

Authentification Anyconnect ASA 8.x avec la carte eID belge

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Informations générales](#)

[Configuration de l'ordinateur local](#)

[Système d'exploitation](#)

[Lecteur de cartes](#)

[Logiciel d'exécution eID](#)

[Certificat d'authentification](#)

[Installation d'AnyConnect](#)

[Exigences ASA](#)

[Configuration ASA](#)

[Étape 1. Activer l'interface externe](#)

[Étape 2. Configurer le nom de domaine, le mot de passe et l'heure système](#)

[Étape 3. Activez un serveur DHCP sur l'interface externe.](#)

[Étape 4. Configurer le pool d'adresses VPN eID](#)

[Étape 5. Importer le certificat d'Autorité de certification racine de Belgique](#)

[Étape 6. Configurer la couche de sockets sécurisés](#)

[Étape 7. Définir la stratégie de groupe par défaut](#)

[Étape 8. Définir le mappage de certificat](#)

[Étape 9. Ajouter un utilisateur local](#)

[Étape 10. Redémarrer l'ASA](#)

[Ajustement fin](#)

[Configuration d'une minute](#)

[Informations connexes](#)

[Introduction](#)

Ce document décrit comment configurer l'authentification Anyconnect ASA 8.x pour utiliser la carte eID belge.

[Conditions préalables](#)

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

- ASA 5505 avec le logiciel ASA 8.0 approprié
- Client AnyConnect
- ASDM 6.0

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

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Informations générales

L'eID est une carte PKI (Public Key Infrastructure) émise par le gouvernement belge que les utilisateurs doivent utiliser pour s'authentifier sur un PC Windows distant. Le client logiciel AnyConnect est installé sur le PC local et prend les informations d'authentification à partir du PC distant. Une fois l'authentification terminée, l'utilisateur distant obtient l'accès aux ressources centrales via un tunnel SSL complet. L'utilisateur distant est provisionné avec une adresse IP obtenue à partir d'un pool géré par l'ASA.

Configuration de l'ordinateur local

Système d'exploitation

Le système d'exploitation (Windows, MacOS, Unix ou Linux) de votre ordinateur local doit être à jour et tous les correctifs requis doivent être installés.

Lecteur de cartes

Un lecteur de carte électronique doit être installé sur votre ordinateur local pour pouvoir utiliser la carte d'identité électronique. Le lecteur de carte électronique est un périphérique matériel qui établit un canal de communication entre les programmes de l'ordinateur et la puce de la carte d'identité.

Pour obtenir la liste des lecteurs de cartes approuvés, reportez-vous à l'URL suivante : <http://www.cardreaders.be/en/default.htm>

Remarque : Pour utiliser le lecteur de carte, vous devez installer les pilotes recommandés par le

fabricant du matériel.

Logiciel d'exécution eID

Vous devez installer le logiciel d'exécution eID fourni par le gouvernement belge. Ce logiciel permet à l'utilisateur distant de lire, valider et imprimer le contenu de la carte eID. Le logiciel est disponible en français et en néerlandais pour Windows, MAC OS X et Linux.

Pour plus d'informations, consultez cette URL :

- http://www.belgium.be/zip/eid_datacapture_nl.html

Certificat d'authentification

Vous devez importer le certificat d'authentification dans le magasin Microsoft Windows sur le PC local. Si vous ne parvenez pas à importer le certificat dans le magasin, le client AnyConnect ne pourra pas établir de connexion SSL à l'ASA.

Procédure

Pour importer le certificat d'authentification dans le magasin Windows, procédez comme suit :

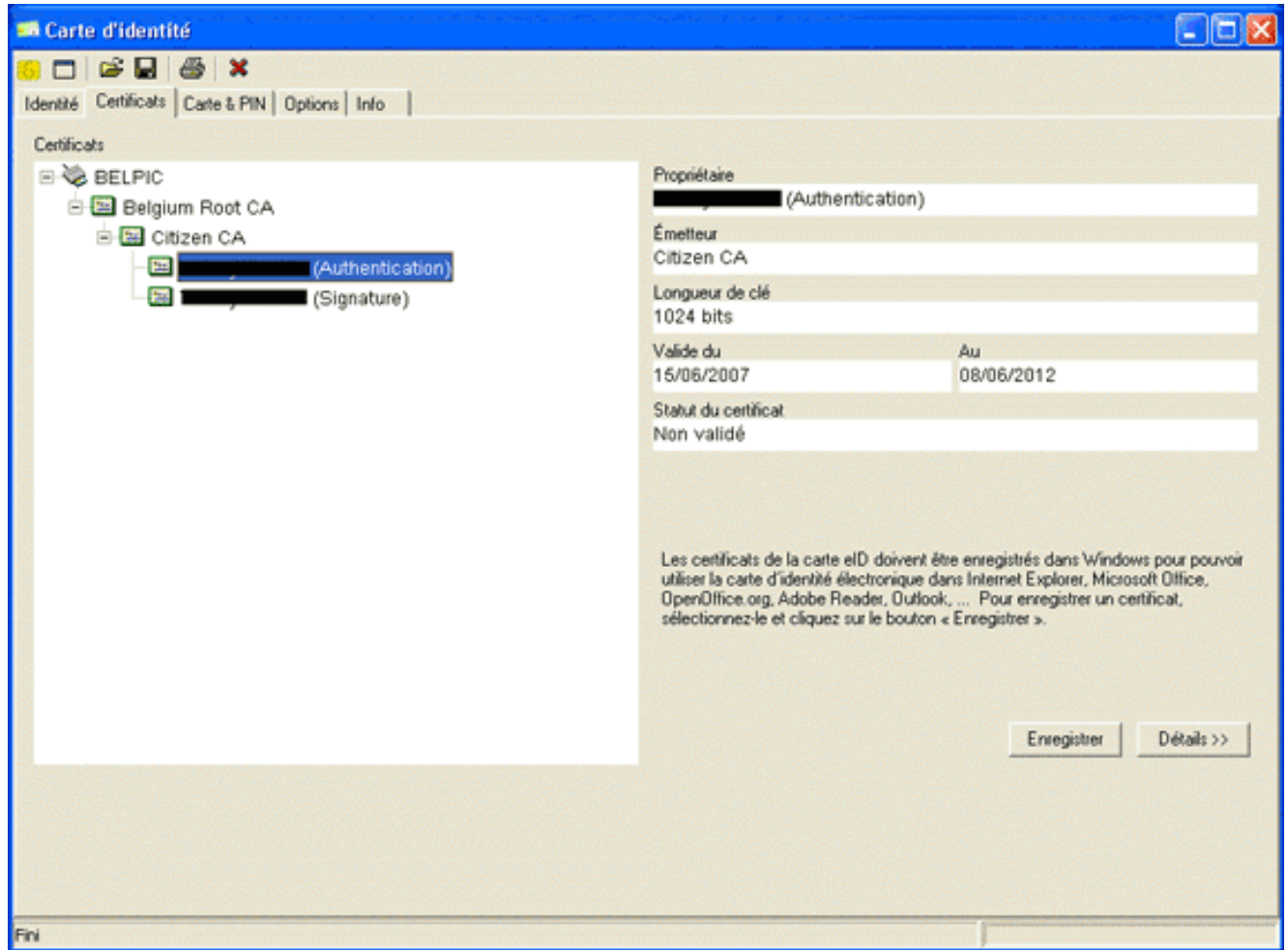
1. Insérez votre eID dans le lecteur de carte et lancez le middleware afin d'accéder au contenu de la carte eID. Le contenu de la carte eID apparaît.

The screenshot shows a software window titled 'Carte d'identité' with a menu bar containing 'Identité', 'Certificats', 'Carte & PIN', 'Options', and 'Info'. The main content area is divided into several sections:

- Header:** Four columns with labels: 'BELGIQUE CARTE D'IDENTITE', 'BELGIE IDENTITEITSKAART', 'BELGIEN PERSONALAUSWEIS', and 'BELGIUM IDENTITY CARD'.
- Identité section:** Fields for 'Nom', 'Prénoms', 'Lieu de naissance', 'Date de naissance' (14/04/1963), 'Sexe' (M), 'Nationalité' (be), 'Titre', and 'Numéro national' (63.04.14-033.25).
- Carte section:** 'Numéro de la puce' (534C494E336600296CFF271507192C36), 'Numéro de la carte' (590.5942800.24), 'Valide du' (07/06/2007) 'Au' (07/06/2012), and 'Commune d'émission'.
- Adresse section:** 'Rue', 'Code postal', 'Commune', and 'Pays' (be).
- Statut spécial section:** Radio buttons for 'Carte blanche', 'Carte jaune', and 'Minorité étendue'.
- Visuals:** A yellow chip icon, a red map of Belgium, the Belgian coat of arms, and a photo of a man with a blacked-out face.

2. Cliquez sur l'onglet **Certificats** (FR). La hiérarchie des certificats

s'affiche.



3. Développez **Belgium Root CA**, puis **Citizen CA**.
4. Choisissez la version **Authentification** de votre certificat nommé.
5. Cliquez sur le bouton **Enregistrer** (FR). Le certificat est copié dans le magasin Windows.

Remarque : lorsque vous cliquez sur le bouton **Détails**, une fenêtre s'affiche et affiche des détails sur le certificat. Dans l'onglet **Détails**, sélectionnez le champ **Objet** afin d'afficher le champ Numéro de série. Le champ Numéro de série contient une valeur unique qui est utilisée pour l'autorisation de l'utilisateur. Par exemple, le numéro de série " 56100307215 " représente un utilisateur dont la date de naissance est le 3 octobre 1956 avec un numéro de séquence 072 et un chiffre de contrôle de 15. *Vous devez soumettre une demande d'approbation des autorités fédérales afin de stocker ces numéros. Il vous incombe de faire les déclarations officielles appropriées relatives à la tenue d'une base de données des citoyens belges dans votre pays.*

