ASA 8.X:AnyConnect SCEP 등록 컨피그레이션 예

목차

소개

SCEP 등록 기능은 AnyConnect 독립형 클라이언트 2.4에 도입되었습니다. 이 프로세스에서 SCEP 관련 구성을 포함하도록 AnyConnect XML 프로파일을 수정하고 인증서 등록을 위해 특정 그룹 정책 및 연결 프로파일을 생성합니다.AnyConnect 사용자가 이 특정 그룹에 연결되면 AnyConnect는 CA 서버에 인증서 등록 요청을 전송하고 CA 서버는 자동으로 요청을 수락하거나 거부합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 8.x를 실행하는 Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco AnyConnect VPN 버전 2.4

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 규칙을 참조하십시오.

배경 정보

AnyConnect용 자동 SCEP 등록은 안전하고 확장 가능한 방식으로 클라이언트에 인증서를 발급하는 것입니다.예를 들어 사용자는 CA 서버에서 인증서를 요청할 필요가 없습니다.이 기능은 AnyConnect 클라이언트에 통합되어 있습니다.인증서는 XML 프로파일 파일에 언급된 인증서 매개변수를 기반으로 클라이언트에 발급됩니다.

필요한 변경 사항 개요

AnyConnect SCEP 등록 기능을 사용하려면 XML 프로필에 특정 인증서 매개변수를 정의해야 합니다.ASA에서 인증서 등록을 위해 그룹 정책 및 연결 프로파일이 생성되고 XML 프로파일이 해당 정책과 연결됩니다.AnyConnect 클라이언트는 이 특정 정책을 사용하는 연결 프로파일에 연결되고 XML 파일에 정의된 매개변수를 사용하여 인증서에 대한 요청을 보냅니다.CA(Certificate Authority)는 자동으로 요청을 수락하거나 거부합니다.<CertificateSCEP> 요소가 클라이언트 프로필에 정의된 경우 AnyConnect 클라이언트는 SCEP 프로토콜로 인증서를 검색합니다.

AnyConnect에서 새 인증서를 자동으로 검색하기 전에 클라이언트 인증서 인증이 실패해야 합니다.따라서 유효한 인증서가 이미 설치되어 있으면 등록이 수행되지 않습니다.

사용자가 특정 그룹에 로그인하면 자동으로 등록됩니다.인증서 검색에 사용할 수 있는 수동 방법이 있으며, 사용자는 **Get Certificate** 버튼을 사용합니다.이는 클라이언트가 터널을 통해서가 아니라 CA 서버에 직접 액세스할 수 있는 경우에만 작동합니다.

자세한 내용은 Cisco AnyConnect VPN 클라이언트 관리자 가이드, 릴리스 2.4를 참조하십시오.

Anyconnect SCEP 기능을 활성화하는 XML 설정

이러한 요소는 AnyConnect XML 파일에 정의해야 하는 중요한 요소입니다.자세한 내용은 Cisco AnyConnect VPN 클라이언트 관리자 가이드, 릴리스 2.4를 참조하십시오.

- <AutomaticSCEPHost> - SCEP 인증서 검색이 구성된 ASA 호스트 이름 및 연결 프로파일(터널 그룹)을 지정합니다.값은 ASA\연결 프로파일 이름의 정규화된 도메인 이름 또는 ASA\연결 프로파일 이름의 IP 주소 형식이어야 합니다.
- <CAURL> - SCEP CA 서버를 식별합니다.
- <CertificateSCEP> - 인증서 내용을 요청하는 방법을 정의합니다.
- <DisplayGetCertButton> - AnyConnect GUI에서 Get Certificate 버튼을 표시할지 여부를 결정합니다.사용자가 수동으로 인증서의 갱신 또는 프로비저닝을 요청할 수 있습니다.

다음은 프로필 예입니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
```

```
<AutomaticCertSelection UserControllable="true">true</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AutoConnectOnStart UserControllable="true">true</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">
     ReconnectAfterResume
   </AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">
    Automatic
  </RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Automatic
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<CertificateEnrollment>
<AutomaticSCEPHost>asa2.cisco.com/certenroll</AutomaticSCEPHost>
<CAURL PromptForChallengePW="false">
     http://10.11.11.1/certsrv/mscep/mscep.dll
   </CAURL>
<CertificateSCEP>
<Name_CN>cisco</Name_CN>
<Company_O>Cisco</Company_O>
<DisplayGetCertButton>true</DisplayGetCertButton>
</CertificateSCEP>
</CertificateEnrollment>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>asa2.cisco.com</HostName>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

AnyConnect용 SCEP 프로토콜을 지원하도록 ASA 구성

RA(Private Registration Authority)에 대한 액세스를 제공하려면 ASA 관리자가 프라이빗 사이드 네트워크 연결을 원하는 RA로 제한하는 ACL이 있는 별칭을 생성해야 합니다.인증서를 자동으로 검색하기 위해 사용자는 이 별칭에 연결하고 인증합니다.

다음 단계를 완료하십시오.

