

PEAP sous UWN avec ACS 5.1 et Windows 2003 Server

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Conventions](#)

[Configurer](#)

[Diagramme du réseau](#)

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

[CA \(démocratie\)](#)

[Cisco 1121 Secure ACS 5.1](#)

[Installation à l'aide de l'appliance de la gamme CSACS-1121](#)

[Installation du serveur ACS](#)

[Configuration du contrôleur Cisco WLC5508](#)

[Créer la configuration nécessaire pour WPAv2/WPA](#)

[Authentification PEAP](#)

[Installation du composant logiciel enfichable Modèles de certificats](#)

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

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

[Configuration du certificat ACS 5.1](#)

[Configurer le certificat exportable pour ACS](#)

[Installation du certificat dans le logiciel ACS 5.1](#)

[Configurer le magasin d'identités ACS pour Active Directory](#)

[Ajouter un contrôleur à ACS en tant que client AAA](#)

[Configuration des stratégies d'accès ACS pour les réseaux sans fil](#)

[Créer une stratégie d'accès ACS et une règle de service](#)

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

[Installation et configuration de base](#)

[Installation de la carte réseau sans fil](#)

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

[Dépannage de l'authentification sans fil avec ACS](#)

[Échec de l'authentification PEAP avec le serveur ACS](#)

[Informations connexes](#)

[Introduction](#)

Ce document décrit comment configurer l'accès sans fil sécurisé à l'aide des contrôleurs de

réseau local sans fil, du système d'exploitation Microsoft Windows 2003 et du Cisco Secure Access Control Server (ACS) 5.1 par l'intermédiaire du protocole PEAP avec la version 2 du Protocole d'authentification de négociation par défi Microsoft (MS-CHAP).

Remarque : pour plus d'informations sur le déploiement d'un réseau sans fil sécurisé, reportez-vous au [site Web Microsoft Wi-Fi](#) et au [Cisco SAFE Wireless Blueprint](#).

Conditions préalables

Exigences

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

Pour obtenir des informations sur l'installation initiale et la configuration des contrôleurs de la gamme Cisco 5508, reportez-vous au [Guide d'installation des contrôleurs sans fil de la gamme Cisco 5500](#). Pour obtenir des informations sur l'installation et la configuration initiales des contrôleurs de la gamme Cisco 2100, reportez-vous au [Guide de démarrage rapide : Contrôleur LAN sans fil de la gamme Cisco 2100](#).

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.

Windows Server 2003 avec SP1, Enterprise Edition, est utilisé pour configurer l'inscription automatique des certificats d'utilisateur et de station de travail pour l'authentification PEAP. L'inscription automatique et le renouvellement automatique des certificats facilitent le déploiement des certificats et améliorent la sécurité en faisant expirer et en renouvelant automatiquement les certificats.

Composants utilisés

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

- Contrôleur de la gamme Cisco 2106 ou 5508 qui exécute 7.0.98.0
- Protocole de point d'accès léger Cisco 1142 (LWAPP) AP
- Windows 2003 Entreprise avec Internet Information Server (IIS), l'autorité de certification (CA), DHCP et le système de noms de domaine (DNS) installés
- Cisco 1121 Secure Access Control System Appliance (ACS) 5.1
- 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 3750

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](#).

Configurer

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

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 :

Topologie de laboratoire sans fil sécurisée Cisco

Access Point



Client

**Cisco 5508
Controller**



Cisco 3750



**Cisco 1121
ACS 5.1**



**Windows 2003
DC/AD, CA,
DHCP, DNS**

L'objectif principal de ce document est de vous fournir la procédure pas à pas pour implémenter le PEAP sous Unified Wireless Networks avec ACS 5.1 et le serveur d'entreprise Windows 2003. L'accent est mis sur l'inscription automatique du client afin que le client s'inscrive automatiquement et récupère 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, reportez-vous à la mise à [jour WPA2/WPS IE \(Wireless Provisioning Services Information](#)

[Element\) pour Windows XP avec Service Pack 2 .](#)

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

CA (démocratie)

CA est un ordinateur qui exécute Windows Server 2003 avec SP2, Enterprise Edition, et qui remplit les rôles suivants :

- Contrôleur de domaine pour le domaine **demo.local** qui exécute IIS
- Un serveur DNS pour le domaine DNS **demo.local**
- Un serveur DHCP
- Autorité de certification racine d'entreprise pour le domaine **demo.local**

Suivez ces étapes afin de configurer l'autorité de certification pour ces services :

1. [Effectuer 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. [Installez et configurez DHCP.](#)
5. [Installez les services de certificat.](#)
6. [Vérifiez les autorisations d'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 des utilisateurs sans fil.](#)
13. [Ajoutez des ordinateurs clients au groupe d'utilisateurs sans fil.](#)

Installation et configuration de base

Effectuez les étapes suivantes :

1. Installez Windows Server 2003 avec SP2, Enterprise Edition en tant que serveur autonome.
2. Configurez le protocole TCP/IP avec l'adresse IP *10.0.10.10* et le masque de sous-réseau *255.255.255.0*.

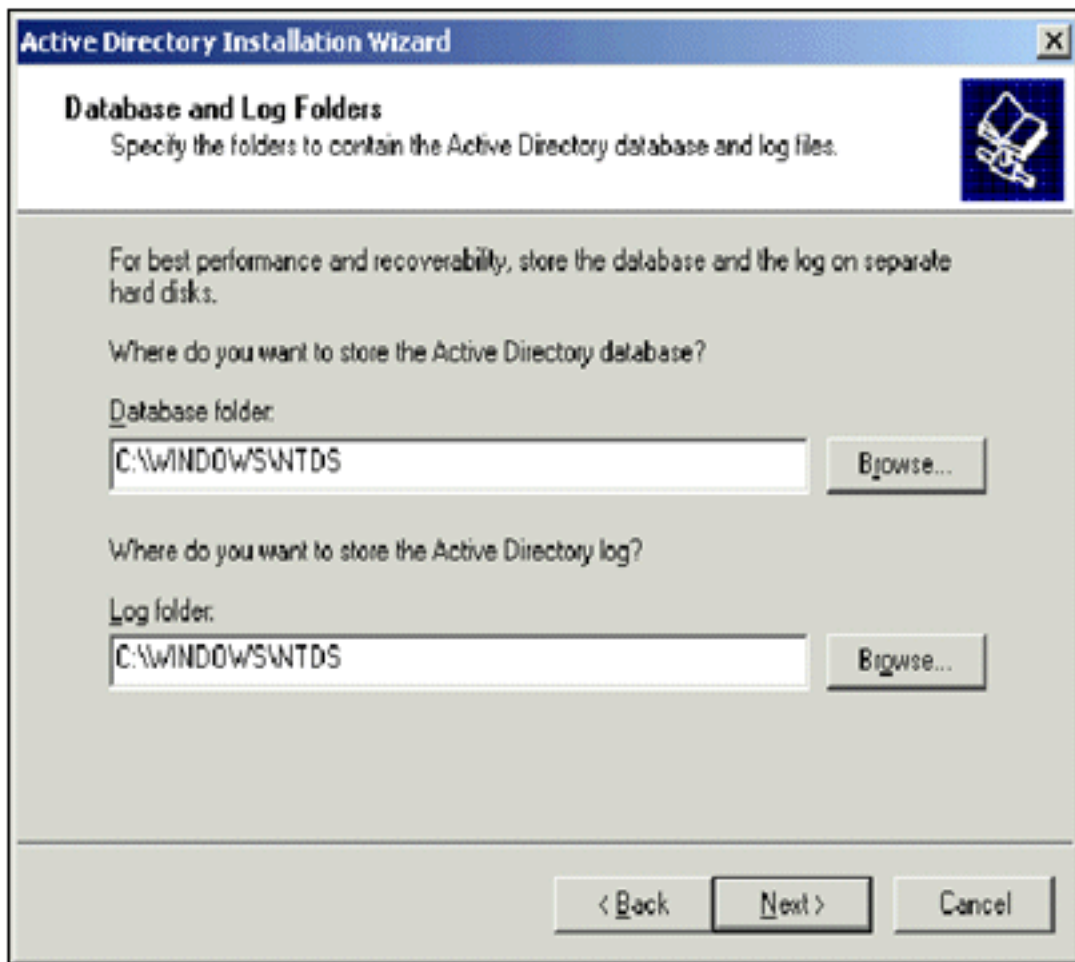
Configurer l'ordinateur en tant que contrôleur de domaine

Effectuez les étapes suivantes :

1. Afin de démarrer l'Assistant Installation d'Active Directory, choisissez **Démarrer > Exécuter**, tapez **dcpromo.exe**, et cliquez sur **OK**.
2. Sur la page Bienvenue dans l'Assistant Installation d'Active Directory, cliquez sur **Suivant**.
3. Sur la page Operating System Compatibility, cliquez sur **Next**.
4. Sur la page Domain Controller Type, sélectionnez **Domain Controller pour un nouveau**

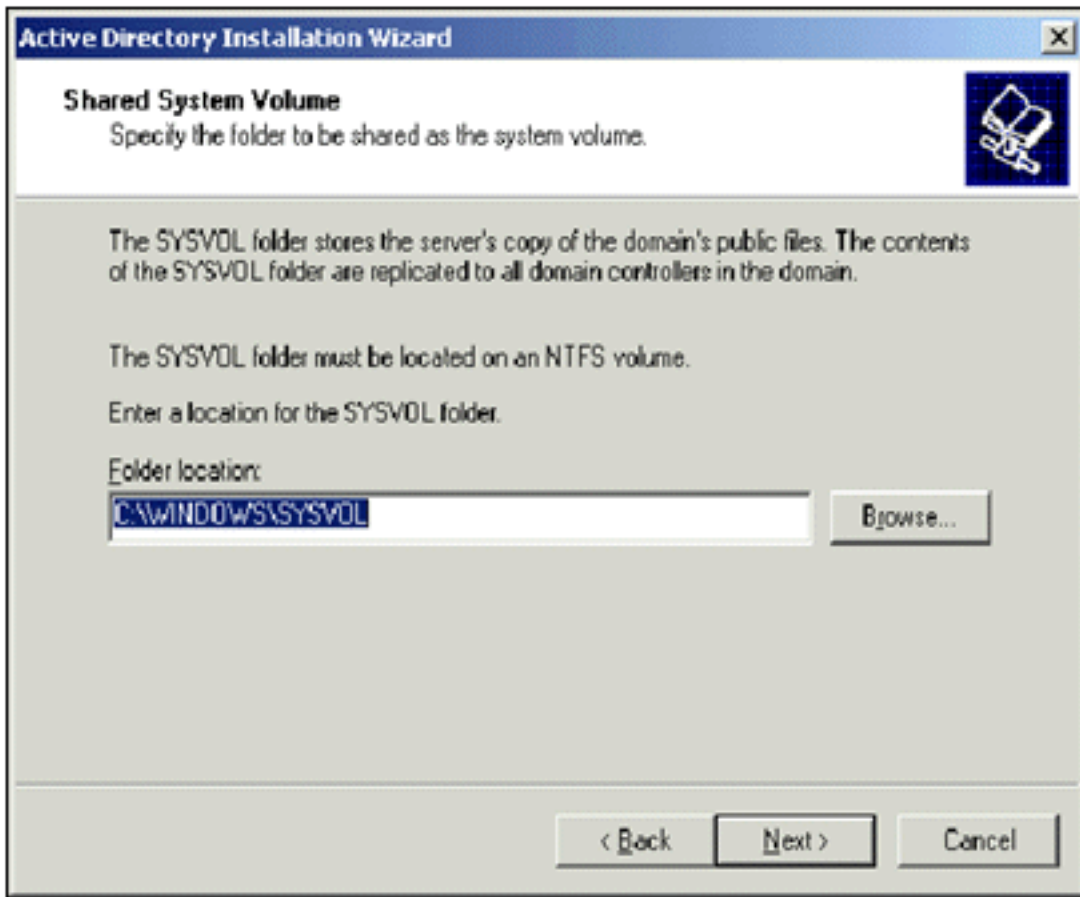
domaine et cliquez sur **Next**.

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 simplement DNS sur cet ordinateur** et cliquez sur **Suivant**.
7. Sur la page New Domain Name, tapez **demo.local** et cliquez sur **Next**.
8. Sur la page Nom de domaine NetBIOS, entrez le nom NetBIOS du domaine en tant que **démo** et cliquez sur **Suivant**.
9. Dans la page Emplacements des bases de données et des dossiers journaux, acceptez les répertoires Base de données et Dossiers journaux par défaut et cliquez sur



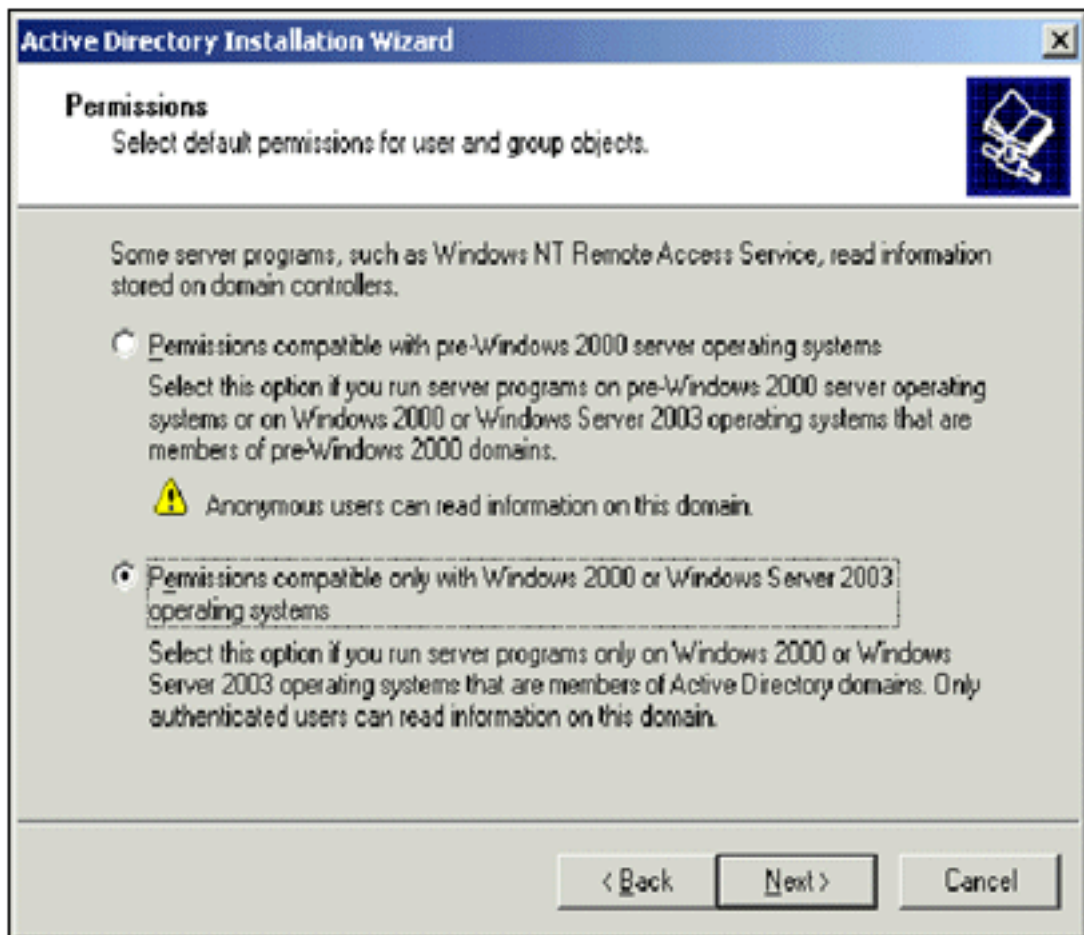
Suivant.

10. Sur la page Shared System Volume, vérifiez que l'emplacement du dossier par défaut est correct et cliquez sur



Next.

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

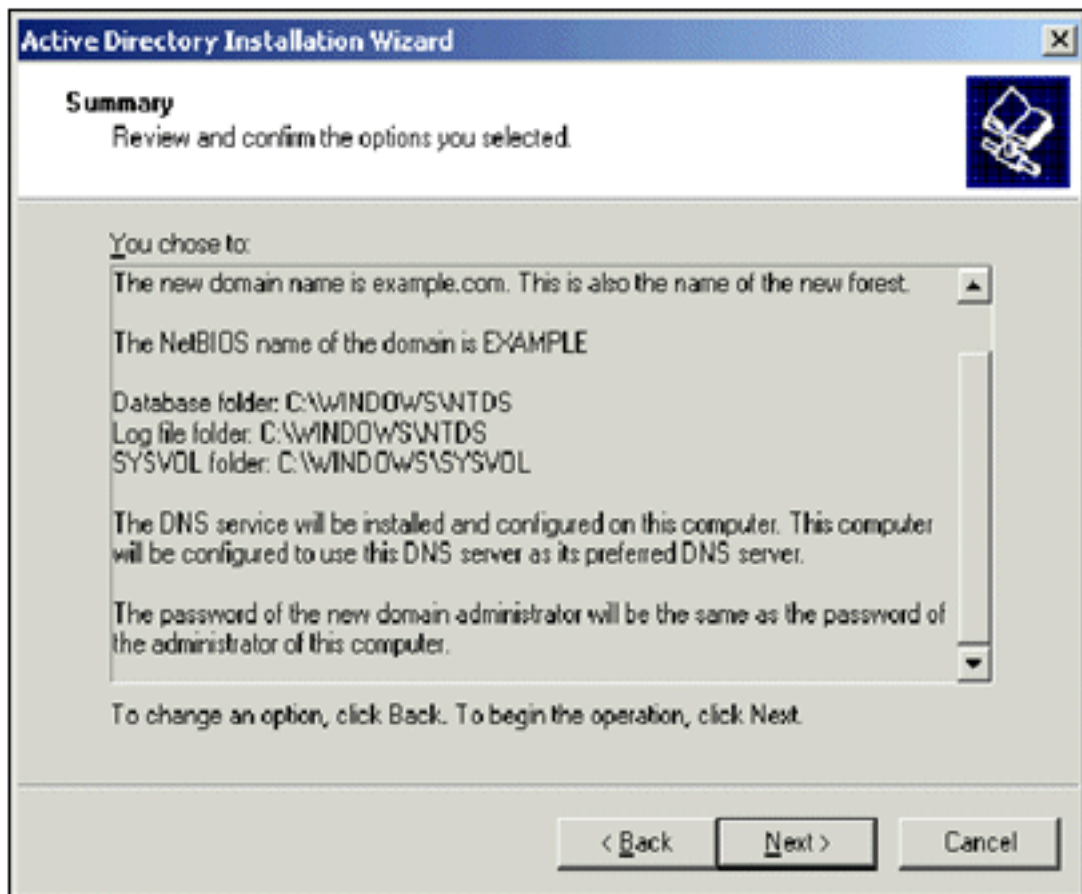


Suivant.

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 sur la page Summary et cliquez sur



Next.

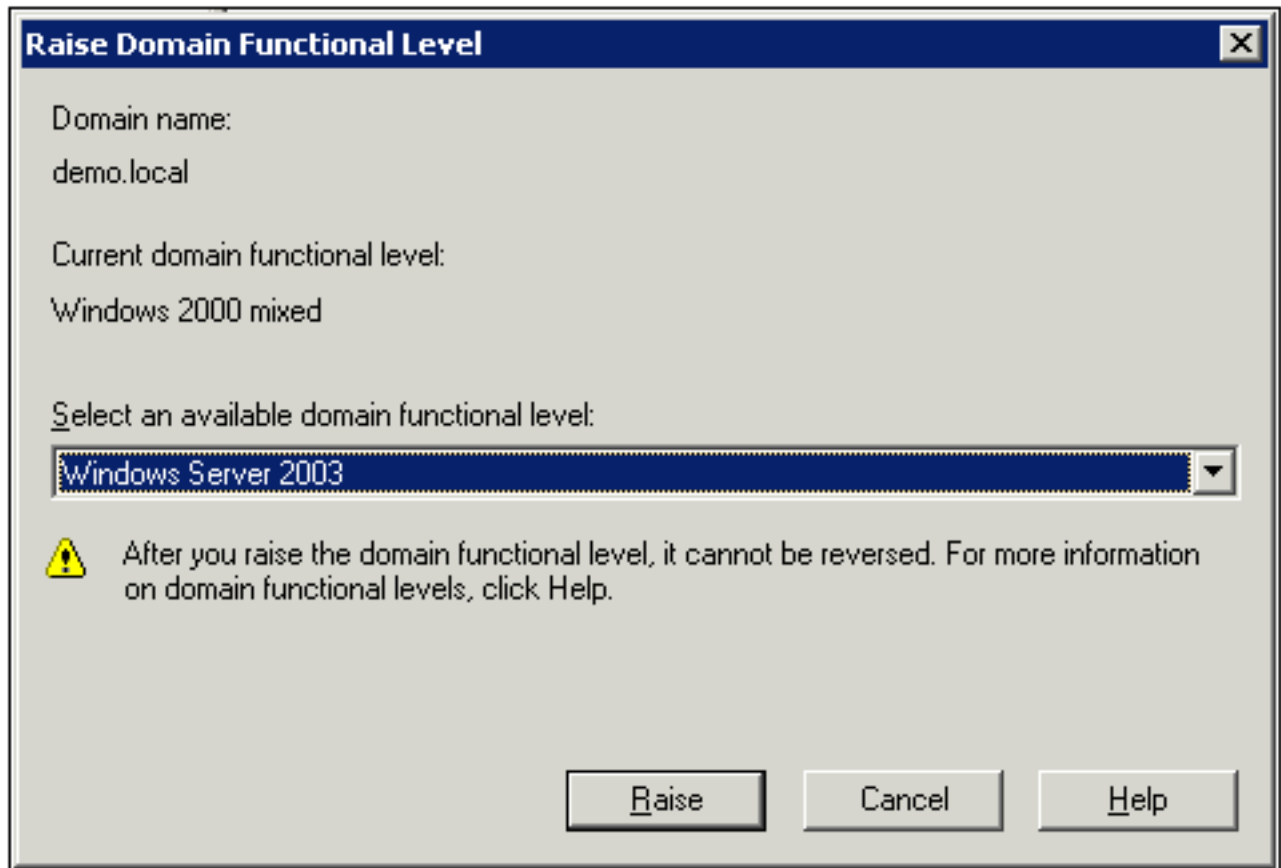
14. Lorsque vous avez terminé l'installation d'Active Directory, cliquez sur **Terminer**.

15. Lorsque vous êtes invité à redémarrer l'ordinateur, cliquez sur **Redémarrer maintenant**.

[Augmenter le niveau fonctionnel du domaine](#)

Effectuez les étapes suivantes :

1. Ouvrez le composant logiciel enfichable Domaines et approbations Active Directory à partir du dossier Outils d'administration (Démarrer > Programmes > Outils d'administration > **Domaines et approbations Active Directory**), puis cliquez avec le bouton droit sur l'ordinateur de domaine **CA.demo.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 **Raise**, cliquez sur **OK**, puis cliquez à nouveau sur **OK**.


[Installation et configuration de DHCP](#)

Effectuez les étapes suivantes :

1. Installez le **protocole DHCP (Dynamic Host Configuration Protocol)** en tant que composant de **service réseau** à l'aide de la fonction **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, **CA.demo.local**.
3. Cliquez sur **Action**, puis sur **Authorize** afin d'autoriser le service DHCP.
4. Dans l'arborescence de la console, cliquez avec le bouton droit sur **CA.demo.local**, puis cliquez sur **Nouvelle étendue**.
5. Sur la page Welcome de l'assistant New Scope, cliquez sur **Next**.
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:

< Back Next > Cancel

7. Cliquez sur **Next** et renseignez ces paramètres : Adresse IP de début - **10.0.20.1** Adresse IP de fin - **10.0.20.200** 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 entrez *10.0.20.1* pour l'adresse IP de début et *10.0.20.100* pour l'adresse IP de fin à exclure. Cliquez ensuite sur **Next**. Cette opération réserve les adresses IP comprises entre *10.0.20.1* et *10.0.20.100*. Ces adresses IP de réserve 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.

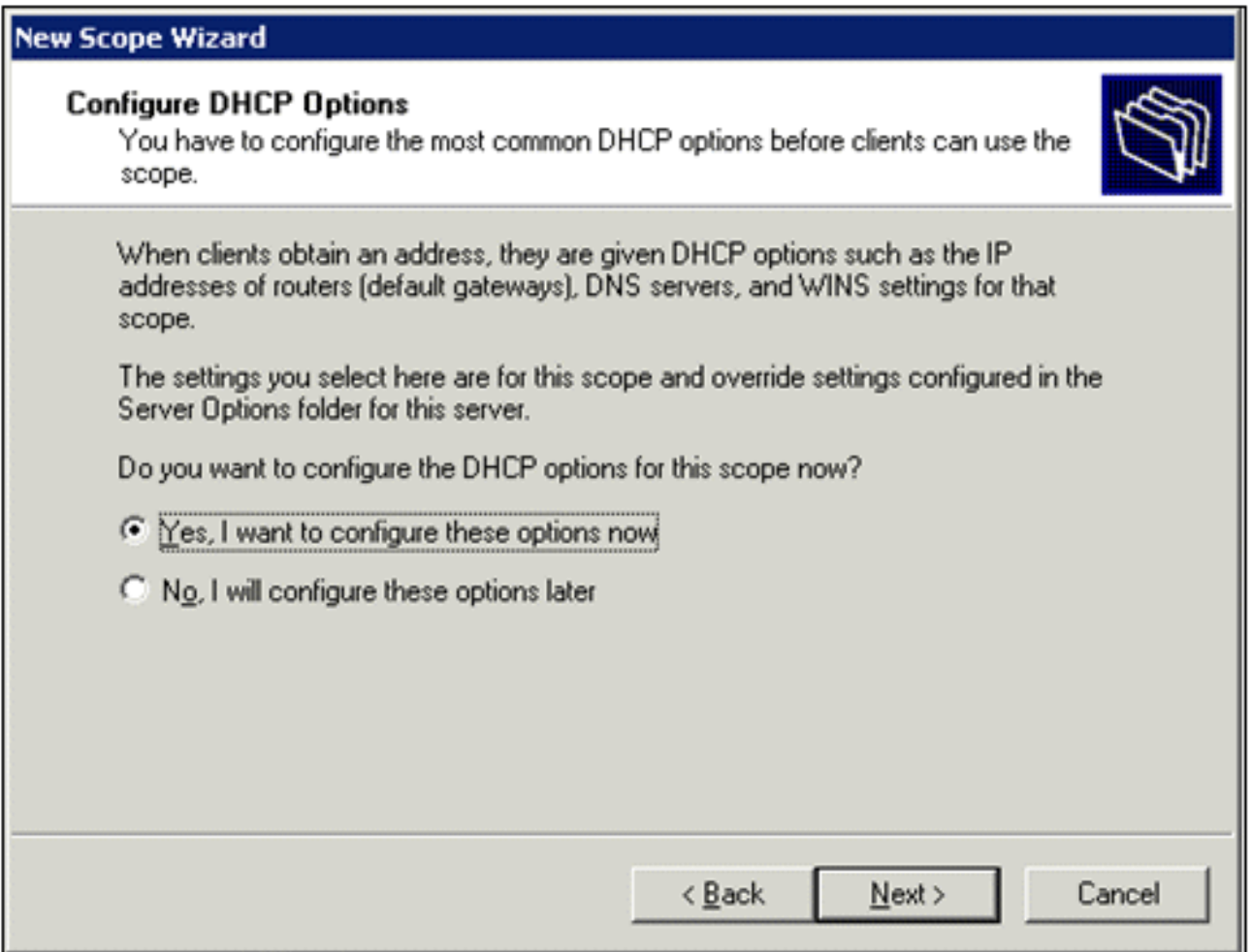
Start IP address: End IP address:

Excluded address range:

<

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


10. Sur la page Configure DHCP Options, choisissez **Yes, I want to configure these options now** et cliquez sur **Next**.



