Configurer ASA : Installation et renouvellement du certificat numérique SSL

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configurer
  - Génération CSR
    - 1. Configurez avec l'ASDM
    - 2. Configurez avec l'ASACLI
    - 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
- Foire 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
  - Commandes de dépannage
  - 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 CA et d'une clé privée
  - Annexe C : Considérations relatives à la sécurité des certificats CA approuvés
    - Risques et recommandations liés à l'authentification des certificats
    - Autorisation Risques et recommandations

Ressources supplémentaires

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.

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.

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.

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. PKI Data Formats explique les différents formats de certificat applicables à l'ASA et à Cisco IOS®.

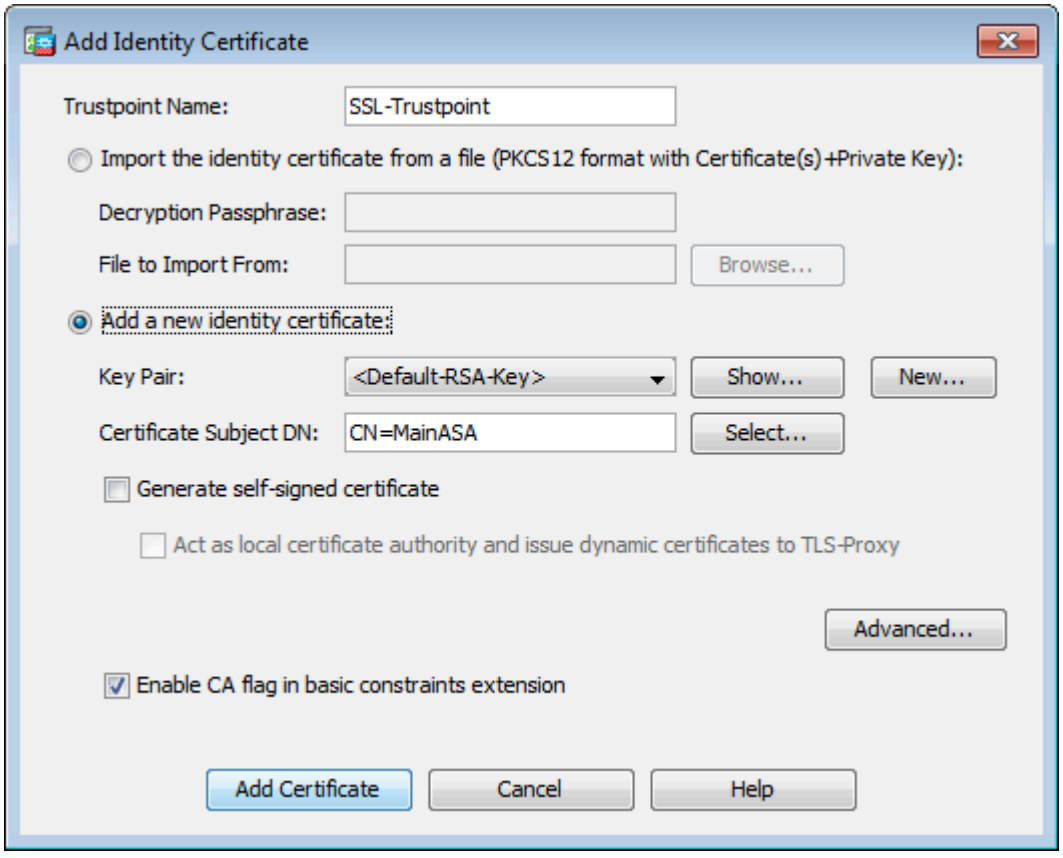
Remarques :
1. Vérifiez auprès de l'autorité de certification la taille de paire de clés requise. Le forum CA/Browser a exigé que tous les certificats générés par leurs CA membres aient une taille minimale de 2048 bits.
2. ASA ne prend actuellement pas en charge les clés 4 096 bits (ID de bogue Cisco 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.

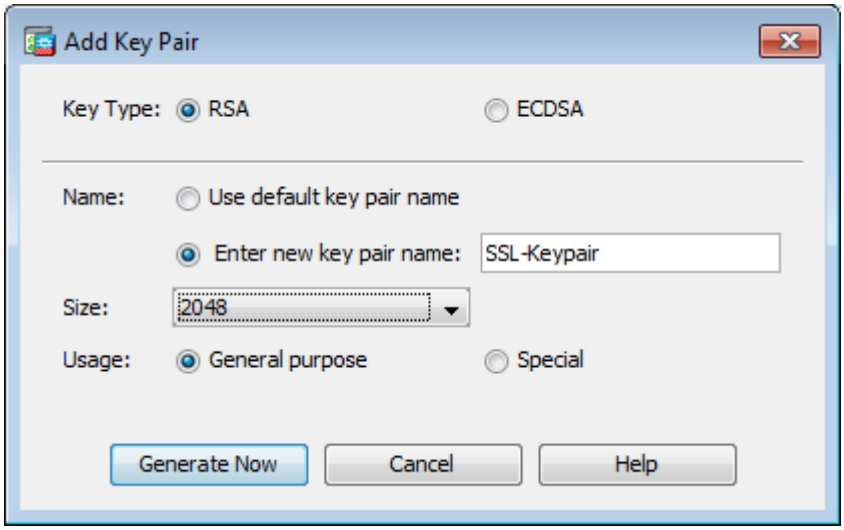
1. Configurez avec ASDM.
2. Configurez avec l'interface CLI ASA.
3. Utilisez OpenSSL pour générer le CSR.

1. Configurez avec l'ASDM

1. Naviguez jusqu'à **Configuration > Remote Access VPN > Certificate Management**, puis sélectionnez **Identity Certificates**.
2. Cliquer **Add**.



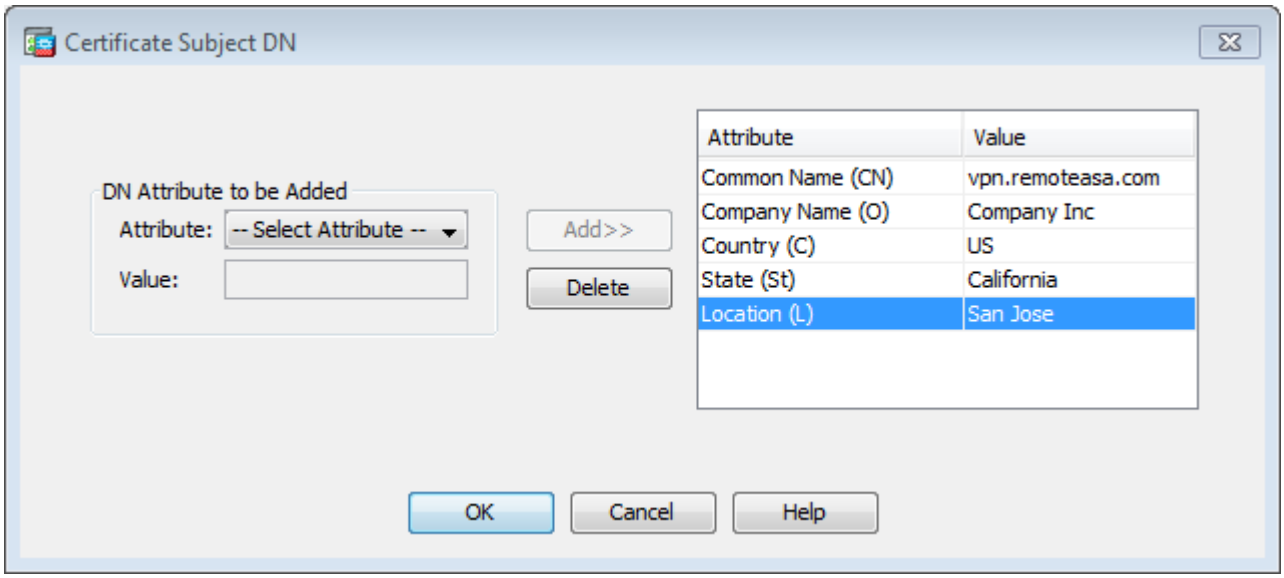
3. Définissez un nom de point de confiance dans le champ d'entrée Nom du point de confiance.
4. Cliquez surAdd a new identity certificatele bouton radio.
5. Pour la paire de clés, cliquez surNew.



6. Choisissez le type de clé - RSA ou ECDSA. (Reportez-vous à l'Annexe A pour comprendre les différences.)
7. Cliquez surEnter new key pair namele bouton radio. Identifiez le nom de la paire de clés à des fins de reconnaissance.
8. Sélectionnez la commandeKey Size. ChoisissezGeneral Purpose for Usage avec RSA.
9. Cliquez surGenerate Now. La paire de clés est créée.
10. Pour définir le DN de l'objet du certificat, cliquezSelect, sur et configurez les attributs répertoriés dans ce tableau :

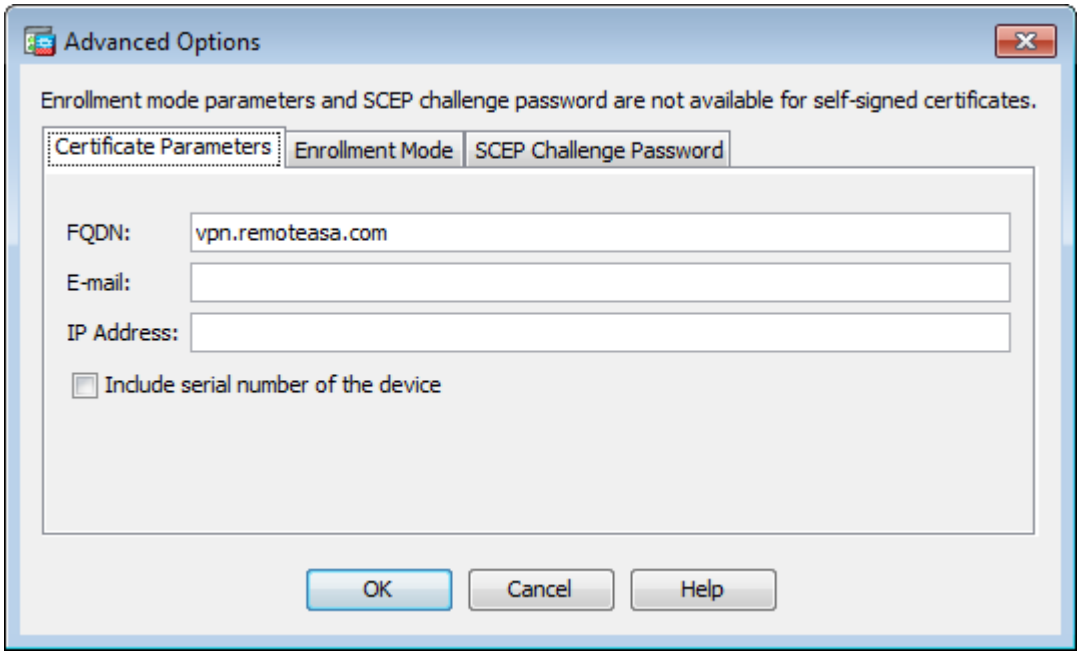
Attribute	Description
CN	FQDN (Full Qualified Domain Name) that will be used for connections to your firewall. For example, webvpn.cisco.com
OU	Department Name
O	Company Name (Avoid using Special Characters)
C	Country Code (2 Letter Code without Punctuation)
St	State (Must be spelled out completely.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



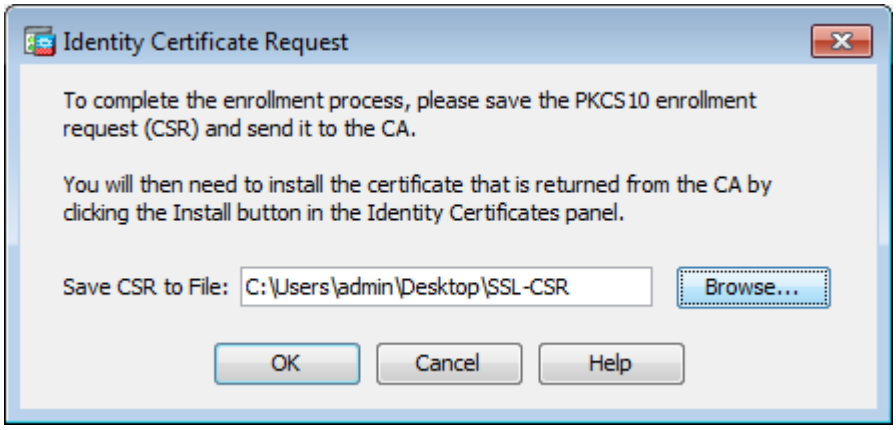
Remarque : Certains fournisseurs tiers exigent l'inclusion d'attributs particuliers avant l'émission d'un certificat d'identité. Si vous n'êtes pas sûr des attributs requis, renseignez-vous auprès du fournisseur.

