

Certificaten installeren en verlengen op ASA, beheerd door CLI

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Certificaatinstallatie](#)

[Zelfondertekende certificaatschrijving](#)

[Inschrijving op verzoek tot ondertekening van certificaten \(CSR\)](#)

[PKCS C12-inschrijving](#)

[Certificaat-verlenging](#)

[Verlengen zelfondertekend certificaat](#)

[Verleng certificaat ingeschreven met aanvraag voor certificaatondertekening \(CSR\)](#)

[PKCS C12-verlenging](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u bepaalde typen certificaten op Cisco ASA-software die met CLI wordt beheerd, kunt aanvragen, installeren, vertrouwen en verlengen.

Voorwaarden

Vereisten

- Controleer dat de adaptieve security applicatie (ASA) de juiste kloktijd, datum en tijdzone heeft. Bij certificaatverificatie wordt het aanbevolen een NTP-server (Network Time Protocol) te gebruiken om de tijd op de ASA te synchroniseren. Controleer verwante informatie voor referentie.
- Om een certificaat aan te vragen dat gebruik maakt van certificaatondertekeningaanvraag (CSR), is toegang nodig tot een vertrouwde interne of externe certificeringsinstantie (CA). Voorbeelden van CA-leveranciers van derden zijn onder meer Entrust, Geotrust, GoDaddy, Thawte en VeriSign.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ASAv 9.18.1
- Voor het maken van PKCS12 wordt OpenSSL gebruikt.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Het type certificaten waarop dit document betrekking heeft, is zelfondertekende certificaten, certificaten die zijn ondertekend door een certificeringsinstantie van een derde partij of een interne certificeringsinstantie, op Cisco adaptieve security applicatie software die wordt beheerd met Command Line Interface (CLI).

Certificaatinstallatie

Zelfondertekende certificaatinschrijving

1. (Optioneel) Maak een benoemde sleutelbaar met een specifieke sleutelgrootte.



Opmerking: standaard wordt de RSA-toets met de naam Default-RSA-Key en een grootte van 2048 gebruikt. Het wordt echter aanbevolen om een unieke naam voor elk certificaat te gebruiken, zodat ze niet hetzelfde private/publieke sleutelbaar gebruiken.

```
<#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...
```

Het gegenereerde sleutelbaar kan met de opdracht worden gezien `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. Maak een trustpoint met een specifieke naam. Inschrijftype zelf configureren.

<#root>

```
ASAv(config)#
```

```
crypto ca trustpoint
```

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

```
enrollment self
```

3. Configureer de volledig gekwalificeerde domeinnaam (FQDN) en onderwerpnaam.



Waarschuwing: de FQDN-parameter moet overeenkomen met de FQDN of het IP-adres van de ASA-interface waarvoor het certificaat wordt gebruikt. Deze parameter stelt de alternatieve onderwerpnaam (SAN) voor het certificaat in.

<#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. (Optioneel) Configureer de naam van het sleutelpaar die in Stap 1 is gemaakt. Niet vereist als het standaard sleutelpaar wordt gebruikt.

<#root>

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

5. Neem het trustpoint in en genereer het certificaat.

```
<#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. Na voltooiing is het nieuwe zelfondertekende certificaat te zien met de opdracht `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

Inschrijving door verzoek tot ondertekening van certificaten (CSR)

1. (Optioneel) Maak een benoemde sleutelpaar met een specifieke sleutelgrootte.

 Opmerking: standaard wordt de RSA-toets met de naam Default-RSA-Key en een grootte van 2048 gebruikt. Het wordt echter aanbevolen om een unieke naam voor elk certificaat te gebruiken, zodat ze niet hetzelfde private/publieke sleutelpaar gebruiken.

<#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...

Het gegenereerde sleutelpaar kan met de opdracht worden gezien `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. Maak een trustpoint met een specifieke naam. Configureer de inschrijvingstype terminal.

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

3. Configureer de volledig gekwalificeerde domeinnaam en onderwerpnaam. De FQDN- en de onderwerpparameters van de GN moeten overeenkomen met het FQDN- of IP-adres van de service waarvoor het certificaat wordt gebruikt.

