

# ASA 8.x:MAC 지원을 통한 AnyConnect SSL VPN CAC-SmartCards 컨피그레이션

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[Cisco ASA 컨피그레이션](#)

[구축 고려 사항](#)

[AAA\(Authentication, Authorization, Accounting\) 컨피그레이션](#)

[LDAP 서버 구성](#)

[인증서 관리](#)

[키 생성](#)

[루트 CA 인증서 설치](#)

[ASA 등록 및 ID 인증서 설치](#)

[AnyConnect VPN 컨피그레이션](#)

[IP 주소 풀 생성](#)

[터널 그룹 및 그룹 정책 생성](#)

[터널 그룹 인터페이스 및 이미지 설정](#)

[인증서 일치 규칙\(OCSP를 사용할 경우\)](#)

[OCSP 구성](#)

[OCSP Responder 인증서 구성](#)

[OCSP를 사용하도록 CA 구성](#)

[OCSP 규칙 구성](#)

[Cisco AnyConnect 클라이언트 컨피그레이션](#)

[Cisco Anyconnect VPN 클라이언트 다운로드 - Mac OS X](#)

[Cisco AnyConnect VPN 클라이언트 시작 - Mac OS X](#)

[새 연결](#)

[원격 액세스 시작](#)

[부록 A - LDAP 매핑 및 DAP](#)

[시나리오 1:원격 액세스 권한 다이얼인을 사용한 Active Directory 적용 - 액세스 허용/거부](#)

[Active Directory 설정](#)

[ASA 컨피그레이션](#)

[시나리오 2:액세스 허용/거부에 그룹 구성원 자격을 사용하는 Active Directory 시행](#)

[Active Directory 설정](#)

[ASA 컨피그레이션](#)

[시나리오 3:여러 MemberOf 특성에 대한 동적 액세스 정책](#)

[ASA 컨피그레이션](#)

[부록 B - ASA CLI 컨피그레이션](#)

[부록 C- 문제 해결](#)

[AAA 및 LDAP 문제 해결](#)

[예 1:올바른 특성 매핑이 있는 허용된 연결](#)

[예 2:잘못 구성된 Cisco 특성 매핑으로 허용된 연결](#)

[DAP 문제 해결](#)

[예 1:DAP와의 연결 허용](#)

[예 2:DAP와의 연결 거부](#)

[인증 기관/OCSP 문제 해결](#)

[부록 D - MS에서 LDAP 개체 확인](#)

[LDAP 뷰어](#)

[Active Directory 서비스 인터페이스 편집기](#)

[부록 E](#)

[관련 정보](#)

## [소개](#)

이 문서에서는 인증을 위해 CAC(Common Access Card)를 사용하는 MAC 지원을 위한 AnyConnect VPN 원격 액세스용 Cisco ASA(Adaptive Security Appliance)의 샘플 컨피그레이션을 제공합니다.

이 문서의 범위는 Cisco ASA with Adaptive Security Device Manager(ASDM), Cisco AnyConnect VPN Client 및 Microsoft AD(Active Directory)/LDAP(Lightweight Directory Access Protocol)의 컨피그레이션을 다룹니다.

이 가이드의 컨피그레이션에서는 Microsoft AD/LDAP 서버를 사용합니다.이 문서에서는 OCSP, LDAP 특성 맵 및 DAP(Dynamic Access Policies)와 같은 고급 기능도 다룹니다.

## [사전 요구 사항](#)

### [요구 사항](#)

Cisco ASA, Cisco AnyConnect Client, Microsoft AD/LDAP 및 PKI(Public Key Infrastructure)에 대한 기본적인 이해는 전체 설정을 이해하는 데 도움이 됩니다.AD 그룹 멤버십, 사용자 속성 및 LDAP 객체에 대한 친숙함은 인증서 특성과 AD/LDAP 객체 간의 권한 부여 프로세스의 상관관계를 분석하는 데 도움이 됩니다.

### [사용되는 구성 요소](#)

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 8.0(x) 이상을 실행하는 Cisco 5500 Series ASA(Adaptive Security Appliance)
- ASA 8.x용 Cisco ASDM(Adaptive Security Device Manager) 버전 6.x
- Cisco AnyConnect VPN Client 2.2(MAC 지원)

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

## [표기 규칙](#)

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 규칙](#)을 참조하십시오.

## [Cisco ASA 컨피그레이션](#)

이 섹션에서는 ASDM을 통한 Cisco ASA의 컨피그레이션에 대해 설명합니다. SSL AnyConnect 연결을 통해 VPN 원격 액세스 터널을 구축하는 데 필요한 단계를 다룹니다. CAC 인증서는 인증에 사용되며 인증서의 UPN(User Principal Name) 특성은 권한 부여를 위해 Active Directory에 채워집니다.

### [구축 고려 사항](#)

- 이 설명서에서는 인터페이스, DNS, NTP, 라우팅, 디바이스 액세스, ASDM 액세스 등의 기본 컨피그레이션에 대해 다루지 않습니다. 네트워크 운영자가 이러한 컨피그레이션에 익숙하다고 가정합니다. 자세한 내용은 [다기능 보안 어플라이언스](#)를 참조하십시오.
- 빨간색으로 강조 표시된 섹션은 기본 VPN 액세스에 필요한 필수 컨피그레이션입니다. 예를 들어 OCSP 검사, LDAP 매핑 및 DAP(Dynamic Access Policy) 검사를 수행하지 않고 CAC 카드로 VPN 터널을 설정할 수 있습니다. DoD는 OCSP 검사를 지정하지만 터널은 OCSP가 구성되지 않은 상태에서 작동합니다.
- 파란색으로 강조 표시된 섹션은 설계에 보안을 추가하기 위해 포함할 수 있는 고급 기능입니다.
- ASDM 및 AnyConnect/SSL VPN은 동일한 인터페이스에서 동일한 포트를 사용할 수 없습니다. 액세스 권한을 얻으려면 하나 이상의 포트를 변경하는 것이 좋습니다. 예를 들어 ASDM에 포트 445를 사용하고 AC/SSL VPN에 443을 씁니다. ASDM URL 액세스가 8.x에서 변경되었습니다.  
.https://<ip\_address>:<port>/admin.html .
- 필요한 ASA 이미지는 최소 8.0.2.19 및 ASDM 6.0.2입니다.
- AnyConnect/CAC는 Vista에서 지원됩니다.
- 추가 [정책 시행](#)을 위한 LDAP 및 동적 액세스 정책 매핑 예는 부록 A를 참조하십시오.
- [MS에서](#) LDAP 객체를 확인하는 방법은 부록 D를 참조하십시오.
- 방화벽 컨피그레이션에 대한 애플리케이션 포트 목록은 관련 정보를 참조하십시오.

## [AAA\(Authentication, Authorization, Accounting\) 컨피그레이션](#)

CA(Common Access Card)에서 인증서를 사용하여 인증됩니다. CA(DisacCertificate Authority) 서버 또는 해당 조직의 CA 서버를 통해 인증됩니다. 인증서가 네트워크에 대한 원격 액세스에 유효해야 합니다. 인증 외에도 Microsoft Active Directory 또는 LDAP(Lightweight Directory Access Protocol) 객체를 사용할 수 있는 권한이 있어야 합니다. DoD(Department of Defense)에서는 인증서의 SAN(Subject Alternative Name) 섹션에 포함된 권한 부여를 위해 UPN(User Principal Name) 특성을 사용해야 합니다. UPN 또는 EDI/PI는 1234567890@mil 형식이어야 합니다. 이러한 컨피그레이션은 권한 부여를 위해 LDAP 서버를 사용하여 ASA에서 AAA 서버를 구성하는 방법을 보여줍니다. LDAP 객체 매핑의 추가 컨피그레이션은 부록 A를 참조하십시오.

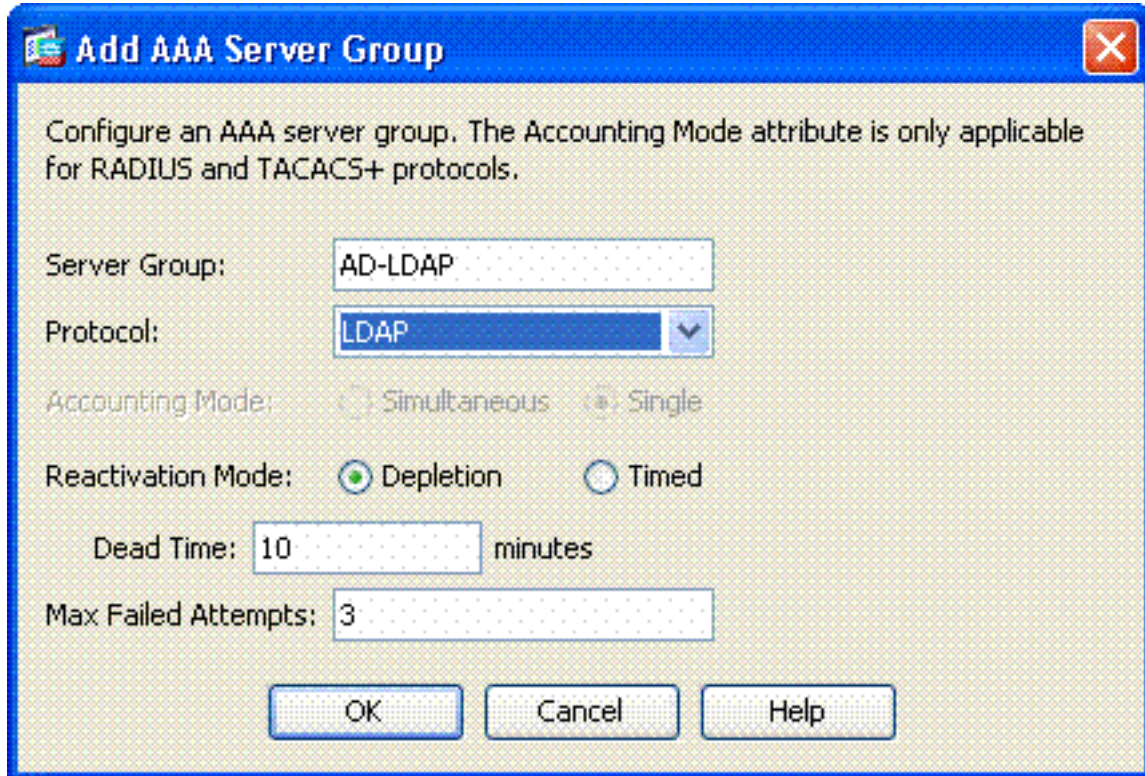
### [LDAP 서버 구성](#)

다음 단계를 완료하십시오.

1. Remote Access VPN(원격 액세스 VPN) > AAA Setup(AAA 설정) > AAA Server Group(AAA

서버 그룹)을 선택합니다.

2. AAA 서버 그룹 테이블에서 Add 3을 클릭합니다.
3. 서버 그룹 이름을 입력하고 프로토콜 라디오 버튼에서 LDAP를 선택합니다.그림 1을 참조하십시오.
4. 선택한 그룹 테이블의 서버에서 추가를 클릭합니다.생성한 서버가 이전 표에서 강조 표시되어 있는지 확인합니다.
5. AAA 서버 수정 창에서 다음 단계를 완료합니다.그림 2를 참조하십시오.참고: LDAP/AD가 이 연결 유형에 대해 구성된 경우 Enable LDAP over SSL 옵션을 선택합니다.LDAP가 있는 인터페이스를 선택합니다.이 가이드는 인터페이스 내부에 표시됩니다.서버의 IP 주소를 입력합니다.서버 포트를 입력합니다.기본 LDAP 포트는 389입니다.Server Type을 선택합니다.Base DN을 입력합니다.AD/LDAP 관리자에게 이 값을 문의하십시오.그림-1



scope 옵션에서 적절한 응답을 선택합니다.이는 기본 DN에 따라 달라집니다.AD/LDAP 관리자에게 도움을 요청하십시오.이름 지정 속성에 userPrincipalName을 입력합니다.AD/LDAP 서버의 사용자 권한 부여에 사용되는 특성입니다.Login DN에 관리자 DN을 입력합니다.참고: 사용자 객체 및 그룹 멤버십이 포함된 LDAP 구조를 보거나 검색할 수 있는 관리자 권한 또는 권한이 있습니다.로그인 비밀번호에 관리자의 비밀번호를 입력합니다.LDAP 특성을 none으로 둡니다.그림-2

참고: 나중

에 컨피그레이션에서 이 옵션을 사용하여 권한 부여를 위해 다른 AD/LDAP 객체를 추가합니다. 확인을 선택합니다.

6. 확인을 선택합니다.

## 인증서 관리

ASA에 인증서를 설치하려면 두 단계가 있습니다. 먼저 필요한 CA 인증서(루트 및 하위 CA)를 설치합니다. 둘째, ASA를 특정 CA에 등록하고 ID 인증서를 가져옵니다. DoD PKI는 ASA가 등록된 Root CA2, Class 3 Root, CA# Intermediate, ASA ID 인증서 및 OCSP 인증서를 사용합니다. 그러나 OCSP를 사용하지 않도록 선택하면 OCSP 인증서를 설치할 필요가 없습니다.

참고: 루트 인증서와 디바이스에 대한 ID 인증서를 등록하는 방법에 대한 지침을 얻으려면 보안 POC에 문의하십시오. SSL 인증서는 ASA에서 원격 액세스하기에 충분해야 합니다. 이중 SAN 인증서가 필요하지 않습니다.

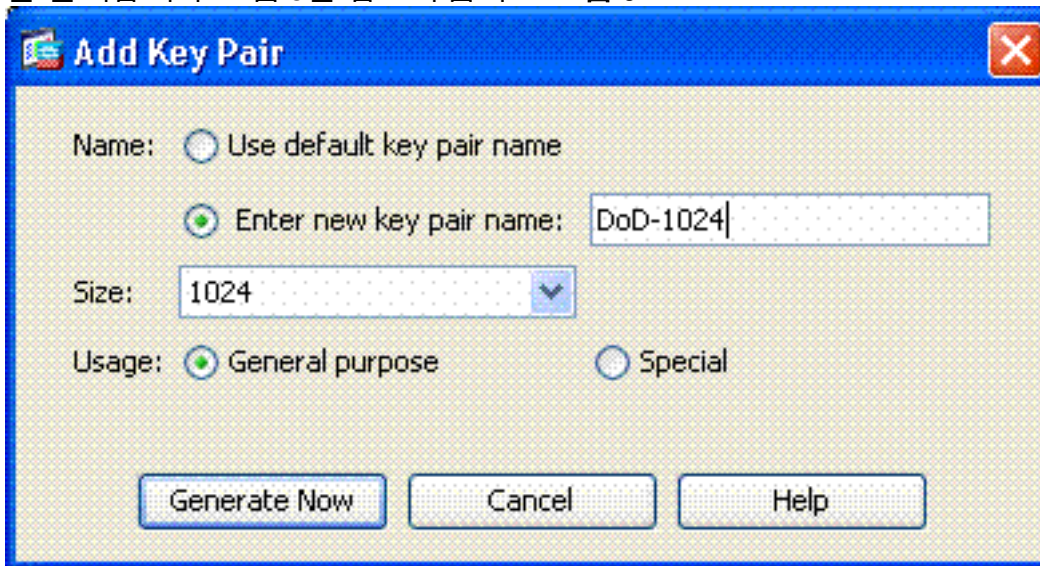
**참고:** 로컬 머신에도 DoD CA 체인이 설치되어 있어야 합니다.인증서는 Internet Explorer를 사용하여 Microsoft 인증서 저장소에서 볼 수 있습니다.DoD는 시스템에 모든 CA를 자동으로 추가하는 배치 파일을 생성했습니다.자세한 내용은 PKI POC에 문의하십시오.

**참고:** DoD CA2 및 Class 3 루트는 물론 ASA 인증서를 발급한 ASA ID 및 CA 증급만 사용자 인증에 필요한 CA여야 합니다.현재 모든 CA 증개자는 CA2 및 Class 3 루트 체인에 속하며 CA2 및 Class 3 루트가 추가되는 한 신뢰할 수 있습니다.

## 키 생성

다음 단계를 완료하십시오.

1. Remote Access VPN(원격 액세스 VPN) > Certificate Management(인증서 관리) > Identity Certificate(ID 인증서) > Add(추가)를 선택합니다.
2. Add a new id certificate(새 ID 인증서 추가)를 선택한 다음 New by the key pair(키 쌍 옵션으로 새로 만들기)를 선택합니다.
3. Add Key Pair(키 쌍 추가) 창에서 키 이름 DoD-1024를 입력합니다.새 키를 추가하려면 라디오를 클릭합니다.그림 3을 참조하십시오.그림 3

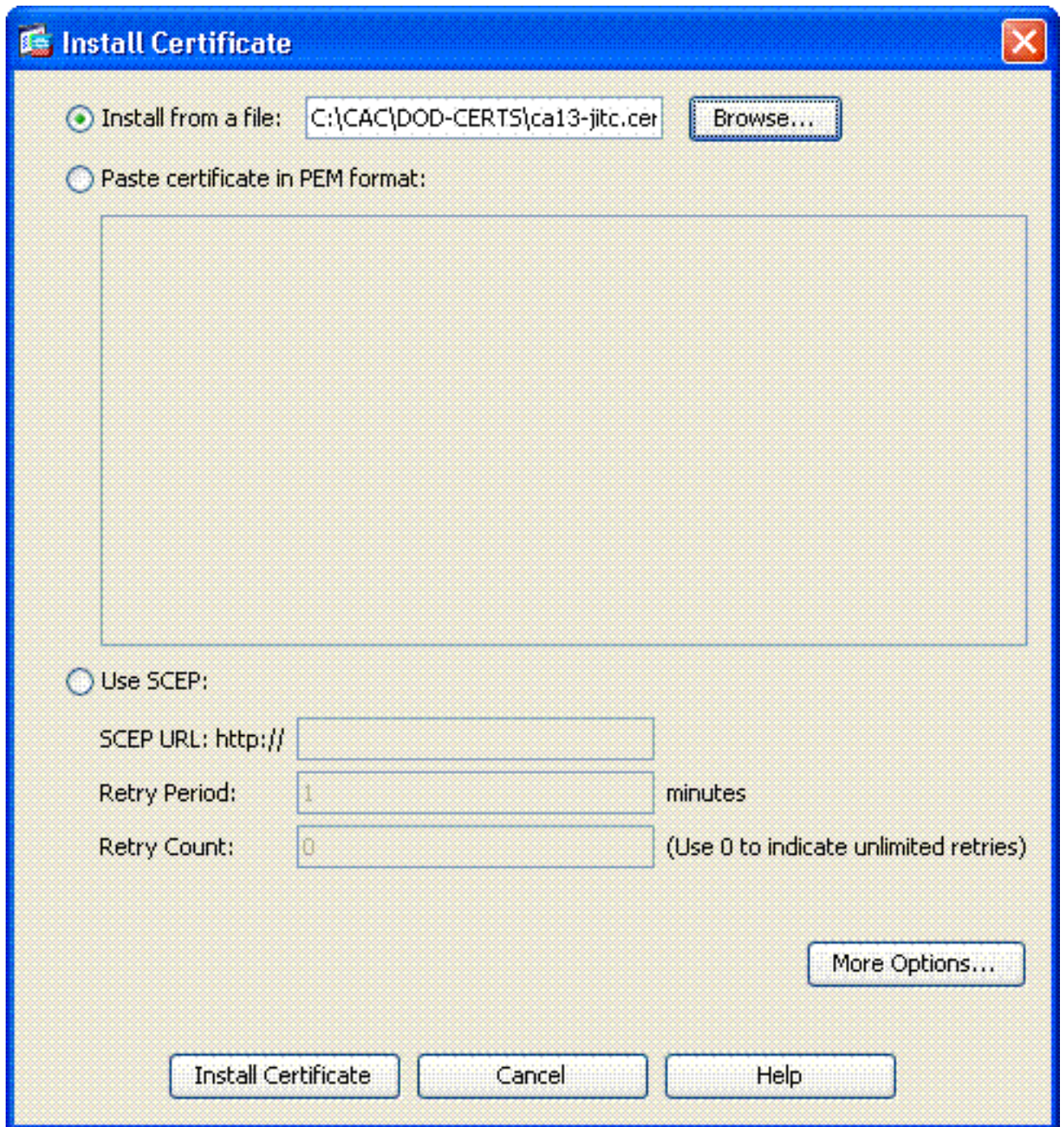


4. 키의 크기를 선택합니다.
5. 범용으로 사용 유지.
6. Generate Now(지금 생성)를 클릭합니다.참고: DoD 루트 CA 2는 2048비트 키를 사용합니다.이 CA를 사용하려면 2048비트 키 쌍을 사용하는 두 번째 키를 생성해야 합니다.두 번째 키를 추가하려면 위의 이전 단계를 완료하십시오.

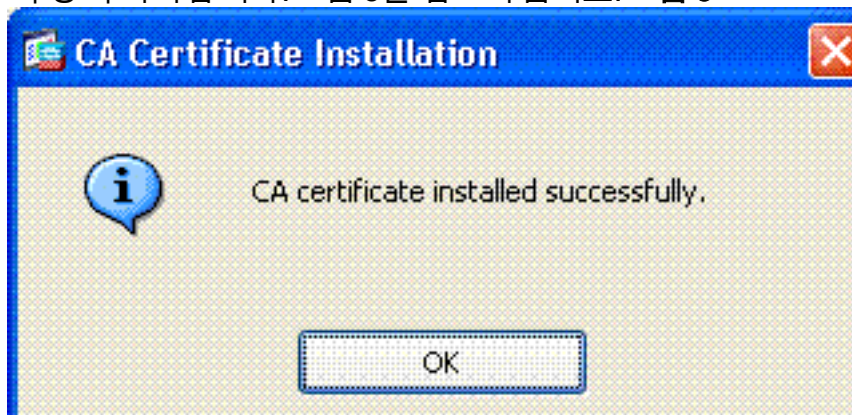
## 루트 CA 인증서 설치

다음 단계를 완료하십시오.

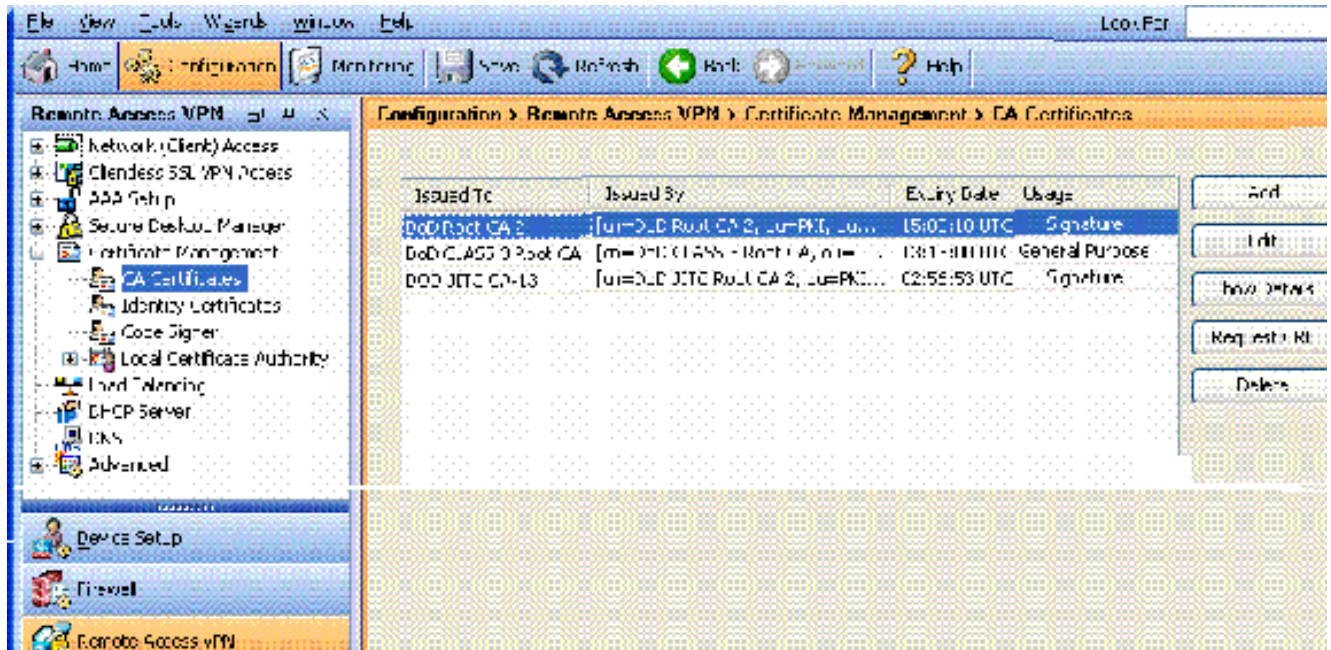
1. Remote Access VPN(원격 액세스 VPN) > Certificate Management(인증서 관리) > CA Certificate(CA 인증서) > Add(추가)를 선택합니다.
2. Install from File(파일에서 설치)을 선택하고 인증서를 찾습니다.
3. Install Certificate를 선택합니다.그림 4:루트 인증서 설치