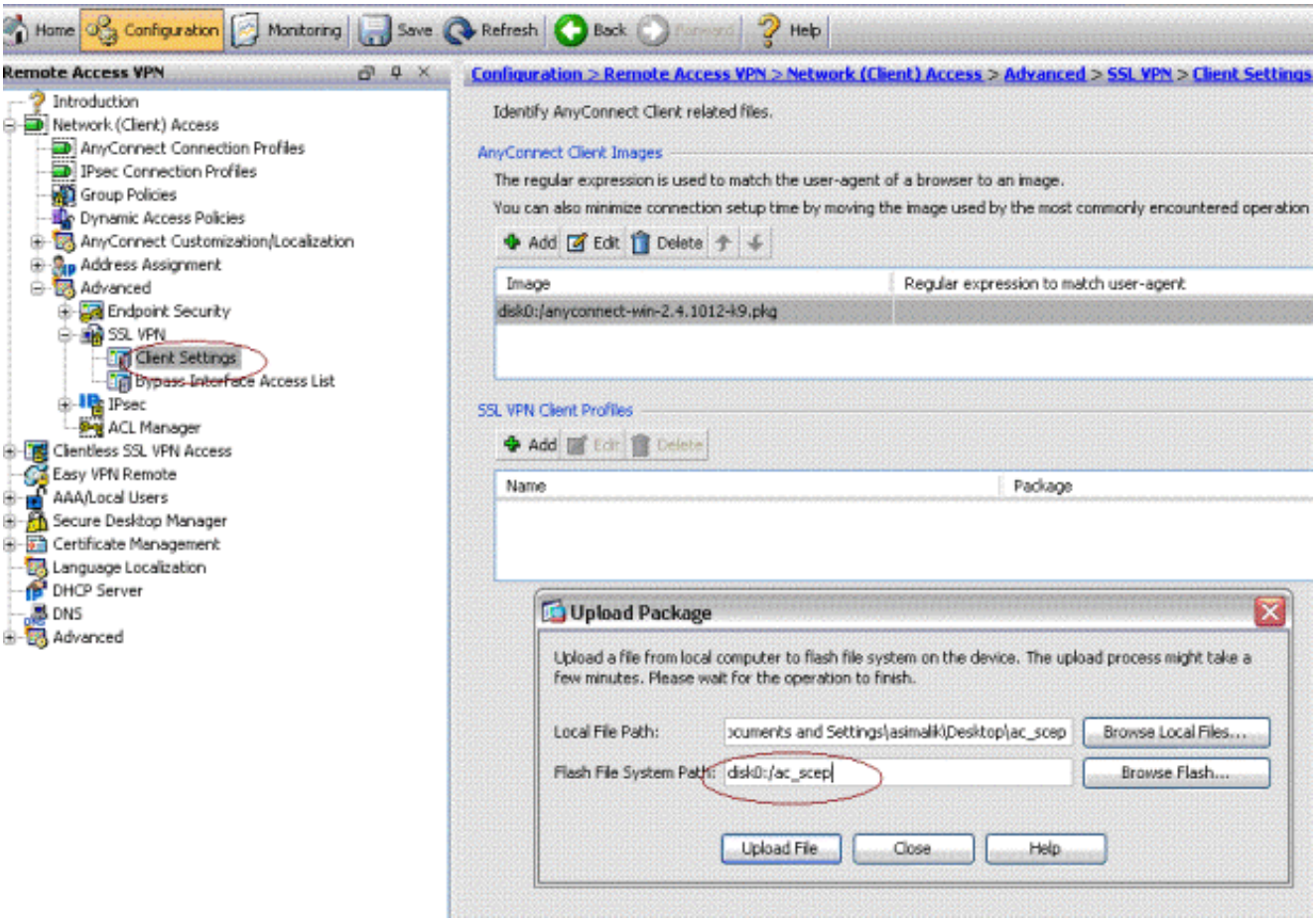
1. 구성된 특정 그룹을 가리키도록 ASA에 별칭을 생성합니다.
2. 사용자의 클라이언트 프로필에 있는 <AutomaticSCEPHost> 요소에서 별칭을 지정합니다.
3. <CertificateEnrollment> 섹션이 포함된 클라이언트 프로파일을 구성된 특정 그룹에 연결합니다.
4. 트래픽을 사설 측면 RA로 제한하려면 구성된 특정 그룹에 대한 ACL을 설정합니다.

다음 단계를 완료하십시오.

1. XML 프로필을 ASA에 업로드합니다.Remote **Access VPN(원격 액세스 VPN) > Network**

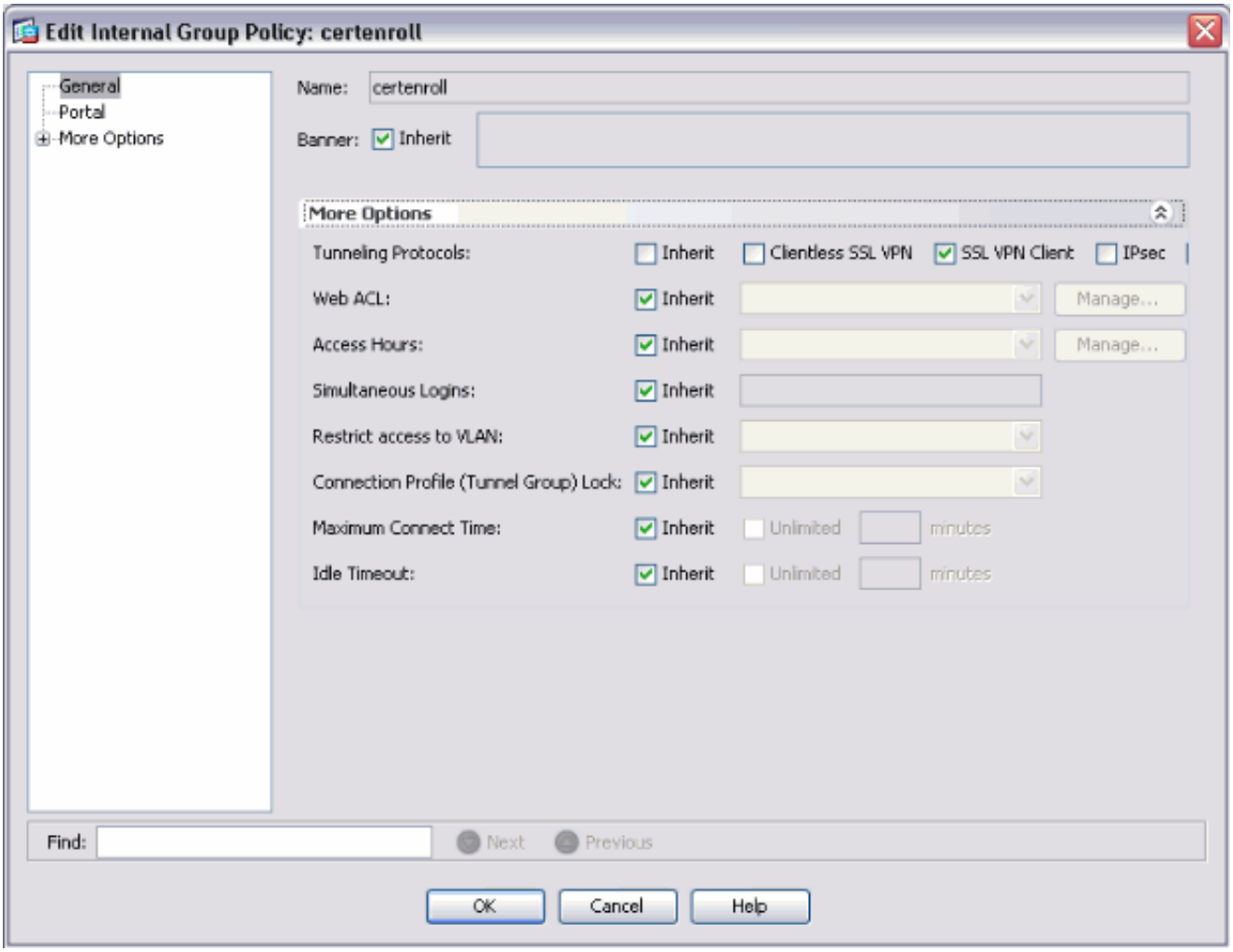
(client) access(네트워크(클라이언트) 액세스) > Advanced(고급) > SSL VPN > Client settings(클라이언트 설정)를 선택합니다.SSL VPN Client profiles(SSL VPN 클라이언트 프로파일)에서 Add(**추가**)를 클릭합니다.Browse **Local Files(로컬 파일 찾아보기)**를 클릭하여 프로파일 파일을 선택하고 **Browse Flash(플래시 찾아보기)를** 클릭하여 플래시 파일 이름을 지정합니다.Upload **File을 클릭합니다**

