FTD에서 SSL AnyConnect 관리 VPN 구성

목차

소개

이 문서에서는 Cisco FMC(Firepower Management Center)에서 관리하는 Cisco FTD(Firepower Threat Defense)에서 Cisco AnyConnect 관리 터널을 구성하는 방법에 대해 설명합니다. 아래 예에서는 SSL(Secure Sockets Layer)을 사용하여 FTD와 Windows 10 클라이언트 간에 VPN(Virtual Private Network)을 생성합니다.

기고자: Daniel Perez Vertti Vazquez, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco AnyConnect 프로파일 편집기
- FMC를 통한 SSL AnyConnect 컨피그레이션입니다.
- 클라이언트 인증서 인증

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco FTD 버전 6.7.0(빌드 65)
- Cisco FMC 버전 6.7.0(빌드 65)
- Windows 10 시스템에 설치된 Cisco AnyConnect 4.9.01095

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

배경 정보

릴리스 6.7부터 Cisco FTD는 AnyConnect 관리 터널 구성을 지원합니다.이렇게 하면 이전에 연 개선 요청 CSCvs78215가 수정됩니다.

AnyConnect 관리 기능을 사용하면 엔드포인트의 시작이 완료된 직후 VPN 터널을 생성할 수 있습니다.시스템 전원이 켜지는 즉시 사용자가 AnyConnect 앱을 수동으로 시작할 필요가 없습니다. AnyConnect VPN 에이전트 서비스는 관리 VPN 기능을 탐지하고 AnyConnect 관리 VPN 프로파일의 서버 목록에 정의된 호스트 항목을 사용하여 AnyConnect 세션을 시작합니다.

제한 사항

- 클라이언트 인증서 인증만 지원됩니다.
- Windows 클라이언트에 대해서는 컴퓨터 인증서 저장소만 지원됩니다.
- Cisco Firepower Device Manager(FDM) CSCvx90058에서는 지원되지 않습니다.
- Linux 클라이언트에서 지원되지 않습니다.

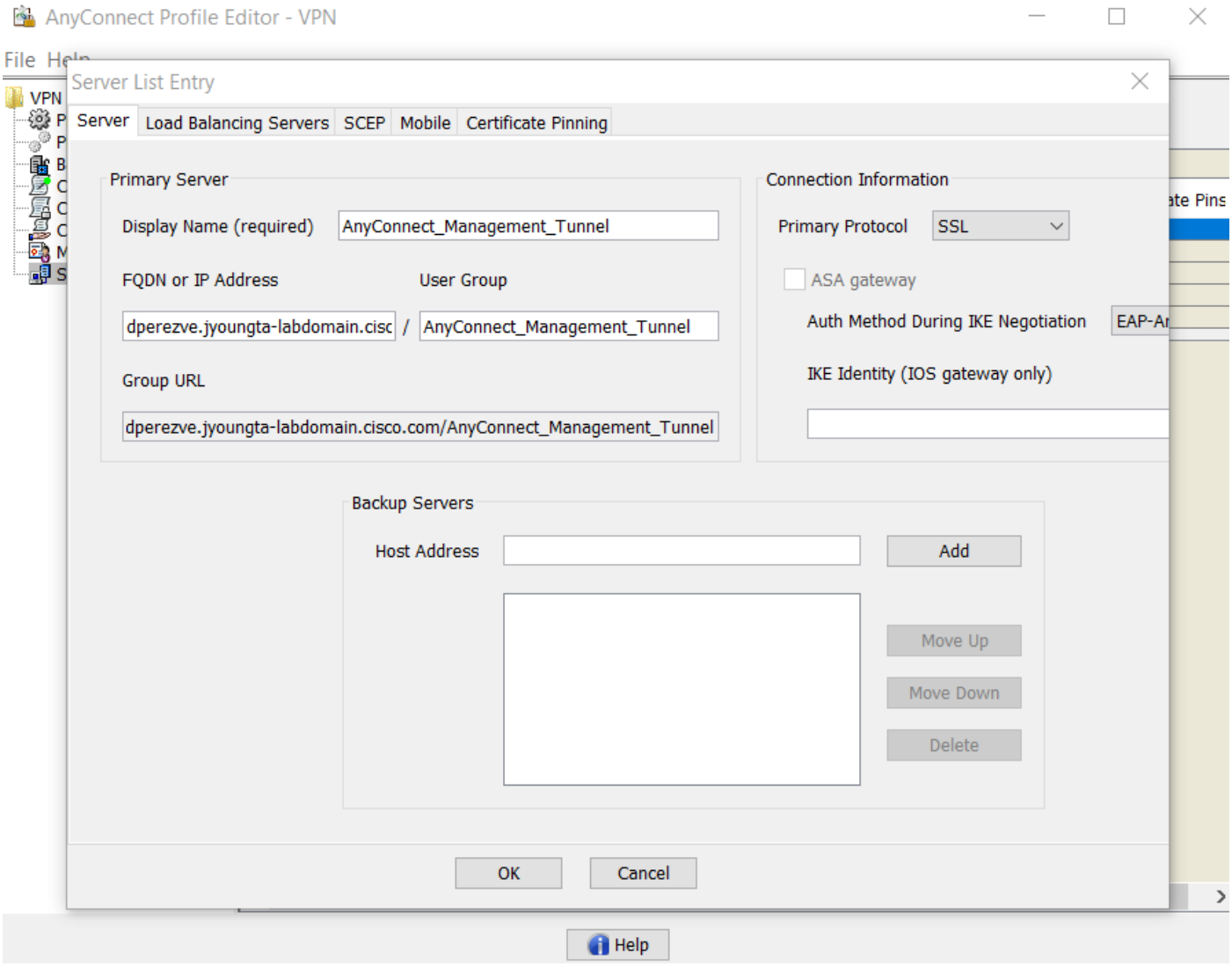
구성

구성

1단계. AnyConnect 관리 VPN 프로파일 생성

AnyConnect 프로파일 편집기를 열어 AnyConnect 관리 VPN 프로파일을 생성합니다.관리 프로파일은 엔드포인트가 부팅된 후 VPN 터널을 설정하는 데 사용되는 모든 설정을 포함합니다.

