

ASA를 로컬 CA 서버 및 AnyConnect 헤드엔드로 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[로컬 CA 서버로서의 ASA](#)

[1단계. ASA에서 로컬 CA 서버 구성 및 활성화](#)

[2단계. ASA 데이터베이스에 사용자 생성 및 추가](#)

[3단계. WAN 인터페이스에서 webvpn 활성화](#)

[4단계. 클라이언트 컴퓨터에서 인증서 가져오기](#)

[AnyConnect 클라이언트에 대한 SSL 게이트웨이로서의 ASA](#)

[ASDM AnyConnect 컨피그레이션 마법사](#)

[AnyConnect용 CLI 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 Cisco ASA(Adaptive Security Appliance)를 Cisco AnyConnect Secure Mobility Client용 CA(Certificate Authority) 서버 및 SSL(Secure Sockets Layer) 게이트웨이로 설정하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 소프트웨어 버전 9.1.x를 실행하는 기본 ASA 구성
- ASDM 7.3 이상

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 9.1(6)을 실행하는 Cisco 5500 Series ASA
- Windows용 AnyConnect Secure Mobility Client 버전 4.x
- [호환성](#) 차트에 따라 지원되는 OS를 실행하는 PC.
- Cisco ASDM(Adaptive Security Device Manager) 버전 7.3

참고: Cisco [Software Download](#)([등록된](#) 고객만)에서 AnyConnect VPN 클라이언트 패키지 (anyconnect-win*.pkg)를 다운로드합니다. ASA와의 SSL VPN 연결을 설정하기 위해 원격 사용자 컴퓨터에 다운로드할 ASA의 플래시 메모리에 AnyConnect VPN 클라이언트를 복사합니다. 자세한 내용은 ASA [컨피그레이션 가이드](#)의 AnyConnect 클라이언트 설치 섹션을 참조하십시오.

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.

배경 정보

ASA의 Certificate Authority는 다음 기능을 제공합니다.

- ASA에서 기본 CA(Certificate Authority) 작업을 통합합니다.
- 인증서를 배포합니다.
- 발급된 인증서의 안전한 폐기 검사를 제공합니다.
- 브라우저 기반(WebVPN) 및 클라이언트 기반(AnyConnect) SSL VPN 연결과 함께 사용할 수 있도록 ASA에서 인증 기관을 제공합니다.
- 외부 인증서 권한 부여에 의존할 필요 없이 사용자에게 신뢰할 수 있는 디지털 인증서를 제공합니다.
- 인증서 인증을 위한 안전한 사내 권한을 제공하며 웹 사이트 로그인을 통해 사용자를 간편하게 등록할 수 있습니다.

지침 및 제한 사항

- 라우팅 및 투명 방화벽 모드에서 지원됩니다.
- 한 번에 하나의 로컬 CA 서버만 ASA에 상주할 수 있습니다.
- 로컬 CA 서버 기능으로서의 ASA는 장애 조치 설정에서 지원되지 않습니다.
- 현재 로컬 CA 서버로 작동하는 ASA는 SHA1 인증서 생성만 지원합니다.
- 로컬 CA 서버는 브라우저 기반 및 클라이언트 기반 SSL VPN 연결에 사용할 수 있습니다. 현재 IPsec에 대해 지원되지 않습니다.
- 로컬 CA에 대해 VPN 부하 균형을 지원하지 않습니다.
- 로컬 CA는 다른 CA의 하위 CA가 될 수 없습니다. 루트 CA로만 작동할 수 있습니다.
- 현재 ASA는 ID 인증서에 대해 로컬 CA 서버에 등록할 수 없습니다.
- 인증서 등록이 완료되면 ASA는 사용자의 키 쌍 및 인증서 체인을 포함하는 PKCS12 파일을 저장합니다. 이 경우 등록당 약 2KB의 플래시 메모리 또는 디스크 공간이 필요합니다. 실제 디스크 공간 크기는 구성된 RSA 키 크기 및 인증서 필드에 따라 달라집니다. 사용 가능한 플래시 메모리의 양이 제한된 ASA에서 보류 중인 인증서 등록을 많이 추가할 때는 이 지침을 염두

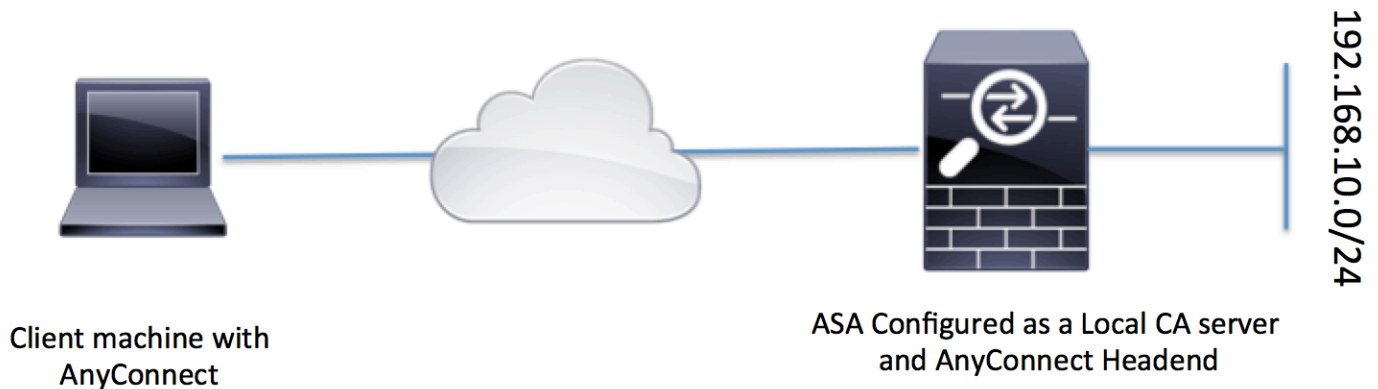
에 두십시오. 이러한 PKCS12 파일은 구성된 등록 검색 시간 제한 동안 플래시 메모리에 저장되기 때문입니다.

구성

이 섹션에서는 Cisco ASA를 로컬 CA 서버로 구성하는 방법에 대해 설명합니다.

참고: 이 섹션에서 사용된 [명령어](#) 대한 자세한 내용을 보려면 [Command Lookup Tool](#)([등록된 고객만 해당](#))을 사용하십시오.

네트워크 다이어그램



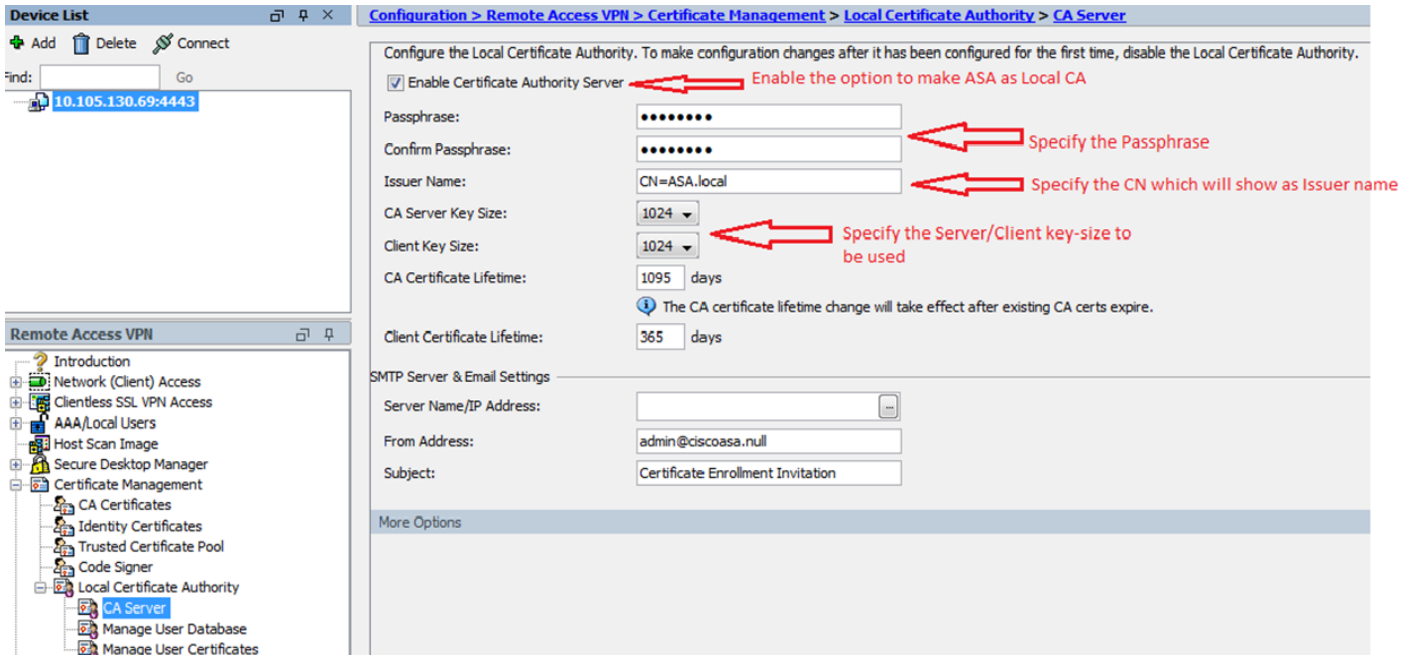
로컬 CA 서버로서의 ASA

1단계. ASA에서 로컬 CA 서버 구성 및 활성화

- Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Certificate Management(인증서 관리) > Local Certificate Authority(로컬 인증 기관) > CA Server(CA 서버)로 이동합니다. Enable Certificate Authority 서버 옵션을 선택합니다.
- 암호를 구성합니다. 패스프레이즈는 로컬 CA 인증서 및 키 쌍을 포함하는 PKCS12 파일을 인코딩하고 저장하는 데 사용되는 7자 이상이어야 합니다. CA 인증서 또는 키 쌍이 손실된 경우 이 패스프레이즈는 PKCS12 아카이브의 잠금을 해제합니다.
- 발급자 이름을 구성합니다. 이 필드는 루트 인증서 CN으로 표시됩니다. CN(Common Name), OU(Organization Unit), (O) Organization, L(Locality), S(State) 및 C(Country) 형식으로 지정할 수 있습니다.
- 선택적 컨피그레이션: 등록을 완료하기 위해 메일을 통해 최종 클라이언트에 OTP를 수신할 수 있도록 SMTP 서버 및 이메일 서버 설정을 구성합니다. 로컬 이메일/SMTP 서버의 호스트 이름 또는 IP 주소를 구성할 수 있습니다. 또한 클라이언트가 수신할 이메일의 From 주소 및

Subject 필드를 구성할 수 있습니다. 기본적으로 발신 주소는 admin@<ASA hostname>.null이고 제목은 Certificate Enrollment Invitation입니다.

- 선택적 컨피그레이션: 클라이언트 키 크기, CA 서버 키 크기, CA 인증서 수명 및 클라이언트 인증서 수명과 같은 선택적 매개 변수를 구성할 수도 있습니다.



CLI에 준하는 기능:

```
ASA(config)# crypto ca server
ASA(config-ca-server)# issuer-name CN=ASA.local
ASA(config-ca-server)# subject-name-default CN=ASA.local
ASA(config-ca-server)# lifetime certificate 365
ASA(config-ca-server)# lifetime ca-certificate 1095
ASA(config-ca-server)# passphrase cisco123
ASA(config-ca-server)# no shutdown
% Some server settings cannot be changed after CA certificate generation.
Keypair generation process begin. Please wait...
```

Completed generation of the certificate and keypair...

Archiving certificate and keypair to storage... Complete

이는 Local CA Server(로컬 CA 서버) 컨피그레이션에서 구성할 수 있는 추가 필드입니다.

<p>CRL 배포 지점 URL</p>	<p>ASA의 CRL 위치입니다. 기본 위치는 http://hostname.domain/+CSCOCA+/asa_ca.cr이지만 url을 수정할 수 있습니다.</p>
<p>Publish- CRL 인터</p>	<p>지정된 인터페이스 및 포트에서 HTTP 다운로드에 CRL을 사용하려면 드롭다운 목록에서 publish-CRL 인터페이스를 선택합니다. 그런 다음 포트 번호를 입력합니다. 이</p>

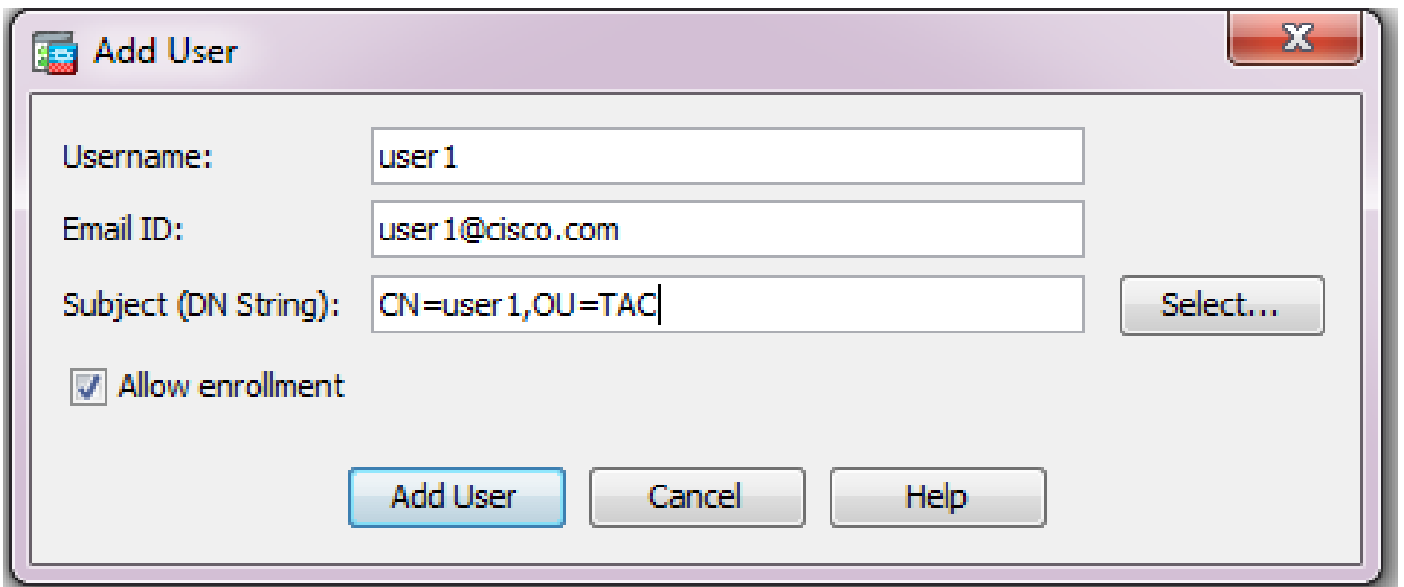
페이스 및 포트	는 1~65535의 포트 번호일 수 있습니다. 기본 포트 번호는 TCP 포트 80입니다.
CRL 수명	로컬 CA는 사용자 인증서가 폐기되거나 폐기되지 않을 때마다 CRL을 업데이트하고 재발급하지만, 폐기 변경이 없는 경우 CRL은 로컬 CA 컨피그레이션 중 lifetime crlcommand로 지정한 기간인 CRL 수명마다 한 번씩 자동으로 재발급됩니다. CRL 수명을 지정하지 않을 경우 기본 기간은 6시간입니다.
데이터베이스 저장소 위치	ASA는 로컬 CA 데이터베이스를 사용하여 사용자 정보, 발급된 인증서 및 해지 목록에 액세스하고 이를 구현합니다. 이 데이터베이스는 기본적으로 로컬 플래시 메모리에 상주하거나, ASA에 마운트되고 액세스할 수 있는 외부 파일 시스템에 상주하도록 구성할 수 있습니다.
기본 주체 이름	발급된 인증서의 사용자 이름에 추가할 기본 주체(DN 문자열)를 입력합니다. 허용된 DN 특성은 이 목록에 제공됩니다. ·CN(일반 이름)SN(성) ·O(조직 이름) ·L(지역) ·C(국가) ·OU(조직 단위) ·EA(이메일 주소) ·ST(주/도) ·T(제목)
등록 기간	사용자가 ASA에서 PKCS12 파일을 검색할 수 있는 등록 시간 제한을 시간 단위로 설정합니다. 기본값은 24시간입니다. 참고: 사용자가 사용자 인증서가 포함된 PKCS12 파일을 검색하기 전에 등록 기간이 만료되면 등록이 허용되지 않습니다.
1회 비밀번호 만료	OTP가 사용자 등록에 유효한 시간(시간)을 정의합니다. 이 기간은 사용자가 등록할 수 있는 시점부터 시작됩니다. 기본값은 72시간입니다.
인증서 만료 미리 알림	인증서 만료 전에 인증서 소유자에게 재등록 초기 알림을 보낼 일수를 지정합니다.