11. Sur la page Router (Default Gateway), ajoutez l'adresse de routeur par défaut *10.0.20.1* et 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:

10 . 0 . 20 . 1	Add
	Remove
	Up
	Down

< Back Next > Cancel

12. Sur la page Domain Name and DNS Servers, tapez *demo.local* dans le champ Parent domain, tapez *10.0.10.10* dans le champ IP address, puis cliquez sur **Add** et cliquez 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.

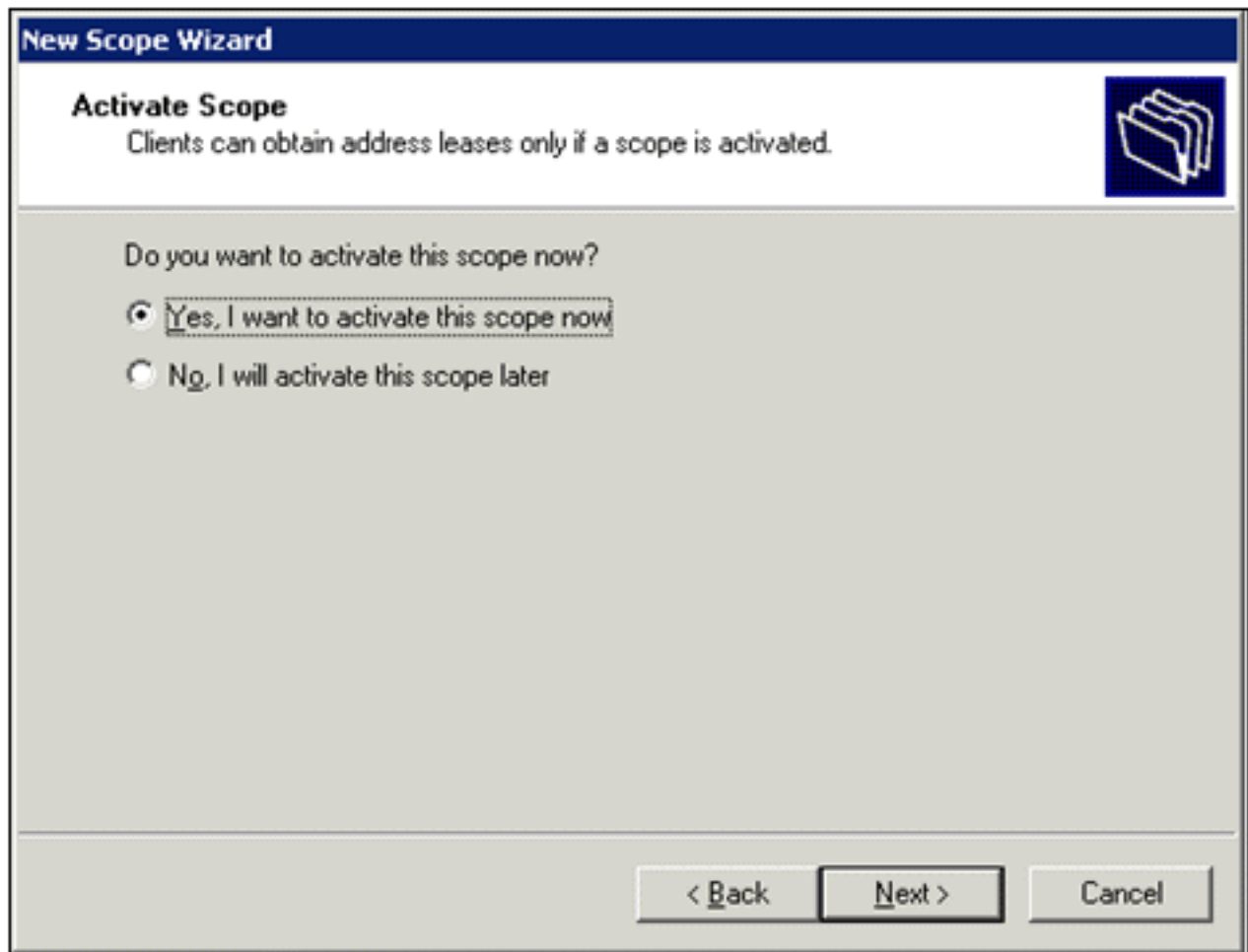
You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

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

Server name:	IP address:	
<input type="text"/>	<input type="text" value=" . . ."/>	<input type="button" value="Add"/>
<input type="button" value="Resolve"/>	<input type="text" value="10.0.10.10"/>	<input type="button" value="Remove"/>
		<input type="button" value="Up"/>
		<input type="button" value="Down"/>

13. Sur la page WINS Servers, cliquez sur **Next**.
14. Sur la page Activate Scope, sélectionnez **Yes, I want to activate this scope now** et cliquez sur **Next**.



15. Lorsque vous avez terminé avec la page Assistant Nouvelle étendue, cliquez sur **Terminer**.

[Installer les services de certificats](#)

Effectuez les étapes suivantes :

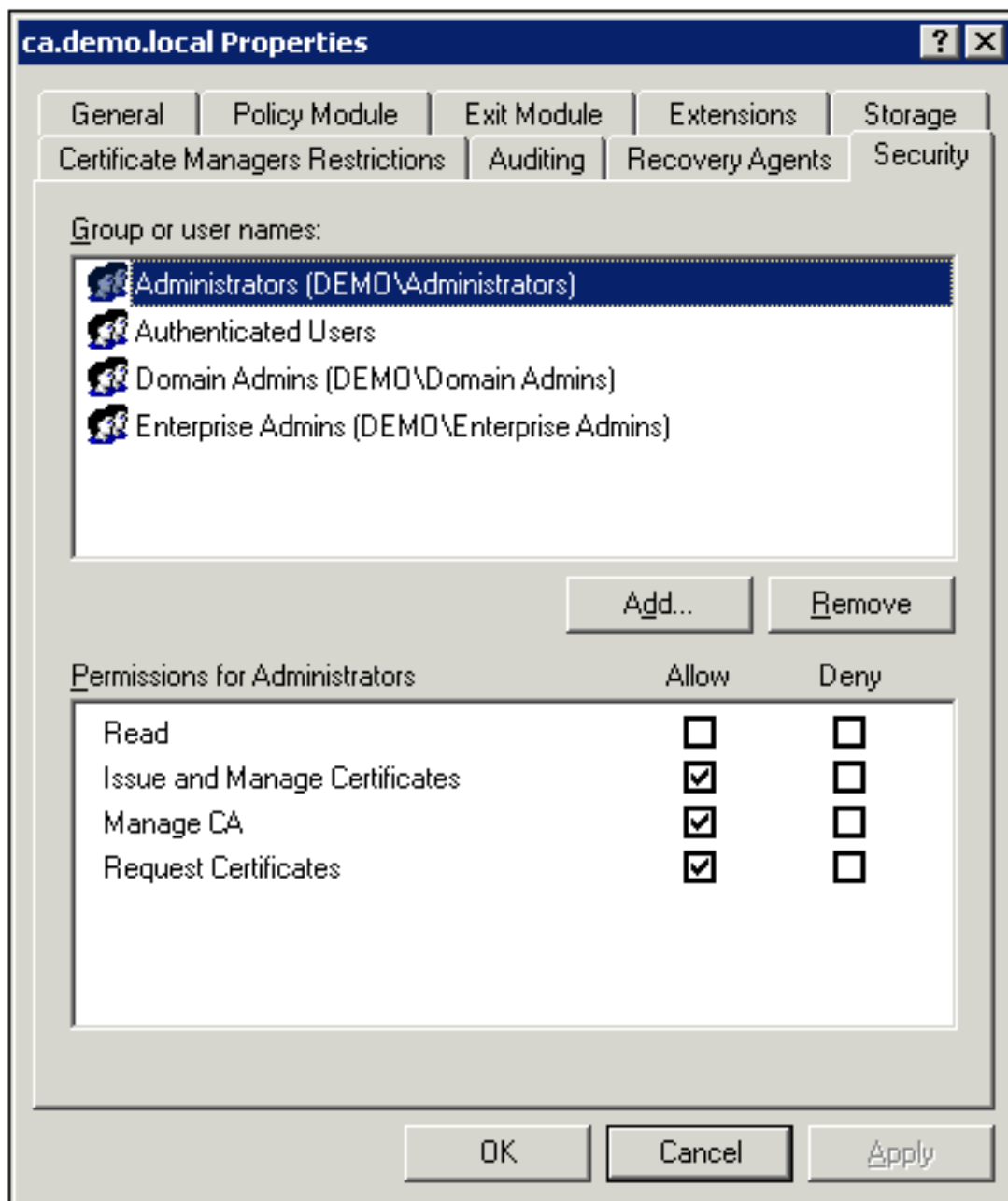
Remarque : IIS doit être installé avant que vous n'installiez les services de certificats et l'utilisateur doit faire partie de l'unité d'organisation d'administration d'entreprise.

1. Dans le Panneau de configuration, ouvrez **Ajout/Suppression de programmes**, puis cliquez sur **Ajouter/Supprimer des composants Windows**.
2. Dans la page Assistant Composants Windows, sélectionnez Services de certificats, puis cliquez sur Suivant.
3. Sur la page Type d'autorité de certification, choisissez Autorité de certification racine d'entreprise et cliquez sur Suivant.
4. Dans la page Informations d'identification de l'autorité de certification, tapez *democracy* dans la zone Nom commun pour cette autorité de certification. Vous pouvez également saisir les autres détails facultatifs. Cliquez ensuite sur **Next** et acceptez les valeurs par défaut sur la page Certificate Database Settings.
5. Cliquez sur **Next** (Suivant). Une fois l'installation terminée, cliquez sur **Finish**.
6. Cliquez sur **OK** après avoir lu le message d'avertissement relatif à l'installation d'IIS.

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

Effectuez les étapes suivantes :

1. Choisissez **Démarrer > Outils d'administration > Autorité de certification**.
2. Cliquez avec le bouton droit sur l'**autorité de certification démocrate**, puis cliquez sur **Propriétés**.
3. Dans l'onglet Sécurité, cliquez sur **Administrateurs** dans la liste Noms de groupe ou d'utilisateur.
4. Dans la liste Autorisations pour les administrateurs, vérifiez que ces options sont définies sur **Autoriser** : Émettre et gérer des certificats, Gérer CA, Demander des certificats. Si l'une de ces options est définie sur Refuser ou n'est pas sélectionnée, définissez les autorisations sur



Autoriser.

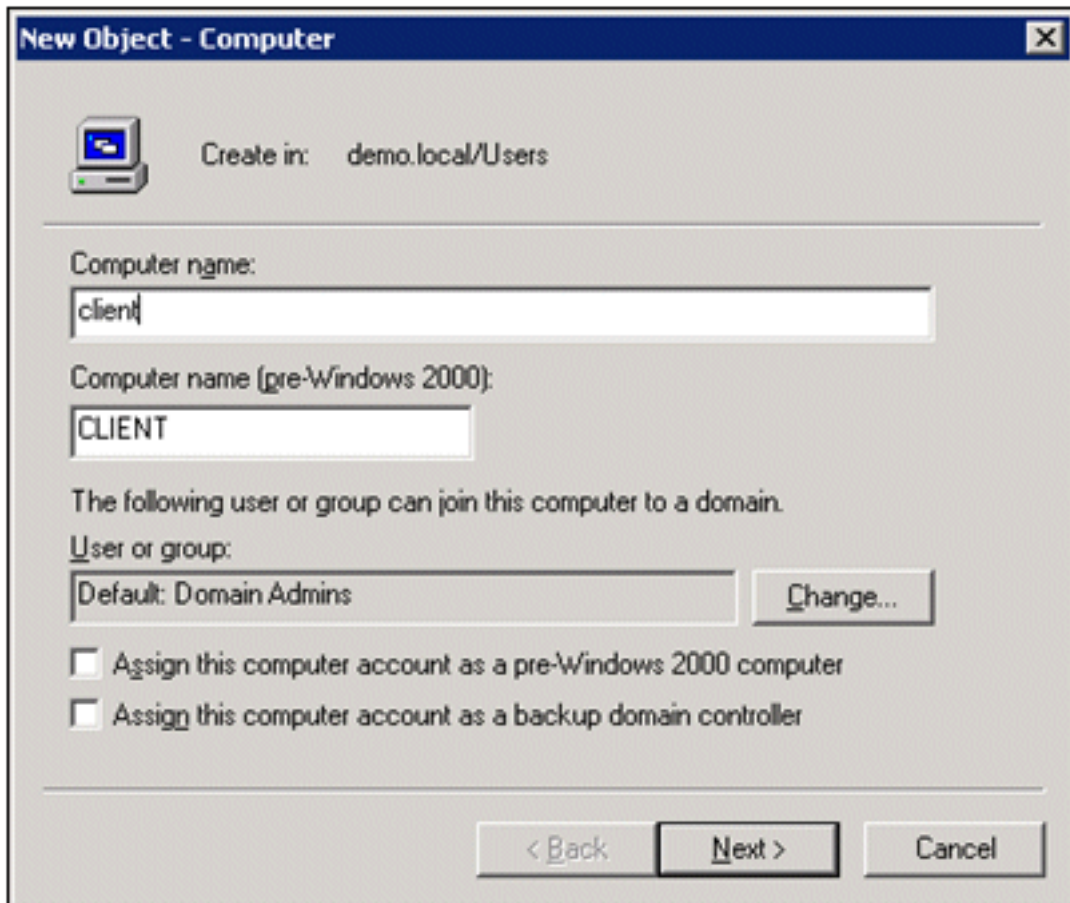
5. Cliquez sur **OK** pour fermer la boîte de dialogue Propriétés de l'autorité de certification démocratique, puis fermez Autorité de certification.

[Ajouter des ordinateurs au domaine](#)

Effectuez les étapes suivantes :

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 **demo.local**.
3. Cliquez avec le bouton droit sur **Ordinateurs**, cliquez sur **Nouveau**, puis cliquez 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



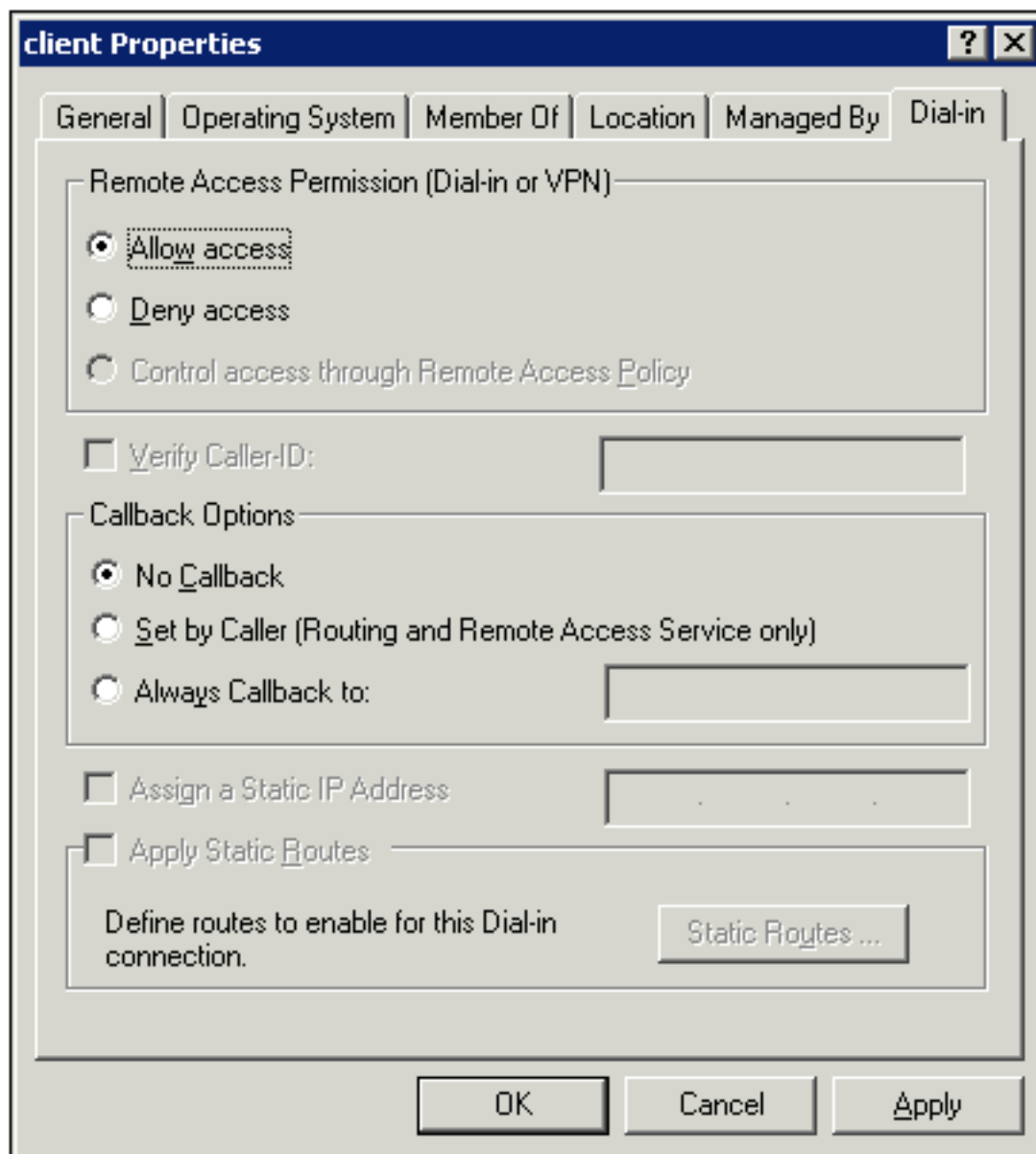
Client.

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.

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

Effectuez les étapes suivantes :

1. Dans l'arborescence de la console Utilisateurs et ordinateurs Active Directory, cliquez sur le dossier **Ordinateurs** et cliquez avec le bouton droit sur l'ordinateur auquel vous souhaitez attribuer un accès sans fil. Cet exemple montre la procédure avec l'ordinateur **Client** que vous avez ajoutée à l'étape 7. Cliquez sur **Properties**, puis accédez à l'onglet **Dial-in**.
2. Dans Autorisation d'accès à distance, sélectionnez **Autoriser l'accès** et cliquez sur




OK.

[Ajouter des utilisateurs au domaine](#)

Effectuez les étapes suivantes :

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 champ First name et *wirelessuser* dans le champ User logon name. Cliquez sur **Next** (Suivant).

New Object - User [X]

 Create in: demo.local/Users

First name: wirelessuser Initials:

Last name:

Full name: wirelessuser

User logon name:
 @demo.local

User logon name (pre-Windows 2000):
 wirelessuser

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

Create in: demo.local/Users

Password: [masked]

Confirm password: [masked]

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back Next > Cancel

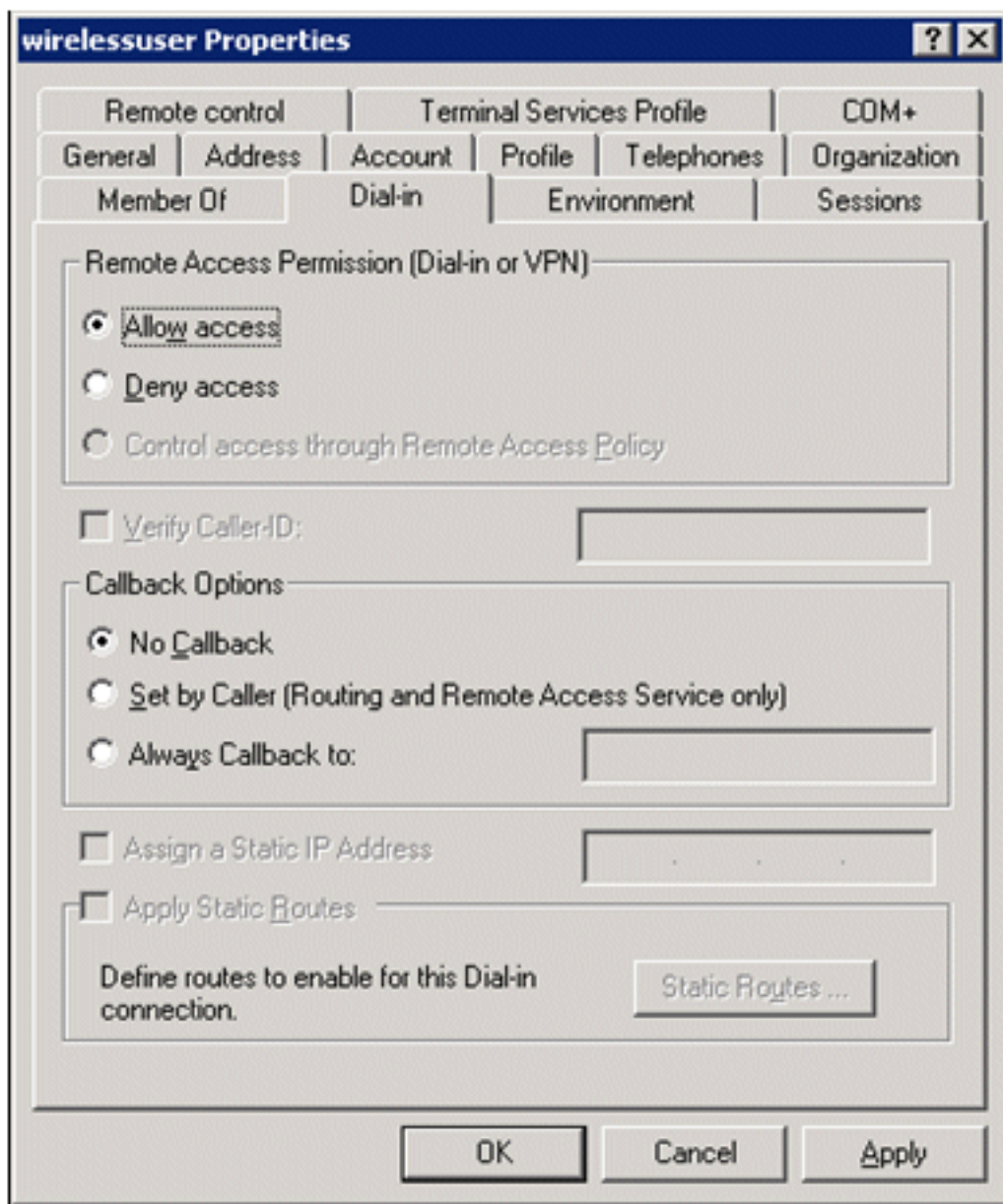
Next.

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

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

Effectuez les étapes suivantes :

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 **Properties**, puis accédez à l'onglet **Dial-in**.
2. Dans Autorisation d'accès à distance, sélectionnez **Autoriser l'accès** et cliquez sur

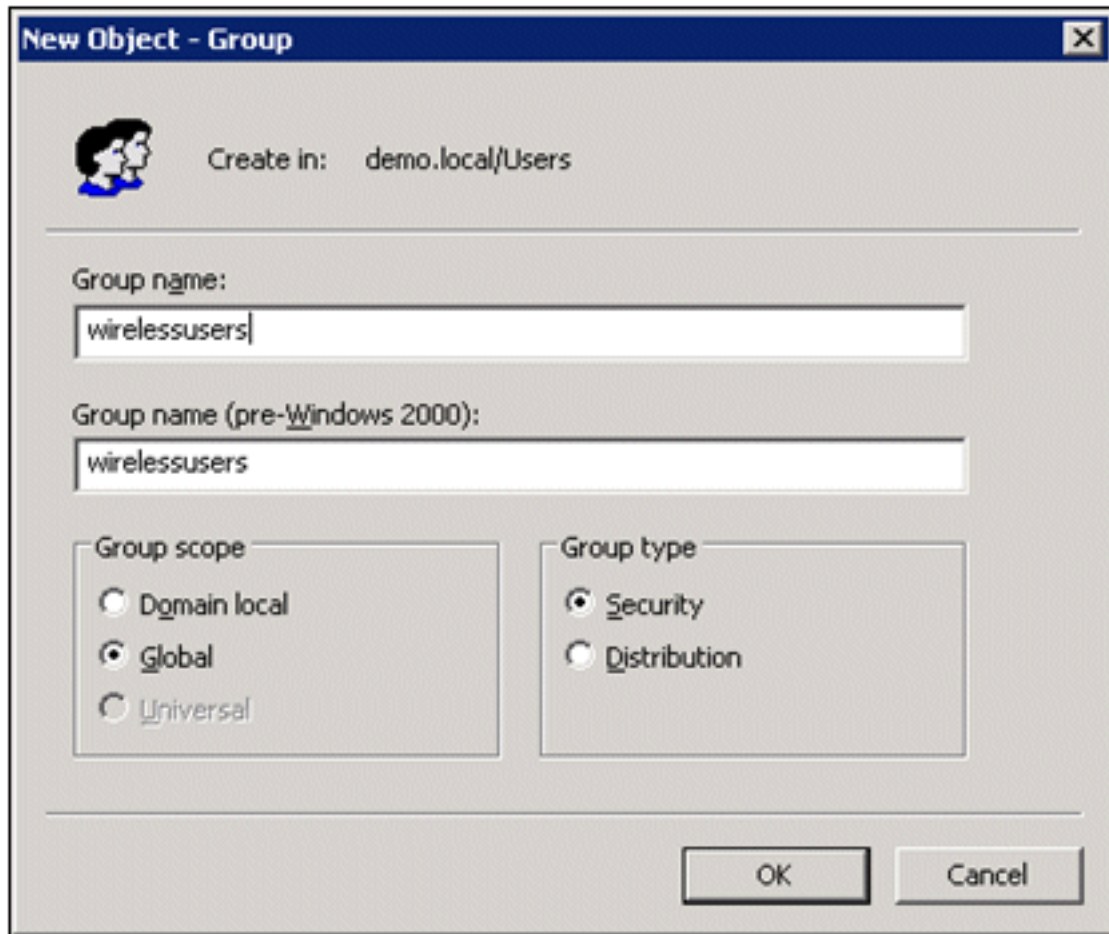


OK.

