Cisco Defense Orchestrator로 온프레미스 Firewall Management Center 관리

Cisco Defense Orchestrator로 온프레미스 Firewall Management Center 관리

정보 온프레미스 **Firewall Management Center**

온프레미스 Management Center 지원은 온보딩, 매니지드 디바이스 보기, 네트워크 개체 보기 개체는 온프레미스 Management Center와 연결되었으며, 버전 6.4 이상을 실행하는 디바이스의 경우 온프레미스 Management Center UI와 교차 실행합니다. 추가 기능은 곧 지원될 예정입니다. 현재 CDO에서 지원하지 않는 기능의 경우, 온프레미스 Management Center 콘솔을 사용해야 합니다. 온프레미스 Management Center에서 제공하는 기능에 대한 자세한 내용은 시스템에서 실행 중인 버전의 Cisco Secure Firewall Management Center 구성 가이드를 참조하십시오.

온프레미스 Management Center는 관리, 분석 및 보고 작업을 수행하는 데 사용할 수 있는 그래픽 유저 인터페이스가 포함된 중앙 집중식 관리 콘솔입니다. ASDM 및 FDM에 비할 수 있는 관리 콘솔이지만 동일하지는 않습니다. CDO에서 지원하는 온프레미스 Management Center 디바이스 및 소프트웨어 버전 목록은 CDO의 소프트웨어 및 하드웨어 지원을 참조하십시오.

버전 지원

CDO은 버전 6.4 이상을 지원합니다. 온프레미스 Management Center는 일반적으로 몇 가지 주요 버전 이전의 이전 디바이스를 관리할 수 있습니다. 예를 들어 버전 6.6.0을 실행하는 디바이스는 버전 6.4.0 디바이스를 관리할 수 있습니다. 온프레미스 Management Center에서 6.4 이전 버전을 실행하는 디바이스를 관리하는 경우 해당 디바이스가 **Inventory(**재고 목록**)** 페이지에 표시될 수 있지만 구축하거나 CDO에서 정책을 수정할 수 없습니다. 온프레미스 Management Center UI에서 변경하고 구축해야 합니다.

Cisco Defense Orchestrator로 온프레미스 Firewall Management Center 관리

참고 매니지드 디바이스가 비활성화되었거나 연결할 수 없는 경우 CDO는 **Inventory(**재고 목록**)** 페이지에 디바이스를 표시할 수 있지만, 성공적으로 요청을 전송하거나 디바이스 정보를 볼 수는 없습니다.

CDO가 FMC와 통신하는 방법

CDO는 REST API 클라이언트로 작동하여 요청을 온프레미스 Management Center로 전송한 다음 온프레미스 Management Center는 지정된 클라이언트를 사용하여 요청을 매니지드 디바이스로 보냅니다. 디바이스에서는 동일한 로그인 자격 증명으로 여러 번 로그인하는 것을 허용하지 않으므로 특히 CDO 통신을 위해 관리자 레벨 권한이 있는 새 사용자를 온프레미스 Management Center에 생성하는 것이 좋습니다. 이 새 사용자는 CDO에서 제공하는 관리자 또는 시스템 및 디바이스 권한이 있는 사용자 지정 사용자 역할로 CDO에 복제되어야 합니다. 관리자 로그인이 없으면 CDO는 REST API 명령을 사용하여 정책, 규칙 또는 개체를 수정하거나 생성할 수 없습니다.

온프레미스 Management Center 온보딩 또는 제거

언제든지 온프레미스 Management Center을 온보딩하거나 제거할 수 있습니다. 온프레미스 Management Center 및 등록된 디바이스를 CDO에서 읽기 위해서는 버전 6.4 이상을 실행해야 합니다. 온프레미스 Management Center 및 관련 등록된 디바이스를 온보딩하려면 FMC 온보딩을 참조하십시오.

온프레미스 Management Center이 온보딩된 후에는 **Services(**서비스**)** 페이지에서 온프레미스 Management Center을 선택하거나 **Management(**관리**)** 아래에서 **Devices(**디바이스**)**를 클릭하거나 오른쪽 창에서 아무 작업을 하면 **Verify FMC Cross Launch URL(FMC** 크로스 실행 **URL** 확인**)** 마법사가 열립니다. 이 마법사에서 관리 센터의 공용 IP 주소나 FQDN 및 포트 번호를 입력할 수 있습니다. **Continue(**계속**)**를 클릭하면 입력한 IP 주소를 사용해 새 탭에서 선택한 온프레미스 Management Center 웹 UI로 교차 실행됩니다. 오른쪽 창의 **External Links(**외부 링크**)**에 있는 **Add External Links(**외부 링크 추가**)** 옵션에서 외부 링크를 수동으로 추가할 수도 있습니다.

CDO 테넌트에서 온프레미스 Management Center을 제거하면 해당 온프레미스 Management Center에 등록된 디바이스도 제거됩니다. 자세한 내용은 CDO에서 FMC 제거를 참조하십시오. 온보딩 후 온프레미스 Management Center에 "잘못된 자격 증명" 상태가 발생하는 경우 어플라이언스를 다시 연결할 수 있습니다. 자세한 내용은 잘못된 자격 증명 문제 해결을 참조하십시오.

참고 Firepower 6.6을 실행하는 디바이스는 다시 연결 기능을 지원하지 않습니다. 어플라이언스를 다시 연결해야 하는 경우, 온프레미스 Management Center을 제거하고 어플라이언스를 다시 온보딩하는 것이 좋습니다.

온프레미스 Management Center 고가용성 쌍

CDO에서는 온프레미스 Management Center 어플라이언스용 고가용성(HA) 기능을 지원하지 않습니다. 온프레미스 Management Center 어플라이언스 쌍이 HA에 대해 구성된 경우 **Services(**서비스**)** 페이지에 개별 어플라이언스로 나열됩니다.

