FTD, ISE, DUO 및 Active Directory를 통해 SSL VPN 인증 구성

목차

소개

이 문서에서는 Cisco ISE 및 AAA용 DUO Security를 사용한 Firepower 위협 방어의 SSLVPN 통합에 대해 설명합니다.

요구 사항

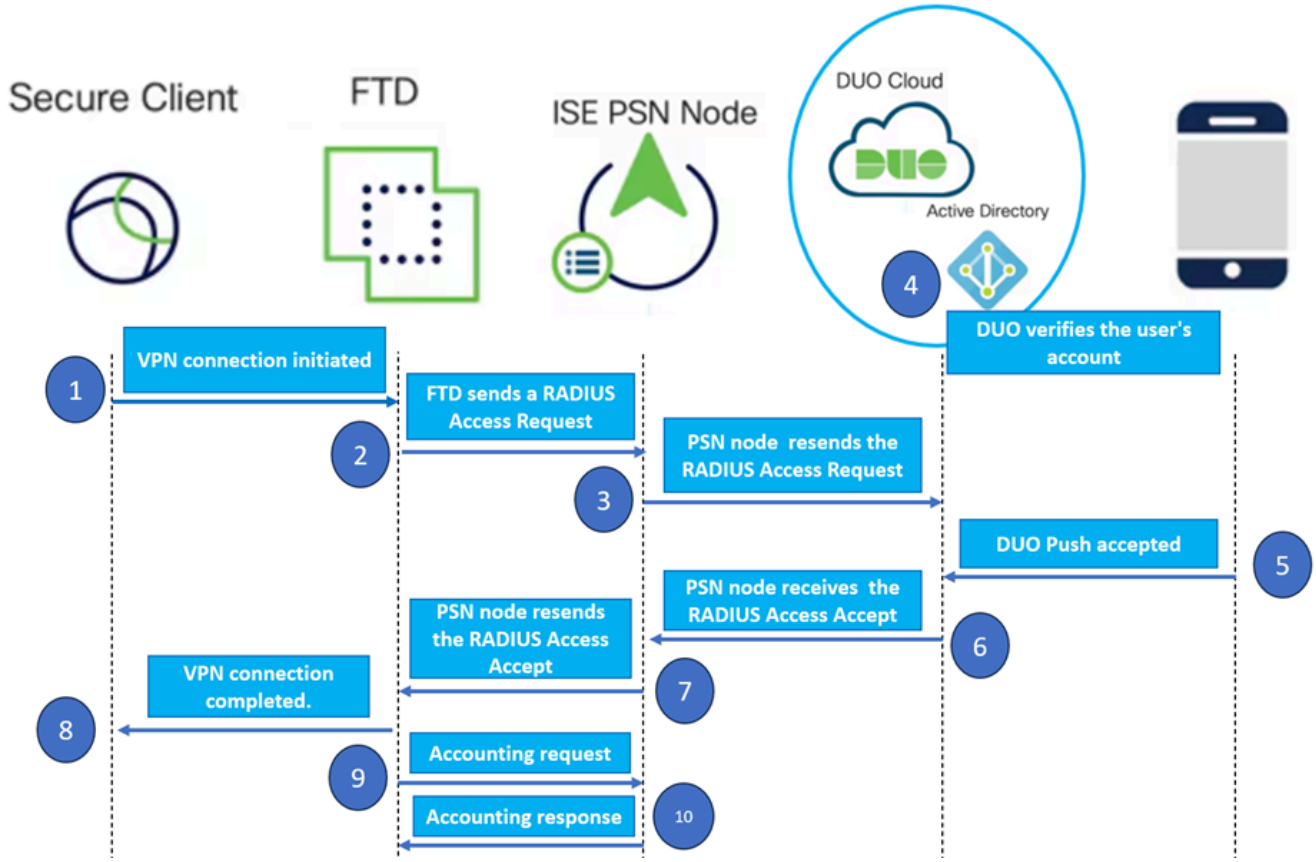
- ISE 3.0 이상
- 7.0 이상.
- FTD 7.0 이상
- DUO 인증 프록시.
- ISE Essentials 라이센스
- DUO Essentials 라이센싱

사용되는 구성 요소

- ISE 3.2 패치 3
- FMC 7.2.5
- FTD 7.2.5
- Proxy DUO 6.3.0
- Any Connect 4.10.08029

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.

네트워크 다이어그램



토폴로지.

제안 된 솔루션에서 Cisco ISE는 중요 한 RADIUS 서버 프록시 입니다. 인증 또는 권한 부여 정책을 직접 평가하는 대신 ISE는 FTD에서 DUO 인증 프록시로 RADIUS 패킷을 전달하도록 구성됩니다.

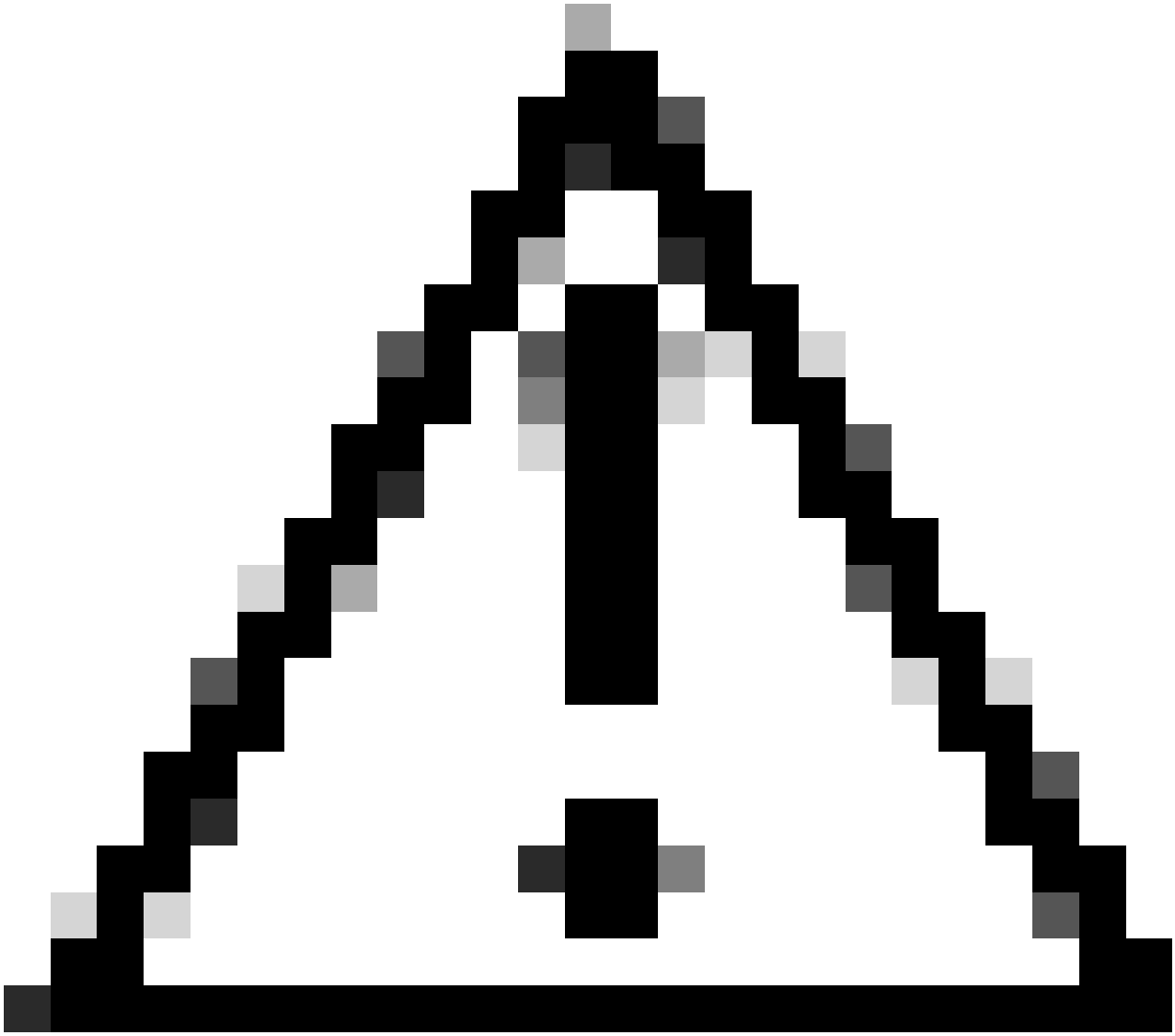
DUO 인증 프록시는 이 인증 흐름 내에서 전용 중재자로 작동합니다. Windows 서버에 설치되어 Cisco ISE와 DUO 클라우드 간의 격차를 해소합니다. 프록시 기본 기능은 RADIUS 패킷에서 캡슐화된 인증 요청을 DUO 클라우드로 전송하는 것입니다. DUO Cloud는 2단계 인증 컨피그레이션을 기반으로 네트워크 액세스를 허용하거나 거부합니다.

1. 사용자가 고유한 사용자 이름과 비밀번호를 입력하여 VPN 인증 프로세스를 시작합니다.

2. FTD(Firewall Threat Defense)가 Cisco ISE(Identity Services Engine)에 인증 요청을 보냅니다.

3. PSN(Policy Services Node)이 DUO 인증 프록시 서버에 인증 요청을 전달합니다. 그런 다음 DUO 인증 서버는 DUO 클라우드 서비스를 통해 자격 증명을 검증합니다.

4. DUO 클라우드는 동기화된 데이터베이스에 대해 사용자 이름 및 비밀번호를 확인합니다.



주의: DUO Cloud에서 최신 사용자 데이터베이스를 유지하려면 DUO Cloud와 조직 Active Directory 간의 동기화를 활성화해야 합니다.

5. 인증에 성공하면 DUO Cloud는 암호화된 보안 푸시 알림을 통해 사용자가 등록한 모바일 디바이스에 대한 DUO Push를 시작합니다. 그런 다음 사용자는 DUO Push를 승인하여 ID를 확인하고 진행해야 합니다.

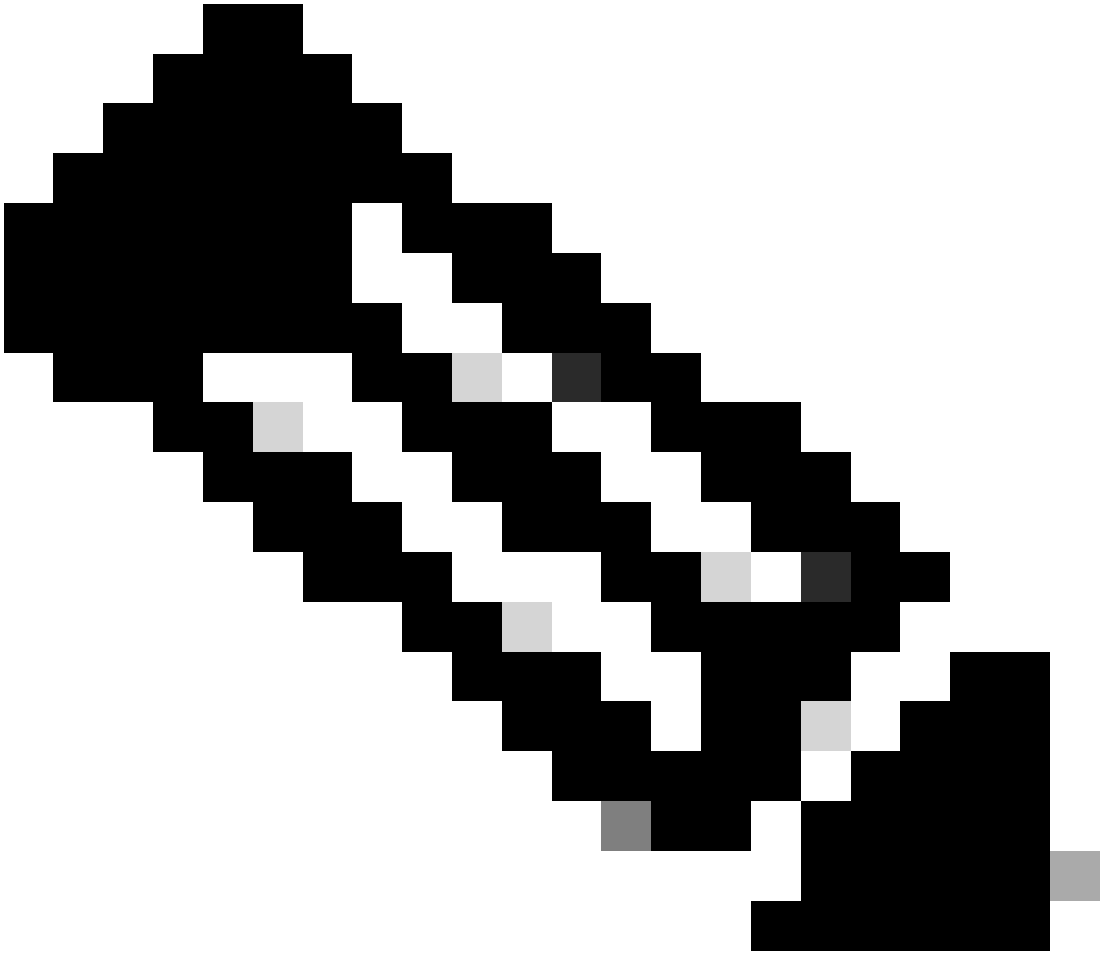
6. 사용자가 DUO Push를 승인하면 DUO 인증 프록시 서버는 인증 요청이 사용자에 의해 수락되었음을 나타내는 확인 메시지를 PSN에 다시 보냅니다.

7. PSN 노드가 확인 메시지를 FTD에 전송하여 사용자가 인증되었음을 알립니다.

8. FTD가 인증 확인을 수신하고 적절한 보안 조치를 적용하여 엔드포인트에 대한 VPN 연결을 설정합니다.

9. FTD는 성공한 VPN 연결의 세부 정보를 기록하고 기록 보관 및 감사를 위해 회계 데이터를 ISE 노드로 안전하게 다시 전송합니다.

10. ISE 노드는 모든 레코드가 안전하게 저장되며 향후 감사 또는 규정 준수 확인을 위해 액세스할 수 있도록 계정 관리 정보를 livelogs에 기록합니다.



참고:

이 가이드의 설정에서는 다음 네트워크 매개변수를 사용합니다.

- 기본 네트워크 서버(PNS) 노드 IP: 10.4.23.21

- 피어 VPN용 FTD(Firepower 위협 방어) IP: 10.4.23.53

- DUO 인증 프록시 IP: 10.31.126.207

- 도메인 이름: testlab.local

설정

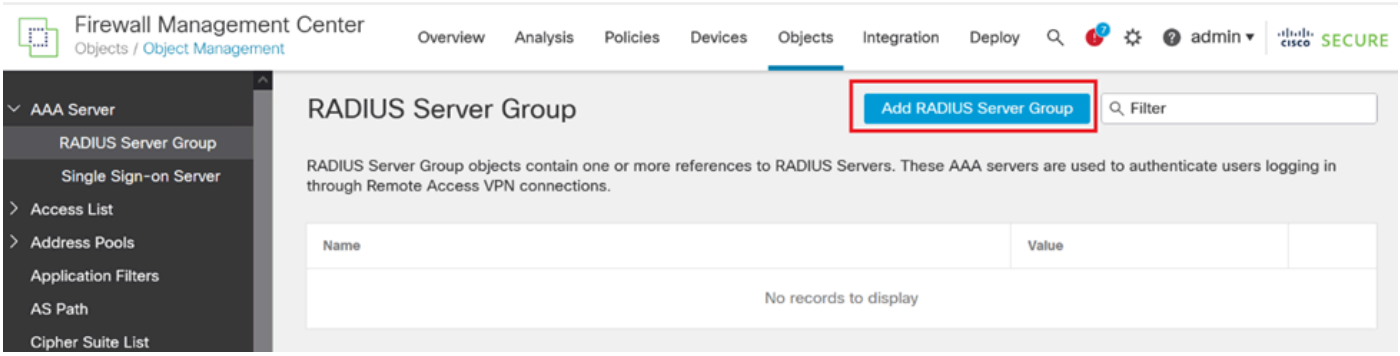
FTD 구성.

FMC(Firepower 관리 센터) 내에 RADIUS 서버 통합

1. 웹 브라우저를 시작하고 FMC IP 주소를 입력하여 GUI를 열어 FMC에 액세스합니다.

2. 객체 메뉴로 이동하여 AAA 서버를 선택한 후 RADIUS 서버 그룹 옵션으로 진행합니다.

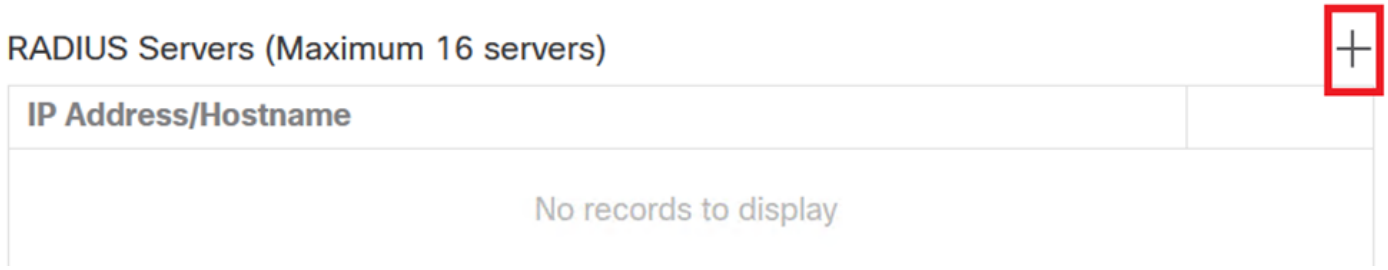
3. Add RADIUS Server Group(RADIUS 서버 그룹 추가) 버튼을 클릭하여 RADIUS 서버에 대한 새 그룹을 생성합니다.



RADIUS 서버 그룹

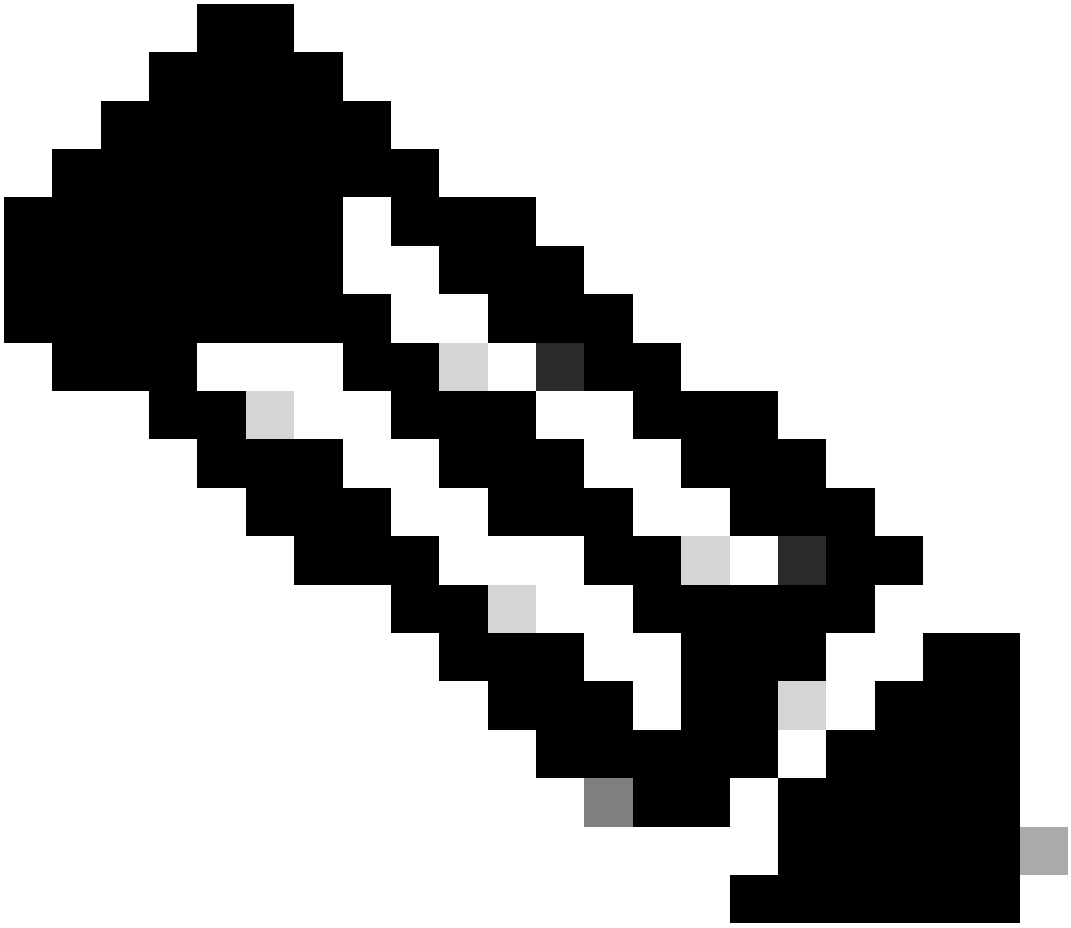
4. 네트워크 인프라 내에서 명확한 식별을 보장하려면 새 AAA RADIUS 서버 그룹에 대한 설명 이름을 입력합니다.

