Defense Orchestrator에 FDM 온보드

목차

소개

이 문서에서는 등록 키를 사용하여 FDM(Firepower Device Manager)에서 관리되는 디바이스를 Cisco CDO(Defense Orchestrator)에 온보딩하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Firepower 장치 관리자(FDM)
- CDO(Cisco Defense Orchestrator)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 버전 7.4.1을 실행하는 FDM(firepower 장치 관리자) Azure

호환되는 버전 및 제품의 포괄적인 목록을 보려면 Secure Firewall Threat Defense 호환성 가이드를 참조하십시오.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

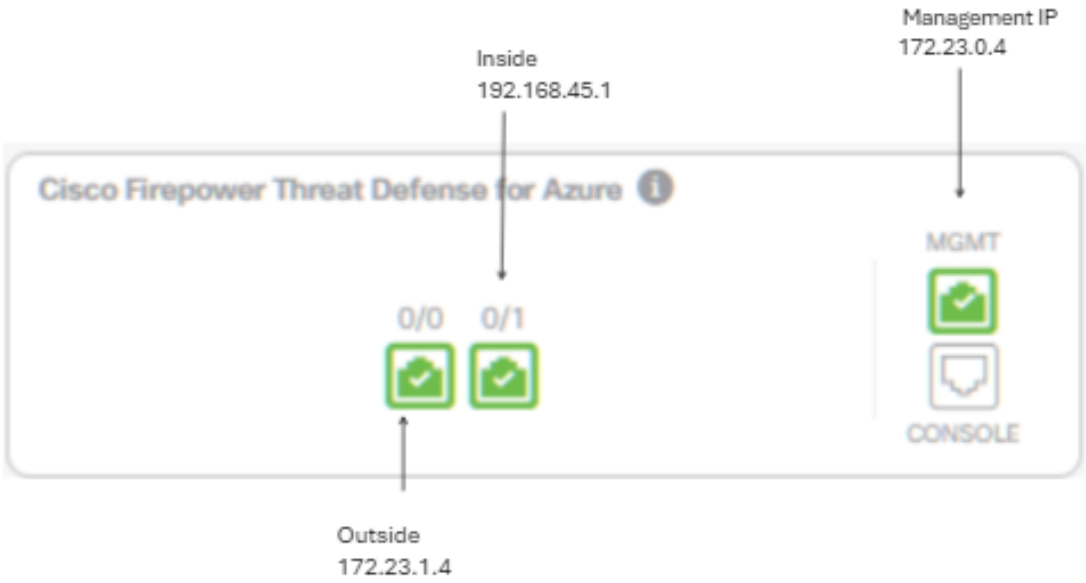
등록 키를 사용하여 FDM 관리 디바이스에서 Cisco Defense Orchestrator(CDO)로 온보딩 프로세스를 시작하기 전에 다음 전제 조건을 충족해야 합니다.

1. 호환되는 버전: 장치에서 버전 6.6 이상을 실행해야 합니다.
2. 네트워크 요구 사항: Cisco Defense Orchestrator를 관리되는 디바이스에 연결
3. 관리 소프트웨어: FDM(Secure Firewall Device Manager)을 통해 디바이스를 관리해야 합니다.
4. 라이센싱: 디바이스에서 90일 평가 라이센스 또는 스마트 라이센스를 사용할 수 있습니다.
5. 기존 등록: 온보딩 프로세스 중에 충돌을 피하려면 디바이스가 Cisco Cloud Services에 이미 등록되어 있지 않은지 확인합니다.
6. Pending Changes(보류 중인 변경 사항): 디바이스에 보류 중인 변경 사항이 없는지 확인합니다.
7. DNS 구성: DNS 설정은 FDM 관리 디바이스에서 올바르게 구성해야 합니다.
8. 시간 서비스: 디바이스의 시간 서비스를 정확하게 구성하여 네트워크 시간 프로토콜과의 동기화를 보장할 수 있습니다.
9. FDM 지원 활성화에 대한 요구 사항입니다. FDM(Firewall Device Manager) 지원 및 해당 기능은 요청 시 배타적으로 부여됩니다. 테넌트에서 FDM 지원이 활성화되지 않은 사용자는 FDM 관리 디바이스에 구성을 관리하거나 배포할 수 없습니다. 이 플랫폼을 활성화하려면 사용자가 FDM 지원 활성화를 위한 요청을 지원 팀에 보내야 합니다.

구성

네트워크 다이어그램

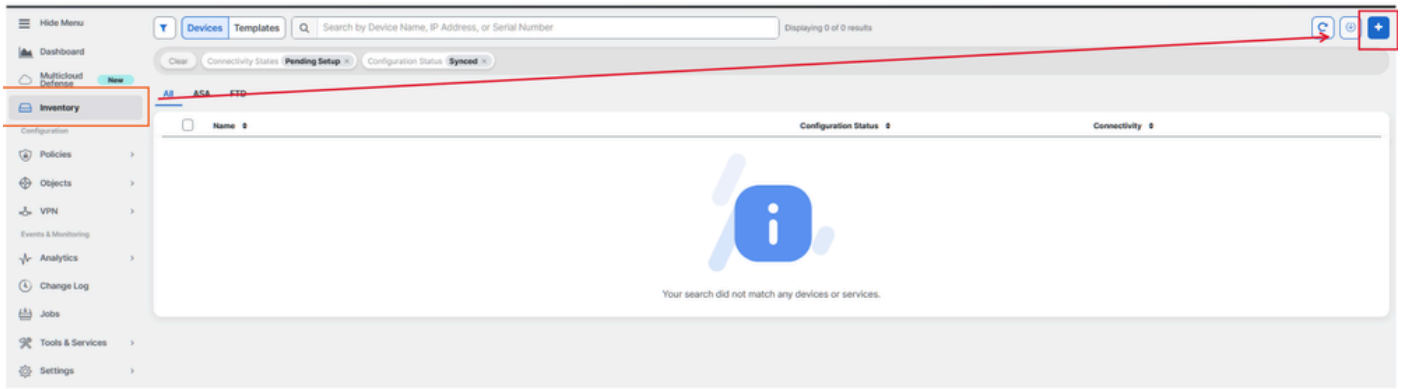
이 문서에서는 관리 인터페이스를 통해 제어되는 FDM(Firepower 장치 관리자) 장치에 대해 중점적으로 설명합니다. 이 인터페이스에는 CDO(Cisco Defense Orchestrator)에 디바이스를 등록하는 데 필수적인 인터넷 액세스가 있습니다.



