

SSL ةداهش تي بثت و دي دجت :ASA 8.x ASDM مادختساب

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [الإجراء](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [كيفية نسخ شهادات SSL من ASA إلى آخر](#)
- [معلومات ذات صلة](#)

المقدمة

الإجراء الوارد في هذا المستند هو مثال ويمكن استخدامه كدليل إرشادي مع أي مورد شهادات أو خادم شهادات رئيسي خاص بك. قد يتطلب مورد الشهادة الخاص متطلبات معلمة الشهادة الخاصة، ولكن هذا المستند يهدف إلى توفير الخطوات العامة المطلوبة لتجديد شهادة SSL وتثبيتها على ASA الذي يستخدم برنامج 8.0.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

يتعلق هذا الإجراء بإصدارات ASA 8.x مع الإصدار 6.0(2) من ASDM أو الإصدارات الأحدث.

يستند الإجراء الوارد في هذا المستند إلى تكوين صالح مع تثبيت شهادة واستخدامها للوصول إلى SSL VPN. لا يؤثر هذا الإجراء على شبكتك طالما لم يتم حذف الشهادة الحالية. هذا الإجراء هو عملية تدريجية حول كيفية إصدار CSR جديد لشهادة حالية بنفس شهادة الجذر التي أصدرت المرجع المصدق الجذر الأصلي.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. 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.](#)

أكمل الخطوات التالية:

1. حدد الشهادة التي تريد تجديدها تحت التكوين < إدارة الأجهزة > شهادات الهوية، ثم انقر على إضافة. شكل 1

The screenshot shows the Cisco ASDM 6.1 for ASA web interface. The main content area displays a table of Identity Certificates. The table has the following data:

Issued To	Issued By	Expiry Date	Usage
cn=*.vpn1.com	cn=MS-CA	00:03:15 UTC Mar 11 2009	General Purpose

Below the table, there is a note: "Identity certificate can be used to authenticate SSL, such as ASDM, access to the security appliance on a given interface. You can go to [SSL Settings](#) to make such configuration."

The interface also includes a navigation tree on the left with "Identity Certificates" selected, and a status bar at the bottom showing "Device configuration refreshed successfully." and the time "3/29/08 8:52:53 PM UTC".

2. تحت إضافة شهادة هوية، حدد زر إضافة شهادة هوية جديدة، واختر زوج المفاتيح من القائمة المنسدلة. ملاحظة: لا يوصى باستخدام <default-RSA-key> لأنك إذا قمت بإعادة إنشاء مفتاح SSH الخاص بك، فأنت تبطل ترخيصك. إذا لم يكن لديك مفتاح RSA، فأكمل الخطوات A و B. وإلا استمر في الخطوة 3. شكل 2

Add Identity Certificate

Import the identity certificate from a file:

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

(إختياري) أكمل هذه الخطوات إذا لم يكن لديك مفتاح RSA تم تكوينه بعد، وإلا فانتقل إلى الخطوة 3. طقطقت جديد....أدخل اسم زوج المفاتيح في حقل إدخال اسم زوج مفاتيح جديد، وانقر إنشاء الآن. شكل 3

