트워크에서 트리거되는 보안 규칙을 명확하게 파악할 수 있습니다. **Logging and Troubleshooting(**기록 및 문제 해결**)** 패키지는 이러한 기능을 제공합니다.

**Logging Analytics and Detection(**로깅 분석 및 탐지**)** 패키지를 통해 시스템은 디바이스 이벤트에 Secure Cloud Analytics 동적 엔터티 모델링을 적용하고, 행동 모델링 분석을 사용하여 Secure Cloud Analytics 관찰 및 알림을 생성할 수 있습니다. **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 패키지를 보유한 경우, 시스템은 디바이스 이벤트와 네트워크 트래픽 모두에 동적 엔터티 모델링을 적용하고, 관찰 및 경고를 생성합니다. Cisco SSO(Single Sign-On, 단일 인증)를 사용하여 CDO에서 사용자에게 프로비저닝된 Cisco Secure Cloud Analytics 포털로 교차 실행할 수 있습니다.

### CDO 이벤트 뷰어에 Secure Firewall Cloud Native 이벤트가 표시되는 방법

Secure Firewall Cloud Native에서 로깅이 활성화되고 네트워크 트래픽이 액세스 제어 규칙 기준과 일치하면 syslog 이벤트 및 NSEL 이벤트가 생성됩니다. 이벤트가 Cisco Cloud에 저장되면 CDO에서 볼 수 있습니다.

모든 디바이스에서 여러 SEC(Secure Event Connector)를 설치하고 규칙에 의해 생성된 이벤트를 마치 시스템 로그 서버인 것처럼 SEC로 전송할 수 있습니다. 그런 다음 SEC는 Cisco Cloud에 이벤트를 전달합니다. 모든 SEC에 동일한 이벤트를 전달하지 마십시오. Cisco Cloud로 전송되는 이벤트를 복제하고 일일 수집 속도를 불필요하게 부풀릴 수 있습니다.

보안 이벤트 커넥터를 통해 **Secure Firewall Cloud Native**에서 **Cisco Cloud**로 시스템 로그 및 **NSEL** 이벤트를 전송하는 방법

**Logging and Troubleshooting(**기본 로그 및 문제 해결 **)** 라이센스를 사용하여, Secure Firewall Cloud Native이벤트가 Cisco cloud에 도달하는 방법은 다음과 같습니다.

1. 클러스터 엔드포인트, 네임스페이스 및 토큰을 사용하여 Secure Firewall Cloud Native를 CDO에 온보딩합니다. .
2. 시스템 로그 및 NSEL 이벤트를 시스템 로그 서버인 것처럼 SEC 중 하나에 전달하고 디바이스에서 로깅을 활성화하도록 Secure Firewall Cloud Native를 구성합니다.
3. SEC는 이벤트가 저장된 Cisco Cloud로 이벤트를 전달합니다.
4. CDO는 설정한 필터에 따라 Cisco Cloud의 이벤트를 이벤트 뷰어에 표시합니다.

**Logging Analytics and Detection(**로깅 분석 및 탐지**)** 또는 **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스를 사용하면 다음 작업도 수행됩니다.

1. Cisco Secure Cloud Analytics는 Cisco 클라우드에 저장된 Secure Firewall Cloud Native 시스템 로그 이벤트에 분석을 적용합니다.
2. 생성된 관찰 및 알림은 CDO 포털과 연결된 Secure Cloud Analytics 포털에서 액세스할 수 있습니다.
3. CDO 포털에서 Secure Cloud Analytics 포털을 교차 실행하여 이러한 관찰 및 알림을 검토할 수 있습니다.

솔루션에 사용된 구성 요소

**SDC(Secure Device Connector)** - SDC는 CDO를 Secure Firewall Cloud Native에 연결합니다. Secure Firewall Cloud Native에 대한 로그인 자격 증명은 SDC에 저장되지 않습니다. 자세한 내용은 SDC(Secure Device Connector), 5 페이지을 참조하십시오.

**SEC(Secure Event Connector)** - SEC는 Secure Firewall Cloud Native에서 이벤트를 수신하여 Cisco Cloud로 전달하는 애플리케이션입니다. Cisco Cloud에 있으면 CDO의 Event Logging(이벤트 로깅) 페이지에서 이벤트를 보거나 Secure Cloud Analytics를 사용하여 분석할 수 있습니다. 환경에 따라 SEC는 보안 디바이스 커넥터(있는 경우)에 설치됩니다. 또는 네트워크에서 유지 관리하는 자체 CDO 커넥터 가상 머신에서 수행할 수 있습니다. 자세한 내용은 보안 이벤트 커넥터, 437 페이지를 참조하십시오.

**Secure Firewall Cloud Native** - Secure Firewall Cloud Native는 확장성과 관리성을 위해 Kubernetes(K8s) 오케스트레이션을 사용하여 Cisco의 업계 최고의 보안을 CNFW(클라우드 네이티브 폼 팩터)로 원활하게 확장합니다. Amazon Elastic Kubernetes Service(Amazon EKS)는 AWS 클라우드에서 Kubernetes

애플리케이션을 시작, 실행 및 확장할 수 있는 유연성을 제공합니다. Amazon EKS는 고가용성 및 보안 클러스터를 제공하고 패치, 노드 프로비저닝, 업데이트 등의 주요 작업을 자동화합니다.

**Secure Cloud Analytics**는 Secure Firewall Cloud Native 이벤트에 동적 엔티티 모델링을 적용하여 이 정보를 기반으로 탐지를 생성합니다. 이렇게 하면 네트워크에서 수집한 텔레메트리를 심층적으로 분석하여 추세를 식별하고 네트워크 트래픽의 이상 동작을 검사할 수 있습니다. **Logging Analytics and Detection(**로깅 분석 및 탐지**)** 또는 **Total Network Analytics and Monitoring(**총 네트워크 분석 및 모니터링**)** 라이선스가 있는 경우 이 서비스를 사용할 수 있습니다.

라이선싱

이 솔루션을 구성하려면 다음 계정 및 라이선스가 필요합니다.

- **Cisco Defense Orchestrator**. CDO 테넌트가 있어야 합니다.
- **Secure Device Connector**. 보안 디바이스 커넥터에 대한 별도의 라이선스는 없습니다.
- **Secure Event Connector**. 보안 이벤트 커넥터에 대한 별도의 라이선스는 없습니다.
- **Secure Logging Analytics(SaaS)**. Security Analytics and Logging 라이선스 테이블을 참조하십시오.
- **Secure Firewall Cloud Native**. 기본 라이선스 이상

### Security Analytics and Logging 라이선싱

SaaS(Security Analytics and Logging)를 구현하려면 다음 라이선스 중 하나를 구매해야 합니다.

| 라이선스 이름 | 제공된 기능 | 사용가능한라이선스기간 | 기능 사전 요건 |
|---|---|---|---|
| 로깅 및 문제 해결 | • 라이브 피드 및 기록 보기로 CDO 내의 Secure Firewall Cloud Native 이벤트 및 이벤트 세부 정보 보기 | • 1년<br>• 3년<br>• 5년 | • CDO<br>• 소프트웨어 버전 9.6 이상을 실행하는 온프레미스 Secure Firewall Cloud Native 구축<br>• Cisco Cloud에 Secure Firewall Cloud Native 이벤트를 전달하기 위한 하나 이상의 SEC 구축 |

| 라이선스 이름 | 제공된 기능 | 사용가능한라이선스기간 | 기능 사전 요건 |
|---|---|---|---|
| 로깅 분석 및 탐지(이전 이름 방화벽 분석 및 모니터링) | 로깅 및 문제 해결 기능 추가:<br>• 이벤트에 동적 엔터티 모델링 및 행동 분석을 적용합니다.<br>• 이벤트 데이터를 기반으로 Secure Cloud Analytics에서 알림 열기, CDO 이벤트 뷰어에서 교차 실행 | • 1년<br>• 3년<br>• 5년 | • CDO<br>• 소프트웨어 버전 9.6 이상을 실행하는 온프레미스 Secure Firewall Cloud Native 구축<br>• Cisco Cloud에 Secure Firewall Cloud Native 이벤트를 전달하기 위한 하나 이상의 SEC 구축<br>• 새로 프로비저닝된 또는 기존의 Cisco Secure Cloud Analytics 포털. |

| 라이선스 이름 | 제공된 기능 | 사용 가능한 라이선스 기간 | 기능 사전 요건 |
|---|---|---|---|
| 총 네트워크 분석 및 모니터링 | 로깅 분석 및 탐지, 추가:<br>• Secure Firewall Cloud Native 이벤트, 온프레미스 네트워크 트래픽 및 클라우드 기반 네트워크 트래픽에 동적 엔터티 모델링 및 동작 분석을 적용합니다.<br>• Secure Firewall Cloud Native 이벤트 데이터, Cisco Secure Cloud Analytics 센서에서 수집한 온프레미스 네트워크 트래픽 플로우 데이터 및 CDO 이벤트 뷰어에서 교차 실행되는 Cisco Secure Cloud Analytics에 전달된 클라우드 기반 네트워크 트래픽의 조합을 기반으로 하는 Cisco Secure Cloud Analytics의 공개 알림 | • 1년<br>• 3년<br>• 5년 | • CDO<br>• 소프트웨어 버전 9.6 이상을 실행하는 온프레미스 Secure Firewall Cloud Native 구축<br>• Cisco Cloud에 이벤트를 전달하기 위한 하나 이상의 SEC 구축<br>• 네트워크 트래픽 플로우 데이터를 클라우드에 전달하기 위해 하나 이상의 Cisco Secure Cloud Analytics 센서 버전 4.1 이상을 구축하거나, 네트워크 트래픽 플로우 데이터를 Cisco Secure Cloud Analytics로 전달하기 위해 Cisco Secure Cloud Analytics를 클라우드 기반 구축과 통합합니다.<br>• 새로 프로비저닝된 또는 기존의 Cisco Secure Cloud Analytics 포털. |

데이터 요금제

Cisco Cloud가 온보딩된 Secure Firewall Cloud Native에서 매일 수신하는 이벤트 수를 반영하는 데이터 요금제를 구매해야 합니다. 이를 "일일 수집 속도"라고 합니다. Logging Volume Estimator 도구를 사용하여 일일 수집 속도를 예측할 수 있으며, 속도가 변경되면 데이터 요금제를 업데이트할 수 있습니다.

데이터 요금제는 일별 볼륨 1GB 단위로 제공되며 1년, 3년 또는 5년 단위로 제공됩니다. 데이터 요금제에 대한 자세한 내용은 Secure Logging Analytics(SaaS) 주문 가이드를 참조하십시오.

참고 Security Analytics and Logging 라이선스 및 데이터 요금제를 보유하고 있는 경우 나중에 다른 라이선스를 취득할 수 있으며, 이것만 있으면 다른 데이터 요금제를 구매할 필요가 없습니다. 네트워크 트래픽 처리량이 변경되어 다른 데이터 플랜을 취득하는 경우에는 다른 Security Analytics and Logging 라이선스를 구입하지 않아도 됩니다.

**30**일 무료 평가판

CDO에 로그인하고 **Monitoring(**모니터링**)** > **Event Logging(**이벤트 로깅**)** 탭으로 이동하여 30일 무료 평가판을 요청할 수 있습니다. 30일 평가판이 끝나면 SaaS(Secure Logging Analytics) 주문 가이드의 지침에 따라 CCW(Cisco Commerce Workspace)에서 서비스를 계속하기 위해 원하는 이벤트 데이터 볼륨을 주문할 수 있습니다.

다음 단계

이동 Secure Firewall Cloud Native용 Secure Logging and Analytics(SaaS) 구현, 422 페이지

# Secure Firewall Cloud Native용 Secure Logging and Analytics(SaaS) 구현

시작하기 전에

- 다음에 대한 자세한 사항은 Secure Firewall Cloud Native용 SaaS(Secure Analytics and Logging), 417 페이지의 내용을 검토합니다.
  - Cisco Cloud로 이벤트를 전송하는 방법
  - 솔루션의 애플리케이션
  - 필요한 라이선스
  - 필요한 데이터 요금제
- CDO 테넌트를 생성하기 위해 매니지드 서비스 제공자 또는 CDO 영업 담당자에게 문의했습니다.
- 를 검토합니다. SDC를 사용하여 CDO를 Secure Firewall Cloud Native에 연결하는 것은 "모범 사례"로 간주되지만 필수 사항은 아닙니다.

  SDC(Secure Device Connector), 5 페이지를 검토합니다. SDC를 사용하여 CDO를 Secure Firewall Cloud Native에 연결하는 것은 "모범 사례"로 간주되지만 필수 사항은 아닙니다.
- 네트워크에서 SDC를 구축하려는 경우 다음 방법 중 하나를 사용하여 설치할 수 있습니다.
  - CDO의 준비된 VM 이미지를 사용하여 SDC를 설치하는 데 CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축, 8 페이지를 사용합니다. 이는 SDC를 구축하는 가장 쉬운 방법입니다.
  - 자체 VM에 보안 디바이스 커넥터 구축, 12 페이지를 사용합니다.

- 보안 이벤트 커넥터 설치했으며 모든 Secure Firewall Cloud Native에서 테넌트에 온보딩된 SEC로 이벤트를 전송할 수 있습니다.
- 어카운트 사용자에 대한 새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성했습니다.

**Cisco SaaS(Security Analytics and Logging)**를 구현하고 보안 이벤트 커넥터를 통해 **Cisco Cloud**로 이벤트를 전송하는 워크플로우

1. 위의 "시작하기 전에"를 검토하여 환경이 올바르게 구성되었는지 확인하십시오.
2. 클러스터 엔드포인트, 네임스페이스 및 토큰을 사용하여 보안 방화벽 Secure Firewall Cloud Native 디바이스를 등록합니다.
3. Secure Firewall Cloud Native 시스템 로그 이벤트를 Cisco Cloud로 전송, 424 페이지.
4. Secure Firewall Cloud Native 디바이스용 NSEL 구성, 428 페이지.
5. 이벤트가 CDO에 표시되는지 확인합니다. 탐색 막대에서 **Monitoring(**모니터링**) > Event Logging(**이벤트 로깅**)**을 선택합니다. 라이브 이벤트를 보려면 Live(라이브) 탭을 클릭합니다.
6. **Firewall Analytics and Monitoring(**방화벽 분석 및 모니터링**)** 또는 **Total Network Analytics and Monitoring(**총 네트워크 분석 및 모니터링**)** 라이선스가 있는 경우 다음 섹션인 **Cisco Secure Cloud Analytics**를 사용하여 이벤트 분석을 계속 진행합니다.

**Cisco Secure Cloud Analytics**를 사용하여 이벤트 분석

**Firewall Analytics and Monitoring(**방화벽 분석 및 모니터링**)** 또는 **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스가 있는 경우 이전 단계와 함께 다음을 수행합니다.

1. Cisco Secure Cloud Analytics 포털 프로비저닝, 458 페이지.
2. **Total Network Analytics and Monitoring** 라이선스를 구매한 경우 하나 이상의 Secure Cloud Analytics 센서를 내부 네트워크에 구축합니다. 전체 네트워크 분석 및 보고를 위한 Cisco Secure Cloud Analytics 센서 구축, 460 페이지의 내용을 참조하십시오.
3. Cisco SSO(Single Sign-On) 자격 증명에 연결된 Secure Cloud Analytics 사용자 어카운트를 생성하도록 사용자를 초대합니다. CDO에서 Cisco Secure Cloud Analytics 알림 보기, 461 페이지의 내용을 참조하십시오.
4. 디바이스 이벤트에서 생성된 Secure Cloud Analytics 알림을 모니터링하려면 CDO에서 Secure Cloud Analytics를 교차 실행합니다. CDO에서 Cisco Secure Cloud Analytics 알림 보기, 461 페이지의 내용을 참조하십시오.

**CDO**에서 교차 실행하여 **Cisco Secure Cloud Analytics** 알림 검토

**Firewall Analytics and Monitoring(**방화벽 분석 및 모니터링**)** 또는 **Total Network Analytics and Monitoring(**총 네트워크 분석 및 모니터링**)** 라이선스를 사용하면 CDO에서 Secure Cloud Analytics로 교차 실행하여 디바이스 이벤트에 의해 생성된 알림을 검토할 수 있습니다.

자세한 내용은 다음 문서를 참조하십시오.

- CDO에 로그인
- CDO에서 Cisco Secure Cloud Analytics 알림 보기, 461 페이지
- Cisco Secure Cloud Analytics 및 동적 엔티티 모델링
- 방화벽 이벤트 기반 알림 작업

보안 이벤트 커넥터 문제 트러블슈팅

다음 문제 해결 항목을 사용하여 다음에 대한 상태 및 로깅 정보를 수집합니다.

- SEC 온보딩 실패 문제 해결
- 문제 해결 로그 파일 이벤트 로깅
- 상태 확인을 사용하여 보안 이벤트 커넥터의 상태 학습

워크플로

보안 및 분석 로깅 이벤트를 사용하여 네트워크 문제 해결에서는 Cisco Security Analytics 및 로깅에서 생성된 이벤트를 사용하여 사용자가 네트워크 리소스에 액세스할 수 없는 이유를 확인하는 방법을 설명합니다.

방화벽 이벤트 기반 알림 작업도 참조하십시오.

# Secure Firewall Cloud Native 시스템 로그 이벤트를 Cisco Cloud로 전송

이 절차에서는 Secure Firewall Cloud Native 시스템 로그 이벤트를 SEC(Secure Event Connector)에 전달한 다음 로깅을 활성화하는 방법을 설명합니다. 이러한 절차에서는 해당 워크플로우를 완료하는 데 필요한 사항만 설명합니다.

참고 명령은 방화벽의 구성 파일에 입력해야 합니다.

시작하기 전에

주의 이 절차는 디바이스 구성 파일의 syntax(명령문)에 익숙한 고급 사용자를 위한 것입니다. 이 방법은 Defense Orchestrator에 저장된 구성 파일의 복사본을 직접 변경합니다. 따라서 수정하기 전에 기존 디바이스 구성을 백업하는 것이 좋습니다. 필요한 경우 백업 구성을 복원할 수 있습니다.

1. 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.
2. **Devices(**디바이스**)** 탭을 클릭합니다.
3. 적절한 디바이스 유형 탭을 클릭하고 구성을 수정할 Secure Firewall Cloud Native 디바이스를 선택합니다.
4. 오른쪽의 관리 창에서 **Configuration(**구성**)**를 클릭합니다.
5. **Download(**다운로드**)**를 클릭합니다.

단계 **1** **Device Configuration(**디바이스 구성**)** 탭에서 **Edit(**편집**)**를 클릭합니다.

단계 **2** 구성 파일에서 "snmp-server-config" 앞에 새 CRD 항목을 생성하고 아래에 설명된 명령을 입력합니다.

명령

```
########## CRD ### name: entry-name, order: order-number, generation: 1 ##########
           logging enable
           logging timestamp
           logging trap {severity_level | message_list}
           logging list name {level level [class message_class] | message start_id[-end_id]}
           logging host interface_name SEC_IP_address [[tcp/port] | [udp/port]]
           logging host interface_name SEC_IP_address [[tcp/port] | [udp/port]]
           logging permit-hostdown
```

예

```
########## CRD ### name: syslog-events, order: 4, generation: 3 ##########
           logging enable
           logging timestamp
           logging list sfcn_syslogs_to_cloud level critical
           logging list sfcn_syslogs_to_cloud level warnings class ha
           logging list sfcn_syslogs_to_cloud message 302013-302018
           logging trap sfcn_syslogs_to_cloud
           logging host outside 192.168.1.5 17/10125
           logging host outside 192.168.1.5 6/10025
           logging permit-hostdown
```

- **entry-name**: CRD 항목의 이름을 지정합니다. 이름에 밑줄(_)을 사용하지 마십시오.
- **order-number**: 원하는 순서대로 명령을 실행할 순서를 지정합니다. 구성 파일에서 사용되는 가장 높은 숫자 앞에 오는 고유한 숫자여야 합니다.
- **logging enable**: 개별 규칙이 아니라 전체 디바이스에 대해 로깅이 활성화됩니다. 참고: 현재 CDO는 보안 로깅 활성화를 지원하지 않습니다.
- **logging timestamp**: logging timestamp 명령을 사용하여 시스템 로그 메시지가 방화벽에서 시작된 날짜 및 시간을 메시지에 추가합니다. 타임스탬프 값은 SyslogTimestamp 필드에 표시됩니다.

- **logging trap** {severity_level | message_list}:

  다음 명령으로 어떤 시스템 로그 메시지를 시스템 로그 서버에 전송할지 지정합니다.

  예:

  ```
  logging trap 3
            logging trap sfcn_syslogs_to_cloud
  ```

  심각도 레벨 숫자(1~7) 또는 이름을 지정할 수 있습니다. 예를 들어, 심각도 레벨을 3으로 설정한 경우 sfcn은 심각도 레벨 3, 2, 1에 대해 시스템 로그 메시지를 보냅니다.

  message_list 인수는 사용자 지정 이벤트 목록을 생성한 경우 해당 목록의 이름으로 교체됩니다. 사용자 지정 이벤트 목록을 지정할 때는 해당 목록에 있는 시스템 로그 메시지만 보안 이벤트 커넥터로 전송합니다. 위의 예에서 sfcn_syslogs_to_cloud는 이벤트 목록의 이름입니다.

  message_list를 사용하면 Cisco Cloud로 전송되는 시스템 로그 메시지를 엄격하게 정의하여 비용을 절약할 수 있습니다.

- **logging list** *name* {**level** *level* [class message_class] | **message** start_id[-end_id]}

  방화벽에 **logging list** 명령을 실행하려면 이 명령 syntax(명령문)를 사용합니다.

  name 인수는 목록의 이름을 지정합니다. level level 키워드 및 인수 쌍은 심각도 레벨을 지정합니다. **class** *message_class* 키워드-인수 쌍은 특정 메시지 클래스를 지정합니다. **message** start_id [-end_id] 키워드-인수 쌍은 개별 시스템 로그 메시지 숫자 또는 숫자 범위를 지정합니다.

  다른 기준에 따라 시스템 로그 메시지를 이벤트 목록에 추가합니다.

  이전 단계와 동일한 명령을 입력하여 기존 메시지 목록의 이름과 추가 기준을 지정합니다. 목록에 추가할 각 기준에 대한 새로운 명령을 입력합니다. 예를 들어 다음과 같이 목록에 포함할 syslog 메시지에 대한 기준을 지정할 수 있습니다.

  - 302013~302018 범위에 해당하는 시스템 로그 메시지 ID.
  - 심각도 레벨이 중요 이상인 모든 syslog 메시지(긴급, 경고 또는 중요).
  - 심각도 레벨이 경고 이상인 모든 HA 클래스 시스템 로그 메시지(긴급, 알림, 심각, 오류 또는 경고).

  참고 다음 조건을 하나라도 충족하면 syslog 메시지가 로깅됩니다. syslog 메시지가 조건을 둘 이상 충족하는 경우 메시지는 한 번만 로깅됩니다.

- **logging host** interface_name SEC_IP_address [[tcp/port] | [udp/port]]
- **logging host** interface_name SEC_IP_address [[tcp/port] | [udp/port]]

TCP 또는 UDP를 사용하여 SEC가 시스템 로그 서버인 것처럼 SEC에 메시지를 전송하도록 Secure Firewall Cloud Native를 구성합니다. SEC는 IPv4 또는 IPv6 주소를 사용할 수 있습니다. TCP 또는 UDP 포트로 이벤트를 전송합니다. 어떤 포트를 사용해야 하는지 확인하려면 Cisco Security Analytics and Logging에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기를 참조하십시오.

logging host interface_name SEC_IP_address [[tcp/port] | [udp/port]]

다음은 logging host 명령 syntax(명령문)의 예입니다.

```
logging host outside 192.168.1.5 tcp/10125
          logging host outside 192.168.1.5 udp/10025
          logging host outside 2002::1:1 tcp/10125
          logging host outside 2002::1:1 udp/10025
```

**interface_name** 인수는 메시지가 시스템 로그 서버로 전송되는 Secure Firewall Cloud Native 인터페이스를 지정합니다. SDC와 통신하는 데 사용되는 것과 동일한 Secure Firewall Cloud Native 인터페이스에서 SEC로 시스템 로그 메시지를 전송하는 것이 "모범 사례"입니다.

**SEC_IP_address** 인수는 SEC가 설치된 VM의 IP 주소를 포함해야 합니다.

**tcp/port** 또는 **udp/port** 키워드-인수 쌍은 시스템 로그 메시지가 TCP 프로토콜 및 관련 포트 또는 UDP 프로토콜 및 관련 포트를 사용하여 전송되도록 지정합니다. UDP 또는 TCP를 사용하여 시스템 로그 서버에 데이터를 전송하도록 Secure Firewall Cloud Native를 구성할 수 있지만, 둘 다 사용할 수는 없습니다. 프로토콜을 지정하지 않으면 기본 프로토콜은 UDP입니다.

TCP를 지정하면 Secure Firewall Cloud Native가 시스템 로그 서버 장애를 검색하고 보안 보호를 위해 Secure Firewall Cloud Native를 통한 새 연결이 차단됩니다. TCP 시스템 로그 서버에 대한 연결에 관계없이 새 연결을 허용하려면 b 단계를 참조하십시오. UDP를 지정한 경우 Secure Firewall Cloud Native는 시스템 로그 서버의 작동 여부에 관계없이 새 연결을 계속 허용합니다.

참고 Secure Firewall Cloud Native 메시지를 별도의 시스템 로그 서버 2개로 전송하려는 경우 다른 시스템 로그 서버의 적절한 인터페이스, IP 주소, 프로토콜 및 포트를 사용하여 두 번째 logging host 명령을 실행할 수 있습니다.

- **logging permit-hostdown**

  (선택 사항) TCP를 통해 이벤트를 SEC로 전송하는 경우 SEC가 중단되었거나 Secure Firewall Cloud Native의 로그 대기열이 꽉 차면 새 연결이 차단됩니다. syslog 서버가 백업되고 로그 대기열이 비워지면 새로운 연결이 다시 허용됩니다. TCP 시스템 로그 서버에 대한 연결에 관계없이 새 연결을 허용하려면 이 명령을 사용하여 TCP 연결 시스템 로그 서버가 다운될 때 새 연결을 차단하는 기능을 비활성화합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

단계 **4** 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.

# 디바이스에 대한 NetFlow NSEL(Secure Event Logging)

보안 방화벽 클라우드 네이티브의 기본 시스템 로그 메시지에는 클라우드 Cisco Secure Cloud Analytics가 보안 방화벽 클라우드 네이티브에서 보고한 이벤트가 위협을 나타내는지 확인하는 데 필요한 데이터가 많이 부족합니다. NSEL(Netflow Secure Event Logging)은 해당 데이터와 함께 Secure Cloud Analytics를 제공합니다.

"플로우는 네트워크 디바이스를 통과하는 몇 가지 공통 속성이 있는 패킷의 단방향 시퀀스로 정의됩니다. 이렇게 수집된 플로우는 외부 디바이스인 NetFlow 컬렉터로 내보내집니다. 네트워크 플로우는 매우 세분화됩니다. 예를 들어 플로우 레코드에는 IP 주소, 패킷 및 바이트 수, 타임스탬프, ToS(서비스 유형), 애플리케이션 포트, 입력 및 출력 인터페이스 등의 세부 정보가 포함됩니다."

보안 방화벽 클라우드 네이티브는 NetFlow 버전 9 서비스를 지원합니다. NSEL의 Secure Firewall Cloud Native 구현은 흐름에서 중요한 이벤트를 나타내는 레코드만 내보내는 상태 저장 IP 흐름 추적 방법을 제공합니다. 스테이트풀 플로우 추적에서 추적된 플로우는 일련의 상태 변경을 거칩니다.

이 설명서에서는 구성 파일의 명령 집합을 사용하여 보안 방화벽 클라우드 네이티브 디바이스에 대해 NetFlow를 구성하는 간단한 접근 방식을 설명합니다. Cisco NetFlow 구현 가이드는 보안 방화벽 클라우드 네이티브에서 NetFlow를 구성하는 방법에 대한 매우 자세한 설명을 제공하며, 이 콘텐츠와 함께 유용한 리소스를 찾을 수 있습니다.

## Secure Firewall Cloud Native 디바이스용 NSEL 구성

Secure Firewall Cloud Native 디바이스는 NSEL(Netflow Secure Event Logging)을 사용하여 세부 연결 이벤트 데이터를 보고합니다. 양방향 플로우 통계를 포함하는 Cisco Secure Cloud Analytics를 이 연결 이벤트 데이터에 적용할 수 있습니다. 이 절차에서는 Secure Firewall Cloud Native 디바이스에서 NSEL을 구성하고 이러한 NSEL 이벤트를 플로우 컬렉터로 전송하는 방법을 설명합니다. 이 경우 플로우 컬렉터는 SEC(Secure Event Connector)입니다.

절차는 방화벽의 구성 파일에 입력할 명령 집합을 나타냅니다.

---

단계 **1** Device Configuration(디바이스 구성) 탭에서 Edit(편집)를 클릭합니다.

단계 **2** 구성 파일에서 "snmp-server-config" 앞에 새 CRD 항목을 생성하고 아래에 설명된 명령을 입력합니다.

명령

```
########## CRD ### name: entry-name, order: order-number, generation: 1 ##########
flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
    flow-export template timeout-rate {{timeout_rate_in_mins}}
    flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
    flow-export active refresh-interval {{refresh_interval_in_mins}}
    class-map {{flow_export_class_name}}
         match {{add_this_traffic_to_class_map}}
    policy-map {{global_policy_map_name}}
         class {{flow_export_class_name}}
              flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}
    service-policy {{global_policy_map_name}} global
    logging flow-export-syslogs disable
    show run flow-export
    show run policy-map {{global_policy_map_name}}
    show run class-map {{flow_export_class_name}}
```

다음은 class-map의 일반 이름 및 global_policy에 추가된 클래스 맵에 모두 기본값이 입력된 예입니다.

```
########## CRD ### name: nsel-config, order: 5, generation: 1 ##########
    flow-export destination outside {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
    flow-export template timeout-rate 60
    flow-export delay flow-create 55
    flow-export active refresh-interval 1
    class-map flow_export_class_map
         match any
    policy-map global_policy
         class flow_export_class_map
              flow-export event-type all destination {{SEC_IPv4_address}}
    service-policy global_policy global
    logging flow-export-syslogs disable
    show run flow-export
    show run policy-map global_policy
    show run class-map flow_export_class_map
```

단계 **3** **Save(**저장**)**를 클릭합니다.

단계 **4**

---

## NSEL 메시지의 대상 및 SEC로 전송되는 간격 정의

NSEL 메시지는 테넌트에 온보딩한 SEC 중 하나로 전송할 수 있습니다. 이 지침은 매크로의 다음 섹션을 참조합니다.

flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}

flow-export template timeout-rate {{timeout_rate_in_mins}}

flow-export delay flow-create {{delay_flow_create_rate_in_secs}}

flow-export active refresh-interval {{refresh_interval_in_mins}}

### Before you begin

이는 더 큰 워크플로우의 일부입니다. 시작하기 전에 CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성, on page 402의 내용을 참조하십시오.

---

단계 **1** **flow-export destination** 명령은 NetFlow 패킷이 전송되는 컬렉터를 정의합니다. 이 경우 SEC로 전송됩니다. 다음 매개변수에 대한 필드를 입력합니다.

- **{{interface}}** - NetFlow 이벤트가 전송되는 ASA의 인터페이스 이름을 입력합니다.
- **{{SEC_IPv4_address}}** - SEC의 IPv4 주소를 입력합니다. SEC는 플로우 컬렉터 역할을 합니다.
- **{{SEC_NetFlow_port}}** - NetFlow 패킷이 전송되는 SEC의 UDP 포트 번호를 입력합니다.

단계 **2** **flow-export template timeout-rate** 명령은 템플릿 레코드가 구성된 모든 출력 대상으로 전송되는 간격을 지정합니다.

- **{{timeout_rate_in_mins}}** - 템플릿을 재전송할 때까지의 시간(분)을 입력합니다. **60**분 값을 사용하는 것이 좋습니다. SEC는 템플릿을 처리하지 않습니다. 숫자가 크면 SEC에 대한 트래픽이 줄어듭니다.

단계 **3** **flow-export delay flow-create** 명령은 flow-create 이벤트의 전송을 지정된 시간(초)만큼 지연시킵니다. 이 값은 권장 Active Timeout(활성 시간 제한) 값과 일치하며 ASA에서 내보낸 플로우 이벤트 수를 줄입니다. 이 속도에서 NSEL 이벤트는 연결 종료 시 또는 연결 생성 후 55초 중 더 빠른 시점에 CDO에 처음 표시됩니다. 이 명령이 구성되지 않은 경우 지연이 없으며 플로우가 생성되는 즉시 flow-create 이벤트가 내보내집니다.

- **{{delay_flow_create_rate_in_secs}}** - 플로우 생성 이벤트 전송 간의 지연 시간(초)을 입력합니다. **55**초 값을 사용하는 것이 좋습니다.

단계 **4** **flow-export active refresh-interval** 명령은 수명이 긴 플로우에 대한 상태 업데이트가 ASA에서 전송되는 빈도를 정의합니다. 유효한 값은 1분~60분입니다. Flow Update Interval(플로우 업데이트 간격) 필드에서 **flow-export active refresh-interval**을 **flow-export delay flow-create** 간격보다 5초 이상 크게 구성하면 flow-update 이벤트가 flow-creation 이벤트보다 먼저 표시되지 않습니다.

- **{{refresh_interval_in_mins}}-1**분 값을 사용하는 것이 좋습니다. 유효한 값은 1분~60분입니다.

---

**What to do next**

SEC로 전송될 NSEL 이벤트를 정의하는 클래스 맵 생성, on page 405를 진행합니다.

## SEC로 전송될 NSEL 이벤트를 정의하는 클래스 맵 생성

매크로의 다음 명령은 클래스의 모든 NSEL 이벤트를 그룹화한 다음 해당 클래스를 SEC(Secure Event Connector)로 내보냅니다. 이 지침은 매크로의 다음 섹션을 참조합니다.

class-map {{flow_export_class_name}}

match {{add_this_traffic_to_class_map}}

**Before you begin**

이는 더 큰 워크플로우의 일부입니다. 시작하기 전에 CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성, on page 402의 내용을 참조하십시오.

---

단계 **1** **class-map** 명령은 SEC로 내보낼 NSEL 트래픽을 식별하는 클래스 맵의 이름을 지정합니다.

- **{{flow-export-class-name}}**- 클래스 맵의 이름을 입력합니다. 이름의 길이는 최대 40자입니다. "class-default"라는 이름 그리고 "_internal" 또는 "_default"로 시작하는 모든 이름은 예약되어 있습니다. 모든 유형의 클래스 맵은 동일한 네임스페이스를 사용하므로, 다른 클래스 맵 유형에서 사용된 이름을 재사용할 수 없습니다.

단계 **2** 클래스 맵과 연결될(일치하는) 트래픽을 식별합니다. **{{add_this_traffic_to_class_map}}**의 값에 대해 다음 옵션 중 하나를 선택합니다.

- **{{add_this_traffic_to_class_map}}** 필드에 **any**를 입력합니다. NSEL 트래픽에 대한 모든 트래픽 유형을 모니터링합니다. **"any"** 값을 사용하는 것이 좋습니다**.**
- **{{add_this_traffic_to_class_map}}** 필드에 **access-list *name-of-access-list***를 입력합니다. 이렇게 하면 생성한 액세스 목록과 연결된 모든 트래픽이 연결됩니다. 자세한 내용은 Cisco ASA NetFlow 구현 가이드에서 모듈러 정책 프레임워크를 통한 플로우 내보내기 구성을 참조하십시오.

---

**What to do next**

NSEL 이벤트에 대한 정책 맵 정의, on page 405를 계속합니다.

## NSEL 이벤트에 대한 정책 맵 정의

이 작업은 이전 작업에서 생성한 클래스에 NetFlow 내보내기 작업을 할당하고 새 정책 맵에 클래스를 할당합니다. 이 지침은 매크로의 다음 섹션을 참조합니다.

policy-map {{global_policy_map_name}}

class {{flow_export_class_name}}

flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}

**Before you begin**

이는 더 큰 워크플로우의 일부입니다. 시작하기 전에 CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성, on page 402의 내용을 참조하십시오.

---

단계 **1** **policy-map** 명령은 policy-map을 생성합니다. 다음 작업에서는 이 정책 맵을 전역 정책과 연결합니다.

- **{{global_policy_map_name}}** - 정책 맵의 이름을 입력합니다. 방화벽의 기존 전역 정책 이름**(**있는 경우**)**을 사용하는 것이 좋습니다. 전역 정책의 기본 이름은 **global_policy**입니다. ASA 전역 정책의 이름 확인을 참조하십시오. Cisco ASA NetFlow 구현 가이드의 Configure Flow-Export Actions Through Modular Policy Framework(모듈형 정책 프레임워크를 통한 플로우 내보내기 작업 구성)에 따라 새 정책 맵을 생성하고 전역적으로 적용하는 경우 나머지 검사 정책은 비활성화됩니다.

단계 **2** **class** 명령은 SEC로 전송될 NSEL 이벤트를 정의하는 클래스 맵 생성, on page 405에서 생성한 클래스 맵의 이름을 상속합니다.

단계 **3** **flow-export event-type** {{event-type}} **destination** {{IPv4_address}} 명령은 플로우 컬렉터(이 경우 SEC)로 전송해야 하는 이벤트 유형을 정의합니다.

- **{{event-type}}** - event_type 키워드는 필터링되는 지원 이벤트의 이름입니다. **"all"** 값을 사용하는 것이 좋습니다.
- **{{SEC_IPv4_address}}** -SEC의 IPv4 주소입니다. 해당 값은 NSEL 메시지의 대상 및 SEC로 전송되는 간격 정의, on page 404에 입력한 값에서 상속됩니다.

---

**What to do next**

중복된 시스템 로그 메시지 비활성화, on page 406를 계속합니다.

중복된 시스템 로그 메시지 비활성화

이 지침은 매크로의 이 섹션을 참조합니다. 명령을 수정할 필요가 없습니다.

logging flow-export-syslogs disable

NetFlow를 활성화하여 플로우 정보를 내보내면 다음 표의 시스템 로그 메시지가 중복됩니다. 동일한 정보를 NetFlow를 통해 내보내므로 성능을 위해 중복 시스템 로그 메시지를 비활성화하는 것이 좋습니다.

**Note** NSEL 및 시스템 로그 메시지가 모두 활성화된 경우 두 로깅 유형 간에 시간순으로 정렬되지 않습니다.

| **Syslog** 메시지 | 설명 | **NSEL** 이벤트 **ID** | **NSEL** 확장 이벤트 **ID** |
|---|---|---|---|
| 106100 | ACL(액세스 제어 규칙)이 발생할 때마다 생성됨 | 1 — 플로우가 생성됨(ACL에서 플로우를 허용한 경우)<br>3 — 플로우가 거부됨(ACL에서 플로우를 거부한 경우) | 0 — ACL이 플로우를 허용한 경우<br>1001 — 인그레스 ACL에서 플로우를 거부함<br>1002 — 이그레스 ACL에서 플로우를 거부함 |
| 106015 | 첫 번째 패킷이 SYN 패킷이 아니므로 TCP 플로우가 거부됨 | 3 — 플로우가 거부됨 | 1004 — 첫 번째 패킷이 TCP SYN 패킷이 아니므로 플로우가 거부됨 |
| 106023 | **access-group** 명령을 통해 인터페이스에 연결된 ACL에서 플로우를 거부한 경우 | 3 — 플로우가 거부됨 | 1001 — 인그레스 ACL에서 플로우를 거부함<br>1002 — 이그레스 ACL에서 플로우를 거부함 |
| 302013, 302015, 302017, 302020 | TCP, UDP, GRE, ICMP 연결 생성 | 1 — 플로우가 생성됨 | 0 — 무시함 |
| 302014, 302016, 302018, 302021 | TCP, UDP, GRE, ICMP 연결 해체 | 2 — 플로우가 삭제됨 | 0 — 무시함<br>>2000 — 플로우가 해체됨 |
| 313001 | 디바이스에 대한 ICMP 패킷이 거부됨 | 3 — 플로우가 거부됨 | 1003 — 구성으로 인해 To-the-box 플로우가 거부됨 |
| 313008 | 디바이스에 대한 ICMP v6 패킷이 거부됨 | 3 — 플로우가 거부됨 | 1003 — 구성으로 인해 To-the-box 플로우가 거부됨 |
| 710003 | 디바이스 인터페이스에 대한 연결 시도가 거부됨 | 3 — 플로우가 거부됨 | 1003 — 구성으로 인해 To-the-box 플로우가 거부됨 |

중복 시스템 로그 메시지를 비활성화하지 않으려면 이 매크로를 편집하고 이 줄만 삭제할 수 있습니다.

**logging flow-export-syslogs disable**

NetFlow 관련 시스템 로그 메시지 비활성화 및 다시 활성화의 절차에 따라 나중에 개별 시스템 로그 메시지를 활성화하거나 비활성화할 수 있습니다.

## ASA 전역 정책의 이름 확인

ASA의 전역 정책 이름을 확인하려면 다음 절차를 수행합니다.

단계 **1** Devices & Services(디바이스 및 서비스) 페이지에서 전역 정책의 이름을 찾을 디바이스를 선택합니다.

단계 **2** Device Actions(디바이스 작업) 창에서 **>_Command Reference(**명령 참조**)**를 선택합니다.

단계 **3** Command Line Interface(명령줄 인터페이스) 창의 프롬프트에 다음을 입력합니다.

**show running-config service-policy**

아래 예의 출력에서 global_policy는 전역 정책의 이름입니다.

예:

> **show running-config service-policy**

**service-policy global_policy global**

# ASA 이벤트 유형

이벤트 로깅 페이지에서 이벤트 검색 및 필터링할 때 이벤트 유형 목록에서 선택할 수 있습니다. 이러한 이벤트 유형은 시스템 로그 ID의 그룹을 나타냅니다. 아래 표는 어떤 시스템 로그 ID가 어떤 ASA 이벤트 유형에 포함되어 있는지 보여줍니다. 특정 시스템 로그 ID에 대해 자세히 알아보려면 Cisco ASA 시리즈 시스템 로그 메시지 가이드에서 검색할 수 있습니다.

일부 시스템 로그 이벤트에는 추가 속성 "EventName"이 있습니다. attribute:value 쌍을 기준으로 필터링하여 EventName 특성을 사용하여 이벤트 테이블을 필터링하여 찾을 수 있습니다. Syslog 이벤트에 대한 이벤트 이름 속성을 참조하십시오.

일부 시스템 로그 이벤트에는 추가 속성 "EventGroup" 및 "EventGroupDefinition"이 있습니다. attribute:value 쌍을 기준으로 필터링하여 이러한 추가 속성을 사용하여 이벤트 테이블을 필터링할 수 있습니다. 일부 시스템 로그 메시지에 대한 EventGroup 및 EventGroupDefinition 속성을 참조하십시오.

ASA 디바이스용 NetFlow Secure Event Logging(NSEL) 는 시스템 로그 이벤트와 다릅니다. NetFlow 필터는 NSEL 레코드를 생성한 모든 NetFlow 이벤트 ID를 검색합니다. 이러한 NetFlow 이벤트 ID는 Cisco ASA NetFlow 구현 가이드에 정의되어 있습니다.

| 필터 이름 | 해당 시스템 로그 이벤트 또는 **NetFlow** 이벤트 |
|---|---|
| AAA | 109001-109035<br>113001-113027 |
| 봇넷 | 338001-338310 |

| 필터 이름 | 해당 시스템 로그 이벤트 또는 **NetFlow** 이벤트 |
|---|---|
| 장애 조치 | 101001-101005, 102001, 103001-103007, 104001-104004, 105001-105048<br>210001-210022<br>311001-311004<br>709001-709007 |
| 방화벽 거부됨 | 106001, 106007, 106012, 106013, 106015, 106016, 106017, 106020, 106021, 106022, 106023, 106025, 106027<br>방화벽 거부됨 이벤트는 NetFlow에 포함될 수 있으며 NetFlow 이벤트 ID 및 시스템 로그 ID와 함께 보고될 수 있습니다. |
| 방화벽 트래픽 | 106001-106100, 108001-108007, 110002-110003<br>201002-201013, 209003-209005, 215001<br>302002-302304, 302022-302027, 303002-303005, 313001-313008, 317001-317006, 324000-324301, 337001-337009<br>400001-400050, 401001-401005, 406001-406003, 407001-407003, 408001-408003, 415001-415020, 416001, 418001-418002, 419001-419003, 424001-424002, 431001-431002, 450001<br>500001-500005, 508001-508002<br>607001-607003, 608001-608005, 609001-609002, 616001<br>703001-703003, 726001<br>방화벽 트래픽 이벤트는 NetFlow에 포함될 수 있으며 NetFlow 이벤트 ID 및 시스템 로그 ID와 함께 보고될 수 있습니다. |
| IPsec VPN | 402001-402148, 602102-602305, 702304-702307 |
| NAT | 201002-201013, 202001-202011, 305005-305012 |
| SSL VPN | 716001-716060, 722001-722053, 723001-723014, 724001-724004, 725001-725015 |
| NetFlow | 0, 1, 2, 3, 5 |

관련 정보:

- 일부 시스템 로그 메시지에 대한 EventGroup 및 EventGroupDefinition 속성, 479 페이지
- Syslog 이벤트에 대한 이벤트 이름 속성

# 구문 분석된 **Secure Firewall Cloud Native** 시스템 로그 이벤트

구문 분석된 시스템 로그 이벤트는 다른 시스템 로그 이벤트보다 더 많은 이벤트 속성을 포함하며, 구문 분석된 특정 필드에서 검색할 수 있습니다. SEC는 사용자가 지정한 모든 Secure Firewall Cloud Native 이벤트를 Cisco Cloud에 전달하지만 아래 표의 시스템 로그 메시지만 구문 분석됩니다. 구문 분석된 모든 시스템 로그 이벤트는 식별을 돕기 위해 이탤릭체로 표시됩니다.

| 시스템 로그 **ID** | 시스템 로그 범주 | 시스템 로그 메시지의 목적 |
|---|---|---|
| 106015 | 방화벽 | 상태가 잘못된 TCP 거부를 나타냅니다. |
| 106023 | 방화벽 | 실제 IP 패킷이 ACL에 의해 거부되었습니다. 이 메시지는 ACL에 대해 로그 옵션을 활성화하지 않은 경우에도 나타납니다. |
| 106100 | 액세스 목록/사용자 세션 | 패킷이 ACL에 의해 허용되거나 거부되었습니다. |
| 113019 | 사용자 인증 | 중요 AnyConnect |
| 302013, 302015, 302017, 302020 | 사용자 세션 | TCP, UDP, GRE 및 ICMP 연결 생성을 위한 연결 시작 및 종료 Syslog. |
| 302014, 302016, 302018, 302021 | 사용자 세션 | TCP, UDP, GRE 및 ICMP 연결 생성을 위한 연결 시작 및 종료 Syslog. |
| 302020 - 302021 | 사용자 세션 | ICMP 세션 설정 및 해제. |
| 305006 | 사용자 세션/NAT 및 PAT | NAT 연결 실패 |
| 305011-305014 | 사용자 세션/NAT 및 PAT | NAT 빌드/해체 관련 |
| 313001, 313008 | IP 스택 | 상자에 거부된 연결을 나타냅니다. |
| 414004 | 시스템 | 중요 AnyConnect |
| 609001 - 609002 | 방화벽 | 영역에 연결된 호스트 **ip-address**에 대해 네트워크 상태 컨테이너가 예약/제거되었습니다. |
| 710002,710004 710005 | 사용자 세션 | 상자 연결 실패 |
| 710003 | 사용자 세션 | 상자에 거부된 연결을 나타냅니다. |

| 시스템 로그 ID | 시스템 로그 범주 | 시스템 로그 메시지의 목적 |
|---|---|---|
| 746012, 746013 | 사용자 세션 | 중요 AnyConnect |

# SaaS(Secure Logging Analytics)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기

SaaS(Secure Logging Analytics)를 사용하면 ASA 또는 FDM 관리 디바이스에서 SEC(Secure Event Connector)의 특정 UDP, TCP 또는 NSEL 포트로 이벤트를 보낼 수 있습니다. 그런 다음 SEC는 해당 이벤트를 Cisco 클라우드로 전달합니다.

이러한 포트가 아직 사용 중이 아닌 경우, SEC는 이벤트를 수신하는 데 포트를 제공하며, SaaS(Secure Logging Analytics) 설명서에서는 기능을 구성할 때 포트 사용을 권장합니다.

- TCP: 10125
- UDP: 10025
- NSEL: 10425

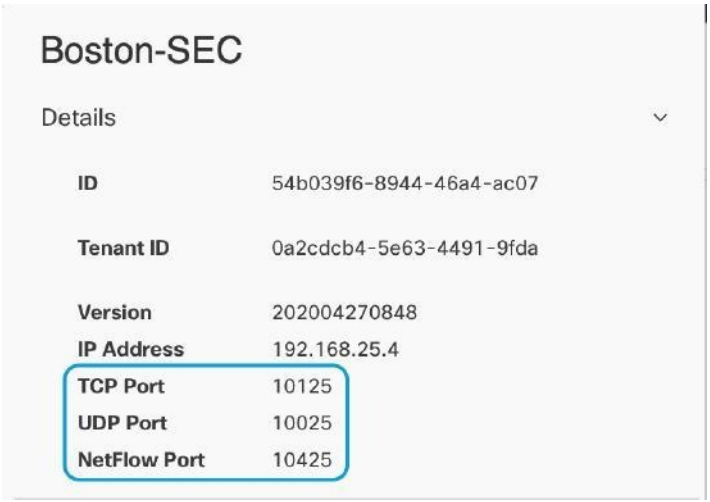
이러한 포트가 이미 사용 중인 경우 SaaS(Secure Logging Analytics)를 구성하기 전에 SEC 디바이스 세부 정보를 확인하여 실제로 이벤트를 수신하는 데 사용 중인 포트를 확인합니다.

SEC에서 사용하는 포트 번호를 찾으려면 다음을 수행합니다.

단계 **1** CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.

단계 **2** Secure Connector(보안 커넥터) 페이지에서 이벤트를 전송할 SEC를 선택합니다.

단계 **3** Details(세부 정보) 창에 이벤트를 전송해야 하는 TCP, UDP 및 NetFlow(NSEL) 포트가 표시됩니다.



# 보안 이벤트 커넥터

SEC(Secure Event Connector)는 보안 분석 및 로깅 SaaS 솔루션의 구성 요소입니다. ASA 및 FDM 관리 디바이스에서 이벤트를 수신하여 Cisco Cloud에 전달합니다. CDO는 관리자가 해당 페이지에서 또는 Cisco Secure Cloud Analytics를 사용하여 이벤트를 분석할 수 있도록 Event Logging(이벤트 로깅) 페이지에 이벤트를 표시합니다.

SEC는 네트워크 또는 AWS Virtual Private Cloud(VPC)에 구축된 보안 디바이스 커넥터 또는 네트워크에 구축된 자체 CDO 커넥터 가상 머신에 설치됩니다.

### 보안 이벤트 커넥터 ID

Cisco TAC(Technical Assistance Center) 또는 기타 CDO 지원과 협력할 때는 SEC의 ID가 필요할 수 있습니다. 이 ID는 CDO의 Secure Connector(보안 커넥터) 페이지에 있습니다. SEC ID를 찾으려면 다음을 수행합니다.

1. 왼쪽의 CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.
2. 식별할 SEC를 클릭합니다.
3. SEC ID는 Details(세부 정보) 창의 Tenant ID(테넌트 ID) 위에 나열되는 ID입니다.

관련 정보:

- ASA에 대한 SAL SaaS(Security Analytics and Logging) 정보
- SDC 가상 머신에 SEC(Secure Event Connector) 설치, 438 페이지
- VM 이미지를 사용하여 SEC 설치
- VM 이미지를 사용하여 SEC 설치
- Terraform 모듈을 사용하여 AWS VPC에 보안 이벤트 커넥터 설치, 455 페이지
- 보안 이벤트 커넥터 제거
- Cisco Security Analytics and Logging(SaaS) 프로비저닝

# 보안 이벤트 커넥터 설치

SEC(보안 이벤트 커넥터)는 SDC가 있거나 없는 테넌트에 설치할 수 있습니다.

보안 디바이스 커넥터(있는 경우)와 동일한 가상 머신에 하나의 SEC를 설치할 수 있습니다. 또는 네트워크에서 유지 관리하는 자체 CDO 커넥터 가상 머신에 SEC를 설치할 수 있습니다.

다양한 설치 사례를 설명하는 다음 항목을 참조하십시오.

- VM 이미지를 사용하여 SEC 설치, 446 페이지
- CDO 이미지를 사용하여 SEC 설치, 441 페이지

• Terraform 모듈을 사용하여 AWS VPC에 보안 이벤트 커넥터 설치, 455 페이지

# SDC 가상 머신에 SEC(Secure Event Connector) 설치

SEC(Secure Event Connector)는 ASA 및 FDM 관리 디바이스에서 이벤트를 수신하여 Cisco Cloud에 전달합니다. CDO는 관리자가 해당 페이지에서 또는 Cisco Secure Cloud Analytics를 사용하여 이벤트를 분석할 수 있도록 Event Logging(이벤트 로깅) 페이지에 이벤트를 표시합니다.

보안 디바이스 커넥터(있는 경우)와 동일한 가상 머신에 하나의 SEC를 설치할 수 있습니다. 또는 네트워크에서 유지 관리하는 자체 CDO 커넥터 가상 머신에 SEC를 설치할 수 있습니다.

이 문서에서는 SDC와 동일한 가상 머신에 SEC를 설치하는 방법을 설명합니다. 더 많은 SEC를 설치하려면 CDO 이미지를 사용하여 SEC 설치, 441 페이지 또는 VM 이미지를 사용하여 SEC 설치, 446 페이지의 내용을 참조하십시오.

시작하기 전에

- Cisco Security and Analytics 로깅, 로깅 및 트러블슈팅 라이선스를 구매합니다. 또는 Cisco Security and Analytics 로그아웃을 먼저 시도하려면 CDO에 로그인하고 기본 탐색 모음에서 분석 > 이벤트 로깅를 선택하고 **Request Trial(**평가판 요청**)**을 클릭합니다. 또한 **Logging Analytics and Detection(**로깅 분석 및 탐지**)** 및 **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스를 구매하여 Secure Cloud Analytics를 이벤트에 적용할 수 있습니다.
- SDC가 설치되었는지 확인합니다. SDC를 설치해야 하는 경우 다음 절차 중 하나를 수행합니다.
  - CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축
  - 자체 VM에 보안 디바이스 커넥터 구축

참고 자체 VM에 온프레미스 SDC를 설치한 경우 이벤트가 SDC에 도달하도록 허용하려면 생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성이 필요합니다.

- SDC가 CDO와 통신하는지 확인합니다.
  1. CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.
  2. SDC의 마지막 하트비트가 SEC 설치 전 10분 미만이었으며 SDC의 상태가 활성인지 확인합니다.
- 시스템 요구 사항 - SDC를 실행하는 가상 머신에 추가 CPU 및 메모리를 할당합니다.
  - CPU: 총 6개의 CPU를 만들기 위해 SEC를 수용할 수 있도록 추가로 4개의 CPU를 할당합니다.
  - 메모리: 총 10GB의 메모리를 만들려면 SEC에 8GB의 메모리를 추가로 할당합니다.

SEC를 수용하도록 VM의 CPU와 메모리를 업데이트한 후 VM의 전원을 켜고 Secure Connector(보안 커넥터) 페이지에 SDC가 "Active(활성)" 상태로 표시되는지 확인합니다.

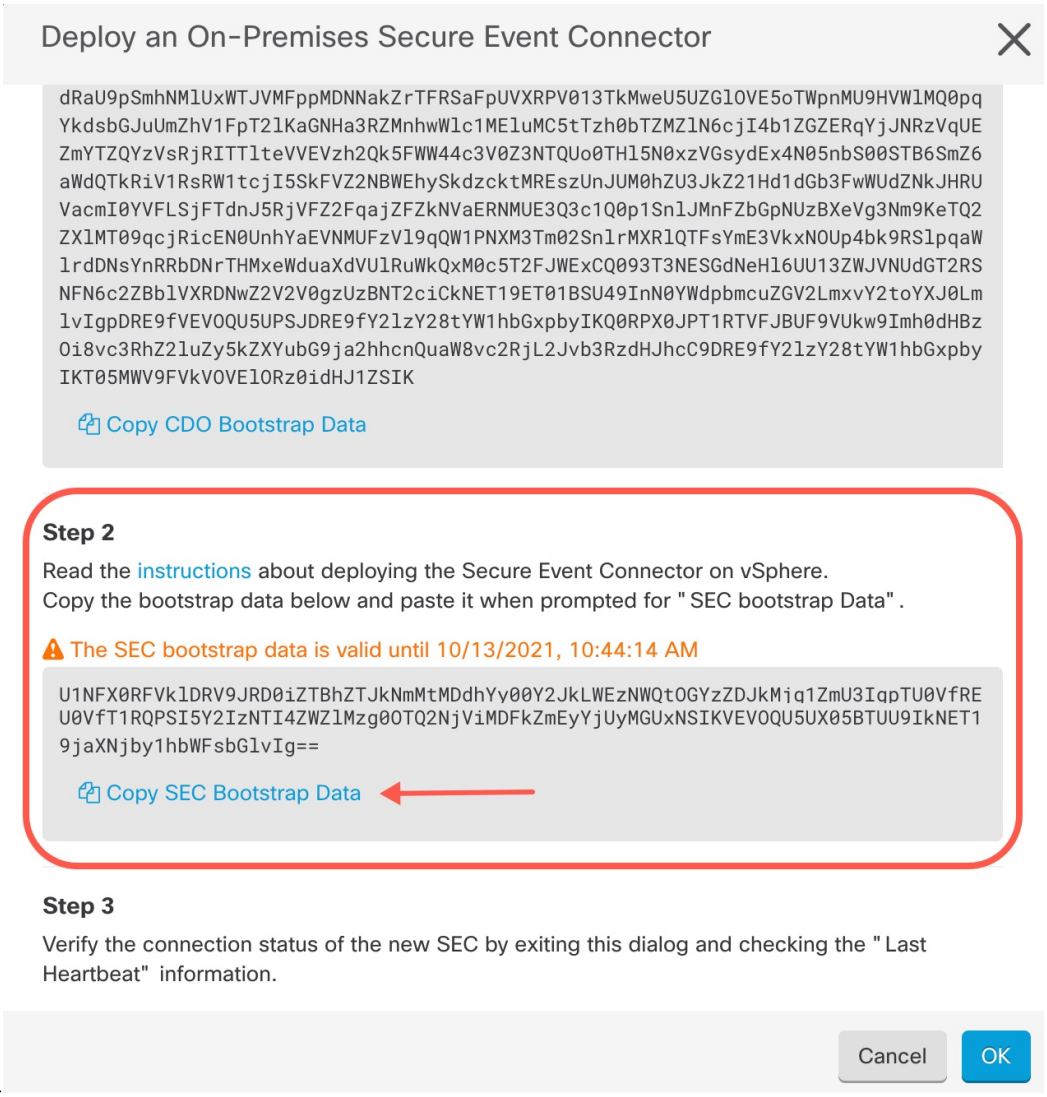
---

단계 **1** CDO에 로그인합니다.

단계 **2** CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.

단계 **3** 파란색 더하기 버튼을 클릭하고 **Secure Event Connector(**보안 이벤트 커넥터**)**를 클릭합니다.

단계 **4** 마법사의 1단계를 건너뛰고 2단계로 이동합니다. 마법사 2단계에서 링크를 클릭하여 **SEC** 부트스트랩 데이터를 복사합니다.




사합니다.

