클라우드 사용 Firewall Management Center에 FTD 온보딩

온보딩 사전 요구 사항 및 절차에 대한 다음 정보를 읽어보십시오.

- 온보딩 개요, 1 페이지
- 디바이스를 클라우드 사용 Firewall Management Center에 온보딩하기 위한 사전 요건, 3 페이지
- 클라우드 사용 Firewall Management Center에서 디바이스 삭제, 10 페이지
- 문제 해결, 11 페이지
- 디바이스 관리 관련 정보, 16 페이지

온보딩 개요

클라우드 사용 Firewall Management Center에 대한 지원되는 모델 및 사용 사례를 검토합니다.

지원되는 장치

다음 디바이스 모델을 온보딩할 수 있습니다.

- Firepower 1000 시리즈
- Firepower 2100 시리즈
- Secure Firewall 3100 시리즈
- Firepower 4100 시리즈
- Firepower 9300 시리즈
- ISA 3000
- Secure Firewall Threat Defense Virtual(가상)

지원되는 사용 사례

클라우드 사용 Firewall Management Center는 현재 온보딩을 위해 다음 디바이스 시나리오를 지원합니다.

- 디바이스는 버전 7.0.3 또는 7.2.0 이상을 실행해야 합니다. 지원되는 모든 버전 및 제품 호환성을 확인하려면 Secure Firewall Threat Defense 호환성 가이드에서 자세한 내용을 참조하십시오.
- device manager에서 관리할 로컬 관리를 위해 구성된 디바이스입니다. 디바이스는 온보딩 전에에 로그인할 수도 있고 로그인되어 있을 수도 있습니다. 로그인하지 않은 디바이스의 경우 로우 터치 프로비저닝을 사용하여 디바이스 온보딩을 사용하여 디바이스를 온보딩할 수 있습니다.

참고 FDM 관리 디바이스를 클라우드 사용 Firewall Management Center에 온보딩하는 경우 더 이상 device manager로 디바이스를 관리할 수 없습니다.

- 온프레미스 Management Center로 관리되는 디바이스.

  온프레미스 Management Center에서 관리하는 위협 방어 디바이스가 이미 있는 경우 클라우드 관리를 위해 디바이스를 마이그레이션할 수 있습니다. 자세한 내용은 Secure Firewall Threat Defense를 클라우드로 마이그레이션을 참조하십시오.

참고 다음 시나리오는 디바이스를 클라우드 사용 Firewall Management Center로 이동하거나 마이그레이션할 때 발생합니다.

- 온프레미스 Management Center 또는 Secure Firewall Threat Defense device manager에서 클라우드 사용 Firewall Management Center에 온보딩하기 위해 디바이스를 삭제하는 경우 관리자가 변경되면 온프레미스 Management Center를 통해 구성된 모든 정책이 지워집니다.
- 디바이스를 온프레미스 Management Center에서 클라우드 사용 Firewall Management Center로 마이그레이션하는 경우, 디바이스는 이전에 구성한 대부분의 정책을 유지합니다.

디바이스가 이미 대체 관리자에 의해 관리되고 있는지 모르는 경우 디바이스의 CLI에서 `show managers` 명령을 사용합니다.

온보딩 방법

클라우드 사용 Firewall Management Center는 다음과 같은 온보딩 방법을 지원합니다.

- CLI 등록 키로 디바이스 온보딩 - 등록 키로 디바이스를 온보딩합니다. 디바이스에서 초기 디바이스 설정 마법사가 완료되었습니다.
- 로우 터치 프로비저닝을 사용하여 디바이스 온보딩 - 디바이스에서 초기 디바이스 설정 마법사가 수행되지 않은 공장 배송 디바이스를 온보드합니다. 이 방법은 Firepower 1000, Firepower 2100 또는 Secure Firewall 3100 디바이스만 지원합니다.

참고 버전 7.0.3은 로우 터치 프로비저닝을 지원하지 않습니다.

- 일련 번호로 디바이스 온보딩 - 초기에 일련 번호로 이미 구성된 디바이스를 온보딩합니다. 이 방법은 Firepower 1000, Firepower 2100 또는 Secure Firewall 3100 디바이스만 지원합니다.

참고 버전 7.0.3은 일련 번호를 사용한 온보딩을 지원하지 않습니다.

디바이스를 클라우드 사용 **Firewall Management Center**에 온보딩하기 위한 사전 요건

온보드 제한 사항 및 요구 사항

디바이스를 클라우드 사용 Firewall Management Center에 온보딩할 때는 다음 제한 사항에 유의하십시오.

- 디바이스에서 버전 7.0.3 또는 버전 7.2 이상을 반드시 실행해야 합니다. 버전 7.2 이상을 사용하는 것이 좋습니다.
- 디바이스를 온보딩하기 위해 온프레미스 또는 가상 SDC가 필요하지 않습니다.
- Migrate FTD to Cloud-Delivered Firewall Management Center(클라우드 제공 방화벽 관리 센터로 FTD 마이그레이션) 프로세스에 따라 온프레미스 Firewall Management Center에서 관리하는 HA 쌍을 마이그레이션할 수 있습니다. 마이그레이션하기 전에 두 피어가 모두 정상 상태인지 확인합니다.
- 로컬 관리를 위해 구성되고 device manager에서 관리하는 디바이스만 일련 번호 및 로우 터치(low-touch) 프로비저닝 방법을 사용하여 온보딩할 수 있습니다.
- 온프레미스 Management Center에서 디바이스를 관리하는 경우 디바이스를 클라우드 사용 Firewall Management Center에 온보딩하거나 마이그레이션할 수 있습니다. 마이그레이션은 기존 정책 및 개체를 유지하는 반면, 디바이스를 온보딩하면 대부분의 정책 및 모든 개체가 제거됩니다. 자세한 내용은 FTD를 클라우드 제공 방화벽 관리 센터로 마이그레이션을 참조하십시오.
- 디바이스가 현재 device manager에서 관리되는 경우 디바이스를 온보딩하기 전에 모든 스마트 라이선스를 등록 취소합니다. 디바이스 관리를 전환하는 경우에도 Cisco Smart Software Manager는 스마트 라이선스를 유지합니다.
- device manager에서 관리하는 디바이스를 이전에 온보딩했고 클라우드 관리를 위해 다시 온보딩할 목적으로 CDO에서 디바이스를 삭제한 경우, 디바이스를 삭제한 후 보안 서비스 익스체인지 클라우드에 device manager를 등록해야 합니다. *Firepower* 및 *Cisco SecureX Threat Response* 통합 가이드의 "Access Security Services Exchange" 장을 참조하십시오.

