FTD에서 로컬 인증을 사용하여 SSL 보안 클라이언트 구성

목차

소개

이 문서에서는 Cisco FMC에서 관리하는 Cisco FTD에서 로컬 인증을 사용하여 Cisco Secure Client(Anyconnect 포함)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FMC(Firepower 관리 센터)를 통한 SSL 보안 클라이언트 구성
- FMC를 통한 firepower 개체 컨피그레이션
- firepower의 SSL 인증서

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco FTD(Firepower Threat Defense) 버전 7.0.0(빌드 94)
- Cisco FMC 버전 7.0.0(빌드 94)
- Cisco Secure Mobility Client 4.10.01075

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

이 예에서는 SSL(Secure Sockets Layer)을 사용하여 FTD와 Windows 10 클라이언트 간에 VPN(Virtual Private Network)을 생성합니다.

릴리스 7.0.0부터 FMC에서 관리하는 FTD는 Cisco Secure Client에 대한 로컬 인증을 지원합니다. 이는 기본 인증 방법으로 정의할 수도 있고 기본 방법이 실패할 경우 대비책으로 정의할 수도 있습니다. 이 예에서는 로컬 인증이 기본 인증으로 구성됩니다.

이 소프트웨어 버전 이전에는 FTD의 Cisco Secure Client 로컬 인증이 Cisco FDM(Firepower Device Manager)에서만 사용 가능했습니다.

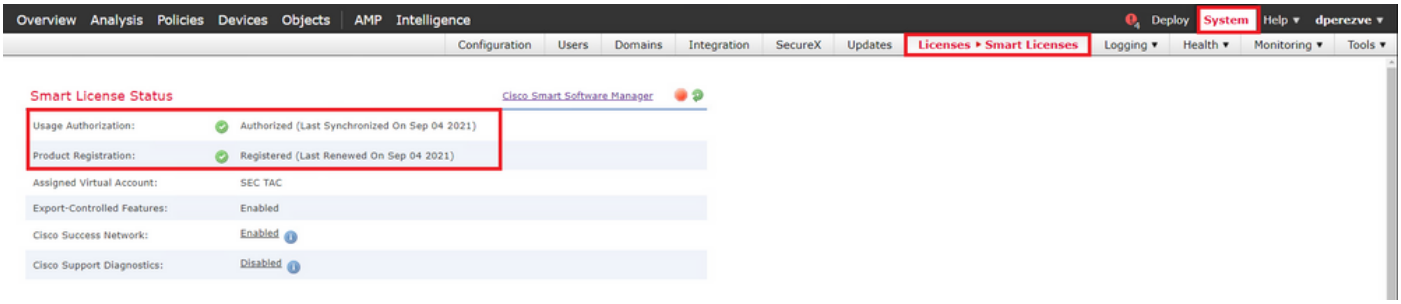
구성

설정

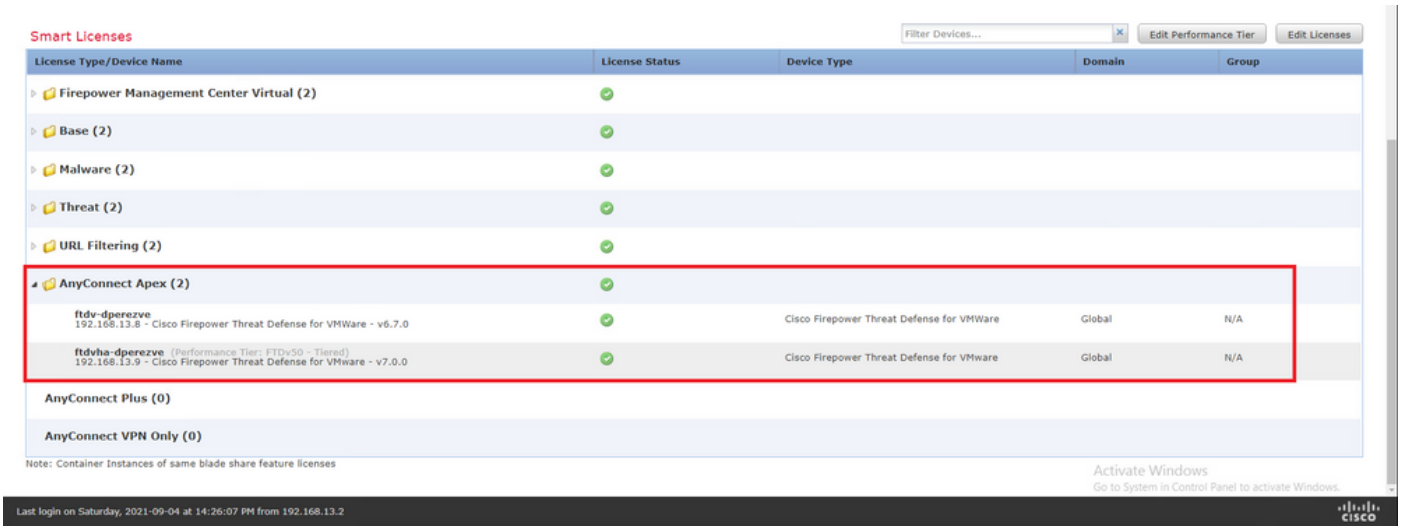
1단계. 라이센싱 확인

Cisco Secure Client를 구성하기 전에 FMC를 등록하고 Smart Licensing Portal을 준수해야 합니다. FTD에 유효한 Plus, Apex 또는 VPN Only 라이센스가 없는 경우 Cisco Secure Client를 구축할 수 없습니다.

FMC가 Smart Licensing Portal에 등록되고 규정을 준수하는지 확인하려면 System(시스템) > Licenses(라이센스) > Smart Licenses(스마트 라이센스)로 이동합니다.



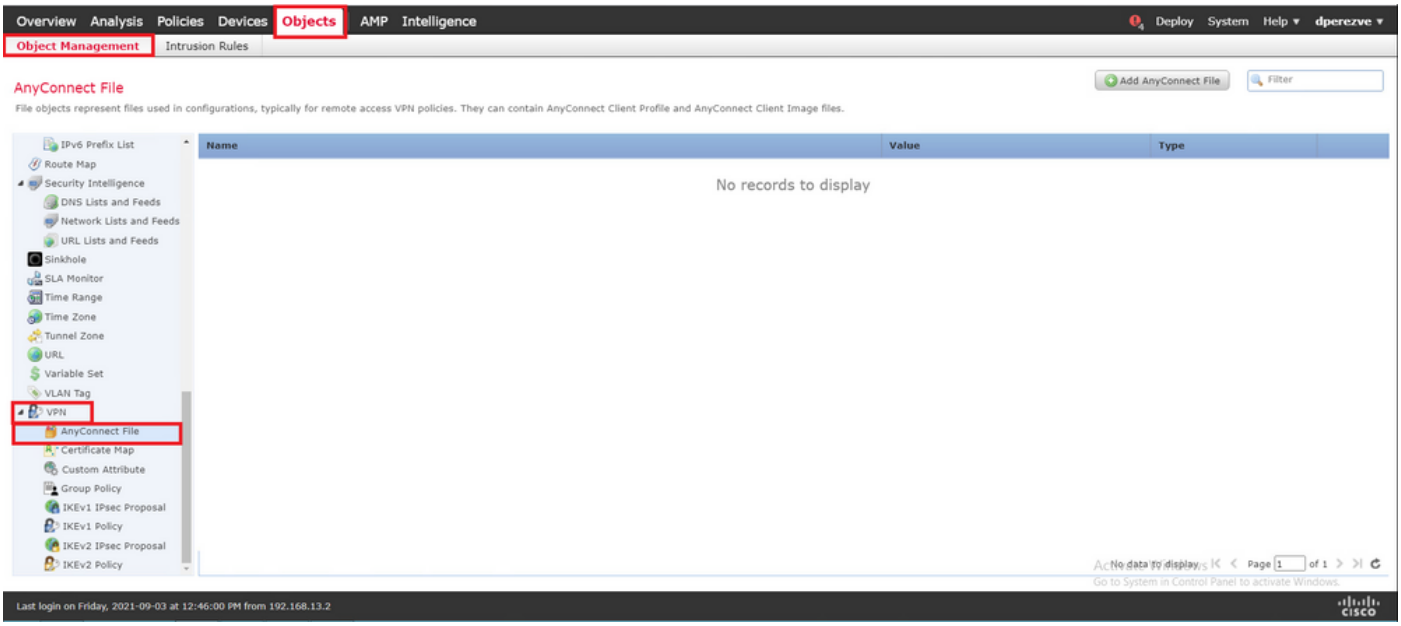
Smart Licenses(Smart 라이센스) 차트 하단의 같은 페이지에서 아래로 스크롤하면 사용 가능한 다양한 유형의 Cisco Secure Client(AnyConnect) 라이센스와 각 라이센스에 가입된 디바이스를 확인할 수 있습니다. 현재 FTD가 다음 범주 중 하나에 등록되어 있는지 확인합니다.