Add Key Pair

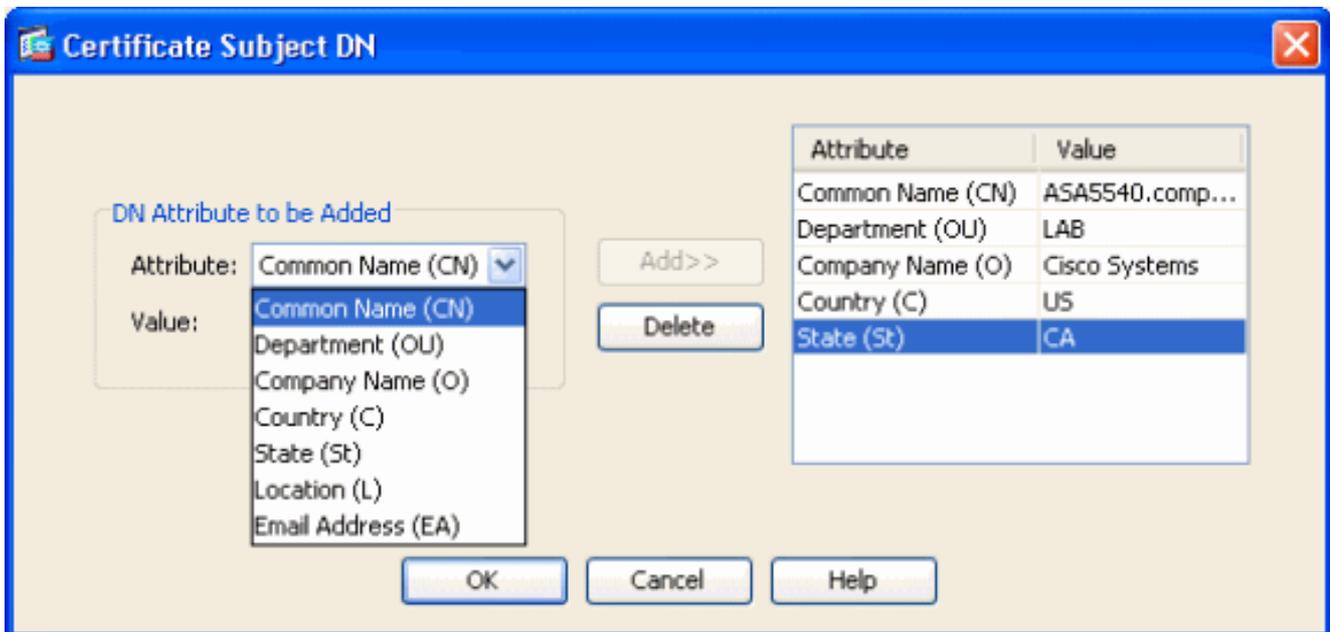
Name: Use default key pair name

Enter new key pair name:

Size:

Usage: General purpose Special

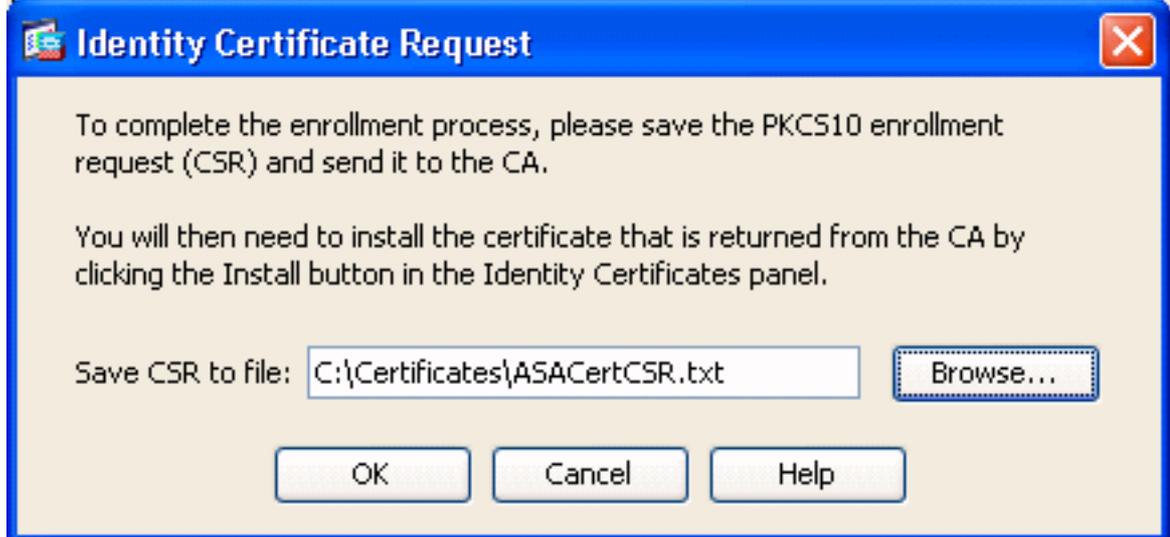
3. انقر فوق تحديد.
4. أدخل سمات الشهادة المناسبة كما هو موضح في الشكل 4. طقطقت ما إن يتم، ok. ثم انقر على إضافة شهادة. الشكل 4



إخراج واجهة سطر الأوامر:

```
crypto ca trustpoint ASDM_TrustPoint0
    keypair CertKey
    id-usage ssl-ipsec
    fqdn 5540-uwe
subject-name CN=ASA5540.company.com,OU=LAB,O=Cisco systems,C=US,St=CA
enrollment terminal
crypto ca enroll ASDM_TrustPoint0
```

