

CLI로 관리되는 ASA에 인증서 설치 및 갱신

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[인증서 설치](#)

[자체 서명 인증서 등록](#)

[CSR\(Certificate Signing Request\)에 의한 등록](#)

[PKCS12 등록](#)

[인증서 갱신](#)

[자체 서명 인증서 갱신](#)

[CSR\(Certificate Signing Request\)로 등록된 인증서 갱신](#)

[PKCS12 갱신](#)

[관련 정보](#)

소개

이 문서에서는 CLI로 관리되는 Cisco ASA Software에서 특정 유형의 인증서를 요청, 설치, 신뢰 및 갱신하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

- ASA(Adaptive Security Appliance)에 올바른 클록 시간, 날짜 및 표준 시간대가 있는지 확인합니다. 인증서 인증에서는 NTP(Network Time Protocol) 서버를 사용하여 ASA의 시간을 동기화하는 것이 좋습니다. 관련 정보를 참조하십시오.
- CSR(Certificate Signing Request)을 사용하는 인증서를 요청하려면 신뢰할 수 있는 내부 또는 서드파티 CA(Certificate Authority)에 액세스해야 합니다. 서드파티 CA 벤더의 예로는 Entrust, Geotrust, GoDaddy, Thawte, VeriSign 등이 있습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ASAv 9.18.1
- PKCS12 생성에는 OpenSSL이 사용됩니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.


배경 정보

이 문서에서 다루는 인증서의 유형은 CLI(Command Line Interface)로 관리되는 Cisco Adaptive Security Appliance Software에서 자체 서명 인증서, 타사 인증 기관에서 서명한 인증서 또는 내부 CA입니다.

인증서 설치

자체 서명 인증서 등록

1. (선택 사항) 특정 키 크기로 명명된 키 쌍을 만듭니다.

 참고: 기본적으로 Default-RSA-Key라는 이름과 2048의 크기를 갖는 RSA 키가 사용됩니다. 그러나 각 인증서에서 동일한 개인/공용 키 쌍을 사용하지 않도록 고유한 이름을 사용하는 것이 좋습니다.

```
<#root>
ASAv(config)#
crypto key generate rsa label
    SELF-SIGNED-KEYPAIR
modulus
    2048
INFO: The name for the keys will be: SELF-SIGNED-KEYPAIR
Keypair generation process begin. Please wait...
```

생성된 키 쌍을 명령과 함께 볼 수 있습니다 `show crypto key mypubkey rsa`.

```
<#root>
ASAv#
show crypto key mypubkey rsa

(...)
Key pair was generated at: 14:52:49 CEDT Jul 15 2022

Key name:
    SELF-SIGNED-KEYPAIR
Usage: General Purpose Key

Key size
```

(bits): 2048
Storage: config
Key Data:

```
30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
...
59dcd7d7 c3ee77f5 bbd0988d 515e390e b8d95177 dfaf6b94 a9df474b 1ec3b4a4
af020301 0001
```

2. 특정 이름으로 신뢰 지점을 만듭니다. 등록 유형을 자체로 구성합니다.

```
<#root>
```

```
ASAv(config)#
```


```
crypto ca trustpoint
```

```
SELF-SIGNED
```

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

```
enrollment self
```

3. FQDN(Fully Qualified Domain Name) 및 주체 이름을 구성합니다.

 주의: FQDN 매개변수는 인증서가 사용되는 ASA 인터페이스의 FQDN 또는 IP 주소와 일치해야 합니다. 이 매개변수는 인증서의 SAN(주체 대체 이름)을 설정합니다.

```
<#root>
```

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

```
fqdn
```

```
asavpn.example.com
```

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

```
subject-name
```

```
CN=
```

```
asavpn.example.com,O=Example Inc,C=US,St=California,L=San Jose
```

4. (선택 사항) 1단계에서 생성한 키 쌍 이름을 구성합니다. 기본 키 쌍을 사용하는 경우에는 필요하지 않습니다.

```
<#root>
```

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

```
keypair
```

```
SELF-SIGNED-KEYPAIR
```

```
ASAv(config-ca-trustpoint)# exit
```

5. 신뢰 지점을 등록하고 인증서를 생성합니다.

```
<#root>
```

```
ASAv(config)#
```

```
crypto ca enroll
```

```
SELF-SIGNED
```

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

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

```
yes
```

```
% The fully-qualified domain name in the certificate will be: asa.example.com  
% Include the device serial number in the subject name? [yes/no]:
```

```
no
```

```
Generate Self-Signed Certificate? [yes/no]:
```

```
yes
```

```
ASAv(config)#
```

```
exit
```