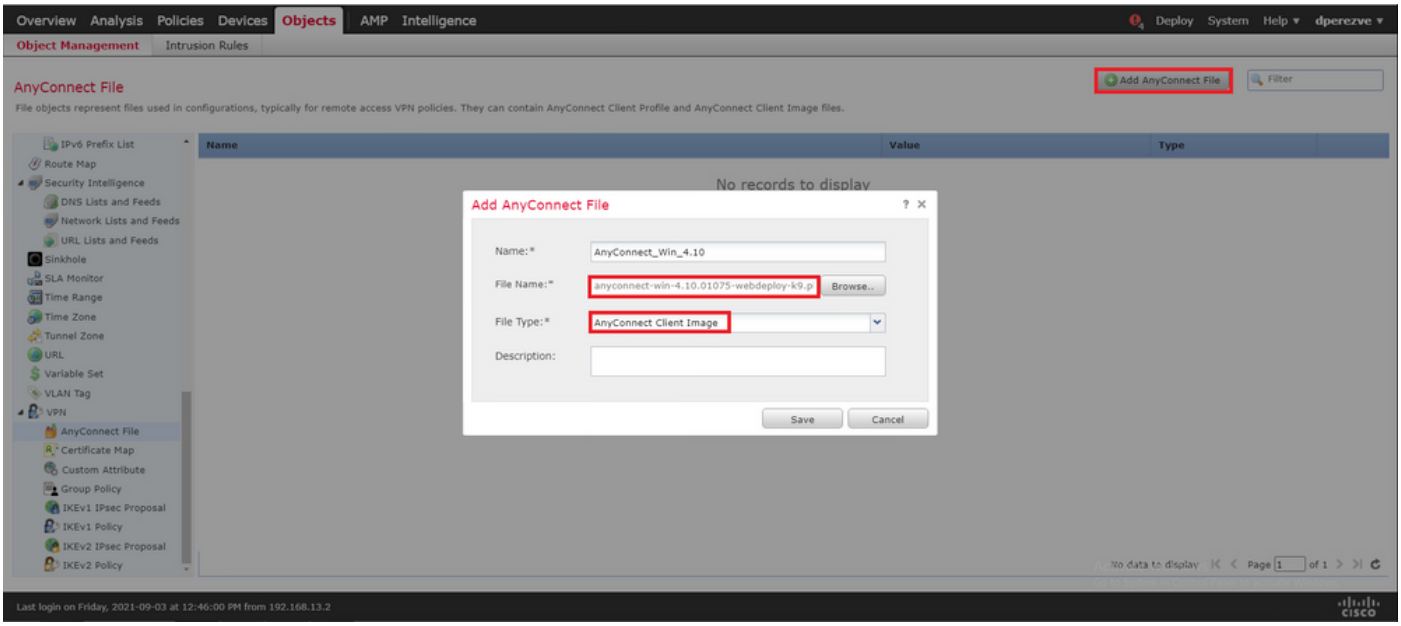
2단계. FMC에 Cisco Secure Client Package 업로드

cisco.com에서 Windows용 Cisco Secure Client(AnyConnect) Headend Deployment Package를 다운로드합니다.

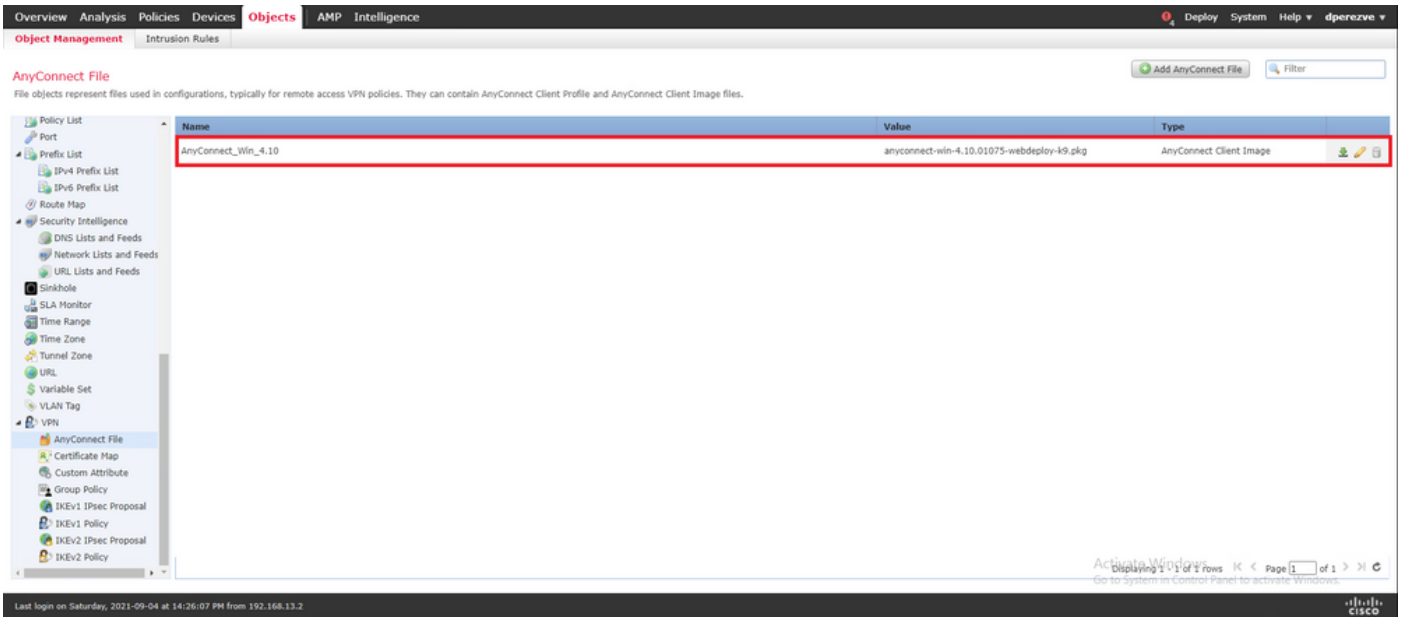
Cisco Secure Client 이미지를 업로드하려면 Objects(개체) > Object Management(개체 관리)로 이동하고 목차의 VPN 카테고리 아래에서 Cisco Secure Client File(Cisco Secure Client 파일)을 선택합니다.



Add AnyConnect File(AnyConnect 파일 추가) 버튼을 선택합니다. Add AnyConnect Secure Client File(AnyConnect 보안 클라이언트 파일 추가) 창에서 개체의 이름을 지정한 다음 Browse...(찾아보기...)를 선택하여 Cisco Secure Client 패키지를 선택한 다음 드롭다운 메뉴에서 파일 유형으로 AnyConnect Client Image(AnyConnect 클라이언트 이미지)를 선택합니다.



저장 버튼을 선택합니다. 객체를 객체 목록에 추가해야 합니다.



