

# ةيمقرلا SSL ةداهش تيبتت: ASA نيوكت اهديجتو

## تايوتحمل

[ةمدقملا](#)

[ةيساسأ تامولعم](#)

[ةيساسأ لابل طتملا](#)

[تابل طتملا](#)

[ةمدختس ملاتانوك ملا](#)

[نيوكت ملا](#)

[عاش نا](#)

[1. ASDM مادختس اب نيوكت ملا](#)

[2. ASA CLI عم طبضا](#)

[3. CSR عاش نال OpenSSL مادختس أ](#)

[CA لعل SSL ةداهش عاش نا](#)

[GoDaddy CA لعل SSL Certificate Generate لعل لاثم](#)

[ASA لعل SSL ةداهش تيبتت](#)

[1. ASDM مادختس اب PEM قيس نيب ةي وهلا ةداهش تيبتت 1.1](#)

[2. رماوأل رطس ةهجو عم PEM ةداهش تيبتت 1.2](#)

[3. ASDM عم PKCS12 ةداهش تيبتت 2.1](#)

[2. رماوأل رطس ةهجو عم PKCS12 ةداهش تيبتت 2.2](#)

[ةحصل لامل نم ققحت ملا](#)

[ASDM ربع ةتبت ملاتاداهش لامل ضرع](#)

[رماوأل رطس ةهجو ربع ةتبت ملاتاداهش لامل ضرع](#)

[بيو ضرعتسم مادختس اب WebVPN ل ةداهش ل تيبتت نم ققحت ملا](#)

[ASA لعل SSL ةداهش ديجت](#)

[قركت ملال ةلئس أ](#)

[1. ؟رأ ASA لمل ASA نم ةي وهلا تاداهش ل قبل ةقير ط لصفأ يه ام](#)

[2. ؟كبتش لاملح ةنزاومت ةصاخلا ASA تادجو عم مادختس ال SSL تاداهش عاش نال كنكمي فيك ؟ \(VPN\) ةي وهلا ةصاخلا](#)

[3. ؟ل اعأل زواجت ل ASA جوز ي ف يونال ل ASA لمل يساس أ ASA نم تاداهش ل خسن بجي له](#)

[4. ؟ SSL ةداهش عاش نال ةيلمع فلخت له ECDSA حيث افم مادختس ام اذا](#)

[اهجالص او عاخال فاش كتسا](#)

[اهجالص او عاخال فاش كتسا رماوأل](#)

[ةعئاش لال تالكش ملا](#)

[ققحت ملا](#)

[RSA او ECDSA: أ قحت ملا](#)

[جات فمو CA ةداهش و ةي وه ةداهش نم PKCS12 ةداهش عاش نال OpenSSL مادختس أ: ب قحت ملا صاخ](#)

[ةلص تاذا تامولعم](#)

## ةمدقملا

تالاصتال ASA ىلع اهب قووثوم ةيچراخ ةهجل ةيمقرر SSL ةداهش تيبتت دنتسملا اذه فصبي SSLVPN و AnyConnect و ليمع نودب SSLVPN.

## ةيساسأ تامولعم

ةلدعمل نامألا ةزهجأ ريديم ءارجا ىلع ةوطخ لك يوتحت .لاثملا اذه يف GoDaddy ةداهش مدختست رماوأل رطس ةهجاو نم هلداغي امو (ASDM).

## ةيساسألا تابلطتملا

### تابلطتملا

ةداهشلا ليچستل (CA) هب قووثوم يچراخ قدصم عجرم ىلا لوصول دنتسملا اذه ببلطتي و Cisco و Baltimore ، رصلال للاثملا لىبس ىلع ، ةيچراخ تاهج نم CA يعباب ةلثمأ لمشت Entrust و Geotrust و G و Microsoft و RSA و Thawte و VeriSign.

عم ةححصلا ةينمزالا ةقطنملاوخييراتلاو ةعاسلا تقو هيدل ASA نأ نم ققحت ، ءدبلا لبق ىلع تقولا ةنمازمل (NTP) ةكبشلا تقو لوكوتورب مداخ مادختساب ىصوي ، ةداهشلا ةقداصم [Cisco ASA Series General](#) ةماعلا [Cisco ASA تايلمعل رماوأل رطس ةهجاو نيوكت ليلى](#) حضوي .ASA .خييراتلاو تقولا دادعإل اءاخإ بجي يتلا تاوطخلال ليصفتلاب 9.1 رادصإل ، [Operations CLI](#) ، ىلع ححص لكشب ASA.

### ةمدختسملا تانوكملا

7.4(1) ةغيص ASDM و 9.4.1 ةغيص ةيچمررب ضكري نأ ASA 5500-X ةقپتو اذه لمعتسي

ةصاخ ةيلمعم ةئيبي يف ةدوجوملا ةزهجالا نم دنتسملا اذه يف ةدراولا تامولعمل ءاشنإ مت تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسملا ةزهجالا عيمج تءب رمايأل لمحتملا ريثأتلل كمهف نم دكأتف ، ليغشتلا ديقتككشب

## نيوكتلا

ةقداصم ءارجال ليملعلل مداخ ةداهش ليملعلل SSL مداخ رفوي نأب SSL لوكوتورب يضيقي مدختسملا موقبي نأ لامتحا ببسب ايتاذه ةعقوم ةداهش مادختساب Cisco يصوتال .مداخال جاعزا اضيا كانه .ءدخم مداخ نم ةداهش يف قثيل دصق ريغ نع ضرعتسم نيوكتب مادختساب ىصوي .ةنمألا ةبوابلاب هلاصتإ دنع نامأ ريذحت ىلا ةباجتسإلل نيمدختسملل ضرغلا اذهل ASA ىلا SSL تاداهش رادصإل اهب قووثوم ةيچراخ ةهجل ةعباتلا CAs

ةيلالال تاوطخلال عم ياساسأ لكشب متت ASA ىلع ثلاث فرط نم ةداهش ةايح ةرود:



CSR ءاشنإل قرط ثالث كانه

- ASDM مادختساب نيوكتل
- ASA CLI مادختساب نيوكتل
- CSR ءاشنإل OpenSSL مادختساب

1. ASDM مادختساب نيوكتل

1. Configuration > Remote Access VPN > Certificate Management، Identity Certificates. رتخاو
2. Add. رقنا

**Add Identity Certificate**

Trustpoint Name:

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:

Certificate Subject DN:

Generate self-signed certificate

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

Enable CA flag in basic constraints extension

3. TrustPoint مسا لاخذل قح ي TrustPoint مسا ديدحتب مق
4. Add a new identity certificate رزللا قوف رقنا
5. New قوف رقنا، حيتافملا جوز يلع لوصحلل

**Add Key Pair**

Key Type:  RSA  ECDSA

---

Name:  Use default key pair name  
 Enter new key pair name:

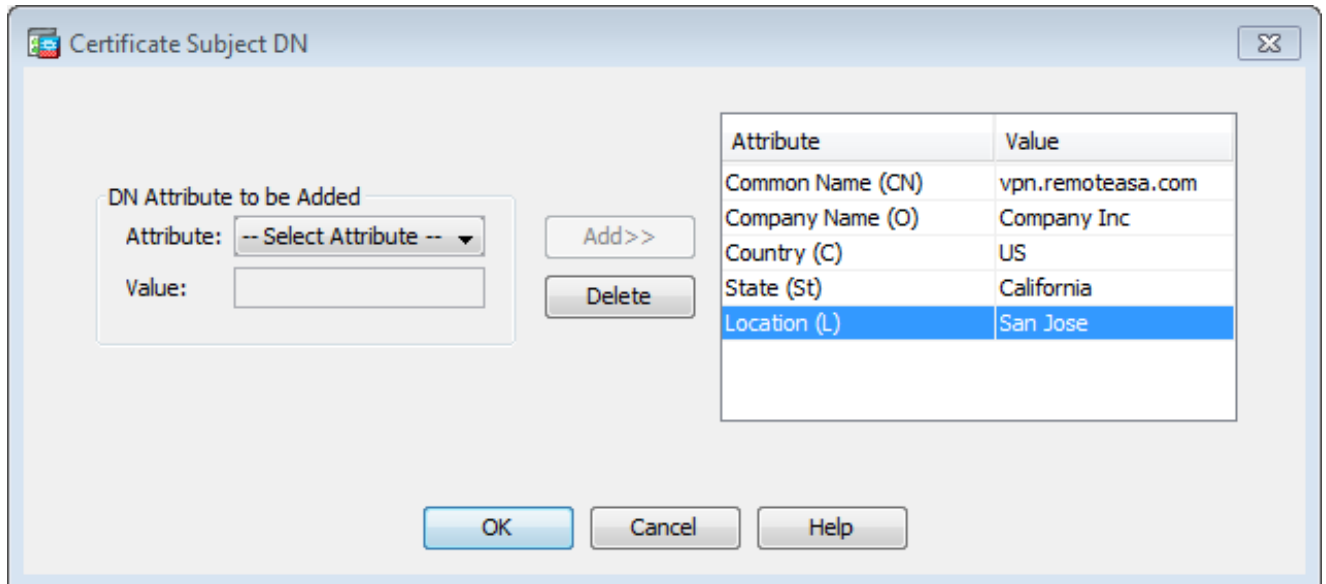
Size:  ▼

Usage:  General purpose  Special

6. (تأفالتخالال مهفل [أقحللملا](#) ىلإ عجرا) RSA وأ ECDSA - حاتفملا عون رتخأ.
7. فرعتللا ضارغأل حيتأفملا جوز مسا ىل ع فرعت. ىدارح Enter new key pair name رزللا قوف رقنا.
8. RSA عم General Purpose for Usage رتخأ. Key Size رتخأ.
9. حيتأفملا جوز عاشنإ متي Generate Now رقنا.
10. مقولودجلا اذف ةجردملا تامسلا قوف Select رقنا، ةداهشلا عوضومل DN ناوع فرعتللا:  
اهن ىوكتب:

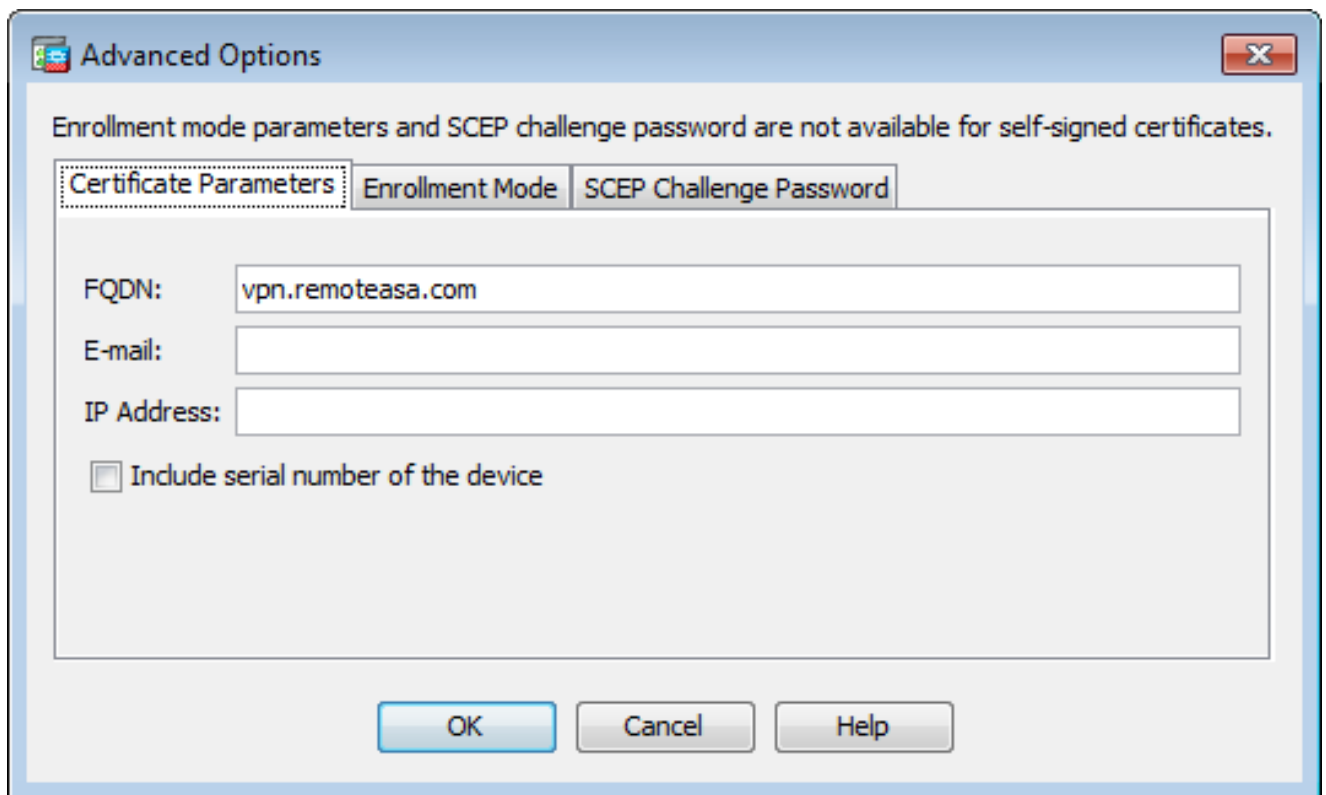
Attribute	Description
CN	FQDN (Full Qualified Domain Name) that will be used for connections to your firewall. For example, webvpn.cisco.com
OU	Department Name
O	Company Name (Avoid using Special Characters)
C	Country Code (2 Letter Code without Punctuation)
St	State (Must be spelled out completely. For example, North Carolina)
L	City
EA	Email Address

مٹ، ةمىقلا لخدأ مٹ، ةمسلا ةلدسنملا ةمئاقلا نم ةمىق رتخأ، مىقلا هذه نىوكتل  
ةفاضا قوف رقنا.



