

Instalación y renovación de certificados en ASA administrados por CLI

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Instalación de certificados](#)

[Inscripción de certificados con firma automática](#)

[Inscripción por solicitud de firma de certificado \(CSR\)](#)

[Inscripción en PKCS12](#)

[Renovación de certificados](#)

[Renovación del certificado autofirmado](#)

[Renovar certificado inscrito con solicitud de firma de certificado \(CSR\)](#)

[Renovación PKCS12](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo solicitar, instalar, confiar y renovar determinados tipos de certificados en el software Cisco ASA administrado con CLI.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Compruebe que el dispositivo de seguridad adaptable (ASA) tiene la hora, fecha y zona horaria del reloj correctas. Con la autenticación de certificados, se recomienda utilizar un servidor de protocolo de tiempo de la red (NTP) para sincronizar la hora en el ASA. Marque Información relacionada para referencia.
- Para solicitar un certificado que utilice la Solicitud de firma de certificado (CSR), se requiere acceso a una Autoridad de certificación (CA) interna o de terceros de confianza. Algunos ejemplos de proveedores de CA de terceros son, entre otros, Entrust, Geotrust, GoDaddy, Thawte y VeriSign.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ASAv 9.18.1
- Para la creación de PKCS12, se utiliza OpenSSL.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El tipo de certificados a los que se dirige este documento son certificados autofirmados, certificados firmados por una autoridad de certificación de terceros o CA interna en el software de dispositivo de seguridad adaptable de Cisco administrado con la interfaz de línea de comandos (CLI).

Instalación de certificados

Inscripción de certificados con firma automática

1. (Opcional) Cree un par de claves con nombre con un tamaño de clave específico.



Nota: De forma predeterminada, se utiliza la clave RSA con el nombre Default-RSA-Key y un tamaño de 2048; sin embargo, se recomienda utilizar un nombre único para cada certificado para que no utilicen el mismo par de claves pública/privada.

```
<#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...
```

El par de claves generado se puede ver con el comando `show crypto key mypubkey rsa`.

```
<#root>
```

ASAv#

```
show crypto key mypubkey rsa
```

(...)

Key pair was generated at: 14:52:49 CEST 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
```

- Cree un punto de confianza con un nombre específico. Configure el tipo de inscripción **automáticamente**.

<#root>

ASAv(config)#

```
crypto ca trustpoint
```

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

enrollment self

- Configure el nombre de dominio completo (FQDN) y el nombre de asunto.



Precaución: el parámetro FQDN debe coincidir con el FQDN o la dirección IP de la interfaz ASA para la que se utiliza el certificado. Este parámetro establece el nombre alternativo del sujeto (SAN) para el certificado.

<#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

- (Opcional) Configure el nombre del par de claves creado en el paso 1. No es necesario si se utiliza el par de claves predeterminado.

<#root>

ASAv(config-ca-trustpoint)#

keypair

SELF-SIGNED-KEYPAIR

ASAv(config-ca-trustpoint)# exit

- Inscriba el punto de confianza y genere el certificado.

<#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

- Una vez completado, el nuevo certificado autofirmado se puede ver con el comando **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
```

Inscripción por solicitud de firma de certificado (CSR)

- (Opcional) Cree un par de claves con nombre con un tamaño de clave específico.



Nota: De forma predeterminada, se utiliza la clave RSA con el nombre Default-RSA-Key y un tamaño de 2048; sin embargo, se recomienda utilizar un nombre único para cada certificado para que no utilicen el mismo par de claves pública/privada.

<#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...

El par de claves generado se puede ver con el comando **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
```

- Cree un punto de confianza con un nombre específico. Configure el **terminal** de tipo de inscripción.

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

- Configure el nombre de dominio completo y el nombre de asunto. Los parámetros FQDN y Subject CN deben coincidir con el FQDN o la dirección IP del servicio para el que se utiliza el certificado.