5. في الإطار المنبثق طلب شهادة الهوية، احفظ طلب توقيع الشهادة (CSR) في ملف نصي، وانقر موافق. شكل 5



6. (إختياري) تحقق في ASDM من أن CSR معلق، كما هو موضح في الشكل 6. الشكل 6

Cisco ASDM 6.1 for ASA - 172.16.242.232

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Management Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Usage
[cn=*,vpn1.com]	[cn=MS-CA]	00:03:16 UTC Mar 11 2009	General Purpose
[ASA5540.company.com]	[Not Available]	Pending...	Unknown

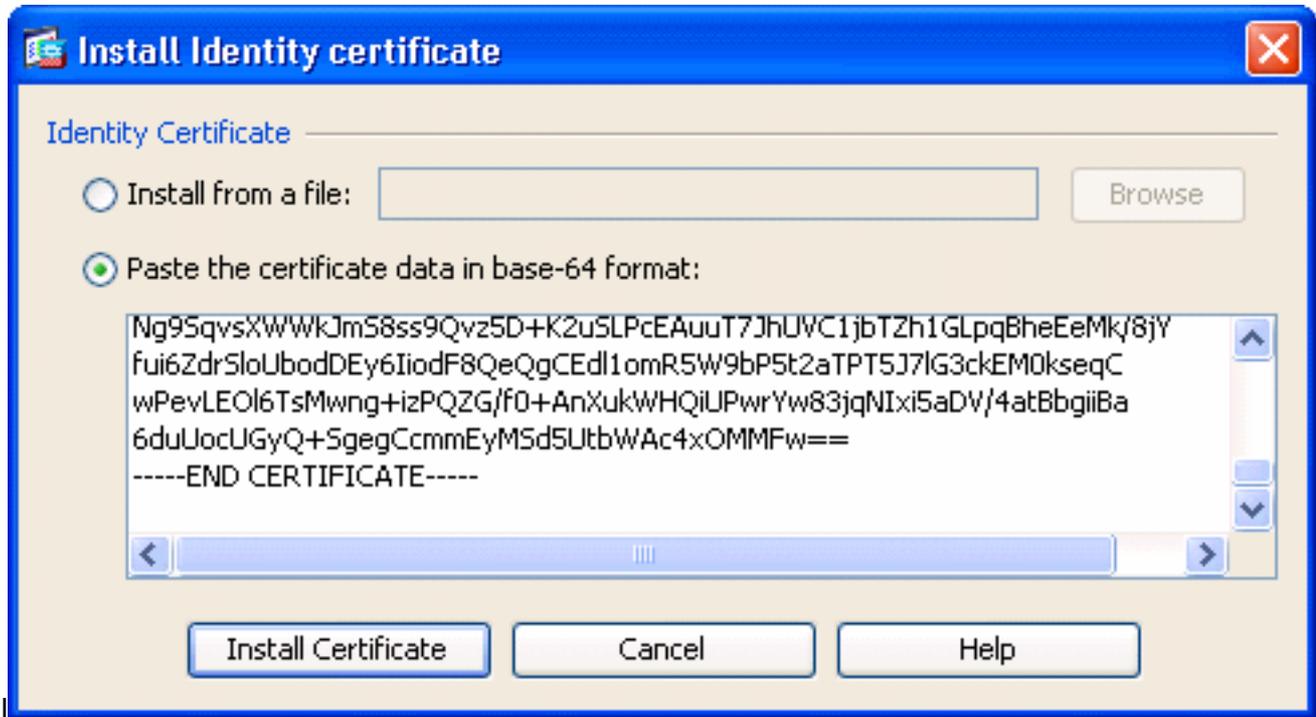
Identity certificate can be used to authenticate SSL, such as ASDM, access to the security appliance on a given interface. You can go to [SSL Settings](#) to make such configuration.

Apply Reset

Configuration changes saved successfully.