5. 그룹 구성 내에서 적절한 옵션을 선택하여 새 RADIUS 서버를 추가합니다.RADIUS

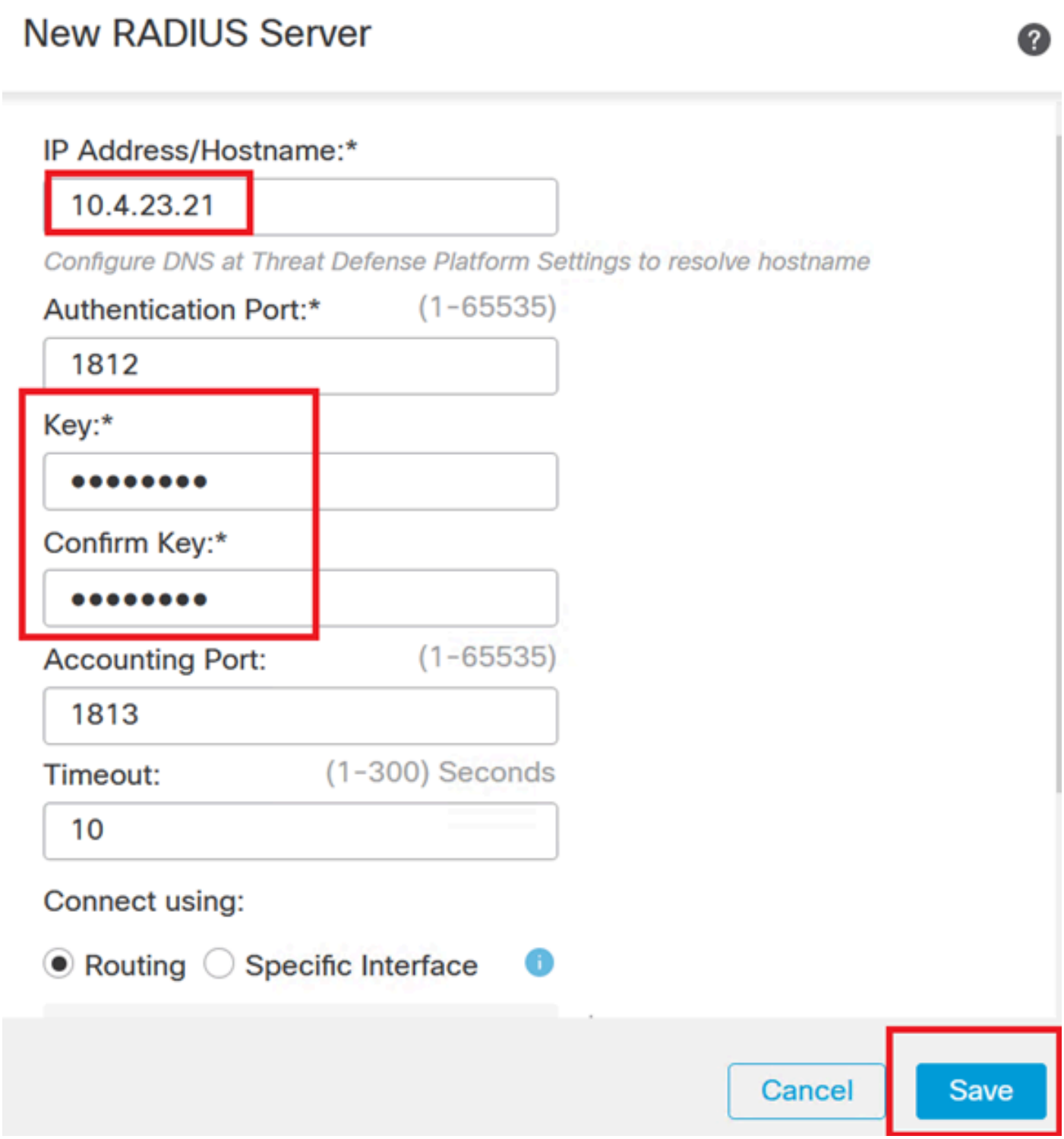


서버.

6. RADIUS 서버 IP 주소를 지정하고 공유 비밀 키를 입력합니다.

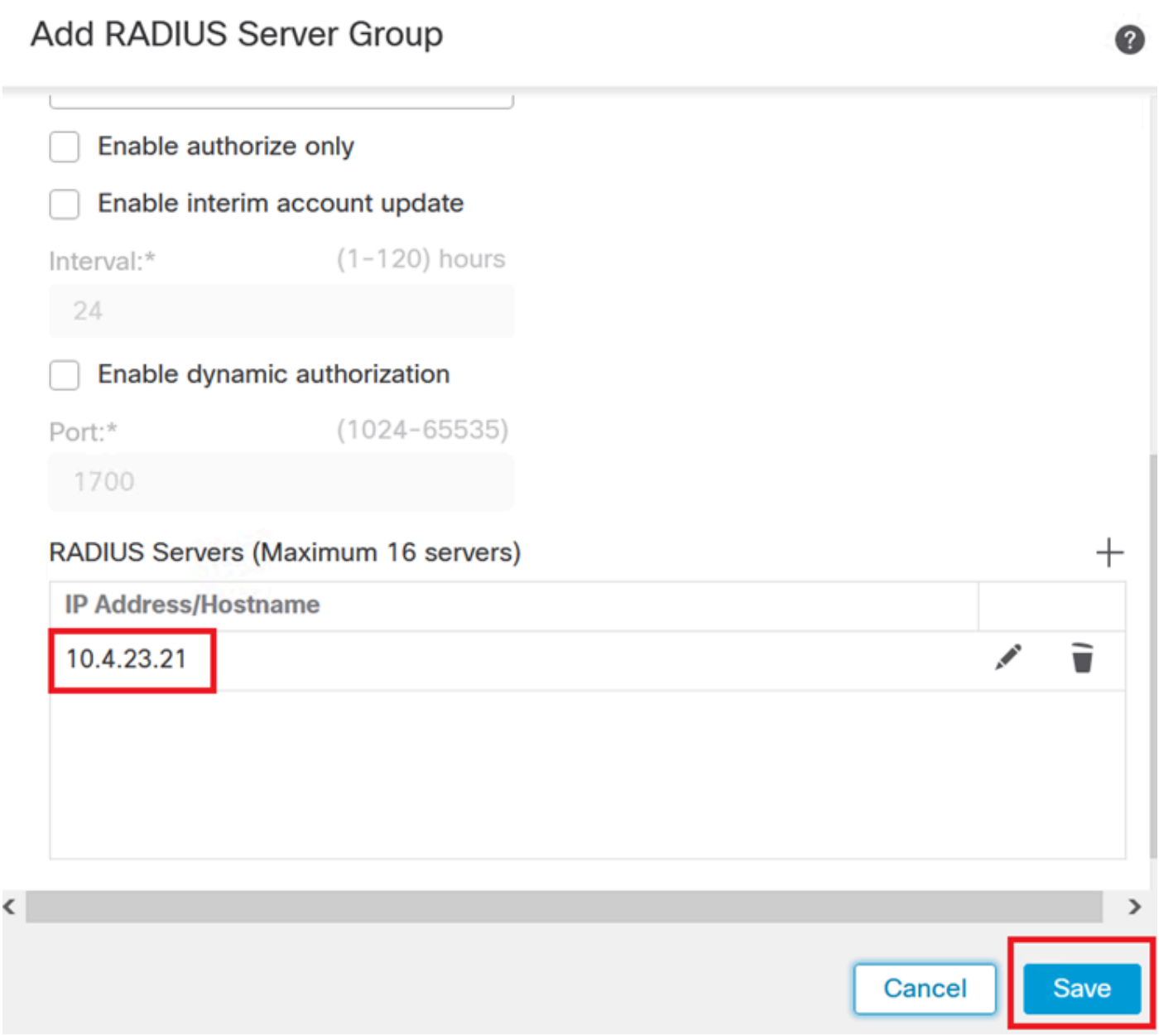


참고: 성공적인 RADIUS 연결을 위해 이 비밀 키를 ISE 서버와 안전하게 공유해야 합니다.



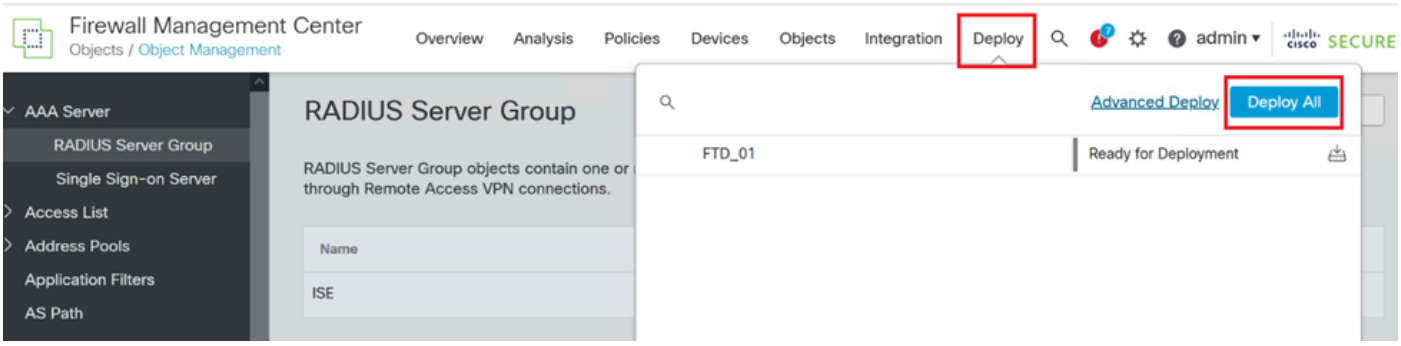
새 *RADIUS* 서버.

7. RADIUS 서버 세부사항을 구성한 후 [저장]을 클릭하여 RADIUS 서버 그룹에 대한 설정을 보존합니다.



서버 그룹 세부 정보.

8. 네트워크 전체에서 AAA 서버 구성을 마무리하고 구현하려면 [배치] 메뉴로 이동한 다음 [모두 배치]를 선택하여 설정을 적용합니다.

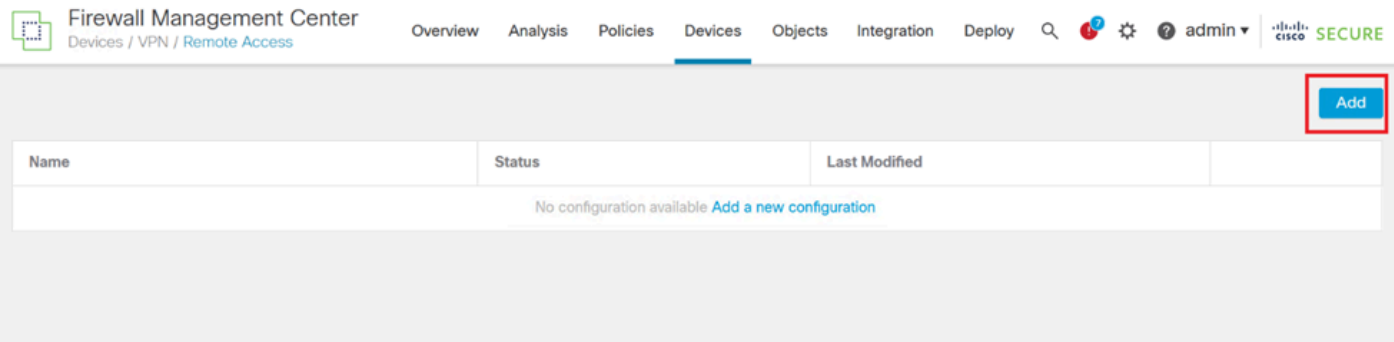


AAA 서버를 구축하는 중입니다.

원격 VPN을 구성합니다.

1. FMC GUI에서 Devices(디바이스) > VPN > Remote Access(원격 액세스)로 이동하여 VPN 컨피그레이션 프로세스를 시작합니다.

2. 새 VPN 연결 프로파일을 생성하려면 Add(추가) 버튼을 클릭합니다.

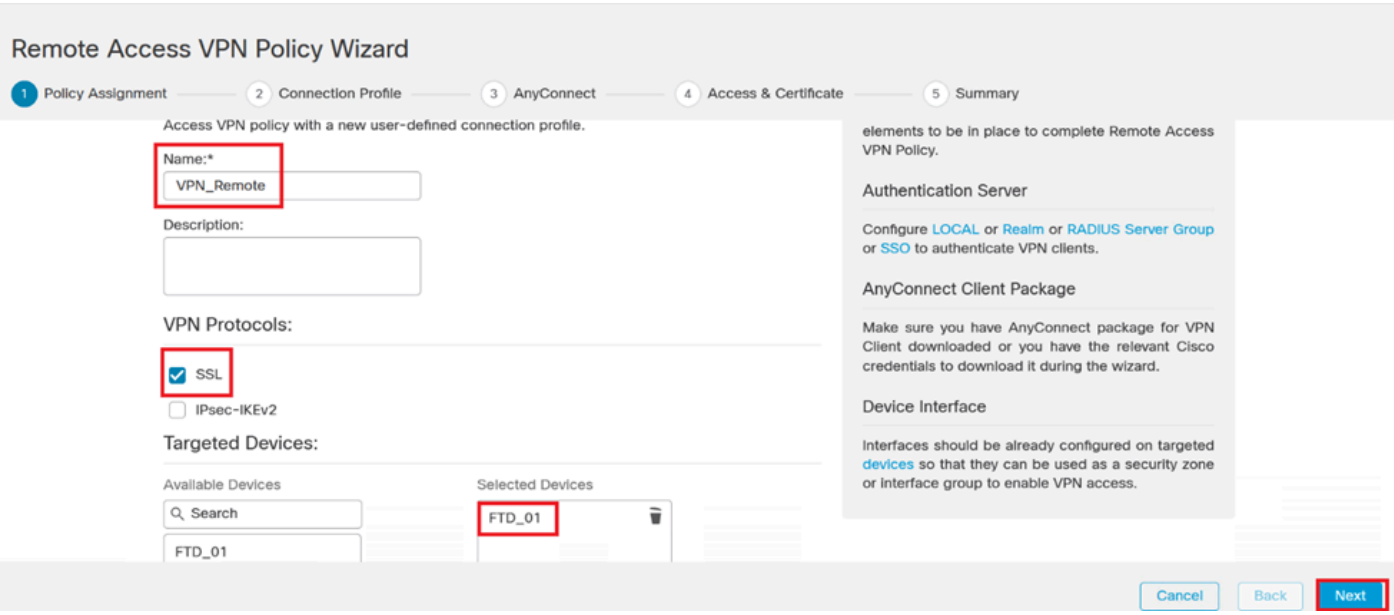


VPN 연결 프로파일

3. 네트워크 설정 내에서 VPN을 식별할 수 있도록 VPN에 대한 고유한 설명 이름을 입력합니다.

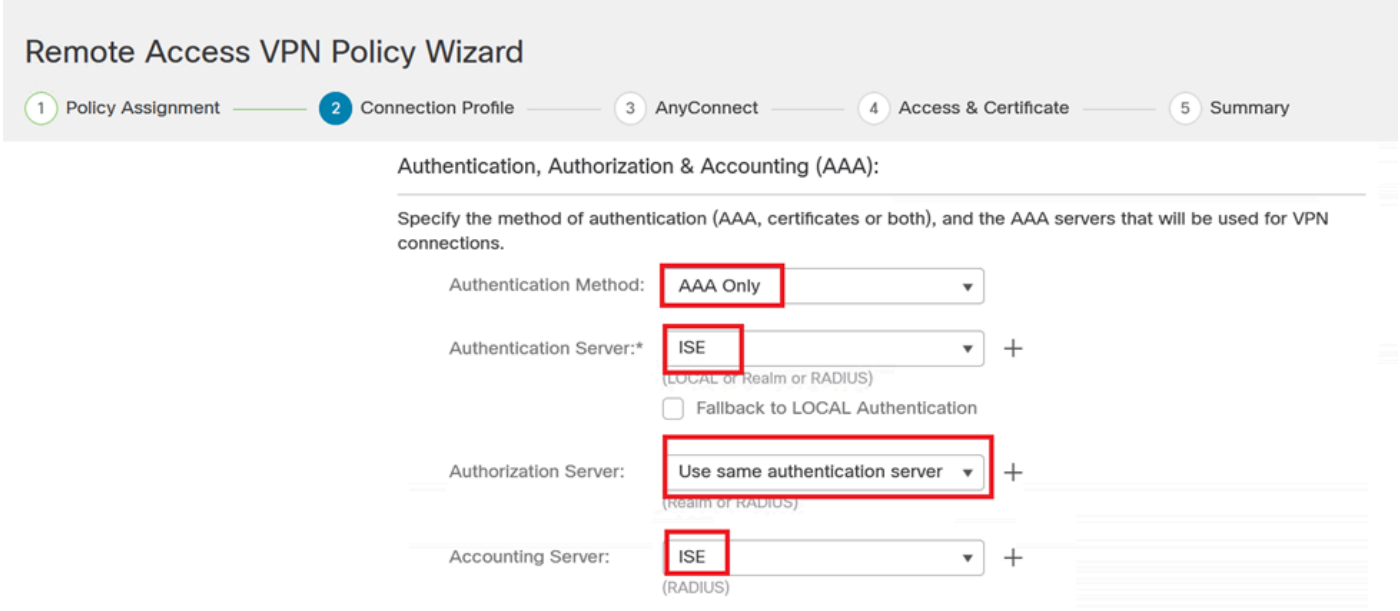
4. SSL VPN 프로토콜을 사용하여 보안 연결을 보장하려면 SSL 옵션을 선택합니다.

5. 디바이스 목록에서 특정 FTD 디바이스를 선택합니다.



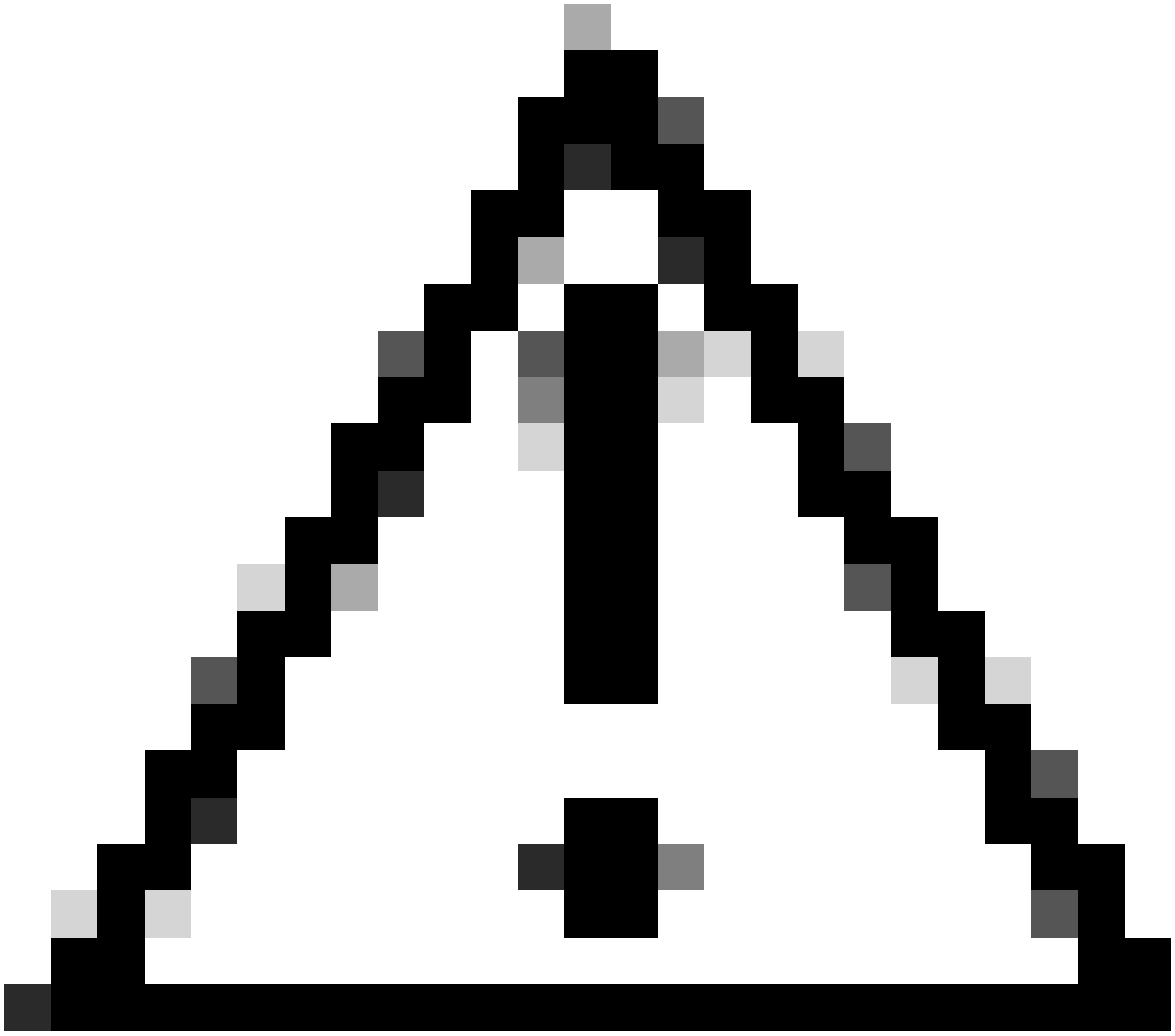
VPN 설정.

6. 인증 설정에서 PSN 노드를 사용하도록 AAA 방법을 구성합니다.

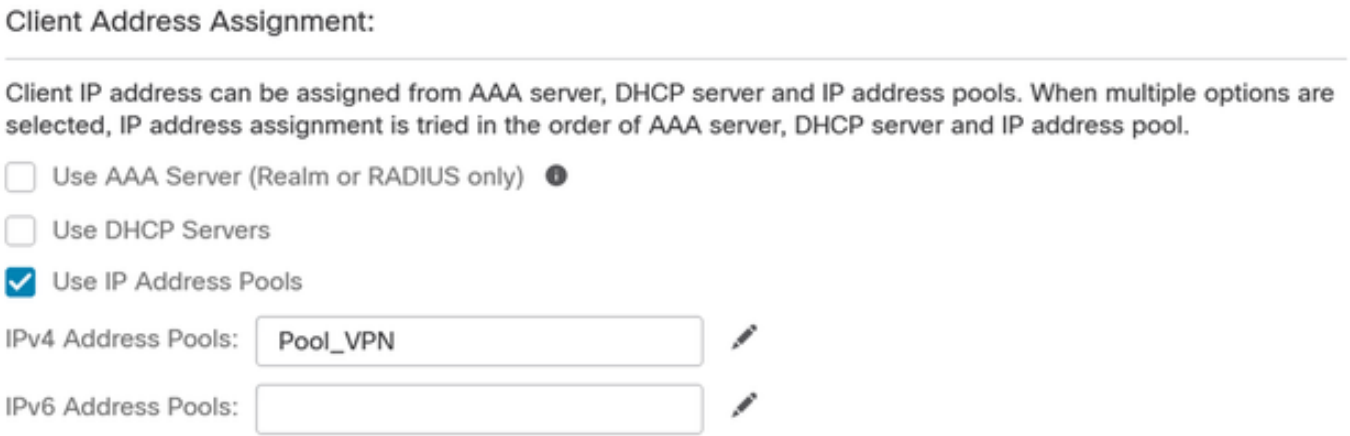


연결 프로파일.

7. VPN에 대한 동적 IP 주소 할당을 설정합니다.

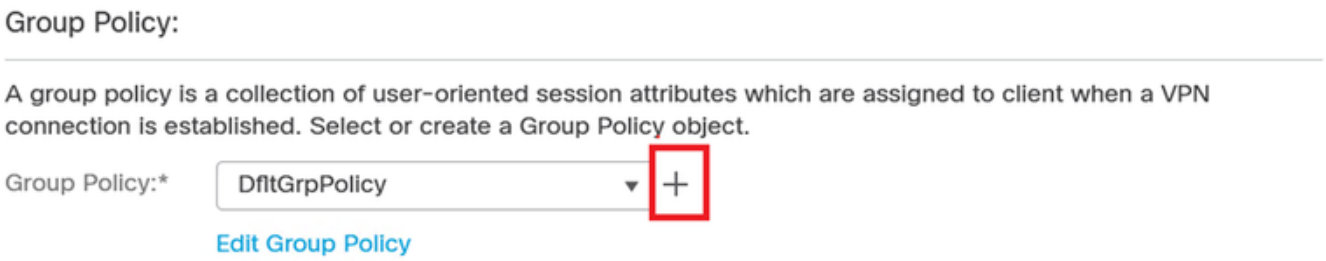


주의: 예를 들어 DHCP VPN 풀이 선택되었습니다.



