ASA 8.x : configuration AnyConnect SSL VPN CAC-SmartCards pour Windows

Table des matières

Introduction

Ce document contient un exemple de configuration d'un serveur de sécurité adaptatif dédié Cisco (ASA) pour l'accès à distance AnyConnect VPN sur Windows au moyen d'une carte d'accès commune (CAC) pour l'authentification.

L'objectif de ce document est de couvrir la configuration de Cisco ASA avec Adaptive Security Device Manager (ASDM), Cisco AnyConnect VPN Client et Microsoft Active Directory (AD)/Lightweight Directory Access Protocol (LDAP).

La configuration de ce guide utilise le serveur Microsoft AD/LDAP. Ce document couvre également des fonctionnalités avancées telles que OCSP, les mappages d'attributs LDAP et les politiques d'accès dynamique (DAP).

Conditions préalables

Exigences

Une compréhension de base de Cisco ASA, du client Cisco AnyConnect, de Microsoft AD/LDAP et de l'infrastructure à clé publique (PKI) est utile pour comprendre la configuration complète. La connaissance de l'appartenance à un groupe AD, des propriétés utilisateur et des objets LDAP permet de corréler le processus d'autorisation entre les attributs de certificat et les objets AD/LDAP.

Composants utilisés

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

- Appareil de sécurité adaptatif (ASA) de la gamme Cisco 5500 qui exécute le logiciel version 8.0(x) et ultérieure

- Cisco Adaptive Security Device Manager (ASDM) version 6.x pour ASA 8.x
- Client VPN Cisco AnyConnect pour Windows

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.

Configuration de Cisco ASA

Cette section couvre la configuration de Cisco ASA via ASDM. Il couvre les étapes nécessaires pour déployer un tunnel d'accès à distance VPN via une connexion SSL AnyConnect. Le certificat CAC est utilisé pour l'authentification et l'attribut User Principal Name (UPN) du certificat est renseigné dans Active Directory pour l'autorisation.

Considérations de déploiement

- Ce guide ne couvre PAS les configurations de base telles que les interfaces, DNS, NTP, le routage, l'accès aux périphériques, l'accès ASDM, etc. Il est supposé que l'opérateur réseau connaît bien ces configurations.

  Référez-vous à Appliances de sécurité multifonction pour plus d'informations.

- Les sections surlignées en ROUGE sont des configurations obligatoires requises pour l'accès VPN de base. Par exemple, un tunnel VPN peut être configuré avec la carte CAC sans effectuer de vérifications OCSP, de mappages LDAP et de vérifications DAP (Dynamic Access Policy). Le DoD impose la vérification OCSP, mais le tunnel fonctionne sans OCSP configuré.
- Les sections surlignées en BLEU sont des fonctionnalités avancées qui peuvent être incluses pour renforcer la sécurité de la conception.
- Les VPN AnyConnect/SSL et ASDM ne peuvent pas utiliser les mêmes ports sur la même interface. Il est recommandé de modifier les ports de l'un ou l'autre pour obtenir l'accès. Par exemple, utilisez le port 445 pour l'ASDM et laissez 443 pour le VPN AC/SSL. L'accès à l'URL ASDM a été modifié dans 8.x. Utilisez `https://<adresse_ip>:<port>/admin.html`.
- L'image ASA requise est au moins 8.0.2.19 et ASDM 6.0.2.
- AnyConnect/CAC est pris en charge avec Vista.
- Reportez-vous à l'Annexe A pour des exemples de mappage LDAP et de stratégie d'accès dynamique pour une application de stratégie supplémentaire.
- Reportez-vous à l'Annexe D pour savoir comment vérifier les objets LDAP dans MS.
- Reportez-vous à Informations associées pour obtenir la liste des ports d'application pour la configuration du pare-feu.

Configuration AAA (Authentication, Authorization, Accounting)

Vous êtes authentifié avec l'utilisation du certificat dans leur Common Access Card (CAC) via le serveur DISACertificate Authority (CA) ou le serveur CA de leur propre organisation. Le certificat doit être valide pour l'accès distant au réseau. Outre l'authentification, vous devez également être autorisé à utiliser un objet Microsoft Active Directory ou LDAP (Lightweight Directory Access Protocol). Le ministère de la Défense (DoD) exige l'utilisation de l'attribut User Principal Name (UPN) pour l'autorisation, qui fait partie de la section Subject Alternative Name (SAN) du certificat. L'UPN ou l'EDI/PI doit être au format suivant : 1234567890@mil. Ces configurations montrent comment configurer le serveur AAA dans l'ASA avec un serveur LDAP pour l'autorisation. Reportez-vous à l'Annexe A pour une configuration supplémentaire avec le mappage d'objet LDAP.

Configurer le serveur LDAP

Procédez comme suit :

1. Choisissez Remote Access VPN > AAA Setup > AAA Server Group.
2. Dans le tableau des groupes de serveurs AAA, cliquez sur Add 3.
3. Entrez le nom du groupe de serveurs et sélectionnez LDAP dans la case d'option Protocol. Voir la figure 1.
4. Dans Serveurs de la table des groupes sélectionnés, cliquez sur Ajouter. Assurez-vous que le serveur que vous avez créé est mis en surbrillance dans le tableau précédent.
5. Dans la fenêtre de modification du serveur AAA, procédez comme suit. Voir la figure 2.

Remarque : sélectionnez l'option Enable LDAP over SSL si votre LDAP/AD est configuré pour ce type de connexion.

---

a. Sélectionnez l'interface où se trouve le serveur LDAP. Ce guide s'affiche à l'intérieur de l'interface.

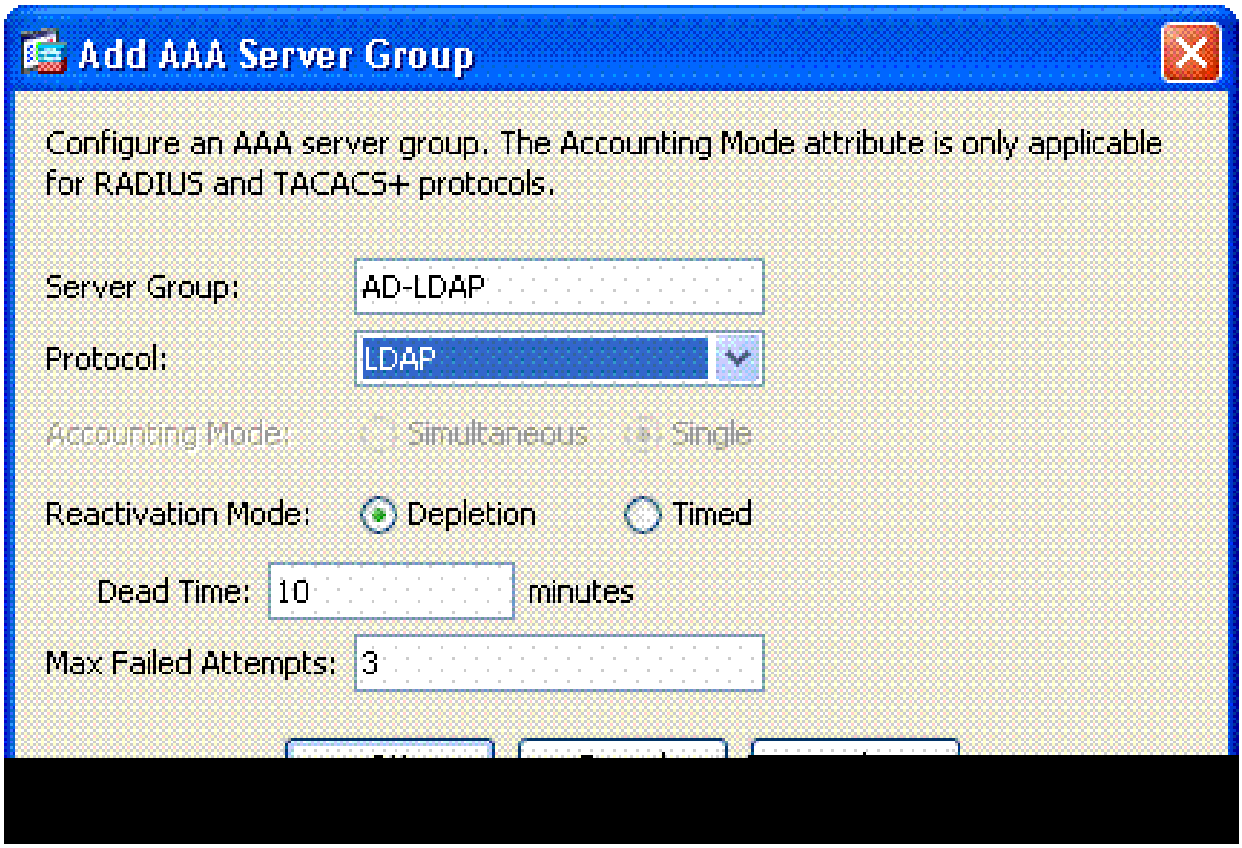
b. Saisissez l'adresse IP du serveur.

c. Saisissez le port du serveur. Le port LDAP par défaut est 389.

d. Sélectionnez Type de serveur.

e. Saisissez le DN de base. Demandez ces valeurs à votre administrateur AD/LDAP.

Figure-1



f. Sous l'option de portée, choisissez la réponse appropriée. Cela dépend du DN de base. Demandez de l'aide à votre administrateur AD/LDAP.

g. Dans l'attribut d'attribution de noms, entrez userPrincipalName. Il s'agit de l'attribut utilisé pour l'autorisation utilisateur dans le serveur AD/LDAP.

h. Dans le champ Login DN, saisissez le DN de l'administrateur.

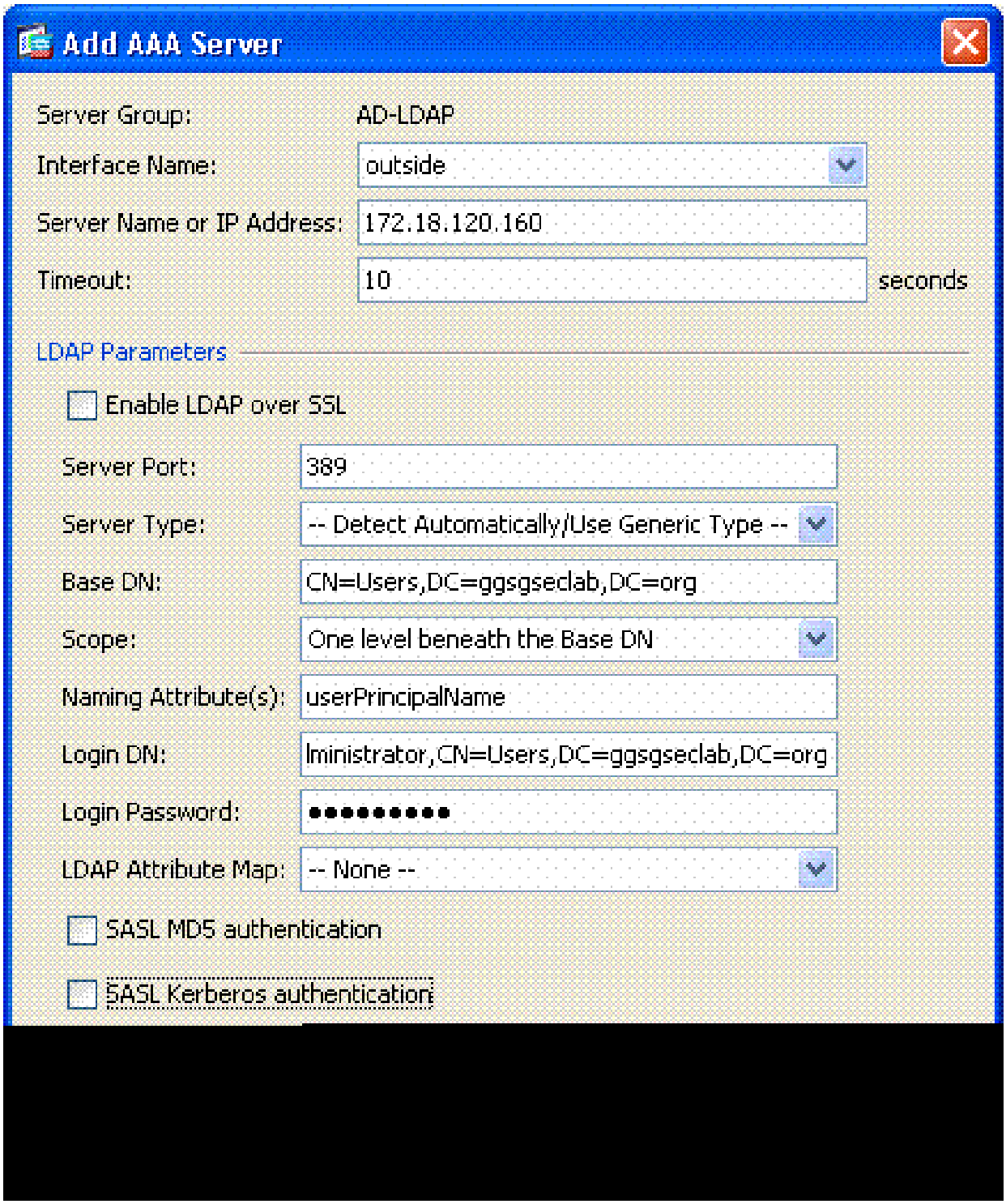
> Remarque : vous disposez de droits d'administration ou de droits d'accès pour afficher/rechercher la structure LDAP qui inclut les objets utilisateur et l'appartenance à un groupe.

---

i. Dans le champ Login Password, saisissez le mot de passe de l'administrateur.

j. Laissez l'attribut LDAP sur aucun.

Figure-2



> Remarque : vous utiliserez cette option ultérieurement dans la configuration pour ajouter d'autres objets AD/LDAP pour l'autorisation.

k. Cliquez sur OK.

6. Cliquez sur OK.

Gérer les certificats

Il y a deux étapes afin d'installer des certificats sur l'ASA. Tout d'abord, installez les certificats CA

(autorité de certification racine et subordonnée) nécessaires. Ensuite, inscrivez l'ASA à une autorité de certification spécifique et obtenez le certificat d'identité. DoD PKI utilise ces certificats, Racine CA2, Racine de classe 3, CA## Intermédiaire avec lequel l'ASA est inscrit, certificat d'ID ASA et certificat OCSP. Cependant, si vous choisissez de ne pas utiliser OCSP, le certificat OCSP n'a pas besoin d'être installé.

Remarque : contactez votre POC de sécurité afin d'obtenir des certificats racine ainsi que des instructions sur la façon de s'inscrire pour obtenir un certificat d'identité pour un périphérique. Un certificat SSL doit être suffisant pour l'ASA pour l'accès à distance. Un certificat double SAN n'est pas requis.

Remarque : la chaîne CA DoD doit également être installée sur l'ordinateur local. Les certificats peuvent être affichés dans le magasin de certificats Microsoft avec Internet Explorer. Le DoD a produit un fichier batch qui ajoute automatiquement toutes les autorités de certification à la machine. Demandez plus d'informations à votre POC PKI.

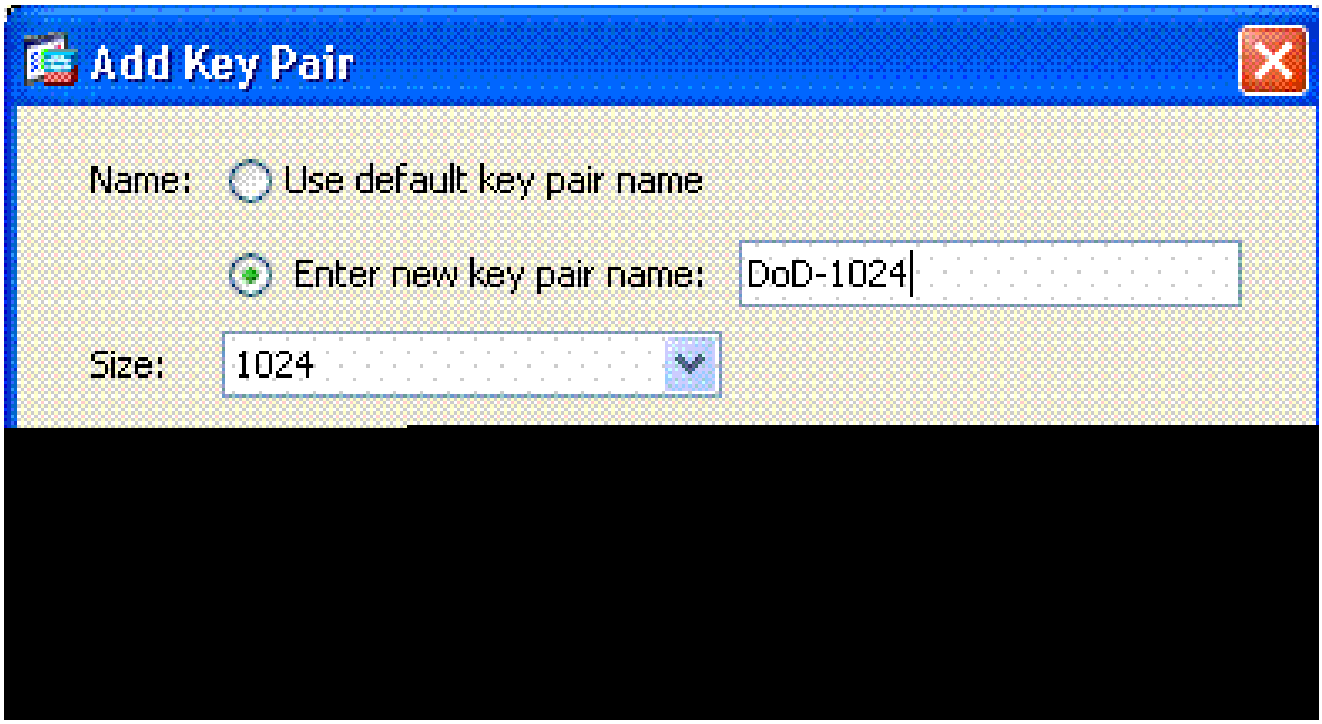
Remarque : la racine CA2 et Classe 3 DoD, ainsi que l'ID ASA et l'intermédiaire CA qui a émis le certificat ASA doivent être les seules CA nécessaires à l'authentification des utilisateurs. Tous les intermédiaires CA actuels appartiennent à la chaîne racine CA2 et Class 3 et sont approuvés tant que les racines CA2 et Class 3 sont ajoutées.

Générer des clés

Procédez comme suit :

1. Choisissez Remote Access VPN > Certificate Management > Identity Certificate > Add.
2. Choisissez Add a new id certificate, puis New by the key pair option.
3. Dans la fenêtre Ajouter une paire de clés, entrez un nom de clé, DoD-1024. Cliquez sur la case d'option pour ajouter une nouvelle clé. Voir la figure 3.

   Figure 3



4. Choisissez la taille de la clé.
5. Conserver l'utilisation à usage général.
6. Cliquez sur Generate Now.

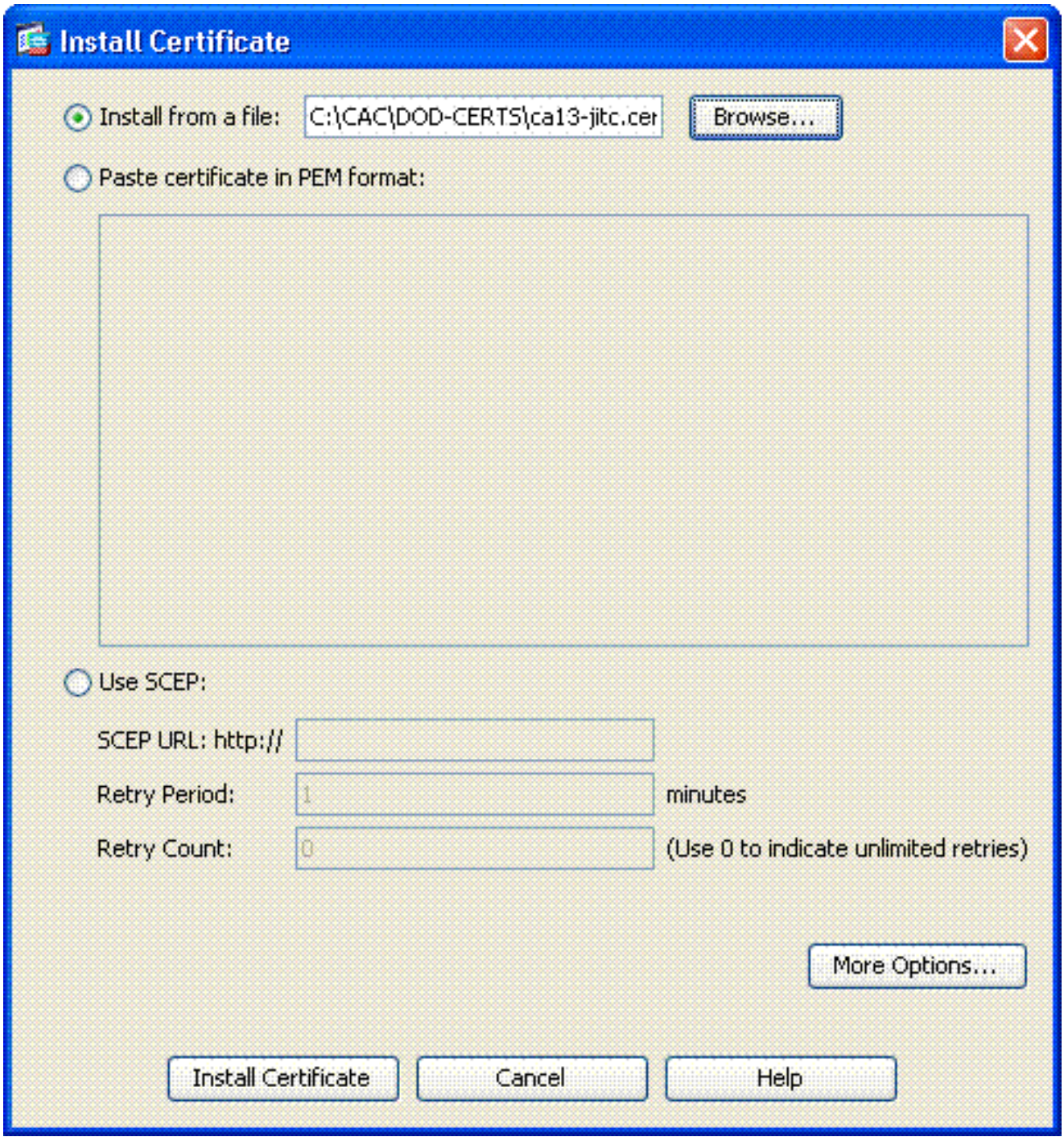
> Remarque : DoD Root CA 2 utilise une clé de 2 048 bits. Une deuxième clé qui utilise une paire de clés de 2 048 bits doit être générée pour pouvoir utiliser cette autorité de certification. Effectuez les étapes précédentes ci-dessus afin d'ajouter une deuxième clé.

Installer les certificats CA racine

Procédez comme suit :

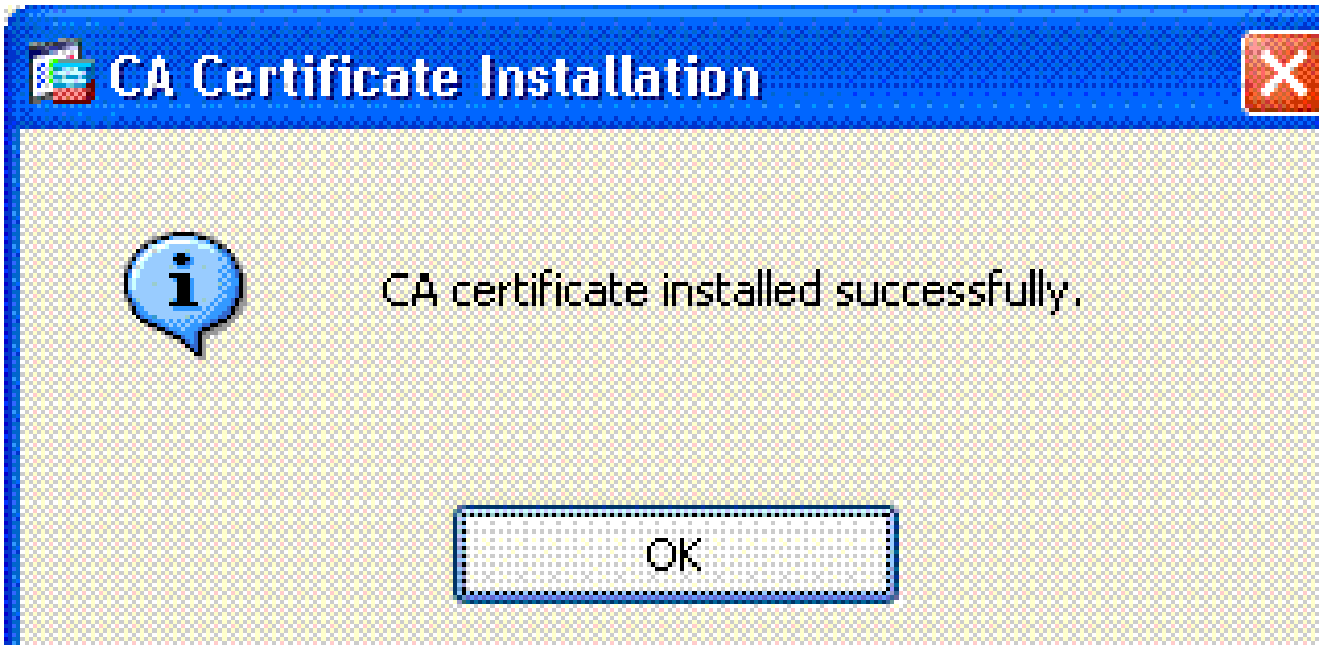
1. Choisissez Remote Access VPN > Certificate Management > CA Certificate > Add.
2. Choisissez Install from File et accédez au certificat.
3. Sélectionnez Installer le certificat.

Figure 4 : Installation du certificat racine



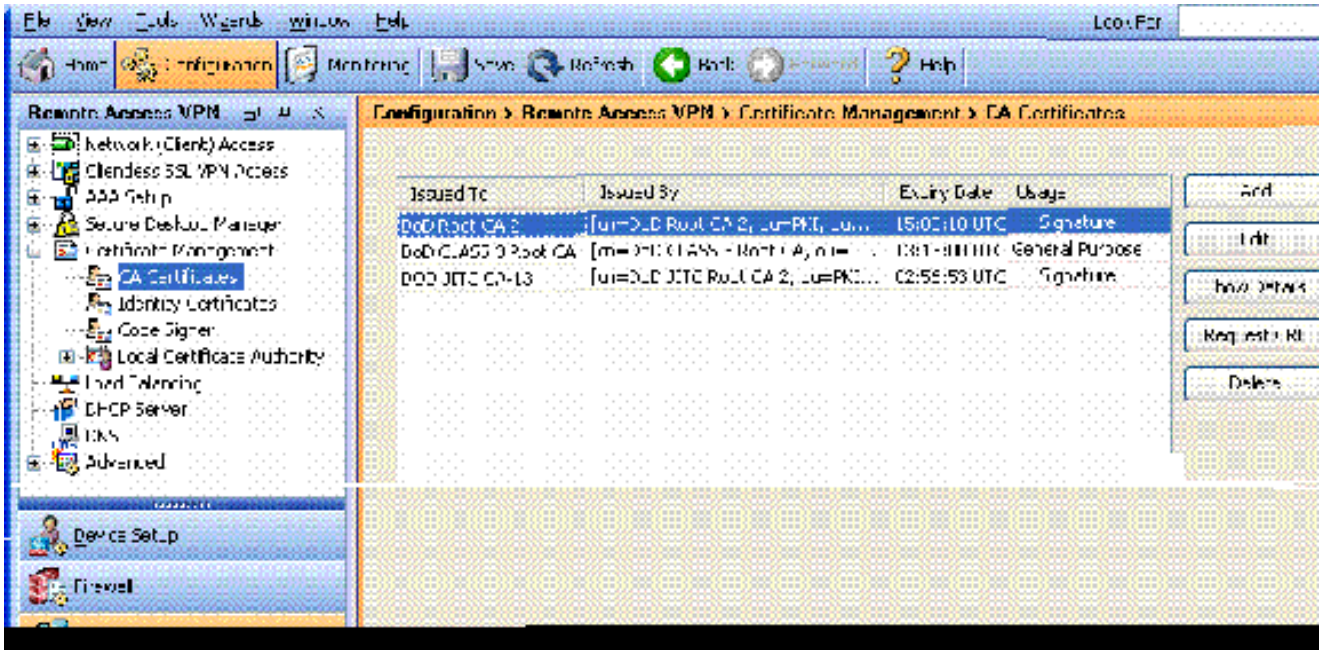
4. Cette fenêtre doit s'afficher. Voir la figure 5.