단계 **5** 터미널 창을 열고 SDC에 "cdo" 사용자로 로그인합니다.

단계 **6** 로그인한 후에는 "sdc" 사용자로 전환합니다. 암호를 묻는 메시지가 표시되면 "cdo" 사용자의 암호를 입력합니다. 다음은 이러한 명령의 예입니다.

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

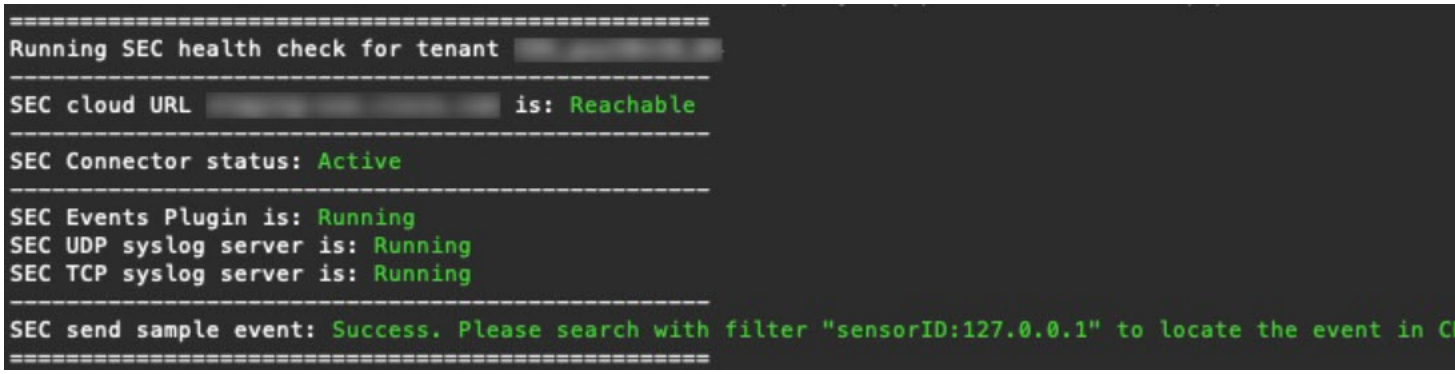
단계 **7** 프롬프트에서 **sec.sh** 설정 스크립트를 실행합니다.

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

단계 **8** 프롬프트 끝에 4단계에서 복사한 부트스트랩 데이터를 붙여넣고 **Enter** 키를 누릅니다.

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

SEC가 온보딩되면 sec.sh는 SEC의 상태를 확인하는 스크립트를 실행합니다. 모든 상태 확인이 "녹색"인 경우 상태 확인은 이벤트 로그에 샘플 이벤트를 전송합니다. 샘플 이벤트는 이벤트 로그에 "sec-health-check"라는 정책으로 표시됩니다.




등록에 실패했거나 SEC 온 보딩에 실패했다는 메시지가 표시되면 SEC 온보딩 실패 문제 해결로 이동하십시오.

단계 **9** SDC 및 SEC가 실행 중인 VM에 추가 구성이 필요한지 확인합니다.

- 자체 가상 머신에 SDC를 설치한 경우 생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성, 452 페이지을 계속 진행합니다.
- CDO 이미지를 사용하여 SDC를 설치한 경우 "다음 작업"을 진행합니다.

---

다음에 수행할 작업

ASA 디바이스에 대한 SaaS(Secure Logging Analytics) 구현, 389 페이지 으로 돌아갑니다.

관련 정보:

- 보안 디바이스 커넥터 문제 해결, 553 페이지
- 보안 이벤트 커넥터 문제 해결
- SEC 온보딩 실패 문제 해결
- 보안 이벤트 커넥터 등록 실패 문제 해결, 561 페이지

# CDO 이미지를 사용하여 SEC 설치

SEC(보안 이벤트 커넥터)는 ASA 및 FTD에서 Cisco cloud로 이벤트를 전달하므로 라이선스에 따라 Event Logging 페이지에서 이벤트를 보고 Secure Cloud Analytics로 조사할 수 있습니다.

테넌트에 두 개 이상의 SEC(보안 이벤트 커넥터)를 설치하고ASAs 및 FDM 관리 디바이스의 이벤트를 설치한 SEC로 보낼 수 있습니다. 여러 SEC를 사용하면 서로 다른 위치에 SEC를 설치하고 Cisco Cloud에 이벤트를 전송하는 작업을 배포할 수 있습니다.

SEC 설치는 2단계로 진행됩니다.

1. CDO VM 이미지를 사용하여 보안 이벤트 커넥터를 지원하기 위한 CDO 커넥터 설치, 441 페이지 설치하는 모든 SEC에 대해 하나의 CDO 커넥터가 필요합니다. CDO 커넥터는 SDC(보안 디바이스 커넥터)와 다릅니다.
2. CDO 커넥터 가상 머신에 보안 이벤트 커넥터 설치, 453 페이지.

참고 고유한 VM을 생성하여 CDO 커넥터를 생성하려면 생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성를 참조하십시오.

다음 작업:

CDO VM 이미지를 사용하여 보안 이벤트 커넥터를 지원하기 위한 CDO 커넥터 설치, 441 페이지를 계속 진행합니다.

## CDO VM 이미지를 사용하여 보안 이벤트 커넥터를 지원하기 위한 CDO 커넥터 설치

시작하기 전에

- Cisco Security and Analytics Logging, **Logging and Troubleshooting(**로깅 및 문제 해결**)** 라이선스를 구매하고, **Logging Analytics and Detection(**로깅 분석 및 탐지**)**, **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스를 구매하여 Secure Cloud Analytics를 이벤트에 적용할 수도 있습니다.

  원하는 경우 CDO에 로그인하여 Security Analytics and Logging(보안 분석 및 로깅) 평가판을 요청하고 기본 내비게이션 바에서 분석 > 이벤트 로깅을 선택하고 **Request Trial(**평가판 요청**)**을 클릭합니다.

- CDO는 엄격한 인증서 확인이 필요하며 CDO 커넥터와 인터넷 간의 웹/콘텐츠 프록시 검사를 지원하지 않습니다. 프록시 서버를 사용하는 경우 CDO 커넥터와 CDO 간의 트래픽 검사를 비활성화합니다.
- 이 프로세스에서 설치된 **CDO** 커넥터는 **TCP** 포트 **443**에서 인터넷에 대한 전체 아웃바운드 액세스 권한을 가져야 합니다**.**
- 매니지드 디바이스에 Cisco Defense Orchestrator 연결를 검토하여 **CDO** 커넥터에 대한 적절한 네트워크 액세스를 확인합니다.

- CDO는 vSphere 웹 클라이언트 또는 ESXi 웹 클라이언트를 사용한 CDO 커넥터 VM OVF 이미지 설치를 지원합니다.
- CDO는 VM vSphere 데스크톱 클라이언트를 사용한 CDO 커넥터 VM OVF 이미지 설치를 지원하지 않습니다.
- ESXi 5.1 하이퍼바이저.
- CDO 커넥터 및 SEC만 호스팅하는 VM의 시스템 요구 사항:
  - VMware ESXi 호스트에는 vCPU 4개가 필요합니다.
  - VMware ESXi 호스트에는 최소 8GB의 메모리가 필요합니다.
  - VMware ESXi에는 프로비저닝 선택에 따라 가상 머신을 지원하기 위해 64GB의 디스크 공간이 필요합니다.
- 설치를 시작하기 전에 다음 정보를 수집하십시오.
  - CDO 커넥터 VM에 사용할 고정 IP 주소.
  - 설치 프로세스 중 생성하는 **root** 및 **cdo** 사용자의 비밀번호.
  - 조직에서 사용하는 DNS 서버의 IP 주소
  - SDC 주소가 있는 네트워크의 게이트웨이 IP 주소
  - 시간 서버의 FQDN 또는 IP 주소.
- CDO 커넥터 가상 머신은 보안 패치를 정기적으로 설치하도록 구성되며, 이를 위해서는 포트 80 아웃바운드를 열어야 합니다.

---

단계 **1** CDO 커넥터를 생성할 CDO 테넌트에 로그온합니다.

단계 **2** CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.

단계 **3** 파란색 더하기 버튼을 클릭하고 **Secure Event Connector(**보안 이벤트 커넥터**)**를 클릭합니다.


단계 **4** 1단계에서 **Download the CDO Connector VM image(CDO** 커넥터 **VM** 이미지 다운로드**)**를 클릭합니다. 이는 SEC를 설치하는 특수 이미지입니다. 최신 이미지를 사용하려면 항상 CDO 커넥터 VM을 다운로드하십시오.


단계 **5** .zip 파일의 모든 파일을 추출합니다. 다음과 같이 표시됩니다.

- CDO-SDC-VM-ddd50fa.ovf
- CDO-SDC-VM-ddd50fa.mf
- CDO-SDC-VM-ddd50fa-disk1.vmdk

단계 **6** vSphere 웹 클라이언트를 사용하여 VMware 서버에 관리자로 로그인합니다.

참고 VM vSphere 데스크톱 클라이언트를 사용하지 마십시오.

단계 **7** 지시에 따라 OVF 템플릿에서 온프레미스 CDO 커넥터 가상 머신을 구축합니다. (템플릿을 구축하려면 .ovf, .mf 및 .vdk 파일이 필요합니다.)

단계 **8** 설정이 완료되면 VM의 전원을 켭니다.

단계 **9** 새 CDO 커넥터 VM의 콘솔을 엽니다.

단계 **10** **cdo** 사용자로 로그인합니다. 기본 암호는 `adm123`입니다.

단계 **11** 프롬프트에 `sudo sdc-onboard setup`을 입력합니다.

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

단계 **12** 프롬프트가 표시되면 cdo 사용자의 기본 비밀번호 `adm123`을 입력합니다.

단계 **13** 지시에 따라 **root** 사용자의 새 암호를 생성합니다.

단계 **14** 지시에 따라 **cdo** 사용자의 새 암호를 생성합니다.

단계 **15** 지시에 따라 Cisco Defense Orchestrator 도메인 정보를 입력합니다.

단계 **16** CDO 커넥터 VM에 사용할 고정 IP 주소를 입력합니다.

단계 **17** CDO 커넥터 VM이 설치된 네트워크의 게이트웨이 IP 주소를 입력합니다.

단계 **18** CDO 커넥터의 NTP 서버 주소 또는 FQDN을 입력합니다.

단계 **19** Docker 브리지 정보를 묻는 프롬프트가 표시되면 정보를 입력하거나 해당되지 않는 경우 비워두고 <Enter> 키를 누릅니다.

단계 **20** 입력을 확인합니다.

단계 **21** "지금 SDC를 설정하시겠습니까?"라는 프롬프트가 나타나면 **n**을 입력합니다.

단계 **22** **cdo** 사용자로 로그인하여 CDO 커넥터에 대한 SSH 연결을 생성합니다.

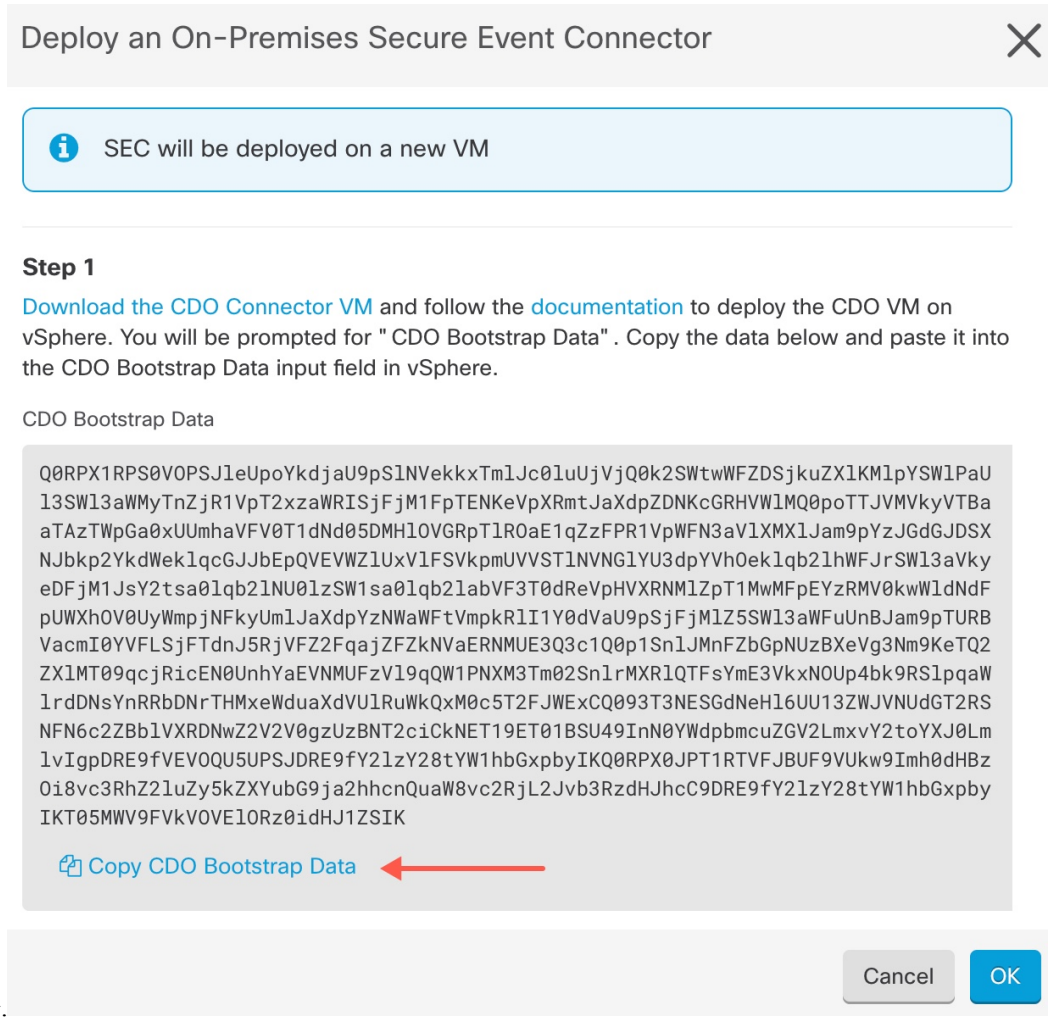
단계 **23** 프롬프트에 **`sudo sdc-onboard bootstrap`**을 입력합니다.

```
[cdo@localhost ~]$ sudo sdc-onboard bootstrap
```

단계 **24** 프롬프트가 표시되면 cdo 사용자의 비밀번호를 입력합니다.

단계 **25** 프롬프트가 표시되면 CDO로 돌아가 CDO 부트스트랩 데이터를 복사한 다음 SSH 세션에 붙여넣습니다. CDO 부트스트랩 데이터를 복사하려면 다음을 수행합니다.

1. CDO에 로그인합니다.
2. CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.
3. 온보딩을 시작한 보안 이벤트 커넥터를 선택합니다. 상태가 "Onboarding(온보딩)"으로 표시되어야 합니다.
4. Actions(작업) 창에서 **Deploy an On-Premises Secure Event Connector(**온프레미스 보안 디바이스 커넥터 구축**)**를 클릭합니다.
5. 대화 상자의 1단계에서 CDO 부트스트랩 데이터를 복사합니




다.

단계 **26** 이 설정을 업데이트하시겠습니까**?**라는메시지가 표시되면 **n**을 입력합니다.

단계 **27** CDO의 Deploy an On-Premises Secure Event Connector(온프레미스 보안 이벤트 커넥터 구축) 대화 상자로 돌아가 **OK(**확인**)**를 클릭합니다. Secure Connector(보안 커넥터) 페이지에서 Secure Event Connector(보안 이벤트 커넥터)가 노란색 Onboarding(온보딩) 상태로 표시됩니다.

---

다음에 수행할 작업

CDO 커넥터 VM에 보안 이벤트 커넥터 설치, 445 페이지를 진행합니다.

## CDO 커넥터 VM에 보안 이벤트 커넥터 설치

시작하기 전에

CDO VM 이미지를 사용하여 보안 이벤트 커넥터를 지원하기 위한 CDO 커넥터 설치, 441 페이지에 설명된 대로 CDO 커넥터 VM을 설치해야 합니다.

---

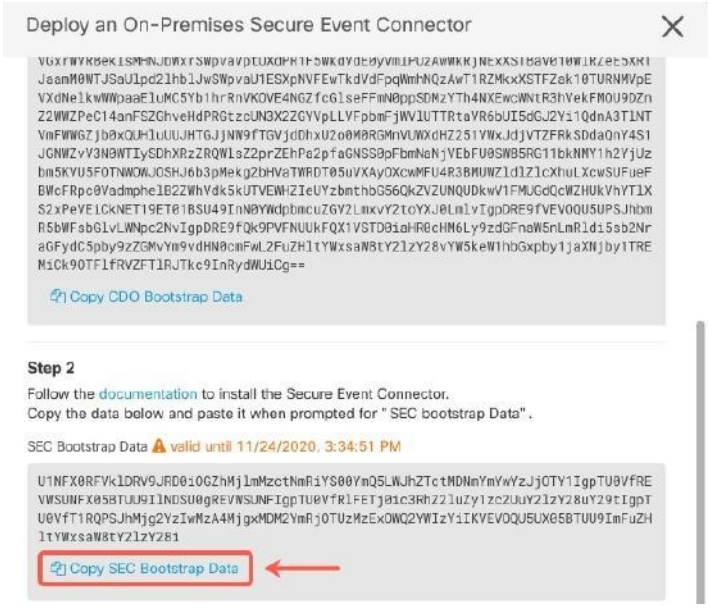
단계 **1** CDO에 로그인합니다.

단계 **2** CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.

단계 **3** 위에서 온보딩한 CDO 커넥터를 선택합니다. Secure Connector(보안 커넥터) 테이블에서는 이를 보안 이벤트 커넥터(보안 이벤트 커넥터)라고 하며 여전히 "Onboading(온보딩)" 상태여야 합니다.

단계 **4** 오른쪽의 작업 창에서 **Deploy an On-Premises Secure Event Connector(**온프레미스 보안 디바이스 커넥터 구축**)**를 클릭합니다.

단계 **5** 마법사 **2**단계에서 링크를 클릭하여 **SEC** 부트스트랩 데이터를 복사합니다.




단계 **6** CDO 커넥터에 대한 SSH 연결을 생성하고 **cdo** 사용자로 로그인합니다.

단계 **7** 로그인한 후에는 **sdc** 사용자로 전환합니다. 암호를 묻는 메시지가 표시되면 "cdo" 사용자의 암호를 입력합니다. 다음은 이러한 명령의 예입니다.

```
[cdo@sdc-vm ~]$ sudo su sdc
 [sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

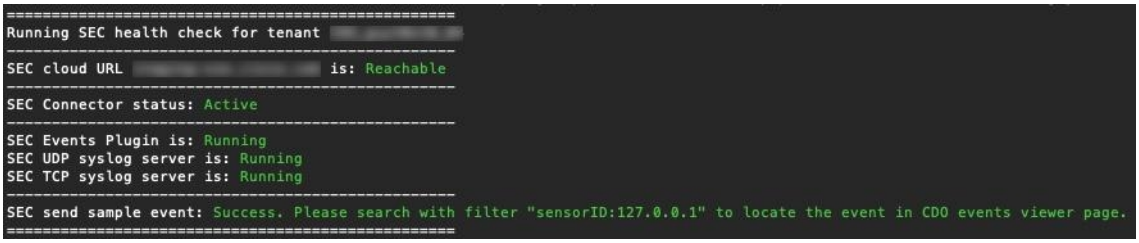
단계 **8** 프롬프트에서 sec.sh 설정 스크립트를 실행합니다.

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

단계 **9** 프롬프트 끝에 4단계에서 복사한 부트스트랩 데이터를 붙여넣고 **Enter** 키를 누릅니다.

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
 RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

SEC가 온보딩되면 sec.sh는 SEC의 상태를 확인하는 스크립트를 실행합니다. 모든 상태 확인이 "녹색"인 경우 상태 확인은 이벤트 로그에 샘플 이벤트를 전송합니다. 샘플 이벤트는 이벤트 로그에 "sec-health-check"라는 정책으로 표시됩니다.




등록에 실패했거나 SEC 온 보딩에 실패했다는 메시지가 표시되면 SEC 온보딩 실패 문제 해결, 558 페이지로 이동하십시오.

성공 메시지가 표시되면 CDO로 돌아가고 **Deploy on-Premise Secure Event Connector(**온프레미스 보안 이벤트 커넥터 구축**)** 대화 상자에서 Done(완료)를 클릭합니다.

단계 **10** "**What to do next(**다음 작업**)**로 계속합니다."

---

다음에 수행할 작업

ASA 디바이스에 대한 SaaS(Secure Logging Analytics) 구현, 389 페이지 으로 돌아갑니다.

관련 정보**:**

- 보안 디바이스 커넥터 문제 해결, 553 페이지
- 보안 이벤트 커넥터 문제 해결, 558 페이지
- SEC 온보딩 실패 문제 해결, 558 페이지

# VM 이미지를 사용하여 SEC 설치

SEC(보안 이벤트 커넥터)는 ASA 및 FTD에서 Cisco cloud로 이벤트를 전달하므로 라이선스에 따라 Event Logging 페이지에서 이벤트를 보고 Secure Cloud Analytics로 조사할 수 있습니다.

테넌트에 두 개 이상의 SEC(보안 이벤트 커넥터)를 설치하고 ASA 및 FDM 매니지드 디바이스의 이벤트를 설치한 SEC로 보낼 수 있습니다. 여러 SEC를 사용하면 서로 다른 위치에 SEC를 설치하고 Cisco Cloud에 이벤트를 전송하는 작업을 배포할 수 있습니다.

자체 VM 이미지를 사용하여 여러 SEC를 설치하는 작업은 3단계로 진행됩니다. 다음 각 단계를 수행해야 합니다.

1. VM 이미지를 사용하여 SEC를 지원하도록 CDO 커넥터 설치, 447 페이지
2. 생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성, 452 페이지를 사용하여 VM에 대한 몇 가지 추가 구성 단계를 수행합니다.
3. CDO 커넥터 가상 머신에 보안 이벤트 커넥터 설치

참고 CDO 커넥터용 CDO VM 이미지를 사용하는 것이 가장 쉽고 정확하며 선호되는 CDO 커넥터 설치 방법입니다. 이 방법을 사용하려면 CDO 이미지를 사용하여 SEC 설치, 441 페이지의 내용을 참조하십시오.

다음 작업:

VM 이미지를 사용하여 SEC를 지원하도록 CDO 커넥터 설치, 447 페이지를 계속합니다.

## VM 이미지를 사용하여 SEC를 지원하도록 CDO 커넥터 설치

CDO 커넥터 VM은 SEC를 설치하는 가상 머신입니다. CDO 커넥터의 목적은 Cisco SaaS(Security Analytics and Logging) 고객을 위한 SEC를 지원하는 것입니다.

시작하기 전에

- Cisco Security and Analytics Logging, **Logging and Troubleshooting(**로깅 및 문제 해결**)** 라이선스를 구매하고, **Logging Analytics and Detection(**로깅 분석 및 탐지**)**, **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스를 구매하여 Secure Cloud Analytics를 이벤트에 적용할 수도 있습니다.

  원하는 경우 CDO에 로그인하여 Security Analytics and Logging(보안 분석 및 로깅) 평가판을 요청하고 기본 탐색 모음에서 분석 > 이벤트 로깅을 선택하고 **Request Trial(**평가판 요청**)**를 클릭합니다.
- CDO는 엄격한 인증서 확인이 필요하며 CDO 커넥터와 인터넷 간의 웹/콘텐츠 프록시를 지원하지 않습니다.
- **CDO** 커넥터는 **TCP** 포트 **443**에서 인터넷에 대한 전체 아웃바운드 액세스 권한을 가져야 합니다**.**
- 매니지드 디바이스에 Cisco Defense Orchestrator 연결을 검토하여 **CDO** 커넥터에 대한 적절한 네트워크 액세스를 확인합니다**.**
- vCenter 웹 클라이언트 또는 ESXi 웹 클라이언트와 함께 설치된 VMware ESXi 호스트

참고 vSphere 데스크톱 클라이언트를 사용한 설치는 지원되지 않습니다.

- ESXi 5.1 하이퍼바이저.
- Cent OS 7 게스트 운영체제.
- CDO 커넥터 및 SEC만 호스팅하는 VM의 시스템 요구 사항:
  - CPU: SEC를 수용할 수 있도록 4개의 CPU를 할당합니다.
  - 메모리: SEC에 대해 8GB의 메모리를 할당합니다.
  - 디스크 공간: 64GB
- 이 절차를 수행하는 사용자는 Linux 환경에서 작업하고 파일 편집을 위해 **vi** 시각적 편집기를 사용하는 데 익숙해야 합니다.
- CentOS 가상 머신에 CDO Connector를 설치하는 경우 정기적으로 Yum 보안 패치를 설치하는 것이 좋습니다. Yum 구성에 따라 Yum 업데이트를 가져오려면 포트 80 및 443에서 아웃바운드 액세스를 열어야 할 수 있습니다. 또한 업데이트를 예약하려면 yum-cron 또는 crontab을 구성해야 합니다. 보안 운영 팀과 함께 Yum 업데이트를 받기 위해 변경해야 하는 보안 정책이 있는지 확인합니다.
- 설치를 시작하기 전에 다음 정보를 수집하십시오.
  - CDO 커넥터에 사용할 고정 IP 주소.
  - 설치 프로세스 중 생성하는 **root** 및 **cdo** 사용자의 비밀번호.
  - 조직에서 사용하는 DNS 서버의 IP 주소
  - CDO 커넥터 주소가 있는 네트워크의 게이트웨이 IP 주소
  - 시간 서버의 FQDN 또는 IP 주소.
- CDO 커넥터 가상 머신은 보안 패치를 정기적으로 설치하도록 구성되며, 이를 위해서는 포트 80 아웃바운드를 열어야 합니다.
- 시작하기 전에: 이 절차의 명령을 복사하여 터미널 창에 붙여넣지 말고 대신 입력하십시오. 일부 명령에는 "n-대시"가 포함되며, 잘라내기 및 붙여넣기 프로세스에서 이러한 명령은 "m-대시"로 적용되어 명령이 실패할 수 있습니다.

단계 **1** 보안 디바이스 커넥터 페이지에서 파란색 플러스 버튼  을 클릭하고 보안 이벤트 커넥터(보안 이벤트 커넥터)를 클릭합니다.

단계 **2** 제공된 링크를 사용하여 "Deploy an On-Premises 보안 이벤트 커넥터(온프레미스 보안 이벤트 커넥터 배포)" 창의 2단계에서 SEC 부트스트랩 데이터를 복사합니다.

단계 **3** 이 절차의 사전 요구 사항에 나와 있는 메모리, CPU 및 디스크 공간 이상으로 CentOS 7 가상 머신 (http://isoredirect.centos.org/centos/7/isos/x86_64/CentOS-7-x86_64-Minimal-1804.iso)을 설치합니다.

단계 **4** 설치가 완료되면 CDO 커넥터의 IP 주소, 서브넷 마스크 및 게이트웨이를 지정하는 등의 기본 네트워킹을 구성합니다.

단계 **5** DNS(Domain Name Server) 서버를 구성합니다.

단계 **6** NTP(Network Time Protocol) 서버를 구성합니다.

단계 **7** CDO 커넥터의 CLI와의 손쉬운 상호 작용을 위해 CentOS에 SSH 서버를 설치합니다.

단계 **8** Yum 업데이트를 실행한 후 **open-vm-tools**, **nettools** 및 **bind-utils** 패키지를 설치합니다.

```
[root@sdc-vm ~]# yum update -y
[root@sdc-vm ~]# yum install -y open-vm-tools net-tools bind-utils
```

단계 **9** **AWS CLI package(AWS CLI** 패키지**)** (https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html)를 설치합니다.

참고 `--user` 플래그를 사용하지 마십시오.

단계 **10** **Docker CE packages(Docker CE** 패키지**)** (https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ce)를 설치합니다.

참고 "저장소를 사용하여 설치" 방법을 사용합니다.

단계 **11** Docker 서비스를 시작하고 부팅 시 시작되도록 활성화합니다.

```
[root@sdc-vm ~]# systemctl start docker
 [root@sdc-vm ~]# systemctl enable docker
Created symlink from /etc/systemd/system/multiuser.target.wants/docker.service to
/usr/lib/systemd/system/docker.service.
```

단계 **12** 두 사용자(**cdo** 및 **sdc**)를 생성합니다. cdo 사용자는 관리 기능을 실행하기 위해 로그인하는 사용자이며(루트 사용자를 직접 사용할 필요가 없음), sdc 사용자는 CDO 커넥터 도커 컨테이너를 실행하는 사용자입니다.

```
[root@sdc-vm ~]# useradd cdo
 [root@sdc-vm ~]# useradd sdc –d /usr/local/cdo
```

단계 **13** cdo 사용자의 비밀번호를 생성합니다.

```
[root@sdc-vm ~]# passwd cdo
Changing password for user cdo.
New password: <type password>
Retype new password: <type password>
passwd: all authentication tokens updated successfully.
```

단계 **14** cdo 사용자를 "Wheel" 그룹에 추가하여 관리(sudo) 권한을 부여합니다.

```
[root@sdc-vm ~]# usermod -aG wheel cdo
 [root@sdc-vm ~]#
```

단계 **15** Docker가 설치되면 사용자 그룹이 생성됩니다. CentOS/Docker 버전에 따라 "docker" 또는 "dockerroot"라고 부를 수 있습니다. /etc/group 파일을 확인하여 어떤 그룹이 생성되었는지 확인한 다음 sdc 사용자를 이 그룹에 추가합니다.

```
 [root@sdc-vm ~]# grep docker /etc/group
docker:x:993:
```

```
[root@sdc-vm ~]#
[root@sdc-vm ~]# usermod -aG docker sdc
[root@sdc-vm ~]#
```

단계 **16** `/etc/docker/daemon.json` 파일이 없는 경우 파일을 생성하고 아래 내용을 입력합니다. 생성되면 docker 데몬을 다시 시작합니다.

참고 "group" 키에 입력한 그룹 이름이 단계 15과 일치하는지 확인합니다.

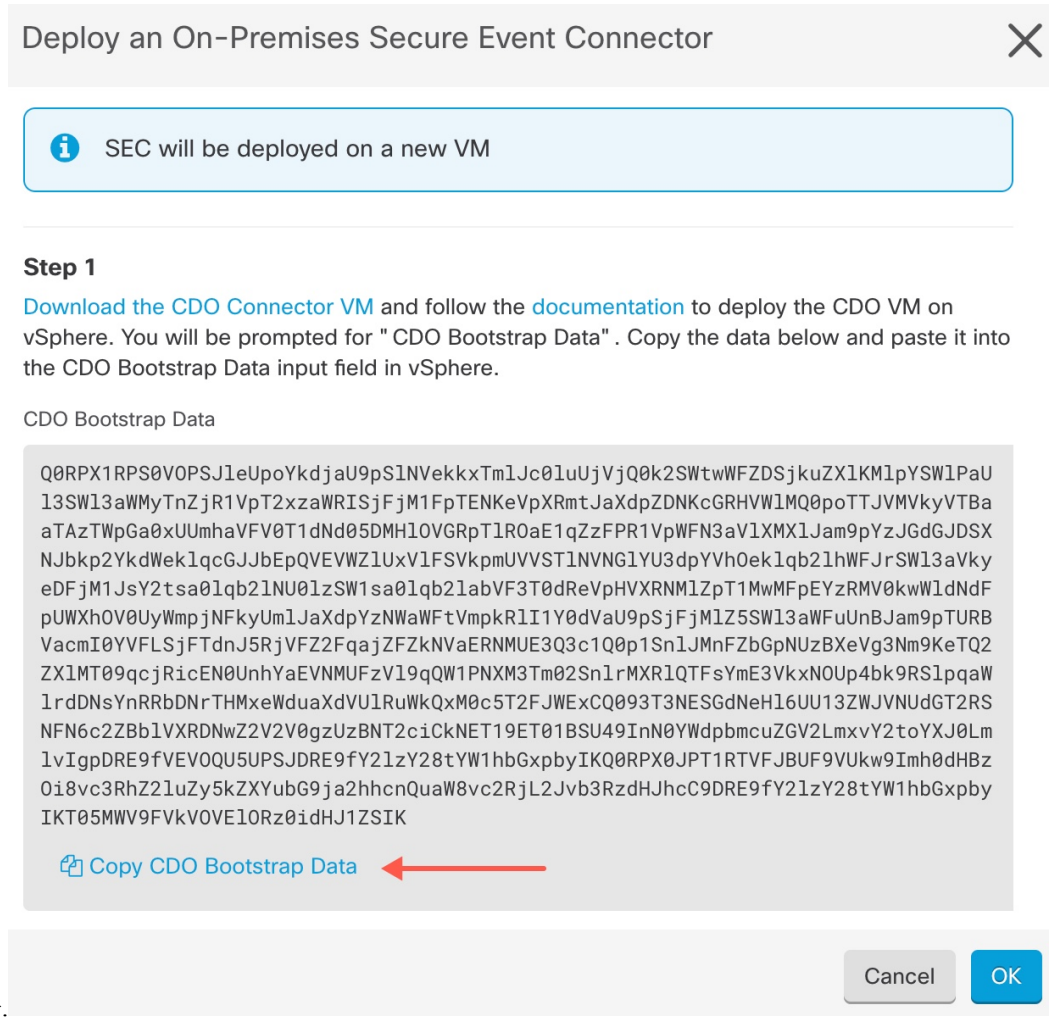
```
 [root@sdc-vm ~]# cat /etc/docker/daemon.json
{
 "live-restore": true,
 "group": "docker"
}
[root@sdc-vm ~]# systemctl restart docker
[root@sdc-vm ~]#
```

단계 **17** 현재 vSphere 콘솔 세션를 사용하는 경우 SSH로 전환하고 **cdo** 사용자로 로그인합니다. 로그인한 후에는 **sdc** 사용자로 변경합니다. 암호를 묻는 메시지가 표시되면 **cdo** 사용자의 암호를 입력합니다.

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

단계 **18** 디렉터리를 **/usr/local/cdo**로 변경합니다.

단계 **19** **bootstrapdata**라는 새 파일을 생성하고 배포 마법사 1단계의 부트스트랩 데이터를 이 파일에 붙여넣습니다. 파일을 **Save(**저장**)**합니다. **vi** 또는 **nano**를 사용하여 파일을 생성할 수 있습니




다.

단계 **20** 부트스트랩 데이터는 base64로 인코딩됩니다. 이를 디코딩하고 **extractedbootstrapdata**라는 파일로 내보냅니다.

```
 [sdc@sdc-vm ~]$ base64 -d /usr/local/cdo/bootstrapdata > /usr/local/cdo/extractedbootstrapdata
[sdc@sdc-vm ~]$
```

cat 명령을 실행하여 디코딩된 데이터를 확인합니다. 명령 및 디코딩된 데이터는 다음과 같이 표시됩니다.

```
[sdc@sdc-vm ~]$ cat /usr/local/cdo/extractedbootstrapdata
CDO_TOKEN="<token string>"
CDO_DOMAIN="www.defenseorchestrator.com"
CDO_TENANT="<tenant-name>"
CDO_BOOTSTRAP_URL="https://www.defenseorchestrator.com/sdc/bootstrap/tenant-name/<tenant-name-SDC>"
ONLY_EVENTING="true"
```

단계 **21** 다음 명령을 실행하여 디코딩된 부트스트랩 데이터의 섹션을 환경 변수로 내보냅니다.

```
 [sdc@sdc-vm ~]$ sed -e 's/^/export /g' extractedbootstrapdata > sdcenv && source sdcenv
[sdc@sdc-vm ~]$
```

단계 **22** CDO에서 부트스트랩 번들을 다운로드합니다.

```
 [sdc@sdc-vm ~]$ curl -O -H "Authorization: Bearer $CDO_TOKEN" "$CDO_BOOTSTRAP_URL"
100 10314 100 10314 0 0 10656 0 --:--:-- --:--:-- --:--:-- 10654
[sdc@sdc-vm ~]$ ls -l /usr/local/cdo/*SDC
-rw-rw-r--. 1 sdc sdc 10314 Jul 23 13:48 /usr/local/cdo/tenant-name-SDC
```

단계 **23** CDO 커넥터 tarball을 추출하고 bootstrap_sec_only.sh 파일을 실행하여 CDO 커넥터 패키지를 설치합니다.

```
 [sdc@sdc-vm ~]$ tar xzvf /usr/local/cdo/tenant-name-SDC
<snipped – extracted files>
[sdc@sdc-vm ~]$
[sdc@sdc-vm ~]$ /usr/local/cdo/bootstrap/bootstrap_sec_only.sh
[2018-07-23 13:54:02] environment properly configured
download: s3://onprem-sdc/toolkit/prod/toolkit.tar to toolkit/toolkit.tar
toolkit.sh
common.sh
es_toolkit.sh
sec.sh
healthcheck.sh
troubleshoot.sh
no crontab for sdc
-bash-4.2$ crontab -l
*/5 * * * * /usr/local/cdo/toolkit/es_toolkit.sh upgradeEventing 2>&1 >>
/usr/local/cdo/toolkit/toolkit.log
0 2 * * * sleep 30 && /usr/local/cdo/toolkit/es_toolkit.sh es_maintenance 2>&1 >>
/usr/local/cdo/toolkit/toolkit.log
You have new mail in /var/spool/mail/sdc
```

---

다음에 수행할 작업

생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성, 452 페이지를 계속합니다.

## 생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성

자체 CentOS 7 가상 머신에 CDO 커넥터를 설치한 경우, 이벤트가 SEC에 도달하도록 허용하려면 다음 추가 구성 절차 중 하나를 수행해야 합니다.

- CentOS 7 VM에서 firewalld 서비스를 비활성화합니다.. 이는 Cisco 제공 SDC VM의 구성과 일치합니다.
- firewalld 서비스가 실행되도록 허용하고 방화벽 규칙을 추가하여 이벤트 트래픽이 SEC에 도달하도록 허용합니다., 453 페이지. 이는 인바운드 이벤트 트래픽을 허용하는 보다 세부적인 접근 방식입니다.

### CentOS 7 VM에서 firewalld 서비스를 비활성화합니다.

1. SDC VM의 CLI에 "cdo" 사용자로 로그인합니다.
2. firewalld 서비스를 중지한 다음, 이후에 VM을 재부팅할 때 비활성화된 상태로 유지되는지 확인합니다. 메시지가 표시되면 **cdo** 사용자의 비밀번호를 입력합니다.

```
[cdo@SDC-VM ~]$ sudo systemctl stop firewalld
cdo@SDC-VM ~]$ sudo systemctl disable firewalld
```

3. Docker 서비스를 다시 시작하여 Docker 관련 항목을 로컬 방화벽에 다시 삽입합니다.

```
[cdo@SDC-VM ~]$ sudo systemctl restart docker
```

4. CDO 커넥터 가상 머신에 보안 이벤트 커넥터 설치, 453 페이지를 진행합니다.

**firewalld** 서비스가 실행되도록 허용하고 방화벽 규칙을 추가하여 이벤트 트래픽이 **SEC**에 도달하도록 허용합니다.

1. SDC VM의 CLI에 "cdo" 사용자로 로그인합니다.
2. 구성한 TCP, UDP 또는 NSEL 포트에서 SEC로 수신되는 트래픽을 허용하도록 로컬 방화벽 규칙을 추가합니다. SEC에서 사용하는 포트에 대해서는 SaaS(Secure Logging Analytics)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기를 참조하십시오. 메시지가 표시되면 **cdo** 사용자의 비밀번호를 입력합니다. 다음은 이러한 명령의 예입니다. 다른 포트 값을 지정해야 할 수 있습니다.

```
[cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10125/tcp
cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10025/udp
[cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10425/udp
```

3. firewalld 서비스를 다시 시작하여 새 로컬 방화벽 규칙을 활성 및 영구 규칙으로 설정합니다.

```
[cdo@SDC-VM ~]$ sudo systemctl restart firewalld
```

4. CDO 커넥터 가상 머신에 보안 이벤트 커넥터 설치, 453 페이지를 진행합니다.

## CDO 커넥터 가상 머신에 보안 이벤트 커넥터 설치

시작하기 전에

다음 두 가지 작업을 수행합니다.

- VM 이미지를 사용하여 SEC를 지원하도록 CDO 커넥터 설치, 447 페이지
- 생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성, 452 페이지

---

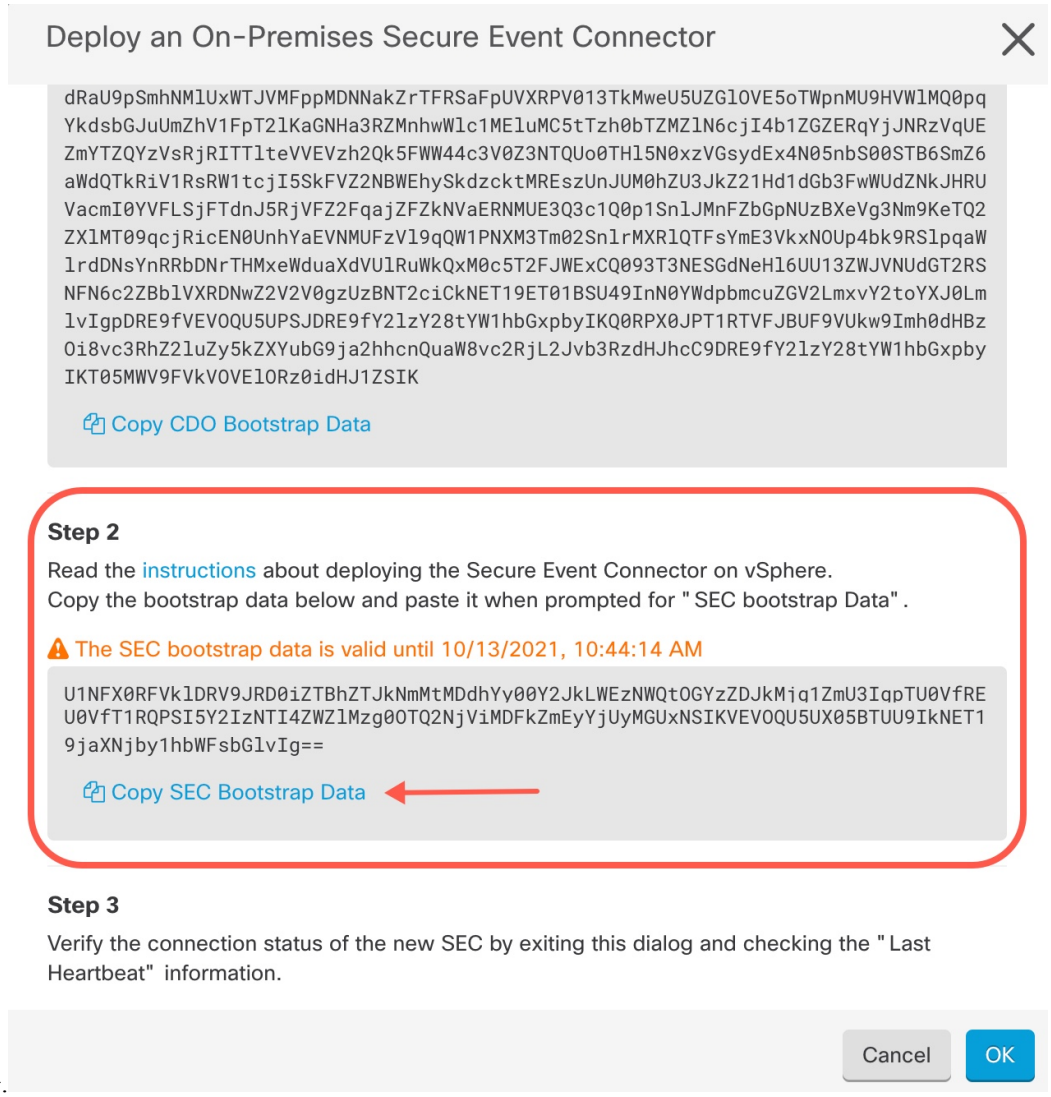
단계 **1** CDO에 로그인합니다.

단계 **2** CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.

단계 **3** 위의 사전 요구 사항에 있는 절차를 사용하여 설치한 CDO 커넥터를 선택합니다. Secure Connector(보안 커넥터) 테이블에서는 이를 보안 이벤트 커넥터(보안 이벤트 커넥터)라고 합니다.

단계 **4** 오른쪽의 작업 창에서 **Deploy an On-Premises Secure Event Connector(**온프레미스 보안 디바이스 커넥터 구축**)**를 클릭합니다.

단계 5 마법사 2단계에서 링크를 클릭하여 **SEC** 부트스트랩 데이터를 복사합니




다.

단계 6 SSH를 사용하여 Secure Connector에 연결하고 **cdo** 사용자로 로그인합니다.

단계 7 로그인한 후에는 **sdc** 사용자로 전환합니다. 암호를 묻는 메시지가 표시되면 "cdo" 사용자의 암호를 입력합니다. 다음은 이러한 명령의 예입니다.

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

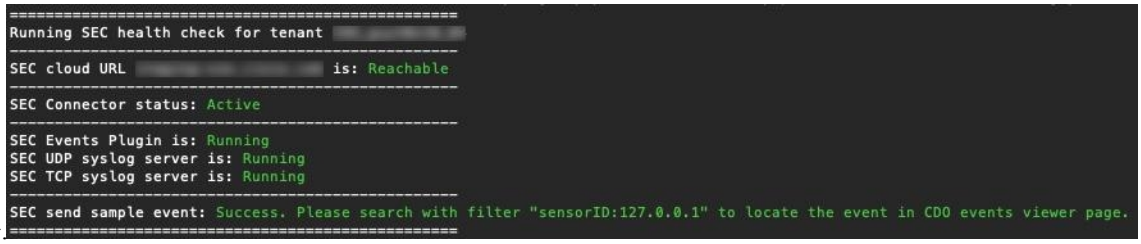
단계 8 프롬프트에서 sec.sh 설정 스크립트를 실행합니다.

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

단계 9 프롬프트 끝에 4단계에서 복사한 부트스트랩 데이터를 붙여넣고 **Enter** 키를 누릅니다.

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
 KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

SEC가 온보딩되면 sec.sh는 SEC의 상태를 확인하는 스크립트를 실행합니다. 모든 상태 확인이 "녹색"인 경우 상태 확인은 이벤트 로그에 샘플 이벤트를 전송합니다. 샘플 이벤트는 이벤트 로그에 "sec-health-check"라는 정책으로표시됩니다.




등록에 실패했거나 SEC 온 보딩에 실패했다는 메시지가 표시되면 보안 이벤트 커넥터 문제 해결로 이동하십시오.

성공 메시지가 표시되면 **Deploy an ON-Premise Secure Event Connector(**온프레미스 보안 이벤트 커넥터 구축**)** 대화 상자에서 **Done(**완료**)**를 클릭합니다. VM 이미지에 SEC 설치를 완료했습니다.

단계 **10** "다음 작업"을 계속합니다.

---

다음에 수행할 작업

SAL SaaS의 구현을 계속하려면 이 절차로 돌아가십시오. ASA 디바이스에 대한 SaaS(Secure Logging Analytics) 구현, 389 페이지 .

관련 정보**:**

- 보안 디바이스 커넥터 문제 해결, 553 페이지
- 보안 이벤트 커넥터 문제 해결
- SEC 온보딩 실패 문제 해결
- 보안 이벤트 커넥터 등록 실패 문제 해결

# Terraform 모듈을 사용하여 AWS VPC에 보안 이벤트 커넥터 설치

시작하기 전에

- 이 작업을 수행하려면 CDO 테넌트에서 SAL을 활성화해야 합니다. 이 섹션에서는 SAL 라이선스가 있다고 가정합니다. 라이선스가 없는 경우 Cisco 보안 및 분석 로깅, 로깅 및 문제 해결 라이선스를 구매합니다.
- 새 SEC가 설치되어 있는지 확인합니다. 새 SEC를 생성하려면 SDC 가상 머신에 SEC(Secure Event Connector) 설치, 438 페이지의 내용을 참조하십시오.
- SEC를 설치할 때 CDO 부트스트랩 데이터 및 SEC 부트스트랩 데이터를 적어 두십시오.

단계 **1** Terraform 레지스트리의 Secure Event Connector Terraform 모듈로 이동하고 지침에 따라 SEC Terraform 모듈을 Terraform 코드에 추가합니다.

단계 **2** Terraform 코드를 적용합니다.

단계 **3** `instance_id` 및 `sec_fqdn` 출력은 나중에 절차에서 필요하므로 인쇄해야 합니다.

참고 SEC 문제를 해결하려면 AWS Systems Manager Session Manager(SSM)를 사용하여 SEC 인스턴스에 연결해야 합니다. SSM을 사용하여 인스턴스에 연결하는 방법에 대한 자세한 내용은 AWS Systems Manager Session Manager 설명서를 참조하십시오.

SSH를 사용하여 SDC 인스턴스에 연결하는 포트는 보안상의 이유로 노출되지 않습니다.

단계 **4** ASA에서 SEC로 로그를 전송하려면 생성한 SEC의 인증서 체인을 가져와 단계 3의 출력과 함께 다음 명령을 실행하여 리프 인증서를 제거합니다.

```
rm -f /tmp/cert_chain.pem && openssl s_client -showcerts -verify 5 -connect <FQDN>:10125 < /dev/null
| awk '/BEGIN CERTIFICATE/,/END CERTIFICATE/{ if(/BEGIN CERTIFICATE/){a++}; out="/tmp/cert_chain.pem";
 if(a > 1) print >>out}'
```

단계 **5** `/tmp/cert_chain.pem`의 내용을 클립보드에 복사합니다.

단계 **6** 다음 명령을 사용하여 SEC의 IP 주소를 기록해 둡니다.

```
nslookup <FQDN>
```

단계 **7** CDO에 로그인하고 새 트러스트 포인트 개체 추가를 시작합니다. 자세한 내용은 신뢰할 수 있는 CA 인증서 개체 추가를 참조하십시오. **Add(**추가**)**를 클릭하기 전에 **Other Options(**기타 옵션**)**에서 **Enable CA flag in basic constraints extension(**기본 제약 조건 확장에서 **CA** 플래그 활성화**)** 확인란의 선택을 취소해야 합니다.

단계 **8** **Add(**추가**)**를 클릭하고 **Install Certificate(**인증서 설치**)** 페이지의 CDO에서 생성한 CLI 명령을 복사한 다음 **Cancel(**취소**)**을 클릭합니다.

단계 **9** `enrollment terminal(등록 터미널)` 아래 텍스트 클립보드에 `no ca-check`를 추가합니다.

단계 **10** SSH로 ASA 디바이스에 연결하거나 CDO에서 ASA CLI 옵션을 사용하고 다음 명령을 실행합니다.

```
DataCenterFW-1> en
Password: *****************
DataCenterFW-1# conf t
DataCenterFW-1(config)# <paste your modified ASA CLIs here and press Enter>
DataCenterFW-1(config)# wr mem
Building configuration...
Cryptochecksum: 6634f35f 4c5137f1 ab0c5cdc 9784bdb6
```

다음에 수행할 작업

SEC가 AWS SSM을 사용하여 패킷을 수신하고 있는지 확인할 수 있습니다.

다음과 유사한 로그가 표시됩니다.

```
time="2023-05-10T17:13:46.135018214Z" level=info msg="[ip-10-100-5-19.ec2.internal][util.go:67
 plugin.createTickers:func1] Events - Processed - 6/s, Dropped - 0/s, Queue size - 0"
```

# Cisco Security Analytics and Logging(SaaS) 프로비저닝

Cisco SaaS(Security Analytics and Logging) 유료 라이선스가 만료되도록 허용하는 경우 90일의 유예 기간이 제공됩니다. 이 유예 기간 동안 유료 라이선스를 갱신하는 경우 서비스가 중단되지 않습니다.

그렇지 않고 90일의 유예 기간이 경과하도록 허용하면 시스템은 모든 고객 데이터를 비웁니다. 더 이상 이벤트 로깅 페이지에서 ASA 또는 FTD 이벤트를 보거나 ASA 또는 FTD 이벤트 및 네트워크 플로우 데이터에 동적 엔터티 모델링 동작 분석을 적용할 수 없습니다.

# 보안 이벤트 커넥터 제거

경고: 이 절차는 보안 디바이스 커넥터에서 보안 이벤트 커넥터를 삭제합니다. 이렇게 하면 SaaS(Secure Logging Analytics)를 사용할 수 없습니다. 이는 되돌릴 수 없습니다. 질문이나 우려 사항이 있는 경우 이 작업을 수행하기 전에 Cisco Defense Orchestrator 지원팀에 문의하십시오.

보안 디바이스 커넥터에서 보안 이벤트 커넥터를 제거하는 작업은 다음의 2단계 프로세스입니다.

1. CDO에서 SEC 제거
2. SDC에서 SEC 파일 제거.

후속 작업:CDO에서 SEC 제거 계속

## CDO에서 SEC 제거

시작하기 전에

보안 이벤트 커넥터 제거, 457 페이지의 내용을 참조하십시오.

단계 **1** CDO에 로그인합니다.

단계 **2** CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.

단계 **3** 디바이스 유형인 보안 이벤트 커넥터가 있는 행을 선택합니다.

경고: 주의하십시오. 보안 디바이스 커넥터를 선택하지 마십시오.

단계 **4** Actions(작업) 창에서 **Remove(**제거**)**를 클릭합니다.

단계 **5** **OK(**확인**)**를 클릭하여 보안 이벤트 커넥터 삭제를 확인합니다.

다음에 수행할 작업

SDC에서 SEC 파일 제거, 458 페이지를 진행합니다.

# SDC에서 SEC 파일 제거

이는 SDC에서 보안 이벤트 커넥터를 제거하는 2단계 절차의 두 번째 부분입니다. 시작하기 전에 보안 이벤트 커넥터 제거, 457 페이지을 참조하십시오.

단계 **1** 가상 머신 하이퍼바이저를 열고 SDC에 대한 콘솔 세션을 시작합니다.

단계 **2** SDC 사용자로 전환합니다.

```
[cdo@tenant toolkit]$sudo su sdc
```

단계 **3** 프롬프트에서 다음 명령 중 하나를 입력합니다.

- 자체 테넌트만 관리하는 경우:

  ```
  [sdc@tenant toolkit]$ /usr/local/cdo/toolkit/sec.sh remove
  ```

- 둘 이상의 테넌트를 관리하는 경우 테넌트 이름의 시작 부분에 CDO_를 추가합니다. 예를 들면 다음과 같습니다.

