

Configuration de l'ASA : installation et renouvellement de certificats numériques SSL

Table des matières

[Introduction](#)

[Informations générales](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Génération CSR](#)

[1. Configurez avec l'ASDM](#)

[2. Configurez avec l'ASACL](#)

[3. Utiliser OpenSSL pour générer le CSR](#)

[Génération de certificat SSL sur l'autorité de certification](#)

[Exemple de génération de certificat SSL sur GoDaddy CA](#)

[Installation du certificat SSL sur l'ASA](#)

[1.1 Installation du certificat d'identité au format PEM avec ASDM](#)

[1.2. Installation d'un certificat PEM avec l'interface de ligne de commande](#)

[2.1 Installation d'un certificat PKCS12 avec ASDM](#)

[2.2 Installation d'un certificat PKCS12 avec l'interface de ligne de commande](#)

[Vérifier](#)

[Afficher les certificats installés via ASDM](#)

[Afficher les certificats installés via la CLI](#)

[Vérification du certificat installé pour WebVPN avec un navigateur Web](#)

[Renouveler le certificat SSL sur l'ASA](#)

[Forum aux questions](#)

[1. Quel est le meilleur moyen de transférer des certificats d'identité d'un ASA vers un autre ASA ?](#)

[2. Comment générer des certificats SSL à utiliser avec les ASA d'équilibrage de charge VPN ?](#)

[3. Les certificats doivent-ils être copiés de l'ASA principal vers l'ASA secondaire dans une paire de basculement ASA ?](#)

[4. Si des clés ECDSA sont utilisées, le processus de génération de certificat SSL est-il différent ?](#)

[Dépannage](#)

[Dépannage des commandes](#)

[Problèmes courants](#)

[Annexe](#)

[Annexe A : ECDSA ou RSA](#)

[Annexe B : Utiliser OpenSSL pour générer un certificat PKCS12 à partir d'un certificat d'identité, d'un certificat d'autorité de certification et d'une clé privée](#)

[Informations connexes](#)

Introduction

Le présent document décrit l'installation d'un certificat numérique SSL approuvé tiers sur l'ASA pour les connexions AnyConnect et SSLVPN sans client.

Informations générales

Un certificat GoDaddy est utilisé dans cet exemple. Chaque étape contient la procédure ASDM (Adaptive Security Device Manager) et l'équivalent de l'interface de ligne de commande.

Conditions préalables

Exigences

Ce document nécessite l'accès à une autorité de certification tierce approuvée pour l'inscription de certificat. Parmi les fournisseurs d'autorité de certification tiers, citons, entre autres, Baltimore, Cisco, Entrust, Geotrust, G, Microsoft, RSA, Thawte et VeriSign.

Avant de commencer, vérifiez que l'ASA dispose de l'heure, de la date et du fuseau horaire corrects. Avec l'authentification de certificat, il est recommandé d'utiliser un serveur NTP (Network Time Protocol) pour synchroniser l'heure sur l'ASA. Le [Guide de configuration CLI des opérations générales de la gamme Cisco ASA, 9.1](#) détaille les étapes à suivre afin de configurer correctement l'heure et la date sur l'ASA.

Composants utilisés

Ce document utilise un ASA 5500-X qui exécute la version logicielle 9.4.1 et ASDM version 7.4(1).

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Le protocole SSL exige que le serveur SSL fournisse au client un certificat de serveur pour que le client effectue l'authentification du serveur. Cisco déconseille l'utilisation d'un certificat auto-signé, car un utilisateur peut configurer par inadvertance un navigateur pour faire confiance à un certificat provenant d'un serveur non autorisé. Il est également gênant pour les utilisateurs de devoir répondre à un avertissement de sécurité lorsqu'ils se connectent à la passerelle sécurisée. Il est recommandé d'utiliser des autorités de certification tierces de confiance pour émettre des certificats SSL à l'ASA à cette fin.

Le cycle de vie d'un certificat tiers sur l'ASA se déroule essentiellement comme suit :



Génération CSR

La génération CSR est la première étape du cycle de vie de tout certificat numérique X.509.

Une fois que la paire de clés privée/publique Rivest-Shamir-Adleman (RSA) ou Elliptic Curve Digital Signature Algorithm (ECDSA) est générée ([l'annexe A](#) détaille la différence entre l'utilisation de RSA ou d'ECDSA), une demande de signature de certificat (CSR) est créée.

Un CSR est un message au format PKCS10 qui contient la clé publique et les informations d'identité de l'hôte qui envoie la demande. [Formats de données PKI](#) explique les différents formats de certificat applicables à l'ASA et à Cisco IOS®.

Remarques :

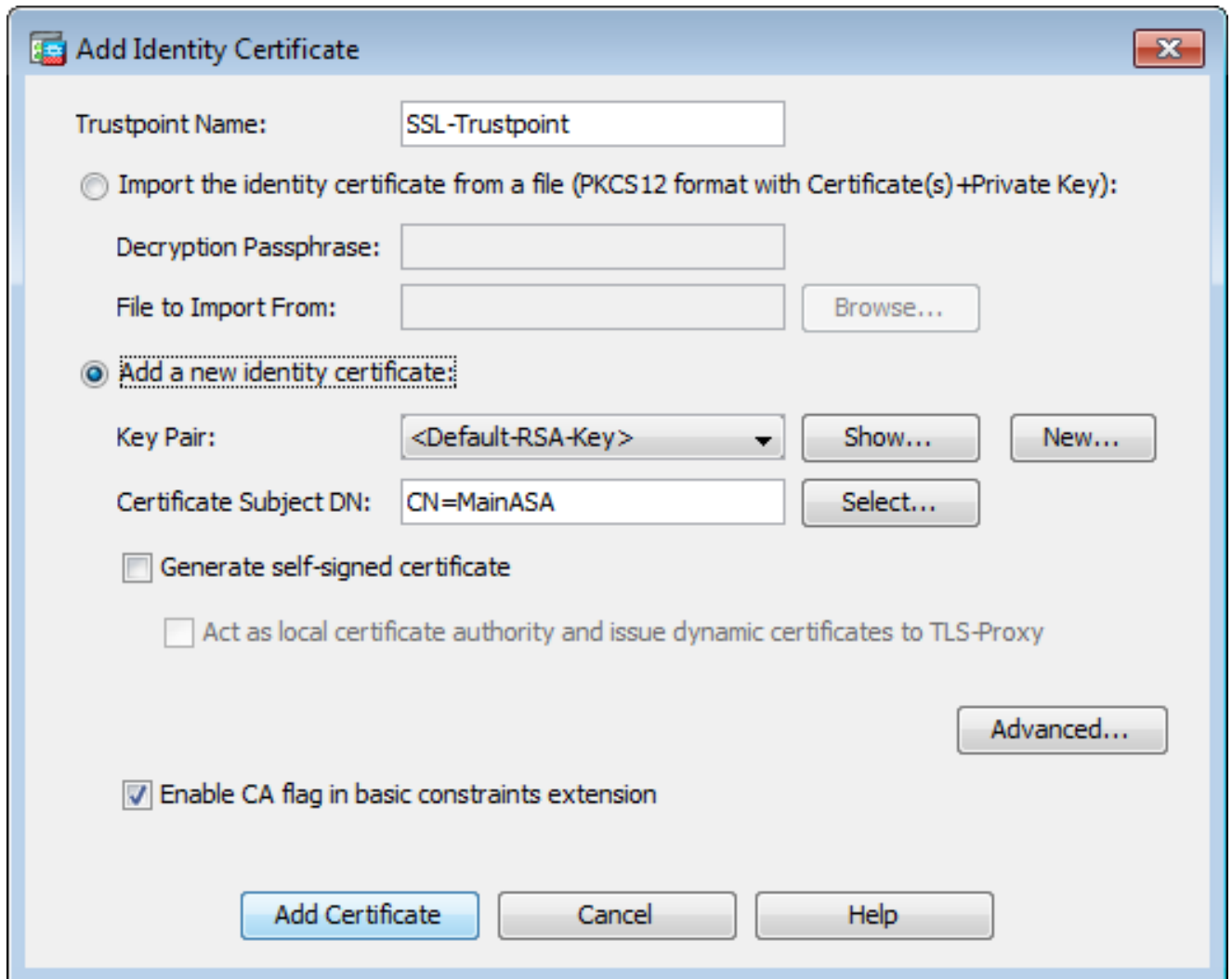
1. Vérifiez auprès de l'autorité de certification la taille de paire de clés requise. Le forum CA/Browser a exigé que tous les certificats générés par leurs CA membres aient une taille minimale de 2048 bits.
 2. ASA ne prend actuellement pas en charge les clés 4 096 bits (ID de bogue Cisco [CSCut53512](#)) pour l'authentification du serveur SSL. Cependant, IKEv2 prend en charge l'utilisation de certificats de serveur 4096 bits sur les plates-formes ASA 5580, 5585 et 5500-X uniquement.
 3. Utilisez le nom DNS de l'ASA dans le champ FQDN du CSR afin d'empêcher les avertissements de certificats non approuvés et de passer le contrôle de certificat strict.
-

Il existe trois méthodes pour générer une RSE.

- Configurer avec ASDM
- Configuration avec l'interface CLI ASA
- Utiliser OpenSSL pour générer le CSR

1. Configurez avec l'ASDM

1. Naviguez jusqu'à **Configuration > Remote Access VPN > Certificate Management** et choisissez **Identity Certificates**.
2. Cliquer **Add**.



Add Identity Certificate

Trustpoint Name:

Import the identity certificate from a file (PKCS12 format with Certificate(s) +Private Key):

Decryption Passphrase:

File to Import From:

Add a new identity certificate:

Key Pair:

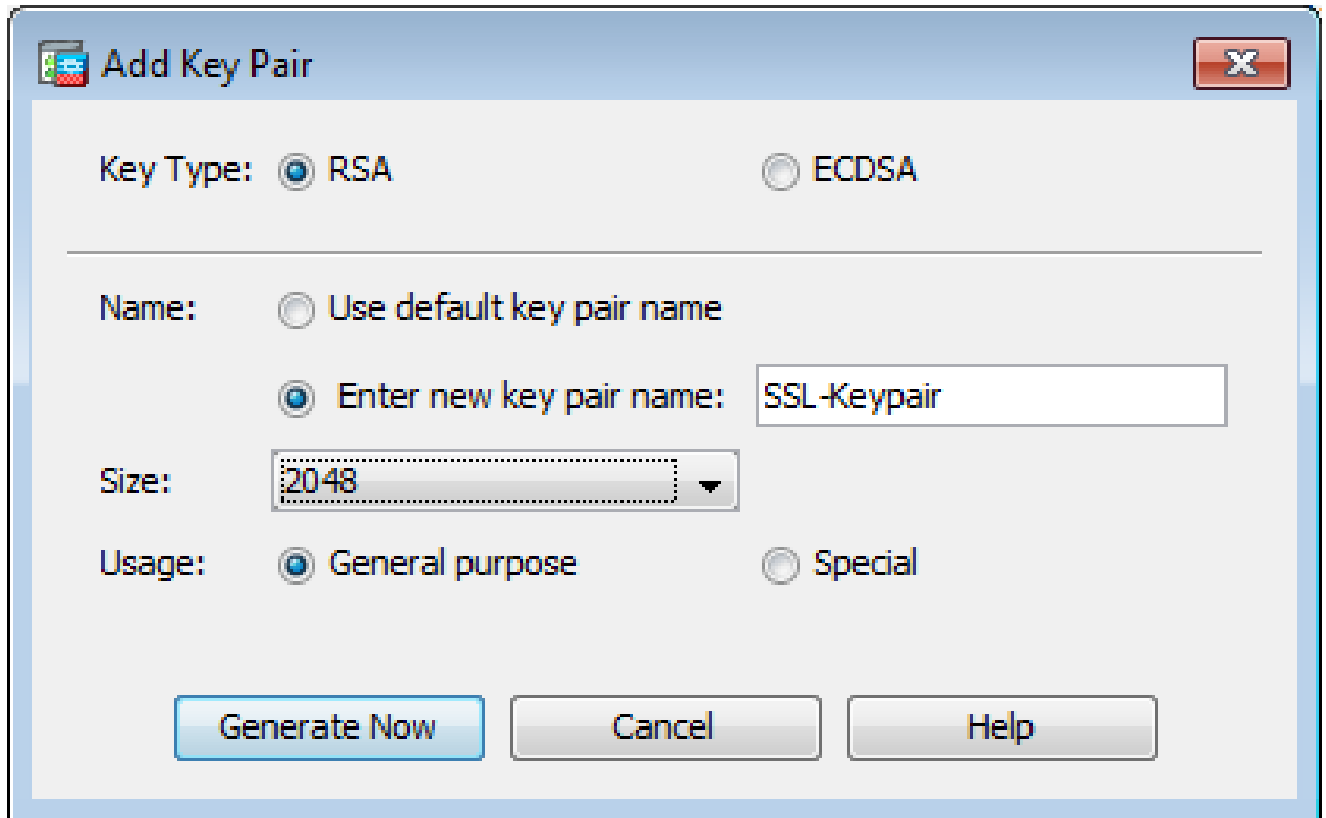
Certificate Subject DN:

Generate self-signed certificate

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

Enable CA flag in basic constraints extension

3. Définissez un nom de point de confiance dans le champ d'entrée Nom du point de confiance.
4. Cliquez sur le bouton **Add a new identity certificate** de l'assistant.
5. Pour la paire de clés, cliquez sur **New**.




