

# Exemple de configuration de l'installation manuelle de certificats de fournisseurs tiers dans ASA 7.x pour une utilisation avec WebVPN

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Étape 1. Vérifiez que les valeurs Date, Time et Time Zone sont exactes](#)

[Étape 2. Générer la paire de clés RSA](#)

[Étape 3. Créer un point de confiance](#)

[Étape 4. Générer l'inscription au certificat](#)

[Étape 5. Authentifier le point de confiance](#)

[Étape 6. Installer le certificat](#)

[Étape 7. Configurer WebVPN pour utiliser le certificat récemment installé](#)

[Vérification](#)

[Remplacer le certificat auto-signé d'ASA](#)

[Afficher les certificats installés](#)

[Vérification du certificat installé pour WebVPN à l'aide d'un navigateur Web](#)

[Étapes de renouvellement du certificat SSL](#)

[Commandes](#)

[Dépannage](#)

[Informations connexes](#)

## Introduction

Cet exemple de configuration décrit comment installer manuellement un certificat numérique tiers sur l'ASA pour une utilisation avec WebVPN. Un certificat d'évaluation Verisign est utilisé dans cet exemple. Chaque étape contient la procédure d'application ASDM et un exemple CLI.

## Conditions préalables

### Conditions requises

Ce document nécessite que vous ayez accès à une autorité de certification (CA) pour l'inscription de certificat. Les fournisseurs de CA tiers pris en charge sont Baltimore, Cisco, Entrust, iPlanet/Netscape, Microsoft, RSA et VeriSign.

### Components Used

Ce document utilise un ASA 5510 qui exécute le logiciel version 7.2(1) et ASDM version 5.2(1). Cependant, les procédures de ce document fonctionnent sur n'importe quel appareil ASA qui exécute 7.x avec n'importe quelle version ASDM compatible.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

## Configuration

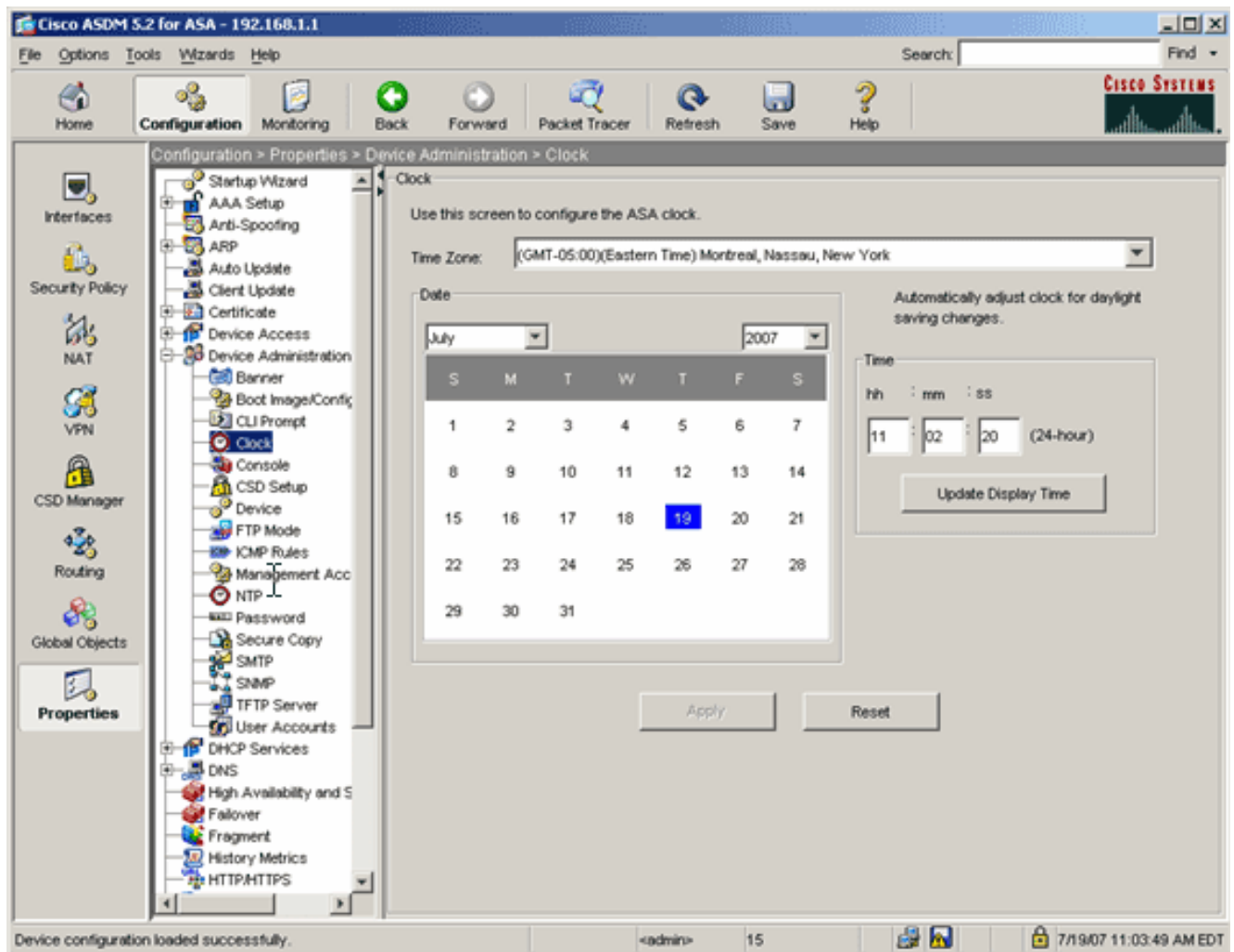
Afin d'installer un certificat numérique de fournisseur tiers sur le PIX/ASA, procédez comme suit :

1. [Vérifiez que les valeurs Date, Heure et Fuseau horaire sont Exactes](#).
2. [Générez la paire de clés RSA](#).
3. [Créez le point de confiance](#).
4. [Générez l'inscription au certificat](#).
5. [Authentifiez le point de confiance](#).
6. [Installez le certificat](#).
7. [Configurez WebVPN pour utiliser le nouveau certificat installé](#).

### Étape 1. Vérifiez que les valeurs Date, Time et Time Zone sont exactes

#### Procédure ASDM

1. Cliquez sur Configuration, et ensuite sur Properties.
2. Développez Device Administration, puis sélectionnez Clock.
3. Vérifiez que les informations répertoriées sont correctes. Les valeurs de Date, Time et Time Zone doivent être exactes pour que la validation du certificat soit correcte.



## Exemple de ligne de commande

```

ciscoasa
-----
ciscoasa#show clock

11:02:20.244 UTC Thu Jul 19 2007
ciscoasa

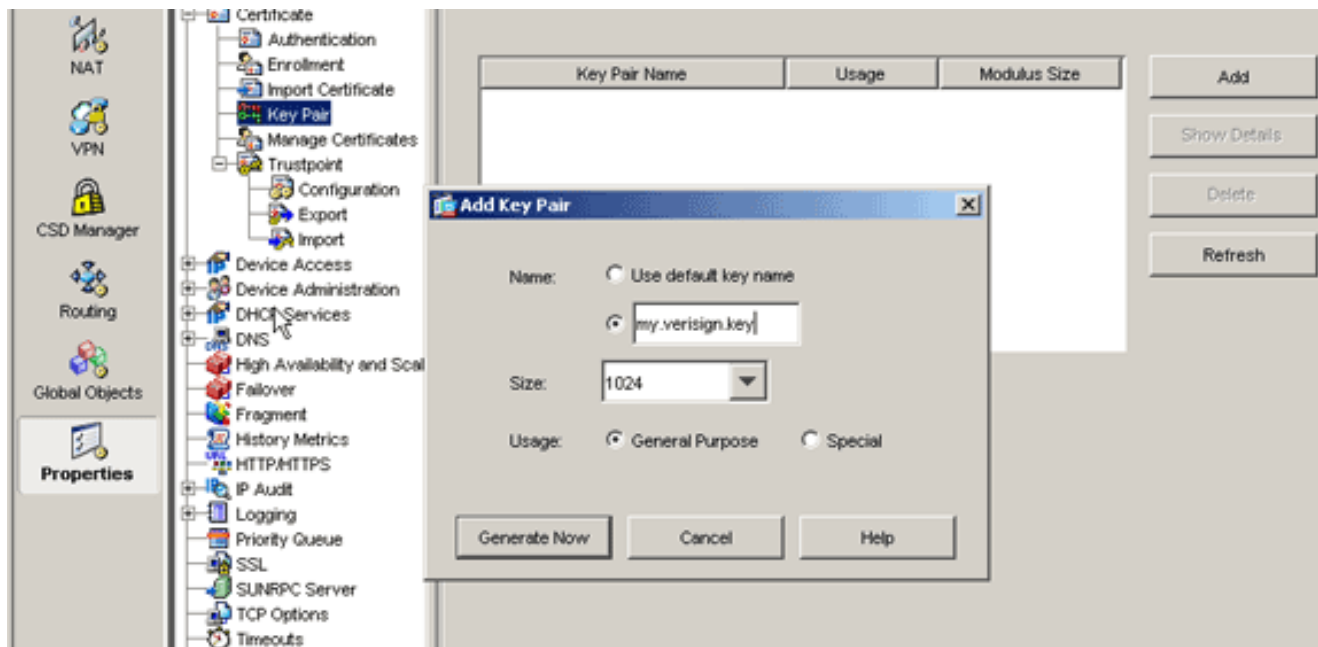
```

## Étape 2. Générer la paire de clés RSA

La clé publique RSA générée est associée aux informations d'identité de l'ASA pour former une demande de certificat PKCS#10. Vous devez identifier distinctement le nom de clé avec le point de confiance pour lequel vous créez la paire de clés.

### Procédure ASDM

1. Cliquez sur **Configuration**, et ensuite sur **Properties**.
2. Développez **Certificate**, puis choisissez **Key Pair**.
3. Cliquez sur **Add**.



4. Entrez le nom de la clé, choisissez la taille du module et sélectionnez le type d'utilisation.  
Note: La taille de paire de clés recommandée est 1024.
5. Cliquez sur **Generate**. La paire de clés que vous avez créée doit figurer dans la colonne Nom de la paire de clés.