Figure 5



Remarque : répétez les étapes 1 à 3 pour chaque certificat que vous souhaitez installer. DoD PKI nécessite un certificat pour chacun de ces éléments : racine CA 2, racine de classe 3, intermédiaire CA##, ID ASA et serveur OCSP. Le certificat OCSP n'est pas nécessaire si vous n'utilisez pas OCSP.

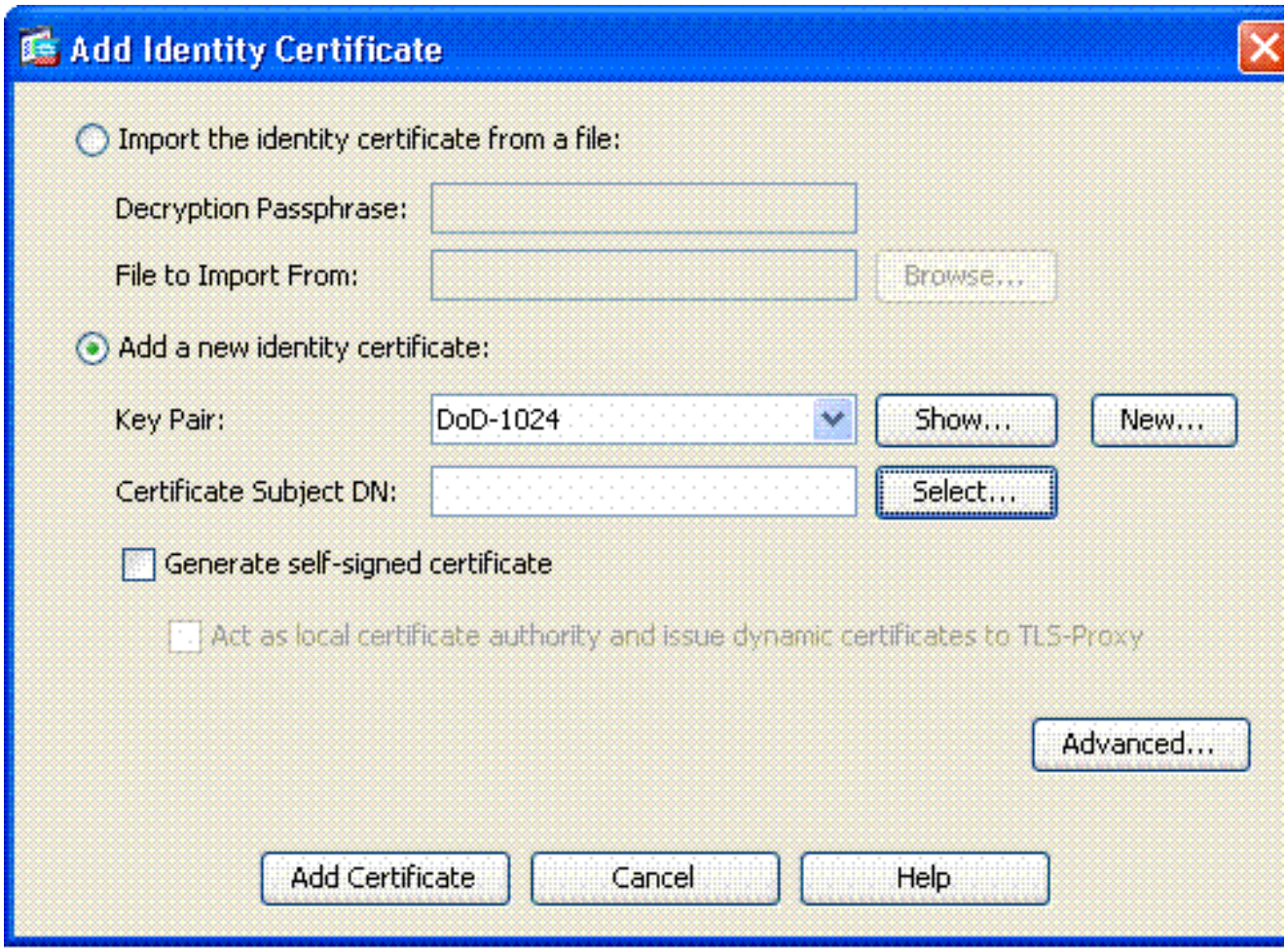
Figure 6 : Installation du certificat racine



Inscrire ASA et installer le certificat d'identité

1. Choisissez Remote Access VPN > Certificate Management > Identity Certificate > Add.
2. Sélectionnez Ajouter un nouveau certificat d'ID.
3. Sélectionnez la paire de clés DoD-1024. Voir figure 7

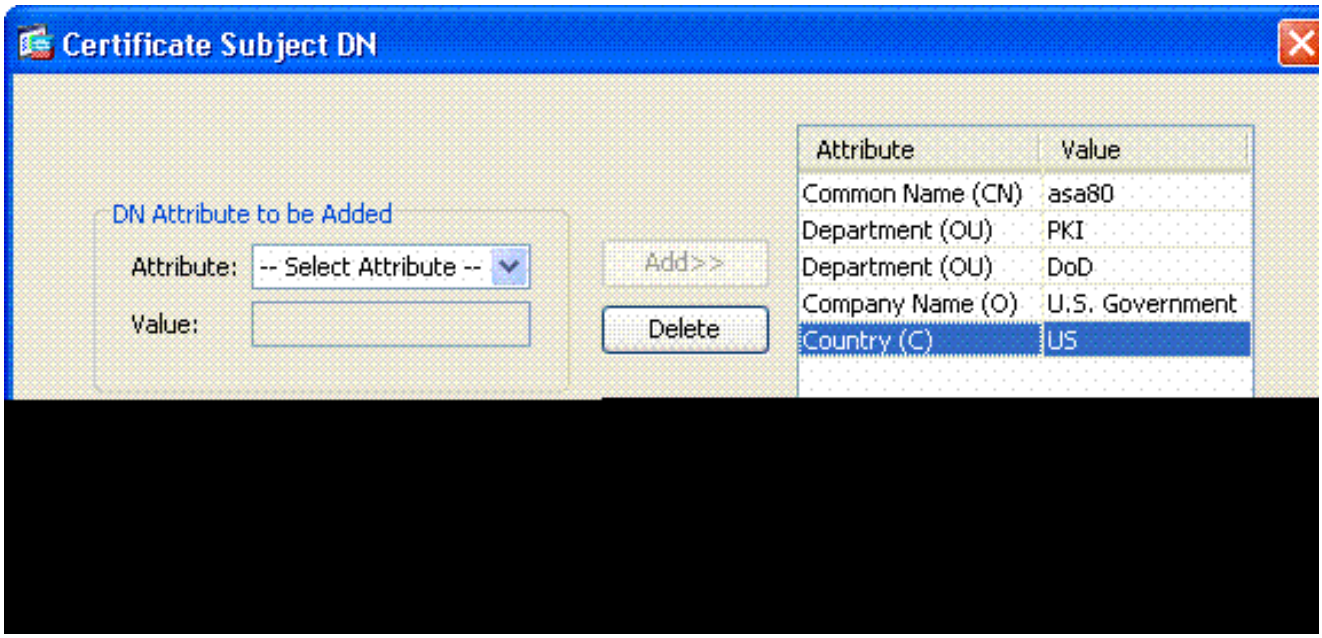
Figure 7 : Paramètres du certificat d'identité



4. Accédez à la zone Certificate subject DN et cliquez sur Select.

5. Dans la fenêtre Certificate Subject DN, saisissez les informations relatives au périphérique. Reportez-vous à la Figure 8 par exemple.

Figure 8 : Modifier le DN



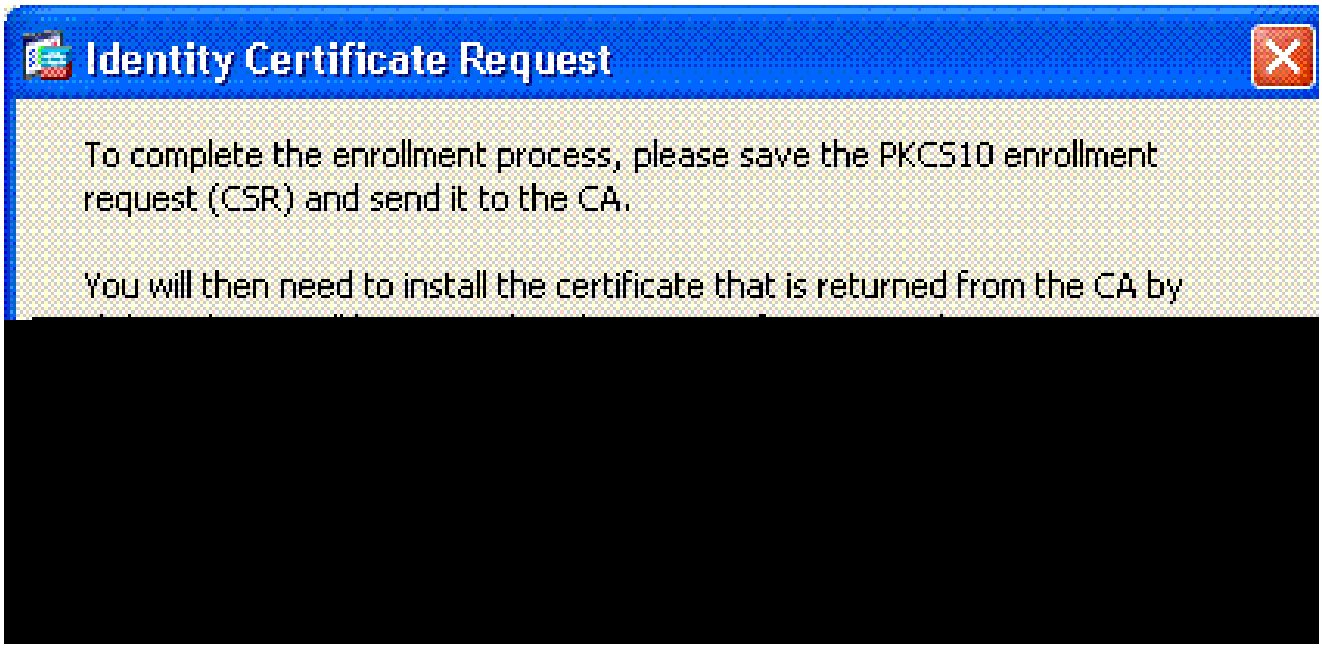
6. Cliquez sur OK.

Remarque : veillez à utiliser le nom d'hôte du périphérique configuré dans votre système lorsque vous ajoutez le DN objet. Le POC PKI peut vous indiquer les champs obligatoires requis.

---

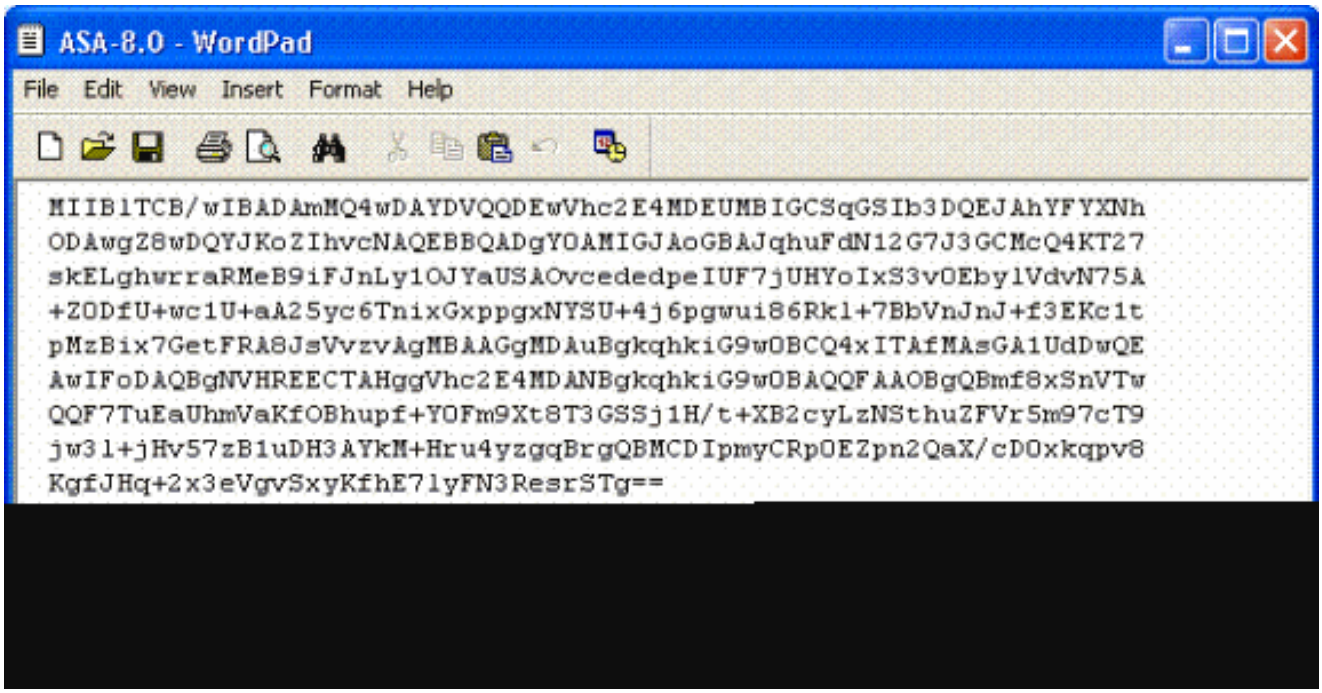
7. Sélectionnez Ajouter un certificat.
8. Cliquez sur Browse afin de sélectionner le répertoire où vous voulez enregistrer la demande. Voir la figure 9.

Figure 9 : Demande de certificat



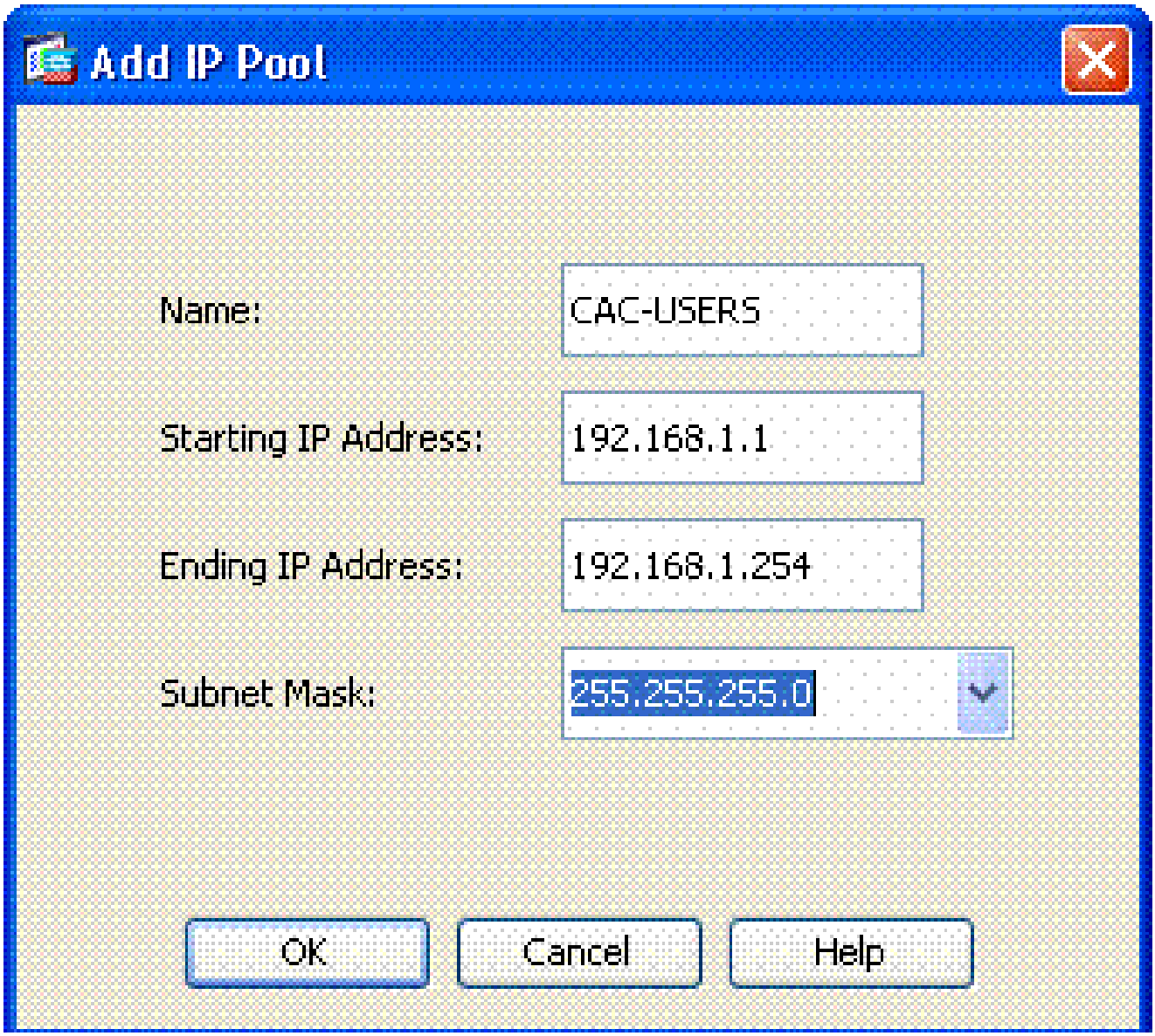
9. Ouvrez le fichier avec WordPad, copiez la demande dans la documentation appropriée et envoyez-la à votre PC ICP. Voir la figure 10.

Figure 10 : Demande d'inscription



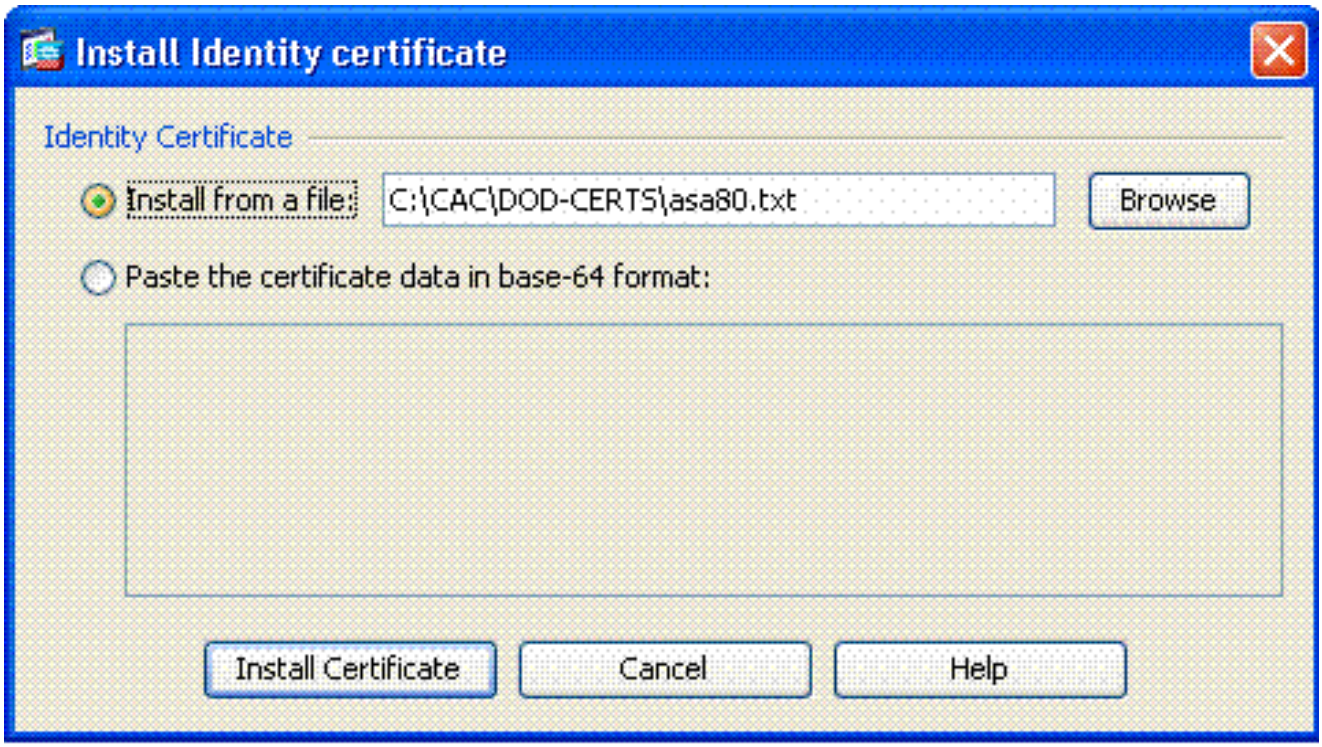
10. Une fois que vous avez reçu le certificat de l'administrateur CA, choisissez Remote Access VPN > Certificate Management > ID Certificate > Install. Voir la figure 11.

    Figure 11 : Importation du certificat d'identité



11. Dans la fenêtre Installer le certificat, accédez au certificat d'ID et sélectionnez Installer le certificat. Reportez-vous à la Figure 12.

    Figure 12 : Installation du certificat d'identité



Remarque : il est recommandé d'exporter le point de confiance du certificat d'ID afin d'enregistrer les paires certificat et clé émises. Cela permet à l'administrateur ASA d'importer le certificat et les paires de clés vers un nouvel ASA en cas de RMA ou de défaillance matérielle. Référez-vous à Exportation et importation de points de confiance pour plus d'informations.

Remarque : cliquez sur SAVE afin d'enregistrer la configuration dans la mémoire flash.

Configuration VPN AnyConnect

Il existe deux options afin de configurer les paramètres VPN dans ASDM. La première option consiste à utiliser l'assistant VPN SSL. Il s'agit d'un outil facile à utiliser pour les utilisateurs qui ne connaissent pas la configuration VPN. La deuxième option est de le faire manuellement et de passer par chaque option. Ce guide de configuration utilise la méthode manuelle.

Remarque : il existe deux méthodes pour transmettre le client AC à l'utilisateur :

1. Vous pouvez télécharger le client à partir du site Web de Cisco et l'installer sur son ordinateur.
2. L'utilisateur peut accéder à l'ASA via un navigateur Web et le client peut être téléchargé.

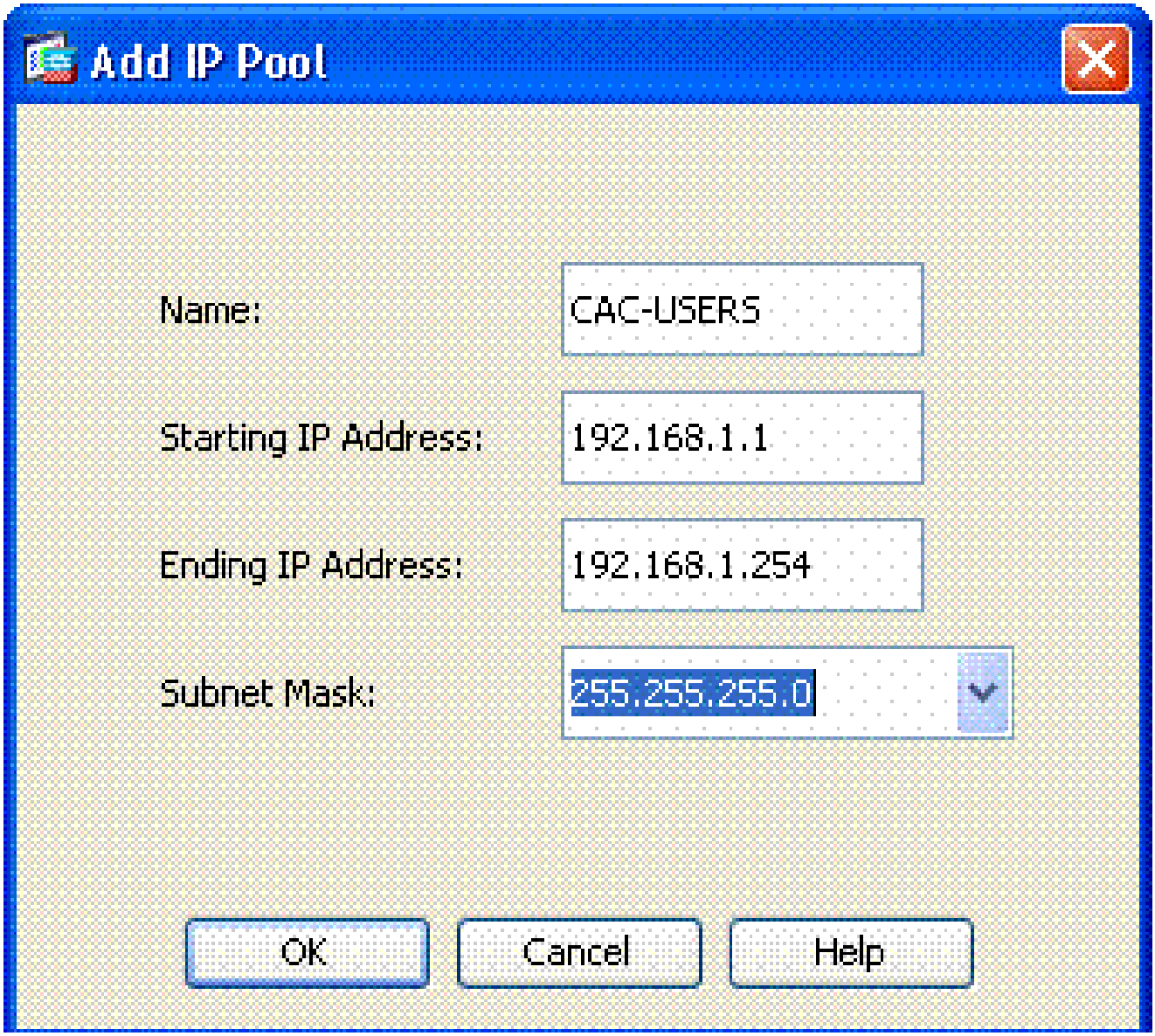
Remarque : par exemple, https://asa.test.com. Ce guide utilise la deuxième méthode. Une fois que le client AC est installé sur l'ordinateur client de manière permanente, vous lancez simplement le client AC à partir de l'application.

Créer un pool d'adresses IP

Cette option est facultative si vous utilisez une autre méthode, telle que DHCP.

1. Choisissez Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools.
2. Cliquez sur Add.
3. Dans la fenêtre Add IP Pool, saisissez le nom du pool d'adresses IP, l'adresse IP de début et de fin, puis choisissez un masque de sous-réseau. Voir la figure 13.

