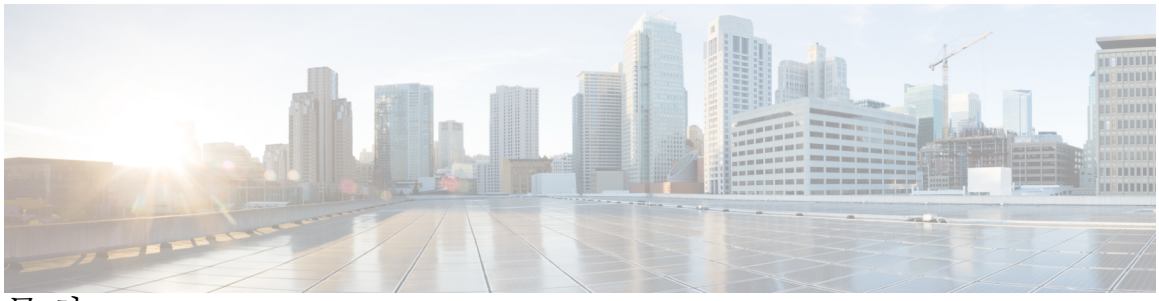
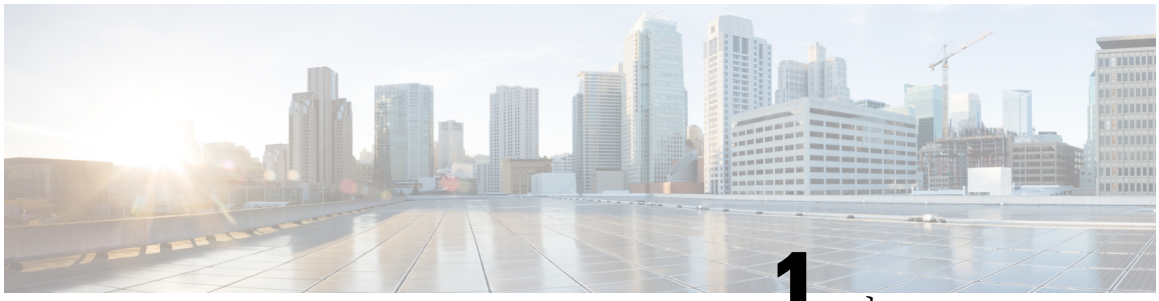
Cisco Defense Orchestrator의 Firewall 마이그레이션 툴을 사용하여 방화벽 마이그레이션

초판: 2023년 2월 21일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차



1 장

Cisco Defense Orchestrator의 Firewall 마이그레이션 툴을 사용하여 방화벽 마이그레이션

이 문서는 CDO(Cisco Defense Orchestrator)에서 호스팅되는 Cisco Secure Firewall 마이그레이션 툴의 클라우드 버전을 사용하는 방법을 지원합니다.

CDO는 Cisco Secure Firewall 마이그레이션 툴의 클라우드 버전을 호스팅합니다. 이 툴을 사용하여 기존 방화벽 구성을 CDO 테넌트에 구축된 클라우드 사용 Firewall Management Center에서 관리하는 Secure Firewall Threat Defense 디바이스로 마이그레이션할 수 있습니다.

가이드의 적합성 확인

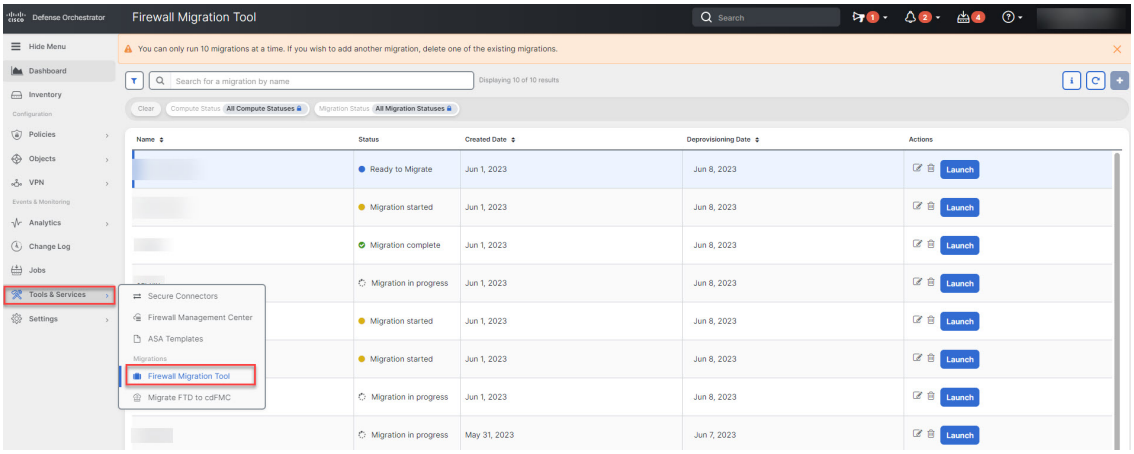
이 설명서는 CDO를 사용하여 Secure Firewall ASA 디바이스 및 FDM 매니지드 Threat Defense 디바이스를 관리하거나 Palo Alto Networks, Check Point 및 Fortinet 방화벽과 같은 타사 방화벽을 사용하여 Cisco Secure Firewall Threat Defense로 이동하려는 경우를 위한 것입니다. CDO의 Secure Firewall 마이그레이션 툴로 클라우드 사용 Firewall Management Center에서 관리하는 Threat Defense 디바이스로 모든 기존 방화벽 구성을 마이그레이션할 수 있습니다. 이 문서에서는 구성을 마이그레이션하기 위해 수행해야 하는 작업에 대해 설명합니다.

