ASA 7.x يريك يديوي شهادات دورم الطرف الثالث للاستخدام مع مثال تكوين WebVPN

المحتويات

المقدمة

يوضح مثال التكوين التالي كيفية تثبيت الشهادة الرقمية لمورد الطرف الثالث ويداي على ASA للاستخدام مع WebVPN. يتم إستخدام شهادة الإصدار التجريبي في هذا المثال. تحتوي كل خطوة على إجراء تطبيق ASDM ومثال واجهة سطر الأوامر.

المتطلبات الأساسية

المتطلبات

يتطلب هذا المستند أن يكون لديك حق الوصول إلى مرجع مصدق (CA) لتسجيل الشهادة. ومورد CA المدعوم من الطرف الثالث هم بالتيمور و Cisco و Entrust و iPlanet/Netscape و Microsoft و RSA و VeriSign.

المكونات المستخدمة

يستعمل هذا وثيقة ASA 5510 أن يركض برمجية صيغة 7.2(1) و ASDM صيغة 5.2(1). وهم

ذلك، تعمل الإجراءات الواردة في هذا المستند على أي جهاز ASA يشغل الإصدار 7.x مع أي إصدار ASDM متوافق.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

التكوين

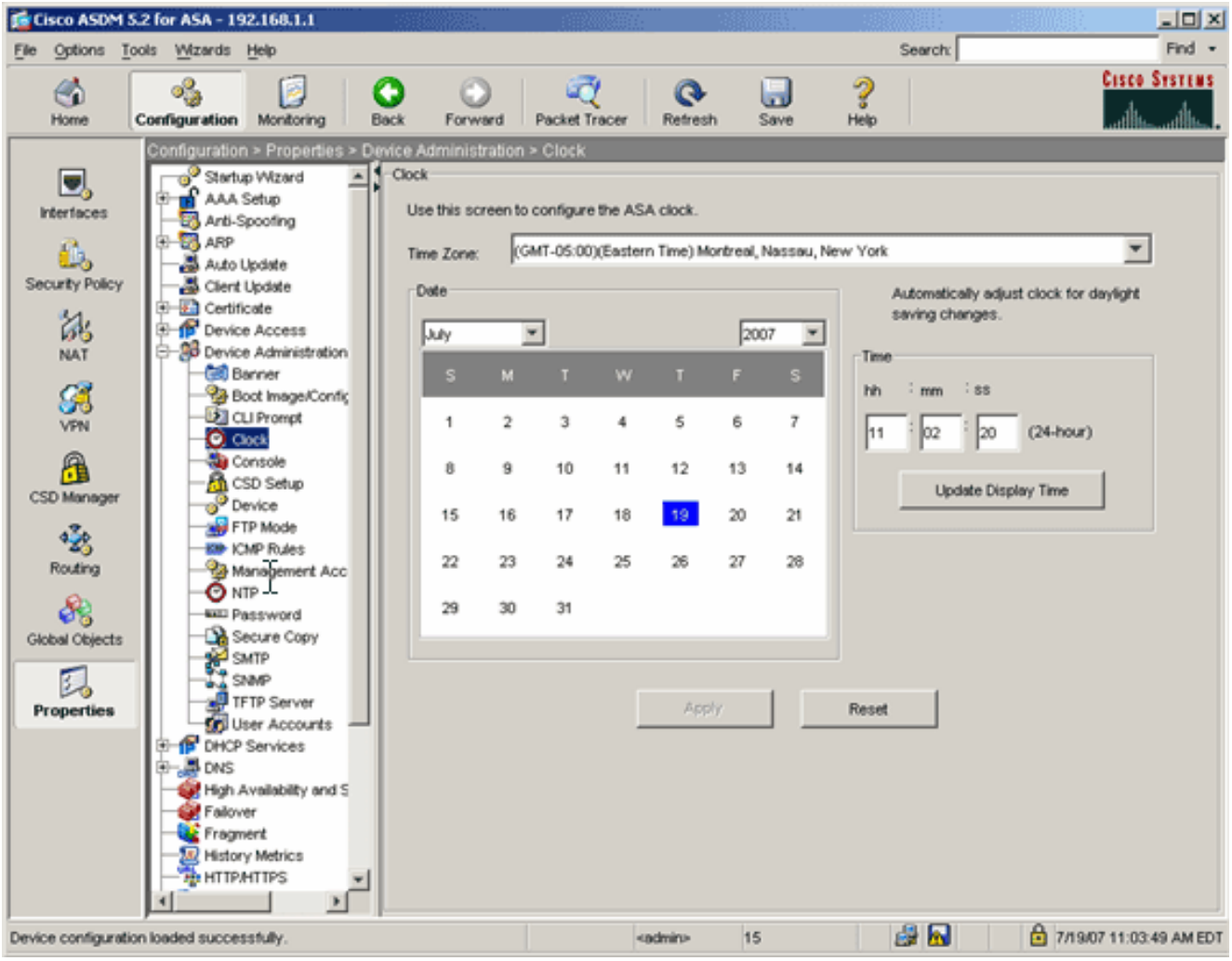
لتثبيت شهادة رقمية لمورد من إنتاج جهة خارجية على PIX/ASA، أكمل الخطوات التالية:

1. تحقق من دقة قيم التاريخ والوقت والمنطقة الزمنية.
2. قم بإنشاء زوج مفاتيح RSA.
3. إنشاء TrustPoint.
4. إنشاء تسجيل الشهادة.
5. مصادقة TrustPoint.
6. قم بتثبيت الشهادة.
7. قم بتكوين WebVPN لاستخدام الشهادة المثبتة حديثا.

الخطوة 1. التحقق من دقة قيم التاريخ والوقت والمنطقة الزمنية

إجراء ASDM

1. انقر فوق تكوين، ثم انقر فوق خصائص.
2. قم بتوسيع إدارة الأجهزة، واختر الساعة.
3. تحقق من صحة المعلومات المدرجة.يجب أن تكون قيم التاريخ والوقت والمنطقة الزمنية دقيقة حتى يتم التحقق من صحة الشهادة بشكل صحيح.



مثال على سطر الأوامر

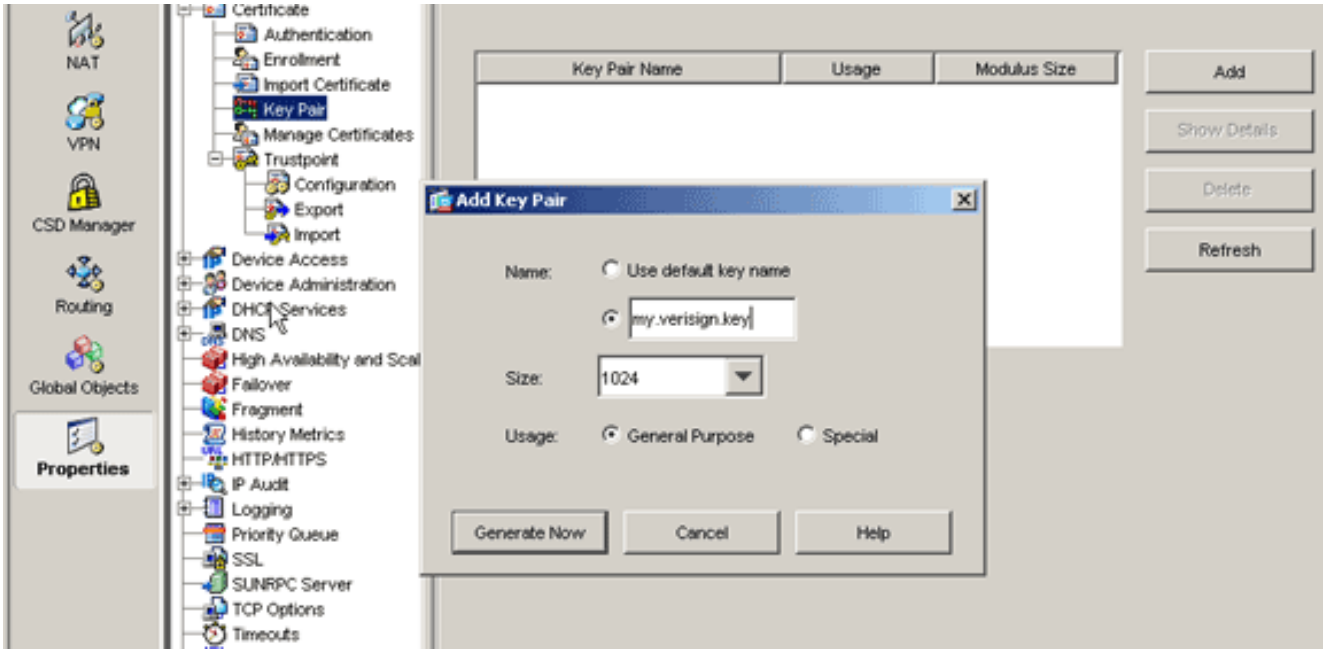
سيسكو اس
ciscoasa#**show clock** 11:02:20.244 UTC Thu Jul 19 2007 ciscoasa

الخطوة 2. إنشاء زوج مفاتيح RSA

يتم دمج مفتاح RSA العام الذي تم إنشاؤه مع معلومات هوية ASA لتكوين طلب شهادة PKCS#10. يجب عليك تحديد اسم المفتاح بشكل واضح باستخدام TrustPoint التي تقوم بإنشاء زوج المفاتيح لها.

إجراء ASDM

1. انقر فوق **تكوين**، ثم انقر فوق **خصائص**.
2. قم بتوسيع **الشهادة**، واختر **زوج المفاتيح**.
3. انقر فوق **إضافة**
   (Add).



4. قم بإدخال اسم المفتاح، واختر حجم المعامل، وحدد نوع الاستخدام. ملاحظة: حجم زوج المفاتيح الموصى به هو 1024.
5. طقطقة **يلد**.يجب إدراج زوج المفاتيح الذي قمت بإنشائه في عمود "اسم زوج المفاتيح".

