

# ASA 8.x : Configuration de cartes à puce CAC VPN SSL AnyConnect avec prise en charge MAC

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configuration de Cisco ASA](#)

[Considérations de déploiement](#)

[Authentification, autorisation, configuration de comptabilité \(d'AAA\)](#)

[Configurez le serveur LDAP](#)

[Gérez les Certificats](#)

[Générez les clés](#)

[Installez les Certificats CA de racine](#)

[Inscrivez-vous l'ASA et installez le certificat d'identité](#)

[Configuration du VPN d'AnyConnect](#)

[Créer un groupe d'adresse IP](#)

[Créer le groupe et la stratégie de groupe de tunnel](#)

[Configurations d'interface de groupe et d'image de tunnel](#)

[Règles assorties de certificat \(si OCSP sera utilisé\)](#)

[Configurez OCSP](#)

[Configurez le certificat de répondre OCSP](#)

[Configurez le CA pour utiliser OCSP](#)

[Configurez les règles OCSP](#)

[Configuration de client de Cisco AnyConnect](#)

[Téléchargeant le Cisco AnyConnect VPN Client – Mac OS X](#)

[Cisco AnyConnect VPN Client de début – Mac OS X](#)

[Nouvelle connexion](#)

[Accès à distance de début](#)

[Annexe A – Mappage de LDAP et DAP](#)

[Scénario 1 : Application de Répertoire actif utilisant l'accès distant d'autorisation d'Accès à distance – Permettez/refusez Access](#)

[Installation de Répertoire actif](#)

[Configuration ASA](#)

[Scénario 2 : L'application de Répertoire actif utilisant l'adhésion à des associations à laisser/refusent Access](#)

[Installation de Répertoire actif](#)

[Configuration ASA](#)

[Scénario 3 : Dynamic Access Policies pour de plusieurs attributs de memberOf](#)

[Configuration ASA](#)

[Annexe B – Configuration ASA CLI](#)

[Annexe dépannage c](#)

[Dépannage de l'AAA et du LDAP](#)

[Exemple 1 : Connexion permise avec le mappage correct d'attribut](#)

[Exemple 2 : Connexion permise avec le mappage SIG-configuré d'attribut de Cisco](#)

[Dépannage de DAP](#)

[Exemple 1 : Connexion permise avec DAP](#)

[Exemple 2 : Connexion refusée avec DAP](#)

[Dépannage de l'autorité de certification/OCSP](#)

[Annexe D – Vérifiez les objets de LDAP dans le MS](#)

[Visionneuse de LDAP](#)

[Éditeur d'interface de services d'annuaire actifs](#)

[Annexe E](#)

[Informations connexes](#)

## **Introduction**

Ce document fournit une configuration d'échantillon sur l'appliance de sécurité adaptable Cisco (ASA) pour l'Accès à distance d'AnyConnect VPN pour le support de MAC en carte d'accès commune (CAC) pour l'authentification.

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

La configuration de ce guide utilise le serveur de Microsoft AD/LDAP. Ce document couvre également la fonctionnalité avancée telle qu'OCSP, des cartes d'attribut de LDAP et l'accès dynamique maintient l'ordre (DAP).

## **Conditions préalables**

### **Conditions requises**

Une compréhension de base de Cisco ASA, de client de Cisco AnyConnect, de Microsoft AD/LDAP et d'Infrastructure à clés publiques (PKI) est salutaire dans la compréhension de l'installation complète. La connaissance de l'adhésion à des associations d'AD, les propriétés d'utilisateur aussi bien que les objets de LDAP aident dans la corrélation du 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 :

- L'appliance de sécurité adaptable de gamme Cisco 5500 (ASA) cette exécute la version de logiciel 8.0(x) et plus tard
- Version 6.x du Cisco Adaptive Security Device Manager (ASDM) pour ASA 8.x
- Cisco AnyConnect VPN Client 2.2 avec le support de MAC

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

## [Conventions](#)

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

## [Configuration de Cisco ASA](#)

Cette section couvre la configuration de Cisco ASA par l'intermédiaire de l'ASDM. Il couvre les étapes nécessaires afin de déployer un tunnel d'Accès à distance VPN par une connexion SSL AnyConnect. Le certificat CAC est utilisé pour l'authentification et l'attribut du nom principal d'utilisateur (UPN) dans le certificat est rempli dans le répertoire actif pour l'autorisation.

## [Considérations de déploiement](#)

- Ce guide ne couvre pas des configurations de base telles que des interfaces, des DN, NTP, routage, accès au périphérique, accès ASDM et ainsi de suite. On le suppose que l'opérateur réseau est au courant de ces configurations. Référez-vous au pour en savoir plus [multifonction de dispositifs de sécurité](#).
- Les sections mises en valeur en ROUGE sont des configurations obligatoires requises pour l'accès VPN de base. Par exemple, un tunnel VPN peut être installé avec la carte CAC sans faire des contrôles OCSP, des mappages de LDAP et des contrôles de la stratégie d'accès dynamique (DAP). Les mandats vérifier OCSP DoD mais le tunnel fonctionne sans OCSP configuré.
- Les sections mises en valeur dans le BLEU sont une fonctionnalité avancée qui peut être incluse pour ajouter plus de Sécurité à la conception.
- ASDM et AnyConnect/SSL VPN ne peuvent pas utiliser les mêmes ports sur la même interface. Il est recommandé pour changer les ports sur un ou l'autre pour accéder. Par exemple, utilisez le port 445 pour l'ASDM et laissez 443 pour AC/SSL VPN. L'accès URL ASDM a changé dans 8.x. <ip\_address> de https:// d'utilisation : <port>/admin.html.
- L'image ASA exigée est au moins 8.0.2.19 et ASDM 6.0.2.
- AnyConnect/CAC est pris en charge avec le vista.
- Voir l'[annexe A](#) pour des exemples de mappage de stratégie de LDAP et d'accès dynamique pour l'application supplémentaire de stratégie.
- Voir l'[annexe D](#) sur la façon dont vérifier des objets de LDAP dans le MS.
- Voir les informations relatives pour des ports d'une liste des applications pour la configuration de Pare-feu.

## [Authentification, autorisation, configuration de comptabilité](#)

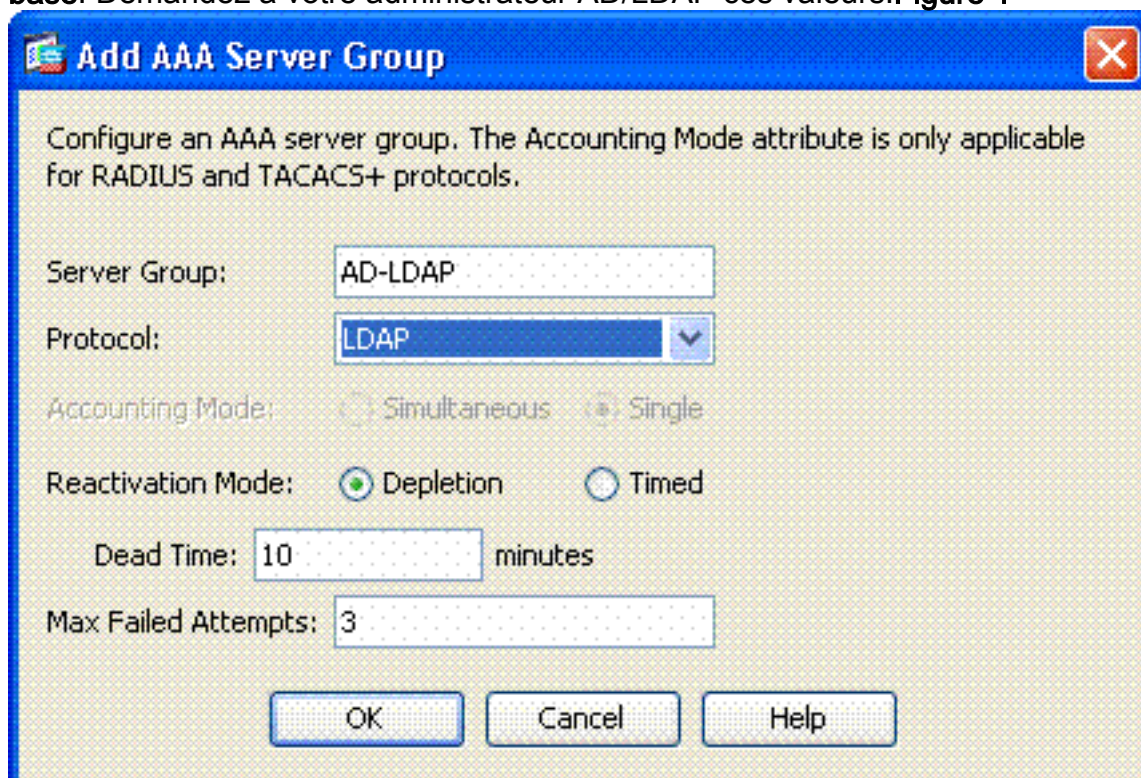
## (d'AAA)

Vous êtes authentifié avec l'utilisation du certificat dans leur carte d'accès commune (CAC) par le serveur de l'autorité de DISACertificate (CA) ou le serveur CA de leur propre organisation. Le certificat doit être valide pour l'Accès à distance au réseau. En plus de l'authentification, vous devez également être autorisé à utiliser un objet de Microsoft Active Directory ou de Protocole LDAP (Lightweight Directory Access Protocol). Le Ministère américain de la Défense (DoD) a besoin de l'utilisation de l'attribut du nom principal d'utilisateur (UPN) pour l'autorisation, qui fait partie de la section alternative soumise du nom (SAN) du certificat. L'UPN ou l'EDI/PI doit être dans ce format, 1234567890@mil. Ces configurations affichent comment configurer le serveur d'AAA dans l'ASA avec un serveur LDAP pour l'autorisation. Voir l'[annexe A](#) pour la configuration supplémentaire avec la cartographie d'objet de LDAP.

### Configurez le serveur LDAP

Procédez comme suit :

1. Choisissez l'**Accès à distance VPN > AAA installé > Groupe de serveurs AAA**.
2. Dans la table de Groupes de serveurs AAA, cliquez sur Add **3**.
3. Écrivez le nom de groupe de serveurs et choisissez le **LDAP** dans la case d'option de protocole. Voir la figure 1.
4. Dans des serveurs dans la table de groupe sélectionné, cliquez sur Add. Assurez-vous que le serveur que vous avez créé est mis en valeur dans la table précédente.
5. Dans la fenêtre de serveur d'AAA d'éditer, terminez-vous ces étapes. Voir la figure 2.**Remarque:** Choisissez le **LDAP d'enable au-dessus de l'option SSL** si votre LDAP/AD est configuré pour ce type de connexion. Choisissez l'interface où le LDAP se trouve. Ce guide affiche à l'intérieur de l'interface. Saisissez l'adresse IP du serveur. Entrez dans le **port de serveur**. Le port par défaut de LDAP est 389. Choisissez le **type de serveur**. Écrivez le **DN de base**. Demandez à votre administrateur AD/LDAP ces valeurs. **Figure 1**



Sous l'option de portée, choisissez la réponse appropriée. Ce dépend du DN de base. Demandez

à votre administrateur AD/LDAP l'assistance. Dans l'attribut nommant, écrivez l'**userPrincipalName**. C'est l'attribut qui est utilisé pour l'autorisation d'utilisateur dans le serveur AD/LDAP. Dans le DN de procédure de connexion, écrivez le DN d'administrateur. **Remarque:** Vous avez visualiser de droites d'administration ou de droits pour/recherche la structure de LDAP qui inclut des objets utilisateurs et l'adhésion à des associations. Dans le mot de passe de connexion, entrez le mot de passe de l'administrateur. Laissez l'attribut de LDAP à **aucun**. **Figure 2**

**Add AAA Server**

Server Group: AD-LDAP

Interface Name: outside

Server Name or IP Address: 172.18.120.160

Timeout: 10 seconds

**LDAP Parameters**

Enable LDAP over SSL

Server Port: 389

Server Type: -- Detect Automatically/Use Generic Type --

Base DN: CN=Users,DC=gsgseclab,DC=org

Scope: One level beneath the Base DN

Naming Attribute(s): userPrincipalName

Login DN: lministrator,CN=Users,DC=gsgseclab,DC=org

Login Password: ●●●●●●●●

LDAP Attribute Map: -- None --

SASL MD5 authentication

SASL Kerberos authentication

Kerberos Server Group:

OK Cancel Help

**Remarque:**

Vous utilisez cette option plus tard la configuration d'ajouter l'autre objet AD/LDAP pour l'autorisation. Choisissez **CORRECT**.

6. Choisissez **CORRECT**.

## Gérez les Certificats

Il y a deux étapes afin d'installer des Certificats sur l'ASA. D'abord, installez les Certificats CA (autorité de certification de racine et de subalterne) a eu besoin. Deuxièmement, inscrivez-vous

l'ASA à une particularité CA et obtenez le certificat d'identité. Le PKI DoD utilise ces Certificats, racine CA2, racine de la classe 3, intermédiaire CA## que l'ASA est inscrite avec, certificat d'ID ASA et certificat OCSP. Mais, si vous choisissez de ne pas utiliser OCSP, le certificat OCSP n'a pas besoin d'être installé.

**Remarque:** Entrez en contact avec votre POC de Sécurité afin d'obtenir des certificats racine aussi bien que des instructions sur la façon dont s'inscrire pour un certificat d'identité pour un périphérique. Un certificat ssl devrait être suffisant pour l'ASA pour l'Accès à distance. Un double certificat SAN n'est pas exigé.

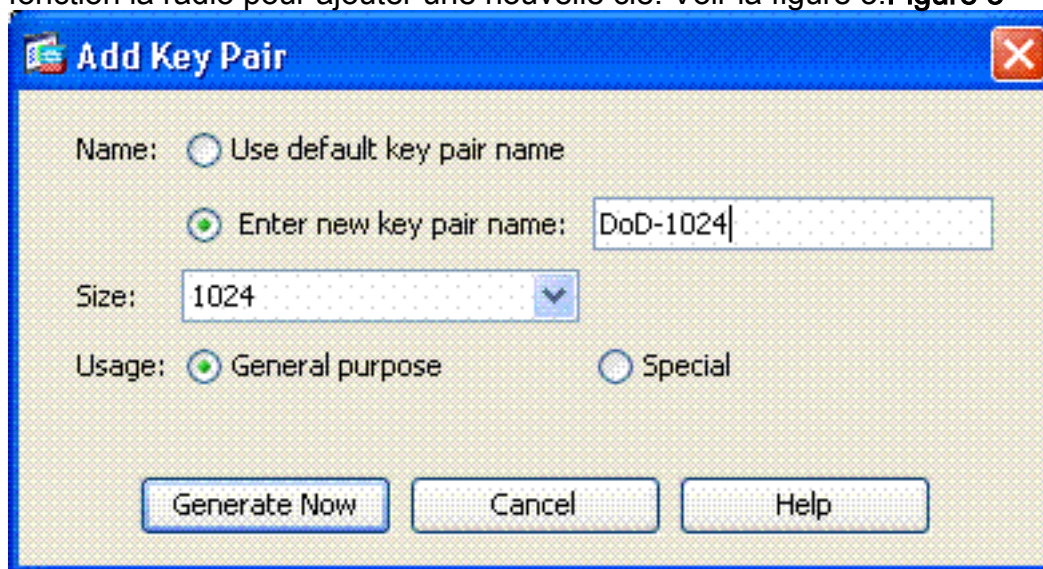
**Remarque:** L'ordinateur local doit également avoir la chaîne DoD CA installée. Les Certificats peuvent être visualisés dans la mémoire de certificat de Microsoft avec l'Internet Explorer. Le DoD a produit un fichier batch qui ajoute automatiquement tout les CAs à l'ordinateur. Demandez votre pour en savoir plus de POC de PKI.

**Remarque:** DoD CA2 et classe 3 s'enracinent aussi bien que l'intermédiaire d'ID et CA ASA qui a émis le CERT ASA devrait être le seul CAs requis pour l'authentification de l'utilisateur. Toutes les intermédiaires du courant CA tombent sous la chaîne de racine CA2 et de classe 3 et sont de confiance tant que les racines CA2 et de classe 3 sont ajoutées.

## Générez les clés

Procédez comme suit :

1. Choisissez l'**Accès à distance VPN > Gestion > certificat d'identité de certificat > ajoutent**.
2. Choisissez **ajoutent un nouveau certificat d'id** et puis **nouveau** par l'option de paire de clés.
3. Dans la fenêtre de paire de clés d'ajouter, écrivez un nom de clé, **DoD-1024**. Cliquez sur en fonction la radio pour ajouter une nouvelle clé. Voir la figure 3. **Figure 3**

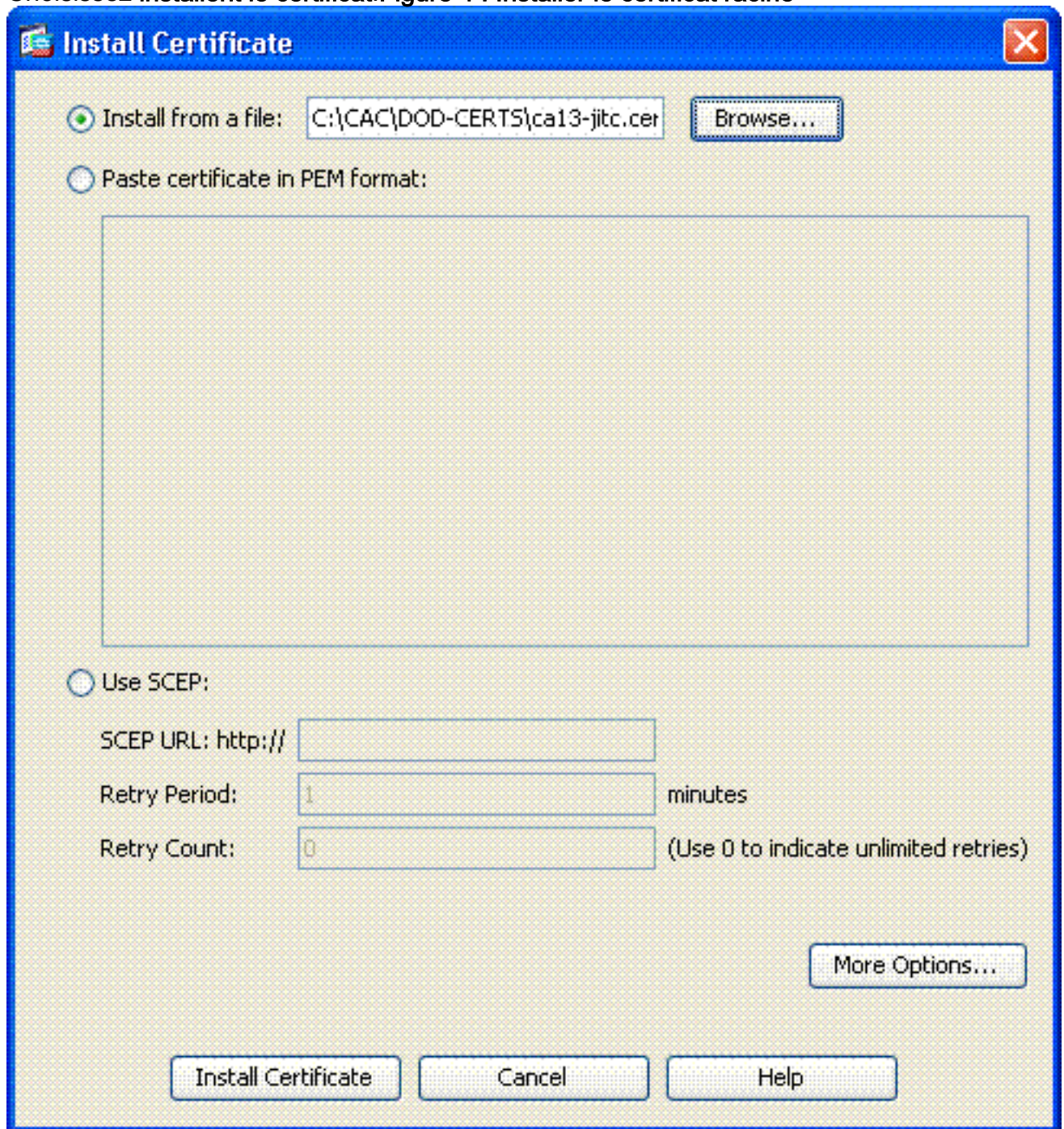


4. Choisissez la taille de la clé.
5. Gardez l'utilisation à l'**usage universel**.
6. Cliquez sur **Generate Now**. **Remarque:** La racine CA 2 DoD utilise une clé de 2048 bits. Une deuxième clé qui utilise une paire de clés de 2048 bits devrait être générée pour pouvoir utiliser ce CA se terminent le précédent au-dessus des étapes afin d'ajouter une deuxième clé.

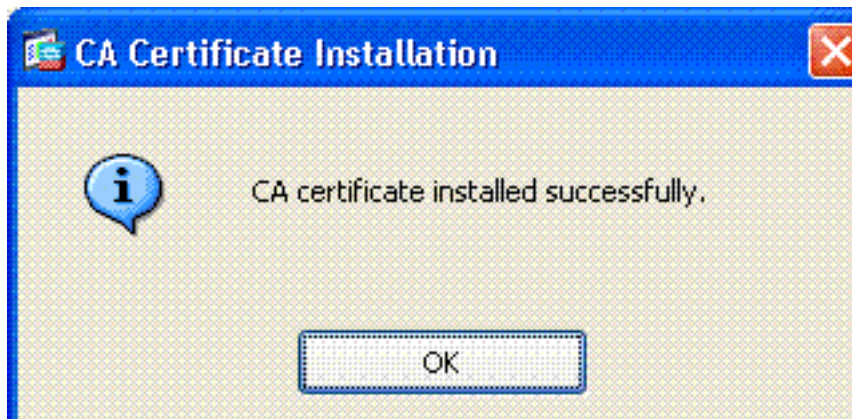
## Installez les Certificats CA de racine

Procédez comme suit :

1. Choisissez l'Accès à distance VPN > Gestion > certificat de CA de certificat > ajoutent.
2. Choisissez installent à partir du fichier et parcourant au certificat.
3. Choisissez installent le certificat.