2단계. ASA 데이터베이스에 사용자 생성 및 추가

- Configuration(컨피그레이션) > Remote Access VPN(원격 액세스 VPN) > Certificate Management(인증서 관리) > Local Certificate Authority(로컬 인증 기관) > Manage User Database(사용자 데이터베이스 관리)로 이동합니다.Add(추가)를 클릭합니다.



- 이 이미지에 표시된 대로 사용자 이름, 이메일 ID 및 주체 이름을 통해 사용자 세부 정보를 지정합니다.



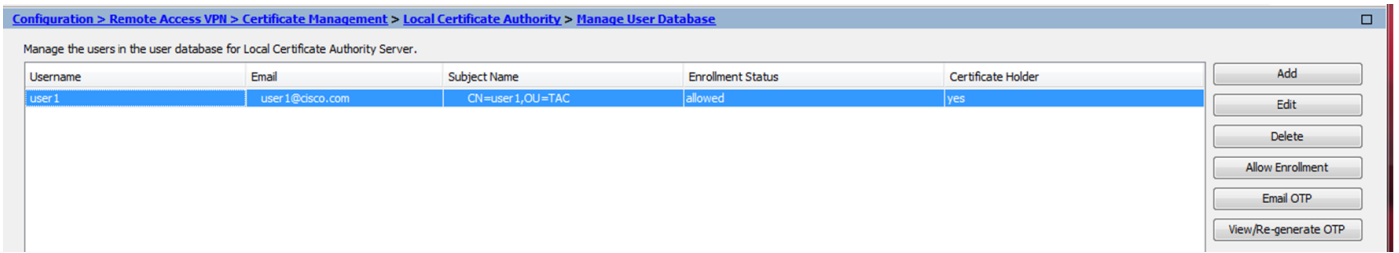
- 인증서에 대한 등록이 허용되도록 Allow Enrollment(등록 허용)가 선택되어 있는지 확인합니다.
- 사용자 컨피그레이션을 완료하려면 Add User를 클릭합니다.

CLI에 준하는 기능:

<#root>

```
ASA(config)# crypto ca server user-db add user1 dn CN=user1,OU=TAC email user1@cisco.com
```

- 사용자가 사용자 데이터베이스에 추가되면 등록 상태가 Allowed to Enroll(등록 허용)로 표시 됩니다.



사용자 상태를 확인하는 CLI:

<#root>

```
ASA# show crypto ca server user-db
```

```
username: user1
email:    user1@cisco.com
dn:      CN=user1,OU=TAC
allowed: 19:03:11 UTC Thu Jan 14 2016
notified: 1 times
enrollment status:

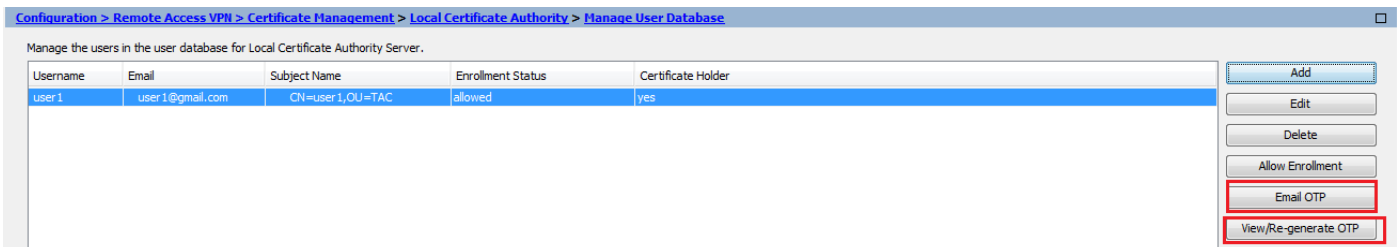
Allowed to Enroll
```

- 사용자가 사용자 데이터베이스에 추가되면 다음 중 하나를 사용하여 사용자가 등록을 완료할 수 있도록 OTP(One Time Password)를 제공할 수 있습니다.

OTP에 이메일을 보냅니다(CA 서버 컨피그레이션에서 SMTP 서버 및 이메일 설정을 구성해야 함).

또는

View/Re-generate OTP(OTP 보기/재생성)를 클릭하여 OTP를 직접 보고 사용자와 공유합니다. 또한 OTP를 재생성하는 데에도 사용할 수 있습니다.



CLI에 준하는 기능:

```
!! Email the OTP to the user
ASA# crypto ca server user-db allow user1 email-otp
```

```
!! Display the OTP on terminal
ASA# crypto ca server user-db allow user1 display-otp
Username: user1
```

OTP: 18D14F39C8F3DD84

Enrollment Allowed Until: 14:18:34 UTC Tue Jan 12 2016

3단계. WAN 인터페이스에서 webvpn 활성화

- 클라이언트가 등록을 요청하도록 ASA에서 웹 액세스를 활성화합니다.

!! Enable web-access on the "Internet" interface of the ASA

```
ASA(config)# webvpn
```

```
ASA(config-webvpn)#enable Internet
```

4단계. 클라이언트 컴퓨터에서 인증서 가져오기

- 클라이언트 워크스테이션에서 브라우저를 열고 링크로 이동하여 등록을 완료합니다.
- 이 링크에서 사용되는 IP/FQDN은 해당 단계에서 webvpn이 활성화된 인터페이스의 IP(인터페이스 인터넷)여야 합니다.

<#root>

<https://>

.

.

.

_____<>

.

.

_____ [IP/FQDN>/+CSCOCA+/enroll.html](https://IP/FQDN/+CSCOCA+/enroll.html)

.

.

_____<>

- [사용자 이름\(ASA에서 2단계, 옵션 A에 구성됨\)과 OTP를 입력합니다. 이는 이메일을 통해 제공되었거나 수동으로 제공되었습니다.](https://IP/FQDN/+CSCOCA+/enroll.html)

Browser window showing the ASA - Local Certificate Authority login page. The URL is <https://10.105.130.69/+CSCOCA+/login.html>. The page title is "ASA - Local Certificate Authority".

The login form contains the following fields and buttons:

- Username: user1
- One-time Password: [Redacted]
- Submit button
- Reset button

A red arrow points to the One-time Password field with the text "Enter the User-Name and OTP provided".


NOTE: On successful authentication:

- Open or Save the generated certificate
- Install the certificate in the browser store
- Close all the browser windows, and
- Restart the SSL VPN connection

- [ASA에서 받은 클라이언트 인증서를 직접 설치하려면 Open\(열기\)을 클릭합니다.](#)
- [클라이언트 인증서를 설치하기 위한 암호가 이전에 받은 OTP와 동일합니다.](#)

File Download dialog box showing the following information:

Do you want to open or save this file?

 Name: user1.p12
Type: Personal Information Exchange
From: 10.105.130.214

Buttons: Open, Save, Cancel

Warning: While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. [What's the risk?](#)

- [Next\(다음\)를 클릭합니다.](#)



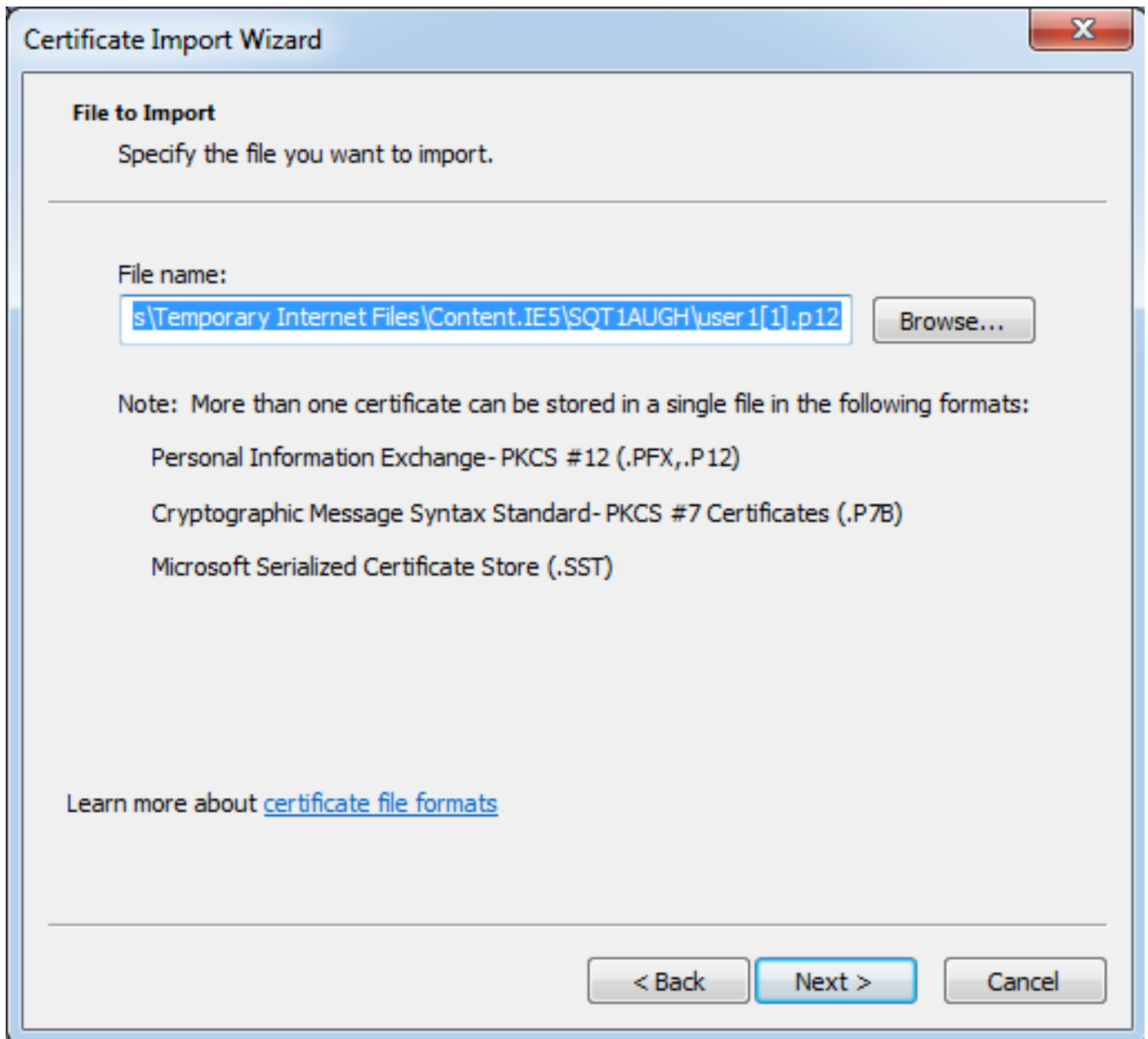
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

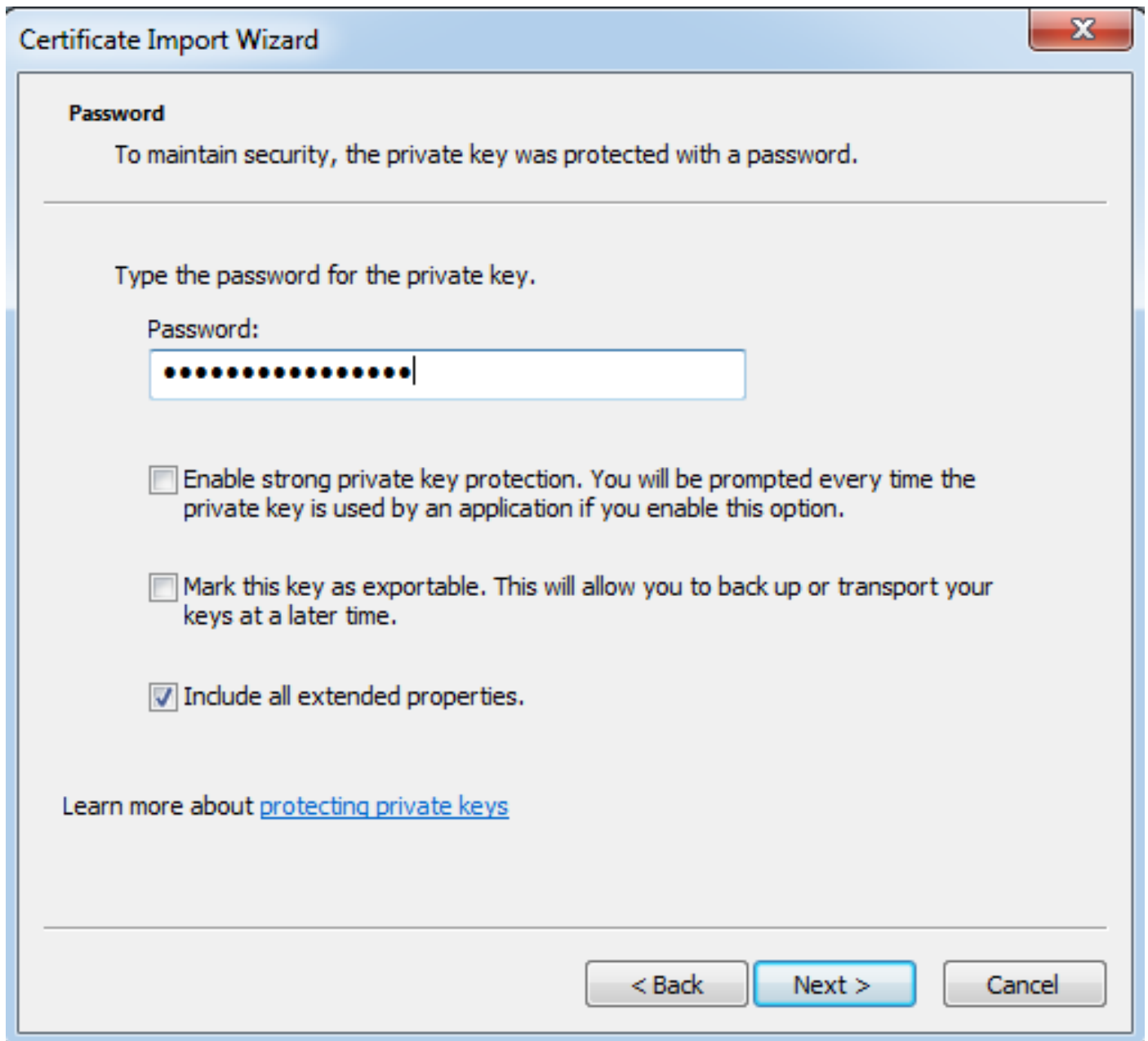
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