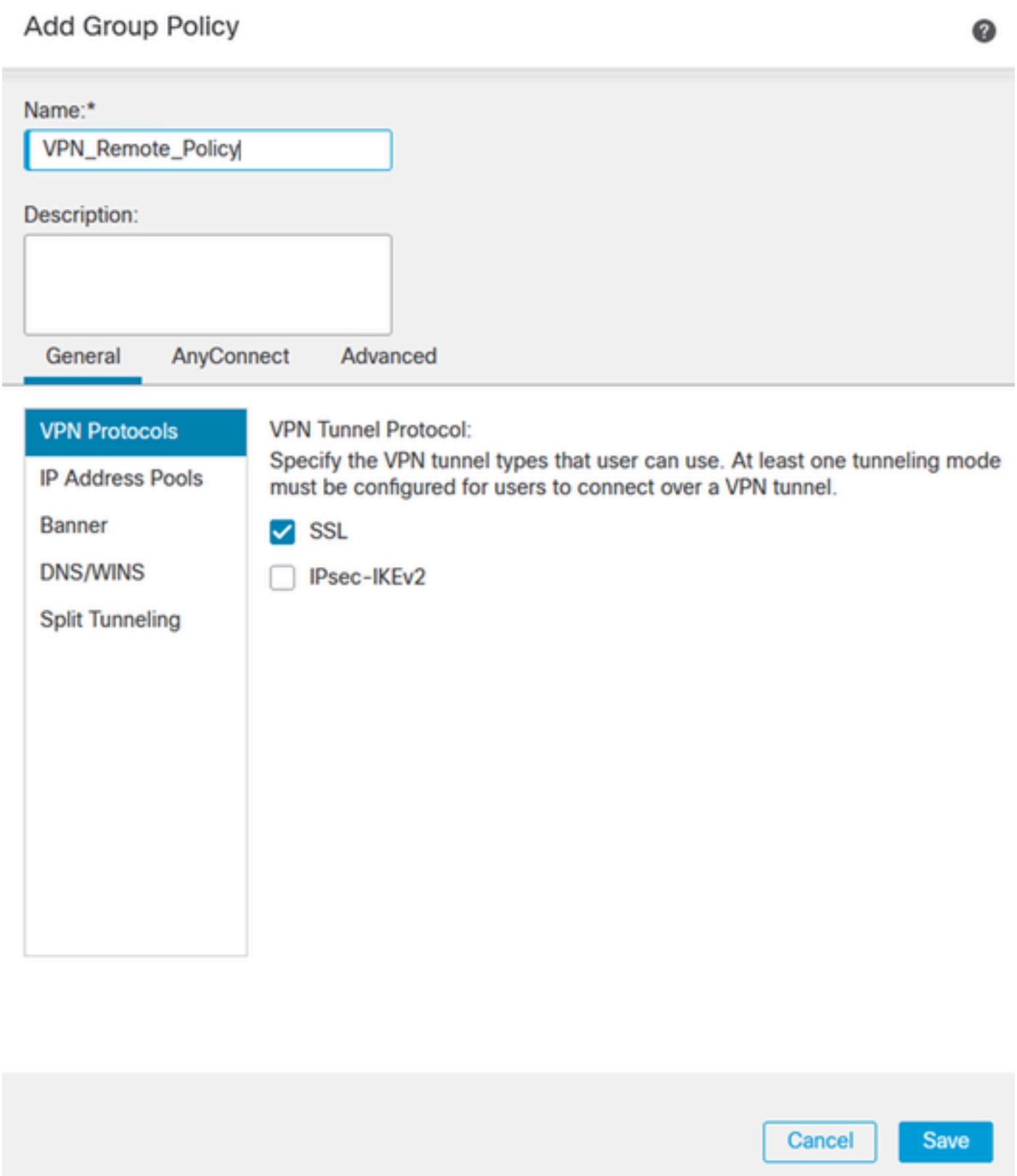
IP 주소 풀.

8. 새 그룹 정책을 생성합니다.



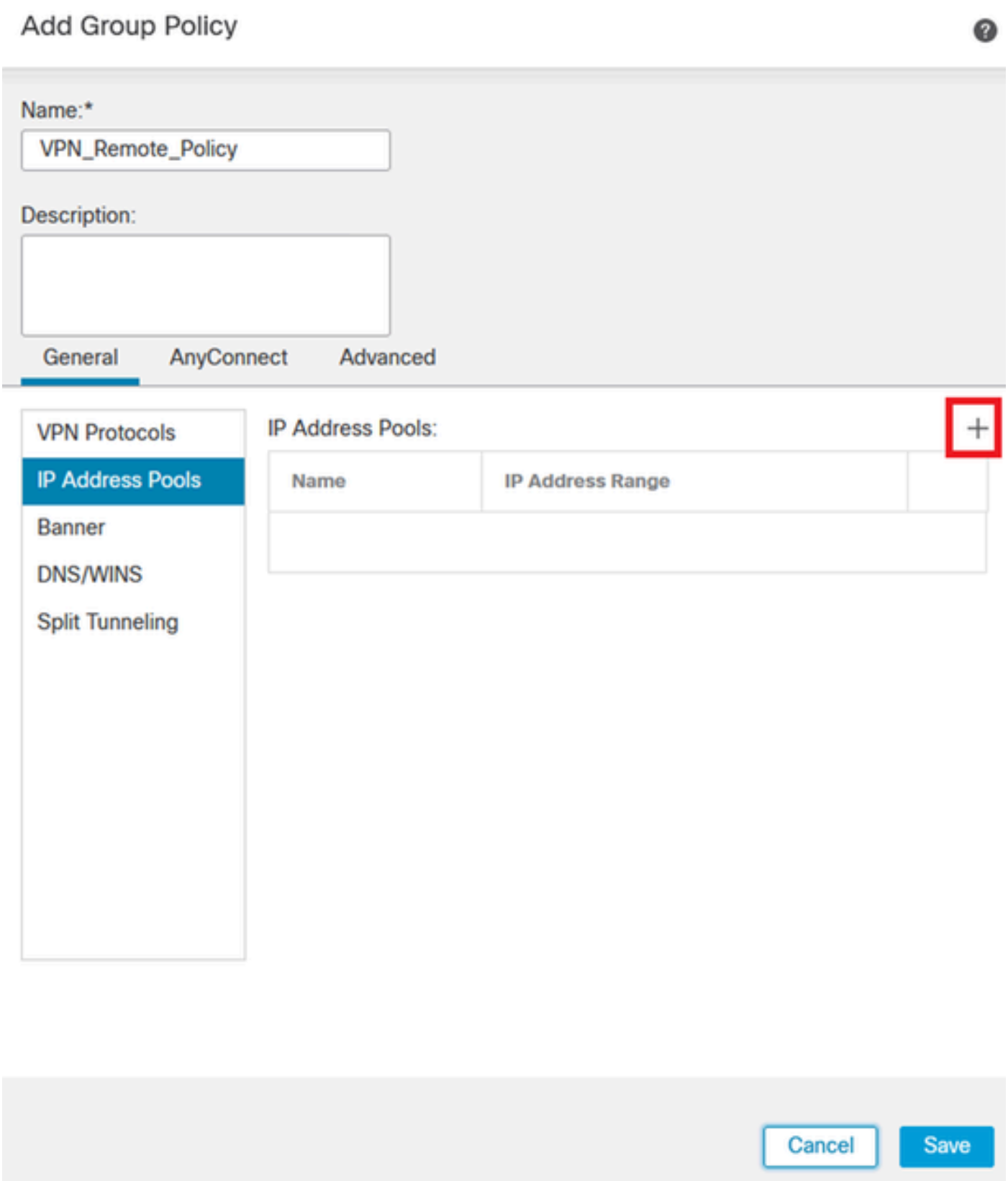
그룹 정책.

9. 그룹 정책 설정에서 SSL 프로토콜이 선택되었는지 확인합니다.



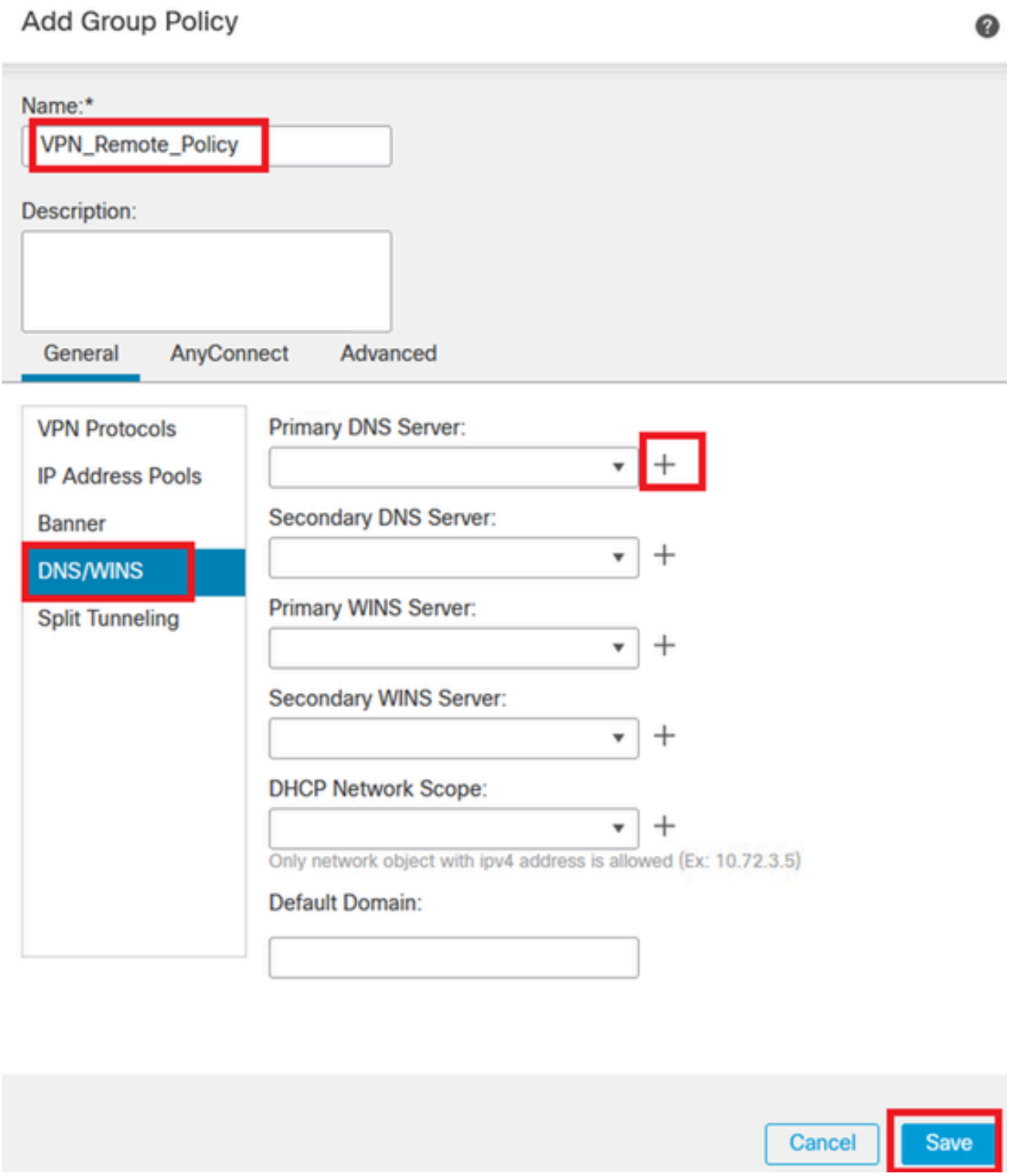
VPN 프로토콜

10. 새 VPN 풀을 생성하거나 기존 풀을 선택하여 VPN 클라이언트에 사용할 수 있는 IP 주소 범위를 정의합니다.

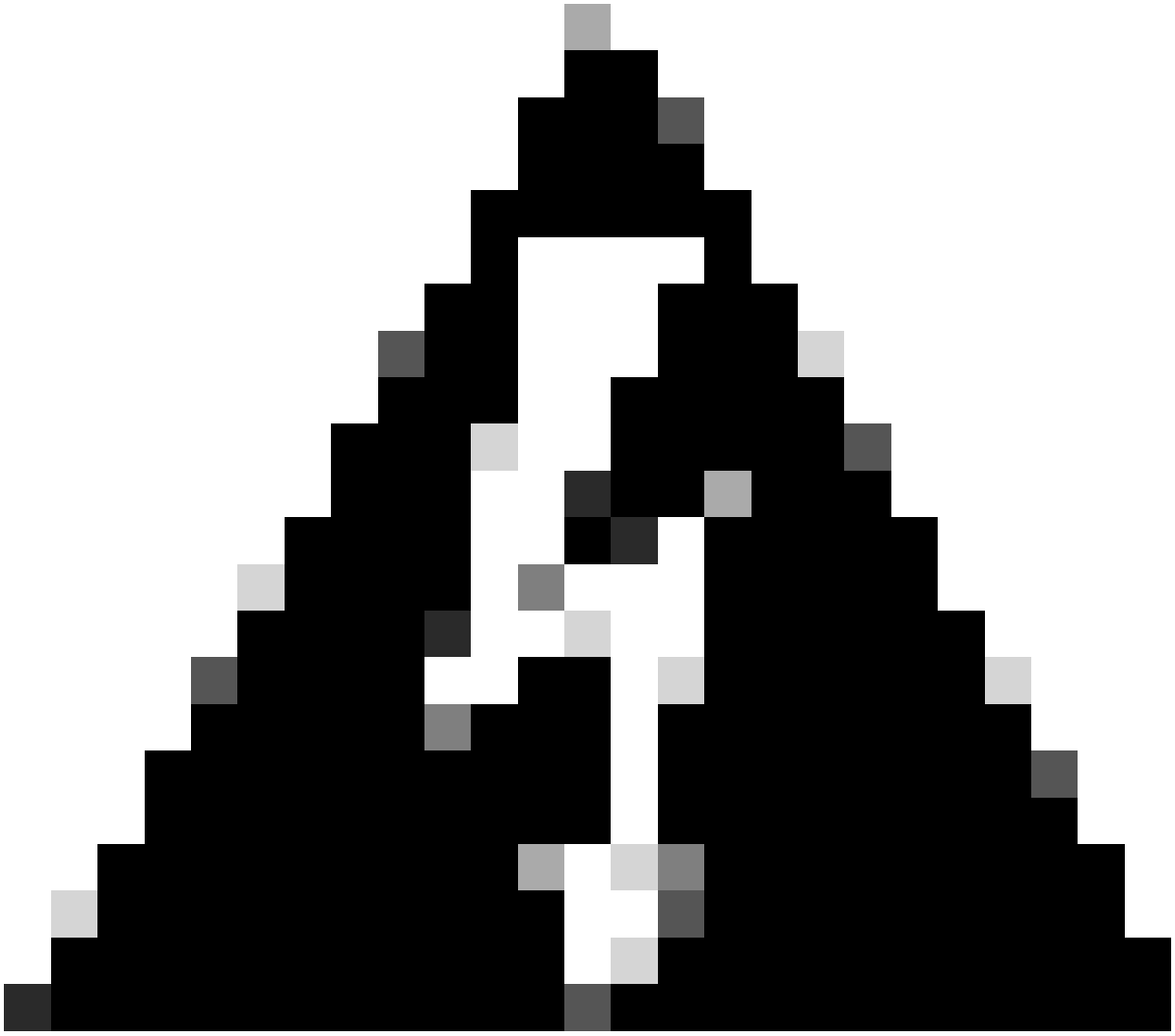


폴 *VPN.*

11. VPN 연결에 대한 DNS 서버 세부 정보를 지정합니다.

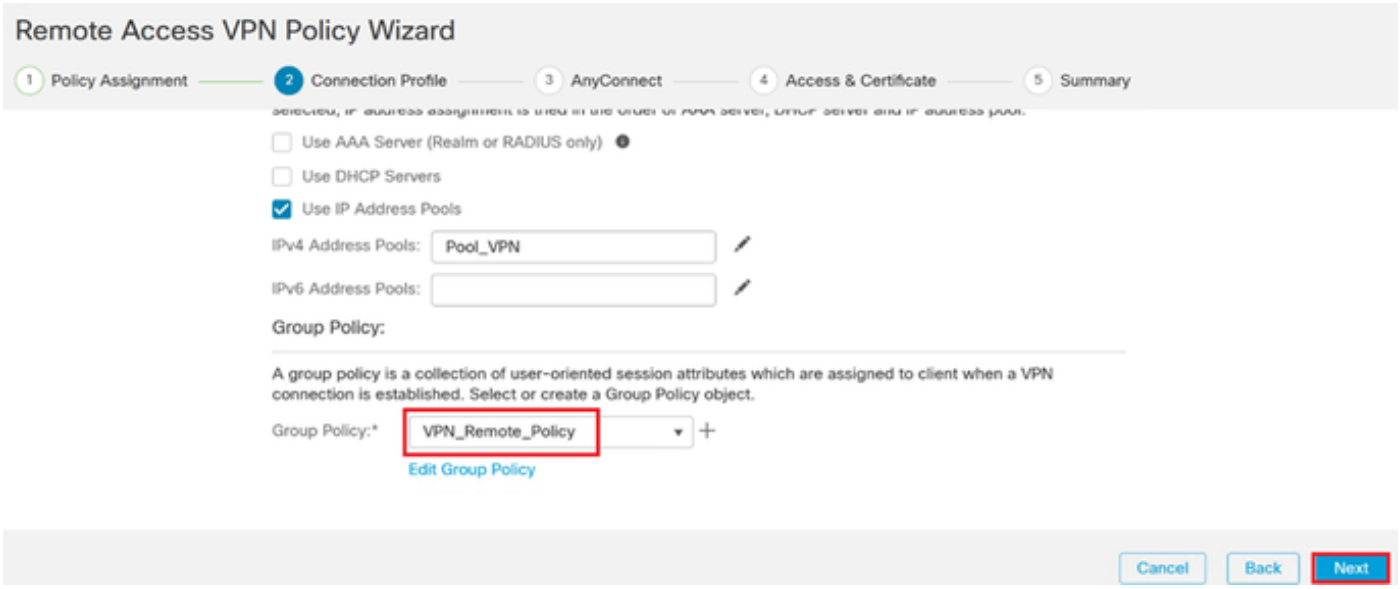

Add Group Policy
Name:*
VPN_Remote_Policy
Description:
General
AnyConnect
Advanced
VPN Protocols
IP Address Pools
Banner
DNS/WINS
Split Tunneling
Primary DNS Server:
Secondary DNS Server:
Primary WINS Server:
Secondary WINS Server:
DHCP Network Scope:
Only network object with ipv4 address is allowed (Ex: 10.72.3.5)
Default Domain:
Cancel
Save

DNS 설정.



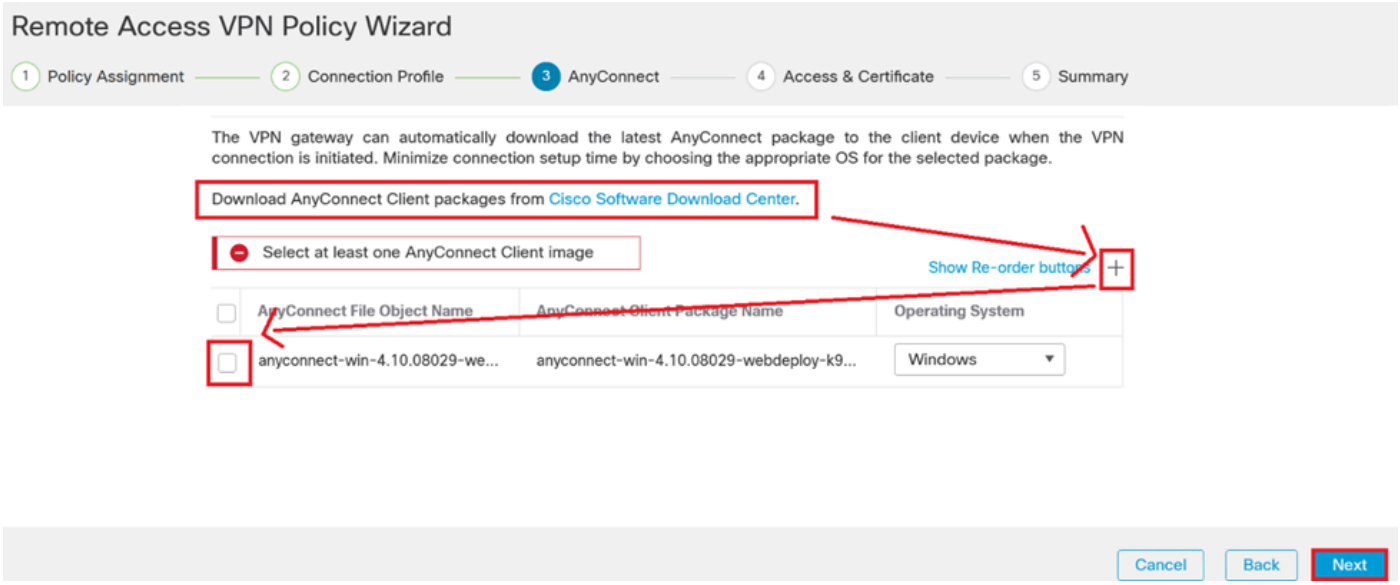
경고: 이 구성에서는 배너, 스플릿 터널링, AnyConnect 및 고급 옵션과 같은 추가 기능이 선택 사항으로 간주됩니다.

12. 필요한 세부 정보를 구성한 후 다음을 눌러 설정 다음 단계로 진행합니다.



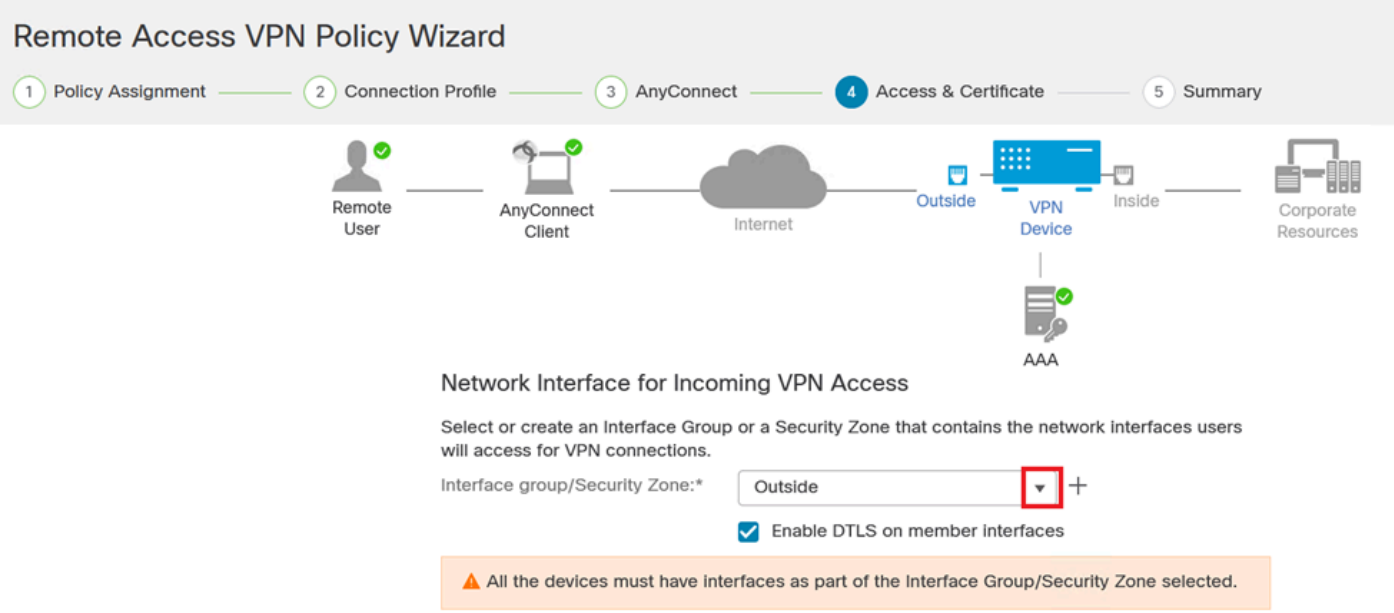
그룹 정책.

