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 <u>site Microsoft Wi-Fi</u> et le <u>plan d'action sans fil Cisco SAFE</u>.

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 : <u>Contrôleurs de réseau local sans fil de la gamme Cisco 4400</u> Pour l'installation initiale et les informations de configuration pour les contrôleurs de la gamme Cisco 2000, consultez le Guide de démarrage rapide : <u>Contrôleurs de réseau local sans fil de la gamme Cisco 2000</u>

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 <u>Authentification EAP-TLS</u> 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 <u>Mise à jour WPA2/Wireless Provisioning Services Information Element (WPS IE)</u> 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 <u>Conventions relatives aux conseils techniques Cisco.</u>

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 sousréseau 255.255.255.0.

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

- 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**.

abase and Log Folders Specify the folders to contain the Active Directory of	database and log file	s. 🔬
For best performance and recoverability, store the o hard disks.	database and the log	i on separate
Where do you want to store the Active Directory da	atabase?	
<u>D</u> atabase folder:		
C:\WINDOWS\NTDS		B <u>r</u> owse
Where do you want to store the Active Directory log	g?	
C:\WINDOWS\NTDS		Br <u>o</u> wse
< [Back <u>N</u> ext>	Cancel
	or best performance and recoverability, store the d ard disks. /here do you want to store the Active Directory da (atabase folder: C:\WINDOWS\NTDS /here do you want to store the Active Directory lo og folder: C:\WINDOWS\NTDS	or best performance and recoverability, store the database and the log ard disks. /here do you want to store the Active Directory database? (atabase folder: D:\WINDOWS\NTDS /here do you want to store the Active Directory log? og folder: D:\WINDOWS\NTDS

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

Active Directory Installation Wizard	×
Shared System Volume Specify the folder to be shared as the system volume.	
The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.	
The SYSVOL folder must be located on an NTFS volume.	
Enter a location for the SYSVOL folder.	
Eolder location:	
C:\WINDOWS\SYSVOL Browse	
< <u>B</u> ack <u>N</u> ext> Cancel	

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.

Active Directory Installation Wizard
Permissions Select default permissions for user and group objects.
Some server programs, such as Windows NT Remote Access Service, read information stored on domain controllers.
 Permissions compatible with pre-Windows 2000 server operating systems Select this option if you run server programs on pre-Windows 2000 server operating systems or on Windows 2000 or Windows Server 2003 operating systems that are members of pre-Windows 2000 domains. Anonymous users can read information on this domain. Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems
Select this option if you run server programs only on Windows 2000 or Windows Server 2003 operating systems that are members of Active Directory domains. Only authenticated users can read information on this domain.
< <u>B</u> ack <u>N</u> ext> Cancel

- 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**.

You chose to: The new domain name is example.com. This is also the name of the new forest. The NetBIOS name of the domain is EXAMPLE Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVOL The DNS service will be installed and configured on this computer. This computer will be configured to use this DNS server as its preferred DNS server. The password of the new domain administrator will be the same as the password of the administrator of this computer.	S ummary Review and confirm the options you selec	sted.
The new domain name is example.com. This is also the name of the new forest. The NetBIOS name of the domain is EXAMPLE Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVOL The DNS service will be installed and configured on this computer. This computer will be configured to use this DNS server as its preferred DNS server. The password of the new domain administrator will be the same as the password of the administrator of this computer. To change an option, click Back. To begin the operation, click Next.	You chose to:	
The NetBIOS name of the domain is EXAMPLE Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVOL The DNS service will be installed and configured on this computer. This computer will be configured to use this DNS server as its preferred DNS server. The password of the new domain administrator will be the same as the password of the administrator of this computer.	The new domain name is example.com. T	his is also the name of the new forest.
Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVOL The DNS service will be installed and configured on this computer. This computer will be configured to use this DNS server as its preferred DNS server. The password of the new domain administrator will be the same as the password of the administrator of this computer.	The NetBIOS name of the domain is EXA	MPLE
The DNS service will be installed and configured on this computer. This computer will be configured to use this DNS server as its preferred DNS server. The password of the new domain administrator will be the same as the password of the administrator of this computer.	Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVOL	_
The password of the new domain administrator will be the same as the password of the administrator of this computer.	The DNS service will be installed and cor will be configured to use this DNS server	nfigured on this computer. This computer as its preferred DNS server.
To change an option, click Back. To begin the operation, click Next.	The password of the new domain adminis the administrator of this computer.	trator will be the same as the password of
	To change an option, click Back. To beg	in the operation, click Next.

