Configurer ASA comme serveur AC local et tête de réseau AnyConnect

Table des matières

Introduction

Ce document décrit comment configurer un dispositif de sécurité adaptatif Cisco (ASA) en tant que serveur d'autorité de certification (CA) et en tant que passerelle SSL (Secure Sockets Layer) pour les clients Cisco AnyConnect Secure Mobility.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration ASA de base qui exécute la version 9.1.x du logiciel
- ASDM 7.3 ou supérieur

Composants utilisés

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

logiciel suivantes :

- ASA de la gamme Cisco 5500 qui exécute le logiciel version 9.1(6)
- Client AnyConnect Secure Mobility version 4.x pour Windows
- PC qui exécute un système d'exploitation pris en charge conformément au tableau de compatibilité.
- Cisco Adaptive Security Device Manager (ASDM) version 7.3

Remarque : téléchargez le package client VPN AnyConnect (anyconnect-win*.pkg) à partir de la page de téléchargement de logiciels Cisco (clients enregistrés uniquement) . Copiez le client VPN d'AnyConnect dans la mémoire flash de l'ASA qui doit être téléchargée sur les ordinateurs des utilisateurs distants afin d'établir la connexion VPN SSL avec l'ASA. Référez-vous à la section Installer le client d'AnyConnect du guide de configuration d'ASA pour plus d'informations.

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

Informations générales

L'autorité de certification sur l'ASA fournit les fonctionnalités suivantes :

- Intègre le fonctionnement de l'autorité de certification de base sur ASA.
- Déploie des certificats.
- Assure la vérification sécurisée de la révocation des certificats émis.
- Fournit une autorité de certification sur l'ASA pour une utilisation avec des connexions VPN SSL basées sur navigateur (WebVPN) et sur client (AnyConnect).
- Fournit des certificats numériques approuvés aux utilisateurs, sans avoir à se fier à une autorisation de certificat externe.
- Fournit une autorité interne sécurisée pour l'authentification des certificats et permet une inscription simple des utilisateurs au moyen d'une connexion au site Web.

Directives et restrictions

- Pris en charge en mode pare-feu routé et transparent.
- Un seul serveur AC local à la fois peut résider sur un ASA.
- La fonctionnalité ASA en tant que serveur AC local n'est pas prise en charge dans une configuration de basculement.
- L'ASA agissant désormais en tant que serveur d'autorité de certification locale prend uniquement en charge la génération de certificats SHA1.
- Le serveur AC local peut être utilisé pour les connexions VPN SSL basées sur navigateur et sur client. Actuellement non pris en charge pour IPSec.
- Ne prend pas en charge l'équilibrage de charge VPN pour l'autorité de certification locale.
- L'autorité de certification locale ne peut pas être subordonnée à une autre autorité de

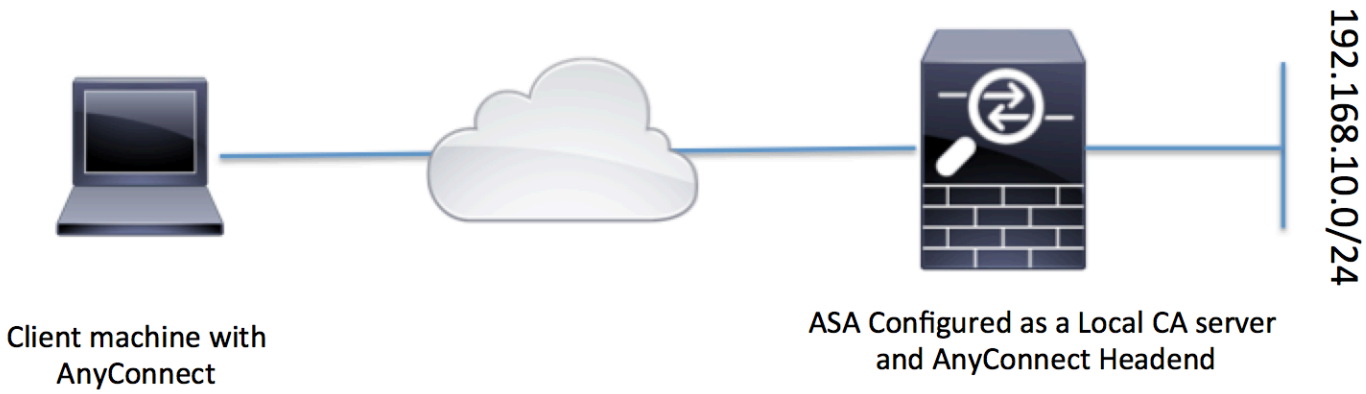
certification. Il ne peut agir qu'en tant qu'autorité de certification racine.
- Actuellement, l'ASA ne peut pas s'inscrire au serveur de l'autorité de certification locale pour le certificat d'identité.
- Lorsqu'une inscription de certificat est terminée, l'ASA stocke un fichier PKCS12 contenant la paire de clés et la chaîne de certificats de l'utilisateur, ce qui nécessite environ 2 Ko de mémoire flash ou d'espace disque par inscription. La quantité réelle d'espace disque dépend de la taille de clé RSA configurée et des champs de certificat. Gardez cette directive à l'esprit lorsque vous ajoutez un grand nombre d'inscriptions de certificats en attente sur un ASA avec une quantité limitée de mémoire flash disponible, car ces fichiers PKCS12 sont stockés dans la mémoire flash pendant la durée du délai d'expiration de récupération d'inscription configuré.

Configurer

Cette section décrit comment configurer Cisco ASA en tant que serveur d'autorité de certification locale.

Remarque : Utilisez l'outil de recherche de commandes (clients enregistrés seulement) pour en savoir plus sur les commandes employées dans cette section.

Diagramme du réseau



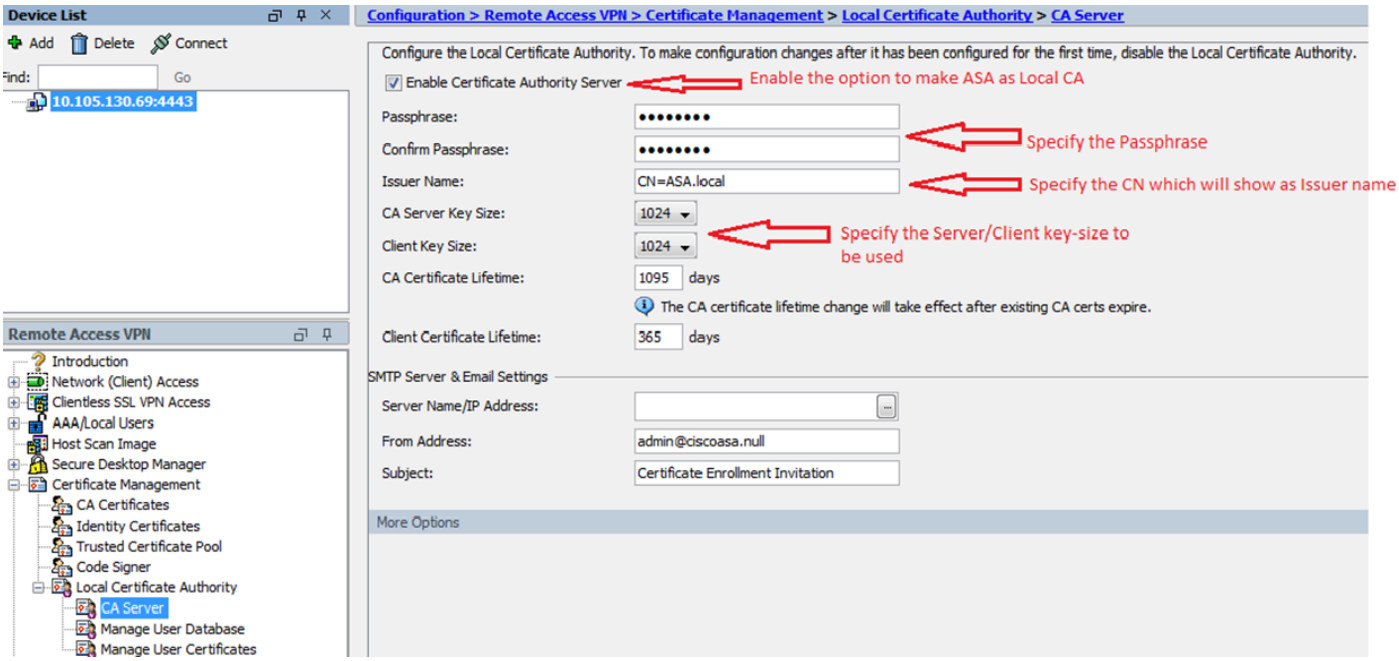
ASA en tant que serveur AC local

Étape 1. Configurer et activer le serveur AC local sur ASA

- Accédez à Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > CA Server. Cochez l'option Enable Certificate Authority server.
- Configurez Passphrase. La phrase de passe doit comporter au moins 7 caractères. Elle est utilisée pour coder et enregistrer un fichier PKCS12 qui inclut le certificat de l'autorité de

certification locale et la paire de clés. La phrase de passe déverrouille l'archive PKCS12 en cas de perte du certificat CA ou de la paire de clés.

- Configurez le nom de l'émetteur. Ce champ apparaît sous la forme CN de certificat racine. Vous pouvez le spécifier dans le format suivant : CN (nom commun), OU (unité d'organisation), (O) Organisation , L (localité) , S (état) et C (pays).
- Configuration facultative : configurez les paramètres du serveur SMTP et du serveur de messagerie pour vous assurer que le protocole OTP peut être reçu par les clients finaux par courrier électronique pour terminer l'inscription. Vous pouvez configurer le nom d'hôte ou l'adresse IP de votre serveur de messagerie électronique/SMTP local. Vous pouvez également configurer l'adresse de l'expéditeur et le champ Objet de l'e-mail que les clients recevraient. Par défaut, l'adresse d'origine est admin@<nom d'hôte ASA>.null et l'objet est l'invitation d'inscription de certificat.
- Configuration facultative : vous pouvez configurer les paramètres facultatifs tels que la taille de la clé du client, la taille de la clé du serveur AC, la durée de vie du certificat AC et la durée de vie du certificat Client.



Équivalent de la CLI :

```
ASA(config)# crypto ca server
ASA(config-ca-server)# issuer-name CN=ASA.local
ASA(config-ca-server)# subject-name-default CN=ASA.local
ASA(config-ca-server)# lifetime certificate 365
ASA(config-ca-server)# lifetime ca-certificate 1095
ASA(config-ca-server)# passphrase cisco123
ASA(config-ca-server)# no shutdown
% Some server settings cannot be changed after CA certificate generation.
Keypair generation process begin. Please wait...

Completed generation of the certificate and keypair...
```

```
Archiving certificate and keypair to storage... Complete
```

Il s'agit de champs supplémentaires qui peuvent être configurés sous Configuration du serveur AC local.

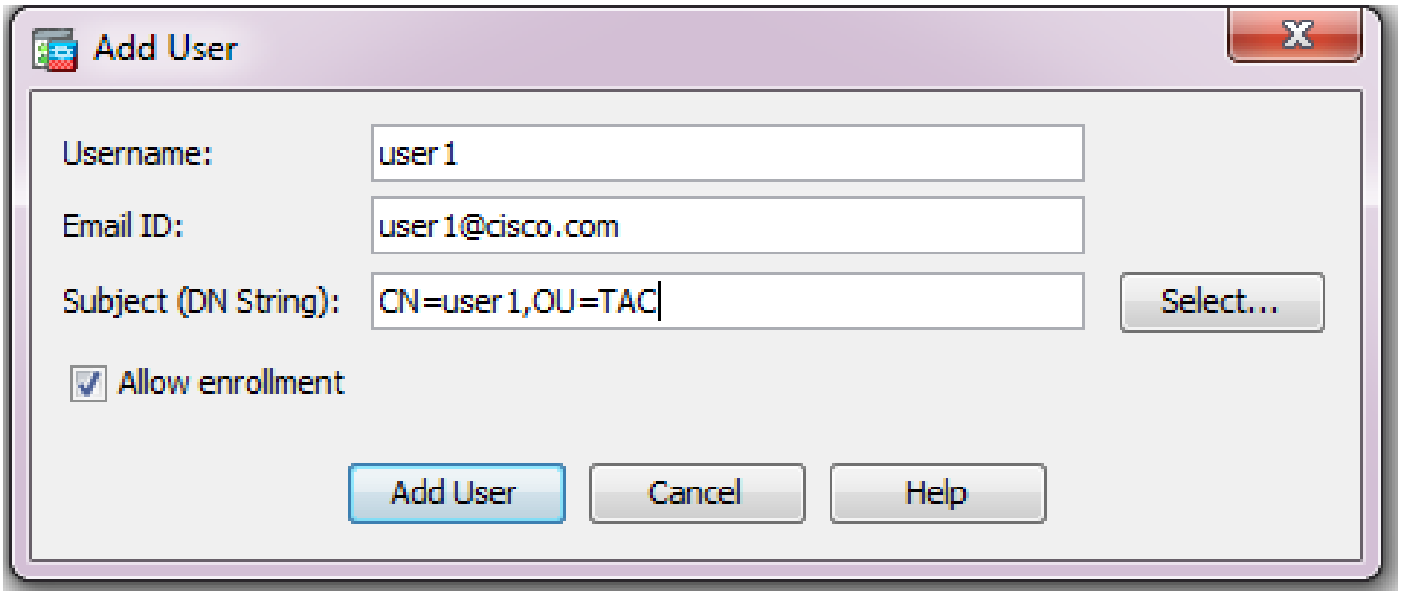
URL du point de distribution CRL	Il s'agit de l'emplacement CRL sur l'ASA. L'emplacement par défaut est http://hostname.domain/+CSCOCA+/asa_ca.crl mais l'URL pourrait être modifiée.
Interface et port de publication-CRL	Pour rendre la liste de révocation de certificats disponible pour le téléchargement HTTP sur une interface et un port donnés, choisissez une interface de publication de liste de révocation de certificats dans la liste déroulante. Saisissez ensuite le numéro de port, qui peut être n'importe quel numéro de port compris entre 1 et 65535. Le numéro de port par défaut est le port TCP 80.
Durée de vie CRL	L'autorité de certification locale met à jour et réémet la liste de révocation de certificats chaque fois qu'un certificat utilisateur est révoqué ou non révoqué, mais si aucune modification n'est apportée à la révocation, la liste de révocation de certificats est réémise automatiquement une fois par durée de vie de la liste de révocation de certificats, la période que vous spécifiez avec la commande crl lifetime lors de la configuration de l'autorité de certification locale. Si vous ne spécifiez pas de durée de vie CRL, la période par défaut est de six heures.
Emplacement de stockage	L'ASA accède aux informations utilisateur, aux certificats émis et aux listes de révocation et les implémente à l'aide d'une base de données CA locale. Cette base de données réside par défaut dans la mémoire flash locale, ou peut être configurée pour résider sur un système de fichiers externe monté et accessible par l'ASA.
Nom du sujet par défaut	Entrez un objet par défaut (chaîne DN) à ajouter à un nom d'utilisateur sur les certificats émis. Les attributs DN autorisés sont fournis dans cette liste : ·CN (nom commun)SN (nom de famille) ·O (Nom de l'organisation) ·L (Localité) ·C (Pays) ·OU (Unité d'organisation) ·EA (Adresse e-mail)

	·ST (État/Province) ·T (Titre)
Période d'inscription	Définit le délai d'inscription, en heures, au cours duquel l'utilisateur peut récupérer le fichier PKCS12 à partir d'ASA. La valeur par défaut est de 24 heures. **Remarque :** si la période d'inscription expire avant que l'utilisateur ne récupère le fichier PKCS12 qui inclut le certificat utilisateur, l'inscription n'est pas autorisée.
Expiration du mot de passe unique	Définit la durée en heures pendant laquelle le protocole OTP est valide pour l'inscription des utilisateurs. Cette période commence lorsque l'utilisateur est autorisé à s'inscrire. La valeur par défaut est 72 heures.
Rappel d'expiration de certificat	Spécifie le nombre de jours avant l'expiration du certificat pendant lesquels un rappel initial de réinscription est envoyé aux propriétaires de certificats.

Étape 2. Créer et ajouter des utilisateurs à la base de données ASA

- Accédez à Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Database.Cliquez sur Add.

- Spécifiez les détails de l'utilisateur, à savoir le nom d'utilisateur, l'ID e-mail et le nom de l'objet, comme indiqué dans cette image.



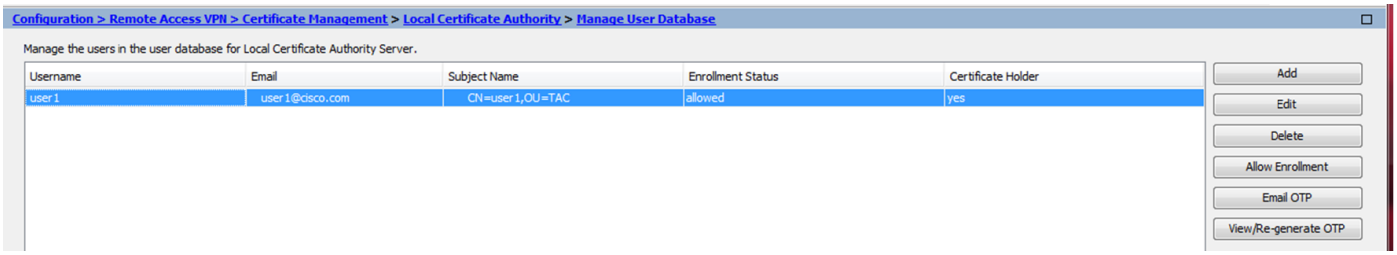
- Assurez-vous que Allow Enrollment est coché afin que vous soyez autorisé à vous inscrire pour le certificat.
- Cliquez sur Add User pour terminer la configuration de l'utilisateur.