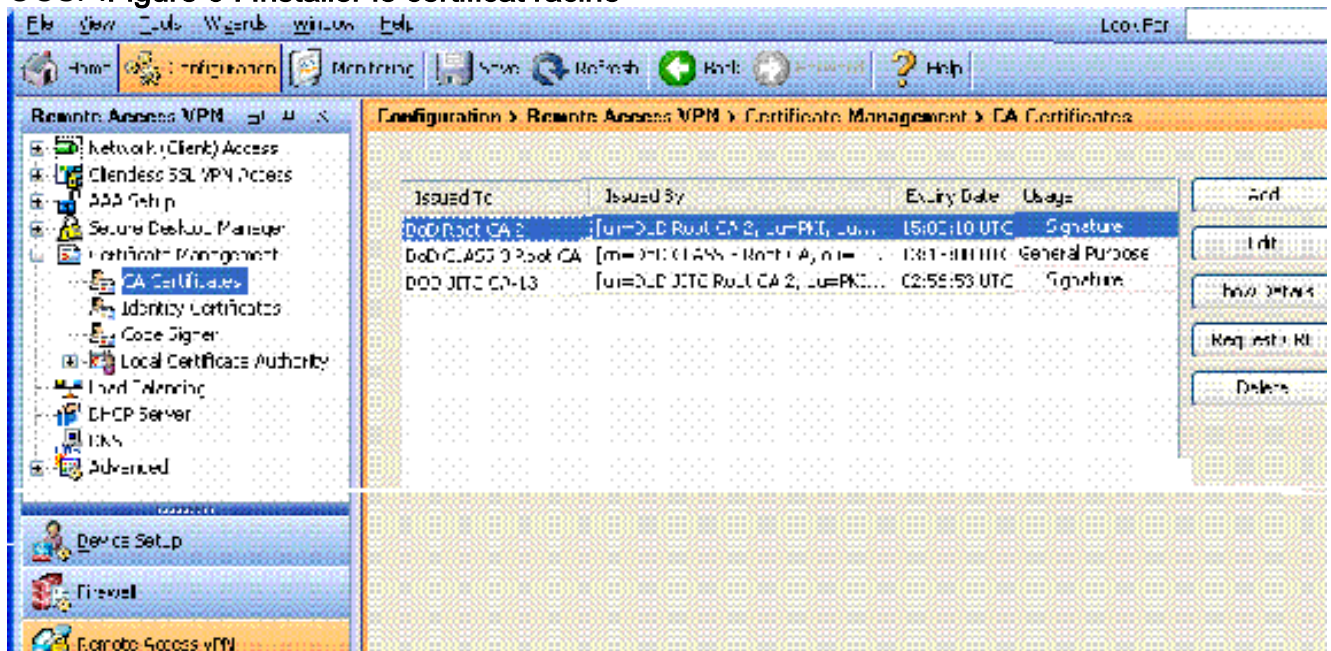
4. Cette fenêtre devrait apparaître. Voir la figure 5.



**Remarque:** Répétez les étapes 1

à 3 pour chaque certificat que vous voulez installer. Le PKI DoD exige un certificat pour chacune de ces derniers : Racine CA 2, racine de la classe 3, serveur d'intermédiaire CA##, d'ID ASA et OCSP. Le certificat OCSP n'est pas nécessaire si vous n'utilisez pas

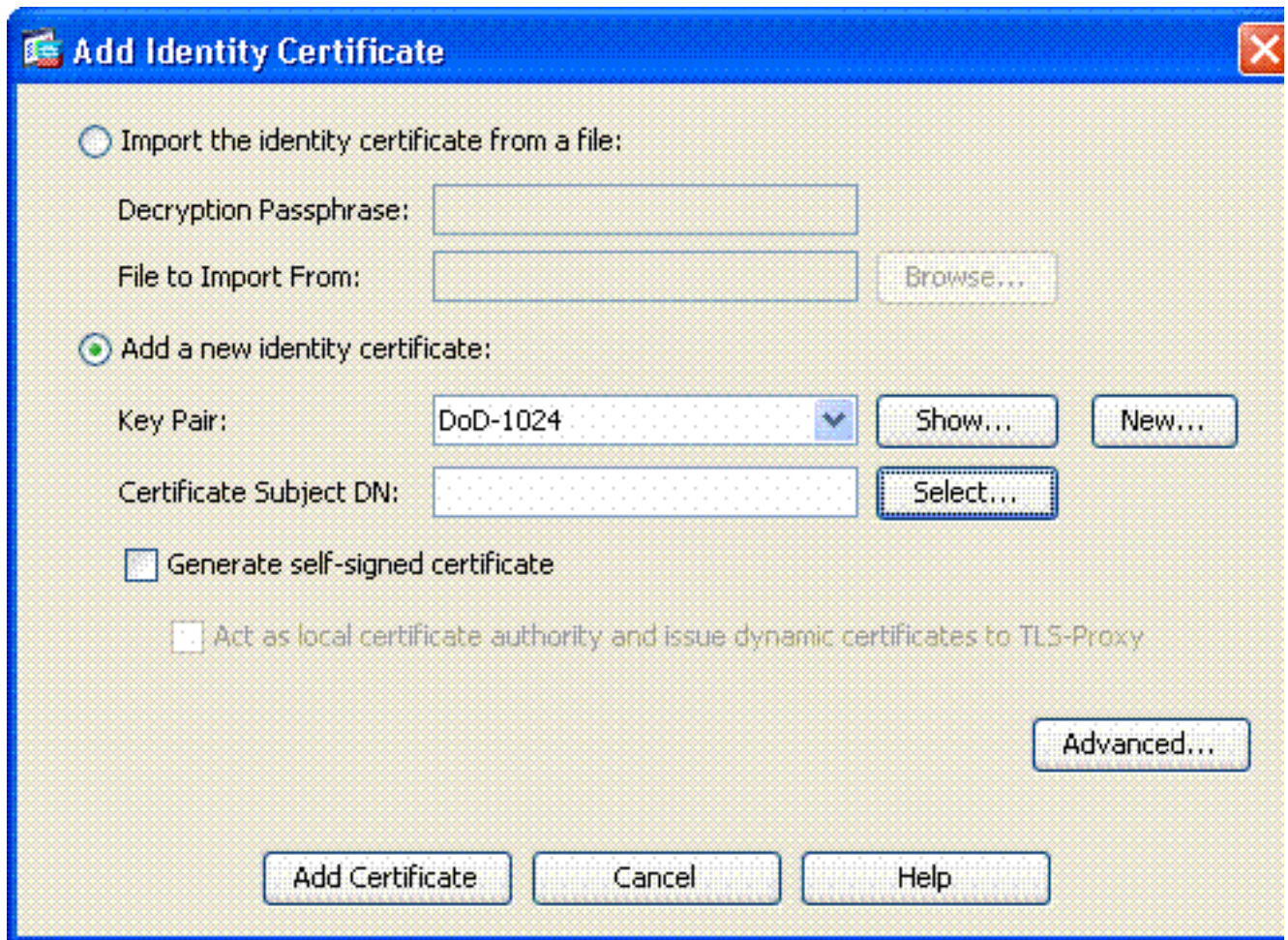
**OCSP.** **Figure 6 : Installer le certificat racine**



## Inscrivez-vous l'ASA et installez le certificat d'identité

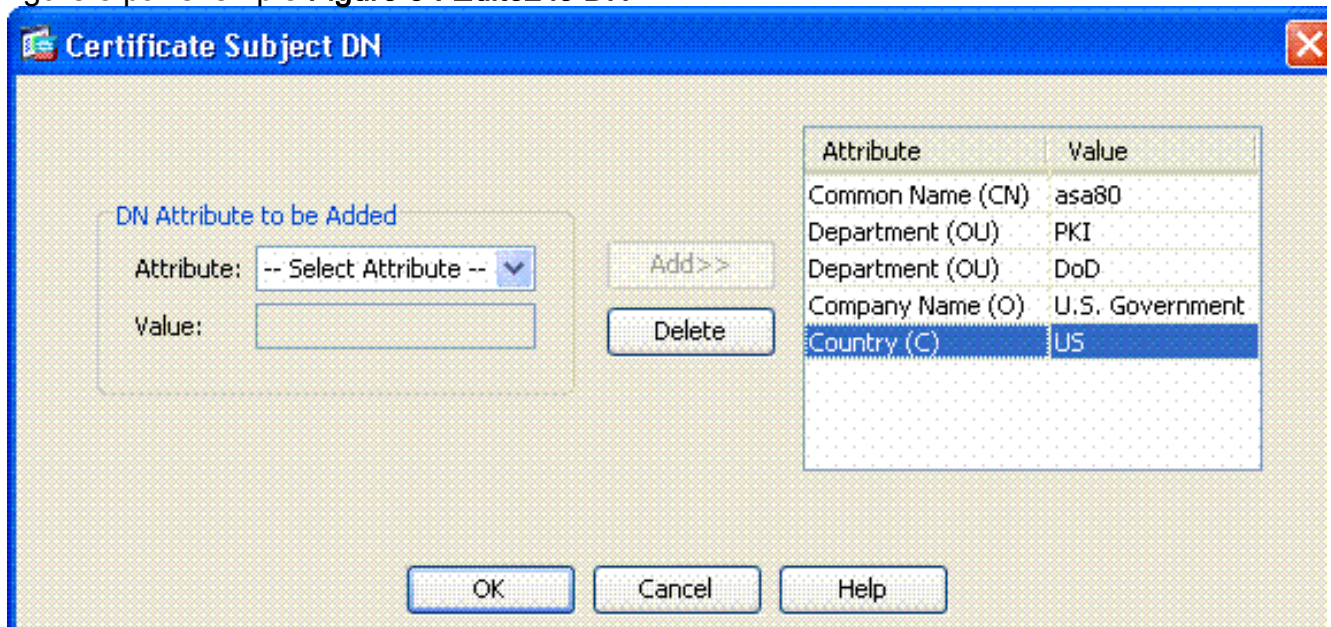
1. Choisissez l'Accès à distance VPN > Gestion > certificat d'identité de certificat > ajoutent.
2. Choisissez ajoutent un nouveau certificat d'id.
3. Choisissez la paire de clés DoD-1024. Voir la figure 7 **Figure 7 : Paramètres de certificat d'identité**





4. Allez dans la case de DN de sujet de certificat et cliquez sur **choisi**.

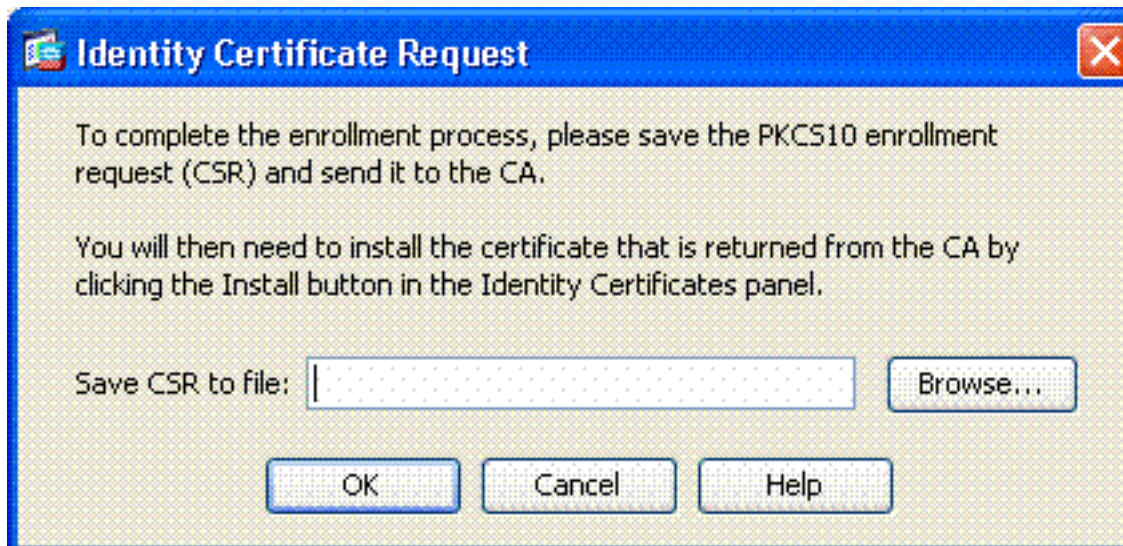
5. Dans la fenêtre de DN de sujet de certificat, écrivez les informations du périphérique. Voir la figure 8 par exemple. **Figure 8 : Éditez le DN**



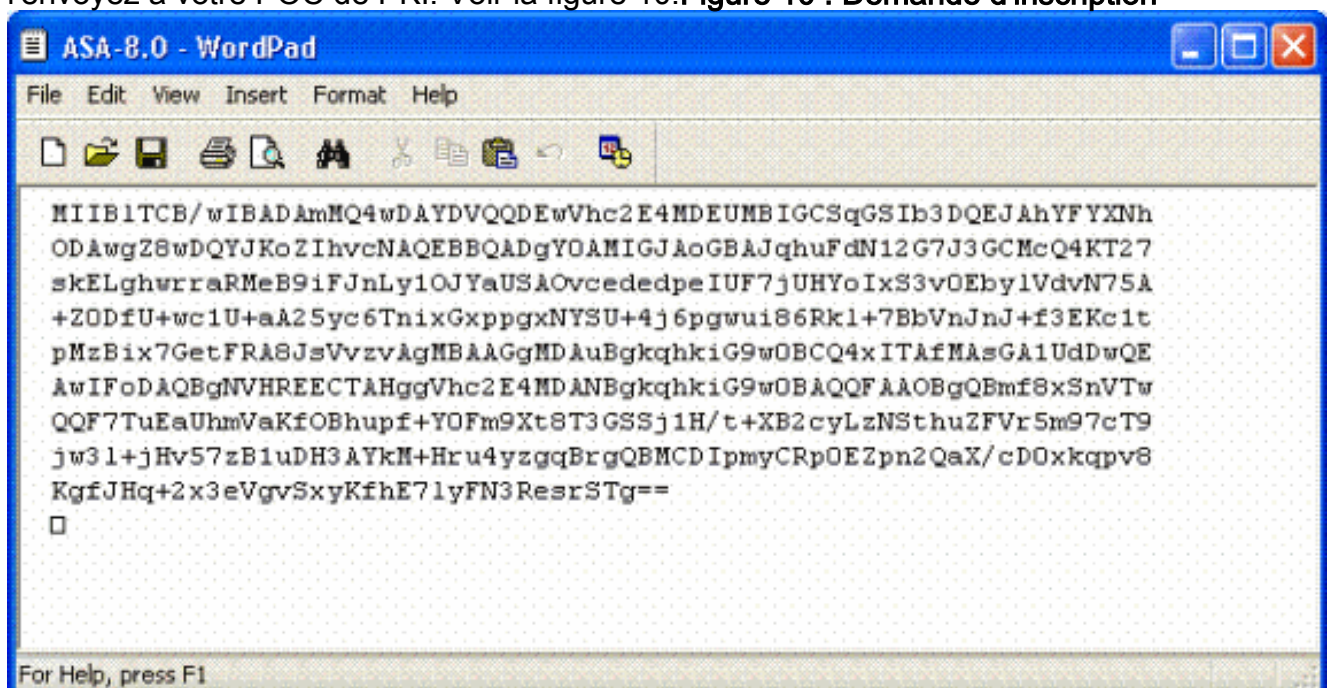
6. Choisissez **CORRECT**. **Remarque:** Assurez-vous que vous utilisez l'adresse Internet du périphérique qui est configuré dans votre système quand vous ajoutez le DN soumis. Le POC de PKI peut t'indiquer les champs obligatoires exigés.

7. Choisissez **ajoutent le certificat**.

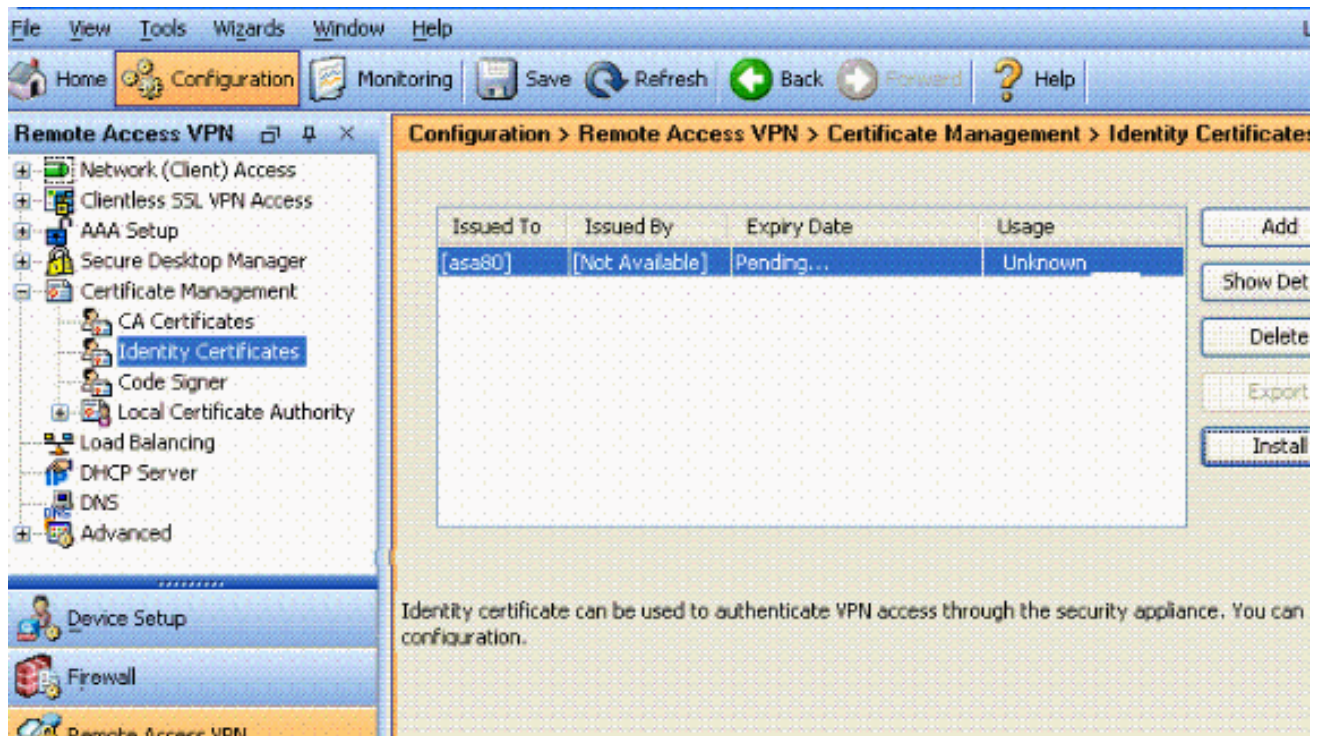
8. Le clic **parcourent** afin de sélectionner le répertoire où vous voulez sauvegarder la demande. Voir la figure 9. **Demande de certificat de figure 9**



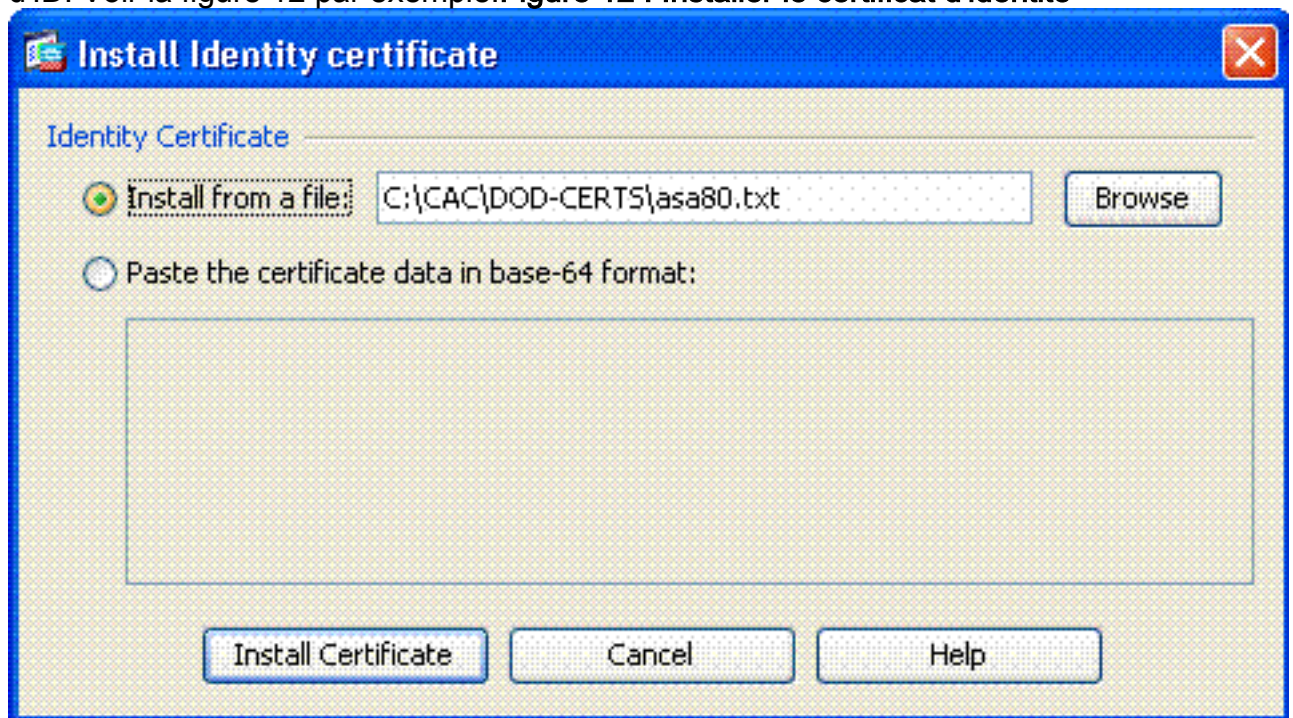
9. Ouvrez le fichier avec WordPad, copiez la demande sur la documentation appropriée et l'envoyez à votre POC de PKI. Voir la figure 10. **Figure 10 : Demande d'inscription**



10. Une fois que vous avez reçu le certificat de l'administrateur CA, choisissez l'**Accès à distance Gestion VPN > de certificat > certificat d'ID > installer**. Voir la figure 11. **Figure 11 : Importer le certificat d'identité**



11. Dans la fenêtre de certificat d'installer, parcourez au **certificat de CERT** et de choose **Install d'ID**. Voir la figure 12 par exemple. **Figure 12 : Installer le certificat d'identité**



**Remarque:** Il est recommandé pour exporter le point de confiance de certificat d'ID dans l'ordewr pour épargner le certificat et les paires de clés délivrés. Ceci permet à l'administrateur ASA pour importer le certificat et les paires de clés à une nouvelle ASA en cas de RMA ou de défaillance matérielle. Référez-vous à [exporter et à importer le](#) pour en savoir plus de [points de confiance](#). **Remarque: SAUVEGARDE** de clic afin de sauvegarder la configuration dans la mémoire flash.