6. 완료되면 새 자체 서명 인증서를 명령과 함께 볼 수 있습니다 `show crypto ca certificates`

```
.
```

```
ASAv# show crypto ca certificates SELF-SIGNED
```

```
Certificate
```

```
Status: Available
```

```
Certificate Serial Number: 62d16084
```

```
Certificate Usage: General Purpose
```

```
Public Key Type: RSA (2048 bits)
```

```
Signature Algorithm: RSA-SHA256
```

```
Issuer Name:
```

```
unstructuredName=asa.example.com
```

```
L=San Jose
```

```
ST=California
```

```
C=US
```

```
O=Example Inc
```

```
CN=asa.example.com
```

```
Subject Name:
```

```
unstructuredName=asa.example.com
```

```
L=San Jose
```

```
ST=California
```

```
C=US
```

```
O=Example Inc
```

```
CN=asa.example.com
```

```
Validity Date:
```

```
start date: 15:00:58 CEDT Jul 15 2022
```


```
end date: 15:00:58 CEDT Jul 12 2032
```

```
Storage: config
```

```
Associated Trustpoints: SELF-SIGNED
```

CSR(Certificate Signing Request)에 의한 등록

1. (선택 사항) 특정 키 크기로 명명된 키 쌍을 만듭니다.

 참고: 기본적으로 Default-RSA-Key라는 이름과 2048의 크기를 갖는 RSA 키가 사용됩니다. 그러나 각 인증서에서 동일한 개인/공용 키 쌍을 사용하지 않도록 고유한 이름을 사용하는 것이 좋습니다.

```
<#root>
ASAv(config)#
crypto key generate rsa label
    CA-SIGNED-KEYPAIR
modulus
    2048
INFO: The name for the keys will be: CA-SIGNED-KEYPAIR
Keypair generation process begin. Please wait...
```

생성된 키 쌍을 명령과 함께 볼 수 있습니다 `show crypto key mypubkey rsa`.

```
<#root>
ASAv#
show crypto key mypubkey rsa

(...)
Key pair was generated at: 14:52:49 CEDT Jul 15 2022

Key name:
    CA-SIGNED-KEYPAIR
Usage: General Purpose Key

Key Size
    (bits): 2048
Storage: config
Key Data:

30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
...
59dcd7d7 c3ee77f5 bbd0988d 515e390e b8d95177 dfaf6b94 a9df474b 1ec3b4a4
af020301 0001
```

2. 특정 이름으로 신뢰 지점을 만듭니다. 등록 유형 터미널을 구성합니다.

```
ASAv(config)# crypto ca trustpoint CA-SIGNED
ASAv(config-ca-trustpoint)# enrollment terminal
```

3. Fully Qualified Domain Name(정규화된 도메인 이름) 및 Subject Name(주체 이름)을 구성합니다. FQDN 및 주체 CN 매개변수는 인증서가 사용되는 서비스의 FQDN 또는 IP 주소와 일치

해야 합니다.

```
ASAv(config-ca-trustpoint)# fqdn asavpn.example.com
ASAv(config-ca-trustpoint)# subject-name CN=asavpn.example.com,O=Example Inc,C=US,St=California,L=
```

4. (선택 사항) 1단계에서 생성한 키 쌍 이름을 구성합니다.

```
ASAv(config-ca-trustpoint)# keypair CA-SIGNED-KEYPAIR
```

5. (선택 사항) CRL(Certificate Revocation List) 또는 OCSP(Online Certificate Status Protocol)를 사용하여 인증서 해지 확인 방법을 구성합니다. 기본적으로 인증서 해지 검사는 비활성화되어 있습니다.

```
ASAv(config-ca-trustpoint)# revocation-check ocsp
```

