

Installer et renouveler des certificats sur ASA géré par CLI

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Installation du certificat](#)

[Inscription de certificat auto-signé](#)

[Inscription par demande de signature de certificat \(CSR\)](#)

[Inscription PKCS12](#)

[Renouvellement du certificat](#)

[Renouveler le certificat auto-signé](#)

[Renouveler le certificat inscrit avec une demande de signature de certificat \(CSR\)](#)

[Renouvellement PKCS12](#)

[Informations connexes](#)

Introduction

Ce document décrit comment demander, installer, approuver et renouveler certains types de certificats sur le logiciel Cisco ASA géré avec CLI.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Vérifiez que l'apppliance ASA (Adaptive Security Appliance) dispose de l'heure, de la date et du fuseau horaire corrects. Avec l'authentification de certificat, il est recommandé d'utiliser un serveur NTP (Network Time Protocol) pour synchroniser l'heure sur l'ASA. Consultez Informations connexes pour référence.
- Pour demander un certificat qui utilise une demande de signature de certificat (CSR), il nécessite l'accès à une autorité de certification (CA) interne ou tierce de confiance. Les exemples de fournisseurs CA tiers incluent, sans s'y limiter, Entrust, Geotrust, GoDaddy, Thawte et VeriSign.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ASAv 9.18.1
- Pour la création de PKCS12, OpenSSL est utilisé.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Les types de certificats auxquels ce document s'adresse sont des certificats auto-signés, des certificats signés par une autorité de certification tierce ou une autorité de certification interne, sur le logiciel Cisco Adaptive Security Appliance géré avec l'interface de ligne de commande (CLI).

Installation du certificat

Inscription de certificat auto-signée

1. (Facultatif) Créez une paire de clés nommée avec une taille de clé spécifique.



Remarque : par défaut, la clé RSA avec le nom Default-RSA-Key et une taille de 2048 est utilisée ; cependant, il est recommandé d'utiliser un nom unique pour chaque certificat afin qu'ils n'utilisent pas la même paire de clés privée/publique.

```
<#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...
```

La paire de clés générée est visible à l'aide de la commande `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
```

- Créez un point de confiance avec un nom spécifique. Configurez le type d'inscription **self**.

<#root>

ASAv(config)#

```
crypto ca trustpoint
```

SELF-SIGNED

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

```
enrollment self
```

- Configurez le nom de domaine complet (FQDN) et le nom du sujet.



Attention : le paramètre FQDN doit correspondre au nom de domaine complet ou à l'adresse IP de l'interface ASA pour laquelle le certificat est utilisé. Ce paramètre définit le nom alternatif du sujet (SAN) pour le certificat.

```
<#root>
```

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

```
fqdn
```

```
asavpn.example.com  
ASAv(config-ca-trustpoint)#
```

```
subject-name
```

```
CN=
```

```
asavpn.example.com,0=Example Inc,C=US,St=California,L=San Jose
```

- (Facultatif) Configurez le nom de la paire de clés créée à l'étape 1. Non requis si la paire de clés par défaut est utilisée.

```
<#root>
```

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

```
keypair
```

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

- Inscrivez le point de confiance et générez le certificat.

```
<#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
```

- Une fois terminé, le nouveau certificat auto-signé peut être vu avec la commande **show crypto ca certificates <truspoint name>**.

```
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 CEST Jul 15 2022
end date: 15:00:58 CEST Jul 12 2032
Storage: config
Associated Trustpoints: SELF-SIGNED
```

Inscription par demande de signature de certificat (CSR)

- (Facultatif) Créez une paire de clés nommée avec une taille de clé spécifique.



Remarque : par défaut, la clé RSA avec le nom Default-RSA-Key et une taille de 2048 est utilisée ; cependant, il est recommandé d'utiliser un nom unique pour chaque certificat afin qu'ils n'utilisent pas la même paire de clés privée/publique.

```
<#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...
```

La paire de clés générée est visible à l'aide de la commande **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
```

- Créez un point de confiance avec un nom spécifique. Configurez le type d'inscription **terminal**.

