ASA 구성: SSL 디지털 인증서 설치 및 갱신

목차

소개

이 문서에서는 클라이언트리스 SSLVPN 및 AnyConnect 연결을 위해 ASA에 신뢰할 수 있는 서드 파티 SSL 디지털 인증서를 설치하는 방법에 대해 설명합니다.

배경 정보

이 예에서는 GoDaddy 인증서가 사용됩니다. 각 단계에는 ASDM(Adaptive Security Device Manager) 절차 및 이에 상응하는 CLI가 포함되어 있습니다.

사전 요구 사항

요구 사항

이 문서에서는 인증서 등록을 위해 신뢰할 수 있는 서드파티 CA(Certificate Authority)에 액세스해야 합니다. 서드파티 CA 벤더의 예로는 Baltimore, Cisco, Entrust, Geotrust, G, Microsoft, RSA, Thawte, VeriSign 등이 있습니다.

시작하기 전에 ASA에 올바른 클록 시간, 날짜 및 표준 시간대가 있는지 확인합니다. 인증서 인증에서는 NTP(Network Time Protocol) 서버를 사용하여 ASA의 시간을 동기화하는 것이 좋습니다. Cisco ASA Series General Operations CLI 컨피그레이션 가이드 9.1에서는 ASA에서 시간과 날짜를 올바르게 설정하기 위해 수행해야 할 단계에 대해 자세히 설명합니다.

사용되는 구성 요소

이 문서에서는 소프트웨어 버전 9.4.1 및 ASDM 버전 7.4(1)을 실행하는 ASA 5500-X를 사용합니다.

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

구성

SSL 프로토콜은 SSL 서버가 클라이언트에 서버 인증을 수행하기 위한 서버 인증서를 제공하도록 요구합니다. Cisco에서는 사용자가 실수로 비인가 서버의 인증서를 신뢰하도록 브라우저를 구성할 수 있기 때문에 자체 서명 인증서의 사용을 권장하지 않습니다. 사용자가 보안 게이트웨이에 연결할 때 보안 경고에 대응해야 하는 불편도 있다. 이를 위해 신뢰할 수 있는 서드파티 CA를 사용하여 ASA에 SSL 인증서를 발급하는 것이 좋습니다.

ASA에서 서드파티 인증서의 라이프사이클은 기본적으로 다음 단계를 통해 이루어집니다.

CSR 생성

CSR 생성은 모든 X.509 디지털 인증서의 수명 주기 중 첫 번째 단계입니다.

프라이빗/퍼블릭 RSA(Rivest-Shamir-Adleman) 또는 ECDSA(Elliptic Curve Digital Signature Algorithm) 키 쌍이 생성되면(부록 A에서는 RSA 또는 ECDSA 사용 간의 차이점을 자세히 설명) CSR(Certificate Signing Request)이 생성됩니다.

CSR은 요청을 전송하는 호스트의 공개 키 및 ID 정보를 포함하는 PKCS10 형식의 메시지입니다. PKI 데이터 형식 - ASA 및 Cisco IOS에 적용할 수 있는 다양한 인증서 형식에 대해 설명합니다®.

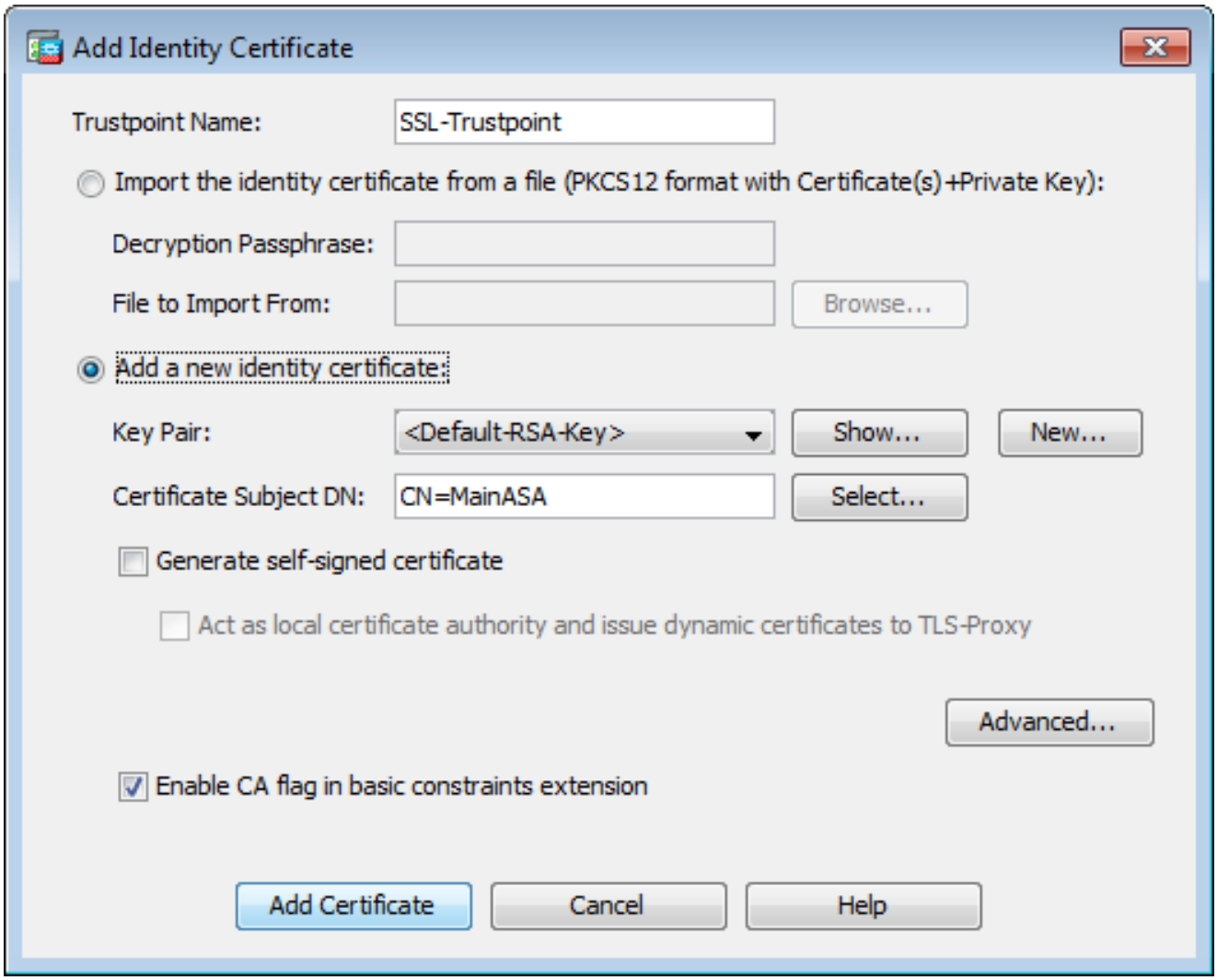
참고:
1. 필요한 키 쌍 크기에 대해 CA에 확인합니다. CA/Browser Forum에서는 구성원 CA가 생성한 모든 인증서의 최소 크기를 2048비트로 설정해야 합니다.
2. ASA는 현재 SSL 서버 인증에 4096비트 키(Cisco 버그 ID CSCut53512)를 지원하지 않습니다. 그러나 IKEv2에서는 ASA 5580, 5585 및 5500-X 플랫폼에서만 4096비트 서버 인증서를 사용할 수 있습니다.
3. 신뢰할 수 없는 인증서 경고를 방지하고 엄격한 인증서 검사를 통과하려면 CSR의 FQDN 필드에 ASA의 DNS 이름을 사용합니다.

CSR을 생성하는 방법에는 세 가지가 있습니다.

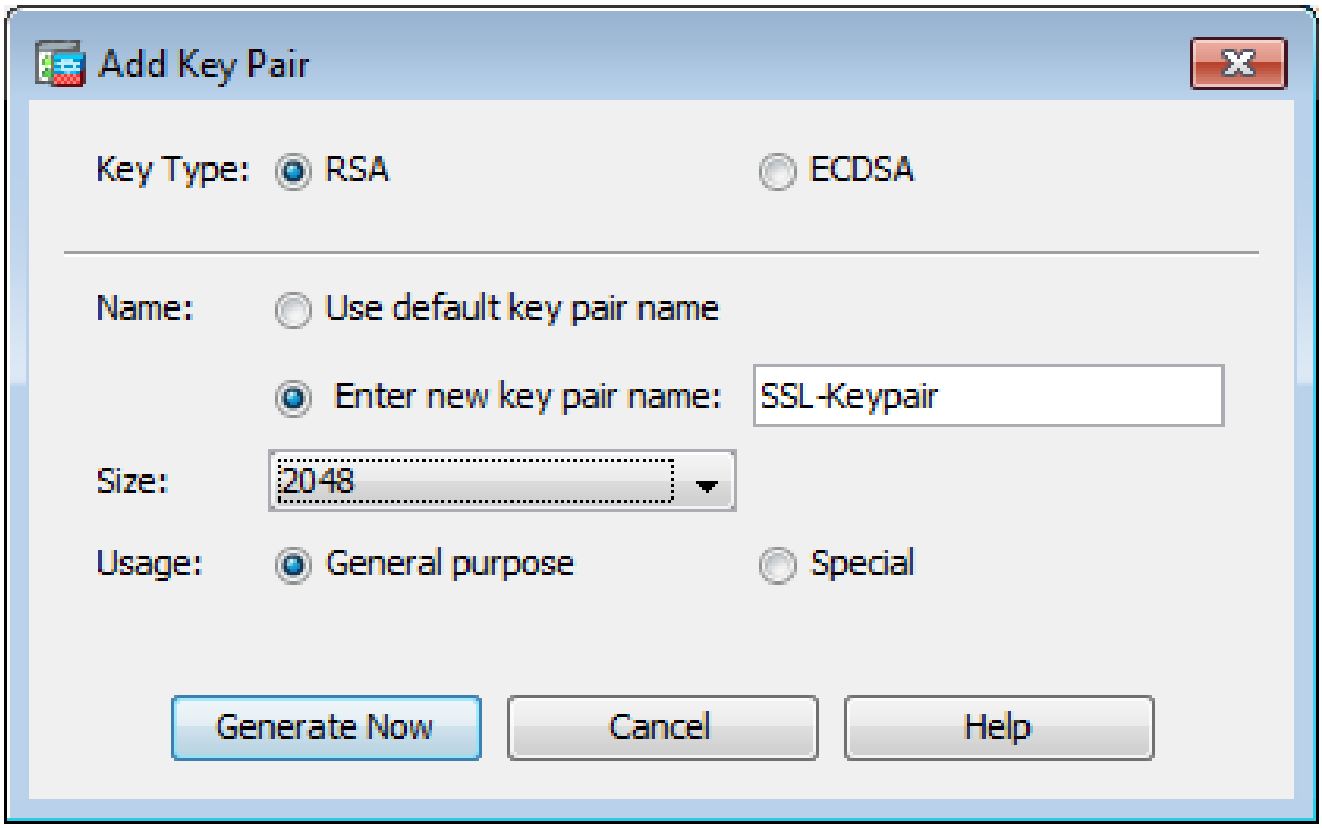
- ASDM으로 구성
- ASA CLI로 구성
- OpenSSL을 사용하여 CSR 생성

1. ASDM으로 구성

1. 로 이동하여 **Configuration** > **Remote Access VPN** > **Certificate Management**을 선택합니다**Identity Certificates.**
2. 를 **Add**클릭합니다.



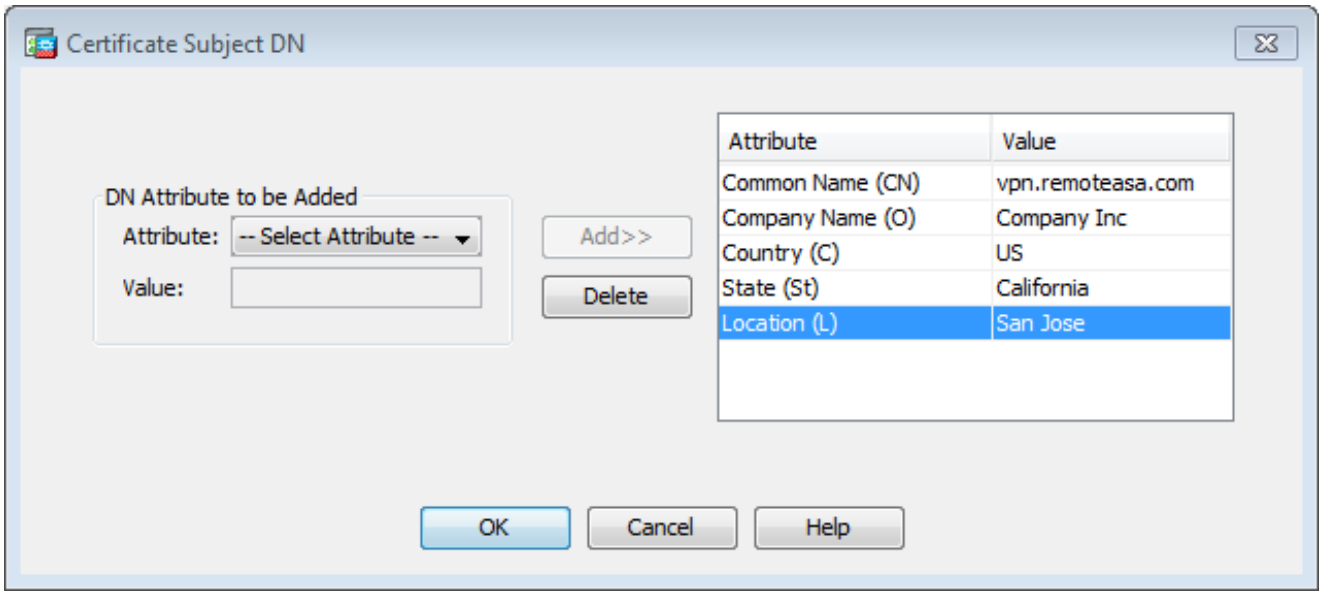
3. 신뢰 지점 이름 입력 필드에 신뢰 지점 이름을 정의합니다.
4. 오디오**Add a new identity certificate**버튼을 클릭합니다.
5. Key Pair(키 쌍)에서 를 클릭합니다**New.**



6. 키 유형(RSA 또는 ECDSA)을 선택합니다. 차이점을 이해하려면 부록 A를 참조하십시오.
7. 오디오**Enter new key pair name**버튼을 클릭합니다. 인식을 위해 키 쌍 이름을 식별합니다.
8. 를**Key Size**선택합니다. RSA를 선택합니다**General Purpose for Usage .**
9. 를 클릭합니다**Generate Now.** 키 쌍이 생성됩니다.
10. Certificate Subject DN(인증서 주체 DN)을 정의하려면 을 클릭하고**Select**이 표에 나열된 특성을 구성합니다.