Cisco Defense Orchestrator로 온프레미스 Firewall Management Center 관리

온프레미스 Management Center에서 관리되는 디바이스

온프레미스 Management Center을 CDO에 온보딩하면 해당 온프레미스 Management Center에 등록된 모든 디바이스도 CDO로 읽혀집니다. **Inventory(**재고 목록**)** 페이지에서 이름, IP 주소, 디바이스 유형, 소프트웨어 버전 및 상태와 같은 디바이스 정보를 확인할 수 있습니다. 온프레미스 Management Center이 **Services(**서비스**)** 페이지에 표시되고 여기서 관리하는 디바이스는 **Inventory(**재고 목록**)** 페이지에 나열됩니다. **Services(**서비스**)** 페이지에서 버전, 매니지드 디바이스, 디바이스 유형 및 상태와 같은 정보를 확인할 수 있습니다. FMC에서 관리하는 디바이스의 수를 표시하는 **Services(**서비스**)** 페이지에서 디바이스 아이콘을 클릭하면 디바이스 필터가 적용된 **Inventory(**재고 목록**)** 페이지로 이동하므로 선택한 온프레미스 Management Center에서 관리하는 모든 디바이스가 표시됩니다.

Inventory(재고 목록**)**의 오른쪽 창에 있는 **Device Actions(**디바이스 작업**)**, **Monitoring(**모니터링**)**, **Device Management(**디바이스 관리**)**, **Policies(**정책**)** 패널의 관련 옵션을 사용하여 작업을 수행할 수 있습니다. 현재 FMC에서 관리되는 디바이스를 선택하고 이러한 옵션을 클릭하면 CDO에서 입력한 교차 실행 URL을 사용하여 디바이스를 관리하는 온프레미스 Management Center 콘솔이 자동으로 시작됩니다. 필터 아이콘을 사용하여 **Inventory(**재고 목록**)** 페이지를 더 구성할 수 있습니다. 여기에서는 기타 지원되는 디바이스 유형뿐만 아니라 온보딩된 온프레미스 Management Center에서 관리하는 디바이스를 모두 보도록 선택할 수 있습니다. 또한 클러스터의 디바이스를 확장 또는 축소하고, 작업을 수행할 개별 또는 그룹을 선택하여 디바이스를 선택할 수 있습니다.

디바이스 상태

CDO은 **Inventory(**재고 목록**)** 페이지에 위협 방어 디바이스의 상태(예: **Normal(**정상**)**, **Error(**오류**)**, **Warning(**경고**)** 및 **Disabled(**비활성화**)**)를 표시합니다. 디바이스의 상태를 클릭하여 온프레미스 Management Center 사용자 인터페이스에서 디바이스에 해당하는 **Health Monitoring(**상태 모니터링**)** 페이지로 이동할 수 있습니다.

참고 CDO는 디바이스 상태를 10분마다 자동으로 업데이트합니다. 하지만 디바이스를 선택하고 **Check for Changes(**변경 사항 확인**)**를 클릭하여 이 작업을 수동으로 수행할 수도 있습니다.

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.

개체

온프레미스 Management Center를 CDO에 온보딩하면 CDO가 온프레미스 Management Center 매니지드 디바이스에서 개체를 가져옵니다. CDO로 가져온 개체는 읽기 전용이 됩니다. 온프레미스 Management Center 개체는 읽기 전용이지만 CDO를 사용하면 온프레미스 Management Center에서 관리하지 않는 테넌트의 다른 디바이스에 개체의 복사본을 적용할 수 있습니다. 복사본은 원본 개체에서 연결 해제되므로 온프레미스 Management Center에서 가져온 개체의 값을 변경하지 않고 복사본을 편집할 수 있습니다. 온프레미스 Management Center 개체는 해당 개체 유형을 지원하는 관리하는 모든 디바이스에서 사용할 수 있습니다.

Cisco Defense Orchestrator로 온프레미스 Firewall Management Center 관리

온프레미스 Management Center에서는 다음 개체 유형을 지원합니다.

- 네트워크 개체
- 네트워크-그룹 개체

개체 문제

CDO은 온프레미스 Management Center에서 중복되거나 일치하지 않거나 사용되지 않는 개체를 식별하지 않습니다. 이러한 문제 상태를 기준으로 개체를 필터링할 수 없습니다.

이벤트

특정 이벤트에 대한 기록 및 라이브 이벤트 테이블을 검색하고 필터링하는 것은 CDO에서 다른 정보를 검색하고 필터링할 때와 동일한 방식으로 작동합니다. 자세한 내용은 Firepower Management Center 및 Cisco SaaS(Security Analytics and Logging) 통합 가이드를 참조하십시오.

Cisco Security Analytics and Logging

Cisco SaaS(Security Analytics and Logging)를 사용하면 모든 디바이스에서 연결, 침입, 파일, 맬웨어 및 보안 인텔리전스 이벤트를 캡처하고, CDO의 한 곳에서 볼 수 있습니다.

이벤트는 Cisco Cloud에 저장되며 CDO의 Event Logging(이벤트 로깅) 페이지에서 볼 수 있습니다. 여기에서 이벤트를 필터링하고 검토하여 네트워크에서 어떤 보안 규칙이 트리거되고 있는지 명확하게 이해할 수 있습니다. **Logging and Troubleshooting(**기록 및 문제 해결**)** 패키지는 이러한 기능을 제공합니다.

방화벽 분석 및 모니터링 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 Secure Cloud Analytics 포털로 교차 실행할 수 있습니다.