

Microsoft CA 컨피그레이션과 함께 디지털 인증서를 사용하는 ASA/PIX 8.x 및 VPN 클라이언트 IPSec 인증 예

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[관련 제품](#)

[표기 규칙](#)

[구성](#)

[네트워크 다이어그램](#)

[구성](#)

[ASA 컨피그레이션](#)

[ASA 구성 요약](#)

[VPN 클라이언트 컨피그레이션](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

[소개](#)

이 문서에서는 Microsoft CA(Certificate Authority) 서버를 사용하여 IPSec 피어를 인증하기 위해 Cisco Security Appliance(ASA/PIX) 8.x 및 VPN 클라이언트에 서드파티 벤더 디지털 인증서를 수동으로 설치하는 방법에 대해 설명합니다.

[사전 요구 사항](#)

[요구 사항](#)

이 문서를 사용하려면 인증서 등록을 위해 인증 기관에 액세스할 수 있어야 합니다. 지원되는 타사 CA 공급업체는 Baltimore, Cisco, Entrust, iPlanet/Netscape, Microsoft, RSA, VeriSign입니다.

이 문서에서는 ASA/PIX에 기존 VPN 컨피그레이션이 없다고 가정합니다.

참고: 이 문서에서는 시나리오의 CA 서버로 Microsoft Windows 2003 서버를 사용합니다.

참고: Windows 2003 서버를 CA로 구성하는 방법에 대한 자세한 내용은 [Windows 서버](#) 에서 CA 구성을 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 8.0(2) 및 ASDM 버전 6.0(2)을 실행하는 ASA 5510
- 소프트웨어 버전 4.x 이상을 실행하는 VPN 클라이언트

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.

관련 제품

ASA 컨피그레이션은 소프트웨어 버전 8.x를 실행하는 Cisco 500 Series PIX와 함께 사용할 수도 있습니다.

표기 규칙

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

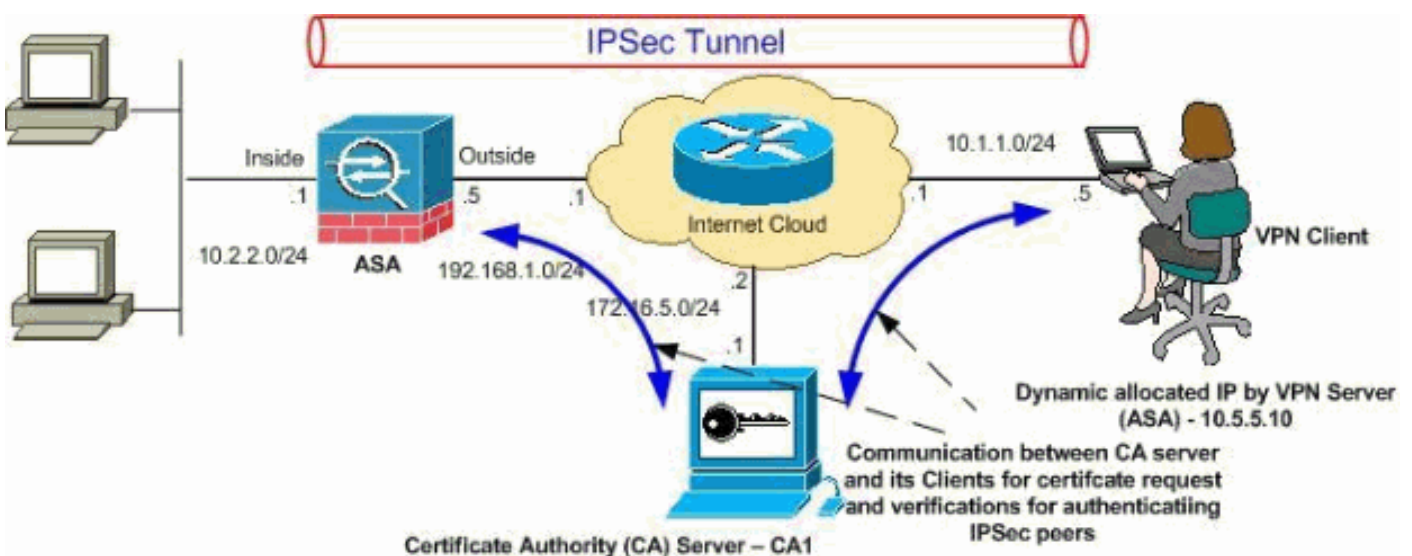
구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

참고: 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 [명령 조회 도구](#)([등록된 고객만 해당](#))를 사용하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다. 실습 환경에서 사용된 RFC 1918 주소입니다.

구성

이 문서에서는 다음 구성을 사용합니다.

- [ASA 컨피그레이션](#)
- [ASA 구성 요약](#)
- [VPN 클라이언트 컨피그레이션](#)

ASA 컨피그레이션

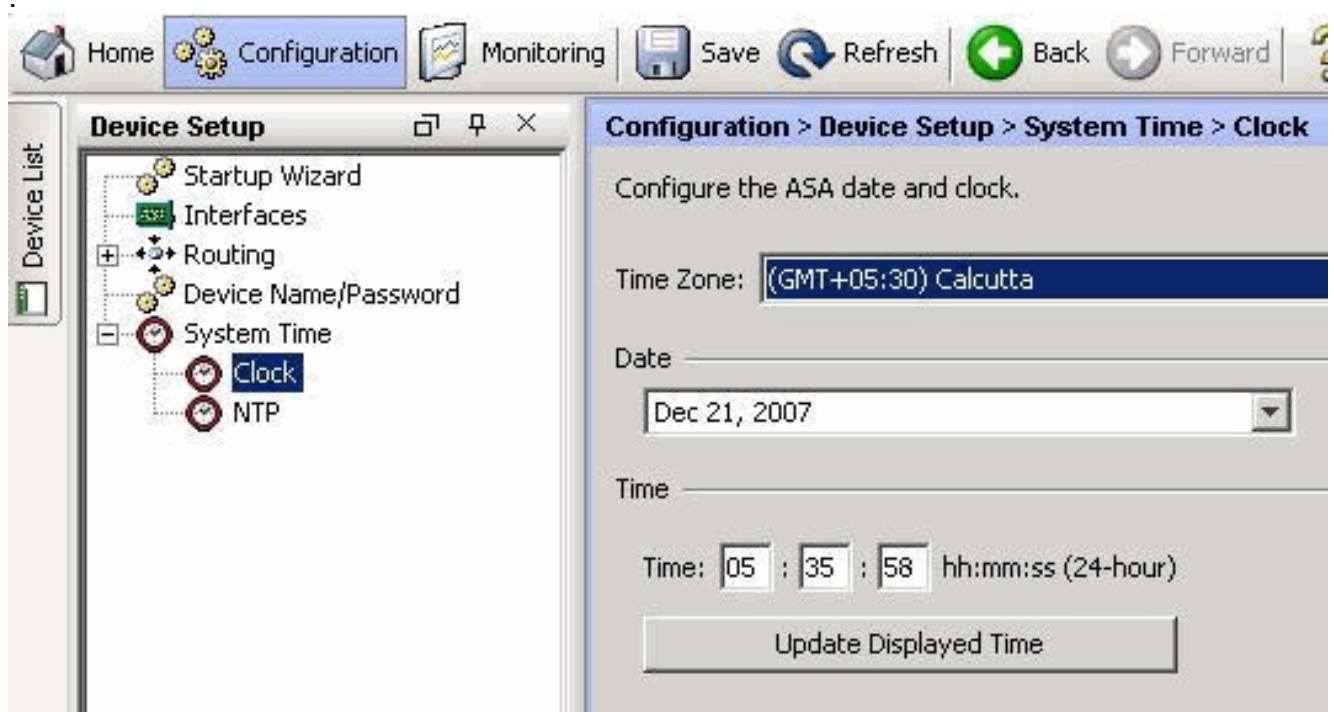
ASA에 타사 공급업체 디지털 인증서를 설치하려면 다음 단계를 완료하십시오.

- [1단계. 날짜, 시간 및 시간대 값이 정확한지 확인합니다.](#)
- [2단계. 인증서 서명 요청 생성](#)
- [3단계. 신뢰 지점 인증](#)
- [4단계. 인증서 설치](#)
- [5단계. 새로 설치된 인증서를 사용하도록 IPSec\(Remote Access VPN\)을 구성합니다.](#)

[1단계. 날짜, 시간 및 시간대 값이 정확한지 확인합니다.](#)

ASDM 절차

1. Configuration(컨피그레이션)을 클릭한 다음 Device Setup(디바이스 설정)을 클릭합니다.
2. System Time(시스템 시간)을 확장하고 Clock(시계)을 선택합니다.
3. 나열된 정보가 정확한지 확인합니다.올바른 인증서 검증이 이루어지려면 날짜, 시간 및 표준 시간대 값이 정확해야 합니다



명령줄 예

```
CiscoASA
```

```
CiscoASA#show clock  
05:37:37.904 UTC Fri Dec 21 2007
```

2단계. 인증서 서명 요청 생성

서드파티 CA가 ID 인증서를 발급하려면 CSR(Certificate Signing Request)이 필요합니다.CSR에는 ASA에서 생성한 공개 키와 함께 ASA의 DN(Distinguished Name) 문자열이 포함됩니다.ASA는 생성된 개인 키를 사용하여 CSR에 디지털 서명을 합니다.

ASDM 절차

1. Configuration(컨피그레이션)을 클릭한 다음 Device Management(디바이스 관리)를 클릭합니다.
2. Certificate Management(인증서 관리)를 확장하고 Identity Certificates(ID 인증서)를 선택합니다.
3. Add(추가)를 클릭합니다

Add Identity Certificate

Import the identity certificate from a file:

Decryption Passphrase:

File to Import From:

Add a new identity certificate:

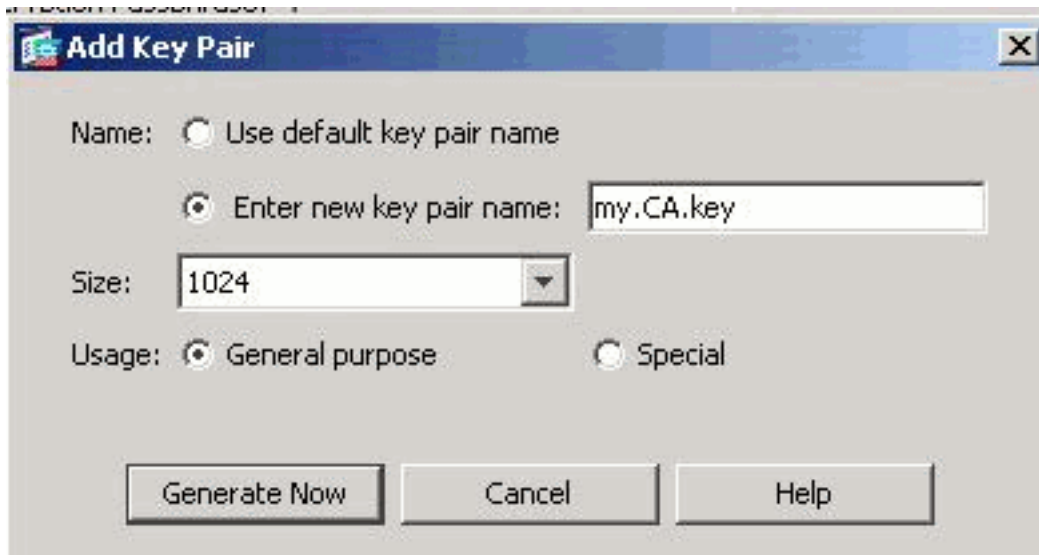
Key Pair:

Certificate Subject DN:

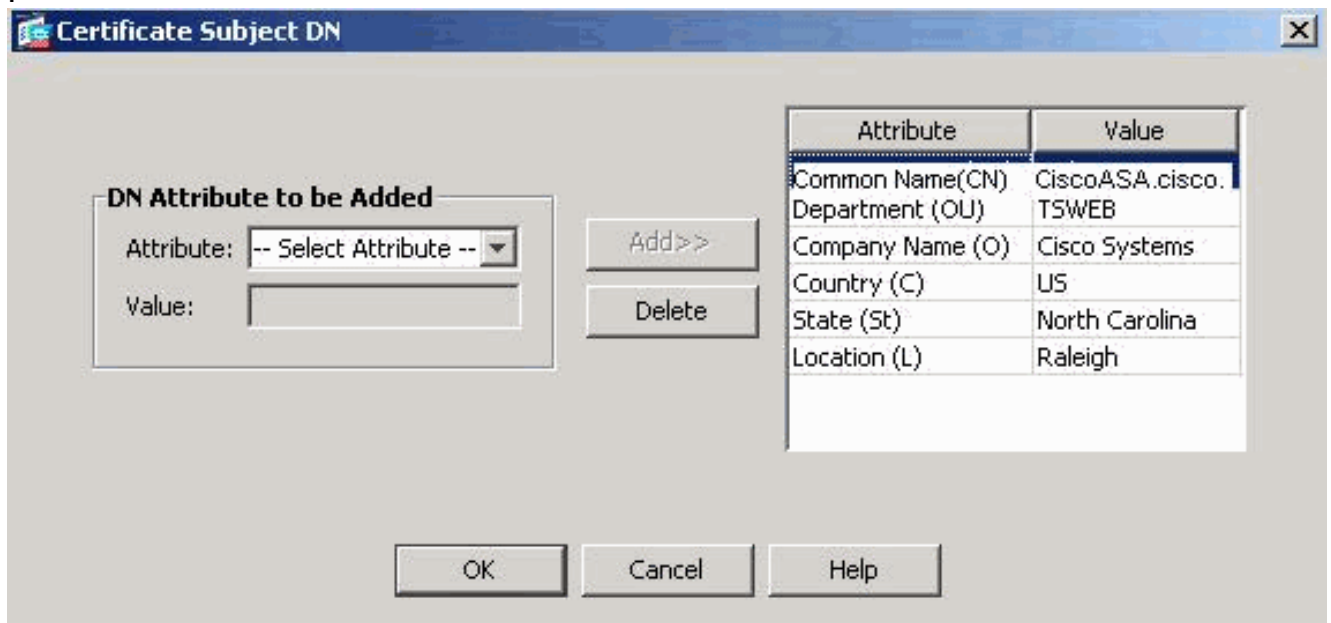
Generate self-signed certificate

Act as local certificate authority and issue dynamic certificates to TLS-Proxy

4. Add a **new identity certificate** 라디오 버튼을 클릭합니다.
5. 키 쌍의 경우 새로 만들기를 클릭합니다

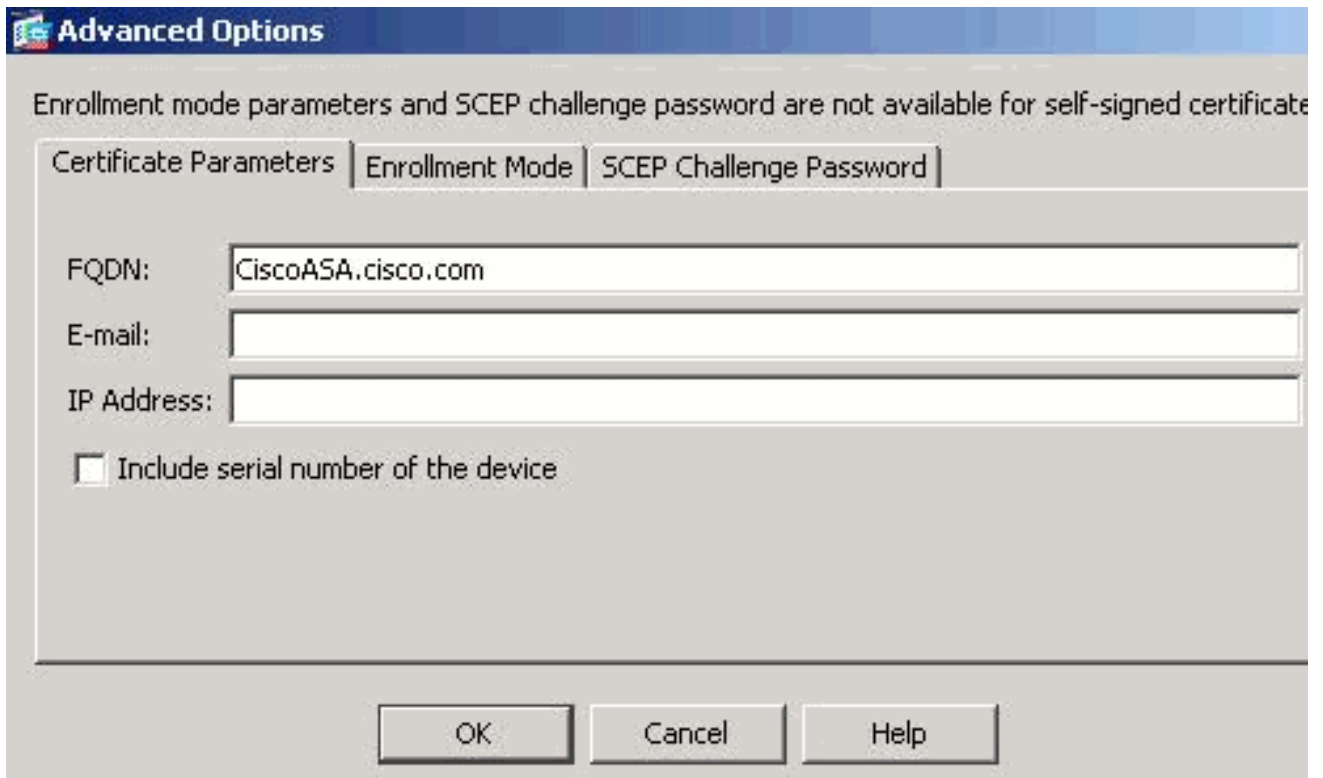


6. Enter new key pair name(새 키 쌍 이름 입력) 라디오 버튼을 클릭합니다.인식 목적으로 키 쌍 이름을 명확하게 식별해야 합니다.
7. Generate Now(지금 생성)를 클릭합니다.이제 키 쌍을 만들어야 합니다.
8. Certificate Subject DN을 정의하려면 Select(선택)를 클릭하고 이 표에 나열된 특성을 구성합니다.이러한 값을 구성하려면 속성 드롭다운 목록에서 값을 선택하고 값을 입력한 다음 추가를 클릭합니다

