

# PEAP sous des réseaux sans fil unifiés avec Microsoft Internet Authentication Service (IAS)

## Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Conventions](#)

[Présentation de PEAP](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configurez le serveur de Microsoft Windows 2003](#)

[Configurez le serveur de Microsoft Windows 2003](#)

[Installez et configurez les services DHCP sur le serveur de Microsoft Windows 2003](#)

[Installez et configurez le serveur de Microsoft Windows 2003 en tant que serveur d'Autorité de certification \(CA\)](#)

[Connectez les clients de routage au domaine de routage](#)

[Installez le service d'authentification Internet sur le serveur de Microsoft Windows 2003 et demandez un certificat](#)

[Configurez le service d'authentification Internet pour l'authentification PEAP-MS-CHAP v2](#)

[Ajoutez les utilisateurs à l'Active Directory](#)

[Permettez l'accès sans fil aux utilisateurs](#)

[Configurez le contrôleur LAN sans fil et les AP légers](#)

[Configurez le WLC pour l'authentification RADIUS par le serveur RADIUS de MS IAS](#)

[Configurez un WLAN pour les clients de routage](#)

[Configurez les clients sans fil](#)

[Configurez les clients sans fil pour l'authentification PEAP-MS CHAPv2](#)

[Vérifiez et dépannez](#)

[Informations connexes](#)

## Introduction

Ce document fournit un exemple de configuration pour installer Protected Extensible Authentication Protocol (PEAP) avec l'authentification de Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) version 2 dans un réseau sans fil unifié Cisco avec le service d'authentification de routage Internet de Microsoft (IAS) en tant que serveur RADIUS.

## Conditions préalables

## Exigences

Il existe la supposition que le lecteur a connaissance de l'installation de base de Windows 2003 et de l'installation du contrôleur de routage Cisco puisque ce document couvre seulement les configurations spécifiques pour faciliter les tests.

**Remarque** : ce document est destiné à donner aux lecteurs un exemple sur la configuration requise sur le serveur MS pour l'authentification PEAP - MS CHAP. La configuration du serveur de Microsoft présentée dans cette section a été testée dans le laboratoire et s'est avérée fonctionner comme prévu. Si vous avez des problèmes pour configurer le serveur de Microsoft, contactez Microsoft pour obtenir de l'aide. TAC de Cisco ne prend pas en charge la configuration du serveur de Microsoft Windows.

Pour obtenir des informations sur l'installation et la configuration initiales des contrôleurs de la gamme Cisco 4400, reportez-vous au [Guide de démarrage rapide : Contrôleurs LAN sans fil de la gamme Cisco 4400](#).

Les guides d'installation et de configuration de Microsoft Windows 2003 peuvent être trouvés sous [Installer Windows Server 2003 R2](#).

Avant de commencer, installez Microsoft Windows Server 2003 avec le système d'exploitation SP sur chacun des serveurs dans le laboratoire de test et mettez à jour tous les Services Pack. Installez les contrôleurs et les points d'accès léger (LAP) et assurez-vous que les dernières mises à jour logicielles sont configurées.

## Composants utilisés

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

- Contrôleur Cisco de la gamme 4400 qui exécute la version 4.0 du microprogramme
- Protocole de point d'accès léger Cisco 1131 (LWAPP) AP
- Serveur Windows 2003 Enterprise (SP1) avec le service d'authentification Internet (IAS), l'autorité de certification (CA), DHCP et les services de système de noms de domaine (DNS) installés
- Windows XP Professional avec SP2 (et les Services Pack mis à jour) et la carte réseau sans fil Cisco Aironet 802.11a/b/g (NIC)
- Utilitaire de bureau Aironet version 4.0
- Commutateur du routage Cisco 3560

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

## Conventions

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

## Présentation de PEAP

PEAP utilise Transport Level Security (TLS) pour créer un canal chiffré crypté entre un client de routage authentifiant PEAP, tel qu'un ordinateur portable sans fil, et un authentificateur PEAP, tel que le Service d'authentification Internet de Microsoft (IAS) ou n'importe quel serveur RADIUS. PEAP ne spécifie pas de méthode d'authentification, mais fournit la sécurité supplémentaire pour d'autres protocoles d'authentification EAP, tels qu'EAP-MSCHAPv2, qui peut fonctionner par le canal crypté par TLS fourni par PEAP. Le processus d'authentification PEAP consiste en deux phases principales :

### **PEAP phase un : canal chiffré TLS**

Le client sans fil s'associe avec l'AP. Une association basée sur IEEE 802.11 fournit un système ouvert ou l'authentification de clé partagée avant qu'une association sécurisée soit créée entre le client de routage et le point d'accès (LAP). Après que l'association basée sur IEEE 802.11 est établie avec succès entre le client de routage et le point d'accès, la session de TLS est négociée avec l'AP. Une fois que l'authentification a abouti avec succès entre le client sans fil et le serveur IAS, la session de TLS est négociée entre eux. La clé qui dérive de cette négociation est utilisée pour crypter toute la communication ultérieure.

### **Deuxième phase PEAP : communication authentifiée par EAP**

La communication d'EAP, qui inclut la négociation d'EAP, se produit à l'intérieur du canal de TLS créé par PEAP dans la première phase du processus d'authentification de PEAP. Le serveur d'IAS authentifie le client sans fil avec EAP-MS-CHAP v2. Le LAP et le contrôleur réachemine seulement les messages entre le client sans fil et le serveur RADIUS. Le WLC et le LAP ne peuvent pas déchiffrer ces messages parce que ce n'est pas le point d'extrémité de TLS.

Une fois que la première phase de PEAP a lieu et que le canal TLS est créé entre le serveur IAS et le client sans fil de 802.1x, pour une tentative réussie d'authentification où l'utilisateur a fourni les identifiants basés sur un mot de passe valide avec PEAP-MS-CHAP v2, l'ordre de message RADIUS est le suivant :

1. Le serveur IAS envoie un message de demande d'identité au client : EAP-Request/Identity.
2. Le client répond avec un message de réponse d'identité : EAP-Response/Identity.
3. Le serveur IAS envoie un message de demande de confirmation MS-CHAP v2 : EAP-Request/EAP-Type=EAP MS-CHAP-V2 (demande).
4. Le client répond par un challenge et une réponse MS-CHAP v2 : EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response).
5. Le serveur IAS renvoie un paquet de réussite MS-CHAP v2 lorsque le serveur a correctement authentifié le client : EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (Success).
6. Le client répond avec un paquet de réussite MS-CHAP v2 lorsque le client a authentifié avec succès le serveur : EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Success).
7. Le serveur d'IAS envoie un EAP-TLV qui indique l'authentification réussie.
8. Le client répond avec un message de réussite d'état EAP-TLV.
9. Le serveur complète l'authentification et envoie un message de réussite-EAP du texte en clair. Si des VLAN sont déployés pour l'isolation du client, les attributs VLAN sont inclus dans ce message.

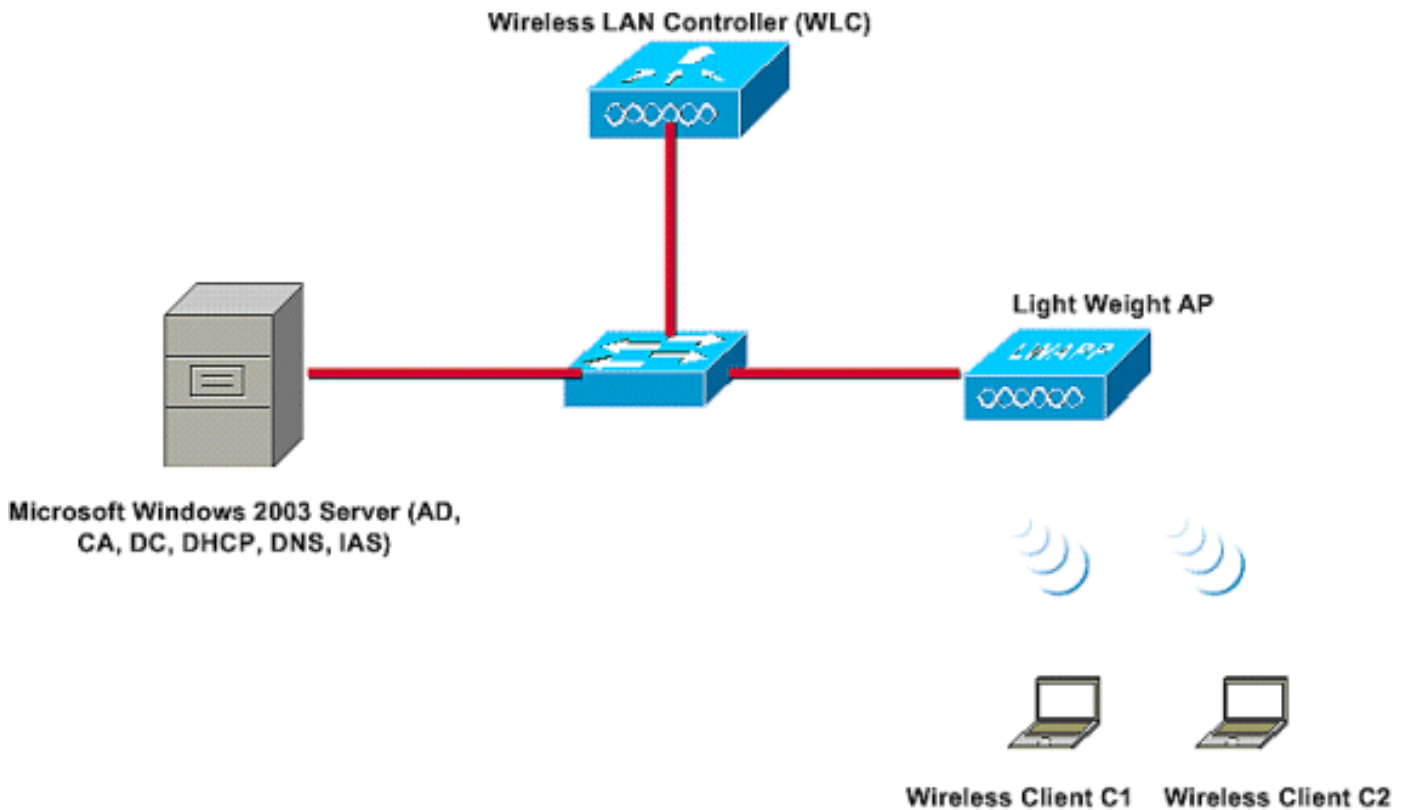
## **[Configurer](#)**

Ce document fournit un exemple pour la configuration de PEAP MS-CHAP v2.

**Remarque :** utilisez l'[outil de recherche de commandes](#) (clients [enregistrés](#) uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

## Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Dans cette configuration, un serveur de Microsoft Windows 2003 effectue ces rôles :

- Contrôleur de domaine pour le domaine de routage **Wireless.com**
- Serveur DHCP/DNS
- Serveur d'Autorité de certification (CA)
- Active Directory - pour mettre à jour la base de données utilisateur
- Service d'authentification Internet (IAS) - pour authentifier les utilisateurs sans fil

Ce serveur se connecte au réseau câblé par un commutateur de la couche 2 comme montré.

Le contrôleur LAN sans fil (WLC) et le LAP enregistré se connectent également au réseau par le commutateur de la couche 2.

Les clients sans fil C1 et C2 emploieront le Wi-Fi Protected Access 2 (WPA2) - authentification PEAP MSCHAP v2 pour se connecter au réseau sans fil.

L'objectif est de configurer le serveur de Microsoft 2003, le contrôleur LAN sans fil et le poids léger AP pour authentifier les clients sans fil avec l'authentification PEAP MSCHAP v2.

La section suivante explique comment paramétrer les périphériques pour cette configuration.

## Configurations

Cette section traite de la configuration requise pour installer l'authentification PEAP MS-CHAP v2 dans ce WLAN :

- Configurez le serveur de Microsoft Windows 2003
- Configurer le contrôleur LAN sans fil (WLC) et les AP de poids léger
- Configurez les clients sans fil

Commencez par la configuration du serveur de Microsoft Windows 2003.

## [Configurez le serveur de Microsoft Windows 2003](#)

### [Configurez le serveur de Microsoft Windows 2003](#)

Comme mentionné dans la section de configuration réseau, utilisez le serveur de Microsoft Windows 2003 dans le réseau pour remplir ces fonctions.

- **Contrôleur de domaine – pour le domaine sans fil**
- **Serveur DHCP/DNS**
- **Serveur d'Autorité de certification (CA)**
- **Service d'authentification Internet (IAS) - pour authentifier les utilisateurs sans fil**
- **Active Directory - pour mettre à jour la base de données utilisateur**

Configurez le serveur de Microsoft Windows 2003 pour ces services. Commencez par la configuration du serveur de Microsoft Windows 2003 comme contrôleur de domaine.

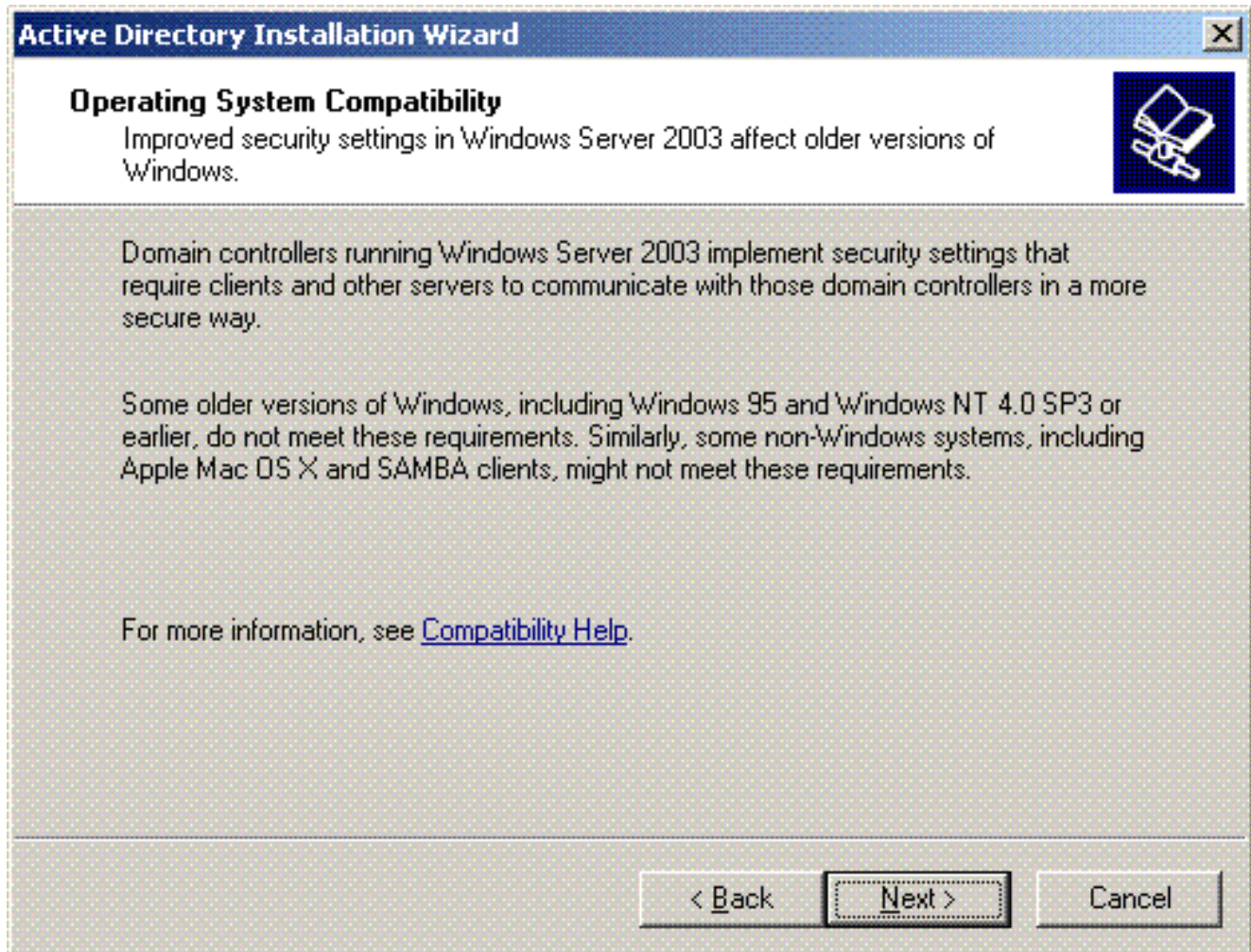
### **Configurez le serveur de Microsoft Windows 2003 comme contrôleur de domaine**

Afin de configurer le serveur de Microsoft Windows 2003 comme contrôleur de domaine, suivez ces étapes :

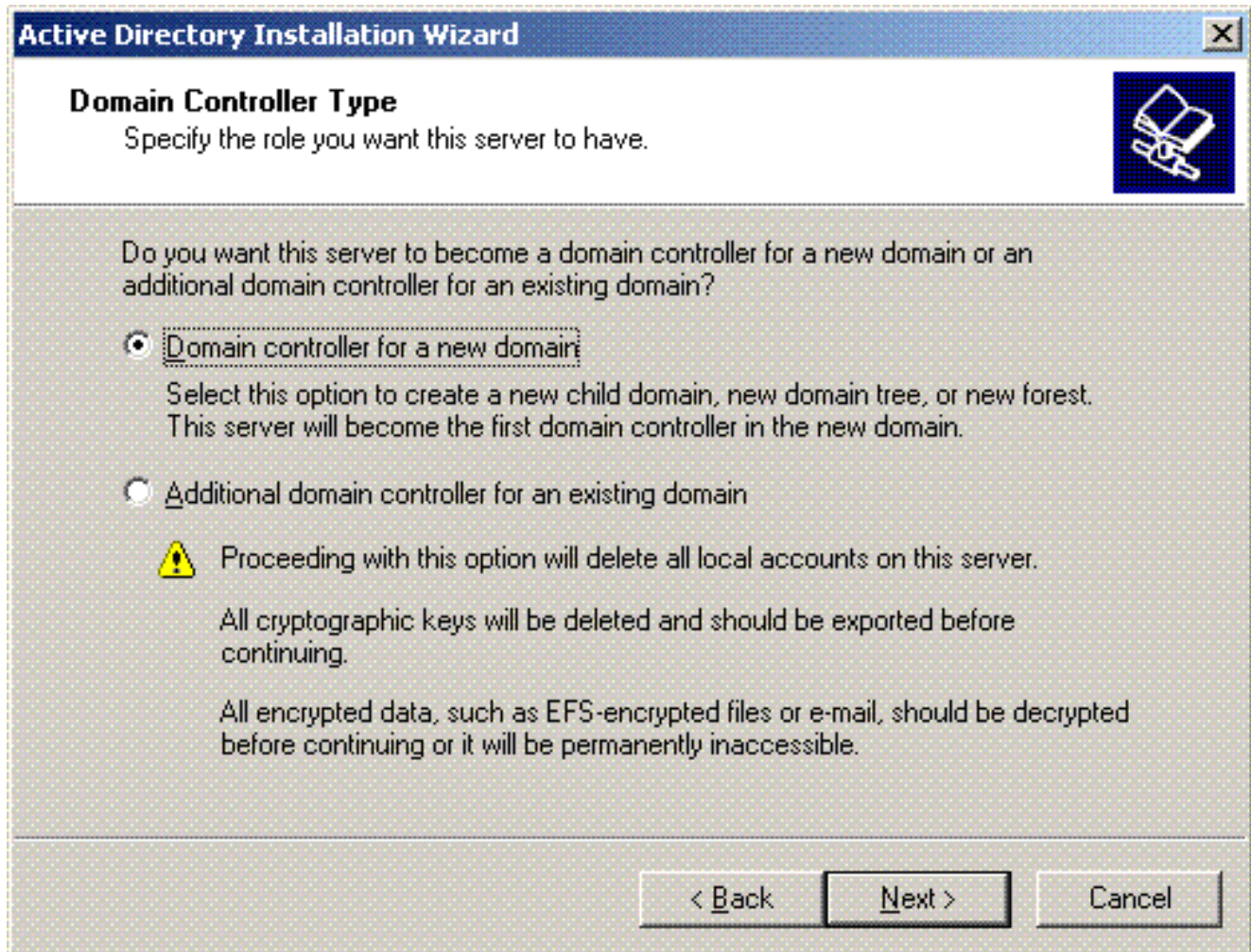
1. Cliquez sur **Start**, cliquez sur **Run**, saisissez `dcpromo.exe`, puis cliquez sur OK pour démarrer l'assistant d'installation d'Active Directory.



2. Cliquer sur **Next** to exécute l'assistant d'installation d'Active Directory.

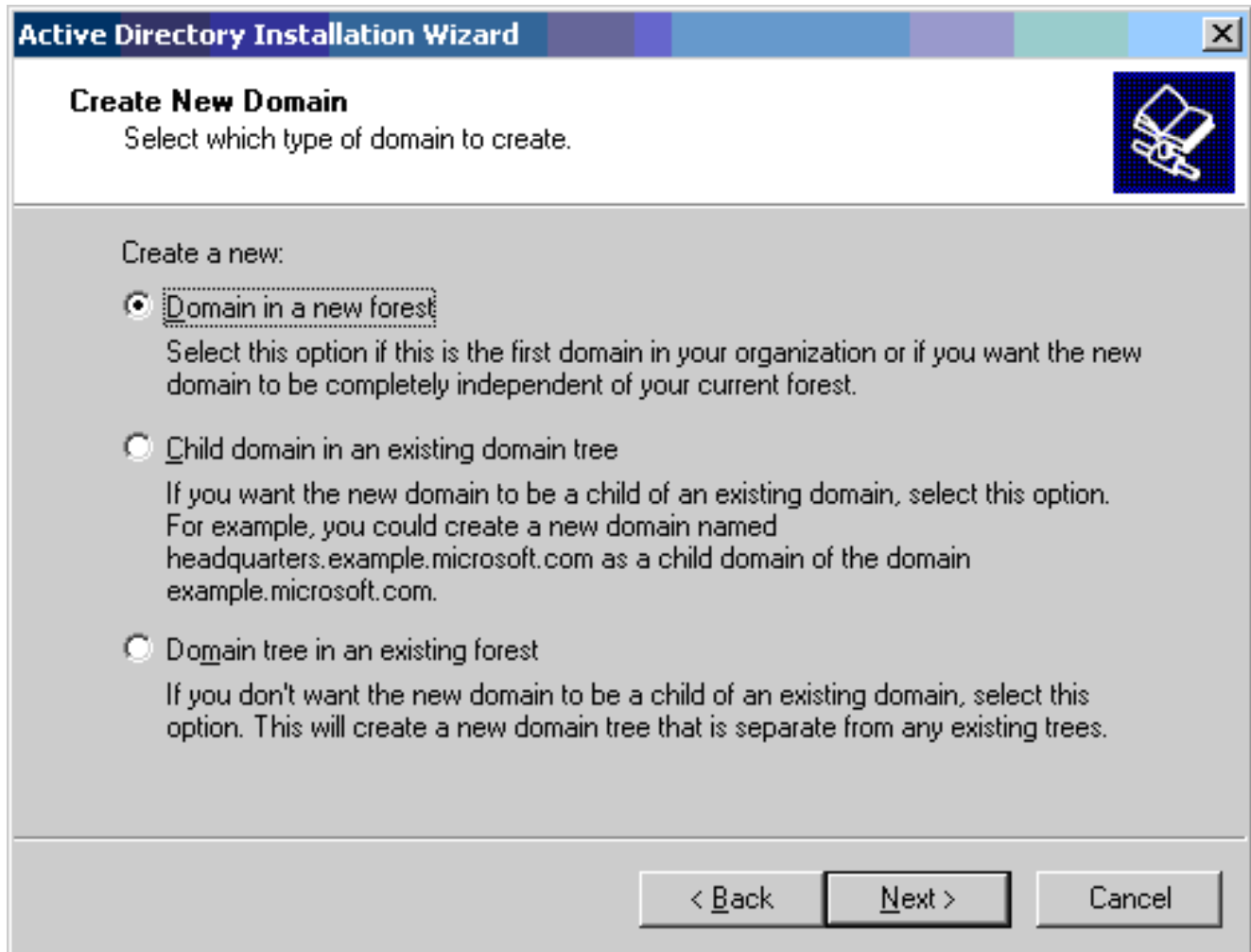


3. Afin de créer un nouveau domaine, choisissez l'option **Contrôleur de domaine pour un nouveau domaine**.

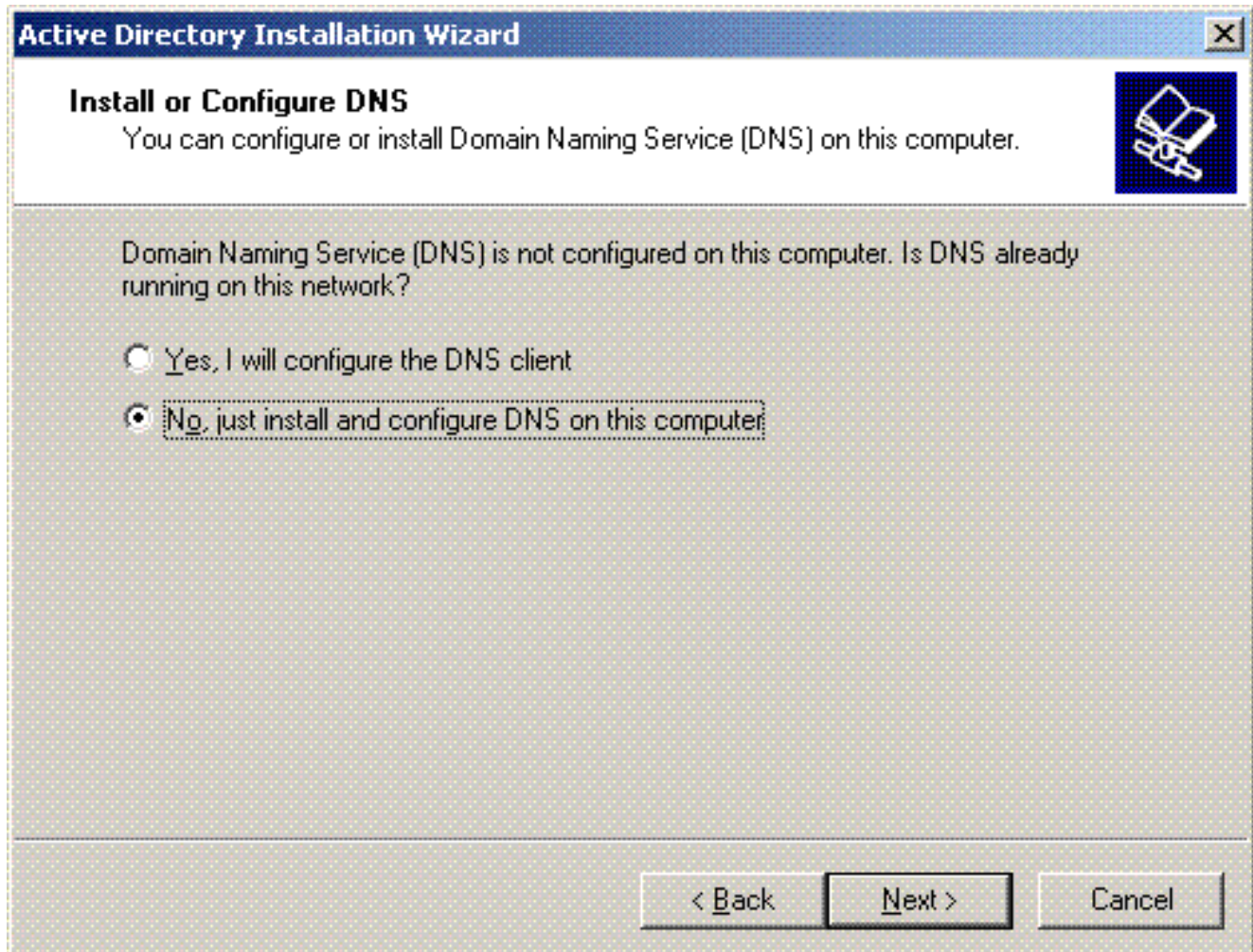


4. Cliquer sur **Next** to créer une nouvelle forêt d'arborescences de domaine.





5. Si DNS n'est pas installé dans le système, l'assistant vous fournit des options avec lesquelles configurer DNS. Choisissez **No, Just Install and Configure DNS sur cet ordinateur**. Cliquez sur **Next** (Suivant).



6. Introduisez le nom DNS complet pour le nouveau domaine de routage. Dans cet exemple **Wireless.com** est utilisé, puis cliquez sur **Next**.

