在ASDM管理的ASA上安裝並續訂證書

目錄

簡介

本文檔介紹如何在由ASDM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

- 開始之前，請確認自適應安全裝置(ASA)具有正確的時鐘時間、日期和時區。對於證書身份驗證，建議使用網路時間協定(NTP)伺服器來同步ASA上的時間。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，必須擁有對受信任內部或第三方憑證授權單位(CA)的存取許可權。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：

- ASAv 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

此文檔處理的證書型別為：

- 自簽名證書
- 由第三方證書頒發機構或內部CA簽名的證書

用於EAP身份驗證協定的安全套接字層(SSL)、傳輸層安全(TLS)和IKEv2 rfc7296要求SSL/TLS/IKEv2伺服器為客戶端提供伺服器證書，以便客戶端執行伺服器身份驗證。建議使用受信任的第三方 CA，以便向 ASA 核發 SSL 憑證做為此用途。

思科建議不要使用自我簽署憑證，因為使用者可能會不當設定瀏覽器信任惡意伺服器的憑證。 如此亦可能造成使用者不便，必須在連線至安全閘道時回應安全性警告。

使用ASDM請求並安裝新的身份證書

可以通過兩種方式從證書頒發機構(CA)請求證書並在ASA上安裝：

- 使用憑證簽署請求(CSR)。生成金鑰對，使用CSR從CA請求身份證書，安裝從CA獲取的簽名身份證書。
- 使用從CA獲取或從其他裝置匯出的PKCS12檔案。PKCS12檔案包含金鑰對、身份證書、

CA證書。

請求並安裝具有證書簽名請求(CSR)的新身份證書

在需要身份證書的裝置上建立CSR，使用在裝置上建立的金鑰對。

CSR包含：

- 證書請求資訊 — 請求的主題和其他屬性，金鑰對中的公鑰，
- 簽名演算法資訊，
- 證書請求資訊的數位簽章，使用金鑰對中的私鑰簽名。

CSR會傳遞至憑證授權單位(CA)，以便其在PKCS#10表單中簽署它。

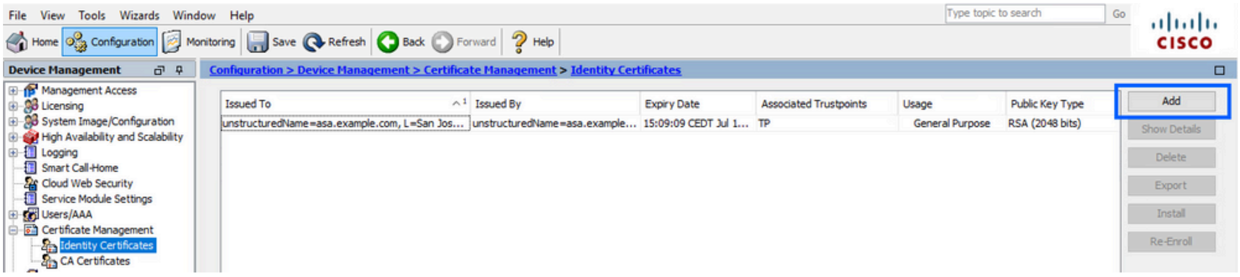
簽名的證書以PEM形式從CA返回。

> 注意：CA在簽署CSR並建立已簽名的身份證書時，可以更改信任點中定義的FQDN和使用者名稱引數。

使用ASDM產生CSR

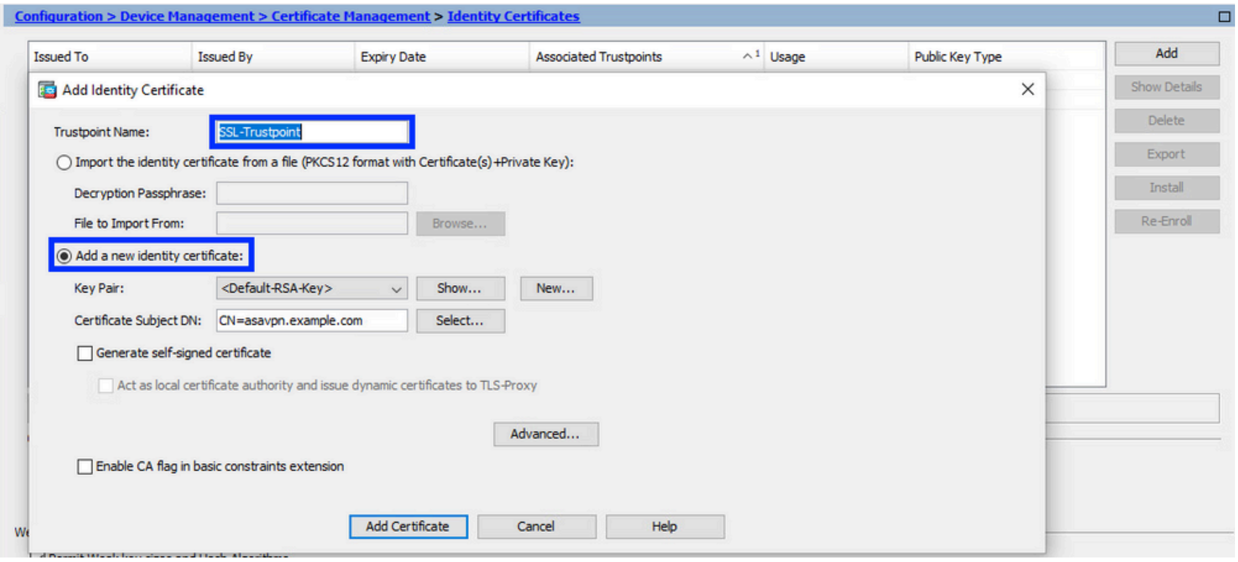
1. 建立具有特定名稱的信任點

    a. 導航到Configuration > Device Management > Certificate Management > Identity Certificates。



Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=asa.example.com, L=San Jos...	unstructuredName=asa.example...	15:09:09 CEDT Jul 1...	TP	General Purpose	RSA (2048 bits)

    b. 按一下「Add」。
    c. 定義信任點名稱。



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: <Default-RSA-Key>

Certificate Subject DN: CN=asavpn.example.com

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

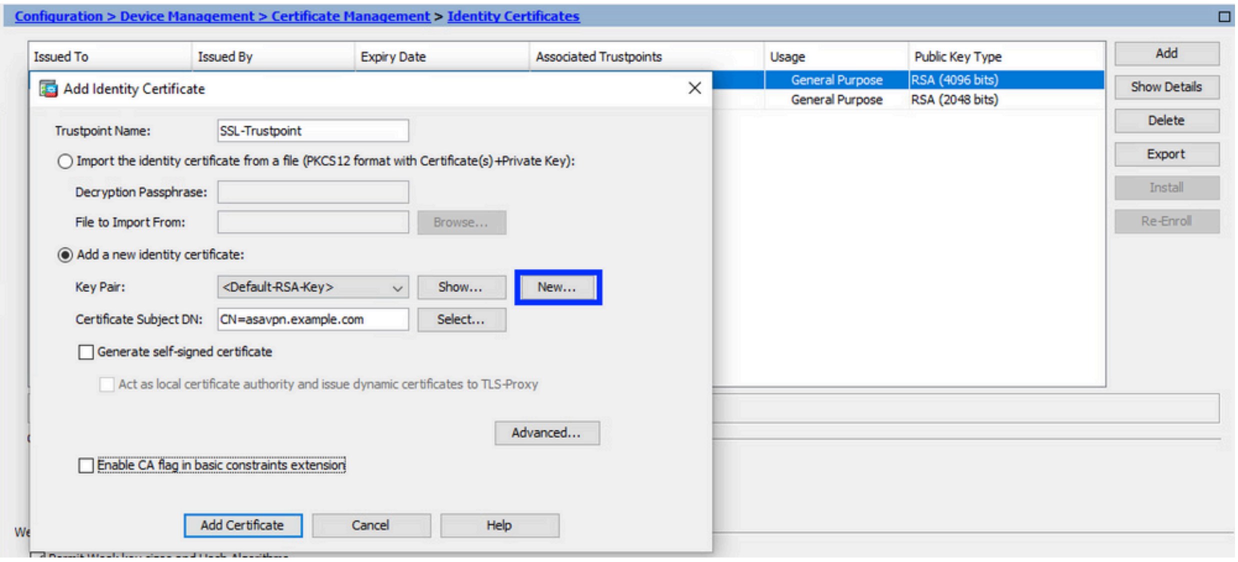
□ Enable CA flag in basic constraints extension

d. 按一下Add a New Identity Certificate單選按鈕。

2. （可選）建立新金鑰對

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，建議對每個身份證書使用唯一的私有/公共金鑰對。

a. 按一下New以生成新的金鑰對。



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
				General Purpose	RSA (4096 bits)
				General Purpose	RSA (2048 bits)

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: <Default-RSA-Key>

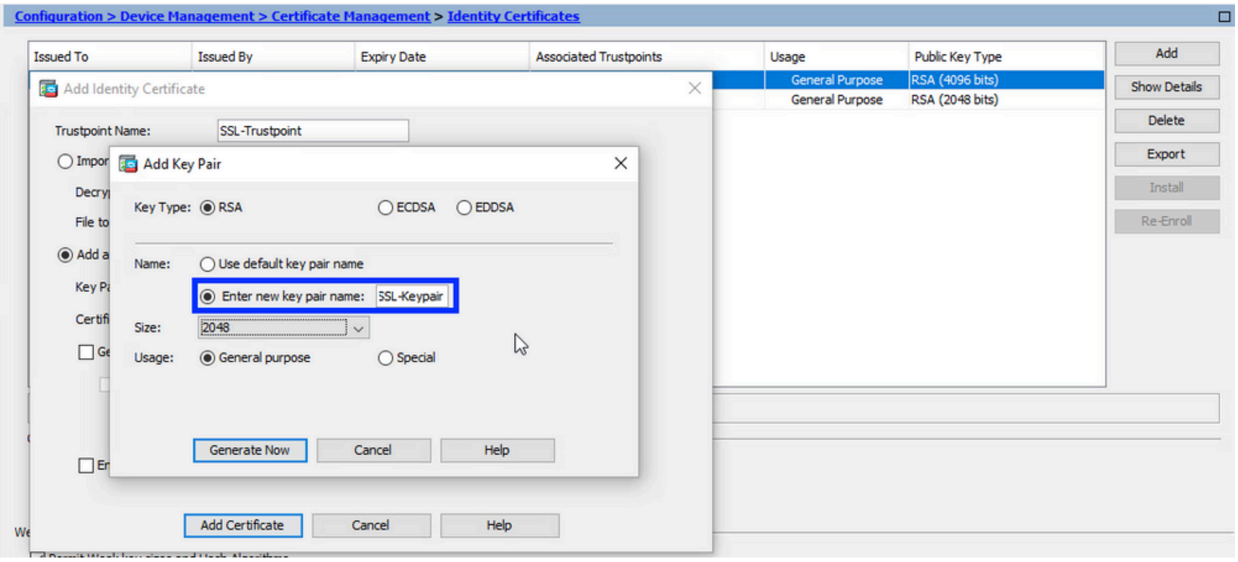
Certificate Subject DN: CN=asavpn.example.com

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

b. 選擇Enter new Key Pair name選項，然後輸入新金鑰對的名稱。
c. 選擇金鑰型別 - RSA或ECDSA。
d. 選擇Key Size；對於RSA，選擇General purpose for Usage。
e. 按一下「Generate Now」。金鑰對現已建立。



Configuration > Device Management > Certificate Management > Identity Certificates

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint

Add Key Pair

Key Type: ● RSA ○ ECDSA ○ EDDSA

Name: ○ Use default key pair name

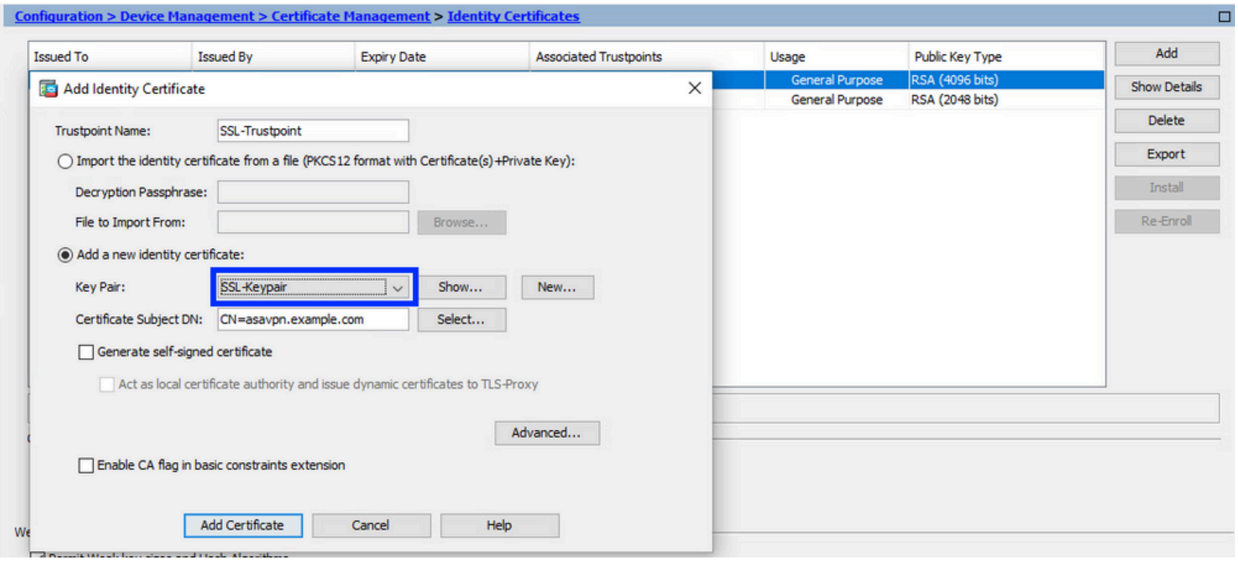
● Enter new key pair name: SSL-Keypair

Size: 2048

Usage: ● General purpose ○ Special

3. 選擇金鑰對名稱

選擇金鑰對以簽署CSR並將與新證書繫結。



Configuration > Device Management > Certificate Management > Identity Certificates

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: SSL-Keypair

Certificate Subject DN: CN=asavpn.example.com

□ Generate self-signed certificate

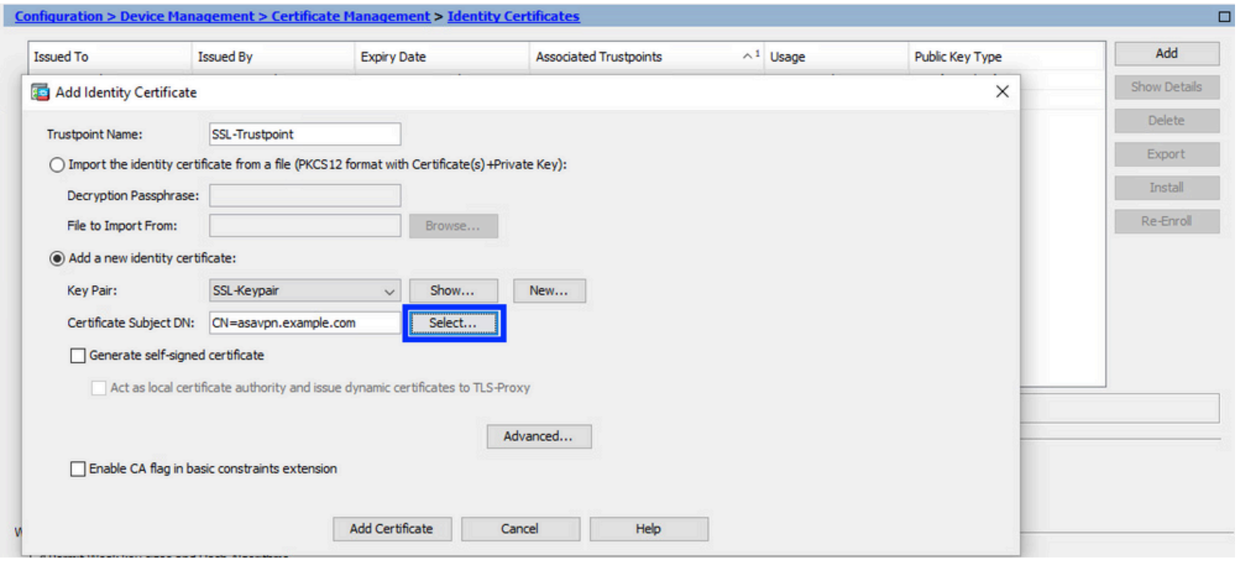
□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

4. 配置證書主題和完全限定域名(FQDN)

注意: FQDN引數必須與身份證書使用的ASA介面的FQDN或IP地址匹配。此引數為身份證書設定請求的主題備用名稱(SAN)擴展。SSL/TLS/IKEv2客戶端使用SAN擴展來驗證證書是否與其連線的FQDN匹配。

a. 按一下「Select」。



Configuration > Device Management > Certificate Management > Identity Certificates

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: SSL-Keypair

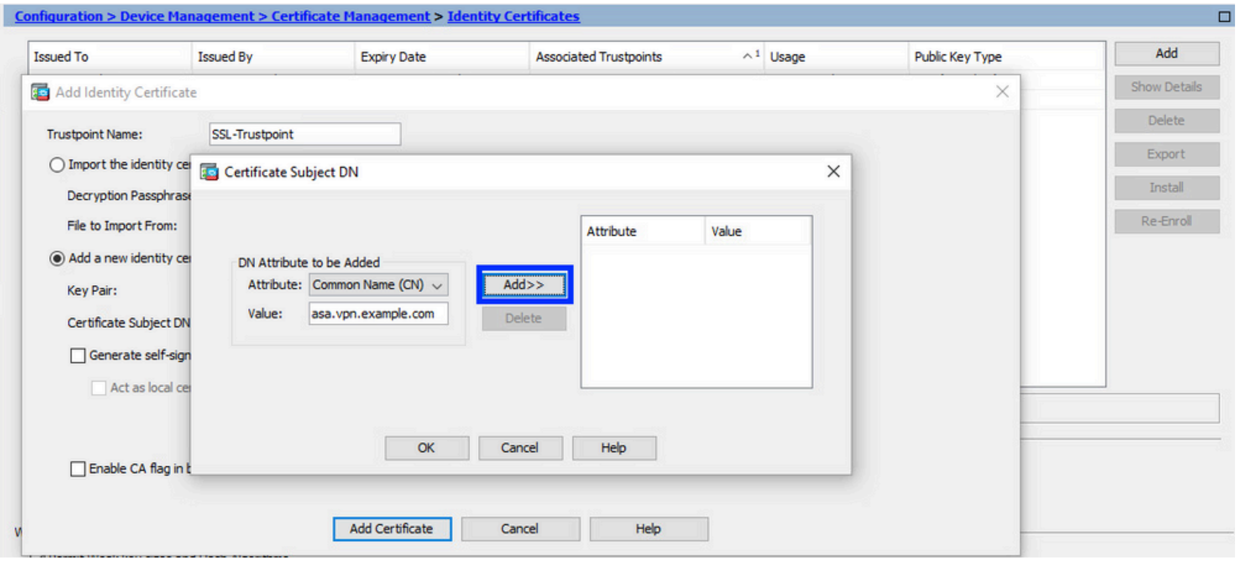
Certificate Subject DN: CN=asavpn.example.com