#### Exemple de ligne de commande

```

ciscoasa

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)#

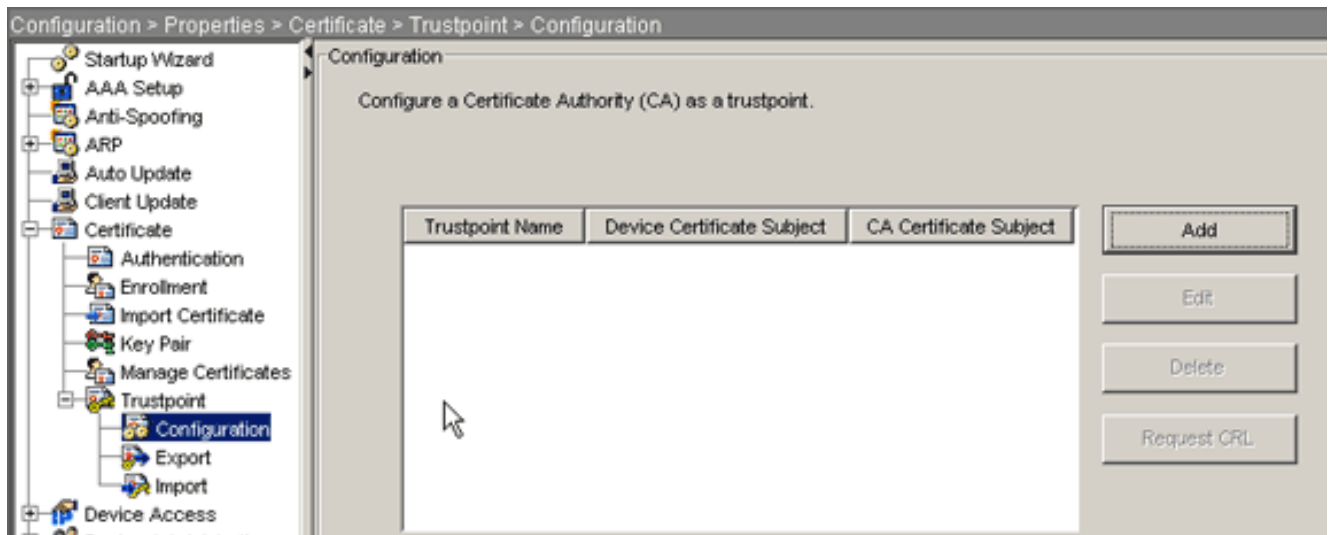
```

### Étape 3. Créer un point de confiance

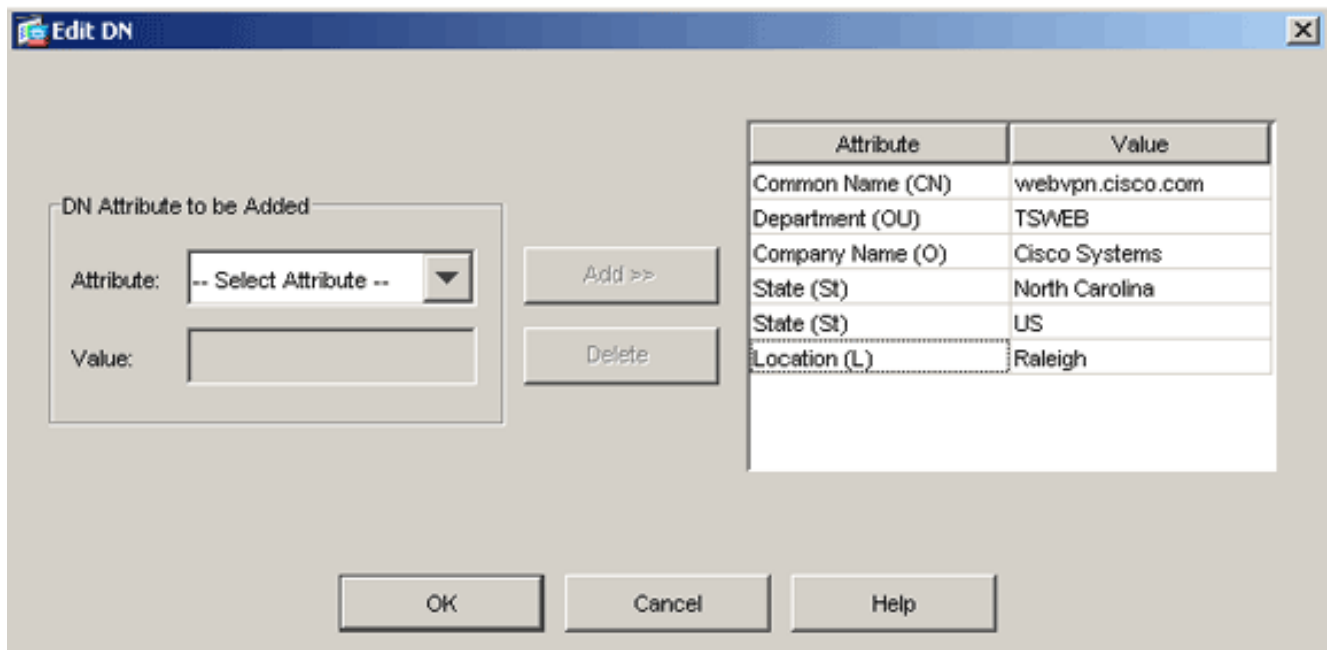
Les points de confiance doivent déclarer l'autorité de certification (CA) que votre ASA utilisera.

#### Procédure ASDM

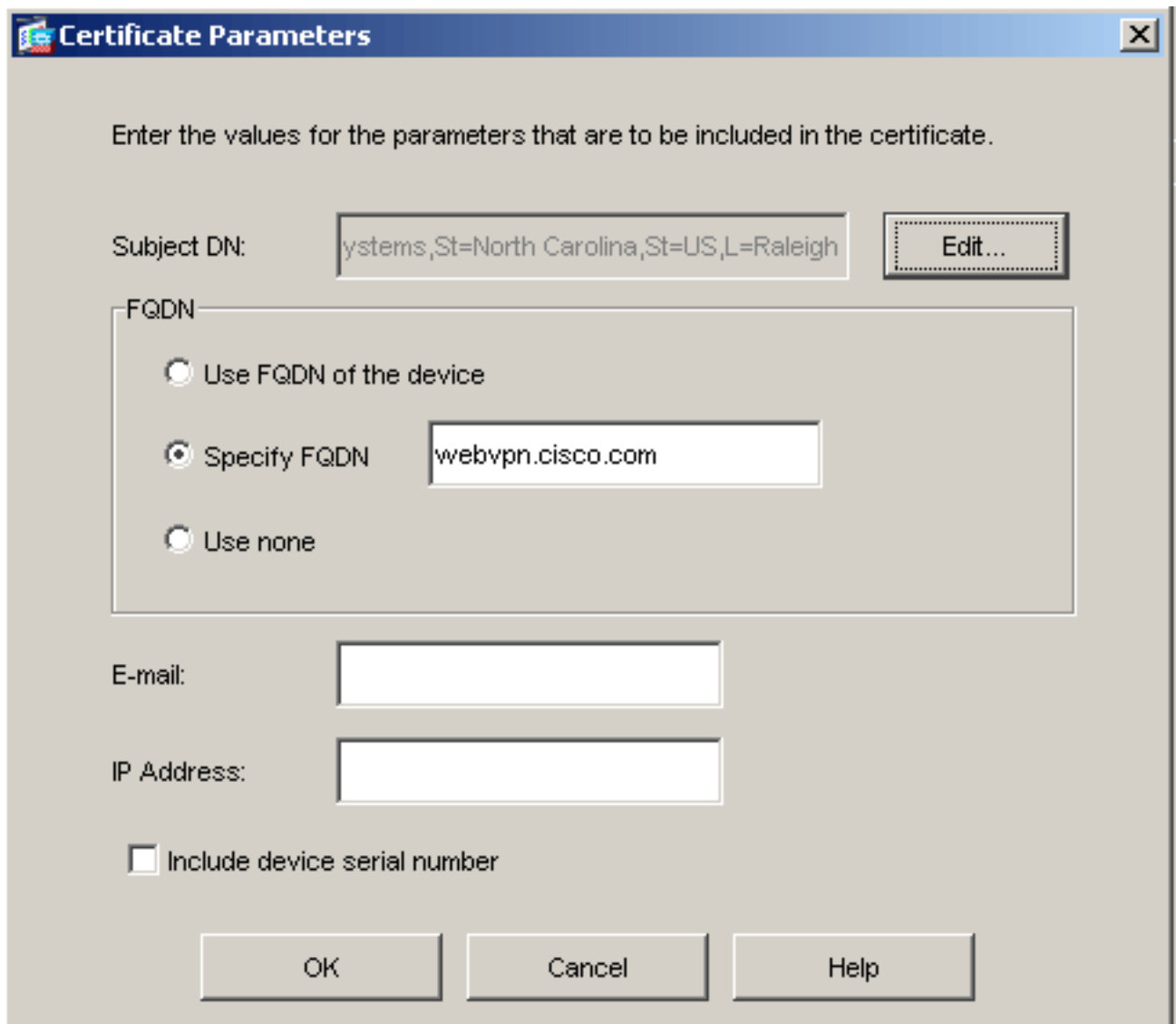
1. Cliquez sur **Configuration**, et ensuite sur **Properties**.
2. Développez **Certificate**, puis **Trustpoint**.
3. Choisissez **Configuration**, puis cliquez sur **Ajouter**.



4. Configurez ces valeurs : **Nom du point de confiance** : Le nom du point de confiance doit correspondre à l'utilisation prévue. (Cet exemple utilise *my.verisign.trustpoint*.) **Paire de clés** : Sélectionnez la paire de clés générée à l'[étape 2](#). (*my.verisign.key*)
5. Assurez-vous que l'inscription manuelle est sélectionnée.
6. Cliquez sur **Paramètres du certificat**. La boîte de dialogue Paramètres du certificat s'affiche.
7. Cliquez sur **Modifier**, puis configurez les attributs répertoriés dans ce tableau : Pour configurer ces valeurs, choisissez une valeur dans la liste déroulante Attribut, entrez la valeur, puis cliquez sur **Add**.



8. Une fois que les valeurs appropriées ont été ajoutées, cliquez sur **OK**.
9. Dans la boîte de dialogue Paramètres du certificat, saisissez le nom de domaine complet (FQDN) dans le champ Spécifier le nom de domaine complet (FQDN). Cette valeur doit être identique au nom de domaine complet que vous avez utilisé pour le nom commun (CN).



The image shows a Windows-style dialog box titled "Certificate Parameters". At the top, it says "Enter the values for the parameters that are to be included in the certificate." Below this, there are several input fields and options:

- Subject DN:** A text box containing "ystems,St=North Carolina,St=US,L=Raleigh" and an "Edit..." button to its right.
- FQDN:** A group box containing three radio button options:
  - Use FQDN of the device
  - Specify FQDN: A text box containing "webvpn.cisco.com"
  - Use none
- E-mail:** An empty text box.
- IP Address:** An empty text box.
- Include device serial number

At the bottom of the dialog box are three buttons: "OK", "Cancel", and "Help".