  ```
  [sdc@tenant toolkit]$ /usr/local/cdo/toolkit/sec.sh remove CDO_[tenant_name]
  ```

단계 **4** SEC 파일을 제거할 것인지 확인합니다.

# Cisco Secure Cloud Analytics 포털 프로비저닝

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

**Logging Analytics and Detection(**로깅 분석 및 탐지**)** 또는 **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스를 구매한 경우, SEC(Secure Event Connector)를 구축하고 구성한 후 Secure Cloud Analytics 포털을 CDO 포털에 연결해야 Secure Cloud Analytics 알림을 볼 수 있습니다. 기존 Secure Cloud Analytics 포털이 있는 경우 라이선스를 구매할 때 Secure Cloud Analytics 포털 이름을 제공하고 CDO 포털에 즉시 연결할 수 있습니다.

그렇지 않은 경우 CDO UI에서 새 Secure Cloud Analytics 포털을 요청할 수 있습니다. Secure Cloud Analytics 알림에 처음 액세스하면 시스템은 Secure Cloud Analytics 포털을 요청할 수 있는 페이지로 이동합니다. 이 포털을 요청하는 사용자에게는 포털에서 관리자 권한이 부여됩니다.

단계 **1** CDO 메뉴에서 분석 > **Secure Cloud Analytics**를 선택하여 새 창에서 Secure Cloud Analytics UI를 엽니다.

단계 **2** **Start Free Trial(**무료 평가판 시작**)**을 클릭하여 Secure Cloud Analytics 포털을 프로비저닝하고 CDO 포털과 연결합니다.

**Note** 포털을 요청한 후 프로비저닝에 몇 시간이 걸릴 수 있습니다.

다음 단계로 이동하기 전에 포털이 프로비저닝되었는지 확인합니다.

1. CDO 메뉴에서 분석 > **Secure Cloud Analytics**를 선택하여 새 창에서 Secure Cloud Analytis UI를 엽니다.
2. 다음 옵션을 이용할 수 있습니다.
   - Secure Cloud Analytics 포털을 요청했는데 시스템에서 포털을 프로비저닝하는 중이라고 표시되면 기다렸다가 나중에 알림에 액세스해 보십시오.
   - Secure Cloud Analytics 포털이 프로비저닝된 경우 **Username(**사용자 이름**)** 및 **Password(**비밀번호**)**를 입력하고 **Sign in(**로그인**)**을 클릭합니다.

**Note** 관리자 사용자는 다른 사용자를 초대하여 Secure Cloud Analytis 포털 내에서 계정을 생성할 수 있습니다. 자세한 내용은 CDO에서 Cisco Secure Cloud Analytics 알림 보기, on page 461를 참조하십시오.

### What to do next

- **Logging Analytics and Detection(**로깅 분석 및 탐지**)** 라이선스를 구매한 경우 구성이 완료된 것입니다. Secure Cloud Analytics 포털 UI에서 CDO 통합 또는 센서 상태를 보려면 Secure Cloud Analytics에서 센서 상태 및 CDO 통합 상태 검토, on page 459에서 자세한 내용을 확인하십시오. Secure Cloud Analytics 포털에서 알림으로 작업하려는 경우 자세한 내용은 CDO에서 Cisco Secure Cloud Analytics 알림 보기, on page 461 및 방화벽 이벤트 기반 알림 작업을 참조하십시오.
- **Total Network Analytics and Monitoring** 라이선스를 구매한 경우 내부 네트워크에 하나 이상의 Secure Cloud Analytics 센서를 구축하여 네트워크 플로우 데이터를 클라우드에 전달합니다. 클라우드 기반 네트워크 플로우 데이터를 모니터링하려면 플로우 데이터를 Secure Cloud Analytics로 전달하도록 클라우드 기반 구축을 구성합니다. 자세한 내용은 전체 네트워크 분석 및 보고를 위한 Cisco Secure Cloud Analytics 센서 구축, on page 460를 참조하십시오.

# Secure Cloud Analytics에서 센서 상태 및 CDO 통합 상태 검토

센서 상태

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

Secure Cloud Analytis 웹 UI의 Sensor List(센서 목록) 페이지에서 CDO 통합 상태 및 구성된 센서를 볼 수 있습니다. CDO 통합은 읽기 전용 연결 이벤트 센서입니다. Stelathwatch Cloud는 기본 메뉴에서 센서의 전반적인 상태를 제공합니다.

- 녹색 클라우드 아이콘() - 모든 센서와 연결 설정됨, 구성된 경우 CDO
- 노란색 클라우드 아이콘() - 일부 센서 또는 CDO(구성된 경우)와의 연결이 설정되었으며 하나 이상의 센서가 제대로 구성되지 않음
- 빨간색 클라우드 아이콘() - 구성된 모든 센서 및 CDO(구성된 경우)와의 연결 끊김

센서 또는 CDO 통합에서 녹색 아이콘은 설정된 연결을 나타내고, 빨간색 아이콘은 연결 끊김을 나타냅니다.

단계 **1** 1. Secure Cloud Analytis 포털 UI에서 **Settings(**설정**)(⚙) > Sensors(**센서**)**를 선택합니다.

단계 **2** **Sensor List(**센서 목록**)**를 선택합니다.

# 전체 네트워크 분석 및 보고를 위한 **Cisco Secure Cloud Analytics** 센서 구축

**Secure Cloud Analytics** 센서 개요 및 배포

필수 라이선스: 전체 네트워크 분석 및 모니터링

**Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스를 취득한 경우 Secure Cloud Analytics 포털을 프로비저닝한 후 다음을 수행할 수 있습니다.

- 분석을 위해 네트워크 플로우 데이터를 클라우드에 전달하기 위해 온프레미스 네트워크 내에 Secure Cloud Analytics 센서를 배포하고 구성합니다.
- 분석을 위해 네트워크 플로우 로그 데이터를 Secure Cloud Analytics에 전달하도록 클라우드 기반 배포을 구성합니다.

네트워크 경계의 방화벽은 내부 네트워크와 외부 네트워크 간의 트래픽에 대한 정보를 수집하는 반면, Secure Cloud Analytics 센서는 내부 네트워크 내의 트래픽에 대한 정보를 수집합니다.

**Note** FDM 관리Secure Firewall Threat Defense 디바이스가 NetFlow 데이터를 전달하도록 구성할 수 있습니다. 센서를 배포할 때, 이벤트 정보를 CDO로 전달하도록 구성한 FDM 관리Secure Firewall Threat Defense 디바이스에서 NetFlow 데이터를 전달하도록 센서를 구성하지 마십시오.

센서 배포 지침 및 권장 사항은 Secure Cloud Analytics 센서 설치 설명서를 참조하십시오.

클라우드 기반 배포 구성 지침 및 권장 사항은 Secure Cloud Analytics 퍼블릭 클라우드 모니터링 가이드를 참조하십시오.

**Note** Secure Cloud Analytics 포털 UI의 지침을 검토하여 센서 및 클라우드 기반 배포을 구성할 수도 있습니다.

Secure Cloud Analytics에 대한 자세한 내용은 Secure Cloud Analytics 무료 평가판 가이드를 참조하십시오.

다음 단계

- CDO에서 Cisco Secure Cloud Analytics 알림 보기, on page 461를 계속 진행합니다.

# CDO에서 Cisco Secure Cloud Analytics 알림 보기

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

Events logging(이벤트 로깅) 페이지에서 방화벽 이벤트를 검토할 수 있지만 CDO 포털 UI에서 Cisco Secure Cloud Analytics 알림을 검토할 수는 없습니다. Security Analytics(보안 분석) 메뉴 옵션을 사용하여 CDO에서 Secure Cloud Analytics 포털로 교차 실행하고, 방화벽 이벤트 데이터(전체 네트워크 분석 및 모니터링을 활성화한 경우 네트워크 플로우 데이터)에서 생성된 알림을 볼 수 있습니다. Security Analytics(보안 분석) 메뉴 옵션은 하나 이상의 열려 있는 워크플로우 상태의 Secure Cloud Analytics 알림 수와 함께 배지를 표시합니다.

Security Analytics and Logging(보안 분석 및 로깅) 라이선스를 사용하여 Secure Cloud Analytics 알림을 생성하고 새 Secure Cloud Analytics 포털을 프로비저닝한 경우, CDO에 로그인한 다음 Cisco Secure Cloud Sign-On을 사용하여 Secure Cloud Analytics를 교차 실행합니다. URL을 통해 Secure Cloud Analytics 포털에 직접 액세스할 수도 있습니다.

자세한 내용은 Cisco Security Cloud Sign On을 참조하십시오.

## Secure Cloud Analytics 포털에 사용자 초대

Secure Cloud Analytics 포털 프로비저닝을 요청하는 초기 사용자는 Secure Cloud Analytics 포털에서 관리자 권한을 갖습니다. 해당 사용자는 이메일로 다른 사용자를 초대하여 포털에 참여할 수 있습니다. 이러한 사용자에게 Cisco Secure Cloud Sign-On 자격증명이 없는 경우 초대 이메일의 링크를 사용하여 생성할 수 있습니다. 그러면 사용자는 Cisco Secure Cloud Sign-On 자격증명을 사용하여 CDO에서 Secure Cloud Analytics로 교차 실행하는 동안 로그인할 수 있습니다.

이메일로 다른 사용자를 Secure Cloud Analytics 포털에 초대하려면 다음을 수행합니다.

단계 **1** Secure Cloud Analytics 포털에 관리자로 로그인합니다.

단계 **2** **Settings(**설정**)** > **Account Management(**계정 관리**)** > **User Management(**사용자 관리**)**를 선택합니다.

단계 **3** 이메일 주소를 입력합니다.

단계 **4** **Invite(**초대**)**를 클릭합니다.

## CDO에서 Secure Cloud Analytics로 교차 실행

CDO에서 보안 알림을 보려면 다음을 수행합니다.

단계 **1** CDO 포털에 로그인합니다.

단계 **2** CDO 메뉴에서 분석 > **Secure Cloud Analytics**를 선택합니다.

단계 **3** Secure Cloud Analytics 인터페이스에서 **Monitor(**모니터링**)** > **Alerts(**알림**)**를 선택합니다.

# Cisco Secure Cloud Analytics 및 동적 엔티티 모델링

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

Secure Cloud Analytics는 온프레미스 및 클라우드 기반 네트워크 구축을 모니터링하는 SaaS(Software as a Service) 솔루션입니다. 방화벽 이벤트 및 네트워크 플로우 데이터를 비롯한 소스에서 네트워크 트래픽에 대한 정보를 수집하여 트래픽에 대한 관찰을 생성하고 트래픽 패턴을 기반으로 네트워크 엔티티의 역할을 자동으로 식별합니다. Secure Cloud Analytics는 Talos와 같은 위협 인텔리전스의 다른 소스와 결합된 이 정보를 사용하여 본질적으로 악의적인 행동이 있음을 나타내는 경고를 생성합니다. 알림과 함께 Secure Cloud Analytics는 알림을 조사하고 악의적인 동작의 소스를 찾기 위한 더 나은 기반을 제공하기 위해 수집한 네트워크 및 호스트 가시성 및 상황 정보를 제공합니다.

동적 엔티티 모델링

동적 엔티티 모델링은 방화벽 이벤트 및 네트워크 플로우 데이터에 대한 동작 분석을 수행하여 네트워크의 상태를 추적합니다. Secure Cloud Analytics의 컨텍스트에서 엔티티는 네트워크의 호스트 또는 엔드포인트와 같이 시간이 지남에 따라 추적할 수 있는 항목입니다. 동적 엔터티 모델링은 전송하는 트래픽 및 네트워크에서 수행하는 활동을 기반으로 엔터티에 대한 정보를 수집합니다. **Logging Analytics and Detection(**로깅 분석 및 탐지**)** 라이선스와 통합된 Secure Cloud Analytics는 엔티티가 일반적으로 전송하는 트래픽 유형을 확인하기 위해 방화벽 이벤트 및 기타 트래픽 정보를 가져올 수 있습니다. **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스를 구매한 경우 Secure Cloud Analytics는 엔티티 트래픽 모델링에 NetFlow 및 기타 트래픽 정보도 포함할 수 있습니다. Secure Cloud Analytics는 각 엔터티의 최신 모델을 유지하기 위해 엔터티가 계속해서 트래픽을 전송하고 잠재적으로 다른 트래픽을 전송하므로 시간이 지남에 따라 이러한 모델을 업데이트합니다. 이 정보에서 Secure Cloud Analytics는 다음을 식별합니다.

- 엔티티의 역할 - 엔티티가 일반적으로 수행하는 작업을 설명합니다. 예를 들어 엔티티가 일반적으로 이메일 서버와 연결된 트래픽을 전송하는 경우, Secure Cloud Analytics는 엔티티를 이메일 서버 역할로 할당합니다. 엔터티는 여러 역할을 수행할 수 있으므로 역할/엔티티 관계는 다대일일 수 있습니다.
- 엔티티에 대한 관찰 - 외부 IP 주소와의 하트비트 연결 또는 다른 엔티티와 설정된 원격 액세스 세션과 같이 네트워크에서의 엔티티 동작에 대한 팩트입니다. CDO와 통합하는 경우 방화벽 이벤트에서 이러한 정보를 가져올 수 있습니다. **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스도 구매한 경우, 시스템은 NetFlow에서 팩트를 가져오고 방화벽 이벤트와 NetFlow 모두에서 관찰을 생성할 수 있습니다. 관찰 자체는 관찰이 나타내는 것 이상의 의미를 전달하지 않습니다. 일반적인 고객은 수천 개의 관찰 및 몇 가지 알림을 가질 수 있습니다.

### 알림 및 분석

역할, 관찰 및 기타 위협 인텔리전스의 조합을 기반으로 Secure Cloud Analytics는 시스템에서 식별한 가능한 악의적인 행동을 나타내는 실행 가능한 항목인 알림을 생성합니다. 하나의 알림이 여러 관찰을 나타낼 수 있습니다. 방화벽이 동일한 연결 및 엔터티와 관련된 여러 연결 이벤트를 로깅하는 경우 하나의 알림만 생성될 수 있습니다.

예를 들어, 새 내부 디바이스 관찰 자체는 악의적인 행동을 구성하지 않습니다. 그러나 시간이 지남에 따라 엔티티가 도메인 컨트롤러와 일치하는 트래픽을 전송하면 시스템은 해당 엔티티에 도메인 컨트롤러 역할을 할당합니다. 이후에 엔티티가 비정상적인 포트를 사용하여 이전에 연결을 설정하지 않은 외부 서버에 연결하고 대량의 데이터를 전송하는 경우, 시스템은 새로운 대규모 연결(외부) 관찰 및 예외적인 도메인 컨트롤러 관찰을 로깅합니다. 해당 외부 서버가 Talos 감시 목록에 있는 것으로 식별된 경우, 이 모든 정보의 조합으로 인해 Secure Cloud Analytics가 이 엔티티의 동작에 대한 알림을 생성하고, 악성 동작을 조사하고 교정하기 위한 추가 작업을 수행하라는 메시지가 표시됩니다.

Secure Cloud Analytics 웹 포털 UI에서 알림을 열면 시스템이 알림을 생성하도록 유도한 지원 관찰을 볼 수 있습니다. 이러한 관찰을 통해 관련 엔터티에 대한 추가 컨텍스트(전송한 트래픽 포함) 및 외부 위협 인텔리전스(사용 가능한 경우)도 볼 수 있습니다. 또한 엔티티가 관련된 다른 관찰 및 알림을 보고 이 동작이 다른 잠재적인 악의적인 동작과 관련이 있는지 확인할 수 있습니다.

Secure Cloud Analytics에서 알림을 보고 닫을 때는 Secure Cloud Analytics UI의 트래픽을 허용하거나 차단할 수 없습니다. 디바이스를 액티브 모드로 구축한 경우에는 트래픽을 허용하거나 차단하도록 방화벽 액세스 제어 규칙을 업데이트하고, 패시브 모드에서 디바이스를 구축한 경우에는 방화벽 액세스 제어 규칙을 업데이트해야 합니다.

# 방화벽 이벤트 기반 알림 작업

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

### 알림 워크플로우

알림의 워크플로우는 상태를 기반으로 합니다. 시스템에서 알림을 생성할 때 기본 상태는 Open(열림)이며 사용자가 할당되지 않습니다. Alerts(알림) 요약을 볼 때 즉시 문제가 되는 모든 열린 알림이 기본적으로 표시됩니다.

참고: **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스가 있는 경우 알림은 NetFlow에서 생성된 관찰, 방화벽 이벤트에서 생성된 관찰 또는 두 데이터 소스의 관찰을 기반으로 할 수 있습니다.

알림 요약을 검토할 때 알림에 대한 상태를 초기 분류로 할당, 태그 지정 및 업데이트할 수 있습니다. 필터 및 검색 기능을 사용하여 특정 알림을 찾거나, 다른 상태의 알림을 표시하거나, 다른 태그 또는 담당자와 연결할 수 있습니다. 알림의 상태를 스누즈로 설정할 수 있습니다. 이 경우 스누즈 기간이 경과할 때까지 미해결 알림 목록에 다시 나타나지 않습니다. 알림에서 스누즈 상태를 제거하여 미해결 알림으로 다시 표시할 수도 있습니다. 알림을 검토할 때 자신 또는 시스템의 다른 사용자에게 할당할 수 있습니다. 사용자는 사용자 이름에 할당된 모든 알림을 검색할 수 있습니다.

Alerts(알림) 요약에서 알림 상세정보 페이지를 볼 수 있습니다. 이 페이지에서는 이 알림을 생성한 지원 관찰에 대한 추가 컨텍스트 및 이 알림과 관련된 엔터티에 대한 추가 컨텍스트를 검토할 수 있습니다. 이 정보는 네트워크에서 문제를 추가로 조사하고 잠재적으로 악의적인 동작을 해결하기 위해 실제 문제를 정확히 찾아내는 데 도움이 될 수 있습니다.

Stealthwatch Cloud 웹 포털 UI, CDO 및 네트워크에서 조사할 때 결과를 설명하는 알림과 함께 코멘트를 남길 수 있습니다. 이렇게 하면 나중에 참조할 수 있는 연구 기록을 만드는 데 도움이 됩니다.

분석을 완료한 경우 상태를 Closed(닫힘)로 업데이트하고 더 이상 기본적으로 미결 알림으로 표시되지 않도록 할 수 있습니다. 상황이 바뀌면 나중에 닫힌 알림을 다시 열 수도 있습니다.

다음은 지정된 알림을 조사하는 방법에 대한 일반적인 지침 및 제안 사항입니다. Stealthwatch Cloud는 알림을 로깅할 때 추가 컨텍스트를 제공하므로 이 컨텍스트를 조사에 활용할 수 있습니다.

이러한 단계는 포괄적이거나 모든 것을 포함하지 않습니다. 이는 알림 조사를 시작하는 데 사용할 수 있는 일반적인 프레임워크를 제공할 뿐입니다.

일반적으로 알림을 검토할 때 다음 단계를 수행할 수 있습니다.

1. 열린 알림 분류, on page 464
2. 나중에 분석하기 위해 알림 일시 중지, on page 465
3. 추가 조사를 위해 알림 업데이트, on page 465
4. 알림 검토 및 조사 시작, on page 466
5. 엔터티 및 사용자 검사, on page 468
6. Secure Cloud Analytics를 사용하여 문제 해결, on page 468
7. 알림 업데이트 및 닫기, on page 469

# 열린 알림 분류

특히 둘 이상의 알림이 아직 조사되지 않은 경우, 미해결 알림을 분류합니다.

- CDO에서 SWC로 교차 실행하고 알림을 보는 방법에 대한 자세한 내용은 CDO에서 Cisco Secure Cloud Analytics 알림 보기을 참조하십시오.

다음 질문을 합니다.

- 이 알림 유형을 높은 우선순위로 구성했습니까?
- 영향을 받는 서브넷에 대해 높은 감도를 설정했습니까?
- 네트워크의 새 엔터티에서 발생하는 비정상적인 동작입니까?
- 엔터티의 일반적인 역할은 무엇이며 이 알림의 동작이 해당 역할과 어떻게 일치합니까?
- 이 엔터티의 정상적인 동작에서 예외적으로 벗어났습니다.
- 사용자가 관련된 경우, 이는 사용자의 예상된 동작입니까, 아니면 예외적인 것입니까?

- 보호되거나 민감한 데이터가 손상될 위험이 있습니까?
- 이 동작이 계속 허용되는 경우 네트워크에 미치는 영향은 어느 정도입니까?
- 외부 엔터티와 통신하는 경우, 이러한 엔터티가 과거에 네트워크의 다른 엔터티와 연결을 설정했습니까?

우선순위가 높은 알림인 경우 조사를 계속하기 전에 인터넷에서 엔티티를 격리하거나 연결을 닫는 것을 고려하십시오.

# 나중에 분석하기 위해 알림 일시 중지

다른 알림에 비해 우선 순위가 낮은 알림을 스누즈합니다. 예를 들어 조직에서 이메일 서버를 FTP 서버로 용도를 변경하고 시스템에서 긴급 프로파일 알림(엔티티의 현재 트래픽이 이전에 일치하지 않았던 행동 프로파일과 일치함을 나타냄)을 생성하는 경우 이 알림을 나중에 다시 확인할 수 있습니다. 스누즈된 알림은 열린 알림과 함께 표시되지 않습니다. 이러한 스누즈된 알림을 검토하려면 특별히 필터링해야 합니다.

알림 스누즈:

단계 **1** **Close Alert(**알림 닫기**)**를 클릭합니다.

단계 **2** Snooze this alert(이 알림 스누즈) 창의 드롭다운에서 스누즈 기간을 선택합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

### What to do next

이러한 알림을 검토할 준비가 되면 다시 알림을 해제할 수 있습니다. 이렇게 하면 상태가 Open(열림)으로 설정되고 다른 Open(열림) 알림과 함께 알림이 표시됩니다.

스누즈된 알림의 스누즈를 해제합니다.

- 스누즈된 알림에서 **Unsnooze Alert(**알림 스누즈 해제**)**를 클릭합니다.

# 추가 조사를 위해 알림 업데이트

알림 세부 정보를 엽니다.

단계 **1** **Monitor(**모니터링**)** > **Alerts(**알림**)**를 선택합니다.

단계 **2** 알림 유형 이름을 클릭합니다.

### What to do next

초기 분류 및 우선순위에 따라 알림을 할당하고 태그를 지정합니다.

1. **Assignee(**담당자**)** 드롭다운에서 사용자를 선택하여 알림을 할당하면 사용자가 조사를 시작할 수 있습니다.
2. 드롭다운에서 하나 이상의 **Tags(**태그**)**를 선택하여 알림에 태그를 추가하여 향후 식별을 위해 알림을 더 잘 분류하고 알림에서 장기적 패턴을 설정합니다.
3. 이 알림에 대한 코멘트를 입력한 다음 **Comment(**코멘트**)**를 클릭하여 초기 결과를 추적하고 알림에 할당된 사람을 지원하는 데 필요한 코멘트를 남깁니다. 알림은 시스템 코멘트와 사용자 코멘트를 모두 추적합니다.

# 알림 검토 및 조사 시작

할당된 알림을 검토하는 경우 알림 세부 정보를 검토하여 Stealthwatch Cloud에서 알림을 생성한 이유를 파악합니다. 지원 관찰을 검토하여 이러한 관찰이 소스 엔터티에 미치는 영향을 파악합니다.

경고가 방화벽 이벤트를 기반으로 생성된 경우, 시스템은 방화벽 구축이 이 경고의 소스임을 인식하지 않습니다.

이 소스 엔터티에 대한 모든 지원 관찰을 확인하여 일반 동작 및 패턴을 파악하고 이 활동이 더 긴 추세의 일부일 수 있는지 확인합니다.

### SUMMARY STEPS

1. 알림 세부사항에서 관찰 유형 옆에 있는 화살표 아이콘(➔)을 클릭하여 해당 유형의 모든 로깅된 관찰을 확인합니다.
2. **All Observations for Network(**네트워크에 대한 모든 관찰**)** 옆에 있는 화살표 아이콘(➔)을 클릭하여 이 알림의 소스 엔티티에 대해 로깅된 모든 관찰을 확인합니다.

### DETAILED STEPS

단계 **1** 알림 세부사항에서 관찰 유형 옆에 있는 화살표 아이콘(➔)을 클릭하여 해당 유형의 모든 로깅된 관찰을 확인합니다.

단계 **2** **All Observations for Network(**네트워크에 대한 모든 관찰**)** 옆에 있는 화살표 아이콘(➔)을 클릭하여 이 알림의 소스 엔티티에 대해 로깅된 모든 관찰을 확인합니다.

이러한 관찰에 대한 추가 분석을 수행하려면 쉼표로 구분된 값 파일로 지원 관찰을 다운로드합니다.

- 알림 세부 정보의 Supporting Observations(지원 관찰) 창에서 **CSV**를 클릭합니다.

관찰 결과에서 소스 엔터티 동작이 악의적인 동작을 나타내는지 확인합니다. 소스 엔터티가 여러 외부 엔터티와의 연결을 설정한 경우, 외부 엔터티가 어떤 식으로든 관련이 있는지 확인합니다(예: 모든 엔터티가 유사한 지리위치 정보를 가지고 있거나 해당 IP 주소가 동일한 서브넷에 있는지 여부).

소스 엔터티 IP 주소 또는 호스트 이름에서 소스 엔터티와 관련된 추가 컨텍스트를 확인합니다. 여기에는 관련될 수 있는 기타 알림 및 관찰, 디바이스 자체에 대한 정보, 전송 중인 세션 트래픽 유형이 포함됩니다.

- 엔티티와 관련된 모든 알림을 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Alerts(**알림**)**를 선택합니다.
- IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Observations(**관찰**)**를 선택하여 엔티티와 관련된 모든 관찰을 확인합니다.
- 디바이스에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Device(**디바이스**)**를 선택합니다.
- 이 엔터티와 관련된 세션 트래픽을 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Session Traffic(**세션 트래픽**)**을 선택합니다.
- IP 주소 또는 호스트 이름 드롭다운에서 **Copy(**복사**)**를 선택하여 IP 주소 또는 호스트 이름을 복사합니다.

Stealthwatch Cloud의 소스 엔티티는 항상 네트워크 내부에 있습니다. 이를 방화벽 이벤트의 Initiator IP(이니시에이터 IP)와 비교해 보십시오. 이 IP는 연결을 시작한 엔티티를 나타내며, 네트워크의 내부 또는 외부에 있을 수 있습니다.

관찰에서 다른 외부 엔터티에 대한 정보를 검토합니다. 지리위치 정보를 검토하고 지리위치 데이터 또는 Umbrella 데이터가 악성 엔티티를 식별하는지 확인합니다. 이러한 엔터티에 의해 생성된 트래픽을 확인합니다. Talos, AbuseIPDB 또는 Google에 이러한 엔터티에 대한 정보가 있는지 확인합니다. 여러 날짜의 IP 주소를 찾고 외부 엔터티가 네트워크의 엔터티와 설정한 다른 유형의 연결을 확인합니다. 필요한 경우 이러한 내부 엔터티를 찾아 보안 침해 또는 의도하지 않은 행동의 증거가 있는지 확인합니다.

소스 엔티티가 연결을 설정한 외부 엔티티 IP 주소 또는 호스트 이름에 대한 컨텍스트를 검토합니다.

- 이 엔티티에 대한 최근 트래픽 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **IP Traffic(IP** 트래픽**)**을 선택합니다.
- 이 엔티티에 대한 최근 세션 트래픽 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Session Traffic(**세션 트래픽**)**을 선택합니다.
- **AbuseIPDB**웹사이트에서 이 엔티티에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 AbuseIPDB를 선택합니다.
- Cisco Umbrella 웹사이트에서 이 엔티티에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Cisco Umbrella**를 선택합니다.
- Google에서 이 IP 주소를 검색하려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Google Search(Google** 검색**)**를 선택합니다.
- Talos 웹사이트에서 이 정보에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Talos Intelligence**를 선택합니다.
- IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Add IP to watchlist(**감시 목록에 **IP** 추가**)**를 선택하여 이 엔터티를 감시 목록에 추가합니다.
- 이 엔티티의 지난 달 트래픽을 검색하려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Find IP on multiple days(**여러 날짜의 **IP** 찾기**)**를 선택합니다.

- IP 주소 또는 호스트 이름 드롭다운에서 **Copy(**복사**)**를 선택하여 IP 주소 또는 호스트 이름을 복사합니다.

Stealthwatch Cloud의 연결된 엔터티는 항상 네트워크 외부에 있습니다. 이를 방화벽 이벤트의 Responder IP(응답자 IP)와 비교해 보십시오. 이는 연결 요청에 응답한 엔터티를 나타내며, 네트워크의 내부 또는 외부에 있을 수 있습니다.

결과에 대한 코멘트를 남겨 주십시오.

- 알림 세부 정보에서 이 알림에 대한 코멘트를 입력하고 **Comment(**코멘트**)**를 클릭합니다.

# 엔터티 및 사용자 검사

Stealthwatch Cloud 포털 UI에서 알림을 검토한 후 소스 엔터티, 이 알림과 관련되었을 수 있는 사용자 및 기타 관련 엔터티에 대해 직접 추가 검사를 수행할 수 있습니다.

- 소스 엔터티가 물리적으로 또는 클라우드에서 네트워크의 어느 위치에 있는지 확인하고 직접 액세스합니다. 이 엔터티에 대한 로그 파일을 찾습니다. 네트워크의 물리적 엔티티인 경우 디바이스에 액세스하여 로그 정보를 검토하고 이 동작의 원인에 대한 정보가 있는지 확인합니다. 가상 엔터티이거나 클라우드에 저장된 경우 로그에 액세스하여 이 엔터티와 관련된 항목을 검색합니다. 무단 로그인, 승인되지 않은 구성 변경 등에 대한 자세한 내용은 로그를 검사합니다.
- 엔터티를 검사합니다. 엔터티 자체에서 악성코드 또는 취약성을 식별할 수 있는지 확인합니다. 조직에서 승인하지 않은 USB 스틱과 같이 디바이스에 대한 물리적 변경이 있는지를 포함하여 악의적인 변경이 있는지 확인합니다.
- 네트워크의 사용자 또는 네트워크 외부의 사용자가 관련되었는지 확인합니다. 가능한 경우 사용자에게 무엇을 하고 있었는지 물어봅니다. 사용자가 사용할 수 없는 경우, 액세스 권한이 있어야 했는지, 그리고 퇴사한 직원이 퇴사 전에 외부 서버에 파일을 업로드하는 등의 상황이 발생했는지 확인합니다.

결과에 대한 코멘트를 남겨 주십시오.

- 알림 세부 정보에서 이 알림에 대한 코멘트를 입력하고 **Comment(**코멘트**)**를 클릭합니다.

# **Secure Cloud Analytics**를 사용하여 문제 해결

악의적인 행동으로 인해 알림이 발생한 경우 악의적인 행동을 교정합니다. 예를 들면 다음과 같습니다.

- 악의적인 엔터티 또는 사용자가 네트워크 외부에서 로그인을 시도한 경우 엔터티 또는 사용자가 네트워크에 액세스하지 못하도록 방화벽 규칙 및 방화벽 구성을 업데이트합니다.
- 엔터티가 무단 도메인 또는 악의적인 도메인에 액세스하려고 시도한 경우 영향을 받는 엔터티를 검사하여 악성코드가 원인인지 확인합니다. 악의적인 DNS 리디렉션이 있는 경우 네트워크의 다른 엔터티 또는 봇넷의 일부가 영향을 받는지 확인합니다. 사용자가 이러한 작업을 수행하려는 경우 방화벽 설정을 테스트하는 등 합법적인 이유가 있는지 확인합니다. 도메인에 대한 추가 액세스를 방지하려면 방화벽 규칙 및 방화벽 구성을 업데이트합니다.

- 엔터티가 기록 엔터티 모델 동작과 다른 동작을 보이는 경우 동작 변경이 의도된 것인지 확인합니다. 의도하지 않은 작업인 경우 네트워크의 다른 권한이 있는 사용자가 변경을 담당하는지 확인합니다. 의도하지 않은 동작이 네트워크 외부의 엔터티와의 연결과 관련된 경우 이를 해결하기 위해 방화벽 규칙 및 방화벽 구성을 업데이트합니다.
- 취약성 또는 익스플로잇을 식별한 경우, 영향을 받는 엔티티를 업데이트 또는 패치하여 취약성을 제거하거나 무단 액세스를 방지하도록 방화벽 구성을 업데이트합니다. 네트워크의 다른 엔터티가 유사하게 영향을 받을 수 있는지 확인하고 해당 엔터티에 동일한 업데이트 또는 패치를 적용합니다. 현재 취약성 또는 익스플로잇에 수정 사항이 없는 경우 해당 벤더에 문의하십시오.
- 악성코드가 확인되면 엔티티를 격리하고 악성코드를 제거합니다. 방화벽 파일 및 악성코드 이벤트를 검토하여 네트워크의 다른 엔터티가 위험에 노출되어 있는지 확인하고, 이 악성코드가 확산되지 않도록 엔터티를 격리 및 업데이트합니다. 이 악성코드 또는 이 악성코드를 유발한 엔티티에 대한 정보로 보안 인텔리전스를 업데이트합니다. 향후 이 악성코드가 네트워크를 감염시키는 것을 방지하려면 방화벽 액세스 제어와 파일 및 악성코드 규칙을 업데이트하십시오. 필요에 따라 벤더에 알립니다.
- 악의적인 행동으로 인해 데이터가 유출된 경우 무단 소스로 전송되는 데이터의 특성을 확인합니다. 무단 데이터 유출에 대한 조직의 프로토콜을 따르십시오. 이 소스에 의한 향후 데이터 유출 시도를 방지하려면 방화벽 구성을 업데이트하십시오.

# 알림 업데이트 및 닫기

결과에 따라 태그를 추가합니다.

단계 **1** Secure Cloud Analytics 포털 UI에서 **Monitor(**모니터링**)** > **Alerts(**알림**)**를 선택합니다.

단계 **2** 드롭다운에서 하나 이상의 **Tags(**태그**)**를 선택합니다.

조사 결과 및 수행한 교정 단계를 설명하는 최종 코멘트를 추가합니다.

- 알림 세부 정보에서 이 알림에 대한 코멘트를 입력하고 **Comment(**코멘트**)**를 클릭합니다.

알림을 닫고 유용하거나 도움이 되지 않음으로 표시합니다.

1. 알림 세부 정보에서 **Close Alert(**알림 닫기**)**를 클릭합니다.
2. 알림이 도움이 되었으면 **Yes(**예**)**를 선택하고, 알림이 도움이 되지 않았다면 **No(**아니요**)**를 선택합니다. 이는 알림이 악의적인 행동으로 인해 발생했음을 의미하는 것이 아니라 해당 알림이 조직에 도움이 되었음을 의미합니다.
3. **Save(**저장**)**를 클릭합니다.

### What to do next

종료된 알림 다시 열기

종료된 알림과 관련된 추가 정보를 발견하거나 알림과 관련된 코멘트를 더 추가하려는 경우 알림을 다시 열어 상태를 Open(열림)으로 변경할 수 있습니다. 그런 다음 필요에 따라 알림을 변경한 다음 추가 조사가 완료되면 알림을 닫을 수 있습니다.

종료된 알림을 다시 엽니다.

- 닫힌 알림의 세부 사항에서 **Reopen Alert(**알림 다시 열기**)**를 클릭합니다.

# 알림 우선순위 수정

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

알림 유형은 기본 우선순위와 함께 제공되며, 이는 시스템이 이 유형의 알림 생성에 대한 민감도에 영향을 미칩니다. 알림은 기본적으로 Cisco 인텔리전스 및 기타 요인에 따라 낮음 또는 보통으로 설정됩니다. 네트워크 환경에 따라 알림 유형의 우선순위를 다시 지정하여 우려되는 특정 알림을 강조할 수 있습니다. 모든 알림 유형을 낮음, 보통 또는 높음 우선순위로 구성할 수 있습니다.

- **Monitor(**모니터링**)** > **Alerts(**알림**)**를 선택합니다.
- Settings(설정) 드롭다운 아이콘()을 클릭한 다음 **Alert Types and Priorities(**알림 유형 및 우선순위**)**를 선택합니다.
- 알림 유형 옆에 있는 편집 아이콘()을 클릭하고 낮음, 중간 또는 높음을 선택하여 우선순위를 변경합니다.

# 라이브 이벤트 보기

Live events(라이브 이벤트) 페이지에는 입력한 이벤트 로깅 페이지에서 이벤트 검색 및 필터링과 일치하는 최신 500개의 이벤트가 표시됩니다. 라이브 이벤트 페이지에 최대 500개의 이벤트가 표시되고 더 많은 이벤트가 스트리밍되는 경우, CDO는 최신 라이브 이벤트를 표시하고 가장 오래된 라이브 이벤트를 기록 이벤트 페이지로 전송하여 총 라이브 이벤트 수를 500개로 유지합니다. 이 전송을 수행하는 데 약 1분이 걸립니다. 필터링 기준이 추가되지 않은 경우, 이벤트를 로깅하도록 구성된 규칙에 의해 생성된 모든 최신 라이브 500 이벤트가 표시됩니다.

이벤트의 타임스탬프는 이벤트를 보는 CDO 관리자의 현지 시간으로 표시됩니다.

라이브 이벤트가 재생 중인지 일시 중지되었는지에 상관없이 필터링 기준을 변경하면 이벤트 화면이 지워지고 수집 프로세스가 다시 시작됩니다.

CDO 이벤트 뷰어에서 라이브 이벤트를 보려면 다음을 수행합니다.

단계 **1** 탐색창에서 분석 > 이벤트 로깅를 선택합니다.

단계 **2** **Live(**라이브**)** 탭을 클릭합니다.

### What to do next

이벤트를 재생하고 일시 중지하는 방법을 참조하십시오.

관련 정보:

- 라이브 이벤트 재생/일시 중지, on page 471
- 과거 이벤트 보기, on page 472
- 이벤트 보기 사용자 지정, on page 472

# 라이브 이벤트 재생/일시 중지

라이브 이벤트가 스트리밍될 때 라이브 이벤트를 "재생" ▶ 또는 "일시 중지" ⏸ 할 수 있습니다. 라이브 이벤트가 "재생" 중인 경우 CDO는 이벤트 뷰어에 지정된 필터링 기준과 일치하는 이벤트를 수신된 순서대로 표시합니다. 이벤트가 일시 중지된 경우 CDO는 라이브 이벤트 재생을 다시 시작할 때까지 라이브 이벤트 페이지를 업데이트하지 않습니다. 이벤트 재생을 다시 시작하면 CDO는 이벤트 재생을 다시 시작한 시점부터 Live(라이브) 페이지에 이벤트를 채우기 시작합니다. 누락된 항목은 다시 채우지 않습니다.

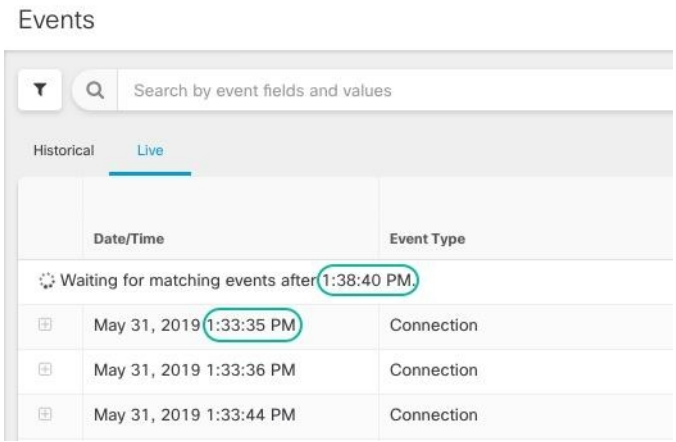
라이브 이벤트 스트리밍을 재생하거나 일시 중지했는지 여부에 관계없이 CDO가 수신한 모든 이벤트를 보려면 Historical(기록) 탭을 클릭합니다.

라이브 이벤트 자동 일시 중지

약 5분 동안 이벤트를 표시한 후 CDO는 라이브 이벤트의 스트림을 일시 중지한다고 경고합니다. 이때 링크를 클릭하여 다른 5분 동안 라이브 이벤트 스트리밍을 계속하거나 스트림을 중지할 수 있습니다. 준비가 되면 라이브 이벤트 스트림을 다시 시작할 수 있습니다.

이벤트 수신 및 보고

라이브 이벤트 뷰어에서 SEC(Secure Event Connector) 수신 이벤트와 CDO 게시 이벤트 사이에 약간의 지연이 발생할 수 있습니다. Live(라이브) 페이지에서 간격을 볼 수 있습니다. 이벤트의 타임스탬프는 SEC에서 이벤트를 수신한 시간입니다.



# 과거 이벤트 보기

Live events(라이브 이벤트) 페이지에는 입력한 이벤트 로깅 페이지에서 이벤트 검색 및 필터링과 일치하는 최신 500개의 이벤트가 표시됩니다. 가장 최근의 500개 이벤트보다 오래된 이벤트는 기록 이벤트 테이블로 전송됩니다. 이 전송을 수행하는 데 약 1분이 걸립니다. 그런 다음 저장한 모든 이벤트를 필터링하여 원하는 이벤트를 찾을 수 있습니다.

과거 이벤트를 보려면:

단계 **1** 탐색창에서 분석 > 이벤트 로깅를 선택합니다.

단계 **2** 기록 탭을 클릭합니다. 기본적으로 기록 이벤트 테이블을 열면 지난 1시간 내에 수집된 이벤트가 표시되도록 필터가 설정됩니다.

이벤트 속성은 FDM(Firepower Device Manager) 또는 ASDM(Adaptive Security Device Manager)에서 보고하는 것과 거의 동일합니다.

- Firepower Threat Defense 이벤트 속성에 대한 전체 설명은 Cisco FTD 시스템 로그 메시지를 참조하십시오.
- ASA 이벤트 속성에 대한 전체 설명은 Cisco ASA Series 시스템 로그 메시지를 참조하십시오.

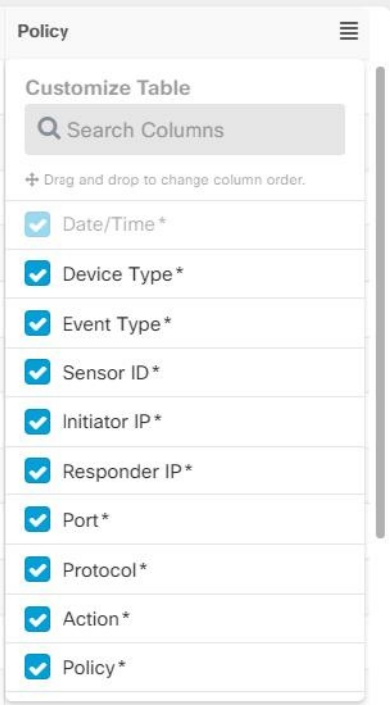
# 이벤트 보기 사용자 지정

Event Logging(이벤트 로깅) 페이지에 대한 모든 변경 사항은 이 페이지에서 빠져나왔다가 나중에 다시 돌아올 때를 위해 자동으로 저장됩니다.

**Note** 라이브 및 기록 이벤트 보기의 구성은 동일합니다. 이벤트 보기를 사용자 정의하면 이러한 변경 사항이 Live(라이브) 및 Historical(기록) 보기에 모두 적용됩니다.

열

원하는 보기에 적용되는 열 헤더만 포함하도록 라이브 및 기록 이벤트에 대한 이벤트 보기를 수정할 수 있습니다. 열 오른쪽에 있는 열 필터 아이콘 을 클릭하고 원하는 열을 선택하거나 선택 취소합니다.




별표가 있는 열은 언제든지 제거할 수 있지만 기본적으로 이벤트 테이블 내에 제공됩니다. 검색 창을 사용하여 포함할 추가 열에 대한 키워드를 수동으로 검색합니다.

순서

Events(이벤트) 보기의 열 순서를 바꿀 수 있습니다. 열 오른쪽에 있는 열 필터 아이콘 ≣ 을 클릭하여 선택한 열 목록을 확장하고 원하는 순서로 열을 수동으로 끌어서 놓습니다. 여기서 드롭다운 메뉴의 목록 맨 위에 있는 열은 이벤트 보기에서 맨 왼쪽에 있는 열입니다.

관련 정보:

- 이벤트 로깅 페이지에서 이벤트 검색 및 필터링
- Security Analytics and Logging의 이벤트 속성

# 이벤트 로깅 페이지의 열 표시 및 숨기기

Event Logging(이벤트 로깅) 페이지에는 구성된 ASA 및 FDM 관리 디바이스에서 Cisco Cloud로 전송된 ASA 및 FTD Syslog 이벤트 및 ASA NSEL(NetFlow Secure Event Logging) 이벤트가 표시됩니다.

테이블과 함께 Show/Hide(표시/숨기기) 위젯을 사용하여 Event Logging(이벤트 로깅) 페이지에서 열을 표시하거나 숨길 수 있습니다.

단계 **1** CDO 탐색 모음에서 분석 > 이벤트 로깅를 선택합니다.

단계 **2** 테이블의 맨 오른쪽으로 스크롤하여 **Show/Hide Columns(**열 표시/숨기기**)** 버튼 ≣를 클릭합니다.

단계 **3** 표시하려는 열을 선택하고, 숨기려는 열을 선택 취소합니다.

단계 **4** Show/Hide Columns(열 표시/숨기기) 드롭다운 메뉴의 열 이름 위에 마우스를 올려 놓고 회색 십자 표시를 눌러 열 순서를 다시 정렬합니다.

---

테넌트에 로그인하는 다른 사용자는 열이 다시 표시되거나 숨겨질 때까지 표시하도록 선택한 것과 동일한 열을 볼 수 있습니다.

이 표에서는 열 헤더에 대해 설명합니다.

| 열 헤더 | 설명 |
|---|---|
| 날짜/시간 | 디바이스가 이벤트를 생성한 시간 시간은 컴퓨터의 로컬 시간으로 표시됩니다. |
| 디바이스 유형 | ASA(Adaptive Security Appliance)<br>또는<br>FTD(Firepower Threat Defense) |

| 열 헤더 | 설명 |
| --- | --- |
| 이벤트 유형 | 이 복합 열에는 다음 중 하나가 포함될 수 있습니다.<br>• **FTD** 이벤트 유형<br>• Connection(연결) - 액세스 제어 규칙의 연결 이벤트를 표시합니다.<br>• File(파일) - 액세스 제어 규칙의 파일 정책에 의해 보고된 이벤트를 표시합니다.<br>• Intrusion(침입) - 액세스 제어 규칙의 침입 정책에 의해 보고된 이벤트를 표시합니다.<br>• Malware(악성코드) - 액세스 제어 규칙의 악성코드 정책에 의해 보고된 이벤트를 표시합니다.<br>• ASA**Event Types(**이벤트 유형**)** -이러한 이벤트 유형은 Syslog 또는 NetFlow 이벤트의 그룹을 나타냅니다. 어떤 Syslog ID 또는 어떤 NetFlow ID가 어떤 그룹에 포함되어 있는지에 대한 자세한 내용은 ASA 이벤트 유형을 참조하십시오.<br>• 구문 분석된 이벤트 - 구문 분석된 Syslog 이벤트는 다른 Syslog 이벤트보다 더 많은 이벤트 속성을 포함하며, CDO는 이러한 속성을 기반으로 더 빠르게 검색 결과를 반환할 수 있습니다. 구문 분석된 이벤트는 필터링 카테고리가 아닙니다. 그러나 구문 분석된 이벤트 ID는 Event Types(이벤트 유형) 열에 기울임꼴로 표시됩니다. 기울임꼴로 표시되지 않은 이벤트 ID는 구문 분석되지 않습니다.<br>• ASA NetFlow Event IDs(NetFlow 이벤트 ID): ASA의 모든 Netflow(NSEL) 이벤트가 여기에 표시됩니다. |
| 센서 ID | 센서 ID는 이벤트가 보안 이벤트 커넥터로 전송되는 IP 주소입니다. 이는 일반적으로 Firepower Threat Defense 또는 ASA의 관리 인터페이스입니다. |

| 열 헤더 | 설명 |
| --- | --- |
| 초기자 IP | 이는 네트워크 트래픽 소스의 IP 주소입니다. Initiator address(이니시에이터 주소) 필드의 값은 이벤트 세부사항의 InitiatorIP(이니시에이터 IP) 필드 값에 해당합니다. 단일 주소(예: 10.10.10.100) 또는 CIDR 표기법으로 정의된 네트워크(예: 10.10.10.0/24)를 입력할 수 있습니다. |
| 응답기 IP | 이것은 패킷의 대상 IP 주소입니다. Destination address(대상 주소) 필드의 값은 이벤트 세부사항의 ResponderIP 필드에 있는 값에 해당합니다. 단일 주소(예: 10.10.10.100) 또는 CIDR 표기법으로 정의된 네트워크(예: 10.10.10.0/24)를 입력할 수 있습니다. |
| 포트 | 세션 **responder**가 사용하는 포트 또는 ICMP 코드 대상 포트의 값은 이벤트 세부사항의 **ResponderPort** 값에 해당합니다. |
| 프로토콜 | 이벤트의 프로토콜을 나타냅니다. |

| 열 헤더 | 설명 |
| --- | --- |
| 작업 | 규칙에 의해 정의된 보안 작업을 지정합니다. 입력하는 값은 찾으려는 값과 정확히 일치해야 합니다. 그러나 대/소문자는 중요하지 않습니다. 연결, 파일, 침입, 악성코드, Syslog 및 NetFlow 이벤트 유형에 대해 서로 다른 값을 입력합니다.<br>• 연결 이벤트 유형의 경우 필터는 AC_RuleAction 특성에서 일치 항목을 검색합니다. 이러한 값은 Allow(허용), Block(차단), Trust(신뢰)일 수 있습니다.<br>• 파일 이벤트 유형의 경우 필터는 FileAction 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Allow(허용), Block(차단), Trust(신뢰)일 수 있습니다.<br>• 침입 이벤트 유형의 경우 필터는 InLineResult 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Allowed(허용됨), Blocked(차단됨), Trusted(신뢰할 수 있음)일 수 있습니다.<br>• 악성코드 이벤트 유형의 경우 필터는 FileAction 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Cloud Lookup Timeout(클라우드 조회 시간 초과)일 수 있습니다.<br>• Syslog 및 NetFlow 이벤트 유형의 경우 필터는 Action(작업) 속성에서 일치하는 항목을 검색합니다. |
| 정책 | 이벤트를 트리거한 정책의 이름입니다. ASA 및 FDM 관리디바이스의 이름은 다릅니다. |

관련 정보:

이벤트 로깅 페이지에서 이벤트 검색 및 필터링, on page 509

# 사용자 지정 가능한 이벤트 필터

SaaS(Secure Logging Analytics) 고객은 자주 사용하는 맞춤형 필터를 생성하고 저장할 수 있습니다.

필터의 요소는 구성할 때 필터 탭에 저장됩니다. Event Logging(이벤트 로깅) 페이지로 돌아갈 때마다 이러한 검색을 사용할 수 있습니다. 테넌트의 다른 CDO 사용자는 사용할 수 없습니다. 둘 이상의 테넌트를 관리하는 경우 다른 테넌트에서는 사용할 수 없습니다.

**Note** 필터 탭에서 작업할 때 필터 기준을 수정하면 해당 변경 사항이 사용자 지정 필터 탭에 자동으로 저장됩니다.

단계 **1** 주 메뉴에서 분석 > 이벤트 로깅을(를) 선택합니다.

단계 **2** 모든 값의 Search(검색) 필드를 지웁니다.

단계 **3** 이벤트 테이블 위에서 파란색 더하기 버튼을 클릭하여 View(보기) 탭을 추가합니다. 필터 보기에는 이름을 지정할 때까지 "View 1", "View 2", "View 3" 등의 레이블이 지정됩니다.


단계 **4** View(보기) 탭을 선택합니다.

단계 **5** 필터 표시줄을 열고 맞춤형 필터에서 원하는 필터 속성을 선택합니다. 이벤트 로깅 페이지에서 이벤트 검색 및 필터링, on page 509의 내용을 참조하십시오. 필터 특성만 맞춤형 필터에 저장됩니다.

단계 **6** 이벤트 로깅 테이블에 표시할 열을 사용자 정의합니다. 열 표시 및 숨기기에 대한 설명은 이벤트 로깅 페이지의 열 표시 및 숨기기, on page 473의 내용을 참조하십시오.

단계 **7** "View X" 레이블이 있는 필터 탭을 두 번 클릭하고 이름을 바꿉니다.

단계 **8** (선택 사항) 맞춤형 필터를 생성했으므로 이제 Search(검색) 필드에 검색 기준을 추가하여 맞춤형 필터를 변경하지 않고도 Event Logging(이벤트 로깅) 페이지에 표시되는 결과를 미세 조정할 수 있습니다. 이벤트 로깅 페이지에서 이벤트 검색 및 필터링, on page 509의 내용을 참조하십시오.

# Security Analytics and Logging의 이벤트 속성

이벤트 속성 설명

CDO에서 사용하는 이벤트 속성은 FDM(Firepower Device Manager) 또는 ASDM(Adaptive Security Device Manager)에서 보고하는 것과 거의 동일합니다.

- ASA(Adaptive Security Appliance) 이벤트 속성에 대한 전체 설명은 Cisco ASA Series 시스템 로그 메시지를 참조하십시오.

일부 ASA 시스템 로그 이벤트는 "구문 분석"되며, 다른 이벤트에는 속성:값 쌍을 사용하여 이벤트 로깅 테이블의 내용을 필터링할 때 사용할 수 있는 추가 속성이 있습니다. 시스템 로그 이벤트의 다른 중요한 속성은 다음 추가 항목을 참조하십시오.

- 구문 분석된 ASA 시스템 로그 이벤트
- 일부 시스템 로그 메시지에 대한 EventGroup 및 EventGroupDefinition 속성
- Syslog 이벤트에 대한 이벤트 이름 속성

• 시스템 로그 이벤트의 시간 속성

# 일부 시스템 로그 메시지에 대한 EventGroup 및 EventGroupDefinition 속성

일부 시스템 로그 이벤트에는 추가 속성 "EventGroup" 및 "EventGroupDefinition"이 있습니다. attribute:value 쌍을 기준으로 필터링하여 이러한 추가 속성을 사용하여 이벤트 테이블을 필터링할 수 있습니다. 예를 들어 Event Logging(이벤트 로깅) 테이블의 검색 필드에 `apfw:415*`를 입력하여 애플리케이션 방화벽 이벤트를 필터링할 수 있습니다.

**Syslog** 메시지 클래스와 연결된 메시지 **ID** 번호

| **EventGroup** | **EventGroupDefinition** | 시스템 로그 메시지 **ID** 번호**(**처음 **3**자리**)** |
|---|---|---|
| aaa/auth | 사용자 인증 | 109, 113 |
| acl/session | 액세스 목록/사용자 세션 | 106 |
| apfw | 애플리케이션 방화벽 | 415 |
| bridge | 투명한 방화벽 | 110, 220 |
| ca | PKI 인증 기관 | 717 |
| citrix | Citrix 클라이언트 | 723 |
| clst | 클러스터링 | 747 |
| cmgr | 카드 관리 | 323 |
| config | CLI(Command Line Interface) | 111, 112, 208, 308 |
| csd | Secure Desktop | 724 |
| cts | Cisco TrustSec | 776 |
| dap | Dynamic Access Policy | 734 |
| eap, eapoudp | Network Admission Control용 EAPoUDP 또는 EAP | 333, 334 |
| eigrp | EIGRP 라우팅 | 336 |
| email | 이메일 프록시 | 719 |
| ipaa/envmon | 환경 모니터링 | 735 |
| HA | 페일오버 | 101, 102, 103, 104, 105, 210, 311, 709 |
| idfw | ID 기반 방화벽 | 746 |
| ids | Intrusion Detection System(침입 탐지 시스템) | 733 |

| **EventGroup** | **EventGroupDefinition** | 시스템 로그 메시지 **ID** 번호**(**처음 **3**자리**)** |
|---|---|---|
| ids/ips | 침입 탐지 시스템/침입 방지 시스템 | 400 |
| ikev2 | IKEv2 툴킷 | 750, 751, 752 |
| ip | IP 스택 | 209, 215, 313, 317, 408 |
| ipaa | IP 주소 할당 | 735 |
| ips | Intrusion Protection System(침입 방지 시스템) | 401, 420 |
| ipv6 | IPv6 | 325 |
| l4tm | 차단 목록, 허용 목록, 그레이리스트 | 338 |
| lic | 라이선싱 | 444 |
| mdm-proxy | MDM 프록시 | 802 |
| nac | NAC(Network Admission Control) | 731, 732 |
| vpn/nap | IKE 및 IPsec/네트워크 액세스 포인트 | 713 |
| np | 네트워크 프로세서 | 319 |
| ospf | OSPF 라우팅 | 318, 409, 503, 613 |
| passwd | 비밀번호 암호화 | 742 |
| PP | 전화 프록시 | 337 |
| rip | RIP 라우팅 | 107, 312 |
| rm | 리소스 관리자 | 321 |
| sch | Smart Call Home | 120 |
| session | 사용자 세션 | 108, 201, 202, 204, 302, 303, 304, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710 |
| session/natpat | 사용자 세션/NAT 및 PAT | 305 |
| snmp | SNMP | 212 |
| ssafe | ScanSafe | 775 |
| ssl/np ssl | SSL 스택/NP SSL | 725 |
| svc | SSL VPN 클라이언트 | 722 |

| EventGroup | EventGroupDefinition | 시스템 로그 메시지 ID 번호(처음 3자리) |
|---|---|---|
| sys | 시스템 | 199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615, 701, 711, 741 |
| tre | 트랜잭션 규칙 엔진 | 780 |
| ucime | UC-IME | 339 |
| tag-switching | 서비스 태그 스위칭 | 779 |
| td | 위협 탐지 | 733 |
| VM | VLAN 매핑 | 730 |
| vpdn | PPTP 및 L2TP 세션 | 213, 403, 603 |
| vpn | IKE 및 IPSEC | 316, 320, 404, 501, 602, 402 |
| vpnc | VPN 클라이언트 | 611 |
| vpnfo | VPN 페일오버 | 720 |
| vpnlb | VPN 로드 밸런싱 | 718 |
| vxlan | VXLAN | 778 |
| webfo | WebVPN 페일오버 | 721 |
| webvpn | WebVPN 및 AnyConnect Client | 716 |
| session/natpat | 사용자 세션/NAT 및 PAT | 305 |

# Syslog 이벤트에 대한 이벤트 이름 속성

일부 시스템 로그 이벤트에는 추가 속성 "EventName"이 있습니다. attribute:value 쌍을 기준으로 필터링하여 EventName 특성을 사용하여 이벤트 테이블을 필터링하여 찾을 수 있습니다. 예를 들어 Event Logging(이벤트 로깅) 테이블의 검색 필드에 **EventName:"Denied IP Packet"**을 입력하여 "Denied IP packet(거부된 IP 패킷)"에 대한 이벤트를 필터링할 수 있습니다.

시스템 로그 이벤트 **ID** 및 이벤트 이름 테이블

- AAA 시스템 로그 이벤트 ID 및 이벤트 이름
- 봇넷 시스템 로그 이벤트 ID 및 이벤트 이름
- 페일오버 시스템 로그 이벤트 ID 및 이벤트 이름
- 방화벽 거부 시스템 로그 이벤트 ID 및 이벤트 이름
- 방화벽 트래픽 시스템 로그 이벤트 ID 및 이벤트 이름
- ID 기반 방화벽 시스템 로그 이벤트 ID 및 이벤트 이름

- IPSec 시스템 로그 이벤트 ID 및 이벤트 이름
- NAT 시스템 로그 이벤트 ID 및 이벤트 이름
- SSL VPN 시스템 로그 이벤트 ID 및 이벤트 이름

**AAA** 시스템 로그 이벤트 **ID** 및 이벤트 이름

| 이벤트 **ID** | 이벤트 이름 |
|---|---|
| 109001 | AAA Begin |
| 109002 | AAA Failed |
| 109003 | AAA Server Failed |
| 109005 | Authentication Success |
| 109006 | Authentication Failed |
| 109007 | Authorization Success |
| 109008 | Authorization Failed |
| 109010 | AAA Pending |
| 109011 | AAA Session Started |
| 109012 | AAA Session Ended |
| 109013 | AAA |
| 109014 | AAA Failed |
| 109016 | AAA ACL not found |
| 109017 | AAA Limit Reach |
| 109018 | AAA ACL Empty |
| 109019 | AAA ACL error |
| 109020 | AAA ACL error |
| 109021 | AAA error |
| 109022 | AAA HTTP limit reached |
| 109023 | AAA auth required |
| 109024 | Authorization Failed |
| 109025 | Authorization Failed |
| 109026 | AAA error |
| 109027 | AAA Server error |

| 이벤트 **ID** | 이벤트 이름 |
|---|---|
| 109028 | AAA Bypassed |
| 109029 | AAA ACL error |
| 109030 | AAA ACL error |
| 109031 | Authentication Failed |
| 109032 | AAA ACL error |
| 109033 | Authentication Failed |
| 109034 | Authentication Failed |
| 109035 | AAA Limit Reach |
| 113001 | AAA Session limit reach |
| 113003 | AAA overridden |
| 113004 | AAA Successful |
| 113005 | Authorization Rejected |
| 113006 | AAA user locked |
| 113007 | AAA User unlocked |
| 113008 | AAA successful |
| 113009 | AAA retrieved |
| 113010 | AAA Challenge received |
| 113011 | AAA retrieved |
| 113012 | Authentication Successful |
| 113013 | AAA error |
| 113014 | AAA error |
| 113015 | Authentication Rejected |
| 113016 | AAA Rejected |
| 113017 | AAA Rejected |
| 113018 | AAA ACL error |
| 113019 | AAA Disconnected |
| 113020 | AAA error |
| 113021 | AAA Logging Fail |

| 이벤트 **ID** | 이벤트 이름 |
|---|---|
| 113022 | AAA Failed |
| 113023 | AAA reactivated |
| 113024 | AAA Client certification |
| 113025 | AAA Authentication fail |
| 113026 | AAA error |
| 113027 | AAA error |

봇넷 시스템 로그 이벤트 **ID** 및 이벤트 이름

| 이벤트 **ID** | 이벤트 이름 |
|---|---|
| 338001 | Botnet Source Block List |
| 338002 | Botnet Destination Block List |
| 338003 | Botnet Source Block List |
| 338004 | Botnet Destination Block List |
| 338101 | Botnet Source Allow List |
| 338102 | Botnet destination Allow List |
| 338202 | Botnet destination Grey |
| 338203 | Botnet Source Grey |
| 338204 | Botnet Destination Grey |
| 338301 | Botnet DNS Intercepted |
| 338302 | Botnet DNS |
| 338303 | Botnet DNS |
| 338304 | Botnet Download successful |
| 338305 | Botnet Download failed |
| 338306 | Botnet Authentication failed |
| 338307 | Botnet Decrypt failed |
| 338308 | Botnet Client |
| 338309 | Botnet Client |
| 338310 | Botnet dyn filter failed |

페일오버 시스템 로그 이벤트 **ID** 및 이벤트 이름

| 이벤트 **ID** | 이벤트 이름 |
|---|---|
| 101001 | Failover Cable OK |
| 101002 | Failover Cable BAD |
| 101003 | Failover Cable not connected |
| 101004 | Failover Cable not connected |
| 101005 | Failover Cable reading error |
| 102001 | Failover Power failure |
| 103001 | No response from failover mate |
| 103002 | Failover mate interface OK |
| 103003 | Failover mate interface BAD |
| 103004 | Failover mate reports failure |
| 103005 | Failover mate reports self failure |
| 103006 | Failover version incompatible |
| 103007 | Failover version difference |
| 104001 | Failover role switch |
| 104002 | Failover role switch |
| 104003 | Failover unit failed |
| 104004 | Failover unit OK |
| 106100 | Permit/Denied by ACL |
| 210001 | Stateful Failover error |
| 210002 | Stateful Failover error |
| 210003 | Stateful Failover error |
| 210005 | Stateful Failover error |
| 210006 | Stateful Failover error |
| 210007 | Stateful Failover error |
| 210008 | Stateful Failover error |
| 210010 | Stateful Failover error |
| 210020 | Stateful Failover error |

| 이벤트 **ID** | 이벤트 이름 |
|---|---|
| 210021 | Stateful Failover error |
| 210022 | Stateful Failover error |
| 311001 | Stateful Failover update |
| 311002 | Stateful Failover update |
| 311003 | Stateful Failover update |
| 311004 | Stateful Failover update |
| 418001 | Denied Packet to Management |
| 709001 | Failover replication error |
| 709002 | Failover replication error |
| 709003 | Failover replication start |
| 709004 | Failover replication complete |
| 709005 | Failover receive replication start |
| 709006 | Failover receive replication complete |
| 709007 | Failover replication failure |
| 710003 | Denied access to Device |

방화벽 거부 시스템 로그 이벤트 **ID** 및 이벤트 이름

| 이벤트 **ID** | 이벤트 이름 |
|---|---|
| 106001 | Denied by Security Policy |
| 106002 | Outbound Deny |
| 106006 | Denied by Security Policy |
| 106007 | Denied Inbound UDP |
| 106008 | Denied by Security Policy |
| 106010 | Denied by Security Policy |
| 106011 | Denied Inbound |
| 106012 | Denied due to Bad IP option |
| 106013 | Dropped Ping to PAT IP |
| 106014 | Denied Inbound ICMP |

| 이벤트 **ID** | 이벤트 이름 |
|---|---|
| 106015 | Denied by Security Policy |
| 106016 | Denied IP Spoof |
| 106017 | Denied due to Land Attack |
| 106018 | Denied outbound ICMP |
| 106020 | Denied IP Packet |
| 106021 | Denied TCP |
| 106022 | Denied Spoof packet |
| 106023 | Denied IP Packet |
| 106025 | Dropped Packet failed to Detect context |
| 106026 | Dropped Packet failed to Detect context |
| 106027 | Dropped Packet failed to Detect context |
| 106100 | Permit/Denied by ACL |
| 418001 | Denied Packet to Management |
| 710003 | Denied access to Device |

방화벽 트래픽 시스템 로그 이벤트 **ID** 및 이벤트 이름

| 이벤트 **ID** | 이벤트 이름 |
|---|---|
| 108001 | Inspect SMTP |
| 108002 | Inspect SMTP |
| 108003 | Inspect ESMTP Dropped |
| 108004 | Inspect ESMTP |
| 108005 | Inspect ESMTP |
| 108006 | Inspect ESMTP Violation |
| 108007 | Inspect ESMTP |
| 110002 | No Router found |
| 110003 | Failed to Find Next hop |
| 209003 | Fragment Limit Reach |
| 209004 | Fragment invalid Length |

| 이벤트 ID | 이벤트 이름 |
|---|---|
| 209005 | Fragment IP discard |
| 302003 | H245 Connection Start |
| 302004 | H323 Connection start |
| 302009 | Restart TCP |
| 302010 | Connection USAGE |
| 302012 | H225 CALL SIGNAL CONN |
| 302013 | Built TCP |
| 302014 | Teardown TCP |
| 302015 | Built UDP |
| 302016 | Teardown UDP |
| 302017 | Built GRE |
| 302018 | Teardown GRE |
| 302019 | H323 Failed |
| 302020 | Built ICMP |
| 302021 | Teardown ICMP |
| 302022 | Built TCP Stub |
| 302023 | Teardown TCP Stub |
| 302024 | Built UDP Stub |
| 302025 | Teardown UDP Stub |
| 302026 | Built ICMP Stub |
| 302027 | Teardown ICMP Stub |
| 302033 | Connection H323 |
| 302034 | H323 Connection Failed |
| 302035 | Built SCTP |
| 302036 | Teardown SCTP |
| 303002 | FTP file download/upload |
| 303003 | Inspect FTP Dropped |
| 303004 | Inspect FTP Dropped |

| 이벤트 **ID** | 이벤트 이름 |
|---|---|
| 303005 | Inspect FTP reset |
| 313001 | ICMP Denied |
| 313004 | ICMP Drop |
| 313005 | ICMP Error Msg Drop |
| 313008 | ICMP ipv6 Denied |
| 324000 | GTP Pkt Drop |
| 324001 | GTP Pkt Error |
| 324002 | Memory Error |
| 324003 | GTP Pkt Drop |
| 324004 | GTP Version 지원하지 않음 |
| 324005 | GTP Tunnel Failed |
| 324006 | GTP Tunnel Failed |
| 324007 | GTP Tunnel Failed |
| 337001 | Phone Proxy SRTP Failed |
| 337002 | Phone Proxy SRTP Failed |
| 337003 | Phone Proxy SRTP Auth Fail |
| 337004 | Phone Proxy SRTP Auth Fail |
| 337005 | Phone Proxy SRTP no Media Session |
| 337006 | Phone Proxy TFTP Unable to Create File |
| 337007 | Phone Proxy TFTP Unable to Find File |
| 337008 | Phone Proxy Call Failed |
| 337009 | Phone Proxy Unable to Create Phone Entry |
| 400000 | IPS IP options-Bad Option List |
| 400001 | IPS IP options-Record Packet Route |
| 400002 | IPS IP options-Timestamp |
| 400003 | IPS IP options-Security |
| 400004 | IPS IP options-Loose Source Route |
| 400005 | IPS IP options-SATNET ID |

| 이벤트 ID | 이벤트 이름 |
|---|---|
| 400006 | IPS IP options-Strict Source Route |
| 400007 | IPS IP Fragment Attack |
| 400008 | IPS IP Impossible Packet |
| 400009 | IPS IP Fragments Overlap |
| 400010 | IPS ICMP Echo Reply |
| 400011 | IPS ICMP Host Unreachable |
| 400012 | IPS ICMP Source Quench |
| 400013 | IPS ICMP Redirect |
| 400014 | IPS ICMP Echo Request |
| 400015 | IPS ICMP Time Exceeded for a Datagram |
| 400017 | IPS ICMP Timestamp Request |
| 400018 | IPS ICMP Timestamp Reply |
| 400019 | ICMP Information Request |
| 400020 | IPS ICMP Information Reply |
| 400021 | ICMP Address Mask Request |
| 400022 | ICMP Address Mask Request |
| 400023 | IPS Fragmented ICMP Traffic |
| 400024 | IPS Large ICMP Traffic |
| 400025 | IPS Ping of Death Attack |
| 400026 | IPS TCP NULL flags |
| 400027 | IPS TCP SYN+FIN flags |
| 400028 | IPS TCP FIN only flags |
| 400029 | IPS FTP Improper Address Specified |
| 400030 | IPS FTP Improper Port Specified |
| 400031 | IPS UDP Bomb attack |
| 400032 | IPS UDP Snork attack |
| 400033 | IPS UDP Chargen DoS attack |
| 400034 | IPS DNS HINFO Request |

| 이벤트 ID | 이벤트 이름 |
|---|---|
| 400035 | IPS DNS Zone Transfer |
| 400036 | IPS DNS Zone Transfer from High Port |
| 400037 | IPS DNS Request for All Records |
| 400038 | IPS RPC Port Registration |
| 400039 | IPS RPC Port Unregistration |
| 400040 | IPS RPC Dump |
| 400041 | IPS Proxied RPC Request |
| 400042 | IPS YP server Portmap Request |
| 400043 | IPS YP bind Portmap Request |
| 400044 | IPS YP password Portmap Request |
| 400045 | IPS YP update Portmap Request |
| 400046 | IPS YP transfer Portmap Request |
| 400047 | IPS Mount Portmap Request |
| 400048 | IPS Remote execution Portmap Request |
| 400049 | IPS Remote execution Attempt |
| 400050 | IPS Statd Buffer Overflow |
| 406001 | Inspect FTP Dropped |
| 406002 | Inspect FTP Dropped |
| 407001 | Host Limit Reach |
| 407002 | Embryonic limit Reached |
| 407003 | Established limit Reached |
| 415001 | Inspect Http Header Field Count |
| 415002 | Inspect Http Header Field Length |
| 415003 | Inspect Http body Length |
| 415004 | Inspect Http content-type |
| 415005 | Inspect Http URL length |
| 415006 | Inspect Http URL Match |
| 415007 | Inspect Http Body Match |

| 이벤트 ID | 이벤트 이름 |
|---|---|
| 415008 | Inspect Http Header match |
| 415009 | Inspect Http Method match |
| 415010 | Inspect transfer encode match |
| 415011 | Inspect Http Protocol Violation |
| 415012 | Inspect Http Content-type |
| 415013 | Inspect Http Malformed |
| 415014 | Inspect Http Mime-Type |
| 415015 | Inspect Http Transfer-encoding |
| 415016 | Inspect Http Unanswered |
| 415017 | Inspect Http Argument match |
| 415018 | Inspect Http Header length |
| 415019 | Inspect Http status Matched |
| 415020 | Inspect Http non-ASCII |
| 416001 | Inspect SNMP dropped |
| 419001 | Dropped packet |
| 419002 | Duplicate TCP SYN |
| 419003 | Packet modified |
| 424001 | Denied IP Packet |
| 424002 | Dropped Packet |
| 431001 | Dropped RTP |
| 431002. | Dropped RTCP |
| 500001 | Inspect ActiveX |
| 500002 | Inspect Java |
| 500003 | Inspect TCP Header |
| 500004 | Inspect TCP Header |
| 500005 | Inspect Connection Terminated |
| 508001 | Inspect DCERPC Dropped |
| 508002 | Inspect DCERPC Dropped |

| 이벤트 ID | 이벤트 이름 |
|---|---|
| 509001 | Prevented No Forward Cmd |
| 607001 | Inspect SIP |
| 607002 | Inspect SIP |
| 607003 | Inspect SIP |
| 608001 | Inspect Skinny |
| 608002 | Inspect Skinny dropped |
| 608003 | Inspect Skinny dropped |
| 608004 | Inspect Skinny dropped |
| 608005 | Inspect Skinny dropped |
| 609001 | Built Local-Host |
| 609002 | Teardown Local Host |
| 703001 | H225 Unsupported Version |
| 703002 | H225 Connection |
| 726001 | Inspect Instant Message |

**ID** 기반 방화벽 시스템 로그 이벤트 **ID** 및 이벤트 이름

| 이벤트 ID | 이벤트 이름 |
|---|---|
| 746001 | Import started |
| 746002 | Import complete |
| 746003 | Import failed |
| 746004 | Exceed user group limit |
| 746005 | AD Agent down |
| 746006 | AD Agent out of sync |
| 746007 | Netbios response failed |
| 746008 | Netbios started |
| 746009 | Netbios stopped |
| 746010 | Import user failed |
| 746011 | Exceed user limit |

| 이벤트 **ID** | 이벤트 이름 |
|---|---|
| 746012 | User IP add |
| 746013 | User IP delete |
| 746014 | FQDN Obsolete |
| 746015 | FQDN resolved |
| 746016 | DNS lookup failed |
| 746017 | Import user issued |
| 746018 | Import user done |
| 746019 | Update AD Agent failed |

**IPSec** 시스템 로그 이벤트 **ID** 및 이벤트 이름

| 이벤트 **ID** | 이벤트 이름 |
|---|---|
| 402114 | Invalid SPI received |
| 402115 | Unexpected protocol received |
| 402116 | Packet doesn't match identity |
| 402117 | Non-IPSEC packet received |
| 402118 | Invalid fragment offset |
| 402119 | Anti-Replay check failure |
| 402120 | Authentication failure |
| 402121 | Packet dropped |
| 426101 | cLACP Port Bundle |
| 426102 | cLACP Port Standby |
| 426103 | cLACP Port Moved To Bundle From Standby |
| 426104 | cLACP Port Unbundled |
| 602103 | Path MTU updated |
| 602104 | Path MTU exceeded |
| 602303 | New SA created |
| 602304 | SA deleted |
| 702305 | SA expiration - Sequence rollover |
| 702307 | SA expiration - Data rollover |

**NAT** 시스템 로그 이벤트 **ID** 및 이벤트 이름

| 이벤트 **ID** | 이벤트 이름 |
|---|---|
| 201002 | Max connection Exceeded for host |
| 201003 | Embryonic limit exceed |
| 201004 | UDP connection limit exceed |
| 201005 | FTP connection failed |
| 201006 | RCMD connection failed |
| 201008 | New connection Disallowed |
| 201009 | Connection Limit exceed |
| 201010 | Embryonic Connection limit exceeded |
| 201011 | Connection Limit exceeded |
| 201012 | Per-client embryonic connection limit exceeded |
| 201013 | Per-client connection limit exceeded |
| 202001 | Global NAT exhausted |
| 202005 | Embryonic connection error |
| 202011 | Connection Limit exceeded |
| 305005 | No NAT group found |
| 305006 | Translation failed |
| 305007 | Connection dropped |
| 305008 | NAT allocation issue |
| 305009 | NAT Created |
| 305010 | NAT teardown |
| 305011 | PAT created |
| 305012 | PAT teardown |
| 305013 | Connection denied |

**SSL VPN** 시스템 로그 이벤트 **ID** 및 이벤트 이름

| 이벤트 **ID** | 이벤트 이름 |
|---|---|
| 716001 | WebVPN Session Started |
| 716002 | WebVPN Session Terminated |
| 716003 | WebVPN User URL access |
| 716004 | WebVPN User URL access denied |
| 716005 | WebVPN ACL error |
| 716006 | WebVPN User Disabled |

| 이벤트 ID | 이벤트 이름 |
|---|---|
| 716007 | WebVPN Unable to Create |
| 716008 | WebVPN Debug |
| 716009 | WebVPN ACL error |
| 716010 | WebVPN User access network |
| 716011 | WebVPN User access |
| 716012 | WebVPN User Directory access |
| 716013 | WebVPN User file access |
| 716014 | WebVPN User file access |
| 716015 | WebVPN User file access |
| 716016 | WebVPN User file access |
| 716017 | WebVPN User file access |
| 716018 | WebVPN User file access |
| 716019 | WebVPN User file access |
| 716020 | WebVPN User file access |
| 716021 | WebVPN user access file denied |
| 716022 | WebVPN Unable to connect proxy |
| 716023 | WebVPN session limit reached |
| 716024 | WebVPN User access error |
| 716025 | WebVPN User access error |
| 716026 | WebVPN User access error |
| 716027 | WebVPN User access error |
| 716028 | WebVPN User access error |
| 716029 | WebVPN User access error |
| 716030 | WebVPN User access error |
| 716031 | WebVPN User access error |
| 716032 | WebVPN User access error |
| 716033 | WebVPN User access error |
| 716034 | WebVPN User access error |
| 716035 | WebVPN User access error |
| 716036 | WebVPN User login successful |
| 716037 | WebVPN User login failed |
| 716038 | WebVPN User Authentication Successful |

| 이벤트 ID | 이벤트 이름 |
|---|---|
| 716039 | WebVPN User Authentication Rejected |
| 716040 | WebVPN User logging denied |
| 716041 | WebVPN ACL hit count |
| 716042 | WebVPN ACL hit |
| 716043 | WebVPN Port forwarding |
| 716044 | WebVPN Bad Parameter |
| 716045 | WebVPN Invalid Parameter |
| 716046 | WebVPN connection terminated |
| 716047 | WebVPN ACL usage |
| 716048 | WebVPN memory issue |
| 716049 | WebVPN Empty SVC ACL |
| 716050 | WebVPN ACL error |
| 716051 | WebVPN ACL error |
| 716052 | WebVPN Session Terminated |
| 716053 | WebVPN SSO Server added |
| 716054 | WebVPN SSO Server deleted |
| 716055 | WebVPN Authentication Successful |
| 716056 | WebVPN Authentication Failed |
| 716057 | WebVPN Session terminated |
| 716058 | WebVPN Session lost |
| 716059 | WebVPN Session resumed |
| 716060 | WebVPN Session Terminated |
| 722001 | WebVPN SVC Connect request error |
| 722002 | WebVPN SVC Connect request error |
| 722003 | WebVPN SVC Connect request error |
| 722004 | WebVPN SVC Connect request error |
| 722005 | WebVPN SVC Connect update issue |
| 722006 | WebVPN SVC Invalid address |
| 722007 | WebVPN SVC Message |
| 722008 | WebVPN SVC Message |
| 722009 | WebVPN SVC Message |
| 722010 | WebVPN SVC Message |

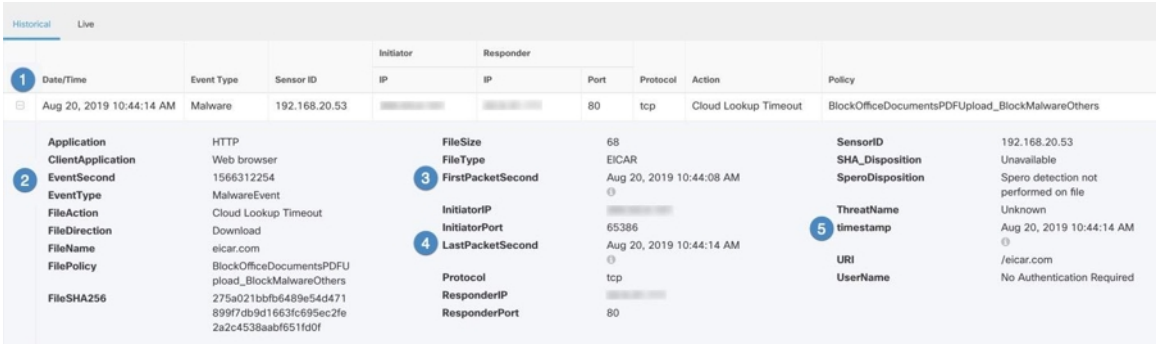
| 이벤트 ID | 이벤트 이름 |
|---|---|
| 722011 | WebVPN SVC Message |
| 722012 | WebVPN SVC Message |
| 722013 | WebVPN SVC Message |
| 722014 | WebVPN SVC Message |
| 722015 | WebVPN SVC invalid frame |
| 722016 | WebVPN SVC invalid frame |
| 722017 | WebVPN SVC invalid frame |
| 722018 | WebVPN SVC invalid frame |
| 722019 | WebVPN SVC Not Enough Data |
| 722020 | WebVPN SVC no address |
| 722021 | WebVPN Memory issue |
| 722022 | WebVPN SVC connection established |
| 722023 | WebVPN SVC connection terminated |
| 722024 | WebVPN Compression Enabled |
| 722025 | WebVPN Compression Disabled |
| 722026 | WebVPN Compression reset |
| 722027 | WebVPN Decompression reset |
| 722028 | WebVPN Connection Closed |
| 722029 | WebVPN SVC Session terminated |
| 722030 | WebVPN SVC Session terminated |
| 722031 | WebVPN SVC Session terminated |
| 722032 | WebVPN SVC connection Replacement |
| 722033 | WebVPN SVC Connection established |
| 722034 | WebVPN SVC New connection |
| 722035 | WebVPN Received Large packet |
| 722036 | WebVPN transmitting Large packet |
| 722037. | WebVPN SVC connection closed |
| 722038 | WebVPN SVC session terminated |
| 722039 | WebVPN SVC invalid ACL |
| 722040 | WebVPN SVC invalid ACL |
| 722041 | WebVPN SVC IPv6 not available |
| 722042 | WebVPN invalid protocol |

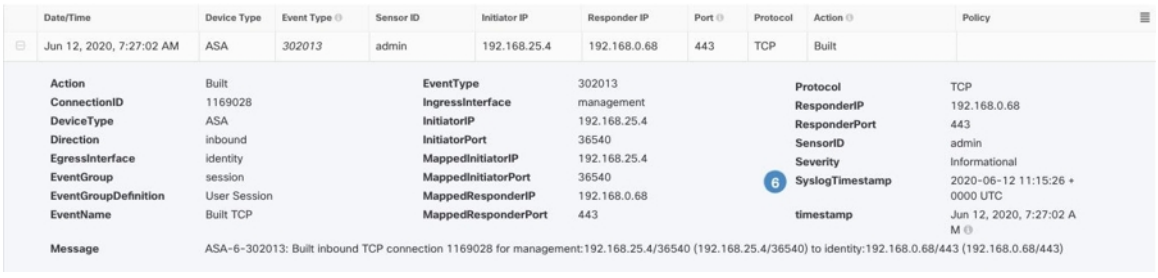
| 이벤트 ID | 이벤트 이름 |
|---|---|
| 722043 | WebVPN DTLS disabled |
| 722044 | WebVPN unable to request address |
| 722045 | WebVPN Connection terminated |
| 722046 | WebVPN Session terminated |
| 722047 | WebVPN Tunnel terminated |
| 722048 | WebVPN Tunnel terminated |
| 722049 | WebVPN Session terminated |
| 722050 | WebVPN Session terminated |
| 722051 | WebVPN address assigned |
| 722053 | WebVPN Unknown client |
| 723001 | WebVPN Citrix connection Up |
| 723002 | WebVPN Citrix connection Down |
| 723003 | WebVPN Citrix no memory issue |
| 723004 | WebVPN Citrix bad flow control |
| 723005 | WebVPN Citrix no channel |
| 723006 | WebVPN Citrix SOCKS error |
| 723007 | WebVPN Citrix connection list broken |
| 723008 | WebVPN Citrix invalid SOCKS |
| 723009 | WebVPN Citrix invalid connection |
| 723010 | WebVPN Citrix invalid connection |
| 723011 | WebVPN citrix Bad SOCKS |
| 723012 | WebVPN Citrix Bad SOCKS |
| 723013 | WebVPN Citrix invalid connection |
| 723014 | WebVPN Citrix connected to Server |
| 724001 | WebVPN Session not allowed |
| 724002 | WebVPN Session terminated |
| 724003 | WebVPN CSD |
| 724004 | WebVPN CSD |
| 725001 | SSL handshake Started |
| 725002 | SSL Handshake completed |
| 725003 | SSL Client session resume |
| 725004 | SSL Client request Authentication |

| 이벤트 **ID** | 이벤트 이름 |
|---|---|
| 725005 | SSL Server request authentication |
| 725006 | SSL Handshake failed |
| 725007 | SSL Session terminated |
| 725008 | SSL Client Cipher |
| 725009 | SSL Server Cipher |
| 725010 | SSL Cipher |
| 725011 | SSL Device choose Cipher |
| 725012 | SSL Device choose Cipher |
| 725013 | SSL Server choose cipher |
| 725014. | SSL LIB error |
| 725015 | SSL client certificate failed |

# 시스템 로그 이벤트의 시간 속성

Event Logging(이벤트 로깅) 페이지에서 다양한 타임스탬프의 목적을 이해하면 원하는 이벤트를 필터링하고 찾을 수 있습니다.




| 번호 | 라벨 | 설명 |
|---|---|---|
| 1 | 날짜/시간 | SEC(Secure Event Connector)가 이벤트를 처리한 시간. 방화벽이 해당 트래픽을 검사한 시간과 다를 수 있습니다. 타임스탬프와 동일한 값입니다. |
| 2 | EventSecond | LastPacketSecond와 같음. |
| 3 | FirstPacketSecond | 연결이 열린 시간입니다. 이때 방화벽은 패킷을 검사합니다.<br>FirstPacketSecond의 값은 LastPacketSecond에서 ConnectionDuration을 빼서 계산됩니다.<br>연결 시작 시 로깅된 연결 이벤트의 경우 FirstPacketSecond, LastPacketSecond 및 EventSecond 값은 모두 동일합니다. |
| 4 | LastPacketSecond | 연결이 닫힌 시간입니다. 연결 종료 시 로깅된 연결 이벤트의 경우, LastPacketSecond 및 EventSecond는 동일합니다. |
| 5 | timestamp | SEC(Secure Event Connector)가 이벤트를 처리한 시간. 방화벽이 해당 트래픽을 검사한 시간과 다를 수 있습니다. 날짜/시간과 동일한 값입니다. |
| 6 | 시스템 로그 타임스탬프 | 'logging timestamp'가 사용되는 경우 시스템 로그가 시작된 시간을 나타냅니다. 시스템 로그에 이 정보가 없으면 SEC가 이벤트를 수신한 시간이 반영됩니다. |

| 번호 | 라벨 | 설명 |
|---|---|---|
| 7 | NetflowTimeStamp | ASA에서 NetFlow 패킷을 채운 다음 플로우 컬렉터로 전송할 충분한 플로우 레코드/이벤트 수집을 완료한 시간입니다. |

# Cisco Secure Cloud Analytics 및 동적 엔티티 모델링

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

Secure Cloud Analytics는 온프레미스 및 클라우드 기반 네트워크 구축을 모니터링하는 SaaS(Software as a Service) 솔루션입니다. 방화벽 이벤트 및 네트워크 플로우 데이터를 비롯한 소스에서 네트워크 트래픽에 대한 정보를 수집하여 트래픽에 대한 관찰을 생성하고 트래픽 패턴을 기반으로 네트워크 엔티티의 역할을 자동으로 식별합니다. Secure Cloud Analytics는 Talos와 같은 위협 인텔리전스의 다른 소스와 결합된 이 정보를 사용하여 본질적으로 악의적인 행동이 있음을 나타내는 경고를 생성합니다. 알림과 함께 Secure Cloud Analytics는 알림을 조사하고 악의적인 동작의 소스를 찾기 위한 더 나은 기반을 제공하기 위해 수집한 네트워크 및 호스트 가시성 및 상황 정보를 제공합니다.

동적 엔티티 모델링

동적 엔티티 모델링은 방화벽 이벤트 및 네트워크 플로우 데이터에 대한 동작 분석을 수행하여 네트워크의 상태를 추적합니다. Secure Cloud Analytics의 컨텍스트에서 엔티티는 네트워크의 호스트 또는 엔드포인트와 같이 시간이 지남에 따라 추적할 수 있는 항목입니다. 동적 엔터티 모델링은 전송하는 트래픽 및 네트워크에서 수행하는 활동을 기반으로 엔터티에 대한 정보를 수집합니다. **Logging Analytics and Detection(**로깅 분석 및 탐지**)** 라이선스와 통합된 Secure Cloud Analytics는 엔티티가 일반적으로 전송하는 트래픽 유형을 확인하기 위해 방화벽 이벤트 및 기타 트래픽 정보를 가져올 수 있습니다. **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스를 구매한 경우 Secure Cloud Analytics는 엔티티 트래픽 모델링에 NetFlow 및 기타 트래픽 정보도 포함할 수 있습니다. Secure Cloud Analytics는 각 엔터티의 최신 모델을 유지하기 위해 엔터티가 계속해서 트래픽을 전송하고 잠재적으로 다른 트래픽을 전송하므로 시간이 지남에 따라 이러한 모델을 업데이트합니다. 이 정보에서 Secure Cloud Analytics는 다음을 식별합니다.

- 엔티티의 역할 - 엔티티가 일반적으로 수행하는 작업을 설명합니다. 예를 들어 엔티티가 일반적으로 이메일 서버와 연결된 트래픽을 전송하는 경우, Secure Cloud Analytics는 엔티티를 이메일 서버 역할로 할당합니다. 엔터티는 여러 역할을 수행할 수 있으므로 역할/엔티티 관계는 다대일일 수 있습니다.
- 엔티티에 대한 관찰 - 외부 IP 주소와의 하트비트 연결 또는 다른 엔티티와 설정된 원격 액세스 세션과 같이 네트워크에서의 엔티티 동작에 대한 팩트입니다. CDO와 통합하는 경우 방화벽 이벤트에서 이러한 정보를 가져올 수 있습니다. **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스도 구매한 경우, 시스템은 NetFlow에서 팩트를 가져오고 방화벽 이벤트와 NetFlow 모두에서 관찰을 생성할 수 있습니다. 관찰 자체는 관찰이 나타내는 것 이상의 의미를 전달하지 않습니다. 일반적인 고객은 수천 개의 관찰 및 몇 가지 알림을 가질 수 있습니다.

알림 및 분석

역할, 관찰 및 기타 위협 인텔리전스의 조합을 기반으로 Secure Cloud Analytics는 시스템에서 식별한 가능한 악의적인 행동을 나타내는 실행 가능한 항목인 알림을 생성합니다. 하나의 알림이 여러 관찰을 나타낼 수 있습니다. 방화벽이 동일한 연결 및 엔터티와 관련된 여러 연결 이벤트를 로깅하는 경우 하나의 알림만 생성될 수 있습니다.

예를 들어, 새 내부 디바이스 관찰 자체는 악의적인 행동을 구성하지 않습니다. 그러나 시간이 지남에 따라 엔티티가 도메인 컨트롤러와 일치하는 트래픽을 전송하면 시스템은 해당 엔티티에 도메인 컨트롤러 역할을 할당합니다. 이후에 엔티티가 비정상적인 포트를 사용하여 이전에 연결을 설정하지 않은 외부 서버에 연결하고 대량의 데이터를 전송하는 경우, 시스템은 새로운 대규모 연결(외부) 관찰 및 예외적인 도메인 컨트롤러 관찰을 로깅합니다. 해당 외부 서버가 Talos 감시 목록에 있는 것으로 식별된 경우, 이 모든 정보의 조합으로 인해 Secure Cloud Analytics가 이 엔티티의 동작에 대한 알림을 생성하고, 악성 동작을 조사하고 교정하기 위한 추가 작업을 수행하라는 메시지가 표시됩니다.

Secure Cloud Analytics 웹 포털 UI에서 알림을 열면 시스템이 알림을 생성하도록 유도한 지원 관찰을 볼 수 있습니다. 이러한 관찰을 통해 관련 엔터티에 대한 추가 컨텍스트(전송한 트래픽 포함) 및 외부 위협 인텔리전스(사용 가능한 경우)도 볼 수 있습니다. 또한 엔티티가 관련된 다른 관찰 및 알림을 보고 이 동작이 다른 잠재적인 악의적인 동작과 관련이 있는지 확인할 수 있습니다.

Secure Cloud Analytics에서 알림을 보고 닫을 때는 Secure Cloud Analytics UI의 트래픽을 허용하거나 차단할 수 없습니다. 디바이스를 액티브 모드로 구축한 경우에는 트래픽을 허용하거나 차단하도록 방화벽 액세스 제어 규칙을 업데이트하고, 패시브 모드에서 디바이스를 구축한 경우에는 방화벽 액세스 제어 규칙을 업데이트해야 합니다.

# 방화벽 이벤트 기반 알림 작업

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

알림 워크플로우

알림의 워크플로우는 상태를 기반으로 합니다. 시스템에서 알림을 생성할 때 기본 상태는 Open(열림)이며 사용자가 할당되지 않습니다. Alerts(알림) 요약을 볼 때 즉시 문제가 되는 모든 열린 알림이 기본적으로 표시됩니다.

참고: **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스가 있는 경우 알림은 NetFlow에서 생성된 관찰, 방화벽 이벤트에서 생성된 관찰 또는 두 데이터 소스의 관찰을 기반으로 할 수 있습니다.

알림 요약을 검토할 때 알림에 대한 상태를 초기 분류로 할당, 태그 지정 및 업데이트할 수 있습니다. 필터 및 검색 기능을 사용하여 특정 알림을 찾거나, 다른 상태의 알림을 표시하거나, 다른 태그 또는 담당자와 연결할 수 있습니다. 알림의 상태를 스누즈로 설정할 수 있습니다. 이 경우 스누즈 기간이 경과할 때까지 미해결 알림 목록에 다시 나타나지 않습니다. 알림에서 스누즈 상태를 제거하여 미해결 알림으로 다시 표시할 수도 있습니다. 알림을 검토할 때 자신 또는 시스템의 다른 사용자에게 할당할 수 있습니다. 사용자는 사용자 이름에 할당된 모든 알림을 검색할 수 있습니다.

Alerts(알림) 요약에서 알림 상세정보 페이지를 볼 수 있습니다. 이 페이지에서는 이 알림을 생성한 지원 관찰에 대한 추가 컨텍스트 및 이 알림과 관련된 엔터티에 대한 추가 컨텍스트를 검토할 수 있습

니다. 이 정보는 네트워크에서 문제를 추가로 조사하고 잠재적으로 악의적인 동작을 해결하기 위해 실제 문제를 정확히 찾아내는 데 도움이 될 수 있습니다.

Stealthwatch Cloud 웹 포털 UI, CDO 및 네트워크에서 조사할 때 결과를 설명하는 알림과 함께 코멘트를 남길 수 있습니다. 이렇게 하면 나중에 참조할 수 있는 연구 기록을 만드는 데 도움이 됩니다.

분석을 완료한 경우 상태를 Closed(닫힘)로 업데이트하고 더 이상 기본적으로 미결 알림으로 표시되지 않도록 할 수 있습니다. 상황이 바뀌면 나중에 닫힌 알림을 다시 열 수도 있습니다.

다음은 지정된 알림을 조사하는 방법에 대한 일반적인 지침 및 제안 사항입니다. Stealthwatch Cloud는 알림을 로깅할 때 추가 컨텍스트를 제공하므로 이 컨텍스트를 조사에 활용할 수 있습니다.

이러한 단계는 포괄적이거나 모든 것을 포함하지 않습니다. 이는 알림 조사를 시작하는 데 사용할 수 있는 일반적인 프레임워크를 제공할 뿐입니다.

일반적으로 알림을 검토할 때 다음 단계를 수행할 수 있습니다.

1. 열린 알림 분류, on page 464
2. 나중에 분석하기 위해 알림 일시 중지, on page 465
3. 추가 조사를 위해 알림 업데이트, on page 465
4. 알림 검토 및 조사 시작, on page 466
5. 엔터티 및 사용자 검사, on page 468
6. Secure Cloud Analytics를 사용하여 문제 해결, on page 468
7. 알림 업데이트 및 닫기, on page 469

## 열린 알림 분류

특히 둘 이상의 알림이 아직 조사되지 않은 경우, 미해결 알림을 분류합니다.

- CDO에서 SWC로 교차 실행하고 알림을 보는 방법에 대한 자세한 내용은 CDO에서 Cisco Secure Cloud Analytics 알림 보기을 참조하십시오.

다음 질문을 합니다.

- 이 알림 유형을 높은 우선순위로 구성했습니까?
- 영향을 받는 서브넷에 대해 높은 감도를 설정했습니까?
- 네트워크의 새 엔터티에서 발생하는 비정상적인 동작입니까?
- 엔터티의 일반적인 역할은 무엇이며 이 알림의 동작이 해당 역할과 어떻게 일치합니까?
- 이 엔터티의 정상적인 동작에서 예외적으로 벗어났습니다.
- 사용자가 관련된 경우, 이는 사용자의 예상된 동작입니까, 아니면 예외적인 것입니까?
- 보호되거나 민감한 데이터가 손상될 위험이 있습니까?
- 이 동작이 계속 허용되는 경우 네트워크에 미치는 영향은 어느 정도입니까?

- 외부 엔터티와 통신하는 경우, 이러한 엔터티가 과거에 네트워크의 다른 엔터티와 연결을 설정했습니까?

우선순위가 높은 알림인 경우 조사를 계속하기 전에 인터넷에서 엔티티를 격리하거나 연결을 닫는 것을 고려하십시오.

## 나중에 분석하기 위해 알림 일시 중지

다른 알림에 비해 우선 순위가 낮은 알림을 스누즈합니다. 예를 들어 조직에서 이메일 서버를 FTP 서버로 용도를 변경하고 시스템에서 긴급 프로파일 알림(엔티티의 현재 트래픽이 이전에 일치하지 않았던 행동 프로파일과 일치함을 나타냄)을 생성하는 경우 이 알림을 나중에 다시 확인할 수 있습니다. 스누즈된 알림은 열린 알림과 함께 표시되지 않습니다. 이러한 스누즈된 알림을 검토하려면 특별히 필터링해야 합니다.

알림 스누즈:

단계 **1** **Close Alert(**알림 닫기**)**를 클릭합니다.

단계 **2** Snooze this alert(이 알림 스누즈) 창의 드롭다운에서 스누즈 기간을 선택합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

### What to do next

이러한 알림을 검토할 준비가 되면 다시 알림을 해제할 수 있습니다. 이렇게 하면 상태가 Open(열림)으로 설정되고 다른 Open(열림) 알림과 함께 알림이 표시됩니다.

스누즈된 알림의 스누즈를 해제합니다.

- 스누즈된 알림에서 **Unsnooze Alert(**알림 스누즈 해제**)**를 클릭합니다.

## 추가 조사를 위해 알림 업데이트

알림 세부 정보를 엽니다.

단계 **1** **Monitor(**모니터링**)** > **Alerts(**알림**)**를 선택합니다.

단계 **2** 알림 유형 이름을 클릭합니다.

### What to do next

초기 분류 및 우선순위에 따라 알림을 할당하고 태그를 지정합니다.

1. **Assignee(**담당자**)** 드롭다운에서 사용자를 선택하여 알림을 할당하면 사용자가 조사를 시작할 수 있습니다.
2. 드롭다운에서 하나 이상의 **Tags(**태그**)**를 선택하여 알림에 태그를 추가하여 향후 식별을 위해 알림을 더 잘 분류하고 알림에서 장기적 패턴을 설정합니다.

3. 이 알림에 대한 코멘트를 입력한 다음 **Comment(**코멘트**)**를 클릭하여 초기 결과를 추적하고 알림에 할당된 사람을 지원하는 데 필요한 코멘트를 남깁니다. 알림은 시스템 코멘트와 사용자 코멘트를 모두 추적합니다.

# 알림 검토 및 조사 시작

할당된 알림을 검토하는 경우 알림 세부 정보를 검토하여 Stealthwatch Cloud에서 알림을 생성한 이유를 파악합니다. 지원 관찰을 검토하여 이러한 관찰이 소스 엔터티에 미치는 영향을 파악합니다.

경고가 방화벽 이벤트를 기반으로 생성된 경우, 시스템은 방화벽 구축이 이 경고의 소스임을 인식하지 않습니다.

이 소스 엔터티에 대한 모든 지원 관찰을 확인하여 일반 동작 및 패턴을 파악하고 이 활동이 더 긴 추세의 일부일 수 있는지 확인합니다.

**SUMMARY STEPS**

1. 알림 세부사항에서 관찰 유형 옆에 있는 화살표 아이콘(➔)을 클릭하여 해당 유형의 모든 로깅된 관찰을 확인합니다.
2. **All Observations for Network(**네트워크에 대한 모든 관찰**)** 옆에 있는 화살표 아이콘(➔)을 클릭하여 이 알림의 소스 엔터티에 대해 로깅된 모든 관찰을 확인합니다.

**DETAILED STEPS**

단계 **1** 알림 세부사항에서 관찰 유형 옆에 있는 화살표 아이콘(➔)을 클릭하여 해당 유형의 모든 로깅된 관찰을 확인합니다.

단계 **2** **All Observations for Network(**네트워크에 대한 모든 관찰**)** 옆에 있는 화살표 아이콘(➔)을 클릭하여 이 알림의 소스 엔터티에 대해 로깅된 모든 관찰을 확인합니다.

이러한 관찰에 대한 추가 분석을 수행하려면 쉼표로 구분된 값 파일로 지원 관찰을 다운로드합니다.

- 알림 세부 정보의 Supporting Observations(지원 관찰) 창에서 **CSV**를 클릭합니다.

관찰 결과에서 소스 엔터티 동작이 악의적인 동작을 나타내는지 확인합니다. 소스 엔터티가 여러 외부 엔터티와의 연결을 설정한 경우, 외부 엔터티가 어떤 식으로든 관련이 있는지 확인합니다(예: 모든 엔터티가 유사한 지리위치 정보를 가지고 있거나 해당 IP 주소가 동일한 서브넷에 있는지 여부).

소스 엔터티 IP 주소 또는 호스트 이름에서 소스 엔터티와 관련된 추가 컨텍스트를 확인합니다. 여기에는 관련될 수 있는 기타 알림 및 관찰, 디바이스 자체에 대한 정보, 전송 중인 세션 트래픽 유형이 포함됩니다.

- 엔티티와 관련된 모든 알림을 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Alerts(**알림**)**를 선택합니다.
- IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Observations(**관찰**)**를 선택하여 엔티티와 관련된 모든 관찰을 확인합니다.

- 디바이스에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Device(**디바이스**)**를 선택합니다.
- 이 엔터티와 관련된 세션 트래픽을 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Session Traffic(**세션 트래픽**)**을 선택합니다.
- IP 주소 또는 호스트 이름 드롭다운에서 **Copy(**복사**)**를 선택하여 IP 주소 또는 호스트 이름을 복사합니다.

Stealthwatch Cloud의 소스 엔티티는 항상 네트워크 내부에 있습니다. 이를 방화벽 이벤트의 Initiator IP(이니시에이터 IP)와 비교해 보십시오. 이 IP는 연결을 시작한 엔티티를 나타내며, 네트워크의 내부 또는 외부에 있을 수 있습니다.

관찰에서 다른 외부 엔터티에 대한 정보를 검토합니다. 지리위치 정보를 검토하고 지리위치 데이터 또는 Umbrella 데이터가 악성 엔티티를 식별하는지 확인합니다. 이러한 엔터티에 의해 생성된 트래픽을 확인합니다. Talos, AbuseIPDB 또는 Google에 이러한 엔터티에 대한 정보가 있는지 확인합니다. 여러 날짜의 IP 주소를 찾고 외부 엔터티가 네트워크의 엔터티와 설정한 다른 유형의 연결을 확인합니다. 필요한 경우 이러한 내부 엔터티를 찾아 보안 침해 또는 의도하지 않은 행동의 증거가 있는지 확인합니다.

소스 엔티티가 연결을 설정한 외부 엔티티 IP 주소 또는 호스트 이름에 대한 컨텍스트를 검토합니다.

- 이 엔티티에 대한 최근 트래픽 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **IP Traffic(IP** 트래픽**)**을 선택합니다.
- 이 엔티티에 대한 최근 세션 트래픽 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Session Traffic(**세션 트래픽**)**을 선택합니다.
- **AbuseIPDB**웹사이트에서 이 엔티티에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 AbuseIPDB를 선택합니다.
- Cisco Umbrella 웹사이트에서 이 엔티티에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Cisco Umbrella**를 선택합니다.
- Google에서 이 IP 주소를 검색하려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Google Search(Google** 검색**)**를 선택합니다.
- Talos 웹사이트에서 이 정보에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Talos Intelligence**를 선택합니다.
- IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Add IP to watchlist(**감시 목록에 **IP** 추가**)**를 선택하여 이 엔터티를 감시 목록에 추가합니다.
- 이 엔티티의 지난 달 트래픽을 검색하려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Find IP on multiple days(**여러 날짜의 **IP** 찾기**)**를 선택합니다.
- IP 주소 또는 호스트 이름 드롭다운에서 **Copy(**복사**)**를 선택하여 IP 주소 또는 호스트 이름을 복사합니다.

Stealthwatch Cloud의 연결된 엔터티는 항상 네트워크 외부에 있습니다. 이를 방화벽 이벤트의 Responder IP(응답자 IP)와 비교해 보십시오. 이는 연결 요청에 응답한 엔터티를 나타내며, 네트워크의 내부 또는 외부에 있을 수 있습니다.

결과에 대한 코멘트를 남겨 주십시오.

- 알림 세부 정보에서 이 알림에 대한 코멘트를 입력하고 **Comment(**코멘트**)**를 클릭합니다.

## 엔터티 및 사용자 검사

Stealthwatch Cloud 포털 UI에서 알림을 검토한 후 소스 엔터티, 이 알림과 관련되었을 수 있는 사용자 및 기타 관련 엔터티에 대해 직접 추가 검사를 수행할 수 있습니다.

- 소스 엔터티가 물리적으로 또는 클라우드에서 네트워크의 어느 위치에 있는지 확인하고 직접 액세스합니다. 이 엔터티에 대한 로그 파일을 찾습니다. 네트워크의 물리적 엔터티인 경우 디바이스에 액세스하여 로그 정보를 검토하고 이 동작의 원인에 대한 정보가 있는지 확인합니다. 가상 엔터티이거나 클라우드에 저장된 경우 로그에 액세스하여 이 엔터티와 관련된 항목을 검색합니다. 무단 로그인, 승인되지 않은 구성 변경 등에 대한 자세한 내용은 로그를 검사합니다.
- 엔터티를 검사합니다. 엔터티 자체에서 악성코드 또는 취약성을 식별할 수 있는지 확인합니다. 조직에서 승인하지 않은 USB 스틱과 같이 디바이스에 대한 물리적 변경이 있는지를 포함하여 악의적인 변경이 있는지 확인합니다.
- 네트워크의 사용자 또는 네트워크 외부의 사용자가 관련되었는지 확인합니다. 가능한 경우 사용자에게 무엇을 하고 있었는지 물어봅니다. 사용자가 사용할 수 없는 경우, 액세스 권한이 있어야 했는지, 그리고 퇴사한 직원이 퇴사 전에 외부 서버에 파일을 업로드하는 등의 상황이 발생했는지 확인합니다.

결과에 대한 코멘트를 남겨 주십시오.

- 알림 세부 정보에서 이 알림에 대한 코멘트를 입력하고 **Comment(**코멘트**)**를 클릭합니다.

## 알림 업데이트 및 닫기

결과에 따라 태그를 추가합니다.

---

단계 **1** Secure Cloud Analytics 포털 UI에서 **Monitor(**모니터링**)** > **Alerts(**알림**)**를 선택합니다.

단계 **2** 드롭다운에서 하나 이상의 **Tags(**태그**)**를 선택합니다.

---

조사 결과 및 수행한 교정 단계를 설명하는 최종 코멘트를 추가합니다.

- 알림 세부 정보에서 이 알림에 대한 코멘트를 입력하고 **Comment(**코멘트**)**를 클릭합니다.

알림을 닫고 유용하거나 도움이 되지 않음으로 표시합니다.

1. 알림 세부 정보에서 **Close Alert(**알림 닫기**)**를 클릭합니다.

2. 알림이 도움이 되었으면 **Yes(**예**)**를 선택하고, 알림이 도움이 되지 않았다면 **No(**아니요**)**를 선택합니다. 이는 알림이 악의적인 행동으로 인해 발생했음을 의미하는 것이 아니라 해당 알림이 조직에 도움이 되었음을 의미합니다.
3. **Save(**저장**)**를 클릭합니다.

### What to do next

종료된 알림 다시 열기

종료된 알림과 관련된 추가 정보를 발견하거나 알림과 관련된 코멘트를 더 추가하려는 경우 알림을 다시 열어 상태를 Open(열림)으로 변경할 수 있습니다. 그런 다음 필요에 따라 알림을 변경한 다음 추가 조사가 완료되면 알림을 닫을 수 있습니다.

종료된 알림을 다시 엽니다.

- 닫힌 알림의 세부 사항에서 **Reopen Alert(**알림 다시 열기**)**를 클릭합니다.

# 알림 우선순위 수정

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

알림 유형은 기본 우선순위와 함께 제공되며, 이는 시스템이 이 유형의 알림 생성에 대한 민감도에 영향을 미칩니다. 알림은 기본적으로 Cisco 인텔리전스 및 기타 요인에 따라 낮음 또는 보통으로 설정됩니다. 네트워크 환경에 따라 알림 유형의 우선순위를 다시 지정하여 우려되는 특정 알림을 강조할 수 있습니다. 모든 알림 유형을 낮음, 보통 또는 높음 우선순위로 구성할 수 있습니다.

- **Monitor(**모니터링**)** > **Alerts(**알림**)**를 선택합니다.
- Settings(설정) 드롭다운 아이콘(⚙)을 클릭한 다음 **Alert Types and Priorities(**알림 유형 및 우선순위**)**를 선택합니다.
- 알림 유형 옆에 있는 편집 아이콘(✎)을 클릭하고 낮음, 중간 또는 높음을 선택하여 우선순위를 변경합니다.

# 이벤트 로깅 페이지에서 이벤트 검색 및 필터링

특정 이벤트에 대한 기록 및 라이브 이벤트 테이블을 검색하고 필터링하는 것은 CDO에서 다른 정보를 검색하고 필터링할 때와 동일한 방식으로 작동합니다. 필터 기준을 추가하면 CDO가 Events(이벤트) 페이지에 표시되는 내용을 제한하기 시작합니다. 검색 필드에 검색 기준을 입력하여 특정 값의 이벤트를 찾을 수도 있습니다. 필터링 및 검색 메커니즘을 결합하는 경우, 검색은 이벤트를 필터링한 후 표시된 결과 중에서 입력한 값을 찾으려고 시도합니다.

다음은 이벤트 로그 검색을 수행하는 옵션입니다.

- 이벤트 로깅 페이지에서 이벤트 검색, 517 페이지
- 백그라운드에서 기록 이벤트 검색, 517 페이지

필터링은 라이브 이벤트를 시간 기준으로 필터링할 수 없다는 점을 제외하고 기록 이벤트와 동일한 방식으로 라이브 이벤트에 대해 작동합니다.

이러한 필터링 방법에 대해 알아보십시오.


- 라이브 또는 과거 이벤트 필터링, 510 페이지
- NetFlow 이벤트만 필터링, 512 페이지
- ASA 또는 FDM-관리 장치 syslog 이벤트에 대한 필터링(ASA NetFlow 이벤트 제외), 512 페이지
- 필터 요소 결합, 512 페이지


# 라이브 또는 과거 이벤트 필터링

이 절차에서는 이벤트 필터링을 사용하여 Event Logging(이벤트 로깅) 페이지에서 이벤트의 하위 집합을 확인하는 방법을 설명합니다. 특정 필터 기준을 반복적으로 사용하는 경우 사용자 지정 필터를 생성하여 저장할 수 있습니다. 자세한 내용은 사용자 지정 가능한 이벤트 필터를 참조하십시오.

단계 **1** 탐색 모음에서 분석 > 이벤트 로깅를 선택합니다.

단계 **2** Historical(기록) 또는 Live(라이브) 탭을 클릭합니다.

단계 **3** 필터 버튼 를 클릭합니다. 필터링 열은 고정 아이콘 을 클릭하여 열 수 있습니다.

단계 **4** 저장된 필터 요소가 없는 View(보기) 탭을 클릭합니다.


단계 **5** 필터링할 이벤트 세부 정보를 선택합니다.

- **FTD** 이벤트 유형
  - Connection(연결) - 액세스 제어 규칙의 연결 이벤트를 표시합니다.
  - File(파일) - 액세스 제어 규칙의 파일 정책에 의해 보고된 이벤트를 표시합니다.
  - Intrusion(침입) - 액세스 제어 규칙의 침입 정책에 의해 보고된 이벤트를 표시합니다.
  - Malware(악성코드) - 액세스 제어 규칙의 악성코드 정책에 의해 보고된 이벤트를 표시합니다.
- ASA**Event Types(**이벤트 유형**)** -이러한 이벤트 유형은 Syslog 또는 NetFlow 이벤트의 그룹을 나타냅니다. 어떤 시스템 로그 ID 또는 어떤 NetFlow ID가 어떤 그룹에 포함되어 있는지에 대한 자세한 내용은 ASA 이벤트 유형을 참조하십시오.
  - 구문 분석된 이벤트 - 구문 분석된 ASA 시스템 로그 이벤트는 다른 Syslog 이벤트보다 더 많은 이벤트 속성을 포함하며, CDO는 이러한 속성을 기반으로 더 빠르게 검색 결과를 반환할 수 있습니다. 구문 분석된 이벤트는 필터링 카테고리가 아닙니다. 그러나 구문 분석된 이벤트 ID는 Event Types(이벤트 유형) 열에 기울임꼴로 표시됩니다. 기울임꼴로 표시되지 않은 이벤트 ID는 구문 분석되지 않습니다.

- **Time Range(**시간 범위**)** - 표시할 기간의 시작과 끝을 선택하려면 Start(시작) 또는 End(종료) 시간 필드를 클릭합니다. 타임스탬프는 컴퓨터의 로컬 시간으로 표시됩니다.
- **Action(**작업**)** - 규칙에 의해 정의된 보안 작업을 지정합니다. 입력하는 값은 찾으려는 값과 정확히 일치해야 합니다. 그러나 대/소문자는 중요하지 않습니다. 연결, 파일, 침입, 악성코드, Syslog 및 NetFlow 이벤트 유형에 대해 서로 다른 값을 입력합니다.
  - 연결 이벤트 유형의 경우 필터는 AC_RuleAction 특성에서 일치 항목을 검색합니다. 이러한 값은 Allow(허용), Block(차단), Trust(신뢰)일 수 있습니다.
  - 파일 이벤트 유형의 경우 필터는 FileAction 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Allow(허용), Block(차단), Trust(신뢰)일 수 있습니다.
  - 침입 이벤트 유형의 경우 필터는 InLineResult 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Allowed(허용됨), Blocked(차단됨), Trusted(신뢰할 수 있음)일 수 있습니다.
  - 악성코드 이벤트 유형의 경우 필터는 FileAction 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Cloud Lookup Timeout(클라우드 조회 시간 초과)일 수 있습니다.
  - Syslog 및 NetFlow 이벤트 유형의 경우 필터는 Action(작업) 속성에서 일치하는 항목을 검색합니다.
- 센서 **ID** - 센서 ID는 이벤트가 보안 이벤트 커넥터로 전송되는 관리 IP 주소입니다.

  FDM 관리 디바이스의 경우 센서 ID는 일반적으로 디바이스 관리 인터페이스의 IP 주소입니다.
- **IP** 주소
  - 이니시에이터 - 네트워크 트래픽 소스의 IP 주소입니다. Initiator address(이니시에이터 주소) 필드의 값은 이벤트 세부사항의 InitiatorIP(이니시에이터 IP) 필드 값에 해당합니다. 단일 주소(예: 10.10.10.100) 또는 CIDR 표기법으로 정의된 네트워크(예: 10.10.10.0/24)를 입력할 수 있습니다.
  - 응답자 - 패킷의 대상 IP 주소입니다. Destination address(대상 주소) 필드의 값은 이벤트 세부사항의 ResponderIP 필드에 있는 값에 해당합니다. 단일 주소(예: 10.10.10.100) 또는 CIDR 표기법으로 정의된 네트워크(예: 10.10.10.0/24)를 입력할 수 있습니다.
- 포트
  - 이니시에이터-세션 이니시에이터가 사용하는 포트 또는 ICMP 유형입니다. 소스 포트의 값은 이벤트 세부 정보의 InitiatorPort 값에 해당합니다. (범위 추가 - 시작 포트 종료 포트 및 이니시에이터와 응답자 사이 또는 둘 다 사이에 공백)
  - **Reponder(**응답기**)**-세션 responder가 사용하는 포트 또는 ICMP 코드입니다. 대상 포트의 값은 이벤트 세부사항의 ResponderPort 값에 해당합니다.
- **NetFlow** - ASA 디바이스용 NetFlow Secure Event Logging(NSEL) 이벤트는 Syslog 이벤트와 다릅니다. NetFlow 필터는 NSEL 레코드를 생성한 모든 NetFlow 이벤트 ID를 검색합니다. 이러한 "NetFlow 이벤트 ID"는 Cisco ASA NetFlow 구현 가이드에 정의되어 있습니다.

단계 **6** (선택 사항) View(보기) 탭에서 클릭하여 필터를 사용자 지정 필터로 저장합니다.

# NetFlow 이벤트만 필터링

이 절차에서는 ASA NetFlow 이벤트만 찾습니다.

단계 **1** CDO 메뉴 모음에서 분석 > 이벤트 로깅를 선택합니다.

단계 **2** Filter(필터) 아이콘 을 클릭하고 필터를 열린 상태로 고정합니다.

단계 **3** **Netflow** ASA 이벤트 필터를 확인합니다.

단계 **4** 다른 모든 ASA 이벤트 필터를 지웁니다.

ASA NetFlow 이벤트만 Event Logging(이벤트 로깅) 테이블에 표시됩니다.

# ASA 또는 FDM-관리 장치 syslog 이벤트에 대한 필터링(ASA NetFlow 이벤트 제외)

이 절차에서는 Syslog 이벤트만 찾습니다.

단계 **1** CDO 메뉴 모음에서 분석 > 이벤트 로깅를 선택합니다.

단계 **2** Filter(필터) 아이콘 을 클릭하고 필터를 열린 상태로 고정합니다.

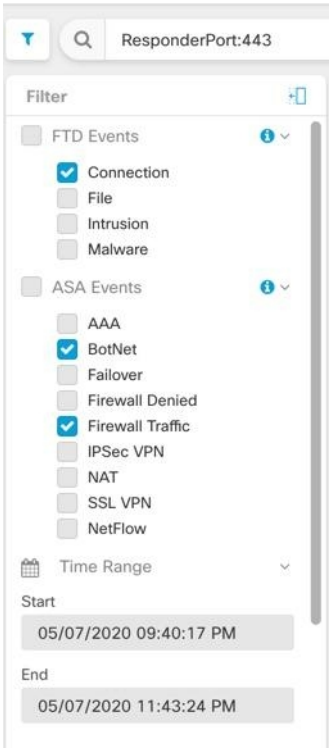
단계 **3** 필터 표시줄의 맨 아래로 스크롤하여 **Include NetFlow Events(NetFlow** 이벤트 포함**)** 필터가 선택 취소되었는지 확인합니다.

단계 **4** ASA Events(이벤트) 필터 트리로 다시 스크롤하여 **NetFlow** 상자가 선택 취소되었는지 확인합니다.

단계 **5** ASA 또는 FTD 필터 기준의 나머지를 선택합니다.

# 필터 요소 결합

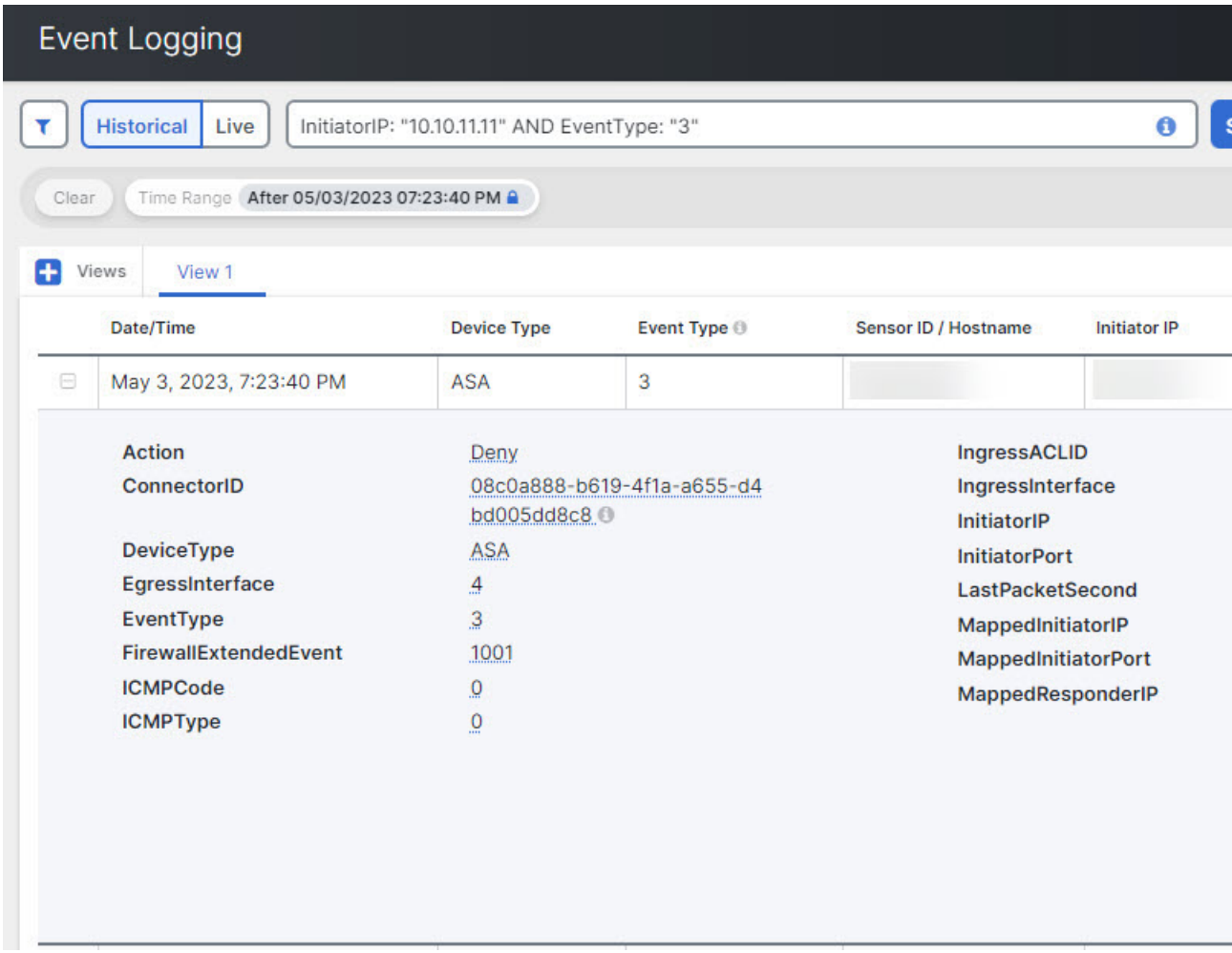
필터링 이벤트는 일반적으로 CDO의 표준 필터링 규칙을 따릅니다. 필터링 범주는 "AND"되고 범주 내의 값은 "OR"됩니다. 필터를 사용자 고유의 검색 기준과 결합할 수도 있습니다. 이벤트 필터의 경우 그러나 디바이스 이벤트 필터도 "OR"됩니다. 예를 들어 필터에서 다음 값을 선택한 경우,




이 필터를 사용하면 CDO는 위협 방어 디바이스 연결 이벤트 또는 ASA BotNet 또는 방화벽 트래픽 이벤트 및 시간 범위의 두 번 사이에 발생한 이벤트 및 ResponderPort 443도 포함하는 이벤트를 표시합니다. 시간 범위 내의 기록 이벤트를 기준으로 필터링할 수 있습니다. 라이브 이벤트 페이지에는 항상 최신 이벤트가 표시됩니다.

특정 속성: 값 쌍 검색

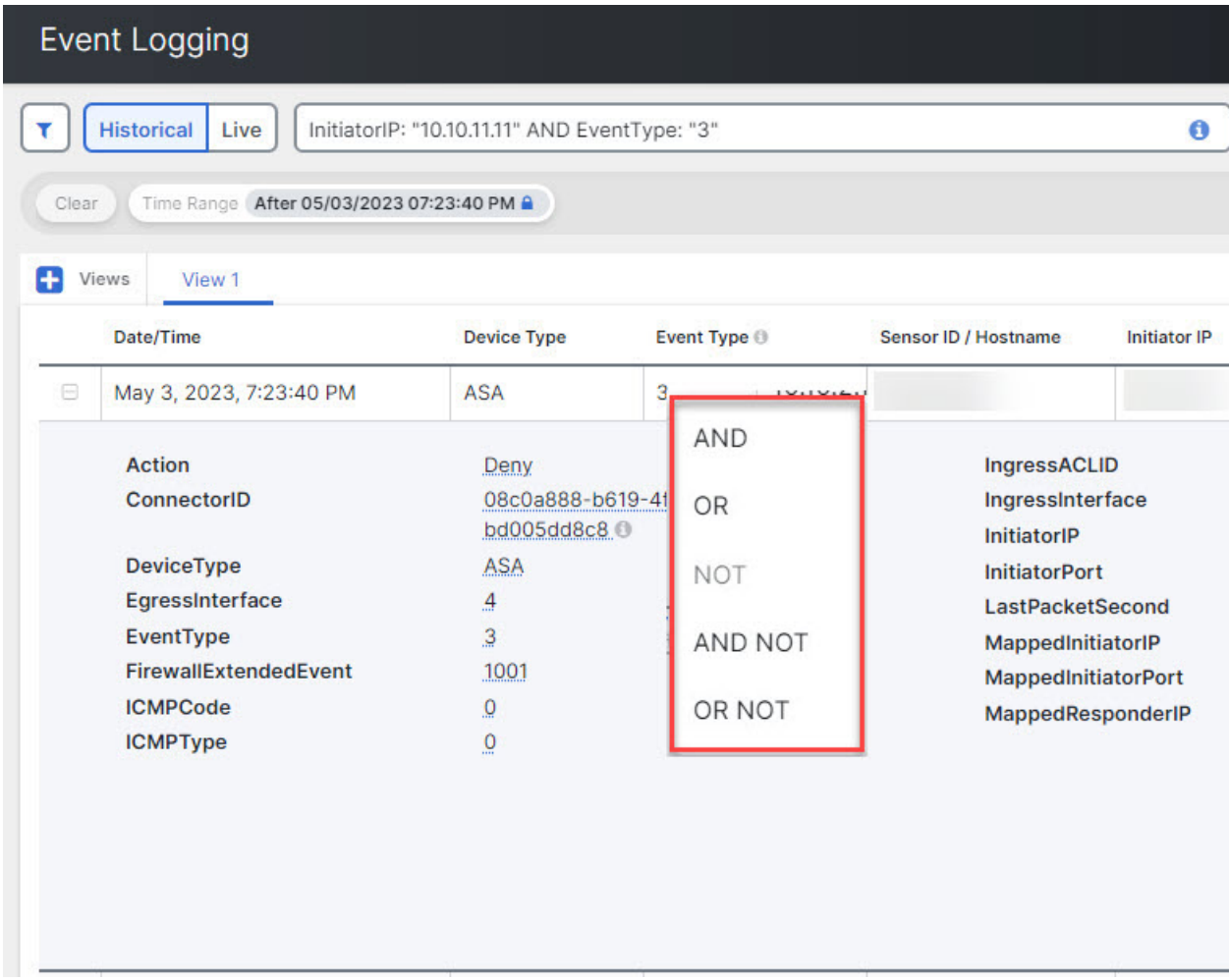
검색 필드에 이벤트 속성 및 값을 입력하여 라이브 또는 기록 이벤트를 검색할 수 있습니다. 이 작업을 수행하는 가장 쉬운 방법은 검색하려는 Event Logging(이벤트 로깅) 테이블의 속성을 클릭하는 것입니다. 그러면 CDO가 Search(검색) 필드에 해당 속성을 입력합니다. 롤오버하면 클릭할 수 있는 이벤트가 파란색으로 표시됩니다. 예를 들면 다음과 같습니다.




이 예에서는 InitiatorIP 값 10.10.11.11을 롤오버하고 이를 클릭하여 검색을 시작했습니다. 이니시에이터 IP 및 해당 값이 검색 문자열에 추가되었습니다. 다음으로, Event Type(이벤트 유형) 3를 클릭하여 검색 문자열에 추가하고 CDO에서 AND를 추가했습니다. 따라서 이 검색의 결과는 10.10.11.11에서 시작된 이벤트 및 3 이벤트 유형의 목록이 됩니다.

위의 예에서 값 3 옆에 돋보기가 있습니다. 돋보기를 롤오버하는 경우 AND, OR, AND NOT, OR NOT 연산자를 선택하여 검색에 추가할 값을 입력할 수도 있습니다.

아래 예에서는 "OR"가 선택되었습니다. 이 검색의 결과는 10.10.11.11에서 시작된 이벤트 또는 106023 이벤트 유형의 목록이 됩니다. 검색 필드가 비어 있고 테이블에서 값을 마우스 오른쪽 버튼으로 클릭하면 다른 값이 없으므로 NOT만 사용할 수 있습니다.




값을 롤오버하고 파란색으로 강조 표시되면 해당 값을 검색 문자열에 추가할 수 있습니다.

### **AND, OR, NOT, AND NOT, OR NOT** 필터 연산자

검색 문자열에서 사용되는 "AND", "OR", "NOT", "AND NOT" 및 "OR NOT"의 동작은 다음과 같습니다.

**AND**

필터 문자열에서 AND 연산자를 사용하여 모든 특성을 포함하는 이벤트를 찾습니다. AND 연산자는 검색 문자열을 시작할 수 없습니다.

예를 들어 아래의 검색 문자열은 이니시에이터IP 주소 10.10.10.43에서 시작되고 이니시에이터 포트 59614에서 전송된 TCP 프로토콜 AND를 포함하는 이벤트를 검색합니다. 각 추가 AND 문을 사용하여 기준을 충족하는 이벤트의 수가 점점 더 적을 것으로 예상됩니다.