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

b. 在「Certificate Subject DN」視窗中，配置證書屬性 — 從下拉選單中選擇屬性，輸入值，然後點選Add。



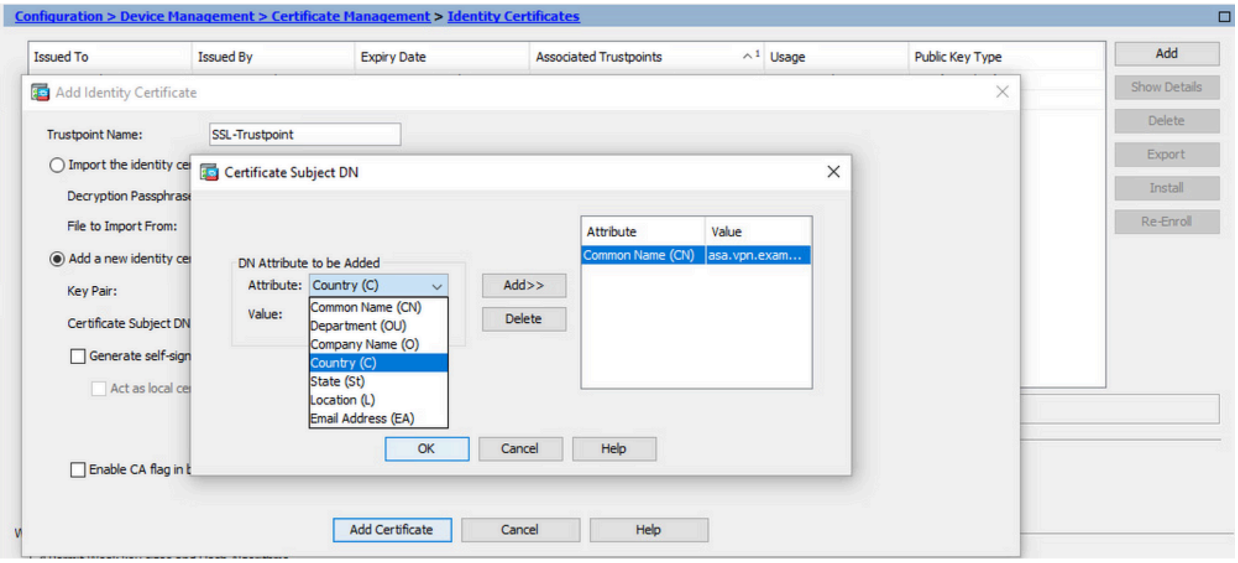
Certificate Subject DN

DN Attribute to be Added

Attribute: Common Name (CN)

Value: asa.vpn.example.com

Attribute	Value



Certificate Subject DN

DN Attribute to be Added

Attribute: Country (C)

Value:

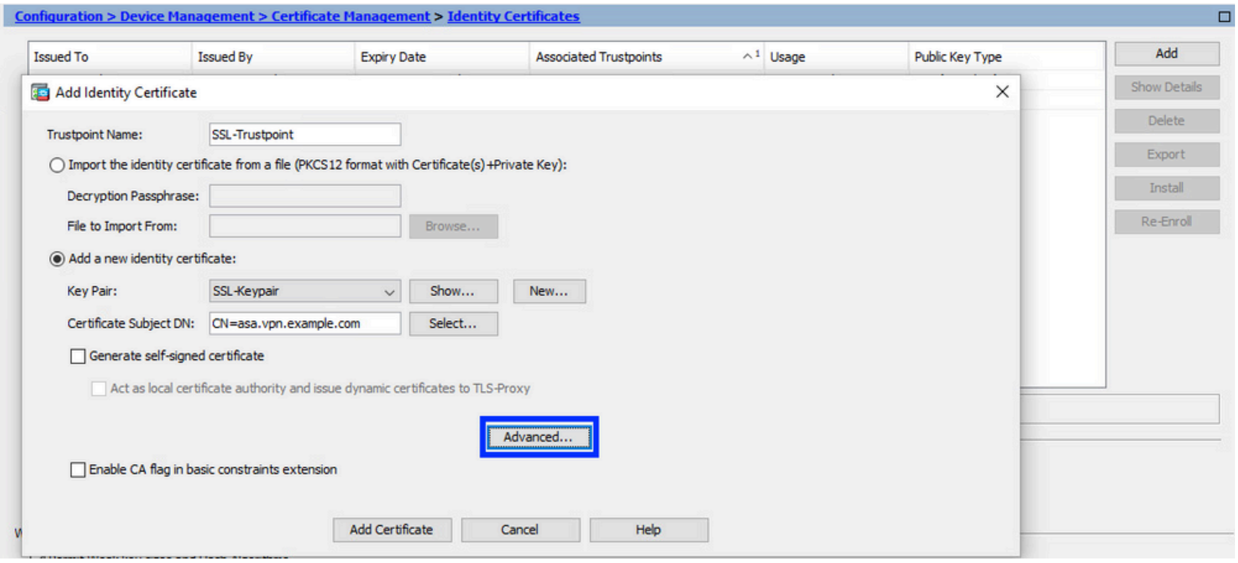
Attribute	Value
Common Name (CN)	asa.vpn.exam...

屬性	說明
CN	用於訪問防火牆的名稱(通常為完全限定域名，例如vpn.example.com)。
OU	組織內您所在部門的名稱
O	您的組織/公司的合法註冊名稱
思	國家/地區代碼（2個不帶標點的字母代碼）
ST	組織所在的狀態。
L	組織所在的城市。
EA	電子郵件地址

> 註：以上欄位值均不能超過64個字元的限制。值越長，可能會導致身份證書安裝問題。此外，不必定義所有DN屬性。

新增完所有屬性後，按一下OK。

c. 配置裝置FQDN — 按一下Advanced。



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: SSL-Keypair

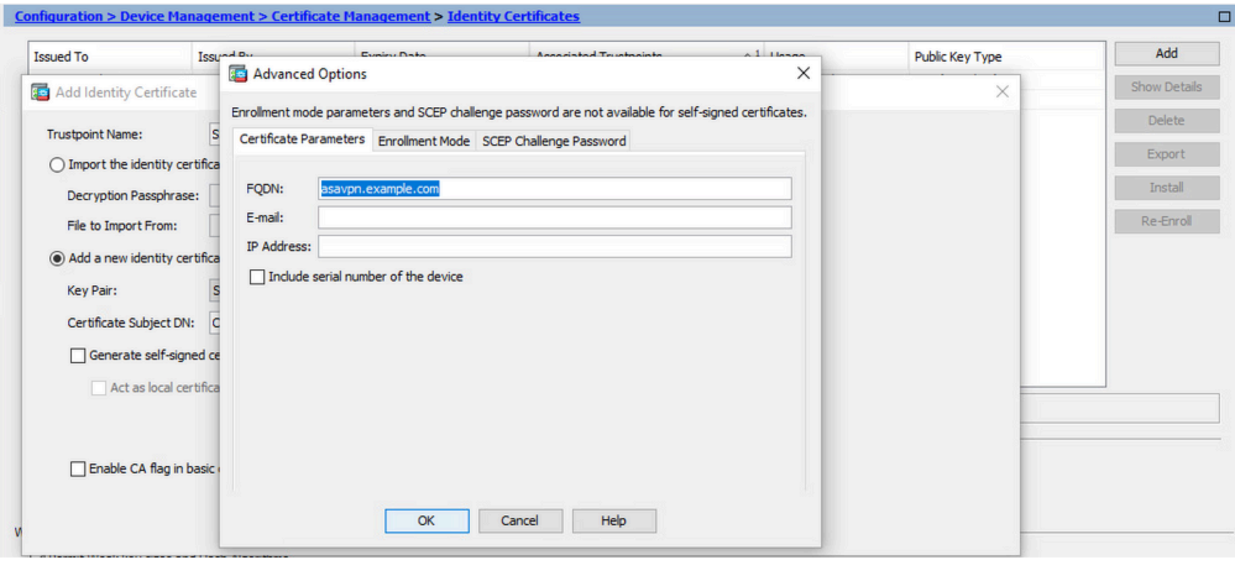
Certificate Subject DN: CN=asa.vpn.example.com

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

d. 在FQDN欄位中，輸入從Internet訪問裝置的完全限定域名。按一下「OK」（確定）。



Advanced Options

Enrollment mode parameters and SCEP challenge password are not available for self-signed certificates.

FQDN: asavpn.example.com

E-mail:

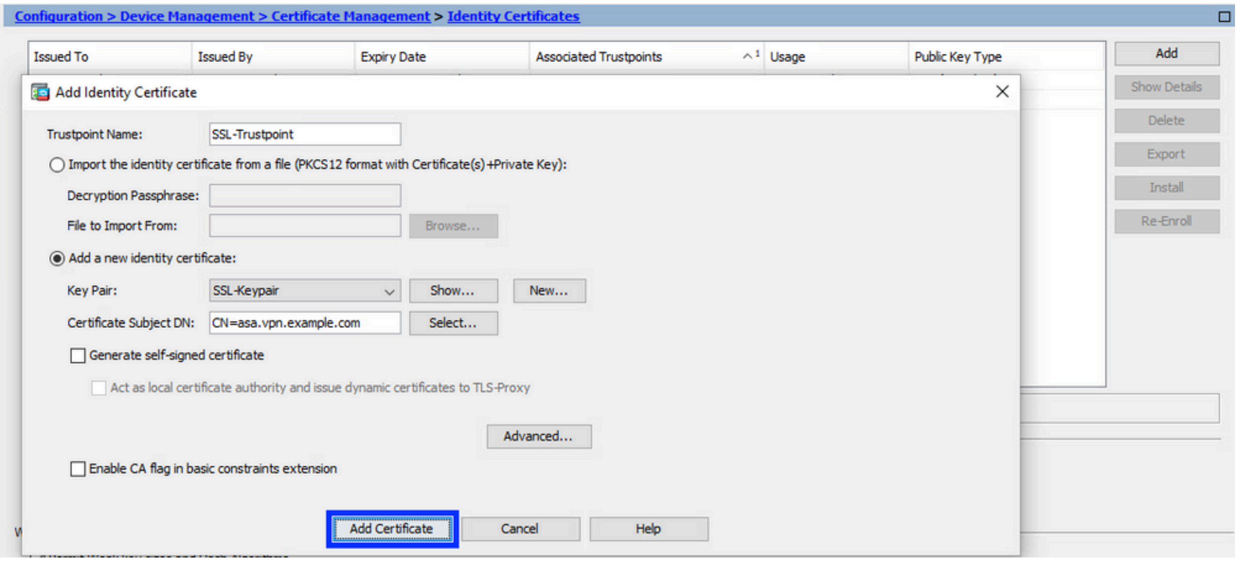
IP Address:

□ Include serial number of the device

Configuration > Device Management > Certificate Management > Identity Certificates
Certificate Parameters
Enrollment Mode
SCEP Challenge Password
OK
Cancel
Help

5. 產生並儲存CSR

a. 按一下「新增憑證」。



Configuration > Device Management > Certificate Management > Identity Certificates

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: SSL-Keypair

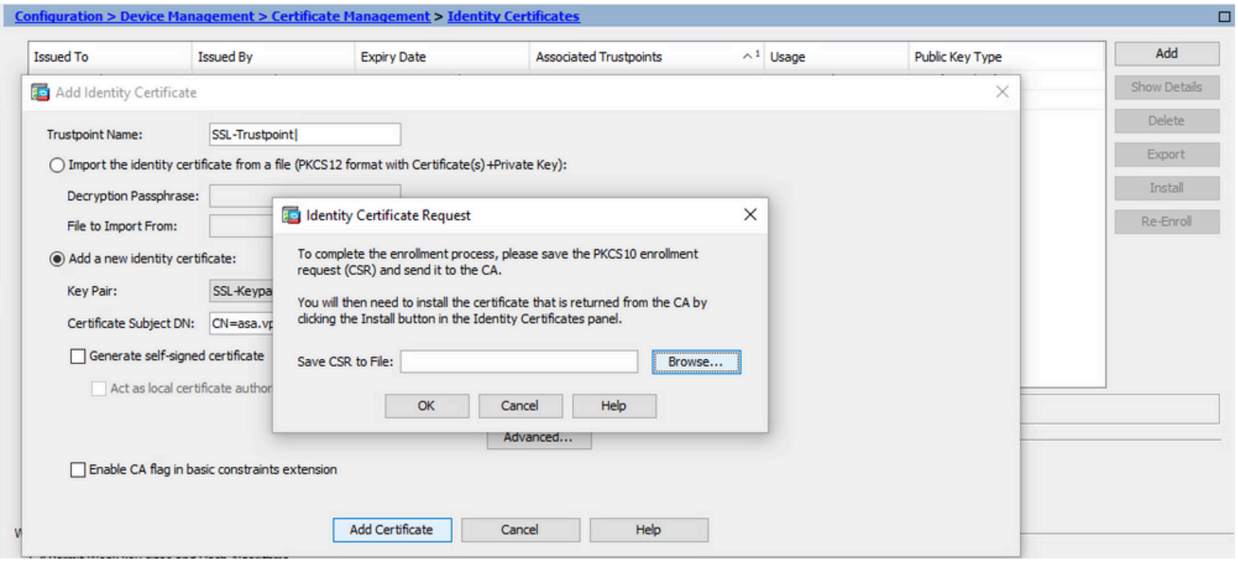
Certificate Subject DN: CN=asa.vpn.example.com

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

b. 提示隨即顯示，可將 CSR 儲存至本機電腦的檔案中。



Configuration > Device Management > Certificate Management > Identity Certificates

Identity Certificate Request

To complete the enrollment process, please save the PKCS10 enrollment request (CSR) and send it to the CA.

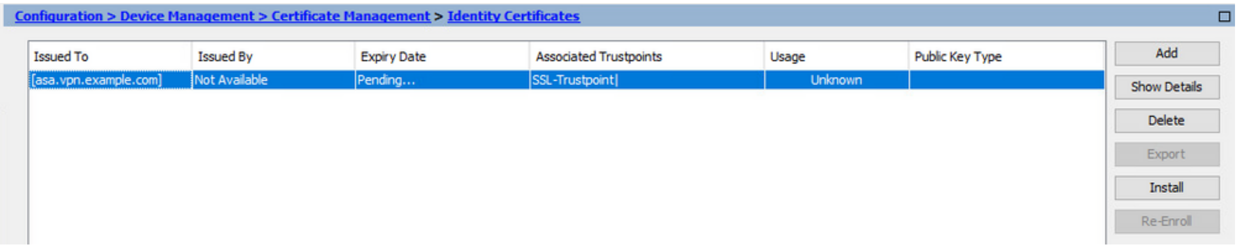
You will then need to install the certificate that is returned from the CA by clicking the Install button in the Identity Certificates panel.

Save CSR to File:

按一下「Browse」，選擇要儲存CSR的位置，並以.txt副檔名儲存檔案。

> 注意：當檔案以.txt副檔名儲存時，可以使用文本編輯器（如記事本）開啟和檢視PKCS#10請求。

c. 現在，新信任點顯示為Pending狀態。



Configuration > Device Management > Certificate Management > Identity Certificates

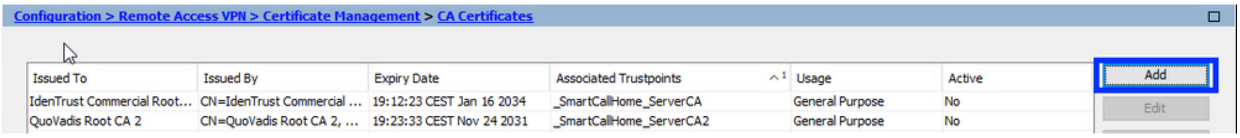
Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
[asa.vpn.example.com]	Not Available	Pending...	SSL-Trustpoint|	Unknown	

使用ASDM安裝PEM格式的身份證書

安裝步驟假設CA對CSR進行簽名，並提供PEM編碼的(.pem、.cer、.crt)身份證書和CA證書捆綁包。

1. 安裝簽署CSR的CA證書

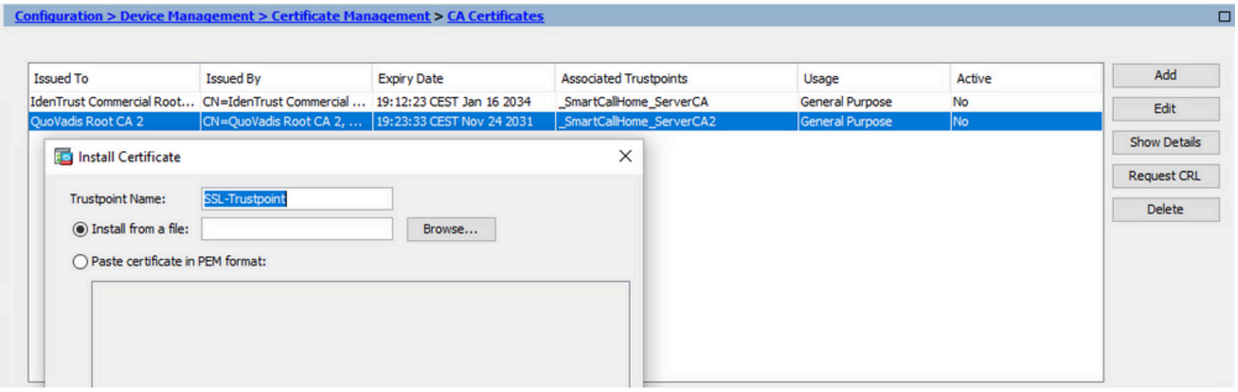
   a. 導覽至Configuration > Device Management > Certificate Management>，然後選擇CA Certificates。按一下「Add」。



Configuration > Remote Access VPN > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
IdenTrust Commercial Root...	CN=IdenTrust Commercial ...	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No
QuoVadis Root CA 2	CN=QuoVadis Root CA 2, ...	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No

   b. 輸入Trustpoint名稱並選擇Install From File，按一下Browse按鈕，然後選擇中間證書。或者，也可以將PEM編碼的CA證書從文本檔案貼上到文本欄位中。



Configuration > Device Management > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
IdenTrust Commercial Root...	CN=IdenTrust Commercial ...	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No
QuoVadis Root CA 2	CN=QuoVadis Root CA 2, ...	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No

Install Certificate

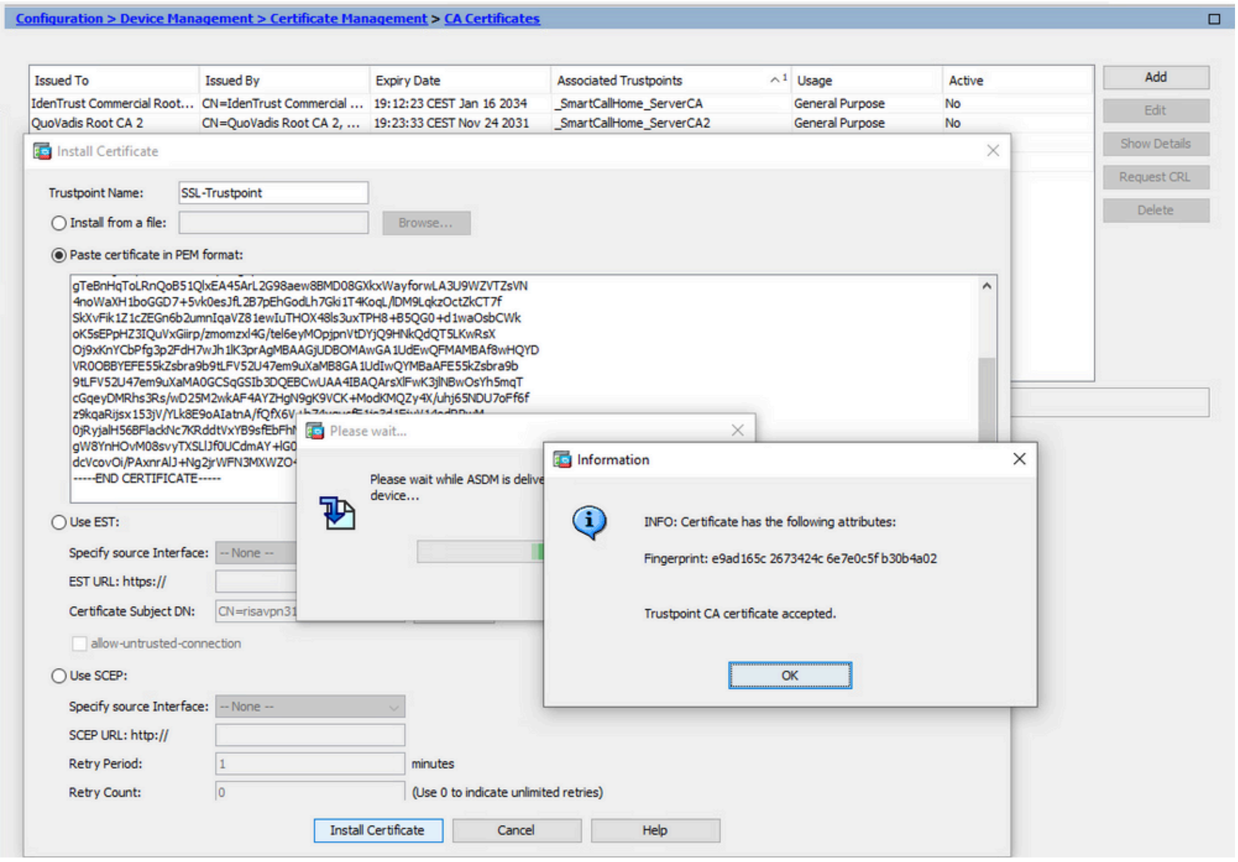
Trustpoint Name: SSL-Trustpoint

● Install from a file:

○ Paste certificate in PEM format:

注意：安裝簽署CSR的CA證書，並使用與身份證書相同的信任點名稱。PKI層次結構中較高的其他CA證書可以安裝在單獨的信任點中。

   c. 按一下「Install Certificate」。



Configuration > Device Management > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
IdenTrust Commercial Root...	CN=IdenTrust Commercial ...	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No
QuoVadis Root CA 2	CN=QuoVadis Root CA 2, ...	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No

Install Certificate

Trustpoint Name: SSL-Trustpoint

○ Install from a file: Browse...