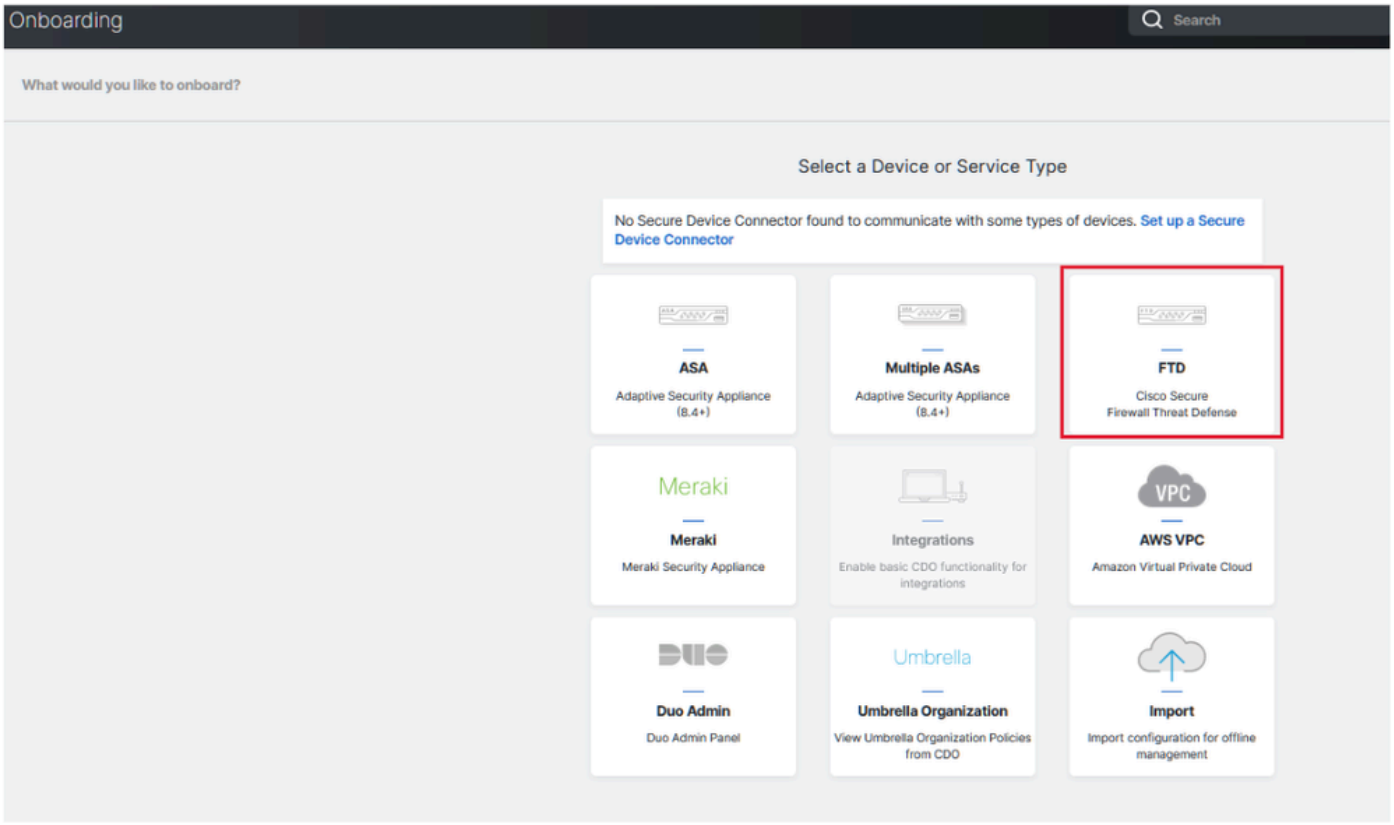
설정

1단계. CDO(Cisco Defense Orchestrator)에 로그인합니다.

2단계. Inventory(인벤토리) 창으로 이동하고 파란색 플러스 버튼을 선택하여 디바이스를 온보딩합니다.



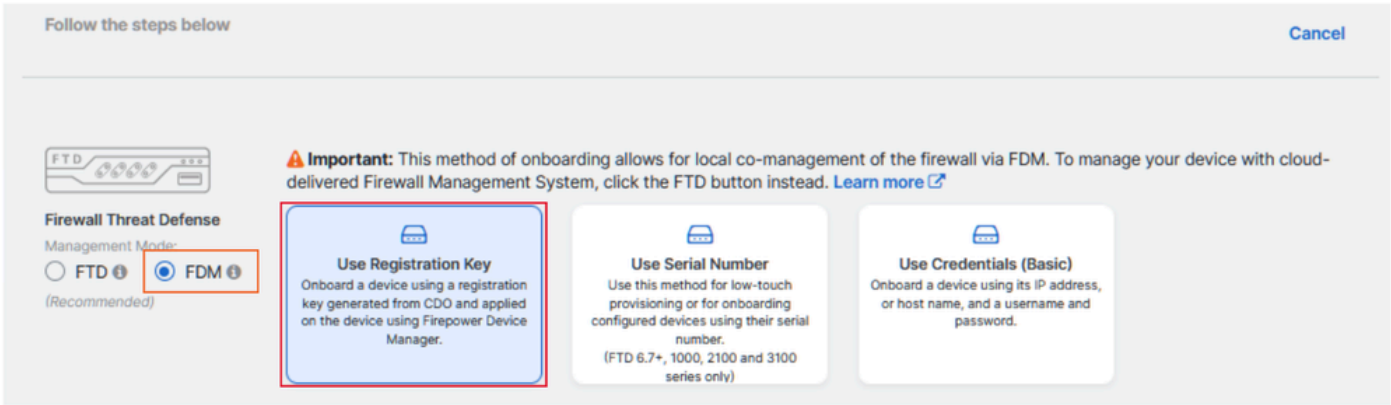
3단계. FTD 옵션을 선택합니다.



4단계 Onboard FTD Device'(온보드 FTD 디바이스) 섹션으로 이동하여 등록 프로세스를 시작합니다. Threat Defense 디바이스를 온보딩하기 위해 사용할 수 있는 방법에 유의해야 합니다.