6. Sélectionnez le type de clé : RSA ou ECDSA. (Reportez-vous à l'[annexe A](#) pour comprendre les différences.)
7. Cliquez sur le bouton `Enter new key pair name` de l'assistant. Identifiez le nom de la paire de clés pour la reconnaissance.
8. Sélectionnez la `Key Size`. Choisissez `General Purpose for Usage` avec RSA.
9. Cliquez `Generate Now`. La paire de clés est créée.
10. Pour définir le DN du sujet du certificat, cliquez sur `Select` et configurez les attributs répertoriés dans ce tableau :

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

Pour configurer ces valeurs, choisissez une valeur dans la liste déroulante Attribut, entrez la valeur, puis cliquez sur Ajouter.

Attribute	Value
Common Name (CN)	vpn.remoteasa.com
Company Name (O)	Company Inc
Country (C)	US
State (St)	California
Location (L)	San Jose

 Remarque : certains fournisseurs tiers exigent l'inclusion d'attributs particuliers avant l'émission d'un certificat d'identité. Si vous n'êtes pas sûr des attributs requis, renseignez-vous auprès du fournisseur.

11. Une fois les valeurs appropriées ajoutées, cliquez sur **OK**. La boîte de dialogue Ajouter un certificat d'identité apparaît avec le certificat **Subject DN** field populated.
12. Cliquez sur **Advanced**.

Enrollment mode parameters and SCEP challenge password are not available for self-signed certificates.

Certificate Parameters | Enrollment Mode | SCEP Challenge Password

FQDN: vpn.remoteasa.com

E-mail:

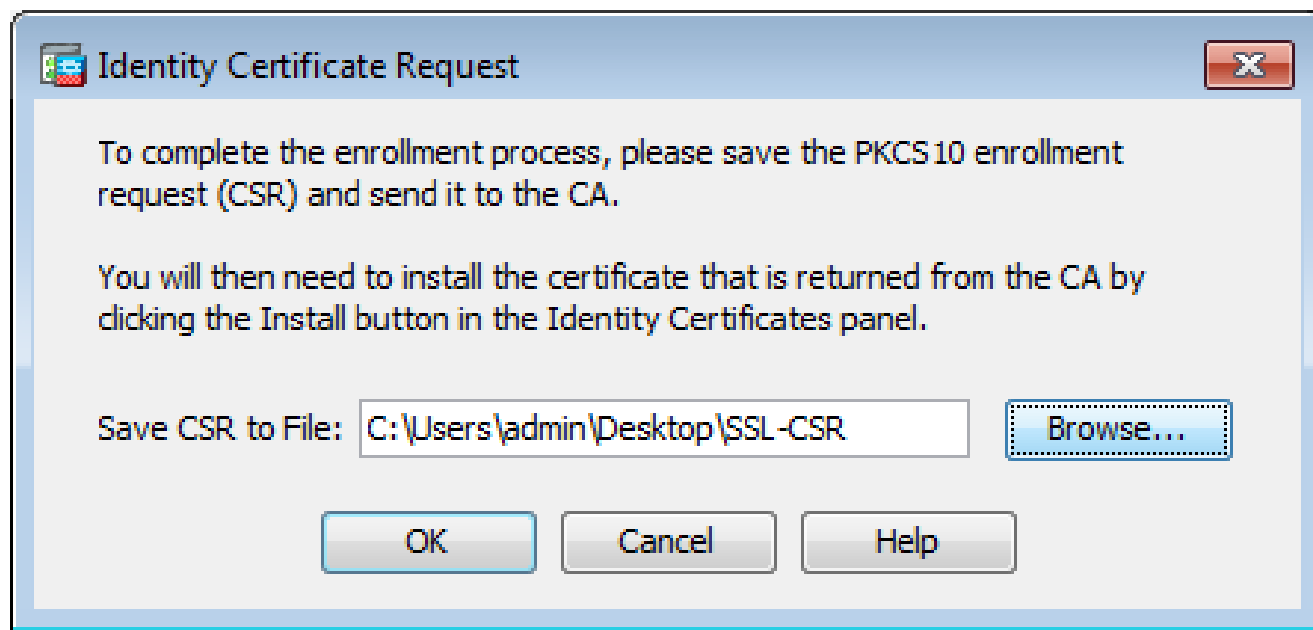
IP Address:

Include serial number of the device


13. Dans la **FQDN** saisissez le nom de domaine complet (FQDN) utilisé pour accéder au

périphérique à partir d'Internet. Cliquez sur **OK**.

14. Laissez l'option d'extension Activer CA dans les contraintes de base cochée. Les certificats sans l'indicateur CA ne peuvent plus être installés sur l'ASA comme certificats CA par défaut. L'extension des contraintes de base identifie si l'objet du certificat est une autorité de certification et la profondeur maximale des chemins d'accès de certification valides qui incluent ce certificat. Décochez l'option permettant de contourner cette exigence.
15. Cliquez sur **OK**, puis cliquez sur **Add Certificate**. Une invite s'affiche pour enregistrer le CSR dans un fichier sur l'ordinateur local.



16. Cliquez sur **Browse**, choisissez un emplacement dans lequel enregistrer le CSR et enregistrez le fichier avec l'extension `.txt`.

 Remarque : lorsque le fichier est enregistré avec une extension `.txt`, la demande PKCS#10 peut être ouverte et affichée à l'aide d'un éditeur de texte (tel que le Bloc-notes).

2. Configurer avec l'interface de ligne de commande ASA

Dans l'ASDM, le point de confiance est automatiquement créé lorsqu'un CSR est généré ou lorsque le certificat CA est installé. Dans l'interface CLI, le point de confiance doit être créé manuellement.

```
<#root>
```

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

```
MainASA(config)#
```

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

```
INFO: The name for the keys are: SSL-Keypair
```

Keypair generation process begin. Please wait...

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

MainASA(config)#

crypto ca trustpoint SSL-Trustpoint

MainASA(config-ca-trustpoint)#

enrollment terminal

MainASA(config-ca-trustpoint)#

fqdn (remoteasavpn.url)

MainASA(config-ca-trustpoint)#

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

MainASA(config-ca-trustpoint)#

keypair SSL-Keypair

MainASA(config-ca-trustpoint)#

exit

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

MainASA(config)#

crypto ca enroll SSL-Trustpoint

WARNING: The certificate enrollment is configured with an fqdn that differs from the system fqdn. If this certificate is used for VPN authentication this may cause connection problems.

Would you like to continue with this enrollment? [yes/no]:

yes

% Start certificate enrollment ..

% The subject name in the certificate is: subject-name CN=

(remoteasavpn.url)

,

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

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

(remoteasavpn.url)

,

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

no

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

yes

Certificate Request:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDDjCCAfYCAQAwYkxETAPBgNVBACTCFNhbiBkb3NlMRMwEQYDVQIQIEwpDYWxp
Zm9ybm1hMQswCQYDVQQGEwJVUzEUMBIGA1UEChMLQ29tcGFueSBjbmMxGjAYBgNV
BAMTEXZwbi5yZW1vdGVhc2EuY29tMSAwHgYJKoZIhvcNAQkCFhF2cG4ucmVtb3Rl
YXNhLmNvbTCCASIdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK62Nhb9kt1K
uR3Q4TmksyuRMqJNrb9KXpvA6H200PuBfQvSF4rVnSwK0mu3c8nweEvYcdVwV6Bz
BhjXeovTVi17F1NTceaUTGikeIdXC+mw1iE7eRsynS/d4mzMWJmrvsDNzpAW/EM
SzTca+BvqF7X2r3LU8Vsv60i8ylhco9Fz7bWvRWvt03NDDbyo1C9b/VgXMuBitcc
rzfUbVnm7VZD0f4jr9EXgUwXxcQi dWEAB1FrXrtYpFgBo9aqJmRp2YABQ1ieP4cY
3rBtgRjLcF+S9TvHG5m4v7v755meV4YqsZIXvytI0zVBihemVxaGA1oDwfkoYSFi
4CzXbFvdG6kCAwEAaA/MD0GCSqGSIb3DQEJJDjEwMC4wDgYDVROPAQH/BAQDAgWg
MBwGA1UdEQQVMBOCEXZwbi5yZW1vdGVhc2EuY29tMA0GCSqGSIb3DQEBBQUAA4IB
AQBZuQzUXGEB0ix1yuPK0ZkRz8bPnwIqLTfxZhagmuyEhrN7N4+aQnCHj85oJane
4ztZDiCCoWTerBS4RSKKEHEspu9oohjCYuNnp5qa91SPrZNEjTww0eRn+qKbId2J
jE6Qy4vdPCexavMLYVQxCny+gVkzPN/sFRk3EcTTvq6DxxaebpJijmiqa7gCph52
YkHXnFne1LQd41BgoL1Cr9+hx74XsTHGBmI1s/9T5oAX26Ym+B21/i/DP5BktIUA
8GvIY1/ypj9K049fP5ap8a10qvLtYYcCcfwrCt+0oj0rZ1YyJb3dFuMNRdAX37t
DuHN12EYNpYkjVk1wI53/5w3
-----END CERTIFICATE REQUEST-----
```


Redisplay enrollment request? [yes/no]:

no

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

3. Utiliser OpenSSL pour générer le CSR

OpenSSL utilise l'`openssl.cnf` pour extraire les attributs à utiliser dans la génération CSR. Ce processus aboutit à la génération d'une CSR et d'une clé privée.

 Attention : vérifiez que la clé privée générée n'est partagée avec personne d'autre car elle compromet l'intégrité du certificat.

1. Assurez-vous qu'OpenSSL est installé sur le système sur lequel ce processus est exécuté. Pour les utilisateurs de Mac OSX et GNU/Linux, cette option est installée par défaut.
2. Basculer vers un répertoire fonctionnel.

Sous Windows : par défaut, les utilitaires sont installés dans `C:\openssl\bin`. Ouvrez une invite de commandes à cet emplacement.

Sous Mac OSX/Linux : ouvrez la fenêtre Terminal dans le répertoire nécessaire à la création du CSR.

3. Créez un fichier de configuration OpenSSL avec un éditeur de texte avec les attributs donnés . Une fois fait, enregistrez le fichier sous le nom `openssl.cnf` à l'emplacement mentionné à l'étape précédente (Si vous utilisez la version 0.9.8h et ultérieure, le fichier est `openssl.cfg`)

<#root>

```

[req]

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

[req_distinguished_name]

commonName = Common Name (eg, YOUR name)
commonName_default = (asa.remotevpn.url)

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

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

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

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

```

```

[req_ext]

subjectAltName = @alt_names

```

```

[alt_names]

DNS.1 = *.remotearsa.com

```

4. Générez le CSR et la clé privée avec cette commande :

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

```
<#root>
```

```
# Sample CSR Generation:
```

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

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

```

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

```

```

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

```

If you enter '.', the field will be left blank.

