AWS 디바이스 구성

이 장에는 다음 섹션이 포함되어 있습니다.

AWS VPC 연결 자격 증명 업데이트

AWS VPC에 연결할 새 액세스 키 및 보안 액세스 키를 생성하는 경우 CDO에서 연결 자격 증명을 업데이트해야 합니다. AWS 콘솔에서 자격 증명을 업데이트한 다음 아래 절차를 사용하여 CDO 콘솔에서 자격 증명을 업데이트합니다. 자세한 내용은 *IAM* 사용자의 액세스 키 관리(https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html) 또는 *AWS* 계정 루트

사용자의 액세스 키 생성, 비활성화 및 삭제 (https://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html)을 참조하십시오.

CDO에서 액세스 키 또는 보안 액세스 키를 변경할 수 없습니다. AWS 콘솔 또는 AWS CLI 콘솔에서 연결 자격 증명을 수동으로 관리해야 합니다.

Note 여러 AWS VPC가 CDO 테넌트에 온보딩된 경우 한 번에 하나의 디바이스에 대한 자격 증명을 업데이트해야 합니다.

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

단계 **2** **Devices(**디바이스**)** 탭을 클릭한 다음 **AWS VPC**를 클릭합니다.

단계 **3** 연결 자격 증명을 업데이트할 AWS VPC를 선택합니다.

필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

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

단계 **5** AWS VPC에 연결하는 데 사용할 새 액세스 키 및 보안 액세스 키를 입력합니다.

단계 **6** **Update(**업데이트**)**를 클릭합니다.

Note 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. 유효하지 않은 자격 증명 문제 해결의 내용을 참조하십시오.

관련 정보

- AWS VPC 온보딩

AWS Transit Gateway를 사용하여 AWS VPC 터널 모니터링

AWS(Amazon Web Service) Transit Gateway는 간소화된 피어링 관계를 허용하는 중앙 허브를 통해 엔터프라이즈 VPC(Virtual Private Cloud)를 AWS VPC에 연결하는 클라우드 라우터 역할을 합니다.

CDO(Cisco Defense Orchestrator)에서는 AWS Transit Gateway를 사용하여 온보딩된 AWS VPC의 연결 상태를 모니터링할 수 있습니다.

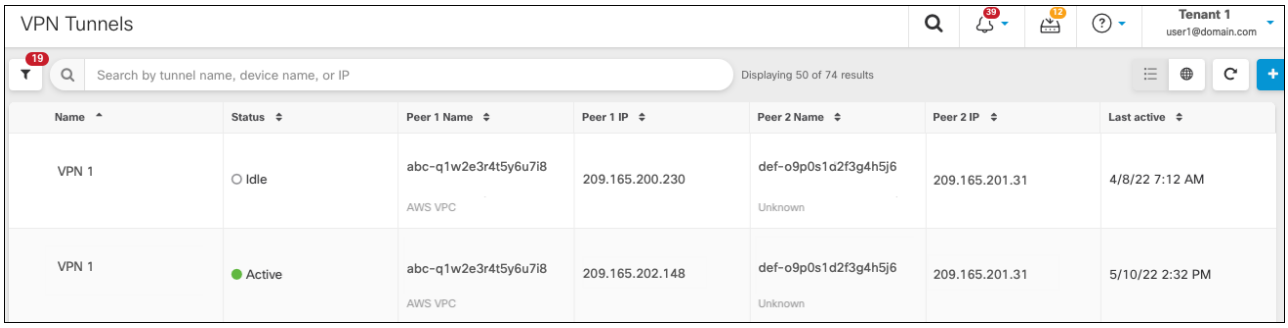
Note AWS Transit Gateway를 사용하여 모니터링하기 위해 CDO에서 SFCN(Secure Firewall Cloud Native) VPC를 온보딩할 필요가 없습니다.

단계 **1** CDO 메뉴 모음에서 **VPN > Site-to-Site VPN**을 선택합니다**.**

단계 2 **VPN Tunnels(VPN** 터널)페이지에는 CDO 테넌트에서 관리하는 모든 네트워크 터널의 연결 상태가 표시됩니다. VPN 터널의 연결 상태는 사이트 간 VPN 터널 검색 및 필터링 상태일 수 있습니다.