3/29/08 9:56:23 PM UTC

7. أرسل طلب الشهادة إلى مسؤول الشهادة الذي يصدر الشهادة على الخادم. يمكن أن يكون ذلك من خلال واجهة ويب، بريد إلكتروني، أو مباشرة إلى خادم CA الجذر لعملية إصدار الشهادة.
8. أكمل هذه الخطوات لتثبيت الشهادة المتجددة. حدد طلب الشهادة المعلقة تحت تشكيل < إدارة الأجهزة > شهادات الهوية، كما هو موضح في الشكل 6، وانقر **تثبيت**. في نافذة "تثبيت شهادة الهوية"، حدد زر الخيار **لصق بيانات الشهادة بتنسيق base-64**، وانقر على **تثبيت الشهادة**. ملاحظة: بدلا من ذلك، إذا تم إصدار الشهادة في ملف cer. بدلا من ملف نصي أو بريد إلكتروني، يمكنك أيضا تحديد **تثبيت من ملف**، والتصفح إلى الملف المناسب على الكمبيوتر، وانقر فوق **تثبيت ملف شهادة المعرف** ثم انقر فوق **تثبيت الشهادة**. الشكل 7



خارج واجهة سطر الأوامر:

```
crypto ca import ASDM_TrustPoint0 certificate
WIID2DCCAsCgAwIBAgIKYb9wewAAAAAAJzANBgkqhkiG9w0BAQUFADAQMQ
output truncated wPevLEO16TsMwng+izPQZG/f0+AnXukWHQiUPwrYw83jqNixi5aDV/4atBbgiiBa ---!
6duUocUGyQ+SgegCcmEyMSd5UtbWAc4xOMMFw== quit
```

9. يظهر إطار يؤكد أن الشهادة مثبتة بنجاح. انقر فوق "موافق" للتأكيد. الشكل 8



10. تأكد من ظهور شهادتك الجديدة تحت شهادات الهوية. الشكل 9

Cisco ASDM 6.1 for ASA - 172.16.242.232

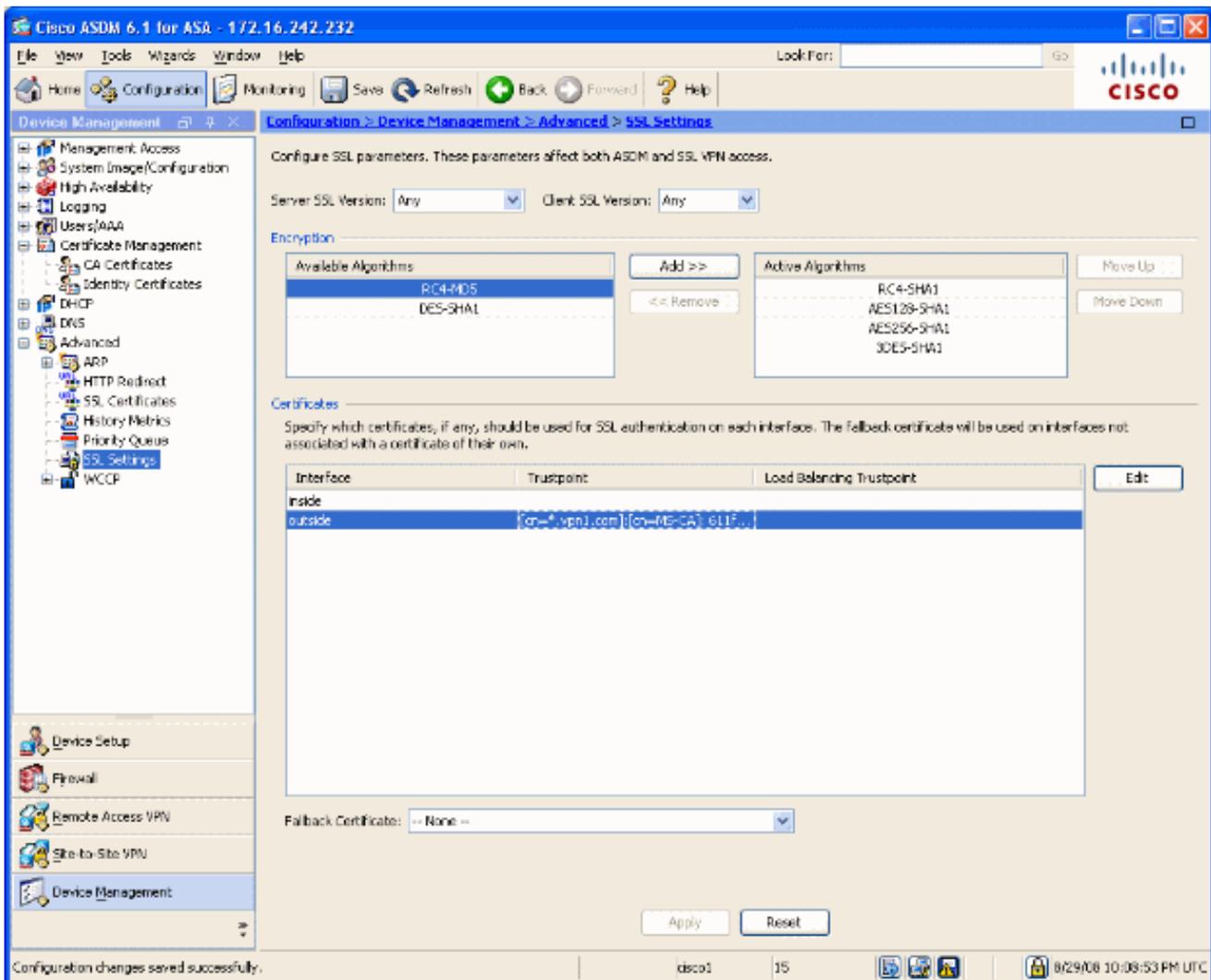
Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Usage
[cn=*@spnt.com]	[cn=MS-CA]	00:03:16 UTC Mar 11 2009	General Purpose
[cn=ASAS540.company.com...]	[cn=MS-CA]	22:49:31 UTC Aug 29 2009	General Purpose