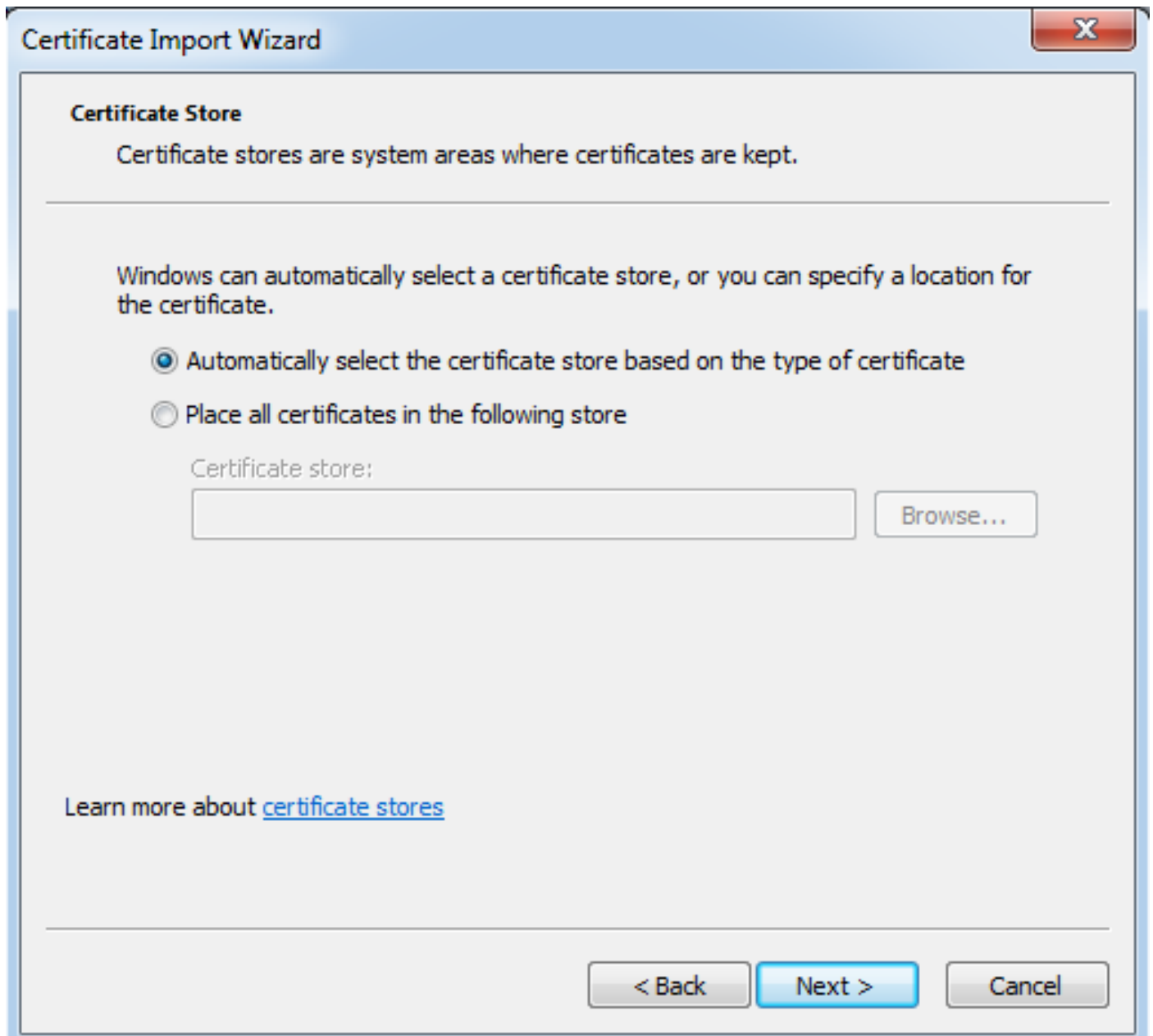
- [경로를 기본값으로 유지하고 Next\(다음\)를 클릭합니다.](#)



- [Password\(비밀번호\) 필드에 OTP를 입력합니다.](#)
- [필요한 경우 나중에 워크스테이션에서 키를 내보낼 수 있도록 이 키를 내보낼 수 있는 것으로 표시하는 옵션을 선택할 수 있습니다.](#)
- [Next\(다음\)를 클릭합니다.](#)



- [특정 인증서 저장소에 인증서를 수동으로 설치하거나 저장소를 자동으로 선택하도록 남겨 둘 수 있습니다.](#)
- [Next\(다음\)를 클릭합니다.](#)



- [설치를 완료하려면 Finish\(마침\)를 클릭합니다.](#)

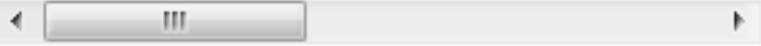


Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

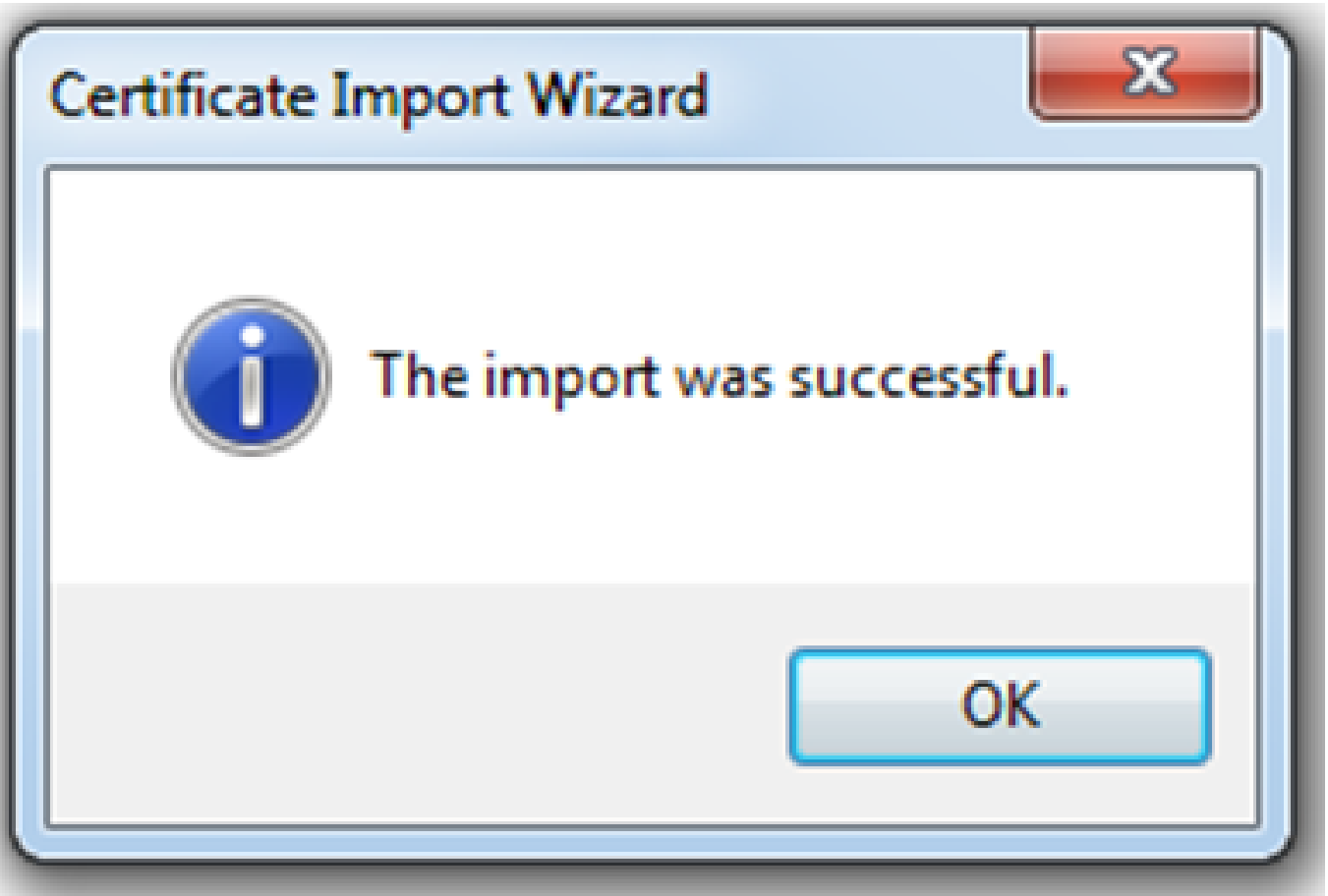
Certificate Store Selected	Automatically determined by t
Content	PFX
File Name	C:\Users\mrsethi\AppData\Lo



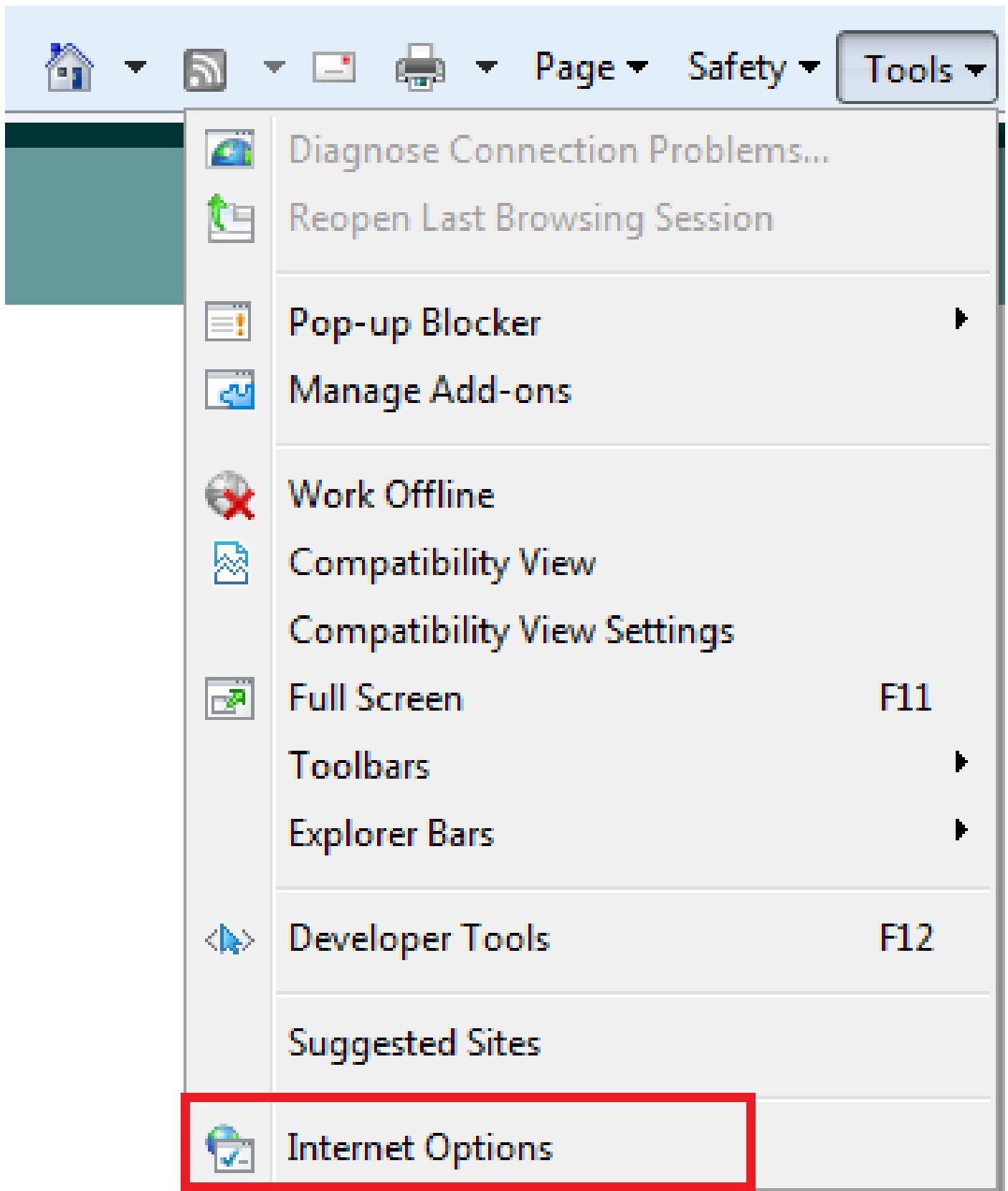
< Back

Finish

Cancel

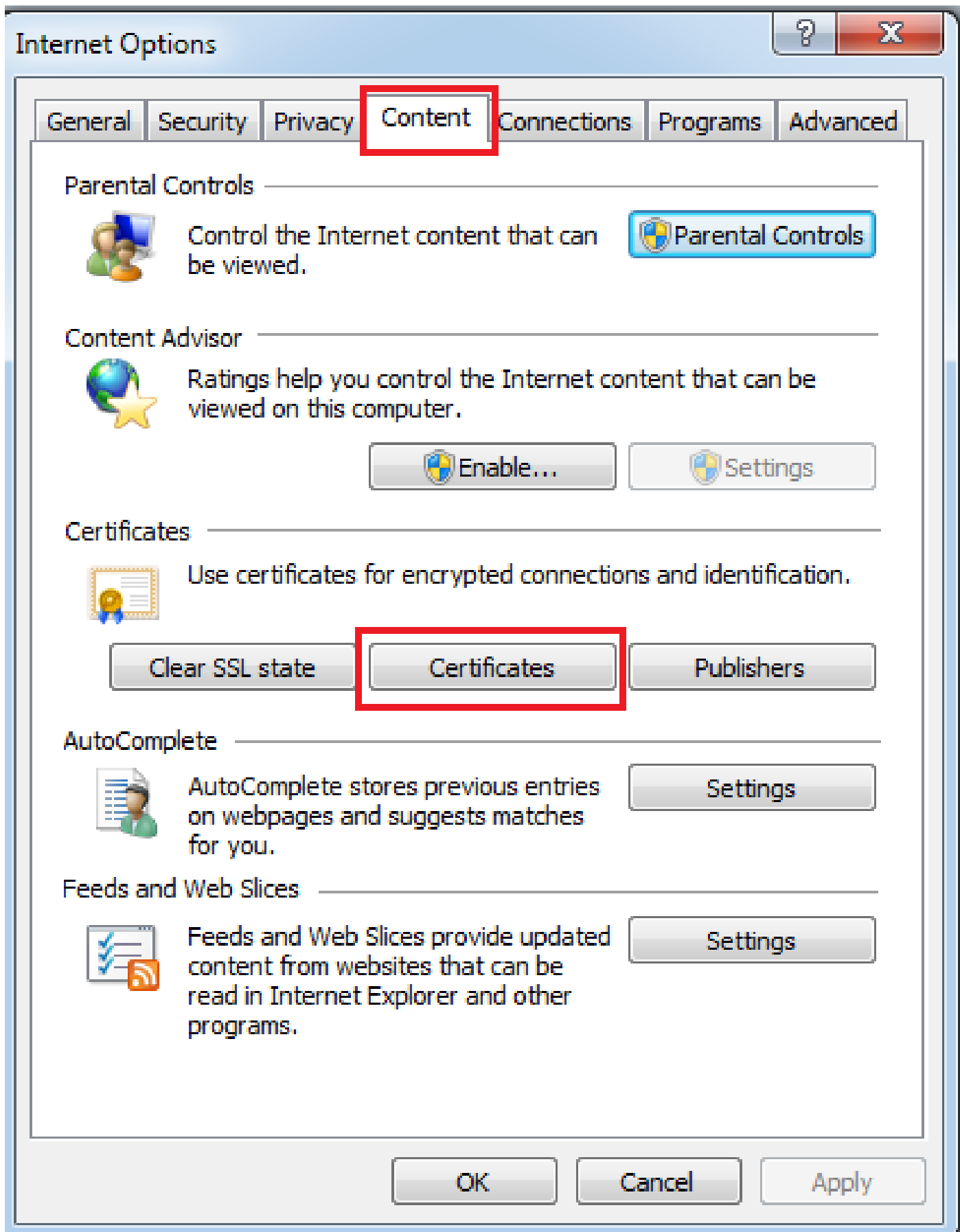


- [인증서가 성공적으로 설치되면 이를 확인할 수 있습니다.](#)
- [IE를 열고 Tools > Internet Options로 이동합니다.](#)

