ASA 8.x:ASDM을 사용하여 SSL 인증서 갱신 및 설치

목차

소개

이 문서의 절차는 예시이며 모든 인증서 공급업체 또는 자체 루트 인증서 서버에서 지침으로 사용할 수 있습니다.특정 인증서 매개 변수 요구 사항은 인증서 공급업체에서 요구하는 경우가 있지만 이 문서는 SSL 인증서를 갱신하고 8.0 소프트웨어를 사용하는 ASA에 설치하는 데 필요한 일반적인 단계를 제공하기 위한 것입니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 절차는 ASDM 버전 6.0(2) 이상의 ASA 버전 8.x와 관련이 있습니다.

이 문서의 절차는 인증서가 설치되어 있고 SSL VPN 액세스에 사용되는 유효한 구성을 기반으로 합니다.이 절차는 현재 인증서가 삭제되지 않는 한 네트워크에 영향을 미치지 않습니다.이 절차는 원래 루트 CA를 발급한 동일한 루트 인증서를 사용하여 현재 인증서에 대해 새 CSR을 발행하는 방법에 대한 단계별 프로세스입니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

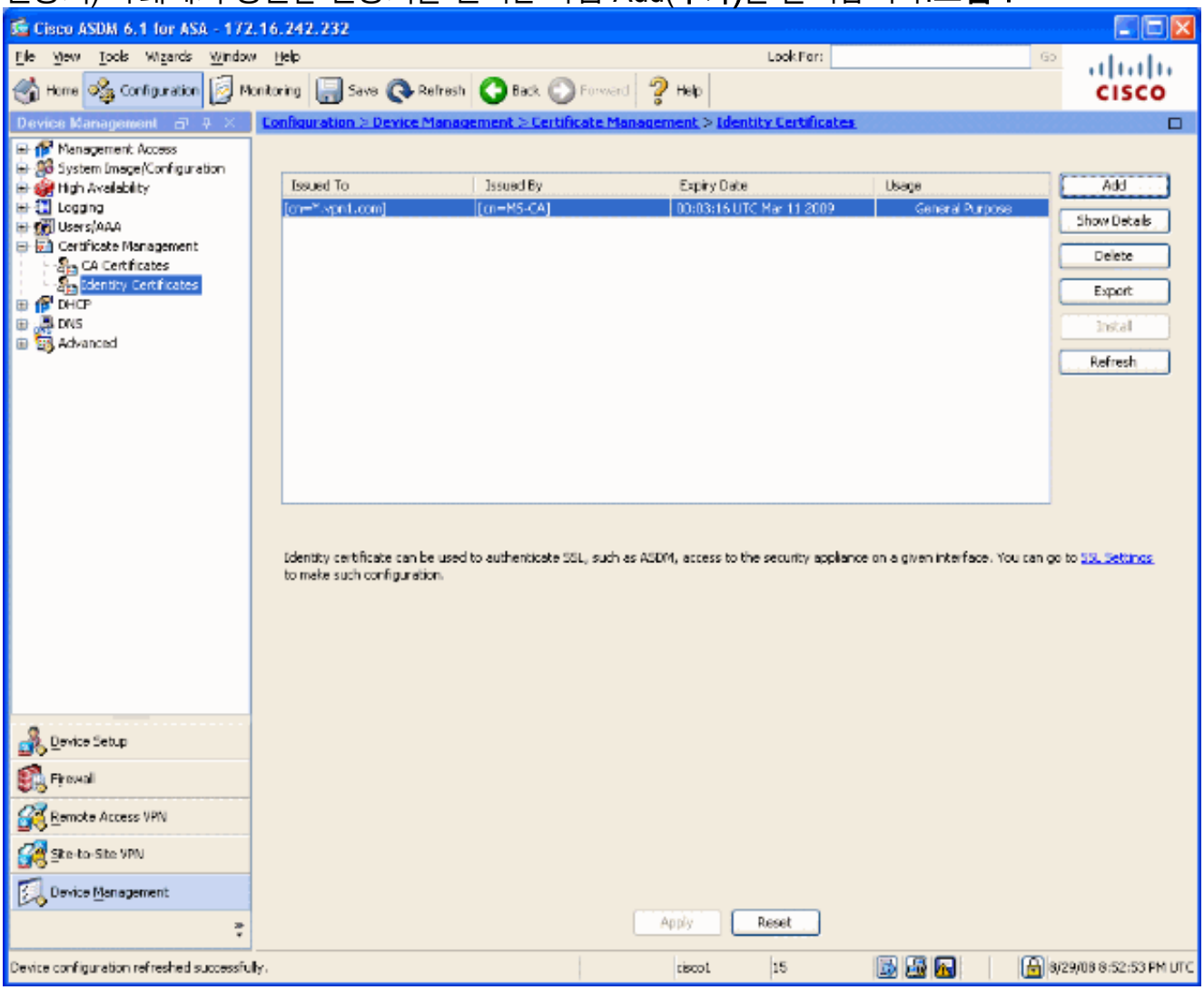
표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