● Paste certificate in PEM format:

```
gTeBnHqToLRnQoB51QlxEA45ArL2G98aew8BMD08GXkxWayforwLA3U9WZVTZsVN
4noWaXH1boGGD7+5vk0esJfL2B7pEhGodLh7Gki1T4KoqL/lDM9LqkzOctZkCT7f
SkXvFik1Z1cZEGn6b2umnIqaVZ81ewIuTHOX48ls3uxTPH8+B5QG0+d1waOsbCWk
oK5sEPpHZ3IQuVxGiirp/zmomzxl4G/tel6eyMOpjpnVtDYjQ9HNkQdQT5LKwRsX
Oj9xKnYCbPfg3p2FdH7wJh1lK3prAgMBAAGjUDBOMAwGA1UdEwQFMAMBAf8wHQYD
VR0OBBYEFE55kZsbra9b9tLFV52U47em9uXaMB8GA1UdIwQYMBaAFE55kZsbra9b
9tLFV52U47em9uXaMA0GCSqGSIb3DQEBCwUAA4IBAQArsXlFwK3jlNBwOsYh5mqT
cGqeyDMRhs3Rs/wD25M2wkAF4AYZHgN9gK9VCK+ModKMQZy4X/uhj65NDU7oFf6f
z9kqaRijsx153jV/YLk8E9oAIatnA/fQfX6V
0jRyjalH56BFlackNc7KRddtVxYB9sfEbFhN
gW8YnHOvM08svyTXSLlJf0UCdmAY+lG0
dcVcovOi/PAxnrAlJ+Ng2jrWFN3MXWZO
-----END CERTIFICATE-----
```

○ Use EST:

Specify source Interface: -- None --

EST URL: https://

Certificate Subject DN: CN=risavpn31

☐ allow-untrusted-connection

○ Use SCEP:

Specify source Interface: -- None --

SCEP URL: http://

Retry Period: 1 minutes

Retry Count: 0 (Use 0 to indicate unlimited retries)

Please wait...

Please wait while ASDM is delive
device...

Information

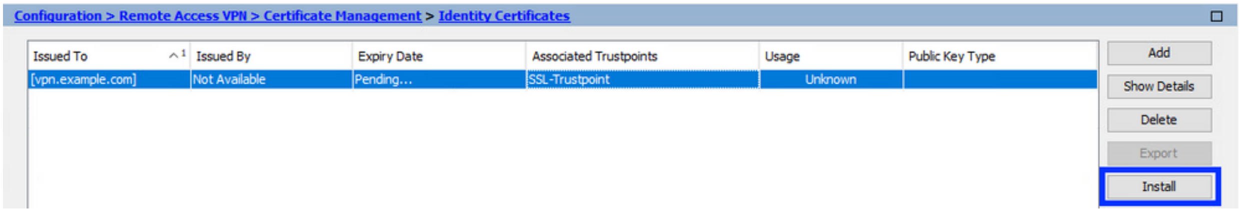
INFO: Certificate has the following attributes:

Fingerprint: e9ad165c 2673424c 6e7e0c5f b30b4a02

Trustpoint CA certificate accepted.

2. 安裝身份證書

a. 選擇之前在CSR生成期間建立的身份證書。按一下「Install」。

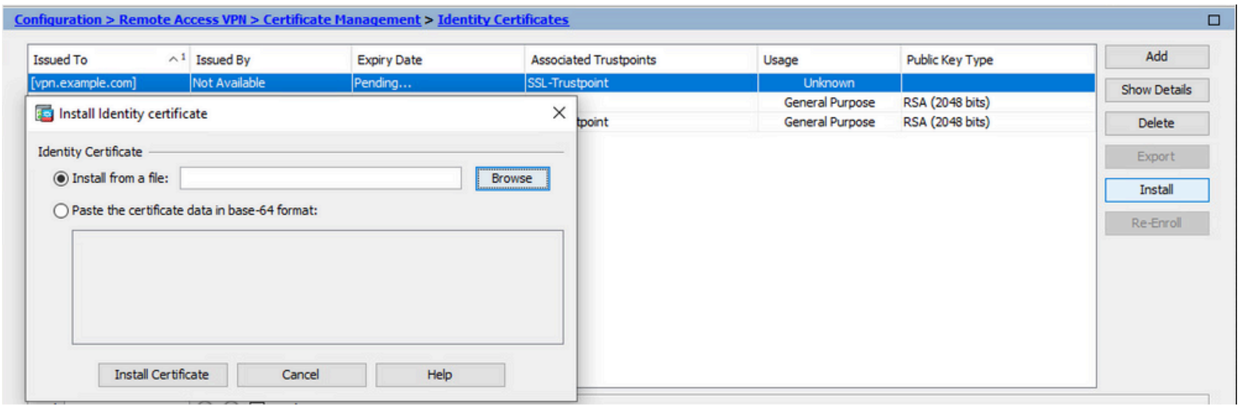


Configuration > Remote Access VPN > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
[vpn.example.com]	Not Available	Pending...	SSL-Trustpoint	Unknown	

注意：身份證書的Issued By欄位可用，Expiry Date欄位可用Pending。

b. 選擇包含從CA接收的PEM編碼身份證書的檔案，或在文本編輯器中開啟PEM編碼證書，然後將CA提供的身份證書複製並貼上到文本欄位中。



Configuration > Remote Access VPN > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
[vpn.example.com]	Not Available	Pending...	SSL-Trustpoint	Unknown	
				General Purpose	RSA (2048 bits)
			tpoint	General Purpose	RSA (2048 bits)

Install Identity certificate

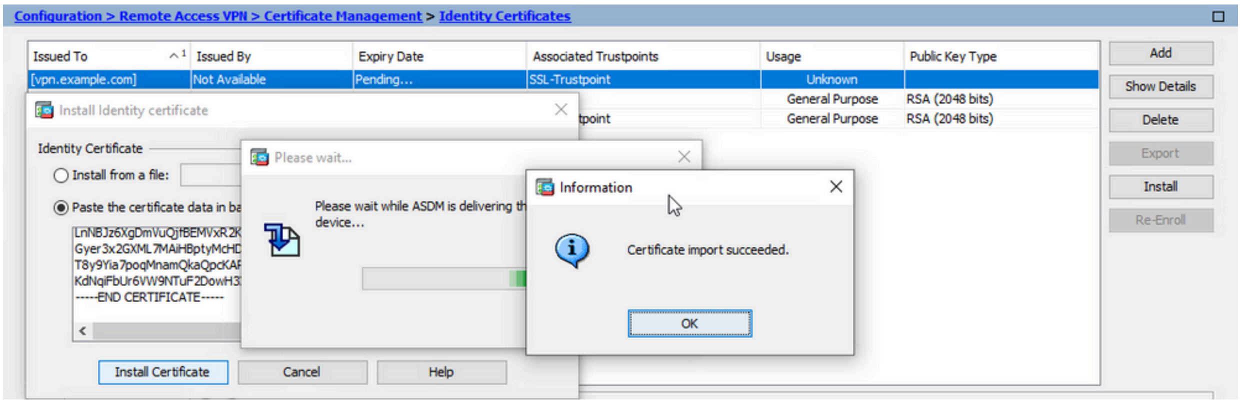
Identity Certificate

● Install from a file: Browse

○ Paste the certificate data in base-64 format:

> 註：身份證書可以採用.pem、.cer、.crt格式進行安裝。

c. 按一下「Install Certificate」。



Configuration > Remote Access VPN > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
[vpn.example.com]	Not Available	Pending...	SSL-Trustpoint	Unknown	
				General Purpose	RSA (2048 bits)
			tpoint	General Purpose	RSA (2048 bits)

Install Identity certificate

Identity Certificate

○ Install from a file:

● Paste the certificate data in ba

```
LnNBJz6XgDmVuQjfBEMVxR2K
Gyer3x2GXML7MAiHBptyMcHD
T8y9Yia7poqMnamQkaQpcKAF
KdNqiFbUr6VW9NTuF2DowH3
-----END CERTIFICATE-----
```

Please wait...

Please wait while ASDM is delivering th device...

Information

Certificate import succeeded.

3. 將新證書繫結到與ASDM的介面

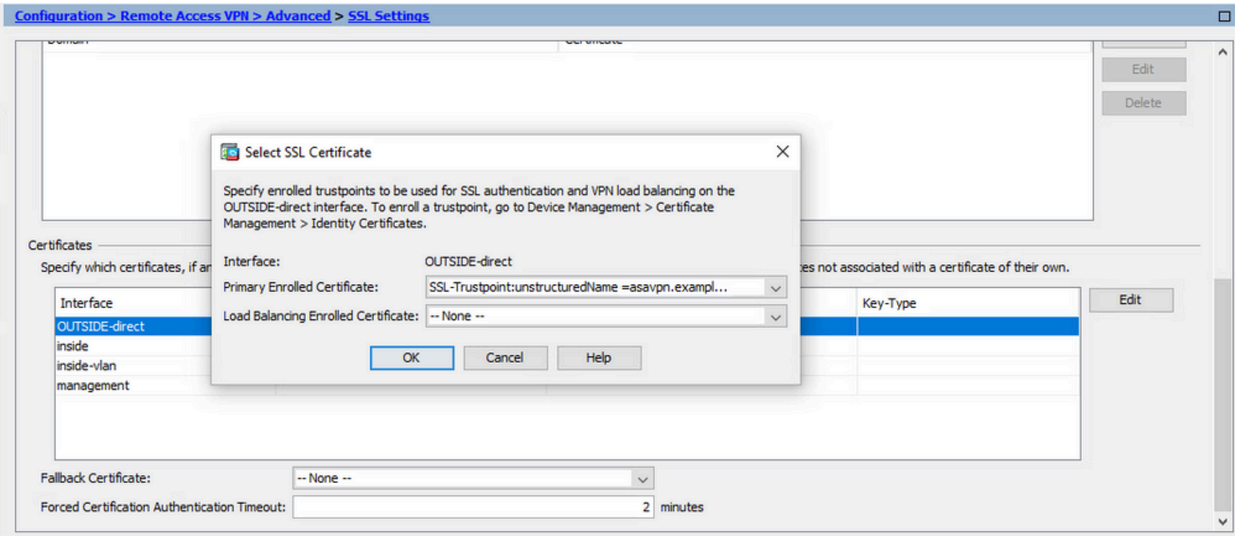
需要將ASA配置為使用新的身份證書，以便在指定介面上終止的WebVPN會話使用。

a. 導覽至「組態 >「遠端存取 VPN」>「進階」>「SSL 設定」。

b. 在「憑證」下方，選擇用於終止 WebVPN 作業階段的介面。在此範例中，所使用的是外部介面。

按一下「Edit」。

c. 在「憑證」下拉式清單中，選擇新安裝的憑證。



Configuration > Remote Access VPN > Advanced > SSL Settings

Select SSL Certificate

Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the OUTSIDE-direct interface. To enroll a trustpoint, go to Device Management > Certificate Management > Identity Certificates.

Interface: OUTSIDE-direct

Primary Enrolled Certificate: SSL-Trustpoint:unstructuredName =asavpn.exampl...

Load Balancing Enrolled Certificate: -- None --

Certificates

Specify which certificates, if ar ... es not associated with a certificate of their own.

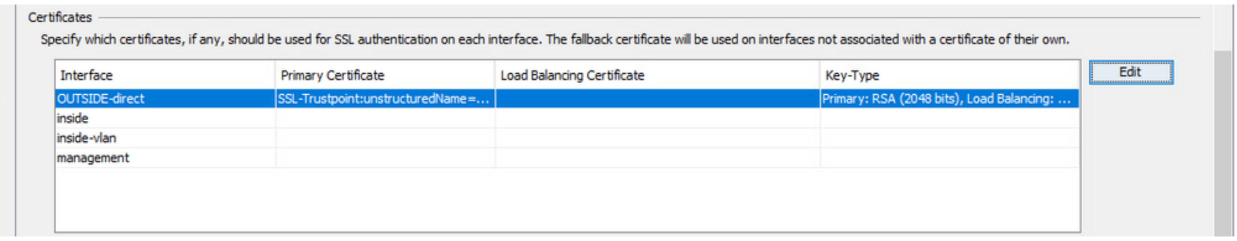
Interface	Key-Type
OUTSIDE-direct	
inside	
inside-vlan	
management	

Fallback Certificate: -- None --

Forced Certification Authentication Timeout: 2 minutes

d. 按一下「OK」（確定）。

e. 按一下「Apply」。



Certificates

Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.

Interface	Primary Certificate	Load Balancing Certificate	Key-Type
OUTSIDE-direct	SSL-Trustpoint:unstructuredName=...		Primary: RSA (2048 bits), Load Balancing: ...
inside			
inside-vlan			
management			

現在，新的身份證書正在使用。

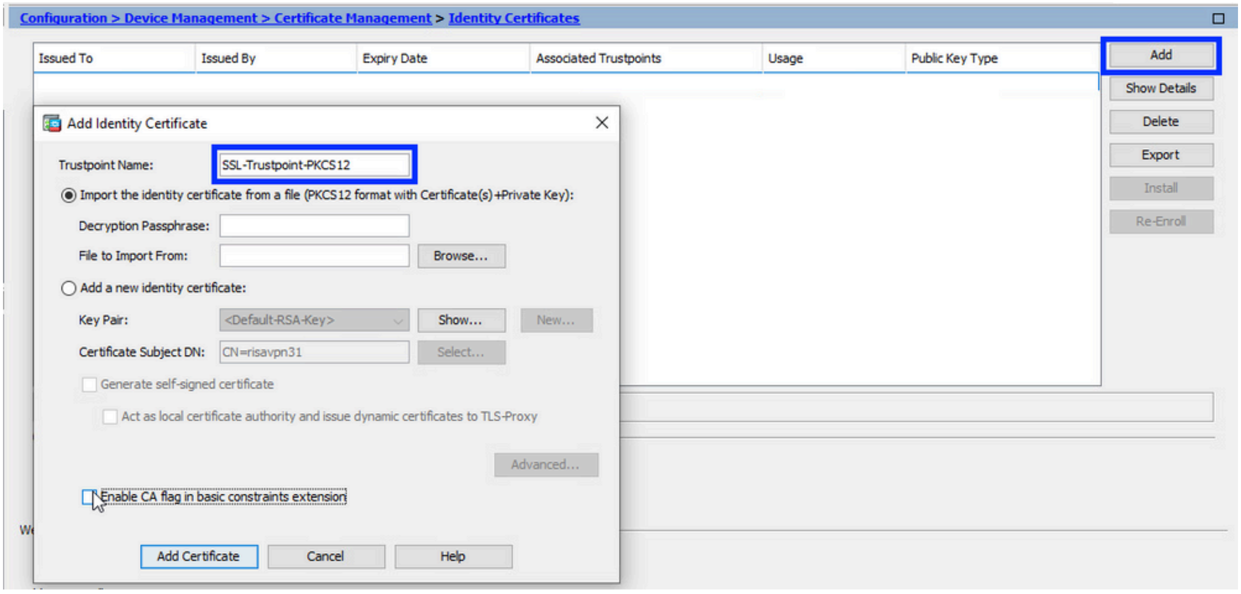
使用ASDM安裝以PKCS12格式接收的身份證書

PKCS12檔案（.p12或.pfx格式）包含身份證書、金鑰對和CA證書。它由CA建立（例如使用萬用字元憑證），或從不同的裝置匯出。它是二進位制檔案，無法使用文本編輯器檢視。

1. 從PKCS12檔案安裝身份證書和CA證書

身份證書、CA證書和金鑰對需要捆綁到單個PKCS12檔案中。

a. 導航到Configuration > Device Management > Certificate Management，然後選擇 Identity Certificates。
b. 按一下「Add」。
c. 指定信任點名稱。



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-PKCS12

● Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

○ Add a new identity certificate:

Key Pair: <Default-RSA-Key>

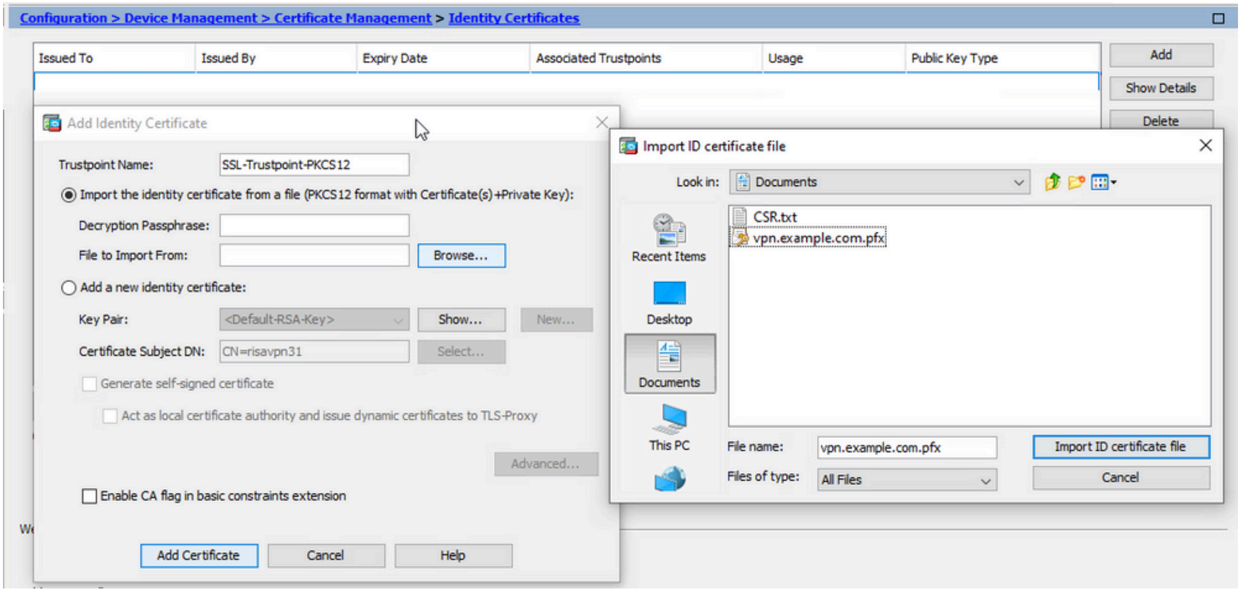
Certificate Subject DN: CN=risavpn31

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

d. 按一下「從檔案匯入身分識別憑證」單選按鈕。



Configuration > Device Management > Certificate Management > Identity Certificates