[Ajouter des groupes au domaine](#)

Effectuez les étapes suivantes :

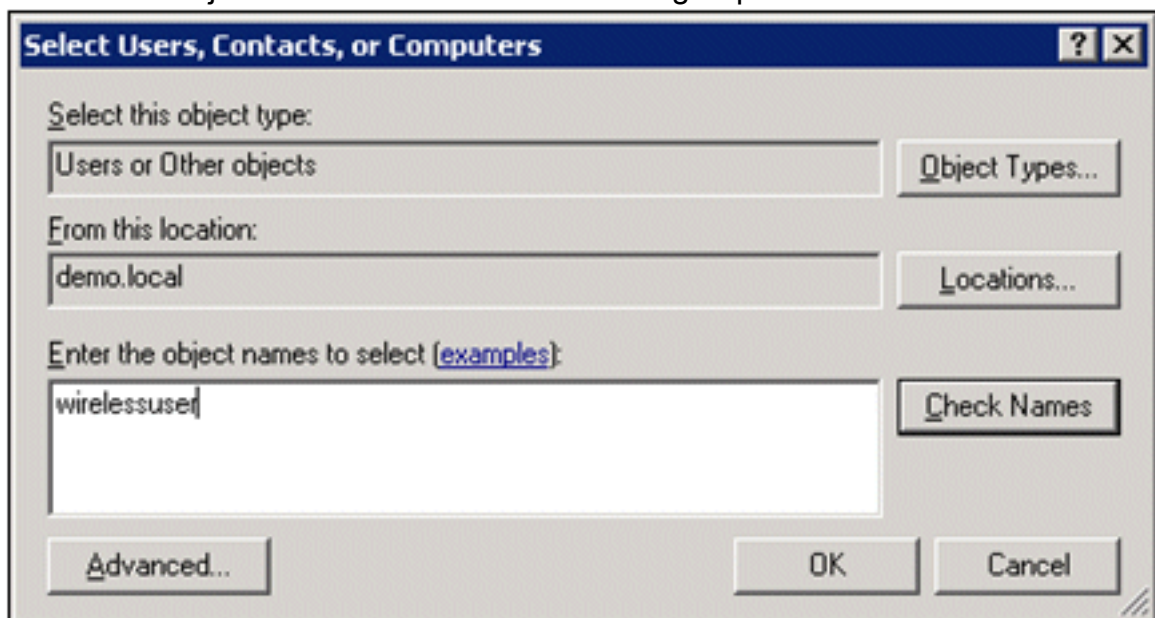
1. Dans l'arborescence de la console Utilisateurs et ordinateurs Active Directory, cliquez avec le bouton droit sur **Utilisateurs**, cliquez sur **Nouveau**, puis cliquez sur **Groupe**.
2. Dans la boîte de dialogue Nouvel objet - Groupe, tapez le nom du groupe dans le champ Nom du groupe et cliquez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



[Ajouter des utilisateurs au groupe d'utilisateurs sans fil](#)

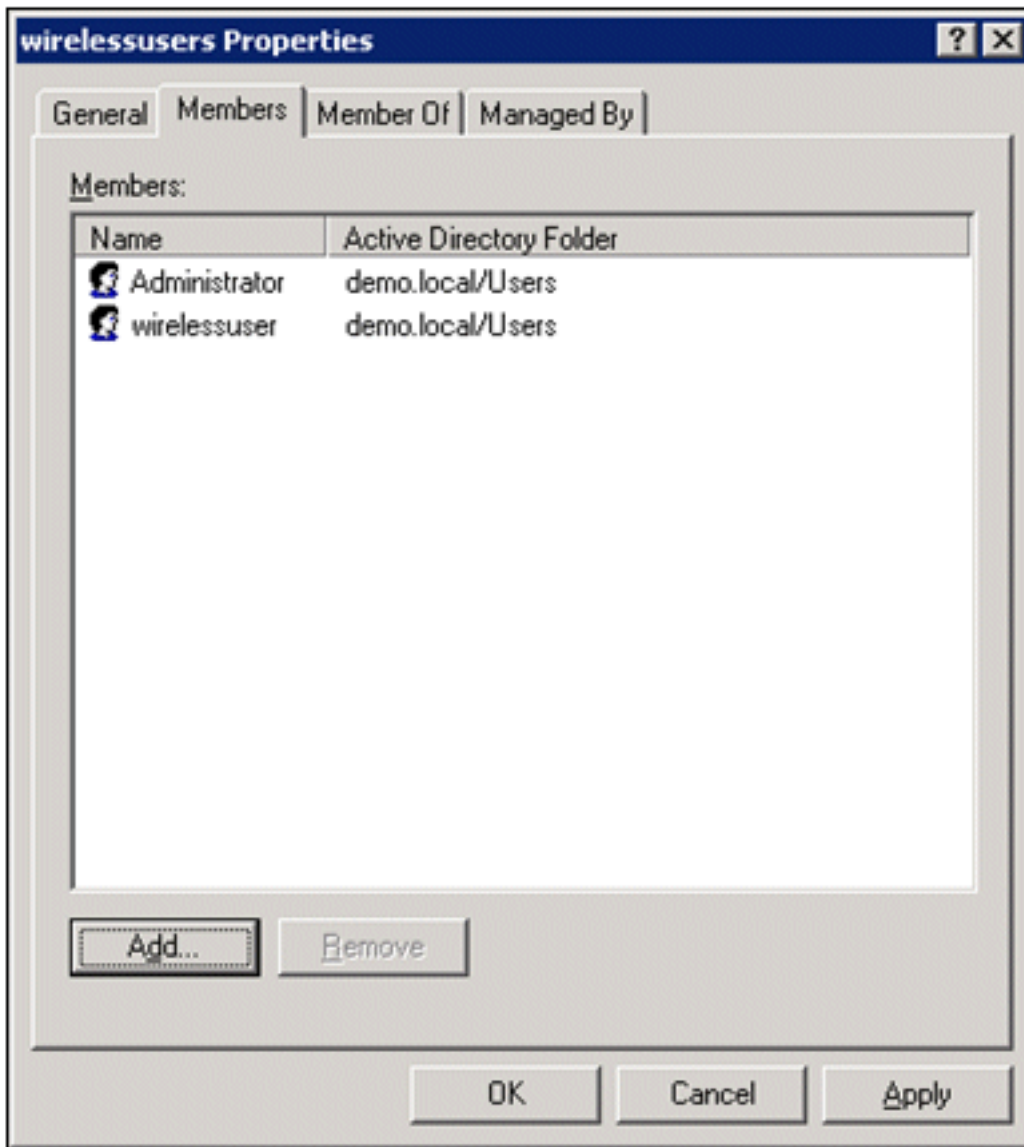
Effectuez les étapes suivantes :

1. Dans le volet d'informations d'Utilisateurs et ordinateurs Active Directory, double-cliquez sur le groupe *UtilisateursSans fil*.
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 que vous souhaitez ajouter au groupe. Cet exemple montre comment ajouter l'utilisateur *wirelesuser* au groupe. Click



OK.

4. Dans la boîte de dialogue Plusieurs noms trouvés, cliquez sur **OK**. Le compte utilisateur sans fil est ajouté au groupe d'utilisateurs sans



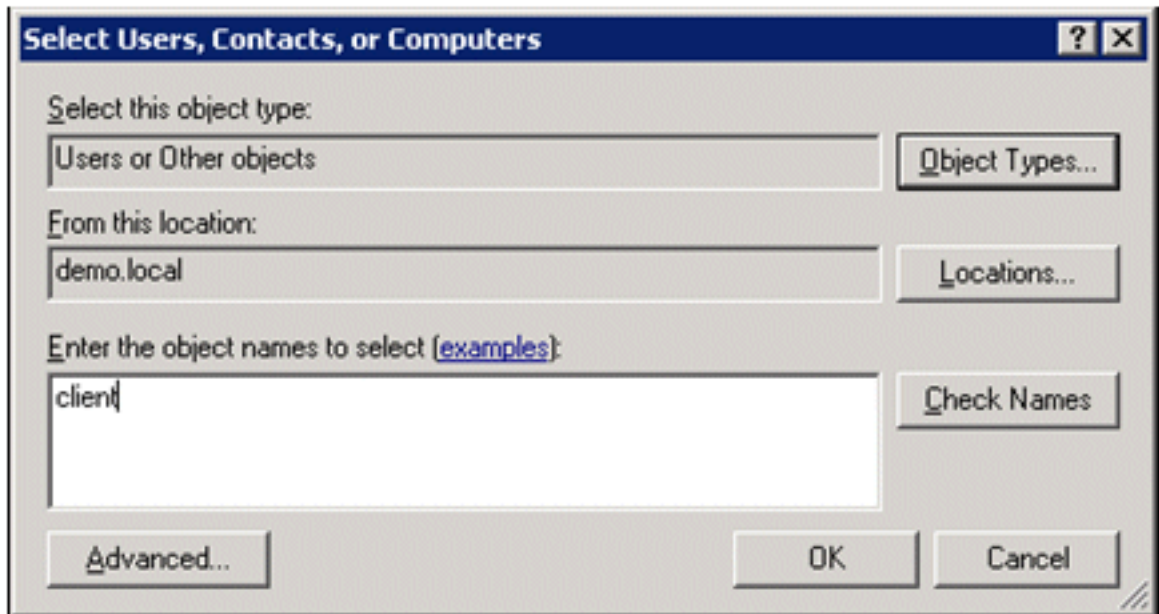
fil.

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

[Ajout d'ordinateurs clients au groupe d'utilisateurs sans fil](#)

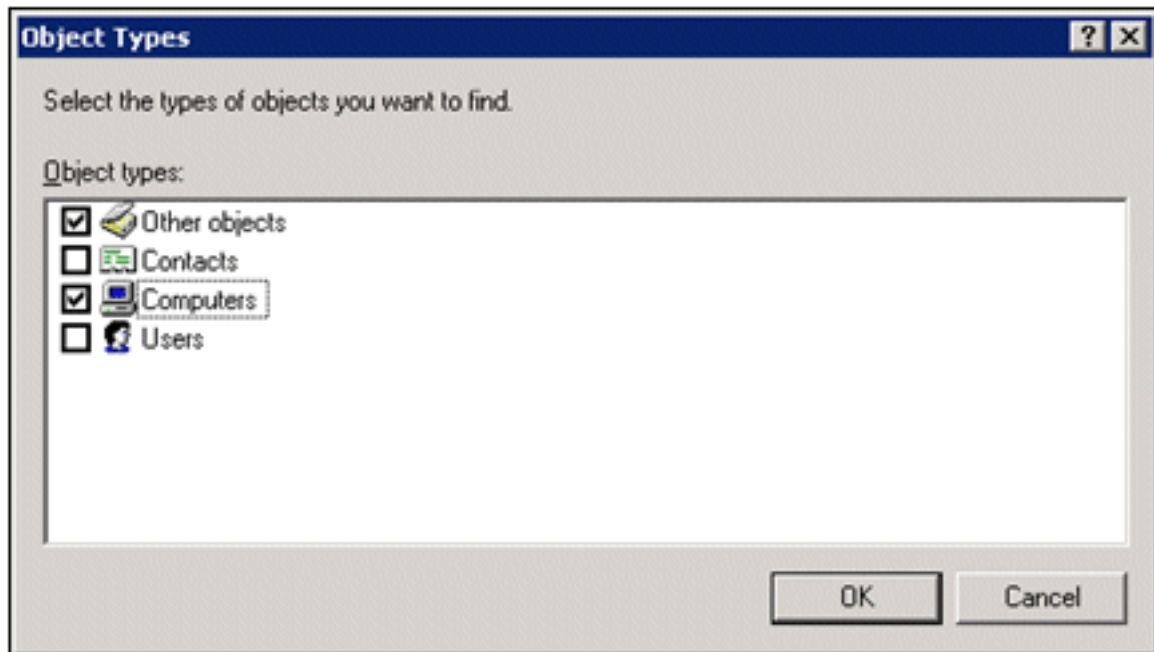
Effectuez les étapes suivantes :

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 que vous souhaitez ajouter au groupe. Cet exemple montre comment ajouter l'ordinateur nommé *client* au

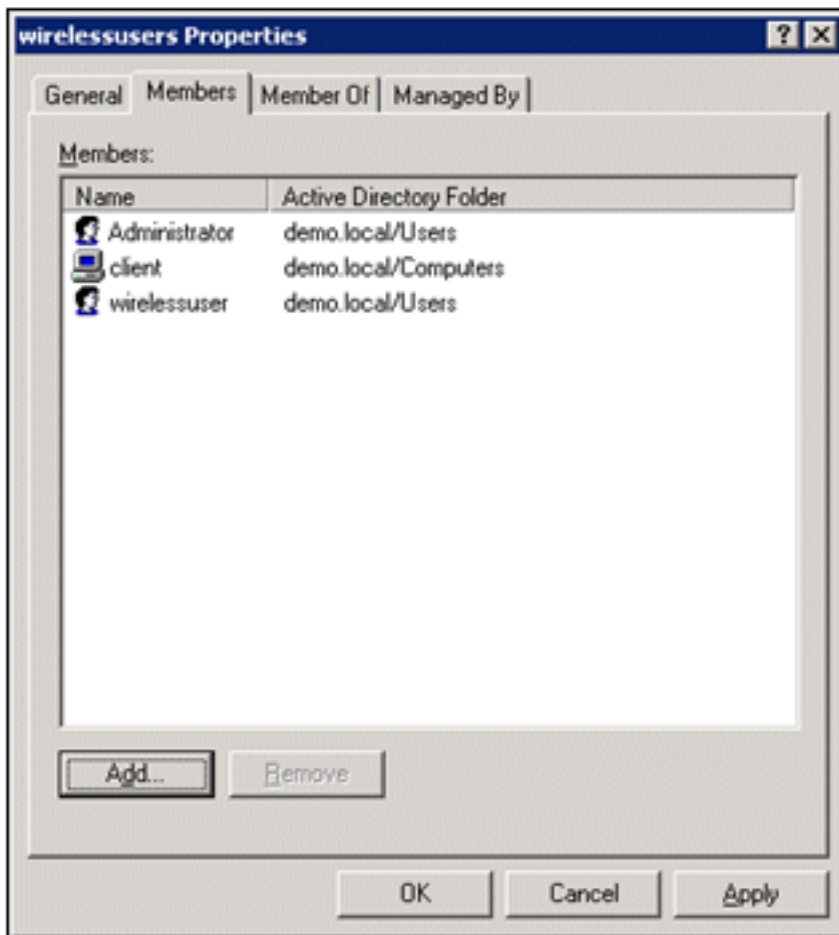


groupe.

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



4. Cliquez deux fois sur **OK**. Le compte d'ordinateur CLIENT est ajouté au groupe d'utilisateurs



sans fil.

5. Répétez la procédure pour ajouter d'autres ordinateurs au groupe.

[Cisco 1121 Secure ACS 5.1](#)

[Installation à l'aide de l'appliance de la gamme CSACS-1121](#)

Le périphérique CSACS-1121 est préinstallé avec le logiciel ACS 5.1. Cette section vous donne une vue d'ensemble du processus d'installation et des tâches que vous devez effectuer avant d'installer ACS.

1. Connectez le CSACS-1121 au réseau et à la console du matériel. Reportez-vous au [Chapitre 4, Connexion des câbles](#).
2. Mettez le périphérique CSACS-1121 sous tension. Reportez-vous au [chapitre 4, « Mise sous tension de l'appliance de la gamme CSACS-1121 »](#).
3. Exécutez la commande **setup** à l'invite CLI pour configurer les paramètres initiaux du serveur ACS. Voir Exécution du programme d'installation.

[Installation du serveur ACS](#)

Cette section décrit la procédure d'installation du serveur ACS sur le périphérique de la gamme CSACS-1121.

- [Exécuter le programme d'installation](#)
- [Vérification du processus d'installation](#)
- [Tâches post-installation](#)

Pour obtenir des informations détaillées sur l'installation du serveur Cisco Secure ACS, reportez-vous au [Guide d'installation et de mise à niveau de Cisco Secure Access Control System 5.1](#).

Configuration du contrôleur Cisco WLC5508

Créer la configuration nécessaire pour WPAv2/WPA

Effectuez les étapes suivantes :

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. Accédez à <https://10.0.1.10> afin de vous connecter au



contrôleur.

2. Cliquez sur **Connexion**.
3. Connectez-vous avec l'utilisateur par défaut *admin* et le mot de passe par défaut *admin*.
4. Créez une interface pour le mappage VLAN dans le menu **Controller**.
5. Cliquez sur **Interfaces**.
6. Cliquez sur **New**.
7. Dans le champ Nom de l'interface, saisissez *Employé*. (Ce champ peut contenir n'importe quelle valeur.)
8. Dans le champ VLAN ID, saisissez *20*. (Ce champ peut être n'importe quel VLAN transporté dans le réseau.)
9. Cliquez sur **Apply**.
10. Configurez les informations comme le montre la fenêtre Interfaces > Edit : Adresse IP de l'interface - **10.0.20.2** Masque réseau - **255.255.255.0** Passerelle - **10.0.10.1** DHCP principal : **10.0.10.10**

Save Configuration | Ping | Logout | Refresh

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Controller

General
Inventory
Interfaces
Multicast
Network Routes
Internal DHCP Server
Mobility Management
Ports
NTP
CDP
Advanced

Interfaces > Edit < Back Apply

General Information

Interface Name employee
MAC Address 00:24:97:69:4d:e0

Configuration

Guest Lan
Quarantine
Quarantine Vlan Id

Physical Information

Port Number
Backup Port
Active Port 0
Enable Dynamic AP Management

Interface Address

VLAN Identifier
IP Address
Netmask
Gateway

DHCP Information

Primary DHCP Server
Secondary DHCP Server

Access Control List

ACL Name

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 l'onglet **WLANs**.
13. Choisissez **Create New**, puis cliquez sur **Go**.
14. Saisissez un nom de profil et, dans le champ WLAN SSID, saisissez *Employee*.

Save Configuration | Ping | Logout | Refresh

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

WLANs

WLANs > New < Back Apply

Type

Profile Name

SSID

ID

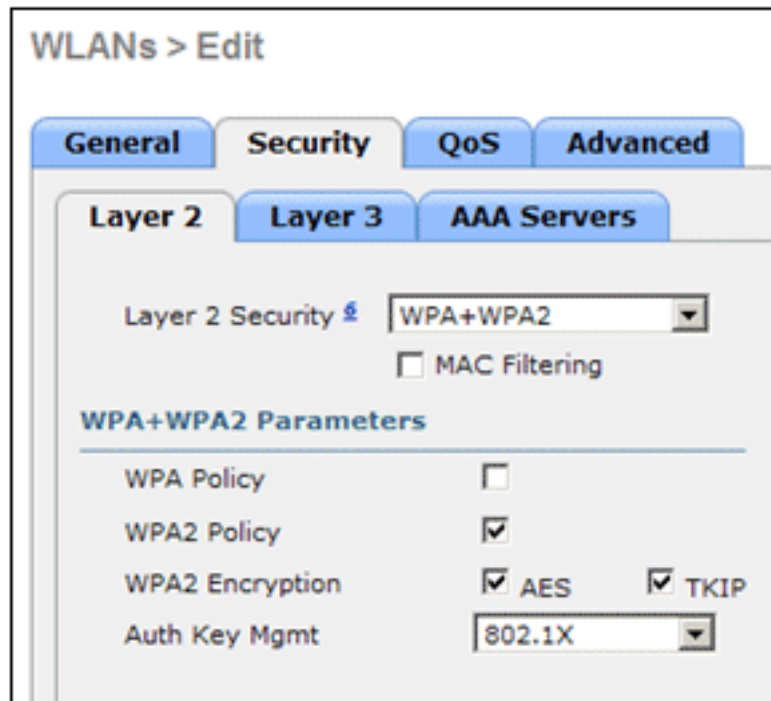
15. Choisissez un ID pour le WLAN, et cliquez sur **Apply**.

16. Configurez les informations pour ce WLAN lorsque la fenêtre WLANs > Edit s'affiche. **Remarque** : WPAv2 est la méthode de cryptage de couche 2 choisie pour ces travaux pratiques. Afin de permettre à WPA avec des clients 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.
17. Dans l'écran WLANs > Edit, cliquez sur l'onglet **General**.
18. Assurez-vous que la case État est cochée pour **Activé** et que l'**interface** appropriée (employé) est sélectionnée. Assurez-vous également de cocher la case **Enabled** pour Broadcast SSID.

The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The main content area is titled 'WLANs > Edit' and has tabs for 'General', 'Security', 'QoS', and 'Advanced'. The 'General' tab is active, showing the following configuration:

Profile Name	Employee
Type	WLAN
SSID	Employee
Status	<input type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface	employee
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

19. Cliquez sur l'onglet **Security**.
20. Sous le sous-menu Layer 2, cochez la case **WPA + WPA2** pour la sécurité de couche 2. Pour le cryptage WPA2, cochez **AES + TKIP** afin d'autoriser les clients TKIP.
21. Sélectionnez **802.1x** comme méthode



d'authentification.

22. Ignorez le sous-menu de couche 3, car il n'est pas obligatoire. Une fois le serveur RADIUS configuré, le serveur approprié peut être choisi dans le menu Authentication.
23. Les onglets **QoS** et **Advanced** peuvent être conservés par défaut, sauf si des configurations spéciales sont requises.
24. Cliquez sur le menu **Security** pour ajouter le serveur RADIUS.
25. Sous le sous-menu RADIUS, cliquez sur **Authentication**. Cliquez ensuite sur **New**.
26. Ajoutez l'adresse IP du serveur RADIUS (10.0.10.20) qui est le serveur ACS configuré précédemment.
27. Assurez-vous que la clé partagée correspond au client AAA configuré dans le serveur ACS. Assurez-vous que la case **Network User** est cochée et cliquez sur **Apply**.

28. La configuration de base est maintenant terminée et vous pouvez commencer à tester PEAP.

Authentification PEAP

PEAP avec MS-CHAP version 2 nécessite des certificats sur les serveurs ACS mais pas sur les clients sans fil. L'inscription automatique des certificats d'ordinateur pour les serveurs ACS peut être utilisée pour simplifier un déploiement.

Afin de configurer le serveur AC pour fournir l'inscription automatique pour les certificats d'ordinateur et d'utilisateur, complétez les procédures dans cette section.

Remarque : Microsoft a modifié le modèle de serveur Web avec la version de l'autorité de certification Windows 2003 Enterprise afin que les clés ne soient plus exportables et que l'option soit grisée. Il n'existe aucun autre modèle de certificat fourni avec les services de certificat qui sont destinés à l'authentification du serveur et qui permettent de marquer les clés comme étant exportables et qui sont disponibles dans la liste déroulante. Vous devez donc créer un nouveau modèle pour ce faire.

Remarque : Windows 2000 permet l'exportation de clés et ces procédures ne doivent pas être suivies si vous utilisez Windows 2000.

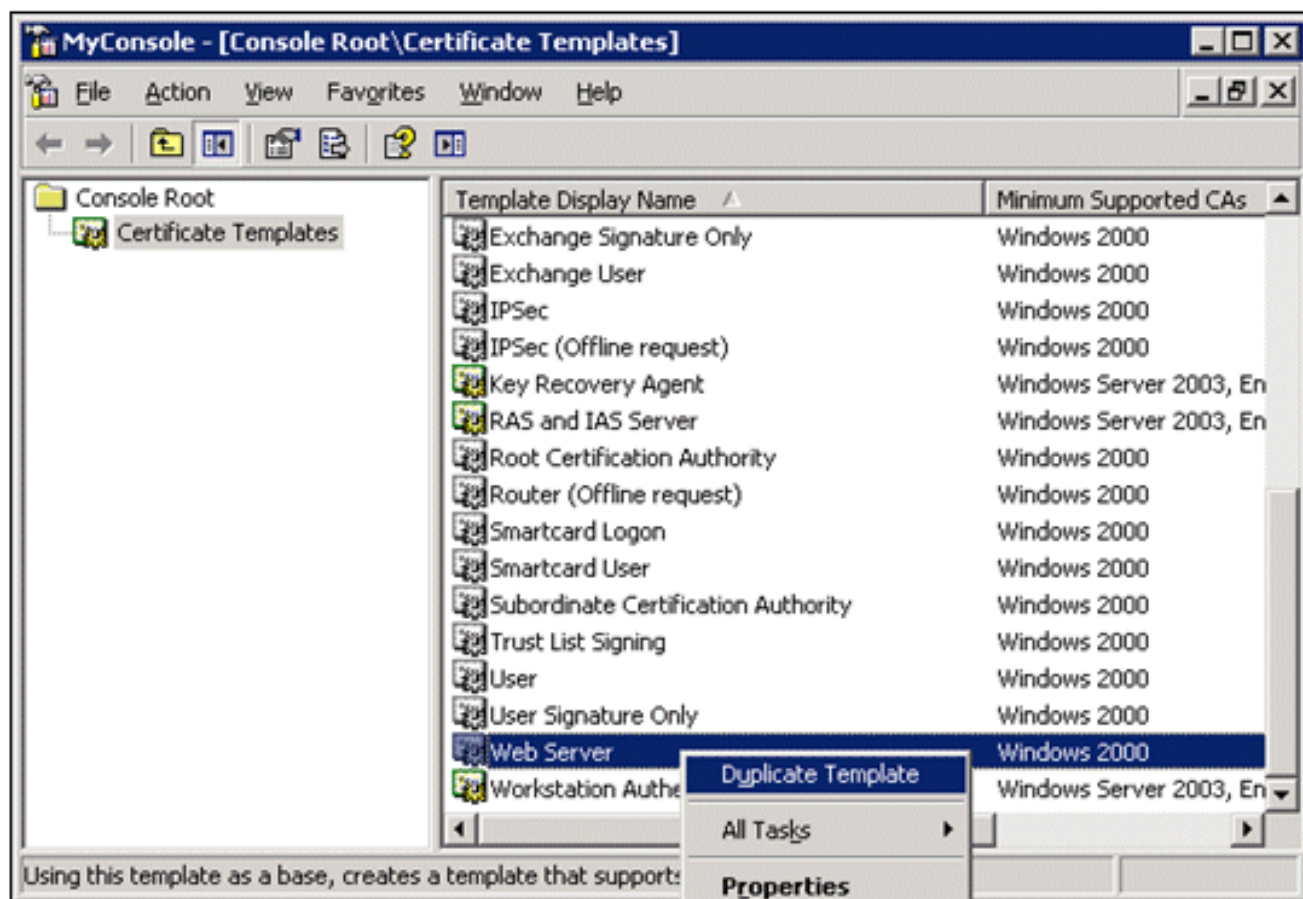
Installation du composant logiciel enfichable Modèles de certificats

Effectuez les étapes suivantes :

1. Choisissez **Démarrer > Exécuter**, entrez *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 cliquez sur **OK**.
4. Dans l'arborescence de la console, cliquez sur **Modèles de certificats**. Tous les modèles de certificats apparaissent dans le volet Détails.
5. Afin de contourner les étapes 2 à 4, entrez *certtmpl.msc* qui ouvre le composant logiciel enfichable Modèles de certificats.



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

Effectuez les étapes suivantes :

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 **Dupliquer le**

Properties of New Template [?] [X]

Issuance Requirements | Superseded Templates | Extensions | Security

General | **Request Handling** | Subject Name

Template display name:

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:

Validity period: years weeks

Renewal period: weeks

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

OK Cancel Apply

modèle.

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

Properties of New Template [?] [X]

Issuance Requirements | Superseded Templates | Extensions | Security

General | **Request Handling** | Subject Name

Template display name:

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:

Validity period: years weeks

Renewal period: weeks

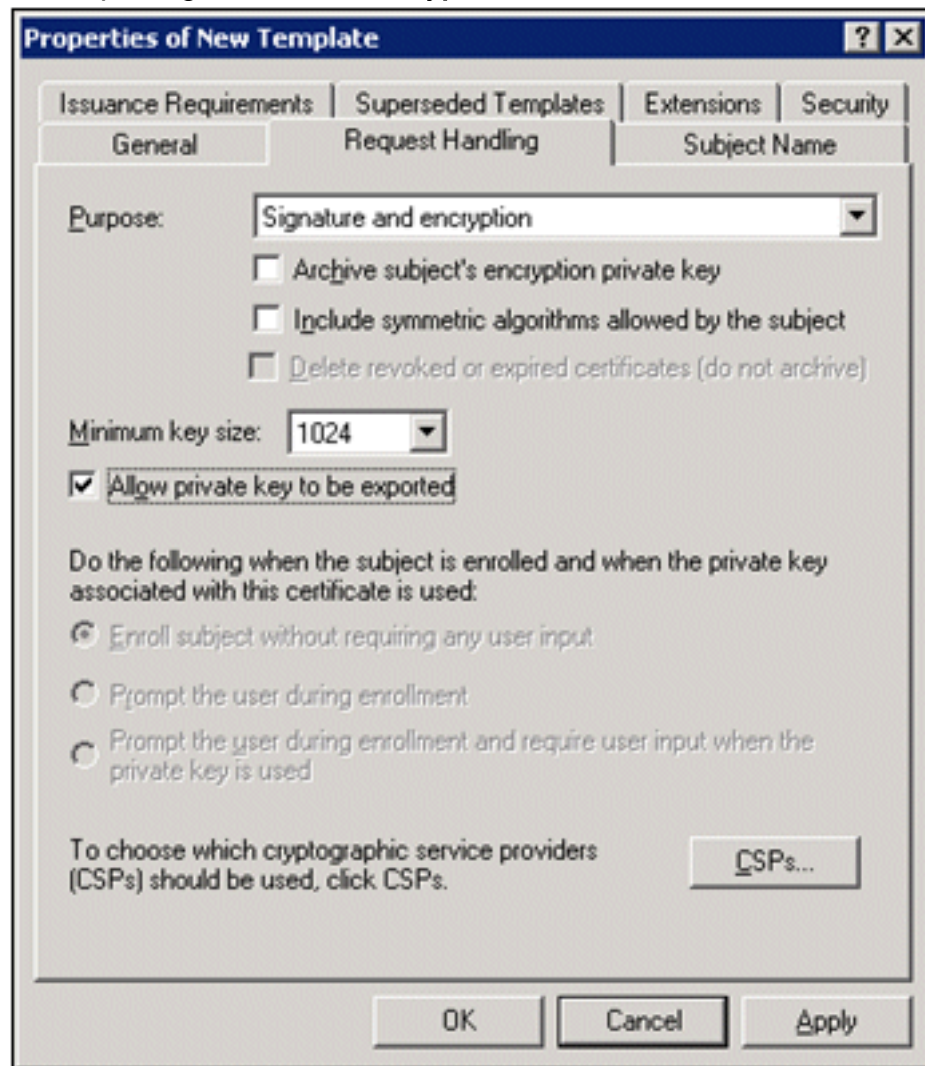
Publish certificate in Active Directory
 Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply

ACS.