11. Une fois les valeurs appropriées ajoutées, cliquez**OK** sur La boîte de dialogue Ajouter un certificat d'identité apparaît avec le champ DN du sujet du certificat rempli.
12. Cliquez sur Avancé.



13. Dans**FQDN**le champ, saisissez le nom de domaine complet qui est utilisé pour accéder au périphérique à partir d'Internet. Cliquer**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**OK**,, puis cliquez**Add Certificate.** sur Une invite s'affiche afin d'enregistrer le CSR dans un fichier sur l'ordinateur local.



16. Cliquez**Browse**, sur 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-----
MIIDDjCCAfYCAQAwgYkxETAPBgNVBAcTCFNhbiBKb3NlMRMwEQYDVQQIEwpDYWxp
Zm9ybmlhMQswCQYDVQQGEwJVUzEUMBIGA1UEChMLQ29tcGFueSBJbmMxGjAYBgNV
BAMTEXZwbi5yZW1vdGVhc2EuY29tMSAwHgYJKoZIhvcNAQkCFhF2cG4ucmVtb3Rl
YXNhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK62Nhb9ktlK
uR3Q4TmksyuRMqJNrb9kXpvA6H2OOPuBfQvSF4rVnSwKOmu3c8nweEvYcdVWV6Bz
BhjXeovTVi17FlNTceaUTGikeIdXC+mw1iE7eRsynS/d4mzMWJmrvrsDNzpAW/EM
SzTca+BvqF7X2r3LU8Vsv6Oi8ylhco9Fz7bWvRWVtO3NDDbyolC9b/VgXMuBitcc
rzfUbVnm7VZDOf4jr9EXgUwXxcQidWEABlFrXrtYpFgBo9aqJmRp2YABQ1ieP4cY
3rBtgRjLcF+S9TvHG5m4v7v755meV4YqsZIXvytIOzVBihemVxaGA1oDwfkoYSFi
4CzXbFvdG6kCAwEAAaA/MD0GCSqGSIb3DQEJDjEwMC4wDgYDVR0PAQH/BAQDAgWg
MBwGA1UdEQQVMBOCEXZwbi5yZW1vdGVhc2EuY29tMA0GCSqGSIb3DQEBBQUAA4IB
AQBZuQzUXGEB0ix1yuPK0ZkRz8bPnwIqLTfxZhagmuyEhrN7N4+aQnCHj85oJane
4ztZDiCCoWTerBS4RSkKEHEspu9oohjCYuNnp5qa91SPrZNEjTWwOeRn+qKbId2J
jE6Qy4vdPCexavMLYVQxCny+gVkzPN/sFRk3EcTTVq6DxxaebpJijmiqa7gCph52
YkHXnFne1LQd41BgoLlCr9+hx74XsTHGBmI1s/9T5oAX26Ym+B2l/i/DP5BktIUA
8GvIY1/ypj9KO49fP5ap8al0qvLtYYcCcfwrCt+OojOrZ1YyJb3dFuMNRedAX37t
DuHNl2EYNpYkjVk1wI53/5w3
-----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 utiliseOpenSSL configle fichier pour extraire les attributs à utiliser dans la génération CSR. Ce processus aboutit à la génération d'une CSR et d'une clé privée.

⚠ Mise en garde : Vérifiez que la clé privée qui est 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 à cet emplacement dans C:\Openssl\bin. Ouvrir une invite de commandes.

   Sous Mac OSX/Linux : Ouvrez la fenêtre Terminal dans le répertoire requis pour créer le

CSR.

3. Créez un fichier de configuration OpenSSL avec un éditeur de texte avec les attributs donnés . Une fois fait, enregistrez le fichier en tant que openssl.cnf à l'emplacement mentionné à l'étape précédente (Si vous utilisez la version 0.9.8h et ultérieure, le fichier isopenssl.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

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


[req_ext]

subjectAltName = @alt_names


[alt_names]