**Active Directory Installation Wizard** [X]

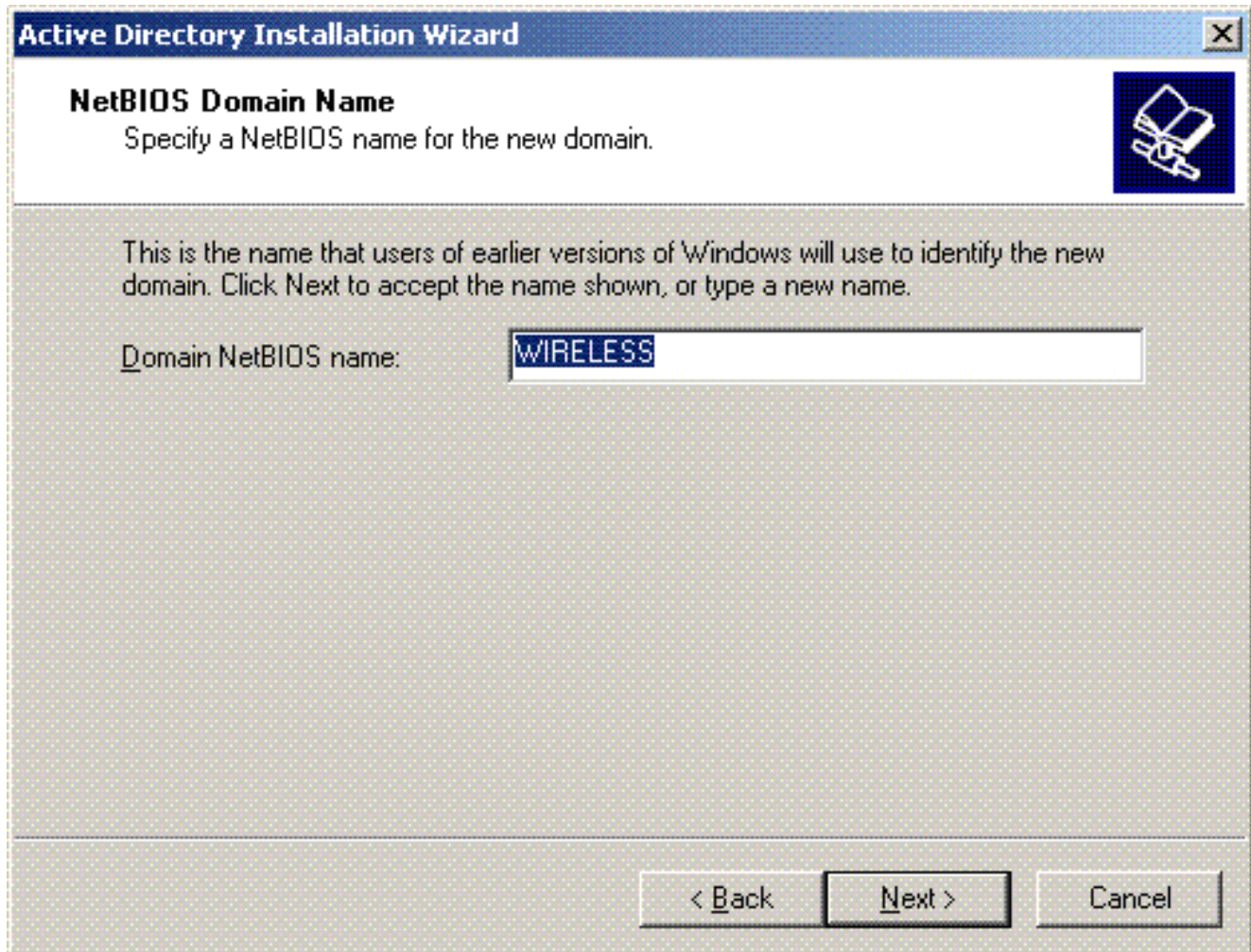
**New Domain Name**  
Specify a name for the new domain.

Type the full DNS name for the new domain  
(for example: headquarters.example.microsoft.com).

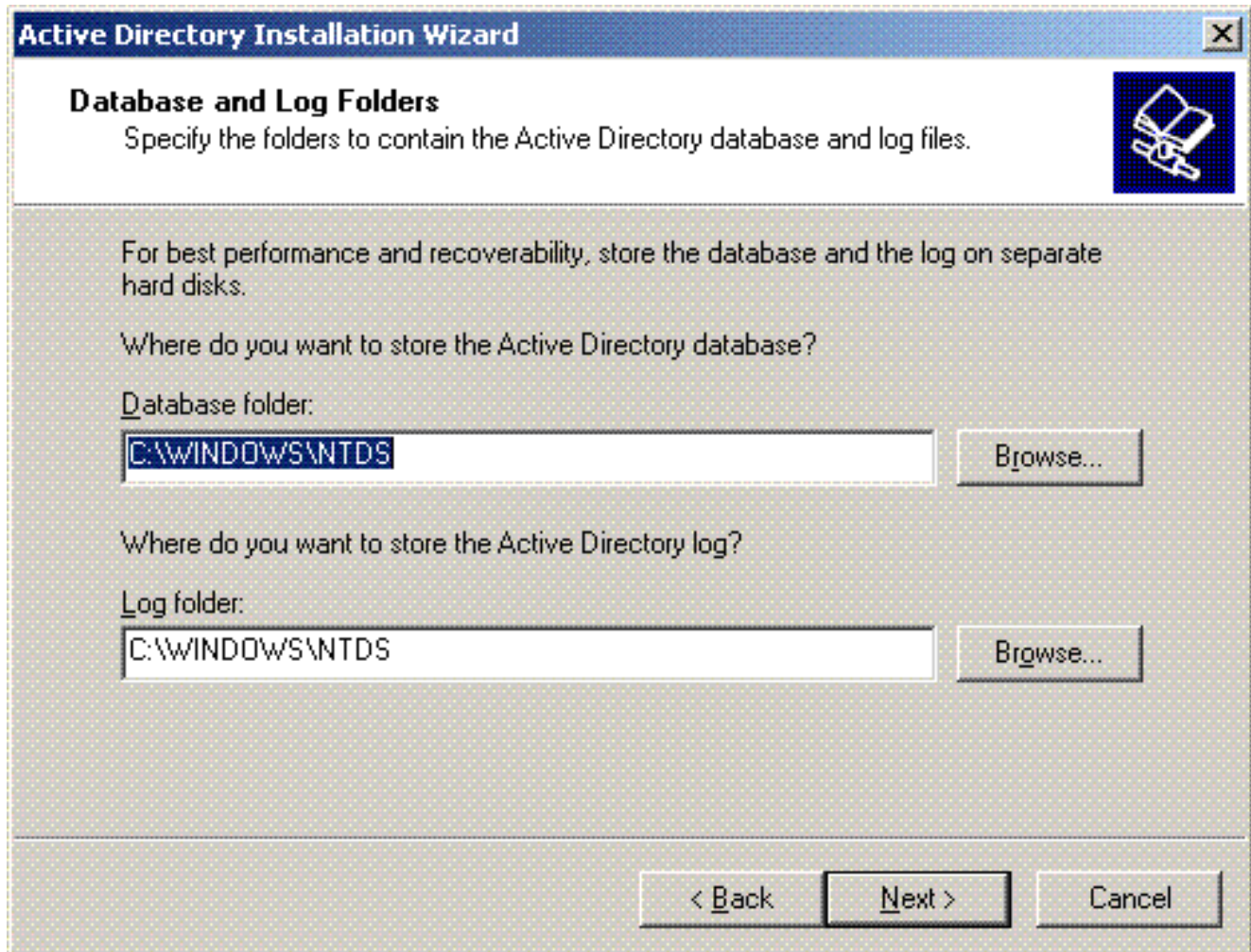
Full DNS name for new domain:

< Back   Next >   Cancel

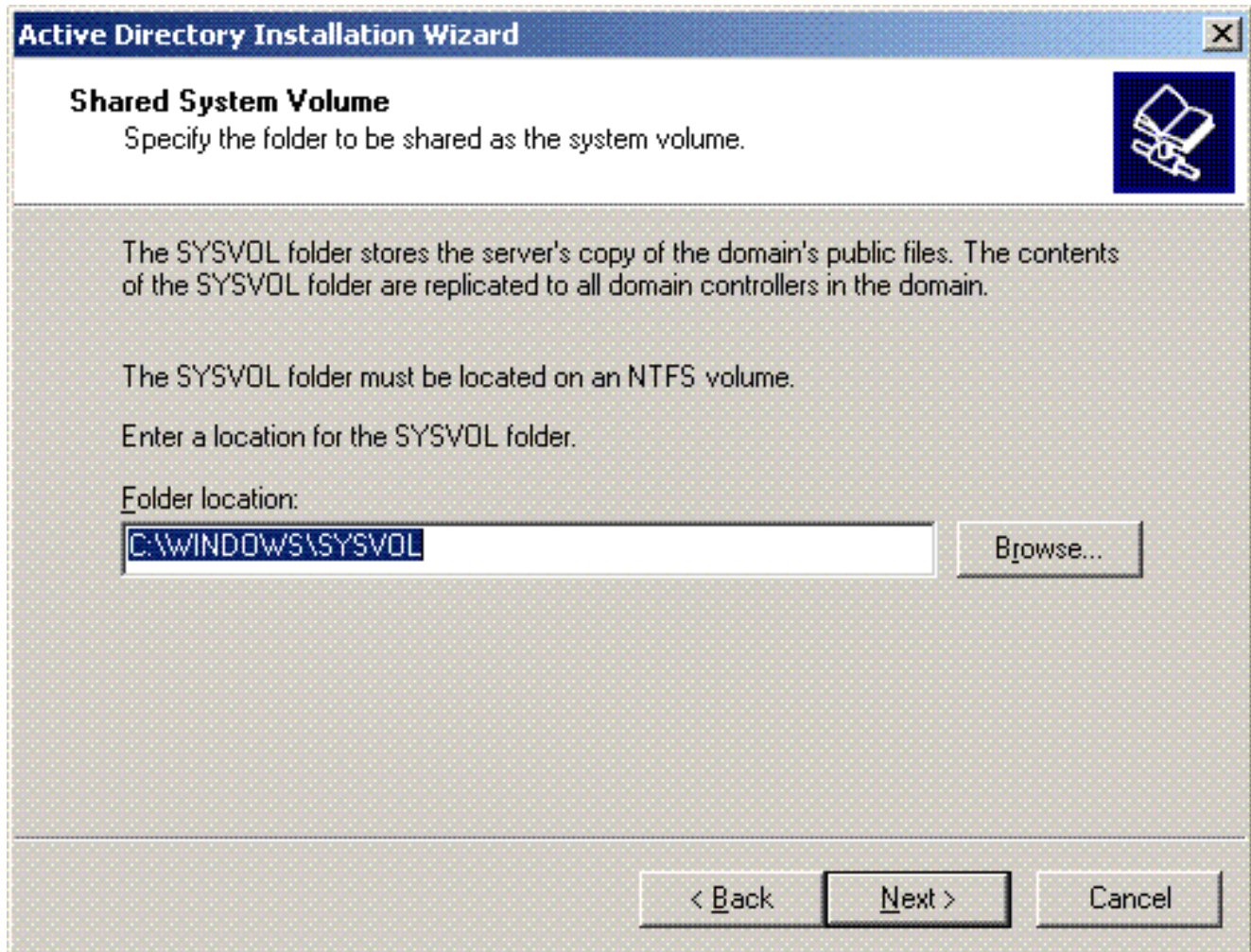
7. Écrivez le nom NetBIOS pour le domaine de routage, puis cliquez sur **Next**. Cet exemple utilise **WIRELESS**.



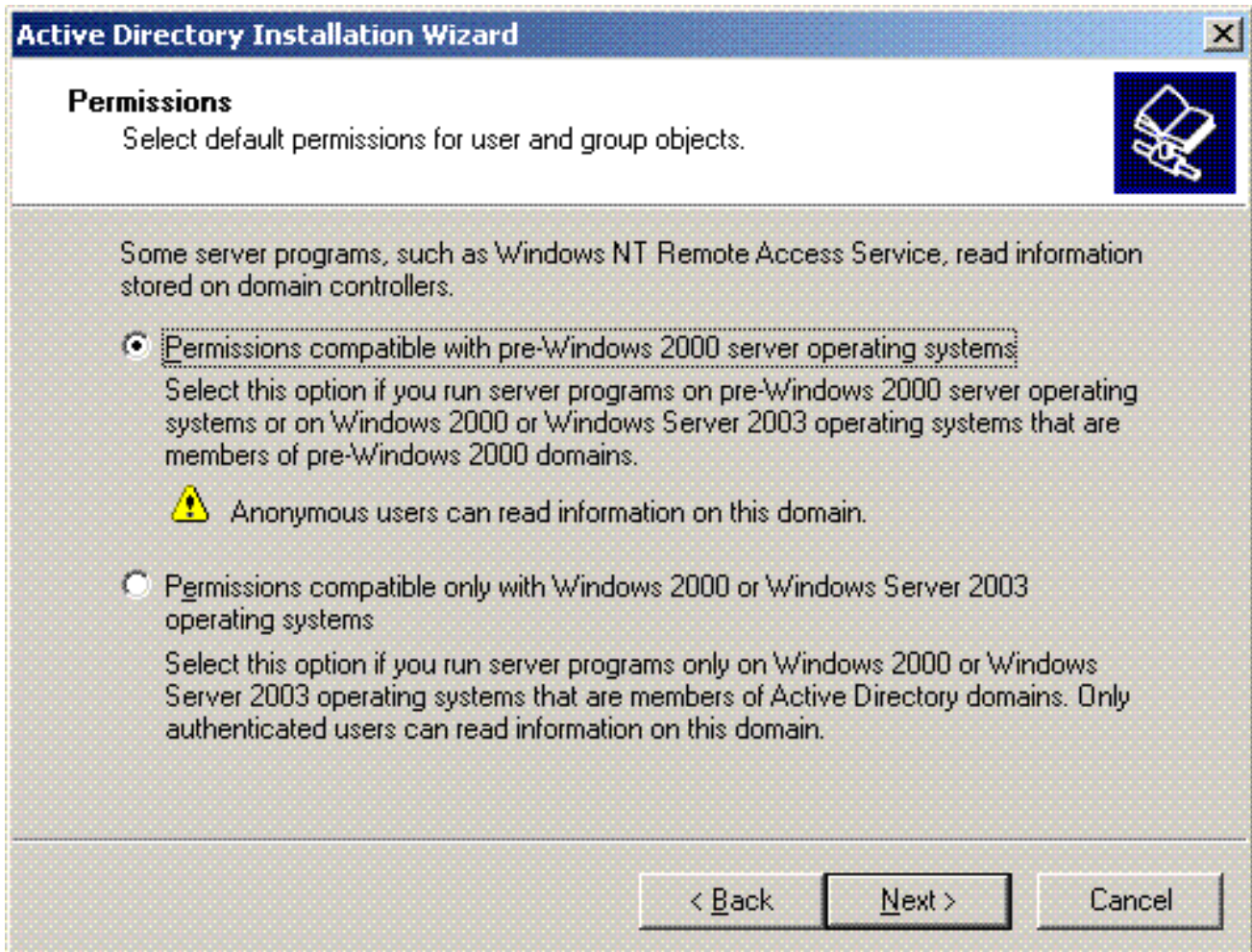
8. Choisissez la base de données et consignez les emplacements pour le domaine. Cliquez sur **Next** (Suivant).



9. Choisissez un emplacement pour le répertoire de Sysvol. Cliquez sur **Next** (Suivant).



10. Choisissez les autorisations par défaut pour les utilisateurs et les groupes. Cliquez sur **Next** (Suivant).




11. Définissez le mot de passe administrateur, puis cliquez sur **Next**.

**Active Directory Installation Wizard** [X]

### Directory Services Restore Mode Administrator Password

This password is used when you start the computer in Directory Services Restore Mode.



Type and confirm the password you want to assign to the Administrator account used when this server is started in Directory Services Restore Mode.

The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both.

Restore Mode Password:

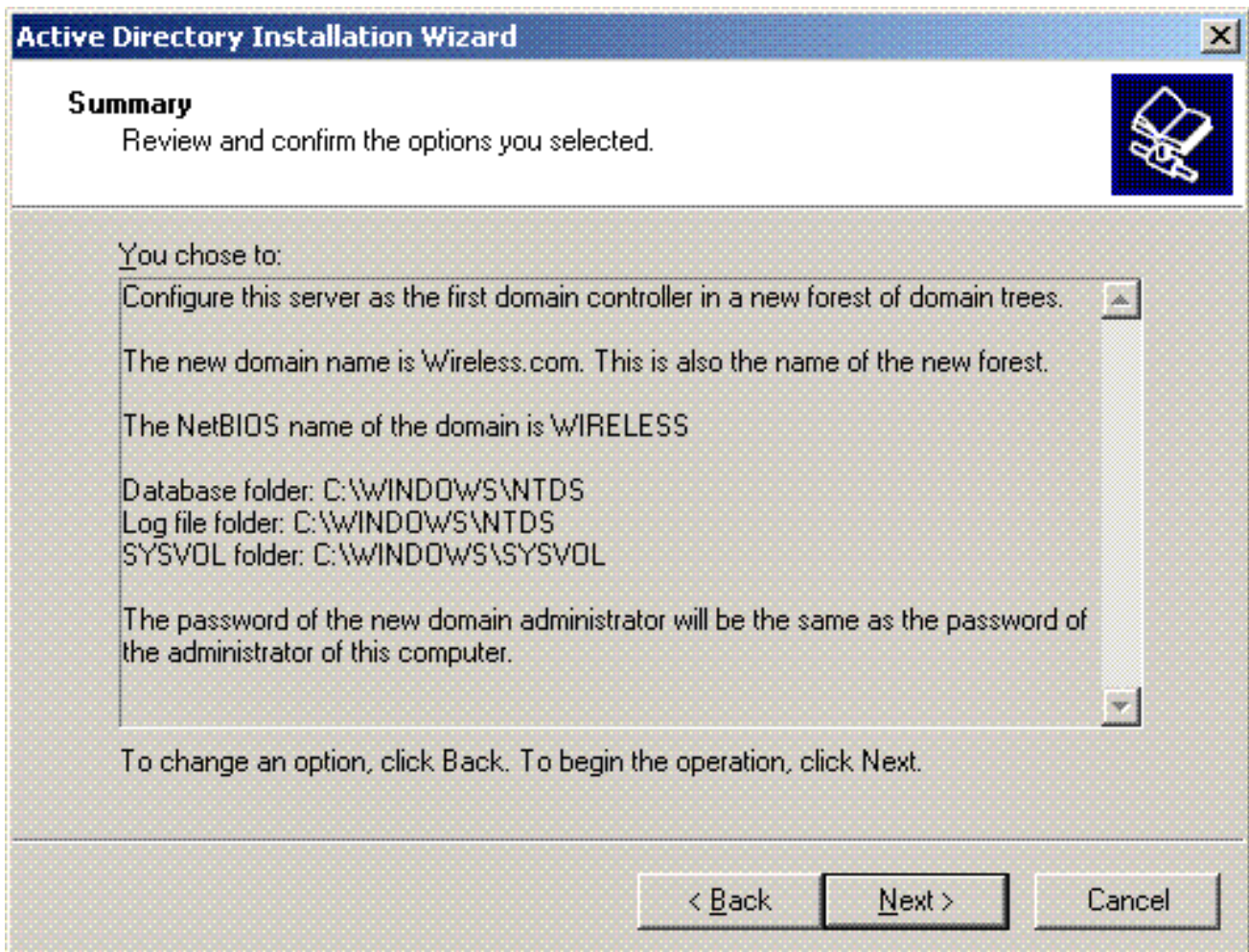
Confirm password:

For more information about Directory Services Restore Mode, see [Active Directory Help](#).

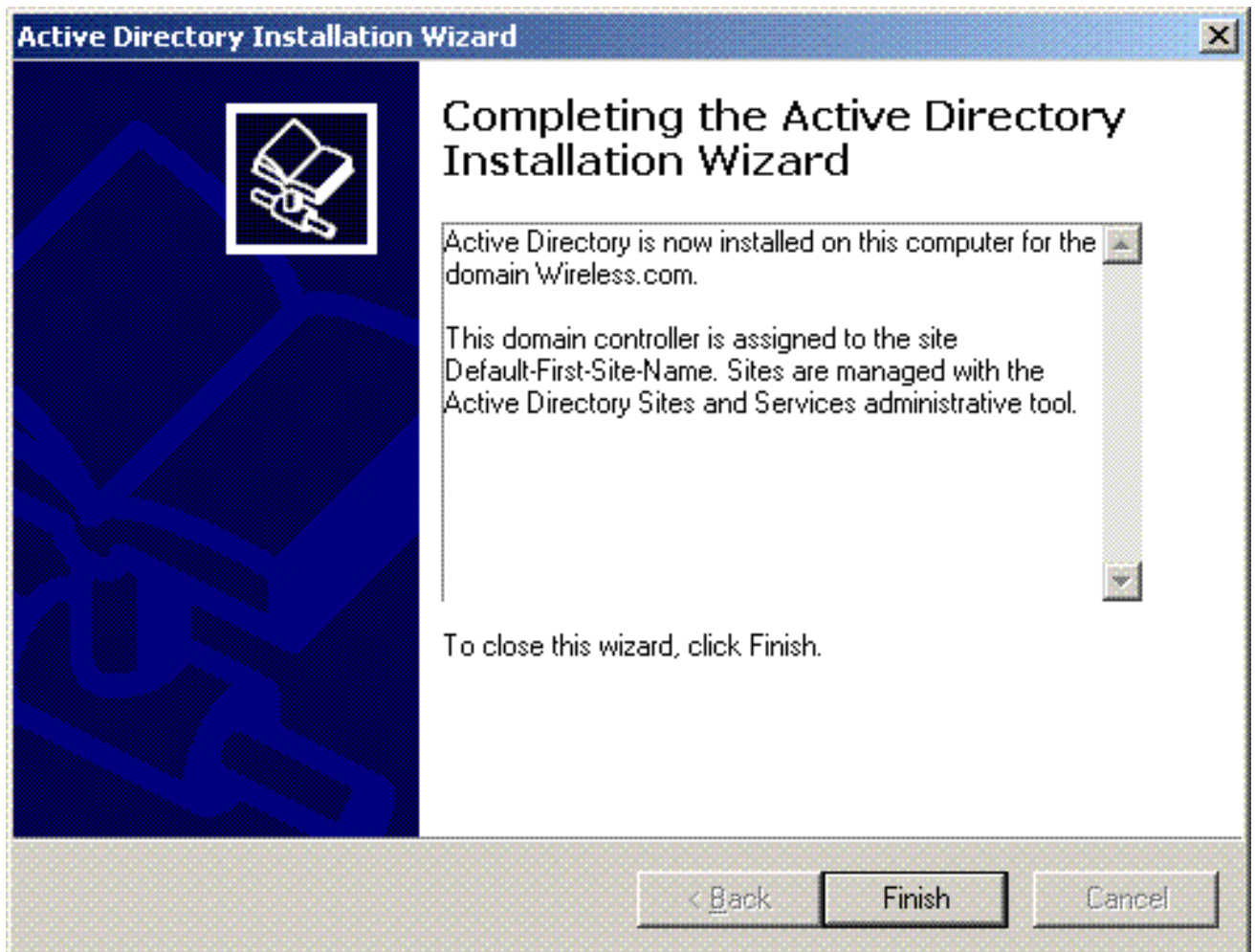
< Back   Next >   Cancel

12. Cliquer sur **Next** pour confirmer les options de domaine définies précédemment.

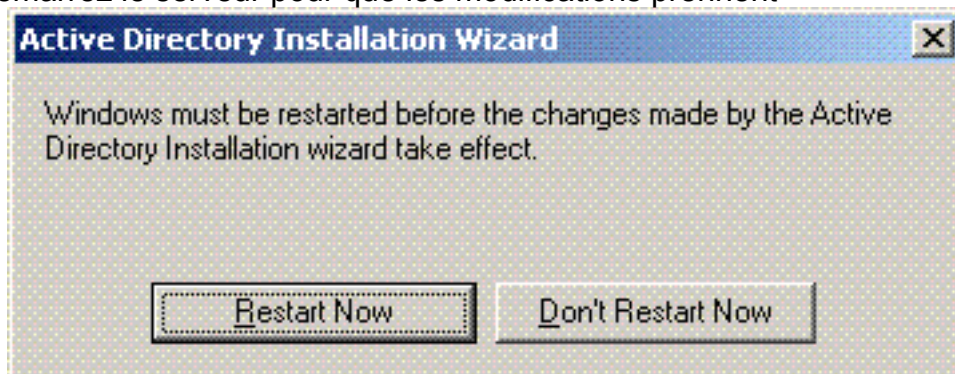




13. Cliquez sur **Finish** pour fermer l'assistant d'installation d'Active Directory.



14. Redémarrez le serveur pour que les modifications prennent



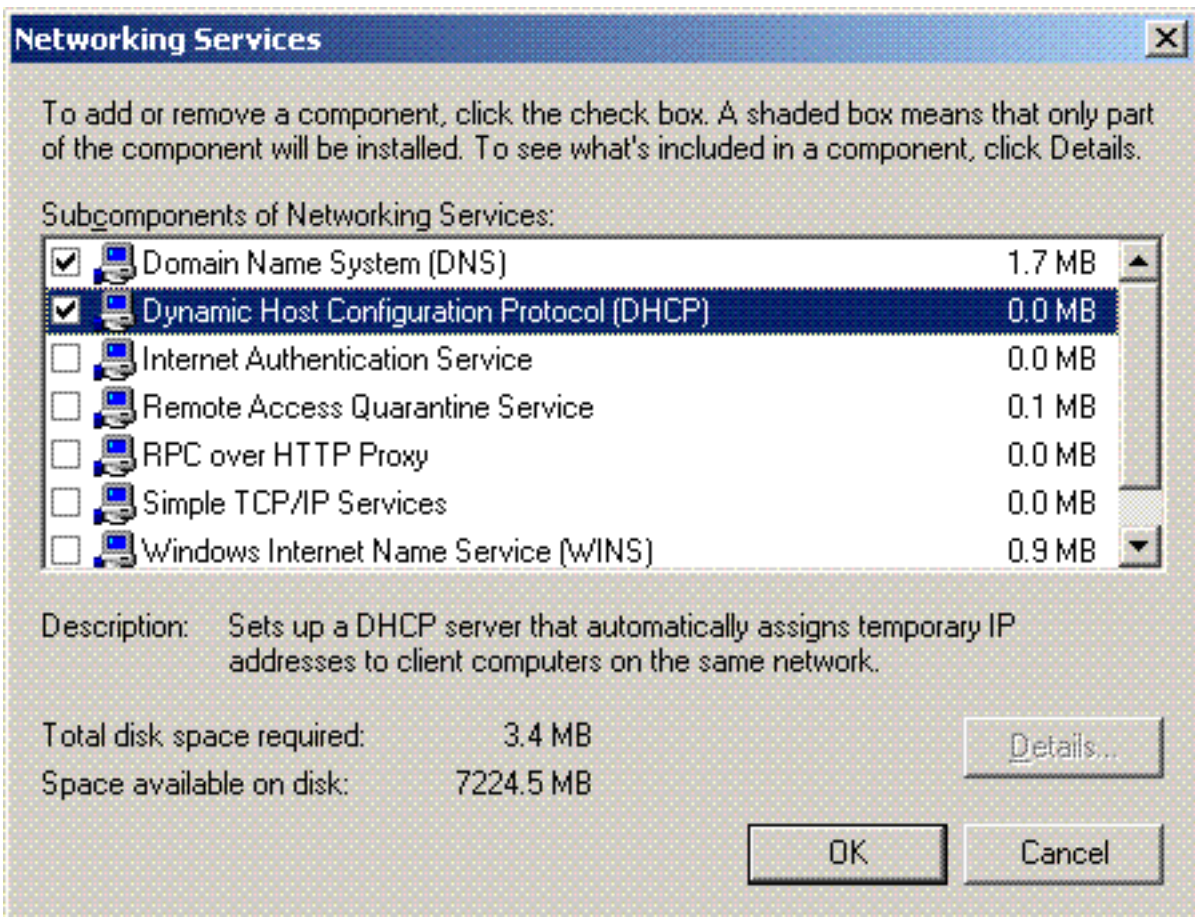
effet.

Au cours de cette étape, vous avez configuré le serveur de Microsoft Windows 2003 comme contrôleur de domaine et avez créé un nouveau domaine de routage **Wireless.com**. Configurez ensuite les services DHCP sur le serveur.

### [Installez et configurez les services DHCP sur le serveur de Microsoft Windows 2003](#)

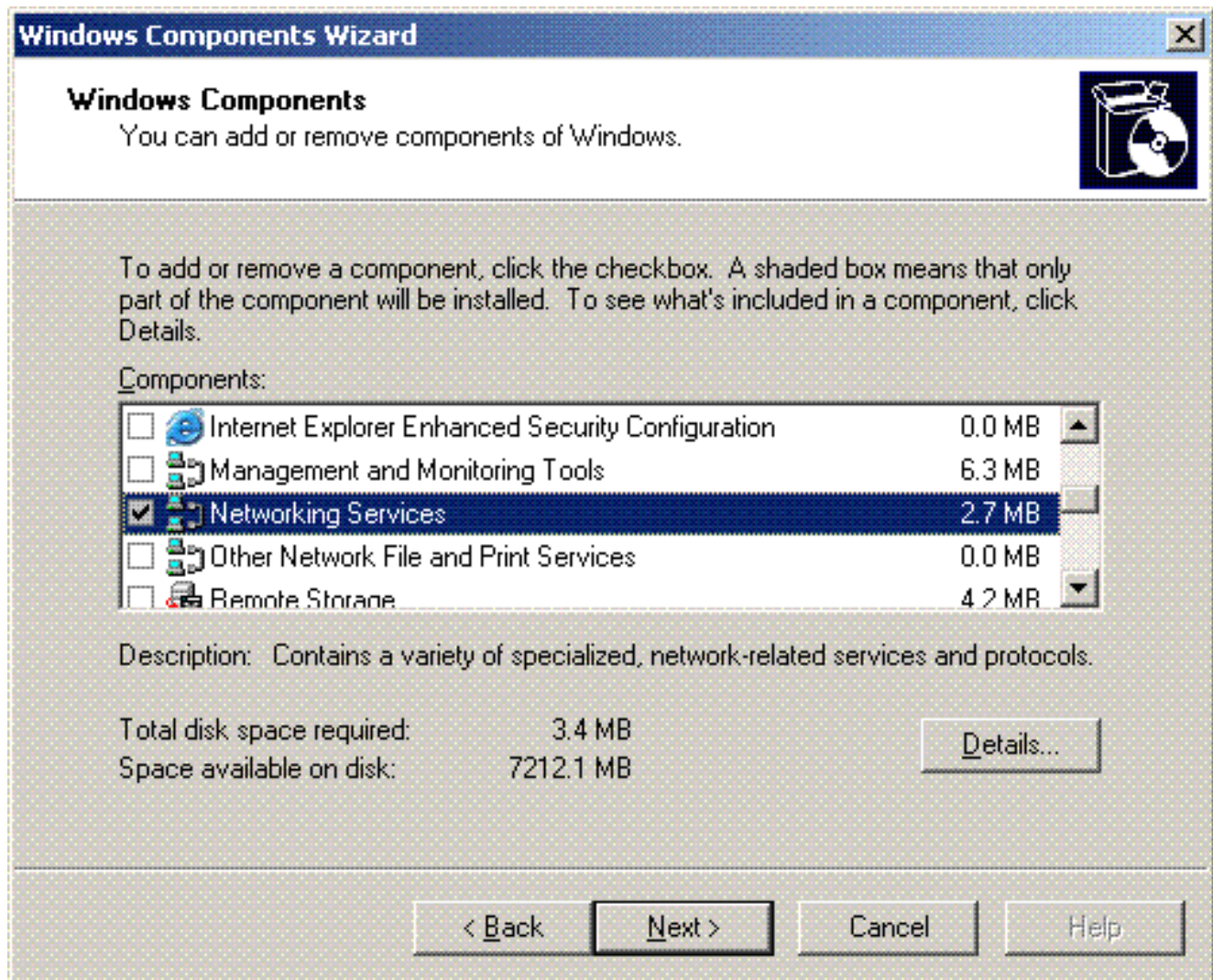
Le service DHCP sur le serveur de Microsoft 2003 est utilisé pour fournir des adresses IP aux clients sans fil. Afin d'installer et de configurer des services DHCP sur ce serveur, suivez ces étapes :

1. Cliquez sur **Add or Remove Programs** dans le panneau de configuration.
2. Cliquez sur **Add/Remove Windows Components**.
3. Choisissez **Networking Services**, puis cliquez sur **Details**.
4. Choisissez **Dynamic Host Configuration Protocol (DHCP)**, puis cliquez sur



OK.