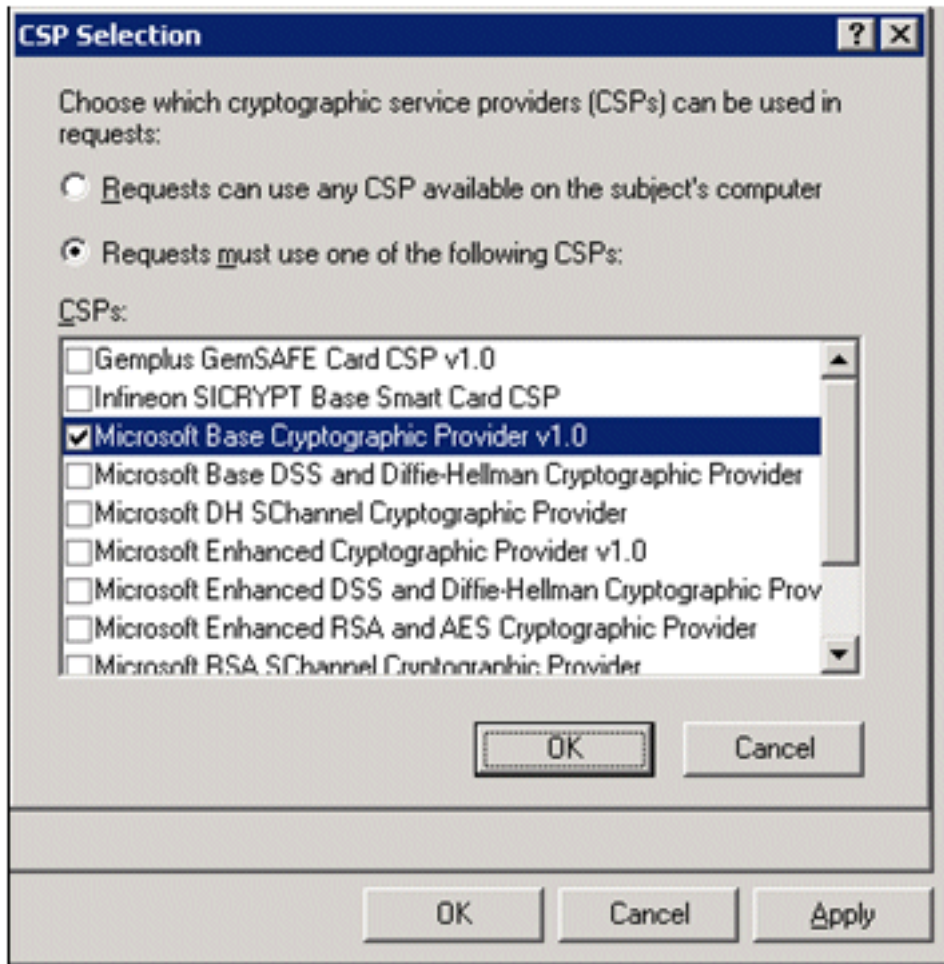
4. Accédez à l'onglet **Gestion des demandes** et cochez **Autoriser l'exportation de la clé privée**.

Assurez-vous également que **Signature and Encryption** est sélectionné dans le menu



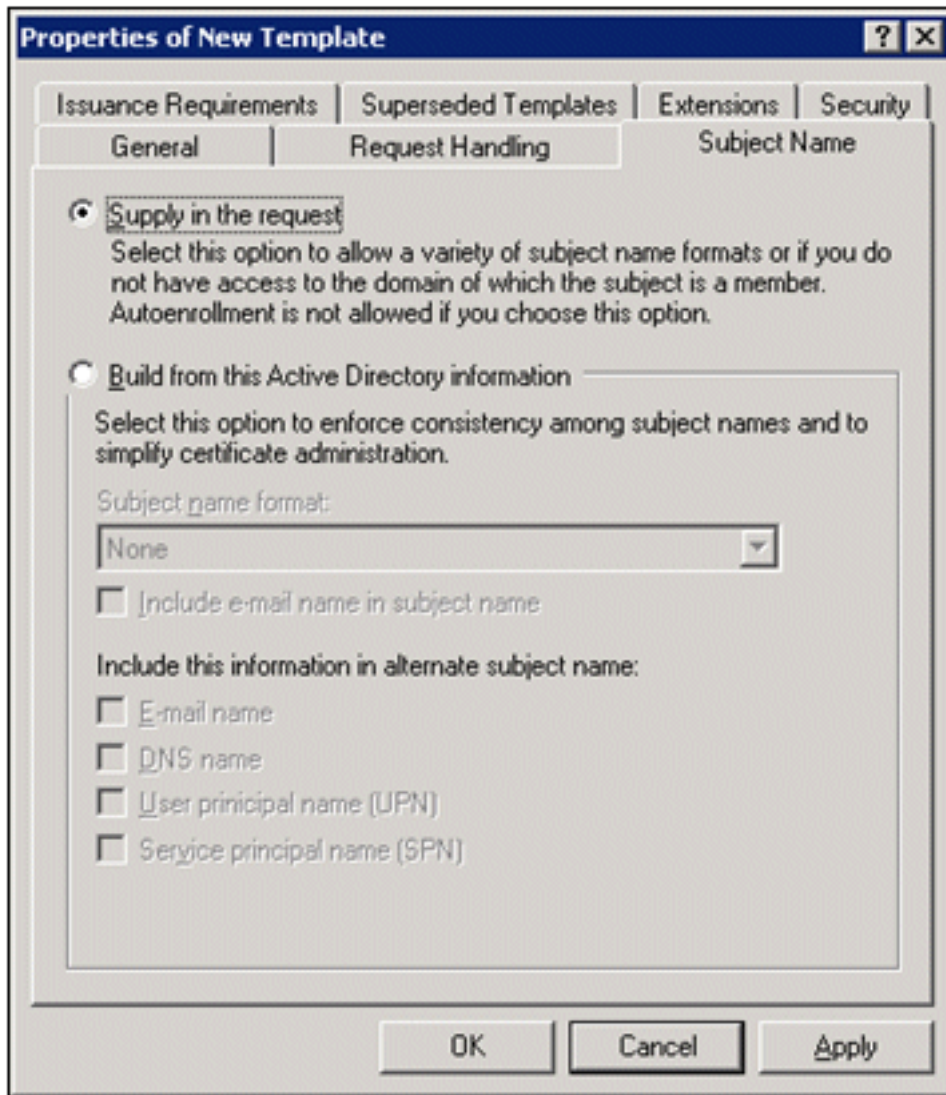
déroulant Purpose.

5. Choisissez **Requests must use l'un des fournisseurs de services de chiffrement suivants** et cochez **Microsoft Base Cryptographic Provider v1.0**. Désélectionnez tous les autres fournisseurs de services cloud cochés, puis cliquez sur



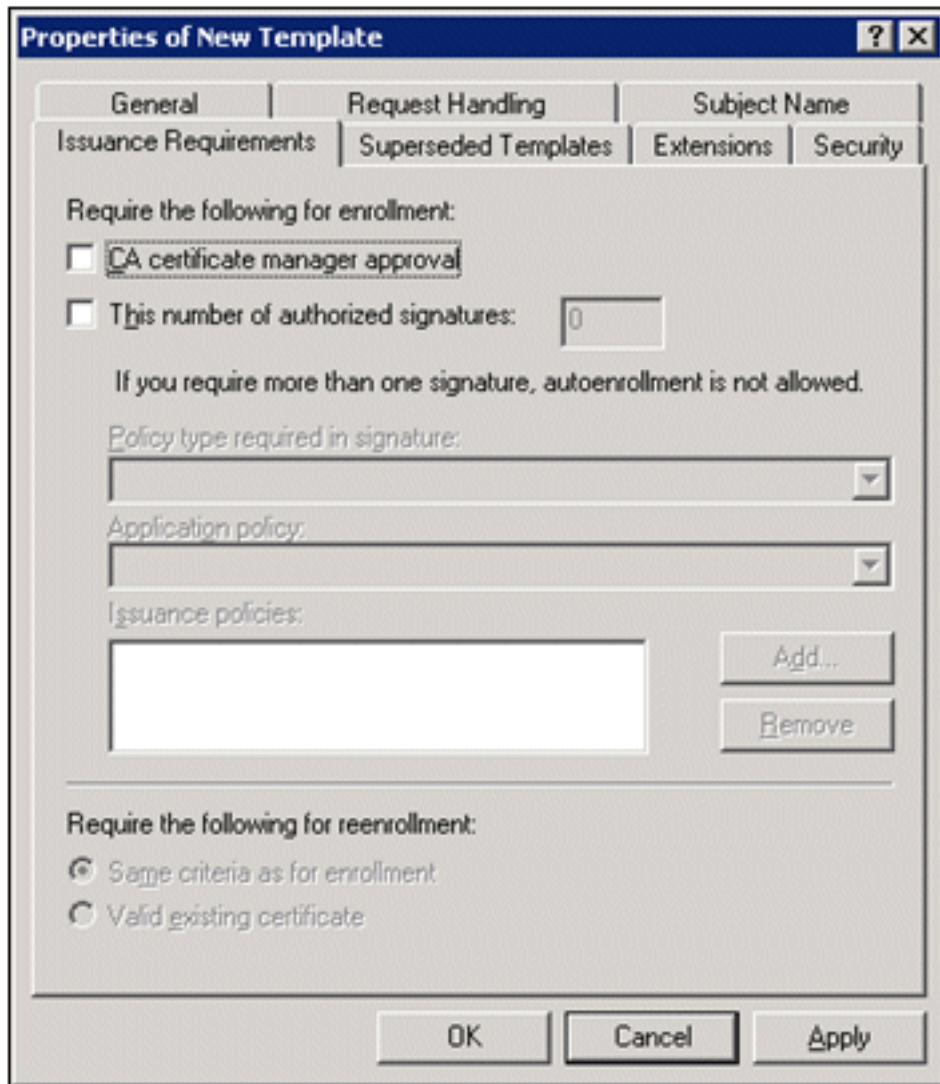
OK.

6. Accédez à l'onglet **Nom de l'objet**, choisissez **Fourniture** dans la demande, puis cliquez sur



OK.

7. Accédez à l'onglet **Security**, mettez en surbrillance **Domain Admins Group**, et assurez-vous que l'option **Enroll** est cochée sous **Allowed**. **Remarque** : si vous choisissez de générer à partir de ces informations Active Directory, vérifiez uniquement le **nom d'utilisateur principal (UPN)** et décochez la case **Inclure le nom de messagerie** dans le nom de l'objet et le nom de messagerie, car aucun nom de messagerie 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 la messagerie 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 repoussés. Vous les trouverez sous l'onglet **Conditions d'émission**. Ce point n'est pas traité plus en détail dans le présent



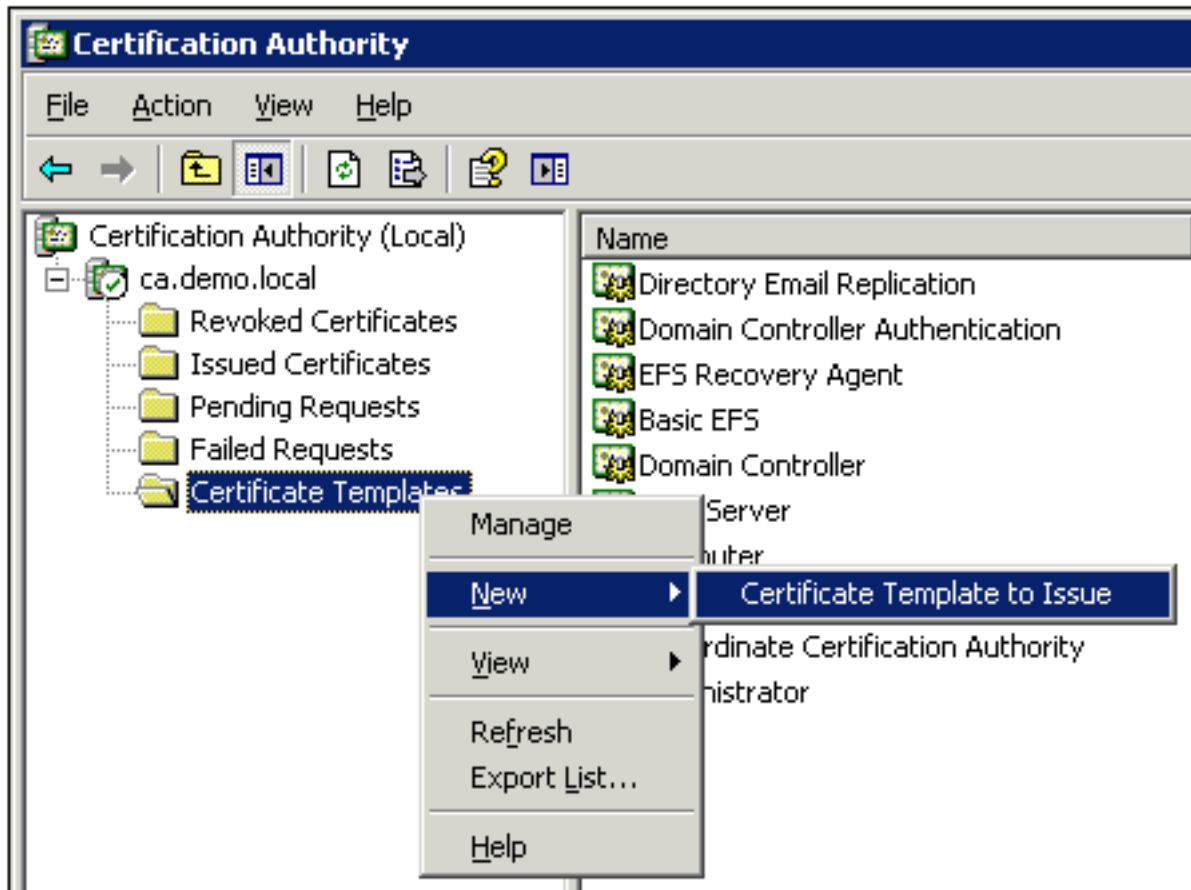
document.

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

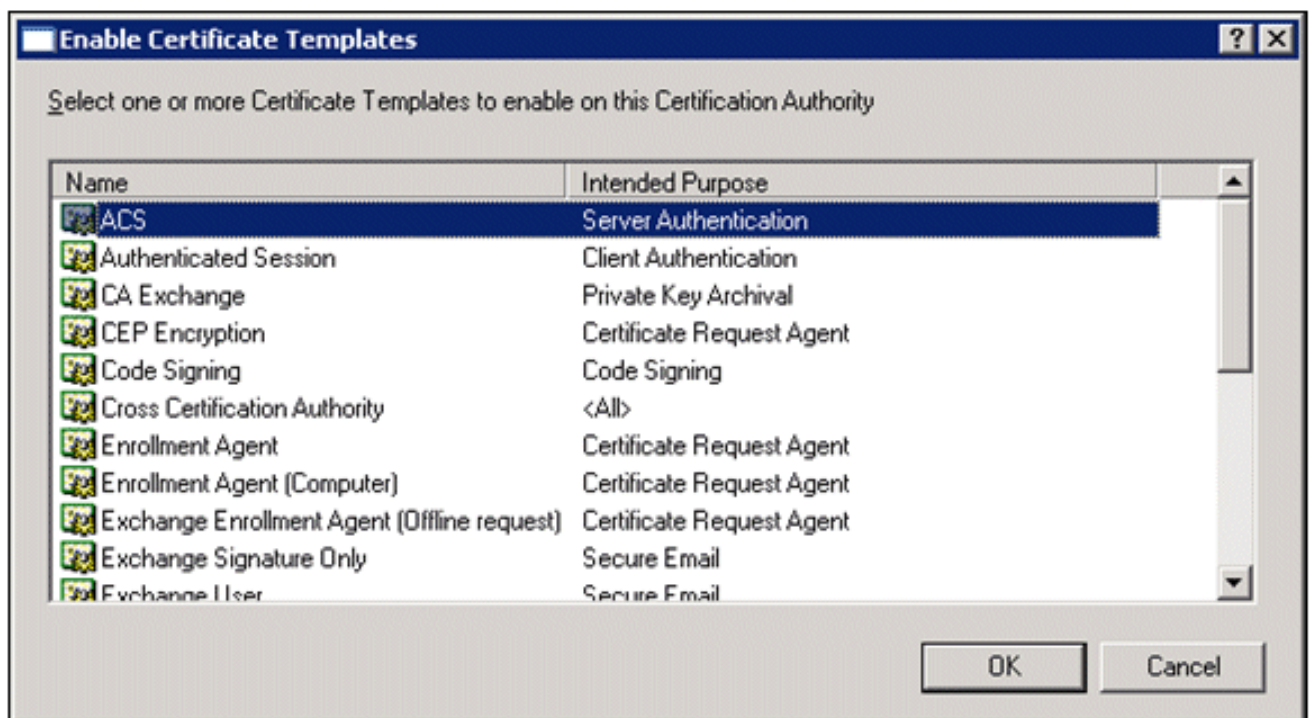
[Activer le nouveau modèle de certificat de serveur Web ACS](#)

Effectuez les étapes suivantes :

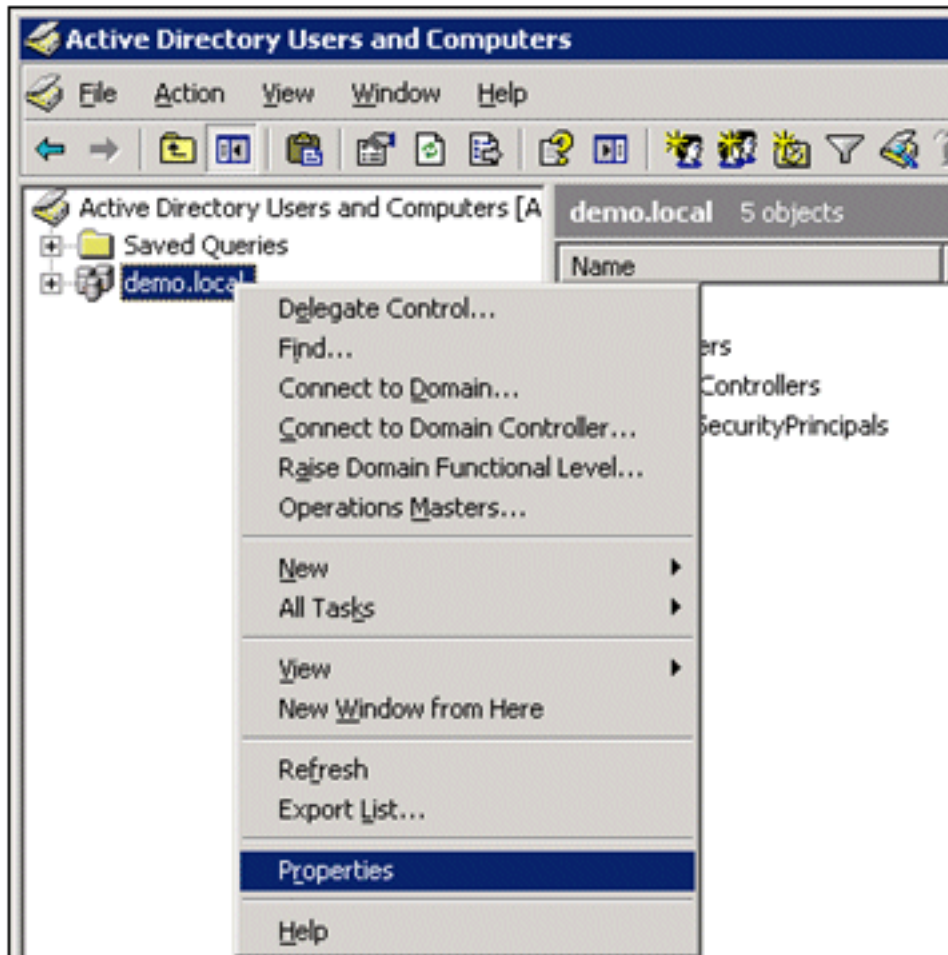
1. Ouvrez le composant logiciel enfichable Autorité de certification. Effectuez les étapes 1 à 3 dans la section [Créer le modèle de certificat pour le serveur Web ACS](#), choisissez l'option **Autorité de certification**, choisissez **Ordinateur local**, et cliquez sur **Terminer**.
2. Dans l'arborescence de la console de l'autorité de certification, développez **ca.demo.local**, puis cliquez avec le bouton droit sur **Modèles de certificat**.
3. Accédez à **Nouveau > Modèle de certificat à émettre**.



4. Cliquez sur le **modèle de certificat ACS**.

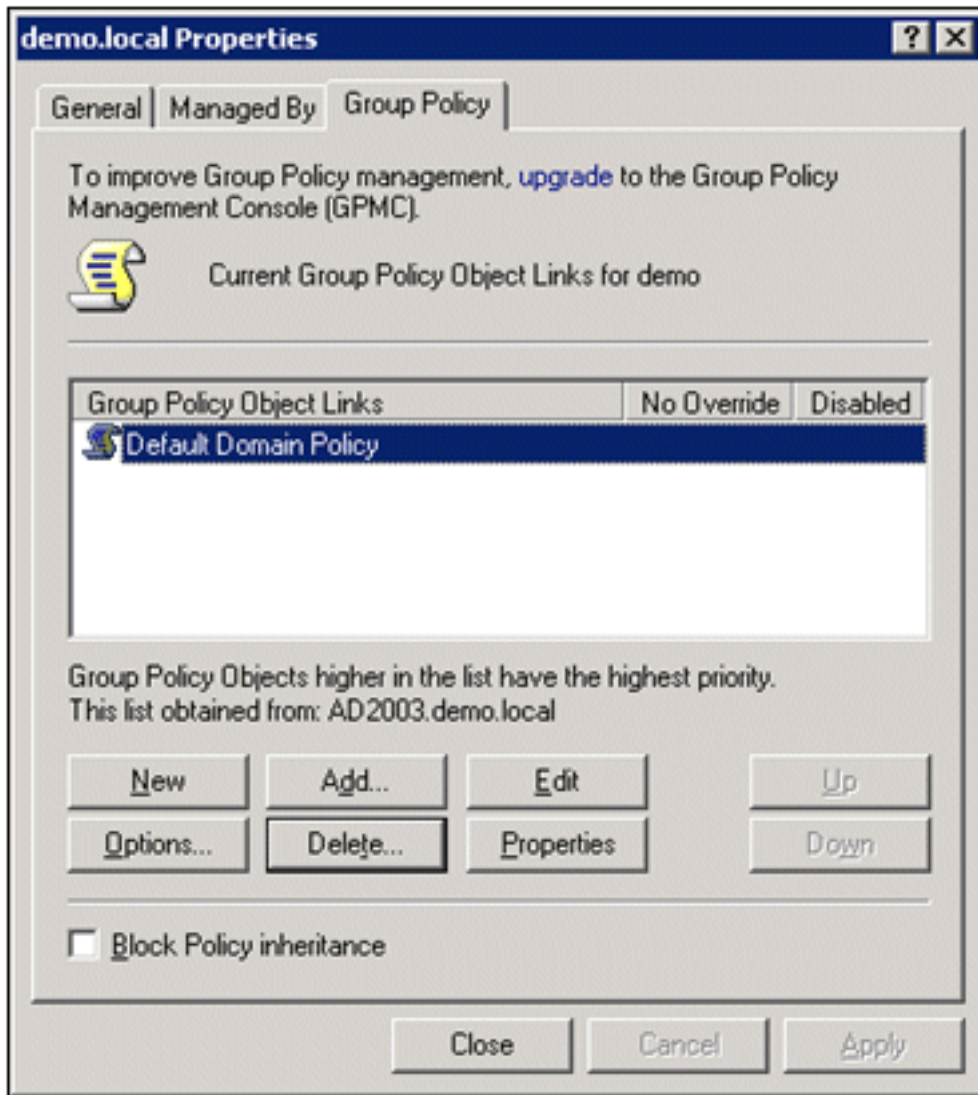


5. Cliquez sur **OK** et ouvrez le **composant logiciel enfichable Utilisateurs et ordinateurs Active Directory**.
6. Dans l'arborescence de la console, double-cliquez sur **Utilisateurs et ordinateurs Active Directory**, cliquez avec le bouton droit sur **demo.local**, puis cliquez sur



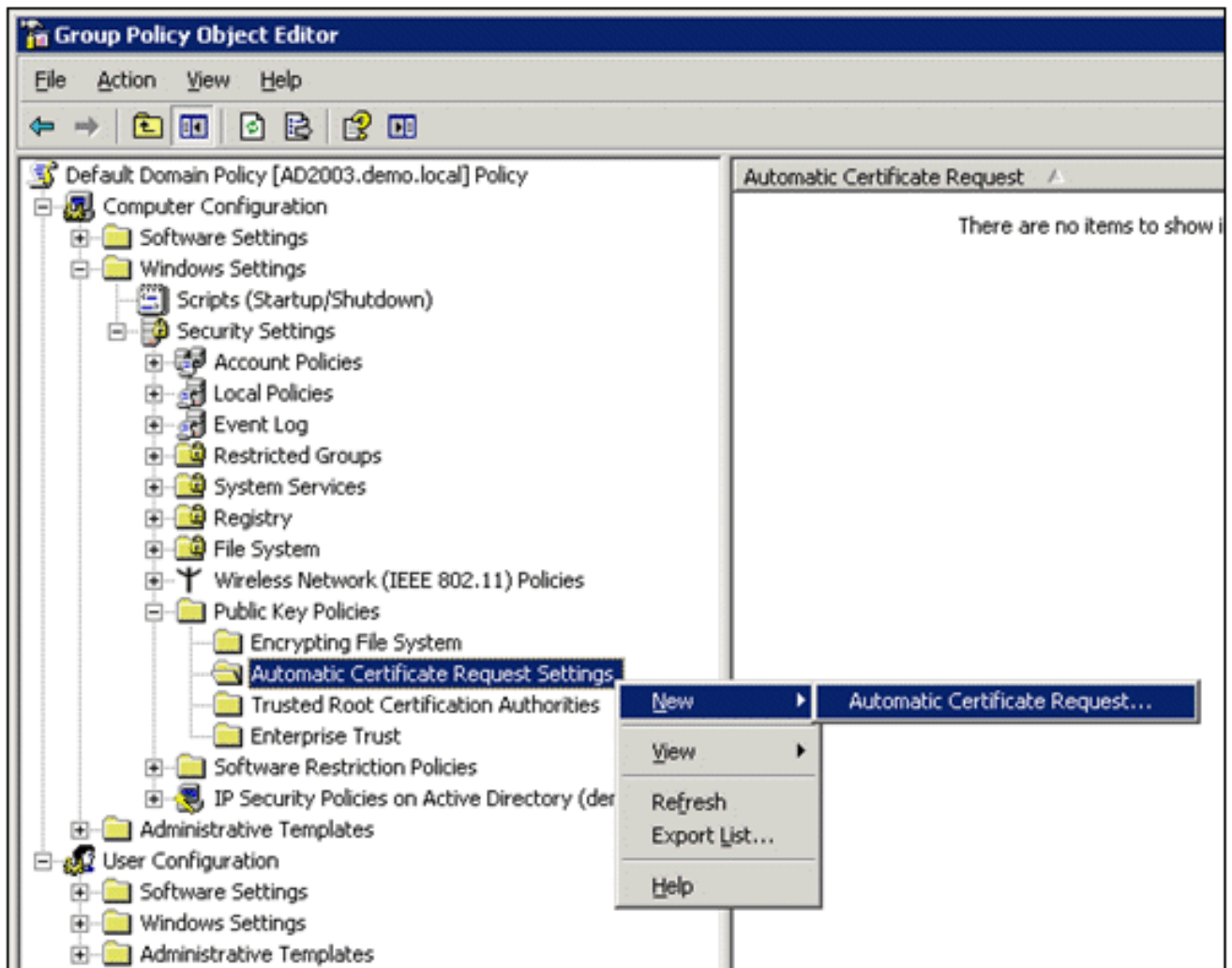
Propriétés.