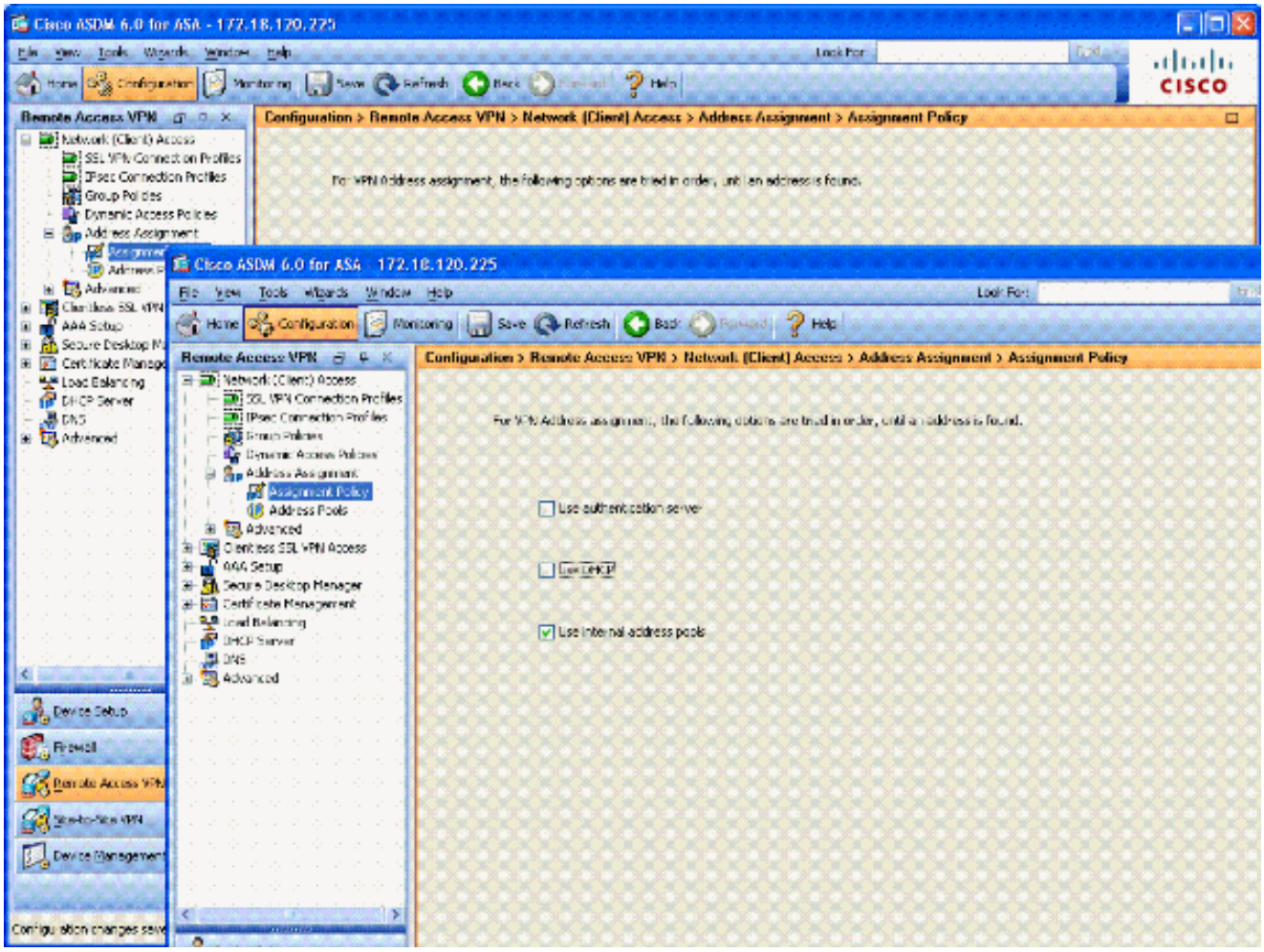
   Figure 13 : Ajout d'un pool IP



4. Cliquez sur Ok.
5. Choisissez Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy.

6. Sélectionnez la méthode d'attribution d'adresse IP appropriée. Ce guide utilise les pools d'adresses internes. Voir la figure 14.

   Figure 14 : Méthode d'attribution des adresses IP



7. Cliquez sur Apply.

Créer un groupe de tunnels et une stratégie de groupe

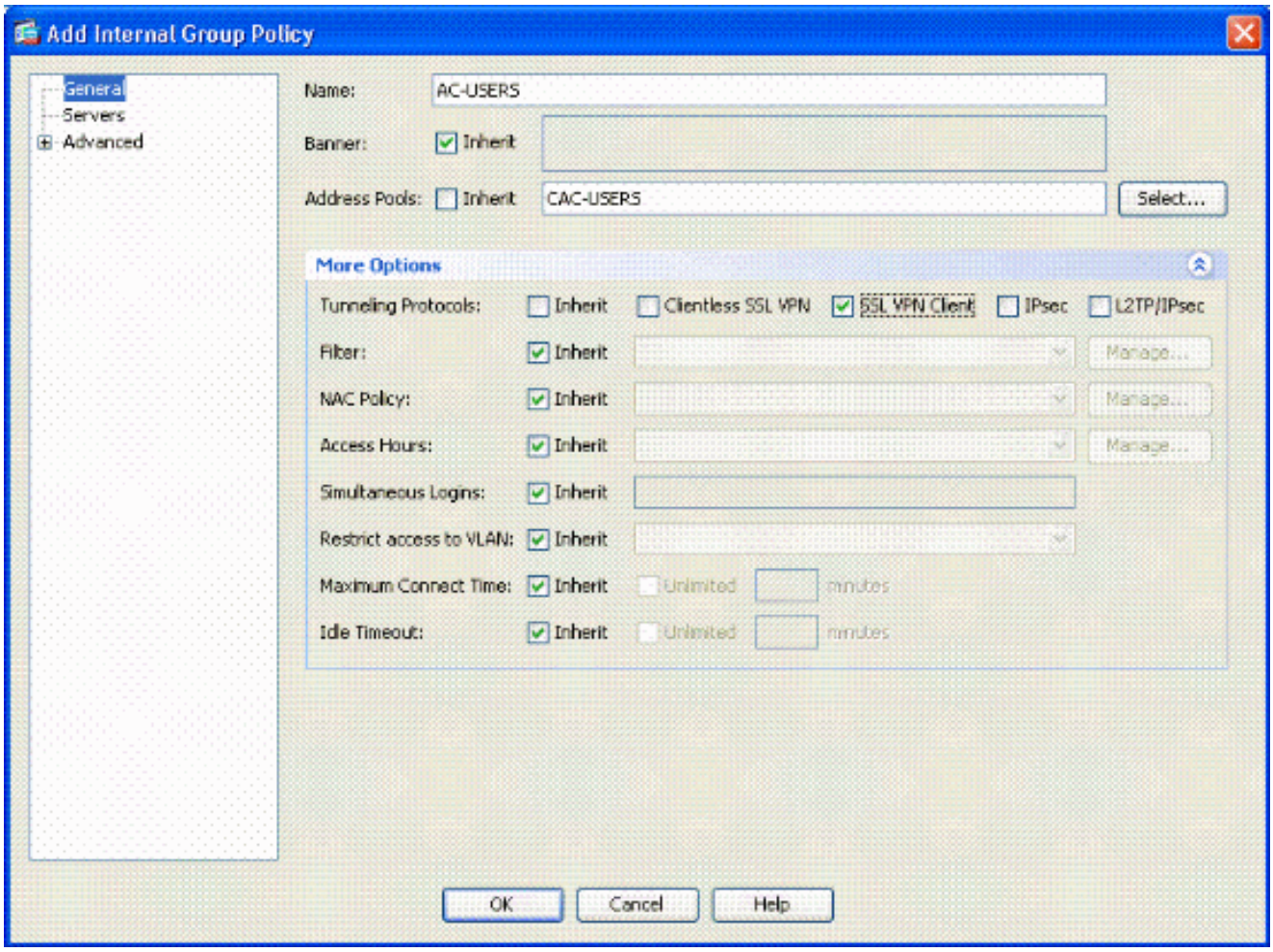
Stratégie de groupe

> Remarque : si vous ne souhaitez pas créer de stratégie, vous pouvez utiliser la stratégie de groupe intégrée par défaut.

---

1. Choisissez Remote Access VPN -> Network (Client) Access -> Group Policies.
2. Cliquez sur Add et choisissez Internal Group Policy.
3. Dans la fenêtre Ajouter une stratégie de groupe interne, entrez le nom de la stratégie de groupe dans la zone de texte Nom. Voir la figure 15.

   Figure 15 : Ajout d'une stratégie de groupe interne



a. Dans l'onglet Général, choisissez le client VPN SSL dans l'option Protocoles de tunnellisation, sauf si vous utilisez d'autres protocoles tels que SSL sans client.

b. Dans la section Servers, décochez la case inherit et entrez l'adresse IP des serveurs DNS et WINS. Saisissez l'étendue DHCP, le cas échéant.

c. Dans la section Serveurs, désélectionnez la case à cocher hériter dans le domaine par défaut et entrez le nom de domaine approprié.

d. Dans l'onglet Général, désactivez la case à cocher hériter dans la section Pool d'adresses et ajoutez le pool d'adresses créé à l'étape précédente. Si vous utilisez une autre méthode d'attribution d'adresse IP, laissez cette option hériter et apportez les modifications appropriées.

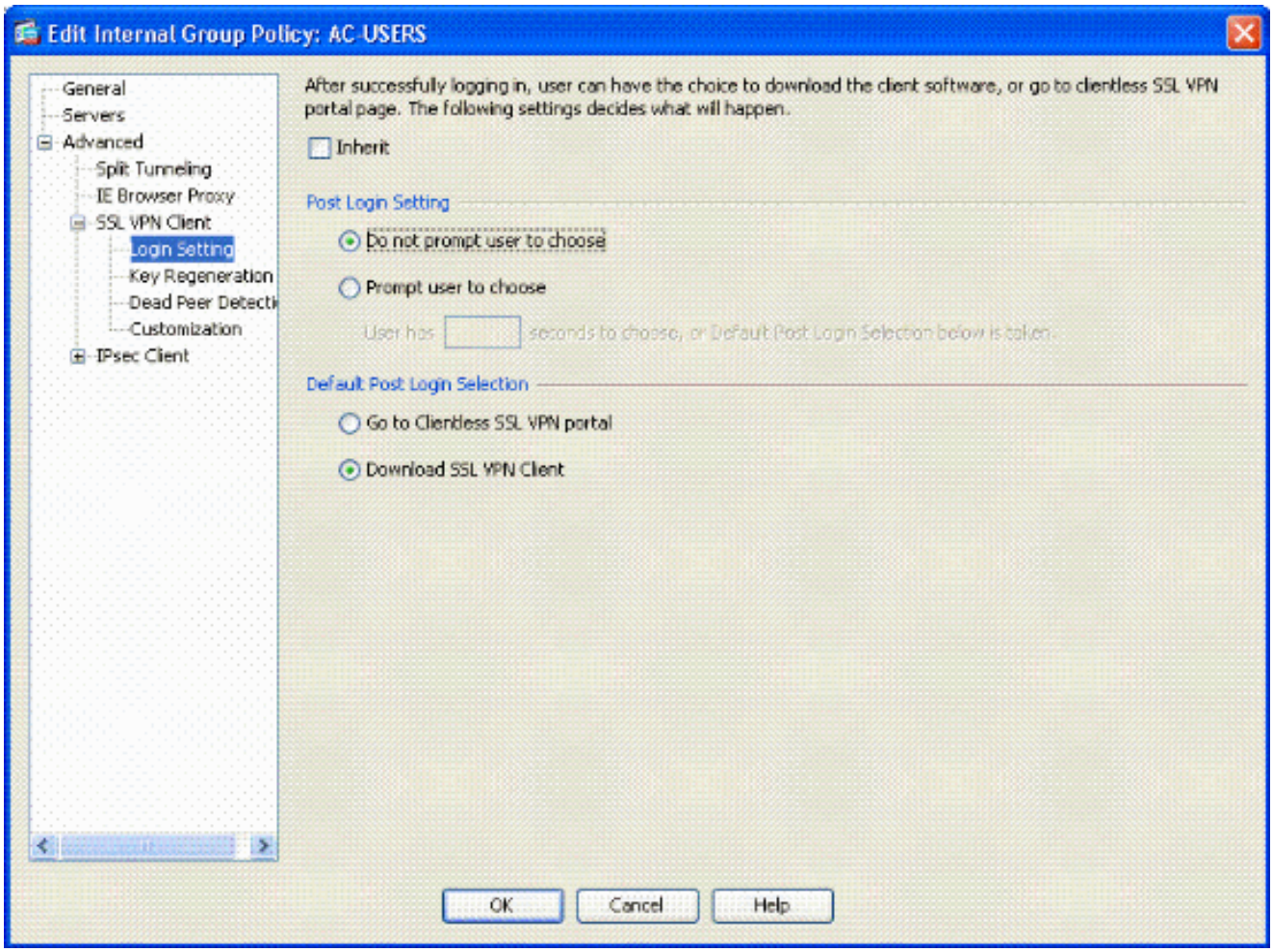
e. Tous les autres onglets de configuration conservent leurs paramètres par défaut.

Remarque : il existe deux méthodes pour acheminer le client AC aux utilisateurs finaux. Une méthode consiste à accéder à Cisco.com et à télécharger le client AC. La deuxième méthode consiste à demander à l'ASA de télécharger le client sur l'utilisateur lorsque celui-ci tente de se connecter. Cet exemple illustre cette dernière méthode.

---

4. Choisissez ensuite Advanced > SSL VPN Client > Login Settings. Voir la figure 16.

Figure 16 : Ajout d'une stratégie de groupe interne



a. Décochez la case Hériter.

b. Sélectionnez le paramètre Post Login approprié à votre environnement.

c. Sélectionnez la sélection de post-connexion par défaut adaptée à votre environnement.

d. Cliquez sur OK.

Interface de groupe de tunnels et paramètres d'image

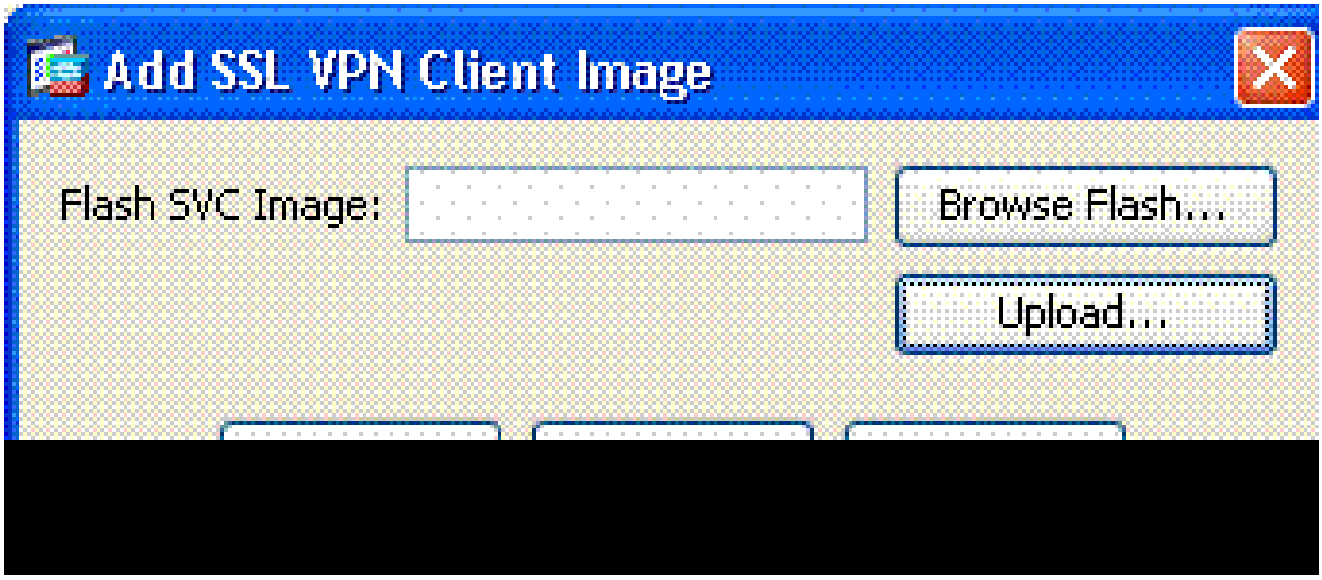
Remarque : si vous ne souhaitez pas créer de groupe, vous pouvez utiliser le groupe intégré par défaut.

---

1. Choisissez Remote Access VPN > Network (Client) Access > SSL VPN Connection Profile.
2. Sélectionnez Activer le client Cisco AnyConnect.....
3. Une boîte de dialogue apparaît avec la question `Voulez-vous désigner une image SVC ?`
4. Sélectionnez Oui.

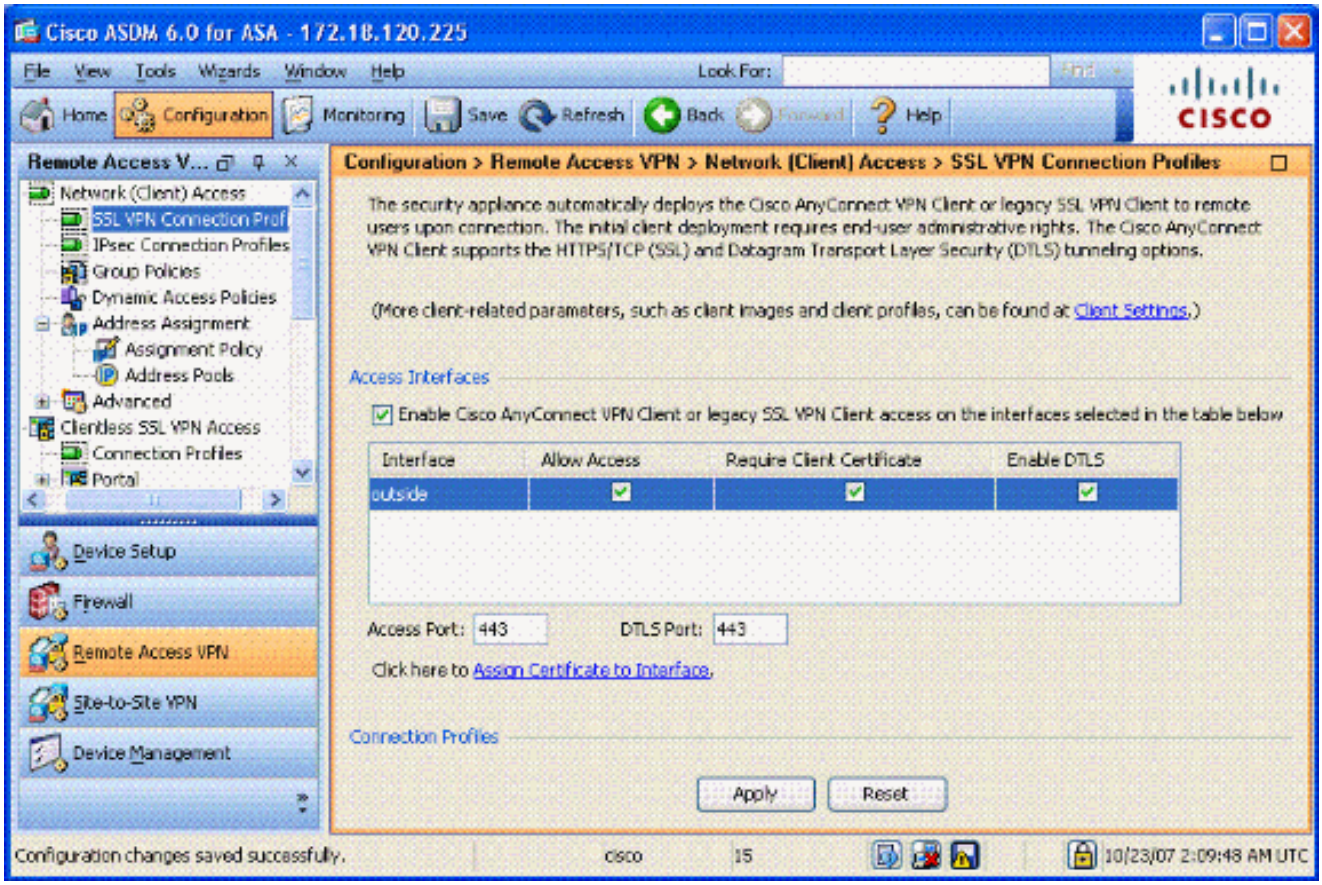
5. S'il existe déjà une image, choisissez l'image à utiliser avec Browse Flash. Si l'image n'est pas disponible, choisissez Upload et recherchez le fichier sur l'ordinateur local. Voir la figure 17. Les fichiers peuvent être téléchargés à partir de Cisco.com ; il y a un fichier Windows, MAC et Linux.

   Figure 17 : Ajout d'une image de client VPN SSL



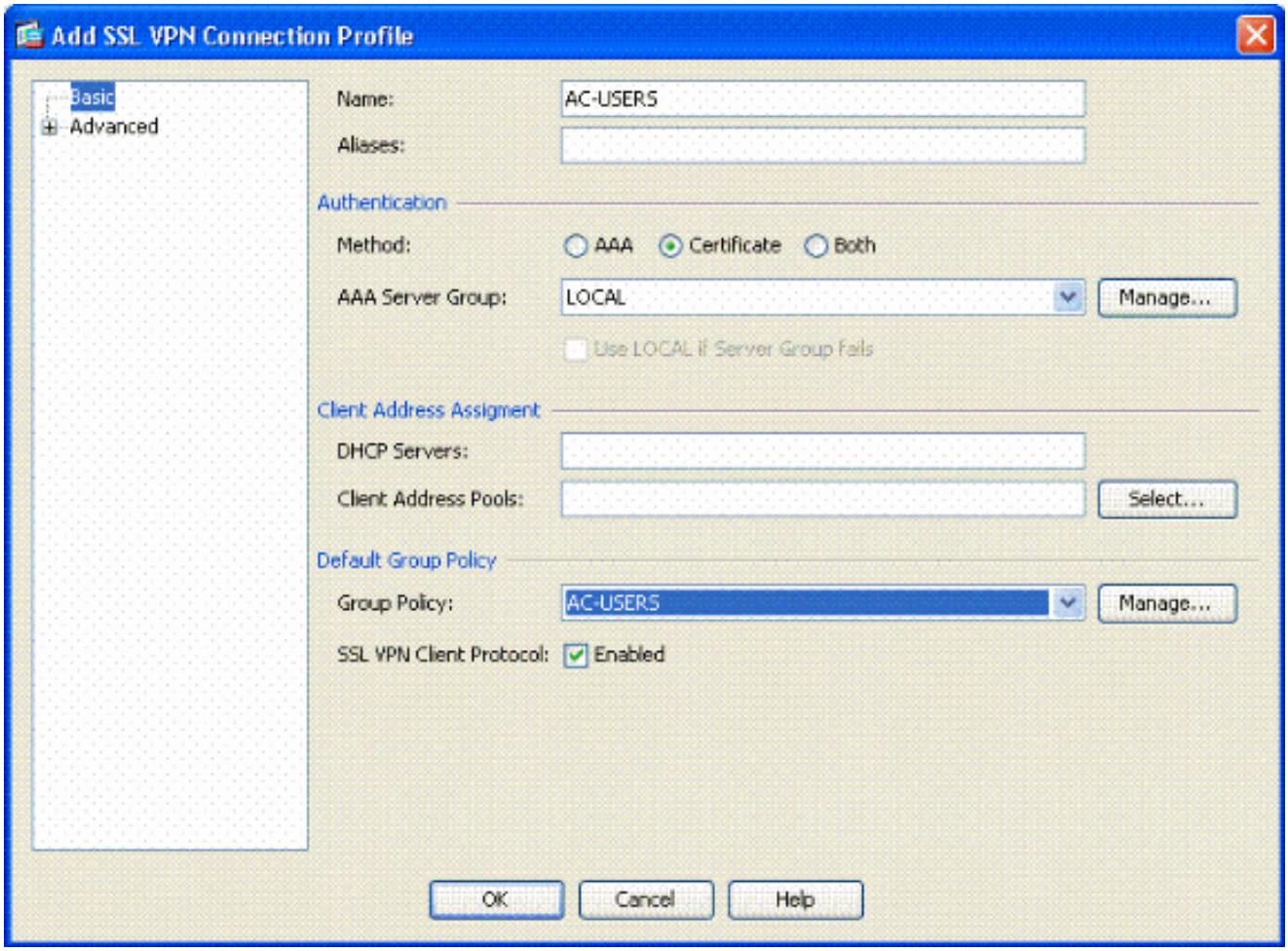
6. Activez ensuite Allow Access, Require Client Cert et éventuellement Enable DTLS. Voir la figure 18.

   Figure 18 : Activation de l'accès



7. Cliquez sur Apply.
8. Créez ensuite un profil de connexion/groupe de tunnels. Choisissez Remote Access VPN > Network (Client) Access > SSL VPN Connection Profile.
9. Dans la section Profils de connexion, cliquez sur Ajouter.

   Figure 19 : Ajout d'un profil de connexion



   a. Nommez le groupe.

   b. Choisissez Certificate dans la méthode d'authentification.

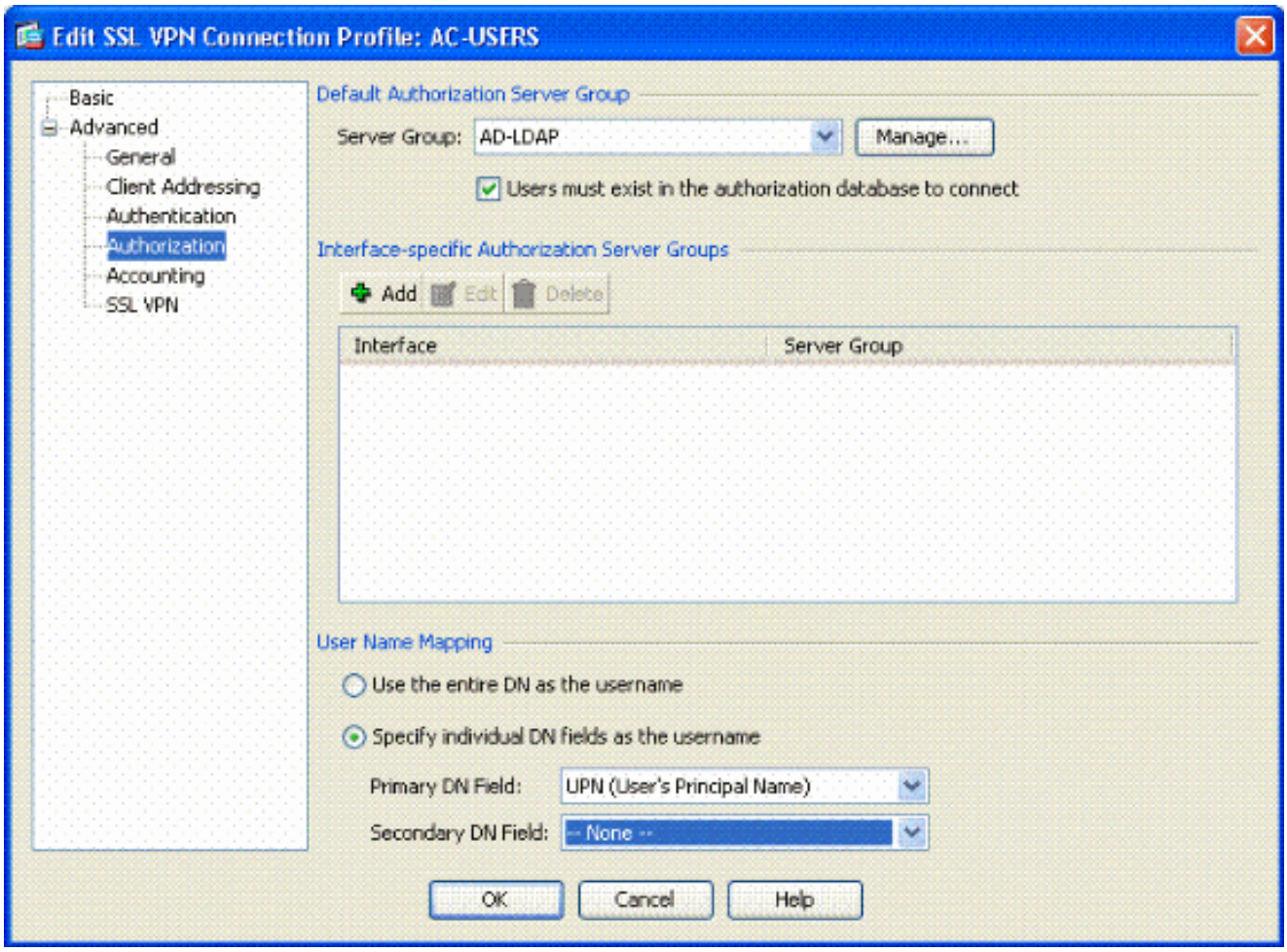
   c. Sélectionnez la stratégie de groupe créée précédemment.

   d. Assurez-vous que le client VPN SSL est activé.

   e. Conservez les autres options par défaut.