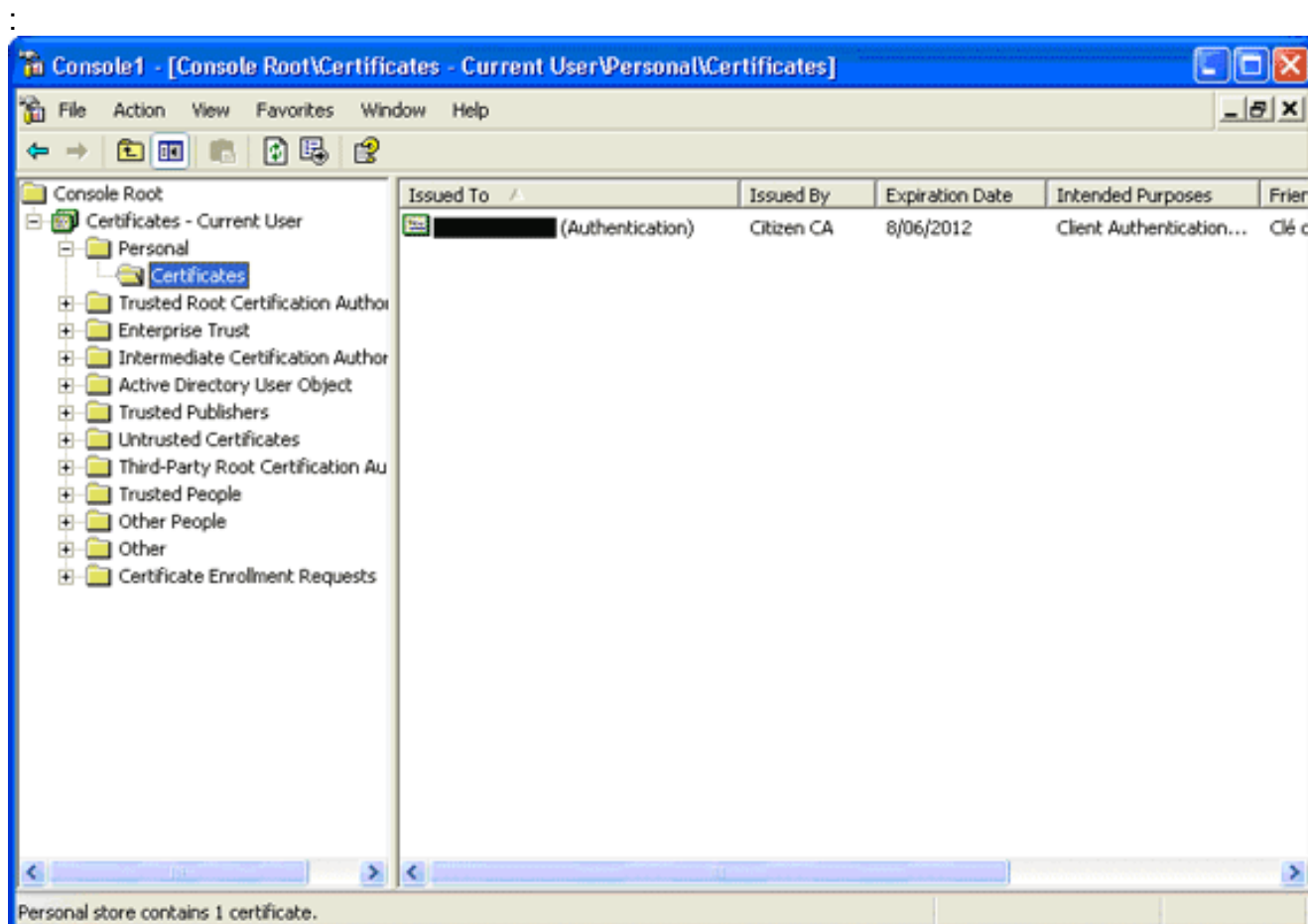
Vérification

Afin de vérifier que le certificat a été importé correctement, procédez comme suit :

1. Sur un ordinateur Windows XP, ouvrez une fenêtre DOS et tapez la commande **mmc**. L'application Console apparaît.
2. Choisissez **Fichier > Ajouter/Supprimer le composant logiciel enfichable** (ou appuyez sur Ctrl+M). La boîte de dialogue Ajouter/Supprimer un composant logiciel enfichable s'affiche.
3. Cliquez sur le bouton **Add**. La boîte de dialogue Ajouter un composant logiciel enfichable autonome s'affiche.
4. Dans la liste Composants logiciels enfichables autonomes disponibles, sélectionnez **Certificats**, puis cliquez sur **Ajouter**.
5. Cliquez sur la case d'option **Mon compte d'utilisateur**, puis cliquez sur **Terminer**. Le

composant logiciel enfichable Certificat apparaît dans la boîte de dialogue Ajouter/Supprimer un composant logiciel enfichable.

6. Cliquez sur **Fermer** afin de fermer la boîte de dialogue Ajouter un composant logiciel enfichable autonome, puis cliquez sur **OK** dans la boîte de dialogue Ajouter/Supprimer un composant logiciel enfichable afin d'enregistrer vos modifications et de revenir à l'application Console.
7. Sous le dossier Racine de la console, développez **Certificats - Utilisateur actuel**.
8. Développez **Personal**, puis **Certificats**. Le certificat importé doit apparaître dans le magasin Windows comme illustré dans cette image



Installation d'AnyConnect

Vous devez installer AnyConnect Client sur le PC distant. Le logiciel AnyConnect utilise un fichier de configuration XML qui peut être modifié afin de prédéfinir une liste de passerelles disponibles. Le fichier XML est stocké dans ce chemin d'accès sur le PC distant :

C:\Documents and Settings\%USERNAME%\Application Data\Cisco\Cisco AnyConnect VPN Client

où %USERNAME% est le nom de l'utilisateur sur le PC distant.

Le nom du fichier XML est *préférences.xml*. Voici un exemple du contenu du fichier :

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectPreferences>
<DefaultHost>192.168.0.1</DefaultHost> </AnyConnectPreferences>
```

où 192.168.0.1 est l'adresse IP de la passerelle ASA.

Exigences ASA

Assurez-vous que l'ASA répond aux conditions suivantes :

- AnyConnect et ASDM doivent être exécutés en mémoire Flash. Afin de terminer les procédures de ce document, utilisez un ASA 5505 avec le logiciel ASA 8.0 approprié installé. Les applications AnyConnect et ASDM doivent être préchargées en mémoire Flash. Utilisez la commande **show flash** afin d'afficher le contenu de la mémoire flash :

```
ciscoasa#show flash:
```

```
--#-- --length-- -----date/time----- path
 66 14524416   Jun 26 2007 10:24:02 asa802-k8.bin
 67 6889764    Jun 26 2007 10:25:28 asdm-602.bin
 68 2635734     Jul 09 2007 07:37:06 anyconnect-win-2.0.0343-k9.pkg
```

- ASA doit être exécuté avec les paramètres d'usine par défaut. Vous pouvez ignorer cette condition si vous utilisez un nouveau châssis ASA afin de terminer les procédures de ce document. Sinon, complétez ces étapes afin de réinitialiser l'ASA aux paramètres d'usine par défaut : Dans l'application ASDM, connectez-vous au châssis ASA, puis choisissez **Fichier > Réinitialiser le périphérique à la configuration par défaut en usine**.

The screenshot shows the Cisco ASDM 6.0 for ASA interface. The title bar reads 'Cisco ASDM 6.0 for ASA - 192.168.100.254'. The 'File' menu is open, highlighting 'Reset Device to the Factory Default Configuration...'. Other menu items include 'Refresh ASDM with the Running Configuration on the Device', 'Show Running Configuration in New Window...', 'Save Running Configuration to Flash', 'Save Running Configuration to TFTP Server...', 'Save Running Configuration to Standby Unit', 'Save Internal Log Buffer to Flash', 'Print...', 'Clear ASDM Cache', 'Clear Internal Log Buffer', and 'Exit'. The main dashboard displays 'Device UpTime: 0d 0h 14m 21s', 'Device Type: ASA 5505', 'Context Mode: Single', and 'Total Memory: 256 MB'. The 'Interface Status' section shows 'inside' as 'up' and 'outside' as 'down'. The 'System Resources Status' section shows CPU usage at 12% and memory usage at 63MB. The 'Latest ASDM Syslog Messages' section shows several error messages related to TCP connections. The status bar at the bottom indicates 'Device configuration loaded successfully.' and the user is logged in as 'admin'.

Laissez les valeurs par défaut dans le modèle. Connectez votre ordinateur sur l'interface interne Ethernet 0/1 et renouvelez votre adresse IP qui sera provisionnée par le serveur DHCP de l'ASA. **Remarque** : Afin de rétablir les paramètres d'usine par défaut de l'ASA à partir de la ligne de commande, utilisez les commandes suivantes :