Équivalent de la CLI :

<#root>

```
ASA(config)# crypto ca server user-db add user1 dn CN=user1,OU=TAC email user1@cisco.com
```

- Une fois l'utilisateur ajouté à la base de données utilisateur, l'état d'inscription est Autorisé à s'inscrire.



CLI pour vérifier l'état de l'utilisateur :

<#root>

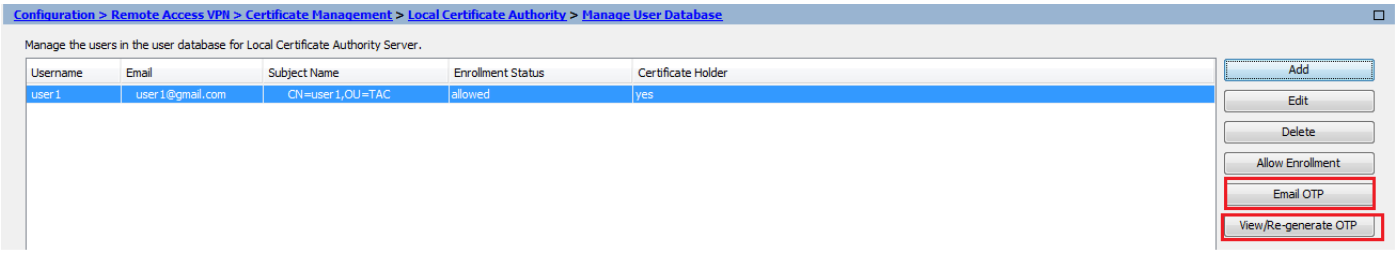
```
ASA# show crypto ca server user-db

username: user1
email:    user1@cisco.com
dn:       CN=user1,OU=TAC
allowed:  19:03:11 UTC Thu Jan 14 2016
notified: 1 times
enrollment status:

Allowed to Enroll
```

- Une fois l'utilisateur ajouté à la base de données utilisateur, le mot de passe à usage unique (OTP), pour que l'utilisateur puisse terminer l'inscription, peut être fourni à l'aide de l'une des méthodes suivantes :

Envoyer un e-mail avec le protocole OTP (nécessite la configuration du serveur SMTP et des paramètres d'e-mail sous la configuration du serveur AC).

OU

Visualisez directement le protocole OTP et partagez-le avec l'utilisateur en cliquant sur View/Re-generate OTP. Cela peut également être utilisé pour régénérer le protocole OTP.



Équivalent de la CLI :

```
!! Email the OTP to the user
ASA# crypto ca server user-db allow user1 email-otp

!! Display the OTP on terminal
ASA# crypto ca server user-db allow user1 display-otp
Username: user1
OTP: 18D14F39C8F3DD84
Enrollment Allowed Until: 14:18:34 UTC Tue Jan 12 2016
```

Étape 3. Activez webvpn sur l'interface WAN

- Activez l'accès Web sur l'ASA pour que les clients demandent l'inscription.

```
!! Enable web-access on the "Internet" interface of the ASA
ASA(config)# webvpn
ASA(config-webvpn)#enable Internet
```

Étape 4. Importer le certificat sur l'ordinateur client

- Sur le poste de travail client, ouvrez un navigateur et accédez au lien afin de terminer l'inscription.
- L'IP/FQDN utilisé dans ce lien doit être l'IP de l'interface sur laquelle webvpn est activé à

cette étape, qui est l'interface Internet.

<#root>

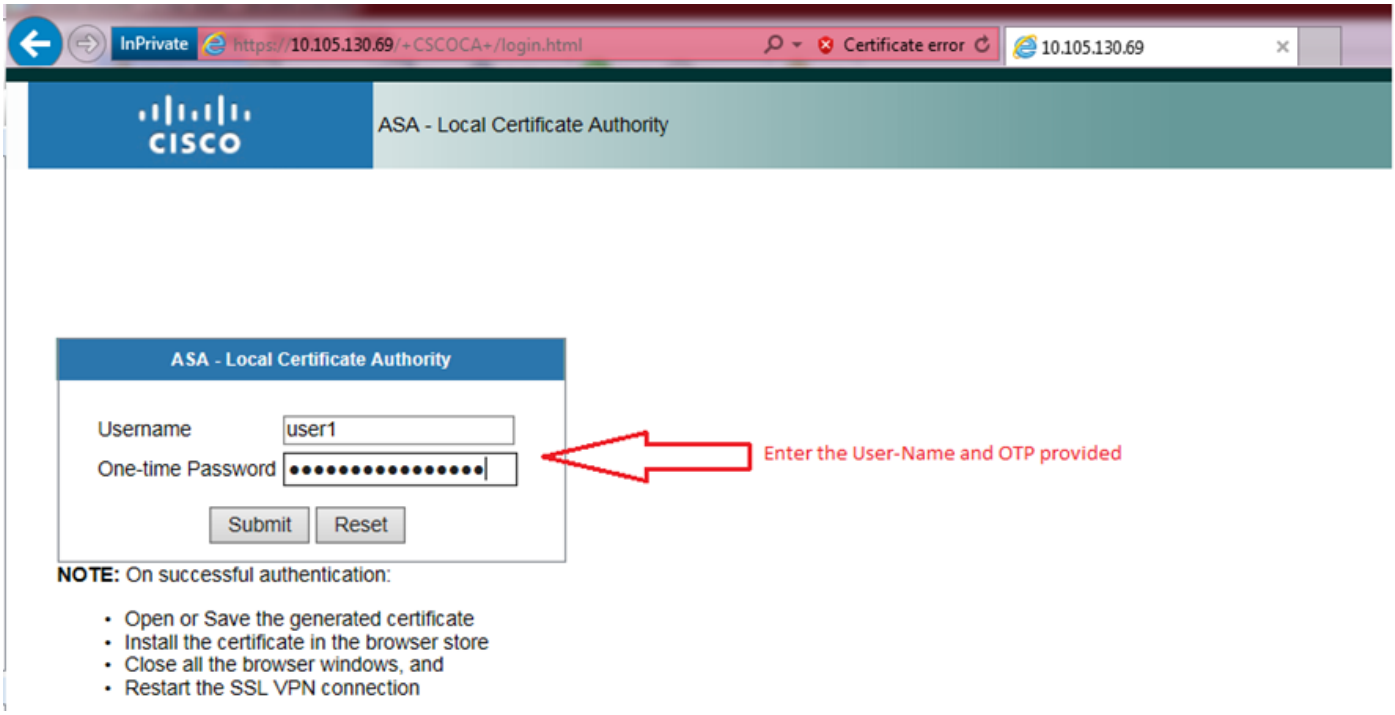
https://

<>

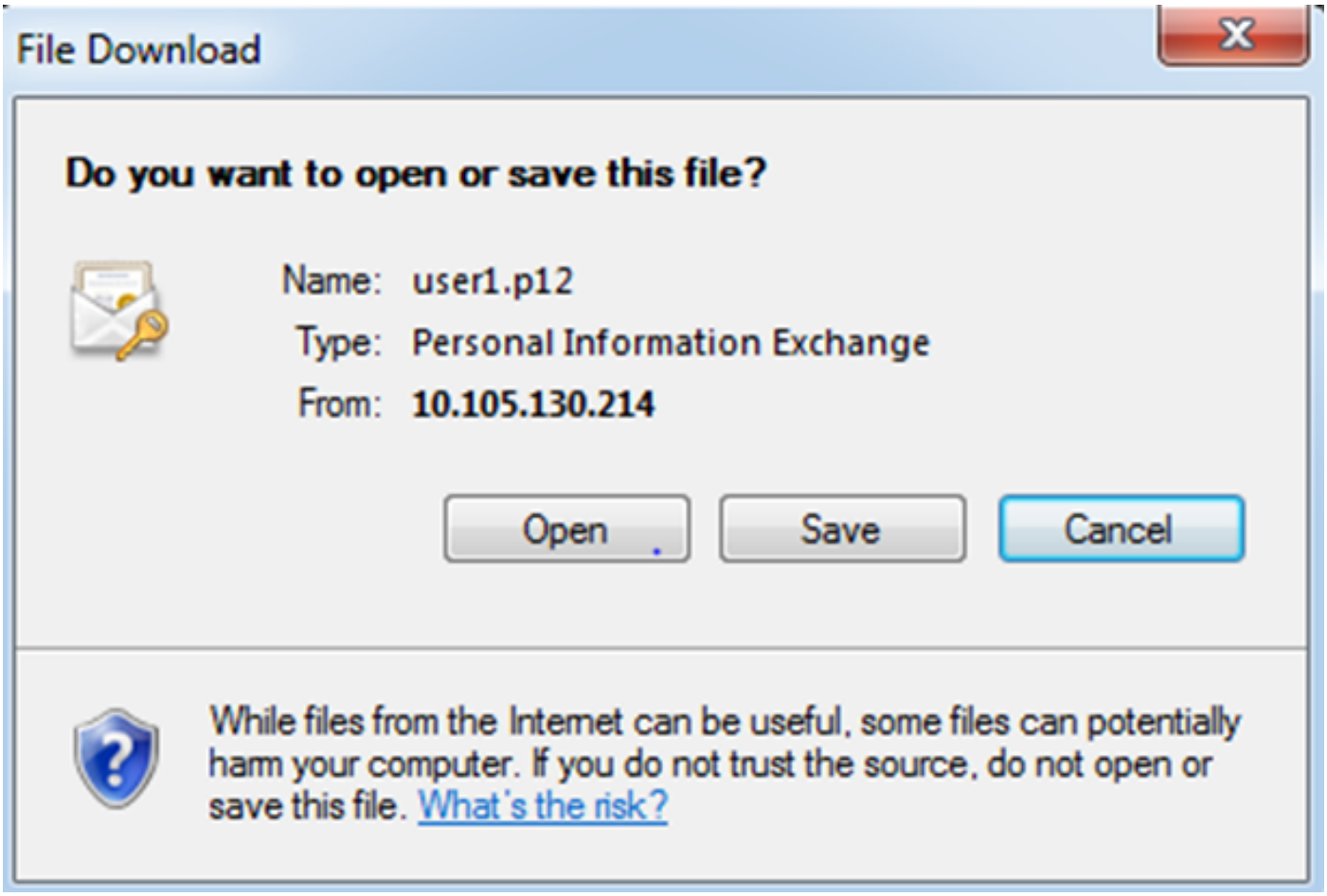
IP/FQDN>/+CSCOCA+/enroll.html

<>

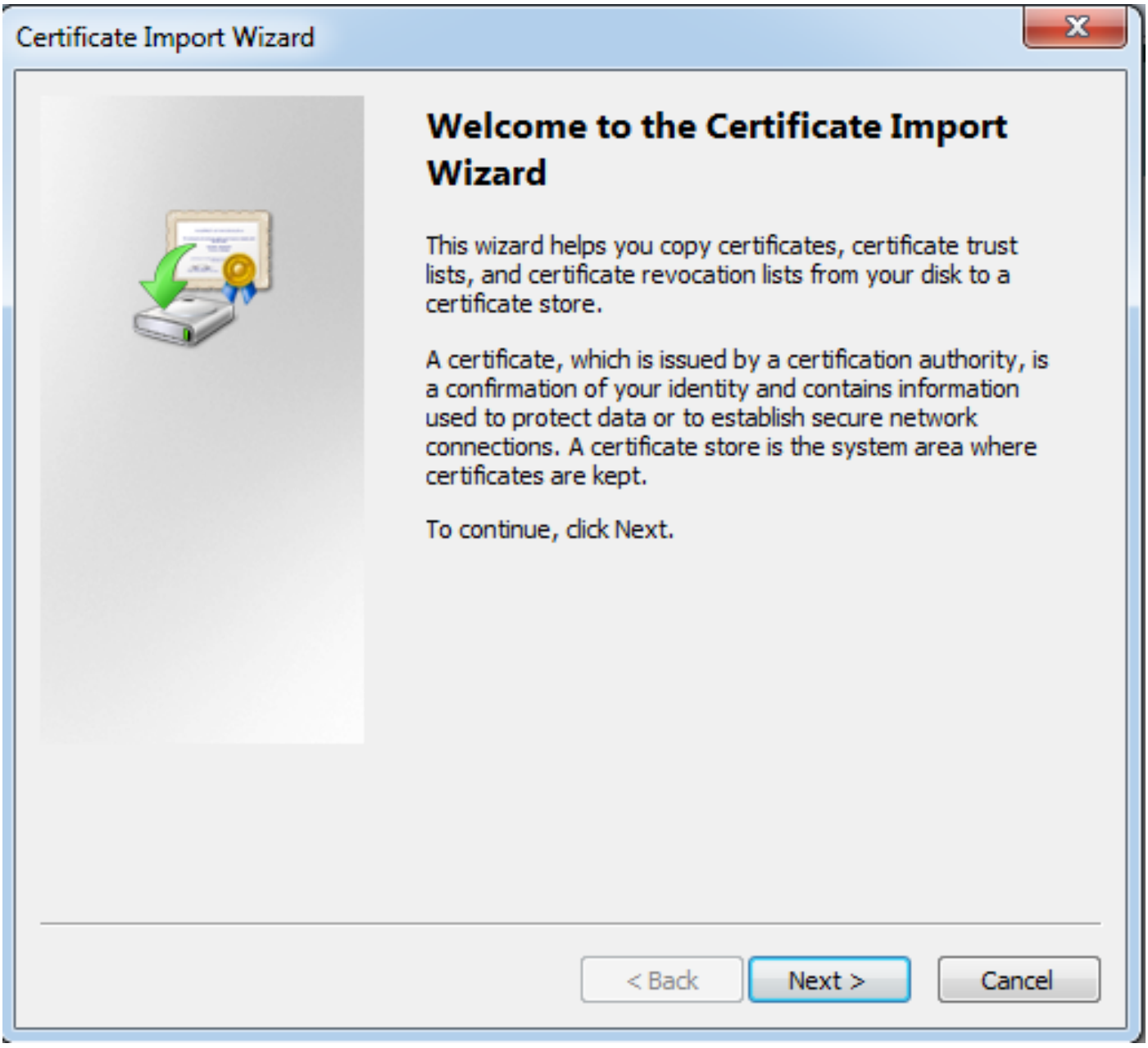
- Saisissez le nom d'utilisateur (configuré sur l'ASA à l'étape 2 , option A) et le mot de passe à usage unique, qui a été fourni par e-mail ou manuellement.



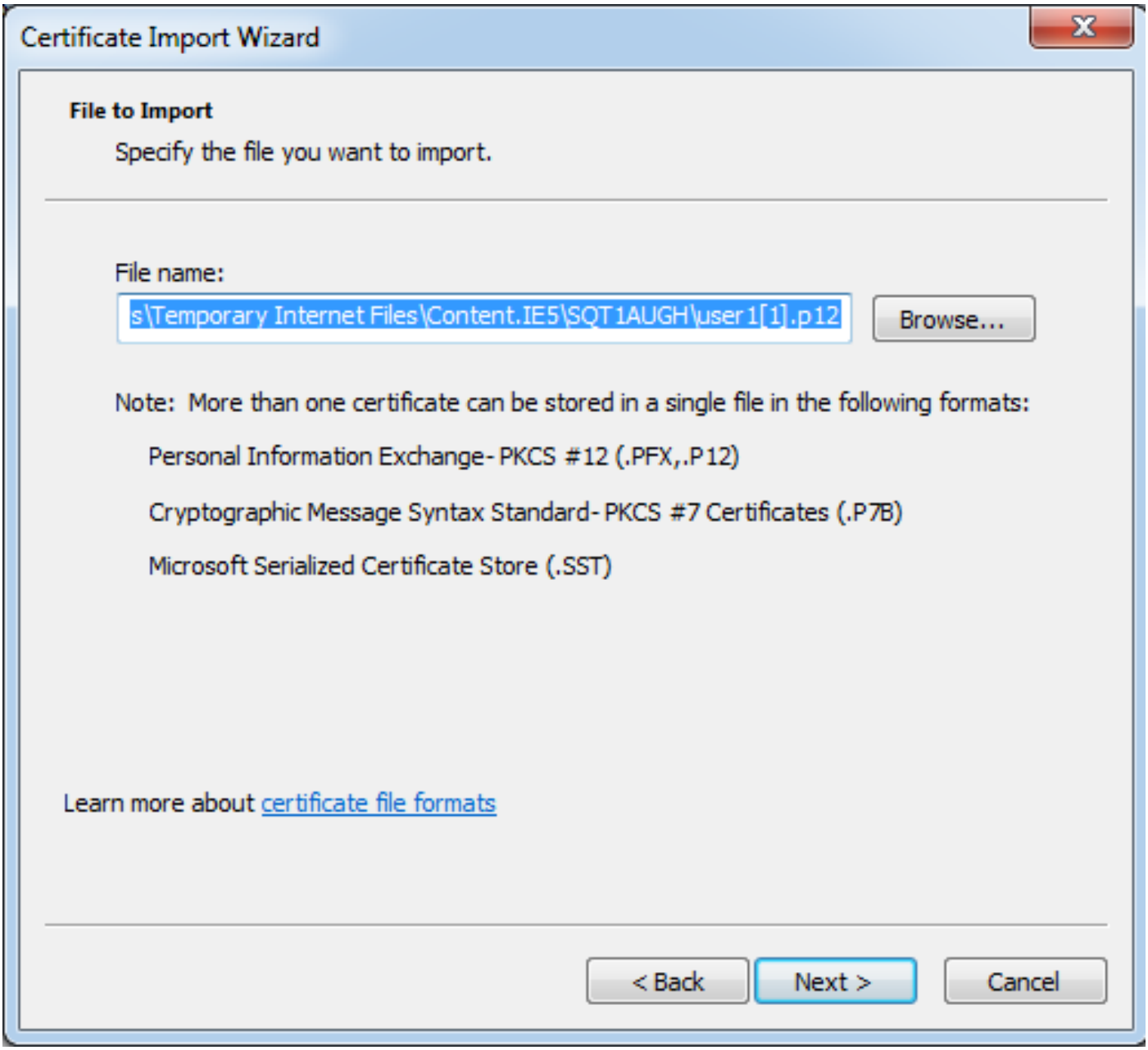
- Cliquez sur Open pour installer directement le certificat client reçu de l'ASA.
- La phrase de passe pour installer le certificat client est identique au mot de passe à usage unique reçu précédemment.



