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 모든 개체를 필터링합니다.
- 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 Orchestrator를 참조하십시오.

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 모든 개체를 필터링합니다.
- 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.

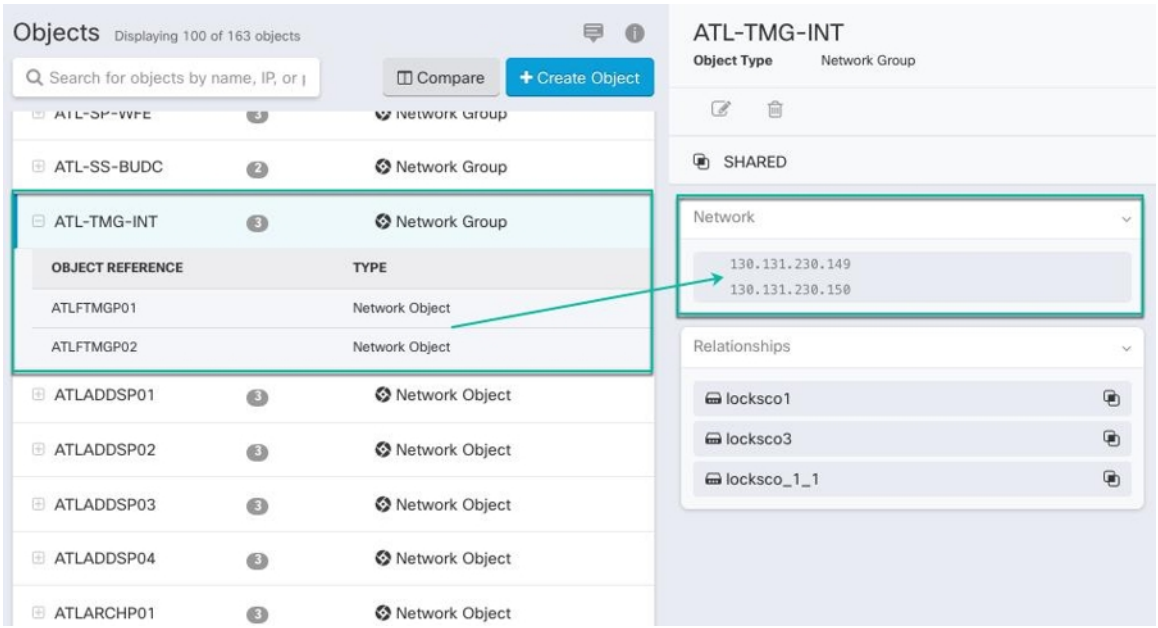
온보딩된 디바이스에서 개체를 생성, 편집 또는 읽는 데 문제가 있는 경우 자세한 내용은 문제 해결 Cisco Defense Orchestrator를 참조하십시오.

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 편집할 수 있으며 변경 사항은 해당 개체를 사용하는 다른 모든 정책에 영향을 미치므로 정책을 쉽게 유지 관리할 수 있습니다. 공유 개체가 없는 경우 동일한 변경이 필요한 모든 정책을 개별적으로 편집해야 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.

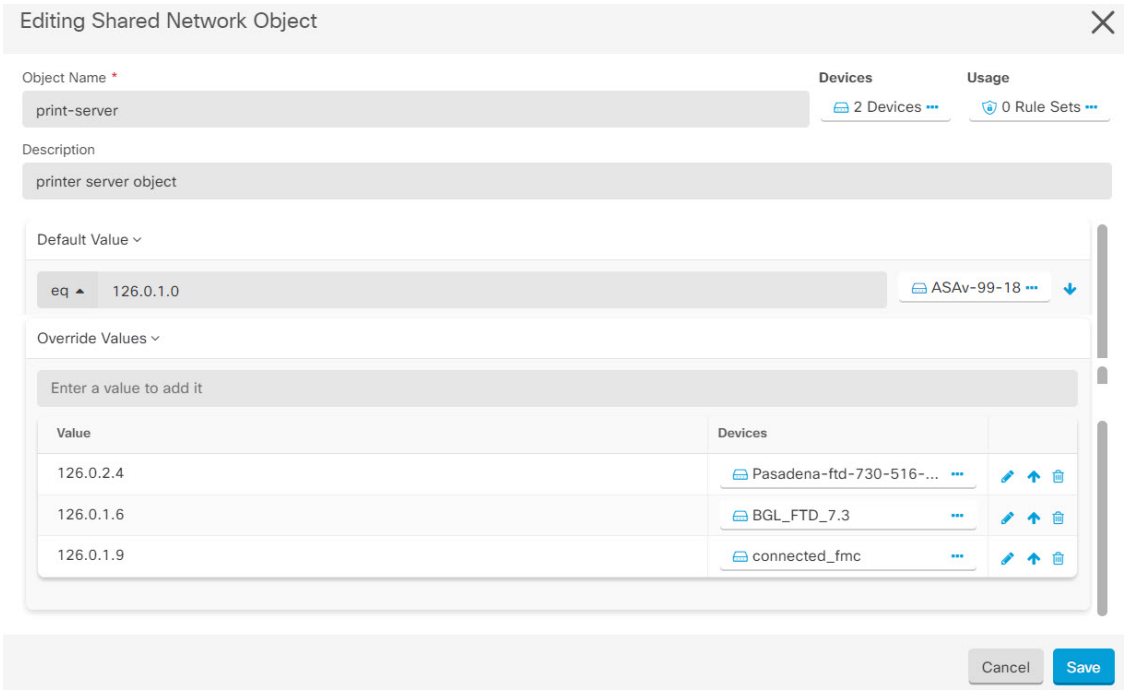


개체 오버라이드

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.