مثال على سطر الأوامر

سيسكو اسا

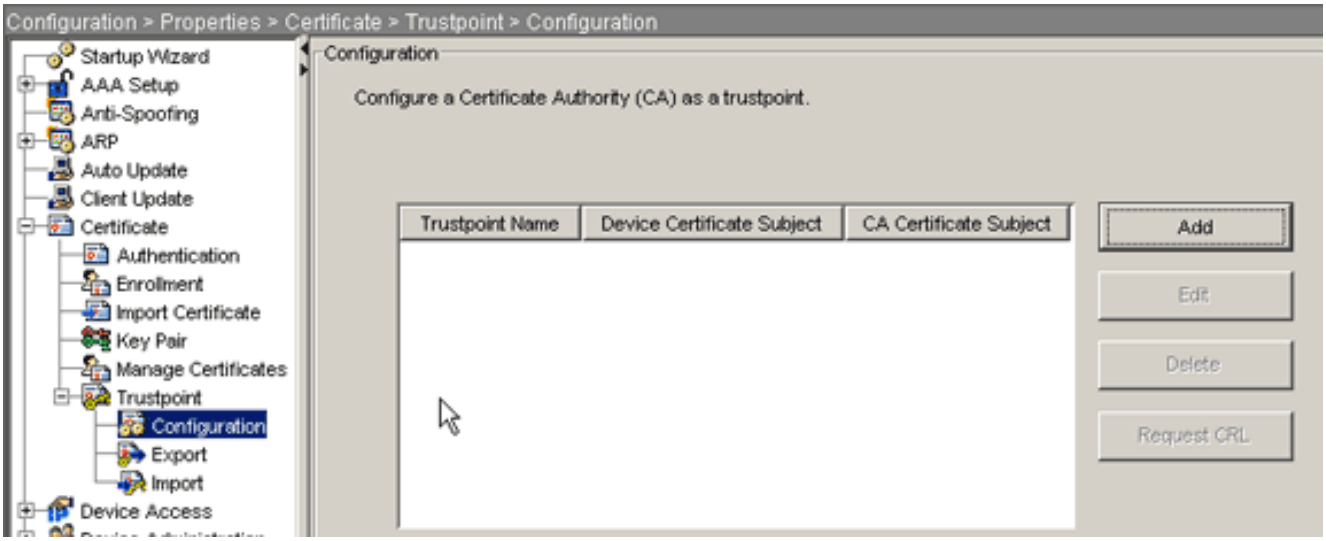
```
ciscoasa#conf t

ciscoasa(config)#crypto key generate rsa label
my.verisign.key modulus 1024

! Generates 1024 bit RSA key pair. "label" defines the
name of the key pair. INFO: The name for the keys will
be: my.verisign.key Keypair generation process begin.
Please wait... ciscoasa(config)#
```

الخطوة 3. إنشاء TrustPoint

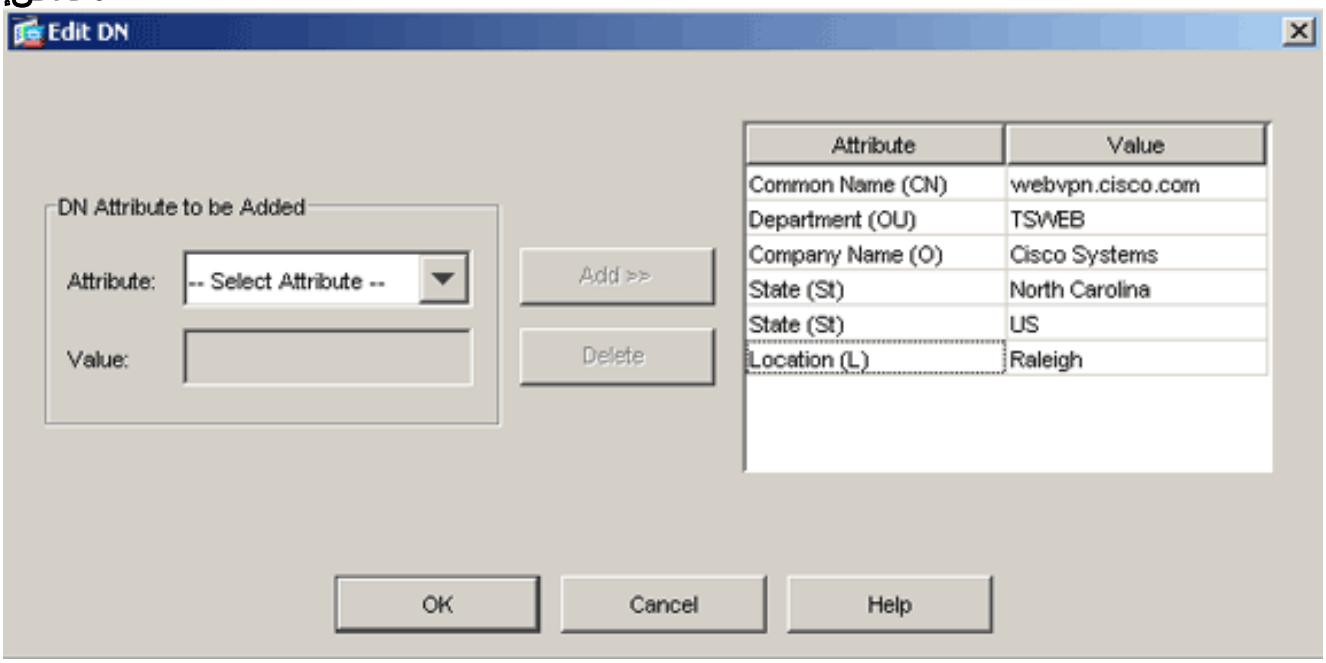
يلزم توفر نقاط الثقة لإعلان المرجع المصدق (CA) الذي سيستخدمه ASA.

إجراء ASDM

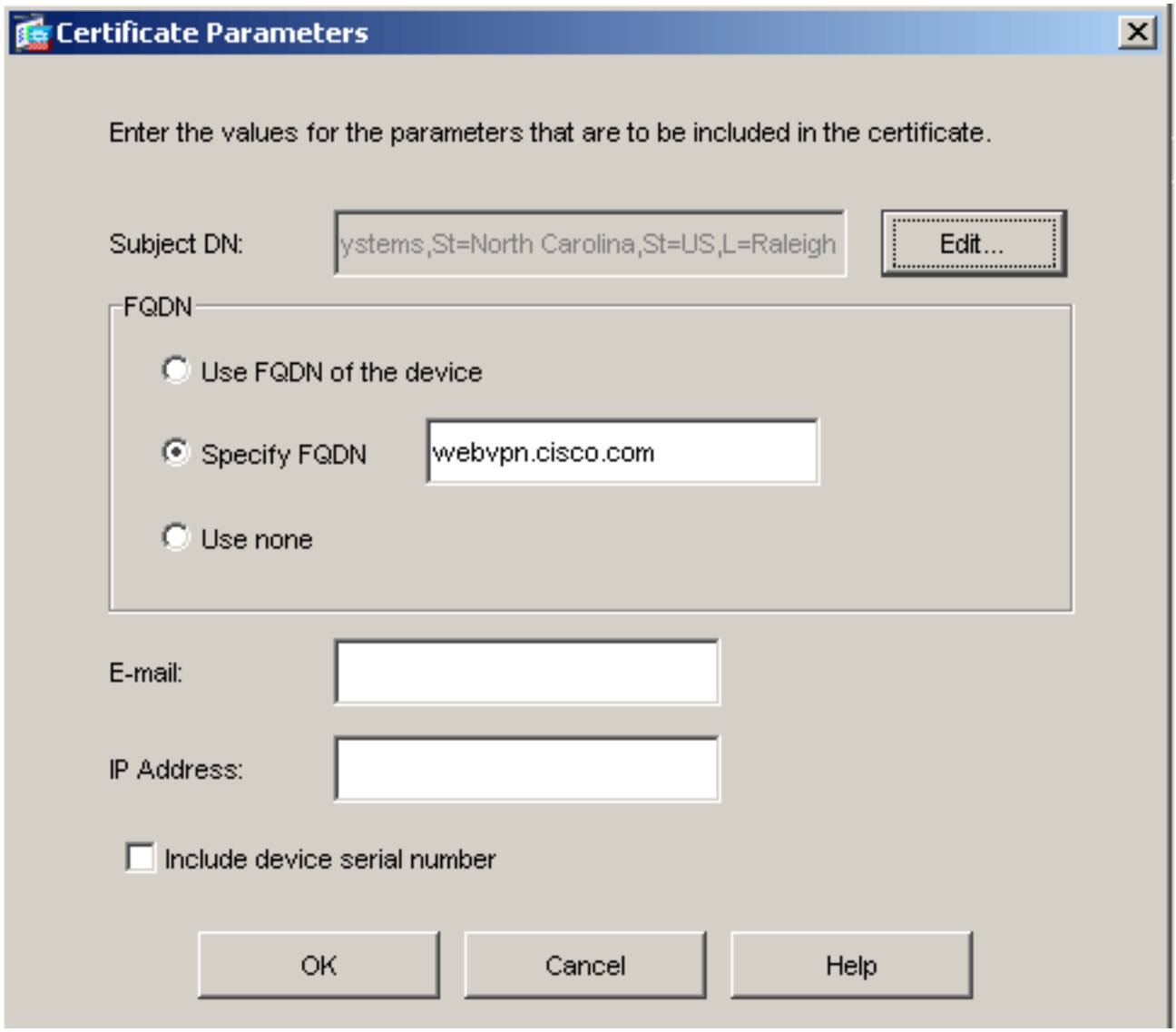
1. انقر فوق **تكوين**، ثم انقر فوق **خصائص**.
2. قم بتوسيع **الشهادة**، ثم قم بتوسيع **TrustPoint**.
3. أختر **تشكيل**، وطقطقة **يضيف**.



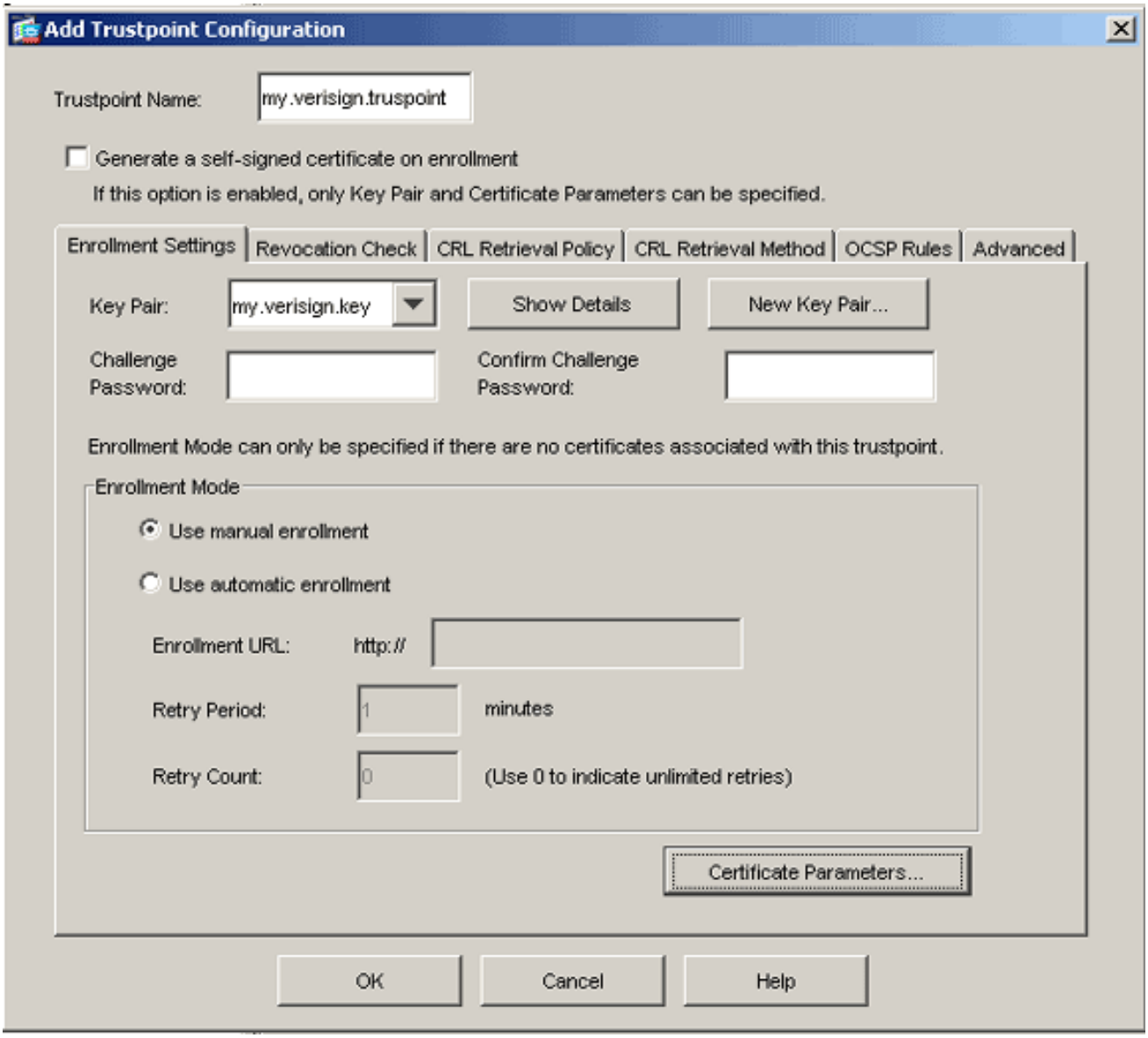
4. قم بتكوين هذه القيم:**اسم TrustPoint**: يجب أن يكون اسم TrustPoint ذا صلة باستخدام المقصود. (يستخدم هذا المثال *my.verisign.trustPoint*.)**زوج المفاتيح**: حدد زوج المفاتيح الذي تم إنشاؤه في الخطوة 2. (*my.verisign.key*)
5. تأكد من تحديد التسجيل اليدوي.
6. انقر على **معلمات الشهادة**.يظهر مربع الحوار معلمات الشهادة.
7. طقطقة **يحرر**، وشكلت الشعار يعدد في هذا طاولة:لتكوين هذه القيم، أختر قيمة من القائمة المنسدلة "سمات"، وأدخل القيمة، وانقر فوق **إضافة**.