팁 디바이스를 클라우드 사용 Firewall Management Center에 온보딩하면 이전 관리자를 통해 구성된 모든 정책 및 대부분의 개체가 제거됩니다. 디바이스가 현재 온프레미스 Management Center에서 관리되는 경우, 디바이스를 마이그레이션하고 정책 및 개체를 유지할 수 있습니다. 자세한 내용은 FTD를 클라우드 제공 방화벽 관리 센터로 마이그레이션을 참조하십시오.

네트워크 요구 사항

디바이스를 온보딩하기 전에 다음 포트에 외부 및 아웃바운드 액세스 권한이 있는지 확인합니다. 디바이스에서 다음 포트가 허용되는지 확인합니다. 통신 포트가 방화벽 뒤에서 차단된 경우 디바이스 온보딩이 실패할 수 있습니다.

참고 CDO UI에서는 이러한 포트를 구성할 수 없습니다. 디바이스의 SSH를 통해 이러한 포트를 활성화해야 합니다.

표 *1:* 디바이스 포트 요구 사항

포트	프로토콜/기능	세부 사항
443/tcp	HTTPS	인터넷에서 데이터 송수신
443	HTTPS	AMP 클라우드와 통신(퍼블릭 또는 프라이빗)
8305/tcp	어플라이언스 통신	구축 어플라이언스 간 보안 통신.

관리 및 데이터 인터페이스

디바이스가 관리 또는 데이터 인터페이스로 올바르게 구성되어 있는지 확인합니다.

디바이스에서 관리 또는 데이터 인터페이스를 구성하려면 CLI를 사용하여 Secure Firewall Threat Defense 디바이스의 초기 구성 완료의 내용을 참조하십시오.

CLI 등록 키로 디바이스 온보딩

아래 절차를 사용하여 CLI 등록 키를 사용하여 클라우드 사용 Firewall Management Center의 디바이스를 온보딩합니다.

참고 디바이스가 현재 온프레미스 Management Center에서 관리되는 경우 디바이스 온보딩이 실패합니다. 온프레미스 Management Center에서 디바이스를 삭제하고 정책 또는 개체가 없는 새 디바이스로 온보딩하거나, 디바이스를 마이그레이션하고 기존 정책 및 개체를 유지할 수 있습니다. 자세한 내용은 FTD를 클라우드 제공 방화벽 관리 센터로 마이그레이션을 참조하십시오.

중요 Secure Firewall 섀시 관리자 또는 FXOS CLI를 사용하여 CDO 매니지드, 독립형 논리적 위협 방어 디바이스를 생성할 수 있습니다.

시작하기 전에

디바이스를 온보딩하기 전에 다음 작업을 완료해야 합니다.

- 클라우드 사용 Firewall Management Center가 테넌트에 대해 활성화되었습니다.
- 디바이스의 CLI 구성이 성공적으로 완료되었는지 확인합니다. 자세한 내용은 CLI를 사용하여 Secure Firewall Threat Defense 디바이스의 초기 구성 완료을 참조하십시오.
- 디바이스를 온보딩하기 전에 사전 요구 사항 및 제한 사항을 검토합니다. 자세한 내용은 Cisco Defense Orchestrator에서 클라우드 제공 Firewall Management Center로 Firewall Threat Defense 관리에서 "디바이스를 클라우드 사용 Firewall Management Center에 온보딩하기 위한 사전 요건"을 참조하십시오.
- Secure Firewall device manager를 사용하여 로컬 관리 또는 Secure Firewall Management Center를 사용하여 원격 관리하도록 디바이스를 구성할 수 있습니다.
- 디바이스는 버전 7.0.3 또는 7.2.0 이상을 실행해야 합니다.

프로시저

단계 **1** CDO에 로그인합니다.

단계 **2** 탐색창에서 **Inventory(**재고 목록**)**를 클릭하고 파란색 더하기 버튼을 클릭합니다.

단계 **3** **FTD tile(**타일**)**을 클릭합니다.

단계 **4** **Management Mode(**관리 모드**)**에서 **FTD**가 선택되어 있는지 확인합니다.

경고! **Management Mode(**관리 모드**)**에서 **FTD**를 선택하면 이전 관리 플랫폼을 사용하여 디바이스를 관리할 수 없습니다. 인터페이스 구성을 제외한 모든 기존 정책 구성이 재설정됩니다. 디바이스를 온보딩한 후에는 정책을 다시 구성해야 합니다.

디바이스가 Secure Firewall device manager에서 관리를 유지하도록 하려면 **FDM**을 선택하고 등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스 온보딩에서 자세한 내용을 확인하십시오.

단계 **5** 온보딩 방법으로 **Use CLI Registration Key(CLI** 등록 키 사용**)**를 선택합니다.

단계 **6** **Device Name(**디바이스 이름**)** 필드에 디바이스 이름을 입력하고 **Next(**다음**)**를 클릭합니다.

단계 **7** Policy Assignment(정책 할당) 단계에서 드롭다운 메뉴를 사용하여 디바이스가 온보딩된 후 구축할 액세스 제어 정책을 선택합니다. 구성된 정책이 없는 경우 **Default Access Control Policy(**기본 액세스 제어 정책**)**를 선택합니다.

단계 **8** 온보딩 중인 디바이스가 물리적 디바이스인지 가상 디바이스인지 지정합니다. 가상 디바이스를 온보딩하는 경우 드롭다운 메뉴에서 디바이스의 성능 계층을 선택해야 합니다.

단계 **9** 디바이스에 적용할 라이선스를 선택합니다. **Next(**다음**)**를 클릭합니다.

단계 **10** CDO는 등록 키를 사용하여 명령을 생성합니다. SSH를 사용하여 온보딩 중인 디바이스에 연결합니다. "admin" 또는 이와 동등한 관리자 권한이 있는 사용자로 로그인하고 전체 등록 키를 있는 그대로 디바이스의 CLI에 붙여넣습니다.