4. 이 창이 나타납니다.그림 5를 참조하십시오.그림 5

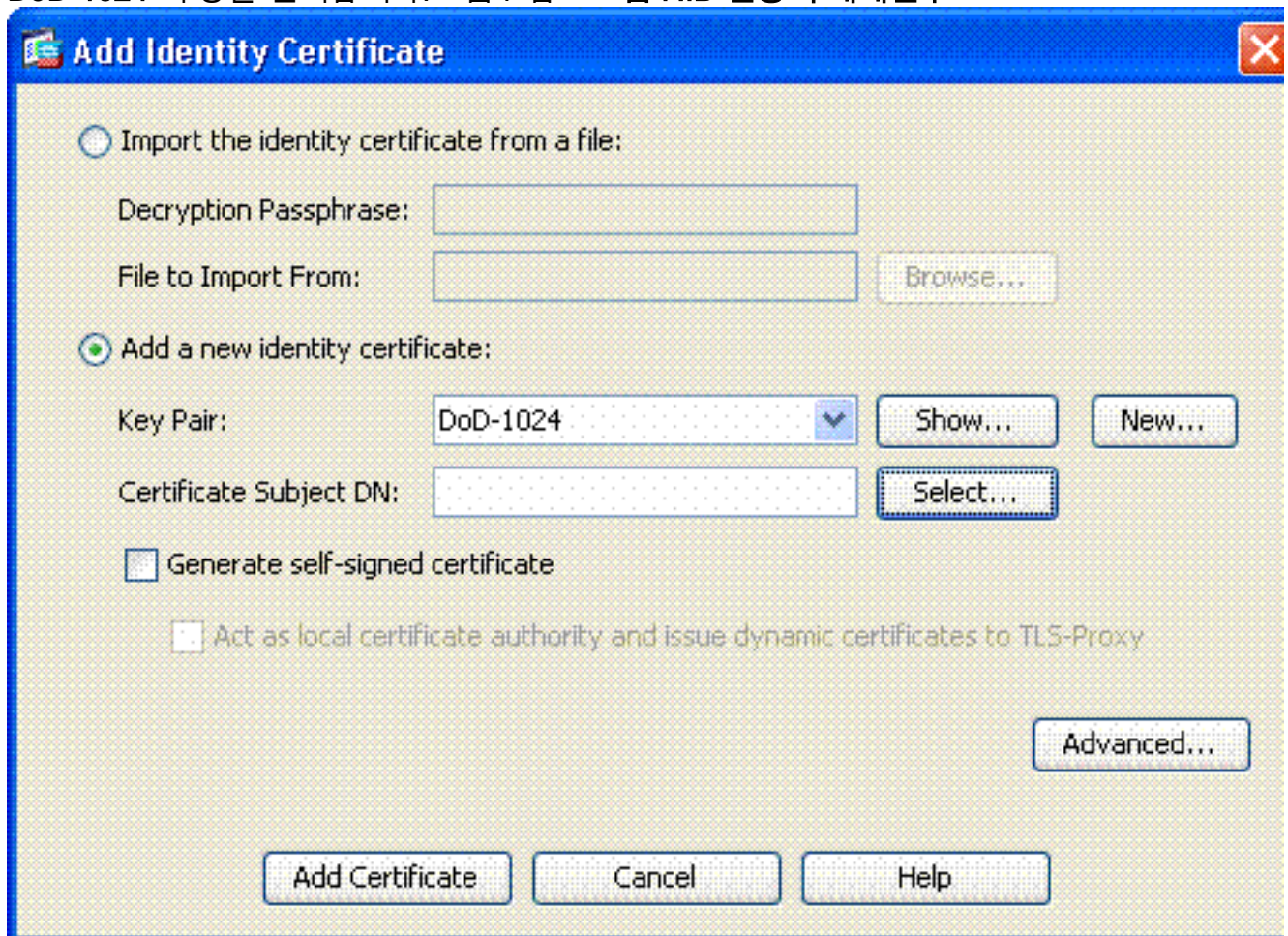


참고: 설치할 모든 인증서에 대해 1~3단계를 반복합니다.DoD PKI에는 다음 각각에 대한 인증서가 필요합니다.루트 CA 2, 클래스 3 루트, CA## 중간, ASA ID 및 OCSP 서버.OCSP를 사용하지 않는 경우 OCSP 인증서가 필요하지 않습니다.그림 6:루트 인증서 설치



## ASA 등록 및 ID 인증서 설치

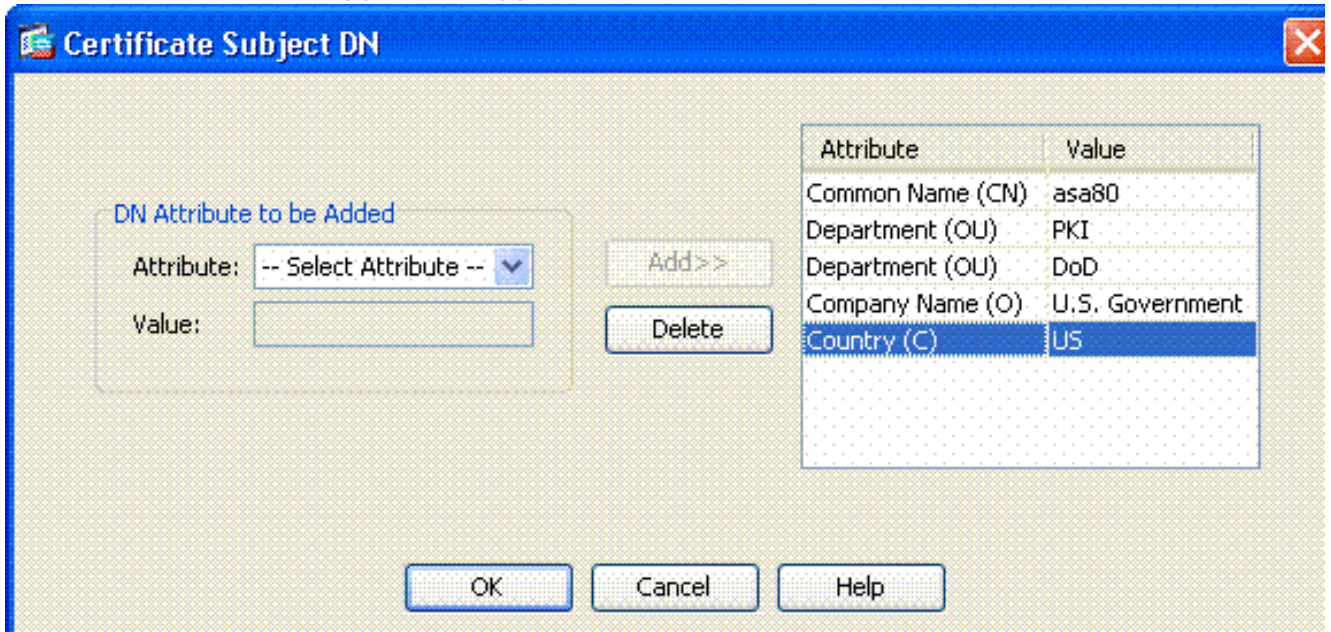
1. Remote Access VPN(원격 액세스 VPN) > Certificate Management(인증서 관리) > Identity Certificate(ID 인증서) > Add(추가)를 선택합니다.
2. 새 ID 인증서 추가를 선택합니다.
3. DoD-1024 키 쌍을 선택합니다.그림 7 참조그림 7:ID 인증서 매개변수



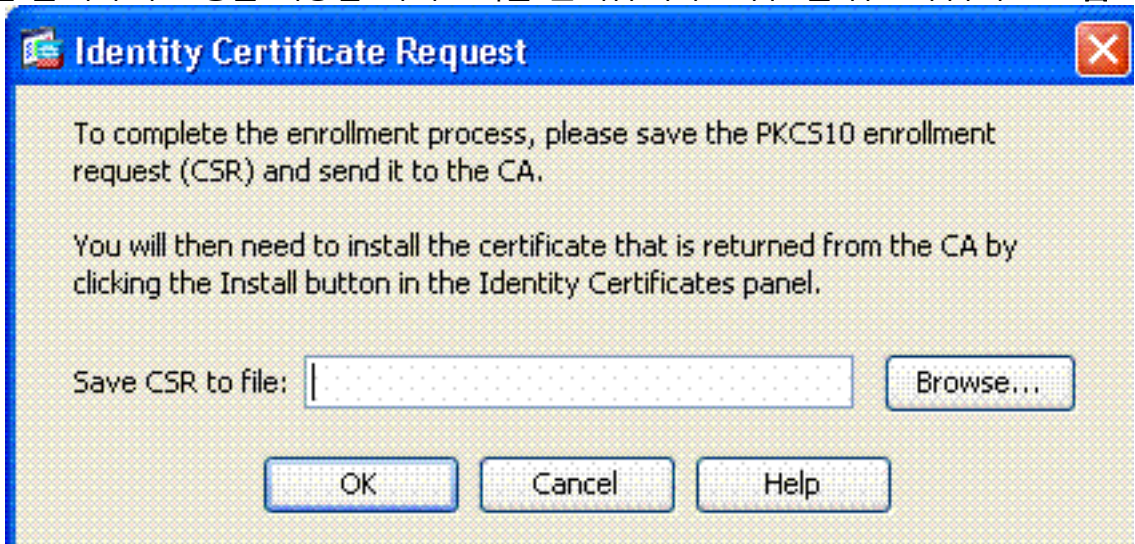
4. Certificate subject DN(인증서 주체 DN) 상자로 이동하고 Select(선택)를 클릭합니다.
5. Certificate Subject DN(인증서 주체 DN) 창에서 디바이스의 정보를 입력합니다.예를 들면 그



림 8을 참조하십시오.그림 8:DN 편집

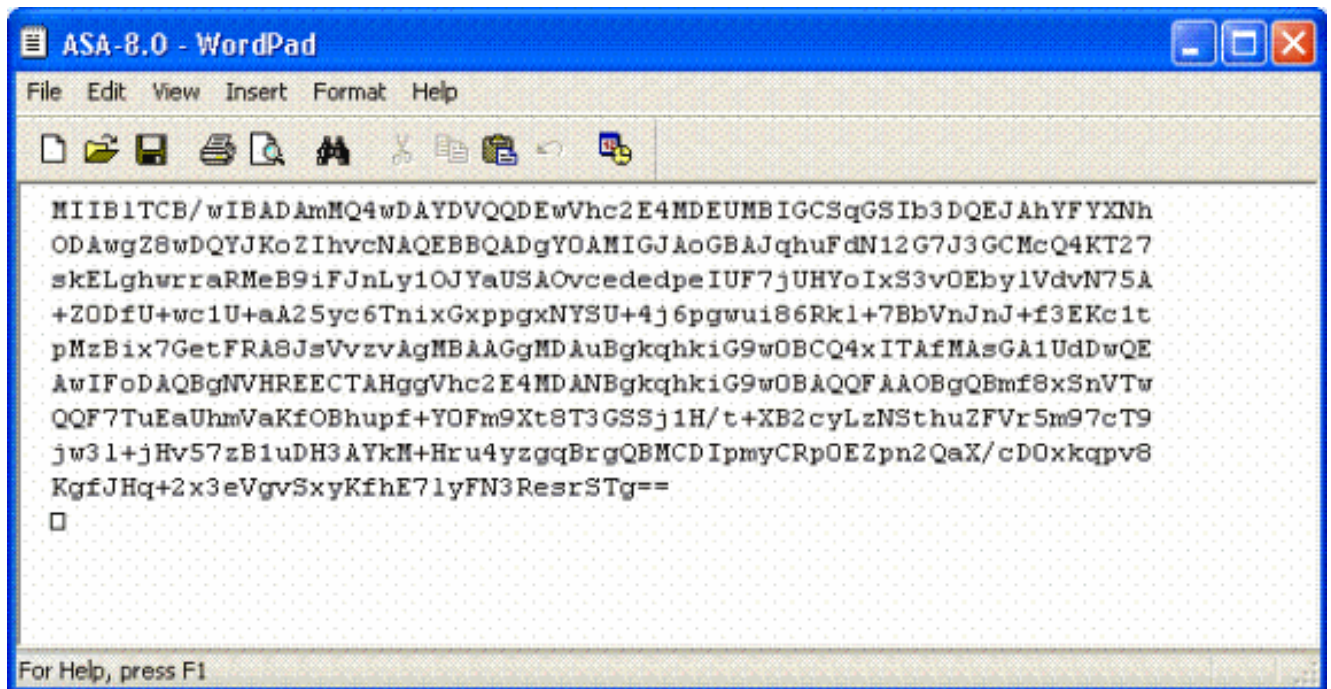


6. 확인을 선택합니다.참고: 주체 DN을 추가할 때 시스템에 구성된 디바이스의 호스트 이름을 사용해야 합니다.PKI POC는 필수 필드에 대해 알려줄 수 있습니다.
7. Add **certificate**를 선택합니다.
8. **찾아보기**를 클릭하여 요청을 저장할 디렉토리를 선택합니다.그림 9를 참조하십시오.그림 9 인

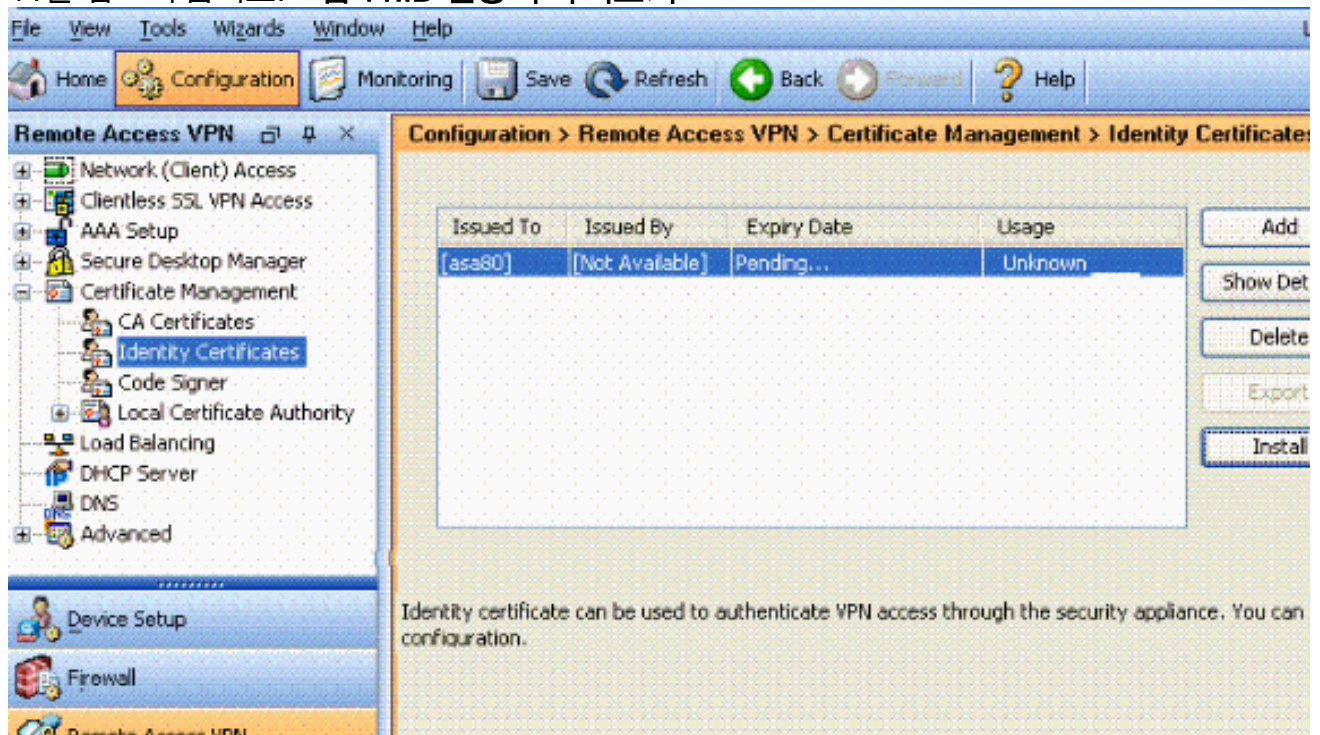


중서 요청

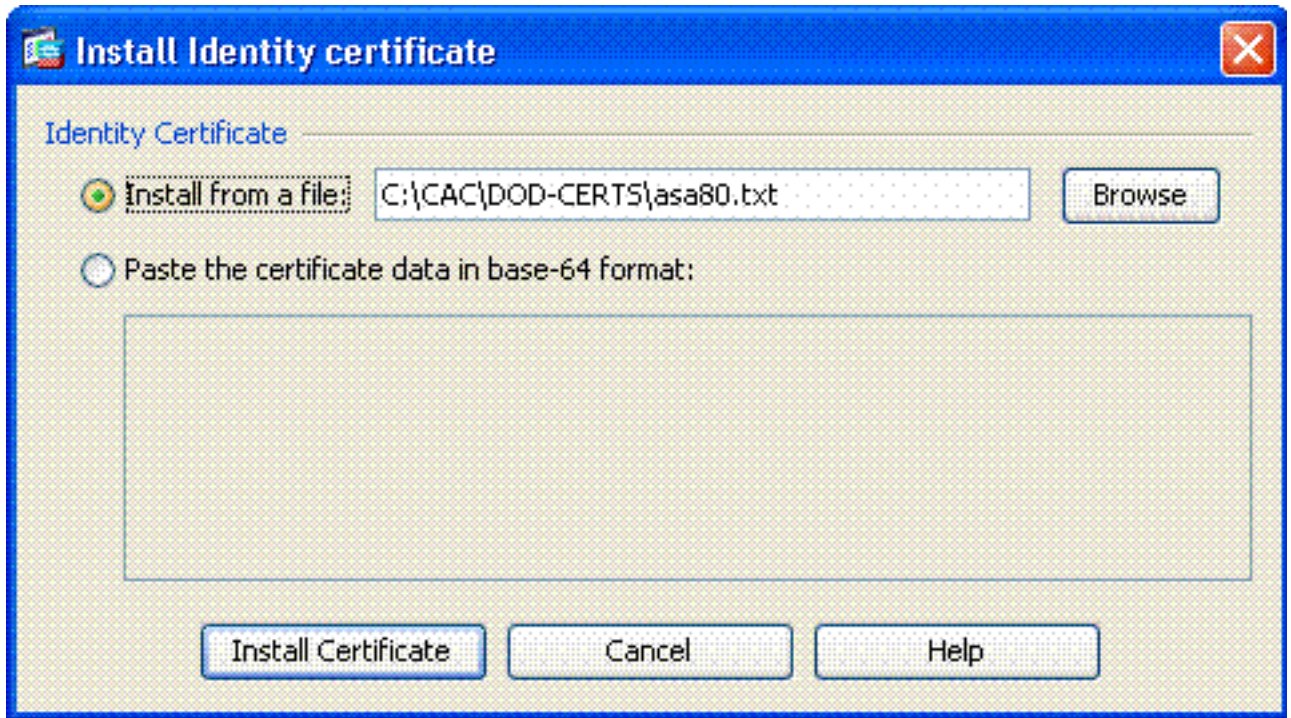
9. WordPad를 사용하여 파일을 열고, 요청을 해당 문서에 복사하고 PKI POC로 전송합니다.그림 10을 참조하십시오.그림 10:등록 요청



10. CA 관리자로부터 인증서를 수신한 후 Remote Access VPN(원격 액세스 VPN) > Certificate Management(인증서 관리) > ID Certificate(ID 인증서) > Install(설치)을 선택합니다.그림 11을 참조하십시오.그림 11:ID 인증서 가져오기



11. Install certificate(인증서 설치) 창에서 ID 인증서를 찾아 Install Certificate(인증서 설치)를 선택합니다.예를 들면 그림 12를 참조하십시오.그림 12:ID 인증서 설치



**참고:** 발급된 인증서 및 키 쌍을 저장하려면 ID 인증서 신뢰 지점을 순서대로 내보내는 것이 좋습니다. 이를 통해 ASA 관리자는 RMA 또는 하드웨어 장애 시 인증서 및 키 쌍을 새 ASA로 가져올 수 있습니다. 자세한 내용은 [신뢰 지점 내보내기 및 가져오기](#)를 참조하십시오. **참고:** 플래시 메모리에 컨피그레이션을 저장하려면 SAVE를 클릭합니다.

## [AnyConnect VPN 컨피그레이션](#)

ASDM에서 VPN 매개변수를 구성하기 위한 두 가지 옵션이 있습니다. 첫 번째 옵션은 SSL VPN 마법사를 사용하는 것입니다. 이 툴은 VPN 컨피그레이션의 새로운 사용자에게 사용하기 쉬운 툴입니다. 두 번째 옵션은 수동으로 수행하고 각 옵션을 진행하는 것입니다. 이 컨피그레이션 가이드에서는 수동 방법을 사용합니다.

**참고:** AC 클라이언트를 사용자에게 가져오는 방법에는 두 가지가 있습니다.

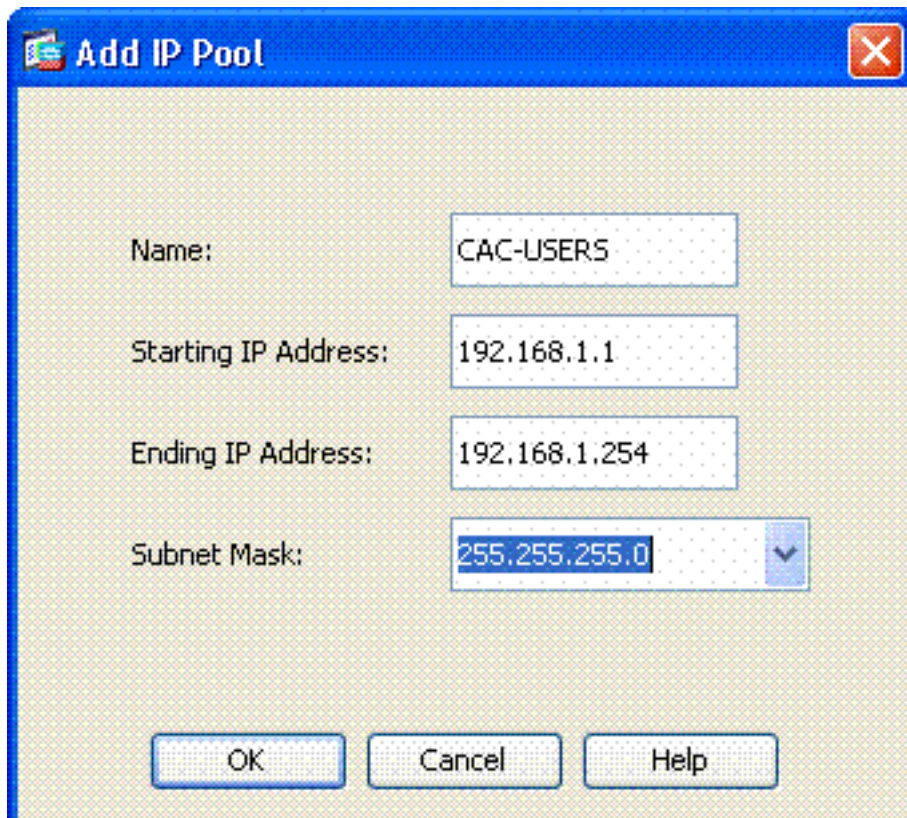
1. Cisco 웹 사이트에서 클라이언트를 다운로드하여 해당 시스템에 설치할 수 있습니다.
2. 사용자는 웹 브라우저를 통해 ASA에 액세스할 수 있으며 클라이언트를 다운로드할 수 있습니다.

**참고:** 예: <https://asa.test.com>. 이 설명서에서는 두 번째 방법을 사용합니다. AC 클라이언트가 클라이언트 시스템에 영구적으로 설치되면 애플리케이션에서 AC 클라이언트를 실행하면 됩니다.

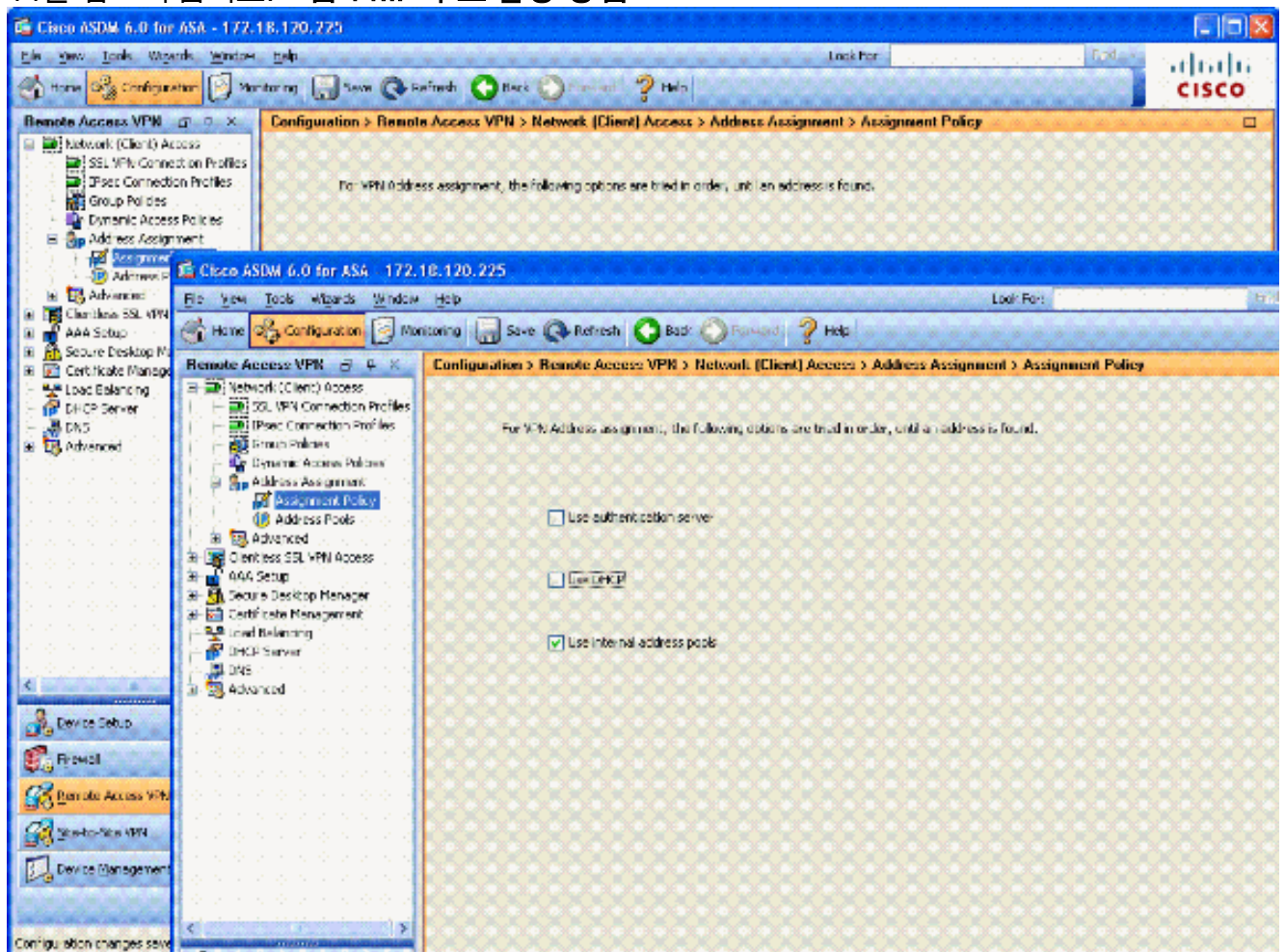
## [IP 주소 풀 생성](#)

DHCP와 같은 다른 방법을 사용하는 경우 선택 사항입니다.

1. Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Address Assignment(주소 할당) > Address Pools(주소 풀)를 선택합니다.
2. Add(추가)를 클릭합니다.
3. Add IP Pool(IP 풀 추가) 창에서 IP 풀의 이름(시작 및 종료 IP 주소)을 입력하고 서브넷 마스크를 선택합니다. 그림 13을 참조하십시오. **그림 13: IP 풀 추가**



4. 확인을 선택합니다.
5. Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Address Assignment(주소 할당) > Assignment Policy(할당 정책)를 선택합니다.
6. 적절한 IP 주소 할당 방법을 선택합니다.이 설명서에서는 내부 주소 풀을 사용합니다.그림 14를 참조하십시오.그림 14:IP 주소 할당 방법



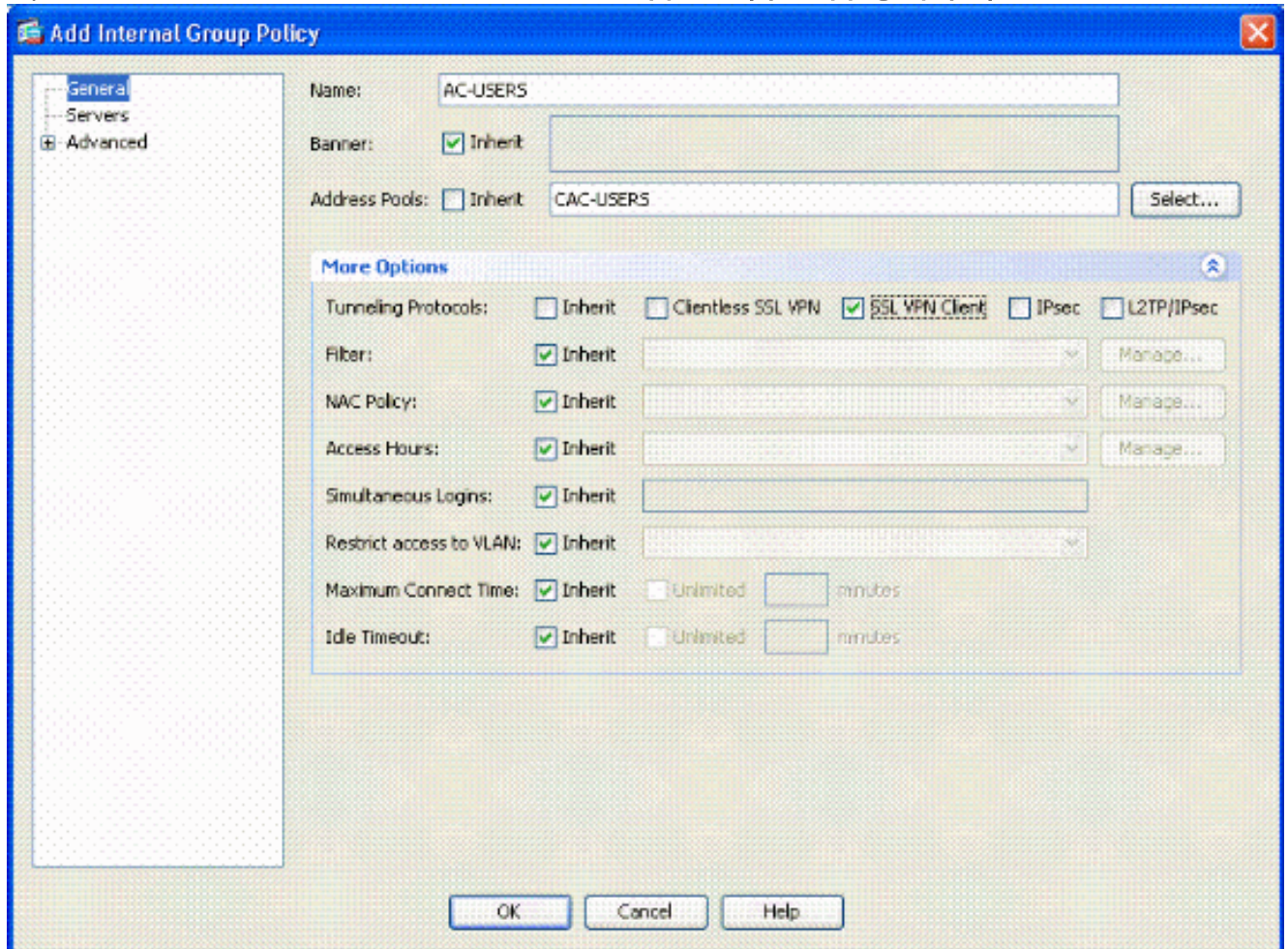
7. Apply를 클릭합니다.

## 터널 그룹 및 그룹 정책 생성

### 그룹 정책

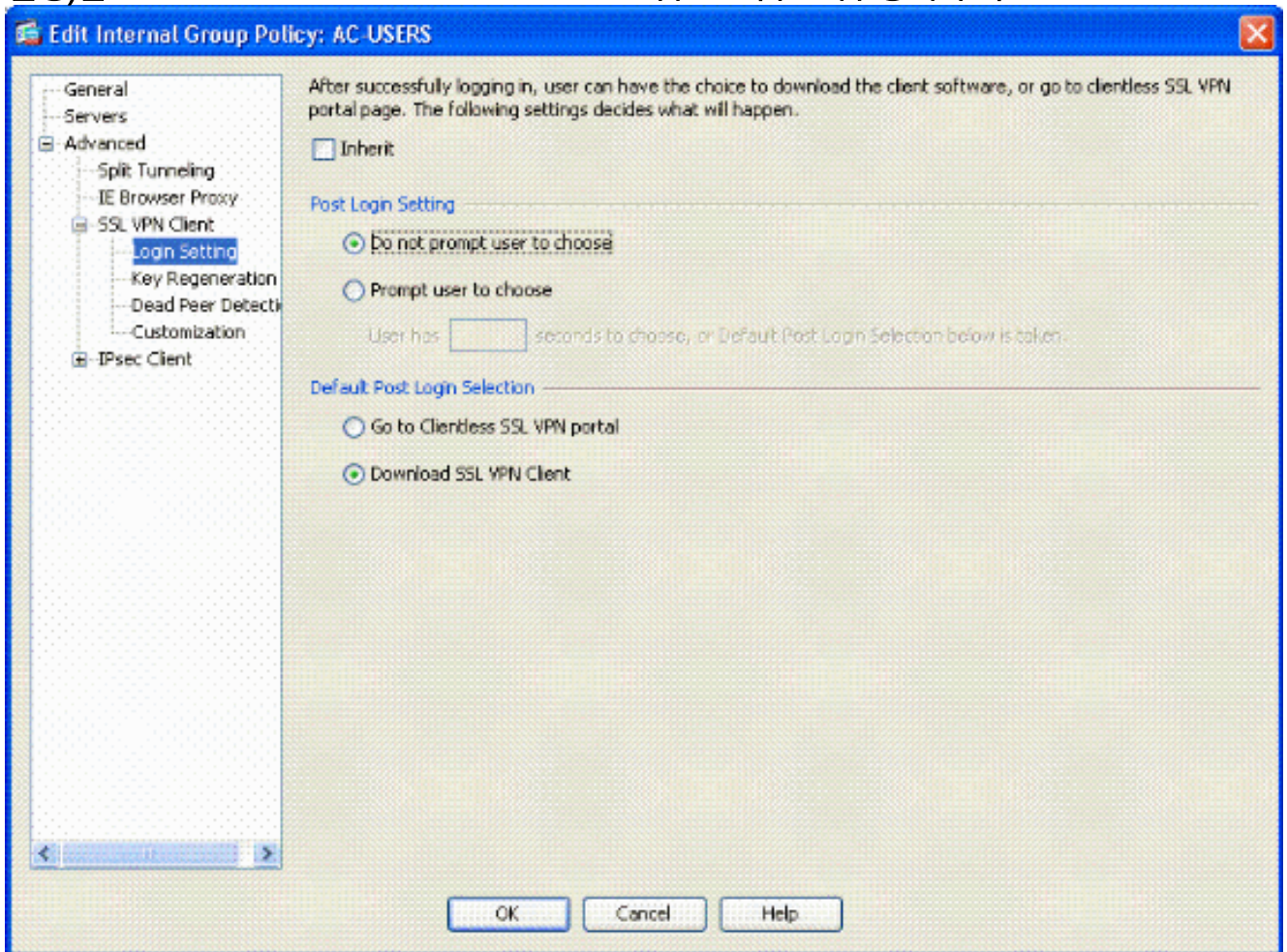
참고: 새 정책을 생성하지 않으려면 기본 기본 기본 그룹 정책을 사용할 수 있습니다.

1. Remote Access VPN(원격 액세스 VPN) -> Network (Client) Access(네트워크(클라이언트) 액세스) -> Group Policies(그룹 정책)를 선택합니다.
2. Add(추가)를 클릭하고 Internal Group Policy(내부 그룹 정책)를 선택합니다.
3. Add Internal Group Policy(내부 그룹 정책 추가) 창의 Name(이름) 텍스트 상자에 그룹 정책의 이름을 입력합니다.그림 15를 참조하십시오.그림 15:내부 그룹 정책 추가



클라이언트리스 SSL과 같은 다른 프로토콜을 사용하지 않는 한 General(일반) 탭에서 Tunneling Protocols(터널링 프로토콜) 옵션에서 SSL VPN Client를 선택합니다.Servers(서버) 섹션에서 inherit(상속) 확인란의 선택을 취소하고 DNS 및 WINS 서버의 IP 주소를 입력합니다. 해당되는 경우 DHCP 범위를 입력합니다.Servers(서버) 섹션에서 Default Domain(기본 도메인)에서 inherit(상속) 확인란의 선택을 취소하고 적절한 도메인 이름을 입력합니다.General(일반) 탭에서 주소 풀 섹션에서 inherit 확인란을 선택 취소하고 이전 단계에서 생성한 주소 풀을 추가합니다.다른 IP 주소 할당 방법을 사용하는 경우 상속하고 적절하게 변경하려면 그대로 둡니다.다른 모든 컨피그레이션 탭은 기본 설정으로 유지됩니다.참고: AC 클라이언트를 최종 사용자에게 가져오는 방법에는 두 가지가 있습니다.한 가지 방법은 Cisco.com으로 이동하여 AC 클라이언트를 다운로드하는 것입니다.두 번째 방법은 사용자가 연결을 시도할 때 ASA에서 클라이언트를 사용자에게 다운로드하도록 하는 것입니다.다음 예제에서는 후자의 메서드를 보여 줍니다.

4. 그런 다음 Advanced(고급) > SSL VPN Client(SSL VPN 클라이언트) > Login Settings(로그인 설정)를 선택합니다.그림 16을 참조하십시오.그림 16:내부 그룹 정책 추가

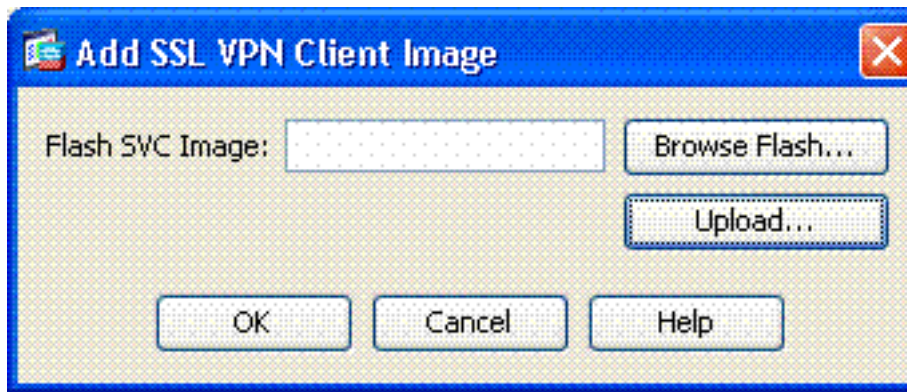


Inherit(상속) 확인란을 선택 취소합니다.환경에 맞는 적절한 포스트 로그인 설정을 선택합니다.환경에 적합한 기본 사후 로그인 선택을 선택합니다.확인을 선택합니다.

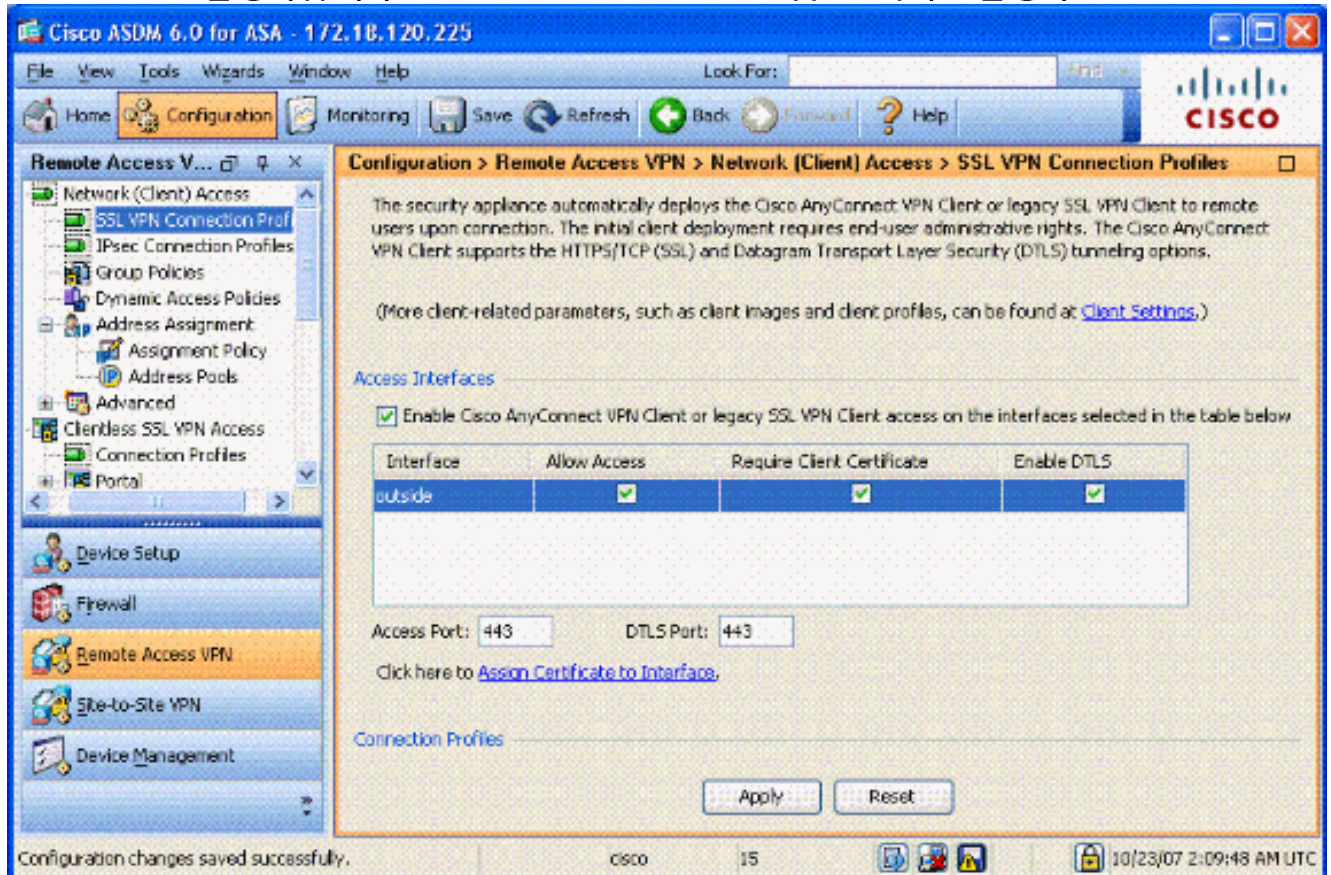
## 터널 그룹 인터페이스 및 이미지 설정

참고: 새 그룹을 만들지 않으려면 기본 내장 그룹을 사용할 수 있습니다.

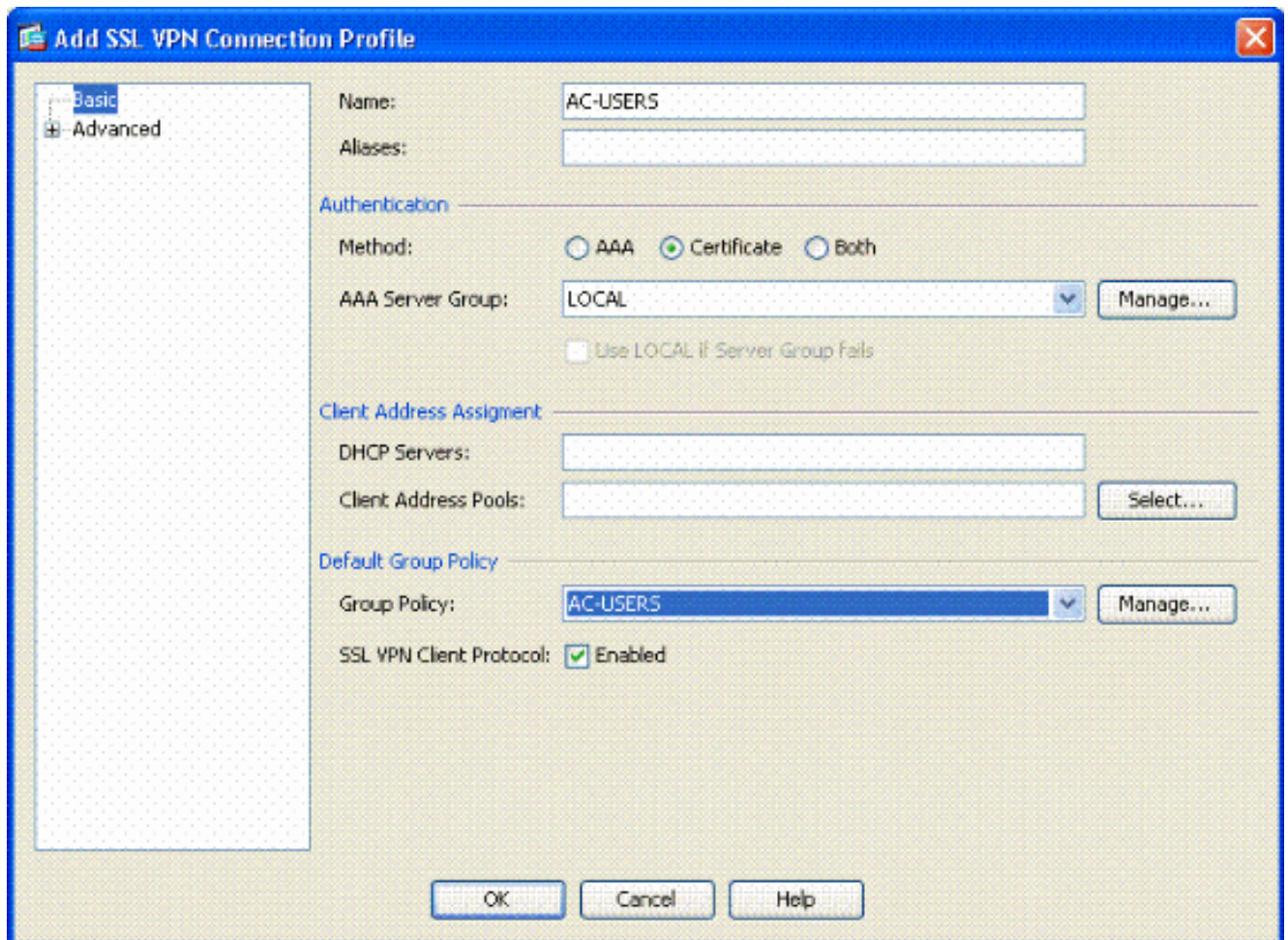
1. Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > SSL VPN Connection Profile(SSL VPN 연결 프로파일)을 선택합니다.
2. Enable Cisco AnyConnect Client....를 선택합니다.
3. SVC 를 ? 질문
4. 예를 선택합니다.
5. 이미지가 이미 있는 경우 [플래시 찾아보기]에서 사용할 이미지를 선택합니다.이미지를 사용할 수 없는 경우 Upload(업로드)를 선택하고 로컬 컴퓨터에서 파일을 찾습니다.그림 17을 참조하십시오. 파일은 Cisco.com에서 다운로드할 수 있습니다.Windows, MAC 및 Linux 파일이 있습니다.그림 17:SSL VPN 클라이언트 이미지 추가



6. 다음으로 Allow Access(액세스 허용), Require Client Cert(클라이언트 인증서 필요) 및 선택적으로 DTLS를 활성화합니다.그림 18을 참조하십시오.그림 18:액세스 활성화



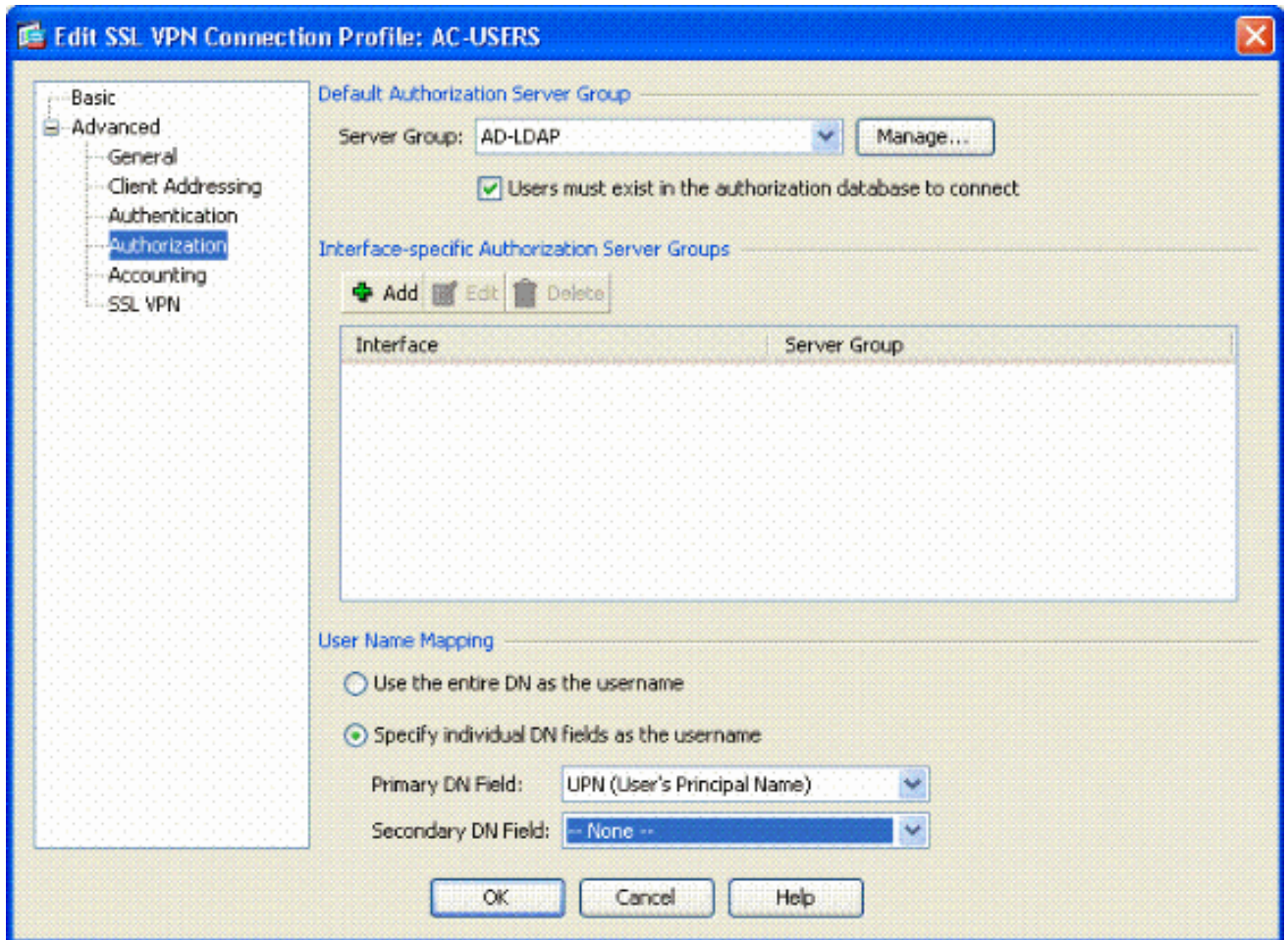
7. Apply를 클릭합니다.
8. 그런 다음 연결 프로파일/터널 그룹을 생성합니다.Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > SSL VPN Connection Profile(SSL VPN 연결 프로파일)을 선택합니다.
9. Connection Profiles(연결 프로파일) 섹션에서 Add(추가)를 클릭합니다.그림 19:연결 프로파일 추가



그룹의 이름을 지정합니다. 인증 방법에서 Certificate를 선택합니다. 이전에 생성한 그룹 정책을 선택합니다. SSL VPN 클라이언트가 활성화되었는지 확인합니다. 다른 옵션은 기본값으로 둡니다.