✎ رادصا لبق ةنبي عم تامس نبي مضت ةثلاثا ل فارطالا ي دروم ضعب بلطاتي :ةظحالم  
 يل ل ووصل ل دروم ل عجار ،ةبولطم ل تامس ل نم دكأت ل مدع ةلاح يف .ةي وه ةداهش  
 لي صافات

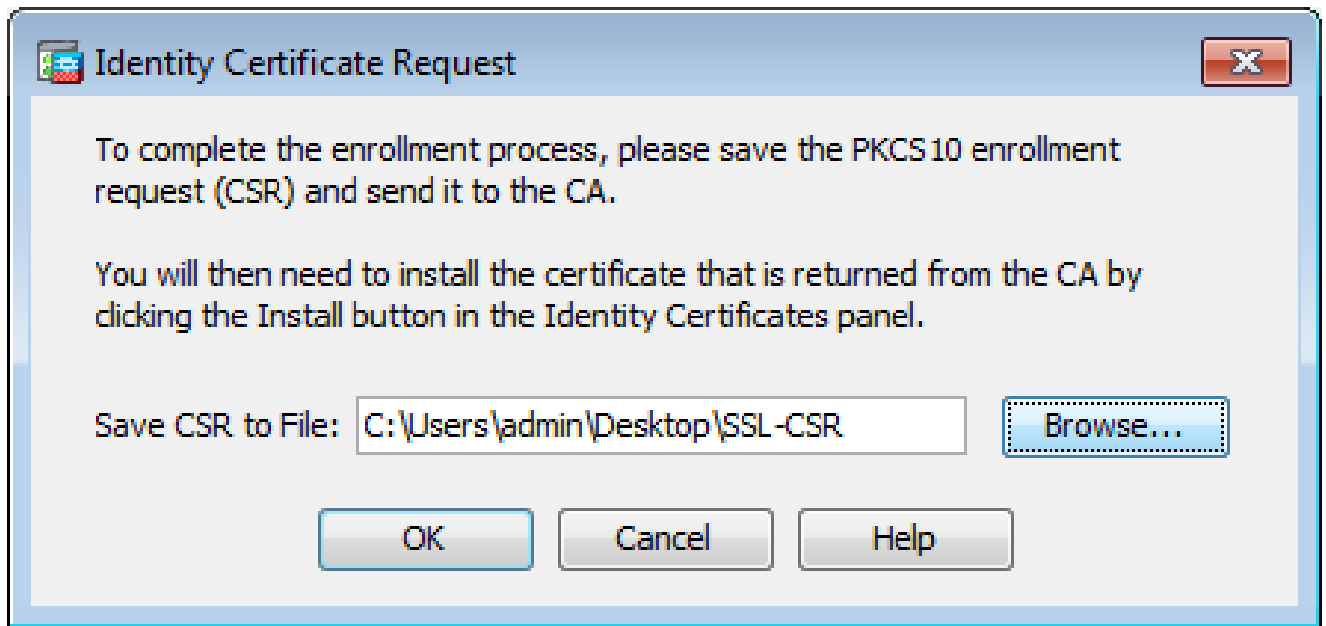
11. عم ةي وه ةداهش ةفاضل راوخل ع برم رهظي .OK قوف رقنا ،ةبسانم ل ميقل ةفاضل دع ب .  
 Subject DN field populated.
12. م دقت م ةق طقط .



13. ت نرتن ل نم زاوجل ل ل ووصل هم ادختسا م تي ي ذل فQDN ل خدأ ،ل قحل ل FQDN يف .  
 OK رقنا
14. تي بثت نكمي ال .ادحم ةي ساسا ل دو يقل قحل م راخي يف CA ني كمت ةم ال كرت  
 قحل م ددحي .ي ضارثا لكشب CA تاداهشك ASA ل عل نال CA ةم ال نودب ي تل تاداهش ل

تاراسم قم عمل ىصقألا دحلأو CA وه ةداهشلا عوضوم ناك اذا ام ةيساسألا دويقلا  
اذه زواجت رايخ دي دحت ءاغلاب مق .ةداهشلا هذه نمضتت يتلا ةحيحصلا تاداهشلا  
ببلملا .

15. يلملا زاهجلا ىلع فلم ىلإ CSR ظفحلا ةبلاطم ضرع .Add Certificate قوف رقنا مث ،OK رقنا .



16. txt دادتماب فلملا ظفح مث ،هيف CSR ظفح ديرت يذلا ناكملا رتخأ ،Browse رقنا .

هضرعو PKCS#10 ببلملا حتف نكمي ،.txt دادتماب فلملا ظفح دنع :ةظحالم  
(Notepad لثم) صوصن ررحم مادختساب

## 2. ASA CLI مادختساب نيوكتلا

يف CA ةداهش تي ببت دنع وأ CSR ءاشن دنع ايئاقلا TrustPoint ءاشن متي ، ASDM يف  
ايودي TrustPoint ءاشن بجي ،(CLI) رماوأل رطس ةهجاو

```
<#root>
```

```
! Generates 2048 bit RSA key pair with label SSL-Keypair.
```

```
MainASA(config)#
```

```
crypto key generate rsa label SSL-Keypair modulus 2048
```

```
INFO: The name for the keys are: SSL-Keypair  
Keypair generation process begin. Please wait...
```

```
! Define trustpoint with attributes to be used on the SSL certificate
```

```
MainASA(config)#
```

```
crypto ca trustpoint SSL-Trustpoint
```

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

enrollment terminal

MainASA(config-ca-trustpoint)#

fqdn (remoteasavpn.url)

MainASA(config-ca-trustpoint)#

subject-name CN=(asa.remotevpn.url),O=Company Inc,C=US,  
St=California,L=San Jose

MainASA(config-ca-trustpoint)#

keypair SSL-Keypair

MainASA(config-ca-trustpoint)#

exit

! Initiates certificate signing request. This is the request to be submitted via Web or Email to the third party vendor.

MainASA(config)#

crypto ca enroll SSL-Trustpoint

WARNING: The certificate enrollment is configured with an fqdn that differs from the system fqdn. If this certificate is 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 is: subject-name CN=

(remoteasavpn.url)

,  
O=Company Inc,C=US,St=California,L=San Jose

% The fully-qualified domain name in the certificate will be:

(remoteasavpn.url)

,

% Include the device serial number in the subject name? [yes/no]:

no

Display Certificate Request to terminal? [yes/no]:

yes

Certificate Request:

-----BEGIN CERTIFICATE REQUEST-----

MIIDDjCCAfyCAQAwgYkxETAPBgNVBACTCFNhbiBkb3NlMRMwEQYDVQQLIEwpcDZmYm1hMQswCQYDVQQGEwJVUzEUMBIGA1UEChMLQ29tcGFueSBJamMxGjAYBgNVBAMTEXZwbi5yZW1vdGVhc2EuY29tMSAwHgYJKoZIhvcNAQkCFhF2cG4ucmVtb3R1YXNhLmNvbTCCASIdDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK62Nhb9kt1K  
uR3Q4TmksyuRMqJNrb9kXpvA6H200PuBfQvSF4rVnSwK0mu3c8nweEvYcdVWV6Bz  
BhjXeovTVi17F1NTceaUTGikeIdXC+mw1iE7eRsynS/d4mzMWJmrvrsDNzpAW/EM  
SzTca+BvqF7X2r3LU8Vsv60i8ylhco9Fz7bwvRWVt03NDDbyo1C9b/VgXMuBitcc



```
rzfUbVnm7VZD0f4jr9EXgUwXxcQidWEAB1FrXrtYpFgBo9aqJmRp2YABQ1ieP4cY
3rBtgRjLcF+S9TvhG5m4v7v755meV4YqsZIXvytIOzVBihemVxaGA1oDwfkoYSFi
4CzXbFvdG6kCAwEAAaA/MD0GCSqGSIB3DQEJJDjEwMC4wDgYDVROPAQH/BAQDAgWg
MBwGA1UdEQQVMB0CEXZwbi5yZW1vdGVhc2EuY29tMA0GCSqGSIB3DQEBBQUAA4IB
AQBZuQzUXGEB0ix1yuPK0ZkRz8bPnwIqLTfxZhagmuyEhrN7N4+aQnCHj85oJane
4ztZDiCCoWTerBS4RSkKEHEspu9oohjCYuNnp5qa91SPrZNEjTWw0eRn+qKbId2J
jE6Qy4vdPCexavMLYVQxXny+gVzkzPN/sFRk3EcTTVq6DxxaebpJijmiqa7gCph52
YkHXnFne1LQd41BgoL1Cr9+hx74XsTHGBmI1s/9T5oAX26Ym+B21/i/DP5BktIUA
8GvIY1/ypj9K049fP5ap8a10qvLtYYcCcfwrCt+0oj0rZ1YyJb3dFuMNRdAX37t
DuHN12EYNpYkjVk1wI53/5w3
-----END CERTIFICATE REQUEST-----
```


Redisplay enrollment request? [yes/no]:

no

! Displays the PKCS#10 enrollment request to the terminal. Copy this from the terminal to a text file to submit to the third party CA.

### 3. إنشاء CSR مع OpenSSL

إنشاء CSR في نظام التشغيل Linux/Mac OS X باستخدام OpenSSL. هذه هي الخطوات لإنشاء CSR باستخدام OpenSSL.

 إن إنشاء CSR في نظام التشغيل Linux/Mac OS X باستخدام OpenSSL يتطلب بعض الخطوات الإضافية. هذه هي الخطوات لإنشاء CSR باستخدام OpenSSL.

1. هذه هي الخطوات لإنشاء CSR باستخدام OpenSSL في نظام التشغيل Linux/Mac OS X. الخطوات هي: إنشاء المفتاح الخاص، إنشاء CSR، ثم إرسال CSR إلى جهة خارجية للحصول على الشهادة.
2. في نظام التشغيل Linux/Mac OS X، الخطوات هي: إنشاء المفتاح الخاص، إنشاء CSR، ثم إرسال CSR إلى جهة خارجية للحصول على الشهادة.

في نظام التشغيل Windows: الخطوات هي: إنشاء المفتاح الخاص، إنشاء CSR، ثم إرسال CSR إلى جهة خارجية للحصول على الشهادة.

في نظام التشغيل Linux/Mac OS X: الخطوات هي: إنشاء المفتاح الخاص، إنشاء CSR، ثم إرسال CSR إلى جهة خارجية للحصول على الشهادة.

3. في نظام التشغيل Linux/Mac OS X، الخطوات هي: إنشاء المفتاح الخاص، إنشاء CSR، ثم إرسال CSR إلى جهة خارجية للحصول على الشهادة. الخطوات هي: إنشاء المفتاح الخاص، إنشاء CSR، ثم إرسال CSR إلى جهة خارجية للحصول على الشهادة.

```
[req]
```

```
default_bits = 2048
default_keyfile = privatekey.key
distinguished_name = req_distinguished_name
req_extensions = req_ext
```

```
[req_distinguished_name]
```

```
commonName = Common Name (eg, YOUR name)
```

```

commonName_default = (asa.remotevpn.url)

countryName = Country Name (2 letter code)
countryName_default = US

stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = California

localityName = Locality Name (eg, city)
localityName_default = San Jose

0.organizationName = Organization Name (eg, company)
0.organizationName_default = Company Inc

```

```
[req_ext]
```

```
subjectAltName = @alt_names
```

```
[alt_names]
```

```
DNS.1 = *.remotesa.com
```

#### 4. رمل اذہ مادختساب صاخلا حاتفملاو CSR ءاشن اب مق :

```
openssl req -new -nodes -out CSR.csr -config openssl.cnf
```

```
<#root>
```

```
# Sample CSR Generation:
```

```
openssl req -new -nodes -out CSR.csr -config openssl.cnf
```

```
Generate a 2048 bit RSA private key
```

```

.....+++
.....+++
writing new private key to 'privatekey.key'
-----

```

```

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----

```

```

Common Name (eg, YOUR name) [(asa.remotevpn.url)]:
Country Name (2 letter code) [US]:
State or Province Name (full name) [California]:
Locality Name (eg, city) [San Jose]:
Organization Name (eg, company) [Company Inc]:

```

عجرملا رفوي، ءداهشلا رادصا درجمبو. ءيجراخلا ءهجلل CA دروم ىلإ ظروف حمللا CSR لاسرا

قدصملا عجرملا ىلع اهتيبثتل قدصملا عجرملا ةداهش و ةيوهلا ةداهش قدصملا

## CA ىلع SSL ةداهش عاشنإ

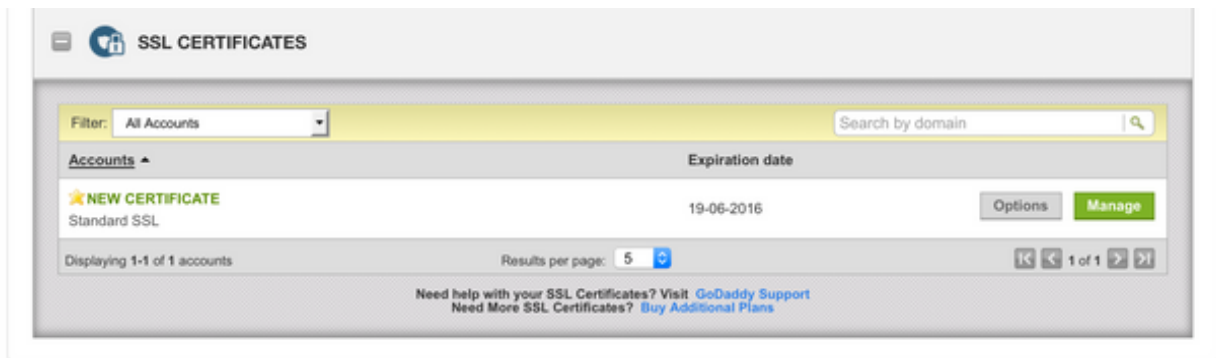
ةيوه ةداهش اما قدصملا عجرملا رفوي. CA نم CSR عيقوت ىلع لوصحلا يه ةيلاتلا ةوطخلا  
CA ةداهش ةمزح عم PKCS12 ةداهش وأ اتيح اهؤاشنإ مت PEM زيمرتب ةزمرم

PEM ةيوه ةداهش نإف، (هسفن CA ىلع وأ OpenSSL لالخ نم اما) ASA جراخ CSR عاشنإ مت اذا  
ةلصفنم تافلماك ةرفوتم نوكت CA ةداهش و صاخلا حاتفملا مادختساب اهزيمرت مت يتلا  
وأ p12) دحاو PKCS12 فلم يف اعم رصانعلا هذه عيمجتل ةمزاللا تاوطخلا رفوي [\(ب\) قحلملا](#)  
.pfx).

ىلإ ةيوهلا تاداهش رادصإل لاثمك GoDaddy قدصملا عجرملا مادختسا متي، دنتسملا اذه يف  
قدصملا عجرملا قئات و أرقا. نيرخآل قدصملا عجرملا يعئاب يف ةيلمعلا هذه فلتختو. ASA  
ةعباتملا لبق ةيانعب.

## GoDaddy CA ىلع SSL Certificate Generate ىلع لاثم

تاداهش ضرعأو GoDaddy باسح ىلإ لقتنا، SSL ةداهش نم يلوألا دادعإل ةلحرم و ءارشلا دعب  
ةعباتملا ل Manage رقنا. ةديج ةداهش كانه نوكت نأ بجي. SSL.