```
ciscoasa#conf t
```

Configuration ASA

Une fois les paramètres d'usine ASA réinitialisés, vous pouvez démarrer ASDM sur 192.168.0.1 afin de vous connecter à l'ASA sur l'interface interne Ethernet 0/1.

Remarque : Votre mot de passe précédent est conservé (ou peut être vide par défaut).

Par défaut, l'ASA accepte une session de gestion entrante avec une adresse IP source dans le sous-réseau 192.168.0.0/24. Le serveur DHCP par défaut activé sur l'interface interne de l'ASA fournit des adresses IP comprises dans la plage 192.168.0.2-129/24, valides pour la connexion à l'interface interne avec ASDM.

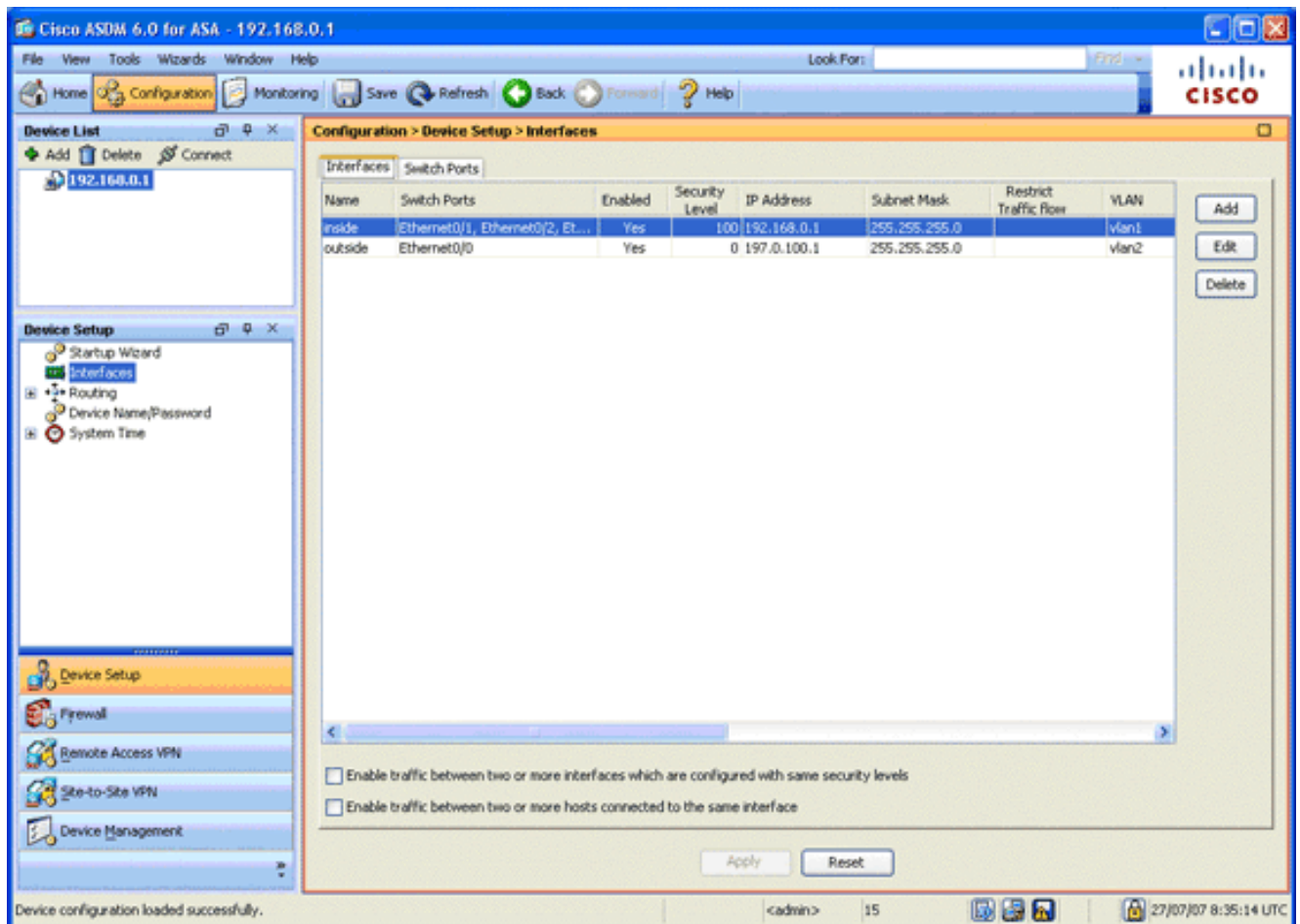
Complétez ces étapes afin de configurer l'ASA :

1. [Activer l'interface externe](#)
2. [Configurer le nom de domaine, le mot de passe et l'heure système](#)
3. [Activer un serveur DHCP sur l'interface externe](#)
4. [Configurer le pool d'adresses VPN eID](#)
5. [Importer le certificat d'Autorité de certification racine de Belgique](#)
6. [Configurer la couche de sockets sécurisés](#)
7. [Définir la stratégie de groupe par défaut](#)
8. [Définir le mappage de certificat](#)
9. [Ajouter un utilisateur local](#)
10. [Redémarrer l'ASA](#)

Étape 1. Activer l'interface externe

Cette étape décrit comment activer l'interface externe.

1. Dans l'application ASDM, cliquez sur **Configuration**, puis sur **Device Setup**.
2. Dans la zone Device Setup, sélectionnez **Interfaces**, puis cliquez sur l'onglet **Interfaces**.

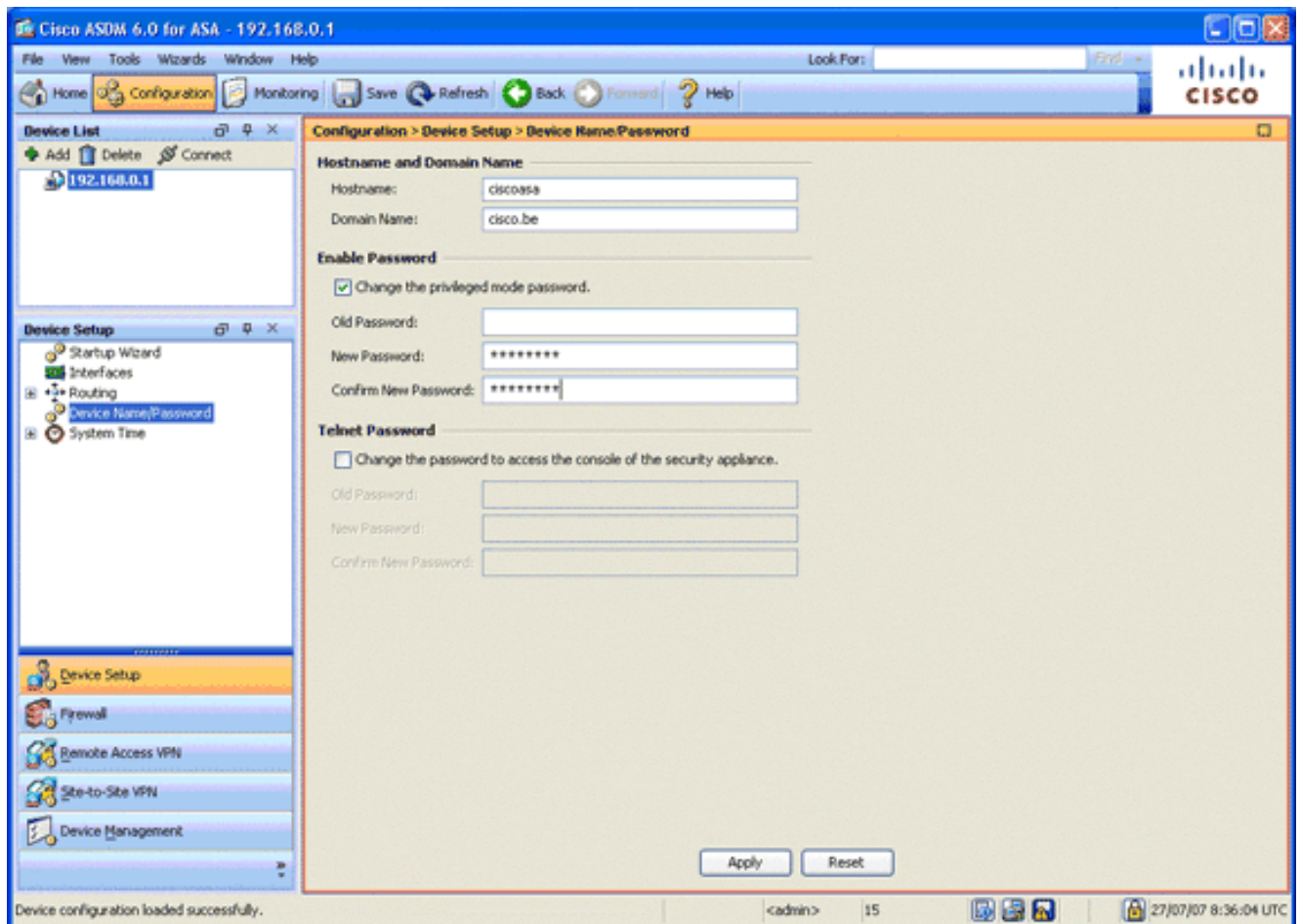


3. Sélectionnez l'interface externe, puis cliquez sur **Modifier**.
4. Dans la section IP address de l'onglet General, sélectionnez l'option **Use Static IP**.
5. Entrez **197.0.100.1** pour l'adresse IP et **255.255.255.0** pour le masque de sous-réseau.
6. Cliquez sur Apply.

Étape 2. Configurer le nom de domaine, le mot de passe et l'heure système

Cette étape décrit comment configurer le nom de domaine, le mot de passe et l'heure système.

1. Dans la zone Device Setup, sélectionnez **Device Name/Password**.

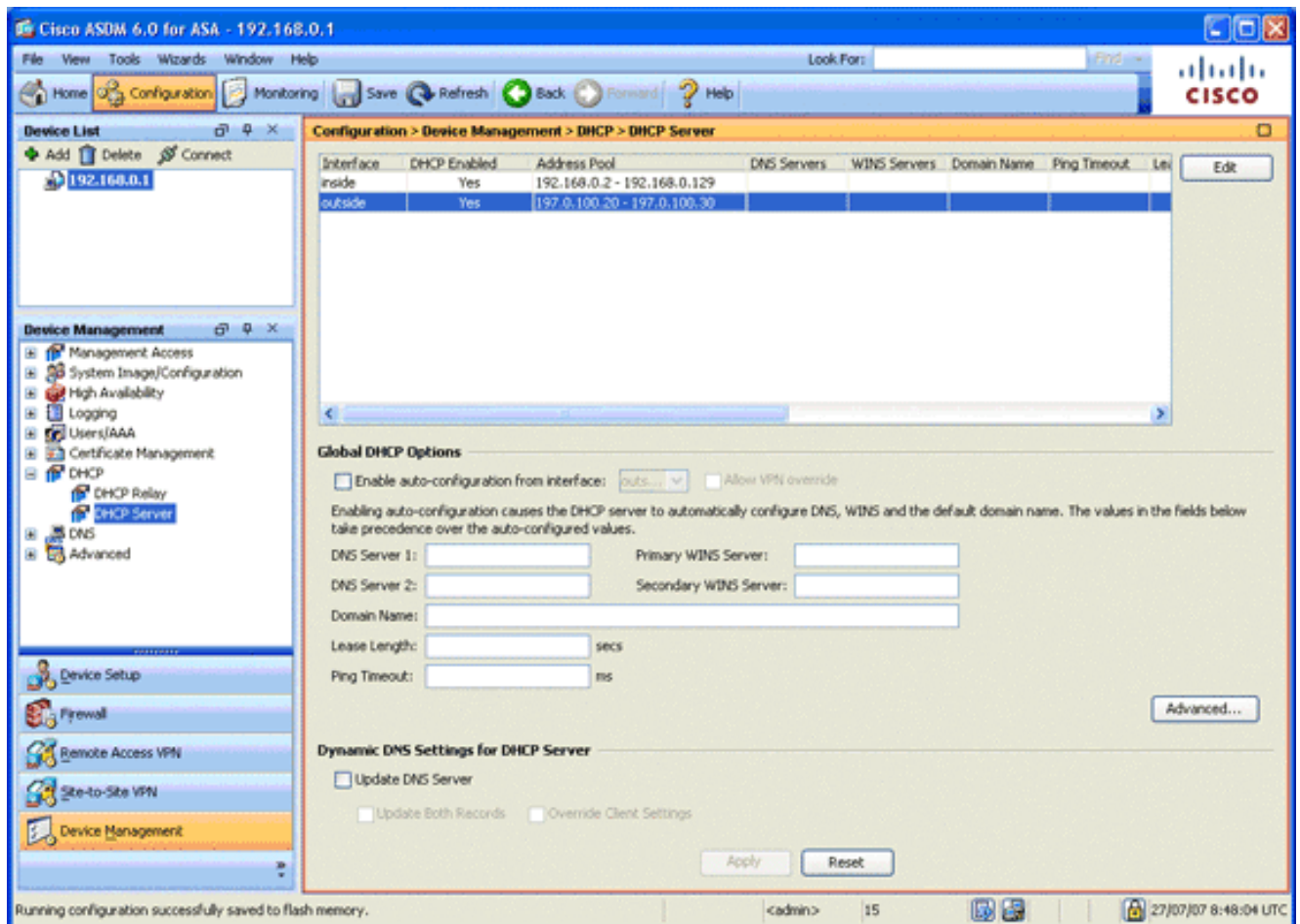