```
Protocol: "tcp" AND InitiatorIP: "10.10.10.43" AND InitiatorPort: "59614"
```

또는

필터 문자열에서 OR 연산자를 사용하여 특성을 포함하는 이벤트를 찾습니다. OR 연산자는 검색 문자열을 시작할 수 없습니다.

예를 들어 아래의 검색 문자열은 TCP 프로토콜을 포함하는 이벤트를 포함하는 이벤트, 또는 이니시에이터 IP 주소 10.10.10.43에서 시작된 또는 이니시에이터 포트 59614에서 전송된 이벤트를 표시합니다. 각 추가 OR 문에서 기준을 충족하는 이벤트의 수가 점점 더 커질 것으로 예상됩니다.

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR InitiatorPort: "59614"
```

**NOT**

특정 속성이 있는 이벤트를 제외하려면 검색 문자열의 시작 부분에만 이를 사용하십시오. 예를 들어 이 검색 문자열은 InitiatorIP 192.168.25.3인 이벤트를 결과에서 제외합니다.

```
 NOT InitiatorIP: "192.168.25.3"
```

**AND NOT**

특정 특성을 포함하는 이벤트를 제외하려면 필터 문자열에서 AND NOT 연산자를 사용합니다. AND NOT은 검색 문자열의 시작 부분에 사용할 수 없습니다.