```
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. (Optioneel) Configureer de sleutelpaar naam die in stap 1 is gemaakt.

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

5. (Optioneel) Controleer de methode voor het intrekken van certificaten - met de certificaatintrekkingslijst (CRL) of met het Online Certificate Status Protocol (OCSP). De standaardinstelling is dat de certificaatherroepingscontrole is uitgeschakeld.

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

6. (Optioneel) Verifieer het trustpoint en installeer het CA-certificaat dat het identiteitscertificaat als vertrouwd zal ondertekenen. Indien niet bij deze stap geïnstalleerd, kan het CA-certificaat later samen met het identiteitscertificaat worden geïnstalleerd.

```
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
BhMCUExwDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECXMdbGFjMRcwFQYDVQDEw5j
YS5leGFtcGxlLmNvbTAeFw0xNTAyMDYxNDEwMDBaFw0xMDEyMDYxNDEwMDBaMEUx
CzAJBgNVBAYTA1BMMQ8wDQYDVQQKEwZ3dy12cG4xDDAKBgNVBAsTA2xhYjEXMBUG
A1UEAxMOY2EuZXhhbXBsZS5jb20wgwEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQDI6pth5KFFTB29Lyn0g9/CTiOGYa+WFTcZXSLHZA6WTUzLYM19IbSFHwa6
gTeBnHqToLRnQoB51Q1xEA45ArL2G98aew8BMD08GXkxWayforwLA3U9WZVTZsVN
4noWaxH1boGGD7+5vk0esJfL2B7pEhGodLh7Gki1T4KoqL/1DM9Lqkz0ctZkCT7f
SkXvFik1Z1cZEGn6b2umnIqaVZ81ewIuTHOX481s3uxTPH8+B5QG0+d1wa0sbCwk
oK5sEPpHZ3IQuVxGiirp/zmomzx14G/te16eyMOpjpnVtDYjQ9HNkQdQT5LKwRsX
Oj9xKnYCbPfg3p2FdH7wJh11K3prAgMBAAGjUDBOMAwGA1UdEwQFMAMBAF8wHQYD
VR0OBBYEF55kZsbra9b9tLFV52U47em9uXaMB8GA1UdIwQYMBaAFE55kZsbra9b
9tLFV52U47em9uXaMA0GCSqGSIb3DQEBCwUAA4IBAQArsX1FwK3j1NBw0sYh5mqT
cGqeyDMRhs3Rs/wD25M2wkAF4AYZHgN9gK9VCK+ModKMQZy4X/uhj65NDU7oFf6f
z9kqarijjsx153jV/YLk8E9oAIatnA/fQfX6V+h74yqucfF1js3d1FjyV14odRPwM
OjRyja1H56BF1ackNc7KRddtVxYB9sfEbFhN8od1BvnUedxGAJFHqxEQKMBE+h4w
gW8YnH0vM08svyTXSL1Jf0UCdmAY+1G0gqhU1S1kFBtLRt6Z2uCoT00NoMHI0hh5
dcVcov0i/PaxnrA1J+Ng2jrwFN3MXWZ04S3CHYMGkqWqHkaHCh1qD0x9badgfsyzz
```

-----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

7. Schrijf het certificaat in en genereer een CSR die kan worden gekopieerd en naar een CA kan worden gestuurd voor ondertekening. De MVO omvat de openbare sleutel van het sleutelbaar dat door trustpoint wordt gebruikt. Het ondertekende certificaat kan alleen worden gebruikt door apparaten die dat sleutelbaar hebben.