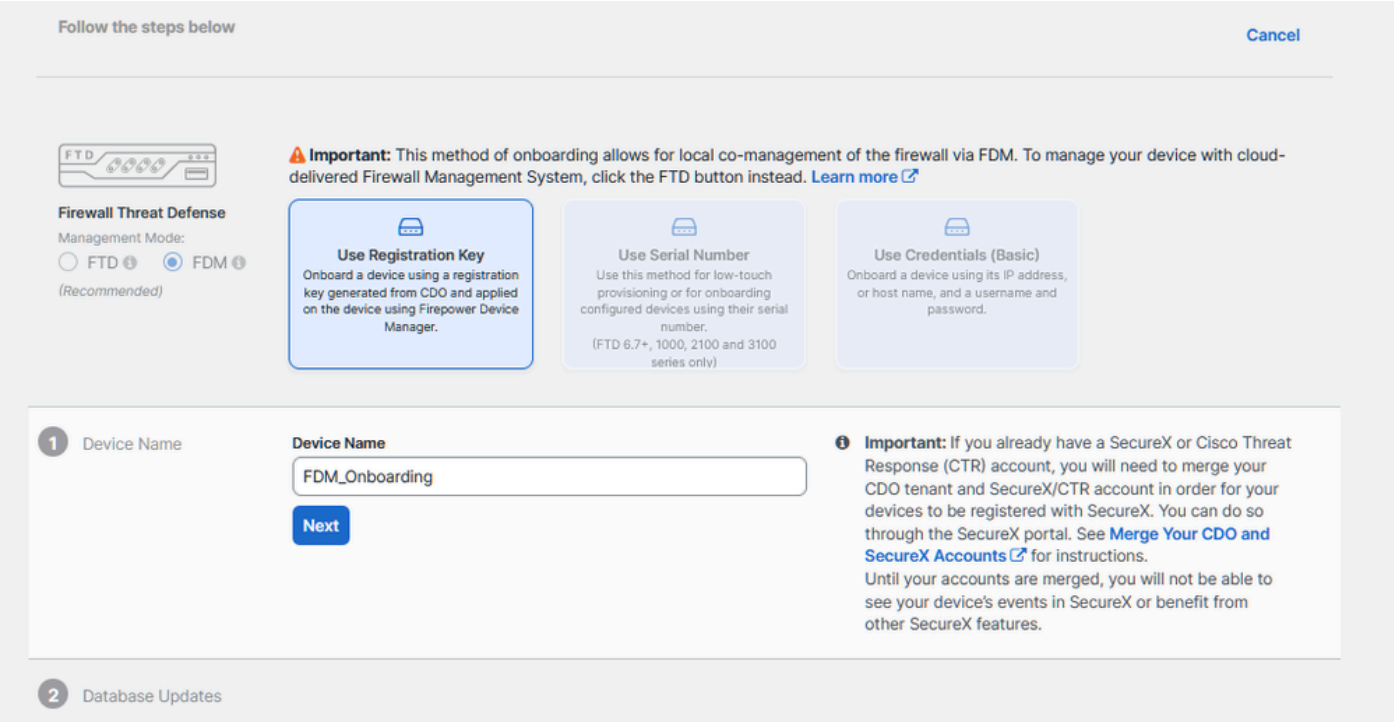
- 일련 번호별: 이 방법은 지원되는 소프트웨어 버전이 있는 Firepower 1000, Firepower 2100 또는 Secure Firewall 3100 Series와 같은 물리적 장치에 적용됩니다. 섀시 또는 PCA 일련 번호와 인터넷에 대한 네트워크 연결이 필요합니다.
- 등록 키 기준: 온보딩에 특히 DHCP를 통해 IP 주소를 수신하는 디바이스에 유리한 방식입니다. 디바이스 IP 주소가 변경되더라도 CDO와의 연결을 유지할 수 있기 때문입니다.
- 자격 증명 사용: 이 대체 방법에는 네트워크 내의 디바이스 컨피그레이션에 맞게 조정된 외부, 내부 또는 관리 인터페이스의 IP 주소와 디바이스 자격 증명을 입력하는 것이 포함됩니다.

이 프로세스에서는 FDM 옵션을 선택한 다음 Use Registration Key(등록 키 사용) 옵션을 선택하여 디바이스 IP 주소의 잠재적인 변경 사항과 상관없이 CDO에 대한 일관된 연결을 보장합니다.