예를 들어 이 필터 문자열은 InitiatorIP 192.168.25.3인 이벤트를 표시하지만 ResponderIP 주소가 10.10.10.1인 이벤트는 표시하지 않습니다.

```
 InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

NOT과 AND NOT을 조합하여 여러 속성을 제외할 수도 있습니다. 예를 들어 이 필터 문자열은 InitiatorIP 192.168.25.3의 이벤트 및 ResponderIP 10.10.10.1의 이벤트를 제외합니다.

```
NOT InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

**OR NOT**

특정 요소를 제외하는 검색 결과를 포함하려면 OR NOT 연산자를 사용합니다. OR NOT 연산자는 검색 문자열의 시작 부분에 사용할 수 없습니다.

예를 들어 이 검색 문자열은 프로토콜이 TCP인 이벤트 또는 InitiatorIP가 10.10.10.43인 이벤트 또는 InitiatorPort 59614가 아닌 이벤트를 찾습니다.

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR NOT InitiatorPort: "59614"
```

(프로토콜: "tcp") OR (InitiatorIP: "10.10.10.43") OR (NOT InitiatorPort: "59614")를 검색할 수도 있습니다.

와일드카드 검색

이벤트 내에서 결과를 찾으려면 **attribute:value** 검색의 value 필드에서 와일드카드를 나타내려면 별표(*)를 사용합니다. 예를 들어, 이 필터 문자열

```
 URL:*feedback*
```

은 문자열 **feedback**을 포함하는 이벤트의 URL 특성 필드에서 문자열을 찾습니다.

관련 정보**:**

- 이벤트 로깅 페이지의 열 표시 및 숨기기
- Security Analytics and Logging의 이벤트 속성

# 백그라운드에서 기록 이벤트 검색

CDO는 검색 기준을 정의하고 정의된 검색 기준에 따라 이벤트 로그를 검색하는 기능을 제공합니다. 백그라운드 검색 기능을 사용하여 백그라운드에서 이벤트 로그 검색을 수행하고 백그라운드 검색이 완료되면 검색 결과를 볼 수도 있습니다.

구성한 구독 알림 및 서비스 통합을 기반으로 백그라운드 검색이 완료되면 알림을 받습니다.

백그라운드 검색 페이지에서 직접 검색 결과를 보거나 다운로드하거나 삭제할 수 있습니다. 또한 백그라운드 검색이 일회성 이벤트에 대해 실행되도록 예약하거나 반복 일정을 예약할 수도 있습니다. 알림 설정 페이지로 이동하여 구독 옵션을 보거나 수정합니다.

# 이벤트 로깅 페이지에서 이벤트 검색

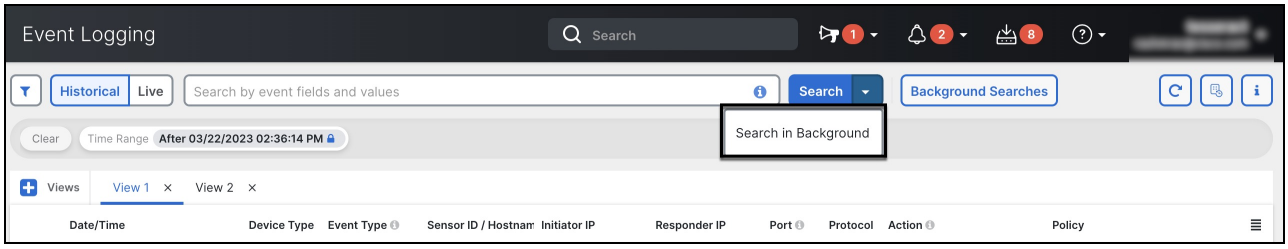
검색 및 백그라운드 검색 기능을 사용하여 Event Logging(이벤트 로깅) 페이지에서 로깅된 모든 이벤트를 볼 수 있습니다. 백그라운드 검색은 기록 이벤트에 대해서만 수행할 수 있습니다.

단계 **1** 탐색 모음에서 분석 > 이벤트 로깅를 선택합니다.

단계 **2** **Historical(**기록**)** 또는 **Live(**라이브**)** 탭을 클릭합니다.

단계 **3** 내비게이션 창으로 이동하여 검색식을 입력하고 **Search(**검색**)** 버튼을 입력하여 검색을 실행합니다. 절대 시간 범위 또는 상대 시간 범위를 사용하여 검색을 좁히거나 확장할 수 있습니다.

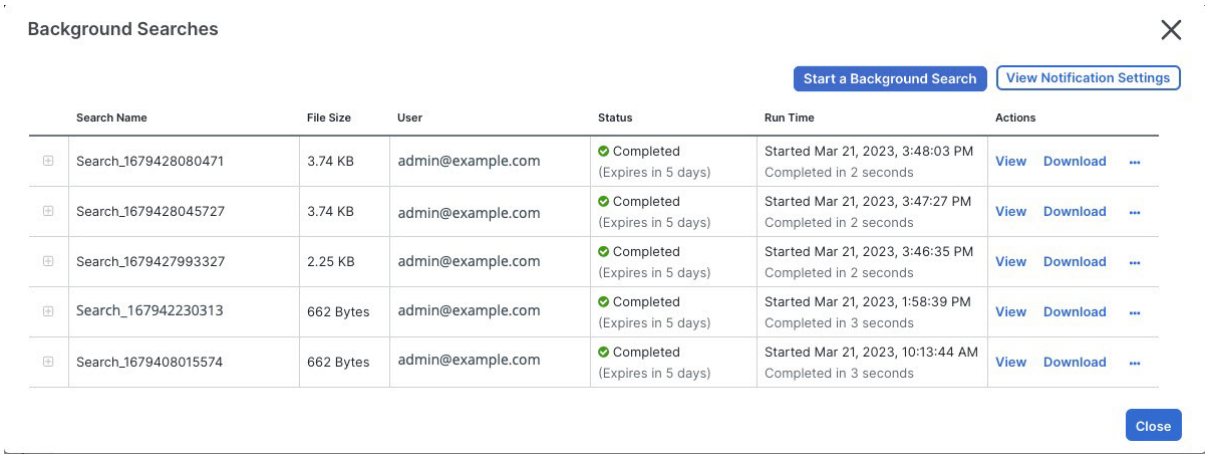
또는 **Search(**검색**)** 드롭다운 목록에서 **Search in Background(**백그라운드에서 검색**)**를 선택하여 검색 페이지에서 벗어나 있는 동안 백그라운드에서 검색을 실행합니다. 검색 결과가 준비되면 알림이 표시됩니다.




**Search(**검색**)** 버튼을 클릭하면 결과가 Event Logging(이벤트 로깅) 보기에 직접 나타납니다. 특정 검색 결과를 선택하면 쉽게 참조할 수 있도록 검색 기준이 검색 창에 나타납니다.

백그라운드에서 검색을 실행하도록 선택하면 검색 작업이 대기열에 추가되고 검색이 완료되면 알림이 표시됩니다. 백그라운드에서 여러 검색 쿼리를 실행할 수 있습니다.

단계 **4** **Background Searches(**백그라운드 검색**)** 버튼을 클릭하여 Background Searches(백그라운드 검색) 페이지를 봅니다.




Background Searches(백그라운드 검색) 페이지에 검색 결과 목록이 표시됩니다. 검색 결과를 보거나, 다운로드하거나, 삭제할 수 있습니다. 알림 설정 페이지로 이동하여 구독 옵션을 보거나 편집할 수도 있습니다. 이 페이지에서 검색을 시작하려면 **Start a Background Search(**백그라운드 검색 시작**)** 버튼을 선택합니다.

구독 옵션을 보거나 수정하는 방법에 대한 정보는 알림 설정, 44 페이지을 참조하십시오.

다음에 수행할 작업

반복 쿼리가 필요한 경우, 모든 백그라운드 검색을 예약된 백그라운드 검색으로 전환할 수 있습니다. 자세한 내용은 이벤트 뷰어에서 백그라운드 검색 예약, 518 페이지를 참조하십시오.

# 이벤트 뷰어에서 백그라운드 검색 예약

이벤트 뷰어 페이지에서 백그라운드에서 반복 쿼리를 예약합니다. 검색은 기록 이벤트에 대해서만 예약할 수 있습니다. 예약된 검색은 언제든지 수정하거나 취소할 수 있습니다. 기존 쿼리를 반복 검색으로 수정할 수도 있습니다.

참고 시작, 완료 또는 실패한 검색에 대한 알림을 수신하도록 선택할 수 있습니다. 자세한 내용은 알림 설정, 44 페이지를 참조하십시오.

기록 이벤트에 대해서만 백그라운드 검색을 예약할 수 있습니다. 예약 백그라운드 검색을 생성하려면 다음 단계를 수행하십시오.

단계 **1** 탐색 모음에서 **Analytics(**애널리틱스**)** > **Event Logging(**이벤트 로깅**)**를 선택합니다.

단계 **2** **Historical(**기록**)** 토글을 클릭하여 선택합니다. 기록 이벤트에 대한 백그라운드 검색만 예약할 수 있습니다.

단계 **3** 검색창에 검색하려는 검색 표현식을 입력합니다. **Search(**검색**)** 드롭다운 버튼을 클릭하고 **Search in background(**백그라운드에서 검색**)**를 선택합니다.

단계 **4** (선택 사항) 검색 이름을 변경합니다.

단계 **5** 기본적으로 **Search Now(**지금 검색**)** 확인란이 선택되어 있습니다. 선택된 경우, 저장 시 검색이 시작됩니다. 이 확인란을 선택하지 않으면 백그라운드 쿼리가 향후 검색으로서만 실행됩니다.

단계 **6** **Setup recurring schedule(**설정 반복 예약**)**을 확인하고 다음 설정을 구성합니다.

- **Search Logs for the Last(**마지막 검색 로그**)** - 얼마나 이전까지 검색하고자 하는지입니다.
- **Frequency(**빈도**)** - 예약 검색을 얼마나 자주 수행할지 선택합니다.

단계 **7** 창 하단에서 예약된 검색 기준을 확인합니다. **Schedule and Search Now(**지금 예약 및 검색**)**를 선택합니다. 또는 즉시 검색을 시작하도록 선택하지 않은 경우 버튼이 **Schedule Search(**검색 예약**)**로 표시됩니다.

---

다음에 수행할 작업

예약된 백그라운드 검색의 결과는 CDO에서 자동으로 삭제하기 전 최대 7일 동안 검토할 수 있습니다.

# 백그라운드 검색 다운로드

검색 결과 및 일정 쿼리는 CDO가 자동으로 제거하기 전까지 7일 동안 저장됩니다. 과거 이벤트에 대해 수행된 백그라운드 검색의 CSV 복사본을 다운로드합니다.

---

단계 **1** 내비게이션 바에서 **Analytics(**분석**)** > **Event Logging(**이벤트 로깅**)**으로 이동합니다.

단계 **2** **Background Searches(**백그라운드 검색**)** > **Actions(**작업**)** > **Download(**다운로드**)**를 클릭합니다.

단계 **3** 검색을 찾습니다. 예약된 검색은 **Queries(**쿼리**)** 탭에 저장됩니다.

단계 **4** **Download(**다운로드**)**를 클릭합니다. .CSV 파일은 로컬 드라이브의 기본 스토리지 위치에 자동으로 다운로드됩니다.

---

# 데이터 스토리지 요금제

Cisco Cloud가 온보딩된 ASA 및 FDM 매니지드 디바이스에서 매일 수신하는 이벤트 수를 반영하는 데이터 스토리지 요금제를 구매해야 합니다. 이를 "일일 수집 속도"라고 합니다. 데이터 요금제는 1년, 3년 또는 5년 단위의 GB/일 단위로 제공됩니다. 수집 속도를 결정하는 가장 좋은 방법은 Secure Logging Analytics(SaaS)를 구매하기 전에 무료 평가판에 참여하는 것입니다. 이를 통해 이벤트 볼륨을 적절하게 예측할 수 있습니다.

고객은 90일의 롤링 데이터 스토리지를 자동으로 수신합니다. 즉, 최근 90일간의 이벤트가 Cisco Cloud에 저장되고 91일이 되면 삭제됩니다.

고객은 기본 90일 이상의 추가 이벤트 보존으로 업그레이드하거나 기존 구독에 변경 주문을 통해 일일 볼륨(GB/일)을 추가할 수 있으며, 남은 구독 기간에 대해서만 일할 계산하여 청구됩니다.

데이터 요금제에 대한 자세한 내용은 Secure Logging Analytics(SaaS) 주문 가이드를 참조하십시오.

**Note** Security Analytics and Logging 라이선스 및 데이터 요금제를 보유하고 있는 경우 나중에 다른 Security Analytics and Logging 라이선스를 취득할 수 있으며, 다른 데이터 요금제를 구매할 필요가 없습니다. 네트워크 트래픽 처리량이 변경되어 다른 데이터 플랜을 취득하는 경우에는 다른 Security Analytics and Logging 라이선스를 구입하지 않아도 됩니다.

내 할당량에 대해 어떤 데이터가 계산됩니까**?**

보안 이벤트 커넥터로 전송된 모든 이벤트는 Secure Logging Analytics(SaaS) 클라우드에 누적되며 데이터 할당량에 포함됩니다.

이벤트 뷰어에 표시되는 내용을 필터링해도 Secure Logging Analytics(SaaS) 클라우드에 저장된 이벤트 수는 줄어들지 않으며, 이벤트 뷰어에서 볼 수 있는 이벤트 수는 줄어듭니다.

이벤트는 90일 동안 Secure Logging Analytics(SaaS) 클라우드에 저장됩니다. 그 후에는 제거됩니다.

스토리지 할당량을 빠르게 사용하고 있습니다**.** 어떻게 해야 합니까**?**

이 문제를 해결하는 두 가지 방법은 다음과 같습니다.

- 추가 스토리지를 요청합니다. 필요한 것을 과소 평가했을 수 있습니다.
- 이벤트를 로깅하는 규칙의 수를 줄입니다. SSL 정책 규칙, 보안 인텔리전스 규칙, 액세스 제어 규칙은 물론 침입 정책, 파일 및 악성코드 정책에서도 이벤트를 로깅할 수 있습니다. 로깅 대상을 확인합니다. 생각보다 많은 규칙 및 정책에서 이벤트를 로깅해야 합니까?

# 이벤트 스토리지 기간 연장 및 이벤트 스토리지 용량 늘리기

Security Analytics and Logging(보안 분석 및 로깅) 고객은 이러한 라이선싱를 구매할 때 90일의 이벤트 스토리지를 받게 됩니다.

- 로깅 및 문제 해결
- 로깅 분석 및 탐지
- 총 네트워크 분석 및 모니터링

라이선스를 처음 구매할 때 또는 라이선스 기간 중 언제든지 1년, 2년 또는 3년치 롤링 이벤트 스토리지로 업그레이드하도록 선택할 수 있습니다.

Security Analytics and Logging 라이선스를 처음 구매할 때 스토리지 용량을 업그레이드할지 묻는 메시지가 표시됩니다. "예"라고 답하면 구매 중인 PID 목록에 추가 PID(Product Identifier)가 추가됩니다.

라이선스 기간 중간에 롤링 이벤트 스토리지를 연장하거나 이벤트 클라우드 스토리지의 양을 늘리기로 결정한 경우 다음을 수행할 수 있습니다.

단계 **1** Cisco Commerce에 사용자 계정으로 로그인합니다.

단계 **2** Cisco Defense Orchestrator PID를 선택합니다.

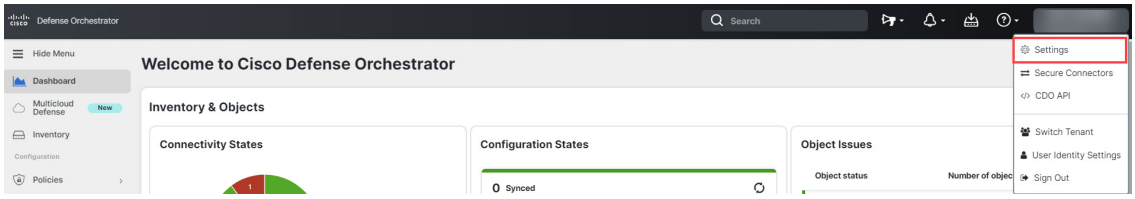
단계 **3** 프롬프트에 따라 스토리지 용량의 길이 또는 용량을 업그레이드합니다.

증가된 비용은 기존 라이선스의 남은 기간에 따라 비례 배분됩니다. 자세한 지침은 Secure Logging Analytics(SaaS) 주문 가이드를 참조하십시오.

## 보안 애널리틱스 및 로깅 데이터 계획 사용량 보기

월별 로깅 제한, 사용한 스토리지의 양, 사용 기간이 0으로 재설정된 경우를 확인하려면 다음을 수행합니다.

단계 **1** 테넌트를 클릭하고 **Settings(**설정**)**를 선택합니다.




단계 **2** **Logging Settings(**로깅 설정**)**를 클릭합니다.

단계 **3** **View Historical Usage(**기록 사용량 보기**)**를 클릭하여 최근 12개월까지의 스토리지 사용량을 확인할 수도 있습니다.

# SaaS(Secure Logging Analytics)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기

SaaS(Secure Logging Analytics)를 사용하면 ASA 또는 FDM 관리 디바이스에서 SEC(Secure Event Connector)의 특정 UDP, TCP 또는 NSEL 포트로 이벤트를 보낼 수 있습니다. 그런 다음 SEC는 해당 이벤트를 Cisco 클라우드로 전달합니다.

이러한 포트가 아직 사용 중이 아닌 경우, SEC는 이벤트를 수신하는 데 포트를 제공하며, SaaS(Secure Logging Analytics) 설명서에서는 기능을 구성할 때 포트 사용을 권장합니다.

- TCP: 10125
- UDP: 10025
- NSEL: 10425

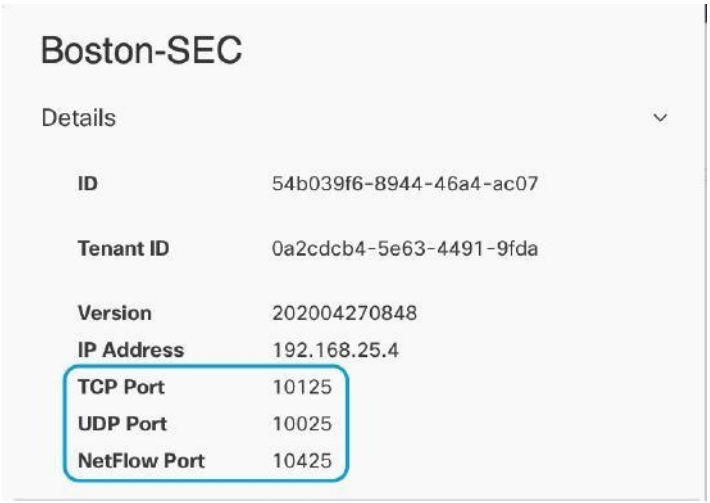
이러한 포트가 이미 사용 중인 경우 SaaS(Secure Logging Analytics)를 구성하기 전에 SEC 디바이스 세부 정보를 확인하여 실제로 이벤트를 수신하는 데 사용 중인 포트를 확인합니다.

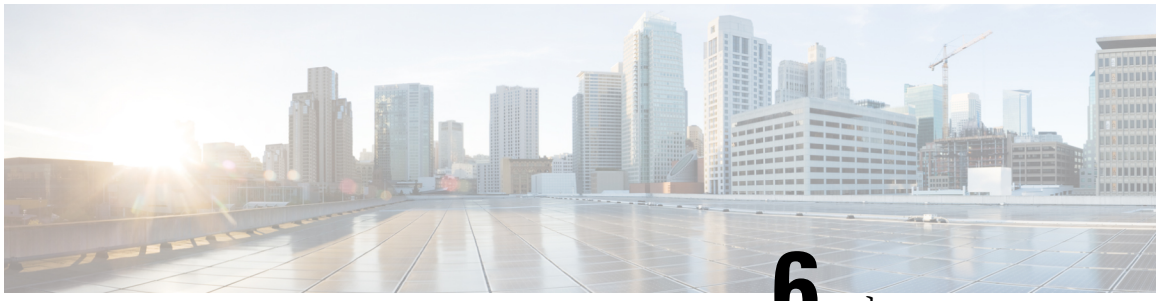
SEC에서 사용하는 포트 번호를 찾으려면 다음을 수행합니다.

단계 **1** CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.

단계 **2** Secure Connector(보안 커넥터) 페이지에서 이벤트를 전송할 SEC를 선택합니다.

단계 **3** Details(세부 정보) 창에 이벤트를 전송해야 하는 TCP, UDP 및 NetFlow(NSEL) 포트가 표시됩니다.





6 장

# Cisco SIG(Secure Internet Gateway)에 고객을 안전하게 연결



## Cisco Defense Orchestrator를 사용한 ASA 관리

Umbrella는 인터넷 기반 위협에 대한 여러 레벨의 방어를 제공하는 Cisco의 클라우드 기반 SIG(Secure Internet Gateway) 플랫폼입니다. Umbrella는 보안 웹 게이트웨이, 방화벽, DNS 레이어 보안 및 CASB(Cloud Access Security Broker) 기능을 통합하여 위협으로부터 시스템을 보호합니다. SIG 및 DNS 보호를 활용하면 ASA 디바이스는 디바이스의 로컬 DNS 검사 정책과 Umbrella 클라우드 기반 DNS 검사 정책 모두로 보호됩니다. Umbrella는 수신 트래픽을 검사하고 탐지할 수 있는 여러 가지 방법을 제공하므로 ASA 디바이스를 FTD 차세대 방화벽(NGFW)과 비교할 수 있습니다.

현재 CDO는 Umbrella 조직과의 ASA 통합만 지원합니다.

### SASE를 사용하여 브리지 구축

SASE(Secure Access Service Edge)는 네트워킹 및 보안 기능이 클라우드 에지에서 작동하여 보호 및 성능을 제공하는 단일 통합 서비스로 통합되는 미래 지향적인 프레임워크입니다. 이러한 노력을 통해 위치에 관계없이 서비스를 안전하게 통합할 수 있으며, 조직의 규모에 관계없이 네트워크를 제어하고 관리할 수 있습니다. 복잡성 감소 및 민첩한 관리는 구축이 간단하고 확장 가능하며 안전함을 의미합니다.

### Umbrella 조직이란?

Umbrella 조직은 단일 라이선스 키와 연결된 다양한 사용자 역할을 가진 사용자 그룹입니다. 단일 사용자가 여러 Umbrella 조직에 액세스할 수 있습니다. 모든 Umbrella 조직은 별도의 Umbrella 인스턴스이며 자체 대시보드가 있습니다. 조직은 이름 및 조직 ID(Org ID)로 식별됩니다. 조직 ID는 가상 어플라이언스와 같은 구성 요소를 구축하기 위해 조직을 식별하는 데 사용되며, 지원 부서에서 조직 ID를 요청할 수도 있습니다.

### SIG 터널이란?

SIG(Secure Internet Gateway) 터널은 ASA와 Umbrella 간에 발생하는 SIG IPSec(Internet Protocol Security) 터널의 인스턴스로, 모든 인터넷 바운드 트래픽이 검사 및 필터링을 위해 Umbrella SIG로 전달됩니다. 이 솔루션은 보안에 대한 중앙 집중식 관리를 제공하므로 네트워크 관리자가 각 브랜치에 대한 보안 설정을 별도로 관리할 필요가 없습니다.

터널이 구성된 Umbrella 조직을 온보딩하면 CDO의 사이트 간 VPN 페이지에 이러한 터널이 나열됩니다. CDO UI에서 Umbrella 조직에 대한 SASE 터널을 생성하려면 Umbrella용 SASE 터널 구성을 참조하십시오.

참고 Umbrella 조직 및 해당 피어 디바이스를 온보딩하는 경우 사이트 간 VPN 페이지는 해당 조직과 연결된 터널에 대한 모든 디바이스를 단일 항목으로 결합합니다. Tunnels(터널) 페이지를 수동으로 새로 고침하고 Umbrella 대시보드에서 변경한 내용을 읽으려면 Umbrella 터널 구성 읽기를 참조하십시오.

### CDO는 Umbrella와 어떻게 통신합니까?

Umbrella 조직 및 조직과 연결된 모든 ASA 디바이스를 온보딩해야 합니다.

ASA 디바이스가 Umbrella 클라우드와 연결된 경우 디바이스와 클라우드 간에 보안 연결을 생성하려면 사이트 간 VPN SIG 터널이 필요합니다. CDO는 Umbrella 조직 및 ASA 디바이스와 통신합니다. 이 이중 통신 방법을 통해 CDO는 구성 또는 터널 변경 사항의 변경 사항을 즉시 탐지하고 Umbrella, ASA 및 터널에 대한 아웃오브바운드 변경 사항, 오류 또는 비정상 상태를 즉시 사용자에게 알릴 수 있습니다.

Umbrella 조직을 CDO에 온보딩할 때 조직의 API 키 및 암호를 사용하여 온보딩합니다. 둘 다 조직 및 해당 조직과 연결된 ASA 디바이스에 고유합니다. CDO는 조직을 온보딩하여 ASA 디바이스에 대한 정보를 요청하고 전송하는 데 사용되는 API 키 및 암호를 사용하여 Umbrella API를 통해 Umbrella 클라우드와 통신합니다. 이 수준의 통신은 ASA와 Umbrella 클라우드 간에 존재하는 SIG 터널을 손상시키지 않습니다.

Umbrella 조직이 온보딩되면 Devices & Services(디바이스 및 서비스) 페이지에 해당 조직과 연결된 모든 탐지된 ASA 디바이스가 "피어"로 표시되고 디바이스가 CDO에 온보딩되었는지 여부가 표시됩니다. 피어 디바이스가 아직 온보딩되지 않은 경우 Onboard Device(디바이스 온보드)를 클릭하여 해당 페이지에서 직접 온보딩할 수 있습니다. Umbrella 조직과 연결된 ASA 디바이스가 CDO에 온보딩된 경우 Devices & Services(디바이스 및 서비스) 페이지에 관계가 표시되고 VPN Tunnels(VPN 터널) 페이지에 디바이스와 조직 간의 터널이 표시됩니다. 조직과 연결된 ASA 디바이스가 CDO에 온보딩되지 않은 경우 디바이스와 연결된 터널이 VPN Tunnels(VPN 터널)에 표시되며 이 페이지에서 디바이스를 직접 온보딩하도록 선택할 수 있습니다.

### CDO에서 Umbrella 클라우드에 액세스하려면 어떻게 해야 합니까?

Umbrella 조직이 CDO에 성공적으로 온보딩되면 조직의 대시보드 또는 CDO UI에서 Umbrella Tunnels(Umbrella 터널) 페이지로 교차 실행할 수 있습니다.

CDO UI에서 Umbrella 클라우드에 액세스하려면 Umbrella 대시보드에 대한 교차 실행, 529 페이지 및 Umbrella 터널 페이지에 대한 교차 실행, 530 페이지을 참조하십시오.

사전 요건

지원되는 하드웨어 및 소프트웨어

Umbrella 조직은 클라우드 기반이므로 버전이 없습니다. Umbrella 조직을 CDO에 온보딩하는 경우 해당 조직을 ASA 디바이스와만 연결할 수 있습니다.

Umbrella 통합의 경우 CDO는 9.1.2 이상을 실행하는 ASA 디바이스를 지원합니다. CDO가 지원하는 ASA 디바이스 모델 및 소프트웨어 목록은 클라우드 디바이스 지원 정보, 38 페이지의 내용을 참조하십시오.

라이센싱 요건

Umbrella 조직을 CDO에 성공적으로 온보딩하려면 다음 라이선스 패키지 중 하나를 선택해야 합니다.

- Umbrella SIG Essentials
- SIG Advantage

온보딩

Umbrella 어카운트를 성공적으로 관리하려면 Umbrella 조직 온보딩 및 이와 연결된 ASA 디바이스 온보딩를 모두 온보딩해야 합니다. Umbrella 조직을 온보딩하면 CDO는 해당 조직과 연결된 기존 ASA 터널을 읽고 이러한 터널의 상태 및 사용자가 생성하여 조직과 연결한 추가 터널을 모니터링합니다. Umbrella 조직을 온보딩하기 전에 일반 디바이스 요구 사항 및 온보딩 사전 요건을 검토합니다.

연결된 ASA 디바이스를 온보딩하기 전에 Umbrella 조직을 온보딩하는 경우 사이트 간 **VPN** 페이지에서 ASA 피어를 보고 VPN 페이지에서 디바이스를 온보딩할 수 있습니다.

참고 페일오버용으로 구성된 ASA 쌍이 있는 경우 두 피어의 액티브 디바이스만 온보드해야 합니다. 액티브 및 스탠바이 디바이스를 CDO에 온보딩하면 Umbrella에 이미 구성된 SASE 터널에 대한 중복 터널 정보가 생성될 수 있습니다.

네트워크 모니터링

CDO는 보안 정책의 영향을 요약한 보고서와 해당 보안 정책에 의해 트리거된 주요 이벤트를 보는 방법을 제공합니다. 또한 CDO는 디바이스에 대한 변경 사항을 기록하고 CDO에서 커밋하는 작업을 도움말 티켓 또는 기타 운영 요청과 연결할 수 있도록 이러한 변경 사항에 레이블을 지정하는 방법을 제공합니다.

변경 로그

변경 로그는 CDO에서 수행되는 구성 변경 사항을 지속적으로 캡처합니다. 이 단일 보기에는 지원되는 모든 디바이스 및 서비스에 대한 변경 사항이 포함됩니다. Umbrella는 클라우드 기반 제품이므로 변경 사항이 즉시 구축됩니다.

다음은 변경 로그의 몇 가지 기능입니다.

- 디바이스 구성에 대한 변경 사항을 나란히 비교합니다.

- 모든 변경 로그 항목에 대한 일반 영어 레이블입니다.
- 디바이스의 온보딩 및 제거를 기록합니다.
- CDO 외부에서 발생하는 정책 변경 충돌 탐지.
- 인시던트 조사 또는 문제 해결 중에 누가, 무엇을, 언제 하는지에 대한 답변을 제공합니다.
- 전체 변경 로그 또는 일부만 CSV 파일로 다운로드할 수 있습니다.

참고 Umbrella 조직과 연결된 SASE 터널을 생성, 편집 또는 삭제하면 Umbrella 조직 및 연결된 모든 ASA 디바이스에 대한 요청 및 구성 변경 사항이 나타납니다.

**Umbrella** 설명서

- Umbrella 도움말
- Umbrella 및 Cisco ASA 구성
- 터널을 통해 Cisco Umbrella에 연결
- Cisco Umbrella API

# Umbrella 조직 온보딩

## Umbrella 라이선스 요건

Umbrella 조직을 CDO에 성공적으로 온보딩하려면 Umbrella 대시보드에서 다음 라이선스 패키지 중 하나를 선택해야 합니다.

- Umbrella SIG Essentials
- SIG Advantage

현재 활성화된 라이선스를 확인하려면 Umbrella 대시보드에 로그인하여 **Admin(**관리자**)** > **Licensing(**라이선싱**)**으로 이동합니다.

## API 키 및 암호 생성

Umbrella 조직을 CDO에 온보딩하기 전에 새 API 키를 생성하고 **API** 키와 해당 암호를 모두 검색합니다.

현재 API 키가 없는 경우 다음 절차를 사용하여 생성합니다.

시작하기 전에

Umbrella의 관리 API 키는 다음 Umbrella 서비스에 사용됩니다.

- 네트워크 및 도메인
- 네트워크 터널
- 사용자 및 역할
- 대상 목록
- 통신 사업자

이러한 서비스에 대한 CDO 액세스를 허용하지 않으면 Umbrella 조직을 온보딩할 수 없습니다.

---

단계 **1** Cisco Umbrella 대시보드에 액세스하여 조직에 로그인합니다.

단계 **2** Umbrella 대시보드의 왼쪽 탐색창에서 **Admin(**관리**)**을 클릭하고 **API Keys(API** 키**)**를 선택합니다.

단계 **3** **Create API Key(API** 키 생성**)**를 클릭합니다.

API 키가 이미 있지만 암호를 저장하지 않은 경우 **Admin(**관리자**)** > **API Keys(API** 키**)** 화면으로 이동하여 **Refresh(**새로 고침**)**를 클릭하여 키와 암호를 업데이트합니다.

단계 **4** 새 API 키와 시크릿을 생성하려면 **+** 버튼을 클릭합니다.

단계 **5** 이름을 입력하고 API 키에 다음 범위를 추가합니다.

- 배포.
- 정책.

단계 **6** 키 생성를 클릭합니다.

단계 **7** API 키 및 해당 암호를 복사합니다. 사용할 준비가 될 때까지 참고 또는 .txt 파일에 임시로 붙여넣는 것이 좋습니다.

---

# Umbrella 조직 ID

조직을 CDO에 성공적으로 온보딩하려면 Umrbrella 조직의 조직 ID를 사용하여 조직 ID를 찾은 다음 로그인 자격 증명과 함께 사용해야 합니다.

---

단계 **1** Cisco Umbrella 대시보드에 액세스하여 조직에 로그인합니다.

단계 **2** 페이지 URL에는 숫자 식별자가 포함됩니다. 예를 들어 https://dashboard.umbrella.com/o/**123456**/#/overview의 조직 ID는 **123456**입니다.

단계 **3** URL에서 조직 ID를 복사합니다. 사용할 준비가 될 때까지 메모에 임시로 붙여넣는 것이 좋습니다.

---

# Umbrella 조직 온보딩

Umbrella 조직을 CDO에 온보딩하려면 다음 절차를 따릅니다.

시작하기 전에

이 환경을 온보딩하기 전에 Umbrella 라이선스 요건, 526 페이지을 읽어보십시오.

단계 **1** Umbrella 대시보드에서 Umbrella 조직 ID, 527 페이지 및 API 키 및 암호 생성, 526 페이지을 찾습니다. 이 절차 중에 이러한 항목을 사용할 수 있도록 준비합니다.

단계 **2** CDO에 로그인합니다.

단계 **3** 내비게이션 바에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **4** 파란색 더하기 버튼을 클릭하여 디바이스 온보딩을 시작합니다.

단계 **5** **Umbrella Organization(Umbrella** 조직**)**을 클릭합니다.

단계 **6** Umbrella 대시보드에서 생성한 Umbrella 네트워크 디바이스의 **API** 키와 해당 암호, Umbrella 대시보드 URL의 조직 **ID**를 입력합니다.

단계 **7** **Next(**다음**)**를 클릭합니다.

단계 **8** (선택 사항) 디바이스의 고유한 레이블을 추가합니다. 나중에 이 레이블을 기준으로 디바이스 목록을 필터링할 수 있습니다.

단계 **9** **Go to Inventory(**재고 목록으로 이동**)**를 클릭합니다.

# Umbrella 조직을 CDO에 다시 연결

경고! CDO는 저장된 자격 증명이 유효하지 않은 경우 Umbrella 조직에서 구성 변경 사항을 성공적으로 구축하거나 읽을 수 없지만, CDO는 조직과 연결된 ASA 디바이스에서 변경 사항을 성공적으로 구축하거나 읽을 수는 있습니다. 자격 증명이 업데이트되고 검증되면 이로 인해 문제가 발생할 수 있습니다. 구성 변경 사항을 구축하기 전에 조직 자격 증명을 업데이트하는 것이 좋습니다.

Umbrella 조직에 대한 API 키 및 암호가 새로 고쳐졌거나 시간이 초과된 경우 또는 Environment를 온보딩한 후 Cisco+ Secure Connect 선택를 활성화했는데 자격 증명이 더 이상 유효하지 않은 경우, 디바이스를 CDO에 수동으로 다시 연결해야 합니다. 다음 절차를 사용하여 다시 연결합니다.

단계 **1** Umbrella 대시보드로 이동합니다. Umbrella 대시보드의 왼쪽 탐색창에서 **Admin(**관리**)**을 클릭하고 Umbrella 관리 **API** 키를 선택합니다.

단계 **2** **Refresh(**새로 고침**)**를 클릭합니다. API 키 및 암호 새로 고침을 확인합니다.

단계 **3** API 키 및 해당 암호를 복사합니다.

단계 **4** CDO에 로그인합니다.

단계 **5** **Inventory(**인벤토리**)** 페이지로 이동합니다.

단계 **6** 필터 또는 검색 창을 사용하여 Umbrella 조직을 찾습니다.

단계 **7** Device Actions(디바이스 작업) 창에서 **Reconnect(**다시 연결**)**를 클릭합니다. CDO는 저장된 API 키 및 암호가 더 이상 유효하지 않음을 확인합니다.

단계 **8** 적절한 팝업 창에 API 키와 암호를 붙여넣습니다.

단계 **9** **Continue(**계속**)**를 클릭합니다.

단계 **10** CDO가 새 키와 암호가 유효함을 확인하면 **Close(**닫기**)**를 클릭합니다.

# Umbrella 대시보드에 대한 교차 실행

ASA 디바이스 및 Umbrella 조직이 CDO에 성공적으로 온보딩되면 CDO UI에서 조직의 대시보드로 교차 실행할 수 있습니다.

디바이스의 Umbrella 대시보드를 교차 실행하려면 다음 절차를 수행합니다.

단계 **1** CDO에 로그인합니다.

단계 **2** **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **3** Umbrella 조직을 찾거나 필터합니다.

단계 **4** Management(관리) 창에서 **Manage Umbrella Organization(Umbrella** 조직 관리**)**을 클릭합니다. CDO가 브라우저에서 선택한 조직과 연결된 Umbrella 대시보드를 여는 새 탭을 실행했습니다.

# CDO에서 디바이스 삭제

CDO에서 디바이스를 삭제하려면 다음 절차를 따르십시오.

단계 **1** CDO에 로그인합니다.

단계 **2** **Inventory(**인벤토리**)** 페이지로 이동합니다.

단계 **3** 삭제할 디바이스를 찾아 디바이스 행에서 디바이스를 확인하고 선택합니다.

단계 **4** 오른쪽에 있는 디바이스 작업 패널에서 **Remove(**제거**)**를 선택합니다.

단계 **5** 메시지가 표시되면 **OK(**확인**)**를 선택하여 선택한 디바이스 제거를 확인합니다. 디바이스를 온보딩 상태로 유지하려면 **Cancel(**취소**)**을 선택합니다.

# Umbrella 조직 구성

## Umbrella 터널 구성 읽기

Umbrella 조직이 CDO에 온보딩되면 수동으로 CDO가 Umbrella에서 터널 구성을 요청하고 업데이트하도록 강제할 수 있습니다. 여기에는 추가, 삭제 또는 편집된 터널이 포함됩니다.

경고! Umbrella 조직 자격 증명이 유효하지 않은 것으로 간주되거나 조직을 온보딩한 이후에 변경된 터널이 CDO에서 삭제된 경우 CDO는 해당 조직과 연결된 ASA 디바이스에만 터널 구성을 배포할 수 있습니다. 자격 증명을 업데이트하면 CDO가 Umbrella 구성을 읽고 삭제된 터널을 다시 채웁니다. Umbrella 조직에는 터널이 있지만 ASA 디바이스에는 없는 터널로 인해 동기화 문제가 발생하며 ASA 디바이스가 조직에 피어로 표시되지 않을 수 있습니다.

단계 **1** CDO에 로그인합니다.

단계 **2** **Devices & Services(**디바이스 및 서비스**)** 페이지에서 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** **SFCN** 탭을 클릭합니다.

단계 **4** Umbrella 조직을 선택하여 강조 표시합니다.

단계 **5** 작업 창에서 **Read Tunnels(**터널 읽기**)**를 선택합니다.

## Umbrella 터널 페이지에 대한 교차 실행

ASA 디바이스 및 Umbrella 조직이 CDO에 성공적으로 온보딩되면 CDO UI에서 터널용 Umbrellas 대시보드로 교차 실행할 수 있습니다.

디바이스의 Umbrella 터널 페이지를 교차 실행하려면 다음 절차를 수행합니다.

단계 **1** CDO에 로그인합니다.

단계 **2** VPN 창으로 이동합니다. **Site-to-Site VPN(**사이트 간 **VPN)**을 선택합니다.

단계 **3** 강조 표시되도록 원하는 터널을 선택합니다.

단계 **4** Actions(작업) 창에서 **Manage Tunnel in Umbrella(Umbrella**에서 터널 관리**)**를 클릭합니다. CDO가 브라우저에서 Tunnels Overview(터널 개요) 페이지를 여는 새 탭을 실행합니다.

## Umbrella용 SASE 터널 구성

다음 절차를 사용하여 Umbrella 조직에 대한 SASE 터널을 생성합니다.

시작하기 전에

터널을 생성할 Umbrella 조직 및 ASA 디바이스가 이미 CDO에 온보딩되어 있어야 합니다.

방금 구축한 터널과 연결된 ASA 또는 Umbrella 조직이 비정상 상태인 경우 CDO가 터널을 성공적으로 구축하지 못할 수 있습니다. 문제가 발생하는 경우 Cisco TAC에 문의하십시오.

단계 **1** CDO에 로그인합니다.

단계 **2** **VPN** 창으로 이동합니다. **Site-to-Site VPN(**사이트 간 **VPN)**을 선택합니다.

단계 **3** 파란색 더하기 버튼을 클릭하고 **Create SASE Tunnel(SASE** 터널 생성**)**을 선택합니다.

단계 **4** Umbrella 피어 정보를 입력합니다.

- **Umbrella** 선택 - 원하는 **Umbrella** 조직을 선택합니다.
- **Datacenter(**데이터 센터**)** - 헤드엔드 데이터 센터를 선택합니다. Umbrella 조직과 연결된 ASA와 지리적으로 가까운 데이터 센터를 선택하는 것이 좋습니다.

단계 **5** ASA 피어 정보를 입력합니다.

- **Select ASA Device(ASA** 디바이스 선택**)** - 드롭다운 목록에서 Umbrella 조직과 연결된 ASA 디바이스를 선택한 다음 **Select(**선택**)**를 클릭합니다.
- **Public Facing Interface(**공용 인터페이스**)** - 공개적으로 라우팅할 수 있는 고정 IPv4 주소를 선택합니다. 사용된 주소는 NAT에 사용할 수 없습니다.
- **LAN Address(LAN** 주소**)** - LAN 서브넷을 제어하는 LAN 인터페이스를 선택합니다. LAN에 대해 하나 이상의 인터페이스를 선택해야 합니다.
- **Virtual Tunnel Interface** - Umbrella 조직 및 ASA 피어 디바이스를 선택하면 이 필드가 자동으로 채워집니다. 필요한 경우 새 VTI로 사용할 IP 주소를 수동으로 입력할 수 있습니다.

단계 **6** Umbrella 조직 및 ASA 피어 디바이스를 선택하면 암호가 자동으로 채워집니다. **Confirm Passphrase(**암호 확인**)**도 자동으로 채워집니다. 필요한 경우 이러한 필드를 수동으로 입력할 수 있습니다.

단계 **7** (선택 사항) 팝업 창 하단에 있는 **Deploy changes to ASA(ASA**에 변경 사항 즉시 구축**)** 토글은 기본적으로 활성화되어 있습니다. 활성화하면 SASE 터널 구성이 터널 구성에서 선택한 ASA 피어에 즉시 구축됩니다. 변경 사항을 스테이징하고 나중에 구축하려면 옵션을 수동으로 전환하여 비활성화합니다.

단계 **8** **Deploy(**구축**)**를 클릭합니다. 선택적으로, 이 SASE 터널을 구축하는 동시에 다른 터널을 생성하려면 **Deploy and Create Another(**구축 및 다른 생성**)**를 클릭합니다. 구축이 완료되면 터널이 VPN Tunnels(VPN 터널) 페이지에 표시됩니다. **Deploy and Create Another SASE tunnel(**다른 **SASE** 터널 구축 및 생성**)**을 선택하는 경우 CDO는 Umbrella 조직 선택 사항과 **Deploy changes to ASA immediately(**즉시 **ASA**에 변경 사항 구축**)** 토글 설정을 모두 저장하고 이러한 선택 사항을 다음 터널 구성에 자동으로 적용합니다. 구축하기 전에 이러한 선택 사항을 수동으로 변경할 수 있습니다.

# SASE 터널 수정

기존 SASE 터널을 수정하려면 다음 절차를 수행합니다.

단계 1 CDO에 로그인합니다.

단계 2 **VPN** 창으로 이동합니다. **Site-to-Site VPN(**사이트 간 **VPN)**을 선택합니다.

단계 3 수정할 터널을 선택합니다.

단계 4 작업 창에서 **Edit(**편집**)**를 클릭합니다.

단계 5 SASE 터널의 다음 필드를 편집합니다.

- **Name(**이름**)** - CDO 및 Umbrella 대시보드에 표시되는 SASE 터널의 이름을 변경합니다.
- **Umbrella** 피어의 데이터 센터 - 드롭다운 메뉴에서 새 헤드엔드 데이터 센터를 선택합니다.
- **ASA Peer's Public Facing Interface(ASA** 피어의 공용 인터페이스**)** - 드롭다운 메뉴에서 새 IPv4 주소를 선택합니다.
- **ASA Peer's LAN Interfaces(ASA** 피어의 **LAN** 인터페이스**)** - 드롭다운 메뉴에서 하나 이상의 새 LAN 인터페이스를 선택합니다.
- **ASA VTI(Virtual Tunnel Interface)** 주소 - VTI를 수동으로 편집합니다.
- **Passphrase(**암호**)** - 터널의 암호를 수동으로 수정합니다.
- **Confirm Passphrase(**암호 확인**)** - 암호와 일치하도록 이 항목을 수동으로 수정하고 새 값을 확인합니다.

단계 6 (선택 사항) 팝업 창 하단에 있는 **Deploy changes to ASA(ASA**에 변경 사항 즉시 구축**)** 토글은 기본적으로 활성화되어 있습니다. 활성화하면 SASE 터널 구성이 터널 구성에서 선택한 ASA 피어에 즉시 구축됩니다. 변경 사항을 스테이징하고 나중에 구축하려면 옵션을 수동으로 전환하여 비활성화합니다. 변경 사항을 스테이징하고 나중에 구축하도록 선택하는 경우 **Inventory(**인벤토리**)** 페이지에서 ASA 피어 상태가 `Deploy Pending(구축 보류 중)`으로 표시됩니다.

단계 7 **Save Updates(**업데이트 저장**)**를 선택합니다.

# Umbrella에서 SASE 터널 삭제

CDO UI를 통해 SASE 터널을 삭제하려면 다음 절차를 수행합니다.

시작하기 전에

SASE 터널을 삭제하려면 연결된 ASA가 CDO에서 동기화된 상태여야 합니다. 디바이스가 비정상인 경우 터널을 삭제할 수 없습니다.

CDO에서 SASE 터널을 삭제하면 ASA 디바이스 및 연결된 Umbrella 조직에서 터널이 제거됩니다.

경고! Umbrella 조직 자격 증명이 유효하지 않은 것으로 간주되거나 조직을 온보딩한 이후 변경된 경우 CDO에서 터널을 삭제하면, CDO는 조직과 연결된 ASA 디바이스에만 터널 구성을 배포할 수 있습니다. 자격 증명을 업데이트하면 CDO가 Umbrella 구성을 읽고 삭제된 터널을 다시 채웁니다. Umbrella 조직에는 터널이 있지만 ASA 디바이스에는 없는 터널로 인해 동기화 문제가 발생하며 ASA 디바이스가 조직에 피어로 표시되지 않을 수 있습니다. 조직과 연결된 터널을 삭제하기 전에 Umbrella 자격 증명을 확인하는 것이 좋습니다.

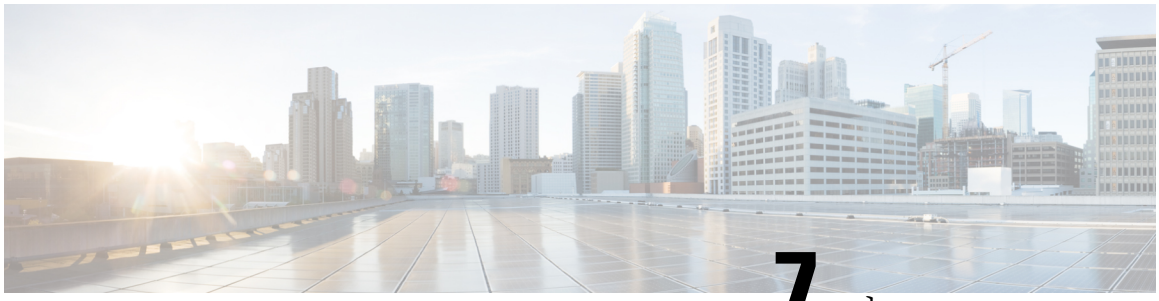
단계 **1** CDO에 로그인합니다.

단계 **2** **VPN** 창으로 이동합니다. **Site-to-Site VPN(**사이트 간 **VPN)**을 선택합니다.

단계 **3** CDO에서 삭제할 터널을 선택합니다.

단계 **4** Actions(작업) 창에서 **Delete(**삭제**)**를 클릭합니다.

단계 **5** 터널 삭제를 확인하고 **OK(**확인**)**를 클릭합니다.



7 장

# CDO와 Cisco Security Cloud Sign On 통합



## SecureX 및 CDO

Cisco SecureX 플랫폼은 가시성을 통합하고 자동화를 가능하게 하며 네트워크, 엔드포인트, 클라우드 및 애플리케이션 전반에서 보안을 강화하는 일관된 경험을 위해 Cisco의 광범위한 통합 보안 포트폴리오와 고객의 인프라를 연결합니다. 통합 플랫폼에서 기술을 연결함으로써 SecureX는 측정 가능한 통찰력, 바람직한 결과 및 더할 나위 없는 팀 간 협업을 제공합니다. SecureX가 무엇이고 이 플랫폼이 제공하는 기능에 대한 자세한 내용은 SecureX 정보를 참조하십시오.

SecureX가 CDO 테넌트에 액세스하도록 허용하면 총 디바이스 수는 물론 오류가 있는 디바이스, 충돌이 있는 디바이스 및 현재 동기화되지 않을 수 있는 디바이스를 포함하여 디바이스 이벤트가 요약됩니다. 이벤트 요약은 또한 현재 적용된 정책 및 해당 정책과 관련된 개체를 집계하는 두 번째 창을 제공합니다. 정책은 디바이스 유형으로 정의되며 개체는 개체 유형을 통해 식별됩니다.

SecureX 대시보드에 CDO 모듈을 추가하려면 여러 단계가 필요합니다. 자세한 내용은 CDO을 SecureX에 추가를 참조하십시오.

**Warning** CDO 및 SecureX 계정을 아직 병합하지 않은 경우, 온보딩된 모든 디바이스에 대한 이벤트가 표시되지 않을 수 있습니다. SecureX에서 CDO 모듈을 생성하기 전에 계정을 병합하는 것을 강력히 권장합니다. 자세한 내용은 CDO 및 SecureX 계정 병합을 참조하십시오.

### SecureX 리본

SecureX 리본은 SecureX 계정 생성 여부와 상관없이 CDO에서 사용할 수 있습니다. 페이지 하단에 있는 SecureX 탭 

을 클릭하여 리본을 확장합니다.

리본을 사용하려면 SecureX 계정을 확인해야 합니다. SecureX에 액세스하는 데 사용하는 것과 동일한 인증 로그인을 사용하는 것이 좋습니다. 리본이 인증되면 CDO에서 직접 SecureX 기능을 활용할 수 있습니다.

자세한 내용은 SecureX 리본 설명서를 참조하십시오.

**SecureX** 문제 해결

이 경험에는 두 가지 제품이 포함됩니다. 발생할 수 있는 문제를 식별, 해결 또는 문의하는 데 도움이 되도록 SecureX 문제 해결 , on page 590을 참조하십시오.

관련 정보:

- SecureX 정보
- CDO 및 SecureX 계정 병합
- CDO에서 SecureX 연결, on page 537
- CDO에서 SecureX 연결 끊김, on page 538
- CDO을 SecureX에 추가
- SecureX 문제 해결 , on page 590

# CDO 및 SecureX 계정 병합

이미 SecureX 또는 CTR(Cisco Threat Response) 계정이 있는 경우 디바이스를 SecureX에 등록하려면 CDO 테넌트와 SecureX/CTR 계정을 병합해야 합니다. 계정을 SecureX 포털에 병합할 수 있습니다. CDO 모듈을 만들기 전에 계정을 병합하는 것이 매우 좋습니다. 계정이 병합될 때까지 SecureX에서 디바이스의 이벤트를 보거나 다른 SecureX 기능을 이용할 수 없습니다.

**Note** 이 프로세스를 시작할 때 유의하십시오. CDO을 SecureX에 병합하는 데에는 시간이 오래 걸릴 수 있습니다.

자세한 내용은 계정 병합을 참조하십시오.

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

관련 정보:

- SecureX 및 CDO
- CDO을 SecureX에 추가
- SecureX 문제 해결

# CDO을 SecureX에 추가

SecureX가 등록된 디바이스에 액세스하도록 허용하고 SecureX 대시보드에 CDO 모듈을 추가하여 보안 포트폴리오의 다른 Cisco 플랫폼과 함께 디바이스 정책 및 개체 요약을 확인합니다.

**Note** 이 프로세스를 시작할 때 유의하십시오. CDO을 SecureX에 병합하는 데에는 시간이 오래 걸릴 수 있습니다.

시작하기 전에

CDO에서 SecureX를 연결하기 전에 다음 항목을 작업하는 것이 매우 좋습니다.

- 최소한 SecureX 계정에 대한 관리자여야 합니다.
- CDO 테넌트에 대한 슈퍼 관리자 사용자 역할이 있어야 합니다.
- 테넌트 통신을 용이하게 하기 위해 보안 서비스 익스체인지에 테넌트 계정을 병합합니다. 자세한 내용은 CDO 및 SecureX 계정 병합을 참조하십시오.
- CDO 테넌트를 보안 서비스 익스체인지와 병합한 후, CDO 테넌트에서 로그아웃하고 다시 로그인해야 합니다.
- 아직 구성하지 않은 경우 Cisco Secure Sign-On을 MFA(Multi-Factor Authentication)용 SAML SSO(Single Sign-On IdP) 및 Duo Security로 구성합니다. CDO 및 SecureX는 이를 인증 방법으로 사용합니다. 자세한 내용은 SAML SSO(Single Sign-On)를 Cisco Defense Orchestrator와 통합을 참조하십시오.

**Note** 참고: 테넌트가 여러 개인 경우 SecureX에서 테넌트당 하나의 모듈을 생성해야 합니다. 각 테넌트는 인증을 위해 고유한 API 토큰이 필요합니다.

## CDO에서 SecureX 연결

SecureX 및 CDO 계정을 병합한 후 두 플랫폼 간의 통신을 승인하고 수동으로 CDO 모듈을 SecureX 대시보드에 추가하도록 활성화해야 합니다. CDO UI를 통해 SecureX를 연결하고 보안 포트폴리오의 다른 Cisco 플랫폼과 함께 디바이스의 정책, 이벤트 유형, 개체 등에 대한 요약을 확인합니다.

**Note** SecureX 대시보드에 구성된 CDO 모듈이 이미 있는 경우 **Connect Tenant to SecureX** 옵션은 중복 CDO 모듈을 생성합니다. 이 문제가 발생하면 자세한 내용은 SecureX 문제 해결 을 참조하십시오.

다음 절차를 사용하여 CDO에서 API 토큰을 조달하고 CDO 모듈을 SecureX에 추가합니다.

단계 **1** CDO에 로그인합니다.

단계 **2** 오른쪽 상단 모서리에 있는 사용자 메뉴에서 **Settings(**설정**)**을 선택합니다.

단계 **3** 창 왼쪽에서 **General Settings(**일반 설정**)** 탭을 선택합니다.

단계 **4** **Tenant Settings(**테넌트 설정**)** 섹션을 찾아 **Connect SecureX(SecureX** 연결**)**를 클릭합니다. 브라우저 창이 SecureX 로그인 페이지로 리디렉션됩니다. CDO 테넌트와 연결하려는 조직 자격 증명으로 SecureX에 로그인합니다.

단계 5 SecureX에 성공적으로 로그인하면 브라우저가 자동으로 다시 CDO로 리디렉션됩니다. **General Settings(**일반 설정**)** 페이지의 **User Management (**사용자 관리**)** 탭에서 SecureX에 로그인한 조직의 이름을 포함하는 새 사용자를 볼 수 있습니다. 이 사용자는 읽기 전용이며 SecureX로 데이터를 보내는 데만 사용됩니다.

## CDO에서 SecureX 연결 끊김

CDO와 SecureX 조직 간의 통신 요청 연결을 끊을 수 있습니다. 이 옵션은 SecureX에서 조직을 제거하지 않지만, CDO에서 읽기 전용 API 사용자를 제거하고 이전에 SecureX 조직과 연결된 테넌트는 이벤트 보고서 전송을 중지합니다.

이것은 CDO의 SecureX 리본에서 테넌트를 로그아웃하거나, 어떠한 방식으로든 리본을 비활성화하지 않습니다. 리본에서 로그아웃하려면 Support Case Manager(지원 사례 매니저)에서 사례를 열어 리본 로그인을 수동으로 재설정해야 합니다. 이 요청은 테넌트를 리본에서 로그아웃합니다.

단계 1 CDO에 로그인합니다.

단계 2 오른쪽 상단 모서리에 있는 사용자 메뉴에서 **Settings(**설정**)**을 선택합니다.

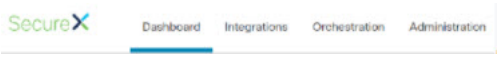
단계 3 창 왼쪽에서 **General Settings(**일반 설정**)** 탭을 선택합니다.

단계 4 **Tenant Settings(**테넌트 설정**)** 섹션을 찾아 SecureX **Disconnect(**연결 끊기**)**를 클릭합니다. **General Settings(**일반 설정**)** 페이지의 **User Management(**사용자 관리**)** 탭에서, SecureX로 데이터를 보내기 위해 생성된 읽기 전용 사용자가 삭제됩니다.

## CDO 타일을 SecureX에 추가

CDO 모듈을 활성화한 후 이제 CDO 타일을 SecureX 대시보드에 추가할 수 있습니다. 제품의 모듈은 CDO의 상태 정보에 액세스하고 두 가지 가능한 타일 선택을 통해 대시보드에 데이터를 보고합니다.

SecureX 대시보드에 CDO 타일을 추가하려면 다음 절차를 따르십시오.

단계 1 SecureX 대시보드탭에서 

**New Dashboard(**새 대시보드**)**를 클릭합니다. SecureX 대시보드에 처음 액세스하는 경우 **Add Tiles(**타일 추가**)**를 클릭할 수도 있습니다.

단계 2 (선택 사항) 대시보드 이름을 변경합니다.

**Tip** 테넌트가 여러 개인 경우 이 이름 변경 옵션을 사용하여 CDO 타일이 연결된 테넌트를 식별합니다.

단계 3 **Available Tiles(**사용 가능한 타일**)** 목록에서 CDO를 선택하고 옵션을 확장하여 사용 가능한 타일을 확인합니다. 대시보드에 포함하려는 모든 타일을 선택합니다.

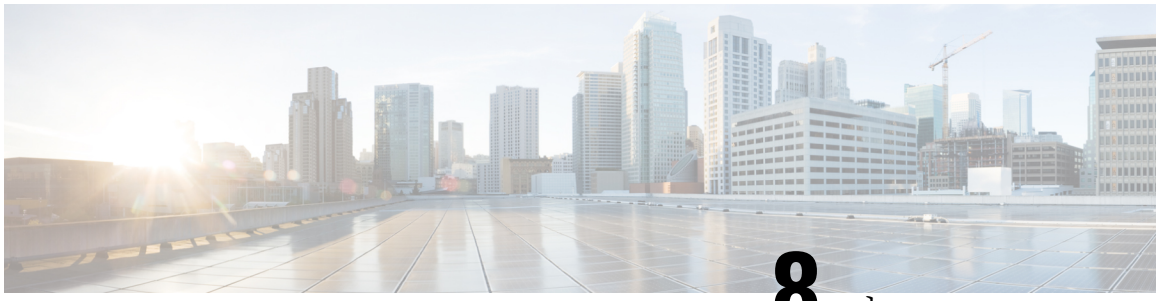
- **CDO Device Summary(CDO** 디바이스 요약**)** - 이 타일에는 현재 CDO 테넌트에 온보딩된 모든 디바이스와 해당 상태가 나열됩니다.
- **CDO Objects and Policies(CDO** 개체 및 선택**)** - 이 타일에는 디바이스에 현재 적용된 모든 정책 및 해당 정책과 관련된 개체가 나열됩니다.

**Note** CDO가 나열되지 않으면, SecureX에 저장된 CDO의 유효한 API 토큰이 없는 것입니다. 자세한 내용은 CDO 타일을 SecureX에 추가을 참조하십시오.

단계 **4** **Save(**저장**)**를 클릭합니다.

관련 정보**:**

- CDO 및 SecureX 계정 병합
- SecureX 문제 해결



8 장

# 문제 해결

이 장에는 다음 섹션이 포함되어 있습니다.



# Secure Firewall ASA 디바이스 문제 해결

## 재부팅 후 ASA가 CDO에 다시 연결하지 못함

ASA를 재부팅한 후 CDO와 ASA가 연결되지 않으면 ASA가 CDO의 SDC(보안 디바이스 커넥터)에서 지원하지 않는 OpenSSL 암호 그룹을 사용하도록 대체되었기 때문일 수 있습니다. 이 문제 해결 항목은 해당 사례를 테스트하고 문제 해결 단계를 제공합니다.

### 증상

- ASA가 재부팅되고 CDO와 ASA가 다시 연결되지 않습니다. CDO는 "다시 연결하지 못했습니다."라는 메시지를 표시합니다.
- ASA 온보딩을 시도할 때 CDO는 다음 메시지를 표시합니다. <*ASA_IP_Address*>에 대한 인증서를 검색할 수 없습니다.

## 인증서 오류로 인해 ASA를 온보딩할 수 없음

환경: ASA가 클라이언트 측 인증서 인증으로 구성되었습니다.

해결책 : 클라이언트 측 인증서 인증을 비활성화합니다.

세부 정보: ASA는 자격 증명 기반 인증 및 클라이언트 측 인증서 인증을 지원합니다. CDO는 클라이언트 측 인증서 인증을 사용하는 ASA에 연결할 수 없습니다. ASA를 CDO에 온보딩하기 전에 다음 절차를 사용하여 클라이언트 인증서 인증이 활성화되어 있지 않은지 확인합니다.

단계 **1** 터미널 창을 열고 SSH를 사용하여 ASA에 연결합니다.

단계 **2** 전역 구성 모드를 시작합니다.

단계 **3** hostname (config)# 프롬프트에서 다음 명령을 입력합니다.

**no ssl certificate-authentication interface***interface-name***port 443**

인터페이스 이름은 CDO가 연결하는 인터페이스의 이름입니다.

## ASA에서 사용하는 OpenSSL 암호 그룹 확인

이 절차를 사용하여 ASA에서 사용 중인 OpenSSL 암호화 제품군을 식별합니다. 명령 출력에 명명된 암호 제품군이 CDO의 보안 디바이스 커넥터가 지원하는 Cipher Suites에 없는 경우 SDC에서 해당 암호 그룹을 지원하지 않으므로 ASA에서 암호 그룹을 업데이트해야 합니다.

단계 **1** SDC에 연결할 수 있는 컴퓨터에서 콘솔 창을 엽니다.

단계 **2** SSH를 사용하여 SDC에 연결합니다. CDO 또는 SDC와 같은 일반 사용자 또는 생성한 다른 사용자로 로그인할 수 있습니다. 루트로 로그인할 필요가 없습니다.

**Tip** SDC IP 주소를 찾으려면 다음을 수행합니다.

**a.** CDO를 엽니다.

**b.** 사용자 메뉴에서 Secure Connector(보안 커넥터)를 선택합니다.

**c.** 표에 표시된 SDC를 클릭합니다. SDC의 IP 주소는 디바이스의 세부 정보 창에 표시됩니다.

단계 **3** 명령 프롬프트에 다음을 입력합니다. **openssl s_client -showcerts -connect***ASA_IP_Address***:443**

단계 **4** 명령 출력에서 다음 행을 찾으십시오.