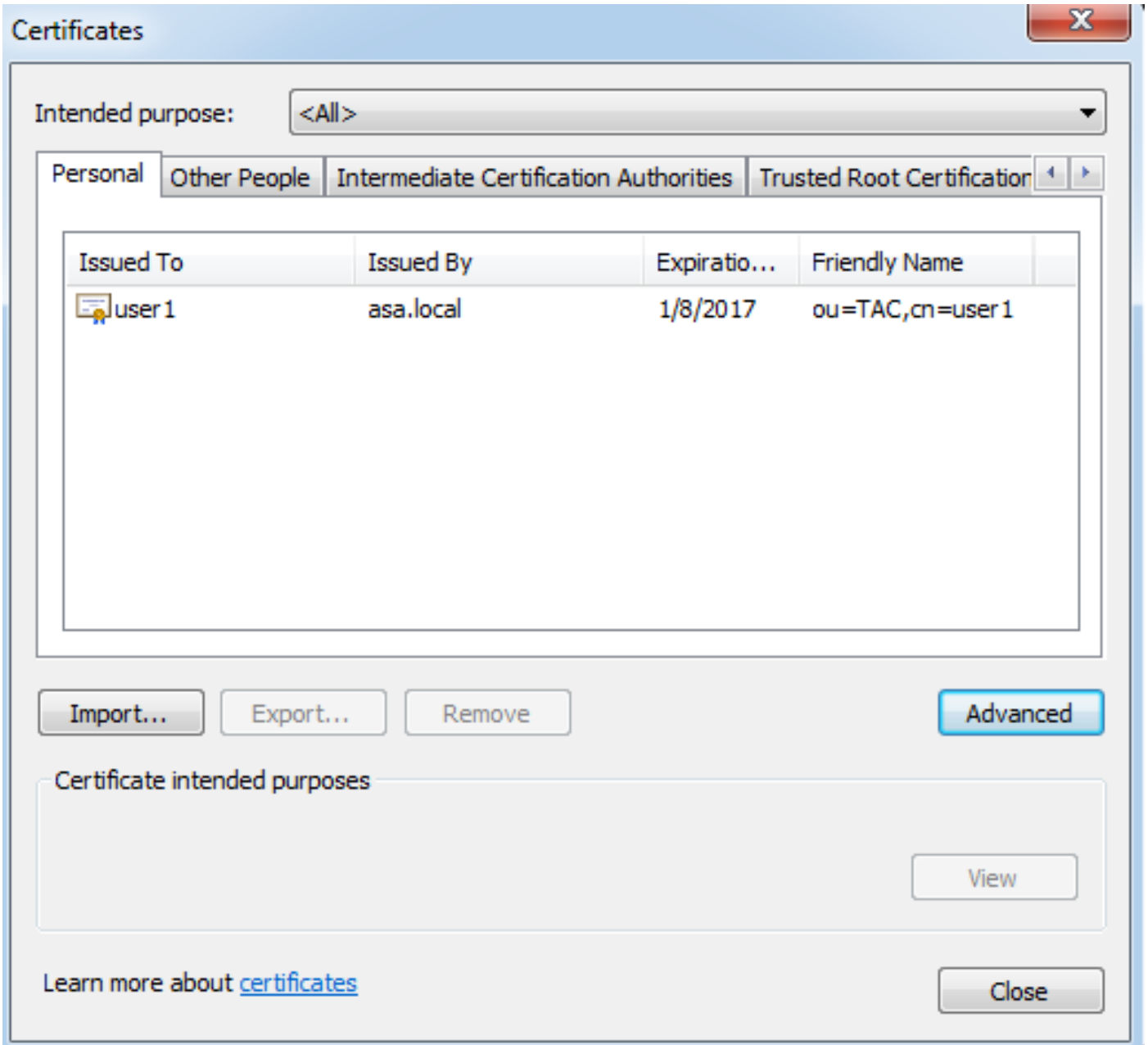


- [이 이미지에 표시된 대로 Content\(콘텐츠\) 탭으로 이동하고 Certificates\(인증서\)를 클릭합니다](#)

•



- [Personal store\(개인 저장소\) 아래에서 ASA에서 받은 인증서를 확인할 수 있습니다.](#)



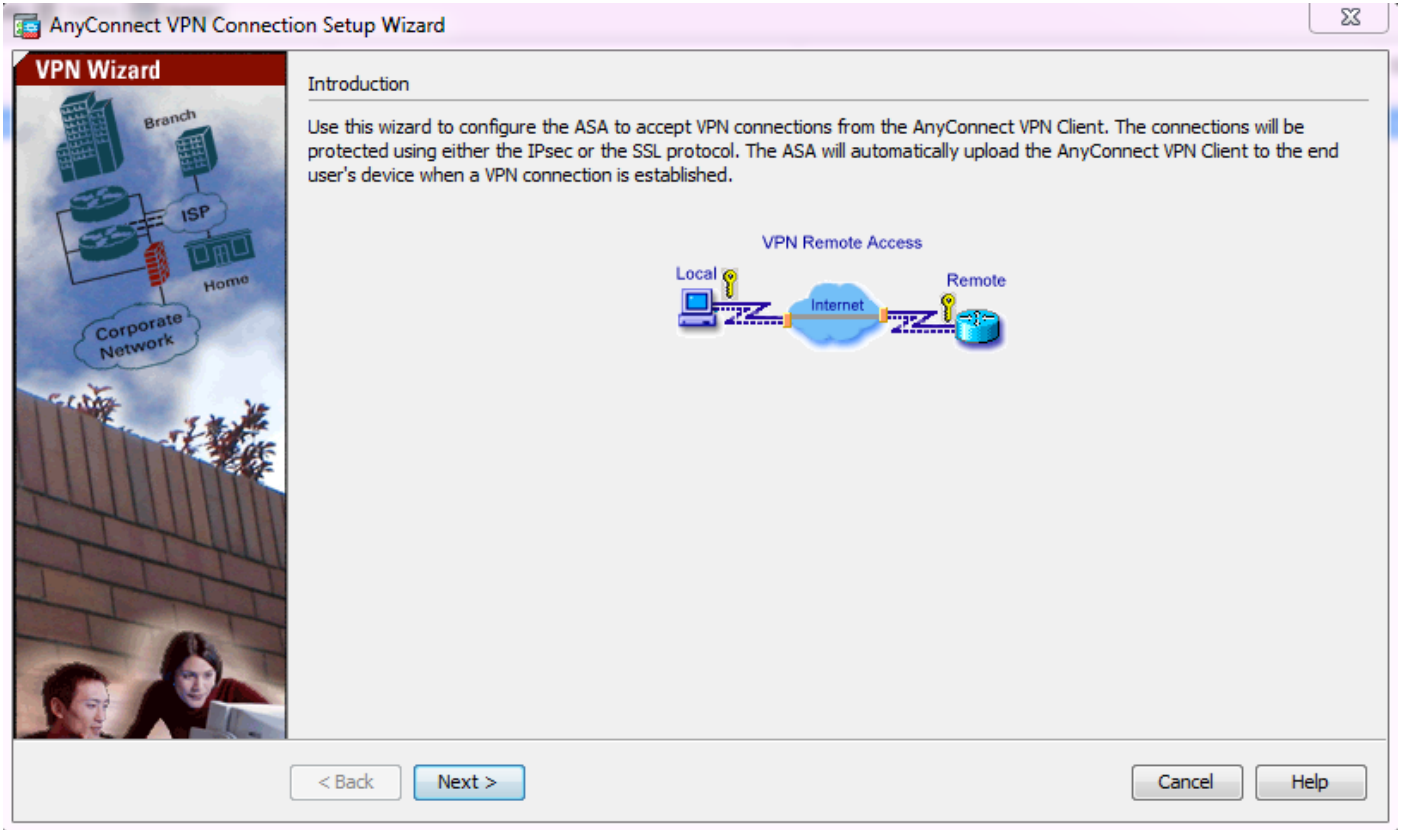
AnyConnect 클라이언트에 대한 SSL 게이트웨이로서의 ASA

ASDM AnyConnect 컨피그레이션 마법사

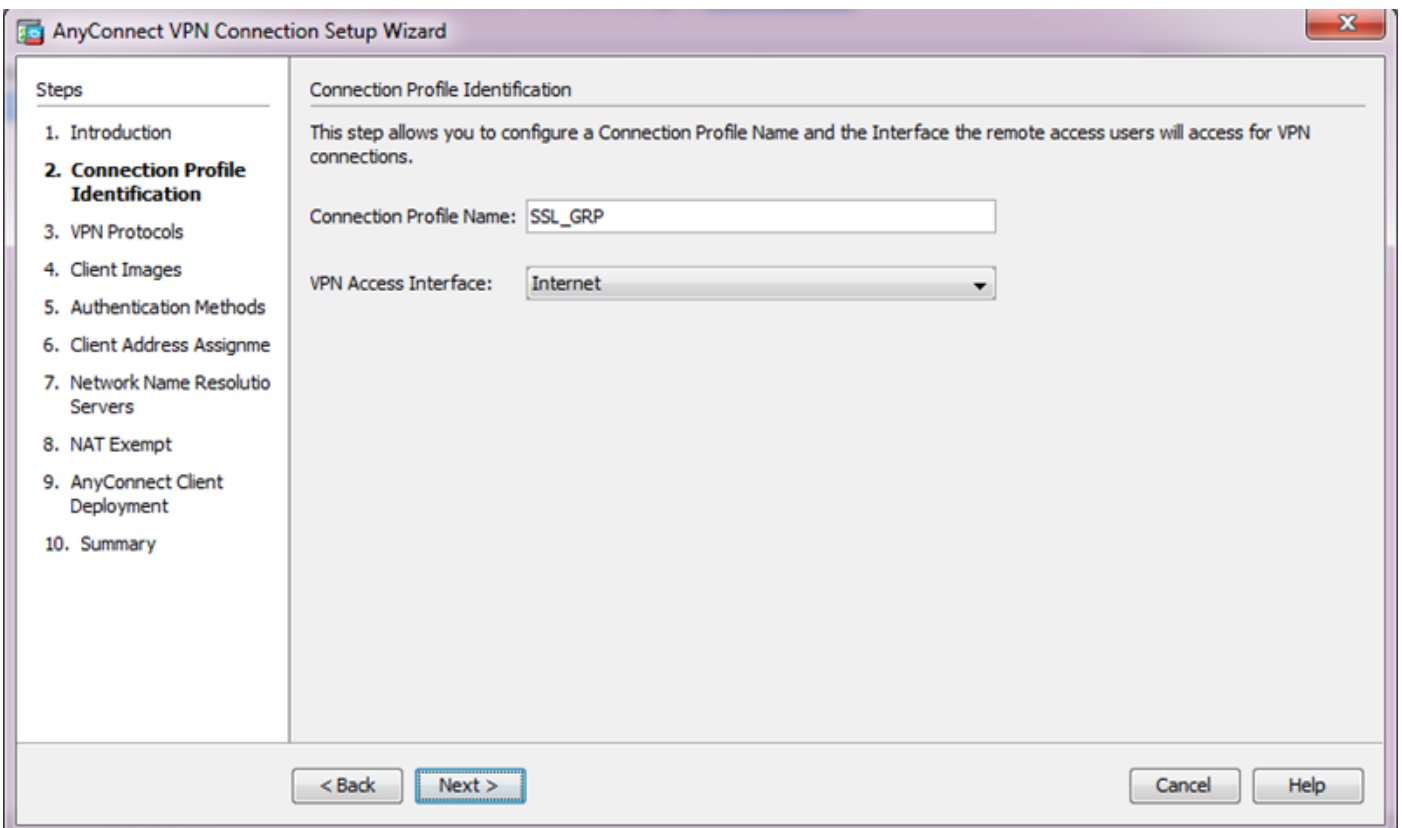
AnyConnect Secure Mobility Client를 구성하기 위해 AnyConnect 컨피그레이션 마법사/CLI를 사용할 수 있습니다. 계속하기 전에 AnyConnect 클라이언트 패키지가 ASA 방화벽의 플래시/디스크에 업로드되었는지 확인합니다.

컨피그레이션 마법사를 통해 AnyConnect Secure Mobility Client를 구성하려면 다음 단계를 완료하십시오.

1. ASDM에 로그인하고 Wizards(마법사) > VPN Wizards(VPN 마법사) > AnyConnect VPN Wizard(AnyConnect VPN 마법사)로 이동하여 Configuration Wizard(컨피그레이션 마법사)를 시작하고 Next(다음)를 클릭합니다.



2. 연결 프로파일 이름을 입력하고 VPN 액세스 인터페이스 드롭다운 메뉴에서 VPN이 종료될 인터페이스를 선택한 후 다음을 클릭합니다.



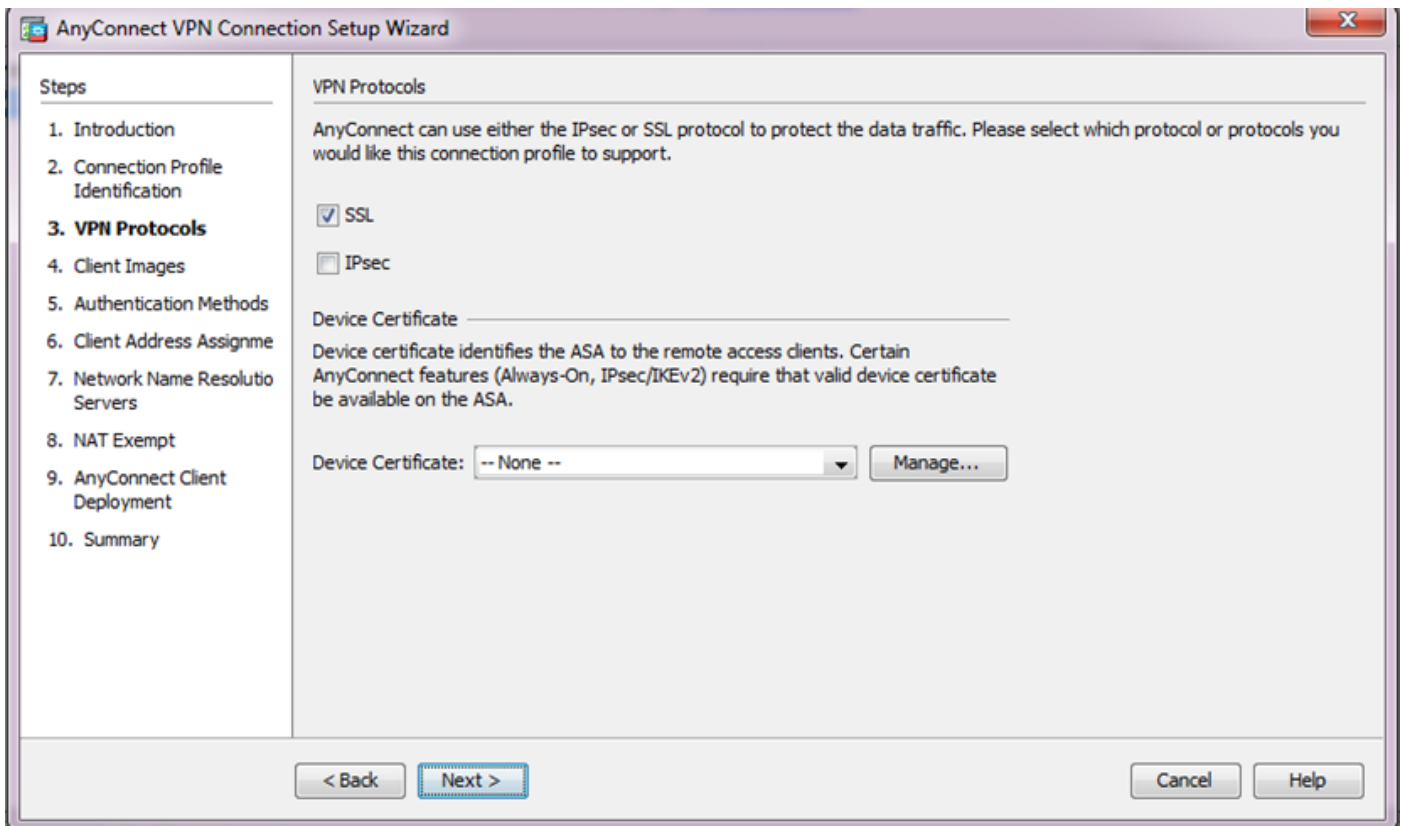
3. SSL(Secure Sockets Layer)을 활성화하려면 SSL 확인란을 선택합니다. 디바이스 인증서는 신뢰할 수 있는 서드파티 CA(Certificate Authority) 발급 인증서(예: Verisign 또는 Entrust) 또는 자체 서명 인증서일 수 있습니다. 인증서가 ASA에 이미 설치되어 있는 경우 드롭다운 메뉴를 통해 선택할

수 있습니다.

1. 참고: 이 인증서는 ASA에서 SSL 클라이언트에 제공할 서버측 인증서입니다. 자체 서명 인증서를 생성해야 하는 것보다 현재 ASA에 설치된 서버 인증서가 없으면 Manage(관리)를 클릭합니다.