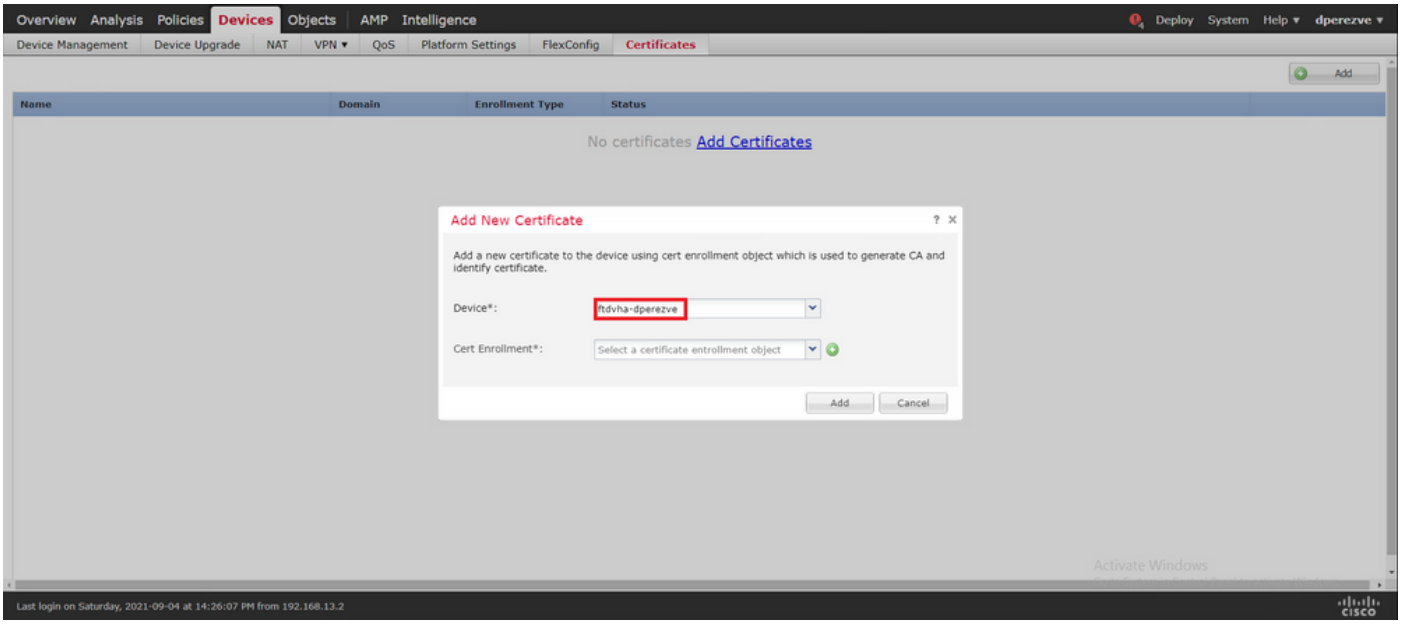
3단계. 자체 서명 인증서 생성

SSL Cisco Secure Client(AnyConnect)에는 VPN 헤드엔드와 클라이언트 간의 SSL 핸드셰이크에 사용할 유효한 인증서 하나가 필요합니다.

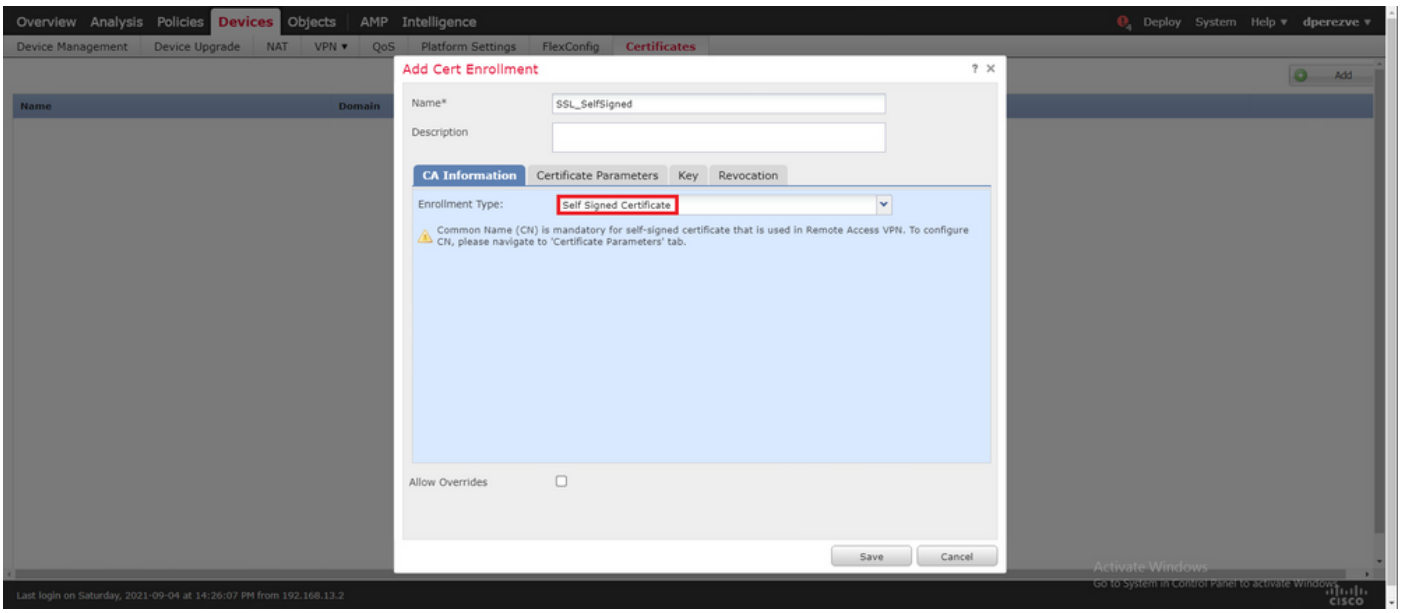
참고: 이 예에서는 이 용도로 자체 서명 인증서가 생성됩니다. 그러나 자체 서명 인증서 외에도 내부 CA(Certificate Authority)나 잘 알려진 CA가 서명한 인증서를 업로드할 수 있습니다.

자체 서명 인증서를 생성하려면 Devices(디바이스) > Certificates(인증서)로 이동합니다.

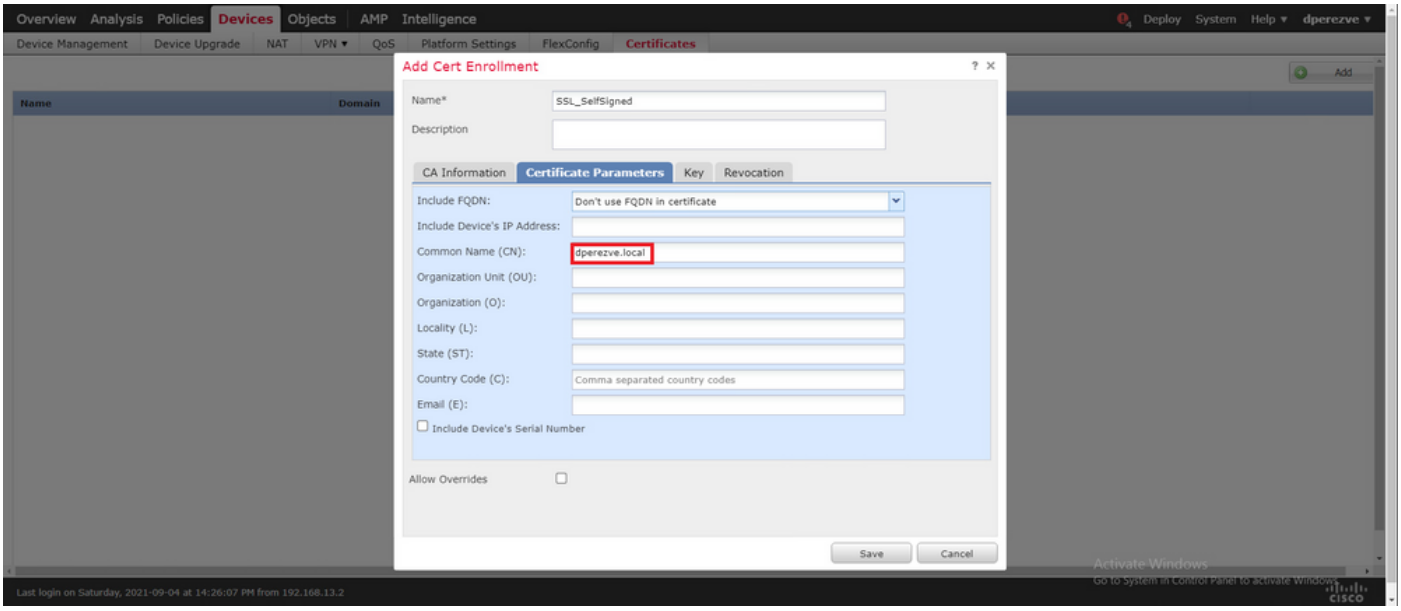
Add(추가) 버튼을 선택합니다. 그런 다음 Add New Certificate(새 인증서 추가) 창의 Device(디바이스) 드롭다운 메뉴에서 FTD를 선택합니다.



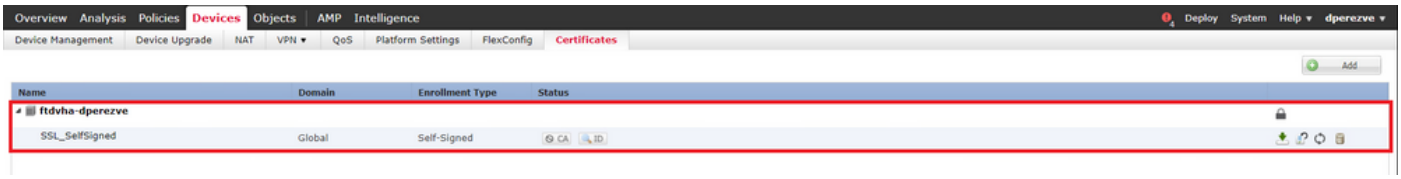
Add Cert Enrollment(인증서 등록 추가) 버튼(녹색 + 기호)을 선택하여 새 등록 객체를 생성합니다. 이제 Add Cert Enrollment(인증서 등록 추가) 창에서 객체의 이름을 지정하고 Enrollment Type(등록 유형) 드롭다운 메뉴에서 Self Signed Certificate(셀프 서명 인증서)를 선택합니다.