10. 그런 다음 Advanced(고급) > Authorization(권한 부여)을 선택합니다. 그림 20 참조 그림 20: Authorization(권한 부여)

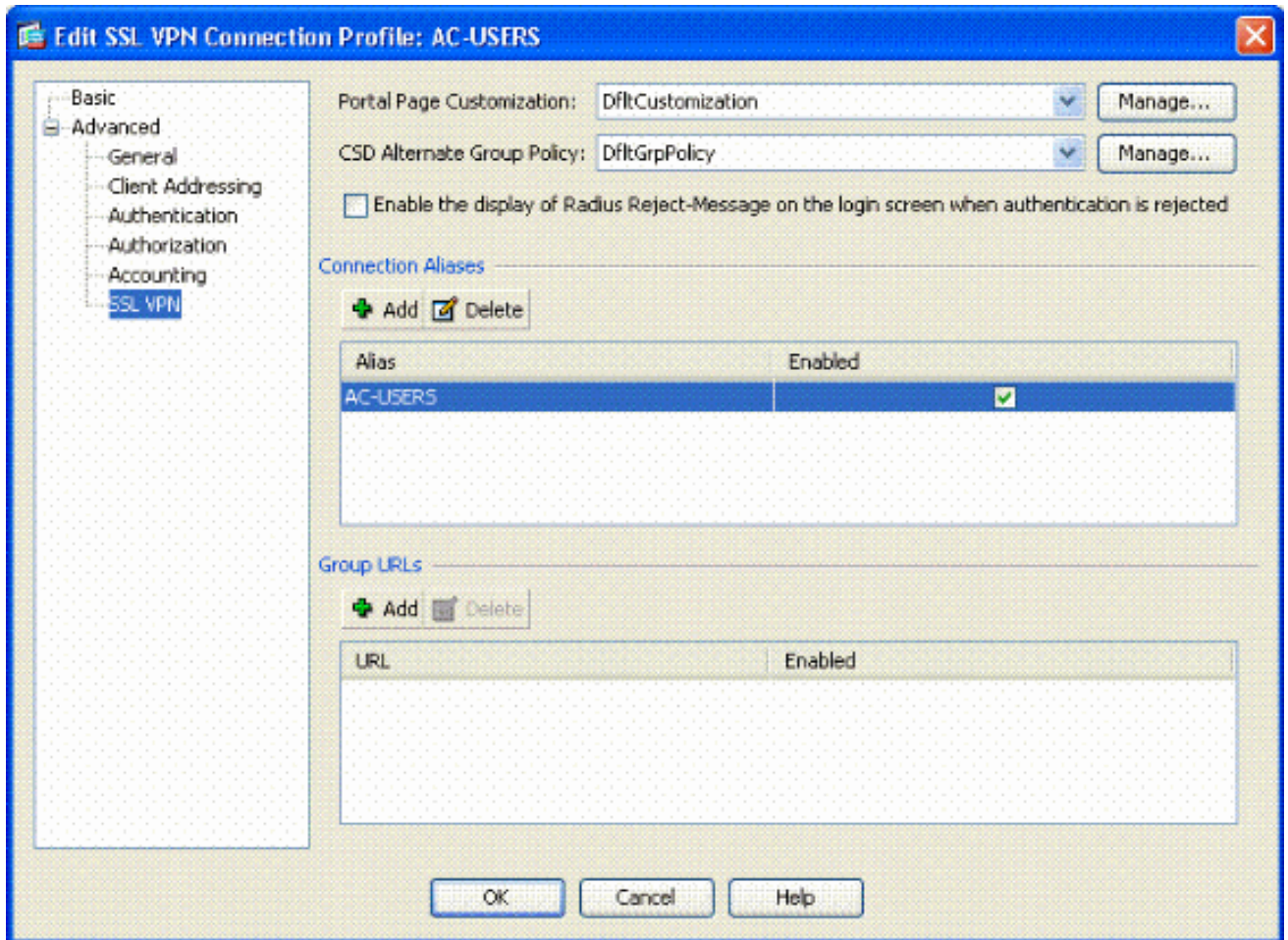




이전에 생성한 AD-LDAP 그룹을 선택합니다. 연결하려면 사용자가 있어야 함...을 선택합니다. 매핑 필드에서 기본에 대해 UPN을 선택하고 보조에 대해서는 none을 선택합니다.

11. 메뉴의 **SSL VPN** 섹션을 선택합니다.

12. Connection Aliases 섹션에서 다음 단계를 완료합니다. **그림 21: 연결 별칭**



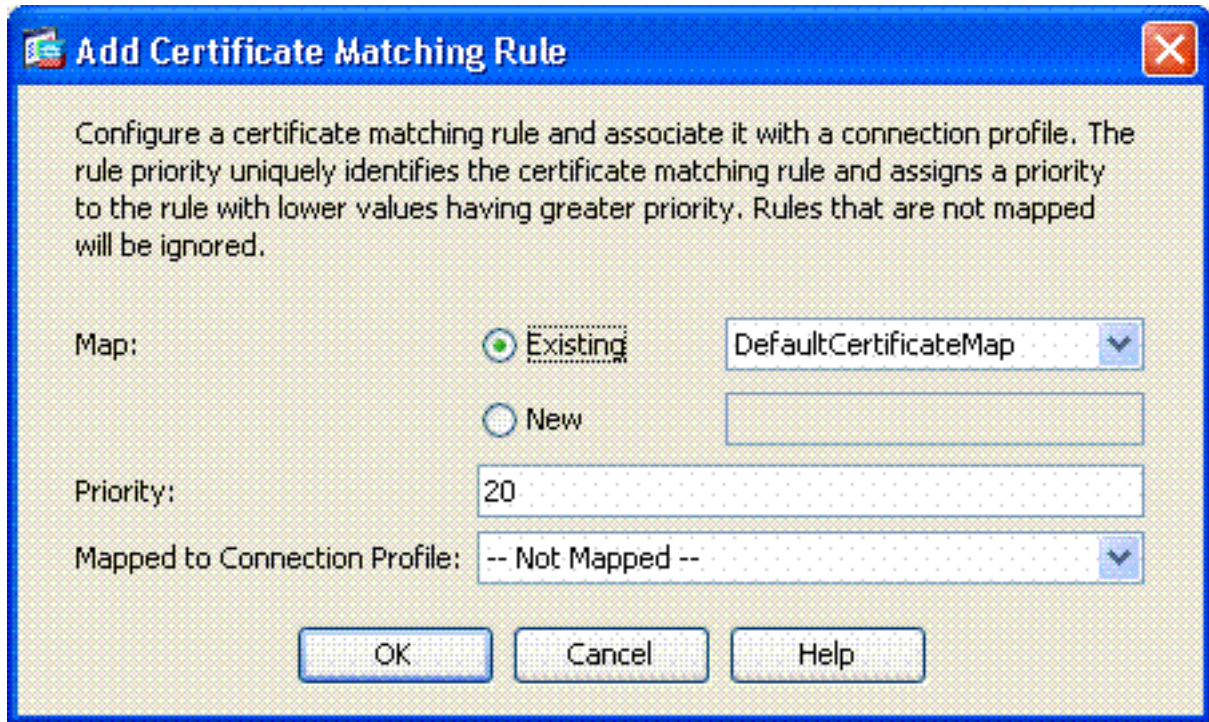
Add(추가)를 선택합니다. 사용할 그룹 별칭을 입력합니다. Enabled(활성화됨)가 선택되어 있는지 확인합니다. 그림 21을 참조하십시오.

13. 확인을 클릭합니다.

참고: 컨피그레이션을 플래시 메모리에 저장하려면 Save(저장)를 클릭합니다.

## 인증서 일치 규칙(OCSP를 사용할 경우)

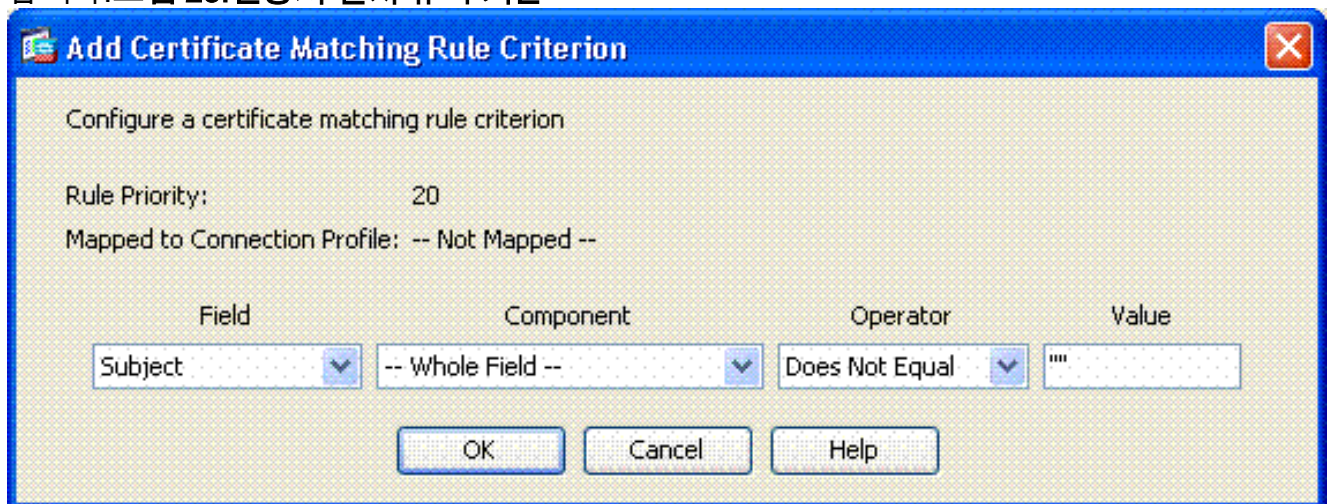
1. Remote Access VPN(원격 액세스 VPN) > Advanced(고급) > Certificate to SSL VPN Connection Profile Maps(SSL VPN에 대한 인증서 연결 프로파일 맵)를 선택합니다. 그림 22를 참조하십시오. Certificate to Connection Profile Maps(연결 프로파일 맵에 인증서) 섹션에서 Add(추가)를 선택합니다. 맵 섹션에서 기존 맵을 DefaultCertificateMap으로 유지하거나 IPsec에 인증서 맵을 이미 사용하는 경우 새 맵을 만들 수 있습니다. 규칙 우선 순위를 유지합니다. 매핑된 그룹 아래에서 — 매핑되지 않음 —으로 둡니다. 그림 22를 참조하십시오. **그림 22:인증서 일치 규칙 추가**



확인을

클릭합니다.

2. 아래쪽 테이블에서 Add를 클릭합니다.
3. Add certificate Matching Rule Criterion(인증서 일치 규칙 조건 추가) 창에서 다음 단계를 완료합니다.그림 23:인증서 일치 규칙 기준



Field(필드) 열을 Subject(제목)로 유지합니다.Component(구성 요소) 열을 Whole(전체) 필드로 유지합니다.연산자 열을 같지 않음으로 변경합니다.Value(값) 열에 큰따옴표 두 개를 입력합니다.확인 및 적용을 클릭합니다.예를 들면 그림 23을 참조하십시오.

## OCSP 구성

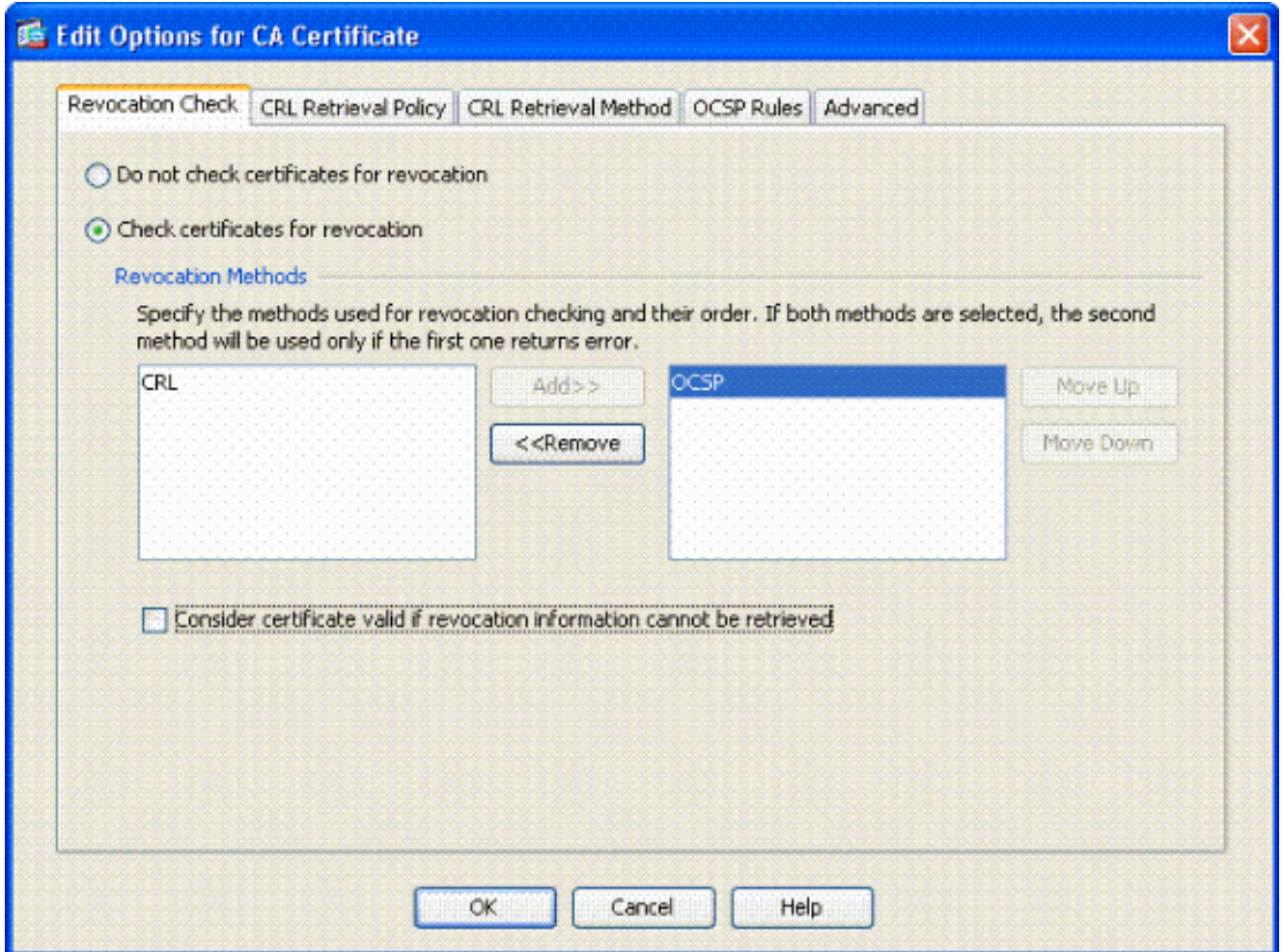
OCSP의 컨피그레이션은 OCSP responder 벤더에 따라 달라질 수 있습니다.자세한 내용은 공급업체의 설명서를 참조하십시오.

### OCSP Responder 인증서 구성

1. OCSP 응답자로부터 자체 생성된 인증서를 가져옵니다.
2. 앞서 설명한 절차를 완료하고 OSCP 서버에 대한 인증서를 설치합니다.참고: OCSP 인증서 신뢰 지점에 대해 인증서 해지 확인 안 함이 선택되었는지 확인하십시오.

## OCSP를 사용하도록 CA 구성

1. Remote Access VPN(원격 액세스 VPN) > Certificate Management(인증서 관리) > CA Certificates(CA 인증서)를 선택합니다.
2. OCSP를 사용하도록 구성할 CA를 선택하려면 OCSP를 선택합니다.
3. Edit를 클릭합니다.
4. Check certificate for revocation(인증서 해지 확인)이 선택되어 있는지 확인합니다.
5. Revocation Methods 섹션에서 OCSP를 추가합니다.그림 24를 참조하십시오.OCSP 해지 확인



6. 엄격한 OCSP 검사를 따르려면 **Consider Certificate valid...cannot be retried(유효한 인증서 고려...)**가 선택 취소되어 있는지 확인합니다.

참고: OCSP를 사용하여 취소를 수행하는 모든 CA 서버를 구성/편집합니다.

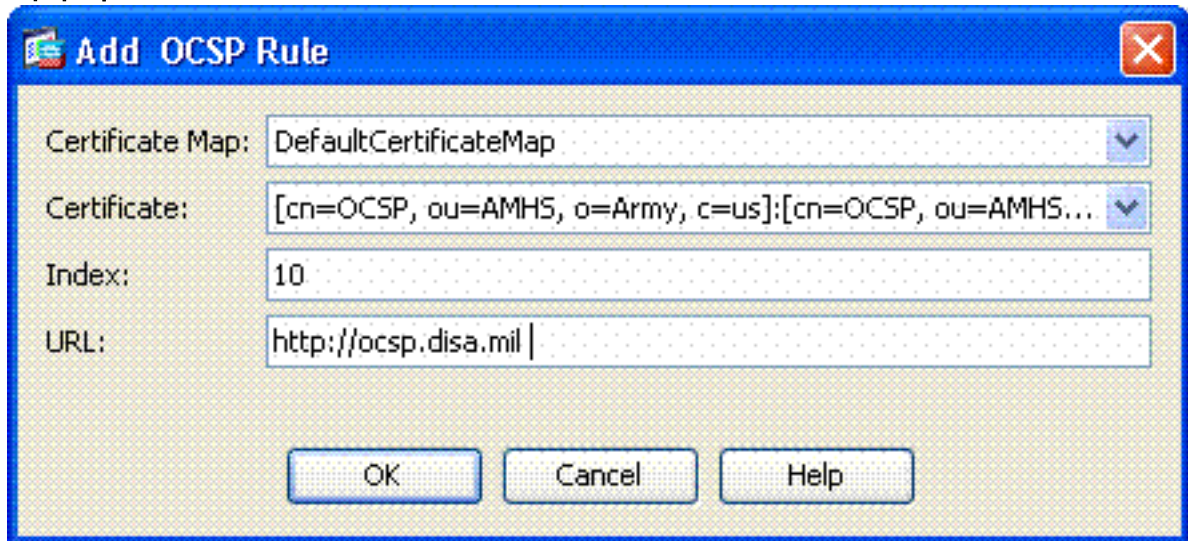
## OCSP 규칙 구성

참고: 이 단계를 완료하기 전에 인증서 그룹 일치 정책이 생성되고 OCSP 응답기가 구성되었는지 확인하십시오.

참고: 일부 OCSP 구현에서는 ASA에 DNS A 및 PTR 레코드가 필요할 수 있습니다.이 확인은 ASA가 .mil 사이트에서 제공되는지 확인하기 위해 수행됩니다.

1. Remote Access VPN(원격 액세스 VPN) > Certificate Management(인증서 관리) > CA Certificates 2를 선택합니다.
2. OCSP를 사용하도록 구성할 CA를 선택하려면 OCSP를 선택합니다.
3. 편집을 선택합니다.

4. OCSP Rule(OCSP 규칙) 탭을 클릭합니다.
5. Add를 클릭합니다.
6. OCSP 규칙 추가 창에서 다음 단계를 완료합니다.그림 25를 참조하십시오.그림 25:OCSP 규칙 추가



Certificate Map(인증서 맵) 옵션에서 DefaultCertificateMap 또는 이전에 생성한 맵을 선택합니다. Certificate(인증서) 옵션에서 OCSP responder를 선택합니다.index 옵션에 10을 입력합니다. URL 옵션에서 OCSP 응답자의 IP 주소 또는 호스트 이름을 입력합니다.호스트 이름을 사용하는 경우 ASA에 DNS 서버가 구성되어 있는지 확인합니다.확인을 클릭합니다.Apply를 클릭합니다.

## [Cisco AnyConnect 클라이언트 컨피그레이션](#)

이 섹션에서는 Cisco AnyConnect VPN 클라이언트 컨피그레이션에 대해 설명합니다.

**가정** - Cisco AnyConnect VPN Client 및 미들웨어 애플리케이션이 호스트 PC에 이미 설치되어 있습니다.ActiveCard Gold 및 ActiveClient가 테스트되었습니다.

**참고:** 이 설명서에서는 초기 AC 클라이언트 설치에만 group-url 방법을 사용합니다.AC 클라이언트가 설치되면 IPsec 클라이언트와 마찬가지로 AC 애플리케이션을 실행합니다.

**참고:** DoD 인증서 체인을 로컬 시스템에 설치해야 합니다.인증서/배치 파일을 가져오려면 PKI POC에 확인하십시오.

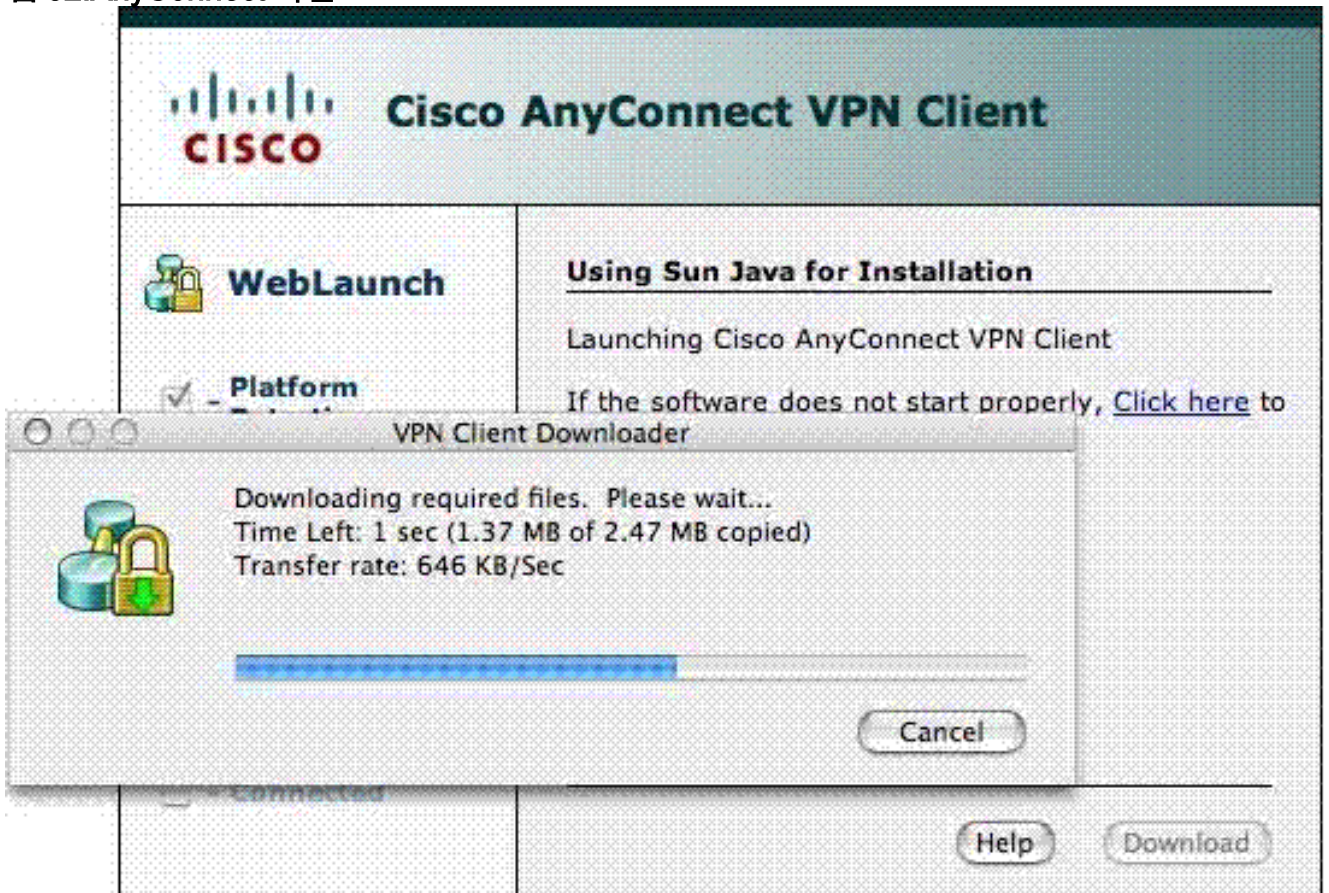
**참고:** MAC OSX용 카드 리더기 드라이버는 이미 설치되어 있으며 사용하는 현재 OS 버전과 호환됩니다.