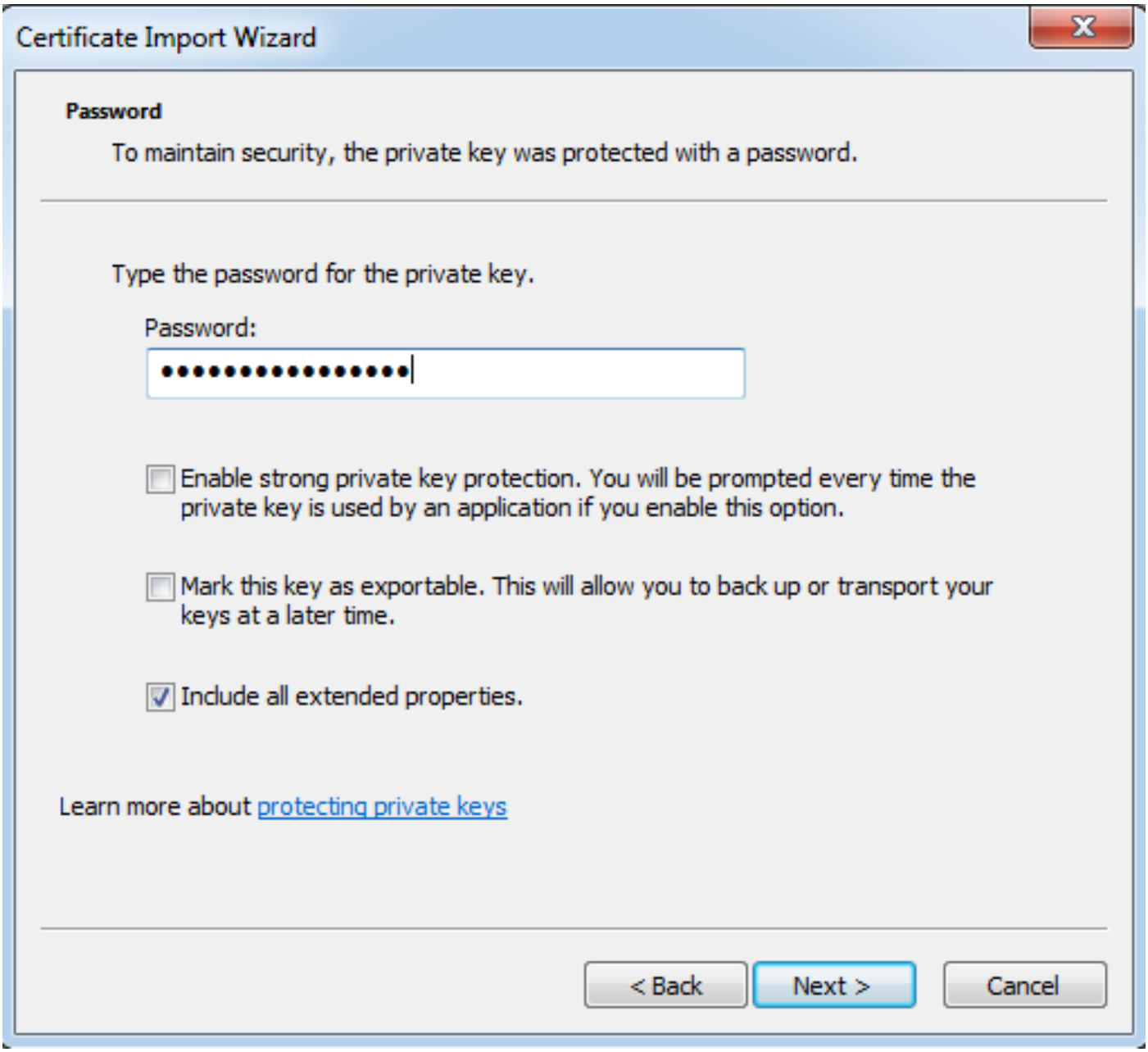
- Cliquez sur Next (Suivant).



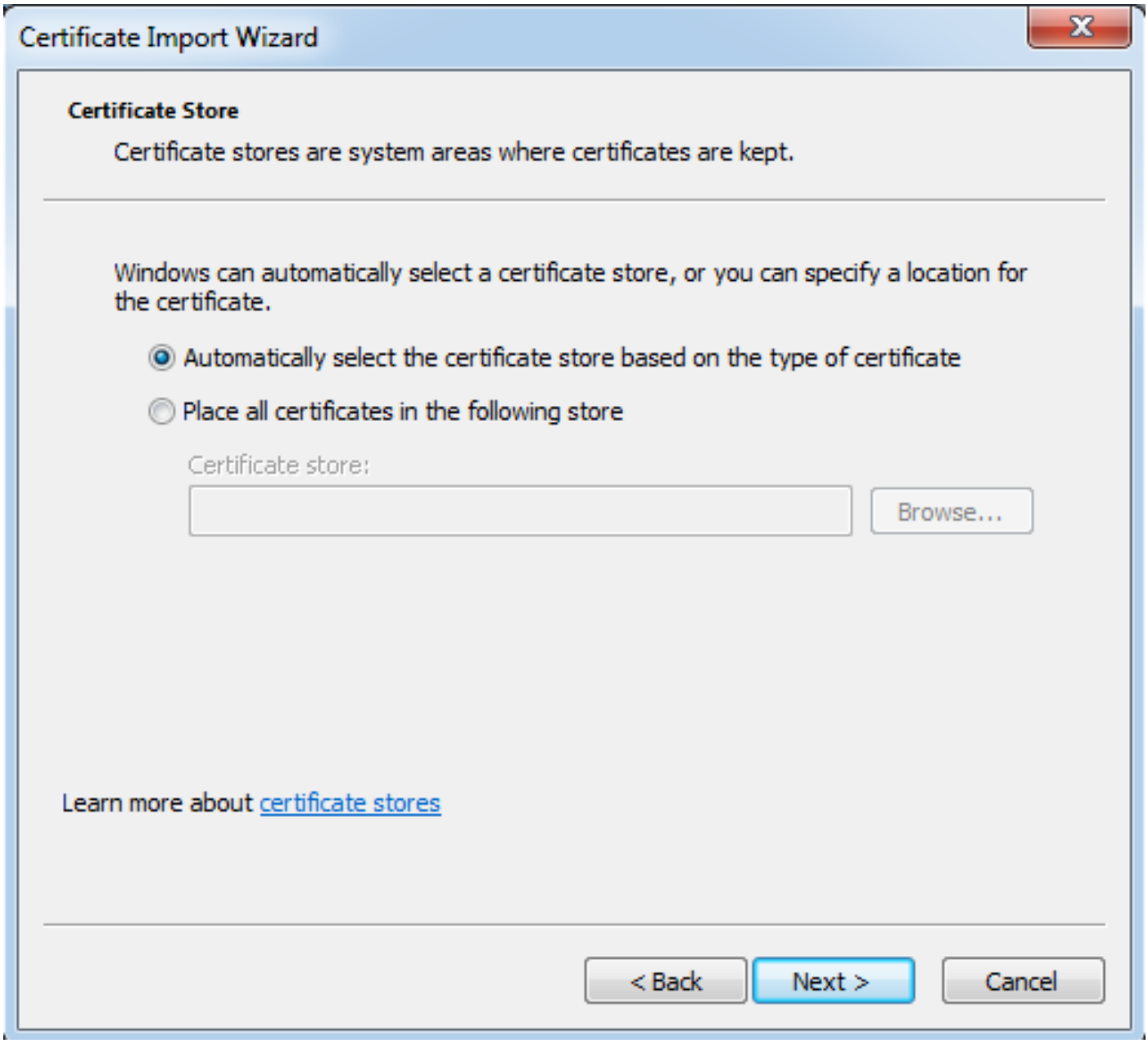
- Conservez le chemin par défaut et cliquez sur Next.



- Saisissez le mot de passe à usage unique dans le champ Mot de passe.
- Vous pouvez sélectionner l'option Marquer cette clé comme exportable afin que la clé puisse être exportée à partir de la station de travail ultérieurement si nécessaire.
- Cliquez sur Next (suivant).



- Vous pouvez installer manuellement le certificat dans un magasin de certificats particulier ou le laisser choisir automatiquement le magasin.
- Cliquez sur Next (Suivant).



- Cliquez sur Finish afin de terminer l'installation.

Certificate Import Wizard

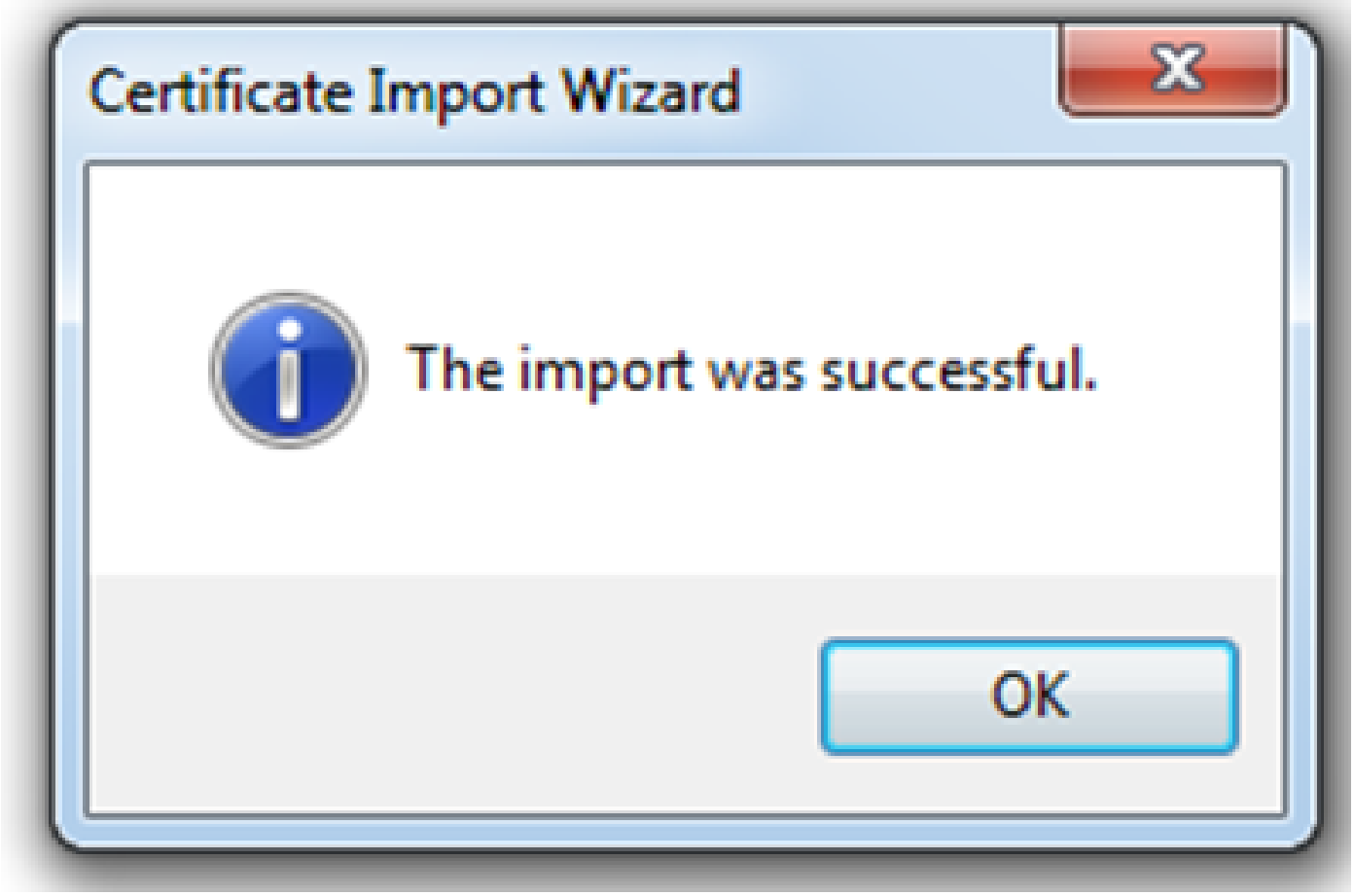
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

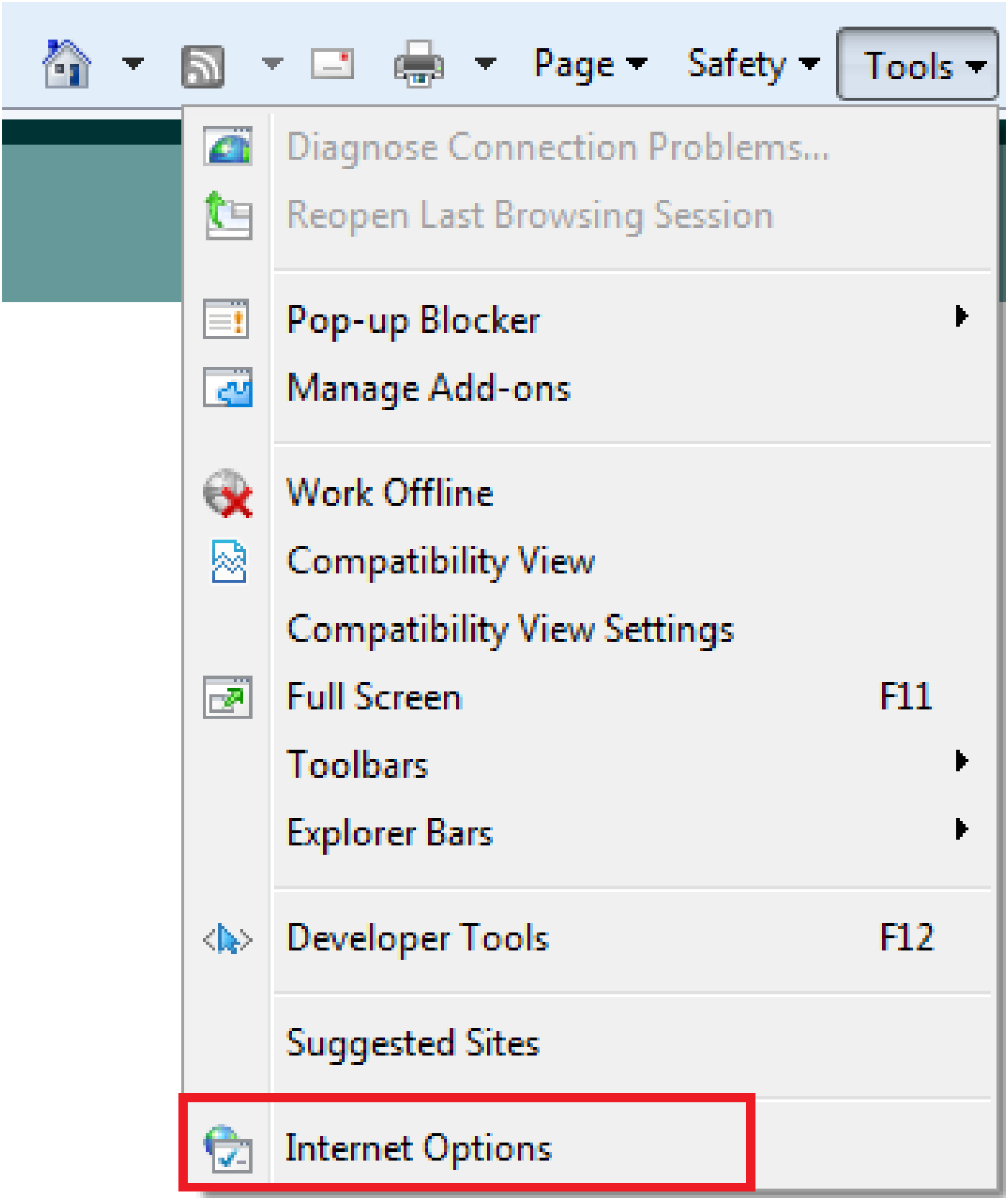
You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	PFX
File Name	C:\Users\mrsethi\AppData\Lo