6. (선택 사항) 신뢰 지점을 인증하고 ID 인증서를 신뢰할 수 있는 인증서로 서명할 CA 인증서를 설치합니다. 이 단계에서 설치되지 않은 경우 나중에 ID 인증서와 함께 CA 인증서를 설치할 수 있습니다.

```
ASAv(config)# crypto ca authenticate CA-SIGNED
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
```

```
ASAv(config)# crypto ca authenticate CA-SIGNED
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----
MIIDXCcAKSgAwIBAgIIDM/QY/h29+kwDQYJKoZIhvcNAQELBQAwRTElMAkGA1UE
BhMCUExwDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxmDbGFMRcwFQYDVQQDEw5j
YS5leGZtcGx1LmNvbTAeFw0xNTAyMDYxNDEwMDEwMDAwFw0xMDEyMDYxNDEw
MDEwMDAwCzAJBgNVBAYTA1BMMQ8wDQYDVQQKEwZ3dy12cG4xDDAKBgNVBAAsTA2xhYjEXMBUG
A1UEAxMOY2EuZXhhbXBsZS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQDI6pth5KFFTB29Lyn0g9/CTi0GYa+WFTcZXSLLHZA6WTUzLYM19IbSFHwa6
gTeBnHqToLRnQoB51Q1xEA45ArL2G98aew8BMD08GXkxWayforwLA3U9WZVTZsVN
4noWaXH1boGGD7+5vkOesJfL2B7pEhGodLh7Gki1T4KoqL/7DM9Lqkz0ctZkCT7f
SkXvFik1Z1cZEGn6b2umnIqaVZ81ewIuTHOX481s3uxTPH8+B5QG0+d1wa0sbCwK
oK5sEPpHZ3IQuVxGii rp/zmomzx14G/te16eyMOpjpnVtDYjQ9HNkQdQT5LKwRsX
Oj9xKnYCbPfg3p2FdH7wJh11K3prAgMBAAGjUDBOMAwGA1UdEwQFMAMBAf8wHQYD
VR0OBBYEFE55kZsbra9b9tLFV52U47em9uXaMB8GA1UdIwQYMBaAFE55kZsbra9b
9tLFV52U47em9uXaMA0GCSqGSIb3DQEBCwUAA4IBAQArsX1FwK3j1NBwOsYh5mqT
cGqeyDMRhs3Rs/wD25M2wkAF4AYZHgN9gK9VCK+ModKMQZy4X/uhj65NDU7oFf6f
z9kqarjjsx153jV/YLk8E9oAIatnA/fQfX6V+h74yqucFF1js3d1FjyV14odRPwM
OjRyja1H56BF1ackNc7KRddtVxYB9sfEbFhN8od1BvnUedxGAJFHqxEQKmBE+h4w
gW8YnH0vM08svyTXSL1Jf0UCdmAY+1G0gqhU1S1kFBtLRt6Z2uCoT00NoMHI0hh5
dcVcov0i/PaxnrA1J+Ng2jrWfN3MXWZ04S3CHYMGkwqHkaHCh1qD0x9badgfsyzz
-----END CERTIFICATE-----
```

```
quit
```

```
INFO: Certificate has the following attributes:
Fingerprint: e9ad165c 2673424c 6e7e0c5f b30b4a02
Do you accept this certificate? [yes/no]: yes
WARNING: CA certificates can be used to validate VPN connections,
by default. Please adjust the validation-usage of this
trustpoint to limit the validation scope, if necessary.
```

Trustpoint CA certificate accepted.

% Certificate successfully imported

- 인증서를 등록하고 서명을 위해 CA에 복사 및 전송할 수 있는 CSR을 생성합니다. CSR에는 신뢰 지점에서 사용하는 키 쌍의 공개 키가 포함됩니다. 서명된 인증서는 해당 키 쌍을 가진 디바이스에서만 사용할 수 있습니다.



참고: CA는 CSR에 서명하고 서명된 ID 인증서를 생성할 때 신뢰 지점에 정의된 FQDN 및 주체 이름 매개변수를 변경할 수 있습니다.

```
ASAv(config)# crypto ca enroll CA-SIGNED
```

```
WARNING: The certificate enrollment is configured with an fqdn that differs from the system fqdn. If this certificate will be 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 will be: CN=asavpn.example.com,O=Example Inc,C=US,St=Califor
```

```
% The fully-qualified domain name in the certificate will be: asavpn.example.com
```