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-PKCS12

● Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

○ Add a new identity certificate:

Key Pair: <Default-RSA-Key>

Certificate Subject DN: CN=risavpn31

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

Import ID certificate file

Look in: Documents

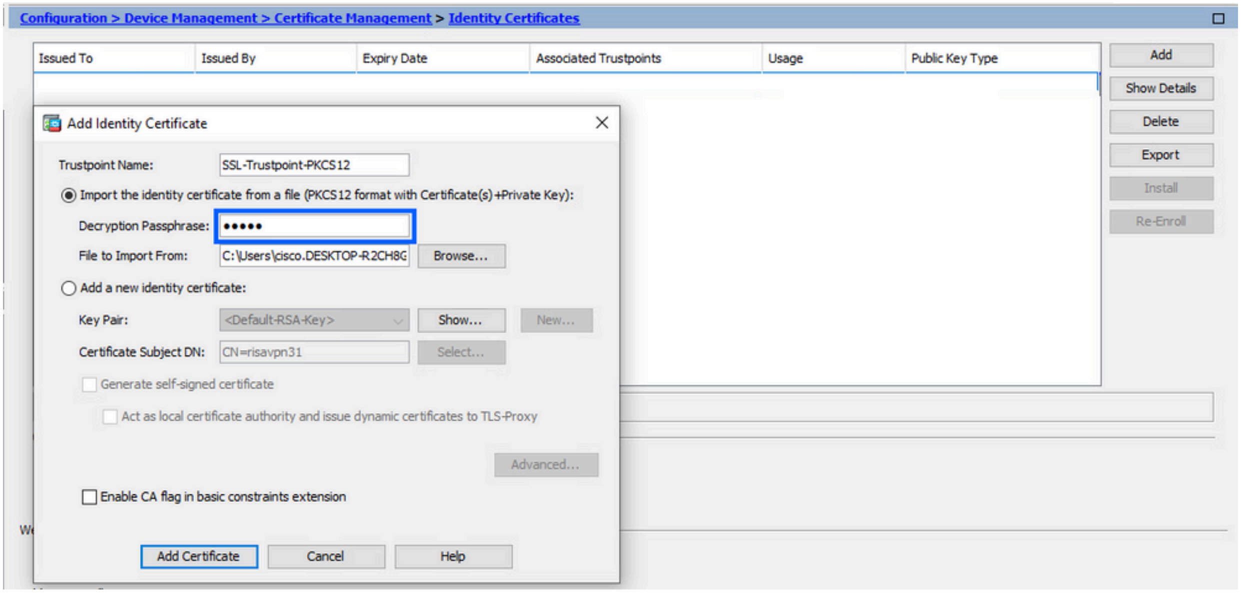
CSR.txt

vpn.example.com.pfx

File name: vpn.example.com.pfx

Files of type: All Files

e. 輸入用於建立 PKCS12 檔案的複雜密碼。



Configuration > Device Management > Certificate Management > Identity Certificates

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-PKCS12

● Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase: •••••

File to Import From: C:\Users\cisco.DESKTOP-R2CH8G

○ Add a new identity certificate:

Key Pair: <Default-RSA-Key>

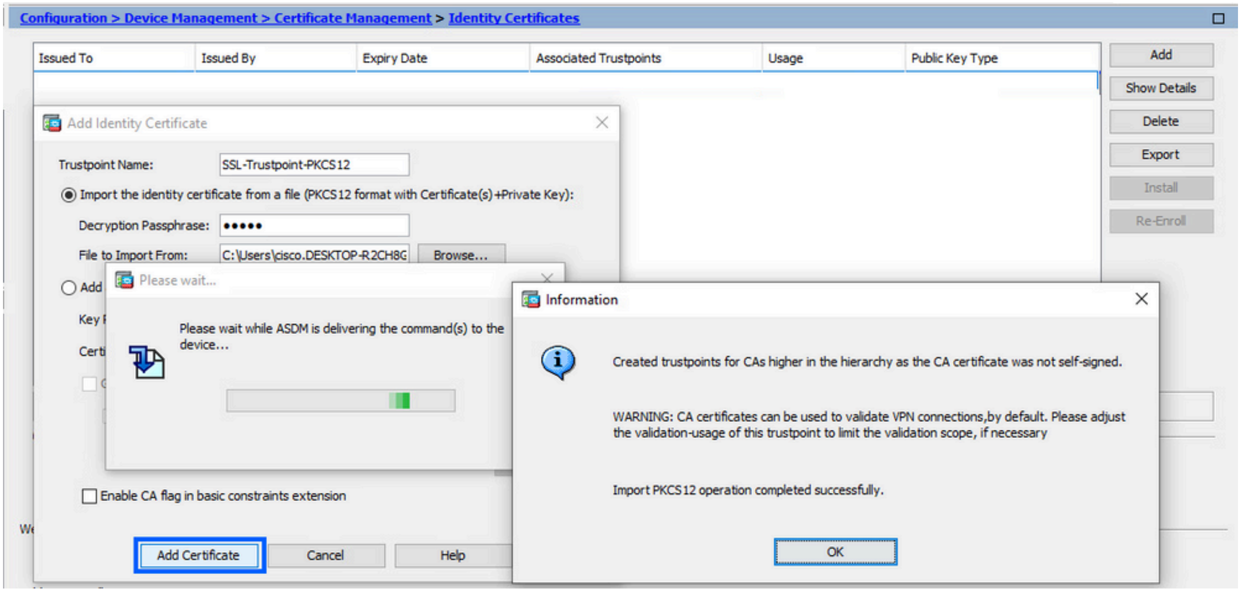
Certificate Subject DN: CN=risavpn31

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

f. 按一下「新增憑證」。



Trustpoint Name: SSL-Trustpoint-PKCS12

● Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase: •••••

File to Import From: C:\Users\cisco.DESKTOP-R2CH8G

○ Add

□ Enable CA flag in basic constraints extension

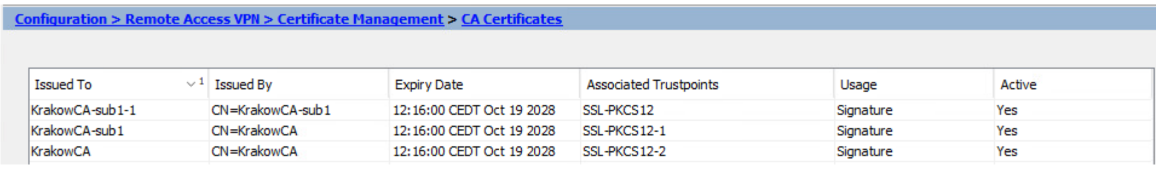
Please wait while ASDM is delivering the command(s) to the device...

Created trustpoints for CAs higher in the hierarchy as the CA certificate was not self-signed.

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

Import PKCS12 operation completed successfully.

注意：匯入帶有CA證書鏈的PKCS12時，ASDM會自動建立帶有新增了 — number字尾的名稱的上游CA信任點。


Configuration > Remote Access VPN > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
KrakowCA-sub1-1	CN=KrakowCA-sub1	12:16:00 CEDT Oct 19 2028	SSL-PKCS12	Signature	Yes
KrakowCA-sub1	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-1	Signature	Yes
KrakowCA	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-2	Signature	Yes

2. 將新證書繫結到與ASDM的介面

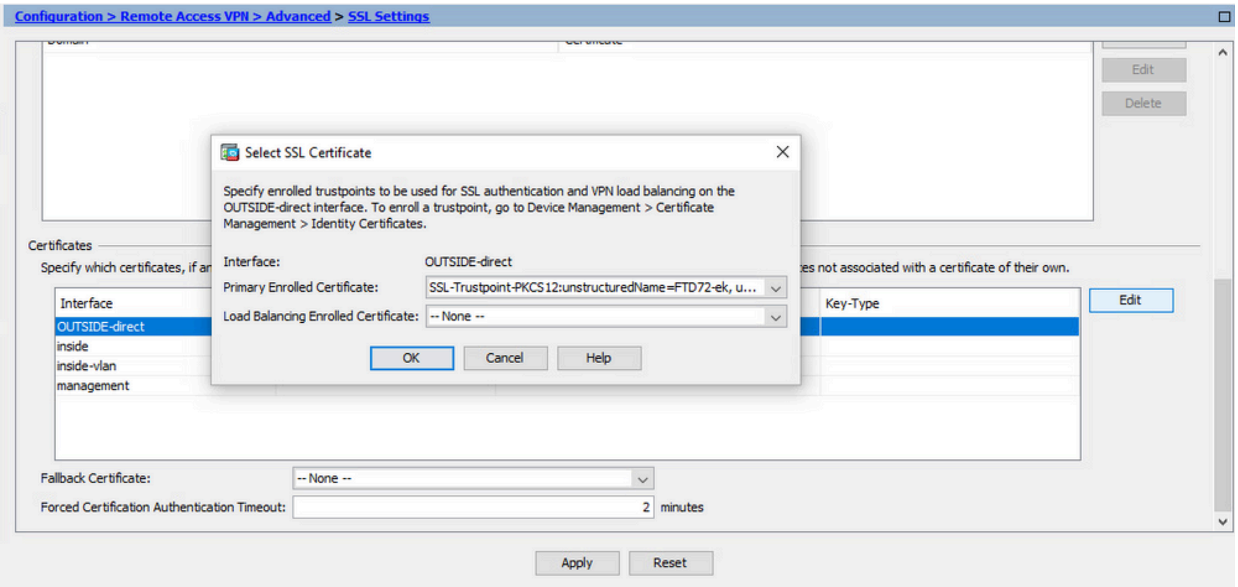
需要將ASA配置為使用新的身份證書，以便在指定介面上終止的WebVPN會話使用。

a. 導覽至「組態 >「遠端存取 VPN」>「進階」>「SSL 設定」。

b. 在「憑證」下方，選取用於終止 WebVPN 作業階段的介面。在此範例中，所使用的是外部介面。

按一下「Edit」。

c. 在「憑證」下拉式清單中，選擇新安裝的憑證。



Configuration > Remote Access VPN > Advanced > SSL Settings

Select SSL Certificate

Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the OUTSIDE-direct interface. To enroll a trustpoint, go to Device Management > Certificate Management > Identity Certificates.

Interface: OUTSIDE-direct

Primary Enrolled Certificate: SSL-Trustpoint-PKCS12:unstructuredName=FTD72-ek, u...

Load Balancing Enrolled Certificate: -- None --

Certificates

Specify which certificates, if an... ...es not associated with a certificate of their own.

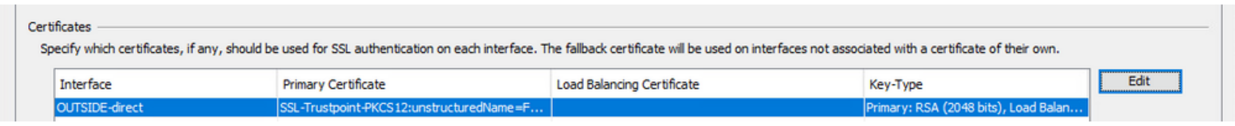
Interface	Key-Type
OUTSIDE-direct	
inside	
inside-vlan	
management	

Fallback Certificate: -- None --

Forced Certification Authentication Timeout: 2 minutes

d. 按一下「OK」（確定）。

e. 按一下「Apply」。



Certificates

Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.

Interface	Primary Certificate	Load Balancing Certificate	Key-Type
OUTSIDE-direct	SSL-Trustpoint-PKCS12:unstructuredName=F...		Primary: RSA (2048 bits), Load Balan...

現在，新的身份證書正在使用。

證書續訂

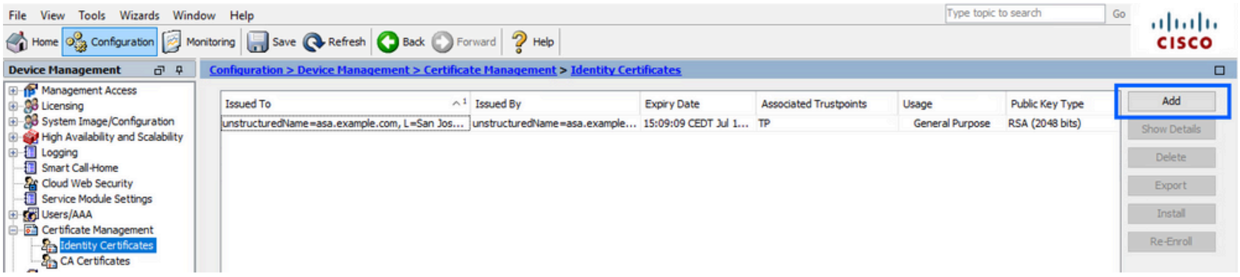
續訂使用ASDM的證書簽名請求(CSR)註冊的證書

CSR註冊證書的證書續訂需要建立和註冊新的信任點。它需要具有不同的名稱（例如，具有登記年度字尾的舊名稱）。它可以使用與舊證書相同的引數和金鑰對，也可以使用不同的引數和金鑰對。

使用ASDM產生CSR

1. 建立具有特定名稱的新信任點。

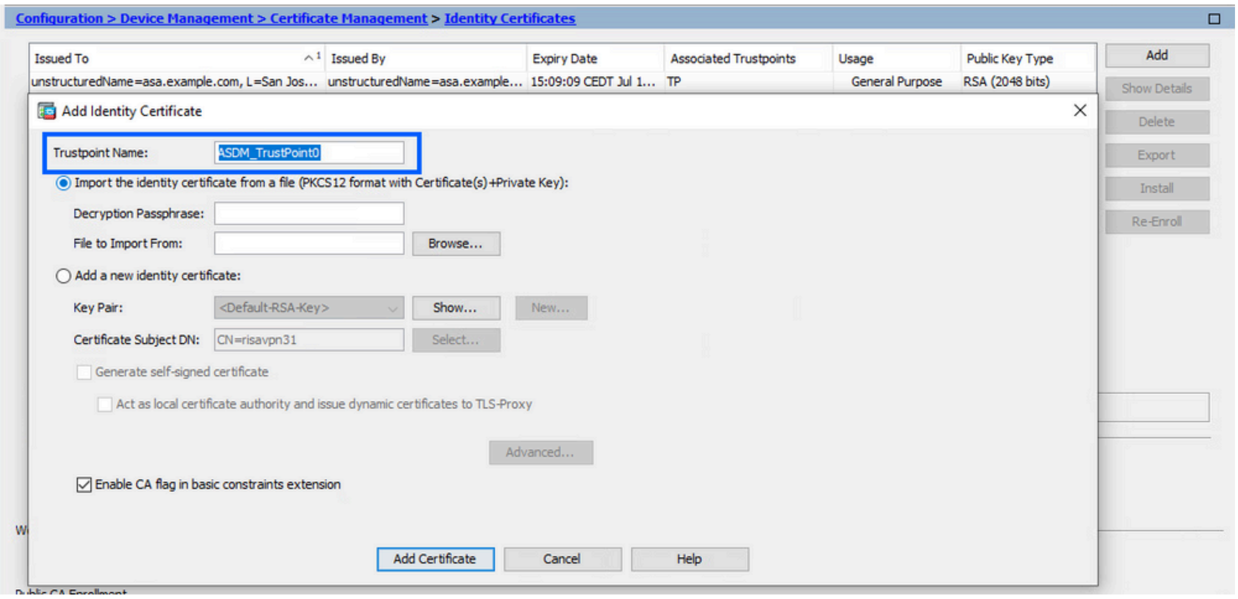
a. 導航到Configuration > Device Management > Certificate Management > Identity Certificates。



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=asa.example.com, L=San Jos...	unstructuredName=asa.example...	15:09:09 CEDT Jul 1...	TP	General Purpose	RSA (2048 bits)

b. 按一下「Add」。
c. 定義信任點名稱。



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=asa.example.com, L=San Jos...	unstructuredName=asa.example...	15:09:09 CEDT Jul 1...	TP	General Purpose	RSA (2048 bits)

Add Identity Certificate

Trustpoint Name: ASDM_TrustPoint0

● Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

○ Add a new identity certificate:

Key Pair: <Default-RSA-Key>

Certificate Subject DN: CN=risavpn31

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

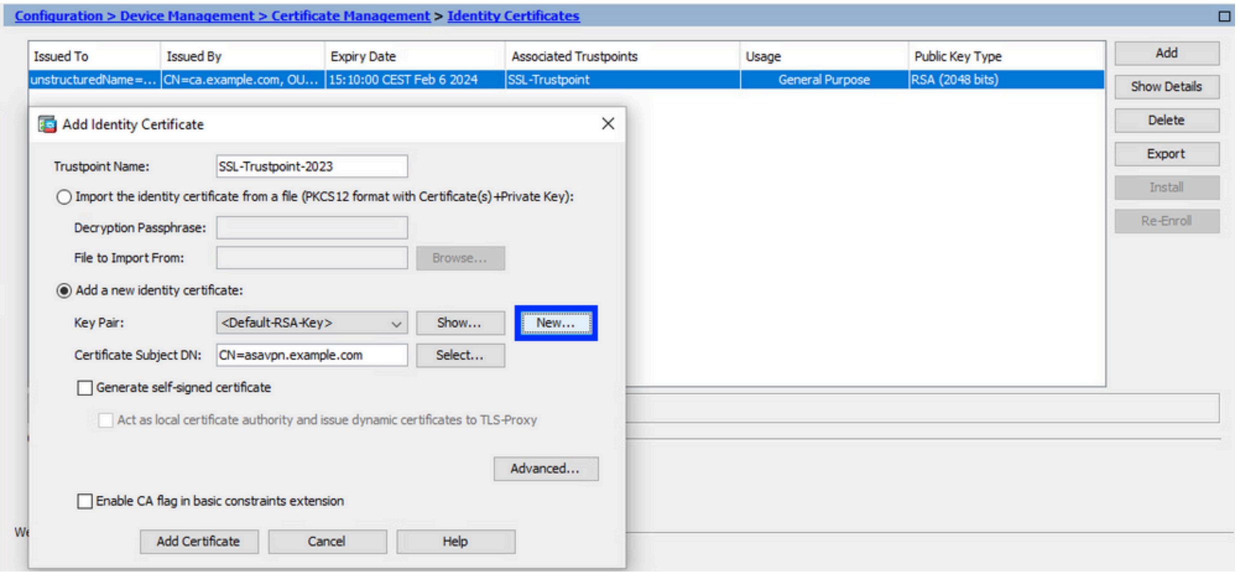
☑ Enable CA flag in basic constraints extension

d. 按一下Add a New Identity Certificate單選按鈕。

2. （可選）建立新金鑰對

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，建議對每個身份證書使用唯一的私有/公共金鑰對。

a. 按一下New以生成新的金鑰對。



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-2023

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: <Default-RSA-Key>

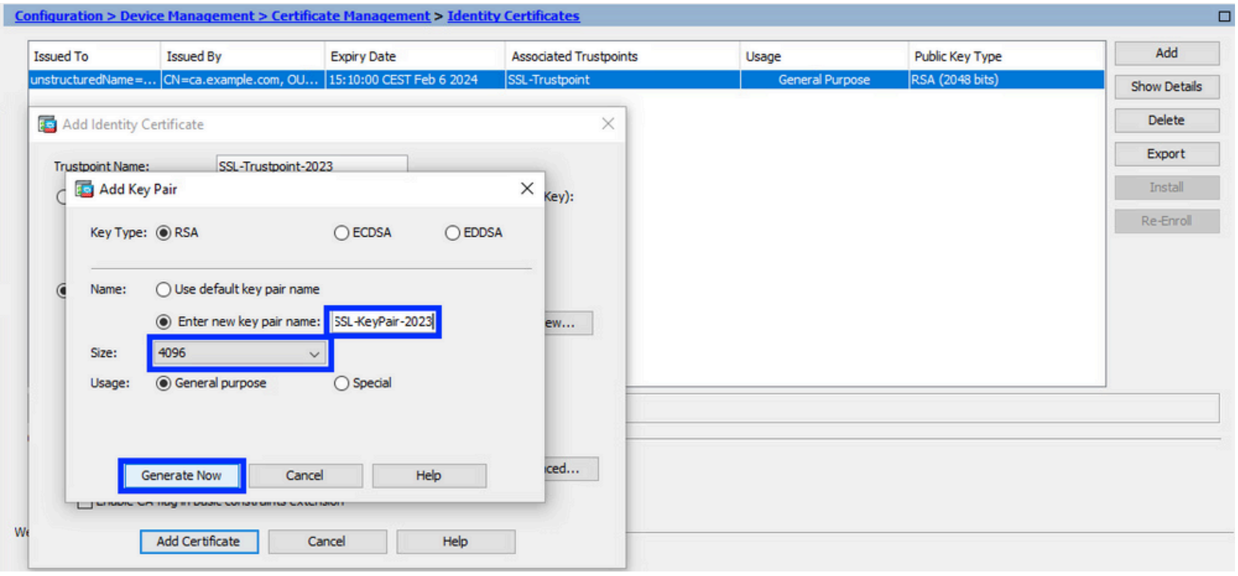
Certificate Subject DN: CN=asavpn.example.com