8. بمجرد إضافة القيم المناسبة، انقر فوق **موافق**.
9. في شاشة معلمات الشهادة، أدخل FQDN في حقل تحديد FQDN.يجب أن تكون هذه القيمة نفس FQDN التي أستخدمتها للاسم الشائع (CN).



10. وانقر فوق **OK**.
11. تحقق من تحديد زوج المفاتيح الصحيح، ثم انقر فوق زر **إستخدام التسجيل اليدوي**.
12. انقر فوق **موافق**، ثم انقر فوق
    تطبيق.



مثال على سطر الأوامر

سيسكو اس

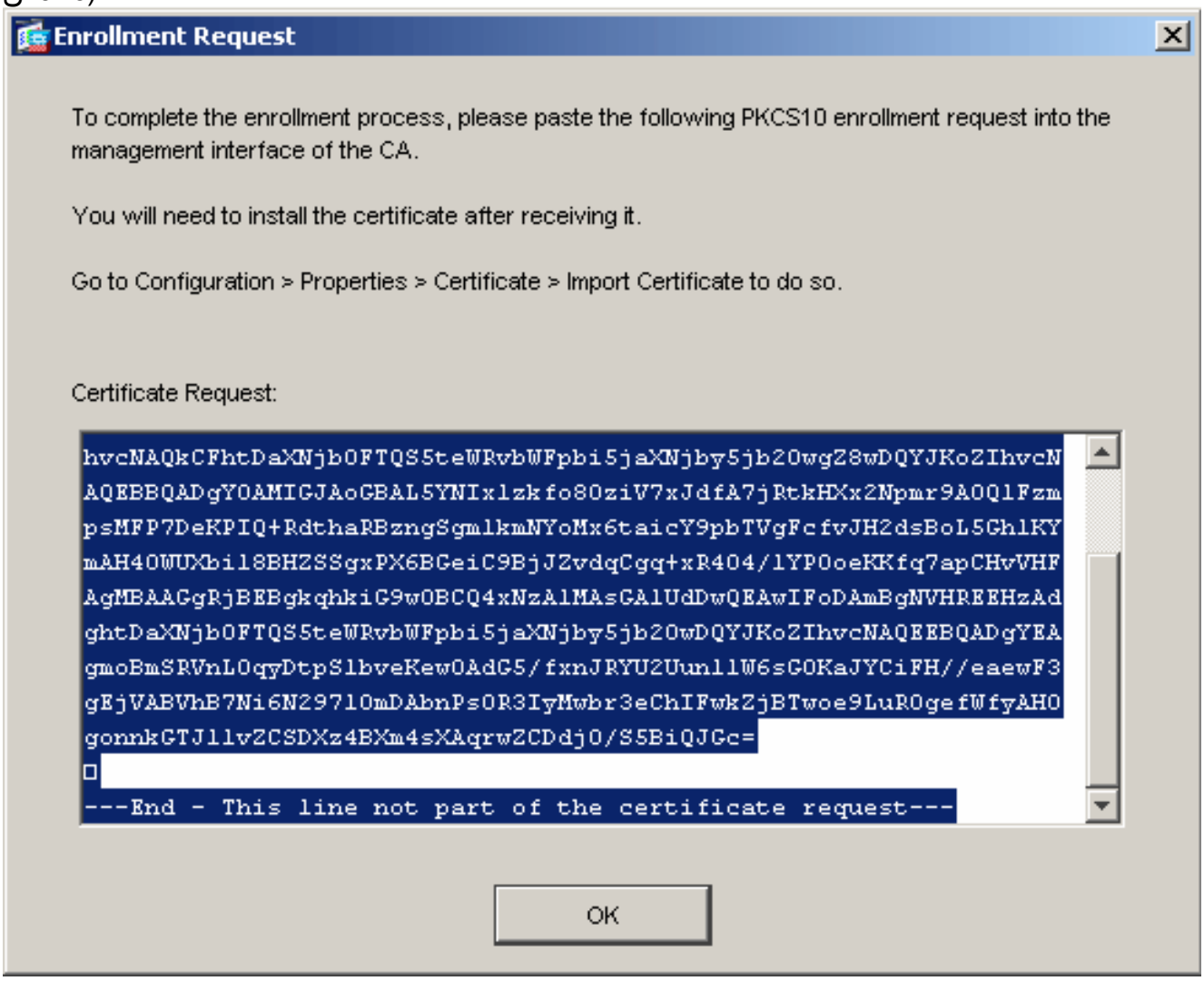
```
ciscoasa(config)#crypto ca trustpoint
my.verisign.trustpoint


! Creates the trustpoint.

ciscoasa(config-ca-trustpoint)#enrollment terminal

! Specifies cut and paste enrollment with this
trustpoint. ciscoasa(config-ca-trustpoint)#subject-name
CN=wepvpn.cisco.com,OU=TSWEB,
                              O=Cisco
Systems,C=US,St=North Carolina,L=Raleigh

! Defines x.500 distinguished name. ciscoasa(config-ca-
trustpoint)#keypair my.verisign.key

! Specifies key pair generated in Step 3.
ciscoasa(config-ca-trustpoint)#fqdn webvpn.cisco.com


! Specifies subject alternative name (DNS:).
```

```
ciscoasa(config-ca-trustpoint)#exit
```

الخطوة 4. إنشاء تسجيل الشهادة

إجراء ASDM

1. انقر فوق **تكوين**، ثم انقر فوق **خصائص**.
2. قم بتوسيع **الشهادة**، واختر **التسجيل**.
3. تحقق من تحديد TrustPoint الذي تم إنشاؤه في الخطوة 3، وانقر فوق **تسجيل**.يظهر مربع حوار يسرد طلب تسجيل الشهادة (يشار إليه أيضا باسم طلب توقيع شهادة).



4. انسخ طلب تسجيل PKCS#10 إلى ملف نصي، ثم قم بإرسال CSR إلى مورد الطرف الثالث المناسب.بعد أن يستقبل مورد الطرف الثالث CSR، يجب عليه إصدار شهادة هوية للتثبيت.

مثال على سطر الأوامر

إسم الجهاز 1
ciscoasa(config)#**crypto ca enroll my.verisign.trustpoint** *! Initiates CSR. This is the request to be ! submitted via web or email to the 3rd party vendor.* % Start certificate enrollment .. % The subject name in the certificate will be: CN=webvpn.cisco.com,OU=TSWEB,

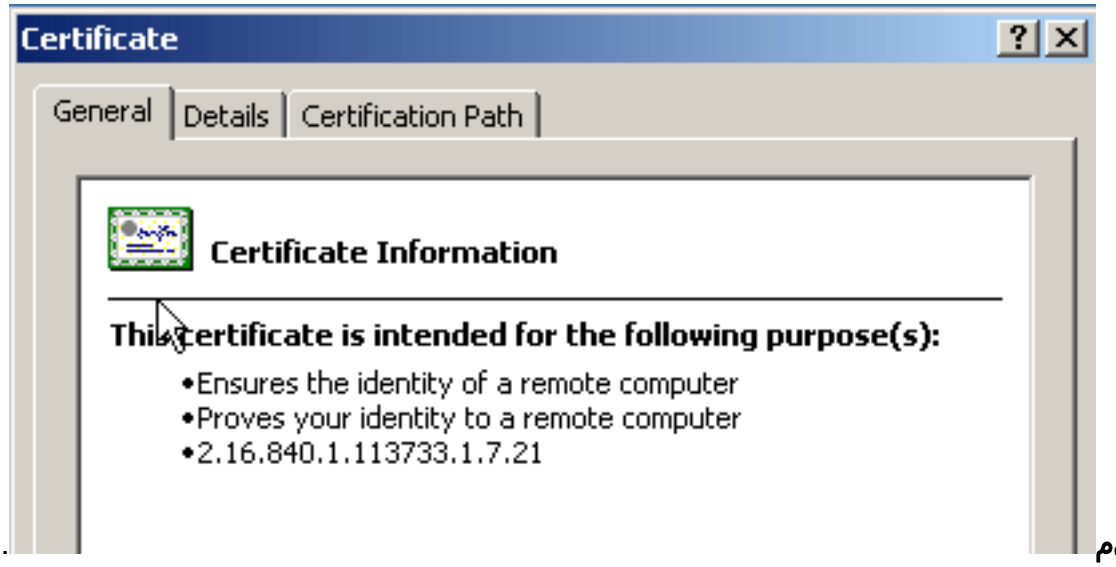
```
O=Cisco Systems,C=US,St=North Carolina,L=Raleigh % The
fully-qualified domain name in the certificate will be:
webvpn.cisco.com % Include the device serial number in
the subject name? [yes/no]: no ! Do not include the
device's serial number in the subject. Display
Certificate Request to terminal? [yes/no]: yes

! Displays the PKCS#10 enrollment request to the
terminal. ! You will need to copy this from the terminal
to a text ! file or web text field to submit to the 3rd
party CA. Certificate Request follows:
MIICHjCCAYcCAQAwgaAxEDAOBgNVBAcTB1JhbGVpZ2gxFzAVBgNVBAgT
Dk5vcnRo
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lz
dGVtczEO
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv
bTEhMB8G
CSqGSIb3DQEJAhYSY2lzY29hc2EuY2lzY28uY29tMIGfMA0GCSqGSIb3
DQEBAQUA
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB
9M4yTx5b
Fm886s8F73WsfQPynBDfBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt
3oMXSNPO
m1dZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX0luBMh7oKar
gwIDAQAB
oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBYw
FIISY2lz
Y29hc2EuY2lzY28uY29tMA0GCSqGSIb3DQEBBAUAA4GBABrxpY0q7SeO
HZf3yEJq
po6wG+oZpsvpYI/HemKUlaRc783w4BMO5lulIEnHgRqAxrTbQn0B7JPI
bkc2ykkm
bYvRt/wiKc8FjpvPpfOkjMK0T3t+HeQ/5QlKx2Y/vrqs+Hg5SLHpbhj/
Uo13yWCe 0Bzg59cYXq/vkoqZV/tBuACr ---End - This line not
part of the certificate request--- Redisplay enrollment
request? [yes/no]:
ciscoasa(config)#
```

الخطوة 5. مصادقة TrustPoint

بمجرد إستلام شهادة الهوية من مورد الطرف الثالث، يمكنك المتابعة بهذه الخطوة.

إجراء ASDM

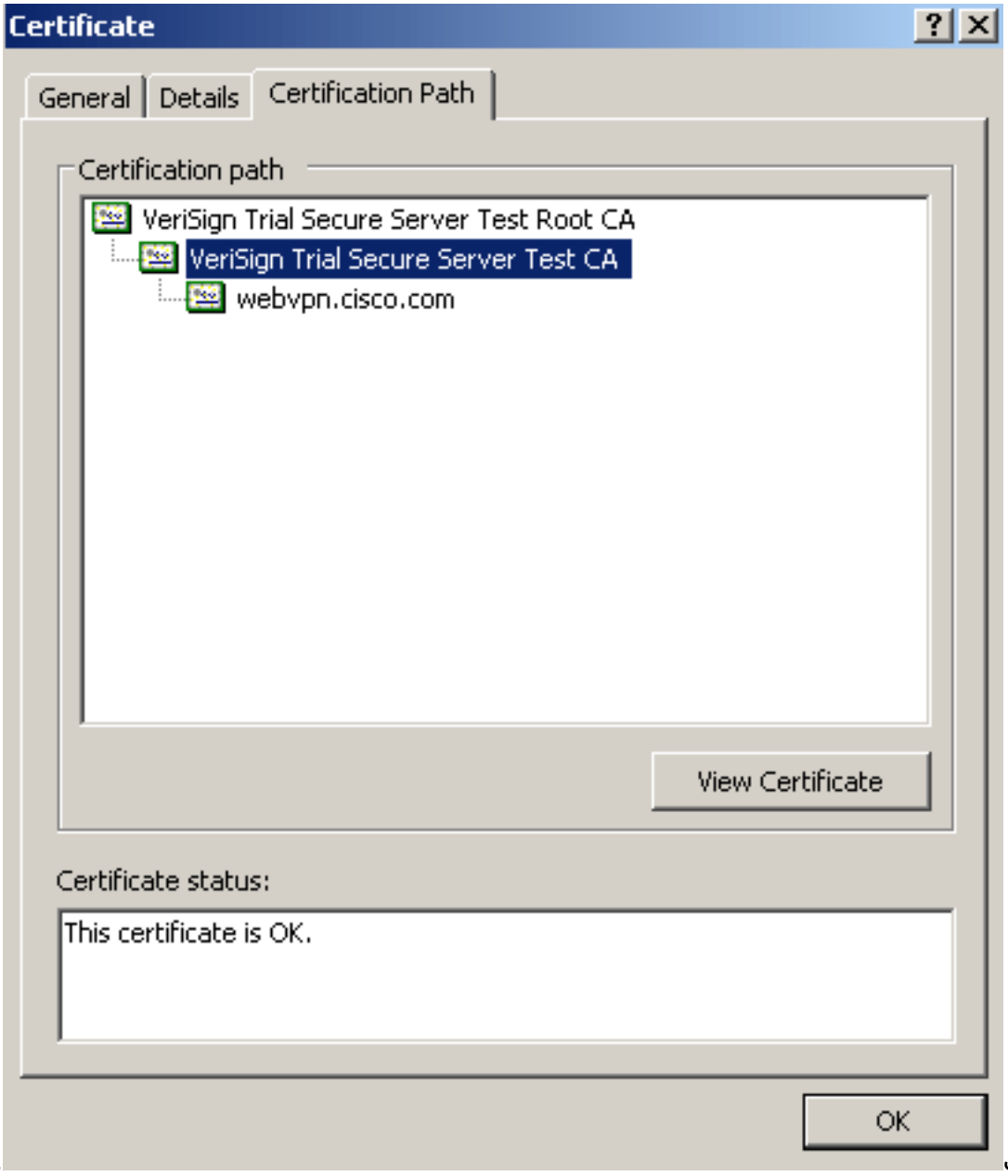
1. قم بحفظ شهادة الهوية على الكمبيوتر المحلي.
2. إذا تم توفير شهادة مرمزة وفقا لمعيار base64 لم يتم إرسالها كملف، فيجب نسخ الرسالة base64 ولصقها في ملف نصي.
3. أعد تسمية الملف بامتداد .cer.**ملاحظة:** بمجرد إعادة تسمية الملف بامتداد .cer، يجب أن تظهر أيقونة الملف كشهادة.
4. قم بالنقر المزدوج على ملف الترخيص.تظهر شاشة



الترخيص.

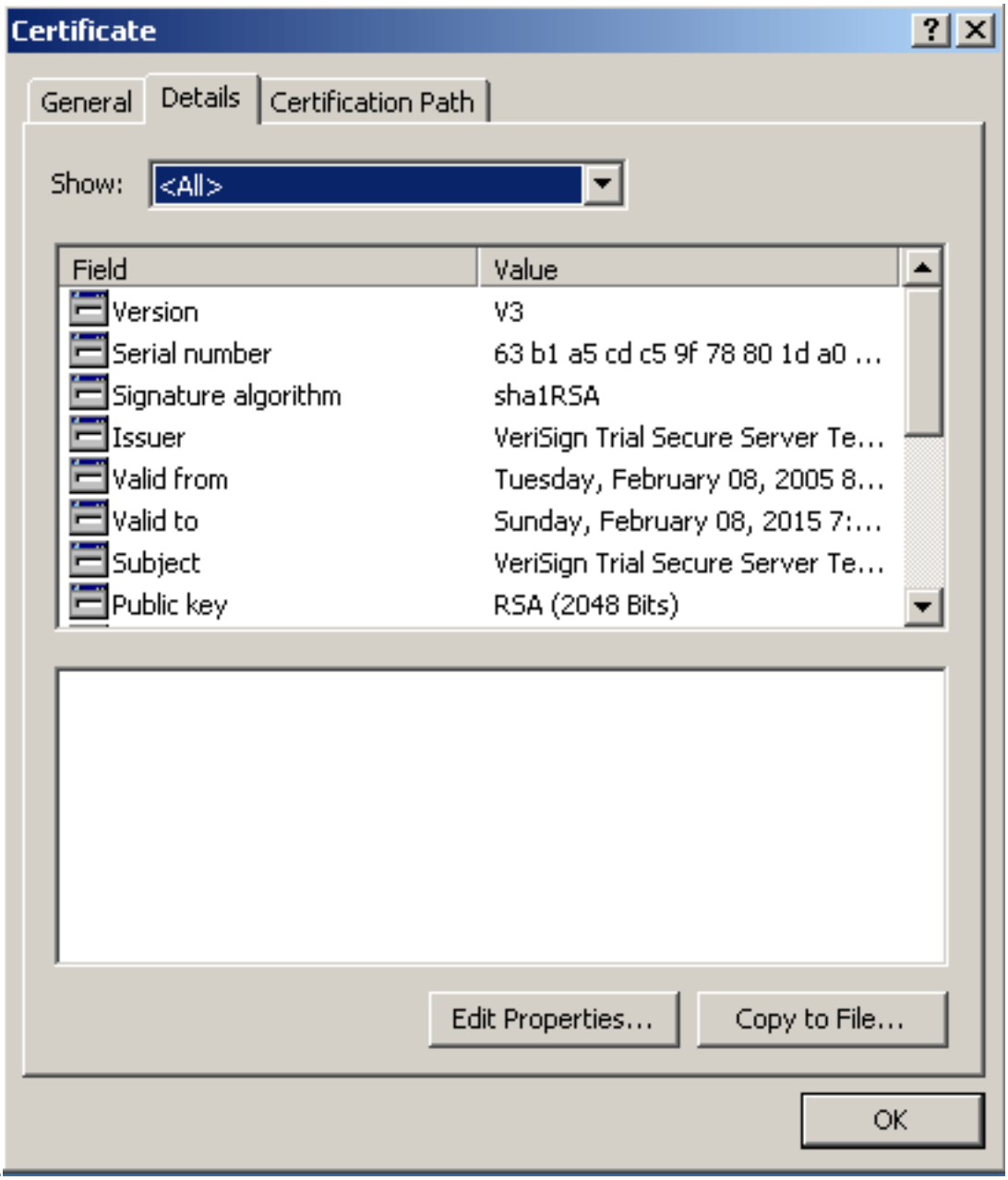
ملاحظة: إذا ظهرت رسالة *Windows ليس لديها معلومات كافية للتحقق من هذه الشهادة* في علامة التبويب "عام"، فيجب عليك الحصول على شهادة المرجع المصدق الجذر (CA) للجهة الخارجية أو شهادة المرجع المصدق الوسيط (CA) قبل متابعة هذا الإجراء. اتصل بمورد الطرف الثالث أو بمسؤول CA للحصول على شهادة CA أو شهادة CA الوسيطة للإصدار.

5. انقر على علامة التبويب **مسار الشهادة**.
6. انقر على شهادة المرجع المصدق الموجودة فوق شهادة الهوية الصادرة، وانقر فوق **عرض**



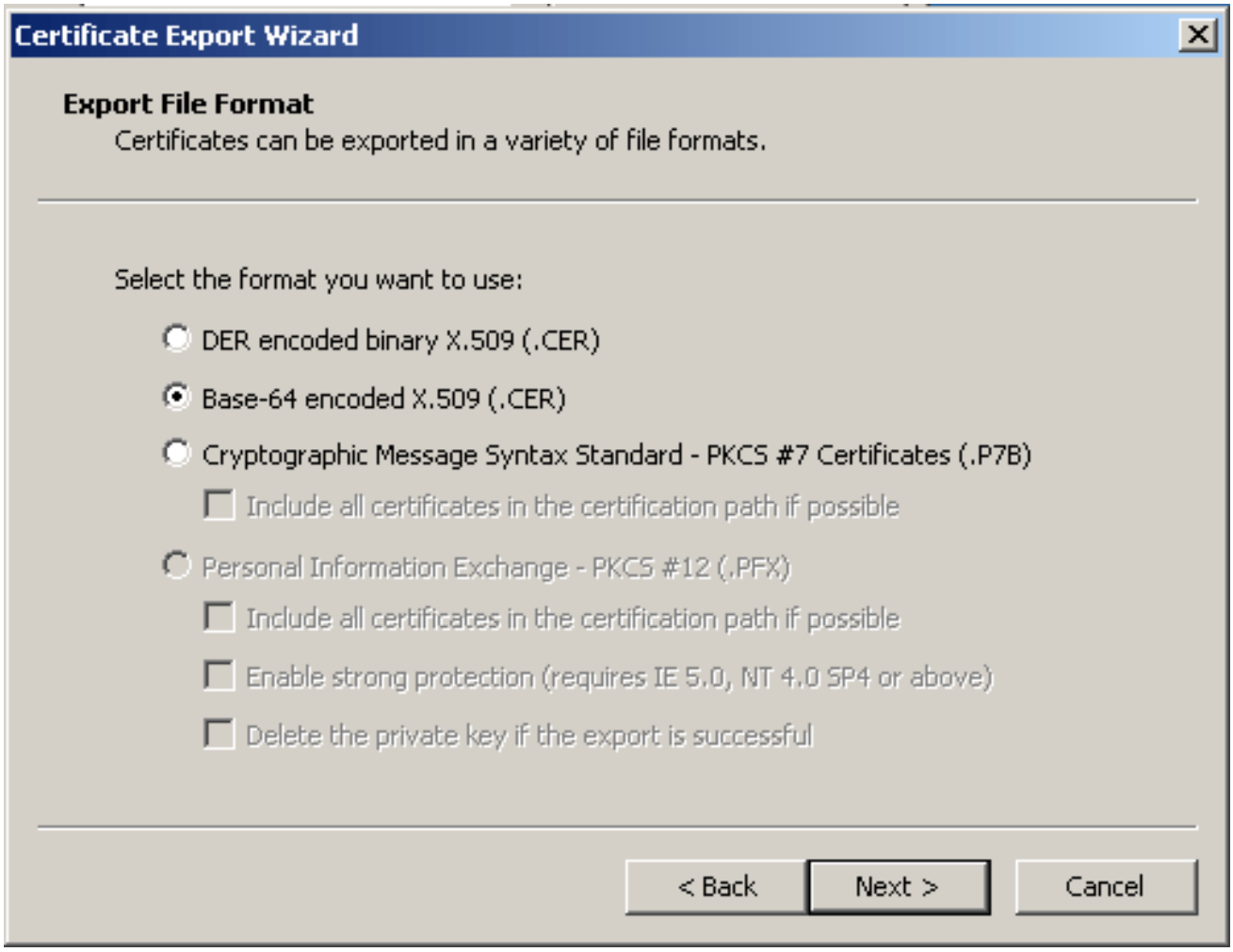
الشهادة. تظهر معلومات تفصيلية حول شهادة CA الوسيطة.**تحذير:** لا تقم بتثبيت شهادة الهوية (الجهاز) في هذه الخطوة. تتم إضافة الجذر أو الجذر الفرعي أو شهادة CA فقط في هذه الخطوة. يتم تثبيت شهادات الهوية (الجهاز) في الخطوة 6.