```
-----  
Common Name (eg, YOUR name) [(asa.remotevpn.ur1)]:  
Country Name (2 letter code) [US]:  
State or Province Name (full name) [California]:  
Locality Name (eg, city) [San Jose]:  
Organization Name (eg, company) [Company Inc]:
```

Envoyez le CSR enregistré au fournisseur de l'autorité de certification tierce. Une fois le certificat émis, l'autorité de certification fournit le certificat d'identité et le certificat d'autorité de certification à installer sur l'ASA.

Génération de certificat SSL sur l'autorité de certification

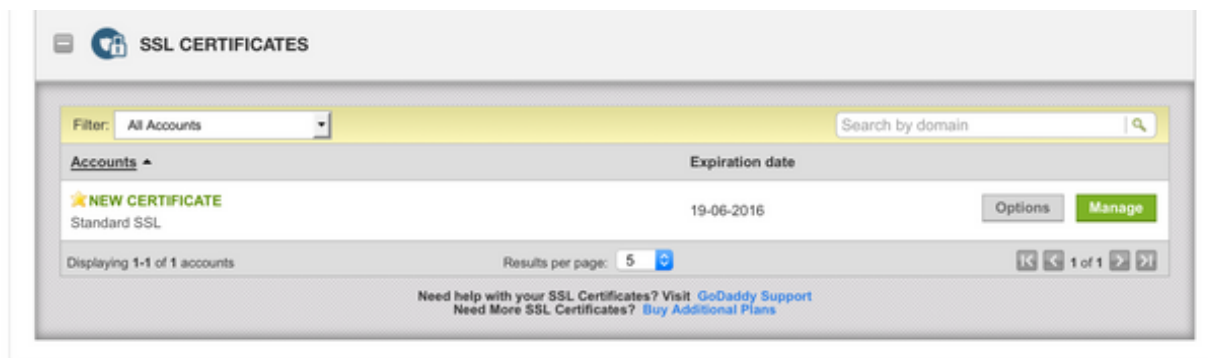
L'étape suivante consiste à faire signer le CSR par l'autorité de certification. L'autorité de certification fournit soit un certificat d'identité codé PEM nouvellement généré, soit un certificat PKCS12 avec l'ensemble de certificats de l'autorité de certification.

Si le CSR est généré en dehors de l'ASA (soit via OpenSSL, soit sur l'autorité de certification elle-même), le certificat d'identité codé PEM avec la clé privée et le certificat de l'autorité de certification sont disponibles sous forme de fichiers séparés. [L'annexe B](#) présente les étapes à suivre pour regrouper ces éléments dans un fichier PKCS12 unique (au format .p12 ou .pfx) .

Dans ce document, l'autorité de certification GoDaddy est utilisée comme exemple pour délivrer des certificats d'identité à l'ASA. Ce processus diffère chez les autres fournisseurs d'autorité de certification. Lisez attentivement la documentation de l'autorité de certification avant de continuer.

Exemple de génération de certificat SSL sur GoDaddy CA

Après l'achat et la phase de configuration initiale du certificat SSL, accédez au compte GoDaddy et affichez les certificats SSL. Il doit y avoir un nouveau certificat. Cliquez sur **Manage** pour continuer.



Une page s'affiche alors pour fournir la RSE telle qu'elle apparaît dans cette image.

En fonction du CSR saisi, l'autorité de certification détermine le nom de domaine auquel le certificat doit être délivré.

Vérifiez qu'il correspond au nom de domaine complet de l'ASA.

Choose website

Select a domain hosted with us

Provide a certificate signing request (CSR)

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

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

Domain Name (based on CSR):

vpn.remoteasa.com

Domain ownership

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

AND

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


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

[Hide advanced options](#)

Signature Algorithm [Learn more](#)

GoDaddy SHA-2

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

 Remarque : GoDaddy et la plupart des autres CA utilisent SHA-2 ou SHA256 comme algorithme de signature de certificat par défaut. ASA prend en charge l'algorithme de signature SHA-2 qui commence à partir de 8.2(5) [versions antérieures à 8.3] et de 8.4(1) [versions postérieures à 8.3] (ID de bogue Cisco [CSCti30937](#)). Sélectionnez l'algorithme de signature SHA-1 si une version antérieure à 8.2(5) ou 8.4(1) est utilisée.

vpn.remoteasa.com > Download Certificate

Standard SSL Certificate

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

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

Server type

Select ...

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

File

Cancel

Le fichier .zip contient le certificat d'identité et les groupes de chaînes de certificats de l'autorité de certification GoDaddy sous la forme de deux fichiers .crt distincts. Passez à l'installation de certificats SSL pour installer ces certificats sur l'ASA.

Installation du certificat SSL sur l'ASA

Le certificat SSL peut être installé sur l'ASA avec l'ASDM ou l'interface de ligne de commande de deux manières :

1. Importez l'autorité de certification et le certificat d'identité séparément dans les formats PEM.
2. Vous pouvez également importer le fichier PKCS12 (codé en base64 pour l'interface de ligne de commande) dans lequel le certificat d'identité, le certificat d'autorité de certification et la clé privée sont regroupés dans le fichier PKCS12.

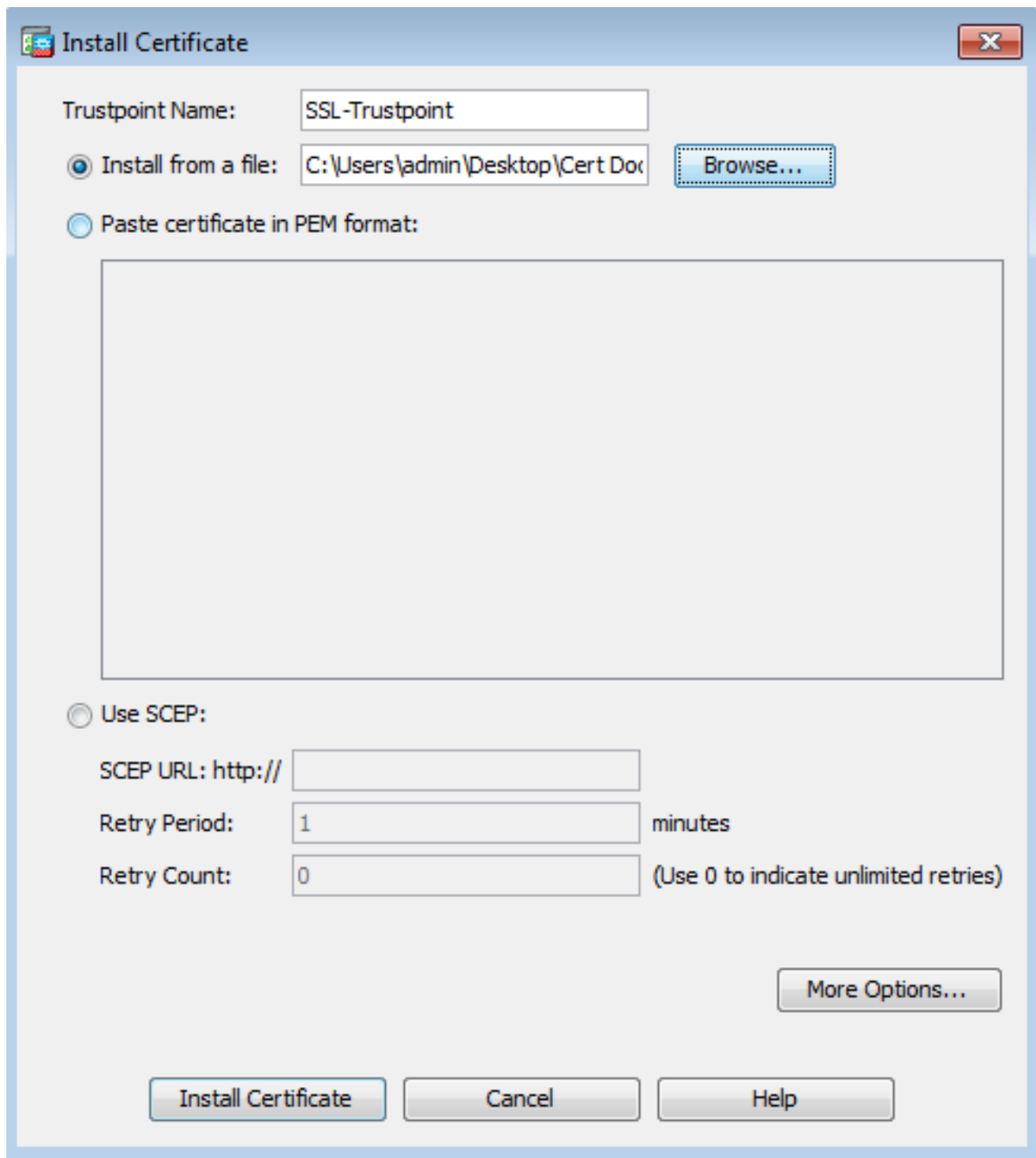


Remarque : si l'autorité de certification fournit une chaîne de certificats d'autorité de certification, installez uniquement le certificat d'autorité de certification intermédiaire immédiat dans la hiérarchie sur le point de confiance utilisé pour générer le CSR. Le certificat d'autorité de certification racine et tout autre certificat d'autorité de certification intermédiaire peuvent être installés dans de nouveaux points de confiance.

1.1 Installation du certificat d'identité au format PEM avec ASDM

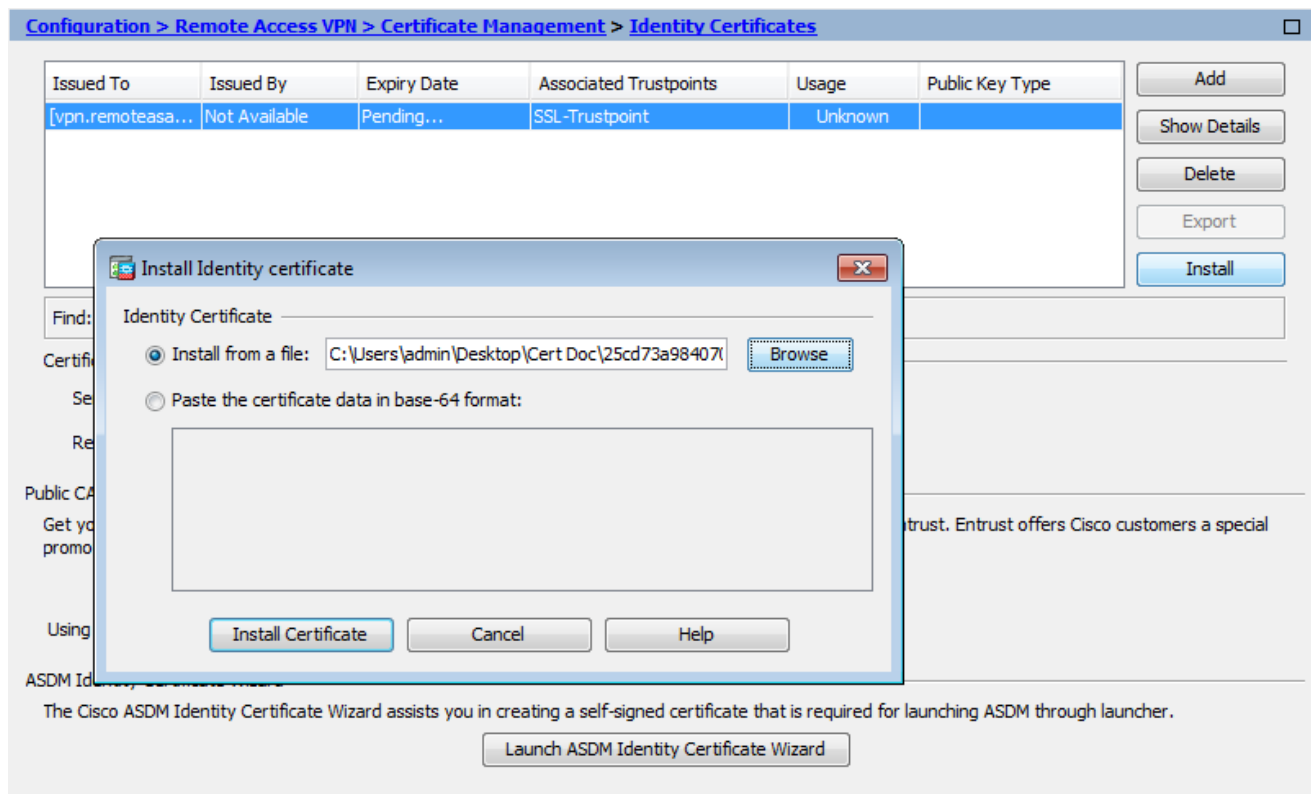
Les étapes d'installation indiquées supposent que l'autorité de certification fournit un certificat d'identité codé PEM (.pem, .cer, .crt) et un ensemble de certificats d'autorité de certification.

1. Naviguez jusqu'à **Configuration > Remote Access VPN > Certificate Management** et choisissez **CA Certificates** (Certificats CA).
2. Le certificat codé PEM dans un éditeur de texte et copiez-collez le certificat CA base64 fourni par le fournisseur tiers dans le champ de texte.

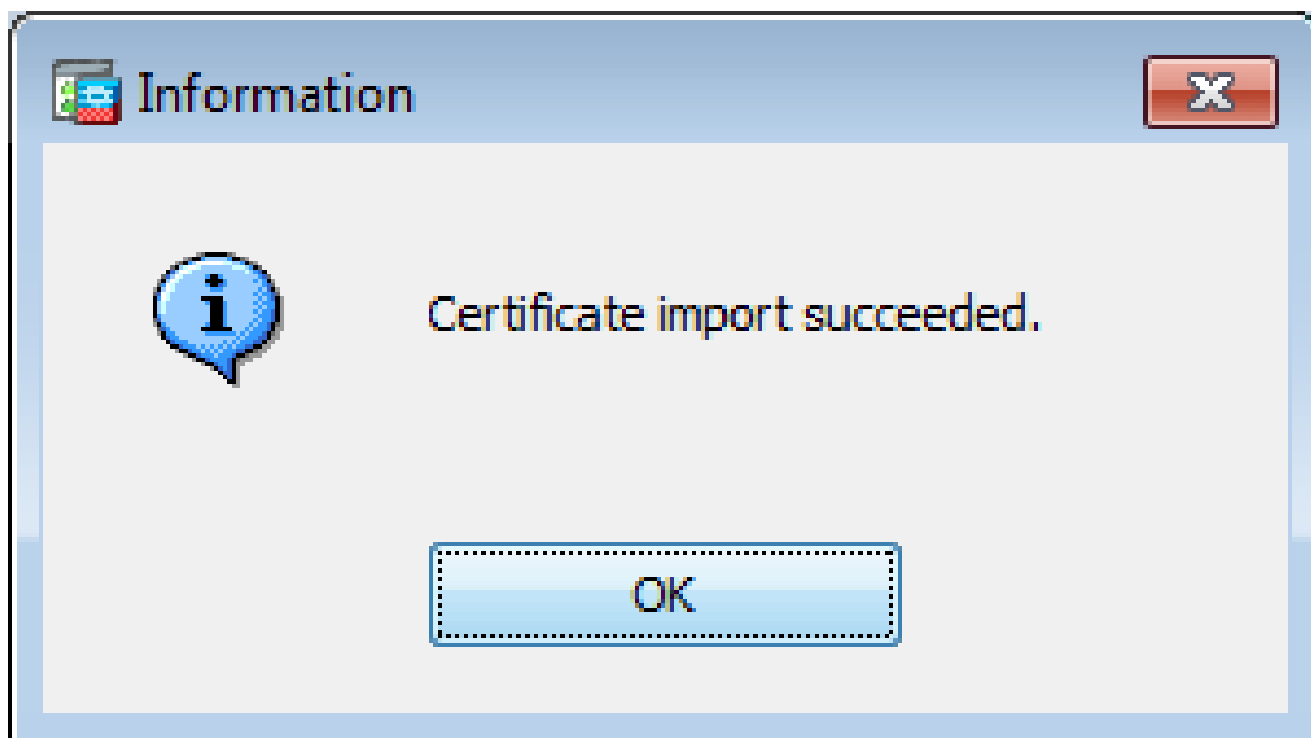


3. Cliquez sur **Install Certificate**.
4. Naviguez jusqu'à **Configuration > Remote Access VPN > Certificate Management** et choisissez **Certificats d'identité**.
5. Sélectionnez le certificat d'identité créé précédemment. Cliquez sur **Install**.
6. Cliquez sur l'option **Install from a file** et choisissez le certificat d'identité codé PEM ou ouvrez le certificat codé PEM dans un éditeur de texte et copiez-collez le certificat d'identité base64

fourni par le fournisseur tiers dans le champ de texte.



7. Cliquer **Add Certificate**.

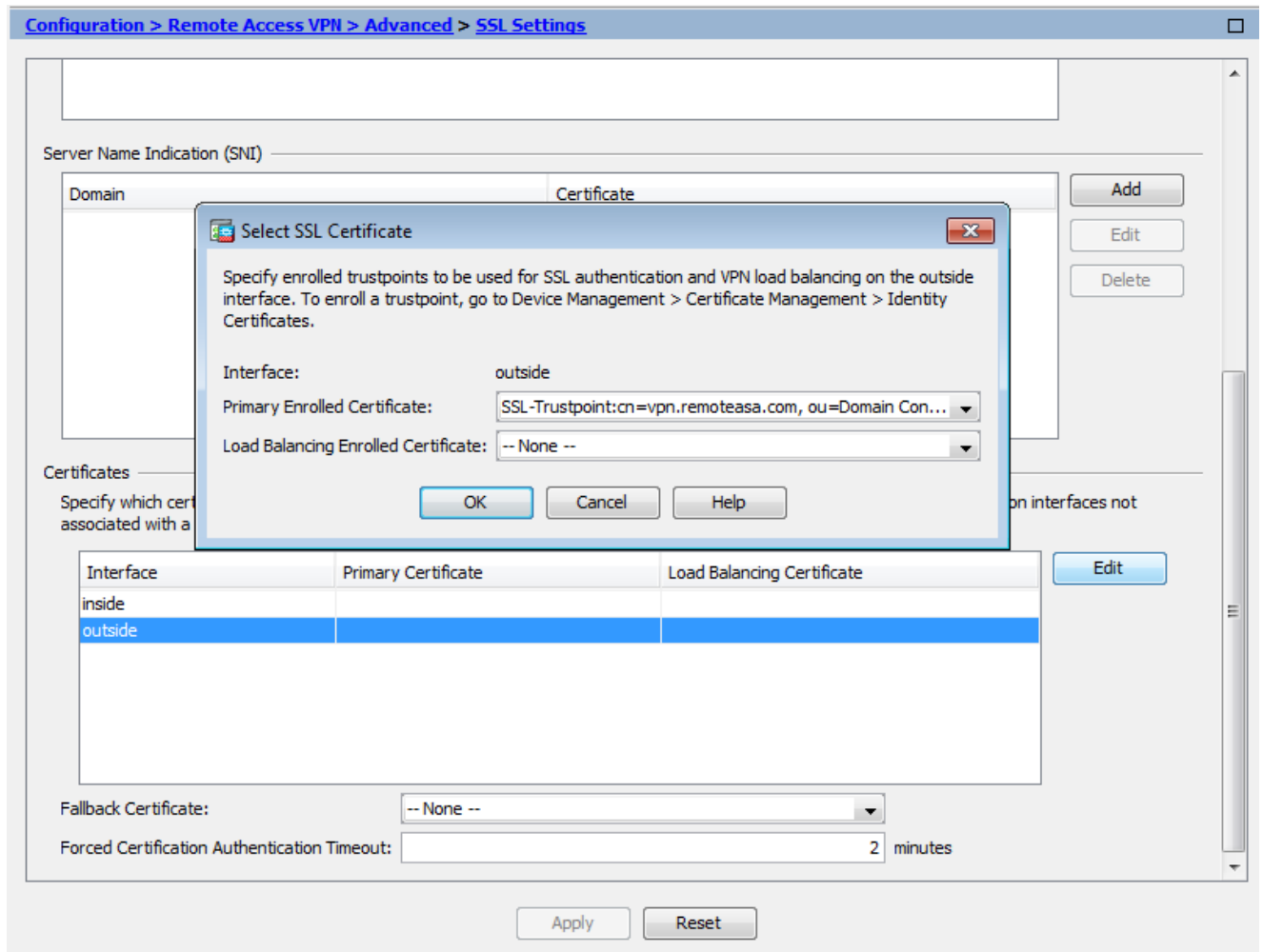


8. Naviguez jusqu'à **Configuration > Remote Access VPN > Advanced > SSL Settings**.

9. Sous **Certificates**, sélectionnez l'interface utilisée pour terminer les sessions WebVPN. Dans cet exemple, l'interface externe est utilisée.

10. Cliquer **Edit**.

11. Dans la liste déroulante **Certificate**, sélectionnez le nouveau certificat installé.



12. Cliquer **OK**.

13. Cliquer **Apply**. Le nouveau certificat est maintenant utilisé pour toutes les sessions WebVPN qui se terminent sur l'interface spécifiée.

1.2. Installation d'un certificat PEM avec l'interface de ligne de commande