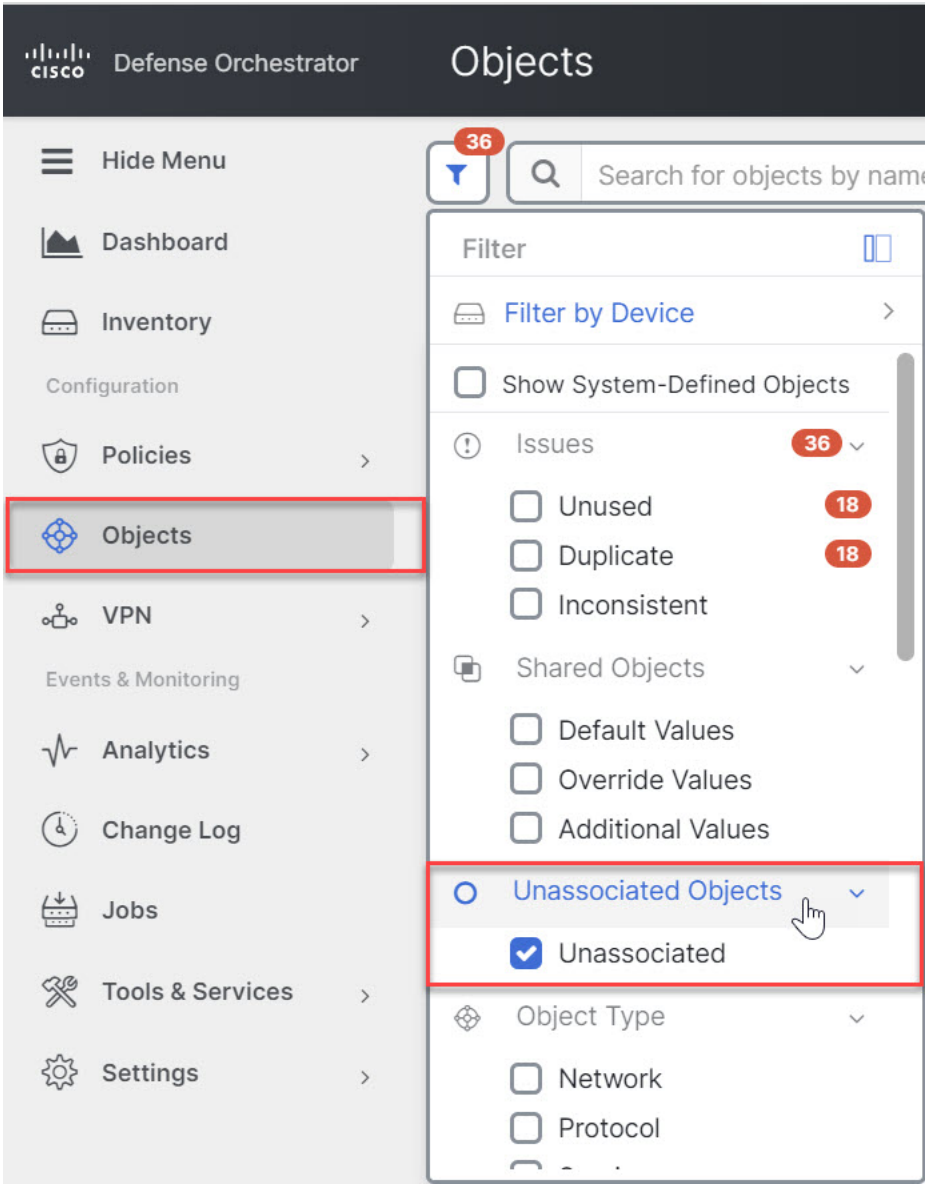
Note 일관되지 않은 개체가 있는 경우 오버라이드를 통해 개체를 단일 공유 개체로 결합할 수 있습니다. 자세한 내용은 불일치 개체 문제 해결를 참조하십시오.

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.

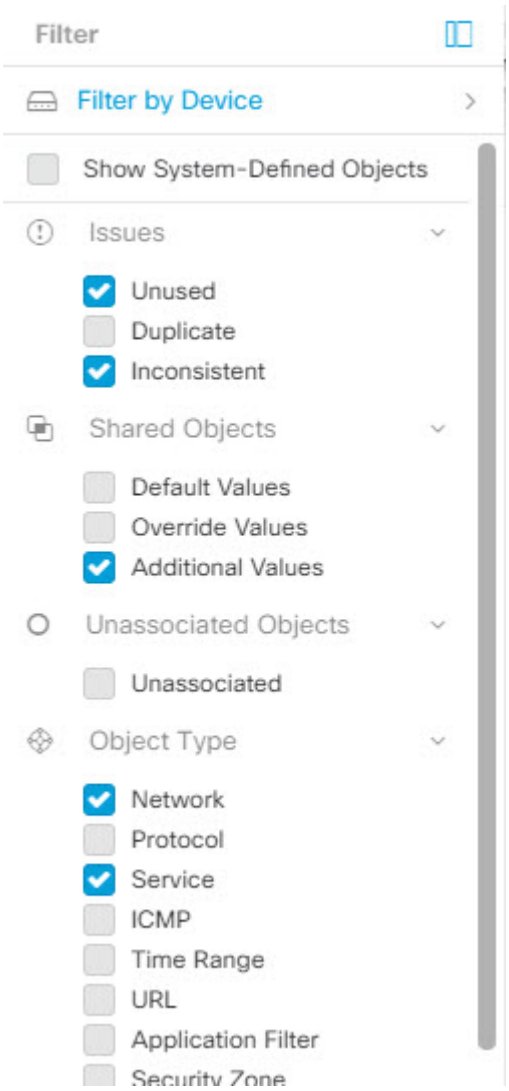
필터링하려면 Devices and Services(디바이스 및 서비스), Policies(정책) 및 Objects(개체) 탭의 왼쪽 창에서 를 클릭합니다.

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. 개체가 사용되지 않거나 중복되거나 일관성이 없더라도 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** 무시된 개체를 필터링하고 검색합니다.

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 배포된 경우:

Objects(개체**) > FTD Network Objects(FTD** 네트워크 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**)** 아이콘 를 클릭합니다.

단계 **5** **OK(**확인**)**을 클릭하여 개체 삭제를 확인합니다.

단계 **6** 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 배포하거나, 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**)** 아이콘 를 클릭합니다.