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

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

```
Certificate Request follows:
```

```
-----BEGIN CERTIFICATE REQUEST-----
```

```
MIIDHzCCAgcCAQAwYsGzAZBgNVBAMMEFZyXWZwbi5leGFtcGxlLmNvbTEUMBIGA1UECgwLRXhhbXBsZSBjbWxkZSBJbmMxZSBJBGNVBAWYTA1VTMRMwEQYDVQIDApDYWxpZm9ybm1hMREwDwYDVQQHDAhTYW4gSm9zZTEhMB8GCSqGSIb3DQEJAgwSYXNhdnBuLmV4YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAE5cvZVr1jMe8Mz4T3vgT1Z8DAAR0avs/TBdYiqGdjyiV/3K92IIT/0r8cuAUe5rR4sjTvaXYCSycSbwKc4kZbr3x120ss8ItD5g4kBdrUSCprl+VMiTphQgBTAqRPk0vFX4rC8k/T0PFDE+2gjT1wMn9reb92jYro1GK4MwZdCzqowLPjEj5cCwu8Pv5h4hqTpudms+v4g3R100Dmeyv4uEMyLS/noPxZXZ8YiQMIG2EP2BgOKOT3Fzx0mVuekonQtRhiZt+czyyFSRoqyBSakEZBwABod8q1Eg5J/pH130J1itOUJEyI1FoVHqv3jL7zfA9i1InuNaHkiR062VQNXwIDAQABoE4wDwYJKoZIhvcNAQkHMqITADA7BgkqhkiG9w0BQCQ4xLjAsMASGA1UdDwQEAwIFoDADBGNVHREEFjAUGhJhc2F2cG4uZXhhbXBsZS5jb20wDQYJKoZIhvcNAQELBQADggEBAM3Q3zvp9G3MWP7R4wkpnBOH2CNUMPENIhHNjQjHYh08EOvWyo09FaLfhKVdLvFXh0vn5osXBmPLuVps6Ta4sBRUNicRoAmmA0pDWL9zDuu8BQnBGUN08T/H3ydjaNoPJ/f6EZ8gXY29NXEKb/+A2Tt0VVUTsYreGS+84GqoixF0tW8R50IXg+afAVOAh81xVUF0vuAi9DsiuvufMb4wdngQSOe1/B9Zgp/BfGM10ApgejACoJAGmyrn9Tj6Z/6/1bpKBKpf4VE5UXdj7WLAjw5JF/X2NrH3/cQscziG2Yg2dr3WpkTIY2W/kVohTiohVRkgXOMCecUaM1YxJyLTRQ=
```

```
-----END CERTIFICATE REQUEST-----
```

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

- ID 인증서를 가져옵니다. CSR이 서명되면 ID 인증서가 제공됩니다.

```
ASAv(config)# crypto ca import CA-SIGNED certificate
```

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

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

% The fully-qualified domain name in the certificate will be: asavpn.example.com

Enter the base 64 encoded certificate.

End with the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----

MIIDoTCCAomgAwIBAgIIKbLY8Qt8N5gwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxMDbGFMRcwFQYDVQQDEw5j
(...)

kzAihRuFqmYYUeQP2Byp/S5fNqUcyZfAczIht8BcPmV0916iSF/ULG1zXMSOUX6N
d/LHXwrcTpc1zU+7qx3TpVDZbJlwwF+BWTBlxgMOBosJx65u/n75KnbBhGUE75jV
HX2eRzuhnnSVExCoeyed7DLiezD8

-----END CERTIFICATE-----

quit

INFO: Certificate successfully imported

9. 인증서 체인을 확인합니다. 완료되면 새 ID 인증서 및 CA 인증서를 명령과 함께 볼 수 있습니

다 `show crypto ca certificates`

.

```
ASAv# show crypto ca certificates CA-SIGNED
```

CA Certificate

Status: Available

Certificate Serial Number: 0ccfd063f876f7e9

Certificate Usage: General Purpose

Public Key Type: RSA (2048 bits)

Signature Algorithm: RSA-SHA256

Issuer Name:

CN=ca.example.com

OU=lab

O=ww-vpn

C=PL

Subject Name:

CN=ca.example.com

OU=lab

O=ww-vpn

C=PL

Validity Date:

start date: 15:10:00 CEST Feb 6 2015

end date: 15:10:00 CEST Feb 6 2030

Storage: config

Associated Trustpoints: CA-SIGNED

Certificate

Status: Available

Certificate Serial Number: 29b2d8f10b7c3798

Certificate Usage: General Purpose

Public Key Type: RSA (2048 bits)

Signature Algorithm: RSA-SHA256

Issuer Name:

CN=ca.example.com

OU=lab

O=ww-vpn

C=PL

Subject Name:


```
unstructuredName=asavpn.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asavpn.example.com
Validity Date:
start date: 15:33:00 CEDT Jul 15 2022
end date: 15:33:00 CEDT Jul 15 2023
Storage: config
Associated Trustpoints: CA-SIGNED
```

PKCS12 등록

CA에서 받은 키 쌍, ID 인증서 및 선택적으로 CA 인증서 체인을 포함하는 PKCS12 파일에 등록합니다.

1. 특정 이름으로 신뢰 지점을 만듭니다.

```
ASAv(config)# crypto ca trustpoint Trustpoint-PKCS12
ASAv(config-ca-trustpoint)# exit
```



참고: 가져온 키 쌍은 신뢰 지점 이름의 이름을 따릅니다.