Cisco Defense Orchestrator에서 Firewall 마이그레이션 툴 시작하기

CDO의 마이그레이션 툴은 선택한 소스 디바이스 또는 사용자가 업로드하는 구성 파일에서 디바이스 구성을 추출하여 구성을 검증한 후 CDO 테넌트에 프로비저닝된 클라우드 사용 Firewall Management Center로 마이그레이션합니다. 마이그레이션 툴은 대부분의 구성을 지원합니다. 지원되지 않는 구성

은 클라우드 사용 Firewall Management Center에서 수동으로 구성해야 합니다. 지원되는 구성, 2 페이지의 내용을 참조하십시오.

Tools & Services(툴 및 서비스**)** > **Firewall Migration Tool(Firewall** 마이그레이션 툴**)**에서 새 마이그레이션을 초기화하고 **Launch(**실행**)**할 경우, 마이그레이션 툴의 클라우드 인스턴스가 새 브라우저 탭에서 열립니다. 여기서 안내되는 워크플로우를 사용하여 마이그레이션 작업을 수행할 수 있습니다. CDO의 마이그레이션 툴을 사용하면 Secure Firewall 마이그레이션 툴의 데스크톱 버전을 다운로드하여 유지 보수할 필요가 없습니다.



CDO에서 호스팅되는 마이그레이션 툴을 사용하여 다음과 같은 Cisco 및 타사 방화벽 구성을 Secure Firewall Threat Defense 디바이스로 마이그레이션할 수 있습니다.

- Cisco Secure Firewall ASA
- Firewall Device Manager에서 관리하는 Secure Firewall Threat Defense
- Check Point 방화벽
- Palo Alto Networks 방화벽
- Fortinet 방화벽

중요 Firewall 마이그레이션 툴을 사용할 수 있으려면 CDO에 관리자 또는 슈퍼 관리 사용자 역할이 필요합니다.

지원되는 구성

마이그레이션 툴은 다음 구성을 지원합니다.

- 네트워크 개체 및 그룹
- 서비스 개체(소스 및 대상에 대해 구성된 서비스 개체 제외)
- 참조된 ACL 및 NAT 규칙

- 서비스 개체 그룹

참고 클라우드 사용 Management Center는 중첩을 지원하지 않으므로, 중첩된 서비스 개체 그룹 콘텐츠는 마이그레이션 전에 개별 개체로 나뉩니다.

- IPv4 및 IPv6 FQDN 개체 및 그룹
- IPv6 변환(인터페이스, 정적 경로, 개체, ACL 및 NAT)
- 인그레스 인터페이스에 적용되는 액세스 규칙
- 전역 ACL
- 자동 NAT, 수동 NAT 및 개체 NAT
- 정적 경로, ECMP(Equal-Cost Multipath) 경로 및 PBR(Policy-Based Routing)
- 물리적 인터페이스
- 하위 인터페이스
- 포트 채널
- 가상 터널 인터페이스
- 투명 모드의 브리지 그룹
- IP SLA 개체 - 마이그레이션 툴이 개체를 생성하고, 정적 경로와 매핑하며, 마이그레이션합니다.
- 시간 기반 개체
- 사이트 간 VPN
  - 사이트 대 사이트 VPN - Firewall 마이그레이션 툴이 소스 ASA 또는 FDM 매니지드 디바이스에서 암호화 맵 구성을 탐지하면 Secure Firewall 마이그레이션 툴이 해당 구성을 Point-to-Point 토폴로지로 Management Center VPN에 마이그레이션합니다.
  - ASA 및 FDM 매니지드 디바이스의 암호화 맵(정적/유동) 기반 VPN
  - 경로 기반(VTI) ASA 및 FDM VPN
  - ASA 및 FDM 매니지드 디바이스의 인증서 기반 VPN 마이그레이션

중요 소스 디바이스에 사이트 대 사이트 VPN 구성이 있는 경우 ASA 및 FDM 매니지드 디바이스의 트러스트 포인트 또는 인증서가 클라우드 사용 Firewall Management Center에서 수동으로 구성되었는지 확인하십시오.

- 원격 액세스 VPN
  - SSL 및 IKEv2 프로토콜

- 인증 방법 - AAA 전용, 클라이언트 인증서 전용, SAML, AAA, 클라이언트 인증서
- AAA - Radius, 로컬, LDAP 및 AD
- 연결 프로파일, 그룹 정책, Dynamic Access Policy, LDAP 속성 맵, 인증서 맵
- 표준 및 확장 ACL
- 사용자 지정 속성 및 VPN 로드 밸런싱

중요 소스 방화벽에서 원격 액세스 VPN을 구성한 경우 다음 작업을 수행해야 합니다.