단계 **4** 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 배포하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

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 서브네트워크의 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 1: 네트워크 개체의 허용되는 값

디바이스 유형	**IPv4 / IPv6**	단일 주소	주소 범위	전체**(Fully Qualified)** 도메인 이름	**CIDR** 표기법의 서브넷
Meraki	IPv4	예	예	예	예

Table 2: 네트워크 그룹의 허용되는 콘텐츠

디바이스 유형	**IP** 값	네트워크 개체	네트워크 그룹
Meraki	예	예	예

제품 간 네트워크 개체 재사용

클라우드 사용 Firewall Management Center가 있는 Cisco Defense Orchestrator tenant 를 보유하고 있는 경우

Secure Firewall Threat Defense, FDM 관리 위협 방어, ASA, or Meraki 네트워크 개체 또는 그룹을 생성하면, 클라우드 사용 Firewall Management Center를 구성할 때 사용되는 **Objects > Other FTD Objects(**개체 > 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 > Other FTD Objects(**개체 > 기타 **FTD** 개체**)** 페이지에서 복제되지 않습니다.
- 온프레미스 Secure Firewall Management Center에서 관리하는 온보딩 위협 방어 디바이스의 네트워크 개체 및 그룹은 **Objects > Other FTD Objects(**개체 > 기타 **FTD** 개체**)** 페이지에 복제되지 않으며 클라우드 사용 Firewall Management Center에서 사용할 수 없습니다.

클라우드 사용 Firewall Management Center로 마이그레이션된 온프레미스 Secure Firewall 관리 센터 인스턴스의 경우, 네트워크 개체 및 그룹이 FTD 디바이스에 배포된 정책에서 사용되는 경우 CDO 개체 페이지에 복제됩니다.

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 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.

Meraki 디바이스와 연결된 개체

Meraki 디바이스에 사용되는 개체 정보

Meraki 대시보드는 아웃바운드 액세스 제어 규칙의 소스 및 대상 필드에서 IP 주소, 프로토콜 또는 포트 범위의 그룹을 활용합니다. 온보딩되면 CDO는 IP 주소를 네트워크 개체로, 애플리케이션 레이어 프로토콜 값을 서비스 개체 또는 프로토콜 개체로 변환합니다.

CDO의 단일 규칙이 대시보드에서 여러 규칙으로 변환될 수 있습니다. 예를 들어 TCP 및 UDP 프로토콜을 모두 포함하는 ASA 프로토콜 그룹을 CDO의 단일 액세스 제어 규칙에 추가하는 경우, CDO는 하나의 CDO 규칙을 대시보드에서 여러 규칙으로 변환합니다. 하나의 규칙은 TCP 프로토콜을 포함하고 하나의 규칙은 UDP 프로토콜을 포함합니다.

Meraki 대시보드와 CDO는 모두 CIDR 서브넷 표기법을 지원합니다. 레이어 3 스위치 인터페이스 및 MX 디바이스 레이아웃에 대한 자세한 내용은 Meraki 기술 자료를 참조하십시오.

CDO에서 Meraki 디바이스와 함께 사용할 수 있는 개체는 무엇입니까?

CDO(Cisco Defense Orchestrator)에는 MX 디바이스 전용인 개체가 없습니다. 대신 FTD, FDM 및 ASA 개체를 생성하거나 공유하고 디바이스에 배포된 규칙에서 이러한 개체를 연결할 수 있습니다. Meraki는 FTD 및 ASA 개체와 완전히 호환되지 않으므로 MX 디바이스에서 개체를 사용하는 방법에 영향을 미치는 몇 가지 제한 사항이 있을 수 있습니다.

참고로 FTD, FDM 및 ASA 개체를 MX 디바이스와 연결하면 해당 개체가 공유됩니다. 해당 개체를 변경하면 해당 개체가 공유되는 모든 디바이스에 영향을 미치며 디바이스의 구성 상태가 *Not Synced(*동기화되지 않음*)*로 표시됩니다. 자세한 내용은 공유 개체를 참조하십시오. 개체에 영향을 미칠 수 있는 추가 개체 상태는 이 페이지의 하단에 있는 관련 문서 섹션을 참조하십시오.

Meraki는 IPv6 주소 또는 FQDN을 포함하는 개체를 지원하지 않습니다.

CDO의 개체	Meraki와 호환
프로토콜 개체	TCP, UDP, ICMP
네트워크 개체	예
네트워크 그룹	예
서비스 개체	예
ASA 서비스 그룹	아니요
FTD 서비스 그룹	아니요

Meraki 클라우드의 로컬 네트워크 개체 및 개체 그룹

네트워크 개체 및 개체 그룹을 사용하면 Meraki 디바이스에 대한 방화벽 규칙을 더 쉽게 관리할 수 있습니다. 이는 방화벽 규칙과 같은 액세스 정책에 사용할 수 있는 IP 서브넷 및 FQDN에 대한 레이블 역할을 합니다. 동일한 IP 서브넷 또는 FQDN을 사용하는 여러 액세스 정책을 편집해야 하는 경우 모든 정책에 반영되도록 네트워크 개체만 편집하면 됩니다. 이때 Meraki 대시보드를 사용하여 이러한 개체를 생성하고 편집해야 합니다. 이러한 개체가 사용자 환경에서 수행할 수 있는 작업에 대한 자세한 내용은 Meraki의 네트워크 개체 하이라이트를 참조하십시오.

Note Meraki 네트워크 개체 또는 네트워크 개체 그룹을 참조하는 디바이스 구성이 CDO UI에 온보딩되거나 동기화되면 이러한 개체는 **FTD** 네트워크 개체로 표시됩니다.

이러한 개체 및 개체 그룹은 CDO에서 읽기 전용입니다.

CDO에서 Meraki 규칙의 모양

디바이스의 정책 페이지에서 개체를 보거나 디바이스를 기준으로 개체 페이지를 필터링할 수 있습니다. 정책 페이지에서 액세스 제어 규칙을 보고, 편집하고, 순서를 바꿀 수 있습니다. CDO는 Meraki 대시보드의 아웃바운드 규칙을 개체가 포함된 액세스 제어 규칙으로 변환하므로 Meraki 대시보드의 규칙 및 프로토콜은 다르게 보일 수 있습니다. 다음 표에서는 디바이스가 CDO에 온보딩된 경우의 새 프로토콜 이름을 다룹니다.