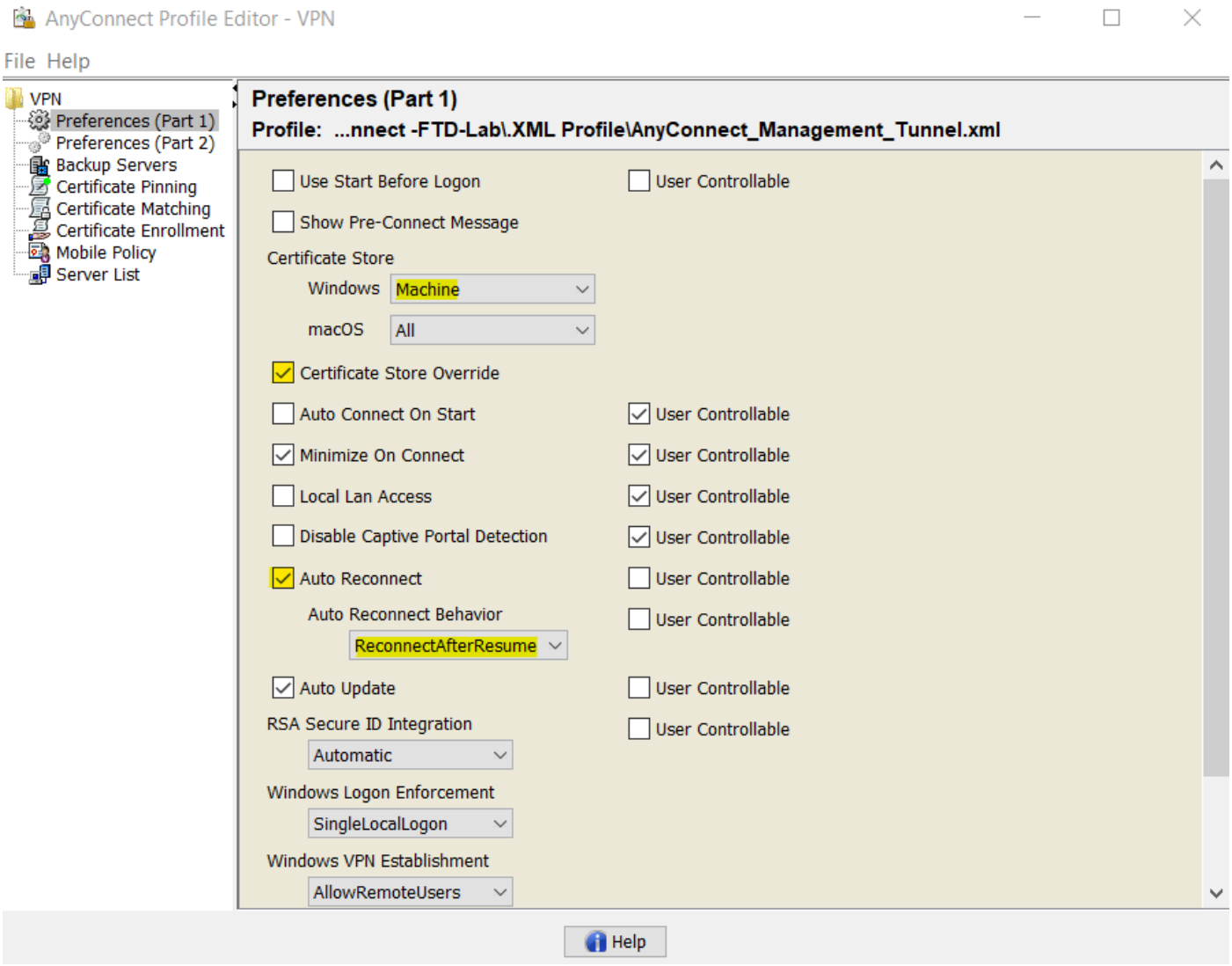
이 예에서는 FQDN(Fully Qualified Domain Name)을 가리키는 서버 목록 항목이 정의되어 있으며 SSL이 기본 프로토콜로 선택됩니다.Server List를 추가하려면 **Server List(서버 목록)로** 이동하고 **Add(추가)** 버튼을 선택하고 필수 필드를 채우고 변경 사항을 저장합니다.



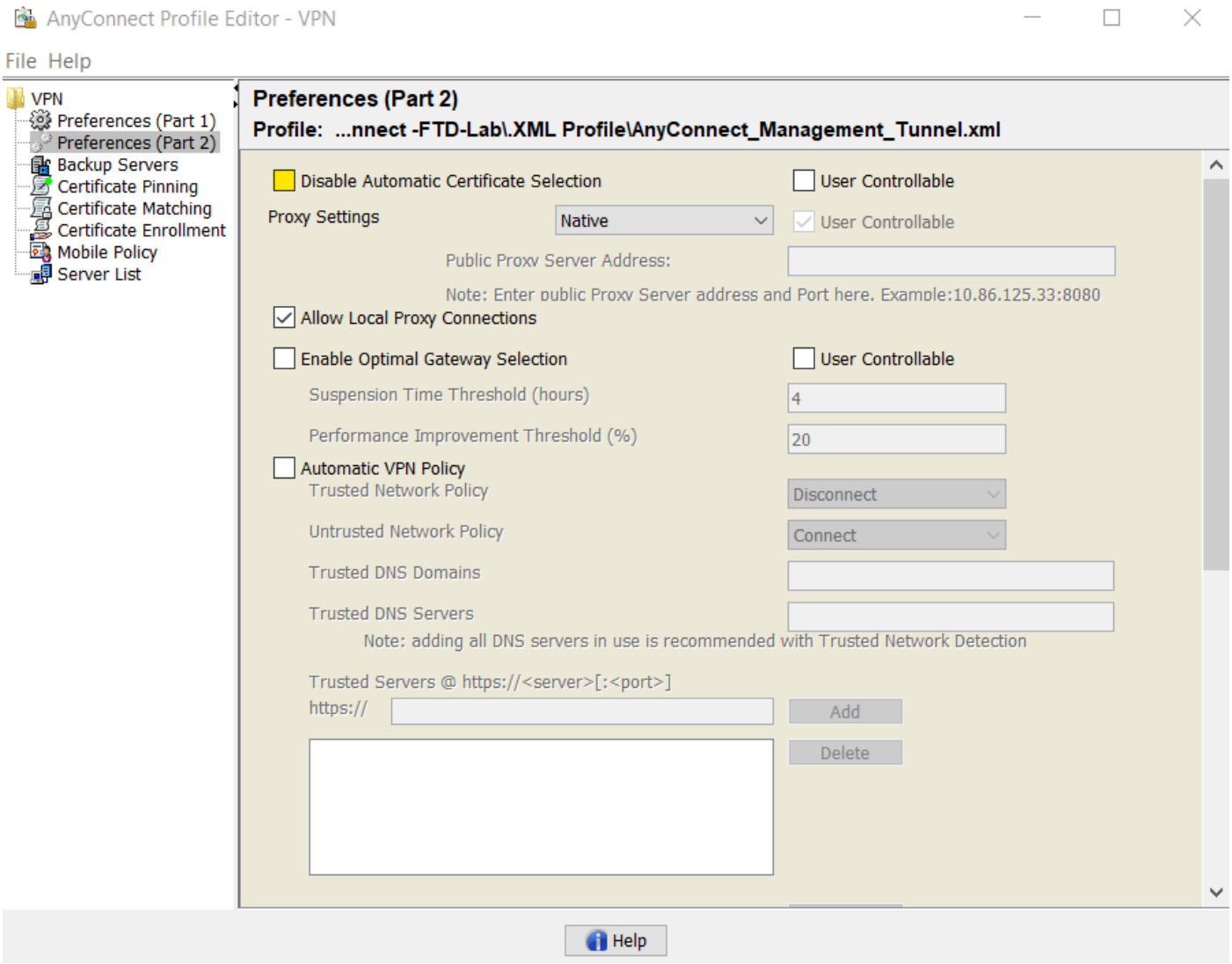
Server List(서버 목록) 외에 관리 VPN 프로필에는 몇 가지 필수 환경 설정이 포함되어야 합니다.

- **AutomaticCertSelection**을 **true**로 설정해야 합니다.
- **AutoReconnect**를 **true**로 설정해야 합니다.
- **ReconnectAfterResume**에 대해 AutoReconnectBehavior를 **구성해야 합니다**.
- **자동 업데이트**는 **false**로 설정해야 합니다.
- **BlockUntrustedServers**를 **true**로 설정해야 합니다.
- **CertificateStore**는 MachineStore에 대해 구성해야 **합니다**.
- **CertificateStoreOverride**를 **true**로 설정해야 합니다.
- **EnableAutomaticServerSelection**을 false로 설정해야 **합니다**.
- **EnableScripting**을 false로 설정해야 **합니다**.
- **RetainVPNOnLogoff**는 **true**로 설정해야 합니다.

AnyConnect 프로파일 편집기에서 기본 설정**(1부)으로 이동하고** 다음과 같이 설정을 조정합니다.



그런 다음 Preferences(**Part 2)로** 이동하고 Disable **Automatic Certificate Selection(자동 인증서 선택 비활성화**) 옵션을 선택 취소합니다.



2단계. AnyConnect VPN 프로파일 생성

관리 VPN 프로필에 추가하여 일반 AnyConnect VPN 프로파일을 구성해야 합니다.AnyConnect VPN 프로파일은 첫 번째 연결 시도에서 사용되며, 이 세션 동안 관리 VPN 프로파일이 FTD에서 다운로드됩니다.