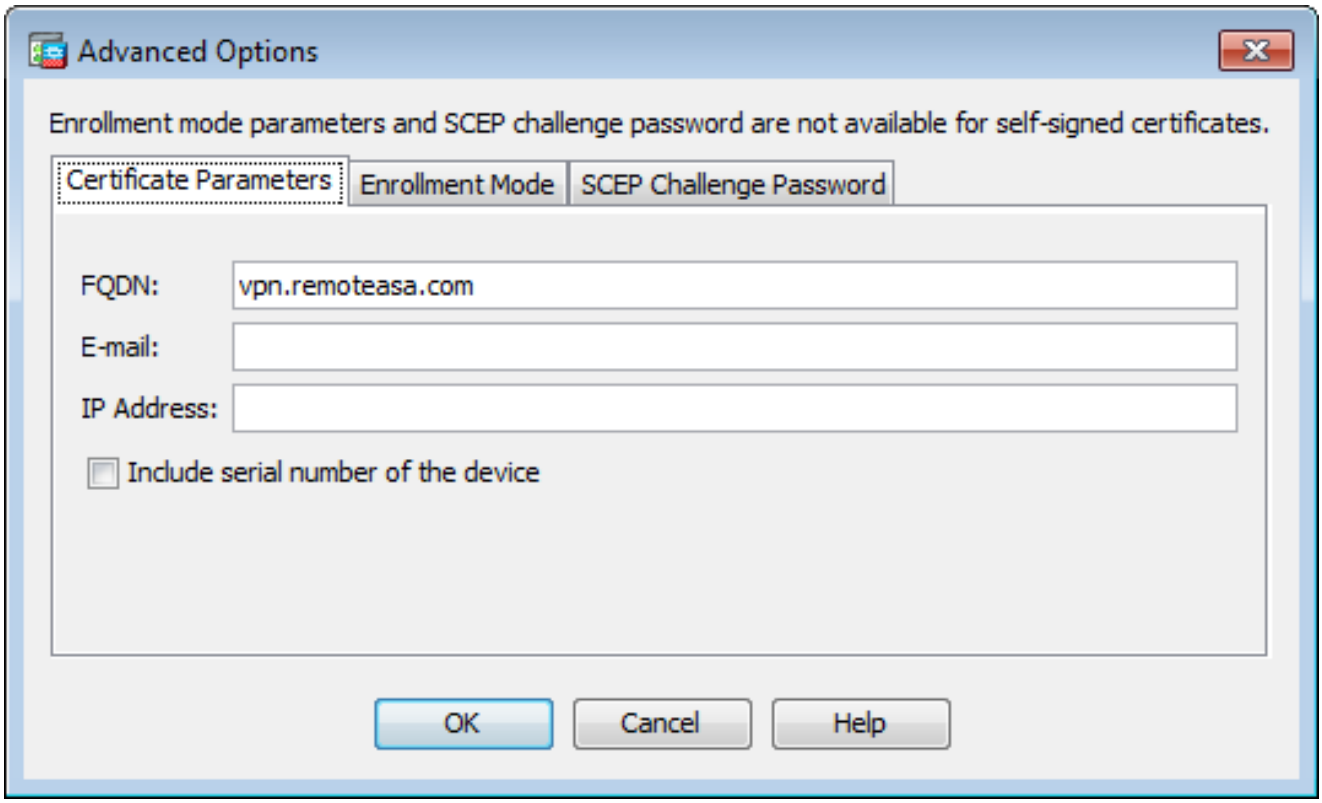
Attribute	Description
CN	FQDN (Full Qualified Domain Name) that will be used for connections to your firewall. For example, webvpn.cisco.com
OU	Department Name
O	Company Name (Avoid using Special Characters)
C	Country Code (2 Letter Code without Punctuation)
St	State (Must be spelled out completely. For example, North Carolina)
L	City
EA	Email Address

이러한 값을 구성하려면 Attribute 드롭다운 목록에서 값을 선택하고 값을 입력한 다음 Add를 클릭합니다.



참고: 일부 서드파티 벤더는 ID 인증서가 발급되기 전에 특정 특성을 포함해야 합니다. 필수 특성을 모를 경우 공급업체에 자세한 내용을 확인하십시오.

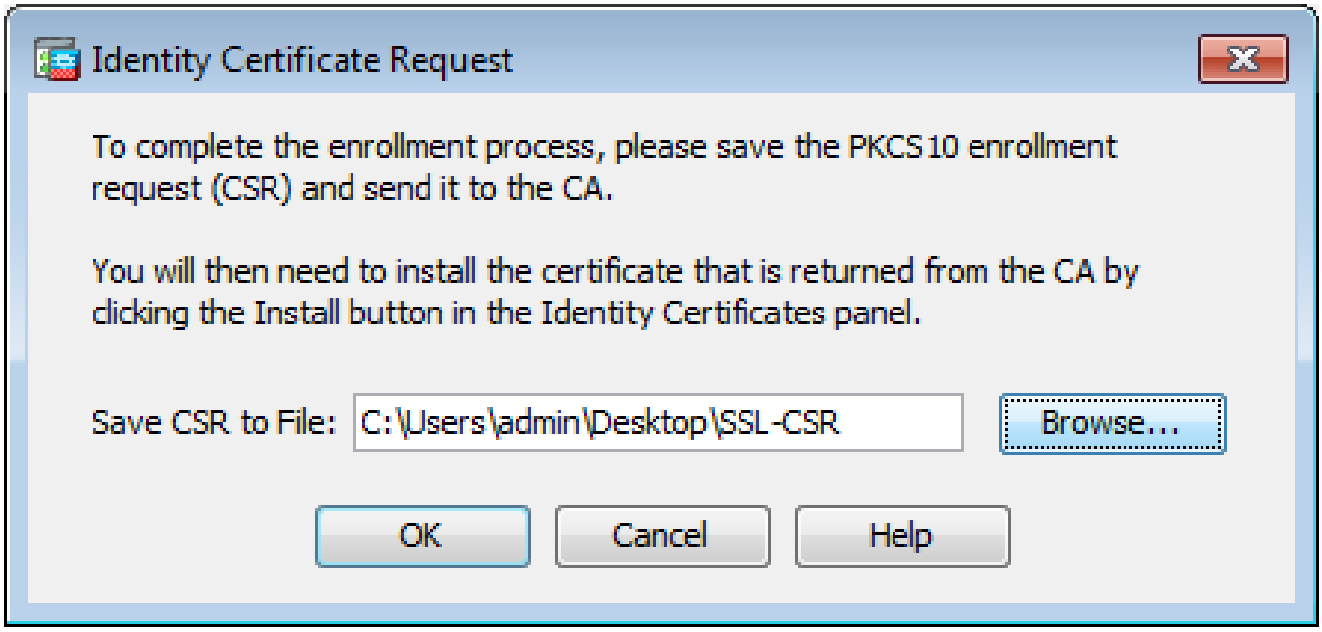
11. 적절한 값을 추가한 후 을 클릭합니다**OK**. Add Identity Certificate 대화 상자가 Certificate와 함께 나타납니다**Subject DN** field populated.
12. Advanced(고급)를 클릭합니다.



13. 필드**FQDN**에 인터넷에서 디바이스에 액세스하는 데 사용되는 FQDN을 입력합니다. 를 클릭합니다**OK**.
14. Enable CA flag in basic constraints extension(기본 제약 조건 확장에서 CA 플래그 활성화) 옵션을 선택한 상태로 둡니다. 이제 CA 플래그가 없는 인증서는 기본적으로 ASA에 CA 인증서로 설치할 수 없습니다. 기본 제약 조건 확장은 인증서의 주체가 CA인지 여부 및 이 인증서를

포함하는 유효한 인증 경로의 최대 깊이를 식별합니다. 이 요구 사항을 우회하는 옵션의 선택을 취소합니다.

15. 로컬OK시스템의 파일에 CSR을 저장하려면 를 클릭한Add Certificate. 다음 프롬프트가 표시됩니다.



16. 를 클릭하고BrowseCSR을 저장할 위치를 선택한 다음 확장자가 .txt인 파일을 저장합니다.

참고: 파일을 .txt 확장자로 저장하면 PKCS#10 요청을 열고 텍스트 편집기(예: 메모장)로 볼 수 있습니다.

2. ASA CLI로 구성

ASDM에서는 CSR이 생성되거나 CA 인증서가 설치되면 신뢰 지점이 자동으로 생성됩니다. CLI에서 신뢰 지점은 수동으로 생성해야 합니다.

```
<#root>

! Generates 2048 bit RSA key pair with label SSL-Keypair.

MainASA(config)#

crypto key generate rsa label SSL-Keypair modulus 2048


INFO: The name for the keys are: SSL-Keypair
Keypair generation process begin. Please wait...

 ! Define trustpoint with attributes to be used on the SSL certificate

MainASA(config)#

crypto ca trustpoint SSL-Trustpoint

MainASA(config-ca-trustpoint)#
```

enrollment terminal

MainASA(config-ca-trustpoint)#

fqdn (remoteasavpn.url)

MainASA(config-ca-trustpoint)#

**subject-name CN=(asa.remotevpn.url),O=Company Inc,C=US,
St=California,L=San Jose**

MainASA(config-ca-trustpoint)#

keypair SSL-Keypair

MainASA(config-ca-trustpoint)#

exit

! Initiates certificate signing request. This is the request to be submitted via Web or Email to the third party vendor.

MainASA(config)#

crypto ca enroll SSL-Trustpoint

WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate is
used for VPN authentication this may cause connection problems.

Would you like to continue with this enrollment? [yes/no]:

yes

% Start certificate enrollment ..
% The subject name in the certificate is: subject-name CN=

(remoteasavpn.url)

,
O=Company Inc,C=US,St=California,L=San Jose

% The fully-qualified domain name in the certificate will be:

(remoteasavpn.url)

,

% Include the device serial number in the subject name? [yes/no]:

no

Display Certificate Request to terminal? [yes/no]:

yes

Certificate Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIDDjCCAfYCAQAwgYkxETAPBgNVBAcTCFNhbiBKb3NlMRMwEQYDVQQIEwpDYWxp
Zm9ybmlhMQswCQYDVQQGEwJVUzEUMBIGA1UEChMLQ29tcGFueSBJbmMxGjAYBgNV
BAMTEXZwbi5yZW1vdGVhc2EuY29tMSAwHgYJKoZIhvcNAQkCFhF2cG4ucmVtb3Rl
YXNhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK62Nhb9ktlK
uR3Q4TmksyuRMqJNrb9kXpvA6H2OOPuBfQvSF4rVnSwKOmu3c8nweEvYcdVWV6Bz
BhjXeovTVi17FlNTceaUTGikeIdXC+mw1iE7eRsynS/d4mzMWJmrvrsDNzpAW/EM
SzTca+BvqF7X2r3LU8Vsv6Oi8ylhco9Fz7bWvRWVtO3NDDbyolC9b/VgXMuBitcc

```
rzfUbVnm7VZDOf4jr9EXgUwXxcQidWEABlFrXrtYpFgBo9aqJmRp2YABQ1ieP4cY
3rBtgRjLcF+S9TvHG5m4v7v755meV4YqsZIXvytIOzVBihemVxaGA1oDwfkoYSFi
4CzXbFvdG6kCAwEAAaA/MD0GCSqGSIb3DQEJDjEwMC4wDgYDVR0PAQH/BAQDAgWg
MBwGA1UdEQQVMBOCEXZwbi5yZW1vdGVhc2EuY29tMA0GCSqGSIb3DQEBBQUAA4IB
AQBZuQzUXGEB0ix1yuPK0ZkRz8bPnwIqLTfxZhagmuyEhrN7N4+aQnCHj85oJane
4ztZDiCCoWTerBS4RSkKEHEspu9oohjCYuNnp5qa91SPrZNEjTWwOeRn+qKbId2J
jE6Qy4vdPCexavMLYVQxCny+gVkzPN/sFRk3EcTTVq6DxxaebpJijmiqa7gCph52
YkHXnFne1LQd41BgoLlCr9+hx74XsTHGBmI1s/9T5oAX26Ym+B2l/i/DP5BktIUA
8GvIY1/ypj9KO49fP5ap8alOqvLtYYcCcfwrCt+OojOrZ1YyJb3dFuMNRedAX37t
DuHNl2EYNpYkjVk1wI53/5w3
-----END CERTIFICATE REQUEST-----

Redisplay enrollment request? [yes/no]:
```

no

```
! Displays the PKCS#10 enrollment request to the terminal. Copy this from the terminal
to a text file to submit to the third party CA.
```

3. OpenSSL을 사용하여 CSR 생성

OpenSSL은 파일**OpenSSL config**을 사용하여 CSR 생성에 사용할 특성을 가져옵니다. 이 프로세스에서는 CSR 및 개인 키를 생성합니다.

⚠ 주의: 생성되는 개인 키가 인증서의 무결성을 손상시키므로 다른 사용자와 공유되지 않는지 확인합니다.

1. 이 프로세스가 실행되는 시스템에 OpenSSL이 설치되어 있는지 확인합니다. Mac OSX 및 GNU/Linux 사용자의 경우 기본적으로 설치됩니다.
2. 기능 디렉터리로 전환합니다.

   Windows의 경우: 기본적으로 유틸리티는에 **C:\Openssl\bin**설치됩니다. 이 위치에서 명령 프롬프트를 엽니다.

   Mac OSX/Linux의 경우: CSR을 생성하는 데 필요한 디렉토리에서 Terminal(터미널) 창을 엽니다.

3. 지정된 특성을 가진 텍스트 편집기를 사용하여 OpenSSL 구성 파일을 생성합니다. 작업이 완료되면 파일을 이전 단계에서 언급한 위치에 openssl.cnf로 저장합니다(버전 0.9.8h 이상인 경우 파일이**openssl.cfg**저장됨)
   <#root>

   [req]

   ```
   default_bits = 2048
   default_keyfile = privatekey.key
   distinguished_name = req_distinguished_name
   req_extensions = req_ext
   ```

   [req_distinguished_name]

```
commonName = Common Name (eg, YOUR name)
commonName_default = (asa.remotevpn.url)

countryName = Country Name (2 letter code)
countryName_default = US

stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = California

localityName = Locality Name (eg, city)
localityName_default = San Jose

O.organizationName = Organization Name (eg, company)
O.organizationName_default = Company Inc


[req_ext]

subjectAltName = @alt_names


[alt_names]

DNS.1 = *.remoteasa.com
```

4. 다음 명령을 사용하여 CSR 및 개인 키를 생성합니다.

openssl req -new -nodes -out CSR.csr -config openssl.cnf

<#root>

```
 # Sample CSR Generation:


openssl req -new -nodes -out CSR.csr -config openssl.cnf


Generate a 2048 bit RSA private key
.....................................................................................+++
.....................................+++
writing new private key to 'privatekey.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg, YOUR name) [(asa.remotevpn.url)]:
Country Name (2 letter code) [US]:
State or Province Name (full name) [California]:
Locality Name (eg, city) [San Jose]:
Organization Name (eg, company) [Company Inc]:
```

저장된 CSR을 서드파티 CA 벤더에 제출합니다. 인증서가 발행되면 CA는 ASA에 설치할 ID

인증서 및 CA 인증서를 제공합니다.

CA의 SSL 인증서 생성

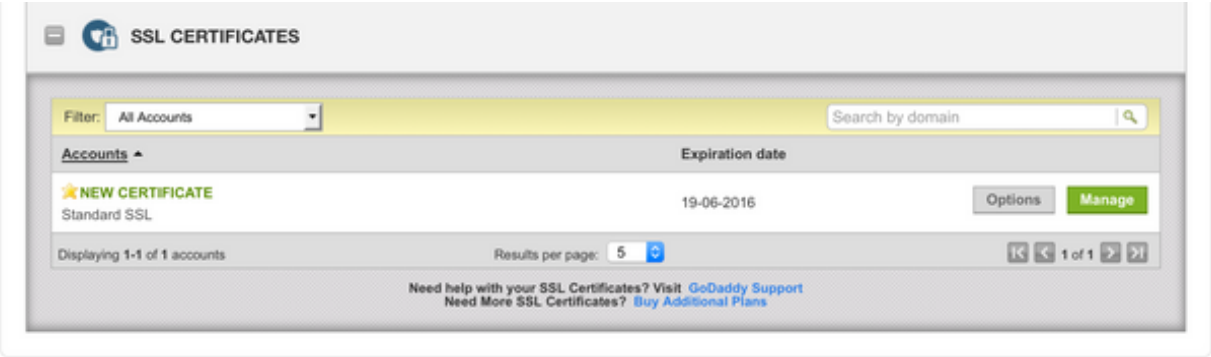
다음 단계는 CA에서 CSR에 서명을 받는 것입니다. CA는 새로 생성된 PEM 인코딩 ID 인증서를 제공하거나 CA 인증서 번들과 함께 PKCS12 인증서를 제공합니다.

CSR이 OpenSSL을 통해 또는 CA 자체에서 ASA 외부에서 생성되는 경우, 개인 키 및 CA 인증서가 포함된 PEM 인코딩 ID 인증서를 별도의 파일로 사용할 수 있습니다. 부록 B에서는 이러한 요소를 단일 PKCS12 파일(.p12 또는 .pfx 형식)로 함께 번들로 구성하는 단계를 제공합니다.

이 문서에서는 ASA에 ID 인증서를 발급하는 예로 GoDaddy CA를 사용합니다. 이 프로세스는 다른 CA 공급업체마다 다릅니다.계속하기 전에 CA 설명서를 주의 깊게 읽어보십시오.