## [Cisco Anyconnect VPN 클라이언트 다운로드 - Mac OS X](#)

1. Safari를 통해 ASA에 대한 웹 세션을 시작합니다.주소는 https://Outside-Interface 형식이어야 합니다.예: https://172.18.120.225.
2. ASA의 인증서를 확인하라는 팝업 창이 나타납니다.Continue(계속)를 클릭합니다.
3. CAC 키 체인의 잠금을 해제하기 위해 다른 팝업 창이 나타납니다.핀 번호를 입력합니다.그림 31을 참조하십시오.그림 31:PIN 입력



4. SSL VPN-service 웹 페이지가 나타나면 Continue(계속)를 클릭합니다.
5. 키 체인의 잠금을 해제하면 ASA에서 인증서를 신뢰하는 경우 브라우저에 프롬프트가 표시됩니다. 신뢰를 클릭합니다.
6. 보안 연결을 설정하기 위해 키 체인의 잠금을 해제하려면 루트 비밀번호를 입력한 다음 확인을 클릭합니다.
7. 클라이언트 인증에 사용할 인증서를 선택한 다음 확인을 클릭합니다.
8. 그런 다음 브라우저는 AnyConnect 클라이언트 다운로드를 허용하기 위해 루트/사용자 비밀번호를 요청합니다.
9. 인증된 경우 AnyConnect 클라이언트가 다운로드되기 시작합니다.그림 32를 참조하십시오.그림 32:AnyConnect 다운로드



10. 애플리케이션이 다운로드되면 브라우저에서 ASA 인증서를 승인하라는 메시지를 표시합니다. Accept(수락)를 클릭합니다.
11. 연결이 설정되었습니다.그림 33.그림 33:AnyConnect 연결



## [Cisco AnyConnect VPN 클라이언트 시작 - Mac OS X](#)

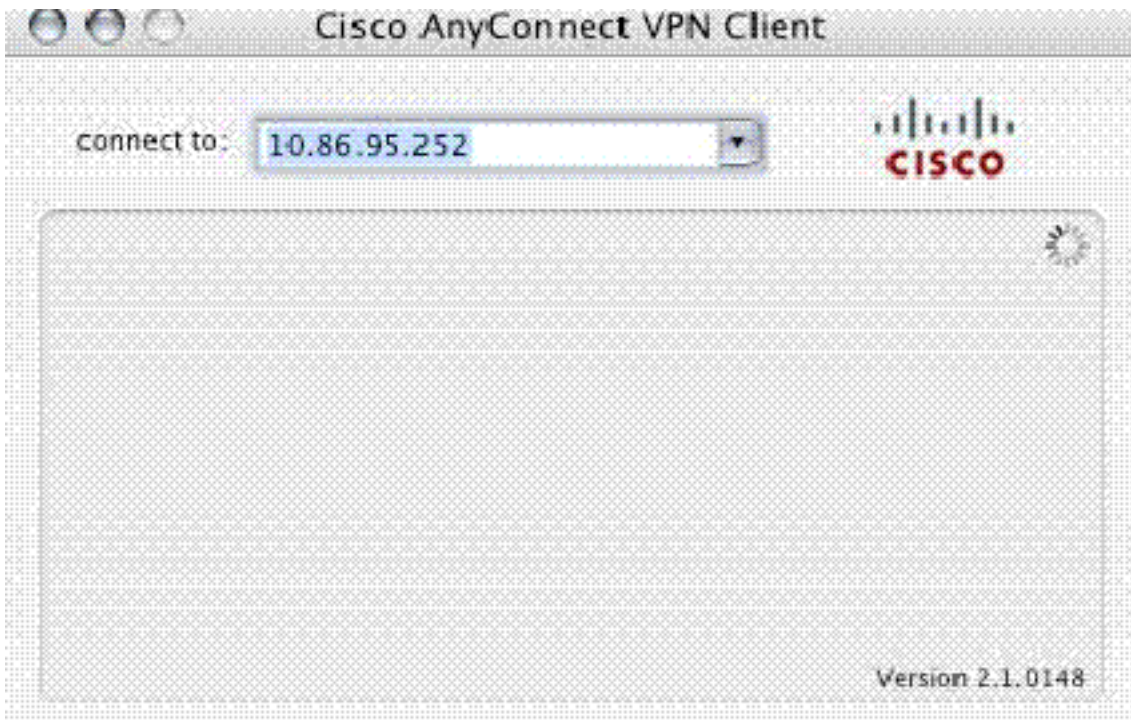
Finder에서—Applications > Cisco AnyConnect VPN Client

참고: AnyConnect 클라이언트 프로파일 컨피그레이션 옵션은 부록 E를 참조하십시오.

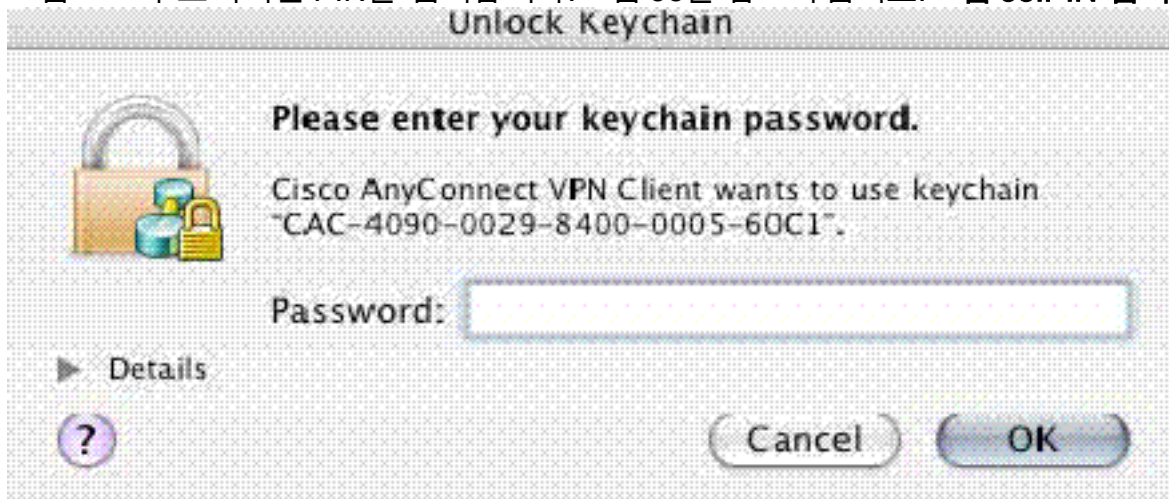
### [새 연결](#)

AC 창이 나타납니다.그림 37을 참조하십시오.

그림 37:새 VPN 연결



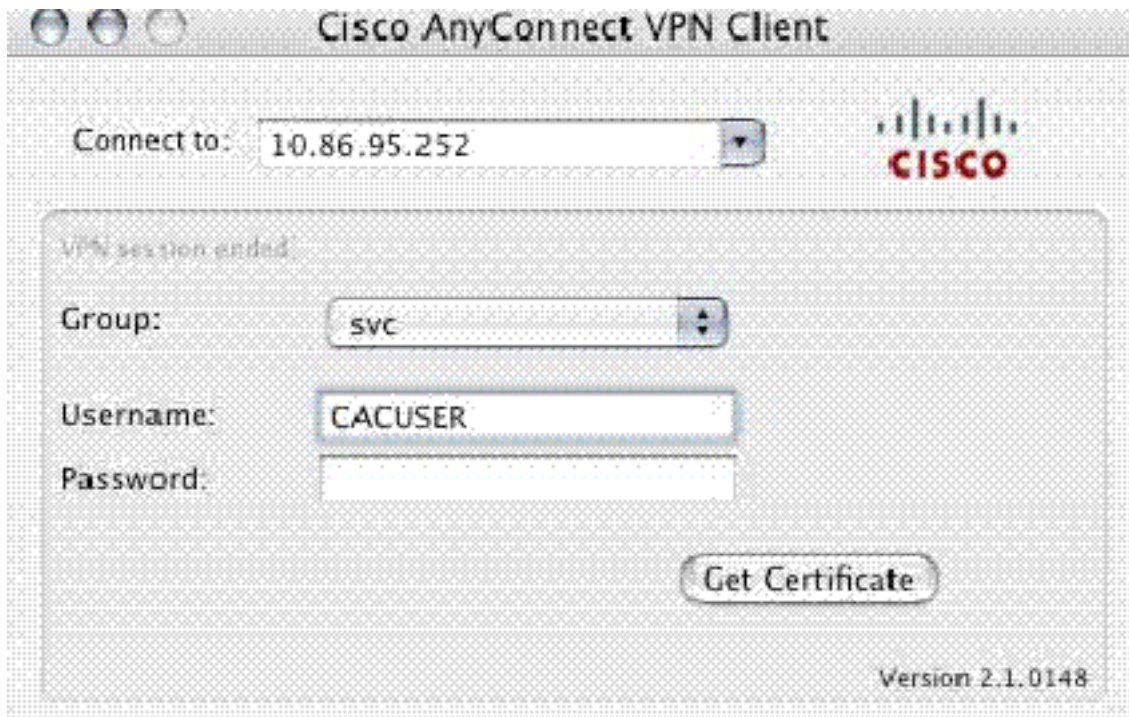
1. AC에서 자동으로 연결을 시도하지 않는 경우 적절한 호스트를 선택합니다.
2. 프롬프트가 표시되면 PIN을 입력합니다.그림 38을 참조하십시오.그림 38:PIN 입력



## 원격 액세스 시작

1. 연결할 그룹 및 호스트를 선택합니다.
2. 인증서가 사용되므로 **Connect(연결)**를 선택하여 VPN을 설정합니다.그림 39를 참조하십시오.  
.참고: 연결에서 인증서를 사용하므로 사용자 이름과 비밀번호를 입력할 필요가 없습니다.그림 39:연결 중





참고:

AnyConnect 클라이언트 프로파일 컨피그레이션 옵션은 부록 E를 참조하십시오.

## 부록 A - LDAP 매핑 및 DAP

ASA/PIX 릴리스 7.1(x) 이상에서는 LDAP 매핑이라는 기능이 도입되었습니다. 이는 Cisco 특성과 LDAP 객체/특성 간의 매핑을 제공하는 강력한 기능으로서 LDAP 스키마 변경이 필요하지 않습니다. CAC 인증 구현의 경우 원격 액세스 연결에 대한 추가 정책 시행을 지원할 수 있습니다. 다음은 LDAP 매핑의 예입니다. AD/LDAP 서버를 변경하려면 관리자 권한이 필요합니다. ASA 8.x 소프트웨어에서 DAP(Dynamic Access Policy) 기능이 도입되었습니다. DAP는 CAC와 함께 작동하여 여러 AD 그룹과 푸시 정책, ACL 등을 살펴볼 수 있습니다.

### 시나리오 1: 원격 액세스 권한 다이얼인을 사용한 Active Directory 적용 - 액세스 허용/거부

이 예에서는 AD 특성 msNPAllowDailin을 Cisco의 특성 cVPN3000-Tunneling-Protocol에 매핑합니다.

- AD 특성 값: TRUE = 허용; FALSE = 거부
- Cisco 특성 값: 1 = FALSE, 4(IPSec) 또는 20(4 IPSEC + 16 WebVPN) = TRUE, ALLOW 조건의 경우 다음을 매핑합니다.

- TRUE = 20

DENY 전화 접속 조건의 경우 다음을 매핑합니다.

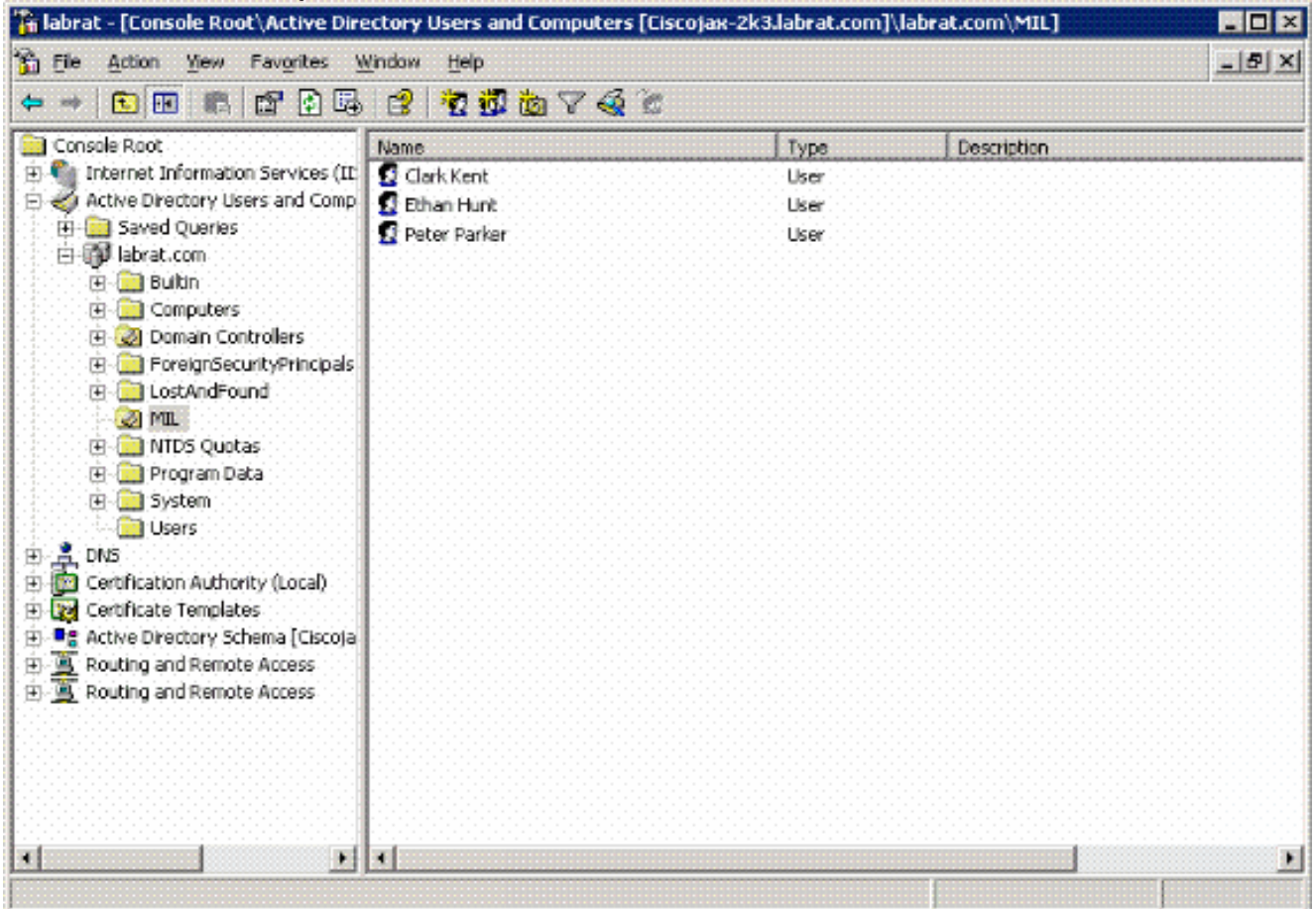
- FALSE = 1

참고: TRUE 및 FALSE가 모두 대문자로 표시되는지 확인합니다. 자세한 내용은 [Security Appliance 사용자 권한 부여를 위한 외부 서버 구성](#)을 참조하십시오.

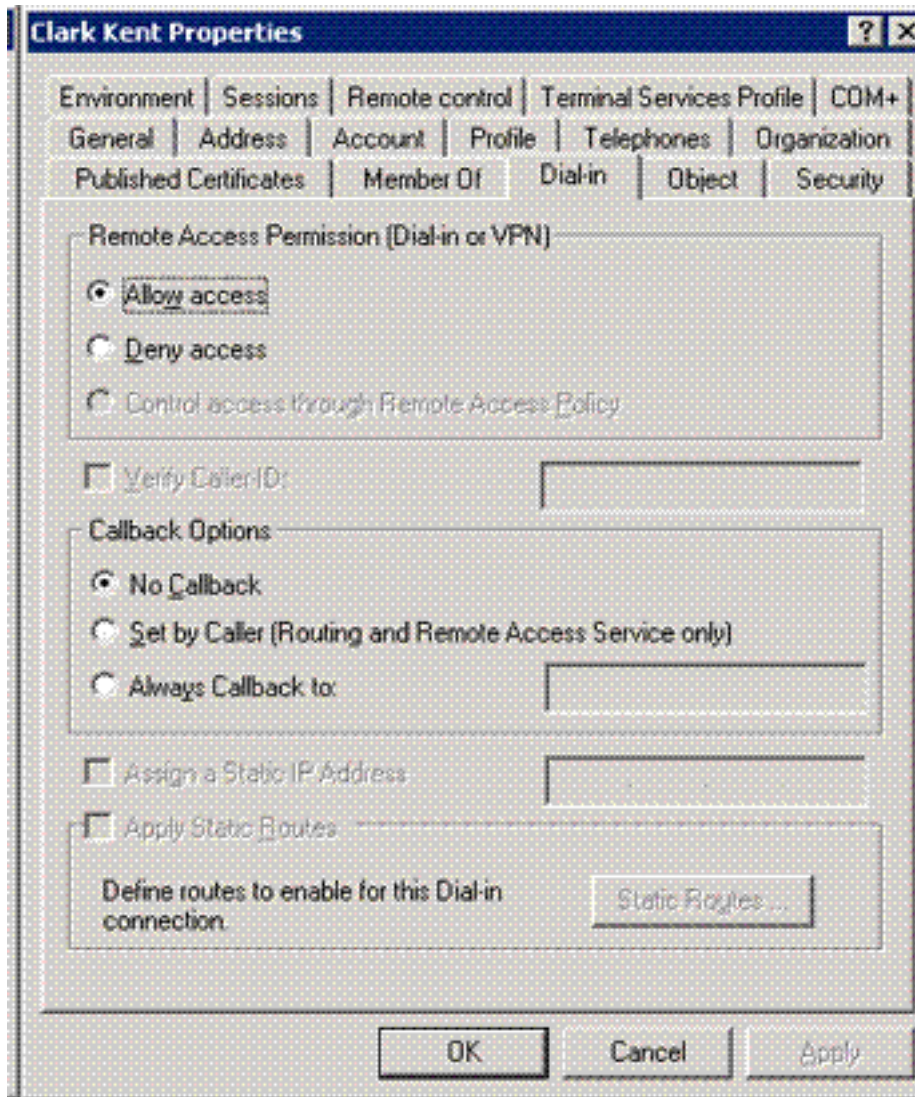
### Active Directory 설정

1. Active Directory Server에서 시작 > 실행을 클릭합니다.

2. 열기 텍스트 상자에 dsa.msc를 입력한 다음 **확인**을 클릭합니다.이렇게 하면 Active Directory 관리 콘솔이 시작됩니다.
3. Active Directory 관리 콘솔에서 더하기 기호를 클릭하여 Active Directory 사용자 및 컴퓨터를 확장합니다.
4. 도메인 이름을 확장하려면 더하기 기호를 클릭합니다.
5. 사용자를 위해 OU를 만든 경우 모든 사용자를 보려면 OU를 확장합니다.모든 사용자가 Users 폴더에 할당된 경우 해당 폴더를 확장하여 해당 사용자를 봅니다.그림 A1을 참조하십시오.**그림 A1:Active Directory 관리 콘솔**



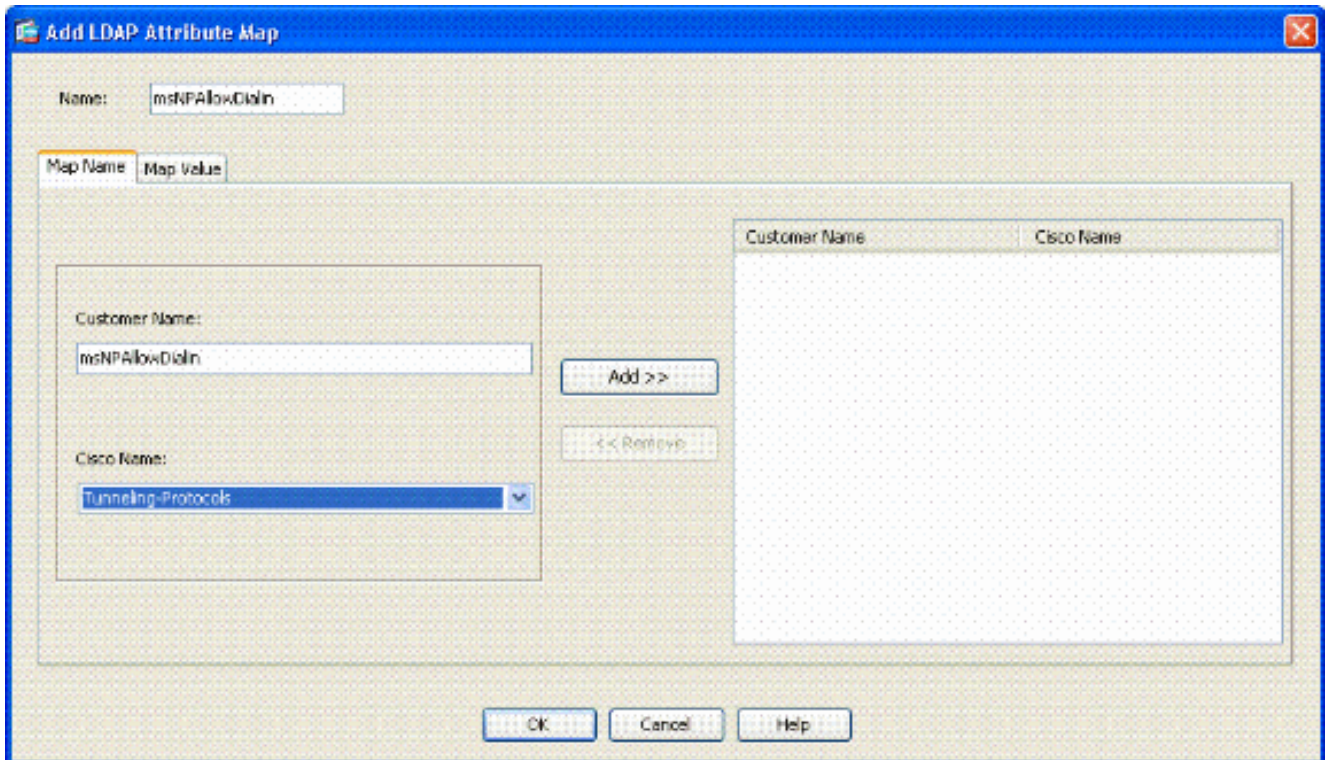
6. 편집할 사용자를 두 번 클릭합니다.사용자 속성 페이지에서 전화 접속 탭을 클릭하고 **허용** 또는 **거부**를 클릭합니다.그림 A2를 참조하십시오.**그림 A2:사용자 속성**



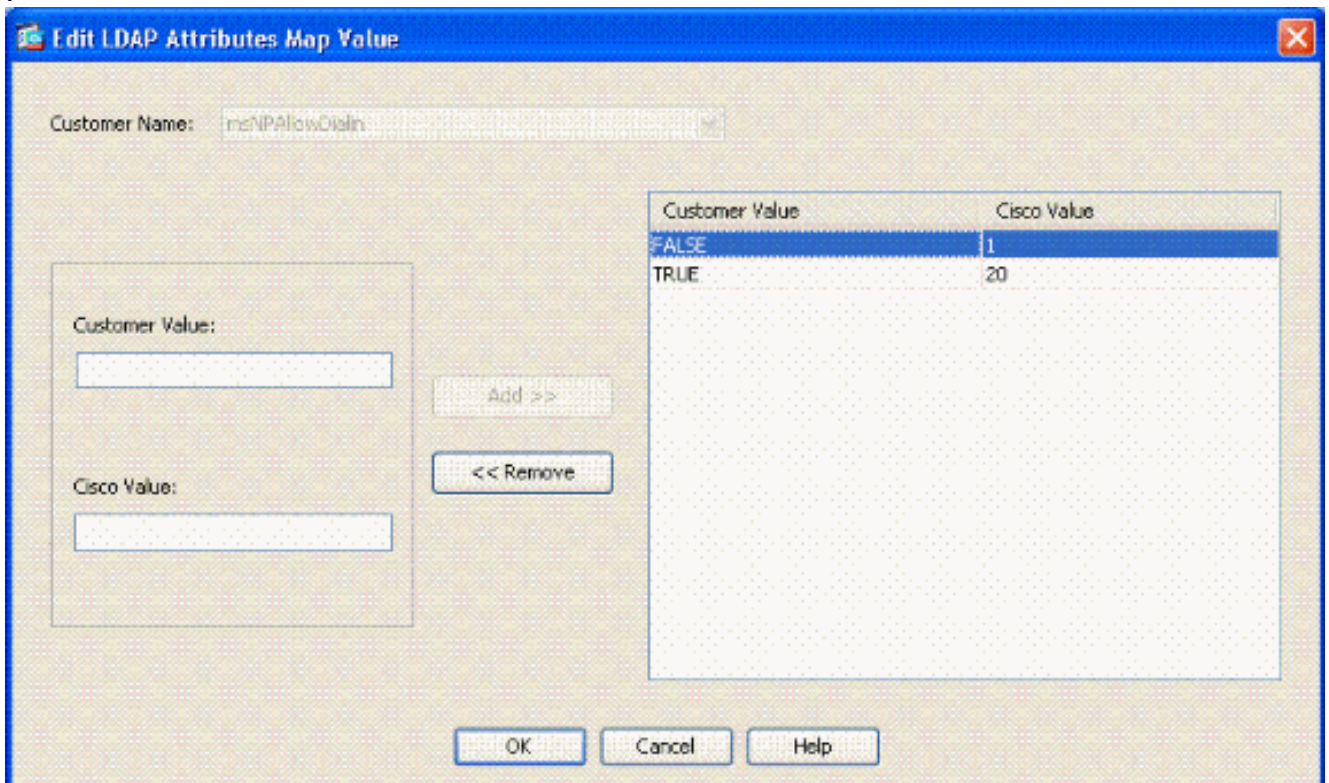
7. 그런 다음 **확인**을 클릭합니다.