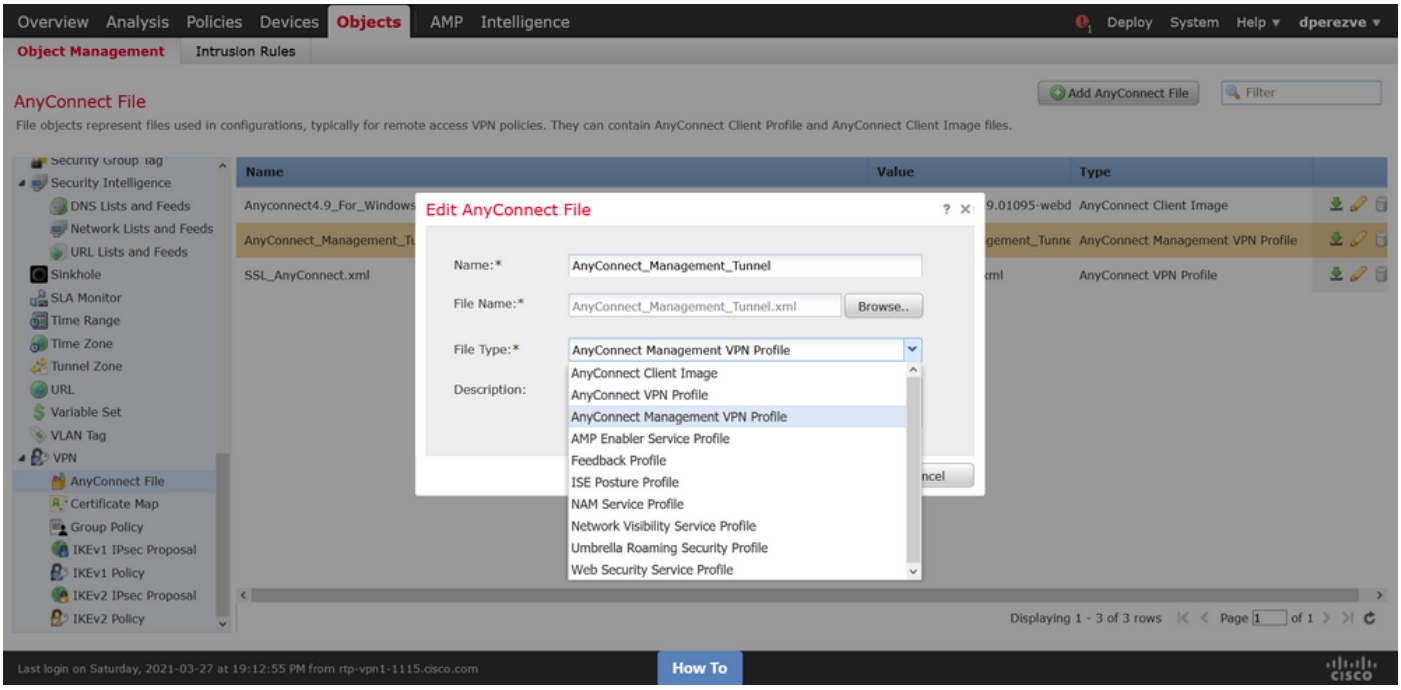
AnyConnect 프로파일 편집기를 사용하여 AnyConnect VPN 프로파일을 생성합니다.이 경우 두 파일에 동일한 설정이 포함되어 있으므로 동일한 절차를 수행할 수 있습니다.

3단계. AnyConnect 관리 VPN 프로파일 및 AnyConnect VPN 프로파일을 FMC에 업로드

프로파일이 생성되면 다음 단계는 FMC에 AnyConnect 파일 객체로 업로드합니다.

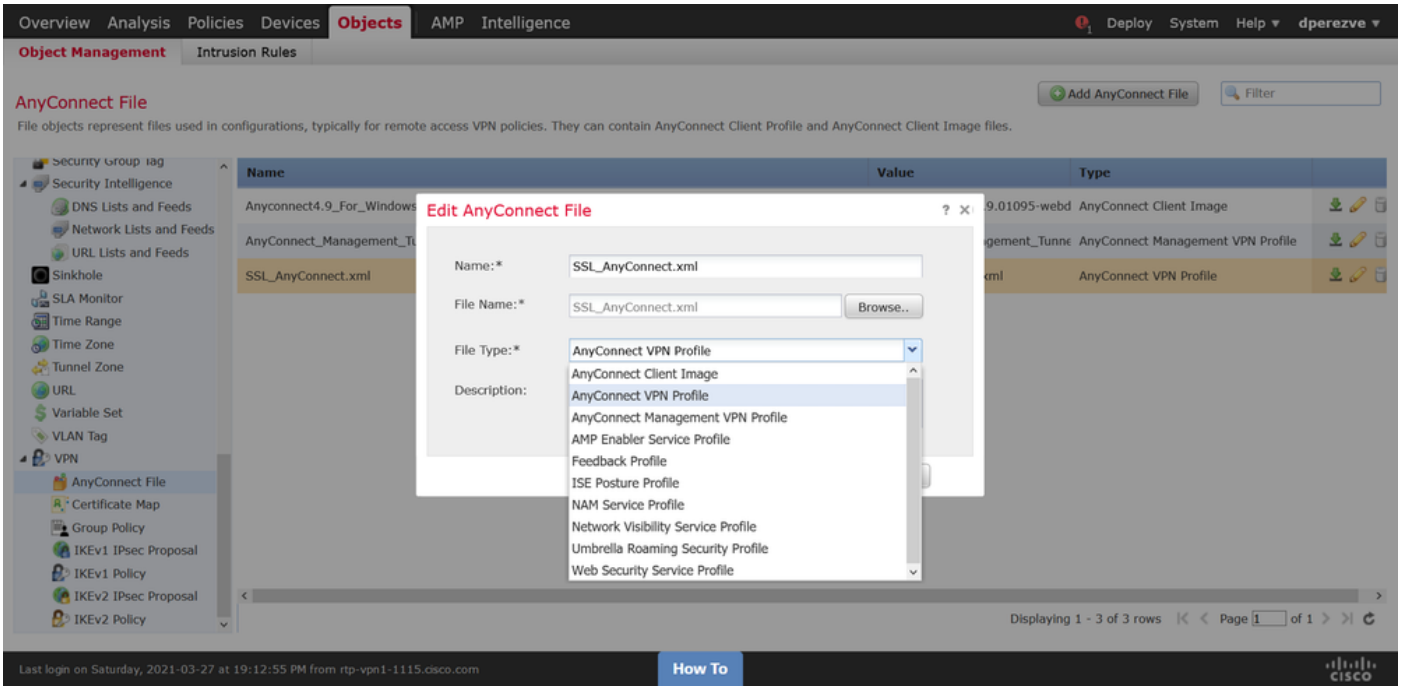
새 AnyConnect 관리 VPN 프로파일을 FMC에 업로드하려면 **Objects(개체) > Object Management(개체 관리)로 이동하고** 목차에서 **VPN** 옵션을 선택한 다음 Add AnyConnect File(AnyConnect 파일 추가) 버튼을 선택합니다.

파일 이름을 제공하고 파일 유형으로 **AnyConnect Management VPN Profile**을 선택하고 개체를 저장합니다.