13. VPN 사용자에 적합한 AnyConnect 패키지를 선택합니다. 필요한 패키지가 목록에 없으면 이 단계에서 필요한 패키지를 추가할 수 있습니다.



패키지 설치.

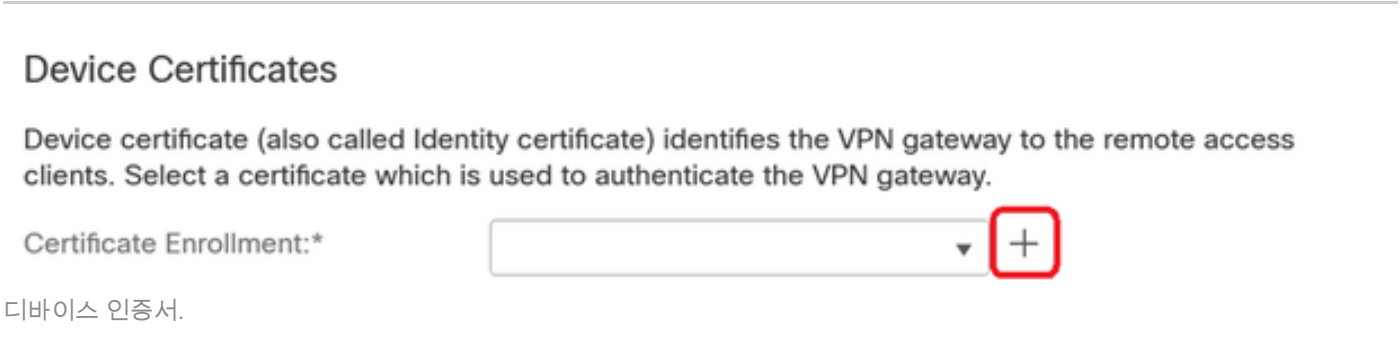
14. VPN 원격 기능을 사용할 FTD 디바이스의 네트워크 인터페이스를 선택합니다.



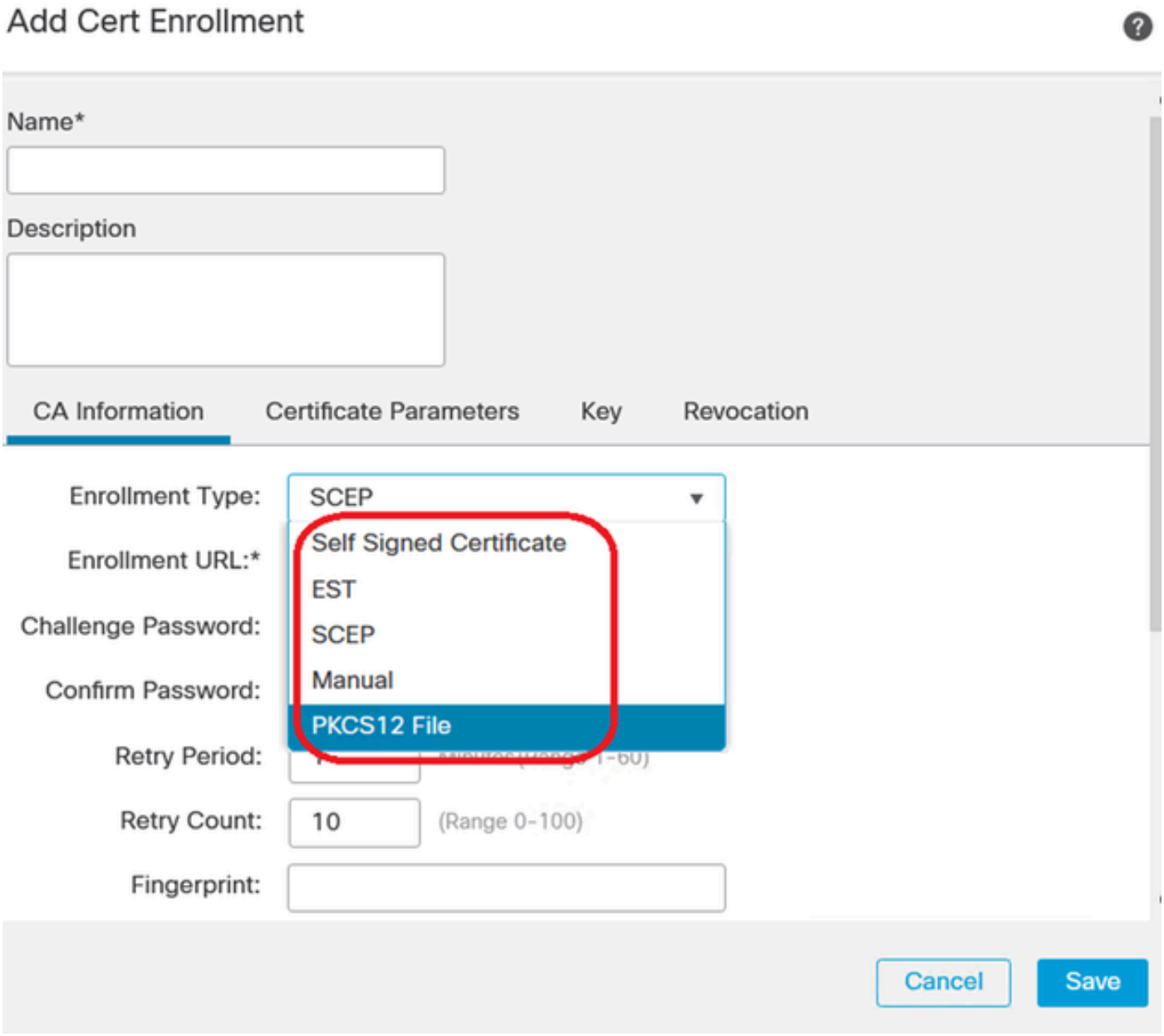
VPN 인터페이스

15. 보안 VPN 연결에 중요한 방화벽에 인증서를 만들고 설치하는 데 사용할 수 있는 방법 중 하나를 선택하여 인증서 등록 프로세스를 설정합니다.

주의: 예를 들어 이 설명서에서 자체 서명 인증서를 선택했습니다.

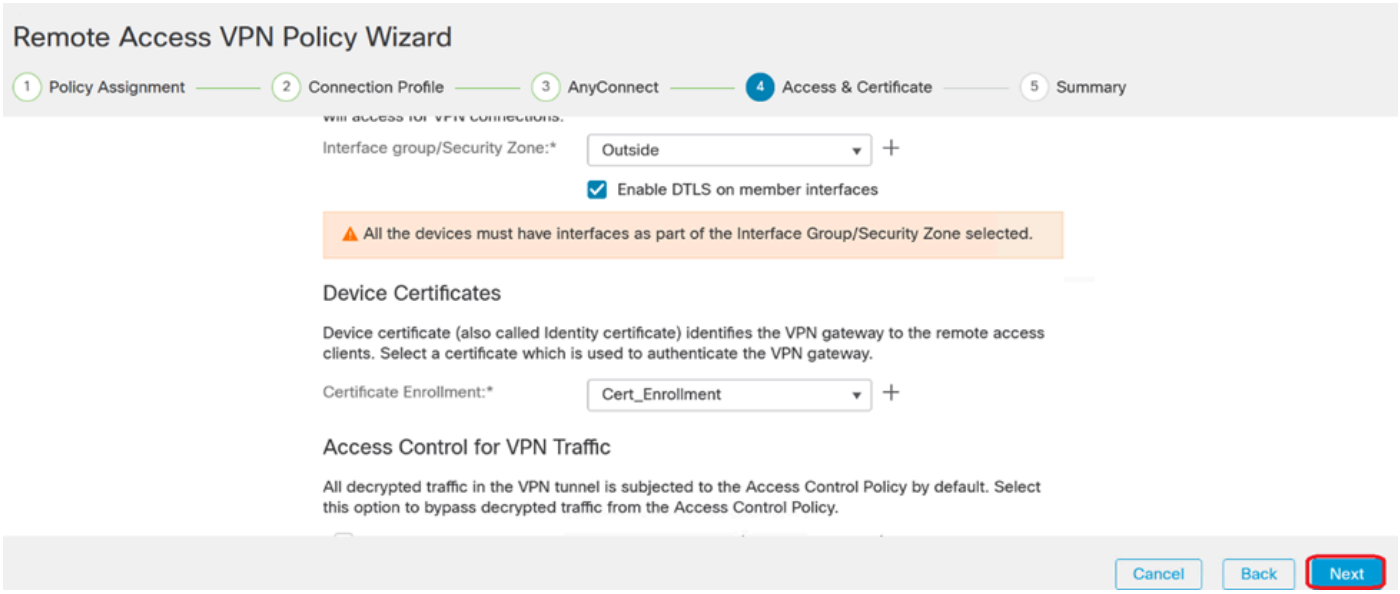


디바이스 인증서.



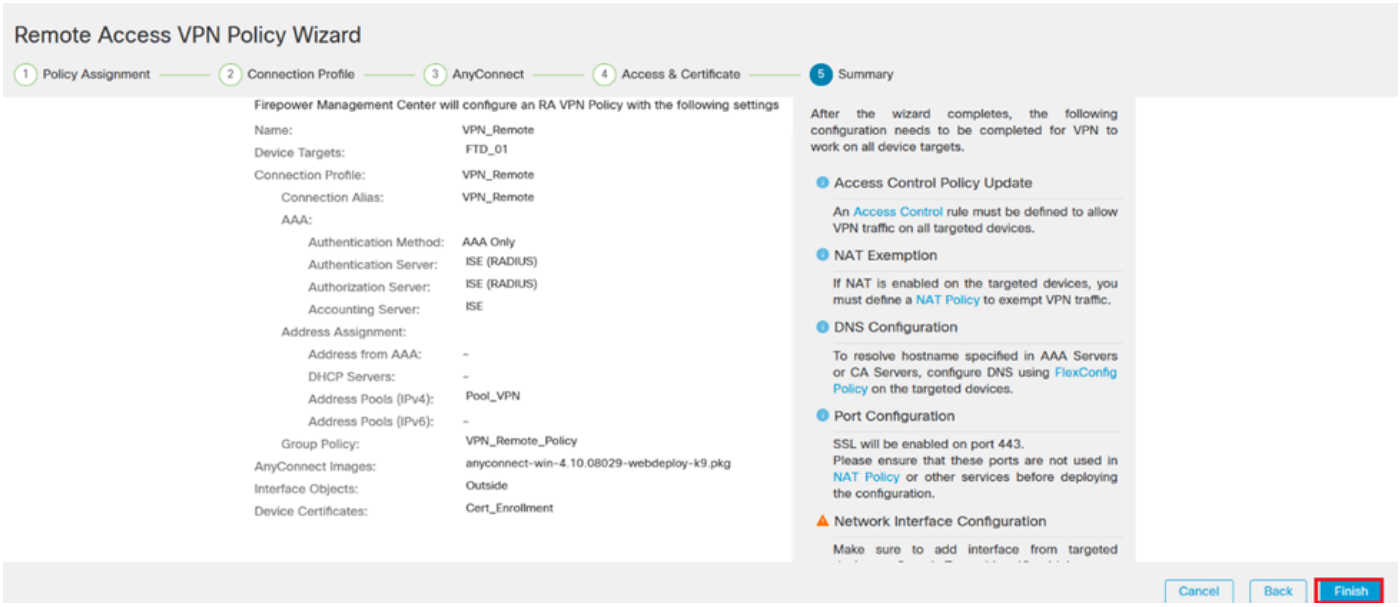
인증서 등록.

16. 인증서 등록이 구성되면 다음을 클릭합니다.



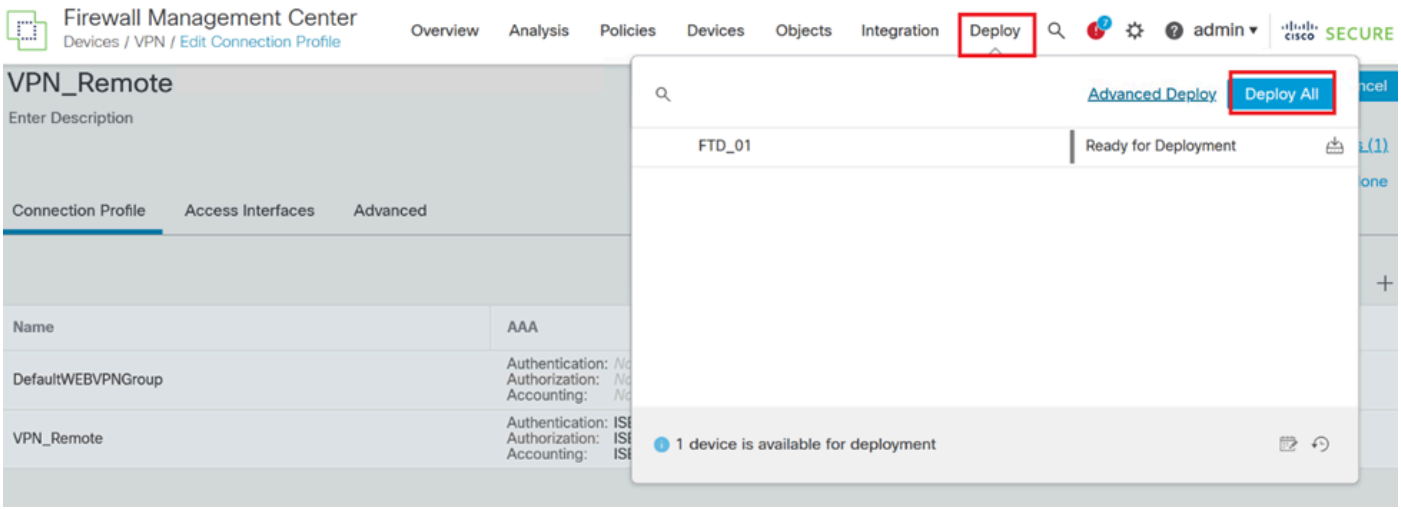
액세스 및 서비스 요약

17. 모든 구성의 요약을 검토하여 정확한지 확인하고 의도한 설정을 반영합니다.



VPN 설정 요약

18. VPN 원격 액세스 구성을 적용 및 활성화하려면 Deploy(구축) > Deploy All(모두 구축)로 이동하여 선택한 FTD 장치에 대한 구축을 실행합니다.



VPN 설정 구축.

ISE 컨피그레이션

DUO를 외부 Radius 서버로 통합합니다.

1. Cisco ISE 관리 인터페이스에서 Administration(관리) > Network Resources(네트워크 리소스) > External RADIUS Servers(외부 RADIUS 서버)로 이동합니다.

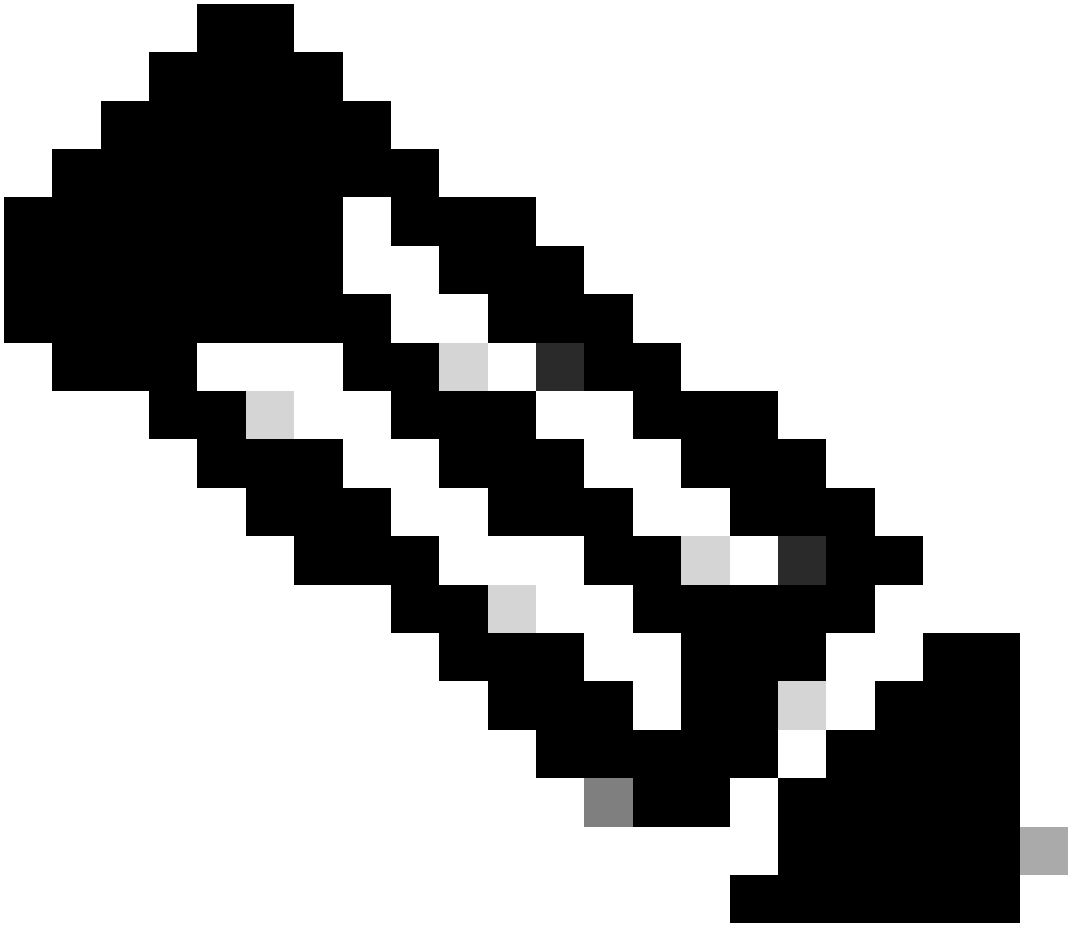
2. 새 외부 RADIUS 서버를 구성 하려면 추가 단추를 클릭 합니다.

외부 Radius 서버

3. 프록시 DUO 서버의 이름을 입력합니다.

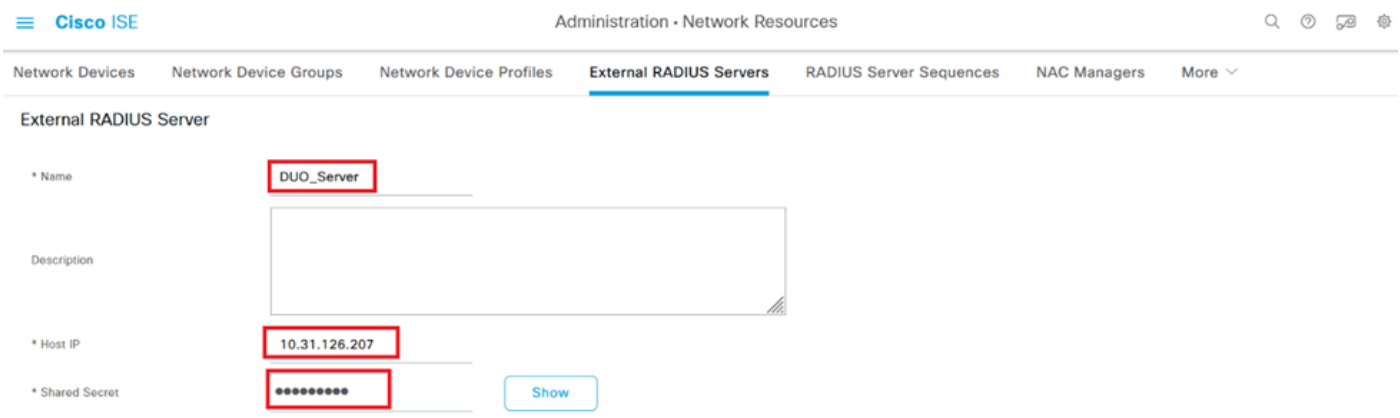
4. ISE와 DUO 서버 간의 올바른 통신을 보장하기 위해 프록시 DUO 서버에 올바른 IP 주소를 입력합니다.

5. 공유 비밀 키를 설정합니다.



참고: RADIUS 연결을 성공적으로 설정하려면 이 공유 비밀 키를 프록시 DUO 서버에 구성해야 합니다.

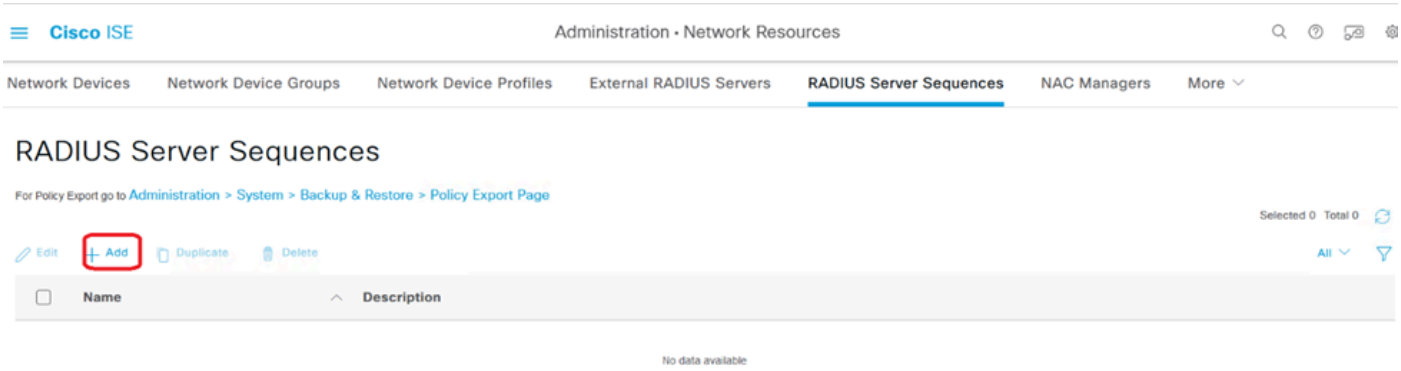
6. 모든 세부 정보를 올바르게 입력한 후 **[제출]**을 클릭하여 새 프록시 DUO 서버 구성을 저장합니다.