Meraki 대시보드의 규칙 또는 프로토콜 헤더	CDO의 규칙 또는 개체 헤더
정책	작업
Source IP	네트워크 개체 또는 네트워크 그룹
목적지 IP	네트워크 개체 또는 네트워크 그룹
소스 포트	네트워크 개체 또는 네트워크 그룹
대상 포트	네트워크 개체 또는 네트워크 그룹

Meraki 대시보드의 규칙 또는 프로토콜 헤더	**CDO**의 규칙 또는 개체 헤더
레이어 3 애플리케이션 프로토콜	포트(프로토콜 그룹, 포트 그룹 또는 서비스 개체)

다음은 Meraki 대시보드의 아웃바운드 규칙이 CDO에 표시되는 내용의 예입니다.

로컬 **Meraki** 네트워크 개체 생성

Merkai 대시보드에서 로컬 Meraki 네트워크 개체를 만들어야 합니다. 아직 CDO에 온보딩되지 않은 Meraki 디바이스가 있는 경우 기존 로컬 개체가 디바이스에 온보딩됩니다. 온보딩된 Meraki 디바이스가 있는 경우 CDO에서 디바이스를 동기화하여 새 구성 및 로컬 개체를 읽습니다.

참고 Meraki 네트워크 개체 또는 네트워크 개체 그룹을 참조하는 디바이스 구성이 CDO UI에 온보딩되거나 동기화되면 이러한 개체는 **FTD** 네트워크 개체 또는 개체 그룹으로 표시됩니다.

이러한 개체 및 개체 그룹은 CDO에서 읽기 전용입니다.

시작하기 전에

Merkai의 오픈 베타 네트워크 개체를 활성화하지 않은 경우, Meraki 대시보드에 로그인하고 조직 > 정책 개체로 이동하여 등록하고 로컬 개체 및 개체 그룹에 대한 액세스 권한을 얻으십시오.

단계 **1** Meraki 대시보드에 로그인하고 로컬 개체 또는 로컬 개체 그룹을 생성합니다. 자세한 내용은 Meraki 네트워크 개체 구성 가이드를 참조하십시오.

단계 **2** CDO에 로그인합니다.

참고: 아직 Meraki 디바이스를 CDO에 온보딩하지 않은 경우 자세한 내용은 CDO에 MX 디바이스 온보딩를 참조하십시오. 디바이스를 온보딩하면 기존 개체도 모두 온보딩됩니다.

단계 **3** 탐색창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **4** Merkai 디바이스를 찾아 디바이스 행이 강조 표시되도록 선택합니다. 디바이스 상태는 충돌 감지됨입니다. 오른쪽에 있는 창에서 **Review Conflict(**충돌 검토**)**를 선택하여 디바이스 구성에 대한 변경 사항을 검토하거나 **Accept without Review(**검토 없이 수락**)**을 선택하여 모든 구성 변경 사항을 수락합니다.

Meraki 네트워크 개체 또는 네트워크 그룹 생성 또는 편집

MX 디바이스는 Firepower 및 ASA 네트워크 개체와 동일한 형식을 사용하며 CIDR 표기법으로 표현된 호스트 이름, IP 주소 또는 서브넷 주소를 포함할 수 있습니다. 네트워크 그룹은 네트워크 개체 및

그룹에 추가하는 기타 개별 주소 또는 서브넷의 모음입니다. 네트워크 개체 및 네트워크 그룹은 액세스 규칙에 사용됩니다. CDO를 사용하여 네트워크 개체 및 네트워크 그룹을 생성, 읽기, 업데이트 및 삭제할 수 있습니다.

네트워크 개체에 추가할 수 있는 **IP** 주소

디바이스 유형	**IPv4 / IPv6**	단일 주소	주소 범위	전체**(Fully Qualified)** 도메인 이름	**CIDR** 표기법의 서브넷
MX	IPv4	예	예	아니요	예

Note 클라우드 사용 Firewall Management Center가 테넌트에 배포된 경우:

Objects(개체**) > FTD Network Objects(FTD** 네트워크 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 배포된 경우:

Objects(개체**) > FTD Network Objects(FTD** 네트워크 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.

Meraki 네트워크 개체 생성

Note 클라우드 사용 Firewall Management Center가 테넌트에 배포된 경우:

Objects(개체**) > FTD Network Objects(FTD** 네트워크 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 탐색 모음에서 **Objects(**개체**) > Meraki Objects(Meraki** 개체**)**를 클릭합니다.

단계 **2** + 를 클릭하고, **FTD** > 네트워크 또는 **ASA** > 네트워크를 클릭합니다.

단계 **3** 개체 이름을 입력합니다.

단계 **4** **Create a network object(**네트워크 개체 생성**)**를 선택합니다.

단계 **5** 값 섹션에서 단일 IP 주소 또는 CIDR 표기법으로 표현된 서브넷 주소를 입력합니다.

단계 **6** **Add(**추가**)**를 클릭합니다.

단계 **7** 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 배포하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

Meraki 네트워크 그룹 생성

네트워크 그룹은 여러 네트워크 개체 또는 IP 주소로 구성됩니다.

네트워크 그룹을 네트워크 개체로 구성하려면 위의 "네트워크 개체 생성" 절차를 사용하여 IP 주소에 대한 개별 네트워크 개체를 생성합니다.

Note 클라우드 사용 Firewall Management Center가 테넌트에 배포된 경우:

Objects(개체**) > FTD Network Objects(FTD** 네트워크 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 탐색 모음에서 **Objects(**개체**) > Meraki Objects(Meraki** 개체**)**를 클릭합니다.

단계 **2**  를 클릭하고, **FTD** > 네트워크 또는 **ASA** > 네트워크를 클릭합니다.

단계 **3** 개체 이름을 입력합니다.

단계 **4** **Create a network group(**네트워크 그룹 생성**)**을 선택합니다.