- Management Center에서 PKI 개체로 수동으로 ASA 및 FDM 매니지드 디바이스의 트러스트 포인트를 구성합니다.
- 소스 ASA 및 FDM 매니지드 디바이스에서 AnyConnect 패키지, Hostscan 파일(dap.xml, data.xml, hostscan 패키지), 외부 브라우저 패키지 및 AnyConnect 프로파일을 검색합니다.
- Management Center에 모든 AnyConnect 패키지 및 프로파일 업로드

- 유동 경로 개체, BGP 및 EIGRP
  - 정책 목록
  - 접두사 목록
  - 커뮤니티 목록
  - AS(자율 시스템) 경로
  - 루트 맵

참고 마이그레이션 툴은 이름과 구성을 기반으로 모든 개체 및 개체 그룹을 분석하고 동일한 이름 및 구성을 가진 개체를 재사용합니다. 그러나 원격 액세스 VPN 구성의 XML 프로파일은 이름만 사용하여 검증합니다.

라이선스

Secure Firewall 마이그레이션 툴은 CDO에서 액세스하는 데 추가 라이선스가 필요하지 않습니다.

하지만 마이그레이션하려는 위협 방어 기능에 대한 CDO 기본 구독 및 라이선스가 있어야 합니다.

새 마이그레이션 인스턴스 초기화

단계 **1** CDO 테넌트에 로그인합니다.

단계 **2** **Tools & Services(**툴 및 서비스**)** > **Firewall Migration Tool(Firewall** 마이그레이션 툴**)**을 선택합니다.

단계 **3** 새 마이그레이션 인스턴스를 초기화하려면 파란색 더하기  버튼을 클릭합니다.

참고 Firewall 마이그레이션 툴을 사용하면 최대 10개의 마이그레이션을 생성하고 모든 마이그레이션을 동시에 시작할 수 있습니다. 각 마이그레이션 인스턴스는 새 브라우저 탭에서 열립니다. 그러나 본인의 테넌트에 여러 사용자가 프로비저닝되어 있는 경우에는 본인이 생성한 마이그레이션만 시작할 수 있습니다.

이미 마이그레이션이 10개인 경우 새 마이그레이션 인스턴스를 초기화하려면 기존 마이그레이션 인스턴스 중 하나를 삭제합니다.

단계 **4** CDO는 마이그레이션을 위해 자동으로 이름을 생성합니다. 자동 생성된 이름을 사용하거나 필요에 맞게 변경할 수 있습니다.

단계 **5** **OK(**확인**)**를 클릭하고 상태가 **Initializing(**초기화**)**에서 **Ready to Migrate(**마이그레이션 준비**)**로 변경될 때까지 기다립니다. 또한 마이그레이션이 준비되면 CDO는 **Notifications(**알림**)** 창에서 새로운 내용을 알립니다.

단계 **6** 새 마이그레이션에서 **Launch(**실행**)**를 클릭합니다.

마이그레이션 툴이 새 브라우저 탭에서 열리며 인증이 필요하지 않습니다.

참고 CDO의 마이그레이션은 생성된 날짜로부터 7일 동안 유효하며, 그 이후에는 자동으로 프로비저닝이 해제됩니다. 이렇게 하면 CDO 리소스를 수시로 확보할 수 있습니다. **Created Date(**생성된 날짜**)** 및 **Deprovisioning Date(**프로비저닝 해제 날짜**)** 열에서 날짜를 확인할 수 있습니다.

CDO는 **Status(**상태**)** 열에 모든 마이그레이션의 상태를 표시합니다. 상태에 따라 마이그레이션을 필터링할 수 있습니다. 마이그레이션을 선택하면 오른쪽 창에서 생성 날짜 및 시간, 시작 날짜 및 시간, 소스 및 대상 디바이스 이름, 생성한 사람과 같은 마이그레이션 세부 정보를 볼 수 있습니다. 본인의 CDO 테넌트에 여러 사용자가 프로비저닝된 경우에는 본인이 생성한 마이그레이션만 실행할 수 있습니다.

마이그레이션 인스턴스 삭제

CDO가 자동으로 프로비저닝을 해제하기 전에 수동으로 마이그레이션을 프로비저닝 해제하려면 아래 단계를 수행하십시오. 예를 들어, 마이그레이션 작업이 완료된 후 마이그레이션을 삭제할 수 있습니다.

단계 **1** **Tools & Services(**툴 및 서비스**)** > **Firewall Migration Tool(Firewall** 마이그레이션 툴**)**을 선택합니다.

단계 **2** 삭제하려는 마이그레이션에서 **Actions(**작업**)** 창 아래에서 **Delete(**삭제**)**를 클릭합니다.

단계 **3** **Delete(**삭제**)**를 클릭하여 작업을 확인합니다.

Cisco Defense Orchestrator에서 관리하는 Secure Firewall ASA 마이그레이션

CDO의 Secure Firewall 마이그레이션 툴을 사용하면 CDO에서 관리하거나 ASA 디바이스에서 추출한 구성 파일을 사용하여 라이브 ASA 디바이스에서 구성을 마이그레이션할 수 있습니다.