```
<#root>
```

```
MainASA(config)#
```

```
crypto ca authenticate SSL-Trustpoint
```

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

```
-----BEGIN CERTIFICATE----- MIEADCCAuigAwIBAgIBADANBgkqhkiG9w0BAQUFADBjMQswCQYDVQQGEwJVuzEh MB8GA1UECh
```

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

```
.
```

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

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

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

```
MIIEFTCCA2WgAwIBAgIDG+cVMA0GCSqGSIb3DQEBCwUAMGMxCzAJBgNVBAYTA1VT
MSEwHwYDVQQKEzhUaGUgR28gRGFkZHKgR3JvdXAsIE1uYy4xMTAvBgNVBAsTKEdv
IERhZGR5IENsYXNzIDIgQ2VydG1maWNhdG1vbiBBdXRob3JpdHkwHhcNMTQwMTAx
MDcwMDAwWhcNMzEwNTMwMDcwMDAwWjCBgZELMAkGA1UEBhMCVVMxEDA0BgNVBAGT
B0FyaXpvcmluZSExZARBgNVBACTC1Njb3R0c2RhbGUxGjAYBgNVBAoTEUdvRGFkZHKu
Y29tLlCBJmMuMTEwLWYDVQQDEyHhbyBEYWRkeSBSb290IEN1cnRpZm1jYXR1IEF1
dGhvcml0eSAtIEcyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3Fi
CPH6WTT3G8kYo/eASVjpIoMTpsUgQwE7hPHmhUmfJ+r2hBt0oLTbcJjHMgGxBT4H
Tu70+k8vWTAi56sZvmvigaF88xZ1gD1Re+X5NbZ0TqmNghPktj+pA4P6or6KFWp/
3gvDthkUBcrqw6gE1DtGfDIN8wBmIisiNaW02jBEYt90yHGC00PoCjM7T3UYH3go+
6118yHz7sCtTpJJiaVE1BWEaRIGMLK1D1iPfrDqBmg4pxRyp6V0etp6eMAo5zvGI
gPtLXcwy7IViQyU0A1YnAZG003AqP26x6JyIAX2f1PnbU21gnb8s51iruF9G/M7E
GwM8CetJMvxpRpRgRwIDAQABo4IBFzCCARMwDwYDVR0TAQH/BAUwAwEB/zA0BgNV
HQ8BAf8EBAMCAQYwHQYDVR00BBYEFdqahQcQZyi27/a9BUFuIMGU2g/eMB8GA1Ud
IwQYMBaAFNLEsNKR1EwRcbNhyz2h/t2oatTjMDQGCCsGAQUFBwEBBCgwJjAkBggr
BgEFBQcwAYYYaHR0cDovL29jc3AuZ29kYWRkeS5jb20vMDIGA1UdHwQrMCKwJ6A1
oCOGIWh0dHA6Ly9jcmwuZ29kYWRkeS5jb20vZ2Ryb290LmNybDBGBGgNVHSAEPzA9
MDsGBFUdIAAAwMzAxBggrBgEFBQcCARY1aHR0cHM6Ly9jZXJ0cy5nb2RlZGR5LmNv
bS9yZXBvc210b3J5LzANBgkqhkiG9w0BAQsFAAOCAQEAWQtTvZKGEacke+1bMc8d
H2xwxbhuvk679r6XU0Ewf7ooXGKUwuN+M/f7QnaF25UcjCJYdQkMiGVn0QowCcWg
0JekxS0TP7QYpgEGRJHj2kntFo1fzq3Ms3dhP8q0CkzpN1nsoX+oYggHFCJyNwq
9kIDN0zmiN/VryTyscPzfLXs4J1et01UIDyUGAZHHFIYSaRt4bNYC8nY7NmuHDK0
KHAN4v6mF56ED71XcLNa6R+gh10773z/aQvgSM03kwwIC1TErF0UZzdsyqUvMQg3
qm5vjLyb41ddJIGv15echK1srDdMZvNhkREg5L4wn3qkKQmw4TRfZHCYQFHfjDCm
rw==
```

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

quit

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

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

Trustpoint CA certificate accepted.

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

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

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

```
MainASA(config)#
```

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

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

```
yes
```

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

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

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

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

```
MIIFRjCCBC6gAwIBAgIIJc1zqYQHbGUwDQYJKoZIhvcNAQELBQAwgBQxZAJBgNV  
BAYTA1VTMRAwDgYDVoQIEwdBcm16b25hMRRMwEQYDVoQHEwpTY290dHNkYWx1MRoW  
GAYDVQQKExFHb0RHZGR5LmNvbSw5jLjEtMCSGA1UECzMkaHR0cDovL2N1cnRz  
LmdvZGFkZHUy29tL3JlCG9zaXRvcnkvMTMwMQYDVoQDEypHbyBEYWRkeSBTZWN1  
cmUgQ2VydG1maWNhdGUgQXV0aG9yaXR5IC0gRzIwHhcNMTUwNzIyMTIwNDM4WhcN  
MTYwNzIyMTIwNDM4WjA/MSEwHwYDVoQLEXhEb21haW4gQ29udHJvbCBWYXpZGF0  
ZWQxGjAYBgNVBAMTEXzWbi5yZW1vdGVhc2EuY29tMIIBIjANBgkqhkiG9w0BAQEF  
AAOCAQ8AMIIIBCgKAQEArrY2Fv2S2Uq5HdDh0aSzK5Eyok2tv2Rem8DofbTQ+4F9  
C9IXitWdLa06a7dzyfB4S9hx1VZxoHMGGNd6i9NWLXsWU1Nx5pRMaKR4h1cL6bDW  
ITt5GzKdL93ibMxYmau+uwM30kBB8QxLNNxr4G+oXtfavctTxWy/o6LzKWFyj0XP  
tta9FZW07c0MNVkiUL1v9WBcy4GK1xyvN9RtWebtVkm5/iOv0ReBTBFFxCJ1YQAG  
UWteu1ikWAGj1qomZGnZgAFDwJ4/hxjesG2BGMtwX5L108cbmbi/u/vnmZ5Xhixq  
<snip>
```