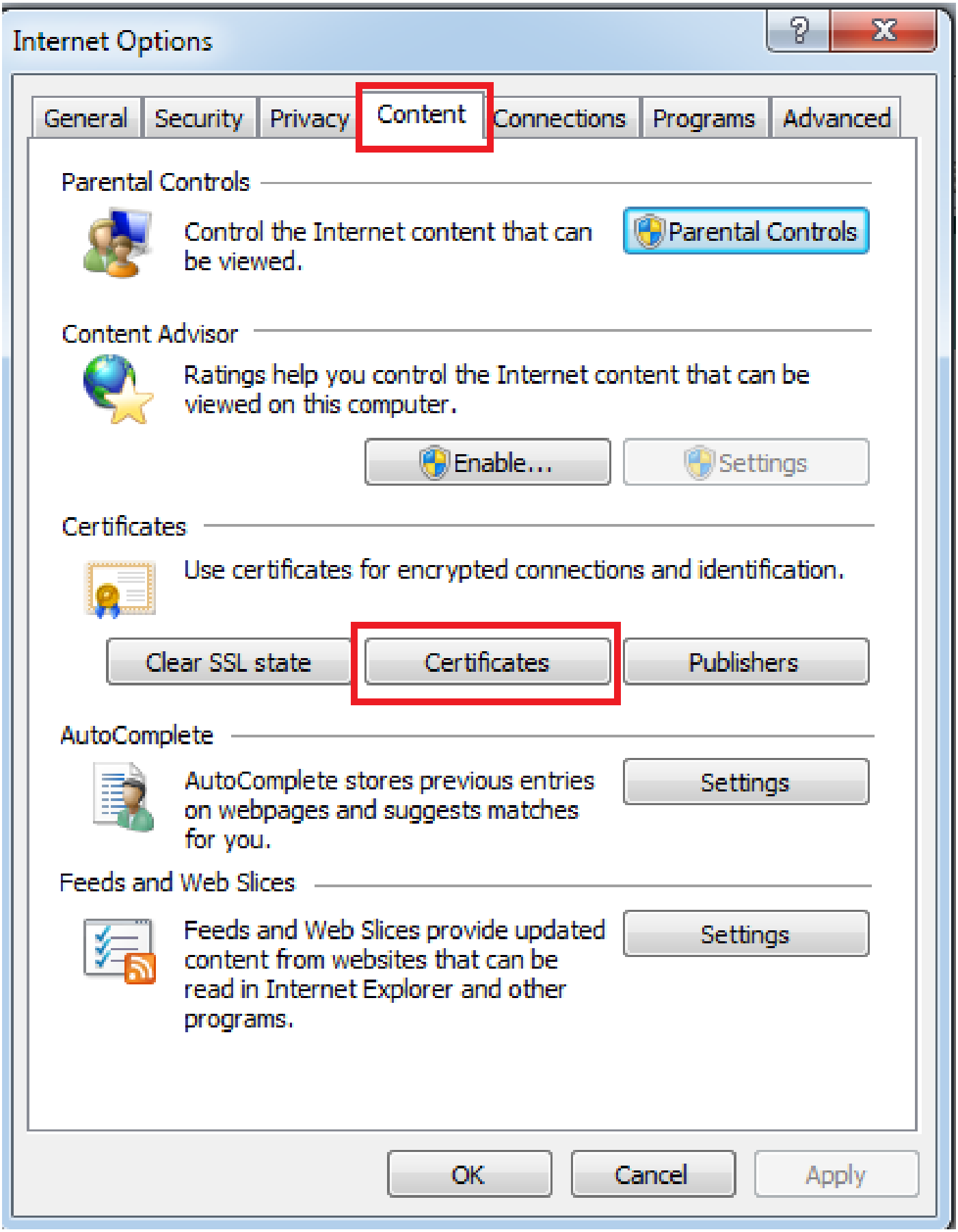
< Back | Finish | Cancel



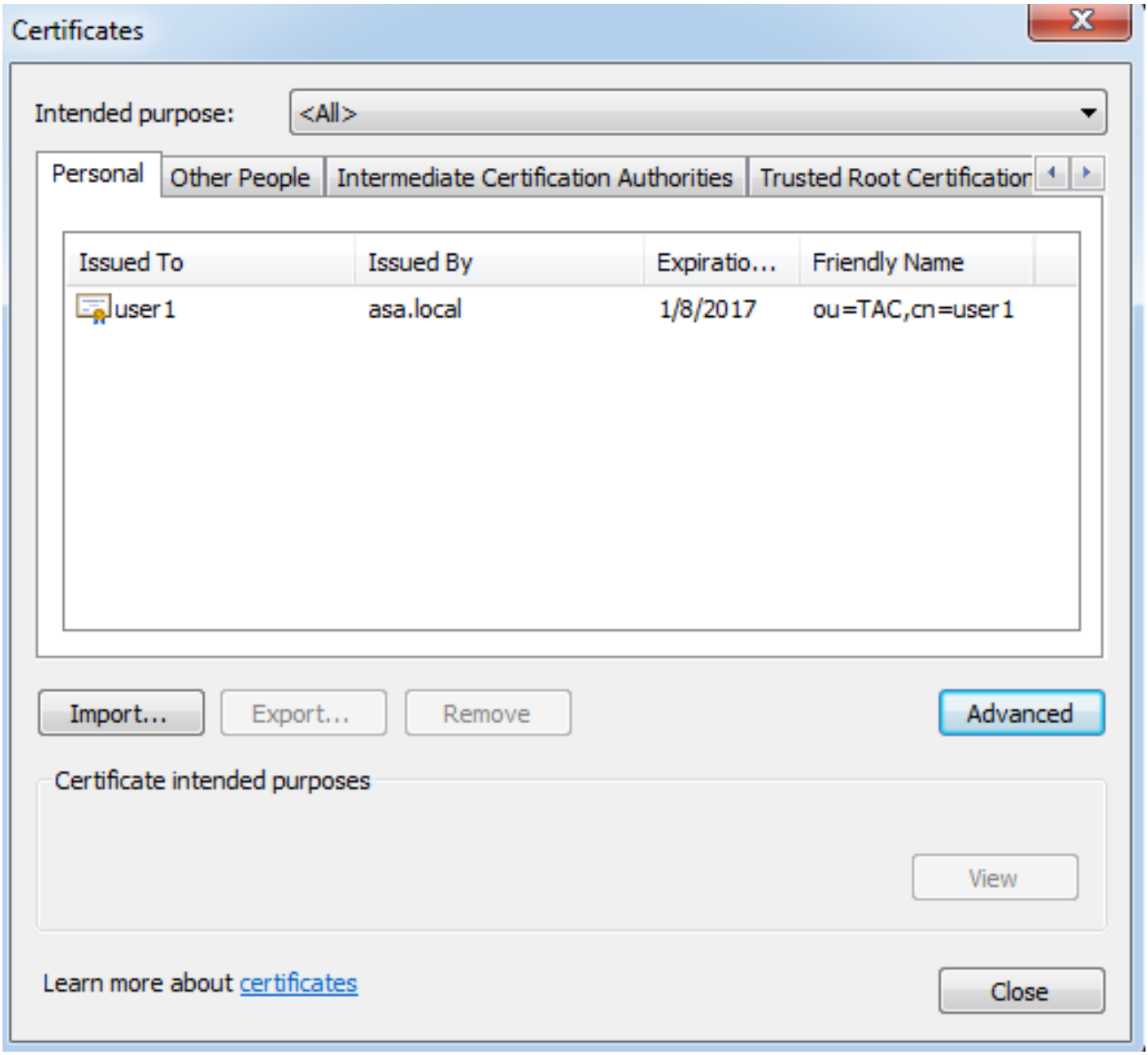
- Une fois le certificat correctement installé, vous pouvez le vérifier.
- Ouvrez IE et accédez à Outils > Options Internet.



- Accédez à l'onglet Contenu et cliquez sur Certificats, comme illustré dans cette image.



- Sous le magasin personnel, vous pouvez voir le certificat reçu de l'ASA.



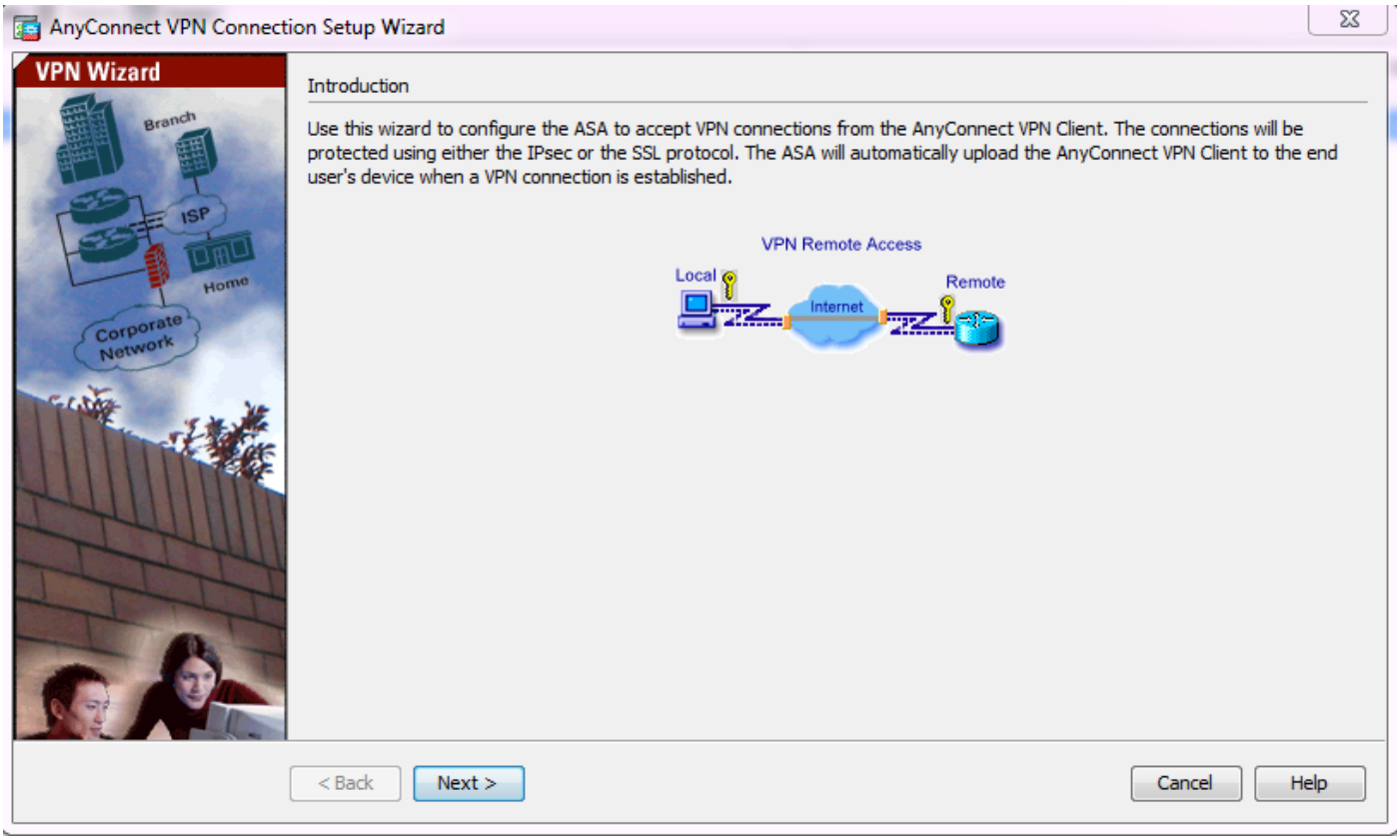
ASA en tant que passerelle SSL pour les clients AnyConnect

Assistant de configuration AnyConnect par ASDM

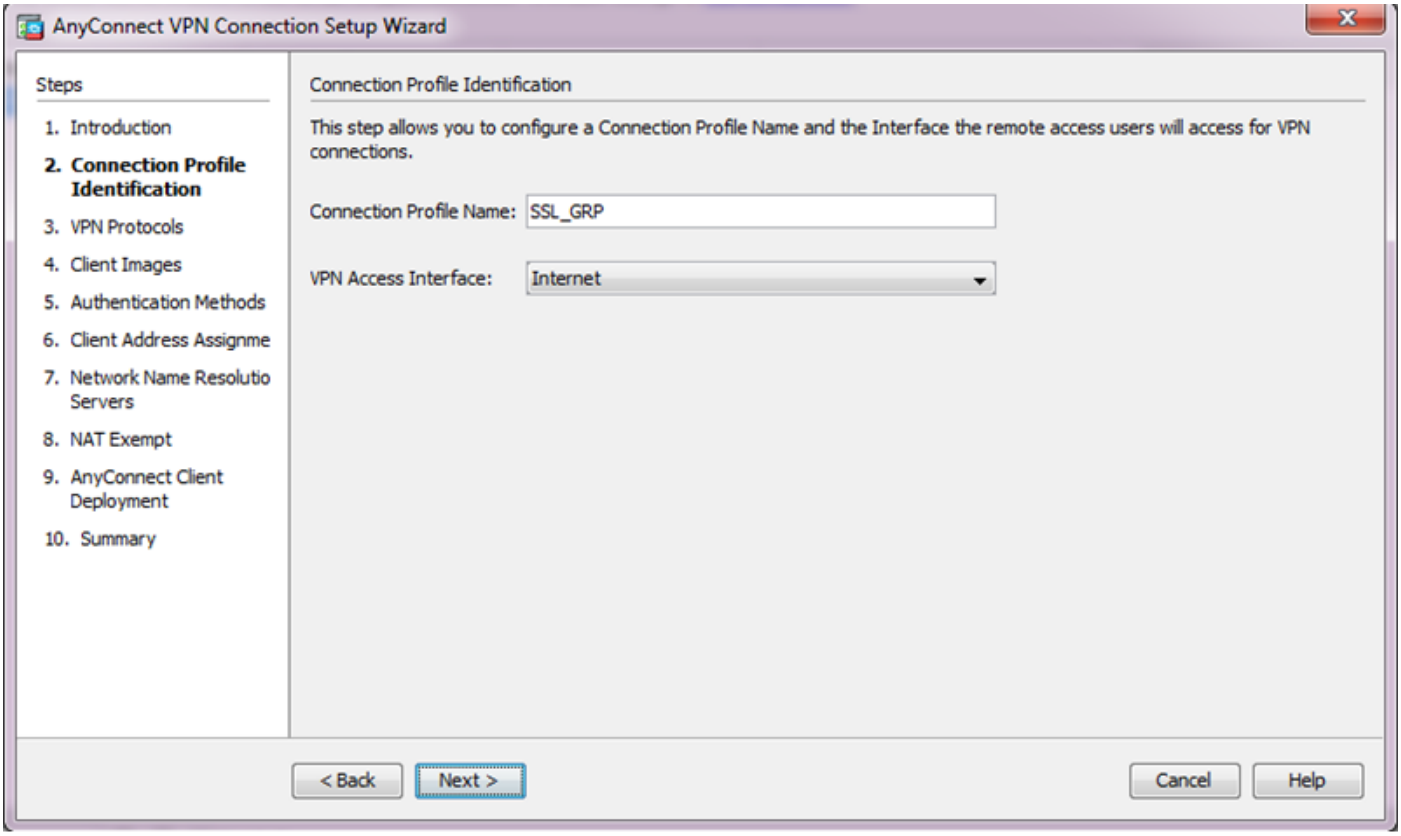
L'interface de ligne de commande/Assistant de configuration AnyConnect peut être utilisée pour configurer le client AnyConnect Secure Mobility. Assurez-vous qu'un paquet client AnyConnect a été chargé sur le disque ou la mémoire flash du pare-feu ASA avant de poursuivre.

Suivez ces étapes pour configurer le client pour la mobilité sécurisée AnyConnect avec l'aide de l'assistant de configuration :

1. Connectez-vous à ASDM et accédez à Wizards > VPN Wizards > AnyConnect VPN Wizard pour lancer l'assistant de configuration et cliquez sur Next.



2. Entrez le nom du profil de connexion, choisissez l'interface sur laquelle le VPN sera arrêté dans le menu déroulant VPN Access Interface, et cliquez sur Next.