외부 RADIUS 서버

7. Administration(관리) > RADIUS Server Sequences(RADIUS 서버 시퀀스)로 이동합니다.

8. 새 RADIUS 서버 시퀀스를 생성하려면 Add를 클릭합니다.

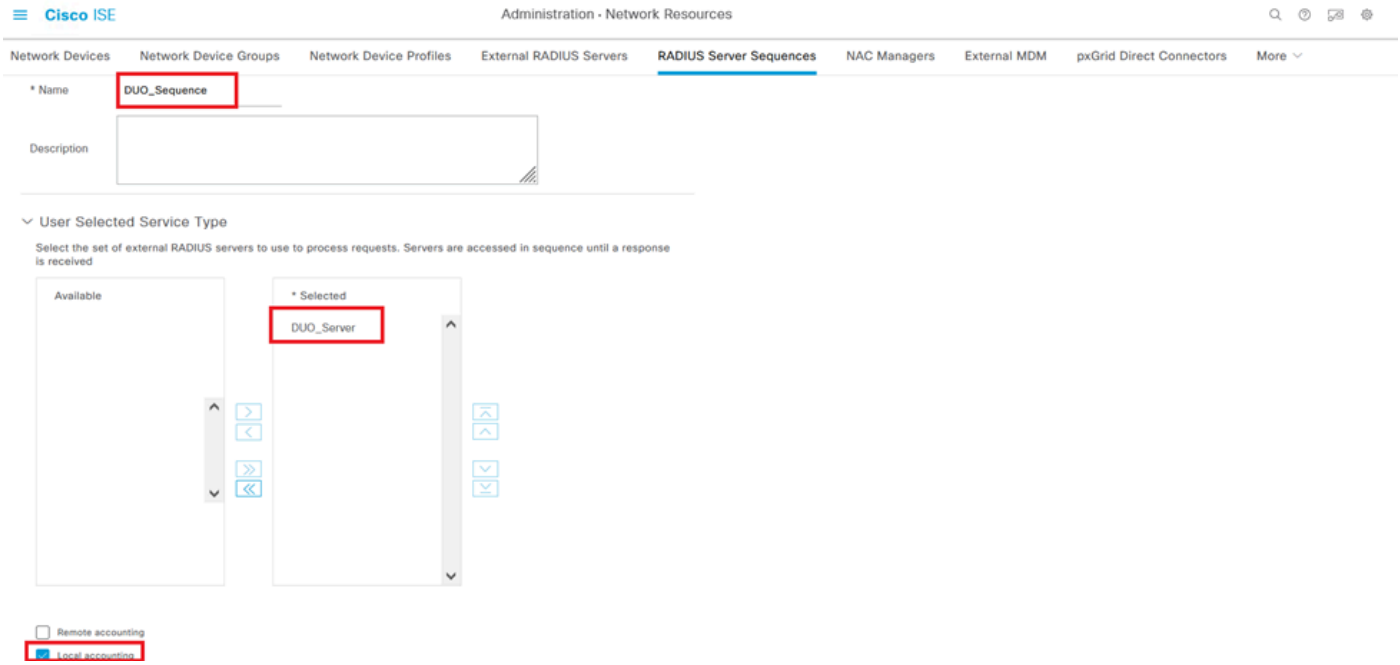


RADIUS 서버 시퀀스

9. 쉽게 식별할 수 있도록 RADIUS 서버 시퀀스의 고유한 이름을 제공합니다.

10. 이전에 구성된 DUO RADIUS 서버(이 가이드에서 DUO_Server라고 함)를 찾아 오른쪽의 선택한 목록으로 이동하여 시퀀스에 포함합니다.

11. Submit(제출)을 클릭하여 RADIUS 서버 시퀀스 구성을 마무리하고 저장합니다.

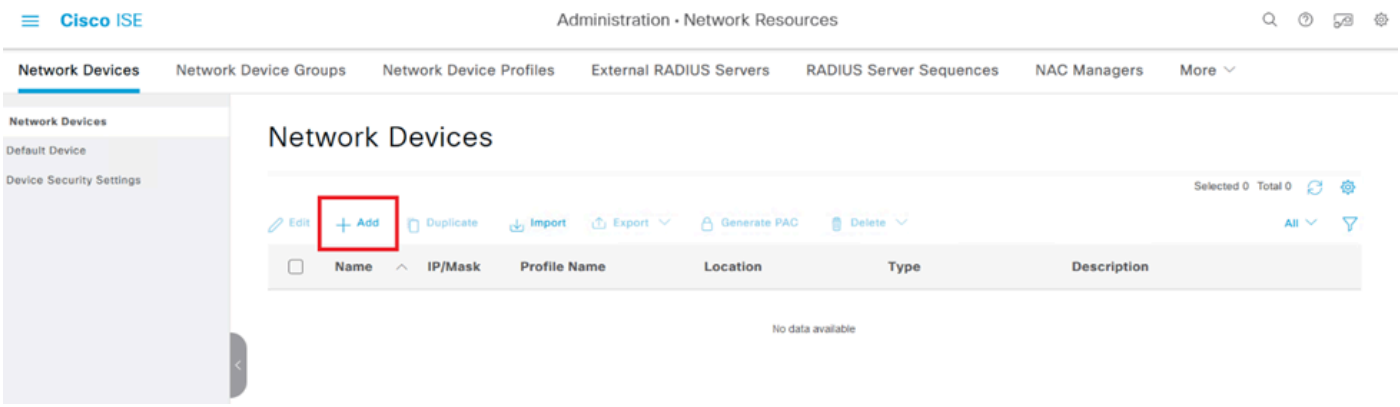


Radius 서버 시퀀스 컨피그레이션입니다.

FTD를 네트워크 액세스 디바이스로 통합합니다.

1. 시스템 인터페이스의 Administration(관리) 섹션으로 이동한 다음 Network Resources(네트워크 리소스)를 선택하여 네트워크 디바이스의 컨피그레이션 영역에 액세스합니다.

2. Network Resources(네트워크 리소스) 섹션에서 Add(추가) 버튼을 클릭하여 새 네트워크 액세스 디바이스를 추가하는 프로세스를 시작합니다.



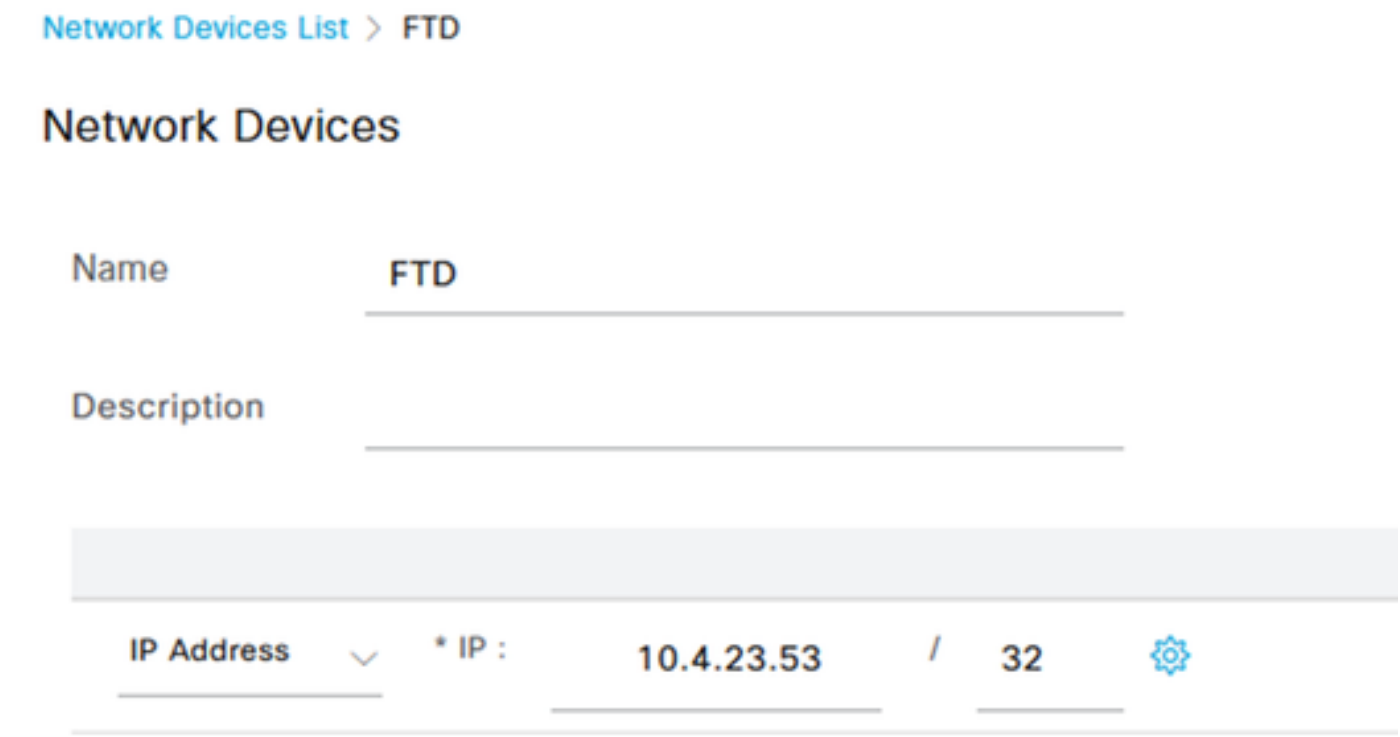
네트워크 액세스 디바이스.

3. 제공된 필드에 네트워크 액세스 장치 이름을 입력하여 네트워크 내의 장치를 식별합니다.

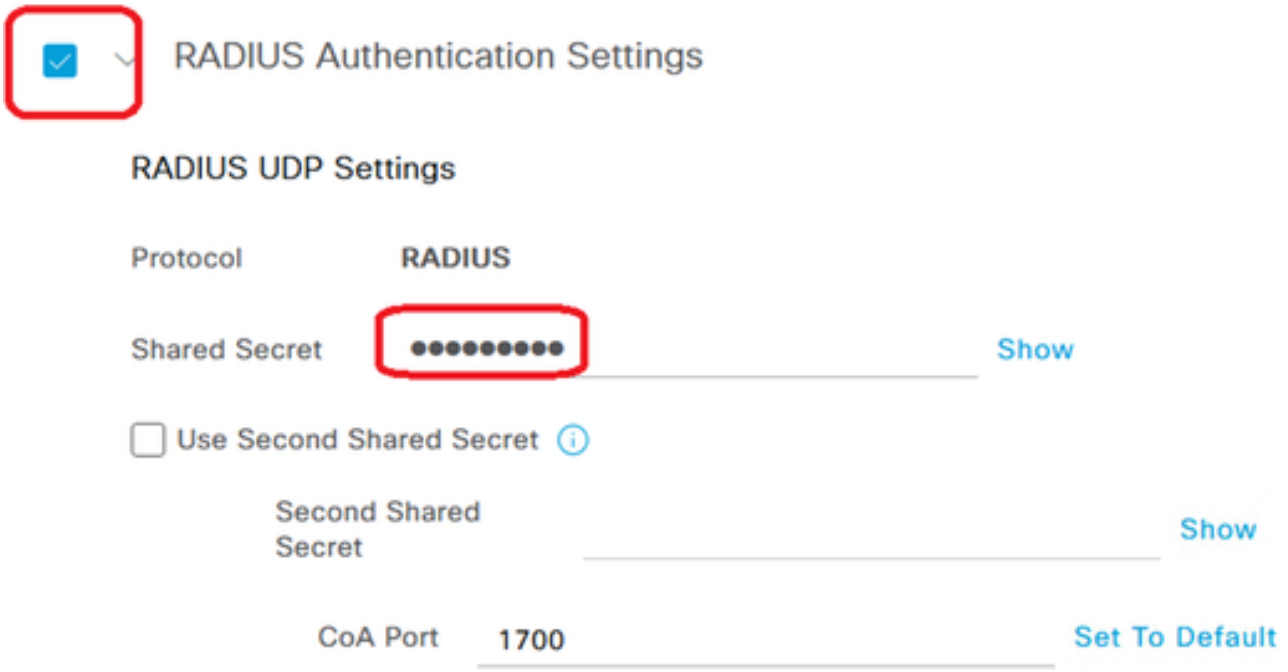
4. FTD(Firepower Threat Defense) 디바이스의 IP 주소를 지정합니다.

5. FMC(Firepower 관리 센터) 설정 중에 이전에 설정했던 키를 입력합니다. 이 키는 장치 간의 보안 통신에 필수적입니다.

6. 제출 버튼을 클릭하여 프로세스를 완료합니다.



FTD를 NAD로 추가



RADIUS 설정

DUO 구성.

DUO 프록시 설치.

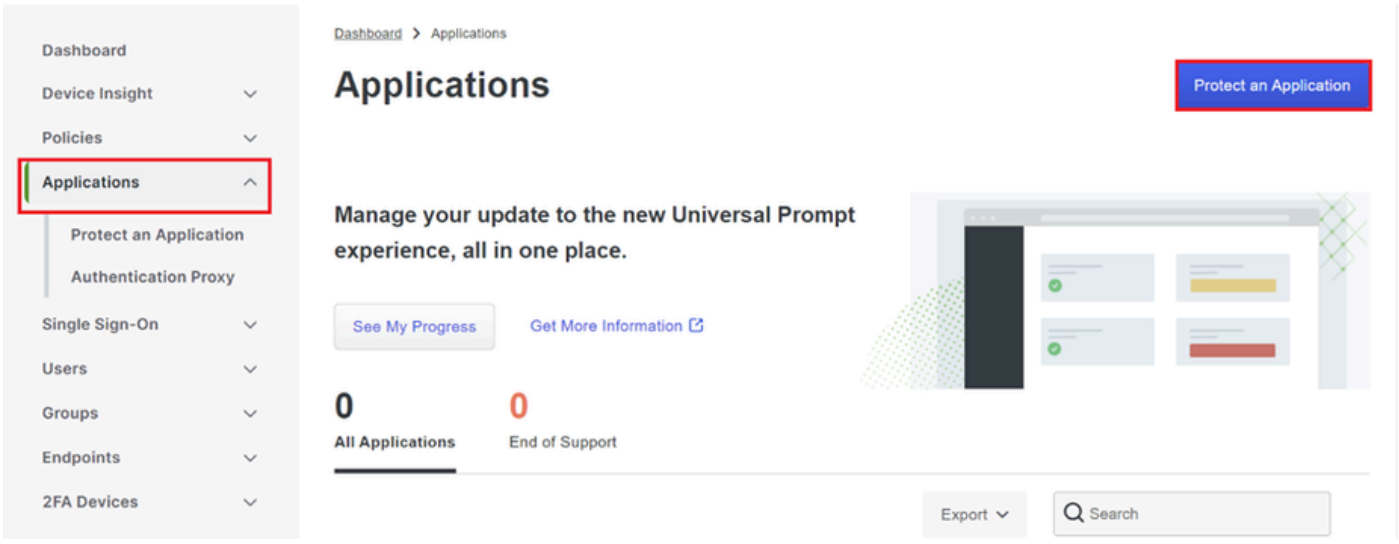
다음 링크를 클릭하여 DUO Proxy Download and Installation Guide에 액세스합니다.

https://duo.com/docs/authproxy-reference

DUO Proxy를 ISE 및 DUO Cloud와 통합합니다.

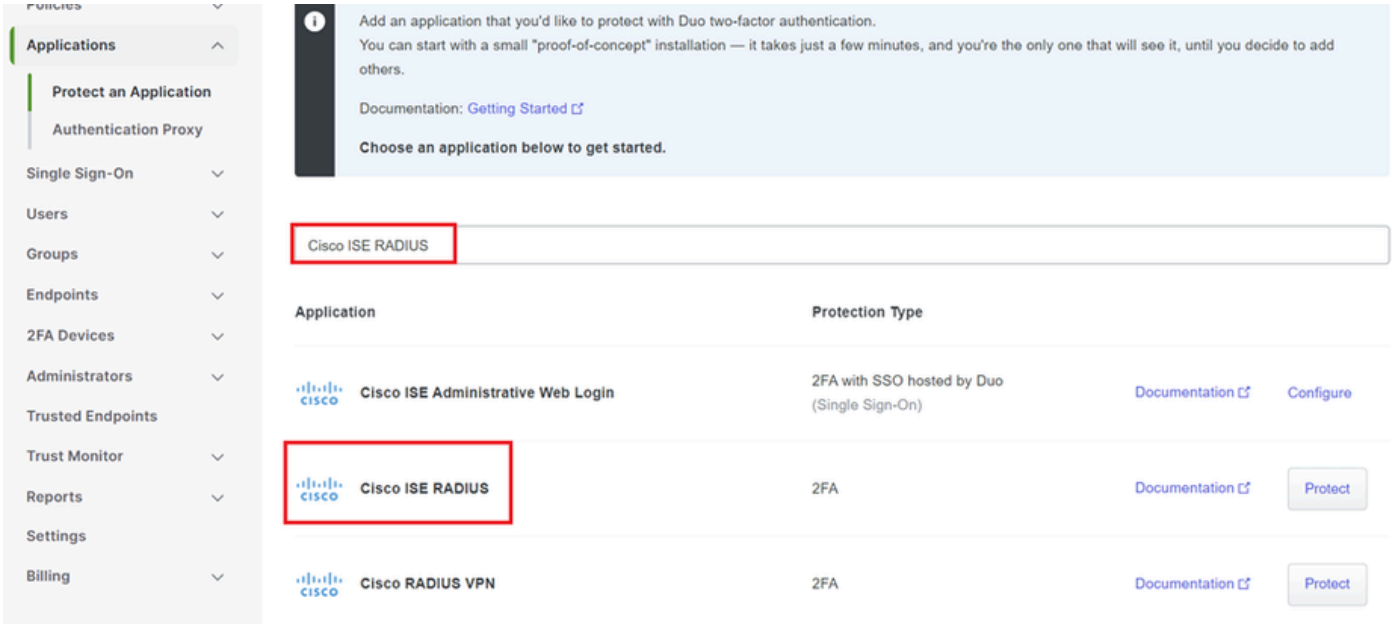
1. DUO 보안 웹 사이트(https://duo.com/)에 자격 증명을 사용하여 로그인합니다.

2. 애플리케이션 섹션으로 이동하여 계속하려면 애플리케이션 보호를 선택합니다.



DUO 애플리케이션

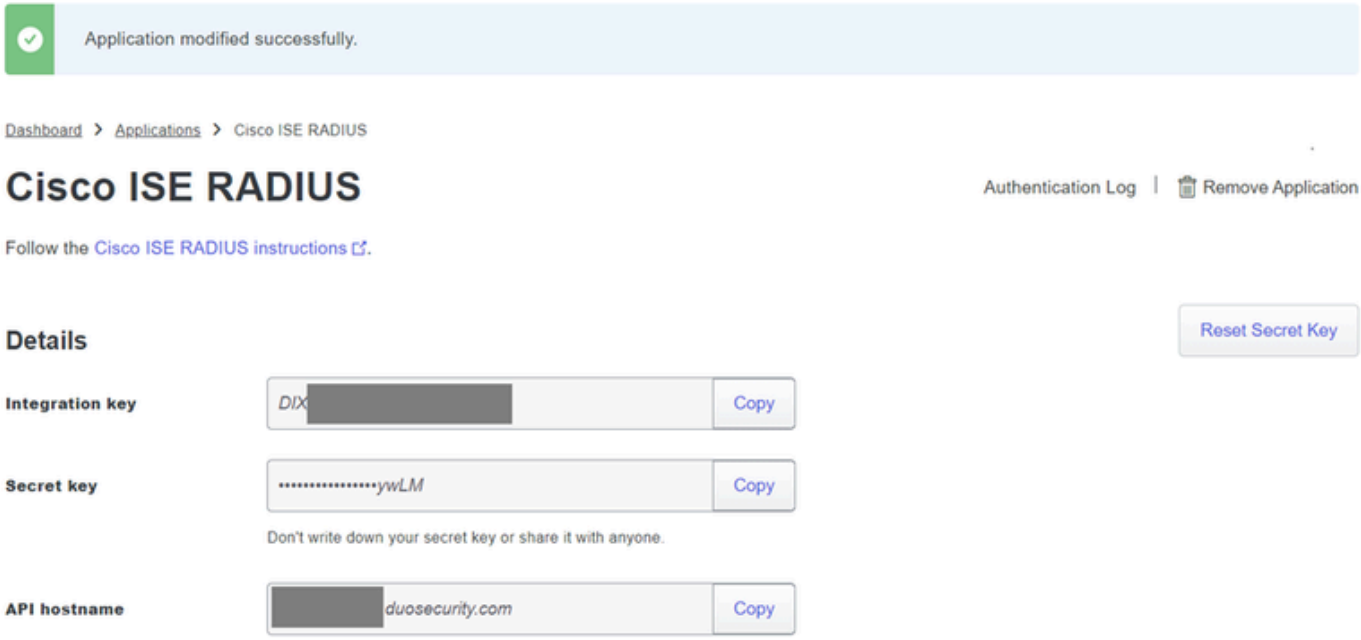
3. 목록에서 "Cisco ISE RADIUS" 옵션을 검색하고 보호를 클릭하여 애플리케이션에 추가합니다.



ISE RADIUS 옵션

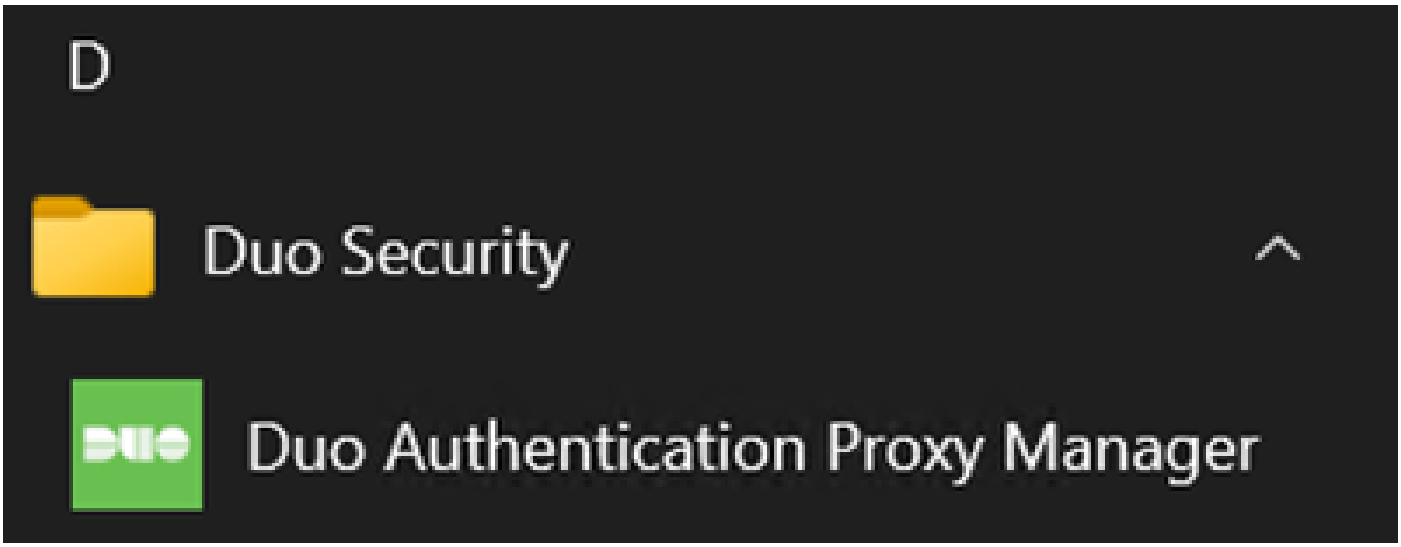
4. 성공적으로 추가되면 DUO 애플리케이션의 세부사항을 확인할 수 있습니다. 아래로 스크롤하고 Save(저장)를 클릭합니다.

