



## Secure Firewall Threat Defense를 클라우드로 마이그레이션

- [Secure Firewall Management Center에서 클라우드로 Secure Firewall Threat Defense 마이그레이션, 1 페이지](#)
- [마이그레이션 절차, 9 페이지](#)
- [위협 방어 마이그레이션 작업 보기, 12 페이지](#)
- [클라우드로의 FTD 마이그레이션 문제 해결, 17 페이지](#)

## Secure Firewall Management Center에서 클라우드로 Secure Firewall Threat Defense 마이그레이션

Cisco Defense Orchestrator을 사용하면 CDO 관리자 권한이 있는 사용자는 management center에서 클라우드로 위협 방어 디바이스를 마이그레이션할 수 있습니다.

위협 방어 디바이스에서 마이그레이션 프로세스를 시작하기 전에 해당 디바이스와 연결된 management center가 CDO에 이미 온보딩되어 있어야 합니다.

위협 방어를 클라우드로 마이그레이션할 때 CDO는 디바이스를 온보딩하고 모든 공유 정책 및 관련 개체, 디바이스별 정책 및 디바이스 구성을 management center에서 CDO로 가져옵니다.



**참고** CDO는 management center 마이그레이션 프로세스 중에 식별된 모든 중복 정책 및 개체 이름을 처리합니다. 이 동작은 이 문서의 뒷부분에 자세히 설명되어 있습니다.

이벤트 및 분석 관리는 CDO로 전송되거나 management center와 함께 유지될 수 있습니다.

마이그레이션을 수행한 후에는 14일 이내에 변경 사항을 평가할 수 있습니다. 평가 기간에는 특정 작업을 수정 또는 변경하거나 이러한 디바이스의 관리를 다시 관리 센터로 변경할 수 있습니다. 평가 기간이 지나면 변경 사항을 되돌릴 수 없습니다.

## 지원되는 소프트웨어

이 섹션에서는 마이그레이션을 위한 최소 소프트웨어 요구 사항에 대해 설명합니다.

- Management Center: 7.2
- Secure Firewall Threat Defense:
  - 7.0.3 이상
  - 7.2 이상




---

참고 소프트웨어 버전 7.1을 실행하는 위협 방어에서는 이 지원이 제공되지 않습니다.

---

## 라이센싱

- 위협 방어가 클라우드로 마이그레이션되면 디바이스와 연결된 모든 기능 라이선스가 CDO로 전송되고 management center에서 스마트 라이선스 풀로 릴리스됩니다. 디바이스는 CDO에 등록하는 동안 디바이스별 라이선스를 회수합니다. 디바이스에 라이선스를 다시 적용할 필요가 없습니다.
- 분석을 위해 디바이스를 management center에 유지하려는 경우에는 디바이스별 라이선스가 필요하지 않습니다.
- 클라우드 사용 Firewall Management Center를 스마트 라이선스로 등록했는지 확인합니다.

## 지원 기능

공유 정책 및 개체 처리

마이그레이션 프로세스가 시작되면 위협 방어 디바이스와 연결된 공유 정책 및 관련 개체를 먼저 가져온 다음 디바이스 구성을 가져옵니다.

위협 방어 디바이스에서 관리자를 변경한 후 다음 공유 정책을 CDO로 가져옵니다.

- 액세스 제어
- IPS
- SSL
- 사전 필터
- NAT
- QoS

- Identity
- 플랫폼 설정
- Flex 설정
- 네트워크 분석
- DNS
- 악성코드 및 파일
- 상태
- 원격 액세스 VPN

CDO의 정책 또는 개체가 Secure Firewall Management Center에서 가져온 정책 또는 개체와 이름이 동일한 경우 CDO는 관리를 성공적으로 변경한 후 다음 작업을 수행합니다.

정책, 개체	조건	조치
액세스 제어, SSL, IPS, 사전 필터, NAT, QoS, ID, 플랫폼 설정, 네트워크 분석, DNS, 악성코드 및 파일 정책.	클라우드 사용 Firewall Management Center 정책의 이름이 management center 정책과 일치합니다.	management center에서 가져온 정책 대신 클라우드 사용 Firewall Management Center 정책이 사용됩니다.
RA VPN 기본 그룹 정책 <b>DfltGrpPolicy</b>	management center의 기본 그룹 정책인 <b>DfltGrpPolicy</b> 는 무시됩니다.	기존 클라우드 사용 Firewall Management Center 기본 그룹 정책인 <b>DfltGrpPolicy</b> 가 대신 사용됩니다.
네트워크, 포트 개체	클라우드 사용 Firewall Management Center에 있는 네트워크 및 포트 개체의 이름과 콘텐츠가 management center에 있는 개체와 일치합니다.	management center에서 가져온 개체 대신 이름과 콘텐츠가 동일한 기존 클라우드 사용 Firewall Management Center 네트워크 및 포트 개체가 사용됩니다.  개체의 이름은 같지만 콘텐츠가 다른 경우 개체 재정의가 생성됩니다. <a href="#">개체 오버라이드</a> 를 참조하십시오.
기타 모든 개체		management center에서 가져온 개체 대신 기존 클라우드 사용 Firewall Management Center 개체가 사용됩니다.

액세스 제어 정책과 연결된 모든 시스템 로그 알림 개체를 Cisco Defense Orchestrator로 가져옵니다.

고가용성 쌍의 위협 방어에 대한 마이그레이션 지원

고가용성 쌍으로 디바이스를 마이그레이션할 수 있습니다. 액티브 및 스탠바이 디바이스의 디바이스 관리가 변경되고 CDO로 가져옵니다.



**중요** 마이그레이션 중인 디바이스에서 HA 구성 생성 또는 HA 해제와 같은 고급 작업을 수행하기 전에 관리자 변경 사항을 커밋하는 것이 좋습니다.

평가 기간 동안 이러한 작업을 수행하는 것은 지원되지 않으며 의도하지 않은 동작이 발생할 수 있습니다.