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

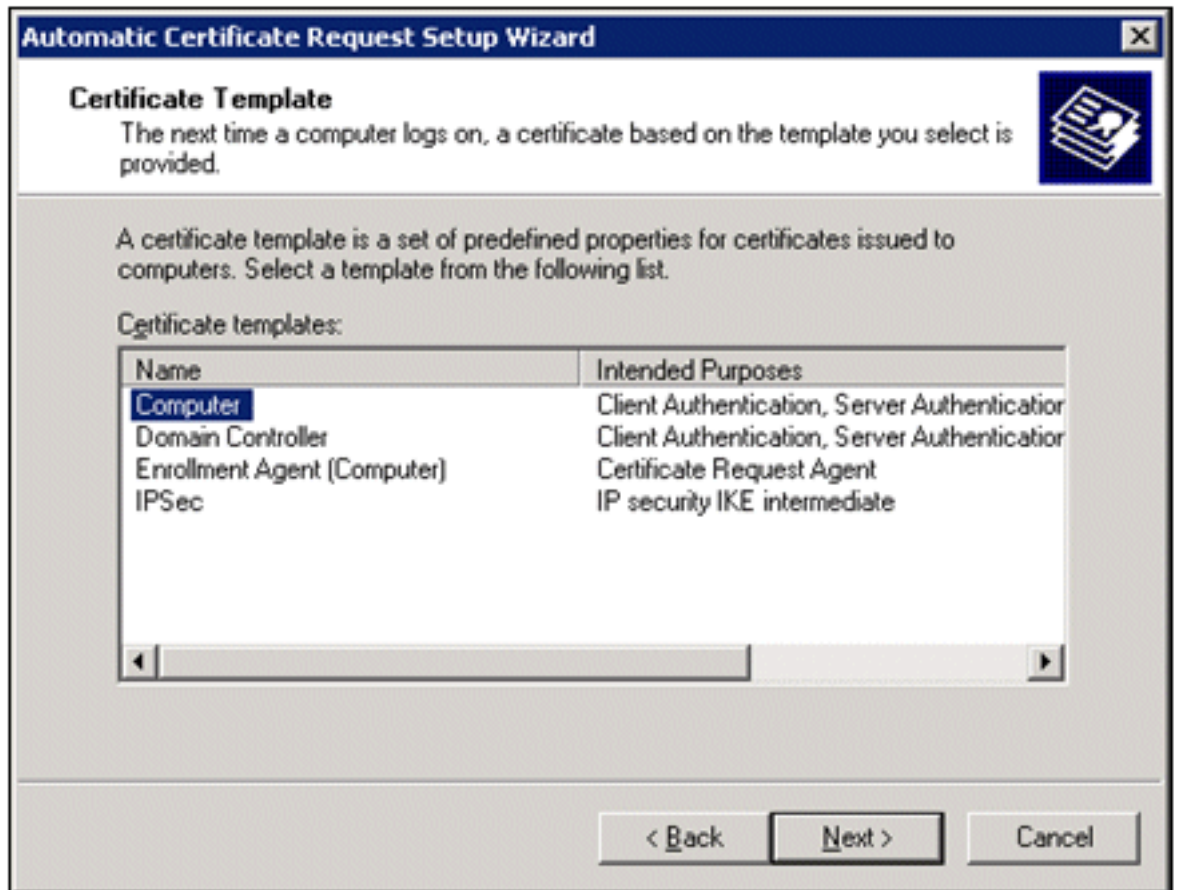


s'ouvre.

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

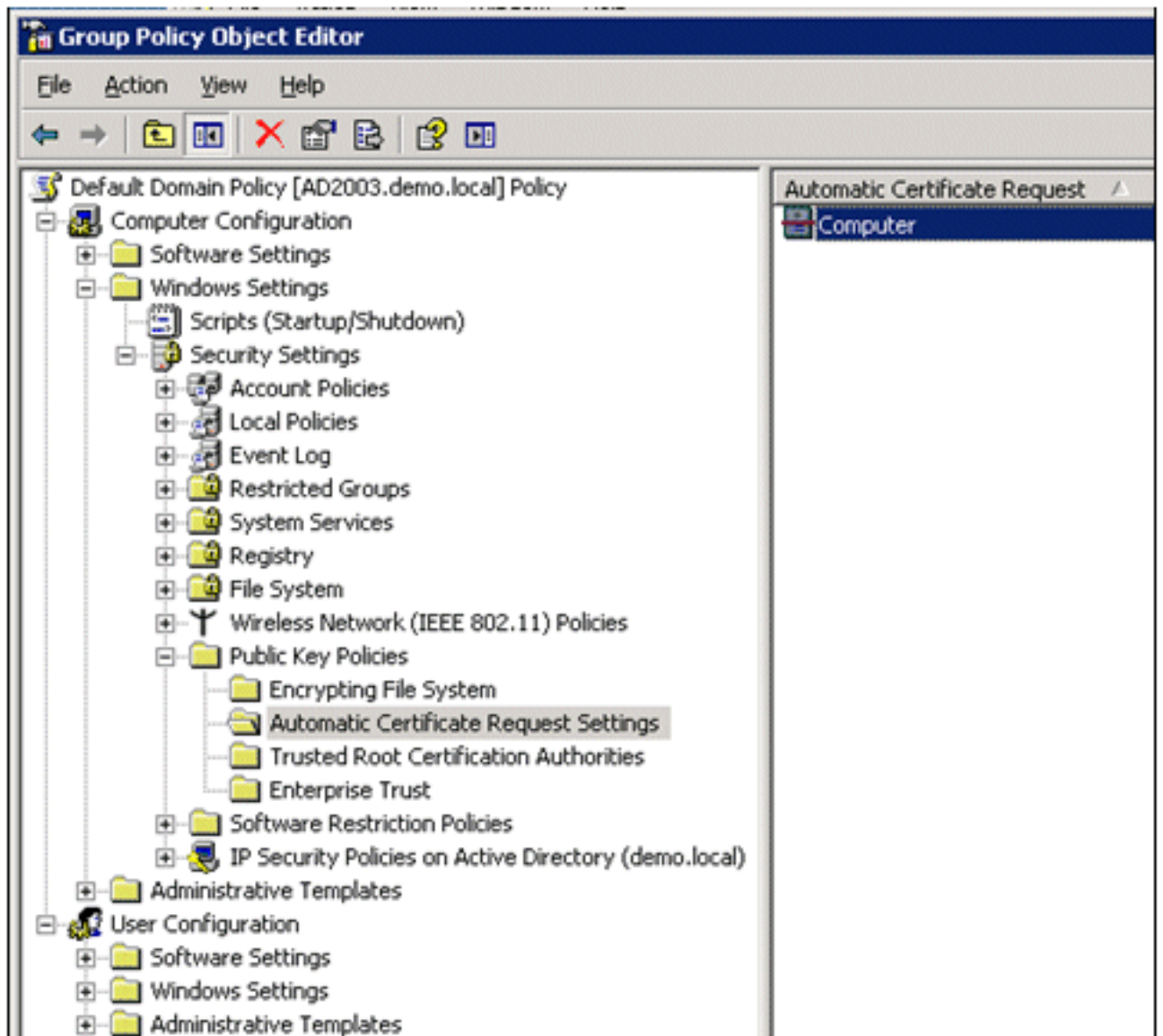


9. Cliquez avec le bouton droit sur **Automatic Certificate Request Settings**, et choisissez **New > Automatic Certificate Request**.
10. Sur la page Assistant Configuration automatique de la demande de certificat, cliquez sur **Suivant**.
11. Sur la page Modèle de certificat, cliquez sur **Ordinateur**, puis sur

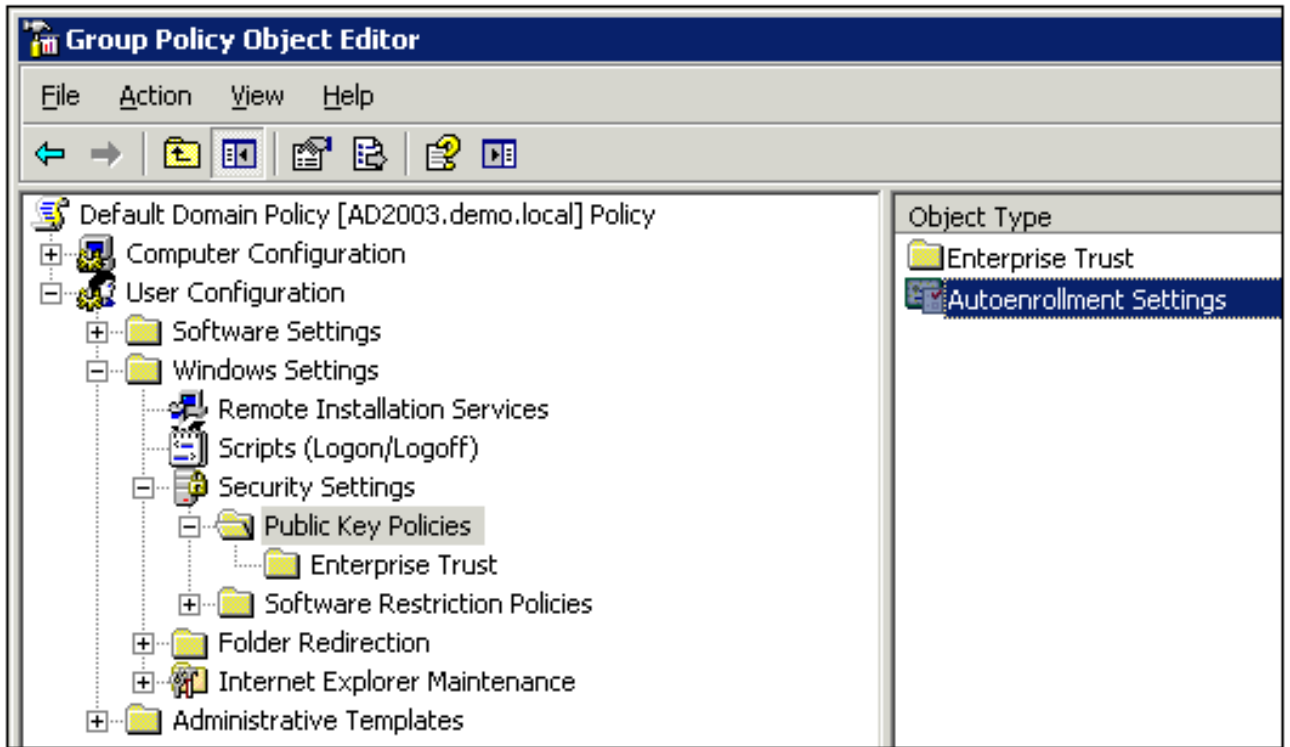


Suivant.

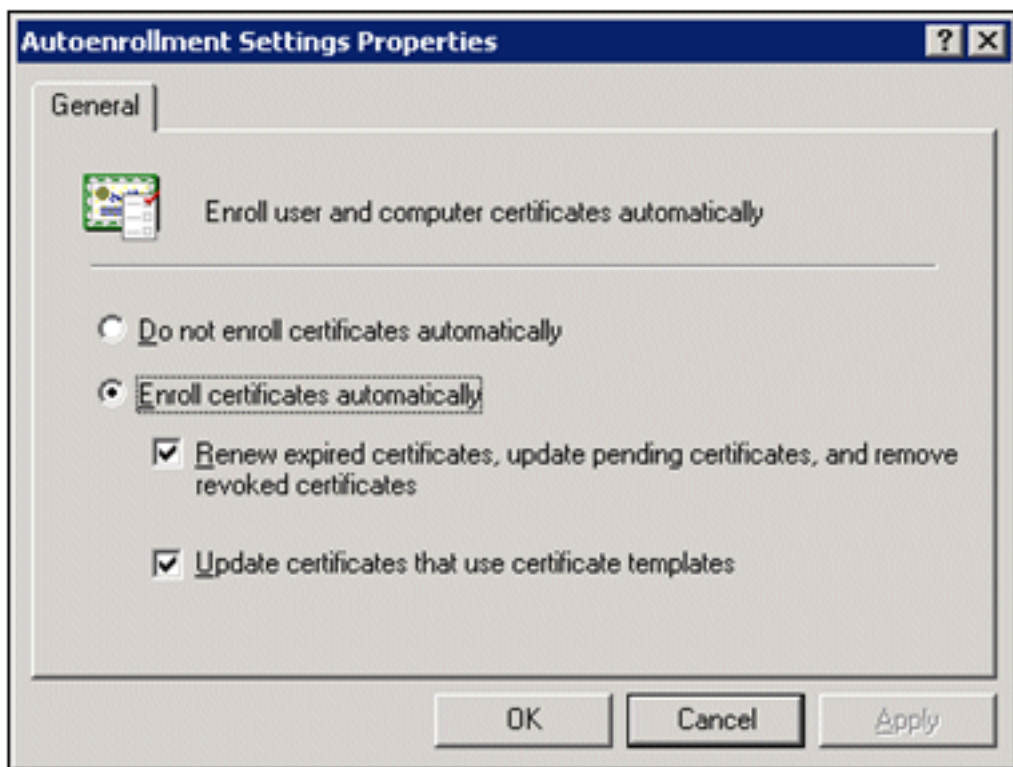
12. Lorsque vous avez terminé la page Assistant Configuration automatique de la demande de certificat, cliquez sur **Terminer**. Le type de certificat Ordinateur apparaît désormais dans le volet d'informations du composant logiciel enfichable Éditeur d'objets de stratégie de groupe.



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 les certificats automatiquement** et cochez **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.

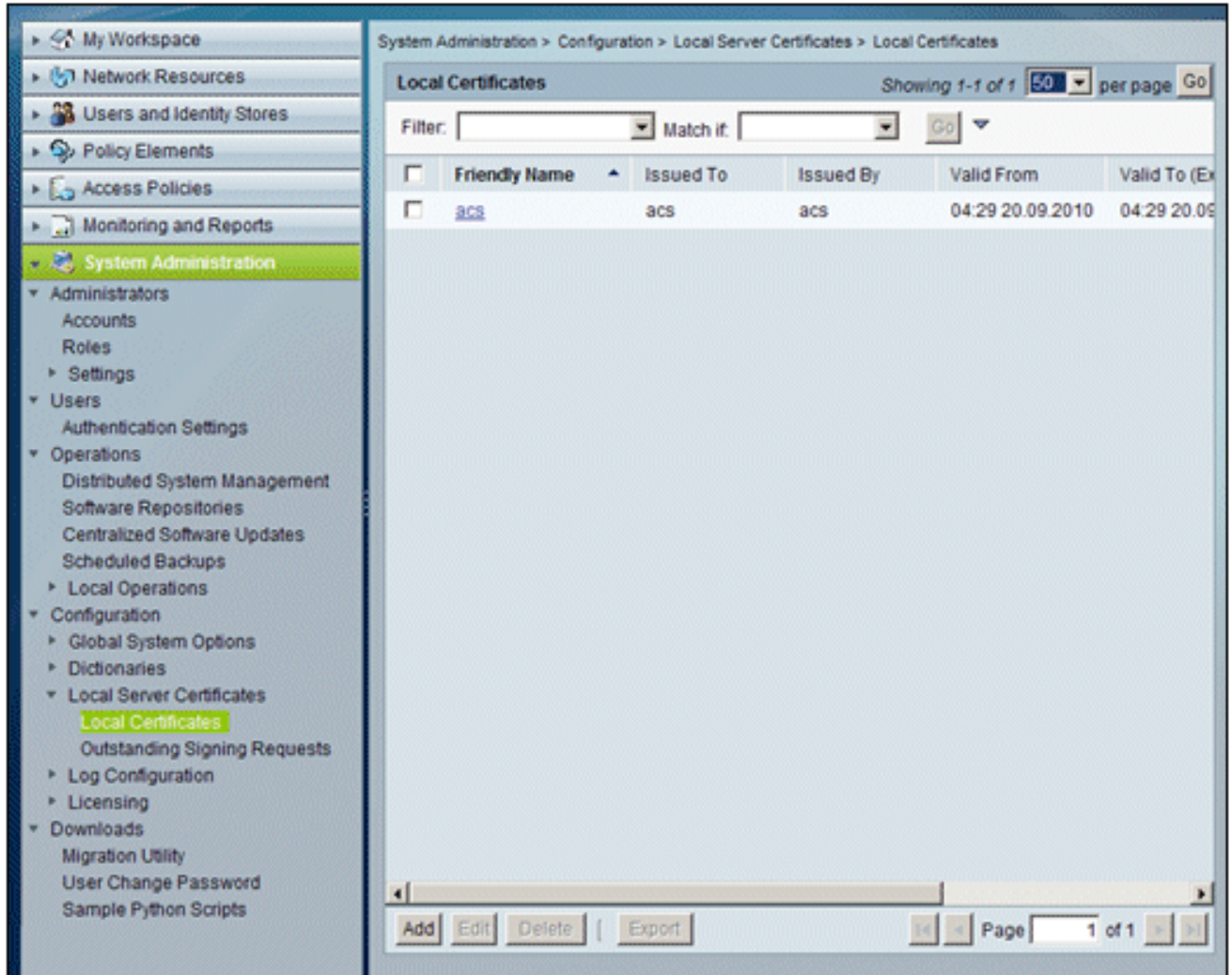
[Configuration du certificat ACS 5.1](#)

[Configurer le certificat exportable pour ACS](#)

Remarque : le serveur ACS doit obtenir un certificat de serveur du serveur AC racine d'entreprise afin d'authentifier un client PEAP WLAN.

Remarque : assurez-vous que le Gestionnaire des services Internet (IIS) n'est pas ouvert pendant le processus de configuration du certificat, car cela entraîne des problèmes avec les informations mises en cache.

1. Connectez-vous au serveur ACS avec des droits d'administrateur de compte.
2. Accédez à **Administration système > Configuration > Certificats du serveur local**. Cliquez sur **Add**.



3. Lorsque vous choisissez une méthode de création de certificat de serveur, choisissez **Generate Certificate Signing Request**. Cliquez sur **Next** (Suivant).

Cisco Secure ACS
NFR(Days left: 296)

acsadmin acs (Primary) Log Out About Help

My Workspace
Network Resources
Users and Identity Stores
Policy Elements
Access Policies
Monitoring and Reports
System Administration
Administrators
Accounts
Roles
Settings
Users
Authentication Settings
Operations
Distributed System Management
Software Repositories
Centralized Software Updates
Scheduled Backups
Local Operations
Configuration
Global System Options
Dictionaries
Local Server Certificates
Local Certificates
Outstanding Signing Requests
Log Configuration
Licensing
Downloads
Migration Utility
User Change Password
Sample Python Scripts

System Administration > Configuration > Local Server Certificates > Local Certificates > Create

Select server certificate creation method

Step 1 - Select server certificate creation method

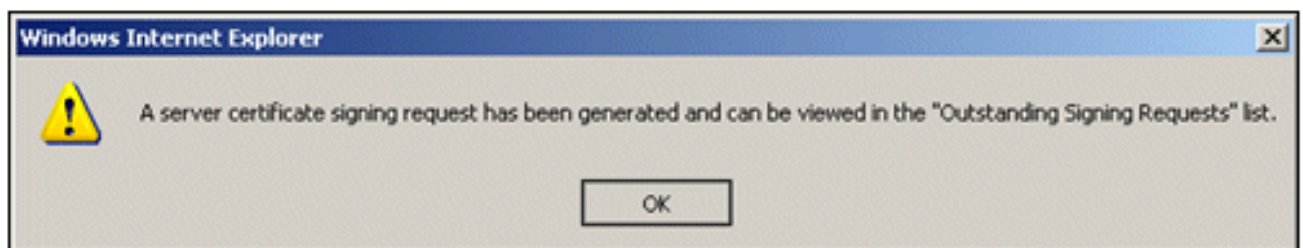
- Import Server Certificate
Use this option if you have a Server Certificate file and corresponding private key file (and password, if the private key file is encrypted).
- Generate Self Signed Certificate
Use this option to have the ACS server generate a Self-Signed Certificate.
- Generate Certificate Signing Request
Use this option to have the ACS server generate a certificate signing request to present to your local Certificate Authority. Once you have generated the signing request, go to the "Outstanding Signing Requests" list, select the signing request, and export a copy of the signing request (save a copy on your client system). Once you receive a certificate from your CA, you will use the "Bind CA Signed Certificate" option below to install it.
- Bind CA Signed Certificate
After using the previous option to generate a certificate signing request, this option is used to bind/install the certificate received from your CA. ACS will automatically match the certificate with the appropriate outstanding signing request.

Back Next Cancel

4. Entrez un objet de certificat et une longueur de clé comme exemple, puis cliquez sur **Terminer** :Objet du certificat - CN=acs.demo.localLongueur de clé - 1024

The screenshot shows the Cisco Secure ACS web interface. The top navigation bar includes the Cisco logo, 'Cisco Secure ACS', 'NFR(Days left: 296)', and user information 'acsadmin', 'acs (Primary)', and 'Log Out'. The left sidebar contains a tree view of system administration options, with 'System Administration' expanded to show 'Local Server Certificates' and 'Local Certificates' selected. The main content area displays the breadcrumb 'System Administration > Configuration > Local Server Certificates > Local Certificates > Create' and a checked radio button for 'Generate Certificate Signing Request'. Below this, the 'Step 2 -Generate Certificate Signing Request' form is visible, with fields for 'Certificate Subject' (CN=acs.demo.local), 'Key Length' (1024), and 'Digest to Sign with' (SHA1). 'Back' and 'Finish' buttons are at the bottom right.

5. ACS vous demande si une demande de signature de certificat a été générée. Click OK.



6. Sous System Administration, accédez à **Configuration > Local Server Certificates > Outstanding Signing Requests**. **Remarque** : la raison de cette étape est que Windows 2003 n'autorise pas les clés exportables et que vous devez générer une demande de certificat basée sur le certificat ACS que vous avez créé précédemment et qui le permet.

Cisco Secure ACS
NFR(Days left: 296)

acsadmin acs (Primary) Log Out About Help

System Administration > Configuration > Local Server Certificates > Outstanding Signing Requests

Certificate Signing Request Showing 1-1 of 1 50 per page Go

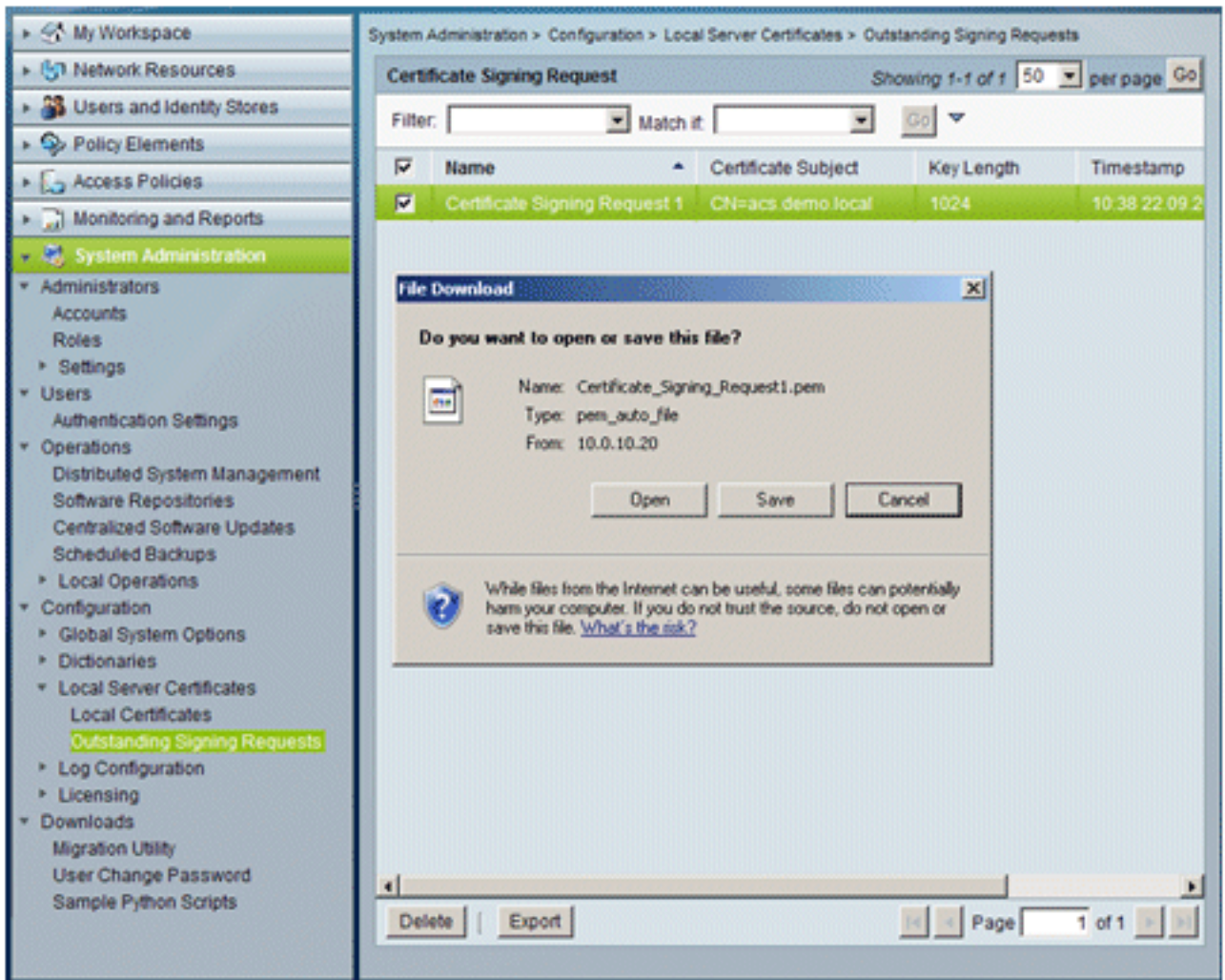
Filter: Match if: Go

<input type="checkbox"/>	Name	Certificate Subject	Key Length	Timestamp
<input type="checkbox"/>	Certificate Signing Request 1	CN=acs.demo.local	1024	10:38 22.09.2