2. Entrez **cisco.be** pour le nom de domaine et **cisco123** pour la valeur Enable Password. **Remarque** : Par défaut, le mot de passe est vide.
3. Cliquez sur Apply.
4. Dans la zone Device Setup (Configuration du périphérique), sélectionnez **System Time**, puis modifiez la valeur d'horloge (si nécessaire).
5. Cliquez sur Apply.

Étape 3. Activez un serveur DHCP sur l'interface externe.

Cette étape décrit comment activer un serveur DHCP sur l'interface externe afin de faciliter les tests.

1. Cliquez sur **Configuration**, puis sur **Device Management**.
2. Dans la zone Device Management, développez **DHCP**, puis sélectionnez **DHCP Server**.

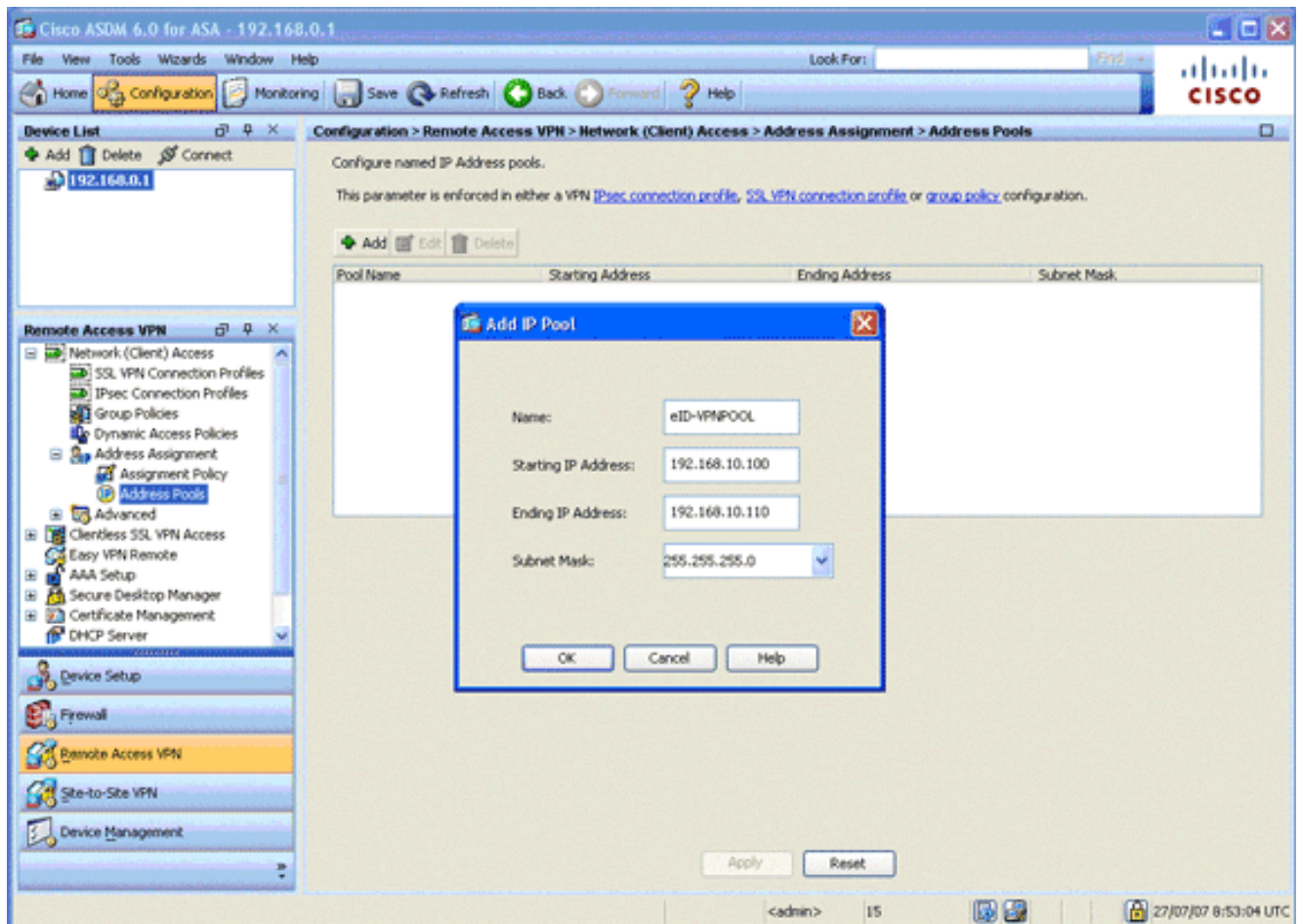


3. Sélectionnez l'interface externe dans la liste Interface, puis cliquez sur **Modifier**. La boîte de dialogue Modifier le serveur DHCP s'affiche.
4. Cochez la case **Activer le serveur DHCP**.
5. Dans le pool d'adresses DHCP, saisissez une adresse IP comprise entre 197.0.100.20 et 197.0.100.30.
6. Dans la zone Options DHCP globales, décochez la case **Activer la configuration automatique à partir de l'interface**.
7. Cliquez sur Apply.

Étape 4. Configurer le pool d'adresses VPN etD

Cette étape décrit comment définir un pool d'adresses IP qui sont utilisées pour approvisionner les clients AnyConnect distants.

1. Cliquez sur **Configuration**, puis sur **Remote Access VPN**.
2. Dans la zone Remote Access VPN, développez **Network (Client) Access**, puis développez **Address Assignment**.
3. Choisissez **Address Pools**, puis cliquez sur le bouton **Add** situé dans la zone Configurer les pools d'adresses IP nommées. La boîte de dialogue Add IP Pool apparaît.



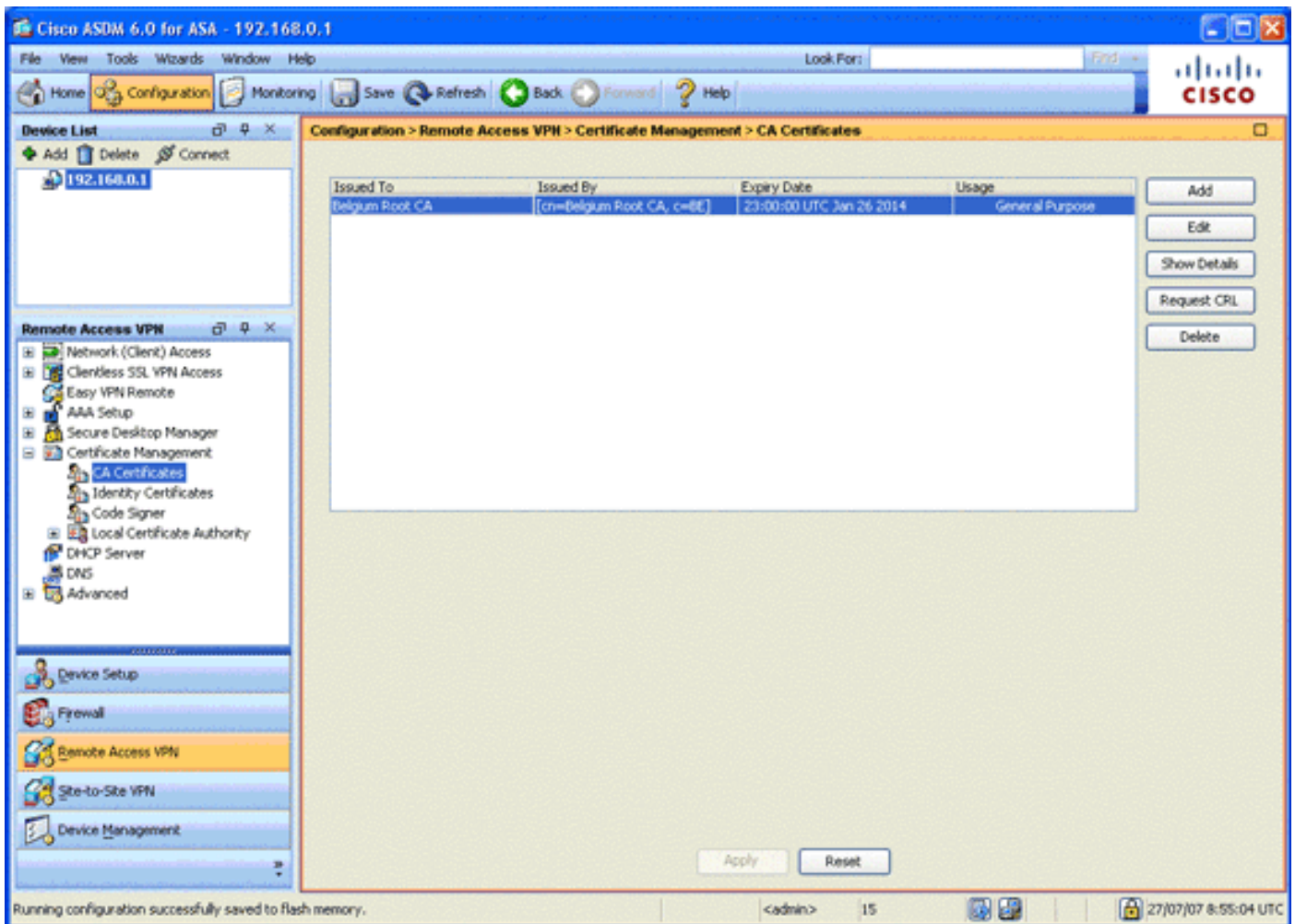
4. Dans le champ Nom, saisissez **eID-VPNPOOL**.
5. Dans les champs Adresse IP de début et Adresse IP de fin, saisissez une plage d'adresses IP comprises entre 192.168.10.100 et 192.168.10.110.
6. Choisissez **255.255.255.0** dans la liste déroulante Masque de sous-réseau, cliquez sur **OK**, puis sur **Appliquer**.

Étape 5. Importer le certificat d'Autorité de certification racine de Belgique

Cette étape décrit comment importer dans l'ASA le certificat d'Autorité de certification racine belge.