2. (선택 사항) CRL(Certificate Revocation List) 또는 OCSP(Online Certificate Status Protocol)를 사용하여 인증서 해지 확인 방법을 구성합니다. 기본적으로 인증서 해지 검사는 비활성화되어 있습니다.

```
ASAv(config-ca-trustpoint)# revocation-check ocsp
```

3. PKCS12 파일에서 인증서를 가져옵니다.



참고: PKCS12 파일은 base64로 인코딩되어야 합니다. 텍스트 편집기에서 파일을 열 때 인쇄 가능한 문자가 표시되면 base64로 인코딩된 것입니다. 이진 파일을 openssl의 base64 인코딩 형식으로 변환하는 데 사용할 수 있습니다.

```
openssl enc -base64 -in asavnpkcs12chain.example.com.pfx -out asavnpkcs12chain.example.com.
```

```
ASAv(config)# crypto ca import TP-PKCS12 pkcs12 cisco123
```

Enter the base 64 encoded pkcs12.

End with the word "quit" on a line by itself:

```
MIIN4gIBAzCCDawGCSqGSIb3DQEHAaCCDZ0Egg2ZMIIN1TCCCBcGCSqGSIb3DQEH
BqCCCAgwgaggEAgEAMIIH/QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIiK0c
wqE3TmOCAggAgIIH0NjxmJBuoPRuY11VxTiawHzsL8kI10310j7tcWmECBwzsKKq
```

```
(...)  
PXowMwYJKoZIhvcNAQkUMSYeJABhAHMAYQB2AHAAbgAuAGUAeABhAG0AcABsAGUA  
LgBjAG8AbTAtMCEwCQYFKw4DAhoFAAQUPXZZtBeq1h98wQ1jHW7J/hqoKcwECD05  
dnxCNJx6  
quit
```

Trustpoint CA certificate accepted.
WARNING: CA certificates can be used to validate VPN connections,
by default. Please adjust the validation-usage of this
trustpoint to limit the validation scope, if necessary.

INFO: Import PKCS12 operation completed successfully.

4. 설치된 인증서를 확인합니다.

```
ASAv# show crypto ca certificates TP-PKCS12
```

```
Certificate  
Status: Available  
Certificate Serial Number: 2b368f75e1770fd0  
Certificate Usage: General Purpose  
Public Key Type: RSA (2048 bits)  
Signature Algorithm: RSA-SHA256  
Issuer Name:  
CN=ca.example.com  
OU=lab  
O=ww-vpn  
C=PL  
Subject Name:  
unstructuredName=asavpn.example.com  
CN=asavpnpkcs12chain.example.com  
O=Example Inc  
L=San Jose  
ST=California  
C=US  
Validity Date:  
start date: 15:33:00 CEDT Jul 15 2022  
end date: 15:33:00 CEDT Jul 15 2023  
Storage: config  
Associated Trustpoints: TP-PKCS12
```

```
CA Certificate  
Status: Available  
Certificate Serial Number: 0ccfd063f876f7e9  
Certificate Usage: General Purpose  
Public Key Type: RSA (2048 bits)  
Signature Algorithm: RSA-SHA256  
Issuer Name:  
CN=ca.example.com  
OU=lab  
O=ww-vpn  
C=PL  
Subject Name:  
CN=ca.example.com  
OU=lab  
O=ww-vpn  
C=PL  
Validity Date:  
start date: 15:10:00 CEST Feb 6 2015  
end date: 15:10:00 CEST Feb 6 2030  
Storage: config
```

Associated Trustpoints: TP-PKCS12

이전 예에서 PKCS12에는 ID 및 CA 인증서, 즉 두 항목, 즉 Certificate와 CA Certificate가 포함되었습니다. 그렇지 않으면 인증서만 표시됩니다.

5. (선택 사항) 신뢰 지점을 인증합니다.

PKCS12에 CA 인증서가 없고 CA 인증서를 PEM 형식으로 따로 가져온 경우 수동으로 설치할 수 있습니다.

```
ASAv(config)# crypto ca authenticate TP-PKCS12
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----
MIIDXCcAKSgAwIBAgIIDM/QY/h29+kwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECzMdbGFjMRcwFQYDVQDEw5j
(...)
gW8YnHOvM08svyTXSL1Jf0UCdmAY+1G0gqhU1S1kFBtLRt6Z2uCot00NoMHI0hh5
dcVcovOi/PAXnrA1J+Ng2jrWfN3MXWZ04S3CHYMGkWqHkaHCh1qD0x9badgfsyzz
-----END CERTIFICATE-----
quit
```

```
INFO: Certificate has the following attributes:
Fingerprint: e9ad165c 2673424c 6e7e0c5f b30b4a02
Do you accept this certificate? [yes/no]: yes
```

```
WARNING: CA certificates can be used to validate VPN connections,
by default. Please adjust the validation-usage of this
trustpoint to limit the validation scope, if necessary.
```

```
Trustpoint CA certificate accepted.
```

```
% Certificate successfully imported
```