GoDaddy CA의 SSL 인증서 생성 예

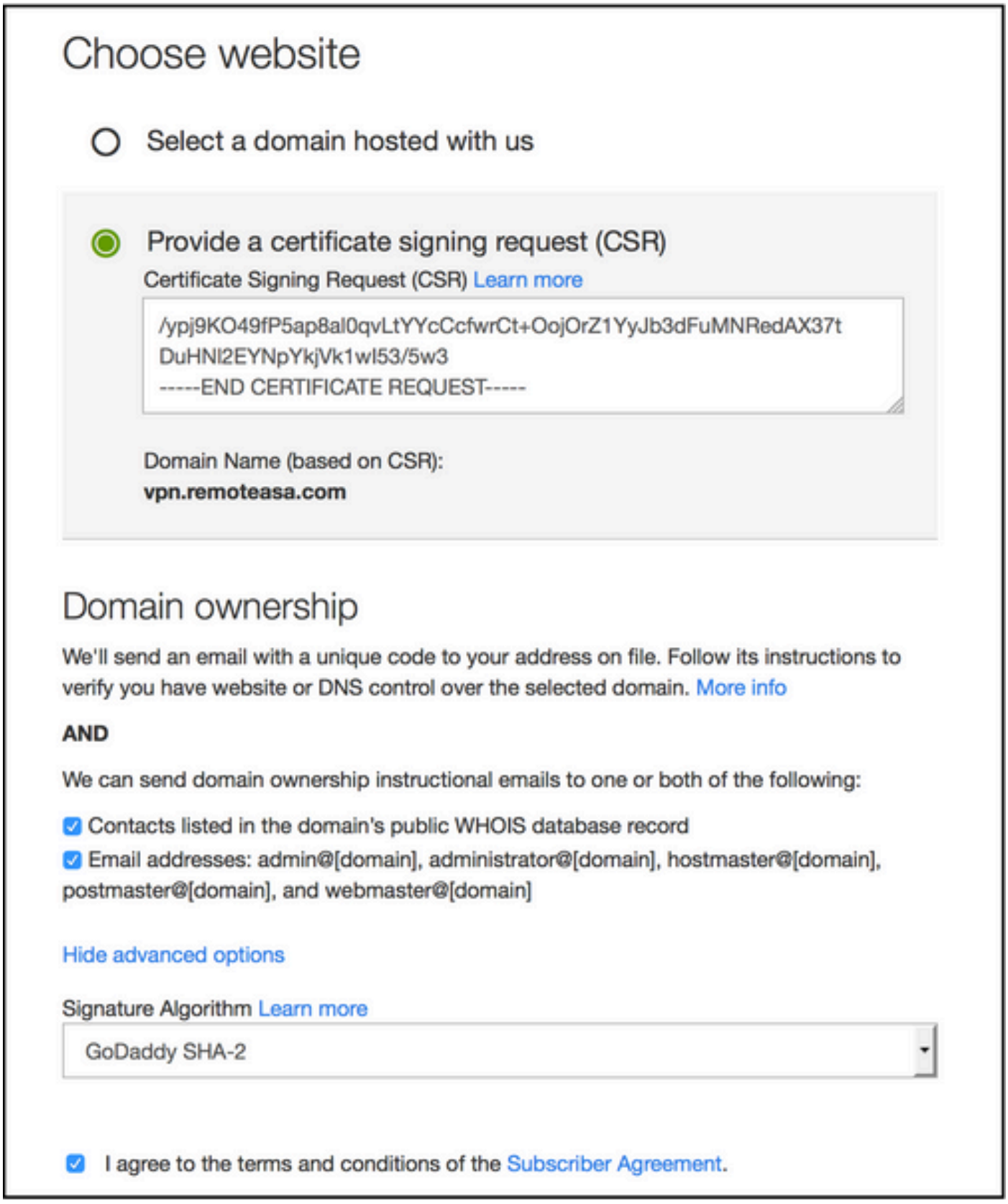
SSL 인증서를 구매한 후 초기 설정 단계에서 GoDaddy Account(GoDaddy 계정)로 이동하여 SSL 인증서를 확인합니다. 새 인증서가 있어야 합니다. 계속하려면 을(를) 클릭합니다**Manage**.



그런 다음 이 이미지에 표시된 CSR을 제공하는 페이지가 나타납니다.

입력한 CSR에 따라 CA는 인증서를 발급할 도메인 이름을 결정합니다.

ASA의 FQDN과 일치하는지 확인합니다.

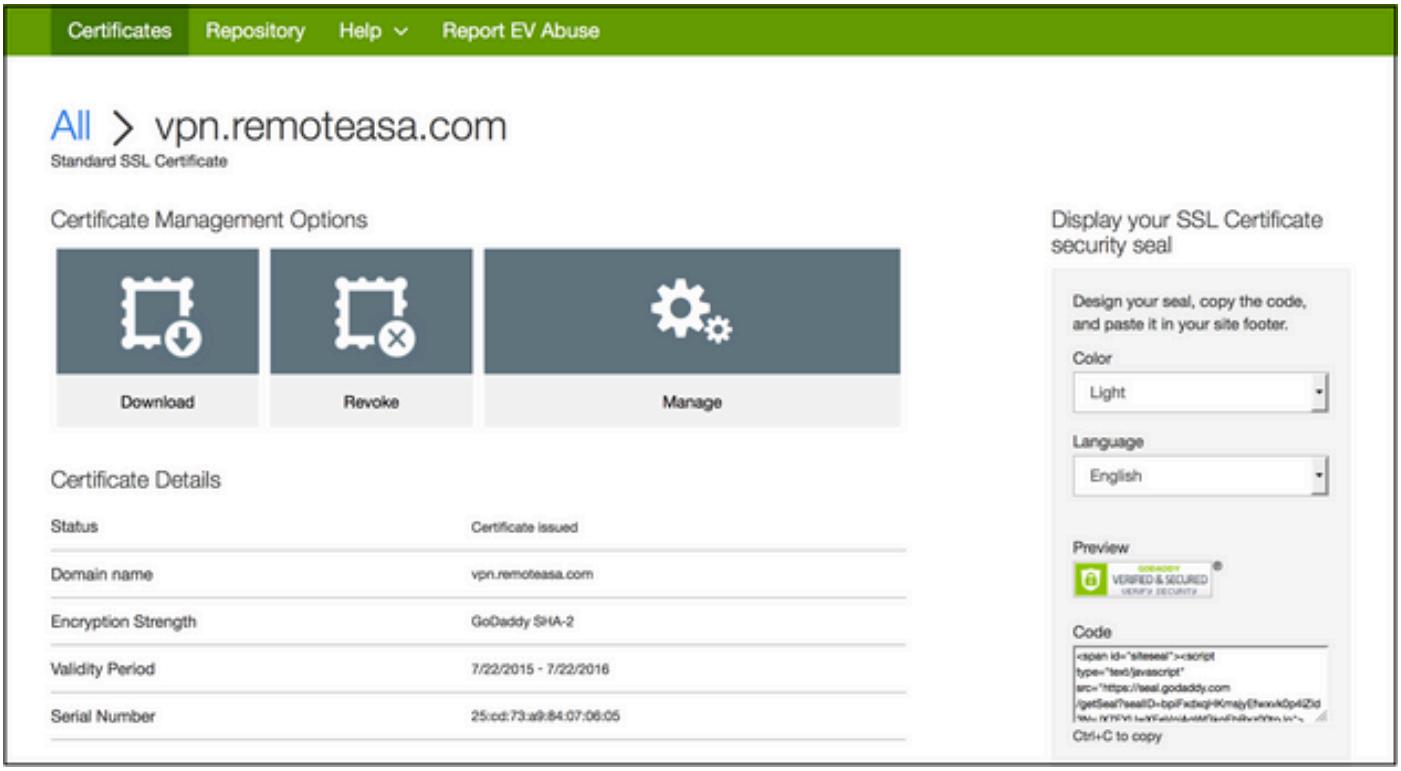


참고: GoDaddy 및 대부분의 다른 CA는 SHA-2 또는 SHA256을 기본 인증서 서명 알고리즘으로 사용합니다. ASA는 8.2(5) [8.3 이전 릴리스] 및 8.4(1) [8.3 이후 릴리스] 이후에서 시작되는 SHA-2 서명 알고리즘을 지원합니다(Cisco 버그 ID CSCti30937). 8.2(5) 또는 8.4(1)보다 오래된 버전이 사용되는 경우 SHA-1 서명 알고리즘을 선택합니다.

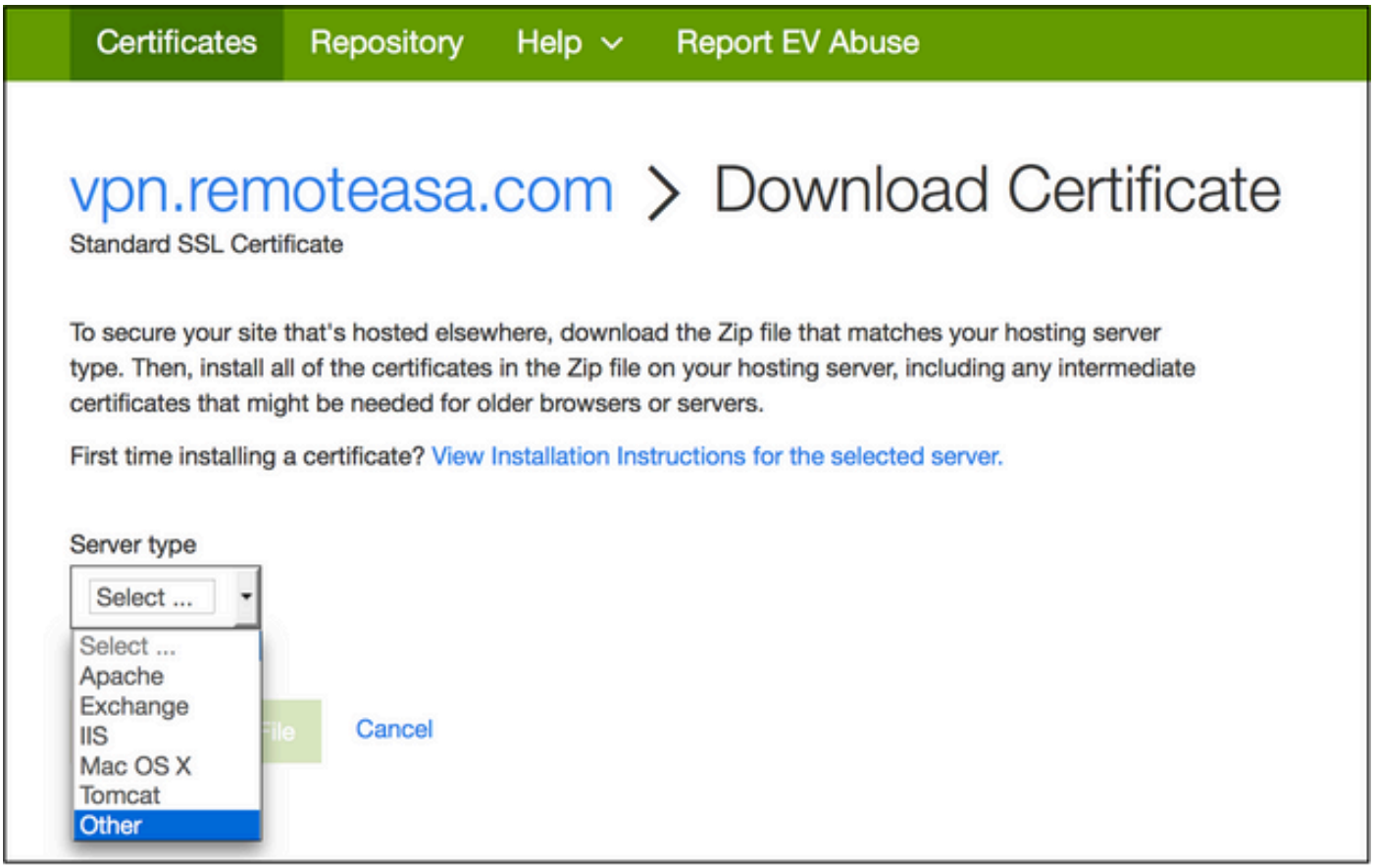
요청이 제출되면 GoDaddy는 인증서를 발급하기 전에 요청을 확인합니다.

인증서 요청이 검증되면 GoDaddy는 계정에 인증서를 발급합니다.

그런 다음 ASA에 설치하기 위해 인증서를 다운로드할 수 있습니다. 더 진행하려면 페이지를 클릭합니다**Download.**



Server Type(서버 유형)을 선택하고**Other** 인증서 zip 번들을 다운로드합니다.



.zip 파일에는 ID 인증서와 GoDaddy CA 인증서 체인 번들이 두 개의 별도의 .crt 파일로 포함되어 있습니다. SSL 인증서 설치로 이동하여 ASA에 이러한 인증서를 설치합니다.

ASA에 SSL 인증서 설치

SSL 인증서는 두 가지 방법으로 ASDM 또는 CLI를 사용하여 ASA에 설치할 수 있습니다.

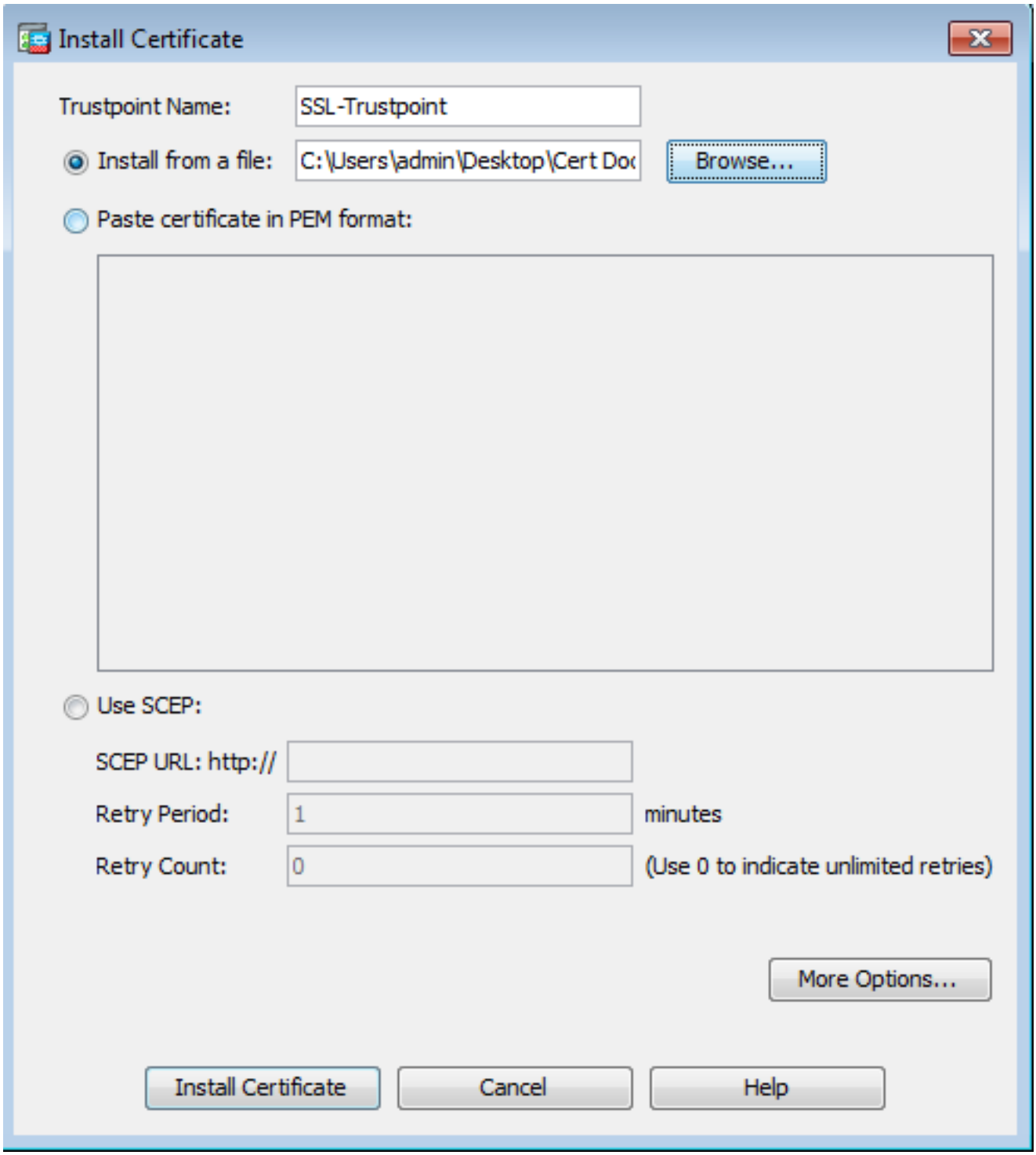
1. CA 및 ID 인증서를 PEM 형식으로 별도로 가져옵니다.
2. 또는 ID 인증서, CA 인증서 및 개인 키가 PKCS12 파일에 번들된 PKCS12 파일(CLI용 base64 인코딩)을 가져옵니다.

> 참고: CA가 CA 인증서 체인을 제공하는 경우, CSR을 생성하는 데 사용된 신뢰 지점의 계층 구조에 중간 CA 인증서만 설치합니다. 루트 CA 인증서 및 기타 중간 CA 인증서는 새 신뢰 지점에 설치할 수 있습니다.