ةروصلا هذه يف حضوم وه امك CSR ريفوتل ةحفص بلجي كلذ دعب اذهو

ه. ىلإ ةداهشلا رادصإ متيس يذلا لاجملا مسا CA ددحي، هلاخدإ مت يذلا CSR ىلإ ادانتسا

ASA. ب صاخلا FQDN قباطي اذه نأ نم ققحت

## Choose website

Select a domain hosted with us

Provide a certificate signing request (CSR)

Certificate Signing Request (CSR) [Learn more](#)

```
/ypj9KO49fP5ap8al0qvLtYYcCcfwrCt+OojOrZ1YyJb3dFuMNRRedAX37t
DuHNI2EYNpYkjVk1wI53/5w3
-----END CERTIFICATE REQUEST-----
```

Domain Name (based on CSR):

**vpn.remoteasa.com**

## Domain ownership

We'll send an email with a unique code to your address on file. Follow its instructions to verify you have website or DNS control over the selected domain. [More info](#)

### AND

We can send domain ownership instructional emails to one or both of the following:

- Contacts listed in the domain's public WHOIS database record
- Email addresses: admin@[domain], administrator@[domain], hostmaster@[domain], postmaster@[domain], and webmaster@[domain]

[Hide advanced options](#)

Signature Algorithm [Learn more](#)

GoDaddy SHA-2

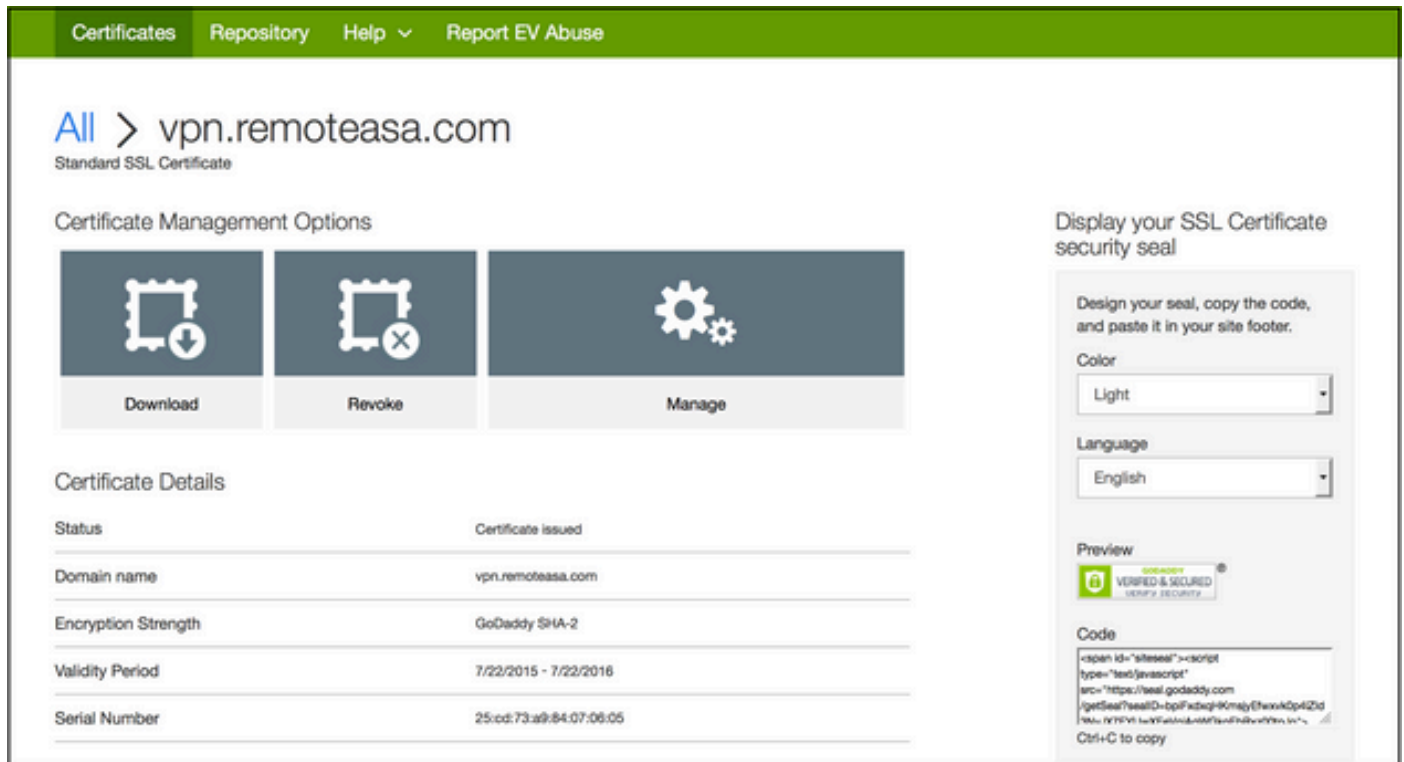
I agree to the terms and conditions of the [Subscriber Agreement](#).

✎ وأ SHA-2 ةداهشلا عي قوت ةيمزراوخ ىرخألأ CAS مظعم و GoDaddy مدختست :ةظحالم SHA-2 عي قوت ةيمزراوخ ASA معدى .ةيضارتفالا ةداهشلا عي قوت ةيمزراوخك SHA256 فرعم) كلذ دعب [8.3 دعب ام تارادصا] [8.4(1) و [8.3 لبق ام تارادصا] [8.2(5) نم أدبت يتلا مادختسا مت اذا SHA-1 عي قوت ةيمزراوخ رتخأ. (Cisco [CSCti30937](#)) نم ءاطخألأ حيحصت 8.4(1) وأ 8.2(5) نم مدقأ رادصا

ةءاهشلا راءصا لبق بلطلا نم GoDaddy ققحتي ، بلطلا لاسرا درجمب

ب.اسحلا لىل ءءاهشلا راءصاب GoDaddy موقى ، ءءاهشلا بلط ءحص نم ققحتلا ءعب

ءعباتملا ءففصلا قوف Download رقنا .ASA لىل ءببثلل ءءاهشلا لىزنن ءلذ ءعب نم ءمىو



Certificates Repository Help Report EV Abuse

All > vpn.remoteasa.com  
Standard SSL Certificate

Certificate Management Options

Download Revoke Manage

Display your SSL Certificate security seal

Design your seal, copy the code, and paste it in your site footer.

Color: Light

Language: English

Preview

Code

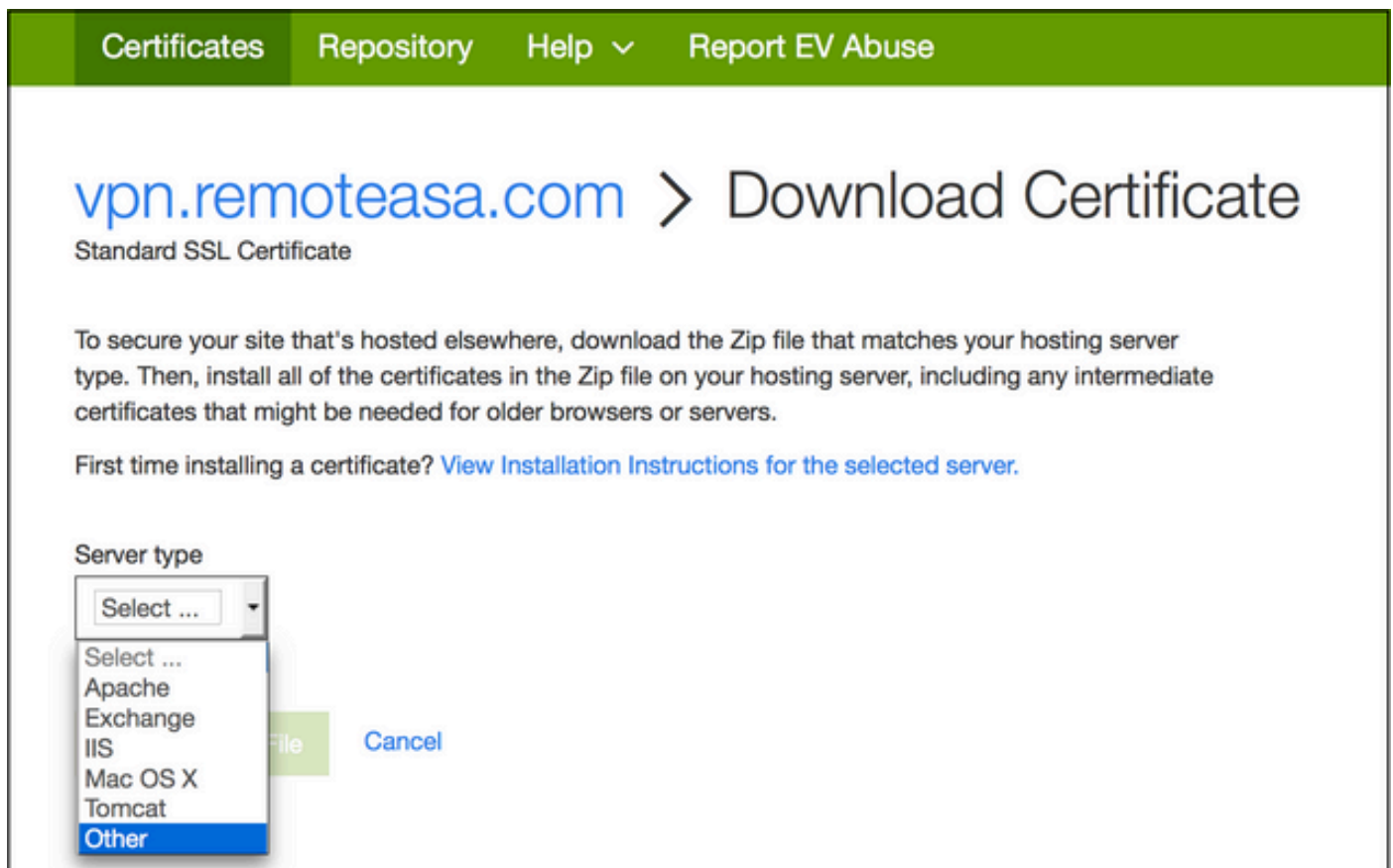
```
<script id="siteSeal" type="text/javascript" src="https://seal.godaddy.com/getSeal?sealID=bpFz2qj9KmjyE7ewkdP42Id&...>
```

Ctrl+C to copy

Certificate Details

Status	Certificate issued
Domain name	vpn.remoteasa.com
Encryption Strength	GoDaddy SHA-2
Validity Period	7/22/2015 - 7/22/2016
Serial Number	25:cd:73:a9:84:07:06:05

ءءاهشلا ل zip ءمزح لىزنن ب مقو مءاخلا ءون ء Other رءءا



Certificates Repository Help Report EV Abuse

vpn.remoteasa.com > Download Certificate  
Standard SSL Certificate

To secure your site that's hosted elsewhere, download the Zip file that matches your hosting server type. Then, install all of the certificates in the Zip file on your hosting server, including any intermediate certificates that might be needed for older browsers or servers.

First time installing a certificate? [View Installation Instructions for the selected server.](#)

Server type

Select ...

Select ...  
Apache  
Exchange  
IIS  
Mac OS X  
Tomcat  
Other

File Cancel

ةئيه ىل ع GoDaddy CA تاداهش ةلسلس تاعومجمو ةيوهلا ةداهش ىل ع zip. فلم يوتحي  
ASA. ىل ع تاداهشلا هذه تىبثت ل SSL ةداهش تىبثت ىل لقتنا. نىلصف نم crt. نىلصف نم

## ASA ىل ع SSL ةداهش تىبثت

نيتقيرطب CLI و ASDM مادختساب ASA ىل ع SSL ةداهش تىبثت نكمي

1. PEM تاقيسنت ي ف لصف نم لكشب ةيوهلا ةداهشو قدصملا عجرملا داريتسا.
2. ةيوهلا ةداهش عيجمت متي شيح (CLI ل زمرملا Base64) PKCS12 فلم داريتساب مق و. PKCS12 فلم ي ف صاخلا حاتفملا و، CA ةداهشو

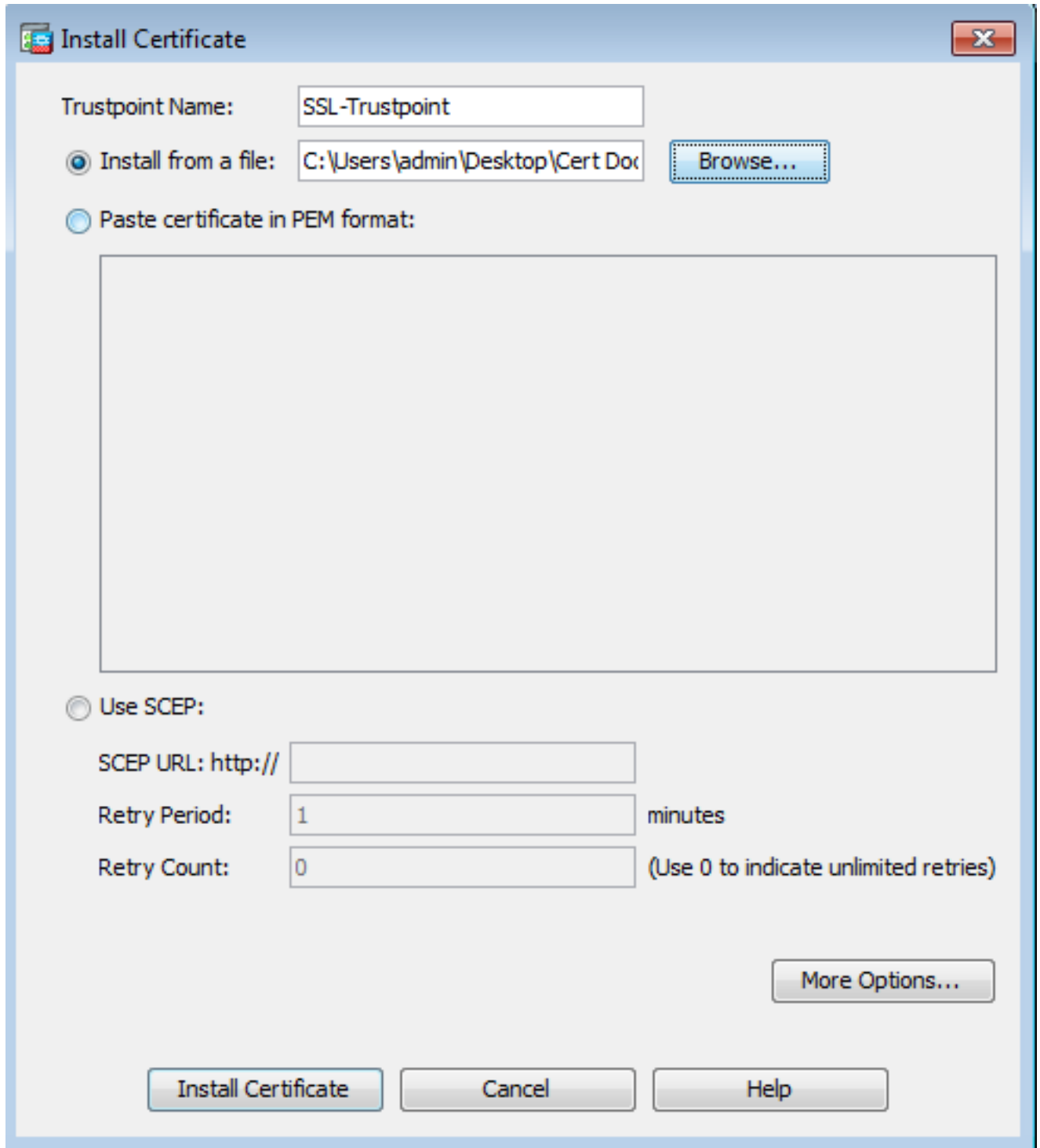


ةداهش تىبثت مق، CA تاداهش ةلسلس رفوي قدصملا عجرملا ناك اذا: ةظحالم  
مدختسملا TrustPoint ىل ع يمرهلا لسلسلا ي ف طقف ةيروفلا ةطيسولا CA  
قدصم عجرم تاداهش ي أوزجل قدصملا عجرملا ةداهش تىبثت نكمي. CSR عاشنال  
ةديجل ةقثلا طاقن ي ف ىرخأ ةطيسو

