

# 在CLI管理的ASA上安裝並續訂證書

## 目錄

---

### [簡介](#)

### [必要條件](#)

#### [需求](#)

#### [採用元件](#)

### [背景資訊](#)

### [證書安裝](#)

#### [自簽名證書註冊](#)

#### [Enrollment By Certificate Signing Request\(CSR\)](#)

#### [PKCS12註冊](#)

### [證書續訂](#)

#### [續訂自簽名證書](#)

#### [使用證書簽名請求\(CSR\)註冊續訂證書](#)

#### [PKCS12續訂](#)

### [相關資訊](#)

---

## 簡介

本文檔介紹如何在通過CLI管理的Cisco ASA軟體上請求、安裝、信任和續訂特定型別的證書。

## 必要條件

### 需求

- 驗證自適應安全裝置(ASA)具有正確的時鐘時間、日期和時區。進行憑證驗證時，建議使用網路時間通訊協定 (NTP) 伺服器同步化 ASA 的時間。檢查相關資訊以供參考。
- 若要請求使用憑證簽署請求(CSR)的憑證，需要存取受信任的內部或第三方憑證授權單位 (CA)。第三方CA供應商的示例包括 ( 但不限於 ) Entrust、Geotrust、GoDaddy、Thawte和VeriSign。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ASA v 9.18.1
- 建立PKCS12時使用OpenSSL。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

# 背景資訊

此文檔解決的證書型別為自簽名證書、第三方證書頒發機構簽名的證書或內部CA(在用命令列介面(CLI)管理的思科自適應安全裝置軟體上)。

## 證書安裝

### 自簽名證書註冊

1. (可選) 建立具有特定金鑰大小的命名金鑰對。



注意：預設情況下，使用名為Default-RSA-Key且大小為2048的RSA金鑰；但是，建議對每個證書使用唯一的名稱，以便它們不使用相同的專用/公共金鑰對。

```
<#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...
```

生成的金鑰對可以使用命令檢視 `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. 建立具有特定名稱的信任點。自行配置註冊型別。

```
<#root>
ASAv(config)#
crypto ca trustpoint
    SELF-SIGNED
ASAv(config-ca-trustpoint)#
enrollment self
```

3. 配置完全限定域名(FQDN)和使用者名稱。

---

 注意: FQDN引數必須與證書使用的ASA介面的FQDN或IP地址匹配。此引數設定證書的使用者替代名稱(SAN)。

---

```
<#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. ( 可選 ) 配置在步驟1中建立的金鑰對名稱。如果使用預設金鑰對，則不需要此項。

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

5. 註冊信任點並生成證書。

```
<#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. 完成後，可以使用命令檢視新的自簽名證書 `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
```

## 按證書簽名請求(CSR)註冊

1. (可選) 建立具有特定金鑰大小的命名金鑰對。



注意：預設情況下，使用名為Default-RSA-Key且大小為2048的RSA金鑰；但是，建議對每個證書使用唯一的名稱，以便它們不使用相同的專用/公共金鑰對。

---

```
<#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...
```

生成的金鑰對可以使用命令檢視 `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:
    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. 建立具有特定名稱的信任點。配置註冊型別終端。

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

## 3. 配置完全限定域名和使用者名稱。FQDN和主題CN引數必須與使用證書的服務的FQDN或IP地址匹配。

```
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. ( 可選 ) 配置在步驟1中建立的金鑰對名稱。