## [ASA 컨피그레이션](#)

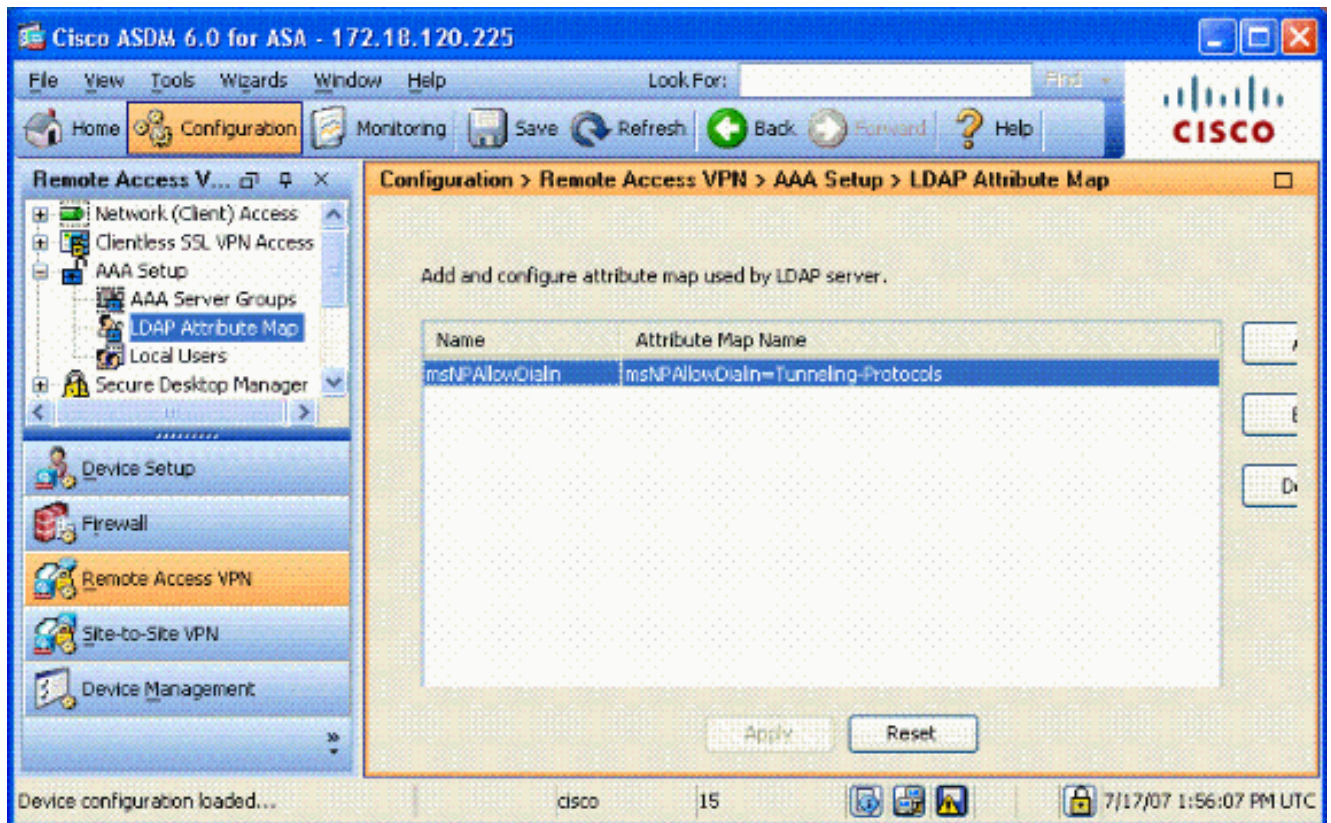
1. ASDM에서 Remote Access VPN(원격 액세스 VPN) > AAA Setup(AAA 설정) > LDAP Attribute Map(LDAP 특성 맵)을 선택합니다.
2. Add(추가)를 클릭합니다.
3. Add LDAP Attribute Map(LDAP 특성 맵 추가) 창에서 다음 단계를 완료합니다.그림 A3를 참조 하십시오.그림 A3:LDAP 특성 맵 추가



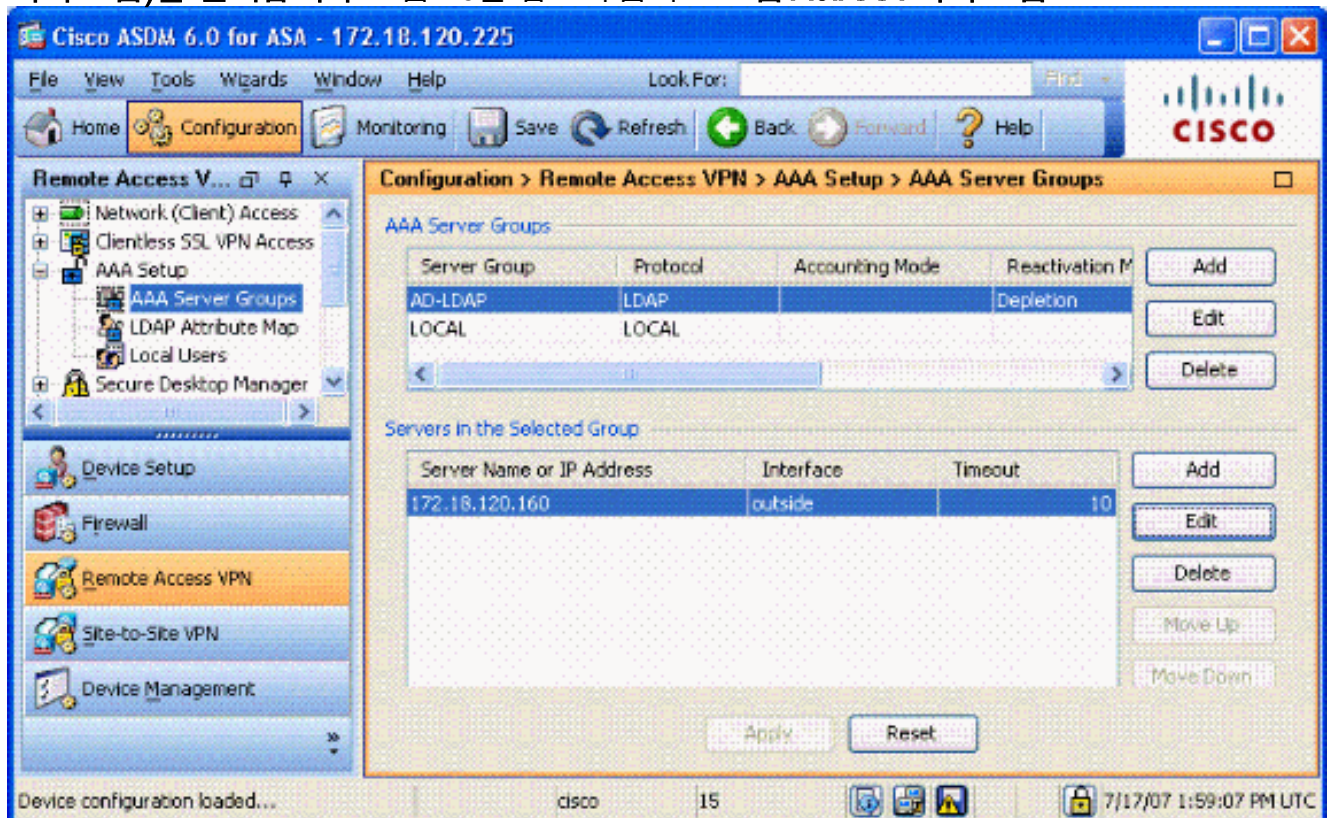
이름 텍스트 상자에 이름을 입력합니다. Map Name(맵 이름) 탭의 Customer Name(고객 이름) 텍스트 상자에 msNPAllowDialin을 입력합니다. Map Name(맵 이름) 탭의 Cisco Name(Cisco 이름)의 드롭다운 옵션에서 Tunneling-Protocols(터널링 프로토콜)를 선택합니다. Add(추가)를 클릭합니다. Map Value 탭을 선택합니다. Add(추가)를 클릭합니다. Add Attribute LDAP Map Value(특성 LDAP 맵 값 추가) 창에서 Customer Name(고객 이름) 텍스트 상자에 TRUE를 입력하고 Cisco Value(Cisco 값) 텍스트 상자에 20을 입력합니다. Add(추가)를 클릭합니다. 고객 이름 텍스트 상자에 FALSE를 입력하고 Cisco 값 텍스트 상자에 1을 입력합니다. 그림 A4를 참조하십시오



확인을 클릭합니다. 확인을 클릭합니다. 적용을 클릭합니다. 구성은 그림 A5와 같아야 합니다. 그림 A5:LDAP 특성 맵 컨피그레이션



4. Remote Access VPN(원격 액세스 VPN) > AAA Setup(AAA 설정) > AAA Server Groups(AAA 서버 그룹)를 선택합니다.그림 A6를 참조하십시오.그림 A6:AAA 서버 그룹



5. 편집할 서버 그룹을 클릭합니다.Servers in the Selected Group(선택한 그룹의 서버) 섹션에서 서버 IP 주소 또는 호스트 이름을 선택한 다음 Edit(수정)를 클릭합니다.
6. Edit AAA Server(AAA 서버 수정) 창의 LDAP Attribute Map(LDAP 특성 맵) 텍스트 상자에서 드롭다운 메뉴에서 생성된 LDAP 특성 맵을 선택합니다.그림 A7 참조그림 A7:LDAP 특성 맵

추가

7. 확인을 클릭합니다.

참고: LDAP 바인딩 및 특성 매핑이 제대로 작동하는지 확인하기 위해 테스트하는 동안 LDAP 디버깅을 켜십시오. 문제 해결 명령은 부록 C를 참조하십시오.

## 시나리오 2: 액세스 허용/거부에 그룹 구성원 자격을 사용하는 Active Directory 시행

이 예에서는 LDAP 특성 memberOf를 사용하여 그룹 멤버십을 조건으로 설정하기 위해 터널링 프로토콜 특성에 매핑합니다. 이 정책이 작동하려면 다음 조건이 있어야 합니다.

- 이미 존재하는 그룹을 사용하거나 ASA VPN 사용자가 ALLOW 조건의 멤버가 되도록 새 그룹을 만듭니다.
- ASA 사용자가 아닌 사용자가 DENY 조건의 멤버가 되도록 이미 존재하는 그룹을 사용하거나 새 그룹을 생성합니다.
- LDAP 뷰어에서 그룹에 적합한 DN이 있는지 확인합니다. 부록 D를 참조하십시오. DN이 잘못되면 매핑이 제대로 작동하지 않습니다.

**참고:** ASA는 이 릴리스에서 memberOf 특성의 첫 번째 문자열만 읽을 수 있습니다. 새로 만든 그룹이 목록의 맨 위에 있는지 확인합니다. 다른 옵션은 AD에서 특수 문자를 먼저 볼 때 이름 앞에 특수 문자를 넣는 것입니다. 이 문제를 해결하려면 8.x 소프트웨어에서 DAP를 사용하여 여러 그룹을 살펴보세요.

**참고:** 사용자가 거부 그룹의 일부인지 또는 최소한 하나의 다른 그룹에 속해 있는지 확인하여 memberOf가 항상 ASA로 다시 전송되도록 하십시오. FALSE 거부 조건을 지정할 필요는 없지만 가장 좋은 방법은 이 조건을 지정하는 것입니다. 기존 그룹 이름 또는 그룹 이름에 공백이 포함된 경우 다음과 같이 특성을 입력합니다.

CN=Backup Operators,CN=Builtin,DC=gsgseclab,DC=org

**참고:** DAP를 사용하면 ASA에서 memberOf 특성의 여러 그룹을 확인하고 그룹의 기본 권한 부여를 확인할 수 있습니다. DAP 섹션을 참조하십시오.

## 매핑

- AD 특성 값: memberOf CN=ASAUsers,CN=사용자,DC=gsgseclab,DC=org memberOf CN=TelnetClients,CN=사용자,DC=labat,DC=com
- Cisco 특성 값: 1 = FALSE, 20 = TRUE, ALLOW 조건에 대해 매핑합니다.

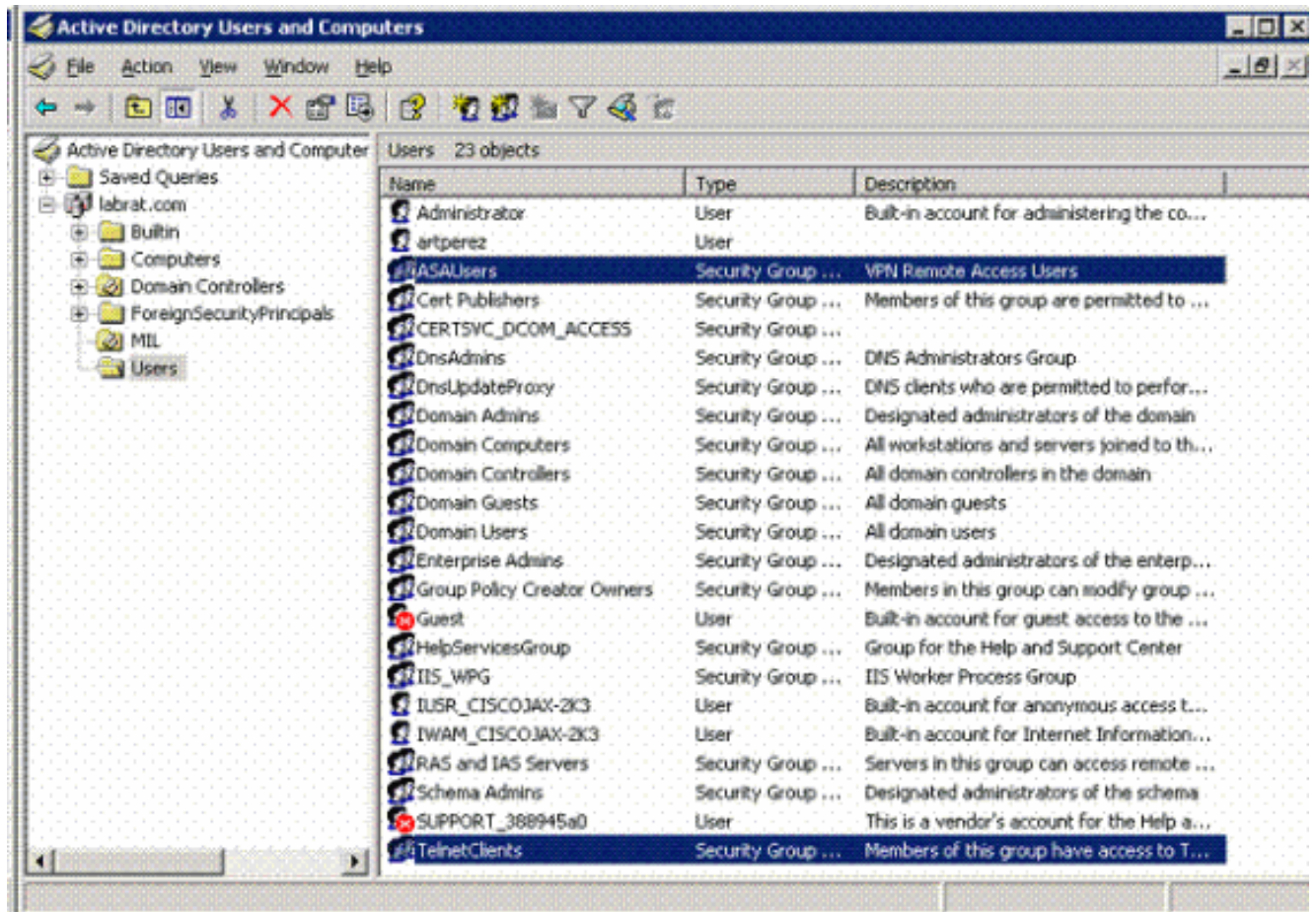
- memberOf CN=ASAUsers,CN=사용자,DC=gsgseclab,DC=org = 20 DENY 조건에 대해 매핑합니다.

- memberOf CN=TelnetClients,CN=사용자,DC=gsgseclab,DC=org = 1

**참고:** 향후 릴리스에서는 연결을 허용하거나 거부하는 Cisco 특성이 있습니다. Cisco 특성에 [대한 자세한 내용은 Security Appliance 사용자 권한 부여를 위한 외부 서버 구성](#)을 참조하십시오.

## Active Directory 설정

1. Active Directory Server에서 시작 > 실행을 선택합니다.
2. 열기 텍스트 상자에 dsa.msc를 입력한 다음 확인을 클릭합니다. 이렇게 하면 Active Directory 관리 콘솔이 시작됩니다.
3. Active Directory 관리 콘솔에서 더하기 기호를 클릭하여 Active Directory 사용자 및 컴퓨터를 확장합니다. 그림 A8 참조 **그림 A8: Active Directory 그룹**

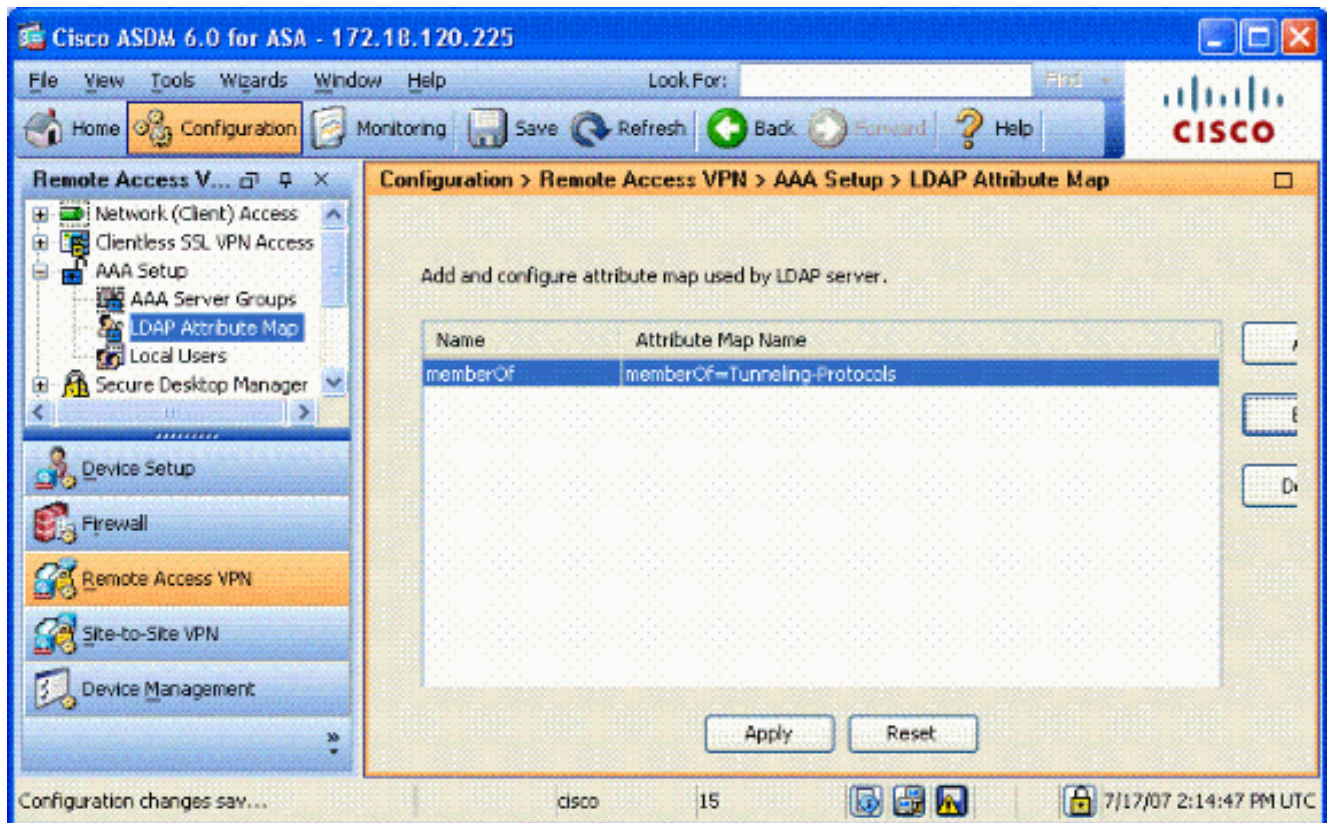


4. 도메인 이름을 확장하려면 더하기 기호를 클릭합니다.
5. **Users** 폴더를 마우스 오른쪽 버튼으로 클릭하고 **New(새로 만들기) > Group(그룹)**을 선택합니다.
6. 그룹 이름을 입력합니다.예:ASAUsers입니다.
7. **확인**을 클릭합니다.
8. **Users** 폴더를 클릭한 다음 방금 만든 그룹을 두 번 클릭합니다.
9. 멤버 탭을 선택한 다음 **추가**를 클릭합니다.
10. 추가할 사용자의 이름을 입력한 다음 **확인**을 클릭합니다.

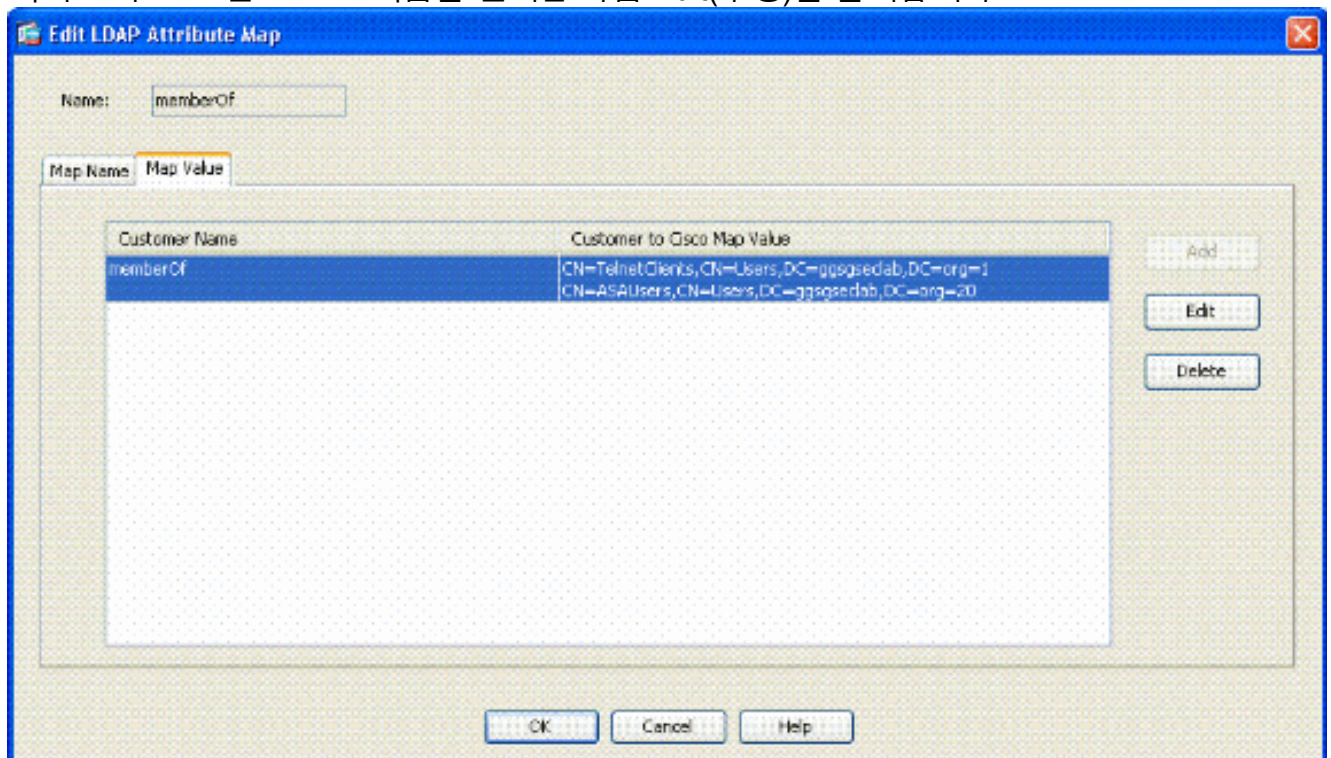
## ASA 컨피그레이션

1. ASDM에서 **Remote Access VPN(원격 액세스 VPN) > AAA Setup(AAA 설정) > LDAP Attribute Map(LDAP 특성 맵)**을 선택합니다.
2. **Add(추가)**를 클릭합니다.
3. Add LDAP Attribute Map(LDAP 특성 맵 추가) 창에서 다음 단계를 완료합니다.그림 A3를 참조하십시오.이름 텍스트 상자에 이름을 입력합니다.Map Name(맵 이름) 탭에서 Customer Name(고객 이름) 텍스트 상자 c에 memberOf를 입력합니다.Map Name(맵 이름) 탭의 Cisco Name(Cisco 이름)의 드롭다운 옵션에서 Tunneling-Protocols(터널링 프로토콜)를 선택합니다.**Add(추가)**를 선택합니다.**Map Value** 탭을 클릭합니다.**Add(추가)**를 선택합니다.Add Attribute LDAP Map Value(특성 LDAP 맵 값 추가) 창에 **CN=ASAUsers,CN=Users,DC=gsgseclab,DC=org**를 Customer Name(고객 이름) 텍스트 상자에 입력하고 Cisco Value(Cisco 값) 텍스트 상자에 **20**를 입력합니다.**Add(추가)**를 클릭합니다.**고객 이름** 텍스트 상자에 **CN=TelnetClients,CN=Users,DC=gsgseclab,DC=org**를 입력하고 Cisco 값 텍스트 상자에 **1**를 입력합니다.그림 A4를 참조하십시오.**확인**을 클릭합니다.**확인**을 클릭합니다.**Apply**를 클릭합니다.구성은 그림 A9와 같아야 합니다.그림 A9 LDAP 특성 맵





4. Remote Access VPN(원격 액세스 VPN) > AAA Setup(AAA 설정) > AAA Server Groups(AAA 서버 그룹)를 선택합니다.
5. 편집할 서버 그룹을 클릭합니다.Servers in the Selected Group(선택한 그룹의 서버) 섹션에서 서버 IP 주소 또는 호스트 이름을 선택한 다음 Edit(수정)를 클릭합니다



6. Edit AAA Server(AAA 서버 수정) 창의 LDAP Attribute Map(LDAP 특성 맵) 텍스트 상자에서 드롭다운 메뉴에서 생성된 LDAP 특성 맵을 선택합니다.
7. 확인을 클릭합니다.

**참고:** LDAP 바인딩 및 특성 매핑이 제대로 작동하는지 확인하기 위해 테스트하는 동안 LDAP 디버깅을 켜십시오.문제 해결 명령은 부록 C를 참조하십시오.

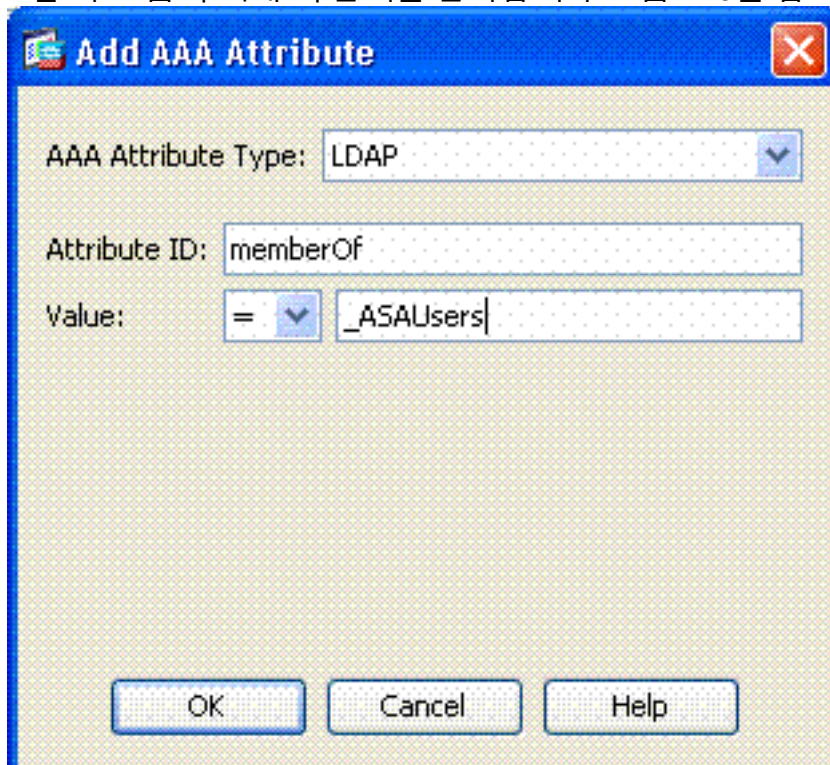
## 시나리오 3: 여러 MemberOf 특성에 대한 동적 액세스 정책

이 예에서는 DAP를 사용하여 여러 memberOf 특성을 확인하여 Active Directory 그룹 멤버십을 기반으로 액세스를 허용합니다. 8.x 이전 버전에서는 ASA가 첫 번째 memberOf 특성만 읽었습니다. 8.x 이상에서는 ASA에서 모든 memberOf 특성을 살펴볼 수 있습니다.