단계 3 VPC를 선택하고 **Actions(**작업**)** 아래에서 **Check Connectivity(**연결 확인**)**를 클릭하여 터널에 대한 실시간 연결 확인을 트리거하고 터널이 현재 사이트 간 VPN 터널 검색 및 필터링 상태인지를 식별합니다. 온디맨드 연결 확인 링크를 클릭하지 않으면 온보딩된 모든 디바이스에서 사용 가능한 모든 터널의 확인이 10분마다 수행됩니다.

Note VPN 터널의 연결이 다운되면 CDO에서 알림을 표시합니다. 그러나 링크가 백업된 경우 알림 프롬프트가 표시되지 않습니다.



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.

AWS VPC 터널에 대한 변경 기록 보기

AWS VPC 터널에 대한 변경 기록을 보려면 다음을 수행합니다.

단계 **1** CDO 메뉴 모음에서 **Change Log(로그 변경)**를 선택합니다.

단계 **2** **Change Log(로그 변경)** 페이지에서 필터 아이콘을 클릭하고 **Filter by device(디바이스 별 필터)** 탭을 선택한 후 **AWS VPC**를 클릭합니다.

단계 **3** 기록을 검토할 AWS VPC를 선택하고 **OK(확인)** 를 클릭합니다.

관련 정보

- 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.

- AWS VPC 정책, 4 페이지

AWS VPC 정책

CDO(Cisco Defense Orchestrator)는 사용자에게 AWS 계정과 연결된 AWS(Amazon Web Services) VPC(Virtual Private Cloud) 전체에서 보안 정책을 일관되게 유지할 수 있는 기능을 제공합니다. 또한

CDO를 사용하여 여러 디바이스 유형에서 개체를 공유할 수 있습니다. 자세한 내용은 다음 항목을 참고하십시오.

CDO의 AWS VPC 및 보안 그룹

AWS VPC 보안 그룹 규칙

AWS 보안 그룹은 모든 AWS EC2 인스턴스 및 보안 그룹과 연결된 기타 엔터티에 대한 인바운드 및 아웃바운드 네트워크 트래픽을 제어하는 규칙의 모음입니다.

AWS(Amazon Web Services) 콘솔과 마찬가지로 CDO는 각 규칙을 개별적으로 표시합니다. SDC가 인터넷에 액세스할 수 있으면 다음 환경에 대한 AWS VPC(Virtual Private Cloud) 규칙을 생성하고 관리할 수 있습니다.

- 동일한 AWS VPC 내의 다른 보안 그룹과 주고받는 정보를 허용하는 보안 그룹입니다.
- IPv4 또는 IPv6 주소와 주고받는 것을 허용하는 보안 그룹입니다.

AWS 보안 그룹을 포함하는 CDO에서 규칙을 생성할 때는 다음 제한 사항에 유의하십시오.

- 인바운드 트래픽을 허용하는 규칙의 경우, 소스는 동일한 AWS VPC, IPv4 또는 IPv6 CIDR 블록 또는 단일 IPv4 또는 IPv6 주소에 있는 하나 이상의 보안 그룹 개체일 수 있습니다. 인바운드 규칙은 하나의 보안 그룹 개체만 대상으로 포함할 수 있습니다.
- 아웃바운드 트래픽을 허용하는 규칙의 경우 대상은 동일한 AWS VPC에 있는 하나 이상의 보안 그룹 개체, 접두사 목록 ID, IPv4 또는 IPv6 CIDR 블록, 단일 IPv4 또는 IPv6 주소일 수 있습니다. 아웃바운드 규칙은 하나의 보안 그룹 개체만 소스로 포함할 수 있습니다.
- CDO는 여러 엔터티(예: 둘 이상의 포트 또는 서브넷)를 포함하는 규칙을 AWS VPC에 구축하기 전에 별도의 규칙으로 변환합니다.
- 규칙을 추가하거나 제거하면 보안 그룹과 연결된 모든 AWS 엔터티에 변경 사항이 자동으로 적용됩니다.
- AWS 보안 그룹은 최대 60개의 인바운드 규칙과 60개의 아웃바운드 규칙을 호스팅하도록 제한됩니다. 이 제한은 IPv4 규칙 및 IPv6 규칙에 대해 별도로 적용됩니다. CDO에서 생성된 추가 규칙은 총 규칙 수에 포함됩니다. 즉, CDO에 온보딩하여 60 규칙 제한을 초과할 수 없습니다.