고가용성 쌍의 **Management Center**에 대한 마이그레이션 지원

구성된 management center 고가용성에서 클라우드로 위협 방어 디바이스를 마이그레이션할 수 있습니다.

management center는 SDC 방법으로 SecureX 또는 자격 증명을 사용하여 온보딩할 수 있습니다. 항상 스탠바이가 아닌 액티브 관리 센터를 온보딩합니다.



**참고** 독립형 관리 센터를 이미 온보딩하고 나중에 스탠바이 관리 센터로 구성한 경우, 스탠바이 관리 센터를 삭제하고 액티브 관리 센터를 온보딩합니다.

기억해야 할 사항:

- **SecureX** 온보딩 방법
  - 14일 평가 기간에는 고가용성 중단이 지원되지 않습니다. 평가 기간 후 수동으로 또는 자동으로 변경 사항을 커밋한 후 고가용성을 해제할 수 있습니다.
  - 고가용성 전환은 14일 평가 기간 동안 지원됩니다.
- **SDC**를 사용하는 자격 증명 온보딩 방법
  - 고가용성 중단 또는 고가용성 전환은 14일 평가 기간 동안 지원되지 않습니다. 변경 사항을 수동으로 커밋한 후 또는 평가 기간 후 자동으로 이러한 작업을 수행할 수 있습니다.
  - 전환 후에는 이전에 대기 모드였던 새 액티브 유닛을 온보딩한 다음 디바이스에서 마이그레이션 작업을 시작합니다.

## 지원되지 않는 기능

다음 조건에서는 FTD를 클라우드로 마이그레이션 화면에서 클라우드로의 디바이스 마이그레이션이 허용되지 않습니다.

- 클러스터의 디바이스 부분입니다.

- management center에 분석 전용으로 등록된 디바이스입니다.

다음 구성은 마이그레이션의 일부로 management center에서 CDO로 가져오지 않습니다.

- 맞춤형 위젯, 애플리케이션 탐지기, 상관관계, SNMP 및 이메일 알림, 스캐너, 그룹, Dynamic Access Policy, 맞춤형 AMP 구성, 사용자, 도메인, 예약된 구축 작업, ISE 구성, 예약된 GeoDB 업데이트, Threat Intelligence Director 구성, 동적 분석 연결.
- ISE 내부 인증서 개체는 마이그레이션의 일부로 가져오지 않습니다. ISE에서 새 시스템 인증서 또는 인증서와 관련 개인 키를 내보내고 CDO로 가져와야 합니다.

### Secure Firewall 권장 규칙

위협 방어를 클라우드로 마이그레이션하면 침입 정책과 연결된 보안 방화벽 IPS 권장 규칙을 가져옵니다. 그러나 클라우드 사용 Firewall Management Center는 마이그레이션 후 새로 고침 스케줄러가 실행될 때 이러한 규칙을 자동으로 업데이트하지 않습니다. [자동 Cisco 권장 규칙](#)을 참조하십시오.

### 사용자 지정 네트워크 분석

디바이스가 사용자 지정 네트워크 분석 정책과 연결된 경우 마이그레이션하기 전에 온프레미스에서 이 정책에 대한 모든 참조를 제거해야 합니다.

1. 온프레미스 management center에 로그인합니다.
2. **Policies(정책) > Access Control(액세스 제어)**을 선택합니다.
3. 사용자 지정 NAP의 연결을 해제하려는 액세스 제어 정책에서 편집 아이콘을 클릭한 다음 **Advanced(고급)** 탭을 클릭합니다.
4. **Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 영역에서 편집 아이콘을 클릭합니다.
5. **Default Network Analysis Policy(기본 네트워크 분석 정책)** 목록에서 시스템 제공 정책을 선택합니다.
6. **OK(확인)**를 클릭합니다.
7. **Save(저장)**를 클릭하여 변경 사항을 저장한 다음 **Deploy(구축)**를 클릭하여 변경 사항을 디바이스에 다운로드합니다.

마이그레이션 후 CDO에서 네트워크 분석 정책을 수동으로 생성할 수 있습니다.

## VPN 구성 마이그레이션 지침 및 제한 사항

VPN 구성을 사용하여 디바이스를 마이그레이션할 때는 다음 사항에 유의하십시오.

원격 액세스 **VPN** 정책에 대한 마이그레이션 지원

CDO는 마이그레이션의 일부로 원격 액세스 VPN 정책의 모든 설정을 가져옵니다.

마이그레이션 프로세스의 일부로 CDO는 다음을 제외하고 원격 액세스 VPN 정책의 모든 설정을 가져옵니다.

- 개체 오버라이드는 가져오지 않습니다.

주소 풀 개체에서 오버라이드가 사용되는 경우 마이그레이션 후 CDO를 사용하여 가져온 개체에 수동으로 추가해야 합니다. **개체 오버라이드**를 참조하십시오.

- 로컬 사용자는 가져오지 않습니다.

인증 서버가 사용자 인증을 위한 로컬 데이터베이스로 구성된 경우 연결된 로컬 영역 개체를 CDO로 가져옵니다. 그러나 마이그레이션 후 CDO를 사용하여 가져온 로컬 영역 개체에 로컬 사용자를 수동으로 추가해야 합니다. **영역 및 영역 디렉터리 생성**을 참조하십시오.

- VPN 로드 밸런싱 구성은 마이그레이션되지 않습니다.

- 도메인 구성이 포함된 RA VPN 인증서 등록을 가져오지 않았습니다.

마이그레이션 후 다음을 수행할 수 있습니다.

1. CDO에서 **Inventory(재고 목록) > FTD**를 클릭합니다.
2. 마이그레이션된 FTD를 선택하고 오른쪽의 **Device Management(디바이스 관리)**에서 **Device Overview(디바이스 개요)**를 클릭합니다.
3. **Devices(디바이스) > Certificates(인증서)**를 선택합니다.

다음 중 하나를 수행하십시오.