```
New, TLSV1/SSLv3, Cipher is DES-CB3-SHA
or
SSL-Session:
            Protocol: TLSv1.2
            Cipher: DES-CB3-SHA
```

이 예에서 ASA에서 사용 중인 암호화 제품군은 `DES-CB3-SHA`입니다.

## CDO의 보안 디바이스 커넥터가 지원하는 Cipher Suites

CDO의 보안 디바이스 커넥터는 가장 안전한 최신 암호만 허용하는 node.js를 사용합니다. 결과적으로 CDO의 SDC는 다음 암호 목록만 지원합니다.

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA256
- DHE-RSA-AES256-SHA256

ASA에서 사용하는 암호 제품군이 이 목록에 없는 경우, SDC에서 지원하지 않으므로 ASA의 암호 그룹 업데이트.

## ASA의 암호 그룹 업데이트

**ASA**에서 **TLS** 암호 그룹을 업데이트하려면 다음을 수행합니다**.**

단계 **1** SSH를 사용하여 ASA에 연결합니다.

단계 **2** ASA에 연결되면 권한을 전역 구성 모드로 승격합니다. 프롬프트는 다음과 같이 표시됩니다. asaname(config)#

단계 **3** 프롬프트에서 다음과 유사한 명령을 입력합니다.

```
ssl cipher tlsv1.2 custom "ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384 DHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256
 DHE-RSA-AES128-SHA256 ECDHE-RSA-AES256-SHA384 DHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA256
DHE-RSA-AES256-SHA256"
```

**Note** 이 명령이 지원하도록 ASA를 구성하는 암호 그룹은 따옴표 사이에 그리고 custom이라는 단어 뒤에 포함됩니다. 이 명령에서 지정된 암호 그룹은 `ECDHE-RSA-AES128-GCM-SHA256`으로 시작하여 `DHE-RSA-AES256-SHA256`으로 끝납니다. ASA에서 명령을 입력할 때 ASA에서 지원하지 않는 모든 암호 그룹을 제거합니다.

단계 **4** 명령을 제출한 후 프롬프트에서 write memory를 입력하여 로컬 구성을 저장합니다. 예: `asaname(config)#` **`write memory`**

# CLI 명령을 사용하여 ASA 문제 해결

이 섹션에서는 ASA 문제를 해결하고 기본 연결을 테스트하는 데 사용할 수 있는 몇 가지 중요한 명령에 대해 설명합니다. 다른 문제 해결 시나리오 및 CLI 명령에 대해 알아보려면 CLI 책 1: Cisco ASA

Series 일반 작업 CLI 구성 가이드를 참조하십시오. '시스템 관리' 섹션에서 '테스트 및 문제 해결' 장으로 이동합니다.

각 ASA 디바이스에서 사용할 수 있는 CDO CLI 인터페이스를 사용하여 이러한 명령을 실행할 수 있습니다. CDO에서 CLI 인터페이스를 사용하는 방법에 대해 알아보려면 CDO 명령줄 인터페이스을 참조하십시오.

### NAT 정책 설정

NAT 설정을 결정하는 몇 가지 중요한 명령은 다음과 같습니다.

- NAT 정책 통계를 확인하려면 **show nat**를 사용합니다.
- 할당된 주소와 포트를 포함한 NAT 풀과 할당된 횟수를 확인하려면 **show nat pool**을 사용합니다.

NAT와 관련된 추가 명령은 CLI 책 2: Cisco ASA Series Firewall CLI 구성 가이드를 참조하고 'NAT(Network Address Translation)' 장으로 이동하십시오.

### 기본 연결 테스트: 주소 ping하기

ASA CLI 인터페이스에서 **ping <IP address>** 명령을 사용하여 ASA 디바이스를 ping할 수 있습니다. 기존

### 라우팅 테이블 표시

라우팅 테이블의 항목을 보려면 **show route** 명령을 사용합니다.

**ciscoasa# show route**

ASA의 라우팅 테이블에 대한 출력 예:

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF
마지막 수단의 게이트웨이는 네트워크 0.0.0.0에 대한 192.168.0.254입니다.
S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.0.254, 관리
C 10.0.0.0 255.0.0.0 직접 연결, 외부
L 10.10.10.1 255.255.255.255 직접 연결, 외부
C 192.168.0.0 255.255.255.0 직접 연결, 관리
L 192.168.0.118 255.255.255.255 직접 연결, 관리
```

스위치 포트 모니터링

- **show interface**

  인터페이스 통계를 표시합니다.

- **show interface ip brief**

  인터페이스 IP 주소와 상태를 표시합니다.

- **show arp**

동적, 정적 및 프록시 ARP 항목을 표시합니다. 동적 ARP 항목에는 ARP 항목의 기간(초)가 포함됩니다.

ARP 항목의 출력 예:

```
관리 10.10.32.129 0050.568a.977b 0
관리 10.10.32.136 0050.568a.5387 21
LANFAIL 20.20.21.1 0050.568a.4d70 96
outsi 10.10.16.6 0050.568a.e6d3 3881
outsi 10.10.16.1 0050.568a.977b 5551
```

# ASA 원격 액세스 VPN 문제 해결

이 섹션에서는 ASA 디바이스에서 원격 액세스 VPN을 구성할 때 발생할 수 있는 몇 가지 문제 해결 문제에 대해 설명합니다.

### RA VPN 모니터링 페이지에서 누락된 정보

이 문제는 Webvpn에 대해 외부 인터페이스가 활성화되지 않은 경우 발생할 수 있습니다.

해결 방법:

1. 탐색 창에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.
2. **Devices(**디바이스**)** 탭을 클릭한 다음 **ASA** 탭을 클릭합니다.
3. 문제가 있는 RA VPN 헤드엔드 ASA 디바이스를 선택합니다.
4. 오른쪽의 관리 창에서 **Configuration(**구성**)**를 클릭합니다.
5. **Edit(**편집**)**를 클릭하고 'webvpn'을 검색합니다.
6. **Enter(**엔터**)**를 누르고 `enable` *interface_name*를 추가합니다. 여기서 interface_name은 원격 액세스 VPN 연결을 만들 때 사용자가 연결하는 외부 인터페이스의 이름입니다. 이 인터페이스는 대개 외부(인터넷 연결) 인터페이스이지만, 이 연결 프로파일을 사용하여 지원하려는 디바이스와 엔드 유저 간의 인터페이스를 선택하면 됩니다.

   예를 들면 다음과 같습니다.

   ```
   webvpn
   ```

```
enable outside
```

7. **Save(**저장**)**를 클릭합니다.
8. 디바이스에 구성을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축합니다.

# 기존 RA VPN 구성에 ASA를 추가할 수 없음

•

시작하기 전에

•

**SUMMARY STEPS**

1.

**DETAILED STEPS**

| | 명령 또는 동작 | 목적 |
|---|---|---|
| 단계 1 | 예제: | |

예

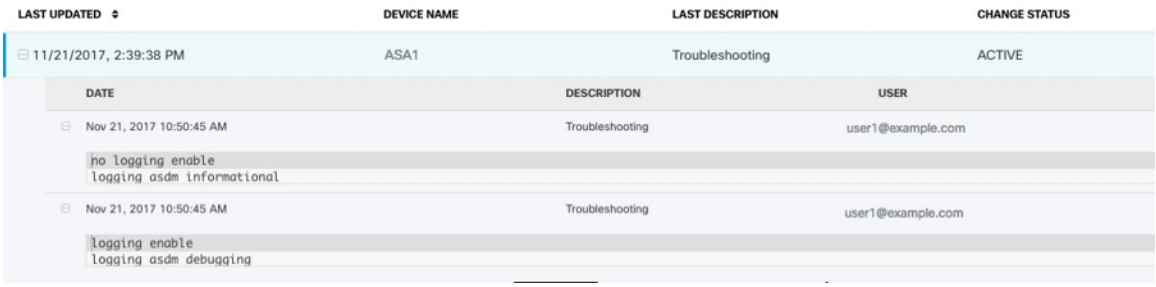
다음에 수행할 작업

•

# ASA 실시간 로깅

실시간 로깅을 사용하여 로깅된 데이터의 마지막 20초 또는 로깅된 데이터의 마지막 10KB 중 먼저 도달하는 한계에 도달하는 데이터를 표시합니다. CDO는 실시간 데이터를 검색할 때, ASDM의 기존 로깅 구성을 검토하고, 디버깅 수준 데이터를 요청하도록 변경한 다음, 로깅 구성을 구성으로 반환합니다. 로깅 CDO 디스플레이에는 ASDM에서 설정했을 수 있는 모든 로깅 필터가 반영됩니다.

변경 로그를 검토하면 CDO가 로깅을 수행하기 위해 보내는 명령을 볼 수 있습니다. 다음은 변경 로그 항목의 예입니다. 첫 번째 항목(하단)은 CDO가 로깅 활성화 명령으로 로깅을 "켜고" ASDM 로깅 수준을 디버깅으로 변경했음을 나타냅니다. 두 번째 항목(상단)은 로깅 구성이 이전 상태로 돌아갔음을 보여줍니다. no logging enable 명령으로 로깅이 "꺼지고" ASDM 로깅 수준이 정보로 돌아갔습니다.




## ASA 실시간 로그 보기

단계 **1** **Devices & Services(**디바이스 및 서비스**)** 페이지에서 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **2** 적절한 디바이스 유형 탭을 클릭하고 실시간 데이터를 보려는 디바이스를 선택합니다.

단계 **3** **Troubleshoot(**문제 해결**)** Troubleshoot 를 클릭합니다.

단계 **4** (선택 사항) 실시간 로그 보기를 클릭하기 전에 왼쪽 창에서 필터를 정의하여 로그 검색 결과를 구체화할 수 있습니다.

단계 **5** **View Real-time Log(**실시간 로그 보기**)**를 클릭합니다. CDO는 필터링 기준에 따라 실시간 로그 데이터를 검색하여 표시합니다.

단계 **6** 기록된 데이터의 추가 20초 또는 기록된 데이터의 마지막 10KB를 보려면. **View Real-Time Log(**실시간 로그 보기**)**를 다시 클릭합니다.

# AT 패킷 트레이서

패킷 트레이서를 사용하면 합성 패킷을 네트워크로 보내고 기존 라우팅 구성, NAT 규칙 및 정책 구성이 해당 패킷에 미치는 영향을 평가할 수 있습니다. 이 도구를 사용하여 다음과 같은 종류의 문제를 해결합니다.

- 사용자가 연결 가능해야 하는 리소스에 연결할 수 없다고 보고합니다.
- 사용자가 연결할 수 없어야 하는 리소스에 연결할 수 있다고 보고합니다.
- 정책을 테스트하여 예상대로 작동하는지 확인합니다.

패킷 트레이서는 실제 또는 가상의 라이브 온라인 ASA 디바이스에서 사용할 수 있습니다. 패킷 트레이서는 디바이스 유형에서 작동하지 않습니다. 패킷 트레이서는 ASA에 저장된 구성을 기반으로 패킷을 평가합니다. CDO의 준비된 변경 사항은 패킷 트레이서에 의해 평가되지 않습니다.

동기화된 ASA에서 패킷 트레이서를 실행하는 것이 모범 사례라고 생각합니다. 디바이스가 동기화되지 않은 경우 패킷 트레이서가 실행되지만 예기치 않은 결과가 발생할 수 있습니다. 예를 들어 CDO의 준비된 구성에서 규칙을 삭제하고 패킷 추적 중에 ASA에서 동일한 규칙이 트리거된 경우 CDO는 해당 규칙과 패킷의 상호 작용 결과를 표시할 수 없습니다.

### ASA 패킷 트레이서 관련 문제 해결

패킷 트레이서는 ASA의 라우팅 구성, NAT 규칙 및 보안 정책을 통해 패킷을 보낼 때 각 단계에서 패킷의 상태를 표시합니다. 정책에서 패킷을 허용하면 녹색 확인 표시가 나타납니다. 패킷이 거부되고 삭제되면 CDO는 빨간색 X를 표시합니다.

패킷 트레이서는 패킷 추적 결과의 실시간 로그도 표시합니다. 아래 예에서 규칙이 tcp 패킷을 거부한 위치를 확인할 수 있습니다.


## ASA 디바이스 보안 정책 문제 해결

단계 **1** **Devices & Services(**디바이스 및 서비스**)** 페이지에서 ASA를 선택하고 Actions 창에서 **Troubleshoot(**문제 해결**)** Troubleshoot 를 클릭합니다.

단계 **2** Values(값) 창에서 ASA를 통해 가상으로 전송할 인터페이스 및 패킷 유형을 선택합니다.

단계 **3** (선택 사항) Layer 2 CMD 헤더(Trustsec)에 보안 그룹 태그 값이 내장된 패킷을 추적하려면 SGT 번호를 확인하고 보안 그룹 태그 번호 0-65535를 입력합니다.

단계 **4** 소스와 대상을 지정합니다. Cisco Trustsec을 사용하는 경우, IPv4 또는 IPv6 주소, 정규화된 도메인 이름(FQDN) 또는 보안 그룹 이름 또는 태그를 지정할 수 있습니다. 소스 주소의 경우, 또한 형식 Domain\username에 사용자 이름을 지정할 수 있습니다.

단계 **5** 기타 프로토콜 특성 지정:

- ICMP - ICMP 유형, ICMP 코드(0-255) 및 선택사항인 ICMP ID를 입력합니다.
- TCP/UDP/SCTP- 목록에서 선택하거나 포트 콤보 상자에 값을 입력하여 소스 및 대상 포트를 입력합니다.
- IP - 0-255 사이의 프로토콜 번호를 입력합니다.

단계 **6** **Run Packet Tracer(**패킷 추적기 실행**)**를 클릭합니다.

단계 **7** 패킷 트레이서 결과 분석를 계속합니다.

## 액세스 규칙 문제 해결

단계 **1** **Policies(**정책**)** > **Network Policies(**네트워크 정책**)** > 를 선택합니다**.**

단계 **2** ASA와 연결된 정책을 선택합니다.

단계 **3** 네트워크 정책에서 문제를 해결할 규칙을 선택하고 세부 정보 창에서 Troubleshoot 문제 해결를 클릭합니다. 문제 해결 페이지의 값 패널에서 많은 필드가 선택한 규칙의 속성으로 미리 채워져 있습니다.

단계 **4** 나머지 필수 필드에 정보를 입력합니다. 모든 필수 필드를 완료하면 Run Packet Tracer(패킷 트레이서 실행)가 활성화됩니다.

단계 **5** **Run Packet Tracer(**패킷 추적기 실행**)**를 클릭합니다.

단계 **6** 패킷 트레이서 결과 분석를 계속합니다.

## NAT 규칙 문제 해결

단계 **1** **Devices & Services(**디바이스 및 서비스**)** 페이지에서 ASA를 선택하고 Actions 창에서 **View NAT Rules(NAT** 규칙 보기**)** View NAT Rules를 클릭합니다.

단계 **2** 문제를 해결할 NAT 규칙 테이블에서 규칙을 선택하고 세부 정보 창에서 문제 해결 Troubleshoot 를 클릭합니다. 문제 해결 페이지의 값 패널에서 많은 필드가 선택한 규칙의 속성으로 미리 채워져 있습니다.

단계 **3** 나머지 필수 필드에 정보를 입력합니다. 모든 필수 필드를 완료하면 Run Packet Tracer(패킷 트레이서 실행)가 활성화됩니다.

단계 **4** **Run Packet Tracer(**패킷 추적기 실행**)**를 클릭합니다.

단계 **5** 패킷 트레이서 결과 분석를 계속합니다.

## 2회 NAT 규칙 문제 해결

단계 **1** **Devices & Services(**디바이스 및 서비스**)** 페이지에서 ASA를 선택하고 Actions 창에서 **View NAT Rules(NAT** 규칙 보기**)** View NAT Rules를 클릭합니다.

단계 **2** 문제를 해결할 NAT 규칙 테이블에서 규칙을 선택하고 세부 정보 창에서 문제 해결 Troubleshoot 를 클릭합니다. 양방향 Twice NAT 규칙의 경우 원본 패킷 변환 또는 대상 패킷 변환의 문제 해결을 선택하는 드롭다운이 열립니다.

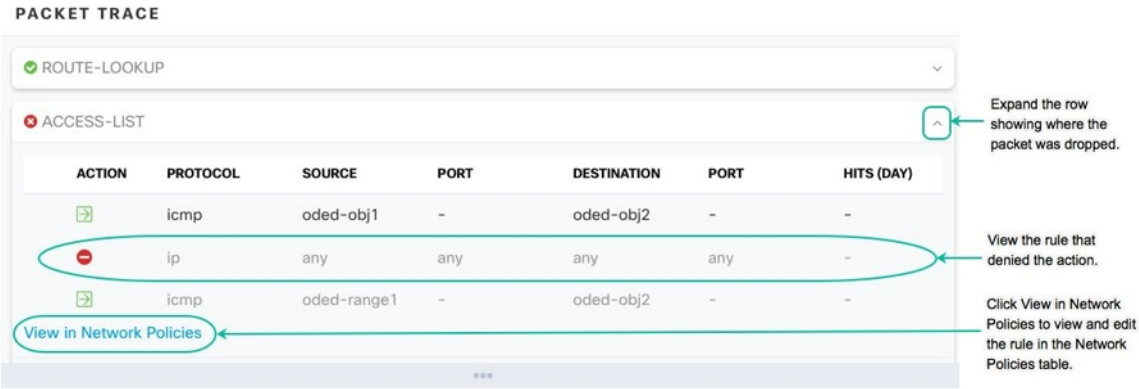
단계 **3** 나머지 필수 필드에 정보를 입력합니다. 모든 필수 필드를 완료하면 Run Packet Tracer(패킷 트레이서 실행)가 활성화됩니다.

단계 **4** **Run Packet Tracer(**패킷 추적기 실행**)**를 클릭합니다.

## 패킷 트레이서 결과 분석

패킷이 삭제되었는지 또는 허용되었는지 여부는 패킷 추적 테이블의 행을 확장하고 해당 작업과 관련된 규칙 또는 로깅 정보를 읽어 그 이유를 알 수 있습니다. 아래 예에서 패킷 트레이서는 모든 소스에서 수신되고 모든 대상으로 이동하는 IP 패킷을 거부하는 규칙이 포함된 액세스 목록 정책을 식별했습니다. 원하는 작업이 아닌 경우 **View in Network Policies(**네트워크 정책에서 보기**)** 링크를 클릭하고 해당 규칙을 즉시 편집할 수 있습니다. 규칙을 편집한 후에는 구성 변경 사항을 ASA에 배포한 다음 패킷 트레이서를 다시 실행하여 예상한 액세스 결과를 얻습니다.

패킷 트레이서 결과와 함께 CDO는 ASA의 ASA 실시간 로깅를 표시합니다.




# Cisco ASA Advisory cisco-sa-20180129-asa1

Cisco PSIRT(Product Security Incident Response Team)은 심각한 심각도의 ASA 및 Firepower 보안 취약점을 설명하는 cisco-sa-20180129-asa1 보안권고를 게시했습니다. 영향을 받는 ASA 및 Firepower 하드웨어, 소프트웨어 및 구성에 대한 자세한 설명은 전체 PSIRT 팀 권고를 읽어보십시오.

ASA가 권고의 영향을 받는다고 판단되면, CDO를 사용하여 ASA를 패치 버전으로 업그레이드할 수 있습니다. 다음 프로세스를 사용합니다.

---

단계 **1** 영향을 받는 각 ASA에서 ASA에서 DNS 구성

단계 **2** 필요한 소프트웨어 패치를 결정하려면 권고로 돌아갑니다.

단계 **3** CDO를 사용하여 ASA를 ASA 권고에 나열된 편집된 릴리스로 업그레이드하는 방법을 설명하는 항목에 대해서는 단일 ASA에서 ASA 및 ASDM 이미지 업그레이드, on page 161을 참조하십시오. ASA 및 ASDM 업그레이드 사전 요건부터 시작한 다음 개별 ASA 업그레이드, 활성-대기 구성에서 ASA 업그레이드 또는 대량 ASA 업그레이드에 대해 읽어보십시오.

편의를 위해 Cisco가 보고한 보안 권고의 요약은 다음과 같습니다.

**2018/5/2** 업데이트: 추가 조사 후 Cisco는 이 취약점의 영향을 받는 추가 공격 벡터와 기능을 확인했습니다. 또한 원래의 편집이 불완전함을 발견하여 새로운 편집 코드 버전을 사용할 수 있습니다. 자세한 내용은 Fixed Software(수정 소프트웨어) 섹션을 참조하십시오. Cisco ASA(Adaptive Security Appliance) 소프트웨어의 XML 파서에 있는 취약점으로 인해 인증되지 않은 원격 공격자가 영향을 받는 시스템을 다시 로드하거나 코드를 원격으로 실행할 수 있습니다. 메모리 부족 상태로 인해 ASA에서 수신되는 VPN(가상 프라이빗망) 인증 요청 처리를 중지할 수도 있었습니다. 이 취약점은 악성 XML 페이로드를 처리할 때 메모리 할당 및 해제 문제로 인해 발생합니다. 공격자는 조작된 XML 패킷을 영향을 받는 시스템의 취약한 인터페이스로 전송하여 이 취약점을 악용할 수 있습니다. 익스플로잇을 통해 공격자는 임의 코드를 실행하고 시스템을 완전히 제어할 수 있으며, 영향을 받는 디바이스를 다시 로드하거나 들어오는 VPN 인증 요청 처리를 중지할 수 있습니다. 취약하려면 ASA에 SSL(Secure Socket Layer) 서비스 또는 IKEv2 원격 액세스 VPN 서비스가 인터페이스에서 활성화되어 있어야 합니다. 취약점이 악용될 위험은 공격자에 대한 인터페이스의 액세스 가능성에 따라 달라집니다. 취약한 ASA 기능의 전체 목록은 취약한 제품 섹션의 표를 참조하십시오. Cisco는 이 취약점을 해결하는 소프트웨어 업데이트를 출시했습니다. 이 취약점의 영향을 받는 모든 기능을 해결하는 해결 방법은 없습니다. 이 권고는 다음 링크에서 확인할 수 있습니다: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1

---

# ASA 실행 구성 크기 확인

실행 중인 구성 파일의 크기를 확인하려면 다음 절차를 수행합니다.

단계 **1** 다음 방법 중 하나로 ASA의 명령줄 인터페이스에 액세스합니다.

- 터미널 창을 열고 SSH를 사용하여 ASA에 로그인합니다. `hostname#`이 포함된 프롬프트가 표시되도록 권한을 "특권 EXEC" 모드로 승격합니다.
- ASA를 온보딩한 경우 **Inventory(**재고 목록**)** 페이지를 열고 연결할 디바이스를 선택한 다음 Device Actions(디바이스 작업) 창에서 **>_ Command Line Interface(**명령줄 인터페이스**)** 버튼을 클릭합니다.

단계 **2** 프롬프트에서 `copy running-config flash`를 입력합니다.

단계 **3** 소스 파일 이름을 묻는 프롬프트가 표시되면 아무 것도 입력하지 않고 <Enter> 키를 누릅니다.

단계 **4** 대상 파일 이름을 입력하라는 메시지가 표시되면 출력 파일의 이름을 입력합니다. ASA는 사용자가 지정한 파일의 실행 중인 구성을 복사한 후 권한 있는 EXEC 프롬프트로 돌아갑니다.

단계 **5** 프롬프트에서 `show flash`를 입력합니다.

단계 **6** 길이 열을 확인합니다. 파일이 4718592바이트를 넘으면 4.5MB보다 큽니다.

다음은 샘플 명령 및 출력 집합입니다.

```
asa1# copy running-config flash
Source filename [running-config]?
Destination filename [running-config]? running-config-output
Cryptochecksum: 725f4c1c 4adfb8a9 8b3e7a6d 49e3420d
23648 bytes copied in 1.380 secs (23648 bytes/sec)
asa1# show flash
--#-- --length-- -----date/time------ path
 107 110325428 Feb 28 2019 15:41:42 asdm-8826067.bin
 122 5018592 Apr 30 2019 21:00:59 running-config-output
 111 102647808 Mar 12 2019 14:26:10 asa9-12-1-smp-k8.bin
```

# 보안 디바이스 커넥터에 영향을 미치는 컨테이너 권한 상승 취약점: cisco-sa-20190215-runc

Cisco PSIRT(제품 보안 사고 대응 팀)는 Docker의 심각도가 높은 취약성에 대해 설명하는 보안 자문 cisco-sa-20190215-runc를 게시했습니다. 취약성에 대한 전체 설명은 전체 PSIRT 팀 자문을 참조하십시오.

이 취약성은 모든 CDO 고객에게 영향을 미칩니다.

- CDO의 클라우드 배포 SDC(보안 디바이스 커넥터)를 사용하는 고객은 CDO 운영 팀에서 교정 단계를 이미 수행했으므로 아무 작업도 수행할 필요가 없습니다.
- 온프레미스에 배포된 SDC를 사용하는 고객은 최신 Docker 버전을 사용하도록 SDC 호스트를 업그레이드해야 합니다. 다음 지침에 따라 이 작업을 수행할 수 있습니다.

# CDO-표준 SDC 호스트 업데이트

CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축한 경우 이 지침을 사용합니다.

단계 1 SSH 또는 하이퍼바이저 콘솔을 사용하여 SDC 호스트에 연결합니다.

단계 2 다음 명령을 실행하여 Docker 서비스 버전을 확인합니다.

```
docker version
```

단계 3 최신 VM(가상 머신) 중 하나를 실행 중인 경우 다음과 같은 출력이 표시됩니다.

```
 > docker version
Client:
     Version: 18.06.1-ce
     API version: 1.38
     Go version: go1.10.3
     Git commit: e68fc7a
     Built: Tue Aug 21 17:23:03 2018
     OS/Arch: linux/amd64
     Experimental: false
```

여기에서 이전 버전을 볼 수 있습니다.

단계 4 다음 명령을 실행하여 Docker를 업데이트하고 서비스를 다시 시작하십시오.

```
> sudo yum update docker-ce
> sudo service docker restart
```

참고 Docker 서비스가 다시 시작되는 동안 CDO와 디바이스 간에 짧은 연결 중단이 발생합니다.

단계 5 docker version 명령을 다시 실행하십시오. 다음 출력이 표시되어야 합니다.

```
> docker version
Client:
    Version: 18.09.2
    API version: 1.39
    Go version: go1.10.6
    Git commit: 6247962
    Built: Sun Feb XX 04:13:27 2019
    OS/Arch: linux/amd64
    Experimental: false
```

단계 6 마쳤습니다. 이제 패치가 적용된 최신 버전의 Docker로 업그레이드되었습니다.

# 사용자 지정 SDC 호스트 업데이트

자체 SDC 호스트를 생성한 경우 Docker 설치 방법에 따라 업데이트 지침을 따라야 합니다. CentOS, yum 및 Docker-ce(커뮤니티 에디션)를 사용한 경우 이전 절차가 작동합니다.

Docker-ee(엔터프라이즈 버전)를 설치했거나 다른 방법을 사용하여 Docker를 설치한 경우 Docker의 고정 버전이 다를 수 있습니다. Docker 페이지를 확인하여 설치할 올바른 버전(Docker 보안 업데이트 및 컨테이너 보안 모범 사례)을 결정할 수 있습니다.

## 버그 추적

Cisco는 이 취약성을 계속 평가하고 있으며 추가 정보가 제공되는 대로 권고를 업데이트할 것입니다. 권고가 최종으로 표시되면 관련 Cisco 버그에서 자세한 내용을 참조할 수 있습니다.

CSCvo33929-CVE-2019-5736: runc container breakout

# 대규모 **ASA** 실행 구성 파일

### **CDO**의 동작

ASA가 온보딩에 실패하거나, CDO가 ASA의 실행 중인 구성 파일에 정의된 모든 구성을 표시하지 않거나, CDO가 변경 로그에 쓰지 못하는 등의 동작을 볼 수 있습니다.

### 가능한 원인

ASA의 실행 중인 구성 파일이 CDO에 대해 "너무 클" 수 있습니다.

ASA를 CDO에 온보딩하면 CDO는 ASA에서 실행 중인 구성 파일의 복사본을 데이터베이스에 저장합니다. 일반적으로 실행 중인 구성 파일이 너무 크거나(4.5MB 이상), 너무 많은 행(약 22,000행)을 포함하거나, 단일 액세스 그룹에 대한 액세스 목록 항목이 너무 많은 경우, CDO는 해당 디바이스를 예측 가능하게 관리할 수 없습니다.

실행 중인 구성 파일의 크기를 확인하려면 ASA 실행 구성 크기 확인을 참조하십시오.

### 해결방법

보안 정책을 방해하지 않고 구성 파일의 크기를 안전하게 줄이는 데 도움이 필요하면 Cisco 어카운트 팀에 문의하십시오.

# 보안 디바이스 커넥터 문제 해결

다음 주제를 사용하여 온프레미스 SDC(Secure Device Connector) 문제를 해결합니다.

이러한 시나리오와 일치하지 않는 경우 CDO 고객이 TAC로 지원 티켓을 여는 방법.

## **SDC**에 연결할 수 없음

CDO에서 연속으로 두 개의 하트비트 요청에 응답하지 못한 경우 SDC는 "도달할 수 없음" 상태입니다. SDC에 연결할 수 없는 경우 테넌트는 온보딩한 디바이스와 통신할 수 없습니다.

CDO는 다음과 같은 방식으로 SDC에 연결할 수 없음을 나타냅니다.

- "일부 보안 디바이스 커넥터(SDC)에 연결할 수 없습니다."라는 메시지가 표시됩니다. CDO 홈페이지에서 이러한 SDC와 연결된 디바이스와 통신할 수 없습니다.
- Secure Connectors(보안 커넥터) 페이지에서 SDC의 상태는 "연결할 수 없음"입니다.

먼저 이 문제를 해결하려면 SDC를 테넌트에 다시 연결해 봅니다.

1. SDC 가상 머신이 실행 중이고 해당 지역의 CDO IP 주소에 도달할 수 있는지 확인합니다. 매니지드 디바이스에 Cisco Defense Orchestrator 연결, 6 페이지을 참조하십시오.
2. 하트비트를 수동으로 요청하여 CDO와 SDC를 다시 연결해 봅니다. SDC가 하트비트 요청에 응답하면 "활성" 상태로 돌아갑니다. 하트비트를 수동으로 요청하려면 다음과 같이 작업합니다.
   1. CDO 메뉴에서 **Admin(관리)** > **Secure Connector(보안 커넥터)**를 선택합니다.
   2. 연결할 수 없는 SDC를 클릭합니다.
   3. 작업 창에서 **Request Heartbeat(하트비트 요청)**를 클릭합니다.
   4. **Reconnect(다시 연결)**를 클릭합니다.
3. 테넌트에 수동으로 다시 연결하려고 시도한 후에도 SDC가 활성 상태로 돌아가지 않으면, 배포 후 SDC 상태가 CDO에서 활성화되지 않음, 554 페이지의 지침을 따르십시오.

.

# 배포 후 SDC 상태가 CDO에서 활성화되지 않음

CDO가 배포 후 약 10분 동안 SDC가 활성 상태임을 나타내지 않으면 SDC를 배포할 때 생성한 `cdo` 사용자 및 암호를 사용하여 SSH를 사용하여 SDC VM에 연결합니다.

---

단계 **1** `/opt/cdo/configure.log`를 검토합니다. SDC에 대해 입력한 구성 설정과 성공적으로 적용되었는지 여부를 보여줍니다. 설정 프로세스에 오류가 있거나 값이 올바르게 입력되지 않은 경우 sdc-onboard 설정을 다시 실행합니다.

a) `[cdo@localhost cdo]$` 프롬프트에서 `sudo sdc-onboard setup`을 입력합니다.

b) `cdo`user의 암호를 입력합니다.

c) 프롬프트에 따라 수행합니다. 설정 스크립트는 설정 마법사에서 수행한 모든 구성 단계를 안내하고 입력한 값을 변경할 수 있는 기회를 제공합니다.

단계 **2** 로그를 검토하고 `sudo sdc-onboard setup`을 실행한 후에도 CDO가 여전히 SDC가 **Active(활성)** 상태임을 나타내지 않으면, Cisco Defense Orchestrator 지원팀에 문의.

---

# SDC의 변경된 IP 주소가 CDO에 반영되지 않음

SDC의 IP 주소를 변경한 경우 GMT 오전 3시 이후까지는 CDO에 반영되지 않습니다.

# SDC와의 디바이스 연결 문제 해결

이 도구를 사용하여 CDO에서 SDC(보안 디바이스 커넥터)를 통해 디바이스로의 연결을 테스트합니다. 디바이스가 온보딩에 실패하거나 온보딩 전에 CDO가 디바이스에 연결할 수 있는지 확인하려는 경우 이 연결을 테스트할 수 있습니다.

단계 **1** CDO 메뉴에서 **Admin(관리)** > **Secure Connector(보안 커넥터)**를 선택합니다.

단계 **2** SDC를 선택합니다.

단계 **3** 오른쪽의 **Troubleshooting(문제 해결)** 창에서 **Device Connectivity(디바이스 연결)**를 클릭합니다.

단계 **4** 문제 해결을 시도하거나 연결을 시도하는 디바이스의 유효한 IP 주소 또는 FQDN 및 포트 번호를 입력하고 **Go(이동)**를 클릭합니다. CDO는 다음 확인을 수행합니다.

a) **DNS** 확인 - IP 주소 대신 FQDN을 제공하는 경우 SDC가 도메인 이름을 확인하고 IP 주소를 가져올 수 있는지 확인합니다.

b) 연결 테스트 - 디바이스에 연결할 수 있는지 확인합니다.

c) **TLS** 지원 - 디바이스와 SDC가 모두 지원하는 TLS 버전 및 암호를 탐지합니다.

- 지원되지 않는 암호 - 디바이스와 SDC에서 모두 지원하는 TLS 버전이 없는 경우 CDO는 디바이스에서 지원하는 TLS 버전 및 암호도 테스트하지만 SDC는 테스트하지 않습니다.

d) SSL 인증서 - 문제 해결에서 인증서 정보를 제공합니다.

단계 **5** 디바이스에 대한 온보딩 또는 연결 문제가 계속 발생하는 경우 Cisco Defense Orchestrator 지원팀에 문의하십시오.

# 간헐적으로 또는 SDC에 연결되지 않음

이 섹션에서 설명하는 솔루션은 온프레미스 SDC(보안 디바이스 커넥터)에만 적용됩니다.

증상: 간헐적으로 또는 SDC에 연결되지 않음

진단: 이 문제는 디스크 공간이 거의 찼을 때(80% 이상) 발생할 수 있습니다.

디스크 공간 사용량을 확인하려면 다음 단계를 수행합니다.

1. SDC(보안 디바이스 커넥터) VM용 콘솔을 엽니다.
2. 사용자 이름 **cdo**로 로그인합니다.
3. 최초 로그인 시 생성한 비밀번호를 입력합니다.
4. 먼저 **`df -h`**를 입력하여 사용 가능한 디스크 공간이 없는지 확인하여 디스크 여유 공간을 확인합니다.

   Docker에서 디스크 공간을 소비한 것을 확인할 수 있습니다. 정상적인 디스크 사용량은 2GB 미만일 것으로 예상됩니다.
5. **Docker** 폴더의 디스크 사용량을 보려면,

   **`sudo du -h /var/lib/docker | sort -h`**를 실행합니다.

   **Docker** 폴더의 디스크 공간 사용량을 볼 수 있습니다.

절차

Docker 폴더의 디스크 공간 사용량이 거의 가득 찬 경우 docker 구성 파일에서 다음을 정의합니다.

- 최대 크기: 현재 파일이 최대 크기에 도달하면 로그 회전을 강제합니다.
- 최대 파일: 최대 한도에 도달했을 때 초과 회전된 로그 파일을 삭제합니다.

다음을 수행하십시오.

1. **sudo vi /etc/docker/daemon.json**를 실행합니다.
2. 파일에 다음 줄을 삽입합니다.

```
{
"log-driver": "json-file",
"log-opts": {"max-size": "100m", "max-file": "5" }
}
```

3. **ESC** 키를 누른 다음 **:wq!**를 입력합니다. 변경 사항을 쓰고 파일을 닫습니다.

참고 **sudo cat /etc/docker/daemon.json**을 실행하여 파일의 변경 사항을 확인할 수 있습니다.

4. **sudo systemctl restart docker**를 실행하여 doker 파일을 다시 시작합니다.

   변경 사항이 적용되려면 몇 분 정도 걸립니다. **sudo du -h /var/lib/docker | sort -h**를 실행하여 docker 폴더의 업데이트된 디스크 사용량을 봅니다.

5. **df -h**를 실행하여 사용 가능한 디스크 크기가 증가했는지 확인합니다.
6. SDC 상태를 Unreachable(연결 불가)에서 Active(활성)로 변경하려면 먼저 CDO에서 Secure Connector(보안 커넥터) 페이지로 이동하여 Actions(작업) 메뉴에서 **Request Reconnect(**재연결 요청**)**를 클릭해야 합니다.

# 보안 디바이스 커넥터에 영향을 미치는 컨테이너 권한 상승 취약점: cisco-sa-20190215-runc

Cisco PSIRT(제품 보안 사고 대응 팀)는 Docker의 심각도가 높은 취약성에 대해 설명하는 보안 자문 **cisco-sa-20190215-runc**를 게시했습니다. 취약성에 대한 전체 설명은 전체 PSIRT 팀 자문을 참조하십시오.

이 취약성은 모든 CDO 고객에게 영향을 미칩니다.

- CDO의 클라우드 배포 SDC(보안 디바이스 커넥터)를 사용하는 고객은 CDO 운영 팀에서 교정 단계를 이미 수행했으므로 아무 작업도 수행할 필요가 없습니다.
- 온프레미스에 배포된 SDC를 사용하는 고객은 최신 Docker 버전을 사용하도록 SDC 호스트를 업그레이드해야 합니다. 다음 지침에 따라 이 작업을 수행할 수 있습니다.
  - CDO-표준 SDC 호스트 업데이트, 552 페이지
  - 사용자 지정 SDC 호스트 업데이트, 552 페이지

• 버그 추적, 553 페이지

## CDO-표준 SDC 호스트 업데이트

CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축한 경우 이 지침을 사용합니다.

단계 **1** SSH 또는 하이퍼바이저 콘솔을 사용하여 SDC 호스트에 연결합니다.

단계 **2** 다음 명령을 실행하여 Docker 서비스 버전을 확인합니다.

```
docker version
```

단계 **3** 최신 VM(가상 머신) 중 하나를 실행 중인 경우 다음과 같은 출력이 표시됩니다.

```
 > docker version
Client:
     Version: 18.06.1-ce
     API version: 1.38
     Go version: go1.10.3
     Git commit: e68fc7a
     Built: Tue Aug 21 17:23:03 2018
     OS/Arch: linux/amd64
     Experimental: false
```

여기에서 이전 버전을 볼 수 있습니다.

단계 **4** 다음 명령을 실행하여 Docker를 업데이트하고 서비스를 다시 시작하십시오.

```
> sudo yum update docker-ce
> sudo service docker restart
```

참고 Docker 서비스가 다시 시작되는 동안 CDO와 디바이스 간에 짧은 연결 중단이 발생합니다.

단계 **5** docker version 명령을 다시 실행하십시오. 다음 출력이 표시되어야 합니다.

```
> docker version
Client:
    Version: 18.09.2
    API version: 1.39
    Go version: go1.10.6
    Git commit: 6247962
    Built: Sun Feb XX 04:13:27 2019
    OS/Arch: linux/amd64
    Experimental: false
```

단계 **6** 마쳤습니다. 이제 패치가 적용된 최신 버전의 Docker로 업그레이드되었습니다.

## 사용자 지정 SDC 호스트 업데이트

자체 SDC 호스트를 생성한 경우 Docker 설치 방법에 따라 업데이트 지침을 따라야 합니다. CentOS, yum 및 Docker-ce(커뮤니티 에디션)를 사용한 경우 이전 절차가 작동합니다.

Docker-ee(엔터프라이즈 버전)를 설치했거나 다른 방법을 사용하여 Docker를 설치한 경우 Docker의 고정 버전이 다를 수 있습니다. Docker 페이지를 확인하여 설치할 올바른 버전(Docker 보안 업데이트 및 컨테이너 보안 모범 사례)을 결정할 수 있습니다.

## 버그 추적

Cisco는 이 취약성을 계속 평가하고 있으며 추가 정보가 제공되는 대로 권고를 업데이트할 것입니다. 권고가 최종으로 표시되면 관련 Cisco 버그에서 자세한 내용을 참조할 수 있습니다.

CSCvo33929-CVE-2019-5736: runc container breakout

# 보안 이벤트 커넥터 문제 해결

이러한 시나리오와 일치하지 않는 경우 CDO 고객이 TAC로 지원 티켓을 여는 방법.

# SEC 온보딩 실패 문제 해결

이러한 문제 해결 항목에서는 SEC(보안 이벤트 커넥터) 온보딩 실패와 관련된 여러 가지 증상에 대해 설명합니다.

### SEC 온보딩 실패

증상: SEC 온보딩에 실패했습니다.

복구: SEC를 제거하고 다시 온보딩합니다.

이 오류가 표시되는 경우:

1. 가상 머신 컨테이너에서 보안 이벤트 커넥터 제거 및 해당 파일을 제거합니다.
2. 보안 디바이스 커넥터 업데이트, 23 페이지. 일반적으로 SDC는 자동으로 업데이트되므로 이 절차를 사용할 필요가 없지만 이 절차는 문제 해결 시 유용합니다.
3. SDC 가상 머신에 SEC(Secure Event Connector) 설치, 438 페이지.

팁 SEC를 온보딩할 때는 항상 복사 링크를 사용하여 부트스트랩 데이터를 복사합니다.

참고 이 절차로 문제가 해결되지 않으면 문제 해결 로그 파일 이벤트 로깅하고 관리 서비스 제공자 또는 Cisco 기술 지원 센터에 문의하십시오.

### SEC 부트스트랩 데이터가 제공되지 않음

메시지: 오류가 발생하여 보안 이벤트 커넥터를 부트스트랩할 수 없습니다. 부트스트랩 데이터가 제공되지 않아 종료하는 중입니다.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
Please input the bootstrap data from Setup Secure Event Connector page of CDO:
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector, bootstrap data not
provided, exiting.
```

진단: 프롬프트가 표시될 때 부스트랩 데이터가 설정 스크립트에 입력되지 않았습니다.

복구: 온보딩 시 부트스트랩 데이터 입력에 대한 프롬프트가 표시되면 CDO UI에서 생성된 SEC 부트스트랩 데이터를 제공합니다.

부트스트랩 구성 파일이 없습니다.

메시지: 오류가 발생하여 테넌트 <tenant_name>에 대한 보안 이벤트 커넥터를 부트스트랩할 수 없습니다. 부트스트랩 구성 파일("/usr/local/cdo/es_bootstrapdata")이 없어 종료하는 중입니다.

진단: SEC 부트스트랩 데이터 파일("/usr/local/cdo/es_bootstrapdata")이 없습니다.

복구: CDO UI에서 생성된 SEC 부트스트랩 데이터를 **/usr/local/cdo/es_bootstrapdata** 파일에 배치하고 다시 온보딩을 시도합니다.

1. 온보딩 절차를 반복합니다.
2. 부트스트랩 날짜를 복사합니다.
3. 'sdc' 사용자로 SEC VM에 로그인합니다.
4. CDO UI에서 생성된 SEC 부트스트랩 데이터를 **/usr/local/cdo/es_bootstrapdata** 파일에 배치하고 다시 온보딩을 시도합니다.

부트스트랩 데이터 디코딩 실패

메시지: 오류가 발생하여 테넌트 <tenant_name>에 대한 보안 이벤트 커넥터를 부트스트랩할 수 없습니다. SEC 부스트랩 데이터를 디코딩하지 못하여 종료하는 중입니다.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
base64: invalid input
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: tenant_XYZ,
 failed to decode SEC bootstrap data, exiting.
```

진단: 부트스트랩 데이터 디코딩 실패

복구: SEC 부트스트랩 데이터를 재생성하고 온보딩을 다시 시도합니다.

부트스트랩 데이터에 **SEC**를 온보딩하는 데 필요한 정보가 없습니다.

메시지:

- ERROR는 테넌트에 대한 보안 이벤트 커넥터 컨테이너를 부트스트랩할 수 없습니다. 보안 서비스 익스체인지 FQDN이 설정되지 않았습니다. 종료됩니다.
- ERROR는 테넌트에 대한 보안 이벤트 커넥터 컨테이너를 부트스트랩할 수 없습니다. 보안 서비스 익스체인지 OTP가 설정되지 않았습니다. 종료됩니다.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: 보안 서비스
익스체인지 FQDN not set, exiting.

[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: 보안 서비스
익스체인지 FQDN not set, exiting.
```

진단: 부트스트랩 데이터에 SEC를 온보딩하는 데 필요한 정보가 없습니다.

복구: 부트스트랩 데이터를 재생성하고 다시 온보딩을 시도합니다.

### 툴킷 **cron** 현재 실행 중

메시지: 오류 SEC 툴킷이 이미 실행 중이어서 종료하는 중입니니다.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
 [2020-06-10 04:37:26] ERROR SEC toolkit already running.
```

진단: 툴킷 cron이 현재 실행 중입니다.

복구: 온보딩 명령을 다시 시도합니다.

### 적절한 **CPU** 및 메모리를 사용할 수 없음

메시지: 오류가 발생하여 보안 이벤트 커넥터를 설정할 수 없습니다. 최소 4개의 CPU와 8GB의 RAM이 필요하여 종료하는 중입니다.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR unable to setup Secure Event Connector, minimum 4 cpus and 8
GB ram required, exiting.
```

진단: 적절한 CPU 및 메모리를 사용할 수 없습니다.

복구: 최소 4개의 CPU 및 8GB RAM이 VM에서 SEC 전용으로 프로비저닝되었는지 확인하고 다시 온보딩을 시도합니다.

### **SEC**가 이미 실행 중

메시지: 오류. 보안 이벤트 커넥터가 이미 실행 중입니다. 새 보안 이벤트 커넥터를 온보딩하기 전에 'cleanup'을 실행하십시오. 종료하는 중입니다.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR Secure Event Connector already running, execute 'cleanup' before
 onboarding a new Secure Event Connector, exiting.
```

진단: SEC가 이미 실행 중입니다.

복구: 새 SEC를 온보딩하기 전에 SEC Cleanup 명령을 실행합니다.