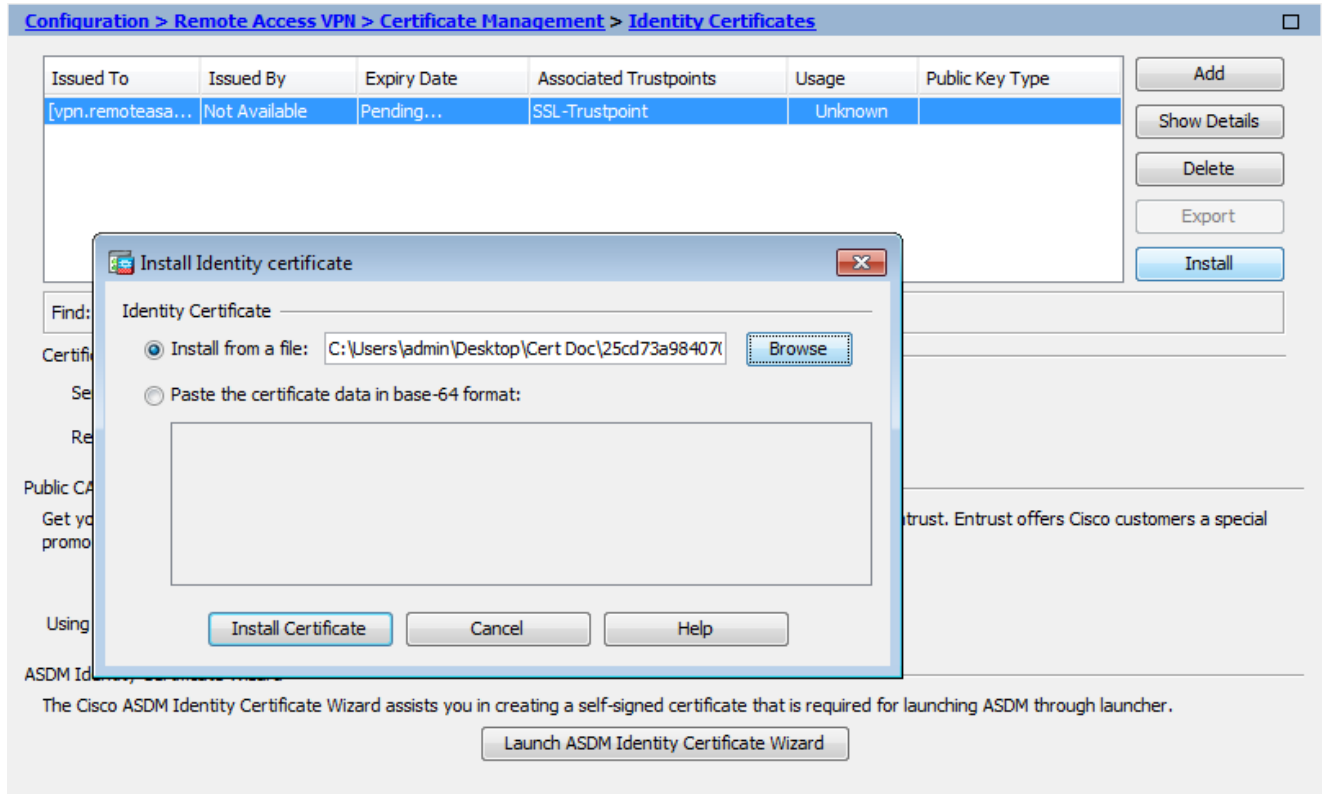
### 1.1 ASDM مادختساب PEM قيسنتب ةيوهلا ةداهش تىبثت

ةزمرم (PEM) ةيوه ةداهش رفوي قدصملا عجرملا نأ ةمدقملا تىبثتلا تاوطخ ضررت  
CA. ةداهش ةمزحو (.pem، .cer، .crt) ريفشبت

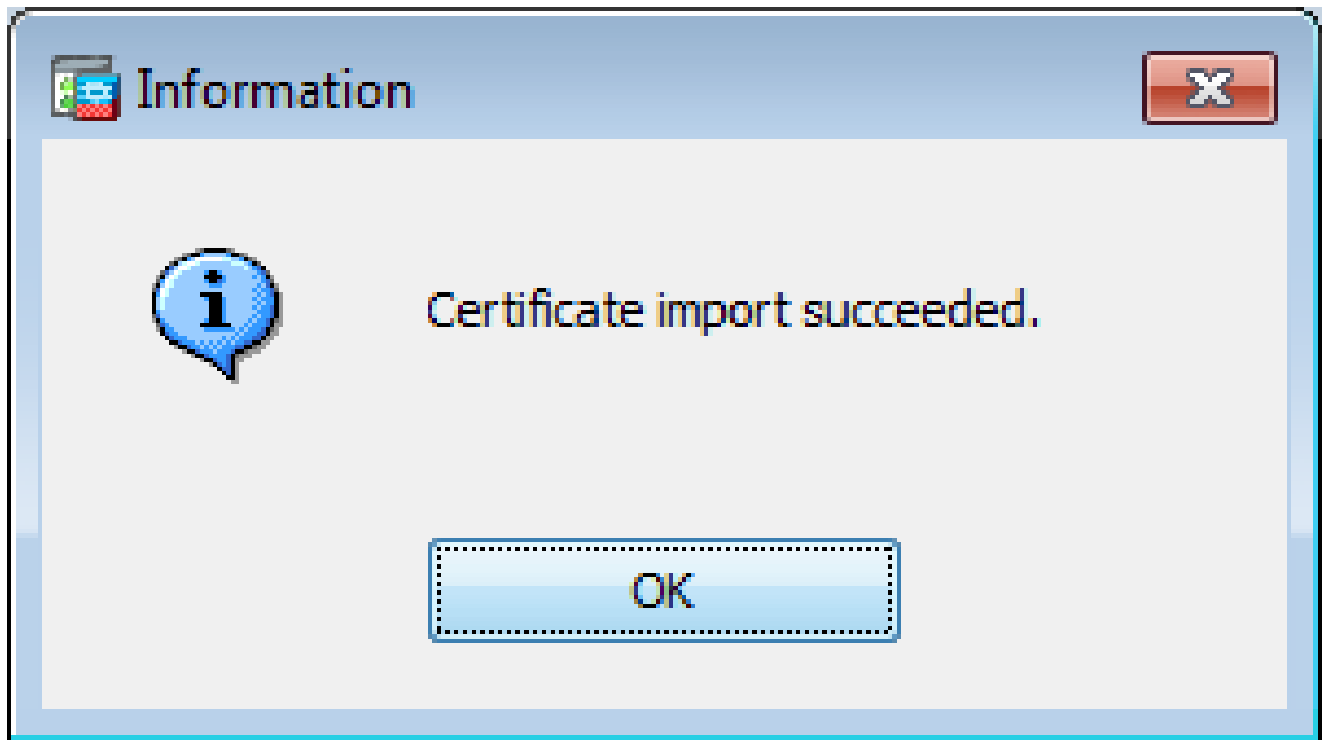
1. قدصملا عجرملا تاداهش رتخاو، Configuration > Remote Access VPN > Certificate Management ىل لقتنا.
2. 64 ةساسألا قدصملا عجرملا ةداهش قصلوخسنو يصن رحم ي ف PEM ةداهش زيمرت  
صنلا لقق ي ف ثلاثلا فرطلا عئاب اهرفوي يتلا



3. ةداهش لآ تبتت لى ع رقنا .
4. ةيوله تاداهش رتخاو ، Configuration > Remote Access VPN > Certificate Management لى لقتنا .
5. Install. رقنا . اقبس م اهأاشنم ت يتلا ةيوله ةداهش دح .
6. حتفت وأ ةزمرم لآ PEM ةيوه ةداهش راتخت و Radio Install from a file رايخ لآ رز قوف رقت نأ ام . نم ةمدقم لآ base64 ةيوه ةداهش قصل و خسنب موقت و صرن رحم يف ةزمرم لآ PEM ةداهش صن لآ لى ح يف ثلاث لآ فرط لآ دروم .



## 7. Add Certificate.



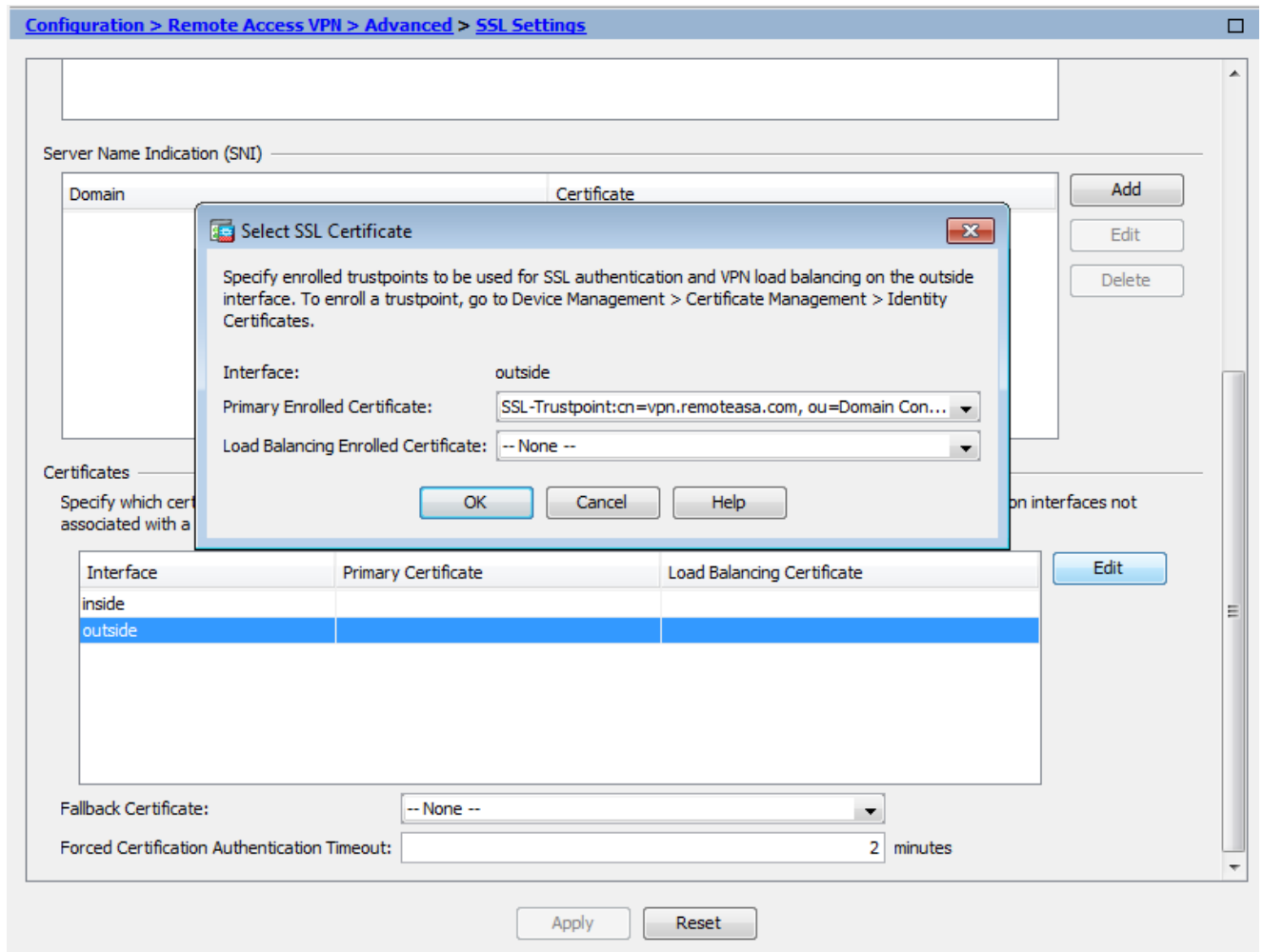
8. Configuration > Remote Access VPN > Advanced > SSL Settings.