 **Opmerking:** CA kan de parameters FQDN en Onderwerpnaam die in het trustpoint zijn gedefinieerd wijzigen bij het ondertekenen van de CSR en het maken van een ondertekend identiteitsbewijs.

```
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-----  
MIIDHZCCAQCgCAQAwYsXGzAZBgNVBAMMEFZyXZwbi5leGFtcGxlLmNvbTEUMBIG  
A1UECgwLRXhhbXBsZSBJbmMxCzAJBgNVBAYTA1VTMRMwEQYDVQIDApDYWxpZm9y  
bm1hMREwDwYDVQQHDAhTYW4gSm9zZTEhMB8GCSqGSIb3DQEJAgwSYXNhdnBuLmV4  
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5cvZVr1j  
Me8Mz4T3vgT1Z8DAAR0avs/TBdYiqGdjyiV/3K92IIT/0r8cuAUe5rR4sjTvaXyC  
SycSbwKc4kZbr3x120ss8It5g4kBdrUSCprl+VMiTphQgBTAqRPk0vFX4rC8k/T  
0PFDE+2gjT1wMn9reb92jYro1GK4MWZdCzqowLPjEj5cCwu8Pv5h4hqTpudms+v4  
g3R100Dmeyv4uEMyLS/noPxZXZ8YiQMIG2EP2BgOKOT3Fzx0mVuekonQtRhiZt+c  
zyyFSRoqyBSakEZBwABod8q1Eg5J/pH130J1itOUJEyI1FoVHqv3jL7zfA9i1Inu  
NaHkiR062VQNxwIDAQABoE4wDwYJKoZIhvcNAQkHMqITADA7BgkqhkiG9w0BCQ4x  
LjAsMAsGA1UdDwQEAwIFoDAdBgNVHREEFjAUGhJhc2F2cG4uZXhhbXBsZS5jb20w  
DQYJKoZIhvcNAQELBQAggEBAM3Q3zvp9G3MWP7R4wkpnBOH2CNUmPENIhHNjQjH  
Yh08EOvWyo09FaLfhKVDLvfXh0vn5osXBmPLuVps6Ta4sBRUNicRoAmmA0pDWL9z  
Duu8BQnBGUN08T/H3ydjaNoPJ/f6EZ8gXY29NxEKb/+A2Tt0VVUTsYreGS+84Gqo  
ixF0tW8R50IXg+aFAVOAh81xVUF0vuAi9DsiuvufMb4wdngQS0e1/B9Zgp/BfGM1  
10ApgeJACoJAGmyrn9Tj6Z/6/1bpKBKpf4VE5UXdj7WLAjw5JF/X2NrH3/cQsczi  
G2Yg2dr3WpKTIY2W/kVohTiohVRkgXOMCecUaM1YxJyLTRQ=
```

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

Redisplay enrollment request? [yes/no]: no

8. Voer het identiteitsbewijs in. Zodra de MVO is ondertekend, wordt een identiteitsbewijs verstrekt.

```
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
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECXMdbGFjMRcwFQYDVQQDEw5j
(...)
kzAihRuFqmYYUeQP2Byp/S5fNqUcyZfAczIHt8BcPmV0916iSF/ULG1zXMSOUX6N
d/LHXwrcTpc1zU+7qx3TpVDZbJlwwF+BWTB1xgM0BosJx65u/n75KnbBhGUE75jV
HX2eRzuhnnSVExCoeyed7DLiezD8
-----END CERTIFICATE-----
quit
INFO: Certificate successfully imported
```

9. Controleer de certificaatketen. Na voltooiing zijn het nieuwe identiteitsbewijs en het CA-certificaat te zien met de opdracht `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

PKCS C12-inschrijving

Schrijf u in met het PKCS12-bestand dat sleutelbaar, identiteitscertificaat en optioneel CA-certificaatketting bevat, ontvangen van uw CA.

1. Maak een trustpoint met een specifieke naam.

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



Opmerking: het geïmporteerde sleutelbaar is genoemd naar de trustpoint naam.

2. (Optioneel) Controleer de methode voor het intrekken van certificaten - met de certificaatintrekkingslijst (CRL) of met het Online Certificate Status Protocol (OCSP). De standaardinstelling is dat de certificaatherroepingscontrole is uitgeschakeld.