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

- Configurez le nom de domaine complet et le nom de sujet. Les paramètres FQDN et Subject CN doivent correspondre au nom de domaine complet ou à l'adresse IP du service pour lequel le certificat est utilisé.

```
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=
```

- (Facultatif) Configurez le nom de la paire de clés créée à l'étape 1.

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

- (Facultatif) Configurez la méthode de vérification de la révocation de certificats - avec la liste de révocation de certificats (CRL) ou avec le protocole OCSP (Online Certificate Status Protocol). Par défaut, la vérification de révocation de certificat est désactivée.

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

- (Facultatif) Authentifiez le point de confiance et installez le certificat d'autorité de certification qui va signer le certificat d'identité comme étant approuvé. S'il n'est pas installé à cette étape, le certificat CA peut être installé ultérieurement avec le certificat d'identité.

```
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
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECXMdbGFjMRcwFQYDVQQDEw5j
YS5leGFtcG9uLmNvLnVudAeFw0xNTAyMDYxNDEwMDBaFw0zMDAyMDYxNDEwMDBa
MEUx
CzAJBgNVBAYTA1BMMQ8wDQYDVQQKEwZ3dy12cG4xDDAKBgNVBAsTA2xhYjEXMBUG
A1UEAxMOY2EuZXhhbXBsZS5jb20wggeiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQDI6pth5KFFTB29Lyn0g9/CTi0GYa+WFTcZXSLHZA6WTUzLYM19IbSFHwA6
gTeBnHqToLRnQoB51Q1xEA45ArL2G98aew8BMD08GXkxWayforwLA3U9WZVTZsVN
4noWaxH1boGGD7+5vk0esJfL2B7pEhGodLh7Gki1T4KqL/1DM9Lqkz0ctZkCT7f
SkXvFik1Z1cZEGn6b2umnIqavZ81ewIuTHOX487s3uxTPH8+B5QG0+d1wa0sbCwk
```



```
NaHki r062VQNxwIDAQABoE4wDwYJKoZIhvcNAQkHMqITADA7BgkqhkiG9w0BCQ4x
LjAsMAsGA1UdDwQEAwIFoDAdBgNVHREEFjAUGhJhc2F2cG4uZXhhbXBsZS5jb20w
DQYJKoZIhvcNAQELBQADggEBAM3Q3zvp9G3MWP7R4wkpnBOH2CNUmPENIhHNjQjH
Yh08EOvWyo09FaL fHKVDLvfXh0vn5osXBmPLuVps6Ta4sBRUNicRoAmmA0pDWL9z
Duu8BQnBGUN08T/H3ydjaNoPJ/f6EZ8gXY29NxEKb/+A2Tt0VVUTsYreGS+84Gqo
ixFOtW8R50IXg+afAV0Ah81xVUF0vuAi9DsiuvuFmB4wdngQSOe1/B9Zgp/BfGM1
l0ApejACoJAGmyrn9Tj6Z/6/lbpKBKpf4VE5UXdj7WLAjw5JF/X2NrH3/cQsczi
G2Yg2dr3WpkTIY2W/kVohTiohVRkgXOMCecUaMlYxJyLTRQ=
-----END CERTIFICATE REQUEST-----
```

Redisplay enrollment request? [yes/no]: no

- Importez le certificat d'identité. Une fois le CSR signé, un certificat d'identité est fourni.

```
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-----
MIIDoTCCAomgAwIBAgIIBkLY8Qt8N5gwDQYJKoZIhvcNAQELBQAwRTElMAkGA1UE
BhMCUExwDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECXMdbGFjMRcwFQYDVQQDEw5j
(...)
kzAihRuFqmYYUeQP2Byp/S5fNqUcyZfAczIHt8BcPmV0916iSF/ULG1zXMSOUX6N
d/LHXwrcTpc1zU+7qx3TpVDZbJlwwF+BWTBlxgMOBosJx65u/n75KnbBhGUE75jV
HX2eRzuhnnSVExCoeyed7DLiezd8
-----END CERTIFICATE-----
quit
INFO: Certificate successfully imported
```

