

EAP-TLS sous un réseau sans fil unifié avec ACS 4.0 et Windows 2003

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Diagramme du réseau](#)

[Conventions](#)

[Installation de Windows Enterprise 2003 avec IIS, autorité de certification, DNS, DHCP \(DC CA\)
DC CA \(sans fil démocrate\)](#)

[Installation de Windows Standard 2003 avec Cisco Secure ACS 4.0](#)

[Installation et configuration de base](#)

[Installation de Cisco Secure ACS 4.0](#)

[Configuration du contrôleur LWAPP Cisco](#)

[Créer la configuration requise pour WPA2/WPA](#)

[Authentification EAP-TLS](#)

[Installer le composant logiciel enfichable Modèles de certificat](#)

[Créer le modèle de certificat pour le serveur Web ACS](#)

[Activer le nouveau modèle de certificat de serveur Web ACS](#)

[Configuration du certificat ACS 4.0](#)

[Configurer un certificat exportable pour ACS](#)

[Installer le certificat dans le logiciel ACS 4.0](#)

[Configuration CLIENT pour EAP-TLS à l'aide de Windows Zero Touch](#)

[Installation et configuration de base](#)

[Configuration de la connexion réseau sans fil](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer un accès sans fil sécurisé à l'aide de contrôleurs de réseau local sans fil (WLC), du logiciel Microsoft Windows 2003 et du serveur de contrôle d'accès sécurisé Cisco (ACS) 4.0 via Extensible Authentication Protocol-Transport Layer Security (EAP-TLS).

Remarque : Pour plus d'informations sur le déploiement d'un réseau sans fil sécurisé, consultez le [site Microsoft Wi-Fi](#) et le [plan d'action sans fil Cisco SAFE](#).

Conditions préalables

Conditions requises

Il est supposé que le programme d'installation connaît l'installation de base de Windows 2003 et l'installation du contrôleur Cisco, car ce document ne couvre que les configurations spécifiques pour faciliter les tests.

Pour l'installation initiale et les informations de configuration pour les contrôleurs de la gamme Cisco 4400, consultez le Guide de démarrage rapide : [Contrôleurs de réseau local sans fil de la gamme Cisco 4400](#) Pour l'installation initiale et les informations de configuration pour les contrôleurs de la gamme Cisco 2000, consultez le Guide de démarrage rapide : [Contrôleurs de réseau local sans fil de la gamme Cisco 2000](#)

Avant de commencer, installez le système d'exploitation Windows Server 2003 avec Service Pack (SP)1 sur chacun des serveurs des travaux pratiques de test et mettez à jour tous les Service Packs. Installez les contrôleurs et les points d'accès et assurez-vous que les dernières mises à jour logicielles sont configurées.

Important : Au moment de la rédaction de ce document, SP1 est la dernière mise à jour de Windows Server 2003 et SP2 avec correctifs de mise à jour est le dernier logiciel pour Windows XP Professionnel.

Windows Server 2003 avec SP1, Enterprise Edition, est utilisé pour que l'inscription automatique des certificats utilisateur et de station de travail pour l'authentification EAP-TLS puisse être configurée. Ceci est décrit dans la section [Authentification EAP-TLS](#) de ce document. L'inscription automatique et le renouvellement automatique des certificats facilitent le déploiement des certificats et améliorent la sécurité en expirant et en renouvelant automatiquement les certificats.

Components Used

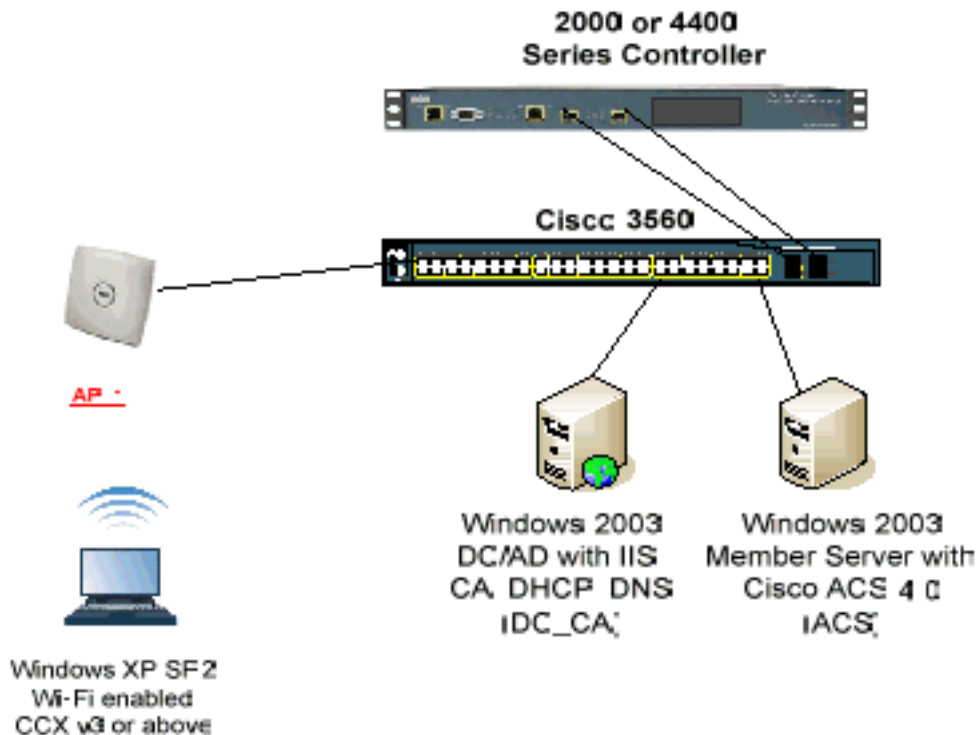
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur de la gamme Cisco 2006 ou 4400 qui exécute 3.2.116.21
- Protocole de point d'accès léger Cisco 1131 (LWAPP) AP
- Windows 2003 Entreprise avec Internet Information Server (IIS), Certificate Authority (CA), DHCP et Domain Name System (DNS) installés
- Windows 2003 Standard avec Access Control Server (ACS) 4.0
- Windows XP Professionnel avec SP (et Service Packs mis à jour) et carte réseau sans fil (avec prise en charge CCX v3) ou demandeur tiers.
- Commutateur du routage Cisco 3560

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Topologie de laboratoire sans fil sécurisée Cisco



L'objectif principal de ce document est de vous fournir la procédure pas à pas pour implémenter EAP-TLS sous Unified Wireless Networks avec ACS 4.0 et le serveur Windows 2003 Enterprise. L'accent principal est mis sur l'inscription automatique du client afin que le client s'inscrit automatiquement et prenne le certificat du serveur.

Remarque : Afin d'ajouter Wi-Fi Protected Access (WPA)/WPA2 avec TKIP (Temporal Key Integrity Protocol)/AES (Advanced Encryption Standard) à Windows XP Professionnel avec SP, référez-vous à [Mise à jour WPA2/Wireless Provisioning Services Information Element \(WPS IE\) pour Windows XP avec SP2](#) .

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

Conventions

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

Installation de Windows Enterprise 2003 avec IIS, autorité de certification, DNS, DHCP (DC_CA)

DC_CA (sans fil démocrate)

DC_CA est un ordinateur qui exécute Windows Server 2003 avec SP1, Enterprise Edition, et qui remplit les rôles suivants :

- Un contrôleur de domaine pour le domaine wirelessdemo.local qui exécute IIS
- Un serveur DNS pour le domaine DNS local de la démo sans fil
- Un serveur DHCP
- Autorité de certification racine de l'entreprise pour le domaine wirelessdemo.local

Complétez ces étapes afin de configurer DC_CA pour ces services :

1. [Effectuez une installation et une configuration de base.](#)
2. [Configurez l'ordinateur en tant que contrôleur de domaine.](#)
3. [Augmentez le niveau fonctionnel du domaine.](#)
4. [Installer et configurer DHCP](#)
5. [Installer les services de certificats.](#)
6. [Vérifiez les autorisations Administrateur pour les certificats.](#)
7. [Ajoutez des ordinateurs au domaine.](#)
8. [Autoriser l'accès sans fil aux ordinateurs.](#)
9. [Ajoutez des utilisateurs au domaine.](#)
10. [Autoriser l'accès sans fil aux utilisateurs.](#)
11. [Ajoutez des groupes au domaine.](#)
12. [Ajoutez des utilisateurs au groupe WirelessUsers.](#)
13. [Ajoutez des ordinateurs clients au groupe WirelessUsers.](#)

Étape 1 : Installation et configuration de base

Procédez comme suit :

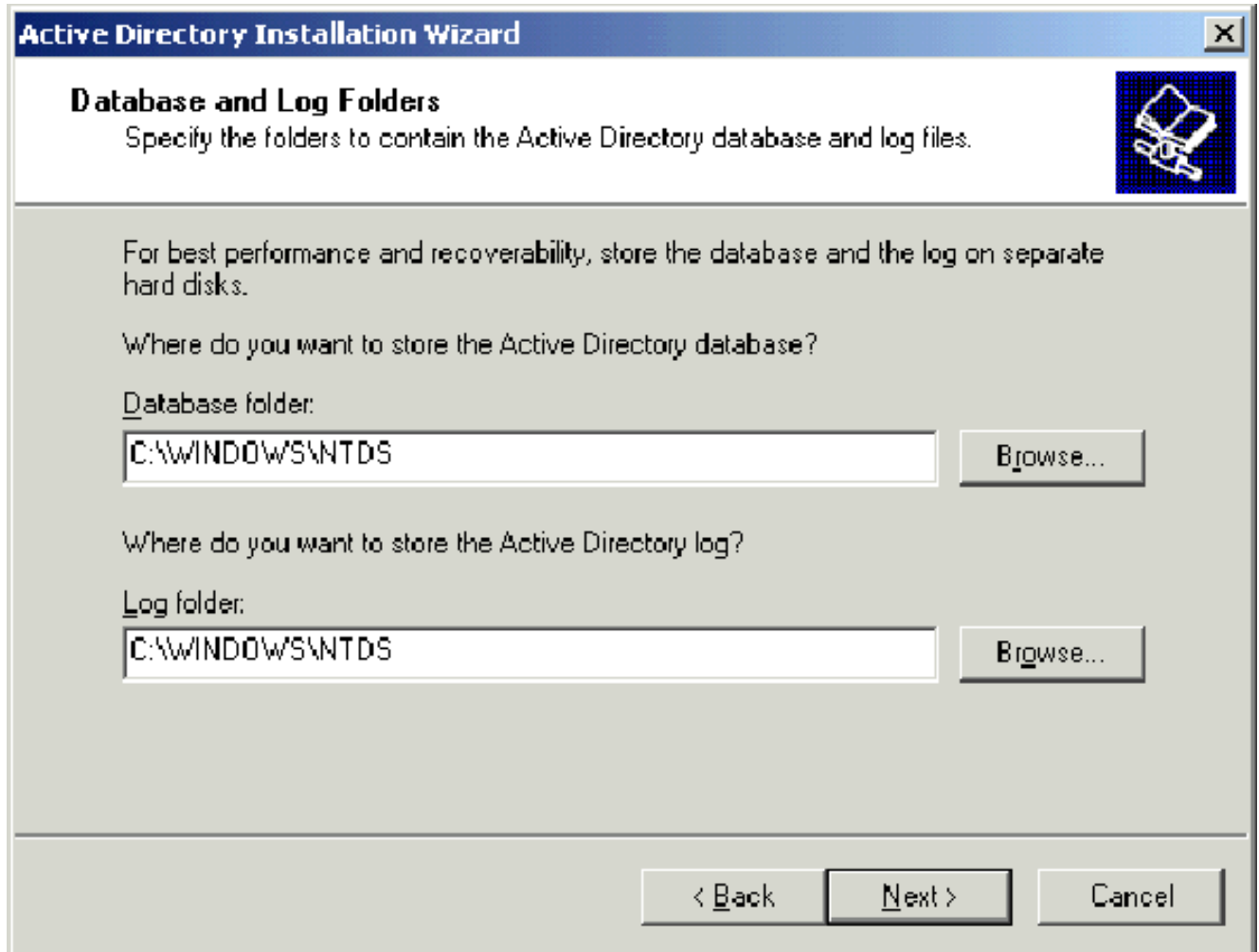
1. Installez Windows Server 2003 avec SP1, Enterprise Edition, en tant que serveur autonome.
2. Configurez le protocole TCP/IP avec l'adresse IP 172.16.100.26 et le masque de sous-réseau 255.255.255.0.

Étape 2 : Configurer l'ordinateur en tant que contrôleur de domaine

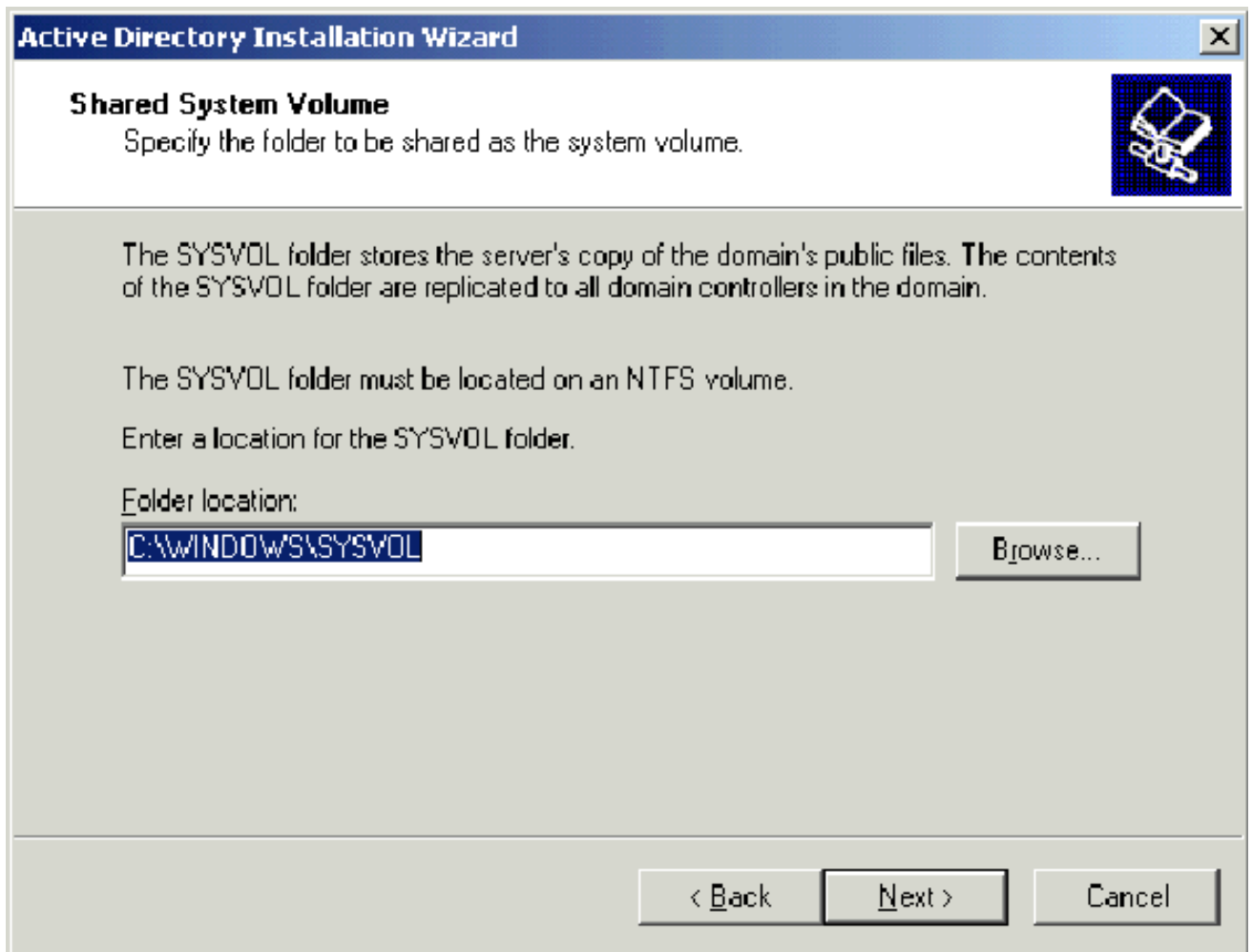
Procédez comme suit :

1. Afin de démarrer l'Assistant Installation d'Active Directory, choisissez **Démarrer > Exécuter**, tapez **dcpromo.exe**, puis cliquez sur **OK**.
2. Dans la page Bienvenue dans l'Assistant Installation d'Active Directory, cliquez sur **Suivant**.
3. Sur la page Compatibilité du système d'exploitation, cliquez sur **Suivant**.
4. Sur la page Type de contrôleur de domaine, sélectionnez **Contrôleur de domaine pour un nouveau domaine** et cliquez sur **Suivant**.
5. Sur la page Créer un nouveau domaine, sélectionnez **Domaine dans une nouvelle forêt** et cliquez sur **Suivant**.
6. Sur la page Installer ou configurer DNS, sélectionnez **Non, installez et configurez DNS sur cet ordinateur** et cliquez sur **Suivant**.
7. Sur la page Nouveau nom de domaine, tapez **wirelessdemo.local** et cliquez sur **Suivant**.
8. Sur la page Nom de domaine NetBIOS, entrez le nom de domaine NetBIOS en tant que **démonstration sans fil** et cliquez sur **Suivant**.

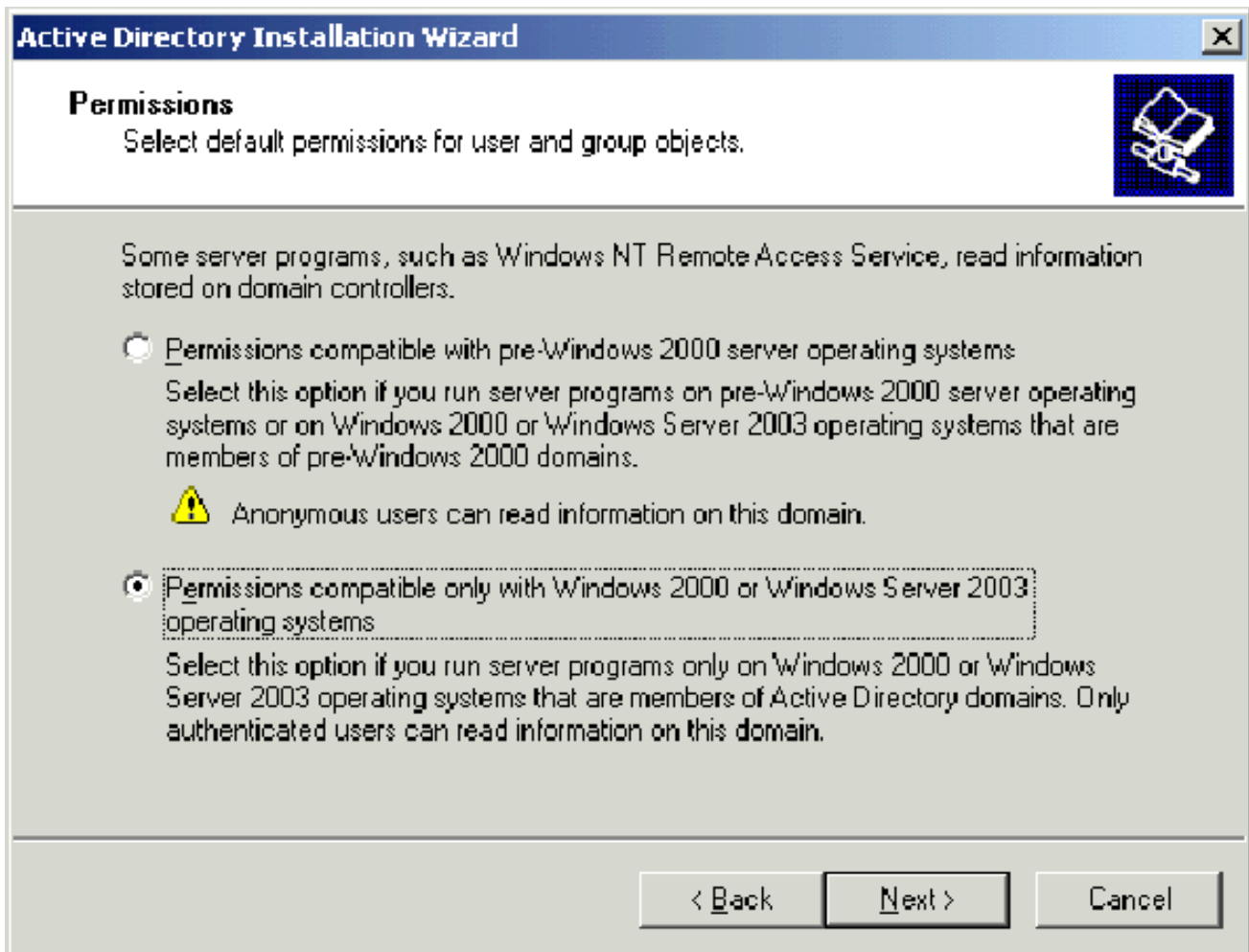
9. Sur la page Emplacement des dossiers de base de données et de journal, acceptez les répertoires de base de données et de dossiers journaux par défaut et cliquez sur **Suivant**.



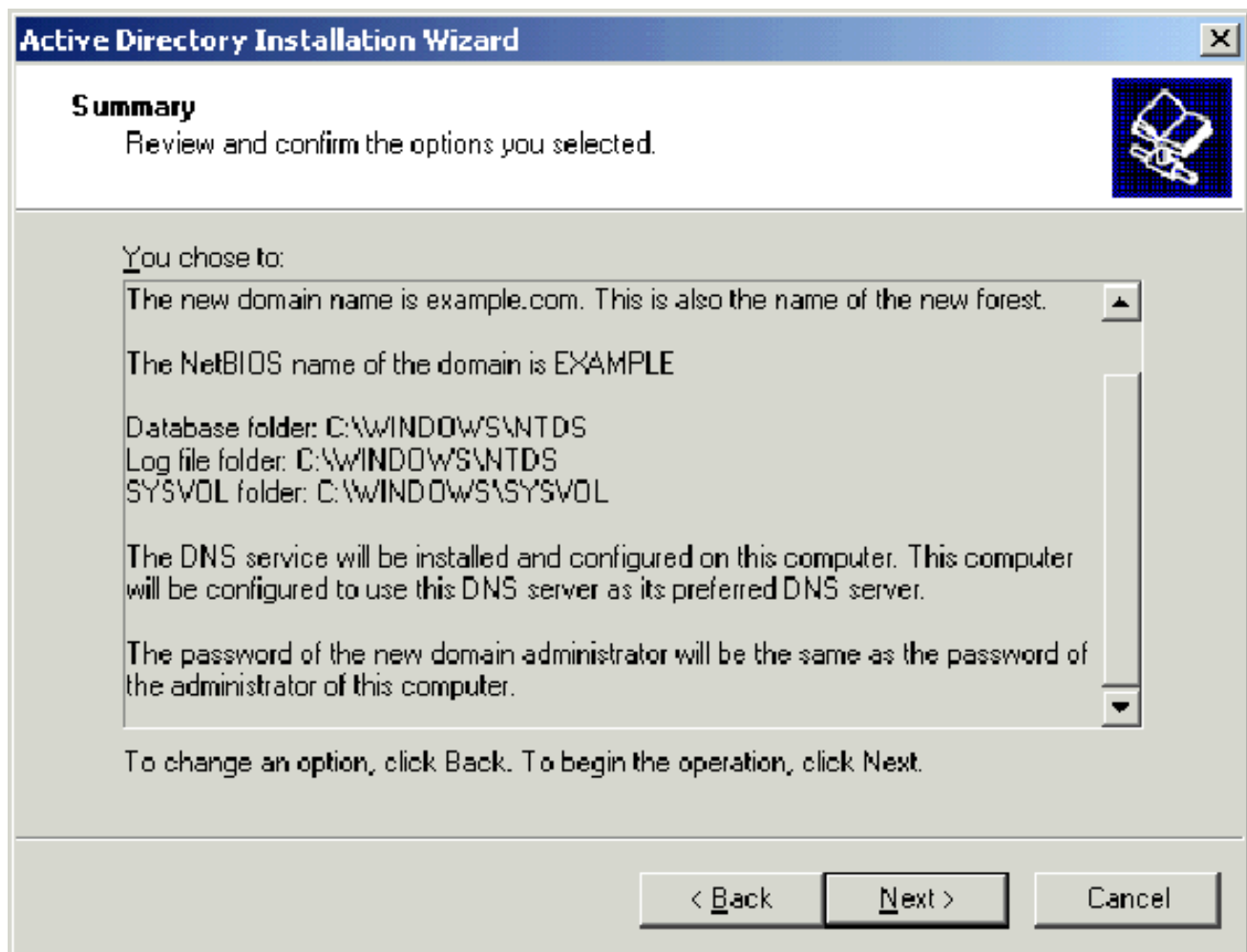
10. Dans la boîte de dialogue Volume du système partagé, vérifiez que l'emplacement du dossier par défaut est correct et cliquez sur **Suivant**.



11. Sur la page Autorisations, vérifiez que **Autorisations compatibles uniquement avec les systèmes d'exploitation Windows 2000 ou Windows Server 2003** est sélectionné et cliquez sur **Suivant**.



12. Sur la page Directory Services Restore Mode Administration Password, laissez les zones de mot de passe vides et cliquez sur **Next**.
13. Vérifiez les informations de la page Résumé et cliquez sur **Suivant**.

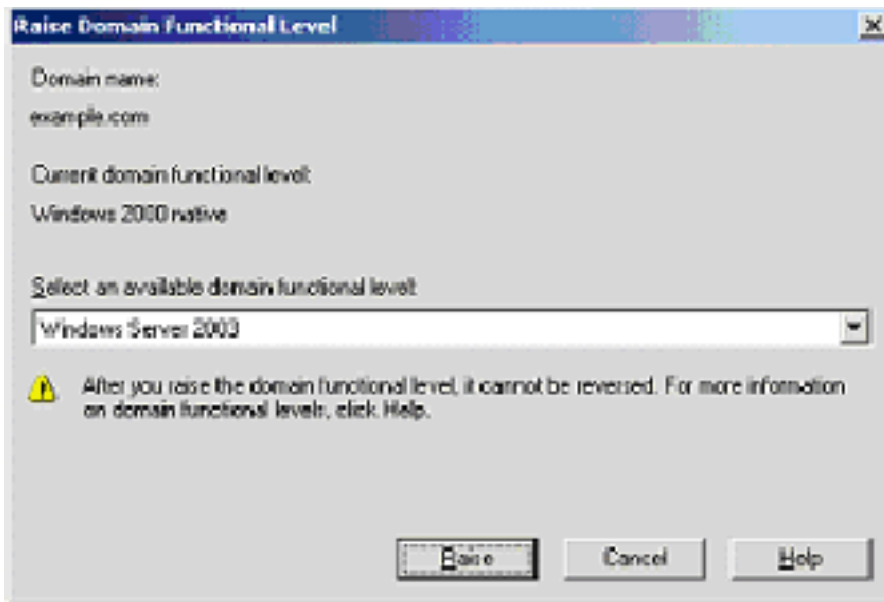


14. Sur la page Fin de l'Assistant Installation d'Active Directory, cliquez sur **Terminer**.
15. Lorsque vous êtes invité à redémarrer l'ordinateur, cliquez sur **Redémarrer maintenant**.

[Étape 3 : Augmenter le niveau fonctionnel du domaine](#)

Procédez comme suit :

1. Ouvrez le composant logiciel enfichable Domaines et approbations Active Directory dans le dossier **Outils d'administration (Démarrer > Outils d'administration > Domaines et approbations Active Directory)**, puis cliquez avec le bouton droit sur l'ordinateur de domaine **DC_CA.wirelessdemo.local**.
2. Cliquez sur **Augmenter le niveau fonctionnel du domaine**, puis sélectionnez **Windows Server 2003** sur la page Augmenter le niveau fonctionnel du



domaine.

3. Cliquez sur **Lever**, sur **OK**, puis sur **OK** à nouveau.

Étape 4 : Installation et configuration de DHCP

Procédez comme suit :

1. Installez le protocole DHCP (Dynamic Host Configuration Protocol) en tant que composant de service réseau à l'aide de l'option **Ajout/Suppression de programmes** du Panneau de configuration.
2. Ouvrez le composant logiciel enfichable DHCP à partir du dossier Outils d'administration (**Démarrer > Programmes > Outils d'administration > DHCP**, puis mettez en surbrillance le serveur DHCP, **DC_CA.wirelessdemo.local**).
3. Cliquez sur **Action**, puis sur **Autoriser** afin d'autoriser le service DHCP.
4. Dans l'arborescence de la console, cliquez avec le bouton droit sur **DC_CA.wirelessdemo.local**, puis cliquez sur **Nouvelle étendue**.
5. Sur la page de bienvenue de l'Assistant Nouvelle étendue, cliquez sur **Suivant**.
6. Sur la page Nom de l'étendue, tapez **CorpNet** dans le champ Nom.