## [Configuration du VPN d'AnyConnect](#)

Il y a deux options afin de configurer les paramètres VPN dans l'ASDM. Le premier choix est d'utiliser l'assistant de VPN SSL. C'est un outil facile à l'utiliser pour les utilisateurs qui sont

nouveaux à la configuration du 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 y a deux méthodes pour obtenir le client à C.A. à l'utilisateur :

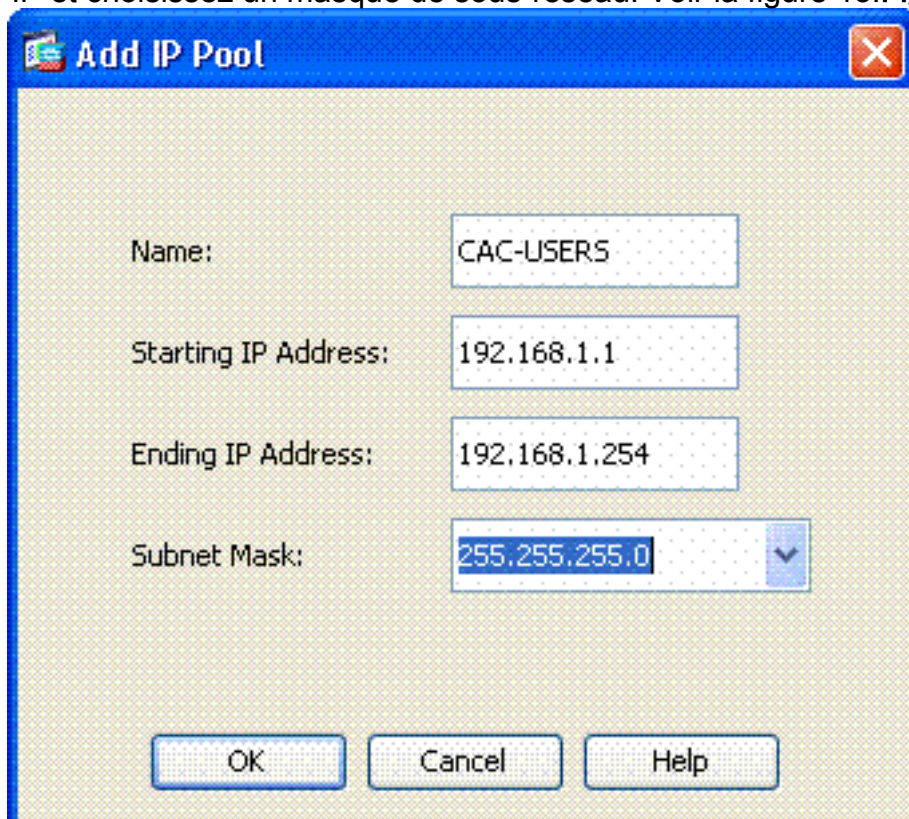
1. Vous pouvez télécharger le client du site Web Cisco et l'installer sur leur ordinateur.
2. L'utilisateur peut accéder à l'ASA par l'intermédiaire d'un navigateur Web et le client peut être téléchargé.

**Remarque:** Par exemple, <https://asa.test.com>. Ce guide utilise la deuxième méthode. Une fois que le client à C.A. est installé sur la machine cliente de manière permanente, vous lancez juste le client à C.A. de l'application.

## Créez un groupe d'adresse IP

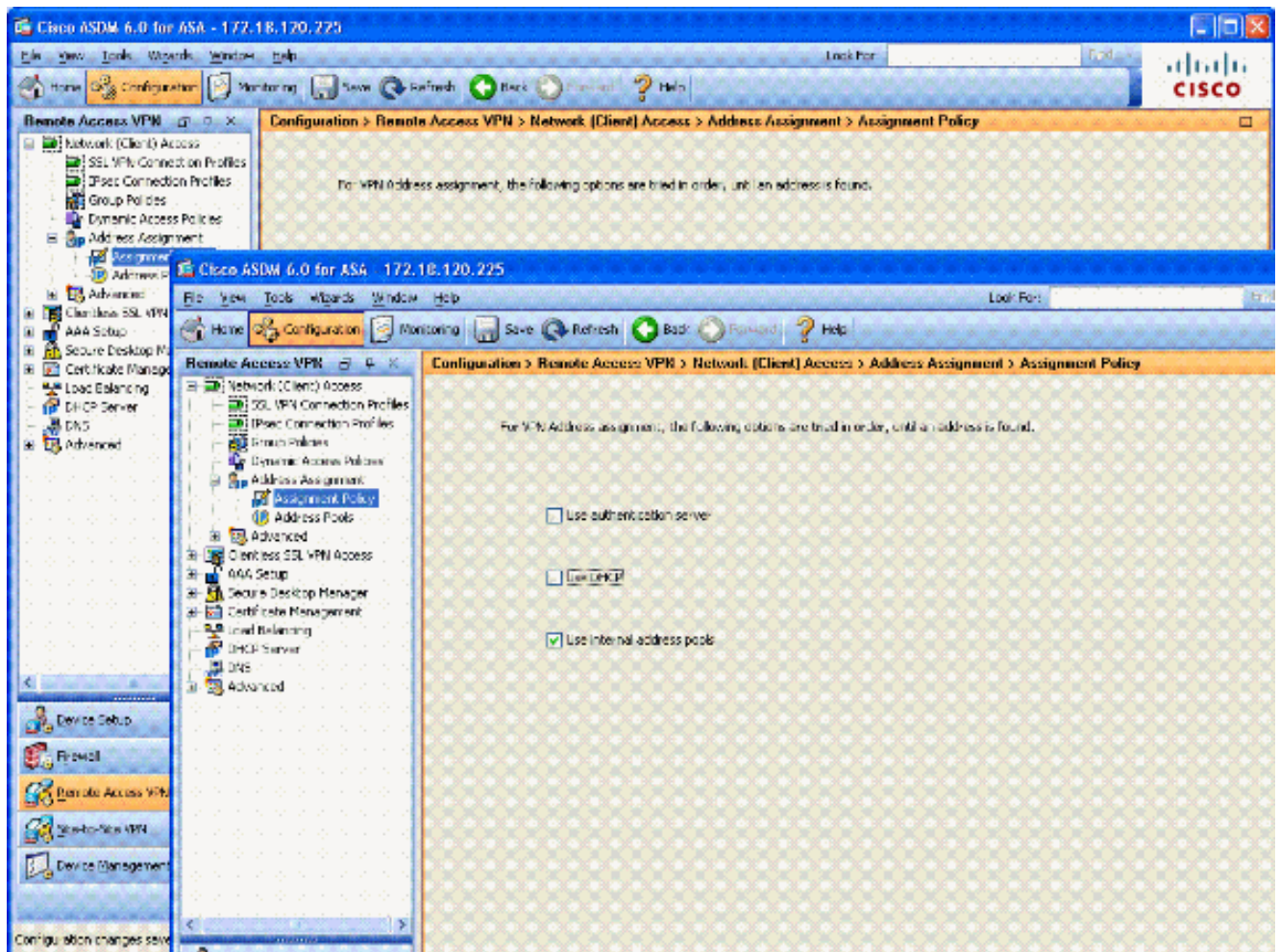
C'est facultatif si vous utilisez une autre méthode telle que le DHCP.

1. Choisissez l'**Accès à distance VPN > réseau (client) Access > affectation d'adresses > pools d'adresses**.
2. Cliquez sur **Add**.
3. Dans la fenêtre de pool d'IP d'ajouter, écrivez le nom du pool d'IP, commençant et finissant l'adresse IP et choisissez un masque de sous-réseau. Voir la figure 13. **Figure 13 : Ajouter le**



pool d'IP

4. Choisissez **correct**.
5. Choisissez l'**Accès à distance VPN > réseau (client) Access > stratégie d'affectation d'adresses > d'affectation**.
6. Sélectionnez la méthode appropriée d'affectation d'adresse IP. Ce guide utilise les groupes d'adresse interne. Voir la figure 14. **Figure 14 : Méthode d'affectation d'adresse IP**



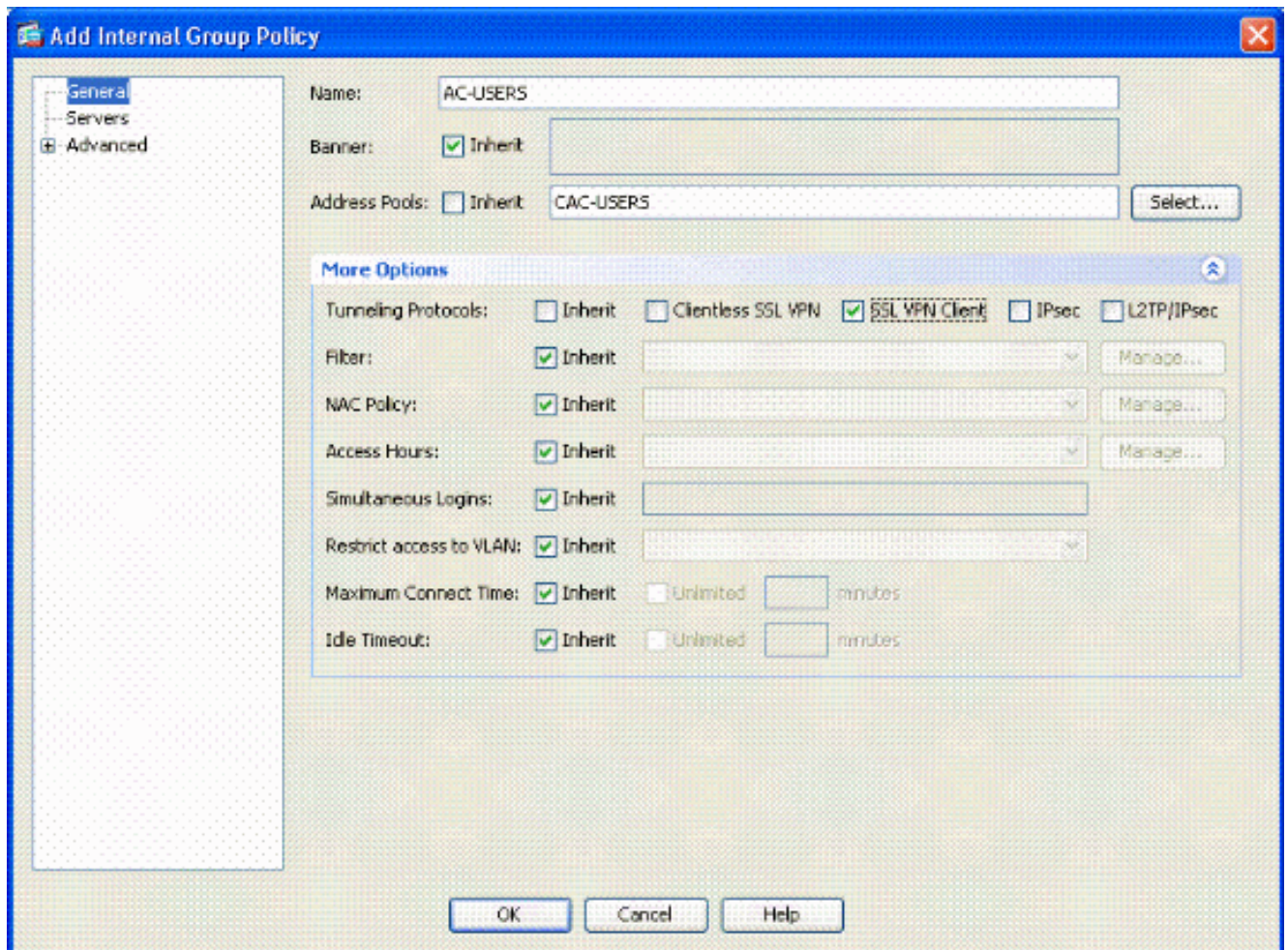
7. Cliquez sur **Apply**.

## [Créez le groupe et la stratégie de groupe de tunnel](#)

### Stratégie de groupe

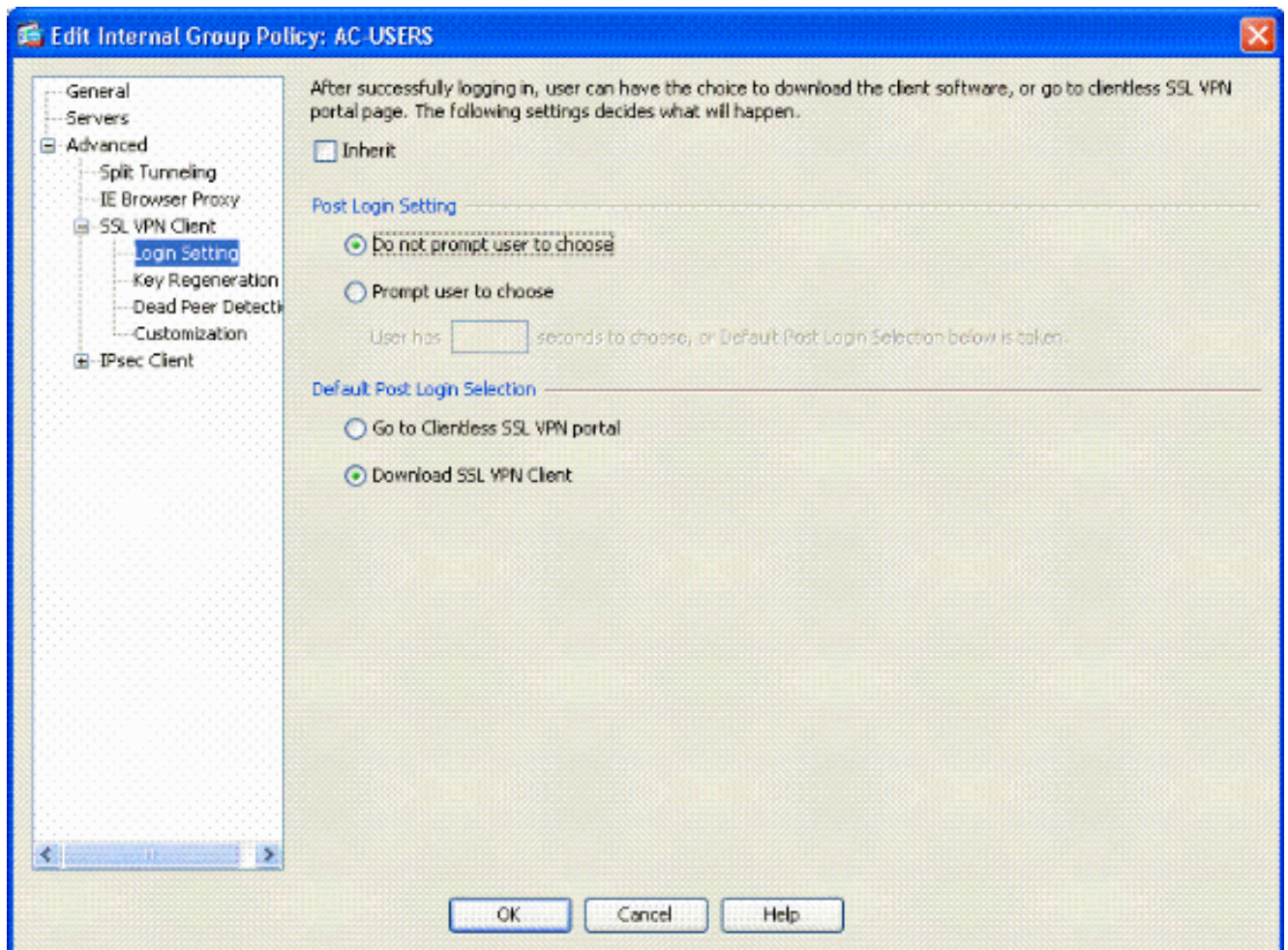
**Remarque:** Si vous ne voulez pas créer une nouvelle stratégie, vous pouvez utiliser la stratégie établie par défaut de groupe d'initiés.

1. Choisissez l'**Accès à distance VPN -> réseau (client) Access -> des stratégies de groupe**.
2. Cliquez sur Add et choisissez la **stratégie de groupe interne**.
3. Dans la fenêtre d'Add Internal Group Policy, écrivez le nom pour la stratégie de groupe dans la zone de texte de nom. Voir la figure 15. **Figure 15 : Ajouter la stratégie de groupe interne**



Dans l'onglet Général, choisissez le **client de VPN SSL** dans l'option de **protocoles de Tunnellisation**, à moins que vous utilisiez d'autres protocoles tels que le SSL sans client. Dans les serveurs sectionnez, décochez la case d'**héritage** et écrivez l'adresse IP des DN et des serveurs WINS. Entrez dans la portée de DHCP si c'est approprié. Dans les serveurs sectionnez, désélectionnez la case d'**héritage** dans le domaine par défaut et écrivez le nom de domaine approprié. Dans l'onglet Général, désélectionnez la case d'**héritage** dans la section de pool d'adresses et ajoutez le pool d'adresses créé dans l'étape précédente. Si le youuse une autre méthode d'affectation d'adresse IP, partent de ceci pour hériter et apporter de la modification appropriée. Tous autres onglets de configuration sont laissés aux valeurs par défaut. **Remarque:** Il y a deux méthodes pour obtenir le client à C.A. aux utilisateurs finaux. Une méthode est d'aller à Cisco.com et de télécharger le client à C.A. La deuxième méthode est d'avoir le téléchargement ASA le client à l'utilisateur quand l'utilisateur essaye de se connecter. Cet exemple affiche la dernière méthode.

4. Ensuite, choisissez **avancé > des configurations de client > de procédure de connexion de VPN SSL**. Voir la figure 16. **Figure 16 : Ajouter la stratégie de groupe interne**

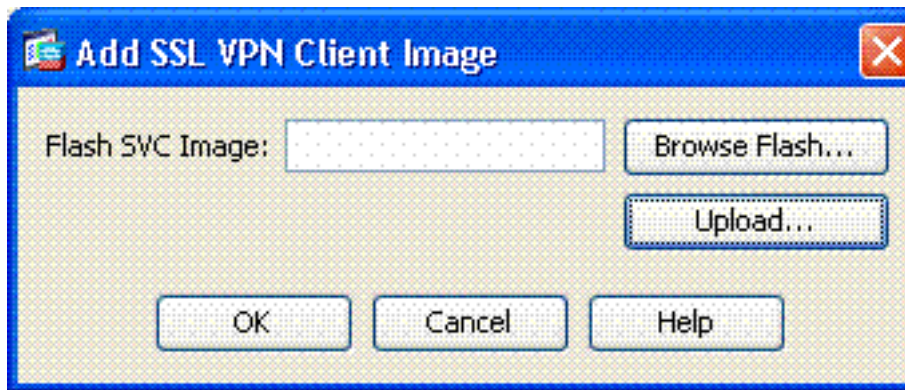


Désélectionnez la case à cocher d'**héritage**. Choisissez la configuration appropriée de procédure de connexion de courrier qui adapte votre environnement. Choisissez la sélection par défaut appropriée de procédure de connexion de courrier qui adapte votre environnement. Choisissez **CORRECT**.

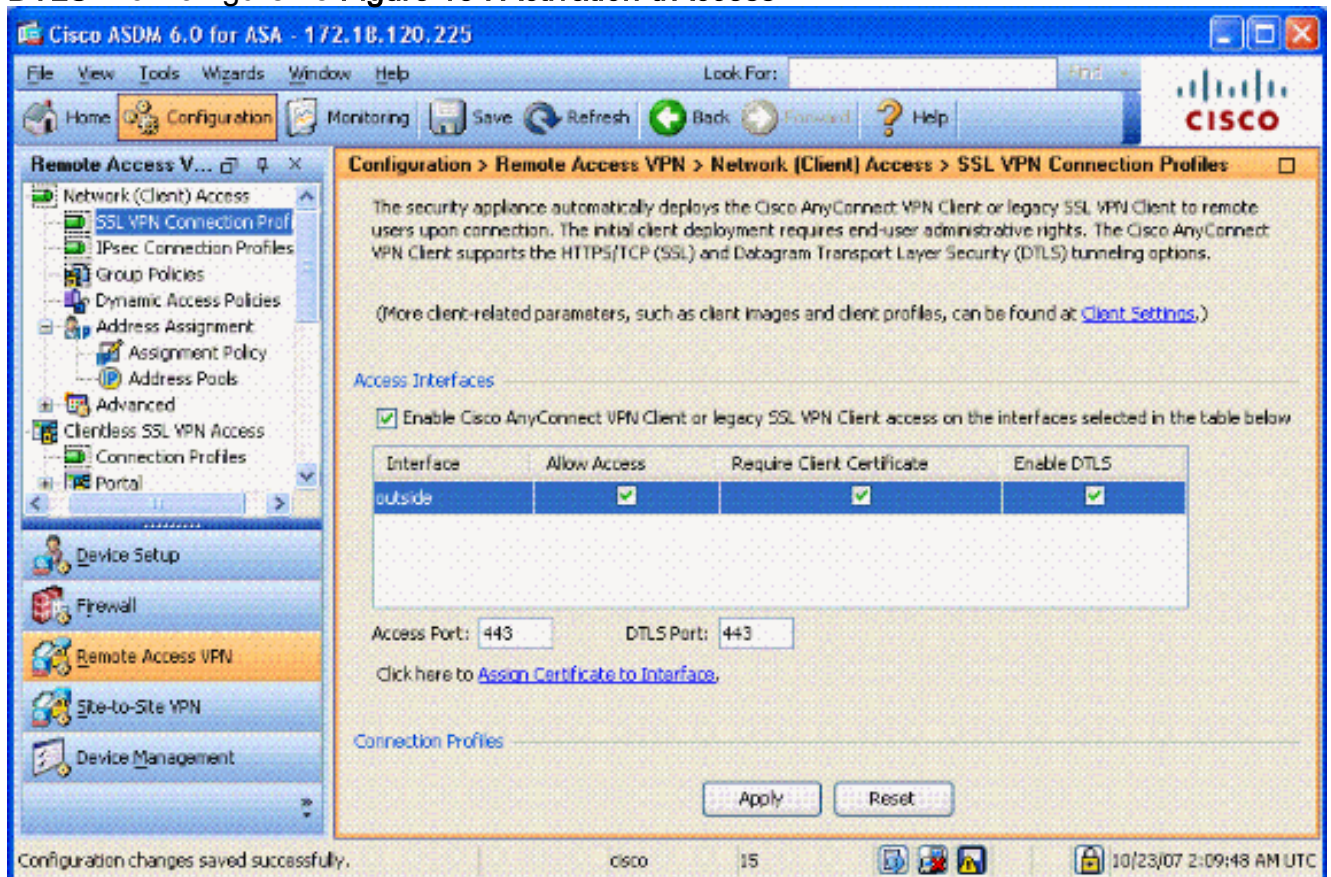
## Configurations d'interface de groupe et d'image de tunnel