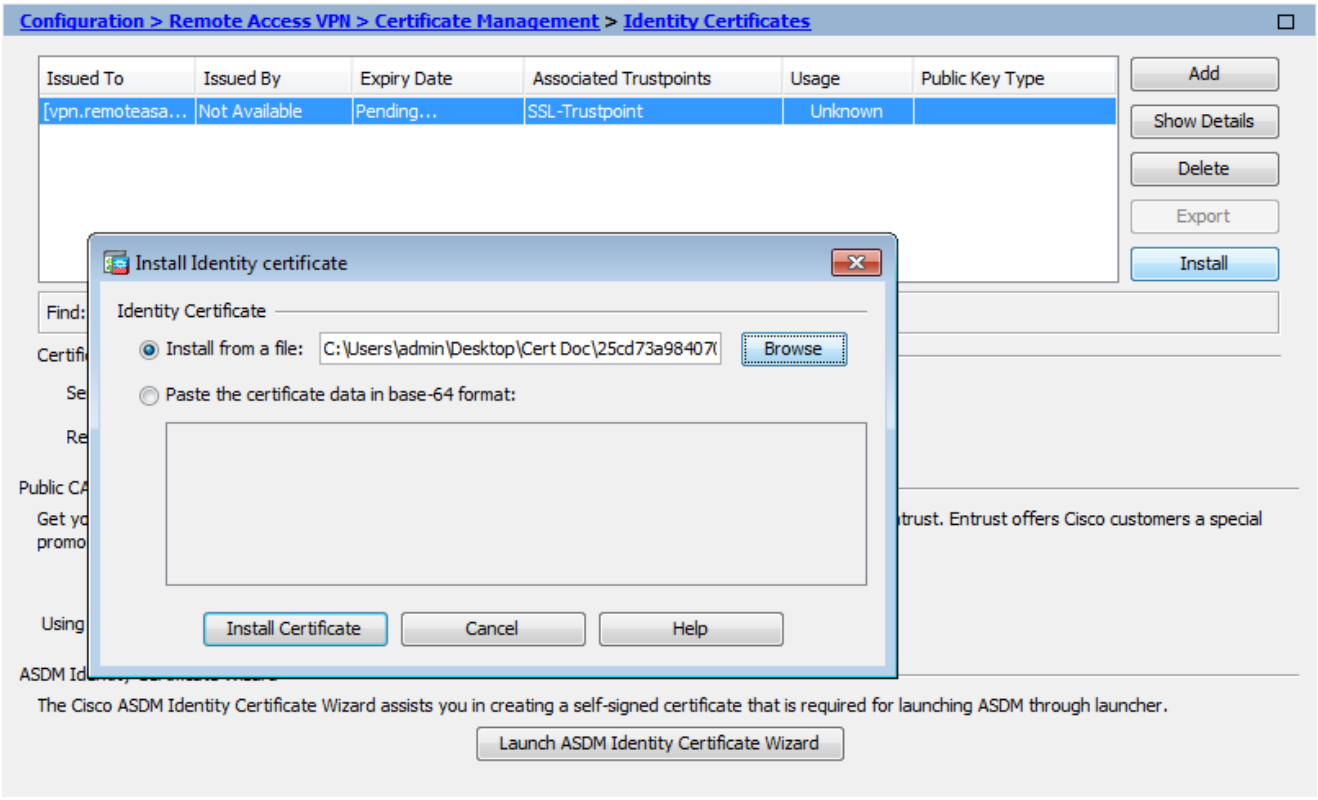
1.1 ASDM에서 PEM 형식의 ID 인증서 설치

제공된 설치 단계에서는 CA가 PEM으로 인코딩된(.pem, .cer, .crt) ID 인증서 및 CA 인증서 번들을 제공한다고 가정합니다.

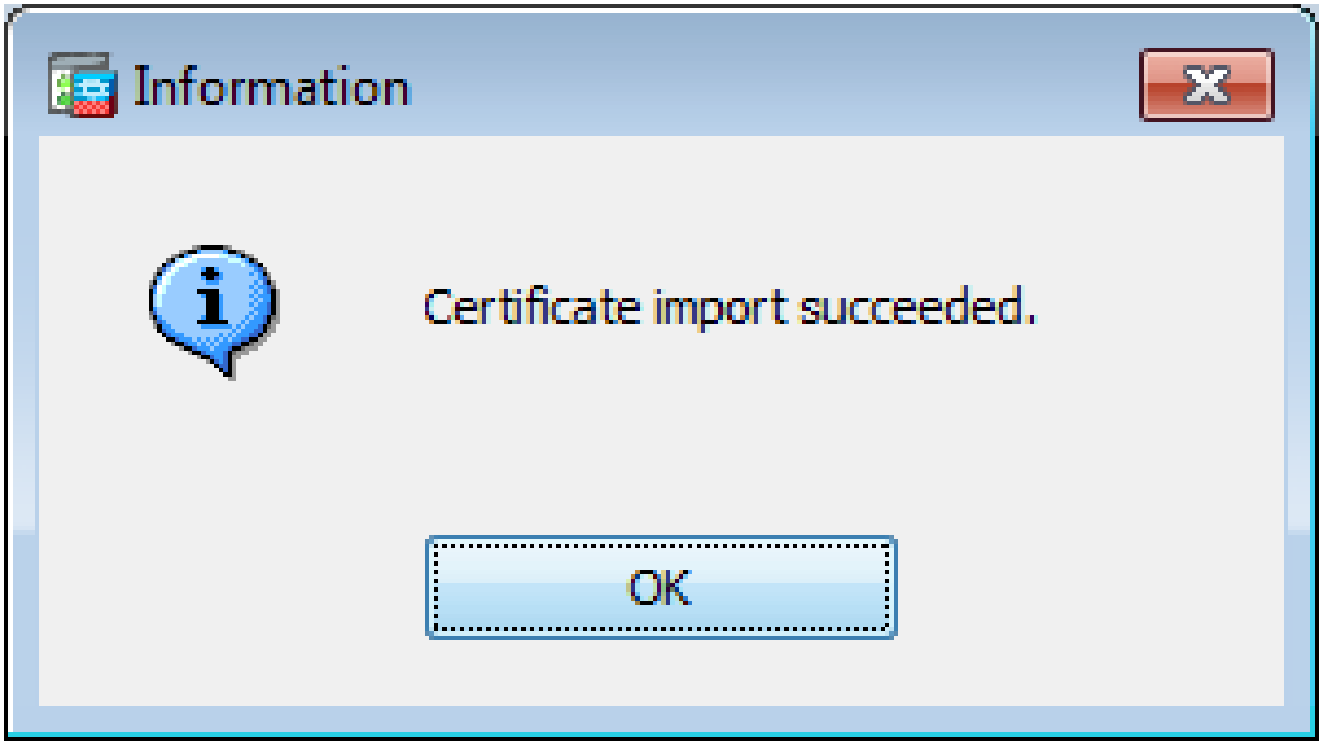
1. CA Certificates(CA 인증서)로 **Configuration > Remote Access VPN > Certificate Management**이동하여 선택합니다.
2. 텍스트 편집기에서 PEM 인코딩 인증서를 사용하고 서드파티 벤더가 제공한 base64 CA 인증서를 복사하여 텍스트 필드에 붙여넣습니다.



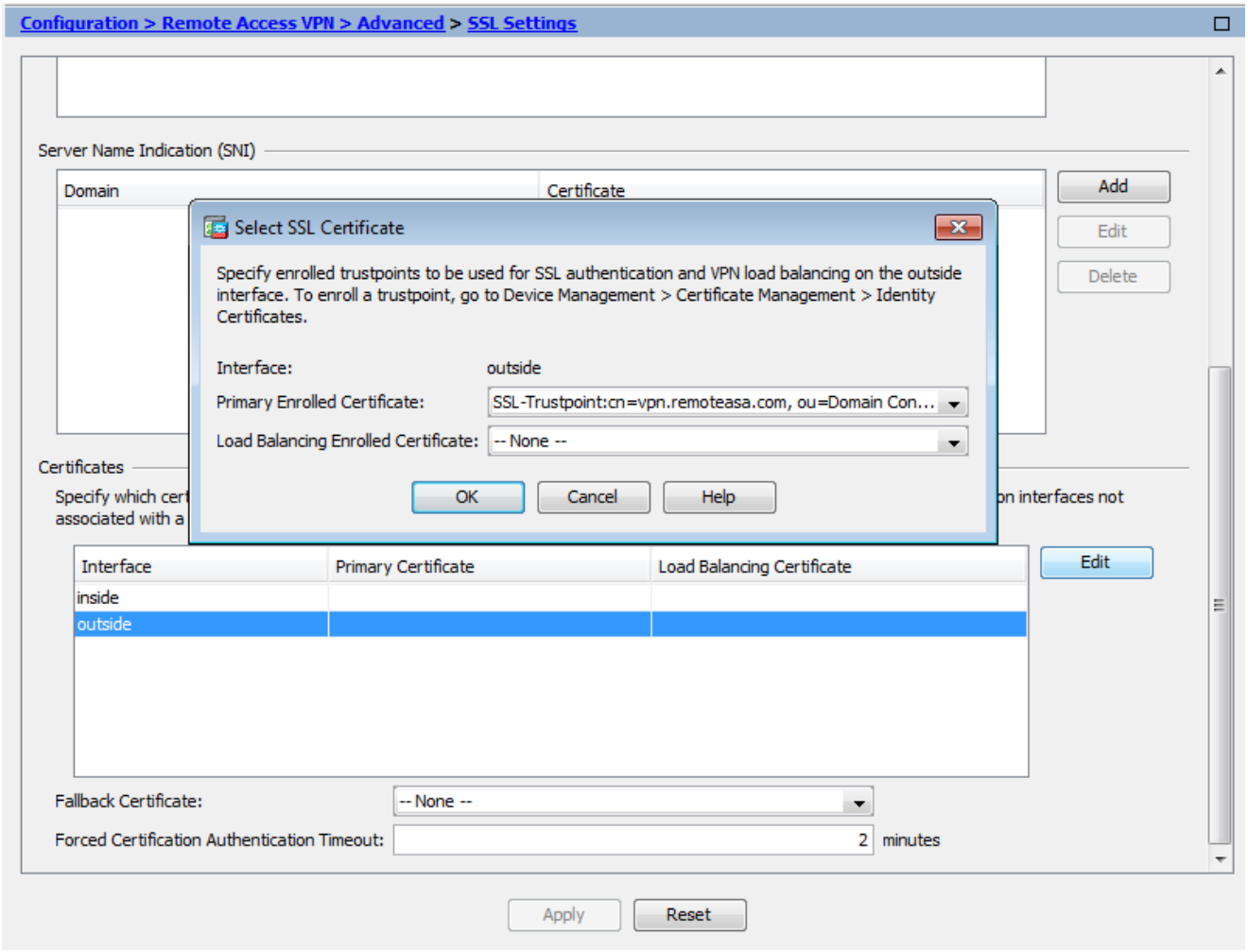
3. Install certificate(인증서 설치)를 클릭합니다.
4. Identity Certificates**Configuration** > **Remote Access VPN** > **Certificate Management**(ID 인증서)로 이동하여 선택합니다.
5. 이전에 생성한 ID 인증서를 선택합니다. 를 **Install**클릭합니다.
6. 옵션**Install from a file** 라디오 버튼을 클릭하고 PEM 인코딩 ID 인증서를 선택하거나, 텍스트 편집기에서 PEM 인코딩 인증서를 열고 서드파티 벤더가 제공한 base64 ID 인증서를 복사하여 텍스트 필드에 붙여넣습니다.



7. 를 클릭합니다**Add Certificate**.



8. 로**Configuration** > **Remote Access VPN** > **Advanced** > **SSL Settings**이동합니다.
9. Certificates(인증서)에서 WebVPN 세션을 종료하는 데 사용되는 인터페이스를 선택합니다. 이 예에서는 외부 인터페이스가 사용됩니다.
10. 를 클릭합니다**Edit**.
11. Certificate(인증서) 드롭다운 목록에서 새로 설치된 인증서를 선택합니다.



12. 를 클릭합니다**OK**.
13. 를 클릭합니다**Apply**. 이제 새 인증서가 지정된 인터페이스에서 종료되는 모든 WebVPN 세션에 사용됩니다.

1.2. CLI를 사용한 PEM 인증서 설치

<#root>

```
MainASA(config)#

crypto ca authenticate SSL-Trustpoint


 Enter the base 64 encoded CA certificate.
End with the word"quit"on a line by itself

-----BEGIN CERTIFICATE----- MIIEADCCAuigAwIBAgIBADANBgkqhkiG9w0BAQUFADBjMQswCQYDVQQGEwJVUzEh MB8GA1UEChI

!!! - Installing Next-level SubCA in the PKI hierarchy

.

!!! - Create a separate trustpoint to install the next subCA certificate (if present)
in the hierarchy leading up to the Root CA (including the Root CA certificate)
```

```
MainASA(config)#crypto ca trustpoint SSL-Trustpoint-1
MainASA(config-ca-trustpoint)#enrollment terminal
MainASA(config-ca-trustpoint)#exit
MainASA(config)#
MainASA(config)# crypto ca authenticate SSL-Trustpoint-1
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself


-----BEGIN CERTIFICATE-----
MIIEfTCCA2WgAwIBAgIDG+cVMA0GCSqGSIb3DQEBCwUAMGMxCzAJBgNVBAYTAlVT
MSEwHwYDVQQKExhUaGUgR28gRGFkZHkgR3JvdXAsIEluYy4xMTAvBgNVBAsTKEdv
IERhZGR5IENsYXNzIDIgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMTQwMTAx
MDcwMDAwWhcNMzEwNTMwMDcwMDAwWjCBgzELMAkGA1UEBhMCVVMxEDAOBgNVBAgT
B0FyaXpvbmExEzARBgNVBAcTClNjb3ROc2RhbGUxGjAYBgNVBAoTEUdvRGFkZHku
Y29tLCBJbmMuMTEwLwYDVQQDEyhHbyBEYWRkeSBSb290IENlcnRpZmljYXRlIEF1
dGhvcml0eSAtIEcyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAv3Fi
CPH6WTT3G8kYo/eASVjpIoMTpsUgQwE7hPHmhUmfJ+r2hBtOoLTbcJjHMgGxBT4H
Tu70+k8vWTAi56sZVmvigAf88xZ1gDlRe+X5NbZ0TqmNghPktj+pA4P6or6KFWp/
3gvDthkUBcrqw6gElDtGfDIN8wBmIsiNaW02jBEYt9OyHGC0OPoCjM7T3UYH3go+
6118yHz7sCtTpJJiaVElBWEaRIGMLKlDliPfrDqBmg4pxRyp6V0etp6eMAo5zvGI
gPtLXcwy7IViQyU0AlYnAZG0O3AqP26x6JyIAX2f1PnbU21gnb8s51iruF9G/M7E
GwM8CetJMVxpRrPgRwIDAQABo4IBFzCCARMwDwYDVR0TAQH/BAUwAwEB/zAOBgNV
HQ8BAf8EBAMCAQYwHQYDVR0OBBYEFDqahQcQZyi27/a9BUFuIMGU2g/eMB8GA1Ud
IwQYMBaAFNLEsNKR1EwRcbNhyz2h/t2oatTjMDQGCCsGAQUFBwEBBCgwJjAkBggr
BgEFBQcwAYYYaHR0cDovL29jc3AuZ29kYWRkeS5jb20vMDIGA1UdHwQrMCkwJ6Al
oCOGIWh0dHA6Ly9jcmwuZ29kYWRkeS5jb20vZ2Ryb29LmNybDBGBgNVHSAEPzA9
MDsGBFUdIAAwMzAxBggrBgEFBQcCARYlaHR0cHM6Ly9jZXJ0cy5nb2RhZGR5LmNv
bS9yZXBvc2l0b3J5LzANBgkqhkiG9w0BAQsFAAOCAQEAWQtTvZKGEacke+1bMc8d
H2xwxbhuvk679r6XUOEwf7ooXGKUwuN+M/f7QnaF25UcjCJYdQkMiGVnOQoWCcWg
OJekxSOTP7QYpgEGRJHjp2kntFolfzq3Ms3dhP8qOCkzpN1nsoX+oYggHFCJyNwq
9kIDN0zmiN/VryTyscPfzLXs4Jlet0lUIDyUGAzHHFIYSaRt4bNYC8nY7NmuHDKO
KHAN4v6mF56ED71XcLNa6R+ghlO773z/aQvgSMO3kwvIClTErF0UZzdsyqUvMQg3
qm5vjLyb4lddJIGvl5echK1srDdMZvNhkREg5L4wn3qkKQmw4TRfZHcYQFHfjDCm
rw==
-----END CERTIFICATE-----
quit

INFO: Certificate has the following attributes:
Fingerprint:     81528b89 e165204a 75ad85e8 c388cd68
Do you accept this certificate? [yes/no]: yes

Trustpoint 'SSL-Trustpoint-1' is a subordinate CA and holds a non self-signed certificate.

Trustpoint CA certificate accepted.

% Certificate successfully imported
BGL-G-17-ASA5500-8(config)#
```

!!! - Similarly create additional trustpoints (of the name "SSL-Trustpoint-n", where n is number thats incremented for every level in the PKI hierarchy) to import the CA certificates leading up to the Root CA certificate.

