



FAQ 및 지원

이 장에는 다음 섹션이 포함되어 있습니다.

- [Cisco Defense Orchestrator, on page 1](#)
- [Cisco Defense Orchestrator에 디바이스 온보딩 관련 FAQ, 2 페이지](#)
- [디바이스 유형, on page 4](#)
- [보안, on page 5](#)
- [문제 해결, on page 7](#)
- [로우 터치\(Low-Touch\) 프로비저닝에 사용되는 용어 및 정의, on page 7](#)
- [정책 최적화, on page 8](#)
- [연결성, on page 8](#)
- [CLI를 사용하여 Secure Firewall Threat Defense 디바이스의 초기 구성 완료, on page 9](#)
- [데이터 인터페이스 정보, 13 페이지](#)
- [CDO가 개인 정보를 처리하는 방법, 13 페이지](#)
- [Cisco Defense Orchestrator 지원팀에 문의, on page 13](#)

Cisco Defense Orchestrator

Cisco Defense Orchestrator란 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 온보딩](#)을 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 온보드](#)를 참조하십시오.

ASA를 온보딩한 후 무엇을 해야 합니까?

시작하려면 [Cisco Defense Orchestrator로 ASA 관리](#)를 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 온보딩](#)을 참조하십시오.

클라우드사용 FirewallManagementCenter에 SecureFirewallThreatDefense 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 하나요?

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 페이지](#)를 참조하십시오.

Secure Firewall Threat Defense 문제를 어떻게 해결하나요?

[Secure Firewall Threat Defense 온보딩 문제 해결](#)을 참조하십시오.

온프레미스 Secure Firewall Management Center 관련 FAQ

온프레미스 Management Center를 온보딩하려면 어떻게 하나요?

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 온보딩](#)을 참조하십시오.

CDO에 Meraki 디바이스 온보딩 관련 FAQ

Meraki 디바이스를 온보딩하려면 어떻게 해야 하나요?

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 온보딩](#)을 참조하십시오.

CDO에 SSH 디바이스 온보딩 관련 FAQ

SSH 디바이스를 어떻게 온보딩하나요?

SSH 디바이스에 저장된 높은 권한을 가진 사용자의 사용자 이름과 암호를 사용하여 SDC(보안 디바이스 커넥터)로 디바이스를 온보딩할 수 있습니다. 시작하려면 [SSH 디바이스 온보딩](#)을 참조하십시오.

디바이스를 삭제하려면 어떻게 하나요?

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 온보딩](#)을 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.

FTD(Firepower Threat Defense)란 무엇입니까?

Cisco의 차세대 방화벽 소프트웨어 이미지. 최고의 Sourcefire 차세대 방화벽 서비스와 ASA 플랫폼을 결합하기 위해 노력합니다. 다양한 Firepower 하드웨어 디바이스 또는 가상 머신에 설치할 수 있습니다. 이것은 ASA FirePOWER 모듈과 동일하지 않습니다. 자세한 내용은 [ASA 소프트웨어 및 하드웨어 지원](#)을 참조하십시오.

FDM(Firepower Device Manager)이란 무엇입니까?

Firepower Device Manager는 FTD 이미지와 함께 제공되는 Firepower Threat Defense 관리 소프트웨어입니다. FDM은 함께 제공되는 하나의 FTD를 관리하도록 설계되었습니다. FDM을 "로컬 디바이스 관리자"라고 부르기도 합니다.

Firepower란 무엇입니까?

Firepower는 차세대 방화벽 하드웨어 및 소프트웨어 그룹을 나타내는 일반적인 용어입니다.

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](#)
- [Defense Orchestrator에서 FTD로 구성 변경 사항 배포](#)

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.

CDO는 Cisco Integrated Services Routers 및 Aggregation Services Routers를 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.

CDO가 SMA를 관리할 수 있습니까?

아니오, CDO는 현재 SMA를 관리하지 않습니다.

보안

CDO는 안전한가요?

CDO는 다음 기능을 통해 고객 데이터에 대한 엔드 투 엔드 보안을 제공합니다.

- 새 CDO 테넌트에 대한 초기 로그인
- 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 프리미엄 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 프리미엄을 떠나지 않도록 모든 인바운드 및 아웃바운드 트래픽을 제어하는 클라우드 또는 고객 자체 네트워크(로드맵)에 "보안 데이터 커넥터"를 배포하여 달성됩니다.

CDO에 처음 로그인할 때 "OTP를 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.

SDC에 추가 비용이나 라이선스가 필요합니까?

아니요.

현재 CDO에서 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

CDO에서 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.

CDO가 내 인증서를 거부하는 이유는 무엇입니까?

[Resolving New Certificates\(새 인증서 확인\)](#)을 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 새도잉되는 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 새도우 문제를 식별할 수 있습니다.