5. 제공된 통합 키, 비밀 키 및 API 호스트 이름을 복사합니다. 이는 향후 단계에서 매우 중요합니다.



ISE 서버 세부 정보

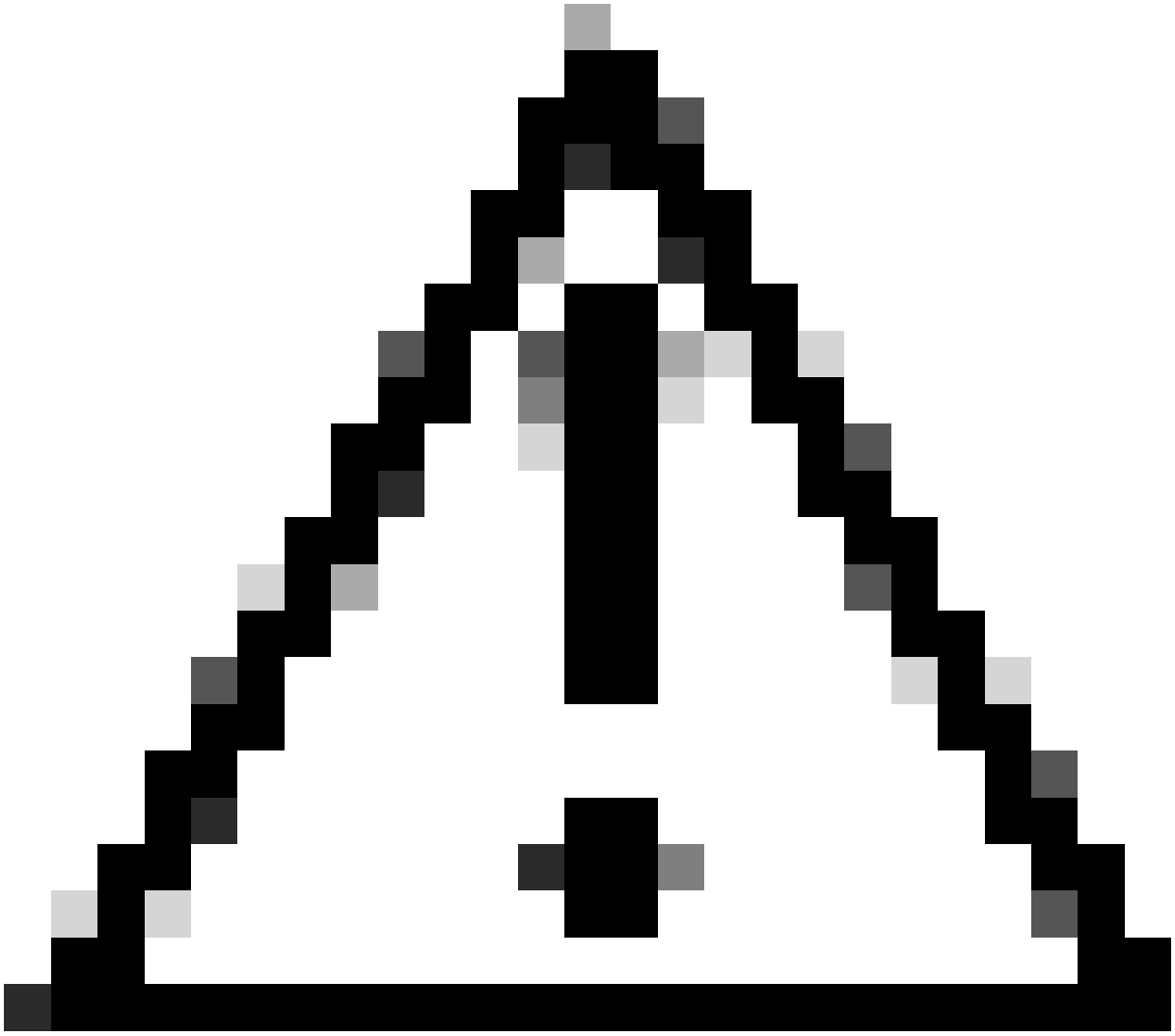
6. 시스템에서 DUO Proxy Manager를 실행하여 설정을 계속합니다.



DUO 프록시 관리자

7. (선택 사항) DUO 프록시 서버에서 DUO 클라우드에 연결하기 위해 프록시 컨피그레이션이 필요한 경우 다음 매개변수를 입력합니다.

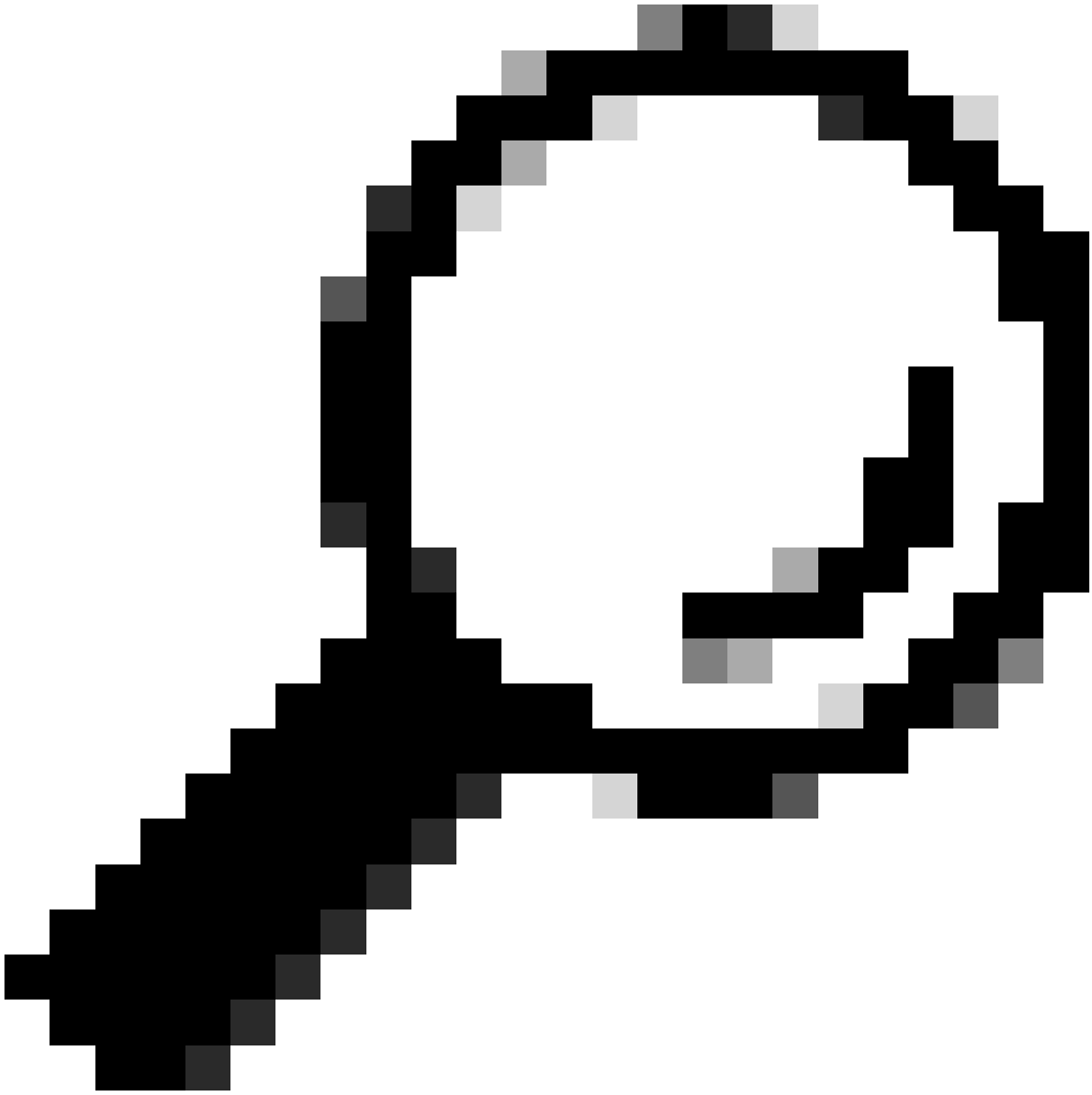
```
[main]
http_proxy_host=<Proxy IP Address or FQDN >
http_proxy_port=<port>
```



주의: 및 을(를) 실제 프록시 세부사항으로 교체해야 합니다.

8. 이제 이전에 복사한 정보를 사용하여 통합 구성을 완료합니다.

```
[radius_server_auto]
ikey=<integration key>
skey=<secret key>
api_host=<API hostname>
radius_ip_1=<ISE IP address>
radius_secret_1=<secret key configured in the external RADIUS server section>
failmode=safe
port=1812
client=ad_client
```



팁: client=ad_client 행은 DUO 프록시가 Active Directory 계정을 사용하여 인증함을 나타냅니다. Active Directory와의 동기화를 완료하려면 이 정보가 올바른지 확인하십시오.

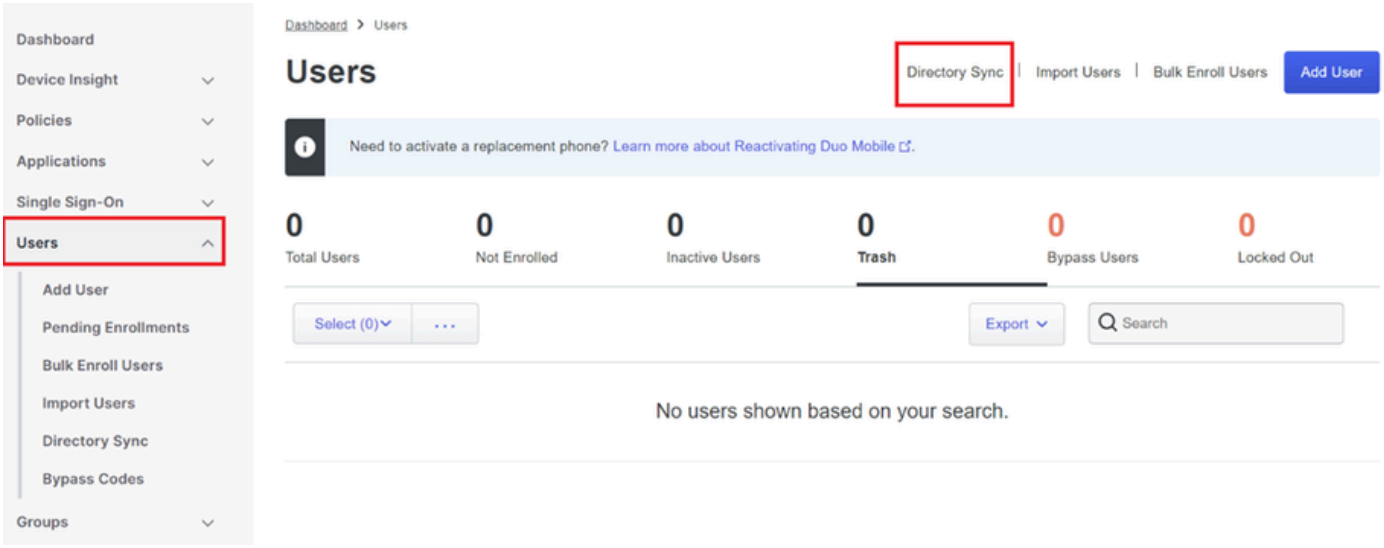
DUO를 Active Directory와 통합합니다.

1. DUO 인증 프록시를 Active Directory와 통합합니다.

```
[ad_client]
host=<AD IP Address>
service_account_username=<service_account_username>
service_account_password=<service_account_password>
search_dn=DC=<domain>,DC=<TLD>
```

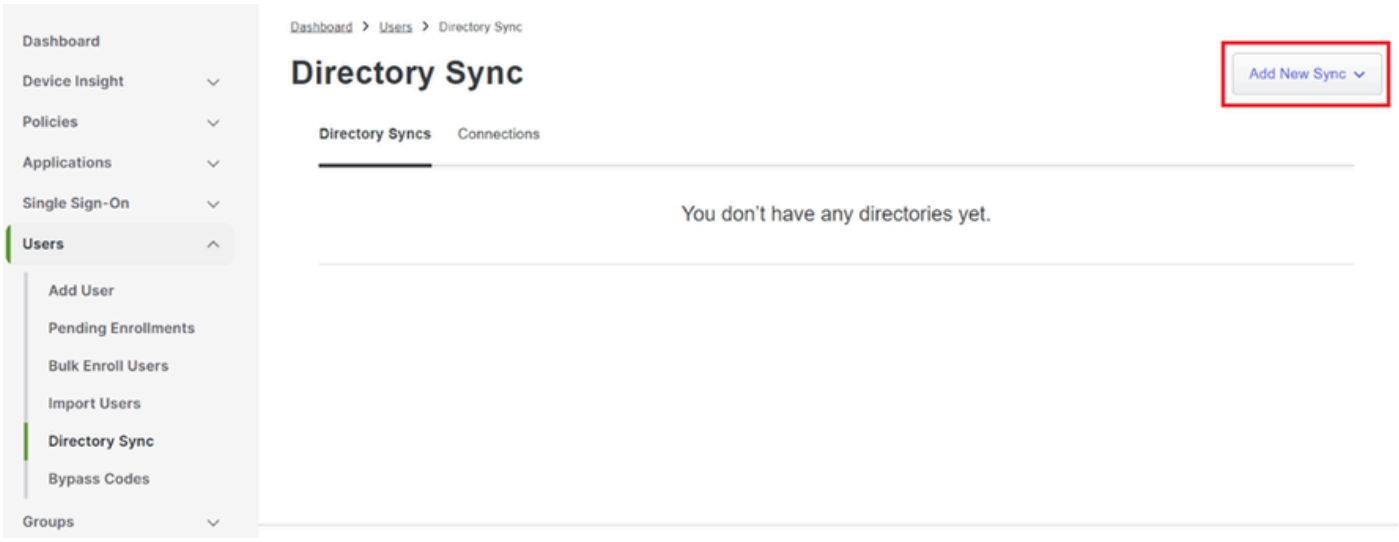
2. DUO 클라우드 서비스로 Active Directory에 가입합니다. https://duo.com/에 로그인합니다.

3. "사용자"로 이동하고 "디렉터리 동기화"를 선택하여 동기화 설정을 관리합니다.



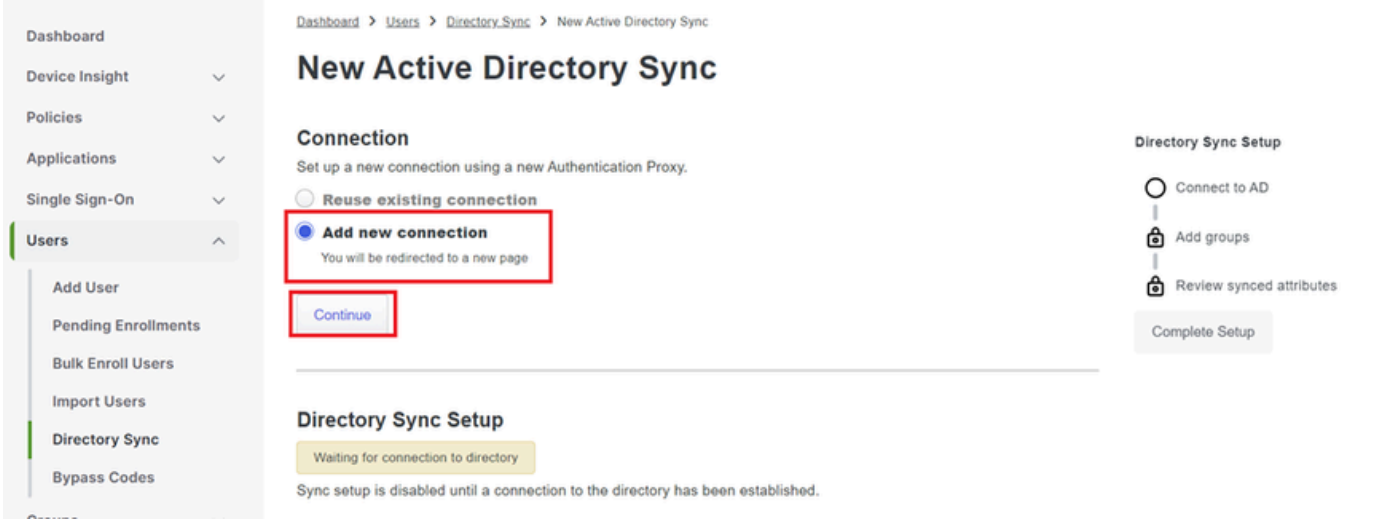
디렉터리 동기화

4. "새 동기화 추가"를 클릭하고 제공된 옵션에서 "Active Directory"를 선택합니다.



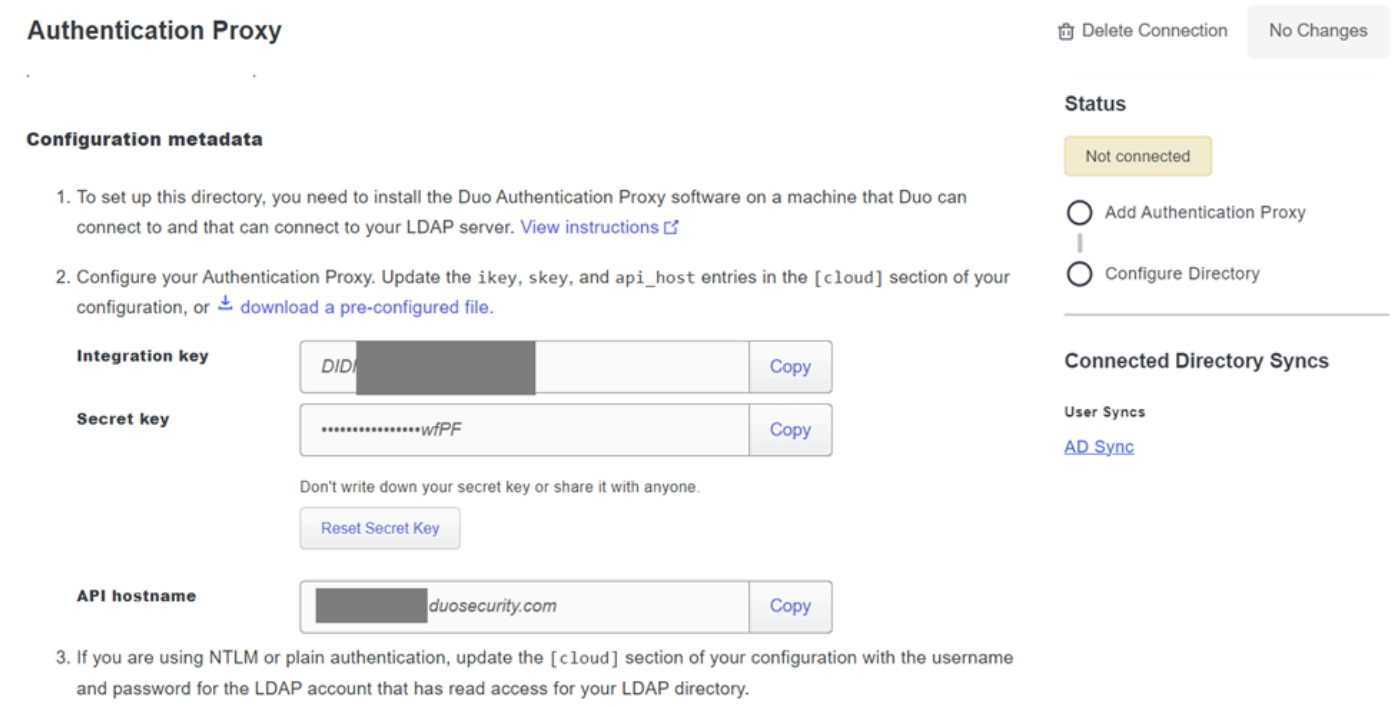
새 동기화 추가

5. [새 연결 추가]를 선택하고 [계속]을 클릭합니다.



새 *Active Directory* 추가

6. 생성된 통합 키, 비밀 키 및 API 호스트 이름을 복사합니다.