.



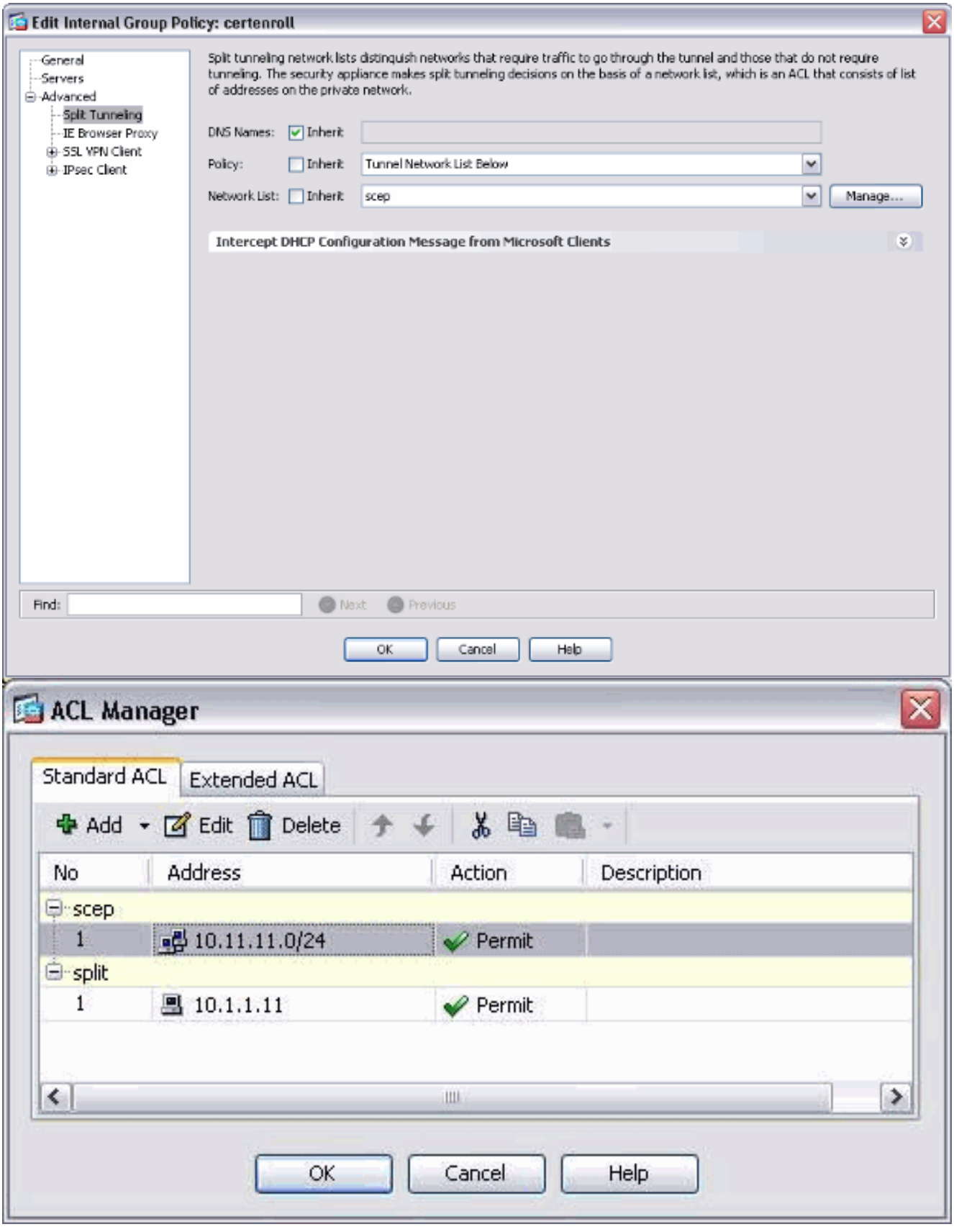
2. 인증서 등록을 **위한** 인증서 그룹 정책을 설정합니다.Remote **access VPN(원격 액세스 VPN) > Network client access(네트워크 클라이언트 액세스) > Group Policy(그룹 정책)**를 선택하고 **Add(추가)**를 클릭합니다

.