단계 **5** **Add Object(**개체 추가**)**를 클릭하고 목록에서 네트워크 개체를 선택한 다음 **Select(**선택**)**를 클릭합니다. 원하는 모든 네트워크 개체를 추가할 때까지 이 작업을 계속합니다.

단계 **6** **Add(**추가**)**를 클릭합니다.

단계 **7** 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 배포하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

Firepower 네트워크 개체 또는 네트워크 그룹 편집

Caution 클라우드 사용 Firewall Management Center가 테넌트에 배포된 경우:

Objects(개체**) > FTD Network Objects(FTD** 네트워크 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**) > Meraki Objects(Meraki** 개체**)**를 클릭합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.

단계 **3** 편집할 개체를 선택합니다.

단계 **4** 세부 정보 창에서 편집 버튼  를 클릭합니다.

단계 **5** 위의 절차에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 편집합니다.

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 모든 디바이스에 대한 구성 변경 사항 미리보기 및 배포하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

관련 정보

- Meraki 디바이스와 연결된 개체
- Meraki 서비스 개체 생성 또는 편집
- 사용되지 않는 개체 문제 해결
- 중복 개체 문제 해결
- 변경 로그

네트워크 개체 및 그룹 삭제

클라우드 사용 Firewall Management Center가 테넌트에 배포된 경우:

Objects(개체**) > FTD Network Objects(FTD** 네트워크 개체**)** 페이지에서 네트워크 개체 또는 그룹을 삭제하면 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지에서 복제된 네트워크 개체 또는 그룹이 삭제되며 그 반대의 경우도 마찬가지입니다.

서비스 개체

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

Meraki 서비스 개체 생성 또는 편집

서비스 개체 정보

서비스 개체는 TCP/IP 프로토콜 및 포트를 지정하는 재사용 가능한 구성 요소입니다. CDO는 이러한 개체를 서비스 개체로 분류합니다. MX 디바이스에 배포할 때 CDO는 개체를 프로토콜 또는 포트 범위로 변환합니다. CDO가 Meraki 프로토콜을 개체로 처리하는 방법에 대한 자세한 내용은 Meraki 디바이스와 연결된 개체을 참조하십시오.

서비스 개체 생성

단계 **1** 좌측의 CDO 탐색 모음에서 **Objects(**개체**) > Meraki Objects(Meraki** 개체**)**를 클릭합니다.

단계 **2**  를 클릭한 다음 **FTD** > **Service(**서비스**)** 또는 **ASA** > **Service(**서비스**)**를 클릭합니다.

단계 **3** 개체 이름과 설명을 입력합니다.

단계 **4** **Create a service object(**서비스 개체 생성**)**를 선택합니다.

단계 **5** **Service Type(**서비스 유형**)** 버튼을 클릭하고 개체를 생성할 프로토콜을 선택합니다.

단계 **6** 다음 작업 중 하나를 수행하여 프로토콜을 식별하기 위한 정보를 입력합니다.

- TCP 또는 UDP 포트의 특정 포트 번호를 입력합니다.
- ICMP 또는 ICMPv6 메시지 유형을 선택합니다.
- "기타" 서비스 유형을 선택한 경우 목록에서 TCP/IP 프로토콜 중 하나를 선택합니다.

단계 **7** **Add(**추가**)**를 클릭합니다.

단계 **8** 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 배포하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

서비스 그룹 생성

단계 **1** 좌측의 CDO 탐색 모음에서 **Objects(**개체**) > Meraki Objects(Meraki** 개체**)**를 클릭합니다.

단계 **2**  를 클릭한 다음 **FTD** > **Service(**서비스**)**를 클릭합니다.

Note Meraki는 ASA 서비스 그룹을 지원하지 않습니다.

단계 **3** 개체 이름과 설명을 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** 서비스 그룹에 서비스 개체 및 서비스 값 추가를 완료하면 **Add(**추가**)**를 클릭합니다.

단계 **7** 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 배포하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

서비스 개체 또는 서비스 그룹 편집

단계 **1** 좌측의 CDO 탐색 모음에서 **Objects(**개체**) > Meraki Objects(Meraki** 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 편집합니다.

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. 이제 개체를 Meraki 정책에서 사용할 준비가 되었습니다.

단계 **7** 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 배포하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

관련 정보

- Meraki 디바이스와 연결된 개체
- 사용되지 않는 개체 문제 해결
- 중복 개체 문제 해결
- 변경 로그

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.

• Meraki 액세스 제어 정책, 21 페이지

Meraki 액세스 제어 정책

Meraki MX 디바이스는 CDO에 온보딩하기 전에 Meraki 대시보드에서 관리되었을 수 있으며 디바이스에 이미 일부 아웃바운드 규칙이 있을 수 있습니다. 이러한 규칙은 CDO에서 액세스 제어 규칙으로 표시됩니다. 이러한 규칙을 편집하고 액세스 제어 정책 내에서 추가 규칙을 생성할 수 있습니다. 액세스 제어 정책을 맞춤화하려면 개체를 생성하고 연결합니다. 자세한 내용은 하단의 관련 문서를 참조하십시오.

Note Meraki 액세스 제어 정책의 작업은 기본적으로 **Allow(**허용**)**입니다. 작업을 변경할 수 없습니다.

CDO를 사용하여 Meraki 액세스 제어 정책을 편집하려면 다음 절차를 수행합니다.

단계 **1** **Devices & Services(**디바이스 및 서비스**)** 페이지를 엽니다.

단계 **2** **Templates(**템플릿**)** 탭을 클릭합니다.

단계 **3** **Meraki** 탭을 클릭하고 액세스 제어 정책을 편집할 Meraki MX 디바이스 템플릿을 선택합니다.

단계 **4** 오른쪽의 **Management(**관리**)** 창에서 **Policy(**정책**)**를 선택합니다.

단계 **5** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 파란색 플러스 버튼  를 클릭합니다.
- 기존 규칙을 편집하려면 규칙을 선택하고 작업 창에서 Edit(편집) 버튼 를 클릭합니다. (간단한 편집은 편집 모드를 시작하지 않고 인라인으로 수행할 수도 있습니다.)
- 더 이상 필요하지 않은 규칙을 삭제하려면 규칙을 선택하고 작업 창에서 Remove(제거) 버튼 를 클릭합니다.
- 정책 내에서 규칙을 이동하려면 액세스 제어 테이블에서 규칙을 선택하고 규칙 행의 끝에 있는 위쪽 또는 아래쪽 화살표를 클릭하여 규칙을 이동합니다.