```
CCsGAQUBwIBFItodHRwOi8vY2VydG1maWNhdGVzLmdvZGFkZHUy29tL3JlCG9z  
aXRvcnkvMHYGCCsGAQUBwEBBGowaDAKBggrBgEFBQcwAYYYaHR0cDovL29jc3Au  
Z29kYWwRkeS5jb20vMEAGCCsGAQUBzAChjRodHRwOi8vY2VydG1maWNhdGVzLmdv  
ZGFkZHUy29tL3JlCG9zaXRvcnkvZ2RpZzIuY3J0MB8GA1UdIwQYMBaAFEDCvSe0  
zDSDMKIz1/tss/COLIDOMEYGA1UdEQQ/MD2CEXZwbi5yZW1vdGVhc2EuY29tghV3  
d3cudnBuLnJlbW90ZWZzYS5jb22CEXZwbi5yZW1vdGVhc2EuY29tMB0GA1UdDgQW  
BBT7en7YS3PH+s4z+wTR1pHr2tSzejANBgkqhkiG9w0BAQsFAAOCAQEA09H8TLN  
x2Y0rYdI6gS8n4imaSYg9Ni/9Nb6mote3J2LELG9HY9m/zUCR5yVkttra9azdrNUAN  
1hjBJ7kkQScLC4sZLONDqG1uTP5rbWR0yikF5wSzyMwd03kOR+vM8q6T57vRst5  
69vzBUUJc5bSu1IjyfPP19z1l+B2eBwUFbVfXLnd9bTfiG9mSmC+4V63TXFxt10q  
xkGNys3GgYuCUy6yRP2cAUV11c2tYtaxoCL8yo72YUDDgZ3a4Py01EvC1F0aUtgv  
6QNEOYwmbJkyumdPUwko6wGOCOWLumzv5gHnhil68HYSZ/4XI1p3B9Y8yfg5pwb  
n7puhazH+xgQRdg==
```

```
-----END CERTIFICATE-----
```

```
quit
```

```
INFO: Certificate successfully imported
```

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

```
MainASA(config)#
```

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

2.1 Installation d'un certificat PKCS12 avec ASDM

Dans les cas où le CSR n'est pas généré sur l'ASA, comme dans le cas d'un certificat générique ou lorsqu'un certificat UC est généré, un certificat d'identité avec la clé privée sont reçus sous forme de fichiers séparés ou d'un fichier PKCS12 unique (format .p12 ou pfx). Afin d'installer ce type de certificat, complétez ces étapes.

1. Le certificat d'identité regroupe le certificat d'autorité de certification et la clé privée dans un

fichier PKCS12 unique. [L'annexe B](#) décrit les étapes à suivre pour effectuer cette opération avec OpenSSL. Si déjà groupé par l'autorité de certification, passez à l'étape suivante.

2. Naviguez jusqu'à **Configuration > Remote Access VPN > Certificate Management**, et choisissez **Identity Certificates**.
3. Cliquez sur **Add**.
4. Spécifiez un nom de point de confiance.
5. Cliquez sur le bouton **Import the identity certificate from a file** de l'assistant.
6. Entrez la phrase de passe utilisée pour créer le fichier PKCS12. Recherchez et sélectionnez le fichier PKCS12. Saisissez la phrase de passe du certificat.

Add Identity Certificate

Trustpoint Name:

Import the identity certificate from a file (PKCS12 format with Certificate(s) +Private Key):

Decryption Passphrase:

File to Import From:

Add a new identity certificate:

Key Pair:

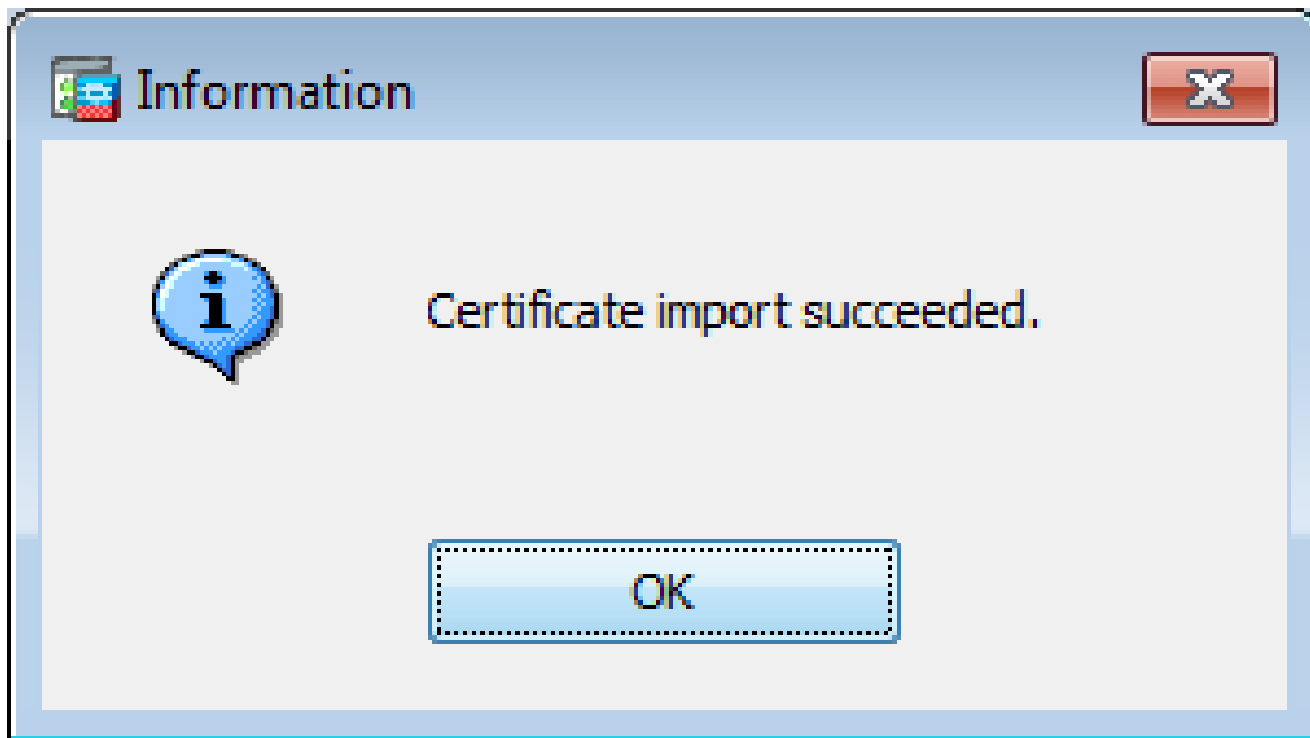
Certificate Subject DN:

Generate self-signed certificate

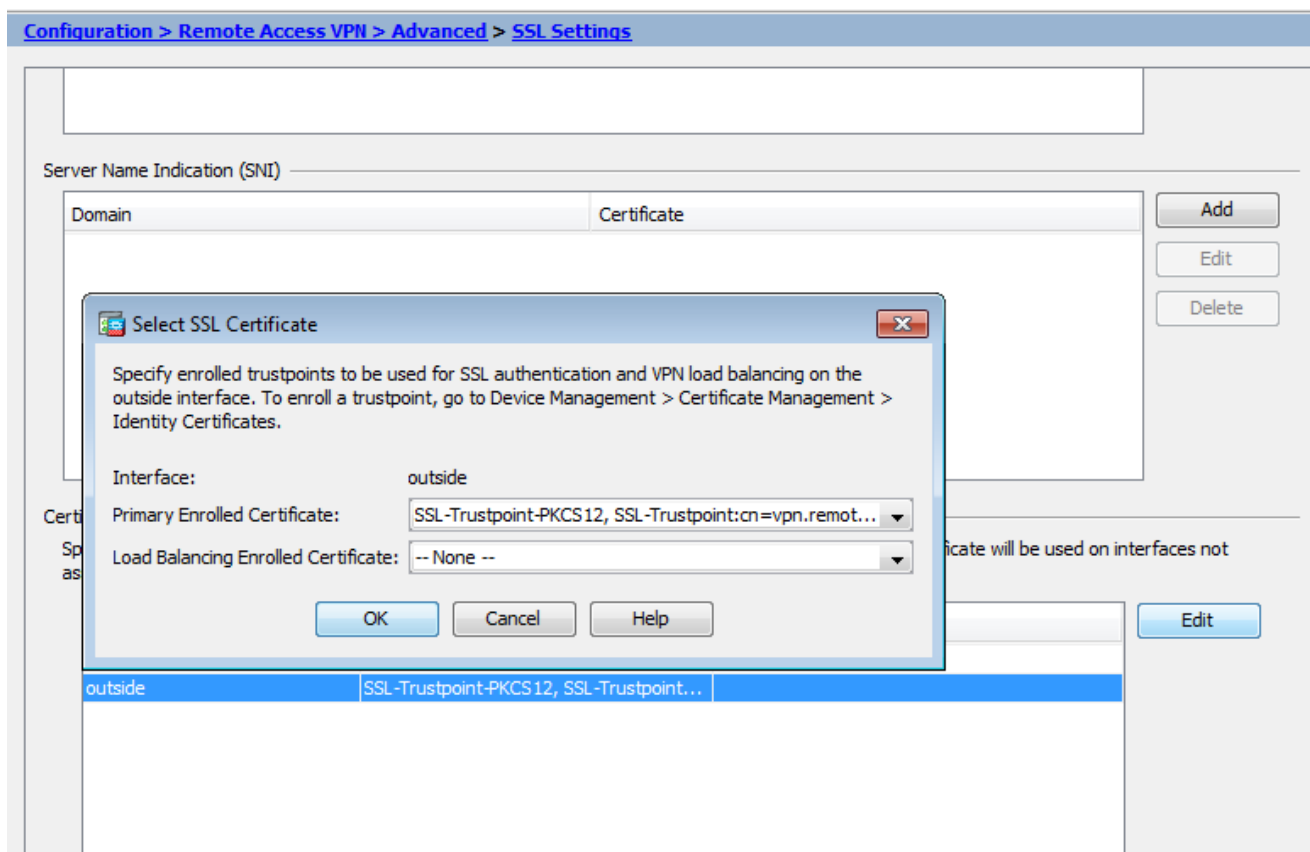
Act as local certificate authority and issue dynamic certificates to TLS-Proxy

Enable CA flag in basic constraints extension

7. Cliquez sur **Ajouter un certificat**.



8. Naviguez jusqu'à **Configuration > Remote Access VPN > Advanced** et choisissez **SSL Settings**.
9. Sous **Certificates**, choisissez l'interface utilisée pour terminer les sessions WebVPN. Dans cet exemple, l'interface externe est utilisée.
10. Cliquez sur **Edit**.
11. Dans la liste déroulante **Certificate**, sélectionnez le nouveau certificat installé.



12. Cliquez sur **OK**.

13. Cliquer **Apply**. Les nouveaux certificats sont maintenant utilisés pour toutes les sessions WebVPN qui se terminent sur l'interface spécifiée.

2.2 Installation d'un certificat PKCS12 avec l'interface de ligne de commande

```
<#root>
```

```
MainASA(config)#
```

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

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

```
enrollment terminal
```

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

```
exit
```

```
MainASA(config)#
```

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

Enter the base 64 encoded pkcs12.

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

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

```
MIISNwIBAzCCEfEGCSqGSIb3DQEHAAcCEeIEghHeMIIR2jCCEdYGCsGSIb3DQEH  
BqCCEccwghHDAgEAMIIRvAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMDQIWO3D  
hDtI/uECAQGAghGQ9ospee/qtIbVZh2T8/Z+5dxRPBcStDTqyKy7q3+9ram5AZdG  
Ce9n5UCckqT4WcTjs7XZtCrUrt/LkNbmGDVhwGBmYWi0S7npgaUq0eoqiJRK+Yc7  
LN0nbho6I5WfL56/JiceAM1XDLr/IqqLg2QAAPGdN+F5vANsHse2GsAATewBDLt7  
Jy+SKfoNvvIw9QvzCiUzMjYZBANmBdMCQ13H+YQTHitT3vn2/iCD1zRSuXcqypEV  
q5e3hei00751E8TDLWm03PMvWIZqi8yzWesjcTt1Kd4FoJBZpB70/v9LntoIUOY7  
kIQM8fHb4ga8BYfbgRmG6mkMm01STtbSv1vTa19WTmdQdTyCa+G5PkrRyRsy3Ww1  
1kGFMhImmrnNADF7Hmzbys1VohQZ7h09iVQY9krJogoXHjmQYxG9brf0oEwxSJD  
mGDhheSh+s/WuFSV9Z9kiTXpJNZxpTASoWBQrrwm05v8ZwbjbVNJ7sVdbwpU16d+  
NNFGR7LTq08hpueeJnY9eJc2yYqAXWXQ5kL0Zo6/gBEdGtEaZBgCFK9JZ3b13A  
xqxGifanWpNLyG611NkuNjTgbjhnEEYI2uZzU0qxn1Ka8zyXw+1zrKuJscDbkAPZ  
wKtw8K+p40zXVHhuANo6MDvffNRY1KQDtyK1inoPH5ksVSE5awkVam4+HTcqEUfa  
16LMana+4QRgSetJhU0LtsMaQFRJGkha4JLq2t+JrCAPz2osAR1TsB0jQBNq6YNj  
0uB+gGk2G18Q5N1n6K1fz0XBFLWEDBLsaBR05MAnE7wWt00+4awGYqVdmIF11kf  
XIRKAiQEr1pZ6BVPuvsCNJxaaUHzufhYI2ZAckasKBZOT8/7YK3fnAaGoBCz4cHa  
o2EEQh2aYb6YTv0+wtLEWGHZsbGZEM/u54XmsXAI7g28LGJYdfwi509KyV+Ac1V  
KzHqXZMM2BbUQCNCtF5JIMiW+r62k42FdahfaQb0vJsIe/IwkAKG7y6DIQFsOhwg  
Z1PXiDbNr1k4e8L4gqupMKWg853PY+oY22rLDC7bu11CKtixIYBCvbn7dAYsI4GQ  
16xXhNu3+iye0HgbUQCfTU/mBrA0Z0+bpKjWOCfqNBuYnZ6kUEdCI7GFLH9QqtM  
K7YinFLoHwTwi3MsmqVv+Z4ttVWv7Xmiko02nMynJMP6/CNV80MxMKdC2qm+c1j  
s4Q1KcAmFsQmNp/7SIP1wnv0c6JbUmC10520U/r8ftTzn8C7WL62W79cLK4H0r7J  
sNsZn0z0J0Z/xdZT+cLTCtVevKJQOMK3vMsiOuy52FkuF3HnfrmbQdkbR7yZxELG  
RCELOEDdbp8VP0+IhNlyz1q7975ScdxFSL0TvjnHGFwd14ndoqN+bLhWbdPjQWV  
13W2NCI95tmHDLGgp3P001S+rjdCEGMg+9cpgBfFC1JocuTDIEcUbjBY8QRUNiS  
/ubyUagdzUKt1ecfb9hMLP65ZnQ93VIw/NJKbIm7b4P/1Zp/1FP5eq7LkQPaxE4/  
bQ4mHcnwrs+JGfK19B8hJmmGoowH3p4IEvwZy7CThB3E1ejw5R4enqmrgrvHqpQe  
B7odN10FLAHdo1G5BsHExlUNeSb40Q0pmKXiDDB5B001bJsr748fZ6L/LGx8A13  
<snip>
```