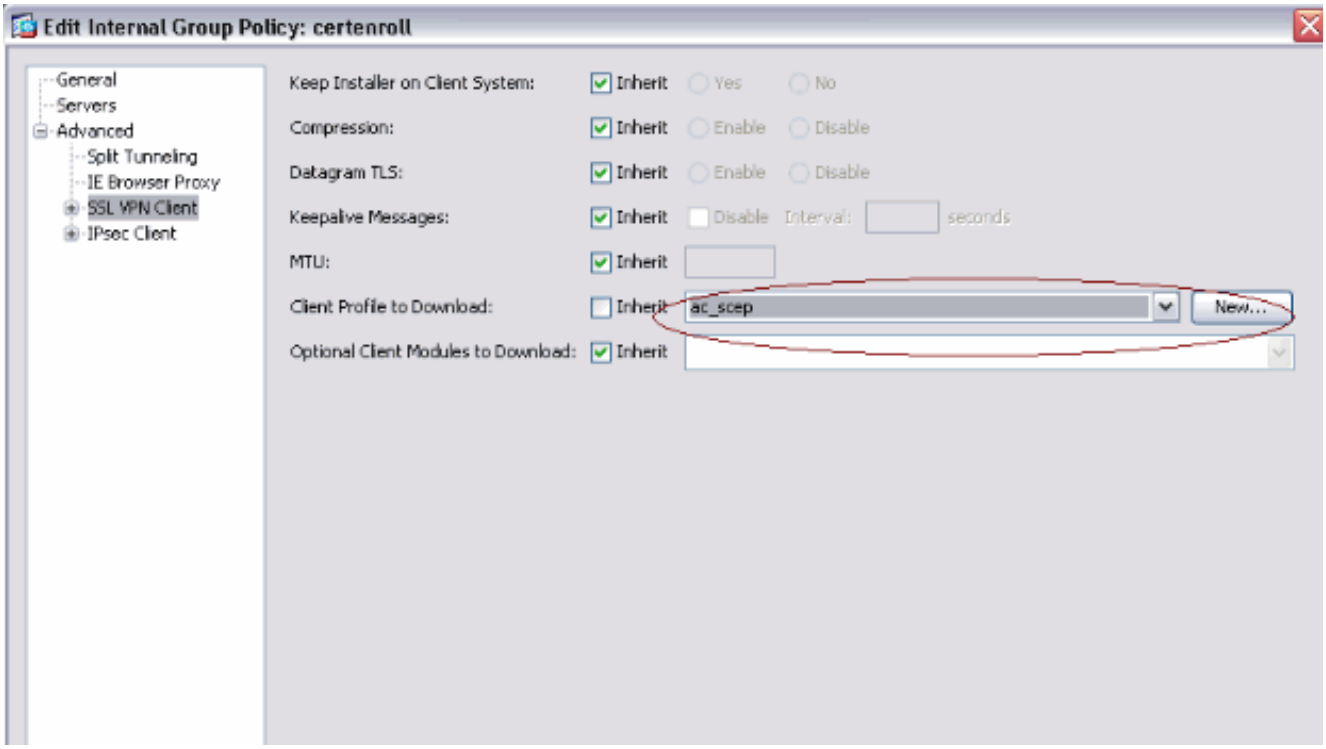
CA 서버에 대한 스플릿 터널을 추가합니다.Advanced(**고급**)를 확장한 다음 **Split Tunneling(스플릿 터널링)을** 선택합니다.Policy 메뉴**에서 Tunnel Network List Below(아래 네트워크 목록**)를 선택하고 **Manage(관리)를** 클릭하여 액세스 제어 목록을 추가합니다

.



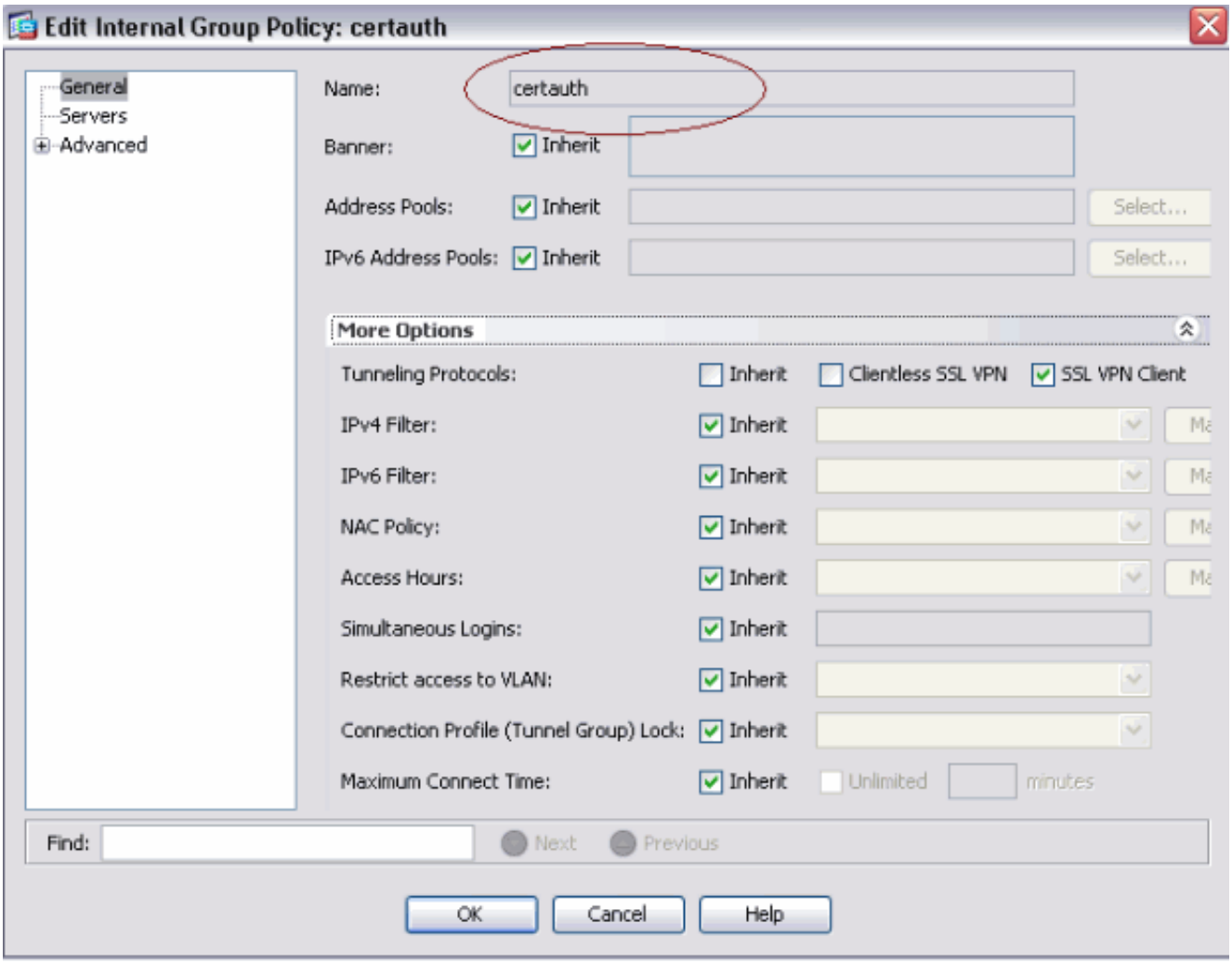
SSL VPN Client를 선택하고 **Client Profile to Download** 메뉴에서 certenroll의 프로파일을 선택합니다

.