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

b. 選擇選項Enter new Key Pair name（輸入新金鑰對名稱），然後輸入新金鑰對的名稱。
c. 選擇Key Type - RSA或ECDSA。
d. 選擇Key Size；對於RSA，選擇General purpose for Usage。
e. 按一下「Generate Now」。金鑰對現已建立。



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-2023

Add Key Pair

Key Type: ● RSA ○ ECDSA ○ EDDSA

Name: ○ Use default key pair name

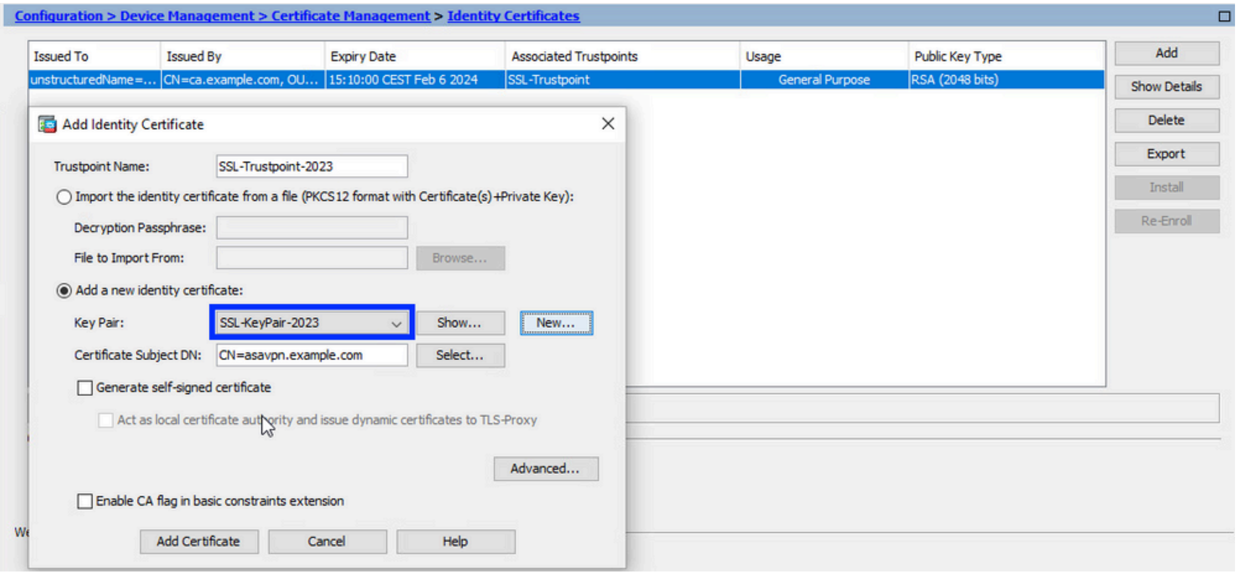
● Enter new key pair name: SSL-KeyPair-2023

Size: 4096

Usage: ● General purpose ○ Special

3. 選擇金鑰對名稱

選擇金鑰對以簽署CSR並將與新證書繫結。



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-2023

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: SSL-KeyPair-2023

Certificate Subject DN: CN=asavpn.example.com

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

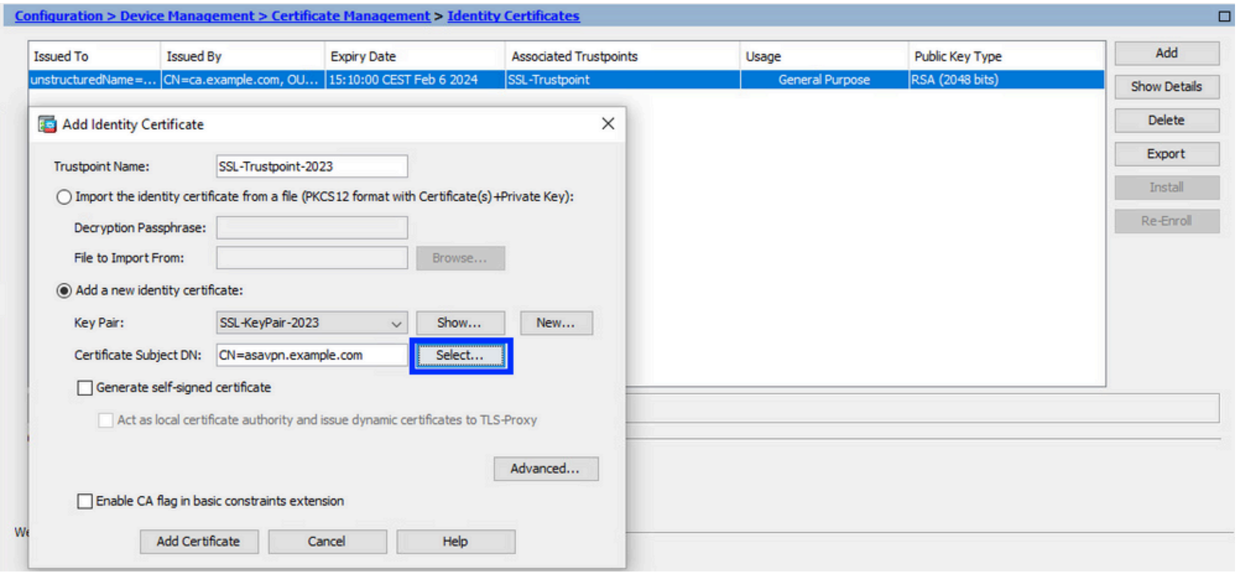
□ Enable CA flag in basic constraints extension

4. 配置證書主題和完全限定域名(FQDN)

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)。SSL/TLS/IKEv2客戶端使用SAN欄位來驗證證書是否與其所連線的FQDN匹配。

注意：CA在簽署CSR並建立已簽名的身份證書時，可以更改信任點中定義的FQDN和使用者名稱引數。

a. 按一下「Select」。



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-2023

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: SSL-KeyPair-2023

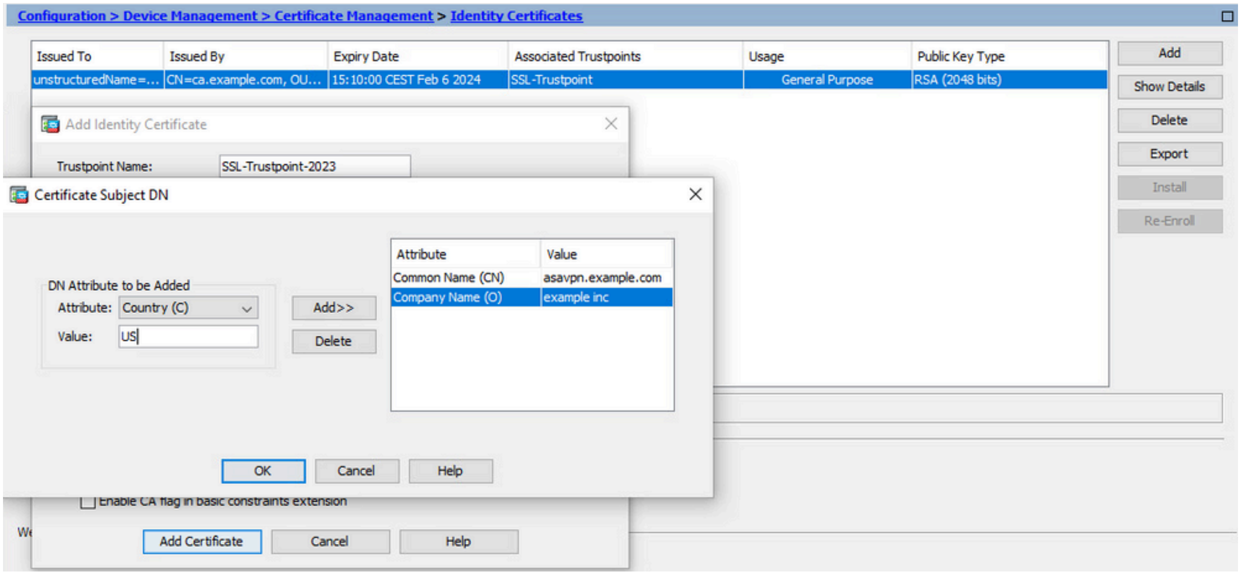
Certificate Subject DN: CN=asavpn.example.com

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

b. 在「Certificate Subject DN」視窗中，配置「certificate attributes - select attribute from」下拉選單，輸入值，然後按一下Add。



Configuration > Device Management > Certificate Management > Identity Certificates

Certificate Subject DN

DN Attribute to be Added

Attribute: Country (C)

Value: US

Attribute	Value
Common Name (CN)	asavpn.example.com
Company Name (O)	example inc

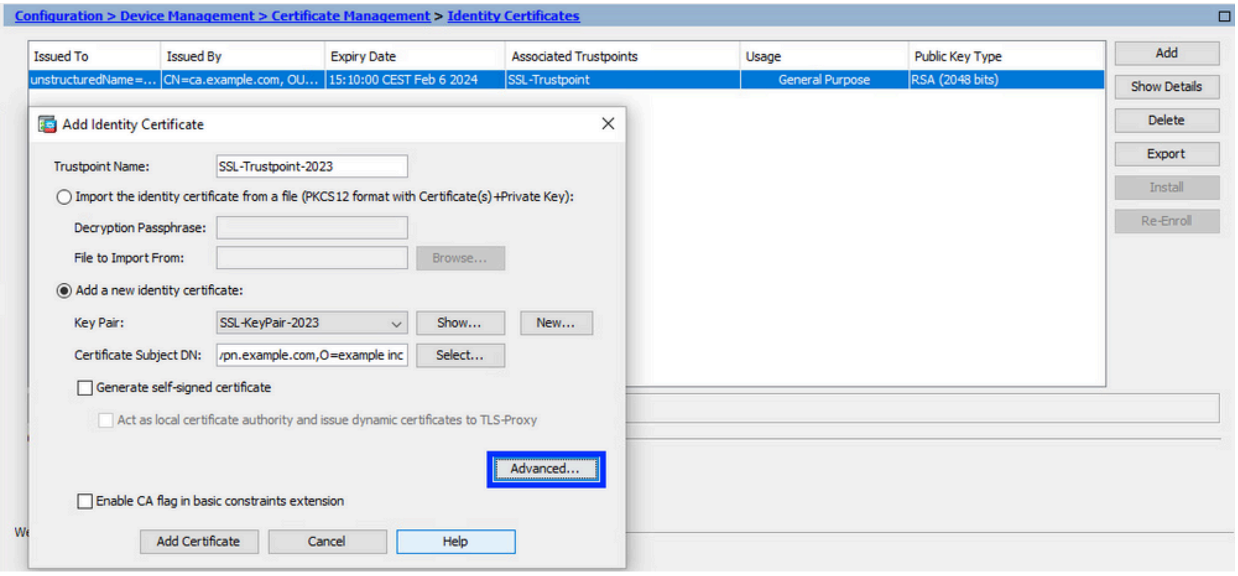
屬性	說明
CN	用於訪問防火牆的名稱(通常為完全限定域名，例如vpn.example.com)。
OU	組織內您所在部門的名稱
O	您的組織/公司的合法註冊名稱
思	國家/地區代碼（2個不帶標點的字母代碼）

屬性	說明
ST	組織所在的狀態。
L	組織所在的城市。
EA	電子郵件地址

> 註：前面的所有欄位都不能超過64個字元的限制。值越長，可能會導致身份證書安裝問題。此外，不必定義所有DN屬性。

新增完所有屬性後，按一下OK。

c. 要配置裝置FQDN，請按一下Advanced。


Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-2023

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: SSL-KeyPair-2023

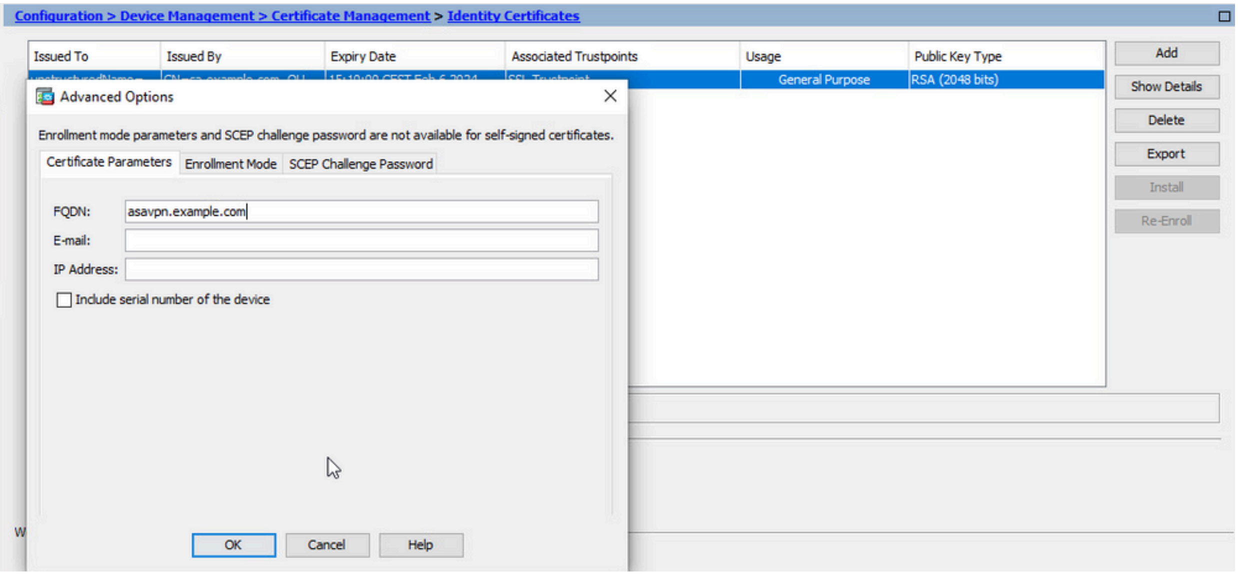
Certificate Subject DN: /pn.example.com,O=example inc

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

d. 在FQDN欄位中，輸入從Internet訪問裝置的完全限定域名。按一下「OK」（確定）。



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
				General Purpose	RSA (2048 bits)

Advanced Options

Enrollment mode parameters and SCEP challenge password are not available for self-signed certificates.

FQDN: asavpn.example.com

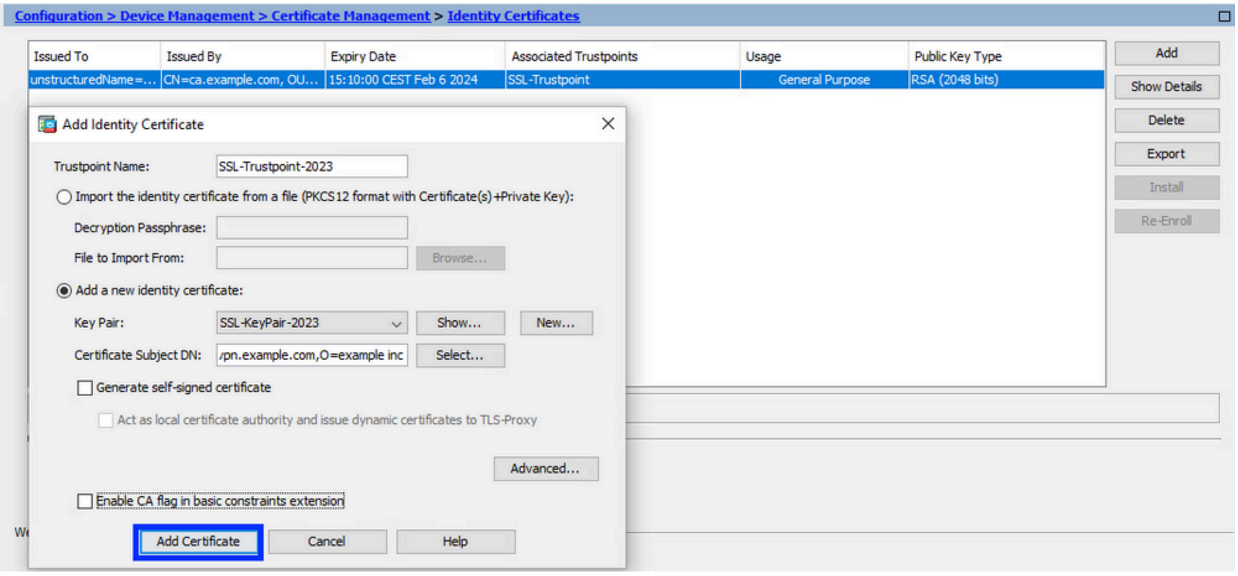
E-mail:

IP Address:

□ Include serial number of the device

5. 產生並儲存CSR

a. 按一下「新增憑證」。



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-2023

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: SSL-KeyPair-2023

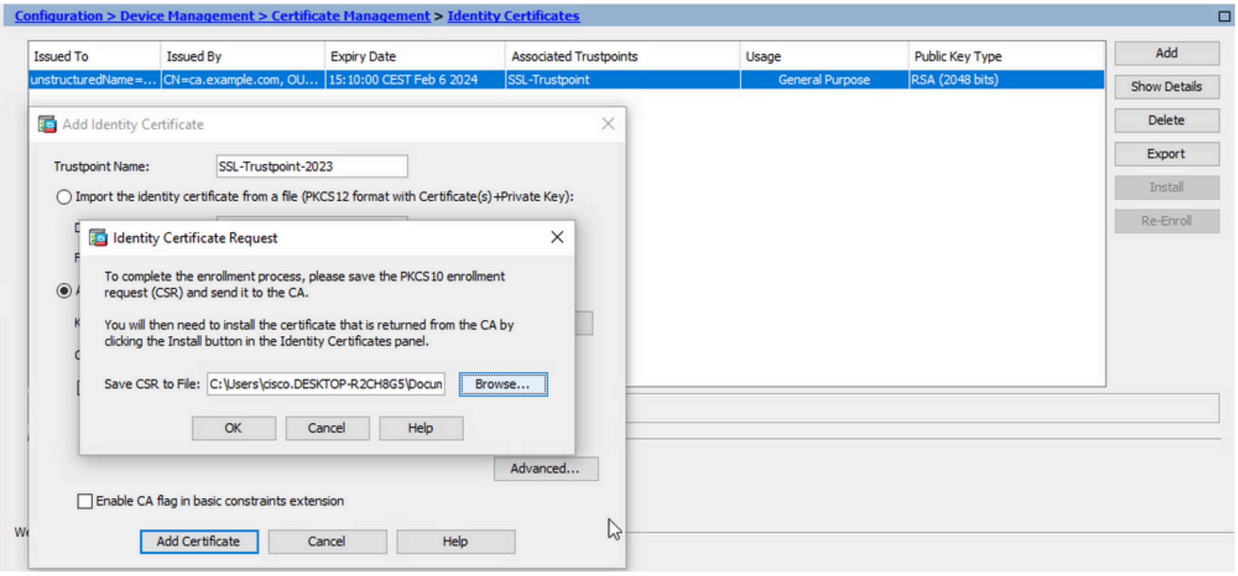
Certificate Subject DN: /pn.example.com,O=example inc

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

b. 提示隨即顯示，可將 CSR 儲存至本機電腦的檔案中。


Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)

Add
Show Details
Delete
Export
Install
Re-Enroll

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-2023

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

●

Identity Certificate Request

To complete the enrollment process, please save the PKCS10 enrollment request (CSR) and send it to the CA.