- 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

- 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

- 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.
- 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.	J.
Type a name and description for this scope. This information helps you quickly ident how the scope is to be used on your network.	ify
Name: CorpNet	
Description:	
<u>≺Back</u> <u>N</u> ext> 0	Cancel

7. Cliquez sur **Suivant** et remplissez les paramètres suivants :Adresse IP de début : 172.16.100.1Adresse IP de fin : 172.16.100.254Longueur : 24Masque 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. <u>Start IP address</u> : 172 . 16 . 100 . 1 <u>End IP address</u> : 172 . 16 . 100 . 254 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: 24
< <u>B</u> ack <u>N</u> ext ≻ Cancel

 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 address, type an address	e that you want to exclude. in Start IP address only.	If you want to exc	lude a single
<u>S</u> tart IP address: 172 . 16 . 100 . 1	End IP address:	A <u>d</u> d	
Excluded address range:			
		Remo <u>v</u> e	
I			
	< <u>B</u>	ack <u>N</u> ext)	Cancel

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
< <u>Back</u> <u>N</u> ext> Cancel

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

New Scope Wizard

Router (Default Gateway)

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



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	Wizar	ď
--	-----	-------	-------	---

Domain Name and DNS Servers

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



wrelessdemo.local		
e clients to use DNS serve	rs on your network, enter the IP	addresses for thos
	I <u>P</u> address:	
		Add
R <u>e</u> solve	172.16.100.26	Bemove
		Up
		Down
ť	e clients to use DNS serve	e clients to use DNS servers on your network, enter the IP IP address: IP address: IResolve I72.16.100.26

- 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.

New Scope Wizard
Activate Scope Clients can obtain address leases only if a scope is activated.
Do you want to activate this scope now?
No, I will activate this scope later
< <u>B</u> ack <u>N</u> ext> Cancel

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**.
- Sur la page Assistant Composants Windows, sélectionnez Services de certificats, puis cliquez sur Suivant.

You can add or remove components of Windows.	
To add or remove a component, click the checkbox part of the component will be installed. To see what Details.	k. A shaded box means that only t's included in a component, click
Components:	
🗹 📻 Accessories and Utilities	4.9 MB 🔺
☑	33.4 MB 💻
Certificate Services	1.4 MB
🔲 💻 E-mail Services	1.1 MB
Eax Services	7.9 MB 💻
Description: Installs a certification authority (CA) to public key security programs.	issue certificates for use with
Total disk space required: 3.4 MB	Details
Space available on disk: 1346.9 MB	100 and
Space available on disk: 1346.9 MB	<u>D</u> etails.

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

Windows Components Wizard	×
CA Type Select the type of CA you want to set up.	Ē
Enterprise root CA.	
C Enterprise subordinate CA	
Stand-alone root CA	
Stand-alone subordinate CA	
Description of CA type The most trusted CA in an enterprise. Should be installed before any other CA.	
Use custom settings to generate the key pair and CA certificate	
< <u>B</u> ack <u>N</u> ext> Cancel	Help

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.

ows Components Wizard	
Certificate Database Settings Enter locations for the certificate database, database log, and cor information.	nfiguration
<u>C</u> ertificate database:	
C:\WIND0WS\system32\CertLog	Br <u>o</u> wse
Certificate database log:	
C:\WINDOWS\system32\CertLog	Bro <u>w</u> se
Store configuration information in a shared folder Shared folder:	
	Browse
Preserve existing certificate database	

- 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

- 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 certificatsGérer CADemander des certificatsSi l'une de ces options est définie sur Refuser ou n'est pas sélectionnée, affectez la valeur Autoriser à l'autorisation.

relessdemoca Properties		?
General Policy Module Exit Mo Certificate Managers Restrictions Audi	odule Extension ting Recovery Ag	ns Storage gents Security
Group or user names:	10	
Administrators (WIRELESSDEMO)	Administrators)	
Authenticated Users		
🛛 🚅 Domain Admins (WIRELESSDEMC)\Domain Admins)	18 M
🕼 🕼 Enterprise Admins (WIRELESSDE)	40\Enterprise Admi	ins)
	Add	Remove (
Permissions for Administrators	Allow.	Deny
Read		
Issue and Manage Certificates		
Manage CA	N	
Request Certificates		
1		
) DK	Cancel	1 Applu

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 <u>Ajouter des utilisateurs au</u> <u>domaine</u>.

- 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**.

ew Object - Computer	x
Create in: wirelessdemo.local/Users	
Computer n <u>a</u> me:	
Client	
Computer name (pre-Windows 2000):	
CLIENT	
I he following user or group can join this computer to a domain.	
<u>U</u> ser or group: Defeatly Descein Adminent	1
Derauk: Domain Admins	
Assign this computer account as a pre-Windows 2000 computer	
Assign this computer account as a backup domain controller	
< <u>B</u> ack <u>N</u> ext >	Cancel

- 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 :

- 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

- 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**.
- 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	
<u>F</u> irst name:	WirelessUser <u>I</u> nitials:	
Last name:		
Full name:	WirelessUser	
<u>U</u> ser logon name:		
WirelessUser	@wirelessdemo.local 🔽	
User logon name (pre	- <u>W</u> indows 2000):	
WIRELESSDEMOV	WirelessUser	
	< <u>B</u> ack <u>N</u> ext ≻ Ca	incel

 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.

ew object - oser		
Create in: wirely	essdemo.local/Users	
<u>P</u> assword:	••••	
Confirm password:	••••	
User <u>m</u> ust change passw	ord at next logon	
User cannot change pas	sword	
Pass <u>w</u> ord never expires		
Account is disabled		
	< <u>B</u> ack <u>N</u> ext >	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

- 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**.
- 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.