DNS.1 = *.remoteasa.com
```

4. Générez la clé CSR et la clé privée à l'aide de 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.url)]:
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

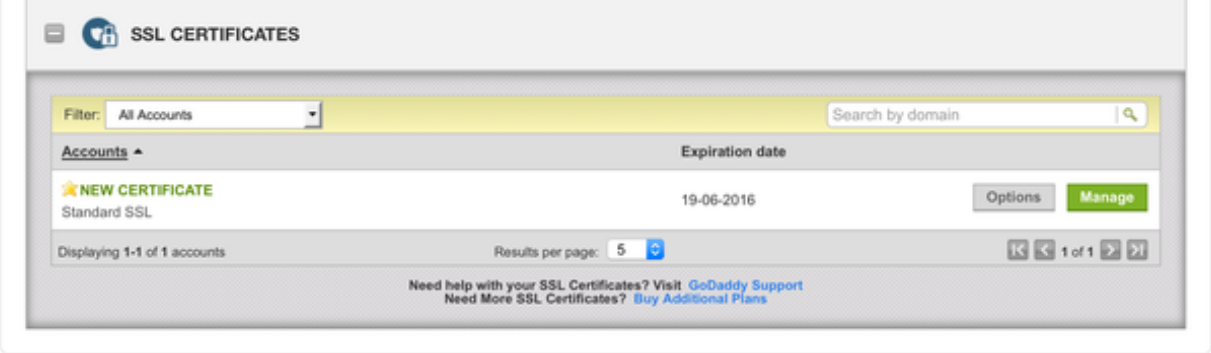
L'étape suivante consiste à faire signer le CSR par l'autorité de certification. L'autorité de certification fournit soit un certificat d'identité codé PEM nouvellement généré, soit un certificat PKCS12 avec l'ensemble de certificats de l'autorité de certification.

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 seul fichier PKCS12 (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 de CA. Lisez attentivement la documentation de l'autorité de certification avant de continuer.

Exemple de génération de certificat SSL sur GoDaddy CA

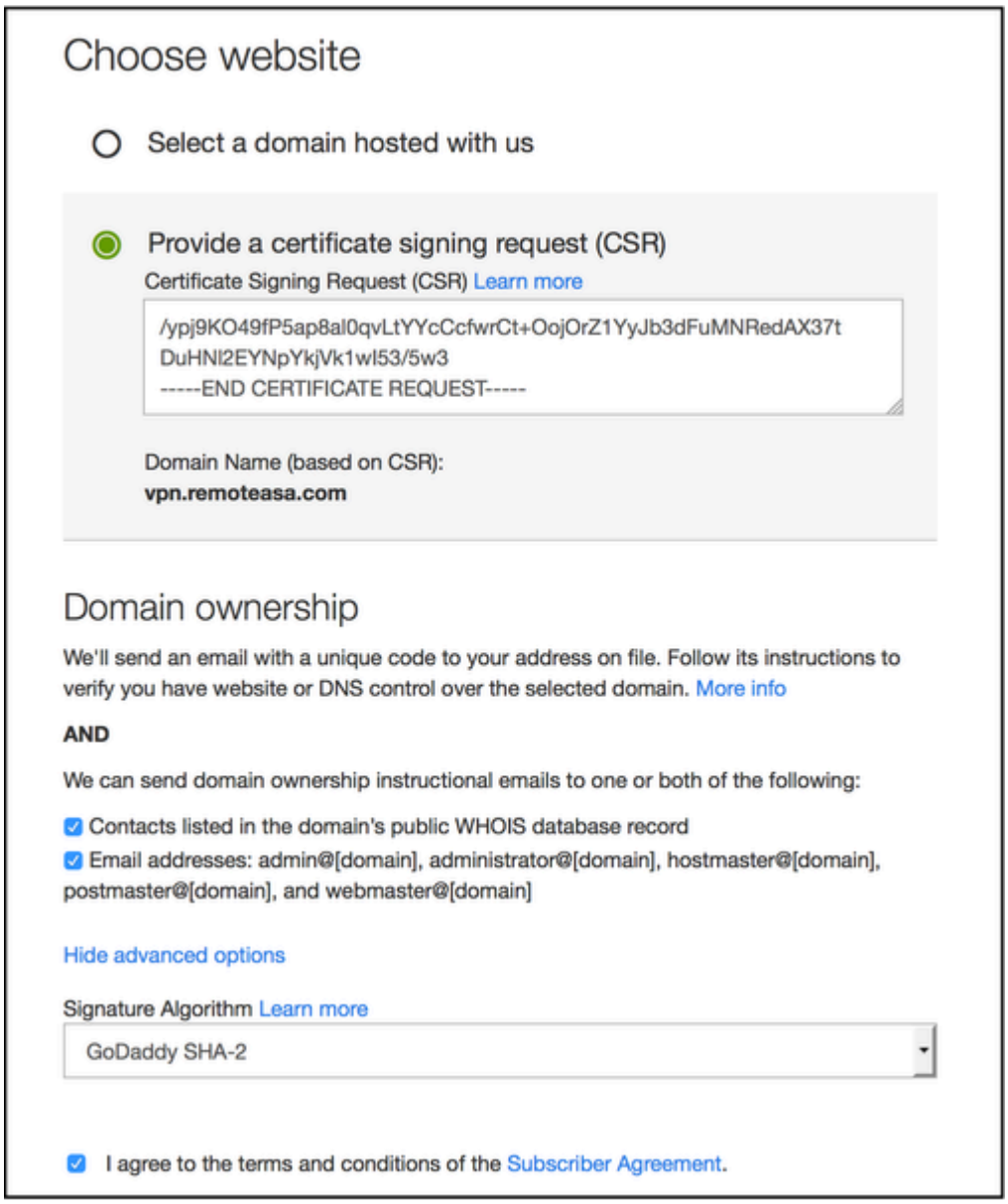
Après l'achat et la phase de configuration initiale du certificat SSL, accédez au compte GoDaddy et affichez les certificats SSL. Il doit y avoir un nouveau certificat. Cliquez**Manage** pour continuer.



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

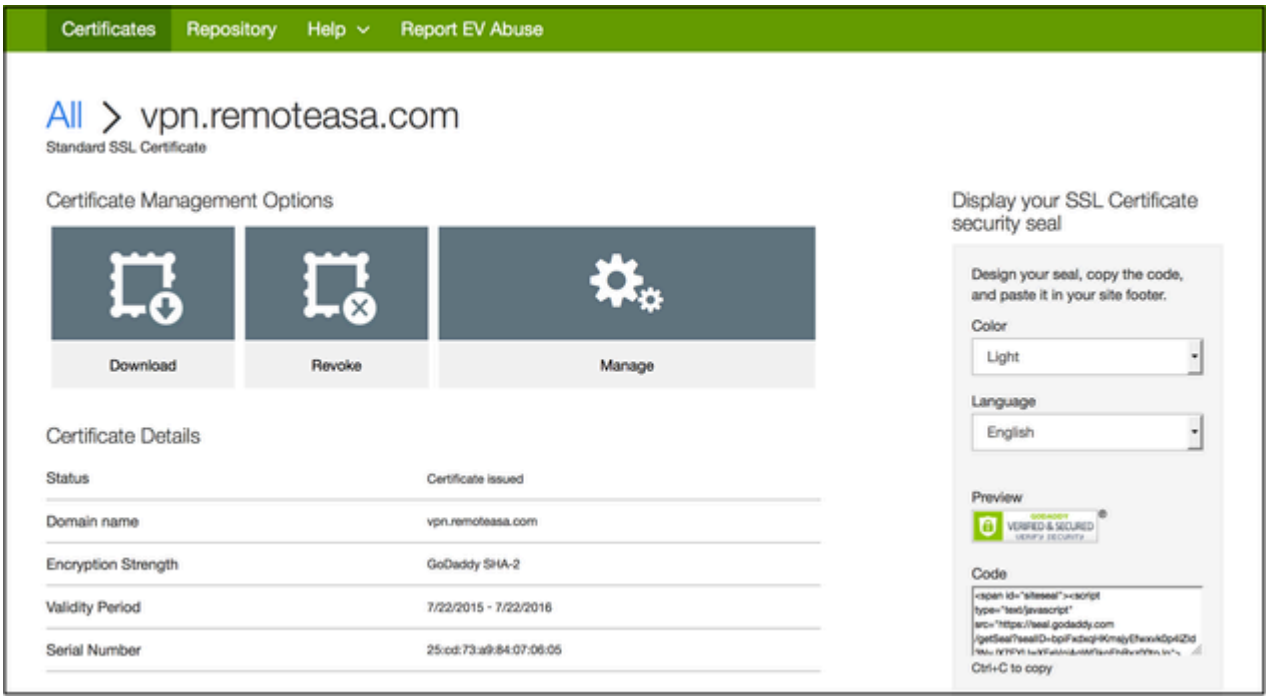
En fonction du CSR saisi, l'autorité de certification détermine le nom de domaine auquel le certificat doit être délivré.

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

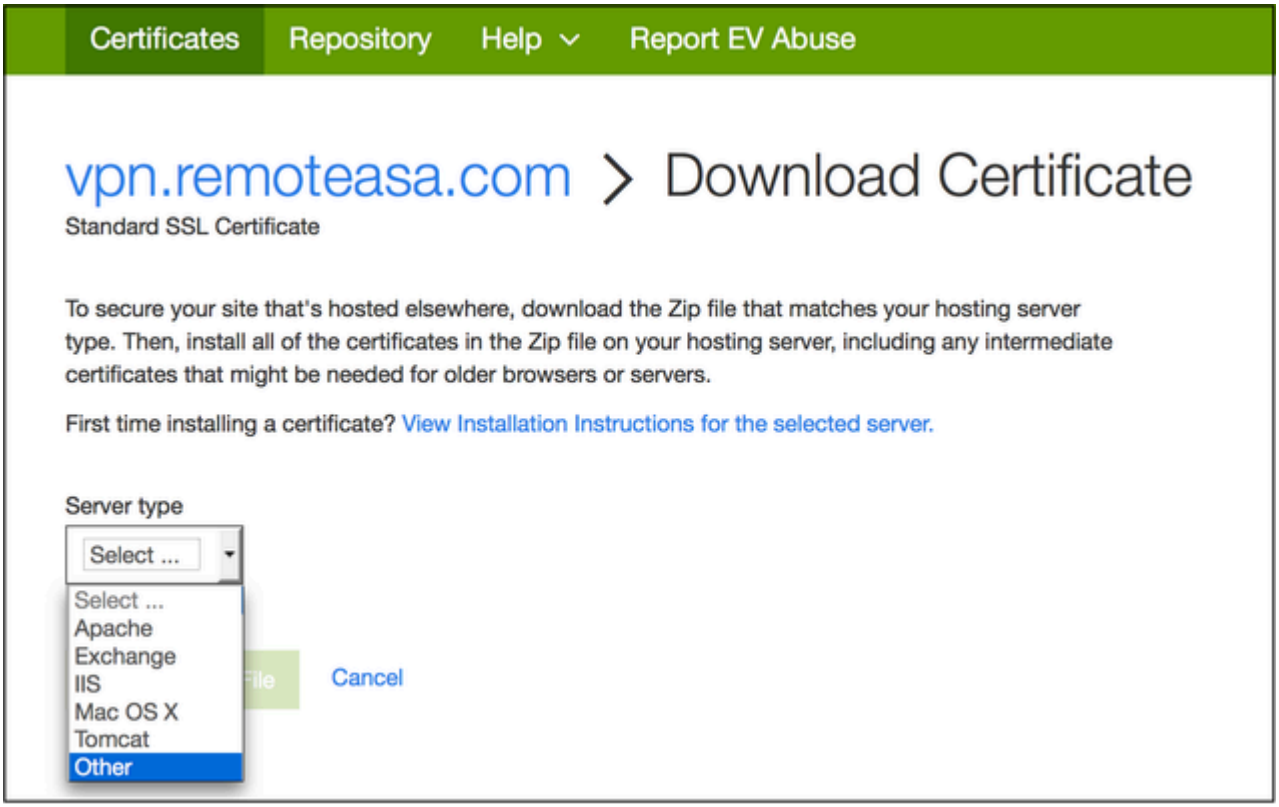


Remarque : GoDaddy et la plupart des autres CA utilisent SHA-2 ou SHA256 comme algorithme de signature de certificat par défaut. ASA prend en charge l'algorithme de signature SHA-2 qui démarre à partir de la version 8.2(5) [versions antérieures à la version 8.3] et de la version 8.4(1) [versions postérieures à la version 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.

Une fois la demande soumise, GoDaddy vérifie la demande avant de délivrer le certificat. Une fois la demande de certificat validée, GoDaddy délivre le certificat au compte. Le certificat peut ensuite être téléchargé pour installation sur l'ASA. Cliquez**Download** sur la page pour continuer.



ChoisissezOther comme type de serveur et téléchargez le bundle certificate zip.



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 :

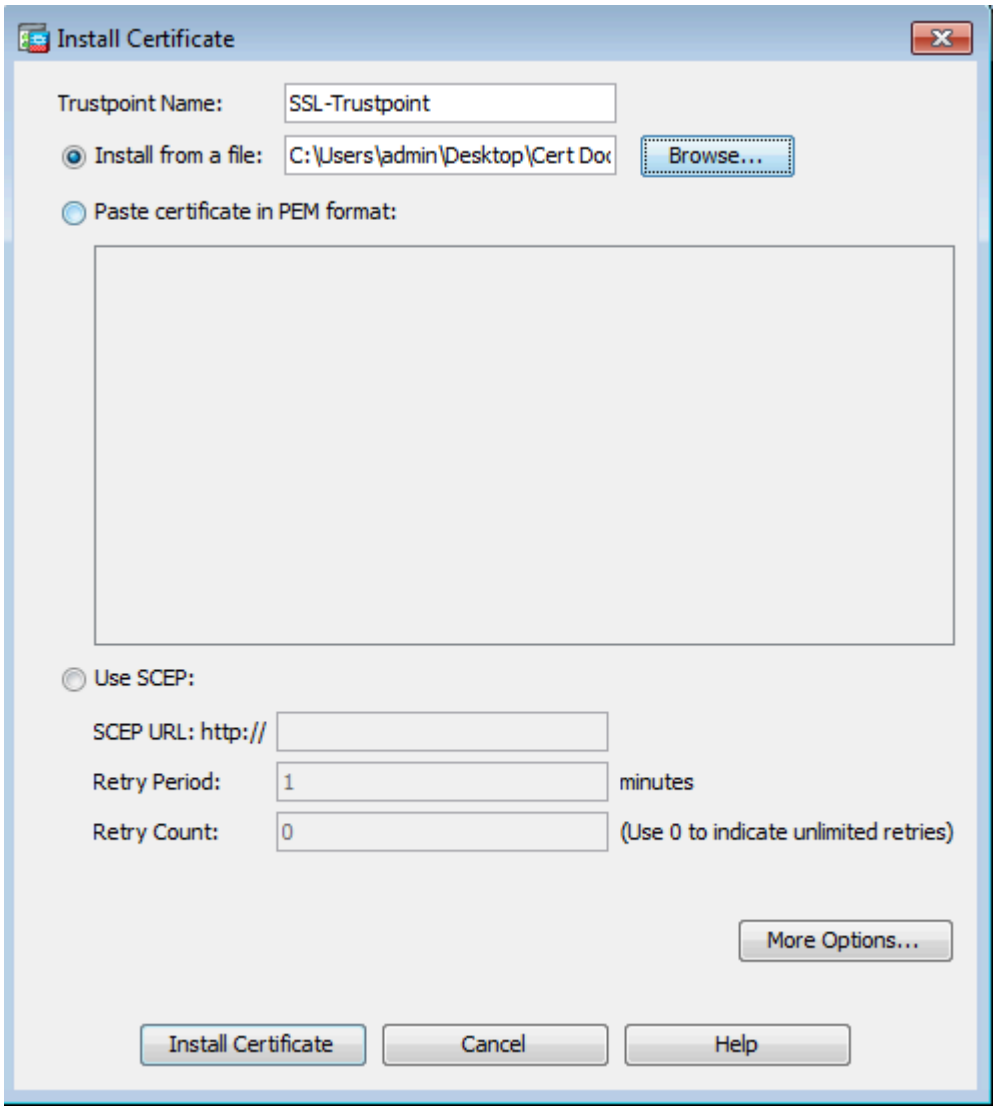
1. Importez l'autorité de certification et le certificat d'identité séparément dans les formats PEM.
2. Vous pouvez également importer le fichier PKCS12 (codé en base64 pour l'interface de ligne de commande) dans lequel le certificat d'identité, le certificat d'autorité de certification et la clé privée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

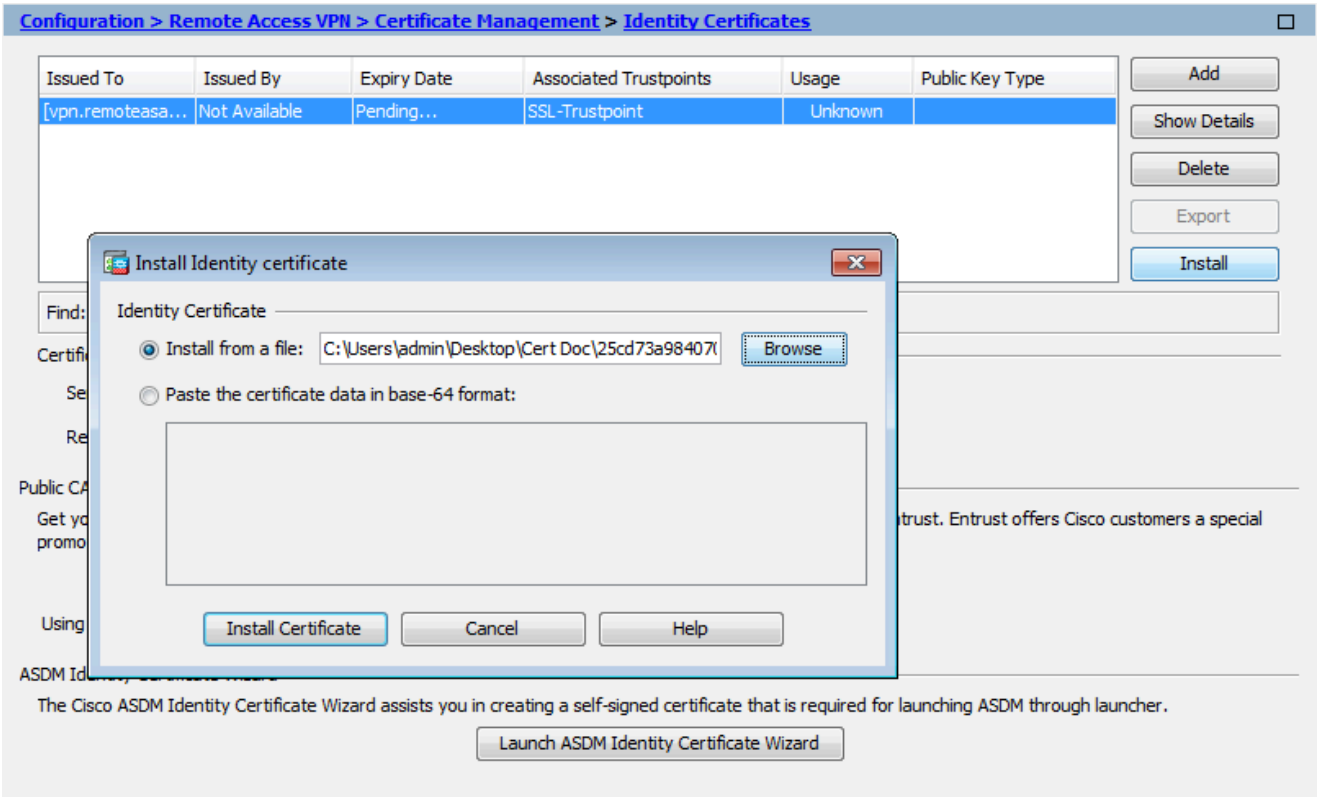
1.1 Installation du certificat d'identité au format PEM avec ASDM

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.

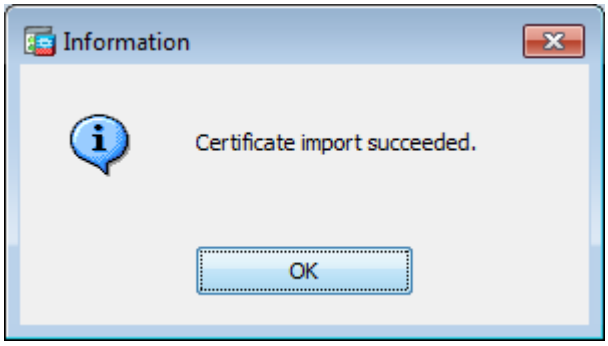
1. Naviguez jusqu **Configuration > Remote Access VPN > Certificate Management**,'à CA Certificates et choisissez CA Certificates.
2. Le certificat codé PEM dans un éditeur de texte et copiez-collez le certificat CA base64 fourni par le fournisseur tiers dans le champ de texte.



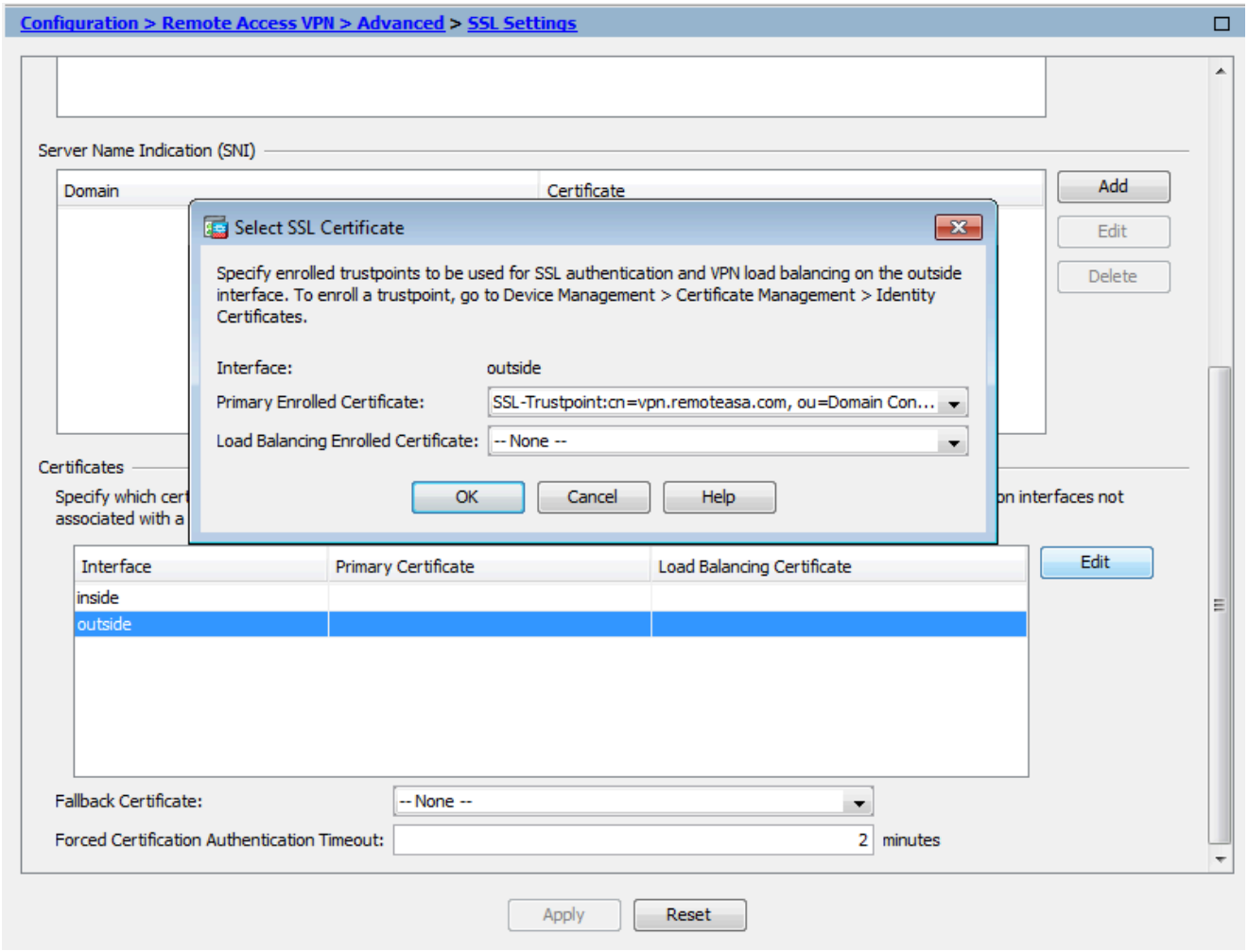
3. Cliquez sur Installer le certificat.
4. Naviguez jusqu**Configuration > Remote Access VPN > Certificate Management**'à et choisissez Certificats d'identité.
5. Sélectionnez le certificat d'identité créé précédemment. Cliquer **Install**.
6. Cliquez sur la case d'option**Install from a file** et choisissez 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 qui est 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 certificat nouvellement installé.



12. Cliquer**OK**.