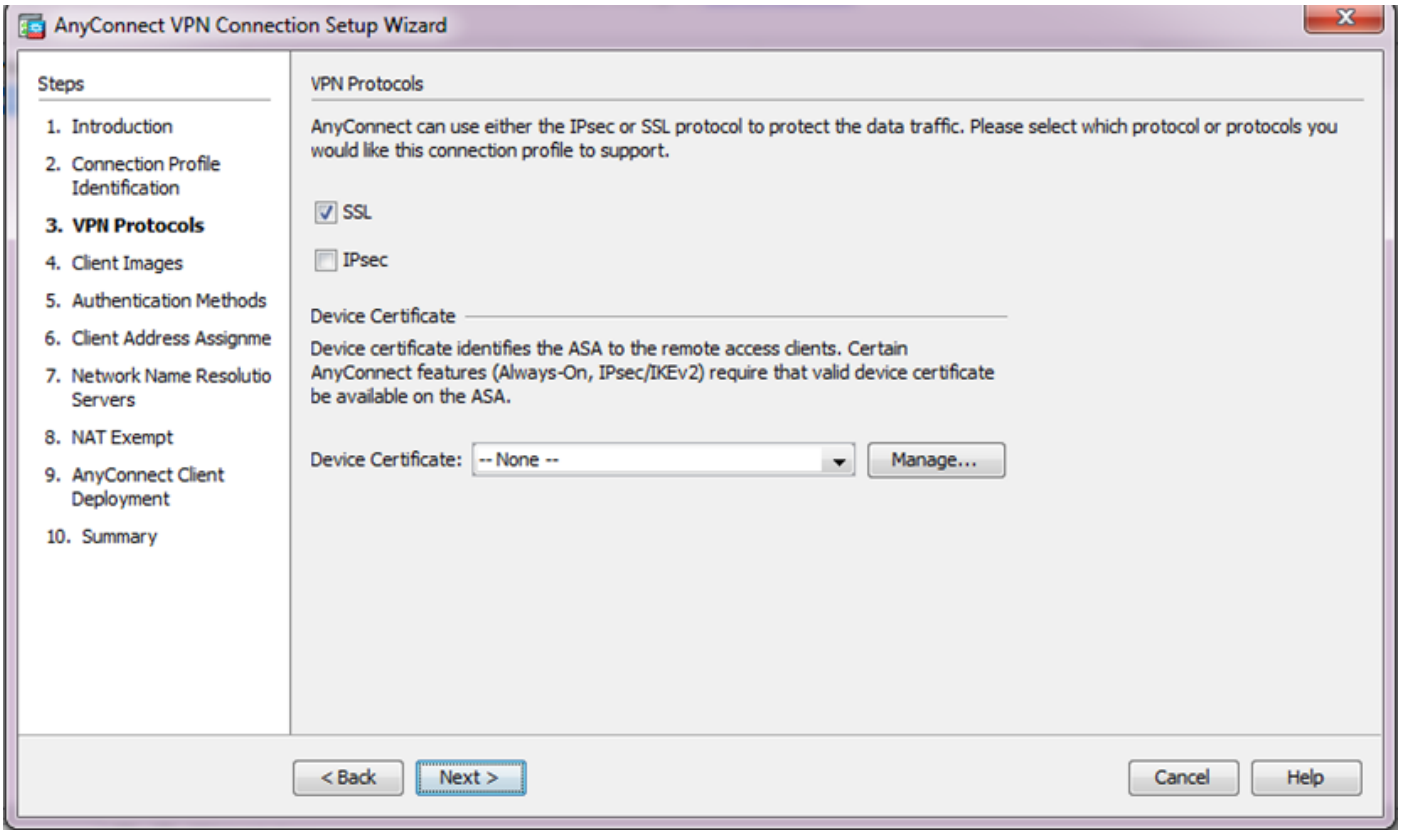
3. Cochez la case SSL afin d'activer le protocole SSL (Secure Sockets Layer). Le certificat de périphérique peut être un certificat émis par une autorité de certification (CA) tierce de confiance (p. ex., Verisign ou Entrust) ou un certificat autosigné. Si le certificat est déjà installé sur l'ASA,

vous pouvez alors le sélectionner dans le menu déroulant.

1. Remarque : ce certificat est le certificat côté serveur qui sera présenté par ASA aux clients SSL. Si aucun certificat de serveur n'est actuellement installé sur l'ASA, un certificat auto-signé doit être généré, puis cliquez sur Manage.

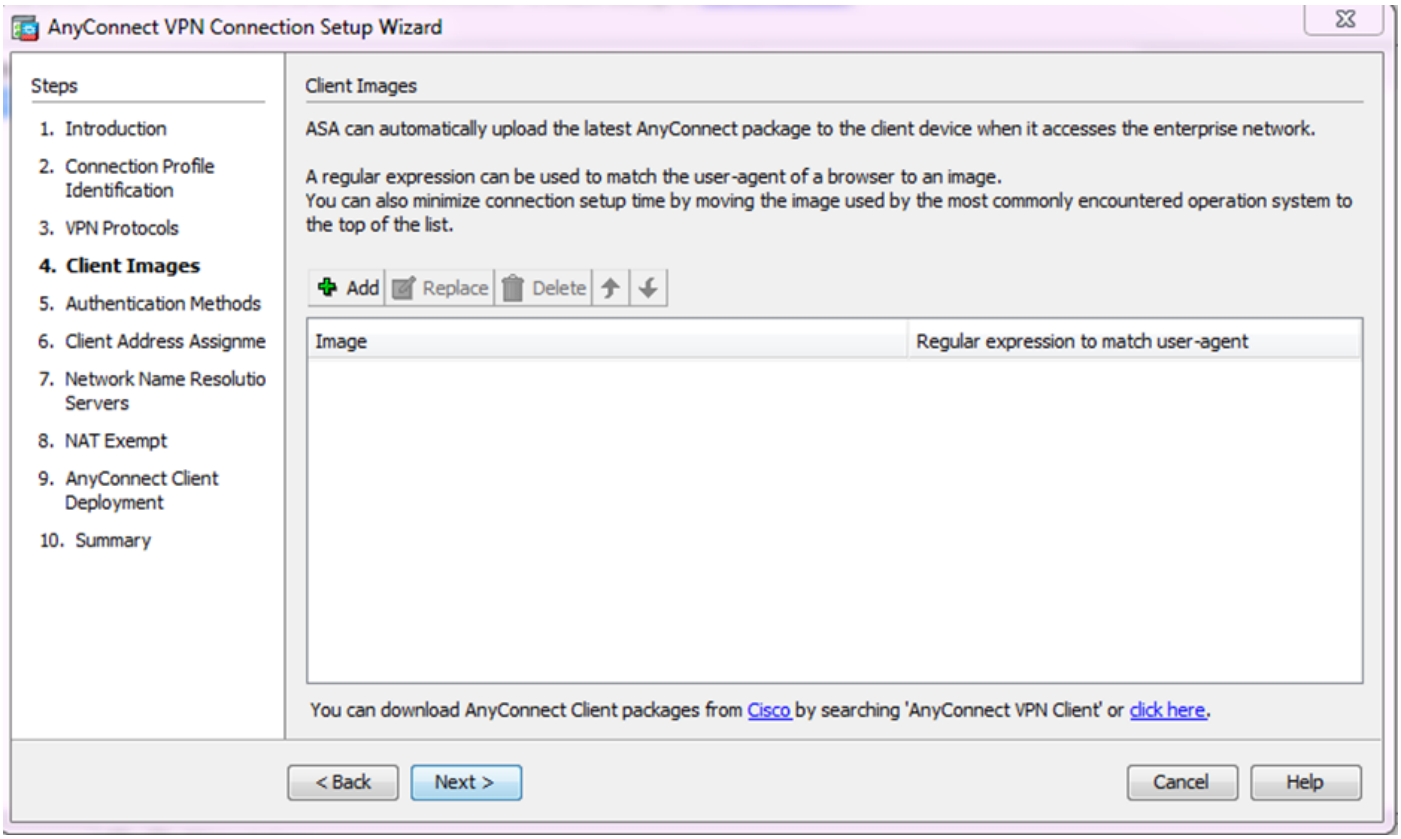
   Afin d'installer un certificat d'un tiers, suivez les étapes indiquées dans le document contenant l'exemple de configuration d'ASA 8.x visant à installer manuellement des certificats de fournisseurs tiers, à utiliser avec WebVPN.

   - Activez les protocoles VPN et le certificat de périphérique.
   - Cliquez sur Next (Suivant).

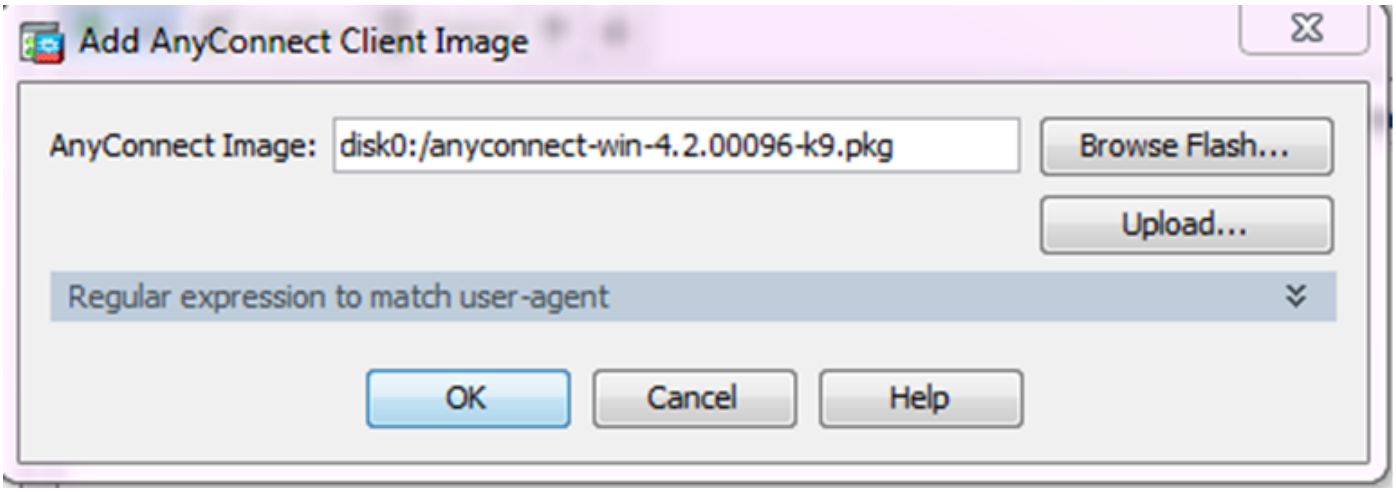


4. Cliquez sur Add afin d'ajouter le package client AnyConnect (fichier .pkg) à partir du lecteur local ou de la mémoire flash/disque de l'ASA.

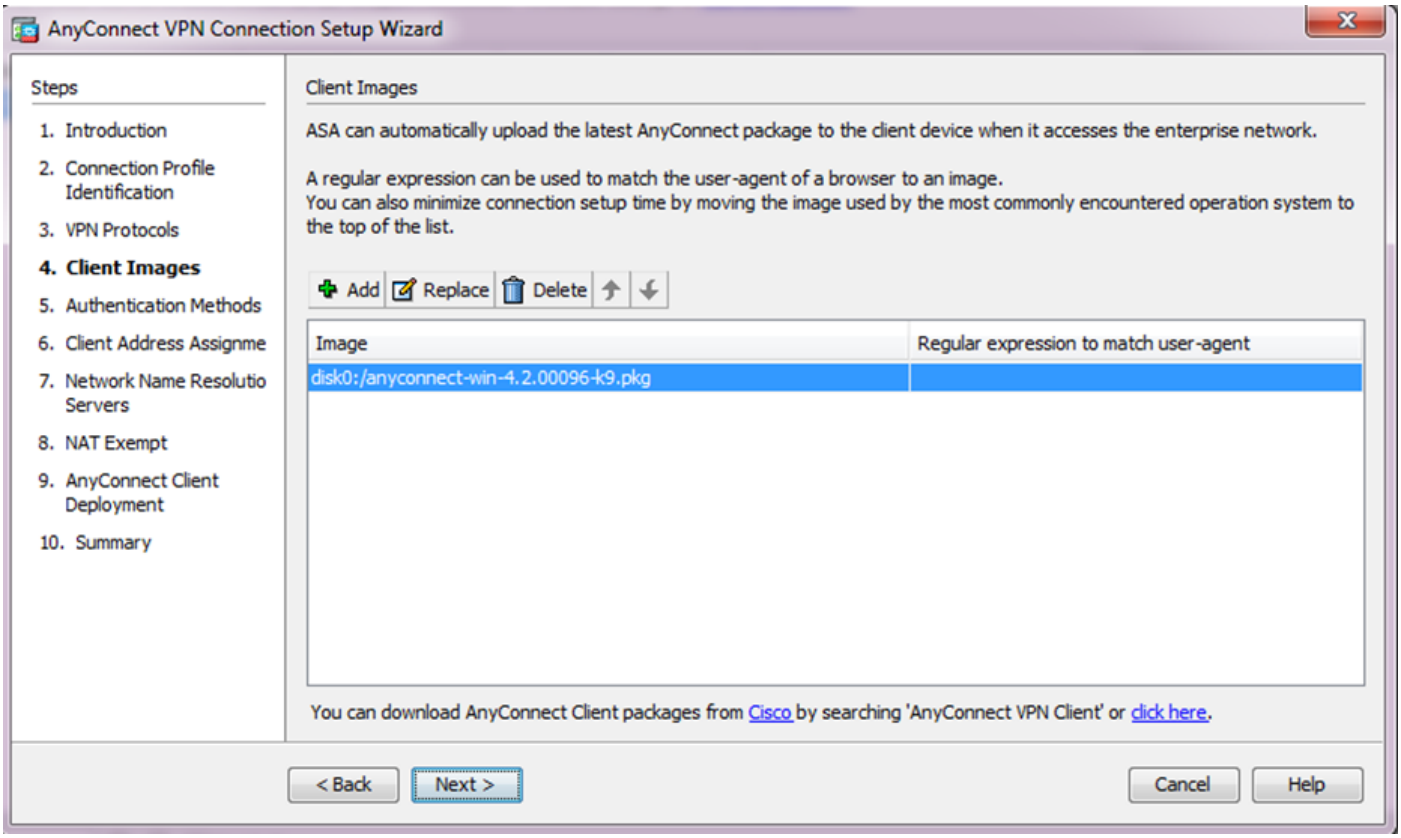
Cliquez sur Browse Flash afin d'ajouter l'image à partir du lecteur flash, ou cliquez sur Upload afin d'ajouter l'image à partir du lecteur local de l'ordinateur hôte.



- Vous pouvez télécharger le fichier AnyConnect.pkg à partir de la mémoire flash/disque ASA (si le package existe déjà) ou du lecteur local.
- Browse flash : pour sélectionner le package AnyConnect à partir du Flash/Disque ASA.
- Téléchargement : pour sélectionner le package AnyConnect à partir du lecteur local de l'ordinateur hôte.
- Click OK.

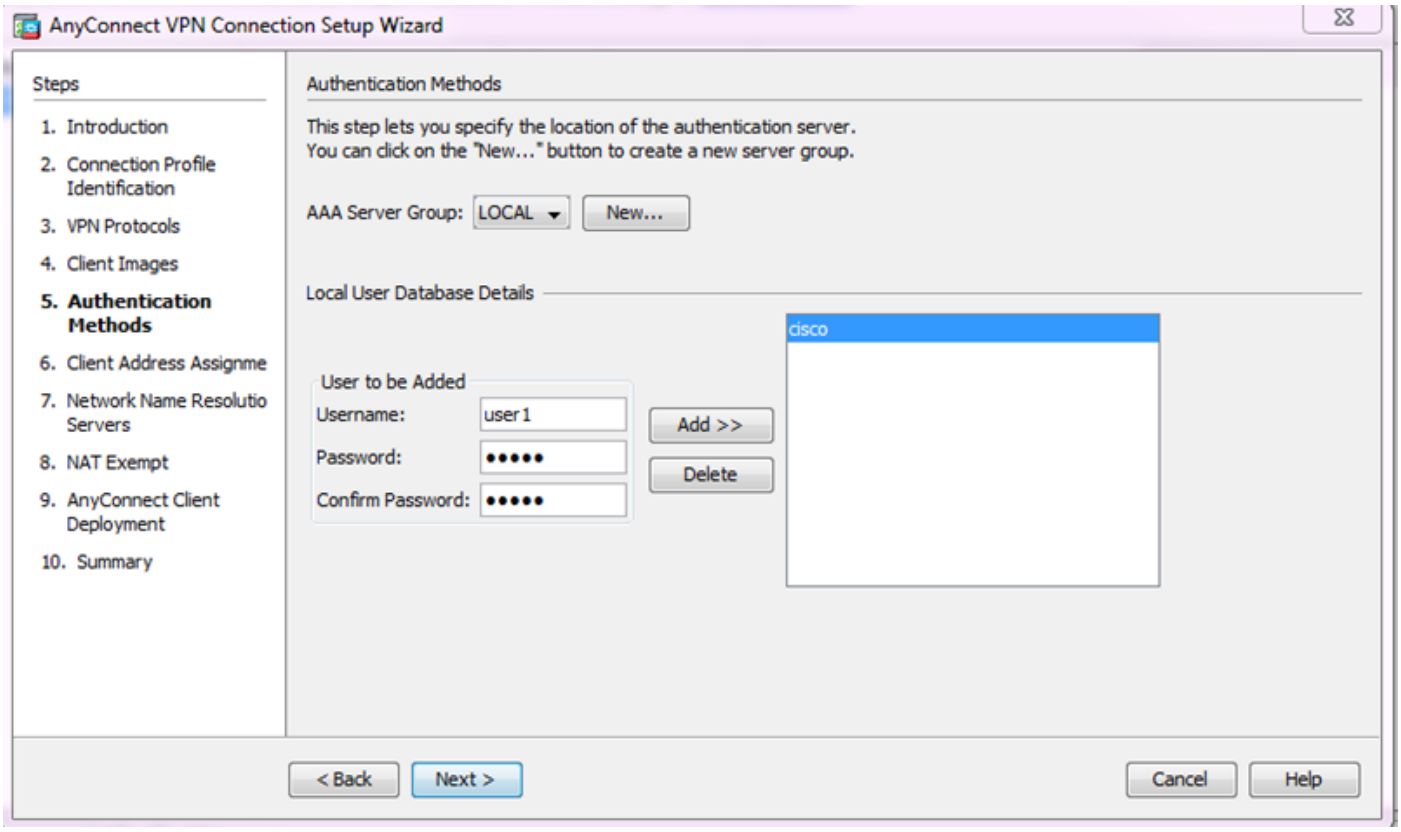


- Cliquez sur Next (Suivant).