10. Ensuite, sélectionnezAvancé > Autorisation. Voir Figure 20

    Figure 20 : Autorisation



a. Sélectionnez le groupe AD-LDAP précédemment créé.

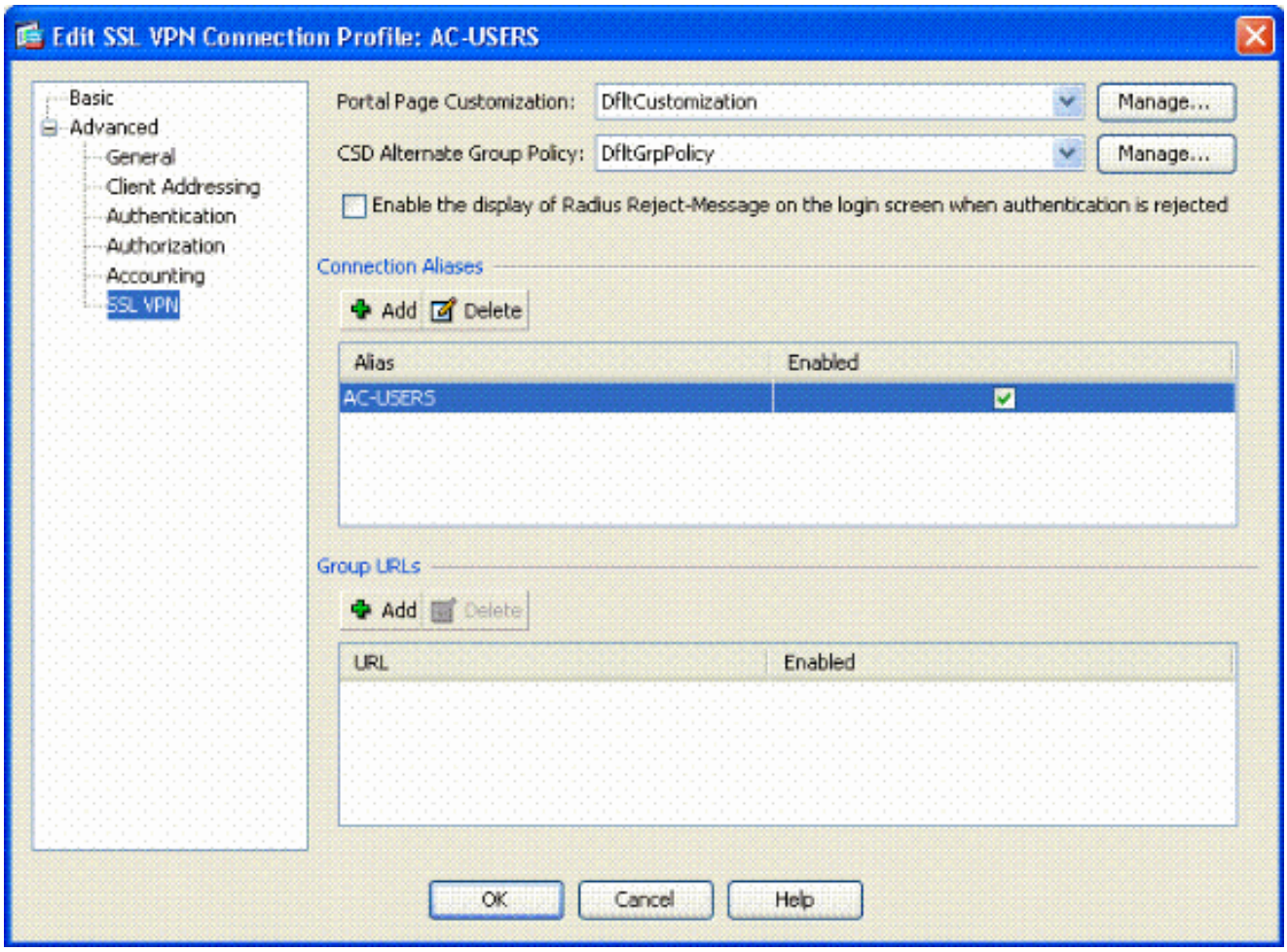
b. Vérifiez que les utilisateurs doivent exister... pour se connecter.

c. Dans les champs de mappage, choisissez UPN pour le primaire et none pour le secondaire.

11. Sélectionnez la section VPN SSL du menu.

12. Dans la section Alias de connexion, procédez comme suit :

Figure 21 : Alias de connexion



a. Sélectionnez Ajouter.

b. Saisissez l'alias de groupe que vous souhaitez utiliser.

c. Assurez-vous que Activé est coché. Voir la figure 21.

13. Click OK.

Remarque : cliquez sur Save afin d'enregistrer la configuration dans la mémoire flash.

Règles de correspondance de certificat (si OCSP sera utilisé)

1. Choisissez Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps. Voir la figure 22.

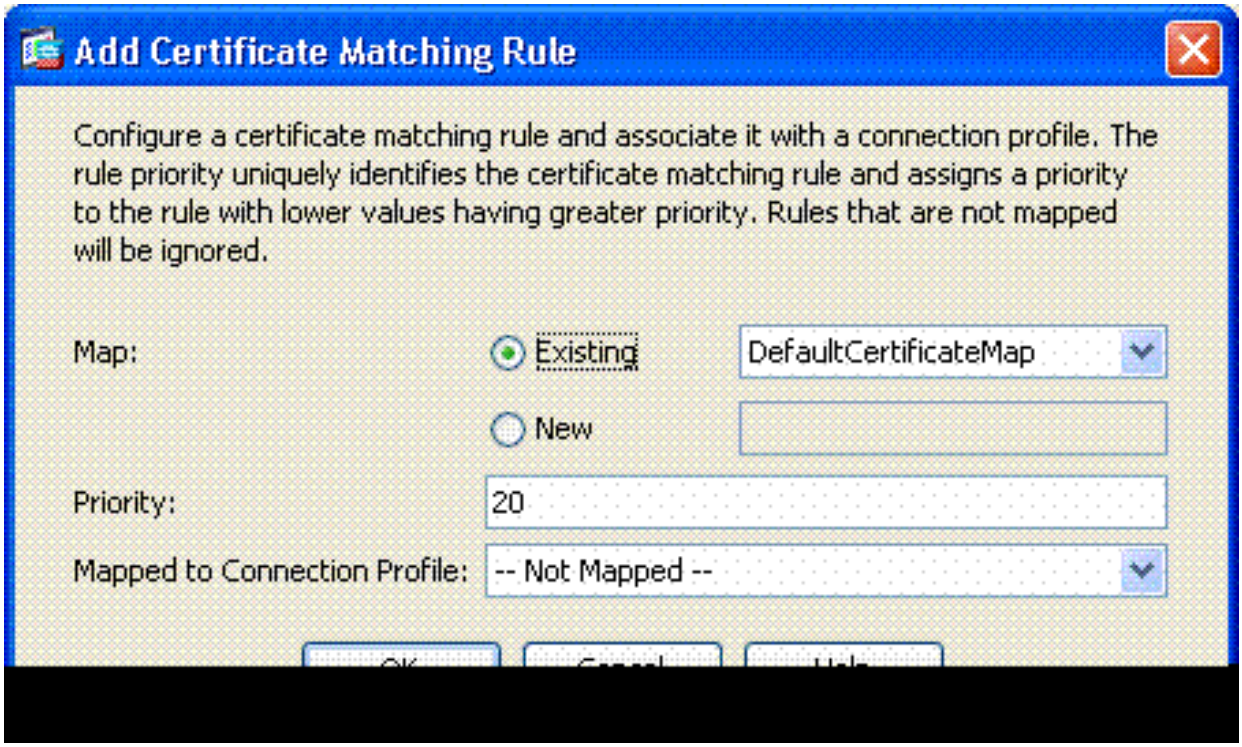
   a. Choisissez Add dans la section Certificate to Connection Profile Maps.

   b. Vous pouvez conserver le mappage existant comme DefaultCertificateMap dans la section de mappage ou en créer un nouveau si vous utilisez déjà des mappages de certificat pour IPsec.

   c. Conservez la priorité de la règle.

d. Sous groupe mappé, laissez comme — Non mappé —. Voir la figure 22.

Figure 22 : Ajout d'une règle de correspondance de certificat

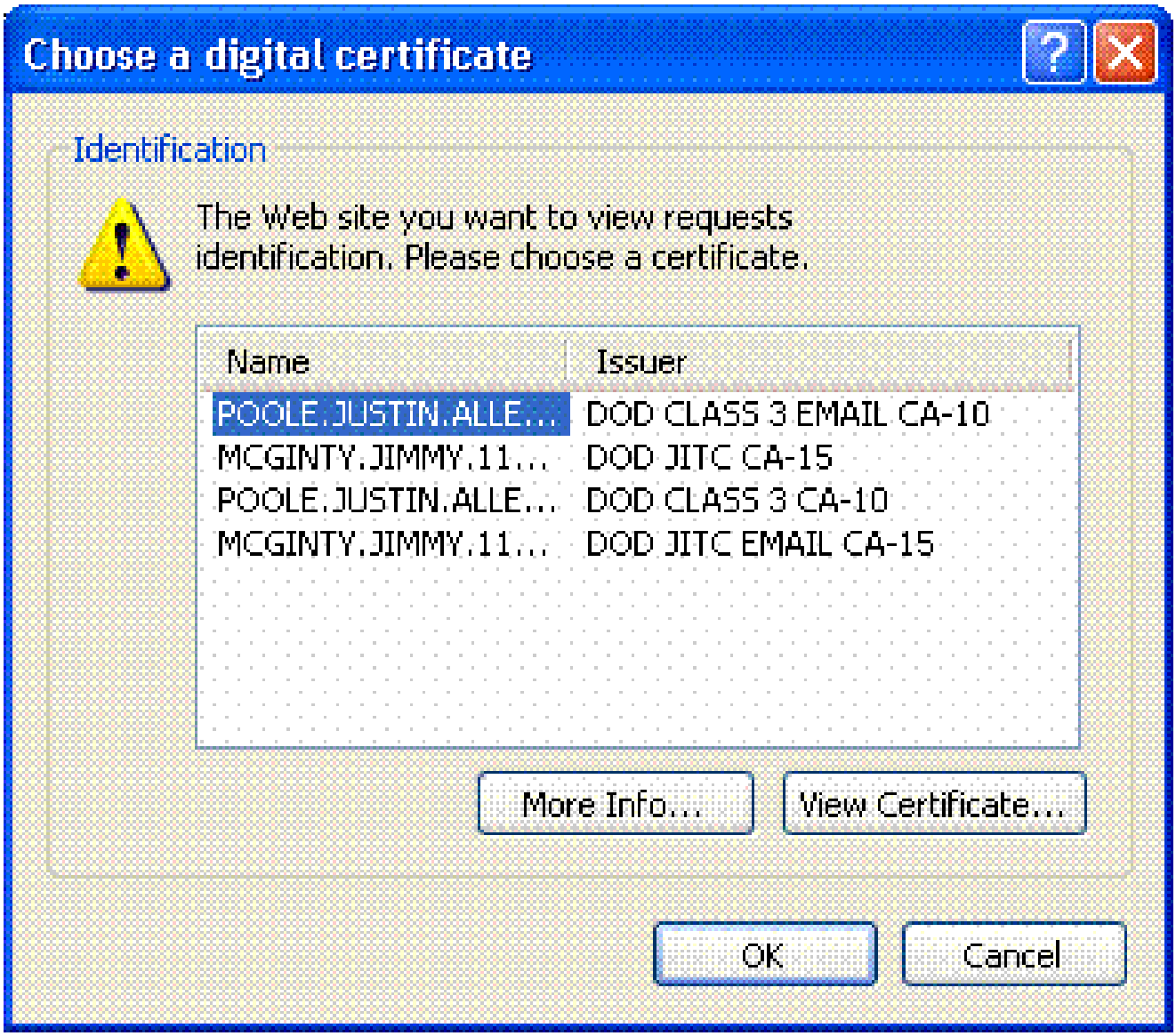


e. Click OK.

2. Cliquez sur Add dans le tableau du bas.

3. Dans la fenêtre Ajouter un critère de règle de correspondance de certificat, procédez comme suit :

Figure 23 : Critère de règle de correspondance de certificat



a. Conservez la colonne Champ sur Objet.

b. Conservez la colonne Component sur Whole Field.

c. Remplacez la colonne Opérateur par N'est pas égal.

d. Dans la colonne Valeur, entrez deux guillemets doubles « ».

e. Cliquez sur OK et sur Apply. Voir l'exemple de la figure 23.

Configurer OCSP

La configuration d'un OCSP peut varier et dépend du fournisseur du répondeur OCSP. Lisez le manuel du vendeur pour plus d'informations.

Configurer le certificat du répondeur OCSP

1. Obtenez un certificat auto-généré auprès du répondeur OCSP.

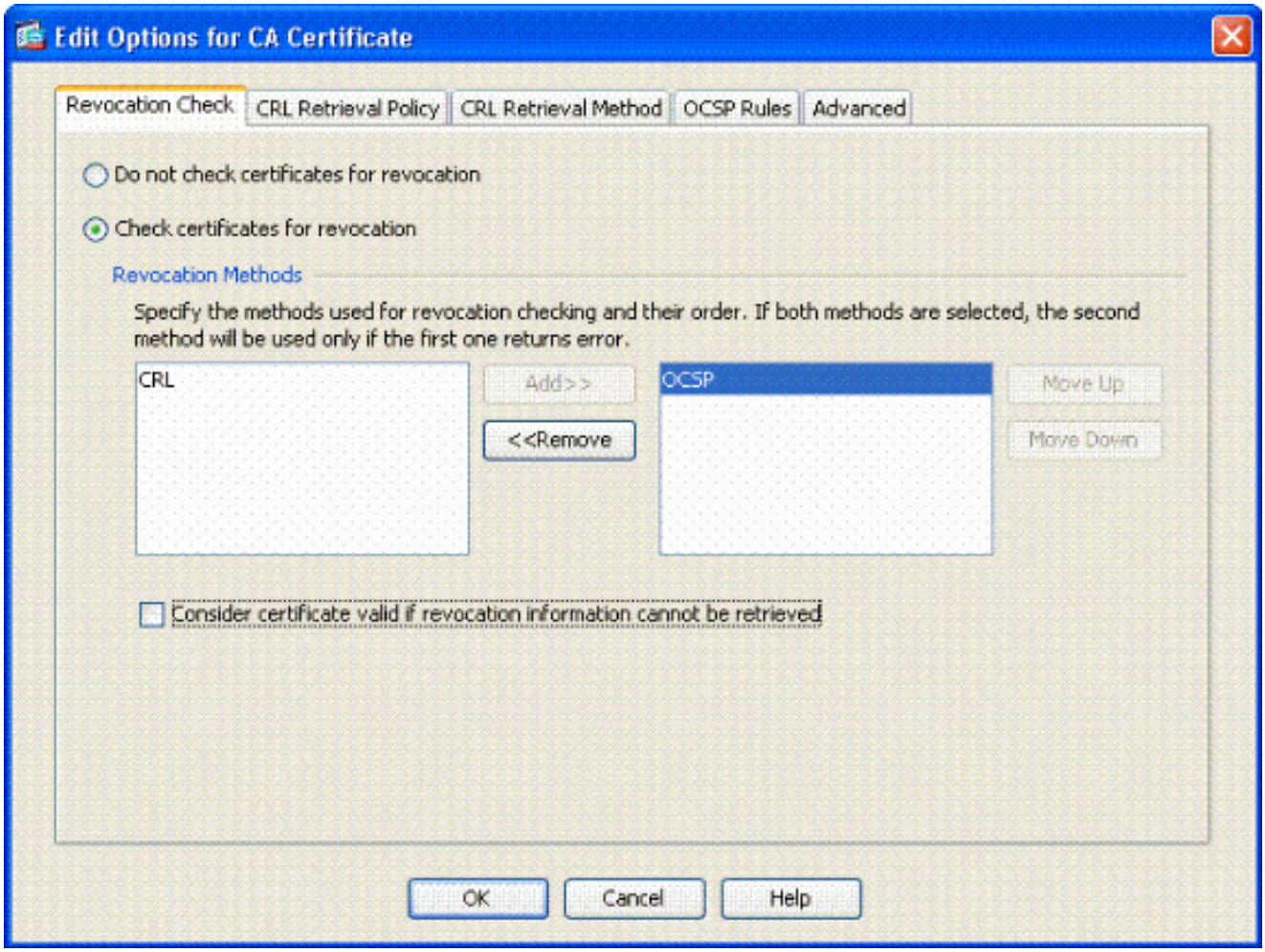
2. Suivez les procédures mentionnées précédemment et installez un certificat pour le serveur OSCP.

Remarque : assurez-vous que l'option Ne pas vérifier les certificats pour la révocation est sélectionnée pour le point de confiance de certificat OCSP.

Configurer l'AC pour utiliser OCSP

1. Choisissez Remote Access VPN > Certificate Management > CA Certificates.
2. Mettez en surbrillance un OCSP afin de choisir une CA à configurer pour utiliser OCSP.
3. Cliquez sur Edit.
4. Assurez-vous que Vérifier le certificat pour la révocation est coché.
5. Dans la section Méthodes de révocation, ajoutez OCSP. Voir la figure 24.

   Contrôle de révocation OCSP



6. Assurez-vous que Prendre en compte le certificat valide...ne peut pas être récupéré est décoché si vous voulez suivre une vérification OCSP stricte.

Remarque : configurez/modifiez tous les serveurs AC qui utilisent OCSP pour la révocation.

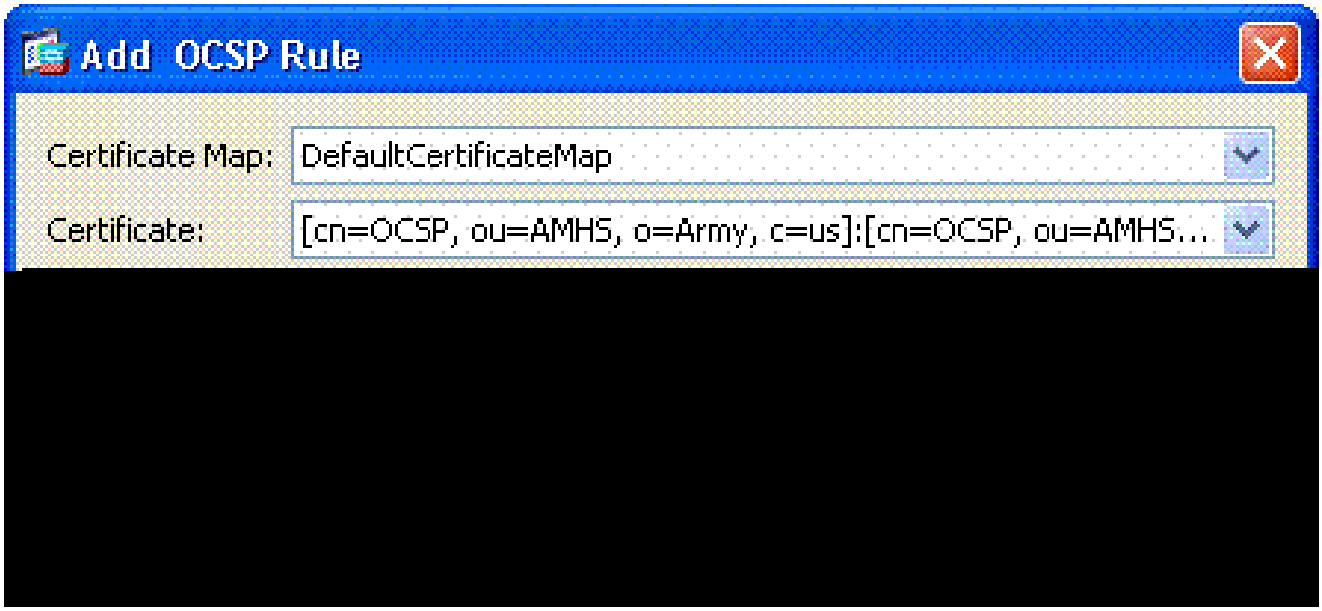
Configurer les règles OCSP

Remarque : vérifiez qu'une stratégie de correspondance de groupe de certificats est créée et que le répondeur OCSP est configuré avant d'effectuer ces étapes.

Remarque : dans certaines implémentations OCSP, un enregistrement DNS A et PTR peut être nécessaire pour l'ASA. Cette vérification est effectuée afin de vérifier que l'ASA provient d'un site .mil.

1. Choisissez Remote Access VPN > Certificate Management > CA Certificates 2.
2. Mettez en surbrillance un OCSP afin de choisir une CA à configurer pour utiliser OCSP.
3. Sélectionnez Modifier.
4. Cliquez sur l'onglet OCSP Rule.
5. Cliquez sur Add.
6. Dans la fenêtre Ajouter une règle OCSP, procédez comme suit. Voir la figure 25.

   Figure 25 : Ajout de règles OCSP



   a. Dans l'option Certificate Map, choisissez DefaultCertificateMap ou un mappage créé précédemment.

   b. Dans l'option Certificate, choisissez OCSP responder.

   c. Dans l'option d'index, entrez 10.

d. Dans l'option URL, entrez l'adresse IP ou le nom d'hôte du répondeur OCSP. Si vous utilisez le nom d'hôte, assurez-vous que le serveur DNS est configuré sur ASA.

e. Cliquez sur OK.

f. Cliquez sur Apply.

Configuration du client Cisco AnyConnect

Cette section traite de la configuration du client VPN Cisco AnyConnect.

Hypothèses - Le client VPN Cisco AnyConnect et l'application intergicielle sont déjà installés sur le PC hôte. ActivCard Gold et ActivClient ont été testés.

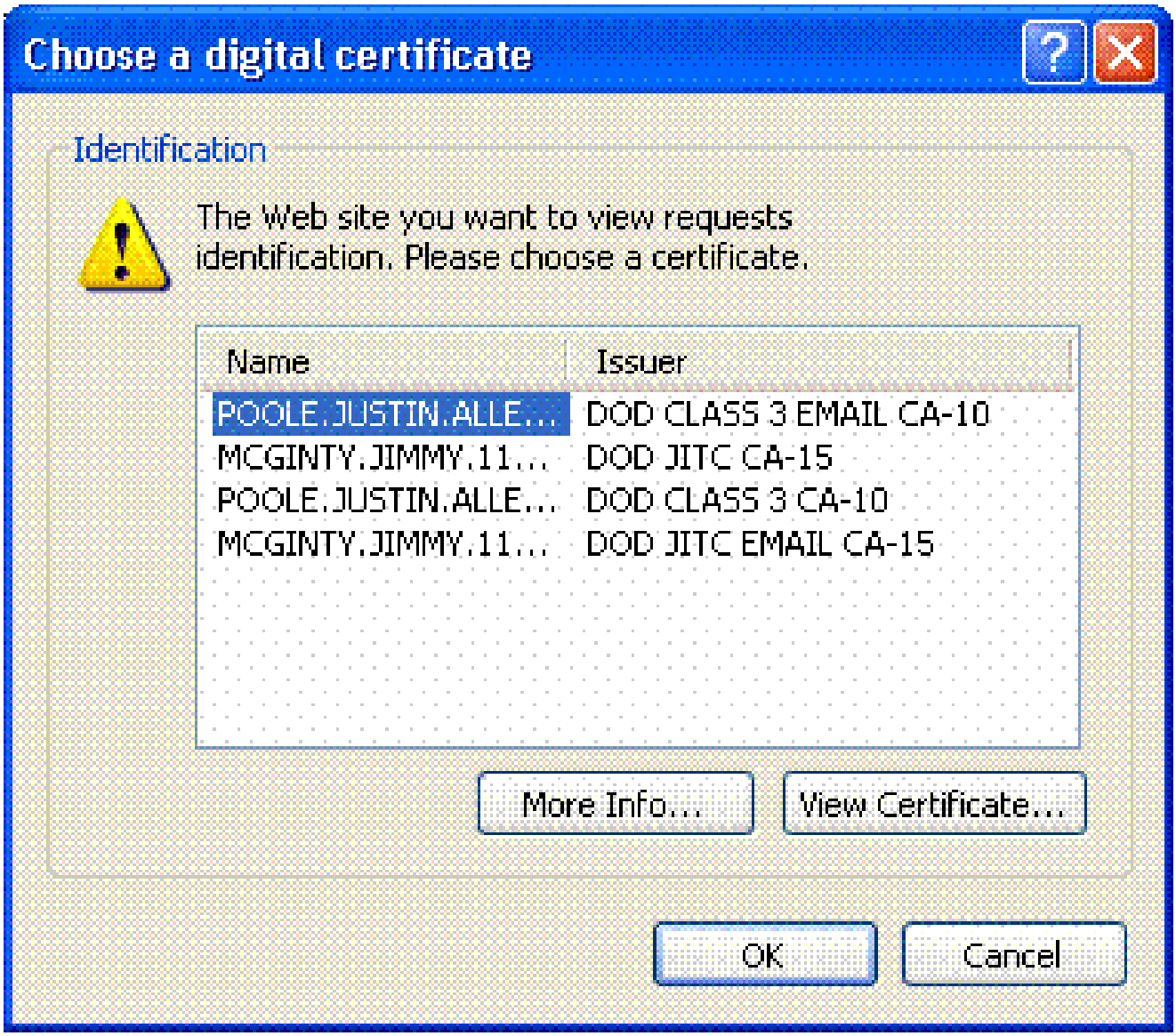
Remarque : ce guide utilise la méthode group-url pour l'installation initiale du client AC uniquement. Une fois le client AC installé, vous lancez l'application AC tout comme le client IPsec.

Remarque : la chaîne de certificats DoD doit être installée sur l'ordinateur local. Vérifiez avec le POC PKI afin d'obtenir les certificats/le fichier batch.