9. اذه في WebVPN لمع تاسلج اهان ال امداد س امتي يتال هاولا دح ، تاداهش تحت اية راولا م ادخت امتي ، لالم

10. Edit.

11. اذ دح تبت م ال ادهش ل رتخ ا م صيخرت ال دس ن الم ام اقل في





12. رقنا .OK

13. رقنا .Apply متي مادي دجلا ةداهشلا مادختسا متي .  
 ةددحمل ةهجاو لا ىلع اهؤاهن

رم اوألا رطس ةهجاو عم PEM ةداهش تيبتت 1-2

<#root>

MainASA(config)#

crypto ca authenticate SSL-Trustpoint

Enter the base 64 encoded CA certificate.  
 End with the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE----- MIEADCCAuigAwIBAgIBADANBgkqhkiG9w0BAQUFADBjMQswCQYDVQQGEwJVUzEhMB8GA1UECh
```

!!! - Installing Next-level SubCA in the PKI hierarchy

!!! - Create a separate trustpoint to install the next subCA certificate (if present)  
 in the hierarchy leading up to the Root CA (including the Root CA certificate)

```
MainASA(config)#crypto ca trustpoint SSL-Trustpoint-1
MainASA(config-ca-trustpoint)#enrollment terminal
MainASA(config-ca-trustpoint)#exit
MainASA(config)#
MainASA(config)# crypto ca authenticate SSL-Trustpoint-1
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
```

-----BEGIN CERTIFICATE-----

```
MIIEFTCCA2WgAwIBAgIDG+cVMA0GCSqGSIb3DQEBCwUAMGMxCzAJBgNVBAYTA1VT
MSEwHwYDVQQKEzhUaGUgR28gRGFkZHKGR3JvdXAsIE1uYy4xMTAvBgNVBAsTKEdv
IERhZGR5IENsYXNzIDIgQ2VydG1maWNhdG1vbiBBdXR0b3JpdHkwHhcNMTQwMTAx
MDcwMDAwWhcNMzEwNTMwMDcwMDAwWjCBgZELMAkGA1UEBhMCVVMxEDA0BgNVBAGT
B0FyaXpvcmluZXRARBgNVBAClT1Njb3R0c2RhbGUxGjAYBgNVBAoTEUdvRGFkZHKu
Y29tLCBjb29tMTEwLWYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYy
dGhvcml0eSAtIEcyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3Fi
CPH6WTT3G8kYo/eASVjpIoMTpsUgQwE7hPHmhUmfJ+r2hBt0oLTbcJjHMgXBT4H
Tu70+k8vWTAi56sZvmvigaF88xZ1gD1Re+X5NbZ0TqmNghPktj+pA4P6or6KFWp/
3gvDthkUBcrqw6gE1DtGfDIN8wBmIisiNaW02jBEYt90yHGC00PoCjM7T3UYH3go+
6118yHz7sCtTpJJiaVE1BWEaRIGMLK1D1iPfrDqBmg4pxRyp6V0etp6eMAo5zvGI
gPtLXcwy7IViQyU0A1YnAZG003AqP26x6JyIAX2f1PnbU21gnb8s51iruF9G/M7E
GwM8CetJMVxpRpRgRwIDAQABo4IBFzCCARMwDwYDVR0TAQH/BAUwAwEB/zA0BgNV
HQ8BAf8EBAMCAQYwHQYDVR00BBYEFdqahQcQZyi27/a9BUFuIMGU2g/eMB8GA1Ud
IwQYMBaAFNLEsNKR1EwRcbNhyz2h/t2oatTjMDQGCCsGAQUFBwEBBCgwJjAkBggr
BgEFBQcwAYYYaHR0cDovL29jc3AuZ29kYWRkeS5jb20vMDIGA1UdHwQrMCKwJ6A1
oCOGIWh0dHA6Ly9jcmwuZ29kYWRkeS5jb20vZ2Ryb290LmNybDBGBGgNVHSAEPzA9
MDsGBFUDIAAwMzAxBggrBgEFBQcCARY1aHR0cHM6Ly9jZXJ0cy5nb2RlZGR5LmNv
bS5yZXBvc210b3J5LzANBgkqhkiG9w0BAQsFAAOCAQEAWQtTvZKGEacke+1bMc8d
H2xwxbhuvk679r6XU0Ewf7ooXGKUwU+N/f7QnaF25UcjCJYdQkMiGVn0QowCcWg
0JekxS0TP7QYpgEGRJHj2kntFo1fzq3Ms3dhP8q0CkzPN1nsoX+oYggHFCJyNwq
9kIDN0zmiN/VryTyscPzfLXs4J1et01UIDyUGAZHHFIYSaRt4bNYC8nY7NmuHDK0
KHAN4v6mF56ED71XcLNa6R+gh10773z/aQvgSM03kwwIC1TErF0UZzdsyqUvMQg3
qm5vjLyb41ddJIGv15echK1srDdMZvNhkREg5L4wn3qkKQmw4TRfZHCyQFHfjDCm
rw==
```

-----END CERTIFICATE-----

quit

```
INFO: Certificate has the following attributes:
Fingerprint:      81528b89 e165204a 75ad85e8 c388cd68
Do you accept this certificate? [yes/no]: yes
```

Trustpoint 'SSL-Trustpoint-1' is a subordinate CA and holds a non self-signed certificate.

Trustpoint CA certificate accepted.

```
% Certificate successfully imported
BGL-G-17-ASA5500-8(config)#
```

!!! - Similarly create additional trustpoints (of the name "SSL-Trustpoint-n", where n is number thats incremented for every level in the PKI hierarchy) to import the CA certificates leading up to the Root CA certificate.

!!! - Importing identity certificate (import it in the first trustpoint that was created namely "SSL-Trustpoint")

```
MainASA(config)#
```

```
crypto ca import SSL-Trustpoint certificate
```

WARNING: The certificate enrollment is configured with an fqdn that differs from the system fqdn. If th  
yes

% The fully-qualified domain name in the certificate will be:

```
(asa.remotevpn.url)
```

Enter the base 64 encoded certificate. End with the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----  
MIIFRjCCBC6gAwIBAgIIJc1zqYQHbGwUwDQYJKoZIhvcNAQELBQAwgQxCzAJBgNV  
BAYTA1VTMRAwDgYDVoQIEwdBcm16b25hMRRMwEQYDVoQHEwpTY290dHNkYWx1MRoW  
GAYDVQQKExFhb0RHZGR5LmNvbSw5jLjEtMCSGA1UECXMkaHR0cDovL2N1cnRz  
LmdvZGFkZHUy29tL3JlCG9zaXRvcnkVMTMwMQYDVoQDEypHbyBEYWRkeSBTZWN1  
cmUgQ2VydG1maWNhdGUGQXV0aG9yaXR5IC0gRzIwHhcNMTUwNzIyMTIwNDM4WhcN  
MTYwNzIyMTIwNDM4WjA/MSEwHwYDVoQLEXhEb21haW4gQ29udHJvbCBWYXpZGF0  
ZWQxGjAYBgNVBAMTEXzWbi5yZW1vdGVhc2EuY29tMIIBIjANBgkqhkiG9w0BAQEF  
AAOCAQ8AMIIIBCgKCAQEArY2Fv2S2Uq5HdDh0aSzK5Eyok2tv2Rem8DofbTQ+4F9  
C9IXitWdLAo6a7dzyfB4S9hx1VZxoHMGGNd6i9NWLXswU1Nx5pRMaKR4h1cL6bDW  
ITt5GzKdL93ibMxYmau+uwM30kBB8QxLNNxr4G+oXtfavctTxWy/o6LzKWfyj0XP  
tta9FZW07c0MNVkiUL1v9WBcy4GK1xyvN9RtWebtVkm5/iOv0ReBTBFFxCJ1YQAG  
UWteu1ikWAGj1qomZGnZgAFDWJ4/hxjesG2BGMtwX5L108cbmbi/u/vnmZ5Xhix  
<snip>  
CCsGAQUBwIBFitodHRwOi8vY2VydG1maWNhdGVzLmdvZGFkZHUy29tL3JlCG9z  
aXRvcnkVMHYGCCsGAQUBwEBBGowaDAKBggrBgEFBQcwAYYYaHR0cDovL29jc3Au  
Z29kYWRkeS5jb20vMEAGCCsGAQUBzAChjRodHRwOi8vY2VydG1maWNhdGVzLmdv  
ZGFkZHUy29tL3JlCG9zaXRvcnkVZ2RpZzIuY3J0MB8GA1UdIwQYMBaAFEDCvSe0  
zDSDMKIz1/tss/COLIDOMEYGA1UdEQQ/MD2CEXZwbi5yZW1vdGVhc2EuY29tghV3  
d3cudnBuLnJlbW90ZWZzYS5jb22CEXZwbi5yZW1vdGVhc2EuY29tMB0GA1UdDgQW  
BBT7en7YS3PH+s4z+wTR1pHr2tSzejANBgkqhkiG9w0BAQsFAAOCAQEAO9H8TLN  
x2Y0rYdI6gS8n4imaSYg9Ni/9Nb6mote3J2LELG9HY9m/zUCR5yVkra9azdrNUAN  
1hJBJ7kKQScLC4sZLONdqG1uTP5rbWR0yikF5wSzyMwd03kOR+vM8q6T57vRst5  
69vzBUUJc5bSu1IjyfPP19z1l+B2eBwUFbVfXLnd9bTfiG9mSmC+4V63TXFxt10q  
xkGNys3GgYuCUy6yRP2cAUV1lc2tYtaxoCL8yo72YUDDgZ3a4Py01EvC1F0aUtgv  
6QNEOYwmbJkyumdPUwko6wGOCOWLumzv5gHnhil68HYSZ/4XI1p3B9Y8yfg5pwb  
7pukahH+xgQRdg==  
-----END CERTIFICATE-----
```

```
quit
```

```
INFO: Certificate successfully imported
```

```
! Apply the newly installed SSL certificate to the interface accepting SSL connections
```

```
MainASA(config)#
```

```
ssl trust-point SSL-Trustpoint outside
```

## 2-1 عدهاش تېبثت PKCS12 عم ASDM

ءاشن دنع وأ لدب فرح ءدهاش ءلاح لثم، ASA ىلع CSR ءاشن اءهف مءى ال ىتلا ءالءال ىف  
PKCS12 فلم وأ ءلصفنم ءافلماك صاءال ءافلم عم ءهوه ءدهاش ىقلت مءى، UC ءدهاش  
ءهءال ءاوطءال لمكأ، ءاداءشال نم ءونلا اءه ءهءبءءل (PFX قىسنت وأ p12). عمءم ءءاو

1. [قءلمءل](#) رفوى. ءءاو PKCS12 فلم ىف صاءال ءافلمءاو CA ءدهاش عمءء، ءهوهءا ءدهاش ن. ا  
ءق قءصمءا ءءرمءا ءءاك اءا. OpenSSL مءءءسءاب كلءب مءى قءلل ءمءالءا ءاوطءال (ب)

ة.لالتل ةوطخلال لىل لقتناف ،لعللاب اهتدوز

2. Identity Certificates رتخاو، Configuration > Remote Access VPN > Certificate Management لىل لقتنا.
3. رقنا .Add
4. TrustPoint مسا ددح .
5. رز رقنا Import the identity certificate from a file لرايخ.
6. لخدأ PKCS12 فلم ددحو حفتت PKCS12 فلم عاشنال ةمدختسملا رورملا ةرابع لخدأ .  
ةداهشلا رورم ةرابع

**Add Identity Certificate**

Trustpoint Name:

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:

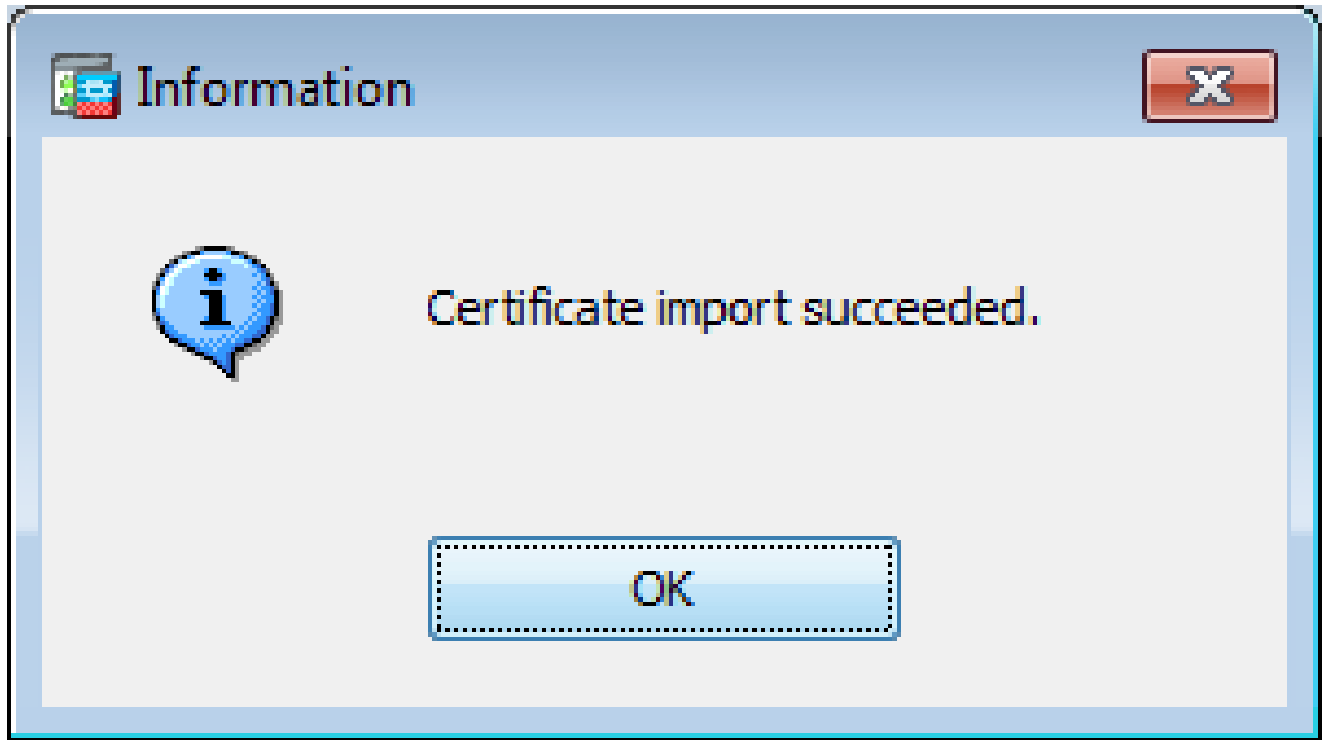
Certificate Subject DN:

Generate self-signed certificate

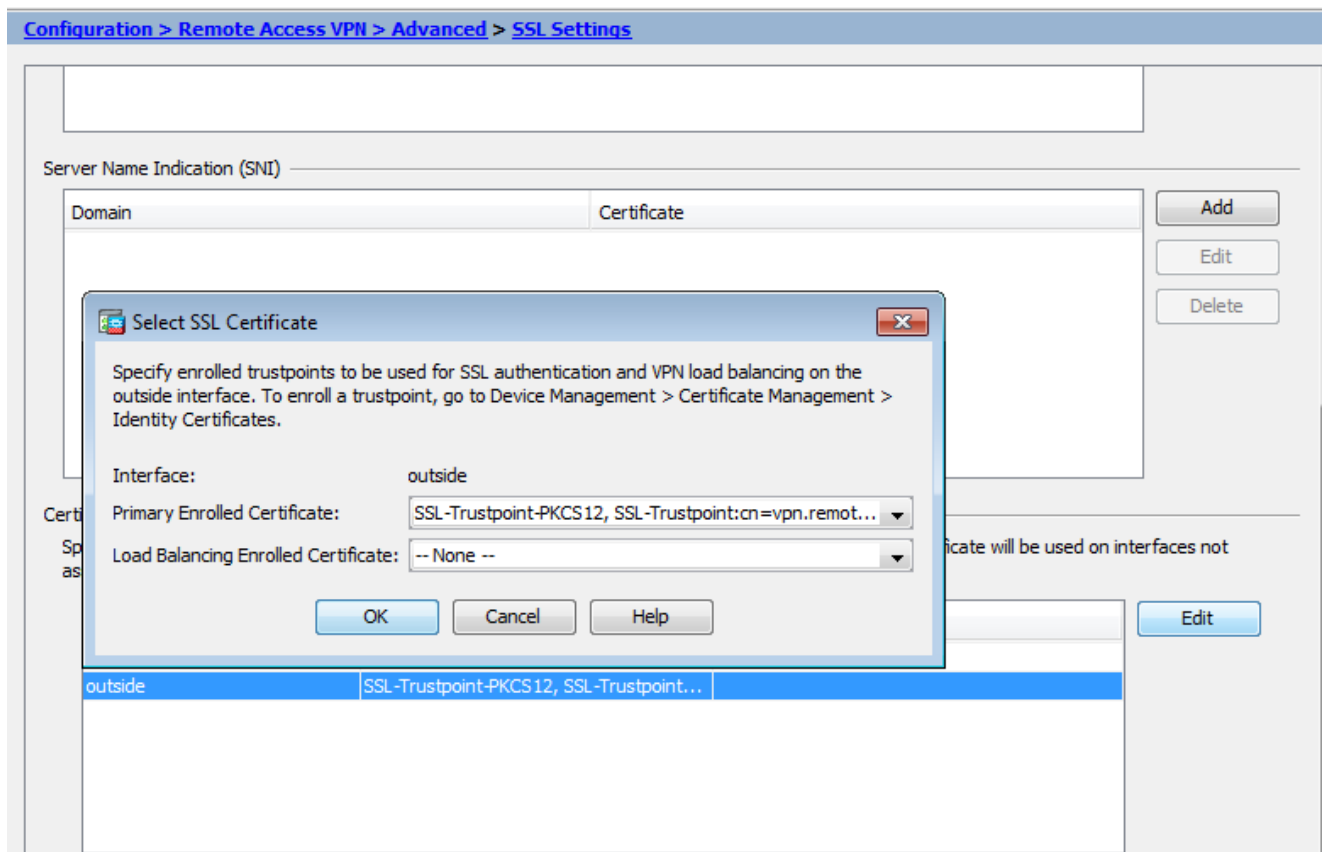
Act as local certificate authority and issue dynamic certificates to TLS-Proxy

Enable CA flag in basic constraints extension

7. ةداهش ةفاضلا لىل رقنا .



8. SSL Settings رتخ او، Configuration > Remote Access VPN > Advanced لي لقتنا.
9. اذه في WebVPN لمع تاسلج اهان ال امداختسا متي يتل ا هجاولا رتخا، تاداهش تحت ل اثلما.
10. Edit رقنا.
11. اثلما تبتلما ادهاشلا رتخا، صيخرت ا لدسنملا عمئاقلا في.



12. OK رقنا.

متمني يتل WebVPN لمع تاسلج عي مجل نأل اةدي دجل اةداهش ل امدختس ا متي Apply. رقنا 13.  
ةودح حملا ةه جاول ا ل ع اهؤاهن ا

رم اوأل رطس ةه ج او عم PKCS12 ةداهش تيبثت 2-2

```
<#root>
```

```
MainASA(config)#
```

```
crypto ca trustpoint SSL-Trustpoint-PKCS12
```

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

```
enrollment terminal
```

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

```
exit
```

```
MainASA(config)#
```

```
crypto ca import SSL-Trustpoint-PKCS12 pkcs12 cisco123
```

Enter the base 64 encoded pkcs12.

End with the word "quit" on a line by itself:

```
-----BEGIN PKCS12-----
```

```
MIISNwIBAzcCEfEGCSqGSIB3DQEHAaCCEeIEghHeMIIR2jCCEdYGCSqGSIB3DQEH  
BqCCEccwghHDAgEAMIIRvAYJKoZIhvcNAQcBMBsGCiqGSIB3DQEAMAQMwDQWIW03D  
hDtI/uECAQGAghGQ9ospee/qtIbVZh2T8/Z+5dxRPBcStDTqyKy7q3+9ram5AZdG  
Ce9n5UCckqT4WcTjs7XZtCrUrt/LkNbmGDVhwGBmYWi0S7npgaUq0eoqiJRK+Yc7  
LN0nbho6I5WfL56/JiceAM1XDLr/IqqLg2QAAPGdN+F5vANsHse2GsAATewBDLt7  
Jy+SKfoNvvIw9QvzCiUzMjYZBANmBdMCQ13H+YQTHitT3vn2/iCD1zRSuXcqypEV  
q5e3hei00751E8TDLWm03PMvWIZqi8yzWesjcTt1Kd4FoJBZpB70/v9LntoIUOY7  
kIQM8fHb4ga8BYfbgRmG6mkMm01STtbSv1vTa19WTmdQdTycCa+G5PkrRyRsy3Ww1  
1kGFMhImmrnNADF7Hmzbys1VohQZ7h09iVQY9krJogoXHjmQYxG9brf0oEwxSJD  
mGDhEhSh+s/WuFSV9Z9kiTXpJNZxpTASoWBQrrwm05v8ZwbjbnVNJ7svdbwpU16d+  
NNFGR7LTq08hpupeeJnY9eJc2yYqAXWXQ5kL0Zo6/gBEdGtEaZBgCFK9JZ3b13A  
xqxGifanWpNLyG611NkUNjTgbjhnEEYI2uZzU0qxn1Ka8zyXw+1zrKuJscDbkAPZ  
wKtw8K+p40zXVHhuANo6MDvffNRY1KQDtyK1inoPH5ksVSE5awkVam4+HTcqEUfa  
16LMana+4QRgSetJhU0LtsMaQFRJGkha4JLq2t+JrCAPz2osAR1TsB0jQBNq6YNj  
0uB+gGk2G18Q5N1n6K1fz0XBFLWEDBLsaBR05MANE7wWt00+4awGYqVdmIF11kf  
XIRKAiQEr1pZ6BVPuvsCNJxaaUHzufhYI2ZAckasKBZOT8/7YK3fnAaGoBCz4cHa  
o2EEQhq2aYb6YTv0+wtLEWGHZsbGZEM/u54XmsXAI7g28LGJYdfWi509KyV+Ac1V  
KzHqXZMM2BbUQCNCtF5JIMiW+r62k42FdahfaQb0vJsIe/IwkAKG7y6DIQFs0hwg  
Z1PXiDbNr1k4e8L4gqumMKWg853PY+oY22rLDC7bu11CKtixIYBCvbn7dAYsI4GQ  
16xXhNu3+iye0HgbUQCfTU/mBrA0Z0+bpKjwOCfqNBuYnZ6kUEdCI7GFLH9QqtM  
K7YinFLoHwTwi3MsmqVv+Z4ttVWv7Xmiko02nMynJMP6/CNV80MxMKdC2qm+c1j  
s4Q1KcAmFsQmNp/7SIP1wnv0c6JbUmC10520U/r8ftTzn8C7WL62W79cLK4H0r7J  
sNsZn0z0JOZ/xdZT+cLTctVevKJQQMK3vMsiOuy52FkuF3HnfrmBqDkBR7yZxELG  
RCELOEDdbp8VP0+IhN1yz1q7975ScdxFSL0TvjnHGFwd14ndoqN+bLhWbdPjQWV  
13W2NCI95tmHDLGgp3P001S+rjdCEGGMg+9cpgBfFC1JocuTDIEcUbJBY8QRUNiS  
/ubyUagdzUKt1ecfb9hMLP65ZnQ93VIw/NJKbIm7b4P/1Zp/1FP5eq7LkQPaxE4/  
bQ4mHcnwrs+JGFkN19B8hJmmGoowH3p4IEvwZy7CThB3E1ejw5R4enqmrghqPqE  
B7odN10FLAhd01G5BsHExluneSEb40Q0pmKXiDDB5B001bJsR748fZ6L/LGx8A13  
<snip>
```

```
ijDqxyfQXY4zSyt1jSMwMtYA9hG5I79Sg7pnME1E9xq1D0oRGg8vgxlwicikLxp  
LL0ReDY31KRYv00vW0gf+tE71ST/3TKZvh0sQ/BE0V3kHnw1dejMFH+dvYAA9Y1E  
c80+tdafBFX4B/HP46E6heP6ZSt0xAfRW1/JF41jNvUNV09vtVfR2FTyWpzZFY8A  
GG5XPIA80WF6wKEPFHICn8scY+Vot8kXxG96hwt2Cm5NQ20nVzxUZQbpKsjs/2jC
```

3HVFe3UJFBsY9UxTLcPXyBSIG+VeqkI8hWZp6c1TFNDLY2ELDy1Qzp1mBg2FujZa  
YuE0avjCJzBzZUG2umtS5mHQnwPF+Xk0UjEyhGMauhGxHp4nghSzrUZrBeuL91UF  
2mbpsOcgZkzxMS/rjdNXjCmPF1oRBvKkZS1xHFRE/5ZopAhn4i7YtHQNrZ9U4RjQ  
xo9cUuaJ+LNmvzE8Yg3epAMYZ16UNGQQkVQ6ME4BcjRONzW8BYgTq4+pmT1ZNq1P  
X87CXCPtYrPHF57eSo+tHDINCgfqYXD6e/7r2ngfiCeUeNDZ4aV12XxvZDaU1BPP  
Tx5fMARqx/Z8BdDyBJDVBjdsxmQau9HLkhPvdFG1ZIwdTe13CzKqXA5Pmpjt4q9  
GnCpC53m76x9Su4ZDw6aUdBcgCTMvfaqJC9gz0bee2Wz+aRRwzSxu6tEWVZo1PEM  
v0AA7po3vPek1g0nLRAwEoTTn4SdgNLWeRoxqZgkw1FC1GrotxF1so7uA+z0aMeU  
1w73reonsNdZvRAcVX3Y6UNFDyt70Ixvo1H4VLzWmOK/oP62C9/eqqMwZ8zoCMPt  
ENna7T+70s66SCbMmXCHwyh00tygNKZFFw/AATFyjQPMWPAxGuPN0rnB6uYcN0Hk  
1BU7tF143RNIzaQqEH3XnaPvUuAA4C0FCoE3h+/tVjtfNKDvFmb6ZLZHYQmUYpyS  
uhdFEpoDrJH1VmI2tik/iqYwaz+oDqXPHQXnJhw25h9ombR4qnd+FCfwFCGtPFON  
o3Qffz53C95n5jPHVMYUr0xDdpwnvzCQPdj6yQm564TwLAmiz7uD1pqJZJe5QxHD  
no1v+4MdGSFvtBq+ykFoVcaamqeaq6sKgvAVujLXXEs4KEmIgcPqATVRG49E1ndI  
L01DEQyKhVoDGebAuVRBjzwAm/qxWxxFv3hrbCjPHCwEYms4Wgt/vKKRFsuWJNZf  
efH1dw11tkd5dKwSvDocPT/7mSLtLJa94c6AfgxYy9z0+FTLDQwzXga7xC2krAN1  
yHxR2KHN5YeRL+KDzu+u6dYoKaz+YAgw1W6KbeavALSuH4EYqcvG8hUEhp/ySiSc  
RDhuygxEovIMGfES4FP5V521PyDhM3Dqwhn0vuYUmYnX8EXURkay44iwwI5HhqYJ  
1ptWYyO8Bdr4Wnwt5xqsZgYR6mmGeAIin7bDunsF1uBHWYF4dyK1z1tsdRNMqQ  
+W5q+QjVdrj1dwv/bMF0aqEjxeNwBRqjzccff3BxMnwVxtgqxFvRh+DZxiJoiBG+  
yx7x8np2AQ1r0METSSxbnZzfNkZKvBVMkIC6Jsm2WEVTQvoFJ8em+nem0WgTi/  
hHSBzjE7RhAucnHuiFOCX0gvR1SDDqyCQbduc1QjXN0svA8Fqbea9WEH5khOPv3  
pbtsL4gsf12pv8diBQkVQgiZDi8Wb++7PR6ttiY65kVwrdsoN11/qq+xW0d3tB4/  
zoH9LEMgTy9Ssz7myWrB9E00Z8BIjL1M8oMigEYrTD0c3KbyW1S9dd7QAxIU0BaX1  
8J8q10ydvTBzmqcjesFH4/1NHn5Vnf0ZnNpui4uHP0XBG+K2zJUJXm6dq1AHB1E  
KQFsFzPNNyave0Kk8JzQnLAPd70UU/Iksy0CGQozGBH+HSzVp1RDjrrbC342rkBj  
wnI+j+/1JdwBmHdJMZCfoMZFLSI9ZBqFirdii1/NRu6jh76TQor5TnNjxIyNREJC  
FE5FZnMFvhM900LaiUZff8WWCOferDMttLXb1nuxPF1+1Rk+LN1PLVptWgcxzfSr  
JXrGiWjxybBB9oCOrAcq8fGAtEs8WRxJyDH3Jjmn9i/G16J1mMcuF//LxAH2WQx8  
Ld/qS50M2iFCffDQjxAj0K6DEN5pUebBv1Em5SOHXvyq5nxgUh4/y84CwaKjwOMQ  
5tbbLM1nc7ALIj9LxZ97YiXSTyeM6oBxBFx6Rpk1kDv05m1BghSpVQiMcQ2ORikh  
UVVNBsh019S3cb5wqxaWqAKBqb4h1uLGVbYWZf2mzLZ8U5U5ioiqoMBqNZbzTXp0  
EqEFuatT11QvCRbcKS3xou4MAixcYUxKwEhbZA/6hd10XSBjwe7jKBV9M6w1iKab  
UfoJCGTaf3sY681qrMPrbt0eewf1C02Sd9Mn+V/jvni17mxYFFUpruRq3r1LeqP  
J5camfTtHwyL8N3Q/Zwp+zQeWziLA8a/iAVu/hYLR1bpF2WCK010tJqkvVmrLVLz  
maZZjbJe0ft5cP/1RxbK1S6Gd5dFEKDE15c6gWUX8RKZP6Q7iaE5hnGmQjm8Lj1  
kXwF+ivox0Q8a+Gg1bVTR0c7tqW9e9/ewisV1mwvEB6Ny7TDS1oPUDHM84pY6dqi  
1+0io07Ked4BySwN1Yy9yaJtBTZSCstfP+ApLiDn7pSBvvXf1aHmeNbkPOZJ+c+t  
fGpUdL6V2UTXfCsOPHTC0ezA15sOHwCuPchrDIj/eGUwMS3NfS25XgcMuvnLqGVO  
RzcrZ1ZiG8G0oLYwOCuzoY0D/m901001ahePyA9tmVB7HRRbytLdaW7gYeikoCv  
7qtBqJFF17ntWJ3EpQHZUCVClbHIKqjNqRbDCY7so4A1IW7kSEUGWMIUDhprE8Ks  
NpvnPH2i9JrYrTeRoYUI0tL/7SATd2P0a21xz/zUwekeqd0bmVCsAgQNbB2XkrR3  
XS0B52o1+63e8KDqS2zL2TZd3daDFidH1B8QB26tFb0Aca0bJH5/dWP8ddo8UYo  
Y3JqT10malxSjhaMhMqDZIqP49utW3TcjgG11YS4HEmcqtHud0ShaUysC6239j1Q  
K1FwrwXT1BC5vnq5IcOMqx5zyNbfXz28969cwoMcyU6+kRw0TyF6kF7EEv6XWca  
XLEwABx+tKRUKHJ673SyDMu96KMV3yZN+RtKbCjqCPVTP/3ZeIp7nCMUcj5sw9HI  
N34yeI/ORCLyeGs0EiBLkucikC32LI9ik5HvImVTELQ0Uz3ceFqU/PkasjJUve6S  
/n/1ZVUHbUk71xKR2bWZgEC17fIe17w1rbjP3Wbk+Er0kfYcsNRHxeTDPKpSt9s  
u/UsyQJiyNARG4X3iyQ1sTce/06Ycyri6GcLHAu58B02nj4Cxo1Cp1ABZ2N79HtN  
/7Kh5L0pS9MwsDCHUUI8KFRtSET7TB1tIU99FdB19L64s1/shYAHbccvVWU50WhT  
PdLoaErrX81Tof41IxbSZbI8grUC4KfG2sdPLJKu3HVTeQ8Lfl1bBLxfs8ZBS+Oc  
v8rH1Q012kY6LsFGLehj+/yJ/uvXORiv0Esp4EhFpFfkp+o+YcFeLUUPd+jzb62K  
HfSCCbLpKyEay80dyWkHfgy1qXmb9ud0oM050aFJyqRONjnt6pcxBRy2A6AJR5S  
IIC26YNwbh0GjF9qL2FiUqnNH/7GTqPnd2qmsB6FTIwSBT6d854qN7PRt+ZXgdtQ  
Ojcyt1r9qpWZpNFK8EzizwKiAYtsiEh2pzPt6YUkpsRb6CXTkIzoG+Klsv2m3b8  
OHyZ9a8z81/gnxrZ11s5SCTf0SU70pHWh8VAYKVHhK+MwGqR0m/2ocV32dkRBLMy  
2R6P4WfHyI/+9de1x3PtIu0iv2knpXhv2fKM6sQw45F7XkmwHxjq1YRJ6vIwPTAh  
MAKGBSs0AwIaBQAeffTRETzpiSHKZR+Kmen68VrTwpV7BBSQi0IesQ4n4E/bSVsd  
qJSzcwh0hgICBAA=  
-----END PKCS12-----