Note CDO는 완전히 새도우 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 daemon>#service docker stop
Change IP address
Start Docker daemon >#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](#)). 그런 다음 장치를 다시 연결합니다(참조 [CDO에 디바이스 대량 다시 연결](#)). 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.

CLI를 사용하여 Secure Firewall Threat Defense 디바이스의 초기 구성 완료

디바이스의 CLI에 연결하여 설정 마법사를 사용하여 관리 IP 주소, 게이트웨이 및 기타 기본 네트워킹 설정을 포함한 초기 설정을 수행합니다. 통신을 위해 모든 DNS 및 방화벽 포트에 액세스할 수 있는지 확인합니다.

전용 관리 인터페이스는 자체 네트워크 설정이 있는 특수 인터페이스입니다. 관리 인터페이스를 사용하지 않으려는 경우, 대신 CLI를 사용하여 데이터 인터페이스를 구성할 수 있습니다.

Before you begin

이 절차는 다음 시나리오에 적용됩니다.

- Firepower 1000, Firepower 2100, Secure Firewall 3100 및 ISA 3000 모델이 해당됩니다.
- 이 구성은 CLI 등록 키로 온보딩될 디바이스에 이상적입니다.



Note 로우터치 프로비저닝으로 온보딩 중인 디바이스에는 이 구성 절차를 사용하지 마십시오.

Procedure

단계 1 콘솔 포트에서 또는 관리 인터페이스에 대한 SSH를 사용하여 디바이스의 CLI에 연결합니다. 네트워크 설정을 변경하려는 경우 연결이 끊어지지 않도록 콘솔 포트를 사용하는 것이 좋습니다.

Firepower 1000, Firepower 2100, Secure Firewall 3100 모델: 콘솔 포트는 FXOS CLI에 연결됩니다. SSH 세션은 threat defense CLI에 직접 연결됩니다.

단계 2 사용자 이름 **admin** 및 비밀번호 **Admin123**으로 로그인합니다.

(Firepower 및 Secure Firewall 하드웨어 모델) 콘솔 포트에서 FXOS CLI에 연결합니다. FXOS에 처음 로그인하면 암호를 변경하라는 메시지가 표시됩니다. 이 비밀번호는 SSH의 threat defense 로그인에도 사용됩니다.

Note 비밀번호가 이미 변경된 경우 모르는 경우, 비밀번호를 기본값으로 재설정하려면 디바이스를 재 이미지화해야 합니다. Firepower 및 Secure Firewall 하드웨어 모델의 경우: [이미지 재설치 절차](#)에 대한 [FXOS 문제 해결 가이드](#)를 참고하십시오.

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1
```

```
[...]
```

```
Hello admin. You must change your password.
Enter new password: *****
Confirm new password: *****
Your password was updated successfully.
```

```
[...]
```

```
firepower#
```

단계 3 (Firepower 및 Secure Firewall 하드웨어 모델) 콘솔 포트에서 FXOS에 연결한 경우 threat defense CLI에 연결합니다.

connect ftd**Example:**