Téléchargement du client VPN Cisco Anyconnect - Windows

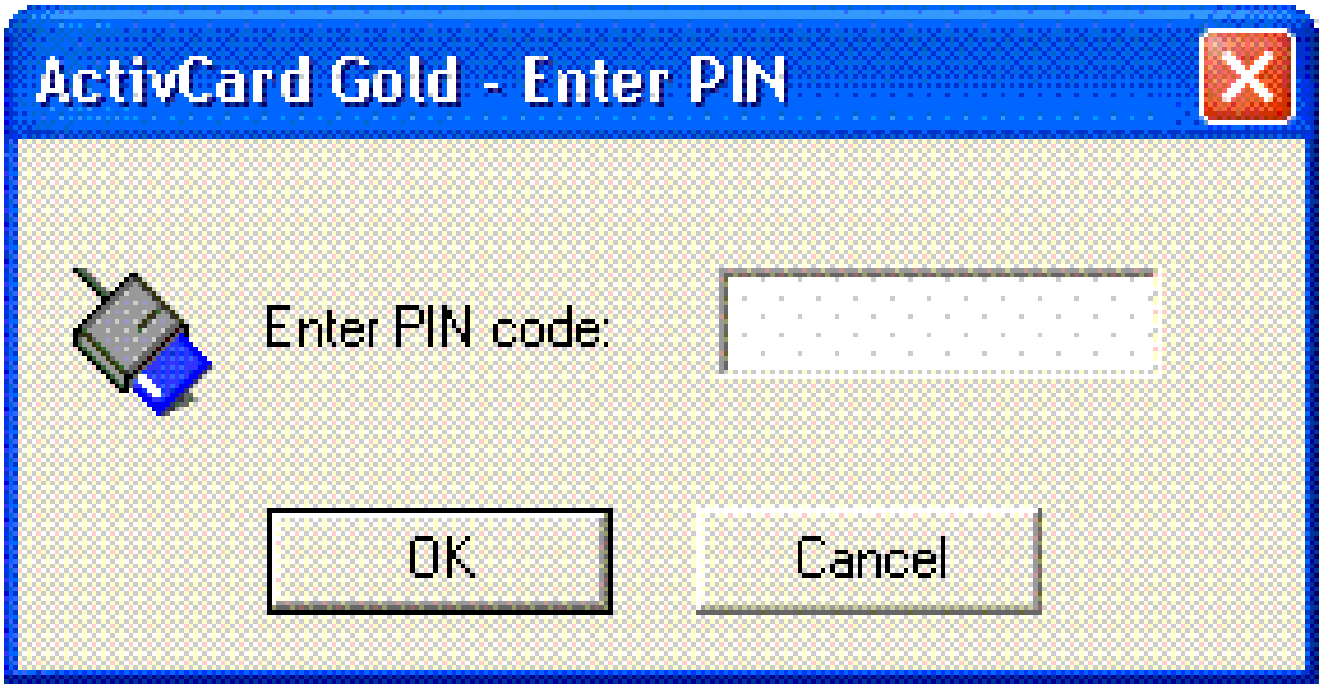
1. Lancez une session Web sur l'ASA via Internet Explorer. L'adresse doit être au format https://Outside-Interface. Par exemple, https://172.18.120.225.
2. Sélectionnez le certificat de signature à utiliser pour l'accès. Voir la figure 26.

   Figure 26 : Choix du certificat approprié



3. Saisissez votre code PIN lorsque vous y êtes invité.

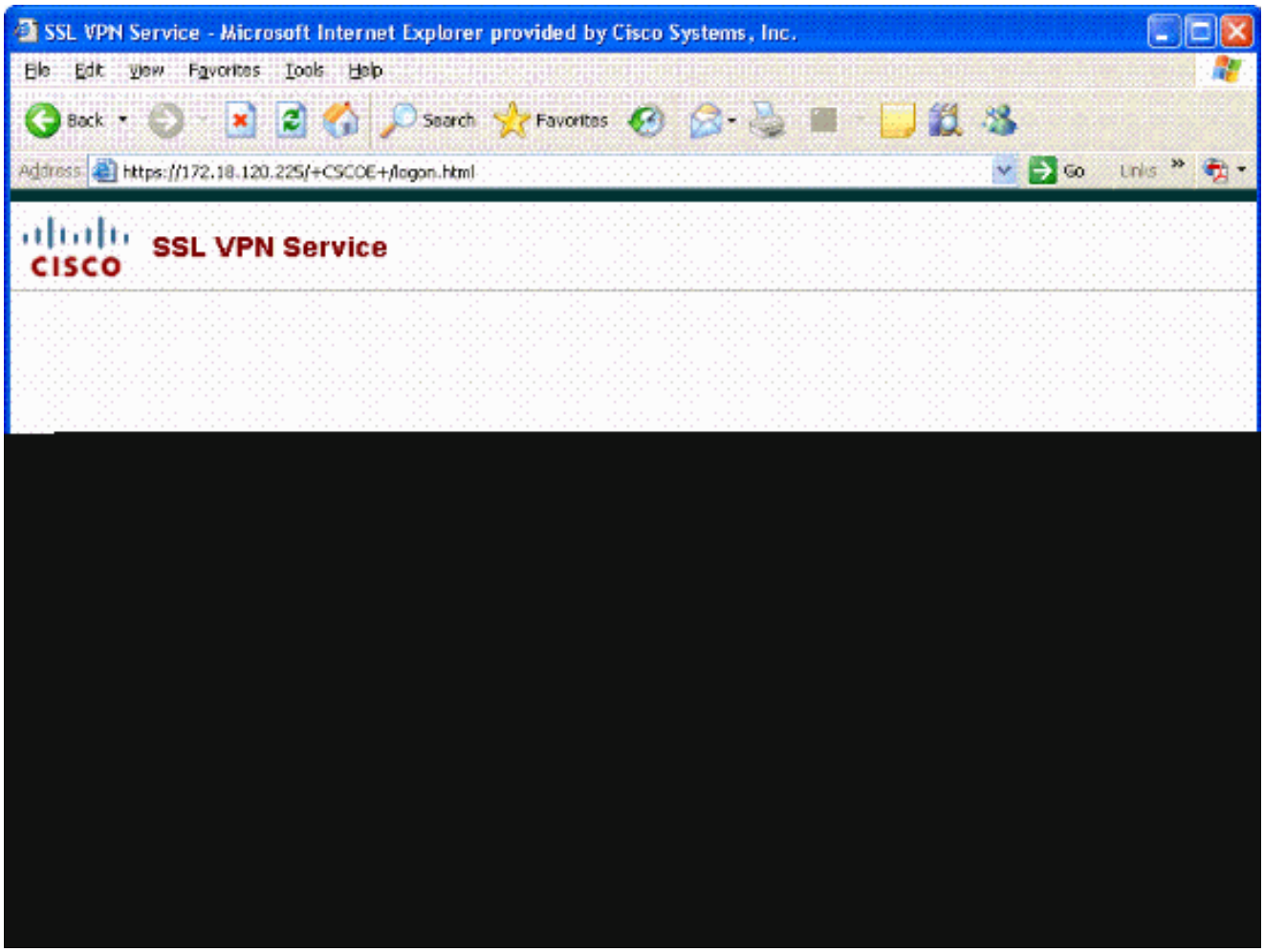
Figure 27 : Saisir le code PIN



4. Choisissez Yes afin d'accepter l'alerte de sécurité.

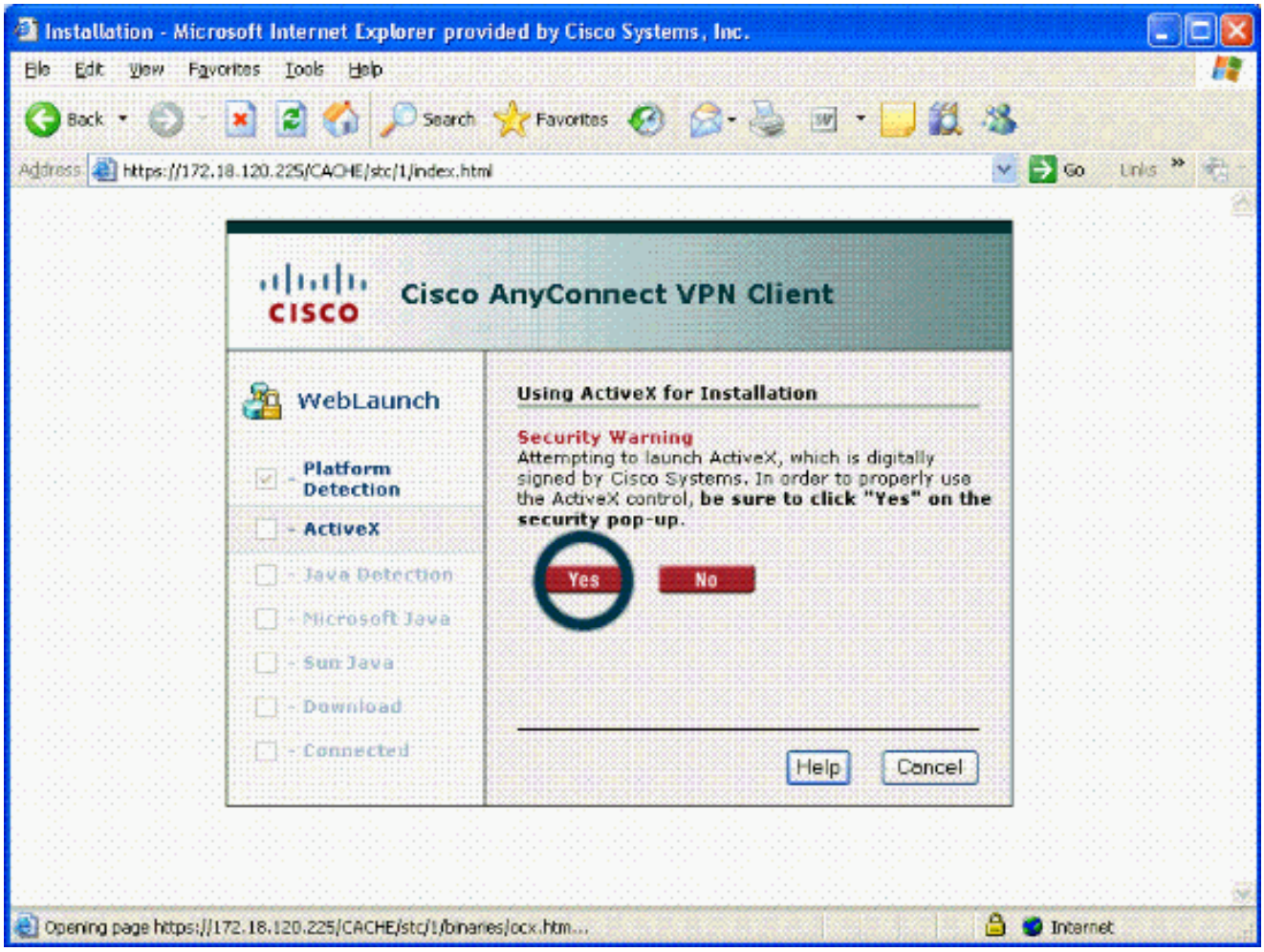
5. Une fois sur la page de connexion SSL, choisissez Login. Le certificat client est utilisé pour la connexion. Voir la figure 28.

   Figure 28 : Connexion SSL



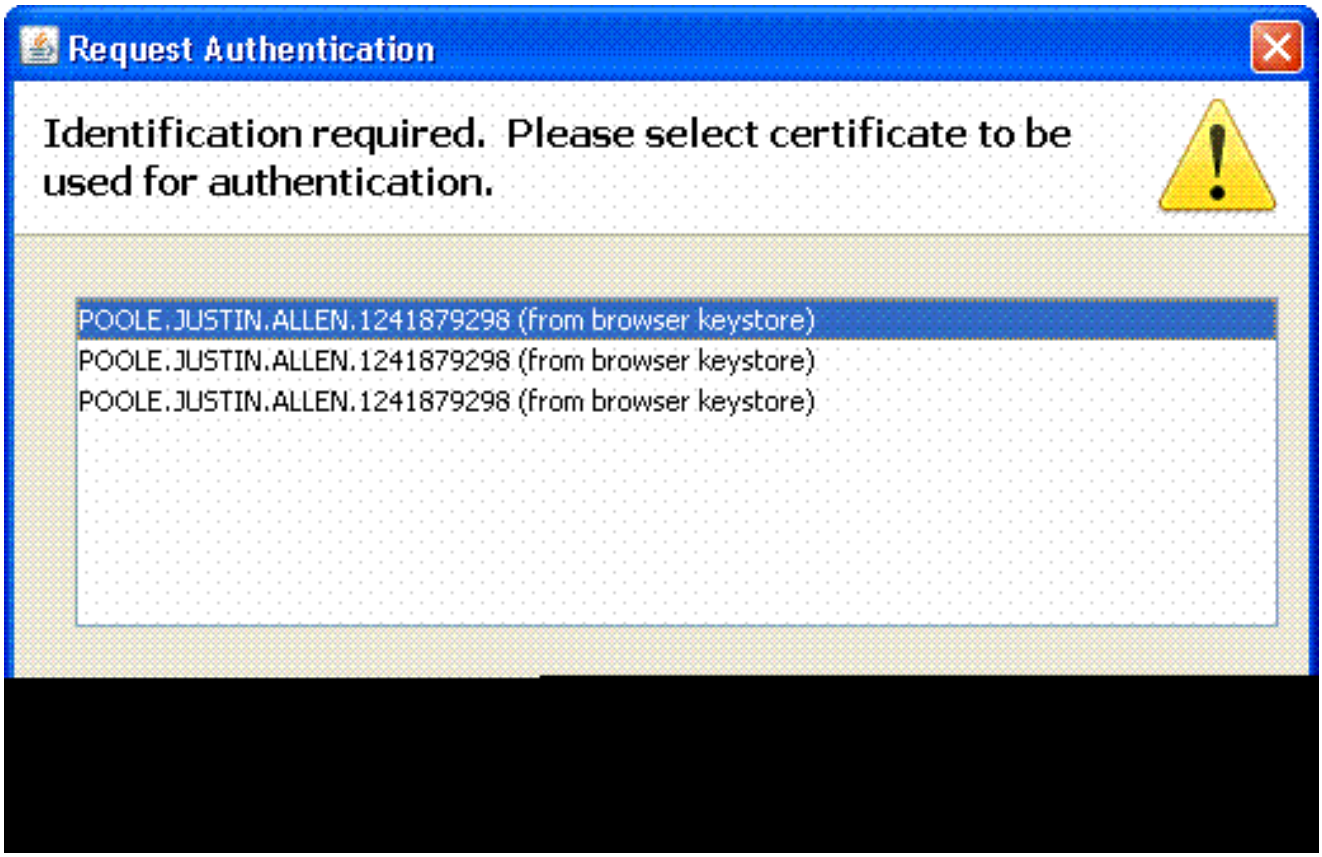
6. AnyConnect commence à télécharger le client. Voir la figure 29.

Figure 29 : Installation d'AnyConnect



7. Sélectionnez le certificat approprié à utiliser. Voir la figure 30. AnyConnect poursuit l'installation. L'administrateur ASA peut permettre au client d'installer ou d'installer de manière permanente sur chaque connexion ASA.

Figure 30 : Certificat



Démarrer le client VPN Cisco AnyConnect - Windows

À partir du PC hôte, choisissez Démarrer > Tous les programmes > Cisco > AnyConnect VPN Client.

Remarque : reportez-vous à l'annexe E pour la configuration facultative du profil client AnyConnect.

Nouvelle connexion

1. La fenêtre AC s'affiche. Voir la figure 34.

   Figure 34 : Nouvelle connexion VPN

2. Sélectionnez l'hôte approprié si AC ne tente pas automatiquement la connexion.

3. Saisissez votre code PIN lorsque vous y êtes invité. Voir la figure 35.

Figure 35 : Saisir le code PIN

Démarrer l'accès distant

Sélectionnez le groupe et l'hôte auxquels vous souhaitez vous connecter.

Puisque les certificats sont utilisés, choisissez Connect afin d'établir le VPN. Voir la figure 36.

Figure 36 : Connexion


Cisco AnyConnect VPN Client
Connection
Statistics
About
CISCO
Connect to:
172.18.120.225
Group:
AC-USERS
Username:
Password:
Connect
Please enter your username and password.

Remarque : comme la connexion utilise des certificats, il n'est pas nécessaire d'entrer un nom d'utilisateur et un mot de passe.

Remarque : reportez-vous à l'annexe E pour la configuration facultative du profil client AnyConnect.

Annexe A - Mappage LDAP et DAP

Dans ASA/PIX version 7.1(x) et ultérieures, une fonctionnalité appelée mappage LDAP a été introduite. Il s'agit d'une fonctionnalité puissante qui fournit un mappage entre un attribut Cisco et des objets/attributs LDAP, ce qui élimine la nécessité de modifier le schéma LDAP. Pour l'implémentation de l'authentification CAC, cela peut prendre en charge une application de stratégie supplémentaire sur la connexion d'accès distant. Voici des exemples de mappage LDAP. N'oubliez pas que vous devez disposer de droits d'administrateur pour apporter des modifications au serveur AD/LDAP. Dans le logiciel ASA 8.x, la fonctionnalité Dynamic Access Policy (DAP) a été introduite. DAP peut travailler en collaboration avec CAC pour examiner plusieurs groupes AD, ainsi que des politiques push, des listes de contrôle d'accès, etc.

Scénario 1 : application Active Directory à l'aide de la numérotation d'autorisation d'accès à distance - Autoriser/refuser l'accès

Cet exemple mappe l'attribut AD msNPAllowDailin à l'attribut cVPN3000-Tunneling-Protocol de Cisco.

- Valeur de l'attribut AD : TRUE = Allow ; FALSE = Deny
- Valeur d'attribut Cisco : 1 = FAUX, 4 (IPSec) ou 20 (4 IPSEC + 16 WebVPN) = VRAI,

Pour la condition ALLOW, vous mappez :

- VRAI = 20

Pour la condition d'appel entrant REFUSÉ, vous mappez :

- FAUX = 1

Remarque : assurez-vous que TRUE et FALSE sont en majuscules. Référez-vous à Configuration d'un serveur externe pour l'autorisation utilisateur du dispositif de sécurité pour plus d'informations.

Installation d'Active Directory

1. Dans le serveur Active Directory, cliquez sur Démarrer > Exécuter.
2. Dans la zone de texte Ouvrir, tapez dsa.msc, puis cliquez sur Ok. La console de gestion

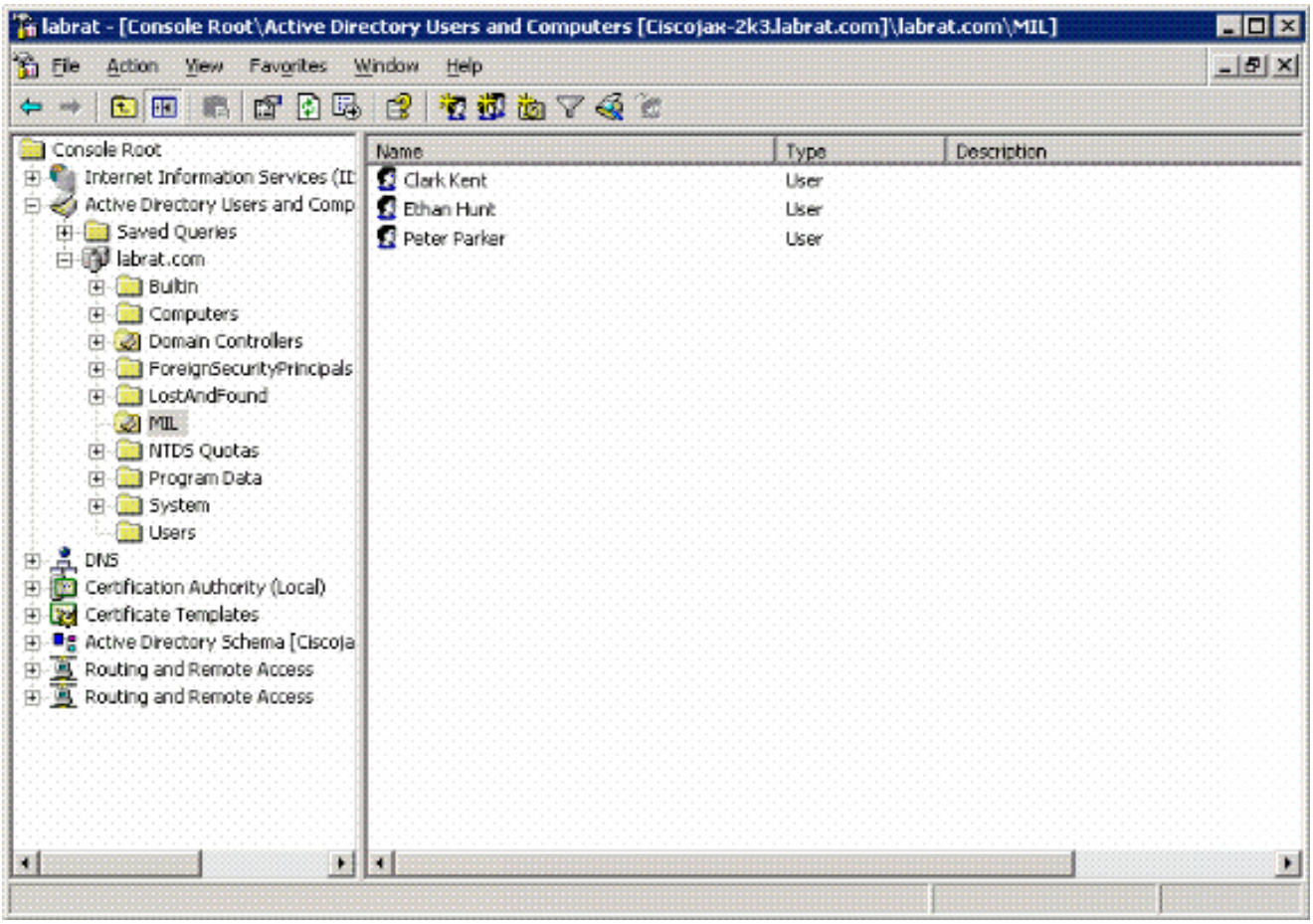
Active Directory démarre.

3. Dans la console de gestion Active Directory, cliquez sur le signe plus afin de développer le groupe Utilisateurs et ordinateurs Active Directory.

4. Cliquez sur le signe plus afin de développer le nom de domaine.

5. Si une unité d'organisation est créée pour vos utilisateurs, développez-la afin d'afficher tous les utilisateurs ; si tous les utilisateurs sont affectés dans le dossier Utilisateurs, développez ce dossier afin de les afficher. Voir Figure A1.

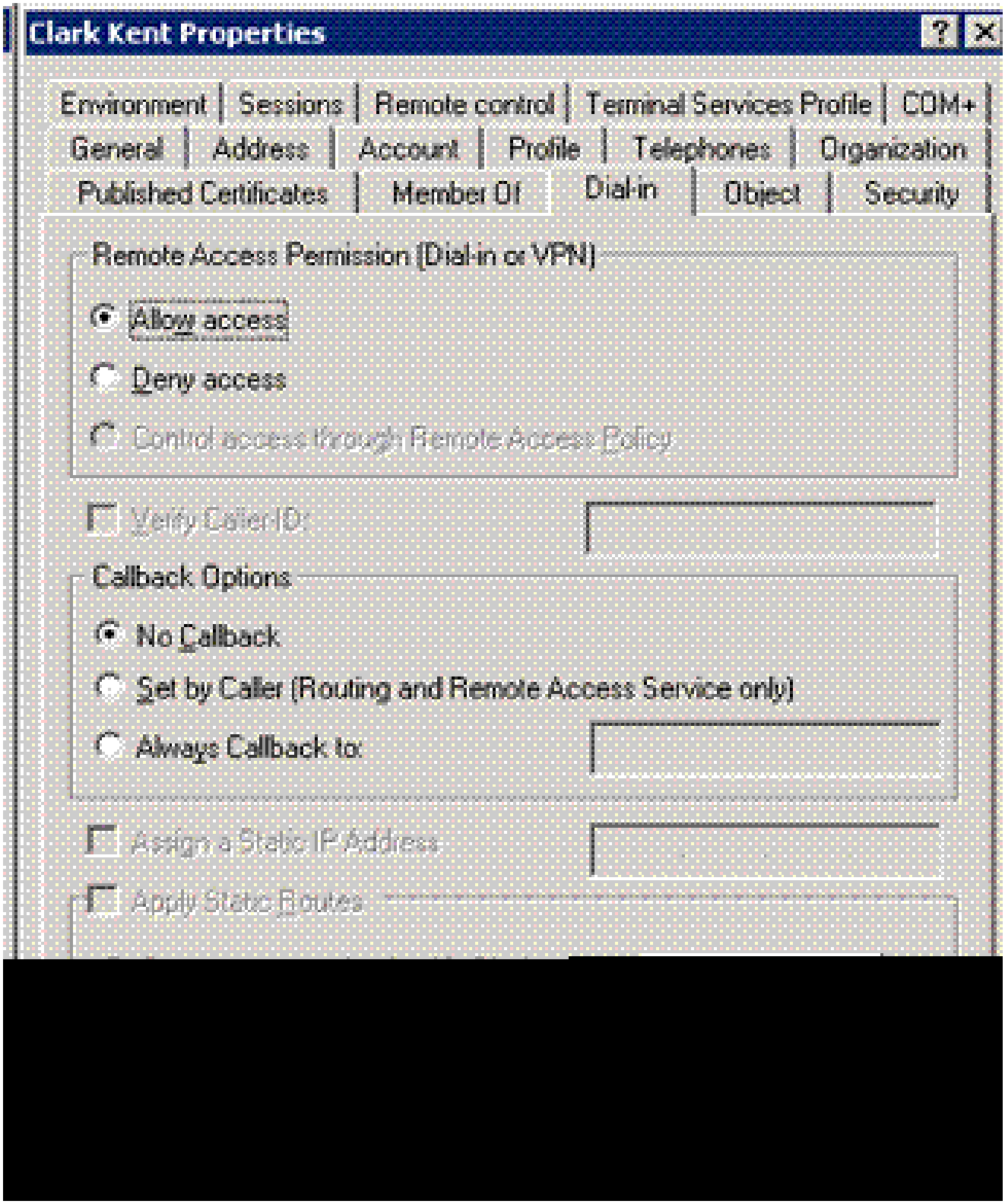
   Figure A1 : Console de gestion Active Directory



6. Double-cliquez sur l'utilisateur que vous souhaitez modifier.

   Cliquez sur l'onglet Numérotation dans la page des propriétés de l'utilisateur, puis cliquez sur Autoriser ou Refuser. Voir Figure A2.

   Figure A2 : Propriétés utilisateur



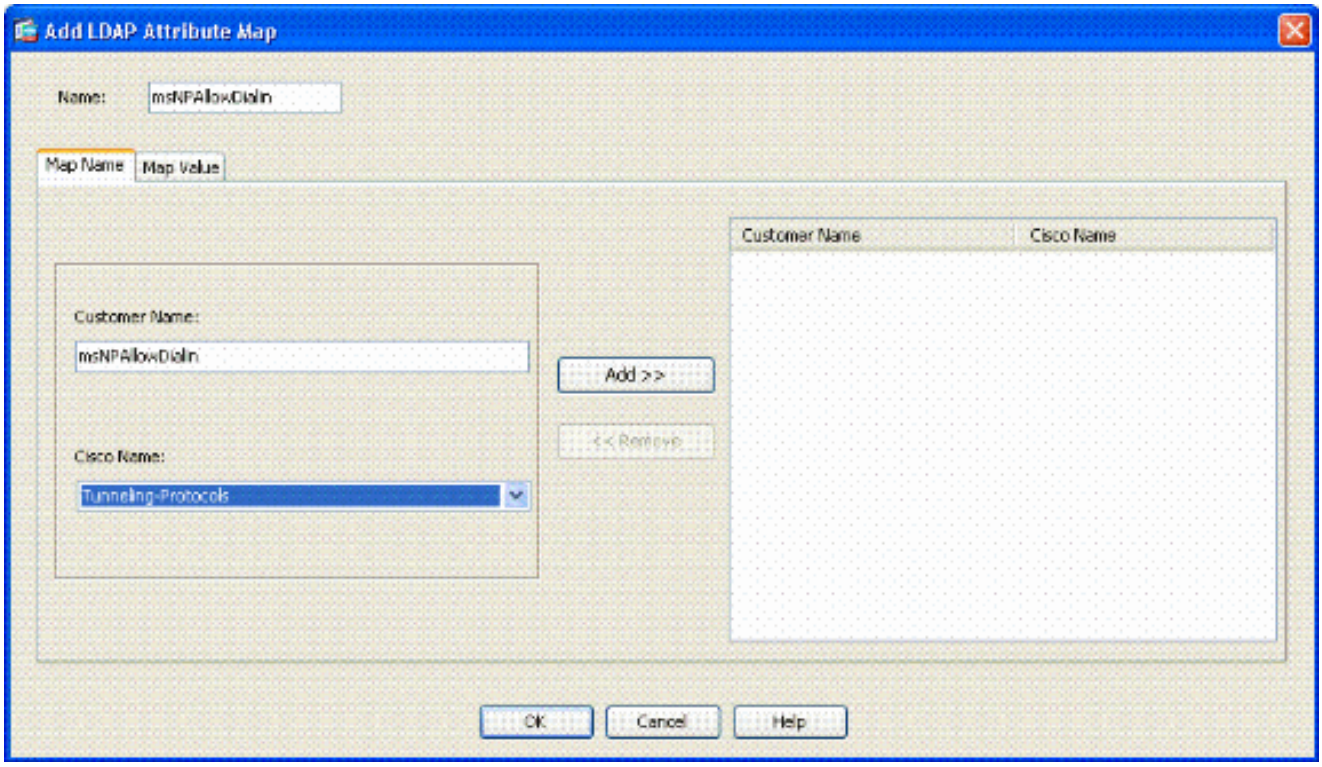
7. Cliquez ensuite sur OK.