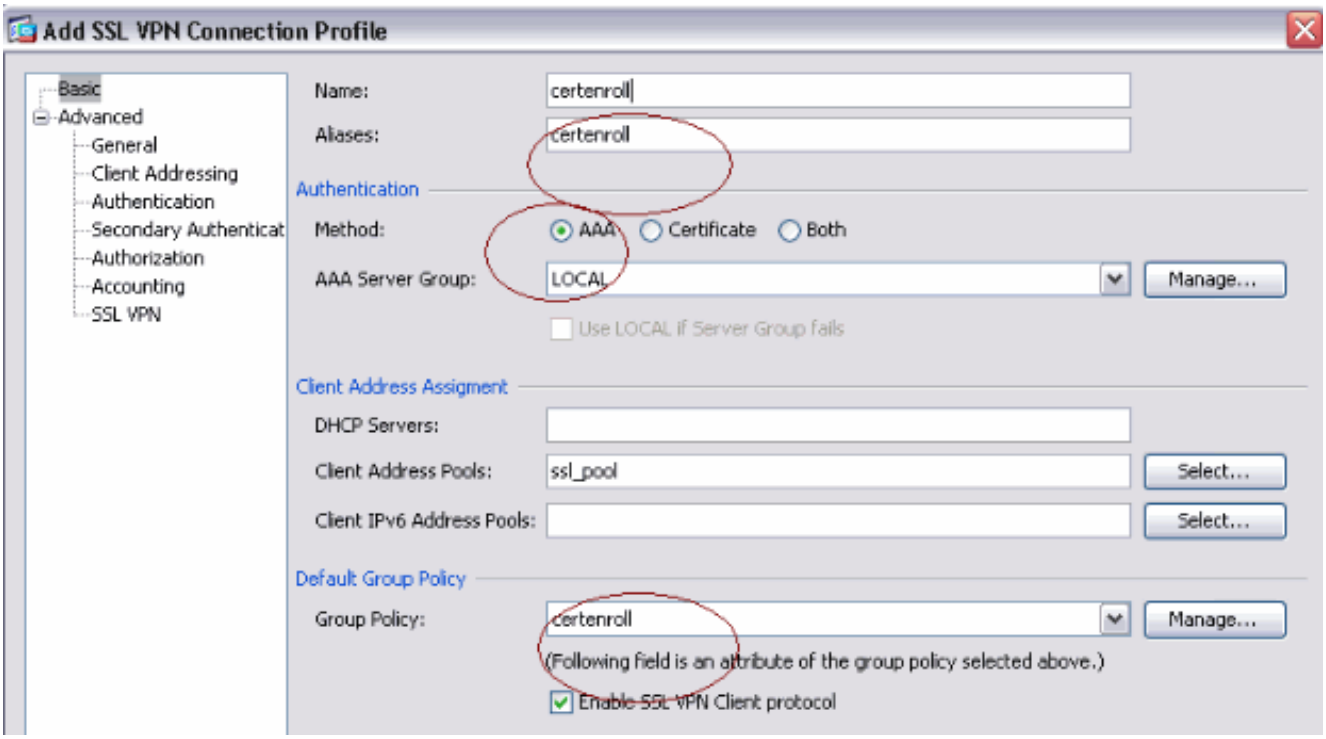
3. 인증서 인증을 위해 certauth라는 다른 그룹을 생성합니다

.



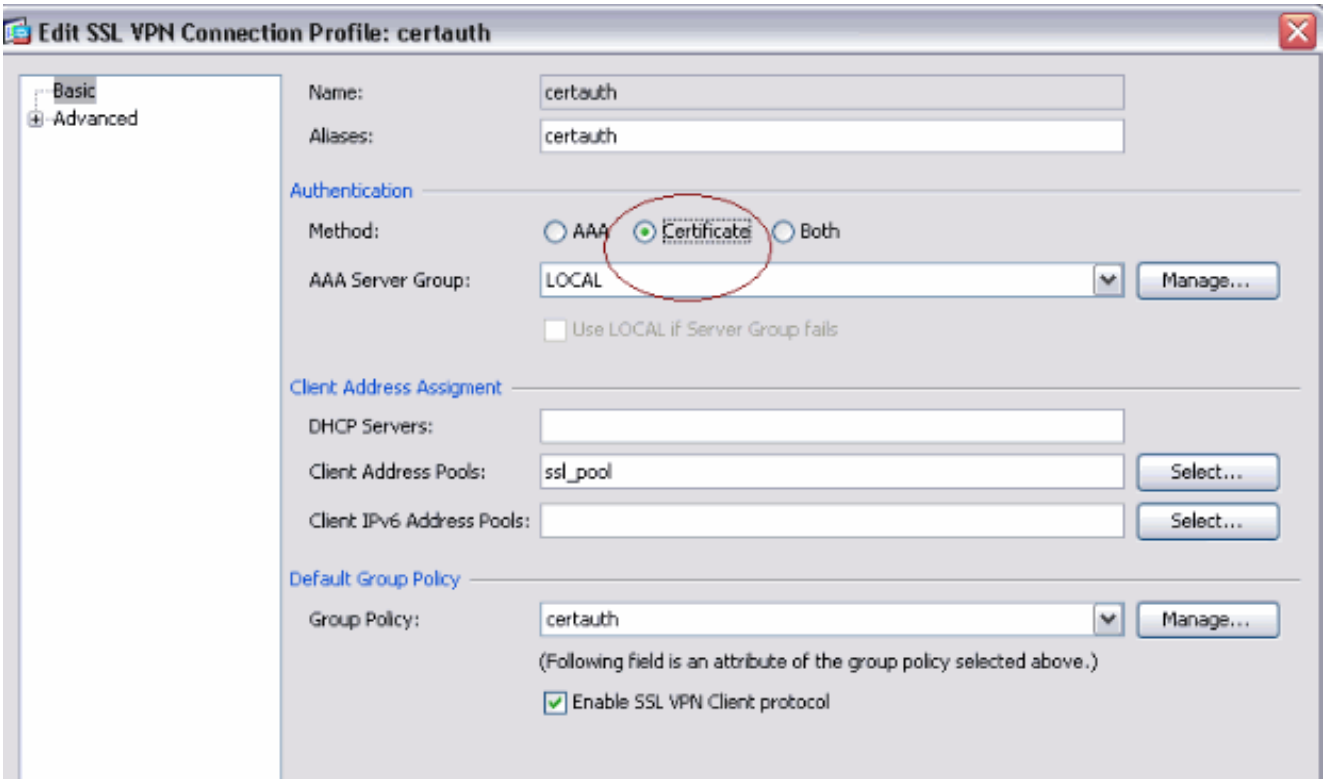
4. certenroll 연결 프로파일을 생성합니다.Remote **access VPN(원격 액세스 VPN) > Network client access(네트워크 클라이언트 액세스) > AnyConnect 연결 프로파일**을 선택하고 **Add(추가)**를 클릭합니다.별칭 필드에 **certenroll** 그룹을 입력합니다.**참고:** 별칭 이름은 AutomaticSCEPHost 아래의 AnyConnect 프로필에 사용된 값과 일치해야 합니다