### **SEC** 도메인 연결 불가

메시지:

- api-sse.cisco.com:443에 연결 실패; 연결 거부됨
- 오류가 발생하여 보안 이벤트 커넥터를 설정할 수 없습니다. 도메인 api-sse.cisco.com에 연결할 수 없어 종료하는 중입니다.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
curl: (7) Failed connect to api-sse.cisco.com:443; Connection refused
[2020-06-10 04:37:26] ERROR unable to setup Secure Event Connector, domain api-sse.cisco.com
 unreachable, exiting.
```

진단: SEC 도메인에 연결할 수 없음

복구: 온프레미스 SDC가 인터넷에 연결되어 있는지 확인하고 다시 온보딩을 시도합니다.

온보딩 **SEC** 명령이 오류 없이 성공했지만 **SEC** 도커 컨테이너가 작동하지 않음

증상: 온보딩 SEC 명령이 오류 없이 성공했지만 SEC 도커 컨테이너가 작동하지 않습니다.

진단: 온보딩 SEC 명령이 오류 없이 성공했지만 SEC 도커 컨테이너가 작동하지 않습니다.

복구**:**

1. 'sdc' 사용자로 SEC에 로그인합니다.
2. SEC 도커 컨테이너 시작 로그(/usr/local/cdo/data/<tenantDir> /event_streamer/logs/startup.log)에 오류가 있는지 확인합니다.
3. 있는 경우 SEC Cleanup 명령을 실행하고 온보딩을 다시 시도합니다.

**CDO** 지원 문의

이러한 시나리오와 일치하지 않는 경우 CDO 고객이 TAC로 지원 티켓을 여는 방법.

# 보안 이벤트 커넥터 등록 실패 문제 해결

증상: 클라우드 이벤트 서비스에 대한 Cisco Secure Event Connector 등록이 실패합니다.

진단: SEC가 이벤트 클라우드 서비스에 등록하지 못하는 가장 일반적인 이유입니다.

- **SEC**가 **SEC**에서 **Eventing** 클라우드 서비스에 연결할 수 없습니다**.**

  복구: 포트 443에서 인터넷에 액세스할 수 있고 DNS가 올바르게 구성되어 있는지 확인합니다.

- **SEC** 부트스트랩 데이터의 유효하지 않거나 만료된 일회용 비밀번호로 인한 등록 실패

  복구:

---

단계 **1** 'sdc' 사용자로 SDC에 로그온합니다.

단계 **2** 커넥터 로그 보기: ( /usr/local/cdo/data/<tenantDir> /event_streamer/logs/connector.log)에서 등록 상태를 확인합니다.

유효하지 않은 토큰으로 인해 등록에 실패한 경우 로그 파일에 아래와 유사한 오류 메시지가 표시됩니다.

컨텍스트**:(*contextImpl).handleFailed]** 등록 **- CE2001:** 등록 실패 - 잘못된 토큰으로 인해 디바이스를 등록하지 못했습니다**.** 유효한 새 토큰을 사용하여 다시 시도하십시오**. -** 실패"

단계 **3** SDC VM에서 SEC Cleanup 명령 단계를 실행하여 보안 커넥터 페이지에서 SEC를 제거합니다.

단계 **4** 새 SEC 부트스트랩 데이터를 생성하고 SEC 온보딩 단계를 다시 시도합니다.

---

# 보안 및 분석 로깅 이벤트를 사용하여 네트워크 문제 해결

다음은 이벤트 뷰어를 사용하여 네트워크 문제를 트러블슈팅하는 데 사용할 수 있는 기본 프레임워크입니다.

이 시나리오에서는 네트워크 운영 팀에서 사용자가 네트워크의 리소스에 액세스할 수 없다는 보고를 받은 것으로 가정합니다. 문제를 보고하는 사용자와 해당 위치를 기반으로, 네트워크 운영 팀은 어떤 방화벽이 리소스에 대한 액세스를 제어하는지를 합리적으로 파악합니다.

**Note** 또한 이 시나리오에서는 FDM 관리 디바이스가 네트워크 트래픽을 관리하는 방화벽이라고 가정합니다. Security Analytics and Logging(보안 분석 및 로깅)은 다른 디바이스 유형에서 로깅 정보를 수집하지 않습니다.

단계 **1** 탐색창에서 분석 > 이벤트 로깅를 선택합니다.

단계 **2** 기록 탭을 클릭합니다.

단계 **3** 시간 범위를 기준으로 이벤트 필터링을 시작합니다. 기본적으로 Historical(기록) 탭에는 이벤트의 마지막 시간이 표시됩니다. 올바른 시간 범위인 경우 현재 날짜와 시간을 **End(**종료**)** 시간으로 입력합니다. 올바른 시간 범위가 아닌 경우 보고된 문제의 시간을 포함하는 시작 및 종료 시간을 입력합니다.

단계 **4** **Sensor ID(**센서 **ID)** 필드에 사용자의 액세스를 제어하는 것으로 의심되는 방화벽의 IP 주소를 입력합니다. 방화벽이 두 개 이상인 경우 검색 창에서 속성**:**값 쌍을 사용하여 이벤트를 필터링합니다. 두 항목을 만들고 OR 문으로 결합합니다. 예: `SensorID:192.168.10.2 OR SensorID:192.168.20.2`.

단계 **5** Events(이벤트) 필터 표시줄의 **Source IP(**소스 **IP)** 필드에 사용자의 IP 주소를 입력합니다.

단계 **6** 사용자가 리소스에 액세스할 수 없는 경우 **Destination IP(**대상 **IP)** 필드에 해당 리소스의 IP 주소를 입력해 보십시오.

단계 **7** 결과에서 이벤트를 확장하고 세부 정보를 확인합니다. 다음은 몇 가지 세부 사항입니다.

- **AC_RuleAction** - 규칙이 트리거될 때 수행된 작업(허용, 신뢰, 차단).
- **FirewallPolicy** - 이벤트를 트리거한 규칙이 상주하는 정책입니다.
- **FirewallRule** - 이벤트를 트리거한 규칙의 이름입니다. 값이 Default Action(기본 작업)인 경우 정책의 규칙 중 하나가 아니라 이벤트를 트리거한 것은 정책의 기본 작업입니다.
- **UserName** - 이니시에이터 IP 주소와 연결된 사용자입니다. 이니시에이터 IP 주소는 소스 IP 주소와 동일합니다.

단계 **8** 규칙 작업이 액세스를 차단하는 경우 FirewallRule 및 FirewallPolicy 필드를 확인하여 액세스를 차단하는 정책의 규칙을 식별합니다.

# NSEL 데이터 플로우 문제 해결

CDO 매크로를 사용하여 ASA 디바이스용 NSEL 구성 및 을 했으면 다음 절차를 사용하여 NSEL 이벤트가 사용자 ASA에서 Cisco Cloud로 전송되고 Cisco Cloud가 이를 수신하는지 확인합니다.

ASA가 NSEL 이벤트를 SEC(보안 이벤트 커넥터)로 보낸 다음 Cisco Cloud로 보내도록 구성된 후에는 데이터가 즉시 흐르지 않습니다. NET에서 생성되는 NSEL 관련 트래픽이 있다고 가정하면 첫 번째 NSEL 패킷이 ASA에 도착하는 데 몇 분 정도 걸릴 수 있습니다.

**Note** 이 워크플로우는 "flow-export counters" 명령 및 "capture" 명령을 사용하여 NSEL 데이터 플로우 문제를 해결하는 방법을 보여줍니다. 이러한 명령 사용에 대한 자세한 내용은CLI Book 1: Cisco ASA 시리즈 일반 운영 CLI 구성 가이드의 "패킷 캡처" 및 Cisco ASA NetFlow 구현 가이드의 "NSEL 모니터링"을 참조하십시오.

다음 세 가지 작업을 수행합니다.

- NetFlow 패킷이 SEC로 전송되고 있는지 확인
- Cisco Cloud에서 NetFlow 패킷을 수신하고 있는지 확인

# 문제 해결 로그 파일 이벤트 로깅

SEC(Secure Event Connector) Troubleshooting.sh는 모든 이벤트 스트리머 로그를 수집하여 single.tar.gz 파일로 압축합니다.

다음 절차를 사용하여 Comparesed.tar.gz 파일을 생성하고 파일의 압축을 풉니다.

1. 문제 해결 스크립트 실행, 563 페이지.
2. sec_troubleshoot.tar.gz 파일 압축 해제, 564 페이지.

## 문제 해결 스크립트 실행

SEC(보안 이벤트 커넥터) Troubleshooting.sh는 모든 이벤트 스트리머 로그를 수집하여 single.tar.gz 파일로 압축합니다. Troubleshooting.sh 스크립트를 실행하려면 다음 절차를 따르십시오.

단계 **1** VM 하이퍼바이저를 열고 SDC(Secure Device Connector)에 대한 콘솔 세션을 시작합니다.

단계 **2** 로그인한 다음 **root** 사용자로 전환합니다.

```
[cdo@localhost ~]$sudo su root
```

**Note** sdc 사용자로 전환할 수도 있지만 루트 역할을 하면 IP 테이블 정보도 수신 됩니다. IP 테이블 정보는 방화벽이 디바이스 및 모든 방화벽 경로에서 실행 중임을 보여줍니다. 방화벽이 보안 이벤트 커넥터 TCP 또는 UDP 포트를 차단하는 경우 이벤트는 이벤트 로깅 테이블에 표시되지 않습니다. IP 테이블은 이러한 경우를 확인하는 데 도움이 됩니다.

단계 **3** 프롬프트에서 문제 해결 스크립트를 실행하고 테넌트 이름을 지정합니다. 다음은 명령 구문입니다.

```
[root@localhost ~]$ /usr/local/cdo/toolkit/troubleshoot.sh --app sec --tenant CDO_[tenant_name]
```

예를 들면 다음과 같습니다.

```
[root@localhost ~]$ /usr/local/cdo/toolkit/troubleshoot.sh --app sec --tenant CDO_example_tenant
```

명령 출력에서 sec_troubleshoot 파일이 SDC의 **/tmp/troubleshoot** 디렉터리에 저장되어 있음을 확인할 수 있습니다. 파일 이름은 sec**_troubleshoot-** ***timestamp*****.tar.gz** 규칙을 따르십시오.

단계 **4** 파일을 검색하려면 CDO 사용자로 로그인하고 SCP 또는 SFTP를 사용하여 파일을 다운로드합니다.

예를 들면 다음과 같습니다.

```
[root@localhost troubleshoot]# scp sec_troubleshoot-timestamp.tar.gz
root@server-ip:/scp/sec_troubleshoot-timestamp.tar.gz
```

### What to do next

sec_troubleshoot.tar.gz 파일 압축 해제, on page 564를 진행합니다.

## sec_troubleshoot.tar.gz 파일 압축 해제

SEC(Secure Event Connector) 문제 해결 스크립트 실행 스크립트는 모든 이벤트 스트리머 로그를 수집하여 단일 sec_troubleshoot.tar.gz 파일로 압축합니다. 다음 절차에 따라 sec_troubleshoot.tar.gz 파일의 압축을 풉니다.

1. VM 하이퍼바이저를 열고 SDC(Secure Device Connector)에 대한 콘솔 세션을 시작합니다.
2. 로그인한 다음 **root** 사용자로 전환합니다.

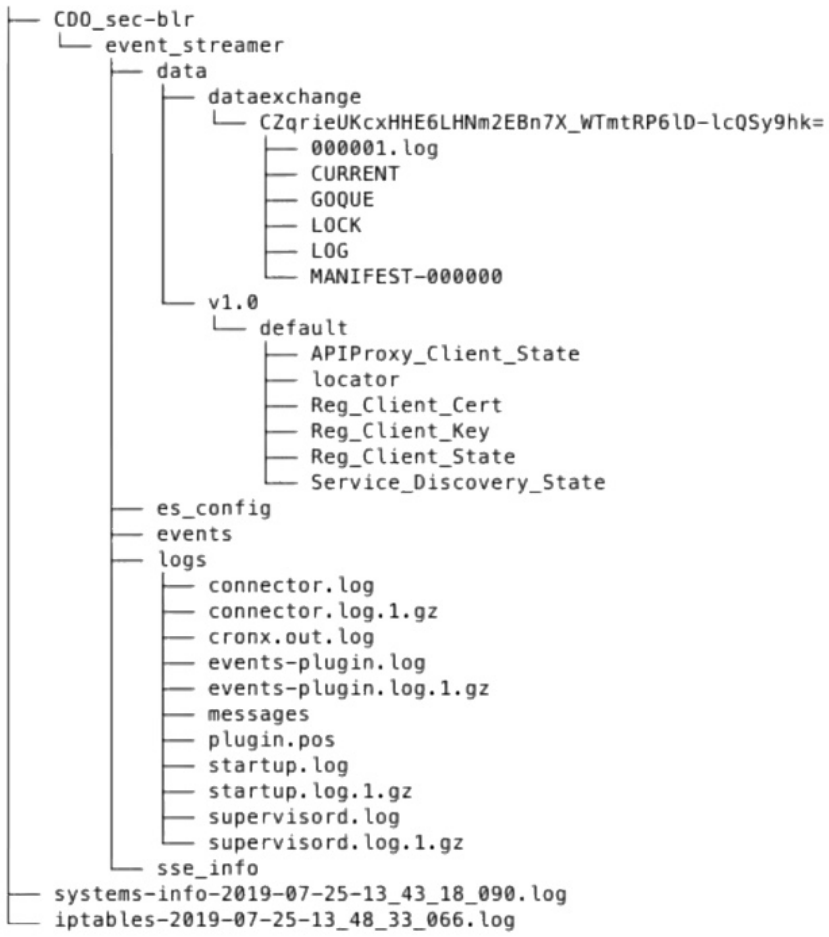
```
[cdo@localhost ~]$sudo su root
```

**Note** **sdc** 사용자로 전환할 수도 있지만 루트 역할을 하면 IP 테이블 정보도 수신 됩니다. IP 테이블 정보는 방화벽이 디바이스 및 모든 방화벽 경로에서 실행 중임을 보여줍니다. 방화벽이 보안 이벤트 커넥터 TCP 또는 UDP 포트를 차단하는 경우 이벤트는 이벤트 로깅 테이블에 표시되지 않습니다. IP 테이블은 이러한 경우를 확인하는 데 도움이 됩니다.

3. 프롬프트에서 다음 명령을 입력합니다.

```
[root@localhost ~]$ tar xvf sec_troubleshoot-timestamp.tar.gz
```

로그 파일은 테넌트의 이름을 따서 명명된 디렉터리에 저장됩니다. 이러한 로그는 sec_troubelshoot-timestamp.tar.gz 파일에 저장됩니다. 루트 사용자로 모든 로그 파일을 수집한 경우 iptables 파일이 포함됩니다.




# SEC 부트스트랩 데이터를 생성하지 못했습니다.

증상: CDO에서 SEC 부트스트랩 데이터를 생성하는 동안, "부트스트랩 생성" 단계가 "부트스트랩 데이터를 가져오는 중에 오류가 발생했습니다." 오류와 함께 실패합니다. 다시 시도하십시오."

수리: 부트스트랩 데이터 생성을 다시 시도하십시오. 여전히 실패하면 CDO 고객이 TAC로 지원 티켓을 여는 방법하십시오.

# 온보딩 후 CDO 보안 커넥터 페이지에서 SEC 상태가 "비활성"임

**Symptom(증상)**: 보안 이벤트 커넥터 상태가 다음 이유 중 하나로 CDO 보안 커넥터 페이지에서 "비활성"으로 표시됩니다.

- 하트비트 실패
- 커넥터 등록 실패

복구:

- **Heartbeat failed(**하트비트 실패**):** SEC 하트비트를 요청하고 보안 커넥터 페이지를 새로 고쳐 상태가 "활성"으로 변경되는지 확인하고 그렇지 않으면 보안 디바이스 커넥터 등록이 실패했는지 확인합니다.
- **Connector registration failed(**커넥터 등록 실패**):** 보안 이벤트 커넥터 등록 실패 문제 해결을 참조하십시오.

# SEC가 "온라인"이지만 CDO 이벤트 로깅 페이지에 이벤트가 없습니다

**Symptom(**증상**)**: CDO 보안 커넥터 페이지에 보안 이벤트 커넥터가 "활성"으로 표시되지만 CDO 이벤트 뷰어에는 이벤트가 표시되지 않습니다.

**Solution or workaround(**해결 방법**)**:

---

단계 **1** 온프레미스 SDC의 VM에 'sdc' 사용자로 로그인합니다. 프롬프트에서 **sudo su - sdc**를 입력합니다.

단계 **2** 다음 확인을 수행합니다.

- SEC 커넥터 로그( /usr/local/cdo/data/<tenantDir>/event_streamer/logs/connector.log )를 확인하고 SEC 등록이 성공했는지 확인합니다. 그렇지 않은 경우 "보안 이벤트 커넥터 등록 실패 문제 해결" 문제를 참조하십시오.
- SEC 이벤트 로그( /usr/local/cdo/data/<tenantDir>/event_streamer/logs/events-plugin.log )를 확인하고 이벤트가 처리되고 있는지 확인합니다. 그렇지 않은 경우 CDO 고객이 TAC로 지원 티켓을 여는 방법.
- SEC 도커 컨테이너에 로그인하고 "supervisorctl -c /opt/cssp/data/conf/supervisord.conf " 명령을 실행하고 출력이 아래와 같고 모든 프로세스가 RUNNING 상태인지 확인합니다. 그렇지 않은 경우 CDO 고객이 TAC로 지원 티켓을 여는 방법.

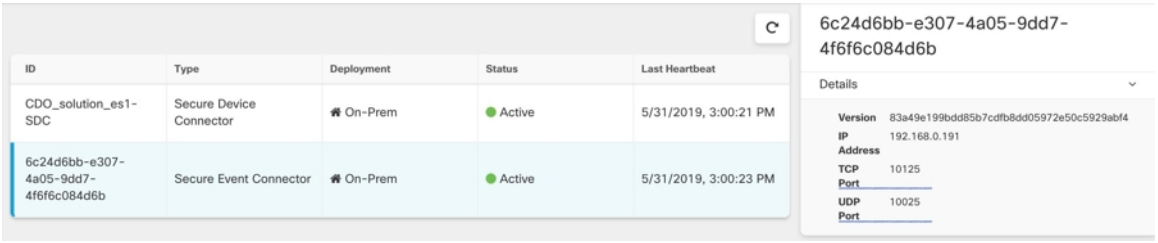
**estreamer-connector RUNNING pid 36,** 업타임 **5:25:17**

**estreamer-cron RUNNING pid 39,** 업타임 **5:25:17**

**estreamer-plugin RUNNING pid 37,** 업타임 **5:25:17**

**estreamer-rsyslog RUNNING pid 38,** 업타임 **5:25:17**

- 온프레미스 SDC의 방화벽 규칙이 보안 커넥터 페이지에서 SEC에 대해 표시된 UDP 및 TCP 포트를 차단하지 않는지 확인합니다. 어떤 포트를 열어야 하는지 확인하려면 SaaS(Secure Logging Analytics)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기를 참조하십시오.




- 자체 CentOS 7 VM을 사용하여 SDC를 수동으로 설정하고 들어오는 요청을 차단하도록 방화벽을 구성한 경우, 다음 명령을 실행하여 UDP 및 TCP 포트의 차단을 해제할 수 있습니다.

**firewall-cmd --zone=public --add-port=<udp_port>/udp --permanent**

**firewall-cmd --zone=public --add-port=<tcp_port>/tcp --permanent**

**firewall-cmd --reload**

- 선택한 Linux 네트워크 도구를 사용하여 이 포트에서 패킷이 수신되고 있는지 확인합니다. 수신되지 않는 경우 FTD 로그 구성을 다시 확인합니다.

위의 수리 중 어느 것도 작동하지 않으면, CDO 고객이 TAC로 지원 티켓을 여는 방법.

# SEC Cleanup 명령

SEC(보안 이벤트 커넥터) cleanup 명령은 SDC(보안 디바이스 커넥터) VM에서 SEC 컨테이너 및 관련 파일을 제거합니다. 보안 이벤트 커넥터 등록 실패 문제 해결, on page 561 또는 온보딩에 실패할 경우 이 명령을 실행할 수 있습니다.

명령을 실행하려면 다음을 수행합니다.

### Before you begin

이 작업을 수행하려면 테넌트의 이름을 알아야 합니다. 테넌트 이름을 찾으려면 CDO에서 사용자 메뉴를 열고 **Settings(**설정**)**를 클릭합니다. 페이지를 아래로 스크롤하여 테넌트 이름을 찾습니다.

단계 **1** 'sdc' 사용자로 SDC에 로그인합니다. 프롬프트에서 `sudo su - sdc`를 입력합니다.

단계 **2** `/usr/local/cdo/toolkit` 디렉터리에 연결합니다.

단계 **3** `sec.sh remove`*`tenant_name`*을 실행하고 SEC를 제거할 의도를 확인합니다.

예:

```
 [sdc@localhost~]$ /usr/local/cdo/toolkit/sec.sh remove tenant_XYZ
Are you sure you want to remove Secure Event Connector for tenant tenant_XYZ? (y/n): y
```

### What to do next

이 명령이 SEC를 제거하지 못한 경우 SEC Cleanup 명령 실패, on page 567를 계속하십시오.

## SEC Cleanup 명령 실패

SEC Cleanup 명령, on page 567가 실패한 경우 이 절차를 사용합니다.

메시지: SEC를 찾을 수 없습니다. 종료합니다.

증상: Cleanup SEC 명령이 기존 SEC를 정리하지 못합니다.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh remove tenant_XYZ Are you sure you want
to remove Secure Event Connector for tenant tenant_XYZ? (y/n): y [2020-06-10 04:50:42] SEC
 not found, exiting.
```

복구: 정리 명령이 실패할 때 보안 이벤트 커넥터를 수동으로 정리합니다.

이미 실행 중인 SEC 도커 컨테이너를 제거합니다.

단계 **1** 'sdc' 사용자로 SDC에 로그인합니다. 프롬프트에서 `sudo su - sdc`를 입력합니다.

단계 **2** **docker ps** 명령을 실행하여 SEC 컨테이너의 이름을 찾습니다. SEC 이름은 "es_ *name*" 형식입니다.

단계 **3** **docker stop** 명령을 실행하여 SEC 컨테이너를 중지합니다.

단계 **4** **rm** 명령을 실행하여 SEC 컨테이너를 제거합니다.

예를 들면 다음과 같습니다**.**

```
$ docker stop <SEC_docker_container_name>
$ docker rm <SEC_docker_container_name>
```

# 상태 확인을 사용하여 보안 이벤트 커넥터의 상태 학습

SEC(보안 이벤트 커넥터) 상태 확인 스크립트는 SEC의 상태에 대한 정보를 제공합니다.

상태 확인을 실행하려면 다음 절차를 따르십시오.

단계 **1** VM 하이퍼바이저를 열고 SDC(보안 디바이스 커넥터)에 대한 콘솔 세션을 시작합니다.

단계 **2** "cdo" 사용자로 SDC에 로그인합니다.

단계 **3** "sdc" 사용자로 전환합니다.

```
[cdo@tenant]$sudo su sdc
```

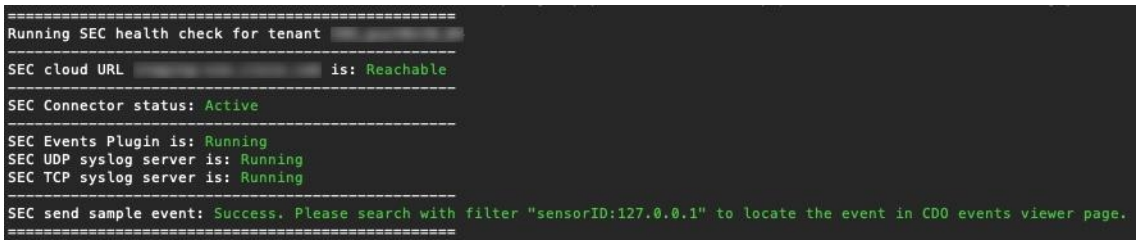
단계 **4** 프롬프트에서 healthcheck.sh 스크립트를 실행하고 테넌트 이름을 지정합니다.

```
[sdc@host ~]$ /usr/local/cdo/toolkit/healthcheck.sh --app sec --tenant CDO_[tenant_name]
```

예를 들면 다음과 같습니다.

```
[sdc@host ~]$ /usr/local/cdo/toolkit/healthcheck.sh --app sec --tenant CDO_example_tenant
```

스크립트의 출력은 다음과 같은 종류의 정보를 제공합니다.




상태 확인 출력의 값:

- **SEC Cloud URL(SEC** 클라우드 **URL)**: CDO 클라우드 URL 및 SEC가 CDO에 연결할 수 있는지 여부를 표시합니다.
- **SEC** 커넥터: SEC 커넥터가 올바르게 온보딩되고 시작된 경우 "Running(실행 중)"으로 표시됩니다.

- **SEC UDP** 시스템 로그 서버: UDP Syslog 서버가 UDP 이벤트를 전송할 준비가 된 경우 "Running(실행 중)"으로 표시됩니다.
- **SEC TCP** 시스템 로그 서버: TCP Syslog 서버가 TCP 이벤트를 전송할 준비가 된 경우 "Running(실행 중)"으로 표시됩니다.
- **SEC** 커넥터 상태: SEC가 실행 중이고 CDO에 온보딩된 경우 Active(활성)로 표시됩니다.
- **SEC Send sample event(SEC** 샘플 이벤트 전송**)**: 상태 확인이 종료될 때 모든 상태 확인이 "녹색"인 경우 툴이 샘플 이벤트를 전송합니다. (프로세스 중 하나라도 "Down" 상태이면 테스트 이벤트 전송을 건너뜁니다.) 샘플 이벤트는 이벤트 로그에 "sec-health-check"라는 정책으로 표시됩니다.

# 문제 해결 Cisco Defense Orchestrator

## 로그인 실패 문제 해결

실수로 잘못된 **CDO** 지역에 로그인했기 때문에 로그인에 실패함

적절한 CDO 지역에 로그인했는지 확인합니다. https://sign-on.security.cisco.com에 로그인하면 액세스할 지역을 선택할 수 있습니다. **CDO**타일을 클릭하여 defenceorchestrator.com에 액세스하거나 **CDO(EU)**를 클릭하여 defenceorchestrator.eu에 액세스합니다.

## 마이그레이션 후 로그인 실패 문제 해결

잘못된 사용자 이름 또는 암호로 인해 **CDO**에 로그인하지 못함

해결 방법 CDO에 로그인하려고 할 때 사용자 이름 및 비밀번호가 올바른 데도 로그인이 실패하는 것을 알고 있거나, "비밀번호를 잊음"를 시도하여 사용 가능한 비밀번호를 복원할 수 없는 경우, 새 Cisco Secure Cloud Sign-On 계정을 사용하려면 새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성, 63 페이지의 지침에 따라 새 Cisco Secure Cloud Sign-On 계정에 등록해야 합니다.

**Cisco Secure Cloud Sign-On** 대시보드 로그인에 성공했지만 **CDO**를 실행할 수 없음

해결 방법 CDO 테넌트와 다른 사용자 이름으로 Cisco Secure Cloud Sign-On 계정을 만들었을 수 있습니다. CDO와 Cisco Secure Sign-On 간의 사용자 정보를 표준화하려면 Cisco TAC(Technical Assistance Center)에 문의하십시오.

저장된 북마크를 사용한 로그인 실패

해결 방법 브라우저에 저장한 이전 북마크를 사용하여 로그인을 시도했을 수 있습니다. 북마크는 https://cdo.onelogin.com을 가리킬 수 있습니다.

해결 방법 https://sign-on.security.cisco.com에 로그인합니다.

- 해결 방법 아직 Cisco Secure Sign-On 계정을 생성하지 않은 경우 새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성

- 해결 방법 새 계정을 생성한 경우 대시보드에서 Cisco Defense Orchestrator(US), Cisco Defense Orchestrator(EU) 또는 Cisco Defense Orchestrator(APJC)에 해당하는 CDO 타일을 클릭합니다.
- 해결 방법 https://sign-on.security.cisco.com을 가리키도록 북마크를 업데이트합니다.

# 액세스 및 인증서 문제 해결

## CDO를 사용하여 사용자 액세스 문제 해결

사용자가 액세스 권한이 있어야 하는 리소스에 대한 액세스가 거부되는 경우를 고려하십시오. 다음은 해당 문제를 진단하고 해결하기 위해 취할 수 있는 접근 방식입니다.

단계 1 사용자는 리소스에 대한 액세스가 차단되었음을 보안 팀에 알립니다. 일반적으로 리소스에 도달하는 방법을 결정합니다. IP 주소는 무엇입니까? 특정 포트에 도달합니까? 리소스에 정보를 보내는 데 사용되는 프로토콜은 무엇입니까?

단계 2 **Devices & Services(**디바이스 및 서비스**)** 페이지에서 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 3 **FTD** 탭을 클릭하고 ASA를 선택하고 패킷 트레이서를 실행합니다. 자세한 지침은 AT 패킷 트레이서를 참조하십시오.

단계 4 리소스에 대한 액세스를 거부했을 수 있는 규칙에 대한 패킷 추적 테이블을 검사합니다.

단계 5 액세스를 거부하는 규칙을 식별한 후 CDO에 변경 요청 레이블을 생성하고 활성화합니다. 변경 요청 관리, on page 375을 참조하십시오. 이렇게 하면 리소스에 대한 액세스를 허용하기 위해 만든 변경 로그 정책 변경 사항을 식별하는 데 도움이 됩니다.

단계 6 동작을 편집하려면 CDO에서 규칙을 편집합니다. 이제 ASA가 CDO와 동기화되지 않습니다.

단계 7 **Devices & Services(**디바이스 및 서비스**)** 페이지에서 변경 사항을 ASA에 배포합니다. CDO는 CDO에 스테이징된 구성이 아닌 ASA에 저장된 구성을 통해 패킷을 추적합니다. CDO에서 준비된 다른 구성 변경 사항도 ASA에 배포하게 됩니다.

단계 8 패킷 트레이서를 다시 실행하여 정책 변경이 원하는 결과를 제공하는지 확인합니다. 이제 사용자가 리소스에 액세스할 수 있는지 확인합니다.

단계 9 이제 사용자에게 액세스 권한이 있다고 가정하고 CDO에서 변경 요청 레이블을 지웁니다. 이렇게 하면 관련 없는 활동이 이 편집 프로그램과 연결되지 않습니다.

**Note** 변경해도 문제가 해결되지 않거나 새로운 문제가 발생하여 이전 구성으로 돌아가고 싶은 경우 ASA 구성을 복원할 수 있습니다. Secure Firewall ASA 구성 복원 정보을 참조하십시오.

## 새 지문 탐지 상태 확인

단계 1 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 2 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 **4** 새 지문 감지됨 상태에서 디바이스를 선택합니다.

단계 **5** 새 지문 감지됨 창에서 지문 검토를 클릭합니다.

단계 **6** 지문을 검토하고 수락하라는 메시지가 표시되면

**a.** **Download Fingerprint(**지문 다운로드**)**를 클릭하고 검토합니다.

**b.** 지문에 만족하면 **Accept(**수락**)**를 클릭합니다. 그렇지 않은 경우 **Cancel(**취소**)**를 클릭합니다.

단계 **7** 새 지문 문제를 해결한 후 디바이스의 연결 상태가 온라인으로 표시되고 구성 상태가 "동기화되지 않음" 또는 "충돌 감지됨"으로 표시될 수 있습니다. 구성 충돌 해결을 검토하여 CDO와 디바이스 간의 구성 차이를 검토하고 해결합니다.

## 보안 및 분석 로깅 이벤트를 사용하여 네트워크 문제 해결

다음은 이벤트 뷰어를 사용하여 네트워크 문제를 트러블슈팅하는 데 사용할 수 있는 기본 프레임워크입니다.

이 시나리오에서는 네트워크 운영 팀에서 사용자가 네트워크의 리소스에 액세스할 수 없다는 보고를 받은 것으로 가정합니다. 문제를 보고하는 사용자와 해당 위치를 기반으로, 네트워크 운영 팀은 어떤 방화벽이 리소스에 대한 액세스를 제어하는지를 합리적으로 파악합니다.

**Note** 또한 이 시나리오에서는 FDM 관리 디바이스가 네트워크 트래픽을 관리하는 방화벽이라고 가정합니다. Security Analytics and Logging(보안 분석 및 로깅)은 다른 디바이스 유형에서 로깅 정보를 수집하지 않습니다.

단계 **1** 탐색창에서 분석 > 이벤트 로깅를 선택합니다.

단계 **2** 기록 탭을 클릭합니다.

단계 **3** 시간 범위를 기준으로 이벤트 필터링을 시작합니다. 기본적으로 Historical(기록) 탭에는 이벤트의 마지막 시간이 표시됩니다. 올바른 시간 범위인 경우 현재 날짜와 시간을 **End(**종료**)** 시간으로 입력합니다. 올바른 시간 범위가 아닌 경우 보고된 문제의 시간을 포함하는 시작 및 종료 시간을 입력합니다.

단계 **4** **Sensor ID(**센서 **ID)** 필드에 사용자의 액세스를 제어하는 것으로 의심되는 방화벽의 IP 주소를 입력합니다. 방화벽이 두 개 이상인 경우 검색 창에서 속성**:**값 쌍을 사용하여 이벤트를 필터링합니다. 두 항목을 만들고 OR 문으로 결합합니다. 예: `SensorID:192.168.10.2 OR SensorID:192.168.20.2`.

단계 **5** Events(이벤트) 필터 표시줄의 **Source IP(**소스 **IP)** 필드에 사용자의 IP 주소를 입력합니다.

단계 **6** 사용자가 리소스에 액세스할 수 없는 경우 **Destination IP(**대상 **IP)** 필드에 해당 리소스의 IP 주소를 입력해 보십시오.

단계 **7** 결과에서 이벤트를 확장하고 세부 정보를 확인합니다. 다음은 몇 가지 세부 사항입니다.

- **AC_RuleAction** - 규칙이 트리거될 때 수행된 작업(허용, 신뢰, 차단).
- **FirewallPolicy** - 이벤트를 트리거한 규칙이 상주하는 정책입니다.

- **FirewallRule** - 이벤트를 트리거한 규칙의 이름입니다. 값이 Default Action(기본 작업)인 경우 정책의 규칙 중 하나가 아니라 이벤트를 트리거한 것은 정책의 기본 작업입니다.
- **UserName** - 이니시에이터 IP 주소와 연결된 사용자입니다. 이니시에이터 IP 주소는 소스 IP 주소와 동일합니다.

단계 **8** 규칙 작업이 액세스를 차단하는 경우 FirewallRule 및 FirewallPolicy 필드를 확인하여 액세스를 차단하는 정책의 규칙을 식별합니다.

## SSL 암호 해독 문제 해결

재서명 암호 해독이 브라우저에서는 작동하지만 앱에서는 작동하지 않는 웹 사이트 처리**(SSL** 또는 인증 기관 피닝**)**

스마트폰 및 기타 디바이스용 일부 앱은 SSL(또는 인증 기관) 피닝이라는 기술을 사용합니다. SSL 피닝 기술은 원래 서버 인증서의 해시를 앱 자체에 포함합니다. 따라서 앱이 Firepower Threat Defense 디바이스에서 재서명된 인증서를 받으면 해시 검증에 실패하고 연결이 중단됩니다.

이때 기본적인 증상은 사용자가 사이트 앱을 사용해서는 웹 사이트에 연결할 수 없지만 웹 브라우저를 사용하면 연결할 수 있다는 것입니다(앱으로 연결에 실패한 디바이스에서 브라우저를 사용할 때도 연결 가능). 예를 들어 사용자는 Facebook iOS 또는 Android 앱을 사용할 수 없지만 Safari 또는 Chrome을 https://www.facebook.com으로 지정하고 성공적으로 연결할 수 있습니다.

SSL 피닝은 특별히 메시지 가로채기(man-in-the-middle) 공격을 차단하는 데 사용되므로 이러한 현상을 해결하는 방법은 없습니다. 다음 옵션 중에서 선택해야 합니다.

기타 세부정보

특정 사이트가 브라우저에서는 작동하는데 동일 디바이스의 앱에서는 작동하지 않는 경우 SSL 피닝 인스턴스를 살펴봐야 합니다. 하지만 심층적으로 확인하려면 연결 이벤트를 사용해 브라우저 테스트와 더불어 SSL 피닝을 확인할 수 있습니다.

앱은 두 가지 방식으로 해시 검증 장애를 처리할 수 있습니다.

- Facebook 등의 그룹 1 앱은 서버에서 SH, CERT, SHD 메시지를 받는 즉시 SSL ALERT 메시지를 보냅니다. Alert는 보통 SSL 피닝을 나타내는 "Unknown CA (48)(알 수 없는 CA(48))" 알림입니다. 알림 메시지 후에는 TCP Reset(TCP 재설정)이 전송됩니다. 이벤트 세부사항에는 다음 증상이 표시됩니다.
  - `SSL Flow Flag(SSL 플로우 플래그)에는 ALERT_SEEN이 포함되어 있습니다.`
  - `SSL Flow Flag(SSL 플로우 플래그)에는 APP_DATA_C2S 또는 APP_DATA_S2C가 포함되어 있지 않습니다.`
  - `SSL Flow Message(SSL 플로우 메시지)는 보통 CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE입니다.`
- Dropbox 등의 그룹 2 앱은 알림을 보내지 않습니다. 대신 핸드셰이크가 완료될 때까지 기다렸다가 TCP Reset(TCP 재설정)을 전송합니다. 이벤트에는 다음 증상이 표시됩니다.

- SSL Flow Flag(SSL 플로우 플래그)에는 ALERT_SEEN, APP_DATA_C2S 또는 APP_DATA_S2C가 포함되어 있지 않습니다.
- SSL Flow Message(SSL 플로우 메시지)는 보통 CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE, CLIENT_KEY_EXCHANGE, CLIENT_CHANGE_CIPHER_SPEC, CLIENT_FINISHED, SERVER_CHANGE_CIPHER_SPEC, SERVER_FINISHED입니다.

# 마이그레이션 후 로그인 실패 문제 해결

잘못된 사용자 이름 또는 암호로 인해 **CDO**에 로그인하지 못함

해결 방법 CDO에 로그인하려고 할 때 사용자 이름 및 비밀번호가 올바른 데도 로그인이 실패하는 것을 알고 있거나, "비밀번호를 잊음"를 시도하여 사용 가능한 비밀번호를 복원할 수 없는 경우, 새 Cisco Secure Cloud Sign-On 계정을 사용하려면 새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성, 63 페이지의 지침에 따라 새 Cisco Secure Cloud Sign-On 계정에 등록해야 합니다.

**Cisco Secure Cloud Sign-On** 대시보드 로그인에 성공했지만 **CDO**를 실행할 수 없음

해결 방법 CDO 테넌트와 다른 사용자 이름으로 Cisco Secure Cloud Sign-On 계정을 만들었을 수 있습니다. CDO와 Cisco Secure Sign-On 간의 사용자 정보를 표준화하려면 Cisco TAC(Technical Assistance Center)에 문의하십시오.

저장된 북마크를 사용한 로그인 실패

해결 방법 브라우저에 저장한 이전 북마크를 사용하여 로그인을 시도했을 수 있습니다. 북마크는 https://cdo.onelogin.com을 가리킬 수 있습니다.

해결 방법 https://sign-on.security.cisco.com에 로그인합니다.

- 해결 방법 아직 Cisco Secure Sign-On 계정을 생성하지 않은 경우 새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성
- 해결 방법 새 계정을 생성한 경우 대시보드에서 Cisco Defense Orchestrator(US), Cisco Defense Orchestrator(EU) 또는 Cisco Defense Orchestrator(APJC)에 해당하는 CDO 타일을 클릭합니다.
- 해결 방법 https://sign-on.security.cisco.com을 가리키도록 북마크를 업데이트합니다.

# 개체 문제 해결

## 중복 개체 문제 해결

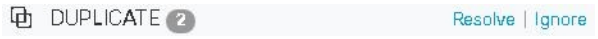
중복 개체 는 이름은 다르지만 값은 동일한 디바이스에 있는 두 개 이상의 개체입니다. 이러한 개체는 대개 실수로 생성되고 유사한 용도로 사용되며 다른 정책에서 사용됩니다. 중복 개체 문제를 해결한 후 CDO는 유지된 개체 이름으로 영향을 받는 모든 개체 참조를 업데이트합니다.

중복 개체 문제를 해결하려면 다음을 수행합니다.

단계 **1** 왼쪽의 CDO 탐색 바에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 그런 다음 개체를 개체 필터하여 중복 개체 문제를 찾습니다.

단계 **3** 결과 중 하나를 선택합니다. 개체 세부 정보 패널에 영향을 받는 중복 수가 포함된 DUPLICATE 필드가 표시됩니다.




단계 **4** **Resolve(**해결**)**를 클릭합니다. CDO는 비교할 중복 개체를 표시합니다.

단계 **5** 비교할 두 개체를 선택합니다.

단계 **6** 이제 다음과 같은 옵션이 제공됩니다.

- 개체 중 하나를 다른 개체로 교체하려면 유지할 개체에 대해 **Pick(**선택**)**을 클릭하고 **Resolve(**확인**)**를 클릭하여 영향을 받을 디바이스 및 네트워크 정책을 확인한 다음, 변경 사항이 마음에 들면 **Confirm(**확인**)**를 클릭합니다. CDO는 선택한 개체를 교체로 유지하고 중복 항목을 삭제합니다.
- 목록에 무시할 개체가 있는 경우 **Ignore(**무시**)**를 클릭합니다. 개체를 무시하면 CDO에 표시되는 중복 개체 목록에서 제거됩니다.
- 개체는 유지하지만 CDO가 중복 개체를 검색할 때 찾지 않도록 하려면 **Ignore All(**모두 무시**)**를 클릭합니다.

단계 **7** 중복 개체 문제가 해결되면 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

## 사용되지 않는 개체 문제 해결

사용되지 않는 개체는 디바이스 구성에 존재하지만 다른 개체, 액세스 목록 또는 NAT 규칙에서 참조하지 않는 개체입니다.

관련 정보**:**

- 디바이스 및 서비스 목록 내보내기, 82 페이지
- CDO에 디바이스 대량 다시 연결, 86 페이지

사용되지 않은 개체 문제 해결

단계 **1** 왼쪽의 CDO 내비게이션 바에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 그런 다음 개체를 개체 필터하여 사용하지 않는 개체 문제를 찾습니다.

단계 **3** 하나 이상의 사용되지 않는 개체를 선택합니다.

단계 **4** 이제 다음과 같은 옵션이 제공됩니다.

- Actions(작업) 창에서 **Remove(**제거**)** 를 클릭하여 CDO에서 사용되지 않는 개체를 제거합니다.
- Issues(문제) 창에서 **Ignore(**무시**)**를 클릭합니다. 개체를 무시하면 CDO는 사용되지 않은 개체의 결과에 해당 개체를 표시하지 않습니다.

단계 **5** 사용되지 않는 개체를 제거한 경우, 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, on page 352지금 변경한 사항을 수행하거나 대기하고 여러 변경 사항을 한 번에 구축합니다.

**Note** 사용되지 않는 개체 문제를 벌크로 해결하려면 대량의 개체 문제 해결을 참조하십시오.

### 사용되지 않는 개체 대량 제거

단계 **1** 왼쪽의 CDO 내비게이션 바에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 그런 다음 개체를 개체 필터하여 사용하지 않는 개체 문제를 찾습니다.

단계 **3** 삭제하려는 사용되지 않는 개체를 선택합니다.

- 개체 테이블 헤더 행의 확인란을 클릭하여 페이지의 모든 개체를 선택합니다.
- 개체 테이블에서 사용하지 않는 개별 개체를 선택합니다.

단계 **4** 오른쪽의 작업 창에서 **Remove(**제거**)** 를 클릭하여 CDO에서 선택한 사용되지 않는 개체를 모두 제거합니다. 한 번에 99개의 개체를 제거할 수 있습니다.

단계 **5** **OK(**확인**)**을 클릭하여 사용하지 않는 개체를 삭제할 것인지 확인합니다.

단계 **6** 이러한 변경 사항을 배포하기 위한 두 가지 선택 사항이 있습니다.

- 지금 변경한 내용을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.
- **Inventory(**인벤토리**)** 페이지를 열고 변경의 영향을 받은 디바이스를 찾습니다. 변경의 영향을 받는 모든 디바이스를 선택하고 관리 창에서 **Deploy All(**모두 배포**)** 를 클릭합니다. 경고를 읽고 적절한 조치를 취합니다.

## 불일치 개체 문제 해결

불일치 개체 INCONSISTENT 2 Resolve | Ignore 는 두 개 이상의 디바이스에서 이름은 같지만 값이 다른 개체입니다. 사용자가 동일한 이름 및 콘텐츠를 사용하여 서로 다른 구성에서 개체를 생성하지만 시간이 지남에 따라 이러한 개체의 값이 달라지므로 불일치가 발생하는 경우가 있습니다.

참고: 일관되지 않은 개체 문제를 벌크로 해결하려면 대량의 개체 문제 해결을 참고하십시오.

일치하지 않는 개체에 대해 다음을 수행할 수 있습니다.

- **Ignore(**무시**)**: CDO가 개체 간의 불일치를 무시하고 해당 값을 유지합니다. 개체가 더 이상 불일치 범주에 나열되지 않습니다.
- **Merge(**병합**)**: CDO가 선택한 모든 개체와 해당 값을 단일 개체 그룹으로 결합합니다.
- **Rename(**이름 바꾸기**)**: CDO를 사용하면 일치하지 않는 개체 중 하나의 이름을 바꾸고 새 이름을 지정할 수 있습니다.

- **Convert Shared Network Objects to Overrides(**공유 네트워크 개체를 오버라이드로 변환**)**: CDO를 사용하면 일관성이 없는 공유 개체(오버라이드가 있거나 없는)를 오버라이드가 있는 단일 공유 개체로 결합할 수 있습니다. 일치하지 않는 개체의 가장 일반적인 기본값은 새로 형성된 개체의 기본값으로 설정됩니다.

**Note** 공통 기본값이 여러 개인 경우 그 중 하나가 기본값으로 선택됩니다. 나머지 기본값 및 재정의 값은 해당 개체의 재정의로 설정됩니다.

- **Convert Shared Network Group to Additional Values(**공유 네트워크 그룹을 추가 값으로 변환**):** - CDO를 사용하면 일치하지 않는 공유 네트워크 그룹을 추가 값이 있는 단일 공유 네트워크 그룹으로 결합할 수 있습니다. 이 기능의 기준은 변환할 일관되지 않은 네트워크 그룹에 동일한 값을 가진 공통 개체가 하나 이상 있어야 한다는 것입니다. 이 기준과 일치하는 모든 기본값은 기본값이 되며, 나머지 개체는 새로 형성된 네트워크 그룹의 추가 값으로 할당됩니다.

  예를 들어, 일치하지 않는 두 개의 공유 네트워크 그룹을 고려하십시오. 첫 번째 네트워크 그룹 'shared_network_group'은 'object_1'(192.0.2.x) 및 'object_2'(192.0.2.y)로 구성됩니다. 여기에는 추가 값 'object_3'(192.0.2.a)도 포함됩니다. 두 번째 네트워크 그룹 'shared_network_group'은 'object_1'(192.0.2.x) 및 추가 값 'object_4'(192.0.2.b)로 구성됩니다. 공유 네트워크 그룹을 추가 값으로 변환할 때 새로 형성된 그룹 'shared_network_group'에는 'object_1'(192.0.2.x) 및 'object_2'(192.0.2.y)'가 포함되며, 'object_3'(192.0. 2.a) 및 'object_4'(192.0.2.b)를 추가 값으로 사용합니다.

**Note** 새 네트워크 개체를 생성하면 CDO는 자동으로 해당 값을 동일한 이름의 기존 공유 네트워크 개체에 오버라이드로 할당합니다. 이는 새 디바이스가 CDO에 온보딩된 경우에도 적용됩니다.

자동 할당은 다음 기준을 충족하는 경우에만 발생합니다.

1. 새 네트워크 개체를 디바이스에 할당해야 합니다.
2. 이름과 유형이 같은 공유 개체는 테넌트에 하나만 있어야 합니다.
3. 공유 개체에 이미 오버라이드가 포함되어 있어야 합니다.

일관성 없는 개체 문제를 해결하려면 다음을 수행합니다.

단계 **1** 왼쪽의 CDO 내비게이션 바에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 그런 다음 개체를 개체 필터하여 일관성 없는 개체 문제를 찾습니다.

단계 **3** 일치하지 않는 개체를 선택합니다. 개체 세부 정보 패널에 영향을 받는 개체의 수가 포함된 INCONSISTENT 필드가 표시됩니다.

단계 **4** **Resolve(**해결**)**를 클릭합니다. CDO는 비교할 일치하지 않는 개체를 표시합니다.

단계 **5** 이제 다음과 같은 옵션이 제공됩니다.

- 모두 무시**:**
  a. 표시된 개체를 비교하고 개체 중 하나에서 **Ignore(**무시**)**를 클릭합니다. 또는 모든 개체를 무시하려면 **Ignore All(**모두 무시**)**을 클릭합니다.
  b. **OK(**확인**)**를 클릭하여 확인합니다.
- 개체를 병합하여 해결합니다**.**
  a. **Resolve by Merging X Objects(X**개 개체를 병합하여 해결**)**를 클릭합니다.
  b. **OK(**확인**)**를 클릭합니다.
- **Rename(**이름 바꾸기**):**
  a. **Rename(**이름 변경**)**을 클릭합니다.
  b. 영향을 받는 네트워크 정책 및 디바이스에 변경 사항을 저장하고 **Confirm(**확인**)**을 클릭합니다.
- **Convert to Overrides(**오버라이드로 변환**)(**일치하지 않는 공유 개체의 경우**)**: 공유 개체를 오버라이드와 비교할 때, 비교 패널의 **Inconsistent Values(**일관되지 않는 값**)** 필드에 기본값만 표시됩니다.
  a. **Convert to Overrides(**재정의로 변환**)**를 클릭합니다. 일치하지 않는 모든 개체는 오버라이드가 포함된 단일 공유 개체로 변환됩니다.
  b. **OK(**확인**)**를 클릭합니다. **Edit Shared Object(**공유 개체 편집**)**를 클릭하여 새로 형성된 개체의 세부 정보를 볼 수 있습니다. 위쪽 및 아래쪽 화살표를 사용하여 기본값과 재정의 간에 값을 이동할 수 있습니다.
- **Convert to Additional Values(**추가 값으로 변환**)(**일치하지 않는 네트워크 그룹의 경우**):**
  a. **Convert to Additional Values(**추가 값으로 변환**)**를 클릭합니다. 일치하지 않는 모든 개체는 추가 값이 있는 단일 공유 개체로 변환됩니다.
  b. 영향을 받는 네트워크 정책 및 디바이스에 변경 사항을 저장하고 **Confirm(**확인**)**을 클릭합니다.

단계 **6** 불일치를 해결한 후 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 대량의 개체 문제 해결

사용되지 않는 개체 문제 해결 중복 개체 문제 해결 불일치 개체 문제 해결, on page 575 문제가 있는 개체를 해결하는 한 가지 방법은 이러한 개체를 무시하는 것입니다. 개체에 둘 이상의 문제가 있더라도 여러 개체를 선택하고 무시할 수 있습니다. 예를 들어 개체가 일치하지 않고 사용되지 않는 경우 한 번에 하나의 문제 유형만 무시할 수 있습니다.

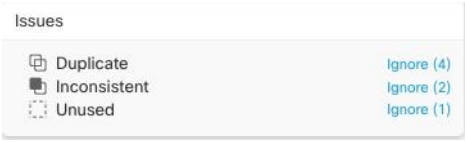
**Important** 나중에 개체가 다른 문제 유형과 연결될 경우 커밋한 무시 작업은 해당 시점에 선택한 문제에만 영향을 미칩니다. 예를 들어, 개체가 중복되었기 때문에 개체를 무시했고 개체가 나중에 일치하지 않는 것으로 표시되는 경우, 중복 개체로 무시한다고 해서 일치하지 않는 개체로 무시되는 것은 아닙니다.

대량으로 문제를 무시하려면 다음 절차를 수행합니다.

단계 **1** 왼쪽의 CDO 내비게이션 바에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 검색 범위를 좁히기 위해 개체 문제를 개체 필터할 수 있습니다.

단계 **3** Object(개체) 테이블에서 무시할 적용 가능한 모든 개체를 선택합니다. Issues(문제) 창은 문제 유형별로 개체를 그룹화합니다.




단계 **4** 유형별로 문제를 무시하려면 **Ignore(**무시**)**를 클릭합니다. 각 문제 유형을 개별적으로 무시해야 합니다.

단계 **5** **OK(**확인**)**를 클릭하여 해당 개체를 무시할 것임을 확인합니다.

# 디바이스 연결 상태

CDO 테넌트에 온보딩된 디바이스의 연결 상태를 볼 수 있습니다. 이 항목은 다양한 연결 상태를 이해하는 데 도움이 됩니다. **Inventory(**인벤토리**)** 페이지에서 **Connectivity(**연결**)** 열은 디바이스 연결 상태를 표시합니다.

디바이스 연결 상태가 '온라인'이면 디바이스의 전원이 켜져 있고 CDO에 연결되어 있음을 의미합니다. 아래 표에 설명된 다른 상태는 일반적으로 여러 가지 이유로 디바이스에 문제가 발생할 때 발생합니다. 이 표는 이러한 문제에서 복원하는 방법을 제공합니다. 연결 실패를 일으키는 문제가 두 개 이상 있을 수 있습니다. 다시 연결을 시도하면, CDO는 다시 연결을 수행하기 전에 먼저 이러한 모든 문제를 편집하라는 메시지를 표시합니다.

| 디바이스 연결 상태 | 가능한 이유 | 해결 방법 |
|---|---|---|
| 온라인 | 디바이스의 전원이 켜져 있고 CDO에 연결되어 있습니다. | 해당 없음 |
| 오프라인 | 디바이스의 전원이 꺼졌거나 네트워크 연결이 끊겼습니다. | 디바이스가 오프라인 상태인지 확인합니다. |
| 불충분한 라이선스 | 디바이스에 충분한 라이선스가 없습니다. | 라이선스 부족 문제 해결, on page 579 |

| 디바이스 연결 상태 | 가능한 이유 | 해결 방법 |
|---|---|---|
| 유효하지 않은 자격 증명 | 디바이스에 연결하기 위해 CDO에서 사용하는 사용자 이름과 암호 조합이 올바르지 않습니다. | 유효하지 않은 자격 증명 문제 해결, on page 579 |
| 새 인증서 탐지됨 | 디바이스의 인증서가 변경되었습니다. 디바이스가 자체 서명된 인증서를 사용하는 경우 디바이스의 전원을 껐다 켜서 이 문제가 발생했을 수 있습니다. | 새 인증서 문제 트러블슈팅, on page 580 |
| 온보딩 오류 | CDO는 디바이스를 온보딩할 때 디바이스와의 연결이 끊어졌을 수 있습니다. | 온보딩 오류 문제 해결, on page 589 |

# 라이선스 부족 문제 해결

디바이스 연결 상태가 "Insufficient License(라이선스 부족)"로 표시되면 다음을 수행합니다.

- 디바이스가 라이선스를 획득할 때까지 잠시 기다립니다. 일반적으로 Cisco Smart Software Manager가 디바이스에 새 라이선스를 적용하는 데 시간이 걸립니다.
- 디바이스 상태가 변경되지 않으면 CDO에서 로그아웃하고 다시 로그인하여 CDO 포털을 새로 고침한 후 라이선스 서버와 디바이스 간의 네트워크 통신 문제를 해결합니다.
- 포털을 새로 고침해도 디바이스 상태가 변경되지 않으면 다음을 수행합니다.

---

단계 **1** Cisco Smart Software Manager에서 새 토큰을 생성하고 복사합니다. 자세한 내용은 스마트 라이선싱 생성 비디오를 참조하십시오.

단계 **2** CDO 탐색 모음에서 **Devices & Services(**디바이스 및 서비스**)** 페이지를 클릭합니다.

단계 **3** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **4** 적절한 디바이스 유형 탭을 클릭하고 **Insufficient License(**라이선스 부족**)** 상태의 디바이스를 선택합니다.

단계 **5** **Device Details(**디바이스 세부 정보**)** 창에서 **Insufficient Licenses(**불충분한 라이선스**)**에 표시되는 **Manage Licenses(**라이선스 관리**)**를 클릭합니다. **Manage Licenses(**라이선스 관리**)** 창이 나타납니다.

단계 **6** 활성화 필드에 새 토큰을 붙여넣고 디바이스 등록를 클릭합니다.

토큰이 디바이스에 성공적으로 적용되면 연결 상태가 온라인으로 바뀝니다.

---

# 유효하지 않은 자격 증명 문제 해결

유효하지 않은 자격 증명으로 인한 디바이스 연결 끊김을 해결하려면 다음을 수행합니다.

단계 **1** **Inventory(**재고 목록**)** 페이지를 엽니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 적절한 디바이스 유형 탭을 클릭하고 **Invalid Credentials(**유효하지 않은 자격 증명**)** 상태의 디바이스를 선택합니다.

단계 **4** **Device Details(**디바이스 세부 정보**)** 창에서 **Invalid Credentials(**잘못된 자격 증명**)**에 나타나는 **Reconnect(**재연결**)**을 클릭합니다. CDO가 디바이스와의 재연결을 시도합니다.

단계 **5** 프롬프트가 나타나면 Linux 사용자 이름 및 비밀번호를 입력합니다.

단계 **6** **Continue(**계속**)**를 클릭합니다.

단계 **7** 디바이스가 온라인 상태가 되고 사용할 준비가 되면 **Close(**닫기**)**를 클릭합니다.

단계 **8** CDO가 잘못된 자격 증명을 사용하여 디바이스에 연결하려고 시도했기 때문에 CDO가 디바이스에 연결하는 데 사용해야 하는 사용자 이름 및 비밀번호 조합이 디바이스에서 직접 변경되었을 수 있습니다. 이제 디바이스가 "Online(온라인)"이지만 구성 상태가 "Conflict Detected(충돌 탐지됨)"인 것을 확인할 수 있습니다. 구성 충돌 해결를 사용하여 CDO와 디바이스 간의 구성 차이를 검토하고 해결합니다.

# 새 인증서 문제 트러블슈팅

**CDO**의 인증서 사용

CDO는 디바이스에 연결할 때 인증서의 유효성을 확인합니다. 특히 CDO는 다음을 요구합니다.

1. 디바이스에서 1.0 이상의 TLS 버전을 사용합니다.
2. 디바이스에서 제시한 인증서가 만료되지 않았으며 발급 날짜가 과거입니다(즉, 이미 유효하며 나중에 유효해질 예정이 아님).
3. 인증서는 SHA-256 인증서여야 합니다. SHA-1 인증서는 허용되지 않습니다.
4. 다음 조건 중 하나가 참입니다.
   - 디바이스가 자체 서명 인증서를 사용하며, 인증된 사용자가 신뢰하는 최신 인증서와 동일합니다.
   - 디바이스는 신뢰할 수 있는 CA(Certificate Authority)에서 서명한 인증서를 사용하며, 제공된 리프 인증서를 관련 CA에 연결하는 인증서 체인을 제공합니다.

다음은 CDO가 브라우저와 다른 방식으로 인증서를 사용하는 방법입니다.

- 자체 서명 인증서의 경우 CDO는 도메인 이름 확인을 오버라이드하며, 그 대신 디바이스 온보딩 또는 재연결 중에 인증된 사용자가 신뢰하는 인증서와 인증서가 정확히 일치하는지 확인합니다.
- CDO는 아직 내부 CA를 지원하지 않습니다. 현재는 내부 CA가 서명한 인증서를 확인할 수 있는 방법이 없습니다.

  디바이스별로 ASA 디바이스에 대한 인증서 확인을 비활성화할 수 있습니다. CDO에서 ASA의 인증서를 신뢰할 수 없는 경우 해당 디바이스에 대한 인증서 검사를 비활성화할 수 있습니다. 디바이스에 대한 인증서 확인을 비활성화하려고 시도했지만 여전히 디바이스를 온보딩할 수 없는

경우, 디바이스에 대해 지정한 IP 주소 및 포트가 잘못되었거나 연결할 수 없는 것일 수 있습니다. 인증서 검사를 전역적으로 비활성화하거나 지원되는 인증서가 있는 디바이스에 대한 인증서 검사를 비활성화할 수 있는 방법은 없습니다. 비 ASA 디바이스에 대한 인증서 확인을 비활성화할 수 있는 방법은 없습니다.

디바이스에 대한 인증서 확인을 비활성화하면 CDO는 TLS를 사용하여 디바이스에 연결하지만 연결을 설정하는 데 사용된 인증서를 검증하지 않습니다. 즉, 수동적인 중간자 공격자는 연결을 도청할 수 없지만, 활성 상태의 중간자 공격자는 CDO에 유효하지 않은 인증서를 제공하여 연결을 가로챌 수 있습니다.