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

- (可選) 配置證書撤銷檢查方法 — 使用證書撤銷清單(CRL)或線上證書狀態協定(OCSP)。預設情況下，證書吊銷檢查處於禁用狀態。

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

- (可選) 對信任點進行身份驗證，並安裝將身份證書簽名為受信任的CA證書。如果在此步驟中未安裝，則稍後可以將CA證書與身份證書一起安裝。

```
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
YS57eGFtcGx1LmNvbTAeFw0xNTAyMDYxNDEwMDBaFw0zMDAyMDYxNDEwMDBaMEUx
CzAJBgNVBAYTA1BMMQ8wDQYDVQQKEwZ3dy12cG4xDDAKBgNVBAsTA2xhYjEXMBUG
A1UEAxMOY2EuZXhhbXBsZS5jb20wgGEMMA0GCSqSISIb3DQEBAQUAA4IBDwAwggEK
AoIBAQDI6pth5KFFTB29Lyn0g9/CTi0GYa+WFTcZXSLHZA6WTUzLYM19IbSFHWa6
gTeBnHqToLRnQoB51Q1xEA45ArL2G98aew8BMD08GXkxWayforwLA3U9WZVTZsVN
4noWaXH1boGGD7+5vk0esJfL2B7pEhGodLh7Gki1T4KoqL/1DM9Lqkz0ctZkCT7f
SkXvFik1Z1cZEGn6b2umnIqaVZ81ewIuTH0X481s3uxTPH8+B5QG0+d1wa0sbCwk
oK5sEPpHZ3IQuVxGiirp/zmomzx14G/te16eyMOpjpnVtDYjQ9HNkQdQT5LKwRsX
Oj9xKnYCbPfg3p2FdH7wJh11K3prAgMBAAGjUDBOMAwGA1UdEwQFMAMBAF8wHQYD
VR00BBYEF55kZsbra9b9tLFV52U47em9uXaMB8GA1UdIwQYMBaAFE55kZsbra9b
9tLFV52U47em9uXaMA0GCSqSISIb3DQEBcWUAA4IBAQArsX1FwK3j1NBw0sYh5mqT
cGqeyDMRhs3Rs/wD25M2wkAF4AYZHgN9gK9VCK+ModKMQZy4X/uhj65NDU7oFF6f
z9kqarjjsx153jV/YLk8E9oAIatnA/fQfX6V+h74yqucfF1js3d1FjyV14odRPwM
0jRyja1H56BF1ackNc7KRddtVxYB9sfEbFhN8od1BvnUedxGAJFHqxEQKmbE+h4w
gW8YnHOvM08svyTXSL1Jf0UCdmAY+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
```

- 註冊證書並生成可複製並傳送到CA進行簽名的CSR。CSR包括信任點使用的金鑰對中的公鑰。只有具有此金鑰對的裝置才能使用已簽名的證書。



注意：簽署CSR和建立簽名身份證書時，CA可以更改信任點中定義的FQDN和主體名稱引數。

```
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-----
MIIDHzCCAgcCAQAwYsGzAZBgNVBAMMEFzYXZwbi5leGFtcGxlLmNvbTEUMBIG
A1UECgwLRXhhbXBsZSBJbmMxCzAJBgNVBAYTA1VTMRMwEQYDVQIDApDYWxpZm9y
bm1hMREwDwYDVQQHDAhTYW4gSm9zZTEhMB8GCSqGSIb3DQEJAgwSYXNhdnBuLmV4
YW1wbGUuY29tMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAS5cvZVr1j
Me8Mz4T3vgT1Z8DAAR0avs/TBdYiqGdjyiV/3K92IIT/0r8cuAUe5rR4sjTvaXYC
SycSbwKc4kZbr3x120ss8ItD5g4kBdrUSCprl+VMiTphQgBTAqRpk0vFX4rC8k/T
0PFDE+2gjT1wMn9reb92jYro1GK4MWZdCzqowLPjEj5cCwu8Pv5h4hqTpudms+v4
g3R100Dmeyv4uEMyLS/noPxZXZ8YiQMIG2EP2BgOKOT3Fzx0mVuekonQtRhiZt+c
zyyFSRoqyBSakEZBwABod8q1Eg5J/pH130J1itOUJEyI1FoVHqv3jL7zfA9i1Inu
NaHkiR062VQNxwIDAQABoE4wDwYJKoZIhvcNAQkHMqITADA7BgkqhkiG9w0BCQ4x
LjAsMAsGA1UdDwQEAwIFoDAdBgNVHREEFjAUGhJhc2F2cG4uZXhhbXBsZS5jb20w
DQYJKoZIhvcNAQELBQADggEBAM3Q3zvp9G3MWP7R4wkpnBOH2CNUmPENIhHNjQjH
Yh08EOvWyo09FaL fHKVDLvfXh0vn5osXBmPLuVps6Ta4sBRUNicRoAmmA0pDWL9z
Duu8BQnBGUN08T/H3yjdjaNoPJ/f6EZ8gXY29NXEKb/+A2Tt0VVUTsYreGS+84Gqo
ixF0tW8R50IXg+afAV0Ah81xVUF0vuaAi9DsiuvufMb4wdngQSOe1/B9Zgp/BfGM1
10ApejACoJAGmyrn9Tj6Z/6/1bpKBKpf4VE5UXdj7WLAjw5JF/X2NrH3/cQsczi
G2Yg2dr3WpkTIY2W/kVohTiohVRkgXOMCecUaM1YxJyLTRQ=
-----END CERTIFICATE REQUEST-----
```

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

8. 匯入身份證書。簽署CSR後，會提供身份證書。

```
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-----
MIIDoTCCAomgAwIBAgIIKbLY8Qt8N5gwDQYJKoZIhvcNAQELBQAwRTELMkGA1UE
BhMCUeWxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECXMdbGFjMRcwFQYDVQQDEw5j
(...)
kzAihRuFqmYYUeQP2Byp/S5fNqUcyZfAczIht8BcPmV0916iSF/ULG1zXMSOUX6N
```

```
d/LHXwrcTpc1zU+7qx3TpVDZbJlwwF+BWTB1xgMOBosJx65u/n75KnbBhGUE75jV
HX2eRzuhnnSVExCoeyed7DLiezD8
-----END CERTIFICATE-----
quit
INFO: Certificate successfully imported
```