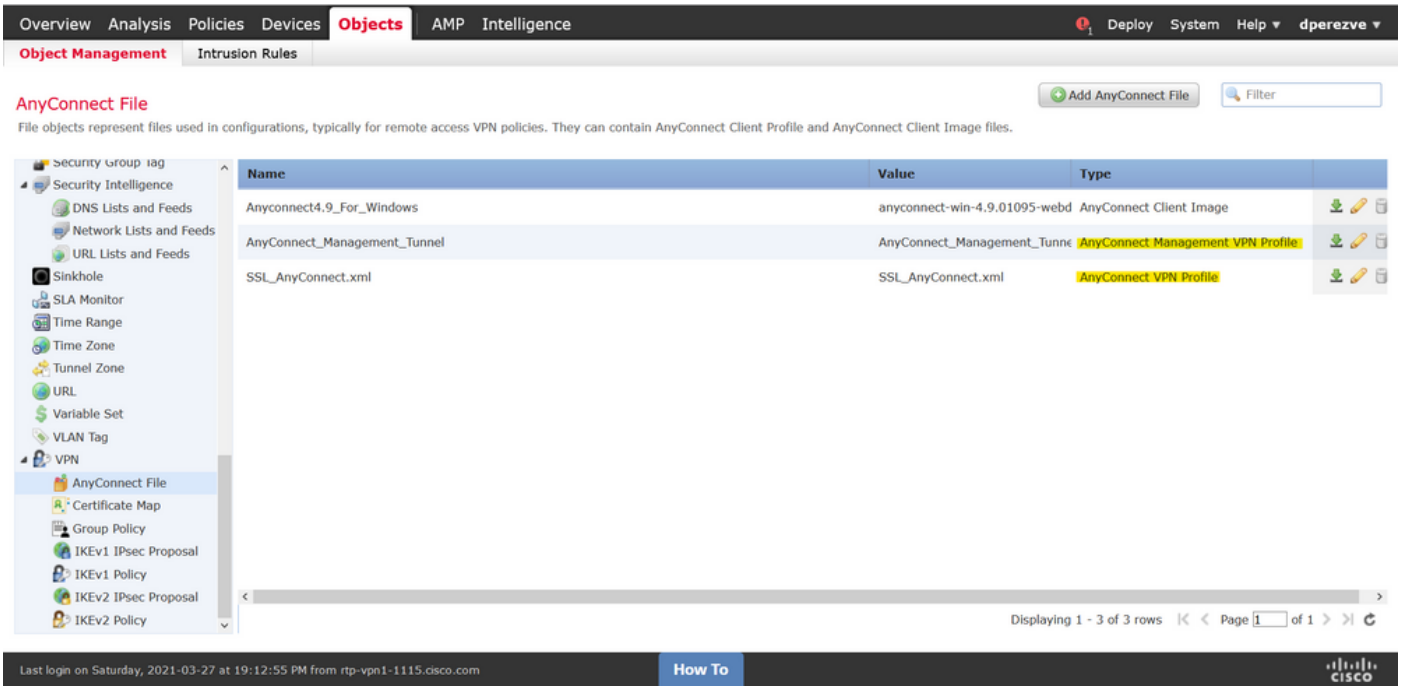


이제 AnyConnect VPN 프로파일을 업로드하려면 다시 Objects(**개체) > Object Management(개체 관리)로** 이동하고 목차**에서 VPN** 옵션을 선택한 다음 Add AnyConnect File(AnyConnect 파일 추가) 버튼을 선택합니다.

파일 이름을 제공하지만 이번에는 AnyConnect **VPN Profile을** 파일 유형으로 선택하고 새 개체를 저장합니다.



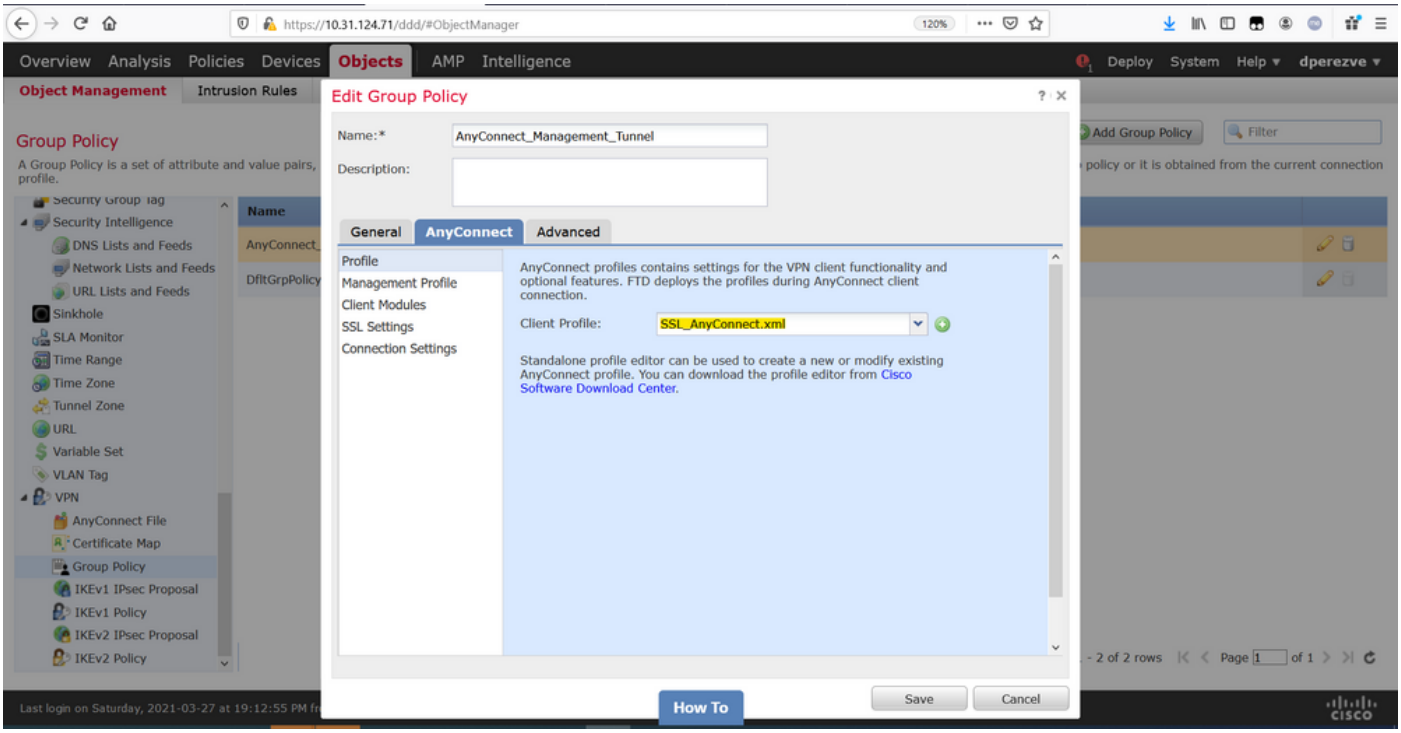
프로필을 개체 목록에 추가하고 AnyConnect **관리 VPN 프로파일** 및 AnyConnect **VPN 프로필로** 각각 표시해야 합니다.