13. Cliquez**Apply**. sur 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----- MIIEADCCAuigAwIBAgIBADANBgkqhkiG9w0BAQUFADBjMQswCQYDVQQGEwJVUzEh MB8GA1UEChM

!!! - 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+cVMA0GCSqGSIb3DQEBCwUAMGMxCzAJBgNVBAYTAlVT
MSEwHwYDVQQKExhUaGUgR28gRGFkZHkgR3JvdXAsIEluYy4xMTAvBgNVBAsTKEdv
IERhZGR5IENsYXNzIDIgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMTQwMTAx
MDcwMDAwWhcNMzEwNTMwMDcwMDAwWjCBgzELMAkGA1UEBhMCVVMxEDAOBgNVBAgT
B0FyaXpvbmExEzARBgNVBAcTClNjb3R0c2RhbGUxGjAYBgNVBAoTEUdvRGFkZHku
Y29tLCBJbmMuMTEwLwYDVQQDEyhHbyBEYWRkeSBSb29tIENlcnRpZmljYXRlIEF1
dGhvcml0eSAtIEcyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAv3Fi
CPH6WTT3G8kYo/eASVjpIoMTpsUgQwE7hPHmhUmfJ+r2hBtOoLTbcJjHMgGxBT4H
Tu70+k8vWTAi56sZVmvigAf88xZ1gDlRe+X5NbZ0TqmNghPktj+pA4P6or6KFWp/
3gvDthkUBcrqw6gElDtGfDIN8wBmIsiNaW02jBEYt9OyHGC0OPoCjM7T3UYH3go+
6118yHz7sCtTpJJiaVElBWEaRIGMLKlDliPfrDqBmg4pxRyp6V0etp6eMAo5zvGI
gPtLXcwy7IViQyU0AlYnAZG003AqP26x6JyIAX2f1PnbU21gnb8s51iruF9G/M7E
GwM8CetJMVxpRrPgRwIDAQABo4IBFzCCARMwDwYDVR0TAQH/BAUwAwEB/zAOBgNV
HQ8BAf8EBAMCAQYwHQYDVR0OBBYEFDqahQcQZyi27/a9BUFuIMGU2g/eMB8GA1Ud
IwQYMBaAFNLEsNKR1EwRcbNhyz2h/t2oatTjMDQGCCsGAQUFBwEBBCgwJjAkBggr
BgEFBQcwAYYYaHR0cDovL29jc3AuZ29kYWRkeS5jb20vMDIGA1UdHwQrMCkwJ6Al
oCOGIWh0dHA6Ly9jcmwuZ29kYWRkeS5jb20vZ2Ryb290LmNybDBGBgNVHSAEPzA9
MDsGBFUdIAAwMzAxBggrBgEFBQcCARYlaHR0cHM6Ly9jZXJ0cy5nb2RhZGR5LmNv
bS9yZXBvc2l0b3J5LzANBgkqhkiG9w0BAQsFAAOCAQEAWQtTvZKGEacke+1bMc8d
H2xwxbhuvk679r6XUOEwf7ooXGKUwuN+M/f7QnaF25UcjCJYdQkMiGVnOQoWCcWg
OJekxSOTP7QYpgEGRJHjp2kntFolfzq3Ms3dhP8qOCkzpN1nsoX+oYggHFCJyNwq
9kIDN0zmiN/VryTyscPfzLXs4Jlet0lUIDyUGAzHHFIYSaRt4bNYC8nY7NmuHDKO
KHAN4v6mF56ED71XcLNa6R+ghlO773z/aQvgSMO3kwvIClTErF0UZzdsyqUvMQg3
qm5vjLyb4lddJIGvl5echK1srDdMZvNhkREg5L4wn3qkKQmw4TRfZHcYQFHfjDCm
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-----
MIIFRjCCBC6gAwIBAgIIJc1zqYQHBgUwDQYJKoZIhvcNAQELBQAwgbQxCzAJBgNV
BAYTAlVTMRAwDgYDVQQIEwdBcml6b25hMRMwEQYDVQQHEwpTY29OdHNkYWxlMRow
GAYDVQQKExFHb0RhZGR5LmNvbSwgSW5jLjEtMCsGA1UECxMkaHR0cDovL2NlcnRz
LmdvZGFkZHkuY29tL3JlcG9zaXRvcnkvMTMwMQYDVQQDEypHbyBEYWRkeSBTZWN1
cmUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5IC0gRzIwHhcNMTUwNzIyMTIwNDM4WhcN
MTYwNzIyMTIwNDM4WjA/MSEwHwYDVQQLExhEb21haW4gQ29udHJvbCBWYWxpZGF0
ZWQxGjAYBgNVBAMTEXZwbi5yZW1vdGVhc2EuY29tMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEArrY2Fv2S2Uq5HdDhOaSzK5Eyok2tv2Rem8DofbTQ+4F9
C9IXitWdLAo6a7dzyfB4S9hx1VZXoHMGGNd6i9NWLXsWU1Nx5pRMaKR4h1cL6bDW
ITt5GzKdL93ibMxYmau+uwM3OkBb8QxLNNxr4G+oXtfavctTxWy/o6LzKWFyj0XP
tta9FZWO7c0MNvKiUL1v9WBcy4GK1xyvN9RtWebtVkM5/iOv0ReBTBfFxCJ1YQAG
UWteu1ikWAGj1qomZGnZgAFDWJ4/hxjesG2BGMtwX5L1O8cbmbi/u/vnmZ5Xhiqx
<snip>
CCsGAQUFBwIBFitodHRwOi8vY2VydGlmaWNhdGVzLmdvZGFkZHkuY29tL3JlcG9z
aXRvcnkvMHYGCCsGAQUFBwEBBGowaDAkBggrBgEFBQcwAYYYaHR0cDovL29jc3Au
Z29kYWRkeS5jb20vMEAGCCsGAQUFBzAChjRodHRwOi8vY2VydGlmaWNhdGVzLmdv
ZGFkZHkuY29tL3JlcG9zaXRvcnkvZ2RpZzIuY3JOMB8GA1UdIwQYMBaAFEDCvSeO
zDSDMKIz1/tss/C0LIDOMEYGA1UdEQQ/MD2CEXZwbi5yZW1vdGVhc2EuY29tghV3
d3cudnBuLnJlbW9OZWFzYS5jb22CEXZwbi5yZW1vdGVhc2EuY29tMB0GA1UdDgQW
BBT7en7YS3PH+s4z+wTRlpHr2tSzejANBgkqhkiG9w0BAQsFAAOCAQEAO9H8TLNx
2YOrYdI6gS8n4imaSYg9Ni/9Nb6mote3J2LELG9HY9m/zUCR5yVktra9azdrNUAN
1hjBJ7kKQScLC4sZLONdqG1uTP5rbWROyikF5wSzgyMWdO3kOR+vM8q6T57vRst5
69vzBUuJc5bSu1IjyfPP19z1l+B2eBwUFbVfXLnd9bTfiG9mSmC+4V63TXFxt1Oq
xkGNys3GgYuCUy6yRP2cAUV1lc2tYtaxoCL8yo72YUDDgZ3a4PyO1EvC1FOaUtgv
6QNEOYwmbJkyumdPUwko6wGOC0WLumzv5gHnhil68HYSZ/4XIlp3B9Y8yfG5pwbn
7puhazH+xgQRdg==
-----END CERTIFICATE-----
quit
INFO: Certificate successfully imported
! Apply the newly installed SSL certificate to the interface accepting SSL connections
```

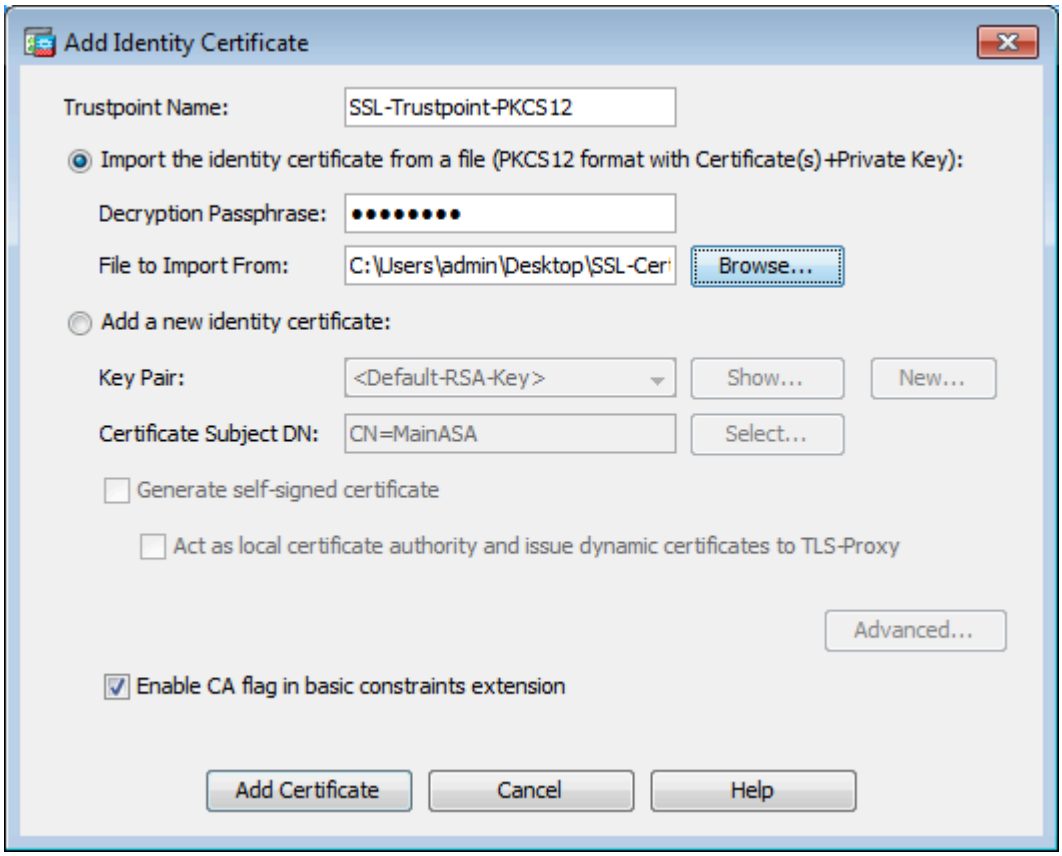
MainASA(config)#

ssl trust-point SSL-Trustpoint outside

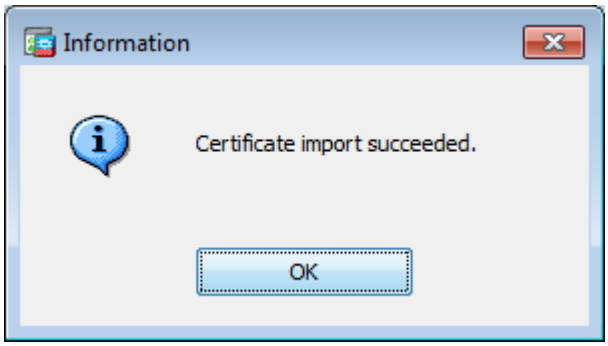
2.1 Installation d'un certificat PKCS12 avec ASDM

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.

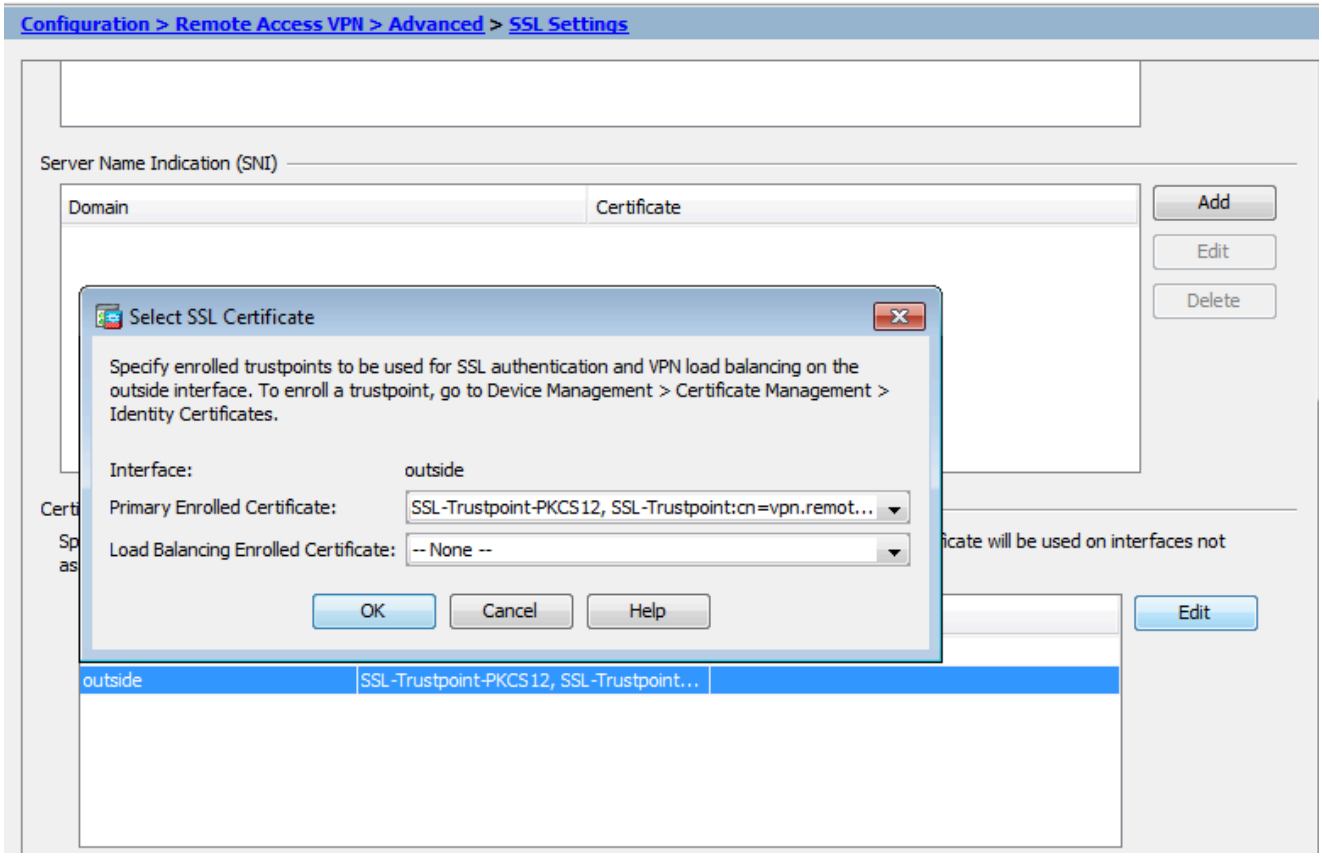
1. Dans le certificat d'identité, groupez le certificat d'autorité de certification et la clé privée dans un fichier PKCS12 unique. L'annexe B décrit les étapes à suivre pour effectuer cette opération avec OpenSSL. Si déjà groupé par l'autorité de certification, passez à l'étape suivante.
2. Naviguez jusqu**Configuration > Remote Access VPN > Certificate Management**,'à et sélectionnez **Identity Certificates**.
3. Cliquer**Add**.
4. Spécifiez un nom de point de confiance.
5. Sélectionnez la case d'**Import the identity certificate from a file**option.
6. Entrez la phrase de passe utilisée pour créer le fichier PKCS12. Recherchez et sélectionnez le fichier PKCS12. Entrez la phrase de passe du certificat.



7. Cliquez sur Ajouter un certificat.



8. Naviguez jusqu'**Configuration > Remote Access VPN > Advanced**,à et choisissez **SSL Settings.**
9. Sous Certificates, choisissez l'interface qui est 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 certificat nouvellement installé.



12. Cliquer**OK**.
13. **Apply**.ClickLe nouveau certificat est maintenant utilisé 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-----
MIISNwIBAzCCEfEGCSqGSIb3DQEHAaCCEeIEghHeMIIR2jCCEdYGCSqGSIb3DQEH
BqCCEccwghHDAgEAMIIRvAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIWO3D
hDti/uECAQGAghGQ9ospee/qtIbVZh2T8/Z+5dxRPBcStDTqyKy7q3+9ram5AZdG
Ce9n5UCckqT4WcTjs7XZtCrUrt/LkNbmGDVhwGBmYWiOS7npgaUqOeoqiJRK+Yc7
LNOnbho6I5WfL56/JiceAMlXDLr/IqqLg2QAApGdN+F5vANsHse2GsAATewBDLt7
Jy+SKfoNvvIw9QvzCiUzMjYZBANmBdMCQ13H+YQTHitT3vn2/iCDlzRSuXcqypEV
q5e3heiOO75lE8TDLWmO3PMvwIZqi8yzWesjcTt1Kd4FoJBZpB7O/v9LntoIUOY7
kIQM8fHb4ga8BYfbgRmG6mkMmO1STtbSvlvTa19WTmdQdTyCa+G5PkrryRsy3Ww1
lkGFMhImmrnNADF7HmzbyslVohQZ7hO9iVQY9krJogoXHjmQYxG9brfOoEwxSJDa
mGDhhESh+s/WuFSV9Z9kiTXpJNZxpTASoWBQrrwmO5v8ZwbjbVNJ7sVdbwpUl6d+
NNFGR7LTqO8hpupeeJnY9eJc2yYqeAXWXQ5kLOZo6/gBEdGtEaZBgCFK9JZ3bl3A
xqxGifanWPnLYG611NKuNjTgbjhnEEYI2uZzUOqxnlKa8zyXw+lzrKuJscDbkAPZ
wKtw8K+p4OzXVHhuANo6MDvffNRY1KQDtyK1inoPH5ksVSE5awkVam4+HTcqEUfa
16LMana+4QRgSetJhUOLtSMaQfRJGkha4JLq2t+JrCAPz2osARlTsBOjQBNq6YNj
OuB+gGk2Gl8Q5Nln6K1fzOXBFZLWEDBLsaBRO5MAnE7wWtOO+4awGYqVdmIF1lkf
XIRKAiQEr1pZ6BVPuvsCNJxaaUHzufhYI2ZAckasKBZOT8/7YK3fnAaGoBCz4cHa
o2EEQhq2aYb6YTvO+wtLEWGHzsbGZEM/u54XmsXAI7g28LGJYdfWi5O9KyV+Ac1V
KzHqXZMM2BbUQCNcTF5JIMiW+r62k42FdahfaQbOvJsIe/IwkAKG7y6DIQFsOhwg
ZlPXiDbNr1k4e8L4gqupMKWg853PY+oY22rLDC7bul1CKtixIYBCvbn7dAYsI4GQ
l6xXhNu3+iyeOHgbUQQCfTU/mBrAOZO+bpKjWOCfqNBuYnZ6kUEdCI7GFLH9QqtM
K7YinFLoHwTWbi3MsmqVv+Z4ttVWy7XmikoO2nMynJMP6/CNV8OMxMKdC2qm+c1j
s4QlKcAmFsQmNp/7SIP1wnvOc6JbUmC1O52OU/r8ftTzn8C7WL62W79cLK4HOr7J
sNsZnOz0JOZ/xdZT+cLTCtVevKJOQMK3vMsiOuy52FkuF3HnfrmBqDkbR7yZxELG
RCELOEDdbp8VP0+IhNlyz1q7975SscdxFSLOTvjnHGFWd14ndoqN+bLhWbdPjQWV
l3W2NCI95tmHDLGgp3POOlS+RjdCEGGMg+9cpgBfFC1JocuTDIEcUbJBY8QRUNiS
/ubyUagdzUKt1ecfb9hMLP65ZNQ93VIw/NJKbIm7b4P/1Zp/lFP5eq7LkQPAxE4/
bQ4mHcnwrs+JGFkN19B8hJmmGoowH3p4IEvwZy7CThB3E1ejw5R4enqmrgvHqpQe
B7odN1OFLAHdo1G5BsHExluNEsEb4OQOpmKXidDB5BOO1bJsr748fZ6L/LGx8Al3
<snip>
ijDqxyfQXY4zSytljSMwMtYA9hG5I79Sg7pnME1E9xq1DOoRGg8vgxlwiciKtLxp
LLOReDY31KRYvOOvWOgf+tE7lST/3TKZvh0sQ/BE0V3kHnwldejMFH+dvyAA9Y1E
c8O+tdafBFX4B/HP46E6heP6ZSt0xAfRW1/JF4ljNvUNVO9VtVfR2FTyWpzZFY8A
GG5XPIA8OWF6wKEPFHIcN8scY+Vot8kXxG96hwt2Cm5NQ2OnVzxUZQbpKsjs/2jC
3HVFe3UJFBsY9UxTLcPXYBSIG+VeqkI8hWZp6clTfNDLY2ELDylQzp1mBg2FujZa
YuEOavjCJzBzZUG2umtS5mHQnwPF+XkOujEyhGMauhGxHp4nghSzrUZrBeuL9lUF
2mbpsOcgZkzxMS/rjdNXjCmPFloRBvKkZSlxHFrE/5ZopAhn4i7YtHQNrz9U4RjQ
xo9cUuaJ+LNmvzE8Yg3epAMYZ16UNGQQkVQ6ME4BcjRONzW8BYgTq4+pmT1ZNq1P
X87CXCPtYRpHF57eSo+tHDINCgfqYXD6e/7r2ngfiCeUeNDZ4aVl2XxvZDaUlBPP
Tx5fMARqx/Z8BdDyBJDVBjdsxmQau9HLkhPvdfGlZIWdTe13CzKqXA5Ppmpjt4q9
GnCpC53m76x9Su4ZDw6aUdBcgCTMvfaqJC9gzObee2Wz+aRRwzSxu6tEWVZolPEM

```
v0AA7po3vPeklgOnLRAwEoTTn4SdgNLWeRoxqZgkw1FC1GrotxF1so7uA+z0aMeU
lw73reonsNdZvRAcVX3Y6UNFdyt70Ixvo1H4VLzWm0K/oP62C9/eqqMwZ8zoCMPt
ENna7T+7Os66SCbMmXCHwyhO0tygNKZFFw/AATFyjqPMWPAxGuPNOrnB6uYCn0Hk
1BU7tF143RNIZaQQEH3XnaPvUuAA4C0FCoE3h+/tVjtfNKDvFmb6ZLZHYQmUYpyS
uhdFEpoDrJH1VmI2Tik/iqYWaZ+oDqXPHQXnJhw25h9ombR4qnD+FCfwFCGtPFON
o3QffZ53C95n5jPHVMyUrOxDdpwnvzCQPdj6yQm564TwLAmiz7uDlpqJZJe5QxHD
nolv+4MdGSfVtBq+ykFoVCaamqeaq6sKgvAVujLXXEs4KEmIgcPqATVRG49ElndI
LO1DEQyKhVoDGebAuVRBjzwAm/qxWxxFv3hrbCjpHCwEYms4Wgt/vKKRFsuWJNZf
efHldwlltkd5dKwSvDocPT/7mSLtLJa94c6AfgxXy9zO+FTLDQwzxga7xC2krAN1
yHxR2KHN5YeRL+KDzu+u6dYoKAz+YAgwlW6KbeavALSuH4EYqcvg8hUEhp/ySiSc
RDhuygxEovIMGfES4FP5V52lPyDhM3DqwhnOvuYUmYnX8EXURkay44iwwI5HhqYJ
lptWyYo8Bdr4WNwt5xqszGzYR6mmGeAIin7bDunsF1uBHWYF4dyKlz1tsdRNMYqQ
+W5q+QjVdrjldWv/bMFOaqEjxeNWBRqjzcff3BxMnwvVxtgqxFvRh+DZxiJoiBG+
yx7x8np2AQ1rOMETSSxbnZzfnKZKVvBVMkIC6Jsmt2WEVTQvoFJ8em+nemOWgTi/
hHSBzjE7RhAucnHuifOCXOgvR1SDDqyCQbiduc1QjXNOsvA8Fqbea9WEH5khOPv3
pbtsL4gsfl2pv8diBQkVQgiZDi8Wb++7PR6ttiY65kVwrdsoNl1/qq+xWOd3tB4/
zoH9LEMgTy9Sz7myWrB9EOOZ8BIjL1M8oMigEYrTDOc3KbyW1S9dd7QAxiuOBaX1
8J8q1OydvTBzmqcjeSsFH4/1NHn5VnfOZnNpui4uhpOXBG+K2zJUJXm6dq1AHBlE
KQFsFZpNNyave0Kk8JzQnLAPd7OUU/IksyOCGQozGBH+HSzVp1RDjrrbC342rkBj
wnI+j+/1JdWBmHdJMZCfoMZFLSI9ZBqFirdii1/NRu6jh76TQor5TnNjxIyNREJC
FE5FZnMFvhM9OOLaiUZff8WWCOfeRDMttLXb1nuxPFl+lRk+LNlPLVptWgcxzfsr
JXrGiwjxybBB9oCOrACq8fGAtEs8WRxJyDH3Jjmn9i/Gl6J1mMCUF//LxAH2WQx8
Ld/qS5OM2iFCffDQjxAj0K6DEN5pUebBv1Em5SOHXvyq5nxgUh4/y84CWaKjwOMQ
5tbbLMlnc7ALIJ9LxZ97YiXSTyeM6oBXBFx6RpklkDvO5mlBghSpVQiMcQ2ORIkh
UVVNbSHOl9S3cb5wqxaWqAKBqb4h1uLGVbYWZf2mzLZ8U5U5ioiqoMBqNZbzTXpO
EqEFuatTllQvCRbcKS3xou4MAixcYUxKwEhbZA/6hd1OXSBJwe7jKBV9M6wliKab
UfoJCGTAf3sY68lqrMPrbBt0eeWf1CO2Sd9Mn+V/jvnil7mxYFFUpruRq3r1LeqP
J5camfTtHwyL8N3Q/Zwp+zQeWZiLA8a/iAVu/hYLR1bpF2WCKOlOtJqkvVmrLVLz
maZZjbJeOft5cP/lRxbKlS6Gd5dFTEKDE15c6gWUX8RKZP6Q7iaE5hnGmQjm8Ljl
kXwF+ivoxOQ8a+Gg1bVTROc7tqW9e9/ewisV1mwvEB6Ny7TDS1oPUDHM84pY6dqi
1+Oio07Ked4BySwNlYy9yaJtBTZSCstfP+ApLidN7pSBvvXf1aHmeNbkPOZJ+c+t
fGpUdL6V2UTXfCsOPHTC0ezA15sOHwCuPchrDIj/eGUwMS3NfS25XgcMuvnLqGVO
RzcRzlZIg8G0oLYwOCuzoY0D/m9O1OO1ahePyA9tmVB7HRRbytLdaW7gYeEikoCv
7qtBqJFF17ntWJ3EpQHZUcVClbHIKqjNqRbDCY7so4AlIW7kSEUGWMIUDhprE8Ks
NpnvPH2i9JrYrTeROyUIOtL/7SATd2POa2lxz/zUWekeqdObmVCsAgQNbB2XkrR3
XS0B52ol+63e8KDqS2zL2TZd3daDFidHlB8QB26tfbfOAcaObJH5/dWP8ddo8UYo
Y3JqTlOmalxSJhaMHmQdZIQp49utW3TcjqGllYS4HEmcqtHud0ShaUysC6239jlQ
KlFWrwXTlBC5vnq5IcOMqx5zyNbfxXz28969cWoMCyU6+kRwOTyF6kF7EEv6XWca
XLEwABx+tKRUKHJ673SyDMu96KMV3yZN+RtKbCjqCPVTP/3ZeIp7nCMUcj5sW9HI
N34yeI/0RCLyeGsOEiBLkucikC32LI9ik5HvImVTELQOUz3ceFqU/PkasjJUve6S
/n/1ZVUHbUk71xKR2bWZgECl7fIel7wlrbjpF3Wbk+Er0kfYcsNRHxeTDpKPSt9s
u/UsyQJiyNARG4X3iYQlsTce/O6Ycyri6GcLHAu58BO2nj4CxolCplABZ2N79HtN
/7Kh5LOpS9MwsDCHuUI8KFrTsET7TB1tIU99FdB19L64sl/shYAHbccvVWU5OWht
PdLoaErrX81Tof41IxbSZbI8grUC4KfG2sdPLJKu3HVTeQ8LfllbBLxfs8ZBS+Oc
v8rHlQO12kY6LsFGLehJ+/yJ/uvXORivOESp4EhFpFfkp+o+YcFeLUUPd+jzb62K
HfSCCbLpCKyEay8OdyWkHfgylqxmb9ud0oMO5OaFJyqR0NjNt6pcxBRY2A6AJR5S
IIC26YNwbhOGjF9qL2FiUqnNH/7GTqPnd2qmsB6FTIwSBT6d854qN7PRt+ZXgdtQ
OjcYt1r9qpWDZpNFK8EzizwKiAYTsiEh2pzPt6YUpksRb6CXTkIzoG+KLsv2m3b8
OHyZ9a8z81/gnxrZlls5SCTfOSU7OpHWh8VAYKVHHK+MWgQrOm/2ocV32dkRBLMy
2R6P4WfHyI/+9de1x3PtIuOiv2knpxHv2fKM6sQw45F7XkmwHxjq1YRJ6vIwPTAh
MAkGBSsOAwIaBQAEFFTRETzpisHKZR+Kmen68VrTwpV7BBSQiOIesQ4n4E/bSVsd
qJSzcwh0hgICBAA=
-----END PKCS12-----
quit
```

INFO: Import PKCS12 operation completed successfully

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

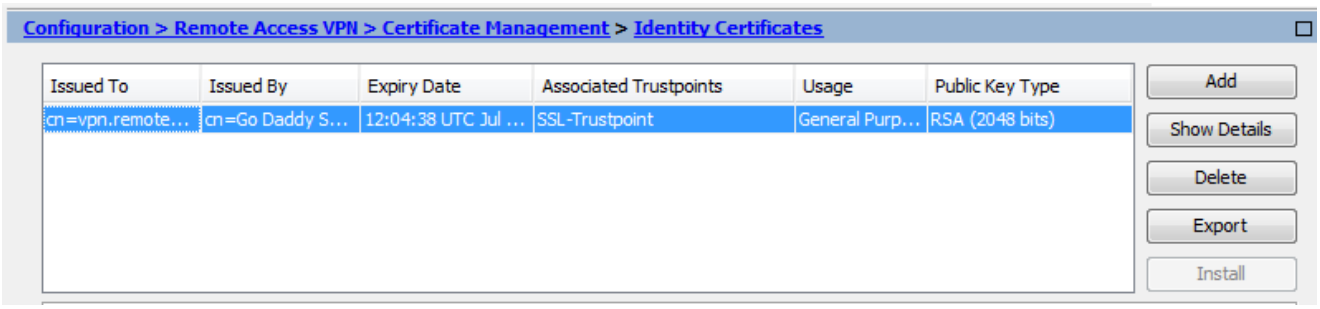
```
ssl trust-point SSL-Trustpoint-PKCS12 outside
```

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'**Configuration** > **Remote Access VPN** > **Certificate Management**,à 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

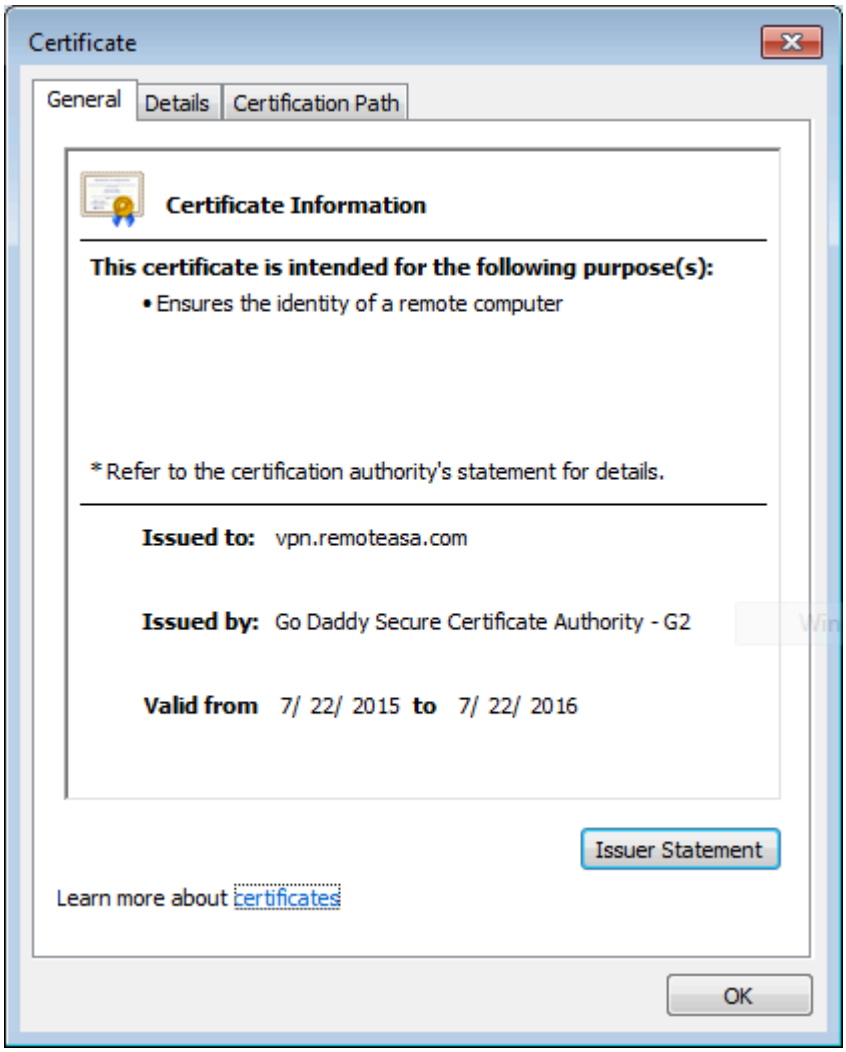


...(and the rest of the Sub CA certificates till the Root CA)
```

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 utilisé afin de demander le certificat (par exemple, Interface WebVPN)
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.

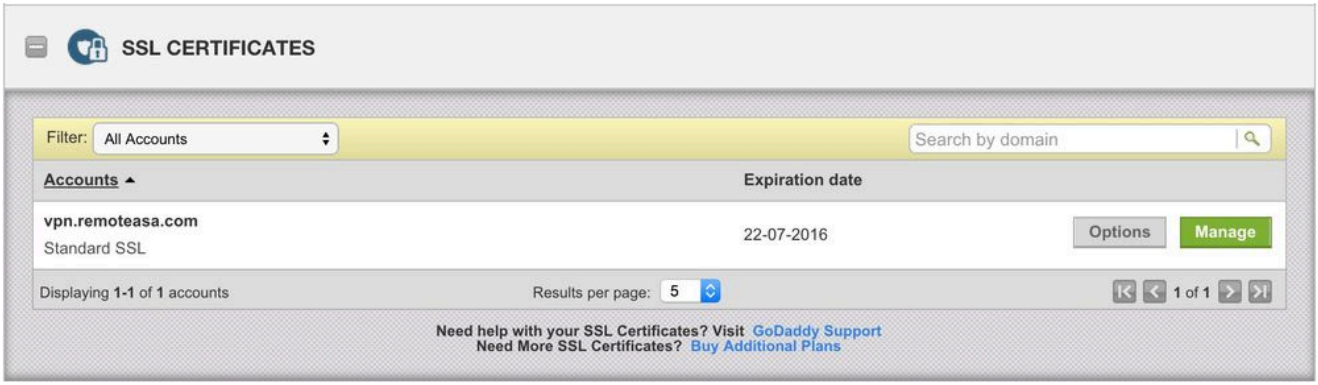


Renouveler le certificat SSL sur l'ASA

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.

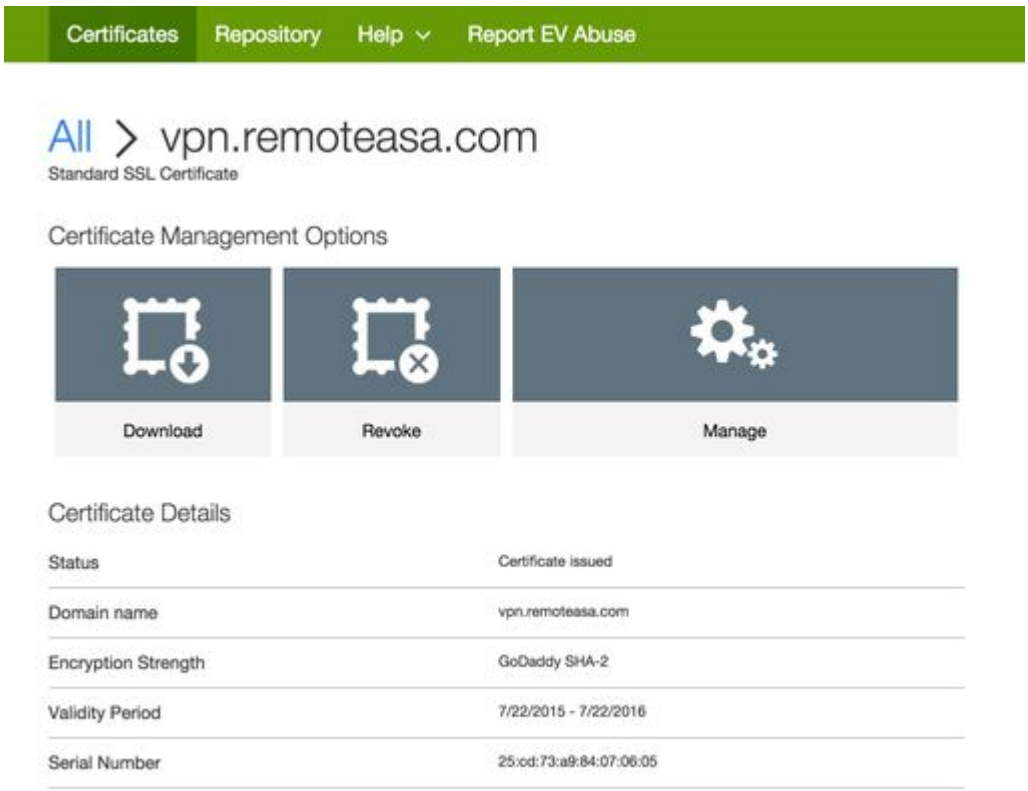
   Accédez au compte GoDaddy et cliquez sur Manage sous SSL Certificates.



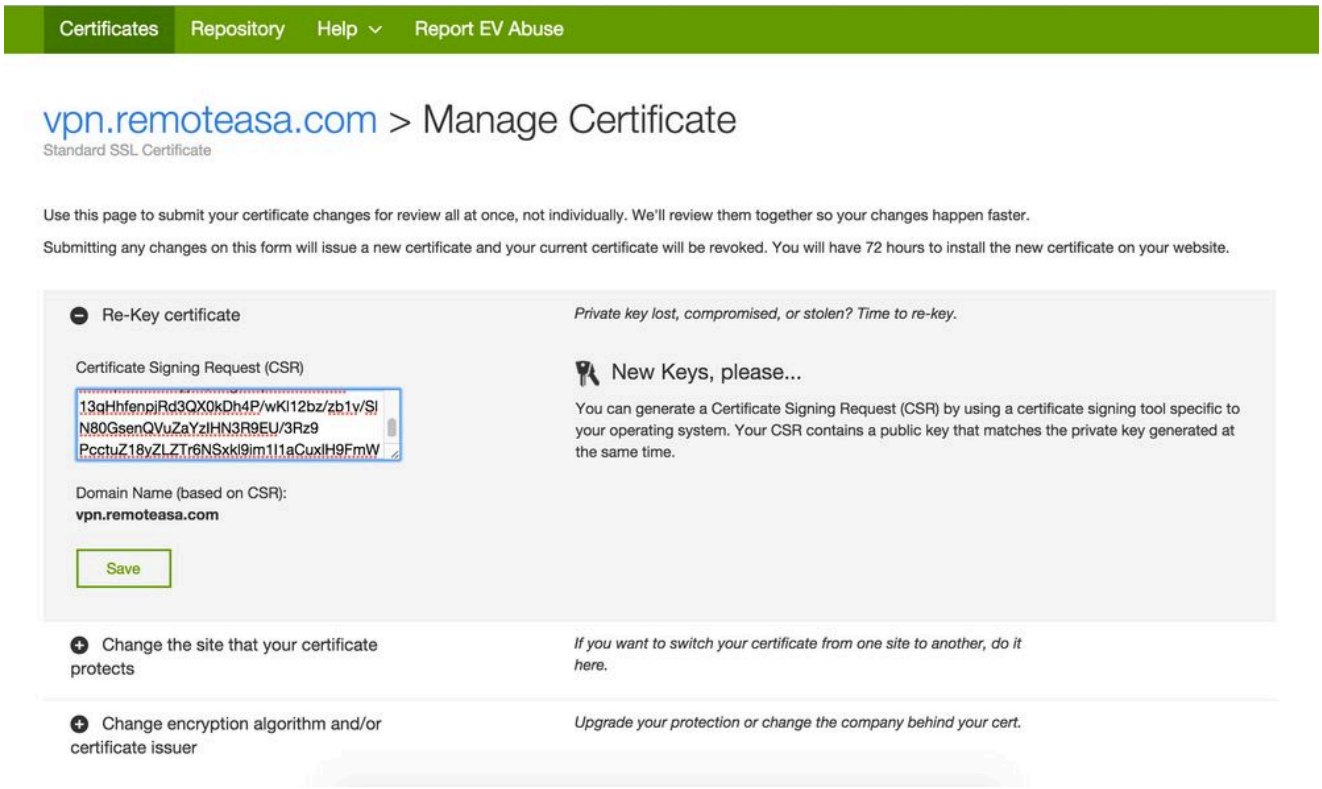
Cliquez sur Afficher l'état pour le nom de domaine requis.



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



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



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.

Foire 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.

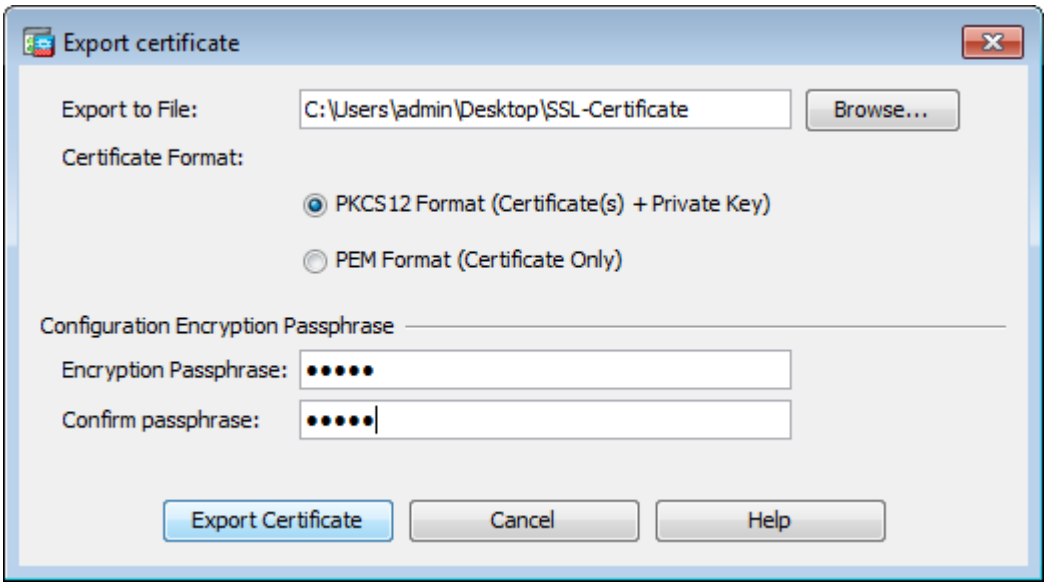
Utilisez cette commande afin d'exporter le certificat via la CLI à partir de l'ASA d'origine :

<#root>