10. Click OK.
11. Vérifiez que la paire de clés correcte est sélectionnée, puis cliquez sur la case d'option **Utiliser l'inscription manuelle**.
12. Cliquez sur **OK**, puis sur **Apply**.

**Add Trustpoint Configuration**

Trustpoint Name:

Generate a self-signed certificate on enrollment  
 If this option is enabled, only Key Pair and Certificate Parameters can be specified.

Enrollment Settings | Revocation Check | CRL Retrieval Policy | CRL Retrieval Method | OCSP Rules | Advanced

Key Pair:

Challenge Password:  Confirm Challenge Password:

Enrollment Mode can only be specified if there are no certificates associated with this trustpoint.

Enrollment Mode

Use manual enrollment  
 Use automatic enrollment

Enrollment URL:

Retry Period:  minutes

Retry Count:  (Use 0 to indicate unlimited retries)

### Exemple de ligne de commande

```

ciscosa
-----
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=webvpn.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:).

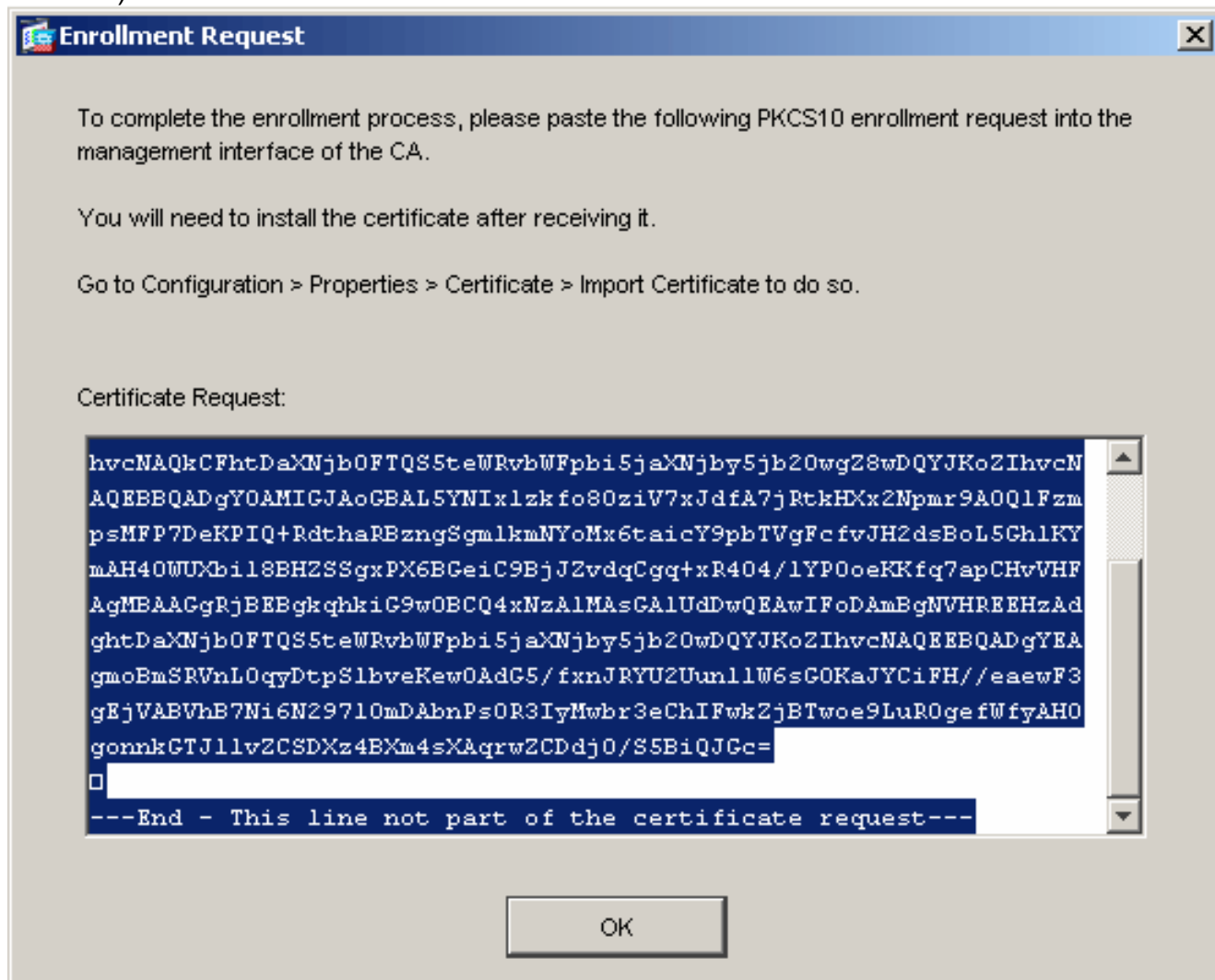
```

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

## Étape 4. Générer l'inscription au certificat

### Procédure ASDM

1. Cliquez sur **Configuration**, et ensuite sur **Propriétés**.
2. Développez **Certificate**, puis sélectionnez **Enrollment**.
3. Vérifiez que le point de confiance créé à l'[étape 3](#) est sélectionné, puis cliquez sur **S'inscrire**. Une boîte de dialogue apparaît qui répertorie la demande d'inscription de certificat (également appelée demande de signature de certificat).



4. Copiez la demande d'inscription PKCS#10 dans un fichier texte, puis envoyez le CSR au fournisseur tiers approprié. Une fois que le fournisseur tiers a reçu le CSR, il doit émettre un certificat d'identité pour l'installation.

### Exemple de ligne de commande

#### Nom du périphérique 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
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ21zY28gU31z
dGVtczEO
MAwGA1UECXMVFVNXRUIxGZAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv
bTEhMB8G
CSqGSIb3DQEJAhYSY21zY29hc2EuY21zY28uY29tMIGfMA0GCSqGSIb3
DQEBAQUA
A4GNADCBiQKBGQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB
9M4yTx5b
Fm886s8F73WsfQPynBDFBSsejDOnBpFYzKsGf7TUMQB2m2RFAqfyNxYt
3oMXSNPO
m1dZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX0luBMh7oKar
gwIDAQAB
oD0wOwYJKoZIhvcNAQkOMs4wLDALBgNVHQ8EBAMCBAwHQYDVR0RBByw
FIISY21z
Y29hc2EuY21zY28uY29tMA0GCSqGSIb3DQEBAUAA4GBABrxpY0q7Se0
HZf3yEJq
po6wG+oZpsvpYI/HemKULaRc783w4BMO5lulIEhHgRqAxrTbQn0B7JPI
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)#