인증서 갱신

자체 서명 인증서 갱신

1. 현재 인증서 만료 날짜를 확인합니다.

```
<#root>
```

```
# show crypto ca certificates SELF-SIGNED
Certificate
Status: Available
Certificate Serial Number: 62d16084
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
unstructuredName=asa.example.com
```

```
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Subject Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Validity Date:

start date: 15:00:58 CEST Jul 15 2022

end date: 15:00:58 CEST Jul 12 2032

Storage: config
Associated Trustpoints: SELF-SIGNED
```

2. 인증서를 다시 생성합니다.

```
ASAv# conf t
ASAv(config)# crypto ca enroll SELF-SIGNED
WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.
Would you like to continue with this enrollment? [yes/no]: yes

WARNING: Trustpoint TP has already enrolled and has
a device cert issued to it.
If you successfully re-enroll this trustpoint,
the current certificate will be replaced.
Do you want to continue with re-enrollment? [yes/no]: yes
% The fully-qualified domain name in the certificate will be: asa.example.com
% Include the device serial number in the subject name? [yes/no]: no
Generate Self-Signed Certificate? [yes/no]: yes
ASAv(config)# exit
```

3. 새 인증서를 확인합니다.

```
<#root>

ASAv# show crypto ca certificates SELF-SIGNED
Certificate
Status: Available
Certificate Serial Number: 62d16085
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Subject Name:
unstructuredName=asa.example.com
L=San Jose
```


```
ST=California
C=US
O=Example Inc
CN=asa.example.com
Validity Date:
```

```
start date: 15:09:09 CEDT Jul 20 2022
```

```
end date: 15:09:09 CEDT Jul 17 2032
```

```
Storage: config
Associated Trustpoints: SELF-SIGNED
```

CSR(Certificate Signing Request)로 등록된 인증서 갱신

 참고: 새 인증서에 대해 새 인증서 요소(주체/fqdn, 키 쌍)를 변경해야 하는 경우 새 인증서를 생성합니다. CSR(Certificate Signing Request) 섹션을 사용하여 등록을 참조하십시오. 다음 절차에서는 인증서 만료 날짜만 새로 고칩니다.

1. 현재 인증서 만료 날짜를 확인합니다.

```
<#root>
```

```
ASA# show crypto ca certificates CA-SIGNED
```

Certificate

```
Status: Available
Certificate Serial Number: 29b2d8f10b7c3798
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Subject Name:
unstructuredName=asavpn.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asavpn.example.com
Validity Date:
start date: 15:33:00 CEDT Jul 15 2022

end date: 15:33:00 CEDT Jul 15 2023
```

```
Storage: config
Associated Trustpoints: CA-SIGNED
```

Certificate

```
Subject Name:
Status: Pending terminal enrollment
Key Usage: General Purpose
Fingerprint: 790aa617 c30c6894 0bdc0327 0d60b032
Associated Trustpoint: CA-SIGNED
```


used for VPN authentication this may cause connection problems.
Would you like to continue with this enrollment? [yes/no]: yes