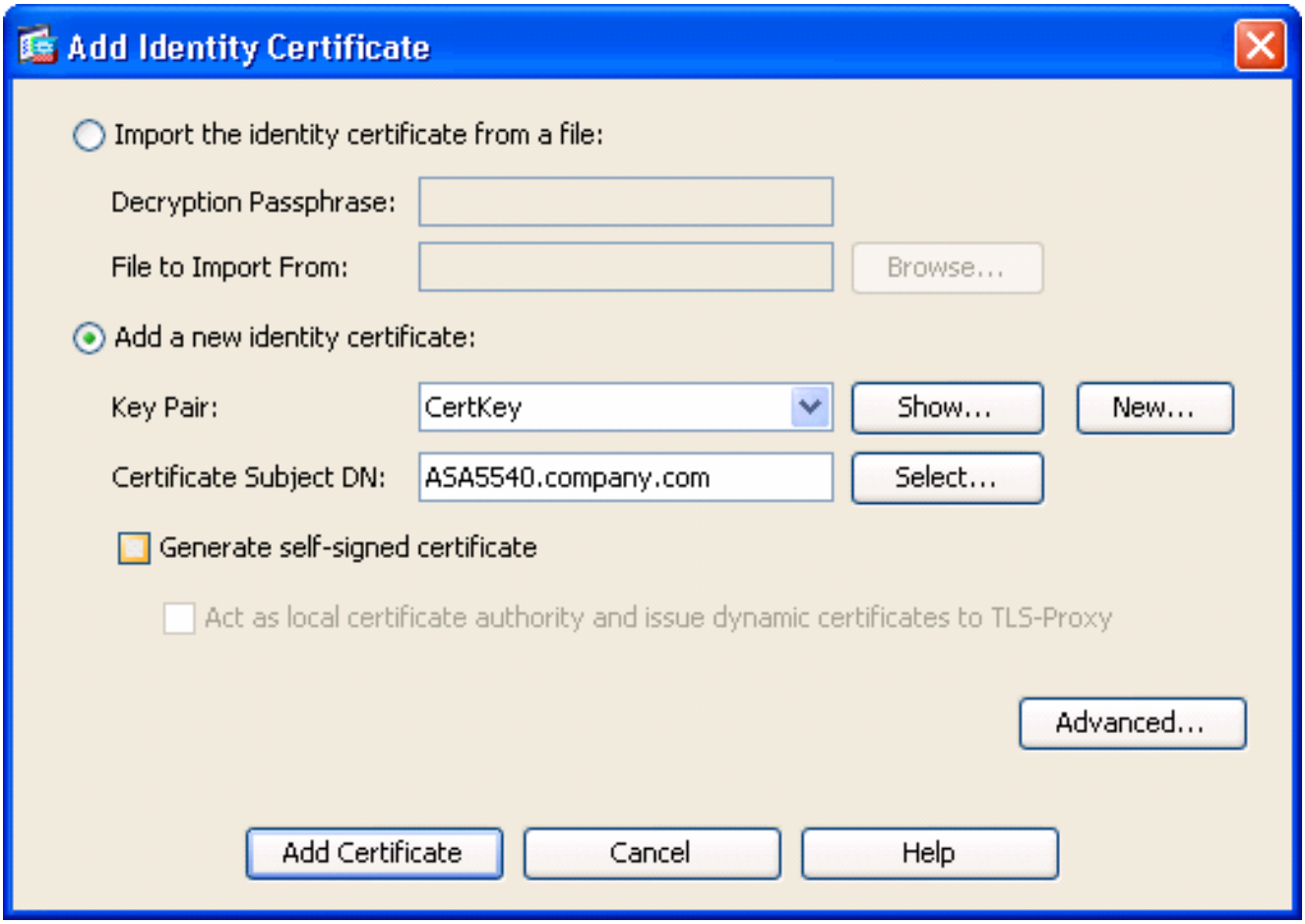
절차

다음 단계를 완료하십시오.

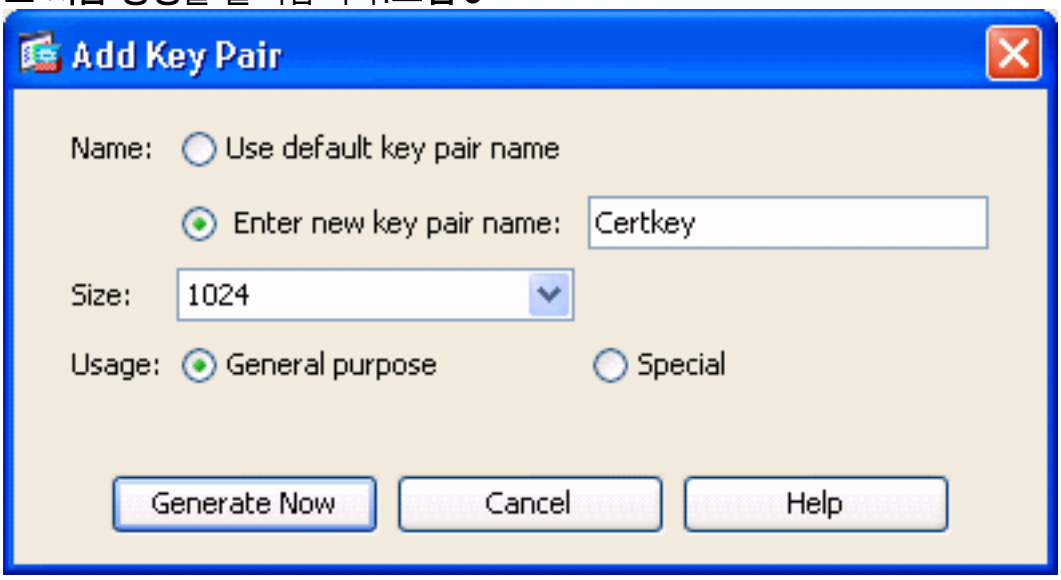
1. Configuration(컨피그레이션) > Device Management(디바이스 관리) > Identity Certificates(ID 인증서) 아래에서 갱신할 인증서를 선택한 다음 Add(**추가**)를 클릭합니다.**그림 1**