New 0	bject -	Group
-------	---------	-------

Create in: wirelessder	mo.local/Users
Group n <u>a</u> me: WirelessUsers	
Group name (pre- <u>W</u> indows 2000): WirelessUsers	
Group scope	Group type
 Global Universal 	O <u>D</u> istribution
	OK Cancel

Étape 12: Ajouter des utilisateurs au groupe WirelessUsers

- 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.
- 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. Click OK.

Select Users, Contacts, Computers, or Groups	? X
<u>S</u> elect this object type:	
Users, Groups, or Other objects	<u>O</u> bject Types
<u>From this location:</u>	
wirelessdemo.local	Locations
Enter the object names to select (<u>examples</u>):	
wirelessuser	<u>C</u> heck Names
	_
<u>A</u> dvanced OK	Cancel

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

WirelessUsers Prope	rties	? ×
General Members	Member Of [Managed By]	
		1
<u>M</u> embers:	1	
Name	Active Directory Folder	
22 Administrator	wirelessdemo.local/Users	
🙎 WirelessUser	wirelessdemo.local/Users	
Add	<u>R</u> emove	
	OK Cancel	<u>A</u> pply

- 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

- 1. Répétez les étapes 1 et 2 de la section <u>Ajouter des utilisateurs au groupe d'utilisateurs sans</u> <u>fil</u> de ce document
- 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.

Select Users, Contacts, Computers, or Groups	? ×
<u>S</u> elect this object type:	
Users, Groups, or Other objects	<u>O</u> bject Types
<u>From this location:</u>	
wirelessdemo.local	Locations
Enter the object names to select (<u>examples</u>):	
client	<u>C</u> heck Names
<u>A</u> dvanced	OK Cancel

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

<u>? x</u>
;

- 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 <u>Guide d'installation de Cisco Secure ACS 4.0 pour Windows</u> pour plus d'informations sur la configuration de Cisco Secure ACS 4.0 pour Windows.

- Àl'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.

- 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.Click 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 Remargue : 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 contrôlées 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 <u>Guide de l'utilisateur de Cisco Secure ACS pour Windows Server, version</u> <u>4.0</u>. 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





- 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.
- Configurez les informations comme le montre la fenêtre Interfaces > Edit.

LISCO SYSTEMS					
allo allo.	MONITOR WUNNS CONTR	OLLER WIRELESS SECURITY			
Controller	Interfaces > Edit				
General Inventory	General Information				
Interfaces	Interface Name en	nployee			
Internal DHCP Server	Interface todace				
Mobility Management Mobility Groups Mobility Statistics Ports Master Controller Mode Network Time Protocol QoS Profiles	VLAN Icentifier IP Address Netmask Gateway Physical Information Port Number DHCP Information	20 172.16.100.4 255.255.255.0 172.16.100.1			
	Primary DHCP Server Secondary DHCP Server Access Control List	172.16.100.25 0.0.0.0			
	ACL Name	none 💙			

- 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.

 $\mathsf{WLANs} > \mathsf{Edit}$

WLAN ID	1				
WLAN 5510	Employee				
Ceneral Policies		Security Policies			
Radio Policy			wata 😡		
Admin Status	Enabled	Luyer 2 Sebundy			
Session Timeout (secs)	1830				
Quality of Scrvics (QoS)	Silver (best offort)	Layer 3 Security	Моге 💌		
WMM Policy	Disabled 🛩		Web Policy "		
7920 P ione Support	🔲 Client CAC Limit 🔄 🗛 CAC Limit				
Broaccast SSID	💌 Enabled				
Allow AAA Override	Enab ed	* Web Policy cannot be used in combination with IPsec and L2TP.			
Client Exclusion	Llient Exclusion 🛛 🗹 Enabled 🏘 60 Timeout Value (secs)		** When plicht exclusion is enabled, a timpout value zero means infinity (will require administrative overhi		
DHCP Server	Overrido 🗌	reset excluded clierts)	É .		
DI CP Addr. Assignment	Required				
Interface Name	emplayee 🔽				
Radius Servers					
	Authentication Servers Accounting Servers				
Server 1	TP:172.16.100.25, Port:1812 💙 none 👽				
Server 2	rone 💌 none 🔽				
Server 3	rone 💙 none 🛩				
WPA2 Parameters					
WPA Compatibility Mode	Encolo				
Allow WPA2 TKIF Clients	🕑 Enable				
Pre-Shared Key	📃 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.