Identity certificate can be used to authenticate SSL, such as ASDM, access to the security appliance on a given interface. You can go to [SSL Settings](#) to make such configuration.

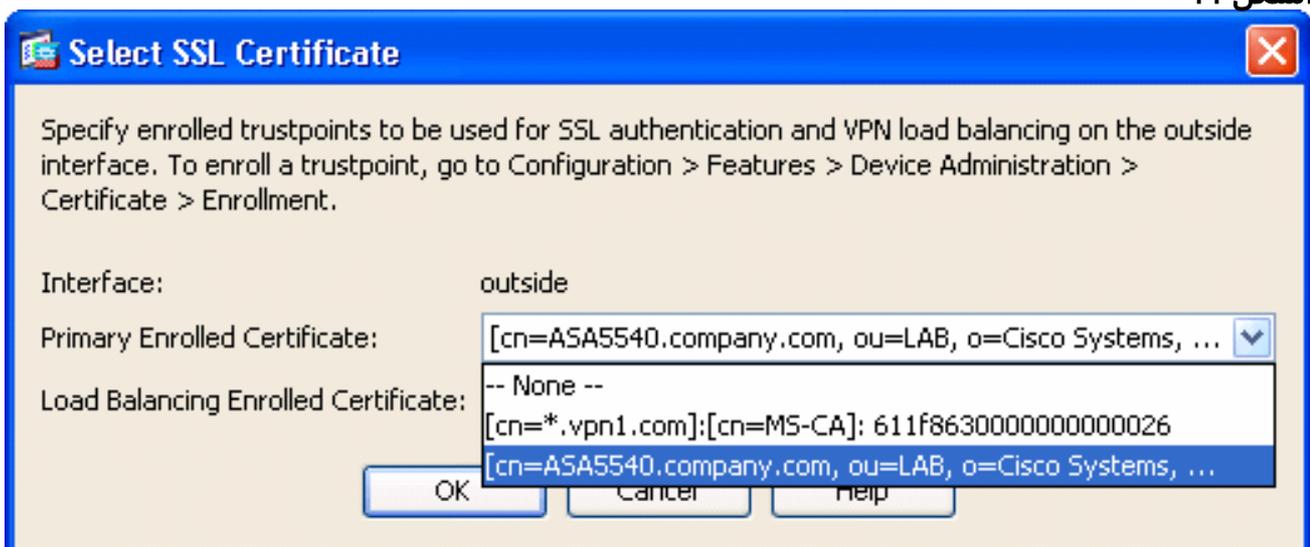
Configuration changes saved successfully.

11. أتمت هذا steps in order to ربطت الشهادة الجديدة إلى القارن:أختر التكوين < إدارة الأجهزة > خيارات متقدمة < إعدادات SSL، كما هو موضح في الشكل 10. حدد الواجهة الخاصة بك تحت الشهادات، وانقر تحرير.الشكل 10



12. أختَر ترخيصك الجديد من القائمة المنسدلة، وانقر موافق، وانقر تطبيق.
 ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1
 ssl trust-point ASDM_TrustPoint0 outside

الشكل 11



13. احفظ التكوين الخاص بك في ASDM أو على واجهة سطر الأوامر.