**Remarque:** Si vous ne voulez pas créer un nouveau groupe, vous pouvez utiliser le groupe intégré par défaut.

1. Choisissez l'**Accès à distance VPN > réseau (client) Access > profil de connexion de VPN SSL**.
2. Choisissez **Enable le client de Cisco AnyConnect .....**
3. Une boîte de dialogue apparaît avec la question *vous voudrait indiquer une image de SVC ?*
4. Choisissez **oui**.
5. S'il y a déjà une image, choisissez l'image pour l'utiliser avec **Browse Flash**. Si l'image n'est pas disponible, choisissez le **téléchargement** et recherchez le fichier sur l'ordinateur local. Voir la figure 17. Les fichiers peuvent être téléchargés de Cisco.com ; il y a Windows, un MAC et un fichier de Linux. **Figure 17 : Ajoutez l'image de client de VPN SSL**

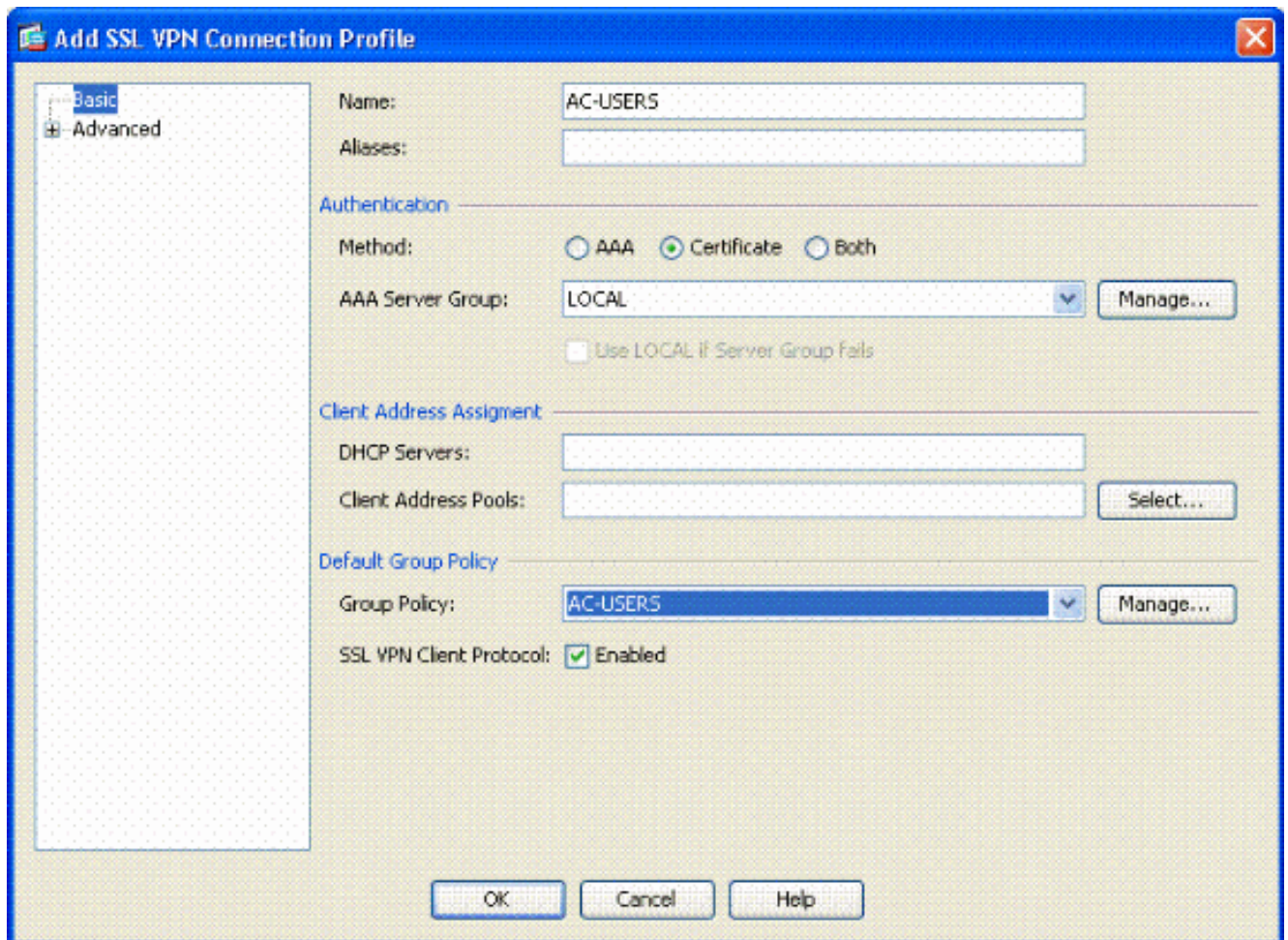


6. Le prochain enable permettent Access, exigent le CERT de client et activent sur option DTLS. Voir la figure 18. Figure 18 : Activation d'Access



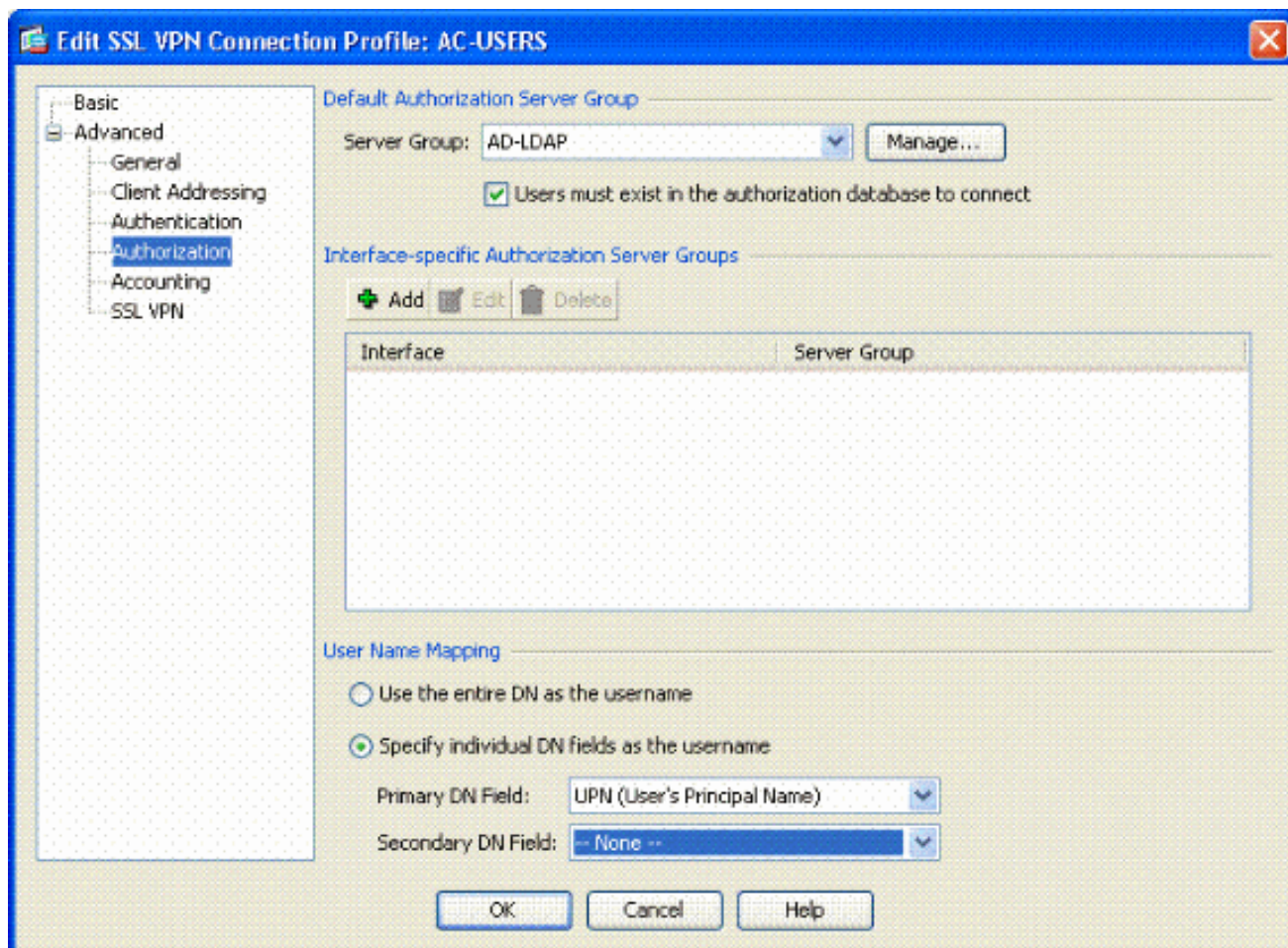
7. Cliquez sur **Apply**.
8. Ensuite, créez un profil de connexion/groupe de tunnel. Choisissez l'**Accès à distance VPN > réseau (client) Access > profil de connexion de VPN SSL**.
9. Dans la section de profils de connexion, cliquez sur Add. Figure 19 : Ajouter le profil de connexion





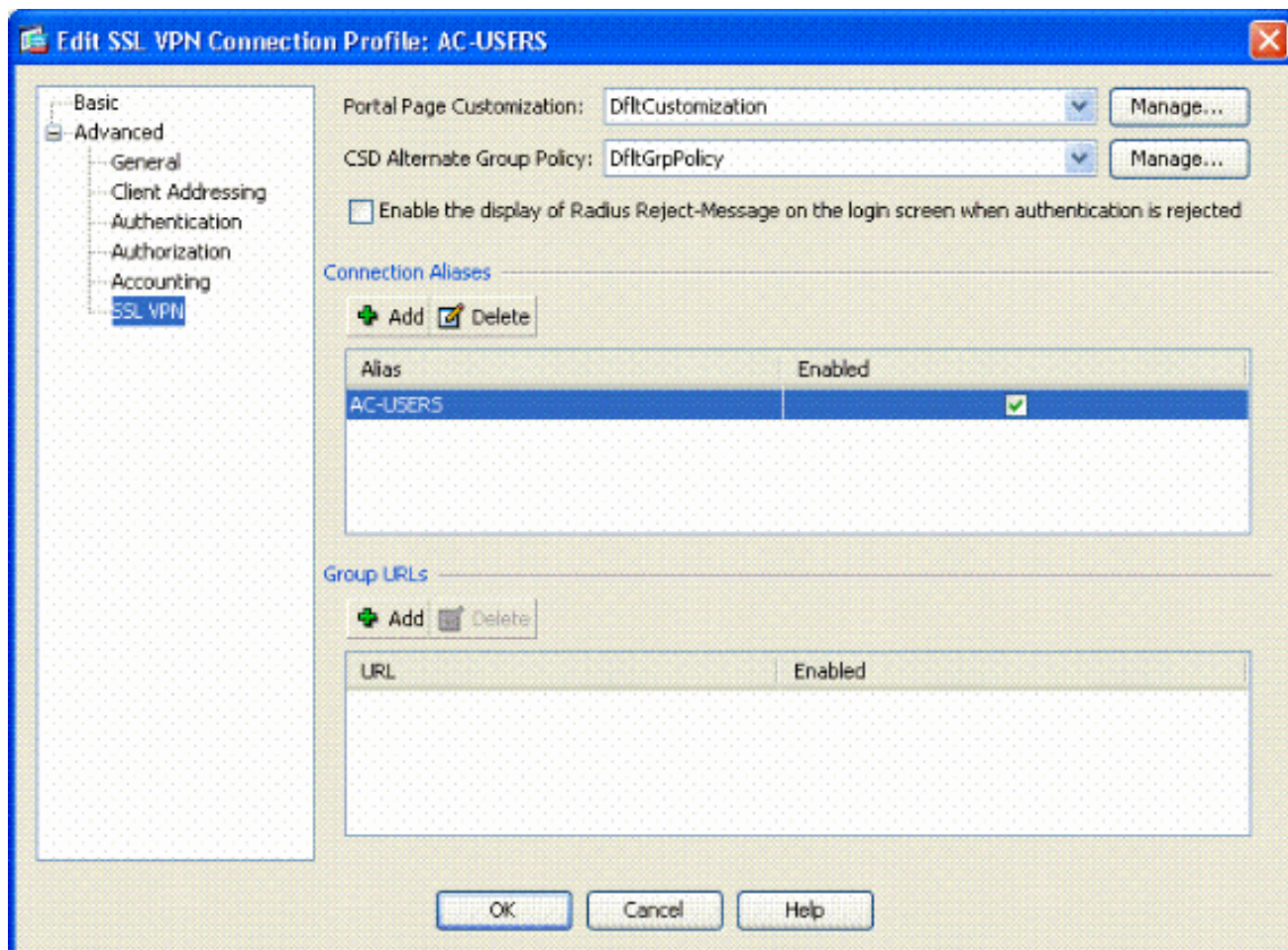
Nommez le groupe. Choisissez le **certificat** dans la méthode d'authentification. Choisissez la stratégie de groupe créée précédemment. Assurez-vous que le **client de VPN SSL** est activé. Laissez d'autres options en tant que par défaut.

10. Ensuite, choose **Advanced > autorisation**. Voir la figure 20 **Figure 20 : Autorisation**



Choisissez le groupe AD-LDAP précédemment créé. **Les utilisateurs de contrôle doivent exister....pour se connecter.** Dans les domaines de mappage, n'en choisissez UPN pour le primaire et **aucun** pour secondaire.

11. Choisissez la section de **VPN SSL** du menu.
12. Dans la section de pseudonymes de connexion, terminez-vous ces étapes : **Figure 21 : Pseudonymes de connexion**



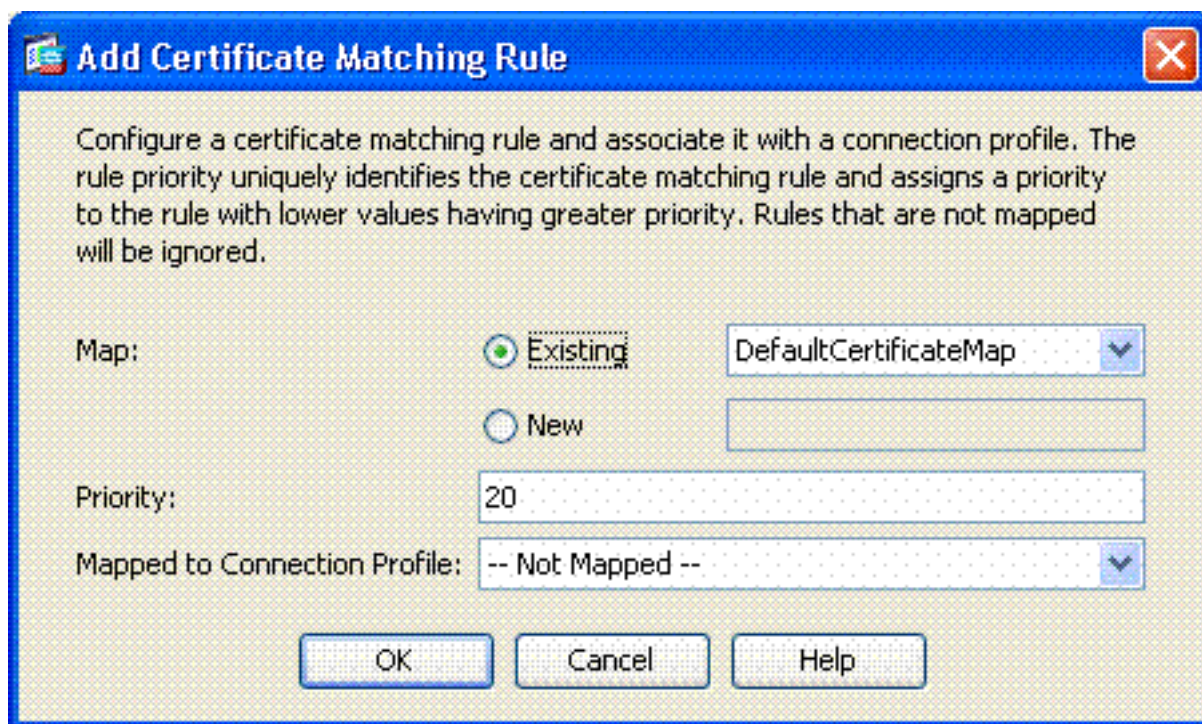
Choisissez **ajoutent**. Présentez le groupe alias que vous voulez utiliser. Assurez que qui a **activé** est vérifié. Voir la figure 21.

13. Cliquez sur **OK**.

**Remarque:** Sauvegarde de clic afin de sauvegarder la configuration dans la mémoire flash.

### Règles assorties de certificat (si OCSP sera utilisé)

1. Choisissez l'**Accès à distance VPN > a avancé > certificat aux cartes de profil de connexion de VPN SSL**. Voir la figure 22. Choisissez **ajoutent** dans le certificat à la section de cartes de profil de connexion. Vous pouvez maintenir la carte existante pendant que DefaultCertificateMap dans la section de carte ou créez un neuf si vous utilisez déjà des cartes de CERT pour IPsec. Gardez la priorité de règle. Sous le groupe tracé, congé As -- **Non tracé --**. Voir la figure 22. **Figure 22 : Ajouter la règle assortie de certificat**

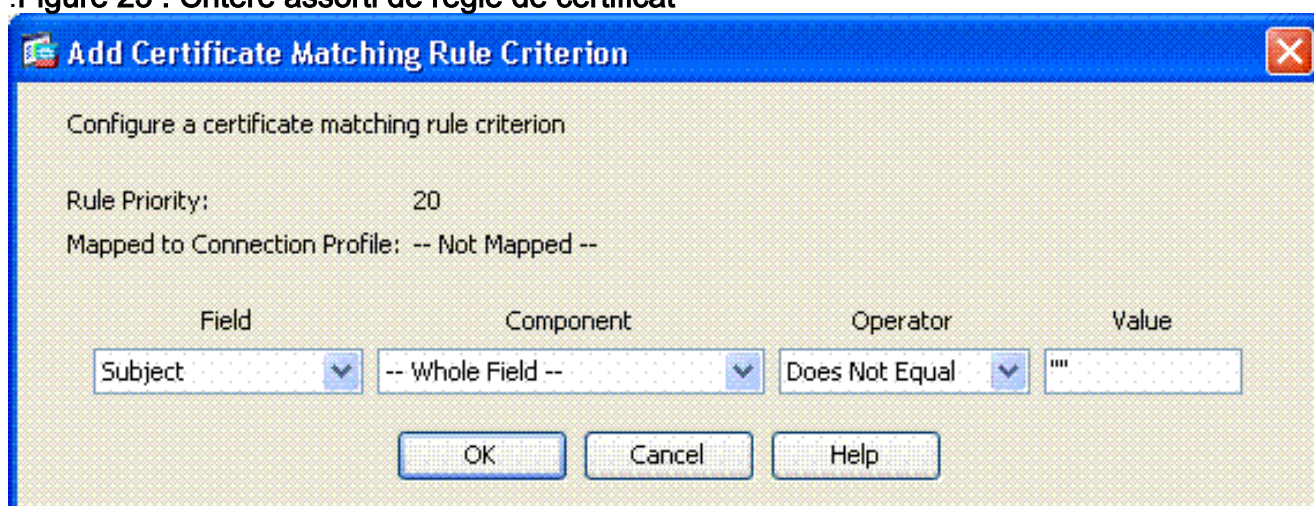


Cliquez

sur OK.

2. Cliquez sur Add sur la table inférieure.
3. Dans la fenêtre assortie de critère de règle de certificat d'ajouter, terminez-vous ces étapes

:Figure 23 : Critère assorti de règle de certificat



Gardez la colonne de champ pour soumettre. Gardez la colonne composante au champ entier. Changez l'opérateur que la colonne n'égal pas. Dans la colonne valeur, écrivez deux guillemets « ». Cliquez sur l'ok et appliquez. Voir la figure 23 par exemple.

## [Configurez OCSP](#)

La configuration d'un OCSP peut varier et dépend du constructeur de responder OCSP. Lisez le manuel du pour en savoir plus de vendeur.

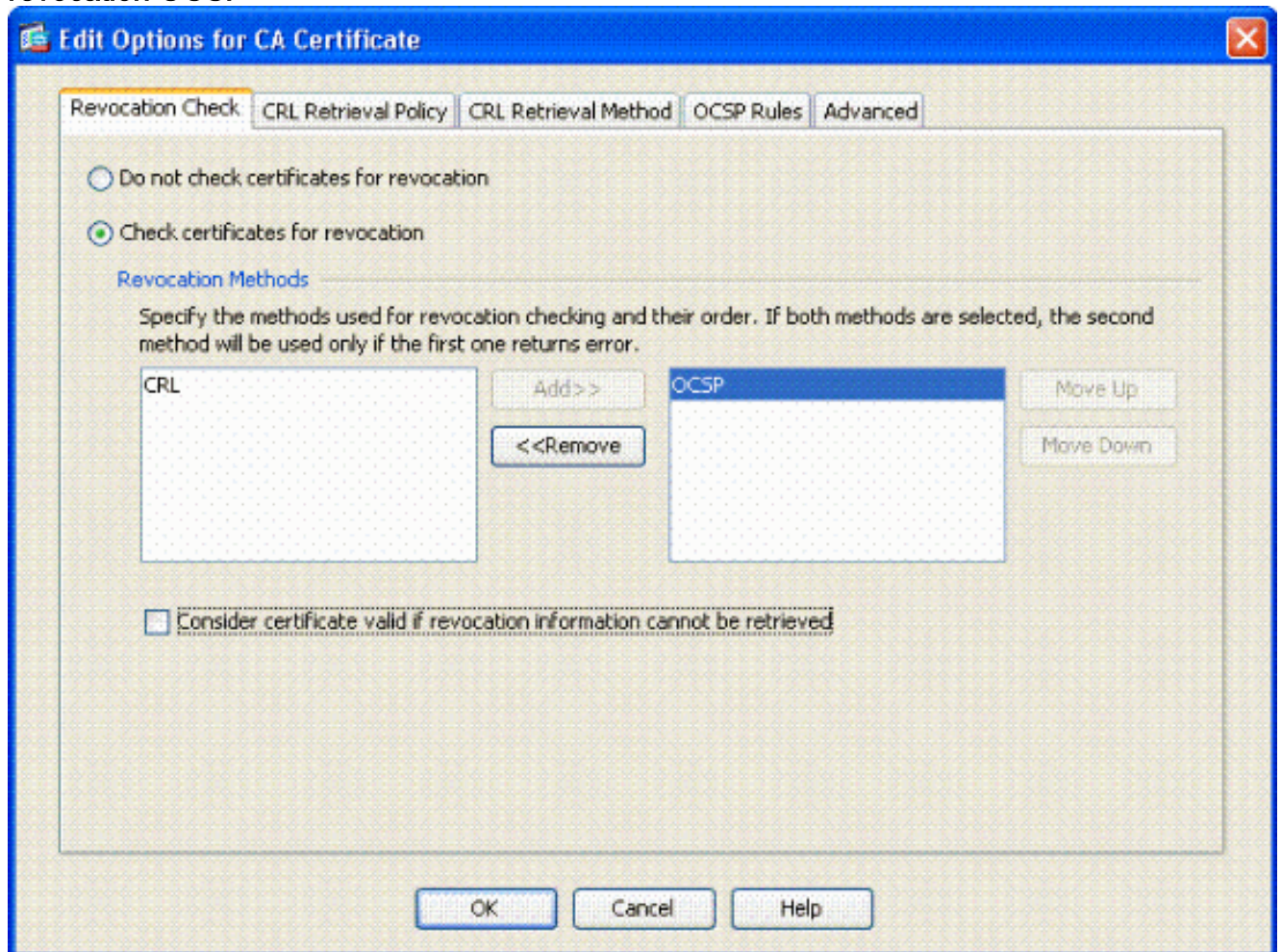
## [Configurez le certificat de responder OCSP](#)

1. Obtenez un certificat auto-généré du responder OCSP.
2. Remplissez les procédures mentionnées précédemment et installez un certificat pour le serveur OSCP. **Remarque:** Assurez-vous que ne vérifiez pas les Certificats pour la révocation

est sélectionné pour le point de confiance de certificat OCSP.