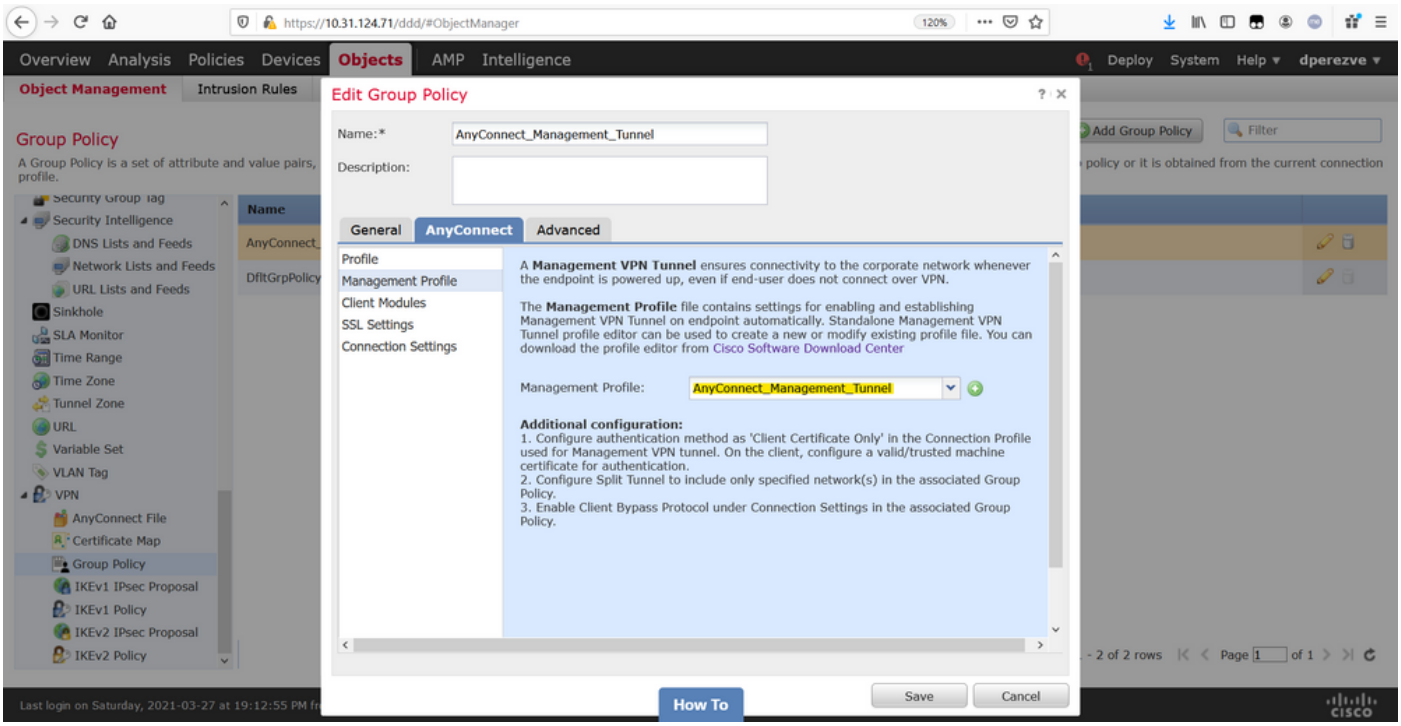
4단계. 그룹 정책 생성

새 그룹 정책을 생성하려면 Objects(**개체**) > **Object Management(개체 관리)로** 이동하고 목차에서 **VPN** 옵션을 선택한 다음 Group Policy(그룹 정책)를 선택하고 **Add Group Policy(그룹 정책 추가)** 버튼을 클릭합니다.

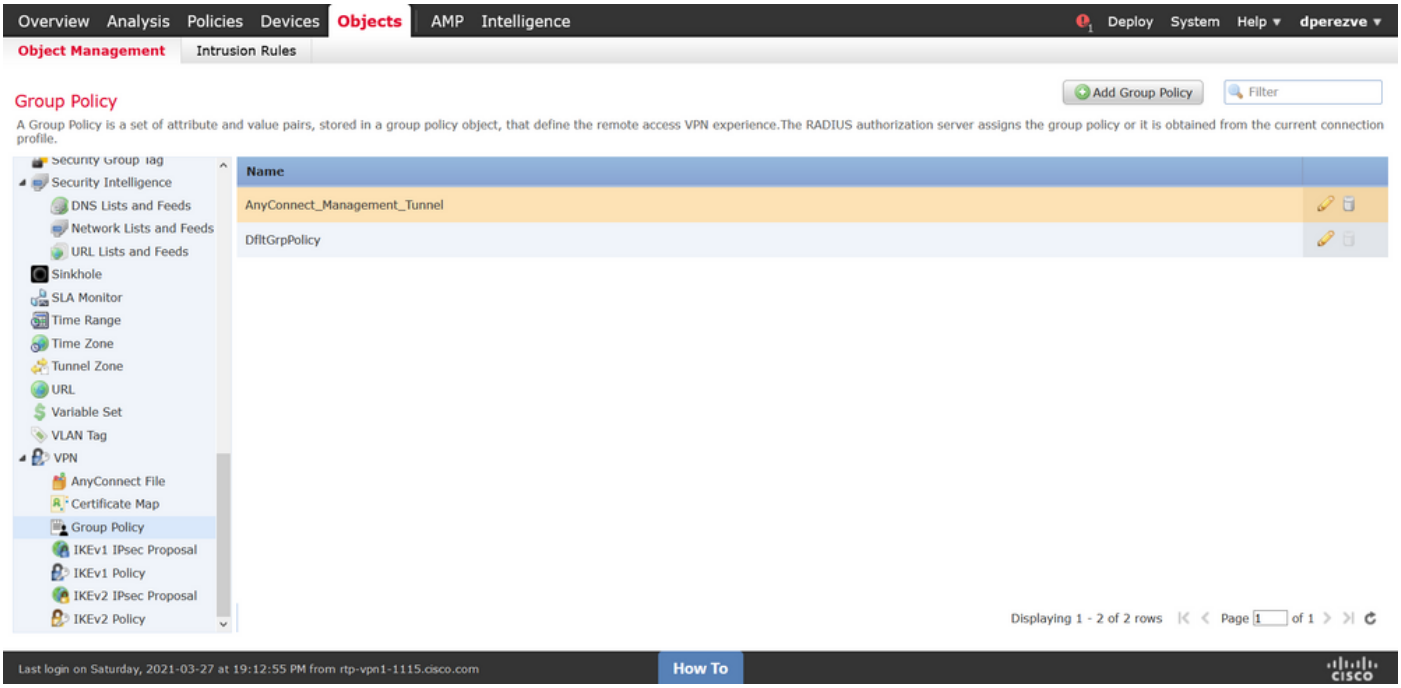
그룹 정책 추가 창이 열리면 이름을 지정하고 AnyConnect 풀을 정의하고 AnyConnect 탭**을** 엽니다 .Profile(**프로파일**)로 이동하고 Client Profile(클라이언트 프로파일) 드롭다운 메뉴에서 일반 AnyConnect VPN Profile(AnyConnect VPN 프로파일)을 나타내는 개체를 선택합니다.



그런 다음 **Management Profile(관리 프로필)** 탭으로 이동하여 Management Profile(**관리 프로필**) 드롭다운 메뉴에서 Management VPN Profile(관리 VPN 프로파일)이 포함된 개체를 선택합니다.



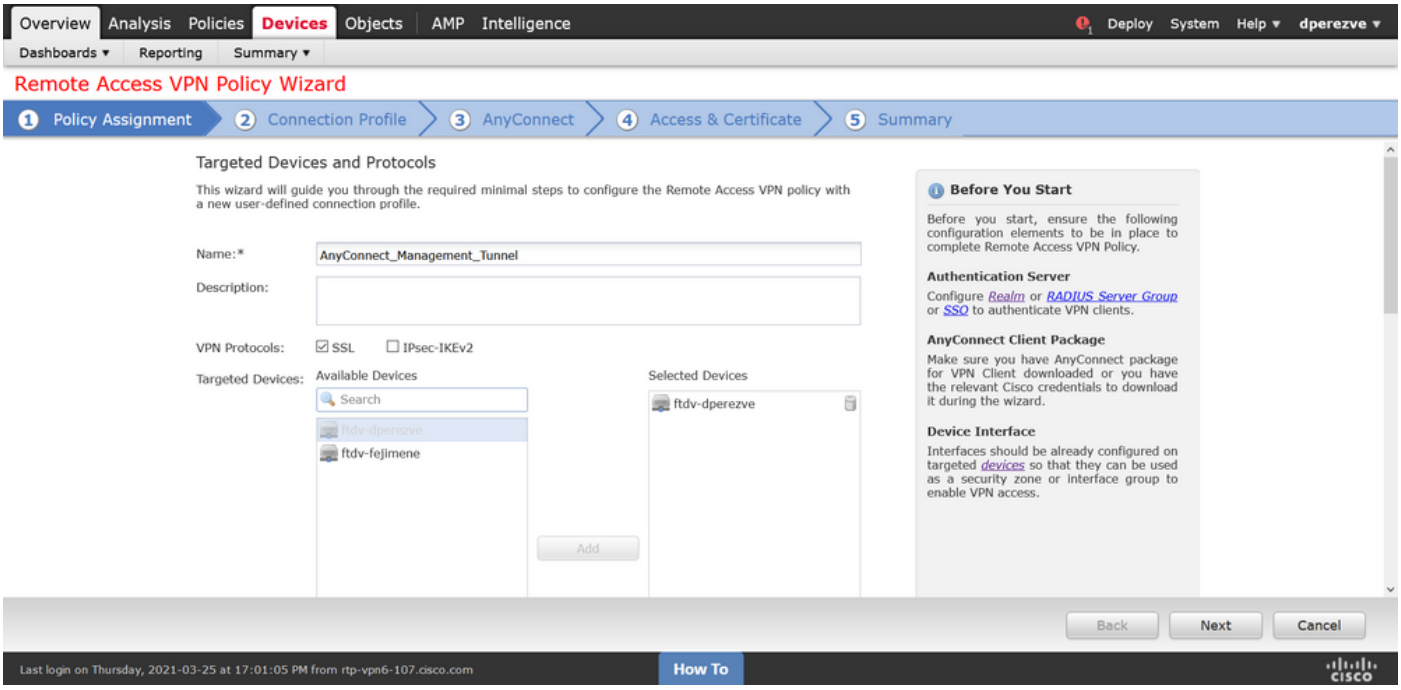
변경 사항을 저장하여 기존 그룹 정책에 새 객체를 추가합니다.