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:

Description:

7. Cliquez sur **Suivant** et remplissez les paramètres suivants : Adresse IP de début : 172.16.100.1 Adresse IP de fin : 172.16.100.254 Longueur : 24 Masque de sous-réseau : 255.255.255.0

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:

End IP address:

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:

Subnet mask:

< Back

Next >

Cancel

8. Cliquez sur **Next** et saisissez **172.16.100.1** pour l'adresse IP de début et **172.16.100.100** pour l'adresse IP de fin à exclure. Cliquez ensuite **Next**. Cela réserve les adresses IP comprises entre 172.16.100.1 et 172.16.100.100. Ces adresses IP réservées ne sont pas attribuées par le serveur DHCP.

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:

Excluded address range:

9. Sur la page Durée du bail, cliquez sur **Suivant**.

10. Sur la page Configurer les options DHCP, sélectionnez **Oui, je veux configurer ces options maintenant** et cliquez sur **Suivant**.

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

11. Sur la page Router (Default Gateway), ajoutez l'adresse de routeur par défaut 172.16.100.1 et cliquez sur **Next**.

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

12. Sur la page Domain Name and DNS Servers, tapez **wirelessdemo.local** dans le champ Parent domain, tapez **172.16.100.26** dans le champ IP address, puis cliquez sur **Add** et sur **Next**.

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

172.16.100.26

Remove

Up

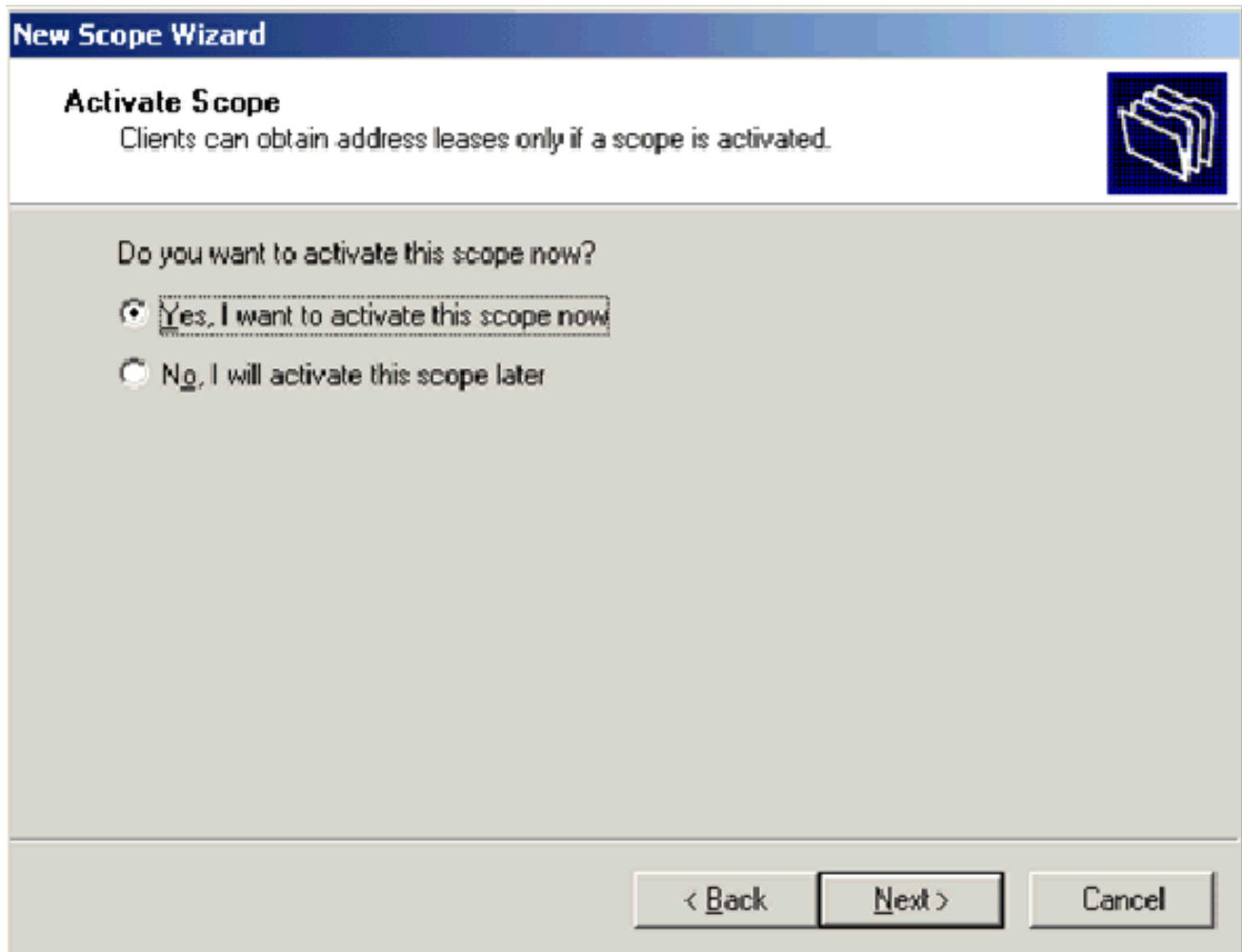
Down

< Back

Next >

Cancel

13. Sur la page WINS Servers, cliquez sur **Next**.
14. Sur la page Activer l'étendue, sélectionnez **Oui, je veux activer cette étendue maintenant** et cliquez sur **Suivant**.



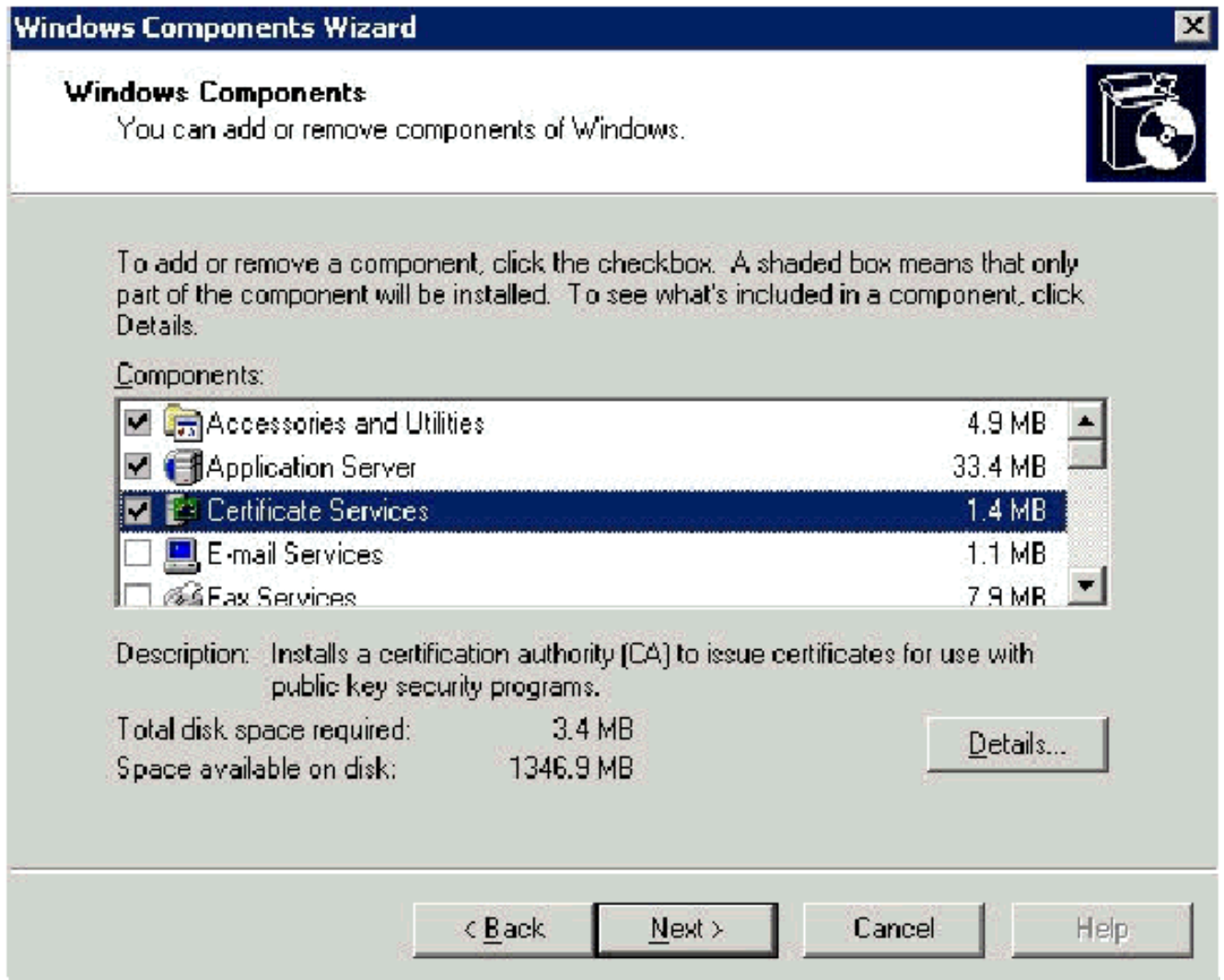
15. Sur la page Fin de l'Assistant Nouvelle étendue, cliquez sur **Terminer**.

[Étape 5 : Installer les services de certificats](#)

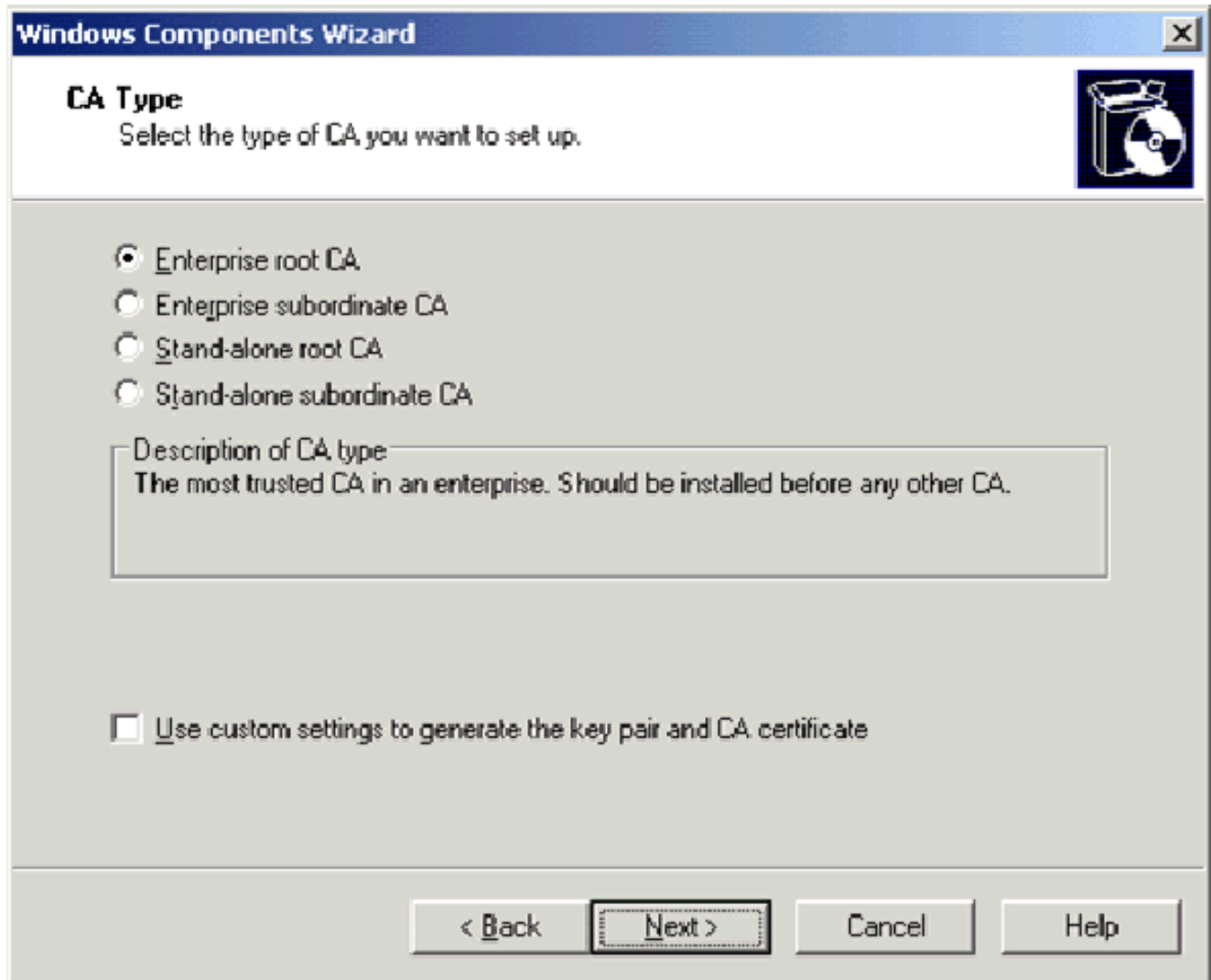
Procédez comme suit :

Remarque : IIS doit être installé avant d'installer les services de certificats et l'utilisateur doit faire partie de l'unité d'organisation Admin d'entreprise.

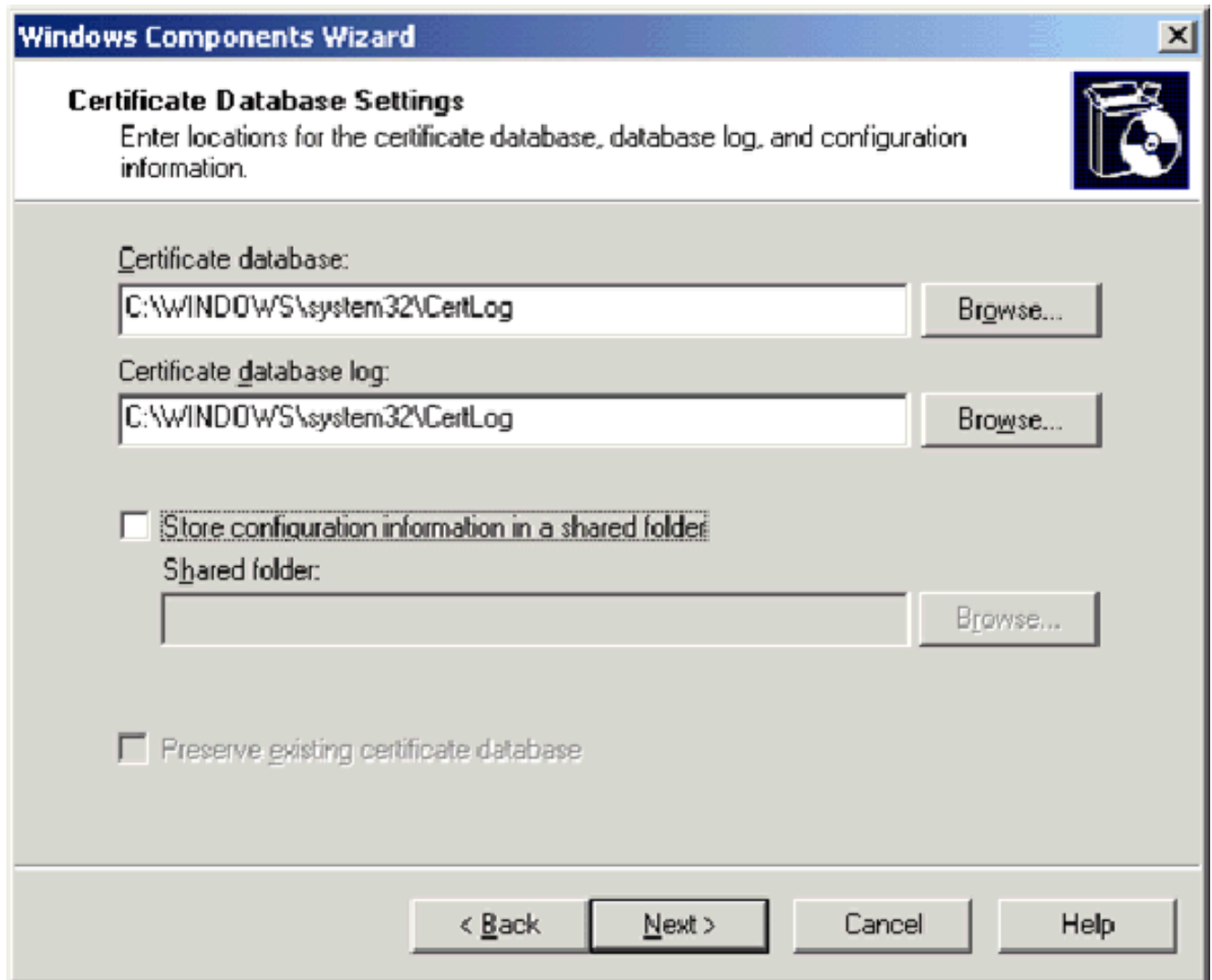
1. Dans le Panneau de configuration, ouvrez **Ajout/Suppression de programmes**, puis cliquez sur **Ajouter/Supprimer des composants Windows**.
2. Sur la page Assistant Composants Windows, sélectionnez **Services de certificats**, puis cliquez sur **Suivant**.



3. Sur la page Type d'autorité de certification, sélectionnez **Autorité de certification racine d'entreprise** et cliquez sur **Suivant**.



4. Sur la page d'informations d'identification de l'autorité de certification, tapez **wireless** democracy dans la zone Common name de cette autorité de certification. Vous pouvez entrer les autres détails facultatifs, puis cliquer sur **Suivant**. Acceptez les valeurs par défaut de la page Paramètres de la base de données de certificats.

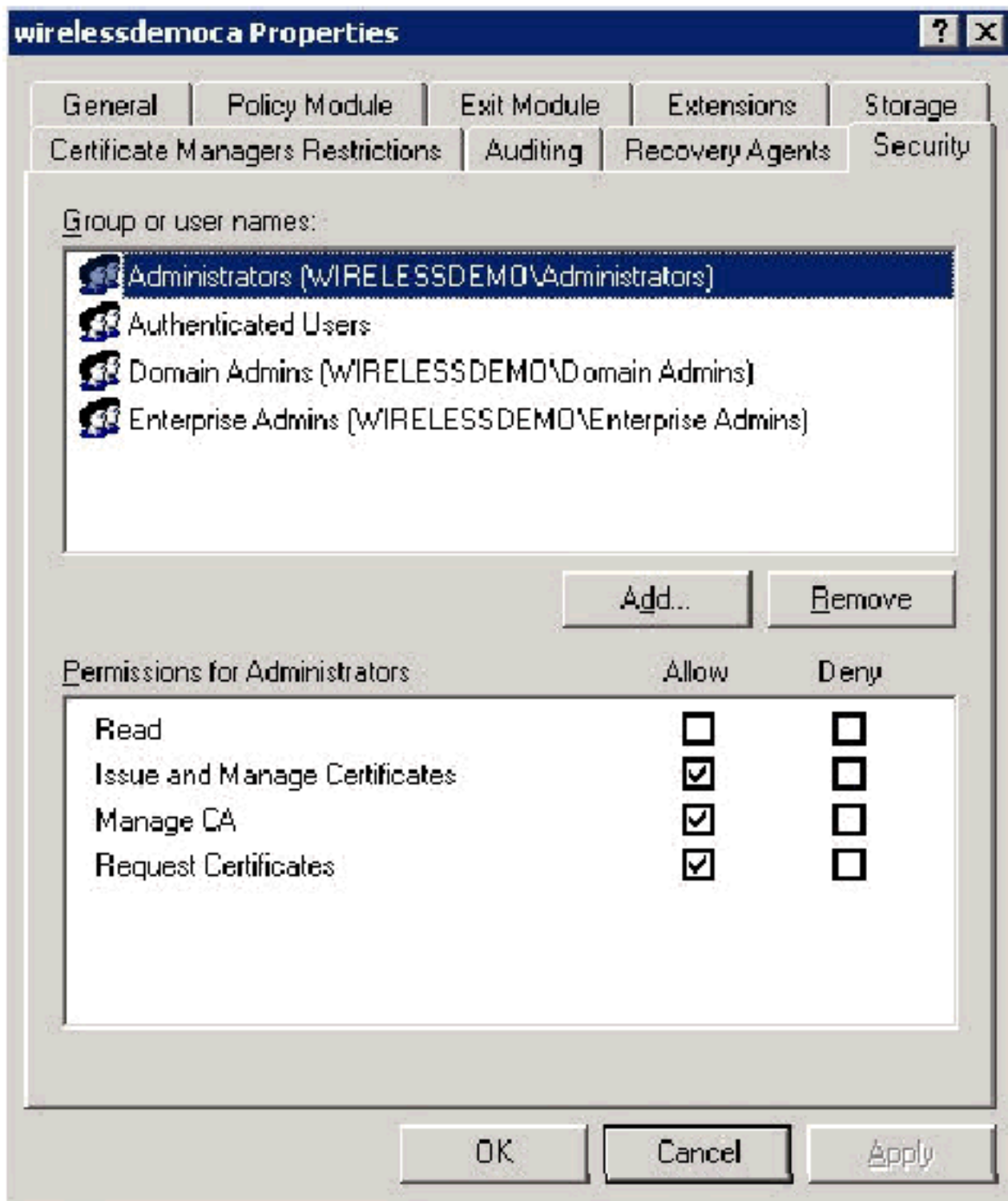


5. Cliquez sur **Next** (Suivant). Une fois l'installation terminée, cliquez sur **Terminer**.
6. Cliquez sur **OK** après avoir lu l'avertissement relatif à l'installation d'IIS.

[Étape 6 : Vérifier les autorisations d'administrateur pour les certificats](#)

Procédez comme suit :

1. Choisissez **Démarrer > Outils d'administration > Autorité de certification**.
2. Cliquez avec le bouton droit de la souris sur **Wireless Democratic CA**, puis cliquez sur **Propriétés**.
3. Dans l'onglet **Sécurité**, cliquez sur **Administrateurs** dans la liste des noms de groupe ou d'utilisateur.
4. Dans la liste **Autorisations** ou **Administrateurs**, vérifiez que ces options sont définies sur **Autoriser** :
Émettre et gérer des certificats
Gérer CAD
Demander des certificats
Si l'une de ces options est définie sur **Refuser** ou n'est pas sélectionnée, affectez la valeur **Autoriser** à l'autorisation.



5. Cliquez sur **OK** pour fermer la boîte de dialogue Propriétés de l'Autorité de certification de la démocratie sans fil, puis fermez Autorité de certification.

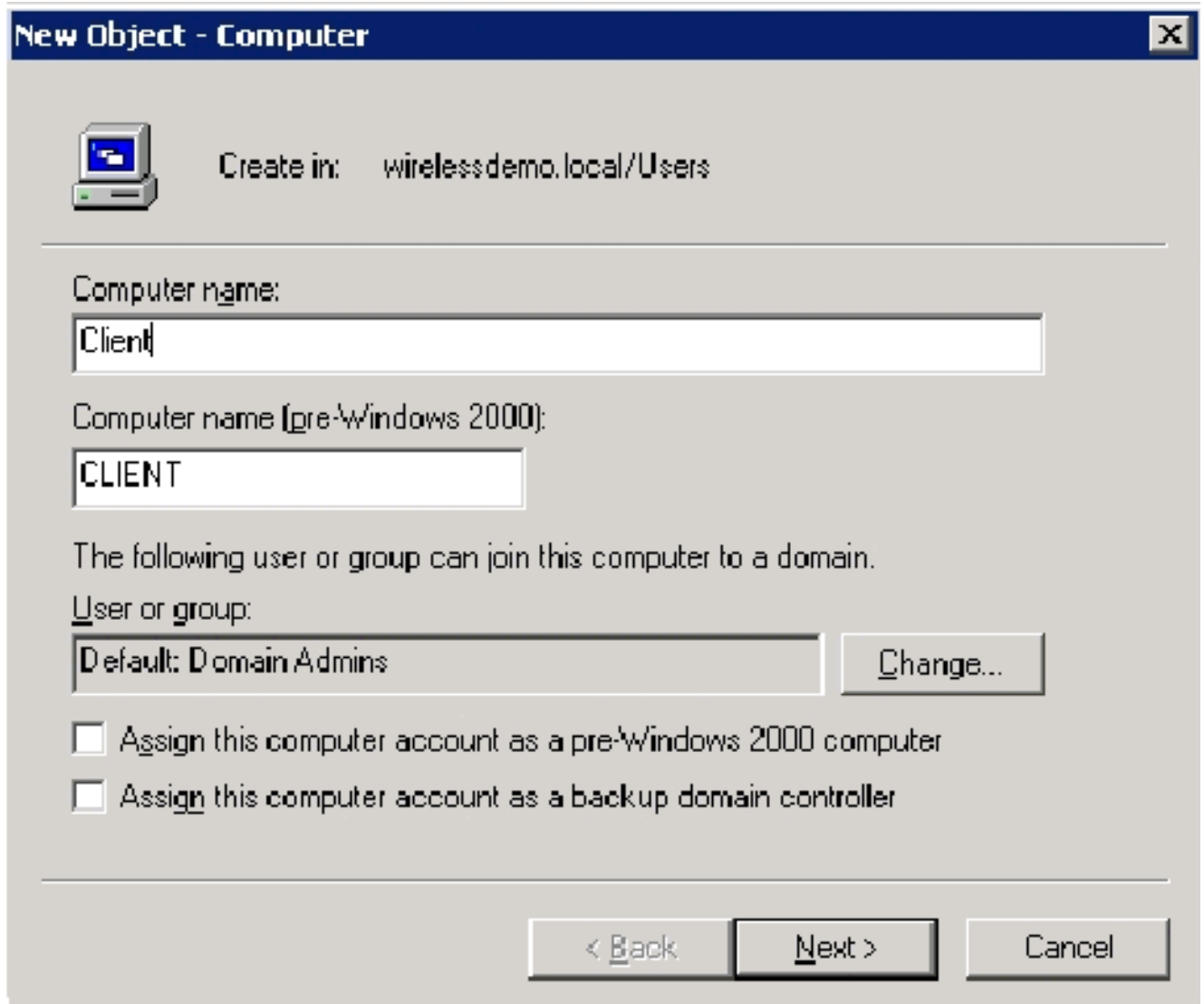
[Étape 7 : Ajouter des ordinateurs au domaine](#)

Procédez comme suit :

Remarque : si l'ordinateur est déjà ajouté au domaine, passez à [Ajouter des utilisateurs au domaine](#).

1. Ouvrez le composant logiciel enfichable Utilisateurs et ordinateurs Active Directory.
2. Dans l'arborescence de la console, développez **wirelessdemo.local**.
3. Cliquez avec le bouton droit sur **Utilisateurs**, cliquez sur **Nouveau**, puis sur **Ordinateur**.

4. Dans la boîte de dialogue Nouvel objet - Ordinateur, tapez le nom de l'ordinateur dans le champ Nom de l'ordinateur et cliquez sur **Suivant**. Cet exemple utilise le nom d'ordinateur **Client**.



5. Dans la boîte de dialogue Géré, cliquez sur **Suivant**.
6. Dans la boîte de dialogue Nouvel objet-ordinateur, cliquez sur **Terminer**.
7. Répétez les étapes 3 à 6 afin de créer des comptes d'ordinateur supplémentaires.