### 인증서 문제 식별

CDO가 디바이스를 온보딩하지 못할 수 있는 몇 가지 이유가 있습니다. UI에 "CDO cannot connect to the device using the certificate presented(CDO가 제공된 인증서를 사용하여 디바이스에 연결할 수 없음)"라는 메시지가 표시되면 인증서에 문제가 있는 것입니다. UI에 이 메시지가 표시되지 않으면 연결 문제(디바이스에 연결할 수 없음) 또는 기타 네트워크 오류와 관련이 있을 가능성이 높습니다.

CDO가 지정된 인증서를 거부하는 이유를 확인하려면 SDC 호스트 또는 관련 디바이스에 연결할 수 있는 다른 호스트에서 openssl 명령줄 툴을 사용할 수 있습니다. 다음 명령을 사용하여 디바이스에서 제공하는 인증서를 보여주는 파일을 생성합니다.

```
openssl s_client -showcerts -connect <host>:<port> &> <filename>.txt
```

이 명령은 인터랙티브 세션을 시작하므로 몇 초 후에 종료하려면 Ctrl-c를 사용해야 합니다.

이제 다음과 같은 출력이 포함된 파일이 생성됩니다.

```
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify return:1
depth=1 C = US, O = Google Inc, CN = Google Internet Authority G2
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google Inc, CN = *.google.com
verify return:1 CONNECTED(00000003)
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
  i:/C=US/O=Google Inc/CN=Google Internet Authority G2
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
  i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
  i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE-----
---
Server certificate
```

```
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits

---
SSL handshake has read 4575 bytes and written 434 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1.2
    Cipher : ECDHE-RSA-AES128-GCM-SHA256
    Session-ID: 48F046F3360225D51BE3362B50CE4FE8DB6D6B80B871C2A6DD5461850C4CF5AB
    Session-ID-ctx:
    Master-Key:
9A9CCBAA4F5A25B95C37EF7C6870F8C5DD3755A9A7B4CCE4535190B793DEFF53F94203AB0A62F9F70B9099FBFEBAB1B6

    Key-Arg : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 100800 (seconds)
    TLS session ticket:
    0000 - 7a eb 54 dd ac 48 7e 76-30 73 b2 97 95 40 5b de z.T..H~v0s...@[.
    0010 - f3 53 bf c8 41 36 66 3e-5b 35 a3 03 85 6f 7d 0c .S..A6f>[5...o}.
    0020 - 4b a6 90 6f 95 e2 ec 03-31 5b 08 ca 65 6f 8f a6 K..o....1[..eo..
    0030 - 71 3d c1 53 b1 29 41 fc-d3 cb 03 bc a4 a9 33 28 q=.S.)A.......3(
    0040 - f8 c8 6e 0a dc b3 e1 63-0e 8f f2 63 e6 64 0a 36 ..n....c...c.d.6
    0050 - 22 cb 00 3a 59 1d 8d b2-5c 21 be 02 52 28 45 9d "..:Y...\!..R(E.
    0060 - 72 e3 84 23 b6 f0 e2 7c-8a a3 e8 00 2b fd 42 1d r..#...|....+.B.
    0070 - 23 35 6d f7 7d 85 39 1c-ad cd 49 f1 fd dd 15 de #5m.}.9...I.....
    0080 - f6 9c ff 5e 45 9c 7c eb-6b 85 78 b5 49 ea c4 45 ...^E.|.k.x.I..E
    0090 - 6e 02 24 1b 45 fc 41 a2-87 dd 17 4a 04 36 e6 63 n.$.E.A....J.6.c
    00a0 - 72 a4 ad
    00a4 - <SPACES/NULS> Start Time: 1476476711 Timeout : 300 (sec)
Verify return code: 0 (ok)
---
```

이 출력에서 가장 먼저 확인할 사항은 반환 코드 확인이 표시되는 마지막 줄입니다. 인증서 문제가 있는 경우 반환 코드는 0이 아니며 오류에 대한 설명이 표시됩니다.

일반적인 오류 및 해결 방법을 보려면 이 인증서 오류 코드 목록을 확장합니다.

0 X509_V_OK 작업에 성공했습니다.

2 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT 신뢰할 수 없는 인증서의 발급자 인증서를 찾을 수 없습니다.

3 X509_V_ERR_UNABLE_TO_GET_CRL 인증서의 CRL을 찾을 수 없습니다.

4 X509_V_ERR_UNABLE_TO_DECRYPT_CERT_SIGNATURE 인증서 서명을 해독할 수 없습니다. 이는 실제 서명 값이 예상 값과 일치하지 않는 것이 아니라 확인할 수 없음을 의미합니다. 이는 RSA 키에만 의미가 있습니다.

5 X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE CRL 서명을 해독할 수 없습니다. 이는 실제 서명 값이 예상 값과 일치하지 않는 것이 아니라 확인할 수 없음을 의미합니다. 사용되지 않음.

6 X509_V_ERR_UNABLE_TO_DECODE_ISSUER_PUBLIC_KEY 인증서 SubjectPublicKeyInfo의 공개 키를 읽을 수 없습니다.

7 X509_V_ERR_CERT_SIGNATURE_FAILURE 인증서의 서명이 유효하지 않습니다.

8 X509_V_ERR_CRL_SIGNATURE_FAILURE 인증서의 서명이 유효하지 않습니다.

9 X509_V_ERR_CERT_NOT_YET_VALID 인증서가 아직 유효하지 않습니다. notBefore 날짜가 현재 시간 이후입니다. 자세한 내용은 아래의 반환 코드 확인: 9(인증서가 아직 유효하지 않음)를 참조하십시오.

10 X509_V_ERR_CERT_HAS_EXPIRED 인증서가 만료되었습니다. 즉, notAfter 날짜는 현재 시간 이전입니다. 자세한 내용은 아래의 반환 코드 확인: 10(인증서가 만료되었습니다)을 참조하십시오.

11 X509_V_ERR_CRL_NOT_YET_VALID CRL이 아직 유효하지 않습니다.

12 X509_V_ERR_CRL_HAS_EXPIRED CRL이 만료되었습니다.

13 X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD 인증서 notBefore 필드에 잘못된 시간이 포함되어 있습니다.

14 X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD 인증서 notAfter 필드에 유효하지 않은 시간이 포함되어 있습니다.

15 X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD CRL lastUpdate 필드에 잘못된 시간이 포함되어 있습니다.

16 X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD CRL nextUpdate 필드에 유효하지 않은 시간이 포함되어 있습니다.

17 X509_V_ERR_OUT_OF_MEM 메모리를 할당하는 동안 오류가 발생했습니다. 이러한 현상은 발생해서는 안 됩니다.

18 X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT 전달된 인증서가 자체 서명되었으며 신뢰할 수 있는 인증서 목록에서 동일한 인증서를 찾을 수 없습니다.

19 X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN 신뢰할 수 없는 인증서를 사용하여 인증서 체인을 배포할 수 있지만 루트를 로컬에서 찾을 수 없습니다.

20 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY 로컬로 조회된 인증서의 발급자 인증서를 찾을 수 없습니다. 이는 일반적으로 신뢰할 수 있는 인증서 목록이 완전하지 않음을 의미합니다.

21 X509_V_ERR_UNABLE_TO_VERIFY_LEAF_SIGNATURE 체인에 하나의 인증서만 포함되어 있으며 자체 서명되지 않았으므로 서명을 확인할 수 없습니다. 자세한 내용은 아래의 "반환 코드 확인: 21(첫 번째 인증서를 확인할 수 없음)"를 참조하십시오. 자세한 내용은 아래의 반환 코드 확인: 21(첫 번째 인증서를 확인할 수 없음)을 참조하십시오.

22 X509_V_ERR_CERT_CHAIN_TOO_LONG 인증서 체인 길이가 제공된 최대 깊이보다 큽니다. 사용되지 않음.

23 X509_V_ERR_CERT_REVOKED 인증서가 해지되었습니다.

24 X509_V_ERR_INVALID_CA CA 인증서가 유효하지 않습니다. CA가 아니거나 확장명이 제공된 목적과 일치하지 않습니다.

25 X509_V_ERR_PATH_LENGTH_EXCEEDED basicConstraints pathlength 매개변수가 초과되었습니다.

26 X509_V_ERR_INVALID_PURPOSE 제공된 인증서를 지정된 용도로 사용할 수 없습니다.

27 X509_V_ERR_CERT_UNTRUSTED 루트 CA가 지정된 용도로 신뢰할 수 있는 것으로 표시되지 않았습니다.

28 X509_V_ERR_CERT_REJECTED 루트 CA가 지정된 용도를 거부하도록 표시되었습니다.

29 X509_V_ERR_SUBJECT_ISSUER_MISMATCH 해당 주체 이름이 현재 인증서의 발급자 이름과 일치하지 않아 현재 후보 발급자 인증서가 거부되었습니다. -issuer_checks 옵션이 설정된 경우에만 표시됩니다.

30 X509_V_ERR_AKID_SKID_MISMATCH 현재 후보 발급자 인증서가 거부되었습니다. 해당 주체 키 식별자가 있고 인증 기관 키 식별자가 현재 인증서와 일치하지 않기 때문입니다. -issuer_checks 옵션이 설정된 경우에만 표시됩니다.

31 X509_V_ERR_AKID_ISSUER_SERIAL_MISMATCH 발급자 이름 및 일련 번호가 존재하고 현재 인증서의 기관 키 식별자와 일치하지 않으므로 현재 발급자 인증서가 거부되었습니다. -issuer_checks 옵션이 설정된 경우에만 표시됩니다.

32 X509_V_ERR_KEYUSAGE_NO_CERTSIGN keyUsage 확장이 인증서 서명을 허용하지 않으므로 현재 발급자 인증서가 거부되었습니다.

50 X509_V_ERR_APPLICATION_VERIFICATION 애플리케이션 관련 오류입니다. 사용되지 않음.

### 새 인증서 탐지됨

자체 서명 인증서가 있는 디바이스를 업그레이드하고 업그레이드 프로세스 후에 새 인증서가 생성되는 경우 CDO는 **Configuration Status(**구성 상태**)** 및 **Connectivity(**연결성**)** 상태로 "New Certificate Detected(새 인증서 탐지됨)" 메시지를 생성할 수 있습니다. CDO에서 계속 관리하려면 이 문제를 수동으로 확인하고 해결해야 합니다. 인증서가 동기화되고 디바이스가 정상 상태가 되면 디바이스를 관리할 수 있습니다.

**Note** 두 개 이상의 관리 디바이스를 동시에 CDO에 다시 CDO에 디바이스 대량 다시 연결하는 경우 CDO는 디바이스에서 새 인증서를 자동으로 검토 및 수락하고 계속해서 다시 연결합니다.

다음 절차를 사용하여 새 인증서를 확인합니다.

1. **Device & Services(**디바이스 및 서비스**)** 페이지로 이동합니다.
2. 필터를 사용하여 **New Certificate Detected(**새 인증서 탐지됨**)** 연결 또는 구성 상태의 디바이스를 표시하고 원하는 디바이스를 선택합니다.
3. Action(작업) 창에서 **Review Certificate(**인증서 검토**)**를 클릭합니다. CDO에서는 검토를 위해 인증서를 다운로드하고 새 인증서를 수락할 수 있습니다.
4. Device Sync(디바이스 동기화) 창에서 **Accept(**수락**)**를 클릭하거나 Reconnecting to Device(디바이스에 다시 연결 중) 창에서 **Continue(**계속**)**를 클릭합니다.

CDO는 디바이스를 새 자체 서명 인증서와 자동으로 동기화합니다. 디바이스가 동기화되면 디바이스를 확인하려면 **Devices & Services(**디바이스 및 서비스**)** 페이지를 수동으로 새로 고쳐야 할 수 있습니다.

인증서 오류 코드

반환 코드 확인**: 0 (ok)** 하지만 **CDO**에서 인증서 오류를 반환합니다**.**

CDO에 인증서가 있으면 "https://<device_ip>:<port>"에 GET 호출을 하여 URL에 연결을 시도합니다. 그래도 문제가 해결되지 않으면 CDO에 인증서 오류가 표시됩니다. 인증서가 유효한 경우(openssl에서 0 ok 반환) 연결하려는 포트에서 다른 서비스가 수신 대기하는 문제일 수 있습니다. 다음 명령을 사용할 수 있습니다.

```
curl -k -u <username>:<password> https://<device_id>:<device_port>/admin/exec/show%20version
```

ASA와 통신하고 있는지 확인하고 HTTPS 서버가 ASA의 올바른 포트에서 실행 중인지 확인합니다.

```
 # show asp table socket
Protocol         Socket         State         Local Address             Foreign Address
SSL              00019b98        LISTEN        192.168.1.5:443             0.0.0.0:*
SSL              00029e18        LISTEN        192.168.2.5:443             0.0.0.0:*
TCP              00032208        LISTEN        192.168.1.5:22              0.0.0.0:*
```

반환 코드 확인**: 9(**인증서가 아직 유효하지 않음**)**

이 오류는 제공된 인증서의 발급 날짜가 미래이므로 클라이언트가 이를 유효한 것으로 처리하지 않음을 의미합니다. 이는 잘못 구성된 인증서로 인해 발생할 수 있으며, 자체 서명 인증서의 경우 인증서를 생성할 때 잘못된 디바이스 시간이 원인일 수 있습니다.

인증서의 notBefore 날짜를 포함하는 오류에 줄이 표시되어야 합니다.

```
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=9:certificate is not yet valid
notBefore=Oct 21 19:43:15 2016 GMT
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
notBefore=Oct 21 19:43:15 2016 GMT
```

이 오류를 통해 인증서가 유효한 시점을 확인할 수 있습니다.

치료

인증서의 notBefore 날짜는 과거여야 합니다. 이전 날짜의 인증서를 재발급할 수 있습니다. 이 문제는 클라이언트 또는 발급 디바이스에서 시간이 올바르게 설정되지 않은 경우에도 발생할 수 있습니다.

반환 코드 확인**: 10(**인증서가 만료되었습니다**)**

이 오류는 제공된 인증서 중 하나 이상이 만료되었음을 의미합니다. 인증서의 notBefore 날짜를 포함하는 오류에 줄이 표시되어야 합니다.

```
error 10 at 0 depth lookup:certificate has expired
```

만료 날짜는 인증서 본문에 있습니다.

치료

인증서가 실제로 만료된 경우 유일한 교정 방법은 다른 인증서를 가져오는 것입니다. 인증서의 만료 날짜가 아직 미래이지만 openssl이 만료되었다고 주장하는 경우, 컴퓨터의 시간과 날짜를 확인합니다. 예를 들어 인증서가 2020년에 만료되도록 설정되어 있지만 컴퓨터의 날짜가 2021년이면 컴퓨터는 해당 인증서를 만료된 것으로 처리합니다.

반환 코드 확인**: 21(**첫 번째 인증서를 확인할 수 없음**)**

이 오류는 인증서 체인에 문제가 있음을 나타내며, openssl은 디바이스에서 제공하는 인증서를 신뢰할 수 있는지 확인할 수 없습니다. 인증서 체인이 작동하는 방식을 확인하려면 위의 예에서 인증서 체인을 살펴보겠습니다.

```
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
i:/C=US/O=Google Inc/CN=Google Internet Authority G2

-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA

-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority

-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE----- ---
```

인증서 체인은 서버에서 제공하는 인증서 목록으로, 서버의 자체 인증서부터 시작하여 점점 더 높은 수준의 중간 인증서를 포함하여 서버의 인증서를 인증 기관의 최상위 인증서와 연결합니다. 각 인증서에는 해당 주체(':'로 시작하는 줄) 및 발급자('i'로 시작하는 줄)가 나열됩니다.

주체는 인증서로 식별되는 엔티티입니다. 여기에는 조직 이름이 포함되며 경우에 따라 인증서가 발급된 엔티티의 공용 이름이 포함됩니다.

발급자는 인증서를 발급한 엔티티입니다. 여기에는 Organization(조직) 필드도 포함되며, 경우에 따라 Common Name(일반 이름)도 포함됩니다.

서버에 신뢰할 수 있는 인증 기관에서 직접 발급한 인증서가 있는 경우 인증서 체인에 다른 인증서를 포함할 필요가 없습니다. 다음과 같은 인증서를 제공합니다.

```
--- Certificate chain 0 s:/C=US/ST=California/L=Anytown/O=ExampleCo/CN=*.example.com
i:/C=US/O=Trusted Authority/CN=Trusted Authority
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE----- ---
```

이 인증서가 제공되면 openssl은 ***.example.com**에 대한 ExampleCo 인증서가 신뢰할 수 있는 기관 인증서에 의해 올바르게 서명되었는지 확인합니다. 이 인증서는 openssl의 기본 제공 신뢰 저장소에 있습니다. 확인 후 openssl이 디바이스에 성공적으로 연결됩니다.

그러나 대부분의 서버에는 신뢰할 수 있는 CA에서 직접 서명한 인증서가 없습니다. 대신 첫 번째 예에서와 같이 서버의 인증서가 하나 이상의 중간 인증서에 의해 서명되고, 최상위 중간 인증서에는 신뢰할 수 있는 CA가 서명한 인증서가 있습니다. OpenSSL은 기본적으로 이러한 중간 CA를 신뢰하지 않으며, 신뢰할 수 있는 CA로 끝나는 완전한 인증서 체인이 제공되는 경우에만 이를 확인할 수 있습니다.

중간 기관이 인증서에 서명한 서버는 모든 중간 인증서를 포함하여 이를 신뢰할 수 있는 CA에 연결하는 모든 인증서를 제공해야 합니다. 이 전체 체인을 제공하지 않는 경우 openssl의 출력은 다음과 같습니다.

```
depth=0 OU = Example Unit, CN = example.com
verify error:num=20:unable to get local issuer certificate
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=27:certificate not trusted
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=21:unable to verify the first certificate
verify return:1

CONNECTED(00000003)

---
Certificate chain
0 s:/OU=Example Unit/CN=example.com
i:/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
-----BEGIN CERTIFICATE-----
...lots of b64...
-----END CERTIFICATE-----
---
Server certificate
subject=/OU=Example Unit/CN=example.com
issuer=/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
---
No client certificate CA names sent
---
SSL handshake has read 1509 bytes and written 573 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: 24B45B2D5492A6C5D2D5AC470E42896F9D2DDDD54EF6E3363B7FDA28AB32414B
Session-ID-ctx:
Master-Key:
21BAF9D2E1525A5B935BF107DA3CAF691C1E499286CBEA987F64AE5F603AAF8E65999BD21B06B116FE9968FB7C62EF7C
```

```
Key-Arg : None
Krb5 Principal: None
PSK identity: None
PSK identity hint: None
Start Time: 1476711760
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

이 출력은 서버가 하나의 인증서만 제공했으며 제공된 인증서가 신뢰할 수 있는 루트가 아닌 중간 기관에 의해 서명되었음을 보여줍니다. 출력에는 특성 확인 오류도 표시됩니다.

치료

이 문제는 디바이스에서 제공하는 인증서가 잘못 구성되어 발생합니다. CDO 또는 다른 프로그램이 디바이스에 안전하게 연결할 수 있도록 이 문제를 해결하는 유일한 방법은 올바른 인증서 체인을 디바이스에 로드하여 연결하는 클라이언트에 완전한 인증서 체인을 제공하도록 하는 것입니다.

트러스트 포인트에 중간 CA를 포함하려면 아래 링크 중 하나를 따르십시오(CSR이 ASA에서 생성되었는지 여부에 따라).

- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc13
- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc15

## 새 인증서 탐지됨

자체 서명 인증서가 있는 디바이스를 업그레이드하고 업그레이드 프로세스 후에 새 인증서가 생성되는 경우 CDO는 **Configuration Status(**구성 상태**)** 및 **Connectivity(**연결성**)** 상태로 "New Certificate Detected(새 인증서 탐지됨)" 메시지를 생성할 수 있습니다. CDO에서 계속 관리하려면 이 문제를 수동으로 확인하고 해결해야 합니다. 인증서가 동기화되고 디바이스가 정상 상태가 되면 디바이스를 관리할 수 있습니다.

참고 두 개 이상의 관리 디바이스를 CDO에 동시에 CDO에 디바이스 대량 다시 연결하는 경우, CDO는 디바이스에서 새 인증서를 자동으로 검토 및 수락하고 계속해서 다시 연결합니다.

다음 절차를 사용하여 새 인증서를 확인합니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 필터를 사용하여 **New Certificate Detected(**새 인증서 탐지됨**)** 연결 또는 구성 상태의 디바이스를 표시하고 원하는 디바이스를 선택합니다.

단계 **5** Action(작업) 창에서 **Review Certificate(**인증서 검토**)**를 클릭합니다. CDO에서는 검토를 위해 인증서를 다운로드하고 새 인증서를 수락할 수 있습니다.

단계 **6** Device Sync(디바이스 동기화) 창에서 **Accept(**수락**)**를 클릭하거나 Reconnecting to Device(디바이스에 다시 연결 중) 창에서 **Continue(**계속**)**를 클릭합니다.

CDO는 디바이스를 새 자체 서명 인증서와 자동으로 동기화합니다. 디바이스가 동기화되면 디바이스를 확인하려면 **Devices & Services(**디바이스 및 서비스**)** 페이지를 수동으로 새로 고쳐야 할 수 있습니다.

# 온보딩 오류 문제 해결

디바이스 온보딩 오류는 여러 가지 이유로 발생할 수 있습니다.

다음과 같은 작업을 수행할 수 있습니다.

단계 **1** **Inventory(**인벤토리**)** 페이지에서 **Devices(**장치 **)** 탭을 클릭합니다.

단계 **2** 적절한 디바이스 유형 탭을 클릭하고 이 오류가 발생하는 디바이스를 선택합니다. 경우에 따라 오른쪽에 오류 설명이 표시됩니다. 설명에 언급된 필요한 조치를 취하십시오.

또는

단계 **3** CDO에서 디바이스 인스턴스를 제거하고 디바이스 온보딩을 다시 시도하십시오.

# "충돌 탐지됨" 상태 해결

CDO를 사용하면 각 라이브 디바이스에서 충돌 탐지를 활성화하거나 비활성화할 수 있습니다. 충돌 탐지, on page 363이 활성화되어 있고 CDO를 사용하지 않고 디바이스의 구성을 변경한 경우, 디바이스의 구성 상태는 **Conflict Detected(**충돌 탐지됨**)**로 표시됩니다.

"충돌 탐지됨" 상태를 해결하려면 다음 절차를 수행합니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 충돌을 보고하는 디바이스를 선택하고 오른쪽의 세부 정보 창에서 **Review Conflict(**충돌 검토**)**를 클릭합니다.

단계 **5** **Device Sync(**디바이스 동기화**)** 페이지에서 강조 표시된 차이점을 검토하여 두 구성을 비교합니다.

- "Last Known Device Configuration(마지막으로 알려진 디바이스 구성)" 패널은 CDO에 저장된 디바이스 구성입니다.
- "Found on Device(디바이스에서 발견됨)" 패널은 ASA에서 실행 중인 구성에 저장된 구성입니다.

단계 **6** 다음 중 하나를 선택하여 충돌을 해결합니다.

- **Accept Device changes(**디바이스 변경 사항 수락**)**: 구성 및 **CDO**에 저장된 보류 중인 변경 사항을 디바이스의 실행 중인 구성으로 덮어씁니다.

  **Note** CDO는 명령줄 인터페이스 외부에서 Cisco IOS 디바이스에 변경 사항을 배포하는 것을 지원하지 않으므로, 충돌을 해결할 때 Cisco IOS 디바이스에 대한 유일한 선택은 **Accept Without Review(**검토 없이 수락**)**를 선택하는 것입니다.

- **Reject Device Changes(**디바이스 변경 거부**)**: 디바이스에 저장된 구성을 CDO에 저장된 구성으로 덮어씁니다.

**Note** 거부되거나 수락된 모든 구성 변경 사항은 변경 로그에 기록됩니다.

## "동기화되지 않음" 상태 해결

다음 절차를 사용하여 구성 상태가 "동기화되지 않음"인 디바이스를 확인합니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 동기화되지 않은 것으로 보고된 디바이스를 선택합니다.

단계 **5** 오른쪽의 동기화되지 않음 패널에서 다음 중 하나를 선택합니다.

- 미리보기 및 배포**...** - CDO에서 디바이스로 구성 변경 사항을 푸시하려면 지금 수행한 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 한 번에 여러 변경 사항을 기다렸다가 배포하십시오.
- 변경 사항 취소 - CDO에서 디바이스로 구성 변경을 푸시하지 않으려는 경우, 또는 CDO에서 시작한 구성 변경을 "취소"하려는 경우. 이 옵션은 CDO에 저장된 구성을 디바이스에 저장된 실행 중인 구성으로 덮어씁니다.

# SecureX 문제 해결

SecureX와 함께 CDO를 사용하려고 시도하는 동안 오류, 경고 및 문제가 발생할 수 있습니다. SecureX UI에 표시되는 문제의 경우 SecureX 설명서를 사용해야 합니다. 자세한 내용은 SecureX 지원을 참조하십시오.

CDO 내의 SecureX 리본 기능 또는 SecureX 리본에 대한 테넌트 액세스 가능성에 대한 사례를 열려면 Cisco Defense Orchestrator 지원팀에 문의에서 자세한 내용을 참조하십시오. 테넌트 ID를 제공하라는 요청을 받을 수 있습니다.

### SecureX UI 문제 해결

**SecureX** 대시보드에 중복된 **CDO** 모듈이 표시됩니다**.**

SecureX에서 단일 제품의 여러 모듈을 수동으로 구성할 수 있습니다. 예를 들어 여러 CDO 테넌트가 있는 경우 테넌트당 하나의 CDO 모듈을 생성할 수 있습니다. 중복 모듈은 동일한 CDO 테넌트에서 두 개의 개별 API 토큰이 있음을 의미합니다. 이러한 중복은 혼란을 야기하고 대시보드를 복잡하게 만들 수 있습니다.

SecureX에서 CDO 모듈을 수동으로 구성한 다음 CDO의 일반 설정 페이지에서 **SecureX** 연결을 선택한 경우 이로 인해 하나의 테넌트가 SecureX에 여러 모듈을 가질 수 있습니다.

이 문제를 해결하려면 SecureX에서 원래 CDO 모듈을 제거하고 중복 모듈로 CDO 성능을 계속 모니터링하는 것이 좋습니다. 이 모듈은 더 안전하고 SecureX 리본과 호환되는 더 강력한 API 토큰으로 생성됩니다.

### CDO UI 문제 해결

SecureX 내의 CDO 모듈에 대한 사례를 열려면 SecureX 약관, 개인 정보 보호, 지원의 지원 섹션에서 자세한 내용을 참조하십시오.

### OAuth 오류

다음 메시지와 함께 oAuth 오류가 발생할 수 있습니다. "사용자가 필요한 모든 범위 또는 충분한 권한을 가지고 있지 않은 것 같습니다." 이 문제가 발생하면 다음 가능성을 고려하십시오.

- 계정이 활성화되지 않았을 수 있습니다. https://visibility.test.iroh.site/에서 등록된 이메일 주소를 사용하여 계정이 활성화되었는지 확인합니다. 계정이 활성화되지 않은 경우 CDO 테넌트가 SecureX와 병합되지 않을 수 있습니다. 이 문제를 해결하려면 Cisco TAC에 문의해야 합니다. 자세한 내용은 Cisco Defense Orchestrator 지원팀에 문의를 참조하십시오.

### 잘못된 조직 자격 증명으로 SecureX에 로그인했습니다.

일반 설정 페이지의 테넌트 설정 섹션에 있는 **Connect SecureX** 옵션을 사용하여 CDO 이벤트를 SecureX로 보내기로 선택했지만 잘못된 자격 증명을 사용하여 SecureX에 로그인한 경우, 잘못된 테넌트의 이벤트가 SecureX 대시보드에 표시될 수 있습니다.

이 문제를 해결하려면 CDO의 일반 설정 페이지에서 **SecureX** 연결 끊기를 클릭합니다. 이렇게 하면 SecureX 조직과 정보를 주고 받는 데 사용되는 읽기 전용 API 사용자가 종료되고 결과적으로 SecureX 대시보드가 종료됩니다.

그런 다음 **Connect Tenant to SecureX**를 다시 활성화하고 SecureX에 로그인하라는 메시지가 표시되면 올바른 조직 로그인 자격 증명을 사용해야 합니다.

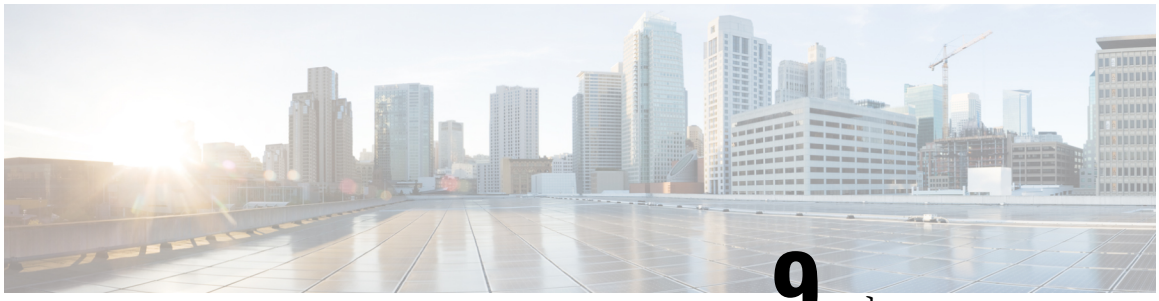
### 잘못된 계정으로 리본에 로그인했습니다.

이때 잘못된 계정 정보로 리본에 로그인하면 리본에서 로그아웃할 수 없습니다. 리본 로그인을 수동으로 재설정하려면 Support Case Manager에서 사례를 열어야 합니다.

### SecureX 리본을 실행할 수 없습니다.

적절한 범위에 대한 액세스 권한이 없을 수 있습니다. 이 문제를 해결하려면 Cisco TAC에 문의해야 합니다. 자세한 내용은 Cisco Defense Orchestrator 지원팀에 문의를 참조하십시오.

SecureX 리본 작동 방식에 대한 자세한 내용은 SecureX 리본 설명서를 참조하십시오.



9 장

# FAQ 및 지원

이 장에는 다음 섹션이 포함되어 있습니다.



## Cisco Defense Orchestrator

**Cisco Defense Orchestrator**란 무엇입니까**?**

Cisco CDO(Defense Orchestrator)는 네트워크 관리자가 다양한 보안 디바이스에서 일관된 보안 정책을 만들고 유지할 수 있도록 하는 클라우드 기반 다중 디바이스 관리자입니다.

CDO를 사용하여 다음 디바이스를 관리할 수 있습니다.

- Cisco Secure Firewall ASA
- Cisco Secure Firewall Threat Defense
- Cisco Secure Firewall Cloud Native
- Cisco Umbrella
- Meraki
- Cisco IOS 디바이스
- 아마존 웹 서비스(AWS) 인스턴스

- SSH 연결을 사용하여 관리되는 디바이스

CDO 관리자는 단일 인터페이스를 통해 이러한 모든 디바이스 유형을 모니터링하고 유지할 수 있습니다.

# Cisco Defense Orchestrator에 디바이스 온보딩 관련 FAQ

## CDO에 Secure Firewall ASA 온보딩 관련 FAQ

**자격 증명을 사용하여 어떻게 ASA를 온보딩합니까?**

ASA를 한 번에 하나씩 온보딩하거나 대량 작업으로 온보딩할 수 있습니다. 고가용성 쌍의 일부인 ASA를 온보딩하는 경우 쌍의 기본 디바이스만 온보딩하는 데 ASA 디바이스 온보딩을 사용합니다. 보안 상황 또는 관리 상황을 온보딩하는 방법은 다른 ASA를 온보딩하는 방법과 동일합니다.

**한 번에 하나 이상의 ASA를 온보딩하려면 어떻게 해야 합니까?**

CSV 파일을 사용하여 ASA 목록을 생성할 수 있으며, CDO는 목록의 모든 ASA를 온보딩합니다. 대량 ASA 온보딩에 대한 지침은 대량 ASA 온보드를 참조하십시오.

**ASA를 온보딩한 후 무엇을 해야 합니까?**

시작하려면 Cisco Defense Orchestrator로 ASA 관리를 참조하십시오.

## CDO에 FDM 매니지드 디바이스 온보딩 관련 FAQ

**FDM 매니지드 디바이스를 온보딩하려면 어떻게 해야 합니까?**

FDM 매니지드 디바이스를 온보딩하는 다양한 방법이 있습니다. 등록 키 방법을 사용하는 것이 좋습니다. 시작하려면 FDM 매니지드 디바이스 온보딩을 참조하십시오.

## 클라우드사용Firewall Management Center에 Secure Firewall Threat Defense 온보딩 관련 FAQ

**Secure Firewall Threat Defense를 온보딩하려면 어떻게 합니까?**

CLI 등록 키, 로우 터치 프로비저닝 또는 일련 번호를 사용하여 FTD 디바이스를 온보딩할 수 있습니다.

**Secure Firewall Threat Defense를 온보딩한 후에는 어떻게 해야 합니까?**

디바이스가 동기화되면 Tools & Services(툴 및 서비스) - Firewall Management Center로 이동하여 Actions(작업), Management(관리) 또는 Settings(설정) 창에서 작업을 선택하여 클라우드 제공 Firewall

Management Center에서 위협 방어 디바이스의 구성을 시작합니다. 시작하려면 클라우드 사용 Firewall Management Center 애플리케이션 페이지를 참조하십시오.

**Secure Firewall Threat Defense** 문제를 어떻게 해결합니까**?**

Secure Firewall Threat Defense 온보딩 문제 해결을 참조하십시오.

# 온프레미스 Secure Firewall Management Center 관련 FAQ

온프레미스 **Management Center**를 온보딩하려면 어떻게 합니까**?**

온프레미스 Management Center를 CDO에 온보딩할 수 있습니다. 온프레미스 Management Center를 온보딩하면 온프레미스 Management Center에 등록된 모든 디바이스도 온보딩됩니다. CDO는 온프레미스 Management Center 또는 온프레미스 Management Center에 등록된 디바이스와 연결된 개체 또는 정책의 생성이나 수정을 지원하지 않습니다. 온프레미스 Management Center UI에서 이러한 변경을 수행해야 합니다. 시작하려면 온프레미스 Management Center 온보딩을 참조하십시오.

# CDO에 Meraki 디바이스 온보딩 관련 FAQ

**Meraki** 디바이스를 온보딩하려면 어떻게 해야 합니까**?**

MX 디바이스는 CDO와 Meraki 대시보드에서 모두 관리할 수 있습니다. CDO는 구성 변경 사항을 Meraki 대시보드에 구축하며, 그러면 구성이 디바이스에 안전하게 구축됩니다. 시작하려면 Meraki MX 디바이스 온보딩을 참조하십시오.

# CDO에 SSH 디바이스 온보딩 관련 FAQ

**SSH** 디바이스를 어떻게 온보딩합니까**?**

SSH 디바이스에 저장된 높은 권한을 가진 사용자의 사용자 이름과 암호를 사용하여 SDC(보안 디바이스 커넥터)로 디바이스를 온보딩할 수 있습니다. 시작하려면 SSH 디바이스 온보딩을 참조하십시오.

디바이스를 삭제하려면 어떻게 합니까**?**

재고 목록 페이지에서 디바이스를 삭제할 수 있습니다.

# CDO에 IOS 디바이스 온보딩 관련 FAQ

**Cisco IOS** 디바이스를 어떻게 온보딩합니까**?**

SDC(보안 디바이스 커넥터)를 사용하여 Cisco IOS(Internetwork Operating System)를 실행하는 라이브 Cisco 디바이스를 온보딩할 수 있습니다. 시작하려면 Cisco IOS 디바이스 온보딩을 참조하십시오.

디바이스를 삭제하려면 어떻게 합니까?

Inventory(재고 목록) 페이지에서 디바이스를 삭제할 수 있습니다.

# 디바이스 유형

**ASA(Adaptive Security Appliance)**란 무엇입니까?

Cisco ASA에서는 고급 스테이트풀 방화벽 및 VPN 집선 디바이스 기능을 하나의 디바이스에서 제공하며 애드온 모듈과 통합된 서비스를 제공합니다. ASA에는 다중 보안 상황(가상 방화벽과 유사), 클러스터링(다중 방화벽을 단일 방화벽으로 통합), 투명(Layer 2) 방화벽 또는 라우팅(Layer 3) 방화벽 가동, 고급 검사 엔진, IPsec VPN, SSL VPN 및 클라이언트리스 SSL VPN 지원 등의 다양한 기능이 포함되어 있습니다. ASA는 가상 머신 또는 지원되는 하드웨어에 설치할 수 있습니다.

**ASA** 모델이란 무엇입니까?

ASA 모델은 CDO에 온보딩한 ASA 디바이스의 실행 중인 구성 파일의 사본입니다. ASA 모델을 사용하여 디바이스 자체를 온보딩하지 않고도 ASA 디바이스의 구성을 분석할 수 있습니다.

디바이스는 언제 동기화됩니까?

CDO의 구성과 디바이스에 로컬로 저장된 구성이 동일한 경우.

디바이스가 언제 동기화되지 않습니까?

CDO에 저장된 구성이 변경되어 이제 디바이스에 로컬로 저장된 구성과 다른 경우.

디바이스가 충돌 감지 상태인 경우는 언제입니까?

디바이스의 구성이 CDO(대역 외) 외부에서 변경되어 이제 CDO에 저장된 구성과 다른 경우.

**OOB(out-of-band)** 변경이란 무엇입니까?

CDO 외부에서 디바이스가 변경된 경우. CLI 명령을 사용하거나 ASDM 또는 FDM과 같은 온디바이스 관리자를 사용하여 디바이스에서 직접 변경합니다. 대역 외 변경으로 인해 CDO는 디바이스에 대해 "충돌 감지" 상태를 보고합니다.

디바이스에 변경 사항을 배포한다는 것은 무엇을 의미합니까?

디바이스를 CDO에 등록한 후 CDO는 해당 구성의 복사본을 유지 관리합니다. CDO를 변경하면 CDO는 디바이스 구성의 사본을 변경합니다. 변경 사항을 디바이스에 다시 "배포"하면 CDO는 디바이스의 구성 복사본에 대한 변경 사항을 복사합니다. 다음 항목을 참조하십시오.

- 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, on page 352
- CDO에서 ASA로 구성 변경 사항 구축

현재 지원되는 **ASA** 명령은 무엇입니까**?**

모든 명령 디바이스 활동 아래에 **Command Line Interface(**명령줄 인터페이스**)**를 클릭하여 ASA CLI를 사용합니다.

디바이스 관리에 대한 규모 제한이 있습니까**?**

CDO의 클라우드 아키텍처를 통해 수천 개의 디바이스로 확장할 수 있습니다.

**CDO**는 **Cisco Integrated Services Routers** 및 **Aggregation Services Routers**를 관리합니까**?**

CDO를 사용하면 ISR 및 ASR에 대한 모델 디바이스를 생성하고 해당 구성을 가져올 수 있습니다. 그런 다음 가져온 구성을 기반으로 템플릿을 생성하고 일관된 보안을 위해 신규 또는 기존 ISR 및 ASR 디바이스에 배포할 수 있는 표준화된 구성으로 구성을 내보낼 수 있습니다.

**CDO**가 **SMA**를 관리할 수 있습니까**?**

아니오, CDO는 현재 SMA를 관리하지 않습니다.

# 보안

**CDO**는 안전한가요**?**

CDO는 다음 기능을 통해 고객 데이터에 대한 엔드 투 엔드 보안을 제공합니다.

- 새 CDO 테넌트에 대한 초기 로그인, on page 34
- API 및 데이터베이스 작업에 대한 인증 호출
- 이동 중 및 유휴 상태의 데이터 격리
- 역할 분리

CDO는 사용자가 클라우드 포털에 연결할 때 다단계 인증을 요구합니다. 다단계 인증은 고객의 신원을 보호하는 데 필요한 필수 기능입니다.

이동 중이거나 유휴 상태의 모든 데이터는 암호화됩니다. 고객 프레미스 및 CDO의 디바이스와의 통신은 SSL로 암호화되며 모든 고객 테넌트 데이터 볼륨은 암호화됩니다.

CDO의 다중 테넌트 아키텍처는 테넌트 데이터를 격리하고 데이터베이스와 애플리케이션 서버 간의 트래픽을 암호화합니다. 사용자가 CDO에 액세스하기 위해 인증하면 토큰을 받습니다. 이 토큰은 키 관리 서비스에서 키를 가져오는 데 사용되며 키는 데이터베이스에 대한 트래픽을 암호화하는 데 사용됩니다.

CDO는 고객 자격 증명을 보호하면서 신속하게 고객에게 가치를 제공합니다. 이는 자격 증명 데이터가 고객 프레미스를 떠나지 않도록 모든 인바운드 및 아웃바운드 트래픽을 제어하는 클라우드 또는 고객 자체 네트워크(로드맵)에 "보안 데이터 커넥터"를 배포하여 달성됩니다.

**CDO**에 처음 로그인할 때 **"OTP**를 확인할 수 없음**"** 오류가 발생했습니다**.**

데스크톱 또는 모바일 디바이스 시계가 세계 시간 서버와 동기화되어 있는지 확인합니다. 시계가 1분 미만 또는 그 이상 동기화되지 않으면 잘못된 OTP가 생성될 수 있습니다.

디바이스가 **Cisco Defense Orchestrator** 클라우드 플랫폼에 직접 연결되어 있습니까**?**

예. 보안 연결은 디바이스와 CDO 플랫폼 간의 프록시로 사용되는 CDO SDC를 사용하여 수행됩니다. 보안을 최우선으로 고려하여 설계된 CDO 아키텍처를 사용하면, 디바이스를 오가는 데이터를 완전히 분리할 수 있습니다.

공용 **IP** 주소가 없는 디바이스를 어떻게 연결할 수 있습니까**?**

네트워크 내에 배포할 수 있고 외부 포트를 열 필요가 없는 SDC(Secure Device Connector)를 활용할 수 있습니다. SDC가 배포되면 내부(인터넷 라우팅 불가) IP 주소로 디바이스를 온보딩할 수 있습니다.

**SDC**에 추가 비용이나 라이선스가 필요합니까**?**

아니요.

현재 **CDO**에서 어떤 유형의 **VPN(**가상 프라이빗망**)**이 지원됩니까**?**

ASA 고객의 경우, CDO는 IPsec 사이트 투 사이트 VPN 터널 관리만 지원합니다. What's New 페이지의 업데이트를 계속 지켜봐 주십시오.

터널 상태를 어떻게 확인할 수 있습니까**?** 상태 옵션

CDO는 매시간 터널 연결 확인을 자동으로 수행하지만, 터널을 선택하고 연결 확인을 요청하여 임시 VPN 터널 연결 확인을 수행할 수 있습니다. 결과를 처리하는 데 몇 초가 걸릴 수 있습니다.

디바이스 이름과 피어 중 하나의 **IP** 주소를 기반으로 터널을 검색할 수 있습니까**?**

예. 이름과 피어 IP 주소 모두에서 사용 가능한 필터 및 검색 기능을 사용하여 특정 VPN 터널 세부 정보를 검색하고 피벗합니다.

# 문제 해결

**CDO**에서 관리 디바이스로 디바이스 구성을 완전히 배포하는 동안 **"**변경 사항을 디바이스에 배포할 수 없습니다**"**라는 경고가 표시됩니다**.** 해결하려면 어떻게 해야 하나요**?**

전체 구성(CDO 지원 명령 이상으로 수행된 변경 사항)을 디바이스에 배포할 때 오류가 발생하면 "변경 사항 확인"을 클릭하여 디바이스에서 사용 가능한 최신 구성을 가져옵니다. 이렇게 하면 문제가 해결될 수 있으며 계속해서 CDO를 변경하고 배포할 수 있습니다. 문제가 지속되면 **Contact Support(**지원 문의**)** 페이지에서 Cisco TAC에 문의하십시오.

대역 외 문제(CDO 외부에서 수행된 변경, 디바이스에 직접 변경)를 해결하는 동안 CDO에 있는 구성과 디바이스의 구성을 비교하는 동안 CDO는 내가 추가하거나 편집하지 않은 추가 메타데이터를 제공합니다. 왜 그럴까요?

CDO가 기능을 확장함에 따라 더 나은 정책 및 디바이스 관리 분석을 위해 필요한 모든 데이터를 강화하고 유지하기 위해 디바이스 구성에서 추가 정보가 수집됩니다. 이는 관리되는 디바이스에서 발생한 변경 사항이 아니라 이미 존재하는 정보입니다. 충돌 감지 상태를 해결하는 것은 디바이스에서 변경 사항을 확인하고 발생한 변경 사항을 검토하여 쉽게 해결할 수 있습니다.

**CDO**가 내 인증서를 거부하는 이유는 무엇입니까?

새 인증서 문제 트러블슈팅을 참조하십시오.

# 로우 터치(Low-Touch) 프로비저닝에 사용되는 용어 및 정의

- 클레임됨 - CDO에서 일련 번호 온보딩의 컨텍스트에서 사용됩니다. 일련 번호가 CDO 테넌트에 온보딩된 경우 디바이스가 "클레임"됩니다.
- 파킹됨 - CDO에서 일련 번호 온보딩의 컨텍스트에서 사용됩니다. Cisco Cloud에 연결되어 있고 CDO 테넌트가 일련 번호를 요청하지 않은 경우 디바이스는 "파킹"됩니다.
- 초기 프로비저닝 - 초기 FTD 설정의 컨텍스트에서 사용됩니다. 이 단계에서 디바이스는 EULA를 수락하고, 새 비밀번호를 생성하고, 관리 IP 주소를 구성하고, FQDN을 설정하고, DNS 서버를 설정하고, FDM을 사용하여 디바이스를 로컬로 관리하도록 선택합니다.
- 로우 터치(Low-touch) 프로비저닝 - 공장에서 고객 사이트(일반적으로 브랜치 오피스)로 FTD를 배송하고, 사이트의 직원이 FTD를 네트워크에 연결하고, 디바이스가 Cisco Cloud에 연결하는 프로세스입니다. 이 시점에서 일련 번호가 이미 "클레임"되었거나 CDO 테넌트가 클레임할 때까지 FTD가 Cisco Cloud에 "파킹"된 경우 디바이스는 CDO 테넌트에 온보딩됩니다.
- 일련 번호 온보딩 - 이미 구성(설치 및 설정)된 일련 번호를 사용하여 FTD를 온보딩하는 프로세스입니다.

# 정책 최적화

두 개 이상의 액세스 목록(동일한 액세스 그룹 내)이 서로 섀도잉되는 경우를 어떻게 식별할 수 있습니까?

Cisco Defense Orchestrator NPM(네트워크 정책 관리)은 규칙 세트 내에서 상위 규칙이 다른 규칙을 가리고 있는지 식별하고 사용자에게 경고할 수 있습니다. 사용자는 모든 네트워크 정책 사이를 탐색하거나 필터링하여 모든 섀도우 문제를 식별할 수 있습니다.자세한 내용은 ASA 레거시 네트워크 정책를 참조하십시오.

**Note** CDO는 완전히 섀도우 규칙만 지원합니다.

# 연결성

보안 장치 커넥터가 **IP** 주소를 변경했지만 **CDO**에 반영되지 않았습니다**.** 변경 사항을 반영하려면 어떻게 해야 합니까**?**

CDO 내에서 새로운 SDC(Secure Device Connector)를 얻고 업데이트하려면 다음 명령을 사용하여 컨테이너를 다시 시작해야 합니다.

```
 Stop Docker deamon>#service docker stop
Change IP address
Start Docker deamon >#service docker start
Restart container on the SDC virtual appliance >bash-4.2$ ./cdo/toolkit/toolkit.sh restartSDC
 <tenant-name>
```

내 장치**( FTD** 또는 **ASA)**를 관리하기 위해 **CDO**에서 사용하는 **IP** 주소가 변경되면 어떻게 됩니까**?**

정적 IP 주소의 변경이든 DHCP로 인한 IP 주소의 변경이든 어떤 이유로든 장치의 IP 주소가 변경되면, CDO가 장치에 연결하는 데 사용하는 IP 주소를 변경할 수 있습니다( 참조 CDO에서 디바이스의 IP 주소 변경, on page 81). 그런 다음 장치를 다시 연결합니다(참조CDO에 디바이스 대량 다시 연결, on page 86). 장치를 다시 연결할 때 장치의 새 IP 주소를 입력하고 인증 자격 증명을 다시 입력하라는 메시지가 표시됩니다.

내 **ASA**를 **CDO**에 연결하려면 어떤 네트워킹이 필요합니까**?**

- ASDM 이미지가 있고 ASA에 대해 활성화되어 있습니다.
- 52.25.109.29, 52.34.234.2, 52.36.70.147에 대한 공용 인터페이스 액세스
- ASA의 HTTPS 포트는 443 또는 1024 이상의 값으로 설정해야 합니다. 예를 들어 포트 636으로 설정할 수 없습니다.
- 관리 중인 ASA도 AnyConnect VPN 클라이언트 연결을 허용하도록 구성된 경우 ASA HTTPS 포트를 1024 이상의 값으로 변경해야 합니다.

# 데이터 인터페이스 정보

디바이스와의 통신에 전용 관리 인터페이스 또는 일반 데이터 인터페이스를 사용할 수 있습니다. 외부 인터페이스에서 원격으로 FTD를 관리하려는 경우 또는 별도의 관리 네트워크가 없는 경우 데이터 인터페이스의 액세스가 유용합니다.

데이터 인터페이스에서의 FTD 관리 액세스에는 다음과 같은 제한이 있습니다.

- 하나의 물리적 데이터 인터페이스에서만 FMC 액세스를 활성화할 수 있습니다. 하위 인터페이스 또는 EtherChannel은 사용할 수 없습니다.

- 라우팅 인터페이스를 사용하는 라우팅 방화벽 모드 전용입니다.
- PPPoE는 지원되지 않습니다. ISP에 PPPoE가 필요한 경우 FTD와 WAN 모뎀 간에 PPPoE를 지원하는 라우터를 설치해야 합니다.
- 인터페이스는 전역 VRF에만 있어야 합니다.
- SSH는 데이터 인터페이스에 대해 기본적으로 활성화되어 있지 않으므로 나중에 를 사용하여 SSH를 활성화해야 합니다. 관리 인터페이스 게이트웨이가 데이터 인터페이스로 변경되므로, **configure network static-routes** 명령을 사용하여 관리 인터페이스에 대한 고정 경로를 추가하지 않는 한 원격 네트워크에서 관리 인터페이스로 SSH 연결할 수도 없습니다.

# CDO가 개인 정보를 처리하는 방법

Cisco Defense Orchestrator가 개인 식별 정보를 처리하는 방법을 알아보려면 Cisco Defense Orchestrator 프라이버시 데이터 시트를 참조하십시오.

# Cisco Defense Orchestrator 지원팀에 문의

이 장에는 다음 섹션이 포함되어 있습니다.

## 워크플로우 내보내기

지원 티켓을 열기 전에 경험 문제가 있는 디바이스의 워크플로우를 내보내는 것이 좋습니다. 이 추가 정보는 지원 팀이 문제 해결 노력을 신속하게 식별하고 편집하는 데 도움이 될 수 있습니다.

워크플로우를 내보내려면 다음 절차를 따르십시오.

단계 **1** 탐색 모음에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 **3** 적절한 디바이스 유형 탭을 클릭하고 문제 해결이 필요한 디바이스를 선택합니다.

필터 또는 검색 표시줄을 사용하여 문제를 해결해야 하는 디바이스를 찾으십시오. 디바이스를 선택하여 강조 표시합니다.

단계 **4** **Device Actions(**장치 작업**)** 창에서 **Workflows(**워크플로우**)**를 선택합니다.

단계 **5** 이벤트 표 위의 페이지 오른쪽 상단에 있는 **Export(**내보내기**)** 버튼을 클릭합니다. 파일은 자동으 로 로컬에 **.json** 파일로 저장됩니다. TAC로 여는 이메일이나 티켓에 이것을 첨부하십시오.

# TAC를 사용하여 지원 티켓 열기

30일 평가판 또는 라이선스가 부여된 CDO 계정을 사용하는 고객은 Cisco TAC(Technical Assistance Center)에서 지원 티켓을 열 수 있습니다.

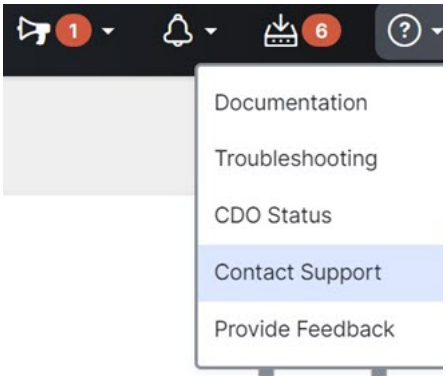
- CDO 고객이 TAC로 지원 티켓을 여는 방법
- CDO 평가판 고객이 TAC를 사용하여 지원 티켓을 여는 방법

## CDO 고객이 TAC로 지원 티켓을 여는 방법

이 섹션에서는 라이선스가 부여된 CDO 테넌트를 사용하는 고객이 Cisco의 TAC(Technical Assistance Center)에서 지원 티켓을 여는 방법을 설명합니다.

단계 1 CDO에 로그인합니다.

단계 2 테넌트 이름 옆에 있는 help(도움말) 버튼을 클릭하고 **Contact Support(**지원 문의**)**를 선택합니다.




단계 3 지원 케이스 관리자를 클릭합니다.

단계 4 파란색 **Open New Case(**새 케이스 열기**)** 버튼을 클릭합니다.

단계 5 **Open a Case(**케이스 열기**)**를 클릭합니다.

단계 6 **Products and Services(**제품 및 서비스**)**를 선택한 다음 **Open Case(**케이스 열기**)**를 클릭합니다.

단계 7 **Request Type(**요청 유형**)**을 선택합니다.

단계 8 **Find Product by Service Agreement(**서비스 계약별 제품 찾기**)** 행을 확장합니다.

단계 9 모든 필드를 입력합니다. 많은 필드가 명확합니다. 다음은 몇 가지 추가 정보입니다.

- **Product Name(**제품 이름**) (PID)** - 이 번호가 더 이상 없는 경우 Cisco Defense Orchestrator 데이터 시트를 참조하십시오.
- **Product Description(**제품 설명**)** - PID에 대한 설명입니다.
- **Site Name(**사이트 이름**)** - 사이트 이름을 입력합니다. 고객 중 한 명의 케이스를 여는 Cisco 파트너인 경우 고객의 이름을 입력합니다.
- **Service Contract(**서비스 계약**)** - 서비스 계약 번호를 입력합니다.

- 중요: 케이스를 Cisco.com 어카운트와 연결하려면 계약 번호를 Cisco.com 프로파일에 연결해야 합니다. 이 절차를 사용하여 계약 번호를 Cisco.com 프로파일에 연결합니다.

  a. Cisco Profile Manager를 엽니다.

  b. **Access Management(**액세스 관리**)** 탭을 클릭합니다.

  c. **Add Access(**액세스 추가**)**를 클릭합니다.

  d. **TAC and RMA case creation, Software Download, support tools, and entitled content on Cisco.com(TAC** 및 **RMA** 케이스 생성**,** 소프트웨어 다운로드**,** 지원 툴**, Cisco.com**의 엔타이틀먼트 콘텐츠**)**를 선택하고 **Go(**이동**)**를 클릭합니다.

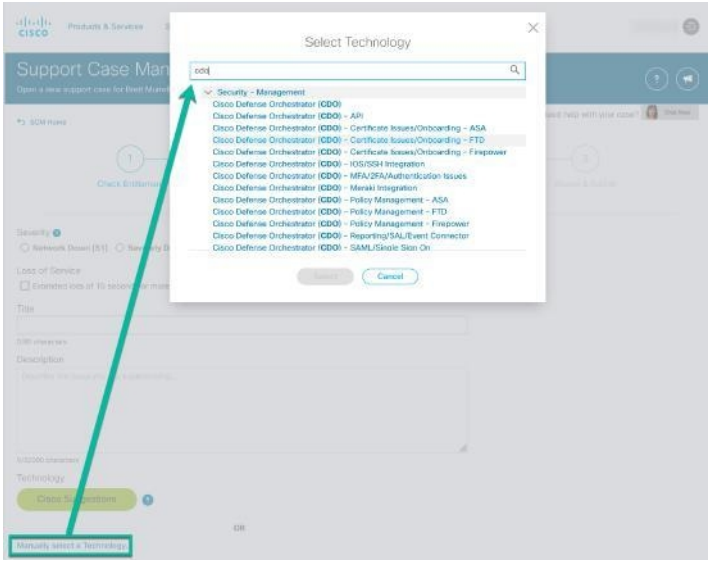
  e. 제공된 공간에 서비스 계약 번호를 입력하고 **Submit(**제출**)**을 클릭합니다. 서비스 계약 연결이 완료되었다는 알림이 이메일로 전송됩니다. 서비스 계약 연결을 완료하는 데 최대 6시간이 걸릴 수 있습니다.

**Important** 중요: 아래 링크에 액세스할 수 없는 경우 공인 Cisco 파트너 또는 리셀러, Cisco 어카운트 담당자 또는 Cisco 서비스 계약 정보를 관리하는 회사 내 담당자에게 문의하십시오.

단계 **10** **Next(**다음**)**를 클릭합니다.

단계 **11** **Describe Problem(**문제 설명**)** 화면에서 아래로 스크롤하여 **Manually select a Technology(**수동으로 기술 선택**)**를 클릭하고 검색 필드에 **CDO**를 입력합니다.

단계 **12** 요청과 가장 일치하는 범주를 선택하고 **Select(**선택**)**를 클릭합니다.



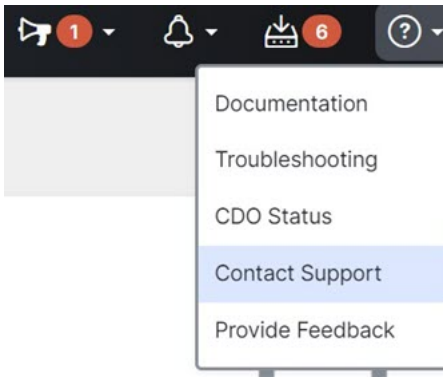

단계 **13** 서비스 요청의 나머지 부분을 완료하고 **Submit(**제출**)**을 클릭합니다.

## CDO 평가판 고객이 TAC를 사용하여 지원 티켓을 여는 방법

이 섹션에서는 CDO 테넌트의 무료 평가판을 사용하는 고객이 Cisco TAC(Technical Assistance Center)에서 지원 티켓을 여는 방법에 대해 설명합니다.

단계 **1** CDO에 로그인합니다.

단계 **2** 테넌트 및 계정 이름 옆에 있는 help(도움말) 버튼을 클릭하고 **Contact Support(**지원 문의**)**를 선택합니다.




단계 **3** 아래에 문제 또는 요청 입력 필드에서 직면한 문제 또는 요청을 지정하고 **Submit(**제출**)**를 클릭합니다.

기술 정보와 함께 귀하의 요청이 지원 팀으로 전송되고 기술 지원 엔지니어가 귀하의 질문에 응답합니다.

# CDO 서비스 상태 페이지

CDO는 CDO 서비스가 작동 중이고 서비스 중단이 있었는지 여부를 보여주는 고객 대면 서비스 상태 페이지를 유지 관리합니다. 일별, 주별 또는 월별 그래프로 가동 시간 정보를 볼 수 있습니다.

CDO의 모든 페이지에 있는 도움말 메뉴에서 **CDO Status(CDO** 상태**)**를 클릭하면 CDO 상태 페이지에 도달할 수 있습니다.

상태 페이지에서 **Subscribe to Updates(**업데이트 구독**)**을 클릭하면 CDO 서비스가 다운될 경우 알림을 받을 수 있습니다.