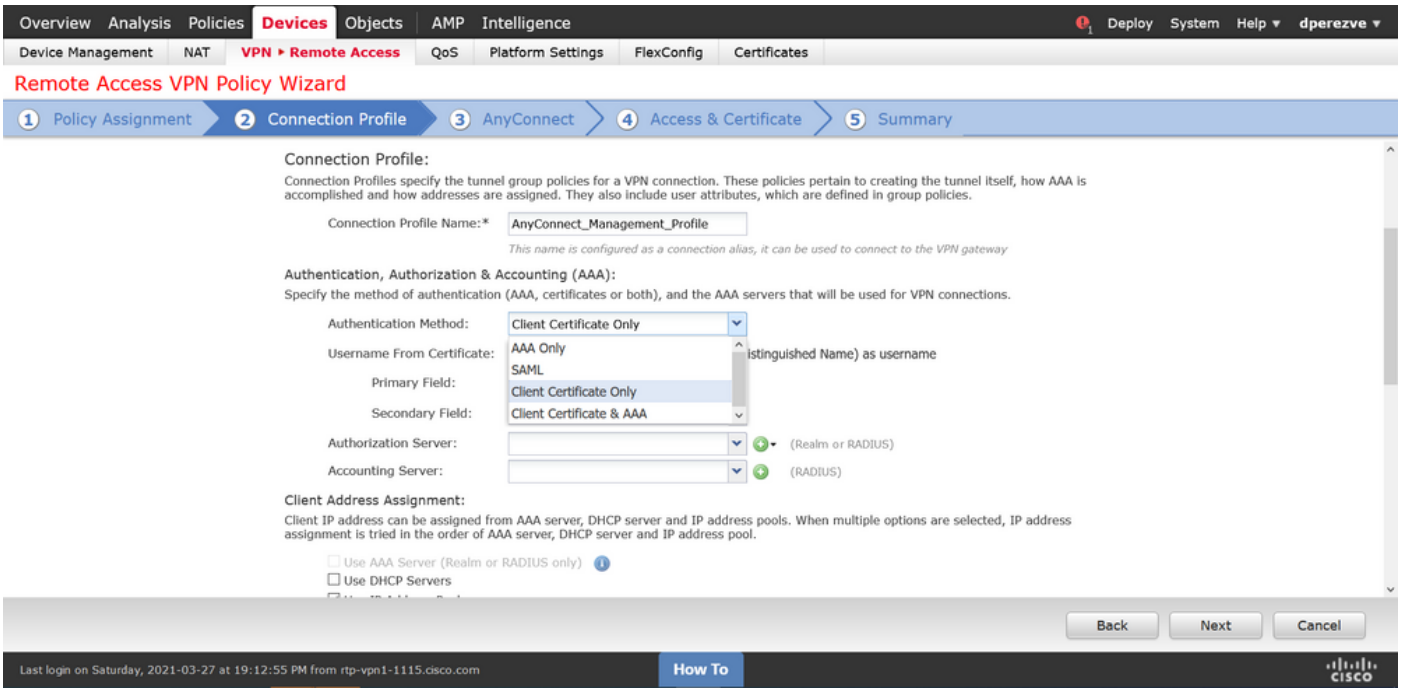
5단계. 새 AnyConnect 컨피그레이션 생성

FMC에서 SSL AnyConnect의 컨피그레이션은 4가지 단계로 구성됩니다.AnyConnect를 구성하려면 Devices(디바이스) **> VPN > Remote Access(원격 액세스)로** 이동하고 Add(**추가**) 버튼을 선택합니다.**원격 액세스 VPN 정책 마법사**를 열어야 합니다.

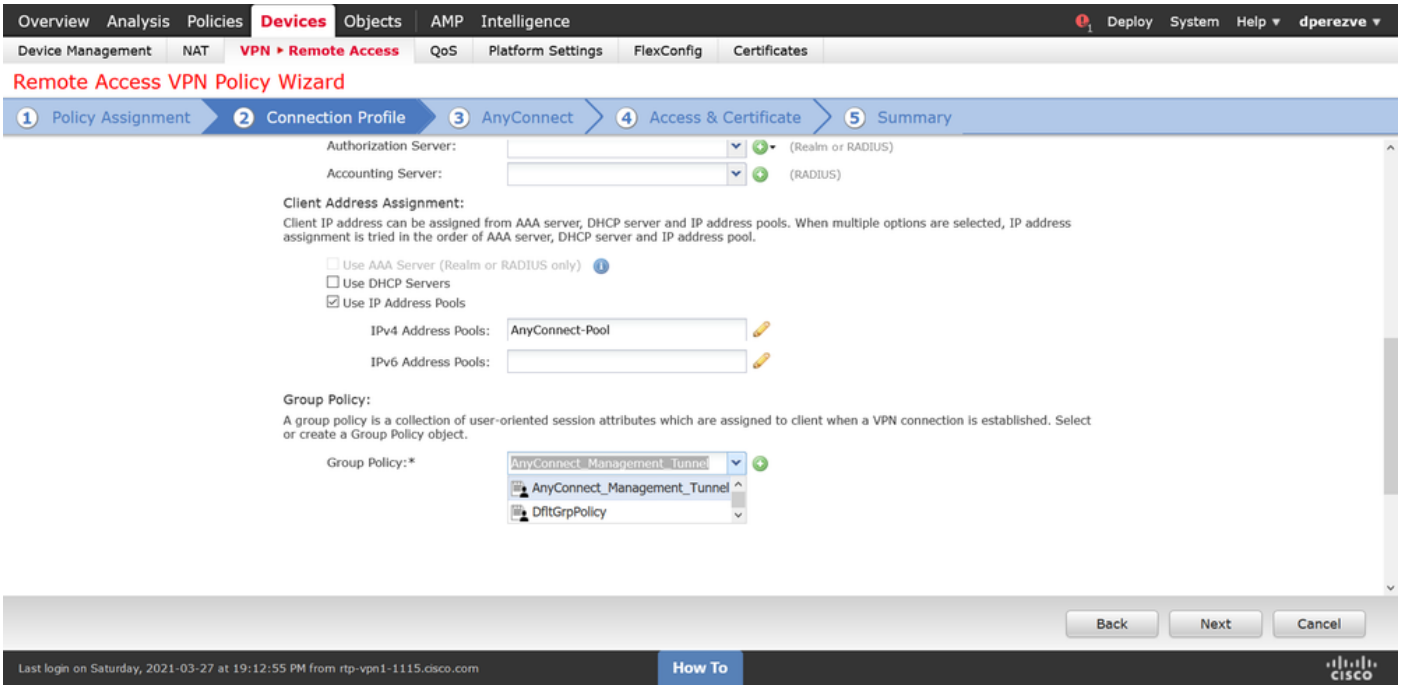
Policy **Assignment(정책 할당**) 탭에서 FTD 디바이스를 선택하고 Connection Profile(연결 프로파일)의 이름을 정의하고 SSL 확인란을 선택합니다.