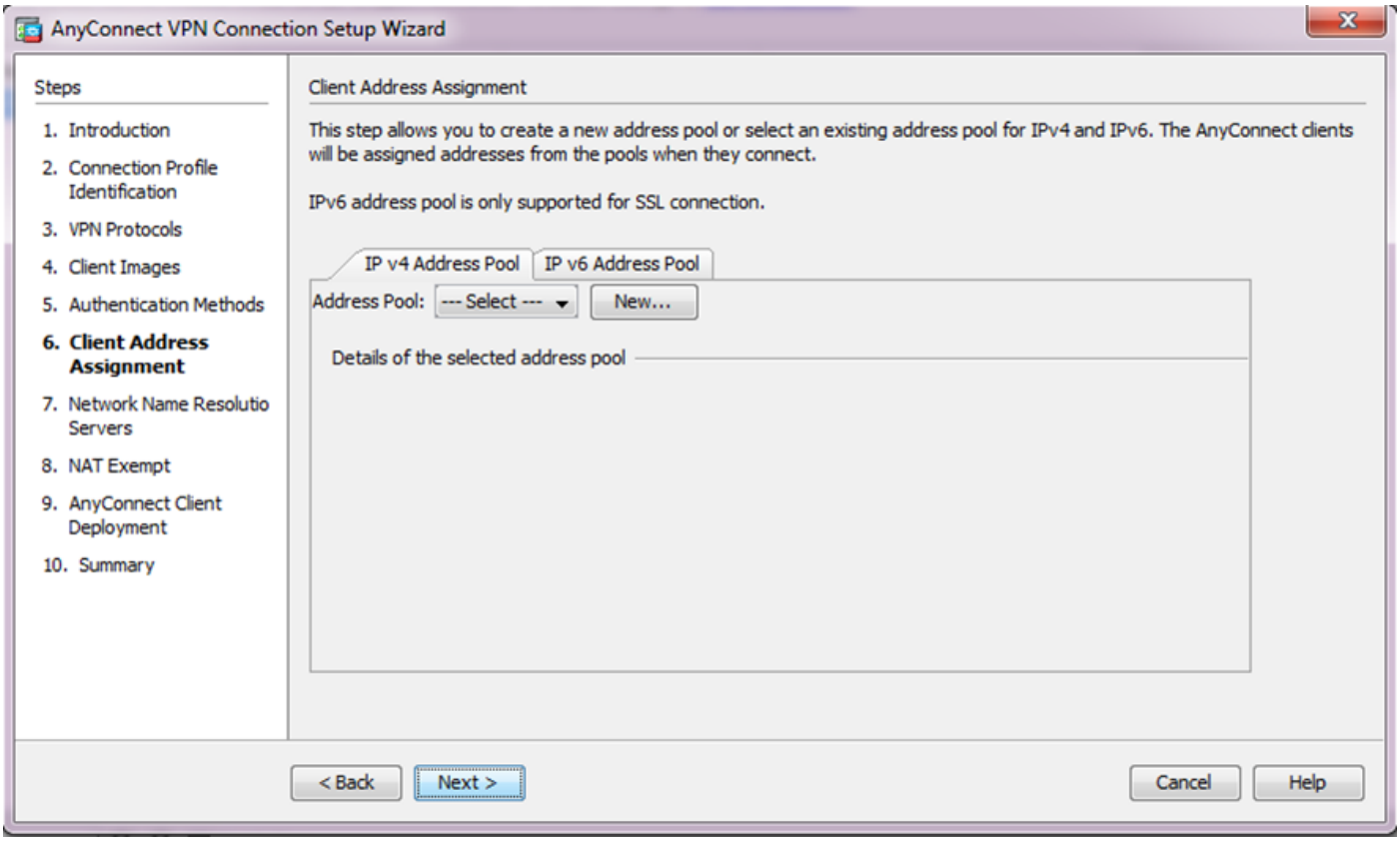


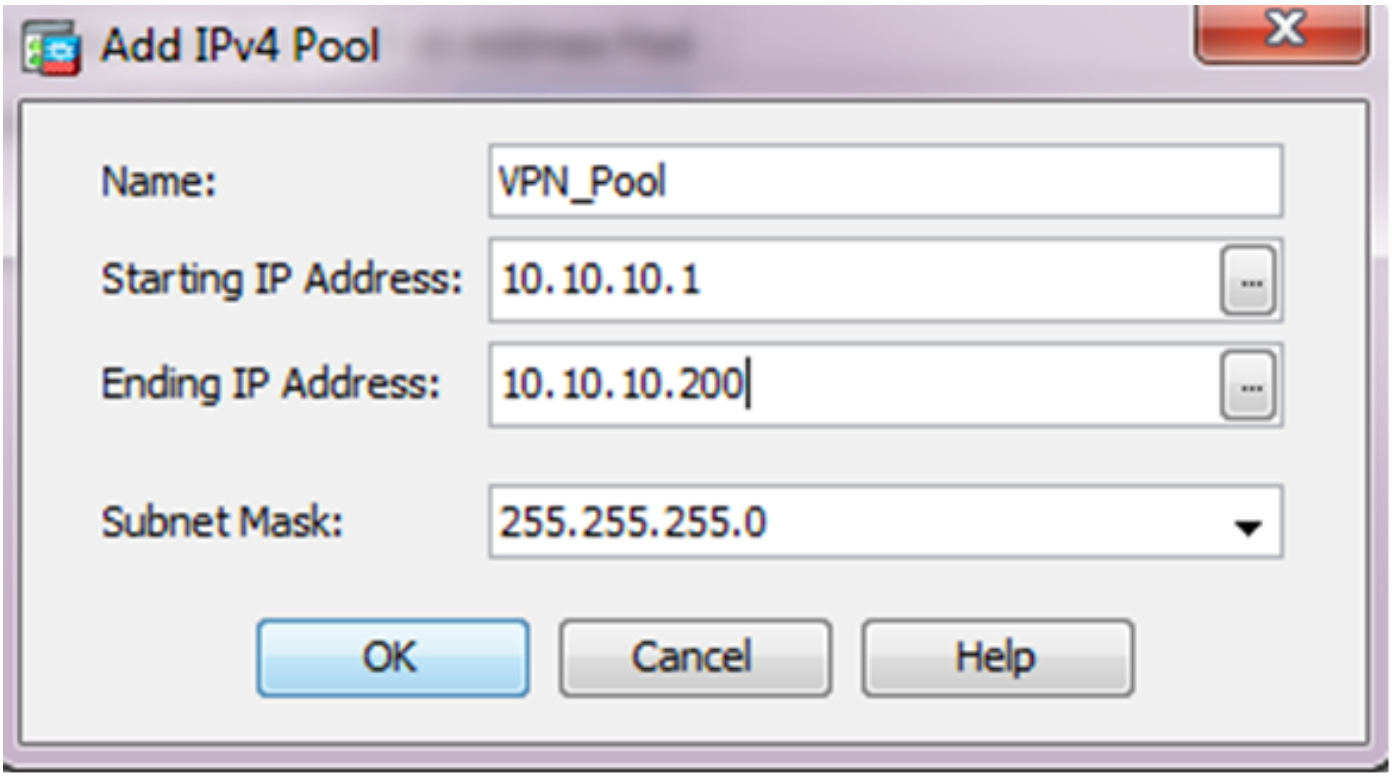
5. L'authentification de l'utilisateur peut être effectuée via les groupes de serveurs AAA (Authentication, Authorization, and Accounting). Si les utilisateurs sont déjà configurés, choisissez LOCAL, puis cliquez sur Next [suivant]. Sinon, ajoutez un utilisateur à la base de données utilisateur locale et cliquez sur Suivant.

Remarque : dans cet exemple, l'authentification LOCAL est configurée, ce qui signifie que la base de données d'utilisateurs locaux sur l'ASA sera utilisée pour l'authentification.

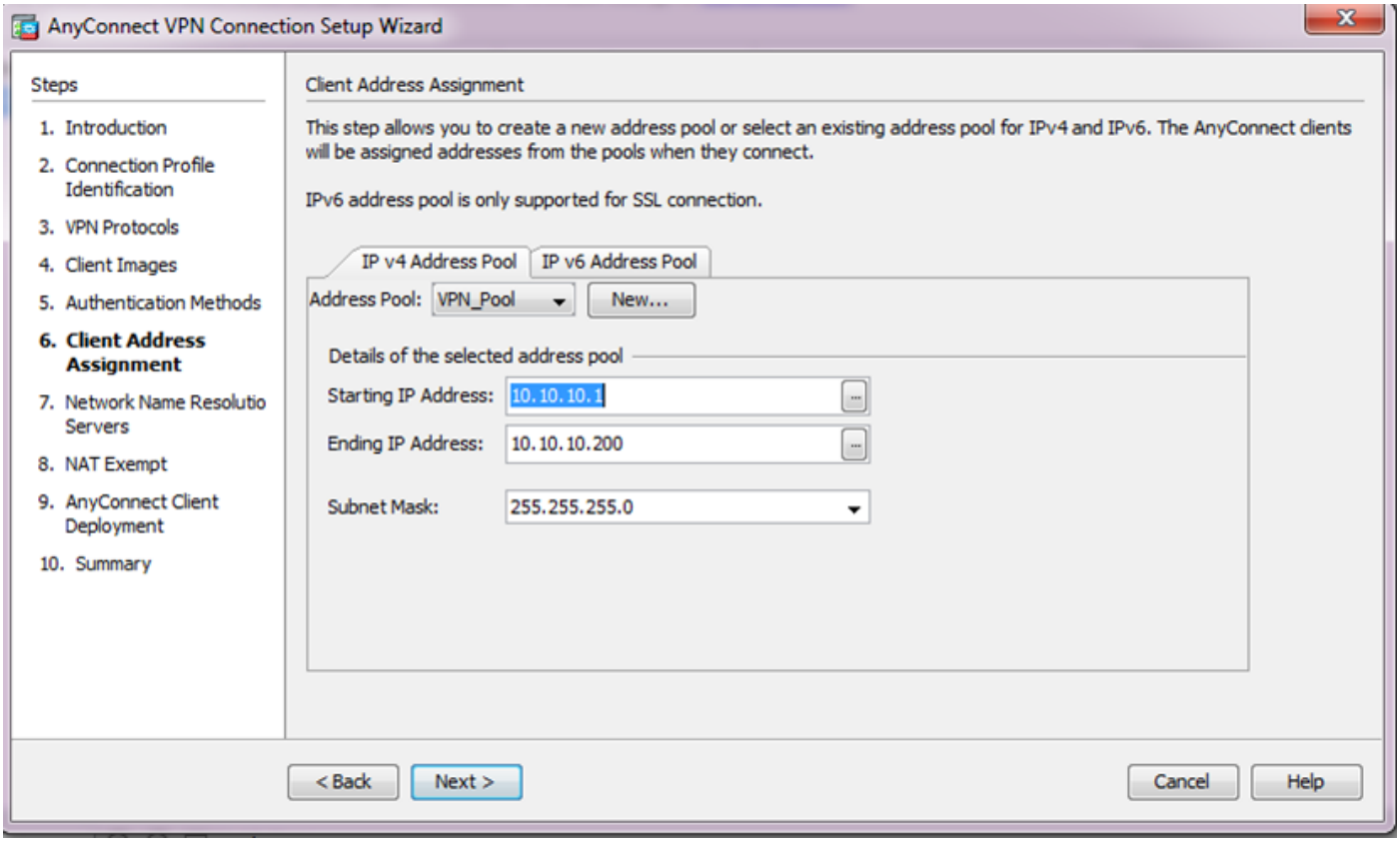


6. Assurez-vous que le pool d'adresses pour les clients VPN est configuré. Si un pool d'adresses IP est déjà configuré, sélectionnez-le dans le menu déroulant. Si ce n'est pas le cas, cliquez sur New afin de configurer. Une fois terminé, cliquez sur Next.