1. Téléchargez et installez les certificats de CA racine belge (belgiumrca.crt et belgiumrca2.crt) à partir du site web du gouvernement et stockez-les sur votre PC local. Le site web du gouvernement belge se trouve à l'adresse suivante : <http://certs.eid.belgium.be/>
2. Dans la zone VPN d'accès à distance, développez **Gestion des certificats**, puis sélectionnez **Certificats CA**.
3. Cliquez sur **Ajouter**, puis sur **Installer à partir du fichier**.
4. Accédez à l'emplacement dans lequel vous avez enregistré le fichier de certificat d'Autorité de certification racine belge (belgiumrca.crt), puis cliquez sur **Installer le certificat**.
5. Cliquez sur Appliquer afin de sauvegarder vos modifications.

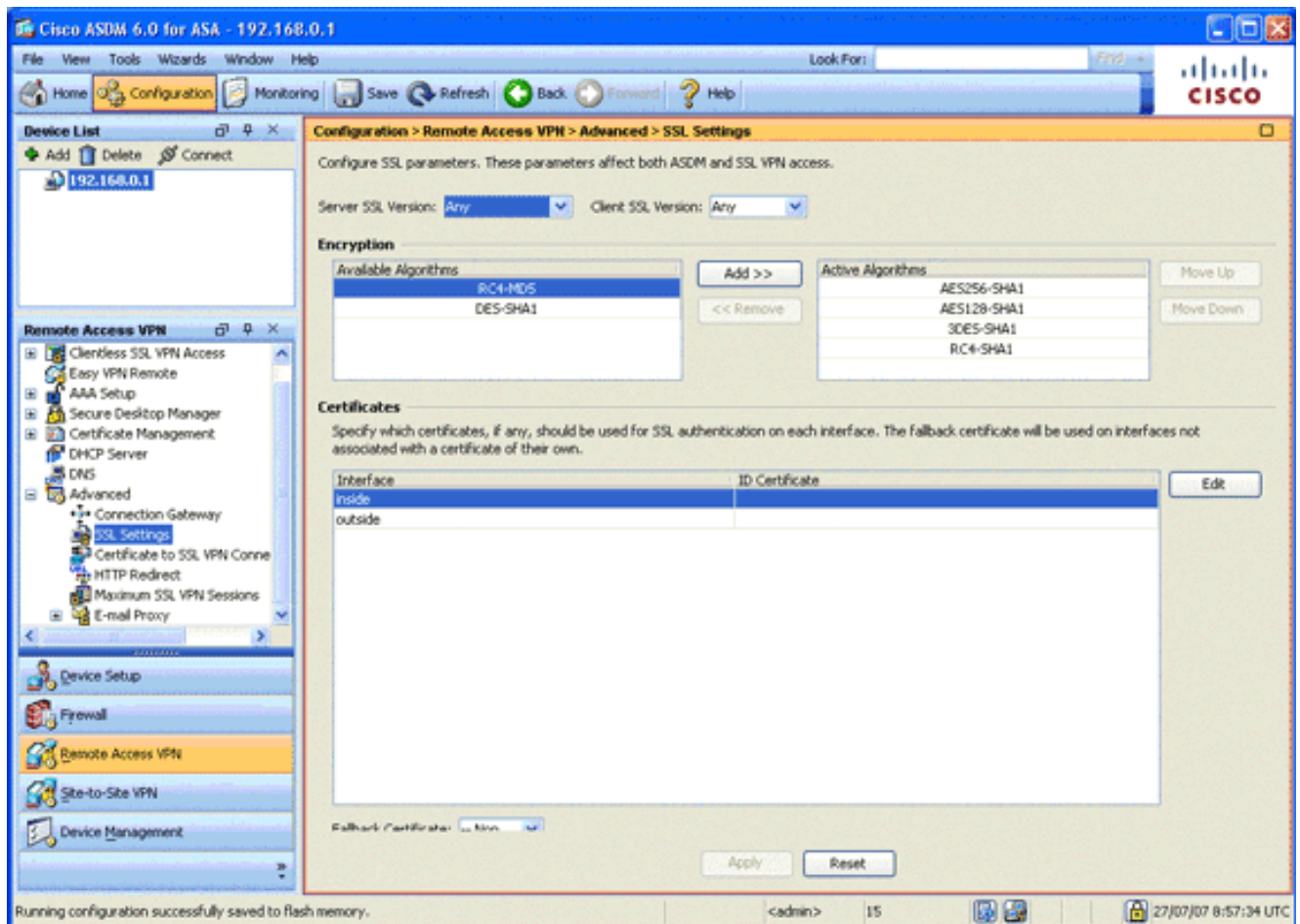
Cette image montre le certificat installé sur l'ASA :



Étape 6. Configurer la couche de sockets sécurisés

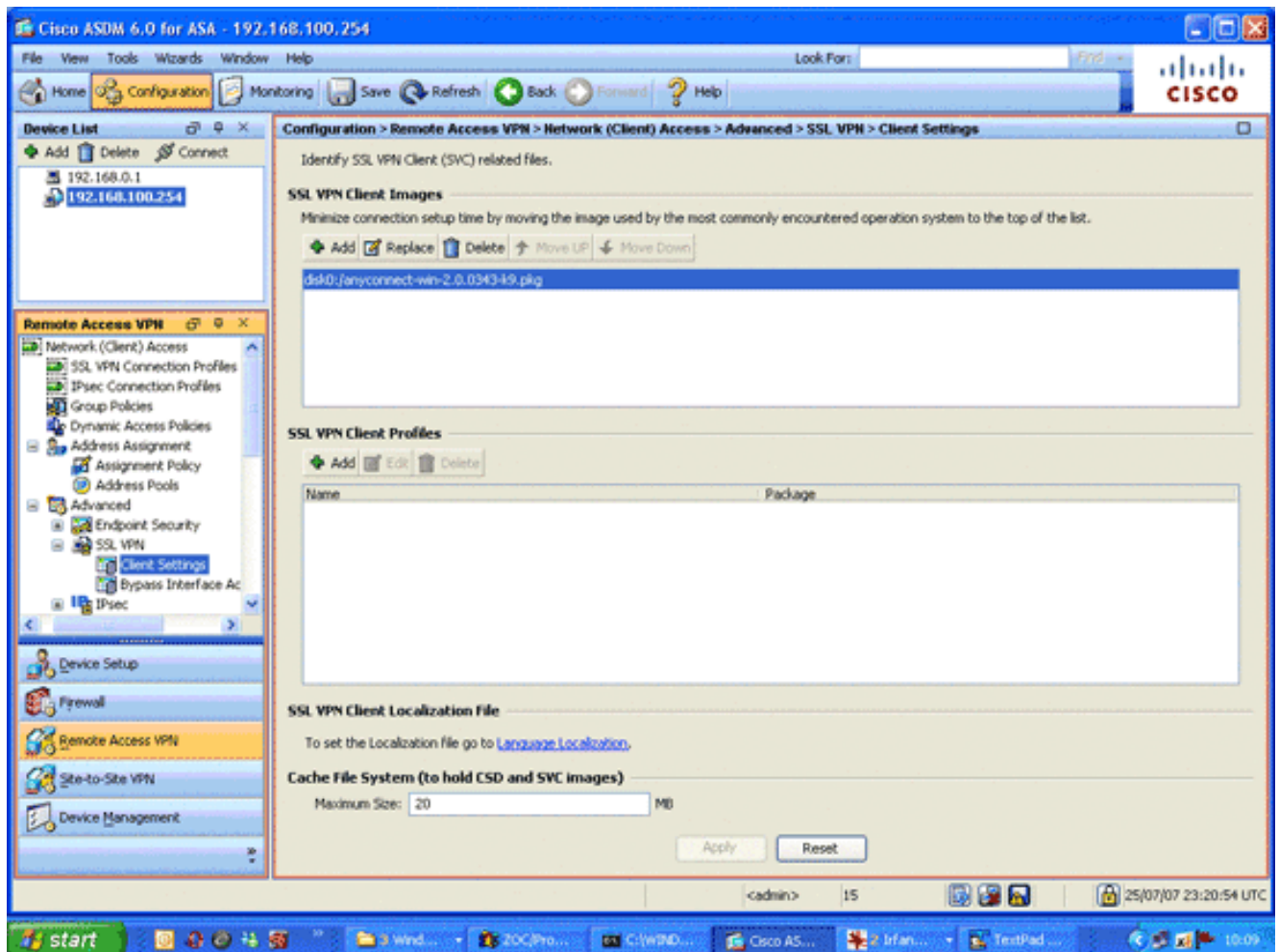
Cette étape décrit comment hiérarchiser les options de cryptage sécurisé, définir l'image du client VPN SSL et définir le profil de connexion.

1. Hiérarchisez les options de cryptage les plus sécurisées. Dans la zone Remote Access VPN, développez **Advanced**, puis sélectionnez **SSL Settings**. Dans la section Chiffrement, les algorithmes actifs sont empilés, de haut en bas, comme suit : AES256-SHA1AES128-SHA13DES-SHA1RC4-SHA1



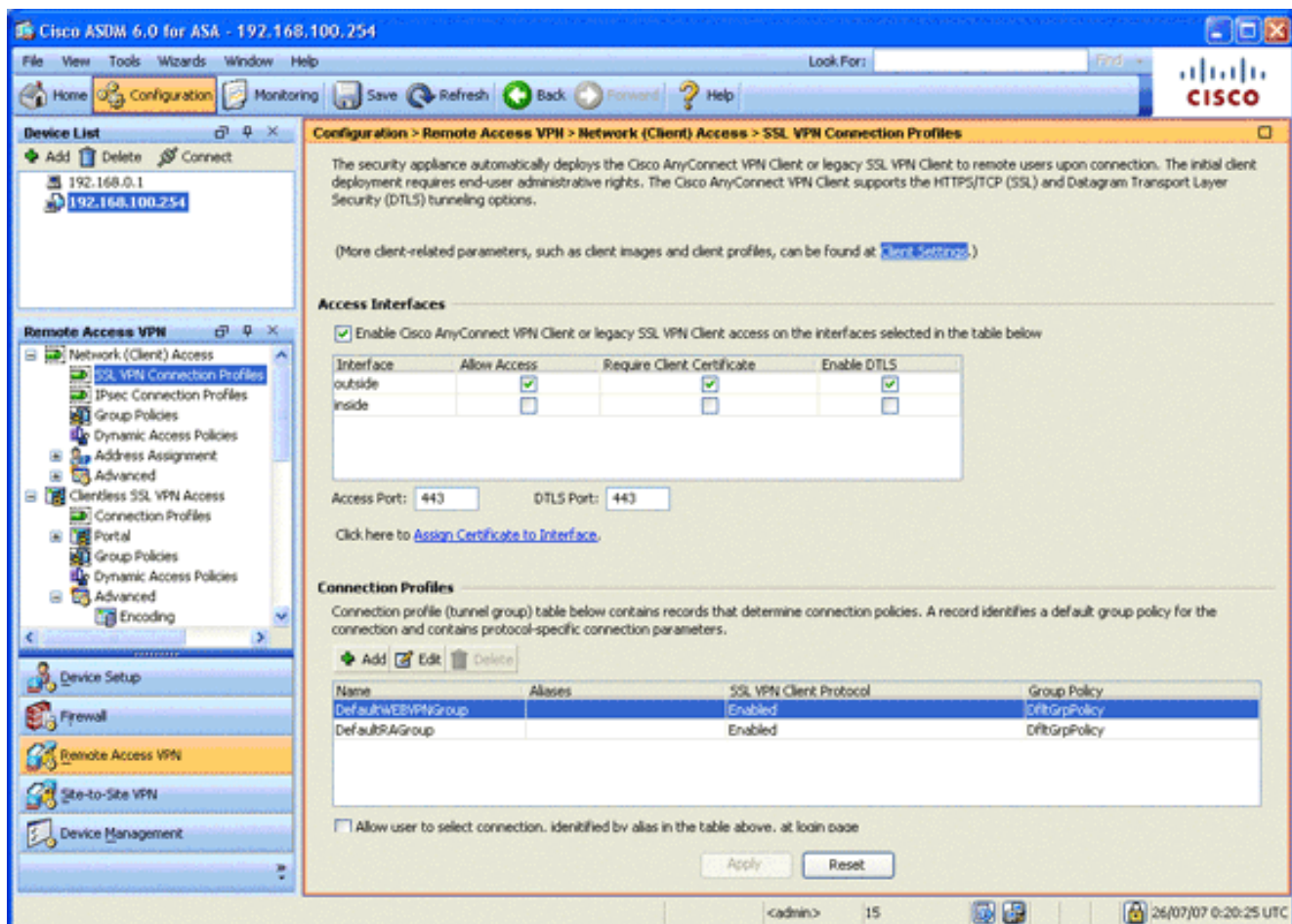
2. Définissez l'image du client VPN SSL pour AnyConnect Client. Dans la zone VPN d'accès à distance, développez **Advanced**, développez **SSL VPN**, et choisissez **Client Settings**. Dans la zone SSL VPN Client Images, cliquez sur **Add**. Choisissez le package AnyConnect stocké dans la mémoire Flash. Le package AnyConnect apparaît dans la liste des images du client VPN SSL, comme illustré dans cette image

:

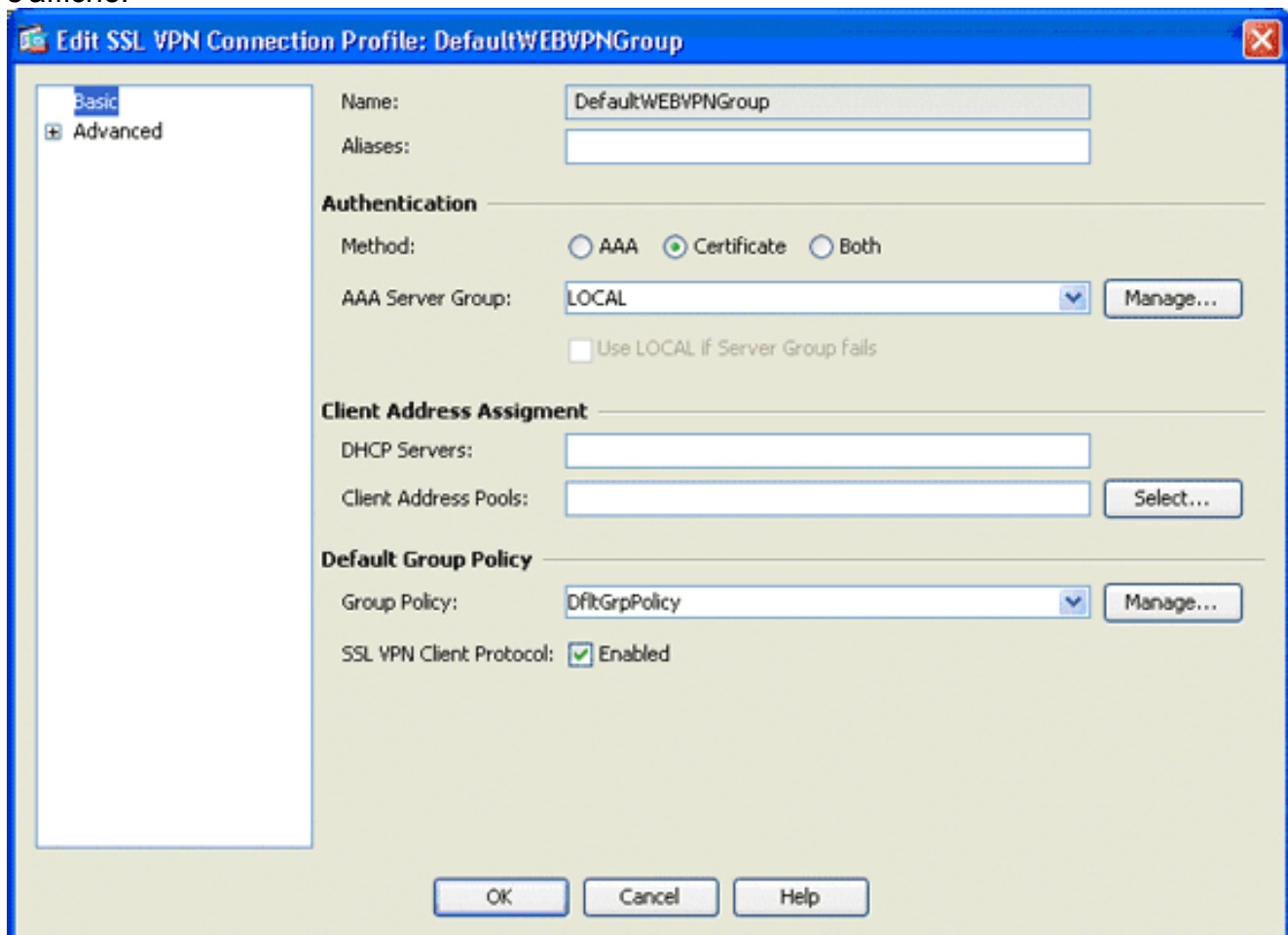


3. Définissez le profil de connexion DefaultWEBVPNGroup. Dans la zone VPN d'accès à distance, développez **Accès réseau (client)** et choisissez **Profils de connexion VPN SSL**. Dans la zone Access Interfaces, cochez la case **Enable Cisco AnyConnect VPN Client**. Pour l'interface externe, cochez les cases **Allow Access**, **Require Client Certificate** et **Enable DTLS** comme indiqué dans cette image