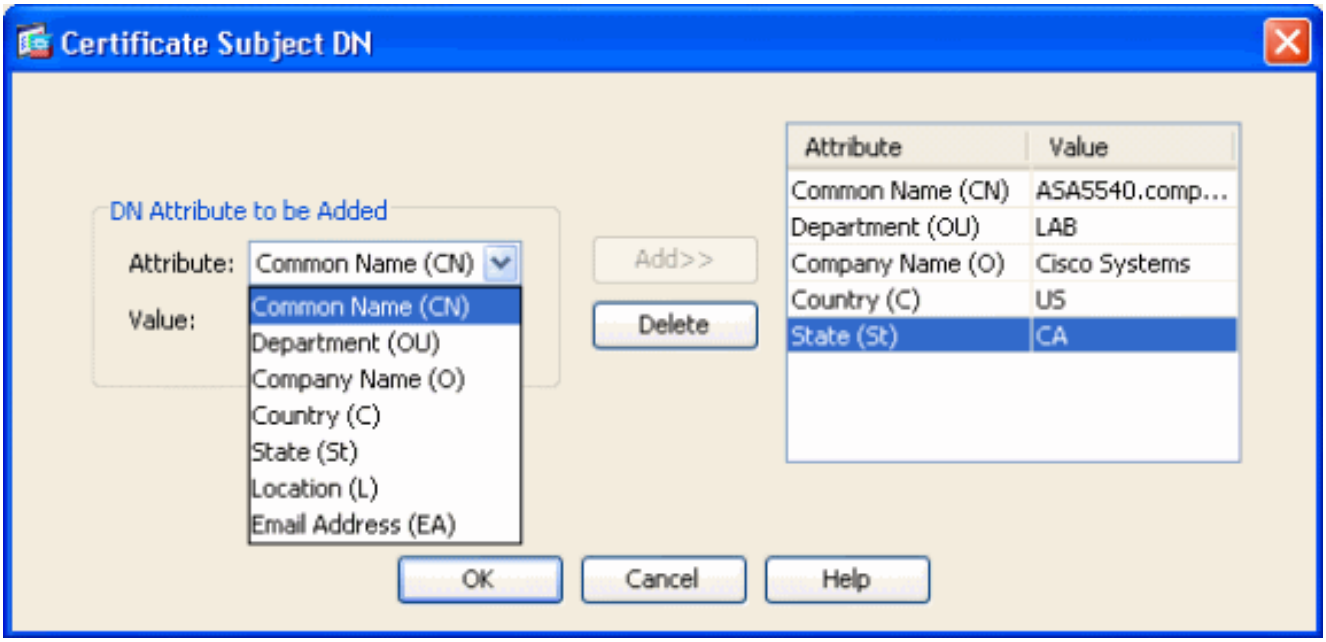
2. Add Identity Certificate(ID 인증서 추가)에서 **Add a new identity certificate(새 ID 인증서 추가)** 라디오 버튼을 선택하고 드롭다운 메뉴에서 키 쌍을 선택합니다.**참고:** <Default-RSA-Key>는 사용하지 않는 것이 좋습니다. SSH 키를 다시 생성하면 인증서가 무효화됩니다.RSA 키가 없는 경우 Steps a 및 b를 완료합니다.그렇지 않으면 3단계로 진행합니다.**그림 2**



(선택 사항) RSA 키를 아직 구성하지 않은 경우 다음 단계를 완료하고, 그렇지 않은 경우 3단계로 건너뜁니다.새로 **만들기...를 클릭합니다..새 키 쌍 이름 입력** 필드에 키 쌍 이름을 입력하고 **지금 생성**을 클릭합니다.**그림 3**