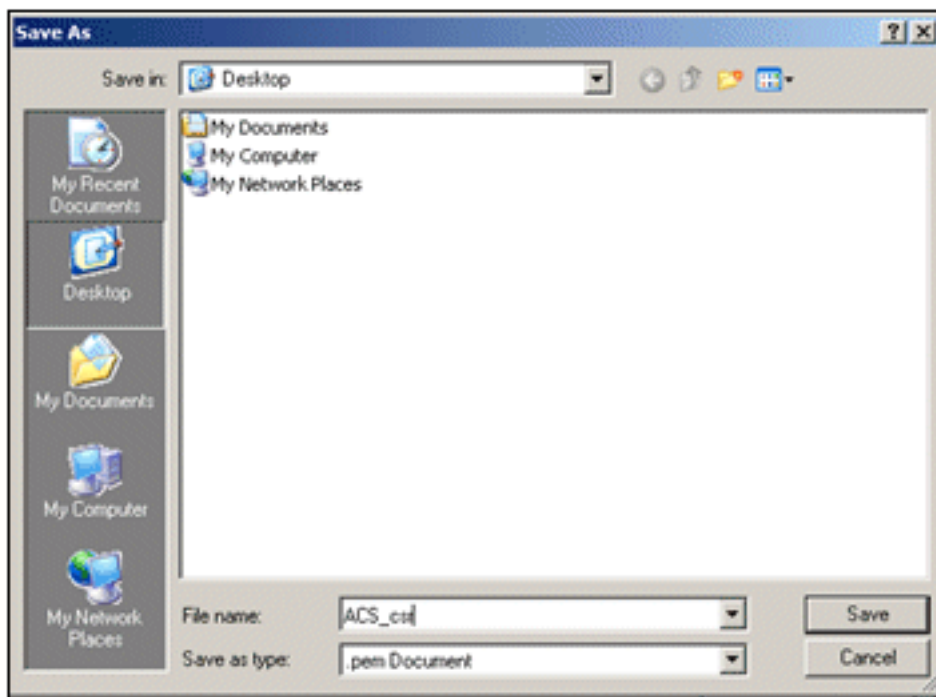
multiple row selection

Delete | Export Page 1 of 1

7. Sélectionnez l'entrée **Demande de signature de certificat**, puis cliquez sur **Exporter**.



8. Enregistrez le fichier certificat .pem ACS sur le

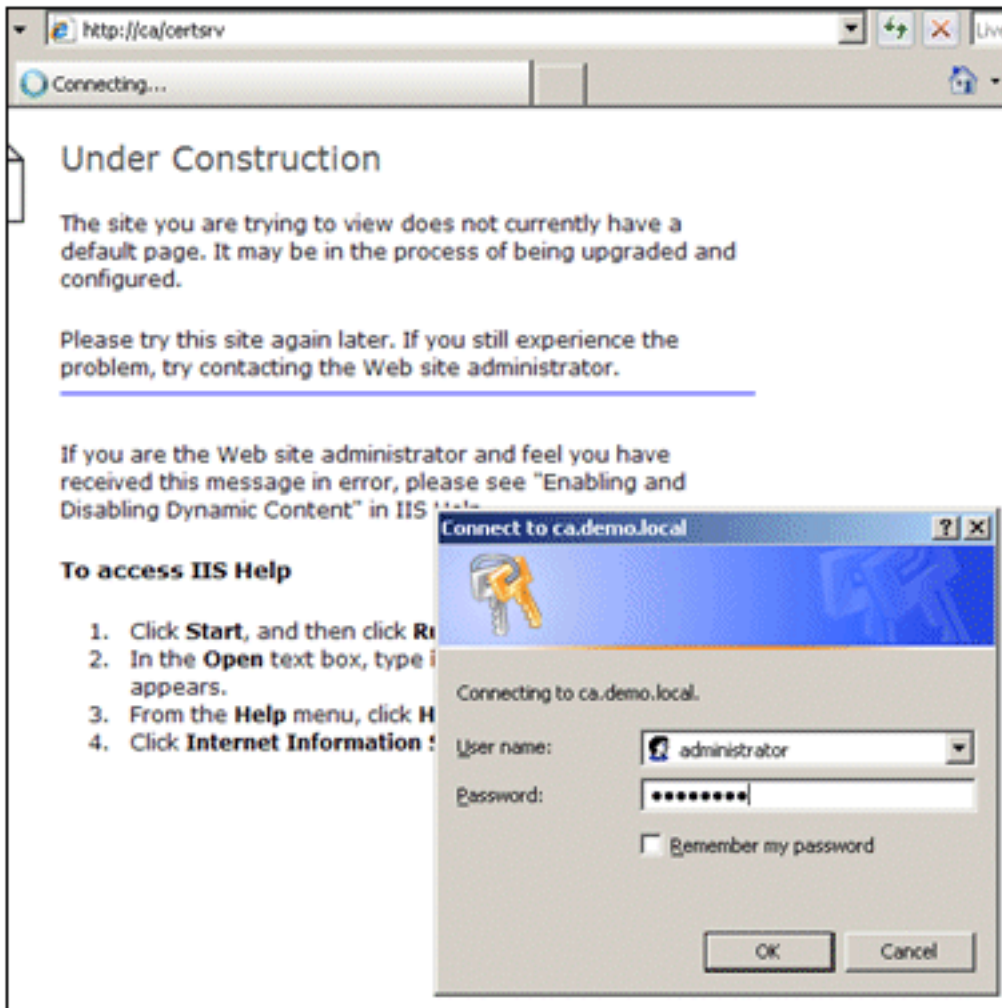


bureau.

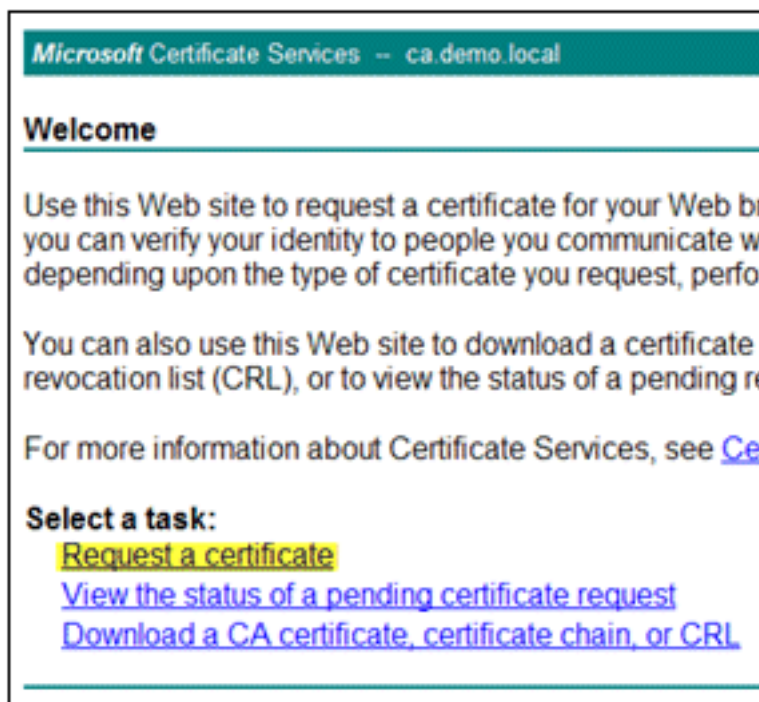
[Installation du certificat dans le logiciel ACS 5.1](#)

Effectuez les étapes suivantes :

1. Ouvrez un navigateur et connectez-vous à l'URL du serveur AC <http://10.0.10.10/certsrv>.

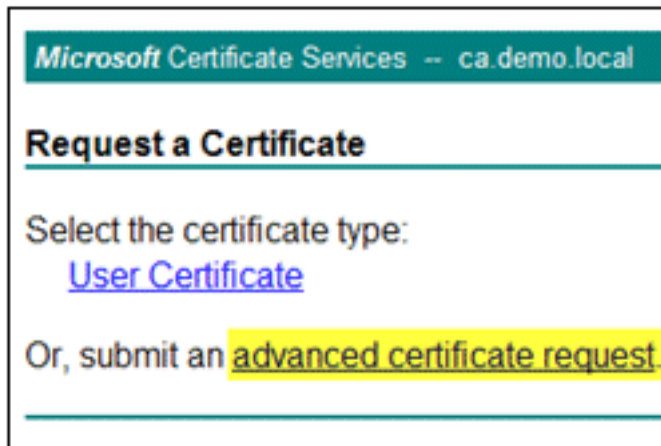


2. La fenêtre Services de certificats Microsoft s'affiche. Sélectionnez **Demander un**



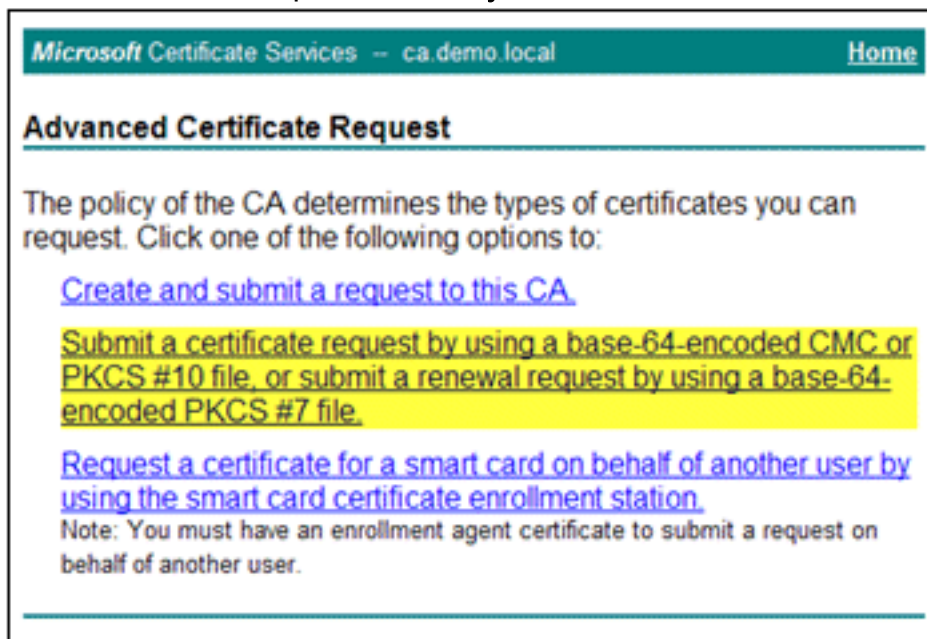
certificat.

3. Cliquez pour envoyer une **demande de certificat**



avancée.

4. Dans la demande avancée, cliquez sur **Envoyer une demande de certificat à l'aide d'un code**



base 64...

5. Dans le champ Requête enregistrée, si la sécurité du navigateur le permet, accédez au fichier de requête de certificat ACS précédent et insérez-

Microsoft Certificate Services – ca demo local Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

[Browse for a file to insert.](#)

Certificate Template:

Administrator

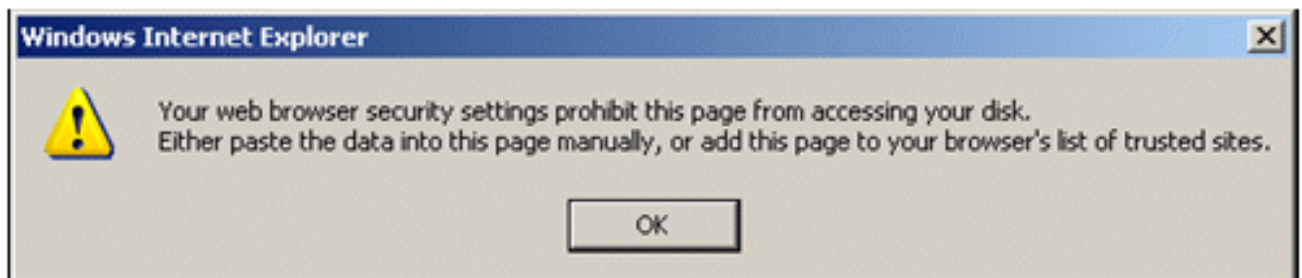
Additional Attributes:

Attributes:

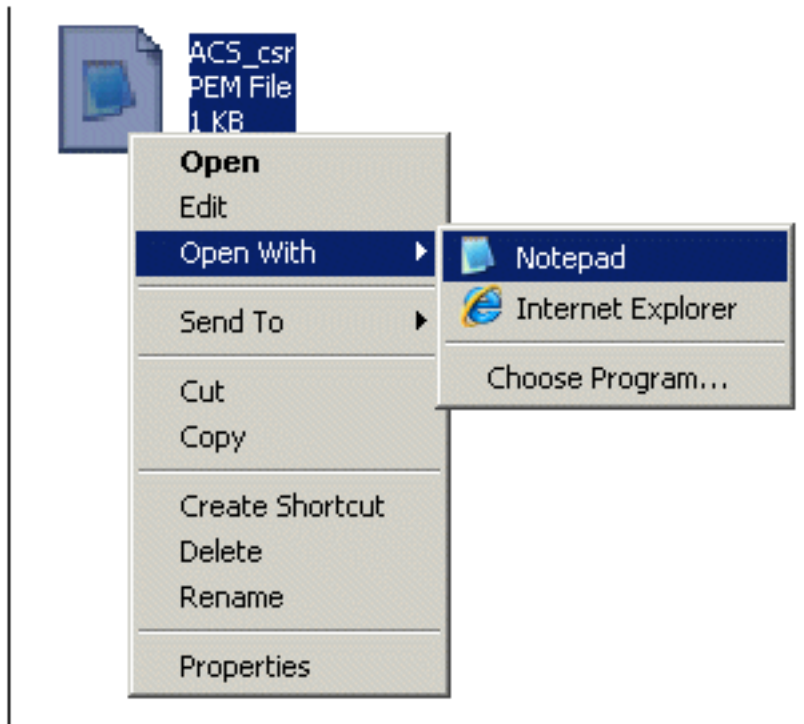
Submit >

le.

6. Les paramètres de sécurité du navigateur risquent de ne pas autoriser l'accès au fichier sur un disque. Si c'est le cas, cliquez sur **OK** pour effectuer un collage manuel.

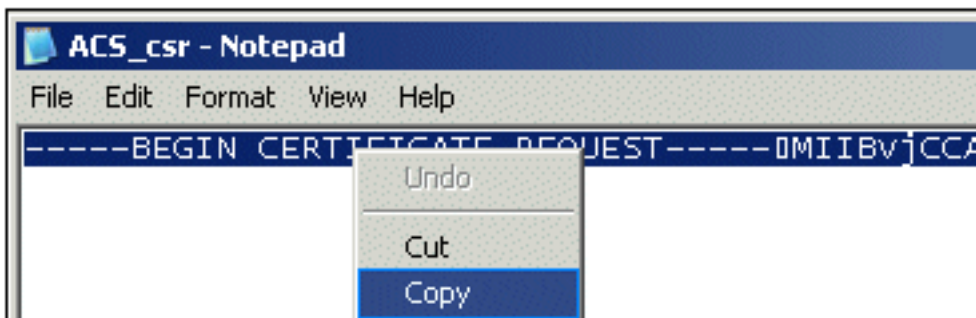


7. Recherchez le fichier ACS *.pem à partir de l'exportation ACS précédente. Ouvrez le fichier à l'aide d'un éditeur de texte (Bloc-notes, par



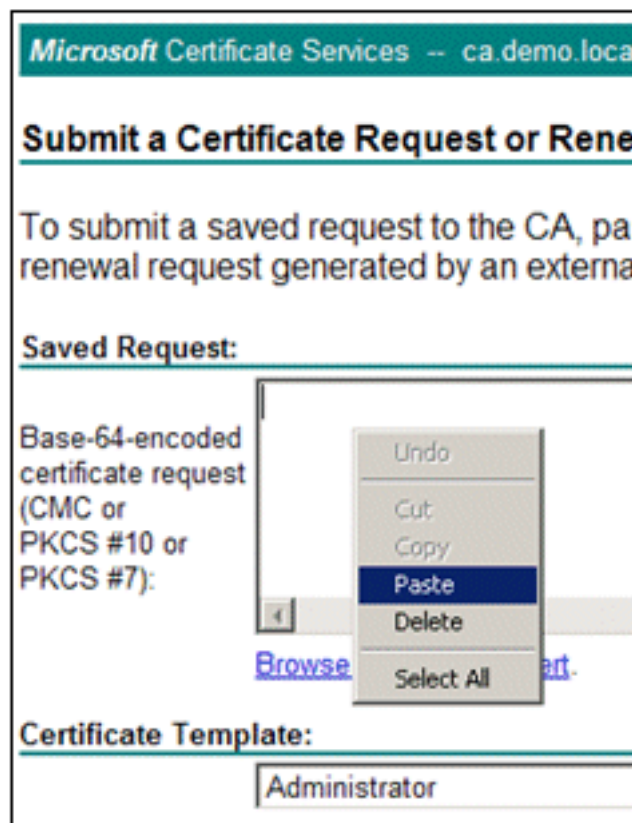
exemple).

8. Mettez en surbrillance l'intégralité du contenu du fichier, puis cliquez sur



Copier.

9. Revenez à la fenêtre de demande de certificat Microsoft. Collez le contenu copié dans le



champ Requête enregistrée.