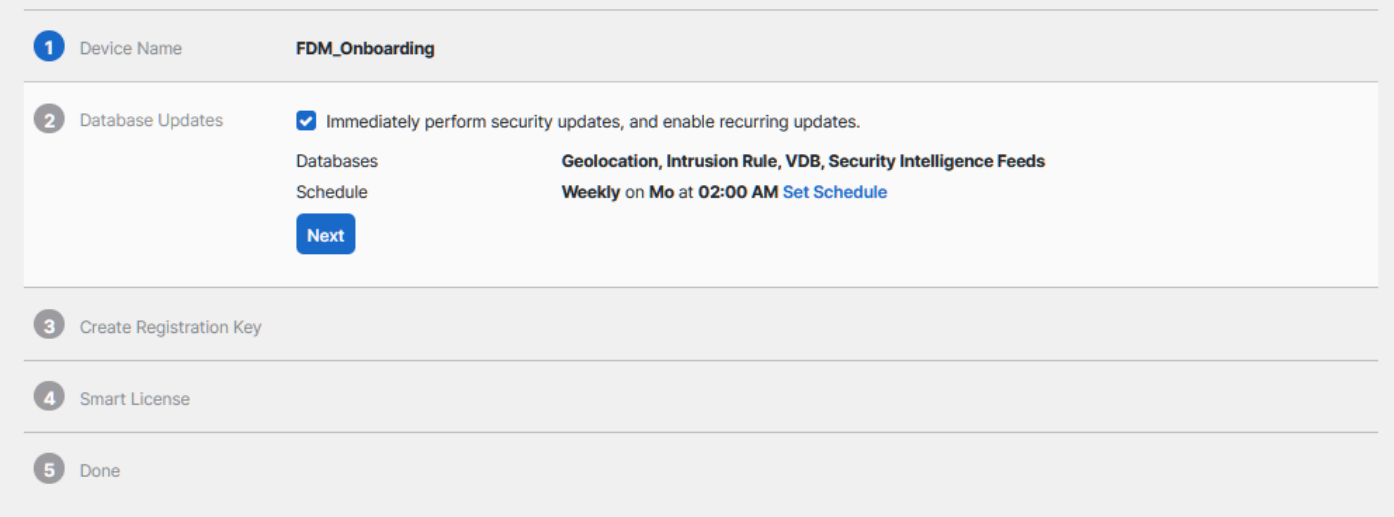


5단계. Device Name(디바이스 이름) 필드에 원하는 디바이스 이름을 입력하고 Policy

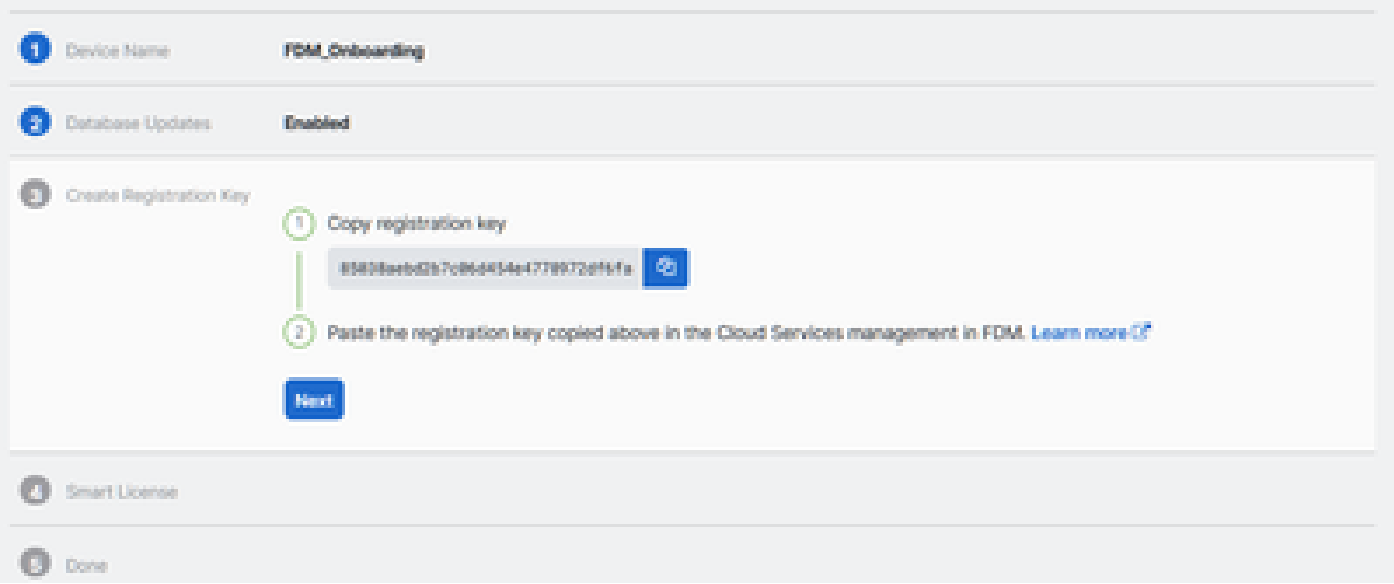
Assignment(정책 할당)를 지정합니다. 또한 디바이스와 연결해야 하는 서브스크립션 라이센스를 선택합니다.



6단계. Database Updates 섹션은 기본적으로 보안 업데이트를 즉시 실행하고 반복 업데이트를 설정하도록 구성됩니다. 이 설정을 변경해도 Secure Firewall 장치 관리자를 통해 설정된 기존 업데이트 일정은 변경되지 않습니다.



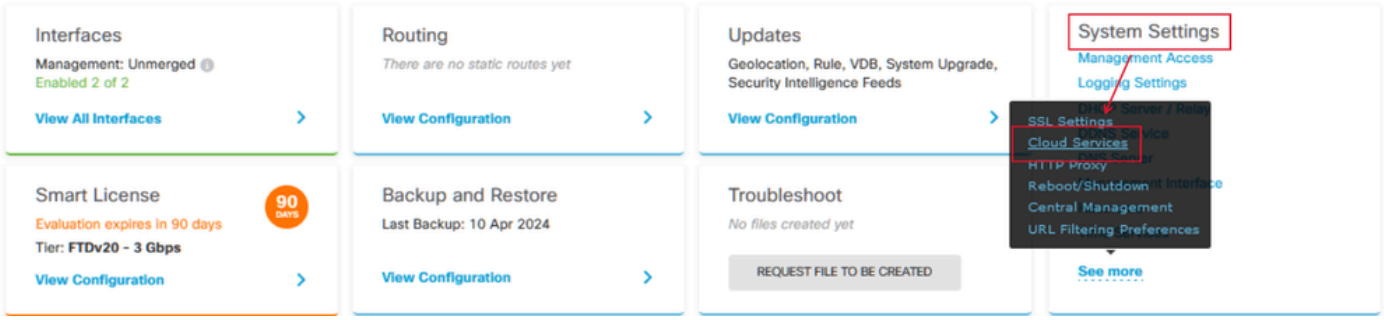
7단계. CLI Registration Key(CLI 등록 키) 섹션에서 CDO는 등록 키를 자동으로 생성합니다. 완료하기 전에 온보딩 인터페이스를 종료하면 인벤토리 내에서 디바이스에 대한 자리 표시자가 생성됩니다. 필요한 경우 나중에 이 위치에서 등록 키를 검색할 수 있습니다.



8단계. Copy(복사) 아이콘을 사용하여 생성된 등록 키를 복사합니다.