참고: Firepower 1000, Firepower 2100, ISA 3000및 threat defense virtual디바이스의 경우 디바이스에 대한 SSH 연결을 열고 관리자로 로그인합니다. 전체 등록 명령을 복사하여 프롬프트에서 디바이스의 CLI 인터페이스에 붙여넣습니다. CLI에서 **Y**를 입력하여 등록을 완료합니다. 이전에 device manager에서 디바이스를 관리한 경우 **Yes(**예**)**를 입력하여 제출을 확인합니다.

단계 **11** CDO 온보딩 마법사에서 **Next(**다음**)**를 클릭합니다.

단계 **12** (선택 사항) **Inventory(**재고 목록**)** 페이지를 정렬하고 필터링하는 데 도움이 되도록 디바이스에 레이블을 추가합니다. 레이블을 입력하고 파란색 더하기 버튼을 선택합니다. 레이블은 CDO에 온보딩된 후 디바이스에 적용됩니다.

다음에 수행할 작업

디바이스가 동기화되면 **Inventory(**인벤토리**)** 페이지에서 방금 온보드한 디바이스를 선택하고 오른쪽에 있는 **Management(**관리**)** 창 아래에 나열된 옵션 중 하나를 선택합니다. 다음 작업을 수행하는 것이 좋습니다.

- 아직 생성하지 않은 경우 사용자 환경에 맞게 보안을 사용자 지정하려면 사용자 지정 액세스 제어 정책을 생성합니다. 자세한 내용은 *Cisco Defense Orchestrator*에서 클라우드 제공 *Firewall Management Center*로 *Firewall Threat Defense* 관리에서 액세스 제어 개요를 참조하십시오.
- Cisco SAL(Security Analytics and Logging)을 활성화하여 CDO 대시보드에서 이벤트를 보거나 보안 분석을 위해 디바이스를 Secure Firewall Management Center에 등록합니다. 자세한 내용은 *Cisco Defense Orchestrator*에서 클라우드 제공 *Firewall Management Center*로 *Firewall Threat Defense* 관리에서 Cisco Security Analytics and Logging을 참조하십시오.

로우 터치 프로비저닝을 사용하여 디바이스 온보딩

Firepower 1000, Firepower 2100 및 Secure Firewall 3100 디바이스만 로우 터치 프로비저닝 방법으로 온보딩할 수 있습니다.

시작하기 전에

온보딩 전에 다음이 완료되었는지 확인합니다.

- 클라우드 사용 Firewall Management Center가 테넌트에 대해 활성화되었습니다.
- 디바이스가 새로 설치되었지만 디바이스 CLI 또는 device manager에서 로그인한 적이 없습니다.
- 디바이스에서 버전 7.2 이상을 실행 중입니다. 버전 7.0.3은 로우 터치 프로비저닝을 지원하지 않습니다.

프로시저

단계 **1** CDO에 로그인합니다.

단계 **2** 탐색창에서 **Inventory(**재고 목록**)**를 클릭하고 파란색 더하기 버튼을 클릭합니다.

단계 **3** **FTD tile(**타일**)**을 클릭합니다.

단계 **4** **Management Mode(**관리 모드**)**에서 **FTD**가 선택되어 있는지 확인합니다.

경고! **Management Mode(**관리 모드**)**에서 **FTD**를 선택하면 이전 관리 플랫폼을 사용하여 디바이스를 관리할 수 없습니다. 인터페이스 구성을 제외한 모든 기존 정책 구성이 재설정됩니다. 디바이스를 온보딩한 후에는 정책을 다시 구성해야 합니다.

디바이스가 Secure Firewall device manager에서 관리를 유지하도록 하려면 **FDM**을 선택하고 등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스 온보딩에서 자세한 내용을 확인하십시오.

단계 **5** 디바이스 일련 번호 및 디바이스 이름을 입력합니다. **Next(**다음**)**를 선택합니다.

단계 **6** 비밀번호 재설정. **Yes, this new device has never been logged into or configured for a manager(**예**,** 이 새 디바이스는 로그인하거나 관리자용으로 구성한 적이 없습니다**)** 옵션을 선택합니다.

디바이스가 이전에 관리자에게 등록되었거나 아직 관리자에게 등록되어 있는 경우 일련 번호로 디바이스 온보딩, 8 페이지의 내용을 참조하십시오.

단계 **7** **Next(**다음**)**를 클릭합니다.

단계 **8** Policy Assignment(정책 할당) 단계에서 드롭다운 메뉴를 사용하여 디바이스가 온보딩된 후 구축할 액세스 제어 정책을 선택합니다. 구성된 정책이 없는 경우 **Default Access Control Policy(**기본 액세스 제어 정책**)**를 선택합니다.

단계 **9** 디바이스에 적용할 모든 를 선택합니다. **Next(**다음**)**를 클릭합니다.

다음에 수행할 작업

디바이스가 동기화되면 **Inventory(**인벤토리**)** 페이지에서 방금 온보드한 디바이스를 선택하고 오른쪽에 있는 **Management(**관리**)** 창 아래에 나열된 옵션 중 하나를 선택합니다. 다음 작업을 수행하는 것이 좋습니다.

- 아직 생성하지 않은 경우 사용자 환경에 맞게 보안을 사용자 지정하려면 사용자 지정 액세스 제어 정책을 생성합니다. 자세한 내용은 *Cisco Defense Orchestrator*에서 클라우드 제공 *Firewall Management Center*로 *Firewall Threat Defense* 관리에서 액세스 제어 개요를 참조하십시오.
- Cisco SAL(Security Analytics and Logging)을 활성화하여 CDO 대시보드에서 이벤트를 보거나 보안 분석을 위해 디바이스를 Secure Firewall Management Center에 등록합니다. 자세한 내용은 *Cisco Defense Orchestrator*에서 클라우드 제공 *Firewall Management Center*로 *Firewall Threat Defense* 관리에서 Cisco Security Analytics and Logging을 참조하십시오.

일련 번호로 디바이스 온보딩

Firepower 1000, Firepower 2100 및 Secure Firewall 3100 디바이스만 일련 번호 온보딩 방법으로 온보딩할 수 있습니다.

시작하기 전에

온보딩 전에 다음을 완료해야 합니다.