10. Sélectionnez **ACS** comme modèle de certificat, puis cliquez sur

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
YI2IAYb4QgEBBAQDAgZAMA0GCSqGSIb3DQEBBQUA  
DXoioRABct447wO77+uAk8ern26oaEhcfG/ZR15X  
ONZQ5xnrK23yxEdQNvSFC30mzRZEBQq4s5MvPEZZ  
/MWqXeJ3NjpicpAgiV8CSwNd  
-----END CERTIFICATE REQUEST-----
```

[Browse for a file to insert.](#)

Certificate Template:

ACS

Additional Attributes:

Attributes:

Submit >

Submit.

11. Une fois le certificat émis, choisissez **Base 64 encoded**, et cliquez sur **Download**

Microsoft Certificate Services -- ca demo.local

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded

[Download certificate](#)

[Download certificate chain](#)

File Download - Security Warning

Do you want to open or save this file?

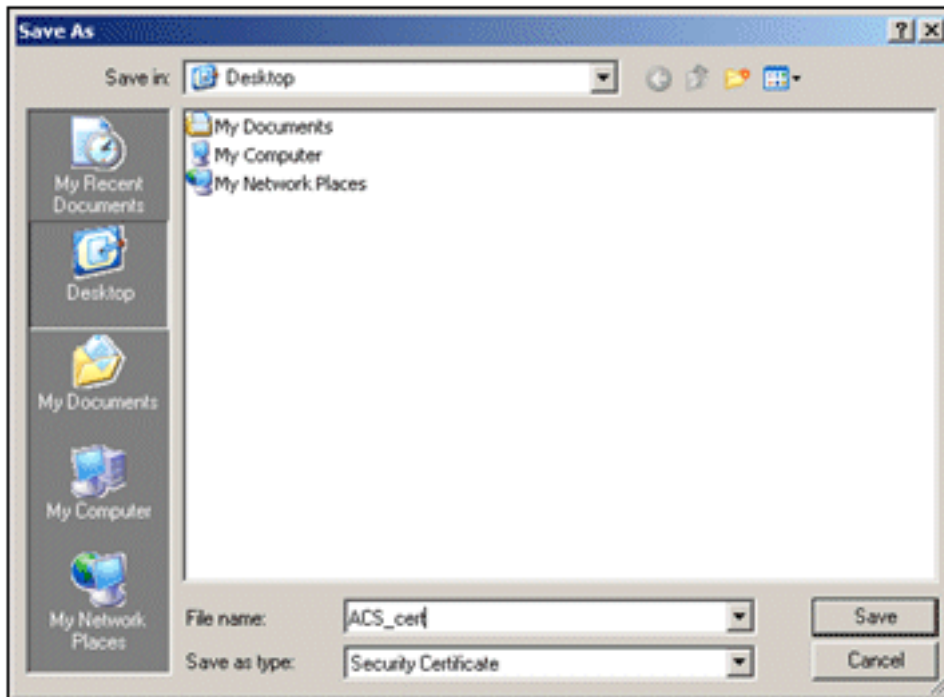
Name: certnew.cer
Type: Security Certificate, 1.88KB
From: ca

Open Save Cancel

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. [What's the risk?](#)

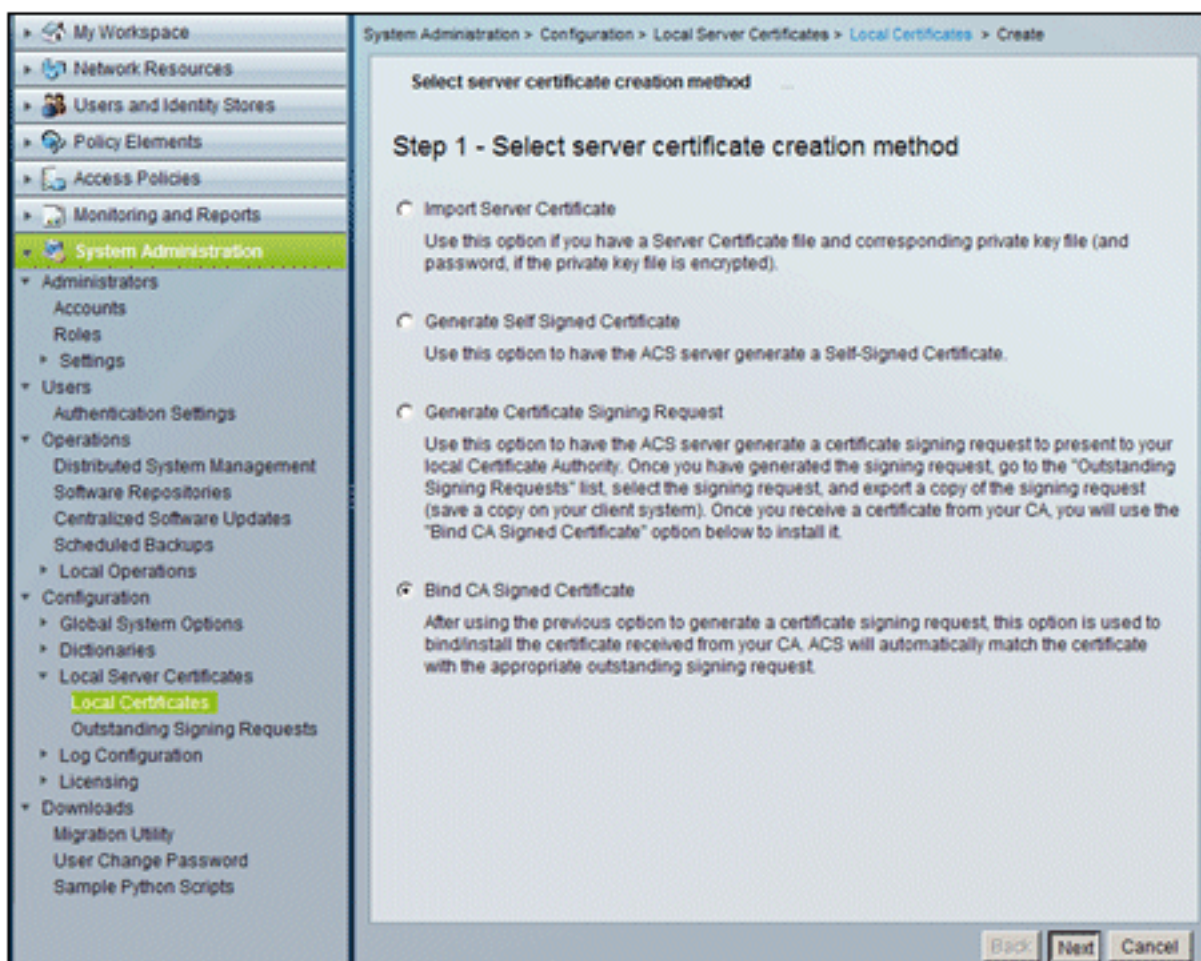
certificate.

12. Cliquez sur **Save** afin d'enregistrer le certificat sur le



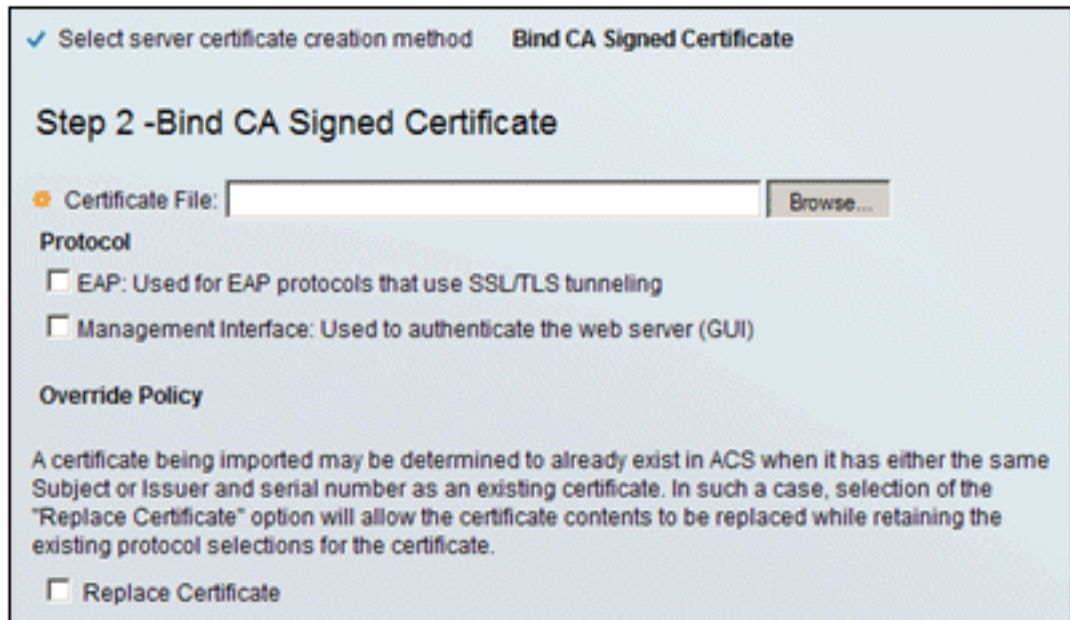
bureau.

13. Accédez à **ACS > Administration système > Configuration > Certificats du serveur local**. Choisissez **Bind CA Signed Certificate**, puis cliquez sur



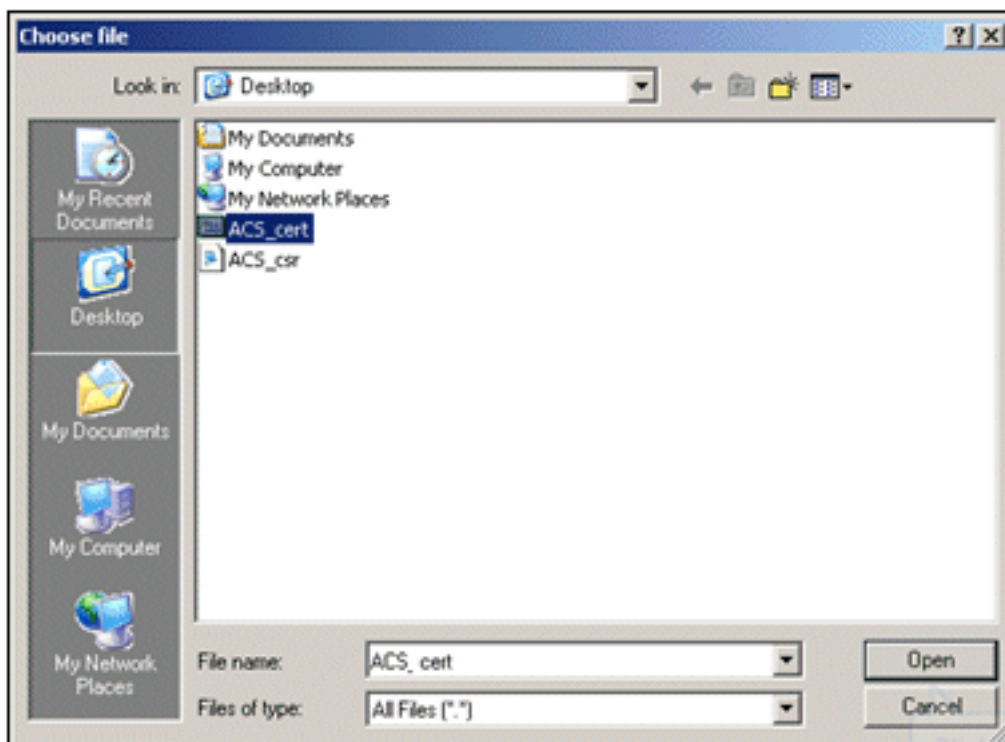
Next.

14. Cliquez sur **Browse**, et localisez le certificat



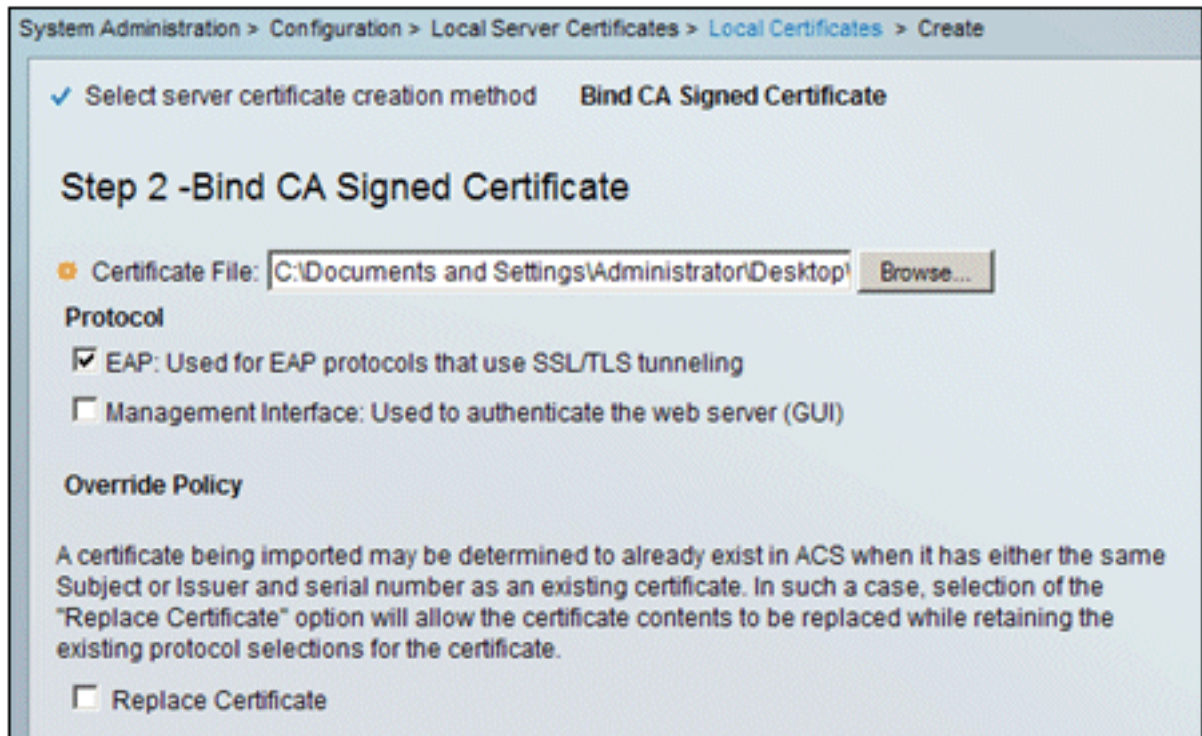
enregistré.

15. Choisissez le certificat ACS qui a été émis par le serveur AC, et cliquez sur

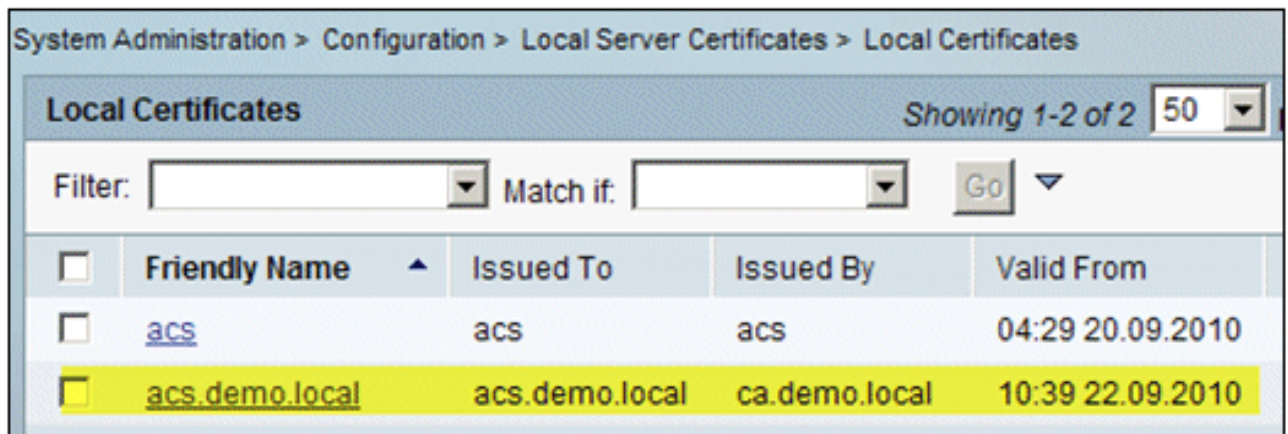


Open.

16. Cochez également la case Protocol pour **EAP**, puis cliquez sur **Finish**.



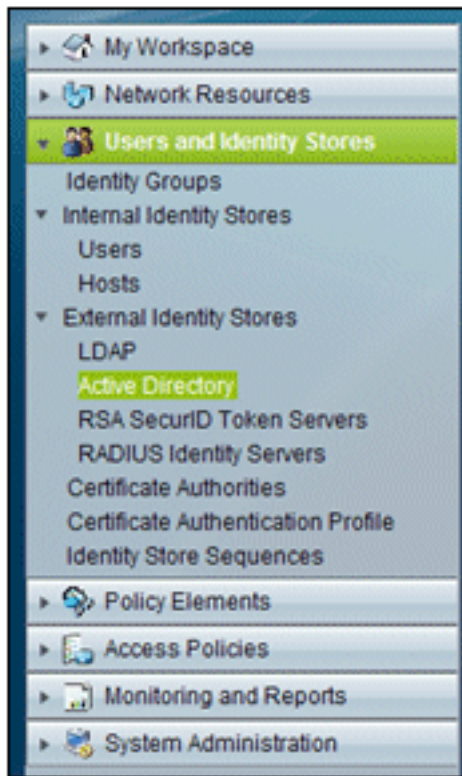
17. Le certificat ACS émis par l'autorité de certification apparaît dans le certificat local ACS.



[Configurer le magasin d'identités ACS pour Active Directory](#)

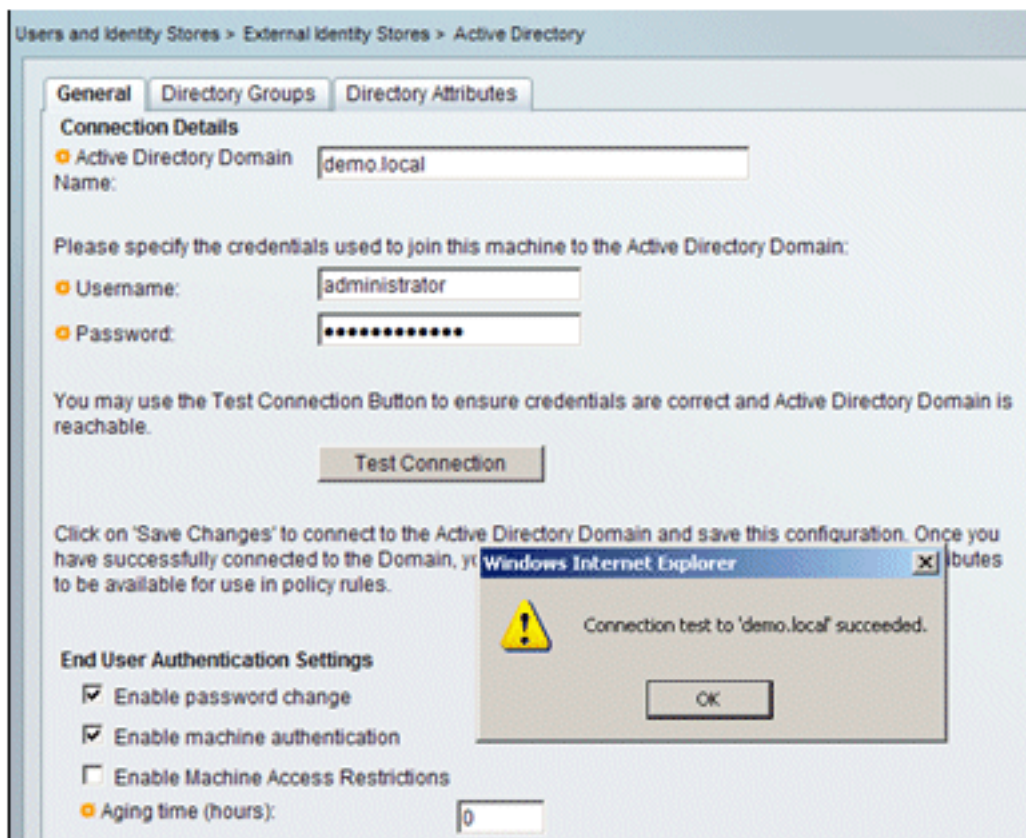
Effectuez les étapes suivantes :

1. Connectez-vous à ACS et connectez-vous avec un compte Admin.
2. Accédez à **Utilisateurs et magasins d'identités > Magasins d'identités externes > Active**



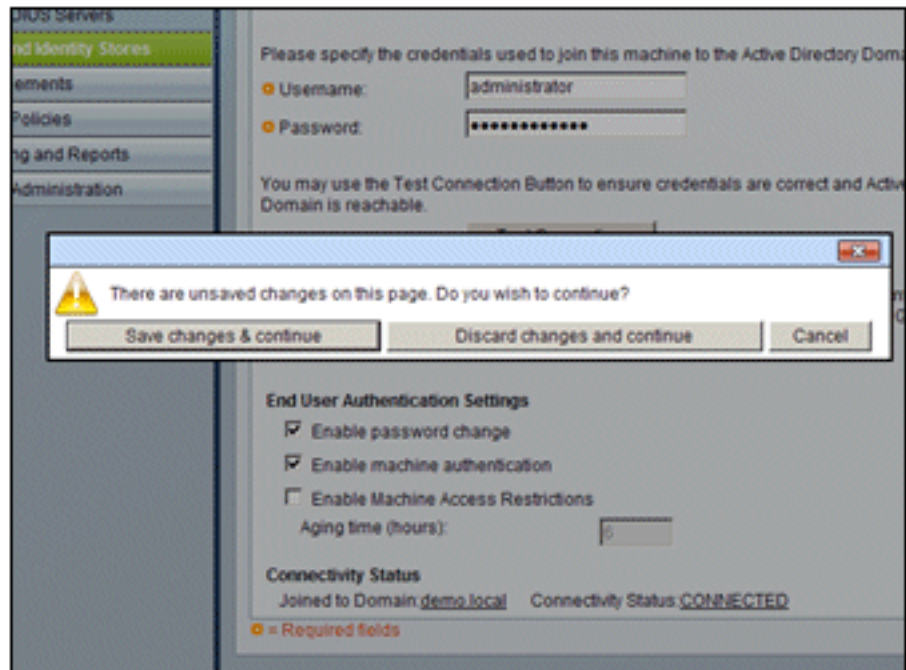
Directory.

3. Entrez le *demo.local* du domaine Active Directory, entrez le mot de passe du serveur et cliquez sur **Test Connection**. Cliquez sur **OK** afin de



continuer.

4. Cliquez sur **Enregistrer les**



modifications.

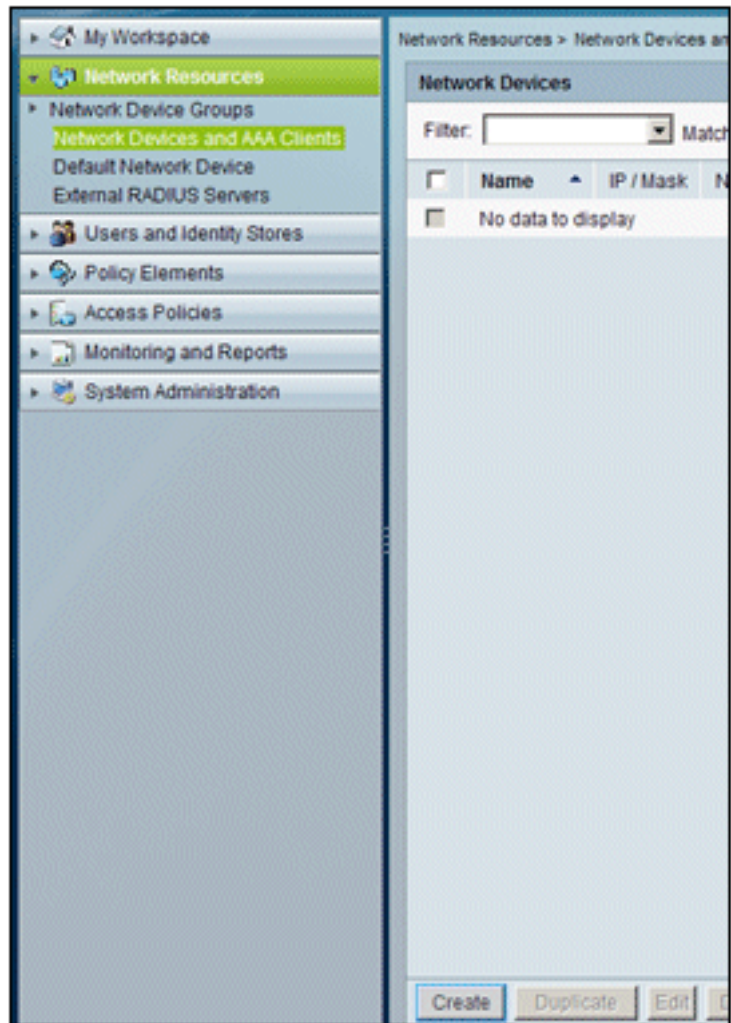
Remarque :

pour plus d'informations sur la procédure d'intégration d'ACS 5.x, reportez-vous à [ACS 5.x et versions ultérieures : Exemple de configuration de l'intégration avec Microsoft Active Directory](#).

Ajouter un contrôleur à ACS en tant que client AAA

Effectuez les étapes suivantes :

1. Connectez-vous à ACS et accédez à **Network Resources > Network Devices and AAA**



Clients. Cliquez sur **Create**.

2. Renseignez les champs suivants : Nom - **wlc** IP - **10.0.1.10** Case à cocher RADIUS - **Cochée** Secret partagé -

Network Resources > Network Devices and AAA Clients > Create

Name: Description:

Network Device Groups

Location:

Device Type:

IP Address

Single IP Address IP Range (s)

IP:

Authentication Options

TACACS+

Shared Secret:

Single Connect Device

Legacy TACACS+ Single Connect Support

TACACS+ Draft Compliant Single Connect Support

RADIUS

Shared Secret:

TrustSec

Use Device ID for TrustSec Identification

Device ID:

Password:

= Required fields

cisco

3. Cliquez sur **Submit** lorsque vous avez terminé. Le contrôleur apparaît sous la forme d'une entrée dans la liste des périphériques réseau ACS.

Network Resources > Network Devices and AAA Clients

Network Devices Showing 1-1 of 1

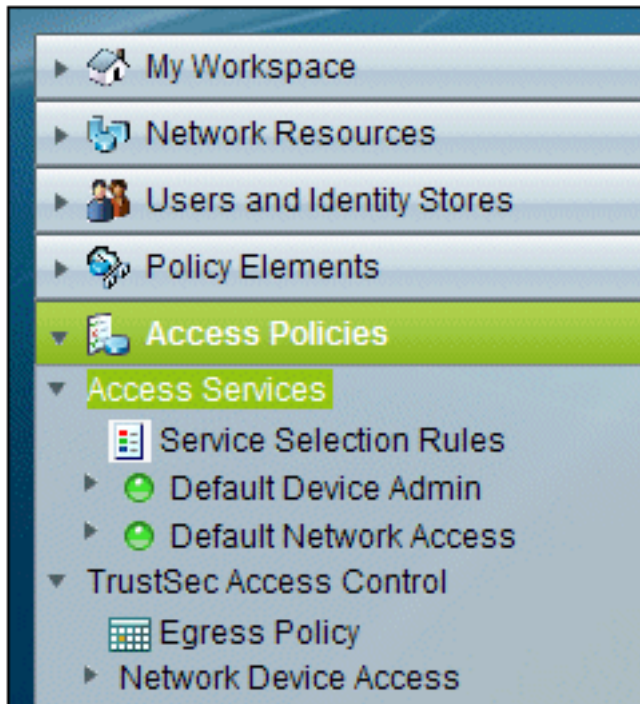
Filter: Match if:

<input type="checkbox"/>	Name	IP / Mask	NDG:Location	NDG:Device Type
<input type="checkbox"/>	wlc	10.0.1.10/32	All Locations	All Device Types

[Configuration des stratégies d'accès ACS pour les réseaux sans fil](#)

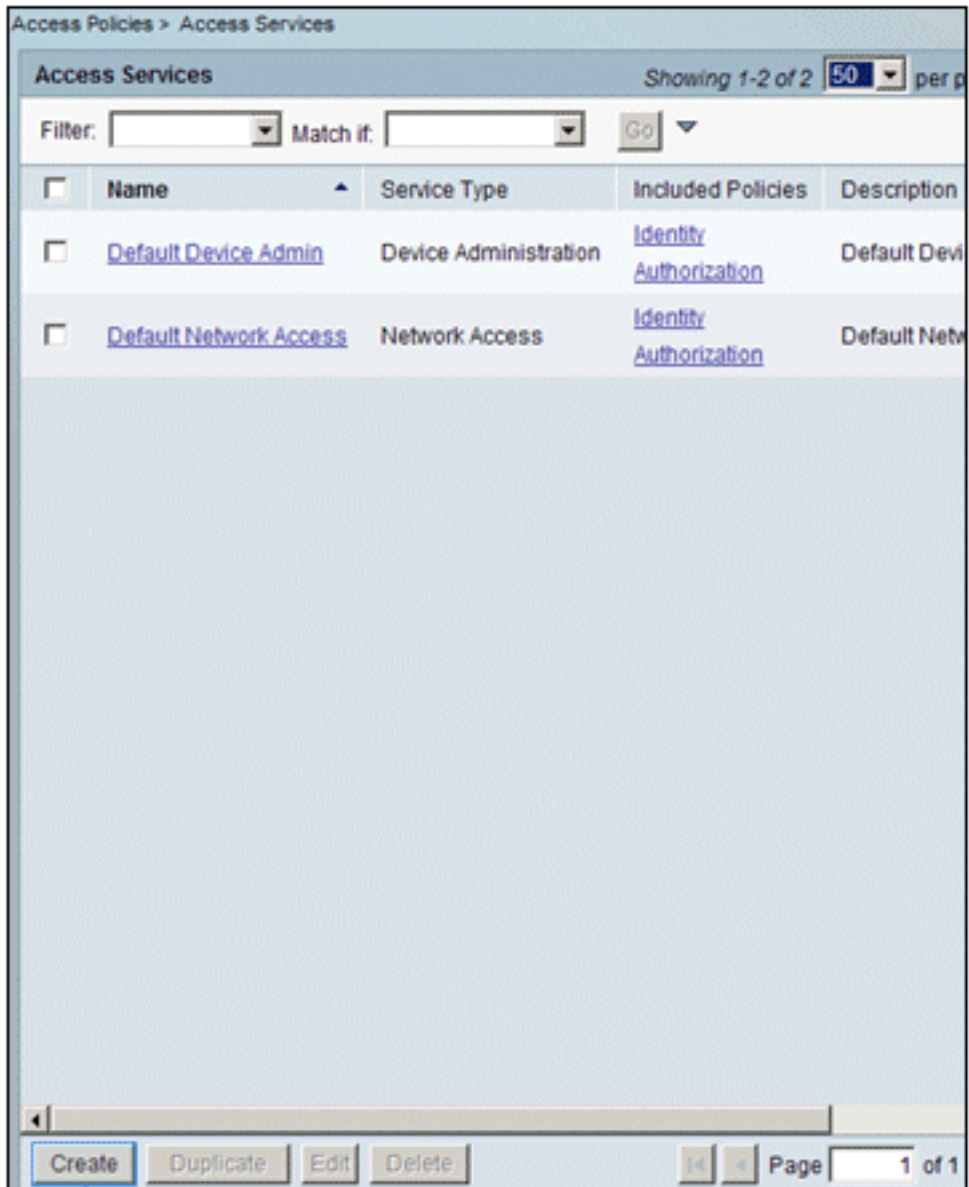
Effectuez les étapes suivantes :

1. Dans ACS, accédez à **Access Policies > Access**



Services.

2. Dans la fenêtre Access Services, cliquez sur



Create.

3. Créez un service d'accès et entrez un nom (par exemple WirelessAD). Choisissez **Basé sur**

le modèle de service, puis cliquez sur Sélectionner.

Access Policies > Access Services > Create

General Allowed Protocols

Step 1 - General

General

Name:

Description:

Access Service Policy Structure

Based on service template

Based on existing service

User Selected Service Type

4. Dans la boîte de dialogue Page Web, sélectionnez **Accès réseau - Simple**. Click OK.

Cisco Secure ACS -- Webpage Dialog

Access Services Showing 1-4 of 4

Filter: Match if:

	Name	Service Type	Description
<input type="radio"/>	Device Admin - Command Auth	Device Administration	
<input type="radio"/>	Device Admin - Simple	Device Administration	
<input type="radio"/>	Network Access - MAC Authentication Bypass	Network Access	
<input checked="" type="radio"/>	Network Access - Simple	Network Access	

5. Dans la boîte de dialogue Page Web, sélectionnez **Accès réseau - Simple**. Click OK. Une fois le modèle sélectionné, cliquez sur

Step 1 - General

General

Name:

Description:

Access Service Policy Structure

Based on service template

Based on existing service

User Selected Service Type

Next.

6. Sous Allowed Protocols, cochez les cases **Allow MS-CHAPv2** et **Allow PEAP**. Cliquez sur

Access Policies > Access Services > Create

✓ General **Allowed Protocols**

Step 2 - Allowed Protocols

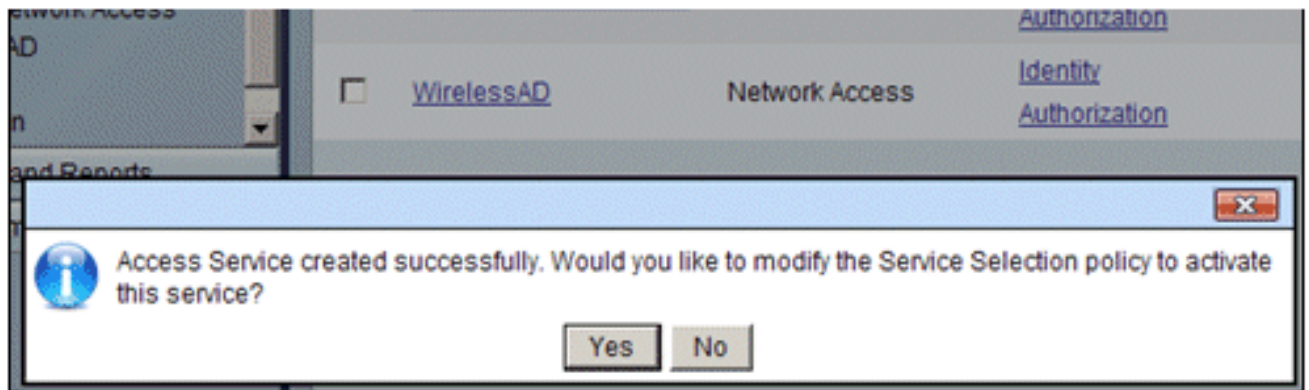
Process Host Lookup

Authentication Protocols

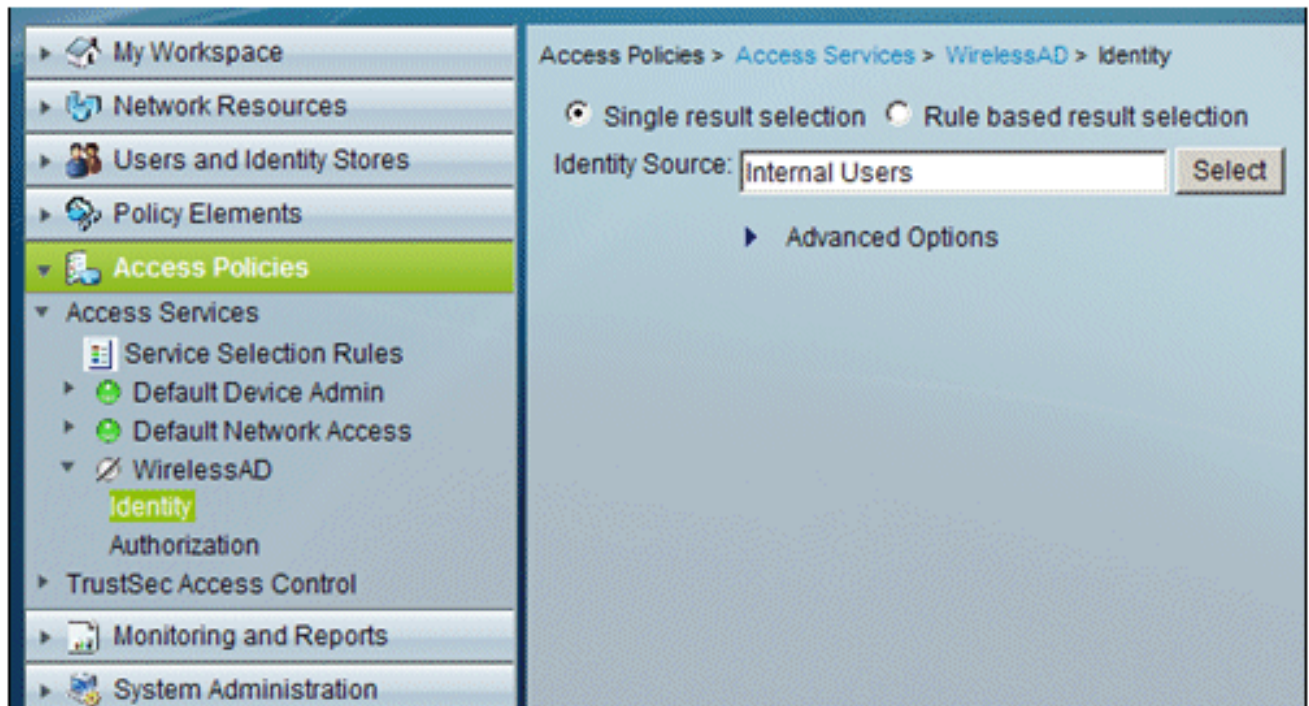
- Allow PAP/ASCII
- Allow CHAP
- Allow MS-CHAPv1
- Allow MS-CHAPv2
- Allow EAP-MD5
- Allow EAP-TLS
- Allow LEAP
- Allow PEAP
- Allow EAP-FAST

Finish (Terminer).

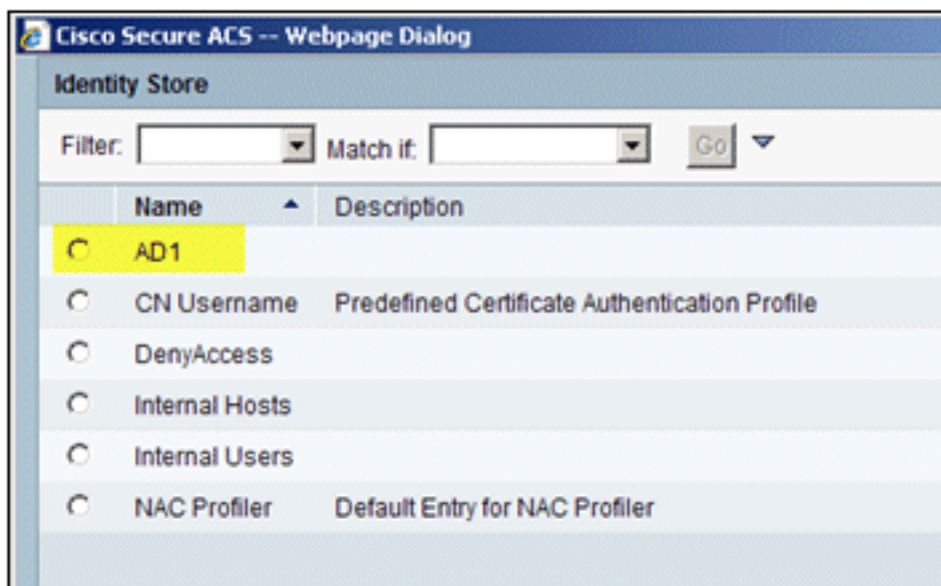
7. Lorsque ACS vous invite à activer le nouveau service, cliquez sur **Yes**.



8. Dans le nouveau service d'accès qui vient d'être créé/activé, développez et choisissez **Identity**. Pour la source d'identité, cliquez sur **Sélectionner**.



9. Choisissez **AD1** pour Active Directory qui a été configuré dans ACS, cliquez sur



OK.

10. Confirmez que la source d'identité est AD1 et cliquez sur **Save**

Access Policies > Access Services > WirelessAD > Identity

Single result selection
 Rule based result selection

Identity Source:

Changes.

Créer une stratégie d'accès ACS et une règle de service

Effectuez les étapes suivantes :

1. Accédez à **Access Policies > Service Selection Rules**.

Access Policies > Access Services > Service Selection Rules

Single result selection
 Rule based result selection

Service Selection Policy

Filter: Match if:

	<input type="checkbox"/>	Status	Name	Protocol	Cond
1	<input type="checkbox"/>	🟢	Rule-1	match Radius	
2	<input type="checkbox"/>	🟢	Rule-2	match Tacacs	

2. Cliquez sur **Créer** dans la fenêtre Politique de sélection de service. Attribuez un nom à la nouvelle règle (par exemple, *WirelessRule*). Cochez la case **Protocol** pour qu'il corresponde à **Radius**.

Cisco Secure ACS -- Webpage Dialog

General

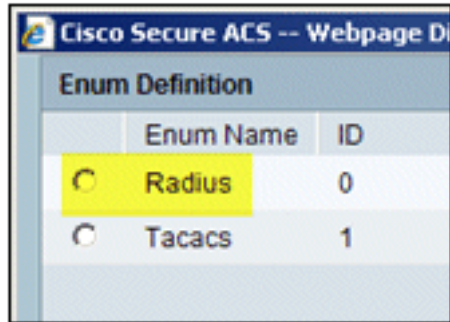
Name: Status: 🟢

Conditions

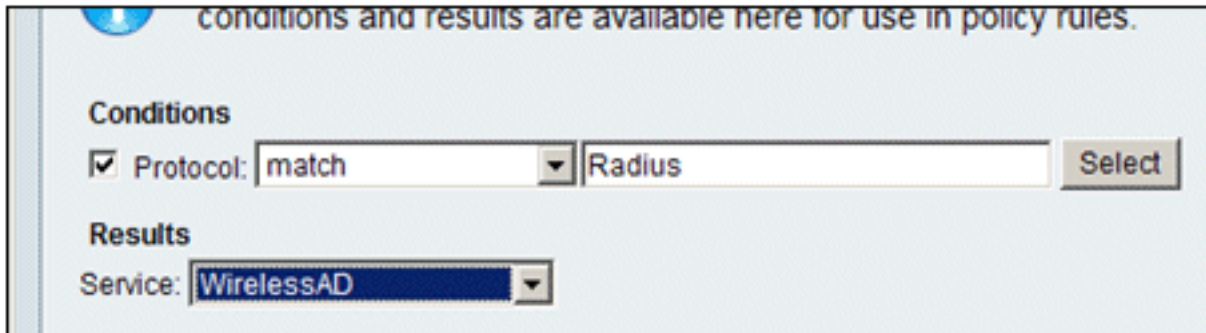
Protocol:

Results

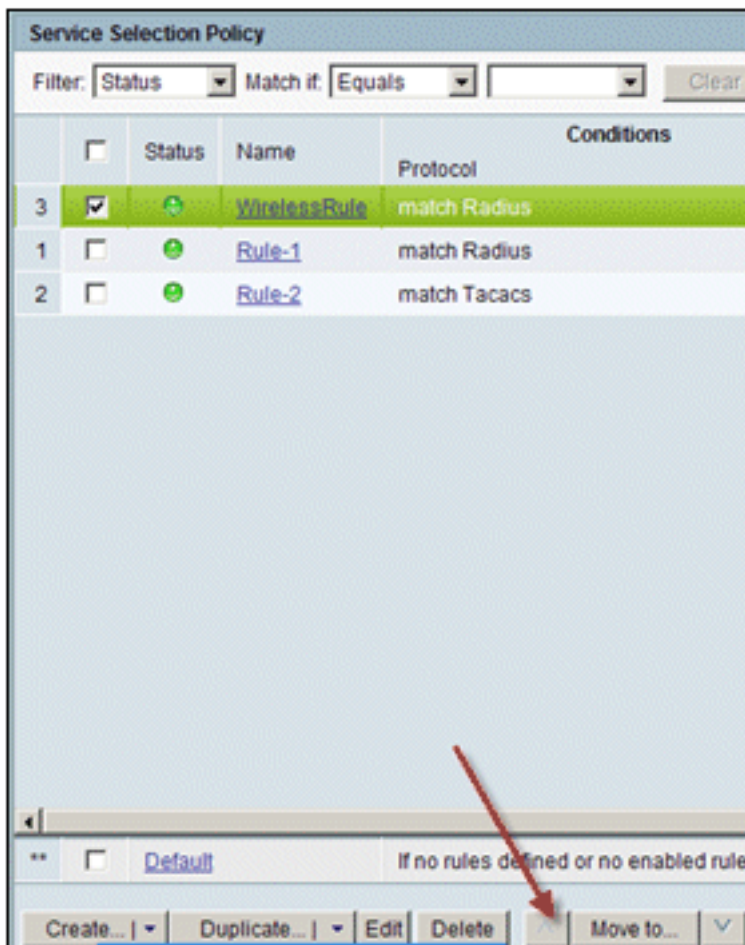
The Customize button in the lower right area of the policy rules screen conditions and results are available here for use in policy rules.



3. Choisissez **Radius**, puis cliquez sur **OK**.
4. Sous Results, choisissez **WirelessAD** for Service (créé à l'étape précédente).



5. Une fois la nouvelle règle sans fil créée, choisissez et **Déplacez** cette règle vers le haut, qui sera la première règle à identifier l'authentification radius sans fil à l'aide d'Active



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

Dans notre exemple, CLIENT est un ordinateur qui exécute Windows XP Professionnel avec SP qui agit comme un client sans fil et obtient l'accès aux ressources Intranet par le biais du 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

Effectuez les étapes suivantes :

1. Connectez le CLIENT au segment de réseau Intranet à l'aide d'un câble Ethernet connecté au concentrateur.
2. Sur CLIENT, installez Windows XP Professionnel avec SP2 en tant qu'ordinateur membre nommé CLIENT du domaine demo.local.
3. Installez Windows XP Professionnel avec SP2. Cette option doit être installée pour que le protocole PEAP soit pris en charge. **Remarque** : le Pare-feu Windows est automatiquement activé dans Windows XP Professionnel avec SP2. N'éteignez pas le pare-feu.