You will then need to install the certificate that is returned from the CA by clicking the Install button in the Identity Certificates panel.

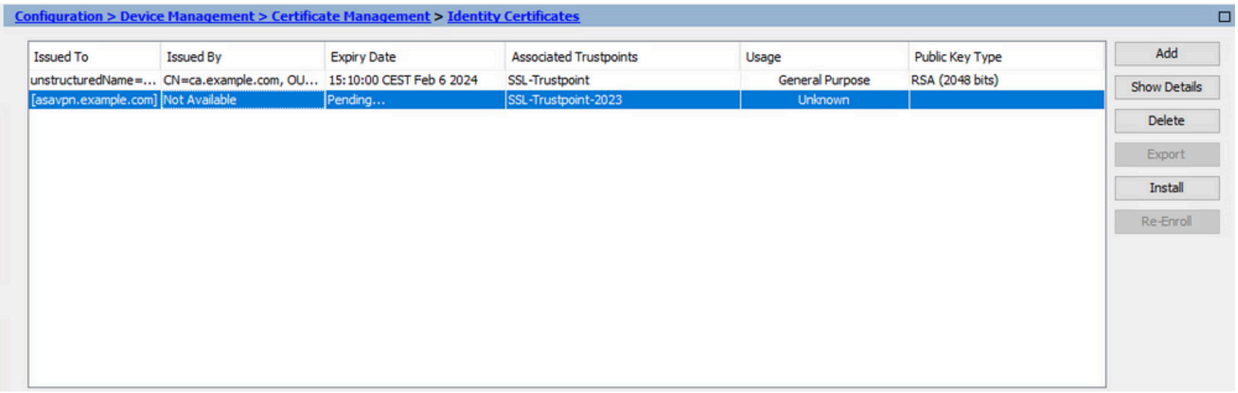
Save CSR to File: C:\Users\cisco.DESKTOP-R2CH8G5\Docun

□ Enable CA flag in basic constraints extension

按一下「Browse」。 選擇要儲存CSR的位置，並使用.txt副檔名儲存檔案。

> 注意：當檔案以.txt副檔名儲存時，可以使用文本編輯器（如記事本）開啟和檢視PKCS#10請求。

c. 現在，新信任點顯示為Pending狀態。


Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)
[asavpn.example.com]	Not Available	Pending...	SSL-Trustpoint-2023	Unknown	

Add
Show Details
Delete
Export
Install
Re-Enroll

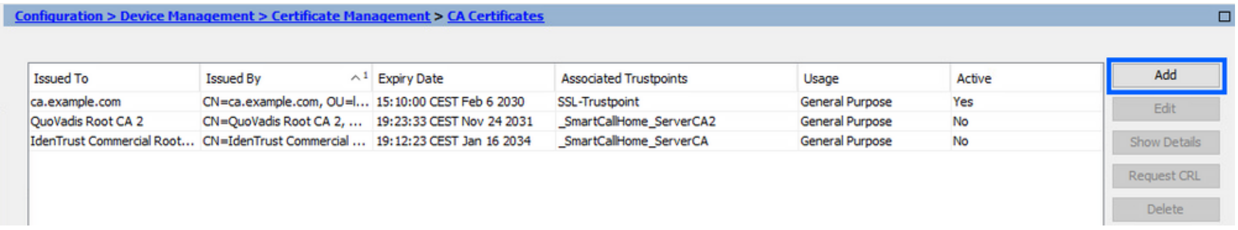
使用ASDM安裝PEM格式的身份證書

安裝步驟假設CA對CSR進行簽名，並提供PEM編碼(.pem、.cer、.crt)的新身份證書和CA證書捆綁包。

1. 安裝簽署CSR的CA證書

   簽名身份證書的CA證書可以安裝在為身份證書建立的信任點中。如果身份證書是由中間CA簽名的，則此CA證書可以安裝在身份證書信任點中。層次結構中上游的所有CA證書可以安裝在單獨的CA信任點中。

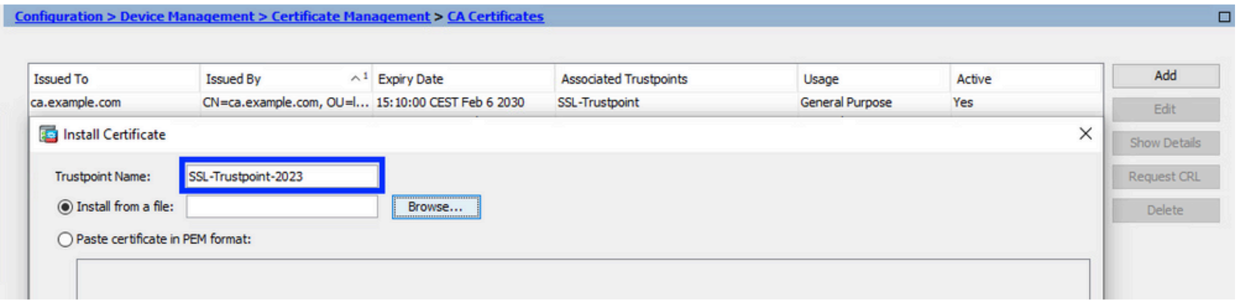
   a. 導覽至Configuration > Device Management > Certificate Management>，然後選擇CA Certificates。按一下「Add」。



Configuration > Device Management > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
ca.example.com	CN=ca.example.com, OU=l...	15:10:00 CEST Feb 6 2030	SSL-Trustpoint	General Purpose	Yes
QuoVadis Root CA 2	CN=QuoVadis Root CA 2, ...	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No
IdenTrust Commercial Root...	CN=IdenTrust Commercial ...	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No

b. 輸入Trustpoint名稱並選擇Install From File，按一下Browse按鈕，然後選擇intermediate證書。或者，也可以將PEM編碼的CA證書從文本檔案貼上到文本欄位中。



Configuration > Device Management > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
ca.example.com	CN=ca.example.com, OU=l...	15:10:00 CEST Feb 6 2030	SSL-Trustpoint	General Purpose	Yes

Install Certificate

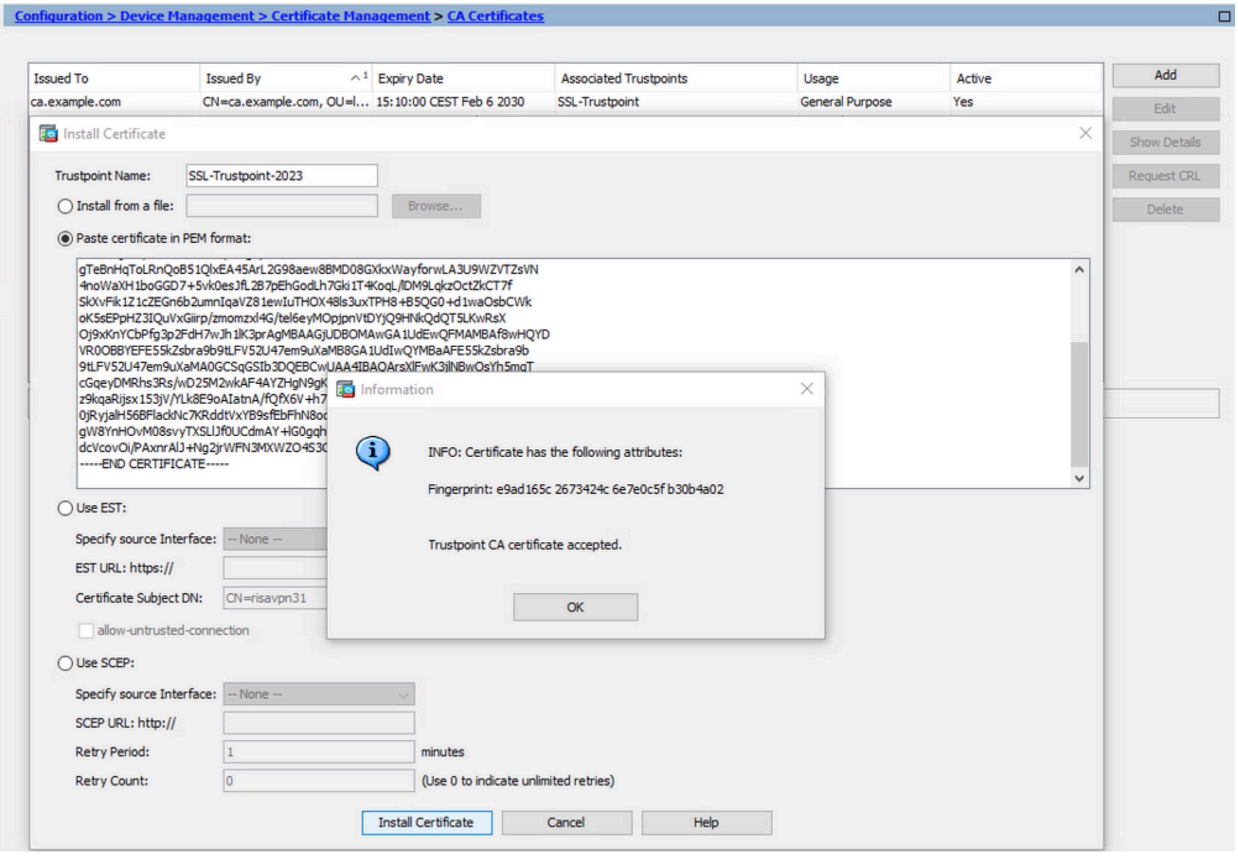
Trustpoint Name: SSL-Trustpoint-2023

● Install from a file:

○ Paste certificate in PEM format:

注意：如果身份證書由中間CA證書簽名，請安裝信任點名稱與身份證書信任點名稱相同的中間證書。

c. 按一下「Install Certificate」。



Configuration > Device Management > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
ca.example.com	CN=ca.example.com, OU=l...	15:10:00 CEST Feb 6 2030	SSL-Trustpoint	General Purpose	Yes

Install Certificate

Trustpoint Name: SSL-Trustpoint-2023

○ Install from a file:

● Paste certificate in PEM format:

```
gTeBnHqToLRnQoB51QlxEA45ArL2G98aew8BMD08GXkxWayforwLA3U9WZVTZsVN
4noWaXH1boGGD7+5vk0esJfL2B7pEhGodLh7Gki1T4KoqL/lDM9LqkzOctZkCT7f
SkXvFik1Z1cZEGn6b2umnIqaVZ81ewIuTHOX48ls3uxTPH8+B5QG0+d1waOsbCWk
oK5sEPpHZ3IQuVxGiirp/zmomzxl4G/tel6eyMOpjpnVtDYjQ9HNkQdQT5LKwRsX
Oj9xKnYCbPfg3p2FdH7wJh1lK3prAgMBAAGjUDBOMAwGA1UdEwQFMAMBAf8wHQYD
VR0OBBYEFE55kZsbra9b9tLFV52U47em9uXaMB8GA1UdIwQYMBaAFE55kZsbra9b
9tLFV52U47em9uXaMA0GCSqGSIb3DQEBCwUAA4IBAQArsXlFwK3ilNBwOsYh5mqT
cGqeyDMRhs3Rs/wD25M2wkAF4AYZHgN9gK
z9kqaRijsx153jV/YLk8E9oAIatnA/fQfX6V+h7
0jRyjalH56BFlackNc7KRddtVxYB9sfEbFhN8oc
gW8YnHOvM08svyTXSLlJf0UCdmAY+lG0gqh
dcVcovOi/PAxnrAlJ+Ng2jrWFN3MXWZO4S3C
-----END CERTIFICATE-----
```

○ Use EST:

Specify source Interface: -- None --

EST URL: https://

Certificate Subject DN: CN=risavpn31

□ allow-untrusted-connection

○ Use SCEP:

Specify source Interface: -- None --

SCEP URL: http://

Retry Period: 1 minutes

Retry Count: 0 (Use 0 to indicate unlimited retries)

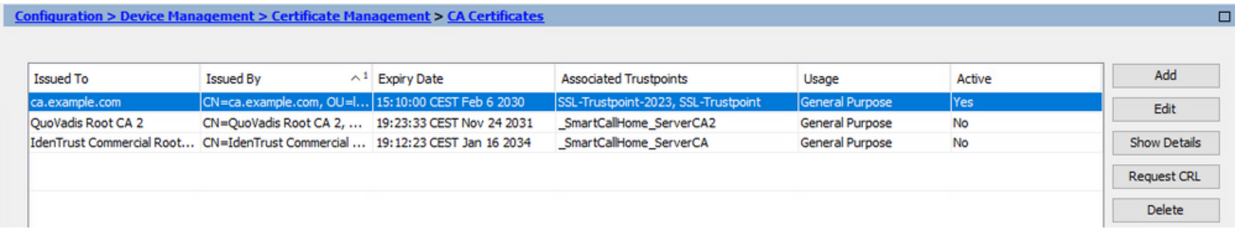
Information

INFO: Certificate has the following attributes:

Fingerprint: e9ad165c 2673424c 6e7e0c5f b30b4a02

Trustpoint CA certificate accepted.

在本例中，新證書使用與舊證書相同的CA證書簽名。同一個CA證書現在與兩個信任點關聯。

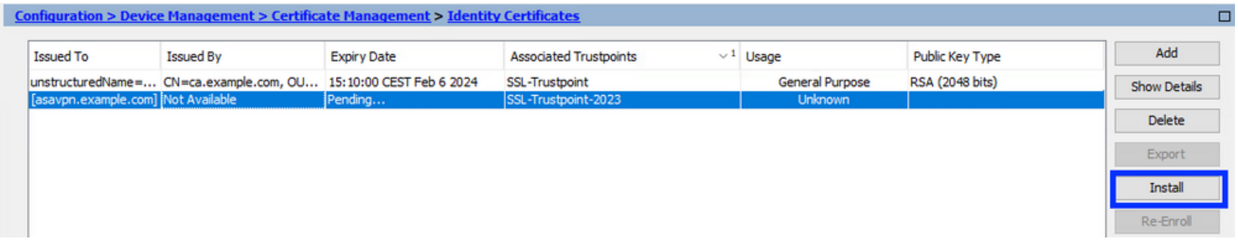


Configuration > Device Management > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
ca.example.com	CN=ca.example.com, OU=l...	15:10:00 CEST Feb 6 2030	SSL-Trustpoint-2023, SSL-Trustpoint	General Purpose	Yes
QuoVadis Root CA 2	CN=QuoVadis Root CA 2, ...	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No
IdenTrust Commercial Root...	CN=IdenTrust Commercial ...	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No

2. 安裝身份證書

a. 選擇之前通過生成CSR建立的身份證書。按一下「Install」。

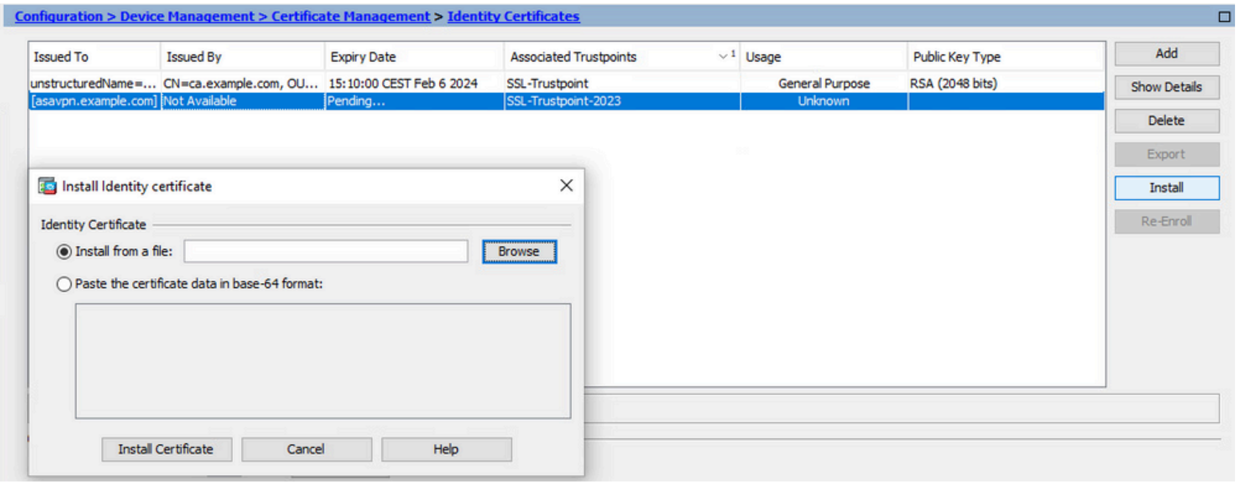


Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)
[asavpn.example.com]	Not Available	Pending...	SSL-Trustpoint-2023	Unknown	

注意：身份證書的Issued By欄位可用，Expiry Date欄位可用Pending。

b. 選擇包含從CA接收的PEM編碼身份證書的檔案，或在文本編輯器中開啟PEM編碼證書，然後將CA提供的身份證書複製並貼上到文本欄位中。



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)
[asavpn.example.com]	Not Available	Pending...	SSL-Trustpoint-2023	Unknown	

Install Identity certificate

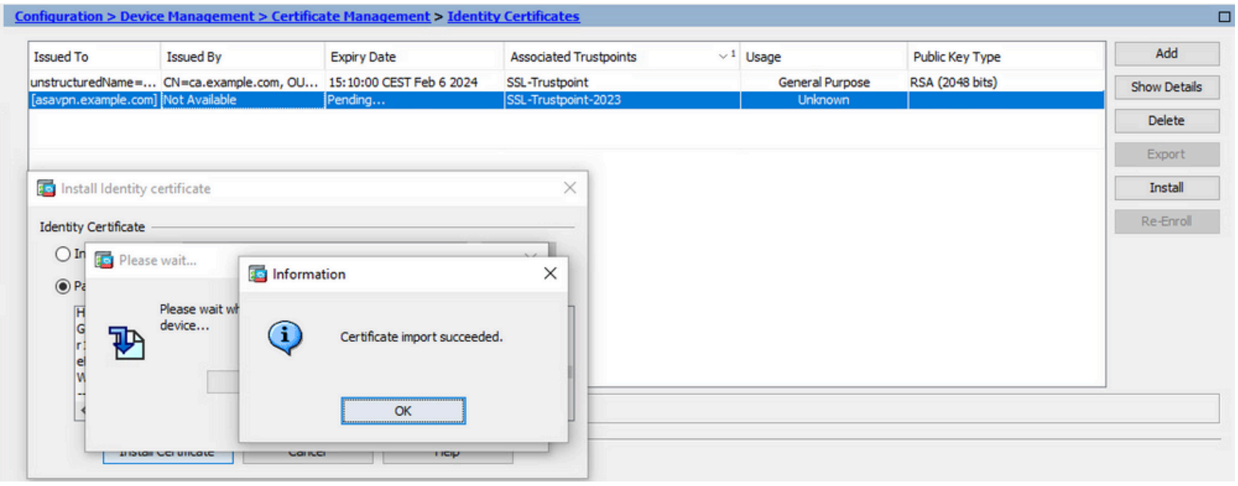
Identity Certificate

● Install from a file:

○ Paste the certificate data in base-64 format:

註：身份證書可以採用.pem、.cer、.crt格式進行安裝。

c. 按一下「Install Certificate」。

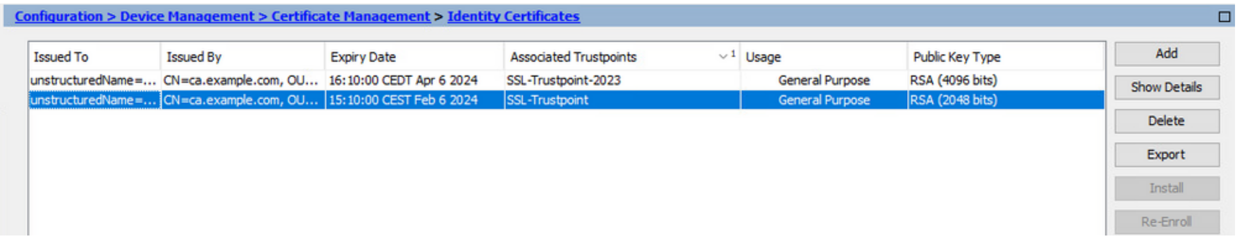


Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)
[asavpn.example.com]	Not Available	Pending...	SSL-Trustpoint-2023	Unknown	

Certificate import succeeded.