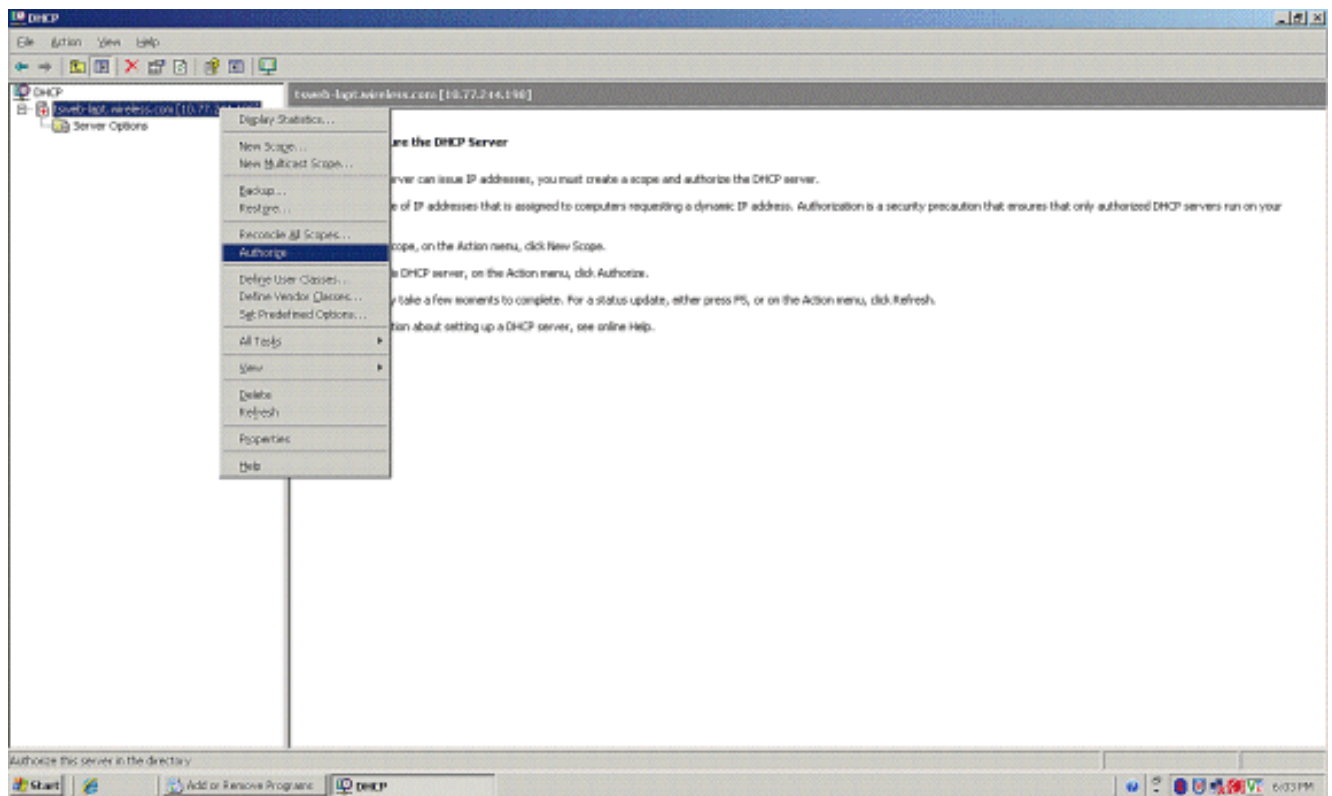
5. Cliquer sur **Next** pour installer le service **DHCP**.



6. Cliquez sur **Finish** pour terminer l'installation.



7. Afin de configurer des services DHCP, cliquez sur **Start > Programs > Administrative tools** , puis cliquez sur le jeu d'outils **DHCP**.
8. Choisissez le serveur DHCP - **tsweb-lapt.wireless.com** (dans cet exemple).
9. Cliquez sur **Action**, puis cliquez sur **Authorize** pour autoriser le service DHCP.



10. Dans l'arborescence de la console, cliquez à droite sur **tsweb-lapt.wireless.com**, puis cliquez sur **New Scope** pour définir une plage d'adresses IP pour les clients sans fil.
11. Sur la page de bienvenue de l'assistant de New Scope, cliquez sur **Next**.



12. À la page du nom de portée, saisissez le nom de la portée DHCP. Dans cet exemple, utilisez **DHCP-Clients** comme nom de portée. Cliquez sur **Next**

(Suivant).

**New Scope Wizard**

**Scope Name**

You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name: DHCP-Clients

Description: DHCP Server for Wireless Clients

< Back   Next >   Cancel

13. À la page de plage d'adresses IP, saisissez les adresses IP de début et de fin pour la portée, puis cliquez sur **Next**.

## New Scope Wizard

### IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.



Enter the range of addresses that the scope distributes.

Start IP address: 10 . 77 . 244 . 218

End IP address: 10 . 77 . 244 . 219

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length: 8

Subnet mask: 255 . 0 . 0 . 0

< Back

Next >

Cancel

14. Sur la page d'ajout des exclusions, mentionnez l'adresse IP que vous voudriez réserver/exclure de la portée DHCP. Cliquez sur **Next** (Suivant).



## New Scope Wizard

### Add Exclusions

Exclusions are addresses or a range of addresses that are not distributed by the server.



Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:

End IP address:

Add

Excluded address range:

Remove

< Back

Next >

Cancel

15. Mentionnez la durée de bail dans la page de durée de bail, puis cliquez sur **Next**.

## New Scope Wizard

### Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.



Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days:	Hours:	Minutes:
<input type="text" value="8"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

< Back

Next >

Cancel

16. Sur la page des options de configuration DHCP, choisissez **Yes, I want to configure DHCP Option now**, puis cliquez sur **Next**.

## New Scope Wizard

### Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.



When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

- Yes, I want to configure these options now
- No, I will configure these options later

< Back

Next >

Cancel

17. S'il existe un routeur de passerelle par défaut, mentionnez l'adresse IP du routeur de passerelle dans la page du routeur (passerelle par défaut), puis cliquez sur **Next**.

## New Scope Wizard

### Router (Default Gateway)

You can specify the routers, or default gateways, to be distributed by this scope.



To add an IP address for a router used by clients, enter the address below.

IP address:

Add

Remove

Up

Down

< Back

Next >

Cancel

18. Sur la page du nom du domaine et des serveurs DNS, introduisez le nom du domaine qui a été configuré précédemment. Dans l'exemple, utilisez **Wireless.com**. Saisissez l'adresse IP du serveur. Cliquez sur **Add**.

## New Scope Wizard

### Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.



You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:

IP address:

Add

Resolve

Remove

Up

Down

< Back

Next >

Cancel

19. Cliquez sur **Next** (Suivant).
20. À la page de serveur WINS, cliquez sur **Next**.
21. Sur la page d'activation du champ, choisissez **Yes, I want to activate the scope now**, puis cliquez sur **Next**.

## New Scope Wizard

### Activate Scope

Clients can obtain address leases only if a scope is activated.



Do you want to activate this scope now?

- Yes, I want to activate this scope now
- No, I will activate this scope later

< Back

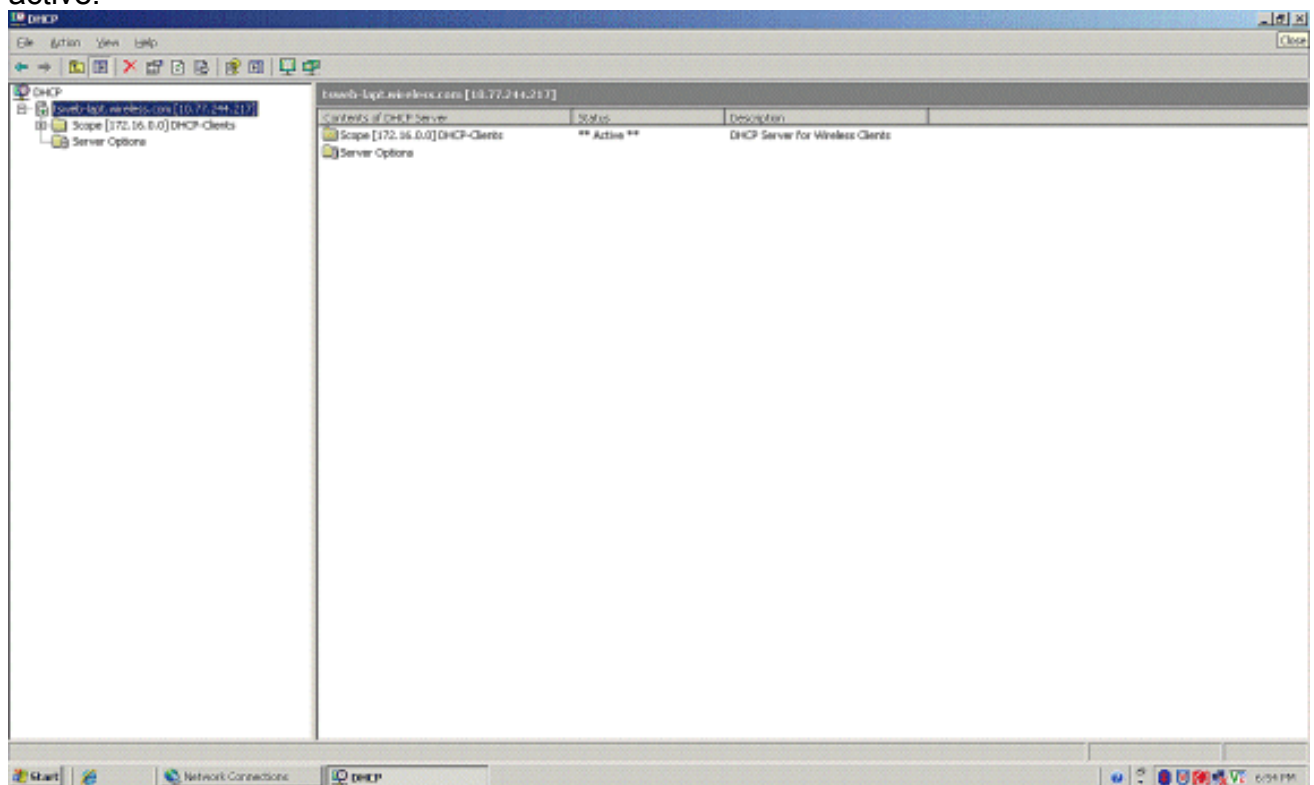
Next >

Cancel

22. Lorsque l'assistant de New Scope aura terminé, cliquez sur **Finish**.



23. Dans la fenêtre DHCP Snapin, vérifiez que la portée DHCP qui a été créée est active.



Maintenant que DHCP / DNS est activé sur le serveur, configurez le serveur en tant que serveur d'Autorité de certification (CA) d'entreprise.

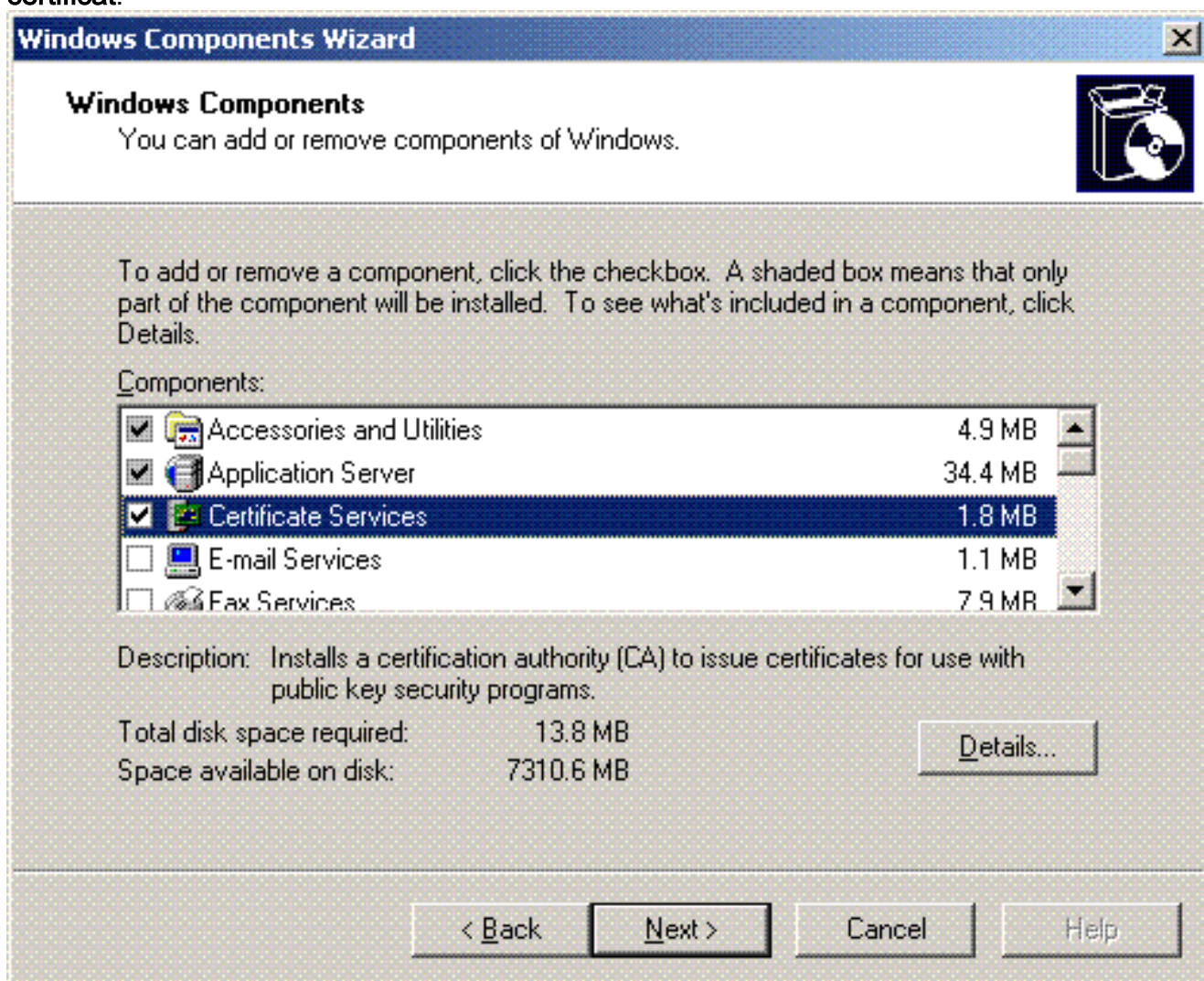
[Installez et configurez le serveur de Microsoft Windows 2003 en tant que serveur](#)

## d'Autorité de certification (CA)

Le PEAP avec EAP-MS-CHAPv2 valide le serveur RADIUS basé sur le certificat actuel sur le serveur. De plus, le certificat du serveur doit être délivré par une autorité publique de certification (CA) que l'ordinateur client considère comme étant de confiance (c'est-à-dire, le certificat public CA existe déjà dans le répertoire Trusted Root Certification Authority dans la mémoire des certificats de l'ordinateur client). Dans cet exemple, configurez le serveur de Microsoft Windows 2003 en tant qu'Autorité de certification (CA) qui fournit le certificat au Service d'authentification Internet (IAS).

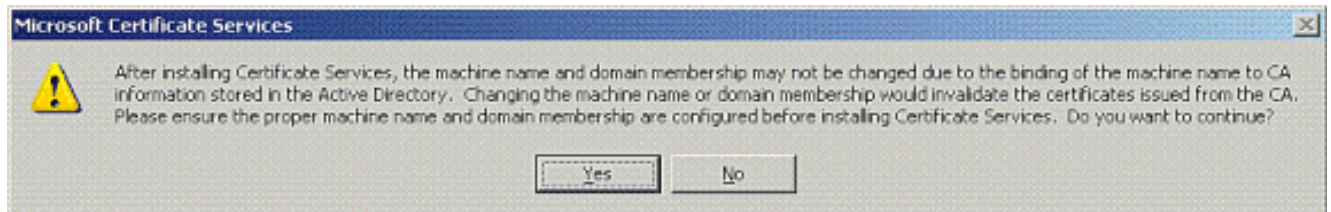
Afin d'installer et de configurer les services de certificat sur le serveur, suivez ces étapes :

1. Cliquez sur **Add or Remove Programs** dans le panneau de configuration.
2. Cliquez sur Add/Remove Windows Components.
3. Cliquez sur **Services de certificat**.

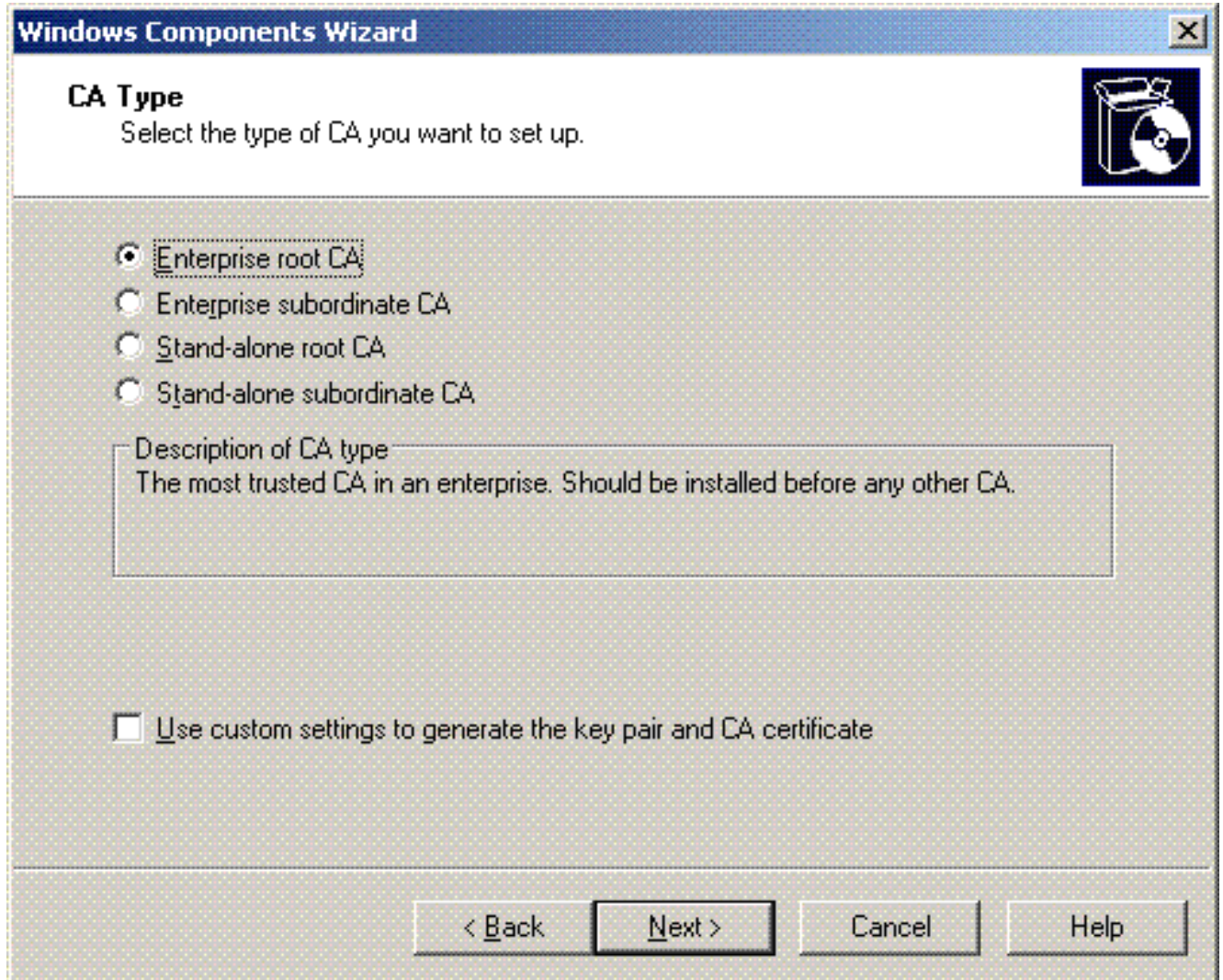


4. Cliquez sur **Yes** au message d'avertissement, après avoir installé les services de certificat, l'ordinateur ne peut pas être renommé, se connecter à un domaine ou être supprimé.  
**Voulez-vous continuer ?**






5. Sous le type d'autorité de certification, choisissez **Enterprise root CA**, puis cliquez sur **Next**.



6. Saisissez un nom pour identifier le CA. Cet exemple utilise **Wireless-CA**. Cliquez sur **Next** (Suivant).

**Windows Components Wizard** X

**CA Identifying Information**   
Enter information to identify this CA.

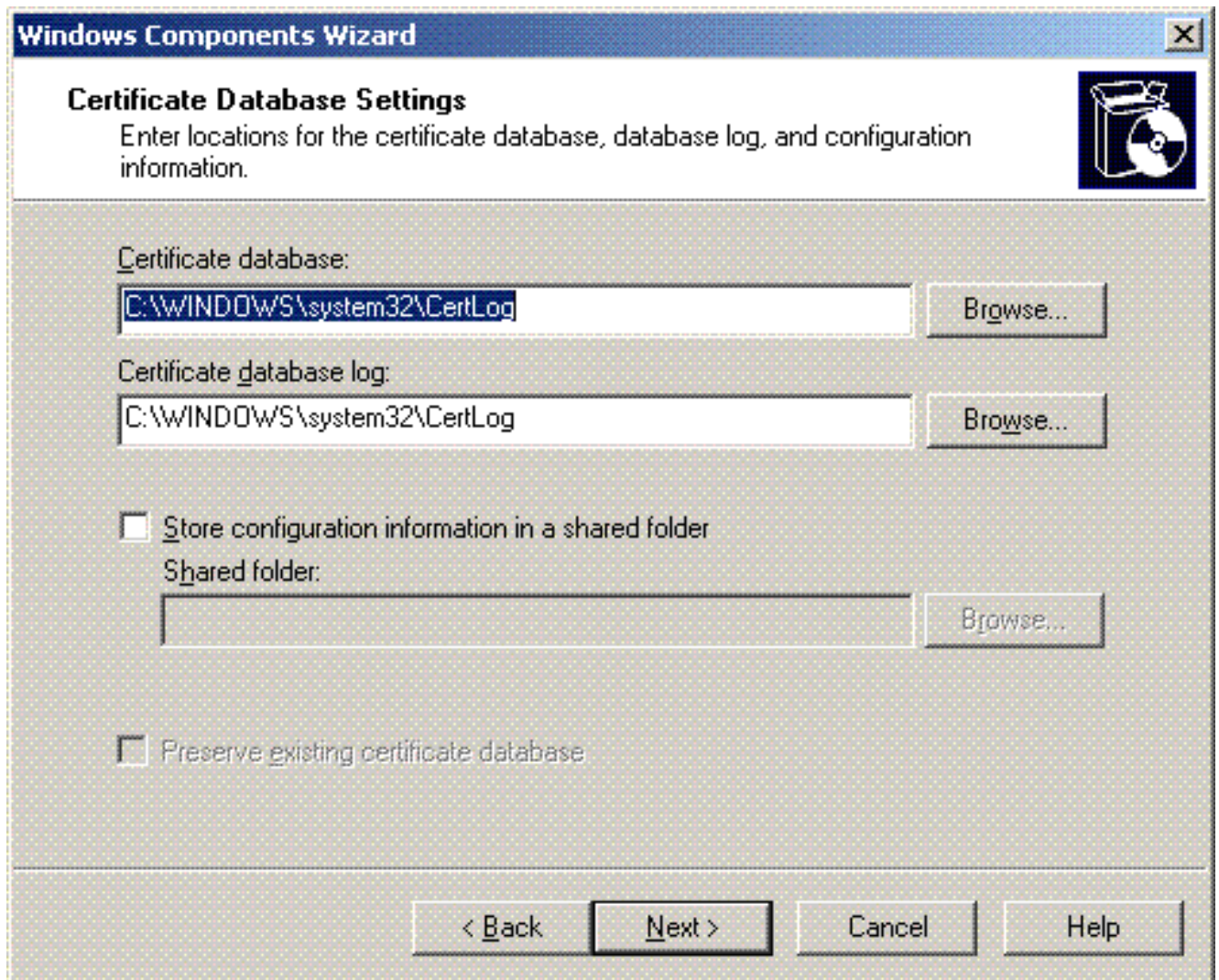
Common name for this CA:

Distinguished name suffix:

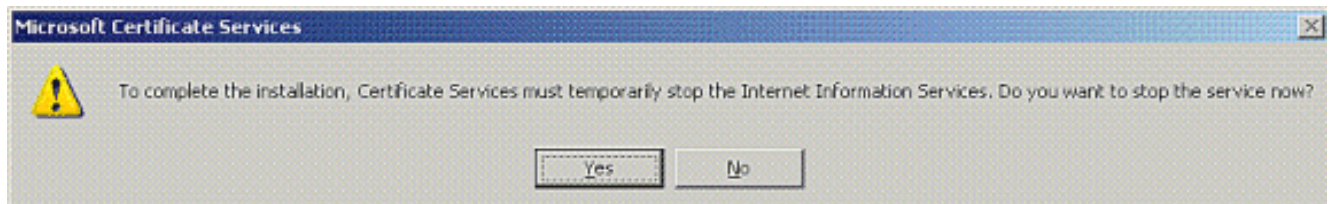
Preview of distinguished name:

Validity period:     
Expiration date: 12/12/2012 7:01 PM

7. Un répertoire « journal de certification » est créé pour le stockage de la base de données de certificats. Cliquez sur **Next** (Suivant).



8. Si IIS est activé, il doit être arrêté avant que vous poursuiviez. Cliquez sur **OK au message d'avertissement qu'IIS doit être arrêté**. Il redémarre automatiquement après l'installation du CA.



9. Cliquez sur **Finish** pour terminer l'installation des services d'Autorité de certification (CA).

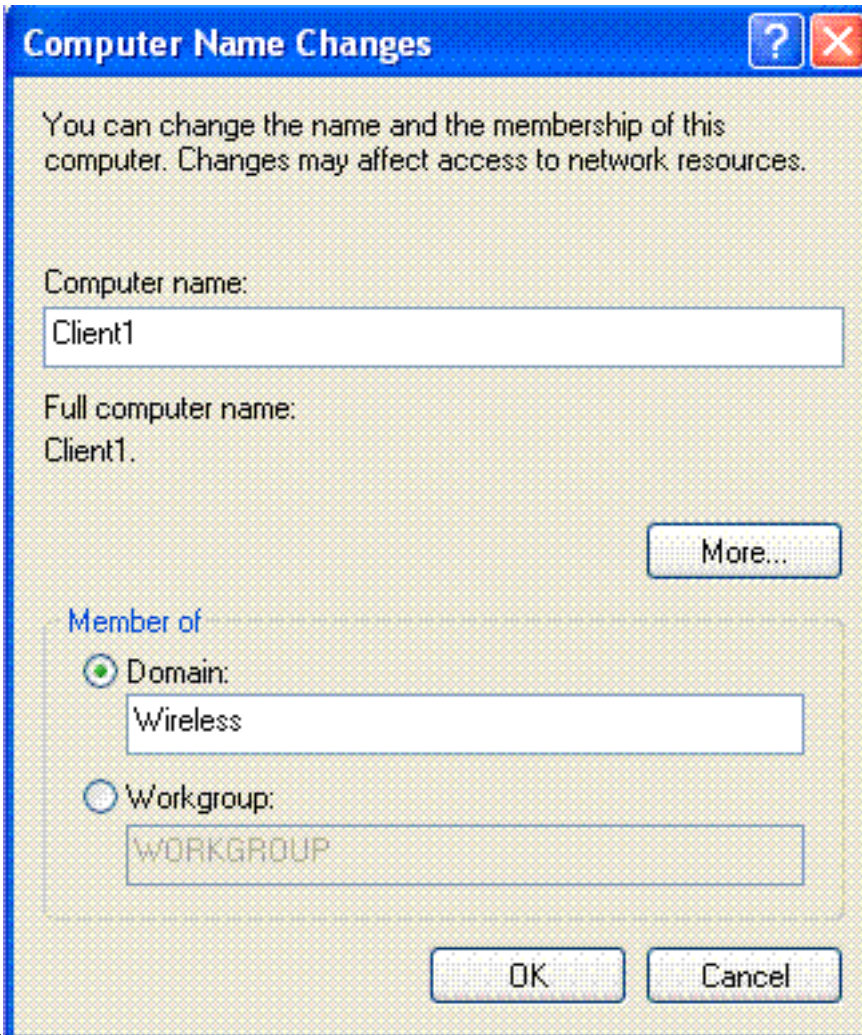


L'étape suivante consiste à installer et à configurer le Service d'authentification Internet sur le serveur de Microsoft Windows 2003.