.



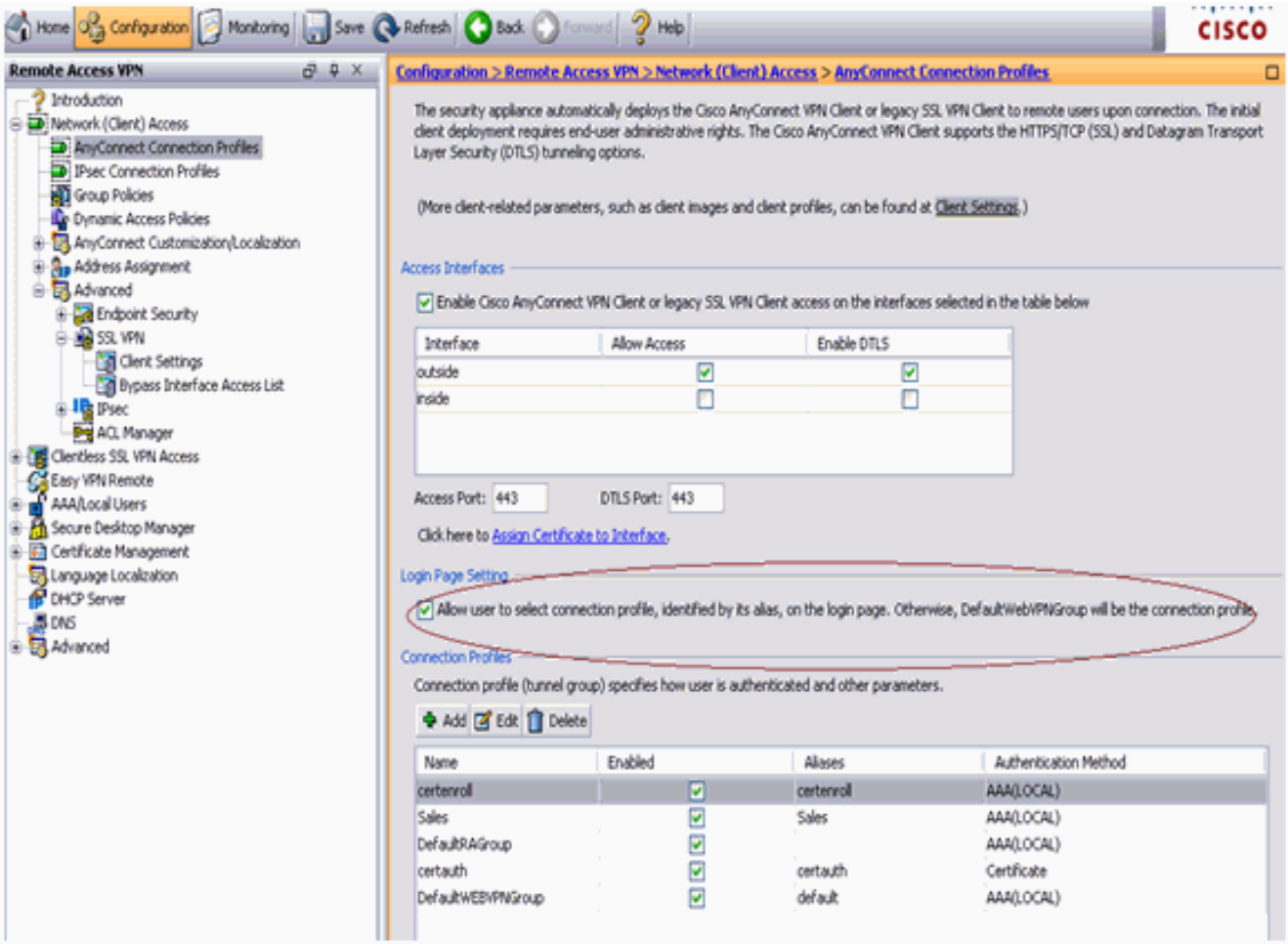
5. 인증서 인증을 사용하여 certauth라는 다른 연결 프로파일을 만듭니다.등록 후에 사용되는 실제 연결 프로파일입니다

.



6. 별칭 사용이 활성화되었는지 확인하려면 **로그인 페이지에서 사용자**가 **별칭으로 식별된 연결 프로파일을 선택할 수 있도록 허용을** 선택합니다.**그렇지 않으면 DefaultWebVPNGroup이 연결 프로파일입니다**

.