- 클라우드 사용 Firewall Management Center가 테넌트에 대해 활성화되었습니다.
- 디바이스의 CLI 구성이 성공적으로 완료되었는지 확인합니다. 자세한 내용은 CLI를 사용하여 Secure Firewall Threat Defense 디바이스의 초기 구성 완료을 참조하십시오.
- 디바이스를 온보딩하기 전에 사전 요구 사항 및 제한 사항을 검토합니다. 자세한 내용은 Cisco Defense Orchestrator에서 클라우드 제공 Firewall Management Center로 Firewall Threat Defense 관리에서 "디바이스를 클라우드 사용 Firewall Management Center에 온보딩하기 위한 사전 요건"을 참조하십시오.
- 디바이스가 온보딩 전에 활성화했을 수 있는 기존 스마트 라이선스를 등록 취소합니다.
- 디바이스가 로컬 관리용으로 구성되었으며 현재 Secure Firewall device manager에서 관리되고 있는지 확인합니다.
- 디바이스에서 버전 7.2 이상을 실행 중입니다. 버전 7.0.3은 일련 번호를 사용한 온보딩을 지원하지 않습니다.

프로시저

단계 **1** Secure Firewall device manager UI에서 **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)**로 이동하여 **Auto-enroll with Tenancy from Cisco Defense Orchestrator(Cisco Defense Orchestrator**에서 테넌시에 자동 등록**)** 옵션을 선택하고 **Register(**등록**)**를 클릭합니다.

단계 **2** CDO에 로그인합니다.

단계 **3** 탐색창에서 **Inventory(**재고 목록**)**를 클릭하고 파란색 더하기 버튼을 클릭합니다.

단계 **4** **FTD tile(**타일**)**을 클릭합니다.

단계 **5** **Management Mode(**관리 모드**)**에서 **FTD**가 선택되어 있는지 확인합니다.

Management Mode(관리 모드**)**에서 **FTD**를 선택하면 이전 관리 플랫폼을 사용하여 디바이스를 관리할 수 없습니다. 인터페이스 구성을 제외한 모든 기존 정책 구성이 재설정됩니다. 디바이스를 온보딩한 후에는 정책을 다시 구성해야 합니다.

단계 **6** 디바이스 일련 번호 및 디바이스 이름을 입력합니다. **Next(**다음**)**를 클릭합니다.

단계 **7** 비밀번호 재설정. **No, this device has been logged into and configured for a manager(**아니요**,** 이 디바이스는 관리자에 대해 로그인되어 구성되었습니다**.)**를 선택합니다. 이는 디바이스가 이미 device manager에 등록되었으며 해당 구성의 일부로 기본 비밀번호가 변경되었음을 의미합니다.

디바이스가 완전히 새로운 것이며 관리자에 대해 구성된 적이 없는 경우 로우 터치 프로비저닝을 사용하여 디바이스 온보딩, 6 페이지의 내용을 참조하십시오.

단계 **8** **Next(**다음**)**를 클릭합니다.

단계 **9** Policy Assignment(정책 할당) 단계에서 드롭다운 메뉴를 사용하여 디바이스가 온보딩된 후 구축할 액세스 제어 정책을 선택합니다. 구성된 정책이 없는 경우 **Default Access Control Policy(**기본 액세스 제어 정책**)**를 선택합니다.

단계 **10** 디바이스에 적용할 모든 라이선스를 선택합니다. **Next(**다음**)**를 클릭합니다.

다음에 수행할 작업

디바이스가 동기화되면 **Inventory(**인벤토리**)** 페이지에서 방금 온보드한 디바이스를 선택하고 오른쪽에 있는 **Management(**관리**)** 창 아래에 나열된 옵션 중 하나를 선택합니다. 다음 작업을 수행하는 것이 좋습니다.

- 아직 생성하지 않은 경우 사용자 환경에 맞게 보안을 사용자 지정하려면 사용자 지정 액세스 제어 정책을 생성합니다. 자세한 내용은 *Cisco Defense Orchestrator*에서 클라우드 제공 *Firewall Management Center*로 *Firewall Threat Defense* 관리에서 액세스 제어 개요를 참조하십시오.
- Cisco SAL(Security Analytics and Logging)을 활성화하여 CDO 대시보드에서 이벤트를 보거나 보안 분석을 위해 디바이스를 Secure Firewall Management Center에 등록합니다. 자세한 내용은 *Cisco Defense Orchestrator*에서 클라우드 제공 *Firewall Management Center*로 *Firewall Threat Defense* 관리에서 Cisco Security Analytics and Logging을 참조하십시오.

AWS VPC와 연결된 Threat Defense 디바이스 온보딩

다음 절차를 사용하여 클라우드 사용 Firewall Management Center에서 관리할 AWS VPC와 연결된 threat defense 디바이스의 방화벽을 온보딩하고 사전에 프로비저닝합니다.

시작하기 전에

온보딩 전에 다음 사전 요구 사항이 충족되었는지 확인합니다.

- 클라우드 사용 Firewall Management Center 기능을 활성화하고 테넌트와 연결해야 합니다.
- AWS VPC가 CDO에 이미 온보딩되어 있어야 합니다. 자세한 내용은 AWS VPC 온보딩을 참조하십시오.

프로시저

단계 **1** CDO에 로그인합니다.

단계 **2** 탐색창에서 **Inventory(**재고 목록**)**를 클릭하고 파란색 더하기 버튼을 클릭합니다.

단계 **3** **FTD** 타일을 선택합니다.

단계 **4** **Management Mode(**관리 모드**)**에서 **FTD**가 선택되어 있는지 확인합니다.

단계 **5** 온보딩 방법으로 **Use AWS VPC(AWS VPC** 사용**)**를 선택합니다. 온보딩된 AWS VPC가 없는 경우 이 단계에서 제공된 링크를 클릭하여 가상 환경을 온보딩할 수 있습니다.

단계 **6** 드롭다운 메뉴에서 **availability zone(**가용성 영역**)**을 선택합니다. 로컬 컴퓨터가 있는 영역이 아니라 클라우드 threat defense가 있는 영역을 선택합니다.

단계 **7** 다음 옵션 중 하나를 사용하여 관리 인터페이스 서브넷을 선택합니다.

- **Use existing subnets(**기존 서브넷 사용**)** - 드롭다운 메뉴를 확장하고 관리 인터페이스, 내부 인터페이스 및 외부 인터페이스 서브넷에 대해 적절한 서브넷을 선택합니다.
- **Create new subnets(**새 서브넷 생성**)** - 디바이스가 온보딩되면 사용할 서브넷 인터페이스 집합을 추가합니다. CDO는 이러한 서브넷을 자동으로 생성하여 온보딩 절차의 일부로 AWS VPC에 적용합니다.