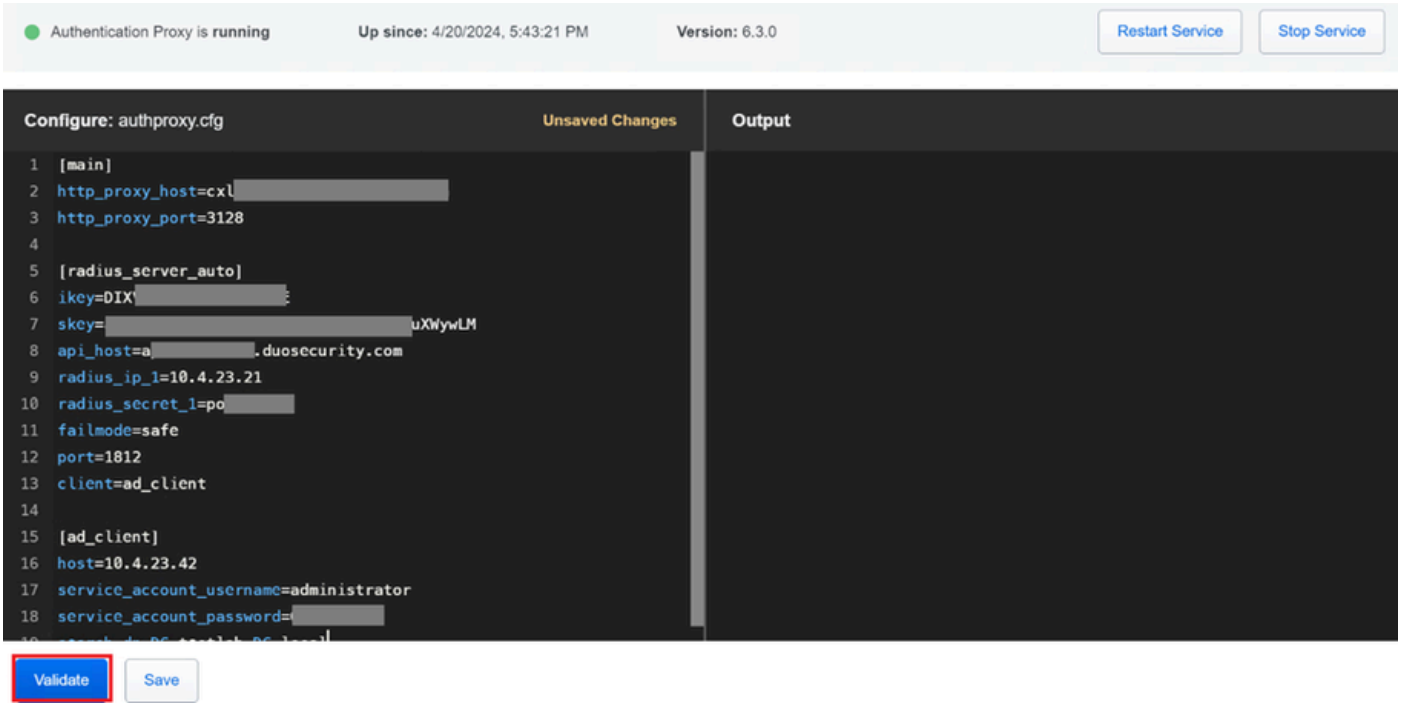


인증 프록시 세부 정보

7. DUO 인증 프록시 컨피그레이션으로 돌아가 [cloud](클라우드) 섹션을 새 매개변수와 Active Directory 관리자를 위한 서비스 계정 자격 증명으로 구성합니다.

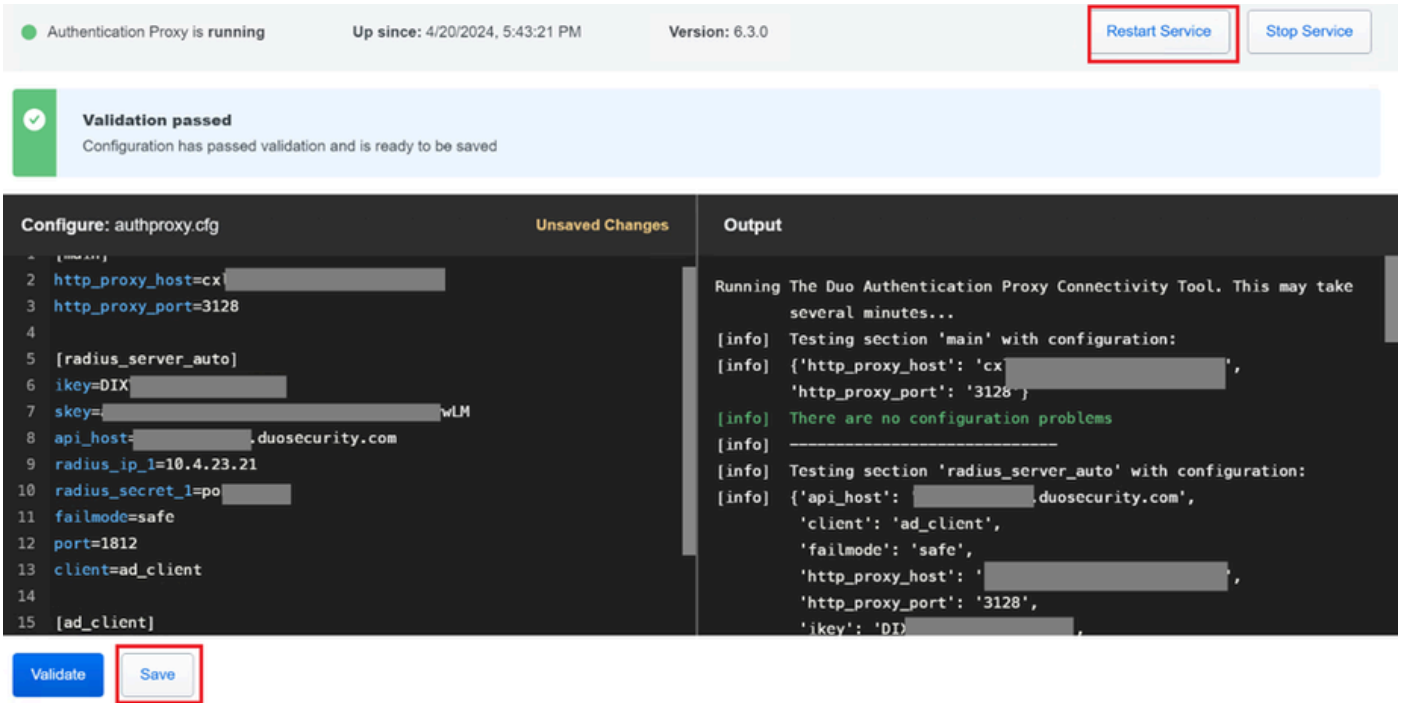
```
[cloud]
ikey=<integration key>
skey=<secret key>
api_host=<API hostname>
service_account_username=<your domain>\<service_account_username>
service_account_password=<service_account_password>
```

8. 모든 설정이 올바른지 확인하려면 "검증" 옵션을 선택하여 구성을 검증합니다.



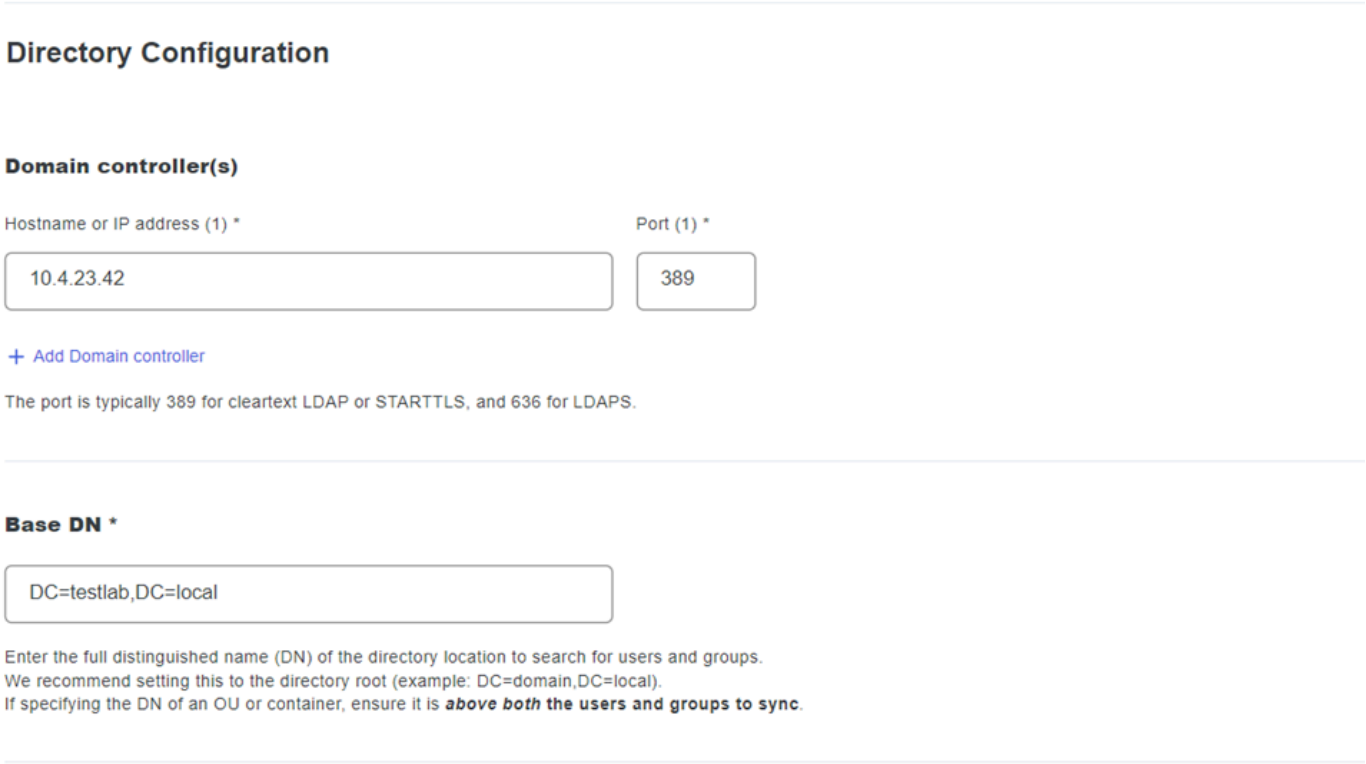
프록시 *DUO* 컨피그레이션

9. 확인 후 컨피그레이션을 저장하고 DUO 인증 프록시 서비스를 다시 시작하여 변경 사항을 적용합니다.



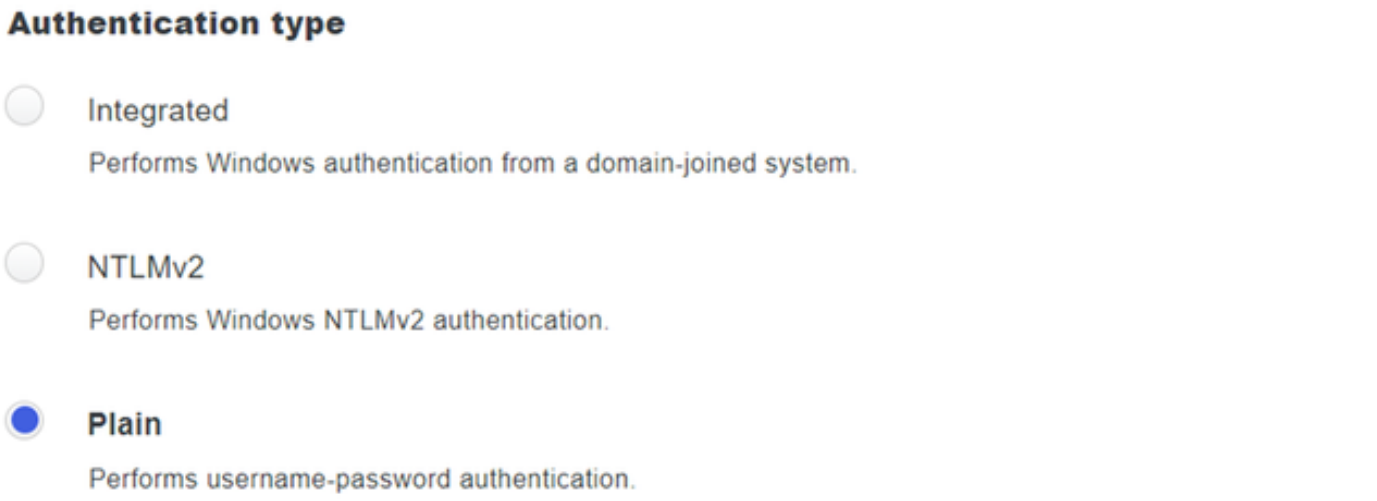
Restart Service(서비스 재시작) 옵션

10. 다시 DUO 관리 대시보드에서 Active Directory 서버의 IP 주소와 사용자 동기화를 위한 기본 DN을 입력합니다.



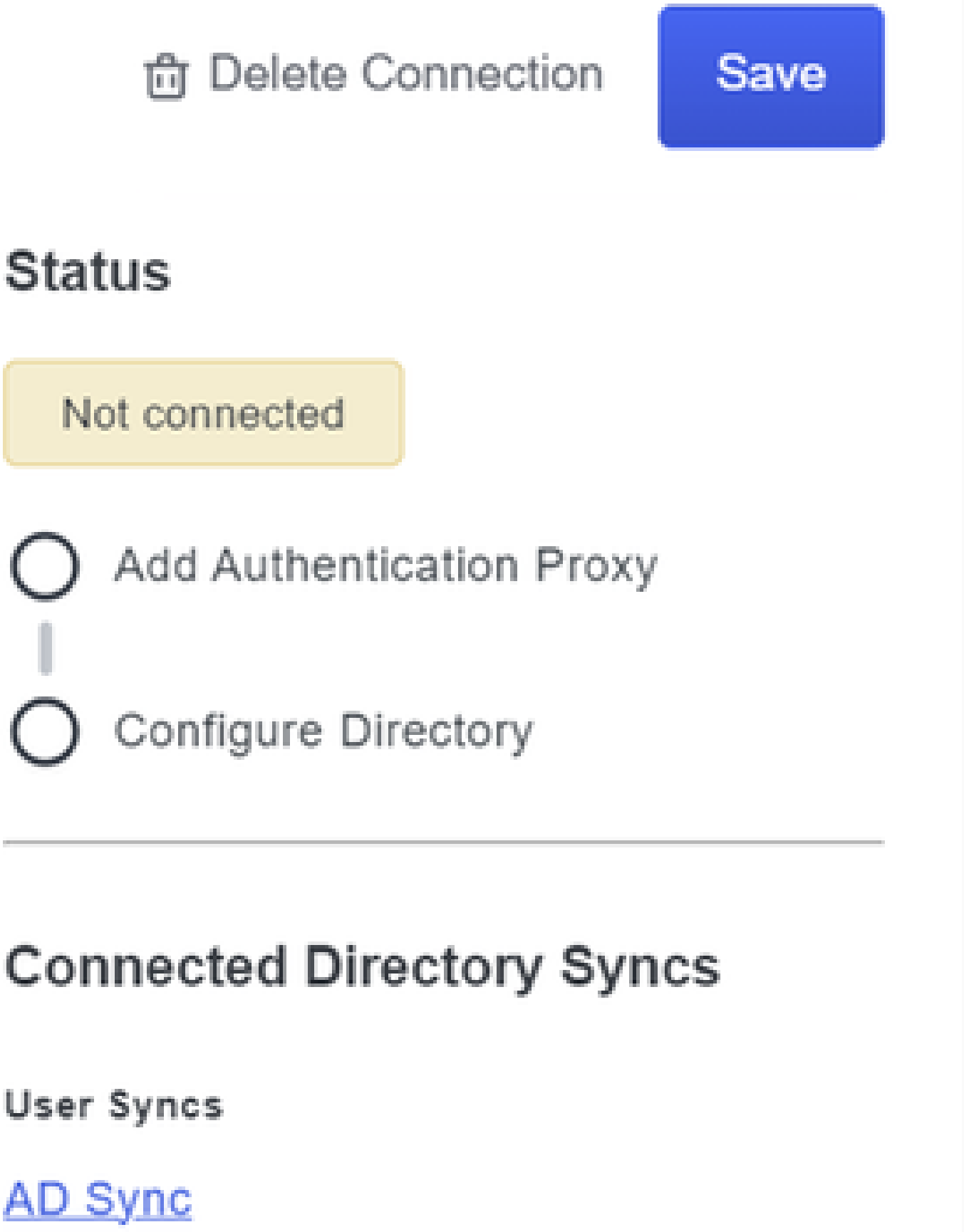
디렉터리 설정

11. 비 NTLMv2 인증을 위해 시스템을 구성하려면 Plain 옵션을 선택합니다.



인증 유형.

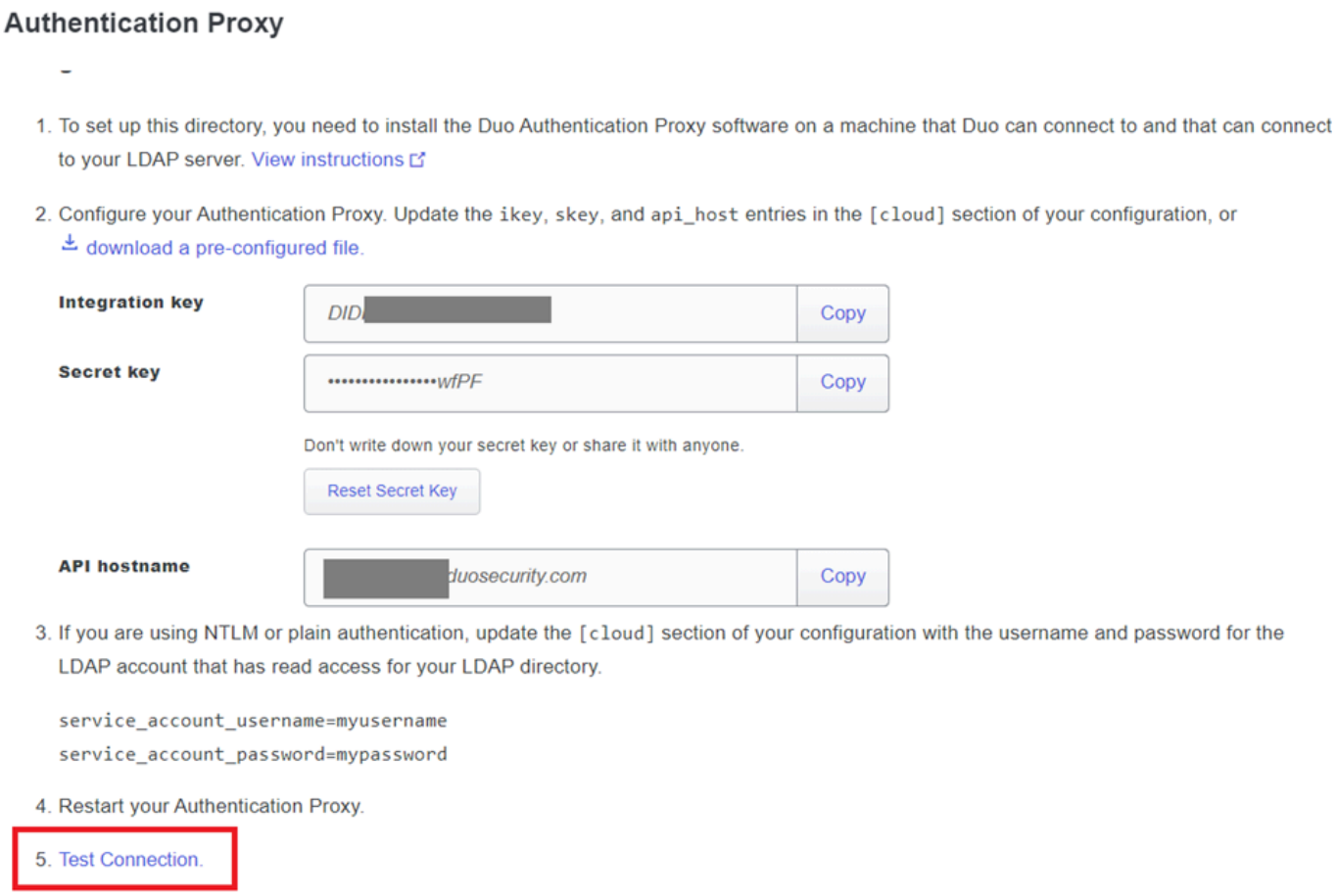
12. 구성이 업데이트되도록 새 설정을 저장합니다.



저장 옵션

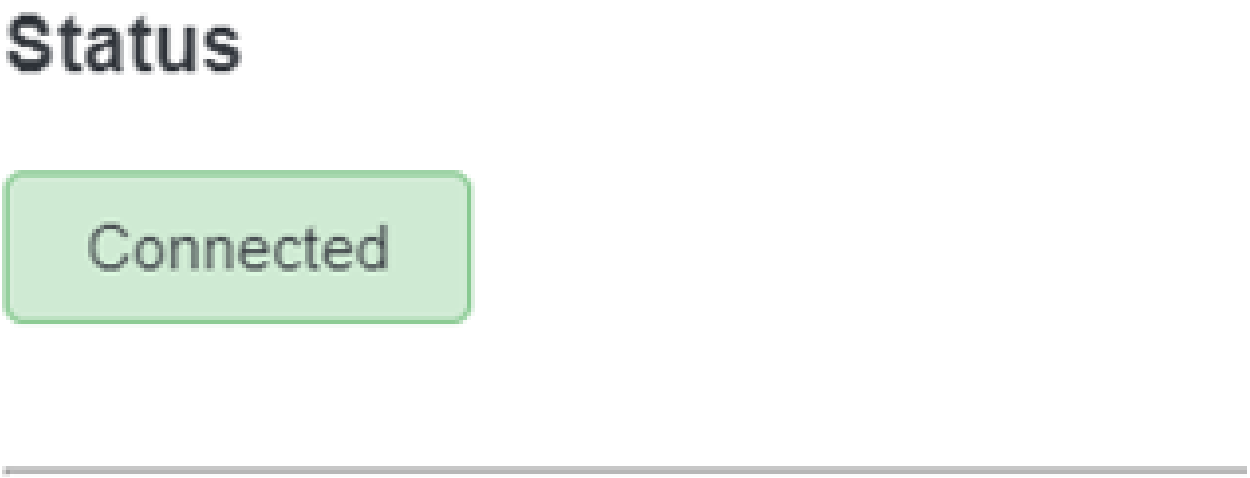
13. "연결 테스트" 기능을 사용하여 DUO 클라우드 서비스가 Active Directory와 통신할 수 있는지

확인합니다.



연결 옵션 테스트

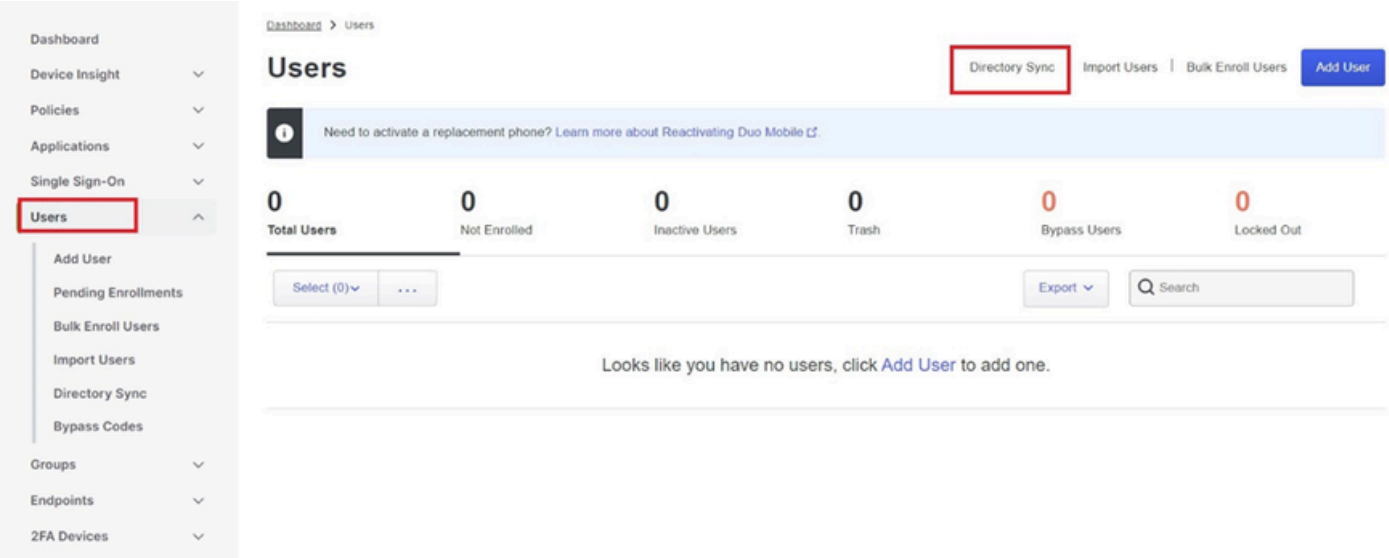
14. Active Directory 상태가 "Connected"로 표시되는지 확인합니다.