!!! - Importing identity certificate (import it in the first trustpoint that was created namely "SSL-Trustpoint")

```
 MainASA(config)#
```

```
crypto ca import SSL-Trustpoint certificate

WARNING: The certificate enrollment is configured with an fqdn that differs from the system fqdn. If th
yes

% The fully-qualified domain name in the certificate will be:
(asa.remotevpn.url)

Enter the base 64 encoded certificate. End with the word "quit" on a line by itself
----BEGIN CERTIFICATE-----
MIIFRjCCBC6gAwIBAgIIJc1zqYQHBgUwDQYJKoZIhvcNAQELBQAwgbQxCzAJBgNV
BAYTAlVTMRAwDgYDVQQIEwdBcml6b25hMRMwEQYDVQQHEwpTY29OdHNkYWxlMRow
GAYDVQQKExFHb0RhZGR5LmNvbSwgSW5jLjEtMCsGA1UECxMkaHR0cDovL2NlcnRz
LmdvZGFkZHkuY29tL3JlcG9zaXRvcnkvMTMwMQYDVQQDEypHbyBEYWRkeSBTZWN1
cmUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5IC0gRzIwHhcNMTUwNzIyMTIwNDM4WhcN
MTYwNzIyMTIwNDM4WjA/MSEwHwYDVQQLExhEb21haW4gQ29udHJvbCBWYWxpZGF0
ZWQxGjAYBgNVBAMTEXZwbi5yZW1vdGVhc2EuY29tMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEArrY2Fv2S2Uq5HdDhOaSzK5Eyok2tv2Rem8DofbTQ+4F9
C9IXitWdLAo6a7dzyfB4S9hx1VZXoHMGGNd6i9NWLXsWU1Nx5pRMaKR4h1cL6bDW
ITt5GzKdL93ibMxYmau+uwM3OkBb8QxLNNxr4G+oXtfavctTxWy/o6LzKWFyjOXP
tta9FZWO7cOMNvKiUL1v9WBcy4GK1xyvN9RtWebtVkM5/iOvOReBTBfFxCJ1YQAG
UWteu1ikWAGj1qomZGnZgAFDWJ4/hxjesG2BGMtwX5L1O8cbmbi/u/vnmZ5Xhiqx
<snip>
CCsGAQUFBwIBFitodHRwOi8vY2VydGlmaWNhdGVzLmdvZGFkZHkuY29tL3JlcG9z
aXRvcnkvMHYGCCsGAQUFBwEBBGowaDAkBggrBgEFBQcwAYYYaHR0cDovL29jc3Au
Z29kYWRkeS5jb20vMEAGCCsGAQUFBzAChjRodHRwOi8vY2VydGlmaWNhdGVzLmdv
ZGFkZHkuY29tL3JlcG9zaXRvcnkvZ2RpZzIuY3JOMB8GA1UdIwQYMBaAFEDCvSeO
zDSDMKIz1/tss/C0LIDOMEYGA1UdEQQ/MD2CEXZwbi5yZW1vdGVhc2EuY29tghV3
d3cudnBuLnJlbW9OZWFzYS5jb22CEXZwbi5yZW1vdGVhc2EuY29tMB0GA1UdDgQW
BBT7en7YS3PH+s4z+wTRlpHr2tSzejANBgkqhkiG9w0BAQsFAAOCAQEAO9H8TLNx
2YOrYdI6gS8n4imaSYg9Ni/9Nb6mote3J2LELG9HY9m/zUCR5yVktra9azdrNUAN
1hjBJ7kKQScLC4sZLONdqG1uTP5rbWROyikF5wSzgyMWdO3kOR+vM8q6T57vRst5
69vzBUuJc5bSu1IjyfPP19z1l+B2eBwUFbVfXLnd9bTfiG9mSmC+4V63TXFxt1Oq
xkGNys3GgYuCUy6yRP2cAUV1lc2tYtaxoCL8yo72YUDDgZ3a4PyO1EvC1FOaUtgv
6QNEOYwmbJkyumdPUwko6wGOC0WLumzv5gHnhil68HYSZ/4XIlp3B9Y8yfG5pwbn
7puhazH+xgQRdg==
-----END CERTIFICATE-----
quit
INFO: Certificate successfully imported
! Apply the newly installed SSL certificate to the interface accepting SSL connections

MainASA(config)#
ssl trust-point SSL-Trustpoint outside
```

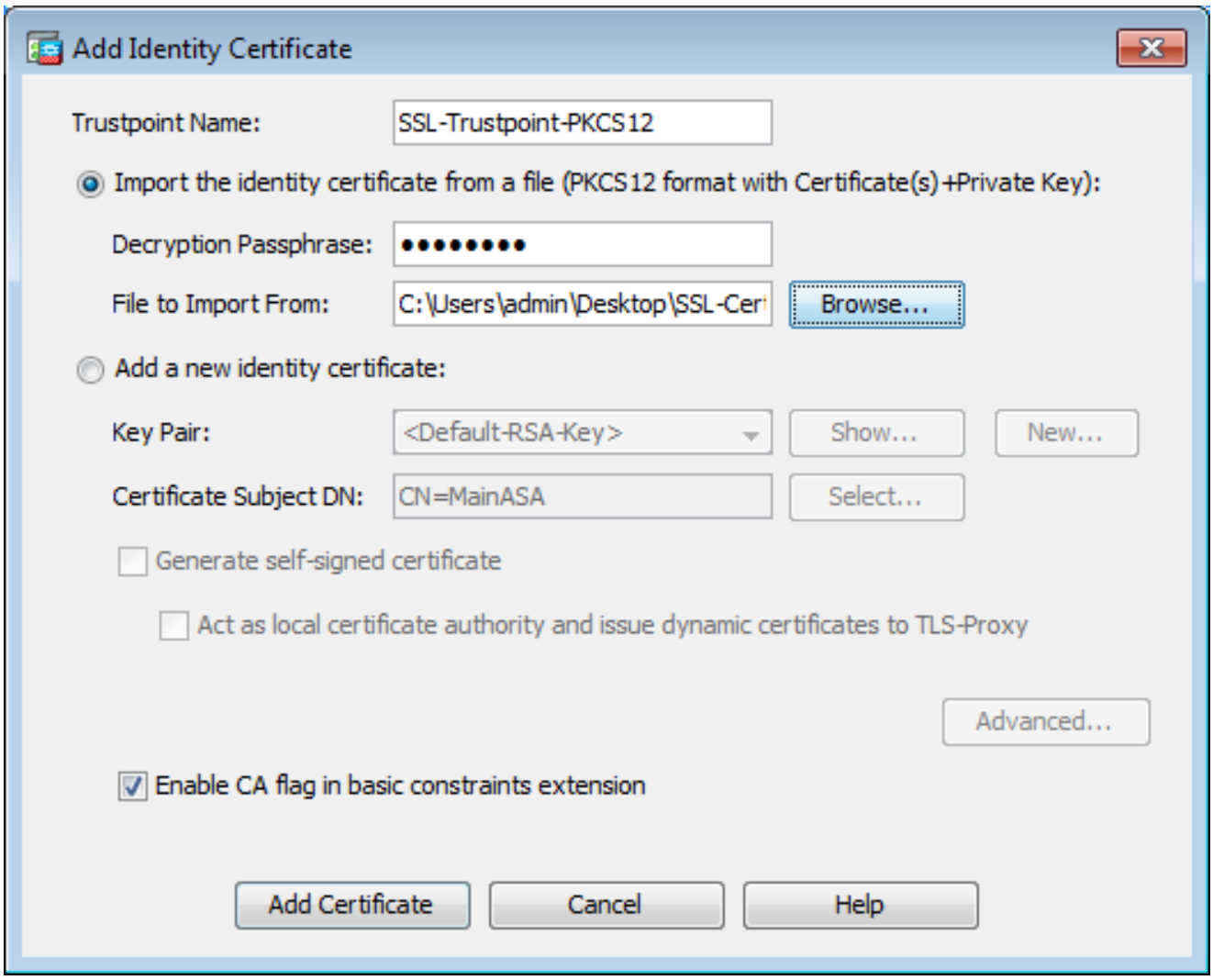
2.1 ASDM을 통한 PKCS12 인증서 설치

와일드카드 인증서의 경우나 UC 인증서가 생성될 때와 같이 ASA에서 CSR이 생성되지 않은 경우, ID 인증서와 개인 키가 별도의 파일 또는 단일 번들 PKCS12 파일(.p12 또는 pfx 형식)로 수신됩니다. 이 유형의 인증서를 설치하려면 다음 단계를 완료하십시오.

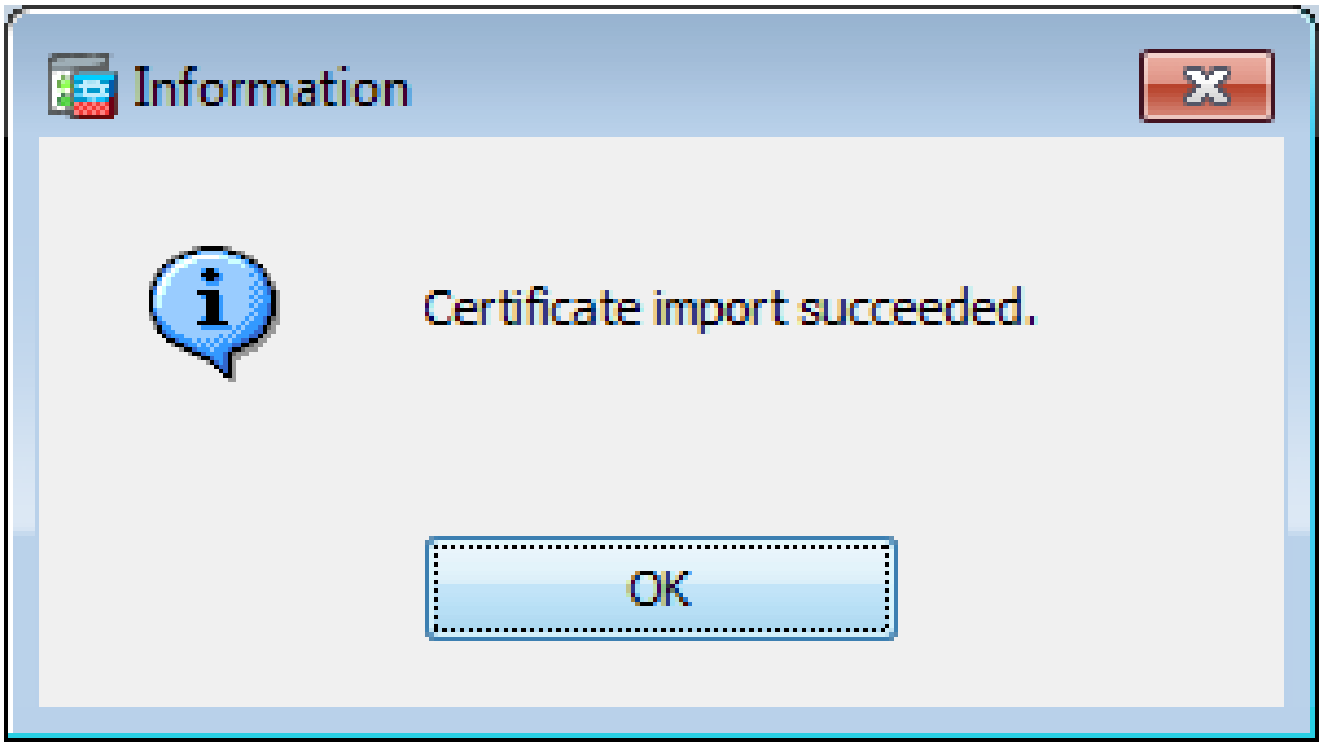
1. ID 인증서는 CA 인증서와 개인 키를 단일 PKCS12 파일에 번들로 묶습니다. 부록 B는 OpenSSL을 사용하여 이 작업을 수행하는 단계를 제공합니다. CA에서 이미 번들로 구성한 경

우 다음 단계로 진행합니다.

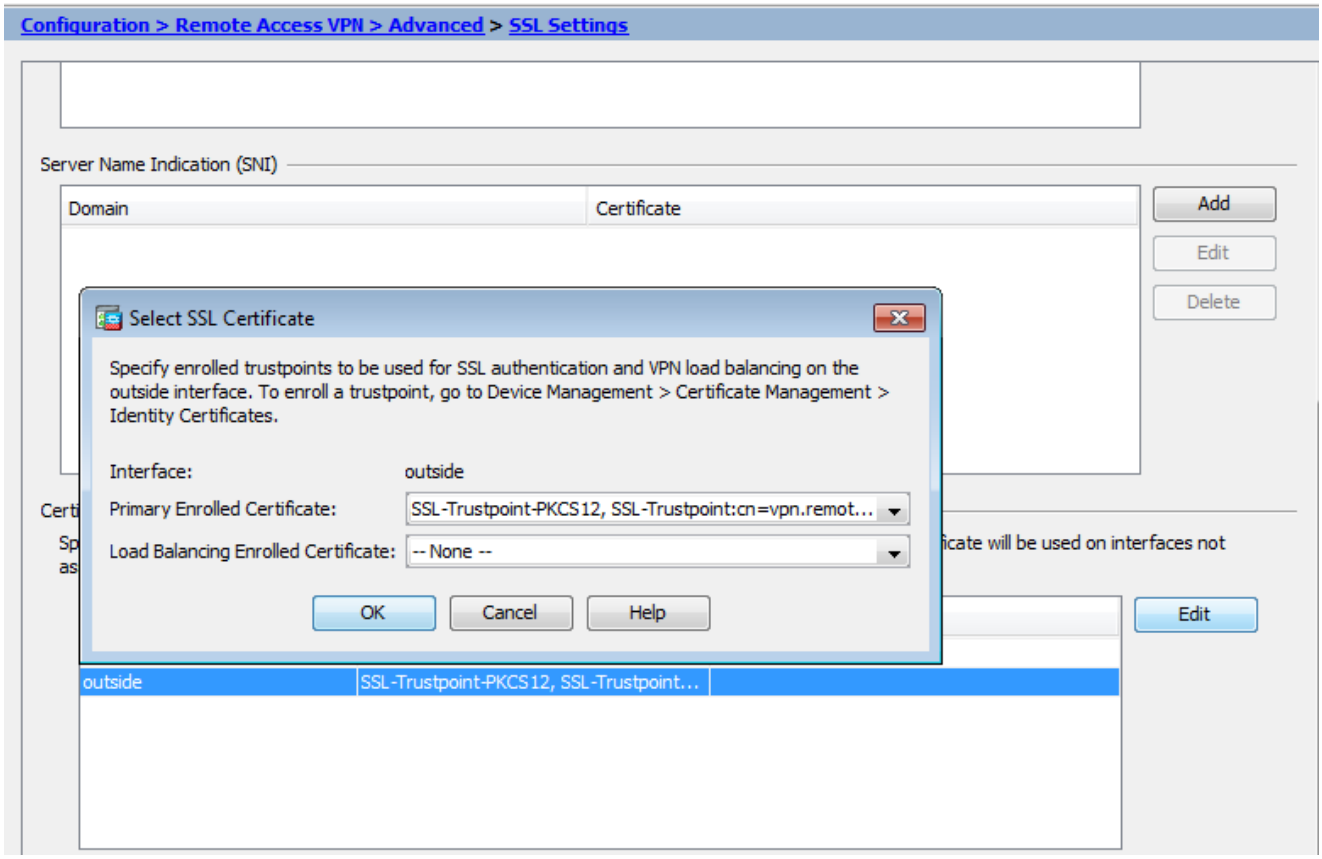
2. 탐색 및**Configuration > Remote Access VPN > Certificate Management,** 선택 **Identity Certificates.**
3. 를 클릭합니다**Add.**
4. 신뢰 지점 이름을 지정합니다.
5. 라디오 버튼을 **Import the identity certificate from a file**클릭합니다.
6. PKCS12 파일을 생성하는 데 사용되는 패스프레이즈를 입력합니다. PKCS12 파일을 찾아 선택합니다. 인증서 패스프레이즈를 입력합니다.