```
firepower# connect ftd
>
```

단계 4 디바이스에 처음 로그인할 경우, 엔드 유저 라이선스 계약(EULA)에 동의하고 SSH 연결을 사용 중인 경우 관리자 비밀번호를 변경하라는 메시지가 표시됩니다. 그 다음에는 CLI 설정 스크립트가 표시됩니다.

Note 이미지 재설치 등을 통해 컨피그레이션을 지우지 않으면 CLI 설정 마법사를 반복할 수 없습니다. 그러나 이러한 모든 설정은 **configure network**(네트워크 구성) 명령을 사용하여 CLI에서 나중에 변경할 수 있습니다. [threat defense 명령 참조](#)를 참조하십시오.

기본값 또는 이전에 입력한 값이 괄호 안에 표시됩니다. 이전에 입력한 값을 승인하려면 **Enter**를 누릅니다.

Note 관리 인터페이스 설정은 데이터 인터페이스에서 threat defense 액세스를 활성화한 경우에도 사용됩니다. 예를 들어 데이터 인터페이스를 통해 백플레인으로 라우팅되는 관리 트래픽은 데이터 인터페이스 DNS 서버가 아닌 관리 인터페이스 DNS 서버를 사용하여 FQDN을 확인합니다.

다음 지침을 참조하십시오.

- **Configure IPv4 via DHCP or manually?**(DHCP를 통해 또는 수동으로 IPv4를 구성하시겠습니까?) - 관리 인터페이스 대신 threat defense 액세스용 데이터 인터페이스를 사용하려면 **manual**(수동)을 선택합니다. 관리 인터페이스를 사용할 계획은 없지만 IP 주소(예: 개인 주소)를 설정해야 합니다. 관리 인터페이스가 DHCP로 설정된 경우 관리를 위해 데이터 인터페이스를 설정할 수 없습니다. 데이터 인터페이스(데이터 인터페이스)여야 하는 기본 경로(다음 글머리 기호 참조)가 DHCP 서버에서 수신한 기본 경로를 덮어 쓸 수 있기 때문입니다.

- **Enter the IPv4 default gateway for the management interface**(관리 인터페이스에 대한 IPv4 기본 게이트웨이 입력) - 관리 인터페이스 대신 threat defense 액세스에 데이터 인터페이스를 사용하면 게이트웨이를 **data-interfaces** 데이터 인터페이스(데이터 인터페이스)로 설정합니다. 이 설정은 관리 트래픽을 백플레인을 통해 전달하므로 FMC 액세스 데이터 인터페이스를 통해 라우팅될 수 있습니다.
- **If your networking information has changed, you will need to reconnect**(네트워킹 정보가 변경된 경우 다시 연결해야 합니다) — SSH를 통해 연결되어 있지만 최초 설정에서 IP 주소를 변경한 경우 연결이 끊깁니다. 새 IP 주소 및 비밀번호를 사용하여 다시 연결합니다. 콘솔 연결에는 영향을 미치지 않습니다.
- 디바이스를 로컬로 관리하시겠습니까? - 클라우드 사용 Firewall Management Center 또는 Secure Firewall device manager에서 관리할 디바이스에 대해 디바이스를 구성하려면 예를 입력합니다.
디바이스를 로컬로 관리하시겠습니까? - 온프레미스 Management Center에서 원격 관리를 위해 디바이스를 구성하려면 아니오를 입력합니다.
- **Configure firewall mode?**(방화벽 모드를 설정하시겠습니까?)—초기 설정에서 방화벽 모드를 설정하는 것이 좋습니다. 초기 설정 후에 방화벽 모드를 변경하면 실행 중인 구성이 지워집니다. 데이터 인터페이스 threat defense 액세스는 라우팅 방화벽 모드에서만 지원됩니다.

단계 5 (Optional) management center 액세스 인터페이스의 이름을 구성합니다.

configure network management-data-interface

그러면 데이터 인터페이스에 대한 기본 네트워크 설정을 구성하라는 메시지가 표시됩니다.

Note 이 명령을 사용할 때는 콘솔 포트를 사용해야 합니다. 관리 인터페이스에 SSH를 사용하는 경우 연결이 끊기고 콘솔 포트에 다시 연결해야 할 수 있습니다. SSH 사용량에 대한 자세한 내용은 아래를 참조하십시오.

이 명령 사용에 대한 자세한 내용은 다음을 참조하십시오. 자세한 내용은 [데이터 인터페이스 정보, on page 13](#)의 내용을 참조하십시오.

- 관리에 데이터 인터페이스를 사용하려는 경우 원래 관리 인터페이스에서 DHCP를 사용할 수 없습니다. 초기 설정 중에 IP 주소를 수동으로 설정하지 않은 경우 지금 **configure network {ipv4 | ipv6} manual** 명령을 사용하여 설정할 수 있습니다. 관리 인터페이스 게이트웨이를 아직 **data-interfaces**로 설정하지 않은 경우, 이 명령이 이제 설정합니다.