소스 구성 선택

CDO에서 마이그레이션 인스턴스를 실행한 후 **Select Source Configuration(**소스 구성 선택**)**에서 **Cisco ASA**를 선택하고 **Start Migration(**마이그레이션 시작**)**을 클릭합니다. ASA 구성 파일을 수동으로 업로드하거나 **Connect to ASA(ASA**에 연결**)** 창에 나열된 CDO 매니지드 ASA 디바이스 중 하나를 선택할 수 있습니다. CDO 매니지드 디바이스를 선택하려는 경우 구성 상태가 **Synced(**동기화**)**로 표시된 디바이스는 마이그레이션 툴에만 나열됩니다. 마이그레이션할 디바이스가 목록에 표시되지 않으면 디바이스 구성 변경 사항이 최신 상태이고 CDO와 동기화되었는지 확인하십시오. 둘 이상의 사용자가 동시에 하나의 ASA 디바이스를 소스 디바이스로 선택할 수 있으며 구성 추출이 원활하게 이루어집니다. ASA 디바이스에 하나 이상의 보안 상황이 구성되어 있는 경우, 마이그레이션 툴을 사용하여 마이그레이션할 상황을 선택할 수 있습니다. 모든 상황을 단일 인스턴스로 병합한 후 마이그레이션할 수도 있습니다. 자세한 내용은 ASA 기본 보안 상황 선택을 참고하십시오.

마이그레이션 툴은 디바이스 구성을 구문 분석하고 구문 분석된 구성을 포함한 요약을 표시합니다. **Next(**다음**)**를 클릭합니다.

대상 선택

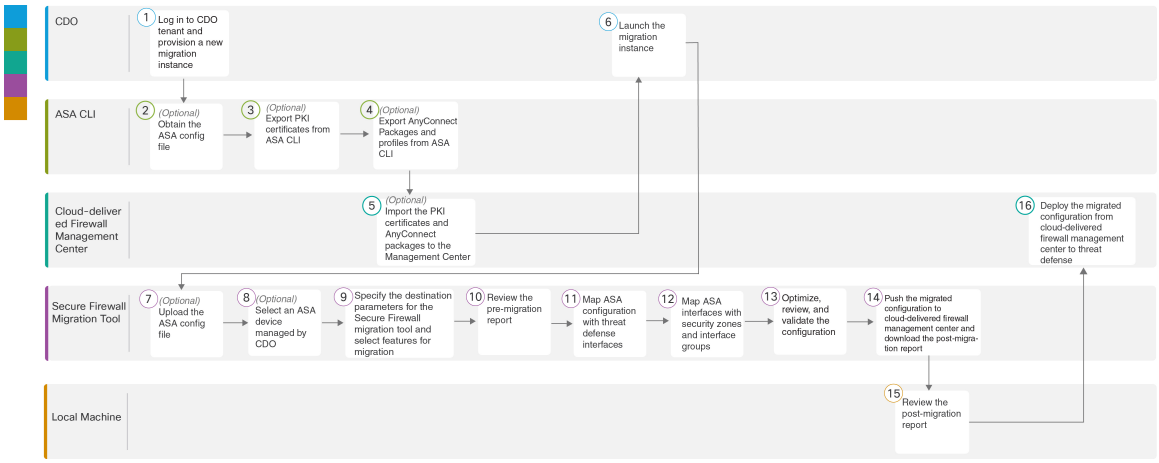
Select Target(대상 선택**)** 페이지에서는 CDO 테넌트에 프로비저닝된 클라우드 사용 Firewall Management Center가 기본적으로 선택되고 해당 Management Center에서 관리하는 위협 방어 디바이스가 나열됩니다. ASA 구성을 마이그레이션할 위협 방어 디바이스를 선택하거나 **Proceed without FTD(FTD** 없이 진행**)**를 선택할 수 있습니다. 나열된 Threat Defense 디바이스는 디바이스가 다른 마이그레이션 인스턴스에서 사용되고 있는지에 따라 **In Use(**사용 중**)** 또는 **Available(**사용 가능**)**로 표시됩니다. 그러나 **Change Device Status(**디바이스 상태 변경**)**를 클릭하고 **In Use(**사용 중**)** 목록에서 디바이스를 선택하고 **Continue(**계속**)**를 클릭하여 재정의를 수행할 수 있습니다. 그러면 디바이스를 대상으로 선택할 수 있습니다.

주의 디바이스 상태를 **In Use(**사용 중**)**에서 **Available(**사용 가능**)**로 변경하면 디바이스를 이미 사용하여 진행 중인 마이그레이션 인스턴스에 영향을 미칩니다. 이 작업을 수행할 때는 주의를 기울이는 것이 좋습니다.

Proceed Without FTD(FTD 없이 진행**)**를 선택하면 NAT 개체, ACL 및 포트 개체만 클라우드 사용 Firewall Management Center로 푸시됩니다. 일반적으로 사용되는 ASA 기능 및 그에 상응하는 Threat Defense 기능에 대한 자세한 정보는 Cisco Secure Firewall ASA-Threat Defense 기능 매핑 가이드를 참고하십시오.