## Configurez le CA pour utiliser OCSP

1. Choisissez la **Gestion de certificat de l'Accès à distance VPN** > > **les Certificats CA**.
2. Mettez en valeur un OCSP afin de choisir un CA pour configurer pour utiliser OCSP.
3. Cliquez sur **Edit**.
4. Assurez-vous que le **certificat de contrôle pour la révocation** est vérifié.
5. Dans la révocation les méthodes sectionnent, ajoutent **OCSP**. Voir la [figure 24](#). **Contrôle de révocation OCSP**



6. Assurez **considèrent le certificat valide... ne peut pas être récupéré** est décoché si vous voulez suivre vérifier strict OCSP.

**Remarque:** Configurez/éditez tout le serveur CA qui utilise OCSP pour la révocation.

## Configurez les règles OCSP

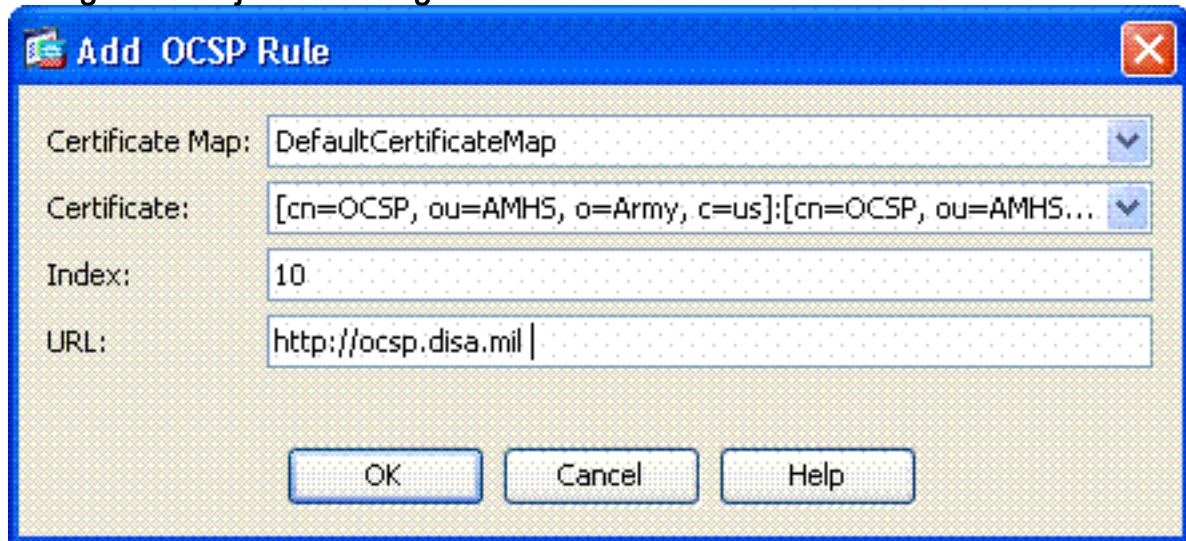
**Remarque:** Vérifiez qu'une stratégie assortie de groupe de certificat est créée et le responder OCSP est configuré avant que vous terminiez ces étapes.

**Remarque:** Dans des réalisations certain OCSP, l'enregistrement des DN A et PTR peut être nécessaire pour l'ASA. Ce contrôle est fait afin de vérifier que l'ASA est d'un site .mil.

1. Choisissez la **Gestion de certificat de l'Accès à distance VPN** > > **les Certificats CA 2**.
2. Mettez en valeur un OCSP afin de choisir un CA pour configurer pour utiliser OCSP.
3. Choisissez **éditent**.

4. Cliquez sur l'onglet de **règle OCSP**.
5. Cliquez sur **Add**.
6. Dans la fenêtre de règle de l'ajouter OCSP, terminez-vous ces étapes. Voir la figure 25.

**Figure 25 : Ajouter des règles OCSP**



Dans

l'option de carte de certificat, choisissez **DefaultCertificateMap** ou une carte créée précédemment. Dans l'option de certificat, choisissez le **responder OCSP**. Dans l'option sur indice, écrivez **10**. Dans l'option URL, entrez dans l'adresse IP ou l'adresse Internet du responder OCSP. Si vous utilisez l'adresse Internet, assurez-vous que le serveur DNS est configuré sur l'ASA. Cliquez sur **OK**. Cliquez sur **Apply**.

## [Configuration de client de Cisco AnyConnect](#)

Cette section couvre la configuration du Cisco AnyConnect VPN Client.

**Suppositions** — L'application de Cisco AnyConnect VPN Client et de middleware est déjà installée dans le PC d'hôte. L'or et l'ActivClient d'ActivCard ont été testés.

**Remarque:** Ce guide utilise la méthode groupe-URL pour le client initial à C.A. installent seulement. Une fois que le client à C.A. est installé, vous lancez l'application à C.A. juste comme le client d'IPsec.

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

**Remarque:** Le gestionnaire de lecteur de cartes pour le MAC OSX est déjà installé et compatible avec la version de système d'exploitation en cours que vous utilisez.

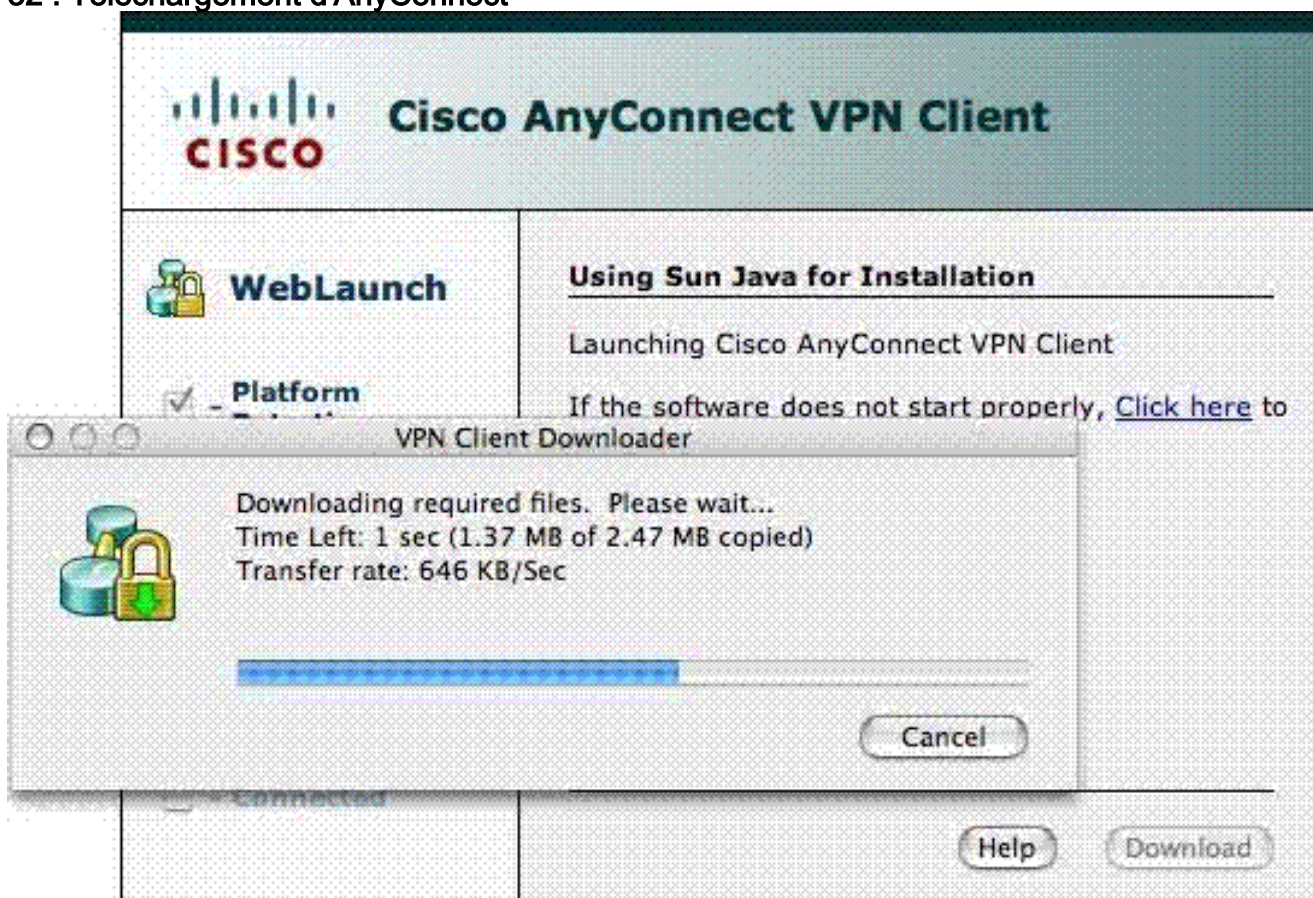
## [Téléchargeant le Cisco AnyConnect VPN Client – Mac OS X](#)

1. Lancez une session Web à l'ASA par le safari. L'adresse devrait être dans le format de https://Outside-Interface. Par exemple, https://172.18.120.225.
2. Une fenêtre contextuelle demande à vérifier le certificat de l'ASA. Cliquez sur **Continue**.
3. Une autre fenêtre contextuelle apparaît afin de déverrouiller le trousseau de clés CAC. Introduisez votre code pin. Voir la figure 31.

**Figure 31 : Écrivez le PIN**



4. Après que la page Web de VPN-service SSL paraisse, le clic **continuer**.
5. Après que vous déverrouillez le trousseau de clés, le navigateur vous incite si vous faites confiance au certificat de l'ASA. **Confiance de clic**.
6. Entrez le mot de passe root afin de déverrouiller le trousseau de clés pour établir la connexion sécurisée, et puis cliquez sur l'**ok**.
7. Choisissez le certificat pour l'utiliser pour l'authentification client, et puis cliquez sur l'**ok**.
8. Le navigateur demande alors la racine/mot de passe utilisateur afin de tenir compte de télécharger des clients d'AnyConnect.
9. Si authentifié, les débuts de client d'AnyConnect pour télécharger. Voir la figure 32. **Figure 32 : Téléchargement d'AnyConnect**



10. Après que l'application soit téléchargée, le navigateur vous incite à recevoir le certificat ASA. Le clic **reçoivent**.
11. La connexion est établie. **Figure 33: AnyConnect connectée**



## [Cisco AnyConnect VPN Client de début – Mac OS X](#)

Du détecteur — Applications > Cisco AnyConnect VPN Client

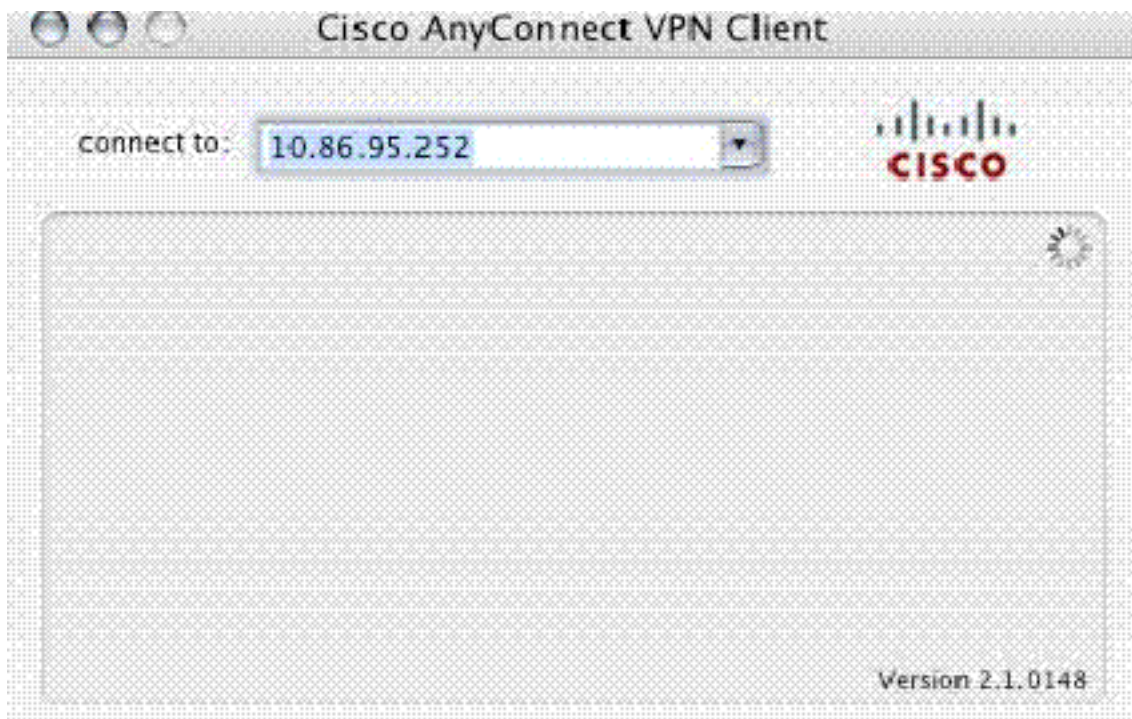
**Remarque:** Voir l'annexe E pour la configuration facultative de profil de client d'AnyConnect.

## [Nouvelle connexion](#)

La fenêtre à C.A. apparaît. Voir la figure 37.

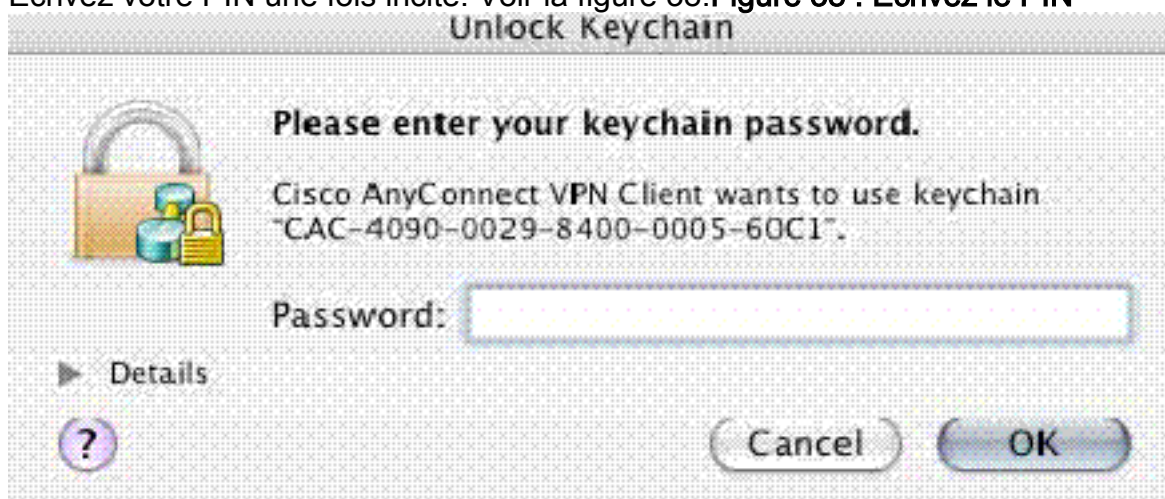
**Figure 37 :** Nouvelle connexion VPN





1. Choisissez l'hôte approprié si le courant alternatif n'essaye pas automatiquement la connexion.
2. Écrivez votre PIN une fois incité. Voir la figure 38.

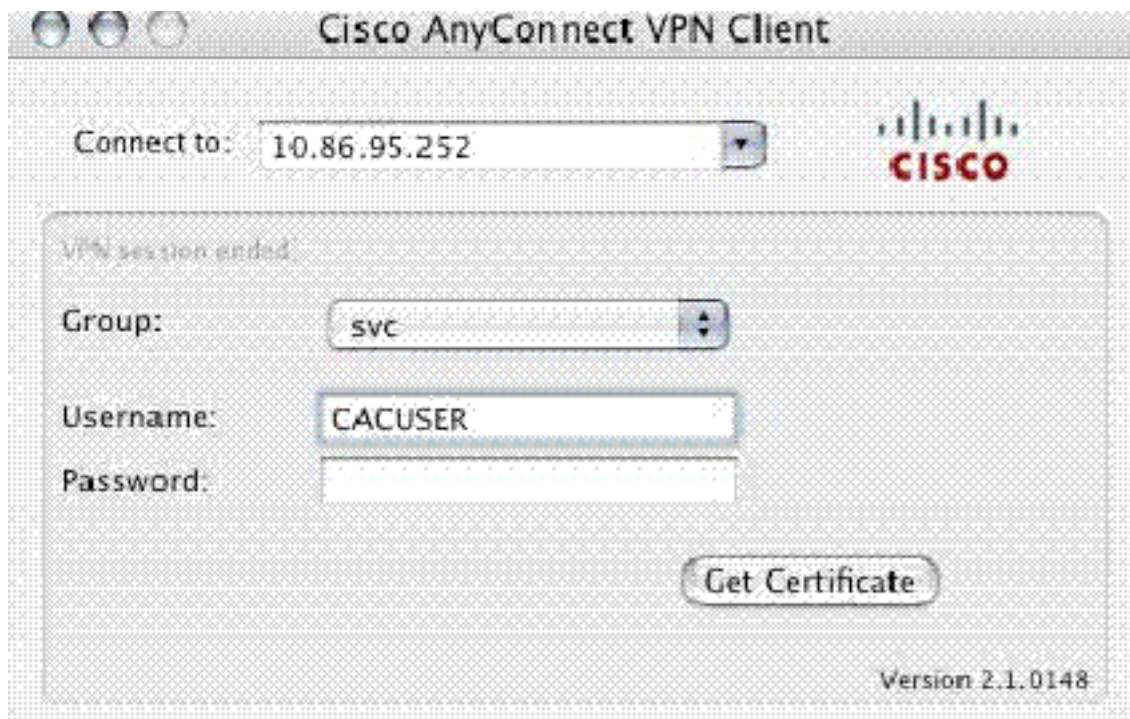
**Figure 38 : Écrivez le PIN**



## Accès à distance de début

1. Choisissez le groupe et le hébergez à ce que vous voulez connecter.
2. Puisque des Certificats sont utilisés, choisissez **se connectent** afin d'établir le VPN. Voir la figure 39. **Remarque:** Puisque la connexion utilise des Certificats, il n'y a aucun besoin d'écrire un nom d'utilisateur et mot de passe.

**Figure 39 : Se connecter**



Remarque:

Voir l'annexe E pour la configuration facultative de profil de client d'AnyConnect.

## [Annexe A – Mappage de LDAP et DAP](#)

Dans la version 7.1(x) et ultérieures ASA/PIX, une caractéristique appelée cartographie de LDAP a été introduite. C'est une fonctionnalité puissante qui fournit un mappage entre un attribut de Cisco et les objets de LDAP/attribut, qui réalise une inversion le besoin de modification de schéma de LDAP. Pour l'implémentation d'authentification CAC, ceci peut prendre en charge l'application supplémentaire de stratégie sur la connexion d'Accès à distance. Ce sont des exemples du mappage de LDAP. Rendez-vous compte que vous avez besoin des droits d'administrateur afin d'apporter des modifications dans le serveur AD/LDAP. En logiciel ASA 8.x, la caractéristique de la stratégie d'accès dynamique (DAP) a été introduite. DAP peut fonctionner en même temps que le CAC pour regarder de plusieurs groupes d'AD aussi bien que pour pousser des stratégies, ACLs et ainsi de suite.

### [Scénario 1 : Application de Répertoire actif utilisant l'accès distant d'autorisation d'Accès à distance – Permettez/refusez Access](#)

Cet exemple trace le msNPAllowDailin d'attribut d'AD à l'attribut cVPN3000-Tunneling- Protocol de Cisco.