```
ijDqxyfQXY4zSyt1jSMwMtYA9hG5I79Sg7pnME1E9xq1D0oRGG8vgxlwiciKtLxp  
LL0ReDY31KRYv00vW0gf+tE71ST/3TKZvh0sQ/BE0V3kHnw1dejMFH+dvYAA9Y1E  
c80+tdafBFX4B/HP46E6heP6ZSt0xAfRW1/JF41jNvUNV09VtVfR2FTyWpzZFY8A  
GG5XPiA80WF6wKEPFHicN8scY+Vot8kXxG96hwt2Cm5NQ20nVzxUZQbpKsjs/2jC
```

3HVFe3UJFBsY9UxTLcPXyBSIG+VeqkI8hWZp6c1TFNDLY2ELDy1Qzp1mBg2FujZa
YuE0avjCJzBzZUG2umtS5mHQnwPF+Xk0UjEyhGMauhGxHp4nghSzrUZrBeuL91UF
2mbpsOcgZkzxMS/rjdNXjCmPF1oRBvKkZS1xHFRE/5ZopAhn4i7YtHQNrZ9U4RjQ
xo9cUuaJ+LNmvzE8Yg3epAMYZ16UNGQQkVQ6ME4BcjRONzW8BYgTq4+pmT1ZNq1P
X87CXCPtYrPHF57eSo+tHDINCgfYXD6e/7r2ngfiCeUeNDZ4aV12XxvZDaU1BPP
Tx5fMARqx/Z8BdDyBJDVBjdsxmQau9HLkhPvdFG1ZIwdTe13CzKqXA5Pmpjt4q9
GnCpC53m76x9Su4ZDw6aUdBcgCTMvfaqJC9gz0bee2Wz+aRRwzSxu6tEWVZo1PEM
v0AA7po3vPek1g0nLRAwEoTTn4SdgNLWeRoxqZgkw1FC1GrotxF1so7uA+z0aMeU
1w73reonsNdZvRAcVX3Y6UNFDyt70Ixvo1H4VLzWmOK/oP62C9/eqqMwZ8zoCMPt
ENna7T+70s66SCbMmXCHwyh00tygNKZFFw/AATFyjQPMWPaxGuPN0rnB6uYcN0Hk
1BU7tF143RNIzaQqEH3XnaPvUuAA4C0FCoE3h+/tVjtfNKDvFmb6ZLZHYQmUYpyS
uhdFEpoDrJH1VmI2tik/iqYwaz+oDqXPHQXnJhw25h9ombR4qnd+FCfwFCGtPFON
o3Qffz53C95n5jPHVMYUr0xDdpwnvzCQPdj6yQm564TwLAmiz7uD1pqJZJe5QxHD
no1v+4MdGSFvtBq+ykFoVcaamqeaq6sKgvAVujLXXEs4KEmIgcPqATVRG49E1ndI
L01DEQyKhVoDGebAuVRBjzwAm/qxWxxFv3hrbCjPHCwEYms4Wgt/vKKRFsuWJNZf
efH1dw11tkd5dKwSvDocPT/7mSLtLJa94c6AfgxYy9z0+FTLDQwzXga7xC2krAN1
yHXR2KHN5YeRL+KDzu+u6dYoKaz+YAgw1W6KbeavALSuH4EYqcvG8hUEhp/ySiSc
RDhuYgxEovIMGfES4FP5V521PyDhM3Dqwhn0vuYUmYnX8EXURkay44iwwI5HhqYJ
1ptWYyO8Bdr4Wnwt5xqsZgYR6mmGeAIin7bDunsF1uBHWYF4dyK1z1tsdRNMqQ
+W5q+QjVdrj1dwv/bMF0aqEjxeNwBRqjzccff3BxMnwVxtgqxFvRh+DZxiJoiBG+
yx7x8np2AQ1r0METSSxbnZzfNkZKvBVMkIC6Jsm2WEVTQvoFJ8em+nem0WgTi/
hHSBzjE7RhAucnHuiFOCX0gvR1SDDqyCQbduc1QjXN0svA8Fqbea9WEH5khOPv3
pbtSL4gsf12pv8diBQkVQgiZDi8Wb++7PR6ttiY65kVwrdsoN11/qq+xW0d3tB4/
zoH9LEMgTy9Sz7myWrB9E00Z8BIjL1M8oMigEYrTD0c3KbyW1S9dd7QAxio0BaX1
8J8q10ydvTBzmqcjesFH4/1NHn5Vnf0ZnNpui4uHP0XBG+K2zJUJXm6dq1AHB1E
KQFsFzPNNyave0Kk8JzQnLAPd70UU/Iksy0CGQozGBH+HSzVp1RDjrrbC342rkBj
wnI+j+/1JdwBmHdJMZCfoMZFLSI9ZBqFirdii1/NRu6jh76TQor5TnNjxIyNREJC
FE5FZnMFvhM900LaiUZff8WWCOferDMttLXb1nuxPF1+1Rk+LN1PLVptWgcxzfSr
JXrGiWjxybBB9oCOrAcq8fGAtEs8WRxJyDH3Jjmn9i/G16J1mMcuF//LxAH2WQx8
Ld/qS50M2iFCffDQjxAj0K6DEN5pUebBv1Em5SOHXvyq5nxgUh4/y84CwaKjwOMQ
5tbbLM1nc7ALIj9LxZ97YiXSTyeM6oBxBfx6Rpk1kDv05m1BghSpVQiMcQ2ORikh
UVVNBsh019S3cb5wqxaWqAKBqb4h1uLGVbYWZf2mzLZ8U5U5ioiqoMBqNZbzTXp0
EqEFuatT11QvCRbcKS3xou4MAixcYUxKwEhbZA/6hd10XSBjwe7jKBV9M6w1iKab
UfoJCGTaf3sY681qrMPrbt0eewf1C02Sd9Mn+V/jvni17mxYFFUpruRq3r1LeqP
J5camfTtHwyL8N3Q/Zwp+zQeWziLA8a/iAVu/hYLR1bpF2WCK010tJqkvVmrLVLz
maZZjbJe0ft5cP/1RxbK1S6Gd5dFEKDE15c6gWUX8RKZP6Q7iaE5hnGmQjm8Lj1
kXwF+ivox0Q8a+Gg1bVTR0c7tqW9e9/ewisV1mwvEB6Ny7TDS1oPUDHM84pY6dqi
1+0io07Ked4BySwN1Yy9yaJtBTZSCstfP+ApLiDn7pSBvvXf1aHmeNbkPOZJ+c+t
fGpUdL6V2UTXfCsOPHTC0ezA15sOHwCuPchrDIj/eGUwMS3NfS25XgcMuvnLqGVO
RzcrZ1ZiG8G0oLYwOCuzoY0D/m901001ahePyA9tmVB7HRRbytLdaW7gYeikoCv
7qtBqJFF17ntWJ3EpQHZUCVClbHIKqjNqRbDCY7so4A1IW7kSEUGWMIUDhprE8Ks
NpvnPH2i9JrYrTeRoYUI0tL/7SATd2P0a21xz/zUwekeqd0bmvCsAgQNbB2XkrR3
XS0B52o1+63e8KDqS2zL2TZd3daDFidH1B8QB26tfbf0Aca0bJH5/dWP8ddo8UYo
Y3JqT10malxSjhaMhMqDZIqP49utW3TcjgG11YS4HEmcqtHud0ShaUysC6239j1Q
K1FWrwXT1BC5vnq5IcOMqx5zyNbfXz28969cwoMcyU6+kRw0TyF6kF7EEv6XWca
XLEwABx+tKRUKHJ673SyDMu96KMV3yZN+RtKbCjqCPVTP/3ZeIp7nCMUcj5sW9HI
N34yeI/ORCLyeGsOEiBLkucikC32LI9ik5HvImVTELQ0Uz3ceFqU/PkasjJUve6S
/n/1ZVUHbUk71xKR2bWZgEC17fIe17w1rbjP3Wbk+Er0kfYcsNRHxeTDpKpSt9s
u/UsyQJiyNARG4X3iyQ1sTce/06Ycyri6GcLHAu58B02nj4Cxo1Cp1ABZ2N79HtN
/7Kh5L0pS9MwsDCHUUI8KFRtSET7TB1tIU99FdB19L64s1/shYAHbccvVWU50WhT
PdLoaErrX81Tof41IxbSZbI8grUC4KfG2sdPLJKu3HVTeQ8Lfl1bBLxfs8ZBS+Oc
v8rH1Q012kY6LsFGLehj+/yJ/uvXORiv0Esp4EhFpFfkp+o+YcFeLUUPd+jzb62K
HfSCCbLpCkyEay80dyWkHfgy1qXmb9ud0oM050aFJyqRONjnt6pcxBRY2A6AJR5S
IIC26YNwbh0GjF9qL2FiUqnNH/7GTqPnd2qmsB6FTIwSBT6d854qN7PRt+ZXgdtQ
Ojcyt1r9qpWZpNFK8EzizwKiAYtsiEh2pzPt6YUkpsRb6CXTkiZog+Klsv2m3b8
OHyZ9a8z81/gnxrZ11s5SCTf0SU70pHWh8VAYKVHhK+MwGqR0m/2ocV32dkRBLMy
2R6P4WfHyI/+9de1x3PtIu0iv2knpxHv2fKM6sQw45F7XkmwHxjq1YRJ6vIwPTAH
MAKGBSs0AwIaBQAeffTRETzpiSHKZR+Kmen68VrTwpV7BBSQi0IesQ4n4E/bSVsd
qJSzcwh0hgICBAA=
-----END PKCS12-----
quit

INFO: Import PKCS12 operation completed successfully

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

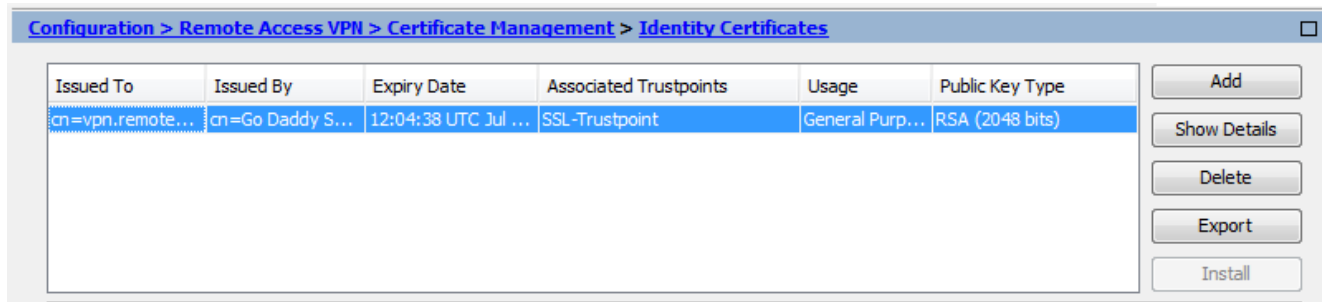
```
ssl trust-point SSL-Trustpoint-PKCS12 outside
```

Vérifier

Suivez ces étapes afin de vérifier que l'installation du Certificat du Fournisseur tiers est réussie et que les connexions SSLVPN sont utilisées.

Afficher les certificats installés via ASDM

1. Naviguez jusqu'à **Configuration > Remote Access VPN > Certificate Management**, et choisissez **Identity Certificates**.
2. Le certificat d'identité émis par le fournisseur tiers s'affiche.



Afficher les certificats installés via la CLI