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

3. Importeer het certificaat uit een PKCS12-bestand.



Opmerking: het PKCS12-bestand moet base64-gecodeerd zijn. Als afdrubbare tekens worden weergegeven wanneer een bestand in een teksteditor wordt geopend, is het base64-gecodeerd. Om een binair bestand om te zetten naar base64 encoded form openssl kan worden gebruikt.

```
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  
BqCCCAgwgggEAgEAMIH/QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIiK0c  
wqE3Tm0CAggAgIIH0NjxmJBuoPRuY11VxTiawHzsL8kI10310j7tcWmECBwzKKq  
(...)
```

```
PXowMwYJKoZIhvcNAQkUMSYeJABhAHMAYQB2AHAAbgAuAGUAeABhAG0AcABsAGUA  
LgBjAG8AbTAtMCEwCQYFKw4DAhoFAAQUPXZZtBeq1h98wQ1jHW7J/hqoKcwECDO5  
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. Controleer de geïnstalleerde certificaten.

```
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=asavnpkcs12chain.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
```

In het vorige voorbeeld bevatte de PKCS12 de identiteit en CA-certificaat - de twee vermeldingen - certificaat en CA-certificaat. Anders is alleen Certificaat aanwezig.

5. (Optioneel) Verifieer het trustpoint.

Als de PKCS12 niet het CA-certificaat bevatte en het CA-certificaat afzonderlijk in PEM-formaat werd verkregen, dan kan het handmatig worden geïnstalleerd.

```
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-----
MIIDXDCCAkSgAwIBAgIIDM/QY/h29+kwDQYJKoZIhvcNAQELBQAwRTElMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECXMdbGFjMRcwFQYDVQQDEw5j
(...)
gW8YnHOvM08svyTXSL1Jf0UCdmAY+1G0gqhU1S1kFBtLRt6Z2uCot00NoMHI0hh5
dcVcovOi/PAXnrA1J+Ng2jrWfN3MXWZ04S3CHYMGkWqHkaHCh1qDOx9badgfsyzz
-----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
```

Certificaat-verlenging

Verlengen zelfondertekend certificaat

1. Controleer de huidige vervaldatum van het certificaat.

```
<#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. Herstel het certificaat.

```
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. Controleer het nieuwe certificaat.

```
<#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 CEST Jul 20 2022

end date: 15:09:09 CEST Jul 17 2032

Storage: config
Associated Trustpoints: SELF-SIGNED

Verleng certificaat ingeschreven met aanvraag voor certificaatondertekening (CSR)

 **Opmerking:** als een van de nieuwe certificaatelementen (onderwerp/fqdn, sleutelpaar) moet worden gewijzigd voor het nieuwe certificaat, maak dan een nieuw certificaat aan. Raadpleeg de sectie Inschrijving met verzoek om certificaatondertekening (CSR). In de volgende procedure wordt alleen de vervaldatum van het certificaat ververst.

1. Controleer de huidige vervaldatum van het certificaat.

<#root>

ASAv# 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

2. Schrijf het certificaat in. Genereer een CSR die kan worden gekopieerd en verzonden naar een CA voor ondertekening. De MVO omvat de openbare sleutel van het sleutelpaar dat door trustpoint wordt gebruikt - het ondertekende certificaat kan slechts door apparaten worden gebruikt die dat sleutelpaar hebben.

 Opmerking: CA kan de parameters FQDN en Onderwerpnaam die in het trustpoint zijn gedefinieerd wijzigen bij het ondertekenen van de CSR en het maken van een ondertekend identiteitsbewijs.