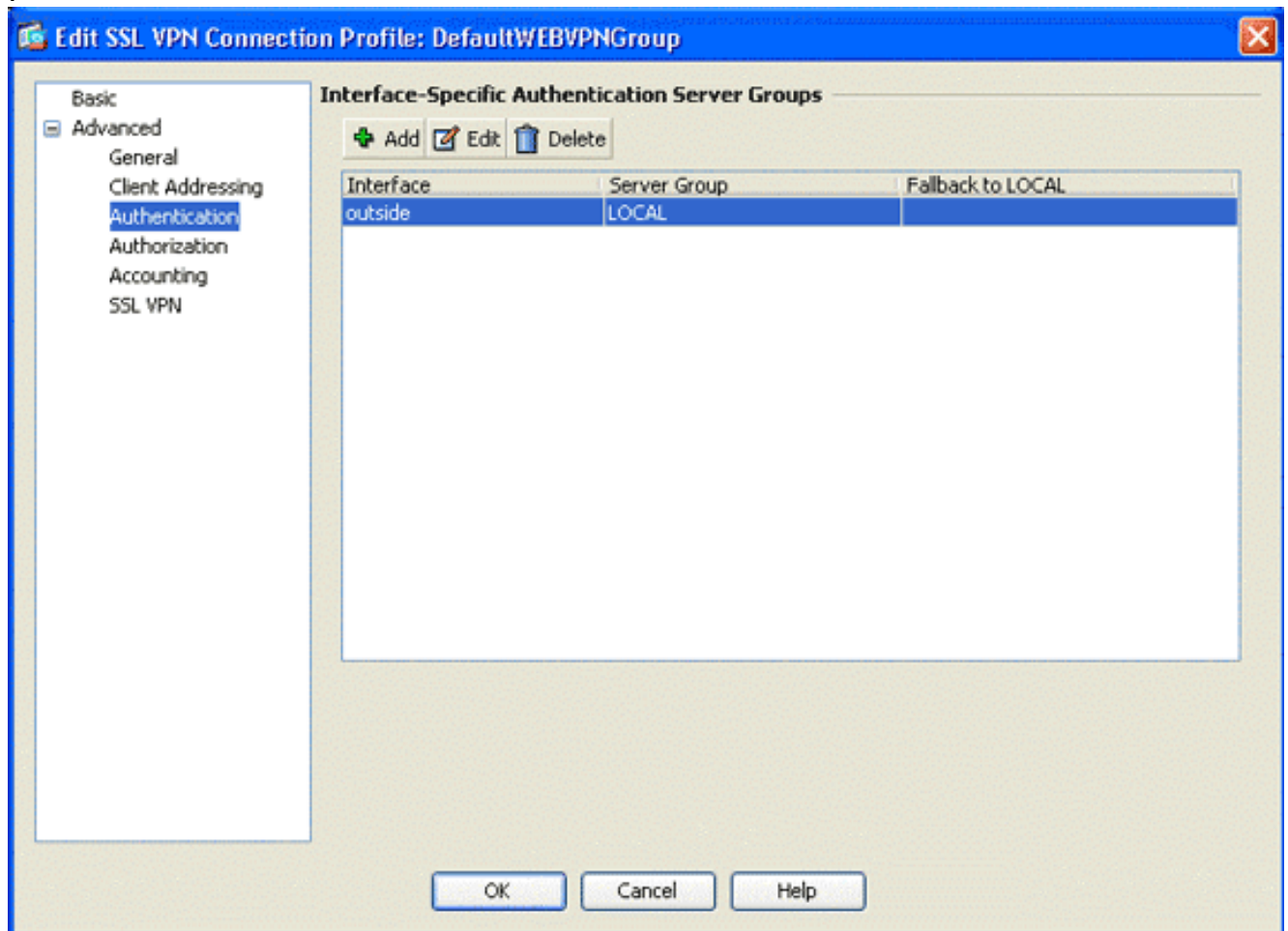
:



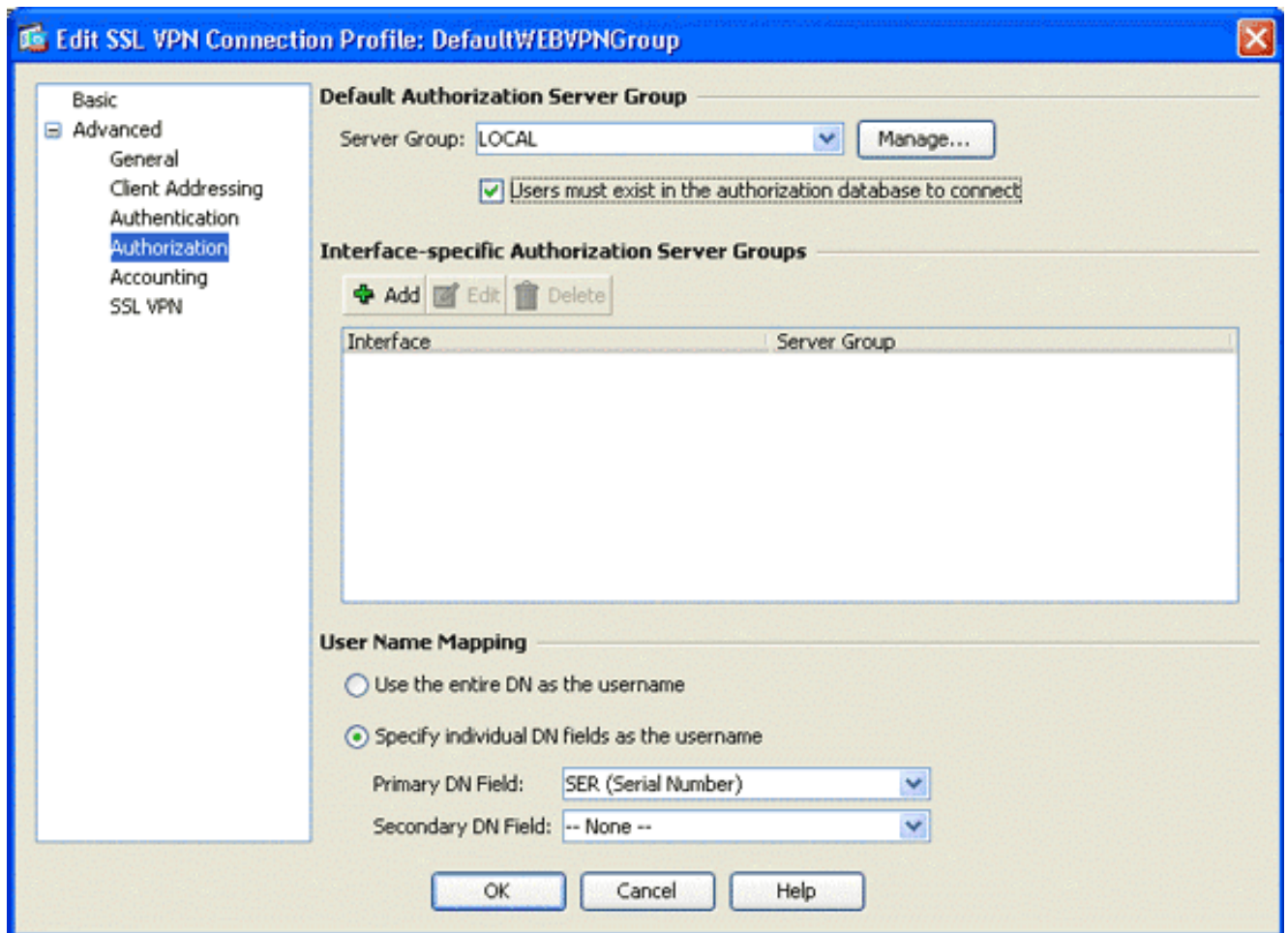
Dans la zone Profils de connexion, sélectionnez **DefaultWEBVPNGroup**, puis cliquez sur **Modifier**. La boîte de dialogue Modifier le profil de connexion VPN SSL s'affiche.



Dans la zone de navigation, sélectionnez **Basic**. Dans la zone Authentication, cliquez sur la case d'option **Certificat**. Dans la zone Stratégie de groupe par défaut, cochez la case **SSL VPN Client Protocol**. Développez **Advanced**, puis sélectionnez **Authentication**. Cliquez sur **Add**, puis ajoutez l'interface externe avec un groupe de serveurs local comme illustré dans cette image



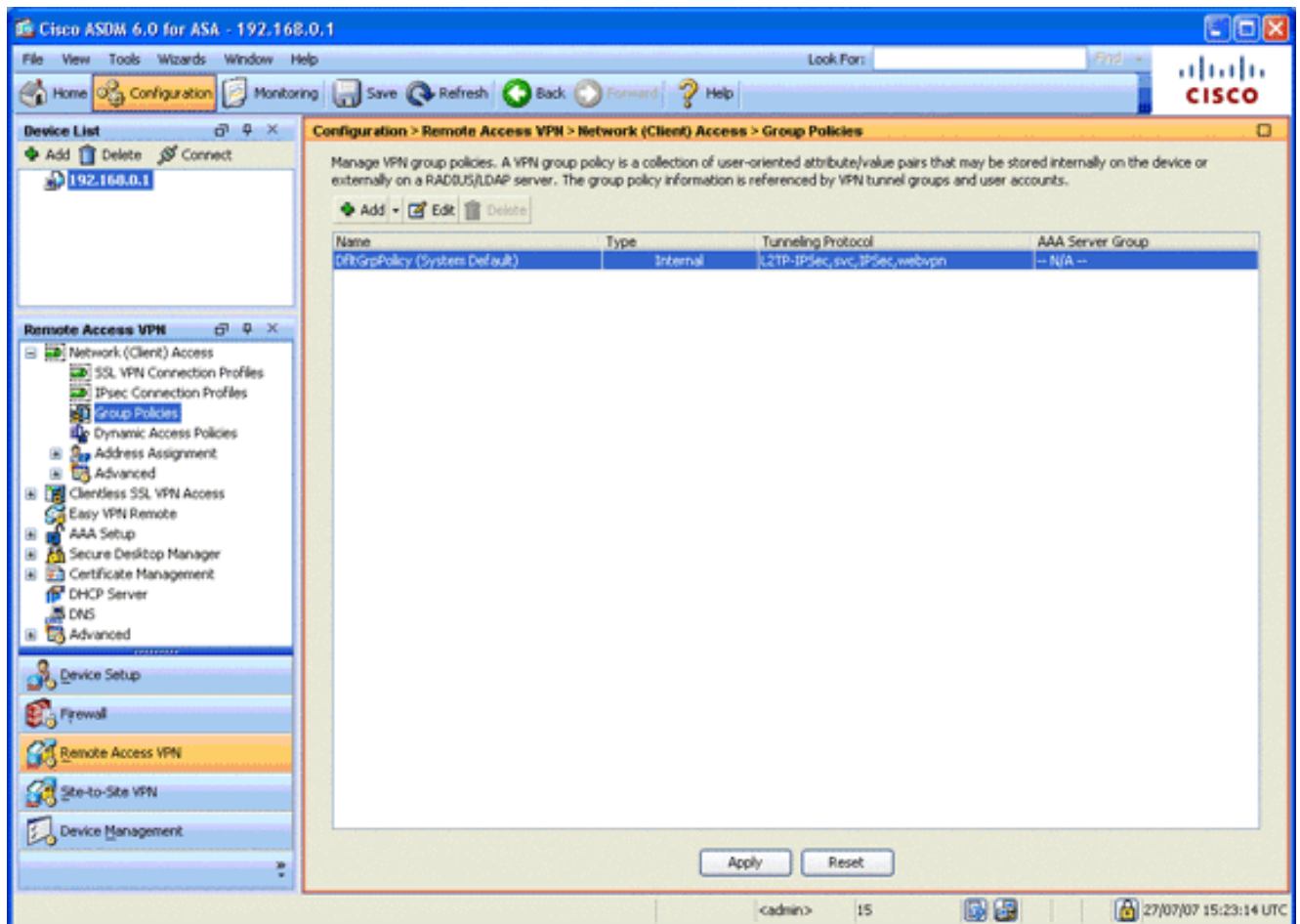
Dans la zone de navigation, sélectionnez **Autorisation**. Dans la zone Groupe de serveurs d'autorisation par défaut, sélectionnez **LOCAL** dans la liste déroulante Groupe de serveurs et cochez la case **Utilisateurs devant exister dans la base de données d'autorisation pour se connecter**. Dans la zone User Name Mapping, sélectionnez **SER (Serial Number)** dans la liste déroulante Primary DN Field, choisissez **None** dans le champ Secondary DN, puis cliquez sur **OK**.



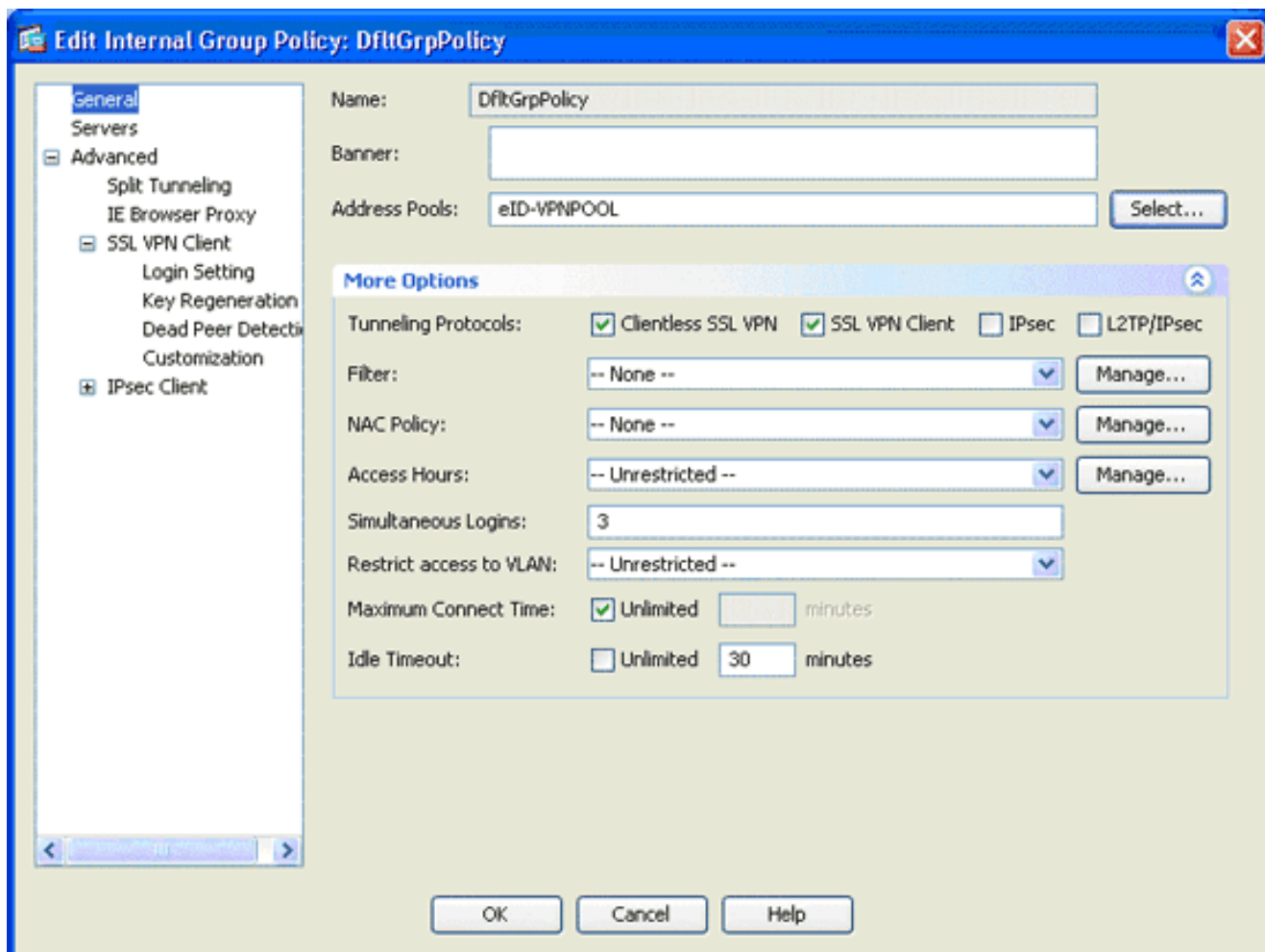
Étape 7. Définir la stratégie de groupe par défaut

Cette étape décrit comment définir la stratégie de groupe par défaut.

1. Dans la zone VPN d'accès à distance, développez **Accès réseau (client)**, puis choisissez **Stratégies de groupe**.



2. Choisissez **DfltGrpPolicy** dans la liste des stratégies de groupe, puis cliquez sur **Modifier**.
3. La boîte de dialogue Modifier la stratégie de groupe interne s'affiche.

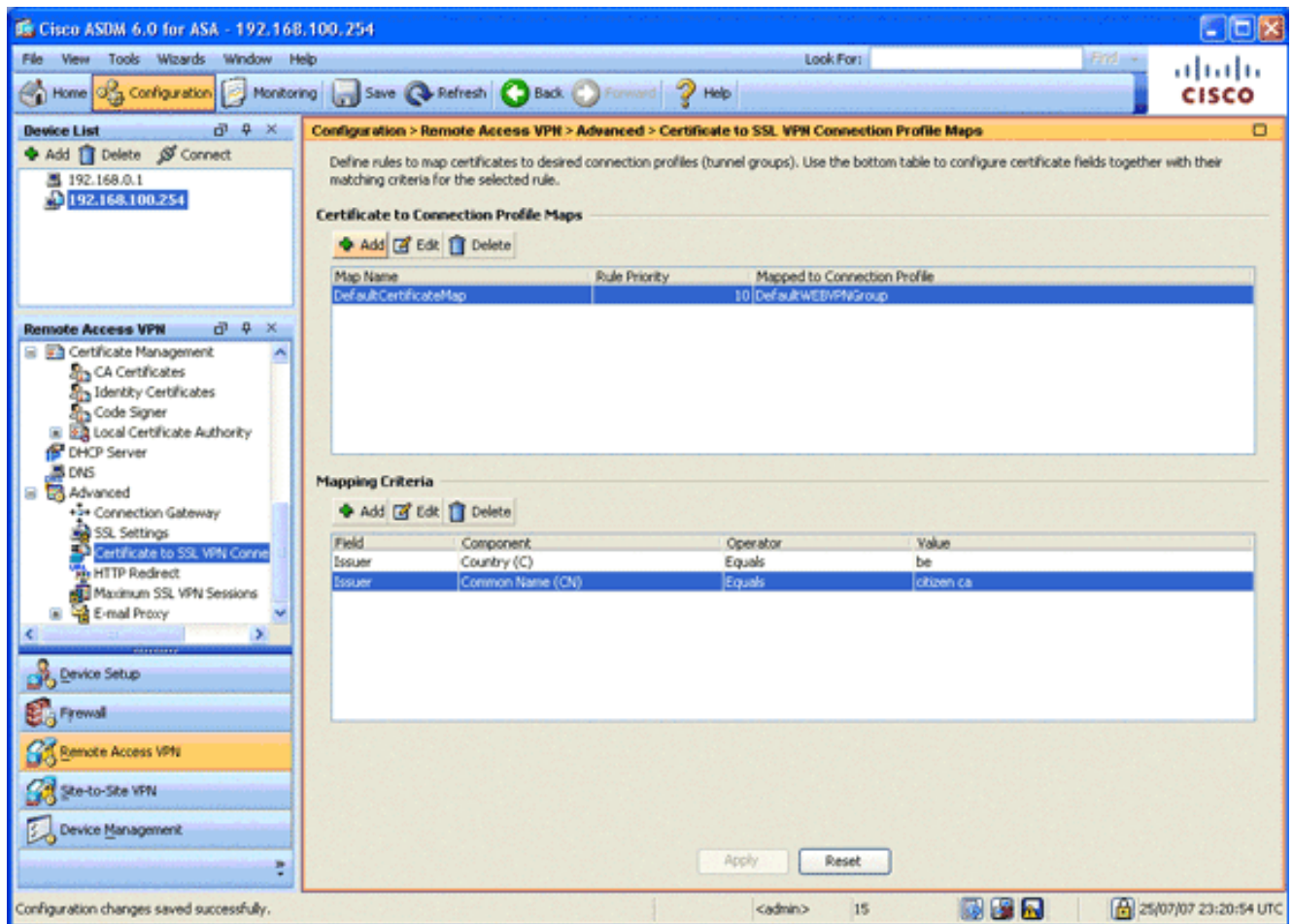


4. Dans la zone de navigation, sélectionnez **Général**.
5. Pour les pools d'adresses, cliquez sur **Sélectionner** afin de choisir un pool d'adresses, puis choisissez **eID-VPNPOOL**.
6. Dans la zone Autres options, décochez les cases **IPsec** et **L2TP/IPsec**, puis cliquez sur **OK**.

Étape 8. Définir le mappage de certificat