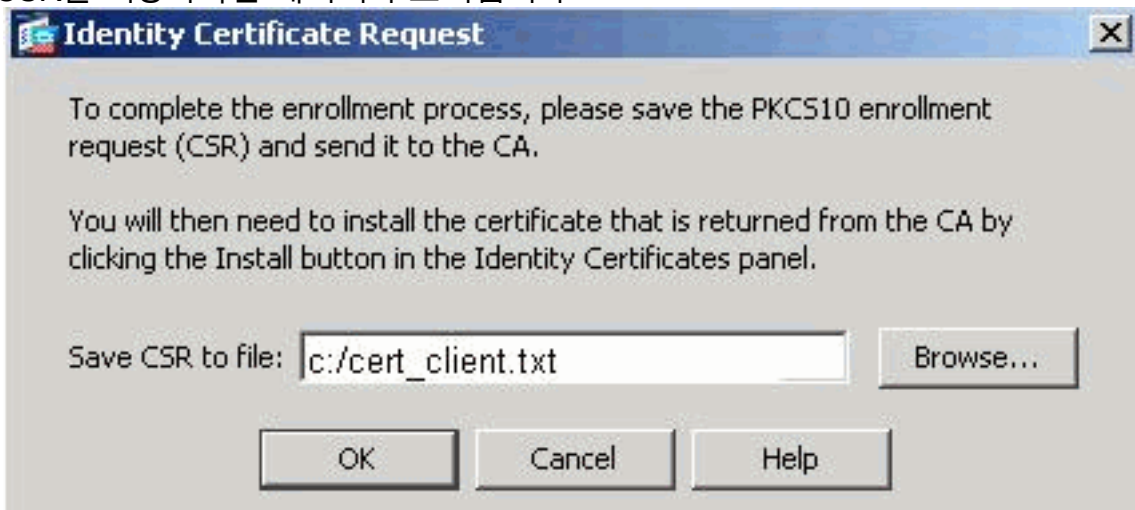


참고: 일부 타사 공급업체는 ID 인증서를 발급하기 전에 특정 특성을 포함해야 합니다.필요한 특성을 잘 모르는 경우 공급업체에 자세한 내용을 확인하십시오.

9. 적절한 값을 추가한 후 **확인**을 클릭합니다.Add Identity Certificate 대화 상자가 나타나고 Certificate Subject DN 필드가 채워집니다.
10. Advanced(고급)를 클릭합니다.
11. FQDN 필드에 인터넷에서 디바이스에 액세스하는 데 사용할 FQDN을 입력합니다.이 값은 CN(Common Name)에 사용한 FQDN과 같아야 합니다



12. OK(확인)를 클릭한 다음 Add **Certificate**(인증서 추가)를 클릭합니다.로컬 시스템의 파일에 CSR을 저장하라는 메시지가 표시됩니다



13. Browse(찾아보기)를 클릭하고 CSR을 저장할 위치를 선택하고 확장자가 .txt인 파일을 저장합니다.참고: .txt 확장자로 파일을 저장하면 텍스트 편집기(예: 메모장)로 파일을 열고 PKCS#10 요청을 볼 수 있습니다

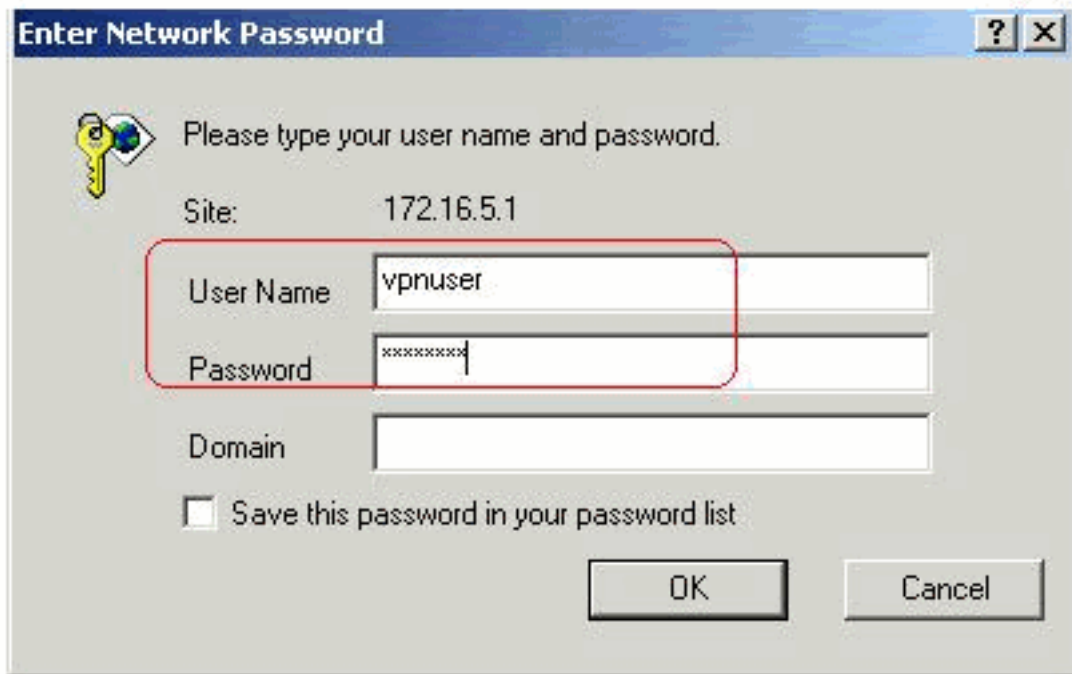
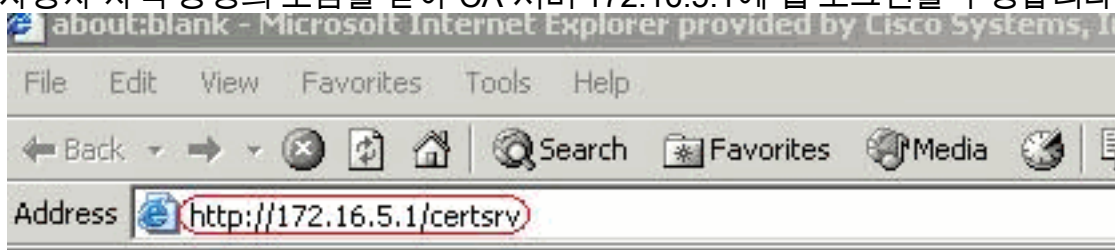
```

cert_client.txt - Notepad
File Edit Format Help
MIICKZCCAQAwga0xEDAObgNVBAcTB1JhbGVpZ2gxZAVBgNVBAgTIE
IENhcm9saw5hMQswCQYDVQQGEWJVUZEWMBQGA1UEChMNQ21zy28gU31zc
MCIGA1UEAxMhQ21zy29BU0EuY21zy28uY29tIE9VPVRTV0VCMTUwEgYD
TVgwOTM1SZA1NDafBgkqhkiG9w0BCQIWEkNpc2NvQVNBbGkqhkiG9w0BAQ
BgkqhkiG9w0BAQEFAAOBjQAwGyKCCgYEAU0IKqDMjVrdbZgBzUAjtC10j>
XgK0H2Pce1cGZ9dUXn+Y09Qjm0Krj68L6KXT1PgNAaFMwB2YsTIOh+hJE
MI6xLyKrGo7bOPAsLPeOBx1/LVLTY3ORqcy2QP3Ir1BSwoyBaoFPsRe:
QX8Jp6qcZE0CAWEAAaA9MDsGCSqGSIb3DQEJdJEUMCwwCWYDVR0PBAQD/
A1UdEQQwMBSCEkNpc2NvQVNBbGkqhkiG9w0BAQQA3tzyAD7o6R5ej9Ew7Ej4BfcXd20LCbXAOP5L1KbPaEeaCkfn/Pp5mATAs
bsxsv1jSSXQsQ1sb842D6MEG6cu7Bxj/K1Z6MxafUvCHROPYWVU1wGRJC
j89/Y458XhQ79fvBwBR8Ux9emhFHpGHnQ/MpsfU0dQ==

---End - This line not part of the certificate request---

```

- 저장된 CSR을 Microsoft CA와 같은 타사 공급업체에 제출합니다.vpnserver에 대해 제공된 사용자 자격 증명의 도움을 받아 CA 서버 172.16.5.1에 웹 로그인을 수행합니다



참고: CA 서

버와 함께 ASA(vpn 서버)에 대한 사용자 계정이 있는지 확인하십시오. Request a certificate(인증서 요청) > advanced certificate request(고급 인증서 요청)를 클릭하여 Submit a certificate request by using a base-64-encoded CMC or PKCS#10 file(base-64 인코딩 CMC 또는 PKCS#10 파일을 사용하여 인증서 요청 제출)을 선택하거나 base-64 인코딩 PKCS#7 파일을 사용하여 갱신 요청을 제출합니다

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

[Create and submit a request to this CA.](#)

[Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.](#)

[Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.](#)

Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

인코딩된 정보를 복사하여 Saved Request 상자에 붙여넣은 다음 Submit(제출)을 클릭합니다

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded C source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```

jvQVNB LmNpc2NvLmNvbTANBgkqhkiG9wOBAQQAo
4BfcXd2OLCbXAoP5L1KbPaEeaCkfN/Pp5mATAsG8
D6MEG6cu7Bxj/K1Z6MxafUvCHrOPYWVU1wgRJGh+
t8Ux9emhFHpGHnQ/MpSfUOdQ==
not part of the certificate request---

```

[Browse for a file to insert.](#)

Certificate Template:

IPSEC

Additional Attributes:

Attributes:

Submit >

Base

64 인코딩 라디오 버튼을 클릭하고 인증서 다운로드를 클릭합니다

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded

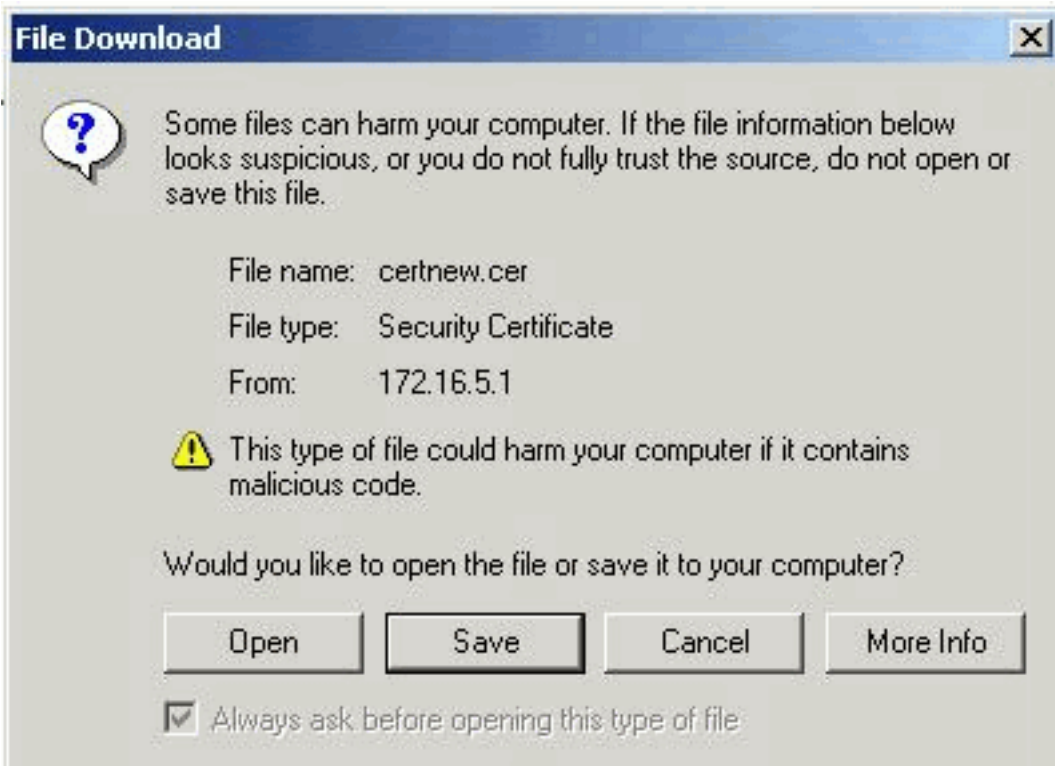


[Download certificate](#)

[Download certificate chain](#)

파일 다운로드 창

이 나타납니다. cert_client_id.cer 이름으로 저장합니다. ASA에 설치할 ID 인증서입니다



명령줄 예

```
CiscoASA
CiscoASA# configure terminal
CiscoASA(config)#crypto key generate rsa label my.ca.key
modulus 1024

!--- Generates 1024 bit RSA key pair. "label" defines
the name of the Key Pair. INFO: The name for the keys
will be: my.CA.key Keypair generation process begin.
Please wait... ciscoasa(config)#crypto ca trustpoint CA1
ciscoasa(config-ca-trustpoint)# subject-name
CN=CiscoASA.cisco.com,OU=TSWEB,
O=Cisco
Systems,C=US,St=North Carolina,L=Raleigh

!--- Defines x.500 distinguished name. Use the
```

```

attributes defined in table as a guide. CiscoASA(config-
ca-trustpoint)#keypair my.CA.key

!--- Specifies key pair generated in Step 3
CiscoASA(config-ca-trustpoint)#fqdn CiscoASA.cisco.com

!--- Specifies the FQDN (DNS:) to be used as the subject
alternative name CiscoASA(config-ca-
trustpoint)#enrollment terminal