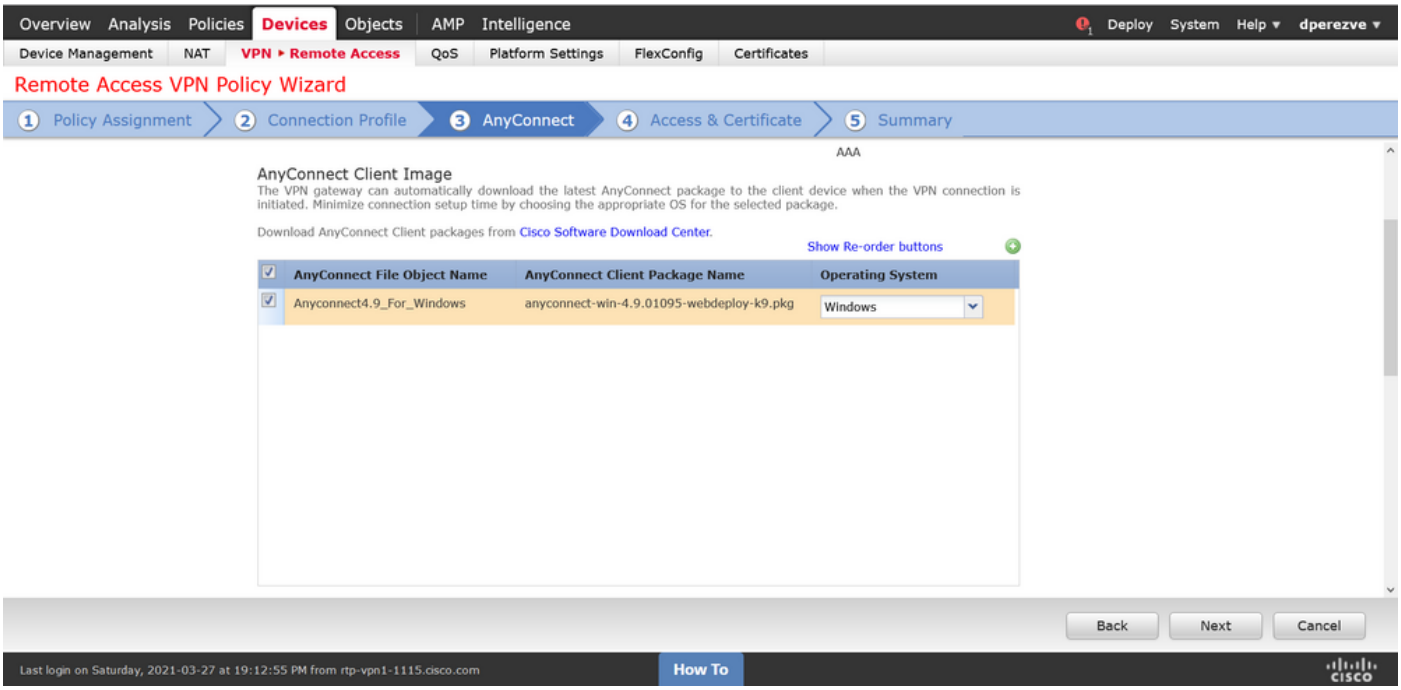
Connection **Profile(연결 프로파일)**에서 인증 방법으로 Client Certificate Only(클라이언트 인증서 전용)를 선택합니다.이 기능에서만 지원되는 인증입니다.



그런 다음 **Group Policy** 드롭다운에서 3단계에서 생성한 Group Policy 개체를 선택합니다.



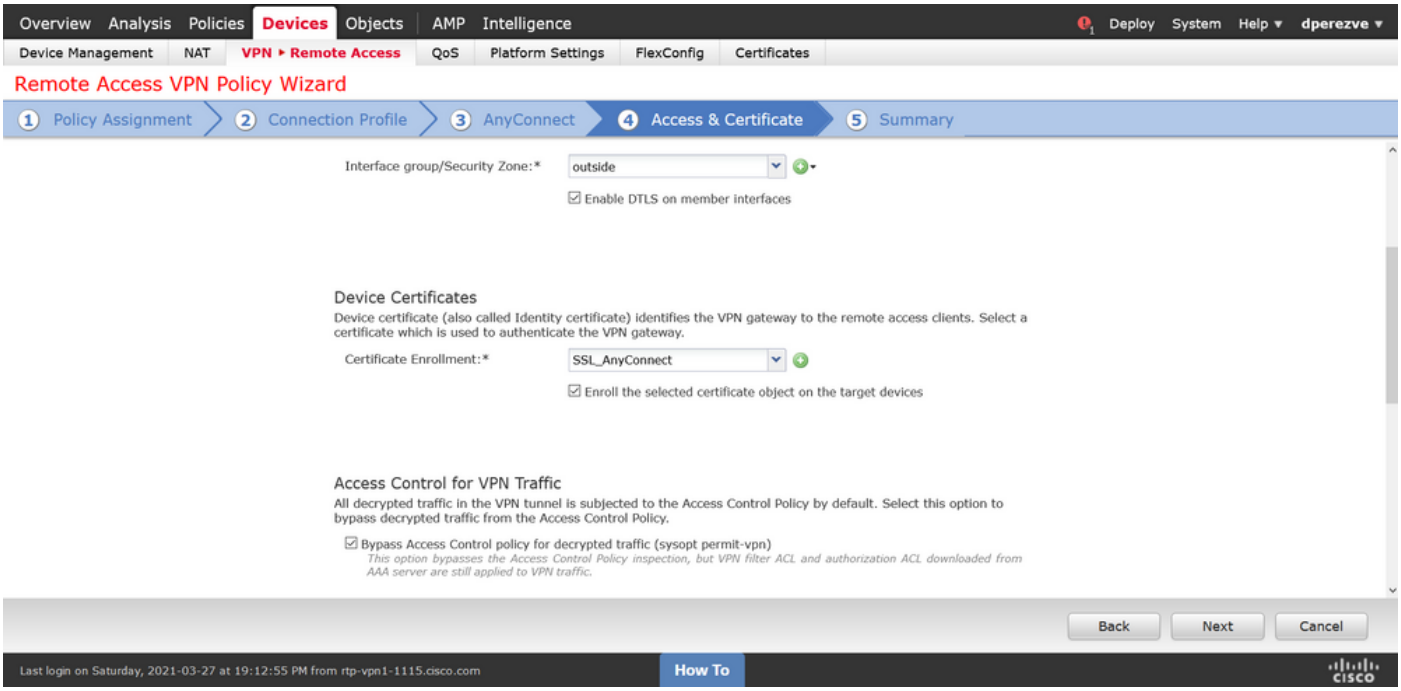
AnyConnect 탭에서 엔드포인트의 운영 체제(OS)에 따라 AnyConnect 파일 객체를 선택합니다.



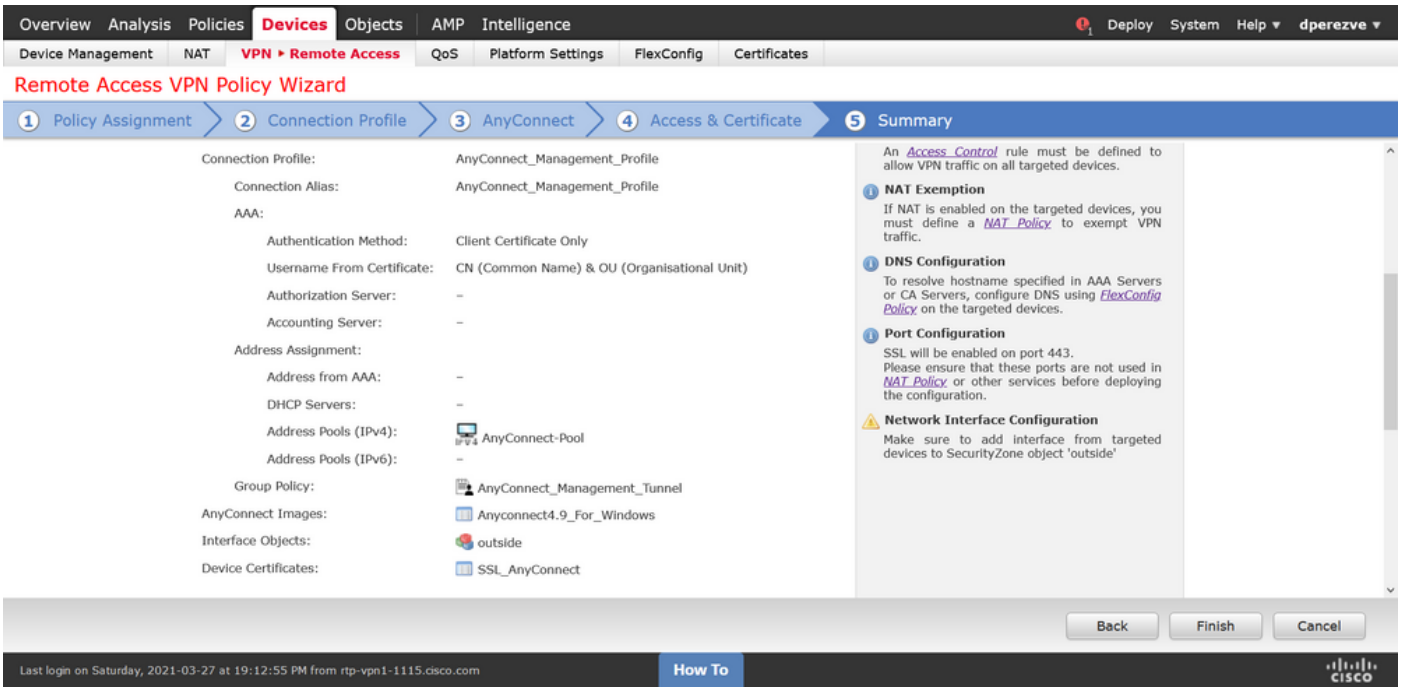
Access & Certificate에서 FTD에서 Windows 클라이언트로 ID를 프로브하기 위해 사용해야 하는 인증서를 지정합니다.