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

CIRCO SYNTEMS					
adha adha	MONITOR WLANS (CONTROLLER	WIRELESS	SECURITY	
Security	RADIUS Authentication Servers > New				
AAA General	Server Index (Priorit	ty) 1	1		
RADIUS Authentication RADIUS Accounting Local Net Users	Server IPAddress	172.1	16.100.25		
MAC Filtering Disabled Clients	Keys Format	ASC	II v		
AP Policies	Shared Secret	••••	••		
Access Control Lists Web Auth Certificate	Confirm Shared Secret	••••	••		
Wireless Protection Policies	Key Wrap				
Rogue Policies Standard Signatures	Port Number	1812			
Custom Signatures Client Exclusion Policies AP Authentication	Server Status	Enab	led 💙		
	Support for RFC 357	6 Enab	led ⊻		
	Retransmit Timeout	2	seconds		
	Network User	E E	inable		
	Management	E 6	nable		



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

- 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

🐹 certtmpl - [Certificate Temp	lates]				٦×
Eie Attion Yiew Window	Н∘р			فلم	1×
← → 🛄 🖺 😂 🕃	Tenniate Dimiau Nama 17	Minimum Suprovided Tite	Verdoo	Autoenrelinent	
Contracto relipiocos	The project of the second seco	Windows 2000	8.1	Not allowed	
	Str CA Exchange	Windows Server 2003 Ep	106.0	Vot allowed	
	Sector Country of	Windows 2000	4.1	Not allowed	
	BalCode Singing	Wind we 2000	3.1	Not allowed	
	Bacomputer	Windows 2000	5.1	Not allowed	
	GO Cross Certification & thority	Windows Server 2003 Fr	105.0	Vot allowed	
	PDEMOACS	Windows Server 2000, En.	100.2	Not allowed	
	Structury Email Rankration	Windows Server 2003 Fn.	1.20	allowed	
	Solution and controller	Windows 2000	4.1	Not allowed	
	Domain Controlor Authenciestion	Windows Server 2003 En	1:00	Allowed	
	BOFFS Recovery Acent	Windows 2000	6.1	Not allowed	
	Secondare it Avent	Windows 2000	4.1	Not allowed	
	Steprolment Agent (Computer)	Windows 2000	5.1	Vot allowed	
	EXExchange Enrolment Agent (Offline request)	Windows 2000	4.1	Vot allowed	
	Exchange Signature On v	Windows 2000	6.1	Not allowed	
	BEyrhange Iser	Windows 2000	7.1	Not allowed	
	(Millesec)	Windows 2000	8.1	Not allowed	
	2010 Sec (Offine request)	Windows 2000	7.1	Not allowed	
	Key Recovery Acent	Windows Server 2003 En	105.0	Allowed	
	BRAS and IAS Server	Windows Server 2003 En	101.0	Allowed	
	Roo: Certification Authority	Windows 2000	5.1	Not allowed	
	Router (Offline request)	Wincows 2000	4.1	Not allowed	
	Smartcard Logon	Wincows 2000	6,1	Not allowed	
	Smartcard User	Wincows 2000	11.1	Not allowed	
	Suburdinate Certification Authority	Wilcows 2000	5.1	Not allowed	
	Trust List Signing	Wincows 2000	3.1	Not allowed	
	GigUser	Wincows 2000	3.1	Not allowed	
	User Signature Only	Wincows 2000	4.1	Not allowed	
	Wigh Same	Wincows 2000	4.1	Not allowed	
	Dypicate Templa:e	Wincows Server 2003, En	1.0.3	Alowed	
	Wi al tasks late	Wincows Server 2003, En	101.0	Alowed	
		Wipcows Server 2003, En	101:0	Alowed	
	Properties			17192425	1

Créer le modèle de certificat pour le serveur Web ACS

- 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 Ten | nplate | | ?) |
|-------------------------------|-------------------------------------|------------------------|----------|
| Issuance Requirement | s Superseded Templates | Extensions 9 | Gecurity |
| Lieneral | Request Handling | Subject Nar | me |
| T <u>e</u> mplate display nam | e: | | |
| Copy of Web Server | | | 8 |
| Minimum Supported C | As: Windows Server 2003, E | nterprise Edition | |
| After you apply chang | es to this tab, you can no long | ier change the ter | mplate |
| name. | | , | 1 |
| Template name: | | | |
| Copy of Web Server | (| | |
| Validity period:
2 years | Renewal period:
6 weeks | | |
| Eublish certificate | in Active Directory | | |
| 🗖 Do not automa | atically reenroll if a duplicate ce | artificate exists in A | Active |
| Directory | | | |
| | | | |
| | | | |
| | OK C | ancel 🛛 👌 | pply |
| | | | |

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

		2 52
Issuance Requirements	Superseded Templates	Extensions Sec
General	Request Handling	Subject Name
Template display name		
JACO		
Minimum Supported C4	As: Windows Server 2003, E	Interprise Edition
After you apply change	es to this tab, you can no long	ger change the templ
name.		
Template name:		
ACS		
Validity period:	<u>R</u> enewal period	: •
Validity period: 2 years ▼	<u>R</u> enewal period	t T
Validity period: 2 years ▼	Benewal period	t T
Validity period: 2 years ▼ Publish certificate i	Benewal period	t T
Validity period: 2 years ▼ Bublish certificate i	Enewal period	
Validity period: 2 years ▼ Eublish certificate i Do not automat	<u>R</u> enewal period 6 weeks in Active Directory tically reenroll if a duplicate o	t The second sec
Validity period: 2 years ▼ Eublish certificate i Do not automat Directory	Enewal period 6 weeks in Active Directory tically reenroll if a duplicate o	t Tertificate exists in Acti
Validity period: 2 years ▼ Publish certificate i Do not automat Directory	Enewal period 6 weeks in Active Directory tically reenrol if a duplicate o	t Tertificate exists in Acti
Validity period: 2 years ▼ Do not automat Directory	Enewal period 6 weeks in Active Directory tically reenroll if a duplicate of	t The state exists in Acti
Validity period: 2 years ▼ Eublish certificate i Do not automat Directory	Enewal period 6 weeks in Active Directory tically reenrol if a duplicate o	t ertificate exists in Acti