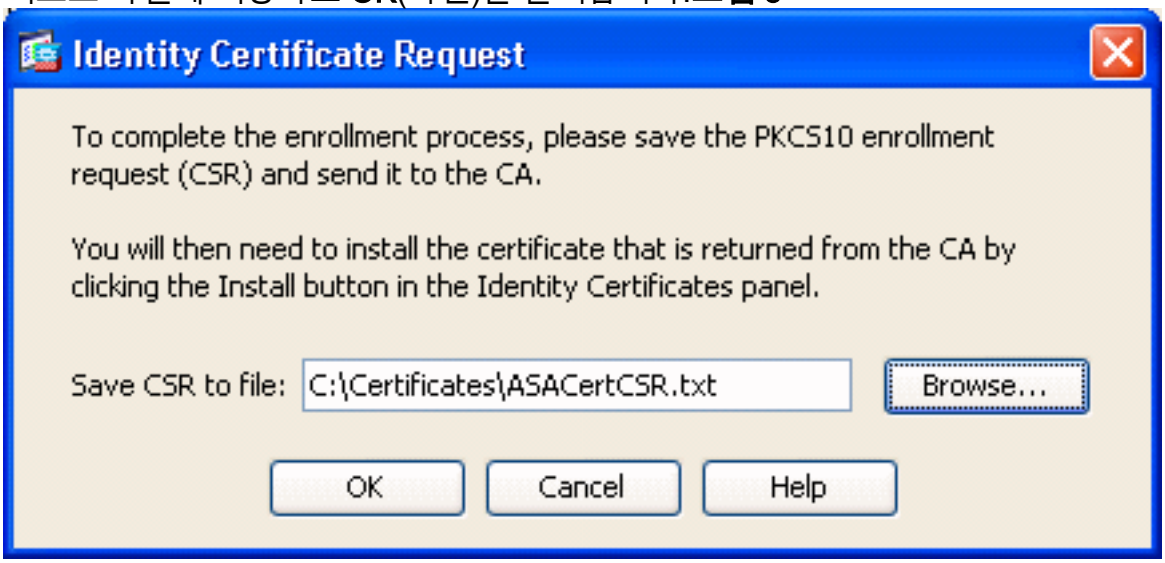
3. 선택을 **클릭합니다**.
4. 그림 4와 같이 적절한 인증서 특성을 입력합니다. 완료되면 **확인**을 클릭합니다.그런 다음 Add **Certificate를 클릭합니다.그림 4**



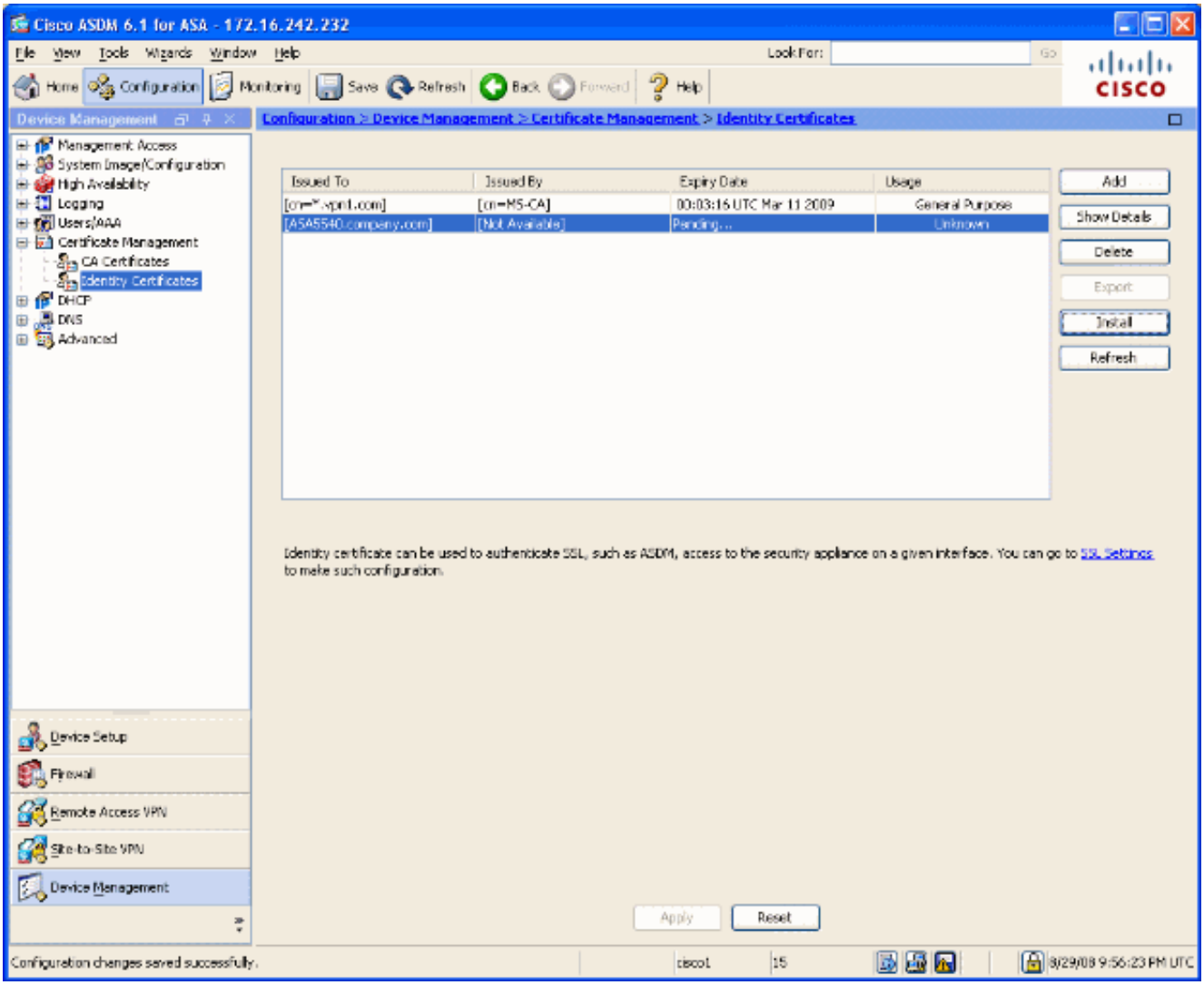
CLI 출력:

```
crypto ca trustpoint ASDM_TrustPoint0
        keypair CertKey
        id-usage ssl-ipsec
        fqdn 5540-uwe
        subject-name CN=ASA5540.company.com,OU=LAB,O=Cisco ystems,C=US,St=CA
        enrollment terminal
 crypto ca enroll ASDM_TrustPoint0
```