- 인증서를 오류 상태로 가져온 경우 **Refresh certificate status(인증서 상태 새로 고침)** 아이콘을 클릭하여 인증서 상태를 디바이스와 동기화합니다. 인증서 상태가 녹색으로 바뀝니다.
- 인증서를 가져오지 않은 경우 **management center**에 구성된 RA VPN 정책에 정의된 인증서를 수동으로 추가해야 합니다

## 사용자 역할

마이그레이션 후에는 CDO에서 관리 센터의 사용자 역할이 더 이상 적용되지 않습니다. 작업 수행 권한은 CDO에서 사용자 역할을 기반으로 합니다.

CDO 사용자 역할	설명
CDO 관리자	Super Admin and Admin(슈퍼 관리자 및 관리자) 사용자는 제품의 모든 항목에 액세스할 수 있습니다. 이 사용자는 모든 정책 및 개체를 생성, 읽기, 수정 및 삭제할 수 있으며 디바이스에 구축할 수 있습니다.

CDO 사용자 역할	설명
CDO 구축 전용	Deploy Only(구축 전용) 사용자는 디바이스 또는 여러 디바이스에 단계적 변경 사항을 구축하는 모든 정책 및 개체를 볼 수 있습니다.
CDO 편집 전용	Edit Only(편집 전용) 사용자는 정책 및 개체를 수정하고 저장할 수 있지만 디바이스에 구축할 수는 없습니다.
CDO 읽기 전용	Read-Only(읽기 전용) 사용자는 모든 정책 및 개체를 볼 수 있지만 디바이스에 구축할 수는 없습니다.

## Threat Defense 이벤트 및 분석 관리

이벤트 및 분석 관리는 **management center**에서 유지되거나 CDO로 전송될 수 있으며, 여기서 CDO로 이벤트를 전송하도록 디바이스를 구성해야 합니다. 마이그레이션 프로세스를 시작하는 동안 분석을 위해 디바이스 이벤트를 전송할 관리자를 선택할 수 있습니다.

분석을 위해 **management center**를 선택하는 경우 CDO는 선택한 디바이스의 관리자가 되지만 분석 전용 모드에서는 해당 디바이스의 복사본을 **management center**에 유지합니다. 디바이스는 계속해서 **management center**에 이벤트를 전송하고 CDO는 구성 변경 사항을 관리합니다.

분석을 위해 CDO를 선택한 경우 CDO는 선택한 디바이스의 관리자가 되고 **management center**에서 이러한 디바이스를 삭제합니다. CDO는 구성 변경과 이벤트 및 분석 관리를 모두 관리합니다. Cisco Cloud에 이벤트를 전송하려면 위협 방어 디바이스를 구성해야 합니다. 보안 서비스 익스체인지 또는 SEC(Secure Event Connector)를 사용하여 디바이스에서 클라우드의 Cisco SAL(Secure Analytics and Logging)로 이벤트를 전송할 수 있습니다.

## 알림 설정 활성화

위협 방어 디바이스를 CDO로 마이그레이션할 때 테넌트와 연결된 디바이스가 특정 작업을 수행할 때마다 CDO에서 이메일 알림을 받도록 구독할 수 있습니다.

FTD를 클라우드로 마이그레이션 작업 중에 다음 상태에 대한 알림을 수신하도록 활성화하면 CDO가 이메일을 전송합니다.

- **Failed(실패)**: 마이그레이션 작업이 실패한 경우입니다.
- **Started(시작됨)**: 마이그레이션 작업이 시작된 경우입니다.
- **Succeeded(성공)**: 마이그레이션 작업이 성공적으로 완료된 경우입니다.
- **Commit Pending(커밋 보류 중)**: 관리자 변경 사항이 커밋된 경우입니다.

알림 설정을 활성화하려면 [알림 설정](#)을 참조하십시오.

## 클라우드 사용 Firewall Management Center와의 Threat Defense 연결 확인

이 섹션에서는 클라우드 사용 Firewall Management Center와의 위협 방어 연결을 확인하는 명령을 제공합니다.

디바이스에서 인터넷 연결을 확인합니다.

**ping system** <any OpenDNS server address> 명령을 실행하여 디바이스가 인터넷에 연결할 수 있는지 여부를 확인합니다.

1. 콘솔 포트 또는 SSH를 사용하여 디바이스의 CLI에 연결합니다.
2. 관리자 사용자 이름 및 비밀번호로 로그인합니다.
3. **ping system** <OpenDNS IPAddress>를 입력합니다.

```
ping system 208.67.222.222
PING 208.67.222.222 (208.67.222.222) 56(84) bytes of data.
64 bytes from 208.67.222.222: icmp_seq=1 ttl=48 time=22.10 ms
64 bytes from 208.67.222.222: icmp_seq=2 ttl=48 time=22.10 ms
64 bytes from 208.67.222.222: icmp_seq=3 ttl=48 time=22.8 ms
64 bytes from 208.67.222.222: icmp_seq=4 ttl=48 time=22.6 ms
^C
--- 208.67.222.222 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 22.588/22.841/22.995/0.223 ms
```

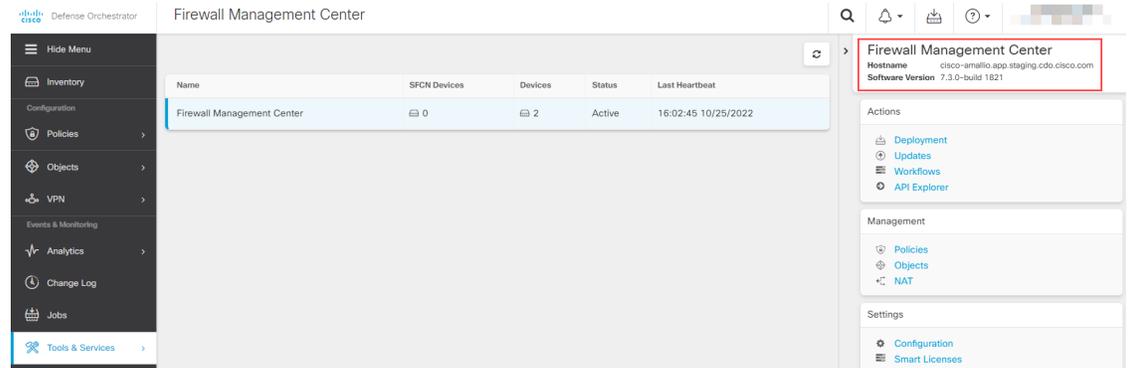
위의 예는 디바이스가 OpenDNS 서버 IP 주소를 사용하여 인터넷에 연결할 수 있음을 보여줍니다. 또한 전송된 패킷의 수가 수신된 것과 동일하며, 이는 디바이스에서 인터넷 연결을 사용할 수 있음을 나타냅니다. 이는 디바이스가 인터넷에 연결할 수 있음을 나타냅니다.