!--- Specifies manual enrollment. CiscoASA(config-ca-
trustpoint)#exit
CiscoASA(config)#crypto ca enroll CA1
!--- Initiates certificate signing request. This is the
request to be !--- submitted via Web or Email to the
third party vendor. % Start certificate enrollment .. %
The subject name in the certificate will be:
cn=CiscoASA.cisco.com OU=TSWEB, O=Cisco Systems,
C=US,St=North Carolina,L=Raleigh % The fully-qualified
domain name in the certificate will be:
CiscoASA.cisco.com % Include the device serial number in
the subject name? [yes/no]: no
!--- Do not include the device's serial number in the
subject. Display Certificate Request to terminal?
[yes/no]: y
!--- Displays the PKCS#10 enrollment request to the
terminal. You will need to !--- copy this from the
terminal to a text file or web text field to submit to
!--- the third party CA. Certificate Request follows:
MIICKzCCAzQCAQAwga0xEDAOBgNVBACtB1JhbGVpZ2gxZmFzAVBgNVBAGT
Dk5vcnRo
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ21zY28gU31z
dGVtczEk
MCIGA1UEAxMbQ21zY29BU0EuY21zY28uY29tIE9VPVRTV0VCMTUwEgYD
VQQFEwtK
TVgwOTM1SzA1NDAfBgkqhkiG9w0BCQIWEkNpc2NvQVNBLmNpc2NvLmNv
bTCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuOIKqDMjVrdbZgBzUAjTc10j
xSlbkkcr
XgKoH2PcelcGZ9dUXn+Y09Qjm0Krj68L6KXT1PgNAaFMwB2YsTIO+hJ
BVq5Sxjv
MI6xLyKrGo7bOPAsLPeOBx1/LVLTy3ORqcy2QP3Ir1BSwoyBaoFPsRe
JGSAYG+O
QX8Jp6qcZE0CAwEAAaA9MDsGCSqGSIB3DQEJJDjEuMCwwCwYDVR0PBAQD
AgWgMB0G
A1UdEQQWMBSEkNpc2NvQVNBLmNpc2NvLmNvbTANBgkqhkiG9w0BAQQF
AAOBgQBM
3tzyAD7o6R5ej9EW7Ej4BfcXd20LCbXAoP5L1KbPaEeaCkfn/Pp5mATA
sG832TBm
bsxSvljSSXQsQ1Sb842D6MEG6cu7Bxj/K1Z6MxafUvCHROPYWVU1wgrJ
Gh+ndCZK j89/Y4S8XhQ79fvBwB8Ux9emhFHpGHnQ/MpSfU0dQ== --
--End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]: n
CiscoASA(config)#

```

3단계. 신뢰 지점 인증

서드파티 벤더로부터 ID 인증서를 받은 후에는 이 단계를 진행할 수 있습니다.

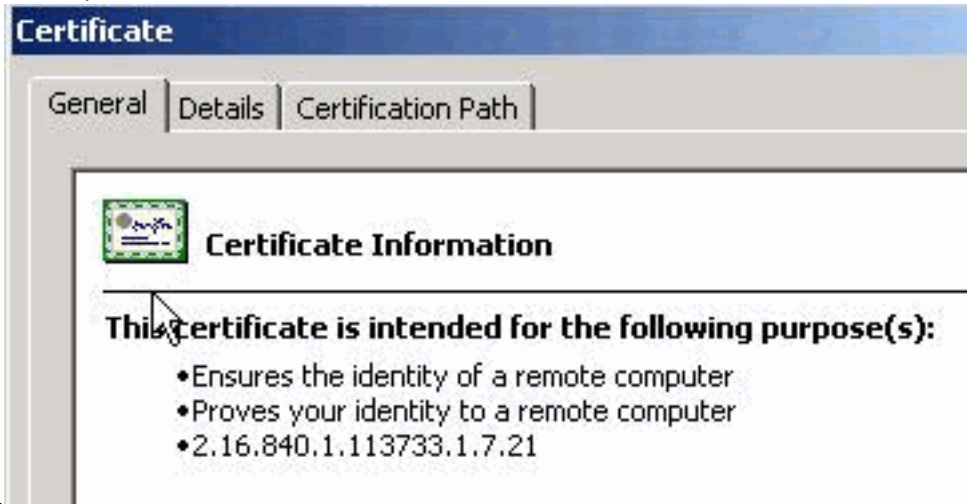
ASDM 절차

1. 로컬 컴퓨터에 ID 인증서를 저장합니다.
2. 에서 base64로 인코딩된 인증서가 파일로 제공되지 않은 경우 base64 메시지를 복사하여 텍스트 파일에 붙여넣어야 합니다.
3. 확장명이 .cer인 파일 이름을 바꿉니다. **참고:** 파일 이름이 .cer 확장명으로 변경되면 파일 아이



콘이 인증서로 표시됩니다.

4. 인증서 파일을 두 번 클릭합니다



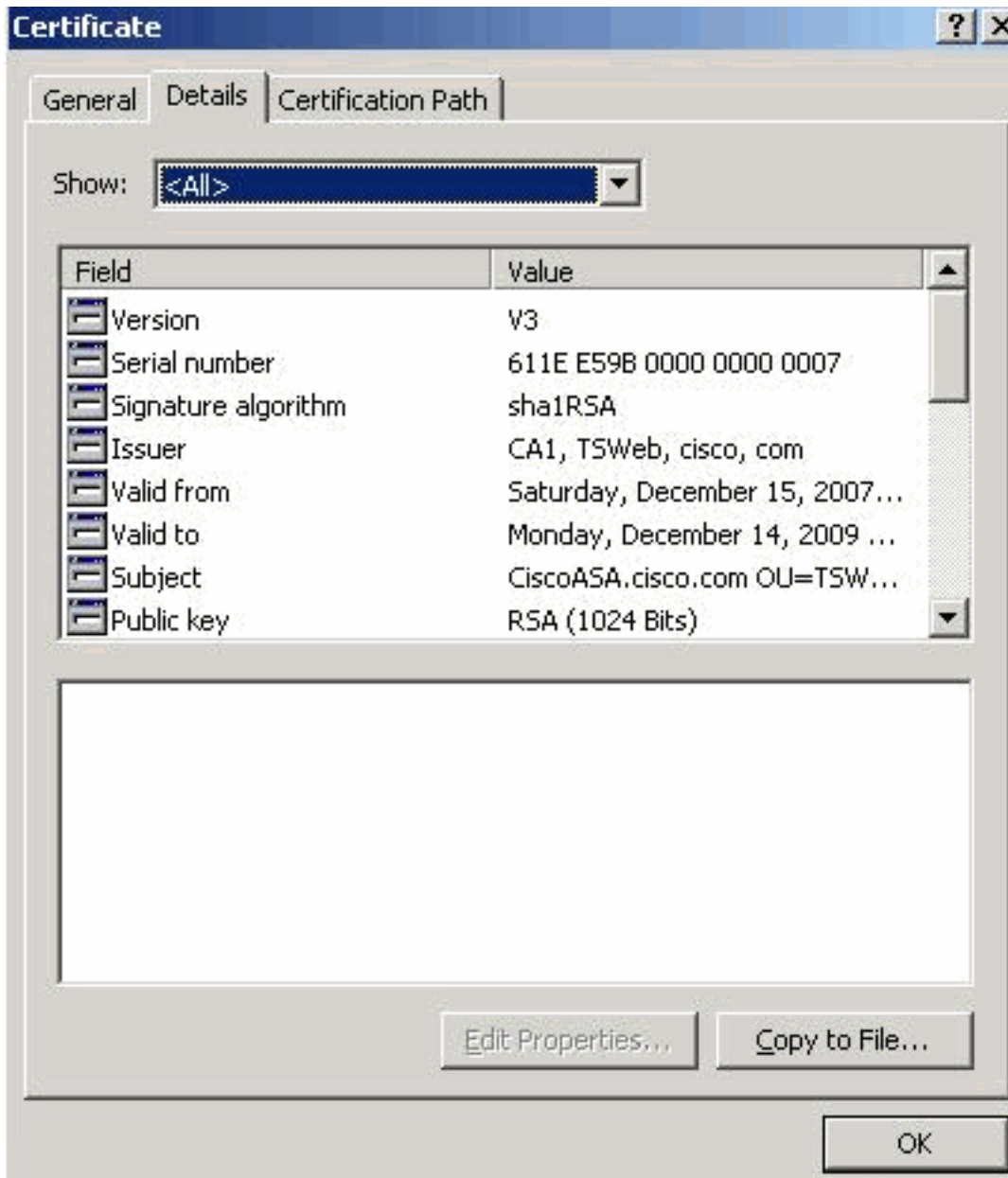
참고: Windows에 메시
지 일반 탭에 표시되는지 수 있는 정보가 경우 이 절차를 계속하기 전에 타사 공급업체 루트 CA 또는 중간 CA 인증서를 얻어야 합니다. 발급 루트 CA 또는 중간 CA 인증서를 얻으려면 타사 공급업체 또는 CA 관리자에게 문의하십시오.

5. Certificate **Path** 탭을 클릭합니다.
6. 발급된 ID 인증서와 연결된 CA 인증서를 클릭하고 View Certificate(인증서 보기)를 클릭합니

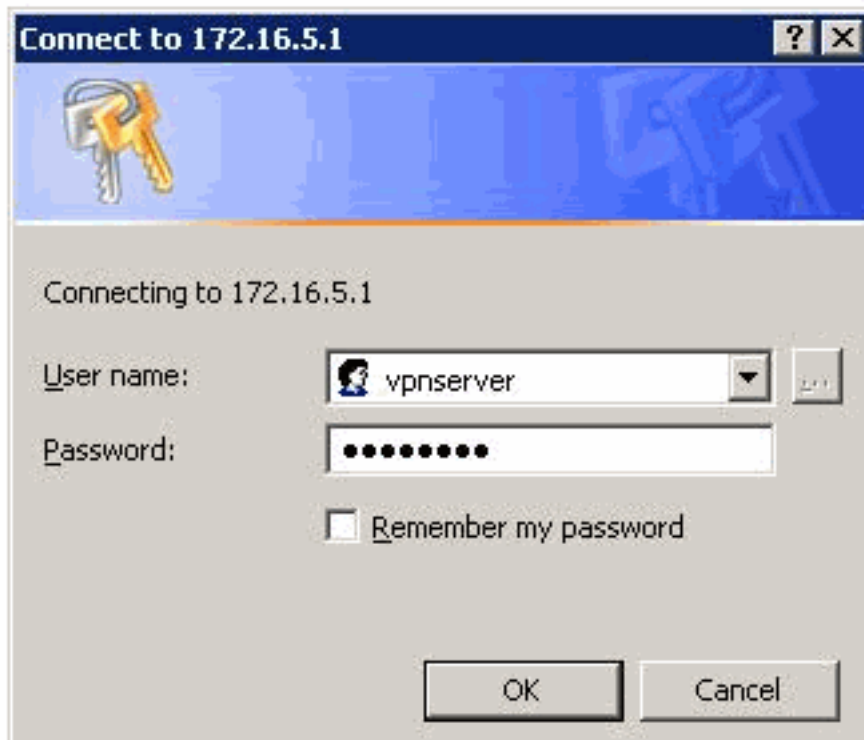
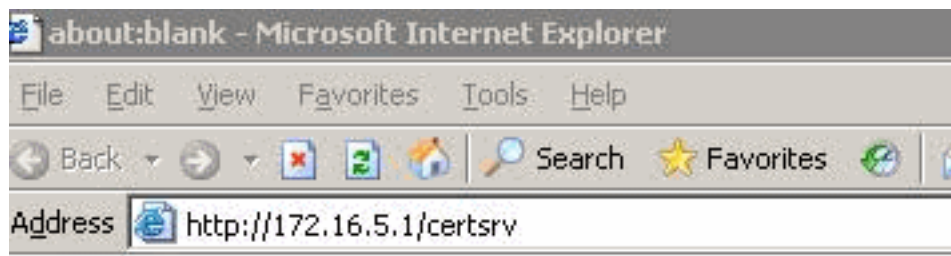


다. CA 인증서에 대한 자세한 정보가 나타납니다.

7. ID 인증서에 대한 자세한 내용을 보려면 Details를 클릭합니다



8. ID 인증서를 설치하기 전에 CA 서버에서 CA 인증서를 다운로드하여 ASA에 설치해야 합니다 (그림 참조). CA1이라는 CA 서버에서 CA 인증서를 다운로드하려면 다음 단계를 완료합니다 .VPN 서버에 제공된 자격 증명의 도움을 받아 CA 서버 172.16.5.1에 웹 로그인을 수행합니다



Download a CA certificate, certificate chain or CRL(CA 인증서, 인증서 체인 또는 CRL 다운로드)을 클릭하여 창을 엽니다(그림 참조). 인코딩 방법으로 Base 64 라디오 버튼을 클릭하고 CA 인증서 다운로드를 클릭합니다

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA cert](#)

To download a CA certificate, certificate chain, or CRL, select the certificate

CA certificate:



Encoding method:

- DER
 Base 64

- [Download CA certificate](#)
- [Download CA certificate chain](#)
- [Download latest base CRL](#)
- [Download latest delta CRL](#)

컴퓨터에 certnew.cer 이름으로 CA 인증서를 저장합니다



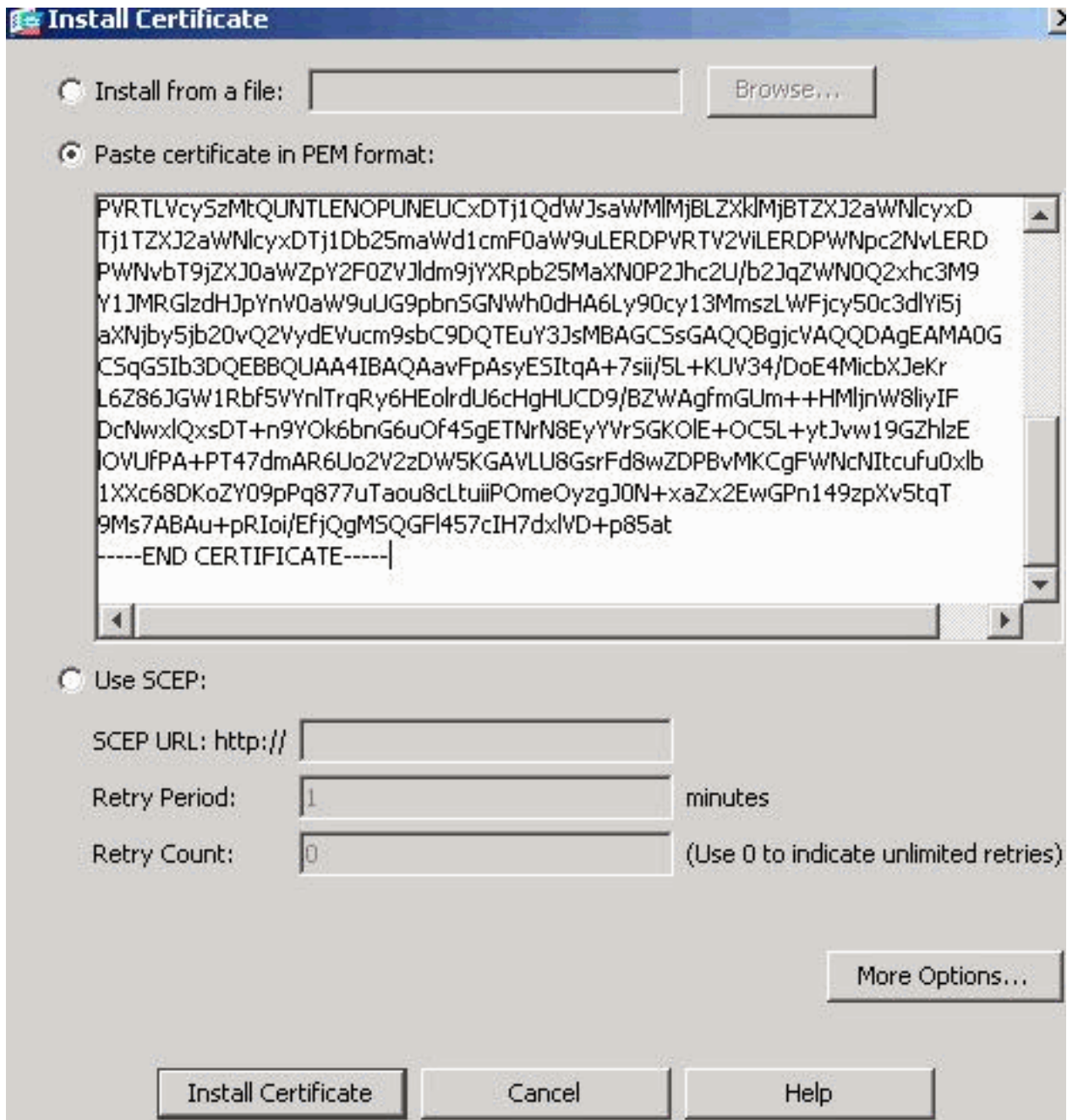
- CA 인증서를 저장한 위치를 찾습니다.
- 메모장과 같은 텍스트 편집기로 파일을 엽니다. 파일을 마우스 오른쪽 버튼으로 클릭하고 Send To(보내기) > Notepad(메모장)를 선택합니다.
- 이 이미지의 인증서와 유사한 base64 인코딩 메시지가 나타납니다

```

certnew.cer - Notepad
File Edit Format Help
-----BEGIN CERTIFICATE-----
MIIEntCCA4wgAwIBAgIQcJnxmUdk4JxGudqAowt0nDANBgkqhkiG9w0BAQUFADBRI
MRMwEQYKZImiZPyLGQBGRYDY29tMRUwEwYKZImiZPyLGQBGRYFY2IzY28xFTAT
BgoJkiajk/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIXNDA2MDE0
Ml0XDTEyMTIXNDA2MTAxNVowUTETMBEGCgmsJomT8ixkARKWA2NvbTEVMBMGCS
JomT8ixkARKwBWNpc2NvMRUwEwYKZImiZPyLGQBGRYFVFNXZWIXDDAKBgNVBAMT
A0NBMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAAOqP7seuvvyiLmA9
BSGZMz3sctR9TCMwOx7qM8mmiD0o7OkGApAvmtHrK431iMuaekBpo5Zd4TNgntjX
bt6czaHpBuyIsyoZ0OU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vweMijcQnwdOq+
Kx+swaenCjslrxeuaHpIBTuaNOckueBUBjxgpJUNPAk1G8YwBfaTV4M7kZf4dbQI
y3GoFGmh8zGx6ys1DEaUQXRvwhdbMivwqYBXWkh4u04xxQmr//5ct1tdwQcvk2V
uBwCsptw7C1akTqfm5XK/d//z2euuxrHYysQCfoFyk1vE6/qlo+fQessz+Tldhxx
wPXRO18CAwEAAaOCaw8wggFrMBMGCSsGAQQBgjCUAgQHggQAQwBBMASGA1UddwQE
AwIBhjAPBgnVHRMBAF8EBTADAQH/MB0GA1UdDgQWBBTZrb8I8jqI8RRDL3myfNQJ
pAPlwDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtwxkYXA6Ly8vQ049Q0ExLENO
PVRTLvcyszmtQUNTLENOPUNEUCxDTj1QdwJsawMlMjBLZxk1MjBTZXJ2awN1cyxD
Tj1TZXJ2awN1cyxDTj1Db25mawd1cmF0aw9uLERDPVRTV2ViLERDPWnpc2NvLERD
PWNvbT9jZXJ0awZpY2F0ZVJ1dm9jYXRpb25MaXN0P2Jhc2U/b2JqZWNOQ2xhc3M9
Y1JMRG1zdHJpYnV0aw9uUG9pbnsGNWwh0dHA6Ly90cy13MmszLWwFjcy50c3dlYi5j
aXNjby5jb20vQ2vydEVucm9sbc9DQTEuY3JsMBAGCSsGAQQBgjcvAQQDAgEAMA0G
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqa+7sii/5L+KUV34/DoE4MibXJekr
L6Z86JGw1Rbf5vyn1TrqRy6HEOlrdU6cHgHUCD9/BZWagfmGum++HMLjnw8liYIF
DcnwxlQxsDT+n9YOk6bnG6uof4SgETNrN8EyyVrSGKOlE+OC5L+ytJvw19Gzh1ze
lOVUFPA+PT47dmAR6Uo2V2ZDW5KGAVLU8GsrFd8wZDPBVMKCGFwNcNItcufu0x1b
1XXc68DKoZY09pPq877uTaou8cLtuipPomeOyzgJ0N+xaZx2EwGPN149zpxv5tqt
9Ms7ABAU+pRIoi/EfjQgMSQGF1457cIH7dx1VD+p85at
-----END CERTIFICATE-----

```

12. ASDM에서 Configuration(컨피그레이션)을 클릭한 다음 Device Management(디바이스 관리)를 클릭합니다.
13. Certificate Management(인증서 관리)를 확장하고 CA Certificates(CA 인증서)를 선택합니다.
14. Add(추가)를 클릭합니다.
15. Paste certificate in PEM Format(PEM 형식으로 인증서 붙여넣기) 라디오 버튼을 클릭하고 서드파티 벤더가 제공한 base64 CA 인증서를 텍스트 필드에 붙여넣습니다.
16. Install Certificate를 클릭합니다



설

치가 성공했음을 확인하는 대화 상자가 나타납니다.

명령줄 예

```

CiscoASA
CiscoASA(config)#crypto ca authenticate CA1
!--- Initiates the prompt for paste-in of base64 CA
intermediate certificate. ! This should be provided by
the third party vendor. Enter the base 64 encoded CA
certificate. End with the word "quit" on a line by
itself -----BEGIN CERTIFICATE-----
MIIE nTCCA4WgAwIBAgIQcJnxmUdk4JxGUDqAoWt0nDANBgkqhkiG9w0B
AQUFADBR
MRMwEQYKCZImiZPyLQG BGRYDY29tMRUwEwYKCZImiZPyLQG BGRYFY21z
Y28xFTAT
BgoJkiaJk/IsZAEZFgVUU1d1YjEMMAoGA1UEAxMDQ0E xMB4XDTA3MTIx
NDA2MDE0
M1oXDTEyMTIxNDA2MTAxNvowUTETMBEGCgmSJomT8ixkARkWA2NvbTEV
MBMGCgMS
JomT8ixkARkWBWNpc2NvMRUwEwYKCZImiZPyLQG BGRYFVFNXZWI xDDAK

```

```

BgNVBAMT
A0NBMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seu
VvyiLmA9
BSGzMz3sCtR9TCMWOx7qM8mmiD0o7OkGApAvmtHrK431iMuaeKBpo5Zd
4TNgNtjX
bt6czaHpBuyIsyoZ0OU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vWeMij
cQnwdOq+
Kx+sWaeNCjs1rxeuAhpIBTuaNOckueBUBjxgPJUNPAk1G8YwBfaTV4M7
kZf4dbQI
y3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvwqYBXWKh4uC04xxQmr//Sct1t
dWQcvk2V
uBwCsptW7C1akTqfm5XK/d//z2eUuXrHYySQcfoFyk1vE6/Q1o+fQeSS
z+T1DhXx
wPXRO18CAwEAAaOCAW8wggFrMBMGCSsGAQQBgjcUAQOQHGAQwBBMAsg
A1UdDwQE
AwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBbTZrb8I8jqI8RRD
L3mYfnQJ
pAP1WDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtWxkYXA6Ly8vQ049
Q0ExLENO
PVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdWJsaWMM1mJBLZXk1mJBTZXJ2
aWN1cyxD
Tj1TZXJ2aWN1cyxDtj1Db25maWd1cmF0aW9uLERDPVRTV2ViLERDPWNp
c2NvLERD
PWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWNO
Q2xhc3M9
Y1JMRG1zdHJpYnV0aW9uUG9pbnsGNWh0dHA6Ly90cy13MmszLWFwcy50
c3dlYi5j
aXNjby5jb20vQ2VydeVucm9sbC9DQTEuY3JsMBAGCSsGAQQBgjcVAQOD
AgEAMA0G
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItQA+7sii/5L+KUV34/DoE4M
icbXJeKr
L6Z86JGW1Rbf5VYnlTrqRy6HEolrdU6cHgHUCD9/BZWAghmGUm++HM1j
nW8liYIF
DcNwxlQxsDT+n9YOk6bnG6uOf4SgETNrN8EyYVrSGK0LE+OC5L+ytJvw
19GZhlzE
lOVUfPA+PT47dmAR6Uo2V2zDW5KGAVLU8GsrFd8wZDPBvMKCGFWNcNI
tcfu0x1b
1XXc68DKoZY09pPq877uTaou8cLtuuiPomeOyZgJ0N+xaZx2EwGpN149
zpXv5tqT
9Ms7ABAU+pRIoi/EfjQgMSQGF1457cIH7dxlVD+p85at
-----END CERTIFICATE-----
quit
!--- Manually pasted certificate into CLI. INFO:
Certificate has the following attributes: Fingerprint:
98d66001 f65d98a2 b455fbce d672c24a Do you accept this
certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

% Certificate successfully imported
CiscoASA(config)#

```

4단계. 인증서 설치

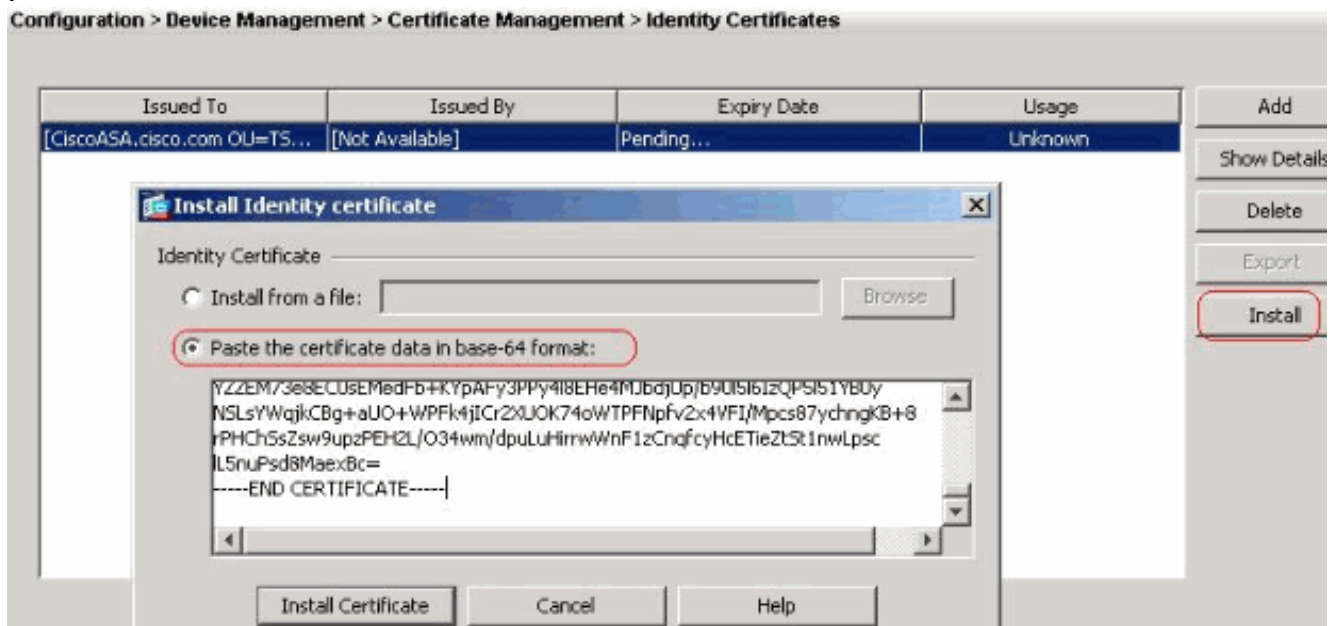
ASDM 절차

다음 단계를 완료하려면 서드파티 벤더가 제공한 ID 인증서를 사용하십시오.

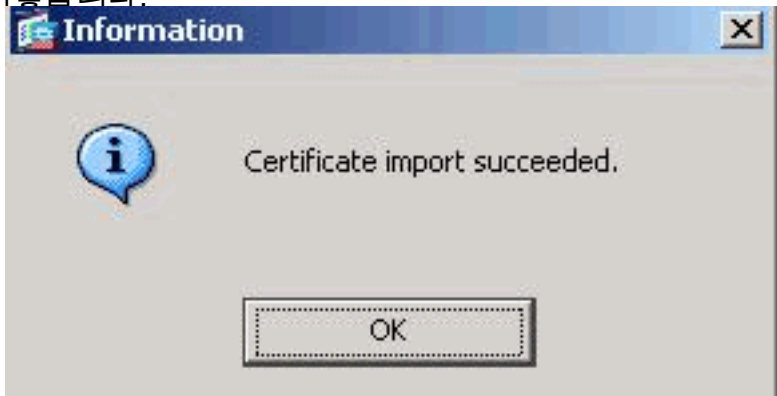
1. Configuration(컨피그레이션)을 클릭한 다음 Device Management(디바이스 관리)를 클릭합니다.
2. Certificate Management(인증서 관리)를 확장한 다음 Identity Certificates(ID 인증서)를 선택합

니다.

- 2단계에서 생성한 ID 인증서를 선택합니다.참고: 만료 날짜가 보류 중으로 표시됩니다.
- Install(설치)을 클릭합니다



Paste the certificate data in base-64 format 라디오 버튼을 클릭하고 서드파티 벤더가 제공한 ID 인증서를 텍스트 필드에 붙여넣습니다.



5. Install Certificate를 클릭합니다.
기가 성공했는지 확인하는 대화 상자가 나타납니다.

가져오

명령줄 예

```
CiscoASA
CiscoASA(config)#crypto ca import CA1 certificate
!--- Initiates prompt to paste the base64 identity !---
certificate provided by the third party vendor. %The
fully-qualified domain name in the certificate will be:
CiscoASA.cisco.com Enter the base 64 encoded
certificate. End with the word "quit" on a line by
itself !--- Paste the base 64 certificate provided by
the third party vendor. -----BEGIN CERTIFICATE-----
MIIFpzCCBI+gAwIBAgIKYR7lmwAAAAAABzANBgkqhkiG9w0BAQUFADBR
MRMwEQYK
CZImiZPyLGQBGRYDY29tMRUwEwYKZImiZPyLGQBGRYFY21zY28xFTAT
BgoJkiaJ
k/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0EzMB4XDTA3MTIxNTA4MzUz
OVoxDTA5
MTIxNDA4MzUzOVowdjELMAkGA1UEBhMCVVMxFTZAVBgNVBAGTDk5vcnRo
IENhcm9s
```

```
aW5hMRAwDgYDVQOHEwdSYWxlaWdoMRYwFAYDVQOKEw1DaXNjbyBTeXNO
ZW1zMSQw
IgyYDVQOQDExtDaXNjb0FTQS5jaXNjby5jb20gT1U9VFNXRUIwgZ8wDQYJ
KoZlhvcN
AQEBBQADgY0AMIGJAoGBALjiCqgzI1a3W2YAc1AI03NdI8UpW5JHK14C
qB9j3HpX
BmfXVF5/mNPUI5tCq4+vC+il05T4DQGhTMAdmLEyDp/oSQVauUsY7zCO
sS8iqxqO
2zjwLcZ3jgcZfy1S08tzkanMstkD9yK9QUsKMgWqBT7EXiRkgGBvjkF/
CaeqnGRN
AgMBAAGjggLeMIIC2jALBgNVHQ8EBAMCBaAwHQYDVROBBYwFIISQ21z
Y29BU0Eu
Y21zY28uY29tMB0GA1UdDgQWBBSJC3bSQzeGv4tY+MeH7KM10xCFjAf
BgNVHSME
GDAWgBTZrb8I8jqI8RRDL3mYfNqJpAP1WCCAQMGA1UdHwSB+zCB+DCB
9aCB8qCB
74aBtWxkYXA6Ly8vQ049Q0ExLENOPVRTLVcySzMtQUNTLENOPUNEUCxID
Tj1QdWJs
aWM1MjBLZXk1MjBTZXJ2aWN1cyxDTj1TZXJ2aWN1cyxDTj1Db25maWd1
cmF0aW9u
LERDPVRTV2ViLERDPWNpc2NvLERDPWNvbT9jZXJ0aWZpY2F0ZVJldm9j
YXRpb25M
aXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbmSG
NWh0dHA6
Ly90cy13MmszLWFjcy50c3dlYi5jaXNjby5jb20vQ2VydeVucm9sbC9D
QTEuY3Js
MIIBHQYIKwYBBQUHAQEgEgEPMIIBCzCBQYIKwYBBQUHMAKGgZxsZGFw
Oi8vL0NO
PUNBMSxDTj1BSUESQ049UHvibG1jJTIwS2V5JTIwU2Vydm1jZXMsQ049
U2Vydm1j
ZXMsQ049Q29uZmlndXJhdG1vbixEQz1UU1dlYixEQz1jaXNjbyxEQz1j
b20/Y0FD
ZXJ0aWZpY2F0ZT9iYXN1P29iamVjdENsYXNzPWN1cnRpZmljYXRpb25B
dXR0b3Jp
dHkwXQYIKwYBBQUHMAKGUWh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5j
aXNjby5j
b20vQ2VydeVucm9sbC9UUy1XMksZLUFDUy5UU1dlYi5jaXNjby5jb21f
Q0ExLmNy
dDAhBgkrBgEEAYI3FAIEFB4SAFcAZQBiAFMAZQByAHYAZQByMAWGA1Ud
EwEB/wQC
MAAwEwYDVRO1BAwwCgyIKwYBBQUHAWEdDQYJKoZIhvcNAQEFBQADggEB
AIqCaA9G
+8h+3IS8rfVAGzcWAEVRXCyBlx0NpR/jlocGJ7QbQxkjKEswXq/O2xDB
7wXQaGph
zRq4dxAL111JkIjhfeQY+7VSkZlGEpuBnENTohdhtz5vBjG1cROXIs8
+3Ghg8hy
YZZEM73e8EC0sEMedFb+KYpAFy3PPy418EHe4MJbdjUp/b901516IzQP
5151YB0y
NSLsYWqjkCBg+aUO+WPFk4jICr2XUOK74oWTFPNpfv2x4VFI/Mpcs87y
chngKB+8
rPHChSsZsw9upzPEH2L/O34wm/dpuLuHirrwWnF1zCnqfcyHcETieZtS
tlnwLpsc
lL5nuPsd8MaexBc=
-----END CERTIFICATE-----
quit
```

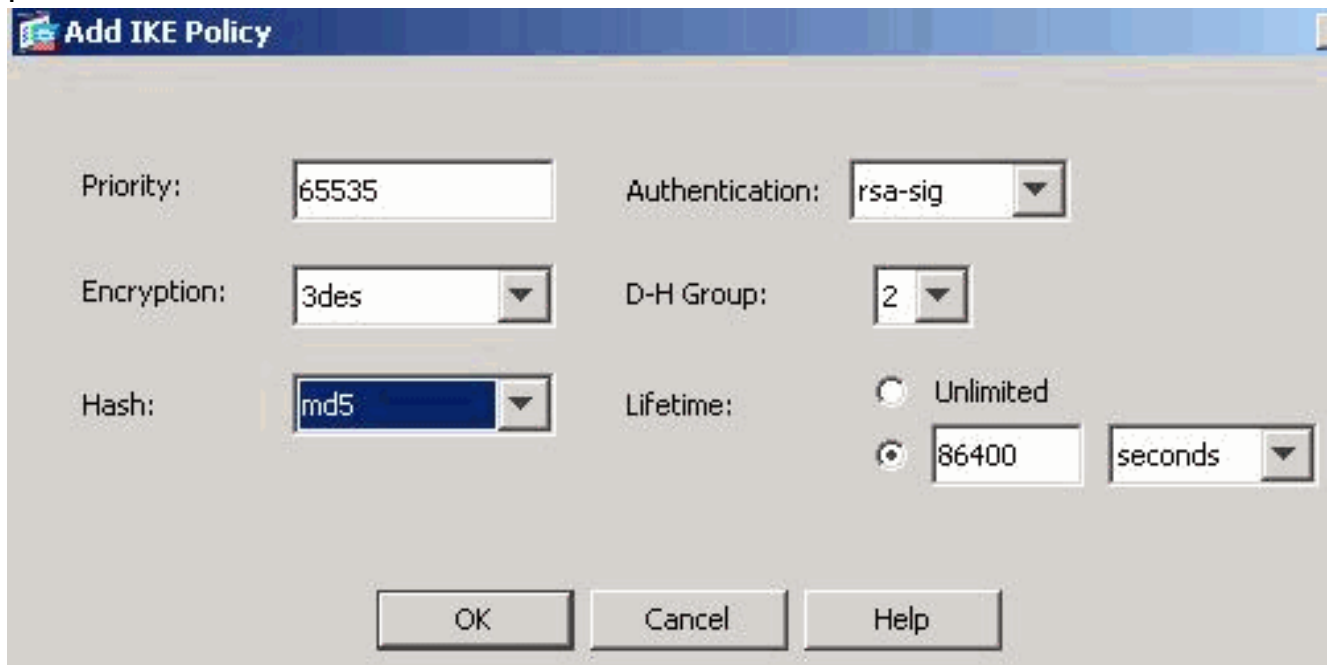
```
INFO: Certificate successfully imported
CiscoASA(config)#
```

[5단계. 새로 설치된 인증서를 사용하도록 IPsec\(Remote Access VPN\)을 구성합니다.](#)

ASDM 절차

원격 액세스 VPN을 구성하려면 다음 단계를 완료합니다.

1. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Advanced(고급) > IPSec > IKE Policies(IKE 정책) > Add(추가)를 선택하여 ISAKMP 정책 65535를 생성합니다



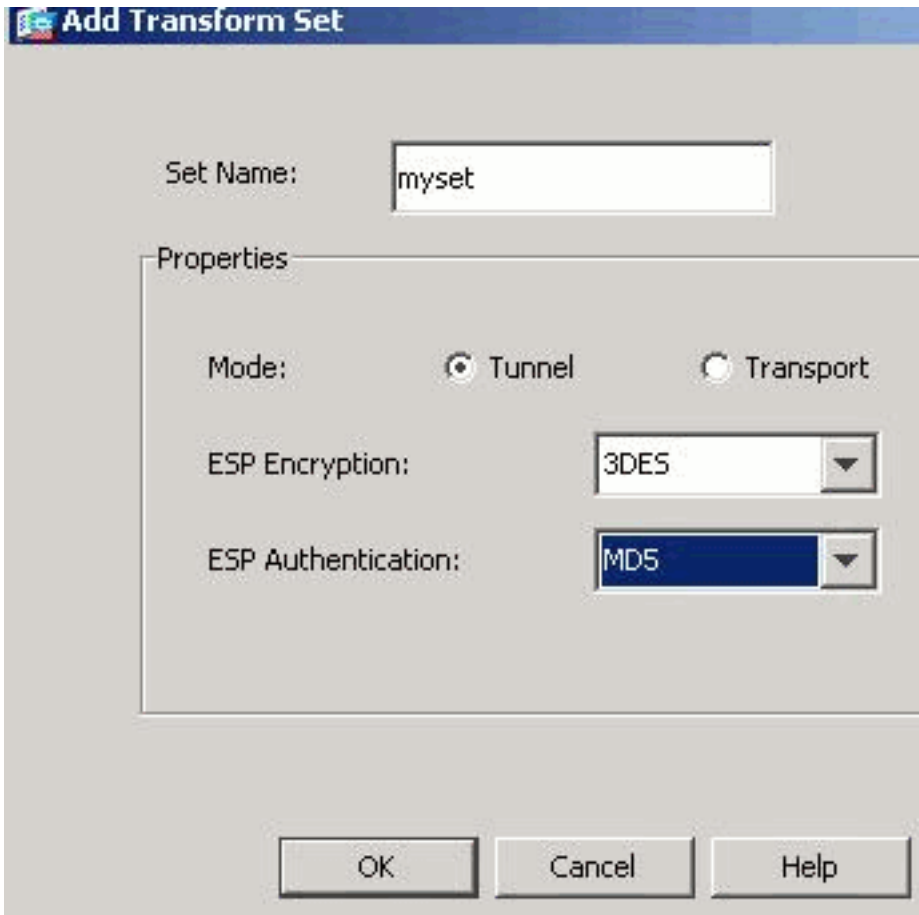
The screenshot shows the 'Add IKE Policy' dialog box with the following settings:

Priority:	65535	Authentication:	rsa-sig
Encryption:	3des	D-H Group:	2
Hash:	md5	Lifetime:	<input checked="" type="radio"/> 86400 seconds

Buttons: OK, Cancel, Help

OK(확인)와 Apply(적용)를 클릭합니다.

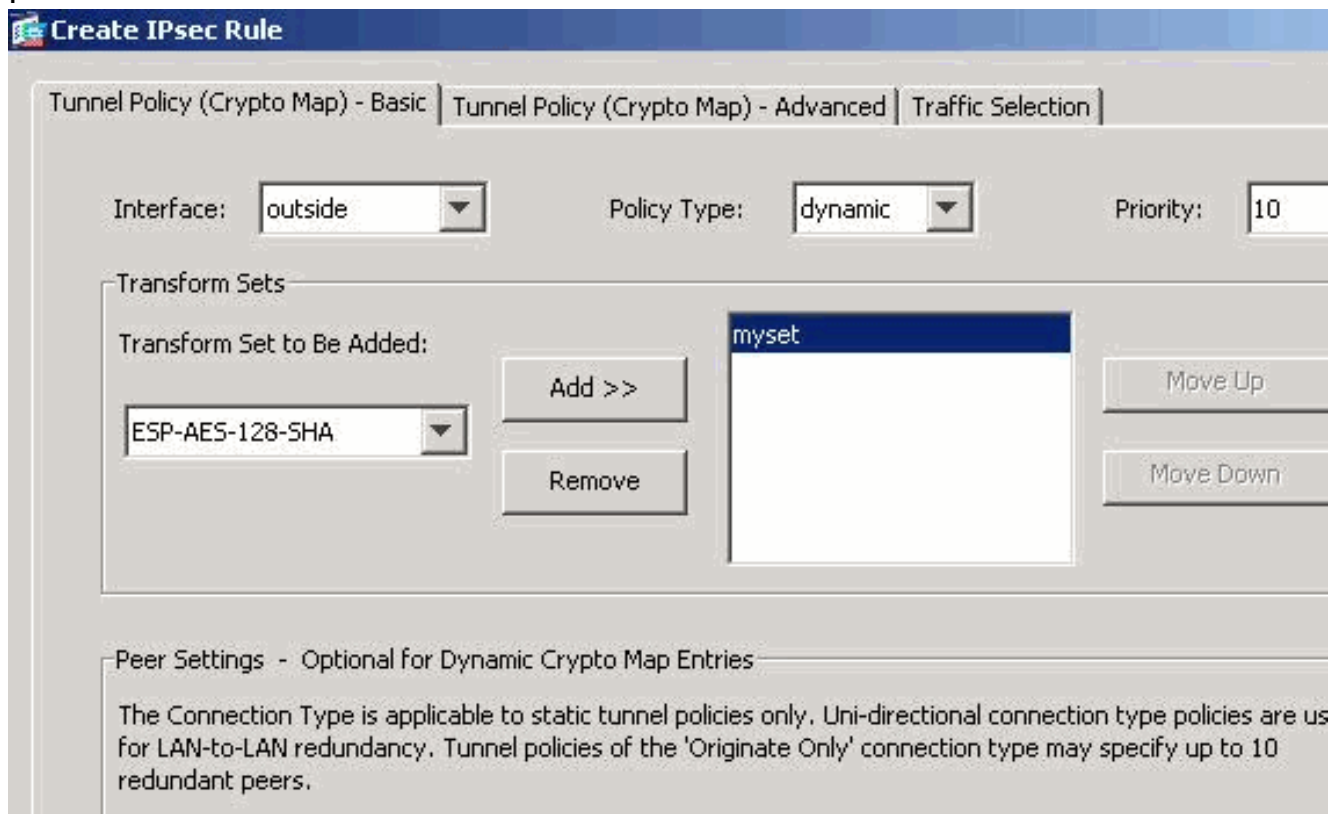
2. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Advanced(고급) > IPSec > IPSec Transform Sets(IPSec 변형 집합) > Add(추가)를 선택하여 myset 변형 집합을 생성합니다



OK(확인)와 Apply(적용)를

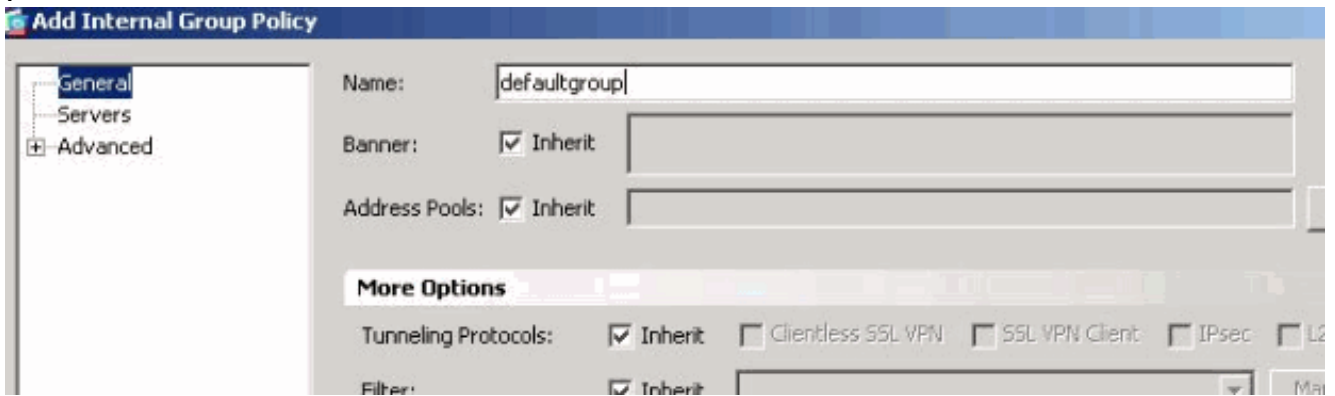
클릭합니다.

3. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Advanced(고급) > IPsec > Crypto Maps(암호화 맵) > Add(추가)를 선택하여 우선순위 10의 동적 정책으로 암호화 맵을 생성합니다



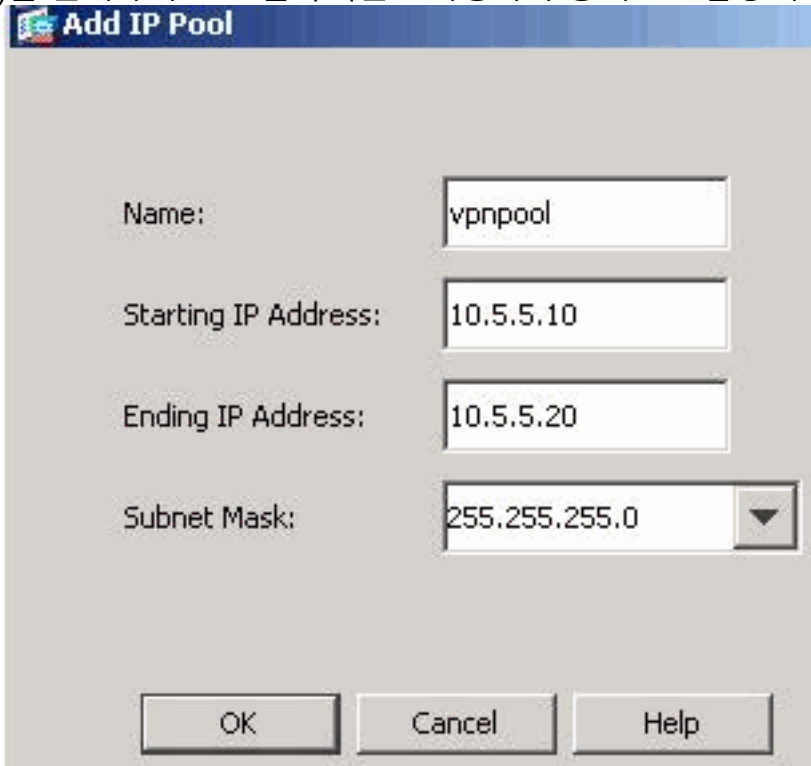
OK(확인)와 Apply(적용)를 클릭합니다.참고: ASA 8.0은 SHA 2를 지원하지 않습니다. 또한 256 해시와 함께 인증서를 사용하는 IPsec 클라이언트는 지원되지 않습니다.

- Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Advanced(고급) > Group Policies(그룹 정책) > Add(추가)를 선택하여 **Defaultgroup** group policy(기본 그룹 정책)를 생성합니다



OK(확인)와 Apply(적용)를 클릭합니다.

- Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Address Assignment(주소 할당) > Address Pools(주소 풀) > Add(추가)를 선택하여 VPN 클라이언트 사용자가 동적으로 할당되도록 **vpnpool** 주소 풀을 구



성합니다.

OK(확인)와 Apply(적용)를 클릭합니다.

OK(확인)와 Apply(적용)

- VPN 클라이언트 액세스를 위한 **vpnuser** 사용자 계정을 생성하려면 Configuration(컨피그레이션) > Remote Access VPN(원격 액세스 VPN) > AAA Setup(AAA 설정) > Local Users(로컬 사용자) > Add(추가)를 선택합니다. 또한 이 사용자를 DefaultRAGroup의 멤버로 설정합니다

Add User Account

Identity
+ VPN Policy

Username:

Password:

Confirm Password:

User authenticated using MSCHAP

Member-of

Member-of:

DefaultRAGroup

Access Restriction

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.
Note: All users have network access, regardless of these settings.

Full access(ASDM, SSH, Telnet and Console)
Privilege level is used with command authorization.
Privilege Level:

CLI login prompt for SSH, Telnet and console (no ASDM access)
This setting is effective only if AAA authenticate console command is configured.

No ASDM, SSH, Telnet or Console access
This setting is effective only if AAA authenticate console command is configured.

7. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > IPsec Connection Profiles(IPsec 연결 프로파일) > Edit(편집)를 선택하여 DefaultRAGroup을 표시된 대로 편집합니다. IKE Peer Authentication(IKE 피어 인증) 필드의 드롭다운에서 적절한 ID 인증서를 선택합니다. User Authentication(사용자 인증) 필드에 대해 서버 그룹을 LOCAL로 선택합니다. Client Address Assignment(클라이언트 주소 할당) 필드에 대한 Client Address Pool(클라이언트 주소 풀)을 선택합니다. 기본 그룹 정책 필드에 대한 그룹 정책으로 기본 그룹을 선택합니다

Add IPsec Remote Access Connection Profile

Basic

- Advanced
 - General
 - Client Addressing
 - Authentication
 - Authorization
 - Accounting
 - IPsec
 - PPP

Name: DefaultRAGroup

IKE Peer Authentication

Pre-shared Key: [Empty]

Identity Certificate: [cn=CiscoASA.cisco.com OU=TSWEB, o=Cisco Systems, ...]

User Authentication

Server Group: LOCAL

Fallback: Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers: [Empty]

Client Address Pools: vpnpool

Default Group Policy

Group Policy: defaultgroup

Client Protocols: IPsec L2TP over IPsec

OK(확인)와 Apply(적용)를 클릭합니다.

명령줄 예

```

CiscoASA
CiscoASA(config)#crypto isakmp enable outside
CiscoASA(config)#crypto isakmp policy 65535
CiscoASA(config-isakmp-policy)#authentication rsa-sig
CiscoASA(config-isakmp-policy)#encryption 3des
CiscoASA(config-isakmp-policy)#hash md5
CiscoASA(config-isakmp-policy)#group 2
CiscoASA(config-isakmp-policy)#lifetime 86400
CiscoASA(config-isakmp-policy)#exit
CiscoASA(config)#crypto isakmp identity auto

!--- Phase 1 Configurations CiscoASA(config)#crypto
ipsec transform-set myset esp-3des esp-md5-hmac
CiscoASA(config)#crypto dynamic-map dynmap 10 set
transform-set myset
CiscoASA(config)#crypto map mymap 10 ipsec-isakmp
dynamic dynmap
CiscoASA(config)#crypto map mymap interface outside

!--- Phase 2 Configurations CiscoASA(config)#group-
policy defaultgroup internal
CiscoASA(config)#group-policy defaultgroup attributes
CiscoASA(config-group-policy)#default-domain value
cisco.com
CiscoASA(config-group-policy)# exit

!--- Create a group policy "defaultgroup" with domain
name !--- cisco.com CiscoASA(config)#username vpnuser
password Cisco123
CiscoASA(config)#username vpnuser attributes
CiscoASA(config-username)#memberof DefaultRAGroup
CiscoASA(config-username)#exit

```

```

!--- Create a user account "vpnuser" and added to !---
"DefaultGroup" CiscoASA(config)#tunnel-group
DefaultRAGroup general-attributes

!--- The Security Appliance provides the default tunnel
groups !--- for remote access (DefaultRAGroup).
CiscoASA(config-tunnel-general)#address-pool vpnpool

!--- Associate the vpnpool to the tunnel group using the
address pool. CiscoASA(config-tunnel-general)#default-
group-policy Defaultgroup

!--- Associate the group policy "Defaultgroup" to the
tunnel group. CiscoASA(config-tunnel-general)# exit
CiscoASA(config)#tunnel-group DefaultRAGroup ipsec-
attributes
CiscoASA(config-tunnel-ipsec)#trust-point CA1
CiscoASA(config-tunnel-ipsec)#exit

!--- Associate the trustpoint CA1 for IPSec peer !---
authentication

```

ASA 구성 요약

CiscoASA

```

CiscoASA#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname CiscoASA
domain-name cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.1.5 255.255.255.0
!
interface Ethernet0/1
 shutdown
 nameif inside
 security-level 100
 ip address 10.2.2.1 255.255.255.0
!
interface Ethernet0/2
 nameif DMZ
 security-level 90
 ip address 10.77.241.142 255.255.255.192
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!

```