% The fully-qualified domain name in the certificate will be: asavpn.example.com

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

```
-----BEGIN CERTIFICATE-----
MIIDgTCCAmmgAwIBAgIIMA+aIxctNtMwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECXMdbGFfMRcwFQYDVoQDEw5j
YS5leGFtcGxlLmNvbTAeFw0yMjA3MjAxNDA5MDBaFw0yMjA3MjAxNDA5MDBaMIIG
MRswGQYDVoQDDDBJhc2F2cG4uZXhhbXBsZS5jb20xFDASBgNVBAoMCOV4YW1wbGUg
SW5jMQswCQYDVoQGEwVUzETMBEGA1UECAwKQ2FsaWZvcn5pYTERMA8GA1UEBwwI
U2FuIEpvc2UxITAFBgkqhkiG9w0BCQIMEFzYXZwbi5leGFtcGxlLmNvbTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAAOXL2Va9YzHvDM+E974E9WfAwAEd
Gr7P0wXWlqhnY8o1f9yvdiCE/9K/HLgFHua0eLI07212AksnEm8Cn0JGW698ddtL
LPCLXeY0JAXa1Egqa5f1TIk6YUIAUwKkT5NLxV+KwvJP09DxQxPtoI09cDJ/a3m/
do2K6JRiuDFmXQs6qMCz4xI+XAsLvD7+YeIak6bnZrPr+IN0dTjg5nsr+LhDGC0v
56D8WV2fGIkDIhthD9gYncjk9xc8dJ1bnPKJ0LUYYmbfnM8sn0kaKsgUmpBGQcAA
aHfKtRiOSf6R9d9CZYrT1CRMiJRaFR6r94y+83wPYpSJ7jWh5Iq90t1UDV8CAwEA
AaMuMCwwCwYDVR0PBAQDAgWgMB0GA1UdEQQWMBSCEmFzYXZwbi5leGFtcGxlLmNv
bTANBgkqhkiG9w0BAQsFAAOCAQEAFQUchY4UjhjkySMJAh7NT3TT5JJ4NzqW8qHa
wNq+YyHR+sQ6G3vn+6cYCU87tqW1Y3fXC27TwwREwMbq8NsJrr80hsChYby8kwE
LnTkrN7dJB17u50VQ3DRjfmFrJ9LEUaYZx1HYvcS1kAeEeVB4VJwVzeujWepcmEM
p7cB6veTcF9ru1DVRImd0KYE0x+HYav2INT2udc0G1yDwm1/mqdf0/ON2SpBBpnE
gtiKshtsST/NAw25WjkrDIfn8uR2z5xpzxnEDUBoHOipG1gb1I6G1ARXW0+Lwfb1
n1QD5b/RdQ0UbLCPfKNPde/9wNnoXGD1J7qfZxr04T71d2Idug==
-----END CERTIFICATE-----
quit
```

INFO: Certificate successfully imported

4. 새 인증서 만료 날짜를 확인합니다.

```
<#root>
```

```
ASAv# show crypto ca certificates CA-SIGNED
Certificate
Status: Available
Certificate Serial Number: 300f9a2310ad36d3
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Subject Name:
unstructuredName=asavpn.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asavpn.example.com
Validity Date:
start date: 16:09:00 CEDT Jul 20 2022

end date: 16:09:00 CEDT Jul 20 2023

Storage: config
```

PKCS12 갱신

PKCS12 파일을 사용하여 등록된 신뢰 지점에서 인증서를 갱신할 수 없습니다. 새 인증서를 설치하려면 새 신뢰 지점을 만들어야 합니다.


1. 특정 이름으로 신뢰 지점을 만듭니다.

```
ASAv(config)# crypto ca trustpoint Trustpoint-PKCS12-2022
ASAv(config-ca-trustpoint)# exit
```

2. (선택 사항) CRL(Certificate Revocation List) 또는 OCSP(Online Certificate Status Protocol)를 사용하여 인증서 해지 확인 방법을 구성합니다. 기본적으로 인증서 해지 검사는 비활성화되어 있습니다.

```
ASAv(config-ca-trustpoint)# revocation-check ocsp
```

3. PKCS12 파일에서 새 인증서를 가져옵니다.

 참고: PKCS12 파일은 base64로 인코딩되어야 합니다. 텍스트 편집기에서 파일을 열 때 인쇄 가능한 문자가 표시되면 base64로 인코딩된 것입니다. 이진 파일을 base64 인코딩 형식으로 변환하기 위해 openssl을 사용할 수 있습니다.

```
openssl enc -base64 -in asavnpkcs12chain.example.com.pfx -out asavnpkcs12chain.example.com.
```

```
ASAv(config)# crypto ca import TP-PKCS12-2022 pkcs12 cisco123
```

Enter the base 64 encoded pkcs12.

End with the word "quit" on a line by itself:

```
MIIN4gIBAzCCDawGCSqGSIb3DQEHAaCCDZ0Egg2ZMIIN1TCCCBcGCSqGSIb3DQEH
BqCCCAgwgaggEAgEAMIH/QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQmDgQIiK0c
wqE3Tm0CAggAgIIHONjxmJBuoPRuY11VxTiawHzsL8kI10310j7tcWmECBwzskKq
(...)
PXowMwYJKoZIhvcNAQkUMSYeJABhAHMAYQB2AHAAbgAuAGUAeABhAG0AcABsAGUA
LgBjAG8AbTAtMCEwCQYFKw4DAhoFAAQUPXZZtBeq1h98wQ1jHW7J/hqoKcwECD05
dnxCNJx6
quit
```

Trustpoint CA certificate accepted.

WARNING: CA certificates can be used to validate VPN connections, by default. Please adjust the validation-usage of this trustpoint to limit the validation scope, if necessary.

INFO: Import PKCS12 operation completed successfully.



참고: 새 PKCS12 파일에 이전 인증서와 함께 사용된 동일한 키 쌍을 가진 ID 인증서가 포함된 경우 새 신뢰 지점은 이전 키 쌍 이름을 참조합니다.