참고 결과가 일치하지 않으면 인터넷 연결을 수동으로 확인합니다.

클라우드 사용 Firewall Management Center으로 디바이스 연결을 확인합니다.

1. 클라우드 사용 Firewall Management Center의 호스트 이름을 가져옵니다.
  1. CDO 탐색 창에서 **Tools & Services**(툴 및 서비스) > **Firewall Management Center**를 클릭합니다.
  2. **Firewall Management Center**를 클릭하여 오른쪽 창에서 상세정보를 확인합니다.
  3. **Hostname**(호스트 이름) 필드에 다음 예시 이미지에 표시된 호스트 이름만 복사합니다.



위의 그림에서 강조 표시된 텍스트는 복사할 FMC의 호스트 이름(*cdo-acc10.app.us.cdo.cisco.com*)입니다.

2. 콘솔 포트 또는 SSH를 사용하여 디바이스의 CLI에 연결합니다.
3. **ping system** <hostname of the FMC>을 입력합니다.

```
ping system cdo-acc10.app.us.cdo.cisco.com
PING cdo-acc10.app.us.cdo.cisco.com (54.187.125.161) 56(84) bytes of data.
^C
--- cdo-acc10.app.us.cdo.cisco.com ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 64ms
```

위의 예에서는 호스트 이름이 IP 주소로 확인되어 연결에 성공했음을 나타냅니다. 응답에 표시되는 "100% packet loss(100% 패킷 손실)" 메시지를 무시하십시오.




---

참고 호스트에 연결할 수 없는 경우 **configure network dns** <address>를 사용하여 CLI에서 DNS 구성을 수정할 수 있습니다.

---

## 마이그레이션 절차

시작하기 전에

프로세스를 시작하기 전에 다음 사전 요구 사항을 충족하는지 확인합니다.

- 프로비저닝된 CDO 테넌트입니다.
- CDO이 스마트 라이선스에 등록되어 있습니다.
- management center이 CDO에 온보딩됩니다. management center 온보딩은 해당 management center에 등록된 모든 위협 방어 디바이스도 온보딩합니다. [FMC 온보딩](#)을 참조하십시오.



**참고** management center에서 온보딩을 위해 관리자 역할 또는 "디바이스" 및 "시스템" 권한이 있는 맞춤형 사용자 역할의 새 사용자를 생성합니다.



**주의** 온프레미스 Management Center를 CDO에 온보딩하는 동시에 동일한 사용자 이름으로 온프레미스 Management Center management center에 로그인하면 온보딩이 실패합니다.

- 위협 방어 디바이스가 동기화되어야 하며 보류 중인 변경 사항이 없어야 합니다. CDO가 디바이스에서 보류 중인 변경 사항을 식별하는 경우 해당 디바이스에서 마이그레이션 작업이 실패합니다.
- Management Center은 아웃바운드 HTTP/HTTPS가 구성을 Amazon S3에 업로드하도록 허용해야 합니다.
- CDO는 management center에서 액세스 제어 정책에 사용된 시스템 로그 알림 개체를 가져옵니다. CDO에 이름은 동일하지만 유형(SNMP, 이메일)이 다른 알림 개체가 이미 포함되어 있으면 구성 가져오기 중에 재사용됩니다.

사용자는 시스템 로그 개체 이름이 CDO의 기존 SNMP 또는 이메일 알림 개체와 일치하는지 확인해야 합니다. 이름이 일치하는 경우, 마이그레이션 프로세스를 시작하기 전에 온프레미스 management center에서 시스템 로그 개체의 이름을 변경해야 합니다.

- 수정된 시스템 정의 FlexConfig 텍스트 개체가 있는 방화벽을 온프레미스 Management Center에서 클라우드 사용 Firewall Management Center로 마이그레이션하려고 하면, 수정된 시스템 정의 FlexConfig 텍스트 개체의 값은 클라우드 사용 Firewall Management Center로 마이그레이션되지 않으며 구축이 실패합니다.

이를 방지하려면 마이그레이션을 시작하기 전에 다음 작업을 수행하십시오.

- 마이그레이션 전에 수정된 시스템 정의 FlexConfig 텍스트 개체 값을 온프레미스 Management Center에서 클라우드 사용 Firewall Management Center로 복사합니다.
- 사전 정의된 FlexConfig 텍스트 개체를 확인한 후 온프레미스 Management Center에서 클라우드 사용 Firewall Management Center로 마이그레이션을 시작합니다.

## 프로시저

**단계 1** 왼쪽의 탐색 모음에서 **Tools & Services(툴 및 서비스) > Migrations(마이그레이션) > FTD**를 클라우드로 마이그레이션을 클릭합니다.

**단계 2**  아이콘을 클릭하여 위협 방어 마이그레이션 프로세스를 시작합니다.

**참고** 한 번에 하나의 마이그레이션 작업만 시작할 수 있습니다.

단계 3 온프레미스 FMC 선택 단계에서 다음을 수행합니다.

1. 아직 수행하지 않은 경우 **Onboard FMC(FMC 온보딩)** 링크를 클릭하여 온프레미스 management center를 온보딩할 수 있습니다. **FMC 온보딩**을 참조하십시오.
2. 사용 가능한 목록에서 management center를 선택하고 **Next(다음)**를 클릭합니다.

**Select Devices(디바이스 선택)**단계에서는 management center에서 관리하는 위협 방어 디바이스를 확인할 수 있습니다.

**Last Synced time(마지막 동기화 시간)** 필드는 디바이스 구성이 management center에 동기화된 이후 경과한 시간을 나타냅니다. **Sync from OnPrem FMC Now(지금 OnPrem FMC에서 동기화)**를 클릭하여 최신 디바이스 변경 사항을 가져올 수 있습니다.