Configuration ASA

1. Dans ASDM, choisissez Remote Access VPN > AAA Setup > LDAP Attribute Map.
2. Cliquez sur Add.
3. Dans la fenêtre Ajouter une correspondance d'attributs LDAP, procédez comme suit. Voir

Figure A3.

Figure A3 : Ajout d'une carte d'attributs LDAP



a. Entrez un nom dans la zone de texte Nom.

b. Dans l'onglet Nom de la carte, tapez msNPAllowDialin dans la zone de texte Nom du client.

c. Dans l'onglet Map Name, choisissez Tunneling-Protocols dans l'option déroulante de Cisco Name.

d. Cliquez sur Add.

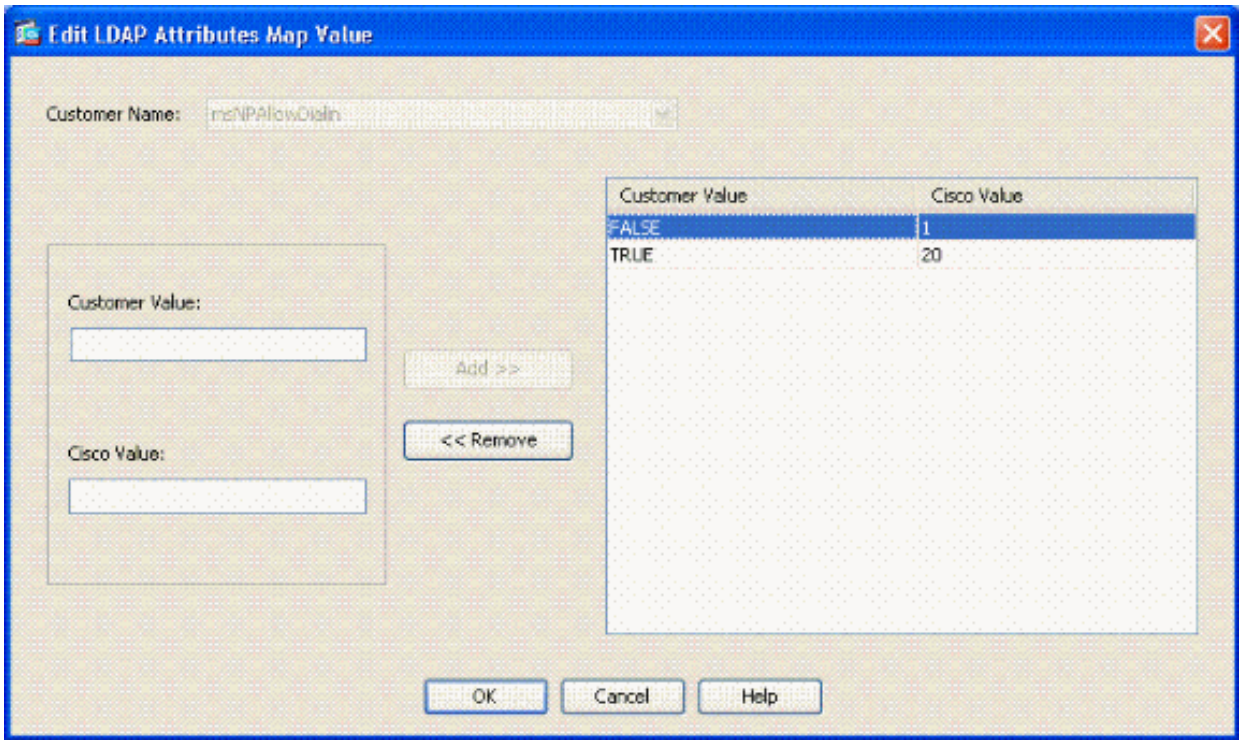
e. Cliquez sur l'onglet Valeur de mappage.

f. Cliquez sur Add.

g. Dans la fenêtre Ajouter une valeur de mappage LDAP d'attribut, tapez TRUE dans la zone de texte Nom du client et tapez 20 dans la zone de texte Valeur Cisco.

h. Cliquez sur Add.

i. Tapez FALSE dans la zone de texte Nom du client et tapez 1 dans la zone de texte Valeur Cisco. Voir Figure A4.



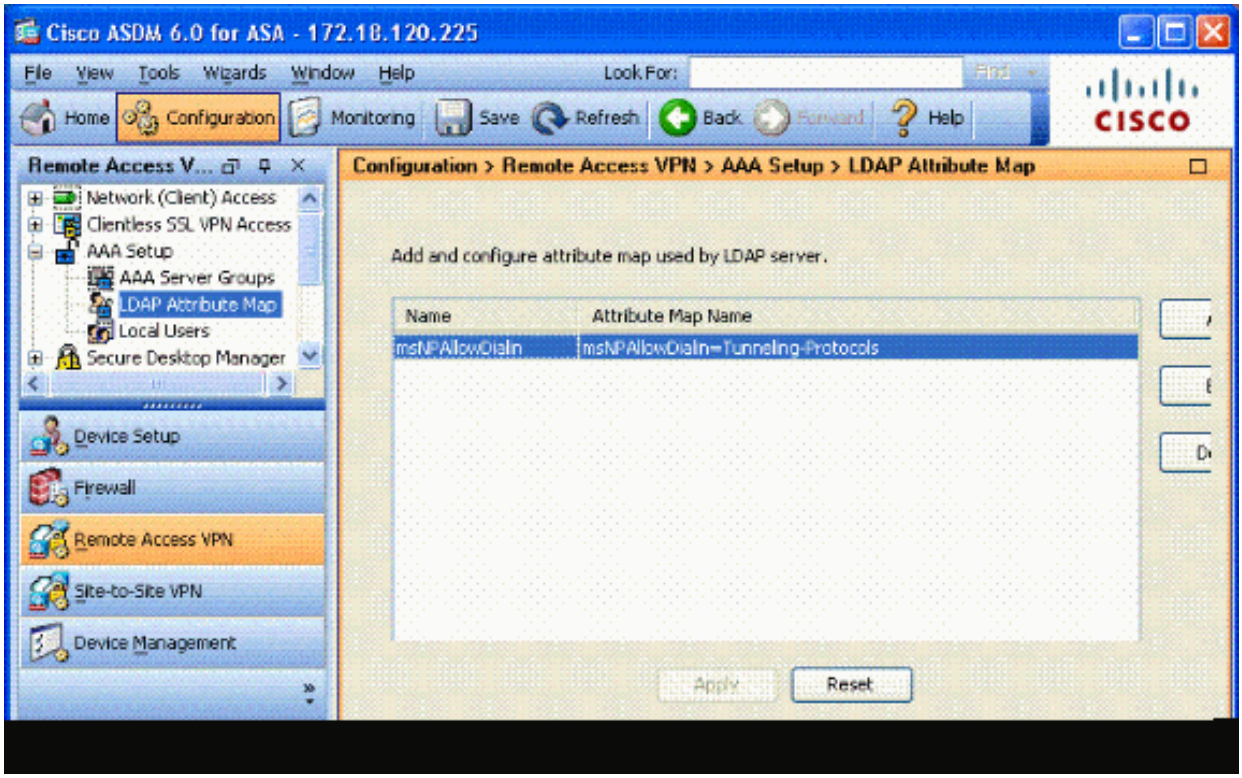
j. Cliquez sur OK.

k. Cliquez sur OK.

l. Cliquez sur Apply.

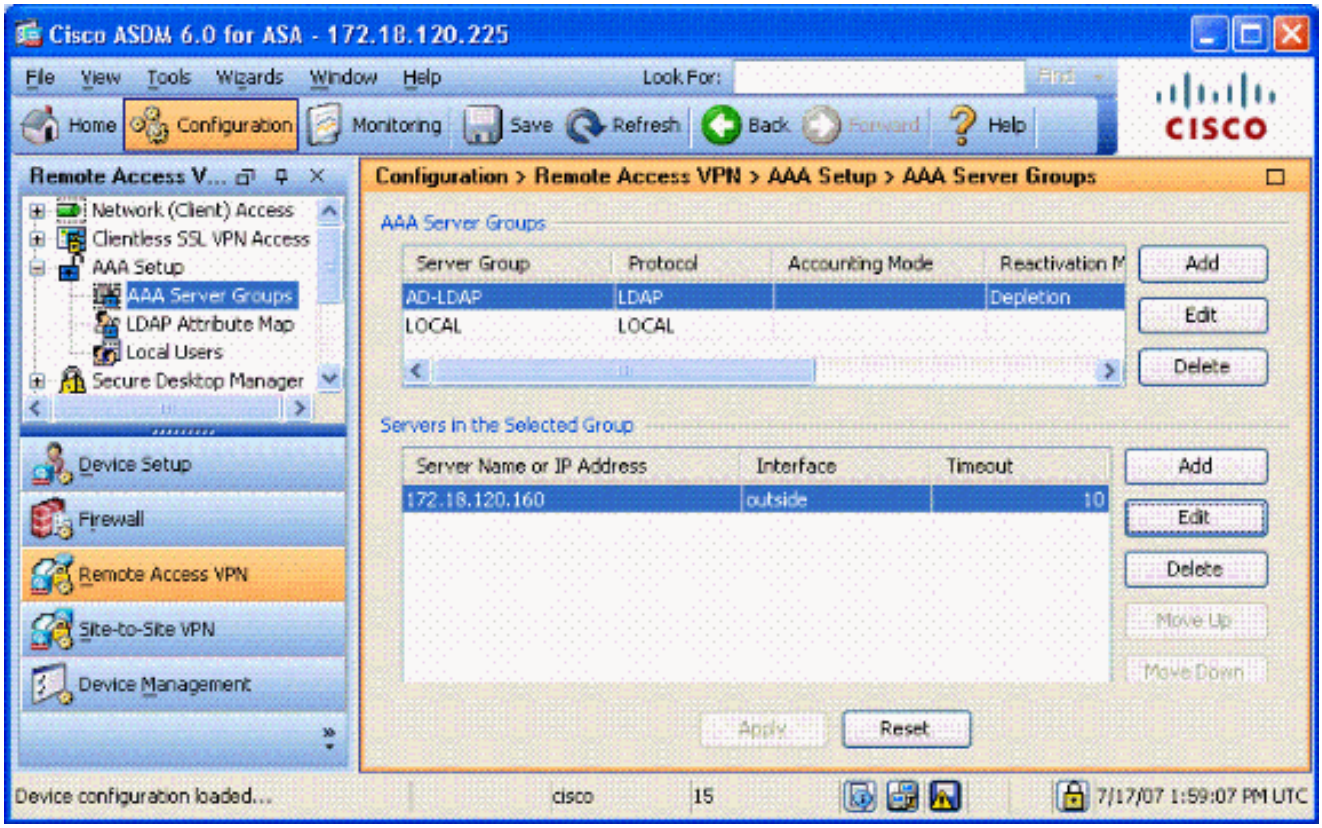
m. La configuration doit ressembler à la figure A5.

Figure A5 : Configuration de la carte d'attributs LDAP



4. Choisissez Remote Access VPN > AAA Setup > AAA Server Groups. Voir Figure A6.

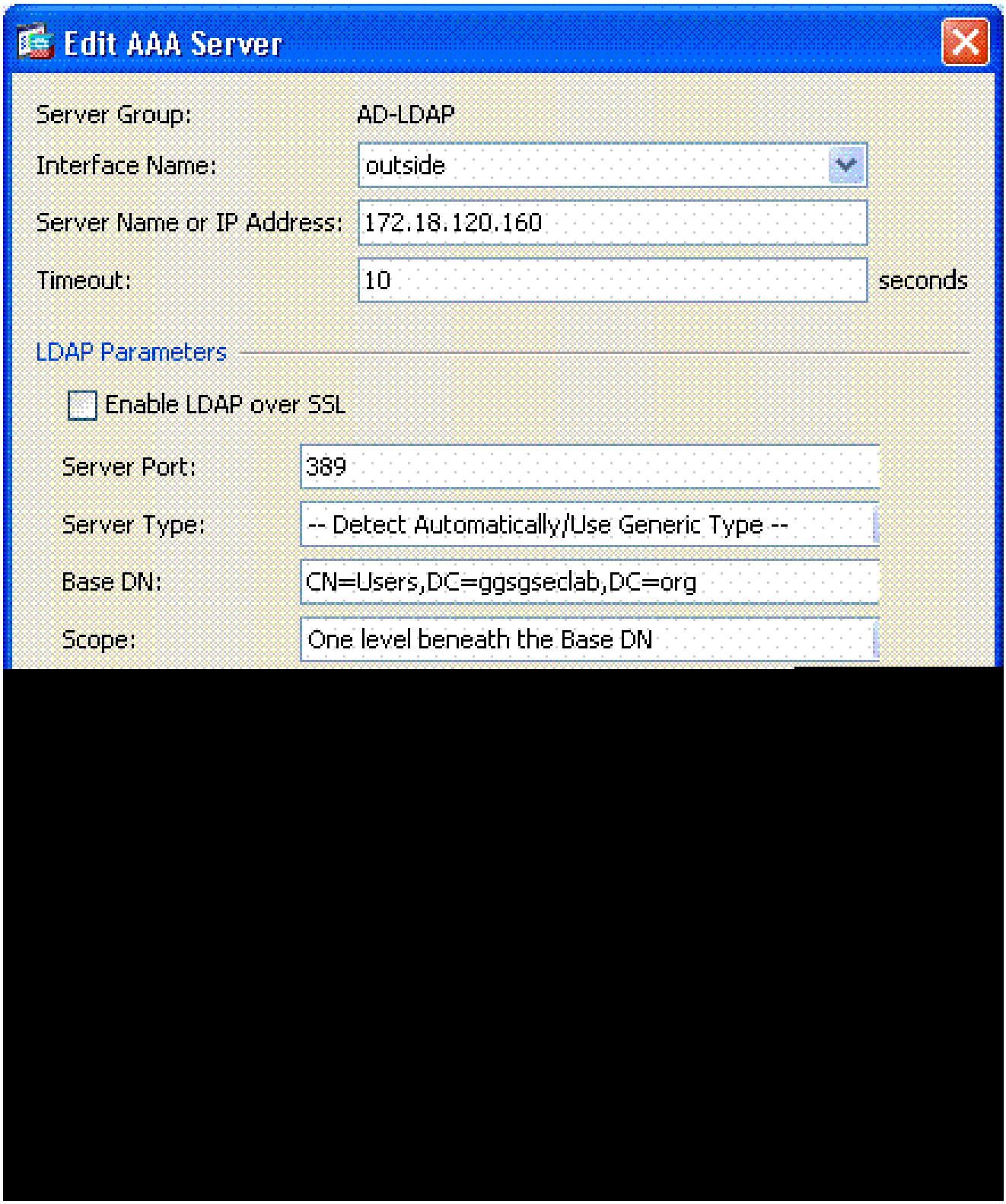
   Figure A6 : Groupes de serveurs AAA



5. Cliquez sur le groupe de serveurs que vous souhaitez modifier. Dans la section Serveurs dans le groupe sélectionné, choisissez l'adresse IP ou le nom d'hôte du serveur, puis cliquez sur Modifier.

6. Dans la fenêtre Edit AAA Server, dans la zone de texte LDAP Attribute Map, sélectionnez la carte d'attribut LDAP créée dans le menu déroulant. Voir Figure A7

   Figure A7 : Ajout d'une carte d'attributs LDAP



7. Cliquez sur OK.

Remarque : activez le débogage LDAP pendant le test afin de vérifier si la liaison LDAP et le mappage d'attributs fonctionnent correctement. Voir l'annexe C pour les commandes de dépannage.

Scénario 2 : application Active Directory utilisant l'appartenance à un groupe pour

autoriser/refuser l'accès

Cet exemple utilise l'attribut LDAP memberOf pour le mapper à l'attribut Tunneling Protocol afin d'établir une appartenance à un groupe comme condition. Pour que cette stratégie fonctionne, vous devez remplir les conditions suivantes :

- Utilisez un groupe qui existe déjà ou créez un nouveau groupe pour que les utilisateurs VPN ASA soient membres de pour les conditions ALLOW.
- Utilisez un groupe qui existe déjà ou créez un nouveau groupe pour que les utilisateurs non ASA soient membres de pour les conditions REFUSER.
- Assurez-vous de vérifier dans la visionneuse LDAP que vous avez le bon DN pour le groupe. Voir Annexe D. Si le DN est incorrect, le mappage ne fonctionne pas correctement.

Remarque : sachez que l'ASA ne peut lire que la première chaîne de l'attribut memberOf dans cette version. Assurez-vous que le nouveau groupe créé figure en haut de la liste. L'autre option consiste à placer un caractère spécial devant le nom, car AD examine d'abord les caractères spéciaux. Afin de contourner cette mise en garde, utilisez DAP dans le logiciel 8.x pour examiner plusieurs groupes.

Remarque : assurez-vous qu'un utilisateur fait partie du groupe de refus ou d'au moins un autre groupe afin que le memberOf soit toujours renvoyé à l'ASA. Vous n'avez pas besoin de spécifier la condition FALSE deny, mais la meilleure pratique consiste à le faire. Si le nom de groupe existant ou le nom de groupe contient un espace, entrez l'attribut de la manière suivante :

```
CN=Opérateurs de sauvegarde,CN=Intégré,DC=ggsgseclab,DC=org
```

Remarque : DAP permet à l'ASA d'examiner plusieurs groupes dans l'attribut memberOf et l'autorisation de base des groupes. Reportez-vous à la section DAP.

CARTOGRAPHIE

- Valeur de l'attribut AD :
  - memberOf CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
  - memberOf CN=ClientsTelnet,CN=Utilisateurs,DC=labrat,DC=com
- Valeur d'attribut Cisco : 1 = FAUX, 20 = VRAI,

Pour la condition ALLOW, vous mappez :

- memberOf CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org= 20

Pour la condition DENY, vous mappez :

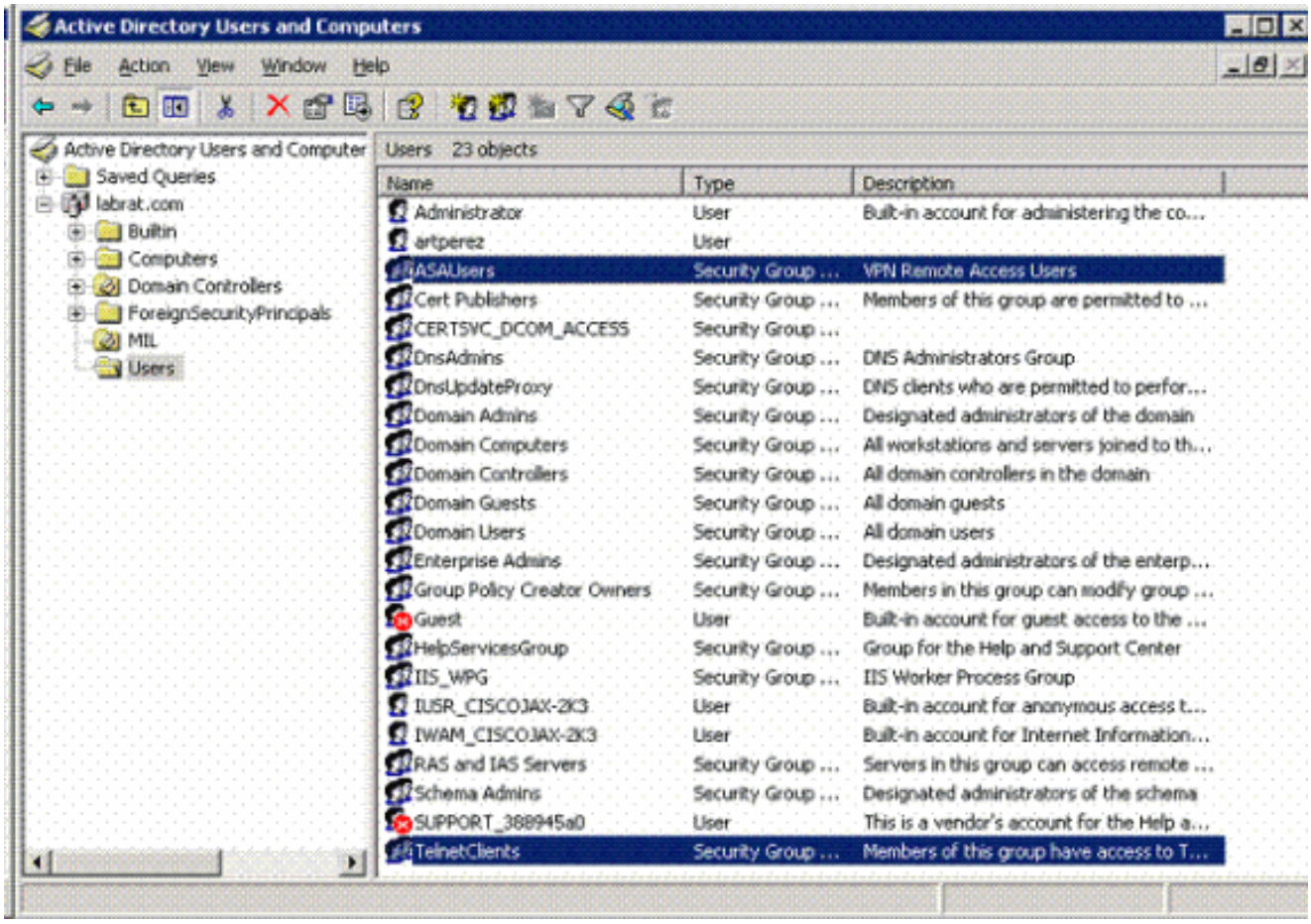
- memberOf CN=ClientsTelnet,CN=Utilisateurs,DC=ggsgseclab,DC=org = 1

Remarque : dans les versions futures, il y a un attribut Cisco afin d'autoriser et de refuser la connexion. Référez-vous à Configuration d'un serveur externe pour l'autorisation utilisateur du dispositif de sécurité pour plus d'informations sur les attributs Cisco.

Installation d'Active Directory

1. Dans le serveur Active Directory, choisissez Démarrer > Exécuter.
2. Dans la zone de texte Ouvrir, tapez dsa.msc, puis cliquez sur Ok. La console de gestion Active Directory démarre.
3. Dans la console de gestion Active Directory, cliquez sur le signe plus afin de développer le groupe Utilisateurs et ordinateurs Active Directory. Voir Figure A8

   Figure A8 : Groupes Active Directory



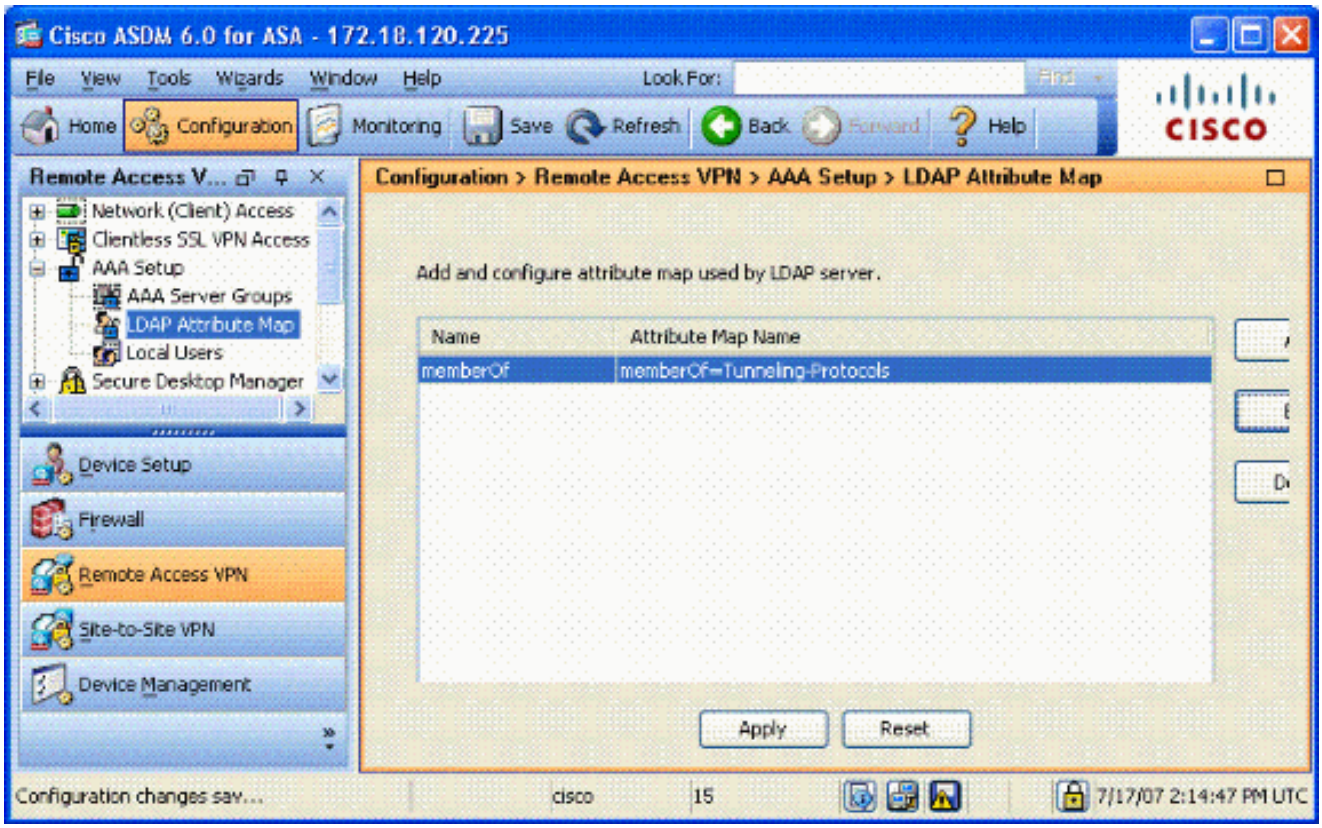
4. Cliquez sur le signe plus afin de développer le nom de domaine.
5. Cliquez avec le bouton droit sur le dossier Users et choisissez New > Group.
6. Saisissez un nom de groupe. Par exemple : ASAUsers.
7. Cliquez sur OK.

8. Cliquez sur le dossier Users, puis double-cliquez sur le groupe que vous venez de créer.
9. Sélectionnez l'onglet Membres, puis cliquez sur Ajouter.
10. Tapez le nom de l'utilisateur que vous souhaitez ajouter, puis cliquez sur Ok.