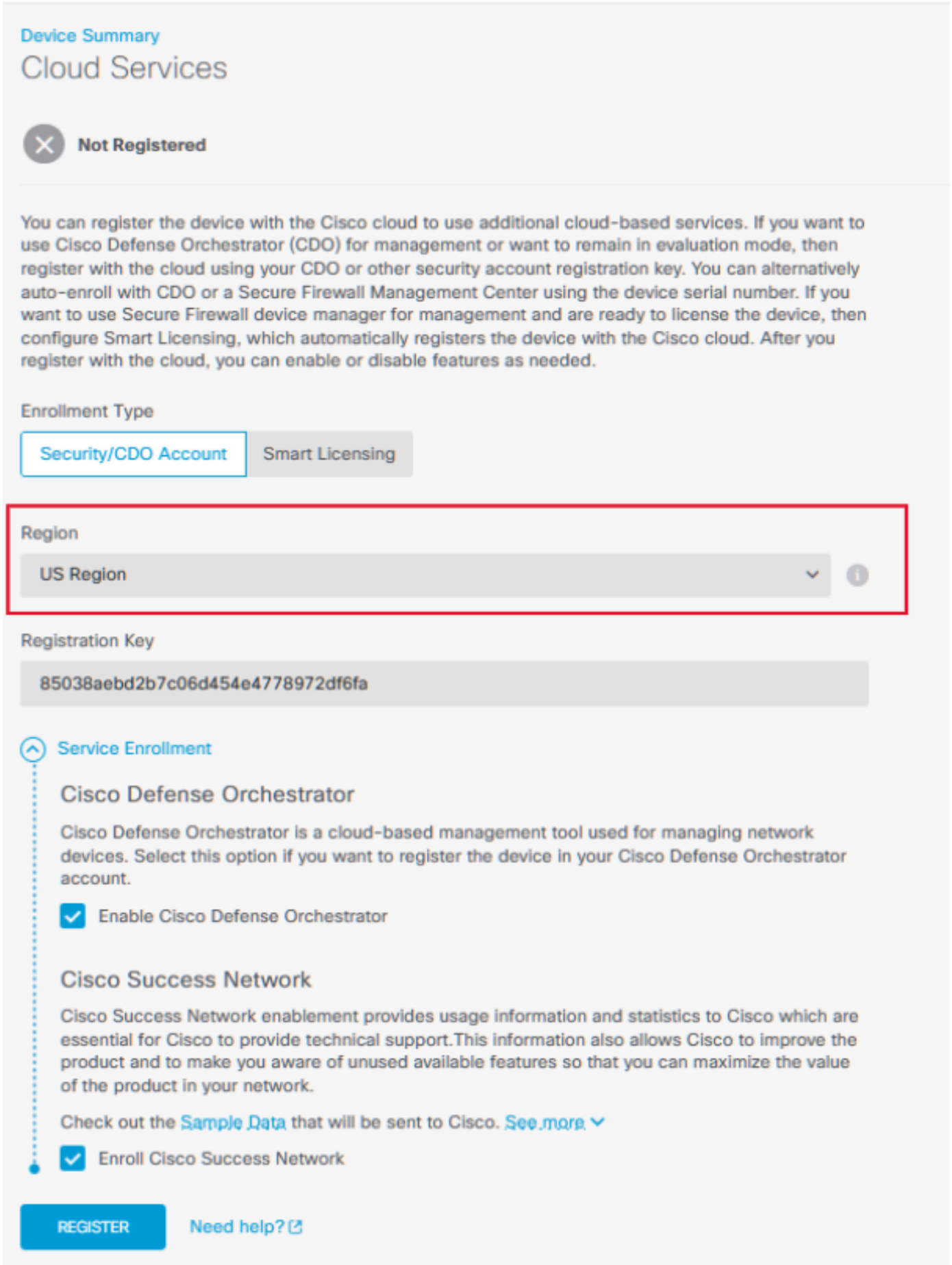
9단계. CDO에 온보딩하기 위한 Secure Firewall Device Manager 디바이스에 액세스합니다.

10단계. System Settings(시스템 설정) 메뉴에서 Cloud Services(클라우드 서비스)를 선택합니다.

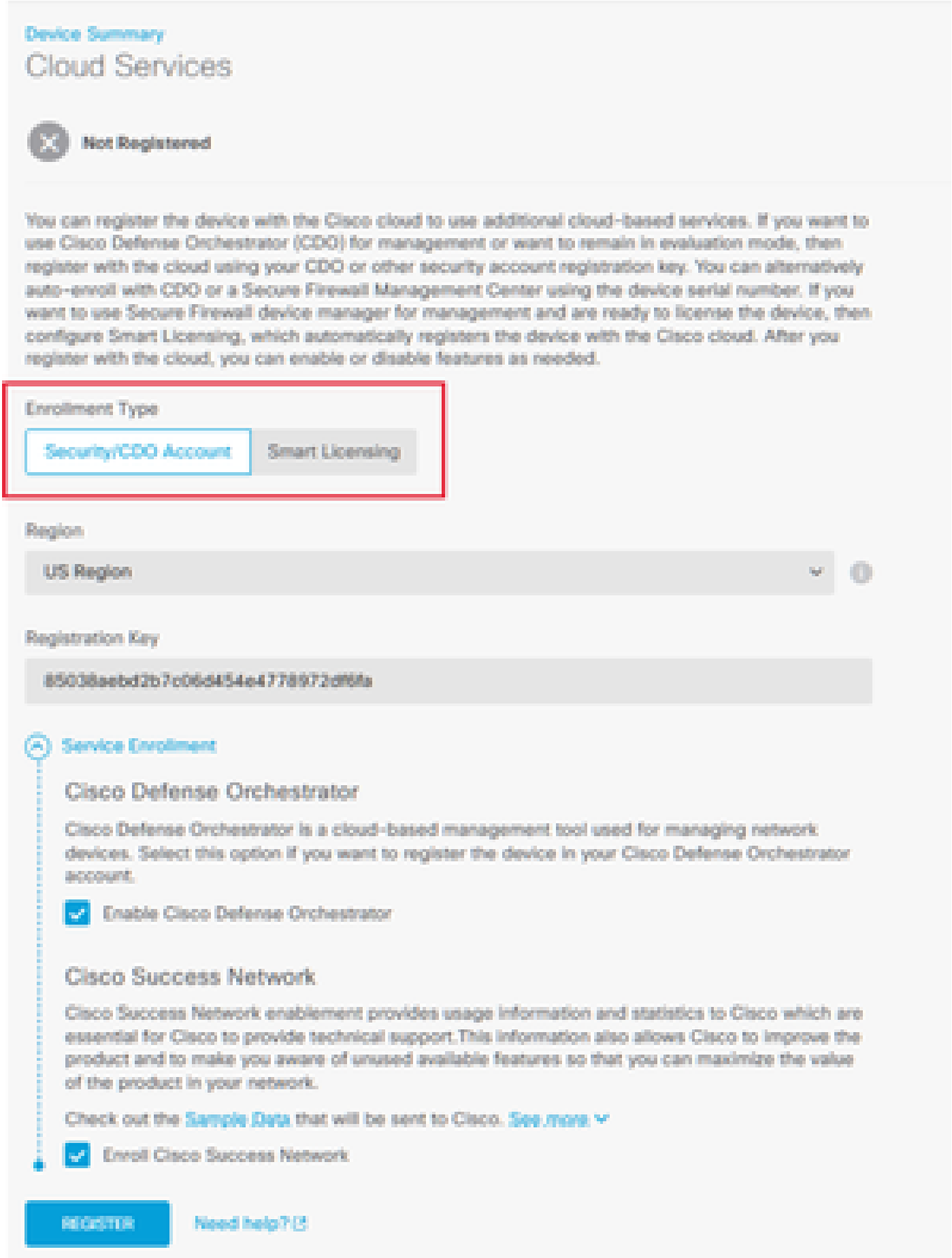


11단계. Region(지역) 드롭다운에서 테넌트 지리적 위치에 맞게 올바른 Cisco 클라우드 지역을 지정합니다.

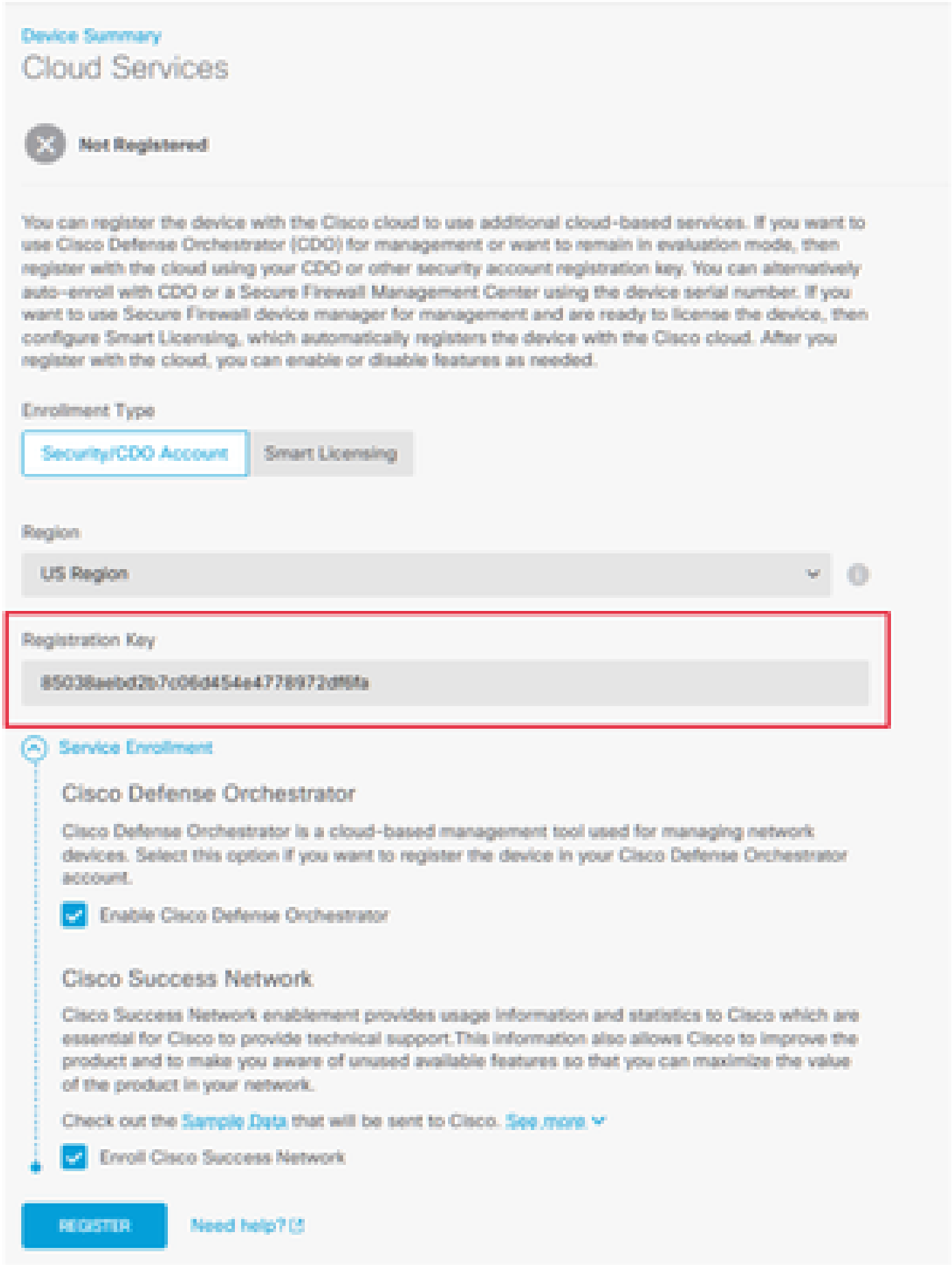
- defenseorchestrator.com에서 US를 선택합니다.
- defenseorchestrator.eu의 경우 EU를 선택합니다.
- apj.cdo.cisco.com에서 APJ를 선택합니다.



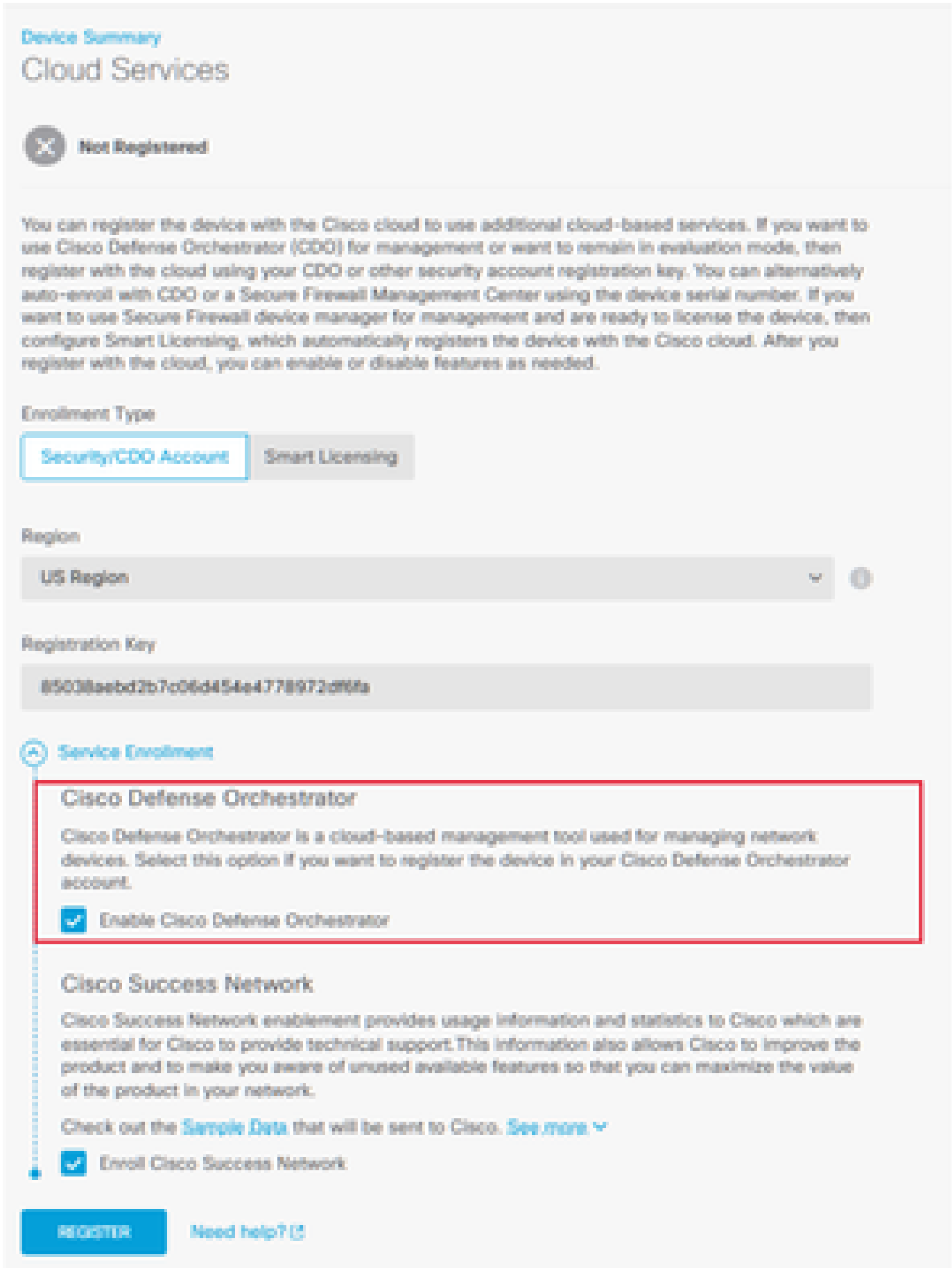
12단계. Enrollment Type(등록 유형) 섹션에서 Security Account(보안 계정)를 선택합니다.