7. طقطقة

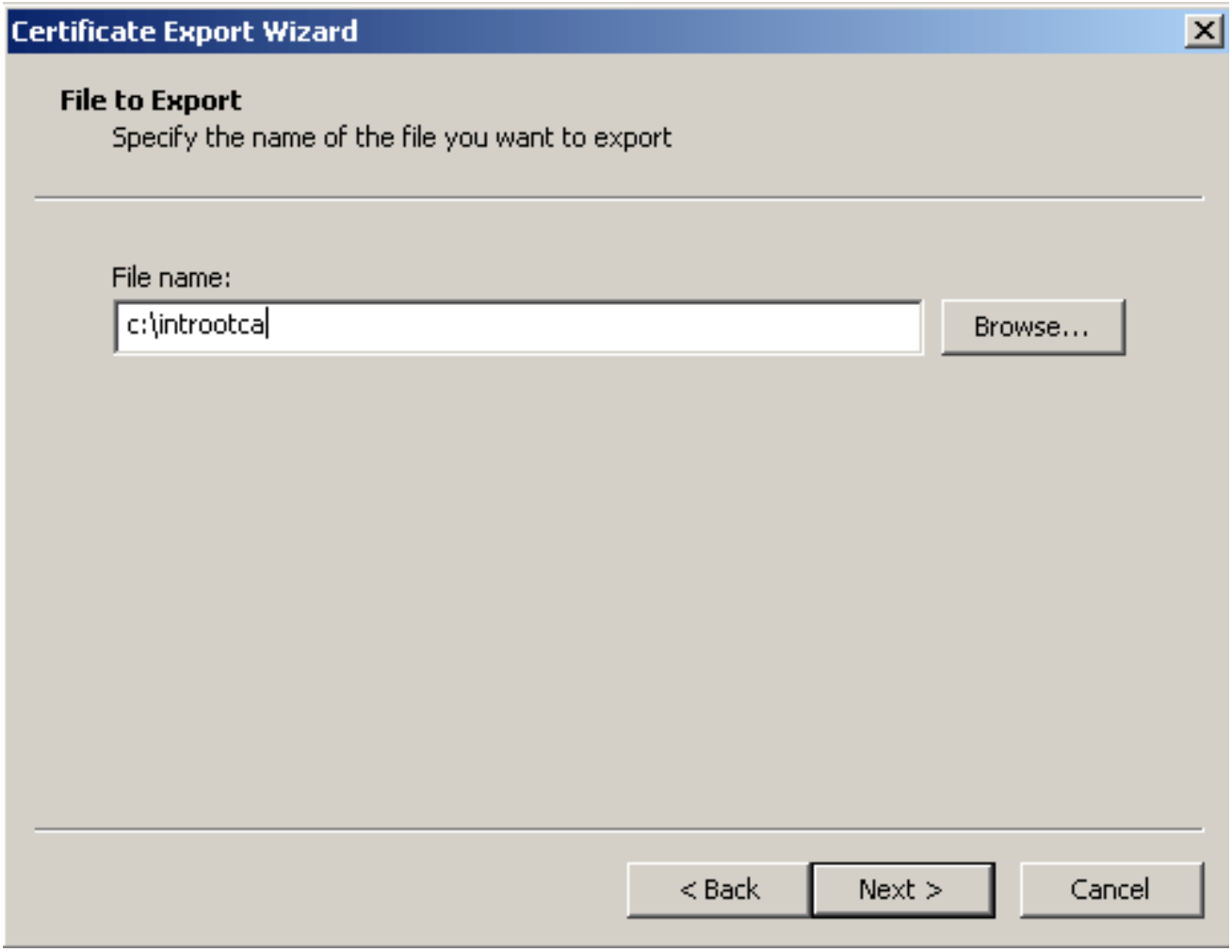


تفاصيل.

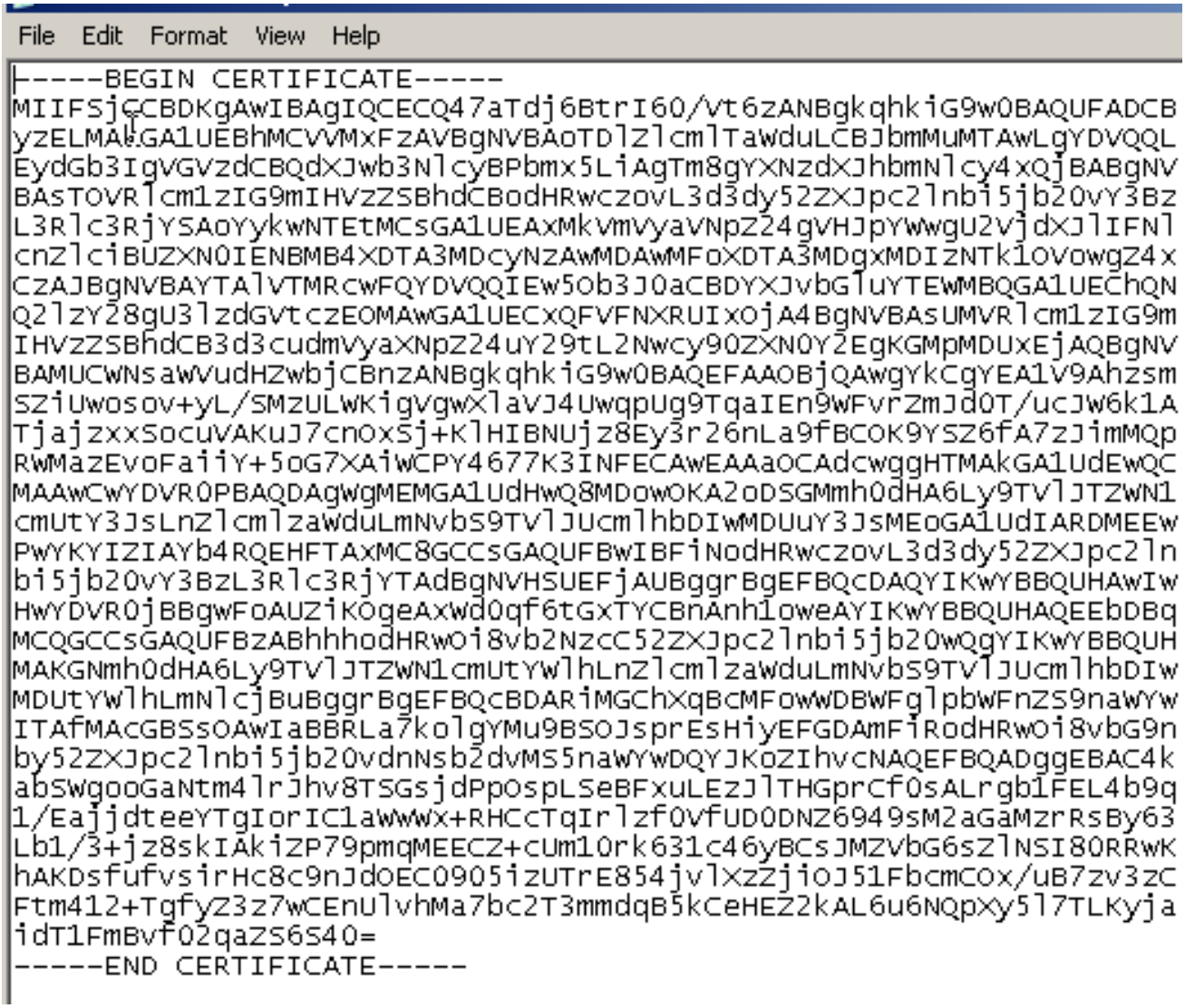
8. انقر فوق **نسخ إلى ملف**.
9. ضمن "معالج تصدير الشهادات"، انقر على **التالي**.
10. في شاشة تنسيق ملف التصدير، انقر زر الخيار **Base-64 المرمز X.509 (.CER)**، وانقر **التالي**.



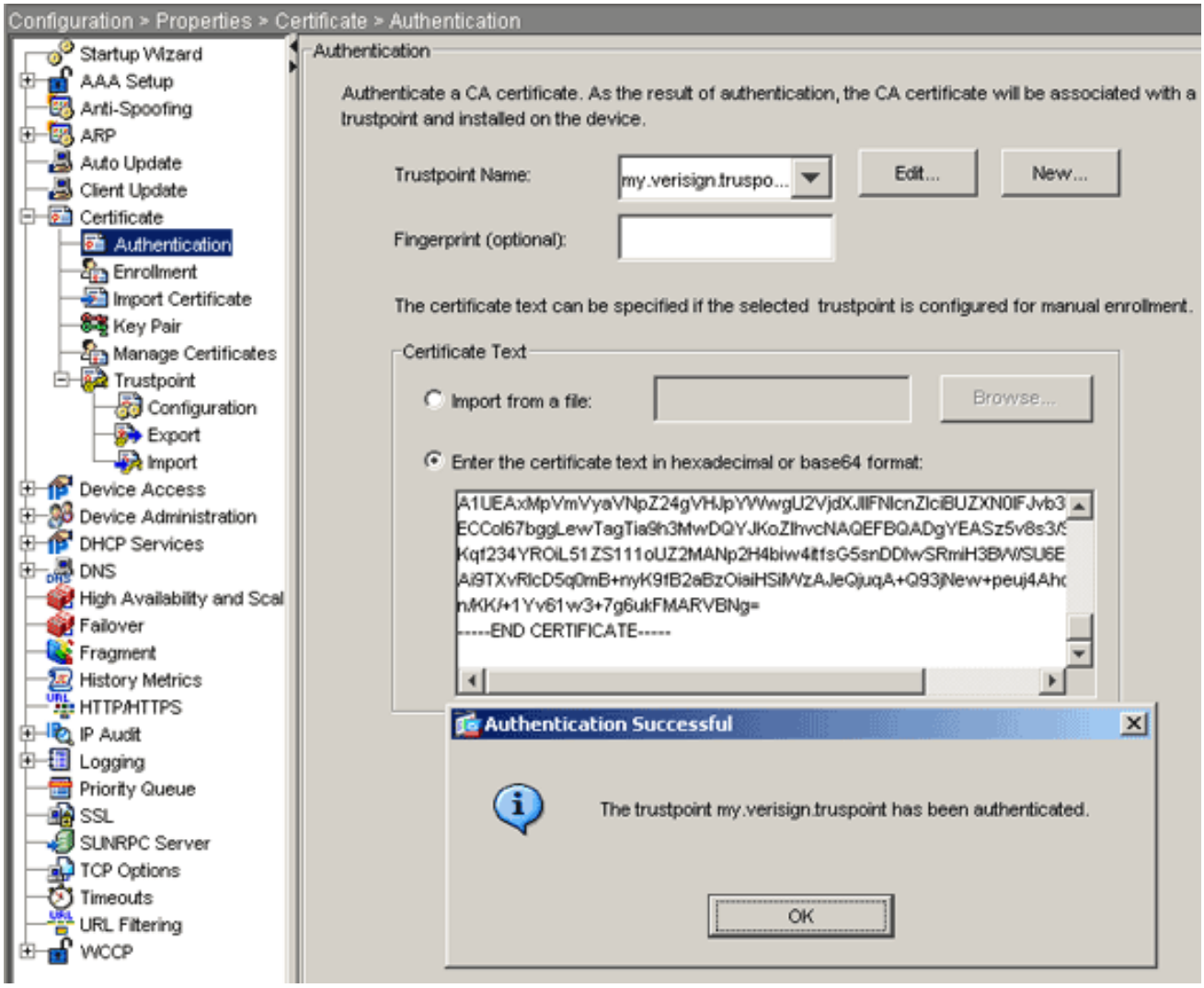
11. أدخل اسم الملف والمكان الذي تريد حفظ شهادة المرجع المصدق عليهما.
12. طقطقت **بعد ذلك**، وبعد ذلك طقطقت
إنجاز.