```
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
 !
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.com
access-list 100 extended permit ip 10.2.2.0
255.255.255.0 10.5.5.0
 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu DMZ 1500
ip local pool vpnpool 10.5.5.10-10.5.5.20
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list 100
route DMZ 0.0.0.0 0.0.0.0 10.77.241.129 1
route outside 10.1.1.0 255.255.255.0 192.168.1.1 1
route outside 172.16.5.0 255.255.255.0 192.168.1.1 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
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 DMZ
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
crypto ipsec transform-set myset esp-3des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap interface outside
crypto ca trustpoint CA1
 enrollment terminal
 subject-name cn=CiscoASA.cisco.com OU=TSWEB, O=Cisco
Systems, C=US,
 St=North Carolina,L=Rale
 serial-number
 keypair my.CA.key
 crl configure
crypto ca certificate chain CA1
 certificate 611ee59b00000000000007
 308205a7 3082048f a030201 02020a61 1ee59b00
00000000 07300d06 092a8648
 86f70d01 01050500 30513113 3011060a 09922689
93f22c64 01191603 636f6d31
 15301306 0a099226 8993f22c 64011916 05636973
636f3115 3013060a 09922689
 93f22c64 01191605 54535765 62310c30 0a060355
```

04031303 43413130 1e170d30
37313231 35303833 3533395a 170d3039 31323134
30383335 33395a30 76310b30
09060355 04061302 55533117 30150603 55040813
0e4e6f72 74682043 61726f6c
696e6131 10300e06 03550407 13075261 6c656967
68311630 14060355 040a130d
43697363 6f205379 7374656d 73312430 22060355
0403131b 43697363 6f415341
2e636973 636f2e63 6f6d204f 553d5453 57454230
819f300d 06092a86 4886f70d
01010105 0003818d 00308189 02818100 b8e20aa8
332356b7 5b660073 5008d373
5d23c529 5b92472b 5e02a81f 63dc7a57 0667d754
5e7f98d3 d4239b42 ab8faf0b
e8a5d394 f80d01a1 4cc01d98 b1320e9f e849055a
b94b18ef 308eb12f 22ab1a8e
db38f02c 2cf78e07 197f2d52 d3cb7391 a9ccb2d9
03f722bd 414b0a32 05aa053e
c45e2464 80606f8e 417f09a7 aa9c644d 02030100
01a38202 de308202 da300b06
03551d0f 04040302 05a0301d 0603551d 11041630
14821243 6973636f 4153412e
63697363 6f2e636f 6d301d06 03551d0e 04160414
2c242ddb 490cde1a fe2d63e3
1e1fb28c 974c4216 301f0603 551d2304 18301680
14d9adbf 08f23a88 f114432f
79987cd4 09a403e5 58308201 03060355 1d1f0481
fb3081f8 3081f5a0 81f2a081
ef8681b5 6c646170 3a2f2f2f 434e3d43 41312c43
4e3d5453 2d57324b 332d4143
532c434e 3d434450 2c434e3d 5075626c 69632532
304b6579 25323053 65727669
6365732c 434e3d53 65727669 6365732c 434e3d43
6f6e6669 67757261 74696f6e
2c44433d 54535765 622c4443 3d636973 636f2c44
433d636f 6d3f6365 72746966
69636174 65526576 6f636174 696f6e4c 6973743f
62617365 3f6f626a 65637443
6c617373 3d63524c 44697374 72696275 74696f6e
506f696e 74863568 7474703a
2f2f7473 2d77326b 332d6163 732e7473 7765622e
63697363 6f2e636f 6d2f4365
7274456e 726f6c6c 2f434131 2e63726c 3082011d
06082b06 01050507 01010482
010f3082 010b3081 a906082b 06010505 07300286
819c6c64 61703a2f 2f2f434e
3d434131 2c434e3d 4149412c 434e3d50 75626c69
63253230 4b657925 32305365
72766963 65732c43 4e3d5365 72766963 65732c43
4e3d436f 6e666967 75726174
696f6e2c 44433d54 53576562 2c44433d 63697363
6f2c4443 3d636f6d 3f634143
65727469 66696361 74653f62 6173653f 6f626a65
6374436c 6173733d 63657274
69666963 6174696f 6e417574 686f7269 7479305d
06082b06 01050507 30028651
68747470 3a2f2f74 732d7732 6b332d61 63732e74
73776562 2e636973 636f2e63
6f6d2f43 65727445 6e726f6c 6c2f5453 2d57324b
332d4143 532e5453 5765622e
63697363 6f2e636f 6d5f4341 312e6372 74302106
092b0601 04018237 14020414
1e120057 00650062 00530065 00720076 00650072

300c0603 551d1301 01ff0402
30003013 0603551d 25040c30 0a06082b 06010505
07030130 0d06092a 864886f7
0d010105 05000382 0101008a 82680f46 fbc87edc
84bc45f5 401b3716 0045515c
2c81971d 0da51fe3 96870627 b41b4319 23284b30
5eafcedb 10c1ef05 d0686a61
cd1ab877 100b965d 499088e1 7de418fb b5529199
46129b81 9c4353a2 1761b61c
f9bc18c6 95c44e5c 8b3cfb71 a183c872 61964433
bddef040 b4b0431e 7456fe29
8a40172d cf3f2e25 f041dee0 c25b7635 29fdbf74
97997a23 340fe65e 75601d32
3522ec61 6aa39020 60f9a50e f963c593 88c80abd
9750e2bb e285933c 53697efd
b1e15148 fcca5cb3 cef27219 e0281fbc acf1c285
2b19b30f 6ea733c4 1f62ff3b
7e309bf7 69b8bb87 8abaf05a 7175cc29 ea7dcc87
7044e279 9b52b759 f02e9b1c
94be67b8 fb1df0c6 9ec417
quit
certificate ca 7099f1994764e09c4651da80a16b749c
3082049d 30820385 a0030201 02021070 99f19947
64e09c46 51da80a1 6b749c30
0d06092a 864886f7 0d010105 05003051 31133011
060a0992 268993f2 2c640119
1603636f 6d311530 13060a09 92268993 f22c6401
19160563 6973636f 31153013
060a0992 268993f2 2c640119 16055453 57656231
0c300a06 03550403 13034341
31301e17 0d303731 32313430 36303134 335a170d
31323132 31343036 31303135
5a305131 13301106 0a099226 8993f22c 64011916
03636f6d 31153013 060a0992
268993f2 2c640119 16056369 73636f31 15301306
0a099226 8993f22c 64011916
05545357 6562310c 300a0603 55040313 03434131
30820122 300d0609 2a864886
f70d0101 01050003 82010f00 3082010a 02820101
00ea8fee c7ae56fc a22e603d
0521b333 3dec0ad4 7d4c2316 3b1eea33 c9a6883d
28ece906 02902f9a d1eb2b8d
f588cb9a 78a069a3 965de133 6036d8d7 6ede9ccd
a1e906ec 88b32a19 38e5353e
6c0032e8 8c003fa6 2fd22a4d b9dda2c2 5fcbb621
876bd678 c8a37109 f074eabe
2b1fac59 a78d0a3b 35af17ae 687a4805 3b9a34e7
24b9e054 063c60a4 9b8d3c09
351bc630 05f69357 833b9197 f875b408 cb71a814
69a1f331 b1eb2b35 0c469443
1455c210 db308bf0 a9805758 a878b82d 38c71426
afffd272 dd6d7564 1cbe4d95
b81c02b2 9b56ec2d 5a913a9f 9b95cafd dfffcf67
94b97ac7 63249009 fa05ca4d
6f13afd0 968f9f41 e492cfe4 e50e15f1 c0f5d13b
5f020301 0001a382 016f3082
016b3013 06092b06 01040182 37140204 061e0400
43004130 0b060355 1d0f0404
03020186 300f0603 551d1301 01ff0405 30030101
ff301d06 03551d0e 04160414
d9adbf08 f23a88f1 14432f79 987cd409 a403e558
30820103 0603551d 1f0481fb
3081f830 81f5a081 f2a081ef 8681b56c 6461703a
2f2f2f43 4e3d4341 312c434e

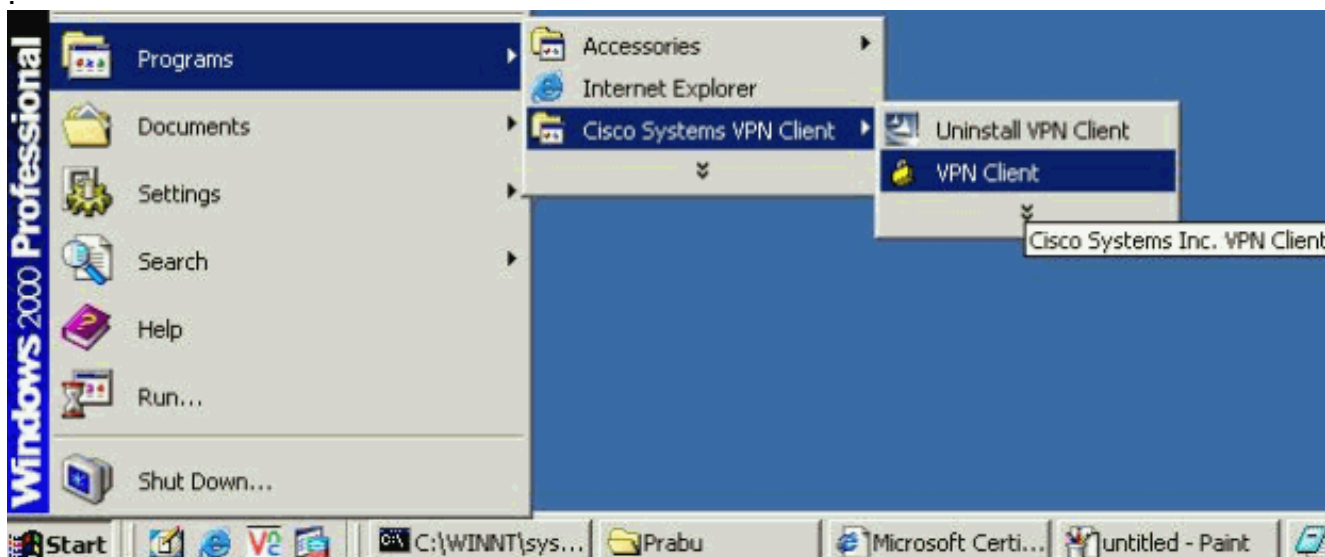
```
3d54532d 57324b33 2d414353 2c434e3d 4344502c
434e3d50 75626c69 63253230
4b657925 32305365 72766963 65732c43 4e3d5365
72766963 65732c43 4e3d436f
6e666967 75726174 696f6e2c 44433d54 53576562
2c44433d 63697363 6f2c4443
3d636f6d 3f636572 74696669 63617465 5265766f
63617469 6f6e4c69 73743f62
6173653f 6f626a65 6374436c 6173733d 63524c44
69737472 69627574 696f6e50
6f696e74 86356874 74703a2f 2f74732d 77326b33
2d616373 2e747377 65622e63
6973636f 2e636f6d 2f436572 74456e72 6f6c6c2f
4341312e 63726c30 1006092b
06010401 82371501 04030201 00300d06 092a8648
86f70d01 01050500 03820101
001abc5a 40b32112 22da80fb bb228bfe 4bf8a515
df8fc3a0 4e0c89c6 d725e2ab
2fa67ce8 9196d516 dfe55627 953aea47 2e871289
6b754e9c 1e01d408 3f7f0595
8081f986 526fbe1c c9639d6f 258b2205 0dc370c6
5431b034 fe9fd60e 93a6e71b
ab8e7f84 a011336b 37c13261 5ad218a3 a513e382
e4bfb2b4 9bf0d7d1 99865cc4
94e5547c f03e3d3e 3b766011 e94a3657 6cc35b92
860152d4 f06b2b15 df306433
c1bcc282 80558d70 d22d72e7 eed3195b d575dceb
c0caa196 34f693ea f3beee4d
aa2ef1c2 edba288f 3a678ecb 3809d0df b1699c76
13018f9f 5e3dce95 efe6da93
f4cb3b00 102efa94 48a22fc4 7e342031 2406165e
39edc207 eddc6554 3fa9f396 ad
quit
crypto isakmp enable outside
crypto isakmp policy 65535
authentication rsa-sig
encryption 3des
hash md5
group 2
lifetime 86400
crypto isakmp identity auto
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
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
group-policy defaultgroup internal
group-policy defaultgroup attributes
  default-domain value cisco.com
username vpnuser password TXttW.eFqbHusJQM encrypted
username vpnuser attributes
  memberof DefaultRAGroup
tunnel-group DefaultRAGroup general-attributes
  address-pool vpnpool
tunnel-group DefaultRAGroup ipsec-attributes
  trust-point CA1
prompt hostname context
Cryptochecksum:dd6f2e3390bf5238815391c13e42cd21
: end
CiscoASA#
```

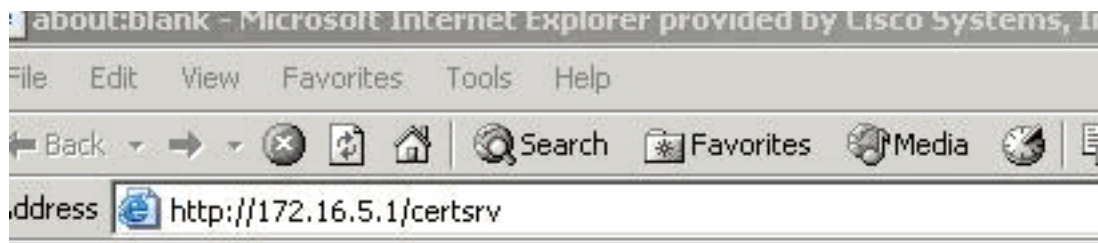
VPN 클라이언트 컨피그레이션

VPN 클라이언트를 구성하려면 다음 단계를 완료합니다.

1. VPN 클라이언트 소프트웨어를 실행하려면 Start(시작) > Programs(프로그램) > Cisco Systems VPN Client(Cisco Systems VPN 클라이언트) > VPN Client(VPN 클라이언트)를 선택합니다



2. CA1이라는 CA 서버에서 CA 인증서를 다운로드하고 Cisco VPN 클라이언트에 설치하려면 다음 단계를 완료합니다.vpnuser에 제공된 자격 증명의 도움을 받아 CA 서버 172.16.5.1에 웹 로그인을 수행합니다



Enter Network Password

Please type your user name and password.

Site: 172.16.5.1

User Name: vpnuser

Password: xxxxxxxx

Domain: [Empty]

Save this password in your password list

OK Cancel

참고: CA 서버가 있는 VPN 클라이언트 사용자에게 대한 사용자 계정이 있는지 확인하십시오. **Download a CA certificate, certificate chain or CRL**(CA 인증서, 인증서 체인 또는 CRL 다운로드)을 클릭하여 창을 엽니다(그림 참조). 인코딩 방법으로 **Base 64** 라디오 버튼을 클릭하고 **CA 인증서 다운로드**를 클릭합니다

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA cert](#)

To download a CA certificate, certificate chain, or CRL, select the certificate

CA certificate:

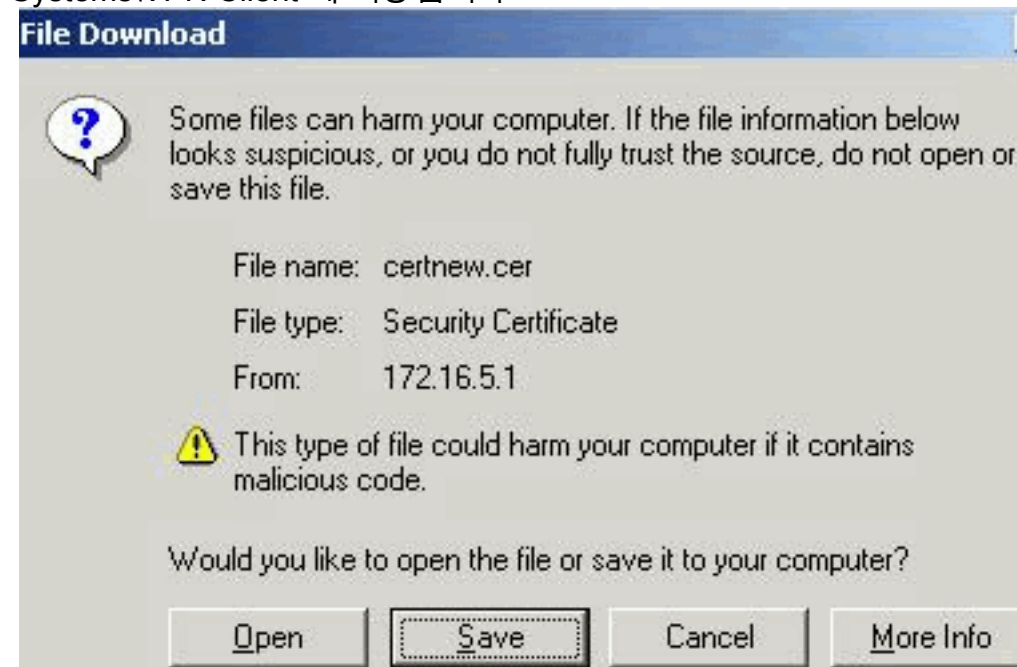


Encoding method:

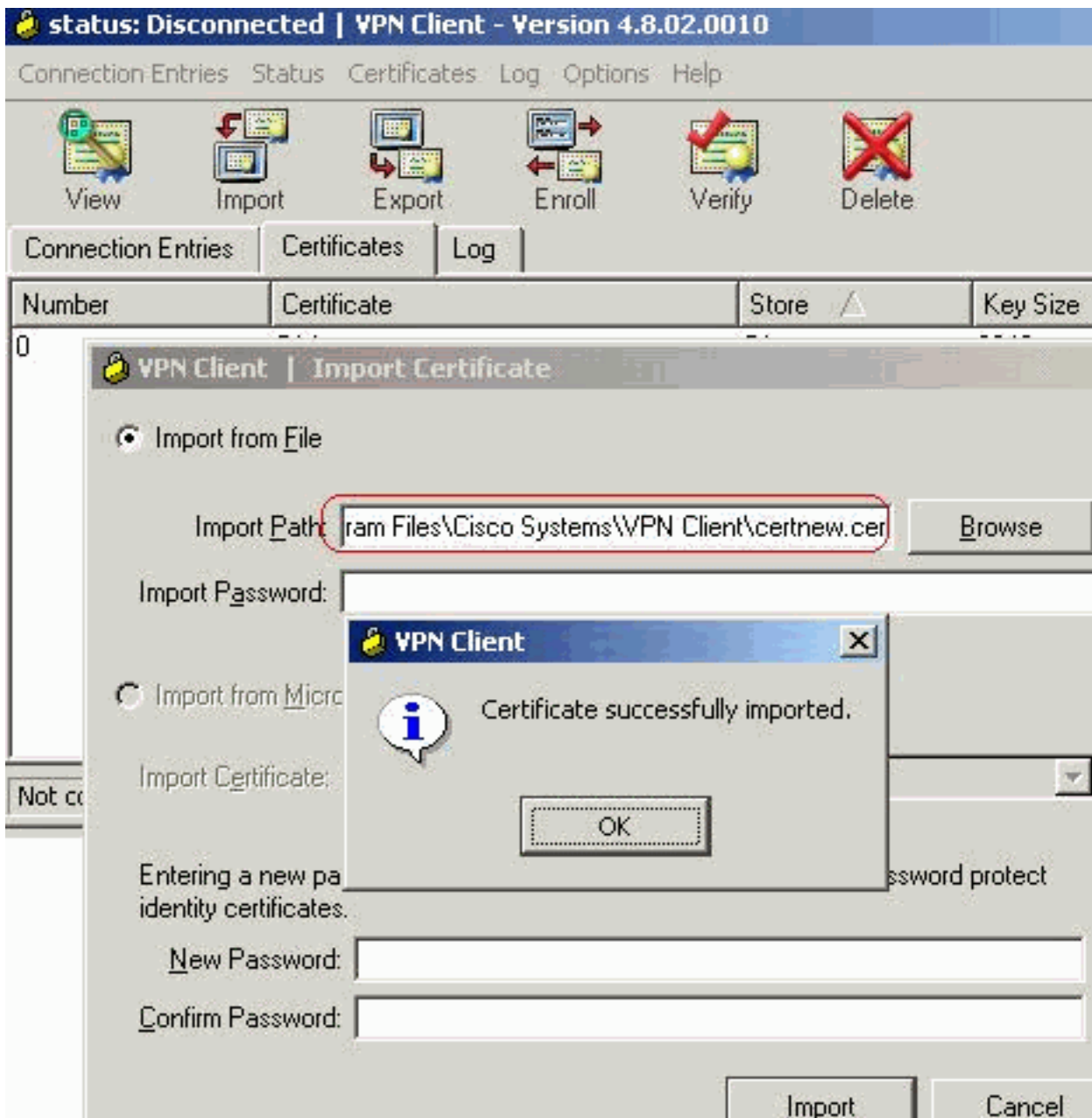
- DER
- Base 64

- [Download CA certificate](#)
- [Download CA certificate chain](#)
- [Download latest base CRL](#)
- [Download latest delta CRL](#)

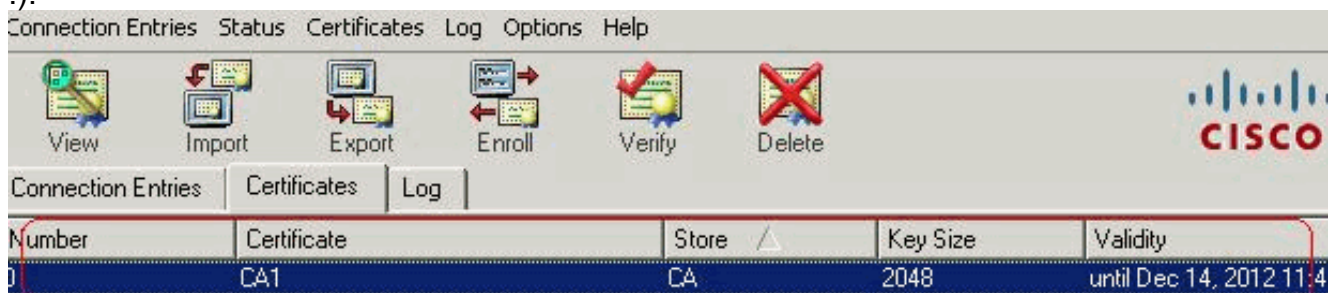
컴퓨터에 certnew.cer 이름으로 CA 인증서를 저장합니다.기본적으로 C:\Program Files\Cisco Systems\VPN Client 에 저장됩니다



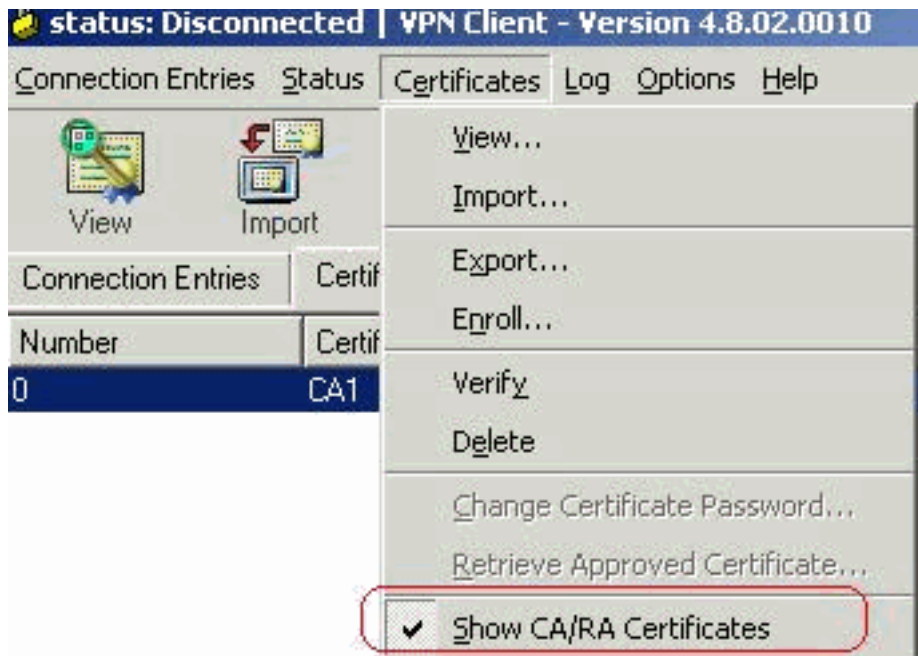
VPN 클라이언트에서 Certificates(인증서) 탭 > Import(가져오기)를 선택하고 Import from Fileradio(파일에서 가져오기) 버튼을 클릭합니다.Browse(찾아보기)를 클릭하여 저장된 위치 C:\Program Files\Cisco Systems\VPN Client에서 CA 인증서 가져옵니다.가져오기를 클릭합니다.표시된 대로 성공 창이 나타납니다



ificates(인증서) 탭에서 CA Certificates CA1이 나타납니다(예
:).



참고: Show CA/RA Certificates(CA/RA 인증서 표시) 옵션이 선택되어 있는지 확인합니다. 그렇지 않으면 CA 인증서가 인증서 창에 표시되지 않아야 합니다



3. ID 인증서를 다운로드하고 VPN 클라이언트에 설치하려면 다음 단계를 완료합니다. CA 서버 CA1에서 Request a Certificate(인증서 요청) > advanced certificate request(고급 인증서 요청) > Create and submit a request to this CA to enroll for the identity certificate(ID 인증서에 등록하기 위해 요청을 생성하고 이 CA에 제출합니다. Submit(제출)을 클릭합니다

Certificate Template:

User ▼

Key Options:

Create new key set Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0 ▼

Key Usage: Exchange

Key Size: 1024 Min: 384 Max: 16384 (common key sizes: [512](#) [1024](#) [2048](#) [4096](#) [8192](#) [16384](#))

Automatic key container name User specified key container name

Mark keys as exportable

Export keys to file

Enable strong private key protection

Store certificate in the local computer certificate store

Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

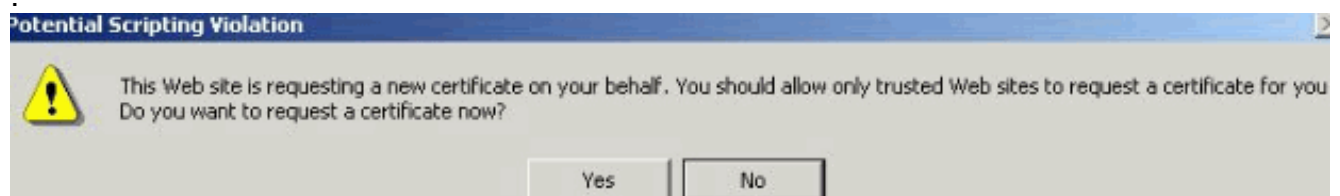
Request Format: CMC PKCS10

Hash Algorithm: MD5 ▼

Only used to sign request.

Save request to a file

계속하려면 [예](#)를 클릭합니다



Install this Certificate를 클릭합니다

Microsoft Certificate Services -- CA1

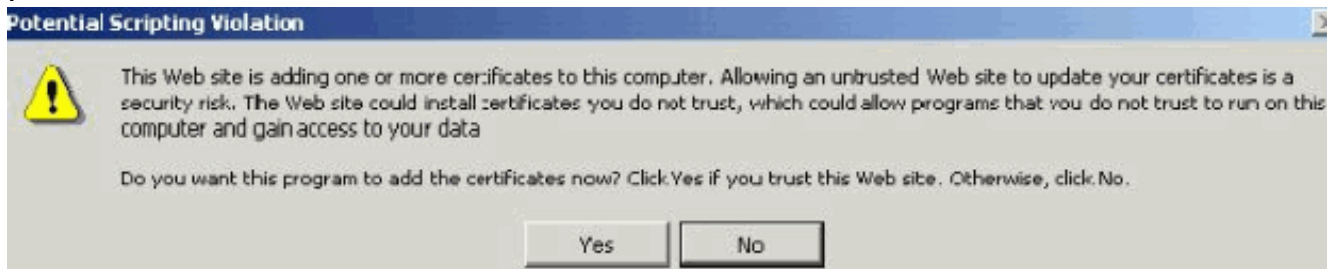
Certificate Issued

The certificate you requested was issued to you.



[Install this certificate](#)

계속하려면 [예](#)를 클릭합니다



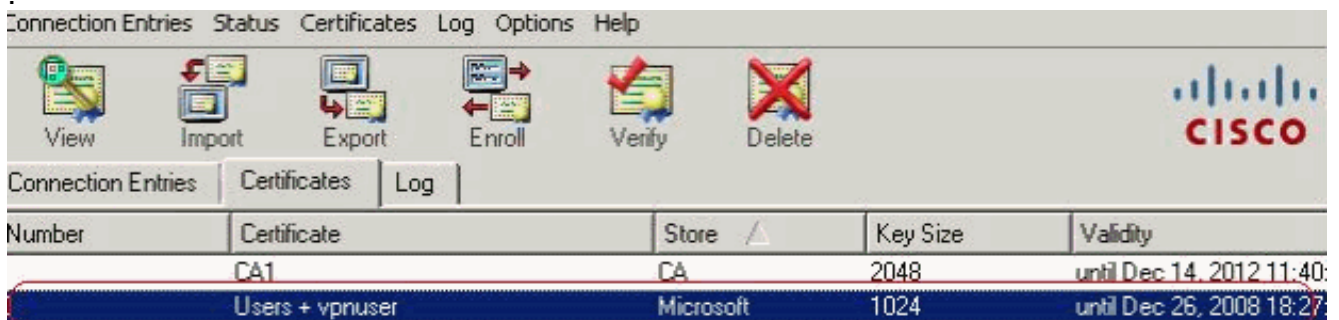
표시된 대로 인증서 설치 메시지를 받아야 합니다

Microsoft Certificate Services -- CA1

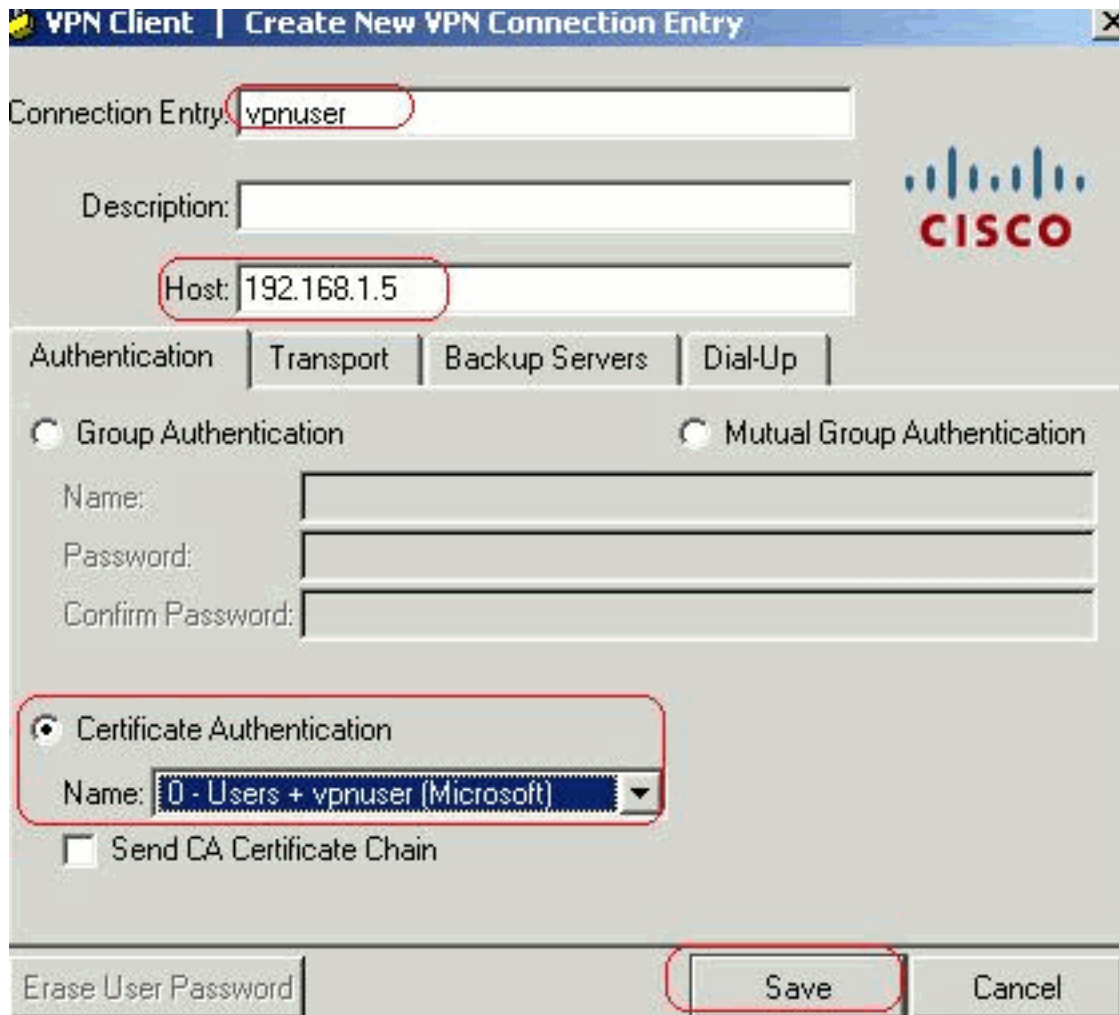
Certificate Installed

Your new certificate has been successfully installed.

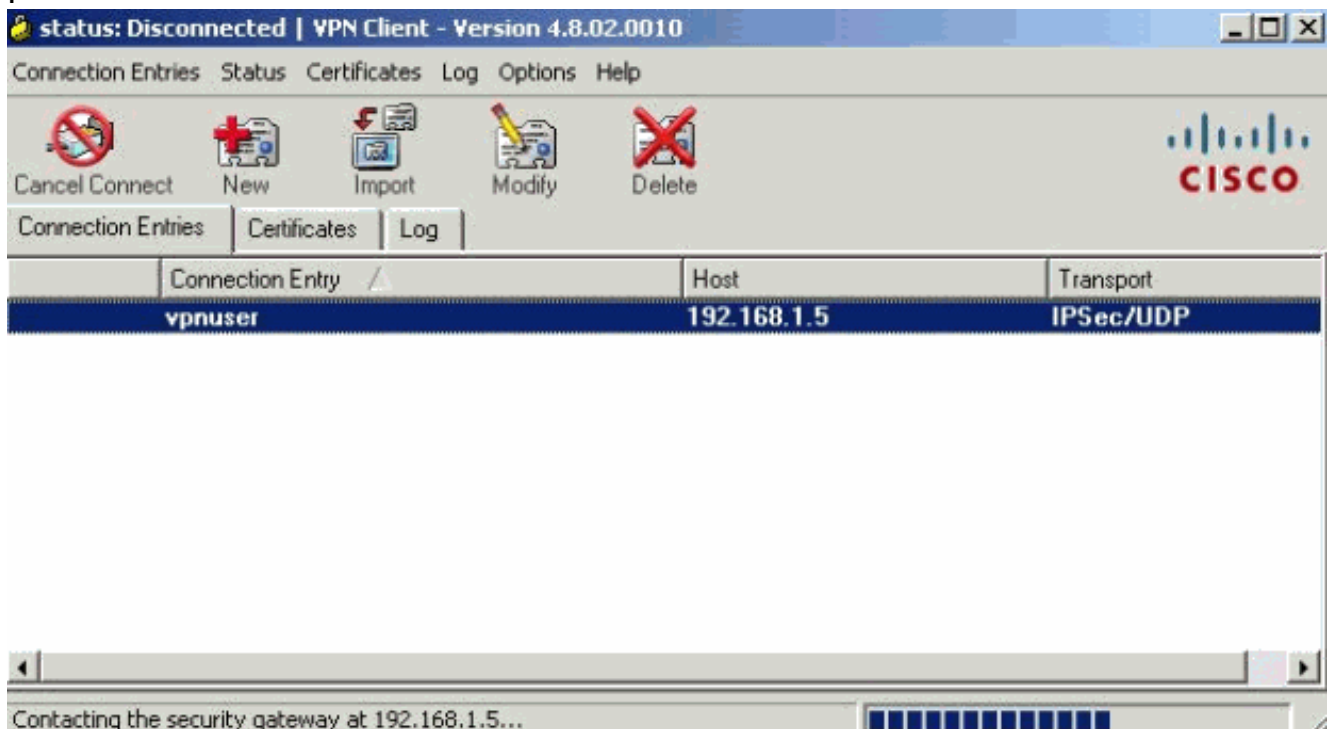
표시된 대로 VPN 클라이언트의 인증서 탭에 설치된 ID 인증서가 나타나도록 하려면 VPN 클라이언트를 종료하고 다시 시작합니다



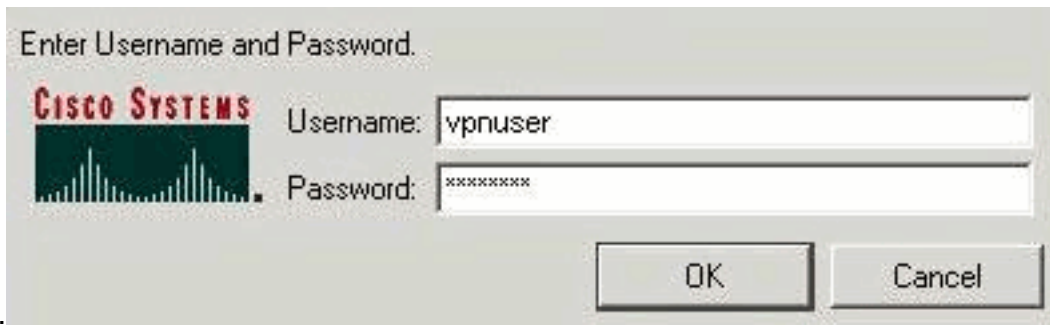
- 연결 항목 탭에서 새로 만들기를 클릭하여 연결 항목 vpnuser를 생성합니다. Host 필드에 원격 피어 IP 주소(라우팅 가능)를 입력합니다. Certificate Authentication(인증서 인증) 라디오 버튼을 클릭하고 표시된 대로 드롭다운 목록에서 ID 인증서를 선택합니다. 저장을 클릭합니다



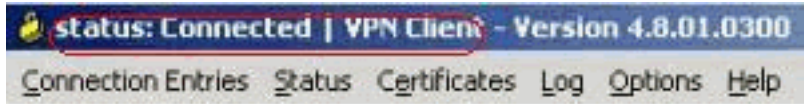
5. 연결을 클릭합니다



6. 프롬프트가 표시되면 xauth에 대한 사용자 이름 및 비밀번호 정보를 입력하고 OK를 클릭하여 원격 네트워크에 연결합니다



7. 표시된 대로 VPN 클라이언트는 ASA에 연결됩니다



다음을 확인합니다.

ASA에서 인증서의 상태를 확인하기 위해 명령줄에서 여러 show 명령을 실행할 수 있습니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

- **show crypto ca trustpoint** 명령은 구성된 신뢰 지점을 표시합니다.