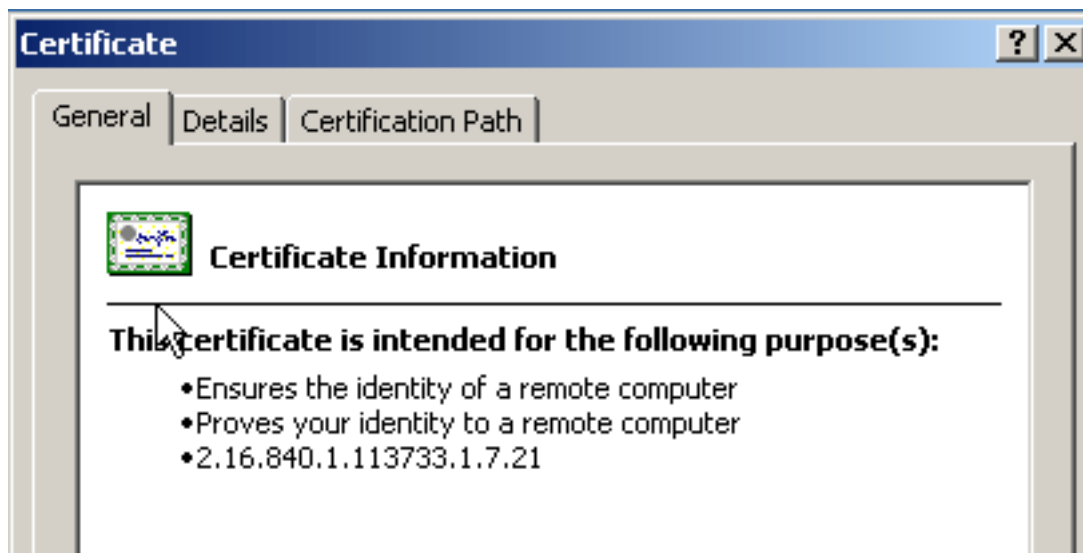
```

## Étape 5. Authentifier le point de confiance

Une fois que vous avez reçu le certificat d'identité du fournisseur tiers, vous pouvez poursuivre cette étape.

### Procédure ASDM

1. Enregistrez le certificat d'identité sur votre ordinateur local.
2. Si un certificat codé en base64 ne vous a pas été fourni en tant que fichier, vous devez copier le message base64 et le coller dans un fichier texte.
3. Renommez le fichier avec une extension **.cer**. **Remarque** : Une fois le fichier renommé avec l'extension **.cer**, l'icône du fichier doit s'afficher en tant que certificat.
4. Double-cliquez sur le fichier de certificat. La boîte de dialogue Certificat



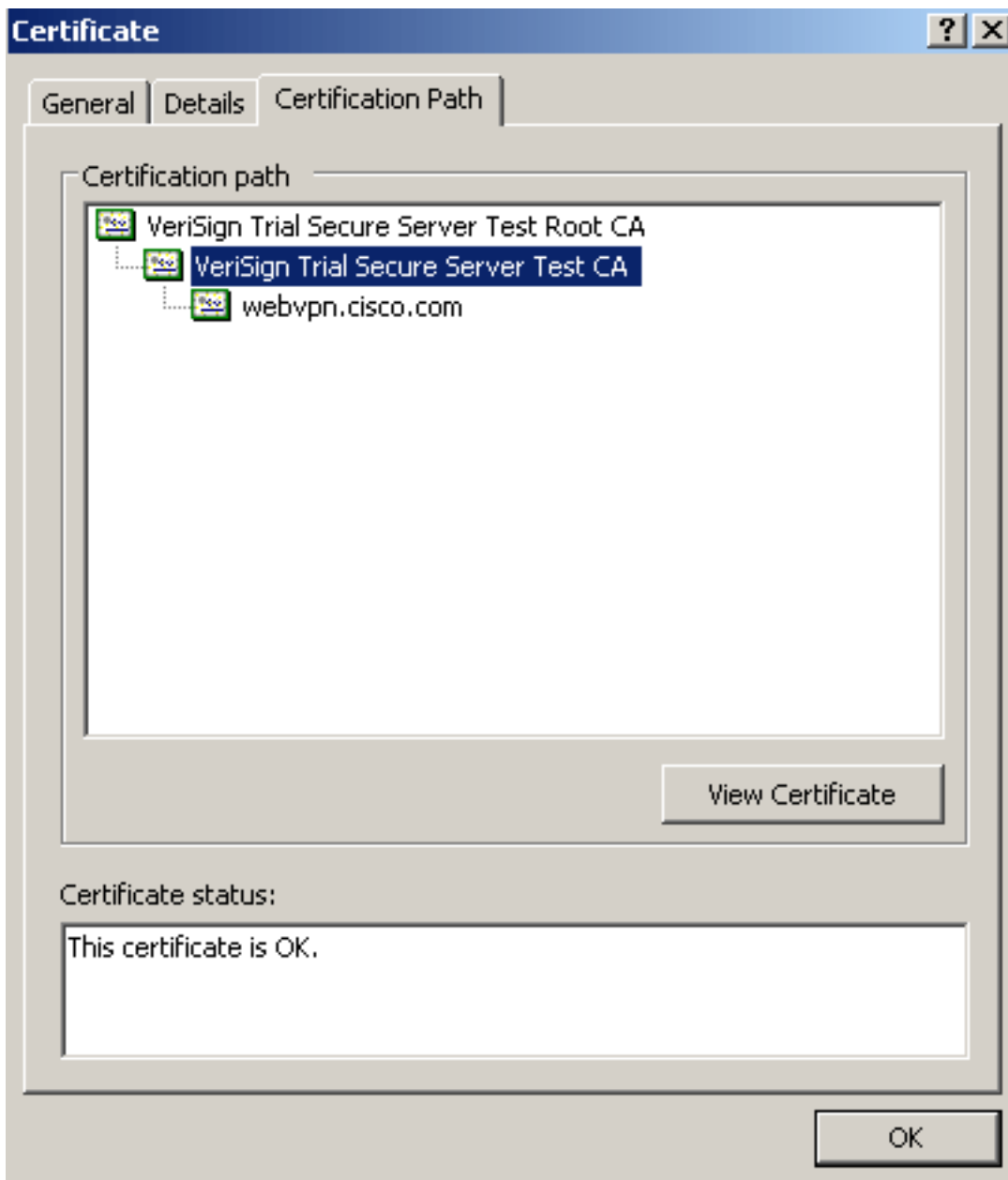
s'affiche.

Remar

**que** : si le message "*Windows ne dispose pas d'informations suffisantes pour vérifier ce certificat*" apparaît dans l'onglet Général, vous devez obtenir le certificat de l'autorité de certification racine ou de l'autorité de certification intermédiaire du fournisseur tiers avant de poursuivre cette procédure. Contactez votre fournisseur tiers ou votre administrateur CA afin d'obtenir le certificat CA racine ou CA intermédiaire émetteur.

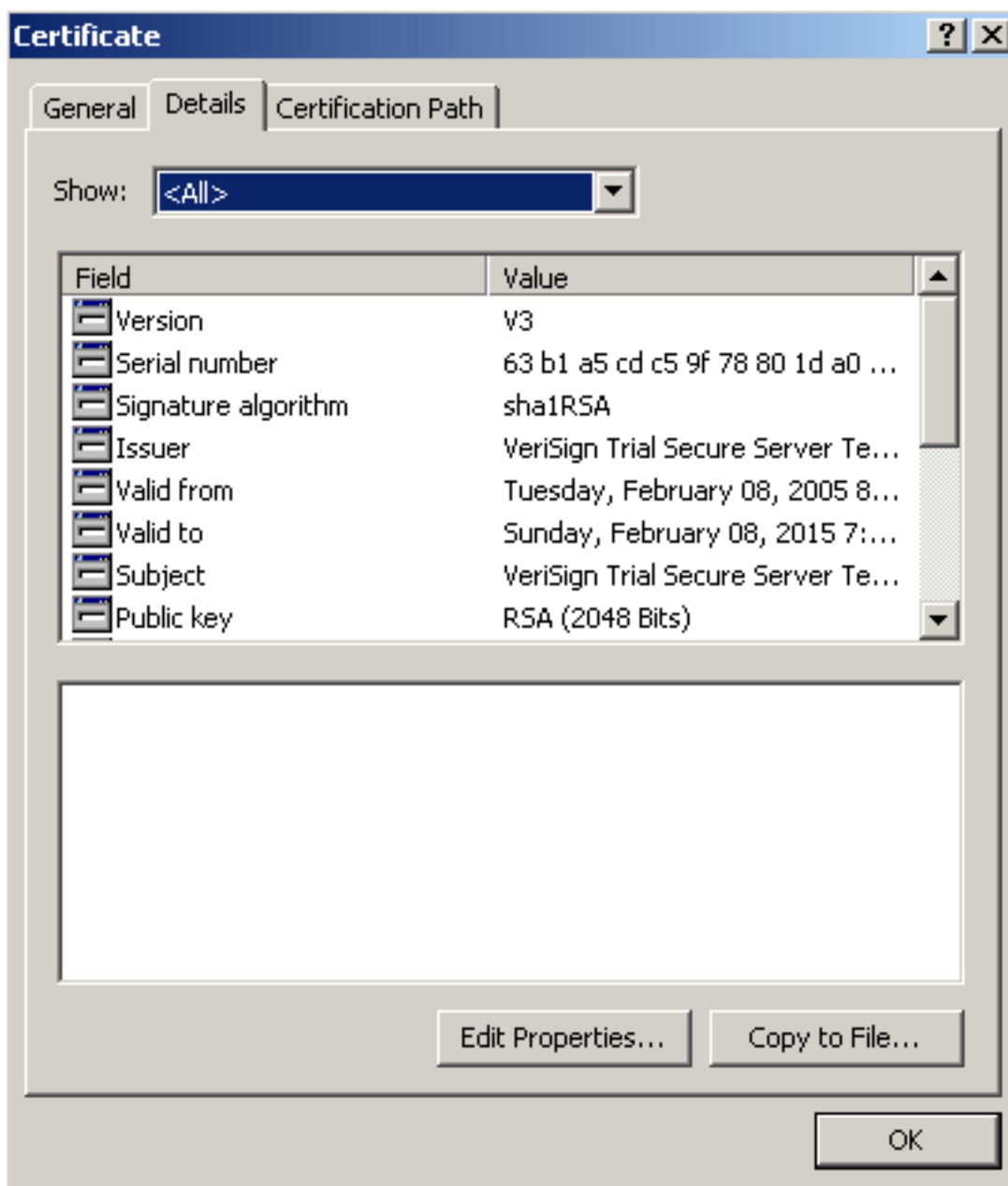
5. Cliquez sur l'onglet de **Certificate Path**.

6. Cliquez sur le certificat CA situé au-dessus de votre certificat d'identité émis, puis cliquez sur **Afficher le**