[Étape 8 : Autoriser l'accès sans fil aux ordinateurs](#)

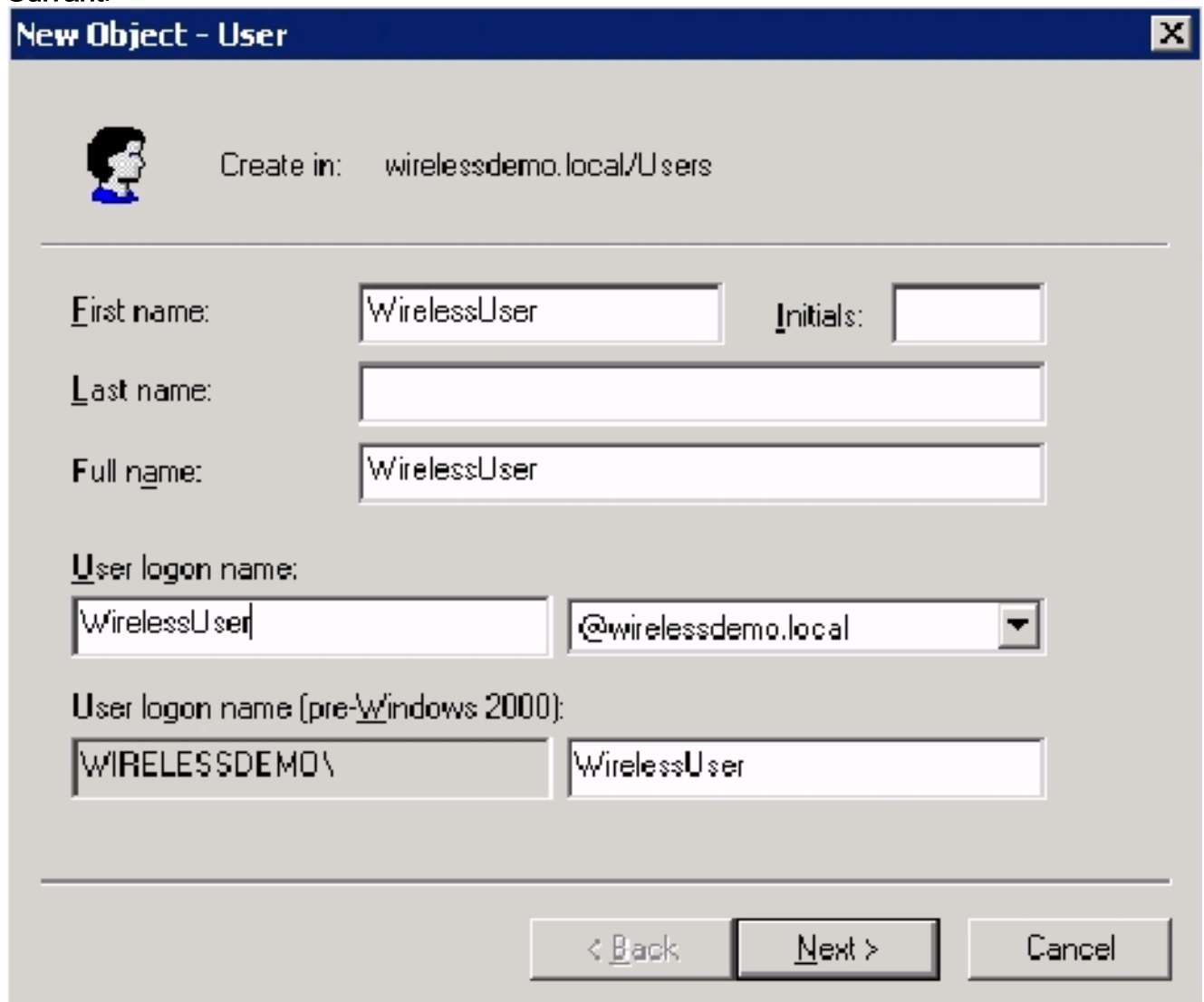
Procédez comme suit :

1. Dans l'arborescence de la console Utilisateurs et ordinateurs Active Directory, cliquez sur le dossier **Ordinateurs** et cliquez avec le bouton droit de la souris sur l'ordinateur pour lequel vous souhaitez attribuer un accès sans fil. Cet exemple montre la procédure avec l'ordinateur **CLIENT** que vous avez ajouté à l'étape 7.
2. Cliquez sur **Propriétés**, puis accédez à l'onglet Composer.
3. Sélectionnez **Autoriser l'accès** et cliquez sur **OK**.

[Étape 9 : Ajouter des utilisateurs au domaine](#)

Procédez comme suit :

1. Dans l'arborescence de la console Utilisateurs et ordinateurs Active Directory, cliquez avec le bouton droit sur **Utilisateurs**, cliquez sur **Nouveau**, puis sur **Utilisateur**.
2. Dans la boîte de dialogue Nouvel objet - Utilisateur, tapez **WirelessUser** dans le champ Prénom et tapez **WirelessUser** dans le champ Nom de connexion de l'utilisateur, puis cliquez sur **Suivant**.



New Object - User

Create in: wirelessdemo.local/Users

First name: Initials:

Last name:

Full name:

User logon name:

User logon name (pre-Windows 2000):

< Back Next > Cancel

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 **Next**.

New Object - User

Create in: wirelessdemo.local/Users

Password: [.....]

Confirm password: [.....]

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back Next > Cancel

4. Dans le nouvel objet - boîte de dialogue d'utilisateur, cliquez sur **Finish**.
5. Répétez les étapes 2 à 4 afin de créer des comptes d'utilisateur supplémentaires.

[Étape 10 : Permettez l'accès sans fil aux utilisateurs](#)

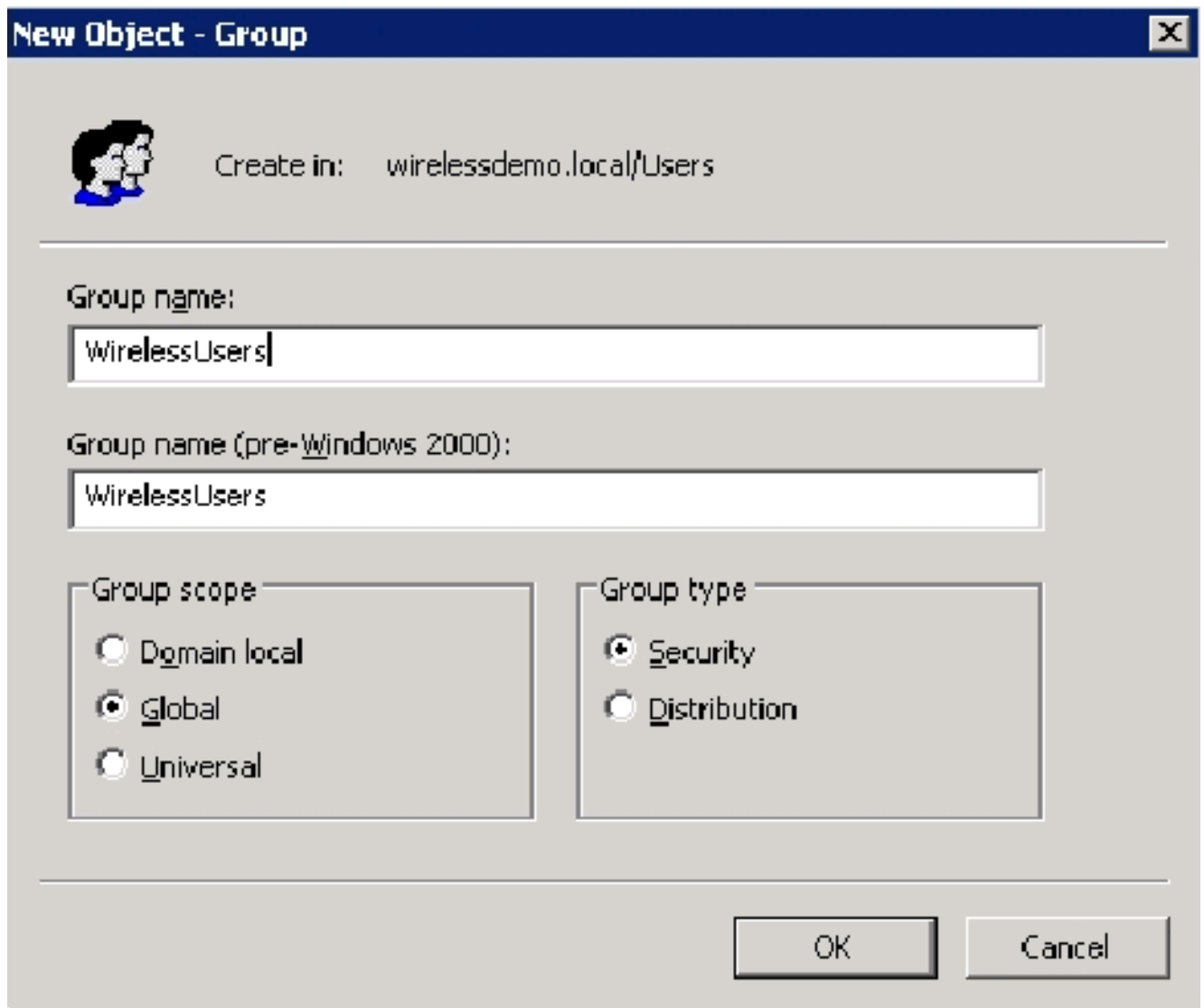
Procédez comme suit :

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 **Composer**.
2. Sélectionnez **Autoriser l'accès** et cliquez sur **OK**.

[Étape 11 : Ajouter des groupes au domaine](#)

Procédez comme suit :

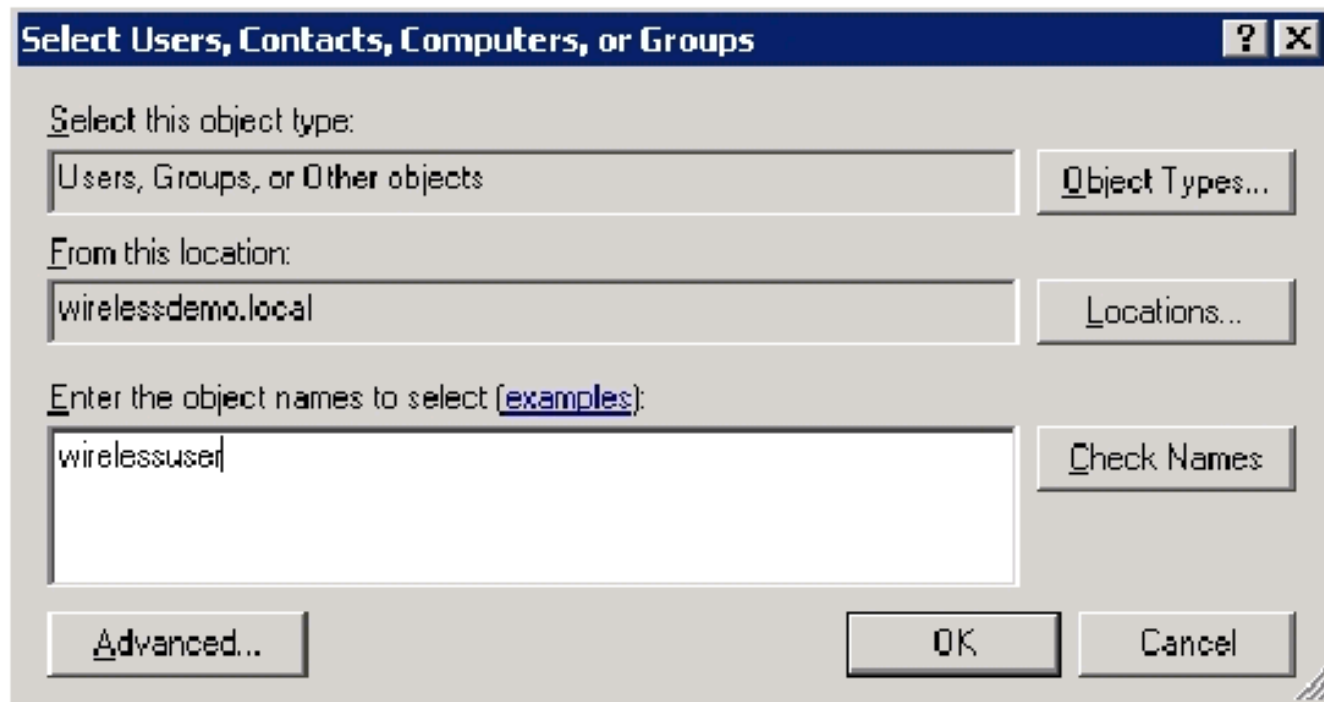
1. Dans l'arborescence de la console Utilisateurs et ordinateurs Active Directory, cliquez avec le bouton droit sur **Utilisateurs**, cliquez sur **Nouveau**, puis sur **Groupe**.
2. Dans la boîte de dialogue Nouveau objet - Groupe, tapez le nom du groupe dans le champ Nom du groupe et cliquez sur **OK**. Ce document utilise le nom de groupe **WirelessUsers**.



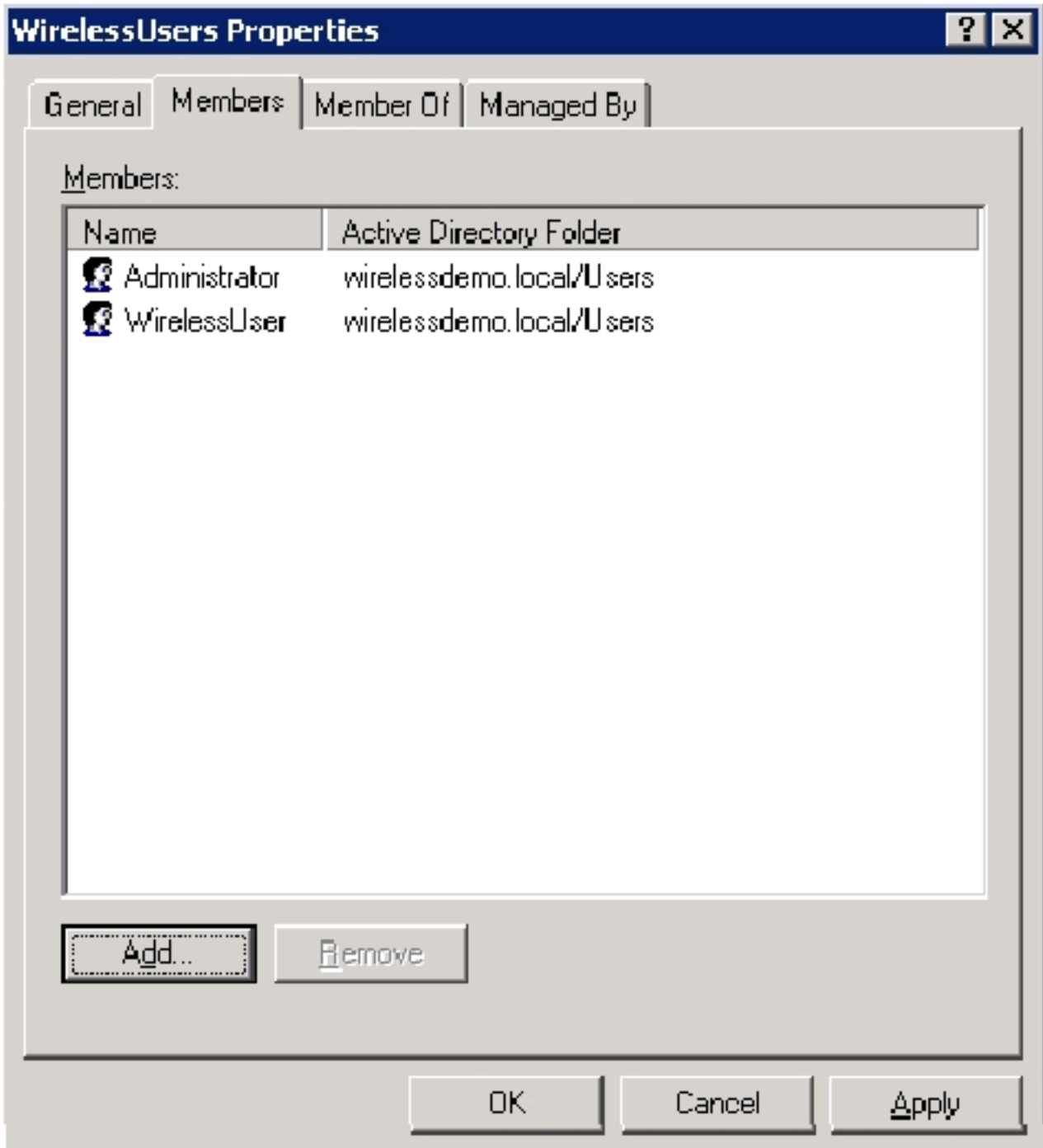
[Étape 12: Ajouter des utilisateurs au groupe WirelessUsers](#)

Procédez comme suit :

1. Dans le volet d'informations Utilisateurs et ordinateurs Active Directory, double-cliquez sur Group **WirelessUsers**.
2. Accédez à l'onglet Membres et cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Sélectionner des utilisateurs, des contacts, des ordinateurs ou des groupes, tapez le nom des utilisateurs à ajouter au groupe. Cet exemple montre comment ajouter l'utilisateur **sans fil** au groupe. Cliquez sur OK.



4. Dans la boîte de dialogue Noms multiples trouvés, cliquez sur **OK**. Le compte utilisateur WirelessUser est ajouté au groupe WirelessUsers.

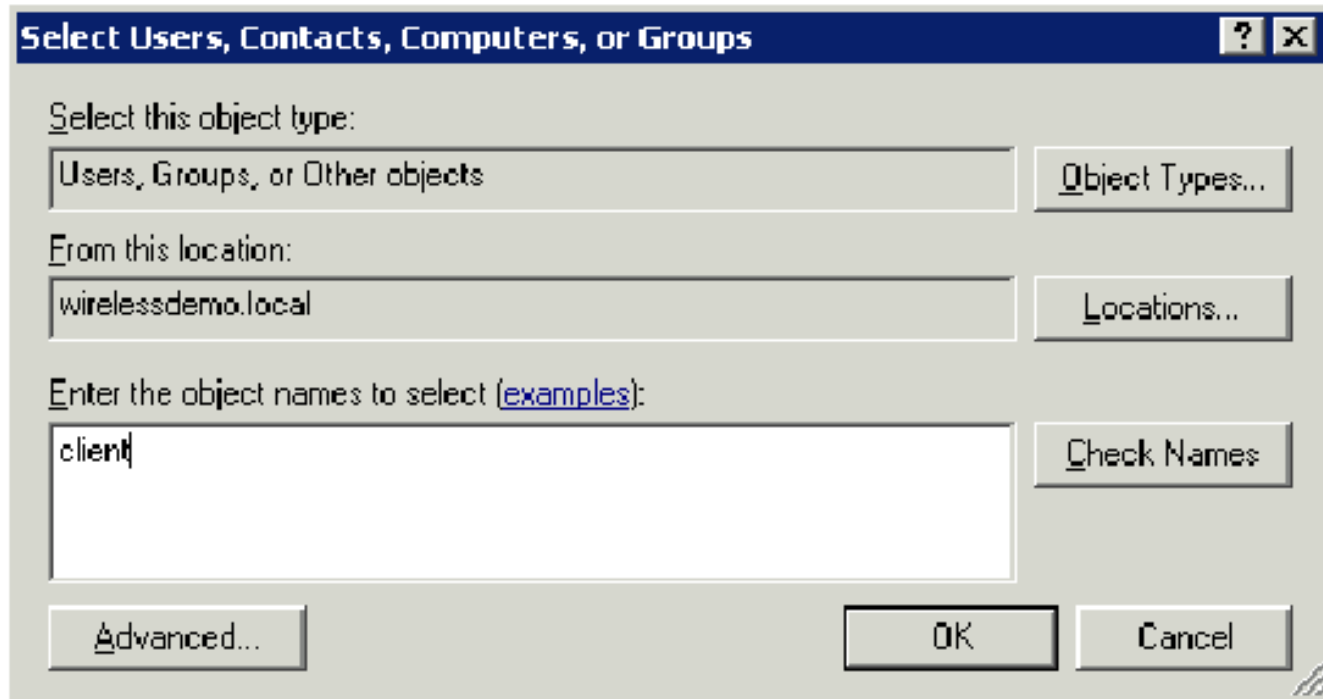


5. Cliquez sur **OK** afin d'enregistrer les modifications apportées au groupe WirelessUsers.
6. Répétez cette procédure pour ajouter d'autres utilisateurs au groupe.

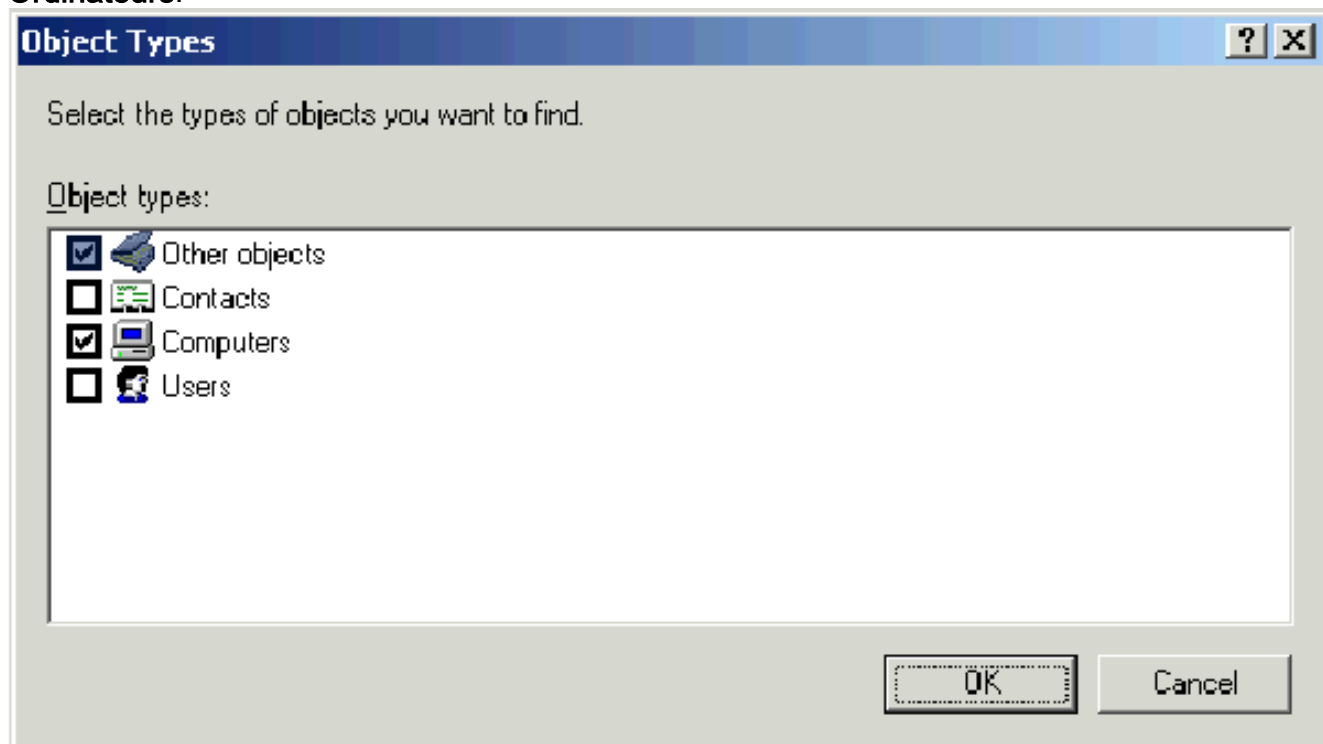
[Étape 13 : Ajouter des ordinateurs clients au groupe WirelessUsers](#)

Procédez comme suit :

1. Répétez les étapes 1 et 2 de la section [Ajouter des utilisateurs au groupe d'utilisateurs sans fil](#) de ce document
2. Dans la boîte de dialogue Sélectionner des utilisateurs, des contacts ou des ordinateurs, tapez le nom de l'ordinateur à ajouter au groupe. Cet exemple montre comment ajouter l'ordinateur nommé **client** au groupe.



3. Cliquez sur **Types d'objets**, désactivez la case à cocher **Utilisateurs**, puis activez **Ordinateurs**.



4. Cliquez deux fois sur **OK**. Le compte d'ordinateur CLIENT est ajouté au groupe WirelessUsers.
5. Répétez la procédure pour ajouter d'autres ordinateurs au groupe.

[Installation de Windows Standard 2003 avec Cisco Secure ACS 4.0](#)

Cisco Secure ACS est un ordinateur qui exécute Windows Server 2003 avec SP1, Standard Edition, qui fournit l'authentification et l'autorisation RADIUS pour le contrôleur. Complétez les procédures de cette section afin de configurer ACS en tant que serveur RADIUS :

Installation et configuration de base

Procédez comme suit :

1. Installez Windows Server 2003 avec SP1, Standard Edition, en tant que **serveur membre** nommé **ACS** dans le domaine **wirelessdemo.local**. **Remarque** : le nom du serveur ACS apparaît sous **cisco_w2003** dans les configurations restantes. Remplacez ACS ou **cisco_w2003** sur la configuration des travaux pratiques restante.
2. Pour la connexion locale, configurez le protocole TCP/IP avec l'adresse IP **172.16.100.26**, le masque de sous-réseau **255.255.255.0** et l'adresse IP du serveur DNS **127.0.0.1**.

Installation de Cisco Secure ACS 4.0

Remarque : reportez-vous au [Guide d'installation de Cisco Secure ACS 4.0 pour Windows](#) pour plus d'informations sur la configuration de Cisco Secure ACS 4.0 pour Windows.

Procédez comme suit :

1. À l'aide d'un compte Administrateur de domaine, connectez-vous à l'ordinateur ACS pour Cisco Secure ACS. **Remarque** : Seules les installations effectuées sur l'ordinateur sur lequel vous installez Cisco Secure ACS sont prises en charge. Les installations distantes effectuées à l'aide des services Terminal Server Windows ou de produits tels que Virtual Network Computing (VNC) ne sont pas testées et ne sont pas prises en charge.
2. Insérez le CD Cisco Secure ACS dans un lecteur de CD-ROM de l'ordinateur.
3. Si le lecteur de CD-ROM prend en charge la fonctionnalité d'exécution automatique de Windows, la boîte de dialogue Cisco Secure ACS pour Windows Server s'affiche. **Remarque** : si aucun Service Pack requis n'est installé sur l'ordinateur, une boîte de dialogue s'affiche. Les Service Packs Windows peuvent être appliqués avant ou après l'installation de Cisco Secure ACS. Vous pouvez poursuivre l'installation, mais le Service Pack requis doit être appliqué une fois l'installation terminée. Sinon, Cisco Secure ACS risque de ne pas fonctionner de manière fiable.
4. Effectuez l'une des tâches suivantes : Si la boîte de dialogue Cisco Secure ACS pour Windows Server apparaît, cliquez sur **Installer**. Si la boîte de dialogue Cisco Secure ACS pour Windows Server n'apparaît pas, exécutez **setup.exe**, situé dans le répertoire racine du CD Cisco Secure ACS.
5. La boîte de dialogue Configuration de Cisco Secure ACS affiche le contrat de licence logicielle.
6. Lisez le contrat de licence logicielle. Si vous acceptez le contrat de licence logicielle, cliquez sur **Accepter**. La boîte de dialogue Bienvenue affiche des informations de base sur le programme de configuration.
7. Après avoir lu les informations dans la boîte de dialogue Bienvenue, cliquez sur **Suivant**.
8. La boîte de dialogue Avant de commencer répertorie les éléments que vous devez terminer avant de poursuivre l'installation. Si vous avez terminé tous les éléments répertoriés dans la boîte de dialogue Avant de commencer, cochez la case correspondante pour chaque élément et cliquez sur **Suivant**. **Remarque** : si vous n'avez pas terminé tous les éléments répertoriés dans la zone Avant de commencer, cliquez sur **Annuler**, puis sur **Quitter le programme d'installation**. Après avoir terminé tous les éléments répertoriés dans la boîte de dialogue Avant de commencer, redémarrez l'installation.