```
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=
```

- (Opcional) Configure el nombre del par de claves creado en el paso 1.

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

- (Opcional) Configure el método de comprobación de revocación de certificados: con la Lista de revocación de certificados (CRL) o con el Protocolo de estado de certificados en línea (OCSP). De forma predeterminada, la comprobación de revocación de certificados está deshabilitada.

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

- (Opcional) Autentique el punto de confianza e instale el certificado de CA que firmará el certificado de identidad como de confianza. Si no se instala en este paso, el certificado de la CA se puede instalar más adelante junto con el certificado de identidad.

```
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
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECzMdbGFjMRcwFQYDVoQDEw5j
```



```
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5cvZVr1j
Me8Mz4T3vgT1Z8DAAR0avs/TBdYiqGdjiV/3K92IIT/0r8cuAUe5rR4sjTvaXYC
SycSbwKc4kZbr3x120ss8ItD5g4kBdrUSCprl+VMiTphQgBTAqRPk0vFX4rC8k/T
0PFDE+2gjT1wMn9reb92jYro1GK4MWZdCzqowLPjEj5cCwu8Pv5h4hqTpudms+v4
g3R100Dmeyv4uEMyLS/noPxZXZ8YiQMiG2EP2BgOKOT3Fzx0mVuekonQtRhiZt+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

- Importe el certificado de identidad. Una vez firmado el CSR, se proporciona un certificado de identidad.

```
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
BhMCUExwDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECXMdbGFjMRcwFQYDVQQDEw5j
(...)
kzAihRuFqmYYUeQP2Byp/S5fNqUcyZfAczIHt8BcPmV0916iSF/ULG1zXMSOUX6N
d/LHXwrcTpc1zU+7qx3TpVDZbJ1wwF+BWTB1xgM0BosJx65u/n75KnbBhGUE75jV
HX2eRzuhnnSVExCoeyed7DLiezd8
-----END CERTIFICATE-----
quit
INFO: Certificate successfully imported
```

- Verifique la cadena de certificados. Una vez completados, el nuevo certificado de identidad y el certificado de la CA se pueden ver con el comando **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
```

Inscripción en PKCS12

Inscríbase con el archivo PKCS12 que contiene el par de claves, el certificado de identidad y, opcionalmente, la cadena de certificados de la CA, recibidos de la CA.

- Cree un punto de confianza con un nombre específico.

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



Nota: El par de claves importado recibe el nombre del punto de confianza.

- (Opcional) Configure el método de comprobación de revocación de certificados: con la Lista de revocación de certificados (CRL) o con el Protocolo de estado de certificados en línea (OCSP). De forma predeterminada, la comprobación de revocación de certificados está deshabilitada.

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

- Importe el certificado desde un archivo PKCS12.



Nota: El archivo PKCS12 debe estar codificado en base64. Si se ven caracteres imprimibles cuando se abre el archivo en el editor de texto, entonces está codificado en base64. Para convertir un archivo binario a base64 se puede utilizar el formato codificado openssl.

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

Comando:

```
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  
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.

- Verifique los certificados instalados.

```
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

En el ejemplo anterior, el PKCS12 contenía la identidad y el certificado de CA, las dos entradas: Certificate y CA Certificate. De lo contrario, sólo está presente el certificado.

- (Opcional) Autentique el punto de confianza.

Si el PKCS12 no contenía el certificado de CA y el certificado de CA se obtuvo por separado en formato PEM, se puede instalar manualmente.

```
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-----  
MIIDXCcCAkSgAwIBAgIIDM/QY/h29+kwDQYJKoZIhvcNAQELBQAwRTElMAkGA1UE  
BhMCUExwEwZzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECXMdbGFjMRcwFQYD  
VQDEw5j (...)  
gW8YnH0vM08svyTXSL1Jf0UCdmAY+1G0gqhU1S1kFBtLRt6Z2uCot00NoMHI0hh5  
dcVcov0i/PAXnrA1J+Ng2jrWFn3MXWZ04S3CHYMGkqHkaHCh1qD0x9badgfsyzz
```

-----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

Renovación de certificados

Renovación del certificado autofirmado

- Compruebe la fecha de vencimiento del certificado actual.

<#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

- Regenere el certificado.