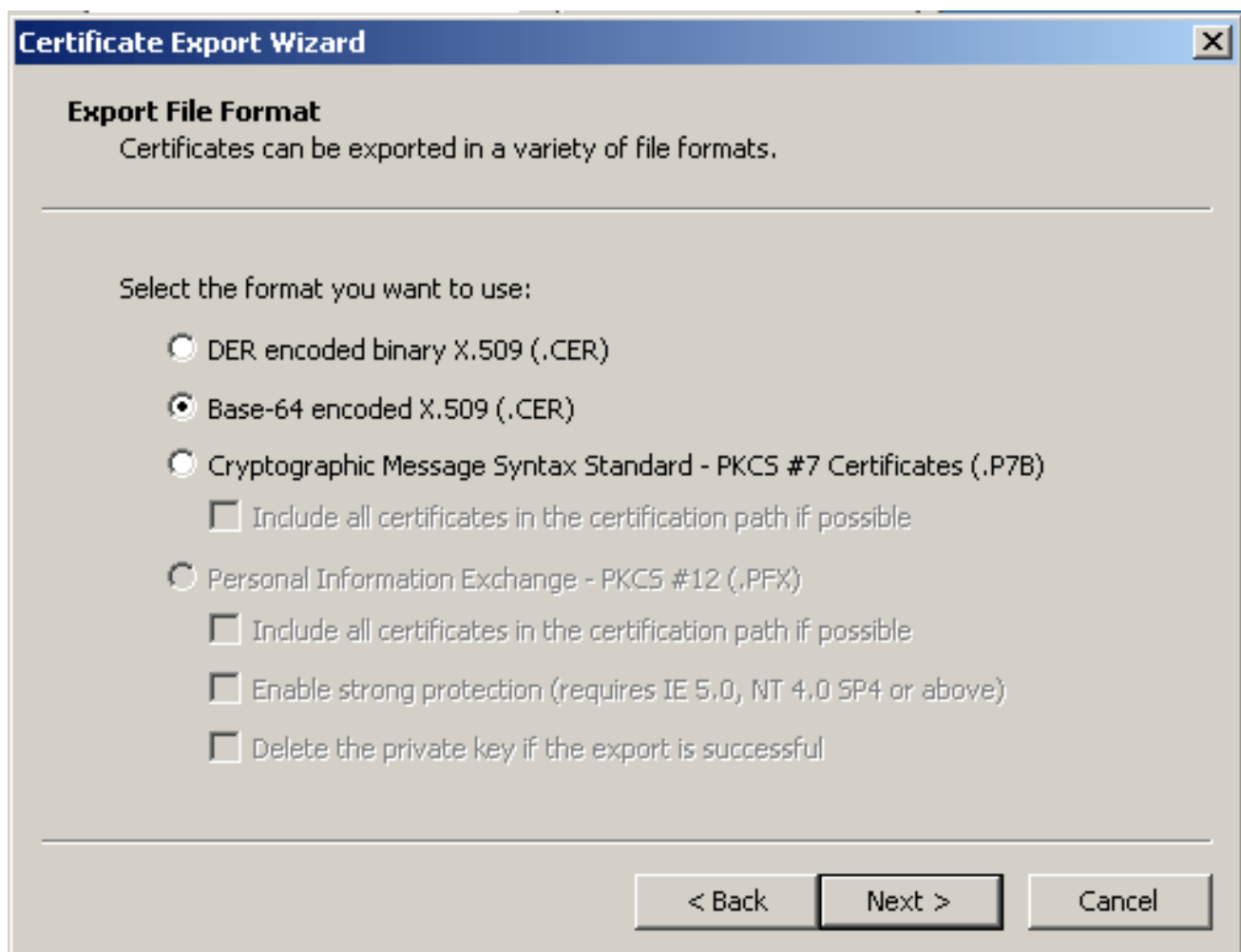
certificat. Des informations détaillées sur le certificat d'autorité de certification intermédiaire s'affichent. **Avertissement** : N'installez pas le certificat d'identité (périphérique) dans cette étape. Seule la racine, la racine subordonnée ou le certificat CA sont ajoutés à cette étape. Les certificats d'identité (périphérique) sont installés à l'[étape 6](#).

7. Cliquez sur **Details**

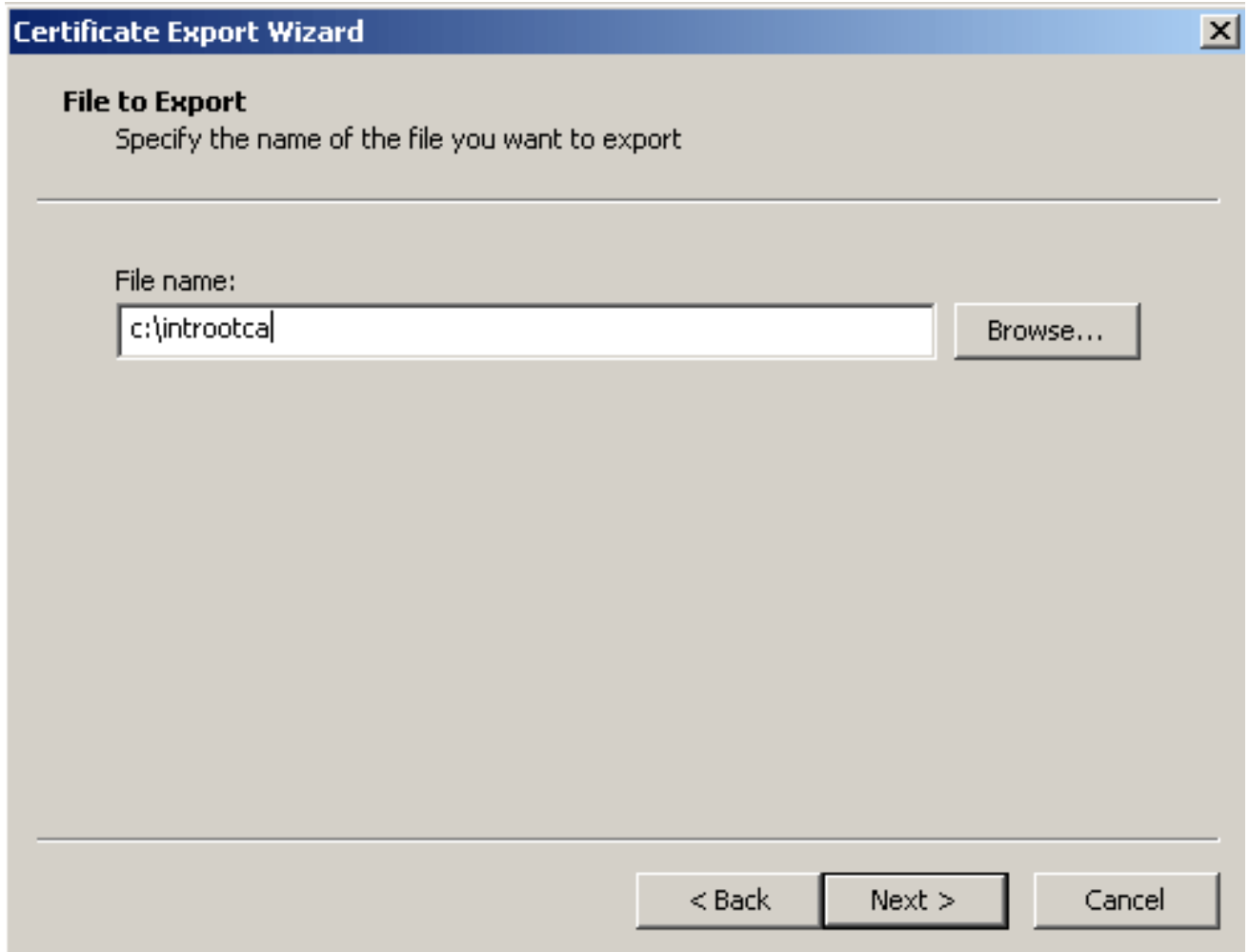


(Détails).

8. Cliquez sur **Copier dans le fichier**.
9. Dans l'Assistant Exportation de certificat, cliquez sur **Suivant**.
10. Dans la boîte de dialogue Format de fichier d'exportation, cliquez sur la case d'option **X.509 codé en base-64 (.CER)**, puis cliquez sur **Suivant**.



11. Entrez le nom et l'emplacement du fichier auquel vous voulez enregistrer le certificat de l'autorité de certification.
12. Cliquez sur **Suivant**, puis sur **Terminer**.



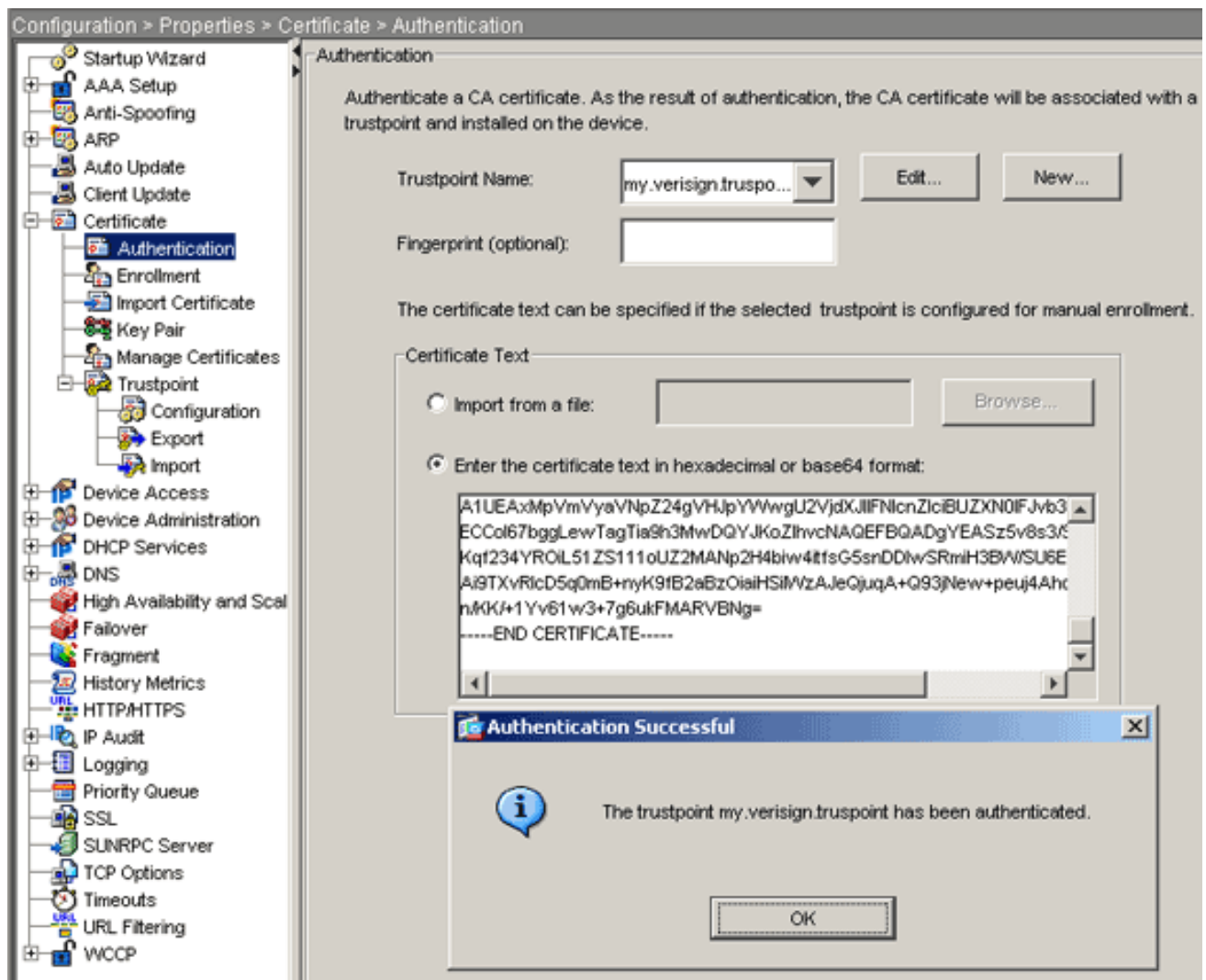
13. Cliquez sur **OK** dans la boîte de dialogue Exportation réussie.
14. Naviguez jusqu'à l'emplacement où vous avez enregistré le certificat d'autorité de certification.
15. Ouvrez le fichier avec un éditeur de texte, tel que le Bloc-notes. (Cliquez avec le bouton droit sur le fichier, puis sélectionnez **Envoyer à > Bloc-notes**.) Le message codé en base64 doit apparaître comme le certificat dans cette image  
:

```

-----BEGIN CERTIFICATE-----
MIIFSjCCBDKgAwIBAgIQCECQ47aTdj6BtrI60/vt6zANBgkqhkiG9w0BAQUFADCB
yzELMAkGA1UEBhMCVVMXFZAVBgnVBAoTDIzIcm1TawduLCBjbMUMTAwLgYDVQQQL
EydGb3IgvGVzdCBQdXJwb3NlcyBpbmx5LjAgTm8gYXNzdXJhbmNlcy4xQjBAGNV
BAStOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vy3Bz
L3Rlc3RjYSAoYykwNTETMCsGA1UEAxMkvmvyaVNpZ24gVHJpYXVwU2VjdxJlIFNl
cnZlciBUZXN0IENBMB4XDTA3MDcyNzAwMDAwMFoXDTA3MDg0MDIzNTk1OVowgZ4x
CZAJBgNVBAYTA1VTMRcwFQYDVQQIEW50b3J0aCBDYXJvbG1uYUwTEWMBQGA1UEChQN
Q2IzY28gU3IzdGvtcZEOMAwGA1UECmFVFNXRUIXo4jA4BgNVBASUMVRlcm1zIG9m
IHVzZSBhdCB3d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMpMDUXEjAQBGNV
BAMUCWNSawvudHZwbjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwGyKCCgYEA1v9Ahzsm
SZiUwosov+yL/SMZULWkigvgwX1avJ4UwqpuG9TgaIEn9wFvrZmJd0T/ucJW6k1A
TjajzxSocuvAKUj7cnOxSj+KlHIBNUjz8Ey3r26nLa9fBCOK9YSZ6fA7zJimmQp
RwMazEvoFaiiy+5oG7XAiwCPY4677K3INFECAwEAaOCAdcwggHTMAkGA1UdEwQC
MAAwCwYDVR0PBAQDAgwgMEMGA1UdHwQ8MDowOKA2oDSGMMh0dHA6Ly9TVlJTZWNI
cmUtY3JzLnZlcm1zawduLmNvbS99TVlJUcm1hbDIwMDUuY3JSMEOGA1UdIARDMEEW
PwYKYIZIAYb4RQEHTAXMC8GCCSGAQUFBwIBFiNodHRwczovL3d3dy52ZXJpc2ln
bi5jb20vy3BzL3Rlc3RjYTAdBgNVHSUEFjAUBggrBgEFBQCDAQYIKwYBBQUHAWIw
HwYDVR0jBBgwFoAUZiKogeAXwd0qf6tGxTYCBnAnhIoweAYIKwYBBQUHAQEEdBQ
MCQGCSGAQUFBzABhhodHRwoi8vb2Nzcc52ZXJpc2lnbi5jb20wQGYIKwYBBQUH
MAKGNmh0dHA6Ly9TVlJTZWNIcmUtYw1hLnZlcm1zawduLmNvbS99TVlJUcm1hbDIw
MDUyYw1hLmNlcm1zBuBgggrBgEFBQCBDARiMGChXqBcMFowWDBWfGlpbwFnZS9nawYw
ITAFMACGBSSoAwIaBBRLa7ko1gYMU9BSOJsprEshiyEFGDAmFiRodHRwoi8vbG9n
by52ZXJpc2lnbi5jb20vdnnsb2dvMS5nawYwDQYJKoZIhvcNAQEFBQADggEBAC4k
abswgoogAntm4lrJhv8TSGsjdPpospLseBFxULEZJlTHGprcf0sALr gbIFEL4b9q
l/Eajjdt eeyTgIorIC1awwwx+RHCCtqIr1zf0vfUD0DNZ6949sM2agAmzrRsBy63
Lb1/3+jz8skIAkizP79pmqMEECZ+cum10rk631c46yBCsJMZVbG6sZlNSI80RRwK
hAKdsfufvsirHc8c9nJdOEC0905izUTRE854jv1XzZjioJ51FbcmCox/ub7zv3zC
Ftm412+TgfyZ3z7wCENulvhMa7bc2T3mmdqB5kCeHEZ2kAL6u6NQpXy5l7TLkyja
idT1FmBvf02qaZS6S40=
-----END CERTIFICATE-----

```

16. Dans ASDM, cliquez sur **Configuration**, puis sur **Propriétés**.
17. Développez **Certificate**, puis sélectionnez **Authentication**.
18. Cliquez sur la case d'option **Entrez le texte du certificat au format hexadécimal ou base64**.
19. Collez le certificat CA formaté en base64 de votre éditeur de texte dans la zone de texte.
20. Cliquez sur **Authentifier**.



21. Click OK.

### Exemple de ligne de commande

```

ciscoasa

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-----
MIIEwDCCBCmgAwIBAgIQY7G1zcWfeIAdoGNs+XVGezANBgkqhkiG9w0B
AQUFADCB
jDELMAkGA1UEBhmCVVMxZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVz
LgYDVQQL
EydGb3IgdGVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVz
MjAwBgNV
BAMTKVZlcm1TaWduIFRyaWFsIFN1Y3VyZSBTZmVzZmVzZmVzZmVzZmVzZmVz
IENBMB4X
DTA1MDIwOTAwMDAwMFoXDTE1MDIwODIzNTk1OVowGcsxCzAJBgNVBAYT
A1VTMRcw
FQYDVQQKEw5WZXJpU2lnbiwSW5jLjEwMjAwMjAwMjAwMjAwMjAwMjAwMjAw
UHVycG9z
ZXMGt25seS4gIE5vIGFzc3VyYW5jZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVz
ZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMp
MDUxLTAr
BgNVBAMTJmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVz

```



```
QTCCASiW
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAu
wElv6IJ/
DV8zgpvxuwdaMv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE6
1BBD6Zqk
d851P1/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45
1P4qoyqS
E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1
D/OCCmZO
5RmNqLLKSVwYHhJ25EskFhgR2qCxx2EQJdnDXuTw0+4t1qj97ydk5iDo
xjKfV6sb
tnp3TIY6S07bTb9gxJcK4pGbcf8DOPvOfGRu1wfpUUZC8v+WKC20+sK6
QMECAwEA
AaOCAVwgggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA
BgpghkgB
hvhFAQcVMDIwMAYIKwYBBQUHAgEwJGh0dHBzOi8vd3d3LnZlcmlzaWdu
LmNvbS9j
cHMvdGVzdG9hLzAObG9NVH08BAf8EBAMCAQYwEQQYJYIZIAyb4QgEBBAQD
AgEGMB0G
A1UdDgQWBRRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGN
oYGSsIGP
MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x
MDAuBgNV
BAstJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICB0byBhc3N1cmFuY2Vz
LjEyMDAG
A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJlIFN1cnZ1ciBUZXN0IFJv
b3QgQ0GC
ECCol67bggLeWTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/
SjzRvY21
Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU
6EEzD9oi
Ai9TXvRIcD5q0mB+nyK9fB2aBzOiaIHSiIWzAJeQjuqA+Q93jNew+peu
j4AhdvGN
n/KK/+1Yv61w3+7g6ukFMARVBNG=
-----END CERTIFICATE-----
quit
```

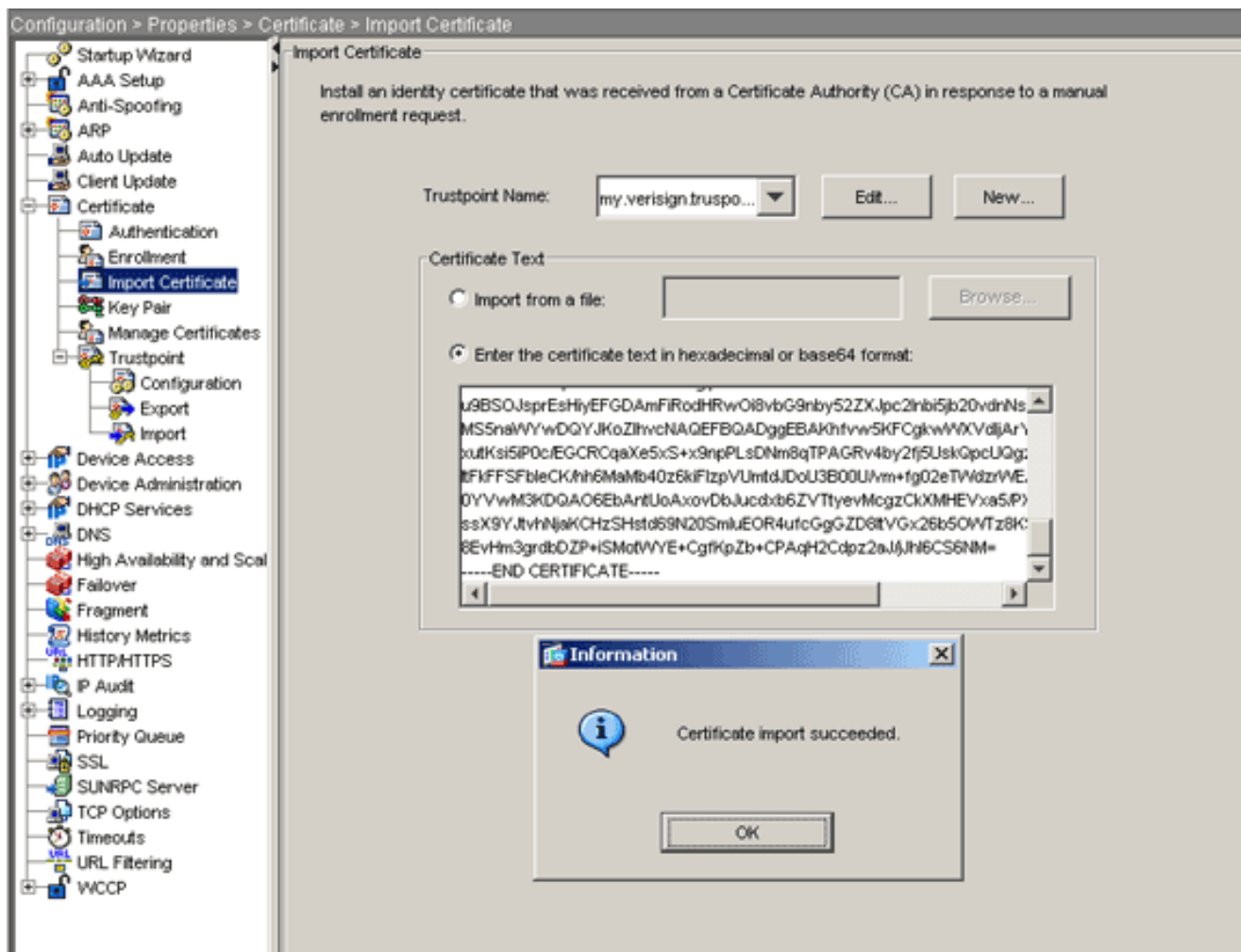
```
! Manually pasted certificate into CLI. INFO:
Certificate has the following attributes: Fingerprint:
8de989db 7fcc5e3b fdde2c42 0813ef43 Do you accept this
certificate? [yes/no]: yes Trustpoint
'my.verisign.trustpoint' is a subordinate CA and holds a
non self-signed certificate. Trustpoint CA certificate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

## Étape 6. Installer le certificat

### Procédure ASDM

Utilisez le certificat d'identité fourni par le fournisseur tiers pour effectuer ces étapes :

1. Cliquez sur **Configuration**, et ensuite sur **Propriétés**.
2. Développez **Certificat**, puis choisissez **Import Certificate**.
3. Cliquez sur la case d'option **Entrez le texte du certificat au format hexadécimal ou base64**, puis collez le certificat d'identité base64 dans le champ de texte.



4. Cliquez sur Importer, puis sur OK.

#### Exemple de ligne de commande

```

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
yzELMAkGA1UEBhMCVVMxZjZAVBgNVBAoTDlZlcm1TaWduLCBjb20vY3Bz
LgYDVQQL
EydgB3IgvGVzdBQdXJwb3NlcYBPbm5LiAgTm8gYXNzdXJhbmNlcY4x
QjBAbG9u
BAStOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5j
b20vY3Bz
L3Rlc3RjYSAoYykwNTEtMCSGA1UEAxMkVmVyaVNPZ24gVHJpYWwgU2Vj
dXJlIFNl
cnZlciBUZXN0IENBMB4XDTA3MDcyNjAwMDAwMFoXDTA3MDgwOTIzNTk1
OVowgbox
CzAJBgNVBAYTA1VTMRcwFQYDVQIEw5OjB3J0aCBDYXJvbGluYTEQM4G
A1UEBxQH
UmFsZWlnaDEwBQGA1UEChQzY28gU3lzdGVtczEOMAwGA1UECxQF
VFNXRUlx

```

```

OjA4BgNVBAsUMVR1cm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29t
L2Nwcy90
ZXN0Y2EgKGMpMDUxHDAaBgNVBAMUE2Npc2NvYXN0MS5jaXNjby5jb20w
gZ8wDQYJ
KoZlHvcNAQEBBQADgY0AMIGJAoGBAL56EvorHH1sIB/VRKaR1JeJKCrQ
/9kER2JQ
9UOkUP3mVPZJtYN63ZxDwACeyNb+liIdKUegJWHI0Mz3GHqcgEkKW1Ec
rO+6aY1R
IaUE8/LiAZba70+k/9Z/UR+v532B1nDRwbx1R9ZVhAJzA1hJTxs1Egry
osBMMazg
5IcLhgSpAgMBAAGjggHXMIIB0zAJBgNVHRMEAjaAMAsGA1UdDwQEAwIF
oDBDBgNV
HR8EPDA6MDigNqA0hjJodHRwOi8vU1ZSU2VjdXJlLWNYbC52ZXJpc2ln
bi5jb20v
U1ZSVHJpYWwyMDA1LmNybDBKBGNVHSAEQzBBMD8GCmCGSAGG+EUBBxUw
MTAvBggr
BgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0
Y2EwHQYD
VR01BBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMCB8GA1UdIwQYMBaAFGYi
joHgMVnd
Kn+rRsU2AgZwJ4daMHgGCCsGAQUFBwEBBGwwajAkBggrBgEFBQcwAYYY
aHR0cDov
L29jc3AudmVyaXNpZ24uY29tMEIGCCsGAQUFBzAChjZodHRwOi8vU1ZS
U2VjdXJl
LWFpYS52ZXJpc2lnbi5jb20vU1ZSVHJpYWwyMDA1LWFpYS5jZXIwbgYI
KwYBBQUH
AQwEYjBgoV6gXDBAMFgwVhYJaW1hZ2UvZ2lmMCEwHZAHBGUrdgMCGGQU
S2u5KJYG
DLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29t
L3ZzbG9n
bzEuZ2lmMA0GCSqGSIb3DQEBBQUAA4IBAQAnym4GVThPIyL/9y1DBd8N
7/yW3Ov3
bIirHfHJyfPJ1znZQXyXdObpZkuA6Jyu03V2CYNnDomn4xRXQTUDD8q8
6ZiKyMIj
XM2VCmCHSajmMMRyjpydxfk6CIddMtMGotCavRHD9T12tvwgrBock/v/
54o021kB
SmLzVV7crlYJEUhgqu3Pz7qNRd8N0Un6c9sbwQ1BuM99QxzIzdAo89FS
ewy8MAIY
rtab5F+oiTc5xGy8w7NARafNgFXihqnLgWTtA35/oWuy86bje1IWbeyq
j8ePM9Td
0LdAw6kUU1PNimPttMDhcF7cuevntROksOgQPBPx5FJSqMiUZGrvju50
-----END CERTIFICATE-----
quit

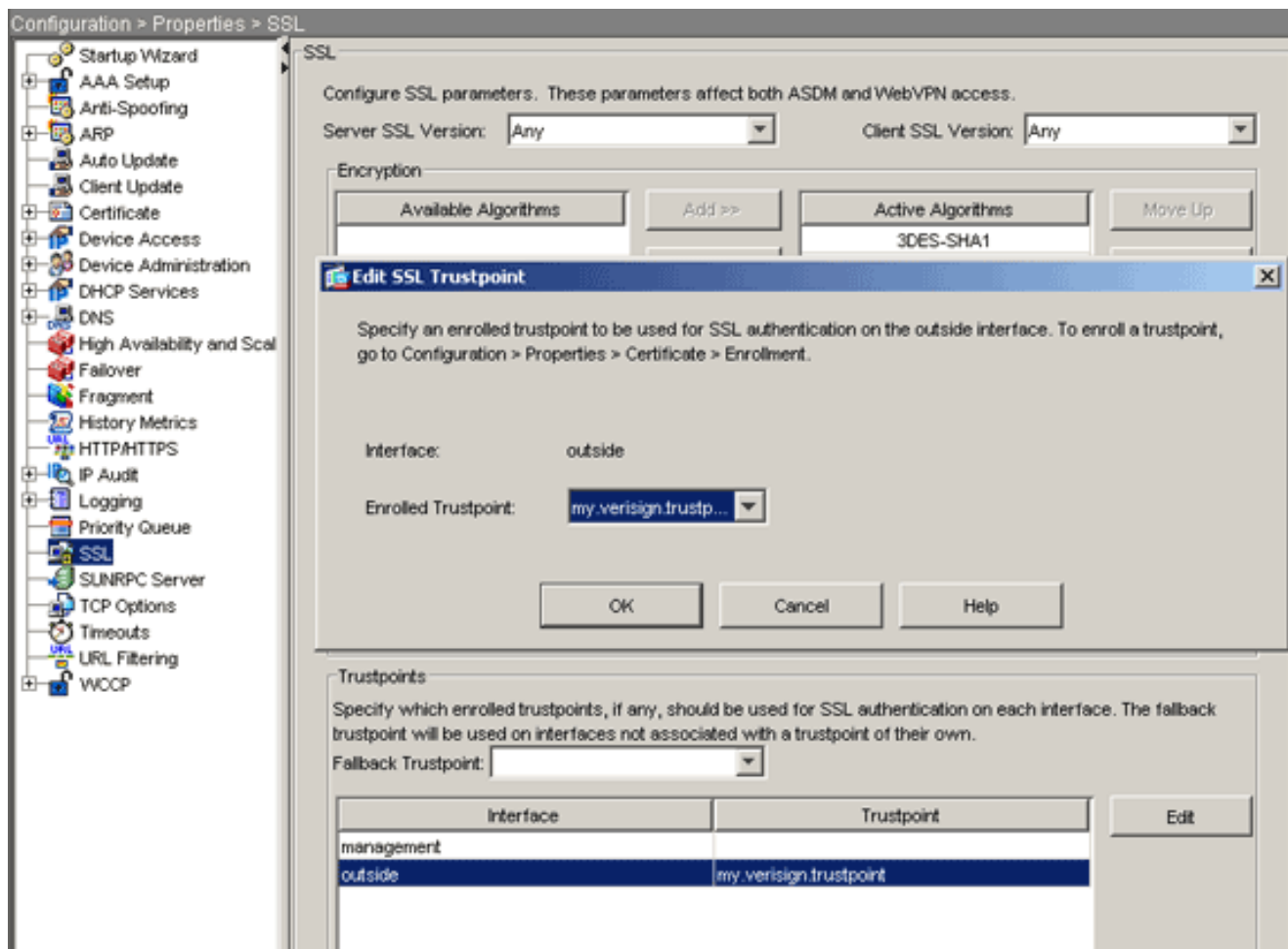
INFO: Certificate successfully imported
ciscoasa(config)#

```

## Étape 7. Configurer WebVPN pour utiliser le certificat récemment installé

### Procédure ASDM

1. Cliquez sur **Configuration**, sur **Propriétés**, puis sélectionnez **SSL**.
2. Dans la zone Trustpoints, sélectionnez l'interface qui sera utilisée pour terminer les sessions WebVPN. (Cet exemple utilise l'interface externe.)
3. Cliquez sur **Edit**. La boîte de dialogue Modifier le point de confiance SSL s'affiche.



4. Dans la liste déroulante Point de confiance inscrit, sélectionnez le point de confiance que vous avez créé à l'étape 3.
5. Cliquez sur **OK**, puis sur **Apply**.

Votre nouveau certificat doit maintenant être utilisé pour toutes les sessions WebVPN qui se terminent sur l'interface spécifiée. Reportez-vous à la section Vérifier de ce document pour obtenir des informations sur la manière de vérifier une installation réussie.

### Exemple de ligne de commande

```

ciscoasa
-----
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.

```

## Vérification

Cette section décrit comment confirmer que l'installation de votre certificat de fournisseur tiers a réussi.

## Remplacer le certificat auto-signé d'ASA

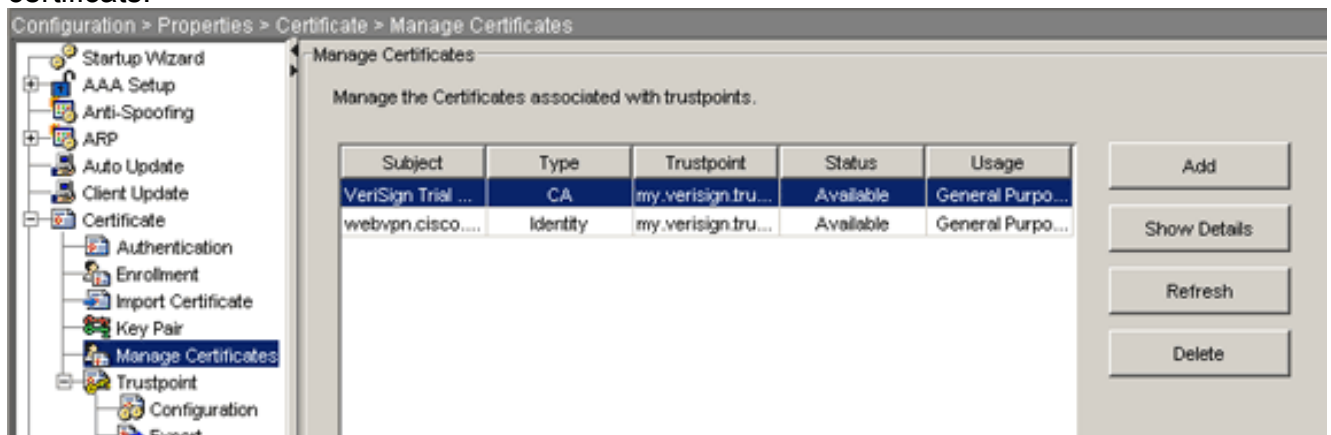
Cette section décrit comment remplacer le certificat auto-signé installé de l'ASA.

1. Émettez une demande de signature de certificat à Verisign. Après avoir reçu le certificat demandé de Verisign, vous pouvez l'installer directement sous le même point de confiance.
2. Tapez cette commande : **crypto ca enroll Verisign** Vous êtes invité à répondre aux questions.
3. Pour Afficher la demande de certificat au terminal, entrez **yes**, et envoyez le résultat à Verisign.
4. Une fois le nouveau certificat obtenu, tapez cette commande : **crypto ca import Verisign certificate**

## Afficher les certificats installés

### Procédure ASDM

1. Cliquez sur **Configuration**, puis sur **Propriétés**.
2. Développez **Certificate**, puis sélectionnez **Manage Certificates**. Le certificat CA utilisé pour l'authentification Trustpoint et le certificat d'identité émis par le fournisseur tiers doivent apparaître dans la zone Gérer les certificats.