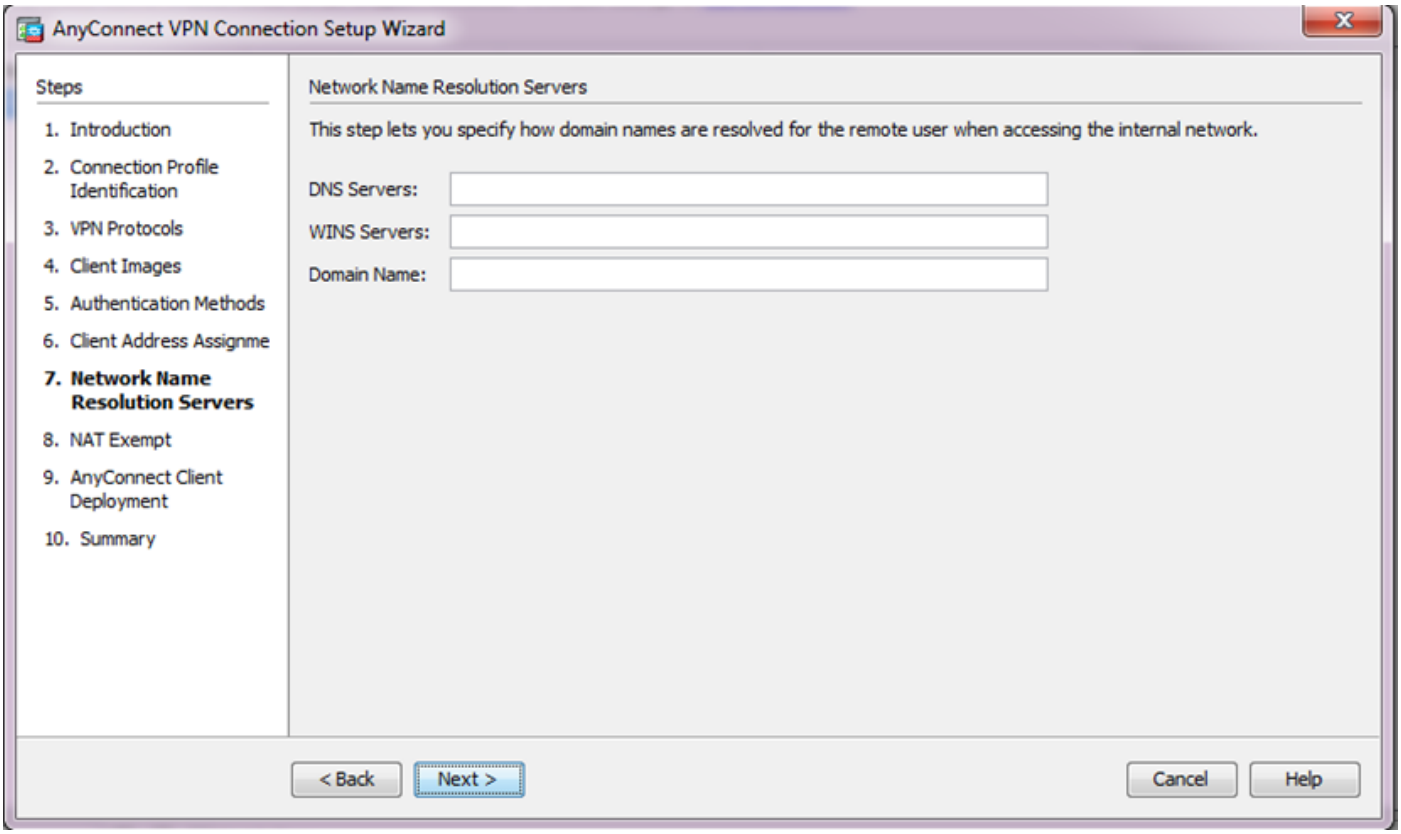




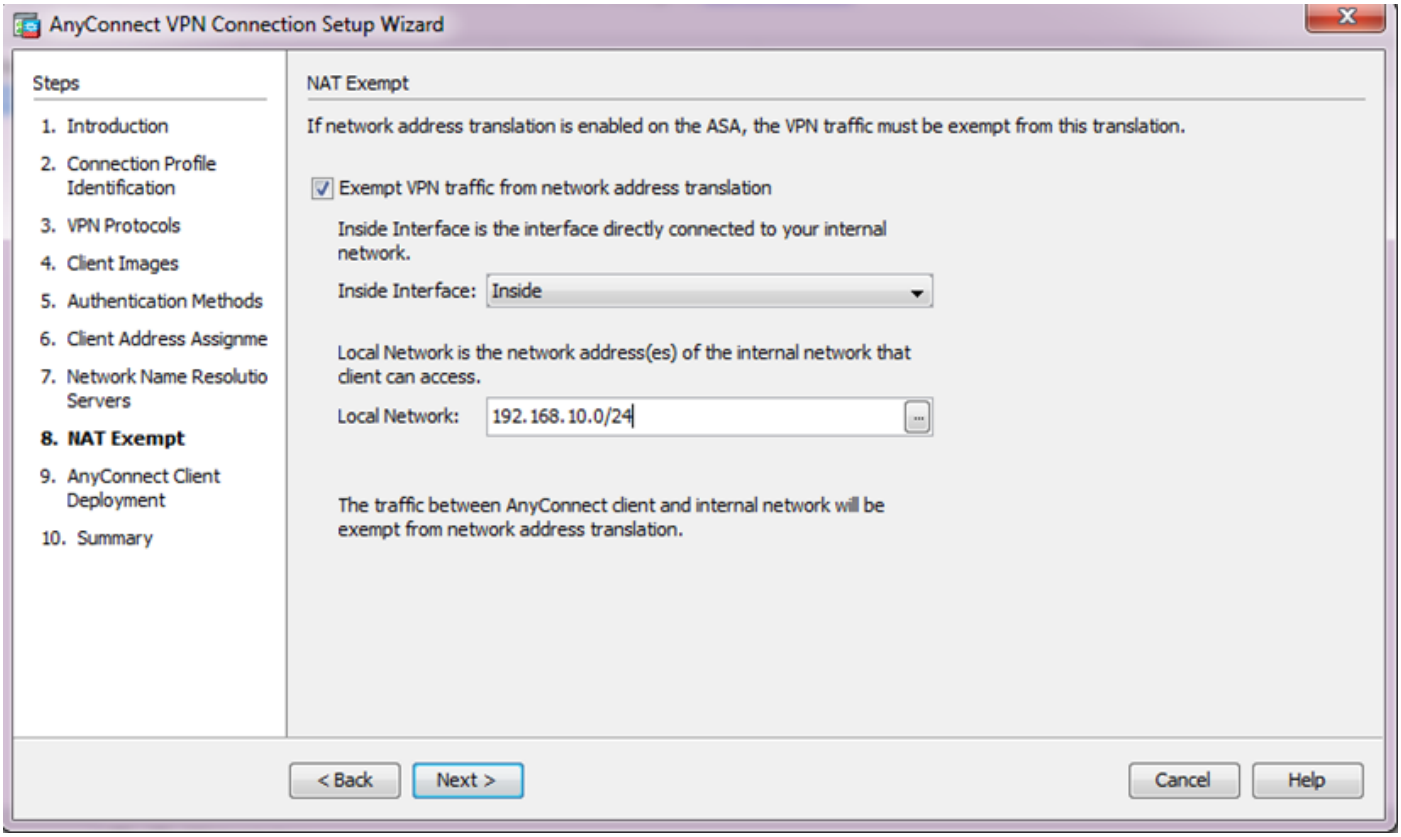
- Cliquez sur Next (Suivant).



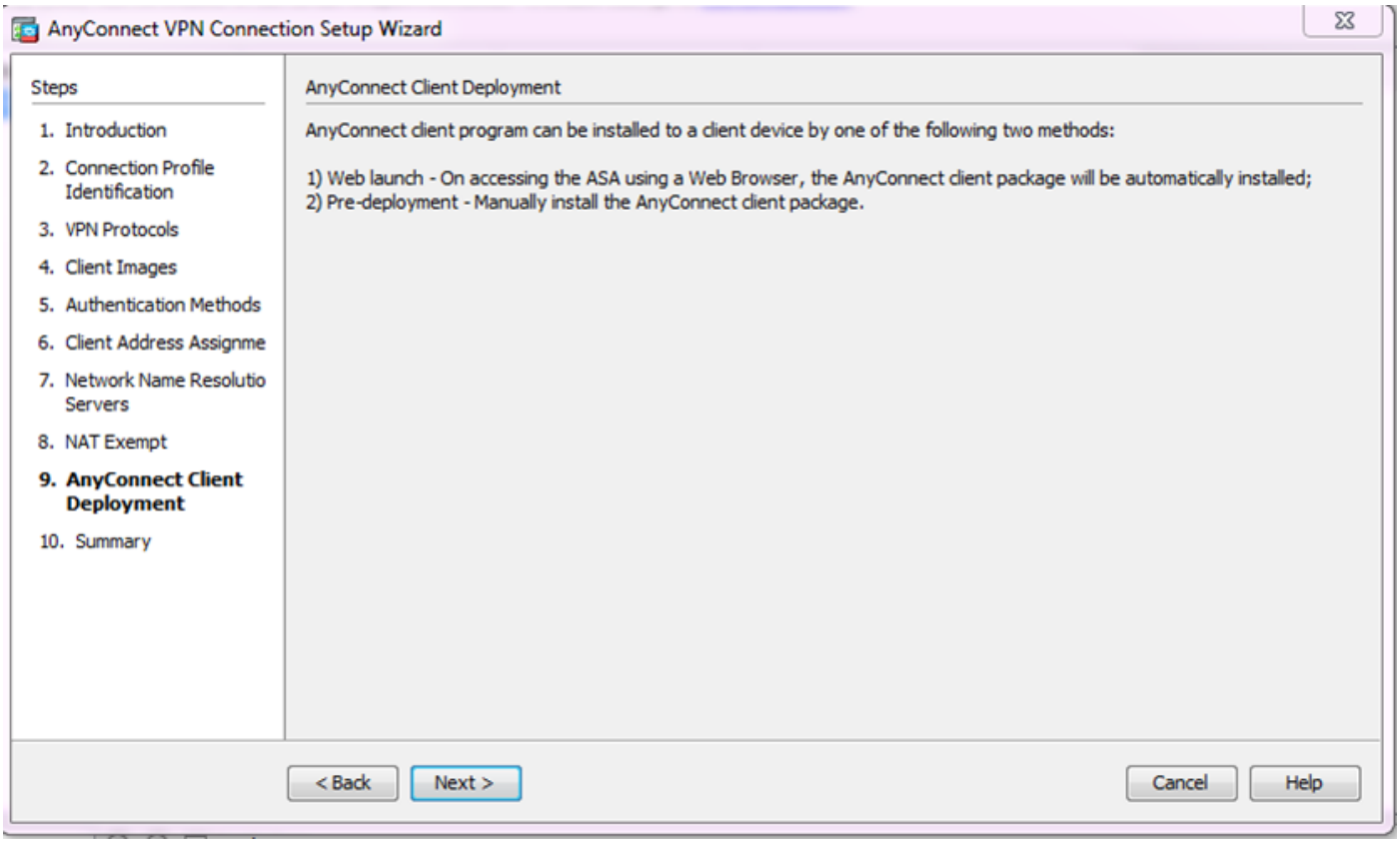
7. Le cas échéant, configurez les serveurs et les noms de domaine DNS (Domain Name System) dans les champs DNS et Domain Name, puis cliquez sur Next.



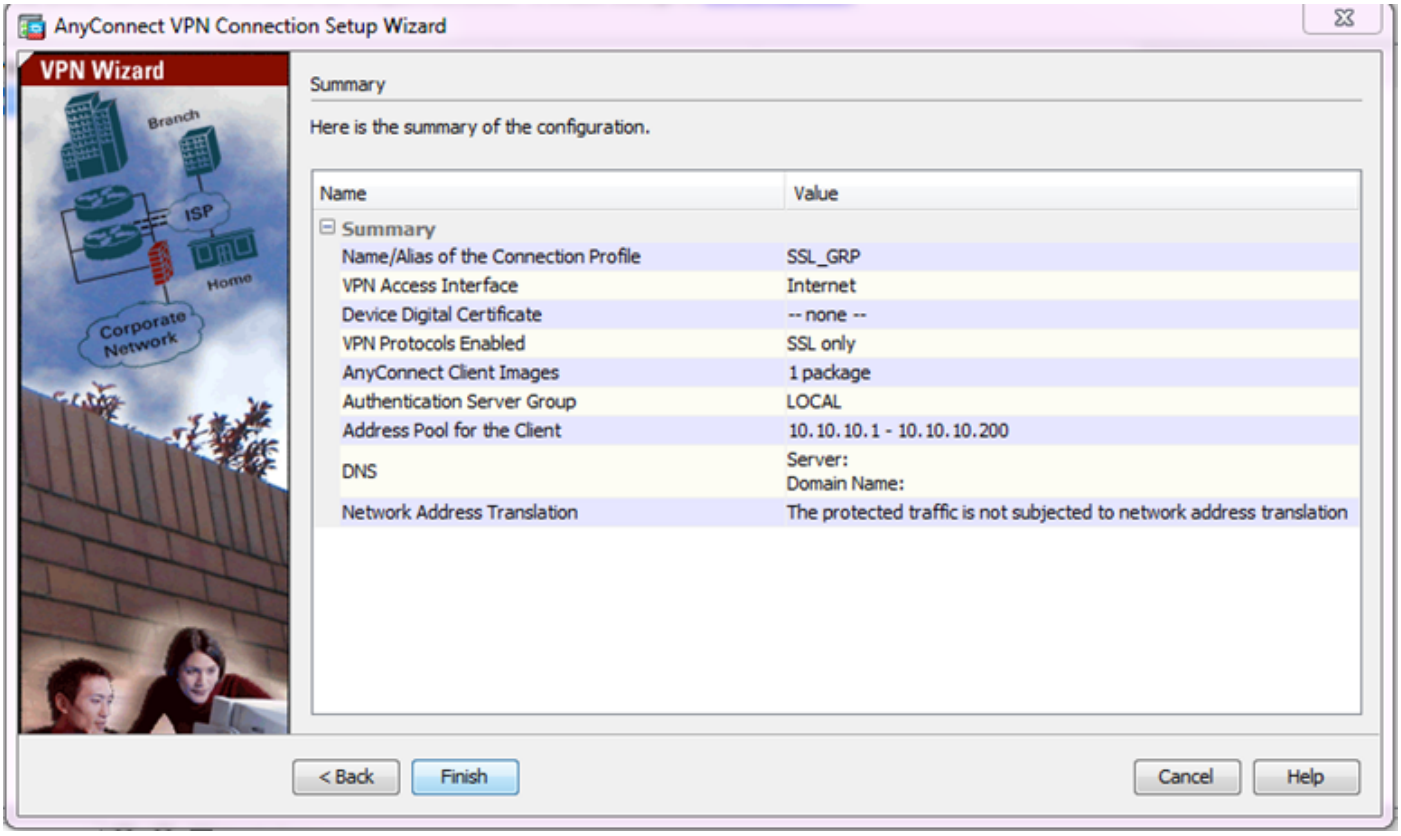
8. Assurez-vous que le trafic entre le client et le sous-réseau interne doit être exempté de toute traduction d'adresses de réseau (NAT) dynamique. Activez la case à cocher Exempt VPN traffic from network address translation et configurez l'interface LAN qui sera utilisée pour l'exemption. Spécifiez également le réseau local qui doit être exempté et cliquez sur Next.



9. Cliquez sur Suivant.



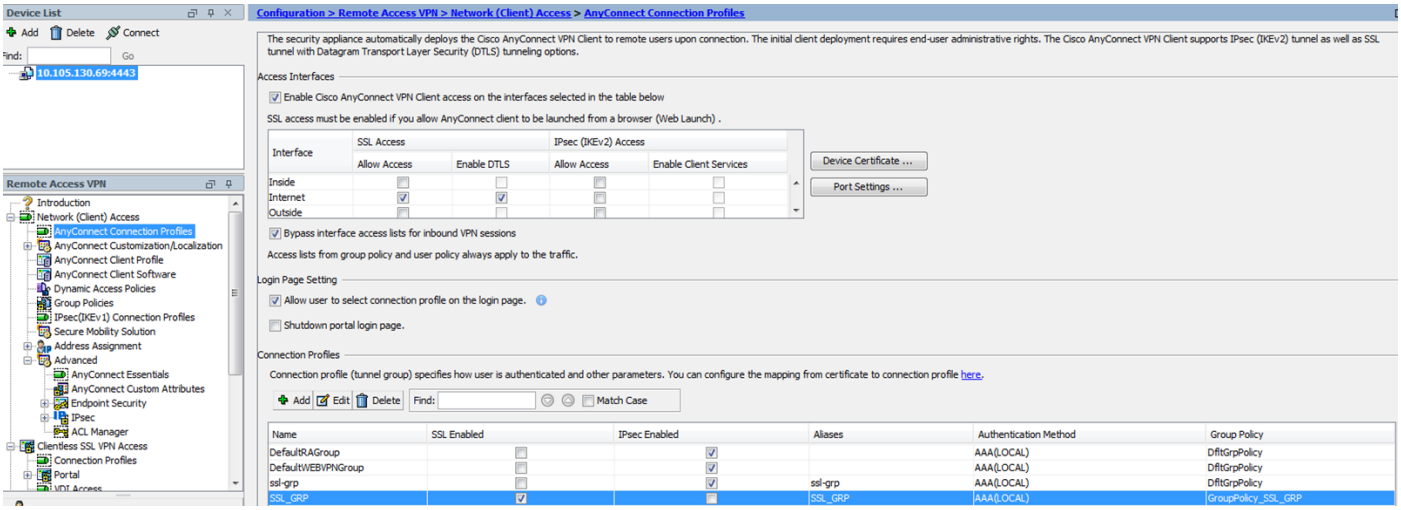
10. La dernière étape affiche le résumé, cliquez sur Terminer pour terminer la configuration.



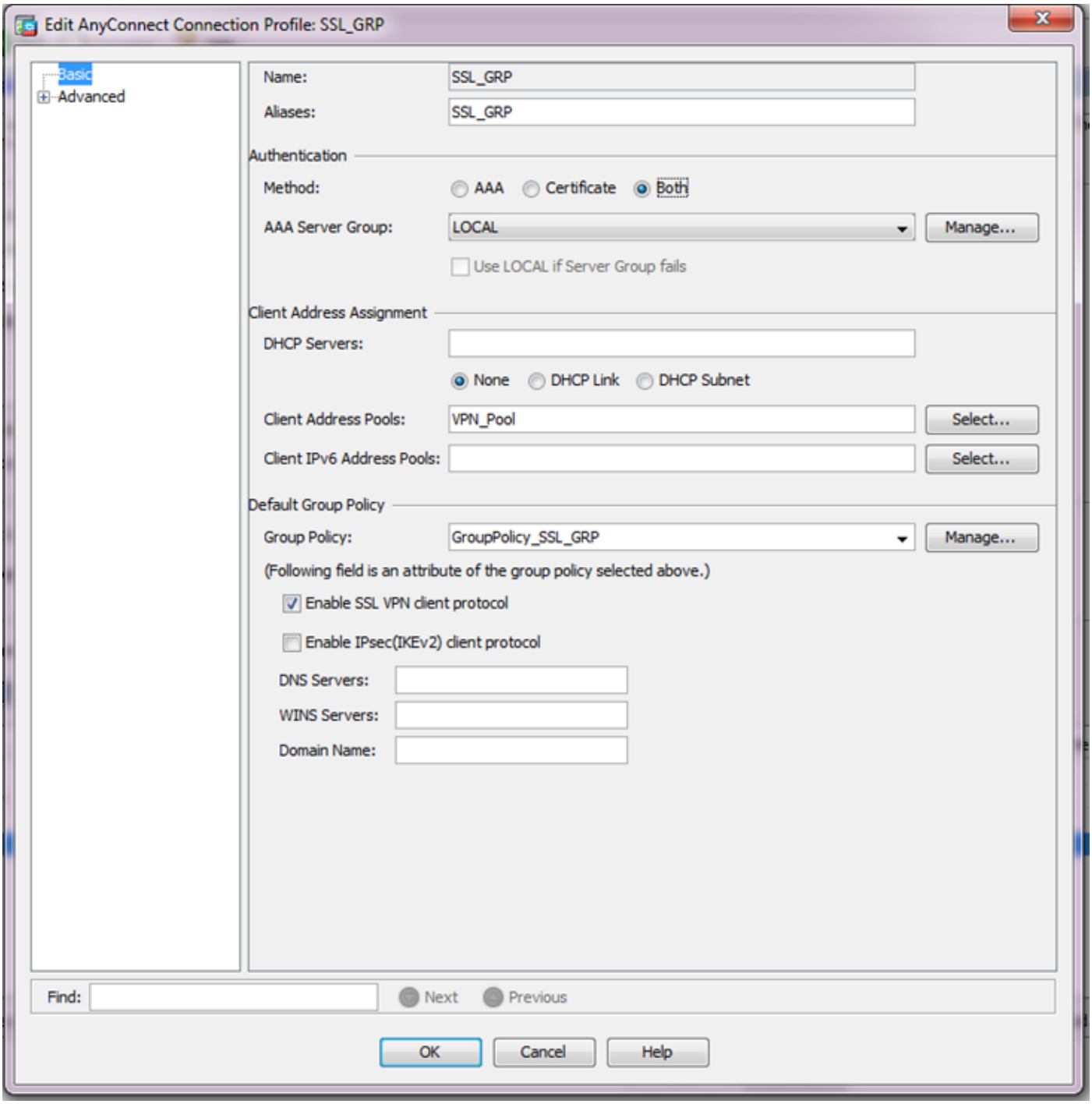
Vous avez terminé la configuration du client AnyConnect. Cependant, lorsque vous configurez AnyConnect via l'Assistant de configuration, il configure la méthode d'authentification AAA par défaut. Afin d'authentifier les clients via des certificats et un nom d'utilisateur/mot de passe, le tunnel-group (profil de connexion) doit être configuré pour utiliser des certificats et AAA comme

méthode d'authentification.