Warning 기존 규칙을 편집하면 편집된 규칙이 삭제되고 새 세부 정보로 새 규칙이 생성됩니다. 이로 인해 새 규칙을 생성할 수 있을 때까지 해당 규칙에 의존하는 트래픽이 매우 짧은 기간 동안 삭제됩니다. 새 규칙을 생성하는 경우에는 이러한 현상이 발생하지 않습니다.

AWS 콘솔에서 생성할 수 있는 규칙 유형에 대한 자세한 내용은 AWS 보안 그룹 개체를 참조하십시오. AWS VPC와 연결할 수 있는 개체에 대한 자세한 내용은 AWS 보안 그룹 및 클라우드 보안 그룹 개체의 내용을 참조하십시오.

관련 정보

- 보안 그룹 규칙 생성, on page 6

• 보안 그룹 규칙 편집, on page 7
• 보안 그룹 규칙 삭제, on page 7

보안 그룹 규칙 생성

기본적으로 AWS(Amazon Web Services) VPC(Virtual Private Cloud)는 모든 네트워크 트래픽을 차단합니다. 즉, 모든 규칙이 트래픽 **Allow(**허용**)**로 자동 구성됩니다. 이 작업은 편집할 수 없습니다.

Note 새 보안 그룹 규칙을 생성할 때는 이를 보안 그룹과 연결해야 합니다.

AWS 콘솔은 둘 이상의 소스 또는 대상을 포함하는 규칙을 지원하지 않습니다. 즉, 둘 이상의 엔터티를 포함하는 단일 보안 그룹 규칙을 구축하는 경우 CDO는 AWS VPC에 구축하기 전에 규칙을 별도의 규칙으로 변환합니다. 예를 들어, 2개의 포트 범위에서 하나의 클라우드 보안 그룹 개체로 트래픽을 허용하는 인바운드 규칙을 생성하는 경우, CDO는 이를 2개의 개별 규칙으로 변환합니다. (1) 첫 번째 포트 범위에서 보안 그룹으로의 트래픽을 허용하고 (2) 두 번째 포트 범위에서 보안 그룹으로의 트래픽을 허용합니다.

다음 절차를 사용하여 보안 그룹 규칙을 생성합니다.

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

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

단계 **3** **AWS** 탭을 클릭하고 액세스 제어 정책을 수정할 AWS VPC 디바이스 템플릿을 선택합니다.

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

단계 **5** 규칙을 추가할 보안 그룹 옆에 있는 파란색 더하기 버튼을 클릭합니다.

단계 **6** **Inbound(**인바운드**)** 또는 **Outbound(**아웃바운드**)**를 클릭합니다.

- **Inbound(**인바운드**)** 규칙 - 소스 네트워크는 하나 이상의 IPv4 주소, IPv6 주소 또는 클라우드 보안 그룹 개체를 포함할 수 있습니다. 대상 네트워크는 단일 클라우드 보안 그룹 개체로 정의되어야 합니다.
- **Outbound(**아웃바운드**)** 규칙 - 소스 네트워크는 단일 클라우드 보안 그룹 개체로 정의되어야 합니다. 대상 네트워크는 하나 이상의 IPv4 주소, IPv6 주소 또는 보안 그룹 개체를 포함할 수 있습니다.

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

단계 **8** 다음 탭의 속성을 적절하게 조합하여 트래픽 일치 기준을 정의합니다.

- **Source(**소스**)** - **Source(**소스**)** 탭을 클릭하고 네트워크(네트워크 및 대륙 포함)를 추가하거나 제거합니다. 포트 또는 포트 범위를 소스로 정의할 수 없습니다.

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

    정의된 네트워크 개체가 없으면 AWS 콘솔에서 IPv4(0.0.0.0/0)에 대한 규칙과 IPv6(::0/0)에 대한 규칙의 두 가지 규칙으로 변환됩니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

단계 **10** 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

Caution 구축에 실패하면 CDO는 AWS VPC의 상태를 구축을 시도하기 전의 상태로 되돌립니다. 이는 "최선의 노력"을 기반으로 수행됩니다. AWS는 상태를 유지하지 않으므로 이 롤백 시도는 실패할 수 있습니다. 이 경우 AWS 관리 콘솔에 로그인하고 AWS VPC를 이전 구성으로 수동으로 되돌린 다음 CDO에서 변경 사항 읽기, 삭제, 확인 및 구축 합니다.