 Opmerking: voor hetzelfde Trustpoint, zonder veranderde onderwerp/fqdn en keypair-configuratie, geven latere inschrijvingen dezelfde CSR als de eerste.

```
ASAv# conf t
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-----
MIIDH2CCAQcCAQAwYsGzAZBgNVBAMEMFZlYXZwbi5leGFtcG91LmNvbTEUMBIG
A1UECGRlRXhhbXBsZSBJbmMxZSBJBgNVBAYTA1VTMRMwEQYDVQIDApDYWxpZm9y
bm1hMREwDwYDVQQHDAhTYW4gSm9zZTEhMB8GCSqGSIb3DQEJAgwSYXNhdnBuLmV4
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5cvZVr1j
Me8Mz4T3vgT1Z8DAAR0avs/TBdYiqGdjyiV/3K92IIT/0r8cuAUe5rR4sjTvaXyC
SycSbwKc4kZbr3x120ss8It5g4kBdrUSCprl+VMiTphQgBTAqRPk0vFX4rC8k/T
0PFDE+2gjT1wMn9reb92jYro1GK4MWZdCzqowLPjEj5cCwu8Pv5h4hqTpudms+v4
g3R100Dmeyv4uEMyLS/noPxZXZ8YiQMIG2EP2BgOK0T3Fzx0mVuekonQtRhiZt+c
```

```
zyyFSRoqyBSakEZBwABod8q1Eg5J/pH130J1itOUJEyI1FoVHqv3jL7zfA9i1Inu
NaHkiR062VQNxwIDAQABoE4wDwYJKoZIHvcNAQkHMqITADA7BgkqhkiG9w0BCQ4x
LjAsMAsGA1UdDwQEAwIFoDAdBgNVHREEfjAUGhJhc2F2cG4uZXhhbXBsZS5jb20w
DQYJKoZIHvcNAQELBQAdggEBAM3Q3zvp9G3MWP7R4wkpnBOH2CNUMPENIhHNjQjH
Yh08EOvWyo09FaLfhKVDLvFXh0vn5osXBmPLuVps6Ta4sBRUNicRoAmmA0pDWL9z
Duu8BQnBGUN08T/H3ydjaNoPJ/f6EZ8gXY29NxEKb/+A2Tt0VVUTsYreGS+84Gqo
ixF0tW8R50IXg+afAV0Ah81xVUF0vuAi9DsiuvufMb4wdngQSOe1/B9Zgp/BFGM1
10ApgejACoJAGmyrn9Tj6Z/6/1bpKBKpf4VE5UXdj7WLAjw5JF/X2NrH3/cQsczi
G2Yg2dr3WpKTIY2W/kVohTiohVRkgXOMCecUaM1YxJyLTRQ=
-----END CERTIFICATE REQUEST-----
```

Redisplay enrollment request? [yes/no]: no

3. Voer het identiteitsbewijs in. Zodra de MVO is ondertekend, wordt een identiteitsbewijs verstrekt.

```
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-----
MIIDgTCCAmgAwIBAgIIMA+aIxCTntMwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECXMdbGFjMRcwFQYDVQDEw5j
YS5leGFtcGx1LmNvbTAeFw0yMjA3MjAxNDA5MDBaFw0yMjA3MjAxNDA5MDBaMIIG
MRswGQYDVQDDbJhc2F2cG4uZXhhbXBsZS5jb20xFDASBgNVBAoMCOV4YW1wbGUg
SW5jMQswCQYDVQQGEWJVVzETMBEGA1UECAwKQ2FsaWZvcn5pYTERMA8GA1UEBwwI
U2FuIEpvc2UxITAfBgkqhkiG9w0BCQIMEFzYXZwbi5leGFtcGx1LmNvbTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAA0XL2Va9YzHvDM+E974E9WfAwAEd
Gr7P0wXWIqhnY8o1f9yvdiCE/9K/HLgFHua0eLI07212AksnEm8CnOJGw698ddtL
LPCLXeY0JAXa1Egqa5f1TIk6YUIAUwKkT5NLxV+KwvJP09DxQxPtoI09cDJ/a3m/
do2K6JRiuDFmXqs6qMCz4xI+XAsLvD7+YeIak6bnZrPr+IN0dTjg5nsr+LhDGC0v
56D8WV2fGIkDIhthD9gYNCjk9xc8dJ1bnpKJ0LUYYmbfnM8sn0kaKsgUmpBGQcAA
aHfKtRIOSf6R9d9CZYrT1CRMiJRaFR6r94y+83wPYpSj7jWh5Iq90t1UDV8CAwEA
AaMuMCwwCwYDVR0PBAQDAgWgMB0GA1UdEQQWMBSEMFzYXZwbi5leGFtcGx1LmNv
bTANBgkqhkiG9w0BAQsFAA0CAQEAFQUchY4UjhjkySMJAh7NT3TT5JJ4NzqW8qHa
wNq+YyHR+sQ6G3vn+6cYCU87tqW1Y3fXC27TtweREwMmq8NsJrr80hsChYby8kwE
LnTkrN7dJB17u50VQ3DRjfmFrJ9LEUaYZx1HYvcS1kAeEeVB4VJwVzeujWepcmEM
p7cB6veTcF9ru1DVRImd0KYEOx+HYav2INT2udcOG1yDwm1/mqdf0/ON2SpBBpnE
gtiKshtsST/NAw25WjkrDIfn8uR2z5xpzxnEDUBoHoipG1gb1I6G1ARXW0+Lwfb1
n1QD5b/RdQOUbLCPfKNPde/9wNnoXGD1J7qfZxr04T71d2Idug==
-----END CERTIFICATE-----
quit
```

```
INFO: Certificate successfully imported
```