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

Issuance Requirem	ents Superseded Templates	Extensions Securi
General	Request Handling	Subject Name
Eurpose:	Signature and encryption	
Γ	Archive subject's encryption	private key
Γ	Include symmetric algorithms	allowed by the subject
Г	Delete revoked or expired oe	rtificates (do not archive)
Minimum key size:	1024	
Allow private k	eu to be evoorted	
and the part part and the	.,	
Do the following w associated with thi	hen the subject is enrolled and s certificate is used:	when the private key
🖲 Enroll subject (without requiring any user input	
C Prompt the use	ar during enrollment	
C Prompt the use	er during enrollment and require used	user input when the
 private key is u 		
To choose which (CSPs) should be u	cryptographic service providers used, click CSPs.	<u>C</u> SPs

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

Issuance Requirements Superseded Template	s Extensions Securit
General Request Handling	Subject Name
SP Selection	? 1
Choose which cryptographic service providers (requests:	CSPs) can be used in
C <u>R</u> equests can use any CSP available on the	e subject's computer
Requests must use one of the following CSF	D _S
CSPs:	
 Gemplus GemSAFE Card CSP v1.0 Infineon SICRYPT Base Smart Card CSP Microsoft Base Cryptographic Provider v1.0 Microsoft Base DSS and Diffie-Hellman Cryp Microsoft DH SChannel Cryptographic Provider Microsoft Enhanced Cryptographic Provider Microsoft Enhanced DSS and Diffie-Hellman Microsoft Enhanced RSA and AES Cryptographic Provider Microsoft BSA SChannel Cryptographic Provider 	tographic Provider der v1.0 Cryptographic Prov aphic Provider
OK	Cancel

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

Issuance Requirement	nts Superseded Templates	Extensions Securit
General	Request Handling	Subject Name
 Supply in the red Select this option not have access Autoenrollment i <u>B</u>uild from this Autoention 	uest n to allow a variety of subject i s to the domain of which the si s not allowed if you choose thi ctive Directory information to enforce consistency among	name formats or if you do ubject is a member. is option. g subject names and to
simplify certificate Subject name for	administration. mat:	
None		-
🔲 🗖 Include e-mai	I name in subject name	
Include this inform	nation in alternate subject nam	ie:
🔲 🔚 E-mail name		
DNIS momo		
Dive name	I nome (LIPM)	
□ <u>D</u> No name □ <u>□</u> <u>U</u> ser prinicipa	i name (or ni)	
☐ <u>U</u> ser prinicipa ☐ Ser <u>v</u> ice princi	pal name (SPN)	
☐ <u>U</u> ser prinicipa ☐ Ser <u>v</u> ice princi	pal name (SPN)	
☐ <u>U</u> ser prinicipa ☐ <u>U</u> ser prinicipa ☐ Ser <u>v</u> ice princi	pal name (SPN)	

- 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

	35	?
General Request Har	ndling S	ubject Name
Issuance Requirements Superseded	d Templates Exter	nsions Security
<u>G</u> roup or user names:		
🙍 Administrator (WIRELESSDEMO	\Administrator)	
🕵 Authenticated Users		
🗩 Domain Admins (WIRELESSDEN	40 \Domain Admins)	
Strate Prise Admins (WIRELESSD)	EMO\Enterprise Adn	nins)
 Here is a second of the second s		
	Add	<u>R</u> emove
	1 AL AL	
Permissions for Domain Admins	Allow	Deny
Permissions for Domain Admins	Allow	Deny
Permissions for Domain Admins Full Control Read	Allow	
Permissions for Domain Admins Full Control Read Write	Allow D V M	 Deny
Permissions for Domain Admins Full Control Read Write Enroll	Allow C V V V V	
Permissions for Domain Admins Full Control Read Write Enroll Autoenroll	Allow	
Permissions for Domain Admins Full Control Read Write Enroll Autoenroll	Allow	
Permissions for Domain Admins Full Control Read Write Enroll Autoenroll	Allow Allow Ø Ø O d settings.	
Permissions for Domain Admins Full Control Read Write Enroll Autoenroll For special permissions or for advance click Advanced.	Allow Allow I I I I I I I I I I I I I I I I I I I	Deny
Permissions for Domain Admins Full Control Read Write Enroll Autoenroll For special permissions or for advance click Advanced.	Allow Allow M M M M M M M M M M M M M	Deny

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.