단계 4 디바이스 선택 단계에서 다음을 수행합니다.

- a) 마이그레이션할 디바이스를 선택합니다.

**Migrate FTD to Cloud**  
Migrate FTD Manager from Firewall Management Center to CDO

1 Select OnPrem FMC **OnPrem FMC: FMC\_OnPrem**

2 Select Devices

Select FTD devices to migrate to cloud from OnPrem FMC to CDO and specify an action in bulk or per device.

1 device(s) selected Multi-Device Action Retain on OnPrem FMC for Analytics

	Name	Domain	Action
<input type="checkbox"/>	FMC_OnPrem_192.168.0.31	Global	Retain on OnPrem FMC for Analytics
<input checked="" type="checkbox"/>	FMC_OnPrem_192.168.0.32	Global	Retain on OnPrem FMC for Analytics

Displaying 2 of 2 results

**Migrate FTD to Cloud**

- 참고
- 지원되지 않는 버전에서 실행 중인 디바이스는 선택할 수 없습니다.
  - management center에 분석용으로만 등록되었거나 구축에 보류 중인 변경 사항이 있는 디바이스는 마이그레이션할 수 없습니다.
  - CDO에서는 고가용성 쌍의 액티브 디바이스만 선택할 수 있습니다. 액티브 디바이스의 관리자가 성공적으로 변경되면 CDO는 스탠바이 디바이스의 관리자를 자동으로 변경하고 디바이스의 고가용성 구성을 유지합니다.

- b) **Multi-Device Action(다중 디바이스 작업)** 목록에서 모든 디바이스에 적용할 공통 작업을 선택할 수 있습니다.

- c) **Commit Action**(커밋 작업) 옆에서 선택한 디바이스에 대해 다음 작업 중 하나를 선택할 수 있습니다.
- **Retain on OnPrem FMC for Analytics**(분석을 위해 **OnPrem FMC**에 유지): 마이그레이션 프로세스가 완료되면 선택한 위협 방어 디바이스에 대한 분석 관리가 **management center**에 유지됩니다.
  - **Delete FTD from OnPrem FMC**(**OnPrem FMC**에서 **FTD** 삭제): 마이그레이션 프로세스가 완료되면 선택한 디바이스가 **management center**에서 제거되고 **CDO**에서 분석을 처리할 수 있습니다. 분석 관리를 위해 이벤트를 **CDO**에 전송할 디바이스를 구성해야 합니다. **management center**에서 삭제된 디바이스는 취소할 수 없습니다.
- 참고 변경 사항이 자동 또는 수동으로 커밋되지 않는 한 디바이스는 **management center**에서 삭제되지 않습니다.

참고 여기에 지정된 작업은 14일의 평가 기간 후 또는 변경 사항을 수동으로 커밋한 후에 자동으로 커밋됩니다.

단계 5 **Migrate FTD to Cloud**(**FTD**를 클라우드로 마이그레이션)를 클릭합니다.

단계 6 **View Migration to Cloud Progress**(클라우드로의 마이그레이션 진행률 보기)를 클릭하여 작업의 진행 상황을 확인합니다.

다음에 수행할 작업

마이그레이션 작업의 전체 및 개별 상태를 보고 작업이 성공적으로 완료되면 보고서를 생성할 수 있습니다. [위협 방어 마이그레이션 작업 보기](#), 12 페이지의 내용을 참조하십시오.

## 위협 방어 마이그레이션 작업 보기

**CDO**에서 시작된 모든 마이그레이션 작업의 상태를 확인할 수 있습니다. 작업을 확장하여 **management center**와 연결된 개별 디바이스의 상태를 확인할 수 있습니다.

디바이스 워크플로우에 대한 알림을 **알림 설정 활성화**한 경우, 알림 아이콘  을 클릭하여 마이그레이션 중에 발생한 알림을 확인합니다. **CDO**에서 이메일 알림을 수신하도록 구독한 경우에도 이메일 알림을 받게 됩니다.

마이그레이션 작업이 성공하면 14일 이내에 **CDO**를 사용하여 디바이스를 평가할 수 있습니다. 이 기간 동안 특정 작업을 수정 또는 변경하거나 이러한 디바이스의 관리를 다시 **management center**로 변경할 수 있습니다.

마이그레이션 변경 사항이 확실하다면 디바이스를 수동으로 커밋하는 것이 좋습니다. **CDO**는 평가 기간이 만료되면 사용자의 추가 작업 없이 변경 사항을 자동 커밋합니다. 커밋 작업은 변경 사항을 디바이스에 적용합니다. [수동으로 관리자 변경 사항 커밋](#), 16 페이지를 참조하십시오.

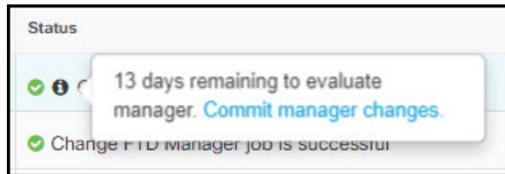
변경 사항이 커밋되면 창에 지정된 작업을 취소할 수 없습니다.



**중요** 평가 기간에 CDO를 사용하여 변경 사항을 적용하고 디바이스에 구축할 수 있습니다. 디바이스 관리를 다시 **management center**로 되돌리도록 선택하는 경우, 평가 기간 동안 적용된 CDO 관련 변경 사항은 관리자를 되돌린 후 디바이스에 유지되지 않습니다. 관리자를 되돌린 후 온프레미스 **management center**에서 디바이스로 변경 사항을 구축해야 합니다.

- **Name(이름)**: 작업이 시작된 날짜 및 시간과 **management center** 이름을 표시하는 작업 이름을 나타냅니다.
- **Number of FTDs(FTD 수)**: 클라우드로 마이그레이션되는 총 디바이스 수를 표시합니다.
- **Status(상태)**: 작업의 상태를 표시합니다. 작업을 확장하여 개별 디바이스의 상태를 확인합니다.

작업이 성공적으로 완료되면 **Status(상태)** 열에 **FTD Migration job is successful(FTD 마이그레이션 작업이 성공했습니다)** 메시지가 나타납니다. 톨팁을 클릭하여 남은 관리자 평가 일수를 확인할 수 있습니다.



수동으로 관리자 변경 사항 커밋을 클릭하여 14일 평가 기간이 끝나기 전에 변경 사항을 수동으로 커밋할 수 있습니다.

- **Last Update(마지막 업데이트)**: 디바이스가 변경된 경우에만 날짜 및 시간이 업데이트됩니다.
- **Actions(작업)**:
  - **Workflows(워크플로우)**: 작업을 모니터링할 수 있는 워크플로우 페이지로 연결되는 링크를 제공합니다. [워크플로우 페이지](#)를 참조하십시오.
  - **Download Report(보고서 다운로드)**: 성공적으로 완료된 모든 작업의 보고서를 생성하고 다운로드할 수 있습니다. [위협 방어 마이그레이션 보고서 생성, 15 페이지](#)를 참조하십시오.
  - **Commit Manager Changes(관리자 변경 사항 커밋)**: 평가 기간이 끝나기 전에 변경 사항을 디바이스에 수동으로 적용할 수 있습니다. [수동으로 관리자 변경 사항 커밋, 16 페이지](#)를 참조하십시오.
  - **Remove Migration Job(마이그레이션 작업 제거)**: 완료된 작업을 제거할 수 있습니다. 링크는 완료된 작업에만 사용할 수 있습니다.

마이그레이션이 성공적으로 완료되면 CDO에서 구성을 디바이스에 구축합니다. 구축할 변경 사항에서 오류나 경고를 식별하면 시스템은 **Validation Messages(검증 메시지)** 창에 이를 표시합니다. 전체 세부 사항을 보려면 경고 또는 오류 앞에 있는 화살표 아이콘을 클릭합니다. 구축이 실패하는 경우, [Firewall Management Center 디바이스 구성 가이드 X,Y](#)의 구성 변경 사항 구축 모범 사례 섹션을 참조하십시오.



중요 14일 평가 기간 중에는 CDO에서 디바이스 또는 OnPrem FMC를 삭제할 수 없습니다. 다음 중 하나를 수행한 후 디바이스 또는 OnPrem FMC를 삭제합니다.

- 삭제할 OnPrem FMC 또는 디바이스와 연결된 [마이그레이션 작업 제거](#)를 수행합니다.
- **Revert Manager to OnPrem FMC**(관리자를 온프레미스 FMC로 되돌리기) 및 [수동으로 관리자 변경 사항 커밋](#)을 선택합니다.

## ID 정책에 대한 영역 시퀀스 구성

디바이스에 영역 또는 ISE 구성의 ID 정책이 포함된 경우 ID 소스와 통신하기 위해 CDO에 대한 프록시 시퀀스를 구성합니다. CDO가 ID 영역에 연결하지 못하면 ID 정책이 작동하지 않습니다.

추가 구성이 필요한 디바이스에 대한 툴팁이 **Status(상태)** 열에 나타납니다.



1. 툴팁 아이콘을 클릭한 다음 **Learn more**(자세한 정보)를 클릭합니다.
2. **Configure Proxy**(프록시 구성) 창에서 **Configure my realms**(내 영역 구성)를 클릭합니다.

프록시 시퀀스를 추가하려면 [Firepower Management Center 디바이스 구성 가이드, 7.2](#)의 프록시 시퀀스 생성 섹션을 참조하십시오.

## 분석 전용 위협 방어 디바이스 예

CDO는 분석을 위해 management center에 유지하도록 구성된 동일한 디바이스의 인스턴스 2개를 생성합니다.

Inventory

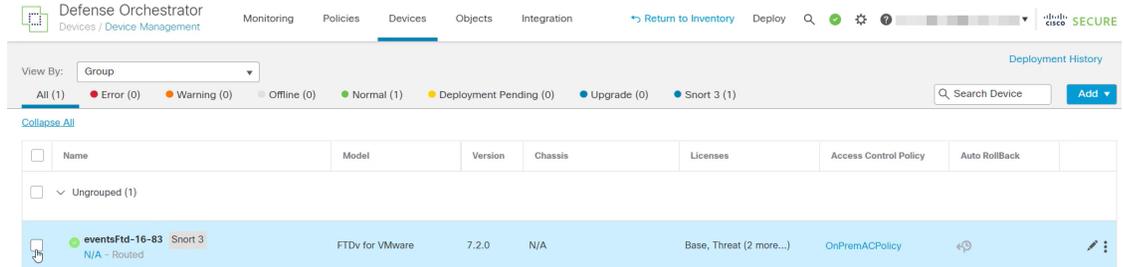
Devices Templates Search by Device Name, IP Address, or Serial Number Displaying 6 of 6 results

Name	Version	Location	Access Policy	Last Deploy	Configuration Status	Connectivity
10.10.16.13 FTD	7.2.0	-	test-policy-1855	-	Synced	Online
FMC_Beta2_OnPremFTD-141 FMC FTD	7.2.0	...:443		-	Synced	Online
FMC_Beta2_OnPremFTD-146 FMC FTD	7.2.0	...:443		-	Synced	Online
FMC_Beta2_OnPremFTD136 FMC FTD	7.2.0	...:443		-	Synced	Online
FMC_Beta2_eventsFtd-16-83 FMC FTD - Analytics Only	7.2.0	...:443		-	Synced	Online
eventsFtd-16-83 FTD	7.2.0	-	OnPremACPolicy	-	Synced	Online

**FMC FTD** 및 **Analytics Only**(분석 전용) 레이블이 있는 디바이스 인스턴스는 management center가 분석을 처리함을 보여줍니다. **FTD** 레이블이 있는 디바이스 인스턴스는 CDO가 구성을 관리함을 나타냅니다.