13. طقطقة **ok** في شاشة التصدير ناجح.
14. تصفح إلى المكان الذي قمت فيه بحفظ شهادة المرجع المصدق.
15. افتح الملف باستخدام محرر نصوص، مثل Notepad. (انقر بزر الماوس الأيمن فوق الملف، واختر **إرسال إلى > Notepad**.)يجب أن تظهر الرسالة التي تم ترميزها بالأساس64 مشابهة للشهادة الموجودة في هذه الصورة:



16. ضمن ASDM، انقر فوق **تكوين**، ثم انقر فوق **خصائص**.
17. قم بتوسيع **الشهادة**، واختر **المصادقة**.
18. انقر على زر **إدخال نص الترخيص بتنسيق سداسي عشر أو تنسيق base64**.
19. الصق شهادة المرجع المصدق بتنسيق base64 من محرر النصوص في منطقة النص.
20. طقطقة
    يصدق.



21. انقر فوق OK.

مثال على سطر الأوامر

سيسكو اس

```
ciscoasa(config)#crypto ca authenticate
my.verisign.trustpoint

! Initiates the prompt to paste in the base64 CA root !
or intermediate certificate. Enter the base 64 encoded
CA certificate. End with the word "quit" on a line by
itself -----BEGIN CERTIFICATE-----
MIIEwDCCBCmgAwIBAgIQY7GlzcWfeIAdoGNs+XVGezANBgkqhkiG9w0B
AQUFADCB
jDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAw
LgYDVQQL
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4x
MjAwBgNV
BAMTKVZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBSb290
IENBMB4X
DTA1MDIwOTAwMDAwMFoXDTE1MDIwODIzNTk1OVowgcsxCzAJBgNVBAYT
AlVTMRcw
FQYDVQQKEw5WZXJpU2lnbiwgSW5jLjEwMC4GA1UECxMnRm9yIFRlc3Qg
UHVycG9z
ZXMgT25seS4gIE5vIGFzc3VyYW5jZXMuMUIwQAYDVQQLEzlUZXJtcyBv
ZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMp
MDUxLTAr
BgNVBAMTJFZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBD
```

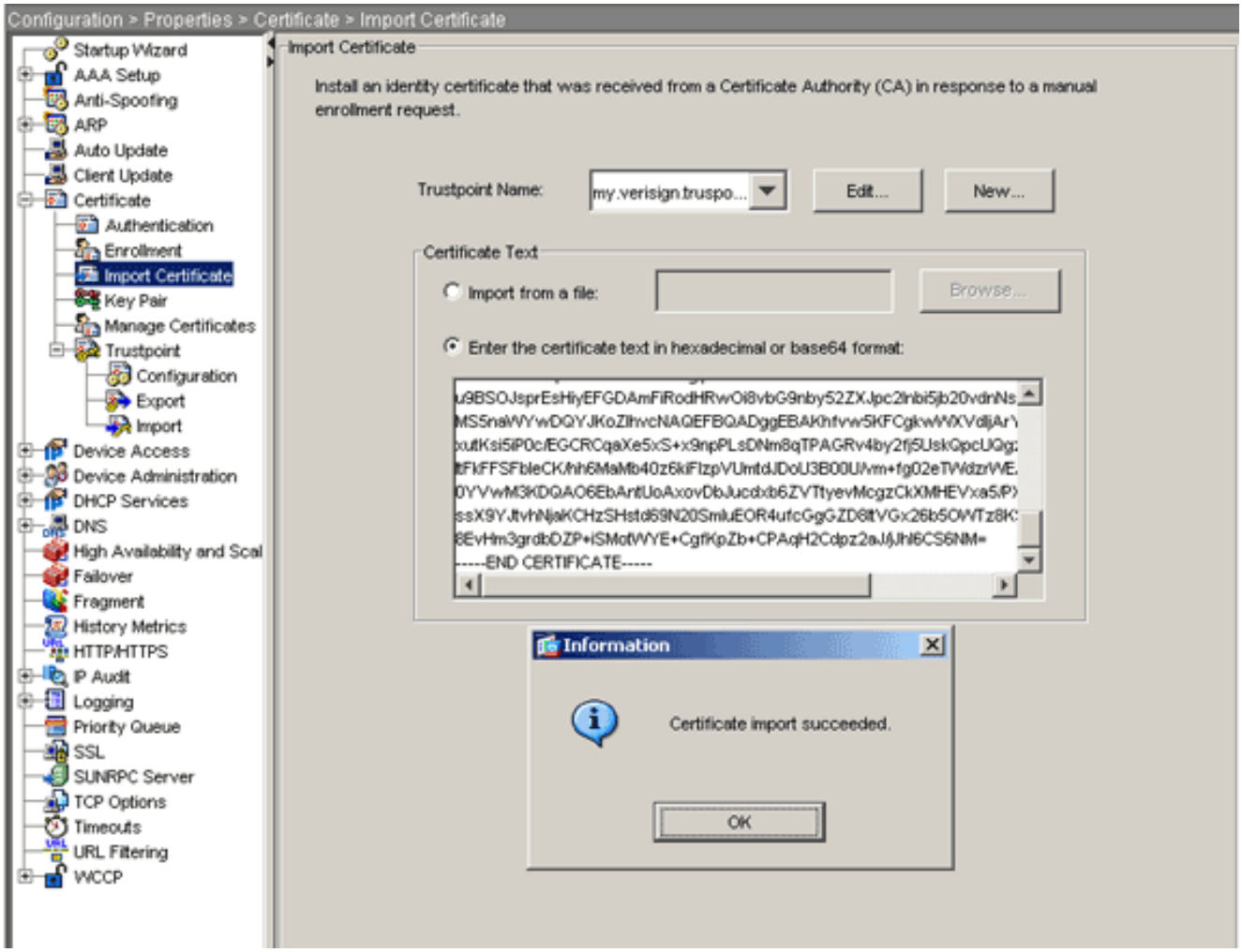
```
QTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAu
wElv6IJ/
DV8zgpvxuwdaMv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE6
1BBD6Zqk
d85lPl/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45
1P4qoyqS
E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1
D/OCCmZO
5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4tlqj97ydk5iDo
xjKfV6sb
tnp3TIY6S07bTb9gxJCk4pGbcf8DOPvOfGRu1wpfUUZC8v+WKC20+sK6
QMECAwEA
AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA
BgpghkgB
hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3LnZlcmlzaWdu
LmNvbS9j
cHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD
AgEGMB0G
A1UdDgQWBBRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGn
oYGSpIGP
MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x
MDAuBgNV
BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz
LjEyMDAG
A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJlIFNlcnZlciBUZXN0IFJv
b3QgQ0GC
ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/
SjzRvY2l
Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDDlwSRmiH3BW/SU
6EEzD9oi
Ai9TXvRIcD5q0mB+nyK9fB2aBzOiaiHSiIWzAJeQjuqA+Q93jNew+peu
j4AhdvGN
n/KK/+1Yv61w3+7g6ukFMARVBNg=
-----END CERTIFICATE-----
quit



! Manually pasted certificate into CLI. INFO:
Certificate has the following attributes: Fingerprint:
8de989db 7fcc5e3b fdde2c42 0813ef43 Do you accept this
certificate? [yes/no]: yes Trustpoint
'my.verisign.trustpoint' is a subordinate CA and holds a
non self-signed certificate. Trustpoint CA certificate
accepted. % Certificate successfully imported
ciscoasa(config)#
```

الخطوة 6. تثبيت الشهادة

إجراء ASDM

أستخدم شهادة الهوية المقدمة من مورد الطرف الثالث لتنفيذ الخطوات التالية:

1. انقر فوق **تكوين**، ثم انقر فوق **خصائص**.
2. قم بتوسيع **الشهادة**، ثم أختر **إستيراد الشهادة**.
3. انقر زر **إدخال نص التررخيص بتنسيق** لاسلكي **Base64 أو سداسي عشر**، وقم بلصق شهادة هوية Base64 في حقل
النص.



4. انقر فوق **استيراد**، ثم انقر فوق **موافق**.