	B. C. Market B. C. M	
General Issuence Requirement	Request Handling	Subject Name
issuance mequilement	 Londerseded Lemplates 	Extensions Security
Require the following	for enrollment:	
🔲 CA certificate mar	nager approval	
This number of au	thorized signatures:	—)
	- 12	
If you require mor	e than one signature, autoer	rollment is not allowed.
Policy type require	ed in signature:	
I		<u></u>
Application policy		
l		<u> </u>
Issuance policies:		
		A <u>d</u> d
		Bemove
Require the following	for reenrollment:	
Same criteria as fr	or enrolment	
C Valid existing certi	ficate	

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 :

 Ouvrez le composant logiciel enfichable Autorité de certification. Suivez les étapes 1 à 3 de la section <u>Créer le modèle de certificat pour le serveur Web ACS</u>, choisissez l'option Autorité de certification, choisissez Ordinateur local et cliquez sur Terminer.

Cert	tification Authority		×
	Select the computer you wa This snap-in will always ma © Local computer: (the © Another computer:	nt this snap-in to manage. mage: computer this console is running on)	Browse
l	Allow the selected co	mputer to be changed when launching from the co	mmand line. This
	only applies if you say	re the console.	
-		< Back Finis	h Cancel

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

Console Root\Certification Authority (Local)\wirelessdemoca\Certificate Templates	Templates.	<u>Window II</u> elp		
Console Root Name Intended Purpose Certification Authority (Local) Wireless I Iser Certificare Template Client A thentication, Server Email Replication Revoled Certificates Diractory Email Replication Directory Servee Email Replication Revoled Certificates Domain Controller Authonitication Directory Servee Email Replication Pending Requests Domain Controller Directory Servee Email Replication Paied Requests Domain Controller Encrypting File System Vew Window from Here Subordinate Certification Authority Certification Authority Vew Taskpad View Refresh Reprot List Help Export List Help	 ⇒ ⇒ È II ⇒ E E Console Root\Certification Console Root Console Root Certification Authority (Loc Pending Revolved Certificates Pending Requests Faied Requests Pending Requests Faied Requests Vew Wind Vew Wind Vew Task Refresh Export Lis 	Jthority (Local) wireless democal Certificate Template Name Wireless Use: Certificate Template Diractory Email Replication Domain Controller Authentication ECFS Recovery Agent Domain Controller Web Server Certificate Template to Issue Wireless Use: Certification Authority Model Server Certificate Template to Issue Subordinate Certification Authority Administrator	plates Intended Purpose Intended Purpose Client Authentication, Service Email, Encry, Directory Service Email Replication Client Authentication, Server Authentication - File Recovery Encrypting File System Client Authentication, Server Authentication Server Authentication Client Authentication, Server Authentication Encrypting File System, Secure Email, Clien (All) Nicrosoft Trust List Signing, Encrypting File	

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

Enable Certificate Templates

Select one or more Certificate Templates to enable on this Certification Authority

Name	Intended Purpose	-
ACS .	Server Authentication	
Authenticated Session	Client Authentication	
🙀 CA Exchange	Private Key Archival	
CEP Encryption	Certificate Request Agent	
😹 Code Signing	Code Signing	
Cross Certification Authority	KAID	
DEMOACS	Server Authentication	
Enrolment Agent	Certificate Request Agent	
🗱 Enrolment Agent (Computer)	Certificate Request Agent	
Exchange Enrollment Agent (Offline request)	Certificate Request Agent	
Exchange Signature Only	Secure Email	5

- 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 le **domaine wirelessdemo.local**, puis cliquez sur

? X

langle Active Direct	ory Users and Comp	iters		
Ile Action	<u>V</u> iew <u>W</u> indow <u>H</u> e	lp		
⇔ → 1 €	3 💼 🖆 🔂 🕾	😫 🦉	📅 造	746
🧳 Active Directo	ory Users and Computer	wirelessder	no.local	5 objects
🗄 🦲 Saved Qu	eries	Name		Туре
	Delegate Control Find Connect to Domain Connect to Domain Cor Raise Domain Function Operations Masters New All Tasks View New Window from Here	ntroller al Level	s pnt cur	builtinDomain Container Organizational . Container Container
	Export List			
	Properties			
	Help			
			_	

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

General Manage	ed By Group Po	olicy		
To improve Grou Management Co	ip Policy manage nsole (GPMC). ent Group Policy	ment <u>jungrade</u> it Object Links for	o the Group Po r wirelessdemo	olicy
Group Policy O	bject Links	Y	No Override	Disabled
S Default Dor	nain Policy			
14 - 18 1				
Group Policy Ob This list obtained <u>N</u> ew	iects higher in the I from: cisco_w20 Add	e list have the hi 103.wirelessdem Edit	ghest priority. o.local	Up
Group Policy Ob This list obtained <u>N</u> ew	iects higher in the from: cisco_w20 	e list have the hi 103.wirelessdem <u>E</u> dit	ghest priority. o.local	∐р
Group Policy Ob This list obtained <u>N</u> ew <u>Options</u>	iects higher in the from: cisco_w20 A <u>d</u> d Dele <u>t</u> e	e list have the hi 103.wirelessdem <u>E</u> dit <u>P</u> roperties	ghest priority. o.local	<u>U</u> p Do <u>w</u> n
Group Policy Ob This list obtained <u>N</u> ew <u>Options</u>	iects higher in the from: cisco_w20 <u>Add</u> Dele <u>t</u> e inheritance	e list have the hi 103.wirelessdem <u>E</u> dit <u>P</u> roperties	ghest priority. o.local	Up Do <u>w</u> n

- s'ouvre.
- 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.

🚡 Group Policy Object Editor			
File Action <u>V</u> iew <u>H</u> elp			
← → 🖻 💽 🛃 😫			
 Default Domain Policy [cisco_w2003.wirel Computer Configuration Software Settings Windows Settings Scripts (Startup/Shutdown) Security Settings Security Settings Security Settings Coal Policies Coal Policies System Services System Services System Site System Wireless Network (IEEE 8 Public Key Policies 	essdemo.local] P 02.11) Policies n	olicy	Automatic Certificate Request A There are r
- Automatic Certificat	<u>N</u> ew	•	Automatic Certificate Request
	⊻iew	•	
E Software Restriction Po E Software Restriction Po E Administrative Templates	Refresh Export List		
 User Configuration Software Settings Windows Settings Administrative Templates 	Help		

- 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**.

provided. A certificate template is a set of pre-	defined properties for certificates issued to
ertificate templates:	The noncovaring inset.
Name	Intended Purposes
Lomputer Domain Controller Enrollment Agent (Computer) IPSec	Client Authentication, Server Authenticati Client Authentication, Server Authenticati Certificate Request Agent IP security IKE intermediate
•	

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.

Group Policy Object Editor	
Eile Action View Help	
 Default Domain Policy [cisco_w2003.wirelessdemo.local] Policy Computer Configuration Software Settings Windows Settings Scripts (Startup/Shutdown) Security Settings Security Settings Coal Policies Event Log Restricted Groups System Services System Services System Services Sight Pile System Wireless Network (IEEE 802.11) Policies 	Automatic Certificate Request
Encrypting File System	
Enterprise Trust	

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

🚡 Group Policy Object Editor	
<u>File Action View Help</u>	
 Default Domain Policy [cisco_w2003.wirelessdemo.local] Policy Computer Configuration Software Settings Mindows Settings Administrative Templates Software Settings Software Settings Software Settings Mindows Settings Software Settings 	Object Type Enterprise Trust
Scripts (Logon/Logoff) Scripts Security Settings Scripts Key Policies Enterprise Trust	

- 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.

Autoenrollment Settings Properties
General
Enroll user and computer certificates automatically
Do not enroll certificates automatically
Enroll certificates automatically
Renew expired certificates, update pending certificates, and remove revoked certificates
Update certificates that use certificate templates
OK Cancel Apply

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.
- 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



Microsoft Certificate Services -- wirelessdemoca

Request a Certificate

Select the certificate type: User Certificate

Or, submit an advanced certificate request.

5. Choisissez Demande avancée et cliquez sur



Create and submit a request to this CA. Submit a certificate request by carry a base 34 encoded CMC or FKC3 #1011e, or submit a reneval request by using a base 64 encoded PKC3 #1 ite. Acquest a certificate for a circan certificate or user by using the smart care certificate error ment station why can put that an exclusion application are user to what the reneval request certificate or to ment station

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.

s Kol nutra	/1/2/16/10/25/carts/v/tertromayasp
rosofi Cer	ficate Services — windresodemuca
an ead (Sattificate Bernast
ancealt	eruncate Request
iticate l e	nplate:
	Administrator
	Apprinistrator
Op tions :	Dasic EF3
	End Keuwery Agen. In-ar
ĊŠ	P Witeless User Capiticate Template
997 2011-2011	
ney Usay	9. [Subordinate Certification Authority] (War Server)
Key Sir	0' 1' 1' 1' 1' 1' 1' 1' 1' 1' 1' 1' 1' 1'
	Automatic key container name O User specified key container name
	💌 Mark keys as expendible
	🗖 Expertikasys to fila
	🔲 Enable ehung private key protection
	Etore certificate in the local complications ficate store
	Stores the certificete in the local computer store
	instand of it the week's contribution state. Does not
	instell the root LAB centricate, You must be an administrator to generate by use a view in the local
	machine store.
tional Op	1005
est Form	al © CIVE - © PKCS10
- Alcorith	m: 3LA-1 -
	Only used to sign request.
	E Save regnes: In a de
Articulo	
10 and 10	
a a loc triace	
e. Cix iv stu	