## 9. 驗證憑證鏈結。完成後，可以使用命令檢視新的身份證書和CA證書 `show crypto ca certificates`

```
ASA# 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
```



使用從您的CA接收的PKCS12檔案，該檔案包含金鑰對、身份證書和（可選）CA證書鏈。

### 1. 建立具有特定名稱的信任點。

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

---

 注意：匯入的金鑰對以信任點名稱命名。


---

### 2. （可選）配置證書撤銷檢查方法 — 使用證書撤銷清單(CRL)或線上證書狀態協定(OCSP)。預設情況下，證書吊銷檢查處於禁用狀態。

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

### 3. 從PKCS12檔案匯入證書。

---

 註：PKCS12檔案需要進行base64編碼。如果在文本編輯器中開啟檔案時看到可列印字元，則該檔案為base64編碼。若要將二進位制檔案轉換為base64編碼格式，可使用openssl。

```
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
wqE3Tm0CAggAgIIH0NjxmJBuoPRuY11VxTiawHzsL8kI10310j7tcWmECBwzsKKq
(...)
```

```
PXowMwYJKoZIhvcNAQkUMSYeJABhAHMAYQB2AHAAbgAuAGUAeABhAG0AcABsAGUA
LgBjAG8AbTAtMCEwCQYFKw4DAhoFAAQUPXZZtBeq1h98wQ1jHW7J/hqKcwECD05
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. 驗證安裝的證書。

```
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
```

在上一個示例中，PKCS12包含身份和CA證書 — 兩個條目 — 證書和CA證書。否則，只有憑證存在。

## 5. ( 可選 ) 驗證信任點。

如果PKCS12不包含CA證書，並且以PEM格式單獨獲取CA證書，則可以手動安裝該證書。

```
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
BhMCUEEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECzMdbGFjMRcwFQYDVQQDEw5j
(...)
gW8YnHOvM08svyTXSL1Jf0UCdmAY+1G0gqhU1S1kFBtLRt6Z2uCot00NoMHI0hh5
dcVcovOi/PAXnrA1J+Ng2jrWFN3MXWZ04S3CHYMGkHqHkaHCh1qD0x9badgfsyzz
-----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
```

## 證書續訂

### 續訂自簽名證書

#### 1. 檢查當前證書到期日期。

```
<#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. 重新生成證書。

```
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. 驗證新憑證。

```
<#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
```

## 使用證書簽名請求(CSR)註冊續訂證書

---

 注意：如果需要為新證書更改任何新證書元素 ( subject/fqdn、金鑰對 )，則建立新證書。請參閱使用憑證簽署請求(CSR)進行註冊部分。下一個過程只是刷新證書到期日期。

---

## 1. 檢查當前證書到期日期。

```
<#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. 註冊證書。生成可以複製並傳送到CA進行簽名的CSR。CSR包括信任點使用的金鑰對中的公鑰 — 只有具有該金鑰對的裝置才能使用已簽名的證書。



注意：簽署CSR和建立簽名身份證書時，CA可以更改信任點中定義的FQDN和主體名稱引數。



注意：對於同一信任點，若沒有更改主題/fqdn和金鑰對配置，後續註冊將給出與初始註冊相同的CSR。

```
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-----
MIIDHzCCAqCAQAwYsGzAZBgNVBAMMEFzYXZwbi5leGFtcGxlLmNvbTEUMBIG
A1UECgwLRXhhbXBsZSBJbmMxCzAJBgNVBAYTA1VTMRMwEQYDVQIDApDYWxpZm9y
bm1hMREwDwYDVQQHDAhTYW4gSm9zZTEhMB8GCSqGSIb3DQEJAgwSYXNhbnBuLmV4
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5cvZVr1j
Me8Mz4T3vgT1Z8DAAR0avs/TBdYiqGdjyiv/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
l0ApgejACoJAGmyrn9Tj6Z/6/lbpKBKpf4VE5UXdj7WLAjw5JF/X2NrH3/cQsczi
G2Yg2dr3WpkTIY2W/kVohTiohVRkgXOMCecUaM1YxJyLTRQ=
-----END CERTIFICATE REQUEST-----
```