단계 **6** **Order(**순서**)** 필드에서 정책 내 규칙의 위치를 선택합니다. 네트워크 트래픽은 1부터 "마지막"까지 숫자 순서대로 규칙 목록을 기준으로 평가됩니다.

규칙은 처음 일치하는 항목을 기준으로 적용되므로, 매우 구체적인 트래픽 일치 기준이 포함된 규칙이 보다 일반적인 기준이 포함된 정책(규칙이 일치하지 않는 경우 일치하는 트래픽에 적용됨) 위에 표시되도록 삽입해야 합니다.

기본적으로는 규칙이 목록의 끝에 추가됩니다. 나중에 규칙의 위치를 변경하려는 경우 이 옵션을 편집합니다.

단계 **7** 규칙 이름을 입력합니다. 영숫자, 공백 및 특수 문자(+, ., _, -)는 사용할 수 있습니다.

참고: 액세스 제어 규칙의 이름은 CDO에서 규칙의 이름으로 사용되는 반면, **Remark(**비고**)** 필드는 Meraki 대시보드에서 규칙의 이름으로 처리됩니다. 두 필드는 서로 종속되지 않습니다.

단계 **8** 네트워크 트래픽이 규칙과 일치하는 경우 적용할 작업을 선택합니다.

- **Block(**차단**)** - 트래픽을 무조건 삭제합니다. 트래픽은 검사되지 않습니다.
- **Allow(**허용**)** - 정책에서 침입 및 기타 검사 설정이 적용되는 트래픽을 허용합니다.

Note 규칙 작업만 설정하거나 편집할 수 있습니다. CDO에서 기본 정책 작업을 변경할 수 없습니다.

단계 **9** 다음 탭의 속성을 적절하게 조합하여 트래픽 일치 기준을 정의합니다.

- **Source(**소스**) - Source(**소스**)** 탭을 클릭하고 네트워크 트래픽이 시작된 네트워크(네트워크 및 대륙 포함) 또는 포트를 추가하거나 제거합니다. 기본값은 "Any(모두)"입니다.
- **Destination(**대상**) - Destination(**대상**)** 탭을 클릭하고 트래픽이 도착하는 네트워크(네트워크 및 대륙 포함) 또는 포트를 추가하거나 제거합니다. 기본값은 "Any(모두)"입니다.

Note 소스 및 대상 네트워크는 구성된 VLAN 서브넷 중 하나 또는 VLAN 서브넷이 수동으로 구성되지 않은 경우 기본 VPN 서브넷 내에 있어야 합니다. 유효하지 않은 소스 또는 대상 네트워크를 포함하는 규칙을 배포하면 실패합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

단계 **11** 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 배포하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

What to do next

관련 문서:

- Meraki 디바이스와 연결된 개체
- Meraki 서비스 개체 생성 또는 편집
- Meraki 네트워크 개체 또는 네트워크 그룹 생성 또는 편집

Meraki 템플릿

Meraki 템플릿은 여러 사이트/네트워크에서 공유하는 네트워크 구성입니다. 개별 사이트 네트워크는 템플릿 네트워크에 바인딩할 수 있으므로 단일 템플릿에 대한 변경 사항은 바인딩된 모든 네트워크에 적용됩니다. CDO에서 바인딩된 네트워크는 바인딩된 디바이스로 표시됩니다. 이는 서로 다른 위치에 있는 여러 네트워크에 걸쳐 하나의 정책을 사용하려는 경우에 적합합니다. 두 개 이상의 네트워크를 단일 템플릿으로 구성하려면 구성 템플릿을 사용하여 여러 네트워크 관리를 참조하십시오. Meraki 템플릿이 무엇인지, 네트워크에서 템플릿 사용을 계획하는 방법 및 템플릿 네트워크를 설정하는 방법에 대한 자세한 내용은 Meraki 템플릿 모범 사례를 참조하십시오.

Meraki 템플릿은 Meraki 디바이스와 동일한 방식으로 작동하며, CDO에 온보딩하기 전에 Meraki 대시보드를 통해 먼저 템플릿을 구성해야 합니다. CDO에 템플릿을 온보딩하면 기존 규칙 또는 IP 그룹이 CDO로 변경 사항 읽기, 삭제, 확인 및 배포 개체로 변환됩니다. 동기화되면 **Inventory(**인벤토리 **)** 페이지의 디바이스 세부 정보 창에 템플릿 이름과 연결(바인딩된 디바이스로 표시됨)된 네트워크 수가 표시됩니다. 즉, CDO에서 템플릿 및 바인딩된 네트워크와 연결된 정책을 관리하고 편집/배포할 수도 있습니다. 자세한 내용은 Meraki 템플릿을 Defense Orchestrator에 온보딩을 참조하십시오.

관련 정보

- CDO가 Meraki와 통신하는 방법
- Meraki 디바이스와 연결된 개체
- 변경 사항 읽기, 삭제, 확인 및 배포

변경 사항 읽기, 삭제, 확인 및 배포

디바이스를 관리하려면, CDO에 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 충돌 탐지를 활성화한 경우 CDO는 10분마다 디바이스의 구성 변경 사항을 확인합니다. 디바이스에 저장된 구성의 복사본이 변경된 경우 CDO는 "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. CDO는 덮어쓰기 작업을 수행하기 전에 두 구성 복사본의 차이점을 확인하라는 메시지를 표시하지 않습니다.

모두 읽기는 대량 작업입니다. 상태에 상관없이 두 개 이상의 디바이스를 선택하고 **Read All(**모두 읽기**)**을 클릭하여 CDO에 저장된 모든 디바이스의 구성을 디바이스에 저장된 구성으로 덮어쓸 수 있습니다.