安裝後，存在舊身份證書和新身份證書。



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	16:10:00 CEDT Apr 6 2024	SSL-Trustpoint-2023	General Purpose	RSA (4096 bits)
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)

3. 將新證書繫結到與ASDM的介面

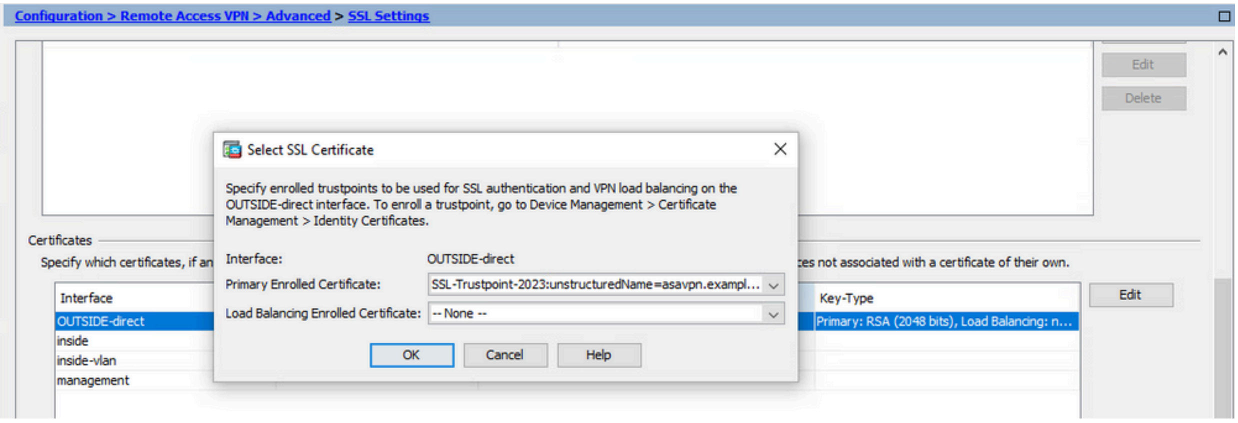
需要將ASA配置為使用新的身份證書，以便在指定介面上終止的WebVPN會話使用。

a. 導覽至「組態 >「遠端存取 VPN」>「進階」>「SSL 設定」。

b. 在「憑證」下方，選擇用於終止 WebVPN 作業階段的介面。在此範例中，所使用的是外部介面。

按一下「Edit」。

c. 在「憑證」下拉式清單中，選擇新安裝的憑證。



Configuration > Remote Access VPN > Advanced > SSL Settings

Select SSL Certificate

Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the OUTSIDE-direct interface. To enroll a trustpoint, go to Device Management > Certificate Management > Identity Certificates.

Interface: OUTSIDE-direct

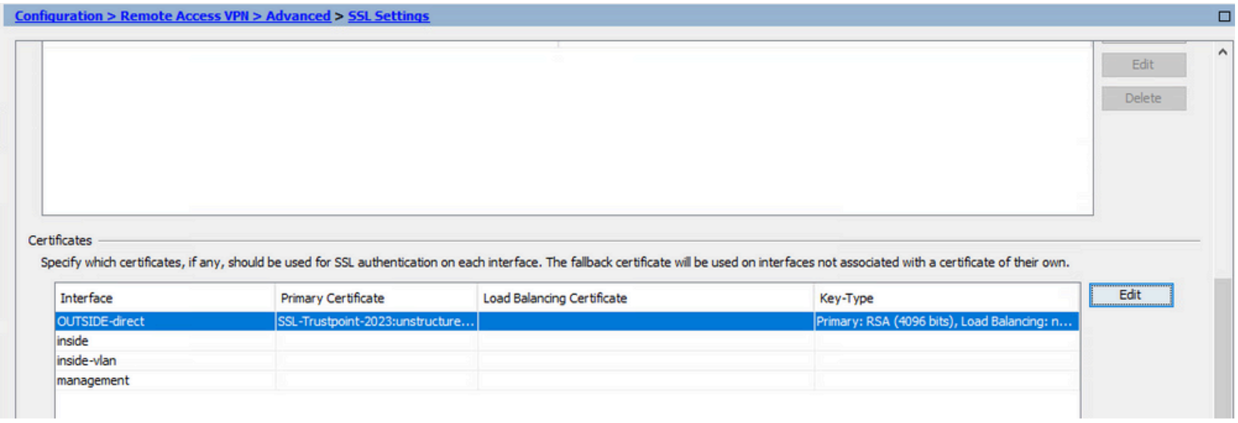
Primary Enrolled Certificate: SSL-Trustpoint-2023:unstructuredName=asavpn.exampl...

Load Balancing Enrolled Certificate: -- None --

OK
Cancel
Help
Edit
Delete
Certificates
Specify which certificates, if an
es not associated with a certificate of their own.
Interface
OUTSIDE-direct
inside
inside-vlan
management
Key-Type
Primary: RSA (2048 bits), Load Balancing: n...

d. 按一下「OK」（確定）。

e. 按一下「Apply」。現在，新的身份證書正在使用。



Configuration > Remote Access VPN > Advanced > SSL Settings

Certificates

Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.

Interface	Primary Certificate	Load Balancing Certificate	Key-Type
OUTSIDE-direct	SSL-Trustpoint-2023:unstructure...		Primary: RSA (4096 bits), Load Balancing: n...
inside			
inside-vlan			
management			

使用ASDM續訂用PKCS12檔案註冊的證書

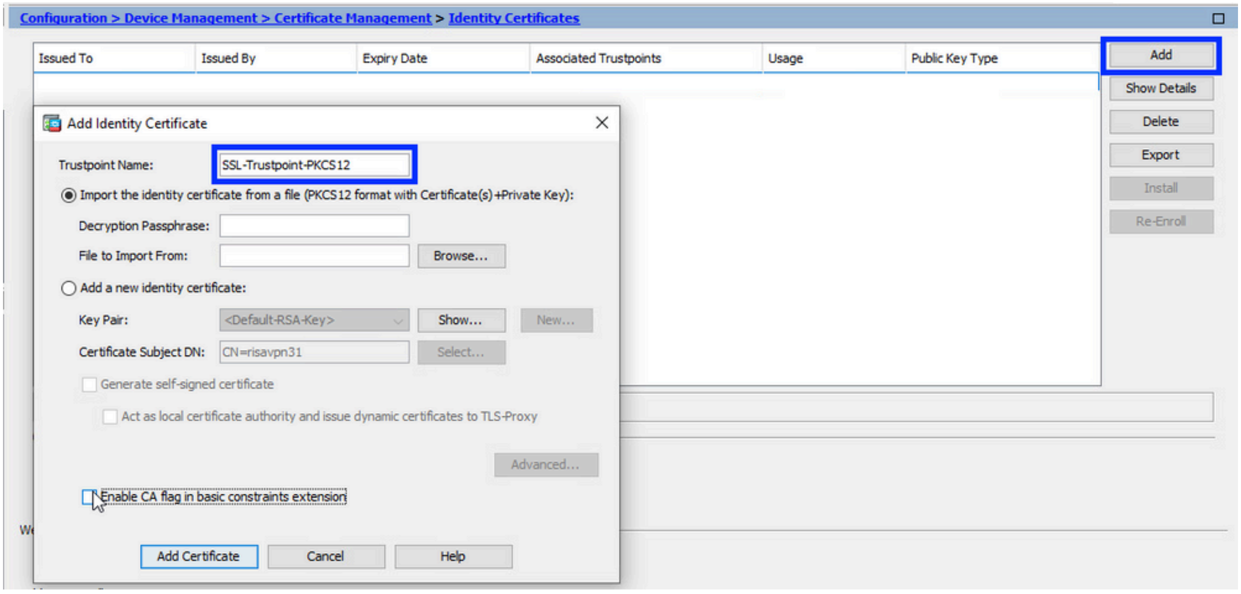
PKCS12註冊證書的證書續訂需要建立和註冊新的信任點。它需要具有不同的名稱（例如，具有登記年度字尾的舊名稱）。

PKCS12檔案（.p12或.pfx格式）包含身份證書、金鑰對和CA證書。例如，遇到萬用字元證書，它由CA建立，或者從其他裝置匯出。它是二進位制檔案，不能使用文本編輯器檢視。

1. 從PKCS12檔案安裝更新的身份證書和CA證書

   身份證書、CA證書和金鑰對需要捆綁到單個PKCS12檔案中。

   a. 導覽至Configuration > Device Management > Certificate Management，然後選擇Identity Certificates。
   b. 按一下「Add」。
   c. 指定新的Trustpoint名稱。



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-PKCS12

● Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

○ Add a new identity certificate:

Key Pair: <Default-RSA-Key>

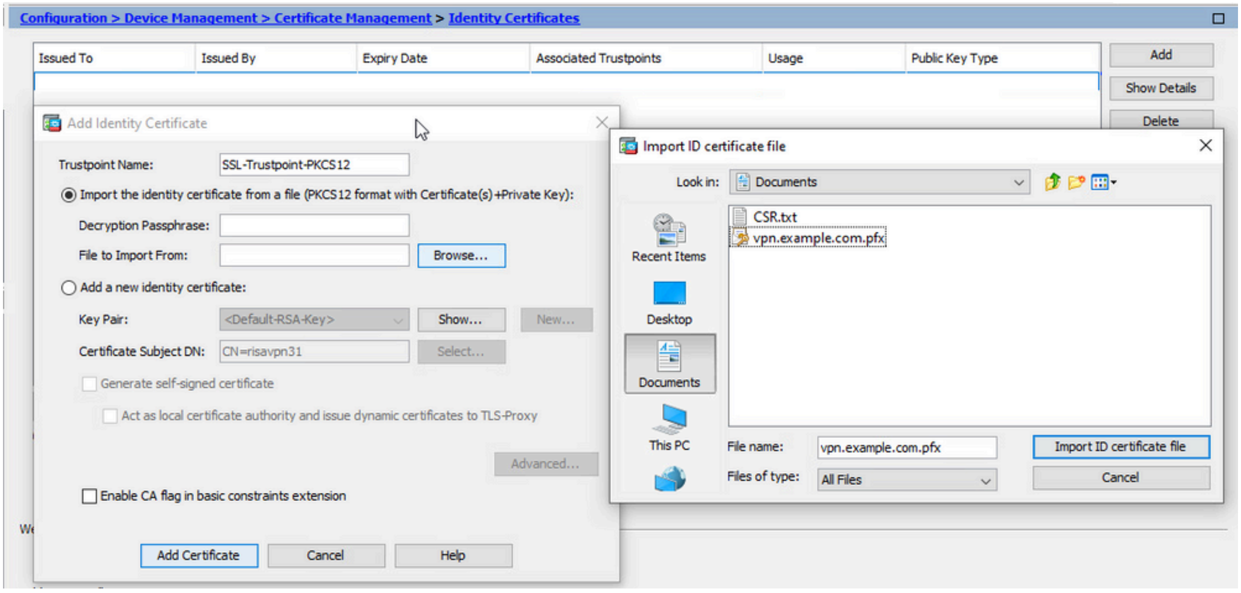
Certificate Subject DN: CN=risavpn31

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

   d. 按一下「從檔案匯入身分識別憑證」單選按鈕。



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-PKCS12

● Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

○ Add a new identity certificate:

Key Pair: <Default-RSA-Key>

Certificate Subject DN: CN=risavpn31

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

Import ID certificate file

Look in: Documents

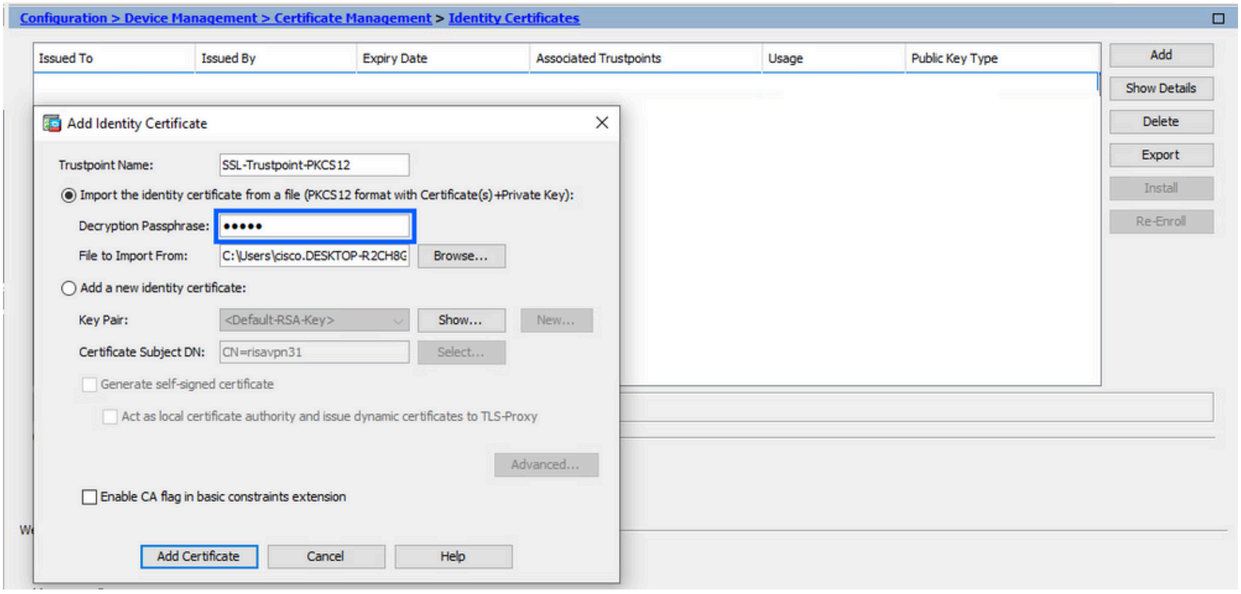
CSR.txt

vpn.example.com.pfx

File name: vpn.example.com.pfx

Files of type: All Files

e. 輸入用於建立 PKCS12 檔案的複雜密碼。



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-PKCS12

● Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase: •••••

File to Import From: C:\Users\cisco.DESKTOP-R2CH8G

○ Add a new identity certificate:

Key Pair: <Default-RSA-Key>

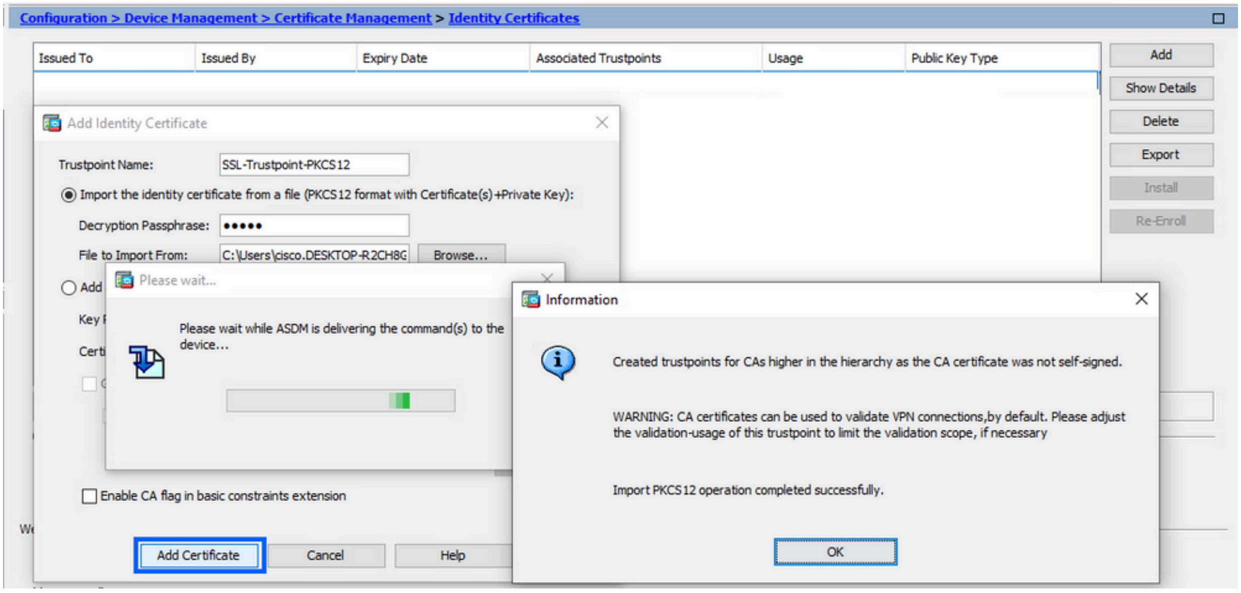
Certificate Subject DN: CN=risavpn31

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

f. 按一下「新增憑證」。



Trustpoint Name: SSL-Trustpoint-PKCS12

● Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase: •••••

File to Import From: C:\Users\cisco.DESKTOP-R2CH8G Browse...

□ Enable CA flag in basic constraints extension

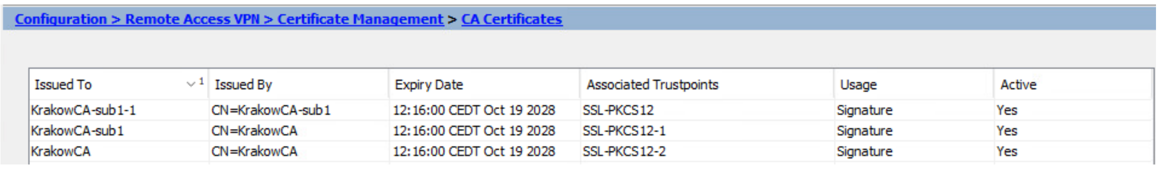
Please wait while ASDM is delivering the command(s) to the device...