quit

INFO: Import PKCS12 operation completed successfully

!!! Link the SSL trustpoint to the appropriate interface  
MainASA(config)#

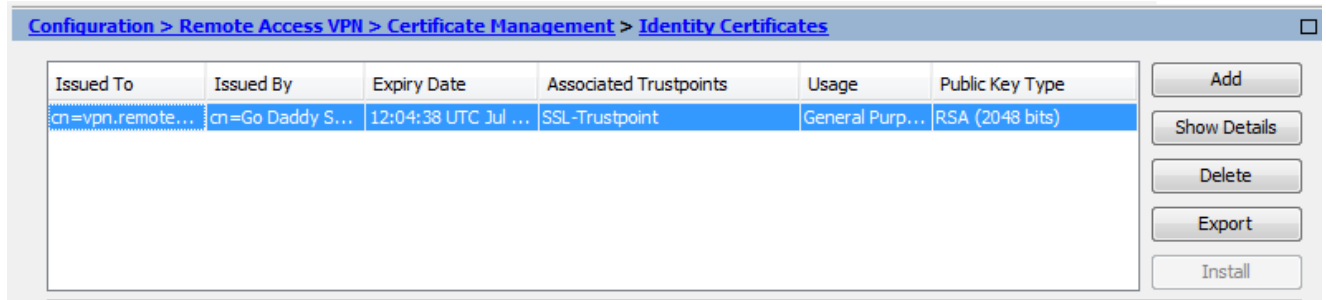
```
ssl trust-point SSL-Trustpoint-PKCS12 outside
```

## تحصيل نم ققحتلا

اهم ادختساو ةي جراخا لة هجلا دروم ةداهش ل حج انلا تي بثتلا نم ققحتلا تاوطلخا ل هذو مدختسا SSLVPN تالاصتال

## ASDM ربع ةت بثملا تاداهش ل ضرع

1. Identity Certificates رتخأ م ث ل، Configuration > Remote Access VPN > Certificate Management ل قنتنا.
2. ثلا ثلا فرطلا دروم نع ةرداصلا ةي وهلا ةداهش رهظت.



## رم اوألا رطس ةهجاو ربع ةت بثملا تاداهش ل ضرع

<#root>

```
MainASA(config)#
```

```
show crypto ca certificate
```

### Certificate

```
Status: Available
Certificate Serial Number: 25cd73a984070605
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA256 with RSA Encryption
Issuer Name:
  cn=Go Daddy Secure Certificate Authority - G2
  ou=http://certs.godaddy.com/repository/
  o=GoDaddy.com\, Inc.
  l=Scottsdale
  st=Arizona
  c=US
Subject Name:
  cn=(asa.remotevpn.url)
  ou=Domain Control Validated
```



OCSP AIA:

URL: <http://ocsp.godaddy.com/>

CRL Distribution Points:

[1] <http://crl.godaddy.com/gdig2s1-96.crl>

Validity Date:

start date: 12:04:38 UTC Jul 22 2015

end date: 12:04:38 UTC Jul 22 2016

Associated Trustpoints:

**SSL-Trustpoint**

**CA Certificate**

Status: Available

Certificate Serial Number: 07

Certificate Usage: General Purpose

Public Key Type: RSA (2048 bits)

Signature Algorithm: SHA256 with RSA Encryption

Issuer Name:

cn=Go Daddy Root Certificate Authority - G2

o=GoDaddy.com\, Inc.

l=Scottsdale

st=Arizona

c=US

Subject Name:

cn=Go Daddy Secure Certificate Authority - G2

ou=<http://certs.godaddy.com/repository/>

o=GoDaddy.com\, Inc.

l=Scottsdale

st=Arizona

c=US

OCSP AIA:

URL: <http://ocsp.godaddy.com/>

CRL Distribution Points:

[1] <http://crl.godaddy.com/gdroot-g2.crl>

Validity Date:

start date: 07:00:00 UTC May 3 2011

end date: 07:00:00 UTC May 3 2031

Associated Trustpoints:

**SSL-Trustpoint**

**CA Certificate**

Status: Available

Certificate Serial Number: 1be715

Certificate Usage: General Purpose

Public Key Type: RSA (2048 bits)

Signature Algorithm: SHA256 with RSA Encryption

Issuer Name:

ou=Go Daddy Class 2 Certification Authority

o=The Go Daddy Group\, Inc.

c=US

Subject Name:

cn=Go Daddy Root Certificate Authority - G2

o=GoDaddy.com\, Inc.

l=Scottsdale

st=Arizona

c=US  
OCSP AIA:  
URL: http://ocsp.godaddy.com/  
CRL Distribution Points:  
[1] http://crl.godaddy.com/gdroot.crl  
Validity Date:  
start date: 07:00:00 UTC Jan 1 2014  
end date: 07:00:00 UTC May 30 2031  
Associated Trustpoints:

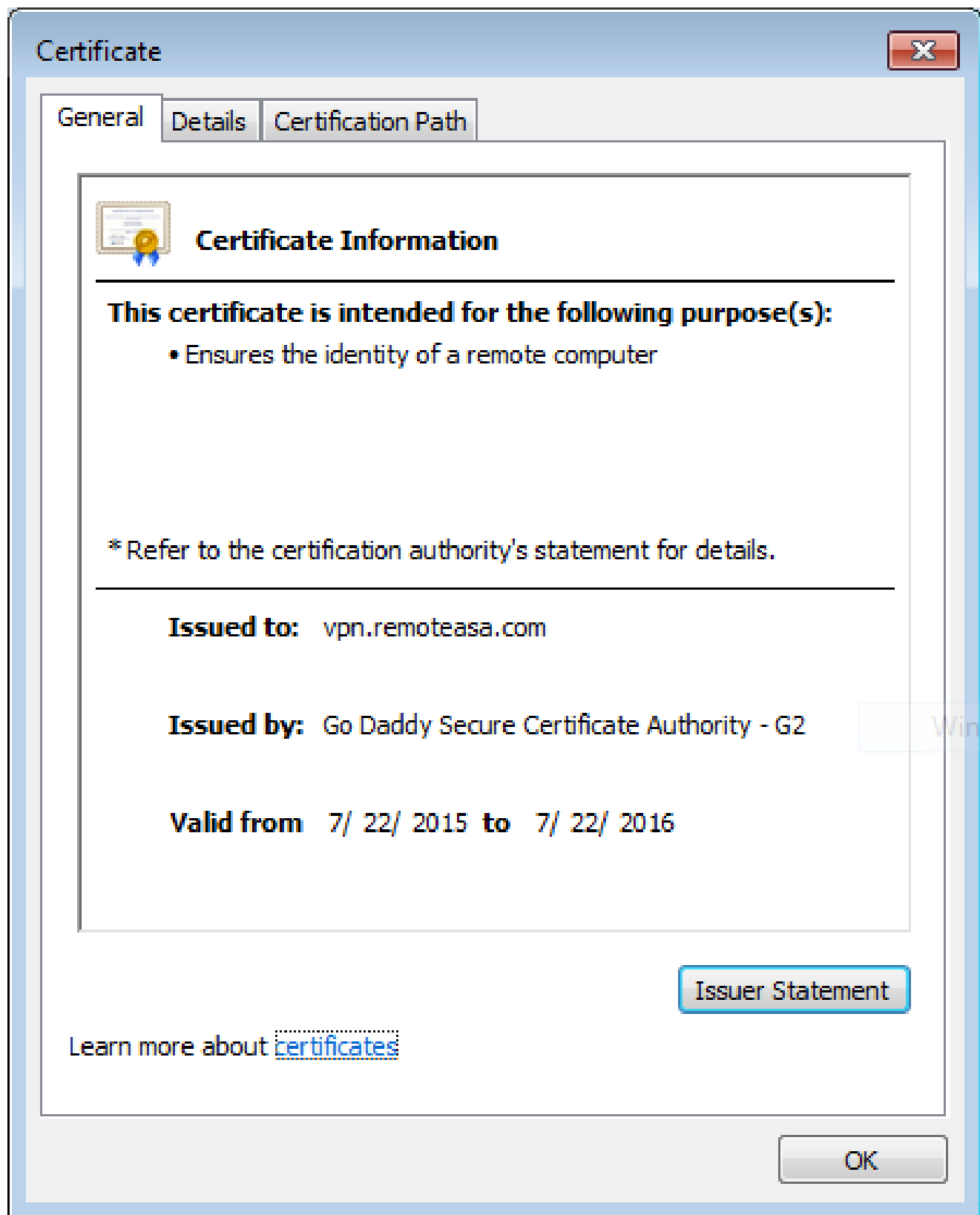
SSL-Trustpoint-1

...(and the rest of the Sub CA certificates till the Root CA)

بېو ضرعت س م م ادخت س اب WebVPN ل ءداهش ل ا تي ب ث ت ن م ق ق ح ت ل ا

ءدي د ج ل ا ءداهش ل ل WebVPN م ادخت س ا ن م ق ق ح ت

1. م دخت س م ل ا FQDN عم https:// م دخت س ا . بېو ضرعت س م ل ل ا خ ن م WebVPN ءه ج ا و ب ل ل اص ت ا ل ا .  
ل ا ث م ل ا ل ي ب س ي ل ع ) ءداهش ل ل ب ل ط ل ([https://\(vpn.remoteasa.com\)](https://vpn.remoteasa.com)).
2. ء ح ف ص ن م ن م ا ل ا ي ل ف س ل ل ن ك ر ل ا ي ف ر ه ط ت ي ت ل ل ل ف ق ل ل ء ن و ق ي ا ي ل ع ا ج و د ز م ا ر ق ن ر ق ن ا .  
ء ت ب ث م ل ا ءداهش ل ل ا م و ل ع م ر ه ط ت ن ا ب ج ي . WebVPN ي ل ل ل و خ د ل ل ل ي ج س ت
3. ء ي ج ر ا خ ل ل ا ءه ج ل ا دروم ل ب ق ن م ء ر د ا ص ل ل ا ءداهش ل ل ا ه ت ق ب ا ط م ن م ق ق ح ت ل ل ا ت ا ي و ت ح م ل ا ع ج ا ر .