### Exemple de ligne de commande

**ciscosa**

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

*! Displays all certificates installed on the ASA.*

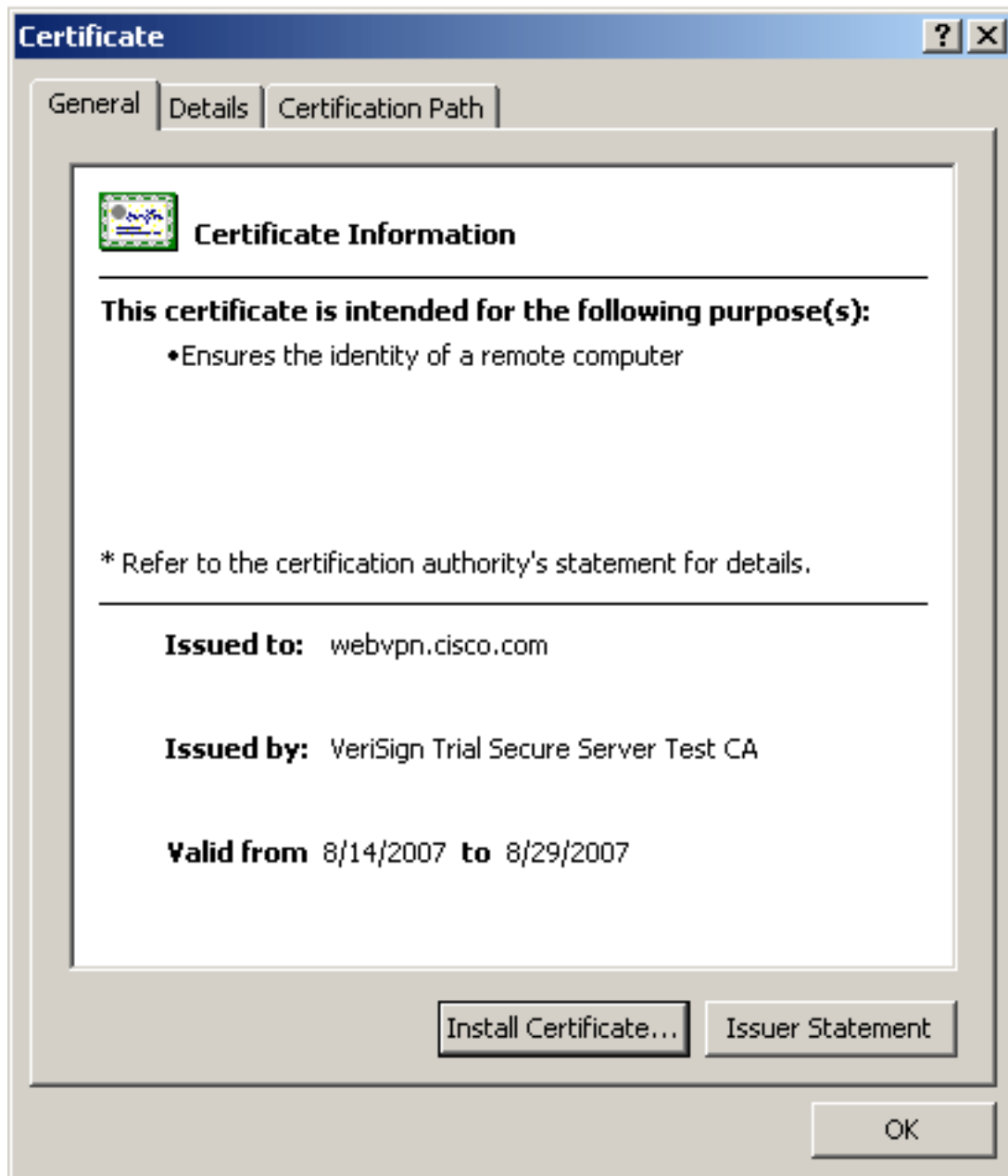
```
Certificate Status: Available Certificate Serial Number:
32cfe85eebbd2b5e1e30649fd266237d Certificate Usage:
General Purpose Public Key Type: RSA (1024 bits) Issuer
Name: cn=VeriSign Trial Secure Server Test CA ou=Terms
of use at https://www.verisign.com/cps/testca (c)05
ou=For Test Purposes Only. 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:
63bla5cdc59f78801da0636cf975467b 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.
```

## Vérification du certificat installé pour WebVPN à l'aide d'un navigateur Web

Afin de vérifier que WebVPN utilise le nouveau certificat, procédez comme suit :

1. Connectez-vous à votre interface WebVPN via un navigateur Web. Utilisez https:// avec le nom de domaine complet que vous avez utilisé pour demander le certificat (par exemple, https://webvpn.cisco.com). Si vous recevez l'une de ces alertes de sécurité, procédez comme suit : **Le nom du certificat de sécurité n'est pas valide ou ne correspond pas au nom du site** Vérifiez que vous avez utilisé le nom de domaine complet (FQDN)/le nom de domaine principal (CN) correct afin de vous connecter à l'interface WebVPN de l'ASA. Vous devez utiliser le FQDN/CN que vous avez défini lorsque vous avez demandé le certificat d'identité. Vous pouvez utiliser la commande **show crypto ca certificate trustpointname** afin de vérifier les certificats FQDN/CN. **Le certificat de sécurité a été émis par une société que vous n'avez pas choisie de faire confiance...** Complétez ces étapes afin d'installer le certificat racine du fournisseur tiers dans votre navigateur Web : Dans la boîte de dialogue Alerte de sécurité, cliquez sur **Afficher le certificat**. Dans la boîte de dialogue Certificat, cliquez sur l'onglet **Chemin du certificat**. Sélectionnez le certificat CA situé au-dessus de votre certificat d'identité émis, puis cliquez sur **Afficher le certificat**. Cliquez sur **Install Certificate**. Dans la boîte de dialogue Assistant Installation de certificat, cliquez sur **Suivant**. Sélectionnez la case d'option **Sélectionner automatiquement le magasin de certificats en fonction du type de certificat**, cliquez sur **Suivant**, puis sur **Terminer**. Cliquez sur **Oui** lorsque vous recevez l'invite de confirmation Installer le certificat. À l'invite Importer a réussi, cliquez sur **OK**, puis sur **Oui**. **Remarque** : Comme cet exemple utilise le certificat d'évaluation Verisign, le certificat racine de l'autorité de certification Verisign Trial doit être installé afin d'éviter les erreurs de vérification lorsque les utilisateurs se connectent.
2. Double-cliquez sur l'icône de verrouillage qui apparaît dans le coin inférieur droit de la page de connexion WebVPN. Les informations de certificat installées doivent apparaître.
3. Vérifiez le contenu pour vérifier qu'il correspond à votre certificat de fournisseurs



tiers.

## Étapes de renouvellement du certificat SSL

Complétez ces étapes afin de renouveler le certificat SSL :

1. Sélectionnez le point d'approbation à renouveler.
2. Choisissez **s'inscrire**. Ce message apparaît : *S'il est de nouveau inscrit, le certificat actuel sera remplacé par les nouveaux. Voulez-vous continuer ?*
3. Choisissez **oui**. Cela générera une nouvelle CSR.
4. Envoyez le CSR à votre CA, puis importez le nouveau certificat d'ID lorsque vous le récupérez.
5. Supprimez et réappliquez le point d'approbation à l'interface externe.

## Commandes

Sur l'ASA, vous pouvez utiliser plusieurs commandes show sur la ligne de commande pour vérifier l'état d'un certificat.

- **show crypto ca trustpoint** — Affiche les points de confiance configurés.
- **show crypto ca certificate** : affiche tous les certificats installés sur le système.
- **show crypto ca crls** - Affiche les listes de révocation de certificats (CRL) mises en cache.
- **show crypto key mypubkey rsa** : affiche toutes les paires de clés de chiffrement générées.

## Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Voici quelques erreurs possibles :

- **% Avertissement : Certificat CA introuvable. Il se peut que les certificats importés ne soient pas utilisables.****INFO : Le certificat a été importé**Le certificat d'autorité de certification n'a pas été authentifié correctement. Utilisez la commande `show crypto ca certificate trustpoint name` afin de vérifier que le certificat de l'autorité de certification a été installé. Recherchez la ligne commençant par le certificat CA. Si le certificat d'autorité de certification est installé, vérifiez qu'il fait référence au point de confiance correct.
- **ERREUR : Failed to parse or verify imported certificate**Cette erreur peut se produire quand vous installez le certificat d'identité et que vous n'avez pas le certificat d'autorité de certification racine ou intermédiaire correct authentifié avec le point de confiance associé. Vous devez supprimer et réauthentifier avec le certificat d'autorité de certification racine ou intermédiaire correct. Contactez votre fournisseur tiers afin de vérifier que vous avez reçu le certificat CA correct.
- **Certificate does not contain general purpose public key**Cette erreur peut se produire quand vous essayez d'installer votre certificat d'identité sur le point de confiance incorrect. Vous essayez d'installer un certificat d'identité non valide ou la paire de clés associée au point de confiance ne correspond pas à la clé publique contenue dans le certificat d'identité. Utilisez la commande `show crypto ca certificate trustpointname` afin de vérifier que vous avez installé votre certificat d'identité sur le point de confiance correct. Recherchez la ligne qui indique *Associated Trustpoints* : Si le point de confiance incorrect est répertorié, utilisez les procédures décrites dans ce document afin de supprimer et réinstaller sur le point de confiance approprié, également Vérifiez que la paire de clés n'a pas changé depuis la génération du CSR.
- **Message d'erreur : %PIX|ASA-3-717023 SSL n'a pas pu définir le certificat de périphérique pour Trustpoint [nom du point de confiance]**Ce message s'affiche lorsqu'une défaillance se produit lorsque vous définissez un certificat de périphérique pour le point de confiance donné afin d'authentifier la connexion SSL. Lorsque la connexion SSL apparaît, une tentative est effectuée pour définir le certificat de périphérique qui sera utilisé. En cas d'échec, un message d'erreur est consigné, qui inclut le point de confiance configuré qui doit être utilisé pour charger le certificat du périphérique et la raison de l'échec.*trustpoint name : nom du point de confiance pour lequel SSL n'a pas pu définir de certificat de périphérique.***Action recommandée** : Résolvez le problème indiqué par la raison signalée pour l'échec.Assurez-vous que le point de confiance spécifié est inscrit et possède un certificat de périphérique.Assurez-vous que le certificat de périphérique est valide.Inscrivez à nouveau le point de confiance, si nécessaire.

## Informations connexes



- [Comment obtenir un certificat numérique d'une autorité de certification Microsoft Windows à l'aide d'ASDM sur un dispositif ASA](#)
- [Avis de champs relatifs aux produits de sécurité](#)
- [Demandes de commentaires \(RFC\)](#)
- [Support et documentation techniques - Cisco Systems](#)