```
CiscoASA#show crypto ca trustpoints
```

```
Trustpoint CA1:
```

```
Subject Name:
```

```
cn=CA1
```

```
dc=TSWeb
```

```
dc=cisco
```

```
dc=com
```

```
Serial Number: 7099f1994764e09c4651da80a16b749c
```

```
Certificate configured.
```

- **show crypto ca certificate** 명령은 시스템에 설치된 모든 인증서를 표시합니다.

```
CiscoASA# show crypto ca certificate
```

```
Certificate
```

```
Status: Available
```

```
Certificate Serial Number: 3f14b70b00000000001f
```

```
Certificate Usage: Encryption
```

```
Public Key Type: RSA (1024 bits)
```

```
Issuer Name:
```

```
cn=CA1
```

```
dc=TSWeb
```

```
dc=cisco
```

```
dc=com
```

```
Subject Name:
```

```
cn=vpnserver
```

```
cn=Users
```

```
dc=TSWeb
```

```
dc=cisco
```

```
dc=com
```

```
PrincipalName: vpnserver@TSWeb.cisco.com
```

```
CRL Distribution Points:
```

```
[1] ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services,
```

```
CN=Services,CN=Configuration,DC=TSWeb,DC=cisco,
```

```
DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
```

```
[2] http://ts-w2k3-acs.tsweb.cisco.com/CertEnroll/CA1.crl
```

```
Validity Date:
```

```
start date: 14:00:36 UTC Dec 27 2007
```

```
end date: 14:00:36 UTC Dec 26 2008
```

```
Associated Trustpoints: CA1
```

CA Certificate

Status: Available
Certificate Serial Number: 7099f1994764e09c4651da80a16b749c
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Issuer Name:
 cn=CA1
 dc=TSWeb
 dc=cisco
 dc=com
Subject Name:
 cn=CA1
 dc=TSWeb
 dc=cisco
 dc=com
CRL Distribution Points:
 [1] ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services,
 CN=Services,CN=Configuration,DC=TSWeb,DC=cisco,
 DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
 [2] http://ts-w2k3-acs.tsweb.cisco.com/CertEnroll/CA1.crl
Validity Date:
 start date: 06:01:43 UTC Dec 14 2007
 end date: 06:10:15 UTC Dec 14 2012
Associated Trustpoints: CA1

Certificate

Subject Name:
 Name: CiscoASA.cisco.com
Status: Pending terminal enrollment
Key Usage: General Purpose
Fingerprint: 1a022cf2 9771e335 12c3a530 1f9a0345
Associated Trustpoint: CA1

- **show crypto ca crls** 명령은 캐시된 CRL(certificate revocation list)을 표시합니다.
- **show crypto key mypubkey rsa** 명령은 생성된 모든 암호화 키 쌍을 표시합니다.

```
CiscoASA# show crypto key mypubkey rsa
Key pair was generated at: 01:43:45 UTC Dec 11 2007
Key name: <Default-RSA-Key>
Usage: General Purpose Key
Modulus Size (bits): 1024
Key Data:

30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00d4a509
99e95d6c b5bdaa25 777aebbe 6ee42c86 23c49f9a bea53224 0234b843 1c0c8541
f5a66eb1 6d337c70 29031b76 e58c3c6f 36229b14 fefd3298 69f9123c 37f6c43b
4f8384c4 a736426d 45765cca 7f04cba1 29a95890 84d2c5d4 adeeb248 a10b1f68
2fe4b9b1 5fa12d0e 7789ce45 55190e79 1364aba4 7b2b21ca de3af74d b7020301 0001
Key pair was generated at: 06:36:00 UTC Dec 15 2007
Key name: my.CA.key
Usage: General Purpose Key
Modulus Size (bits): 1024
Key Data:

30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00b8e20a
a8332356 b75b6600 735008d3 735d23c5 295b9247 2b5e02a8 1f63dc7a 570667d7
545e7f98 d3d4239b 42ab8faf 0be8a5d3 94f80d01 a14cc01d 98b1320e 9fe84905
5ab94b18 ef308eb1 2f22ab1a 8edb38f0 2c2cf78e 07197f2d 52d3cb73 91a9ccb2
d903f722 bd414b0a 3205aa05 3ec45e24 6480606f 8e417f09 a7aa9c64 4d020301 0001
Key pair was generated at: 07:35:18 UTC Dec 21 2007
CiscoASA#
```

- **show crypto isakmp sa** 명령은 IKE 1 터널 정보를 표시합니다.

```
CiscoASA#show crypto isakmp sa
```



```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
```

```
1 IKE Peer: 10.1.1.5
Type      : user          Role      : responder
Rekey     : no           State     : MM_ACTIVE
```

- **show crypto ipsec sa 명령은 IPsec 터널 정보를 표시합니다.**

```
CiscoASA#show crypto ipsec sa
interface: outside
Crypto map tag: dynmap, seq num: 10, local addr: 192.168.1.5

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.5.5.10/255.255.255.255/0/0)
current_peer: 10.1.1.5, username: vpnuser
dynamic allocated peer ip: 10.5.5.10

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 144, #pkts decrypt: 144, #pkts verify: 144
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.1.5, remote crypto endpt.: 10.1.1.5

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: FF3EEE7D

inbound esp sas:
spi: 0xEFDF8BA9 (4024404905)
transform: esp-3des esp-md5-hmac none
in use settings = {RA, Tunnel, }
slot: 0, conn_id: 4096, crypto-map: dynmap
sa timing: remaining key lifetime (sec): 28314
IV size: 8 bytes
replay detection support: Y
outbound esp sas:
spi: 0xFF3EEE7D (4282314365)
transform: esp-3des esp-md5-hmac none
in use settings = {RA, Tunnel, }
slot: 0, conn_id: 4096, crypto-map: dynmap
sa timing: remaining key lifetime (sec): 28314
IV size: 8 bytes
replay detection support: Y
```

Output [Interpreter 도구\(등록된 고객만 해당\)](#)(OIT)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 OIT를 사용합니다.

문제 해결

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

다음과 같은 몇 가지 오류가 발생할 수 있습니다.

- **오류: 가져온 인증서를 구문 분석하거나 확인하지 못했습니다.** 이 오류는 ID 인증서를 설치하고 관련 신뢰 지점으로 인증된 올바른 중간 또는 루트 CA 인증서가 없을 때 발생할 수 있습니다. 올바른 중간 또는 루트 CA 인증서를 제거하고 다시 인증해야 합니다. 올바른 CA 인증서를 받았는

지 확인하려면 타사 공급업체에 문의하십시오.

- **인증서에 범용 공개 키가 없습니다.** 이 오류는 ID 인증서를 잘못된 신뢰 지점에 설치하려고 할 때 발생할 수 있습니다. 잘못된 ID 인증서를 설치하려고 시도했거나, 신뢰 지점과 연결된 키 쌍이 ID 인증서에 포함된 공개 키와 일치하지 않습니다. ID 인증서를 올바른 신뢰 지점에 설치했는지 확인하기 위해 `show crypto ca certificates trustpointname` 명령을 실행합니다. 연결된 신뢰 지점을 나타내는 줄을 찾습니다. 잘못된 신뢰 지점이 나열된 경우 해당 신뢰 지점을 제거하고 다시 설치하려면 이 문서에 설명된 절차를 사용하십시오. 또한 CSR이 생성된 후 키 쌍이 변경되지 않았는지 확인합니다.
- **오류:ASA/PIX.Sev=경고/3 IKE/0xE300081 잘못된 원격 인증서 ID:**인증서에 인증 문제가 있는 경우 이 오류 메시지가 VPN 클라이언트에 나타날 수 있습니다.문제를 해결하려면 ASA/PIX 컨피그레이션에서 `crypto isakmp identity auto` 명령을 사용합니다.

관련 정보

- [Cisco Adaptive Security Appliance 지원 페이지](#)
- [Cisco VPN 클라이언트 지원 페이지](#)
- [Microsoft 서버를 CA\(Certificate Authority\)로 구성](#)
- [기술 지원 및 문서 - Cisco Systems](#)