### [Connectez les clients de routage au domaine de routage](#)

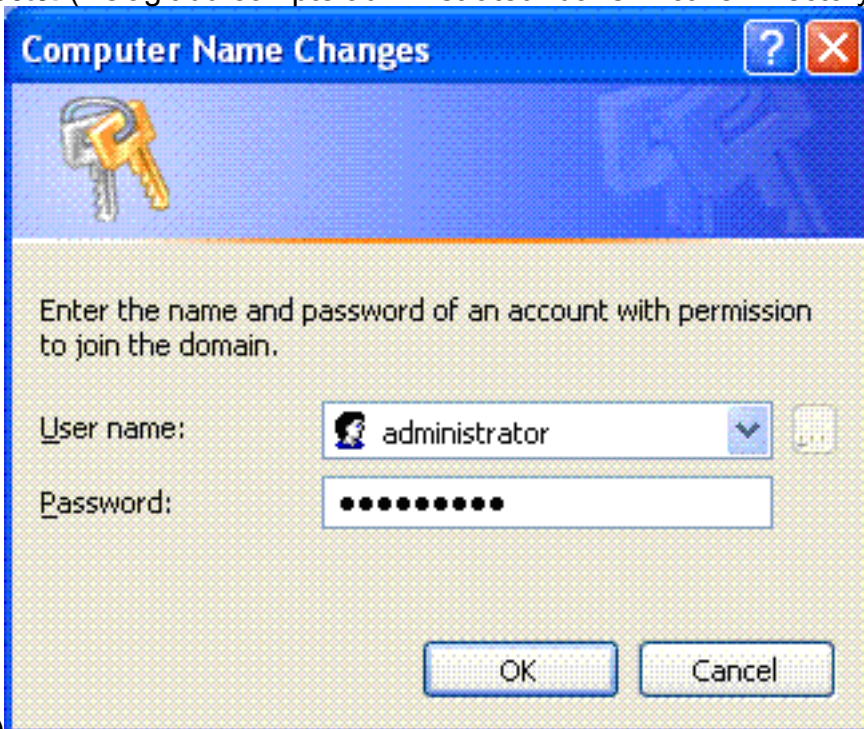
L'étape suivante consiste à connecter les clients au réseau câblé et à télécharger les informations spécifiques au domaine depuis le nouveau domaine. En d'autres termes, connectez les clients au domaine. Pour ce faire, suivez ces étapes :

1. Connectez les clients au réseau câblé avec une droite par un câble Ethernet.
2. Initialisez le client et la connexion avec le nom d'utilisateur/mot de passe du client.
3. Cliquez sur **Démarrer** ; cliquez sur **Exécuter** ; tapez **cmd** ; et cliquez sur **OK**.
4. À l'invite de commande, saisissez **ipconfig**, puis cliquez sur **Enter pour vérifier que le DHCP fonctionne correctement et que le client a reçu une adresse IP du server DHCP**.
5. Afin de connecter le client au domaine, cliquez à droite sur My Computer, puis choisissez **Properties**.
6. Cliquez sur l'onglet **Computer Name**.
7. Cliquez sur **Change**.
8. Cliquez sur **Domain** ; tapez **wireless.com** ; et cliquez sur



OK.

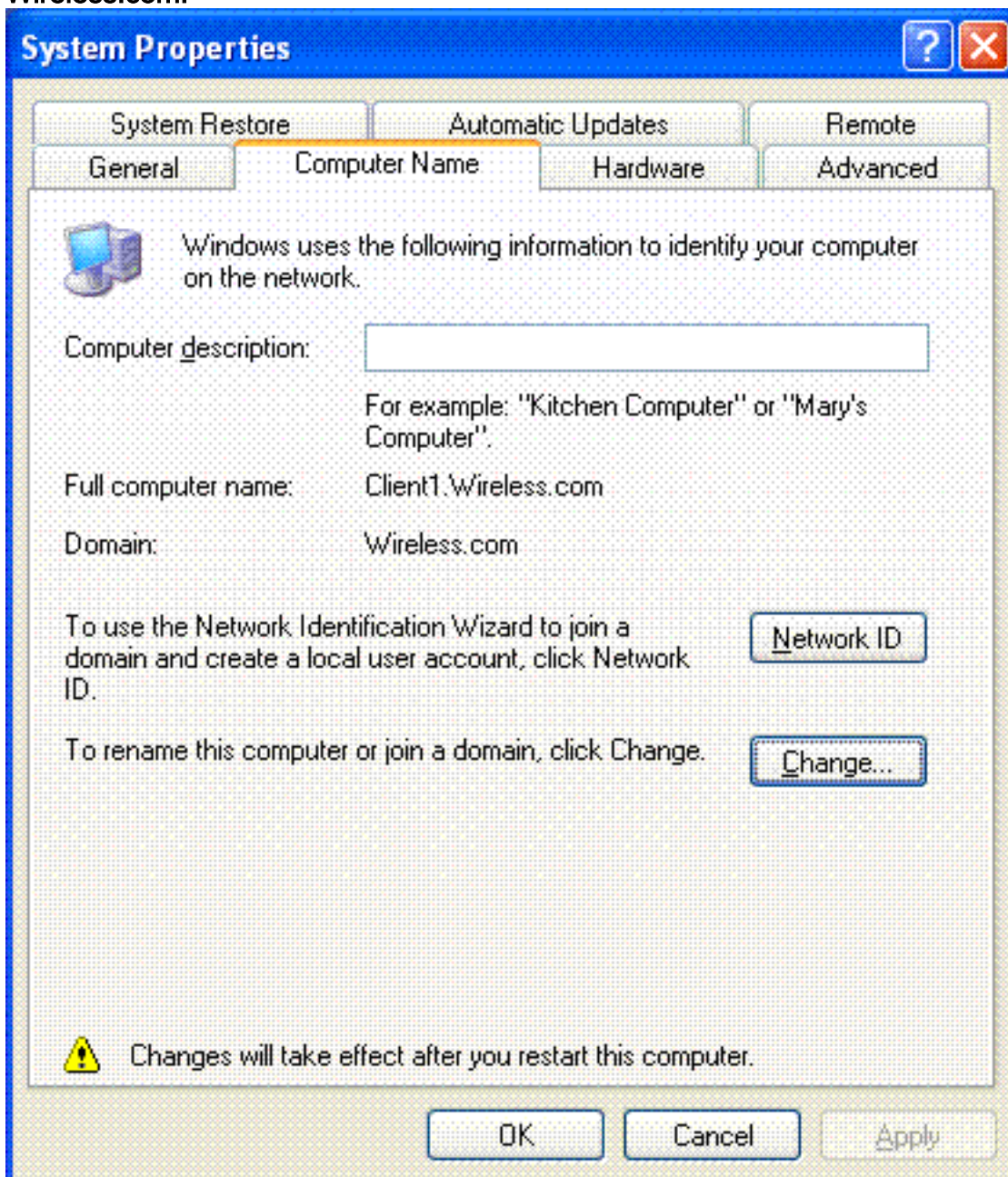
9. Saisissez **Username Administrator** et le mot de passe spécifique au domaine auquel le client se connecte. (Il s'agit du compte administrateur dans l'Active Directory sur le



serveur.)

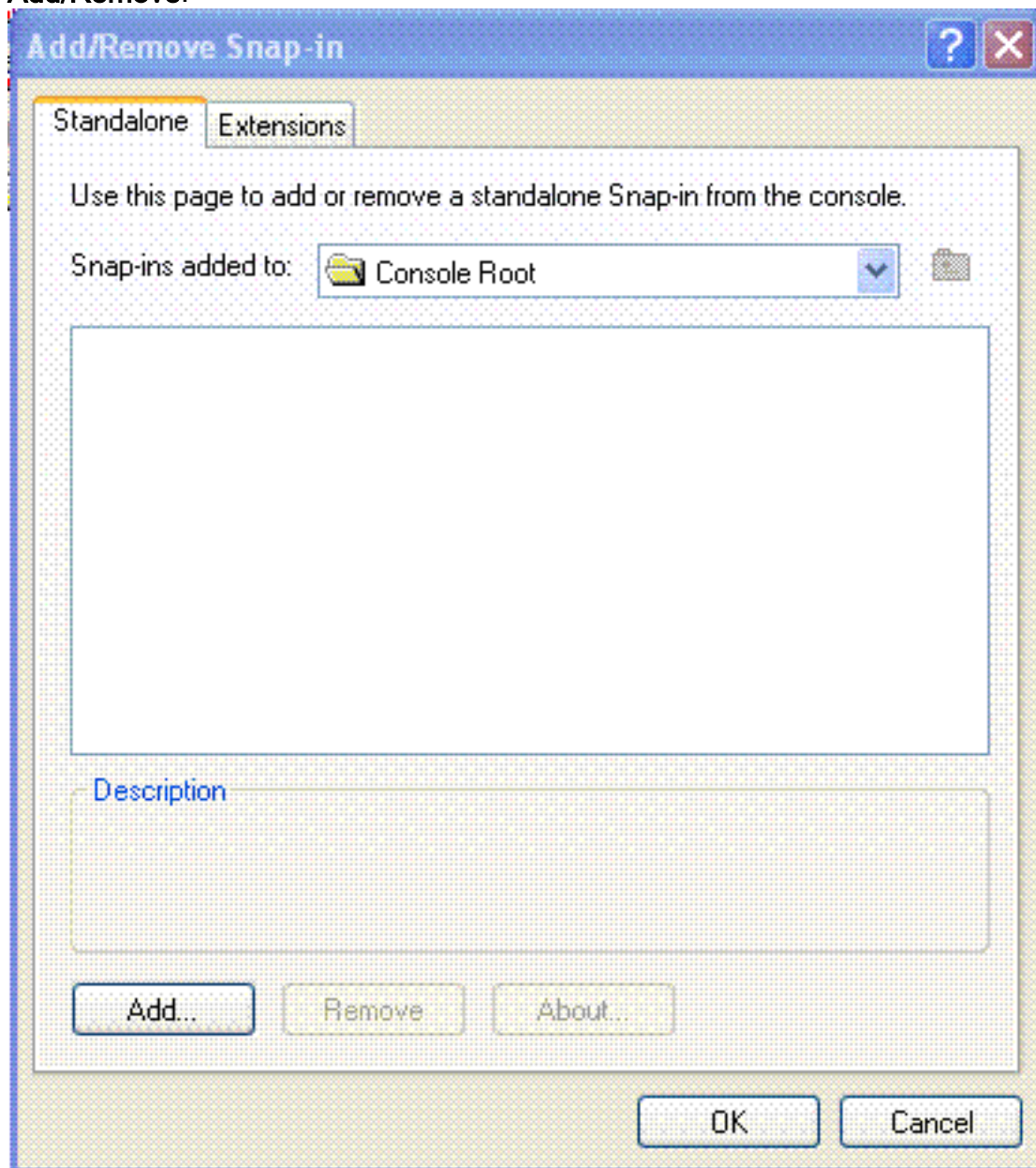


10. Click OK.
11. Cliquez sur **Yes pour redémarrer l'ordinateur**.
12. Une fois l'ordinateur redémarré, connectez-vous avec ces informations : Username = **Administrator**; Password = <domain password>; Domain = **Wireless**.
13. Cliquez à droite sur **My Computer**, puis cliquez sur **Properties**.
14. Cliquez sur l'onglet **Computer Name** pour vérifier que vous êtes sur le domaine **Wireless.com**.

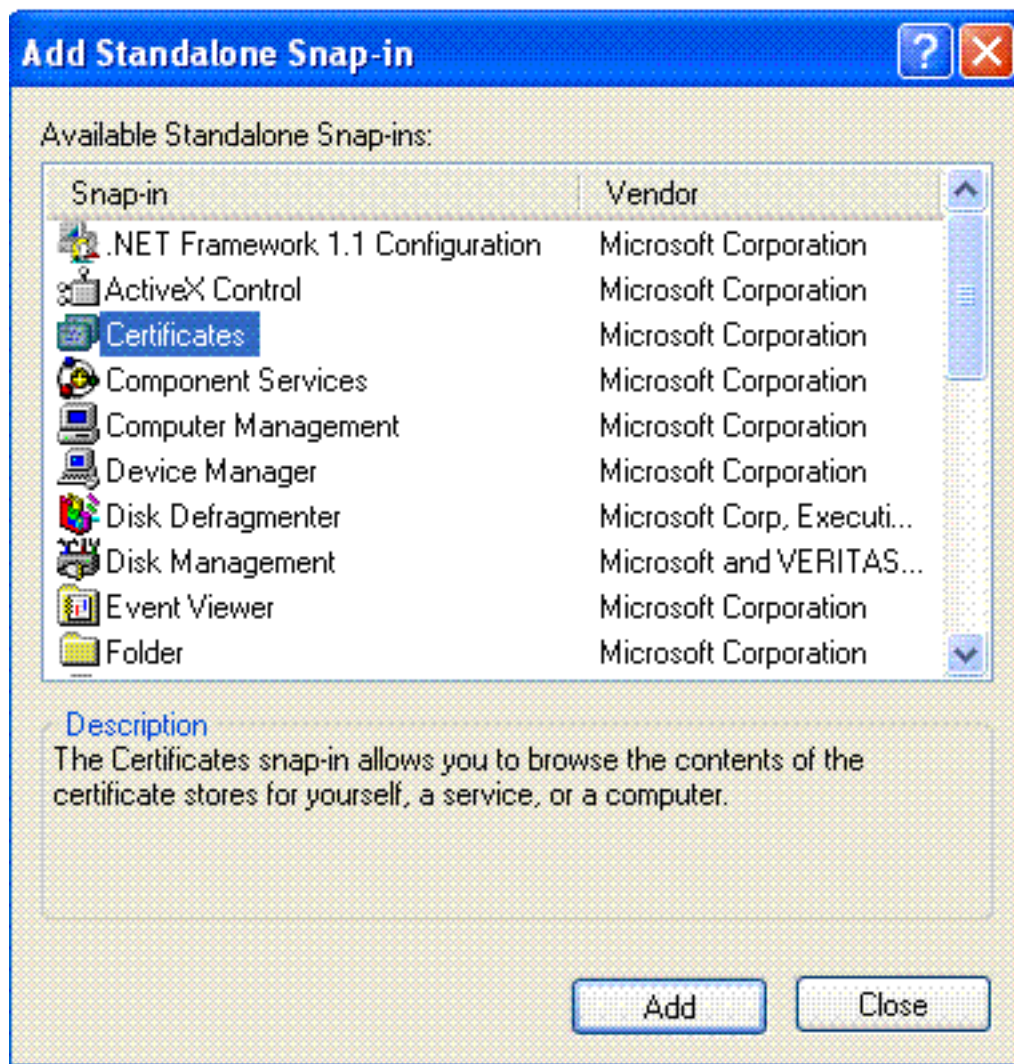


15. L'étape suivante consiste à vérifier que le client a reçu le certificat d'authentification (de confiance) du serveur.
16. Cliquez sur **Démarrer** ; cliquez sur **Exécuter** ; tapez **mmc**, puis cliquez sur **OK**.

17. Cliquez sur **File**, puis cliquez sur le jeu d'outils **Add/Remove**.



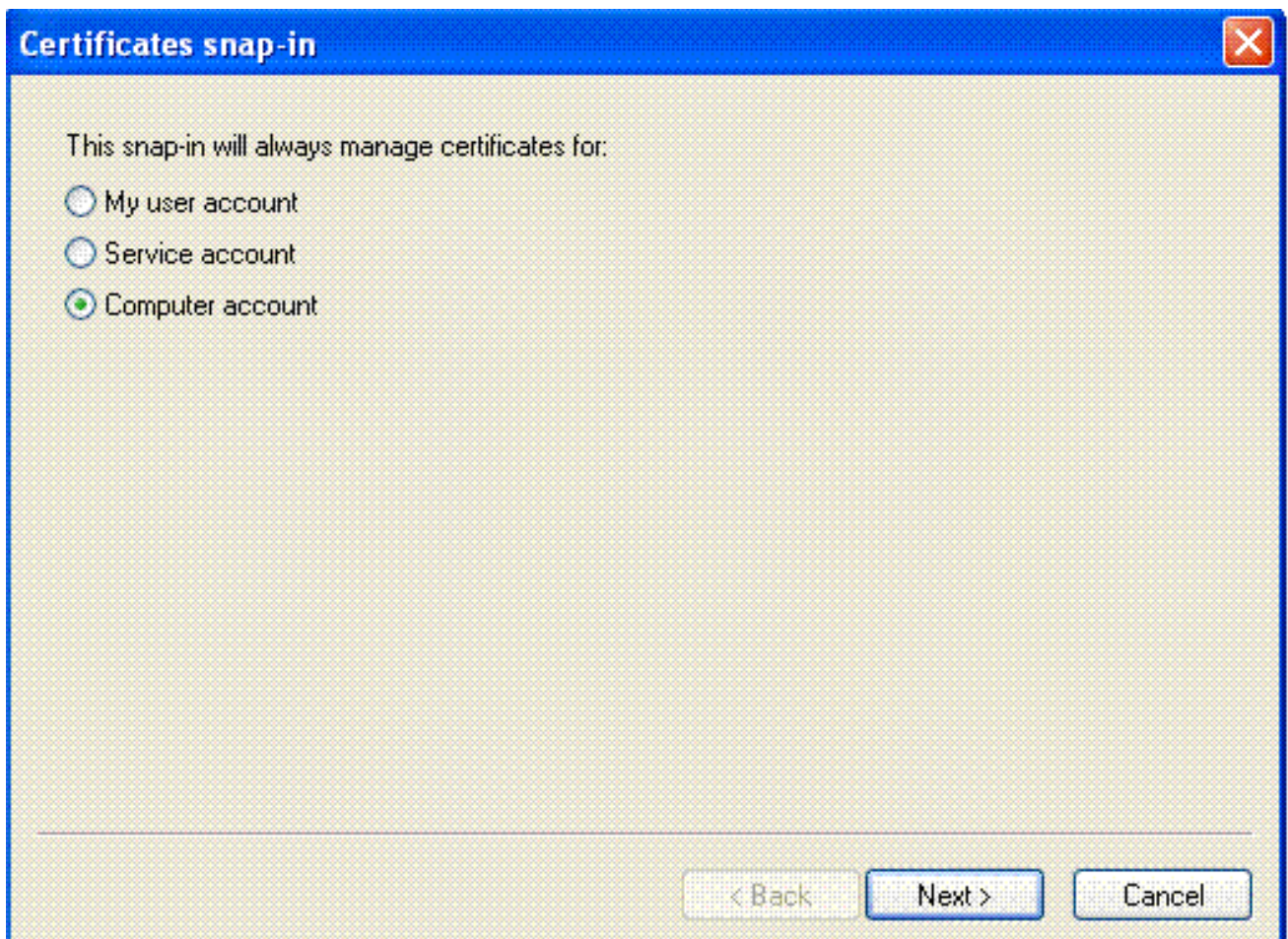
18. Cliquez sur **Add**.  
19. Choisissez **Certificate**, puis cliquez sur



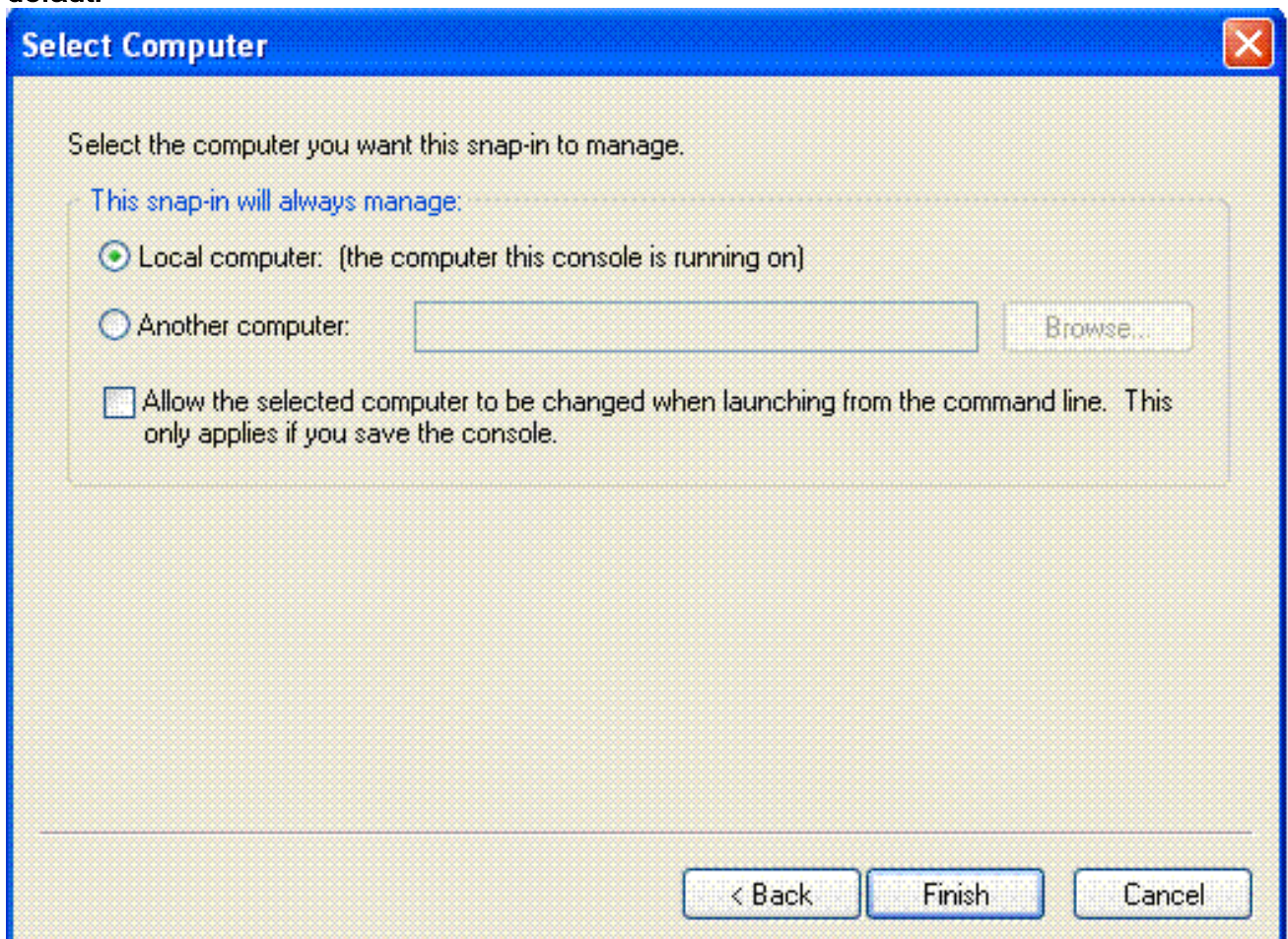
Add.

20. Choisissez **Computer Account**, puis cliquez sur **Next**.



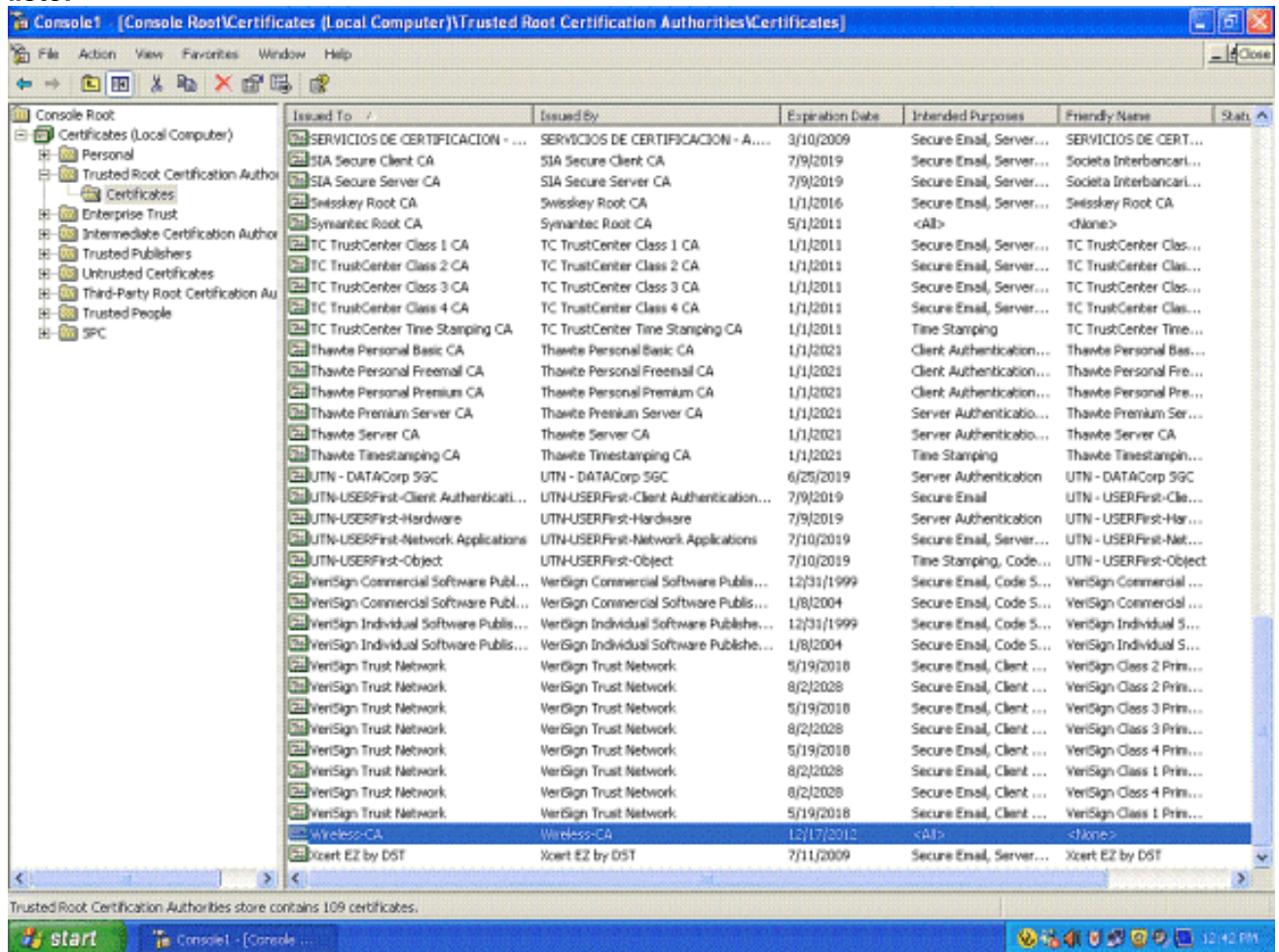


21. Cliquez sur **Finish** pour accepter l'ordinateur local par défaut.



22. Cliquez sur **Close**, puis cliquez sur **OK**.

23. Développez **Certificates (Local Computer)**, **Trusted Root Certification Authorities** et cliquez sur **Certificates**. Trouvez **Wireless** dans la liste.



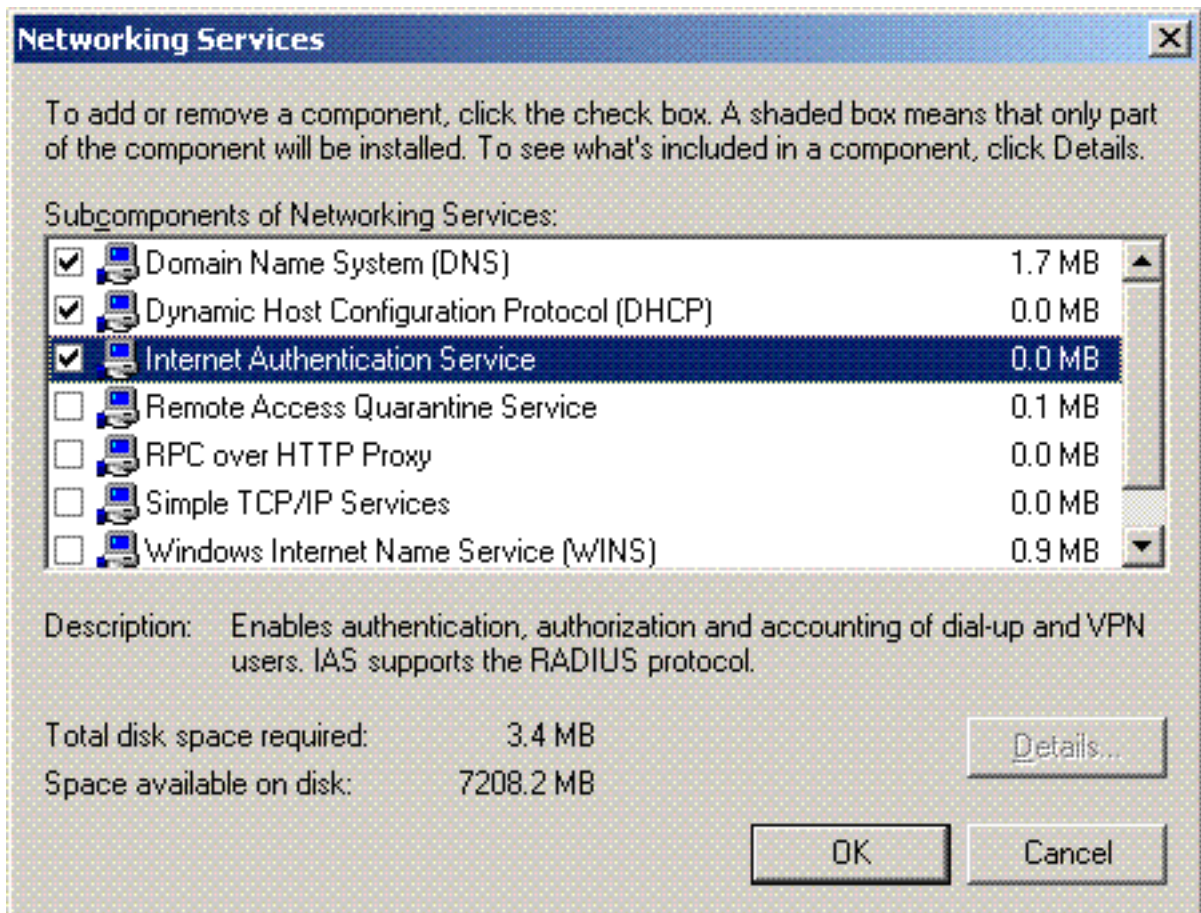
24. Répétez cette procédure pour ajouter plus de clients au domaine.