AnyConnect SCEP 테스트

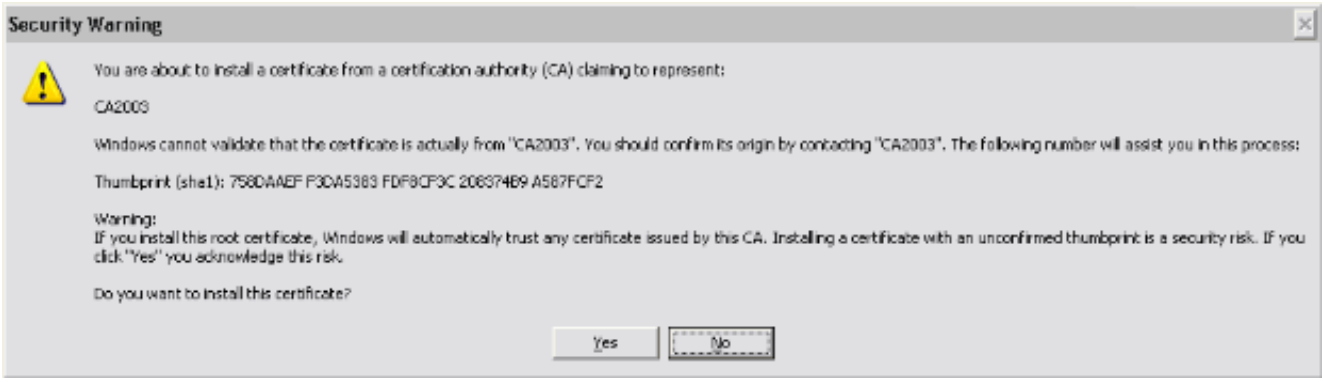
이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

1. AnyConnect 클라이언트를 시작하고 certenroll 프로필에 연결합니다

AnyConnect는 SCEP를 통해 등록 요청을 CA 서버로 전달합니다

Get Certificate 버튼을 사용하는 경우 AnyConnect는 등록 요청을 직접 전달하며 터널을 거치지 않습니다

2. 이 경고가 나타납니다.사용자 및 루트 인증서를 설치하려면 **예**를 클릭하십시오



3. 인증서가 등록되면 인증서 프로필에 **연결합니다**.

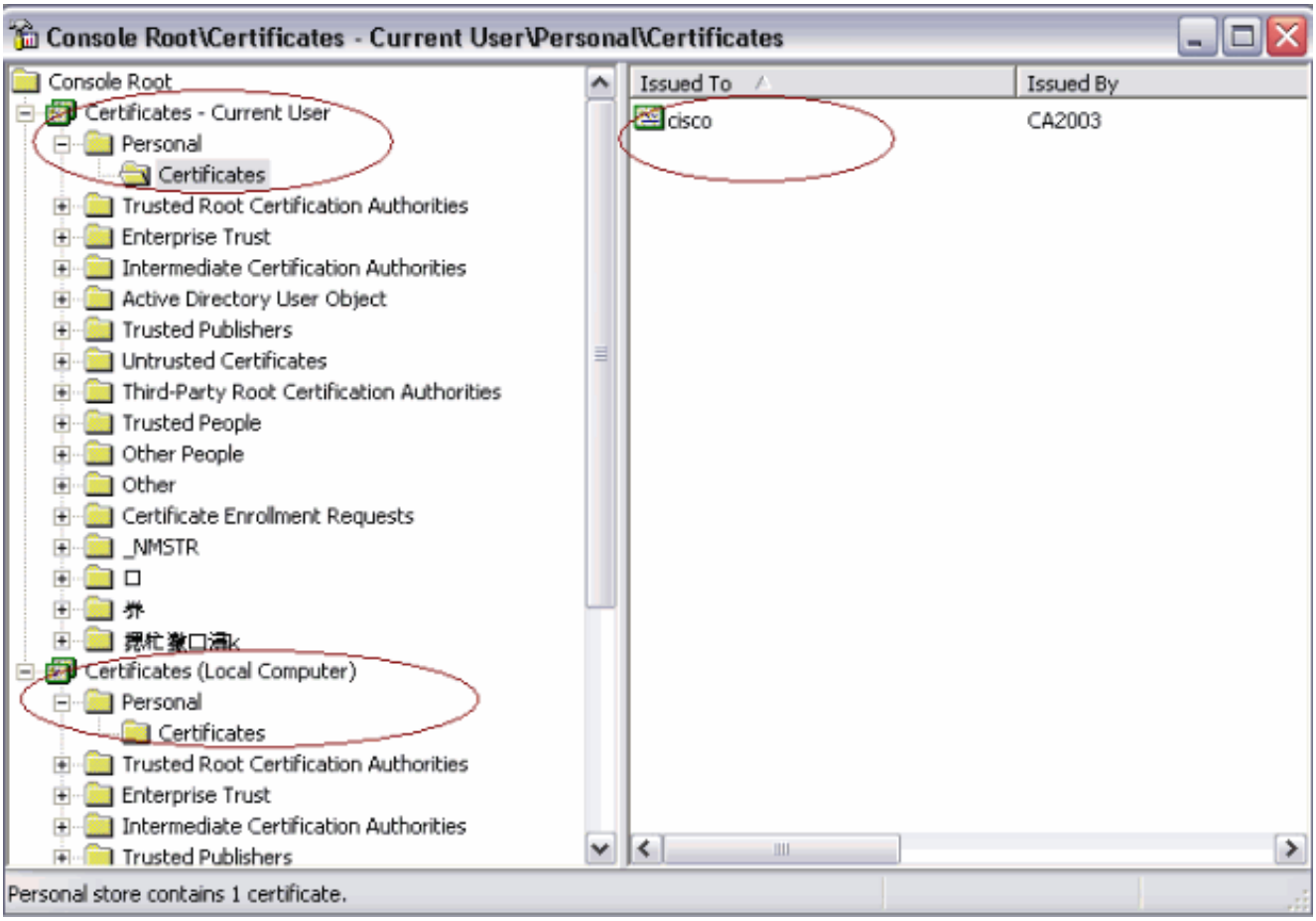
SCEP 요청 후 Microsoft Windows의 인증서 저장소

다음 단계를 완료하십시오.