보안 그룹 규칙 편집

CDO를 사용하여 AWS VPC에 대한 액세스 제어 규칙을 편집하려면 다음 절차를 수행합니다.

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

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

단계 **3** **AWS** 탭을 클릭하고 액세스 제어 정책을 수정할 AWS VPC를 선택합니다.

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

단계 **5** 기존 보안 그룹 규칙을 편집하려면 규칙을 선택하고 Actions(작업) 창에서 편집 아이콘을 클릭합니다. (간단한 편집은 편집 모드를 시작하지 않고 인라인으로 수행할 수도 있습니다.) 규칙 제한 및 예외는 AWS VPC 보안 그룹 규칙을 참조하십시오.

단계 **6** **Save(**저장**)**를 클릭합니다.

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

Caution 구축에 실패하면 CDO는 AWS VPC의 상태를 구축을 시도하기 전의 상태로 되돌립니다. 이는 "최선의 노력"을 기반으로 수행됩니다. AWS는 상태를 유지하지 않으므로 이 롤백 시도는 실패할 수 있습니다. 이 경우 AWS 관리 콘솔에 로그인하고 AWS VPC를 이전 구성으로 수동으로 되돌린 다음 AWS VPC 디바이스 구성과 CDO의 구성 간의 변경 사항을 폴링해야 합니다.

보안 그룹 규칙 삭제

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

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

단계 3 **AWS** 탭을 클릭하고 액세스 제어 정책을 수정할 AWS VPC를 선택합니다.

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

단계 5 더 이상 필요하지 않은 보안 그룹 규칙을 삭제하려면 규칙을 선택하고 **Actions(**작업**)** 창에서 제거 아이콘을 클릭합니다.

단계 6 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

Caution 구축에 실패하면 CDO는 AWS VPC의 상태를 구축을 시도하기 전의 상태로 되돌립니다. 이는 "최선의 노력"을 기반으로 수행됩니다. AWS는 상태를 유지하지 않으므로 이 롤백 시도는 실패할 수 있습니다. 이 경우 AWS 관리 콘솔에 로그인하고 AWS VPC를 이전 구성으로 수동으로 되돌린 다음 AWS VPC 디바이스 구성과 CDO의 구성 간의 변경 사항을 폴링해야 합니다.

가상 프라이빗 네트워크 관리

VPN(Virtual Private Network)은 인터넷과 같은 공용 네트워크를 통해 엔드포인트 간에 보안 터널을 설정합니다.

이 섹션은 디바이스의 원격 액세스 및 사이트 투 사이트 VPN에 적용됩니다. 또한 에서 VPN 연결을 배포하고 원격 액세스하는 데 사용되는 SSL 표준에 대해서도 설명합니다.

CDO 에서는 다음과 같은 유형의 VPN 연결을 지원합니다.

• 사이트 간 가상 프라이빗 네트워크, 8 페이지

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 에 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.

관련 정보:

- AWS 사이트 간 가상 사설망 모니터링

AWS 사이트 간 가상 사설망 모니터링

CDO를 사용하면 온보딩된 AWS 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 에서 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 에서 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 11

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 아이콘을 클릭하여 필터 패널을 엽니다.

단계 **4** 감지된 문제를 확인합니다.

단계 **5** 문제를 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 아이콘을 클릭하여 필터 패널을 엽니다.

단계 **4** 문제를 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 아이콘 을 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, 18 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
- AWS VPC 온보딩

AWS 사이트 간 **VPN** 터널 보기

AWS 사이트 간 VPN은 보안 터널을 통해 VPC(Virtual Private Cloud)를 엔터프라이즈 네트워크에 연결합니다.

모든 사이트 간 VPN 구성은 AWS Management 콘솔에서 수행됩니다. VPC를 온보딩하면 CDO는 AWS VPC에서 유지 관리하는 사이트 간 VPN 연결을 표시하고 VPN Tunnels(VPN 터널) 페이지에 표시하여 다른 모든 사이트 간 연결과 함께 관리할 수 있습니다. 네트워크에서 VPC로의 각 VPN 연결은 2개의 개별 VPN 터널로 구성됩니다.