```
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
```

- Verifique el nuevo certificado.

<#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

Renovar certificado inscrito con solicitud de firma de certificado (CSR)

 **Nota:** Si es necesario cambiar alguno de los nuevos elementos del certificado (subject/fqdn, keypair) para el nuevo certificado, cree un nuevo certificado. Consulte la sección Inscripción mediante la solicitud de firma de certificado (CSR). El siguiente procedimiento simplemente actualiza la fecha de vencimiento del certificado.

- Compruebe la fecha de vencimiento del certificado actual.

<#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

- Inscriba el certificado. Genere una CSR que se pueda copiar y enviar a una CA para su firma. El CSR incluye la clave pública del par de claves utilizado por trustpoint: el certificado firmado sólo puede ser utilizado por dispositivos que tengan ese par de claves.



Nota: CA puede modificar los parámetros FQDN y nombre de sujeto definidos en el punto de confianza al firmar el CSR y crear el certificado de identidad firmado.



Nota: Para el mismo Trustpoint, sin cambio de sujeto/fqdn y configuración de par de claves, las inscripciones subsiguientes dan el mismo CSR que la inicial.

```
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-----
MIIDHzCCAQcCAQAwYsxCzAUBgNVBAMEMFZlYXZwbi5leGFtcGx1LmNvbTEUMBIG
A1UECgwLRXhhbXBsZSBJamMxCzAJBgNVBAYTA1VTMRMwEQYDVQQIDApDYWxpZm9y
bm1hMREwDwYDVQQHDAhTYW4gSm9zZTEhMB8GCSqGSIb3DQEJAgwSYXNhdnBuLmV4
```

```
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAE5cvZVr1j
Me8Mz4T3vgT1Z8DAAR0avs/TBdYiqGdjyiV/3K92IIT/0r8cuAUe5rR4sjTvaXYC
SycSbwKc4kZbr3x120ss8ItD5g4kBdrUSCprl+VMiTphQgBTAqRPk0vFX4rC8k/T
0PFDE+2gjT1wMn9reb92jYro1GK4MWZdCzqowLPjEj5cCwu8Pv5h4hqTpudms+v4
g3R100Dmeyv4uEMyLS/noPxZXZ8YiQMIG2EP2BgOKOT3Fzx0mVuekonQtRhiZt+c
zyyFSRoqyBSakEZBwABod8q1Eg5J/pH130J1iTOUJEyI1FoVHqv3jL7zfA9i1Inu
NaHkiR062VQNxwIDAQABoE4wDwYJKoZIhvcNAQkHMqITADA7BgkqhkiG9w0BCQ4x
LjAsMAsGA1UdDwQEAwIFoDAdBgNVHREEFjAUGhJhc2F2cG4uZXhhbXBsZS5jb20w
DQYJKoZIhvcNAQELBQADggEBAM3Q3zvp9G3MWP7R4wkpnBOH2CNUMPENIhHNjQjH
Yh08EOvWyo9FaLfhKVDLvfXh0vn5osXBmPLuVps6Ta4sBRUNicRoAmmA0pDWL9z
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