- La valeur d'attribut d'AD : VRAI = laissez ; FAUX = refusez
- Valeur d'attribut de Cisco : 1 = FAUX, 4 (IPSec) ou 20 (4 IPSEC + webvpn 16) = RECTIFIANT,

Pour l'état ALLOW, vous tracez :

- RECTIFIEZ = 20

Pour l'état d'accès distant DENY, vous tracez :

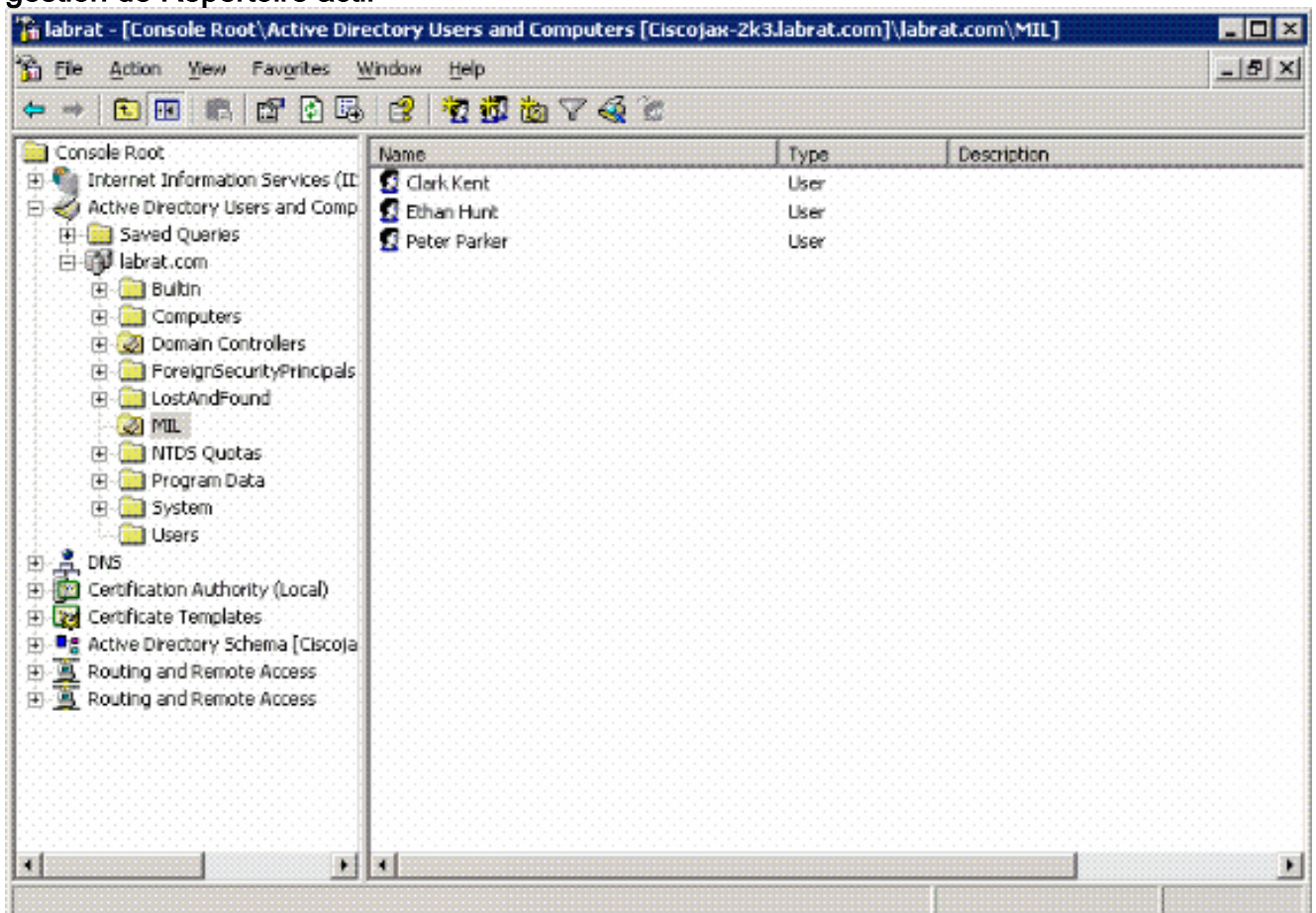
- = 1 FAUX

**Remarque:** Assurez-vous que VRAI et FAUX soyez dans des tous les CAPS. Référez-vous à

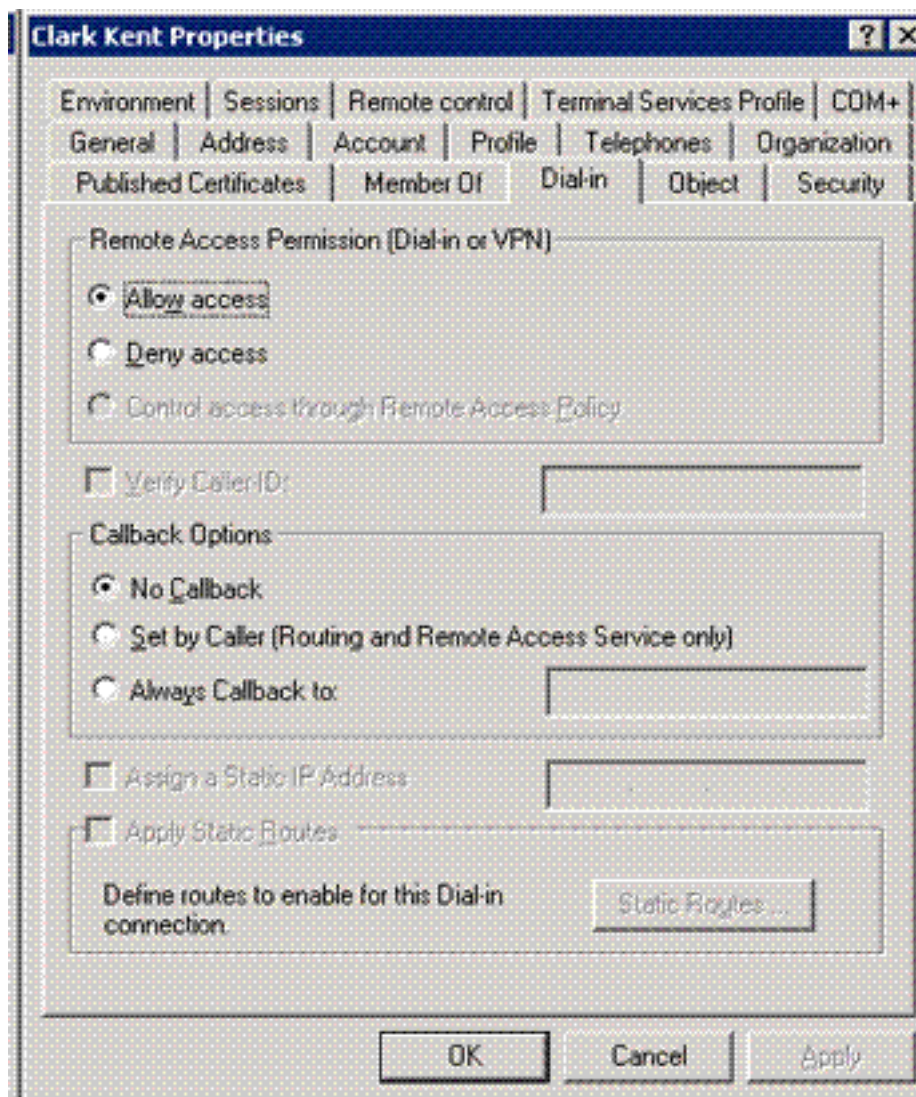
[configurer un serveur externe pour le](#) pour en savoir plus d'[autorisation d'utilisateur de dispositifs de sécurité](#).

## Installation de Répertoire actif

1. Dans le serveur de Répertoire actif, **Start > Run de clic**.
2. Dans la zone de texte ouverte, le type **dsa.msc** cliquent sur **alors l'ok**. Ceci met en marche la console de gestion active de répertoire.
3. Dans la console de gestion de Répertoire actif, cliquez sur le signe plus afin de développer les utilisateurs et les ordinateurs de Répertoire actif.
4. Cliquez sur le signe plus afin de développer le nom de domaine.
5. Si vous avez une OU créée pour vos utilisateurs, développez l'OU afin de visualiser tous les utilisateurs ; si vous faites assigner tous les utilisateurs dans le répertoire d'utilisateurs, développez ce répertoire afin de les visualiser. Voir la figure A1.**Figure A1 : Console de gestion de Répertoire actif**



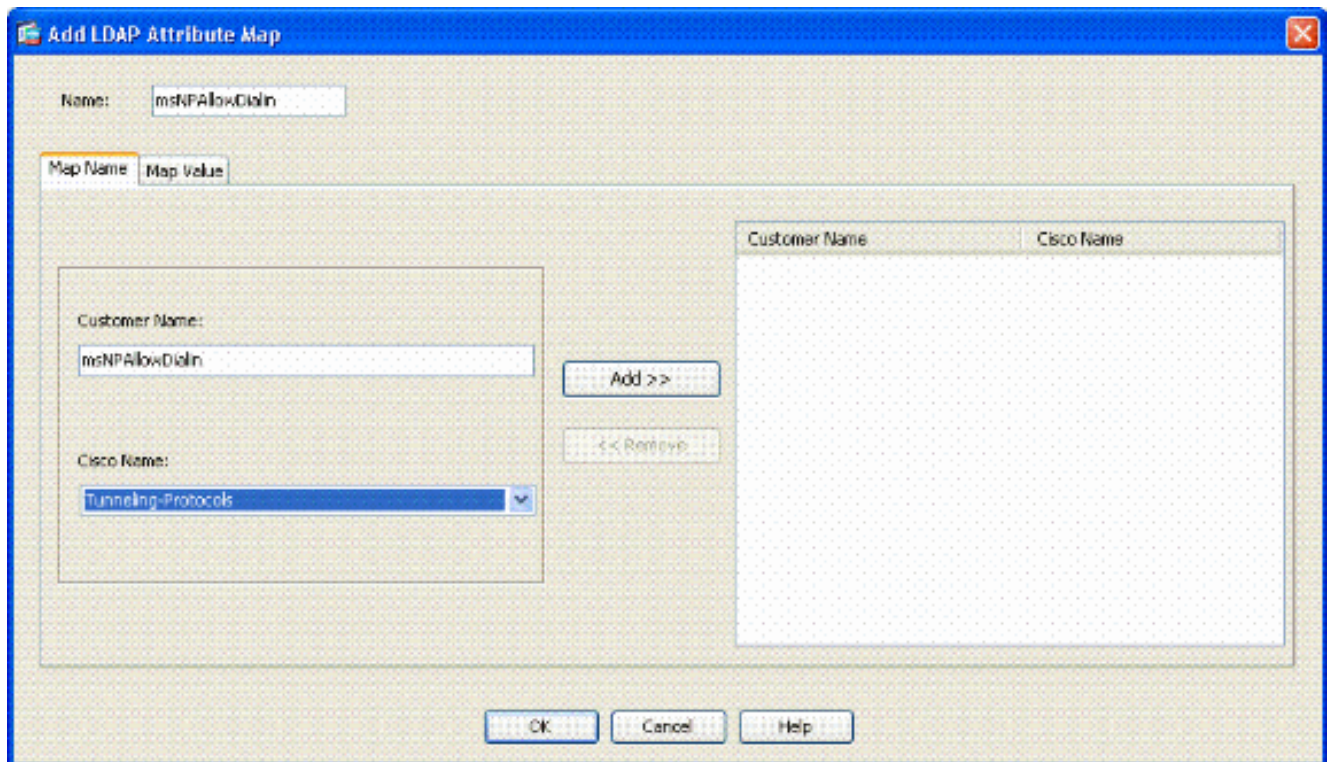
6. Double-cliquer sur l'utilisateur que vous voulez éditer. Cliquez sur en fonction l'onglet Numérotation dans la page de propriétés d'utilisateur et cliquez sur en fonction **laissent** ou **refusent**. Voir la figure A2.**Figure A2 : Utilisateur Properties**



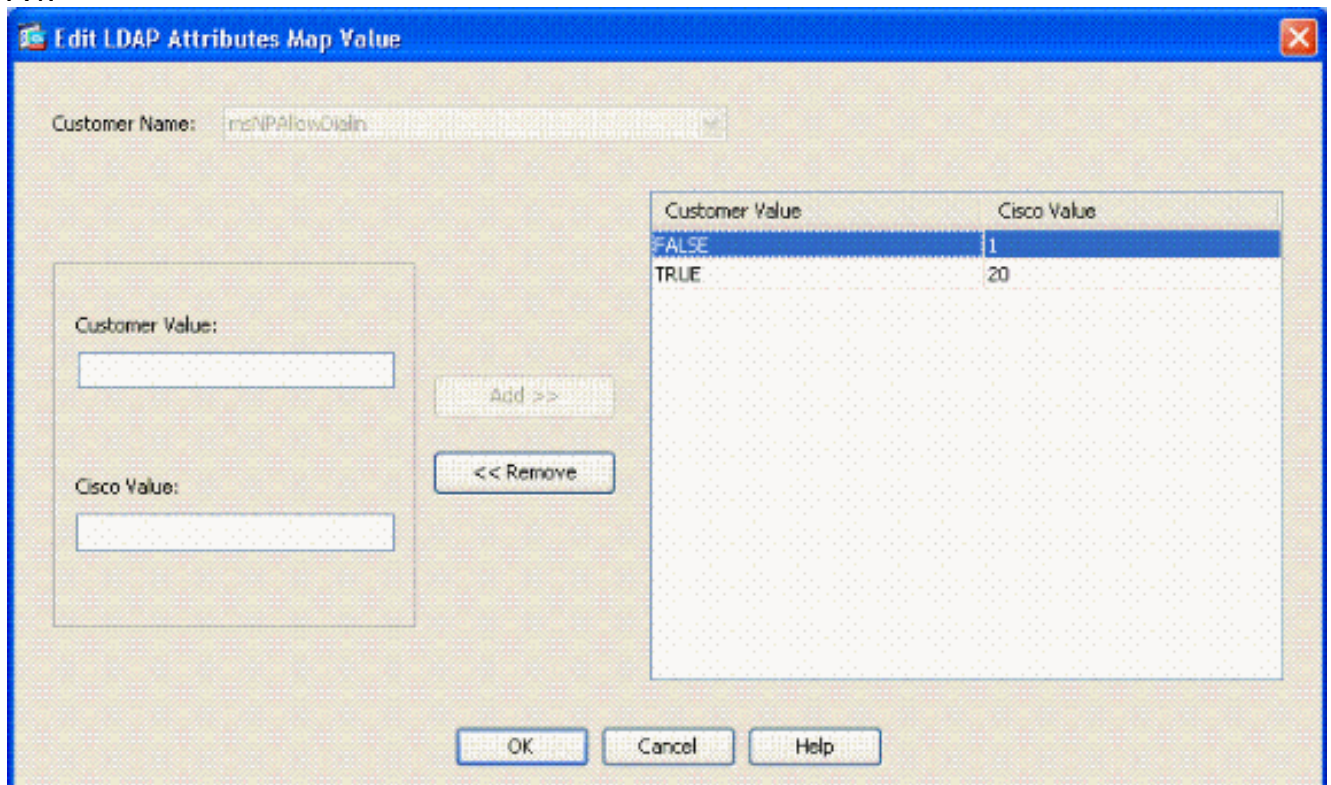
7. Cliquez sur alors l'ok.

## [Configuration ASA](#)

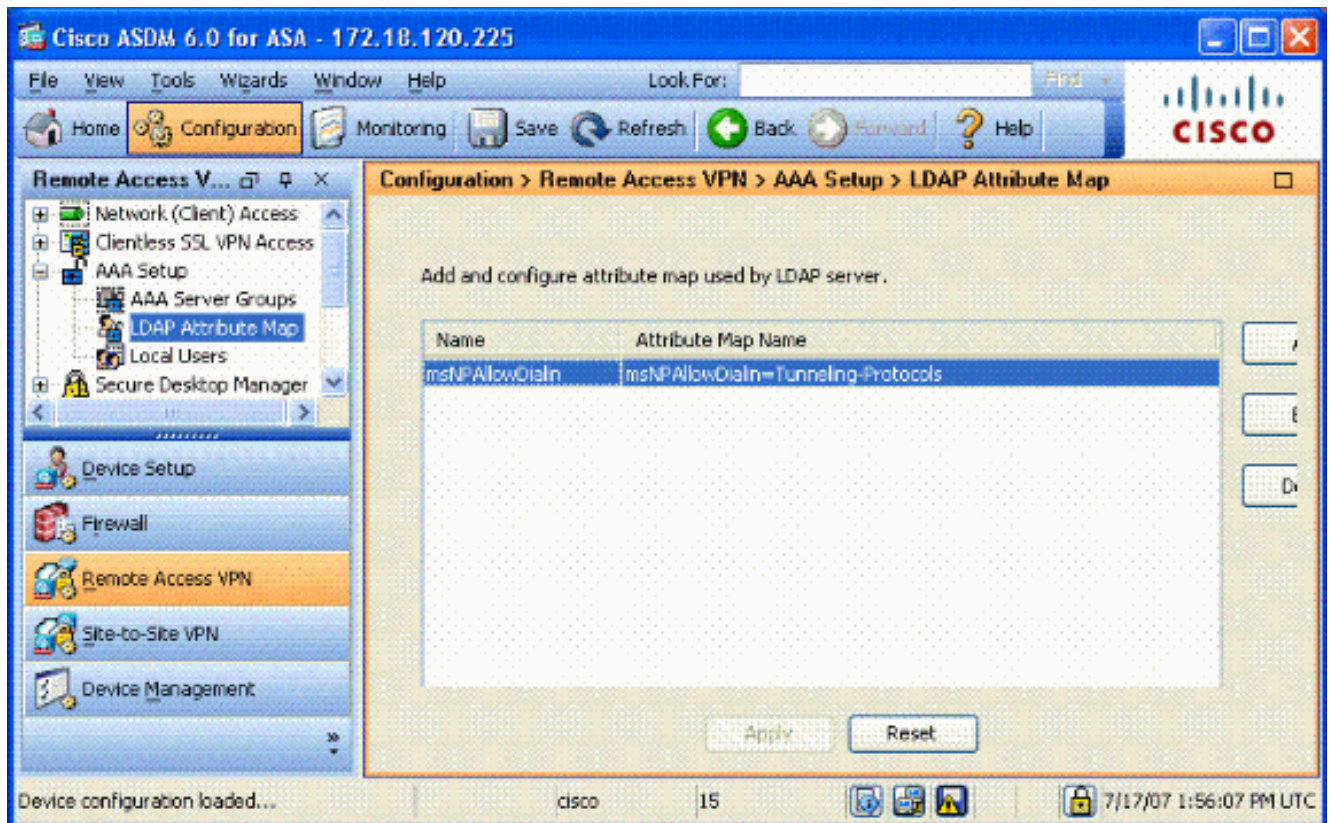
1. Dans l'ASDM, choisissez l'AAA de l'Accès à distance VPN> installé > carte d'attribut de LDAP.
2. Cliquez sur Add.
3. Dans la fenêtre de carte d'attribut de LDAP d'ajouter, terminez-vous ces étapes. Voir la figure A3.**Figure A3 : Ajouter la carte d'attribut de LDAP**



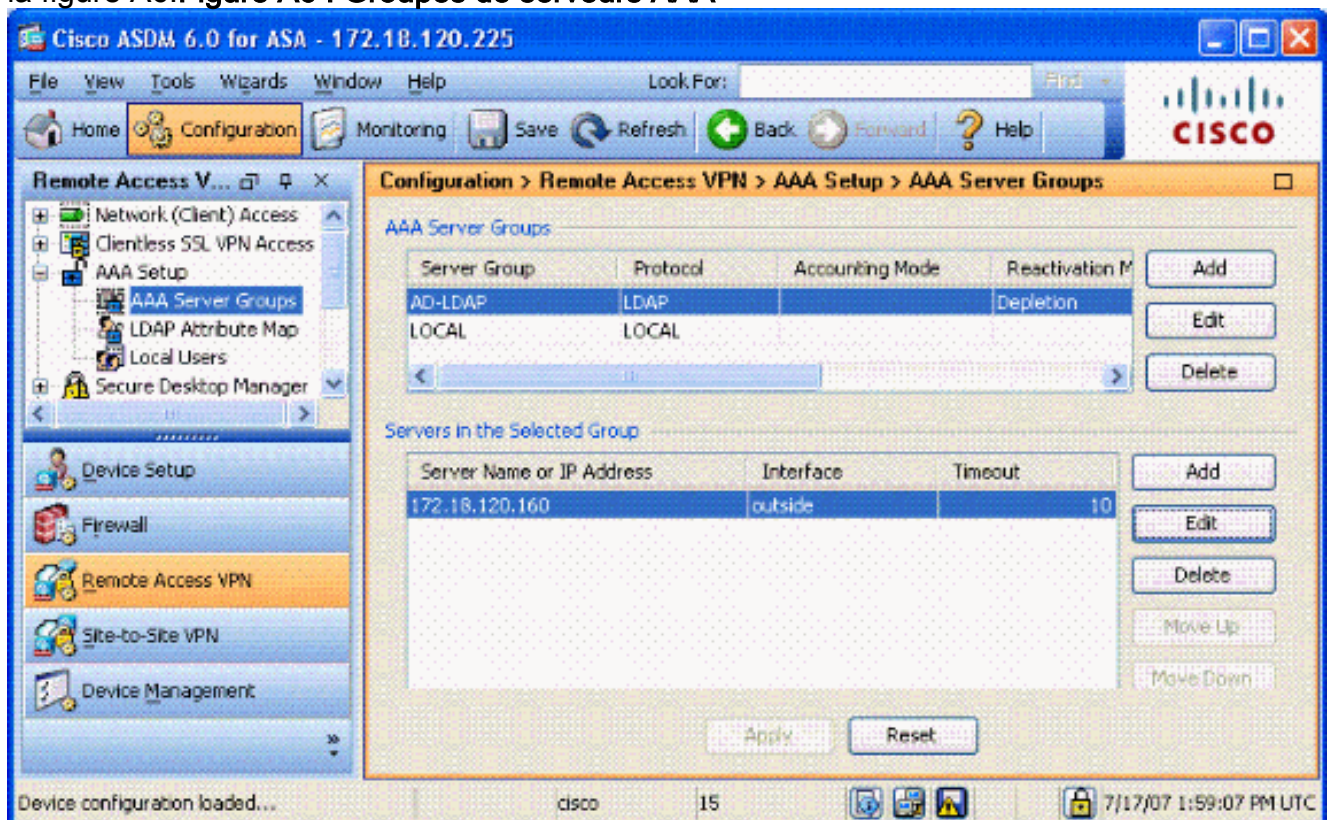
Écrivez un nom dans la zone de texte de nom. Dans l'onglet de map name, **msNPAllowDialIn** de type dans la zone de texte de nom de client. Dans l'onglet de map name, choisissez les Tunnellisation-**protocoles** dans l'option de déroulant dans le nom de Cisco. Cliquez sur **Add**. Choisissez l'onglet de **valeur de carte**. Cliquez sur **Add**. Dans la fenêtre de valeur de carte de LDAP d'attribut d'ajouter, tapez **VRAI** dans la zone de texte de nom de client et le type **20** dans la zone de texte de valeur de Cisco. Cliquez sur **Add**. Tapez **FAUX** dans la zone de texte et le type **1** de nom de client dans la zone de texte de valeur de Cisco. Voir la figure A4.