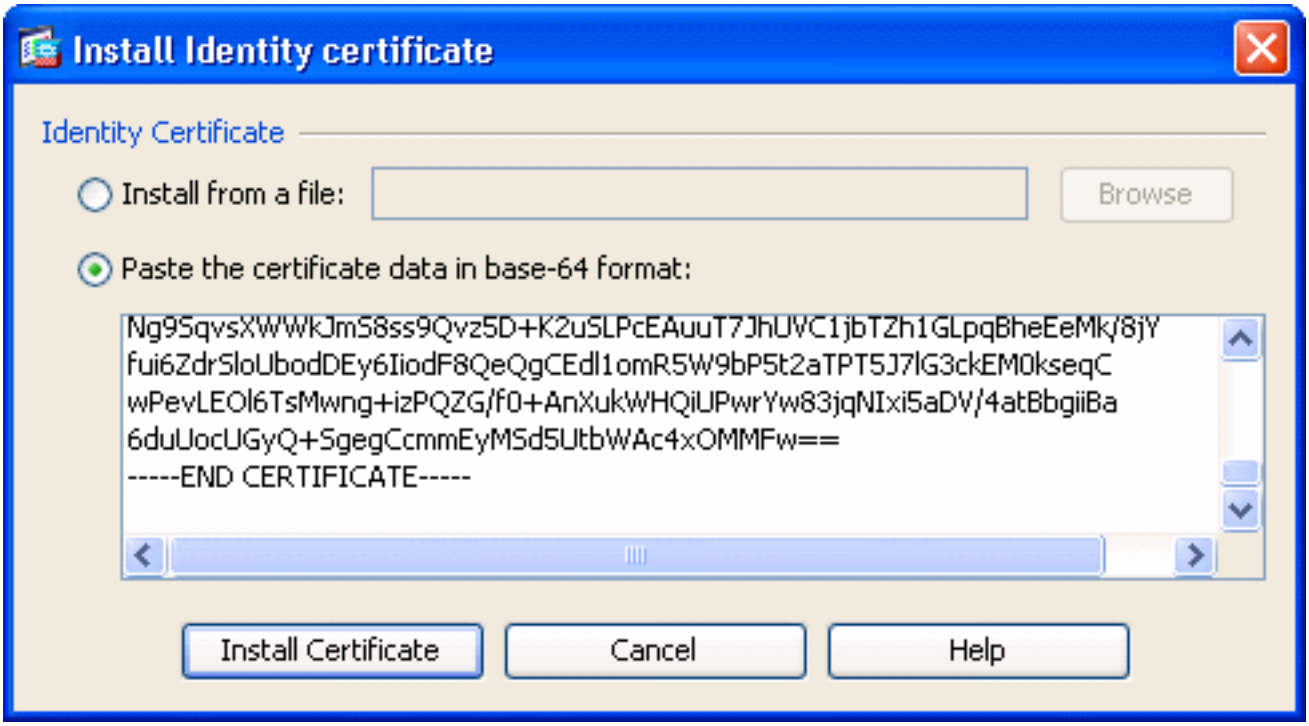
5. Identity **Certificate Request(ID 인증서 요청)** 팝업 창에서 CSR(Certificate Signing Request)을 텍스트 파일에 저장하고 **OK**(확인)를 클릭합니다.**그림 5**



6. (선택 사항) 그림 6과 같이 ASDM에서 CSR이 보류 중인지 확인합니다.**그림 6**



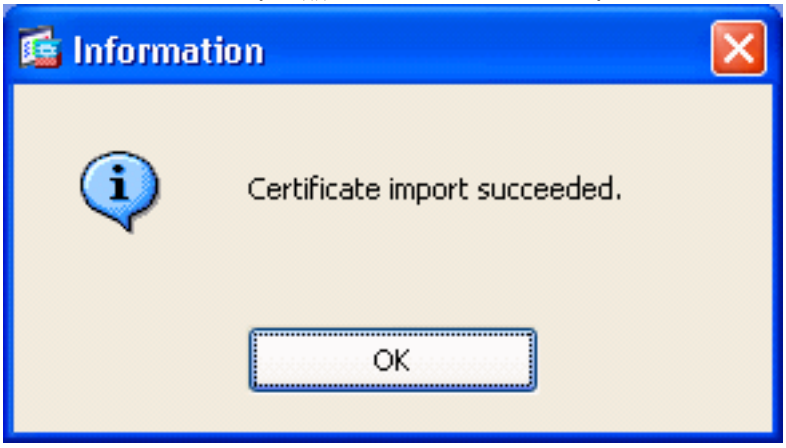
7. 서버에서 인증서를 발급하는 인증서 관리자에게 인증서 요청을 제출합니다.이는 웹 인터페이스, 이메일 또는 루트 CA 서버에 직접 연결하여 인증서 문제 프로세스를 수행할 수 있습니다.
8. 갱신된 인증서를 설치하려면 다음 단계를 완료하십시오.그림 6과 같이 Configuration > Device Management > Identity Certificates 아래에서 보류 중인 인증서 요청을 선택하고 **Install**을 클릭합니다.Install Identity Certificate(ID 인증서 설치) 창에서 **Paste the certificate data in base-64 format** 라디오 버튼**을** 선택하고 Install Certificate(인증서 **설치)**를 클릭합니다.**참고:** 또는 인증서가 텍스트 기반 파일 또는 전자 메일이 아닌 .cer 파일로 발급된 경우 **파일에서 설치를** 선택하고 PC**에서** 적절한 파일을 찾은 다음 **Install ID certificate file(ID 인증서 파일 설치)을 클릭한** 다음 **Install Certificate(인증서 설치)를** 클릭할 수도 있습니다.**그림 7**