진단 인터페이스는 관리 인터페이스와 동일한 인터페이스를 사용합니다.

단계 **8** **Select(**선택**)**를 클릭하여 서브넷을 할당합니다. **Next(**다음**)**를 클릭합니다.

단계 **9** **Device Name(**디바이스 이름**)** 필드에 디바이스 이름을 입력하고 **Next(**다음**)**를 클릭합니다.

단계 **10** Policy Assignment(정책 할당) 단계에서 드롭다운 메뉴를 사용하여 디바이스가 온보딩된 후 구축할 액세스 제어 정책을 선택합니다. 구성된 정책이 없는 경우 **Default Access Control Policy(**기본 액세스 제어 정책**)**를 선택합니다.

단계 **11** 디바이스에 적용할 **Subscription Licenses(**구독 라이선스**)**를 선택합니다. 가상 threat defense 디바이스에 대해 최소한 URL 라이선스가 선택되어 있어야 합니다.

다음에 수행할 작업

CDO가 클라우드 형성을 성공적으로 구축하고, 디바이스 연결을 초기화하고, 가상 디바이스 및 AWS VPC 환경과의 통신을 설정할 때까지 동기화할 수 없으므로 디바이스가 CDO의 **Inventory(**인벤토리**)** 페이지에 표시되는 데 몇 분 정도 걸릴 수 있습니다.

필요한 경우 온보딩 후 클라우드 사용 Firewall Management Center UI를 통해 가상 threat defense디바이스 성능 계층 선택을 수정할 수 있습니다.

클라우드 사용 **Firewall Management Center**에서 디바이스 삭제

디바이스가 클라우드 사용 Firewall Management Center에 등록된 경우에도 CDO는 디바이스 등록을 관리합니다. 클라우드 사용 Firewall Management Center에서 디바이스를 제거하려면 CDO 대시보드에서 디바이스를 삭제해야 합니다.

참고 CDO는 AWS VPC 환경과 연결된 디바이스의 삭제를 동기화하지 않습니다. AWS VPC UI에서 디바이스를 삭제해야 합니다. 자세한 내용은 AWS 설명서를 참조하십시오.

프로시저

단계 **1** CDO에 로그인하고 **Inventory(**인벤토리**)**를 클릭합니다.

단계 **2** 필터 또는 검색 창을 사용하여 삭제할 디바이스를 찾습니다. 디바이스 행이 강조 표시되도록 선택합니다.

단계 **3** 오른쪽의 Device Actions(디바이스 작업) 창에서 **Remove(**제거**)**를 클릭합니다.

단계 **4** 메시지가 표시되면 **OK(**확인**)**를 선택하여 선택한 디바이스 제거를 확인합니다. 디바이스를 온보드 상태로 유지하려면 **Cancel(**취소**)**을 클릭합니다.

문제 해결

다음 시나리오를 사용하여 온보딩 문제를 해결합니다.

CLI 등록 키를 사용하여 클라우드 사용 **Firewall Management Center**에 디바이스 온보딩 문제 해결

오류**:** 온보딩 후 디바이스가 설정 보류 중 상태로 유지됨

디바이스 등록에 실패하면 디바이스의 연결 상태가 **Pending Setup(**설정 보류 중**)**으로 표시됩니다. CDO는 오른쪽에 있는 패널에서 **Registration Failed(**등록 실패**)** 메시지와 **Retry Onboarding(**온보딩 재시도**)** 버튼을 표시하여 즉시 디바이스 온보딩을 다시 시도할 수 있습니다.

CDO에 온보딩한 후 3분 이내에 디바이스 CLI에서 `configuration manager` 명령을 실행하지 않으면 디바이스의 등록 시도가 만료되고 등록 실패가 발생합니다. 다음 절차를 사용하여 문제를 해결합니다.

프로시저

단계 **1** CDO에 로그인하여 **Inventory(**인벤토리**)** 페이지로 이동합니다. 등록에 실패한 디바이스를 찾습니다.

단계 **2** 오른쪽에 있는 패널에서 **Registration Failed(**등록 실패**)** 창을 찾습니다. 디바이스의 CLI 등록 키 옆에 있는 **Copy(**복사**)**를 클릭합니다. 이 작업은 CLI 키를 로컬 클립보드에 복사합니다.

단계 **3** 디바이스에 대한 SSH 연결을 열고 관리자로 로그인합니다.

단계 **4** CLI 등록 키를 디바이스의 CLI 인터페이스에 붙여넣습니다. CLI에서 **Y**를 입력하여 등록을 완료합니다. 이전에 device manager에서 디바이스를 관리한 경우 **Yes(**예**)**를 입력하여 제출을 확인합니다.

일련 번호를 사용하도록 클라우드 사용 **Firewall Management Center**에 디바이스 온보딩 문제 해결

디바이스가 오프라인이거나 연결 불가능

온보딩 프로세스 중에 또는 온보딩 후 특정 시점에 디바이스에 연결할 수 없는 경우 CDO에 연결 불가 연결 상태가 표시됩니다. 디바이스는 연결할 수 있을 때까지 CDO에 완전히 온보딩할 수 없습니다. 다음 시나리오가 원인일 수 있습니다.

- 디바이스가 잘못 연결되었습니다.
- 네트워크에 디바이스의 고정 IP 주소가 필요할 수 있습니다.
- 네트워크에서 맞춤형 DNS를 사용하거나 네트워크에서 외부 DNS 차단이 있습니다.
- 디바이스가 유럽 지역(https://defenseorchestrator.eu/)과 연결된 경우 PPPoE 인증을 활성화해야 할 수 있습니다. 다른 도메인의 경우 도메인 요구 사항을 검토합니다.
- 디바이스가 방화벽에 의해 차단되었거나 연결을 위해 포트를 잘못 차단하고 있습니다. 디바이스 네트워크 요구 사항, 4 페이지를 검토하고 올바른 발신 포트가 활성화되어 있는지 확인합니다.

오류: 일련 번호가 이미 요청됨

디바이스를 외부 벤더에서 구매했음

디바이스를 외부 벤더에서 구매했는데 일련 번호가 이미 요청됨 오류와 함께 온보딩에 실패하는 경우 디바이스가 여전히 벤더의 테넌트에 연결되어 있을 수 있습니다. 디바이스 및 일련 번호를 요청하려면 다음 단계를 수행합니다.