다음의 순서도는 CDO의 Firewall 마이그레이션 툴을 사용하여 ASA를 위협 방어로 마이그레이션하는 단계별 절차를 보여줍니다.

그림 *1: CDO*의 *Firewall* 마이그레이션 툴을 사용하여 *ASA-FTD*로 마이그레이션하기 위한 엔드 투 엔드 절차



더 자세한 단계가 포함된 절차를 수행하려면 마이그레이션 툴을 사용하여 Cisco Secure Firewall ASA를 Threat Defense로 마이그레이션 가이드의 ASA 구성 파일 가져오기를 계속 진행하십시오.

	업무 환경	단계
1	CDO	CDO 테넌트에 로그인하고 **Tools & Services(**툴 및 서비스**)** > **Firewall Migration Tool(Firewall** 마이그레이션 툴**)**로 이동한 다음, 파란색 더하기 버튼을 클릭하여 새 마이그레이션 인스턴스의 프로비저닝을 시작합니다.
2	ASA CLI	(선택 사항) ASA 구성 파일 가져오기: ASA CLI에서 ASA 구성 파일을 가져오려면 ASA 구성 파일 가져오기를 참고하십시오. **Select Source Configuration(**소스 구성 선택**)**에서 CDO 매니지드 ASA 디바이스를 선택하려면 3단계로 건너뜁니다.
3	ASA CLI	(선택 사항) ASA CLI에서 PKI(Public Key Infrastructure) 인증서 내보내기: 이 단계는 사이트 대 사이트 VPN 및 RAVPN 구성을 ASA에서 Threat Defense로 마이그레이션하려는 경우에만 필요합니다. ASA CLI에서 PKI 인증서를 내보내려면 ASA에서 PKI 인증서 내보내기 및 Management Center로 가져오기를 참고하십시오. 디바이스에 원격 액세스 VPN 구성이 없는 경우나 사이트 대 사이트 VPN 및 원격 액세스 VPN을 마이그레이션할 계획이 없는 경우 7단계로 건너뜁니다.
4	ASA CLI	(선택 사항) ASA CLI에서 AnyConnect 패키지와 프로파일 내보내기: 이 단계는 원격 액세스 VPN 기능을 ASA에서 Threat Defense로 마이그레이션하려는 경우에만 필요합니다. ASA CLI에서 AnyConnect 패키지 및 프로파일을 내보내려면 AnyConnect 패키지 및 프로파일 검색을 참고하십시오.

	업무 환경	단계
5	클라우드 사용 Firewall Management Center	(선택 사항) PKI 인증서 및 AnyConnect 패키지를 Management Center로 가져오기: PKI 인증서를 Management Center로 가져오려면 ASA에서 PKI 인증서 내보내기 및 Management Center로 가져오기 및 AnyConnect 패키지 및 프로파일 검색의 2단계를 참고하십시오.
6	CDO	생성한 마이그레이션 인스턴스의 상태가 **Ready to Migrate(**마이그레이션 준비**)**인지 확인하고 **Launch(**실행**)**를 클릭합니다. Secure Firewall 마이그레이션 툴이 새 브라우저 탭에서 열립니다.
7	Secure Firewall 마이그레이션 툴	(선택 사항) ASA CLI에서 가져온 ASA 구성 파일을 업로드합니다. ASA 구성 파일 업로드를 참고하십시오. CDO에서 관리하는 ASA 디바이스에서 구성을 마이그레이션하려는 경우 8단계로 건너뜁니다.
8	Secure Firewall 마이그레이션 툴	표시된 ASA 디바이스(CDO 테넌트에서 관리) 목록에서 마이그레이션할 구성의 디바이스를 선택합니다. ASA 디바이스에 하나 이상의 보안 상황을 구성한 경우, 마이그레이션할 상황을 선택하거나 **Primary Context Selection(**기본 상황 선택**)** 드롭다운에서 모든 상황을 단일 인스턴스로 병합하도록 선택합니다. 자세한 내용은 ASA 기본 보안 상황 선택을 참고하십시오.
9	Secure Firewall 마이그레이션 툴	**Select Target(**대상 선택**)** 페이지에서는 CDO 테넌트에서 프로비저닝된 클라우드 사용 Firewall Management Center가 기본적으로 선택됩니다.
10	Secure Firewall 마이그레이션 툴	클라우드 사용 Firewall Management Center에서 관리하는 Threat Defense 디바이스 목록에서 대상 디바이스를 선택하거나 **Proceed without FTD(FTD** 없이 진행**)**를 선택하고 계속 진행합니다.
11	Secure Firewall 마이그레이션 툴	마이그레이션 전 보고서를 다운로드하고 구문 분석된 구성의 자세한 요약을 검토합니다. 자세한 단계는 마이그레이션 전 보고서 검토를 참고하십시오.
12	Secure Firewall 마이그레이션 툴	**FTD** 인터페이스를 **ASA** 구성과 매핑합니다. ASA 및 Threat Defense 디바이스의 물리적 및 포트 채널 인터페이스 이름이 항상 동일한 것은 아니므로, ASA 인터페이스를 매핑할 대상 Threat Defense 디바이스의 인터페이스를 선택할 수 있습니다. 자세한 정보는 Secure Firewall Device Manager Threat Defense 인터페이스와 ASA 구성 매핑을 참고하십시오.
13	Secure Firewall 마이그레이션 툴	ASA 인터페이스를 기존 Threat Defense 보안 영역 및 인터페이스 그룹에 매핑합니다. 자세한 단계는 ASA 인터페이스를 보안 영역 및 인터페이스 그룹에 매핑을 참고하십시오.