CDO의 VPN Tunnels(VPN 터널) 페이지에서 사이트 간 VPN 터널 정보 보기, VPC의 사이트 간 VPN 터널 검색 및 필터링, 관리되지 않는 디바이스 온보딩할 수 있습니다.

CDO는 10분마다 AWS Management 콘솔을 폴링하여 사이트 간 VPN 구성에 대한 변경 사항을 찾습니다. CDO는 변경 사항이 있음을 발견하면 해당 구성의 변경 사항을 폴링하고 해당 데이터베이스에 변경 사항을 저장합니다. 그러면 CDO 관리자가 CDO에서 새 구성을 볼 수 있습니다.

AWS(Amazon Web Services) 참조 자료

AWS 가상 프라이빗 네트워크 설명서

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**)** 창을 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.

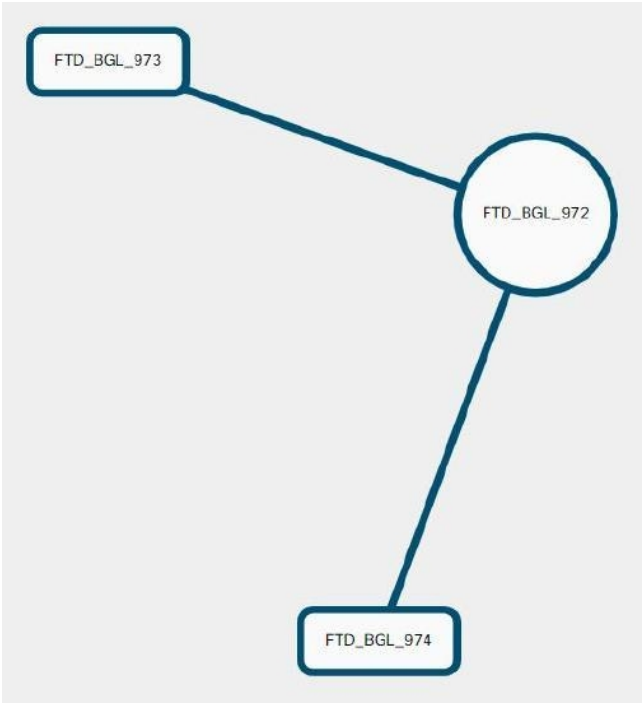
단계 **1** 기본 탐색 모음에서 **VPN > ASA/FDM Site-to-Site VPN**를 클릭합니다.

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

다음은 전역 보기의 예입니다. 그림에서 'FTD_BGL_972'에는 FTD_BGL_973 및 FTD_BGL_974 디바이스와의 사이트 투 사이트 연결이 있습니다.



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.

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.

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 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**)**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 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 구축
- 변경 사항 취소
- 구성 변경 사항 확인

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 요청을 생성합니다.
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 요청을 생성합니다.

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

디바이스에 변경 사항 배포

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

단계 **2** 내비게이션 바에서 **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 구축, on page 18를 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 구축하지 않은 기타 변경 사항이 삭제됩니다. CDO는 보류 중인 구성을 변경하기 전에 마지막으로 읽거나 구축한 구성으로 되돌립니다.

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**)** 버튼  을 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.

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 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 17
- 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, on page 18

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.

- AWS 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.

- 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 29를 참조하십시오.

충돌 탐지 활성화

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

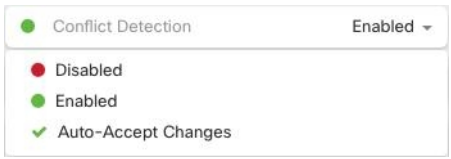
단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

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 26를 활성화합니다.

변경 사항 자동 수락 구성

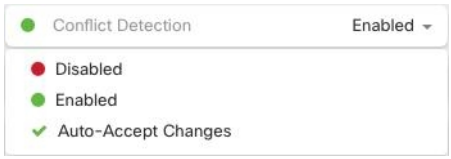
단계 **1** 관리자 또는 슈퍼 관리자 권한이 있는 계정을 사용하여 CDO에 로그인합니다.

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 26이 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 26를 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 Default Conflict Detection Interval(기본 충돌 탐지 간격)로 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.