Configuration ASA

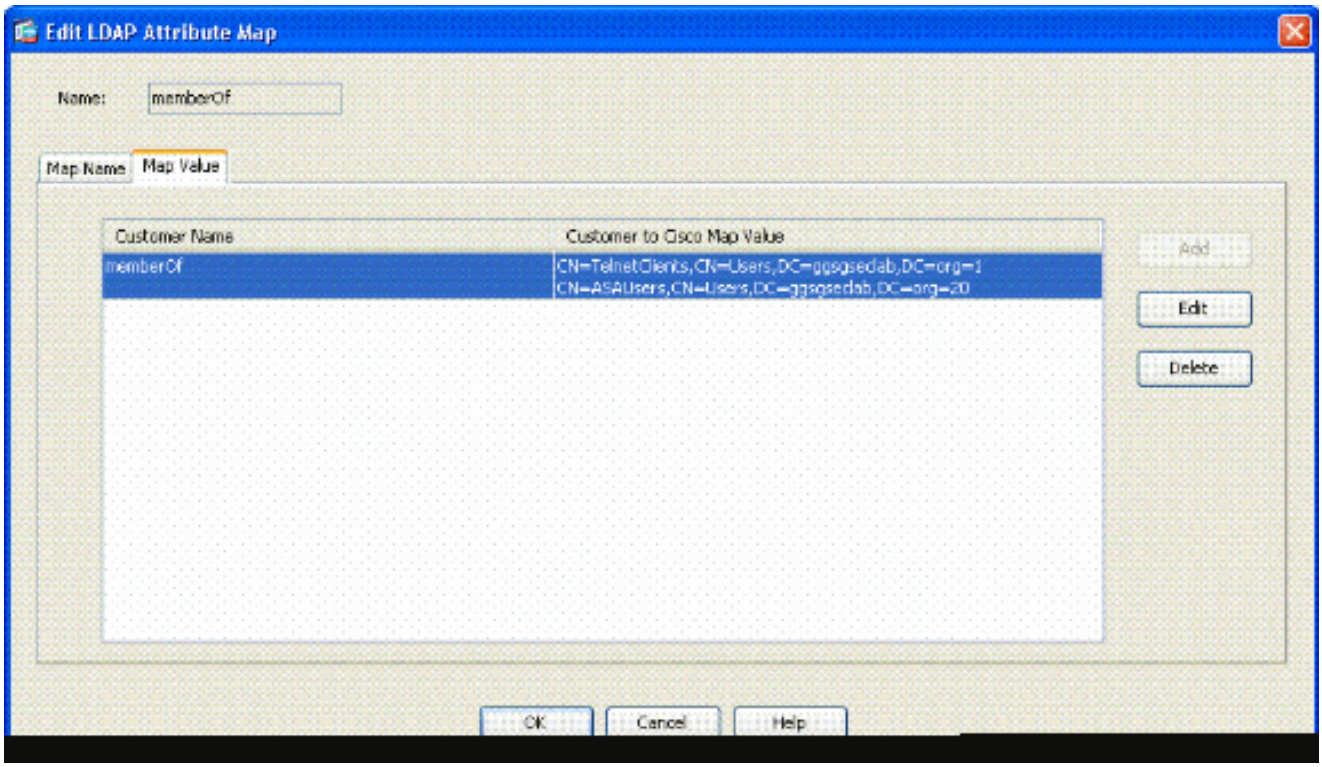
1. Dans ASDM, choisissez Remote Access VPN > AAA Setup > LDAP Attribute Map.
2. Cliquez sur Add.
3. Dans la fenêtre Ajouter une correspondance d'attributs LDAP, procédez comme suit. Voir Figure A3.
    a. Entrez un nom dans la zone de texte Nom.
    b. Dans l'onglet Nom du mappage, tapez memberOf dans la zone de texte Nom du client c.
    c. Dans l'onglet Map Name, choisissez Tunneling-Protocols dans l'option déroulante de Cisco Name.
    d. Sélectionnez Ajouter.
    e. Cliquez sur l'onglet Valeur de mappage.
    f. Sélectionnez Ajouter.
    g. Dans la fenêtre Ajouter une valeur de mappage LDAP d'attribut, tapez CN=ASAUsers, CN=Users, DC=ggsgseclab, DC=org dans la zone de texte Nom du client et tapez 20 dans la zone de texte Valeur Cisco.
    h. Cliquez sur Add.
    i. Tapez CN=TelnetClients,CN=Users,DC=ggsgseclab,DC=org dans la zone de texte Nom du client et tapez 1 dans la zone de texte Valeur Cisco. Voir Figure A4.
    j. Cliquez sur OK.
    k. Cliquez sur OK.
    l. Cliquez sur Apply.
    m. La configuration doit ressembler à la figure A9.

Figure A9 Mappage des attributs LDAP



4. Choisissez Remote Access VPN > AAA Setup > AAA Server Groups.

5. Cliquez sur le groupe de serveurs que vous souhaitez modifier. Dans la section Serveurs du groupe sélectionné, sélectionnez l'adresse IP ou le nom d'hôte du serveur, puis cliquez sur Modifier



6. Dans la fenêtre Edit AAA Server, dans la zone de texte LDAP Attribute Map, sélectionnez la carte d'attribut LDAP créée dans le menu déroulant.

7. Cliquez sur OK.

Remarque : activez le débogage LDAP pendant le test afin de vérifier que la liaison LDAP et les mappages d'attributs fonctionnent correctement. Voir l'annexe C pour les commandes de dépannage.

Scénario 3 : Stratégies d'accès dynamique pour plusieurs attributs memberOf

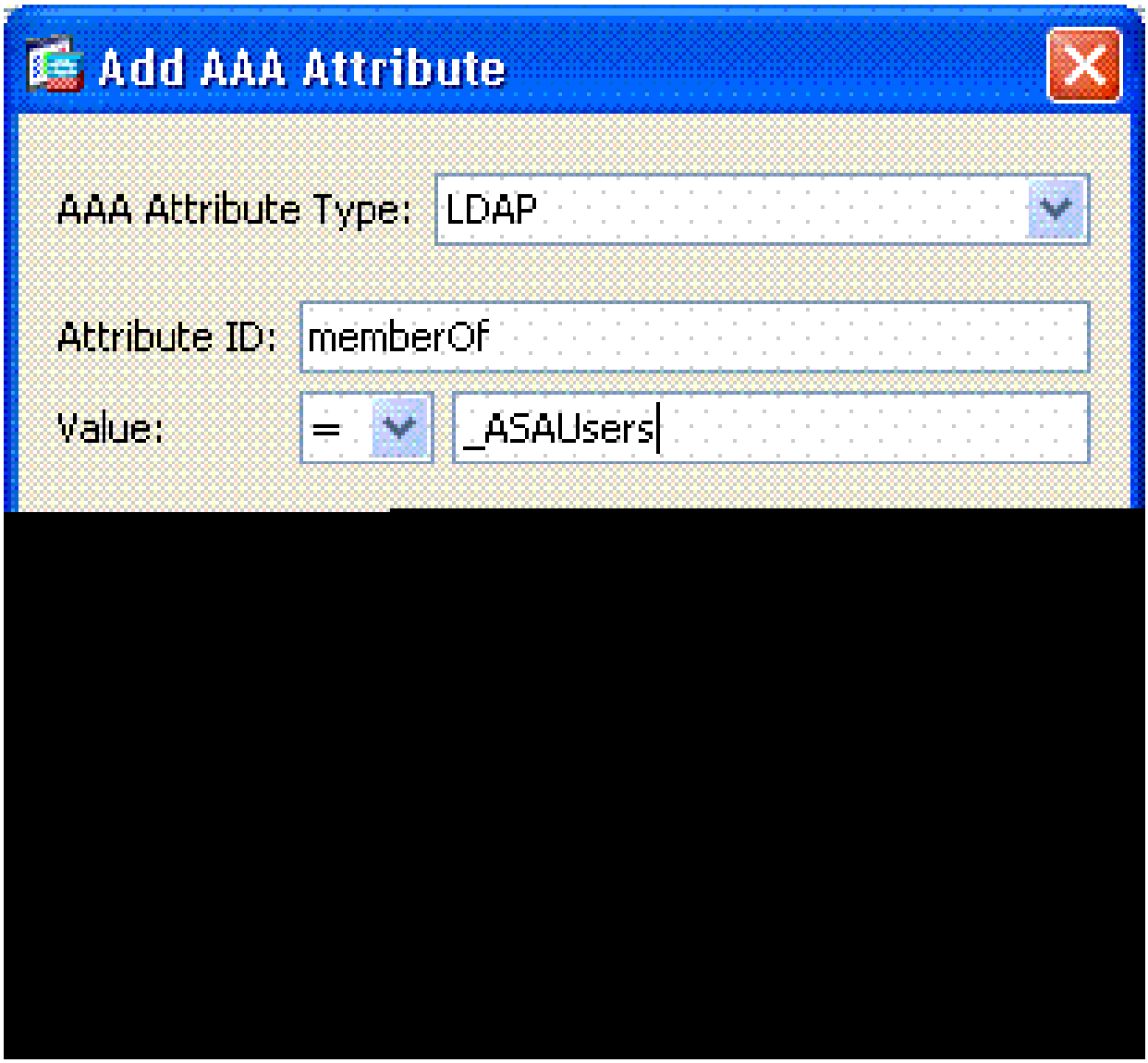
Cet exemple utilise DAP pour examiner plusieurs attributs memberOf afin d'autoriser l'accès basé sur l'appartenance à un groupe Active Directory. Avant 8.x, l'ASA ne lisait que le premier attribut memberOf. Avec 8.x et les versions ultérieures, l'ASA peut examiner tous les attributs memberOf.

- Utilisez un groupe qui existe déjà ou créez un nouveau groupe (ou plusieurs groupes) pour que les utilisateurs VPN ASA soient membres des conditions ALLOW.
- Utilisez un groupe qui existe déjà ou créez un nouveau groupe pour que les utilisateurs non ASA soient membres de pour les conditions REFUSER.
- Assurez-vous de vérifier dans la visionneuse LDAP que vous avez le bon DN pour le groupe. Voir Annexe D. Si le DN est incorrect, le mappage ne fonctionne pas correctement.

Configuration ASA

1. Dans ASDM, choisissez Remote Access VPN> Network (Client) Access > Dynamic Access Policies.
2. Cliquez sur Add.
3. Dans Ajouter une stratégie d'accès dynamique, procédez comme suit :
    a. Entrez un nom dans la zone de texte Nom b.
    b. Dans la section priority, entrez 1, ou un nombre supérieur à 0.
    c. Dans le champ Critères de sélection, cliquez sur Ajouter.
    d. Dans Ajouter un attribut AAA, choisissez LDAP .
    e. Dans la section ID d'attribut, entrez memberOf.
    f. Dans la section Value, choisissez = et entrez le nom du groupe AD. Répétez cette étape pour chaque groupe que vous souhaitez référencer. Voir figure A10.

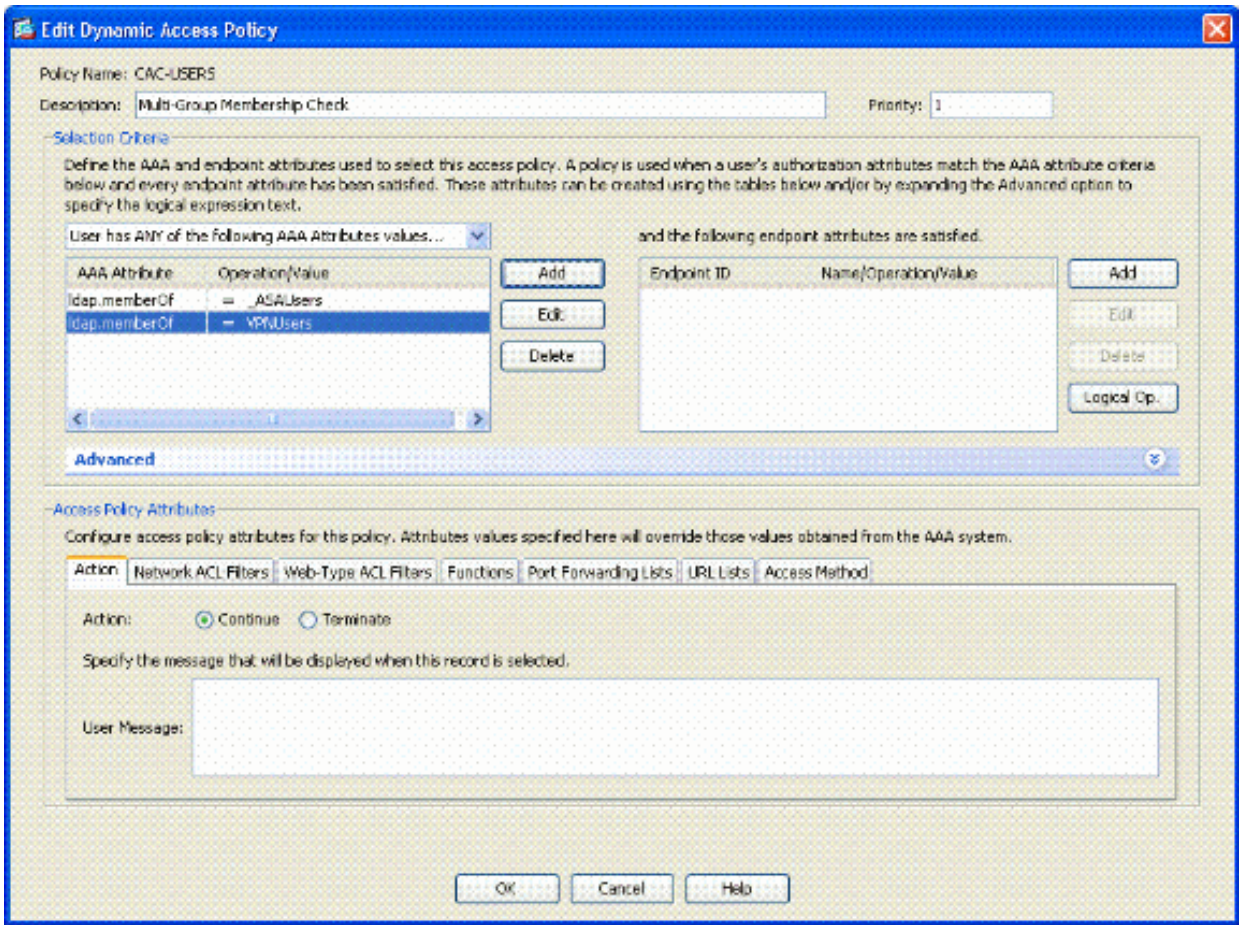
    Figure A10 Carte des attributs AAA



g. Click OK.

h. Dans la section Attributs de stratégie d'accès, sélectionnez Continuer. Voir figure A11.

Figure A11 Ajout d'une politique dynamique

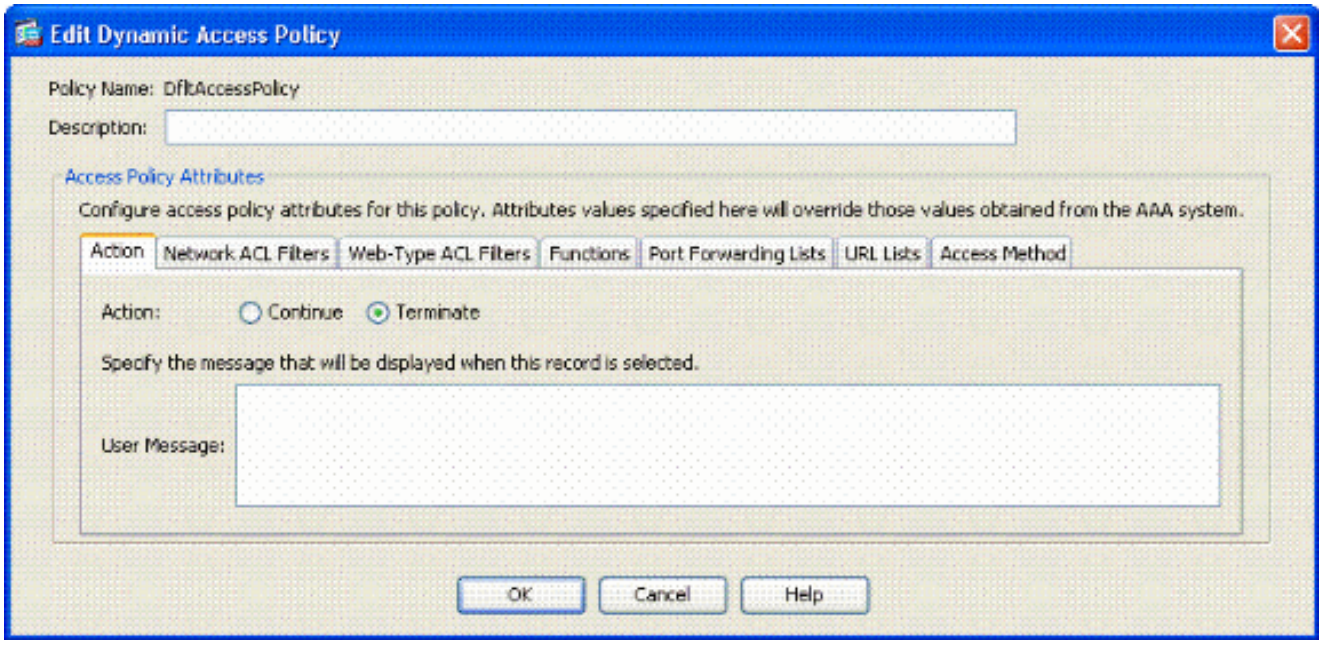


4. Dans ASDM, choisissez Remote Access VPN> Network (Client) Access > Dynamic Access Policies.

5. Choisissez Default Access Policy et choisissez Edit.

6. L'action par défaut doit être définie sur Terminate. Voir figure A12.

   Figure A12 Modifier une politique dynamique



7. Cliquez sur OK.

Remarque : si l'option Terminer n'est pas sélectionnée, vous pouvez y accéder même si vous ne faites partie d'aucun groupe, car la valeur par défaut est Continuer.

Annexe B - Configuration de l'interface CLI ASA

ASA 5510

```
<#root>

ciscoasa#

show running-config

: Saved
:
ASA Version 8.0(2)
!
hostname asa80
domain-name army.mil
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address x.x.x.x 255.255.255.128
!
interface GigabitEthernet0/1
nameif inside
security-level 100
no ip address
!
boot system disk0:/asa802-k8.bin
ftp mode passive
dns server-group DefaultDNS
domain-name army.mil
!
--------------ACL's-----------------------------------------------
access-list out extended permit ip any any
------------------------------------------------------------------
pager lines 24
logging console debugging
mtu outside 1500
!
---------------VPN Pool-------------------------------------------
ip local pool CAC-USERS 192.168.1.1-192.168.1.254 mask 255.255.255.0
------------------------------------------------------------------
!
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin
no asdm history enable
arp timeout 14400
access-group out in interface outside
route outside 0.0.0.0 0.0.0.0 172.18.120.129 1
```

```
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00
timeout uauth 0:05:00 absolute
!
-------------------------LDAP Maps & DAP--------------------------
ldap attribute-map memberOf
map-name memberOf Tunneling-Protocols
March 11, 2008 ASA - CAC Authentication for AnyConnect VPN Access
Company Confidential. A printed copy of this document is considered uncontrolled.
49
map-value memberOf CN=_ASAUsers,CN=Users,DC=ggsgseclab,DC=org 20
ldap attribute-map msNPAllowDialin
map-name msNPAllowDialin Tunneling-Protocols
map-value msNPAllowDialin FALSE 1
map-value msNPAllowDialin TRUE 20
dynamic-access-policy-record CAC-USERS
description "Multi-Group Membership Check"
priority 1
dynamic-access-policy-record DfltAccessPolicy
action terminate
------------------------------------------------------------------------
!
--------------------LDAP Server-------------------------------------
aaa-server AD-LDAP protocol ldap
aaa-server AD-LDAP (outside) host 172.18.120.160
ldap-base-dn CN=Users,DC=ggsgseclab,DC=org
ldap-scope onelevel
ldap-naming-attribute userPrincipalName
ldap-login-password *
ldap-login-dn CN=Administrator,CN=Users,DC=ggsgseclab,DC=org
------------------------------------------------------------------------
!
aaa authentication http console LOCAL
http server enable 445
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
!
----------------CA Trustpoints-----------------------------------
crypto ca trustpoint ASDM_TrustPoint0
revocation-check ocsp
enrollment terminal
keypair DoD-1024
match certificate DefaultCertificateMap override ocsp trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
crl configure
crypto ca trustpoint ASDM_TrustPoint1
revocation-check ocsp
enrollment terminal
fqdn asa80
subject-name CN=asa80,OU=PKI,OU=DoD,O=U.S. Government,C=US
keypair DoD-1024
match certificate DefaultCertificateMap override ocsp trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
no client-types
crl configure
crypto ca trustpoint ASDM_TrustPoint2
```

```
revocation-check ocsp
enrollment terminal
keypair DoD-2048
match certificate DefaultCertificateMap override ocsp trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
no client-types
crl configure
crypto ca trustpoint ASDM_TrustPoint3
revocation-check ocsp none
enrollment terminal
crl configure
!
------------------Certificate Map-----------------------------
crypto ca certificate map DefaultCertificateMap 10
subject-name ne ""
--------------------CA Certificates (Partial Cert is Shown)------------
crypto ca certificate chain ASDM_TrustPoint0
certificate ca 37
3082044c 30820334 a0030201 02020137 300d0609 2a864886 f70d0101
05050030
60310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603
55040b13
03504b49 311b3019 06035504 03131244 6f44204a 49544320 526f6f74
crypto ca certificate chain ASDM_TrustPoint1
certificate 319e
30820411 3082037a a0030201 02020231 9e300d06 092a8648 86f70d01
01050500
305c310b 30090603 55040613 02555331 18301606 0355040a 130f552e
532e2047
6f766572 6e6d656e 74310c30 0a060355 040b1303 446f4431 0c300a06
0355040b
crypto ca certificate chain ASDM_TrustPoint2
certificate ca 37
3082044c 30820334 a0030201 02020137 300d0609 2a864886 f70d0101
05050030
60310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603
55040b13
f766e045 f15ddb43 9549d1e9 a0ea6814 b64bcece 089e1b6e 1be959a5
6fc20a76
crypto ca certificate chain ASDM_TrustPoint3
certificate ca 05
30820370 30820258 a0030201 02020105 300d0609 2a864886 f70d0101
05050030
5b310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603
55040b13
03504b49 31163014 06035504 03130d44 6f442052 6f6f7420 43412032
301e170d
30343132 31333135 30303130 5a170d32 39313230 35313530 3031305a
305b310b
30090603 55040613 02555331 18301606 0355040a 130f552e 532e2047
6f766572
6e6d656e 74310c30 0a060355 040b1303 446f4431 0c300a06 0355040b
1303504b
49311630 14060355 0403130d 446f4420 526f6f74 20434120 32308201
crypto ca certificate chain ASDM_TrustPoint4
certificate ca 04
```

```
30820267 308201d0 a0030201 02020104 300d0609 2a864886 f70d0101
05050030
61310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603
55040b13
03504b49 311c301a 06035504 03131344 6f442043 4c415353 20332052
6f6f7420
!
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
!
-------------------------SSL/WEBvpn-windows-----------------------------------
ssl certificate-authentication interface outside port 443
webvpn
enable outside
svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1
svc enable
tunnel-group-list enable
-----------------------------------------------------------------------
-----------------------VPN Group/Tunnel Policy--------------------
group-policy CAC-USERS internal
ggroup-policy AC-USERS internal
group-policy AC-USERS attributes
vpn-windows-tunnel-protocol svc
address-pools value CAC-USERS
webvpn
svc ask none default svc
tunnel-group AC-USERS type remote-access
tunnel-group AC-USERS general-attributes
authorization-server-group AD-LDAP
default-group-policy AC-USERS
authorization-required
authorization-dn-attributes UPN
tunnel-group AC-USERS webvpn-windows-attributes
authentication certificate
group-alias AC-USERS enable
tunnel-group-map enable rules
```

```
no tunnel-group-map enable ou
no tunnel-group-map enable ike-id
no tunnel-group-map enable peer-ip
------------------------------------------------------------------
prompt hostname context
```

Annexe C - Dépannage

Dépannage des protocoles AAA et LDAP

- debug ldap 255 : affiche les échanges LDAP
- debug aaa common 10 : affiche les échanges AAA

Exemple 1 : Connexion autorisée avec mappage d'attribut correct

Cet exemple montre le résultat de debug ldap et de debug aaa common pendant une connexion réussie avec le scénario 2 montré dans l'Annexe A.

Figure C1 : sortie commune debug LDAP et debug aaa - mappage correct

```
AAA API: In aaa_open
AAA session opened: handle = 39
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(1a87a64) received message type 0
AAA FSM: In AAA_StartAAATransaction
AAA FSM: In AAA_InitTransaction
Initiating authorization query (Svr Grp: AD-LDAP)
-------------------------------------------------
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: 172.18.120.160
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
Resp:
[78] Session Start
[78] New request Session, context 0x26f1c44, reqType = 0
[78] Fiber started
[78] Creating LDAP context with uri=ldap:// 172.18.120.160:389
[78] Binding as administrator
[78] Performing Simple authentication for Administrator to
172.18.120.160
[78] Connect to LDAP server: ldap:// 172.18.120.160, status =
Successful
[78] LDAP Search:
Base DN = [CN=Users,DC=ggsgseclab,DC=org]
Filter = [userPrincipalName=1234567890@mil]
Scope = [SUBTREE]
[78] Retrieved Attributes:
[78] objectClass: value = top
[78] objectClass: value = person
[78] objectClass: value = organizationalPerson
```

```
[78] objectClass: value = user
[78] cn: value = Ethan Hunt
[78] sn: value = Hunt
[78] userCertificate: value =
0..50........./........60...*.H........0@1.0.....&...,d....com1.0.....
&...,d...
[78] userCertificate: value =
0..'0........./..t.....50...*.H........0@1.0.....&...,d....com1.0.....
&...,d...
[78] givenName: value = Ethan
[78] distinguishedName: value = CN=Ethan
Hunt,OU=MIL,DC=labrat,DC=com
[78] instanceType: value = 4
[78] whenCreated: value = 20060613151033.0Z
[78] whenChanged: value = 20060622185924.0Z
[78] displayName: value = Ethan Hunt
[78] uSNCreated: value = 14050
[78] memberOf: value = CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
[78] mapped to cVPN3000-Tunneling-Protocols: value = 20
[78] uSNChanged: value = 14855
[78] name: value = Ethan Hunt
[78] objectGUID: value = ..9...NJ..GU..z.
[78] userAccountControl: value = 66048
[78] badPwdCount: value = 0
[78] codePage: value = 0
[78] countryCode: value = 0
[78] badPasswordTime: value = 127954717631875000
[78] lastLogoff: value = 0
[78] lastLogon: value = 127954849209218750
[78] pwdLastSet: value = 127946850340781250
[78] primaryGroupID: value = 513
[78] objectSid: value = ................q......mY...
[78] accountExpires: value = 9223372036854775807
[78] logonCount: value = 25
[78] sAMAccountName: value = 1234567890
[78] sAMAccountType: value = 805306368
[78] userPrincipalName: value = 1234567890@mil
[78] objectCategory: value =
[78] mail: value = Ethan.Hunt@labrat.com
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
[78] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
[78] Session End
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
------------------
Authorization Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE, auth_status = ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_TUNN_GRP_POLICY,
AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(CAC-USERS)
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp: GROUP_POLICY_DB)
-------------------------------------------------
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: <Internal Server>
AAA FSM: In AAA_SendMsg
```

```
User: CAC-USER
Pasw:
Resp:
grp_policy_ioctl(12f1b20, 114698, 1a870b4)
grp_policy_ioctl: Looking up CAC-USERS
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
------------------
Tunnel Group Policy Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY, auth_status =
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_DONE,
AAA FSM: In AAA_ProcessFinal
Checking time simultaneous login restriction for user 1234567890@mil
AAA FSM: In AAA_Callback
user attributes:
1 Tunnelling-Protocol(4107) 20 20
user policy attributes:
None
tunnel policy attributes:
1 Primary-DNS(4101) 4 IP: 10.0.10.100
2 Secondary-DNS(4102) 4 IP: 0.0.0.0
3 Tunnelling-Protocol(4107) 4 4
4 Default-Domain-Name(4124) 10 "ggsgseclab.org"
5 List of address pools to assign addresses from(4313) 10
"CAC-USERS"
Auth Status = ACCEPT
AAA API: In aaa_close
AAA task: aaa_process_msg(1a87a64) received message type 3
In aaai_close_session (39)
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop
CAC-Test#
```

Exemple 2 : Connexion autorisée avec mappage d'attribut Cisco mal configuré

Cet exemple montre le résultat de debug ldap et de debug aaa common pendant une connexion autorisée avec le scénario 2 montré dans l'Annexe A.