	업무 환경	단계
14	Secure Firewall 마이그레이션 툴	신중하게 구성을 최적화, 검토 및 검증하고 ACL, 개체, NAT, 인터페이스, 경로, 사이트 대 사이트 VPN 및 원격 액세스 VPN 규칙이 대상 Threat Defense 디바이스에 맞게 구성되었는지 확인해야 합니다. 구성 최적화, 검토 및 검증을 참고하십시오.
15	Secure Firewall 마이그레이션 툴	구성 검증이 성공적으로 완료되면 클라우드 사용 Firewall Management Center로 구성을 푸시합니다. 자세한 정보는 마이그레이션된 구성을 Management Center에 푸시를 참고하십시오.
16	로컬 컴퓨터	마이그레이션 후 보고서를 다운로드하고 검토합니다. 마이그레이션 후 보고서에 포함된 정보에 대한 자세한 내용은 마이그레이션 후 보고서 검토 및 마이그레이션 완료를 참고하십시오.
17	클라우드 사용 Firewall Management Center	새로 마이그레이션된 구성을 Threat Defense 디바이스에 구축합니다.

Cisco Defense Orchestrator에서 관리하는 FDM 매니지드 디바이스 마이그레이션

구성 파일을 사용하거나 CDO에 온보딩된 FDM 매니지드 디바이스를 선택하여 FDM 매니지드 디바이스 구성을 마이그레이션할 수 있습니다.

소스 구성 선택

CDO에서 마이그레이션 인스턴스를 실행한 후 **Select Source Configuration**(소스 구성 선택)에서 **Cisco Secure Firewall Device Manager**를 선택하고 다음 옵션 중 하나를 선택합니다.

- **Firepower Device Manager** 마이그레이션(공유 구성만 해당)
- **Firepower Device Manager** 마이그레이션(디바이스 및 공유 구성 포함)
- **Firepower Device Manager**(디바이스 및 공유 구성 포함)를 **FTD** 디바이스(새 하드웨어)로 마이그레이션

Continue(계속)를 클릭하면 마이그레이션 툴을 사용하여 FDM 매니지드 디바이스 구성 파일을 수동으로 업로드하거나 **Connect to FDM**(FDM에 연결) 창에 나와 있는 CDO에 온보딩된 FDM 매니지드 디바이스 중 하나를 선택하고 **Next**(다음)를 클릭할 수 있습니다.

대상 선택

Select Target(대상 선택) 페이지에서는 CDO 테넌트에 프로비저닝된 클라우드 사용 Firewall Management Center가 기본적으로 선택되고 해당 Management Center에서 관리하는 위협 방어 디바이스가 나열됩니다. 구성을 마이그레이션할 위협 방어 디바이스를 선택하고 마이그레이션을 진행할 수 있습니다.

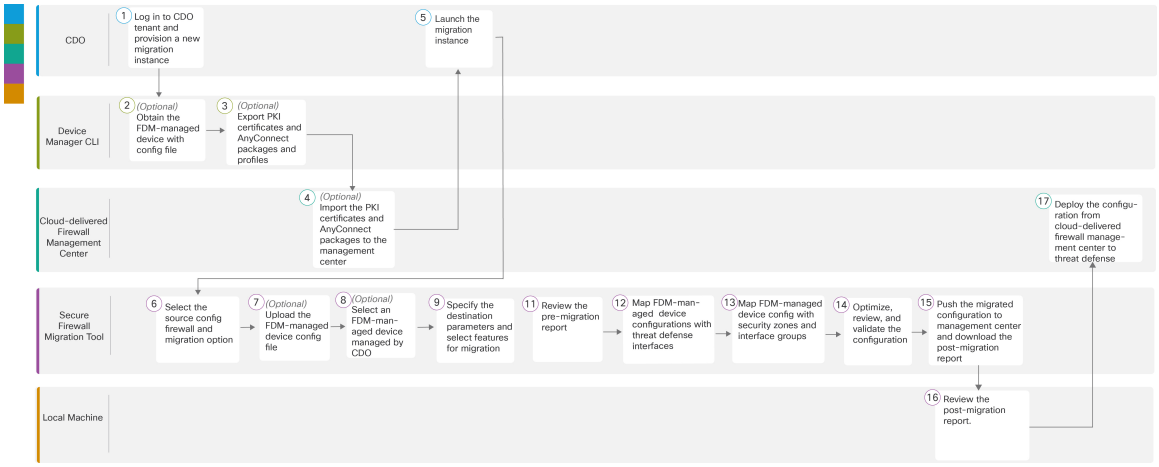
나열된 Threat Defense 디바이스는 디바이스가 다른 마이그레이션 인스턴스에서 사용되고 있는지에 따라 **In Use**(사용 중) 또는 **Available**(사용 가능)로 표시됩니다. 그러나 **Change Device Status**(디바이스 상태 변경)를 클릭하고 **In Use**(사용 중) 목록에서 디바이스를 선택하고 **Continue**(계속)를 클릭하여 재정의를 수행할 수 있습니다. 그러면 디바이스를 대상으로 선택할 수 있습니다.