[التحقق من الصحة](#)

يمكنك استخدام واجهة سطر الأوامر (CLI) للتحقق من تثبيت الشهادة الجديدة على ASA بشكل صحيح، كما هو موضح في إخراج النموذج هذا:

```

ASA(config)#show crypto ca certificates
Certificate
Status: Available
Certificate Serial Number: 61bf707b000000000027
Certificate Usage: General Purpose
(Public Key Type: RSA (1024 bits)
:Issuer Name
cn=MS-CA
:Subject Name
cn=ASA5540.company.com !---new certificate ou=LAB o=Cisco Systems st=CA c=US CRL
Distribution Points: [1] http://win2k3-basel/CertEnroll/MS-CA.crl [2] file://\win2k3-
basel\CertEnroll\MS-CA.crl Validity Date: start date: 22:39:31 UTC Aug 29 2008 end date:
22:49:31 UTC Aug 29 2009 Associated Trustpoints: ASDM_TrustPoint0 CA Certificate Status:
Available Certificate Serial Number: 211020a79cfd96b34ba93f3145d8e571 Certificate Usage:
Signature Public Key Type: RSA (2048 bits) Issuer Name: cn=MS-CA Subject Name: cn=MS-CA !---
'old' certificate CRL Distribution Points: [1] http://win2k3-basel/CertEnroll/MS-CA.crl [2]
file://\win2k3-basel\CertEnroll\MS-CA.crl Validity Date: start date: 00:26:08 UTC Jun 8 2006
end date: 00:34:01 UTC Jun 8 2011 Associated Trustpoints: test Certificate Status: Available
Certificate Serial Number: 611f8630000000000026 Certificate Usage: General Purpose Public Key
Type: RSA (1024 bits) Issuer Name: cn=MS-CA Subject Name: cn=*.vpn1.com CRL Distribution Points:
[1] http://win2k3-basel/CertEnroll/MS-CA.crl [2] file://\win2k3-basel\CertEnroll\MS-CA.crl
Validity Date: start date: 23:53:16 UTC Mar 10 2008 end date: 00:03:16 UTC Mar 11 2009
#(Associated Trustpoints: test ASA(config)

```

استكشاف الأخطاء وإصلاحها

(إختياري) تحقق على واجهة سطر الأوامر (CLI) من تطبيق الشهادة الصحيحة على الواجهة:

```

ASA(config)#show running-config ssl
ssl trust-point ASDM_TrustPoint0 outside
Shows that the correct trustpoint is tied to the outside interface that terminates SSL VPN. ---!
#(ASA(config)

```

كيفية نسخ شهادات SSL من ASA إلى آخر

يمكن القيام بذلك إذا قمت بإنشاء مفاتيح قابلة للتصدير. تحتاج لتصدير الترخيص إلى ملف PKCS. ويتضمن ذلك تصدير جميع المفاتيح المقترنة.

أستخدم هذا الأمر لتصدير شهادتك عبر CLI:

```
ASA(config)#crypto ca export
```

ملاحظة: عبارة المرور - تستخدم لحماية ملف PKCS12.

أستخدم هذا الأمر لاستيراد ترخيصك عبر CLI:

```
SA(config)#crypto ca import
```

ملاحظة: يجب أن تكون عبارة المرور هذه هي نفسها المستخدمة عند تصدير الملف.

كما يمكن القيام بذلك من خلال ASDM لزوج تجاوز فشل ASA. أكمل الخطوات التالية لتنفيذ ما يلي:

1. قم بتسجيل الدخول إلى ASA الأساسي عبر ASDM واختر أدوات—> تكوين النسخ الاحتياطي.
2. يمكنك نسخ كل شيء احتياطياً أو الشهادات فقط.
3. في وضع الاستعداد، افتح ASDM واختر أدوات—> إستعادة التكوين.

معلومات ذات صلة

- [صفحة دعم أجهزة الأمان المعدلة \(ASA\) من Cisco](#)
- [ASA 8.x يركب يدويا شهادات مورد الطرف الثالث للاستخدام مع مثال تكوين WebVPN](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن مة و مچم مادختساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء ن أ عي مچ ي ف ن ي م دختسمل ل معد ي و تحم م ي دقتل ل ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ل أ مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ل ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ل ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (رف و تم ط بار ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا