Installer et renouveler des certificats sur ASA géré par ASDM

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Informations générales
Demander et installer un nouveau certificat d'identité avec ASDM
Demander et installer un nouveau certificat d'identité avec une demande de signature de certificat (CSR)
Générer un CSR avec ASDM
Créer un point de confiance avec un nom spécifique
(Facultatif) Créer une nouvelle paire de clés
Choisissez le nom de la paire de clés
Configurer l'objet du certificat et le nom de domaine complet (FQDN)
Générer et enregistrer le CSR
Installer le certificat d'identité au format PEM avec ASDM
Installer le certificat AC qui a signé le CSR
Installer le certificat d'identité
Lier le nouveau certificat à l'interface avec ASDM
Installer un certificat d'identité reçu au format PKCS12 avec ASDM
Installer les certificats d'identité et d'autorité de certification à partir d'un fichier PKCS12
Lier le nouveau certificat à l'interface avec ASDM
Renouvellement du certificat
Renouveler un certificat inscrit avec une demande de signature de certificat (CSR) avec ASDM
Générer un CSR avec ASDM
Créez un nouveau point de confiance avec un nom spécifique.
(Facultatif) Créer une nouvelle paire de clés
Sélectionnez le nom de la paire de clés
Configurer l'objet du certificat et le nom de domaine complet (FQDN)
Générer et enregistrer le CSR
Installer le certificat d'identité au format PEM avec ASDM
Installer le certificat AC qui a signé le CSR
Installer le certificat d'identité
Lier le nouveau certificat à l'interface avec ASDM
Renouveler un certificat inscrit avec un fichier PKCS12 avec ASDM
Installer le certificat d'identité renouvelé et les certificats CA à partir d'un fichier PKCS12
Lier le nouveau certificat à l'interface avec ASDM
Vérifier
Afficher les certificats installés via ASDM

Dépannage
Forum aux questions

Introduction

Ce document décrit comment demander, installer, approuver et renouveler certains types de certificats sur le logiciel Cisco ASA géré avec ASDM.

Conditions préalables

Exigences

- Avant de commencer, vérifiez que l'appliance ASA (Adaptive Security Appliance) 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. Consultez Informations connexes pour référence.
- Pour demander un certificat qui utilise une demande de signature de certificat (CSR), il est nécessaire d'avoir accès à une autorité de certification (CA) interne ou tierce de confiance. Les exemples de fournisseurs CA tiers incluent, sans s'y limiter, Entrust, Geotrust, GoDaddy, Thawte et VeriSign.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ASAv 9.18.1
- Pour la création de PKCS12, OpenSSL est utilisé.

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

Les types de certificats auxquels ce document s'adresse sont les suivants :

- certificats auto-signés
- certificats signés par une autorité de certification tierce ou une autorité de certification interne

Les protocoles d'authentification SSL (Secure Socket Layer), TLS (Transport Layer Security) et IKEv2 rfc7296 pour EAP exigent que le serveur SSL/TLS/IKEv2 fournisse au client un certificat de serveur pour que le client effectue l'authentification du serveur. Il est recommandé d'utiliser des autorités de certification tierces de confiance pour émettre des certificats SSL à l'ASA à cette fin.

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.

Demander et installer un nouveau certificat d'identité avec ASDM

Un certificat peut être demandé à une autorité de certification (CA) et installé sur un ASA de deux manières :

- Utiliser la demande de signature de certificat (CSR). Générez une paire de clés, demandez un certificat d'identité à l'autorité de certification avec un CSR, installez le certificat d'identité signé obtenu auprès de l'autorité de certification.
- Utilisez le fichier PKCS12 obtenu d'une autorité de certification ou exporté à partir d'un autre périphérique. Le fichier PKCS12 contient la paire de clés, le certificat d'identité, le ou les certificats d'autorité de certification.

Demander et installer un nouveau certificat d'identité avec une demande de signature de certificat (CSR)

Un CSR est créé sur le périphérique qui a besoin d'un certificat d'identité, utilisez une paire de clés créée sur le périphérique.

Un CSR contient :

- informations sur la demande de certificat - objet demandé et autres attributs, clé publique de la paire de clés,
- informations sur l'algorithme de signature,
- signature numérique des informations de demande de certificat, signée avec la clé privée de la paire de clés.

Le CSR est transmis à l'autorité de certification (CA), afin qu'elle le signe, dans un formulaire PKCS#10.

Le certificat signé est renvoyé par l'autorité de certification sous la forme d'un PEM.

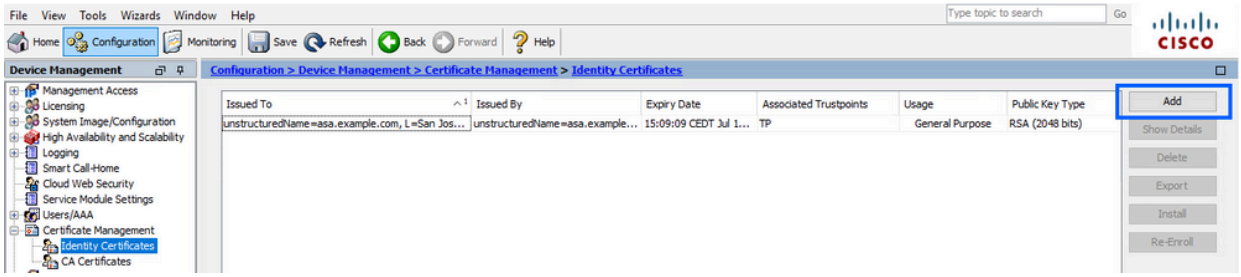
> Remarque : l'autorité de certification peut modifier les paramètres FQDN et Subject Name définis dans le point de confiance lorsqu'elle signe le CSR et crée un certificat d'identité signé.

Générer un CSR avec ASDM

1. Créer un point de confiance avec un nom spécifique

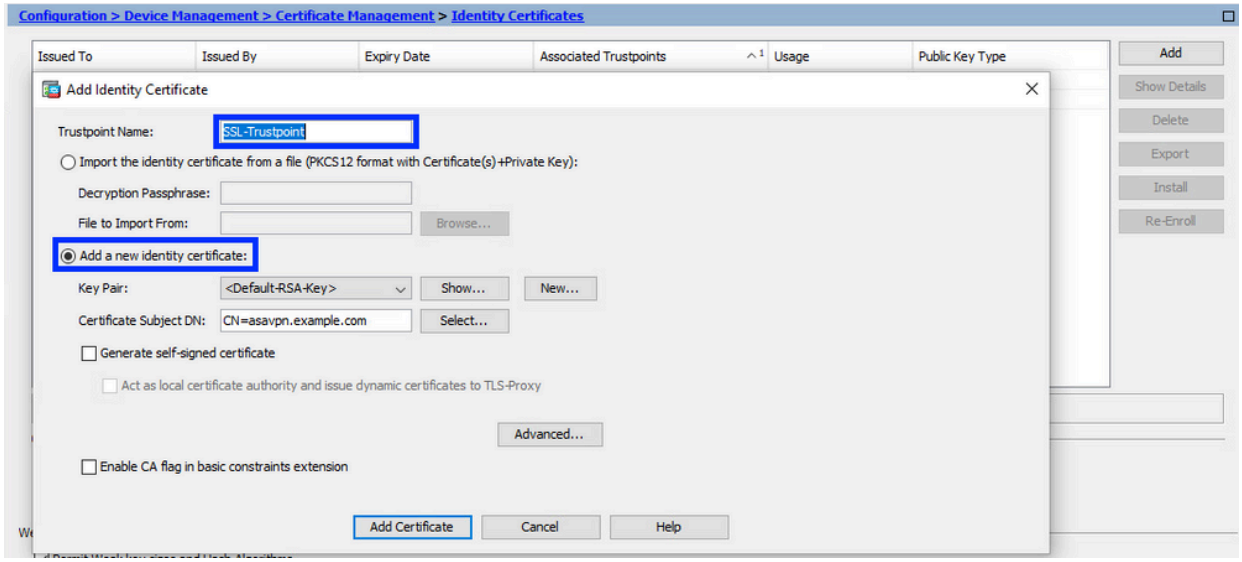
    a. Accédez à Configuration > Device Management > Certificate Management > Identity

Certificates.



b. Cliquez sur Add.

c. Définissez un nom de point de confiance.



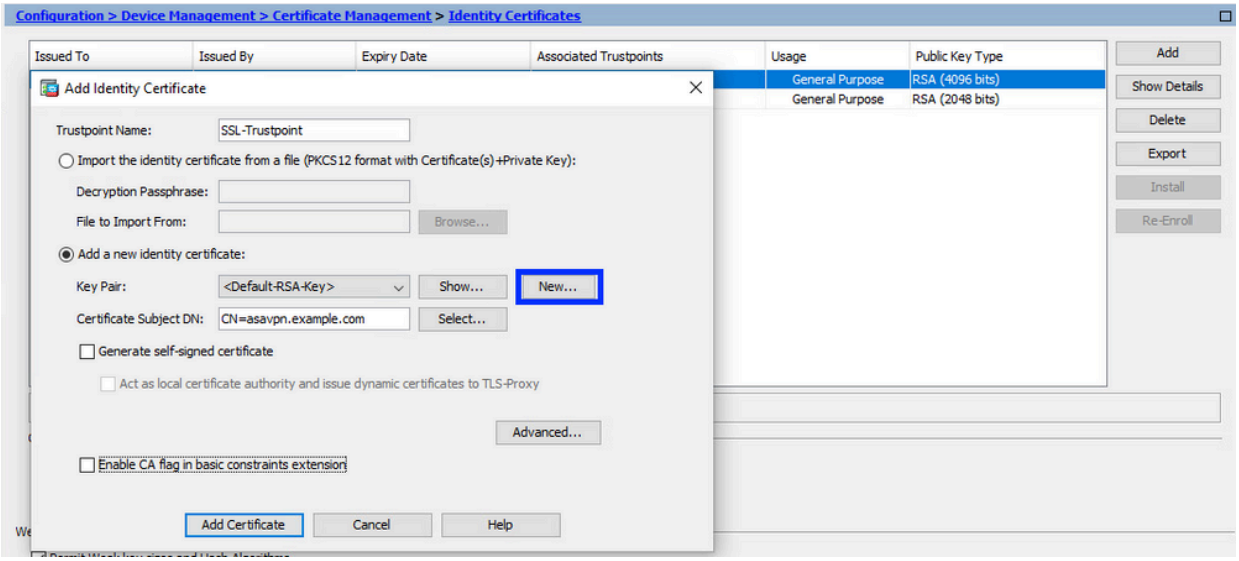
d. Cliquez sur la case d'option Add a new identity certificate.

2. (Facultatif) Créer une nouvelle paire de clés

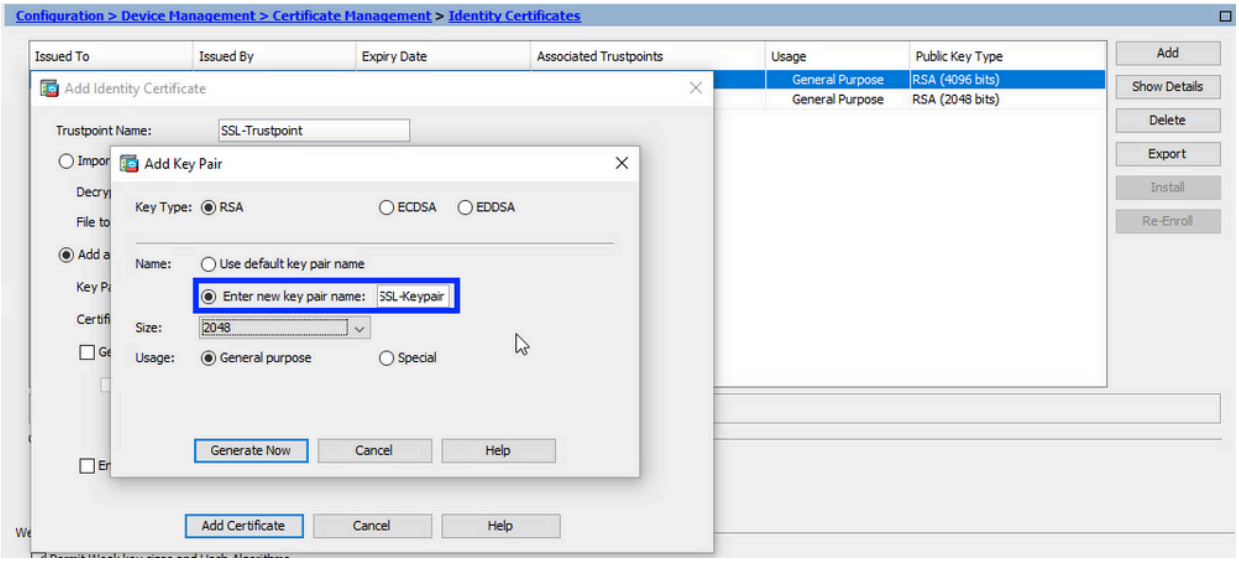
Remarque : par défaut, la clé RSA avec le nom Default-RSA-Key et une taille de 2048 est utilisée ; cependant, il est recommandé d'utiliser une paire de clés privée/publique unique pour chaque certificat d'identité.

---

a. Cliquez sur New pour générer une nouvelle paire de clés.

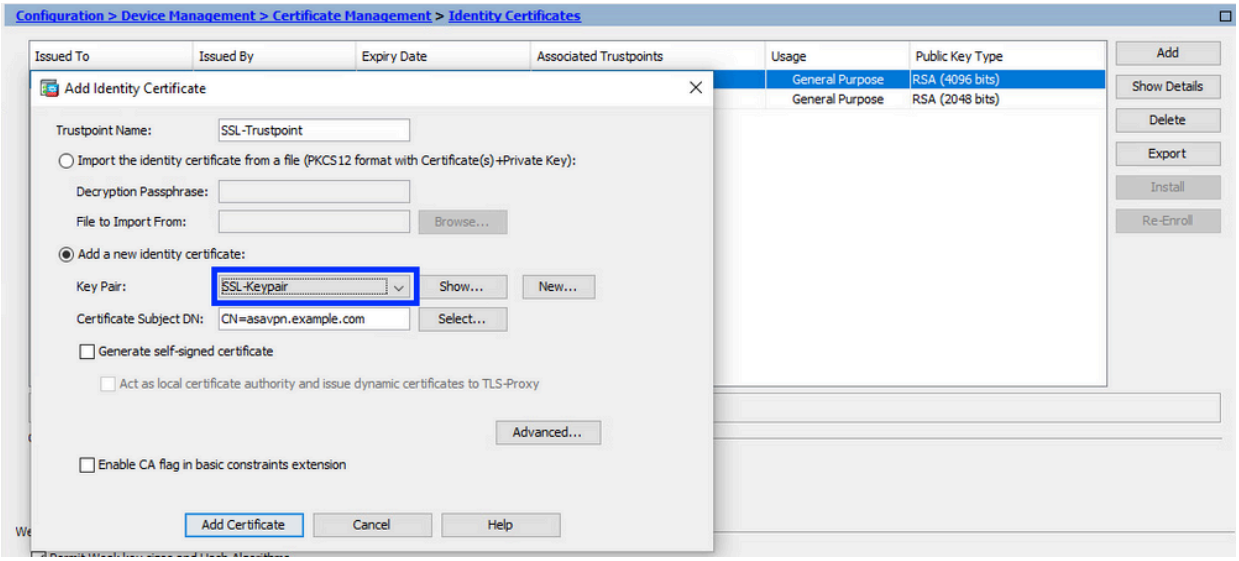


b. Choisissez l'option Enter new Key Pair name et entrez un nom pour la nouvelle paire de clés.
c. Sélectionnez le type de clé - RSA ou ECDSA.
d. Choisissez la Key Size ; pour RSA, choisissez General purpose for Usage.
e. Cliquez sur Generate Now. La paire de clés est maintenant créée.



3. Choisissez le nom de la paire de clés

Sélectionnez la paire de clés avec laquelle signer le CSR et à lier au nouveau certificat.

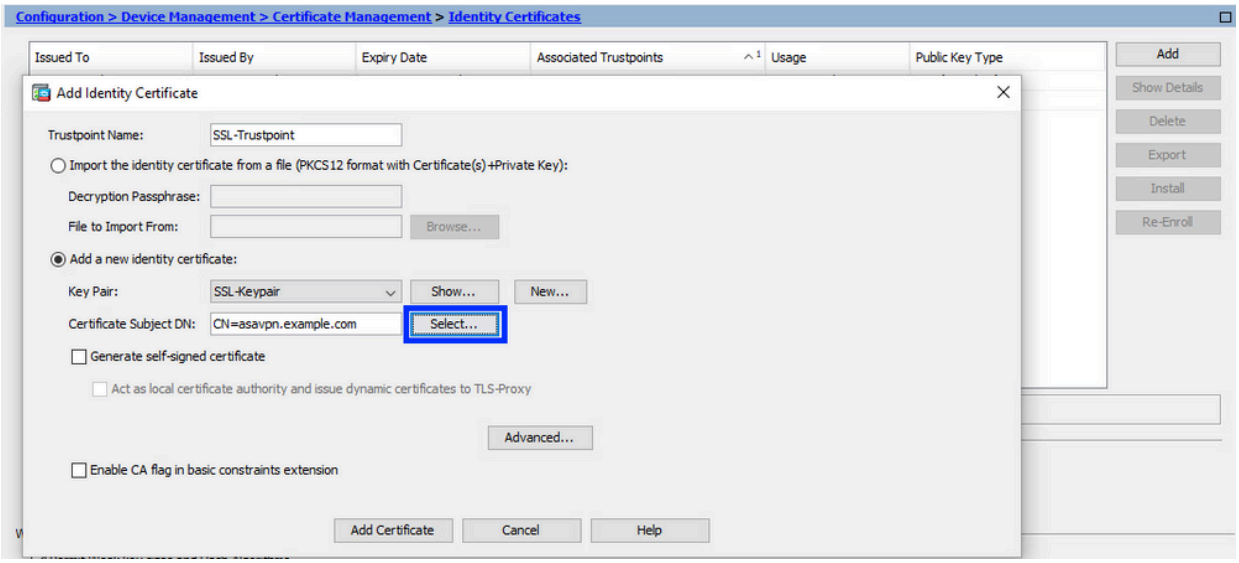


4. Configurer l'objet du certificat et le nom de domaine complet (FQDN)

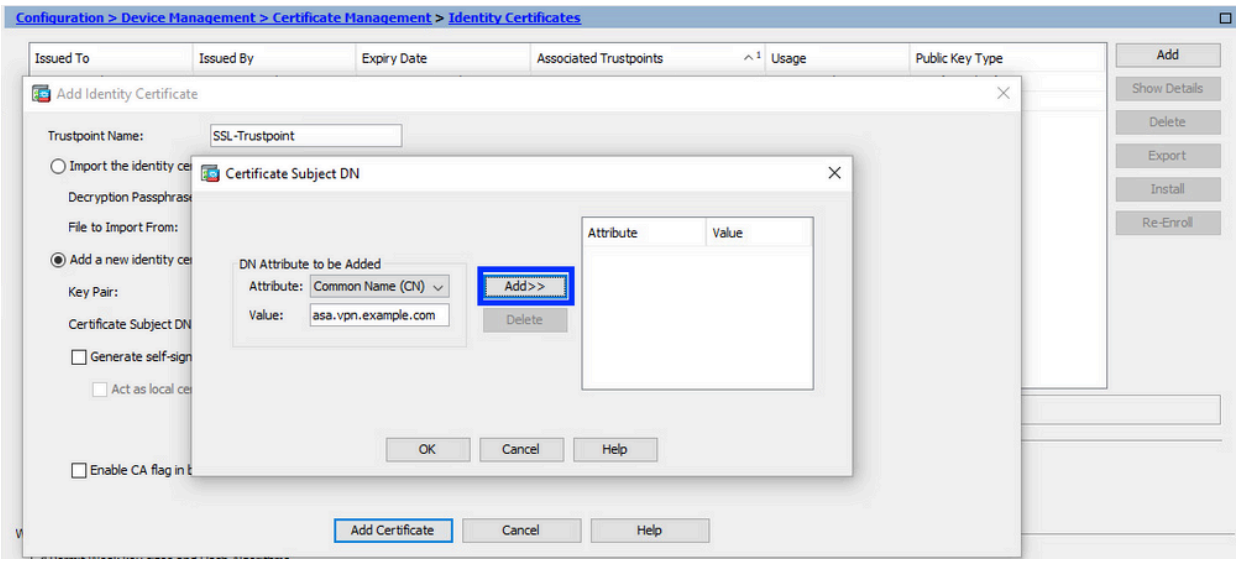
Attention : le paramètre FQDN doit correspondre au FQDN ou à l'adresse IP de l'interface ASA pour laquelle le certificat d'identité est utilisé. Ce paramètre définit l'extension de nom alternatif de sujet (SAN) demandée pour le certificat d'identité. L'extension SAN est utilisée par le client SSL/TLS/IKEv2 pour vérifier si le certificat correspond au nom de domaine complet auquel il se connecte.

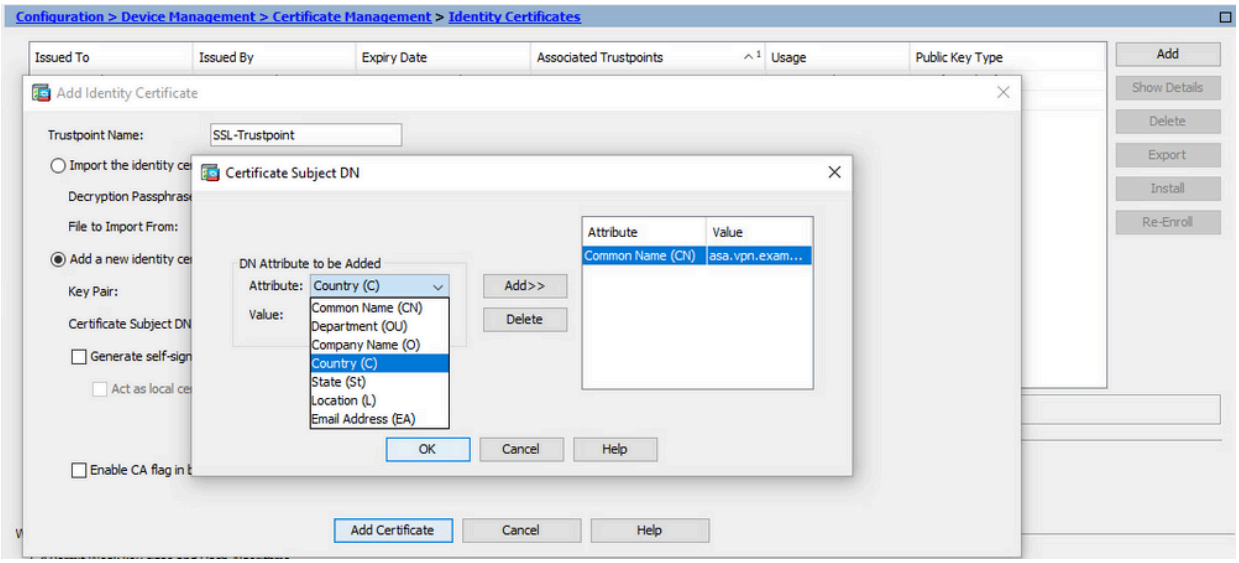
---

a. Cliquez sur Sélectionner.



b. Dans la fenêtre Certificate Subject DN, configurez les attributs de certificat - choisissez un attribut dans la liste déroulante, entrez la valeur, cliquez sur Add.



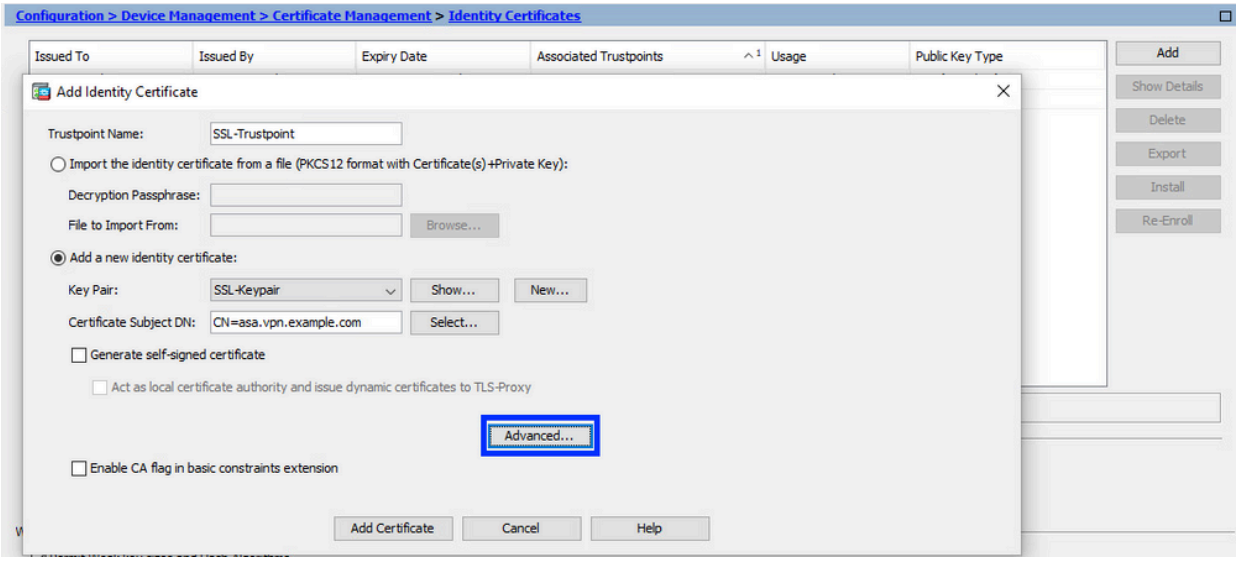


Attribut	Description
CN	Nom par lequel le pare-feu est accessible (généralement le nom de domaine complet, par exemple, vpn.example.com).
OU	Nom de votre service au sein de l'organisation
O	Le nom enregistré légalement de votre organisation/société
C	Code du pays (code de 2 lettres sans ponctuation)
ST	État dans lequel se trouve votre organisation.
L	Ville dans laquelle se trouve votre entreprise.
CE	Adresse électronique

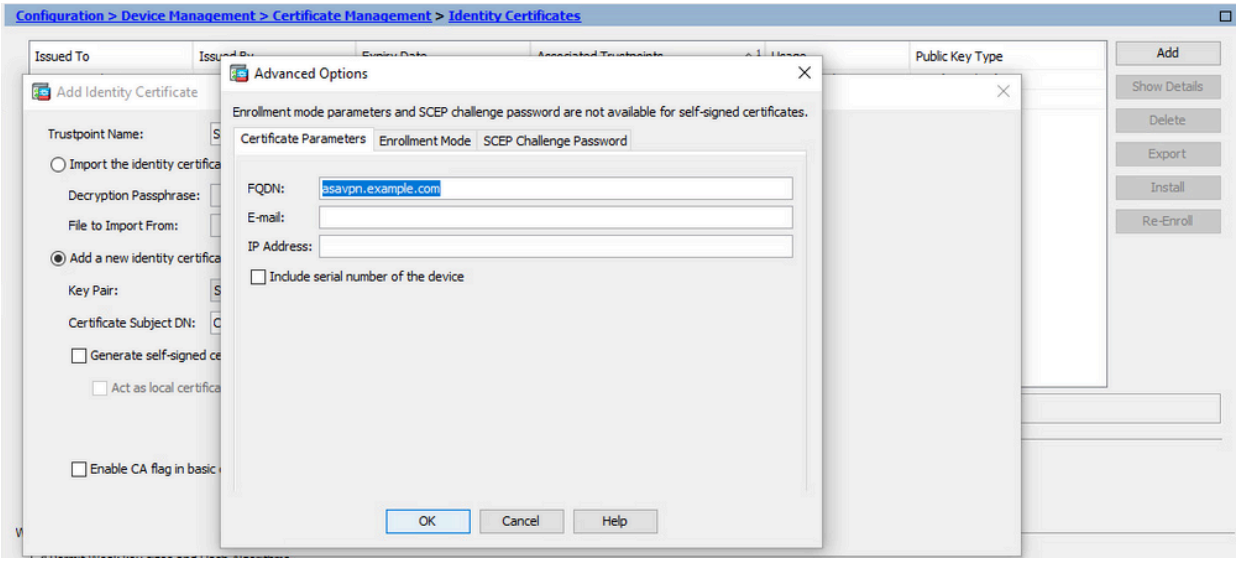
Remarque : aucune des valeurs des champs précédents ne peut dépasser une limite de 64 caractères. Une valeur plus longue peut entraîner des problèmes avec l'installation du certificat d'identité. En outre, il n'est pas nécessaire de définir tous les attributs DN.

Cliquez sur OK après avoir ajouté tous les attributs.

c. Configurez le nom de domaine complet du périphérique - cliquez sur Avancé.

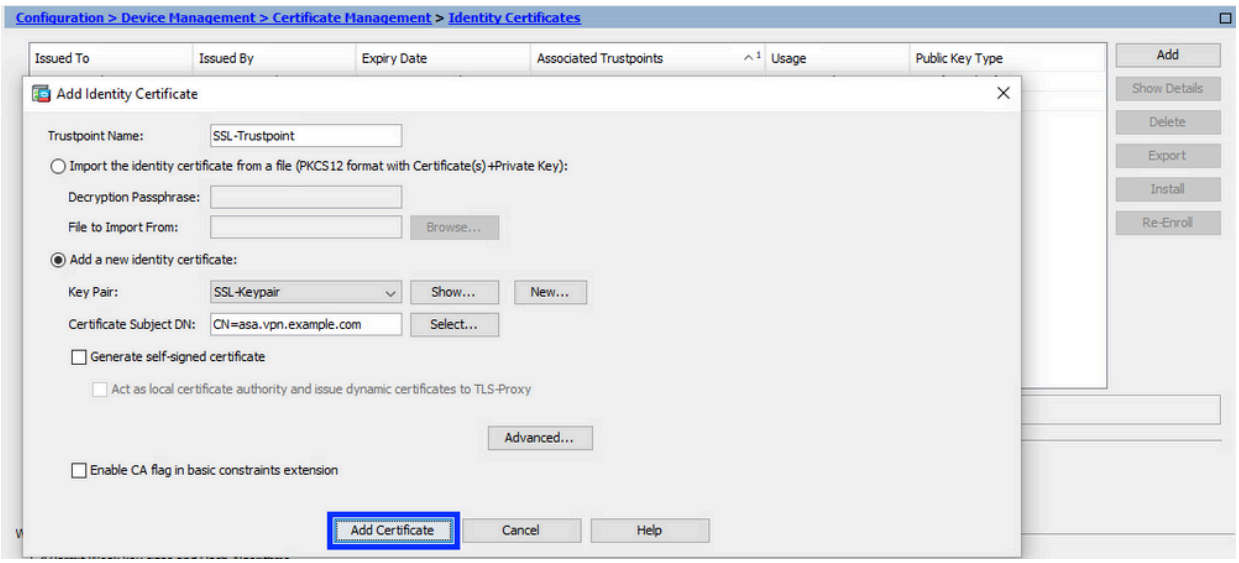


d. Dans le champ FQDN, saisissez le nom de domaine complet par lequel le périphérique est accessible à partir d'Internet. Click OK.

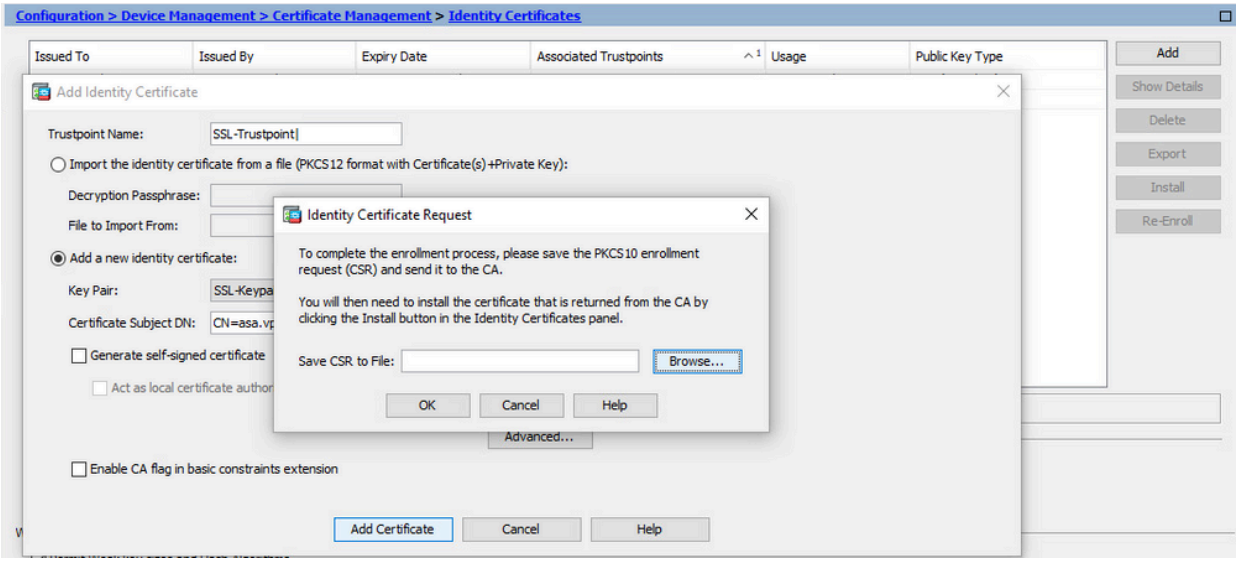


5. Générer et enregistrer le CSR

a. Cliquez sur Ajouter un certificat.



b. Une invite s'affiche afin d'enregistrer le CSR dans un fichier sur la machine locale.

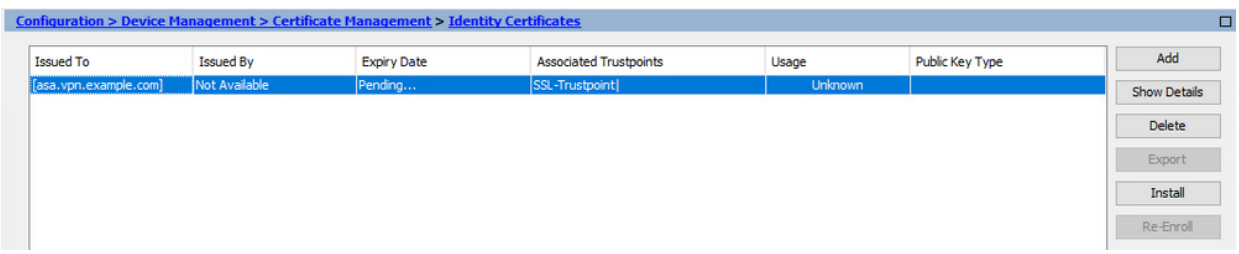


Cliquez sur Browse, choisissez un emplacement dans lequel enregistrer la CSR, puis enregistrez le fichier avec l'extension .txt.

> 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).

---

c. Le nouveau point de confiance est maintenant affiché à l'état En attente.

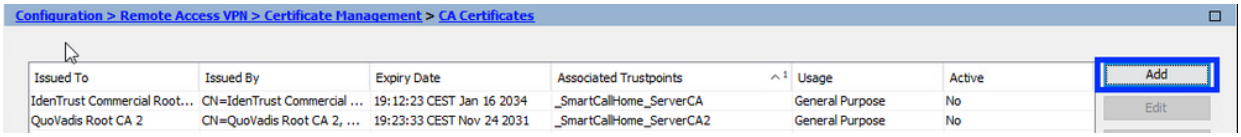


Installer le certificat d'identité au format PEM avec ASDM

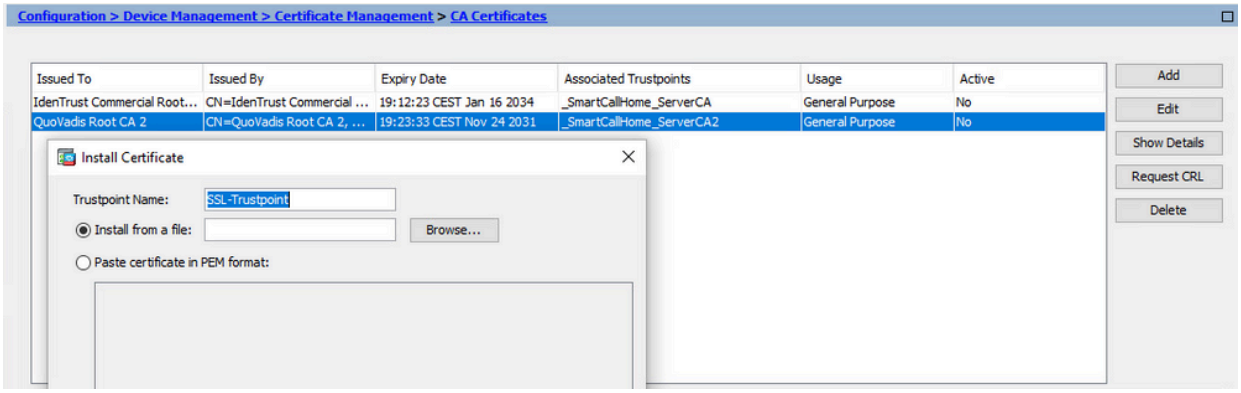
Les étapes d'installation supposent que l'autorité de certification a signé le CSR et fourni un certificat d'identité codé PEM (.pem, .cer, .crt) et un ensemble de certificats d'autorité de certification.

1. Installer le certificat AC qui a signé le CSR

   a. Accédez à Configuration > Device Management > Certificate Management > , et choisissez CA Certificates. Cliquez sur Add.



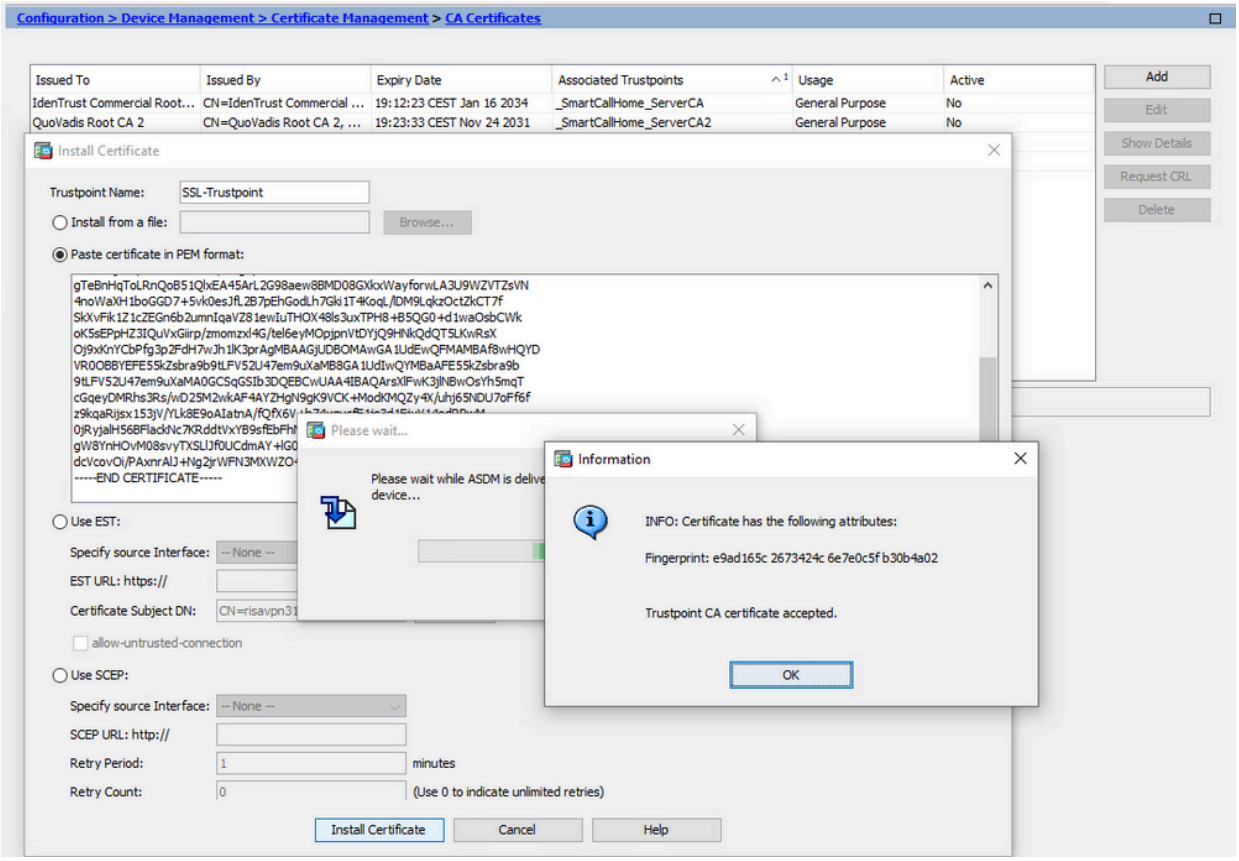
   b. Entrez le nom du point de confiance et sélectionnez Installer à partir du fichier, cliquez sur le bouton Parcourir, puis sélectionnez le certificat intermédiaire. Vous pouvez également coller le certificat CA codé PEM d'un fichier texte dans le champ texte.



Remarque : installez le certificat d'autorité de certification qui a signé le CSR et utilisez le même nom de point de confiance que le certificat d'identité. Les autres certificats d'autorité de certification situés plus haut dans la hiérarchie PKI peuvent être installés dans des points de confiance distincts.

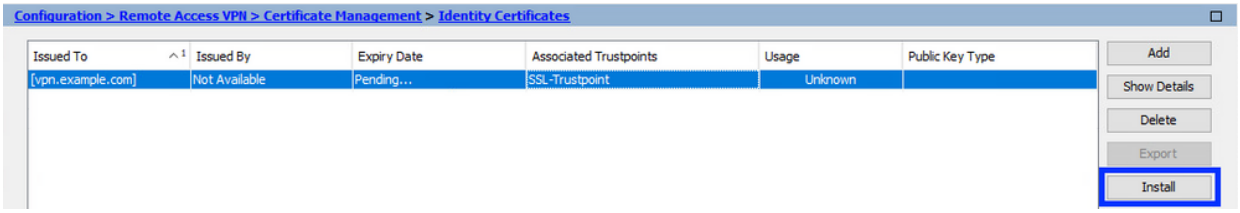
---

   c. Cliquez sur Install Certificate.



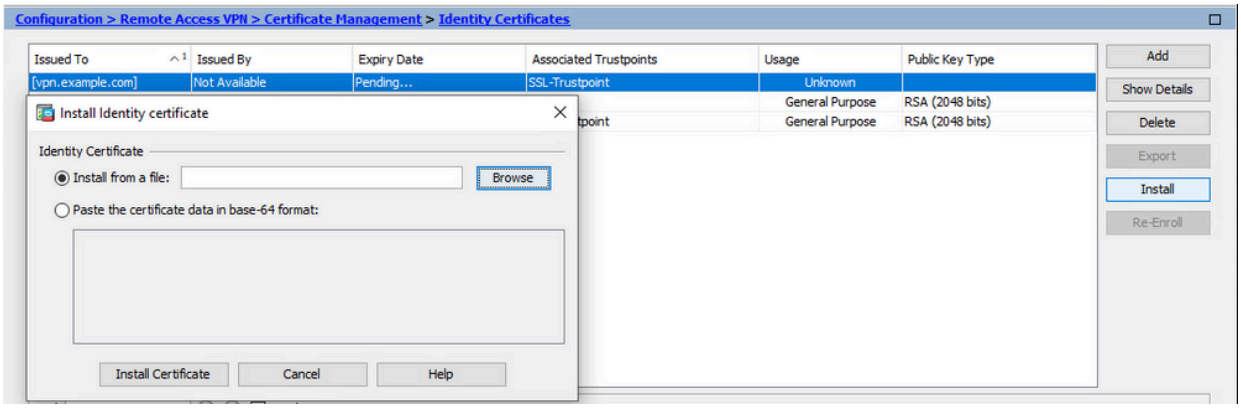
2. Installer le certificat d'identité

   a. Sélectionnez le certificat d'identité créé précédemment lors de la génération CSR. Cliquez sur Install.



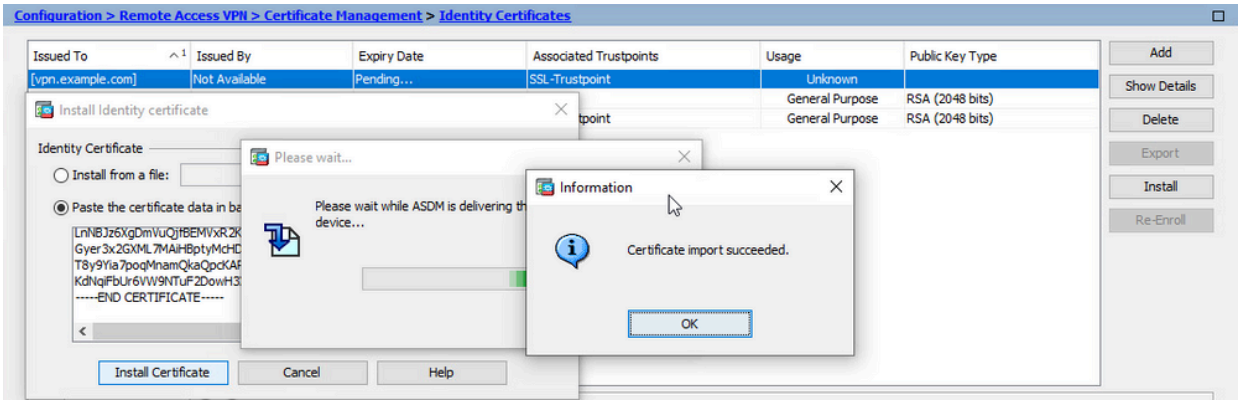
> Remarque : le champ Émis par peut avoir la valeur Non disponible et le champ Date d'expiration la valeur En attente.

   b. Choisissez un fichier qui contient le certificat d'identité codé PEM reçu de l'autorité de certification, ou ouvrez le certificat codé PEM dans un éditeur de texte et copiez et collez le certificat d'identité fourni par l'autorité de certification dans le champ de texte.



Remarque : le certificat d'identité peut être au format .pem, .cer, .crt à installer.

c. Cliquez sur Install Certificate.



3. Lier le nouveau certificat à l'interface avec ASDM

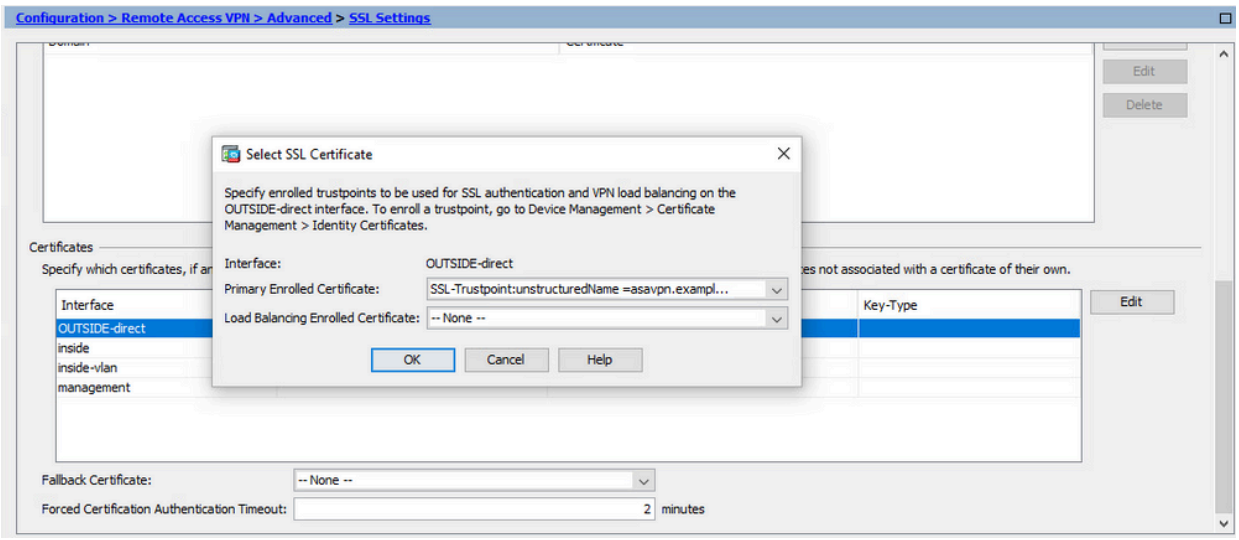
L'ASA doit être configuré pour utiliser le nouveau certificat d'identité pour les sessions WebVPN qui se terminent sur l'interface spécifiée.

a. Accédez à Configuration > Remote Access VPN > Advanced > SSL Settings.

b. Sous Certificates, choisissez l'interface utilisée pour terminer les sessions WebVPN. Dans cet exemple, l'interface externe est utilisée.

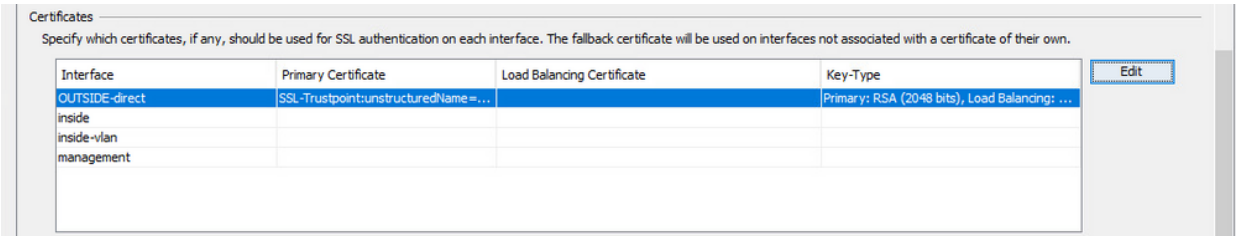
Cliquez sur Edit.

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



d. Click OK.

e. Cliquez sur Apply.



Le nouveau certificat d'identité est maintenant utilisé.

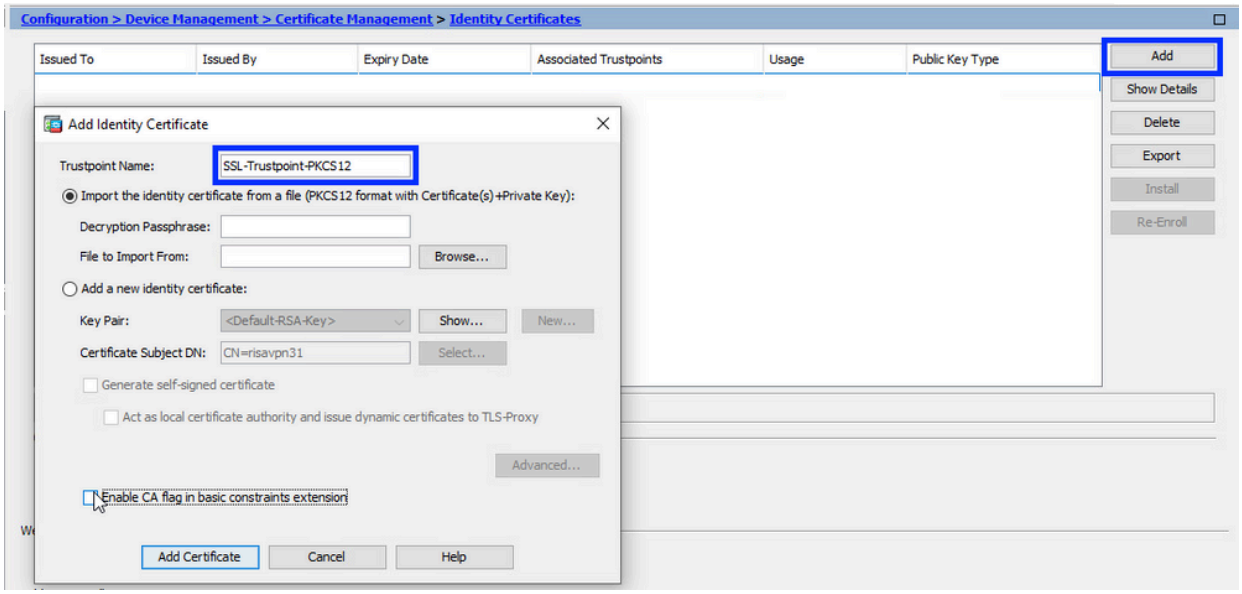
Installer un certificat d'identité reçu au format PKCS12 avec ASDM

Le fichier PKCS12 (format .p12 ou .pfx) contient un certificat d'identité, une paire de clés et un ou plusieurs certificats d'autorité de certification. Il est créé par l'autorité de certification, par exemple en cas de certificat générique, ou exporté à partir d'un autre périphérique. Il s'agit d'un fichier binaire qui ne peut pas être affiché avec l'éditeur de texte.

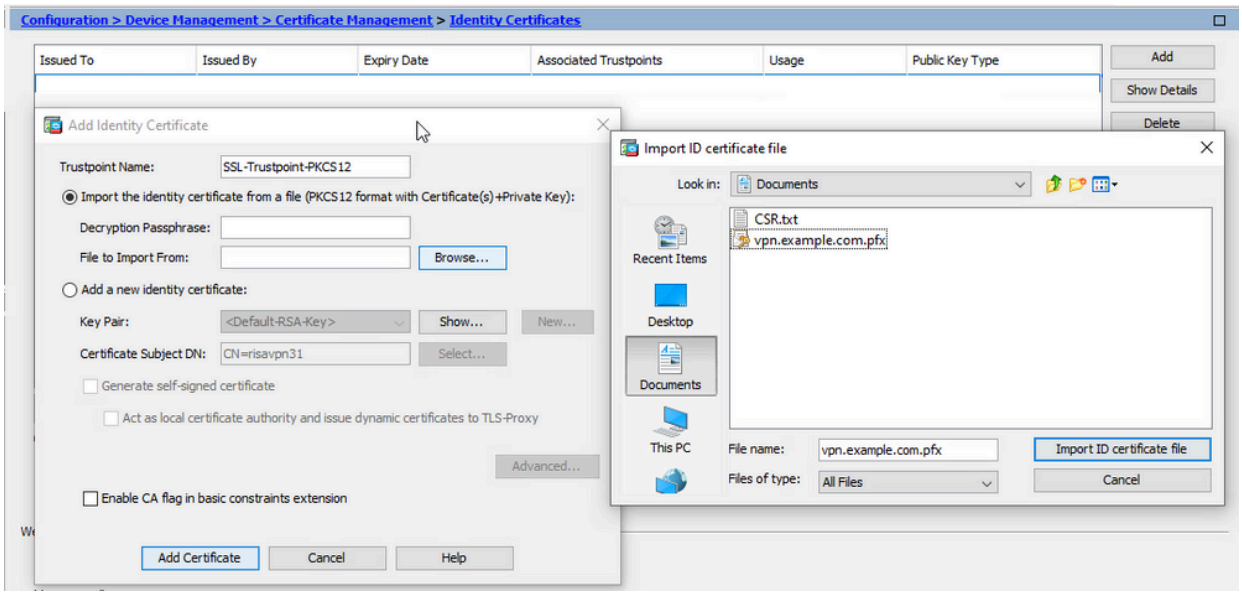
1. Installer les certificats d'identité et d'autorité de certification à partir d'un fichier PKCS12

   Le certificat d'identité, le ou les certificats d'autorité de certification et la paire de clés doivent être regroupés dans un fichier PKCS12 unique.

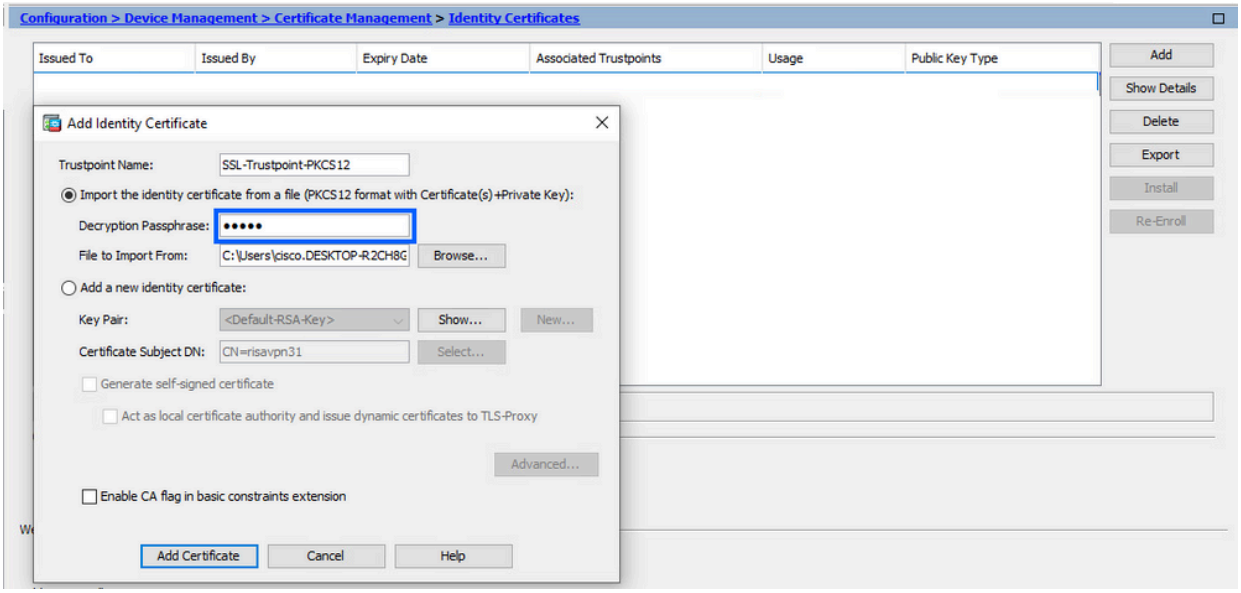
   a. Accédez à Configuration > Device Management > Certificate Management, et choisissez Identity Certificates.
   b. Cliquez sur Add.
   c. Spécifiez un nom de point de confiance.



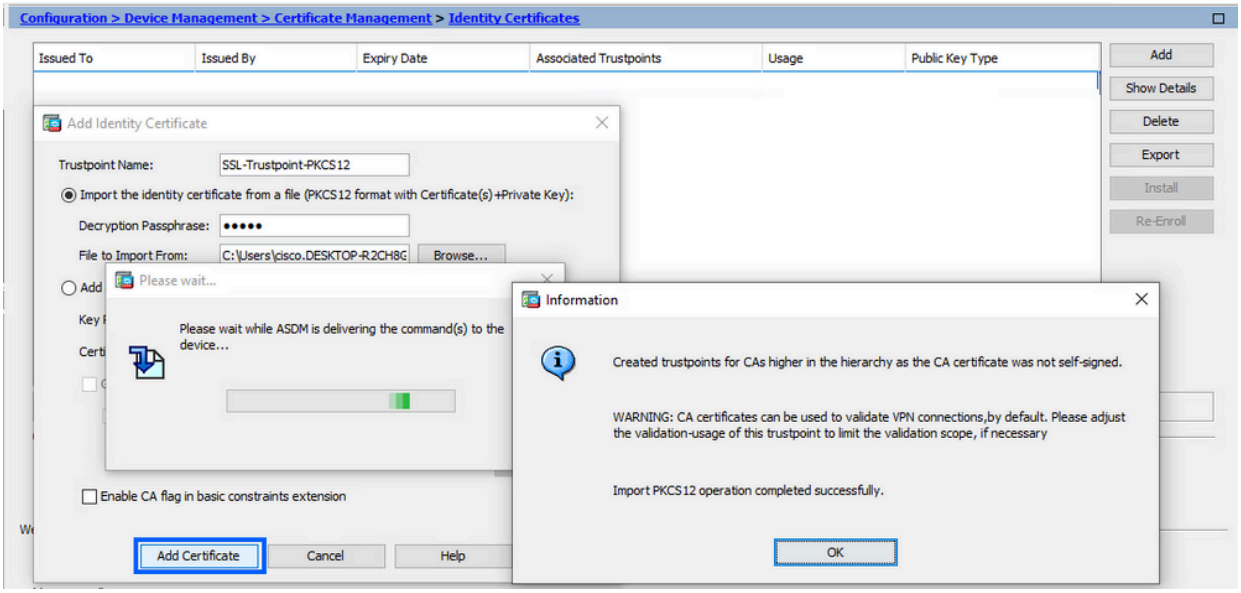
d. Activez la case d'option Importer le certificat d'identité à partir d'un fichier.



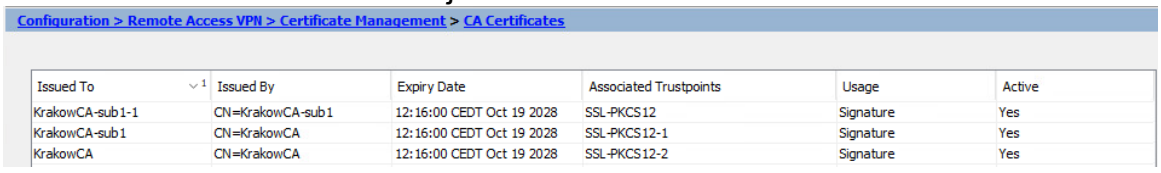
e. Entrez la phrase de passe utilisée pour créer le fichier PKCS12.



f. Cliquez sur Add Certificate.



Remarque : lorsque vous importez une chaîne de certificats PKCS12 avec CA, l'ASDM crée automatiquement les points de confiance CA en amont avec des noms avec le suffixe -number ajouté.



Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
KrakowCA-sub1-1	CN=KrakowCA-sub1	12:16:00 CEDT Oct 19 2028	SSL-PKCS12	Signature	Yes
KrakowCA-sub1	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-1	Signature	Yes
KrakowCA	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-2	Signature	Yes

2. Lier le nouveau certificat à l'interface avec ASDM

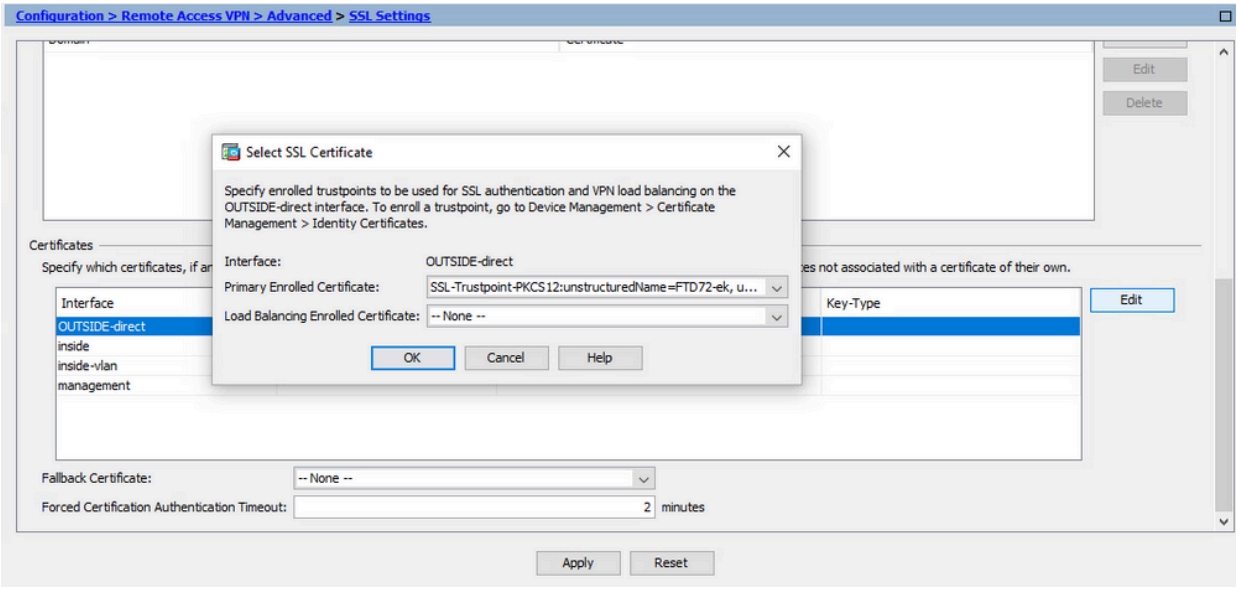
L'ASA doit être configuré pour utiliser le nouveau certificat d'identité pour les sessions WebVPN qui se terminent sur l'interface spécifiée.

a. Accédez à Configuration > Remote Access VPN > Advanced > SSL Settings.

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

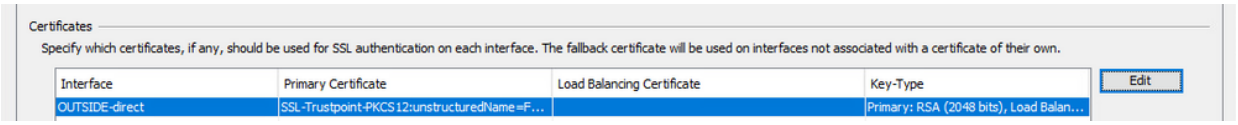
Cliquez sur Edit.

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



d. Click OK.

e. Cliquez sur Apply.



Le nouveau certificat d'identité est maintenant utilisé.

Renouvellement du certificat

Renouveler un certificat inscrit avec une demande de signature de certificat (CSR) avec ASDM

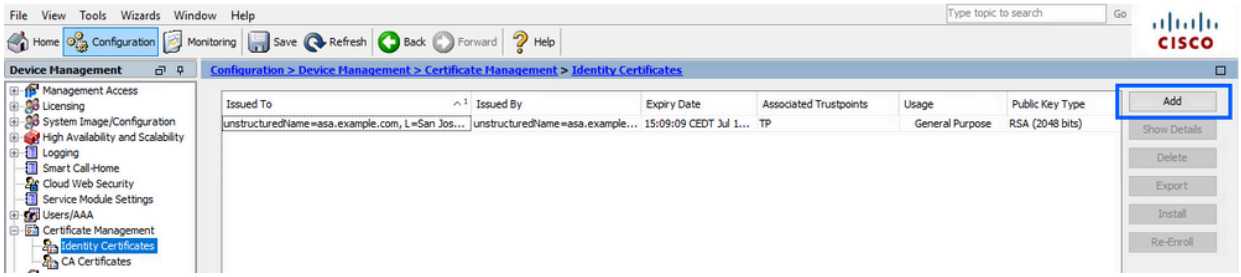
Le renouvellement de certificat du certificat inscrit CSR nécessite la création et l'inscription d'un nouveau point de confiance. Il doit avoir un nom différent (par exemple, ancien nom avec suffixe de l'année d'inscription). Il peut utiliser les mêmes paramètres et la même paire de clés que l'ancien certificat, ou peut utiliser des paramètres différents.

Générer un CSR avec ASDM

1. Créez un nouveau point de confiance avec un nom spécifique.

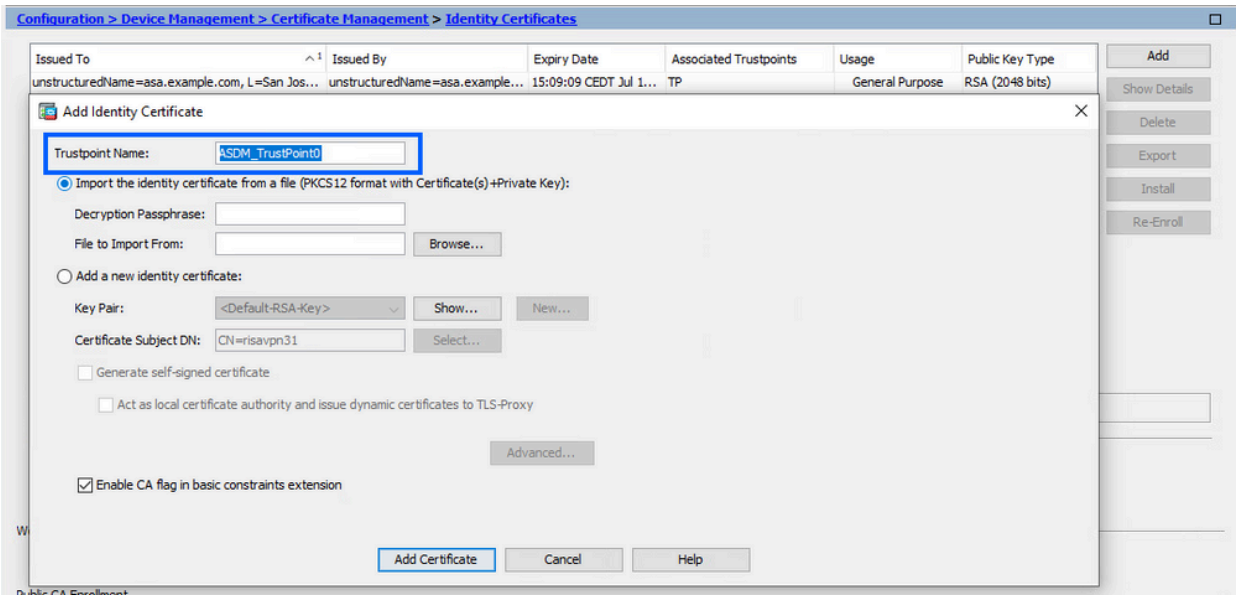
a. Accédez à Configuration > Device Management > Certificate Management > Identity

Certificates.



b. Cliquez sur Add.

c. Définissez un nom de point de confiance.



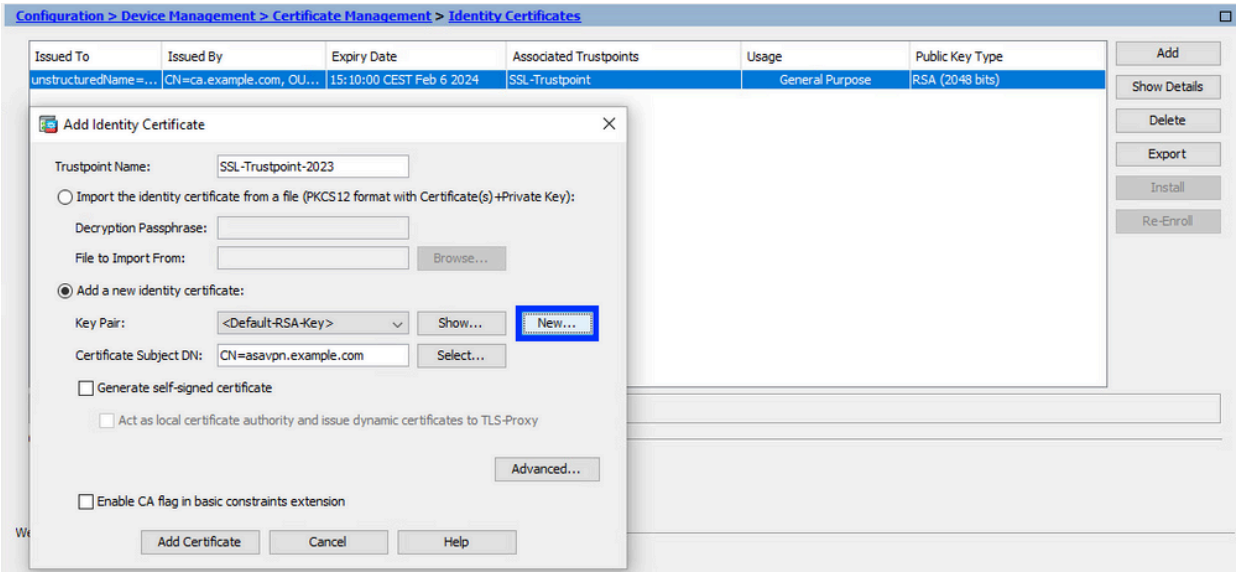
d. Cliquez sur la case d'option Add a new identity certificate.

2. (Facultatif) Créer une nouvelle paire de clés

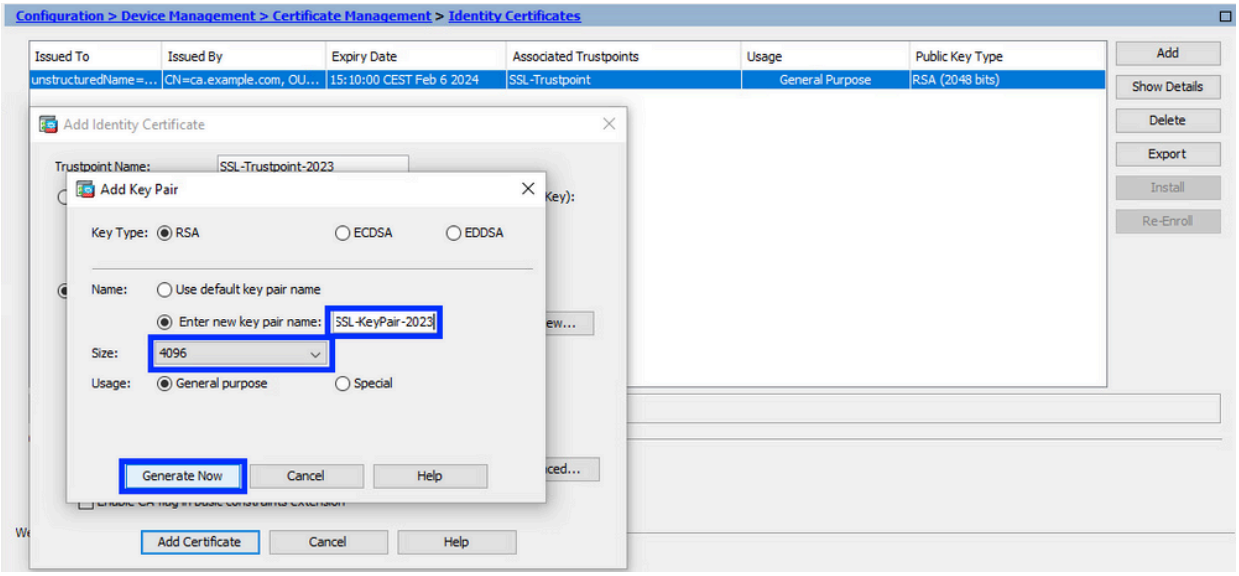
Remarque : par défaut, la clé RSA avec le nom Default-RSA-Key et une taille de 2048 est utilisée ; cependant, il est recommandé d'utiliser une paire de clés privée/publique unique pour chaque certificat d'identité.

---

a. Cliquez sur New pour générer une nouvelle paire de clés.

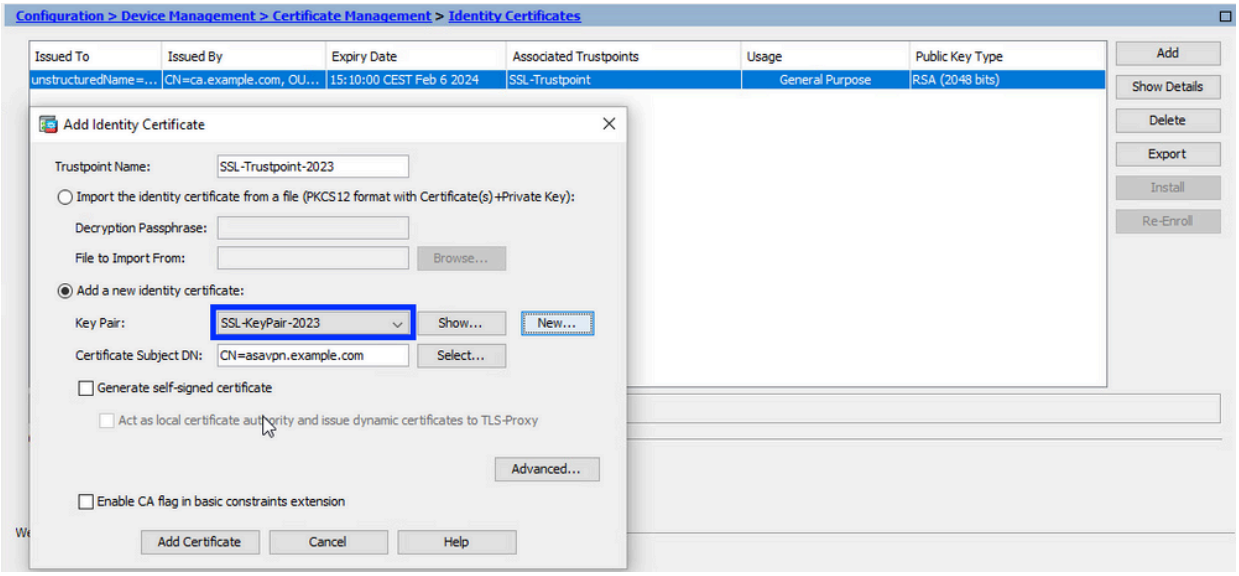


b. Choisissez l'option Saisir le nom de la nouvelle paire de clés et entrez un nom pour la nouvelle paire de clés.
c. Sélectionnez le type de clé : RSA ou ECDSA.
d. Choisissez la taille de clé ; pour RSA, choisissez Fonction générale pour Utilisation.
e. Cliquez sur Generate Now. La paire de clés est maintenant créée.



3. Sélectionnez le nom de la paire de clés

Sélectionnez la paire de clés avec laquelle signer le CSR et à lier au nouveau certificat.



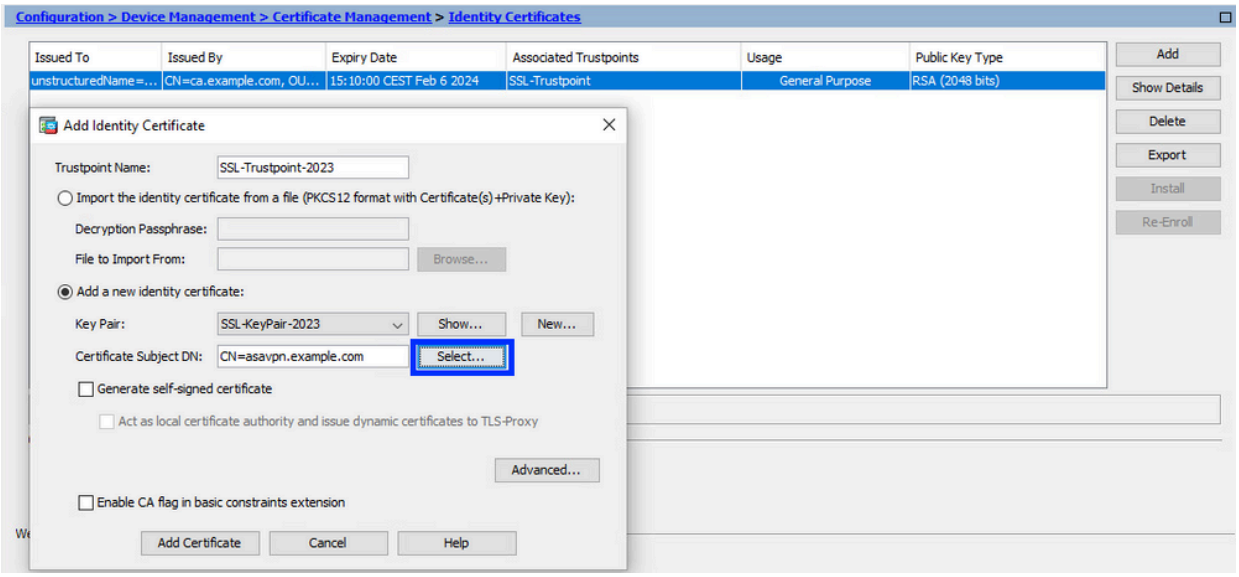
4. Configurer l'objet du certificat et le nom de domaine complet (FQDN)

Attention : le paramètre FQDN doit correspondre au nom de domaine complet ou à l'adresse IP de l'interface ASA pour laquelle le certificat est utilisé. Ce paramètre définit le nom alternatif du sujet (SAN) pour le certificat. Le champ SAN est utilisé par le client SSL/TLS/IKEv2 pour vérifier si le certificat correspond au nom de domaine complet auquel il est connecté.

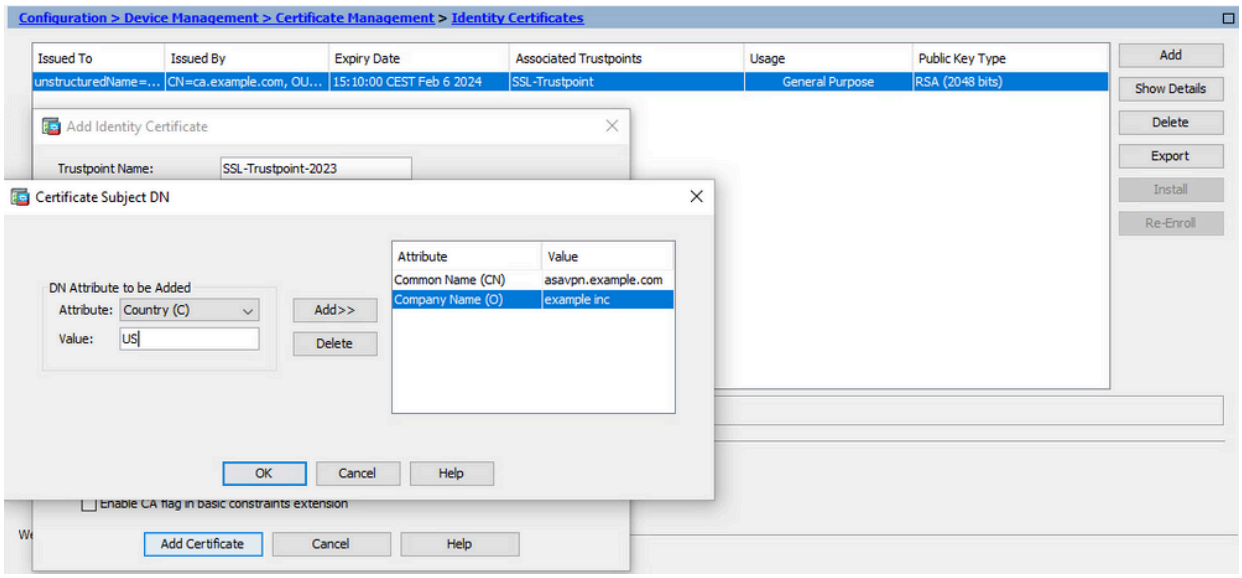
Remarque : l'autorité de certification peut modifier les paramètres FQDN et Subject Name définis dans le point de confiance lorsqu'elle signe le CSR et crée un certificat d'identité signé.

---

a. Cliquez sur Sélectionner.



b. Dans la fenêtre Certificate Subject DN, configurez les attributs du certificat - sélectionnez l'attribut dans la liste déroulante, entrez la valeur, cliquez sur Add.

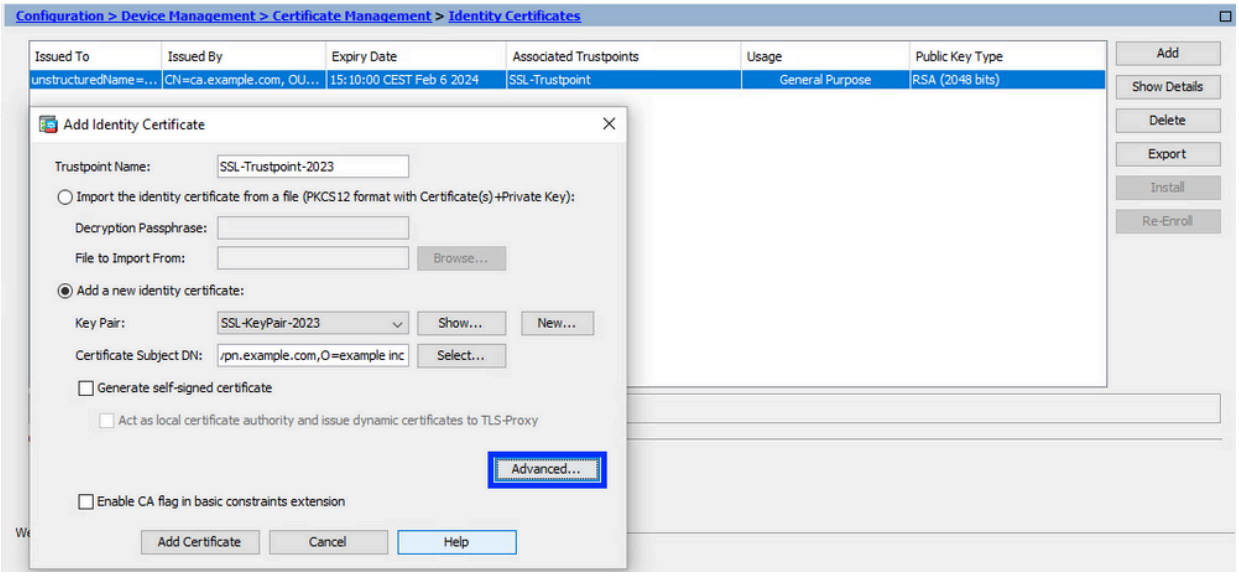


Attribut	Description
CN	Nom par lequel le pare-feu est accessible (généralement le nom de domaine complet, par exemple, vpn.example.com).
OU	Nom de votre service au sein de l'organisation
O	Le nom enregistré légalement de votre organisation/société
C	Code du pays (code de 2 lettres sans ponctuation)
ST	État dans lequel se trouve votre organisation.
L	Ville dans laquelle se trouve votre entreprise.
CE	Adresse électronique

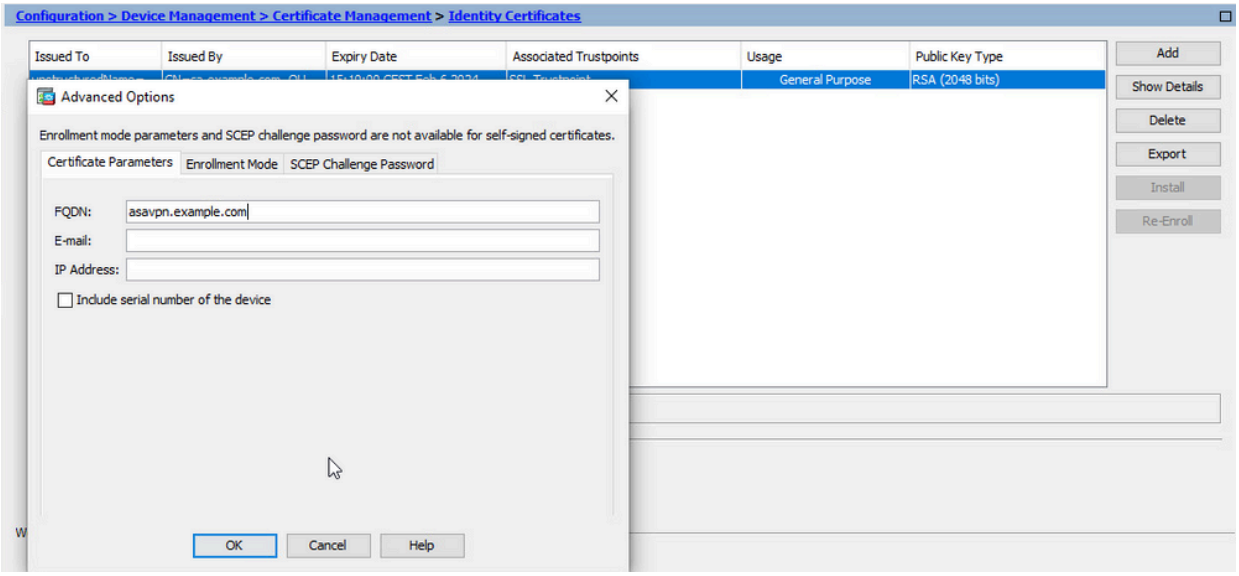
Remarque : aucun des champs précédents ne peut dépasser une limite de 64 caractères. Une valeur plus longue peut entraîner des problèmes avec l'installation du certificat d'identité. En outre, il n'est pas nécessaire de définir tous les attributs DN.

Cliquez sur OK après avoir ajouté tous les attributs.

c. Pour configurer le nom de domaine complet du périphérique, cliquez sur Avancé.

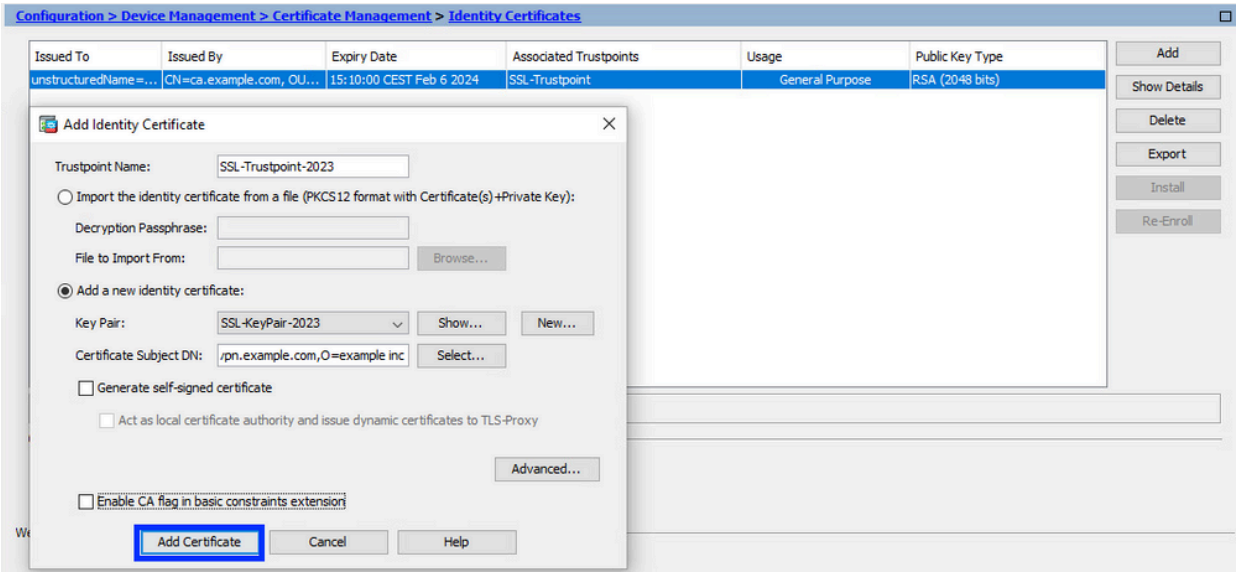


d. Dans le champ FQDN, saisissez le nom de domaine complet par lequel le périphérique est accessible à partir d'Internet. Click OK.

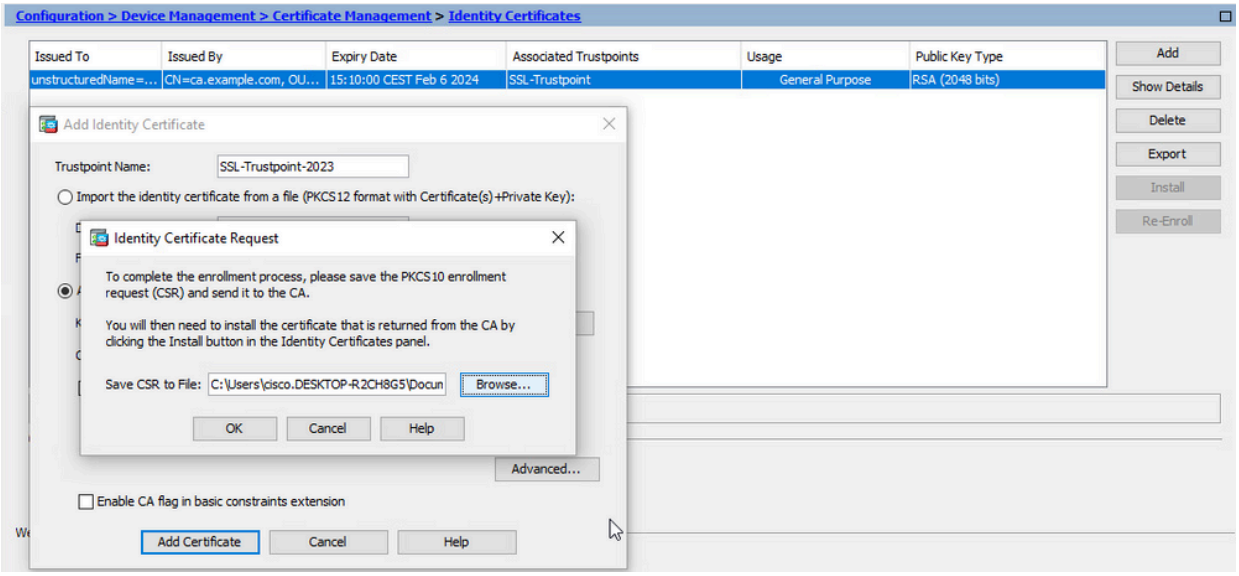


5. Générer et enregistrer le CSR

a. Cliquez sur Ajouter un certificat.



b. Une invite s'affiche pour enregistrer le CSR dans un fichier sur l'ordinateur local.

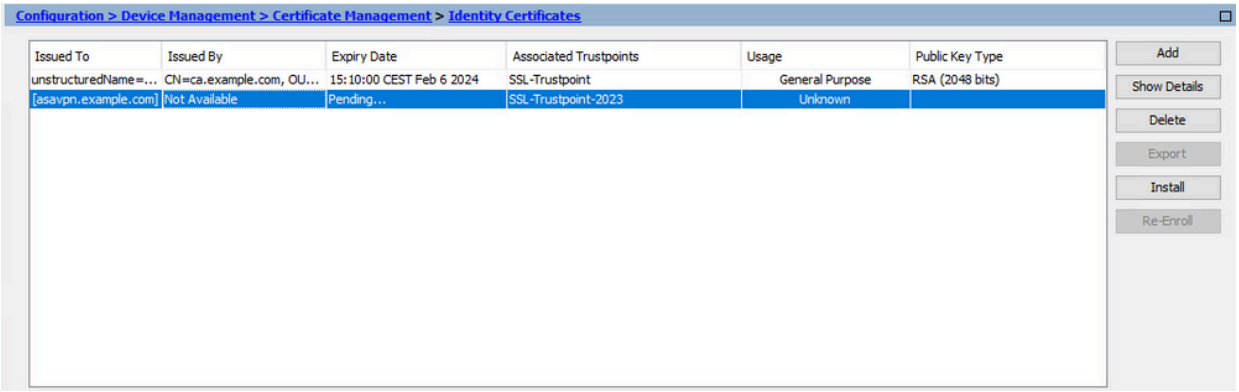


Cliquez sur Browse. Choisissez un emplacement dans lequel enregistrer le CSR, et enregistrez le fichier avec l'extension .txt.

> 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).

---

c. Le nouveau point de confiance est maintenant affiché à l'état En attente.



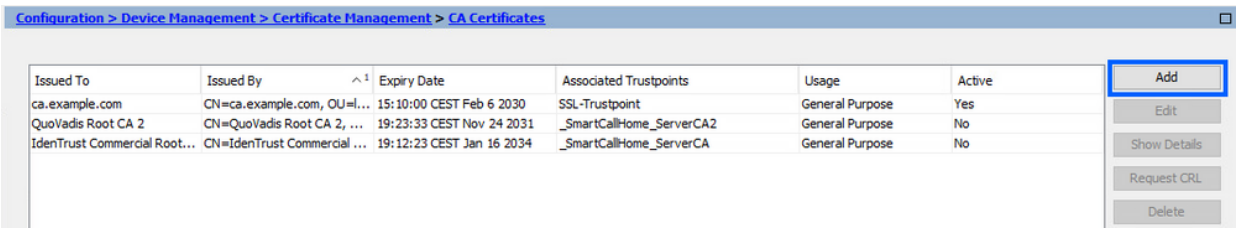
Installer le certificat d'identité au format PEM avec ASDM

Les étapes d'installation supposent que l'autorité de certification a signé le CSR et fourni un nouveau certificat d'identité codé PEM (.pem, .cer, .crt) et un ensemble de certificats d'autorité de certification.

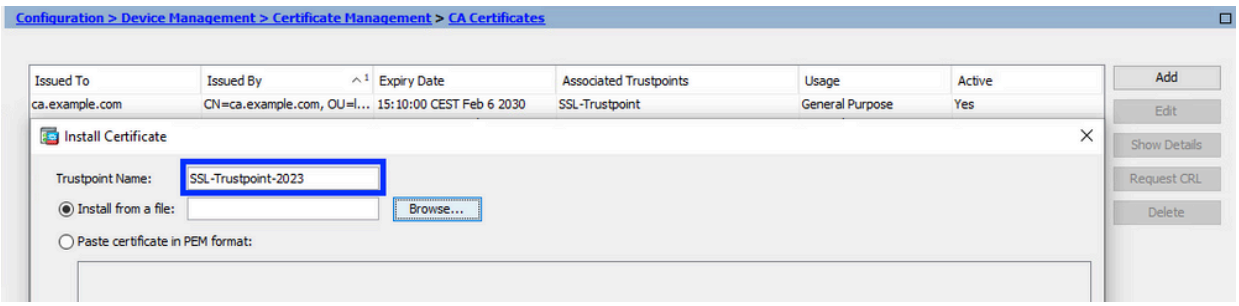
1. Installer le certificat AC qui a signé le CSR

   Le certificat d'autorité de certification qui a signé le certificat d'identité peut être installé dans le point de confiance créé pour le certificat d'identité. Si le certificat d'identité est signé par une autorité de certification intermédiaire, ce certificat peut être installé dans le point de confiance du certificat d'identité. Tous les certificats d'autorité de certification en amont dans la hiérarchie peuvent être installés dans des points de confiance d'autorité de certification distincts.

   a. Accédez à Configuration > Device Management > Certificate Management >, et choisissez CA Certificates. Cliquez sur Add.

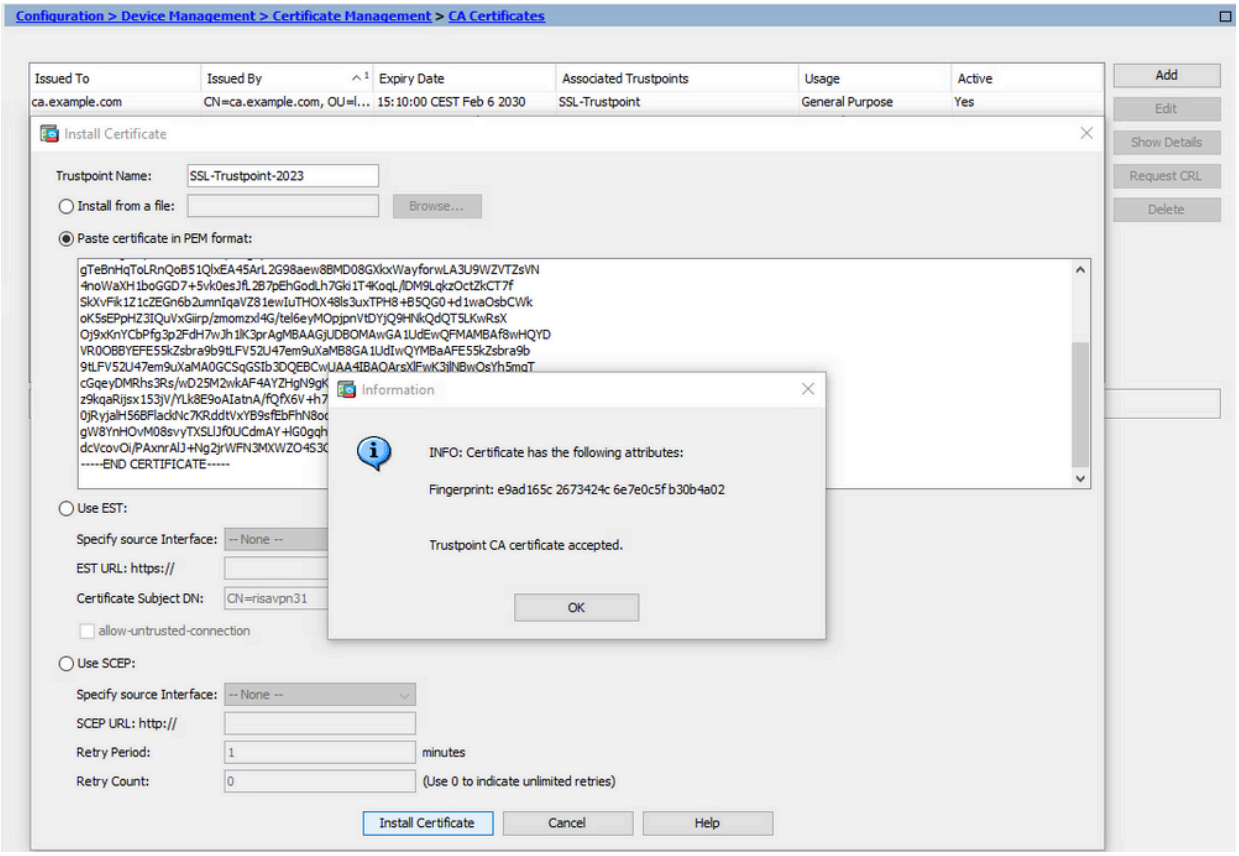


   b. Entrez le nom du point de confiance et choisissez Install From File, cliquez sur Browse button, et choisissez le certificat intermédiaire. Vous pouvez également coller le certificat CA codé PEM d'un fichier texte dans le champ texte.

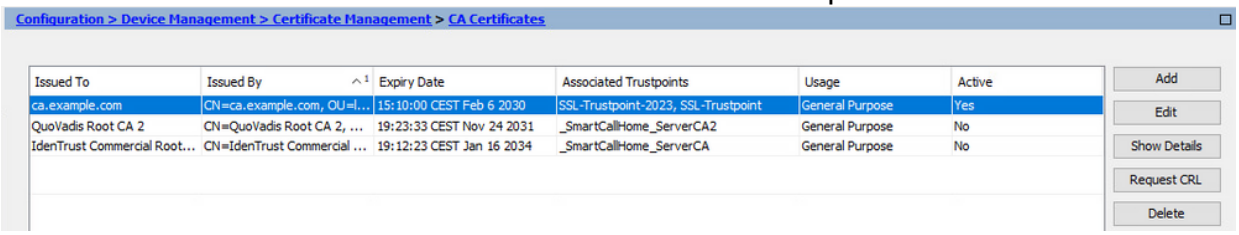


> Remarque : installez le certificat intermédiaire avec le même nom de point de confiance que le nom de point de confiance du certificat d'identité, si le certificat d'identité est signé par le certificat d'autorité de certification intermédiaire.

c. Cliquez sur Install Certificate.

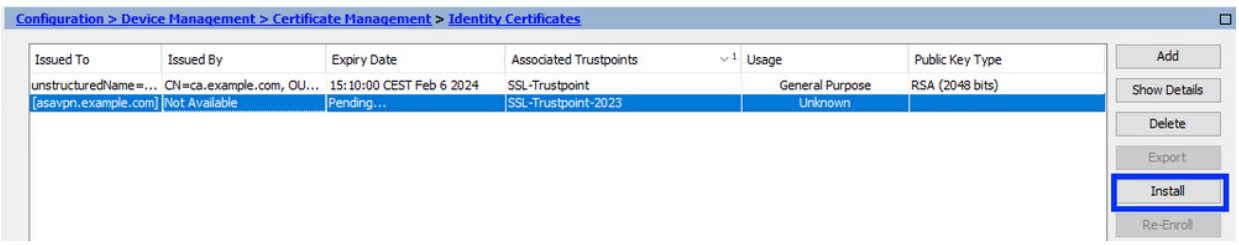


Dans l'exemple, le nouveau certificat est signé avec le même certificat CA que l'ancien. Le même certificat CA est désormais associé à deux Trustpoints.



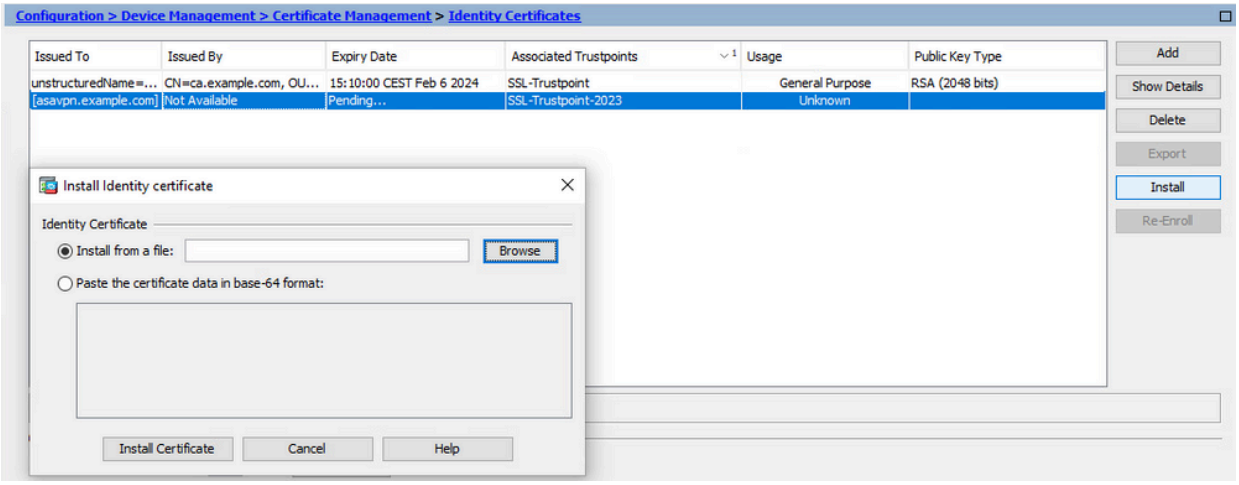
2. Installer le certificat d'identité

a. Sélectionnez le certificat d'identité créé précédemment avec la génération CSR. Cliquez sur Install.



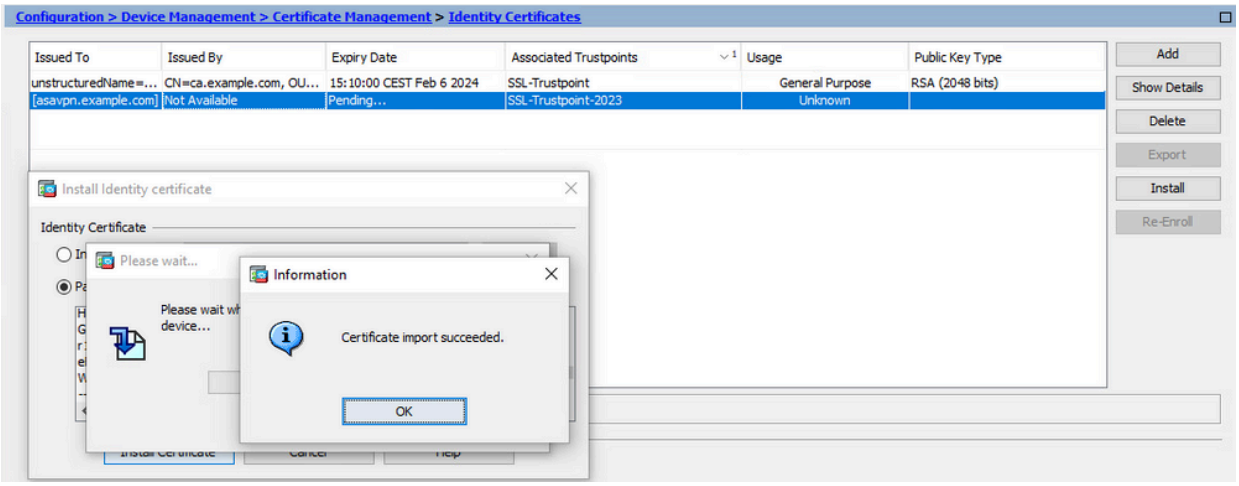
> Remarque : le champ Émis par du certificat d'identité peut avoir la valeur Non disponible, et le champ Date d'expiration la valeur En attente.

b. Choisissez un fichier qui contient le certificat d'identité codé PEM reçu de l'autorité de certification, ou ouvrez le certificat codé PEM dans un éditeur de texte, puis copiez et collez le certificat d'identité fourni par l'autorité de certification dans le champ de texte.

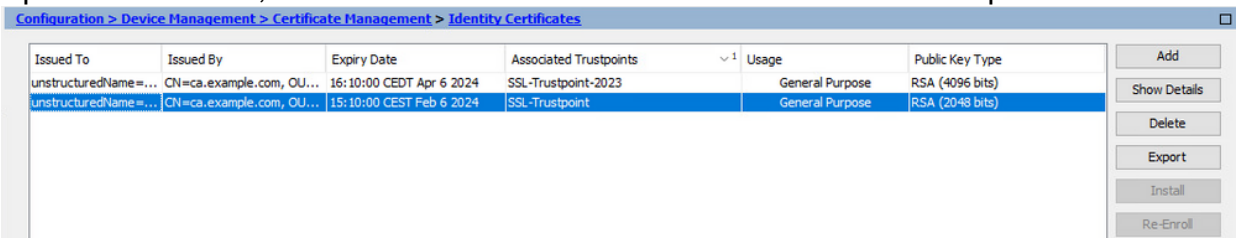


> Remarque : le certificat d'identité peut être au format .pem, .cer, .crt à installer.

c. Cliquez sur Install Certificate.



Après l'installation, des certificats d'identité anciens et nouveaux sont présents.



3. Lier le nouveau certificat à l'interface avec ASDM

L'ASA doit être configuré pour utiliser le nouveau certificat d'identité pour les sessions

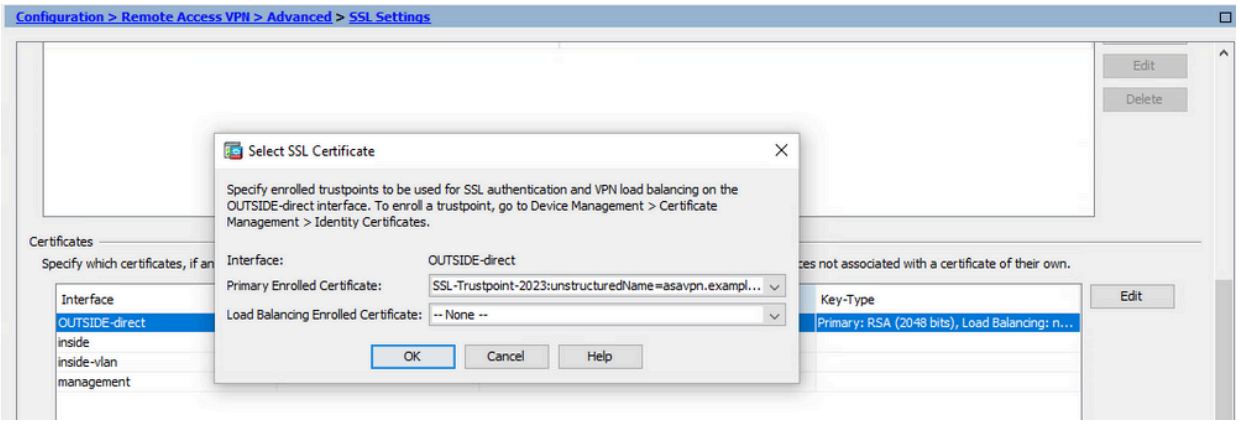
WebVPN qui se terminent sur l'interface spécifiée.

a. Accédez à Configuration > Remote Access VPN > Advanced > SSL Settings.

b. Sous Certificates, choisissez l'interface utilisée pour terminer les sessions WebVPN. Dans cet exemple, l'interface externe est utilisée.

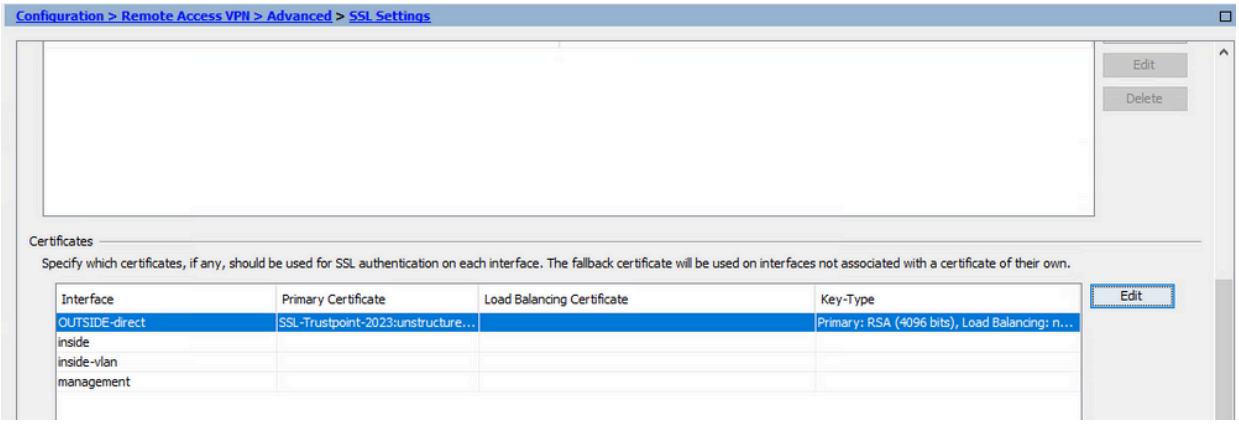
   Cliquez sur Edit.

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



d. Click OK.

e. Cliquez sur Apply. Le nouveau certificat d'identité est maintenant utilisé.



Renouveler un certificat inscrit avec un fichier PKCS12 avec ASDM

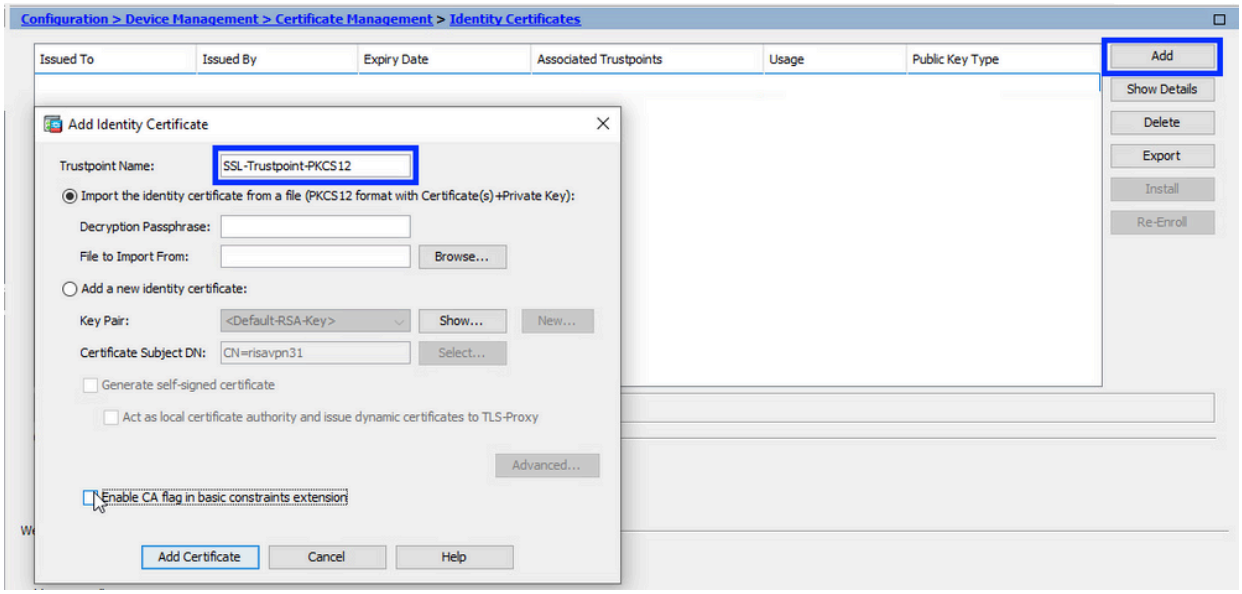
Le renouvellement du certificat inscrit PKCS12 nécessite la création et l'inscription d'un nouveau point de confiance. Il doit avoir un nom différent (par exemple, ancien nom avec suffixe de l'année d'inscription).

Le fichier PKCS12 (format .p12 ou .pfx) contient un certificat d'identité, une paire de clés et un ou plusieurs certificats d'autorité de certification. Il est créé par l'autorité de certification, par exemple, en cas de certificat générique, ou exporté à partir d'un autre périphérique. Il s'agit d'un fichier binaire qui ne peut pas être affiché avec l'éditeur de texte.

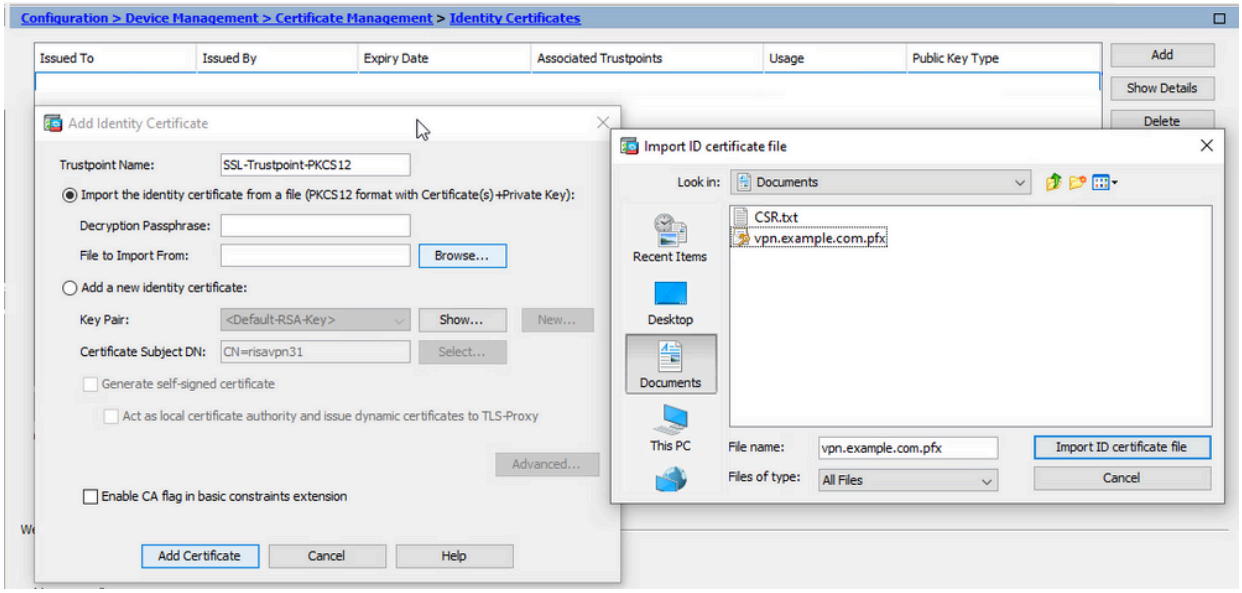
1. Installer le certificat d'identité renouvelé et les certificats CA à partir d'un fichier PKCS12

Le certificat d'identité, le ou les certificats d'autorité de certification et la paire de clés doivent être regroupés dans un fichier PKCS12 unique.

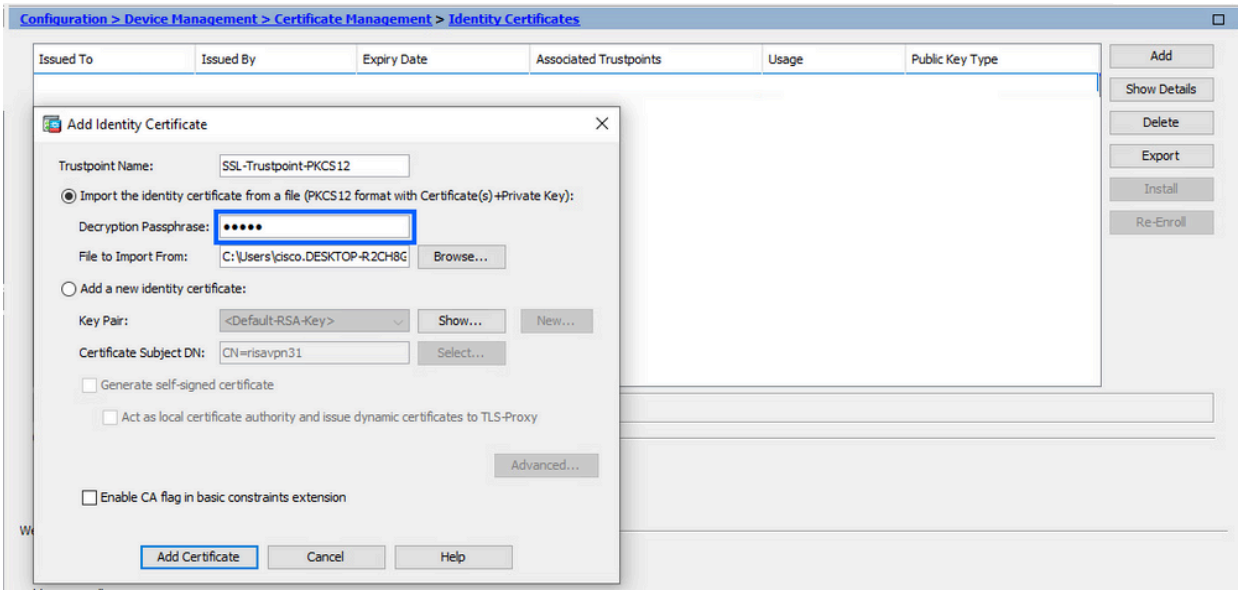
a. Accédez à Configuration > Device Management > Certificate Management, et choisissez Identity Certificates.
b. Cliquez sur Add.
c. Spécifiez un nouveau nom de point de confiance.



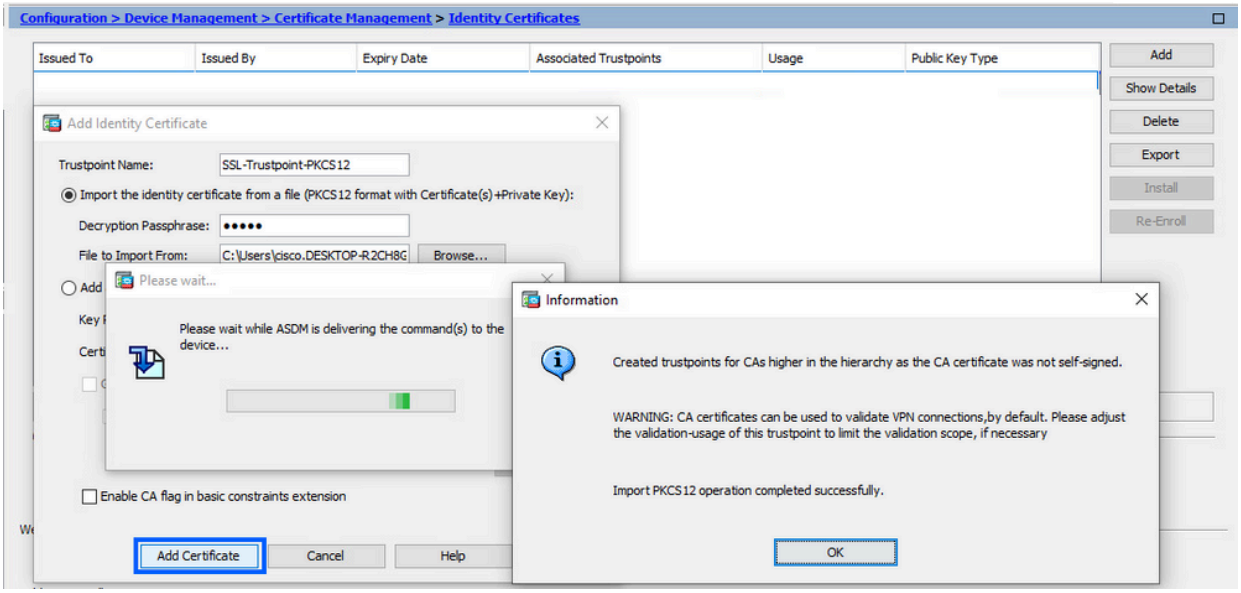
d. Activez la case d'option Importer le certificat d'identité à partir d'un fichier.



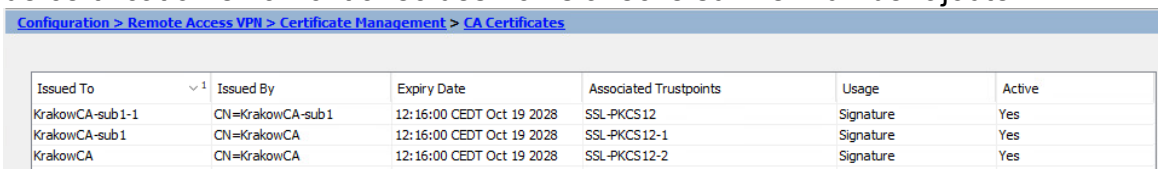
e. Entrez la phrase de passe utilisée pour créer le fichier PKCS12.



f. Cliquez sur Add Certificate.



Remarque : lorsqu'une chaîne PKCS12 avec certificats d'autorités de certification est importée, l'ASDM crée automatiquement les points de confiance des autorités de certification en amont avec des noms avec le suffixe -number ajouté.



Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
KrakowCA-sub1-1	CN=KrakowCA-sub1	12:16:00 CEDT Oct 19 2028	SSL-PKCS12	Signature	Yes
KrakowCA-sub1	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-1	Signature	Yes
KrakowCA	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-2	Signature	Yes

2. Lier le nouveau certificat à l'interface avec ASDM

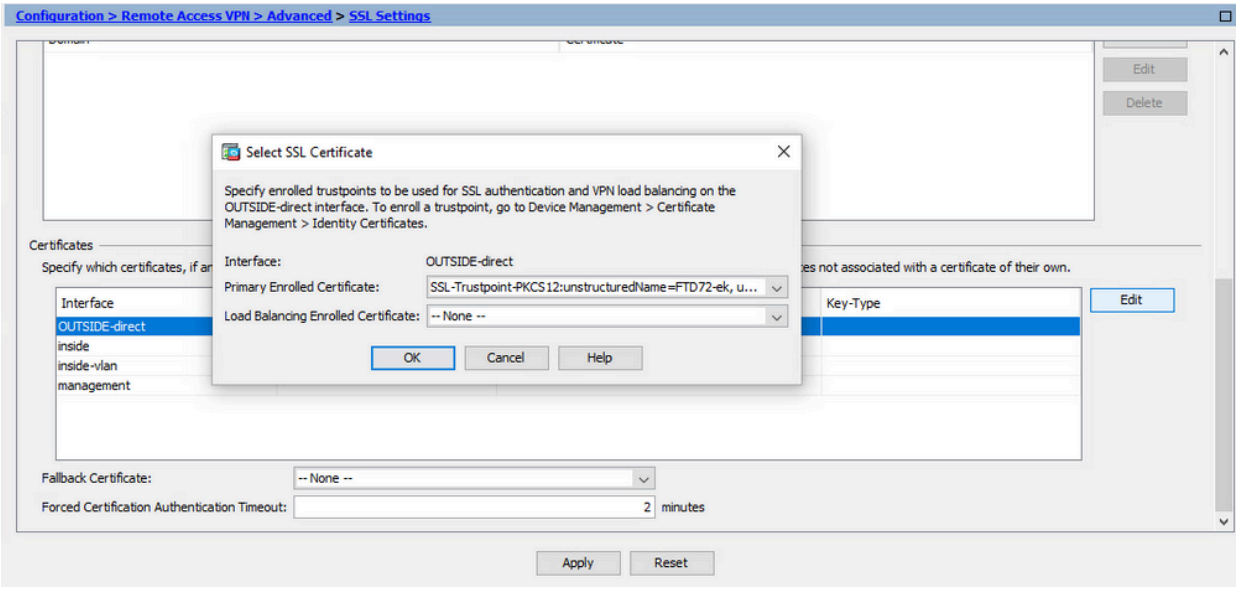
L'ASA doit être configuré pour utiliser le nouveau certificat d'identité pour les sessions WebVPN qui se terminent sur l'interface spécifiée.

a. Accédez à Configuration > Remote Access VPN > Advanced > SSL Settings.

b. Sous Certificates, choisissez l'interface utilisée pour terminer les sessions WebVPN. Dans cet exemple, l'interface externe est utilisée.

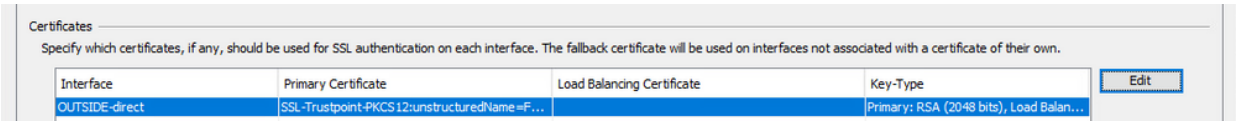
Cliquez sur Edit.

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



d. Click OK.

e. Cliquez sur Apply.



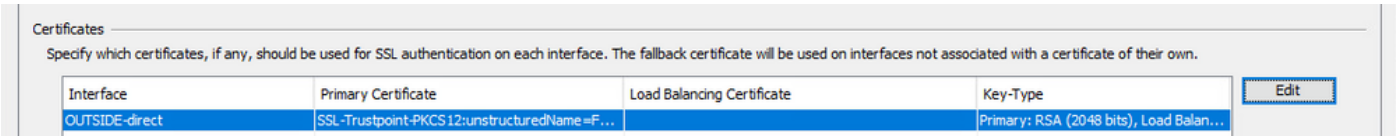
Le nouveau certificat d'identité est maintenant utilisé.

Vérifier

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

Afficher les certificats installés via ASDM

1. Accédez à Configuration > Remote Access VPN > Certificate Management, et choisissez Identity Certificates.
2. Le certificat d'identité émis par le fournisseur tiers peut s'afficher.



Dépannage

Cette commande debug doit être collectée sur l'interface de ligne de commande en cas d'échec de l'installation du certificat SSL.

- debug crypto ca 14

Forum aux questions

Q.Qu'est-ce qu'un PKCS12 ?
R.Dans le domaine de la cryptographie, PKCS12 définit un format de fichier d'archive créé pour stocker de nombreux objets de cryptographie sous la forme d'un fichier unique. Il est couramment utilisé pour regrouper une clé privée avec son certificat X.509 ou pour regrouper tous les membres d'une chaîne de confiance.

Q.Qu'est-ce qu'une RSE ?
R. Dans les systèmes d'infrastructure à clé publique (ICP), une demande de signature de certificat (également une demande de CSR ou de certification) est un message envoyé par un demandeur à une autorité d'enregistrement de l'infrastructure à clé publique afin de demander un certificat d'identité numérique. Il contient généralement la clé publique pour laquelle le certificat peut être émis, les informations utilisées pour identifier le certificat signé (par exemple, un nom de domaine dans Subject) et la protection de l'intégrité (par exemple, une signature numérique).

Q. Où se trouve le mot de passe de PKCS12 ?
R. Lorsque les certificats et les paires de clés sont exportés vers un fichier PKCS12, le mot de passe est indiqué dans la commande export. Pour importer un fichier pkcs12, le mot de passe doit être fourni par le propriétaire du serveur AC ou par la personne qui a exporté le PKCS12 à partir d'un autre périphérique.

Q. Quelle est la différence entre la racine et l'identité ?
R.Dans le domaine de la cryptographie et de la sécurité informatique, un certificat racine est un certificat à clé publique qui identifie une autorité de certification racine. Les certificats racine sont auto-signés (et il est possible qu'un certificat ait plusieurs chemins d'accès d'approbation, par exemple si le certificat a été émis par un racine qui a été signé de manière croisée) et forment la base d'une infrastructure de clé publique (PKI) basée sur X.509. Un certificat de clé publique, également appelé certificat numérique ou certificat d'identité, est un document électronique utilisé pour prouver la propriété d'une clé publique. Le certificat comprend des informations sur la clé, des informations sur l'identité de son propriétaire (appelée objet) et la signature numérique d'une entité qui a vérifié le contenu du certificat (appelée émetteur). Si la signature est valide et que le logiciel qui examine le certificat fait confiance à l'émetteur, il peut utiliser cette clé pour communiquer en toute sécurité avec l'objet du certificat.

Q.J'ai installé le certificat, pourquoi il ne fonctionne pas ?
R. Cela pourrait être dû à de nombreuses raisons, par exemple :

1. Le certificat et le point de confiance sont configurés, mais ils n'ont pas été liés au processus qui

devrait l'utiliser. Par exemple, le point de confiance à utiliser n'est pas lié à l'interface externe qui termine les clients Anyconnect.

2. Un fichier PKCS12 est installé, mais présente des erreurs en raison de l'absence du certificat d'autorité de certification intermédiaire dans le fichier PKCS12. Les clients dont le certificat d'autorité de certification intermédiaire est approuvé, mais dont le certificat d'autorité de certification racine n'est pas approuvé, ne sont pas en mesure de vérifier l'ensemble de la chaîne de certificats et de signaler le certificat d'identité du serveur comme n'étant pas approuvé.

3. Un certificat renseigné avec des attributs incorrects peut entraîner un échec de l'installation ou des erreurs côté client. Par exemple, certains attributs peuvent être codés avec un format incorrect. Une autre raison est que le certificat d'identité ne contient pas de nom alternatif de sujet (SAN) ou que le nom de domaine utilisé pour accéder au serveur n'est pas présent en tant que SAN.

Q. L'installation d'un nouveau certificat nécessite-t-elle une fenêtre de maintenance ou entraîne-t-elle des temps d'arrêt ?
R. L'installation d'un nouveau certificat (identité ou autorité de certification) n'est pas intrusive et ne devrait pas entraîner d'interruption ou nécessiter une fenêtre de maintenance. L'activation d'un nouveau certificat pour un service existant est une modification et peut nécessiter une demande de modification / une fenêtre de maintenance.

Q. L'ajout ou la modification d'un certificat peut-il déconnecter les utilisateurs connectés ?
R.Non, les utilisateurs actuellement connectés restent connectés. Le certificat est utilisé lors de l'établissement de la connexion. Une fois les utilisateurs reconnectés, le nouveau certificat est utilisé.

Q. Comment créer une demande de service client avec un caractère générique ? Ou un autre nom de sujet (SAN) ?
R. Actuellement, l'ASA/FTD ne peut pas créer de CSR avec un caractère générique ; cependant, ce processus peut être effectué avec OpenSSL. Pour générer la clé CSR et ID, vous pouvez exécuter les commandes suivantes :

```
openssl genrsa -out id.key 2048

openssl req -out id.csr -key id.key -new
```

Lorsqu'un point de confiance est configuré avec l'attribut FQDN (Fully Qualified Domain Name), le CSR créé par ASA/FTD contient le SAN avec cette valeur. L'autorité de certification peut ajouter d'autres attributs SAN lorsqu'elle signe le CSR, ou le CSR peut être créé avec OpenSSL

Q. Le remplacement du certificat prend-il effet immédiatement ?

R. Le nouveau certificat d'identité du serveur est utilisé uniquement pour les nouvelles connexions. Le nouveau certificat est prêt à être utilisé immédiatement après la modification, mais il est en fait utilisé avec les nouvelles connexions.

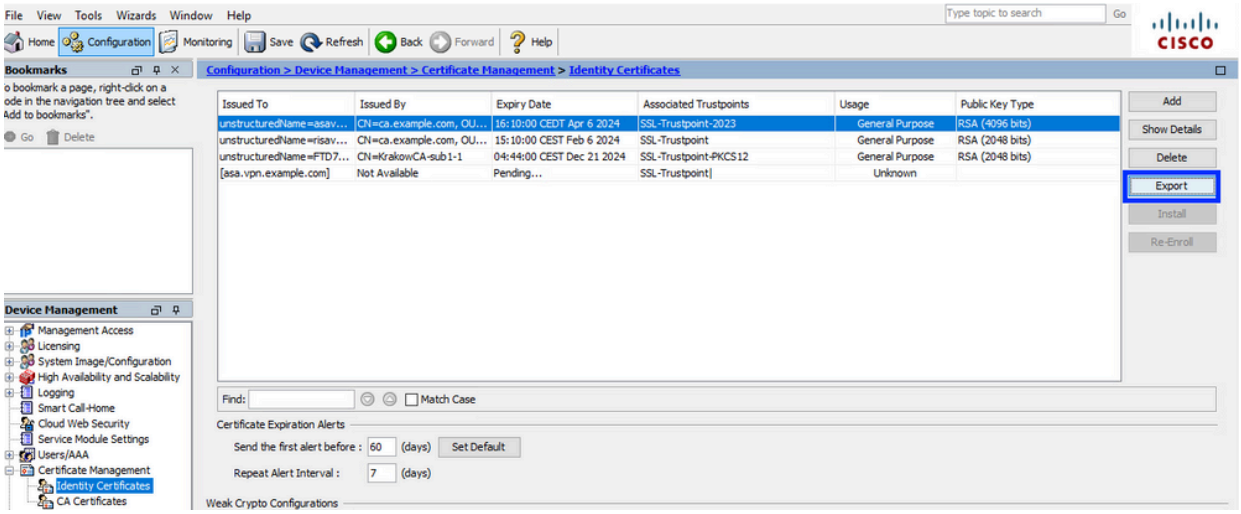
Q.Comment puis-je vérifier si l'installation a fonctionné ?
A.La commande CLI pour vérifier : show crypto ca cert **<trustpointname>**

Q.Comment générer PKCS12 à partir d'un certificat d'identité, d'un certificat d'autorité de certification et d'une clé privée ?
R. PKCS12 peut être créé avec OpenSSL, avec la commande :
openssl pkcs12 -export -out p12.pfx -inkey id.key -in id.crt -certfile ca.crt

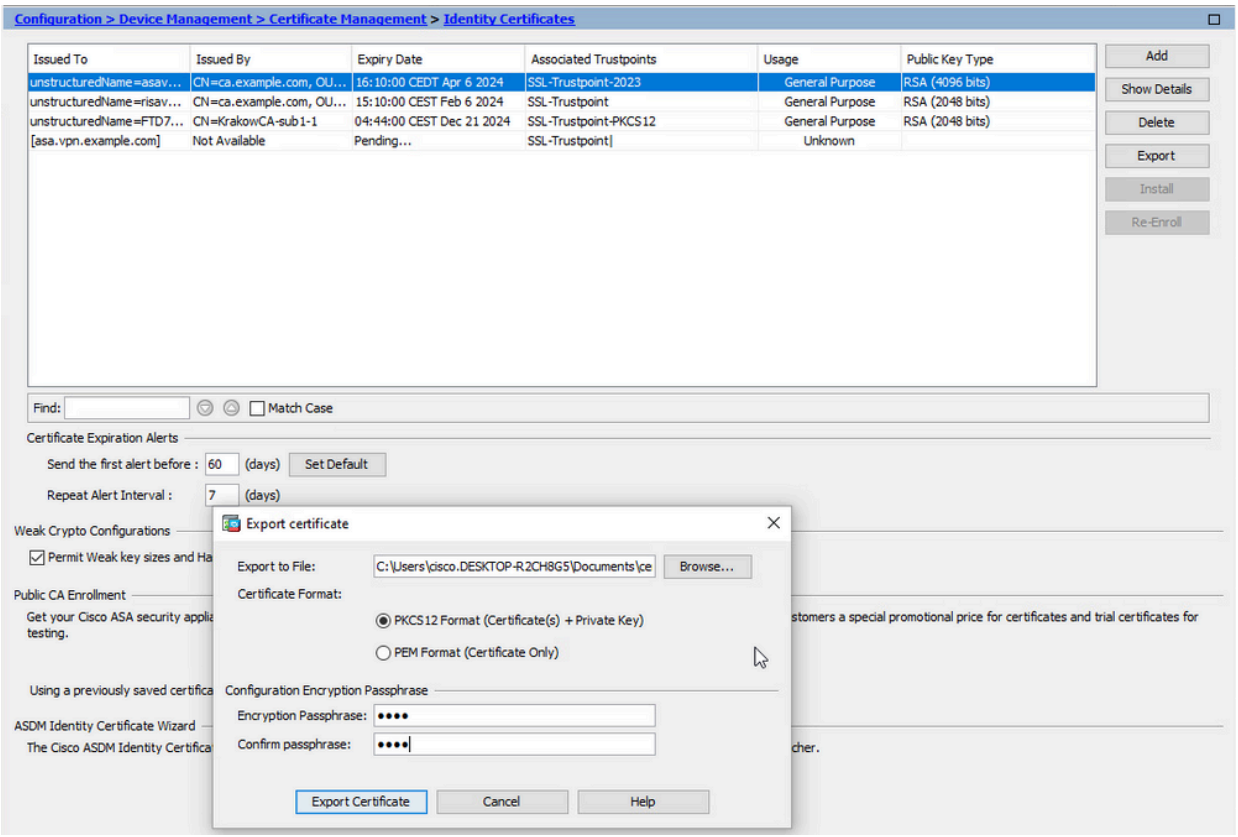
Q. Comment exporter un certificat pour l'installer dans un nouvel ASA ?
A.

- Avec l'interface de ligne de commande : utilisez la commande : crypto ca export <trustpointname> pkcs12 <password>
- Avec ASDM :

a. Accédez à Configuration > Device Management > Certificate Management > Identity Certificates et choisissez Identity Certificate. Cliquez sur Exporter.



b. Choisissez où exporter le fichier, spécifiez le mot de passe d'exportation, cliquez sur Export Certificate.



Le certificat exporté peut se trouver sur le disque de l'ordinateur. Veuillez prendre note de la phrase de passe dans un endroit sûr, le fichier est inutile sans elle.

Q. Si des clés ECDSA sont utilisées, le processus de génération de certificat SSL est-il différent ?
R. La seule différence de configuration est l'étape de génération de paire de clés, où une paire de clés ECDSA peut être générée à la place d'une paire de clés RSA. Le reste des étapes reste le même.

Q. Est-il toujours nécessaire de générer une nouvelle paire de clés ?
R. L'étape de génération de la paire de clés est facultative. La paire de clés existante peut être utilisée ou, dans le cas de PKCS12, la paire de clés est importée avec le certificat. Reportez-vous à la section Sélectionner le nom de la paire de clés pour le type d'inscription/réinscription correspondant.

Q. Est-il sûr de générer une nouvelle paire de clés pour un nouveau certificat d'identité ?
R.Le processus est sûr tant qu'un nouveau nom de paire de clés est utilisé. Dans ce cas, les anciennes paires de clés ne sont pas modifiées.

Q. Faut-il générer à nouveau une clé lorsqu'un pare-feu est remplacé (comme RMA) ?
R.Le nouveau pare-feu n'a pas de paires de clés sur l'ancien pare-feu.
La sauvegarde de la configuration en cours ne contient pas les paires de clés.
La sauvegarde complète effectuée avec ASDM peut contenir les paires de clés.
Les certificats d'identité peuvent être exportés à partir d'un ASA avec ASDM ou CLI, avant qu'il

n'échoue.
En cas de paire de basculement, les certificats et les paires de clés sont synchronisés sur une unité en veille avec la commande write standby. En cas de remplacement d'un noeud de la paire de basculement, il suffit de configurer le basculement de base et de transmettre la configuration au nouveau périphérique.
Si une paire de clés est perdue avec le périphérique et qu'il n'y a pas de sauvegarde, un nouveau certificat doit être signé avec la paire de clés présente sur le nouveau périphérique.

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.