- Vérifiez la chaîne de certificats. Une fois terminé, le nouveau certificat d'identité et le certificat de l'autorité de certification s'affichent à l'aide de la commande **show crypto ca certificates <trustpoint name>**.

```
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

Inscription PKCS12

Inscrivez-vous avec le fichier PKCS12 qui contient la paire de clés, le certificat d'identité et éventuellement la chaîne de certificats d'autorité de certification, reçus de votre autorité de certification.

- Créez un point de confiance avec un nom spécifique.

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



Remarque : la paire de clés importée porte le nom du point de confiance.

- (Facultatif) Configurez la méthode de vérification de la révocation de certificats - avec la liste de révocation de certificats (CRL) ou avec le protocole OCSP (Online Certificate Status Protocol). Par défaut, la vérification de révocation de certificat est désactivée.

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

- Importez le certificat à partir d'un fichier PKCS12.



Remarque : le fichier PKCS12 doit être codé en base64. Si des caractères imprimables apparaissent lorsque le fichier est ouvert dans l'éditeur de texte, il est codé en base64. Pour convertir un fichier binaire au format codé en base64, openssl peut être utilisé.

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

commande :

```
crypto ca import trustpoint pkcs12 passphrase \[ nointeractive \]
```

```
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  
BqCCCAgwgggEAgEAMIIH/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.

- Vérifiez le ou les certificats installés.

```
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
```

Dans l'exemple précédent, le PKCS12 contenait l'identité et le certificat CA (les deux entrées Certificat et Certificat CA). Sinon, seul le certificat est présent.

- (Facultatif) Authentifiez le point de confiance.

Si le PKCS12 ne contenait pas le certificat CA et que le certificat CA a été obtenu séparément au format PEM, il peut être installé manuellement.

```
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
BhMCUExwDzANBgNVBAoTBnd3LXZwbnJEMMAoGA1UECXMdbGFzMRcwFQYD
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

Renouvellement du certificat

Renouveler le certificat auto-signé

- Vérifiez la date d'expiration du certificat actuel.

<#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 CEDT Jul 15 2022
```

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

Storage: config
Associated Trustpoints: SELF-SIGNED

- Régénérez le certificat.

```
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
```

- Vérifiez le nouveau certificat.

<#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

Renouveler le certificat inscrit avec une demande de signature de certificat (CSR)

 **Remarque :** si l'un des nouveaux éléments de certificat (sujet/nom de domaine complet, paire de clés) doit être modifié pour le nouveau certificat, créez un nouveau certificat. Reportez-vous à la section Inscription à l'aide de la demande de signature de certificat (CSR). La procédure suivante actualise simplement la date d'expiration du certificat.

- Vérifiez la date d'expiration du certificat actuel.

<#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 CEST Jul 15 2022
```


end date: 15:33:00 CEST 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

- Inscrivez le certificat. Générez un CSR qui peut être copié et envoyé à une autorité de certification pour signature. Le CSR inclut la clé publique de la paire de clés utilisée par trustpoint - le certificat signé ne peut être utilisé que par les périphériques qui ont cette paire de clés.



Remarque : l'autorité de certification peut modifier les paramètres FQDN et Subject Name définis dans le point de confiance lors de la signature du CSR et de la création du certificat d'identité signé.



Remarque : pour le même point de confiance, sans modification de l'objet/du nom de domaine complet et de la configuration de la paire de clés, les inscriptions suivantes donnent le même CSR que le CSR initial.