CLI 출력:

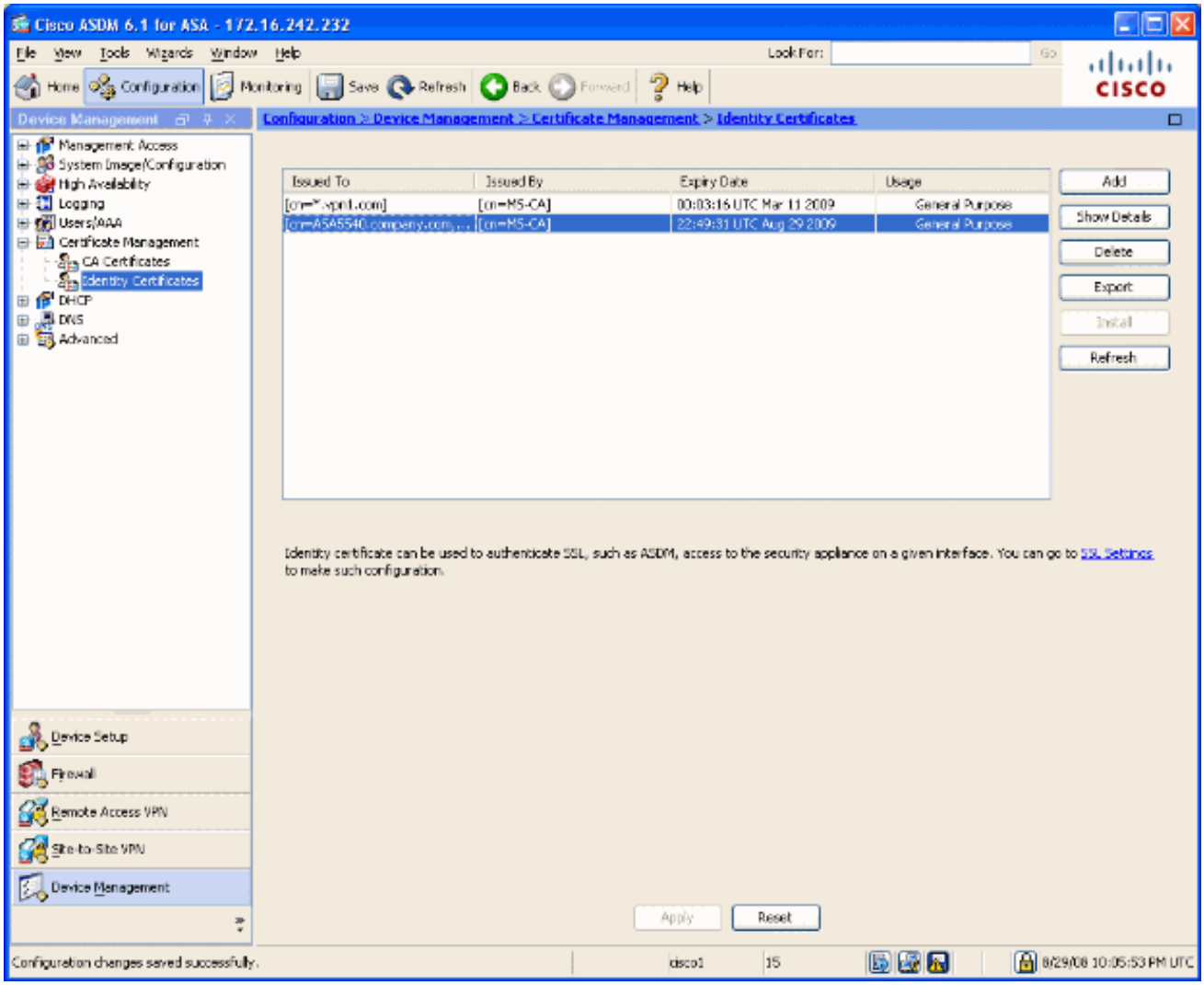
```
crypto ca import ASDM_TrustPoint0 certificate
WIID2DCCAsCgAwIBAgIKYb9wewAAAAAAJzANBgkqhkiG9w0BAQUFADAQMQ
!--- output truncated wPevLEOl6TsMwng+izPQZG/f0+AnXukWHQiUPwrYw83jqNIxi5aDV/4atBbgiiBa
6duUocUGyQ+SgegCcmmEyMSd5UtbWAc4xOMMFw== quit
```

