# 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 <u>Conventions relatives aux conseils techniques Cisco.</u>

# Configuration

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

- 1. <u>Vérifiez que les valeurs Date, Heure et Fuseau horaire sont Exactes</u>.
- 2. <u>Générez la paire de clés RSA</u>.
- 3. <u>Créez le point de confiance</u>.
- 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.
- 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

ciscosa	
ciscoasa# <b>show clock</b>	
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.

24	Certificate					
00	Authentication					
net l	- Import Certificate	Key	/ Pair Name	Usage	Modulus Size	Add
	- Rey Pair					
VPN	- Anage Certificates					Show Details
	E- A Trustpoint					
l 🔒	Configuration	fe Add Key Pair			X	Delete
CSD Manager	- Sector		and the second	. <u>. 1116, 415, 415</u>		
-	E Contra Access					Refresh
428	E-S Device Administration	Name:	C Use default key nam	e .		
Routing	E-P DHCI Services		G mu unsisten trad	-		
on l	E-B DNS		(* Imy.vensign.key)			
68	High Availability and Scal	Con				
Global Objects	Fallover	Size.	1024			
	Fragment	Hereit	C. C. L.	Country		
20	HISTORY METRICS	Usage:	<ul> <li>General Purpose</li> </ul>	Special		
Properties	E-ID IP Audit					
	E Logging				_	
	- Priority Queue	Generate Now	Cancel	Help		
	SUNRPC Server					
	TCP Options					
	Timeouts					

- 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

ciscosa
ciscoasa# <b>conf t</b>
ciscoasa(config)# <b>crypto key generate rsa label my.verisign.key modulus 1024</b>
<pre>! 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)#</pre>

# 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**.

Configuration > Properties > Certificate > Trustpoint > Configuration						
Startup Wizard	Configuration					
🕀 🚮 AAA Setup	Configure a Certificate Authority (CA) as a trustopist					
	comigure a certificate Authority (CA) as a trustport.					
🔁 🖳 🖓 ARP						
Client Update	ſ					
E-M Certificate		Trustpoint Name	Device Certificate Subject	CA Certificate Subject	Add	
Authentication						
Enrolment					Edit	
Import Certificate						
- Sig Key Pair						
Manage Certificates					Delete	
E-Ba Trustpoint		N				
- 30 Contiguration		45			Request CRL	
Export						
- import						
Device Access						

- 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'<u>étape 2</u>. (*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 Attribute, entrez la valeur, puis cliquez sur

			Common Name (CN)	webypp cisco com
Attribute to be Ade	ded		Department (OU)	TSWEB
			Company Name (O)	Cisco Systems
tribute: Select	Attribute	Add >>	State (St)	North Carolina
			State (St)	US
ilue:		Delete	Location (L)	Raleigh
			,	

- 8. Une fois que les valeurs appropriées ont été ajoutées, cliquez sur OK.
- 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).

🚰 Certificate Parameters	×
Enter the values for the parameters that are to be included in the certificate.	
Subject DN: ystems,St=North Carolina,St=US,L=Raleigh Edit	
C Use FQDN of the device	
Specify FQDN     webvpn.cisco.com	
E-mail:	
IP Address:	
OK Cancel 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 Cor				
	niguration			
		-		
Trustpoint Name:	my.verisign.truspoint			
-	· · · · · · ·			
Generate a self	-signed certificate on enr	ollment		
If this option is e	nabled, only Key Pair and	l Certificate Parameters c	an be specified.	
Enrollment Settings	Revocation Check CE	L Retrieval Policy CRL 6	etrieval Method OCSP Rules	Advanced
				Haranooa
Key Pair:	my.verisign.key 🔻	Show Details	New Key Pair	
Challenge		Confirm Challenge		
Passworu. j		Fassword.		
Eprollment Mode	can only be specified if th	nere ere no certificates er	encipted with this trustmoint	
En onnore mode	carronity be specified in a	fore are no contributes a.	socialeu wan uns trustpoint.	
Enrollment Mode	,			
G Haama	we wall a second back and			
ve Use ma	nuai enroiment			
C Use ma	nual enroiment			
C Use aut	omatic enrollment			
C Use aut	omatic enrollment			
C Use aut Enrollmen	nuaien rollment comatic en rollment t URL: http://			
C Use aut Enrolmen	nual en rollment comatic en rollment t URL: http://	minutes		
C Use aut Enrollmen Retry Per	iomatic enrollment t URL: http://	minutes		
C Use aut Enrollmen Retry Per	nual en rollment comatic en rollment t URL: http://	minutes (Use 0 to indicate unlin	ited retries)	
C Use aut Enrollmen Retry Per Retry Cou	iomatic enrollment t URL: http://	minutes (Use 0 to indicate unlin	ited retries)	
C Use aut Enrollmen Retry Per Retry Cou	iomatic enrollment t URL: http://	minutes (Use 0 to indicate unlin	ited retries)	
C Use aut Enrollmen Retry Per Retry Cou	iomatic enrollment t URL: http://	minutes (Use 0 to indicate unlin	ited retries) Certificate Parameters	
C Use aut Enrollmen Retry Per Retry Cou	iomatic enrollment t URL: http://	minutes (Use 0 to indicate unlin	ited retries) Certificate Parameters	
C Use aut Enrollmen Retry Per Retry Cou	nual enrollment comatic enrollment t URL: http://	minutes (Use 0 to indicate unlin	ited retries) Certificate Parameters	
C Use aut Enrollmen Retry Per Retry Cou	iomatic enrollment t URL: http://	minutes (Use 0 to indicate unlin	ited retries) Certificate Parameters	

# Exemple de ligne de commande

ciscosa
ciscoasa(config)#crypto ca trustpoint my.verisign.trustpoint
! Creates the trustpoint.
ciscoasa(config-ca-trustpoint)# <b>enrollment terminal</b>
<pre>! Specifies cut and paste enrollment with this trustpoint. ciscoasa(config-ca-trustpoint)#subject-name CN=wepvpn.cisco.com,OU=TSWEB,</pre>
<pre>! Defines x.500 distinguished name. ciscoasa(config-ca- trustpoint)#keypair my.verisign.key</pre>
! Specifies key pair generated in <u>Step 3</u> . ciscoasa(config-ca-trustpoint)# <b>fqdn webvpn.cisco.com</b>
! Specifies subject alternative name (DNS:).

# Étape 4. Générer l'inscription au certificat

### Procédure ASDM

- 1. Cliquez sur Configuration, et ensuite sur Properties.
- 2. Développez Certificate, puis sélectionnez Enrollment.
- Vérifiez que le point de confiance créé à l'<u>étape 3</u> 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).

nrollment Request	
To complete the enrollment process, please paste the following PKCS10 enrollment request in management interface of the CA.	nto the
You will need to install the certificate after receiving it.	
Go to Configuration > Properties > Certificate > Import Certificate to do so.	
Certificate Request:	
hvcNAQkCFhtDaXNjbOFTQS5teWRvbWFpbi5jaXNjby5jb20wgZ8wDQYJKoZIhvc	N 📥
AQEBBQAD gYOAMIGJA oGBAL 5YNIx 1 zk fo80 ziV7 xJdfA7 jRtkHX x2Npmr9A0Q1Fz	m 
pshFF7/DekF1Q+RachaRbzngsgmirmNfonx6calcf9pb1vgFc1v3H2dsB6b3Gnik mAH40MDXhi18BH2SSgxPX6BGeiC9BiJ2vdgCgg+xB404/1YP0oeKKfg7anCHvVH	T T
AqMBAAGqRjBEBqkqhkiG9w0BCQ4xNzA1MAsGA1UdDwQEAwIFoDAmBqNVHREEHzA	a
ghtDaXNjb0FTQS5teWRvbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQBBBQADgYB	A
gmoBmSRVnL0qyDtpS1bveKew0AdG5/fxnJRYU2Uunl1W6sG0KaJYCiFH//eaewF	3
gEjVABVhB7Ni6N29710mDAbnPs0R3IyMwbr3eChIFwkZjBTwoe9LuR0gefWfyAH	o
gonnkGTJ11vZCSDXz4BXm4sXAqrwZCDdj0/S5BiQJGc=	
U	
kid - inis line not part of the certificate request	
<b>A</b> 14	
ОК	

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
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lz
dGVtczEO
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv
bTEhMB8G
CSqGSIb3DQEJAhYSY2lzY29hc2EuY2lzY28uY29tMIGfMA0GCSqGSIb3
DQEBAQUA
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB
9M4yTx5b
Fm886s8F73WsfQPynBDfBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt
30MXSNPO
mldZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX0luBMh7oKar
gwIDAQAB
oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBYw
FIISY2lz
Y29hc2EuY2lzY28uY29tMA0GCSqGSIb3DQEBBAUAA4GBABrxpY0q7Se0
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)#
```

# 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

Cert	ificate	? ×
Ge	neral Details Certification Path	
	Certificate Information	
	This certificate is intended for the following purpose(s):	
	<ul> <li>Ensures the identity of a remote computer</li> <li>Proves your identity to a remote computer</li> <li>2.16.840.1.113733.1.7.21</li> </ul>	

**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

Certificate	×
General Details Certification Path	
Certification path VeriSign Trial Secure Server Test Root CA VeriSign Trial Secure Server Test CA Webvpn.cisco.com	
View Certificate	
Certificate status:	
This certificate is OK.	
ОК	

#### certificat.

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'<u>étape 6</u>.

7. Cliquez sur Details

Certificate	<u>? ×</u>
General Details Certification Path	1
Show: <ali></ali>	
Field	Value
	V3
E Serial number	63 b1 a5 cd c5 9f 78 80 1d a0
🔚 Signature algorithm	sha1RSA
Issuer	VeriSign Trial Secure Server Te
Valid from	Tuesday, February 08, 2005 8
Valid to	Sunday, February 08, 2015 7:
Subject	VeriSign Trial Secure Server Te
	RSA (2048 Bits)
I	
E	dit Properties Copy to File
	ОК

(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.

Certificates can be exported in a variety of file formats. Select the format you want to use:
Select the format you want to use:
O DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
$\square$ Include all certificates in the certification path if possible
C Personal Information Exchange - PKC5 #12 (.PFX)
$\square$ Include all certificates in the certification path if possible
Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
Delete the private key if the export is successful
< Back Next > Cancel

- 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**.

ertificate Export Wizard				
File to Export Specify the name of the file you want to expo	rt			
File name:				
c:\introotca			Browse	
	< Back	Next >	Cano	:el

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

File Edit Format View Help

----BEGIN CERTIFICATE--MIIFSjçCBDKqAwIBAqIQCECQ47aTdj6BtrI60/Vt6zANBqkqhkiG9w0BAQUFADCB yzelMA&GA1UEBhMCVVMxFzAVBqNVBAoTD]Z]cm]TaWduLCBJbmMuMTAwLqYDVQQL ÉydGb3IqVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4xQjBABgNV BĀsTOVRĪcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3Bz L3R]c3RjYSAOYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwqU2VidXJ1IFN] cnZlciBUZXNOIENBMB4XDTA3MDcyNzAwMDAwMFoXDTA3MDgxMDIzNTkloVowgZ4x CZAJB9NVBAYTA]VTMRCwFQYDVQQIEw50b3J0aCBDYXJVbG]uYTEWMBQGA1UEČhQN Q21zY28qU31zdGVtczEOMAwGA1UECXQFVFNXRUIX0jA4BqNVBAsUMVR1cm1zIG9m IHVzZSBhdCB3d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMpMDUxEjAQBgNV BAMUCWNsaWVudHZwbjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA1V9Ahzsm SZiUwosov+yL/SMZUĹWKigVgwズlaVJ4UwqpUg9TqaIEn9wFvrZmJdOT/ucJW6k1A TjajzxxSocuVAKuJ7cnOxSj+KlHIBNUjz8Ey3r26nLa9fBCOK9YSZ6fA7zJimMQp RŴMāzEvoFaiiY+5oG7XAiWCPY4677K3INFECAWEAAaOCAdcwqqHTMAkGA1UdEwQC MAAwCwYDVR0PBAQDAgWgMEMGA1UdHwQ8MDowOKA2oDSGMmh0dHA6Ly9TV]JTZWN1 cmUtY3JsLnZlcmlzaŴdūLmNvbS9TVlJUcmlhbDIwMDUuY3JsMEoGALUdIARDMEEw PWYKYIZIAYb4RQEHFTAXMC8GCCsGAQUFBWIBFiNodHRwczovL3d3dy52ZXJpc2ln bi5jb20vY3BzL3Rlc3RjYTAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIw HwYDVR0jBBgwFoAUZiKOgeAxWd0qf6tGxTYCBnAnh1oweAYIKwYBBQUHAQEEbDBq MCQGCCsGAQUFBzABhhhodHRwOi8vb2NzcC52ZXJpc2lnbi5jb20wQgYIKwYBBQUH MAKGNmh0dHA6Ly9TvljTZWN1cmUtyWlhLnZlcmlzaWduLmNvbS9TvljUcmlhbDIw MDUtywlhLmNlcjBuBqqrBqEFBQcBDARiMGChXqBcMFowWDBWFqlpbWFnZS9naWYw ITAFMACGBSsOAwIaBBRLa7ko]gYMu9BSOJspresHiyEFGDAmFiRodHRw0i8vbG9n by52zxJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKozIhvcNAQEFBQADggEBAC4k abSwqooGaNtm4lrJhv8TSGsjdPpOspLSeBFxuLEzJlTHGprCf0sALrqb1FEL4b9q 1/EajjdteeYTqIorIC1aWwWx+RHCcTqIrlzf0vfUD0DNZ6949sM2aGaMzrRsBy63 Lb1/3+jz8skIAkiZP79pmqMEECZ+cUm10rk631c46yBCsJMZVbG6sZlNSI80RRwK hAKDsfufvsirHc8c9nJdoEC0905izUTrE854jvl×zŹji0J51FbcmCOx/uB7zv3zC Ftm412+TgfyZ3z7wCEnUlvhMa7bc2T3mmdqB5kCeHEZ2kAL6u6N0pXy5l7TLKy1a |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.

Configuration > Properties > C	ertificate > Authentication
Startup Wizard	Authentication
🕀 🚮 AAA Setup	Authenticate a CA certificate. As the result of authentication, the CA certificate will be associated with a
Anti-Spoofing	Inustroint and installed on the device
E-B ARP	
	Trustpoint Name:
	my vensign truspo
E E Certificate	
Authentication	Fingerprint (optional):
Enrollment	
- El Import Certificate	The certificate text can be specified if the selected trustpoint is configured for manual enrolment.
Key Pair	
Manage Certificates	Certificate Text
E-62 Trustpoint	Church from a Rev
Configuration	Comport from a file:
- Bxport	
	Inter the certificate text in hexadecimal or base64 format:
Device Access	A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJIIFNIcnZiciBUZXN0IFJvb3
Device Administration	ECCol67bggLewTagTia9h3MwDQYJKoZlhvcNAQEFBQADgYEASz5v8s3/
H-15 DHCP Services	Kqf234YROIL51ZS111oUZ2MANp2H4biw4itfsG5snDDIwSRmiH3BA//SU6E
DNS	Ai9TXvRlcD5q0mB+nyK9fB2aBzOiaiHSilWzAJeQjuqA+Q93jNew+peuj4Ahc
High Availability and Scal	n/KK/+1Yv61w3+7g6ukFMARVBNg=
Falover	END CERTIFICATE
Fragment	
HISTORY METRICS	
	📬 Authentication Successful
Priority Queue	
	(i) The trustpoint my verisign truspoint has been authenticated.
SINRPC Server	
- Timeouts	
URL Filtering	OK
H- S WCCP	

### 21. Click OK.

# Exemple de ligne de commande

ciscosa
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
itselfBEGIN CERTIFICATE
MIIEwDCCBCmgAwIBAgIQY7GlzcWfeIAdoGNs+XVGezANBgkqhkiG9w0B
AQUFADCB
${\tt jDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTD1Z1cm1TaWduLCBJbmMuMTAw}$
LGYDVQQL
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4x
MjAwBgNV
BAMTKVZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBSb290
IENBMB4X
DTA1MDIwOTAwMDAwMFoXDTE1MDIwODIzNTk10VowgcsxCzAJBgNVBAYT
Alvimcw
FQYDVQQKEw5WZXJpU21nbiwgSW5jLjEwMC4GA1UECxMnRm9yIFR1c3Qg
UHVycG9z
ZXMgT25seS4gIE5vIGFzc3VyYW5jZXMuMUIwQAYDVQQLEz1UZXJtcyBv
ZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMp
MDUxLTAr
BgNVBAMTJFZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBD

QTCCASIW
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAu
wElv6IJ/
${\tt DV8zgpvxuwdaMv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE6}$
1BBD6Zqk
d851P1/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45
1P4qoyqS
E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1
D/OCCmZO
5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4tlqj97ydk5iDo
xjKfV6sb
tnp3TIY6S07bTb9gxJCk4pGbcf8DOPvOfGRu1wpfUUZC8v+WKC20+sK6
QMECAWEA
AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA
BgpghkgB
hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3LnZ1cmlzaWdu
LmNvbS9j
CHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD
ALUADGQWBBRmI06B4DFZ3Sp/qUbFNgIGcCeHWjCBsgYDVR0jBIGqMIGn
MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIE1uYy4x
BASTJUZVCIBUZXNUIFBICHBVC2VZIE9UDHRUICBODYBHC3NICMFUY2VZ
AIOEAXMPVMVYAVNPZZ4GVHJPIWWGOZVJAXJIIFNICHZICIBOZXNOIFUV
CCCCIC/DGGLewiagIIa9H5MwDQIDKOZIHVCNAQEFBQADGIEA525V055/
SJZKVIZI Kaf234YBOiL51ZS111oUZ2MANo2H4biw4itfeG5enDD1wSBmiH3BW/SU
Adissing in the second se
Ai9TXvRTcD5a0mB+nvK9fB2aBz0iaiHSiTWzA.TeOiuaA+093iNew+neu
i4AhdwGN
n/KK/+1Yy61w3+7g6ukFMARVBNg=
END CERTIFICATE
guit
! 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 Properties.
- 2. Développez Certificate, 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.

Configuration > Properties > C	ertificate > Import Certificate
- 39 Startup Wizard	Import Certificate
🕀 🚮 AAA Setup	Install an identity cartificate that was received from a Cartificate Authority (CA) in resource to a menual
- B Anti-Spoofing	enrolled net set
🟵 🐻 ARP	en ennen i copiesi.
	Trustediet Manuel
E Certificate	my.vensign.truspo
- Authentication	
- 2 Enrolment	Certificate Text
Import Certificate	C hand from a flat
Key Pair	s import from a life.
Manage Certificates	
E-82 Trustpoint	1. Enter the certificate text in nexadecimal or baseb4 format.
Configuration	
- Seport	MS5pd4/V46DOV_Ko7IkusN4.0EEB0.4DapEB.4/06/auSKE0/daaA/V/d84/c
import	missian with the range in the state of the s
Device Access	tFkFFSFbleCK/hh6MaMb40z6kiFizo/Umt6JDoU3B00U/vm+tg02eTWdzr/VE
E-SD Device Administration	0YVwM3kDQA06EbArtUoAxovDbJucdxb6ZVTtyevMcgzCkXMHEVxa5/P)
P-B DNS	ssX9YJtvhNjaKCHzSHstd69N20SmluEOR4utcGgGZD8itVGx26b5OWTz8K:
High Availability and Scal	8EvHm3grdbDZP+ISMotWYYE+CgfKpZb+CPAqH2Cdpz2aJljJhl6CS6NM=
Failover	END CERTIFICATE
- K Fragment	
- Istory Metrics	
- TP/HTTP/	fig Information
🖅 🔩 IP Audit	
E-1 Logging	
- Priority Queue	Certificate import succeeded.
- 📲 SSL	
SUNRPC Server	
TCP Options	
Timeouts	L
UKL Fitering	
E- WCCP	
I	

4. Cliquez sur Importer, puis sur OK.

# Exemple de ligne de commande

ciscosa
ciscoasa(config)#crypto ca import my.verisign.trustpoint
certificate
<pre>! 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 itselfBEGIN CEPTIFICATE</pre>
MITEZiCCBE6gAwIBAgIOMs/oXuu9K14eMGSf0mYifTANBgkghkiG9w0B
AOUFADCB
yzELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAw
LgYDVQQL
EydGb3IgVGVzdCBQdXJwb3N1cyBPbmx5LiAgTm8gYXNzdXJhbmN1cy4x
QJBABGNV BAsTOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc21nbi5j b20vY3Bz
L3Rlc3RjYSAoYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2Vj dXJ11FN1
cnZlciBUZXN0IENBMB4XDTA3MDcyNjAwMDAwMFoXDTA3MDgwOTIzNTk1 OVowgbox
CzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3J0aCBDYXJvbGluYTEQMA4G A1UEBxOH
UmFsZWlnaDEWMBQGA1UEChQNQ2lzY28gU3lzdGVtczEOMAwGA1UECxQF VFNXRUIx

OjA4BgNVBAsUMVRlcm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29t
L2Nwcy90
ZXN0Y2EgKGMpMDUxHDAaBgNVBAMUE2Npc2NvYXNhMS5jaXNjby5jb20w
gZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL56EvorHHlsIB/VRKaRlJeJKCrQ
/9ker2jQ
9UOkUP3mVPZJtYN63ZxDwACeyNb+1iIdKUegJWHI0Mz3GHqcgEkKW1Ec
rO+6aY1R
IaUE8/LiAZbA70+k/9Z/UR+v532B1nDRwbx1R9ZVhAJzA1hJTxSlEgry
osBMMazg
5IcLhgSpAgMBAAGjggHXMIIB0zAJBgNVHRMEAjAAMAsGA1UdDwQEAwIF
oDBDBgNV
HR8EPDA6MDigNqA0hjJodHRwOi8vU1ZSU2VjdXJ1LWNybC52ZXJpc21n
bi5jb20v
U1ZSVHJpYWwyMDA1LmNybDBKBgNVHSAEQzBBMD8GCmCGSAGG+EUBBxUw
MTAvBggr
BgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0
Y2EwHQYD
VR01BBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMB8GA1UdIwQYMBaAFGYi
joHgMVnd
Kn+rRsU2AgZwJ4daMHgGCCsGAQUFBwEBBGwwajAkBggrBgEFBQcwAYYY
aHR0cDov
L29jc3AudmVyaXNpZ24uY29tMEIGCCsGAQUFBzAChjZodHRwOi8vU1ZS
U2VjdXJ1
LWFpYS52ZXJpc21nbi5jb20vU1ZSVHJpYWwyMDA1LWFpYS5jZXIwbgYI
KwYBBQUH
AQwEYjBgoV6gXDBaMFgwVhYJaW1hZ2UvZ21mMCEwHzAHBgUrDgMCGgQU
S2u5KJYG
DLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29t
L3ZzbG9n
bzEuZ21mMA0GCSqGSIb3DQEBBQUAA4IBAQAnym4GVThPIyL/9y1DBd8N
7/y₩30v3
bIirHfHJyfPJ1znZQXyXdObpZkuA6Jyu03V2CYNnDomn4xRXQTUDD8q8
6ZiKyMIj
XM2VCmcHSajmMMRyjpydxfk6CIdDMtMGotCavRHD9Tl2tvwgrBock/v/
540021kB
SmLzVV7crlYJEuhgqu3Pz7qNRd8N0Un6c9sbwQ1BuM99QxzIzdAo89FS
ewy8MAIY
rtab5F+oiTc5xGy8w7NARAfNgFXihqnLgWTtA35/oWuy86bje1IWbeyq
j8ePM9Td
0LdAw6kUU1PNimPttMDhcF7cuevntR0ks0gQPBPx5FJSqMiUZGrvju50
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.

Configuration > Properties > SS	
Startup Wizard	SSL
🕀 🚽 AAA Setup	Configure SSI parameters. These parameters affect both ASDM and MehV/BN access
-3 Anti-Spoofing	Configure 35L parameters. These parameters affect our ASUM and Yeb/YEM access.
te-103 ARP	Server SSL Version: Any Client SSL Version: Any
	Encryption
	a no post
🕀 🚰 Certificate	Available Algorithms Add >> Active Algorithms Move Up
E Device Access	3DES-SHA1
E-B Device Administration	file Edit SSL Trustpoint
E DHCP Services	
🕀 🚚 DNS	Specify an enrolled trustpoint to be used for SSL authentication on the outside interface. To enroll a trustpoint
High Availability and Scal	go to Configuration > Properties > Certificate > Enrolment.
Failover	
- Fragment	
History Metrics	
- HTTP/HTTPS	Interface: outside
E-IO IP Audit	
E Logging	Enrolled Trustpoint: my.verisign.trustp 💌
Priority Queue	
- <u>16 551</u>	
SUNRPC Server	
TCP Options	Cancer nep
UPI Filtering	
E ONL Filtering	Trustpoints
W-W WOOP	Sherify which enrolled tructments if any should be used for SSI authentication on each interfere. The fallback
	business of the second statements in any second with a trustroint of their own
	Fallback Trustroidt
	Interface Trustroint Eve
	management
	norrogenetic
	ourside my werrarge un daupoin in

- 4. Dans la liste déroulante Point de confiance inscrit, sélectionnez le point de confiance que vous avez créé à l'<u>étape 3</u>.
- 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

```
CiSCOSA

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: 694687al 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 VerisignVous 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



#### Exemple de ligne de commande

ciscosa
ciscoasa(config)# <b>show crypto ca certificates</b>
<pre>! 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</pre>



### 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 siteVérifiez 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. Àl'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

Certificate	?
General Details Certification Path	
Certificate Information	
This certificate is intended for the following purpose(s):	
•Ensures the identity of a remote computer	
* Refer to the certification authority's statement for details.	
Issued to: webvpn.cisco.com	
Issued hur VeriSian Trial Secure Server Test CA	
ISSUED BY: Vensight mail becure berver fest CA	
Valid from 8/14/2007 to 8/29/2007	
Install Certificate Issuer Staten	nent
	ок
	5

# 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 cris 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 importéLe 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 certificateCette 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 keyCette 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.Assurezvous 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

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