Cliquez sur **OK**. Cliquez sur **OK**. Cliquez sur **Apply**. La configuration devrait ressembler à la figure A5. **Figure A5 : Configuration de carte d'attribut de LDAP**



4. Choisissez l'AAA de l'Accès à distance VPN> installé > des Groupes de serveurs AAA. Voir la figure A6. **Figure A6 : Groupes de serveurs AAA**



5. Cliquez sur en fonction le groupe de serveurs que vous voulez éditer. Dans les serveurs dans la section de groupe sélectionné, choisissez l'adresse IP du serveur ou l'adresse Internet, et puis cliquez sur Edit.
6. Dans éditez la fenêtre de serveur d'AAA, dans la zone de texte de carte d'attribut de LDAP, choisissez la carte d'attribut de LDAP créée dans le menu déroulant. Voir la figure A7. **Figure A7 : Ajouter la carte d'attribut de LDAP**

**Edit AAA Server**

Server Group: AD-LDAP

Interface Name: outside

Server Name or IP Address: 172.18.120.160

Timeout: 10 seconds

**LDAP Parameters**

Enable LDAP over SSL

Server Port: 389

Server Type: -- Detect Automatically/Use Generic Type --

Base DN: CN=Users,DC=gsgseclab,DC=org

Scope: One level beneath the Base DN

Naming Attribute(s): userPrincipalName

Login DN: CN=Administrator,CN=Users,DC=gsgseclab,DC=o

Login Password: ●●●●●●●●

LDAP Attribute Map: msNPAllowDialin

SASL MD5 authentication

SASL Kerberos authentication

Kerberos Server Group:

OK Cancel Help

7. Cliquez sur **OK**.

**Remarque:** Activez l'élimination des imperfections de LDAP tandis que vous testez afin de vérifier si l'attache de LDAP et le mappage d'attribut fonctionnent correctement. Voir l'annexe C pour des commandes de dépannage.

## [Scénario 2 : L'application de Répertoire actif utilisant l'adhésion à des associations à laisser/refusent Access](#)

Cet exemple emploie le memberOf d'attribut de LDAP pour tracer à l'attribut de perçage d'un tunnel Protocol afin d'établir une adhésion à des associations comme condition. Pour que cette stratégie fonctionne, vous devez avoir ces conditions :

- Utilisez un groupe qui existe déjà ou créez un nouveau groupe pour que les utilisateurs ASA VPN soient un membre de pour des états ALLOW.
- Utilisez un groupe qui existe déjà ou créez un nouveau groupe pour que non les utilisateurs

ASA soient un membre de pour des états DENY.

- Veillez à signer la visionneuse de LDAP que vous avez le bon DN pour le groupe. Voir l'annexe D. Si le DN est erroné, le mappage ne fonctionne pas correctement.

**Remarque:** Rendez-vous compte que l'ASA peut seulement lire la première chaîne de l'attribut de memberOf dans cette release. Assurez-vous que le nouveau groupe créé est sur le haut de la liste. L'autre option est de mettre un caractère particulier devant le nom car l'AD regarde des caractères particuliers d'abord. Afin de fonctionner autour de cette mise en garde, utilisation DAP en logiciel 8.x de regarder de plusieurs groupes.

**Remarque:** Assurez-vous qu'un utilisateur fait partie du groupe de refuser ou au moins d'un autre groupe de sorte que le memberOf soit toujours renvoyé à l'ASA. Vous ne devez pas spécifier le FAUX refusez la condition mais la pratique recommandée est de faire ainsi. Si le nom de groupe existant ou le nom de groupe contient un espace, écrivez l'attribut de cette manière :

CN=Backup Operators,CN=Builtin,DC=gsgseclab,DC=org

**Remarque:** DAP permet à l'ASA pour regarder de plusieurs groupes dans l'attribut de memberOf et l'autorisation de base outre des groupes. Voyez la section DAP.

## CARTOGRAPHIE

- La valeur d'attribut d'AD :memberOf CN=ASAUsers, CN=Users, DC=gsgseclab, DC=orgmemberOf CN=TelnetClients, CN=Users, DC=labrat, DC=com
- Valeur d'attribut de Cisco : 1 = FAUX, 20 = RECTIFIANT,

Pour l'état **ALLOW**, vous tracez :

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

Pour l'état **DENY**, vous tracez :

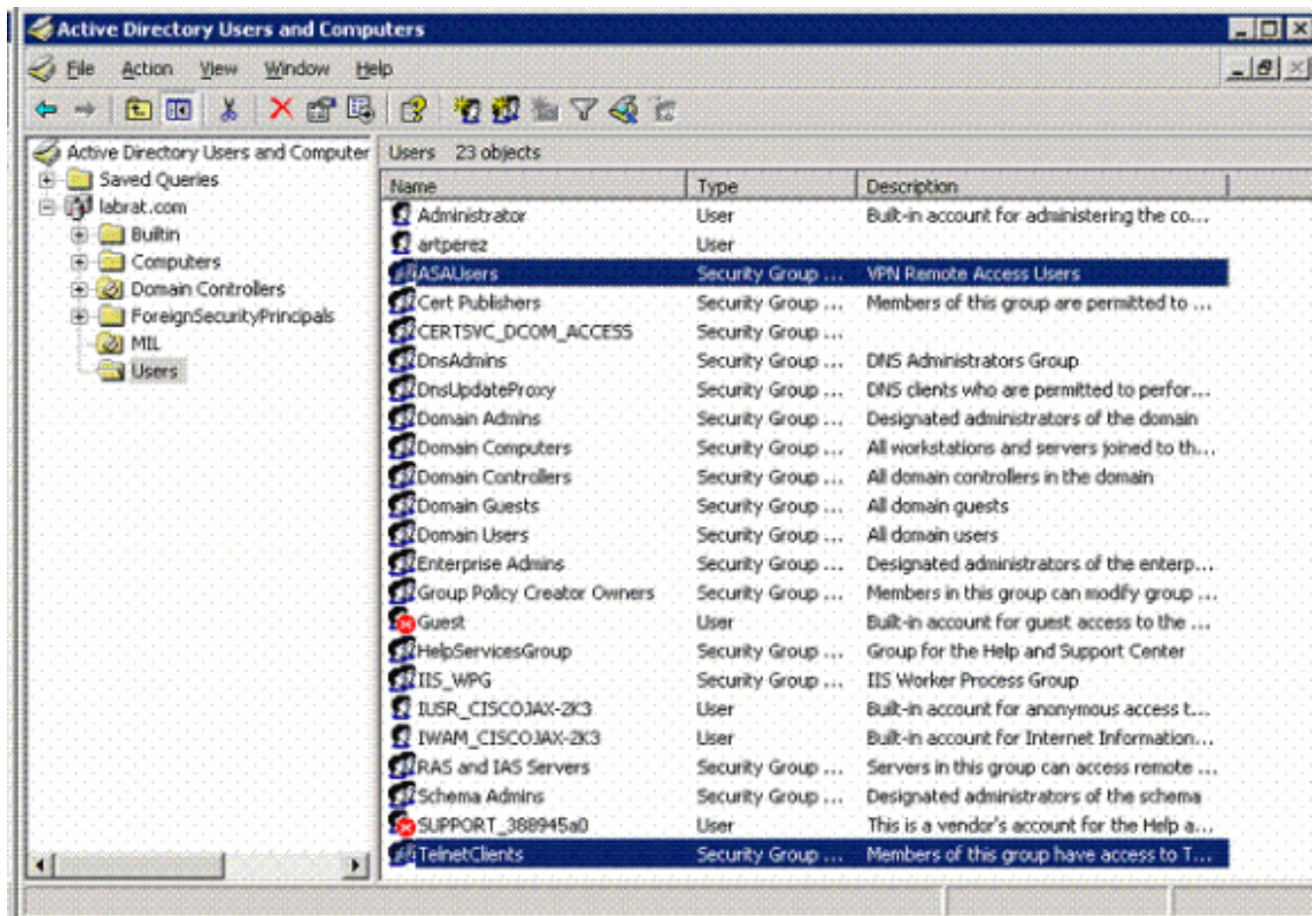
- memberOf CN=TelnetClients, CN=Users, DC=gsgseclab, DC=org = 1

**Remarque:** Dans la version future, il y a un attribut de Cisco afin de permettre et refuser la connexion. Référez-vous à [configurer un serveur externe pour l'autorisation d'utilisateur de dispositifs de sécurité](#) pour plus d'informations sur des attributs de Cisco.

## Installation de Répertoire actif

1. Dans le serveur de Répertoire actif, choisissez le **Start > Run**.
2. Dans la zone de texte ouverte, le type **dsa.msc**, et cliquent sur alors l'ok. Ceci met en marche la console de gestion active de répertoire.
3. Dans la console de gestion de Répertoire actif, cliquez sur le signe plus afin de développer les utilisateurs et les ordinateurs de Répertoire actif. Voir la figure A8 **Figure A8 : Groupes de Répertoire actif**

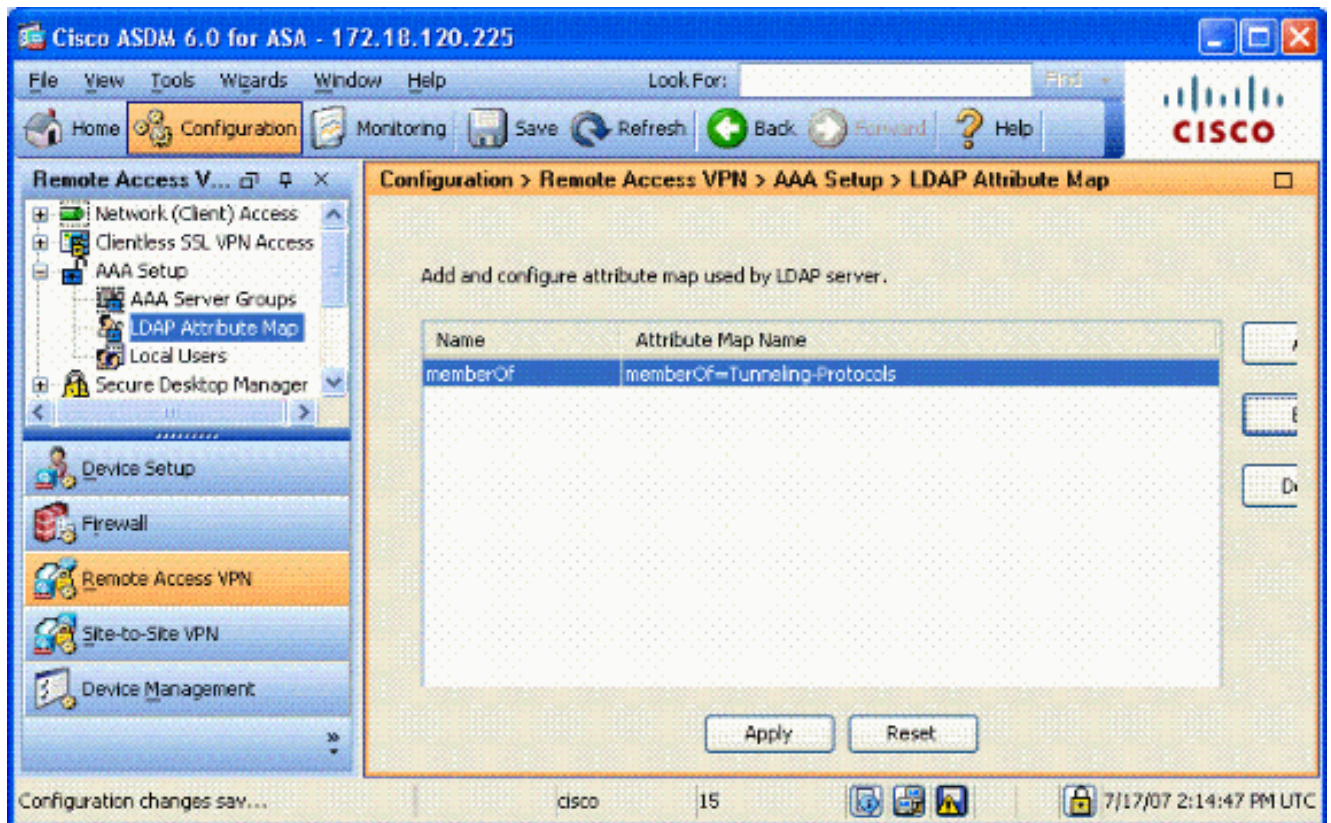




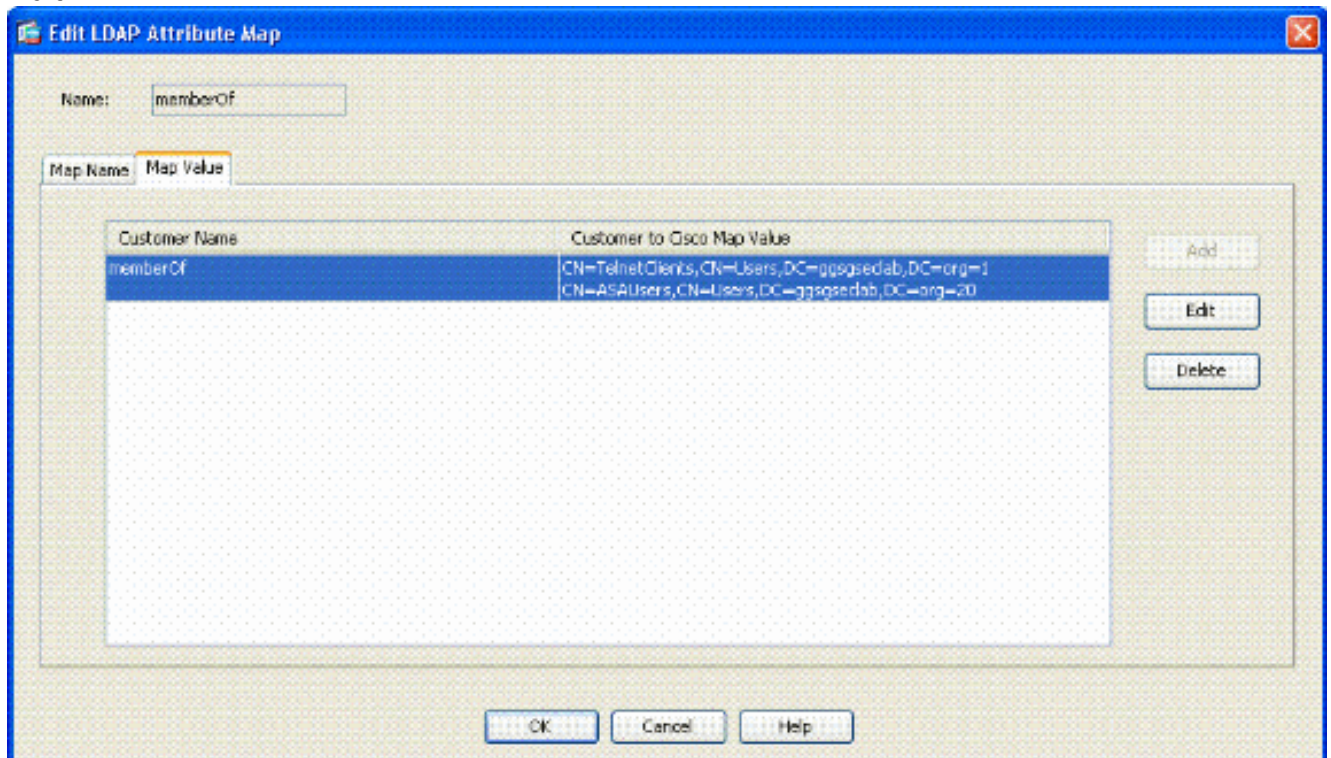
4. Cliquez sur le signe plus afin de développer le nom de domaine.
5. Cliquez avec le bouton droit sur le répertoire d'utilisateurs et choisissez **nouveau > groupe**.
6. Écrivez un nom de groupe. Exemple : ASAUsers.
7. Cliquez sur **OK**.
8. Cliquez sur en fonction le répertoire d'utilisateurs, et double-cliquez alors sur le groupe que vous avez juste créé.
9. Choisissez l'onglet de **membres**, et puis cliquez sur **Add**.
10. Introduisez le nom d'utilisateur que vous voulez ajouter, et puis cliquez sur **l'ok**.

## Configuration ASA

1. Dans l'ASDM, choisissez l'**Accès à distance VPN > AAA installé > carte d'attribut de LDAP**.
2. Cliquez sur **Add**.
3. Dans la fenêtre de carte d'attribut de LDAP d'ajouter, terminez-vous ces étapes. Voir la figure A3. Écrivez un nom dans la zone de texte de nom. Dans l'onglet de map name, **memberOf** de type dans la zone de texte C. de nom de client. Dans l'onglet de map name, choisissez les **Tunnellisation-protocoles** dans l'option de déroulant dans le nom de Cisco. Choisissez **ajoutent**. Cliquez sur l'onglet de **valeur de carte**. Choisissez **ajoutent**. Dans la fenêtre de valeur de carte de LDAP d'attribut d'ajouter, le type **CN=ASAUsers, CN=Users, DC=gsgseclab, DC=org** dans la zone de texte de nom de client et le type **20** dans la zone de texte de valeur de Cisco. Cliquez sur **Add**. Tapez **CN=TelnetClients, CN=Users, DC=gsgseclab, DC=org** dans la zone de texte et le type **1** de nom de client dans la zone de texte de valeur de Cisco. Voir la figure A4. Cliquez sur **OK**. Cliquez sur **OK**. Cliquez sur **Apply**. La configuration devrait ressembler à la figure A9. **Carte d'attribut de LDAP de figure A9**



4. Choisissez l'AAA de l'Accès à distance VPN> installé > des Groupes de serveurs AAA.
5. Cliquez sur en fonction le groupe de serveurs que vous voulez éditer. Dans les serveurs dans la section de groupe sélectionné, sélectionnez l'adresse IP du serveur ou l'adresse Internet, et puis cliquez sur Edit



6. Dans éditez la fenêtre de serveur d'AAA, dans la zone de texte de carte d'attribut de LDAP, sélectionnent la carte d'attribut de LDAP créée dans le menu déroulant.
7. Cliquez sur OK.

**Remarque:** Activez l'élimination des imperfections de LDAP tandis que vous testez afin de vérifier l'attache de LDAP et attribuer des mappages fonctionnez correctement. Voir l'annexe C pour des commandes de dépannage.

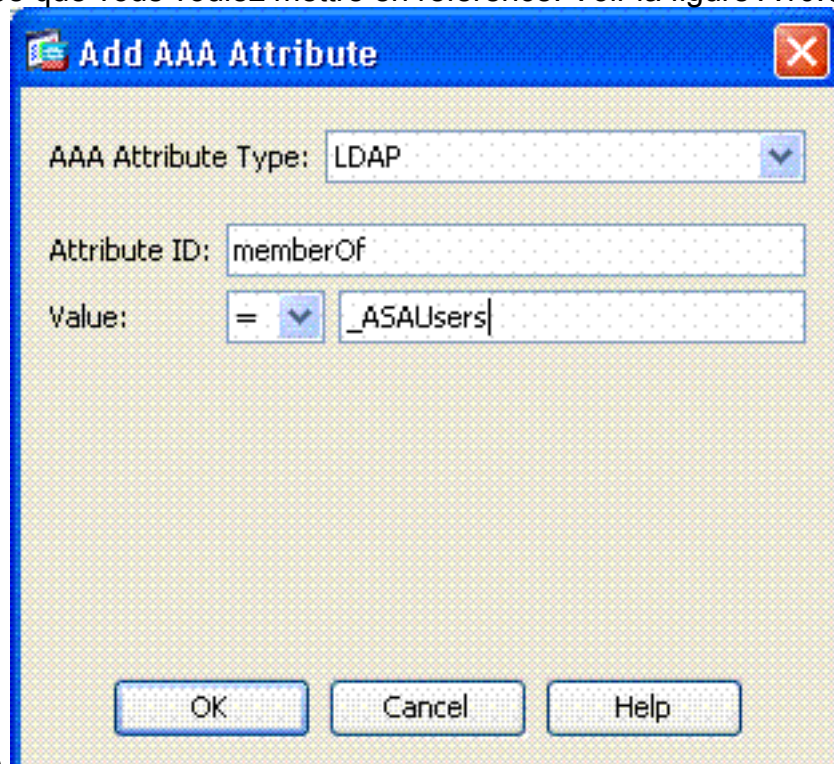
## Scénario 3 : Dynamic Access Policies pour de plusieurs attributs de memberOf

Cet exemple emploie DAP pour regarder de plusieurs attributs de memberOf afin de permettre accès basé sur hors fonction de l'adhésion à des associations de Répertoire actif. Avant 8.x, l'ASA a seulement lu le premier attribut de memberOf. Avec 8.x et plus tard, l'ASA peut regarder tous les attributs de memberOf.

- Utilisez un groupe qui existe déjà ou créez un nouveau groupe (ou les plusieurs groupes) pour que les utilisateurs ASA VPN soient un membre de pour des états ALLOW.
- Utilisez un groupe qui existe déjà ou créez un nouveau groupe pour que non les utilisateurs ASA soient un membre de pour des états DENY.
- Veillez à signer la visionneuse de LDAP que vous avez le bon DN pour le groupe. Voir l'annexe D. Si le DN est erroné, le mappage ne fonctionne pas correctement.