## ASA یلج SSL ةداهش ديدجت

1. قدصملا عجرملا یلج و OpenSSL مادختساب و ASA یلج اما CSR ءاشنإ ةداعإب مق .  
CSR [ءاشنإ](#) یف ةدجمل تاوطخل لمكأ . ةمیدقلا ةداهشلا تامس سفنب
2. عم PEM ( .pem ، .cer ، .crt ) قيسنتب ةديج ةيوه ةداهش ءاشنإب مق و CA یلج CSR لسراً .  
ديج صاخحاتفم اضيأ دجوي ، PKCS12 ةداهش ةلاح یفو . CA ةداهش

هؤاشنإ م ت ديدج CSR مادختساب ةداهشلا نيوكت ةداعإ نكمي GoDaddy CA ةلأح يف.  
SSL تاداهش نمض ةرادإ قوف رقن او GoDaddyaccount ىلإ لقتنا

Accounts	Expiration date	
vpn.remoteasa.com Standard SSL	22-07-2016	Options Manage

Displaying 1-1 of 1 accounts Results per page: 5 1 of 1

Need help with your SSL Certificates? Visit [GoDaddy Support](#)  
Need More SSL Certificates? [Buy Additional Plans](#)

بولطملا لاجملا مسال ةلأحلا ضرع قوف رقنا

Certificates Repository Help Report EV Abuse

Certificates

Search domains All Certificate Types All Statuses Not Expired or Revoked Action

vpn.remoteasa.com	1 Year Standard SSL Certificate	Certificate issued	7/22/2016	View status
-------------------	---------------------------------	--------------------	-----------	-------------

ةداهشلا حيتافم ةداعإل تارايخ ءاطعإل ةرادإ ىل ع رقنا

# All > vpn.remoteasa.com

Standard SSL Certificate

## Certificate Management Options



Download



Revoke



Manage

## Certificate Details

Status	Certificate issued
Domain name	vpn.remoteasa.com
Encryption Strength	GoDaddy SHA-2
Validity Period	7/22/2015 - 7/22/2016
Serial Number	25:cd:73:a9:84:07:06:05

ديج CSR ل ا تفض او ةداهش حاتفم ةداع ا رايخل ا تدم

# vpn.remoteasa.com > Manage Certificate

Standard SSL Certificate

Use this page to submit your certificate changes for review all at once, not individually. We'll review them together so your changes happen faster.

Submitting any changes on this form will issue a new certificate and your current certificate will be revoked. You will have 72 hours to install the new certificate on your website.

Re-Key certificate *Private key lost, compromised, or stolen? Time to re-key.*

Certificate Signing Request (CSR)

```
13qHfepIRd3QX0kDh4P/wKI12bz/zb1v/SI  
N80GsenQVuzayZiH-N3R9EU/3Rz9  
PcctuZ18yZLZTr6NSxki9im111aCuxlH9FmW
```

Domain Name (based on CSR):  
**vpn.remoteasa.com**

Change the site that your certificate protects *If you want to switch your certificate from one site to another, do it here.*

Change encryption algorithm and/or certificate issuer *Upgrade your protection or change the company behind your cert.*

إلى دن تست ةديج ةداهش GoDaddy ردصي .ةيلال ةوطخلإ إلى ةعباتمل او ظحلإب مق  
اهرفوت مت يلال CSR

3. ةداهش تيبثت " ي ف حضم وه امك ةديج TrustPoint لىل ةديجل ةداهشل تيبثت مق  
ASA مسق ي ف " SSL

## ةرركتم لىل ةلىسأل

1. رخآ ASA لىل ASA نم ةيوهل اءداهش لىل ةقيرط لىل فاه ام .

PKCS12 فلم لىل حيتافم لىل عم ةداهشل ريدصت

يلىل لىل ASA نم CLI ربع ةداهشل ريدصت لىل رمأل اءه مدختسأ

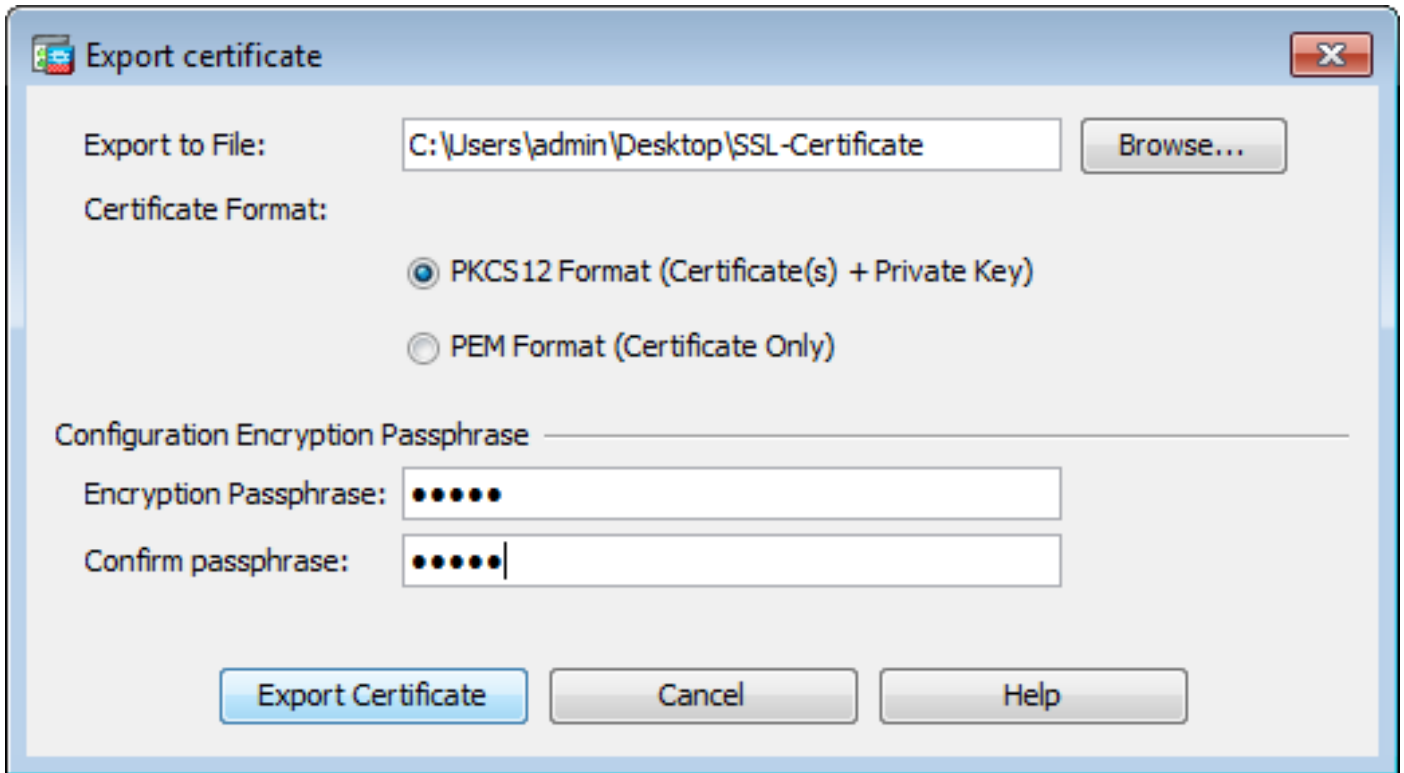
```
<#root>
```

```
ASA(config)#
```

```
crypto ca export
```

```
pkcs12
```

ASDM نيوكت:



فده ل ASA لى لى CLI ربع ةداهش لى داريت سال رم ألى اذه مدخت س أ

<#root>

ASA(config)#

crypto ca import

pkcs12

ASDM: ني وكت

مادختساب ASDM ىلع "ةداعتسال/ايطايتحالآخسنلا" ةزيم ربع كلذب مايقلا نكمي امك ةليلال تاوطخال

1. **Tools > Backup Configuration** رتخاو ASDM ربع ASA ىلى لوخدلا لآس.
2. طقف ةيوهال تاداهش وأ نيوكتال تايلمع عيمجل يطايتحالآخسن ءارجاب مق.
3. **Tools > Restore Configuration** رتخاو ASDM حتفا ، فدهال ASA ىلع.

ةنزاومب ةصاخال ASA تادحو عم مادختسالل SSL تاداهش ءاشنإ كنكمي فيك 2. ةيرهاظال ةصاخال ءكبشال لمح (VPN)؟

لمح ةنزاوم ةئيبل SSL تاداهش مادختساب ASAs دادعال اهمادختسال نكمي ةددعتم قرط كانه VPN.

1. ةنزاوم FQDN ىلع يوتحت ةدحو او (UCC) ةددعتم تالاجم/ةدحوم تالاصتإ ةداهش مدختسأ (SAN) لصفنم عوضوملل ليدب مساك ASA FQDN تاكبش نم لك و DN ءكبشك لامحالآ يتال اهريغو Comodo و Entrust و GoDaddy لثم ةفورعمل ءبقارملا زكارم نم ديدعلا كانه ايلاح معدى ال ASA نأ ركذت مهمال نم ، ةقيرطال هذه راتخت ام دنع . تاداهشال هذه لثم معدت ايلاح معدى ال cisco نيسحتال في اذتقثو . ةددعتم SAN لوقح عم CSR ءاشنإ [CSCso70867](https://www.cisco.com/c/en/us/td/docs/configuration/guide/ssl/ssl_csr.html) id قب . CSR ءاشنإل نارايخ كانه ، ةلحال هذه في



- a. لاسرا دنع (ASDM) لوحمل تانايب ةدعاق ةرادا وأ (CLI) رمأوالا رطس ةهجاو لالخال نم.
- ب. قطنم تاكبش فضا، (CA) قدصملا عجرملا لىل (CSR) ةيساسألا ةيلوؤسملا افسن CA ةباوب لىل ةددعتملا (SAN) نيزختلا.
- b. (SAN) نيزختلا قطنم تاكبش نيمضتو CSR عاشنل OpenSSL مدختسا.
- لما فم ي ةددعتملا openssl.cnf.

لىل هذه PEM ةداهش داريتساب مق، اهؤاشنل مت يتلا ةداهشل او CA لىل CSR لاسرا درجمب ةداهشل هذه داريتسا ويرى صتب مق، اءاتنال درجمبو. CSR عاشنل اب تماق يتلا ASA نيزخال اءاضعالاب ةصخال ASA تادحو لىل PKCS12 قيسنتب.

2. تالاصتالا ةداهشب اهت نراقم دنع ةنورمو انام لقا ةقيرط هذه. لذب فرح ةداهش مادختسا. لىل CA لىل CSR عاشنل متي، ةدحوملا تالاصتالا تاداهشل CA معد مدع ةلاح ي. ةدحوملا لىل CSR لاسرا درجمب \*.domain.com لكش لىل FQDN نوكي شيح OpenSSL مادختساب وأ ماظن ي ف ASAs عيمج لىل PKCS12 ةداهش داريتساب مق، اهؤاشنل مت يتلا ةداهشل او CA ةعومجملا.
3. اذهو. FQDN لمح ةنزاوملو وضعلا ASA نيزختلا تادحو نم لكل ةلصفنم ةداهش مدختسا. (ASA) لوصول ي ف مكحتلا تادحو نم لكل تاداهشل عاشنل نكمي. ةيلاعف لقالا لجال وه VPN ب ةصخال ةداهشل عاشنل متي. دننتسمل اذه ي ف حضوم وه امك ةيدرفل لىل PKCS12 ةداهشك اءاريتسا و اءري صت متي و دحاو ASA لىل LoadBalancing FQDN لىل ASAs لىل.

### 3. ASA جوز ي ف يونثال لىل ASA لىل ياساسألا ASA نم تاداهشل لىل خسن بجي له. لاطعال زواجتل

تاداهشل ةنمازم متي شيح يونثال لىل ياساسألا ASA نم ايودي تاداهشل لىل خسنل ةجاج دجوت ال زاهج لىل تاداهشل ضرع متي مل اذا. ةلاحلا وذل لىل زواجت نيوكت مت هنأ املاط ASA نيب رابجل write standby رمال رادصا كىل لىل، لىل زواجتل لىل دادعال لىل دادعتسال ةنمازمل.

### 4. SSL ةداهش عاشنل ةيللمع فللخت له، ECDSA حيتافم مادختسا مت اذا.

حيتافم جوز عاشنل متي شيح، حيتافملا جوز عاشنل ةوطخ وه نيوكتلا ي ف دىحولا قرفلاو ةهجاو رما ضرع متي. يه امك تي قبب تاوطخال يقاب اما. RSA حيتافم جوز نم ال دب ECDSA انه: ECDSA حيتافم عاشنل (CLI) رمال رطس

```
<#root>
```

```
MainASA(config)#
```

```
cry key generate ecdsa label SSL-Keypair elliptic-curve 256
```

```
INFO: The name for the keys will be: SSL-Keypair
Keypair generation process begin. Please wait...
```

## اهجالص او اءخال فاشكتسا



## ةداهش و،ةيوه ةداهش نم PKCS12 ةداهش ءاشنإل OpenSSL مدختسأ :ب ققحلملإ صاخحاتفم و، CA

1. هيلع ةيلمعلل هذه ليلغشت متي يذلل ماظنلل ىلعل OpenSSL تيبتت نم ققحت .  
يضا رتفا لكشب اذه تيبتت متي ، GNU/Linux و Mac OSX يمدختسمل ةبسنلاب .
2. حلص ليلدلىل ليلدبتل .

C:\Openssl\bin. يف ةدعاسملا تاودألل تيبتت متي ، يضا رتفا لكشب : Windows ىلعل  
عقوملا اذه يف رماو ءجومحتف .

ةداهش ءاشنإل بولطملا ليلدلل يف ةيفرطلل ةطحملل ةذفانحتفا : Mac OSX/Linux ىلعل  
PKCS12.

3. صاخحاتفملا تافل مظفحا ، ةقباسللا ةوطخلل يف روكذملل ليلدلل يف  
(CACert.crt) رذجلل قدصملا ءجرملا ةداهش و (certificate.crt) ةيوهلا ةداهش و ، (privateKey.key)

يف رذجلل قدصملا ءجرملا ةداهش ةلسلسو ةيوهلا ةداهش و صاخحاتفملا ءمدب مق  
PKCS12 ةداهش ةيامحل رورم ةرابع لخدأ . PKCS12 فلم

```
strong> openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in certificate.crt -cer
```

4. Base64 ةزرم ةداهش ىلعل ةدلوملا PKCS12 ةداهش ليلوحت :  
<#root>

```
openssl base64 -in certificate.pfx -out certificate.p12
```

SSL عم مادختسالل ةريخألل ةوطخلل يف اهؤاشنإل متي تلل ةداهشلا داريتساب مق ، كلذ دعب

## ةلص تاذتامولعم

- [ةيمقرلا تاداهشلا نيوكت - ASA 9.x نيوكت ليلد](#)
- [ASA ىلعل ASDM عم Microsoft Windows CA نم ةيمقر ةداهش ىلعل لوصحلل ةيفي](#)
- [تادنتسمللاو يئقتلا معدلا - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت  
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبلاو  
امك ةقيد نوك تنل ةللأل ةمچرت لصف انءمچال مچرئى. ةصاغل مهتغب  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه  
ىل اءءاد ةوچرلاب يصوت وتامچرتل هذه ةقدنع اهتيلوئسم Cisco  
Systems (رفوتم طبارلا) يلصلأل يزىلچنل دن تسمل