9. La boîte de dialogue Choisir l'emplacement de destination s'affiche. Sous Dossier de destination, l'emplacement d'installation apparaît. Il s'agit du lecteur et du chemin d'accès sur lesquels le programme d'installation installe Cisco Secure ACS.
10. Pour modifier l'emplacement d'installation, procédez comme suit : Cliquez sur **Browse**. La boîte de dialogue Choisir un dossier s'affiche. La zone Chemin contient l'emplacement d'installation. Modifiez l'emplacement d'installation. Vous pouvez entrer le nouvel emplacement dans la zone Chemin ou utiliser les listes Lecteurs et répertoires pour sélectionner un nouveau lecteur et répertoire. L'emplacement d'installation doit se trouver sur un lecteur local de l'ordinateur. **Remarque** : ne spécifiez pas de chemin d'accès contenant un caractère de pourcentage, "%" . Si vous le faites, l'installation peut sembler se poursuivre correctement mais échoue avant de se terminer. Cliquez OK. **Remarque** : si vous avez spécifié un dossier qui n'existe pas, le programme d'installation affiche une boîte de dialogue pour confirmer la création du dossier. Afin de continuer, cliquez sur **Yes**.
11. Dans la boîte de dialogue Choisir l'emplacement de destination, le nouvel emplacement d'installation apparaît sous Dossier de destination.
12. Cliquez sur **Next** (Suivant).
13. La boîte de dialogue Configuration de la base de données d'authentification répertorie les options d'authentification des utilisateurs. Vous pouvez vous authentifier uniquement avec la base de données des utilisateurs Cisco Secure, ou également avec une base de données des utilisateurs Windows. **Remarque** : après avoir installé Cisco Secure ACS, vous pouvez configurer la prise en charge de l'authentification pour tous les types de base de données utilisateur externe en plus des bases de données utilisateur Windows.
14. Si vous voulez authentifier les utilisateurs avec la base de données des utilisateurs Cisco Secure uniquement, sélectionnez l'option **Vérifier la base de données Cisco Secure ACS uniquement**.
15. Si vous voulez authentifier des utilisateurs avec une base de données utilisateur Windows Security Access Manager (SAM) ou Active Directory en plus de la base de données utilisateur Cisco Secure, procédez comme suit : Sélectionnez l'option **Également vérifier la base de données des utilisateurs Windows**. La case à cocher **Oui, reportez-vous à la case à cocher Accorder l'autorisation de numérotation à l'utilisateur**. **Remarque** : La case à cocher **Oui, reportez-vous à la rubrique « Octroi d'une autorisation de numérotation à l'utilisateur »** s'applique à toutes les formes d'accès contrôlés par Cisco Secure ACS, et pas seulement à l'accès commuté. Par exemple, un utilisateur accédant au réseau via un tunnel VPN ne compose pas de numéro sur un serveur d'accès au réseau. Toutefois, si la case **Oui, reportez-vous à la case « Octroyer l'autorisation de numérotation à l'utilisateur »** est cochée, Cisco Secure ACS applique les autorisations de numérotation utilisateur Windows afin de déterminer si l'utilisateur doit accorder l'accès au réseau. Si vous souhaitez autoriser l'accès aux utilisateurs authentifiés par une base de données d'utilisateurs de domaine Windows uniquement lorsqu'ils disposent d'une autorisation de numérotation dans leur compte Windows, cochez la case **Oui, reportez-vous à la case de paramétrage « Accorder l'autorisation de numérotation à l'utilisateur »**.
16. Cliquez sur **Next** (Suivant).
17. Le programme d'installation installe Cisco Secure ACS et met à jour le Registre Windows.
18. La boîte de dialogue Options avancées répertorie plusieurs fonctionnalités de Cisco Secure ACS qui ne sont pas activées par défaut. Pour plus d'informations sur ces fonctionnalités, reportez-vous au [Guide de l'utilisateur de Cisco Secure ACS pour Windows Server, version 4.0](#). **Remarque** : Les fonctionnalités répertoriées apparaissent dans l'interface HTML de Cisco Secure ACS uniquement si vous les activez. Après l'installation, vous pouvez les

activer ou les désactiver sur la page Options avancées de la section Configuration de l'interface.

19. Pour chaque fonction à activer, cochez la case correspondante.
20. Cliquez sur **Next** (Suivant).
21. La boîte de dialogue Surveillance du service actif s'affiche.**Remarque** : après l'installation, vous pouvez configurer les fonctions de surveillance active du service sur la page Gestion active du service dans la section Configuration du système.
22. Si vous souhaitez que Cisco Secure ACS surveille les services d'authentification des utilisateurs, cochez la case **Activer la surveillance de connexion**. Dans la liste Script à exécuter, sélectionnez l'option à appliquer en cas d'échec du service d'authentification :**Aucune action corrective** : Cisco Secure ACS n'exécute pas de script.**Remarque** : cette option est utile si vous activez les notifications par courrier d'événement.**Reboot** - Cisco Secure ACS exécute un script qui redémarre l'ordinateur qui exécute Cisco Secure ACS.**Redémarrer tout** - Cisco Secure ACS redémarre tous les services Cisco Secure ACS.**Restart RADIUS/TACACS+**—Cisco Secure ACS redémarre uniquement les services RADIUS et TACACS+.
23. Si vous souhaitez que Cisco Secure ACS envoie un message électronique lorsque le contrôle des services détecte un événement, cochez la case **Notification par courrier**.
24. Cliquez sur **Next** (Suivant).
25. La boîte de dialogue Mot de passe de chiffrement de base de données s'affiche.**Remarque** : Le mot de passe de chiffrement de base de données est chiffré et stocké dans le Registre ACS. Vous devrez peut-être réutiliser ce mot de passe lorsque des problèmes critiques surviennent et que la base de données doit être accessible manuellement. Gardez ce mot de passe à portée de main pour que le support technique puisse accéder à la base de données. Le mot de passe peut être modifié chaque période d'expiration.
26. Entrez un mot de passe pour le chiffrement de la base de données. Le mot de passe doit comporter au moins huit caractères et doit contenir à la fois des caractères et des chiffres. Il n'y a pas de caractères non valides. Cliquez sur **Next** (Suivant).
27. Le programme d'installation se termine et la boîte de dialogue Cisco Secure ACS Service Initiation s'affiche.
28. Pour chaque option Cisco Secure ACS Services Initiation souhaitée, cochez la case correspondante. Les actions associées aux options se produisent une fois le programme d'installation terminé.**Oui, je veux démarrer le service Cisco Secure ACS maintenant** : démarre les services Windows qui composent Cisco Secure ACS. Si vous ne sélectionnez pas cette option, l'interface HTML de Cisco Secure ACS n'est pas disponible, sauf si vous redémarrez l'ordinateur ou démarrez le service CSAdmin.**Oui, je veux que le programme d'installation lance Cisco Secure ACS Administrator à partir de mon navigateur après l'installation** : ouvre l'interface HTML de Cisco Secure ACS dans le navigateur Web par défaut pour le compte d'utilisateur Windows actuel.**Oui, je veux afficher le fichier Lisez-moi** : ouvre le fichier README.TXT dans le Bloc-notes Windows.
29. Cliquez sur **Next** (Suivant).
30. Si vous avez sélectionné une option, les services Cisco Secure ACS démarrent. La boîte de dialogue Setup Complete (Configuration terminée) affiche des informations sur l'interface HTML de Cisco Secure ACS.
31. **Cliquez sur Finish**.**Remarque** : Le reste de la configuration est documenté dans la section pour le type EAP configuré.

Configuration du contrôleur LWAPP Cisco

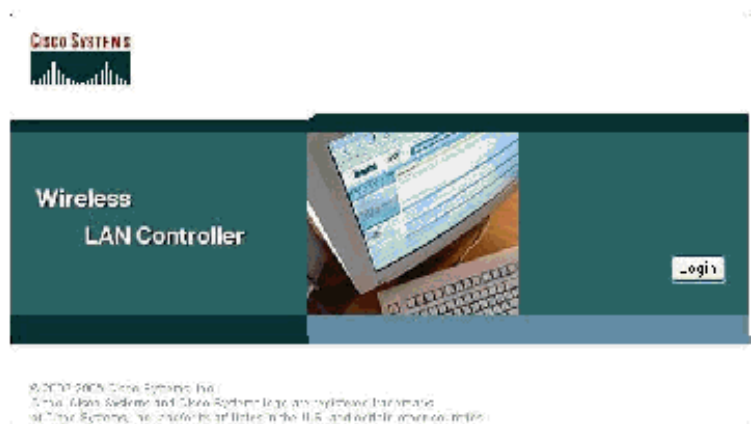
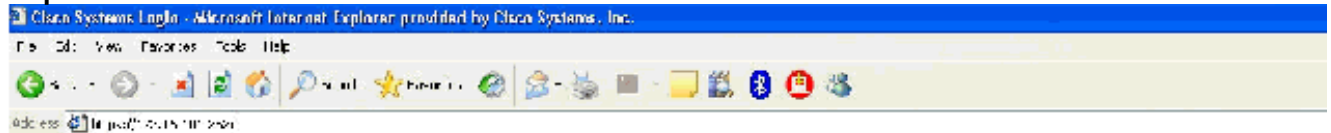
Créer la configuration requise pour WPA2/WPA

Procédez comme suit :

Remarque : l'hypothèse est que le contrôleur a une connectivité de base au réseau et que l'accessibilité IP à l'interface de gestion est réussie.

1. Connectez-vous au contrôleur en accédant à

https://172.16.101.252.



2. Cliquez sur **Connexion**.
3. Connectez-vous avec l'utilisateur par défaut **admin** et le mot de passe par défaut **admin**.
4. Créez le mappage VLAN d'interface dans le menu Controller.
5. Cliquez sur **Interfaces**.
6. Cliquez sur **New**.
7. Dans le champ Nom de l'interface, tapez **Employé**. (Ce champ peut être n'importe quelle valeur que vous souhaitez.)
8. Dans le champ VLAN ID, tapez **20**. (Ce champ peut être n'importe quel VLAN transporté sur le réseau.)
9. Cliquez sur Apply.
10. Configurez les informations comme le montre la fenêtre Interfaces > Edit.

Back Search Favorites

Address: https://172.16.101.252/screens/frameset.html

CISCO SYSTEMS

MONITOR WLANs CONTROLLER WIRELESS SECURITY

Controller

General

Inventory

Interfaces

Internal DHCP Server

Mobility Management
Mobility Groups
Mobility Statistics

Ports

Master Controller Mode

Network Time Protocol

QoS Profiles

Interfaces > Edit

General Information

Interface Name employee

Interface Address

VLAN Identifier 20

IP Address 172.16.100.1

Netmask 255.255.255.0

Gateway 172.16.100.1

Physical Information

Port Number 1

DHCP Information

Primary DHCP Server 172.16.100.25

Secondary DHCP Server 0.0.0.0

Access Control List

ACL Name none

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

11. Cliquez sur Apply.
12. Cliquez sur **WLAN**.
13. Cliquez sur **New**.
14. Dans le champ WLAN SSID, saisissez **Employee**.
15. Cliquez sur Apply.
16. Configurez les informations comme indiqué dans la fenêtre WLANs > Edit. **Remarque :** WPA2 est la méthode de chiffrement de couche 2 choisie pour ces travaux pratiques. Afin de permettre aux clients WPA avec TKIP-MIC de s'associer à ce SSID, vous pouvez également cocher les cases **Mode de compatibilité WPA** et **Autoriser les clients TKIP WPA2** ou les clients qui ne prennent pas en charge la méthode de cryptage AES 802.11i.

WLAN6 > Edit

WLAN ID	1
WLAN SSID	Employee

General Policies

Radius Policy	All
Admin Status	<input checked="" type="checkbox"/> Enabled
Session Timeout (secs)	1800
Quality of Services (QoS)	Silver (best effort)
WMM Policy	Disabled
7920 Pkts Support	<input type="checkbox"/> Client CAC Limit <input type="checkbox"/> AP CAC Limit
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
Allow PPP Override	<input type="checkbox"/> Enabled
Client Exclusion	<input checked="" type="checkbox"/> Enabled ** 60 Timeout Value (secs)
DHCP Server	<input type="checkbox"/> Override
DHCP Addr. Assignment	<input checked="" type="checkbox"/> Required
Interface Name	employee

Security Policies

Layer 2 Security	WPA2
	<input type="checkbox"/> MAC Filtering
Layer 3 Security	None
	<input type="checkbox"/> Web Policy **

* Web Policy cannot be used in combination with IPsec and L2TP.

** When client exclusion is enabled, a timeout value of zero means infinity (will require administrative override to reset excluded clients)

Radius Servers

	Authentication Servers	Accounting Servers
Server 1	IP:172.16.100.25, Port:1812	none
Server 2	none	none
Server 3	none	none

WPA2 Parameters

WPA Compatibility Mode	<input checked="" type="checkbox"/> Enable
Allow WPA2 TKIP Clients	<input checked="" type="checkbox"/> Enable
Pre-Shared Key	<input type="checkbox"/> Enabled (WPA2 passphrase has been set)

17. Cliquez sur Apply.
18. Cliquez sur le menu **Sécurité** et ajoutez le serveur RADIUS.
19. Cliquez sur **New**.
20. Ajoutez l'adresse IP du serveur RADIUS (172.16.100.25), qui est le serveur ACS configuré précédemment.
21. Assurez-vous que la clé partagée correspond au client AAA configuré dans le serveur ACS.
22. Cliquez sur Apply.



Security

AAA

- General
- RADIUS Authentication
- RADIUS Accounting
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies

Access Control Lists

Web Auth Certificate

Wireless Protection Policies

- Trusted AP Policies
- Rogue Policies
- Standard Signatures
- Custom Signatures
- Client Exclusion Policies
- AP Authentication

RADIUS Authentication Servers > New

Server Index (Priority)

Server IP Address

Keys Format

Shared Secret

Confirm Shared Secret

Key Wrap

Port Number

Server Status

Support for RFC 3576

Retransmit Timeout seconds

Network User Enable

Management Enable

23. La configuration de base est maintenant terminée et vous pouvez commencer à tester l'EAP-TLS.

[Authentification EAP-TLS](#)

L'authentification EAP-TLS nécessite des certificats d'ordinateur et d'utilisateur sur le client sans fil, l'ajout d'EAP-TLS en tant que type EAP à la stratégie d'accès à distance pour l'accès sans fil et une reconfiguration de la connexion réseau sans fil.

Afin de configurer DC_CA pour fournir l'inscription automatique des certificats d'ordinateur et d'utilisateur, complétez les procédures de cette section.

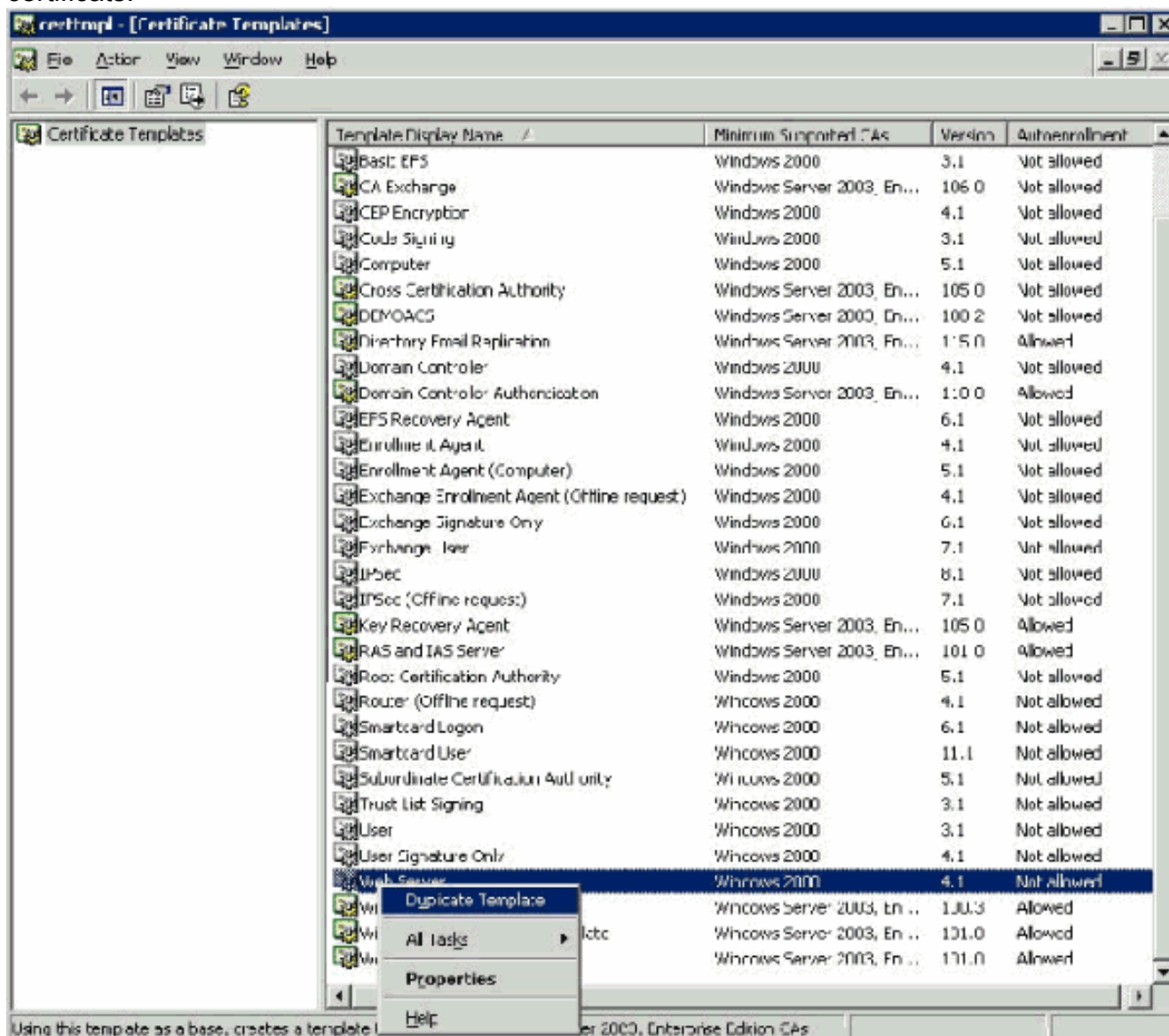
Remarque : Microsoft a modifié le modèle Web Server avec la version de Windows 2003 Enterprise CA afin que les clés ne soient plus exportables et que l'option soit grisée. Aucun autre modèle de certificat fourni avec les services de certificat n'est destiné à l'authentification du serveur et permet de marquer les clés comme exportables disponibles dans la liste déroulante. Vous devez donc créer un nouveau modèle pour cela.

Remarque : Windows 2000 autorise les clés exportables et ces procédures ne doivent pas être suivies si vous utilisez Windows 2000.

[Installer le composant logiciel enfichable Modèles de certificat](#)

Procédez comme suit :

1. Choisissez **Démarrer > Exécuter**, tapez **mmc**, puis cliquez sur **OK**.
2. Dans le menu Fichier, cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**, puis sur **Ajouter**.
3. Sous Composant logiciel enfichable, double-cliquez sur **Modèles de certificat**, cliquez sur **Fermer**, puis sur **OK**.
4. Dans l'arborescence de la console, cliquez sur **Modèles de certificats**. Tous les modèles de certificat apparaissent dans le volet Détails.
5. Afin de contourner les étapes 2 à 4, tapez **certtmpl.msc** qui ouvre le composant logiciel enfichable Modèles de certificats.



[Créer le modèle de certificat pour le serveur Web ACS](#)

Procédez comme suit :

1. Dans le volet Détails du composant logiciel enfichable Modèles de certificats, cliquez sur le modèle **serveur Web**.
2. Dans le menu Action, cliquez sur **Modèle en**

Properties of New Template [?] [X]

Issuance Requirements | Superseded Templates | Extensions | Security

General | Request Handling | Subject Name

Template display name:
Copy of Web Server

Minimum Supported CAs: Windows Server 2003, Enterprise Edition

After you apply changes to this tab, you can no longer change the template name.

Template name:
Copy of Web Server

Validity period: 2 years
Renewal period: 6 weeks

Publish certificate in Active Directory
 Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply

double.

3. Dans le champ Nom d'affichage du modèle, tapez

Properties of New Template [?] [X]

Issuance Requirements | Superseded Templates | Extensions | Security

General | **Request Handling** | Subject Name

Template display name:
[ACS]

Minimum Supported CAs: Windows Server 2003, Enterprise Edition

After you apply changes to this tab, you can no longer change the template name.

Template name:
[ACS]

Validity period: [2] years [▼] Renewal period: [6] weeks [▼]

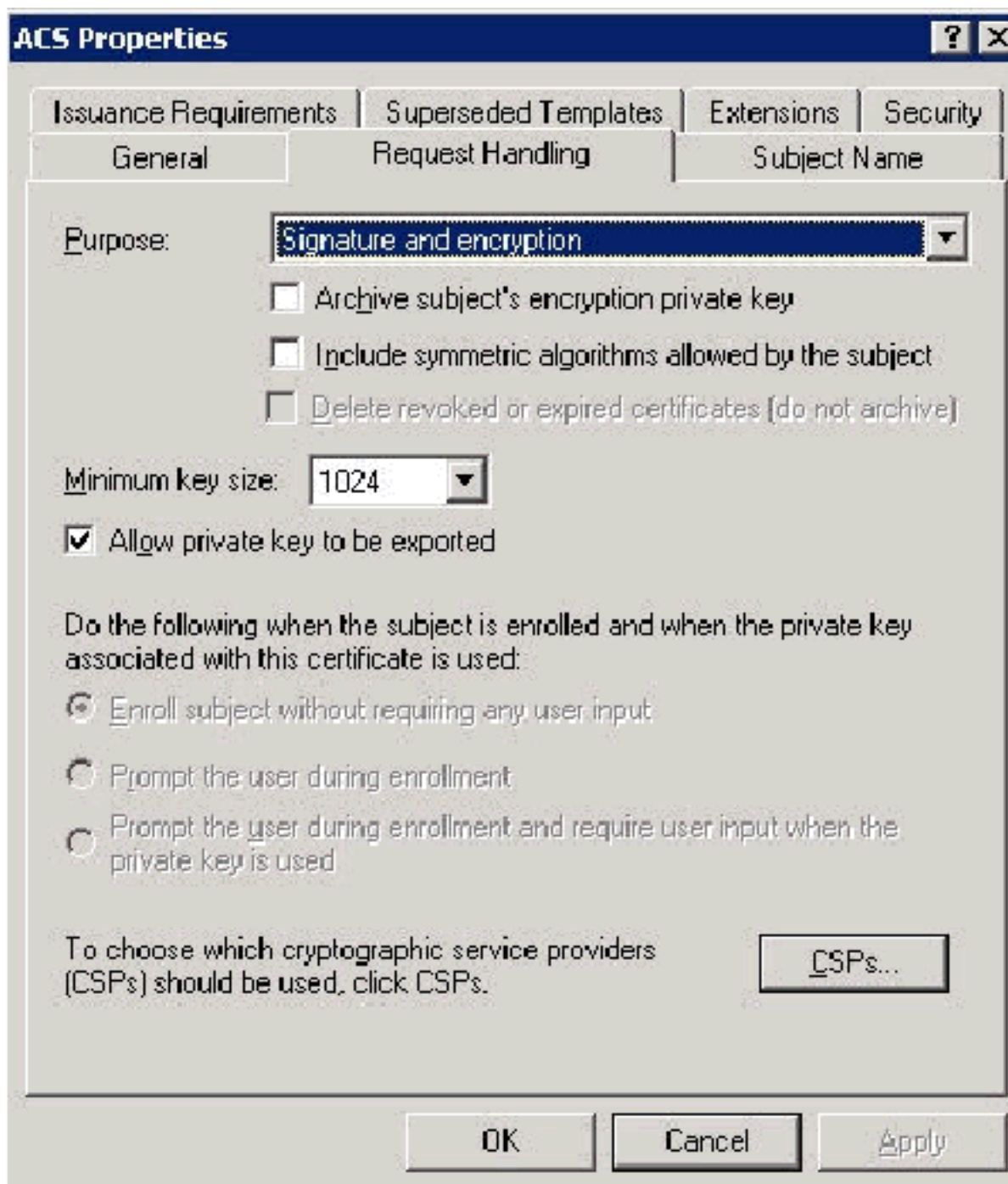
Publish certificate in Active Directory

Do not automatically reenroll if a duplicate certificate exists in Active Directory

[OK] [Cancel] [Apply]

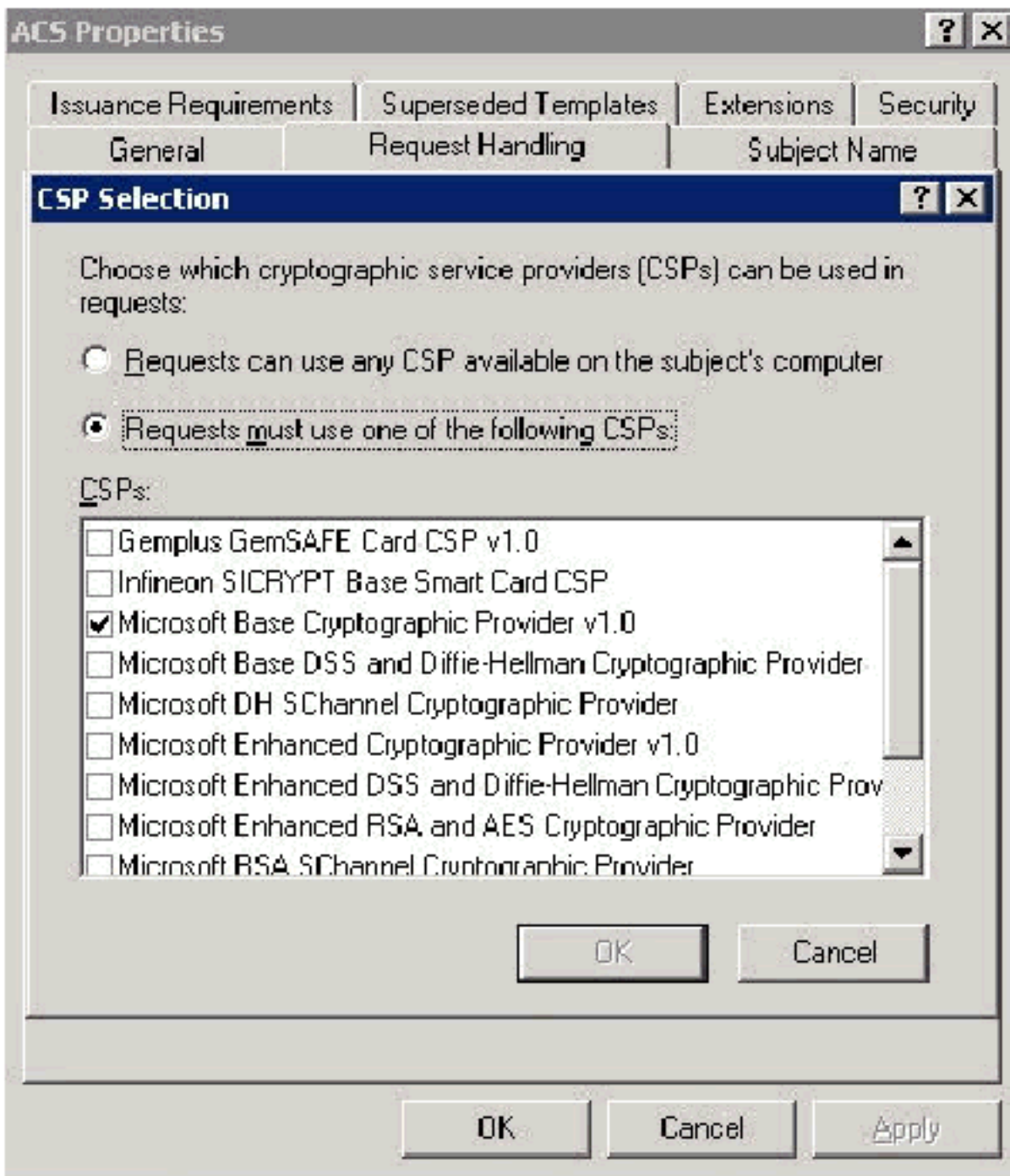
ACS.