변경 사항 배포

디바이스의 구성을 변경하면 CDO는 변경 사항을 구성의 자체 복사본에 저장합니다. 이러한 변경 사항은 디바이스에 배포될 때까지 CDO에서 "보류 중"입니다. 디바이스에 배포되지 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 배포한 후에야 적용됩니다. CDO는 디바이스의 구성에 변경 사항을 배포할 때 변경된 구성의 요소만 덮어씁니다. 디바이스에 저장된 전체 구성 파일을 덮어쓰지 않습니다. 배포은 단일 디바이스 또는 두 개 이상의 디바이스에서 동시에 시작할 수 있습니다.

Discard All(모두 취소**)**은 **Preview and Deploy(**미리보기 및 배포**)...**를 클릭한 후에만 사용할 수 있는 옵션입니다.. Preview and Deploy(미리보기 및 배포)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 배포되지 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 배포을 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 **Devices & Services(**디바이스 및 서비스**)**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 레이블을 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**)**를 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**)**를 클릭합니다.

단계 **8** Read All(모두 읽기) 구성 작업의 진행 상황은 알림 탭에서 확인합니다. 대량 작업의 개별 작업이 성공하거나 실패한 방식에 대한 자세한 내용을 보려면 파란색 Review(검토) 링크를 클릭합니다. 그러면 Jobs(작업) 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 배포
- 변경 사항 취소
- 구성 변경 사항 확인

모든 디바이스에 대한 구성 변경 사항 미리보기 및 배포

테넌트의 디바이스에 대한 구성을 변경했지만 해당 변경 사항을 배포하지 않은 경우 Deploy(배포) 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 배포할 수 있습니다.

이 배포 방법은 지원되는 모든 디바이스에서 사용할 수 있습니다.

단일 구성 변경 사항에 이 배포 방법을 사용하거나, 기다렸다가 여러 변경 사항을 한 번에 배포할 수 있습니다.

SUMMARY STEPS

1. 화면의 오른쪽 상단에서 **Deploy(**구축**)** 아이콘 을 클릭합니다**.**
2. 배포하려는 변경 사항이 있는 디바이스를 선택합니다. 디바이스에 노란색 주의 삼각형이 있는 경우 해당 디바이스에 변경 사항을 배포할 수 없습니다. 노란색 주의 삼각형 위에 마우스를 올려놓으면 해당 디바이스에 변경 사항을 배포할 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 요청을 생성합니다.
6. 선택한 디바이스에 변경 사항을 즉시 배포하려면 **Deploy Now(**지금 구축**)**를 클릭합니다. 작업 트레이의 활성 작업 표시기에 진행 상황이 표시됩니다.
7. (선택 사항) 배포이 완료되면 CDO 탐색 모음에서 **Jobs(**작업**)**를 클릭합니다. 배포 결과를 보여주는 최근 "Deploy Changes(변경 사항 배포)" 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** 배포하려는 변경 사항이 있는 디바이스를 선택합니다. 디바이스에 노란색 주의 삼각형이 있는 경우 해당 디바이스에 변경 사항을 배포할 수 없습니다. 노란색 주의 삼각형 위에 마우스를 올려놓으면 해당 디바이스에 변경 사항을 배포할 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 요청을 생성합니다.

단계 **6** 선택한 디바이스에 변경 사항을 즉시 배포하려면 **Deploy Now(**지금 구축**)**를 클릭합니다. 작업 트레이의 활성 작업 표시기에 진행 상황이 표시됩니다.

단계 **7** (선택 사항) 배포이 완료되면 CDO 탐색 모음에서 **Jobs(**작업**)**를 클릭합니다. 배포 결과를 보여주는 최근 "Deploy Changes(변경 사항 배포)" 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

디바이스에 변경 사항 배포

단계 **1** CDO를 사용하여 디바이스에 대한 구성을 변경하고 저장하면 해당 변경 사항이 디바이스 구성의 CDO 인스턴스에 저장됩니다.

단계 **2** 탐색 모음에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **3** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **4** 해당 디바이스 탭을 클릭합니다. 변경한 디바이스의 구성 상태가 이제 "동기화되지 않음"으로 표시되어야 합니다.

단계 **5** 다음 방법 중 하나를 사용하여 변경 사항을 배포합니다.

- 디바이스를 선택하고 오른쪽의 동기화되지 않음 창에서 **Preview and Deploy(**미리 보기 및 배포**)**를 클릭합니다. Pending Changes 화면에서 변경 사항을 검토합니다. 보류 중인 버전에 만족하면 **Deploy Now(**지금 배포**)**를 클릭합니다. 변경 사항이 성공적으로 배포되면 변경 로그를 보고 방금 일어난 일을 확인할 수 있습니다.

- 화면의 오른쪽 상단에 있는 **Deploy(**구축**)** 아이콘  를 클릭합니다. 자세한 내용은 모든 디바이스에 대한 구성 변경 사항 미리보기 및 배포, on page 25를 참조하십시오.

변경 취소

CDO에서 디바이스로 변경 사항을 배포할 때 **Cancel(**취소**)**를 클릭하면 변경 사항이 디바이스에 배포되지 않습니다. 프로세스가 취소됩니다. 변경 사항은 여전히 CDO에서 보류 중이며 최종적으로 FDM 관리 디바이스에 배포하기 전에 추가로 편집할 수 있습니다.

변경 사항 취소

변경 사항을 미리 볼 때 **Discard all(**모두 취소**)**을 클릭하면 변경 사항 및 다른 사용자가 수행했지만 디바이스에 배포하지 않은 기타 변경 사항이 삭제됩니다. CDO는 보류 중인 구성을 변경하기 전에 마지막으로 읽거나 배포한 구성으로 되돌립니다.

디바이스 구성 대량 배포

예를 들어 공유 개체를 편집하여 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 배포합니다.

- 화면의 오른쪽 상단에 있는 **Deploy(**구축**)** 버튼  를 클릭합니다. 이렇게 하면 배포하기 전에 선택한 디바이스에서 보류 중인 변경 사항을 검토할 수 있습니다. **Deploy Now(**지금 구축**)**를 클릭하여 변경 사항을 배포합니다.