13단계. 등록 키를 Registration Key(등록 키) 필드에 붙여넣습니다.

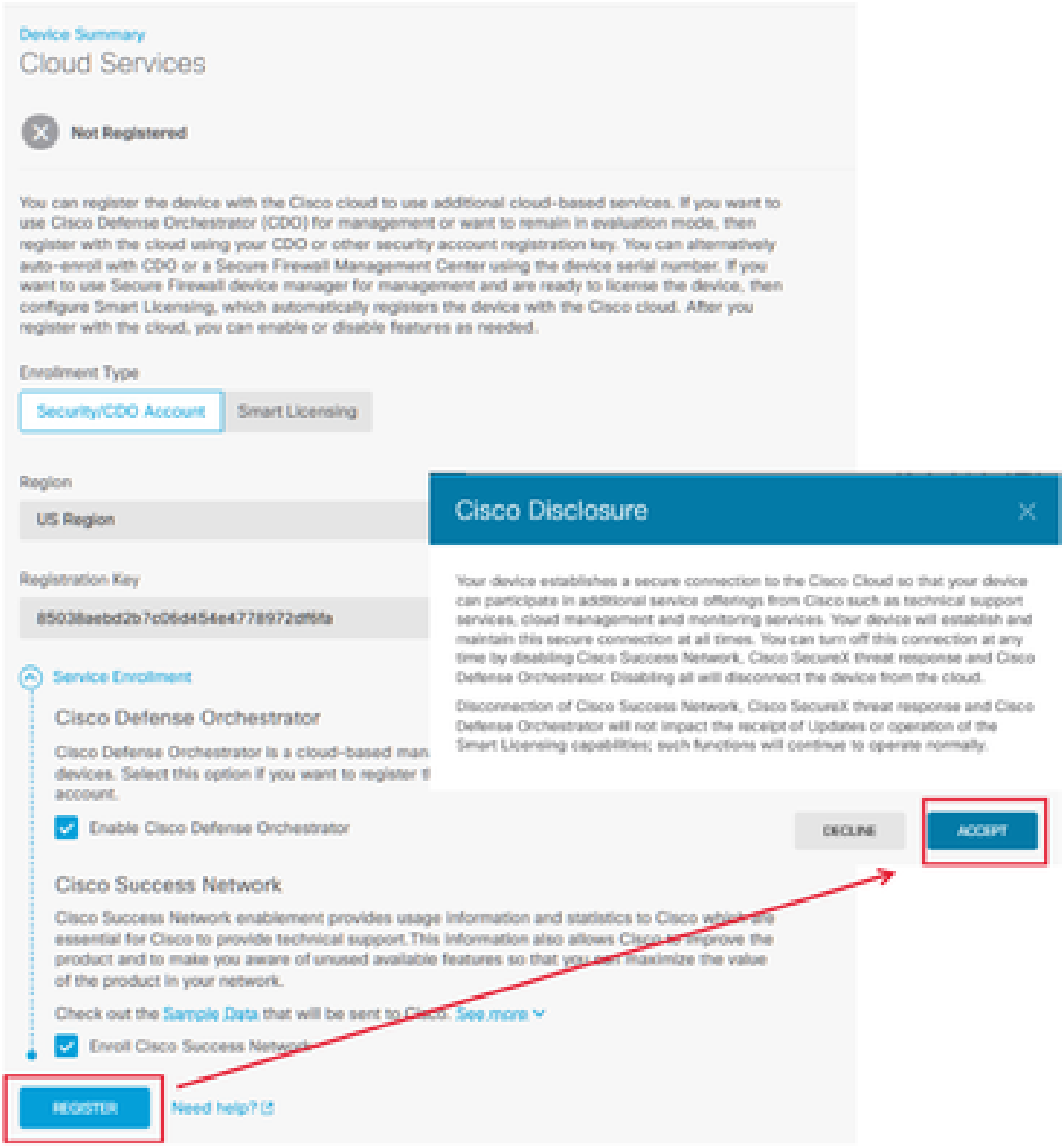


14단계. 버전 6.7 이상의 디바이스의 경우 Service Enrollment(서비스 등록) 섹션에서 Cisco Defense Orchestrator가 활성화되어 있는지 확인합니다.



15단계. (선택 사항) Cisco Success Network Enrollment 세부 사항을 검토합니다. 참여를 원하지 않으면 Enroll Cisco Success Network(Cisco 성공 네트워크 등록) 확인란의 선택을 취소합니다.

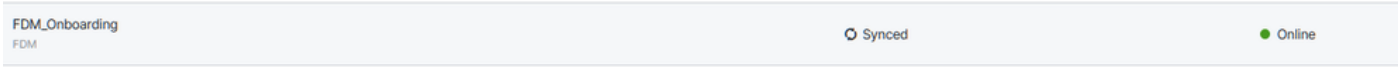
16단계. Register(등록)를 선택하고 Cisco Disclosure(Cisco 공개)에 동의합니다. Secure Firewall Device Manager가 CDO에 등록을 제출합니다.



17단계. CDO의 등록 키 생성 영역에서 Next(다음)를 선택합니다.

18단계. (선택 사항) 디바이스에 사용할 라이센스를 식별하고 선택한 다음 Next(다음)를 선택하여 진행합니다.