- Accédez à Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles.
- Le nouveau profil de connexion SSL_GRP ajouté devrait s'afficher.



- Afin de configurer AAA et l'authentification de certificat, sélectionnez le profil de connexion SSL_GRP et cliquez sur Edit.
- Sous Authentication Method, sélectionnez Both.



Configuration de CLI pour AnyConnect

<#root>

```
!! *****Configure the VPN Pool*****

ip local pool VPN_Pool 10.10.10.1-10.10.10.200 mask 255.255.255.0

!! *****Configure Address Objects for VPN Pool and Local Network*****

object network NETWORK_OBJ_10.10.10.0_24
 subnet 10.10.10.0 255.255.255.0
```

```
object network NETWORK_OBJ_192.168.10.0_24
 subnet 192.168.10.0 255.255.255.0
 exit


!! *****Configure WebVPN*****



webvpn
 enable Internet
 anyconnect image disk0:/anyconnect-win-4.2.00096-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
 exit


!! *****Configure User*****

username user1 password mbO2jYs13AXlIAGa encrypted privilege 2


!! *****Configure Group-Policy*****



group-policy GroupPolicy_SSL_GRP internal
group-policy GroupPolicy_SSL_GRP attributes
 vpn-tunnel-protocol ssl-client
 dns-server none
 wins-server none
 default-domain none
 exit


!! *****Configure Tunnel-Group*****

tunnel-group SSL_GRP type remote-access
tunnel-group SSL_GRP general-attributes
 authentication-server-group LOCAL
 default-group-policy GroupPolicy_SSL_GRP
 address-pool  VPN_Pool
tunnel-group SSL_GRP webvpn-attributes
 authentication aaa certificate
 group-alias SSL_GRP enable
 exit


!! *****Configure NAT-Exempt Policy*****

nat (Inside,Internet) 1 source static NETWORK_OBJ_192.168.10.0_24 NETWORK_OBJ_192.168.10.0_24 destinati
```

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Remarque : l'outil Output Interpreter Tool (clients enregistrés uniquement) prend en charge certaines commandes show. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Assurez-vous que le serveur AC est activé.

show crypto ca server

<#root>

```
ASA(config)# show crypto ca server
Certificate Server LOCAL-CA-SERVER:


  Status: enabled


    State: enabled
    Server's configuration is locked  (enter "shutdown" to unlock it)


Issuer name: CN=ASA.local


    CA certificate fingerprint/thumbprint: (MD5)
        32e868b9 351a1b07 4b59cce5 704d6615
    CA certificate fingerprint/thumbprint: (SHA1)
        6136511b 14aa1bbe 334c2659 ae7015a9 170a7c4d
    Last certificate issued serial number: 0x1
    CA certificate expiration timer: 19:25:42 UTC Jan 8 2019
    CRL NextUpdate timer: 01:25:42 UTC Jan 10 2016
    Current primary storage dir: flash:/LOCAL-CA-SERVER/

    Auto-Rollover configured, overlap period 30 days
    Autorollover timer: 19:25:42 UTC Dec 9 2018

    WARNING: Configuration has been modified and needs to be saved!!
```

Assurez-vous que l'utilisateur est autorisé à s'inscrire après avoir ajouté :

<#root>

```
*****Before Enrollment*****


ASA#

show crypto ca server user-db

username: user1
email:    user1@cisco.com
dn:       CN=user1,OU=TAC
allowed:  19:03:11 UTC Thu Jan 14 2016
notified: 1 times
enrollment status: Allowed to Enroll
```

```
>>> Shows the status "Allowed to Enroll"

*****After Enrollment*****


username: user1
email:    user1@cisco.com
dn:       CN=user1,OU=TAC
allowed:  19:05:14 UTC Thu Jan 14 2016
notified: 1 times

enrollment status: Enrolled

, Certificate valid until 19:18:30 UTC Tue Jan 10 2017,
Renewal: Allowed
```

Vous pouvez vérifier les détails de la connexion anyconnect via l'interface de ligne de commande ou l'ASDM.

Via CLI

show vpn-sessiondb detail anyconnect

<#root>

```
ASA# show vpn-sessiondb detail anyconnect


Session Type: AnyConnect Detailed

Username     : user1                  Index        : 1
Assigned IP  : 10.10.10.1             Public IP    : 10.142.189.181
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel: (1)AES128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 13822                  Bytes Rx     : 13299
Pkts Tx      : 10                     Pkts Rx      : 137
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : GroupPolicy_SSL_GRP    Tunnel Group : SSL_GRP
Login Time   : 19:19:10 UTC Mon Jan 11 2016
Duration     : 0h:00m:47s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 1.1
  Public IP    : 10.142.189.181
  Encryption   : none                   Hashing      : none
  TCP Src Port : 52442                  TCP Dst Port : 443
  Auth Mode    : Certificate and userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Client OS    : Windows
```

```
  Client Type  : AnyConnect
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.2.00096
  Bytes Tx     : 6911                    Bytes Rx     : 768
  Pkts Tx      : 5                       Pkts Rx      : 1
  Pkts Tx Drop : 0                       Pkts Rx Drop : 0

SSL-Tunnel:
  Tunnel ID    : 1.2
  Assigned IP  : 10.10.10.1              Public IP    : 10.142.189.181
  Encryption   : RC4                     Hashing      : SHA1
  Encapsulation: TLSv1.0                 TCP Src Port : 52443
  TCP Dst Port : 443                     Auth Mode    : Certificate and userPassword
  Idle Time Out: 30 Minutes              Idle TO Left : 29 Minutes
  Client OS    : Windows
  Client Type  : SSL VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.2.00096
  Bytes Tx     : 6911                    Bytes Rx     : 152
  Pkts Tx      : 5                       Pkts Rx      : 2
  Pkts Tx Drop : 0                       Pkts Rx Drop : 0

DTLS-Tunnel:
  Tunnel ID    : 1.3
  Assigned IP  : 10.10.10.1              Public IP    : 10.142.189.181
  Encryption   : AES128                  Hashing      : SHA1
  Encapsulation: DTLSv1.0                UDP Src Port : 59167
  UDP Dst Port : 443                     Auth Mode    : Certificate and userPassword
  Idle Time Out: 30 Minutes              Idle TO Left : 30 Minutes
  Client OS    : Windows
  Client Type  : DTLS VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.2.00096
  Bytes Tx     : 0                       Bytes Rx     : 12907
  Pkts Tx      : 0                       Pkts Rx      : 142
  Pkts Tx Drop : 0                       Pkts Rx Drop : 0

NAC:
  Reval Int (T): 0 Seconds               Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds               EoU Age(T)   : 51 Seconds
  Hold Left (T): 0 Seconds               Posture Token:
  Redirect URL :
```

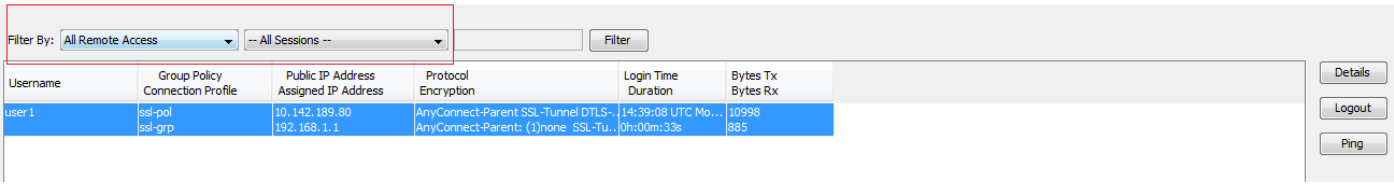
Via ASDM

- Accédez à Monitoring > VPN > VPN Statistics > Sessions.
- Sélectionnez Filtrer par comme Tous les accès à distance.
- Vous pouvez effectuer l’une ou l’autre des actions pour le client AnyConnect sélectionné.

Détails - Fournir plus d'informations sur la session

Déconnexion : pour déconnecter manuellement l'utilisateur de Headend

Ping : pour envoyer une requête ping au client AnyConnect depuis la tête de réseau



Dépannage

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

> Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de débogage.

> Attention : sur l'ASA, vous pouvez définir différents niveaux de débogage ; par défaut, le niveau 1 est utilisé. Si vous modifiez le niveau de débogage, le niveau de détail des débogages peut augmenter. Faites-le avec prudence, en particulier dans les environnements de production.

- debug crypto ca
- debug crypto ca server
- debug crypto ca messages
- debug crypto ca transactions
- debug webvpn anyconnect

Cette sortie de débogage indique quand le serveur AC est activé à l'aide de la commande no shut.

<#root>

```
ASA# debug crypto ca 255
ASA# debug crypto ca server 255
ASA# debug crypto ca message 255
ASA# debug crypto ca transaction 255
```

```
CRYPTO_CS: input signal enqueued: no shut   >>>>> Command issued to Enable the CA server
Crypto CS thread wakes up!

CRYPTO_CS: enter FSM: input state disabled, input signal no shut
CRYPTO_CS: starting enabling checks
CRYPTO_CS: found existing serial file.
CRYPTO_CS: started CA cert timer, expiration time is 17:53:33 UTC Jan 13 2019
CRYPTO_CS: Using existing trustpoint 'LOCAL-CA-SERVER' and CA certificate
CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser
CRYPTO_CS: DB version 1
CRYPTO_CS: last issued serial number is 0x4
CRYPTO_CS: closed ser file
CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.crl
CRYPTO_CS: CRL file LOCAL-CA-SERVER.crl exists.
CRYPTO_CS: Read 220 bytes from crl file.
CRYPTO_CS: closed crl file
```

```
CRYPTO_PKI: Storage context locked by thread Crypto CA Server

CRYPTO_PKI: inserting CRL
CRYPTO_PKI: set CRL update timer with delay: 20250
CRYPTO_PKI: the current device time: 18:05:17 UTC Jan 16 2016

CRYPTO_PKI: the last CRL update time: 17:42:47 UTC Jan 16 2016
CRYPTO_PKI: the next CRL update time: 23:42:47 UTC Jan 16 2016
CRYPTO_PKI: CRL cache delay being set to: 20250000
CRYPTO_PKI: Storage context released by thread Crypto CA Server

CRYPTO_CS: Inserted Local CA CRL into cache!

CRYPTO_CS: shadow not configured; look for shadow cert
CRYPTO_CS: failed to find shadow cert in the db
CRYPTO_CS: set shadow generation timer
CRYPTO_CS: shadow generation timer has been set
CRYPTO_CS: Enabled CS.
CRYPTO_CS: exit FSM: new state enabled
CRYPTO_CS: cs config has been locked.

Crypto CS thread sleeps!
```

Cette sortie de débogage montre l'inscription du client

<#root>

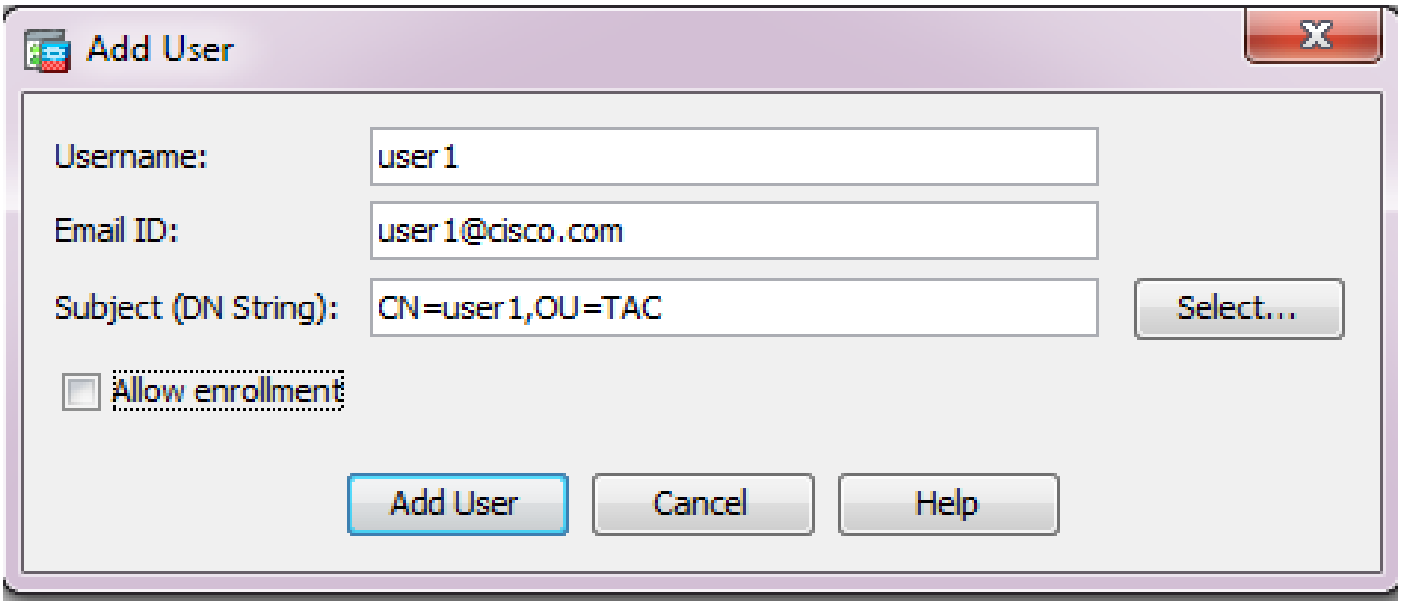
```
ASA# debug crypto ca 255
ASA# debug crypto ca server 255
ASA# debug crypto ca message 255
ASA# debug crypto ca transaction 255
```

```
CRYPTO_CS: writing serial number 0x2.
CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser
CRYPTO_CS: Writing 32 bytes to ser file
CRYPTO_CS: Generated and saving a PKCS12 file for user user1
at flash:/LOCAL-CA-SERVER/user1.p12
```

L'Inscription du Client peut échouer dans les conditions suivantes :

Scénario 1.

- L'utilisateur est créé dans la base de données du serveur AC sans l'autorisation de s'inscrire.



Équivalent de la CLI :

<#root>

```
ASA(config)# show crypto ca server user-db

username: user1
email:    user1@cisco.com
dn:       CN=user1,OU=TAC
allowed:  <not allowed>
notified: 0 times

enrollment status: Not Allowed to Enroll
```

- Dans le cas où l'utilisateur n'est pas autorisé à s'inscrire, la tentative de génération/d'envoi par e-mail du mot de passe à usage unique pour l'utilisateur génère ce message d'erreur.

Scénario 2.

- Vérifiez le port et l'interface sur lesquels le portail d'inscription est disponible en utilisant la commande show run webvpn. Le port par défaut est 443 mais il peut être modifié.

- Assurez-vous que le client dispose d'une accessibilité réseau à l'adresse IP de l'interface sur laquelle webvpn est activé sur le port utilisé pour accéder avec succès au portail d'inscription.

Le client peut ne pas accéder au portail d'inscription de l'ASA dans les cas suivants :

1. Si un périphérique intermédiaire bloque les connexions entrantes du client vers l'adresse IP webvpn de l'ASA sur le port spécifié.
2. L'état de l'interface est down sur laquelle webvpn est activé.

- Ce résultat montre que le portail d'inscription est disponible à l'adresse IP de l'interface Internet sur le port personnalisé 4433.

<#root>

```
ASA(config)# show run webvpn

webvpn


port 4433


enable Internet

 no anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.2.00096-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
```

Scénario 3.

- L'emplacement par défaut du stockage de base de données du serveur AC est la mémoire Flash de l'ASA.
- Assurez-vous que la mémoire flash dispose d'un espace libre pour générer et enregistrer le fichier pkcs12 pour l'utilisateur lors de l'inscription.
- Dans le cas où la mémoire flash n'a pas assez d'espace libre, ASA ne réussit pas à terminer le processus d'inscription du client et génère ces journaux de débogage :

<#root>

```
ASA(config)# debug crypto ca 255
ASA(config)# debug crypto ca server 255
ASA(config)# debug crypto ca message 255
ASA(config)# debug crypto ca transaction 255
ASA(config)# debug crypto ca trustpool 255

CRYPTO_CS: writing serial number 0x2.
CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser
CRYPTO_CS: Writing 32 bytes to ser file
CRYPTO_CS: Generated and saving a PKCS12 file for user user1
at flash:/LOCAL-CA-SERVER/user1.p12
```

```
CRYPTO_CS: Failed to write to opened PKCS12 file for user user1, fd: 0, status: -1.

CRYPTO_CS: Failed to generate pkcs12 file for user user1 status: -1.

CRYPTO_CS: Failed to process enrollment in-line for user user1. status: -1
```

Informations connexes

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Guide de dépannage de client VPN AnyConnect – Problèmes fréquents
- Gestion, surveillance et dépannage des sessions AnyConnect
- 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.