- Cisco Defense Orchestrator를 통해 위협 방어 관리를 위해 디바이스에 온보딩하면 Cisco Defense Orchestrator는 인터페이스 이름과 IP 주소, 게이트웨이에 대한 정적 경로, DNS 서버 및 DDNS 서버 설정을 포함하여 인터페이스 구성을 검색하고 유지 관리합니다. DNS 서버 설정에 관한 자세한 내용은 아래를 참조하십시오. 나중에 액세스 인터페이스 구성을 변경할 수 있지만, 디바이스 또는 Cisco Defense Orchestrator가 관리 연결을 재설정하지 못하게 할 수 있는 변경은 수행하지 않아야 합니다. 관리 연결이 중단되면 디바이스에 이전 구축을 복구하는 **configure policy rollback** 명령이 포함됩니다.
- 이 명령은 데이터 인터페이스 DNS 서버를 설정합니다. 설정 스크립트로 설정하거나 **configure network dns servers** 명령을 사용하여 설정한 관리 DNS 서버는 관리 트래픽에 사용됩니다. 데이터 DNS 서버는 DDNS(설정된 경우) 또는 이 인터페이스에 적용된 보안 정책에 사용됩니다.

또한 로컬 DNS 서버는 초기 등록시 DNS 서버가 검색된 경우에만 유지됩니다. 예를 들어 관리 인터페이스를 사용하여 디바이스를 등록한 다음 나중에 **configure network management-data-interface** 명령을 사용하여 데이터 인터페이스를 구성하는 경우 디바이스 구성과 일치하도록 DNS 서버를 포함하여 CDO에서 이러한 모든 설정을 수동으로 구성해야 합니다.

- Threat Defense를 통해 위협 방어 관리용 **threat defense**를 온보딩한 후 관리 인터페이스를 관리 인터페이스 또는 다른 데이터 인터페이스로 변경할 수 있습니다.
- 설정 마법사에서 설정한 FQDN이 이 인터페이스에 사용됩니다.
- 명령의 일부로 전체 디바이스 구성을 지울 수 있습니다. 복구 시나리오에서는 이 옵션을 사용할 수 있지만 초기 설정 또는 정상 작동에는 이 옵션을 사용하지 않는 것이 좋습니다.
- 데이터 관리를 비활성화하려면 **configure network management-data-interface disable** 명령을 입력합니다.

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichton:pa$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

단계 6 (Optional) 특정 네트워크에서 Cisco Defense Orchestrator에 대한 데이터 인터페이스 액세스를 제한합니다.

configure network management-data-interface client ip_address netmask

기본적으로 모든 네트워크가 허용됩니다.

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 시트](#)를 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.

프로시저

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 자동으로 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

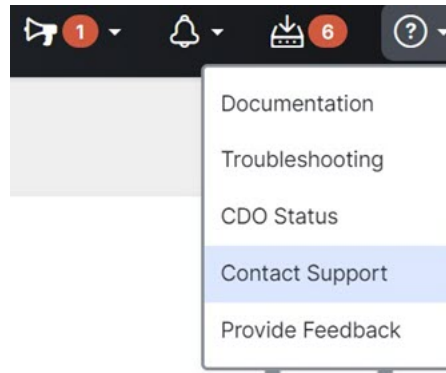
CDO 고객이 TAC로 지원 티켓을 여는 방법

이 섹션에서는 라이선스가 부여된 CDO 테넌트를 사용하는 고객이 Cisco의 TAC(Technical Assistance Center)에서 지원 티켓을 여는 방법을 설명합니다.

Procedure

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 시트](#)를 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 Manager](#)를 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.com의 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.

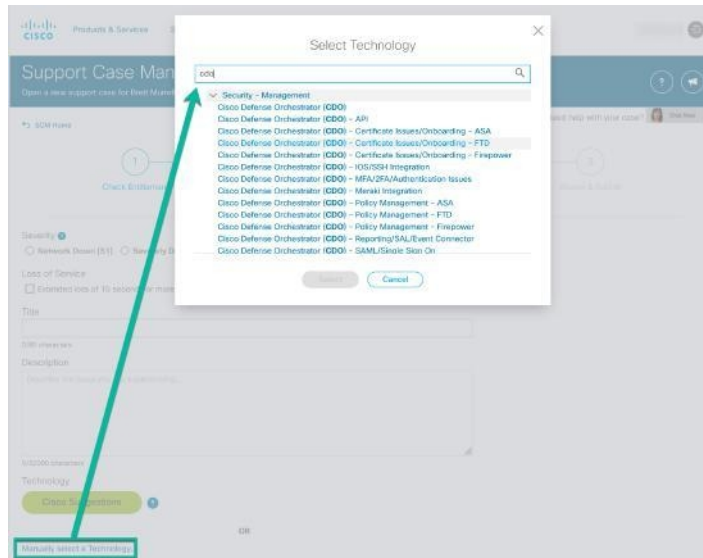
Important 중요: 아래 링크에 액세스할 수 없는 경우 공인 Cisco 파트너 또는 리셀러, Cisco 어카운트 담당자 또는 Cisco 서비스 계약 정보를 관리하는 회사 내 담당자에게 문의하십시오.

CDO 평가판 고객이 TAC를 사용하여 지원 티켓을 여는 방법

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.

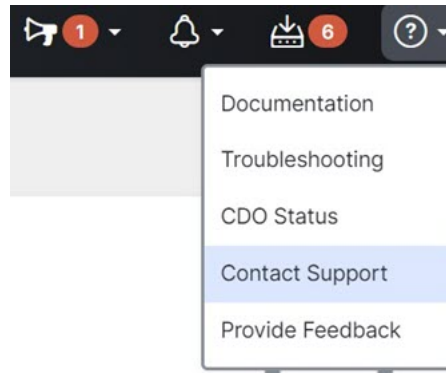
CDO 평가판 고객이 TAC를 사용하여 지원 티켓을 여는 방법

이 섹션에서는 CDO 테넌트의 무료 평가판을 사용하는 고객이 Cisco TAC(Technical Assistance Center)에서 지원 티켓을 여는 방법에 대해 설명합니다.

프로시저

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.

번역에 관하여

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