4. Accédez à l'onglet Gestion des demandes et cochez la case **Autoriser l'exportation de la clé**



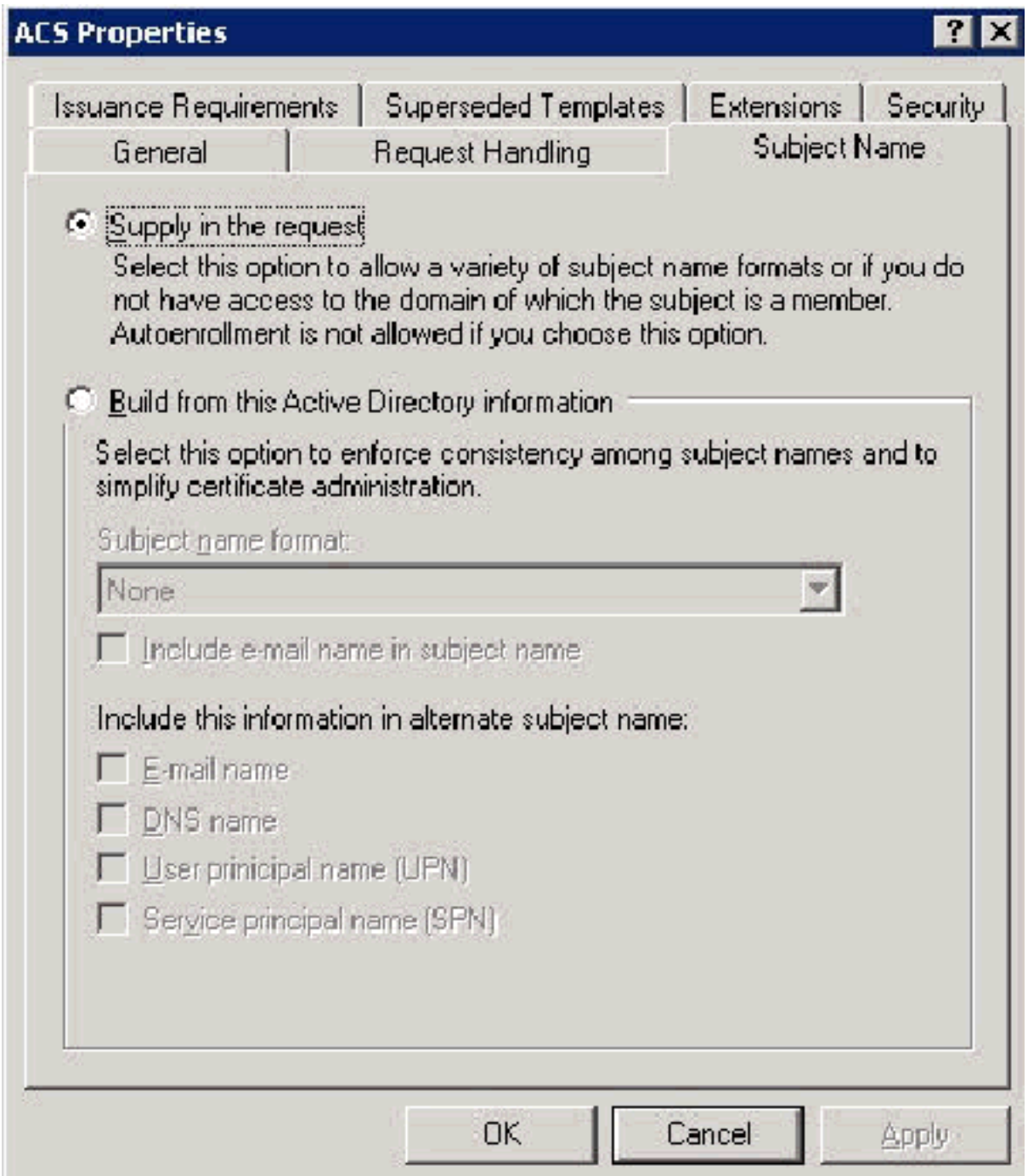
privée.

5. Choisissez Demandes doit utiliser l'un des CSP suivants et cochez Fournisseur de chiffrement Microsoft Base v1.0. Désélectionnez les autres fournisseurs de services de contact cochés, puis cliquez sur



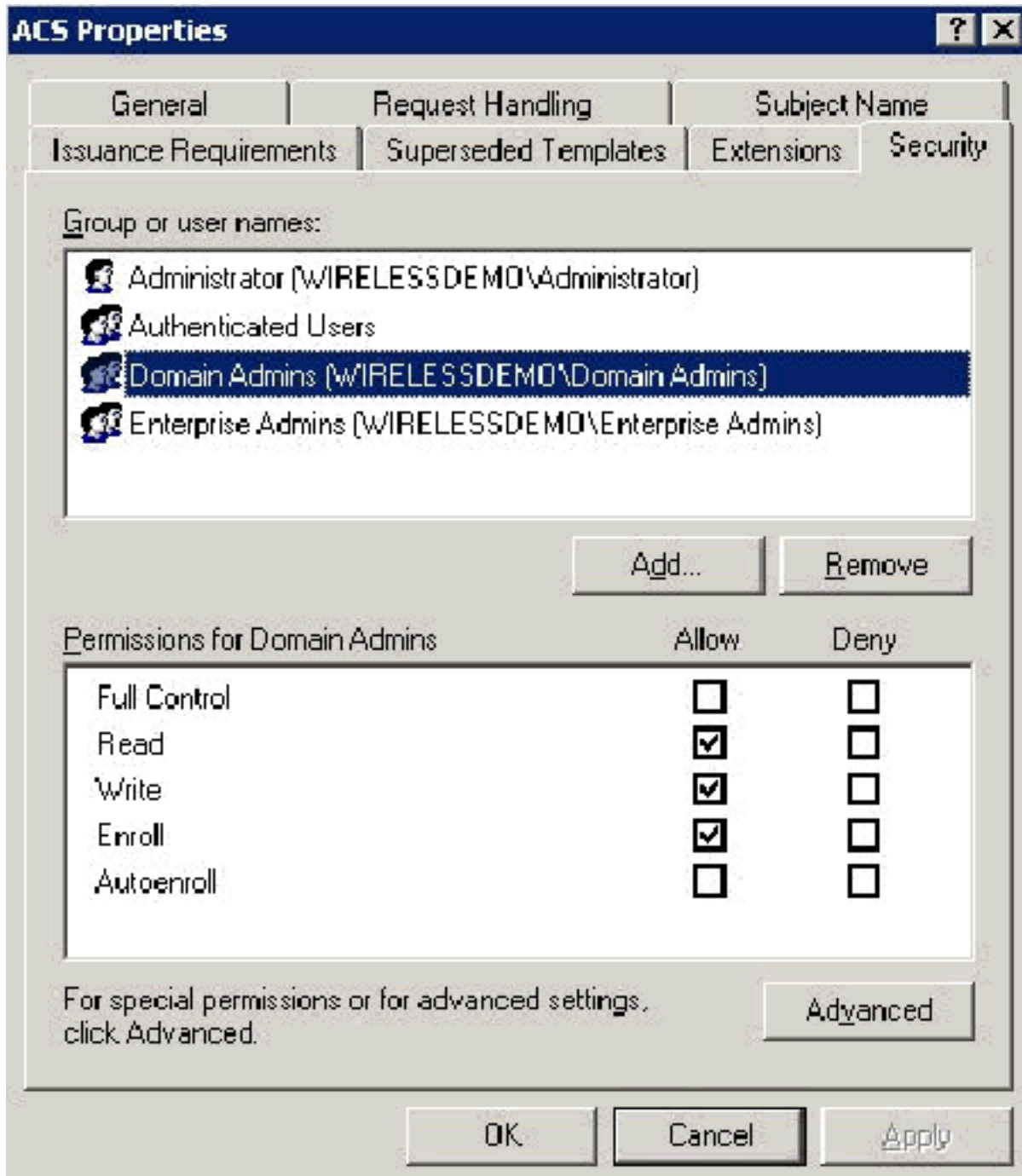
OK.

6. Accédez à l'onglet Nom du sujet, choisissez **Approvisionnement dans la demande** et cliquez

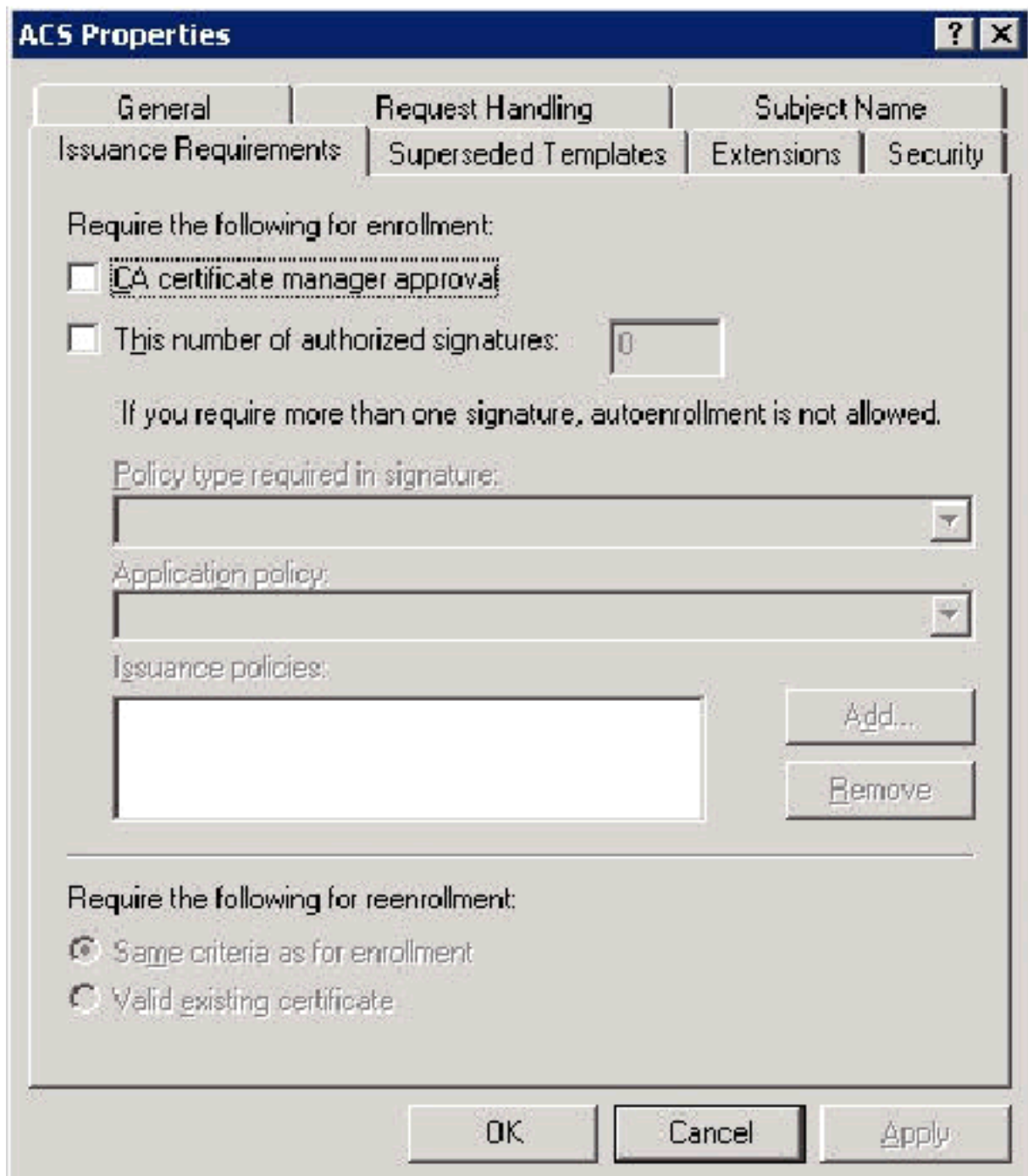


sur OK.

7. Accédez à l'onglet Sécurité, mettez en surbrillance le **groupe d'administrateurs de domaine** et assurez-vous que l'option **Inscription** est cochée sous Autorisé. **Important** : Si vous choisissez de créer à partir de ces informations Active Directory uniquement, cochez la case **Nom principal de l'utilisateur (UPN)** et décochez la case **Inclure le nom du courrier électronique** dans le nom du sujet et le nom du courrier électronique, car aucun nom de courrier électronique n'a été entré pour le compte d'utilisateur sans fil dans le composant logiciel enfichable Utilisateurs et ordinateurs Active Directory. Si vous ne désactivez pas ces deux options, l'inscription automatique tente d'utiliser le courrier électronique, ce qui entraîne une erreur d'inscription automatique.



8. Des mesures de sécurité supplémentaires sont nécessaires pour empêcher que les certificats ne soient automatiquement exclus. Vous pouvez les trouver dans l'onglet Conditions d'émission. Cette question n'est pas abordée plus en détail dans le présent document.

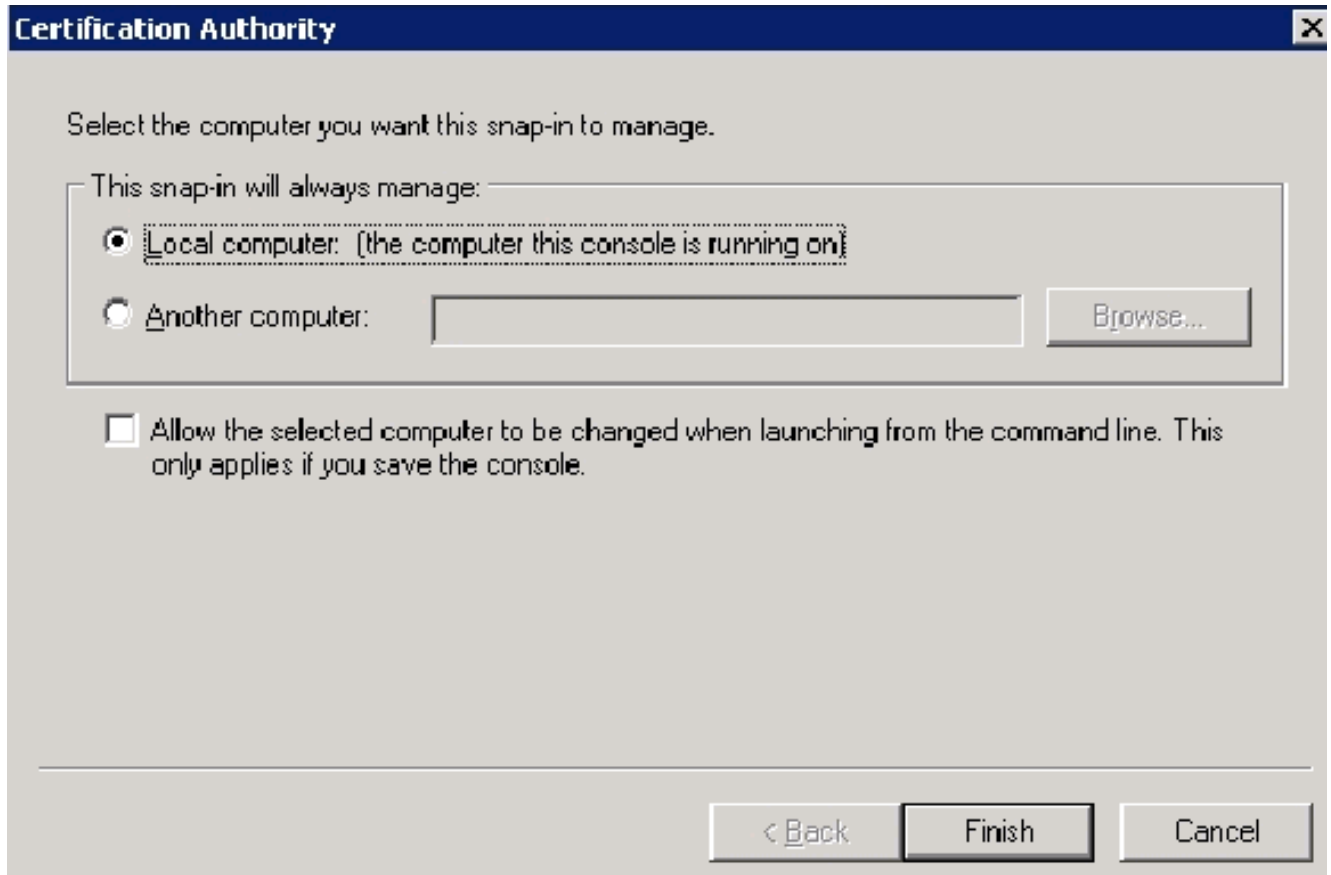


9. Cliquez sur **OK** pour enregistrer le modèle et passer à l'émission de ce modèle à partir du composant logiciel enfichable Autorité de certification.

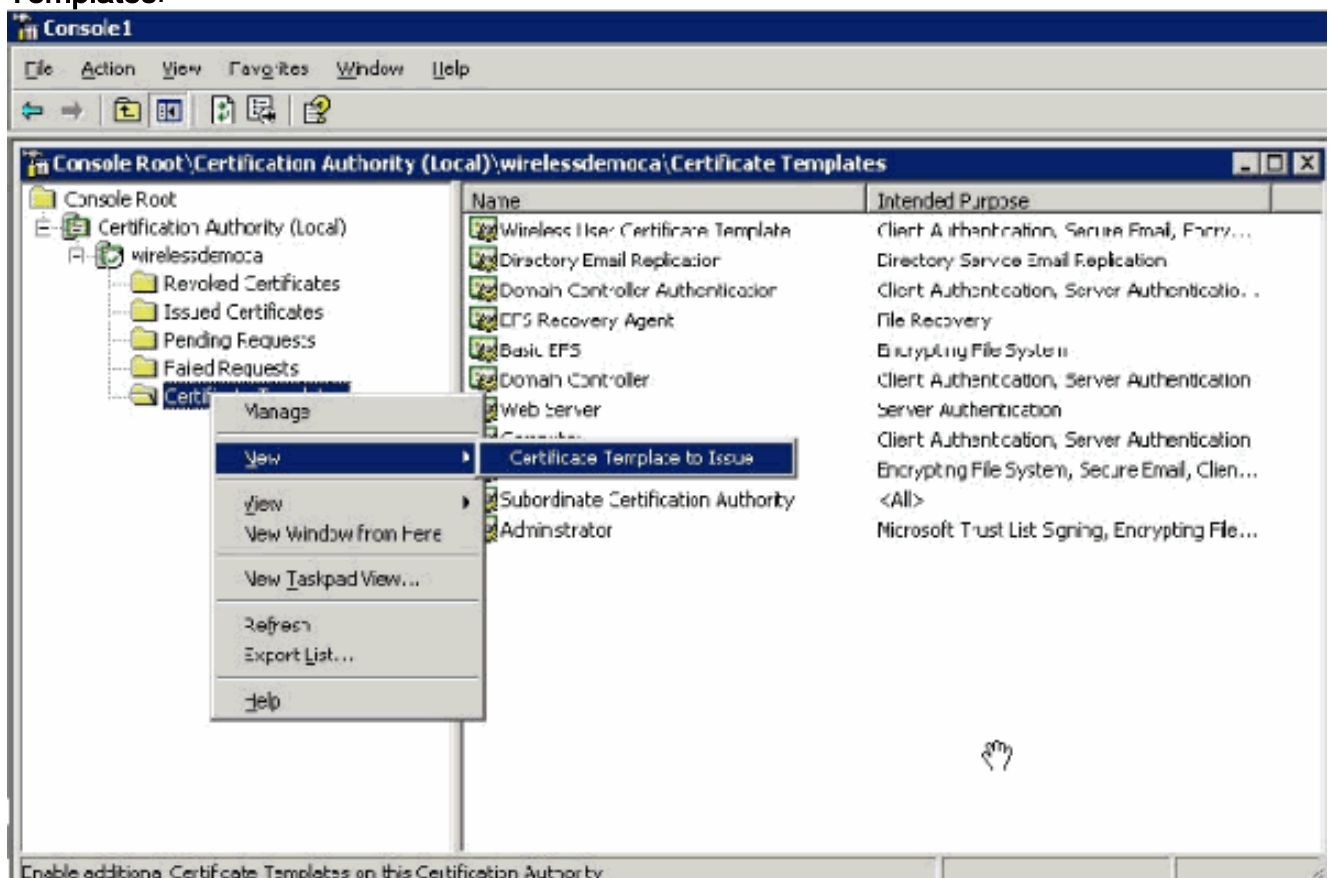
[Activer le nouveau modèle de certificat de serveur Web ACS](#)

Procédez comme suit :

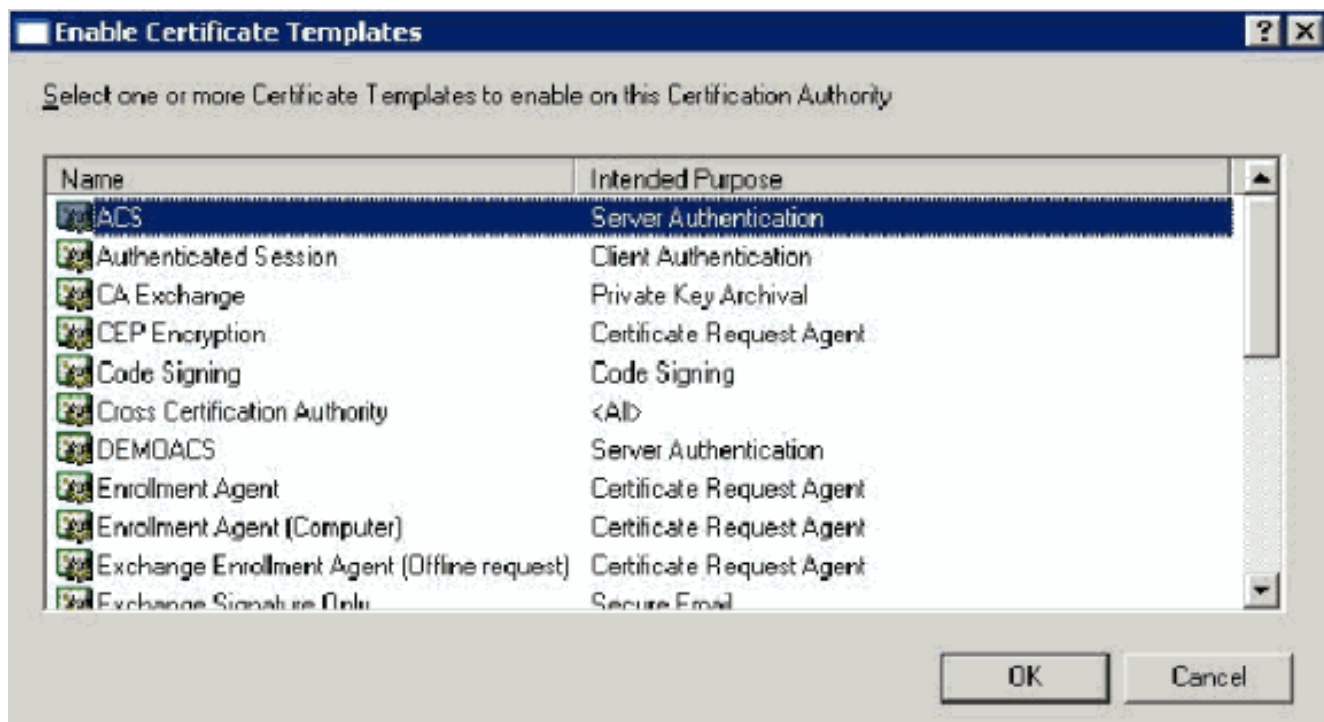
1. Ouvrez le composant logiciel enfichable **Autorité de certification**. Suivez les étapes 1 à 3 de la section [Créer le modèle de certificat pour le serveur Web ACS](#), choisissez l'option **Autorité de certification**, choisissez **Ordinateur local** et cliquez sur **Terminer**.



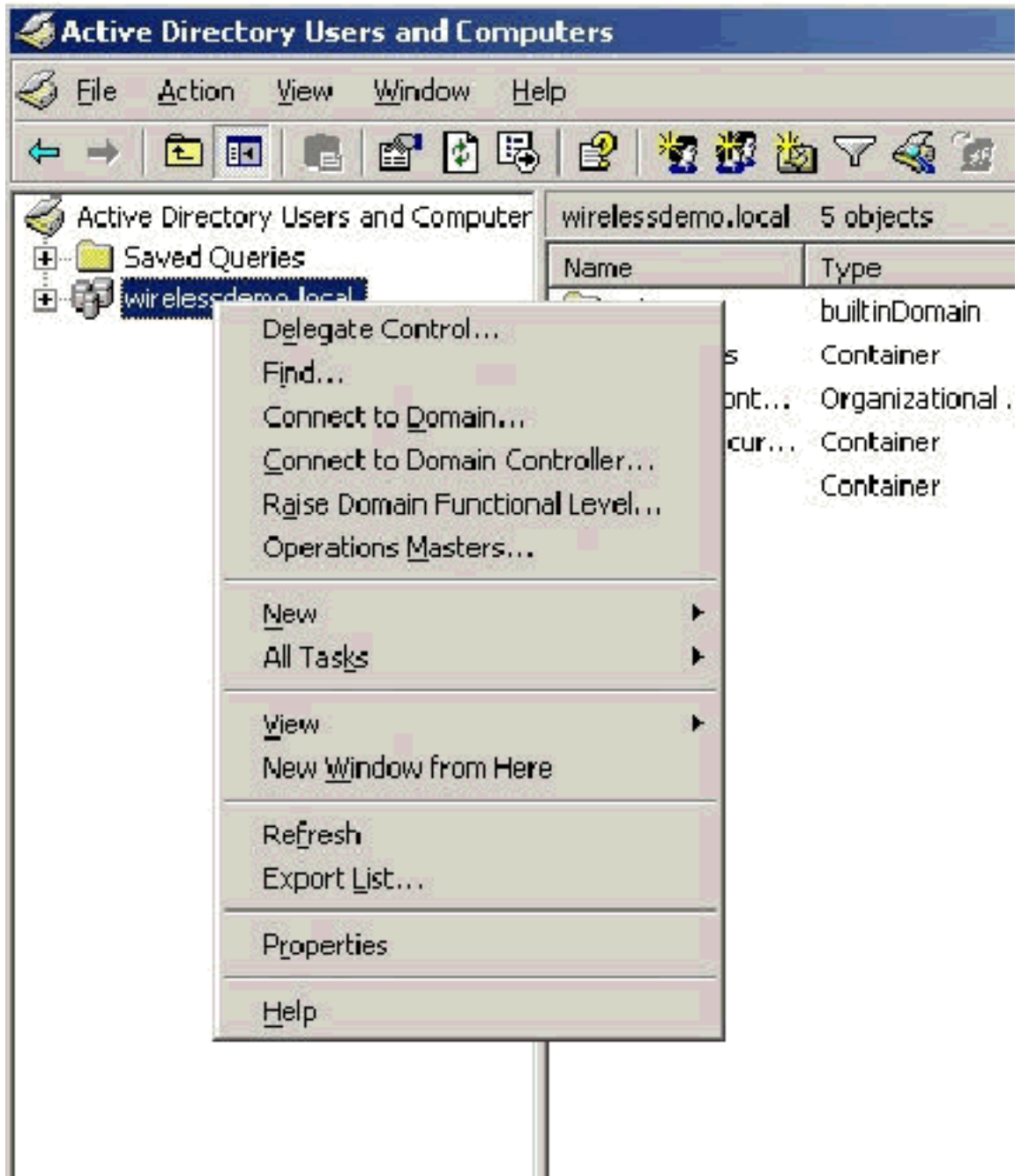
2. Dans l'arborescence de la console, développez **Wireless**, puis cliquez avec le bouton droit de la souris sur **Certificate Templates**.