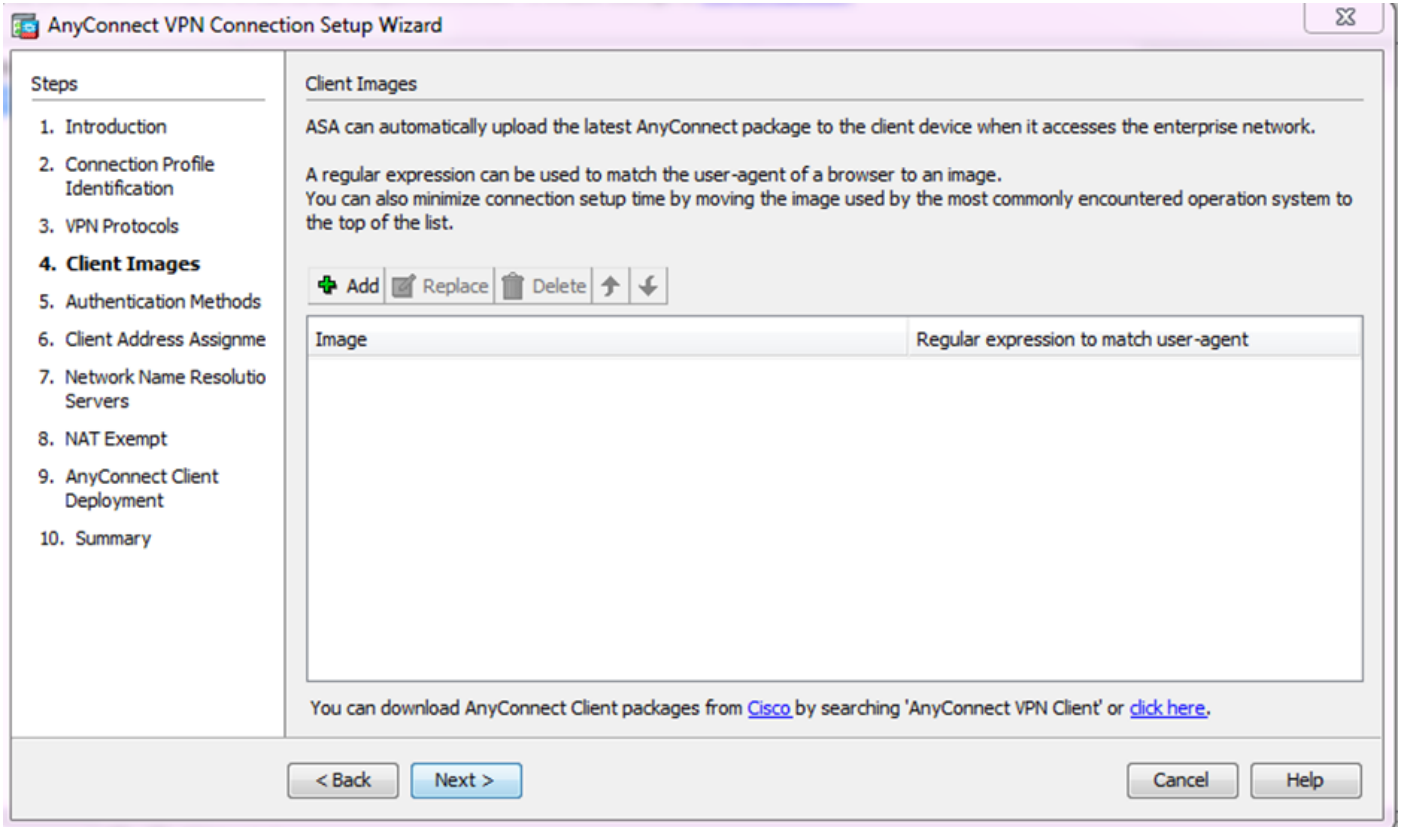
서드파티 인증서를 설치하려면 [ASA 8.x Manually Install 3rd Party Vendor Certificates for use with WebVPN Configuration](#) 예 Cisco 문서에 설명된 단계를 완료합니다.

- VPN 프로토콜 및 디바이스 인증서를 활성화합니다.
- Next(다음)를 클릭합니다.

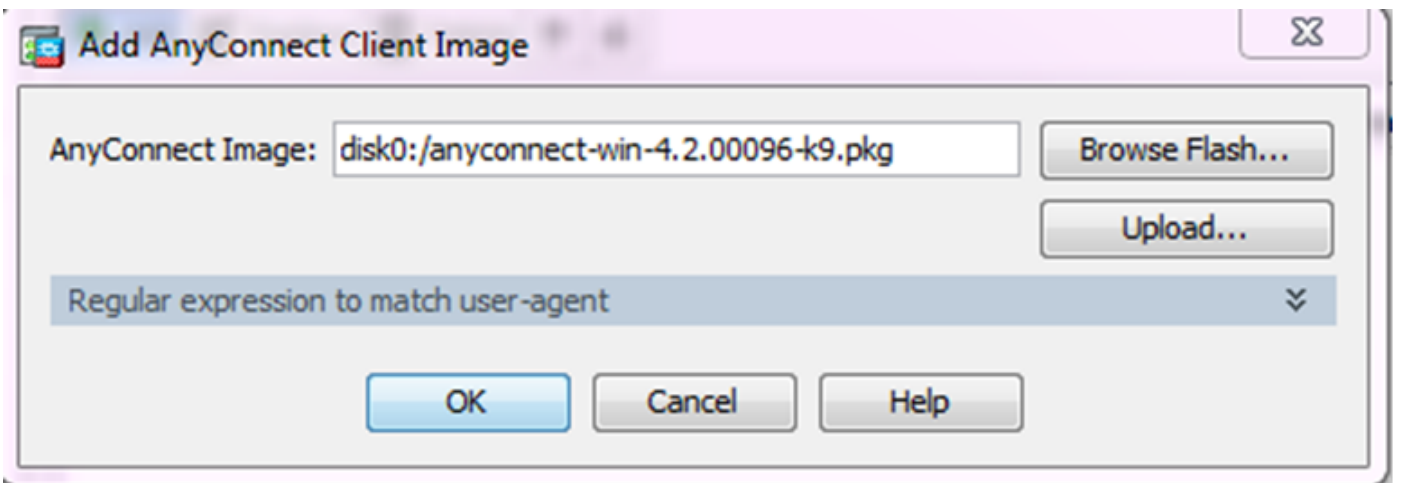


4. 로컬 드라이브 또는 ASA의 플래시/디스크에서 AnyConnect 클라이언트 패키지(.pkg 파일)를 추가하려면 Add를 클릭합니다.

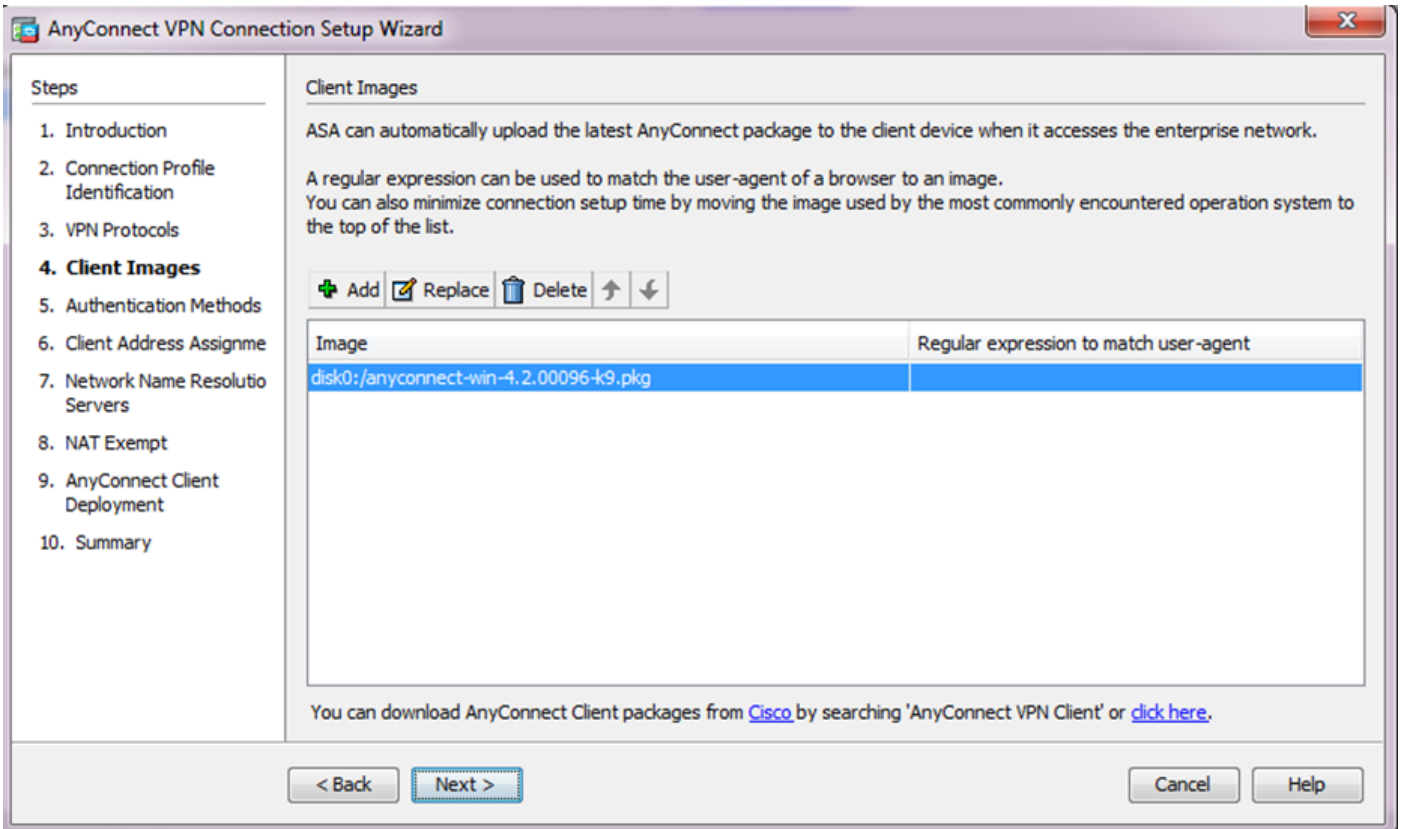
플래시 드라이브에서 이미지를 추가하려면 Browse Flash(플래시 찾아보기)를 클릭하고, 호스트 시스템의 로컬 드라이브에서 이미지를 추가하려면 Upload(업로드)를 클릭합니다.



- ASA Flash/Disk(패키지가 이미 있는 경우) 또는 로컬 드라이브에서 AnyConnect.pkg 파일을 업로드할 수 있습니다.
- Browse flash(플래시 찾아보기) - ASA Flash/Disk에서 AnyConnect 패키지를 선택합니다.
- Upload(업로드) - 호스트 컴퓨터의 로컬 드라이브에서 AnyConnect 패키지를 선택합니다.
- OK(확인)를 클릭합니다.

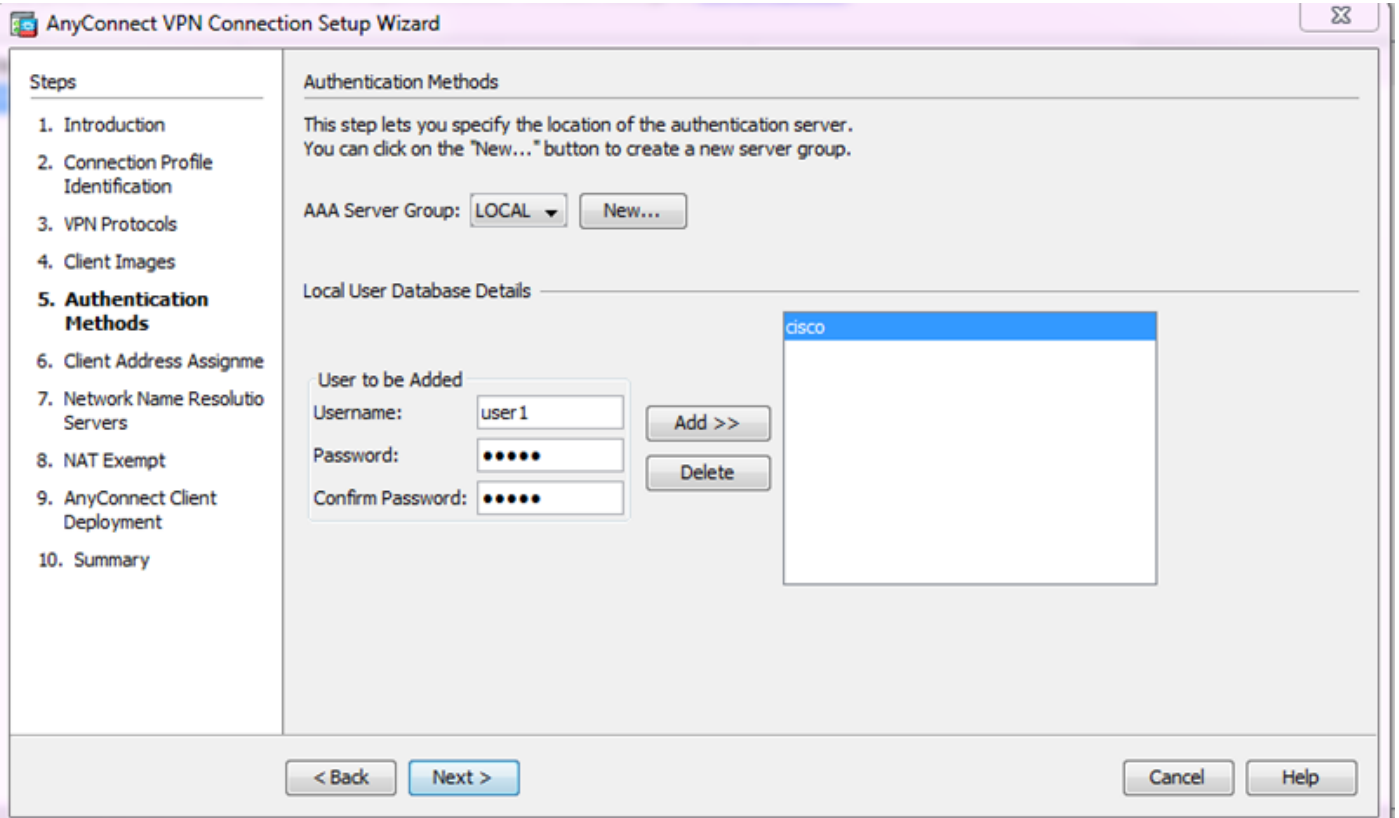


- Next(다음)를 클릭합니다.