마지막으로, 자체 서명 인증서의 경우 CN(Common Name)을 반드시 포함해야 합니다. CN을 정의하려면 Certificate Parameters(인증서 매개변수) 탭으로 이동합니다.



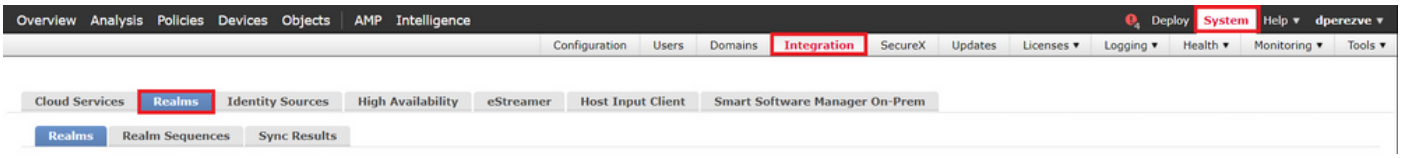
저장 및 추가 버튼을 선택합니다. 몇 초 후에 새 인증서를 인증서 목록에 추가해야 합니다.



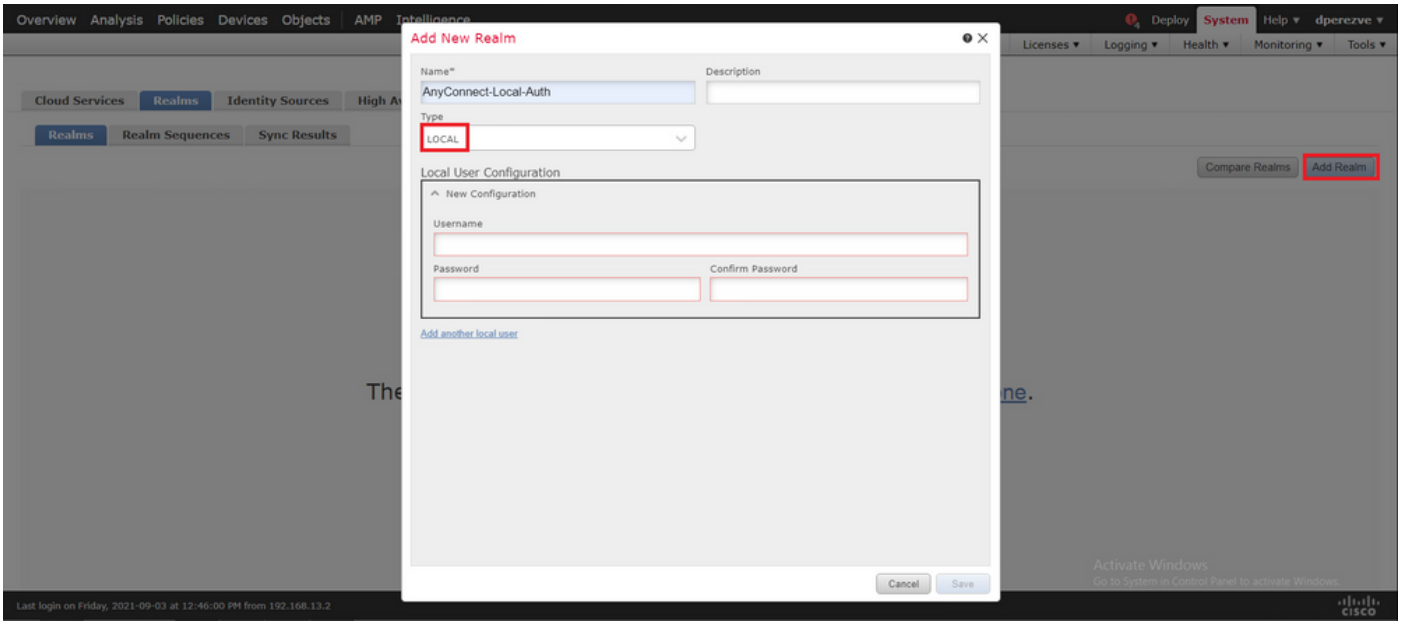
4단계. FMC에서 로컬 영역 생성

로컬 사용자 데이터베이스 및 각 비밀번호는 로컬 영역에 저장됩니다. 로컬 영역을 생성하려면

System > Integration > Realms로 이동합니다.

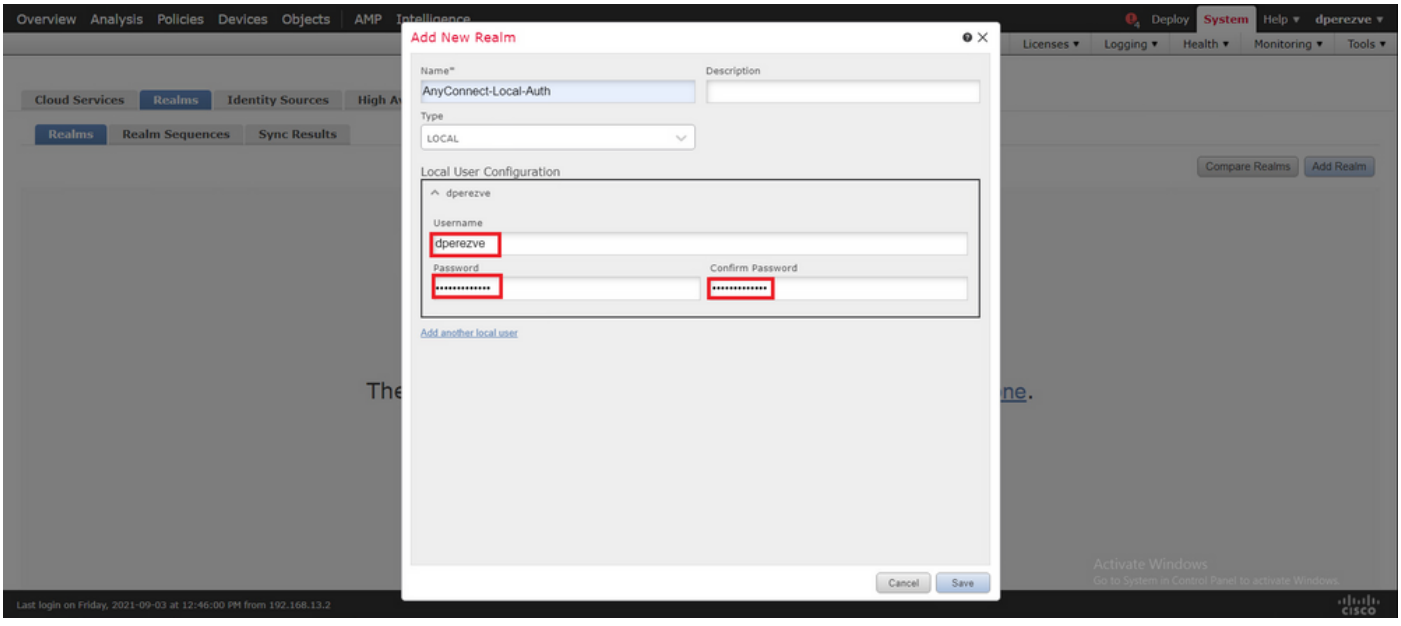


Add Realm(영역 추가) 버튼을 선택합니다. Add New Realm(새 영역 추가) 창에서 이름을 지정하고 Type(유형) 드롭다운 메뉴에서 LOCAL(로컬) 옵션을 선택합니다.

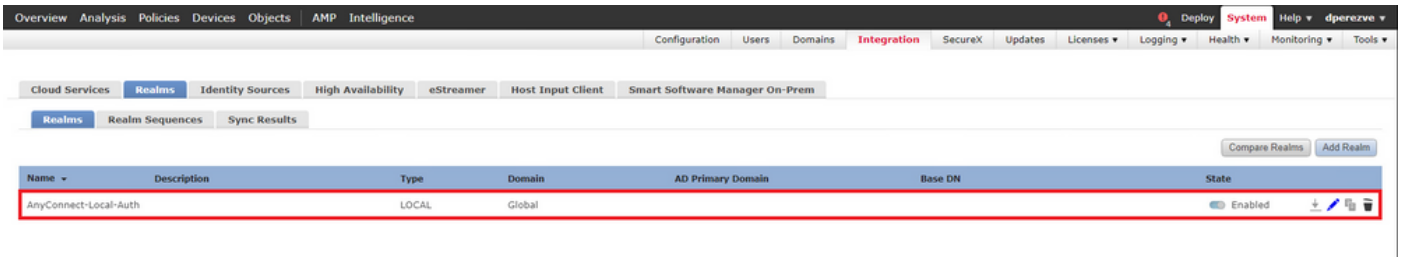


사용자 계정 및 비밀번호는 Local User Configuration(로컬 사용자 컨피그레이션) 섹션에서 생성됩니다.