- Importe el certificado de identidad. Una vez firmado el CSR, se proporciona un certificado de identidad.

```
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
BhMCUExwDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECXMdbGFjMRcwFQYDVQQDEw5j
YS51eGFtcGxlLmNvbTAeFw0yMjA3MjAxNDA5MjA3MjAxNDA5MjA3MjAxNDA5MjA3
MRswGQYDVQQDDHJhc2F2cG4uZXhhbXBsZS5jb20wFDASBgNVBAoMCOV4YW1wbGUg
SW5jMjA3MjA3MjA3MjA3MjA3MjA3MjA3MjA3MjA3MjA3MjA3MjA3MjA3MjA3MjA3
U2FuIEpvc2UxITAfBgkqhkiG9w0BCQIMFzYXZwbi51eGFtcGxlLmNvbTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAAOXL2Va9YzHvDM+E974E9WfAwAEd
Gr7P0wXWlqhnY8o1f9yvdiCE/9K/HLgFHua0eLI07212AksnEm8Cn0JGW698ddtL
LPCLXeYOJAXa1Egga5f1TIk6YUIAUwKkT5NLxV+KwwJP09DxQxPtIoI09cDJ/a3m/
do2K6JRiudFmXQs6qMCz4xI+XAsLvD7+YeIak6bnZrPr+IN0dTjg5nsr+LhDGC0v
56D8WV2fGIkDIhthD9gYncjk9xc8dJ1bnPKJ0LUYYmbfnM8sn0kaKsgUmpBGQcAA
aHfKtRIOsF6R9d9CZYrT1CRMiJRaFR6r94y+83wPYpSJ7jWh5Iq90t1UDV8CAwEA
AaMuMCwwCwYDVR0PBAQDAgWgMB0GA1UdEQQWMBSCEmFzYXZwbi51eGFtcGxlLmNv
bTANBgkqhkiG9w0BAQsFAAOCAQEAFUchY4UjhjkySMJAh7NT3TT5JJ4NzqW8qHa
wNq+YyHR+sQ6G3vn+6cYCU87tqW1Y3fXC27TtweREwMmq8NsJrr80hsChYby8kwE
LnTkrN7dJB17u50VQ3DRjfmFrJ9LEUaYZx1HYvcS1kAeEeVB4VJwVzeujWepcmEM
p7cB6veTcF9ru1DVRImd0KYE0x+HYav2INT2udc0G1yDwm1/mqdf0/ON2SpBBpnE
gtiKshtsST/NAw25WjkrDIfn8uR2z5xpzxnEDUBoHoipG1gb1I6G1ARXW0+Lwfb1
n1QD5b/RdQ0UblCpFKNPdE/9wNnoXGD1J7qfZxr04T71d2Idug==
-----END CERTIFICATE-----
quit
```

```
INFO: Certificate successfully imported
```

- Verifique la fecha de vencimiento del nuevo certificado.

<#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
```

Renovación PKCS12

No es posible renovar un certificado en el punto de confianza inscrito mediante el archivo PKCS12. Para instalar un nuevo certificado, es necesario crear un nuevo punto de confianza.

- Cree un punto de confianza con un nombre específico.

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

- (Opcional) Configure el método de comprobación de revocación de certificados: con la Lista de revocación de certificados (CRL) o con el Protocolo de estado de certificados en línea (OCSP). De forma predeterminada, la comprobación de revocación de certificados está deshabilitada.

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

- Importe el nuevo certificado desde un archivo PKCS12.



Nota: El archivo PKCS12 debe estar codificado en base64. Si se ven caracteres imprimibles cuando se abre el archivo en el editor de texto, entonces está codificado en base64. Para convertir un archivo binario a una forma codificada en base64, se puede utilizar openssl.

```
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  
wqE3Tm0CAggAgIIH0NjxmJBuoPRuYl1VxTiawHzsL8kI10310j7tcWmECBwzsKKq  
(...)  
PXowMwYJKoZIhvcNAQkUMSYeJABhAHMAYQB2AHAAbgAuAGUAeABhAG0AcABSAGUA  
LgBjAG8AbTAtMCEwCQYFKw4DAhoFAAQUPXZZtBeqlh98wQ1jHW7J/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.



Nota: Si el nuevo archivo PKCS12 contiene un certificado de identidad con el mismo par de claves que se utilizó con el certificado anterior, el nuevo punto de confianza hace referencia al nombre del par de claves anterior.
Ejemplo:

```
<#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
```

- Verifique los certificados instalados.

```
<#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
```



```
trustpoint to limit the validation scope, if necessary.
```

```
Trustpoint CA certificate accepted.
```

```
% Certificate successfully imported
```

- Vuelva a configurar ASA para utilizar el nuevo punto de confianza en lugar del anterior.

Ejemplo:

```
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
```



Nota: Se puede utilizar un punto de confianza en diferentes elementos de configuración. Compruebe la configuración en la que se utiliza el punto de confianza antiguo.

Información Relacionada

Cómo configurar la hora en un ASA.

Consulte esta referencia para conocer los pasos necesarios para configurar la fecha y la hora correctamente en el ASA. [Manual de CLI 1: Guía de configuración de CLI de las operaciones generales de Cisco Secure Firewall ASA, 9.18](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).