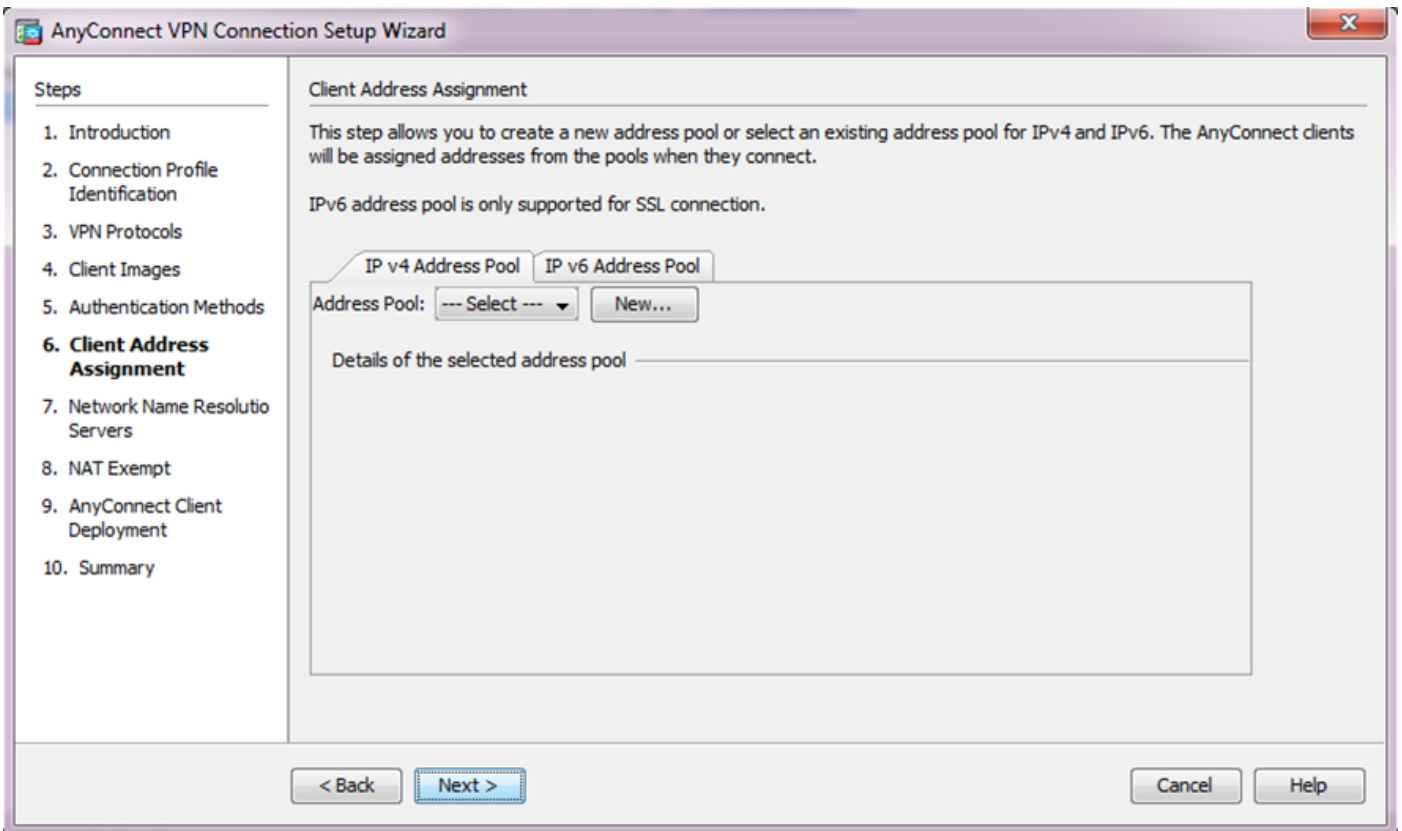


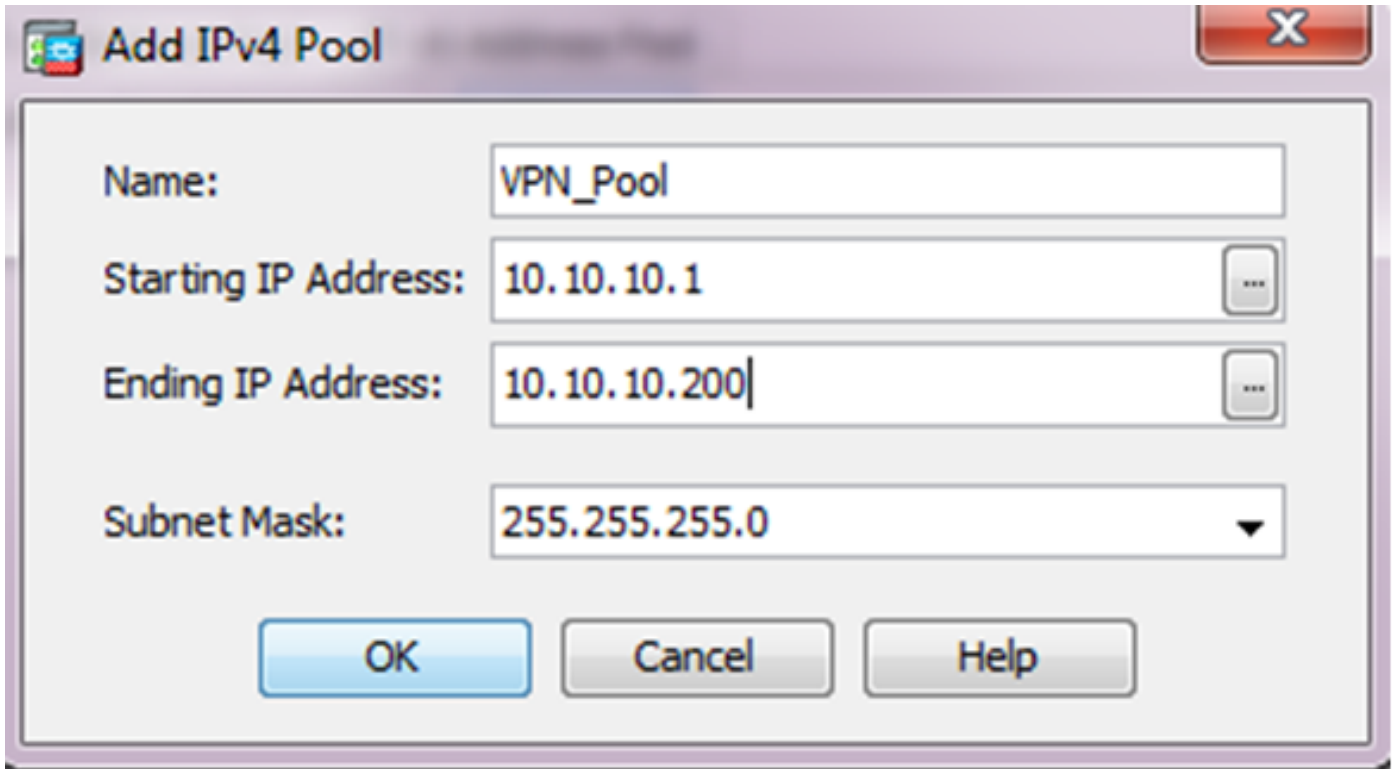
5. 사용자 인증은 AAA(Authentication, Authorization, and Accounting) 서버 그룹을 통해 완료할 수 있습니다. 사용자가 이미 구성된 경우 LOCAL(로컬)을 선택하고 Next(다음)를 클릭합니다. 또는 로컬 사용자 데이터베이스에 사용자를 추가하고 다음을 누릅니다.

참고: 이 예에서는 LOCAL 인증이 구성되므로 ASA의 로컬 사용자 데이터베이스가 인증에 사용됩니다.

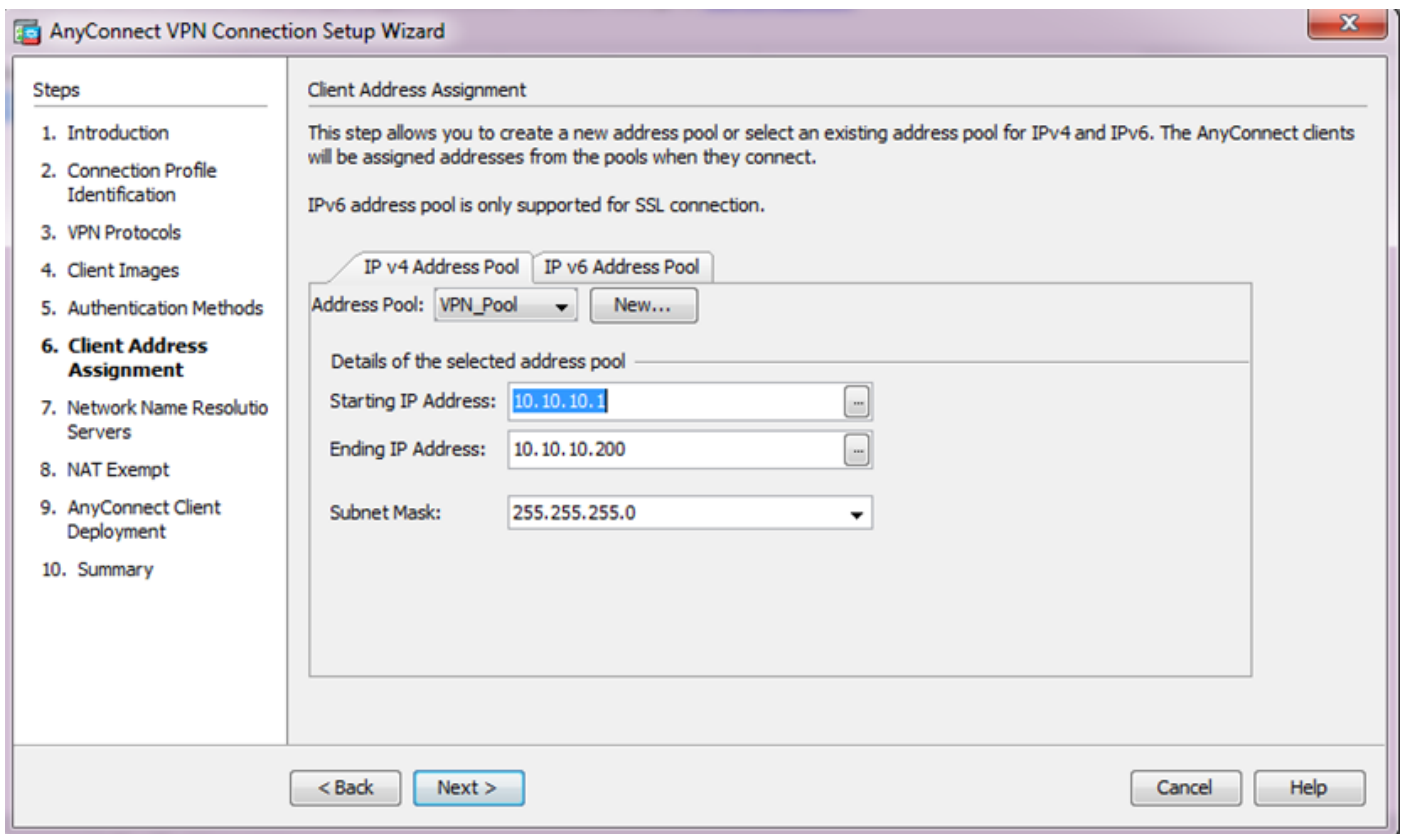


6. VPN 클라이언트의 주소 풀이 구성되었는지 확인합니다. IP 풀이 이미 구성된 경우 드롭다운 메뉴에서 선택합니다. 그렇지 않은 경우 New(새로 만들기)를 클릭하여 구성합니다. 완료되면 Next(다음)를 클릭합니다.

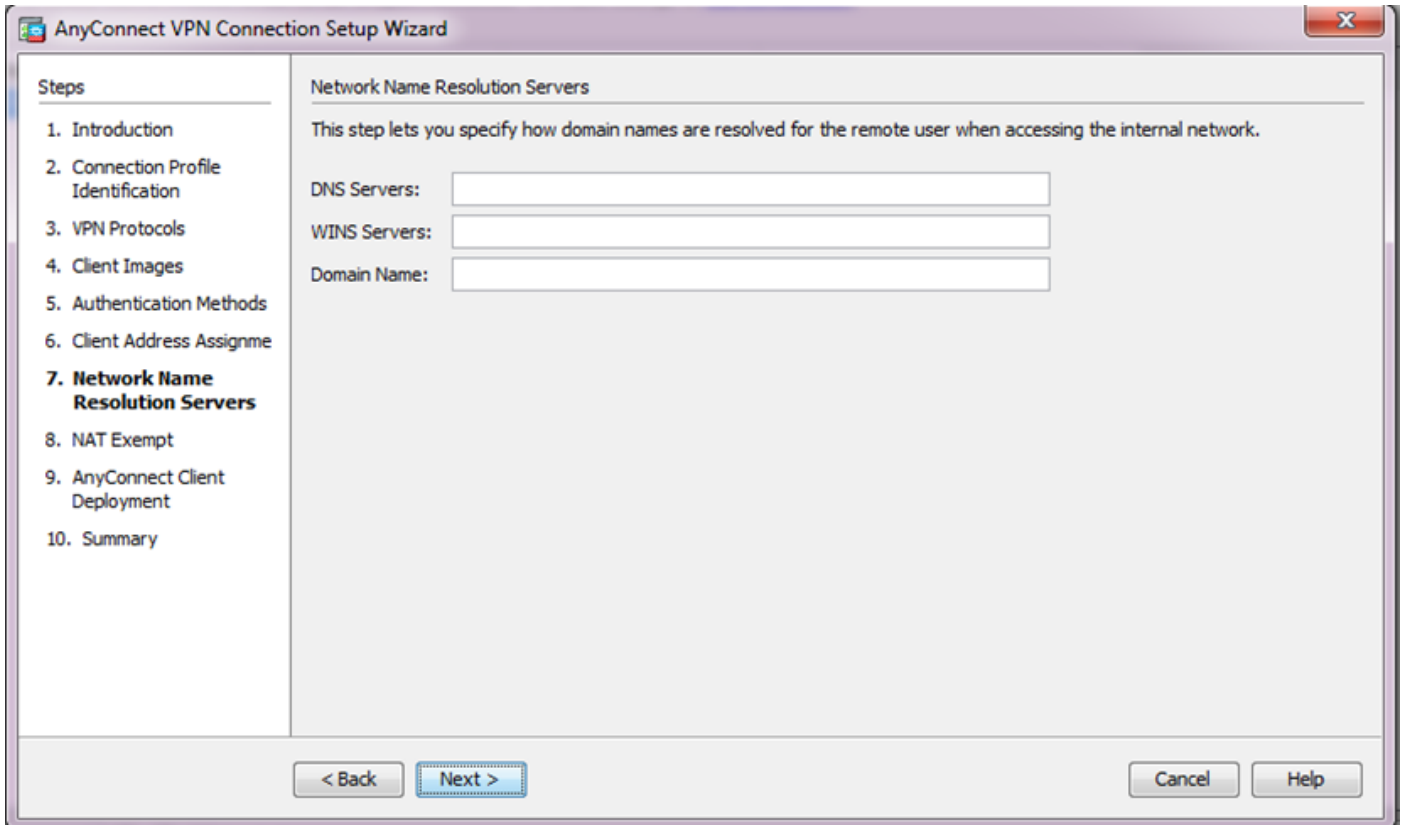




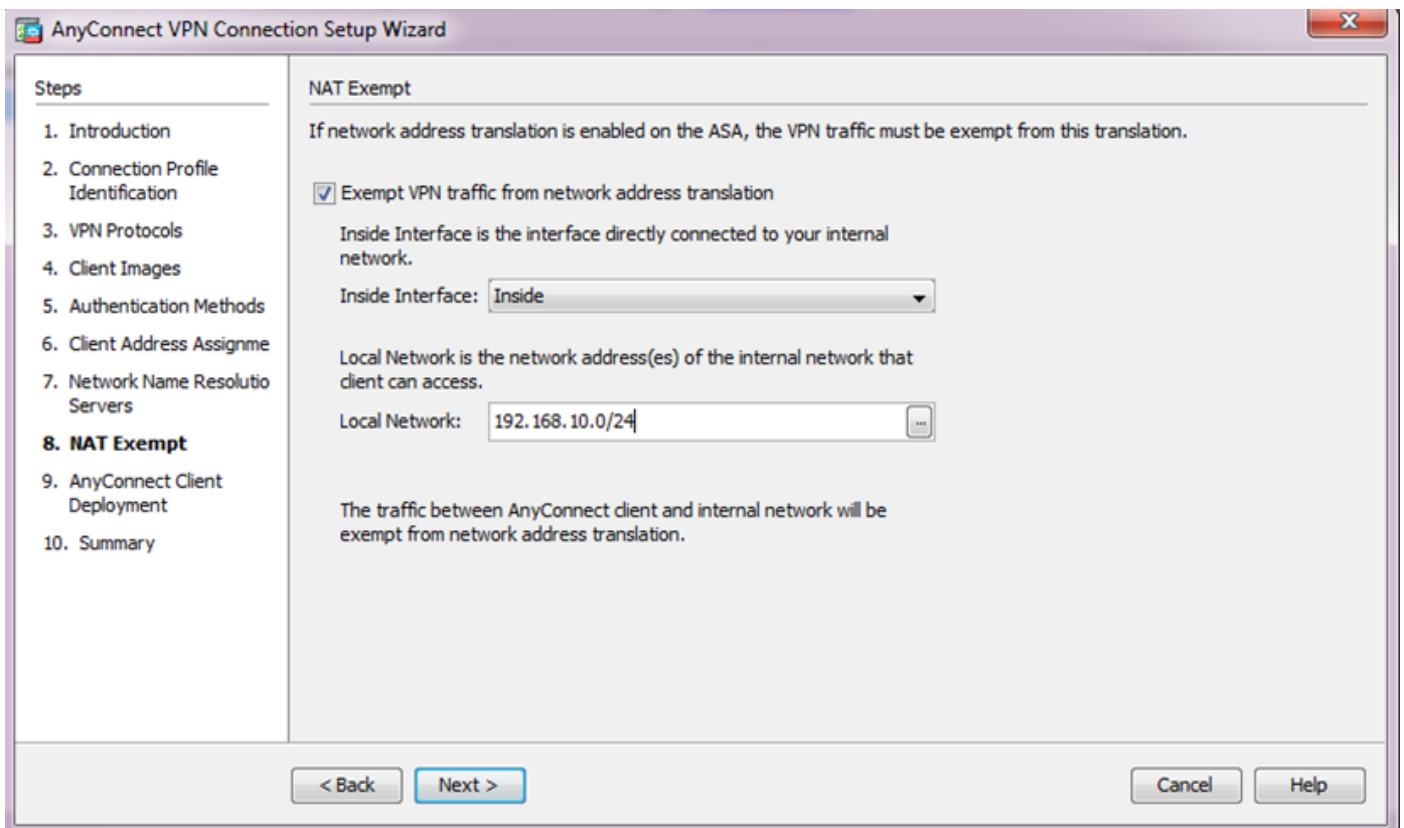
- Next(다음)를 클릭합니다.