참고: 비밀번호는 대문자, 소문자, 숫자 및 특수 문자를 각각 하나 이상 포함해야 합니다.

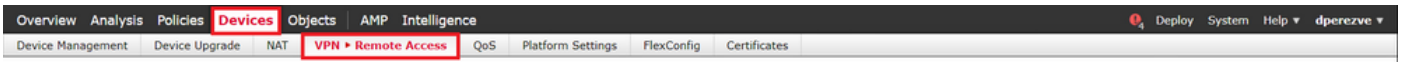


변경 사항을 저장하고 새 영역을 기존 영역 목록에 추가해야 합니다.

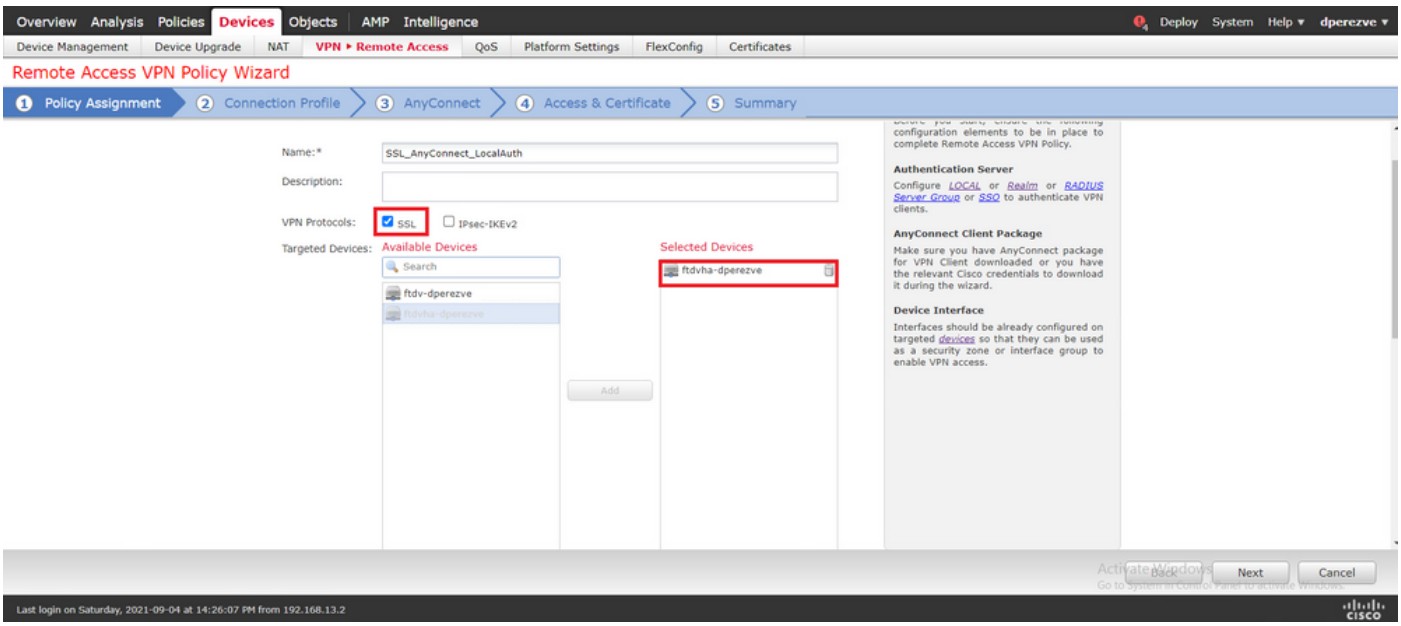


5단계. SSL Cisco Secure Client 구성

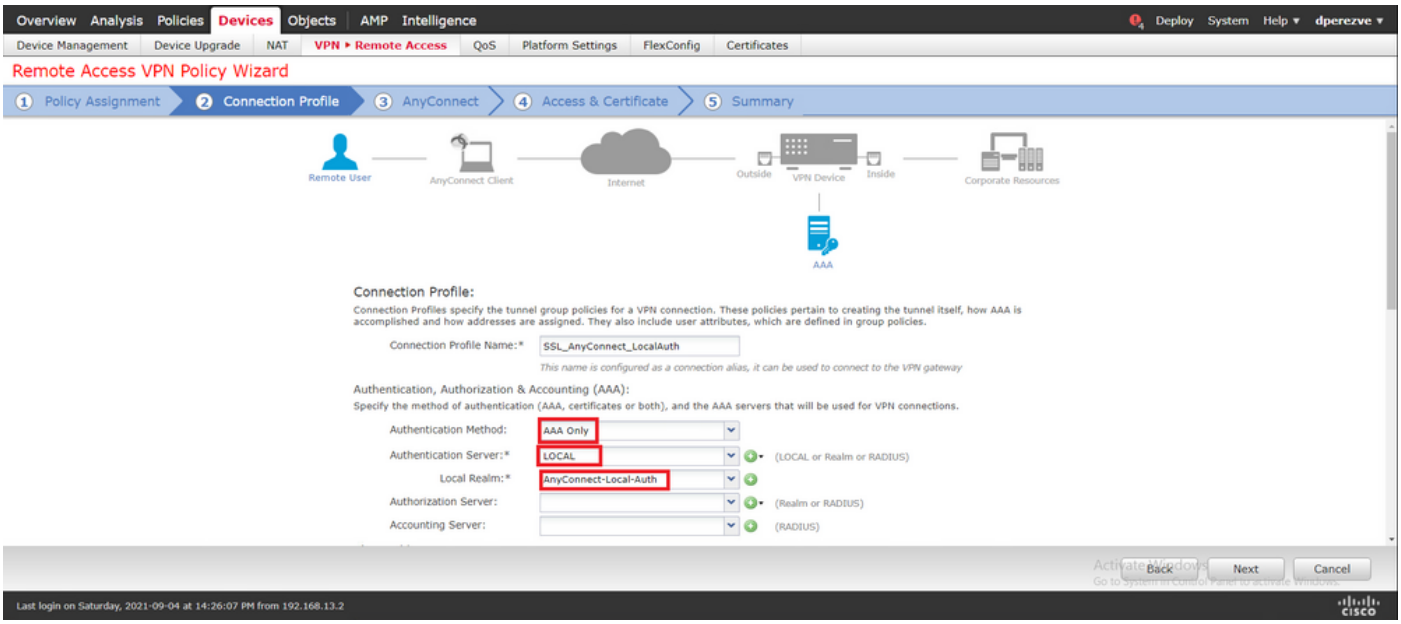
SSL Cisco Secure Client를 구성하려면 Devices(디바이스) > VPN > Remote Access(원격 액세스)로 이동합니다.



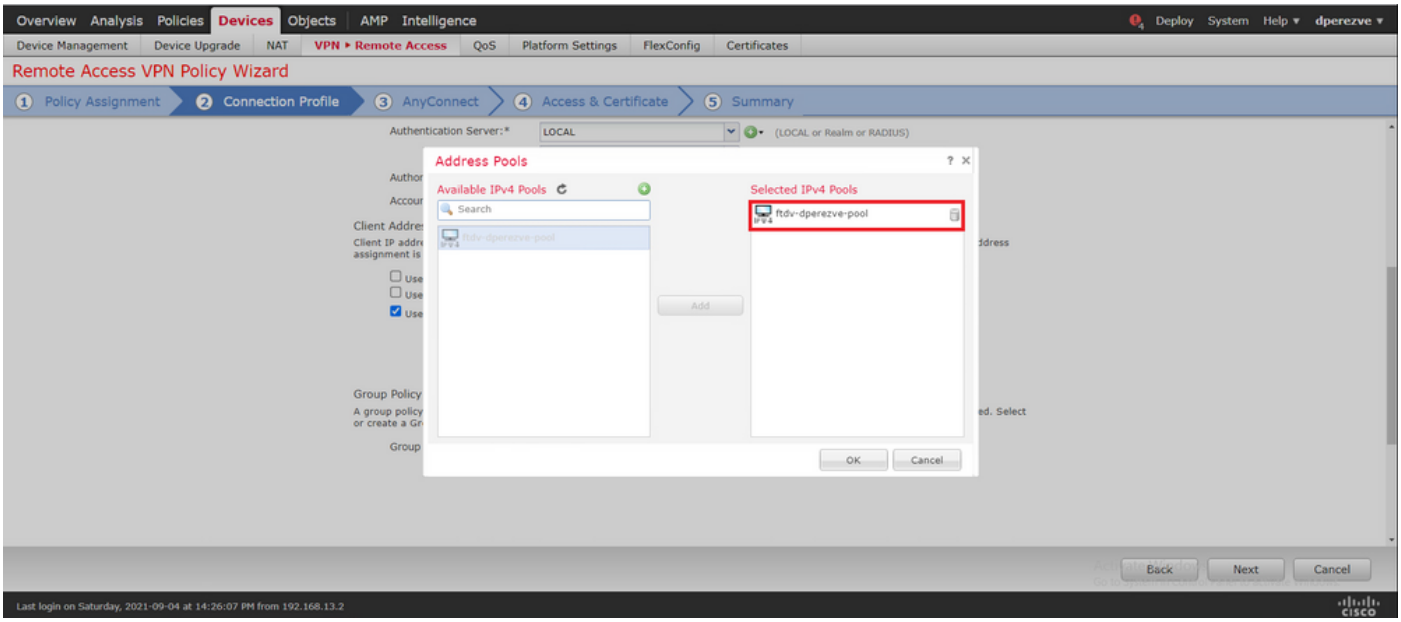
새 VPN 정책을 생성하려면 Add(추가) 버튼을 선택합니다. 연결 프로파일의 이름을 정의하고 SSL 확인란을 선택한 다음 대상 디바이스로 현재 FTD를 선택합니다. 원격 액세스 VPN 정책 마법사의 Policy Assignment(정책 할당) 섹션에서 모든 항목을 구성해야 합니다.