1. CDO 테넌트에서 디바이스를 삭제합니다.
2. 디바이스에 FXOS 이미지를 설치합니다. 자세한 내용은 Firepower 1000/21000 및 Secure Firewall 3100 Firepower Threat Defense용 Cisco FXOS 문제 해결 가이드의 "리이미징 절차" 장을 참조하십시오.
3. 노트북을 디바이스의 콘솔 포트에 연결합니다.
4. FXOS CLI에 연결하고 관리자로 로그인합니다.
5. FXOS CLI에서 `firepower # connect local-mgmt` 명령을 사용하여 **local-mgmt**에 연결합니다.
6. `firepower(local-mgmt) # cloud deregister` 명령을 실행하여 클라우드 테넌시에서 디바이스를 등록 취소합니다.
7. 디바이스가 등록 취소되면 CLI 인터페이스가 성공 메시지를 반환합니다. 메시지의 예:

```
Example: firepower(local-mgmt) # cloud deregister Release Image Detected RESULT=success
 MESSAGE=SUCCESS 10, X-Flow-Id: 2b3c9e8b-76c3-4764-91e4-cfd9828e73f9
```

참고 디바이스가 다른 CDO 테넌트에 등록된 적이 없는 경우 `RESULT=success MESSAGE=DEVICE_NOT_FOUND` 메시지가 표시됩니다.

8. 일련 번호를 사용하여 디바이스를 CDO 테넌트에 온보딩합니다. 자세한 내용은 일련 번호로 디바이스 온보딩, 8 페이지을 참조하십시오.

다른 지역의 **CDO** 테넌트가 디바이스를 요청함

디바이스가 이전에 다른 지역의 다른 CDO 인스턴스에 의해 관리되었으며 여전히 해당 테넌트에 등록되어 있을 수 있습니다.

디바이스가 현재 등록되어 있는 테넌트에 액세스할 수 있는 경우 다음 절차를 사용합니다.

1. CDO 테넌트에서 디바이스를 삭제합니다.
2. 디바이스의 device manager UI에 로그인합니다.
3. **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)**로 이동합니다.
4. **Cloud Services(**클라우드 서비스**)**를 클릭하고 드롭다운 목록에서 **Unregister Cloud Services(**클라우드 서비스 등록 취소**)**를 선택합니다.
5. 작업을 확인하고 **Unregister(**등록 취소**)**를 클릭합니다. 이 작업은 디바이스가 CDO에서 제거되었음을 나타내는 경고를 생성합니다. 이는 정상적인 동작입니다.
6. 올바른 지역의 CDO 테넌트에 로그인하고 디바이스를 온보딩합니다. 자세한 내용은 일련 번호로 디바이스 온보딩, 8 페이지을 참조하십시오.
7. **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)**로 이동합니다.
8. **Cloud Services(**클라우드 서비스**)**를 클릭하고 드롭다운 목록에서 **Unregister Cloud Services(**클라우드 서비스 등록 취소**)**를 선택합니다.
9. **Auto-enroll with Tenancy from Cisco Defense Orchestrator(Cisco Defense Orchestrator**에서 테넌시로 자동 등록**)**를 선택하고 **Register(**등록**)**를 클릭합니다. 디바이스는 새 지역에 속하는 새 테넌트에 매핑되고 CDO는 디바이스를 온보딩합니다.

테넌트에 액세스할 수 없는 경우 아래 절차를 사용합니다.

1. 콘솔 포트에서 FXOS CLI에 연결하고 관리자로 로그인합니다. FXOS CLI에 로그인하는 방법에 대한 자세한 내용은 FXOS CLI 액세스를 참조하십시오.
2. FXOS CLI에서 `firepower # connect local-mgmt` 명령을 사용하여 **local-mgmt**에 연결합니다.
3. `firepower(local-mgmt) # cloud deregister` 명령을 실행하여 클라우드 테넌시에서 디바이스를 등록 취소합니다.
4. 디바이스가 등록 취소되면 CLI 인터페이스가 성공 메시지를 반환합니다. 메시지의 예:

```
Example: firepower(local-mgmt) # cloud deregister Release Image Detected RESULT=success
 MESSAGE=SUCCESS 10, X-Flow-Id: 2b3c9e8b-76c3-4764-91e4-cfd9828e73f9
```

참고 디바이스가 다른 CDO 테넌트에 등록된 적이 없는 경우 `RESULT=success MESSAGE=DEVICE_NOT_FOUND` 메시지가 표시됩니다.

5. 올바른 도메인의 CDO 테넌트에서 디바이스를 온보딩합니다. 자세한 내용은 일련 번호로 디바이스 온보딩, 8 페이지을 참조하십시오.
6. 디바이스의 device manager UI에서 **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)**로 이동합니다.
7. **Auto-enroll with Tenancy from Cisco Defense Orchestrator(Cisco Defense Orchestrator**에서 테넌시로 자동 등록**)**를 선택하고 **Register(**등록**)**를 클릭합니다. 디바이스는 새 지역에 속하는 새 테넌트에 매핑되고 CDO는 디바이스를 온보딩합니다.

오류: 클레임 오류

디바이스를 온보딩할 때 잘못된 일련 번호를 입력하면 CDO에서 **Claim Error(**클레임 오류**)** 상태를 생성합니다.

참고 디바이스가 CDO 내의 올바른 지역에서 클레임되었는지 확인합니다.

아래의 절차를 사용하여 이 문제를 해결합니다.

프로시저

단계 **1** CDO에 로그인하여 **Inventory(**인벤토리**)** 페이지로 이동합니다. 오류가 있는 디바이스를 찾습니다.

단계 **2** 강조 표시할 디바이스를 선택하고 디바이스를 CDO에서 제거합니다.

단계 **3** 다음을 확인합니다.

- 디바이스가 온라인 상태이며 인터넷에 연결할 수 있습니다.
- 디바이스가 아직 CDO 인스턴스에 온보딩되지 않았거나 다른 지역의 CDO 테넌트가 클레임하지 않았습니다.

단계 **4** 디바이스의 일련 번호를 찾습니다. 다음 방법 중 하나를 사용할 수 있습니다.

- 1000, 2100 및 3100 시리즈 모델의 경우 물리적 디바이스에서 일련 번호를 찾습니다.
- 디바이스에 대한 SSH 연결을 열고 `show serial-number` 명령을 실행합니다.
- 디바이스가 현재 FDM 관리인 경우 device manager UI에 로그인하여 **Cloud Services(**클라우드 서비스**)** 페이지에서 일련 번호를 찾습니다.