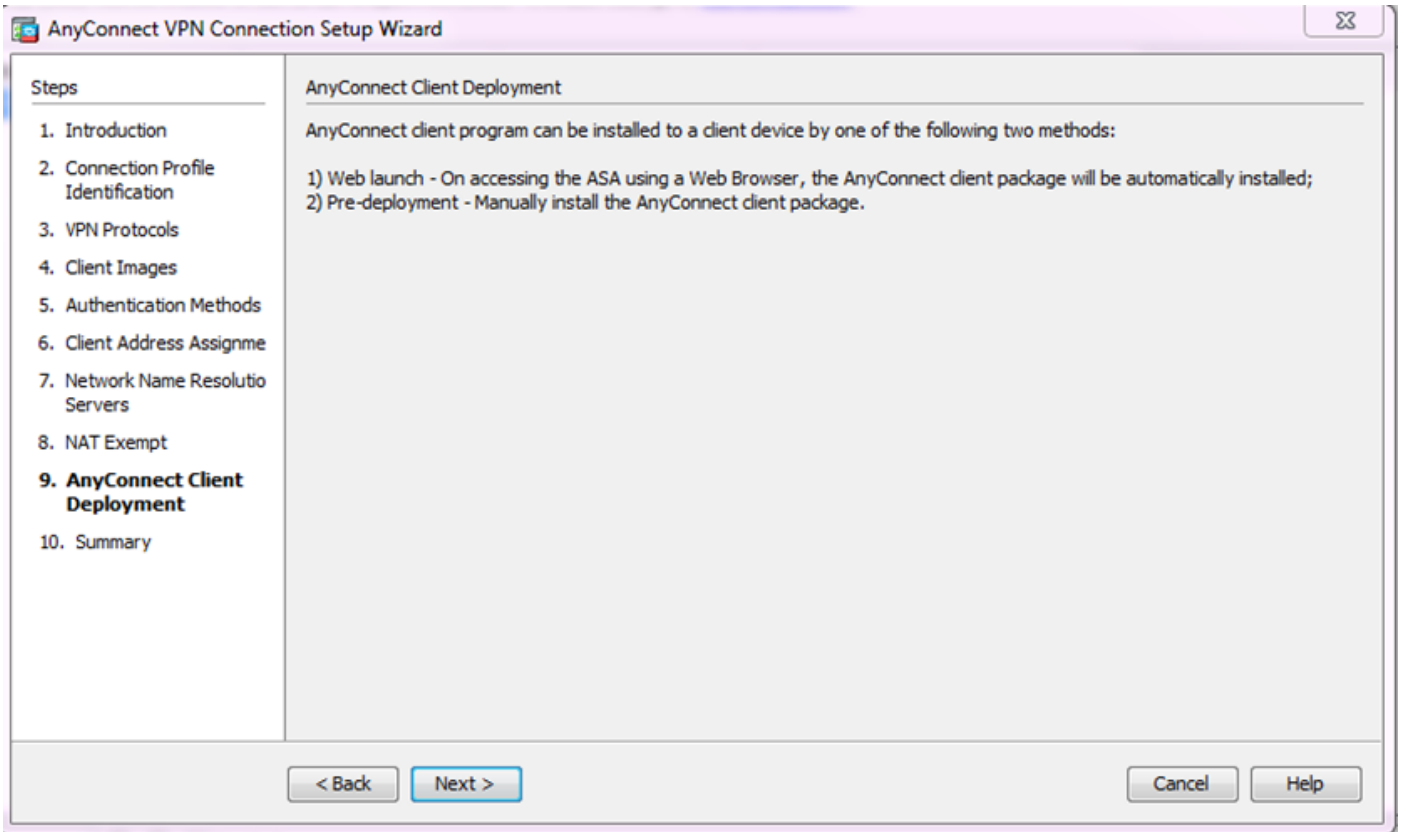
7. 선택적으로, DNS(Domain Name System) 서버 및 DN을 DNS 및 Domain Name 필드에 구성하고 Next(다음)를 클릭합니다.



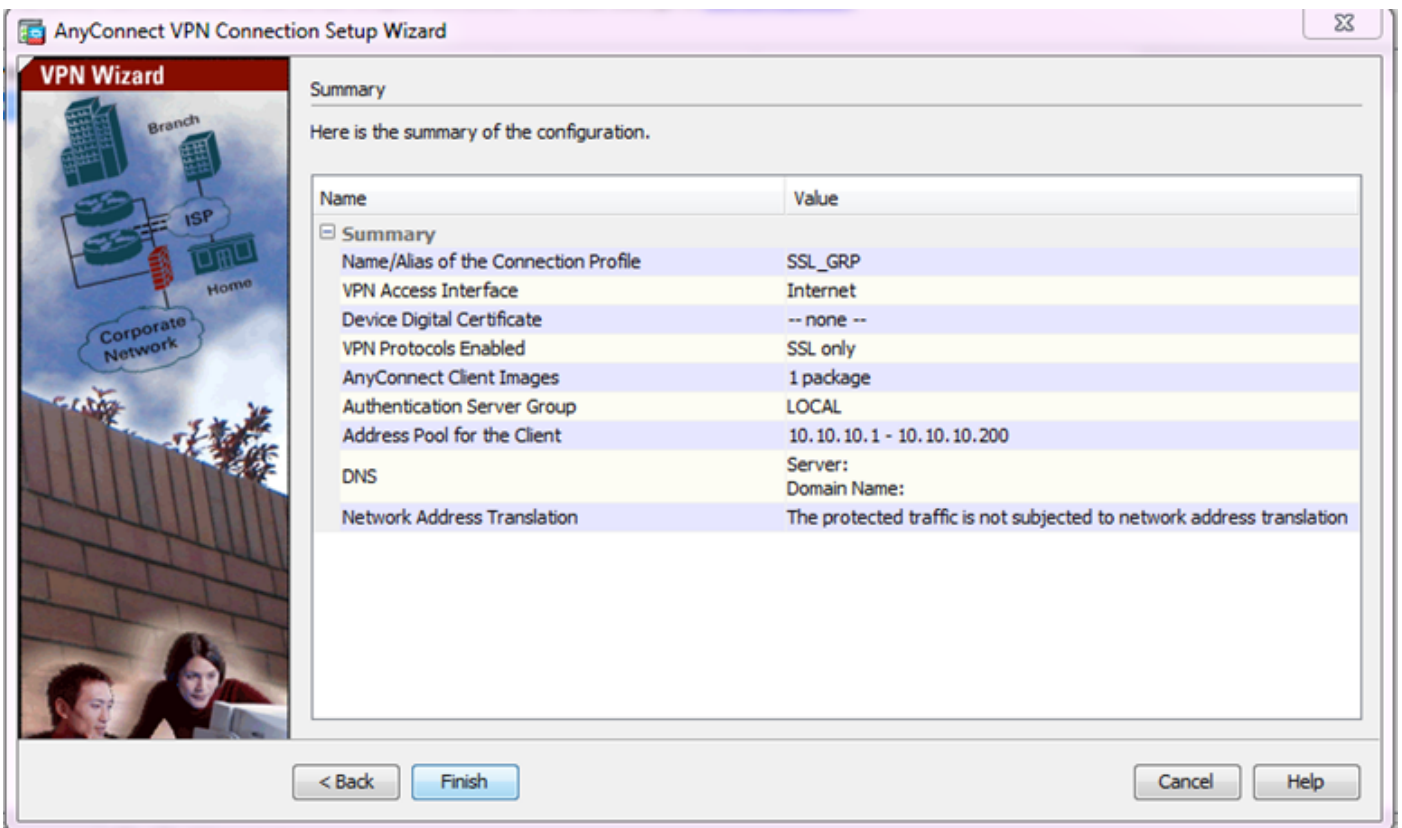
8. 클라이언트와 내부 서브넷 간의 트래픽은 동적 NAT(Network Address Translation)에서 제외되어야 합니다. Exempt VPN traffic from network address translation(네트워크 주소 변환에서 VPN 트래픽 제외) 확인란을 활성화하고 제외에 사용할 LAN 인터페이스를 구성합니다. 또한 면제되어야 하는 로컬 네트워크를 지정하고 Next(다음)를 클릭합니다.



9. 다음을 클릭합니다.

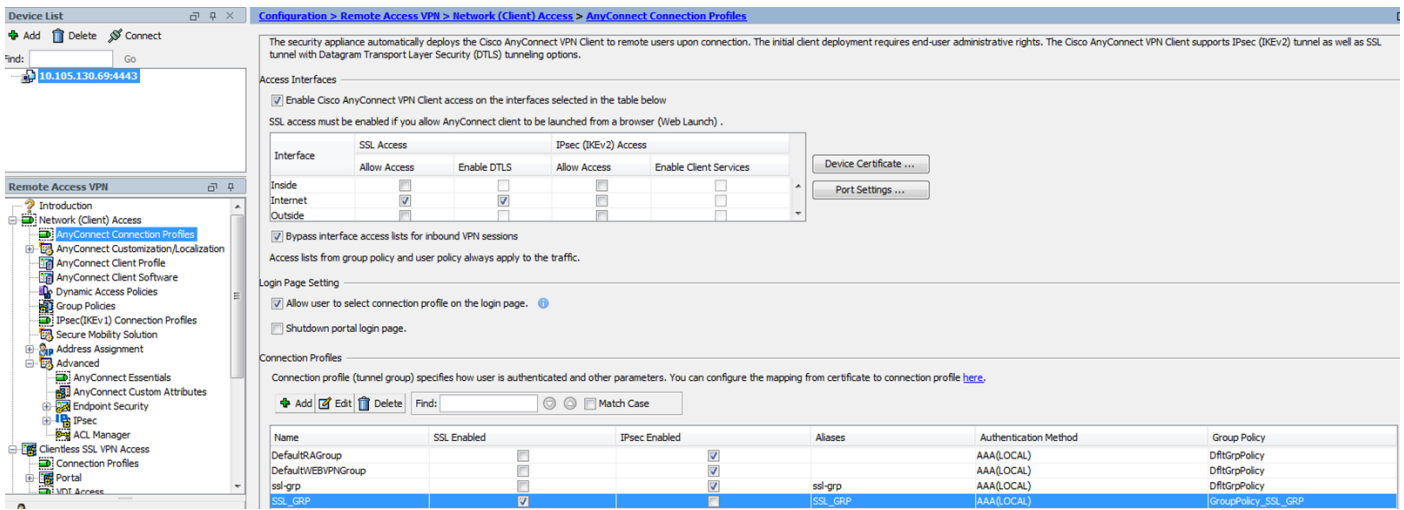


10. 마지막 단계에서는 요약을 표시하고 완료를 눌러 설정을 완료합니다.

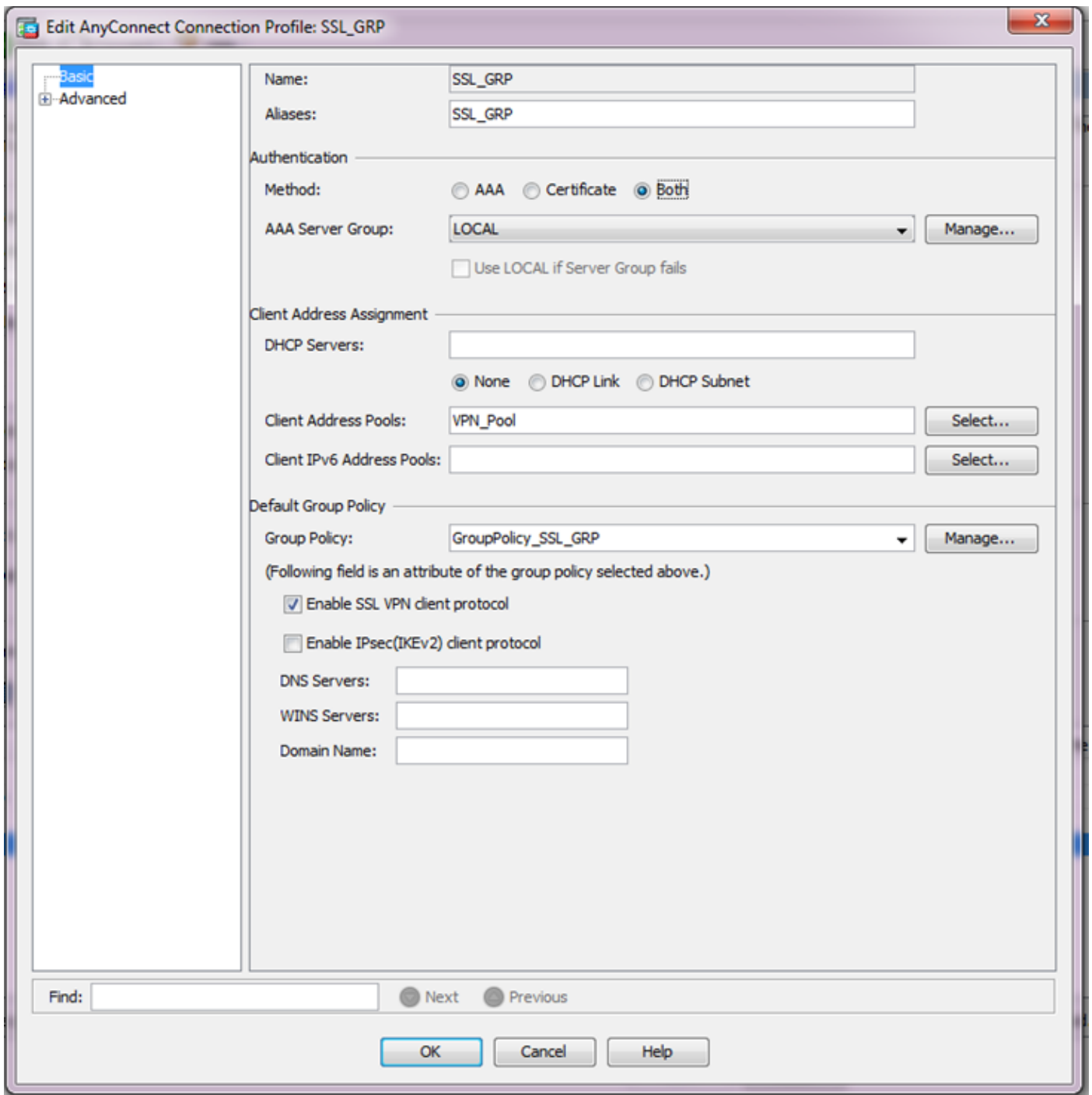


이제 AnyConnect 클라이언트 컨피그레이션이 완료되었습니다. 그러나 컨피그레이션 마법사를 통해 AnyConnect를 구성할 때 기본적으로 인증 방법을 AAA로 구성합니다. 인증서 및 사용자 이름/비밀번호를 통해 클라이언트를 인증하려면 인증 방법으로 인증서 및 AAA를 사용하도록 터널 그룹(연결 프로파일)을 구성해야 합니다.

- Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > AnyConnect Connection Profiles(AnyConnect 연결 프로파일)로 이동합니다.
- 새로 추가된 연결 프로파일 SSL_GRP가 나열되어 있어야 합니다.



- AAA 및 Certificate Authentication(인증서 인증)을 구성하려면 Connection Profile(연결 프로파일) SSL_GRP를 선택하고 Edit(편집)를 클릭합니다.
- Authentication Method(인증 방법)에서 Both(둘 다)를 선택합니다.



AnyConnect용 CLI 구성

<#root>

!! *****Configure the VPN Pool*****

```
ip local pool VPN_Pool 10.10.10.1-10.10.10.200 mask 255.255.255.0
```

!! *****Configure Address Objects for VPN Pool and Local Network*****

```
object network NETWORK_OBJ_10.10.10.0_24  
 subnet 10.10.10.0 255.255.255.0
```

```
object network NETWORK_OBJ_192.168.10.0_24
 subnet 192.168.10.0 255.255.255.0
 exit
```

```
!! *****Configure WebVPN*****
```

```
webvpn
 enable Internet
 anyconnect image disk0:/anyconnect-win-4.2.00096-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
 exit
```

```
!! *****Configure User*****
```

```
username user1 password mb02jYs13AXlIAGa encrypted privilege 2
```

```
!! *****Configure Group-Policy*****
```

```
group-policy GroupPolicy_SSL_GRP internal
group-policy GroupPolicy_SSL_GRP attributes
 vpn-tunnel-protocol ssl-client
 dns-server none
 wins-server none
 default-domain none
 exit
```

```
!! *****Configure Tunnel-Group*****
```

```
tunnel-group SSL_GRP type remote-access
tunnel-group SSL_GRP general-attributes
 authentication-server-group LOCAL
 default-group-policy GroupPolicy_SSL_GRP
 address-pool VPN_Pool
tunnel-group SSL_GRP webvpn-attributes
 authentication aaa certificate
 group-alias SSL_GRP enable
 exit
```

```
!! *****Configure NAT-Exempt Policy*****
```

```
nat (Inside,Internet) 1 source static NETWORK_OBJ_192.168.10.0_24 NETWORK_OBJ_192.168.10.0_24 destination
```

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

참고: Output [Interpreter Tool](#)([등록된](#) 고객만 해당)은 특정 show 명령을 지원합니다. show 명령 출력의 분석을 보려면 아웃풋 인터프리터 툴을 사용합니다.

CA 서버가 활성화되었는지 확인합니다.

crypto ca server 표시

<#root>

```
ASA(config)# show crypto ca server
Certificate Server LOCAL-CA-SERVER:
```

```
  Status: enabled
```

```
  State: enabled
  Server's configuration is locked (enter "shutdown" to unlock it)
```

```
Issuer name: CN=ASA.local
```

```
CA certificate fingerprint/thumbprint: (MD5)
  32e868b9 351a1b07 4b59cce5 704d6615
CA certificate fingerprint/thumbprint: (SHA1)
  6136511b 14aa1bbe 334c2659 ae7015a9 170a7c4d
Last certificate issued serial number: 0x1
CA certificate expiration timer: 19:25:42 UTC Jan 8 2019
CRL NextUpdate timer: 01:25:42 UTC Jan 10 2016
Current primary storage dir: flash:/LOCAL-CA-SERVER/
```

```
Auto-Rollover configured, overlap period 30 days
Autorollover timer: 19:25:42 UTC Dec 9 2018
```

```
WARNING: Configuration has been modified and needs to be saved!!
```

다음을 추가한 후 사용자가 등록 가능한지 확인합니다.

<#root>

```
*****Before Enrollment*****
```

```
ASA#
```

```
show crypto ca server user-db
```

```
username: user1
email:    user1@cisco.com
dn:      CN=user1,OU=TAC
allowed: 19:03:11 UTC Thu Jan 14 2016
notified: 1 times
enrollment status: Allowed to Enroll
```

```
>>> Shows the status "Allowed to Enroll"
```

*****After Enrollment*****

username: user1
email: user1@cisco.com
dn: CN=user1,OU=TAC
allowed: 19:05:14 UTC Thu Jan 14 2016
notified: 1 times

enrollment status: Enrolled

, Certificate valid until 19:18:30 UTC Tue Jan 10 2017,
Renewal: Allowed

CLI 또는 ASDM을 통해 anyconnect 연결의 세부사항을 확인할 수 있습니다.

CLI를 통해

show vpn-sessiondb detail anyconnect

<#root>

ASA# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : user1 Index : 1
Assigned IP : 10.10.10.1 Public IP : 10.142.189.181
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Essentials
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 13822 Bytes Rx : 13299
Pkts Tx : 10 Pkts Rx : 137
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_SSL_GRP Tunnel Group : SSL_GRP
Login Time : 19:19:10 UTC Mon Jan 11 2016
Duration : 0h:00m:47s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 1.1
Public IP : 10.142.189.181
Encryption : none Hashing : none
TCP Src Port : 52442 TCP Dst Port : 443
Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.2.00096
Bytes Tx : 6911 Bytes Rx : 768
Pkts Tx : 5 Pkts Rx : 1

Pkts Tx Drop : 0

Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 1.2
Assigned IP : 10.10.10.1 Public IP : 10.142.189.181
Encryption : RC4 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 52443
TCP Dst Port : 443 Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.2.00096
Bytes Tx : 6911 Bytes Rx : 152
Pkts Tx : 5 Pkts Rx : 2
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:

Tunnel ID : 1.3
Assigned IP : 10.10.10.1 Public IP : 10.142.189.181
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 UDP Src Port : 59167
UDP Dst Port : 443 Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.2.00096
Bytes Tx : 0 Bytes Rx : 12907
Pkts Tx : 0 Pkts Rx : 142
Pkts Tx Drop : 0 Pkts Rx Drop : 0

NAC:

Reval Int (T): 0 Seconds Reval Left(T): 0 Seconds
SQ Int (T) : 0 Seconds EoU Age(T) : 51 Seconds
Hold Left (T): 0 Seconds Posture Token:
Redirect URL :

ASDM을 통해

- Monitoring(모니터링) > VPN > VPN Statistics(VPN 통계) > Sessions(세션)로 이동합니다.
- Filter By(필터링 기준)를 All Remote Access(모든 원격 액세스)로 선택합니다.
- 선택한 AnyConnect 클라이언트에 대한 작업 중 하나를 수행할 수 있습니다.

Details(세부 정보) - 세션에 대한 추가 정보 제공

Logout(로그아웃) - Headend에서 사용자를 수동으로 로그아웃합니다.

Ping - 헤드엔드에서 AnyConnect 클라이언트에 ping합니다.

Username	Group Policy Connection Profile	Public IP Address Assigned IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx
user1	ssl-pol ssl-grp	10.142.189.80 192.168.1.1	AnyConnect-Parent-SSL-Tunnel-DTLS-... AnyConnect-Parent: (1)none-SSL-Tu...	14:39:08 UTC Mo... 0h:00m:33s	10998 885

문제 해결

이 섹션에서는 설정 문제 해결을 위해 사용할 수 있는 정보를 제공합니다.

참고: debug 명령을 사용하기 [전에 Debug 명령](#)에 대한 중요 정보를 참조하십시오.

주의: ASA에서는 다양한 디버그 레벨을 설정할 수 있습니다. 기본적으로 레벨 1이 사용됩니다. 디버그 수준을 변경하면 디버그의 세부 정도가 증가할 수 있습니다. 특히 프로덕션 환경에서는 이 작업을 신중하게 수행해야 합니다.

- debug crypto ca
- crypto ca server 디버그
- crypto ca 메시지 디버그
- crypto ca 트랜잭션 디버그
- webvpn anyconnect 디버그

이 디버그 출력은 no shut 명령을 사용하여 CA 서버가 Enabled일 때 표시됩니다.

<#root>

```
ASA# debug crypto ca 255
ASA# debug crypto ca server 255
ASA# debug crypto ca message 255
ASA# debug crypto ca transaction 255
```

```
CRYPTO_CS: input signal enqueued: no shut >>>> Command issued to Enable the CA server
Crypto CS thread wakes up!
```

```
CRYPTO_CS: enter FSM: input state disabled, input signal no shut
CRYPTO_CS: starting enabling checks
CRYPTO_CS: found existing serial file.
CRYPTO_CS: started CA cert timer, expiration time is 17:53:33 UTC Jan 13 2019
CRYPTO_CS: Using existing trustpoint 'LOCAL-CA-SERVER' and CA certificate
CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser
CRYPTO_CS: DB version 1
CRYPTO_CS: last issued serial number is 0x4
CRYPTO_CS: closed ser file
CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.crl
CRYPTO_CS: CRL file LOCAL-CA-SERVER.crl exists.
CRYPTO_CS: Read 220 bytes from crl file.
CRYPTO_CS: closed crl file
CRYPTO_PKI: Storage context locked by thread Crypto CA Server
```

```
CRYPTO_PKI: inserting CRL
CRYPTO_PKI: set CRL update timer with delay: 20250
CRYPTO_PKI: the current device time: 18:05:17 UTC Jan 16 2016
```

```
CRYPTO_PKI: the last CRL update time: 17:42:47 UTC Jan 16 2016
CRYPTO_PKI: the next CRL update time: 23:42:47 UTC Jan 16 2016
CRYPTO_PKI: CRL cache delay being set to: 20250000
CRYPTO_PKI: Storage context released by thread Crypto CA Server
```

```
CRYPTO_CS: Inserted Local CA CRL into cache!
CRYPTO_CS: shadow not configured; look for shadow cert
CRYPTO_CS: failed to find shadow cert in the db
CRYPTO_CS: set shadow generation timer
CRYPTO_CS: shadow generation timer has been set
CRYPTO_CS: Enabled CS.
CRYPTO_CS: exit FSM: new state enabled
CRYPTO_CS: cs config has been locked.

Crypto CS thread sleeps!
```

이 디버그 출력은 클라이언트의 등록을 표시합니다

<#root>

```
ASA# debug crypto ca 255
ASA# debug crypto ca server 255
ASA# debug crypto ca message 255
ASA# debug crypto ca transaction 255
```

```
CRYPTO_CS: writing serial number 0x2.
CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser
CRYPTO_CS: Writing 32 bytes to ser file
CRYPTO_CS: Generated and saving a PKCS12 file for user user1
at flash:/LOCAL-CA-SERVER/user1.p12
```

다음 조건에서는 클라이언트 등록이 실패할 수 있습니다.

시나리오 1.

- 사용자는 등록 권한 없이 CA 서버 데이터베이스에 생성됩니다.

The screenshot shows a dialog box titled "Add User" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Username:** user 1
- Email ID:** user1@cisco.com
- Subject (DN String):** CN=user1,OU=TAC
- Select...** button (to the right of the Subject field)
- Allow enrollment** (checkbox is unchecked)
- Add User** button (highlighted in blue)
- Cancel** button
- Help** button

CLI에 준하는 기능:

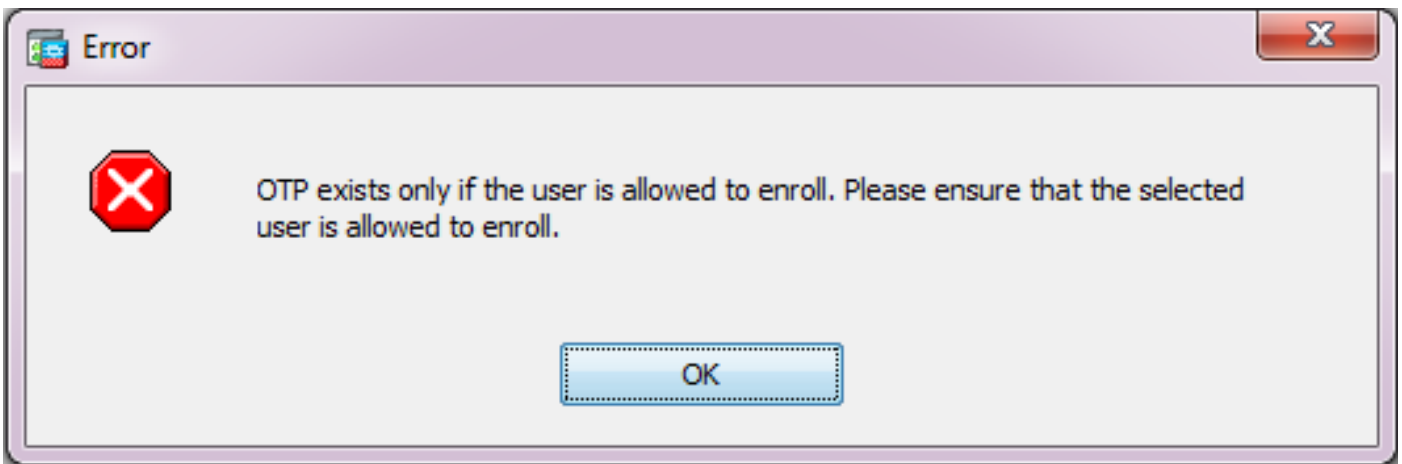
<#root>

```
ASA(config)# show crypto ca server user-db
```

```
username: user1
email:      user1@cisco.com
dn:         CN=user1,OU=TAC
allowed:    <not allowed>
notified:   0 times
```

```
enrollment status: Not Allowed to Enroll
```

- 사용자가 등록할 수 없는 경우, 사용자를 위해 OTP를 생성/이메일로 보내려고 하면 이 오류 메시지가 생성됩니다.



시나리오 2.

- show run webvpn 명령을 사용하여 등록 포털을 사용할 수 있는 포트 및 인터페이스를 확인합니다. 기본 포트는 443이지만 수정할 수 있습니다.
- 클라이언트가 등록 포털에 성공적으로 액세스하는 데 사용된 포트에서 webvpn이 활성화된 인터페이스의 IP 주소에 네트워크 연결이 가능해야 합니다.

다음과 같은 경우 클라이언트가 ASA의 등록 포털에 액세스하지 못할 수 있습니다.

1. 중간 디바이스가 클라이언트에서 ASA의 webvpn IP로 들어오는 연결을 지정된 포트에서 차단하는 경우
 2. webvpn이 활성화된 인터페이스의 상태가 다운되었습니다.
- 이 출력은 사용자 지정 포트 4433에서 등록 포털을 인터페이스 인터넷의 IP 주소에서 사용할 수 있음을 보여줍니다.

<#root>

```
ASA(config)# show run webvpn
```

```
webvpn
```

port 4433

enable Internet

```
no anyconnect-essentials
anyconnect image disk0:/anyconnect-win-4.2.00096-k9.pkg 1
anyconnect enable
tunnel-group-list enable
```

시나리오 3.

- CA 서버 데이터베이스 스토리지의 기본 위치는 ASA의 플래시 메모리입니다.
- 플래시 메모리에 등록 중에 사용자에게 대한 pkcs12 파일을 생성하고 저장할 여유 공간이 있는지 확인합니다.
- 플래시 메모리에 충분한 여유 공간이 없는 경우 ASA가 클라이언트의 등록 프로세스를 완료하지 못하고 다음 디버그 로그를 생성합니다.

<#root>

```
ASA(config)# debug crypto ca 255
ASA(config)# debug crypto ca server 255
ASA(config)# debug crypto ca message 255
ASA(config)# debug crypto ca transaction 255
ASA(config)# debug crypto ca trustpool 255
```

```
CRYPTO_CS: writing serial number 0x2.
CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser
CRYPTO_CS: Writing 32 bytes to ser file
CRYPTO_CS: Generated and saving a PKCS12 file for user user1
at flash:/LOCAL-CA-SERVER/user1.p12
```

```
CRYPTO_CS: Failed to write to opened PKCS12 file for user user1, fd: 0, status: -1.
```

```
CRYPTO_CS: Failed to generate pkcs12 file for user user1 status: -1.
```

```
CRYPTO_CS: Failed to process enrollment in-line for user user1. status: -1
```

관련 정보

- [Cisco ASA 5500 Series Adaptive Security Appliance](#)
- [AnyConnect VPN 클라이언트 문제 해결 가이드 - 일반 문제](#)
- [AnyConnect 세션 관리, 모니터링 및 문제 해결](#)
- [기술 지원 및 문서 - Cisco Systems](#)

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.