7. Add Certificate(인증서 추가)를 클릭합니다.



8. 탐색**Configuration > Remote Access VPN > Advanced**후 선택 **SSL Settings.**
9. Certificates(인증서)에서 WebVPN 세션을 종료하는 데 사용되는 인터페이스를 선택합니다. 이 예에서는 외부 인터페이스가 사용됩니다.
10. 를 클릭합니다**Edit.**
11. Certificate(인증서) 드롭다운 목록에서 새로 설치된 인증서를 선택합니다.



12. 를 클릭합니다**OK.**

13. 를 클릭합니다**Apply**. 이제 새 인증서가 지정된 인터페이스에서 종료되는 모든 WebVPN 세션에 사용됩니다.

2.2 CLI를 사용한 PKCS12 인증서 설치

```
<#root>

  MainASA(config)#

crypto ca trustpoint SSL-Trustpoint-PKCS12

MainASA(config-ca-trustpoint)#

enrollment terminal

MainASA(config-ca-trustpoint)#

exit


MainASA(config)#

crypto ca import SSL-Trustpoint-PKCS12 pkcs12 cisco123


Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
-----BEGIN PKCS12-----
MIISNwIBAzCCEfEGCSqGSIb3DQEHAaCCEeIEghHeMIIR2jCCEdYGCSqGSIb3DQEH
BqCCEccwghHDAgEAMIIRvAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIWO3D
hDti/uECAQGAghGQ9ospee/qtIbVZh2T8/Z+5dxRPBcStDTqyKy7q3+9ram5AZdG
Ce9n5UCckqT4WcTjs7XZtCrUrt/LkNbmGDVhwGBmYWiOS7npgaUqOeoqiJRK+Yc7
LNOnbho6I5WfL56/JiceAMlXDLr/IqqLg2QAApGdN+F5vANsHse2GsAATewBDLt7
Jy+SKfoNvvIw9QvzCiUzMjYZBANmBdMCQ13H+YQTHitT3vn2/iCDlzRSuXcqypEV
q5e3heiOO75lE8TDLWmO3PMvwIZqi8yzWesjcTt1Kd4FoJBZpB7O/v9LntoIUOY7
kIQM8fHb4ga8BYfbgRmG6mkMmO1STtbSvlvTa19WTmdQdTyCa+G5PkrryRsy3Ww1
lkGFMhImmrnNADF7HmzbyslVohQZ7hO9iVQY9krJogoXHjmQYxG9brf0oEwxSJDa
mGDhhESh+s/WuFSV9Z9kiTXpJNZxpTASoWBQrrwmO5v8ZwbjbVNJ7sVdbwpUl6d+
NNFGR7LTqO8hpupeeJnY9eJc2yYqeAXWXQ5kLOZo6/gBEdGtEaZBgCFK9JZ3bl3A
xqxGifanWPnLYG611NKuNjTgbjhnEEYI2uZzUOqxnlKa8zyXw+lzrKuJscDbkAPZ
wKtw8K+p4OzXVHhuANo6MDvffNRY1KQDtyK1inoPH5ksVSE5awkVam4+HTcqEUfa
16LMana+4QRgSetJhUOLtSMaQfRJGkha4JLq2t+JrCAPz2osARlTsBOjQBNq6YNj
OuB+gGk2Gl8Q5Nln6K1fzOXBFZLWEDBLsaBRO5MAnE7wWtOO+4awGYqVdmIF1lkf
XIRKAiQEr1pZ6BVPuvsCNJxaaUHzufhYI2ZAckasKBZOT8/7YK3fnAaGoBCz4cHa
o2EEQhq2aYb6YTvO+wtLEWGHzsbGZEM/u54XmsXAI7g28LGJYdfWi5O9KyV+Ac1V
KzHqXZMM2BbUQCNcTF5JIMiW+r62k42FdahfaQbOvJsIe/IwkAKG7y6DIQFsOhwg
ZlPXiDbNr1k4e8L4gqupMKWg853PY+oY22rLDC7bul1CKtixIYBCvbn7dAYsI4GQ
l6xXhNu3+iyeOHgbUQQCfTU/mBrAOZO+bpKjWOCfqNBuYnZ6kUEdCI7GFLH9QqtM
K7YinFLoHwTWbi3MsmqVv+Z4ttVWy7XmikoO2nMynJMP6/CNV8OMxMKdC2qm+c1j
s4QlKcAmFsQmNp/7SIP1wnvOc6JbUmC1O52OU/r8ftTzn8C7WL62W79cLK4HOr7J
sNsZnOz0JOZ/xdZT+cLTCtVevKJOQMK3vMsiOuy52FkuF3HnfrmBqDkbR7yZxELG
RCELOEDdbp8VPO+IhNlyz1q7975SscdxFSLOTvjnHGFWd14ndoqN+bLhWbdPjQWV
l3W2NCI95tmHDLGgp3POOlS+RjdCEGGMg+9cpgBfFC1JocuTDIEcUbJBY8QRUNiS
/ubyUagdzUKt1ecfb9hMLP65ZNQ93VIw/NJKbIm7b4P/1Zp/lFP5eq7LkQPAxE4/
bQ4mHcnwrs+JGFkN19B8hJmmGoowH3p4IEvwZy7CThB3E1ejw5R4enqmrgvHqpQe
B7odN1OFLAHdo1G5BsHExluNEsEb4OQOpmKXidDB5BOO1bJsr748fZ6L/LGx8Al3
<snip>
ijDqxyfQXY4zSytljSMwMtYA9hG5I79Sg7pnME1E9xq1DOoRGg8vgxlwiciKtLxp
LLOReDY31KRYvOOvWOgf+tE7lST/3TKZvhOsQ/BEOV3kHnwldejMFH+dvyAA9Y1E
c8O+tdafBFX4B/HP46E6heP6ZStOxAfRW1/JF4ljNvUNVO9VtVfR2FTyWpzZFY8A
GG5XPIA8OWF6wKEPFHIcN8scY+Vot8kXxG96hwt2Cm5NQ2OnVzxUZQbpKsjs/2jC
```

3HVFe3UJFBsY9UxTLcPXYBSIG+VeqkI8hWZp6clTfNDLY2ELDylQzp1mBg2FujZa
YuE0avjCJzBzZUG2umtS5mHQnwPF+XkOujEyhGMauhGxHp4nghSzrUZrBeuL9lUF
2mbpsOcgZkzxMS/rjdNXjCmPFloRBvKkZSlxHFrE/5ZopAhn4i7YtHQNrz9U4RjQ
xo9cUuaJ+LNmvzE8Yg3epAMYZ16UNGQQkVQ6ME4BcjRONzW8BYgTq4+pmT1ZNq1P
X87CXCPtYRpHF57eSo+tHDINCgfqYXD6e/7r2ngfiCeUeNDZ4aVl2XxvZDaUlBPP
Tx5fMARqx/Z8BdDyBJDVBjdsxmQau9HLkhPvdfGlZIWdTe13CzKqXA5Ppmpjt4q9
GnCpC53m76x9Su4ZDw6aUdBcgCTMvfaqJC9gzObee2Wz+aRRwzSxu6tEWVZolPEM
v0AA7po3vPeklgOnLRAwEoTTn4SdgNLWeRoxqZgkw1FC1GrotxF1so7uA+z0aMeU
lw73reonsNdZvRAcVX3Y6UNFdyt70Ixvo1H4VLzWm0K/oP62C9/eqqMwZ8zoCMPt
ENna7T+7Os66SCbMmXCHwyhO0tygNKZFFw/AATFyjqPMWPAxGuPNOrnB6uYCn0Hk
1BU7tF143RNIZaQQEH3XnaPvUuAA4C0FCoE3h+/tVjtfNKDvFmb6ZLZHYQmUYpyS
uhdFEpoDrJH1VmI2Tik/iqYWaZ+oDqXPHQXnJhw25h9ombR4qnD+FCfwFCGtPFON
o3QffZ53C95n5jPHVMyUrOxDdpwnvzCQPdj6yQm564TwLAmiz7uDlpqJZJe5QxHD
nolv+4MdGSfVtBq+ykFoVCaamqeaq6sKgvAVujLXXEs4KEmIgcPqATVRG49ElndI
LO1DEQyKhVoDGebAuVRBjzwAm/qxWxxFv3hrbCjpHCwEYms4Wgt/vKKRFsuWJNZf
efHldwlltkd5dKwSvDocPT/7mSLtLJa94c6AfgxXy9zO+FTLDQwzxga7xC2krAN1
yHxR2KHN5YeRL+KDzu+u6dYoKAz+YAgwlW6KbeavALSuH4EYqcvg8hUEhp/ySiSc
RDhuygxEovIMGfES4FP5V52lPyDhM3DqwhnOvuYUmYnX8EXURkay44iwwI5HhqYJ
lptWyYo8Bdr4WNwt5xqszGzYR6mmGeAIin7bDunsF1uBHWYF4dyKlz1tsdRNMYqQ
+W5q+QjVdrjldWv/bMFOaqEjxeNWBRqjzcff3BxMnwvVxtgqxFvRh+DZxiJoiBG+
yx7x8np2AQ1rOMETSSxbnZzfnKZKVvBVMkIC6Jsmt2WEVTQvoFJ8em+nemOWgTi/
hHSBzjE7RhAucnHuifOCXOgvR1SDDqyCQbiduc1QjXNOsvA8Fqbea9WEH5khOPv3
pbtsL4gsfl2pv8diBQkVQgiZDi8Wb++7PR6ttiY65kVwrdsoNl1/qq+xWOd3tB4/
zoH9LEMgTy9Sz7myWrB9EOOZ8BIjL1M8oMigEYrTDOc3KbyW1S9dd7QAxiuOBaX1
8J8q1OydvTBzmqcjeSsFH4/1NHn5VnfOZnNpui4uhpOXBG+K2zJUJXm6dq1AHBlE
KQFsFZpNNyave0Kk8JzQnLAPd7OUU/IksyOCGQozGBH+HSzVp1RDjrrbC342rkBj
wnI+j+/1JdWBmHdJMZCfoMZFLSI9ZBqFirdii1/NRu6jh76TQor5TnNjxIyNREJC
FE5FZnMFvhM9OOLaiUZff8WWCOfeRDMttLXb1nuxPFl+lRk+LNlPLVptWgcxzfsr
JXrGiwjxybBB9oCOrACq8fGAtEs8WRxJyDH3Jjmn9i/Gl6J1mMCUF//LxAH2WQx8
Ld/qS5OM2iFCffDQjxAj0K6DEN5pUebBv1Em5SOHXvyq5nxgUh4/y84CWaKjwOMQ
5tbbLMlnc7ALIJ9LxZ97YiXSTyeM6oBXBFx6RpklkDvO5mlBghSpVQiMcQ2ORIkh
UVVNbSHOl9S3cb5wqxaWqAKBqb4h1uLGVbYWZf2mzLZ8U5U5ioiqoMBqNZbzTXpO
EqEFuatTllQvCRbcKS3xou4MAixcYUxKwEhbZA/6hd1OXSBJwe7jKBV9M6wliKab
UfoJCGTAf3sY68lqrMPrbBtOeeWf1CO2Sd9Mn+V/jvnil7mxYFFUpruRq3r1LeqP
J5camfTtHwyL8N3Q/Zwp+zQeWZiLA8a/iAVu/hYLR1bpF2WCKOlOtJqkvVmrLVLz
maZZjbJeOft5cP/lRxbKlS6Gd5dFTEKDE15c6gWUX8RKZP6Q7iaE5hnGmQjm8Ljl
kXwF+ivoxOQ8a+Gg1bVTROc7tqW9e9/ewisV1mwvEB6Ny7TDS1oPUDHM84pY6dqi
1+Oio07Ked4BySwNlYy9yaJtBTZSCstfP+ApLidN7pSBvvXf1aHmeNbkPOZJ+c+t
fGpUdL6V2UTXfCsOPHTC0ezA15sOHwCuPchrDIj/eGUwMS3NfS25XgcMuvnLqGVO
RzcRzlZIg8G0oLYwOCuzoY0D/m9O1OO1ahePyA9tmVB7HRRbytLdaW7gYeEikoCv
7qtBqJFF17ntWJ3EpQHZUcVClbHIKqjNqRbDCY7so4AlIW7kSEUGWMIUDhprE8Ks
NpnvPH2i9JrYrTeROyUIOtL/7SATd2POa2lxz/zUWekeqd0bmVCsAgQNbB2XkrR3
XS0B52ol+63e8KDqS2zL2TZd3daDFidHlB8QB26tfbfOAcaObJH5/dWP8ddo8UYo
Y3JqTl0malxSJhaMHmQdZIQp49utW3TcjqGllYS4HEmcqtHud0ShaUysC6239jlQ
KlFWrwXTlBC5vnq5IcOMqx5zyNbfxXz28969cWoMCyU6+kRwOTyF6kF7EEv6XWca
XLEwABx+tKRUKHJ673SyDMu96KMV3yZN+RtKbCjqCPVTP/3ZeIp7nCMUcj5sW9HI
N34yeI/0RCLyeGsOEiBLkucikC32LI9ik5HvImVTELQOUz3ceFqU/PkasjJUve6S
/n/1ZVUHbUk71xKR2bWZgECl7fIel7wlrbjpF3Wbk+Er0kfYcsNRHxeTDpKPSt9s
u/UsyQJiyNARG4X3iYQlsTce/O6Ycyri6GcLHAu58BO2nj4CxolCplABZ2N79HtN
/7Kh5LOpS9MwsDCHuUI8KFrTsET7TB1tIU99FdB19L64sl/shYAHbccvVWU5OWht
PdLoaErrX81Tof41IxbSZbI8grUC4KfG2sdPLJKu3HVTeQ8LfllbBLxfs8ZBS+Oc
v8rHlQO12kY6LsFGLehJ+/yJ/uvXORivOESp4EhFpFfkp+o+YcFeLUUPd+jzb62K
HfSCCbLpCKyEay8OdyWkHfgylqxmb9ud0oMO5OaFJyqR0NjNt6pcxBRY2A6AJR5S
IIC26YNwbhOGjF9qL2FiUqnNH/7GTqPnd2qmsB6FTIwSBT6d854qN7PRt+ZXgdtQ
OjcYt1r9qpWDZpNFK8EzizwKiAYTsiEh2pzPt6YUpksRb6CXTkIzoG+KLsv2m3b8
OHyZ9a8z81/gnxrZlls5SCTfOSU7OpHWh8VAYKVHHK+MWgQrOm/2ocV32dkRBLMy
2R6P4WfHyI/+9de1x3PtIuOiv2knpxHv2fKM6sQw45F7XkmwHxjq1YRJ6vIwPTAh
MAkGBSsOAwIaBQAEFFTRETzpisHKZR+Kmen68VrTwpV7BBSQiOIesQ4n4E/bSVsd
qJSzcwh0hgICBAA=
-----END PKCS12-----
quit

INFO: Import PKCS12 operation completed successfully

```
!!! Link the SSL trustpoint to the appropriate interface
MainASA(config)#
```

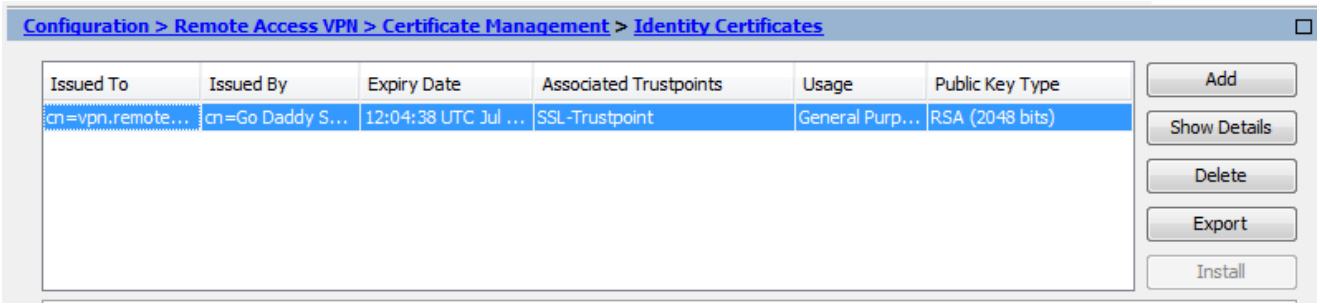
ssl trust-point SSL-Trustpoint-PKCS12 outside

다음을 확인합니다.

타사 공급업체 인증서의 성공적인 설치를 확인하고 SSLVPN 연결에 을 사용하려면 다음 단계를 수행합니다.

ASDM을 통해 설치된 인증서 보기

1. 탐색**Configuration > Remote Access VPN > Certificate Management,**후 선택 **Identity Certificates.**
2. 서드파티 벤더에서 발급한 ID 인증서가 나타납니다.