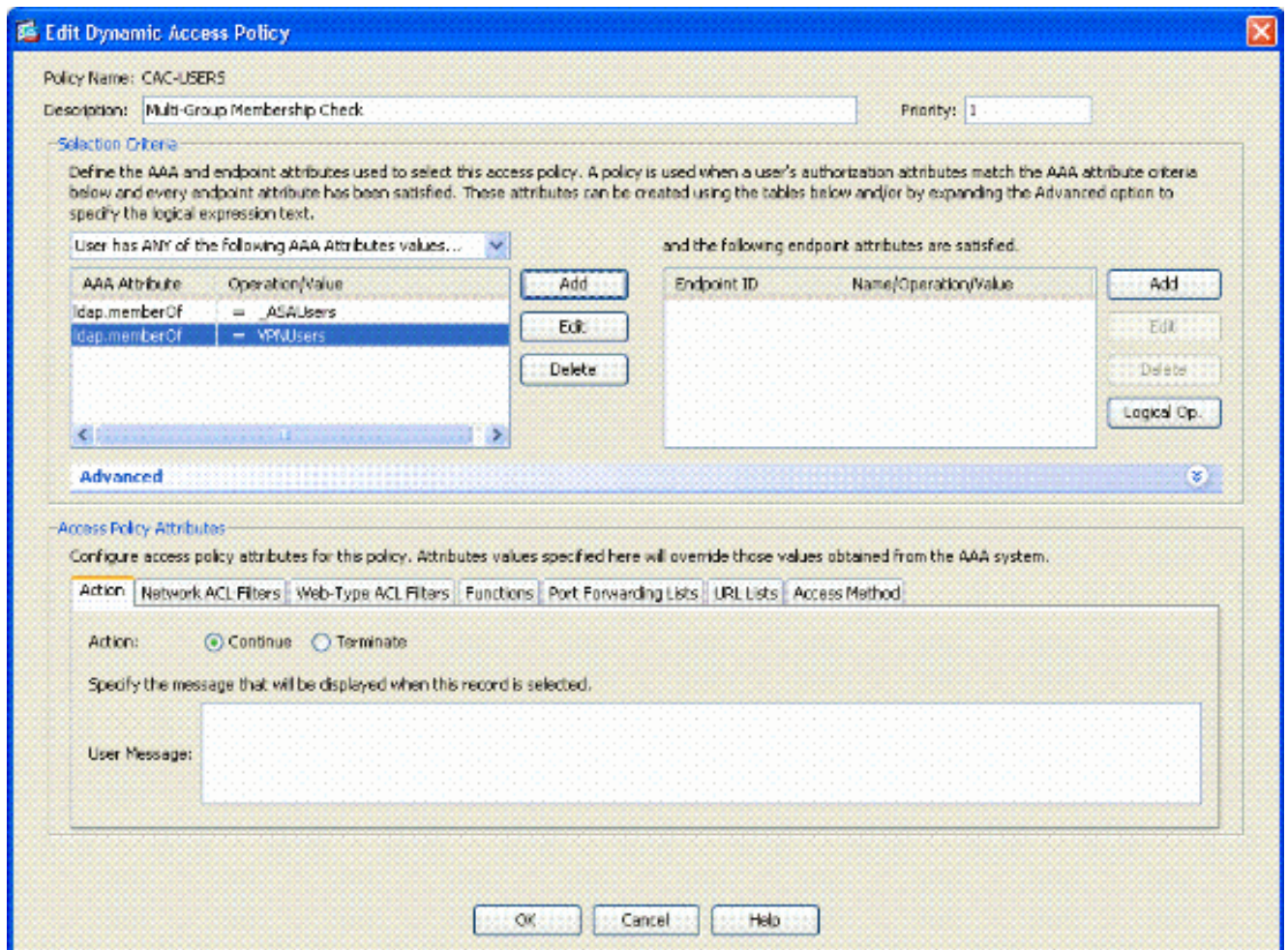
- ASA VPN 사용자가 ALLOW 조건의 멤버가 되도록 이미 존재하는 그룹을 사용하거나 새 그룹 (또는 여러 그룹)을 생성합니다.
- ASA 사용자가 아닌 사용자가 DENY 조건의 멤버가 되도록 이미 존재하는 그룹을 사용하거나 새 그룹을 생성합니다.
- LDAP 뷰어에서 그룹에 적합한 DN이 있는지 확인합니다. 부록 D를 참조하십시오. DN이 잘못되면 매핑이 제대로 작동하지 않습니다.

## ASA 컨피그레이션

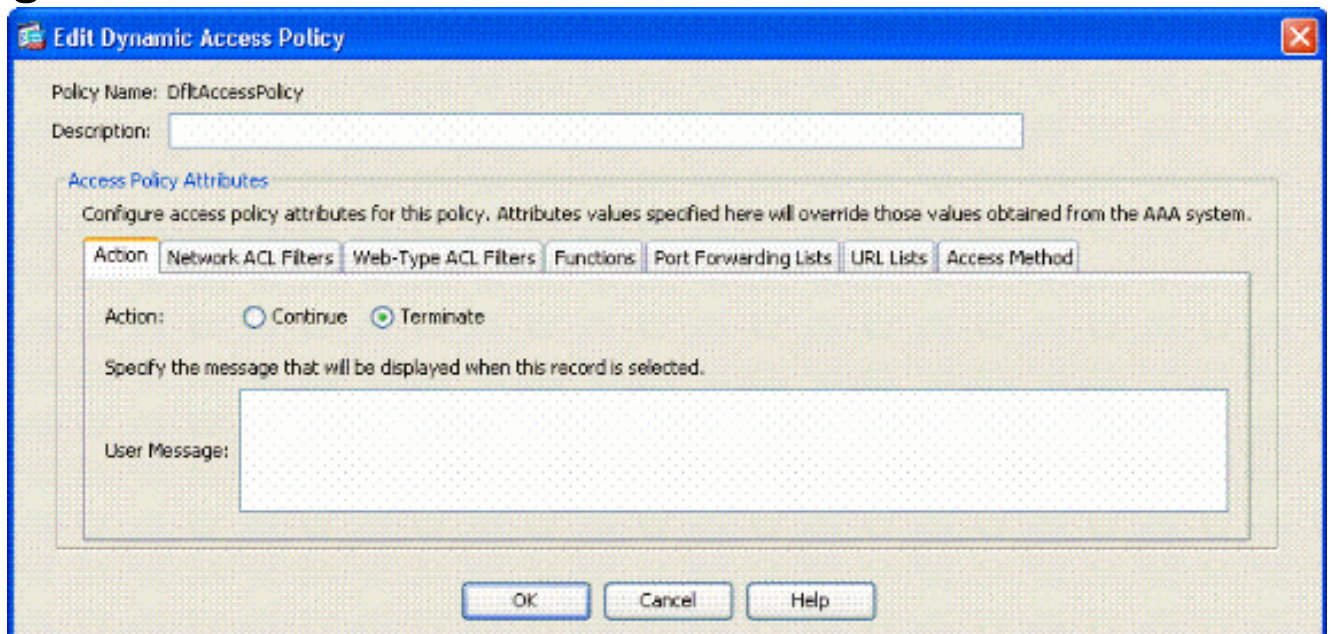
1. ASDM에서 Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Dynamic Access Policies(동적 액세스 정책)를 선택합니다.
2. Add(추가)를 클릭합니다.
3. Add Dynamic Access Policy(동적 액세스 정책 추가)에서 다음 단계를 완료합니다. 이름 텍스트 상자 b에 이름을 입력합니다. 우선 순위 섹션에서 1 또는 0보다 큰 숫자를 입력합니다. 선택 기준에서 추가를 클릭합니다. Add AAA Attribute(AAA 특성 추가)에서 LDAP를 선택합니다. 특성 ID 섹션에서 memberOf를 입력합니다. 값 섹션에서 =을 선택하고 AD 그룹 이름을 입력합니다. 참조할 각 그룹에 대해 이 단계를 반복합니다. 그림 A10을 참조하십시오. 그림 A10 AAA 특



성 맵 확인을 클릭합니다. Access Policy Attributes(액세스 정책 특성) 섹션에서 Continue(계속)를 선택합니다. 그림 A11을 참조하십시오. 그림 A11 동적 정책 추가



4. ASDM에서 Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Dynamic Access Policies(동적 액세스 정책)를 선택합니다.
5. Default Access Policy(기본 액세스 정책)를 선택하고 Edit(수정)를 선택합니다.
6. 기본 작업은 Terminate로 설정해야 합니다.그림 A12를 참조하십시오.그림 A12 동적 정책 수정



7. 확인을 클릭합니다.

참고: Terminate(종료)를 선택하지 않은 경우, 기본값이 Continue(계속)이므로 그룹에 없는 경우에도 가 허용됩니다.

## 부록 B - ASA CLI 컨피그레이션

### ASA 5510

```
ciscoasa#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname asa80
domain-name army.mil
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address x.x.x.x 255.255.255.128
!
interface GigabitEthernet0/1
nameif inside
security-level 100
no ip address
!
boot system disk0:/asa802-k8.bin
ftp mode passive
dns server-group DefaultDNS
domain-name army.mil
!
-----ACL's-----
-----
access-list out extended permit ip any any
-----
-----
pager lines 24
logging console debugging
mtu outside 1500
!
-----VPN Pool-----
-----
ip local pool CAC-USERS 192.168.1.1-192.168.1.254 mask
255.255.255.0
-----
-----
!
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin
no asdm history enable
arp timeout 14400
access-group out in interface outside
route outside 0.0.0.0 0.0.0.0 172.18.120.129 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat
0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect
0:02:00
```

```
timeout uauth 0:05:00 absolute
!
-----LDAP Maps & DAP-----
-----
ldap attribute-map memberOf
map-name memberOf Tunneling-Protocols
March 11, 2008 ASA - CAC Authentication for AnyConnect
VPN Access
Company Confidential. A printed copy of this document is
considered uncontrolled.
49
map-value memberOf
CN=_ASAUsers,CN=Users,DC=gsgseclab,DC=org 20
ldap attribute-map msNPAllowDialin
map-name msNPAllowDialin Tunneling-Protocols
map-value msNPAllowDialin FALSE 1
map-value msNPAllowDialin TRUE 20
dynamic-access-policy-record CAC-USERS
description "Multi-Group Membership Check"
priority 1
dynamic-access-policy-record DfltAccessPolicy
action terminate
-----
-----
!
-----LDAP Server-----
-----
aaa-server AD-LDAP protocol ldap
aaa-server AD-LDAP (outside) host 172.18.120.160
ldap-base-dn CN=Users,DC=gsgseclab,DC=org
ldap-scope onelevel
ldap-naming-attribute userPrincipalName
ldap-login-password *
ldap-login-dn
CN=Administrator,CN=Users,DC=gsgseclab,DC=org
-----
-----
!
aaa authentication http console LOCAL
http server enable 445
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
!
-----CA Trustpoints-----
-----
crypto ca trustpoint ASDM_TrustPoint0
revocation-check ocsp
enrollment terminal
keypair DoD-1024
match certificate DefaultCertificateMap override ocsp
trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
crl configure
crypto ca trustpoint ASDM_TrustPoint1
revocation-check ocsp
enrollment terminal
fqdn asa80
subject-name CN=asa80,OU=PKI,OU=DoD,O=U.S.
Government,C=US
keypair DoD-1024
match certificate DefaultCertificateMap override ocsp
```

```
trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
no client-types
crl configure
crypto ca trustpoint ASDM_TrustPoint2
revocation-check ocsp
enrollment terminal
keypair DoD-2048
match certificate DefaultCertificateMap override ocsp
trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
no client-types
crl configure
crypto ca trustpoint ASDM_TrustPoint3
revocation-check ocsp none
enrollment terminal
crl configure
!
-----Certificate Map-----
-----
crypto ca certificate map DefaultCertificateMap 10
subject-name ne ""
-----CA Certificates (Partial Cert is
Shown)-----
crypto ca certificate chain ASDM_TrustPoint0
certificate ca 37
3082044c 30820334 a0030201 02020137 300d0609 2a864886
f70d0101
05050030
60310b30 09060355 04061302 55533118 30160603 55040a13
0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c
300a0603
55040b13
03504b49 311b3019 06035504 03131244 6f44204a 49544320
526f6f74
crypto ca certificate chain ASDM_TrustPoint1
certificate 319e
30820411 3082037a a0030201 02020231 9e300d06 092a8648
86f70d01
01050500
305c310b 30090603 55040613 02555331 18301606 0355040a
130f552e
532e2047
6f766572 6e6d656e 74310c30 0a060355 040b1303 446f4431
0c300a06
0355040b
crypto ca certificate chain ASDM_TrustPoint2
certificate ca 37
3082044c 30820334 a0030201 02020137 300d0609 2a864886
f70d0101
05050030
60310b30 09060355 04061302 55533118 30160603 55040a13
0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c
300a0603
55040b13
f766e045 f15ddb43 9549dle9 a0ea6814 b64bcece 089e1b6e
1be959a5
6fc20a76
crypto ca certificate chain ASDM_TrustPoint3
certificate ca 05
```

```
30820370 30820258 a0030201 02020105 300d0609 2a864886
f70d0101
05050030
5b310b30 09060355 04061302 55533118 30160603 55040a13
0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c
300a0603
55040b13
03504b49 31163014 06035504 03130d44 6f442052 6f6f7420
43412032
301e170d
30343132 31333135 30303130 5a170d32 39313230 35313530
3031305a
305b310b
30090603 55040613 02555331 18301606 0355040a 130f552e
532e2047
6f766572
6e6d656e 74310c30 0a060355 040b1303 446f4431 0c300a06
0355040b
1303504b
49311630 14060355 0403130d 446f4420 526f6f74 20434120
32308201
crypto ca certificate chain ASDM_TrustPoint4
certificate ca 04
30820267 308201d0 a0030201 02020104 300d0609 2a864886
f70d0101
05050030
61310b30 09060355 04061302 55533118 30160603 55040a13
0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c
300a0603
55040b13
03504b49 311c301a 06035504 03131344 6f442043 4c415353
20332052
6f6f7420
!
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
```

```

!
-----SSL/WEBVPN-----
-----
ssl certificate-authentication interface outside port
443
webvpn
enable outside
svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1
svc enable
tunnel-group-list enable
-----
-----VPN Group/Tunnel Policy-----
-----
group-policy CAC-USERS internal
ggroup-policy AC-USERS internal
group-policy AC-USERS attributes
vpn-tunnel-protocol svc
address-pools value CAC-USERS
webvpn
svc ask none default svc
tunnel-group AC-USERS type remote-access
tunnel-group AC-USERS general-attributes
authorization-server-group AD-LDAP
default-group-policy AC-USERS
authorization-required
authorization-dn-attributes UPN
tunnel-group AC-USERS webvpn-attributes
authentication certificate
group-alias AC-USERS enable
tunnel-group-map enable rules
no tunnel-group-map enable ou
no tunnel-group-map enable ike-id
no tunnel-group-map enable peer-ip
-----
-----
prompt hostname context

```

## 부록 C- 문제 해결

### AAA 및 LDAP 문제 해결

- debug ldap 255 - LDAP 교환을 표시합니다.
- debug aaa common 10 - AAA 교환을 표시합니다.

### 예 1:올바른 특성 매핑이 있는 허용된 연결

이 예에서는 부록 A에 표시된 시나리오 2와 성공적으로 연결하는 동안 debug ldap 및 debug aaa common의 출력을 보여 줍니다.

#### **그림 C1:디버그 LDAP 및 디버그 aaa 공통 출력 - 올바른 매핑**

```

AAA API: In aaa_open
AAA session opened: handle = 39
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS

```



```
AAA task: aaa_process_msg(1a87a64) received message type
0
AAA FSM: In AAA_StartAAATransaction
AAA FSM: In AAA_InitTransaction
Initiating authorization query (Svr Grp: AD-LDAP)
-----
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: 172.18.120.160
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
Resp:
[78] Session Start
[78] New request Session, context 0x26f1c44, reqType = 0
[78] Fiber started
[78] Creating LDAP context with uri=ldap://
172.18.120.160:389
[78] Binding as administrator
[78] Performing Simple authentication for Administrator
to
172.18.120.160
[78] Connect to LDAP server: ldap:// 172.18.120.160,
status =
Successful
[78] LDAP Search:
Base DN = [CN=Users,DC=gsgseclab,DC=org]
Filter = [userPrincipalName=1234567890@mil]
Scope = [SUBTREE]
[78] Retrieved Attributes:
[78] objectClass: value = top
[78] objectClass: value = person
[78] objectClass: value = organizationalPerson
[78] objectClass: value = user
[78] cn: value = Ethan Hunt
[78] sn: value = Hunt
[78] userCertificate: value =
0..50...../.....60...*.H.....0@1.0.....&....,d
....com1.0.....
&....,d...
[78] userCertificate: value =
0..'0...../..t.....50...*.H.....0@1.0.....&....,d
....com1.0.....
&....,d...
[78] givenName: value = Ethan
[78] distinguishedName: value = CN=Ethan
Hunt,OU=MIL,DC=labrat,DC=com
[78] instanceType: value = 4
[78] whenCreated: value = 20060613151033.0Z
[78] whenChanged: value = 20060622185924.0Z
[78] displayName: value = Ethan Hunt
[78] uSNCreated: value = 14050
[78] memberOf: value =
CN=ASAUsers,CN=Users,DC=gsgseclab,DC=org
[78] mapped to cVPN3000-Tunneling-Protocols: value = 20
[78] uSNChanged: value = 14855
[78] name: value = Ethan Hunt
[78] objectGUID: value = ..9...NJ..GU..z.
[78] userAccountControl: value = 66048
[78] badPwdCount: value = 0
[78] codePage: value = 0
[78] countryCode: value = 0
[78] badPasswordTime: value = 127954717631875000
[78] lastLogoff: value = 0
[78] lastLogon: value = 127954849209218750
```

```
[78] pwdLastSet: value = 127946850340781250
[78] primaryGroupID: value = 513
[78] objectSid: value = .....q.....mY...
[78] accountExpires: value = 9223372036854775807
[78] logonCount: value = 25
[78] sAMAccountName: value = 1234567890
[78] sAMAccountType: value = 805306368
[78] userPrincipalName: value = 1234567890@mil
[78] objectCategory: value =
[78] mail: value = Ethan.Hunt@labrat.com
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
[78] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
[78] Session End
AAA task: aaa_process_msg(1a87a64) received message type
1
AAA FSM: In AAA_ProcSvrResp
Back End response:
-----
Authorization Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE,
auth_status = ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-
LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state =
IFSM_TUNN_GRP_POLICY,
AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(CAC-USERS)
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp:
GROUP_POLICY_DB)
-----
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: <Internal Server>
AAA FSM: In AAA_SendMsg
User: CAC-USER
Pasw:
Resp:
grp_policy_ioctl(12f1b20, 114698, 1a870b4)
grp_policy_ioctl: Looking up CAC-USERS
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
AAA task: aaa_process_msg(1a87a64) received message type
1
AAA FSM: In AAA_ProcSvrResp
Back End response:
-----
Tunnel Group Policy Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY,
auth_status =
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-
LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_DONE,
AAA FSM: In AAA_ProcessFinal
Checking time simultaneous login restriction for user
1234567890@mil
AAA FSM: In AAA_Callback
```

```

user attributes:
1 Tunneling-Protocol(4107) 20 20
user policy attributes:
None
tunnel policy attributes:
1 Primary-DNS(4101) 4 IP: 10.0.10.100
2 Secondary-DNS(4102) 4 IP: 0.0.0.0
3 Tunneling-Protocol(4107) 4 4
4 Default-Domain-Name(4124) 10 "ggsgseclab.org"
5 List of address pools to assign addresses from(4313)
10
"CAC-USERS"
Auth Status = ACCEPT
AAA API: In aaa_close
AAA task: aaa_process_msg(1a87a64) received message type
3
In aaai_close_session (39)
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop
CAC-Test#

```

## 예 2: 잘못 구성된 Cisco 특성 매핑으로 허용된 연결

이 예에서는 부록 A에 표시된 시나리오 2와 허용되는 연결 중에 **debug ldap** 및 **debug aaa common**의 출력을 보여줍니다.

### 그림 C2: debug LDAP 및 debug aaa common output - 잘못된 매핑

```

AAA API: In aaa_open
AAA session opened: handle = 41
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(1a87a64) received message type
0
AAA FSM: In AAA_StartAAATransaction
AAA FSM: In AAA_InitTransaction
Initiating authorization query (Svr Grp: AD-LDAP)
-----
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: 172.18.120.160
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
Resp:
[82] Session Start
[82] New request Session, context 0x26f1c44, reqType = 0
[82] Fiber started
[82] Creating LDAP context with
uri=ldap://172.18.120.160:389
[82] Binding as administrator
[82] Performing Simple authentication for Administrator
to
172.18.120.160
[82] Connect to LDAP server: ldap:// 172.18.120.160:389,
status =
Successful
[82] LDAP Search:
Base DN = [CN=Users,DC=ggsgseclab,DC=org]
Filter = [userPrincipalName=1234567890@mil]
Scope = [SUBTREE]

```

```
[82] Retrieved Attributes:
[82] objectClass: value = top
[82] objectClass: value = person
[82] objectClass: value = organizationalPerson
[82] objectClass: value = user
[82] cn: value = Ethan Hunt
[82] sn: value = Hunt
[82] userCertificate: value =
0..50...../.....60...*.H.....0@1.0.....&....,d
....com1.0.....
&....,d...
[82] userCertificate: value =
0..'0...../..t.....50...*.H.....0@1.0.....&....,d
....com1.0.....
&....,d...
[82] givenName: value = Ethan
[82] distinguishedName: value = CN=Ethan
Hunt,OU=MIL,DC=labrat,DC=com
[82] instanceType: value = 4
[82] whenCreated: value = 20060613151033.0Z
[82] whenChanged: value = 20060622185924.0Z
[82] displayName: value = Ethan Hunt
[82] uSNCreated: value = 14050
[82] memberOf: value =
CN=ASAUsers,CN=Users,DC=gsgseclab,DC=org
[82] mapped to cVPN3000-Tunneling-Protocols: value =
CN=ASAUsers,CN=Users,DC=gsgseclab,DC=org
[82] uSNChanged: value = 14855
[82] name: value = Ethan Hunt
[82] objectGUID: value = ..9...NJ..GU..z.
[82] userAccountControl: value = 66048
[82] badPwdCount: value = 0
[82] codePage: value = 0
[82] countryCode: value = 0
[82] badPasswordTime: value = 127954717631875000
[82] lastLogoff: value = 0
[82] lastLogon: value = 127954849209218750
[82] pwdLastSet: value = 127946850340781250
[82] primaryGroupID: value = 513
[82] objectSid: value = .....q.....mY...
[82] accountExpires: value = 9223372036854775807
[82] logonCount: value = 25
[82] sAMAccountName: value = 1234567890
[82] sAMAccountType: value = 805306368
[82] userPrincipalName: value = 1234567890@mil
[82] objectCategory: value =
CN=Person,CN=Schema,CN=Configuration,DC=gsgseclab,DC=or
g
[82] mail: value = Ethan.Hunt@labrat.com
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 41, pAcb = 2ae115c
[82] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
[82] Session End
AAA task: aaa_process_msg(1a87a64) received message type
1
AAA FSM: In AAA_ProcSvrResp
Back End response:
-----
Authorization Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE,
auth_status = ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-
```

```
LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state =
IFSM_TUNN_GRP_POLICY,
AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(USAFE)
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp:
GROUP_POLICY_DB)
-----
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: <Internal Server>
AAA FSM: In AAA_SendMsg
User: CAC-USERS
Pasw:
Resp:
grp_policy_ioctl(12f1b20, 114698, 1a870b4)
grp_policy_ioctl: Looking up CAC-USERS
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 41, pAcb = 2ae115c
AAA task: aaa_process_msg(1a87a64) received message type
1
AAA FSM: In AAA_ProcSvrResp
Back End response:
-----
Tunnel Group Policy Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY,
auth_status =
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-
LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_DONE,
AAA FSM: In AAA_ProcessFinal
Checking time simultaneous login restriction for user
1234567890@mil
AAA FSM: In AAA_Callback
user attributes:
1 Tunnelling-Protocol(4107) 20 0
user policy attributes:
None
tunnel policy attributes:
1 Primary-DNS(4101) 4 IP: 10.0.10.100
2 Secondary-DNS(4102) 4 IP: 0.0.0.0
3 Tunnelling-Protocol(4107) 4 4
4 Default-Domain-Name(4124) 10 "ggsgseclab.org"
5 List of address pools to assign addresses from(4313)
10
"CAC-USERS"
Auth Status = ACCEPT
AAA API: In aaa_close
AAA task: aaa_process_msg(1a87a64) received message type
3
In aaai_close_session (41)
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop
```

## DAP 문제 해결

- **debug dap errors** - DAP 오류를 표시합니다.
- **debug dap trace** - DAP 함수 추적을 표시합니다.