9. 인증서가 성공적으로 설치되었음을 확인하는 창이 나타납니다."확인"을 클릭하여 확인합니다

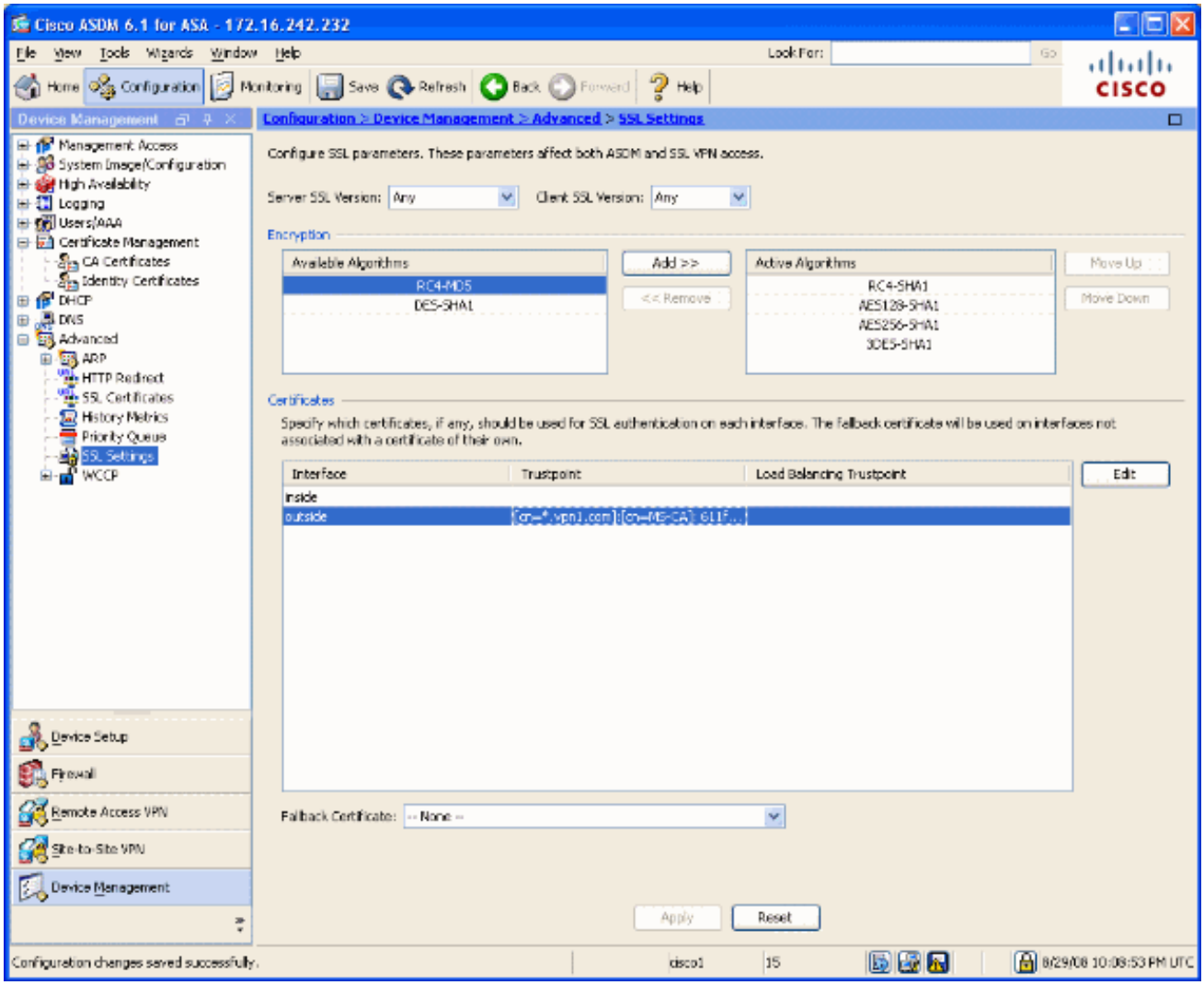


.**그림 8**

10. 새 인증서가 Identity Certificates 아래에 나타나게 합니다.**그림 9**



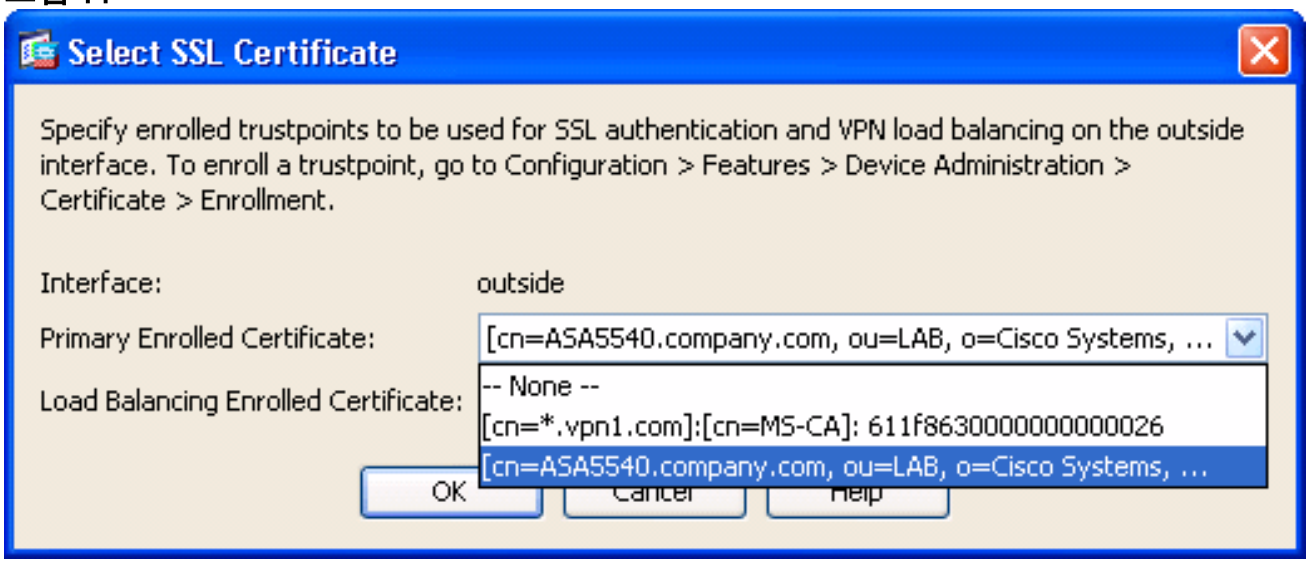
11. 새 인증서를 인터페이스에 바인딩하려면 다음 단계를 완료합니다.그림 10**과 같이 Configuration > Device Management > Advanced > SSL Settings**를 선택합니다 .Certificates(인증서)에서 인터페이스를 선택하고 Edit(**편집**)를 클릭합니다.**그림 10**