3. Choisissez **Nouveau > Modèle de certificat à émettre**.
4. Cliquez sur le modèle de certificat **ACS**.

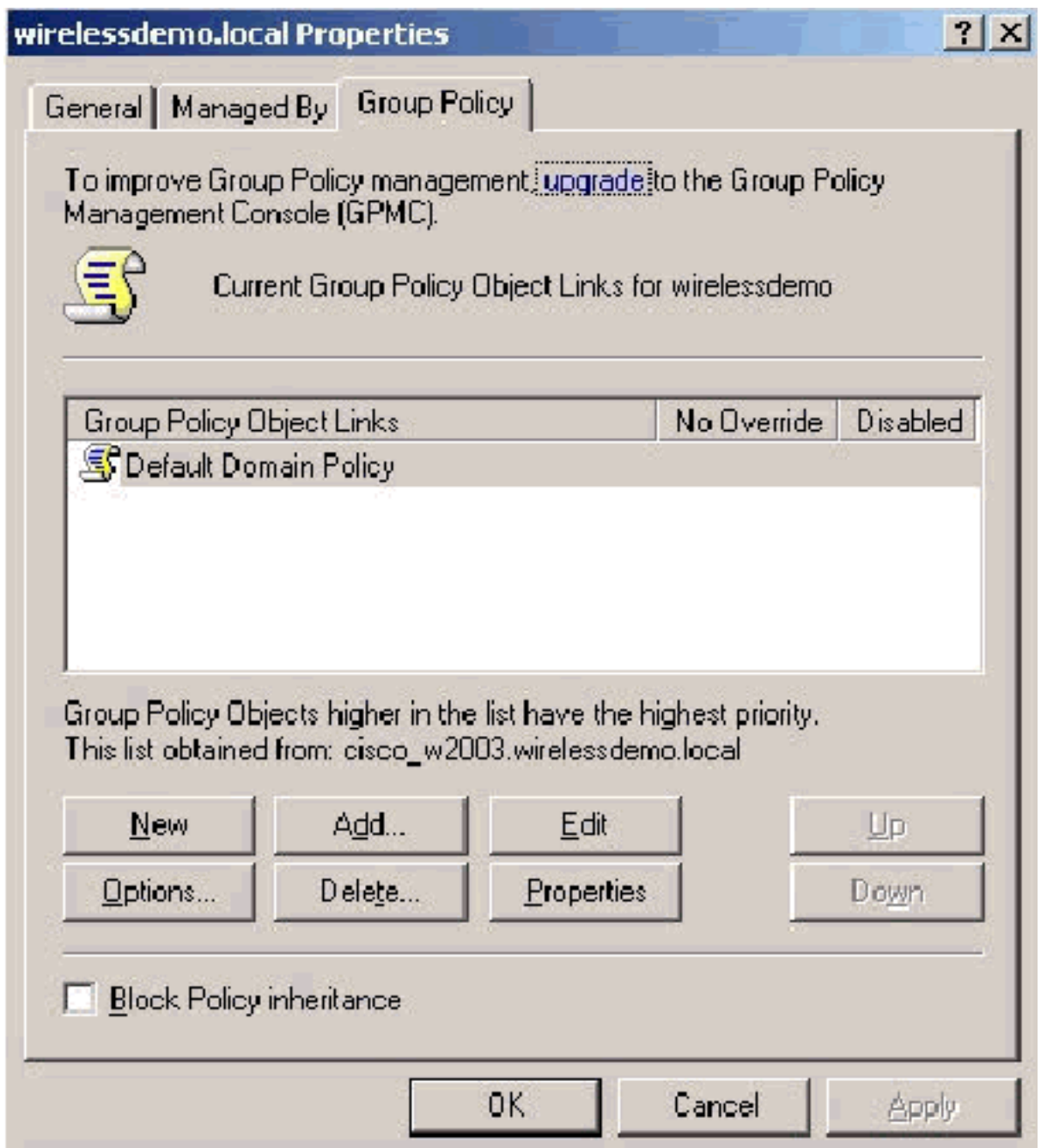


5. Cliquez sur **OK** et ouvrez le **composant logiciel enfilable Utilisateurs et ordinateurs Active Directory**.
6. Dans l'arborescence de la console, double-cliquez sur **Utilisateurs et ordinateurs Active Directory**, cliquez avec le bouton droit sur le **domaine wirelessdemo.local**, puis cliquez sur



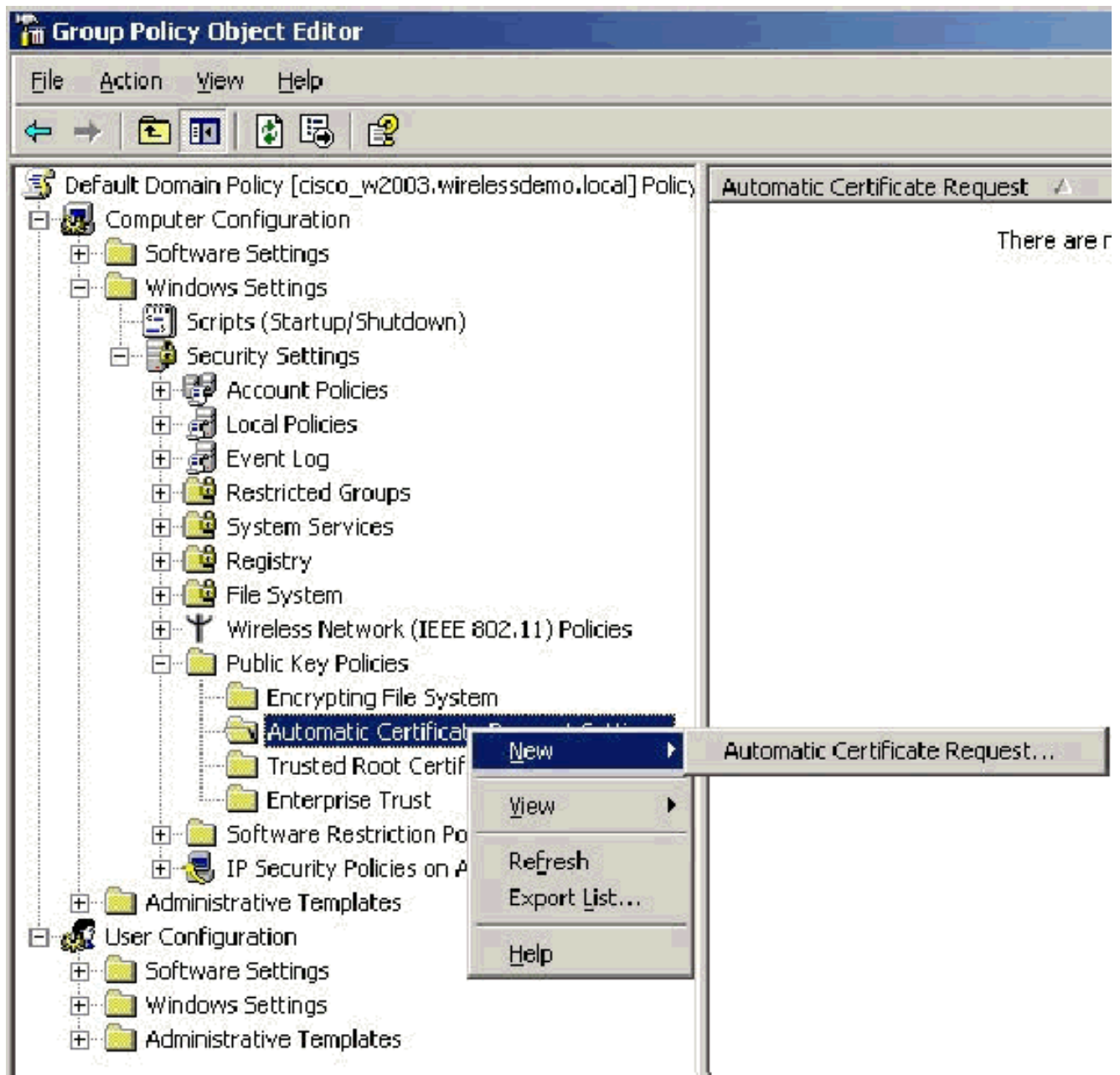
Propriétés.

7. Dans l'onglet Stratégie de groupe, cliquez sur **Stratégie de domaine par défaut**, puis sur **Modifier**. Le composant logiciel enfichable Éditeur d'objets de stratégie de groupe



s'ouvre.

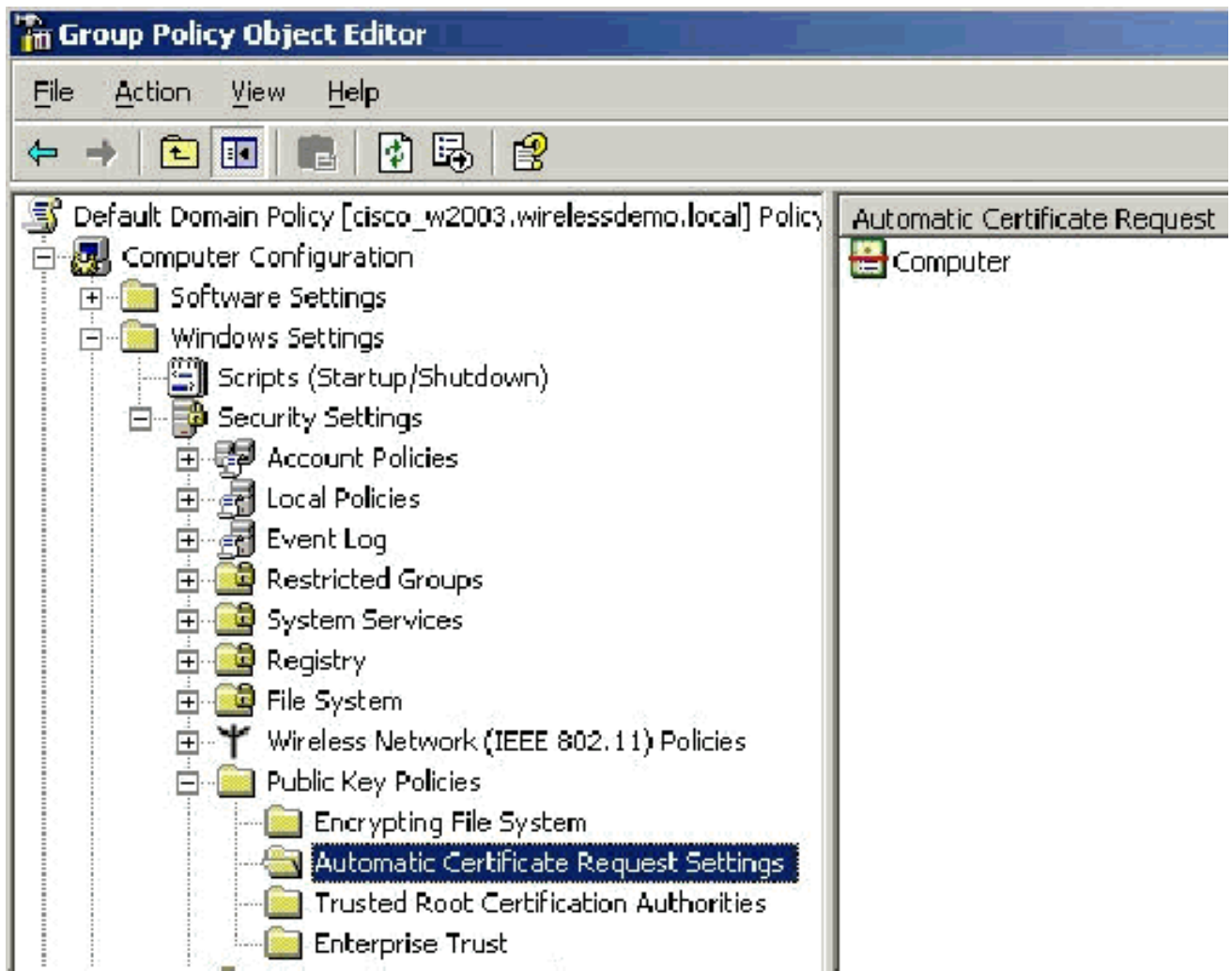
8. Dans l'arborescence de la console, développez **Configuration de l'ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies de clé publique**, puis sélectionnez **Paramètres de demande de certificat automatique**.



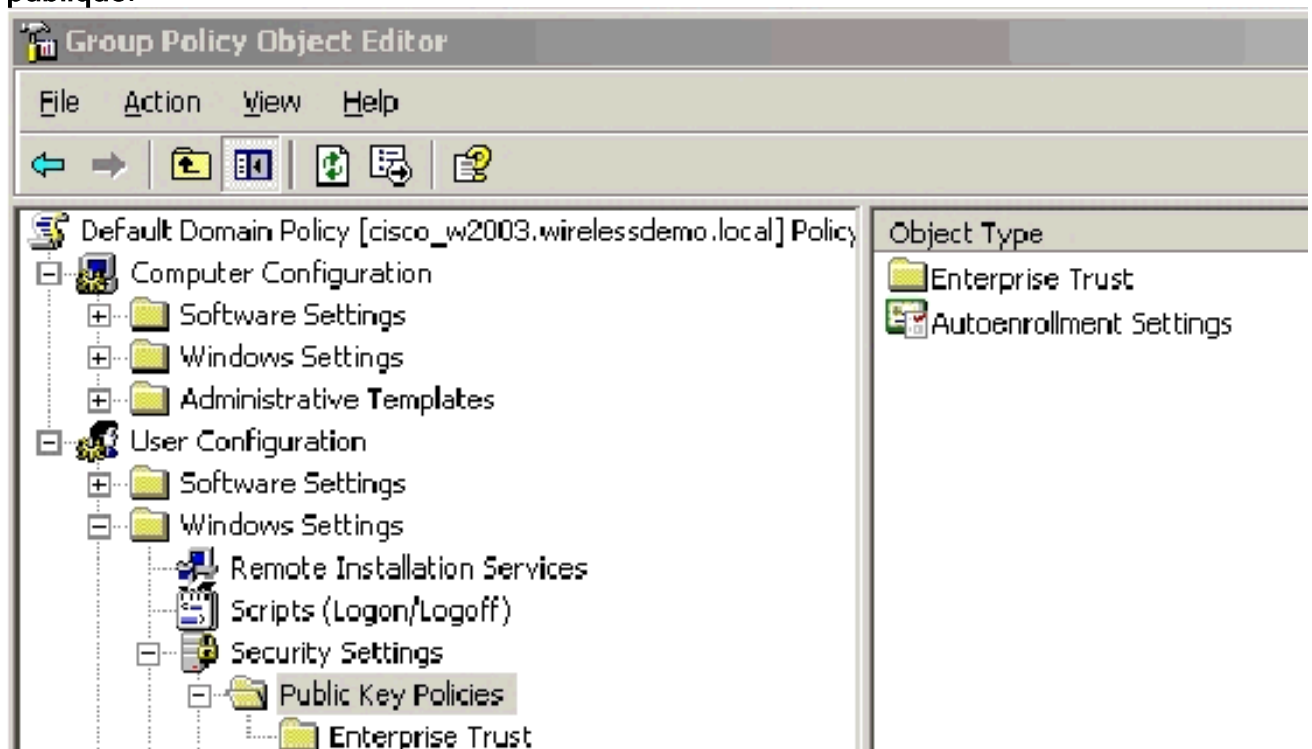
9. Cliquez avec le bouton droit sur **Paramètres de demande de certificat automatique** et sélectionnez **Nouveau > Demande de certificat automatique**.
10. Sur la page Welcome to the Automatic Certificate Request Setup Wizard, cliquez sur **Next**.
11. Sur la page Modèle de certificat, cliquez sur **Ordinateur** et cliquez sur **Suivant**.



12. Sur la page Fin de l'Assistant Configuration de la demande de certificat automatique, cliquez sur **Terminer**. Le type de certificat Ordinateur apparaît maintenant dans le volet d'informations du composant logiciel enfichable Éditeur d'objets de stratégie de groupe.

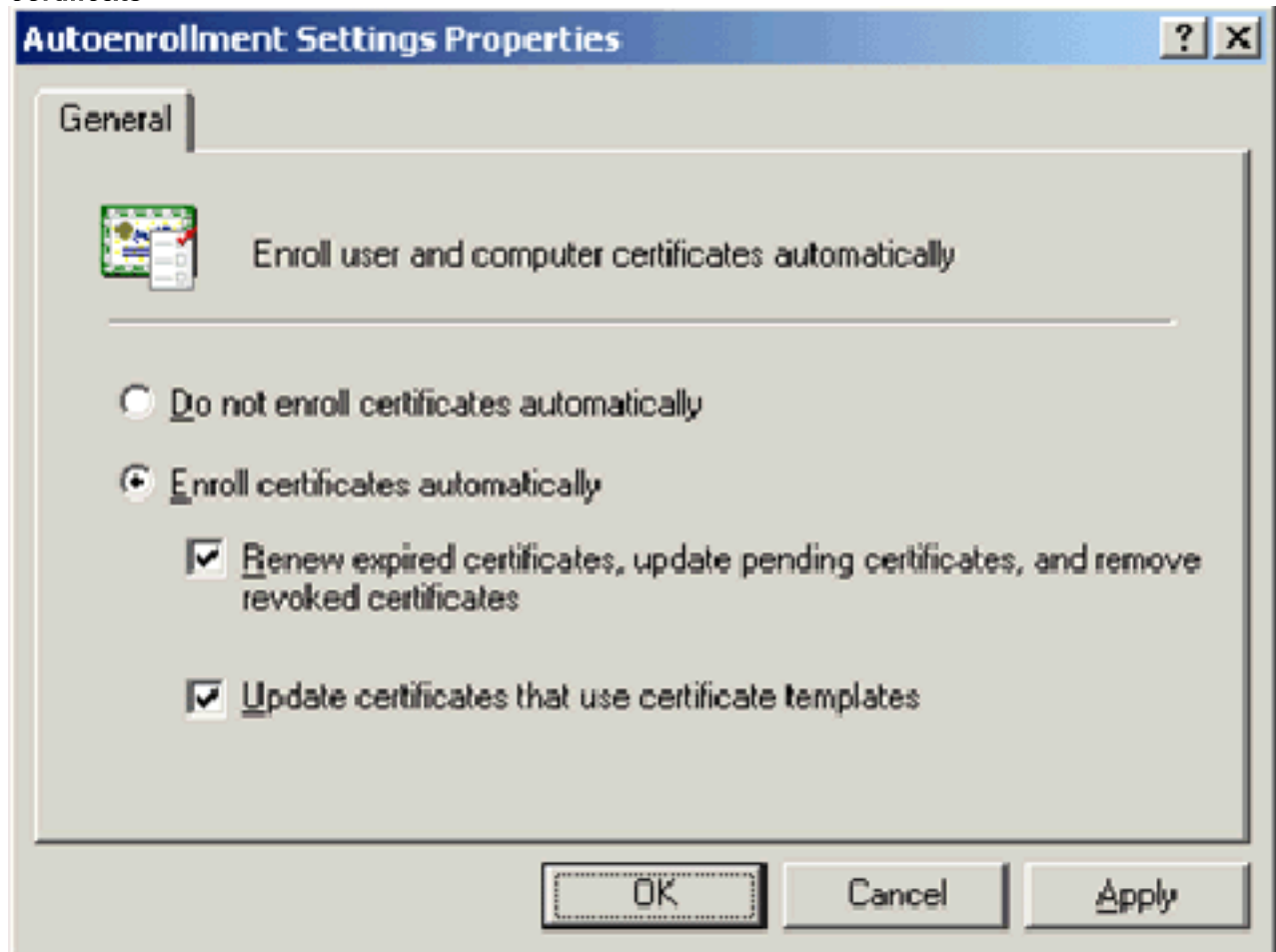


13. Dans l'arborescence de la console, développez Configuration utilisateur > Paramètres Windows > Paramètres de sécurité > Stratégies de clé publique.



14. Dans le volet d'informations, double-cliquez sur Paramètres d'inscription automatique.
 15. Choisissez Inscrire automatiquement les certificats et cochez la case Renouveler les

certificats expirés, mettre à jour les certificats en attente et supprimer les certificats révoqués et Mettre à jour les certificats qui utilisent des modèles de certificats.



16. Click OK.

[Configuration du certificat ACS 4.0](#)

[Configurer un certificat exportable pour ACS](#)

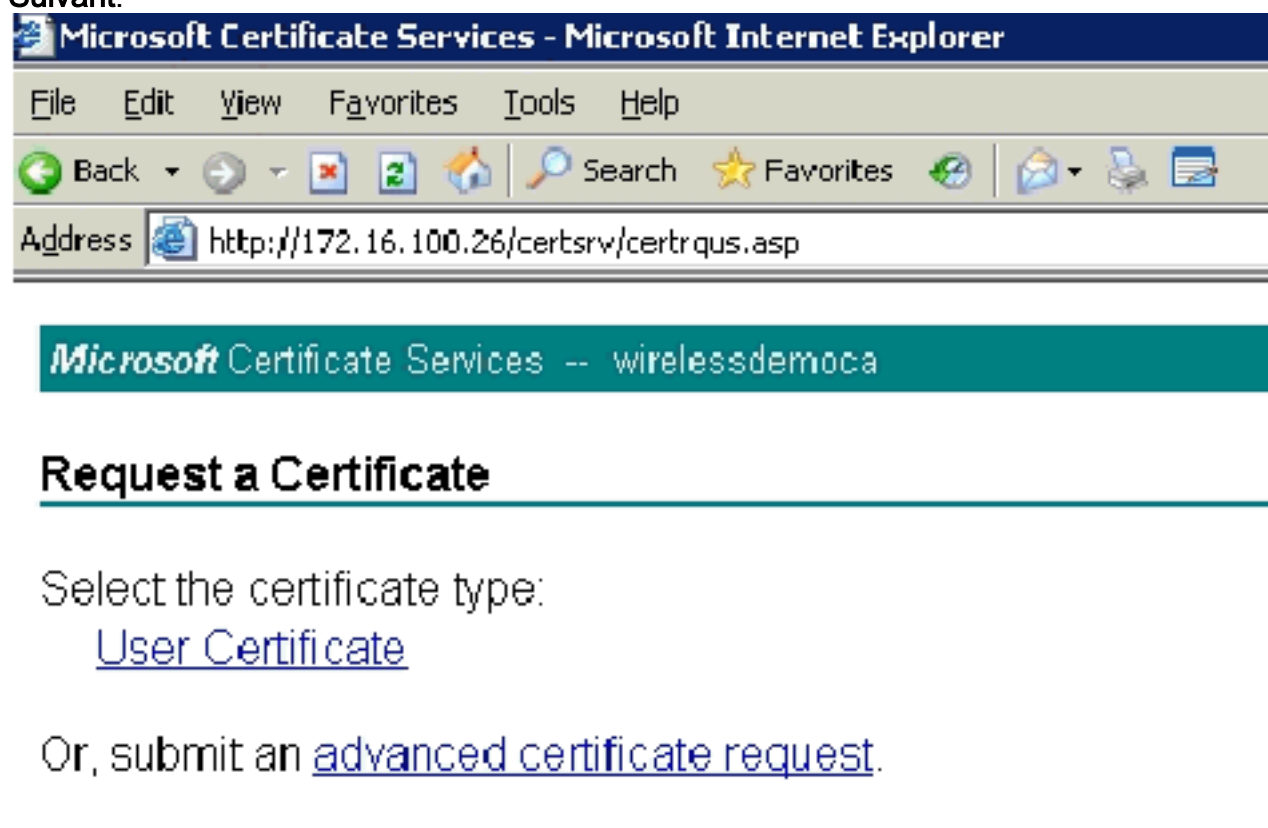
Important : Le serveur ACS doit obtenir un certificat de serveur du serveur AC racine d'entreprise afin d'authentifier un client EAP-TLS WLAN.

Important : Assurez-vous que le Gestionnaire IIS n'est pas ouvert pendant le processus de configuration du certificat car il entraîne des problèmes avec les informations mises en cache.

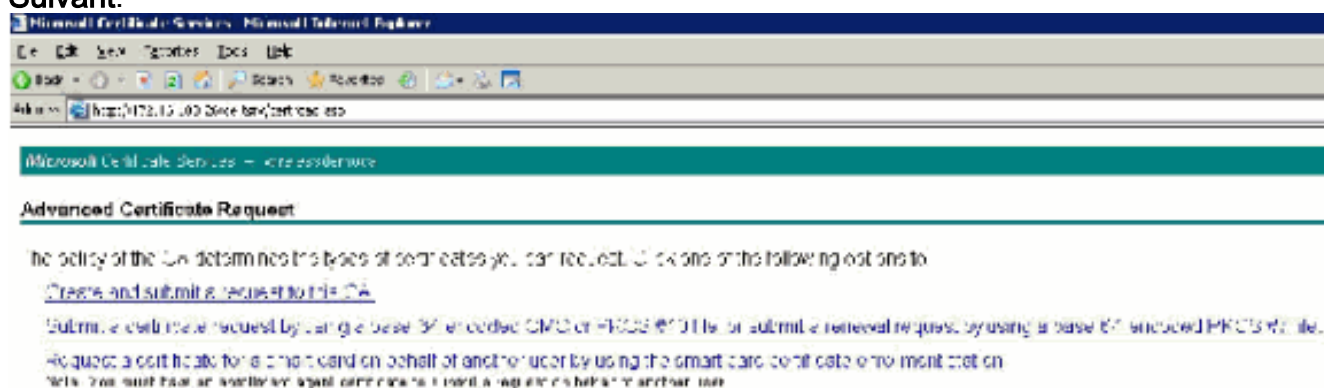
1. Connectez-vous au serveur ACS avec un compte disposant des droits d'administrateur Enterprise.
2. Sur la machine ACS locale, pointez le navigateur sur le serveur de l'autorité de certification Microsoft à l'adresse <http://IP-address-of-Root-CA/certsrv>. Dans ce cas, l'adresse IP est **172.16.100.26**.
3. Connectez-vous en tant qu'administrateur.



4. Choisissez **Demander un certificat** et cliquez sur **Suivant**.



5. Choisissez **Demande avancée** et cliquez sur **Suivant**.



6. Choisissez **Créer et soumettre une demande à cette autorité de certification** et cliquez sur **Suivant**. **Important** : Cette étape s'explique par le fait que Windows 2003 ne permet pas les clés exportables et que vous devez générer une demande de certificat basée sur le certificat ACS que vous avez créé

précédemment.

Microsoft Certificate Services - wirelessdemo.local

Advanced Certificate Request

Certificate Template:

Administrator

Key Options:

Administrator
Basic EFS
EFS Recovery Agent
User
CSP: Wireless User Certificate Template
Key Usage: S.Ordinary Certification Authority
Key Store: Web Server
Max: 15384
1024 2048 4096 8192 16384

Automatic key container name User specified key container name

Mark keys as exportable
 Export keys to file

Enable strong private key protection

Store certificate in the local computer certificate store
Saves the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

Request Format: CMC PKCS10

Hash Algorithm: SHA-1
Only used to sign request.

Save request to file

Attributes:

Friendly Name:

7. Dans Modèles de certificat, sélectionnez le modèle de certificat créé précédemment nommé **ACS**. Les options changent après avoir sélectionné le modèle.
8. Configurez le nom comme nom de domaine complet du serveur ACS. Dans ce cas, le nom du serveur ACS est cisco_w2003.wirelessdemo.local. Assurez-vous que le **certificat du magasin de certificats de l'ordinateur local** est coché et cliquez sur

Microsoft Certificate Services - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites

Address http://172.16.100.25/certsrv/certreqs.asp

Certificate Template:

ACS

Identifying Information For Offline Template:

Name:

E-Mail:

Company:

Department:

City:

State:

Country/Region:

Key Options:

Create new key set Use existing key set

CSP:

Key Usage: Exchange

Key Size: Min:1024 Max:1024 (common key sizes: 3024)

Automatic key container name User specified key container name

Mark keys as exportable

Export keys to file

Store certificate in the local computer certificate store
Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

Request Format: CMC PKCS10

Hash Algorithm:
Only used to sign request.

Save request to a file

Attributes:

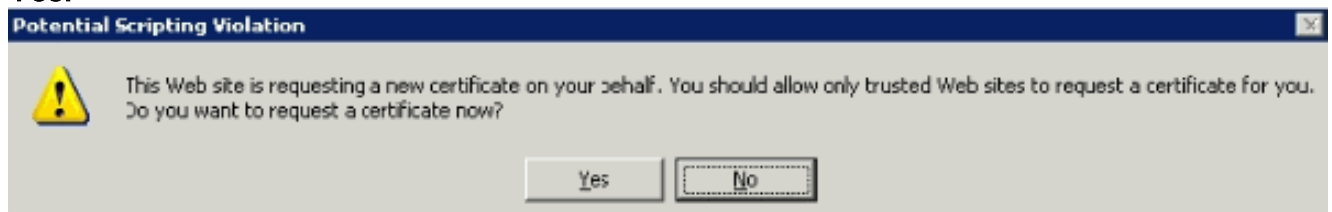
Friendly Name:

Soumettre.

9. Une fenêtre contextuelle s'affiche et vous avertit d'une violation potentielle des scripts.

Cliquez sur

Yes.



10. Cliquez sur **Installer ce certificat.**



Microsoft Certificate Services -- wirelessdemoca

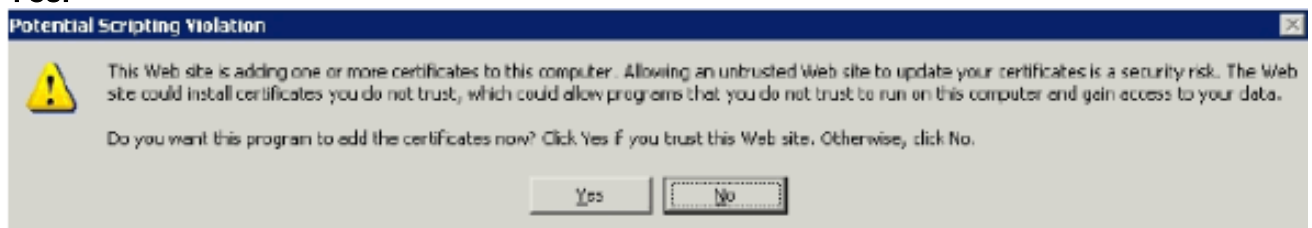
Certificate Issued

The certificate you requested was issued to you.