```
ASA(config)#
```

crypto ca export <trust-point-name> pkcs12 <passphrase>

Configuration ASDM :



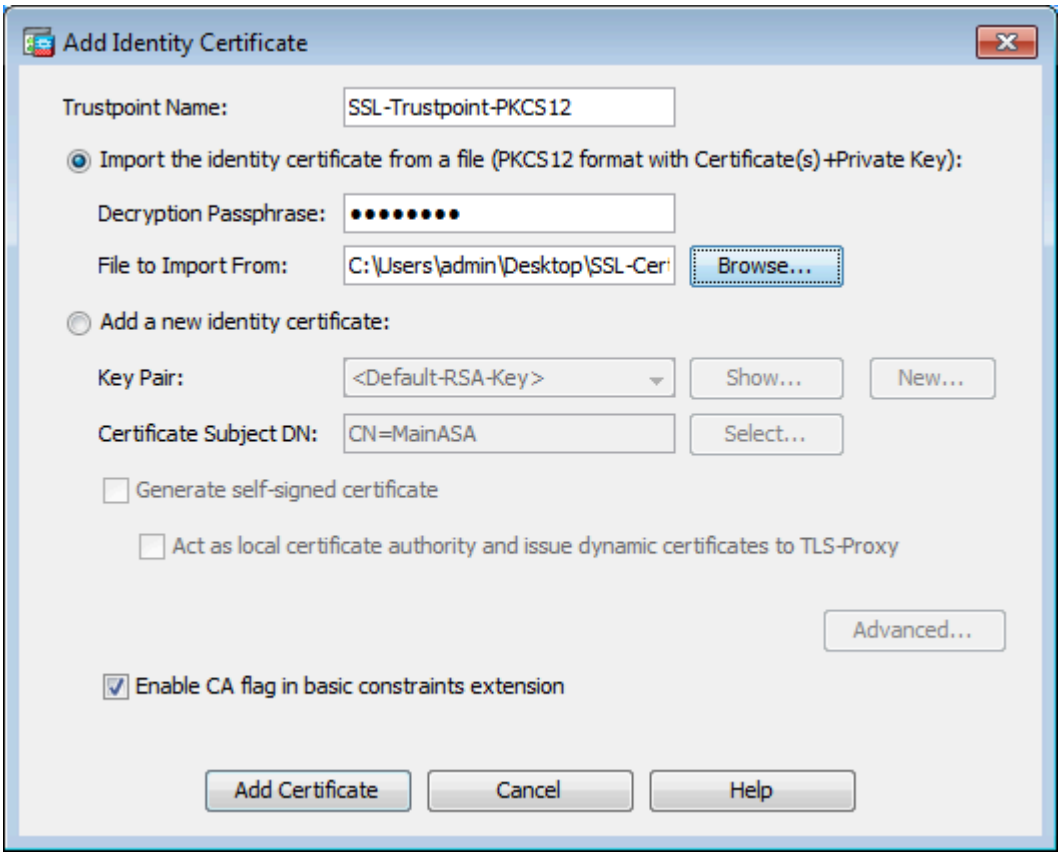
Utilisez cette commande afin d'importer le certificat via CLI vers l'ASA cible :

<#root>

```
ASA(config)#
```

crypto ca import <trust-point-name> pkcs12 <passphrase>

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 de l'ID de bogue Cisco CSCso70867. Dans ce cas, il y a

deux options pour générer le CSR

1. 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.
2. 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

Commandes de dépannage

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

Dans les versions logicielles plus récentes, une seule commande debug doit être utilisée :

debug crypto ca 14

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 tlsv1.2 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, naviguez**Configuration** > **Remote Access VPN** > **Advanced**,vers et**SSL Settings**.choisissezSous la section Encryption, sélectionnez tlsv1.2 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 fournit des informations plus détaillées.

Annexe B : Utiliser OpenSSL pour générer un certificat PKCS12 à partir d'un certificat d'identité, d'un certificat CA 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 requis pour créer le certificat PKCS12.

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

Annexe C : Considérations relatives à la sécurité des certificats CA approuvés

Risques et recommandations liés à l'authentification des certificats

Comportement par défaut de validation de point de confiance-utilisation

Lorsqu'un certificat d'autorité de certification approuvée est installé, avec **crypto ca trustpoint authenticate**,elle peut être utilisé pour authentifier différents types de connexions VPN à l'aide de l'authentification de certificat. Elle est contrôlée par la commande **validation-usage** trustpoint. Les types d'utilisation de validation sont :

- ipsec-client: Valide les connexions client IPsec.
- ssl-client: Valide les connexions client SSL.
- ssl-server: Valide les certificats de serveur SSL.

Par défaut, la commande permet la validation pour ipsec-client et ssl-client.

Risques de configuration par défaut

- Tout certificat d'autorité de certification installé en tant que certificat approuvé peut être utilisé par défaut pour authentifier les certificats d'identité client entrants pour tout groupe de tunnels utilisant l'authentification de certificat.
- Ce paramètre par défaut peut constituer un risque de sécurité si vous ne le connaissez pas.

Action recommandée

Désactivez l'utilisation de validation pour les points de confiance non intentionnels. Si un certificat d'autorité de certification n'est pas destiné à authentifier des homologues ou des utilisateurs VPN, désactivez la validation-utilisation pour ce point de confiance.

Exemple de configuration :

```
trustpoint public-root-ca
    no validation-usage
```

Autorisation Risques et recommandations

Par défaut, un certificat CA approuvé peut être utilisé pour authentifier l'homologue ou l'utilisateur VPN se connectant à n'importe quel groupe de tunnels. Une autorisation appropriée doit être conçue.

Action recommandée

Utilisez des mappages de certificats et des mappages de groupes de tunnels pour vous assurer que seuls les certificats autorisés sont utilisés pour des groupes de tunnels spécifiques. Définissez une règle de mappage de groupe de tunnels par défaut, qui pointe vers un groupe de tunnels sans accès pour limiter les accès non autorisés.

Exemple de configuration

L'authentification de certificat est uniquement autorisée pour :

- Machines avec certificat émis par cn=example.com et ayant OU=machines dans l'objet de certificat.
- Utilisateurs avec certificat émis par cn=example.com et ayant OU=users dans l'objet du certificat.

Les utilisateurs possédant d'autres certificats sont assignés à no_access tunnel-group par défaut, en raison de la **tunnel-group-map default-group no_access** commande. Les règles de mappage de certificat ont la priorité sur group-url grâce à la **tunnel-group-map enable rules** commande. Connaître group-url n'aide pas à contourner les règles de mappage de certificat.

```
tunnel-group mgmt-tunnel type remote-access
tunnel-group mgmt-tunnel general-attributes
address-pool vpn_pool
default-group-policy mgmt-tunnel
tunnel-group mgmt-tunnel webvpn-attributes
authentication certificate
group-url https://ftd.example.com/mgmt enable
!
tunnel-group users_access type remote-access
tunnel-group usets_access general-attributes
default-group-policy user_access_gp
address-pool vpn_pool
tunnel-group users_access webvpn-attributes
authentication certificate
group-url https://ftd.example.com/users enable
!
tunnel-group no_access type remote-access
tunnel-group no_access general-attributes
default-group-policy no_access_gp
address-pool vpn_pool
tunnel-group no_access webvpn-attributes
authentication certificate
!
group-policy no_access_gp internal
group-policy no_access_gp attributes
banner value NO ACCESS GROUP POLICY
(...)
vpn-simultaneous-logins 0
!
crypto ca certificate map mgmt_tunnel 10
issuer-name attr cn eq example.com
subject-name attr ou eq machines
crypto ca certificate map users 10
issuer-name attr cn eq example.com
subject-name attr ou eq users
!
webvpn
(...)
certificate-group-map mgmt_tunnel 10 mgmt-tunnel
certificate-group-map no-access 10 users_access
!
tunnel-group-map enable rules
tunnel-group-map default-group no_access
```

Ressources supplémentaires

Pour obtenir des instructions de configuration plus détaillées, reportez-vous à la documentation Cisco suivante :

- Configuration de l'utilisation de la validation - Référence des commandes de la gamme Cisco Secure Firewall ASA, commandes T - Z
- Configuration du plan de certificat - Référence des commandes de la gamme Cisco Secure Firewall ASA, commandes T - Z

- Configuration de la carte de groupe de tunnels - Référence des commandes de la gamme Cisco Secure Firewall ASA, commandes T - Z
- Configuration de l'activation de la carte de groupe de tunnels - Référence des commandes de la gamme Cisco Secure Firewall ASA, commandes T - Z

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.