Figure C2 : résultat commun de debug LDAP et debug aaa - mappage incorrect

```
AAA API: In aaa_open
AAA session opened: handle = 41
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(1a87a64) received message type 0
AAA FSM: In AAA_StartAAATransaction
AAA FSM: In AAA_InitTransaction
Initiating authorization query (Svr Grp: AD-LDAP)
```

```
-----------------------------------------------
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: 172.18.120.160
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
Resp:
[82] Session Start
[82] New request Session, context 0x26f1c44, reqType = 0
[82] Fiber started
[82] Creating LDAP context with uri=ldap://172.18.120.160:389
[82] Binding as administrator
[82] Performing Simple authentication for Administrator to
172.18.120.160
[82] Connect to LDAP server: ldap:// 172.18.120.160:389, status =
Successful
[82] LDAP Search:
Base DN = [CN=Users,DC=ggsgseclab,DC=org]
Filter = [userPrincipalName=1234567890@mil]
Scope = [SUBTREE]
[82] Retrieved Attributes:
[82] objectClass: value = top
[82] objectClass: value = person
[82] objectClass: value = organizationalPerson
[82] objectClass: value = user
[82] cn: value = Ethan Hunt
[82] sn: value = Hunt
[82] userCertificate: value =
0..50.........../........60...*.H........0@1.0.....&...,d....com1.0.....
&...,d...
[82] userCertificate: value =
0..'0.........../..t.....50...*.H........0@1.0.....&...,d....com1.0.....
&...,d...
[82] givenName: value = Ethan
[82] distinguishedName: value = CN=Ethan
Hunt,OU=MIL,DC=labrat,DC=com
[82] instanceType: value = 4
[82] whenCreated: value = 20060613151033.0Z
[82] whenChanged: value = 20060622185924.0Z
[82] displayName: value = Ethan Hunt
[82] uSNCreated: value = 14050
[82] memberOf: value = CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
[82] mapped to cVPN3000-Tunneling-Protocols: value =
CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
[82] uSNChanged: value = 14855
[82] name: value = Ethan Hunt
[82] objectGUID: value = ..9...NJ..GU..z.
[82] userAccountControl: value = 66048
[82] badPwdCount: value = 0
[82] codePage: value = 0
[82] countryCode: value = 0
[82] badPasswordTime: value = 127954717631875000
[82] lastLogoff: value = 0
[82] lastLogon: value = 127954849209218750
[82] pwdLastSet: value = 127946850340781250
[82] primaryGroupID: value = 513
[82] objectSid: value = ................q......mY...
[82] accountExpires: value = 9223372036854775807
[82] logonCount: value = 25
[82] sAMAccountName: value = 1234567890
[82] sAMAccountType: value = 805306368
[82] userPrincipalName: value = 1234567890@mil
```

```
[82] objectCategory: value =
CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=org
[82] mail: value = Ethan.Hunt@labrat.com
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 41, pAcb = 2ae115c
[82] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
[82] Session End
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
------------------
Authorization Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE, auth_status = ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_TUNN_GRP_POLICY,
AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(USAFE)
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp: GROUP_POLICY_DB)
-------------------------------------------------
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: <Internal Server>
AAA FSM: In AAA_SendMsg
User: CAC-USERS
Pasw:
Resp:
grp_policy_ioctl(12f1b20, 114698, 1a87Ob4)
grp_policy_ioctl: Looking up CAC-USERS
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 41, pAcb = 2ae115c
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
------------------
Tunnel Group Policy Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY, auth_status =
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_DONE,
AAA FSM: In AAA_ProcessFinal
Checking time simultaneous login restriction for user 1234567890@mil
AAA FSM: In AAA_Callback
user attributes:
1 Tunnelling-Protocol(4107) 20 0
user policy attributes:
None
tunnel policy attributes:
1 Primary-DNS(4101) 4 IP: 10.0.10.100
2 Secondary-DNS(4102) 4 IP: 0.0.0.0
3 Tunnelling-Protocol(4107) 4 4
4 Default-Domain-Name(4124) 10 "ggsgseclab.org"
5 List of address pools to assign addresses from(4313) 10
"CAC-USERS"
Auth Status = ACCEPT
AAA API: In aaa_close
AAA task: aaa_process_msg(1a87a64) received message type 3
```

```
In aaai_close_session (41)
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop
```

Dépannage de DAP

- debug dap errors : affiche les erreurs DAP
- debug dap trace : affiche le suivi de la fonction DAP

Exemple 1 : Connexion autorisée avec DAP

Cet exemple montre le résultat des erreurs debug dap et debug dap trace pendant une connexion réussie avec le scénario 3 présenté dans l'Annexe A. Notez plusieurs attributs memberOf. Vous pouvez appartenir à la fois à _ASAUsers et à VPNUsers ou à l'un ou l'autre groupe, ce qui dépend de la configuration ASA.

Figure C3 : debug DAP

```
<#root>

#

debug dap errors

debug dap errors enabled at level 1
#

debug dap trace

debug dap trace enabled at level 1
#
The DAP policy contains the following attributes for user:
1241879298@mil
-------------------------------------------------------------------------
---
1: action = continue
DAP_TRACE: DAP_open: C8EEFA10
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.1 = top
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.2 = person
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.3 =
organizationalPerson
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.4 = user
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.cn = 1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.physicalDeliveryOfficeName = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.distinguishedName =
CN=1241879298,CN=Users,DC=ggsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenCreated =
20070626163734.0Z
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenChanged =
20070718151143.0Z
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.displayName = 1241879298
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNCreated = 33691
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf.1 = VPNUsers
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf.2 = _ASAUsers
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNChanged = 53274
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.department = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.name = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectGUID =
....+..F.."5....
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userAccountControl =
328192
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPwdCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.codePage = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.countryCode = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPasswordTime = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogoff = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogon = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.pwdLastSet =
128273494546718750
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.primaryGroupID = 513
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userParameters = m:
d.
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectSid = ..
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.accountExpires =
9223372036854775807
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.logonCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountName =
1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountType =
805306368
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userPrincipalName =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectCategory =
CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.msNPAllowDialin = TRUE
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.username =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.tunnelgroup = CAC-USERS
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] = "top";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] =
"user";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"] = "1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeName"] =
"NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["givenName"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298,CN=Users,DC=ggsgseclab,DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"] = "33691";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["1"] =
"VPNUsers";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["2"] =
```

```
"_ASAUsers";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"] = "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"] = "NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["name"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"] =
"128273494546718750";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] = "513";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userParameters"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectSid"] contains binary
data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["logonCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] = "TRUE";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username"] =
"1241879298@mil";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["tunnelgroup"] = "CACUSERS";
DAP_TRACE: dap_add_to_lua_tree:endpoint["application"]["clienttype"] =
"IPSec";
DAP_TRACE: Username: 1241879298@mil, Selected DAPs: CAC-USERS
DAP_TRACE: dap_request: memory usage = 33%
DAP_TRACE: dap_process_selected_daps: selected 1 records
DAP_TRACE: Username: 1241879298@mil, dap_aggregate_attr: rec_count = 1
DAP_TRACE: Username: 1241879298@mil, DAP_close: C8EEFA10
d.
```

Exemple 2 : Connexion refusée avec DAP

Cet exemple montre le résultat des erreurs debug dap et debug dap trace pendant une connexion infructueuse avec le scénario 3 présenté dans l'Annexe A.

Figure C4 : debug DAP

```
<#root>

#

debug dap errors
```

```
debug dap errors enabled at level 1
#
debug dap trace

debug dap trace enabled at level 1
#
The DAP policy contains the following attributes for user:
1241879298@mil
------------------------------------------------------------------------
---
1: action = terminate
DAP_TRACE: DAP_open: C91154E8
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.1 = top
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.2 = person
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.3 =
organizationalPerson
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.4 = user
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.cn = 1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.physicalDeliveryOfficeName = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.distinguishedName =
CN=1241879298,CN=Users,DC=ggsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenCreated =
20070626163734.0Z
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenChanged =
20070718151143.0Z
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.displayName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNCreated = 33691
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf = DnsAdmins
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNChanged = 53274
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.department = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.name = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectGUID =
....+..F.."5....
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userAccountControl =
328192
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPwdCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.codePage = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.countryCode = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPasswordTime = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogoff = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogon = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.pwdLastSet =
128273494546718750
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.primaryGroupID = 513
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userParameters = m:
d.
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectSid = ..
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.accountExpires =
9223372036854775807
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.logonCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountName =
1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountType =
805306368
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userPrincipalName =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectCategory =
CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=org
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.msNPAllowDialin = TRUE
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.username =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.tunnelgroup = CAC-USERS
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] = "top";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] =
"user";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"] = "1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeName"] =
"NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["givenName"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298,CN=Users,DC=ggsgseclab,DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"] = "33691";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"] = "DnsAdmins";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"] = "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"] = "NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["name"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"] =
"128273494546718750";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] = "513";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userParameters"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectSid"] contains binary
data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["logonCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] = "TRUE";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username"] =
"1241879298@mil";
DAP_TRACE: Username: 1241879298@mil, Selected DAPs:
```

```
DAP_TRACE: dap_request: memory usage = 33%
DAP_TRACE: dap_process_selected_daps: selected 0 records
DAP_TRACE: Username: 1241879298@mil, dap_aggregate_attr: rec_count = 1
```

Dépannage de l'autorité de certification / OCSP

- debug crypto ca 3
- En mode de configuration : logging class ca console(or buffer) debugging

Ces exemples montrent une validation de certificat réussie avec le répondeur OCSP et une stratégie de correspondance de groupe de certificats ayant échoué.

La Figure C3 montre la sortie de débogage qui a un certificat validé et un groupe de certificats de travail correspondant à la stratégie.

La Figure C4 montre la sortie de débogage d'une stratégie de correspondance de groupe de certificats mal configurée.

La Figure C5 montre la sortie de débogage d'un utilisateur avec un certificat révoqué.

Figure C5 : Débogage OCSP - validation de certificat réussie

```
CRYPTO_PKI: Found a suitable authenticated trustpoint
ASDM_TrustPoint11.
CRYPTO_PKI: Allocated OCSP data handle 0xca2d27b8
CRYPTO_PKI: Certificate validation: Successful, status: 0. Attempting
to retrieve revocation status if necessary
CRYPTO_PKI: status = 0: poll revocation status
CRYPTO_PKI: Attempting to find OCSP override for peer cert: serial
number: 0F192B, subject name:
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-
15,ou=PKI,ou=DoD,o=U.S. Government,c=US.
CRYPTO_PKI: Processing map rules for SSL.
CRYPTO_PKI: Processing map SSL sequence 20...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field:
= cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: SSL sequence: 20.
CRYPTO_PKI: Found OCSP override match. Override URL:
http://198.154.68.90, Override trustpoint: ASDM_TrustPoint12
CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
CRYPTO_PKI: Destroying OCSP data handle 0xca2d27b8
Crypto CA thread sleeps!
CRYPTO_PKI: Attempting to find tunnel group for cert with serial
number: 0F192B, subject name:
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-
15,ou=PKI,ou=DoD,o=U.S. Government,c=US.
CRYPTO_PKI: Processing map rules for DefaultCertificateMap.
CRYPTO_PKI: Processing map DefaultCertificateMap sequence 10...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field:
```

```
= cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: DefaultCertificateMap
sequence: 10.
CRYPTO_PKI: Ignoring match on map DefaultCertificateMap, index 10 for
WebVPN group map processing. No tunnel group is configured.
CRYPTO_PKI: Peer cert could not be authorized with map:
DefaultCertificateMap.
CRYPTO_PKI: Processing map rules for SSL.
CRYPTO_PKI: Processing map SSL sequence 20...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field:
= cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: SSL sequence: 20.
CRYPTO_PKI: Ignoring match on map SSL, index 20 for WebVPN group map
```

Figure C5 : Résultats d'une stratégie de correspondance de groupe de certificats ayant échoué

Figure C5 : Résultats d'un certificat révoqué

```
n %PI=X-3-7E17t02h7a Certinf icaHtue cnhta,in faioled uvalidation=.
CMertifiIcLa,ted ccha=inl ais eibtrhaer tin,valdid cor =noct
oamuthori,zed.
map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: DefaultCertificateMap
sequence: 10.
Tunnel Group Match on map DefaultCertificateMap sequence # 10.
Group name is CAC-USERS
CRYPTO_PKI: Checking to see if an identical cert is
already in the database...
CRYPTO_PKI: looking for cert in handle=2467668, digest=
CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
CRYPTO_PKI: Cert not found in database.
CRYPTO_PKI: Looking for suitable trustpoints...
CRYPTO_PKI: Found a suitable authenticated trustpoint trustpoint0.
CRYPTO_PKI: Certificate validation: Successful, status: 0. Attempting
to retrieve revocation status if necessary
CRYPTO_PKI: Attempting to find OCSP override for peer cert: serial
number: 2FB5FC74000000000035, subject name: cn=Ethan
Hunt,ou=MIL,dc=ggsgseclab,dc=org, issuer_name:
cn=ggsgseclab,dc=ggsgseclab,dc=org.
CRYPTO_PKI: Processing map rules for DefaultCertificateMap.
CRYPTO_PKI: Processing map DefaultCertificateMap sequence 10...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field:
= cn=Ethan Hunt,ou=MIL,dc=ggsgseclab,dc=org, map rule: subject-name
ne "".
CRYPTO_PKI: Peer cert has been authorized by map: DefaultCertificateMap
sequence: 10.
CRYPTO_PKI: Found OCSP override match. Override URL:
http://ocsp.disa.mil, Override trustpoint: OCSP
CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
CRYPTO_PKI: Found a subject match
ERROR: Certificate validation failed, Certificate is revoked, serial
number: 2FB5FC74000000000035, subject name: cn=Ethan
Hunt,ou=MIL,dc=ggsgseclab,dc=org
CRYPTO_PKI: Certificate not validated
```

Annexe D - Vérification des objets LDAP dans MS

Le CD de Microsoft Server 2003 contient des outils supplémentaires qui peuvent être installés afin d'afficher la structure LDAP ainsi que les objets/attributs LDAP. Afin d'installer ces outils, allez dans le répertoire Support dans le CD, puis Tools. Installez SUPTOOLS.MSI.

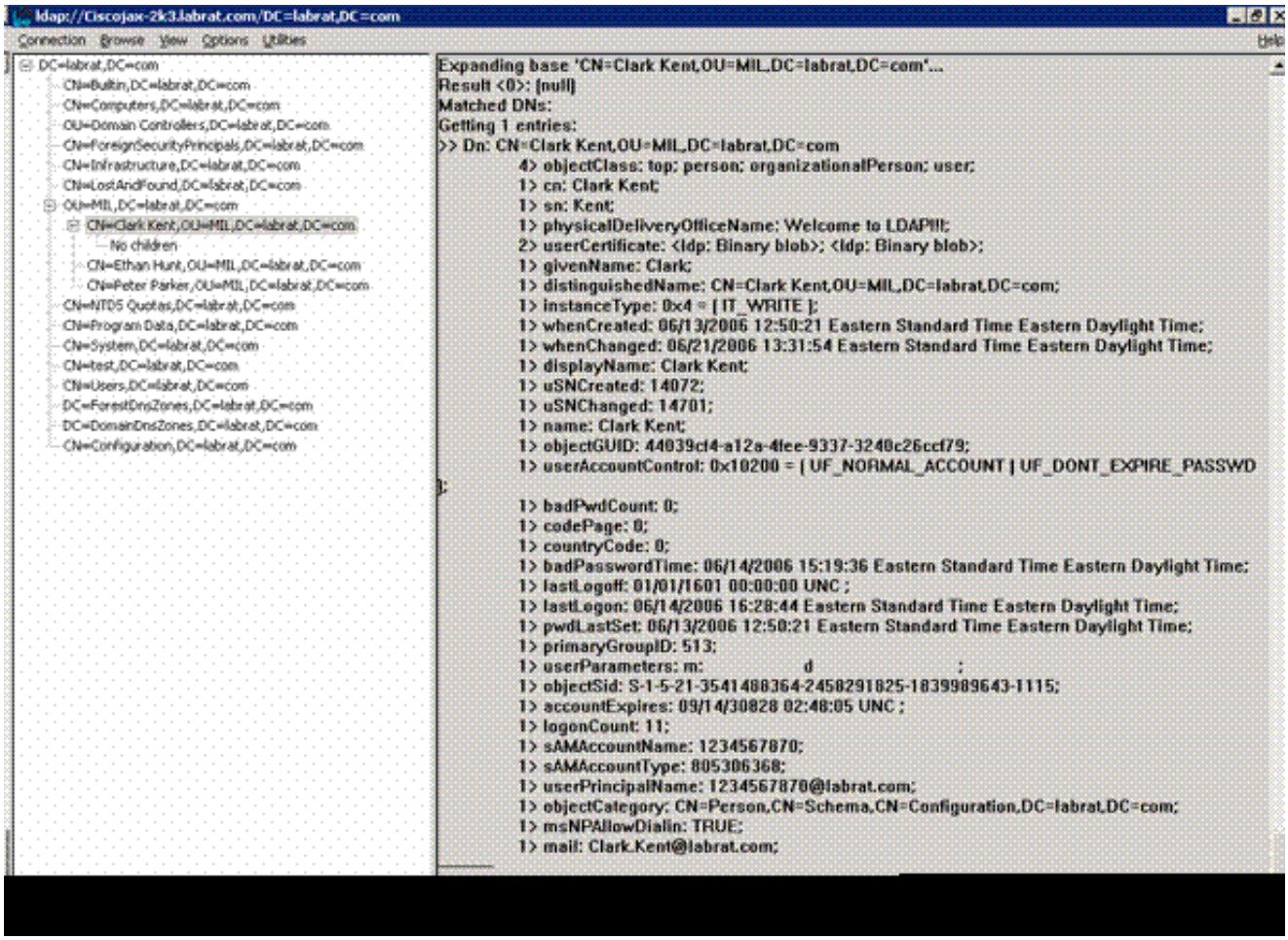
Visionneuse LDAP

1. Après l'installation, choisissez Démarrer > Exécuter.
2. Tapez ldp, puis cliquez sur Ok. La visionneuse LDAP démarre.
3. Choisissez Connection > Connect.
4. Entrez le nom du serveur, puis cliquez sur Ok.
5. Choisissez Connection > Bind.
6. Saisissez un nom d'utilisateur et un mot de passe.

   Remarque : vous devez disposer de droits d'administrateur.

7. Click OK.
8. Afficher les objets LDAP. Voir Figure D1.

   Figure D1 : Visionneuse LDAP

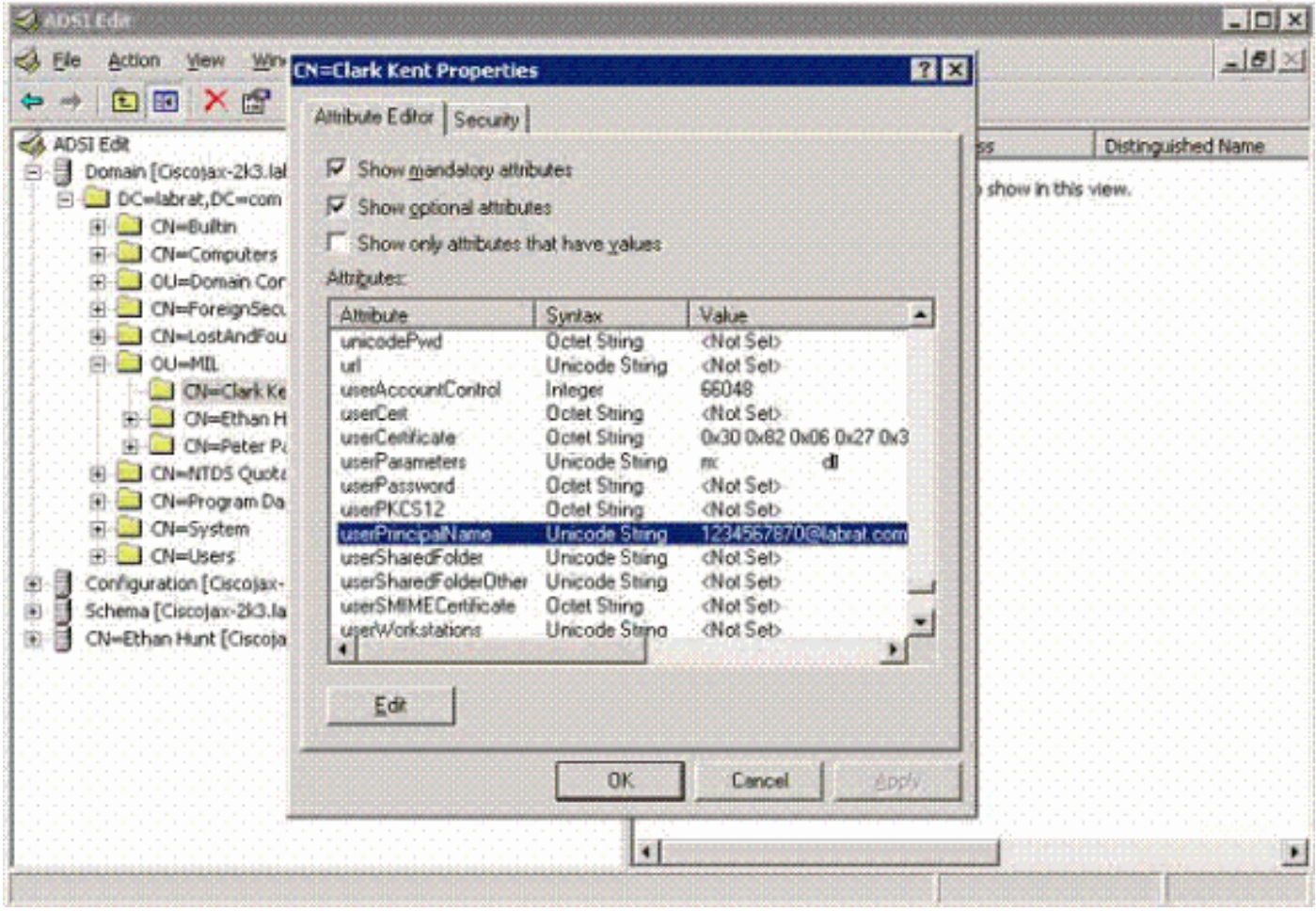


Éditeur d'interface des services Active Directory

- Dans le serveur Active Directory, choisissez Démarrer > Exécuter.
- Tapez adsiedit.msc. L'éditeur démarre.
- Cliquez avec le bouton droit sur un objet, puis cliquez sur Propriétés.

Cet outil affiche tous les attributs d'objets spécifiques. Voir Figure D2.

Figure D2 : Édition ADSI



Annexe E

Un profil AnyConnect peut être créé et ajouté à une station de travail. Le profil peut référencer diverses valeurs telles que des hôtes ASA ou des paramètres de correspondance de certificat tels que le nom distinctif ou l'émetteur. Le profil est stocké sous la forme d'un fichier .xml et peut être modifié à l'aide du Bloc-notes. Le fichier peut être ajouté manuellement à chaque client ou transmis à partir de l'ASA via une stratégie de groupe. Le fichier est stocké dans :

```
C:\Documents and Settings\All Users\Application Data\Cisco\Cisco
AnyConnect VPN Client\Profile
```

Procédez comme suit :

1. Sélectionnez le fichier AnyConnectProfile.tmpl et ouvrez-le avec le Bloc-notes.
2. Apportez les modifications appropriées au fichier, telles que l'adresse IP de l'émetteur ou de l'hôte. Voir l'exemple de la figure F1.
3. Lorsque vous avez terminé, enregistrez le fichier au format .xml.

Reportez-vous à la documentation Cisco AnyConnect concernant la gestion des profils. En bref :

- Un profil doit porter un nom unique pour votre entreprise. Exemple : CiscoProfile.xml
- Le nom du profil doit être le même, même s'il diffère pour des groupes individuels au sein de la société.

Ce fichier est destiné à être géré par un administrateur Secure Gateway, puis distribué avec le logiciel client. Le profil basé sur ce code XML peut être distribué aux clients à tout moment. Les mécanismes de distribution pris en charge sont sous la forme d'un fichier groupé avec la distribution de logiciels ou dans le cadre du mécanisme de téléchargement automatique. Le mécanisme de téléchargement automatique est uniquement disponible avec certains produits Cisco Secure Gateway.

> Remarque : les administrateurs sont vivement encouragés à valider le profil XML qu'ils créent à l'aide d'un outil de validation en ligne ou de la fonctionnalité d'importation de profil dans ASDM. La validation peut être effectuée à l'aide du fichier AnyConnectProfile.xsd situé dans ce répertoire. AnyConnectProfile est l'élément racine qui représente le profil client AnyConnect.

Voici un exemple de fichier XML de profil de client VPN Cisco AnyConnect.

```
<#root>

xml version="1.0" encoding="UTF-8"
- - <AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd">

!--- The ClientInitialization section represents global settings !--- for the client. In some cases, fo
!--

-->
-
 <ClientInitialization>

!--- The Start Before Logon feature can be used to activate !--- the VPN as part of the logon sequence.


-->
<UseStartBeforeLogon UserControllable="false">false</UseStartBeforeLogon>

!--- This control enables an administrator to have a one time !--- message displayed prior to a users t



<ShowPreConnectMessage>false</ShowPreConnectMessage>
```

```
!-- This section enables the definition of various attributes !--- that can be used to refine client ce


-->
-
<CertificateMatch>

!--- Certificate Distinguished Name matching allows !--- for exact match criteria in the choosing of ac


- <DistinguishedName>
- <DistinguishedNameDefinition Operator="Equal" Wildcard="Disabled">
<Name>ISSUER-CN</Name>
<Pattern>DoD-Issuer-ABC</Pattern>
</DistinguishedNameDefinition>
</DistinguishedName>
</CertificateMatch>
</ClientInitialization>

-
!-- This section contains the list of hosts from which !--- the user is able to select.

-
<ServerList>



!--- This is the data needed to attempt a connection to !--- a specific host.

-->
-
<HostEntry>
<HostName>host-02</HostName>
<HostAddress>host-02.dod.gov</HostAddress>
</HostEntry>
- <HostEntry>
<HostName>host-01</HostName>
<HostAddress>192.168.1.1</HostAddress>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

Informations connexes

- Certificats et LCR spécifiés par X.509 et RFC 3280
- OCSP spécifié par la RFC 2560
- Introduction à l'infrastructure à clé publique
- « OCSP léger » profilé par projet de norme
- SSL / TLS spécifié par RFC 2246
- 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.