단계 **5** CDO에서 올바른 일련 번호를 사용하여 디바이스를 온보딩합니다. 자세한 내용은 일련 번호로 디바이스 온보딩, 8 페이지를 참조하십시오.

오류: 클레임 실패

디바이스 온보딩을 시도한 후 **Error: Failed to Claim connectivity status(**오류**:** 연결 상태를 요청하지 못함**)** 또는 오류 메시지가 표시되는 경우 다음이 원인일 수 있습니다.

- 보안 서비스 익스체인지 플랫폼에 연결되지 않는 일시적인 문제가 있을 수 있습니다.
- CDO 서버가 다운되었을 수 있습니다.

이 문제를 해결하려면 아래 절차를 따르십시오.

프로시저

단계 **1** CDO에 로그인하여 **Inventory(**인벤토리**)** 페이지로 이동합니다. 등록에 실패한 디바이스를 찾습니다.

단계 **2** 강조 표시할 디바이스를 선택하고 디바이스를 CDO 테넌트에서 제거합니다.

단계 **3** 디바이스를 CDO 테넌트에 다시 온보딩하기 전에 10분 이상 기다립니다. 자세한 내용은 로우 터치 프로비저닝을 사용하여 디바이스 온보딩, 6 페이지을 참조하십시오.

다음에 수행할 작업

여전히 디바이스를 클레임할 수 없는 경우 디바이스의 워크플로우를 검토하여 오류 메시지가 있는지 확인합니다. 있는 경우 워크플로를 내보내고 지원 케이스를 열어 문제를 추가로 해결합니다.

오류: 임시 오류

디바이스 비밀번호가 변경되지 않았음

원격 관리를 위해 디바이스를 구성할 때 디바이스의 기본 비밀번호를 변경하지 않았고 디바이스를 CDO에 온보딩할 때 **No, this device has been logged into and configured for a manager(**아니요**,** 이 디바이스는 관리자에 대해 로그인되어 구성되었습니다**.)** 옵션을 선택한 경우 디바이스가 **Inventory(**인벤토리**)** 페이지에서 **UnProvisioned(**프로비저닝되지 않음**)** 연결 상태를 생성합니다.

이 문제를 해결하려면 다음 절차를 수행합니다.

1. CDO에 로그인하여 **Inventory(**인벤토리**)** 페이지로 이동합니다.
2. **UnProvisioned(**프로비저닝되지 않음**)** 연결 상태가 강조 표시되도록 디바이스를 찾아 선택합니다.
3. 오른쪽에 있는 창에서 **Change Password(**비밀번호 변경**)** 창을 찾습니다.
4. **Change Password(**비밀번호 변경**)**를 클릭하고 디바이스의 새 비밀번호를 입력합니다. 기본 비밀번호를 덮어씁니다.

디바이스가 CDO에 온보딩되고 완전히 동기화되는 데 몇 분 정도 걸릴 수 있습니다.

디바이스 비밀번호가 이미 변경됨

원격 관리를 위해 디바이스를 구성할 때 디바이스의 기본 비밀번호를 변경했고 디바이스를 CDO에 온보딩할 때 **Is this device that has never belogin or configured before(**이전에 로그인하거나 구성한 적이 없는 새 디바이스입니까**?)** 옵션을 선택한 경우 CDO은 **Invenotry(**인벤토리**)** 페이지에서 **UnProvisioned(**프로비저닝되지 않음**)** 연결 상태를 생성합니다.

이 문제를 해결하려면 다음 절차를 수행합니다.

1. CDO에 로그인하여 **Inventory(**인벤토리**)** 페이지로 이동합니다.
2. **UnProvisioned(**프로비저닝되지 않음**)** 연결 상태가 강조 표시되도록 디바이스를 찾아 선택합니다.
3. 오른쪽에 있는 창에서 **Confirm and Proceed(**확인 후 진행**)** 창을 찾습니다.
4. **Confirm and Proceed(**확인 후 진행**)**를 클릭합니다. 이 작업은 온보딩 마법사에서 제공된 비밀번호를 무시하고 디바이스의 기본 비밀번호를 복원합니다. CDO은 디바이스 온보드를 계속 진행합니다.

기타 임시 오류 시나리오

디바이스의 기본 비밀번호 구성과 상관없이, 온보딩 프로세스 중에 디바이스가 **UnProvisioned(**프로비저닝되지 않음**)** 연결 상태가 될 수 있습니다. 온보딩 마법사에서 선택한 비밀번호가 디바이스의 상태에 대해 정확한지 확인한 경우 다음 옵션을 고려하여 문제를 해결합니다.

- 디바이스를 선택하여 강조 표시합니다. 화면의 오른쪽 창에 있는 창에서 **Retry(**재시도**)**를 클릭하여 CDO에서 기존 임시 매개변수로 디바이스를 다시 온보딩합니다.
- **Inventory(**인벤토리**)** 페이지에서 디바이스를 삭제하고 디바이스를 다시 온보딩해 보십시오.
- 디바이스의 device manager UI에서 **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)**로 이동합니다. **Auto-enroll with Tenancy from Cisco Defense Orchestrator(Cisco Defense Orchestrator**에서 테넌시로 자동 등록**)**를 선택하고 **Register(**등록**)**를 클릭합니다.

여전히 디바이스를 클레임할 수 없는 경우 디바이스의 워크플로우를 검토하여 오류 메시지가 있는지 확인합니다. 있는 경우 워크플로를 내보내고 지원 케이스를 열어 문제를 추가로 해결합니다.

디바이스 관리 관련 정보

management center를 사용하여 디바이스를 관리합니다.

Management Interfaces(관리 인터페이스)관리 인터페이스

디바이스를 설정할 때 연결할 IP 주소를 지정합니다. 관리 및 이벤트 트래픽은 초기 등록 시 이 주소로 이동합니다.

참고 일부 경우에 디바이스는 다른 관리 인터페이스에서 초기 연결을 설정할 수 있습니다. 후속 연결은 지정된 IP 주소가 있는 관리 인터페이스를 사용해야 합니다.

디바이스에 별도의 이벤트 전용 인터페이스가 있는 경우, 네트워크가 허용하는 경우 매니지드 디바이스에서 후속 이벤트 트래픽을 이벤트 전용 인터페이스로 보냅니다. 또한 일부 매니지드 디바이스 모델에는 이벤트 전용 트래픽에 대해 구성할 수 있는 추가 관리 인터페이스가 포함되어 있습니다.