مثال على سطر الأوامر

سيسكو اس

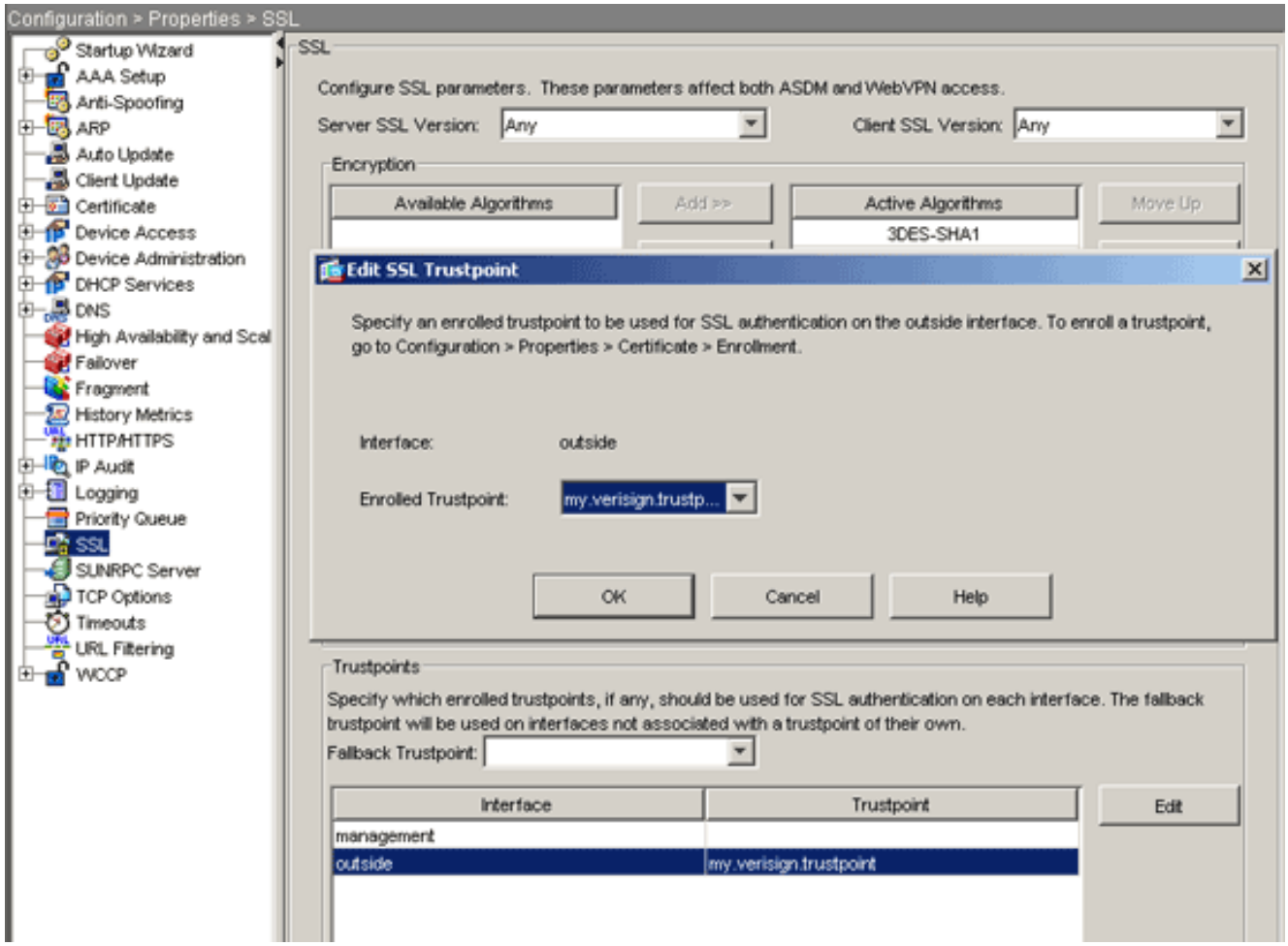
```
ciscoasa(config)#crypto ca import my.verisign.trustpoint
certificate

! Initiates prompt to paste the base64 identity
certificate ! provided by the 3rd party vendor. % The
fully-qualified domain name in the certificate will be:
webvpn.cisco.com Enter the base 64 encoded certificate.
End with the word "quit" on a line by itself -----BEGIN
CERTIFICATE-----
MIIFZjCCBE6gAwIBAgIQMs/oXuu9K14eMGSf0mYjfTANBgkqhkiG9w0B
AQUFADCB
yzELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAw
LgYDVQQL
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4x
QjBABgNV
BAsTOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5j
b20vY3Bz
L3Rlc3RjYSAoYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2Vj
dXJlIFN1
cnZlciBUZXN0IENBMB4XDTA3MDcyNjAwMDAwMFoXDTA3MDgwOTIzNTk1
OVowgbox
CzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3J0aCBDYXJvbGluYTEQMA4G
A1UEBxQH
UmFsZWlnaDEWMBQGA1UEChQNQ2lzY28gU3lzdGVtczEOMAwGA1UECxQF
VFNXRUIx
```

```
OjA4BgNVBAsUMVRlcm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29t
L2Nwcy90
ZXN0Y2EgKGMpMDUxHDAaBgNVBAMUE2Npc2NvYXNhMS5jaXNjby5jb20w
gZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL56EvorHHlsIB/VRKaRlJeJKCrQ
/9kER2JQ
9UOkUP3mVPZJtYN63ZxDwACeyNb+liIdKUegJWHI0Mz3GHqcgEkKW1Ec
rO+6aY1R
IaUE8/LiAZbA70+k/9Z/UR+v532B1nDRwbx1R9ZVhAJzA1hJTxSlEgry
osBMMazg
5IcLhgSpAgMBAAGjggHXMIIB0zAJBgNVHRMEAjAAMAsGA1UdDwQEAwIF
oDBDBgNV
HR8EPDA6MDigNqA0hjJodHRwOi8vU1ZSU2VjdXJlLWNybC52ZXJpc2ln
bi5jb20v
U1ZSVHJpYWwyMDA1LmNybDBKBgNVHSAEQzBBMD8GCmCGSAGG+EUBBxUw
MTAvBggr
BgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0
Y2EwHQYD
VR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMB8GA1UdIwQYMBaAFGYi
joHgMVnd
Kn+rRsU2AgZwJ4daMHgGCCsGAQUFBwEBBGwwajAkBggrBgEFBQcwAYYY
aHR0cDov
L29jc3AudmVyaXNpZ24uY29tMEIGCCsGAQUFBzAChjZodHRwOi8vU1ZS
U2VjdXJl
LWFpYS52ZXJpc2lnbi5jb20vU1ZSVHJpYWwyMDA1LWFpYS5jZXIwbgYI
KwYBBQUH
AQwEYjBgoV6gXDBaMFgwVhYJaW1hZ2UvZ2lmMCEwHzAHBgUrDgMCGgQU
S2u5KJYG
DLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29t
L3ZzbG9n
bzEuZ2lmMA0GCSqGSIb3DQEBBQUAA4IBAQAnym4GVThPIyL/9ylDBd8N
7/yW3Ov3
bIirHfHJyfPJ1znZQXyXdObpZkuA6Jyu03V2CYNnDomn4xRXQTUDD8q8
6ZiKyMIj
XM2VCmcHSajmMMRyjpydxfk6CIdDMtMGotCavRHD9Tl2tvwgrBock/v/
54o02lkB
SmLzVV7crlYJEuhgqu3Pz7qNRd8N0Un6c9sbwQ1BuM99QxzIzdAo89FS
ewy8MAIY
rtab5F+oiTc5xGy8w7NARAfNgFXihqnLgWTtA35/oWuy86bje1IWbeyq
j8ePM9Td
0LdAw6kUU1PNimPttMDhcF7cuevntROksOgQPBPx5FJSqMiUZGrvju5O
-----END CERTIFICATE-----
quit

INFO: Certificate successfully imported
ciscoasa(config)#
```

الخطوة 7. تكوين WebVPN لاستخدام الشهادة المثبتة حديثا

إجراء ASDM

1. انقر فوق **تكوين**، ثم انقر فوق **خصائص**، ثم أختر **SSL**.
2. في منطقة TrustPoints، حدد الواجهة التي سيتم إستخدامها لإنهاء جلسات عمل WebVPN. (يستخدم هذا المثال الواجهة الخارجية.)
3. انقر فوق **تحرير**.يظهر مربع الحوار تحرير SSL TrustPoint.



4. من القائمة المنسدلة TrustPoint المسجلة، أختر نقطة الثقة التي قمت بإنشائها في الخطوة 3.
5. انقر فوق **موافق**، ثم انقر فوق **تطبيق**.

يجب إستخدام شهادتك الجديدة الآن لجميع جلسات عمل WebVPN التي تنتهي على الواجهة المحددة. راجع قسم التحقق في هذا المستند للحصول على معلومات حول كيفية التحقق من التثبيت الناجح.

مثال على سطر الأوامر

سيسكو اسا

```
ciscoasa(config)#ssl trust-point my.verisign.trustpoint
outside

! Specifies the trustpoint that will supply the SSL !
certificate for the defined interface.
ciscoasa(config)#write memory

Building configuration...
Cryptochecksum: 694687a1 f75042af ccc6addf 34d2cb08

8808 bytes copied in 3.630 secs (2936 bytes/sec)
[OK]
ciscoasa(config)#

! Save configuration.
```

التحقق من الصحة

يوضح هذا القسم كيفية تأكيد نجاح تثبيت شهادة مورد الجهة الخارجية.

إستبدال الشهادة الموقعة ذاتيا من ASA

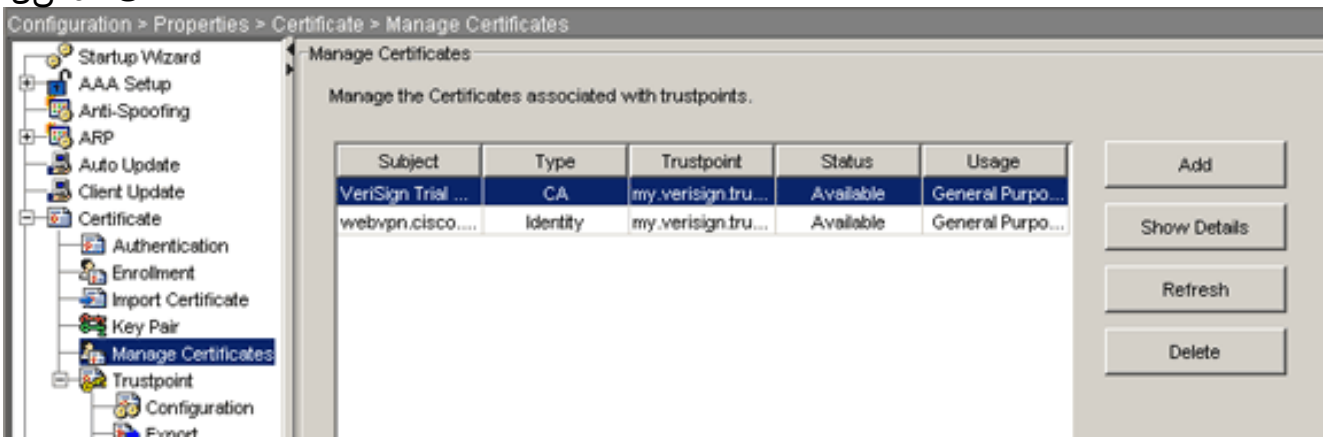
يوضح هذا القسم كيفية إستبدال الشهادة الموقعة ذاتيا والمثبتة من ASA.

1. قم بإصدار طلب توقيع شهادة للإصدار.بعد أن تستلم الشهادة المطلوبة من Verising، يمكنك تثبيتها مباشرة تحت نفس TrustPoint.
2. اكتب هذا الأمر: **إصدار تسجيل التشفير**فيطلب منك ان تجيب عن الاسئلة.
3. لعرض "طلب شهادة العرض" للإنهاء، أدخل **نعم**، وأرسل الإخراج إلى الإصدار.
4. بمجرد أن يعطوك الشهادة الجديدة، اكتب هذا الأمر: **تشفير ca إستيراد شهادة إصدار**

عرض الشهادات المثبتة

إجراء ASDM

1. طقطقت **تشكيل**، وطقطقت **خاصية**.
2. قم بتوسيع **التر**خيص، واختر **إدارة الشهادات**.يجب أن تظهر شهادة المرجع المصدق المستخدمة لمصادقة TrustPoint وشهادة الهوية التي تم إصدارها من قبل مورد الطرف الثالث في منطقة إدارة الشهادات.