### Configuration ASA

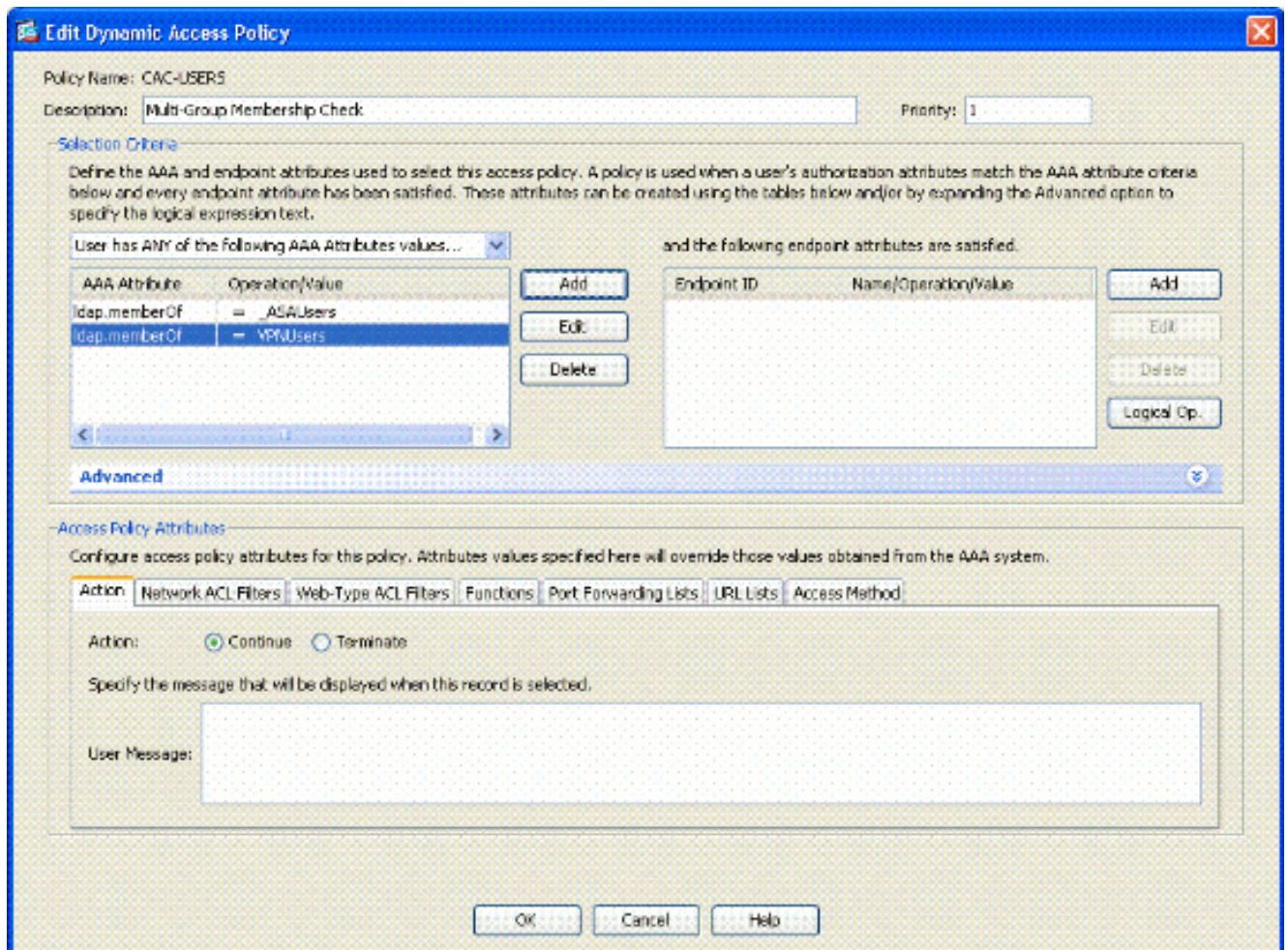
1. Dans l'ASDM, choisissez le **réseau de l'Accès à distance VPN> (client) Access > Dynamic Access Policies**.
2. Cliquez sur **Add**.
3. Dans la stratégie d'accès dynamique d'ajouter, terminez-vous ces étapes :Écrivez un nom dans la zone de texte B. de nom.Dans la section prioritaire, entrez dans **1**, ou un nombre plus grand que 0.Dans les critères de sélection, cliquez sur Add.Dans l'aaa attribute d'ajouter, choisissez le **LDAP**.Dans la section d'ID d'attribut, écrivez le **memberOf**.Dans la section de valeur, choisissez **=** et écrivez le nom de groupe d'AD. Répétez cette étape pour chaque groupe que vous voulez mettre en référence. Voir la figure A10.**Carte d'aaa attribute**



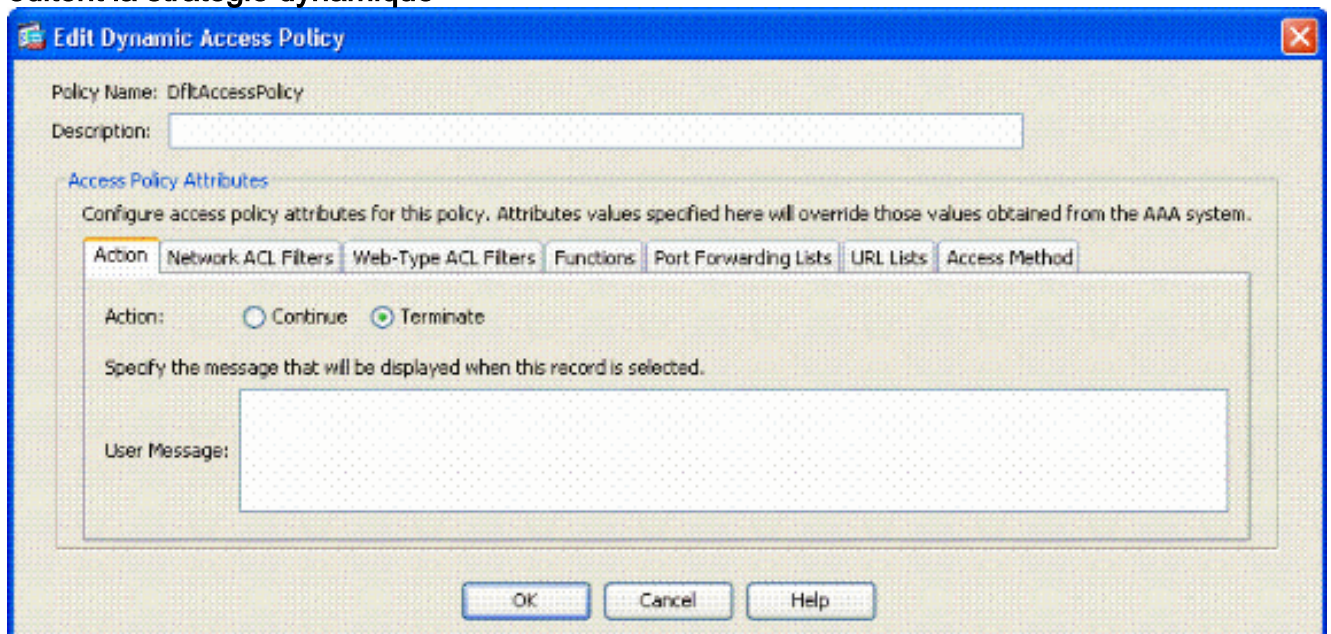
de figure A10

Cliquez sur

**OK**. Dans la section d'attributs de stratégie d'Access, choose **Continue**. Voir la figure A11. La figure A11 ajoutent la stratégie dynamique



4. Dans l'ASDM, choisissez le réseau de l'Accès à distance VPN> (client) Access > Dynamic Access Policies.
5. Choisissez la stratégie par défaut d'Access et choisissez éditent.
6. L'action par défaut devrait être placée pour se terminer. Voir la figure A12. La figure A12 éditent la stratégie dynamique



7. Cliquez sur OK.

**Remarque:** Si **Terminate** n'est pas sélectionnée, on te permet dedans même si pas dans tous les groupes parce que le par défaut est de continuer.

## Annexe B – Configuration ASA CLI

### ASA 5510

```
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=gsgseclab,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=gsgseclab,DC=org ldap-scope onelevel ldap-
naming-attribute userPrincipalName ldap-login-password *
ldap-login-dn
CN=Administrator,CN=Users,DC=gsgseclab,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 ocsf trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil no client-
types crl configure crypto ca trustpoint
ASDM_TrustPoint2 revocation-check ocsf enrollment
terminal keypair DoD-2048 match certificate
DefaultCertificateMap override ocsf trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil no client-
types crl configure crypto ca trustpoint
ASDM_TrustPoint3 revocation-check ocsf 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
esmtcp inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
! -----SSL/WEBVPN-----
----- 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-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-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 dépannage c

### Dépannage de l'AAA et du LDAP

- mettez au point le LDAP 255 — Échanges de LDAP d'affichages
- terrain communal 10 de debug aaa — Échanges d'AAA d'affichages

### Exemple 1 : Connexion permise avec le mappage correct d'attribut

Cet exemple affiche que la sortie de **mettent au point le LDAP** et le **debug aaa communs** pendant une connexion réussie avec le scénario 2 affiché dans l'annexe R.

#### **Figure C1 : mettez au point la sortie commune de LDAP et de 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=gsgseclab,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=gsgseclab,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 permise avec le mappage SIG-configuré d'attribut de Cisco](#)

Cet exemple affiche que la sortie de **mettent au point le LDAP** et le **debug aaa communs** pendant une connexion permise avec le scénario 2 affiché dans l'annexe R.

### Figure C2 : mettez au point la sortie commune de LDAP et de 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=gsgseclab,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=gsgseclab,DC=org
```

```
[82] mapped to cVPN3000-Tunneling-Protocols: value =
CN=ASAUsers,CN=Users,DC=gsgseclab,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=gsgseclab,DC=or
g
[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, 1a870b4)
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](#)

- **mettez au point les erreurs de dap** — Erreurs des affichages DAP
- **mettez au point le suivi de dap** — Suivi de fonction des affichages DAP

### [Exemple 1 : Connexion permise avec DAP](#)

Cet exemple affiche que la sortie de **mettent au point des erreurs de dap** et **mettent au point le suivi de dap** pendant une connexion réussie avec le scénario 3 affiché dans l'annexe R. Plusieurs attributs de memberOf d'avis. Vous pouvez appartenir aux \_ASAUUsers et le VPNUUsers ou le tp l'un ou l'autre de groupe, qui dépend du config ASA.

#### **Figure C3 : mettez au point DAP**

```

#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=gsgseclab,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 = VPUsers
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf.2
= _ASUsers 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=gsgseclab,DC=or
g 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=gsgsec1ab,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"] =
"_ASAPUsers"; 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=gsgsec1ab,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

L'exemple de Thia affiche que la sortie de **mettent au point des erreurs de dap** et **mettent au point le suivi de dap** pendant une connexion infructueuse avec le scénario 3 affiché dans l'annexe R.

### Figure C4 : mettez au point DAP

```
#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=gsgseclab,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=gsgseclab,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=gsgseclab,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=gsgseclab,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 config — en se connectant la classe Ca consolez (ou mémoire tampon)  
l'élimination des imperfections

Ces exemples affichent une validation réussie de certificat avec le responder OCSP et une stratégie assortie défectueuse de groupe de certificat.

La figure C3 affiche la sortie de débogage qui a un certificat validé et une stratégie assortie fonctionnante de groupe de certificat.

La figure C4 affiche la sortie de débogage d'une stratégie assortie SIG-configurée de groupe de certificat.

La figure C5 affiche la sortie de débogage d'un utilisateur avec un certificat retiré.

### **Figure C5 : Élimination des imperfections OCSP – validation réussie de certificat**

```

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 : Sortie d'une stratégie assortie défectueuse de groupe de certificat

### Figure C5 : Sortie d'un certificat retiré

```

n %PI=X-3-7E17t02h7a Certinf icaHtue cnhta,in faioled
uvalidation=.
CMertifiIcLa,ted ccha=inl ais eibtrhaer tin,validid 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=gsgseclab,dc=org, issuer_name:
cn=gsgseclab,dc=gsgseclab,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=gsgseclab,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=gsgseclab,dc=org
CRYPTO_PKI: Certificate not validated
```

## [Annexe D – Vérifiez les objets de LDAP dans le MS](#)

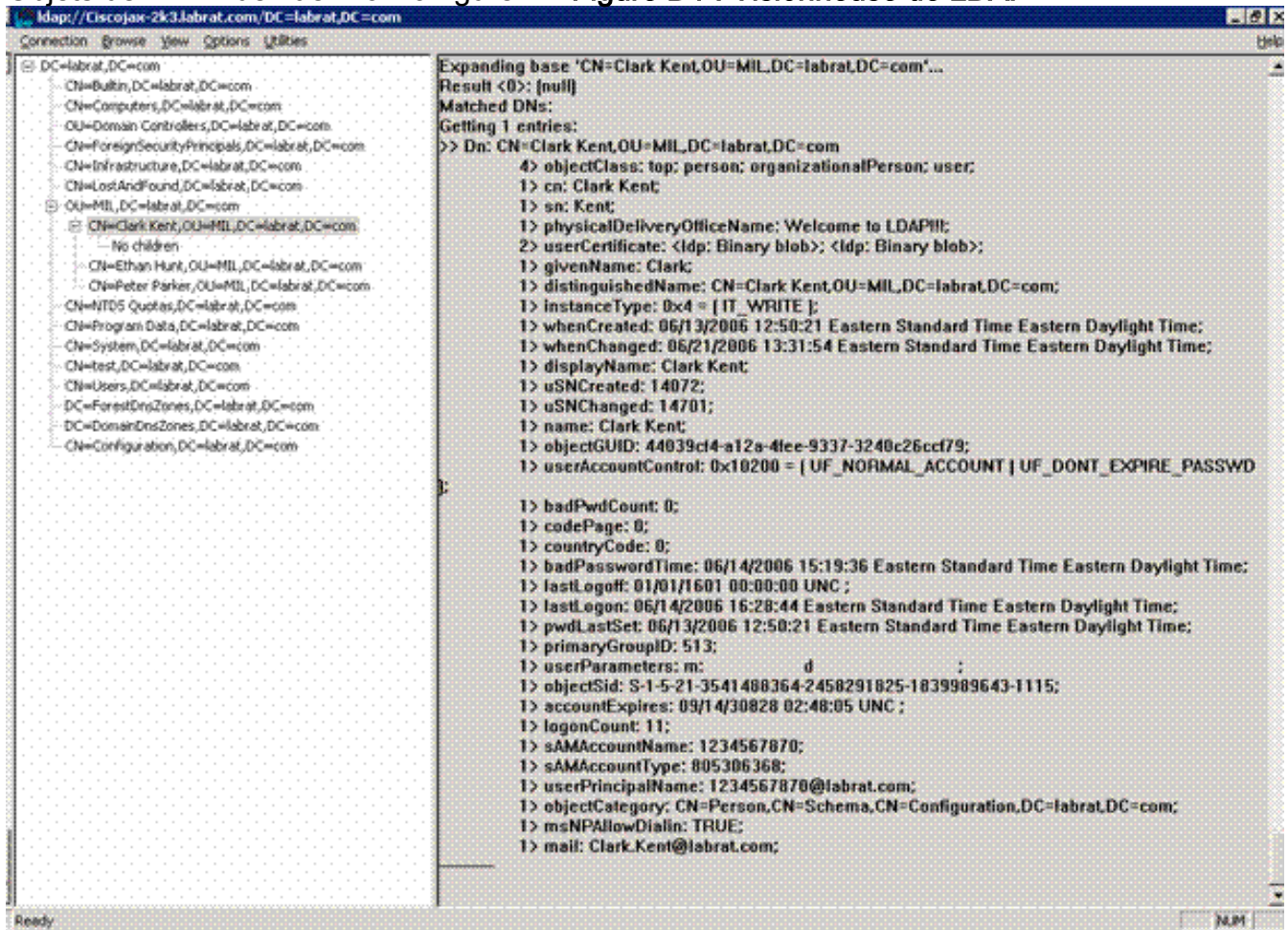
Dans le CD du serveur 2003 de Microsoft, il y a des outils supplémentaires qui peuvent être installés afin de visualiser la structure de LDAP aussi bien que les objets de LDAP/attributs. Afin d'installer ces outils, allez au répertoire de **support** dans le CD et puis les **outils**. Installez **SUPTOOLS.MSI**.

### [Visionneuse de LDAP](#)

- Après installation, choisissez le **Start > Run**.
- **Le LDP de type**, cliquent sur alors l'**ok**. Ceci met en marche la visionneuse de LDAP.
- Choisissez la **connexion > se connectent**.
- Écrivez le nom du serveur et puis cliquez sur l'**ok**.
- Choisissez la **connexion > le grippage**.
- Écrivez un nom d'utilisateur et mot de passe.**Remarque:** Vous avez besoin des droits

d'administrateur.

- Cliquez sur OK.
- Objets de LDAP de vue. Voir la figure D1.

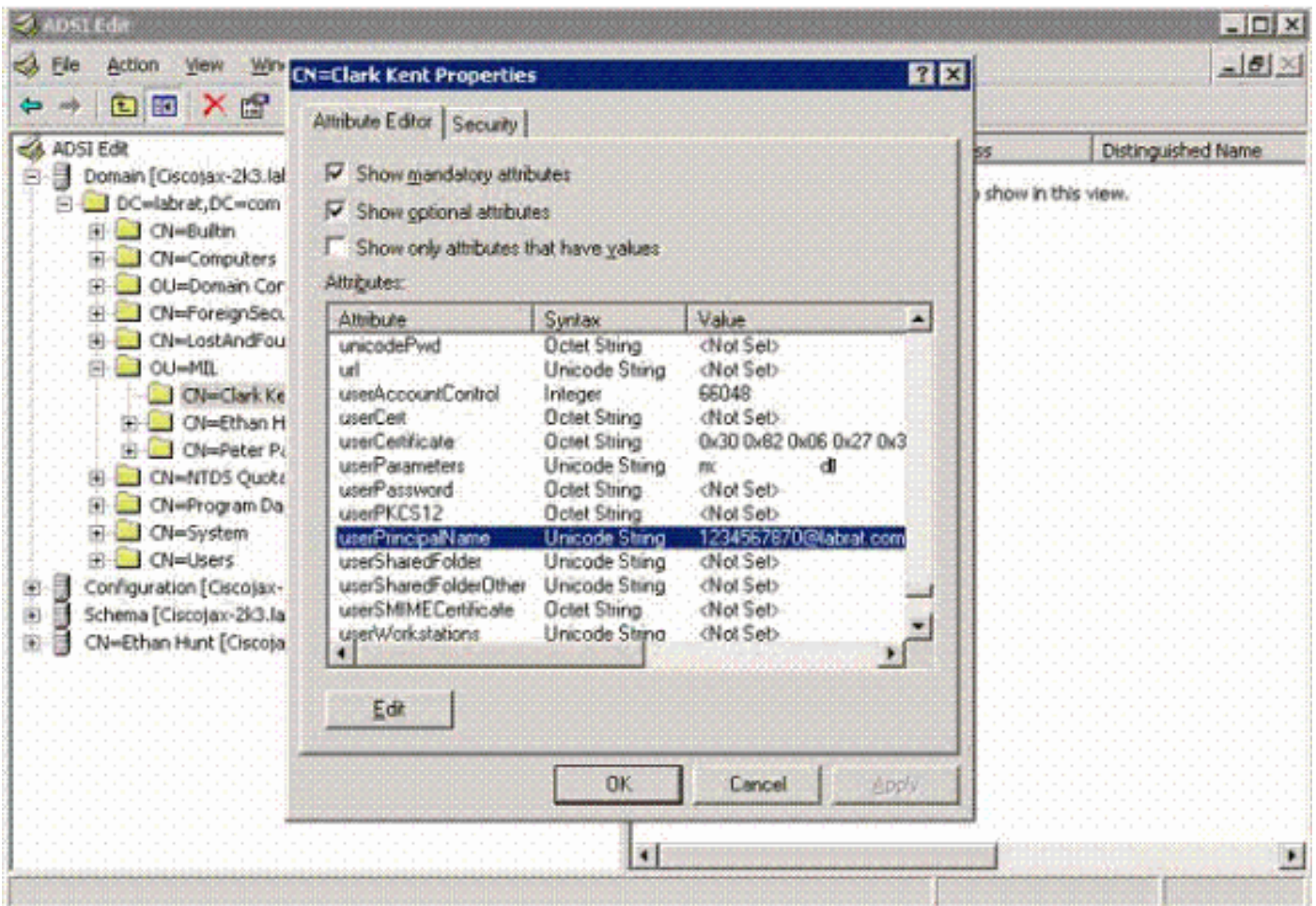


## Éditeur d'interface de services d'annuaire actifs

- Dans le serveur de Répertoire actif, choisissez le **Start > Run**.
- Type **adsiedit.msc**. Ceci commence l'éditeur.
- Clic droit sur un objet et un clic **Properties**.

Cet outil affiche tous les attributs pour les objets spécifiques. Voir la figure D2.

Figure D2 : ADSI éditent



## Annexe E

Un profil d'AnyConnect peut être créé et ajouté à un poste de travail. Le profil peut mettre en référence de diverses valeurs telles que des hôtes ASA ou délivrer un certificat des paramètres assortis tels que le nom unique ou l'émetteur. Le profil est enregistré comme un fichier .xml et peut être édité avec Notepad. Le fichier peut être ajouté à chaque client manuellement ou être poussé de l'ASA par une stratégie de groupe. Le fichier est enregistré dans :

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

Procédez comme suit :

1. Choisissez l'AnyConnectProfile.tmpl et ouvrez le fichier avec Notepad.
2. Apportez les modifications appropriées au fichier tel que l'IP d'émetteur ou d'hôte. Voir la figure F1 par exemple.
3. Une fois terminé, sauvegardez le fichier comme .xml.

C'est un échantillon d'un fichier XML de profil de Cisco AnyConnect VPN Client.

Référez-vous à la documentation de Cisco AnyConnect en vue de la Gestion de profil. En bref :

- Un profil devrait être seulement nommé pour votre société. Un exemple est : CiscoProfile.xml
- Le nom de profil devrait être identique même si différent pour le groupe individuel au sein de la société.

Ce fichier est destiné pour être mis à jour par un administrateur sécurisé de passerelle et pour être puis distribué avec le logiciel client. Le profil basé sur ce XML peut être distribué aux clients à tout moment. Les mécanismes de distribution pris en charge sont comme un fichier empaqueté avec la

distribution logicielle ou en tant qu'élément du mécanisme automatique de téléchargement. Le mécanisme automatique de téléchargement seulement disponible avec certains Produits Cisco Secures de passerelle.

**Remarque:** Des administrateurs sont fortement encouragés à valider le profil XML qu'ils créent avec l'utilisation d'un outil de validation en ligne ou par la fonctionnalité d'importation de profil dans l'ASDM. La validation peut être accomplie avec l'AnyConnectProfile.xsd trouvé dans ce répertoire. AnyConnectProfile est l'élément de racine qui représente le profil de client d'AnyConnect.

```
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, for example, BackupServerList, host
specific !-- overrides are possible. !-- --> -
<ClientInitialization> !-- The Start Before Logon
feature can be used to activate !-- the VPN as part of
the logon sequence. !-- UserControllable: Does the
administrator of this profile allow the user !-- to
control this attribute for their own use. Any user
setting !-- associated with this attribute is stored
elsewhere. --> <UseStartBeforeLogon
UserControllable="false">false</UseStartBeforeLogon> !--
- This control enables an administrator to have a one
time !-- message displayed prior to a users first
connection attempt. As an !-- example, the message can
be used to remind a user to insert their smart !-- card
into its reader. !-- The message to be used with this
control is localizable and can be !-- found in the
AnyConnect message catalog. !-- (default: "This is a
pre-connect reminder message.")
<ShowPreConnectMessage>false</ShowPreConnectMessage> !--
This section enables the definition of various
attributes !-- that can be used to refine client
certificate selection. --> - <CertificateMatch> !--
Certificate Distinguished Name matching allows for exact
!-- match criteria in the choosing of acceptable client
!-- certificates. - <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 CRLs spécifiés par X.509 et RFC 3280](#)

- [OCSP spécifié par RFC 2560](#)
- [Introduction d'infrastructure de clé publique](#)
- [« OCSP léger » a profilé par projet de norme](#)
- [SSL/TLS spécifié par RFC 2246](#)
- [Support et documentation techniques - Cisco Systems](#)