Cette étape décrit comment définir les critères de mappage de certificat.

1. Dans la zone VPN d'accès à distance, cliquez sur **Advanced**, puis sélectionnez **Certificate to SSL VPN Connection Profile Maps**.
2. Dans la zone Cartes de profil de certificat à connexion, cliquez sur **Ajouter**, puis choisissez **DefaultCertificateMap** dans la liste de mappage. Ce mappage doit correspondre à *DefaultWEBVPNProfile* dans le champ Mappé au profil de connexion.
3. Dans la zone Critères de mappage, cliquez sur **Ajouter**, et ajoutez les valeurs suivantes : Champ: Émetteur, Pays (C), Égal, " être " Champ: Émetteur, Nom commun (CN), Équals, " citoyen peut " Les critères de mappage doivent apparaître comme illustré dans cette image :

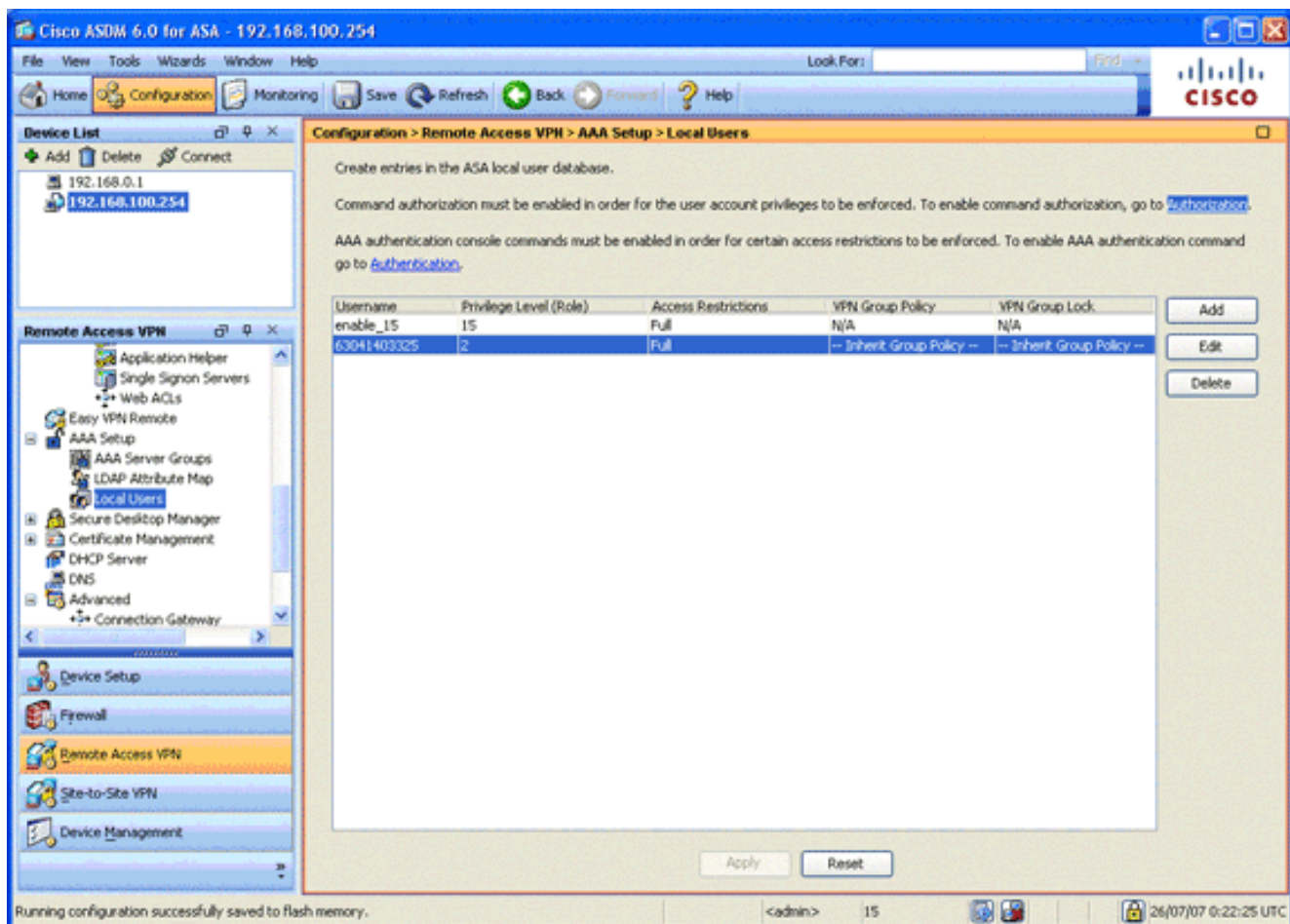


4. Cliquez sur Apply.

Étape 9. Ajouter un utilisateur local

Cette étape décrit comment ajouter un utilisateur local.

1. Dans la zone Remote Access VPN, développez **AAA Setup**, puis choisissez **Local Users**.
2. Dans la zone Utilisateurs locaux, cliquez sur **Ajouter**.
3. Dans le champ Username, saisissez le numéro de série du certificat utilisateur. Par exemple, 56100307215 (comme décrit dans la section [Certificat d'authentification](#) de ce document).



4. Cliquez sur Apply.

Étape 10. Redémarrer l'ASA

Redémarrez l'ASA afin de vous assurer que toutes les modifications sont appliquées aux services système.

Ajustement fin

Lors du test, certains tunnels SSL risquent de ne pas se fermer correctement. Puisque l'ASA suppose que le client AnyConnect peut se déconnecter et se reconnecter, le tunnel n'est pas abandonné, ce qui lui donne une chance de revenir. Cependant, lors des tests de laboratoire avec une licence de base (2 tunnels SSL par défaut), vous pouvez épuiser votre licence lorsque les tunnels SSL ne sont pas fermés correctement. Si ce problème se produit, utilisez la commande `vpn-sessiondb logoff <option>` afin de déconnecter toutes les sessions SSL actives.

Configuration d'une minute

Afin de créer rapidement une configuration fonctionnelle, réinitialisez votre ASA sur la valeur par défaut d'usine, et collez cette configuration en mode de configuration :