```
<#root>
```

```
MainASA(config)#
```

```
show crypto ca certificate
```

Certificate

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


OCSP AIA:

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

CRL Distribution Points:

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

Validity Date:

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

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

Associated Trustpoints:

SSL-Trustpoint

CA Certificate

Status: Available

Certificate Serial Number: 07

Certificate Usage: General Purpose

Public Key Type: RSA (2048 bits)

Signature Algorithm: SHA256 with RSA Encryption

Issuer Name:

cn=Go Daddy Root Certificate Authority - G2

o=GoDaddy.com\, Inc.

l=Scottsdale

st=Arizona

c=US

Subject Name:

cn=Go Daddy Secure Certificate Authority - G2

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

o=GoDaddy.com\, Inc.

l=Scottsdale

st=Arizona

c=US

OCSP AIA:

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

CRL Distribution Points:

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

Validity Date:

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

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

Associated Trustpoints:

SSL-Trustpoint

CA Certificate

Status: Available

Certificate Serial Number: 1be715

Certificate Usage: General Purpose

Public Key Type: RSA (2048 bits)

Signature Algorithm: SHA256 with RSA Encryption

Issuer Name:

ou=Go Daddy Class 2 Certification Authority

o=The Go Daddy Group\, Inc.

c=US

Subject Name:

cn=Go Daddy Root Certificate Authority - G2

o=GoDaddy.com\, Inc.

l=Scottsdale

st=Arizona

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

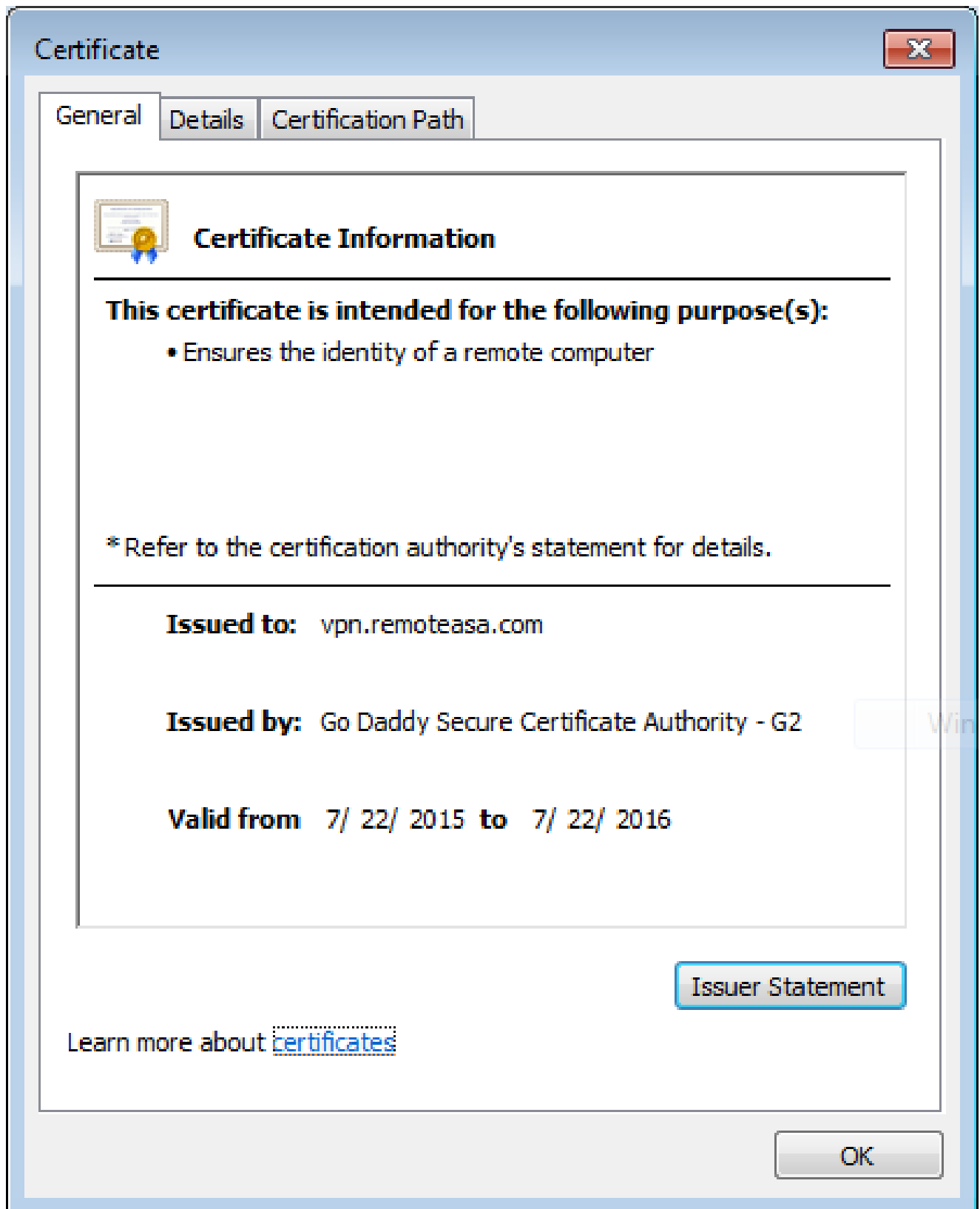
SSL-Trustpoint-1

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

Vérification du certificat installé pour WebVPN avec un navigateur Web

Vérifiez que WebVPN utilise le nouveau certificat.

1. Connectez-vous à l'interface WebVPN via un navigateur Web. Utilisez `https://` avec le nom de domaine complet (FQDN) utilisé afin de demander le certificat (par exemple, [https://\(vpn.remoteasa.com\)](https://(vpn.remoteasa.com))).
2. Double-cliquez sur l'icône de verrouillage qui apparaît dans le coin inférieur droit de la page de connexion WebVPN. Les informations relatives au certificat installé doivent apparaître.
3. Vérifiez le contenu afin de vérifier qu'il correspond au certificat émis par le fournisseur tiers.

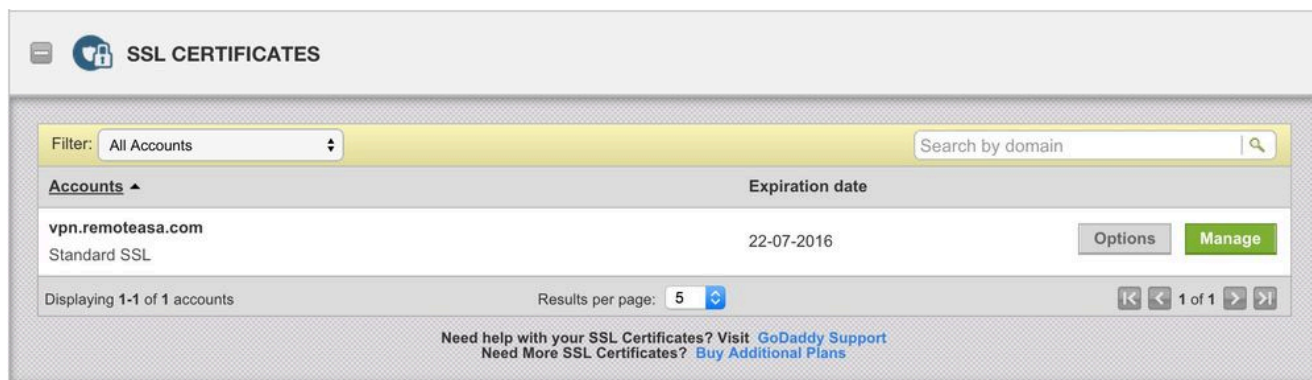


Renouveler le certificat SSL sur l'ASA

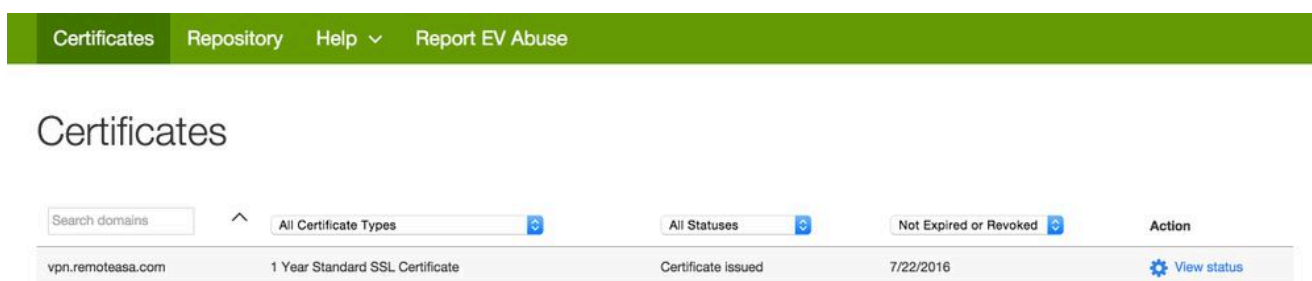
1. Régénérez le CSR soit sur l'ASA, soit avec OpenSSL ou sur l'AC avec les mêmes attributs que l'ancien certificat. Suivez les étapes décrites dans la section [Génération de CSR](#).
2. Envoyez le CSR sur l'autorité de certification et générez un nouveau certificat d'identité au format PEM (.pem, .cer, .crt) avec le certificat de l'autorité de certification. Dans le cas d'un certificat PKCS12, il existe également une nouvelle clé privée.

Dans le cas d'une autorité de certification GoDaddy, le certificat peut être renouvelé avec un nouveau CSR généré.

Accédez au compte GoDaddy et cliquez sur Manage sous SSL Certificates.



Cliquez sur Afficher l'état pour le nom de domaine requis.



Cliquez sur Manage afin de donner des options pour ressaisir le certificat.

All > vpn.remoteasa.com

Standard SSL Certificate

Certificate Management Options



Download



Revoke



Manage

Certificate Details

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

Développez l'option Re-Key certificate et ajoutez le nouveau CSR.

vpn.remoteasa.com > Manage Certificate

Standard SSL Certificate

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

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

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

Certificate Signing Request (CSR)

```
13qHfepIRd3QX0kDh4P/wKI12bz/zb1v/SI  
N80GsenQVuZaYzIH-N3R9EU/3Rz9  
PcctuZ18yZLZTr6NSxk9im111aCuxlH9FmW
```

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

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

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

Enregistrez et passez à l'étape suivante. GoDaddy délivre un nouveau certificat basé sur le CSR fourni.

3. Installez le nouveau certificat sur un nouveau point de confiance, comme indiqué dans la section Installation du certificat SSL sur l'ASA.

Forum aux questions

1. Quel est le meilleur moyen de transférer des certificats d'identité d'un ASA vers un autre ASA ?

Exportez le certificat avec les clés dans un fichier PKCS12.

Utilisez cette commande afin d'exporter le certificat via la CLI à partir de l'ASA d'origine :

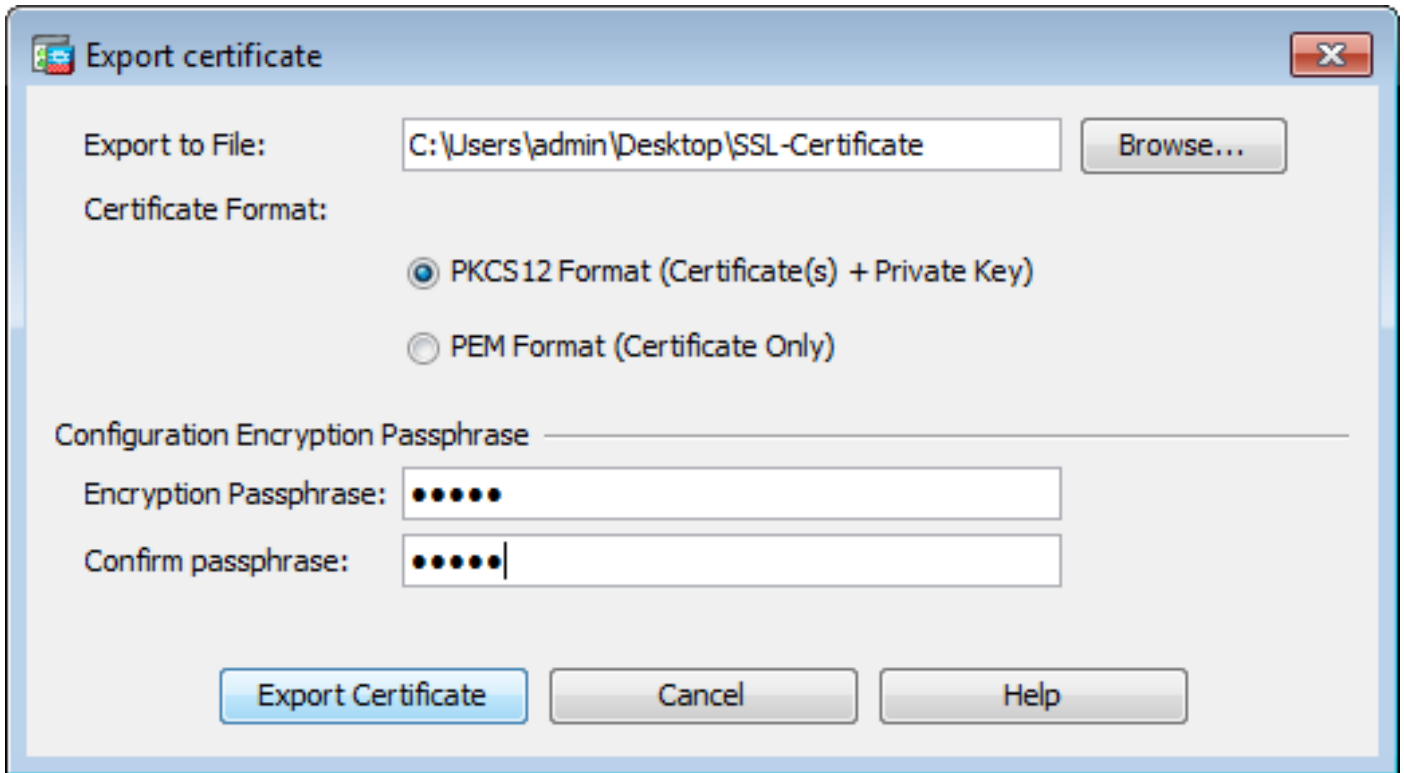
```
<#root>
```