```
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-----
MIIDHzCCAGcCAQAwYsXGzAZBgNVBAMEMFzYXZwbi5leGFtcGxlLmNvbTEUMBIG
A1UECGRlRXhhdXBsZSBjb250ss8ITd5g4kBdrUSCprl+VMi TphQgBTAqRPk0vFX4rC8k/T
bm1hMREwDwYDVoQHDahTYW4gSm9zZTEhMB8GCSqGSIb3DQEJAgwSYXNhbnBuLmV4
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5cvZVr1j
Me8Mz4T3vgT1Z8DAAR0avs/TBdYiqGdjyiV/3K92IIT/0r8cuAUe5rR4sjTvaXYC
SycSbwKc4kZbr3x120ss8ITd5g4kBdrUSCprl+VMi TphQgBTAqRPk0vFX4rC8k/T
0PFDE+2gjT1wMn9reb92jYro1GK4MWZdCzqowLPjEj5cCwu8Pv5h4hqTpudms+v4
g3R100Dmeyv4uEMyLS/noPxZXZ8YiQMIG2EP2BgOKOT3Fzx0mVuekonQtRhizt+c
zyyFSRoqyBSakEZBwABod8q1Eg5J/pH130J1itOUJEyI1FoVHqv3jL7zfA9i1IInu
```

```
NaHki r062VQNxwIDAQABoE4wDwYJKoZIhvcNAQkHMqITADA7BgkqhkiG9w0BCQ4x
LjAsMAsGA1UdDwQEAwIFoDAdBgNVHREEFjAUGhJhc2F2cG4uZXhhbXBsZS5jb20w
DQYJKoZIhvcNAQELBQADggEBAM3Q3zvp9G3MWP7R4wkpnBOH2CNUMPENIhHNjQjH
Yh08EOvWyo9FaL fHKVDLvFxh0vn5osXBmPLuVps6Ta4sBRUNicRoAmmA0pDWL9z
Duu8BQnBGUN08T/H3ydjaNoPJ/f6EZ8gXY29NxEKb/+A2Tt0VVUTsYreGS+84Gqo
ixF0tW8R50IXg+afAV0Ah81xVUF0vuAi9DsiuvufMb4wdngQSOe1/B9Zgp/BfGM1
l0ApgejACoJAGmyrn9Tj6Z/6/lbpKBKpf4VE5UXdj7WLAjw5JF/X2NrH3/cQsczi
G2Yg2dr3WpkTIY2W/kVohTiohVRkgXOMCecUaMlYxJyLTRQ=
-----END CERTIFICATE REQUEST-----
```

Redisplay enrollment request? [yes/no]: no

- Importez le certificat d'identité. Une fois le CSR signé, un certificat d'identité est fourni.

```
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-----
MIIDgTCCAmmgAwIBAgIIMA+aIxCTntMwDQYJKoZIhvcNAQELBQAwRTElMAkGA1UE
BhMCUExwDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECXMdbGFjMRcwFQYDVQDEw5j
YS5leGFtcGxlLmNvbTAeFw0yMjA3MjAxNDA5MDBaFw0yMjA3MjAxNDA5MDBaMIIG
MRswGQYDVQDDbJhc2F2cG4uZXhhbXBsZS5jb20xZDAsBgNVBAoMCOV4YW1wbGUg
SW5jMjQwCQYDVQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcn5pYTERMA8GA1UEBwwI
U2FuIEpvc2UxITAFBgkqhkiG9w0BCQIMemFzYXZwbi5leGFtcGxlLmNvbTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOXL2Va9YzHvDM+E974E9WfAwAEd
Gr7P0wXWIqhnY8o1f9yvdiCE/9K/HLgFHua0eLI07212AksnEm8Cn0JGW698ddtL
LPCLXeY0JAXa1Egqa5f1TIk6YUIAUwKkT5NLxV+KwvJP09DxQxPtoI09cDJ/a3m/
do2K6JRiudFmXQs6qMCz4xI+XAsLvD7+YeIak6bnZrPr+IN0dTjg5nsr+LhDGC0v
56D8WV2fGIkdIhthD9gYncjk9xc8dJlbnPKJ0LUYYmbfnM8sn0kaKsgUmpBGQcAA
aHfKtRi0Sf6R9d9CZyrtlCRMiJRaFR6r94y+83wPYpSJ7jWh5Iq90t1UDV8CAwEA
AaMuMCwwCwYDVR0PBAQDAgWgMB0GA1UdEQQWMBSCemFzYXZwbi5leGFtcGxlLmNv
bTANBgkqhkiG9w0BAQsFAA0CAQEAFQuChY4UjhjkySMJAh7NT3TT5JJ4NzqW8qHa
wNq+YyHR+sQ6G3vn+6cYCU87tqWlY3fXC27TtweREwM8q8NsJrr80hsChYby8kwE
LnTkrN7dJB17u50VQ3DRjfmFrJ9LEUaYZx1HYvcS1kAeEeVB4VJwVzeujWepcmEM
p7cB6veTcF9ru1DVRImd0KYEOx+HYav2INT2udc0G1yDwm1/mqdf0/ON2SpBBpnE
gtiKshtsST/NAw25WjkrDIfn8uR2z5xpzxNEDUBoHOipG1gb1I6G1ARXW0+LwfB1
n1QD5b/RdQ0UblCpFKNPdE/9wNnoXGD1J7qfZxr04T71d2Idug==
-----END CERTIFICATE-----
quit
```