## [Installez le service d'authentification Internet sur le serveur de Microsoft Windows 2003 et demandez un certificat](#)

Dans cette configuration, le Service d'authentification Internet (IAS) est utilisé en tant que serveur RADIUS pour authentifier des clients sans fil avec l'authentification PEAP.

Suivez ces étapes pour installer et configurer IAS sur le serveur.

1. Cliquez sur **Add or Remove Programs** dans le panneau de configuration.
2. Cliquez sur **Add/Remove Windows Components**.
3. Choisissez **Networking Services**, puis cliquez sur **Details**.
4. Choisissez **Internet Authentication Service** ; cliquez sur **OK** ; et cliquez sur

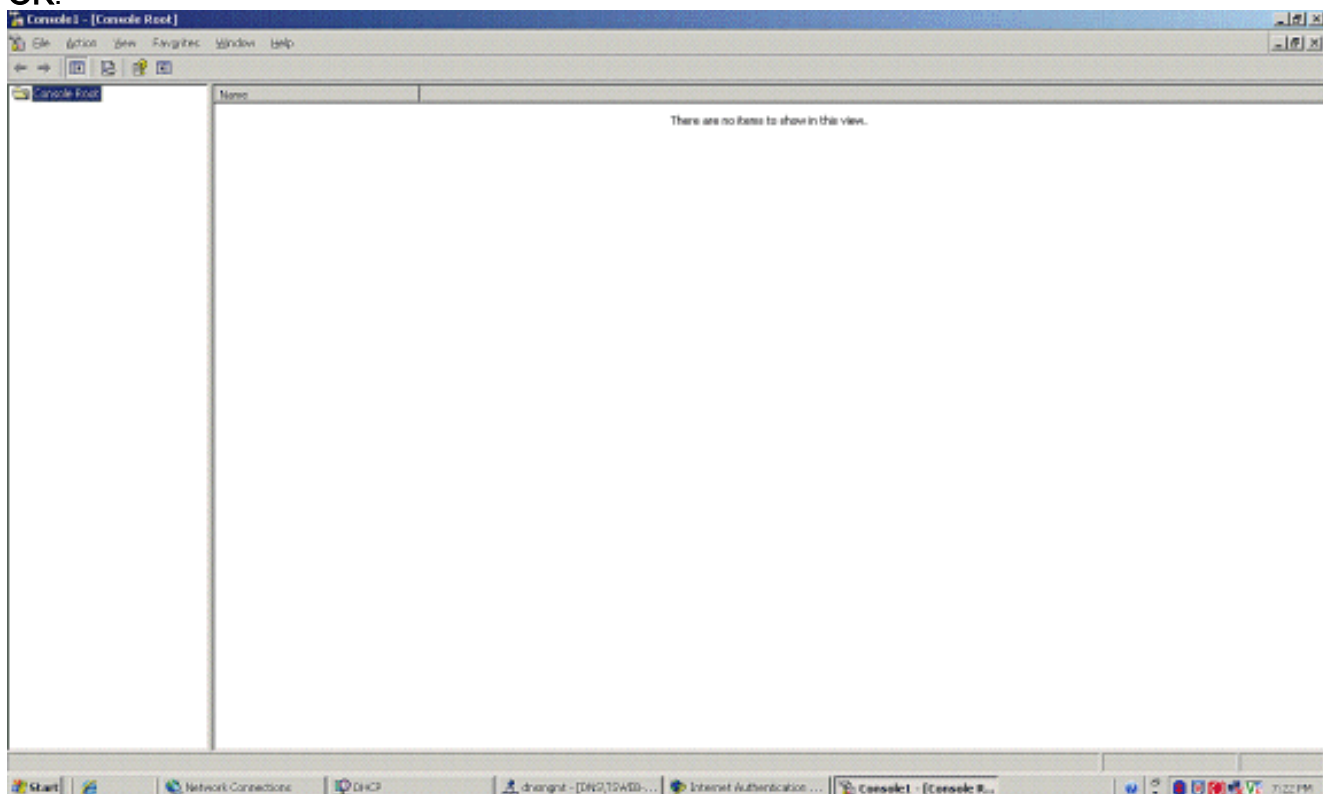


Next.

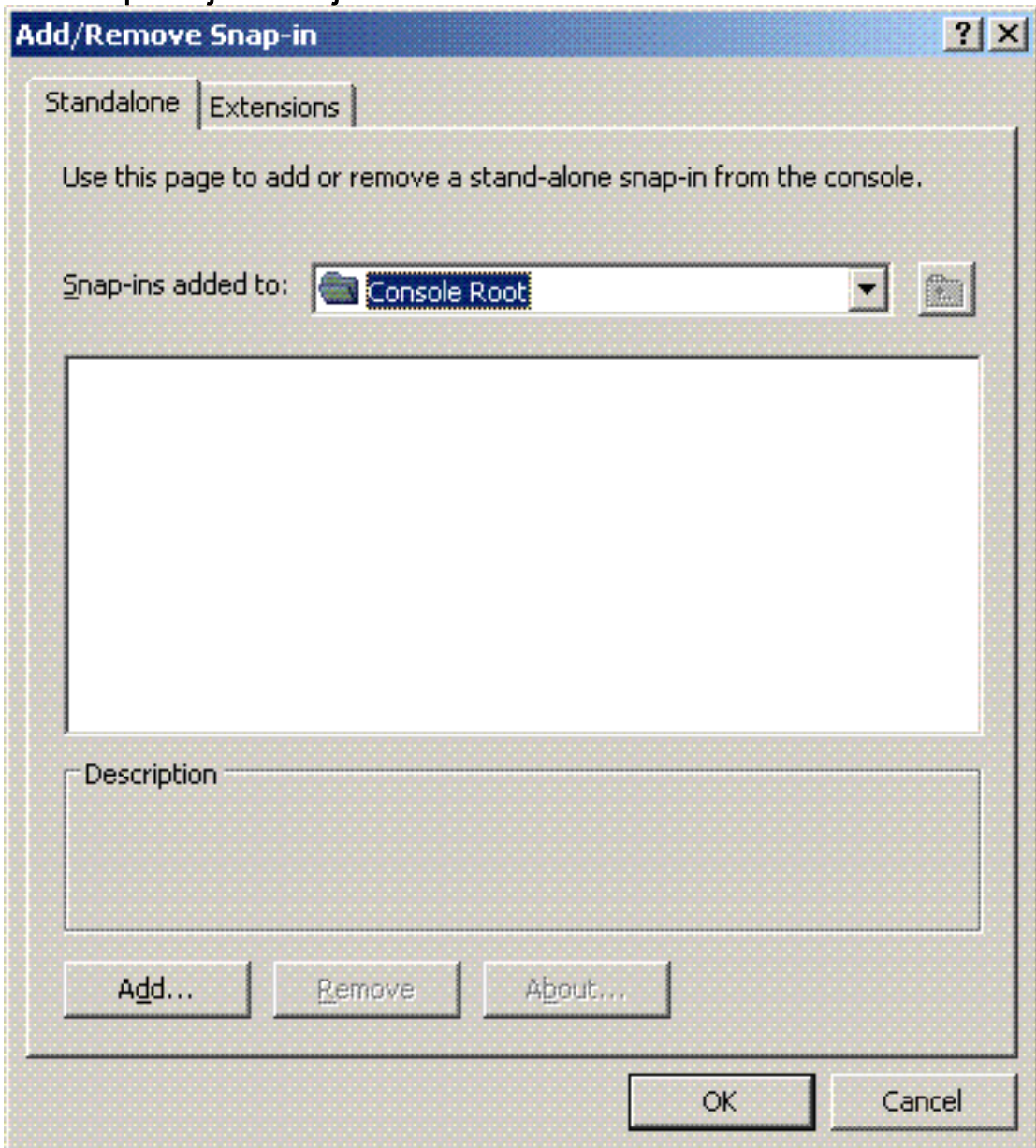
5. Cliquez sur **Finish** pour terminer l'installation IAS.



6. L'étape suivante consiste à installer le certificat de l'ordinateur pour le Service d'authentification Internet (IAS).
7. Cliquez sur **Démarrer** ; cliquez sur **Exécuter** ; tapez **mmc** ; et cliquez sur **OK**.

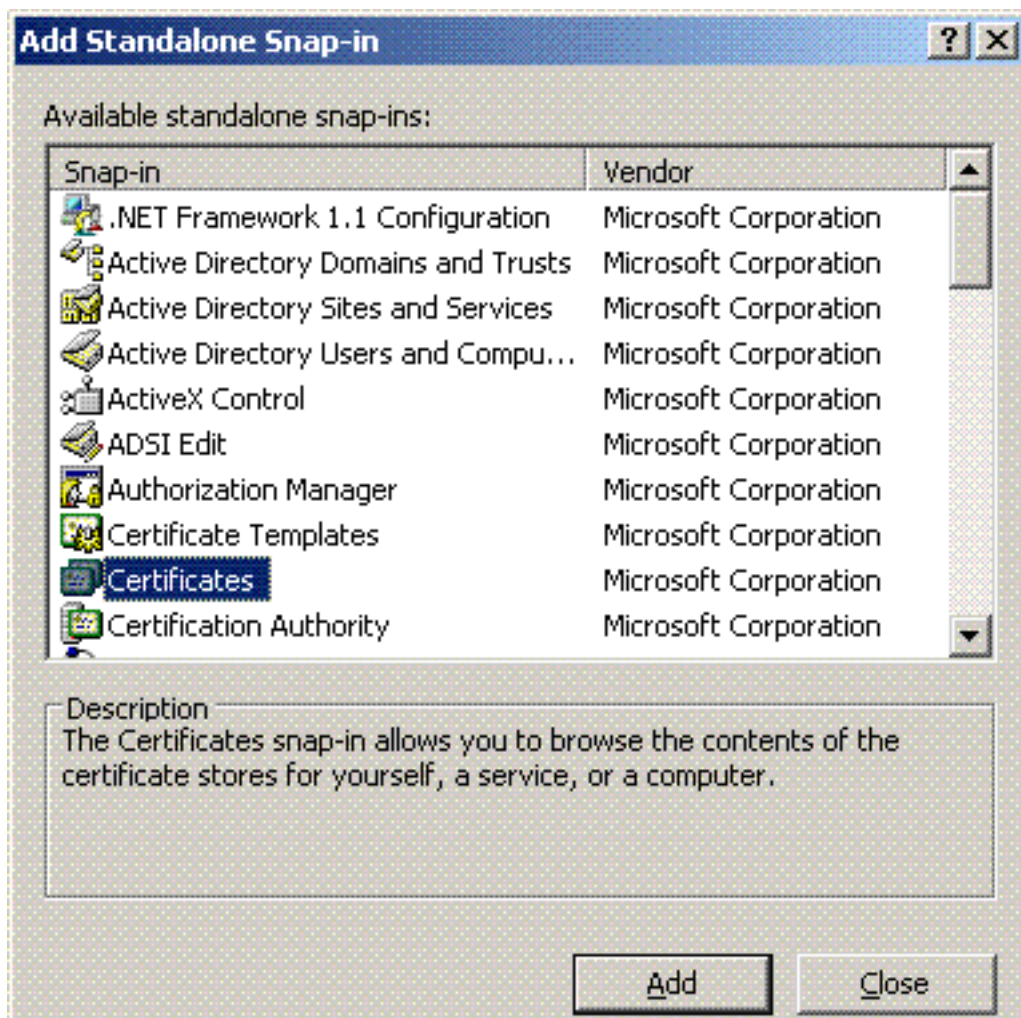


8. Cliquez sur **Console** dans le menu **Fichier**, puis choisissez le jeu d'outils **Add/Remove**.
9. Cliquez sur **Add** pour ajouter un jeu



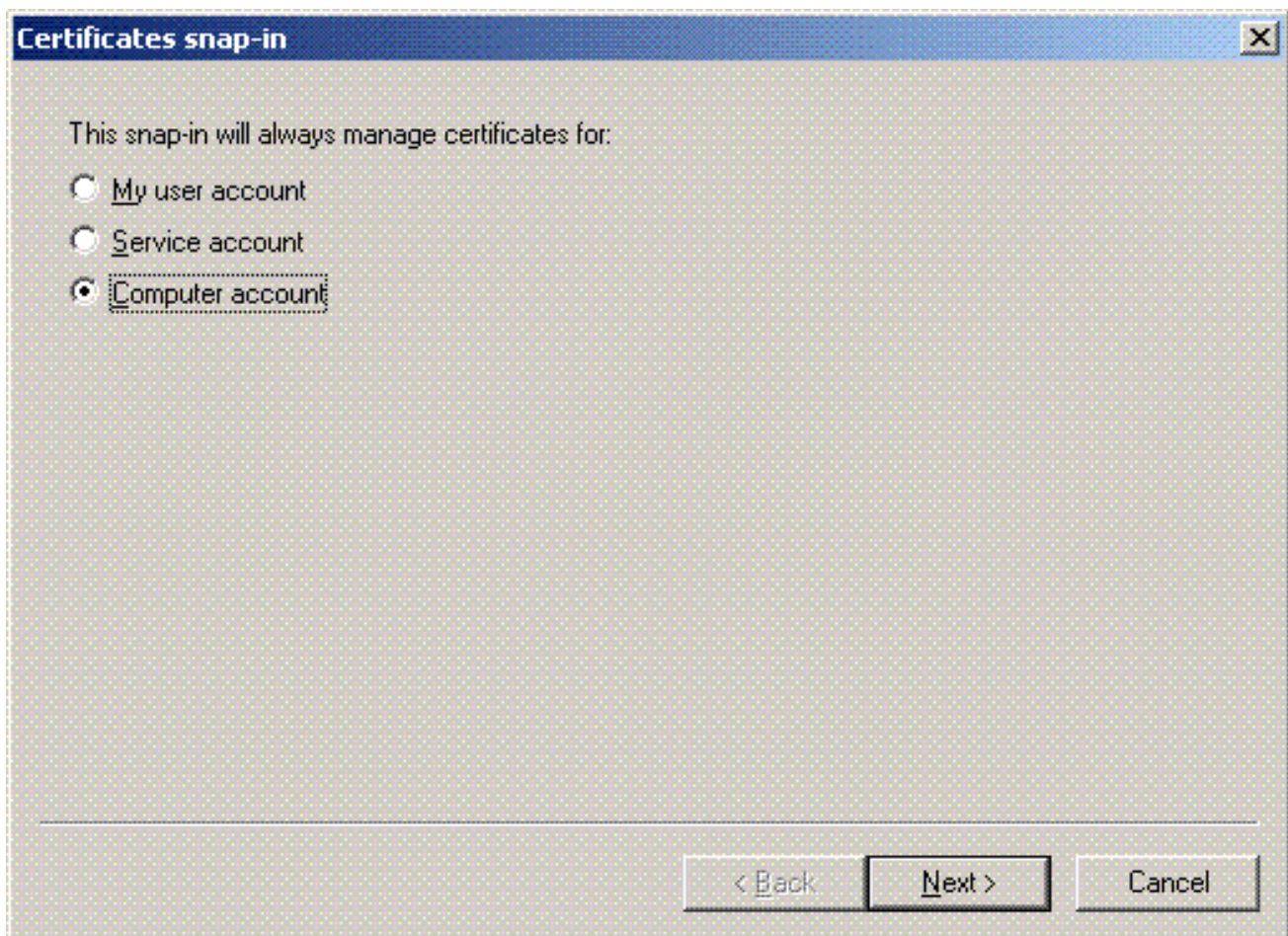
d'outils.

10. Choisissez **Certificates** dans la liste des jeux d'outil, puis cliquez sur

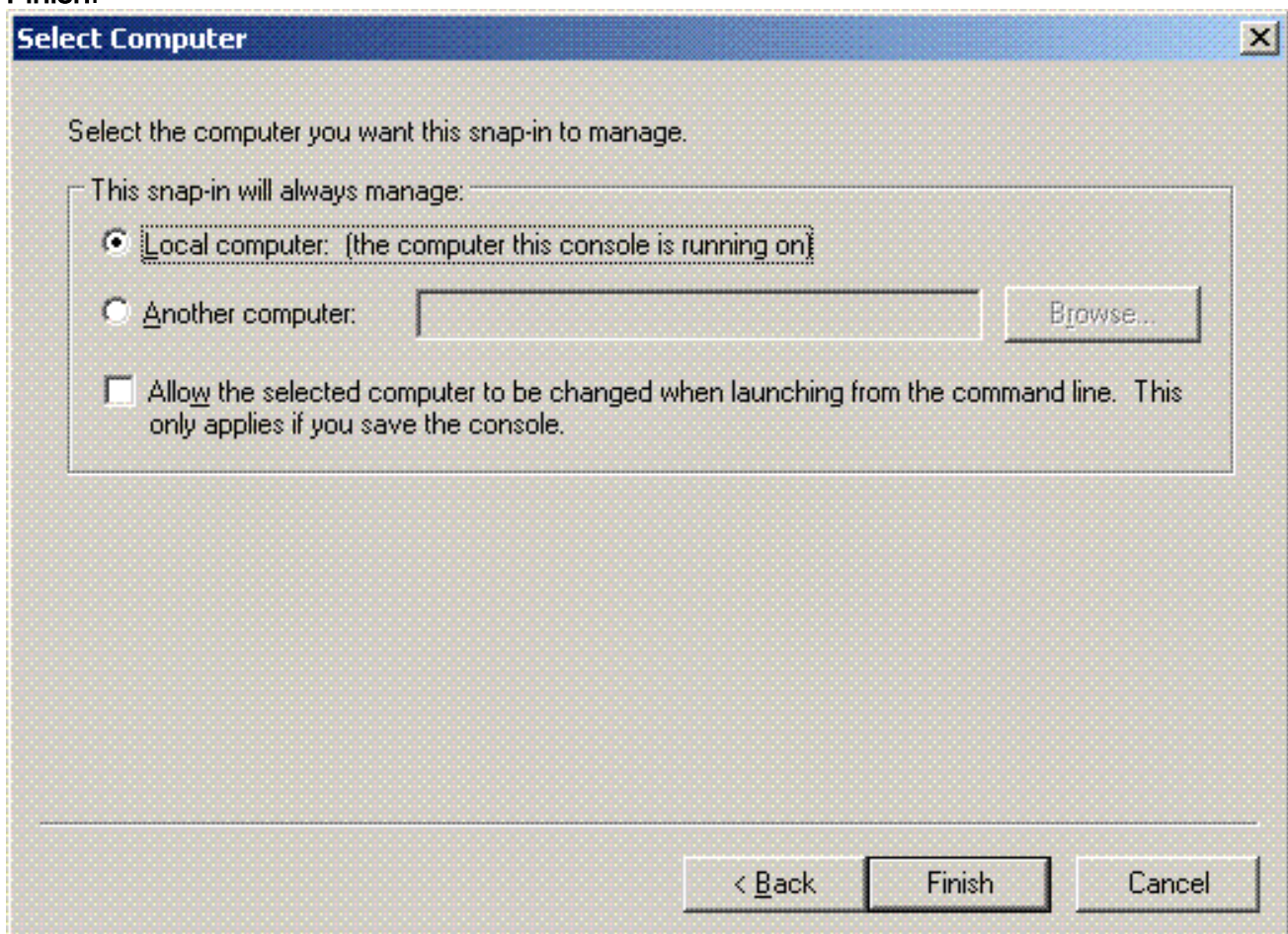


**Add.**

11. Choisissez **Computer Account**, puis cliquez sur **Next**.

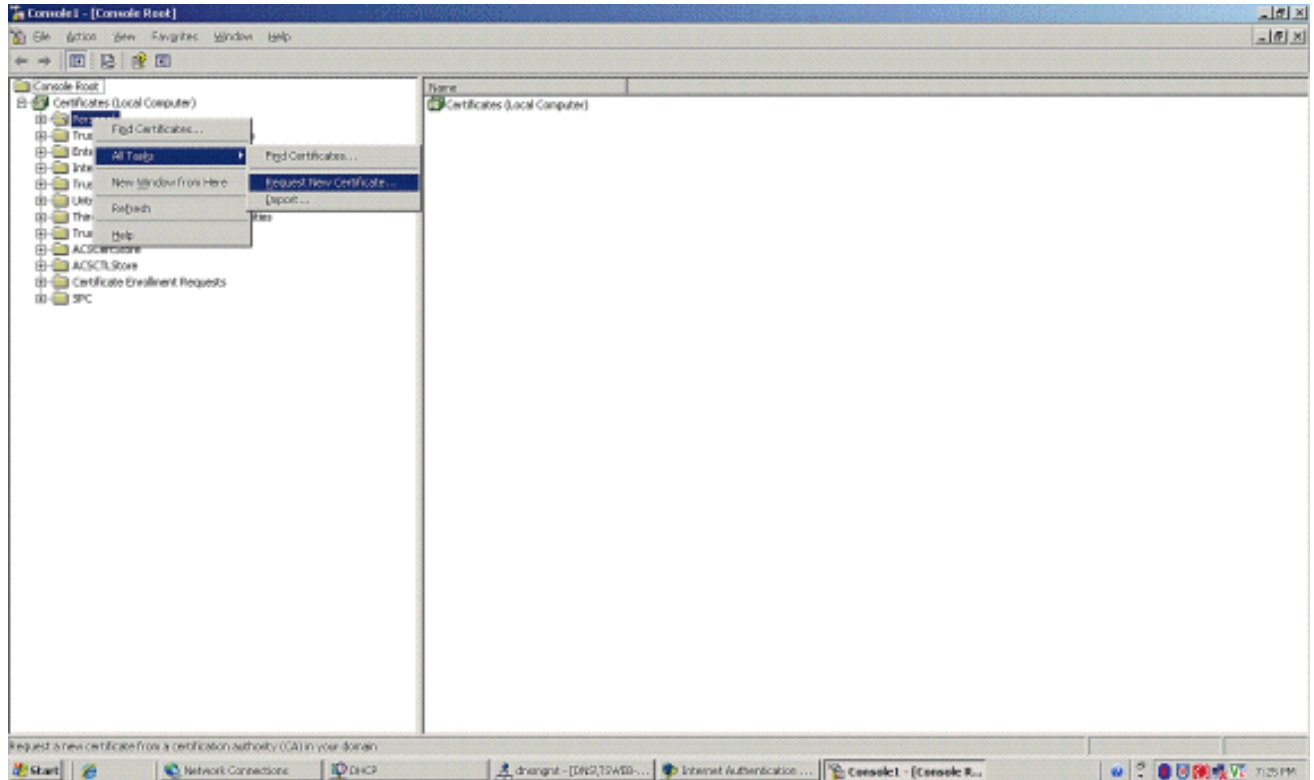


12. Choisissez **Local computer**, puis cliquez sur **Finish**.



13. Cliquez sur **Close**, puis cliquez sur **OK**.

14. Développez **Certificats (Ordinateur local)**; cliquez avec le bouton droit sur **Dossier personnel**; choisissez **Toutes les tâches**, puis **Demandez un nouveau certificat**.



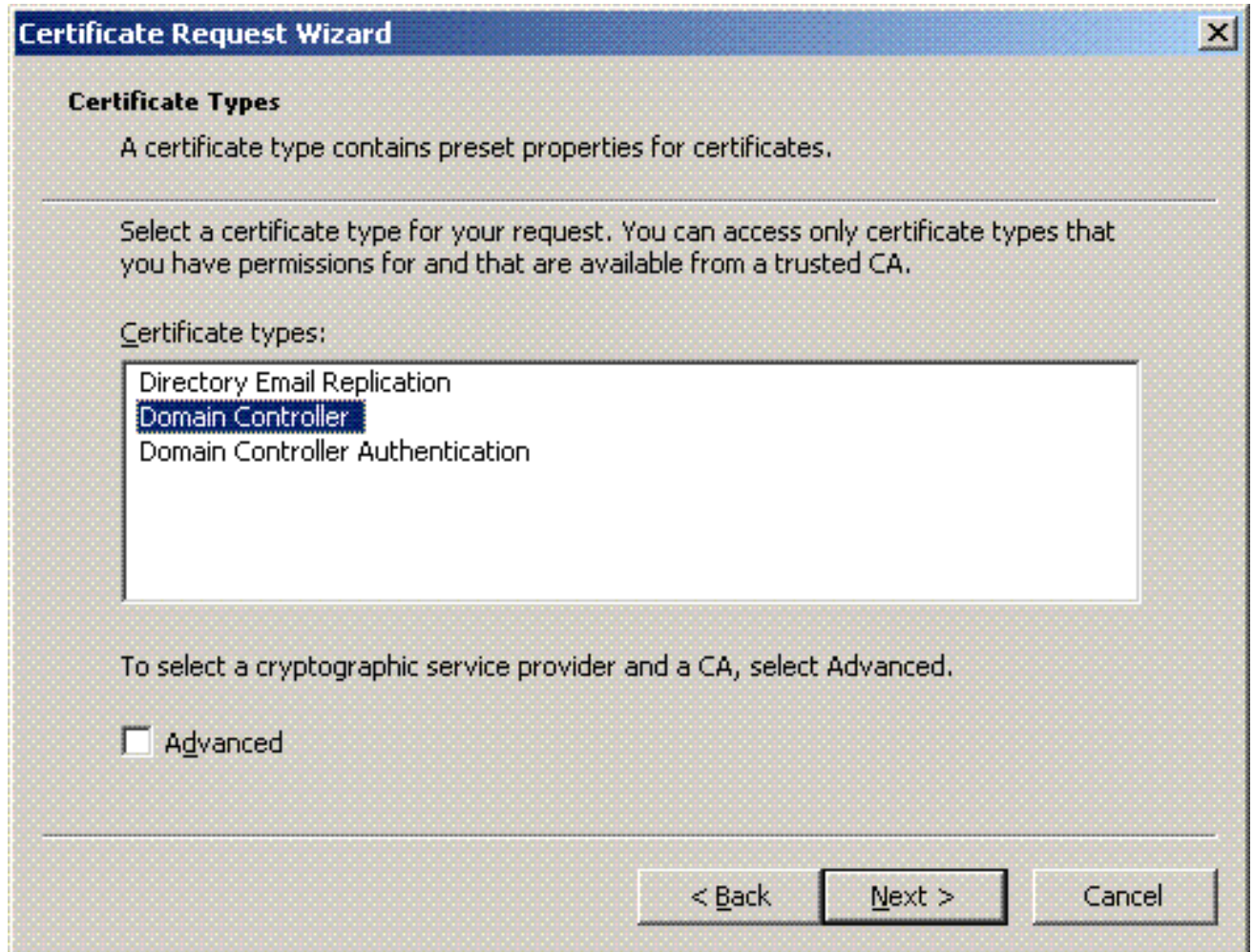
15. Cliquez sur **Next** dans **Welcome to the Certificate Request Wizard**.



16. Choisissez le modèle de certificat du **contrôleur de domaine** (si vous demandez un certificat



d'ordinateur sur un serveur autre que DC, choisissez un modèle de certificat d'ordinateur), puis cliquez sur Next.



17. Saisissez un nom et une description pour le certificat.

**Certificate Request Wizard** [X]

**Certificate Friendly Name and Description**

You can provide a name and description that help you quickly identify a specific certificate.

---

Type a friendly name and description for the new certificate.