Created trustpoints for CAs higher in the hierarchy as the CA certificate was not self-signed.

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

Import PKCS12 operation completed successfully.

注意：匯入具有CAs證書鏈的PKCS12時，ASDM會自動建立具有新增了 —number字尾的名稱的上游CAs信任點。


Configuration > Remote Access VPN > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
KrakowCA-sub1-1	CN=KrakowCA-sub1	12:16:00 CEDT Oct 19 2028	SSL-PKCS12	Signature	Yes
KrakowCA-sub1	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-1	Signature	Yes
KrakowCA	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-2	Signature	Yes

2. 將新證書繫結到與ASDM的介面

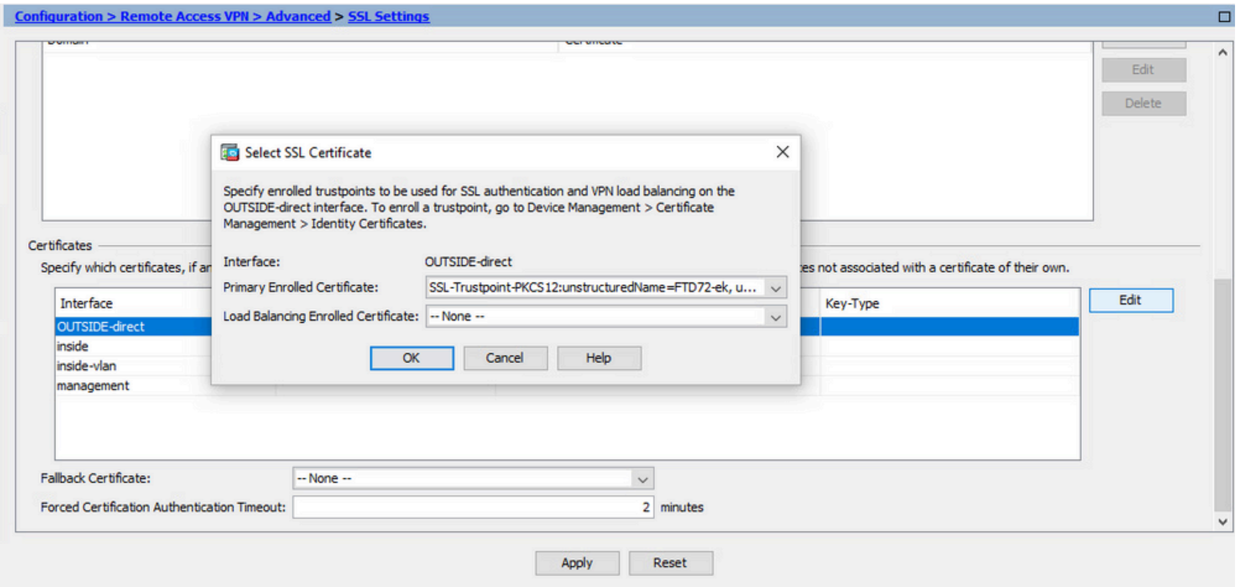
需要將ASA配置為使用新的身份證書，以便在指定介面上終止的WebVPN會話使用。

a. 導覽至「組態 >「遠端存取 VPN」>「進階」>「SSL 設定」。

b. 在「憑證」下方，選擇用於終止 WebVPN 作業階段的介面。在此範例中，所使用的是外部介面。

按一下「Edit」。

c. 在「憑證」下拉式清單中，選擇新安裝的憑證。



Configuration > Remote Access VPN > Advanced > SSL Settings

Select SSL Certificate

Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the OUTSIDE-direct interface. To enroll a trustpoint, go to Device Management > Certificate Management > Identity Certificates.

Interface: OUTSIDE-direct

Primary Enrolled Certificate: SSL-Trustpoint-PKCS12:unstructuredName=FTD72-ek, u...

Load Balancing Enrolled Certificate: -- None --

Certificates

Specify which certificates, if ar... es not associated with a certificate of their own.

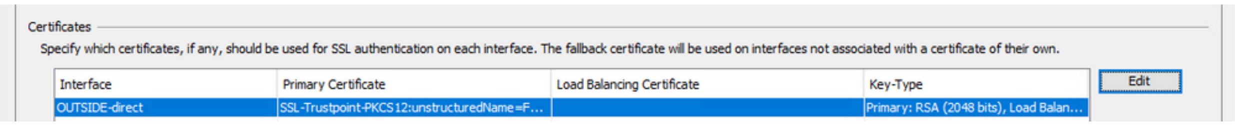
Interface	Key-Type
OUTSIDE-direct	
inside	
inside-vlan	
management	

Fallback Certificate: -- None --

Forced Certification Authentication Timeout: 2 minutes

d. 按一下「OK」（確定）。

e. 按一下「Apply」。



Certificates

Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.

Interface	Primary Certificate	Load Balancing Certificate	Key-Type
OUTSIDE-direct	SSL-Trustpoint-PKCS12:unstructuredName=F...		Primary: RSA (2048 bits), Load Balan...

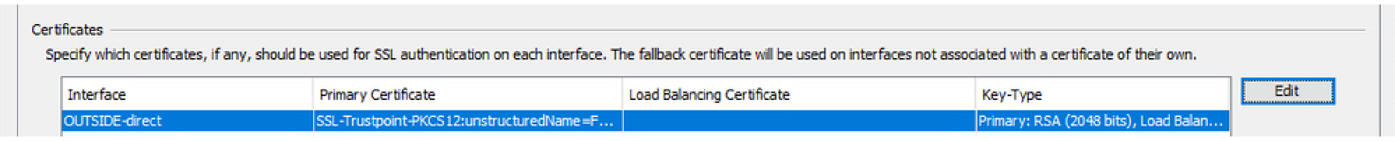
現在，新的身份證書正在使用。

驗證

使用以下步驟驗證第三方廠商憑證的成功安裝以及用於SSL VPN連線。

透過 ASDM 檢視安裝的憑證

1. 導覽至「組態」>「遠端存取 VPN」>「 Certificate Management」，然後選擇「身分識別憑證」。
2. 可能會顯示第三方供應商頒發的身份證書。



Certificates

Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.

Interface	Primary Certificate	Load Balancing Certificate	Key-Type
OUTSIDE-direct	SSL-Trustpoint-PKCS12:unstructuredName=F...		Primary: RSA (2048 bits), Load Balan...

疑難排解

如果SSL證書安裝失敗，則會在CLI上收集此debug命令。

- debug crypto ca 14

常見問題

問。什麼是PKCS12?
A.在加密中，PKCS12定義了一種存檔檔案格式，建立該格式是為了將許多加密對象儲存為一個檔案。它通常用於將私鑰與其X.509證書捆綁在一起，或者用於捆綁信任鏈中的所有成員。

問：什麼是CSR?
A.在公鑰基礎設施(PKI)系統中，證書簽名請求（也稱為CSR或證書請求）是從申請人傳送到公鑰基礎結構的註冊機構以申請數位身份證書的消息。它通常包含可為其頒發證書的公鑰、用於標識已簽名證書的資訊（如主題中的域名）以及完整性保護（如數位簽章）。

問：PKCS12的口令在哪裡？
A.將證書和金鑰對匯出到PKCS12檔案時，在export命令中給出口令。 對於匯入pkcs12檔案，密碼需要由所有者從另一裝置匯出PKCS12的CA伺服器或人員提供。

根與身份之間有什麼區別？
答：在密碼學和電腦保安領域，根證書是用來標識根證書頒發機構(CA)的公鑰證書。根證書是自簽名的（並且證書可以具有多個信任路徑，例如證書是否由交叉簽名的根頒發），並構成基於X.509的公鑰基礎架構(PKI)的基礎。公鑰證書也稱為數位證書或身份證書，是一種用於證明公鑰所有權的電子文檔。證書包括有關金鑰的資訊、有關其所有者（稱為主題）的標識的資訊以及驗證證書內容的實體（稱為頒發者）的數位簽章。如果簽名有效，並且檢查證書的軟體信任頒發者，那麼它就可以使用該金鑰與證書的使用者安全地通訊。

問：我安裝了證書，為什麼它無法工作？
A.這可能是由於多種原因，例如：

1.已配置證書和信任點，但尚未將其繫結到應使用該證書和信任點的進程。 例如，要使用的信任點不會繫結到終止Anyconnect客戶端的外部介面。

2.已安裝PKCS12檔案，但由於PKCS12檔案中缺少中間CA證書而出現錯誤。如果客戶端的中間CA證書為受信任，但根的CA證書不是受信任，則無法驗證整個證書鏈並報告伺服器身份證書為不受信任。

3.使用不正確的屬性填充的證書可能會導致安裝失敗或客戶端錯誤。例如，某些屬性可能使用錯誤的格式進行編碼。另一個原因是標識證書缺少主體備用名稱(SAN)，或者用於訪問伺服器的域名沒有作為SAN存在。

問：安裝新證書是否需要維護視窗或導致停機時間？
A.安裝新證書（身份或CA）不會帶來干擾，不應導致停機或要求維護視窗。要啟用新證書用於已存在的服務，需要更改並且可能需要更改請求/維護視窗。

問：添加或更改證書可以斷開連線的使用者嗎？
答：不，當前連線的使用者保持連線。該證書在建立連線時使用。使用者重新連線後，會使用新憑證。

問：如何使用萬用字元建立CSR?還是主題備用名稱(SAN)?
A.目前，ASA/FTD無法使用萬用字元建立CSR；但是，此過程可以使用OpenSSL完成。若要產生CSR和ID金鑰，您可以執行以下命令：

```
openssl genrsa -out id.key 2048
```

```
openssl req -out id.csr -key id.key -new
```

使用完全限定域名(FQDN)屬性配置信任點時，由ASA/FTD建立的CSR包含具有該值的SAN。CA在簽署CSR時可以新增更多SAN屬性，或可以使用OpenSSL建立CSR

問：證書更換是否立即生效？

A.新伺服器身份證書僅用於新連線。新證書可在更改後立即使用，但實際上用於新連線。

問：如何檢查安裝是否成功？
A.要驗證的CLI命令：show crypto ca cert <trustpointname>

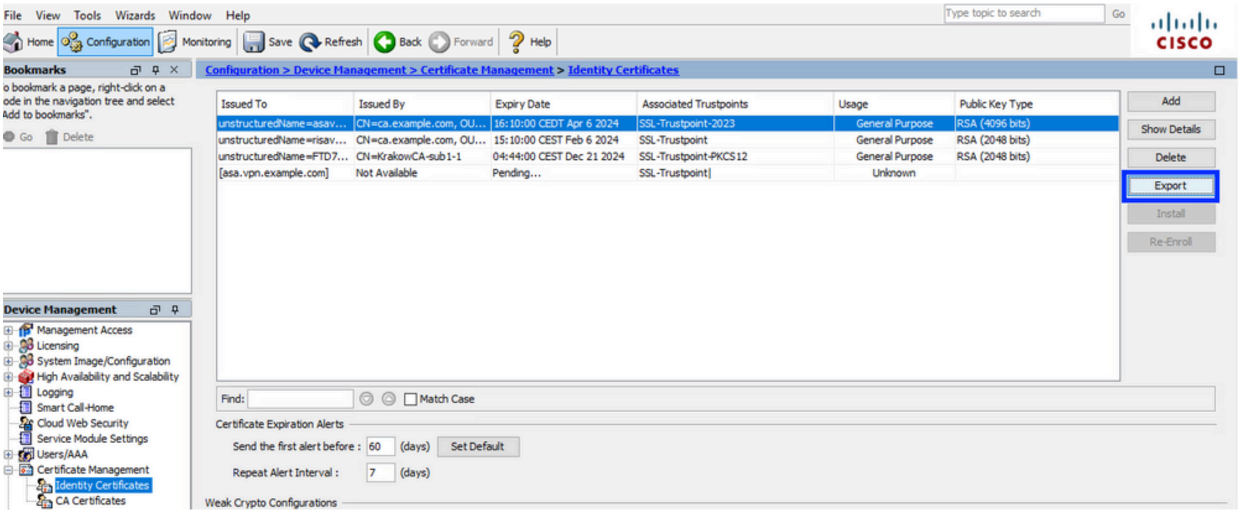
問。如何從身份證書、CA證書和私鑰生成PKCS12?
A.PKCS12可以使用OpenSSL使用以下命令建立：

```
openssl pkcs12 -export -out p12.pfx -inkey id.key -in id.crt -certfile ca.crt
```

問：如何匯出證書以在新ASA中安裝該證書？
A.

- 使用CLI：使用命令：crypto ca export <trustpointname> pkcs12 <password>
- 使用ASDM:

  a. 導航到Configuration > Device Management > Certificate Management > Identity Certificates，然後選擇Identity Certificate。按一下「Export」。



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=asav...	CN=ca.example.com, OU...	16:10:00 CEDT Apr 6 2024	SSL-Trustpoint-2023	General Purpose	RSA (4096 bits)
unstructuredName=risav...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)
unstructuredName=FTD7...	CN=KrakowCA-sub1-1	04:44:00 CEST Dec 21 2024	SSL-Trustpoint-PKCS12	General Purpose	RSA (2048 bits)
[asa.vpn.example.com]	Not Available	Pending...	SSL-Trustpoint|	Unknown	

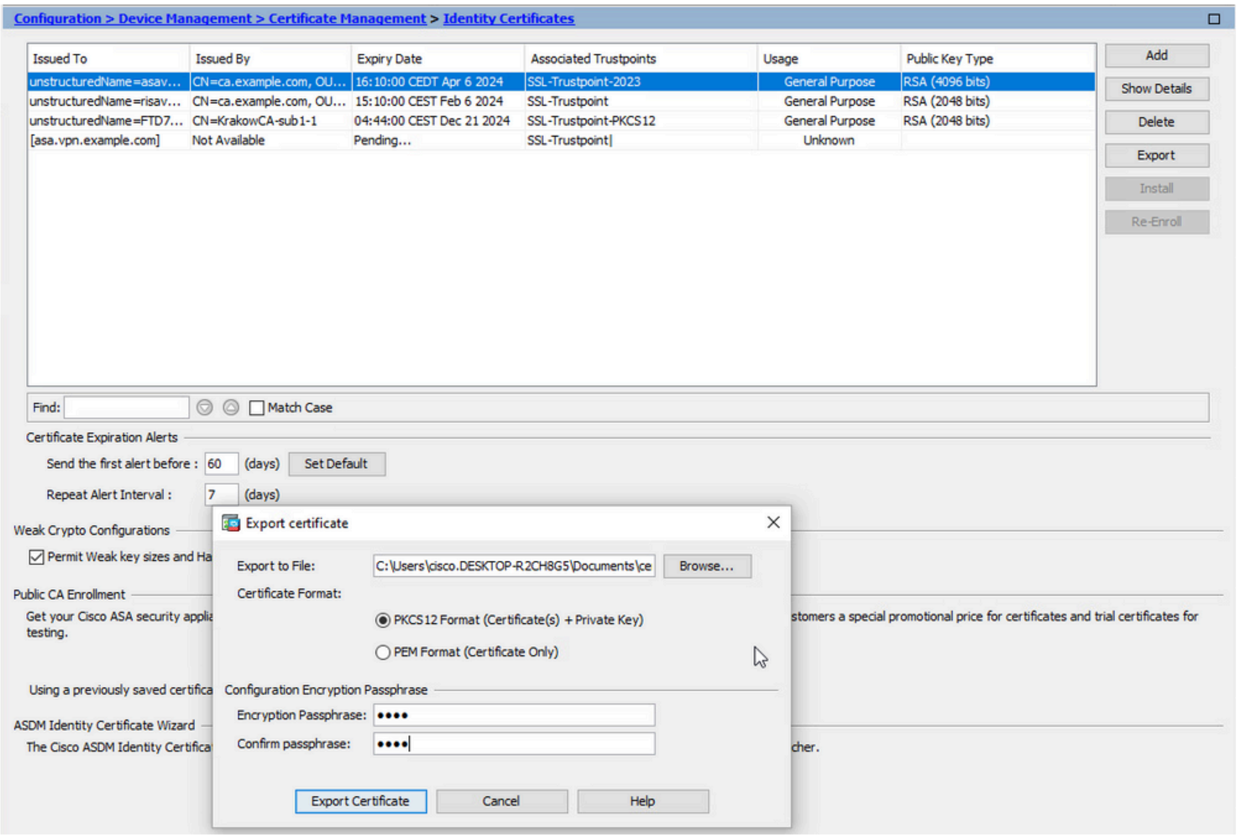
Certificate Expiration Alerts

Send the first alert before : 60 (days)

Repeat Alert Interval : 7 (days)

Weak Crypto Configurations

  b. 選擇匯出檔案的位置，指定匯出密碼，然後按一下Export Certificate。



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=asav...	CN=ca.example.com, OU...	16:10:00 CEDT Apr 6 2024	SSL-Trustpoint-2023	General Purpose	RSA (4096 bits)
unstructuredName=risav...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)
unstructuredName=FTD7...	CN=KrakowCA-sub1-1	04:44:00 CEST Dec 21 2024	SSL-Trustpoint-PKCS12	General Purpose	RSA (2048 bits)
[asa.vpn.example.com]	Not Available	Pending...	SSL-Trustpoint|	Unknown	

Certificate Expiration Alerts

Send the first alert before : 60 (days) Set Default

Repeat Alert Interval : 7 (days)

Weak Crypto Configurations

☑ Permit Weak key sizes and Ha

Public CA Enrollment

Get your Cisco ASA security appli stomers a special promotional price for certificates and trial certificates for testing.

Using a previously saved certifica

ASDM Identity Certificate Wizard

The Cisco ASDM Identity Certifica cher.

Export certificate

Export to File: C:\Users\cisco.DESKTOP-R2CH8G5\Documents\ce

Certificate Format:

● PKCS12 Format (Certificate(s) + Private Key)

○ PEM Format (Certificate Only)

Configuration Encryption Passphrase

Encryption Passphrase: ••••

Confirm passphrase: ••••

匯出的證書可以在電腦磁碟上。請記下安全位置的密碼，否則檔案將無用。

問：如果使用ECDSA金鑰，則SSL證書生成過程是否不同？
A.配置的唯一區別是金鑰對生成步驟，在該步驟中可生成ECDSA金鑰對，而不是RSA金鑰對。其他步驟皆維持不變。

問：是否總是需要生成新的金鑰對？
答：金鑰對生成步驟是可選的。可以使用現有的金鑰對，或者，在PKCS12的情況下，金鑰對隨證書匯入。請參閱選擇金鑰對名稱部分，瞭解相應的註冊/重新註冊型別。

問：為新的身份證書生成新的金鑰對是否安全？
A.只要使用新的金鑰對名稱，該過程就是安全的。在這種情況下，舊金鑰對不會更改。

問：在更換防火牆（如RMA）時，是否需要再次生成金鑰？
A.新防火牆的設計沒有在舊防火牆上提供金鑰對。
運行配置的備份不包含金鑰對。
使用ASDM完成的完全備份可以包含金鑰對。
可以在身份證書失敗之前通過ASDM或CLI從ASA中匯出身份證書。
在故障轉移對的情況下，使用write standby命令將證書和金鑰對同步到備用裝置。如果替換了故障轉移對中的一個節點，則只需配置基本故障轉移並將配置推送到新裝置即可。
如果裝置丟失了金鑰對，並且沒有備份，則需要使用新裝置上存在的金鑰對來簽署新證書。

關於此翻譯