## 예 1:DAP와의 연결 허용

이 예에서는 디버그 **dap** 오류 및 디버그 **dap** 추적을 부록 A에 표시된 시나리오 3과 성공적으로 연결하는 동안 출력을 보여 줍니다. 여러 **memberOf** 특성을 확인합니다. **\_ASAUUsers** 및 **VPNUsers** 둘 다에 속하거나 ASA 컨피그레이션에 종속된 두 그룹 중 하나에 속할 수 있습니다.

### 그림 C3:디버그 DAP

```
#debug dap errors
debug dap errors enabled at level 1
#debug dap trace
debug dap trace enabled at level 1
#
The DAP policy contains the following attributes for
user:
1241879298@mil
-----
---
1: action = continue
DAP_TRACE: DAP_open: C8EEFA10
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.1 = top
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.2 = person
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.3 =
organizationalPerson
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.4 = user
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.cn =
1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.physicalDeliveryOfficeName = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName
= 1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.distinguishedName =
CN=1241879298,CN=Users,DC=ggsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.whenCreated =
20070626163734.0Z
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.whenChanged =
20070718151143.0Z
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.displayName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNCreated
= 33691
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf.1
= VPNUsers
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf.2
= _ASAUUsers
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNChanged
= 53274
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.department
= NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.name =
1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectGUID
=
....+..F.."5....
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.userAccountControl =
328192
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.badPwdCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.codePage =
0
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.countryCode = 0
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.badPasswordTime = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogoff
= 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogon
= 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.pwdLastSet
=
128273494546718750
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.primaryGroupID = 513
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.userParameters = m:
d.
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectSid
= ..
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.accountExpires =
9223372036854775807
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.logonCount
= 0
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.sAMAccountName =
1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.sAMAccountType =
805306368
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.userPrincipalName =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectCategory =
CN=Person,CN=Schema,CN=Configuration,DC=gsgseclab,DC=or
g
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.msNPAllowDialin = TRUE
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.username
=
1241879298@mil
DAP_TRACE: Username: 1241879298@mil,
aaa.cisco.tunnelgroup = CAC-USERS
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] =
"top";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person";
DAP_TRACE:
```

```
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] =
"user";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"] =
"1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeName"] =
"NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["givenName"]
= "1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298,CN=Users,DC=gsgsecclab,DC=org";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"]
= "33691";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["1"] =
"VPNUsers";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["2"] =
"_ASAUsers";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"]
= "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"]
= "NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["name"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"]
contains
binary data
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] =
"0";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] =
"0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"]
= "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"]
= "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"]
=
"128273494546718750";
DAP_TRACE:
```



```

dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] =
"513";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userParameters"]
contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectSid"]
contains binary
data
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["logonCount"]
= "0";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"] =
"1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person,CN=Schema,CN=Configuration,DC=gsgseclab,DC=org";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] =
"TRUE";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username"]
=
"1241879298@mil";
DAP_TRACE:
dap_add_to_lua_tree:aaa["cisco"]["tunnelgroup"] =
"CACUSERS";
DAP_TRACE:
dap_add_to_lua_tree:endpoint["application"]["clienttype"]
] =
"IPSec";
DAP_TRACE: Username: 1241879298@mil, Selected DAPs: CAC-
USERS
DAP_TRACE: dap_request: memory usage = 33%
DAP_TRACE: dap_process_selected_daps: selected 1 records
DAP_TRACE: Username: 1241879298@mil, dap_aggregate_attr:
rec_count = 1
DAP_TRACE: Username: 1241879298@mil, DAP_close: C8EEFA10
d.

```

## 예 2:DAP와의 연결 거부

Thia 예는 부록 A에 표시된 시나리오 3과 연결되지 않은 연결 중에 debug dap 오류 및 debug dap 추적의 출력을 보여줍니다.

### 그림 C4:디버그 DAP

```

#debug dap errors
debug dap errors enabled at level 1
#debug dap trace
debug dap trace enabled at level 1
#

```

```
The DAP policy contains the following attributes for
user:
1241879298@mil
-----
-----
1: action = terminate
DAP_TRACE: DAP_open: C91154E8
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.1 = top
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.2 = person
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.3 =
organizationalPerson
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.4 = user
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.cn =
1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.physicalDeliveryOfficeName = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName
= 1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.distinguishedName =
CN=1241879298,CN=Users,DC=gsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.whenCreated =
20070626163734.0Z
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.whenChanged =
20070718151143.0Z
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.displayName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNCreated
= 33691
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf =
DnsAdmins
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNChanged
= 53274
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.department
= NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.name =
1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectGUID
=
....+..F..5....
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.userAccountControl =
328192
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.badPwdCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.codePage =
0
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.countryCode = 0
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.badPasswordTime = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogoff
= 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogon
= 0
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.pwdLastSet
=
128273494546718750
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.primaryGroupID = 513
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.userParameters = m:
d.
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectSid
= ..
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.accountExpires =
9223372036854775807
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.logonCount
= 0
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.sAMAccountName =
1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.sAMAccountType =
805306368
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.userPrincipalName =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectCategory =
CN=Person,CN=Schema,CN=Configuration,DC=gsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.msNPAllowDialin = TRUE
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.username
=
1241879298@mil
DAP_TRACE: Username: 1241879298@mil,
aaa.cisco.tunnelgroup = CAC-USERS
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] =
"top";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] =
"user";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"] =
"1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeName"] =
"NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["givenName"]
= "1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298,CN=Users,DC=gsgseclab,DC=org";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z";
DAP_TRACE:
```

```
dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"]
= "33691";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"] =
"DnsAdmins";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"]
= "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"]
= "NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["name"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"]
contains
binary data
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] =
"0";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] =
"0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"]
= "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"]
= "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"]
=
"128273494546718750";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] =
"513";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userParameters"]
contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectSid"]
contains binary
data
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["logonCount"]
= "0";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"] =
"1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person,CN=Schema,CN=Configuration,DC=gsgseclab,DC=o
```

```
rg";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] =
"TRUE";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username"]
=
"1241879298@mil";
DAP_TRACE: Username: 1241879298@mil, Selected DAPs:
DAP_TRACE: dap_request: memory usage = 33%
DAP_TRACE: dap_process_selected_daps: selected 0 records
DAP_TRACE: Username: 1241879298@mil, dap_aggregate_attr:
rec_count = 1
```

## [인증 기관/OCSP 문제 해결](#)

### • 디버그 암호화 ca 3

#### • 컨피그레이션 모드에서 — 로깅 클래스 ca console(또는 버퍼) 디버깅

다음 예에서는 OCSP 응답자와 일치하는 정책에 실패한 인증서 그룹 및 성공적인 인증서 검증을 보여줍니다.

그림 C3는 검증된 인증서와 일치하는 작업 인증서 그룹이 있는 디버그 출력을 보여줍니다.

그림 C4는 잘못 구성된 인증서 그룹 일치 정책의 디버그 출력을 보여줍니다.

그림 C5는 폐기된 인증서를 가진 사용자의 디버그 출력을 보여줍니다.

### 그림 C5:OCSP 디버깅 - 인증서 유효성 검사 성공

```
CRYPTO_PKI: Found a suitable authenticated trustpoint
ASDM_TrustPoint11.
CRYPTO_PKI: Allocated OCSP data handle 0xca2d27b8
CRYPTO_PKI: Certificate validation: Successful, status:
0. Attempting
to retrieve revocation status if necessary
CRYPTO_PKI: status = 0: poll revocation status
CRYPTO_PKI: Attempting to find OCSP override for peer
cert: serial
number: 0F192B, subject name:
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-
15,ou=PKI,ou=DoD,o=U.S. Government,c=US.
CRYPTO_PKI: Processing map rules for SSL.
CRYPTO_PKI: Processing map SSL sequence 20...
CRYPTO_PKI: Match of subject-name field to map PASSED.
Peer cert field:
=
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne ".
CRYPTO_PKI: Peer cert has been authorized by map: SSL
sequence: 20.
CRYPTO_PKI: Found OCSP override match. Override URL:
http://198.154.68.90, Override trustpoint:
ASDM_TrustPoint12
CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
CRYPTO_PKI: Destroying OCSP data handle 0xca2d27b8
Crypto CA thread sleeps!
CRYPTO_PKI: Attempting to find tunnel group for cert
with serial
```

```

number: 0F192B, subject name:
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-
15,ou=PKI,ou=DoD,o=U.S. Government,c=US.
CRYPTO_PKI: Processing map rules for
DefaultCertificateMap.
CRYPTO_PKI: Processing map DefaultCertificateMap
sequence 10...
CRYPTO_PKI: Match of subject-name field to map PASSED.
Peer cert field:
=
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne ".
CRYPTO_PKI: Peer cert has been authorized by map:
DefaultCertificateMap
sequence: 10.
CRYPTO_PKI: Ignoring match on map DefaultCertificateMap,
index 10 for
WebVPN group map processing. No tunnel group is
configured.
CRYPTO_PKI: Peer cert could not be authorized with map:
DefaultCertificateMap.
CRYPTO_PKI: Processing map rules for SSL.
CRYPTO_PKI: Processing map SSL sequence 20...
CRYPTO_PKI: Match of subject-name field to map PASSED.
Peer cert field:
=
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne ".
CRYPTO_PKI: Peer cert has been authorized by map: SSL
sequence: 20.
CRYPTO_PKI: Ignoring match on map SSL, index 20 for
WebVPN group map

```

## 그림 C5: 실패한 인증서 그룹 일치 정책의 출력

### 그림 C5: 폐기된 인증서의 출력

```

n %PI=X-3-7E17t02h7a Certinf icaHtue cnhta,in faioled
uvalidation=.
CMertifiIcLa,ted ccha=inl ais eibtrhaer tin,validid cor
=noct
oamuthorized.
map rule: subject-name ne ".
CRYPTO_PKI: Peer cert has been authorized by map:
DefaultCertificateMap
sequence: 10.
Tunnel Group Match on map DefaultCertificateMap sequence
# 10.
Group name is CAC-USERS
CRYPTO_PKI: Checking to see if an identical cert is
already in the database...
CRYPTO_PKI: looking for cert in handle=2467668, digest=
CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
CRYPTO_PKI: Cert not found in database.
CRYPTO_PKI: Looking for suitable trustpoints...
CRYPTO_PKI: Found a suitable authenticated trustpoint
trustpoint0.
CRYPTO_PKI: Certificate validation: Successful, status:
0. Attempting
to retrieve revocation status if necessary
CRYPTO_PKI: Attempting to find OCSP override for peer

```

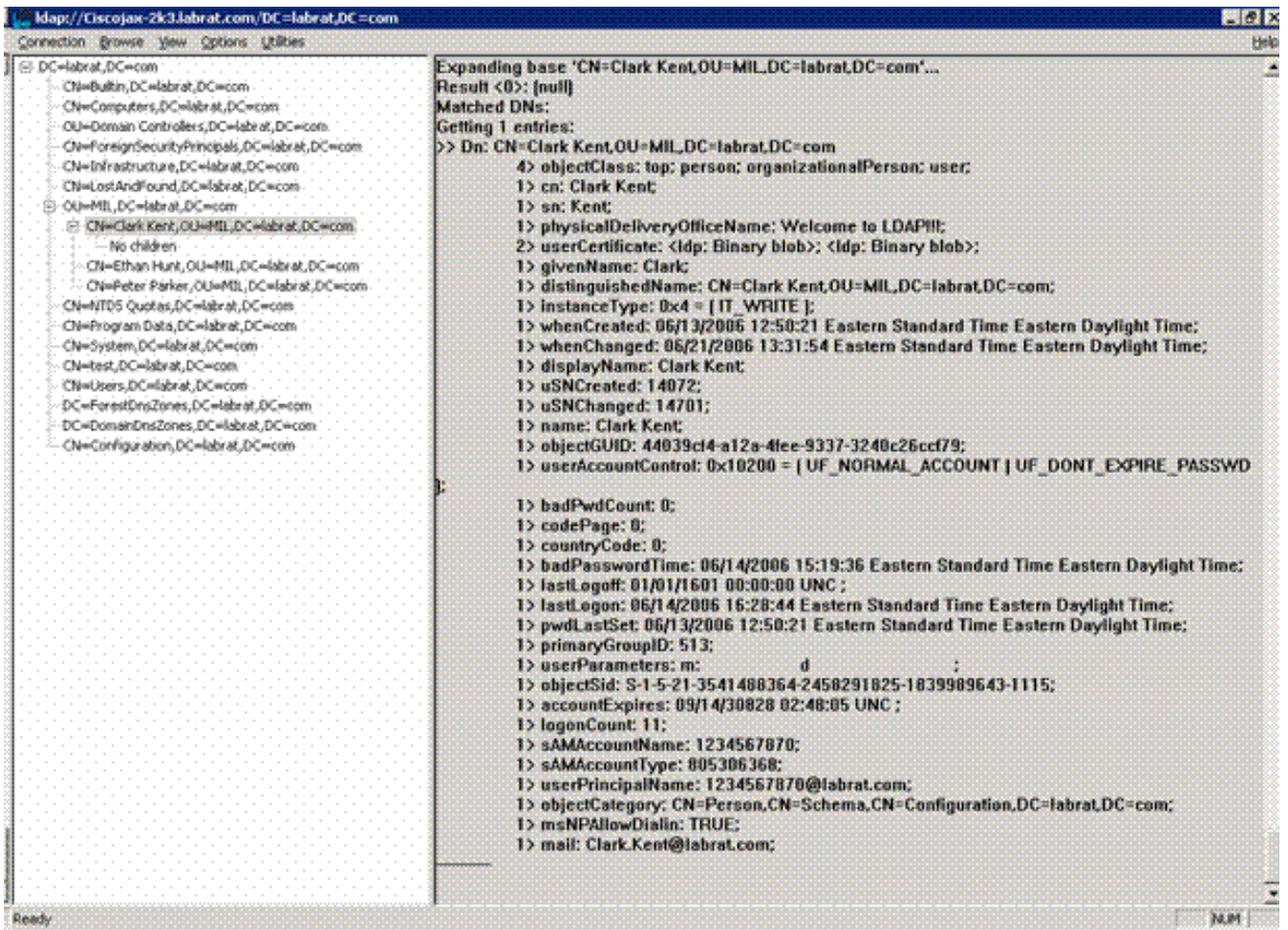
```
cert: serial
number: 2FB5FC74000000000035, subject name: cn=Ethan
Hunt,ou=MIL,dc=gsgseclab,dc=org, issuer_name:
cn=gsgseclab,dc=gsgseclab,dc=org.
CRYPTO_PKI: Processing map rules for
DefaultCertificateMap.
CRYPTO_PKI: Processing map DefaultCertificateMap
sequence 10...
CRYPTO_PKI: Match of subject-name field to map PASSED.
Peer cert field:
= cn=Ethan Hunt,ou=MIL,dc=gsgseclab,dc=org, map rule:
subject-name
ne "".
CRYPTO_PKI: Peer cert has been authorized by map:
DefaultCertificateMap
sequence: 10.
CRYPTO_PKI: Found OCSP override match. Override URL:
http://ocsp.disa.mil, Override trustpoint: OCSP
CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
CRYPTO_PKI: Found a subject match
ERROR: Certificate validation failed, Certificate is
revoked, serial
number: 2FB5FC74000000000035, subject name: cn=Ethan
Hunt,ou=MIL,dc=gsgseclab,dc=org
CRYPTO_PKI: Certificate not validated
```

## [부록 D - MS에서 LDAP 개체 확인](#)

Microsoft Server 2003 CD에는 LDAP 구조 및 LDAP 개체/특성을 보기 위해 설치할 수 있는 추가 도구가 있습니다. 이러한 도구를 설치하려면 CD의 **지원 디렉터리**와 **도구**를 차례로 **선택합니다** .SUPTOOLS.MSI를 **설치합니다**.

### [LDAP 뷰어](#)

- 설치 후 **시작 > 실행**을 선택합니다.
- **ldp**를 입력한 다음 **확인**을 클릭합니다. 이렇게 하면 LDAP 뷰어가 시작됩니다.
- **Connection > Connect**를 선택합니다.
- 서버 이름을 입력한 다음 **확인**을 클릭합니다.
- **Connection > Bind**를 선택합니다.
- 사용자 이름과 비밀번호를 입력합니다. **참고:** 관리자 권한이 필요합니다.
- **확인**을 클릭합니다.
- LDAP 객체를 봅니다. 그림 D1을 참조하십시오. **그림 D1:LDAP 뷰어**



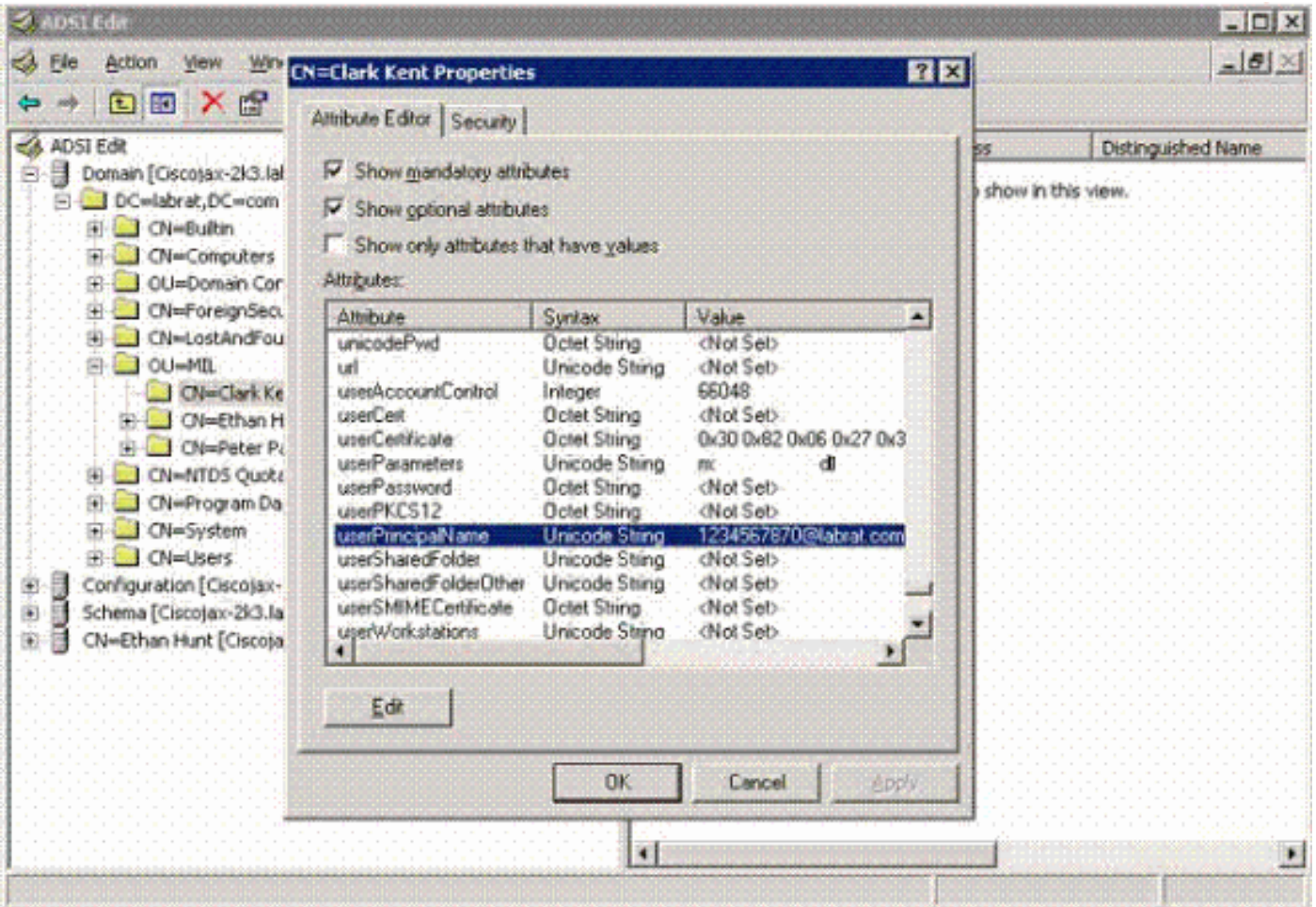
## Active Directory 서비스 인터페이스 편집기

- Active Directory 서버에서 시작 > 실행을 선택합니다.
- adsiedit.msc를 입력합니다.이렇게 하면 편집기가 시작됩니다.
- 개체를 마우스 오른쪽 단추로 클릭하고 속성을 클릭합니다.

이 도구는 특정 객체에 대한 모든 속성을 표시합니다.그림 D2를 참조하십시오.

### 그림 D2:ADSI 수정





## 부록 E

AnyConnect 프로파일을 생성하여 워크스테이션에 추가할 수 있습니다. 프로파일은 ASA 호스트 또는 DN 또는 발급자 같은 인증서 일치 매개변수와 같은 다양한 값을 참조할 수 있습니다. 프로파일은 .xml 파일로 저장되며 메모장으로 편집할 수 있습니다. 파일을 각 클라이언트에 수동으로 추가하거나 그룹 정책을 통해 ASA에서 푸시할 수 있습니다. 파일은 다음 위치에 저장됩니다.

C:\Documents and Settings\All Users\Application Data\Cisco\Cisco  
AnyConnect VPN Client\Profile

다음 단계를 완료하십시오.

1. AnyConnectProfile.tmpl을 선택하고 Notepad(메모장)로 파일을 엽니다.
2. 발급자 또는 호스트 IP와 같은 파일을 적절하게 수정합니다. 예를 들면 그림 F1을 참조하십시오.
3. 완료되면 파일을 .xml로 저장합니다.

Cisco AnyConnect VPN 클라이언트 프로파일 XML 파일의 샘플입니다.

프로필 관리에 대해서는 Cisco AnyConnect 설명서를 참조하십시오. 간단히 말해,

- 프로파일은 회사의 고유한 이름을 지정해야 합니다. 예를 들면 다음과 같습니다. CiscoProfile.xml
- 회사 내의 개별 그룹에 대해 다른 경우에도 프로파일 이름은 동일해야 합니다.

이 파일은 보안 게이트웨이 관리자가 유지 관리한 다음 클라이언트 소프트웨어와 함께 배포하기 위한 것입니다. 이 XML을 기반으로 하는 프로파일은 언제든지 클라이언트에 배포할 수 있습니다. 지원되는 배포 메커니즘은 소프트웨어 배포와 함께 번들로 제공되는 파일이거나 자동 다운로드 메커니즘의 일부로 제공됩니다. 자동 다운로드 메커니즘은 특정 Cisco Secure Gateway 제품에서만 사용

할 수 있습니다.

**참고:** 관리자는 온라인 검증 툴을 사용하거나 ASDM의 프로파일 가져오기 기능을 통해 자신이 생성한 XML 프로파일을 검증하는 것이 좋습니다. 이 디렉터리에 있는 AnyConnectProfile.xsd를 사용하여 유효성 검사를 수행할 수 있습니다. AnyConnectProfile은 AnyConnect 클라이언트 프로파일을 나타내는 루트 요소입니다.

```
xml version="1.0" encoding="UTF-8"
```

```
- -
```

```
!--- The ClientInitialization section represents global settings !--- for the client. In some cases, for example, BackupServerList, host specific !--- overrides are possible. !-- --> -
```

```
!--- The Start Before Logon feature can be used to activate !--- the VPN as part of the logon sequence. !-- - UserControllable: Does the administrator of this profile allow the user !--- to control this attribute for their own use. Any user setting !--- associated with this attribute is stored elsewhere. -->
```

```
!--- This control enables an administrator to have a one time !--- message displayed prior to a users first connection attempt. As an !--- example, the message can be used to remind a user to insert their smart !--- card into its reader. !--- The message to be used with this control is localizable and can be !--- found in the AnyConnect message catalog. !--- (default: "This is a pre-connect reminder message.")
```

```
!-- This section enables the definition of various attributes !--- that can be used to refine client certificate selection. --> -
```

```
!--- Certificate Distinguished Name matching allows for exact !--- match criteria in the choosing of acceptable client !--- certificates. -
```

```
- !-- This section contains the list of hosts from which  
!--- the user is able to select. -
```

```
!--- This is the data needed to attempt a connection to  
a specific !--- host. --> -
```

-

## 관련 정보

- [X.509 및 RFC 3280에 의해 지정된 인증서 및 CRL](#)
- [RFC 2560에 의해 지정된 OCSP](#)
- [공개 키 인프라 소개](#)
- [초안 표준으로 프로파일링된 "경량 OCSP"](#)
- [RFC 2246에 의해 지정된 SSL/TLS](#)
- [기술 지원 및 문서 - Cisco Systems](#)