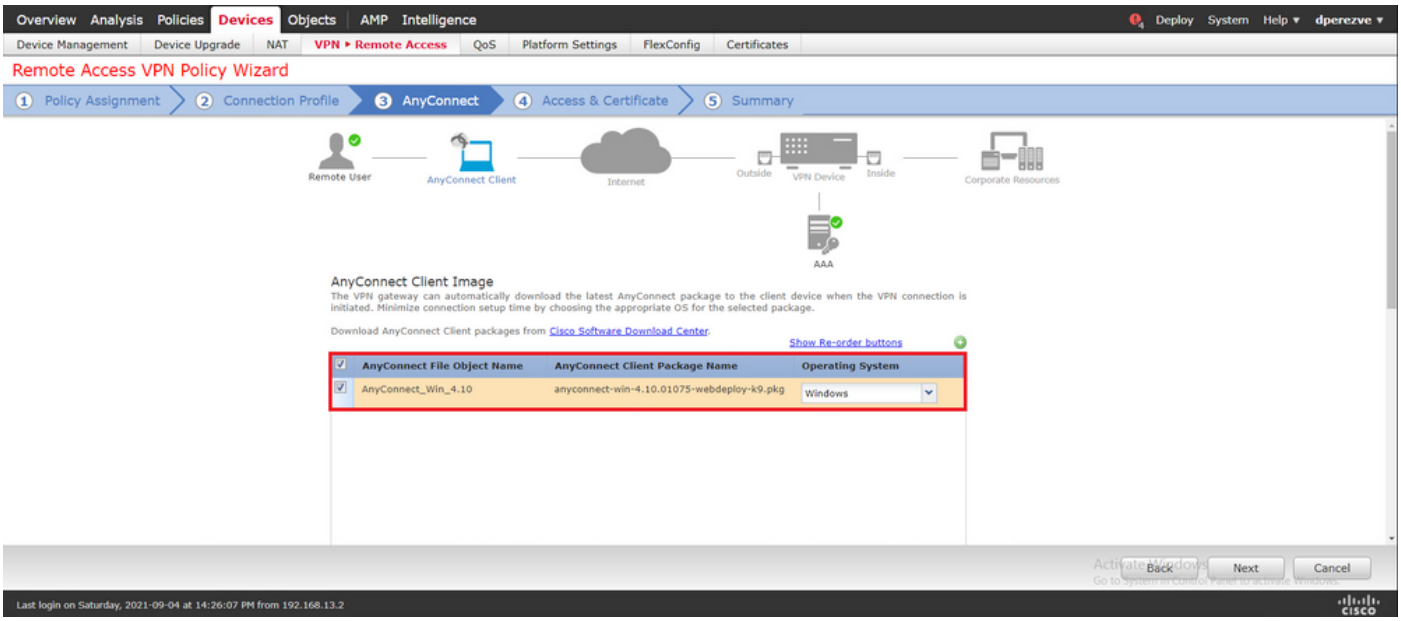
연결 프로파일 컨피그레이션으로 이동하려면 Next(다음)를 선택합니다. 연결 프로파일의 이름을 정의하고 인증 방법으로 AAA Only(AAA만)를 선택합니다. 그런 다음 Authentication Server 드롭다운 메뉴에서 LOCAL을 선택하고 마지막으로 Local Realm 드롭다운 메뉴의 4단계에서 생성한 로컬 영역을 선택합니다.



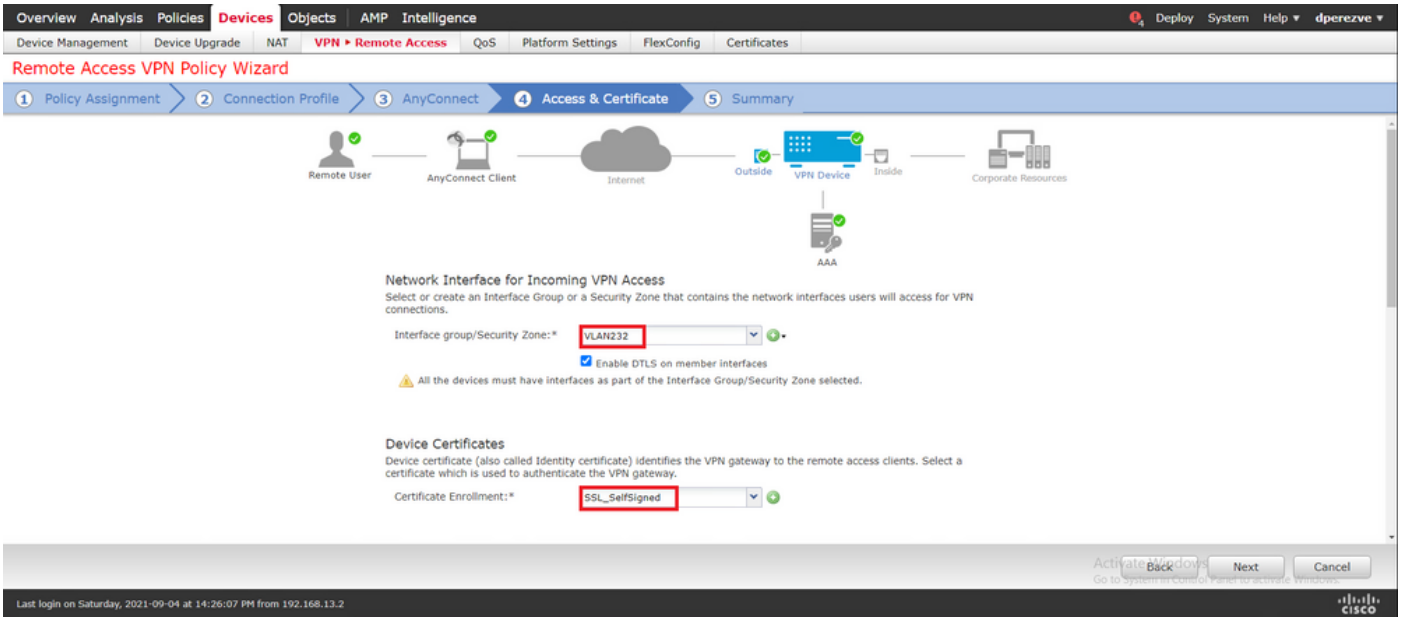
Cisco Secure Client에서 사용하는 IP 풀을 정의하기 위해 동일한 페이지에서 아래로 스크롤한 다음 IPv4 Address Pool(IPv4 주소 풀) 섹션에서 연필 아이콘을 선택합니다.