참고:사용자가 관리 VPN 기능을 사용할 때 AnyConnect 앱과 상호 작용하지 않아야 하므로 인증서를 완전히 신뢰해야 하며 경고 메시지를 인쇄해서는 안 됩니다.

참고:인증서 검증 오류를 방지하려면 인증서의 주체 이름에 포함된 CN(Common Name) 필드가 XML 프로파일 서버 목록(1단계 및 2단계)에 정의된 FQDN과 일치해야 합니다.



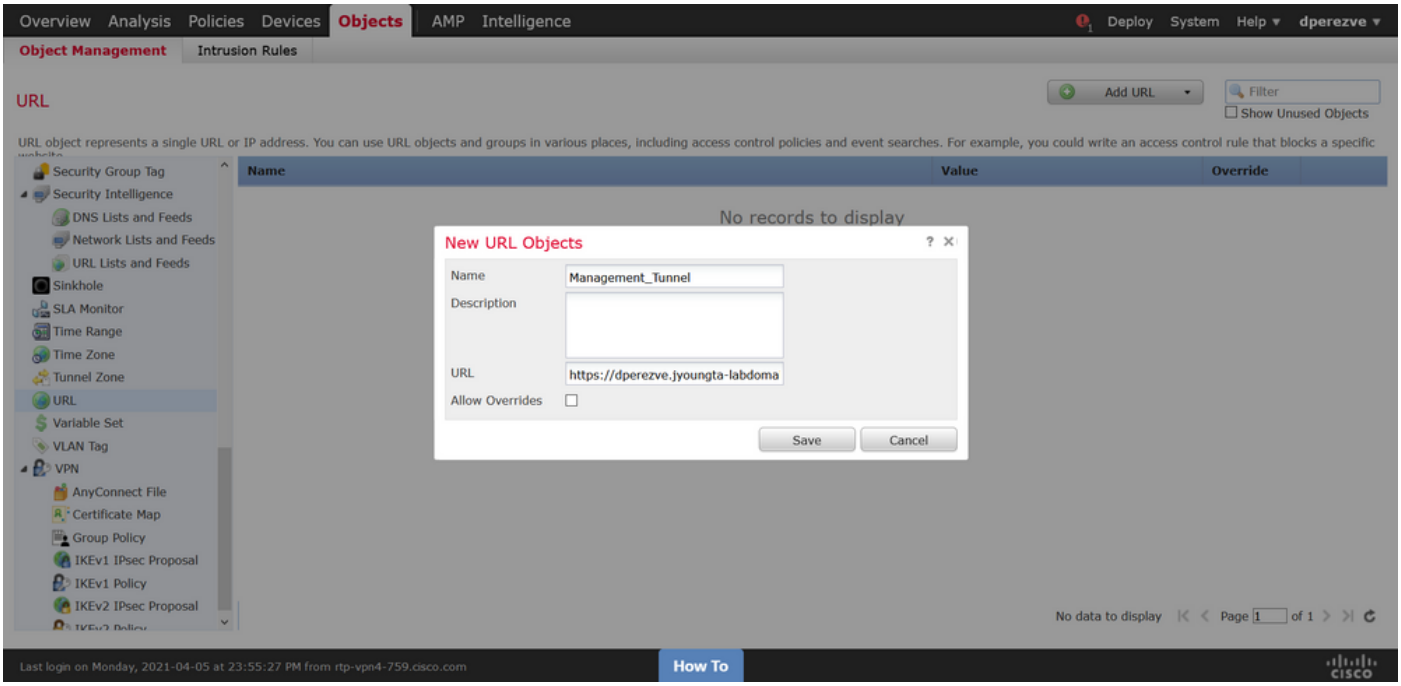
마지막으로, **요약** 탭에서 **마침** 버튼을 선택하여 새 AnyConnect 구성을 추가합니다.



6단계. URL 객체 생성

Objects(**개체**) > **Object Management(개체 관리)로** 이동하고 목차에서 **URL**을 선택합니다.그런 다음 **Add URL** 드롭다운에서 Add **Object를** 선택합니다.

개체의 이름을 제공하고 관리 VPN 프로파일 서버 목록(2단계)에 지정된 것과 동일한 FQDN/사용자 그룹을 사용하여 URL을 정의합니다. 이 예에서 URL은 dperezve.jyoungta-labdomain.cisco.com/AnyConnect_Management_Tunnel이어야 합니다.



변경 사항을 저장하여 객체 목록에 객체를 추가합니다.

7단계. URL 별칭 정의

AnyConnect 컨피그레이션에서 URL 별칭을 활성화하려면 Devices(디바이스) **> VPN > Remote Access(원격 액세스)로 이동하고** 연필 아이콘을 클릭하여 수정합니다.

그런 다음 **Connection Profile(연결 프로파일)** 탭에서 현재 구성을 선택하고 **Aliases(별칭)**로 이동한 다음 **Add(추가)** 버튼을 클릭하고 **URL Alias(URL 별칭) 드롭다운**에서 **URL Object(URL 개체)를 선택합니다.**Enabled(활성화됨) 확인란이 선택되었는지 확인합니다.

변경 사항을 저장하고 FTD에 컨피그레이션을 구축합니다.

다음을 확인합니다.

구축이 완료되면 AnyConnect VPN 프로필과 함께 첫 번째 수동 AnyConnect 연결이 필요합니다.이 연결 중에 관리 VPN 프로파일이 FTD에서 다운로드되어 C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun에 **저장됩니다**.이 시점부터 사용자 상호 작용 없이 관리 VPN 프로파일을 통해 후속 연결을 시작해야 합니다.

문제 해결

인증서 검증 오류:

- CA(Certificate Authority)의 루트 인증서가 FTD에 설치되어 있는지 확인합니다.
- 동일한 CA에서 서명한 ID 인증서가 Windows 컴퓨터 저장소에 설치되어 있는지 확인합니다.
- CN 필드가 인증서에 포함되어 있고 URL 별칭에 정의된 관리 VPN 프로필 및 FQDN의 서버 목록에 정의된 FQDN과 동일한지 확인합니다.

관리 터널이 시작되지 않은 경우:

- 관리 VPN 프로파일이 다운로드되어 C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun에 저장되었는지 **확인합니다**.
- 관리 VPN 프로필의 이름이 VpnMgmtTunProfile**.xml인지 확인합니다**.

연결 문제가 발생하면 DART 번들을 수집하고 자세한 내용은 Cisco TAC에 문의하십시오.