1. 시작 **> 실행 > mmc를 클릭합니다**.
2. 스냅인 **추가/제거를 클릭합니다**.

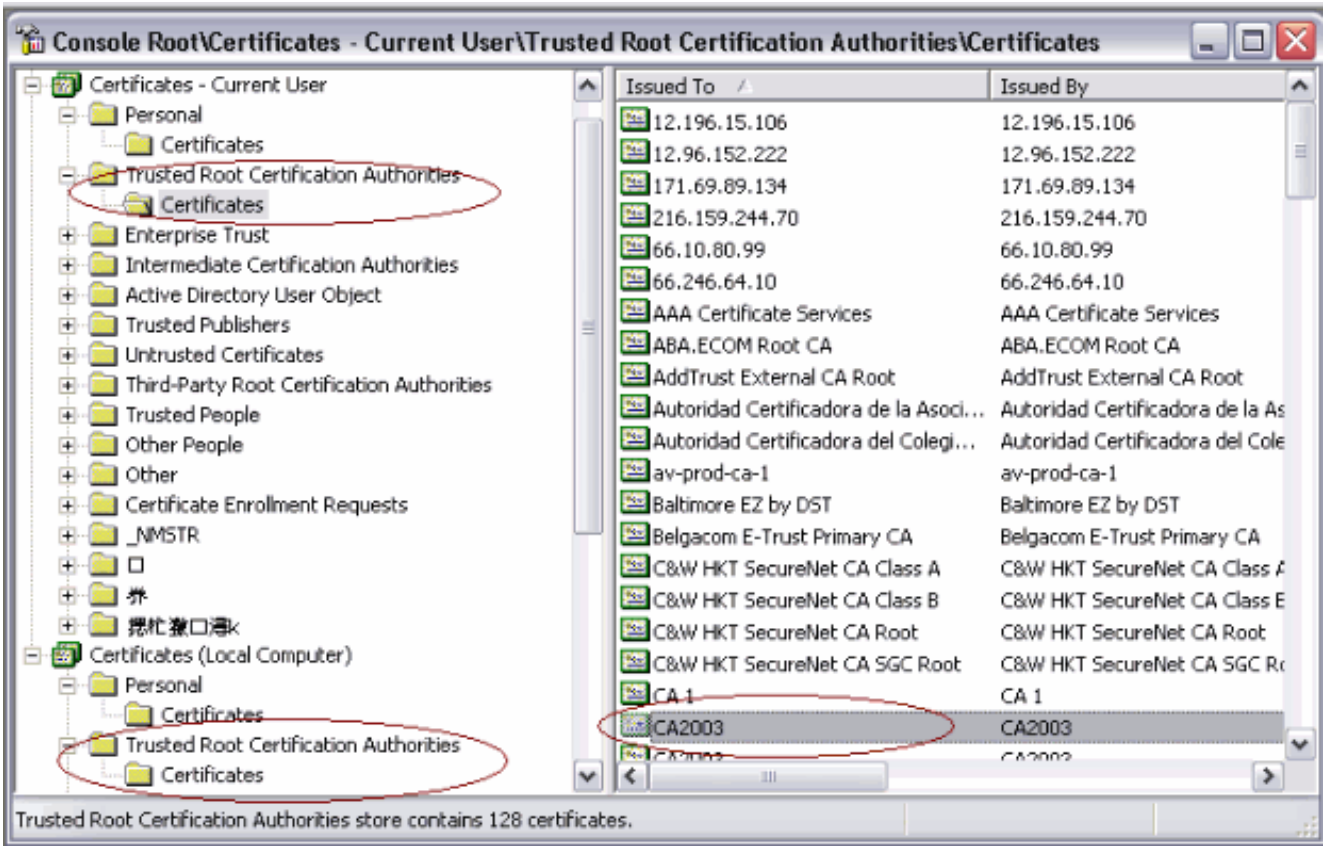
3. Add(**추가**)를 클릭하고 **인증서**를 선택합니다.
4. 내 **사용자 계정** 및 **컴퓨터 계정** 인증서를 추가합니다.이 그림에서는 Windows 인증서 저장소에 설치된 사용자 인증서를 보여 줍니다

.



이 그림에서는 Windows 인증서 저장소에 설치된 CA 인증서를 보여 줍니다

.



문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

- AnyConnect SCEP 등록은 인증서 인증이 실패할 경우에만 작동합니다.등록 중이 아니면 인증서 저장소를 확인합니다.인증서가 이미 설치되어 있으면 삭제하고 다시 테스트하십시오.
- **포트 443** 명령을 제외한 **ssl certificate-authentication interface outside**를 사용하지 않으면 SCEP 등록이 작동하지 않습니다.자세한 내용은 다음 Cisco 버그 ID를 참조하십시오.Cisco Bug ID CSCtf06778(등록된 고객만 해당) —AnyConnect SCEP 등록은 Per Group Cert Auth 2에서 작동하지 않습니다.Cisco Bug ID CSCtf06844(등록된 고객만 해당) —AnyConnect SCEP 등록이 ASA Per Group Cert Auth로 작동하지 않음
- CA 서버가 ASA 외부에 있는 경우 **same-security-traffic permit intra-interface** 명령을 사용하여 헤어피닝**을 허용해야** 합니다.또한 다음 예와 같이 nat outside 및 access-list 명령을 추가합니다.

```
nat (outside) 1
access-list natoutside extended permit ip 172.16.1.0 255.255.255.0 host 171.69.89.87
```

여기서 172.16.1.0은 AnyConnect 풀이며 171.69.89.87은 CA 서버 IP 주소입니다.

- CA 서버가 내부에 있는 경우 certenroll 그룹 정책에 대한 스플릿 터널 액세스 목록에 포함시켜야 **합니다**.이 문서에서는 CA 서버가 내부에 있는 것으로 가정합니다.

```
group-policy certenroll attributes
split-tunnel-policy tunnelspecified
 split-tunnel-network-list value scep

access-list scep standard permit 171.69.89.0 255.255.255.0
```

관련 정보

- Cisco AnyConnect VPN 클라이언트 관리자 가이드, 릴리스 2.4
- 기술 지원 및 문서 – Cisco Systems