```
ciscosa
```

```
ciscoasa#conf t
ciscoasa#clear configure all
ciscoasa#domain-name cisco.be
```

```
ciscoasa#enable password 9jNfZuG3TC5tCVH0 encrypted
!
interface Vlan1
  nameif inside
  security-level 100
  ip address 192.168.0.1 255.255.255.0
interface Vlan2
  nameif outside
  security-level 0
  ip address 197.0.100.1 255.255.255.0
interface Ethernet0/0
  switchport access vlan 2
  no shutdown
interface Ethernet0/1
  no shutdown
!
passwd 2KFQnbNIdI.2KYOU encrypted
dns server-group DefaultDNS
  domain-name cisco.be
ip local pool eID-VPNPOOL 192.168.10.100-192.168.10.110
mask 255.255.255.0
asdm image disk0:/asdm-602.bin
no asdm history enable
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.255.0 inside
crypto ca trustpoint ASDM_TrustPoint0
  enrollment terminal
  crl configure
crypto ca certificate map DefaultCertificateMap 10
  issuer-name attr c eq be
  issuer-name attr cn eq citizen ca
crypto ca certificate chain ASDM_TrustPoint0
  certificate ca 580b056c5324dbb25057185ff9e5a650
    30820394 3082027c a0030201 02021058 0b056c53
24dbb250 57185ff9 e5a65030
    0d06092a 864886f7 0d010105 05003027 310b3009
06035504 06130242 45311830
    16060355 0403130f 42656c67 69756d20 526f6f74
20434130 1e170d30 33303132
    36323330 3030305a 170d3134 30313236 32333030
30305a30 27310b30 09060355
    04061302 42453118 30160603 55040313 0f42656c
6769756d 20526f6f 74204341
    30820122 300d0609 2a864886 f70d0101 01050003
82010f00 3082010a 02820101
    00c8a171 e91c4642 7978716f 9daea9a8 ab28b74d
c720eb30 915a75f5 e2d2cfc8
    4c149842 58adc711 c540406a 5af97412 2787e99c
e5714e22 2cd11218 aa305ea2
    21b9d9bb fff674eb 3101e73b 7e580f91 164d7689
a8014fad 226670fa 4b1d95c1
    3058eabc d965d89a b488eb49 4652dfd2 531576cb
145d1949 b16f6ad3 d3fdbcc2
    2dec453f 093f58be fcd4ef00 8c813572 bff718ea
96627d2b 287f156c 63d2caca
    7d05acc8 6d076d32 be68b805 40ae5498 563e66f1
30e8efc4 ab935e07 de328f12
    74aa5b34 2354c0ea 6ccef36 92a80917 eaa12dcf
6ce3841d de872e33 0b3c74e2
    21503895 2e5ce0e5 c631f9db 40fa6aa1 a48a939b
a7210687 1d27d3c4 a1c94cb0
```

```
6f020301 0001a381 bb3081b8 300e0603 551d0f01
01ff0404 03020106 300f0603
551d1301 01ff0405 30030101 ff304206 03551d20
043b3039 30370605 60380101
01302e30 2c06082b 06010505 07020116 20687474
703a2f2f 7265706f 7369746f
72792e65 69642e62 656c6769 756d2e62 65301d06
03551d0e 04160414 10f00c56
9b61ea57 3ab63597 6d9fddb9 148edbe6 30110609
60864801 86f84201 01040403
02000730 1f060355 1d230418 30168014 10f00c56
9b61ea57 3ab63597 6d9fddb9
148edbe6 300d0609 2a864886 f70d0101 05050003
82010100 c86d2251 8a61f80f
966ed520 b281f8c6 dca31600 dacd6ae7 6b2afa59
48a74c49 37d773a1 6a01655e
32bde797 d3d02e3c 73d38c7b 83efd642 c13fa8a9
5d0f37ba 76d240bd cc2d3fd3
4441499c fd5b29f4 0223225b 711bbf58 d9284e2d
45f4dae7 b5634544 110d2a7f
337f3649 b4ce6ea9 0231ae5c fdc889bf 427bd7f1
60f2d787 f6572e7a 7e6a1380
1ddce3d0 631e3d71 31b160d4 9e08caab f094c748
755481f3 1bad779c e8b28fdb
83ac8f34 6be8bfc3 d9f543c3 6455eb1a bd368636
ba218c97 1a21d4ea 2d3bacba
eca71dab beb94a9b 352f1c5c 1d51a71f 54ed1297
fff26e87 7d46c974 d6efeb3d
7de6596e 069404e4 a2558738 286a225e e2be7412
b004432a
quit
no crypto isakmp nat-traversal
!
dhcpd address 192.168.0.2-192.168.0.129 inside
dhcpd enable inside
dhcpd address 197.0.100.20-197.0.100.30 outside
dhcpd enable outside
!
service-policy global_policy global
ssl encryption aes256-sha1 aes128-sha1 3des-sha1 rc4-
sha1
ssl certificate-authentication interface outside port
443
webvpn
enable outside
svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1
svc enable
certificate-group-map DefaultCertificateMap 10
DefaultWEBVPNGroup
group-policy DfltGrpPolicy attributes
vpn-tunnel-protocol svc webvpn
address-pools value eID-VPNPOOL
username 63041403325 nopassword
tunnel-group DefaultWEBVPNGroup general-attributes
authentication-server-group (outside) LOCAL
authorization-server-group LOCAL
authorization-required
authorization-dn-attributes SER
tunnel-group DefaultWEBVPNGroup webvpn-attributes
authentication certificate
exit
copy run start
```

Informations connexes

- [Logiciels pare-feu Cisco PIX](#)
- [Références des commandes du pare-feu Cisco Secure PIX](#)
- [Notices de champs relatives aux produits de sécurité \(y compris PIX\)](#)
- [Demandes de commentaires \(RFC\)](#)
- [Support et documentation techniques - Cisco Systems](#)