Installation de la carte réseau sans fil

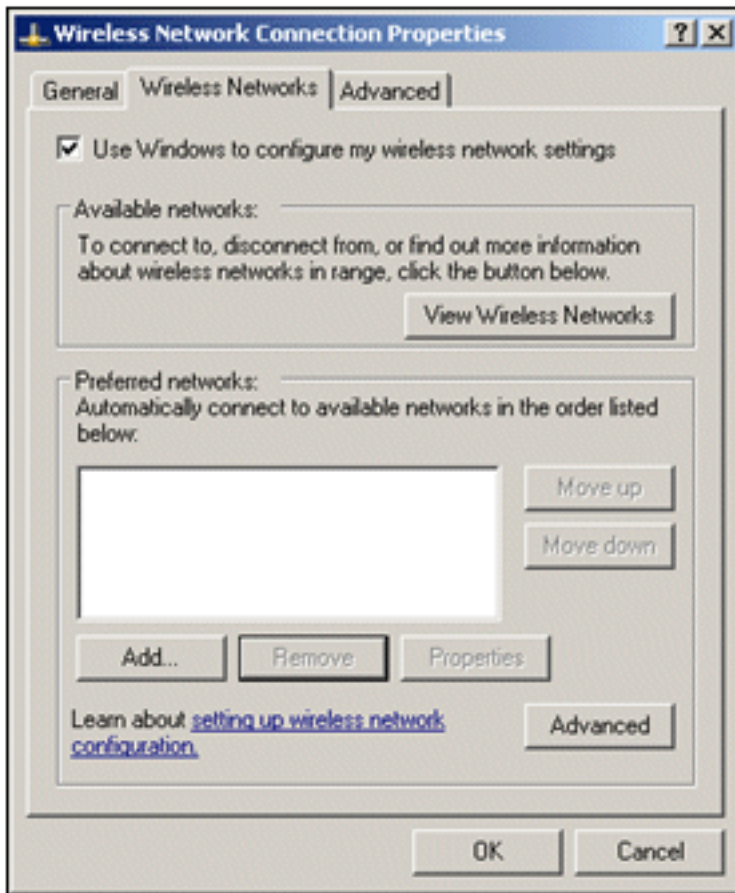
Effectuez les étapes suivantes :

1. Arrêtez l'ordinateur CLIENT.
2. Déconnectez l'ordinateur CLIENT du segment de réseau Intranet.
3. Redémarrez l'ordinateur CLIENT, puis ouvrez une session à l'aide du compte d'administrateur local.
4. Installez la carte réseau sans fil. **Remarque** : n'installez pas le logiciel de configuration du fabricant de la carte sans fil. Installez les pilotes de la carte réseau sans fil à l'aide de l'Assistant Ajout de matériel. Lorsque vous y êtes invité, fournissez également le CD fourni par le fabricant ou un disque contenant des pilotes mis à jour à utiliser avec Windows XP Professionnel avec SP2.

Configuration de la connexion réseau sans fil

Effectuez les étapes suivantes :

1. Déconnectez-vous, puis connectez-vous à l'aide du compte **WirelessUser** dans le domaine **demo.local**.
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 **Properties**, accédez à l'onglet **Wireless Networks** et vérifiez que la case à cocher **Use Windows to configure my wireless network settings** est

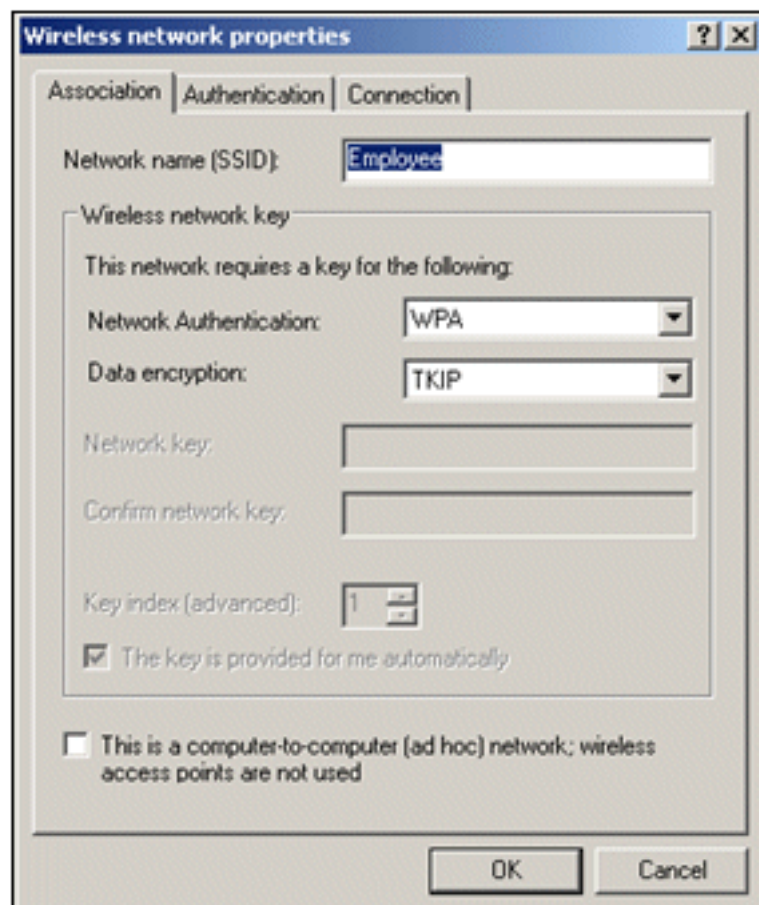


activée.

4. Cliquez sur **Add**.

5. Sous l'onglet Association, saisissez *Employee* dans le champ Network name (SSID).

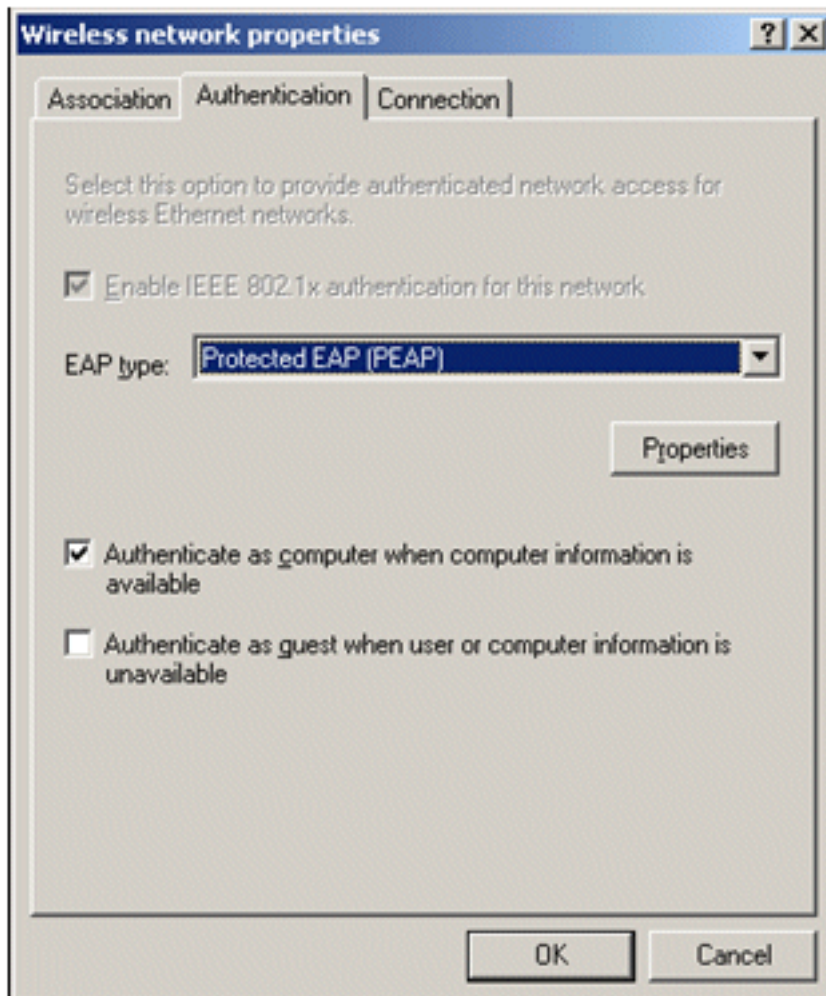
6. Choisissez **WPA** pour l'authentification réseau et assurez-vous que le cryptage des données



est défini sur TKIP.

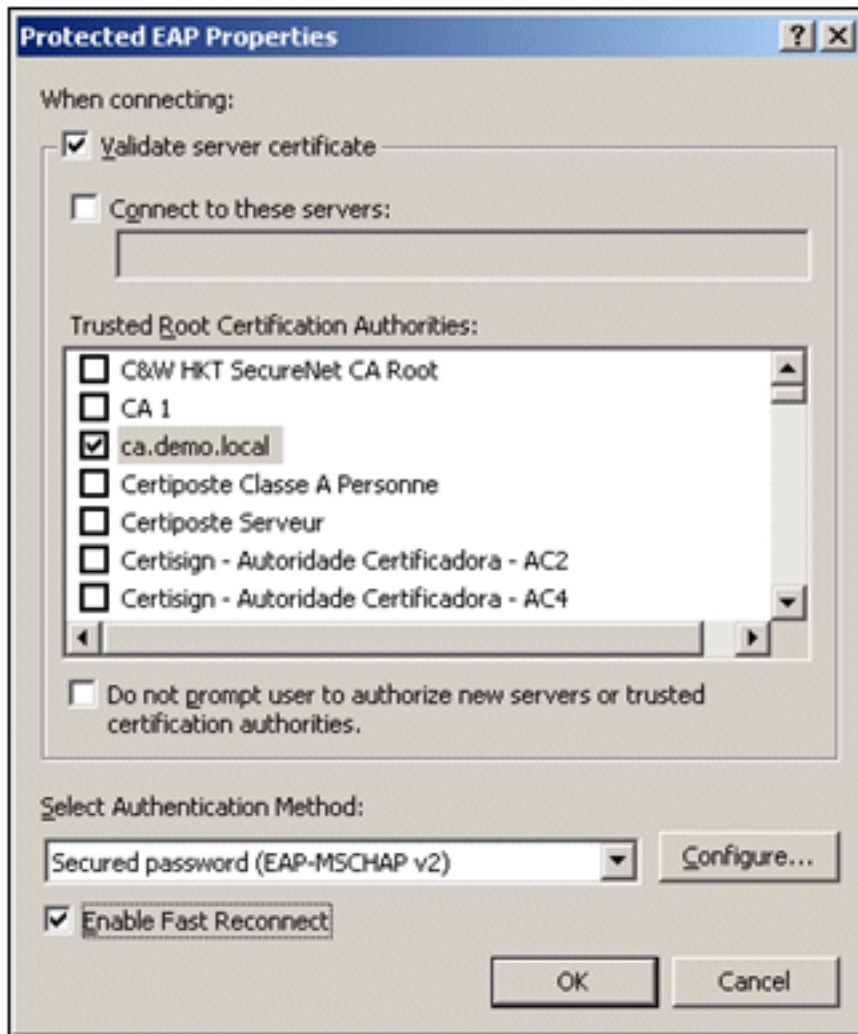
7. Cliquez sur l'onglet **Authentification**.

8. Vérifiez que le type EAP est configuré pour utiliser **Protected EAP (PEAP)**. Si ce n'est pas le cas, sélectionnez-le dans le menu déroulant.
9. Si vous souhaitez que l'ordinateur soit authentifié avant la connexion (ce qui permet l'application de scripts de connexion ou d'impulsions de stratégie de groupe), cochez la case **Authenticate as computer when computer information is**



available.

10. Cliquez sur **Properties**.
11. Comme le protocole PEAP implique l'authentification du serveur par le client, assurez-vous que le **certificat de serveur Validate** est vérifié. Assurez-vous également que l'autorité de certification qui a émis le certificat ACS est cochée dans le menu Autorités de certification racine de confiance.
12. Choisissez **Secured password (EAP-MSCHAP v2)** sous Authentication Method (Méthode d'authentification) car il est utilisé pour l'authentification



interne.

13. Assurez-vous que la case **Enable Fast Reconnect** est cochée. Cliquez ensuite trois fois sur **OK**.
14. Cliquez avec le bouton droit sur l'icône de connexion réseau sans fil dans Systray, puis cliquez sur **Afficher les réseaux sans fil disponibles**.
15. Cliquez sur le réseau sans fil Employé, puis sur **Connect**. Le client sans fil affiche **Connected** si la connexion réussit.

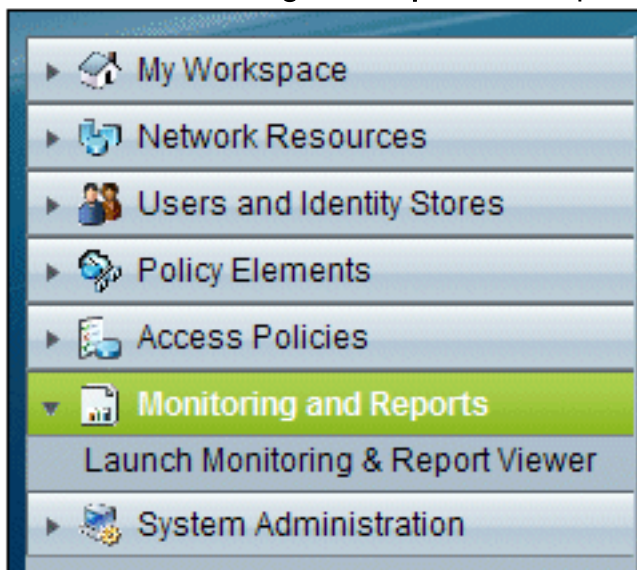


16. Une fois l'authentification réussie, vérifiez la configuration TCP/IP de la carte sans fil à l'aide de Connexions réseau. Elle doit avoir une plage d'adresses de 10.0.20.100 à 10.0.20.200 à partir de la portée DHCP ou de la portée créée pour les clients sans fil CorpNet.
17. Afin de tester la fonctionnalité, ouvrez un navigateur et accédez à <http://10.0.10.10> (ou l'adresse IP du serveur AC).

[Dépannage de l'authentification sans fil avec ACS](#)

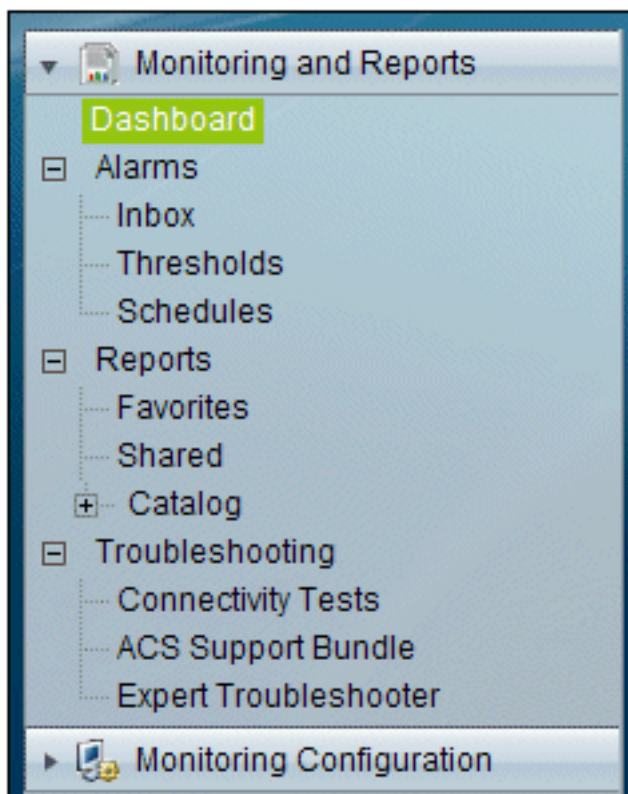
Effectuez les étapes suivantes :

1. Accédez à **ACS > Monitoring and Reports**, et cliquez sur **Launch Monitoring & Report**



Viewer.

2. Une fenêtre ACS distincte s'ouvre. Cliquez sur **Tableau de**



bord.

3. Dans la section Mes rapports favoris, cliquez sur **Authentications - RADIUS - Aujourd'hui**.

My Favorite Reports	
Favorite Name	Report Name
ACS - Configuration Audit - Today	ACS Instance>ACS_Configuration_Audit
ACS - System Errors - Today	ACS Instance>ACS_System_Diagnostics
Authentications - RADIUS - Today	AAA Protocol>RADIUS_Authentication

4. Un journal affichera toutes les authentifications RADIUS comme ayant réussi ou échoué. Dans une entrée enregistrée, cliquez sur l'icône de la loupe dans la colonne Détails.

AAA Protocol > RADIUS Authentication							
Authentication Status : Pass or Fail							
Date : September 22, 2010 (Last 30 Minutes Last Hour Last 12 Hours Today Yesterday Last 7 Days Last 30 Days)							
Generated on September 22, 2010 5:51:34 PM PDT							
Reload							
✔=Pass ✖=Fail 🔍=Click for details 🖱️=Mouse over item for additional information							
Logged At	RADIUS Status	NAS Failure	Details	Username	MAC/IP Address	Access Service	Authentication Method
Sep 22, 10 5:51:17.843 PM	✔		🔍	wirelessuser	00-21-5c-69-9a-39	WirelessAD	PEAP (EAP-MSCHAPv2)

5. RADIUS Authentication Detail fournit de nombreuses informations sur les tentatives

AAA Protocol > RADIUS Authentication Detail	
ACS session ID :	acs/74551189/31
Date :	September 22, 2010
Generated on September 22, 2010 5:52:16 PM PDT	
Authentication Summary	
Logged At:	September 22, 2010 5:51:17.843 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	wirelessuser
MAC/IP Address:	00-21-5c-69-9a-39
Network Device:	wlc : 10.0.1.10 :
Access Service:	WirelessAD
Identity Store:	AD1
Authorization Profiles:	Permit Access
CTS Security Group:	
Authentication Method:	PEAP(EAP-MSCHAPv2)

consignées.

6. Le nombre d'occurrences de service ACS peut fournir un aperçu des tentatives correspondant aux règles créées dans ACS. Accédez à **ACS > Access Policies > Access Services**, et cliquez sur **Service Selection**

Results	
Service	Hit Count
WirelessAD	33
Default Network Access	0

Rules.

[Échec de l'authentification PEAP avec le serveur ACS](#)

Lorsque votre client échoue à l'authentification PEAP avec un serveur ACS, vérifiez si vous trouvez le message d'erreur `NAS duplicated authentication try` dans l'option **Failed attempts** sous le menu **Report and Activity** de l'ACS.

Ce message d'erreur peut s'afficher lorsque Microsoft Windows XP SP2 est installé sur l'ordinateur client et que Windows XP SP2 s'authentifie auprès d'un serveur tiers autre qu'un serveur Microsoft IAS. En particulier, le serveur Cisco RADIUS (ACS) utilise une méthode différente de celle utilisée par Windows XP pour calculer l'ID EAP-TLV (Extensible Authentication Protocol Type:Length:Value format). Microsoft a identifié ceci comme un défaut dans le demandeur XP SP2.

Pour obtenir un correctif, contactez Microsoft et consultez l'article [L'authentification PEAP échoue lorsque vous vous connectez à un serveur RADIUS tiers](#). Le problème sous-jacent est que, côté client, avec l'utilitaire Windows, l'option de reconnexion rapide est désactivée par défaut pour PEAP. Cependant, cette option est activée par défaut côté serveur (ACS). Afin de résoudre ce problème, décochez l'option **Fast Reconnect** sur le serveur ACS (sous **Global System Options**). Vous pouvez également activer l'option **Fast Reconnect** côté client pour résoudre le problème.

Procédez comme suit afin d'activer la reconnexion rapide sur le client qui exécute Windows XP à l'aide de l'utilitaire Windows :

1. Accédez à **Démarrer > Paramètres > Panneau de configuration**.
2. Double-cliquez sur l'icône **Connexions réseau**.
3. Cliquez avec le bouton droit sur l'icône **Connexion réseau sans fil**, puis cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Wireless Networks**.
5. Choisissez l'option **Use Windows to configure my wireless network settings** afin d'activer Windows pour configurer la carte client.
6. Si vous avez déjà configuré un SSID, choisissez le SSID et cliquez sur **Properties**. Si ce n'est pas le cas, cliquez sur **New** afin d'ajouter un nouveau WLAN.
7. Saisissez le SSID sous l'onglet **Association**. Assurez-vous que l'authentification réseau est **ouverte** et que le cryptage des données est défini sur **WEP**.
8. Cliquez sur **Authentification**.
9. Sélectionnez l'option **Enable IEEE 802.1x authentication for this network**.
10. Sélectionnez **PEAP** comme type EAP, puis cliquez sur **Properties**.

11. Sélectionnez l'option **Enable Fast Reconnect** au bas de la page.

Informations connexes

- [PEAP sous des réseaux sans fil unifiés avec ACS 4.0 et Windows 2003](#)
- [Exemple de configuration du contrôleur LAN sans fil Cisco \(WLC\) et de Cisco ACS 5.x \(TACACS+\) pour l'authentification Web](#)
- [Guide d'installation et de mise à niveau de Cisco Secure Access Control System 5.1](#)
- [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.