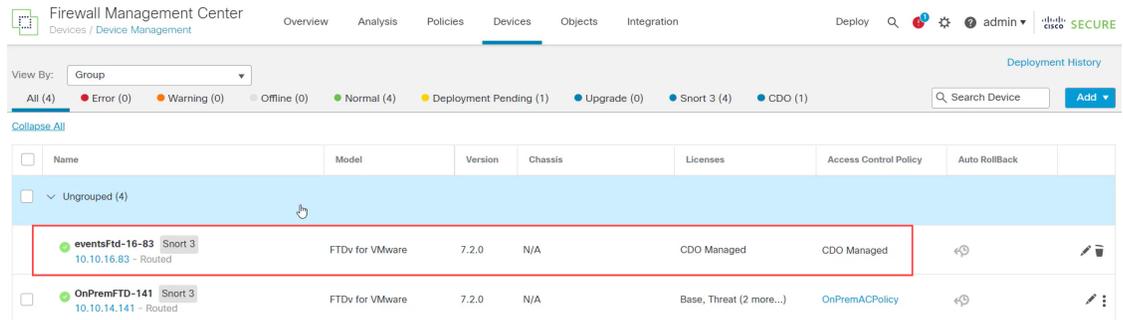
CDO를 사용하여 디바이스의 구성을 관리할 수 있습니다. 클라우드 사용 Firewall Management Center에서 디바이스를 확인하려면 다음을 수행합니다.

**FTD** 레이블이 있는 디바이스를 선택하고 오른쪽의 **Management(관리)** 창에서 **Device Summary(디바이스 요약)**를 클릭합니다.



management center에서 디바이스의 이벤트를 볼 수 있습니다. 이벤트를 보려면 다음을 수행합니다.

1. **FMC FTD 및 Analytics Only(분석 전용)** 레이블이 있는 디바이스를 선택하고 오른쪽에서 **Manage Devices(디바이스 관리)** 링크를 클릭합니다.
2. 온프레미스 management center에 로그인합니다.
3. **Devices(디바이스) > Device Management(디바이스 관리)**를 클릭합니다.



CDO가 구성을 관리하므로 이 디바이스를 선택할 수 없습니다. management center에 이 디바이스의 **CDO Managed(CDO 매니지드)** 레이블이 표시됩니다.

management center에서 라이브 이벤트를 보려면 **Analysis(분석) > Events(이벤트)**를 클릭합니다.

## 위협 방어 마이그레이션 보고서 생성

마이그레이션 작업이 성공하면 PDF 형식으로 보고서를 생성하고 다운로드하여 관리 센터에서 CDO로 가져온 모든 매개변수의 값을 분석할 수 있습니다. 보고서는 작업과 연결된 각 디바이스의 세부 정보를 제공합니다. 세부 정보에는 디바이스, 공유 정책 값, 개체, 라우팅 세부 정보, 인터페이스, 네트워크 설정 등에 대한 정보가 포함됩니다.

마이그레이션 작업 페이지에서 완료된 작업의 **Actions(작업)** 열 아래에 있는 **...** 을 클릭한 다음 **Download Report(보고서 다운로드)**를 클릭합니다..

## 수동으로 관리자 변경 사항 커밋

변경 사항에 동의하고 CDO가 변경 사항을 자동 커밋할 때까지 기다리지 않는 경우 관리자 변경 사항을 수동으로 커밋하는 것이 좋습니다. 창에는 management center에 디바이스 관리자로 되돌리거나 작업을 변경하고 변경 내용을 CDO에 커밋할 수 있는 남은 일 수가 표시됩니다. 평가 기간에는 변경 사항을 커밋하기 전에 선택한 위협 방어 디바이스에 대해 지정된 작업을 변경할 수 있습니다.

변경 사항이 커밋되면 창에 지정된 작업을 취소할 수 없습니다.



참고 커밋 관리자 변경 작업은 다음 조건에서 비활성화됩니다.

- 14일의 평가 기간이 지났습니다.
- 위협 방어 디바이스를 되돌렸거나 삭제한 경우 추가 작업을 수행할 수 없습니다.

### 프로시저

- 단계 1 마이그레이션 작업 페이지에서 완료된 작업의 **Actions**(작업) 열 아래에 있는 **...** 을 클릭합니다.
- 단계 2 **Commit Manager Changes**(관리자 변경 사항 커밋)를 클릭합니다. 이 링크는 작업이 성공적으로 완료된 경우에만 사용할 수 있습니다.
- 단계 3 디바이스에 대해 지정된 작업을 변경하려면 디바이스를 선택하고 **Actions**(작업) 목록에서 작업을 선택합니다.

- **Retain on OnPrem FMC for Analytics**(분석을 위해 OnPrem FMC에 유지): 변경 사항을 커밋하면 선택한 위협 방어 디바이스에 대한 분석 관리가 관리 센터에 유지됩니다.
- **Delete FTD from OnPrem FMC**(OnPrem FMC에서 FTD 삭제): 변경 사항을 커밋하면 선택한 디바이스가 관리 센터에서 제거되고 CDO에서 분석을 처리할 수 있습니다. 분석 관리를 위해 CDO에 이벤트를 전송할 위협 방어를 구성해야 합니다. 위협 방어 디바이스가 management center에서 삭제되면 취소할 수 없습니다.
- **Revert Manager to OnPrem FMC**(관리자를 OnPrem FMC로 되돌리기): 변경 사항을 커밋하면 디바이스 관리가 CDO에서 management center로 돌아갑니다.

- 참고
- 이 작업을 커밋한 후에는 디바이스의 관리를 CDO로 다시 변경할 수 없습니다.  
해결 방법: management center에서 디바이스를 제거하고 온보딩해야 합니다. 그런 다음 CDO에서 디바이스의 관리를 변경할 수 있습니다.
  - 이 작업을 커밋한 후 디바이스는 management center에서 "Out-of-Date(최신 상태)" 상태를 표시하지 않습니다.  
해결 방법: 온프레미스 management center에서 디바이스에 변경 사항을 구축합니다.

단계 4 **Commit**(커밋)을 클릭하면 추가 확인 없이 지정된 작업이 즉시 실행됩니다.

단계 5 마이그레이션 작업 화면에서 작업을 확장하여 지정된 작업의 진행 상황을 확인할 수 있습니다.