상태가 성공했습니다.

DUO Cloud를 통해 AD(Active Directory)에서 사용자 계정을 내보냅니다.

1. Duo Admin Panel(듀오 관리자 패널)에서 Users(사용자) > Directory Sync(디렉토리 동기화)로 이동하여 Active Directory와의 디렉토리 동기화와 관련된 설정을 찾습니다.

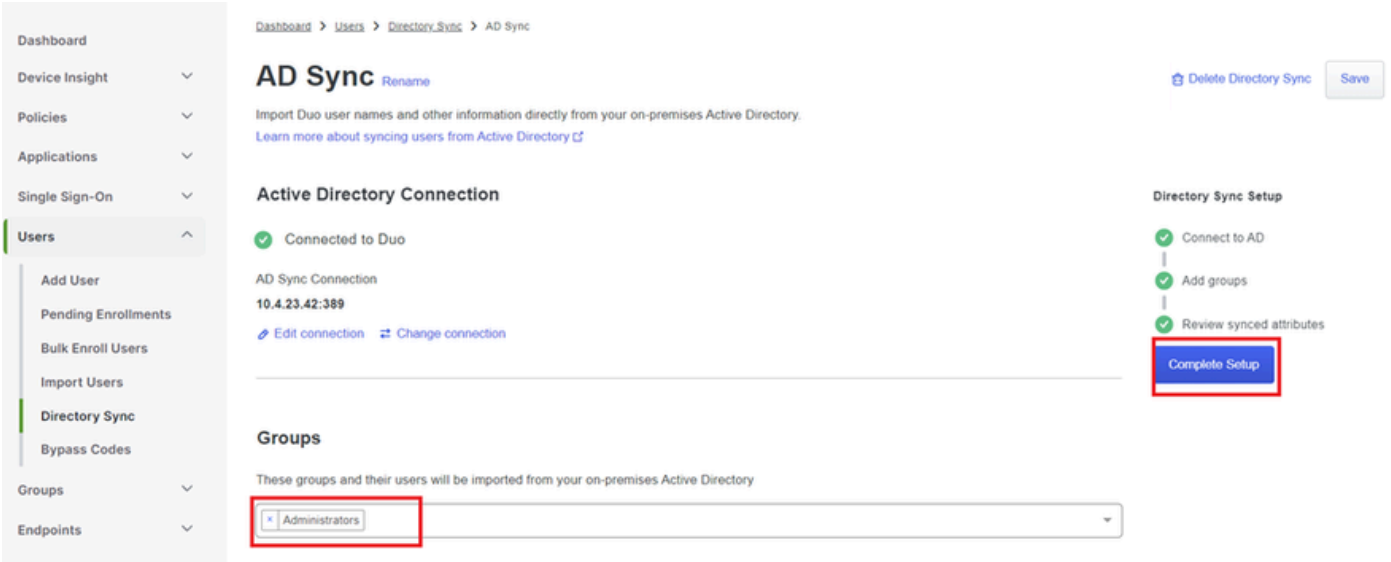


사용자 목록.

2. 관리할 Active Directory 구성을 선택합니다.

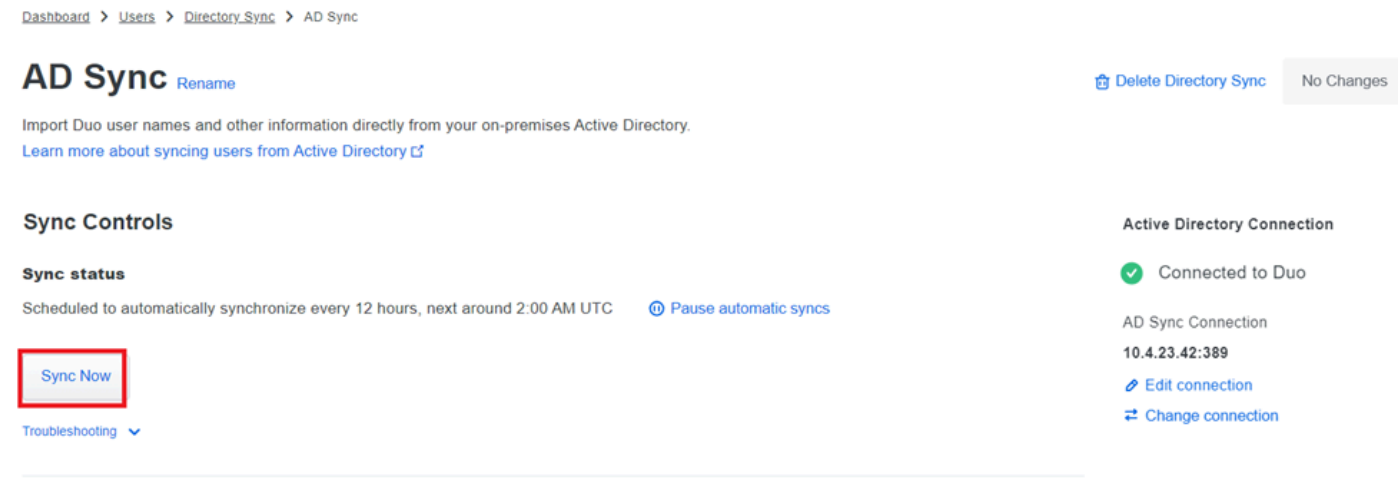
3. 컨피그레이션 설정에서 Active Directory 내에서 Duo 클라우드와 동기화할 특정 그룹을 식별하고 선택합니다. 선택 항목에 대해 필터링 옵션을 사용하는 것이 좋습니다.

4. 설정 완료를 클릭합니다.



AD 동기화

5. 즉시 동기화를 시작하려면 [지금 동기화]를 클릭합니다. 이렇게 하면 Active Directory의 지정된 그룹에서 Duo Cloud로 사용자 계정을 내보내므로 Duo Security 환경 내에서 관리할 수 있습니다.



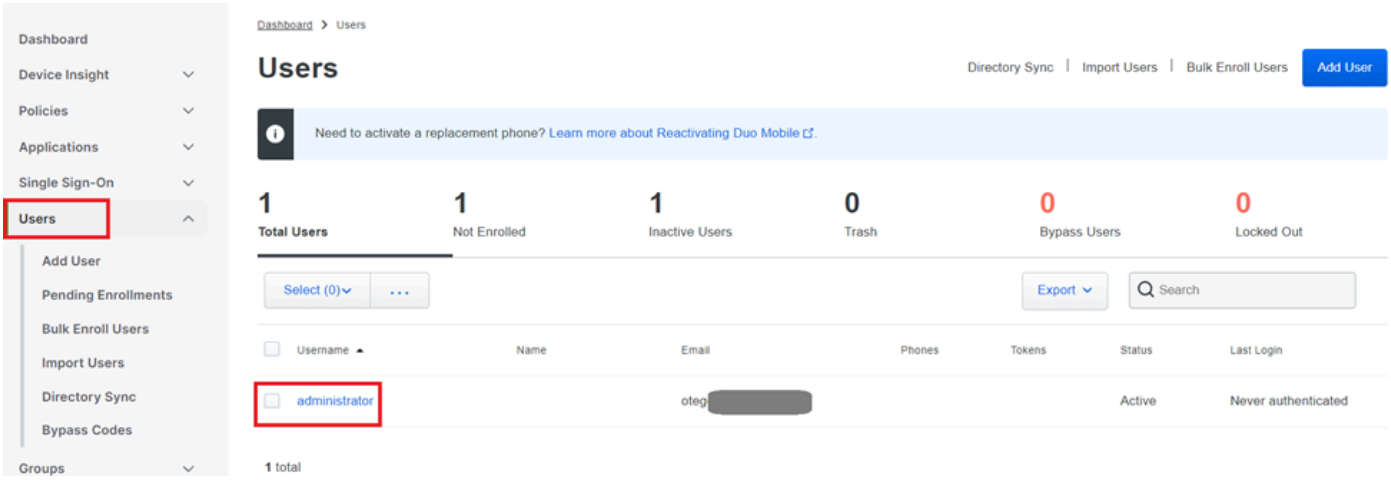
동기화 시작

Cisco DUO 클라우드에 사용자를 등록합니다.

사용자 등록은 코드 액세스, DUO 푸시, SMS 코드, 토큰 등 다양한 방법을 통해 신원 확인이 가능하다.

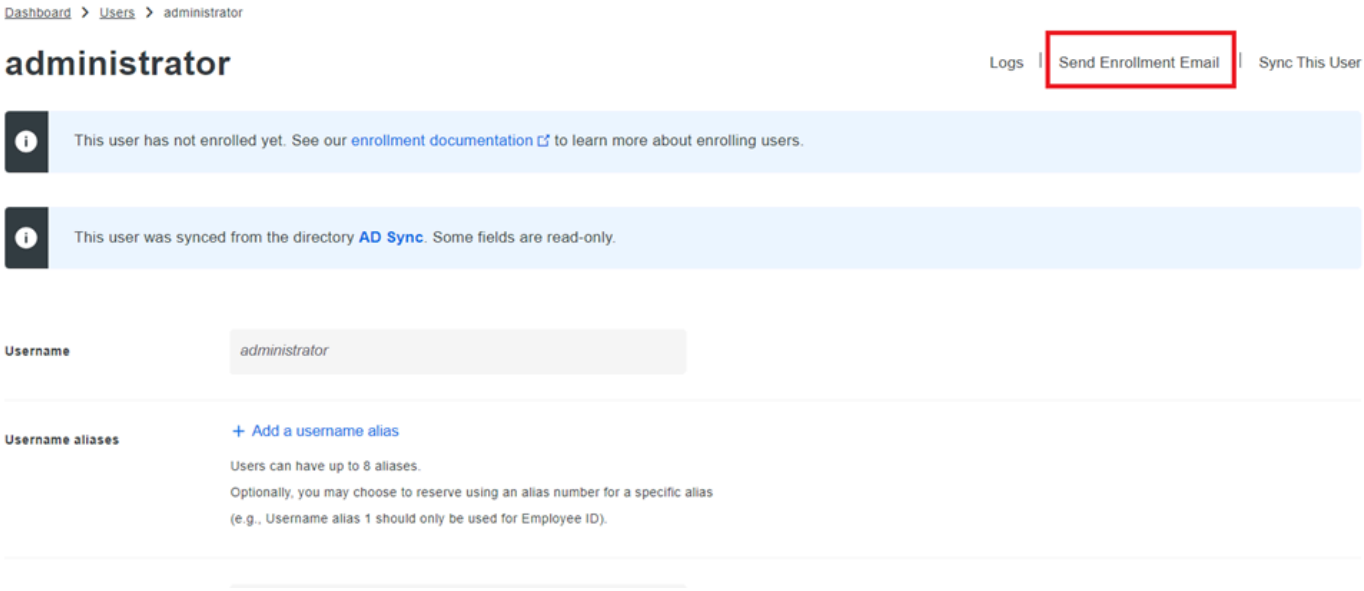
1. Cisco Cloud 대시보드에서 사용자 섹션으로 이동합니다.

2. 등록할 사용자의 계정을 찾아 선택합니다.



사용자 계정 목록

3. 등록 프로세스를 시작하려면 등록 전자 메일 발송 버튼을 클릭합니다.



이메일을 통한 등록

4. 전자 메일 받은 편지함을 확인하고 등록 초대를 열어 인증 프로세스를 완료합니다.

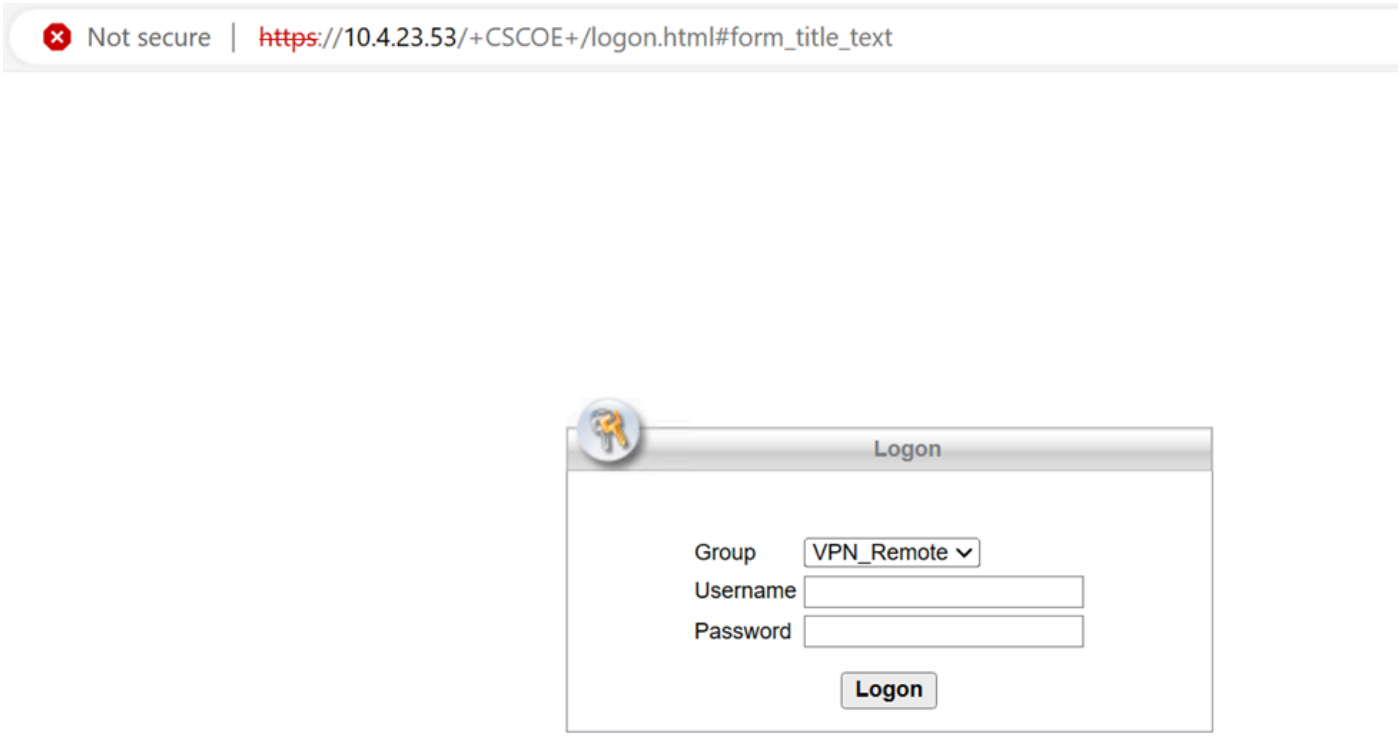
등록 프로세스에 대한 자세한 내용은 다음 리소스를 참조하십시오.

- 범용 등록 가이드: https://guide.duo.com/universal-enrollment
- 기존 등록 가이드: https://guide.duo.com/traditional-enrollment

구성 검증 절차.

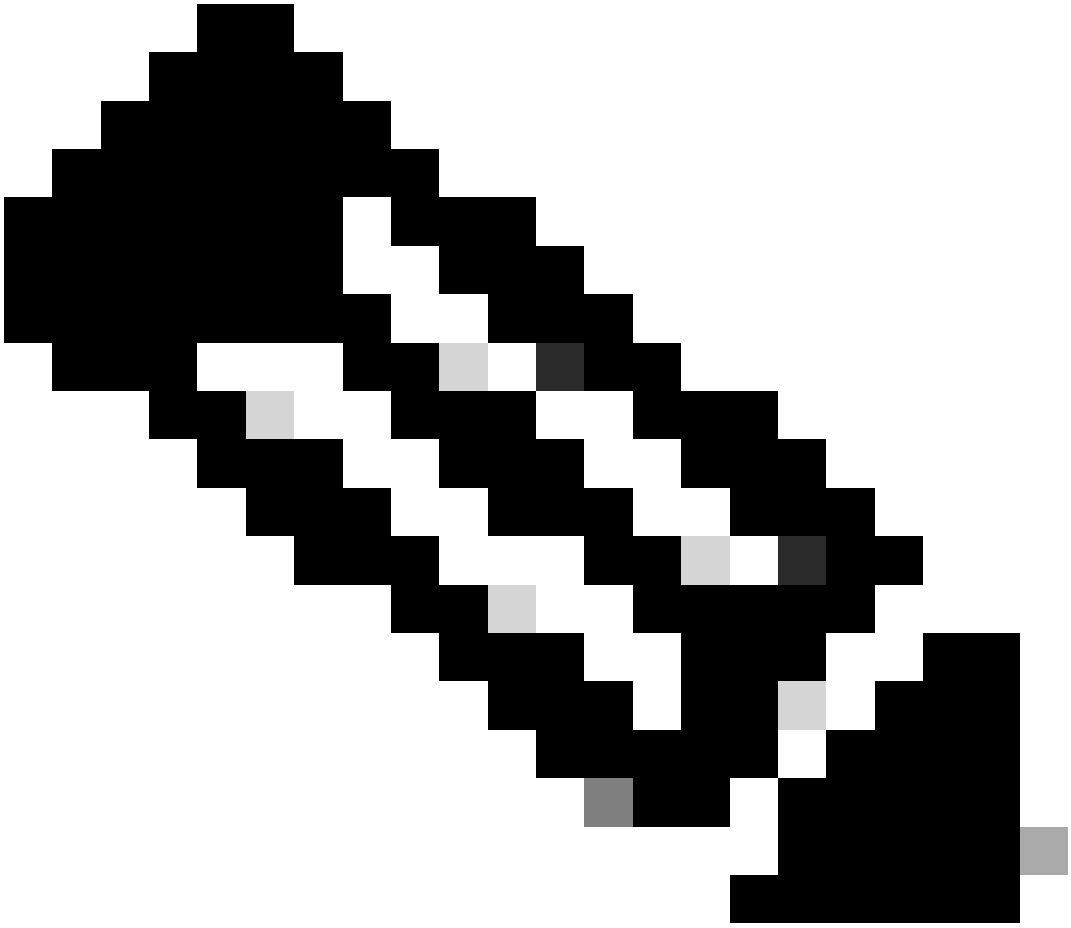
컨피그레이션이 정확하고 작동하는지 확인하려면 다음 단계를 검증하십시오.

1. 웹 브라우저를 시작하고 VPN 인터페이스에 액세스하기 위해 FTD(Firepower Threat Defense) 디바이스의 IP 주소를 입력합니다.



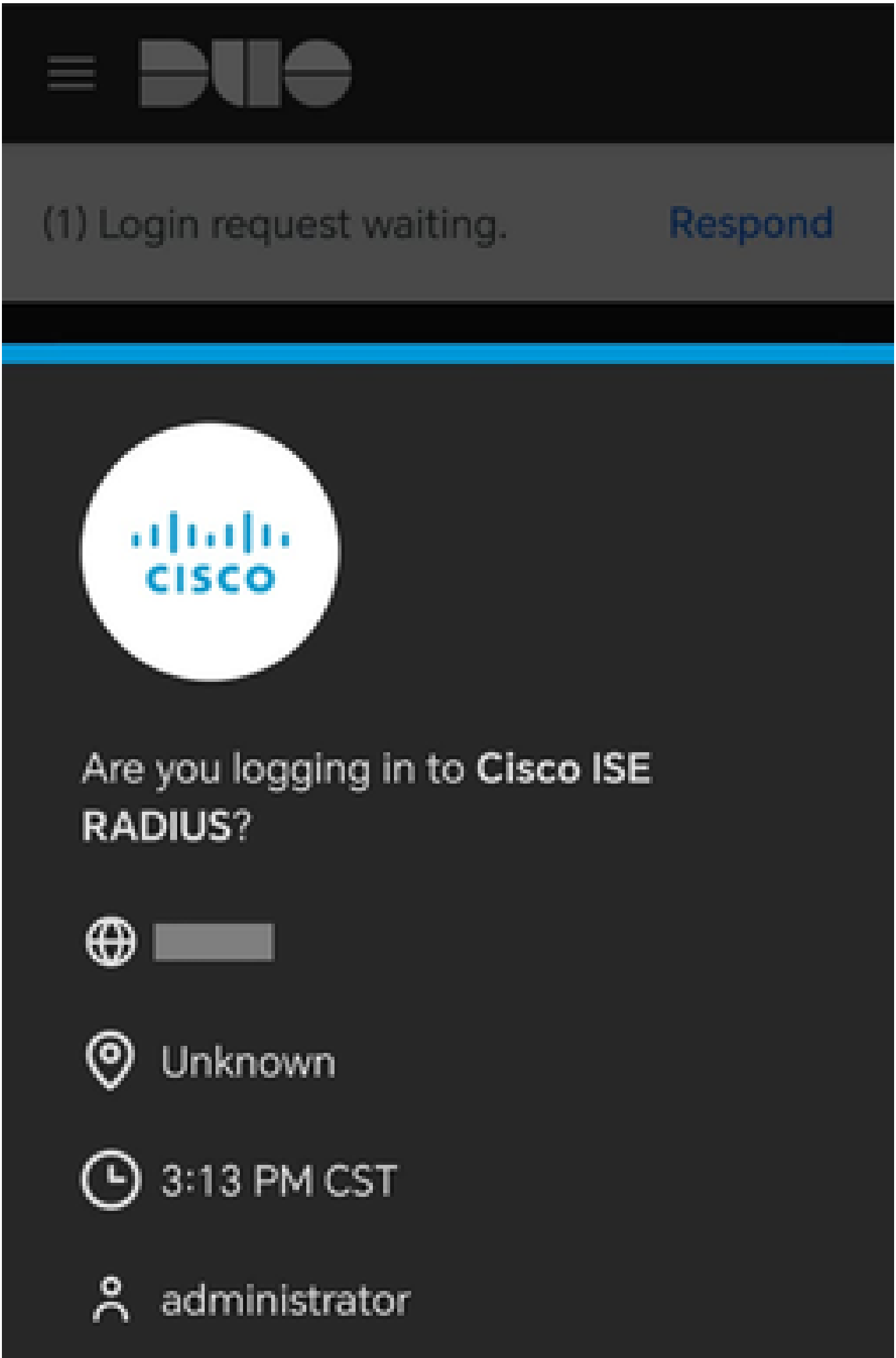
VPN 로그온

2. 프롬프트가 표시되면 사용자 이름과 비밀번호를 입력합니다.



참고: 자격 증명은 Active Directory 계정의 일부입니다.

3. DUO 푸시 알림을 받으면 DUO Mobile Software를 사용하여 승인하고 검증 프로세스를 진행합니다.


(1) Login request waiting.
Respond
Are you logging in to Cisco ISE RADIUS?
Unknown
3:13 PM CST
administrator

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.