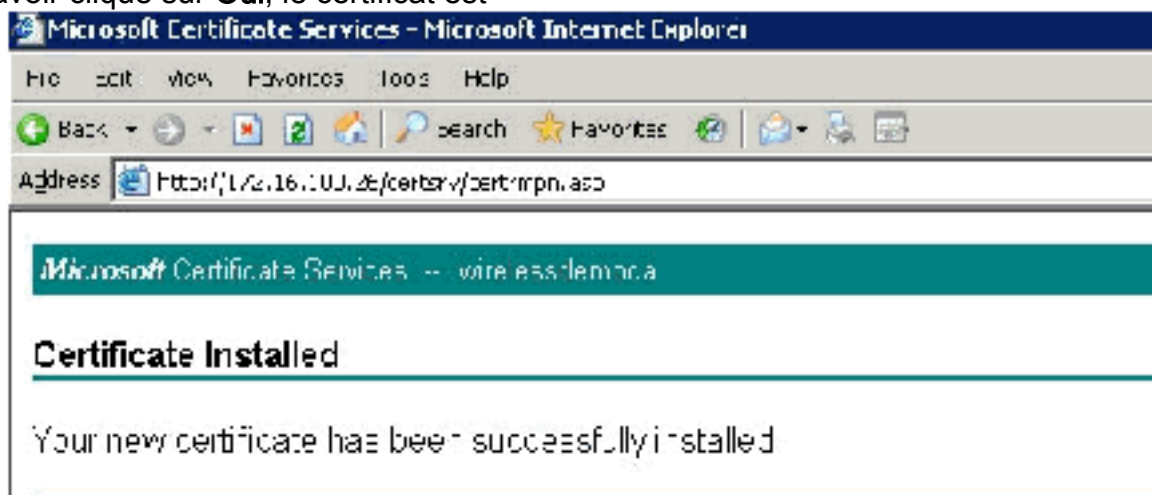


[Install this certificate](#)

11. Une fenêtre contextuelle s'affiche à nouveau et met en garde contre une violation potentielle des scripts. Cliquez sur **Yes**.

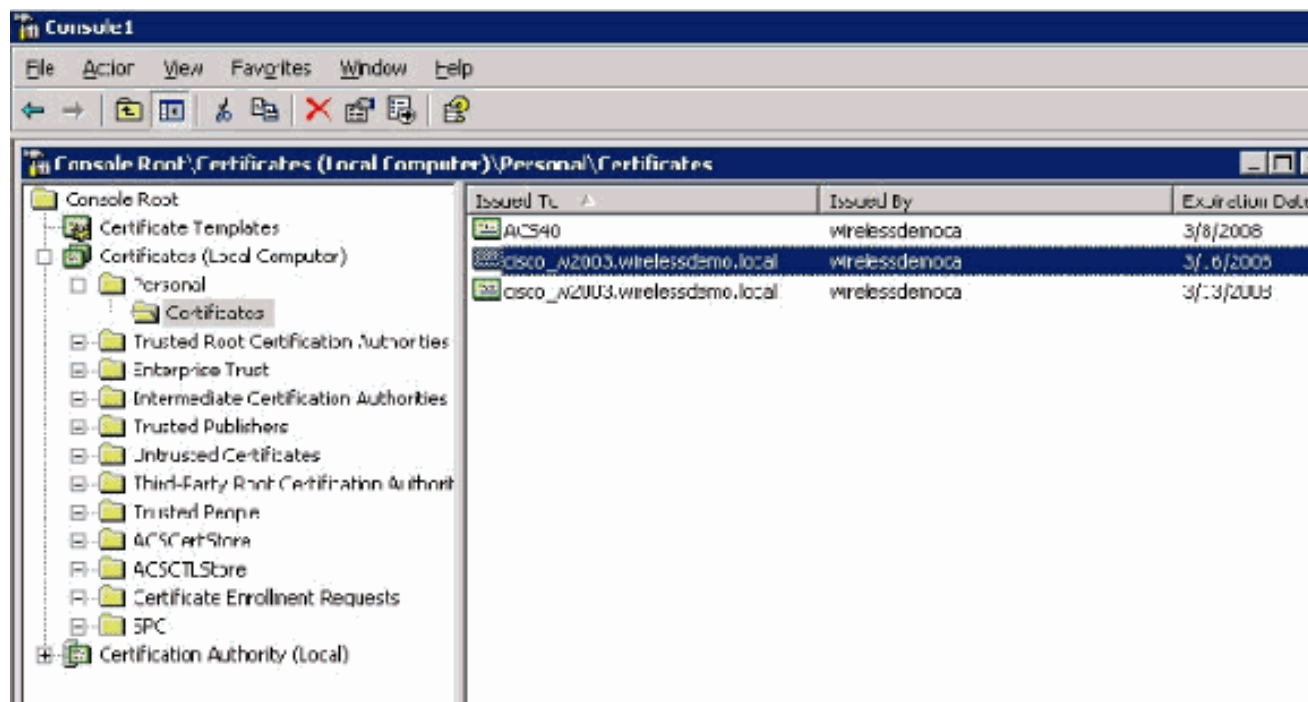


12. Après avoir cliqué sur **Oui**, le certificat est



installé.

13. À ce stade, le certificat est installé dans le dossier Certificates. Pour accéder à ce dossier, choisissez **Démarrer > Exécuter**, tapez **mmc**, appuyez sur **Entrée**, puis choisissez **Personnel > Certificats**.



14. Maintenant que le certificat est installé sur l'ordinateur local (ACS ou cisco_w2003 dans cet exemple), vous devez générer un fichier de certificat (.cer) pour la configuration du fichier de certificat ACS 4.0.
15. Sur le serveur ACS (cisco_w2003 dans cet exemple), pointez le navigateur du serveur de l'Autorité de certification Microsoft sur [http://172.16.100.26 /certsrv](http://172.16.100.26/certsrv).

[Installer le certificat dans le logiciel ACS 4.0](#)

Procédez comme suit :

1. Sur le serveur ACS (cisco_w2003 dans cet exemple), pointez le navigateur sur le serveur Microsoft CA vers [http://172.16.100.26 /certsrv](http://172.16.100.26/certsrv).
2. Dans l'option Sélectionner une tâche, sélectionnez **Télécharger un certificat CA, une chaîne de certificats ou une liste de révocation de certificats**.
3. Choisissez la méthode de codage radio **Base 64** et cliquez sur **Télécharger le certificat CA**.

Microsoft Certificate Services - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address http://172.16.100.26/certs/certnew.asp

Microsoft Certificate Services -- wirelessdemora

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority [install this CA certificate chain](#).

To download a CA certificate, certificate chain, or CRL, select the certificate encoding method:

CA certificate:

Current (wirelessdemora)

Encoding method:

DER

Base 64

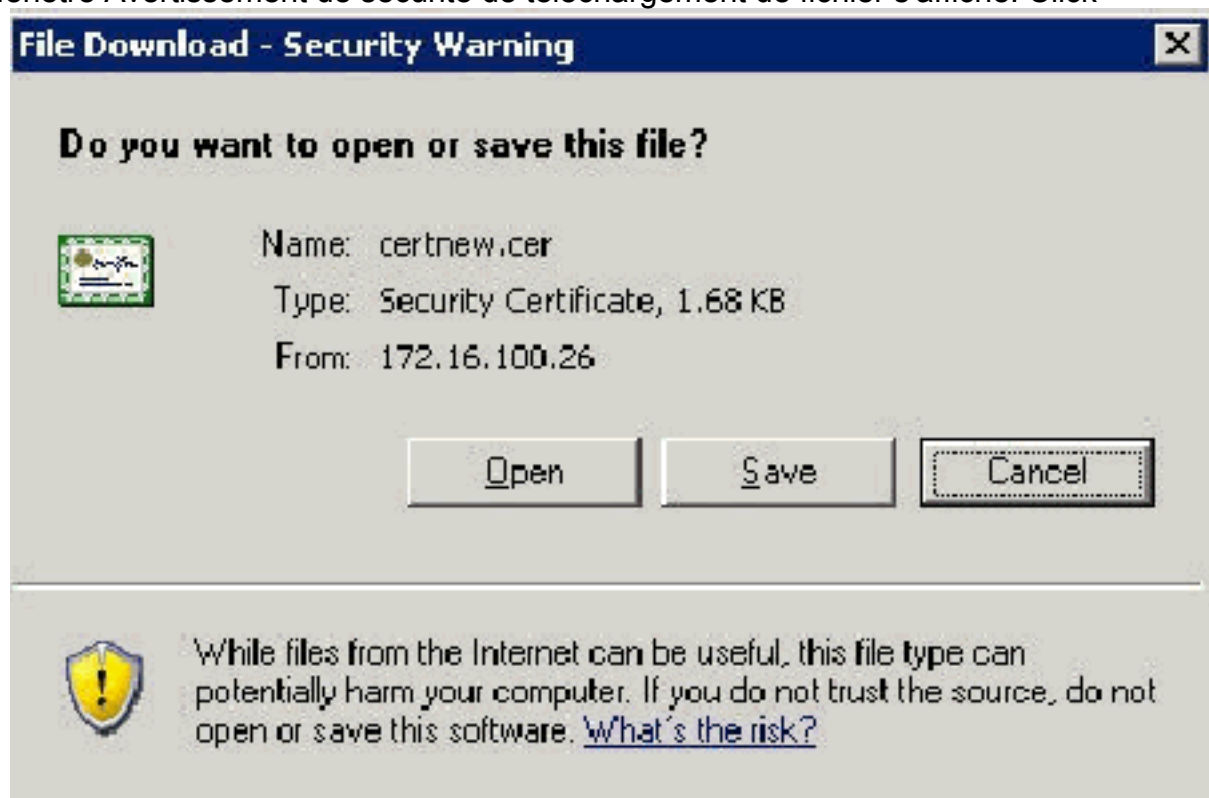
[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

[Download latest delta CRL](#)

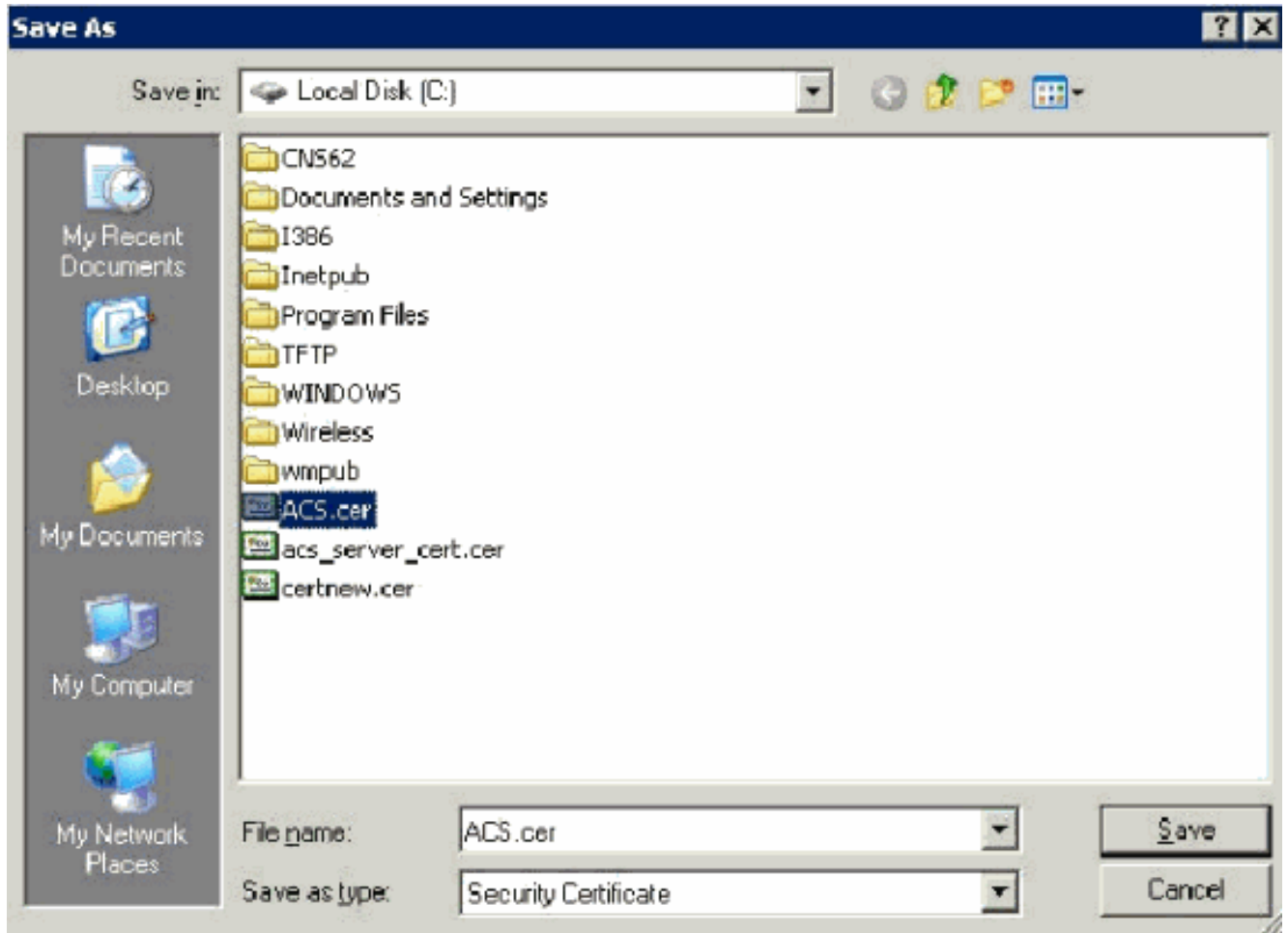
4. Une fenêtre Avertissement de sécurité de téléchargement de fichier s'affiche. Cliquez



Save.

5. Enregistrez le fichier avec un nom tel que ACS.cer ou tout autre nom que vous souhaitez. N'oubliez pas ce nom car vous l'utilisez lors de la configuration de l'autorité de certification ACS dans ACS

4.0.








6. Ouvrez **ACS Admin** à partir du raccourci de bureau créé lors de l'installation.

7. Cliquez sur **Configuration du**



System Configuration

Select

 User Setup	 Service Control
 Group Setup	 Logging
 Shared Profile Components	 Date Format Control
 Network Configuration	 Local Password Management
 System Configuration	 ACS Internal Database Replication
 Interface Configuration	 ACS Backup
 Administration Control	 ACS Restore
 External User Databases	 ACS Service Management
	 VoIP Accounting Configuration
	 ACS Certificate Setup
	 Global Authentication Setup

systeme.

8. Cliquez sur **Configuration du certificat ACS**.

System Configuration

Select

ACS Certificate Setup

-  [Install ACS Certificate](#)
-  [ACS Certification Authority Setup](#)
-  [Edit Certificate Trust List](#)
-  [Certificate Revocation Lists](#)
-  [Generate Certificate Signing Request](#)
-  [Generate Self-Signed Certificate](#)

Cancel

9. Cliquez sur **Installer le certificat ACS**.

System Configuration

Edit

Install ACS Certificate

Install new certificate 	
<input type="radio"/> Read certificate from file	
Certificate file	<input type="text"/>
<input checked="" type="radio"/> Use certificate from storage	
Certificate CN	<input type="text"/>
Private key file	<input type="text"/>
Private key password	<input type="text"/>

10. Choisissez **Use certificate from storage** et saisissez le nom de domaine complet **cisco_w2003.wirelessdemo.local** (ou **ACS.wirelessdemo.local** si vous avez utilisé ACS comme

nom).

System Configuration

Edit

Install ACS Certificate


Install new certificate 	
<input type="radio"/> Read certificate from file	
Certificate file	<input type="text"/>
<input checked="" type="radio"/> Use certificate from storage	
Certificate CN	<input type="text" value="cisco_w2003.wirelessde"/>
Private key file	<input type="text"/>
Private key password	<input type="text"/>

11. Cliquez sur
Submit.

System Configuration

Edit

Install ACS Certificate

Installed Certificate Information 	
Issued to:	cisco_w2003.wirelessdemo.local
Issued by:	wirelessdemoca
Valid from:	March 17 2006 at 08:33:25
Valid to:	March 16 2008 at 08:33:25
Validity:	OK

**The current configuration has been changed.
Restart ACS in "System Configuration:Service
Control" to adopt the new settings for EAP-TLS or
PEAP support only.**

12. Cliquez sur Configuration du système.


13. Cliquez sur **Contrôle de service** puis sur **Redémarrer**.

System Configuration

Select

CiscoSecure ACS on cisco_w2003 

Is Currently Running

Services Log File Configuration 

Level of detail

None

Low

Full

Generate New File

Every day

Every week


Every month

When size is greater than KB

Manage Directory

Keep only the last files


Delete files older than days

 [Back to Help](#)

14. Cliquez sur **Configuration du système**.
15. Cliquez sur **Configuration de l'authentification globale**.
16. Cochez **Allow EAP-TLS** et toutes les cases en dessous.

System Configuration

Global Authentication Setup

EAP Configuration 

PEAP

Allow EAP-MSCHAPv2

Allow EAP-GTC

Allow Posture Validation

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

EAP-FAST

[EAP-FAST Configuration](#)

EAP-TLS

Allow EAP-TLS

Select one or more of the following options:

- Certificate SAN comparison
- Certificate CN comparison
- Certificate Binary comparison

EAP-TLS session timeout (minutes):

17. Cliquez sur **Soumettre + Redémarrer**.
18. Cliquez sur **Configuration du système**.
19. Cliquez sur **Configuration de l'autorité de certification ACS**.
20. Dans la fenêtre Configuration de l'autorité de certification ACS, tapez le nom et l'emplacement du fichier *.cer créé précédemment. Dans cet exemple, le fichier *.cer créé est **ACS.cer** dans le répertoire racine c:\.
21. Tapez **c:\acs.cer** dans le champ du fichier de certificat CA et cliquez sur **Soumettre**.

System Configuration

Edit

ACS Certification Authority Setup

CA Operations	
Add new CA certificate to local certificate storage	
CA certificate file	<input type="text" value="c:\acs.cer"/>

System Configuration

ACS Certification Authority Setup	
CA Operations	
Add new CA certificate to local certificate storage	
CA certificate file	<input type="text" value="c:\acs.cer"/>
The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.	

New CA certificate is successfully added into the global system certificate storage.	
CA certificate common name	wirelessdemo.ca

22. Redémarrez le service ACS.

[Configuration CLIENT pour EAP-TLS à l'aide de Windows Zero Touch](#)

CLIENT est un ordinateur qui exécute Windows XP Professionnel avec SP2 qui agit en tant que client sans fil et obtient l'accès aux ressources intranet via le point d'accès sans fil. Suivez les procédures de cette section afin de configurer CLIENT en tant que client sans fil.

[Installation et configuration de base](#)

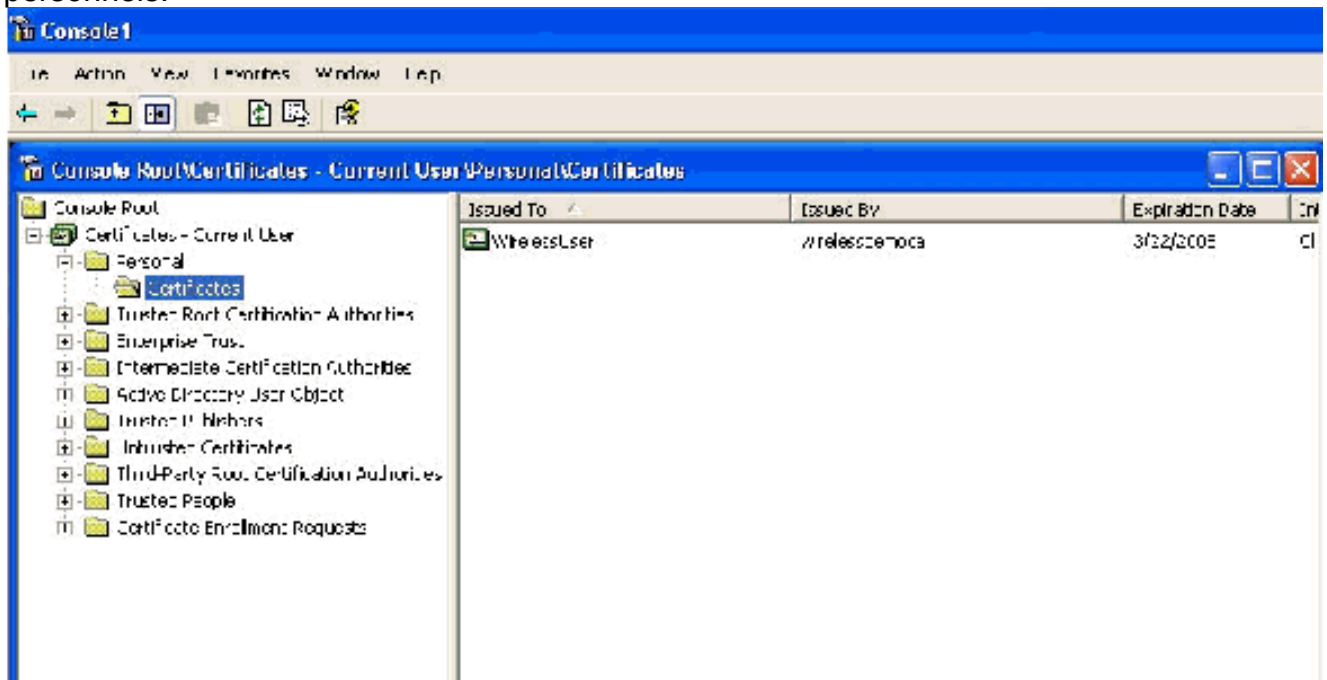
Procédez comme suit :

1. Connectez le CLIENT au segment de réseau intranet à l'aide d'un câble Ethernet connecté au commutateur.
2. Sur CLIENT, installez Windows XP Professionnel avec SP2 en tant qu'ordinateur membre nommé **CLIENT** sur le domaine wirelessdemo.local.
3. Installer Windows XP Professionnel avec SP2. Ceci doit être installé afin d'avoir la prise en charge EAP-TLS et PEAP. **Remarque** : Le pare-feu Windows est automatiquement activé dans Windows XP Professionnel avec SP2. N'éteignez pas le pare-feu.

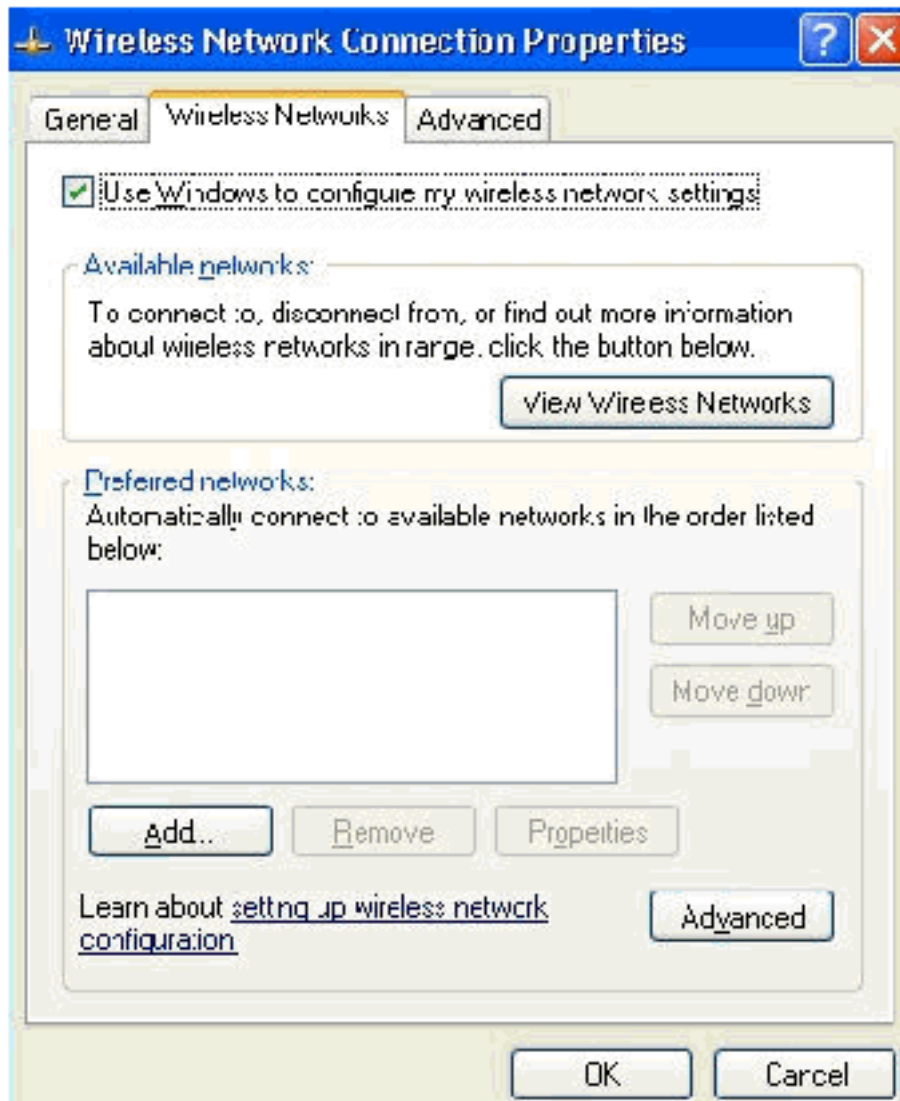
[Configuration de la connexion réseau sans fil](#)

Procédez comme suit :

1. Déconnectez-vous, puis ouvrez une session à l'aide du compte WirelessUser du domaine wirelessdemo.local. **Remarque** : mettez à jour les paramètres de stratégie de groupe de configuration de l'ordinateur et de l'utilisateur et obtenez immédiatement un certificat d'ordinateur et d'utilisateur pour l'ordinateur client sans fil, en tapant **gpupdate** à une invite de commandes. Sinon, lorsque vous vous déconnectez, puis que vous vous connectez, il exécute la même fonction que **gpupdate**. Vous devez être connecté au domaine en vous connectant via le câble. **Remarque** : afin de valider que le certificat est installé automatiquement sur le client, ouvrez le certificat MMC et vérifiez que le certificat WirelessUser est disponible dans le dossier Certificats personnels.