مثال على سطر الأوامر

سيسكو اس

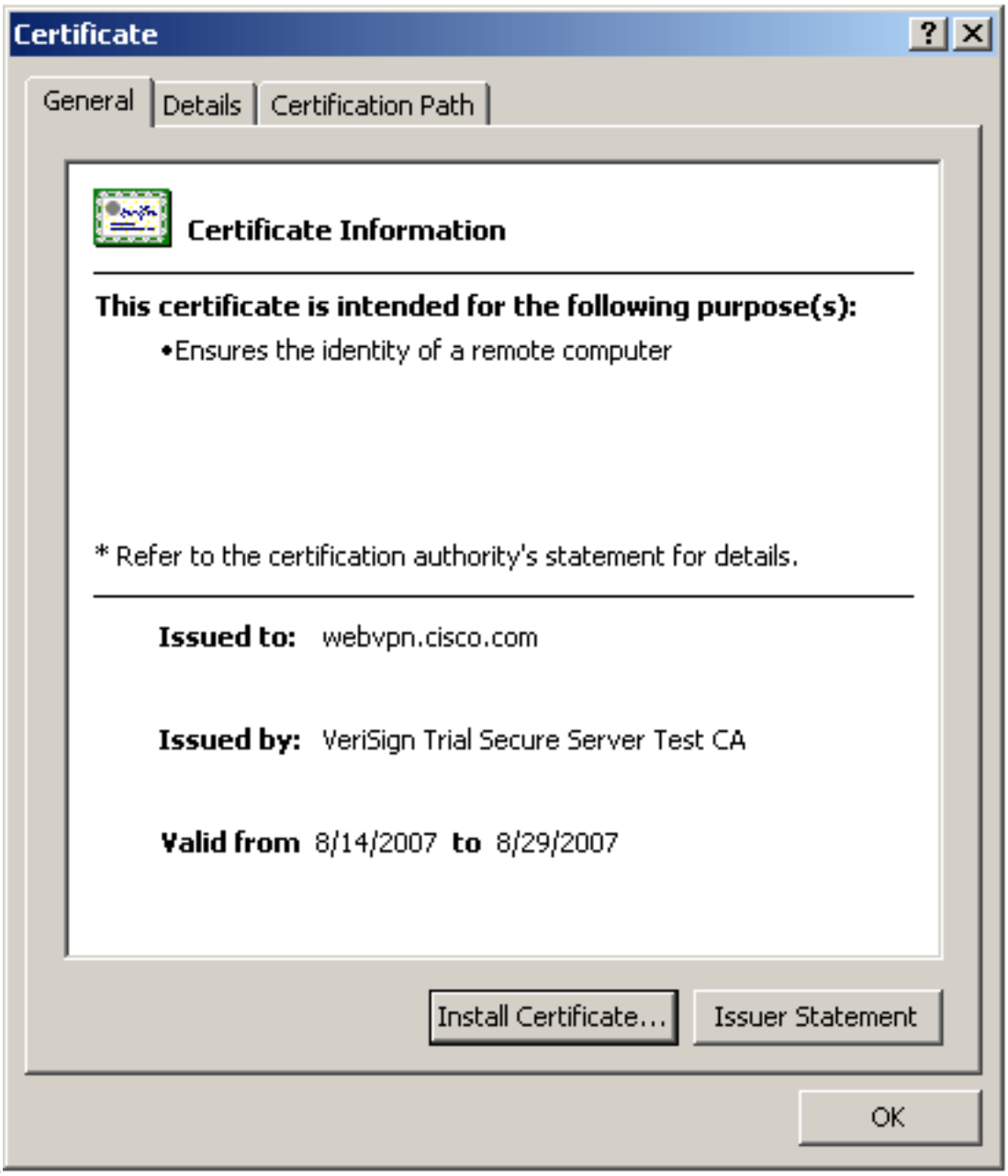
```
ciscoasa(config)#show crypto ca certificates

! Displays all certificates installed on the ASA.
Certificate Status: Available Certificate Serial Number:
32cfe85eebbd2b5e1e30649fd266237d Certificate Usage:
General Purpose Public Key Type: RSA (1024 bits) Issuer
Name: cn=VeriSign Trial Secure Server Test CA ou=Terms
of use at https://www.verisign.com/cps/testca (c)05
ou=For Test Purposes Only. No assurances. o=VeriSign\,
Inc. c=US Subject Name: cn=webvpn.cisco.com ou=Terms of
use at www.verisign.com/cps/testca (c)05 ou=TSWEB
o=Cisco Systems l=Raleigh st=North Carolina c=US OCSP
AIA: URL: http://ocsp.verisign.com CRL Distribution
Points: [1] http://SVRSecure-
crl.verisign.com/SVRTrial2005.crl Validity Date: start
date: 00:00:00 UTC Jul 19 2007 end date: 23:59:59 UTC
Aug 2 2007 Associated Trustpoints:
```

```
my.verisign.trustpoint ! Identity certificate received
from 3rd party vendor displayed above. CA Certificate
Status: Available Certificate Serial Number:
63b1a5cdc59f78801da0636cf975467b Certificate Usage:
General Purpose Public Key Type: RSA (2048 bits) Issuer
Name: cn=VeriSign Trial Secure Server Test Root CA
ou=For Test Purposes Only. No assurances. o=VeriSign\,
Inc. c=US Subject Name: cn=VeriSign Trial Secure Server
Test CA ou=Terms of use at
https://www.verisign.com/cps/testca (c)05 ou=For Test
Purposes Only. No assurances. o=VeriSign\, Inc. c=US
Validity Date: start date: 00:00:00 UTC Feb 9 2005 end
date: 23:59:59 UTC Feb 8 2015 Associated Trustpoints:
my.verisign.trustpoint ! CA intermediate certificate
displayed above.
```

التحقق من تثبيت الشهادة ل WebVPN باستخدام مستعرض ويب

للتحقق من إستخدام WebVPN للشهادة الجديدة، أكمل الخطوات التالية:

1. الاتصال بواجهة WebVPN من خلال مستعرض ويب. أستخدم https:// مع FQDN التي أستخدمتها لطلب الشهادة (على سبيل المثال، https://webvpn.cisco.com).إذا تلقيت أحد تنبيهات الأمان هذه، فقم بتنفيذ الإجراء المتوافق مع هذا التنبيه:**اسم شهادة الأمان غير صحيح أو أن الاتصال تم قطعه مع اسم المضيف**تحقق من إستخدام FQDN/CN الصحيح للاتصال بواجهة WebVPN الخاصة ب ASA. يجب إستخدام FQDN/CN الذي قمت بتعريفه عند طلب شهادة الهوية. يمكنك إستخدام الأمر **show crypto ca certificates trustPointName** للتحقق من الشهادات FQDN/CN.**تم إصدار شهادة الأمان من قبل شركة لم تختر الوثوق بها...**أكمل الخطوات التالية لتثبيت شهادة جذر مورد الجهة الخارجية في مستعرض الويب الخاص بك:في شاشة تنبيه التأمين، انقر **عرض الشهادة**.في شاشة الترخيص، انقر على صفحة **مسار الترخيص**.حدد شهادة المرجع المصدق الموجودة فوق شهادة الهوية الصادرة، وانقر فوق **عرض الشهادة**.انقر على **تثبيت الشهادة**.في شاشة معالج "تثبيت الشهادات"، انقر على **التالي**.حدد **تحديد مخزن الشهادات تلقائيا بناء** على نوع زر الخيار، وانقر **التالي**، ثم انقر على **إنهاء**.انقر على **نعم** عندما تستلم مطالبة تأكيد تثبيت الشهادة.في المطالبة الخاصة بعملية الاستيراد التي نجحت، انقر فوق **موافق**، ثم انقر فوق **نعم**.**ملاحظة:** بما أن هذا المثال يستخدم شهادة الإصدار التجريبي، فيجب تثبيت شهادة جذر CA للإصدار التجريبي لتجنب أخطاء التحقق من الصحة عند اتصال المستخدمين.
2. انقر نقرا مزدوجا على أيقونة القفل التي تظهر في الركن السفلي الأيمن من صفحة تسجيل الدخول إلى WebVPN.يجب أن تظهر معلومات الشهادة المثبتة.
3. راجع المحتويات للتحقق من مطابقتها لشهادة مورد الجهات



الخارجية.

خطوات تجديد شهادة SSL

أكمل الخطوات التالية لتجديد شهادة SSL:

1. حدد نقطة الثقة التي تحتاج إلى تجديدها.
2. أختر **التسجيل**.تظهر هذه الرسالة:*إذا تم تسجيله مرة أخرى بنجاح، سيتم إستبدال الوحدة الحالية بأخرى جديدة. هل تريد المتابعة؟*
3. أختر **نعم**.سيؤدي هذا إلى إنشاء CSR جديد.
4. قم بإرسال CSR إلى المرجع المصدق الخاص بك ثم قم باستيراد شهادة المعرف الجديدة عند استعادتها.
5. قم بإزالة نقطة الثقة وإعادة تطبيقها على الواجهة الخارجية.

الأوامر

على ال ASA، أنت يستطيع استعملت عدة عرض أمر في الأمر خط أن يدقق الحالة من شهادة.

- **show crypto ca trustPoint**— يعرض نقاط الثقة المكونة.

- **show crypto ca certificate**—يعرض جميع الشهادات المثبتة على النظام.
- **show crypto ca crl**—يعرض قوائم إبطال الشهادات المخزنة مؤقتا (CRL).
- **show crypto key mypubkey rsa**— يعرض جميع أزواج مفاتيح التشفير التي تم إنشاؤها.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

فيما يلي بعض الأخطاء المحتملة التي قد تواجهها:

- **تحذير: لم يتم العثور على شهادة CA. قد لا تكون الشهادات المستردة هي** ٪ **usable.INFO: تم استيراد الشهادة بنجاح**لم تتم مصادقة شهادة المرجع المصدق بشكل صحيح. أستخدم الأمر show crypto ca certificate trustPointName للتحقق من تثبيت شهادة CA. ابحث عن السطر الذي يبدأ بشهادة المرجع المصدق. إذا كانت شهادة المرجع المصدق مثبتة، فتحقق من أنها تشير إلى TrustPoint الصحيح.
- خطأ: فشل تحليل الشهادة المستردة أو التحقق منها يمكن أن يحدث هذا الخطأ عندما تقوم بتثبيت شهادة الهوية وليس لديك شهادة CA الوسيطة أو الجذر الصحيحة التي تم مصادقتها مع TrustPoint المقترنة. يجب عليك إزالة وإعادة المصادقة باستخدام شهادة CA الوسيطة أو الجذر الصحيحة. اتصل بمورد الجهة الخارجية للتحقق من أنك إستلمت شهادة المرجع المصدق الصحيحة.
- لا تحتوي الشهادة على مفتاح عام للأغراض العامةقد يحدث هذا الخطأ عند محاولة تثبيت شهادة هويتك في TrustPoint غير صحيح. تحاول تثبيت شهادة هوية غير صحيحة، أو أن زوج المفاتيح المقترن ب TrustPoint لا يطابق المفتاح العام الموجود في شهادة الهوية. أستخدم الأمر **show crypto ca certificates** *trustPointName* للتحقق من تثبيت شهادة هويتك على TrustPoint الصحيح. ابحث عن السطر الذي يحدد *نقاط الثقة المرتبطة:* إذا تم سرد نقطة الثقة غير الصحيحة، فاستخدم الإجراءات الموضحة في هذا المستند لإزالة نقطة الثقة المناسبة وإعادة تثبيتها عليها، تحقق أيضا من أن أزواج المفاتيح لم تتغير منذ إنشاء CSR.
- **رسالة الخطأ: ٪PIX|ASA-3-717023 SSL فشل في تعيين شهادة الجهاز ل trustPoint [trustPoint name]**تظهر هذه الرسالة عند حدوث فشل عند تعيين شهادة جهاز ل TrustPoint المحددة لمصادقة اتصال SSL. عند ظهور اتصال SSL، يتم إجراء محاولة لتعيين شهادة الجهاز التي سيتم إستخدامها. في حالة حدوث فشل، يتم تسجيل رسالة خطأ تتضمن TrustPoint التي تم تكوينها والتي يجب إستخدامها لتحميل شهادة الجهاز وسبب الفشل.*اسم TrustPoint—اسم TrustPoint الذي فشل SSL في تعيين شهادة جهاز له.***الإجراء الموصى به:** حل المشكلة التي يشير إليها السبب الذي تم الإبلاغ عنه للفشل.تأكد من تسجيل TrustPoint المحدد ومن وجود شهادة جهاز.تأكد من صحة شهادة الجهاز.إعادة تسجيل نقطة الثقة، إذا لزم الأمر.

معلومات ذات صلة

- [كيفية الحصول على شهادة رقمية من Microsoft Windows CA باستخدام ASDM على ASA]
- [إعلامات حقل منتج الأمان]
- [طلبات التعليقات (RFCs)]
- [الدعم التقني والمستندات - Cisco Systems]

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).