```
ASA(config)#
```

```
crypto ca export
```

```
pkcs12
```

Configuration ASDM :



Utilisez cette commande afin d'importer le certificat via CLI vers l'ASA cible :

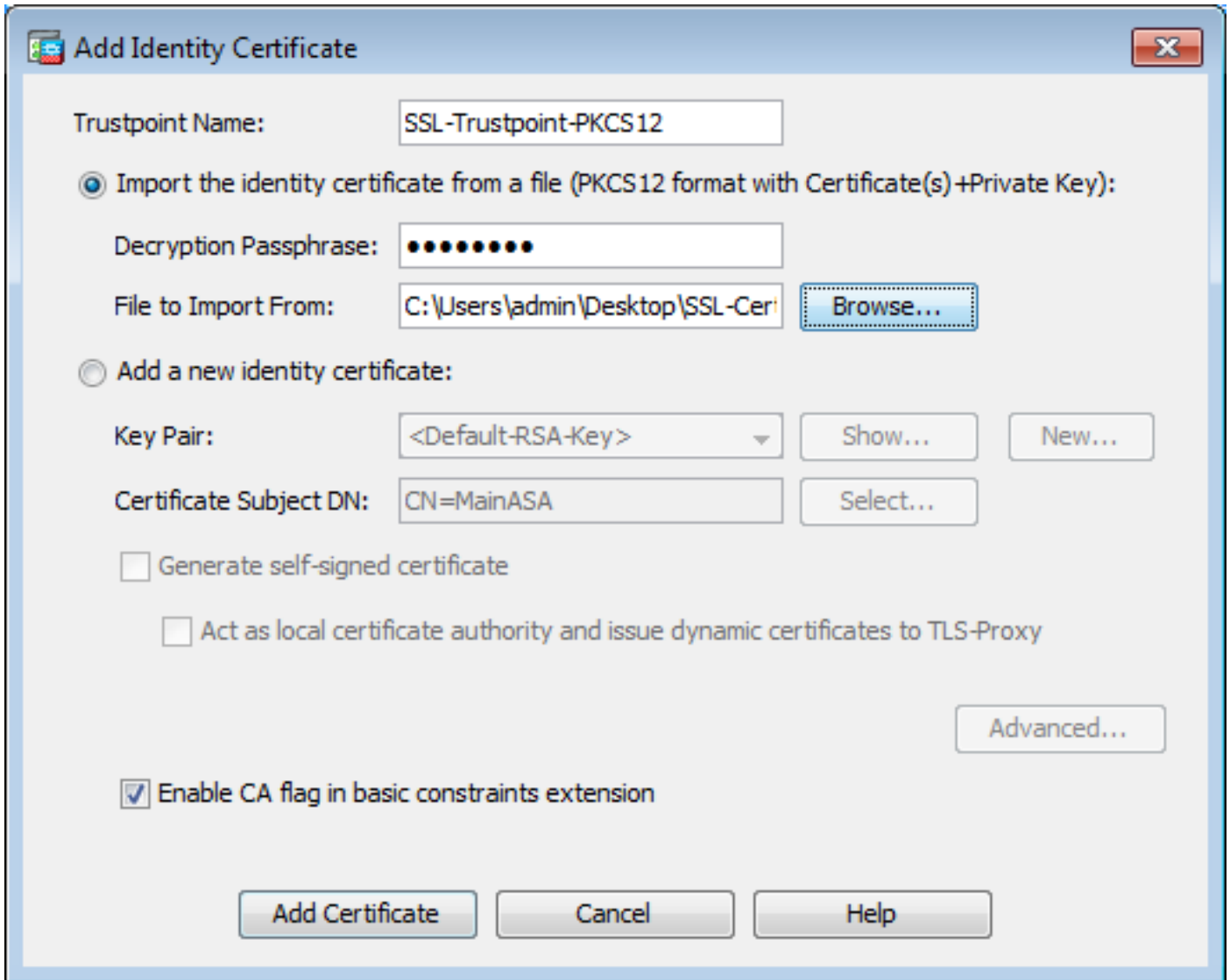
```
<#root>
```

```
ASA(config)#
```

```
crypto ca import
```

```
pkcs12
```

Configuration ASDM :



Vous pouvez également effectuer cette opération via la fonction de sauvegarde/restauration de l'ASDM en procédant comme suit :

1. Connectez-vous à l'ASA via ASDM et choisissez **Tools > Backup Configuration**.
2. Sauvegarder toute la configuration ou uniquement les certificats d'identité.
3. Sur l'ASA cible, ouvrez l'ASDM et choisissez **Tools > Restore Configuration**.

2. Comment générer des certificats SSL à utiliser avec les ASA d'équilibrage de charge VPN ?

Plusieurs méthodes peuvent être utilisées pour configurer des ASA avec des certificats SSL pour un environnement d'équilibrage de charge VPN.

1. Utilisez un seul certificat UCC (Unified Communications/Multiple Domains Certificate) dont le nom de domaine complet (FQDN) d'équilibrage de charge est le nom de domaine complet (DN) et dont chacun des noms de domaine complets (FQDN) ASA est un autre nom de sujet (SAN) distinct. Il existe plusieurs autorités de certification bien connues comme GoDaddy, Entrust, Comodo et d'autres qui prennent en charge de tels certificats. Lorsque vous choisissez cette méthode, il est important de se rappeler que l'ASA ne prend pas

actuellement en charge la création d'un CSR avec plusieurs champs SAN. Ceci a été documenté dans l'amélioration du bogue Cisco ID [CSCso70867](#) . Dans ce cas, il existe deux options pour générer le CSR

- a. Via la CLI ou l'ASDM. Lorsque le CSR est envoyé à l'autorité de certification, ajoutez les différents SAN sur le portail de l'autorité de certification.
- b. Utilisez OpenSSL pour générer le CSR et inclure les différents SAN dans le fichier openssl.cnf.

Une fois que le CSR a été soumis à l'autorité de certification et que le certificat a été généré, importez ce certificat PEM vers l'ASA qui a généré le CSR. Une fois terminé, exportez et importez ce certificat au format PKCS12 sur les autres ASA membres.

2. Utilisez un certificat générique. Il s'agit d'une méthode moins sécurisée et moins souple qu'un certificat de communications unifiées. Dans le cas où l'autorité de certification ne prend pas en charge les certificats UC, un CSR est généré soit sur l'autorité de certification, soit avec OpenSSL où le nom de domaine complet est sous la forme *.domain.com. Une fois que le CSR a été soumis à l'autorité de certification et que le certificat a été généré, importez le certificat PKCS12 vers tous les ASA du cluster.
3. Utilisez un certificat distinct pour chaque ASA membre et le pour le nom de domaine complet d'équilibrage de charge. C'est la solution la moins efficace. Les certificats pour chacun des ASA individuels peuvent être créés comme indiqué dans ce document. Le certificat pour le FQDN d'équilibrage de charge VPN est créé sur un ASA et exporté et importé en tant que certificat PKCS12 sur les autres ASA.

3. Les certificats doivent-ils être copiés de l'ASA principal vers l'ASA secondaire dans une paire de basculement ASA ?

Il n'est pas nécessaire de copier manuellement les certificats de l'ASA principal vers l'ASA secondaire car les certificats sont synchronisés entre les ASA tant que le basculement dynamique est configuré. Si lors de la configuration initiale du basculement, les certificats ne sont pas vus sur le périphérique de secours, émettez la commande `write standby` afin de forcer une synchronisation.

4. Si des clés ECDSA sont utilisées, le processus de génération de certificat SSL est-il différent ?

La seule différence dans la configuration est l'étape de génération de paire de clés, où une paire de clés ECDSA est générée à la place d'une paire de clés RSA. Le reste des étapes reste le même. La commande CLI permettant de générer des clés ECDSA est illustrée ci-dessous :

```
<#root>
```

```
MainASA(config)#
```

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

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

Dépannage

Dépannage des commandes

Ces commandes debug doivent être collectées sur l'interface de ligne de commande en cas d'échec de l'installation du certificat SSL :

```
debug crypto ca 255
```

```
debug crypto ca messages 255
```

```
debug crypto ca transactions 255
```

Problèmes courants

Avertissement de certificat non approuvé avec un certificat SSL tiers valide sur l'interface externe sur ASA avec 9.4(1) et versions ultérieures.

Solution : ce problème se présente lorsqu'une paire de clés RSA est utilisée avec le certificat. Sur les versions ASA à partir de la version 9.4(1), tous les chiffrements ECDSA et RSA sont activés par défaut et le chiffrement le plus fort (généralement un chiffrement ECDSA) est utilisé pour la négociation. Dans ce cas, l'ASA présente un certificat auto-signé au lieu du certificat RSA actuellement configuré. Une amélioration est en place pour modifier le comportement quand un certificat basé sur RSA est installé sur une interface et est suivi par l'ID de bogue Cisco [CSCuu02848](#).

Action recommandée : désactivez les chiffrements ECDSA avec ces commandes CLI :

```
ssl cipher tls1.2 custom "AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA:RC4-SHA:RC4-MD5"
```

Ou, avec l'ASDM, accédez à **Configuration > Remote Access VPN > Advanced** et choisissez **SSL Settings**. Dans la section **Encryption**, sélectionnez **tls1.2 Cipher version** et modifiez-le avec la chaîne personnalisée **AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA:RC4-SHA:RC4-MD5**

Annexe

Annexe A : ECDSA ou RSA

L'algorithme ECDSA fait partie de la cryptographie à courbe elliptique (ECC) et utilise une équation d'une courbe elliptique pour générer une clé publique tandis que l'algorithme RSA utilise le produit de deux nombres premiers plus un nombre plus petit pour générer la clé publique. Cela

signifie qu'avec ECDSA, le même niveau de sécurité que RSA peut être atteint, mais avec des clés plus petites. Cela réduit le temps de calcul et augmente les temps de connexion pour les sites qui utilisent des certificats ECDSA.

Le document sur le [chiffrement de nouvelle génération et l'ASA](#) fournit des informations plus détaillées.

Annexe B : Utiliser OpenSSL pour générer un certificat PKCS12 à partir d'un certificat d'identité, d'un certificat d'autorité de certification et d'une clé privée

1. Vérifiez que OpenSSL est installé sur le système sur lequel ce processus est exécuté. Pour les utilisateurs de Mac OSX et GNU/Linux, cette option est installée par défaut.
2. Basculer vers un répertoire valide.

Sous Windows : par défaut, les utilitaires sont installés dans C:\Openssl\bin. Ouvrez une invite de commandes à cet emplacement.

Sous Mac OSX/Linux : ouvrez la fenêtre Terminal dans le répertoire nécessaire à la création du certificat PKCS12.

3. Dans le répertoire mentionné à l'étape précédente, enregistrez les fichiers de clé privée (privateKey.key), de certificat d'identité (certificate.crt) et de chaîne de certificats d'autorité de certification racine (CACert.crt).

Combinez la clé privée, le certificat d'identité et la chaîne de certificats de l'autorité de certification racine dans un fichier PKCS12. Entrez une phrase de passe pour protéger votre certificat PKCS12.

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

4. Convertissez le certificat PKCS12 généré en certificat codé en Base64 :

```
<#root>
```

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

Ensuite, importez le certificat qui a été généré à la dernière étape pour une utilisation avec SSL.

Informations connexes

- [Guide de configuration d'ASA 9.x - Configuration des certificats numériques](#)
- [Comment obtenir un certificat numérique d'une autorité de certification Microsoft Windows avec ASDM sur un ASA](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.