⚠

주의 디바이스 상태를 **In Use**(사용 중)에서 **Available**(사용 가능)로 변경하면 디바이스를 이미 사용하여 진행 중인 마이그레이션 인스턴스에 영향을 미칩니다. 이 작업을 수행할 때는 주의를 기울이는 것이 좋습니다.

다음의 순서도는 CDO의 Firewall 마이그레이션 툴을 사용하여 FDM 매니지드 디바이스를 마이그레이션하는 단계별 절차를 보여줍니다.

그림 *2: CDO*의 *Firewall* 마이그레이션 툴을 사용하여 *FDM* 매니지드 디바이스*-FTD* 마이그레이션을 위한 엔드 투 엔드 절차



더 자세한 단계가 포함된 절차를 수행하려면 마이그레이션 툴을 사용하여 Secure Firewall Threat Defense로 FDM 매니지드 디바이스 마이그레이션 가이드의 FDM 매니지드 디바이스 구성 파일 가져오기를 계속 진행하십시오.

	업무 환경	단계
1	CDO	CDO 테넌트에 로그인하고 **Tools & Services**(툴 및 서비스) > **Firewall Migration Tool**(**Firewall** 마이그레이션 툴)로 이동한 다음, 파란색 더하기 + 버튼을 클릭하여 새 마이그레이션 인스턴스의 프로비저닝을 시작합니다.
2	Device Manager CLI	(선택 사항) FDM 매니지드 디바이스 구성 파일 가져오기: Device Manager CLI에서 FDM 매니지드 디바이스 구성 파일을 가져오려면 FDM 매니지드 디바이스 구성 파일 가져오기를 참고하십시오. **Select Source Configuration**(소스 구성 선택)에서 CDO 매니지드 FDM 디바이스를 선택하려면 3단계로 건너뜁니다.

	업무 환경	단계
3	Device Manager CLI	(선택 사항) PKI 인증서 및 AnyConnect 패키지와 프로파일 내보내기: 이 단계는 사이트 대 사이트 VPN 및 원격 액세스 VPN 기능을 FDM 매니지드 디바이스에서 Threat Defense로 마이그레이션하려는 경우에만 필요합니다. Device Manager CLI에서 PKI 인증서를 내보내려면 Firewall Management Center에서 PKI 인증서 내보내기 및 Firewall Management Center로 가져오기의 1단계를 참고하십시오. Device Manager CLI에서 AnyConnect 패키지 및 프로파일을 내보내려면 AnyConnect 패키지 및 프로파일 검색의 1단계를 참고하십시오. 사이트 대 사이트 VPN 및 원격 액세스 VPN 구성을 마이그레이션할 계획이 없는 경우 7단계로 건너뜁니다.
4	클라우드 사용 Firewall Management Center	(선택 사항) PKI 인증서 및 AnyConnect 패키지를 Management Center로 가져오기: PKI 인증서를 Management Center로 가져오려면 Firewall Management Center에서 PKI 인증서 내보내기 및 Firewall Management Center로 가져오기 및 AnyConnect 패키지 및 프로파일 검색의 2단계를 참고하십시오.
5	CDO	생성한 마이그레이션 인스턴스의 상태가 **Ready(**준비**)**인지 확인하고 **Launch(**실행**)**를 클릭합니다. Secure Firewall 마이그레이션 툴이 새 브라우저 탭에서 열립니다.
6	Secure Firewall 마이그레이션 툴	소스 구성 방화벽 및 마이그레이션 옵션을 선택하려면 소스 구성 방화벽 및 마이그레이션 선택을 참고하십시오.
7	Secure Firewall 마이그레이션 툴	(선택 사항) Device Manager CLI에서 가져온 FDM 매니지드 디바이스 구성 파일을 업로드합니다(FDM 매니지드 디바이스 구성 파일 업로드 참조). 구성을 CDO에 온보딩된 FDM 매니지드 디바이스에서 마이그레이션하는 경우 8단계로 건너뜁니다.
8	Secure Firewall 마이그레이션 툴	표시된 FDM 매니지드 디바이스(CDO 테넌트에서 관리) 목록에서 마이그레이션할 구성의 디바이스를 선택합니다.
9	Secure Firewall 마이그레이션 툴	**Select Target(**대상 선택**)** 페이지에서는 CDO 테넌트에서 프로비저닝된 클라우드 사용 Firewall Management Center가 기본적으로 선택됩니다.
10	Secure Firewall 마이그레이션 툴	클라우드 사용 Firewall Management Center에서 관리하는 Threat Defense 디바이스 목록에서 대상 디바이스를 선택하거나 **Proceed without FTD(FTD** 없이 진행**)**를 선택하고 계속 진행합니다.
11	Secure Firewall 마이그레이션 툴	마이그레이션 전 보고서를 다운로드하고 구문 분석된 구성의 자세한 요약을 검토합니다. 자세한 단계는 마이그레이션 전 보고서 검토를 참고하십시오.