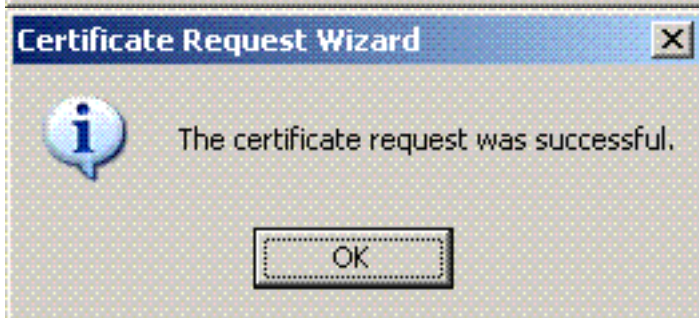
Friendly name:

Description:

---

< Back    Next >    Cancel

18. Cliquez sur **Finish** pour terminer avec l'assistant de requête de certification.

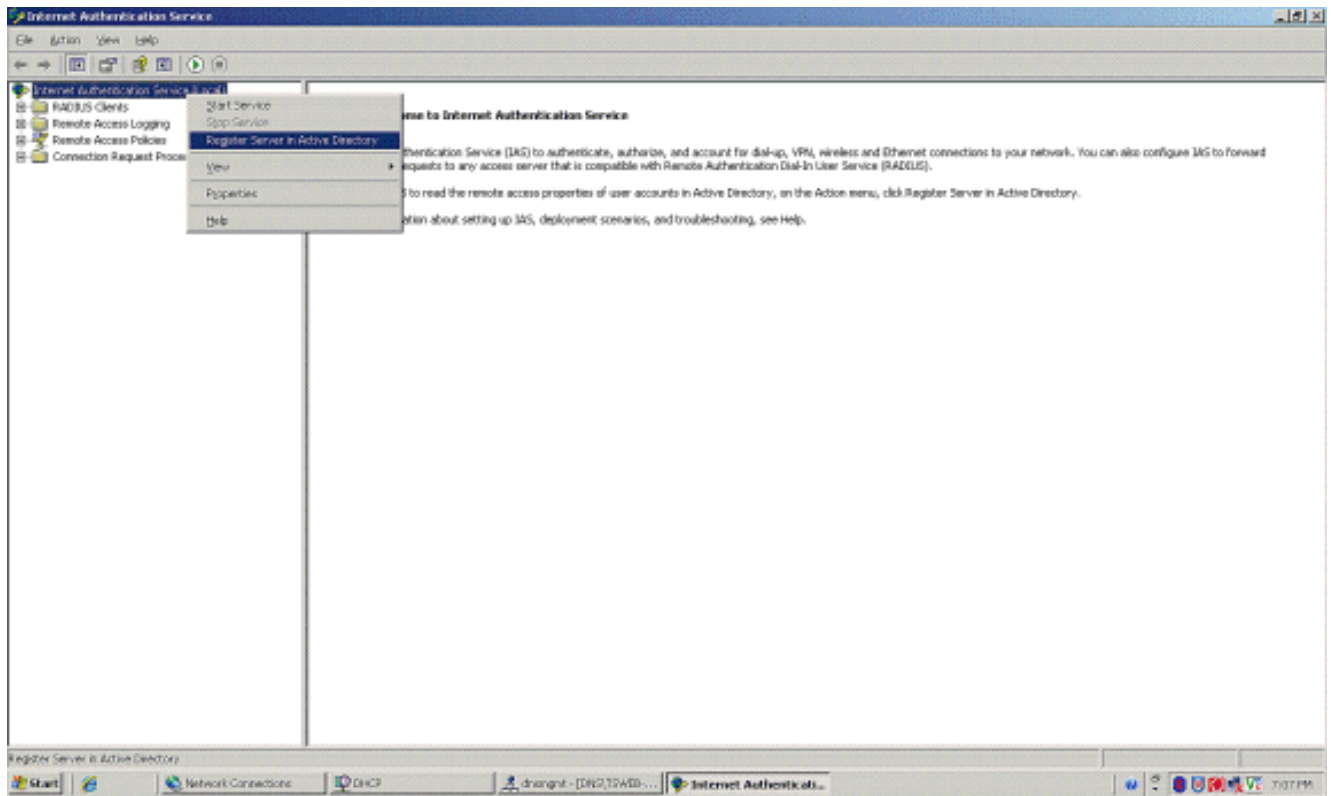


## [Configurez le service d'authentification Internet pour l'authentification PEAP-MS-CHAP v2](#)

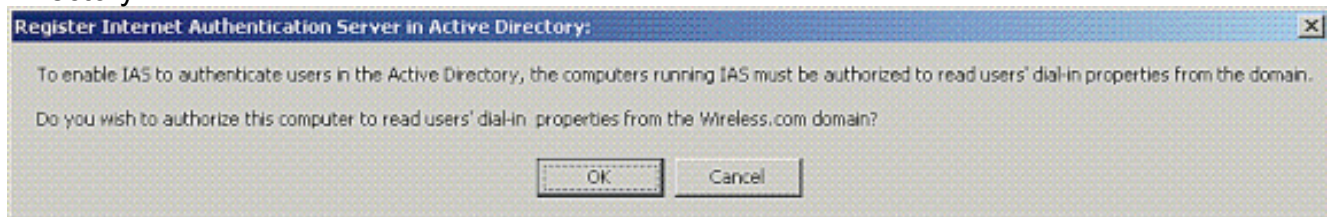
Maintenant que vous avez installé et que vous avez demandé un certificat pour IAS, configurez IAS pour l'authentification.

Procédez comme suit :

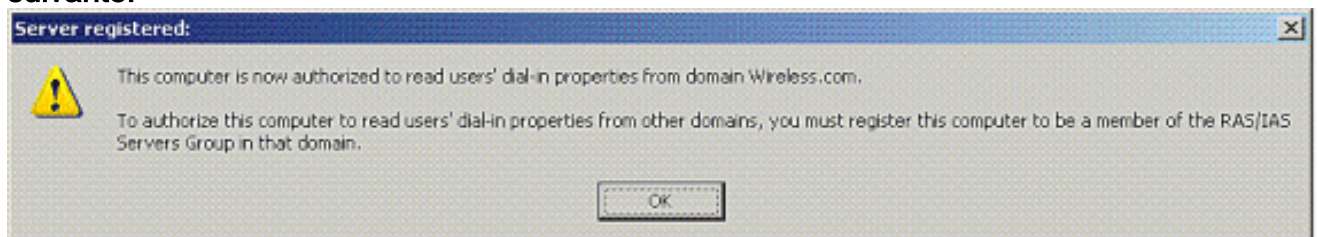
1. Cliquez sur **Start > Programs > Administrative Tools**, puis cliquez sur le jeu d'outils Internet Authentication Service.
2. Cliquez à droite sur **Internet Authentication Service (IAS)**, puis cliquez sur **Register Service in Active Directory**.



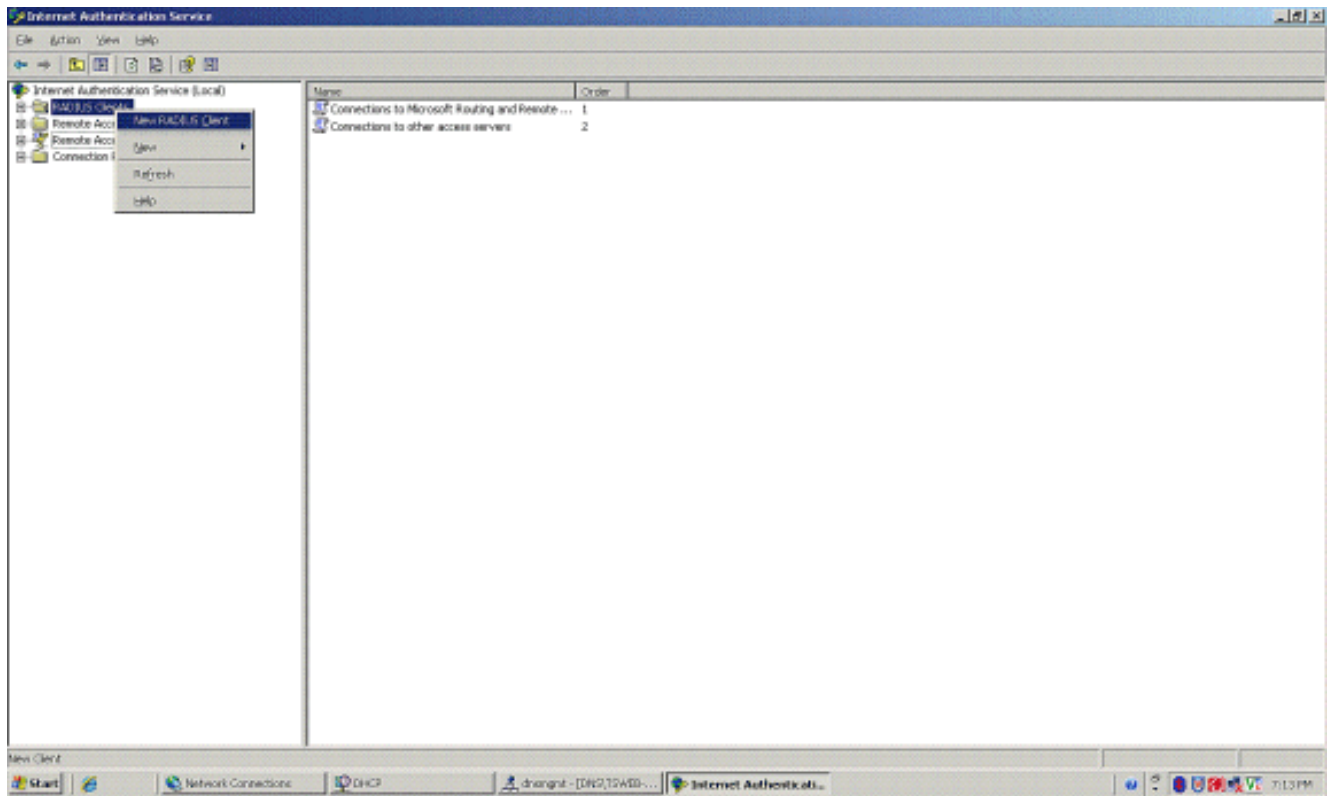
3. La boîte de dialogue **Register Internet Authentication Service in Active Directory** s'affiche ; cliquez sur **OK**. Ceci permet à IAS d'authentifier des utilisateurs dans Active Directory.



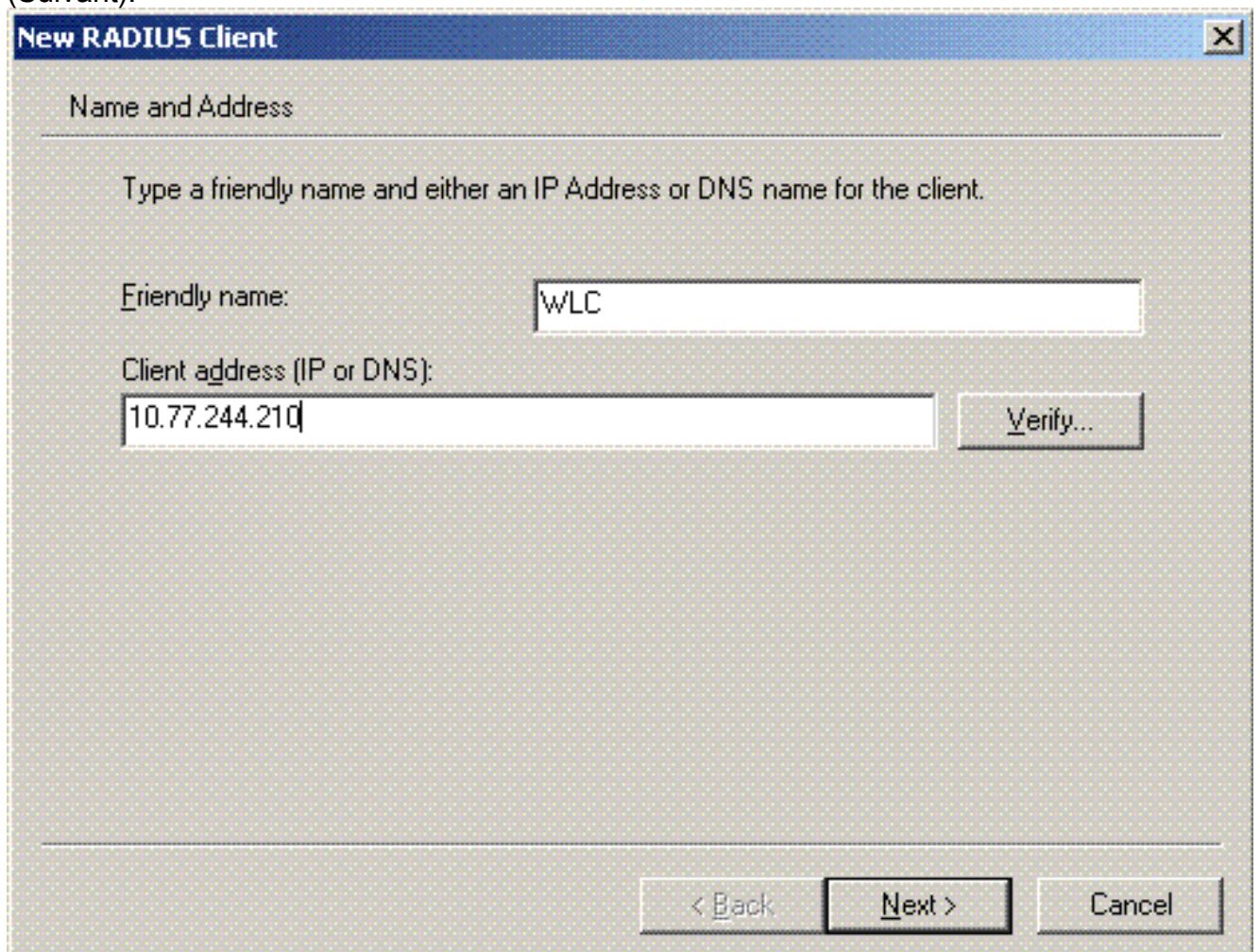
4. Cliquez sur **OK** dans la boîte de dialogue suivante.



5. Ajoutez le contrôleur LAN sans fil en tant que client AAA sur le serveur MS IAS.
6. Cliquez à droite sur **RADIUS Clients**, puis choisissez **New RADIUS Client**.

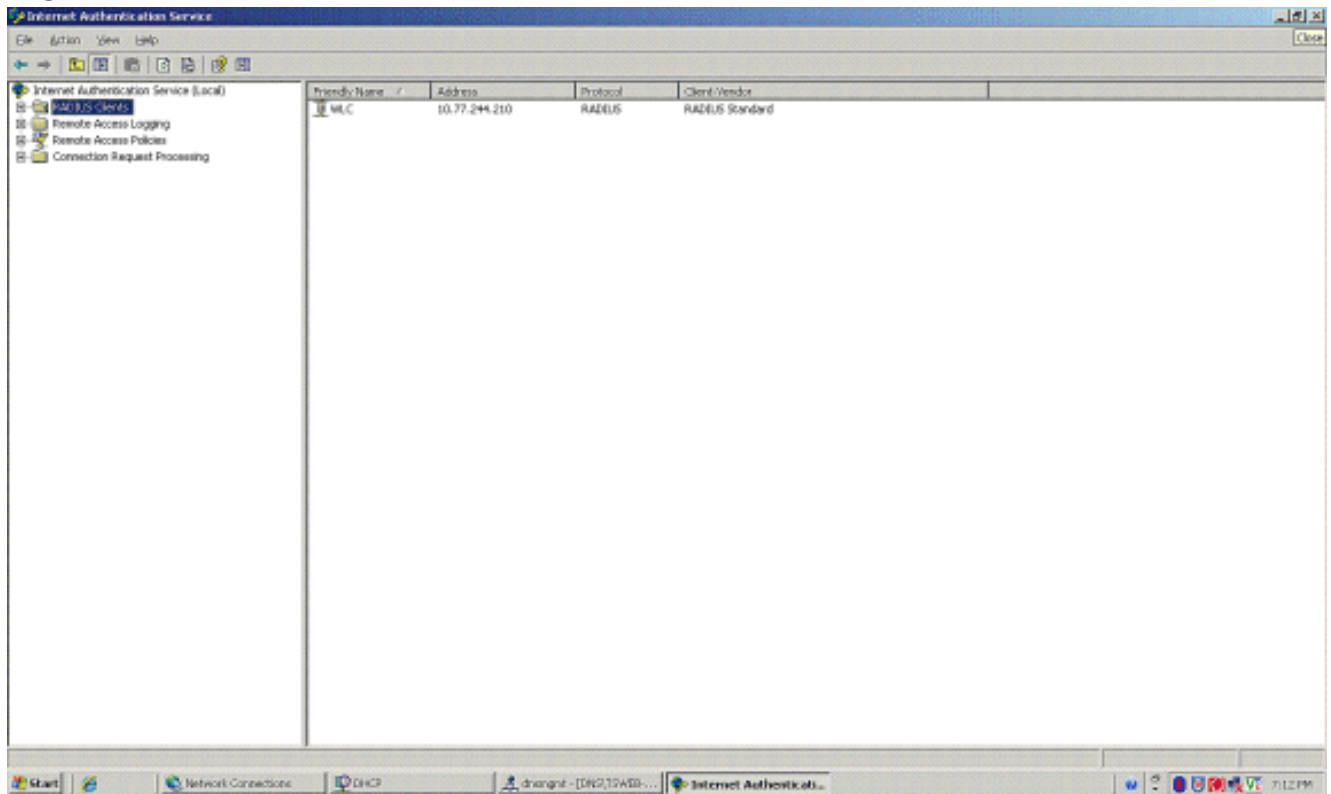


7. Introduisez le nom du client (WLC, dans ce cas), puis saisissez l'adresse IP du WLC. Cliquez sur **Next** (Suivant).



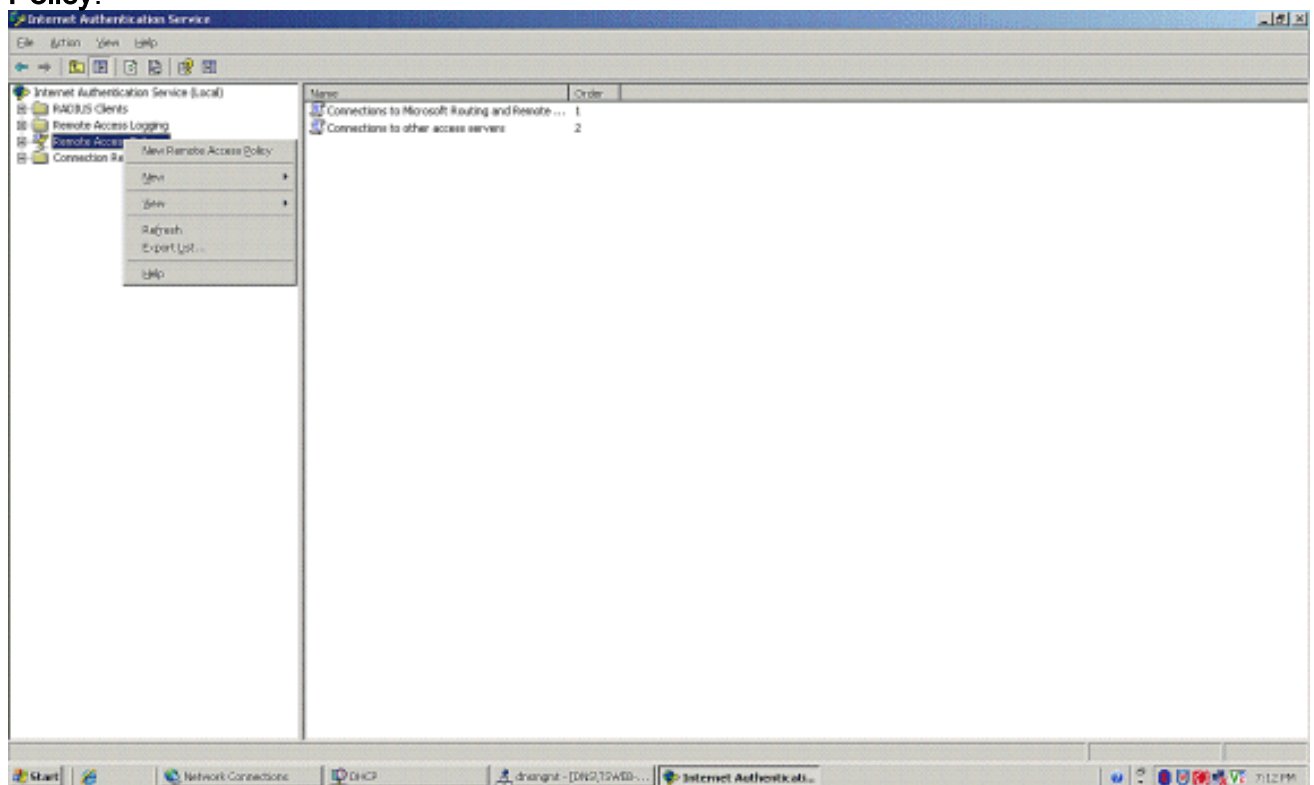
8. Sur la page suivante, sous Client-Vendor, choisissez **RADIUS Standard** ; entrez le secret partagé et cliquez sur **Finish**.

9. Notez que le WLC est ajouté en tant que client AAA sur IAS.



10. Créez une stratégie d'accès à distance pour les clients.

11. À cette fin, cliquez à droite sur **Remote Access Policies**, puis choisissez **New Remote Access Policy**.




12. Saisissez un nom pour la stratégie d'accès à distance. Dans cet exemple, utilisez le nom **PEAP**. Cliquez ensuite sur **Next**.

**New Remote Access Policy Wizard** [X]

**Policy Configuration Method**

The wizard can create a typical policy, or you can create a custom policy.



How do you want to set up this policy?

Use the wizard to set up a typical policy for a common scenario

Set up a custom policy

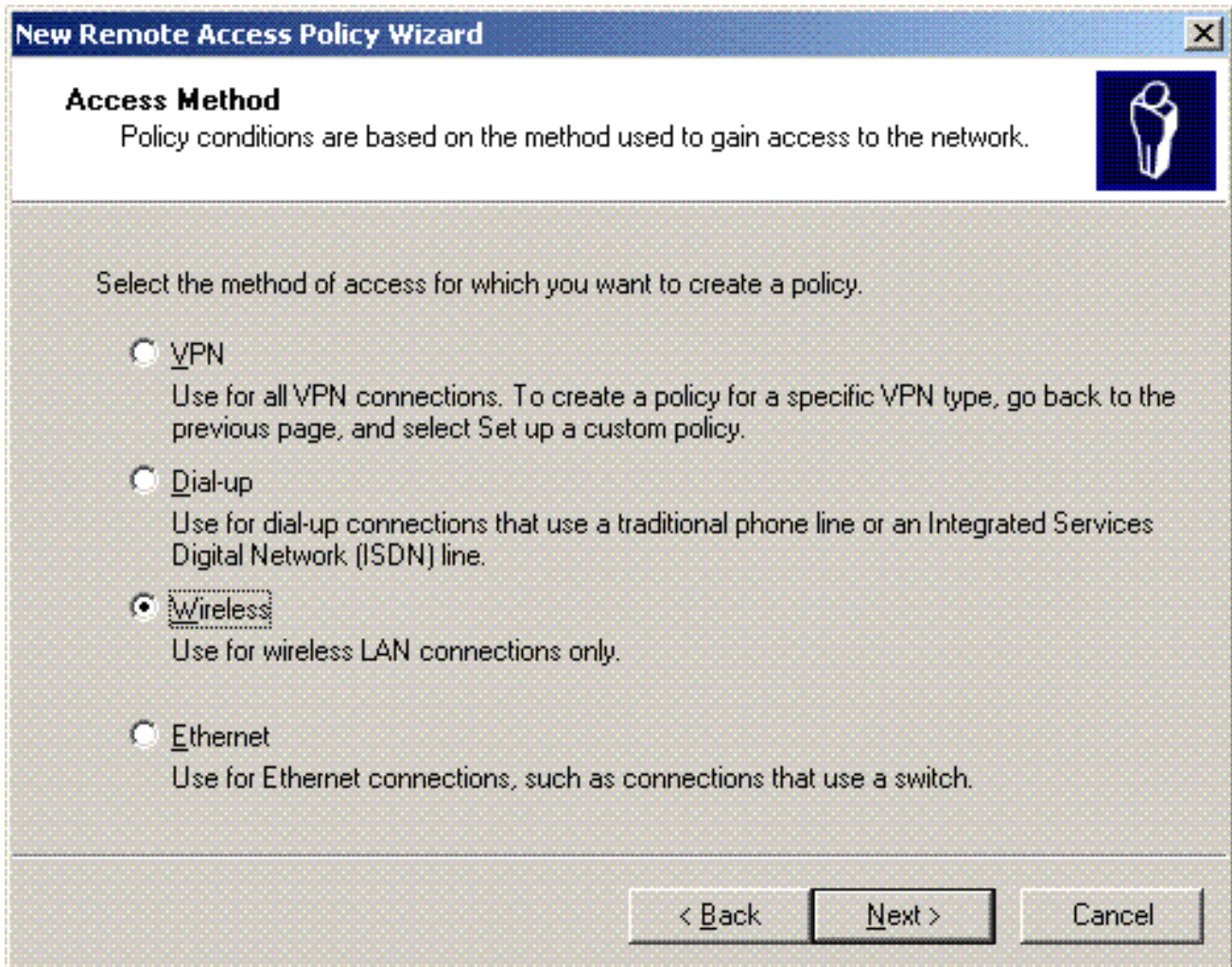
Type a name that describes this policy.

Policy name:

Example: Authenticate all VPN connections.

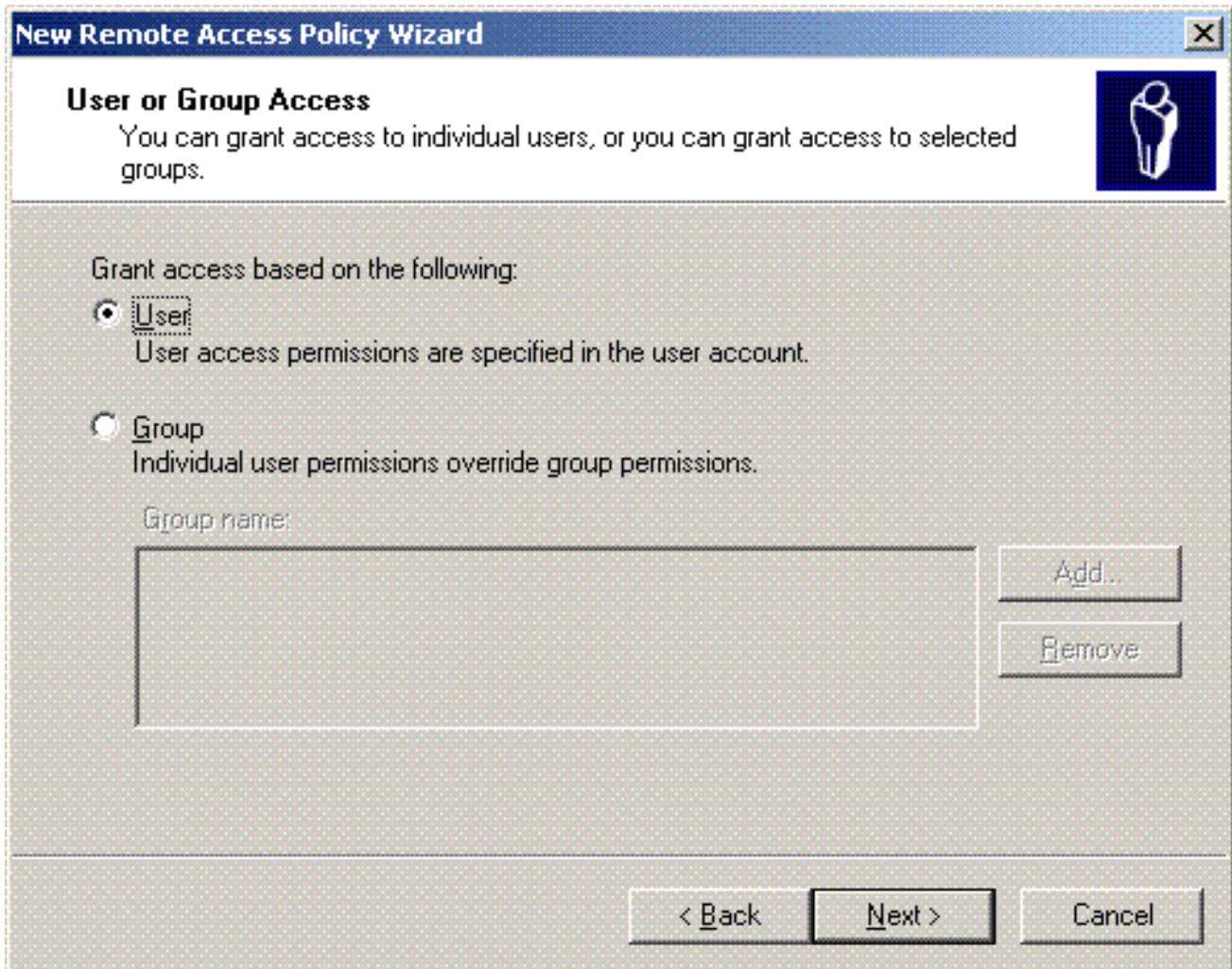
< Back   Next >   Cancel

13. Choisissez les attributs de la politique en fonction de vos nécessités. Dans cet exemple, choisissez **Wireless**.

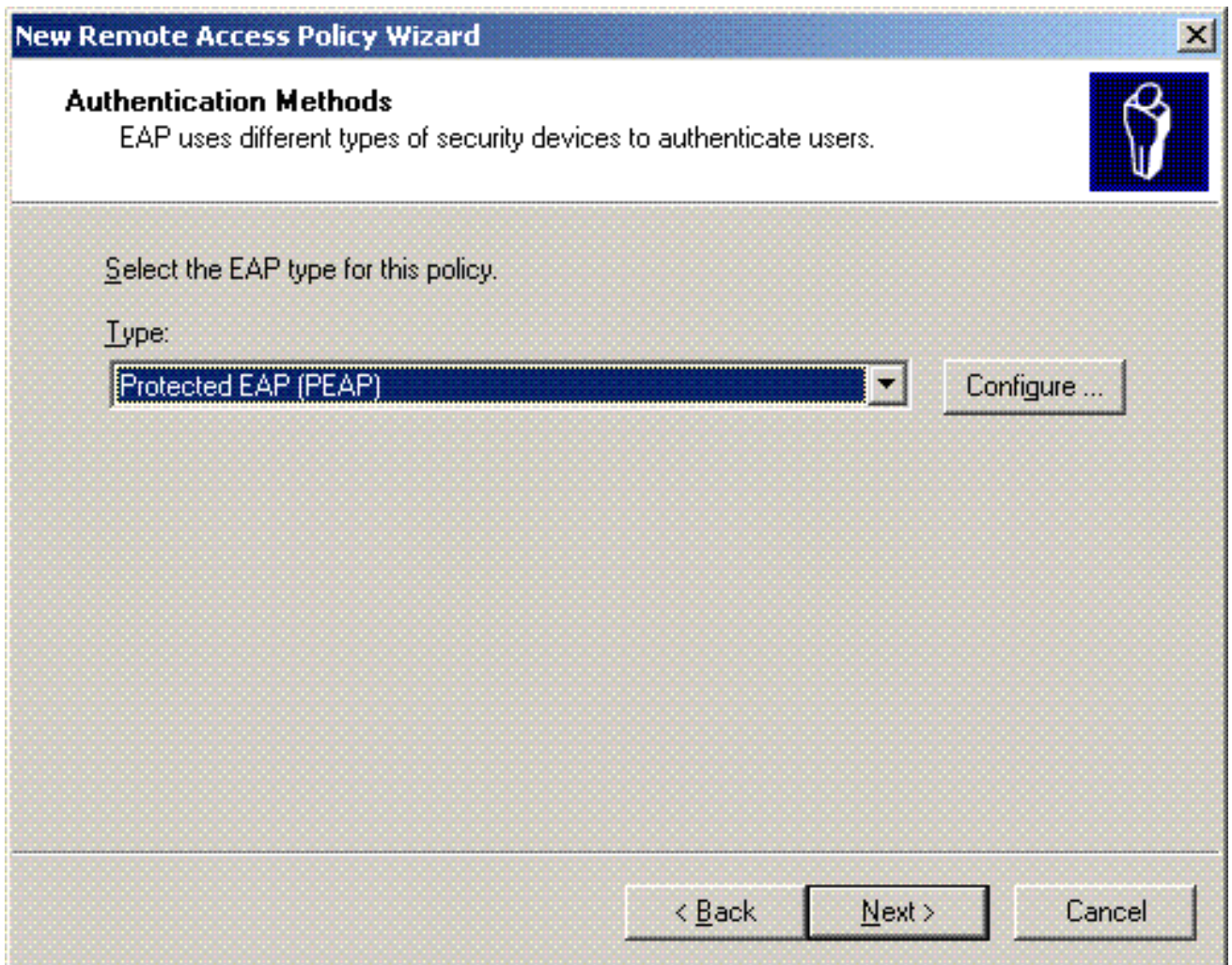


14. Sur la page suivante, choisissez **User pour appliquer cette stratégie d'accès à distance à la liste des utilisateurs.**