CLI를 통해 설치된 인증서 보기

<#root>

```
 MainASA(config)#
```

show crypto ca certificate

Certificate

```
  Status: Available
  Certificate Serial Number: 25cd73a984070605
  Certificate Usage: General Purpose
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: SHA256 with RSA Encryption
  Issuer Name:
    cn=Go Daddy Secure Certificate Authority - G2
    ou=http://certs.godaddy.com/repository/
    o=GoDaddy.com\, Inc.
    l=Scottsdale
    st=Arizona
    c=US
  Subject Name:
    cn=(asa.remotevpn.url)
    ou=Domain Control Validated
```

```
  OCSP AIA:
    URL: http://ocsp.godaddy.com/
  CRL Distribution Points:
    [1]  http://crl.godaddy.com/gdig2s1-96.crl
  Validity Date:
    start date: 12:04:38 UTC Jul 22 2015
    end   date: 12:04:38 UTC Jul 22 2016
  Associated Trustpoints:
```

SSL-Trustpoint

CA Certificate

```
  Status: Available
  Certificate Serial Number: 07
  Certificate Usage: General Purpose
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: SHA256 with RSA Encryption
  Issuer Name:
    cn=Go Daddy Root Certificate Authority - G2
    o=GoDaddy.com\, Inc.
    l=Scottsdale
    st=Arizona
    c=US
  Subject Name:
    cn=Go Daddy Secure Certificate Authority - G2
    ou=http://certs.godaddy.com/repository/
    o=GoDaddy.com\, Inc.
    l=Scottsdale
    st=Arizona
    c=US
  OCSP AIA:
    URL: http://ocsp.godaddy.com/
  CRL Distribution Points:
    [1]  http://crl.godaddy.com/gdroot-g2.crl
  Validity Date:
    start date: 07:00:00 UTC May 3 2011
    end   date: 07:00:00 UTC May 3 2031
  Associated Trustpoints:
```

SSL-Trustpoint

CA Certificate

```
  Status: Available
  Certificate Serial Number: 1be715
  Certificate Usage: General Purpose
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: SHA256 with RSA Encryption
  Issuer Name:
    ou=Go Daddy Class 2 Certification Authority
    o=The Go Daddy Group\, Inc.
    c=US
  Subject Name:
    cn=Go Daddy Root Certificate Authority - G2
    o=GoDaddy.com\, Inc.
    l=Scottsdale
    st=Arizona
```

```
    c=US
  OCSP AIA:
    URL: http://ocsp.godaddy.com/
  CRL Distribution Points:
    [1]  http://crl.godaddy.com/gdroot.crl
  Validity Date:
    start date: 07:00:00 UTC Jan 1 2014
    end   date: 07:00:00 UTC May 30 2031
  Associated Trustpoints:
```

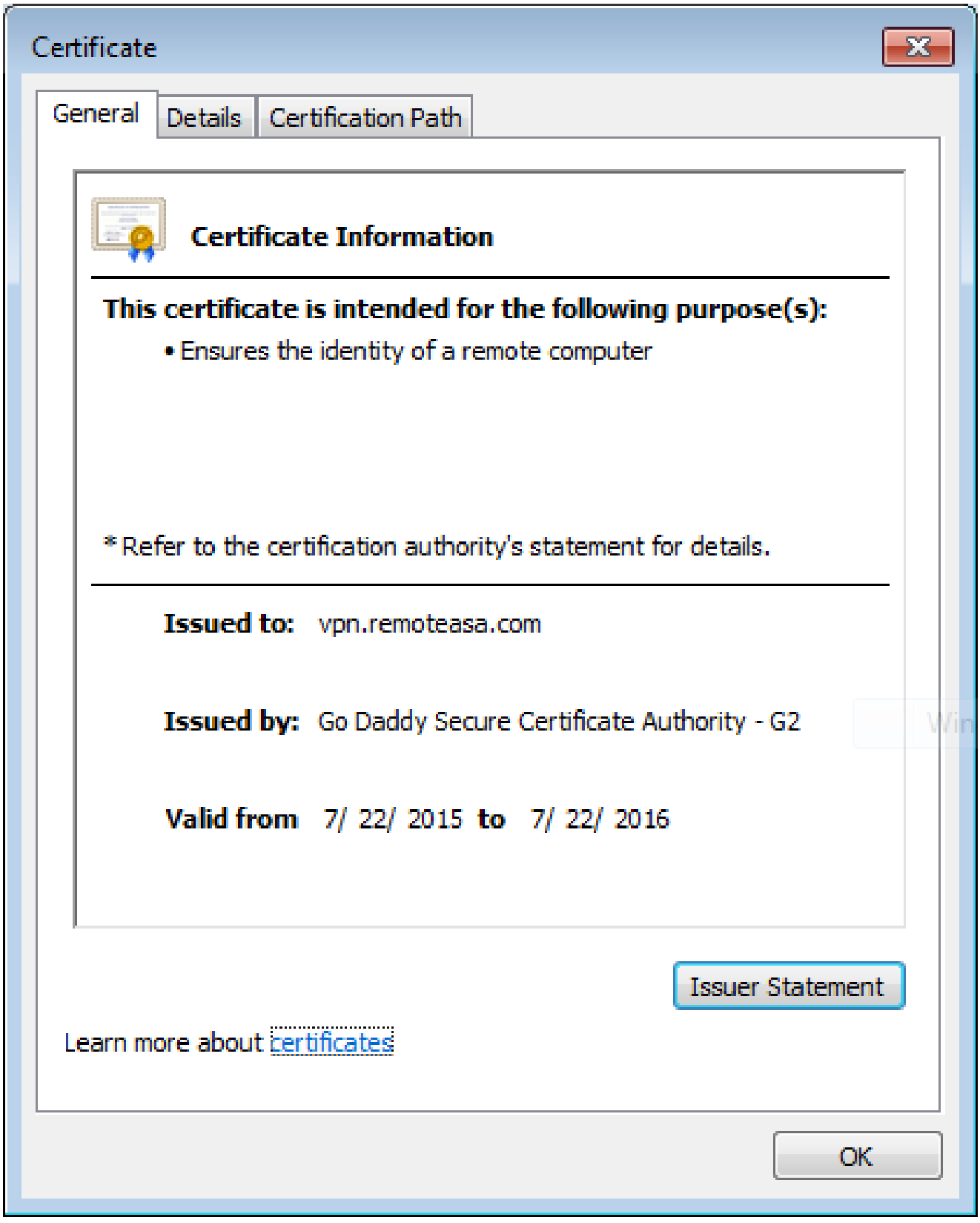
SSL-Trustpoint-1

```
...(and the rest of the Sub CA certificates till the Root CA)
```

웹 브라우저를 사용하여 WebVPN에 설치된 인증서 확인

WebVPN에서 새 인증서를 사용하는지 확인합니다.

1. 웹 브라우저를 통해 WebVPN 인터페이스에 연결합니다. 인증서를 요청하는 데 사용되는 FQDN과 함께 https://을 사용합니다(예: https:///(vpn.remoteasa.com)).
2. WebVPN 로그인 페이지의 오른쪽 아래 모서리에 나타나는 잠금 아이콘을 두 번 클릭합니다. 설치된 인증서 정보가 표시되어야 합니다.
3. 서드파티 벤더가 발급한 인증서와 일치하는지 확인하기 위해 내용을 검토합니다.

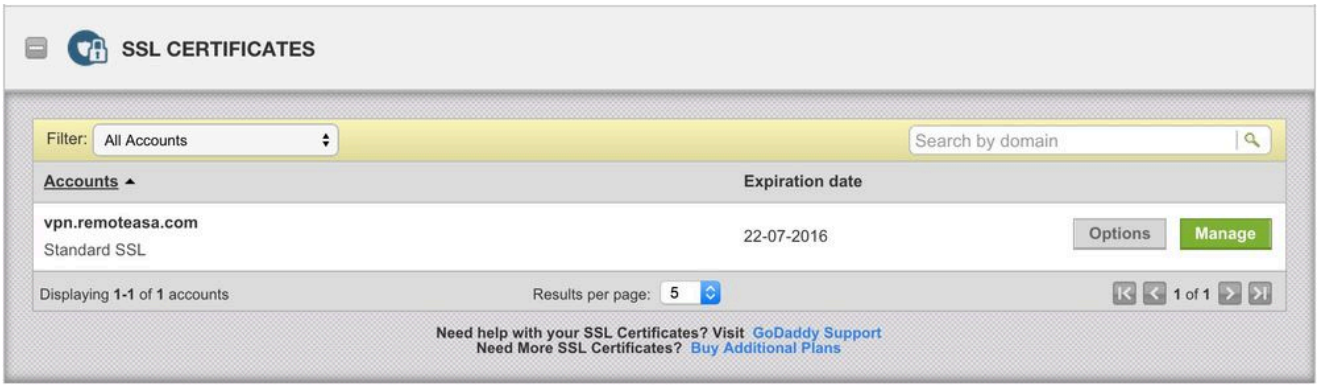


ASA에서 SSL 인증서 갱신

1. ASA, OpenSSL 또는 CA에서 기존 인증서와 동일한 속성으로 CSR을 재생성합니다. CSR 생성에 지정된 단계를 완료합니다.
2. CA에서 CSR을 제출하고 CA 인증서와 함께 PEM 형식(.pem, .cer, .crt)의 새 ID 인증서를 생성합니다. PKCS12 인증서의 경우 새 개인 키도 있습니다.

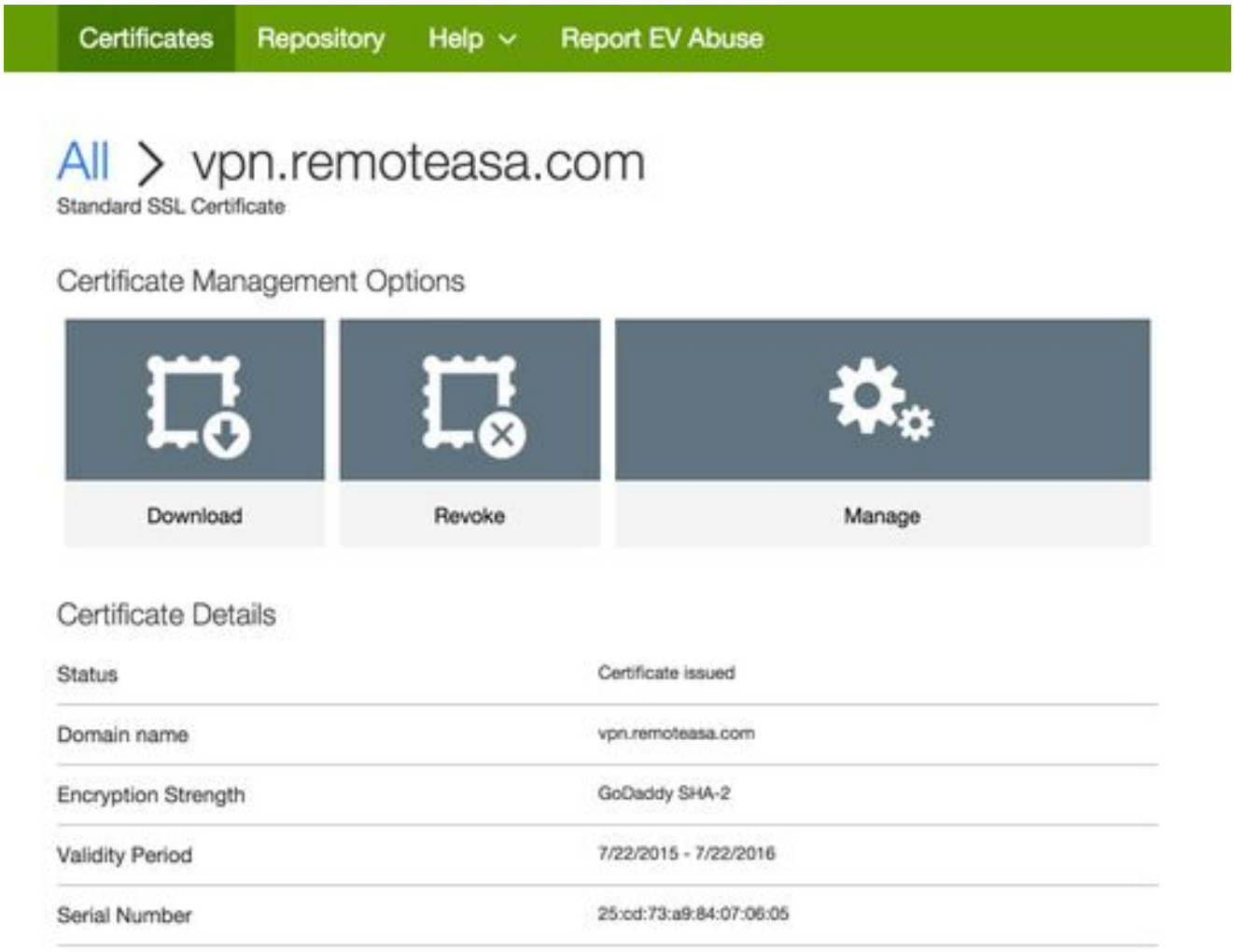
GoDaddy CA의 경우 생성된 새 CSR로 인증서를 다시 입력할 수 있습니다.

GoDaddyaccount(GoDaddyaccount)로 이동하고 SSL Certificates(SSL 인증서)에서 Manage(관리)를 클릭합니다.

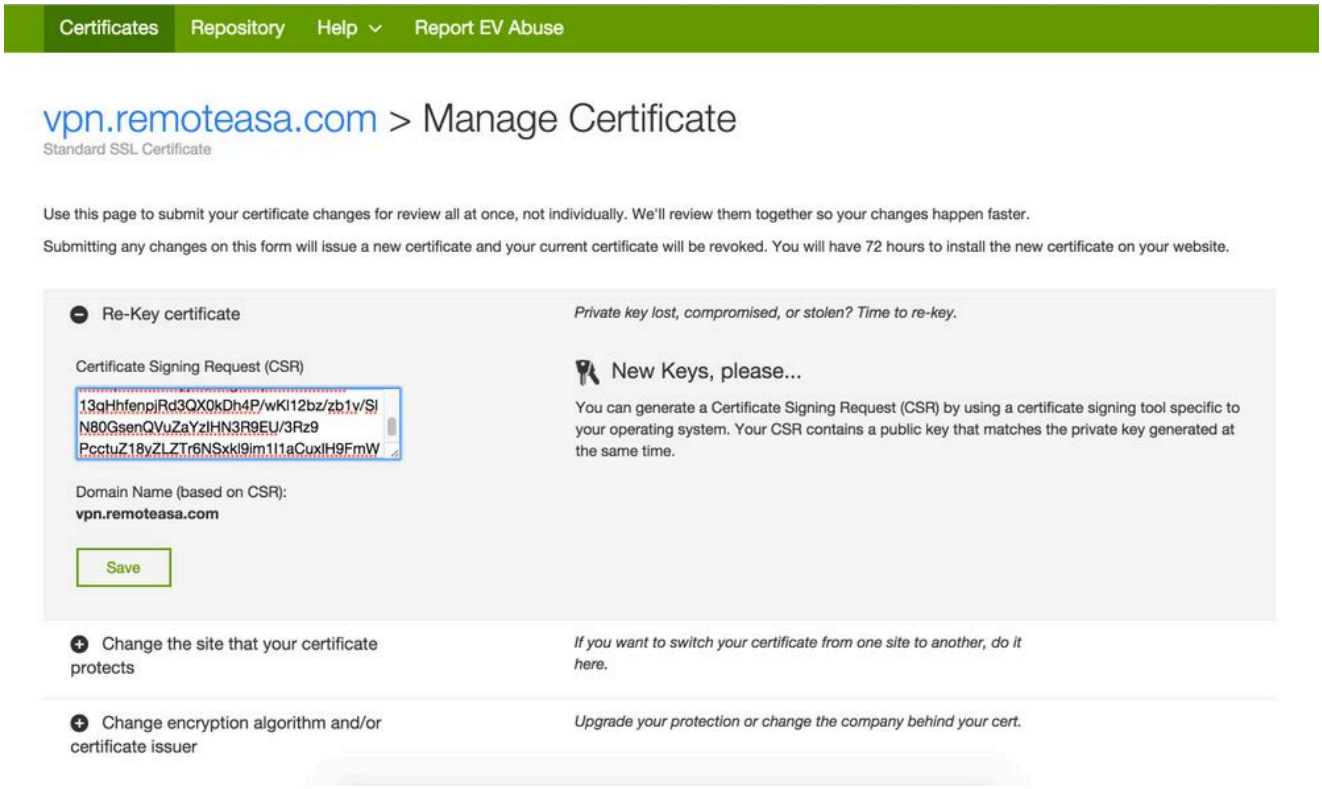


필요한 도메인 이름에 대해 View Status(상태 보기)를 클릭합니다.