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

### 3. 匯入身份證書。簽署CSR後，會提供身份證書。

```
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
BhMCUEwDzANBgNVBAoTBnd3LXZwbiEMMAoGA1UECXMdbGFjMRcwFQYDVQQDEw5j
YS5leGFtcGxlLmNvbTAeFw0yMjA3MjAxNDA5MDBaFw0yMjA3MjAxNDA5MDBaMIIG
MRswGQYDVQQDBHJhc2F2cG4uZXhhbXBsZS5jb20xZDAsBgNVBAoMCOV4YW1wbGUg
SW5jMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcj5pYTERMA8GA1UEBwwI
U2FuIEpvc2UxITAFBgkqhkiG9w0BCQIMFzYXZwbi5leGFtcGxlLmNvbTEUMBIG
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOXL2Va9YzHvDM+e974E9WfAwAEd
Gr7P0wXWlqhnY8o1f9yvdiCE/9K/HLgFHua0eLI07212AksnEm8Cn0JGW698ddtL
LPCLXeY0JAXa1Egga5f1TIk6YUIAUwKkT5NLxV+KwvJP09DxQxPtoI09cDJ/a3m/
do2K6JRiudFmXqs6qMCz4xI+XAsLvD7+YeIak6bnZrPr+IN0dTjg5nsr+LhDGC0v
56D8WV2fGIkDIhthD9gYncjk9xc8dJlbnPKJ0LUYYmbfnM8sn0kaKsgUmpBGQcAA
aHfKtRiOsF6R9d9CZyrt1CRMiJRaFR6r94y+83wPypSj7jWh5Iq90t1UDV8CAwEA
AaMuMCwwCwYDVR0PBAQDAgWgMB0GA1UdEQQWMBSCEmFzYXZwbi5leGFtcGxlLmNv
bTANBgkqhkiG9w0BAQsFAAOCAQEAfQUchY4UjhjkySMJAh7NT3TT5JJ4NzqW8qHa
wNq+YyHR+sQ6G3vn+6cYCU87tqW1Y3fXC27TwwerEWmbq8NsJrr80hsChYby8kwE
LnTkrN7dJB17u50VQ3DRjfmFrJ9LEUaYzX1HYvcS1kAeEeVB4VJwVzeujWepcmEM
```

```
p7cB6veTcF9ru1DVRImd0KYE0x+HYav2INT2udc0G1yDwm1/mqdf0/ON2SpBBpnE
gtiKshtsST/NAw25WjkrDIfn8uR2z5xpzxnEDUBoHOipG1gb1I6G1ARXW0+LwfB1
n1QD5b/RdQ0UbLCpfKNPdE/9wNnoXGD1J7qfZxr04T71d2Idug==
-----END CERTIFICATE-----
quit
```

INFO: Certificate successfully imported

#### 4. 驗證新證書到期日期。

```
<#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
```

## PKCS12續訂

無法在使用PKCS12檔案註冊的信任點中續訂證書。要安裝新證書，需要建立新的信任點。

### 1. 建立具有特定名稱的信任點。


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

### 2. ( 可選 ) 配置證書撤銷檢查方法 — 使用證書撤銷清單(CRL)或線上證書狀態協定(OCSP)。預設情況下，證書吊銷檢查處於禁用狀態。

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

### 3. 從PKCS12檔案匯入新證書。

---

 註：PKCS12檔案需要進行base64編碼。如果在文本編輯器中開啟檔案時看到可列印字元，則該檔案為base64編碼。要將二進位制檔案轉換為base64編碼形式，可以使用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  
BqCCCAgwgggEAgEAMIIH/QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIiK0c  
wqE3Tm0CAggAgIIH0NjxmJBuoPRuY11VxTiawHzsL8kI10310j7tcWmECBwzsKKq  
(...)  
PXowMwYJKoZIhvcNAQkUMSYeJABhAHMAYQB2AHAAbgAuAGUAeABhAG0AcABsAGUA  
LgBjAG8AbTAtMCEwCQYFKw4DAhoFAAQUPXZZtBeq1h98wQ1jHW7J/hqKcWECDO5  
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.
```

---

 注意：如果新PKCS12檔案包含身份證書，該身份證書具有與舊證書一起使用的相同金鑰對，則新信任點將引用舊金鑰對名稱。  
範例：

```
<#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. 驗證安裝的證書。

```
<#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
```

在上一個示例中，PKCS12包含身份證書和CA證書，因此，在匯入、證書和CA證書之後會顯示兩個條目。否則，僅存在證書條目。

#### 5. ( 可選 ) 驗證信任點。

如果PKCS12不包含CA證書，並且以PEM格式單獨獲取CA證書，則可以手動安裝該證書。

```
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  
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECzMdbGFjMRcwFQYDVQQDEw5j  
(...)  
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
```

## 6. 重新配置ASA以使用新信任點而不是舊信任點。

範例：

```
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
```



注意：信任點可以在不同的配置元素中使用。檢查使用舊信任點的配置。

---

## 相關資訊

如何在ASA上配置時間設定。

有關在ASA上正確設定時間和日期所需的步驟，請檢視Cisco ASA系列常規操作CLI配置指南9.18。  
<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>

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。