12. 드롭다운 메뉴에서 새 인증서를 선택하고 **확인**을 클릭한 다음 **적용**을 클릭합니다.

```
ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1
ssl trust-point ASDM_TrustPoint0 outside
```

그림 11



13. ASDM 또는 CLI에서 컨피그레이션을 저장합니다.

다음을 확인합니다.

다음 샘플 출력에 표시된 대로 새 인증서가 ASA에 올바르게 설치되었는지 확인하려면 CLI 인터페이스를 사용할 수 있습니다.

```
ASA(config)#show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 61bf707b000000000027
  Certificate Usage: General Purpose
  Public Key Type: RSA (1024 bits)
  Issuer Name:
    cn=MS-CA
  Subject Name:
    cn=ASA5540.company.com !---new certificate ou=LAB o=Cisco Systems st=CA c=US CRL
Distribution Points: [1] http://win2k3-base1/CertEnroll/MS-CA.crl [2] file://\\win2k3-
base1\CertEnroll\MS-CA.crl Validity Date: start date: 22:39:31 UTC Aug 29 2008 end date:
22:49:31 UTC Aug 29 2009 Associated Trustpoints: ASDM_TrustPoint0 CA Certificate Status:
Available Certificate Serial Number: 211020a79cfd96b34ba93f3145d8e571 Certificate Usage:
Signature Public Key Type: RSA (2048 bits) Issuer Name: cn=MS-CA Subject Name: cn=MS-CA !---
'old' certificate CRL Distribution Points: [1] http://win2k3-base1/CertEnroll/MS-CA.crl [2]
file://\\win2k3-base1\CertEnroll\MS-CA.crl Validity Date: start date: 00:26:08 UTC Jun 8 2006
end date: 00:34:01 UTC Jun 8 2011 Associated Trustpoints: test Certificate Status: Available
Certificate Serial Number: 611f8630000000000026 Certificate Usage: General Purpose Public Key
Type: RSA (1024 bits) Issuer Name: cn=MS-CA Subject Name: cn=*.vpn1.com CRL Distribution Points:
[1] http://win2k3-base1/CertEnroll/MS-CA.crl [2] file://\\win2k3-base1\CertEnroll\MS-CA.crl
Validity Date: start date: 23:53:16 UTC Mar 10 2008 end date: 00:03:16 UTC Mar 11 2009
Associated Trustpoints: test ASA(config)#
```

문제 해결

(선택 사항) CLI에서 올바른 인증서가 인터페이스에 적용되었는지 확인합니다.

```
ASA(config)#show running-config ssl
ssl trust-point ASDM_TrustPoint0 outside
!--- Shows that the correct trustpoint is tied to the outside interface that terminates SSL VPN.
ASA(config)#
```

한 ASA에서 다른 ASA로 SSL 인증서를 복사하는 방법

내보내기 가능한 키를 생성한 경우 이 작업을 수행할 수 있습니다.인증서를 PKCS 파일로 내보내야 합니다.여기에는 연결된 모든 키 내보내기가 포함됩니다.

CLI를 통해 인증서를 내보내려면 이 명령을 사용합니다.

```
ASA(config)#crypto ca export
```

참고: Passphrase - pkcs12 파일을 보호하는 데 사용됩니다.

CLI를 통해 인증서를 가져오려면 다음 명령을 사용합니다.

```
SA(config)#crypto ca import
```

참고: 이 패스프레이즈는 파일을 내보낼 때와 동일해야 합니다.

ASA 장애 조치 쌍에 대해 ASDM을 통해 이를 수행할 수도 있습니다.다음 단계를 수행하여 다음을 수행합니다.

1. ASDM을 통해 기본 ASA에 로그인하고 **Tools—> Backup Configuration을** 선택합니다.
2. 모든 것을 백업하거나 인증서만 백업할 수 있습니다.
3. 대기 모드에서 ASDM을 열고 **Tools —> Restore Configuration을** 선택합니다.

관련 정보

- Cisco ASA(Adaptive Security Appliance) 지원 페이지
- ASA 8.x Manually Install third Party Vendor Certificates for use with WebVPN Configuration 예
- 기술 지원 및 문서 – Cisco Systems