참고 관리를 위해 데이터 인터페이스를 구성하는 경우 별도의 관리 및 이벤트 인터페이스를 사용할 수 없습니다.

이벤트 네트워크가 다운되면 이벤트 트래픽은 매니지드 디바이스의 일반 관리 인터페이스로 되돌아갑니다.

데이터 인터페이스 정보

장치와의 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 CDO 액세스가 유용합니다. CDO는 데이터 인터페이스에서 원격으로 관리되는 FTD의 고가용성을 지원합니다.

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 CDO를 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. Amazon Web Services의 FTDv에서는 콘솔 포트를 사용할 수 없으므로 구성을 계속하기 전에 관리 인터페이스에 대한 SSH 액세스를 유지해야 합니다. 또는 데이터 인터페이스를 설정하기 전에 모든 CLI 구성(**configure manager add** 명령 포함)을 완료해야 합니다.

디바이스 관리 인터페이스의 네트워크 라우트

관리 인터페이스(이벤트 전용 인터페이스 포함)는 정적 경로만 지원하여 원격 네트워크에 연결할 수 있습니다. 매니지드 디바이스를 설정하면 설정 과정에서 지정한 게이트웨이 IP 주소에 대한 기본 경로가 생성됩니다. 이 경로는 삭제할 수 없으며 게이트웨이 주소만 수정할 수 있습니다.

참고 전용 관리 인터페이스를 사용하는 대신 관리용 데이터 인터페이스를 설정하는 경우 데이터 라우팅 테이블을 사용하도록 트래픽이 백플레인을 통해 라우팅됩니다. 이 섹션의 정보는 적용되지 않습니다.

원격 네트워크에 액세스하기 위해서는 관리 인터페이스당 최소 1개의 정적 경로가 권장됩니다. 다른 디바이스에서 디바이스로의 라우팅 문제를 비롯하여 잠재적인 라우팅 문제를 방지하려면 각 인터페이스를 별도의 네트워크에 배치하는 것이 좋습니다. 동일한 네트워크의 인터페이스에서 문제가 발생하지 않으면 고정 경로를 올바르게 설정해야 합니다. 예를 들어 management0과 management1은 동일한 네트워크에 있지만 FTD 관리 및 이벤트 인터페이스는 서로 다른 네트워크에 있습니다. 게이트웨이는 192.168.45.1입니다. 10.6.6.1/24에서 management1을 관리 이벤트 전용 인터페이스에 연결하려는 경우 동일한 게이트웨이 192.168.45.1로 10.6.6.0/24에서 management1까지의 고정 경로를 생성할 수 있습니다. 10.6.6.0/24 트래픽은 기본 경로에 도달하기 전에 이 경로에 도달하므로 management1이 예상대로 사용됩니다.

Threat Defense 디바이스의 명령줄 인터페이스에 로그인

threat defense 디바이스에서 명령줄 인터페이스에 직접 로그인 할 수 있습니다.

참고 사용자가 3회 연속 SSH를 통한 CLI 로그인에 실패한 경우, 시스템이 SSH 연결을 종료합니다.

시작하기 전에

기본 관리자 사용자를 사용하여 초기 로그인에 대한 초기 설정 프로세스를 완료합니다. **configure user add** 명령을 사용하여 CLI에 로그인할 수 있는 사용자 어카운트를 추가로 생성할 수 있습니다.

프로시저

단계 **1** 콘솔 포트 또는 SSH를 사용하여 threat defense CLI에 연결합니다.

관리 인터페이스에 SSH를 수는 threat defense 디바이스의 관리 인터페이스에 SSH할 수 있습니다. SSH 연결용 인터페이스를 여는 경우 데이터 인터페이스에 있는 주소에 연결할 수도 있습니다. 데이터 인터페이스에 대한 SSH 액세스는 기본값으로 사용 해제 상태입니다. 보안 셸 설정를 참조하여 특정 데이터 인터페이스에 SSH를 연결합니다.

물리적 디바이스의 경우 디바이스에서 콘솔 포트에 직접 연결할 수 있습니다. 디바이스에 포함된 콘솔 케이블을 사용하여 PC를 콘솔에 연결합니다(터미널 에뮬레이터 9600보드, 8 데이터 비트, 패리티

없음, 1 정지 비트, 흐름 제어 없음). 콘솔 케이블에 대한 자세한 내용은 디바이스용 하드웨어 가이드를 참조하십시오.

사용자가 콘솔 포트에서 액세스하는 초기 CLI는 디바이스 유형에 따라 다릅니다.

- ISA 3000 및 threat defense virtual—콘솔 포트의 CLI는 일반 threat defense CLI입니다.
- 기타 모듈—콘솔 포트의 CLI는 FXOS입니다. **connect ftd** 명령을 사용하여 threat defense CLI로 이동할 수 있습니다. FXOS CLI를 섀시 레벨 컨피그레이션 및 문제 해결용으로만 사용합니다. 기본 컨피그레이션, 모니터링 및 일반 시스템 트러블슈팅 시에는 threat defense CLI를 사용합니다. FXOS 명령에 대한 자세한 내용은 FXOS 설명서를 참조하십시오.

단계 **2** 관리자 사용자 이름 및 비밀번호로 로그인합니다.

단계 **3** CLI 프롬프트(>)에서 명령줄 액세스 수준에서 허용되는 명령 중 하나를 사용합니다.

단계 **4** (선택 사항) 진단 CLI에 액세스합니다.

system support diagnostic-cli

고급 문제 해결용으로 이 CLI를 사용합니다. 이 CLI에는 추가 **show** 및 기타 명령이 포함되어 있습니다.

이 CLI는 사용자 EXEC 모드 및 권한 EXEC 모드라는 두 개의 하위 모드가 있습니다. 권한 EXEC 모드에서 더 많은 명령을 사용할 수 있습니다. 권한 EXEC 모드로 들어가려면 **enable** 명령을 입력합니다. 메시지가 표시되면 비밀번호를 입력하지 않고 enter 키를 누릅니다.

예제**:**

```
> system support diagnostic-cli
firepower> enable
Password:
firepower#
```

일반 CLI로 돌아가려면 **Ctrl-a**, **d**를 입력합니다.