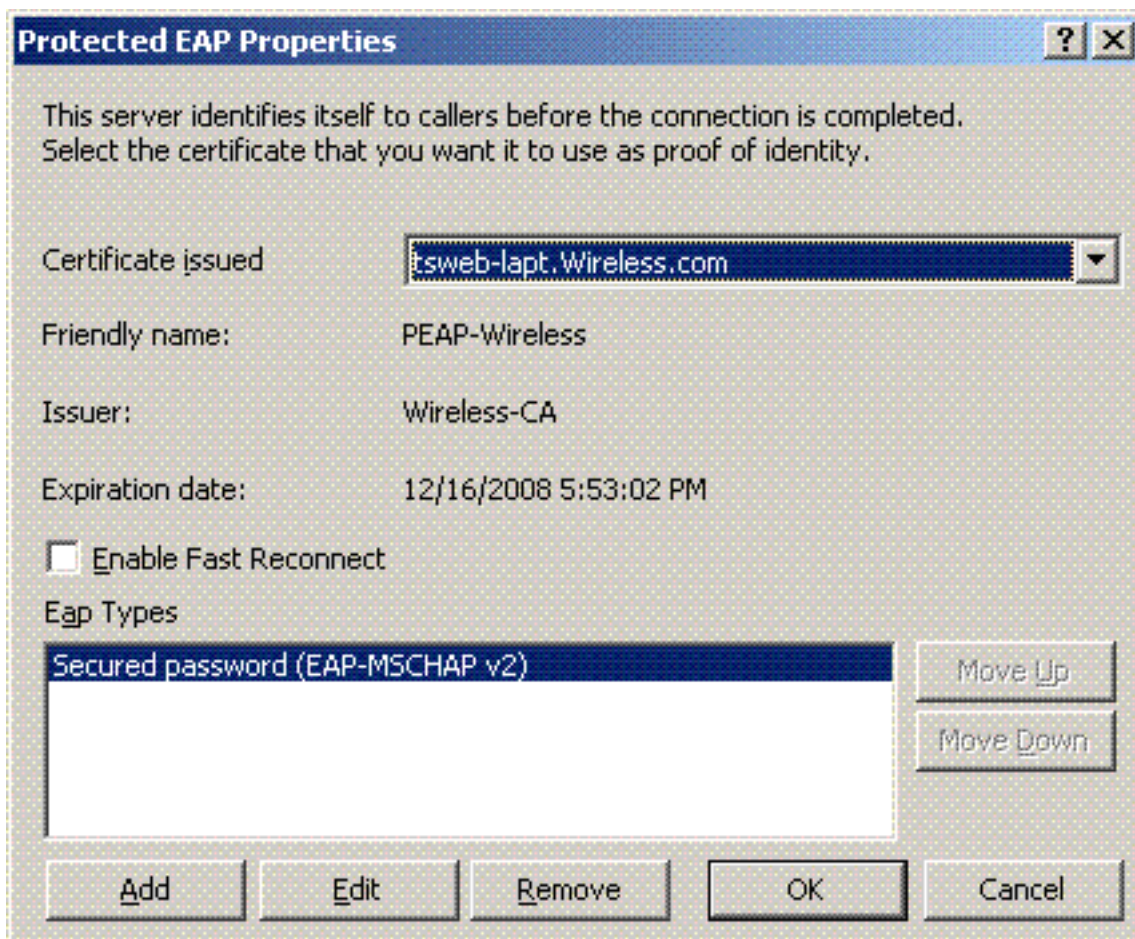




15. Sous les méthodes d'authentification, choisissez **Protected EAP (PEAP)**, puis cliquez sur **Configure**.

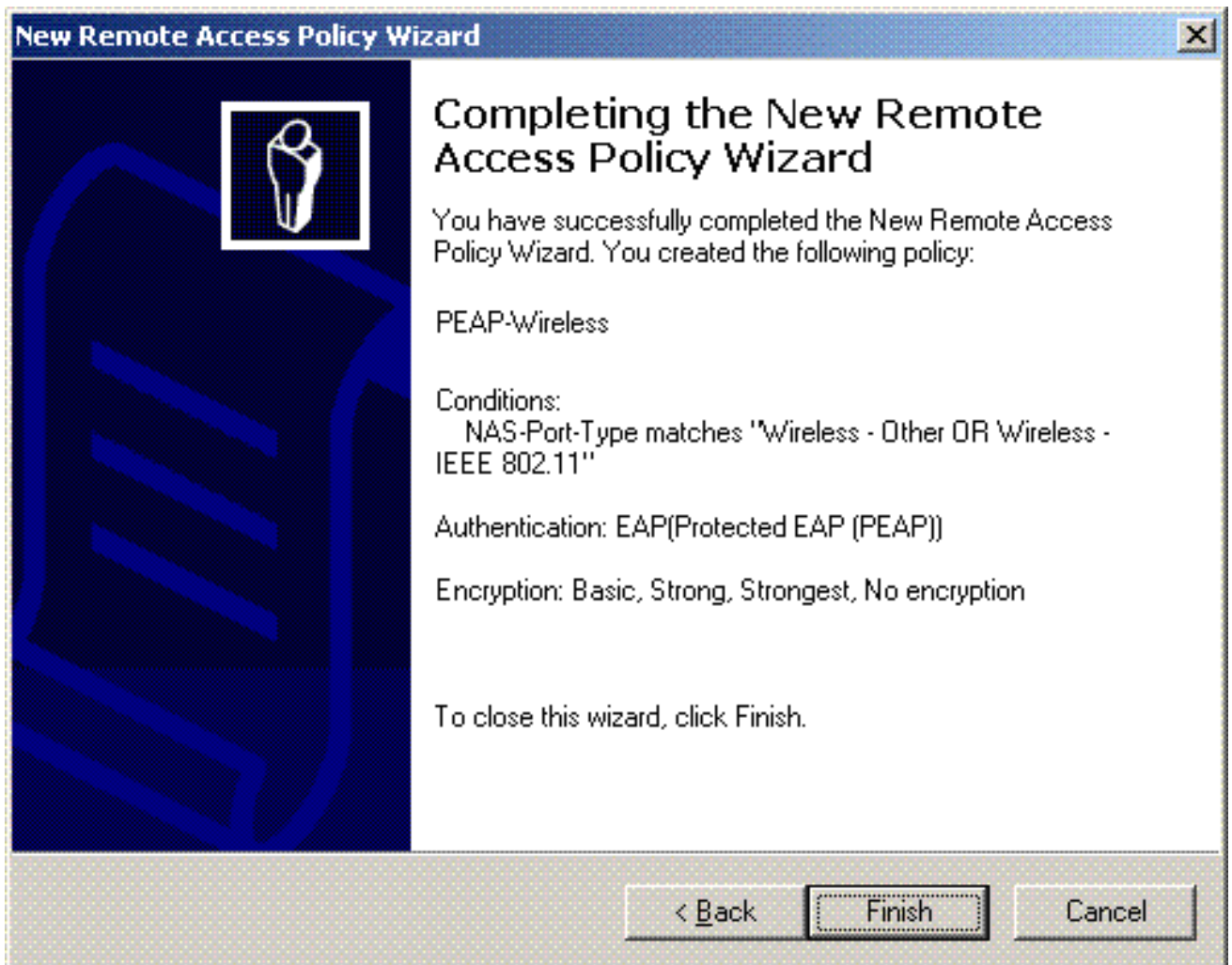


16. Sur la page **Protected EAP Properties** , choisissez le certificat approprié du menu déroulant des certificats émis, puis cliquez sur

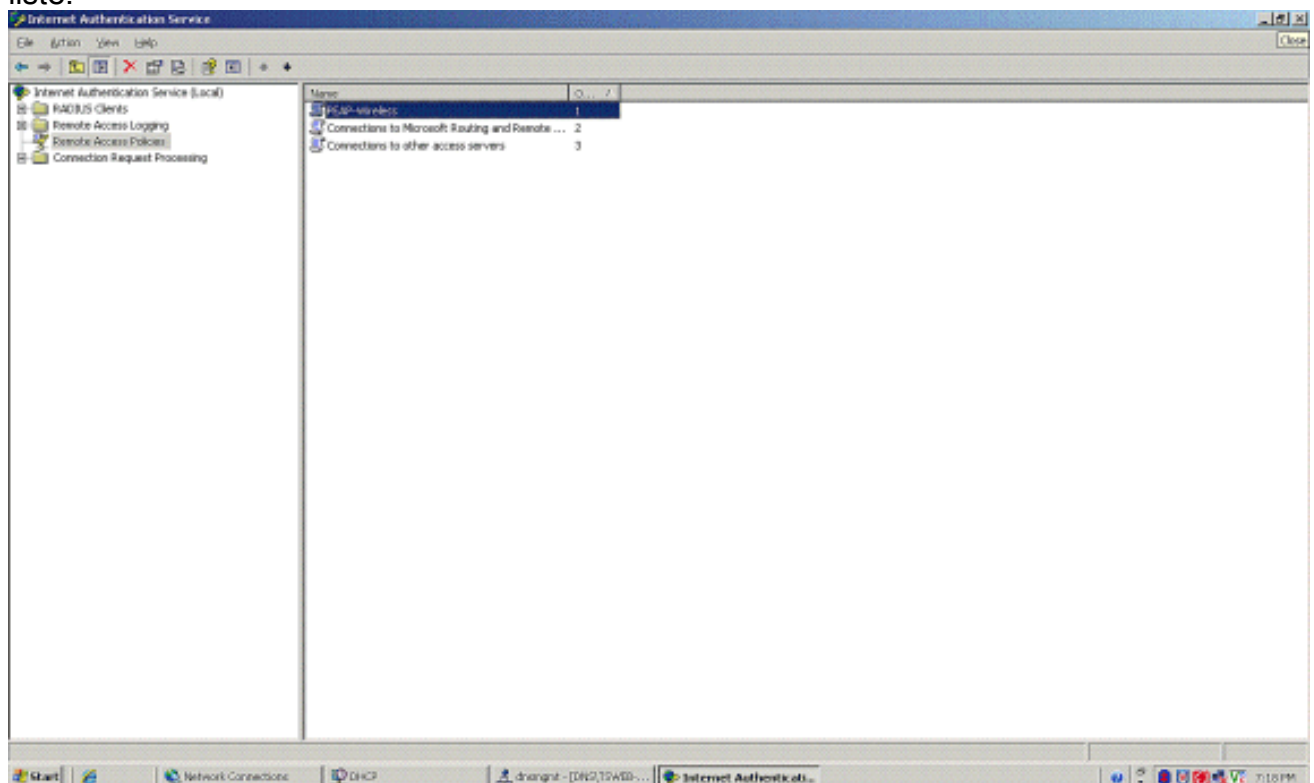


OK.

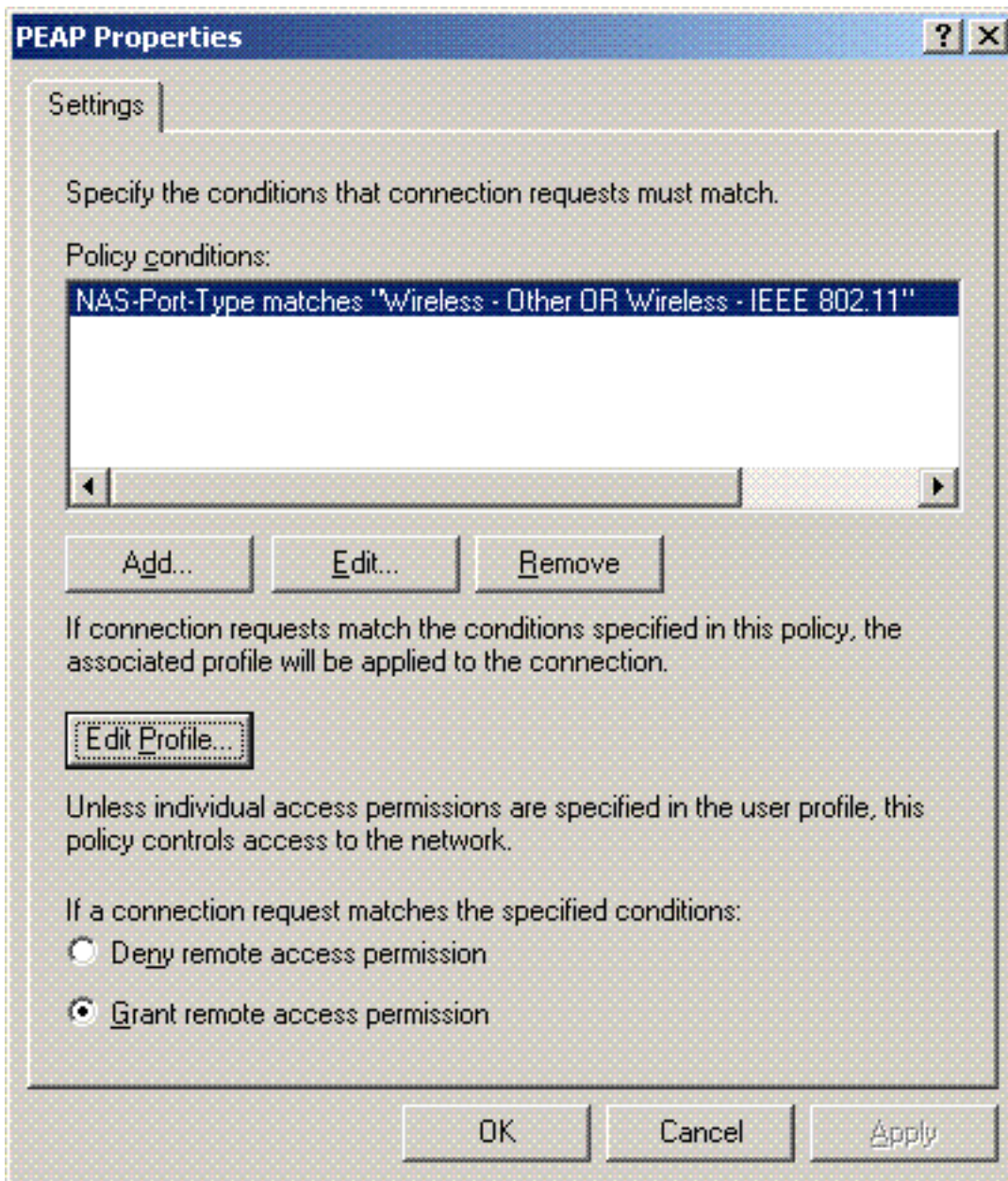
17. Vérifiez les détails de la stratégie d'accès à distance, puis cliquez sur **Finish**.



18. La stratégie d'accès à distance a été ajoutée à la liste.



19. Cliquez à droite sur la stratégie, puis cliquez **Properties**. Sélectionnez « **Grant remote access permission** » sous « **If a connection request matches the specified conditions**

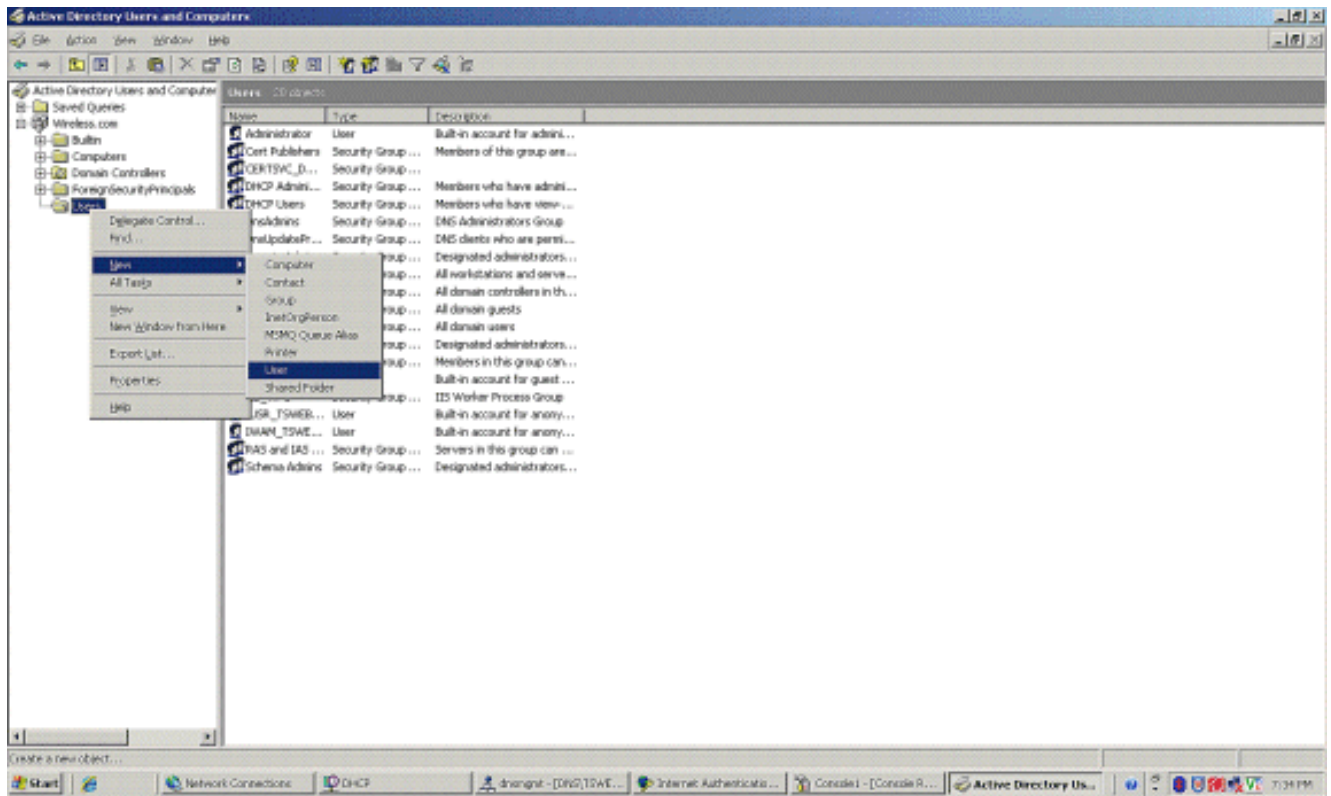


## [Ajoutez les utilisateurs à l'Active Directory](#)

Dans cette configuration, la base de données de l'utilisateur est mise à jour dans l'Active Directory.

Afin d'ajouter des utilisateurs à la base de données d'Active Directory, suivez ces étapes :

1. Dans l'arborescence de la console Utilisateurs et ordinateurs Active Directory, cliquez avec le bouton droit sur **Utilisateurs** ; cliquez sur **Nouveau** ; puis cliquez sur **Utilisateur**.




2. Dans le nouvel objet - boîte de dialogue de l'utilisateur, introduisez le nom de l'utilisateur sans fil. Cet exemple utilise le nom **WirelessUser** dans le premier champ d'identification et **WirelessUser** dans le champ d'identification de connexion d'utilisateur. Cliquez sur **Next**

The 'New Object - User' dialog box is shown. The 'Create in' field is set to 'Wireless.com/Users'. The 'First name' field contains 'Client 1' and the 'Initials' field is empty. The 'Last name' field is empty. The 'Full name' field contains 'Client 1'. The 'User logon name' field contains 'Client1' and the domain dropdown is set to '@Wireless.com'. The 'User logon name (pre-Windows 2000)' field contains 'WIRELESS\'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

(Suivant).

3. Dans le nouvel objet - boîte de dialogue d'utilisateur, saisissez un mot de passe de votre choix dans le champ mot de passe, puis confirmez les champs du mot de passe. Effacez la case à cocher **User must change password at next logon**, puis cliquez sur

**New Object - User** [X]

 Create in: Wireless.com/Users

---

Password:

Confirm password:

User must change password at next logon

User cannot change password

Password never expires

Account is disabled


---

< Back    Next >    Cancel

Next.

4. Dans le nouvel objet - boîte de dialogue d'utilisateur, cliquez sur

**New Object - User** [X]

 Create in: Wireless.com/Users

---

When you click Finish, the following object will be created:

Full name: Client 1

User logon name: Client1@Wireless.com

---

< Back    Finish    Cancel

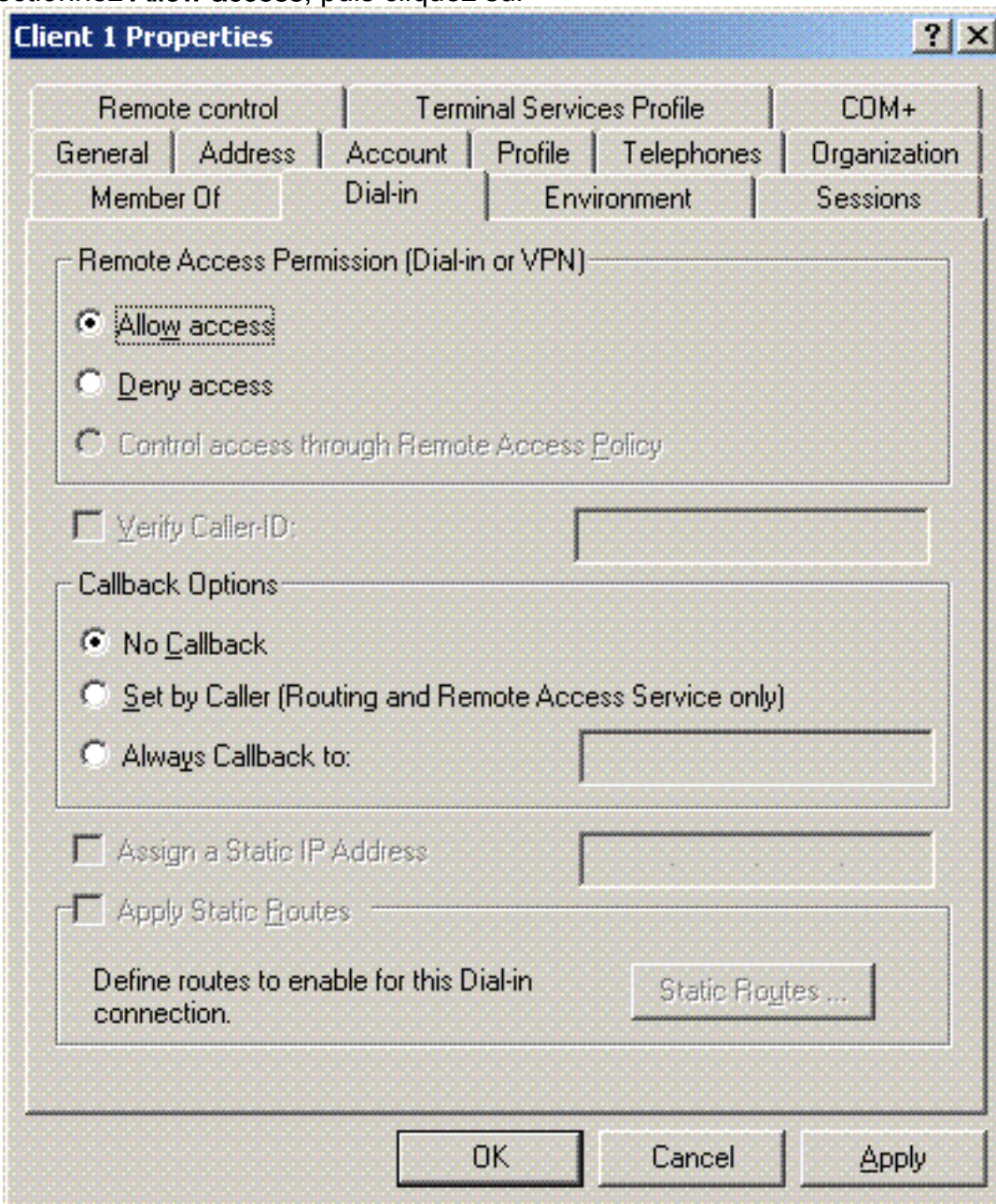
Finish.

5. Répétez les étapes 2 à 4 afin de créer des comptes d'utilisateur supplémentaires.

## Permettez l'accès sans fil aux utilisateurs

Procédez comme suit :

1. Dans l'arborescence de la console Utilisateurs et ordinateurs Active Directory, cliquez sur le dossier **Utilisateurs**, cliquez avec le bouton droit sur **WirelessUser**, cliquez sur **Propriétés**, puis accédez à l'onglet **Accès à distance**.
2. Sélectionnez **Allow access**, puis cliquez sur



OK.

## Configurez le contrôleur LAN sans fil et les AP légers

Configurez maintenant les périphériques sans fil pour cette configuration. Ceci inclut la configuration des contrôleurs LAN sans fil, des AP légers et des clients sans fil.

## Configurez le WLC pour l'authentification RADIUS par le serveur RADIUS de MS



## IAS

Configurez d'abord le WLC pour utiliser MS IAS en tant que serveur d'authentification. WLC doit être configuré afin de transférer les identifiants de l'utilisateur à un serveur RADIUS externe. Le serveur RADIUS externe valide alors les identifiants de l'utilisateur et permet d'accéder aux clients sans fil. À cette fin, ajoutez le serveur MS IAS en tant que serveur RADIUS dans la page **Security > RADIUS Authentication**.

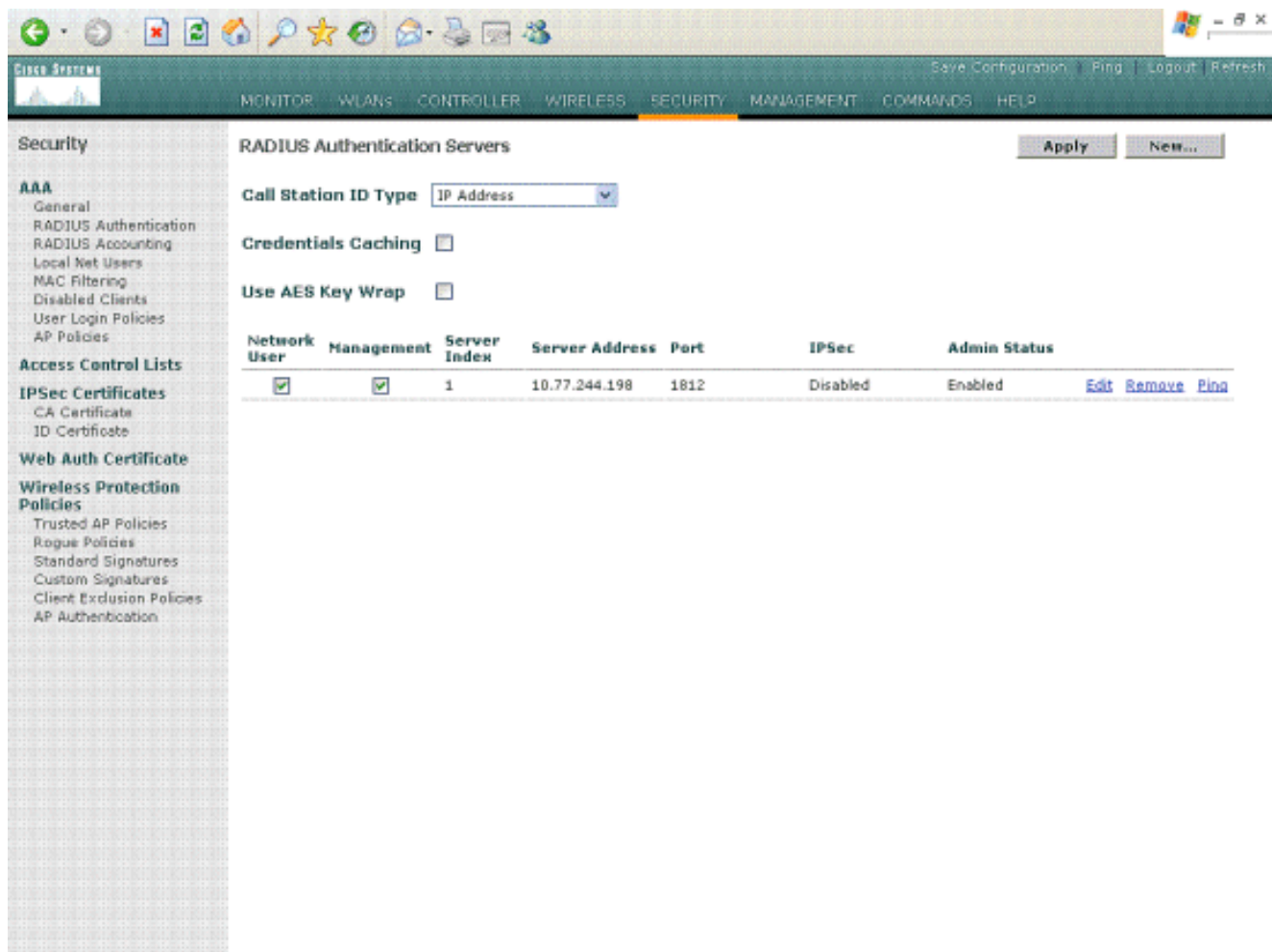
Procédez comme suit :

1. Sélectionnez **Security et RADIUS Authentication** depuis la GUI du contrôleur pour afficher la page des serveurs d'authentification RADIUS. Cliquez alors sur **New afin de définir un serveur RADIUS**.