4. Controleer de vervaldatum van het nieuwe certificaat.

```
<#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
Associated Trustpoints: CA-SIGNED
```

PKCS C12-verlenging

Het is niet mogelijk om een certificaat te verlengen in trustpoint dat is ingeschreven met behulp van PKCS12-bestand. Om een nieuw certificaat te installeren, moet een nieuw trustpoint worden gecreëerd.

1. Maak een trustpoint met een specifieke naam.

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

2. (Optioneel) Controleer de methode voor het intrekken van certificaten - met de certificaatintrekkingslijst (CRL) of met het Online Certificate Status Protocol (OCSP). De standaardinstelling is dat de certificaatherroepingscontrole is uitgeschakeld.

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

3. Importeer het nieuwe certificaat uit een PKCS12-bestand.



Opmerking: het PKCS12-bestand moet base64-gecodeerd zijn. Als afdruckbare tekens worden weergegeven wanneer een bestand in een teksteditor wordt geopend, is het base64-gecodeerd. Om een binair bestand om te zetten naar base64 encoded form, kan openssl worden gebruikt.

```
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/QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMWdGQIiK0c
wqE3TmOCAggAgIIHONjxmJBuoPRuY11VxTiawHzsL8kI10310j7tcWmECBwzsKKq
(...)
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.



Opmerking: Als het nieuwe PKCS12-bestand een identiteitsbewijs met hetzelfde sleutelpaar bevat dat met het oude certificaat is gebruikt, verwijst het nieuwe trustpoint naar de oude sleutelpaar naam.

Voorbeeld:

```
<#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:

```
MIIN4gIBAzCCDawGCSqGSIb3DQEHAaCCDZ0Egg2ZMIIN1TCCCBcGCSqGSIb3DQEH
...
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. Controleer de geïnstalleerde certificaten.

```
<#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
```

In het vorige voorbeeld bevatte de PKCS12 het identificatiecertificaat en het CA-certificaat. Daarom worden na de invoer, het certificaat en het CA-certificaat twee vermeldingen weergegeven. Anders is alleen de vermelding Certificaat aanwezig.

5. (Optioneel) Verifieer het trustpoint.

Als de PKCS12 niet het CA-certificaat bevatte en het CA-certificaat afzonderlijk in PEM-formaat werd verkregen, dan kan het handmatig worden geïnstalleerd.

```
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  
BhMCUEw5DzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxMDbGFhbnRwYXN0aW50  
(...)  
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. Herstel ASA om het nieuwe trustpoint in plaats van de oude te gebruiken.

Voorbeeld:

```
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
```



Opmerking: Een trustpoint kan worden gebruikt in verschillende configuratie-elementen. Controleer uw configuratie waar het oude trustpoint wordt gebruikt.

Gerelateerde informatie

Hoe configureer ik tijdsinstellingen op een ASA.

Controleer of de Cisco ASA Series General Operations CLI Configuration Guide 9.18 de stappen bevat die nodig zijn om de tijd en datum correct in te stellen op de ASA.

<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>

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.