```
INFO: Certificate successfully imported
```

- Vérifiez la date d'expiration du nouveau certificat.

```
<#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
```

Renouvellement PKCS12

Il n'est pas possible de renouveler un certificat dans un point de confiance inscrit à l'aide du fichier PKCS12. Pour installer un nouveau certificat, un nouveau point de confiance doit être créé.

- Créez un point de confiance avec un nom spécifique.

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

- (Facultatif) Configurez la méthode de vérification de la révocation de certificats - avec la liste de révocation de certificats (CRL) ou avec le protocole OCSP (Online Certificate Status Protocol). Par défaut, la vérification de révocation de certificat est désactivée.

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

- Importez le nouveau certificat à partir d'un fichier PKCS12.



Remarque : le fichier PKCS12 doit être codé en base64. Si des caractères imprimables apparaissent lorsque le fichier est ouvert dans l'éditeur de texte, il est codé en base64. Pour convertir un fichier binaire au format codé en base64, openssl peut être utilisé.

```
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
BqCCCAgwgggEAgEAMIH/QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMDgQIiK0c
wqE3Tm0CaggAgIIH0NjxmJBuoPRuY11VxTiawHzsL8kI10310j7tcWmECBwzsKKq
(...)
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.



Remarque : si le nouveau fichier PKCS12 contient un certificat d'identité avec la même paire de clés que celle utilisée avec l'ancien certificat, le nouveau point de confiance fait référence à l'ancien nom de paire de clés.
Exemple :

```
<#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

- Vérifiez le ou les certificats installés.

<#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=asavnpkcs12chain.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
```

Dans l'exemple précédent, le PKCS12 contenait le certificat d'identité et le certificat d'autorité de certification. Par conséquent, deux entrées apparaissent après l'importation, Certificate et CA Certificate. Sinon, seule l'entrée de certificat est présente.

- (Facultatif) Authentifiez le point de confiance.

Si le PKCS12 ne contenait pas le certificat CA et que le certificat CA a été obtenu séparément au format PEM, il peut être installé manuellement.

```
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
BhMCUExwDzANBgNVBAoTBnd3LXZwbyEMMAoGA1UECXMdbGFjMRcwFQYDVQQDEw5j
(...)
gW8YnHOvM08svyTXSL1Jf0UCdmAY+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
```

- Reconfigurez l'ASA pour utiliser le nouveau point de confiance au lieu de l'ancien.

Exemple :

```
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
```

 **Remarque :** un point de confiance peut être utilisé dans différents éléments de configuration. Vérifiez votre configuration à l'endroit où l'ancien point de confiance est utilisé.

Informations connexes

Comment configurer les paramètres d'heure sur un ASA.

Consultez cette référence pour connaître les étapes requises pour configurer correctement l'heure et la date sur l'ASA. [Guide de configuration CLI 1 : Cisco Secure Firewall ASA Series General Operations CLI Configuration Guide, 9.18](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.