The screenshot shows the Cisco Systems GUI for configuring a new RADIUS Authentication Server. The page title is "RADIUS Authentication Servers > New". The configuration fields are as follows:

Field	Value
Server Index (Priority)	1
Server IP Address	10.77.244.198
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Key Wrap	<input type="checkbox"/>
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Retransmit Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

2. Définissez les paramètres du serveur RADIUS sur la page **RADIUS Authentication Servers > New** . Ces paramètres incluent l'adresse IP du serveur RADIUS, secret partagé, numéro de port et état du serveur. Les cases à cocher d'utilisateur du réseau et de gestion déterminent si l'authentification basée sur RADIUS s'applique pour la gestion et les utilisateurs du réseau. Cet exemple utilise MS IAS en tant que serveur RADIUS avec l'adresse IP 10.77.244.198.



3. Cliquez sur **Apply**.

4. Le serveur MS IAS a été ajouté au WLC en tant que serveur RADIUS et peut être utilisé pour authentifier des clients sans fil.

## Configurez un WLAN pour les clients de routage

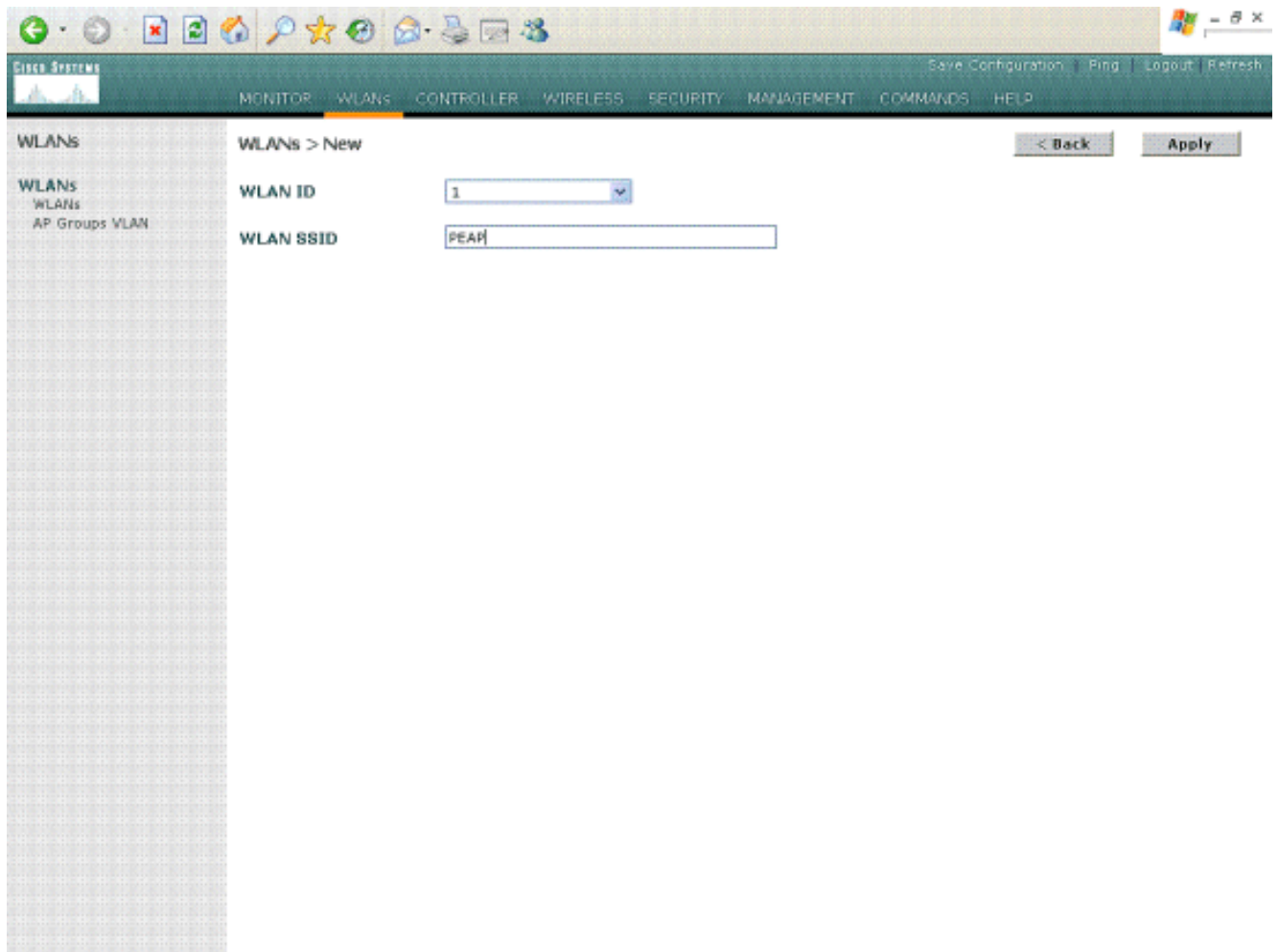
Configurez le SSID (WLAN) auquel les clients sans fil se connectent. Dans cet exemple, créez le SSID, puis nommez-le **PEAP**.

Définissez l'authentification de la couche 2 comme WPA2 de sorte que les clients exécutent l'authentification basée par EAP (PEAP-MSCHAPv2 dans ce cas) et utilise AES comme mécanisme de cryptage. Laissez toutes autres valeurs à leurs paramètres par défaut.

**Remarque** : ce document lie le WLAN aux interfaces de gestion. Quand vous avez plusieurs VLAN dans votre réseau, vous pouvez créer un VLAN séparé et le relier au SSID. Pour les informations sur la façon de configurer des VLAN sur les WLC, reportez-vous aux [VLAN sur l'exemple de configuration de contrôleurs LAN sans fil](#).

Afin de configurer un WLAN sur le WLC, suivez ces étapes :

1. Cliquez sur les **WLAN de la GUI du contrôleur afin d'afficher la page des WLAN**. Cette page énumère les WLAN qui existent sur le contrôleur.
2. Sélectionnez **New afin de créer un nouveau WLAN**. Saisissez l'ID WLAN et le SSID WLAN pour le WLAN, puis cliquez sur **Apply**.



3. Une fois que vous avez créé un nouveau WLAN, la page **WLAN > Edit du nouveau WLAN apparaît**. Sur cette page, vous pouvez définir les divers paramètres spécifiques à ce WLAN qui incluent des stratégies générales, des serveurs RADIUS, des stratégies de sécurisation et des paramètres 802.1x.

4. Vérifiez l'état admin sous les stratégies générales afin d'activer le WLAN. Si vous voulez qu'AP diffuse le SSID dans ses trames balises, vérifiez le **SSID de diffusion**.
5. Sous Layer 2 Security, sélectionnez **WPA1+WPA2**. Ceci active le WPA sur le WLAN. Déroulez la page et choisissez le stratégie WPA. Cet exemple utilise le WPA2 et le cryptage AES. Choisissez le serveur RADIUS approprié du menu déroulant sous serveurs RADIUS. Dans cet exemple, utilisez **10.77.244.198 (adresse IP du serveur MS IAS)**. Les autres paramètres peuvent être modifiés sur les conditions requises du réseau WLAN.

6. Cliquez sur **Apply**.

Profile Name	WLAN ID	WLAN SSID	Admin Status	Security Policies
PEAP	1	PEAP	Enabled	[WPA2][Auth(802.1x)]

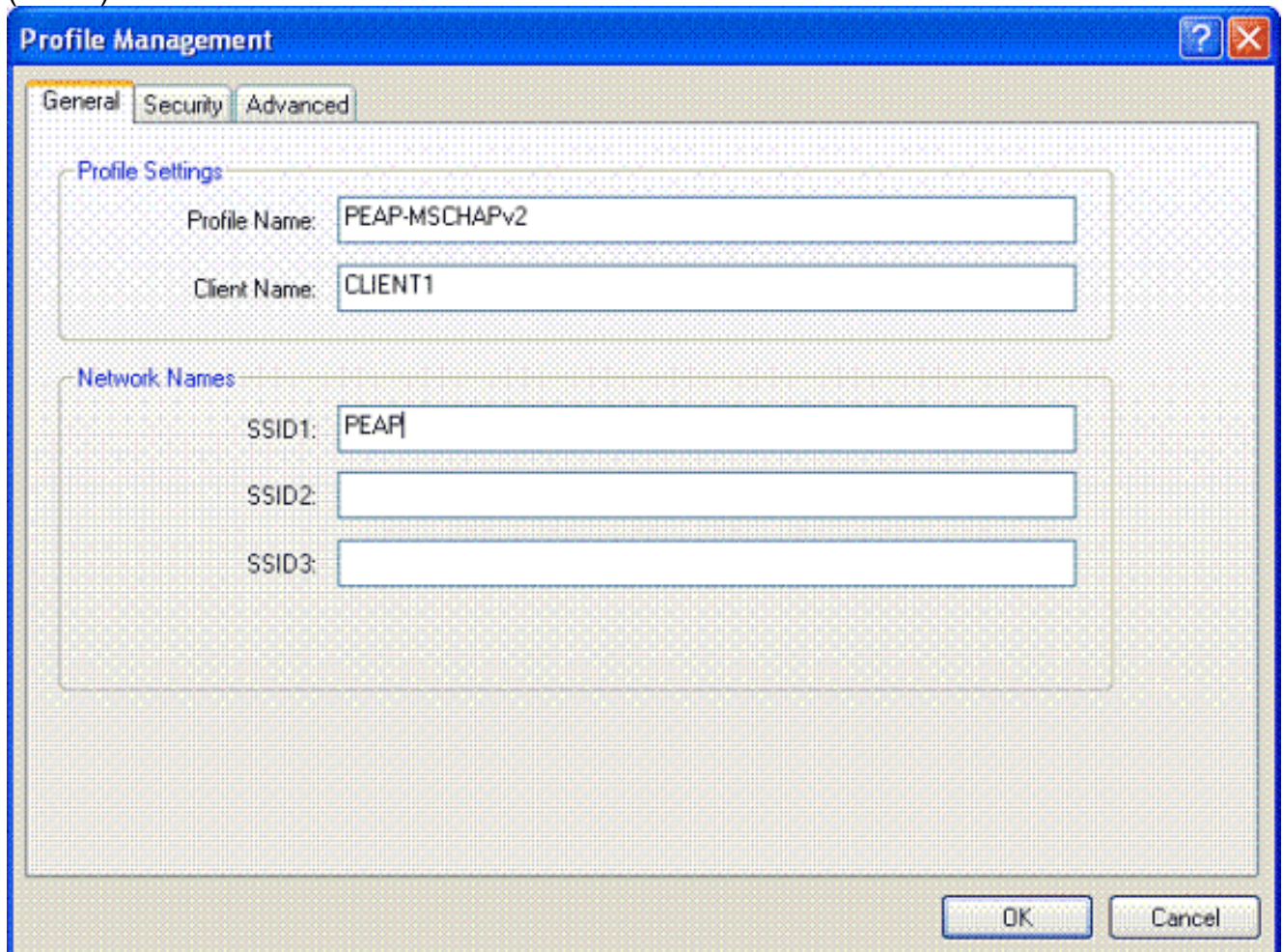
## Configurez les clients sans fil

### Configurez les clients sans fil pour l'authentification PEAP-MS CHAPv2

Cet exemple fournit des informations sur la façon de configurer le client sans fil avec l'utilitaire de bureau Cisco Aironet. Avant de configurer l'adaptateur client, assurez-vous que la dernière version du microprogramme et l'utilitaire sont utilisés. Recherchez la dernière version du microprogramme et les utilitaires dans la page de téléchargements sans fil sur Cisco.com.

Afin de configurer l'adaptateur du client sans fil de Cisco Aironet 802.11 a/b/g avec l'ADU, suivez ces étapes :

1. Ouvrez l'utilitaire de bureau d'Aironet.
2. Cliquez sur **Profile Management**, puis cliquez sur **New pour définir un profil**.
3. Sous l'onglet général, saisissez le nom du profil et le SSID. Dans cet exemple, utilisez le SSID que vous avez configuré sur le WLC (PEAP).

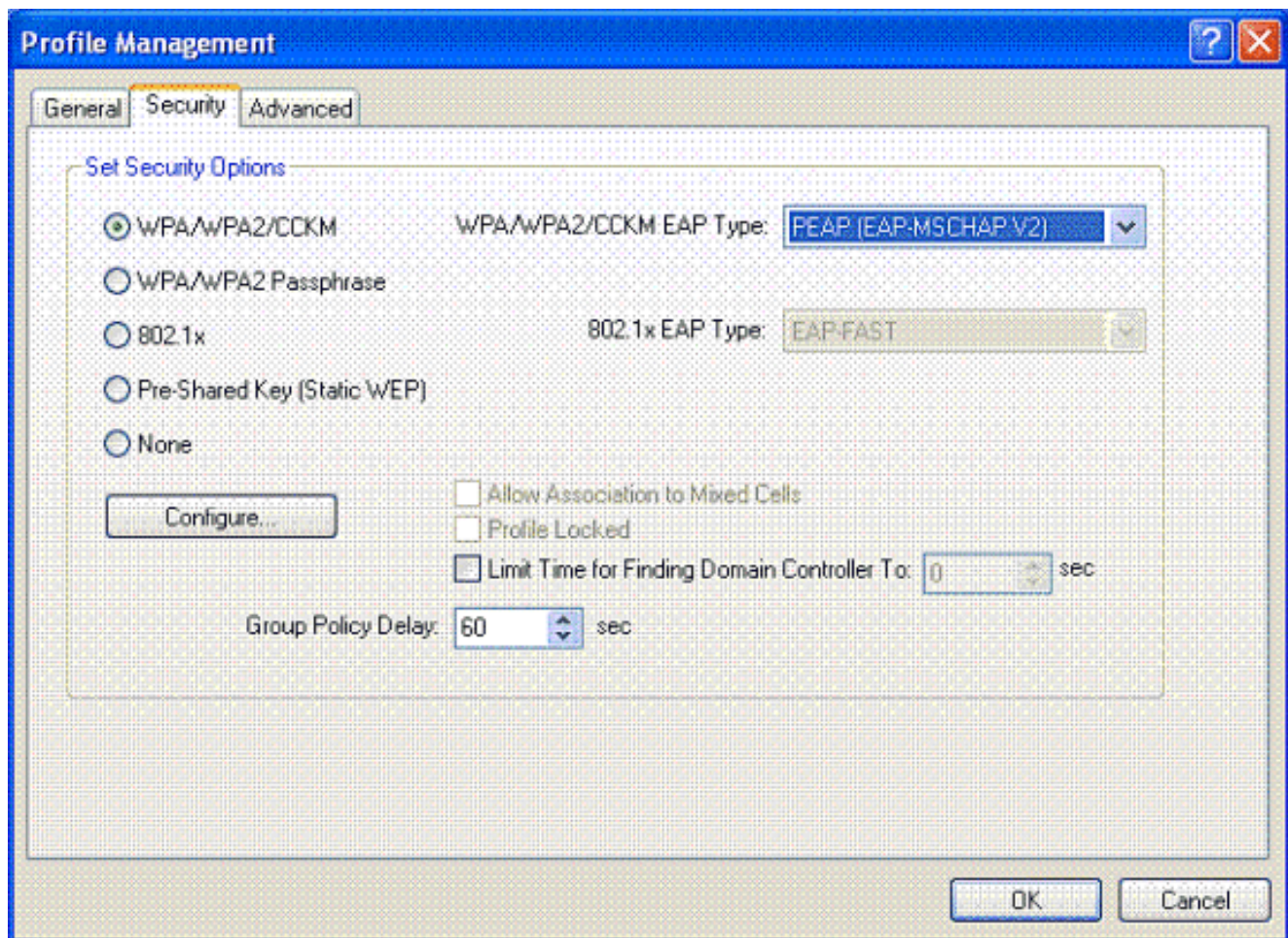


The screenshot shows the 'Profile Management' dialog box with the following fields:

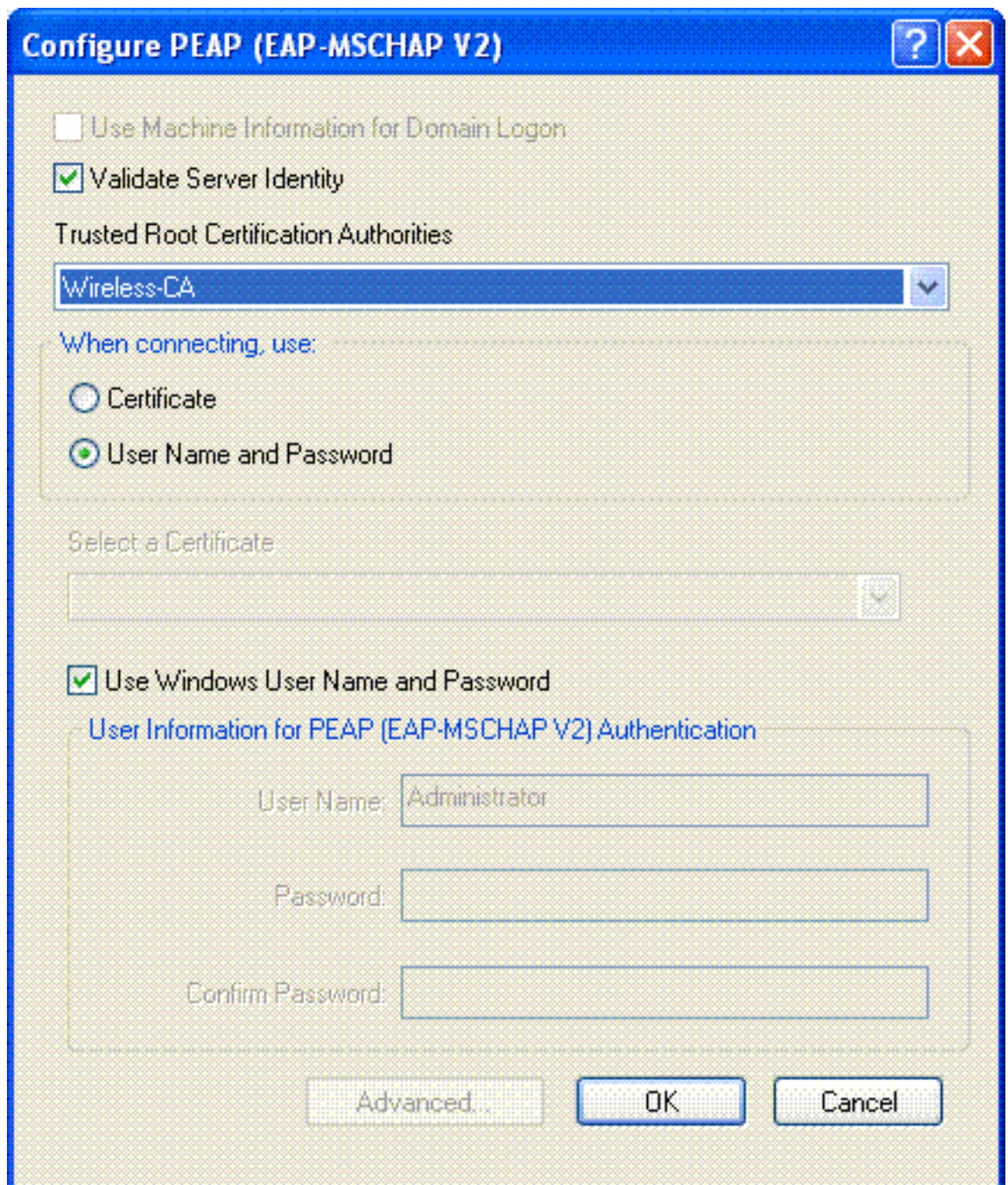
- Profile Name:** PEAP-MSCHAPv2
- Client Name:** CLIENT1
- SSID1:** PEAP
- SSID2:** (empty)
- SSID3:** (empty)

Buttons: OK, Cancel

4. Sélectionnez l'onglet Security, choisissez **WPA/WPA2/CCKM**, sous WPA/WPA2/CCKM EAP, tapez **PEAP [EAP-MSCHAPv2]**, puis cliquez sur **Configure**.



5. Sélectionnez **Validate Server Certificate**, puis choisissez **Wireless-CA** dans le menu déroulant **Trusted Root Certificate**

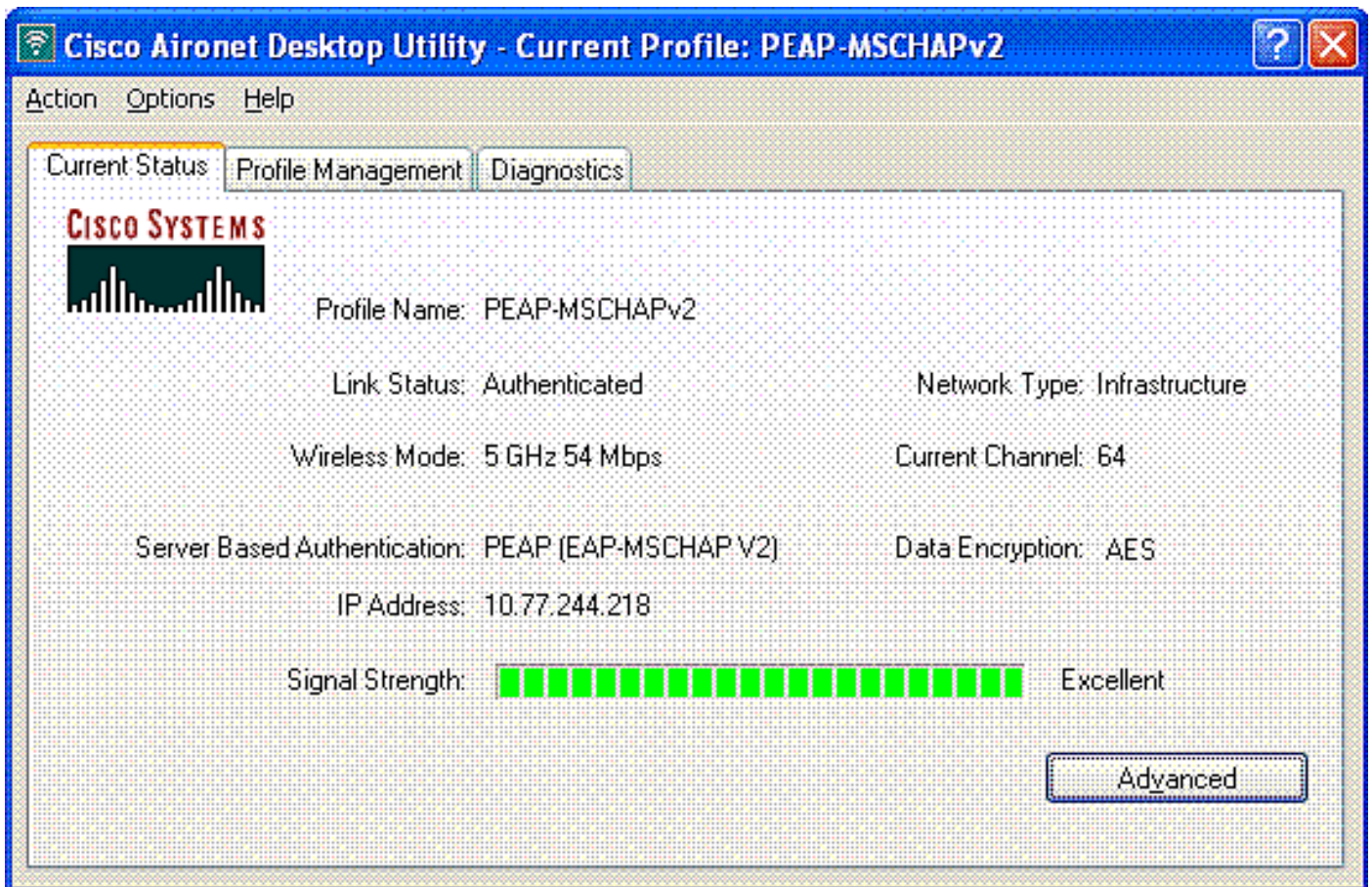


**Authorities.**

6. Cliquez sur **OK**, puis activez le profil. **Remarque** : lorsque vous utilisez le protocole PEAP-MSCHAPv2 (Protected EAP-Microsoft Challenge Handshake Authentication Protocol Version 2) avec Microsoft XP SP2 et que la carte sans fil est gérée par le système WZC (Microsoft Wireless Zero Configuration), vous devez appliquer le correctif logiciel Microsoft KB885453. Ceci évite plusieurs problèmes d'authentification liés à PEAP Fast Resume.

## Vérifiez et dépannez

Afin de vérifier si la configuration fonctionne comme prévu, activez le profil PEAP-MSCHAPv2 sur le client sans fil Client1.



Une fois que le profil PEAP-MSCHAPv2 est activé sur l'ADU, le client exécute l'authentification ouverte de 802.11, puis exécute l'authentification PEAP-MSCHAPv2. Voici un exemple d'authentification PEAP-MSCHAPv2 réussie.

Utilisez les commandes de débogage pour comprendre l'ordre des opérations qui se produisent.

L'[Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\)](#) prend en charge certaines commandes `show`. Utilisez l'OIT pour afficher une analyse de la sortie de la commande `show`.

Ces commandes de débogage sur le contrôleur LAN sans fil sont utiles.

- **debug dot1x events enable** - Afin de configurer le débogage des événements de 802.1x
- **debug aaa events enable** - Afin de configurer le débogage des événements AAA
- **debug mac addr <mac address>** - Afin de configurer le débogage MAC, utilisez la commande de débogage mac
- **debug dhcp message enable** - Afin de configurer le débogage des messages d'erreur DHCP

Ce sont les exemples de résultat de la commande **debug dot1x events enable** et de la commande **debug client <mac address>**.

**debug dot1x events enable:**

```
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received EAPOL START from
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Sending EAP-Request/Identity to
mobile 00:40:96:ac:e6:57 (EAP Id 2)
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received Identity Response (count=2) from
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
```





**mobile 00:40:96:ac:e6:57 (EAP Id 13)**  
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending default RC4 key to**  
**mobile 00:40:96:ac:e6:57**  
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending Key-Mapping RC4 key to**  
**mobile 00:40:96:ac:e6:57**  
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Received Auth Success while in**  
**Authenticating state for mobile 00:40:96:ac:e6:57**

**debug mac addr <MAC Address>:**

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Association received from**  
**mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0**  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 STA: 00:40:96:ac:e6:57 -  
rates (8): 12 18 24 36 48 72 96 108 0 0 0 0 0 0  
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 RUN (20)**  
**Change state to START (0)**  
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0)**  
**Initializing policy**  
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0)**  
**Change state to AUTHCHECK (2)**  
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 AUTHCHECK (2)**  
**Change state to 8021X\_REQD (3)**  
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 8021X\_REQD (3)**  
Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Changing state for**  
**mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated**  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Stopping deletion of  
Mobile Station: 00:40:96:ac:e6:57 (callerId: 48)  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending Assoc Response to  
station 00:40:96:ac:e6:57 on BSSID 00:0b:85:51:5a:e0 (status 0)  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Changing state for  
mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 Removed NPU entry.  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 dot1x - moving  
mobile 00:40:96:ac:e6:57 into Connecting state  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Sending EAP-**  
**Request/Identity to mobile 00:40:96:ac:e6:57 (EAP Id 1)**  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Received EAPOL START from**  
**mobile 00:40:96:ac:e6:57**  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **EAP State update from**  
**Connecting to Authenticating for mobile 00:40:96:ac:e6:57**  
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 dot1x -**  
**moving mobile 00:40:96:ac:e6:57 into Authenticating state**  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Processing Access-Challenge for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Req state (id=3) for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
**Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 3)**  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
**Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25)**  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Processing Access-Challenge for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Req state (id=4) for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 4)  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57

Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25)  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Processing Access-Challenge for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Req state (id=5) for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 5)  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25)  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Processing Access-Challenge for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Req state (id=6) for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6)  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25)  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Processing Access-Challenge for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Req state (id=10) for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10)  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25)  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Processing Access-Challenge for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Req state (id=11) for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
**Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 11)**  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
**Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25)**  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
**Processing Access-Accept for mobile 00:40:96:ac:e6:57**  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
**Creating a new PMK Cache Entry for station 00:40:96:ac:e6:57 (RSN 0)**  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
**Sending EAP-Success to mobile 00:40:96:ac:e6:57 (EAP Id 12)**  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
**Sending default RC4 key to mobile 00:40:96:ac:e6:57**  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
**Sending Key-Mapping RC4 key to mobile 00:40:96:ac:e6:57**  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218  
8021X\_REQD (3) **Change state to L2AUTHCOMPLETE (4)**  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218  
L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218  
L2AUTHCOMPLETE (4) Change state to RUN (20)  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN  
(20) Reached PLUMBFASPATH: from line 4041  
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN  
(20) Replacing Fast Path rule  
type = Airespace AP Client

```
on AP 00:0b:85:51:5a:e0, slot 0, interface = 2
ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20)
Card = 0 (slot 0), InHandle = 0x00000000,
OutHandle = 0x00000000, npuCryptoFlag = 0x0000
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Successfully plumbed mobile rule (ACL ID 255)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Reached RETURN: from line 4041
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend
Auth Success state (id=12) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Received Auth Success
while in Authenticating state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 dot1x -
moving mobile 00:40:96:ac:e6:57 into Authenticated state
```

**Remarque :** si vous utilisez le demandeur Microsoft pour vous authentifier auprès d'un Cisco Secure ACS pour l'authentification PEAP, le client risque de ne pas s'authentifier correctement. Parfois la connexion initiale peut authentifier avec succès, mais les tentatives ultérieures d'authentification de connexion rapide ne se connectent pas avec succès. Il s'agit d'un problème identifié. Les détails de ce problème et du respectif correctif sont disponibles [ici](#).

## [Informations connexes](#)

- [PEAP sous des réseaux sans fil unifiés avec ACS 4.0 et Windows 2003](#)
- [Exemple de configuration de l'authentification EAP avec des contrôleurs de réseau local sans fil \(WLC\)](#)
- [Mise à niveau logicielle de Wireless LAN Controller \(WLC\) aux versions 3.2, à 4,0 et 4,1](#)
- [Guides de configuration de Wireless LAN Controllers de la gamme Cisco 4400](#)
- [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.