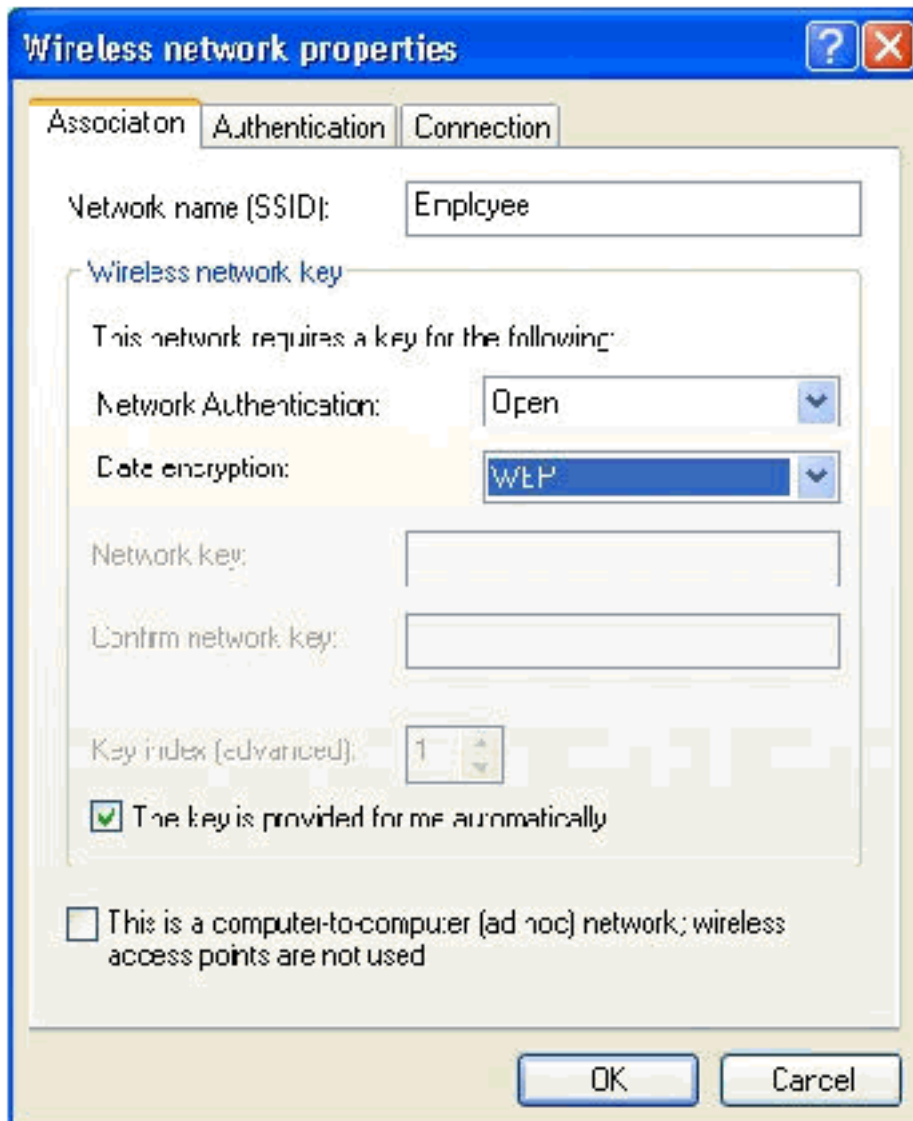


2. Choisissez **Démarrer > Panneau de configuration**, double-cliquez sur **Connexions réseau**, puis cliquez avec le bouton droit sur **Connexion réseau sans fil**.
3. Cliquez sur **Propriétés**, accédez à l'onglet **Réseaux sans fil** et assurez-vous que **Windows utilisateur pour configurer mes paramètres réseau sans fil** est



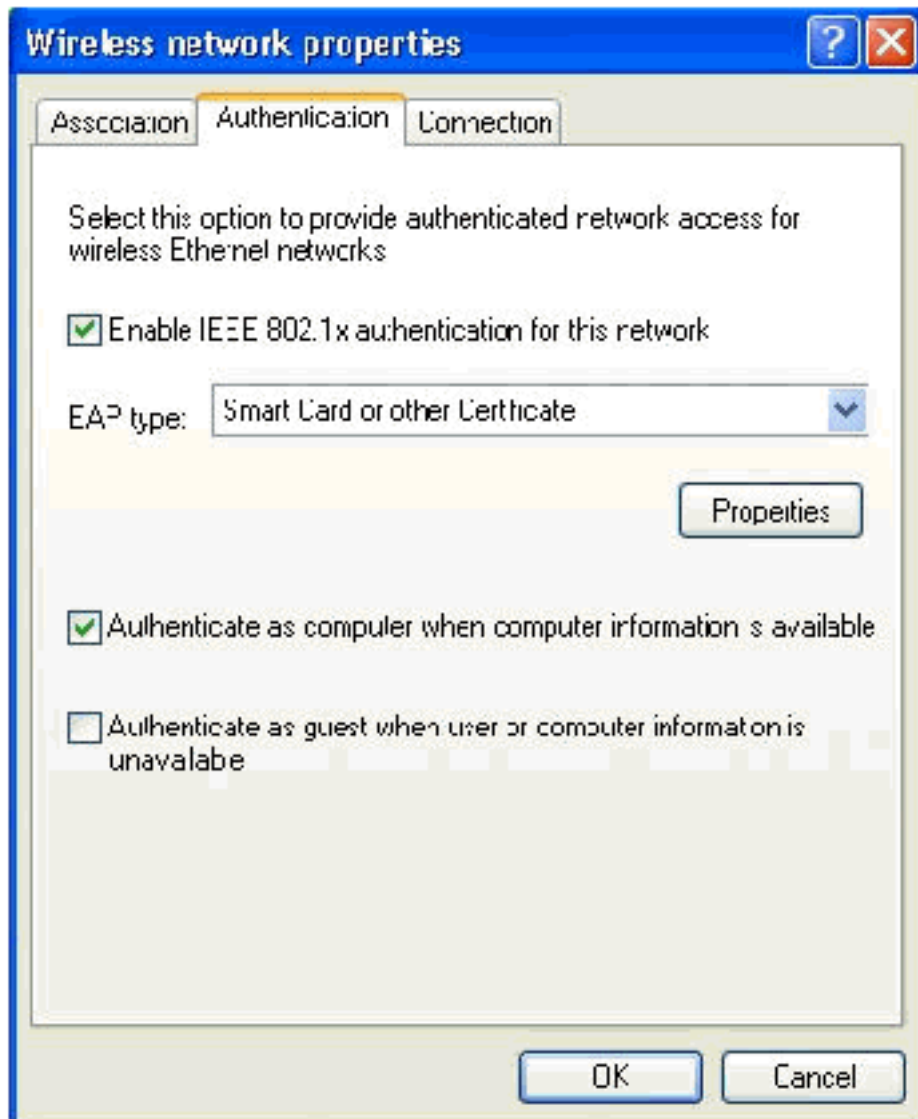
coché.

4. Cliquez sur **Add**.
5. Accédez à l'onglet Association et tapez **Employee** dans le champ Network name (SSID).
6. Assurez-vous que le chiffrement des données est défini sur **WEP** et que la clé est fournie automatiquement est



cochée.

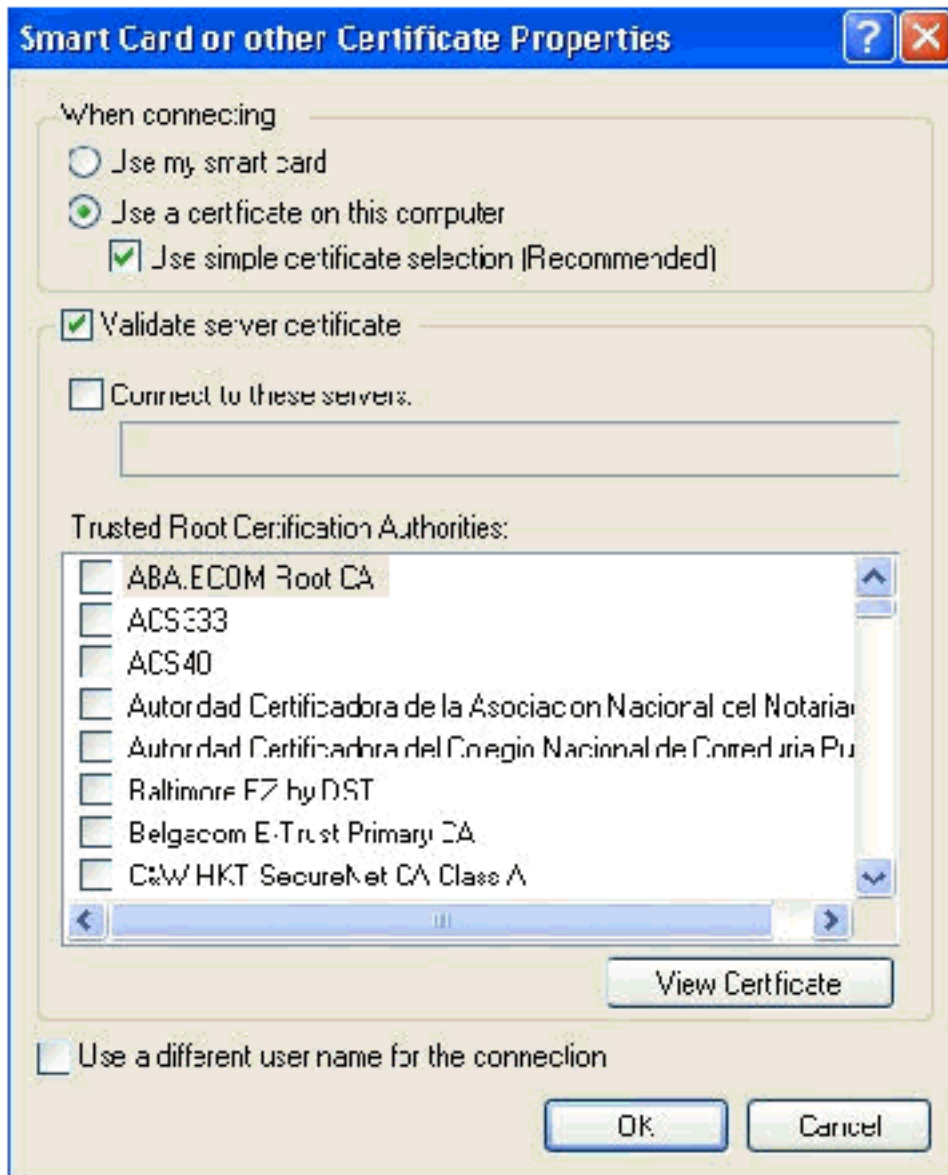
7. Accédez à l'onglet Authentification.
8. Validez que le type EAP est configuré pour utiliser **Smart Card ou un autre certificat**. Si ce n'est pas le cas, sélectionnez-le dans le menu déroulant.
9. Si vous voulez que l'ordinateur soit authentifié avant la connexion (ce qui permet l'application de scripts de connexion ou de politiques de groupe), choisissez l'option **Authentifier en tant qu'ordinateur lorsque des informations d'ordinateur sont**



disponibles.

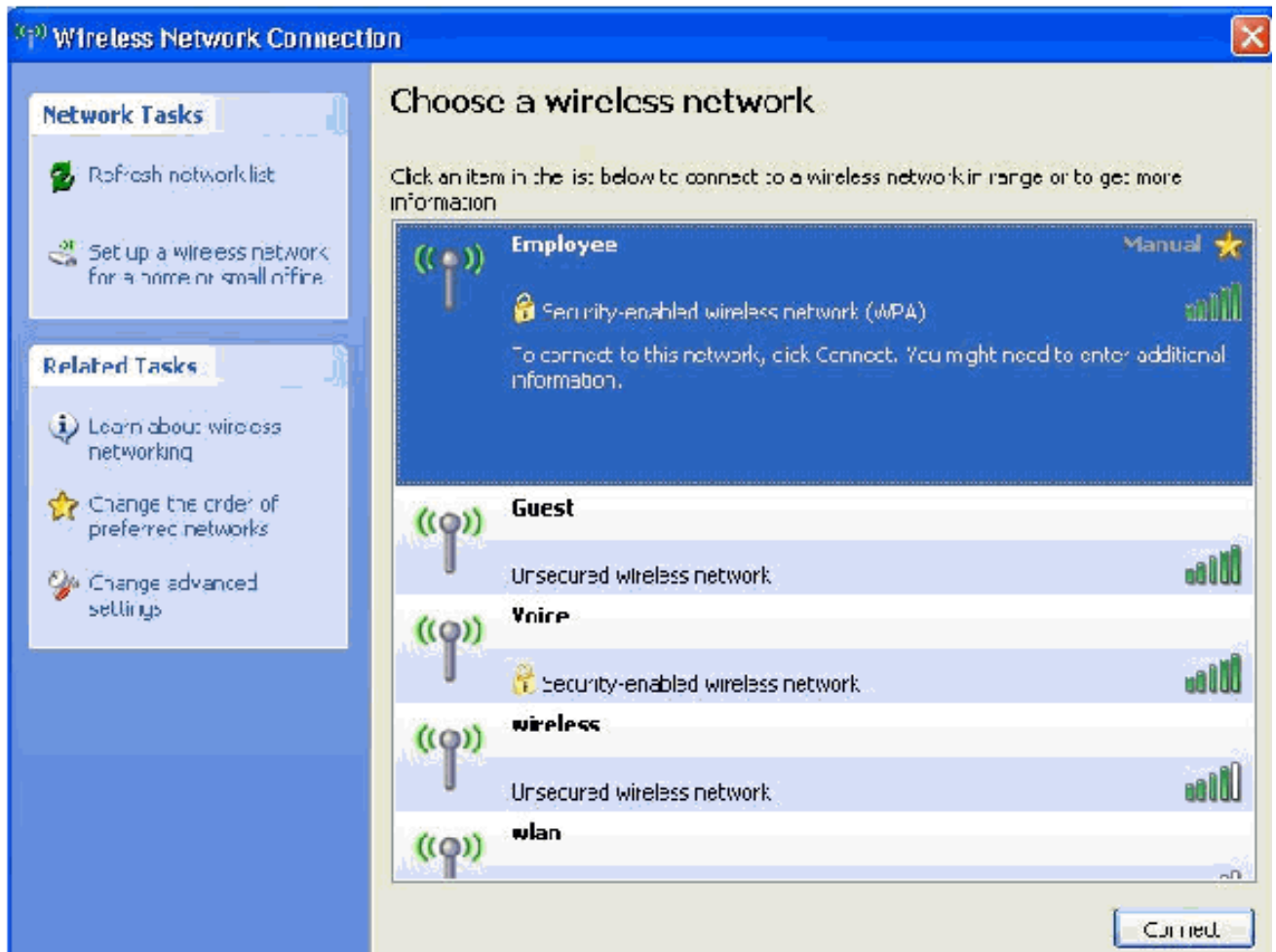
10. Cliquez sur **Properties**.

11. Vérifiez que les cases de cette fenêtre sont

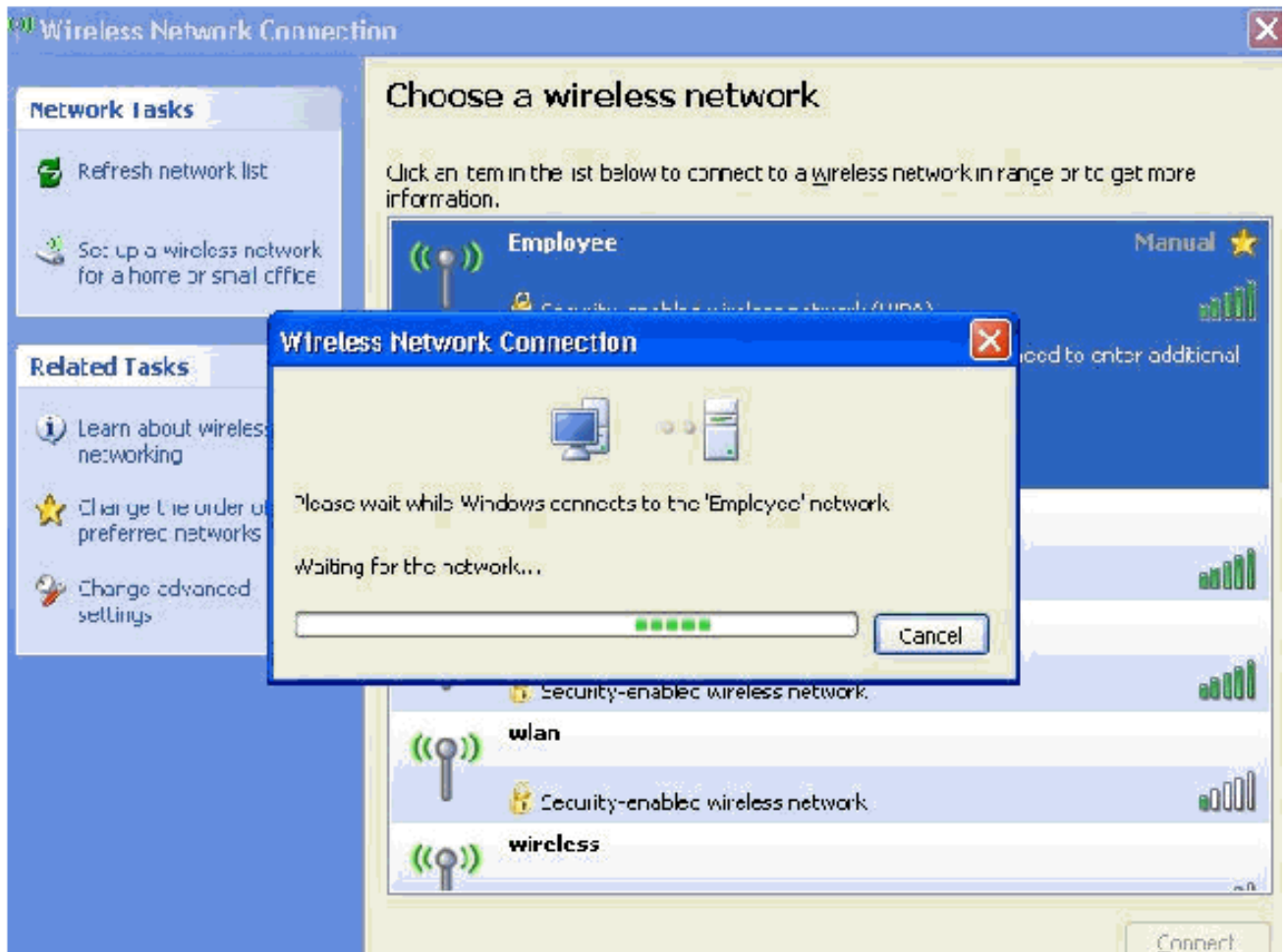


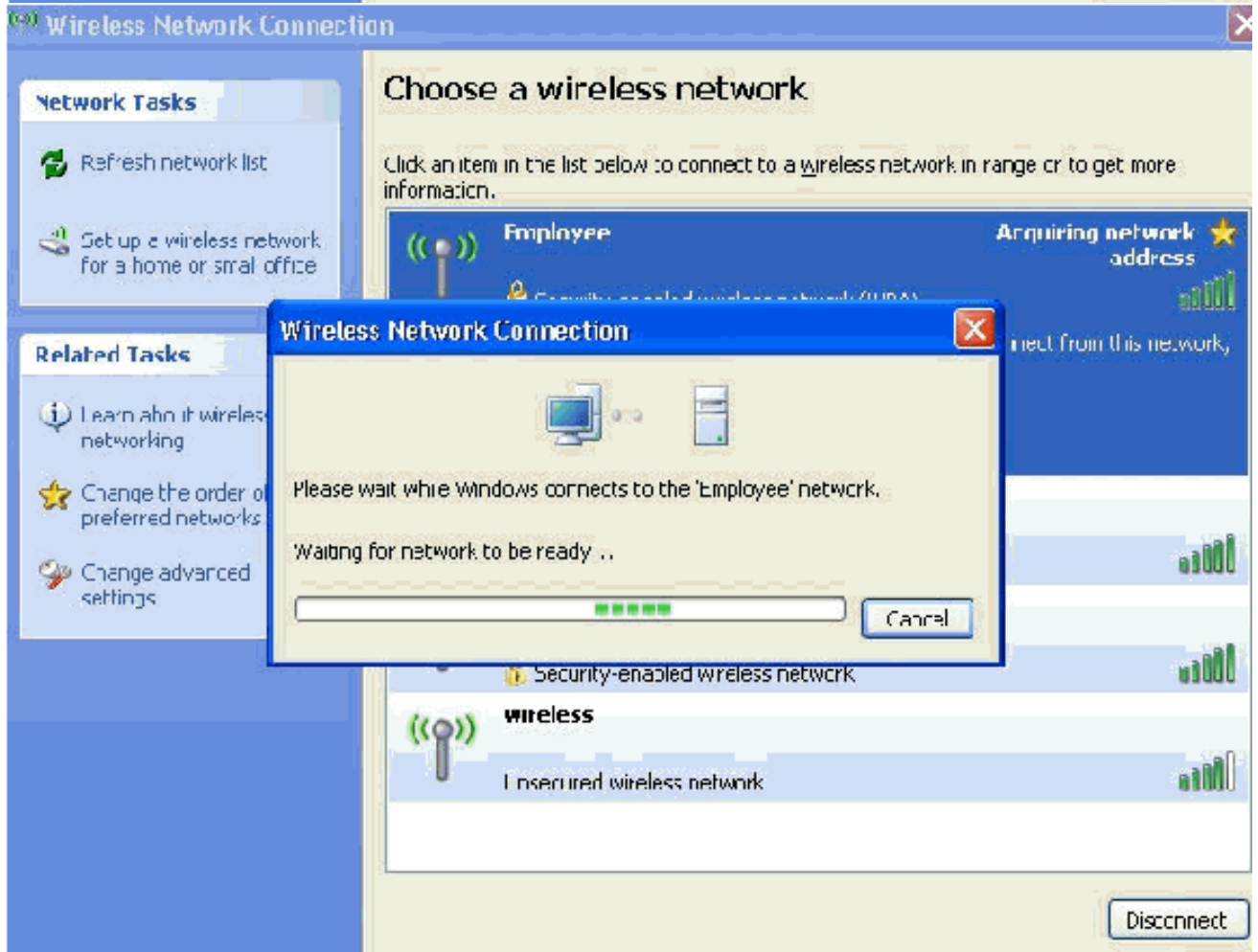
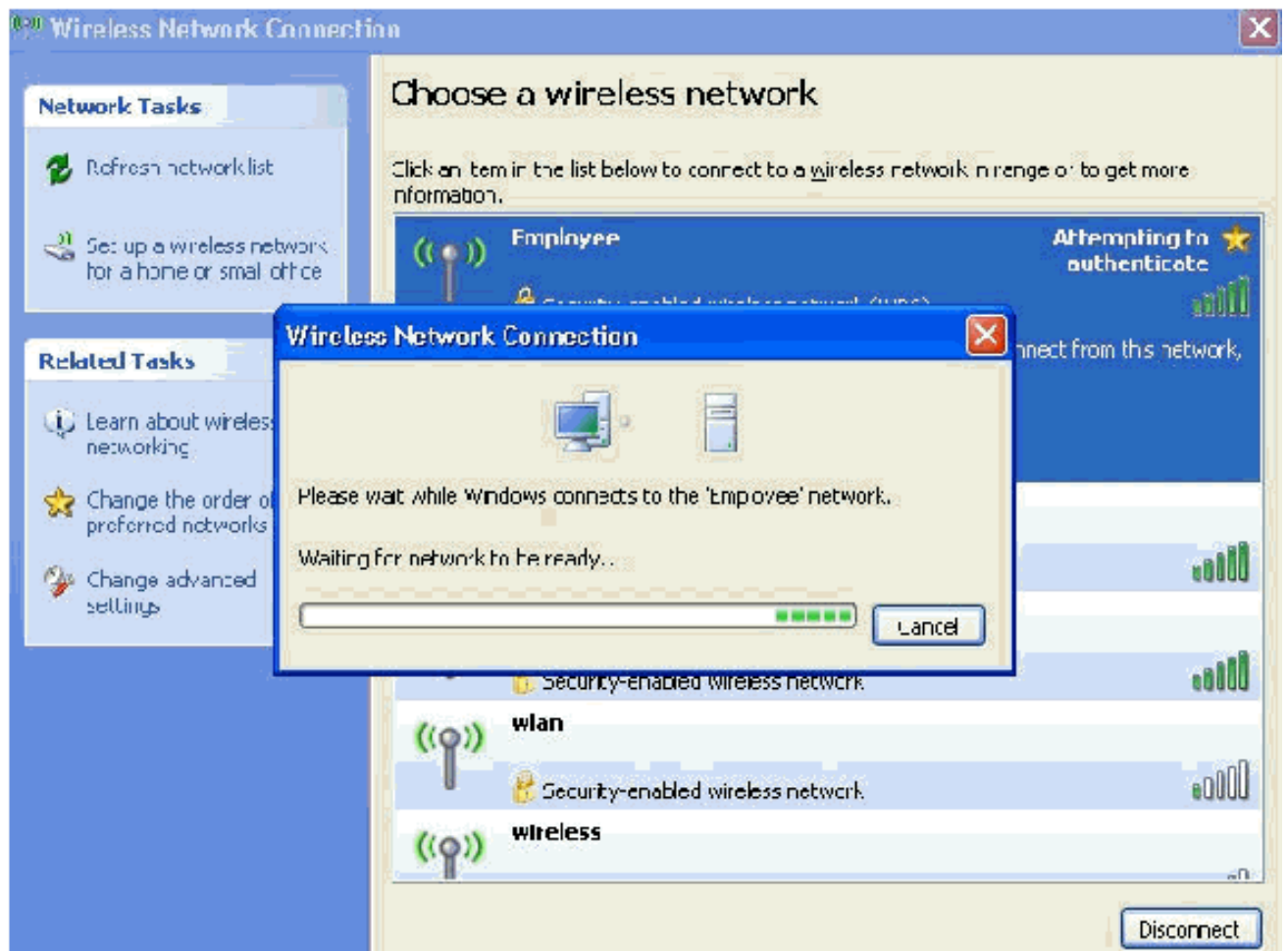
cochées.

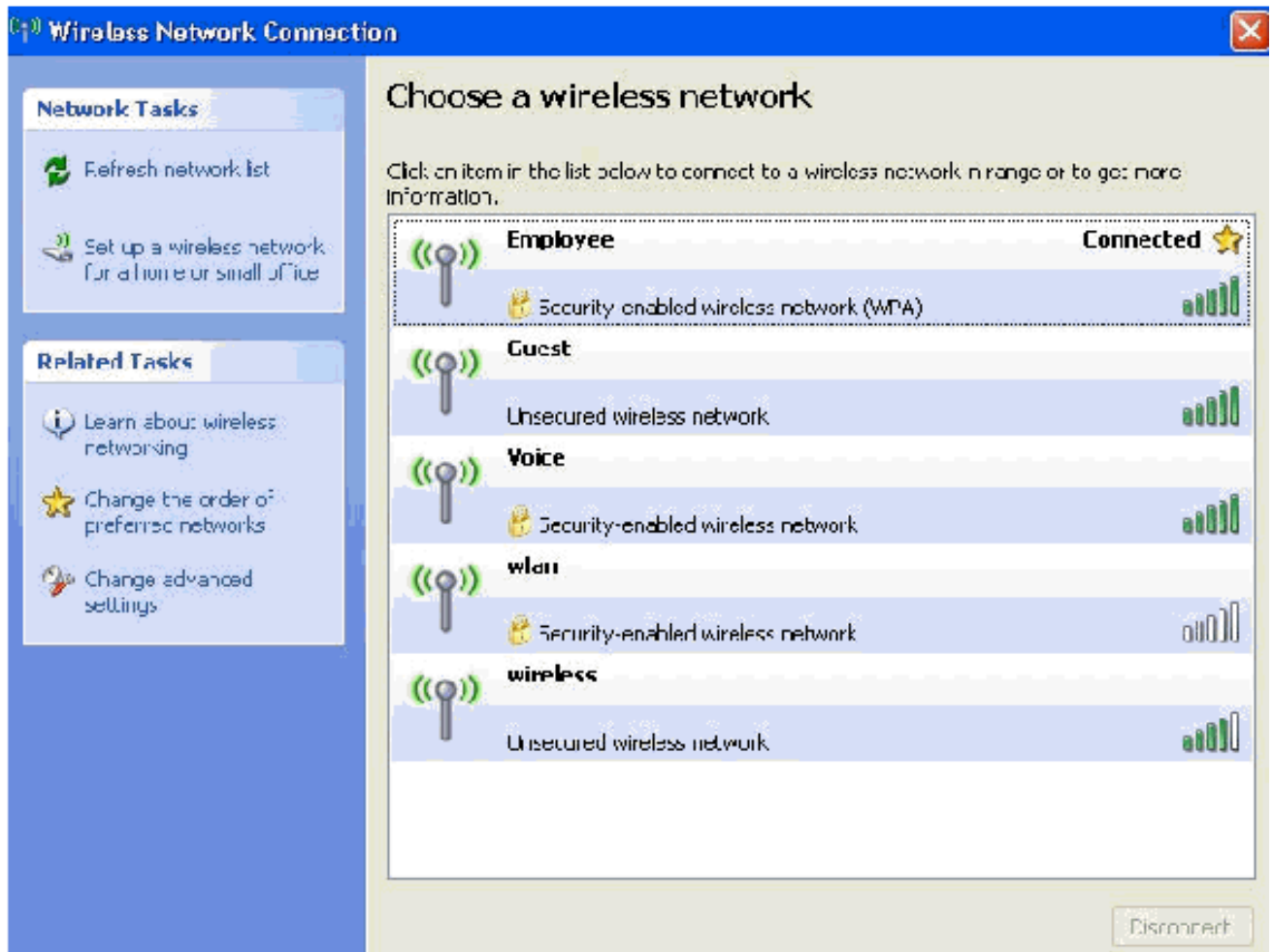
12. Cliquez trois fois sur **OK**.
13. Cliquez avec le bouton droit sur l'icône de connexion au réseau sans fil dans Systray, puis cliquez sur **Afficher les réseaux sans fil disponibles**.
14. Cliquez sur le réseau sans fil **Employé** et cliquez sur **Connexion**.



Ces captures d'écran indiquent si la connexion s'est terminée correctement.







15. Une fois l'authentification réussie, vérifiez la configuration TCP/IP de la carte sans fil à l'aide de Connexions réseau. Il doit avoir une plage d'adresses de 172.16.100.100-172.16.100.254 à partir de la portée DHCP ou de la portée créée pour les clients sans fil.
16. Afin de tester la fonctionnalité, ouvrez un navigateur et accédez à <http://wirelessdemoca> (ou l'adresse IP du serveur AC d'entreprise).

Informations connexes

- [Exemple de configuration de l'authentification EAP avec des contrôleurs de réseau local sans fil \(WLC\)](#)
- [Guide de configuration du contrôleur LAN sans fil](#)
- [Exemple de configuration de base d'un contrôleur LAN sans fil et d'un point d'accès léger](#)
- [Exemple de configuration de réseaux VLAN sur des contrôleurs de réseau local sans fil](#)
- [Exemple de configuration de réseaux VLAN de groupe de points d'accès avec des contrôleurs de réseau local sans fil](#)
- [Support et documentation techniques - Cisco Systems](#)