  Note **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 화면에서 디바이스 옆에 노란색 경고 삼각형이 표시되면 해당 디바이스에 변경 사항을 배포할 수 없습니다. 변경 사항을 해당 디바이스에 배포할 수 없는 이유에 대한 정보를 보려면 경고 삼각형 위에 마우스를 올려놓습니다.

- 세부 정보 창에서 **Deploy All(**모두 구축**)**  를 클릭합니다. 경고를 검토하고 **OK(**확인**)**를 클릭합니다. 대량 배포은 변경 사항을 검토하지 않고 즉시 시작됩니다.

단계 **6** (선택 사항) 탐색 모음에서 Jobs(작업) 아이콘  을 클릭하여 대량 배포의 결과를 확인합니다.

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 배포 예약 옵션 활성화 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 배포 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 배포 예약

배포 일정은 단일 이벤트 또는 반복 이벤트일 수 있습니다. 반복 자동 배포을 사용하면 유지 보수 기간에 맞춰 반복 배포을 편리하게 이용할 수 있습니다. 단일 디바이스에 대해 일회성 또는 반복 배포을 예약하려면 다음 절차를 따르십시오.

Note 기존 배포이 예약된 디바이스에 대한 배포을 예약하는 경우 새로 예약된 배포이 기존 배포을 덮어씁니다.

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(디바이스 세부 정보) 창에서 Scheduled Deployments(예약된 배포) 탭을 찾아 **Schedule(**예약**)**를 클릭합니다.

단계 **6** 배포을 수행해야 하는 시기를 선택합니다.

- 일회성 배포의 경우 **Once on(**한 번**)** 옵션을 클릭하여 달력에서 날짜와 시간을 선택합니다.
- 반복 배포의 경우 **Every(**마다**)** 옵션를 클릭합니다. 매일 또는 일주일에 한 번 배포을 선택할 수 있습니다. 배포을 수행해야 하는 날짜와 시간을 선택합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

예약된 배포 편집

예약된 배포를 편집하려면 다음 절차를 따르십시오.

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(**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 배포
- 모든 디바이스 구성 읽기, on page 24
- 모든 디바이스에 대한 구성 변경 사항 미리보기 및 배포, on page 25

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** 탐색 모음에서 **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.

- Meraki 디바이스의 경우 디바이스의 구성이 변경된 경우 다음 메시지가 표시됩니다.

  디바이스에서 정책을 읽는 중입니다. 디바이스에 활성 배포이 있는 경우 완료 후 읽기가 시작됩니다.

- 계속하려면 **OK(**확인**)**를 클릭합니다. 디바이스의 구성이 CDO에 저장된 구성을 덮어씁니다.
- 작업을 취소하려면 **Cancel(**취소**)**를 클릭합니다.

• 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 배포되지 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 동기화되지 않음 창에서 **Discard Changes(**변경 사항 취소**)**를 클릭합니다.

- FTD 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**)**를 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 충돌 탐지가 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 배포되지 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 배포하면 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 36를 참조하십시오.

충돌 탐지 활성화

충돌 감지를 활성화하면 Defense Orchestrator 외부의 디바이스가 변경된 인스턴스에 대해 경고합니다.

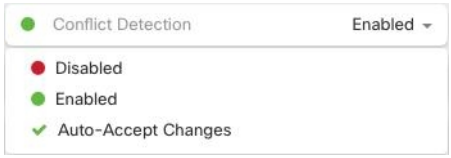
단계 **1** 탐색 모음에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

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 관리 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 배포되지 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 Devices & Services(디바이스 및 서비스) 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 33를 활성화합니다.

변경 사항 자동 수락 구성

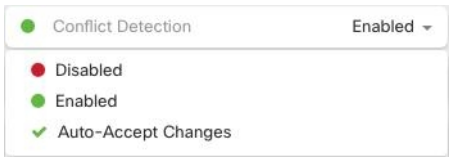
단계 **1** 관리자 또는 슈퍼 관리자 권한이 있는 계정을 사용하여 CDO에 로그인합니다.

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** 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** 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 배포하거나 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 33이 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** 탐색 모음에서 **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 33를 활성화했거나 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 두 개 이상의 디바이스에 적용할 수 있습니다.

디바이스에 대해 구성된 선택 항목이 없는 경우 "테넌트 기본값"에 대한 간격이 자동으로 구성됩니다.

Note **Devices & Services(**디바이스 및 서비스**)** 페이지에서 디바이스별 간격을 맞춤 설정하면 **General Settings(**일반 설정**)** 페이지에서 Default Conflict Detection Interval(기본 충돌 탐지 간격)로 선택한 폴링 간격이 오버라이드됩니다.

Devices & Services(디바이스 및 서비스**)** 페이지에서 **Conflict Detection(**충돌 탐지**)**을 활성화하거나 설정 페이지에서디바이스 변경 사항을 자동 수락하는 옵션을 활성화한 후 다음 절차를 사용하여 CDO가 디바이스를 폴링할 빈도를 예약합니다.

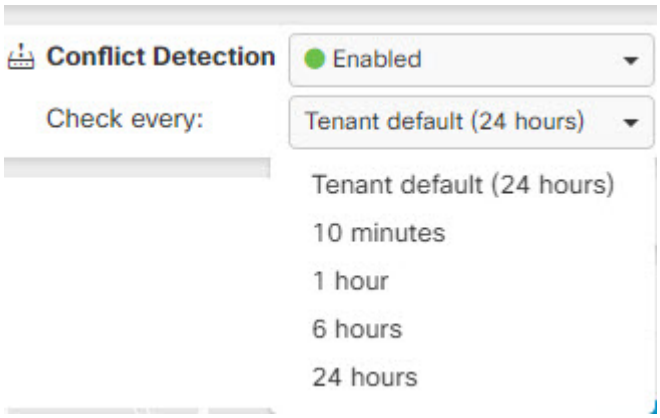
단계 **1** 탐색 모음에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

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.


Conflict Detection
Enabled
Check every:
Tenant default (24 hours)
Tenant default (24 hours)
10 minutes
1 hour
6 hours
24 hours