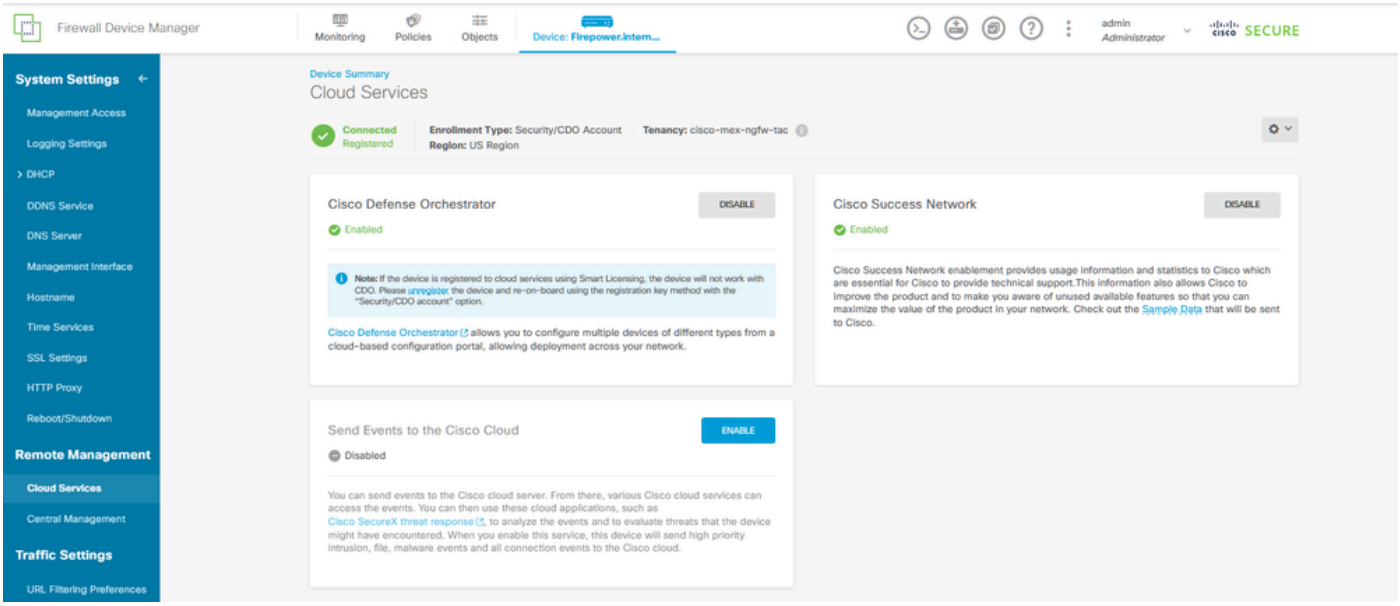
19단계. CDO 인벤토리의 디바이스 상태를 Unprovisioned(프로비저닝되지 않음)에서 Locating(찾기)으로 전환한 다음 Syncing(동기화)으로 전환하고, 마지막으로 Synced(동기화됨)로 전환합니다.



다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

CDO 포털로 이동하여 Online(온라인) 및 Synced(동기화됨)를 나타내는 디바이스 상태를 확인합니다. 또한 FDM GUI를 통해 상태 검증을 수행할 수 있습니다. System(시스템) > Cloud Services(클라우드 서비스)로 이동하여 Cisco Defense Orchestrator 및 Cisco Success Network의 연결 상태를 확인합니다. 인터페이스에 Connected(연결됨) 상태가 표시되어 서비스와의 성공적인 통합을 확인합니다.



문제 해결

이 섹션에서는 설정 문제 해결을 위해 사용할 수 있는 정보를 제공합니다.

- 클라우드 서비스 FQDN 오류 해결

클라우드 서비스 FQDN을 확인할 수 없어 디바이스 등록이 실패할 경우 네트워크 연결이나 DNS 컨피그레이션을 확인하고 디바이스 온보딩을 다시 시도합니다.

- 잘못된 등록 키 오류

방화벽 디바이스 관리자에 잘못된 등록 키가 입력되어 디바이스 등록이 완료되지 않은 경우, 계속해서 Cisco Defense Orchestrator에서 올바른 등록 키를 복사하고 등록 프로세스를 다시 시도하십시오. 디바이스가 이미 스마트 라이센스인 경우 방화벽 디바이스 관리자에서 등록 키를 입력하기 전에 스마트 라이센스를 제거하십시오.

- 라이센스 문제 부족

디바이스 연결 상태가 "Insufficient License(라이센스 부족)"인 경우 다음으로 진행합니다.

1. Cisco Smart Software Manager에서 디바이스에 새 라이센스를 적용하는 데 기간이 필요할 수 있으므로 디바이스에서 라이센스를 가져오는 데 어느 정도 시간이 걸립니다.

2. 디바이스 상태가 변경되지 않은 경우 로그아웃한 다음 다시 로그인하여 CDO 포털을 새로 고쳐 라이센스 서버와 디바이스 간의 잠재적인 네트워크 통신 문제를 해결하십시오.

3. 포털 새로고침이 디바이스 상태를 업데이트하지 않으면 다음 작업을 수행합니다.

    - Cisco Smart Software Manager에서 새 등록 키를 생성하고 복사합니다. 지침은 Generate Smart Licensing 비디오를 참조하십시오.
    - CDO 탐색 모음에서 Inventory(인벤토리) 페이지를 선택합니다.
    - Insufficient License(라이센스 부족) 상태가 표시된 디바이스를 선택합니다.
    - Device Details(디바이스 세부사항) 창의 Insufficient Licenses(라이센스 부족) 알림에서 Manage Licenses(라이센스 관리)를 클릭합니다. Manage Licenses(라이센스 관리) 창에 프롬프트가 표시됩니다.
    - Activate(활성화) 필드에서 새 등록 키를 붙여넣고 Register Device(디바이스 등록)를 선택합니다.

새 등록 키가 성공적으로 적용되면 장치 연결 상태가 'Online'으로 변경되어야 합니다.

대체 방법을 사용하여 등록 키에 Firepower 장치 관리자(FDM)를 등록하는 방법에 대한 자세한 내용은 다음 링크에서 제공하는 자세한 설명서를 참조하십시오. Troubleshoot FDM-Managed Devices

이 리소스는 FDM을 CDO(Cisco Defense Orchestrator)에 성공적으로 온보딩하는 데 사용할 수 있는 다양한 등록 기술에 대한 단계별 지침 및 문제 해결 팁을 제공합니다.

관련 정보

- FDM 관리 디바이스 문제 해결
- Cisco Defense Orchestrator로 FDM 디바이스 관리
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.