## 마이그레이션 작업 제거

마이그레이션 작업을 삭제할 수 있으며, 결과는 해당 작업이 삭제된 시점에 따라 달라집니다.

- 14일 평가 기간 동안: 마이그레이션을 중지하고, 마이그레이션 작업과 연결된 디바이스의 구성이 원래 상태로 돌아갑니다.
- 마이그레이션 변경 사항을 커밋한 후: 마이그레이션 작업 목록에서 레코드가 삭제됩니다.

프로시저

단계 1 마이그레이션 작업 페이지에서 **Actions**(작업) 열 아래의  을 클릭한 다음 **Remove Migration Job**(마이그레이션 작업 제거)을 클릭합니다.

단계 2 **Delete**(삭제)를 클릭하여 작업을 확인합니다.

## 클라우드로의 **FTD** 마이그레이션 문제 해결

이 섹션에서는 FTD를 클라우드로 마이그레이션할 때 발생할 수 있는 특정 오류를 문제 해결하기 위한 정보를 제공합니다.

**FMC** 응답에서 **HTTP** 상태 코드 **201**(생성됨) 발견

CDO는 디바이스 레벨에서 이 오류를 표시합니다.

문제:

SDC(Secure Device Connector) 버전이 호환되지 않습니다.

Number of FTDs	Status
1 devices	  Change FTD Manager job failed
IP ADDRESS	STATUS
10.10.90.32	 Device Connectivity with CDO failed. (HTTP status code 201 (Created) found in FMC response.)

해결 방법:

SDC가 "202205191350" 이상 버전으로 업그레이드되었는지 확인합니다.

1. **Admin**(관리) > **Secure Connector**(보안 커넥터)로 이동합니다.

- SDC를 클릭하여 오른쪽의 **Details**(세부 정보) 창에서 기존 SDC 버전을 확인합니다.
- 보안 디바이스 커넥터를 업데이트합니다.

### CDO에 대한 디바이스 연결 실패

Name	Number of FTDs	Status	Last Updated	Actions
1771Fmc_change-management_2022-02-28-104213	2 devices	Change FTD Manager job failed	Feb 28, 2022, 4:14:12 PM	...
DEVICE NAME	IP ADDRESS	STATUS	LAST UPDATED	
1771Fmc_10.10.16.84	10.10.16.84	Device Connectivity with CDO failed	Feb 28, 2022, 4:12:53 PM	

다음 이유 중 하나로 인해 장치가 CDO에 연결할 수 없습니다:

- 디바이스가 잘못 연결되었습니다.
- 네트워크에 디바이스의 고정 IP 주소가 필요할 수 있습니다.
- 네트워크에서 맞춤형 DNS를 사용하거나 고객 네트워크에서 외부 DNS 차단이 있습니다.
- PPPoE 인증이 필요합니다.
- 디바이스가 프록시 뒤에 있습니다.

해결 방법:

- 케이블링 및 네트워크 연결을 확인합니다.
- 방화벽이 트래픽을 차단하고 있지 않은지 확인합니다.
- 클라우드 사용 Firewall Management Center와의 Threat Defense 연결 확인.

CDO를 구성 관리자로 구성하지 못했습니다.

CDO가 네트워크 손실로 인해 디바이스와 통신할 수 없는 경우 클라우드 제공 방화벽 관리 센터를 사용하여 `configure manager` 명령을 실행하지 못합니다.

Name	Number of FTDs	Status	Last Updated	Actions
1771Fmc_change-management_2022-03-04-055700	2 devices	Change FTD Manager job is in progress	Mar 4, 2022, 11:33:07 AM	...
DEVICE NAME	IP ADDRESS	STATUS	LAST UPDATED	
1771Fmc_10.10.16.86	10.10.16.86	Syncing	Mar 4, 2022, 11:29:03 AM	
1771Fmc_10.10.16.84	10.10.16.84	Failed to configure CDO as Configuration Manager	Mar 4, 2022, 11:28:16 AM	

해결 방법:

- 케이블링 및 네트워크 연결을 확인합니다.
- 방화벽이 트래픽을 차단하고 있지 않은지 확인합니다.
- FTD가 인터넷에 연결되어 있고 DNS 주소가 IP 주소로 확인되었는지 확인합니다. 클라우드 사용 Firewall Management Center와의 Threat Defense 연결 확인, 8 페이지를 참조하십시오.
- 새 변경 관리자 작업에서 CDO의 이 FTD에 대한 마이그레이션을 다시 시도하십시오.

변경 관리자가 이미 존재하거나 소스 관리자에 대해 진행 중

이전 작업이 완료된 경우에만 온프레미스 Management Center에 대한 FTD 마이그레이션 작업을 생성할 수 있습니다.

이 오류는 이전 작업이 진행 중일 때 새 작업을 생성할 때 발생합니다.

**Migrate FTD to Cloud**  
Change FTD Manager from Firewall Management Center to CDO

1 Select OnPrem FMC **OnPrem FMC: fmc-beta2-18-3**

2 Select Devices **change ftd management already exists or in progress for source manager fmc-beta2-18-3**

Select FTD devices to migrate to cloud from OnPrem FMC to CDO and specify an action in bulk or per device.

1 device(s) selected Multi-Device Action Retain on OnPrem FMC for Analytics

Name	Domain	Action
fmc-beta2-18-3_10.10.16.20	Global	Retain on OnPrem FMC for Analytics
<input checked="" type="checkbox"/> fmc-beta2-18-3_10.10.16.25	Global	Retain on OnPrem FMC for Analytics
fmc-beta2-18-3_10.10.16.9	Global	Retain on OnPrem FMC for Analytics

Displaying 3 of 3 results

Migrate FTD to Cloud

3 Finish

해결 방법:

1. 마이그레이션 테이블로 이동하여 특정 소스 온프레미스 관리 센터에 대해 다른 작업이 진행 중인 지 확인합니다.
2. 현재 마이그레이션 작업이 완료될 때까지 기다립니다.
3. 다음 마이그레이션 작업을 시작합니다.



## 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.