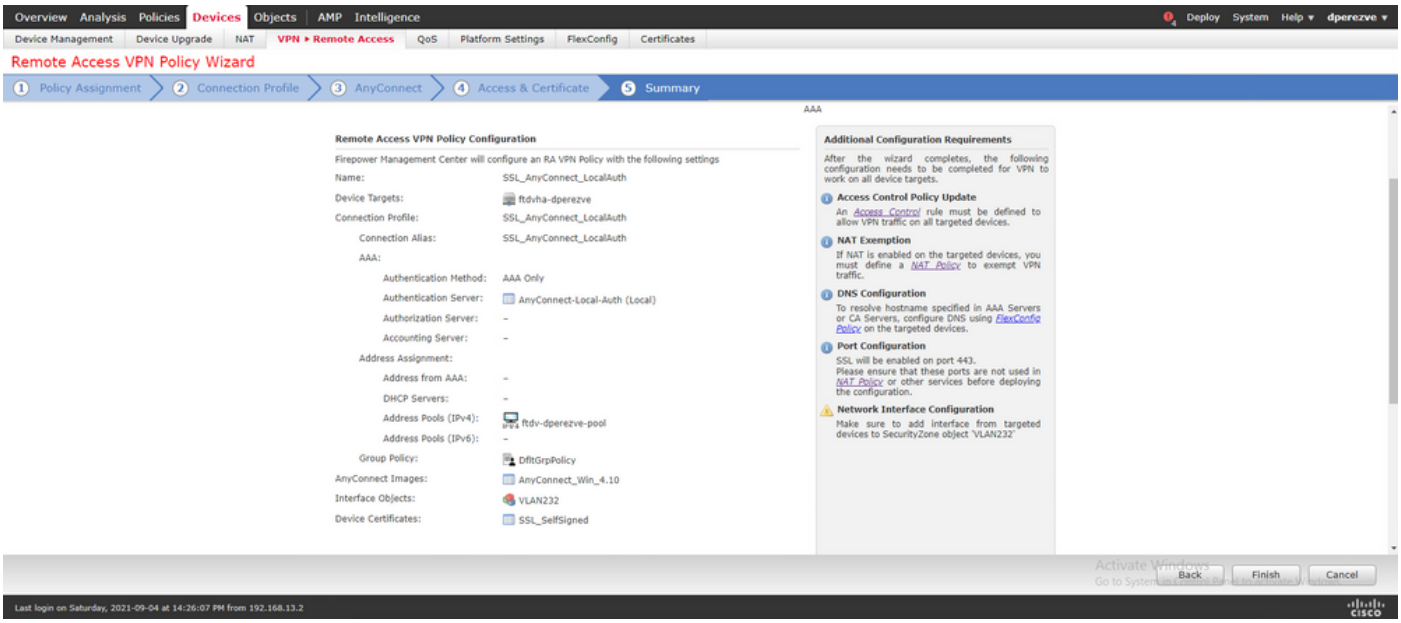
AnyConnect 섹션으로 이동하려면 Next(다음)를 선택합니다. 이제 2단계에서 업로드한 Cisco Secure Client 이미지를 선택합니다.



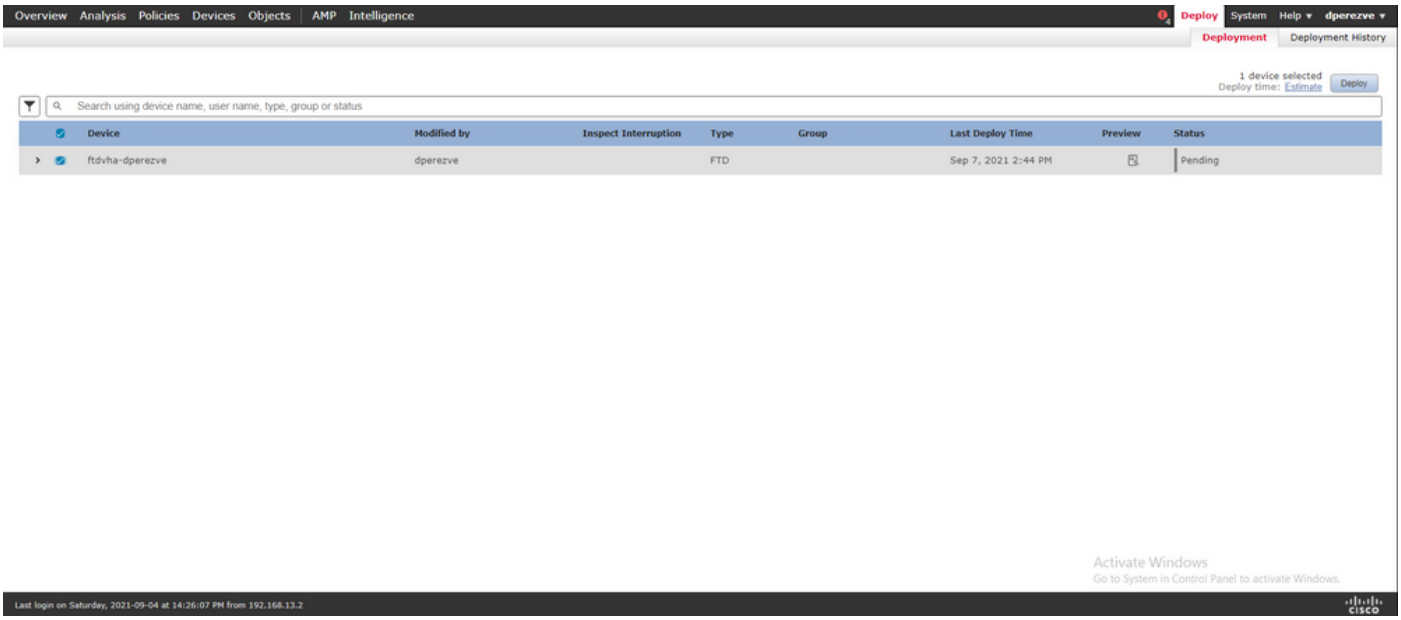
Access & Certificate(액세스 및 인증서) 섹션으로 이동하려면 Next(다음)를 선택합니다. Interface group/Security Zone 드롭다운 메뉴에서 Cisco Secure Client(AnyConnect)를 활성화해야 하는 인터페이스를 선택합니다. 그런 다음 Certificate Enrollment 드롭다운 메뉴에서 3단계에서 생성한 인증서를 선택합니다.



마지막으로, Cisco Secure Client 컨피그레이션의 요약을 보려면 Next(다음)를 선택합니다.

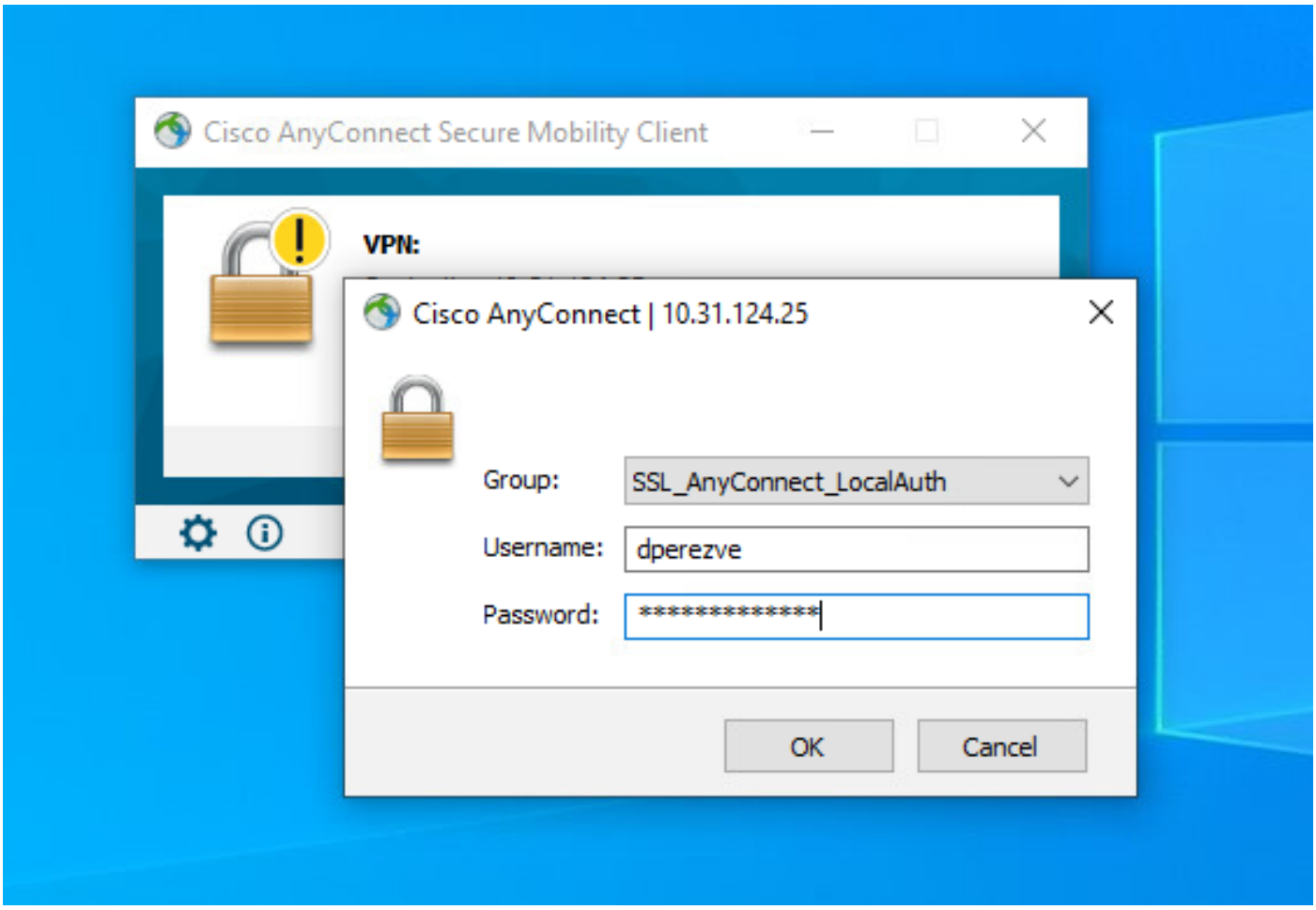


모든 설정이 올바르면 Finish(마침)를 선택하고 FTD에 변경 사항을 구축합니다.