	업무 환경	단계
12	Secure Firewall 마이그레이션 툴	**FTD** 인터페이스를 **FDM** 매니지드 디바이스 구성과 매핑합니다. FDM 및 Threat Defense 디바이스의 물리적 및 포트 채널 인터페이스 이름이 항상 동일한 것은 아니므로, FDM 매니지드 디바이스 인터페이스를 매핑할 대상 Threat Defense 디바이스의 인터페이스를 선택할 수 있습니다. 자세한 정보는 Secure Firewall Device Manager Threat Defense 인터페이스와 FDM 매니지드 디바이스 구성 매핑을 참고하십시오.
13	Secure Firewall 마이그레이션 툴	FDM 매니지드 디바이스 인터페이스를 기존 Threat Defense 보안 영역 및 인터페이스 그룹에 매핑합니다. 자세한 단계는 FDM 매니지드 인터페이스를 보안 영역 및 인터페이스 그룹에 매핑을 참고하십시오.
14	Secure Firewall 마이그레이션 툴	신중하게 구성을 최적화, 검토 및 검증하고 ACL, 개체, NAT, 인터페이스, 경로, 사이트 대 사이트 VPN 및 원격 액세스 VPN 규칙이 대상 Threat Defense 디바이스에 맞게 구성되었는지 확인해야 합니다. 구성 최적화, 검토 및 검증을 참고하십시오.
15	Secure Firewall 마이그레이션 툴	구성 검증이 성공적으로 완료되면 클라우드 사용 Firewall Management Center로 구성을 푸시합니다. 자세한 정보는 마이그레이션된 구성을 Management Center에 푸시를 참고하십시오.
16	로컬 컴퓨터	마이그레이션 후 보고서를 다운로드하고 검토합니다. 마이그레이션 후 보고서에 포함된 정보에 대한 자세한 내용은 마이그레이션 후 보고서 검토 및 마이그레이션 완료를 참고하십시오.
17	클라우드 사용 Firewall Management Center	새로 마이그레이션된 구성을 Threat Defense 디바이스에 구축합니다.

마이그레이션 재개

CDO에서 마이그레이션을 시작했는데 나중에 계속하려면 Firewall 마이그레이션 툴 탭을 닫으면 됩니다. 마이그레이션을 계속 진행하려면 CDO에 로그인한 다음, **Firewall Migration Tool(Firewall** 마이그레이션 툴**)**에서 실행하려는 마이그레이션의 **Launch(**실행**)**를 클릭합니다. 마이그레이션 툴은 사용자가 마이그레이션 중임을 탐지하고, 중단한 지점부터 계속 진행할 수 있도록 합니다. 하지만 진행 중인 마이그레이션이 마이그레이션 툴에서 탐지되도록 최소한 소스 구성의 구문 분석을 수행해야 합니다. 이 단계를 수행하기 전에 마이그레이션을 중단하는 경우에도 CDO에서 동일한 마이그레이션을 실행할 수는 있지만, 처음부터 마이그레이션을 시작해야 합니다.

관련 설명서

CDO의 Secure Firewall 마이그레이션 툴을 사용하여 타사 방화벽을 마이그레이션하는 방법에 대한 자세한 내용은 요구 사항에 따라 다음 문서를 참고하십시오.

- Firewall 마이그레이션 툴의 최신 기능 및 릴리스별 정보에 대한 내용은 Cisco Secure Firewall 마이그레이션 툴 릴리스 노트를 참고하십시오.

참고 Cisco Defense Orchestrator는 최신 버전의 Secure Firewall 마이그레이션 툴을 호스팅합니다.

- Check Point 방화벽에서 Threat Defense로 구성을 마이그레이션하려면 Check Point 방화벽을 Threat Defense로 마이그레이션 가이드의 Check Point 구성 파일 내보내기부터 시작합니다.
- Palo Alto Networks 방화벽에서 Threat Defense로 구성을 마이그레이션하려면 Palo Alto Networks 방화벽을 Threat Defense로 마이그레이션 가이드의 Palo Alto Networks 방화벽에서 구성 내보내기부터 시작합니다.
- Fortinet 방화벽에서 Threat Defense로 구성을 마이그레이션하려면 Fortinet 방화벽을 Threat Defense로 마이그레이션 가이드의 Fortinet 방화벽에서 구성 내보내기부터 시작합니다.

중요 ASA 및 FDM 매니지드 디바이스 마이그레이션과 달리 타사 방화벽 구성을 Threat Defense로 마이그레이션하는 경우에는 수동으로 추출한 구성 파일만 업로드할 수 있습니다.

Secure Firewall 마이그레이션 툴에 대한 전체 정보 및 모든 관련 설명서를 읽으려면 Cisco Secure Firewall 마이그레이션 툴을 참고하십시오.

관련 설명서