예:

<#root>

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

```
TP-PKCS12-2022
```

```
pkcs12 cisco123
```

Enter the base 64 encoded pkcs12. End with the word "quit" on a line by itself:

```
MIIN4gIBAzCCDawGCSqGSIb3DQEHAaCCDZ0Egg2ZMIIN1TCCBcGCSqGSIb3DQEH
```

```
...
```

```
dnxCNJx6
```

```
quit
```

```
WARNING: Identical public key already exists as TP-PKCS12
```

```
ASAv(config)# show run crypto ca trustpoint
```

```
TP-PKCS12-2022
```

```
crypto ca trustpoint TP-PKCS12-2022
```

```
keypair TP-PKCS12
```

```
no validation-usage crl configure
```

4. 설치된 인증서를 확인합니다.

<#root>

```
ASAv# show crypto ca certificates TP-PKCS12-2022
```

```
Certificate
```

```
Status: Available
```

```
Certificate Serial Number: 2b368f75e1770fd0
```

```
Certificate Usage: General Purpose
```

```
Public Key Type: RSA (2048 bits)
```

```
Signature Algorithm: RSA-SHA256
```

```
Issuer Name: CN=ca.example.com OU=lab O=ww-vpn C=PL
```

```
Subject Name: unstructuredName=asavpn.example.com CN=asavpnpkcs12chain.example.com O=Example Inc
```

```
Validity Date:
```

```
start date: 15:33:00 CEDT Jul 15 2022
```

```
end date: 15:33:00 CEDT Jul 15 2023
```

```
Storage: config
```

```
Associated Trustpoints: TP-PKCS12-2022
```

```
CA Certificate
```

```
Status: Available
```

```
Certificate Serial Number: 0ccfd063f876f7e9
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name: CN=ca.example.com OU=lab O=ww-vpn C=PL
Subject Name: CN=ca.example.com OU=lab O=ww-vpn C=PL
Validity Date:
start date: 15:10:00 CEST Feb 6 2015
end date: 15:10:00 CEST Feb 6 2030
Storage: config
Associated Trustpoints: TP-PKCS12-2022
```

이전 예에서 PKCS12에는 ID 인증서 및 CA 인증서가 포함되었으므로, 가져오기, 인증서 및 CA 인증서 다음에 두 개의 항목이 표시됩니다. 그렇지 않으면 인증서 항목만 표시됩니다.

5. (선택 사항) 신뢰 지점을 인증합니다.

PKCS12에 CA 인증서가 없고 CA 인증서를 PEM 형식으로 따로 가져온 경우 수동으로 설치할 수 있습니다.

```
ASAv(config)# crypto ca authenticate TP-PKCS12-2022
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----
MIIDXCCAKSgAwIBAgIIDM/QY/h29+kwDQYJKoZIhvcNAQELBQAwRTElMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECXMdbGFjMRcwFQYD
VQDEw5j
(...)
gW8YnH0vM08svyTXSL1Jf0UCdmAY+1G0gqhU1S1kFBtLRt6Z2uCot00NoMHI0hh5
dcVcov0i/PAXnrA1J+Ng2jrWfN3MXWZ04S3CHYMGkWqHkaHCh1qD0x9badgfsyzz
-----END CERTIFICATE-----
quit
```

```
INFO: Certificate has the following attributes:
Fingerprint: e9ad165c 2673424c 6e7e0c5f b30b4a02
Do you accept this certificate? [yes/no]: yes
```

```
WARNING: CA certificates can be used to validate VPN connections,
by default. Please adjust the validation-usage of this
trustpoint to limit the validation scope, if necessary.
```

```
Trustpoint CA certificate accepted.
```


```
% Certificate successfully imported
```

6. 기존 신뢰 지점 대신 새 신뢰 지점을 사용하도록 ASA를 재구성합니다.

예:

```
ASAv# show running-config ssl trust-point
ssl trust-point TP-PKCS12
ASAv# conf t
```

```
ASAv(config)#ssl trust-point TP-PKCS12-2022
ASAv(config)#exit
```

 참고: 신뢰 지점은 여러 구성 요소에서 사용할 수 있습니다. 이전 신뢰 지점이 사용되는 컨피그레이션을 확인합니다.

관련 정보

ASA에서 시간 설정을 구성하는 방법.

ASA에서 시간과 날짜를 올바르게 설정하는 데 필요한 단계는 Cisco ASA Series General Operations CLI Configuration Guide 9.18을 참조하십시오.

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa918/configuration/general/asa-918-general-config/basic-hostname-pw.html#ID-2130-000001bf>

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.