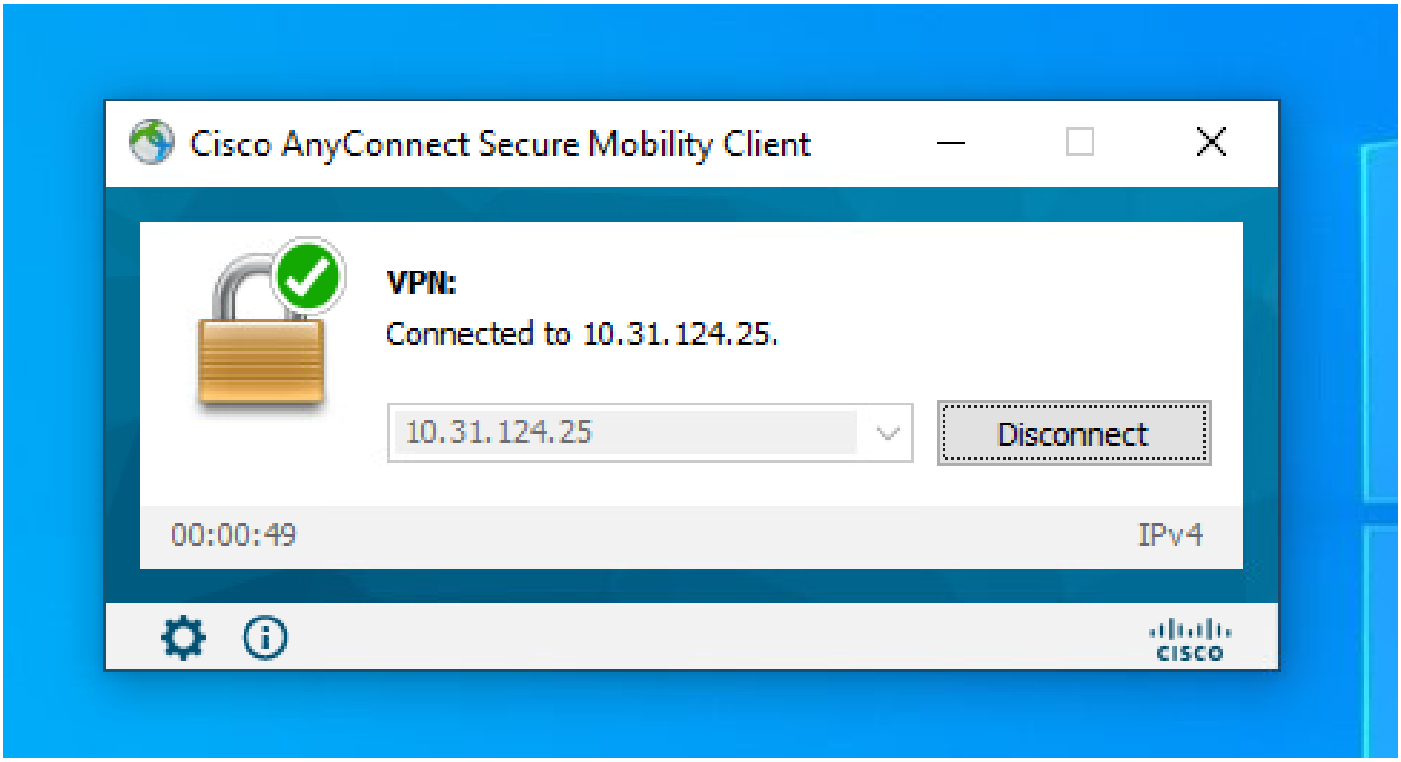


다음을 확인합니다.

구축에 성공하면 Windows 클라이언트에서 FTD로의 Cisco AnyConnect Secure Mobility Client 연결을 시작합니다. 인증 프롬프트에서 사용되는 사용자 이름 및 비밀번호는 4단계에서 생성한 것과 동일해야 합니다.



FTD에서 자격 증명을 승인하면 Cisco AnyConnect Secure Mobility Client 앱이 연결된 상태를 표시해야 합니다.



FTD에서 show vpn-sessiondb anyconnect 명령을 실행하여 현재 방화벽에서 활성 상태인 Cisco

Secure Client 세션을 표시할 수 있습니다.

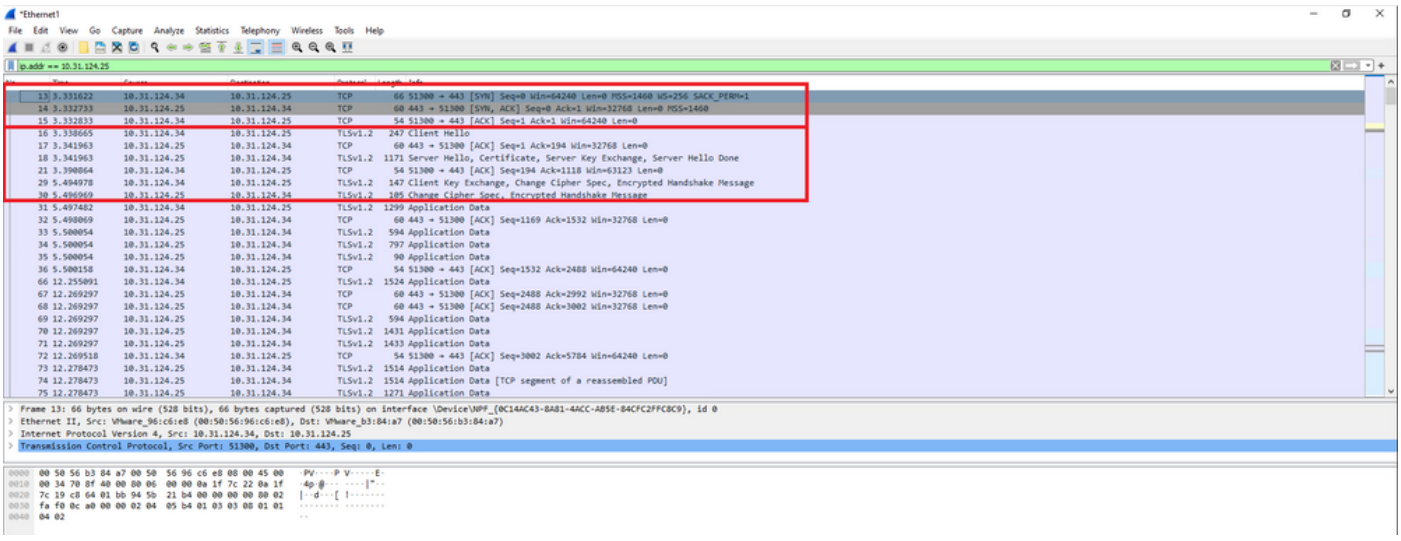
```
firepower# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : dperezve               Index        : 8
Assigned IP  : 172.16.13.1            Public IP    : 10.31.124.34
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA384
Bytes Tx     : 15756                  Bytes Rx     : 14606
Group Policy : DfltGrpPolicy
Tunnel Group : SSL_AnyConnect_LocalAuth
Login Time   : 21:42:33 UTC Tue Sep 7 2021
Duration     : 0h:00m:30s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0000000000000080006137dcc9
Security Grp : none                   Tunnel Zone  : 0
```

문제 해결

FTD에서 SSL 연결 흐름을 보려면 FTD에서 debug webvpn anyconnect 255 명령을 실행합니다.

```
firepower# debug webvpn anyconnect 255
```

Cisco Secure Client 디버깅 외에 TCP 패킷 캡처에서도 연결 흐름을 관찰할 수 있습니다. 성공적인 연결의 예로, Windows 클라이언트와 FTD 간의 정기적인 3회 핸드셰이크가 완료된 다음, 동의하는 암호에 사용되는 SSL 핸드셰이크가 나옵니다.



프로토콜 핸드셰이크 후 FTD는 로컬 영역에 저장된 정보로 자격 증명을 검증해야 합니다.

DART 번들을 수집하고 추가 조사를 위해 Cisco TAC에 문의하십시오.

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.