인증서를 다시 키 지정하는 옵션을 제공하려면 Manage(관리)를 클릭합니다.



Re-Key certificate(인증서 키 재설정) 옵션을 확장하고 새 CSR을 추가합니다.



저장하고 다음 단계로 진행합니다. GoDaddy는 제공된 CSR을 기반으로 새 인증서를 발급합니다.

3. ASA의 SSL Certificate Installation(SSL 인증서 설치) 섹션에 표시된 대로 새 신뢰 지점에 새 인증서를 설치합니다.

자주 묻는 질문(FAQ)

1. ID 인증서를 한 ASA에서 다른 ASA로 전송하는 가장 좋은 방법은 무엇입니까?

키와 함께 인증서를 PKCS12 파일로 내보냅니다.

원래 ASA에서 CLI를 통해 인증서를 내보내려면 다음 명령을 사용합니다.

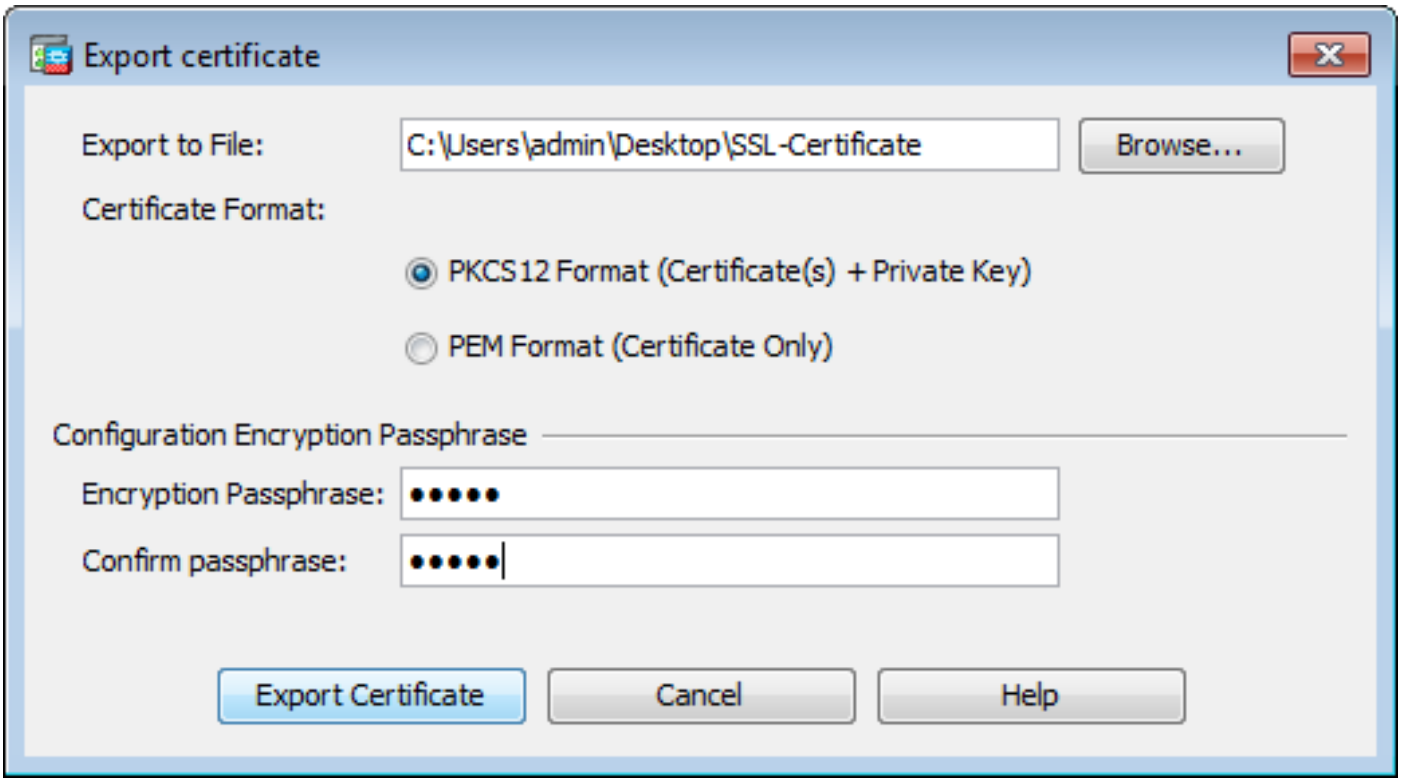
<#root>

ASA(config)#

crypto ca export

pkcs12

ASDM 구성:



CLI를 통해 대상 ASA로 인증서를 가져오려면 다음 명령을 사용합니다.

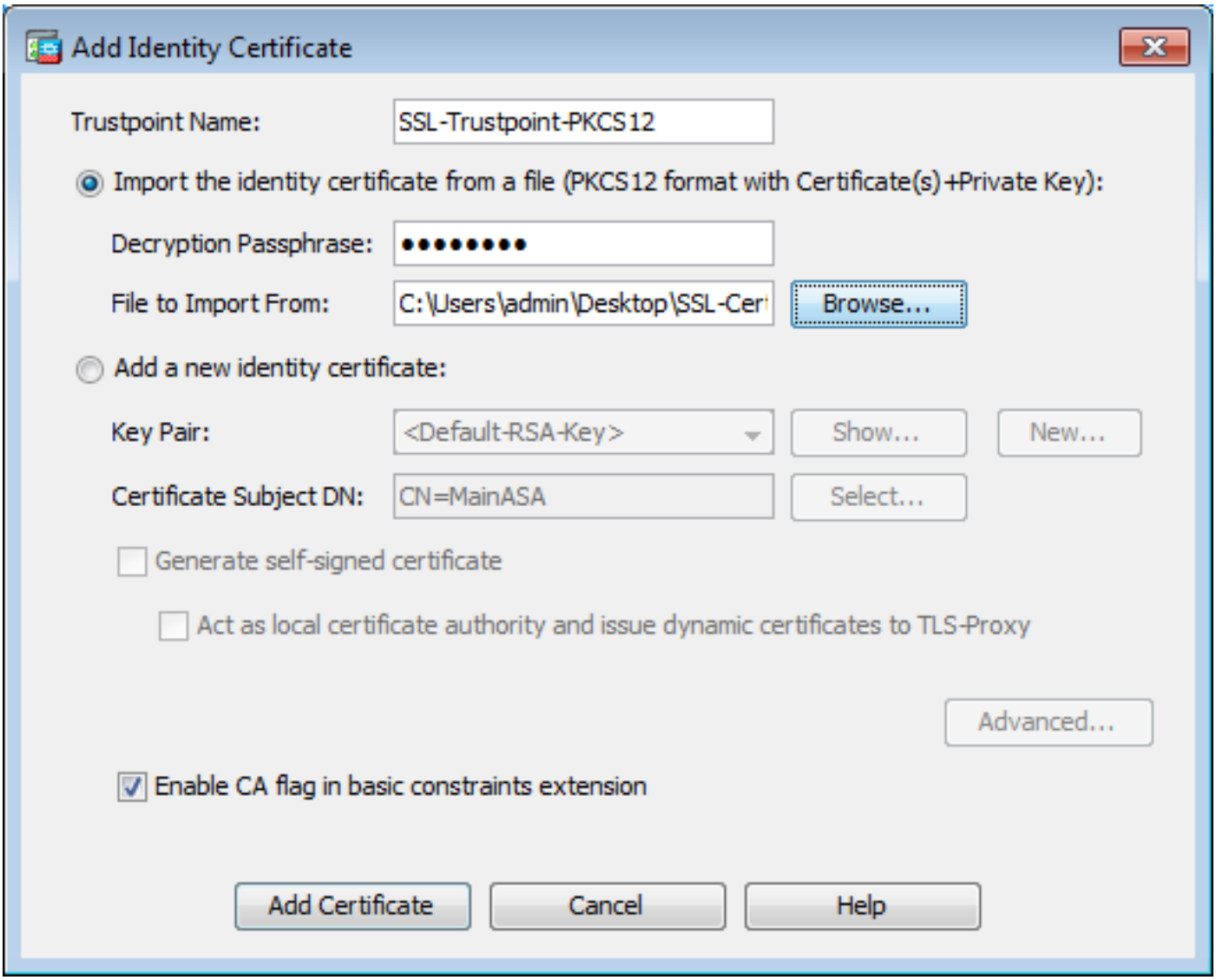
<#root>

ASA(config)#

crypto ca import

pkcs12

ASDM 구성:



이 작업은 ASDM의 백업/복원 기능을 통해서도 수행할 수 있으며 다음 단계를 수행합니다.

1. ASDM을 통해 ASA에 로그인하고 를 선택합니다**Tools > Backup Configuration.**
2. 모든 컨피그레이션 또는 ID 인증서만 백업합니다.
3. 대상 ASA에서 ASDM을 열고 다음을 선택합니다**Tools > Restore Configuration.**

2. VPN 부하 균형 ASA에 사용할 SSL 인증서를 생성하는 방법

VPN 로드 밸런싱 환경을 위해 SSL 인증서를 사용하여 ASA를 설정하는 데 사용할 수 있는 여러 방법이 있습니다.

1. 로드 밸런싱 FQDN을 DN으로 사용하고 각 ASA FQDN을 별도의 주체 대체 이름(SAN)으로 사용하는 단일 UCC(Unified Communications/Multiple Domains Certificate)를 사용합니다. 이러한 인증서를 지원하는 GoDaddy, Entrust, Comodo 및 기타 잘 알려진 CA가 있습니다. 이 방법을 선택할 때 ASA는 현재 여러 SAN 필드가 있는 CSR 생성을 지원하지 않습니다. 이 내용은 개선 사항 Cisco 버그 ID CSCso70867에 설명되어 있습니다. 이 경우 CSR을 생성하는 두 가지 옵션이 있습니다
   a. CLI 또는 ASDM을 통해 액세스합니다. CSR이 CA에 제출되면 CA 포털 자체에 있는 여러 SAN을 추가합니다.

b. OpenSSL을 사용하여 CSR을 생성하고 여러 SAN을 openssl.cnf 파일에 포함합니다.

CSR이 CA에 제출되고 인증서가 생성되면 이 PEM 인증서를 CSR을 생성한 ASA로 가져옵니다. 완료되면 이 인증서를 PKCS12 형식으로 다른 멤버 ASA로 내보내고 가져옵니다.

2. 와일드카드 인증서를 사용 합니다. 이는 UC 인증서와 비교할 때 덜 안전하고 유연한 방법입니다. CA가 UC 인증서를 지원하지 않는 경우 CSR은 CA에서 생성되거나 OpenSSL을 통해 생성됩니다. 여기서 FQDN은 *.domain.com 형식입니다. CSR이 CA에 제출되고 인증서가 생성되면 클러스터의 모든 ASA에 PKCS12 인증서를 가져옵니다.
3. 각 멤버 ASA 및 로드 밸런싱 FQDN에 대해 별도의 인증서를 사용합니다. 이것이 가장 효과가 낮은 해결책입니다. 각 개별 ASA에 대한 인증서는 이 문서에 표시된 대로 생성할 수 있습니다. VPN Loadbalancing FQDN에 대한 인증서는 하나의 ASA에서 작성되고 다른 ASA에 PKCS12 인증서로 내보내기 및 가져오기됩니다.

3. ASA 장애 조치 쌍의 기본 ASA에서 보조 ASA로 인증서를 복사해야 합니까?

스테이트풀 장애 조치가 구성된 경우 인증서가 ASA 간에 동기화되므로 기본 ASA에서 보조 ASA로 인증서를 수동으로 복사할 필요가 없습니다. 장애 조치를 처음 설정할 때 인증서가 스탠바이 디바이스에 표시되지 않는 경우, 동기화를 강제하기 위해 write standby 명령을 실행합니다.

4. ECDSA 키를 사용하는 경우 SSL 인증서 생성 프로세스가 다릅니까?

컨피그레이션의 유일한 차이점은 RSA 키 쌍 대신 ECDSA 키 쌍이 생성되는 키 쌍 생성 단계입니다. 나머지 단계는 동일하게 유지됩니다. ECDSA 키를 생성하는 CLI 명령은 다음과 같습니다.

<#root>

```
 MainASA(config)#
```

cry key generate ecdsa label SSL-Keypair elliptic-curve 256

```
INFO: The name for the keys will be: SSL-Keypair
Keypair generation process begin. Please wait...
```

문제 해결

명령 문제 해결

이러한 debug 명령은 SSL 인증서 설치 실패 시 CLI에서 수집됩니다.

debug crypto ca 255

debug crypto ca messages 255

crypto ca 트랜잭션 디버그 255

일반적인 문제

9.4(1) 이상의 ASA에서 외부 인터페이스에 유효한 서드파티 SSL 인증서가 있는 신뢰할 수 없는 인증서 경고

해결 방법: 이 문제는 RSA 키 쌍을 인증서와 함께 사용할 때 나타납니다. 9.4(1) 이후의 ASA 버전에서는 모든 ECDSA 및 RSA 암호가 기본적으로 활성화되어 있으며 가장 강력한 암호(일반적으로 ECDSA 암호)가 협상에 사용됩니다. 이 경우 ASA는 현재 구성된 RSA 기반 인증서 대신 자체 서명 인증서를 표시합니다. RSA 기반 인증서가 인터페이스에 설치되고 Cisco 버그 ID CSCuu02848에 의해 추적되는 경우 동작을 변경할 수 있는 향상된 기능이 있습니다.

권장 조치: 다음 CLI 명령으로 ECDSA 암호를 비활성화합니다.

```
ssl cipher tlsv1.2 custom "AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:
DES-CBC3-SHA:DES-CBC-SHA:RC4-SHA:RC4-MD5"
```

또는 ASDM을 사용하여 로 이동하여**Configuration** > **Remote Access VPN** > **Advanced**선택합니다**SSL Settings.** Encryption(암호화) 섹션에서 tlsv1.2 Cipher version(tlsv1.2 암호 버전)을 선택하고 사용자 지정 문자열 AES256-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA:RC4-SHA:RC4-MD5로 편집합니다

부록

부록 A: ECDSA 또는 RSA

ECDSA 알고리즘은 ECC(Elliptic Curve Cryptography)의 일부로서 타원 곡선의 방정식을 사용하여 공개 키를 생성하는 반면, RSA 알고리즘은 두 개의 소수점과 더 작은 수의 곱을 사용하여 공개 키를 생성합니다. 즉, ECDSA를 사용할 경우 RSA와 동일한 수준의 보안을 제공할 수 있지만 키가 더 작습니다. 이렇게 하면 계산 시간이 줄어들고 ECDSA 인증서를 사용하는 사이트의 연결 시간이 늘어납니다.

Next Generation Cryptography 및 ASA에 대한 문서는 보다 심층적인 정보를 제공합니다.

부록 B: OpenSSL을 사용하여 ID 인증서, CA 인증서 및 개인 키에서 PKCS12 인증서 생성

1. 이 프로세스가 실행되는 시스템에 OpenSSL이 설치되어 있는지 확인합니다. Mac OSX 및 GNU/Linux 사용자의 경우 기본적으로 설치됩니다.
2. 올바른 디렉터리로 전환합니다.

   Windows: 기본적으로 유틸리티는 C:\Openssl\bin에 설치됩니다. 이 위치에서 명령 프롬프트를 엽니다.

   Mac OSX/Linux의 경우: PKCS12 인증서를 만드는 데 필요한 디렉토리에서 Terminal(터미널) 창을 엽니다.

3. 이전 단계에서 언급한 디렉토리에서 개인 키(privateKey.key), ID 인증서(certificate.crt) 및 루

트 CA 인증서 체인(CACert.crt) 파일을 저장합니다.

개인 키, ID 인증서 및 루트 CA 인증서 체인을 PKCS12 파일에 결합합니다. PKCS12 인증서를 보호하기 위한 암호를 입력합니다.

```
strong> openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in certificate.crt -cer
```

4. 생성된 PKCS12 인증서를 Base64 인코딩 인증서로 변환합니다.
<#root>

```
openssl base64 -in certificate.pfx -out certificate.p12
```

그런 다음 마지막 단계에서 생성된 인증서를 가져와 SSL과 함께 사용합니다.

관련 정보

- ASA 9.x 컨피그레이션 가이드 - 디지털 인증서 구성
- ASA에서 ASDM을 사용하여 Microsoft Windows CA에서 디지털 인증서를 얻는 방법
- 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.