- 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

Elle Edik <u>V</u> lew	Fgvarites Icols Help
🕽 Deck 💌 💮 🗠 🛛	🛿 😰 🐔 🔎 Search 🔅 Parontes 🛷 🔝 🐷
ddrees 🔊 http://17	72.16.L00.26(certsrv/certropia.asp
Certificate Temp	plate:
	ACS
ldentilving lafor	mation For Offline Template:
Name:	Iciaco w2009. wirelessdemo. local
E-Mail:	
Company:	
Department:	
City	
State:	
Country/Region:	
Key Options:	
	Create new key set C Use existing key set
CSP:	Microsoft Base Cryptographic Provider v1.D 💌
Key Usage:	@ Eschange
Key Size:	1024 Min:1024 (common key sizes: 3029.) Mar:1029
	Automatic key container name O User specified key container name
	☑ Mark keys as exportable
	Export keys to file
	Store certificate in the local computer certificate store
	instead of in the user's certificate store. Does not
	insta0 the root CA's certificate. You must be an
	administrator to generate or use a key in the local mechine store
Additional Onlin	
Request Format:	R CMC C PKCS10
Hash Almost	
nasn Algananm:	Only used to sign request.
	Save request to a file
	×
Attributes:	V X
Friendly Name:	
	Submit >

- Soumettre.
- 9. Une fenêtre contextuelle s'affiche et vous avertit d'une violation potentielle des scripts. **Cliquez sur**

	Yes.		
	Potential	Scripting Violation	×
	⚠	This Web site is requesting a new certificate on your cehalf Do you want to request a certificate now?	You should allow only trusted Web sites to request a certificate for you.
		Yes	
n	Clique	z sur Installer ce	

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

Eile	Edit	View	F <u>a</u> vorites	Tools	Help		
🔾 Ba	ack 🔻	0 -	🗵 🗈 🏠		5earch	📌 Favorites	😣 🙆 - 💺 🖃

Microsoft Certificate Services -- wirelessdemoca

Certificate Issued

The certificate you requested was issued to you.



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

res.	
Potentia	al Scripting Violation 🛛 🕅 🕅
4	This Web site is adding one or more certificates to this computer. Allowing an unbrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.
	Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.
	<u>Х</u> ез

12. Après avoir cliqué sur Oui, le certificat est

Hic ≞cit vîo∾	Fovoricos 1003	Help		
🕒 Back 👻 🕘 🕤	💌 🛿 🛃 🔎	earch 👷 Havorites	🐵 🔝 - 🚴 📼	}
Address 😸 Http:	(172.16.10J.26/certs	rv/pertrmpn.asp		
	•	• • • • • • • • •		
10	Gente Onician	0.0.02.000.000.00		
Microsoft Ce	tificate Services	wire esstlemoca		
Microsoft Ce	tificate Services	wire essilementa		
<i>Microsoft</i> Ce Certificate	tificate Services n stal led	wire esstlemoca		
<i>Microsoft</i> Ce Certificate I	tificate Services n stal led	wire essilementa		
<i>Microsoft</i> Ce Certificate I	tificate Services n stal led	wire esstemada		
<i>Microsoft</i> Ce Certificate I Your new ce	tificate Services n stalled tificate has bee	vire esstlemada	stalled	

ins

13. Àce stade, le e certificat est dans le dossier Certificates. Pour ac 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.

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.
- 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**.

🗿 Mir	crosoft	Cerli	ficale Servi	ires - M	ii rusul	O Tobernet Explorer	
[]e	Edt	ģe≁	Favorites	Loois	Uelo		
🕜 Ba	ack 👻 (ð -	🗉 🗟 🖁	<u>ه (ر</u> ا	earch	👷 =avortes 🧔 🙆 • 😓 🚍	
Acdro	:53 🙋	-tt:://	172.10.101.	26/certs	v/œrte	arc asc	

Micmsoff Centricate Geroces -- whelesedemocal

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from the certification authority install this CA certificate chain.

To down date a CA cost ficate, certificate chain, or CRL isolate the certificate and encoding method.

CA certificate:

 inent	[W16	esso	1em or	a)

Locoding method:

⊂D_R ©Esso 64

<u>Down dad CA certificate</u> <u>Down dad CA certificate chain</u> Down dad latest base CRL Down dad latest delta CRL

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

	Name: Tupe:	certnew.cer Security Certific	ate 1.68 KB	
8000-100G	From:	172, 16, 100, 26	ate, 1.00 KD	
		<u>O</u> pen	Save	Cancel
		2	_	

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. Save As ? X 💽 🕝 😰 🔛 -Save in: 🧼 Local Disk (C:) CNS62 Documents and Settings My Recent Documents DI386 Inetpub Program Files TFTP Desktop) WINDOWS Wireless) wmpub ACS.cer My Documents 🕮 acs_server_cert.cer 🔛 certnew.cer My Computer Save ACS.cer • My Network File name: Places Security Certificate Ŧ Save as type: Cancel

- 6. Ouvrez ACS Admin à partir du raccourci de bureau créé lors de l'installation.
- 7. Cliquez sur **Configuration du**



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

System Configuration



	Install new certificate	
C Read o	ertificate from file	
	Certificate file	
⊙ Use ce	ertificate from storage	
	Certificate CN	
	Private key file	
	Private key password	

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

	Install ACS Certificate	
	Install new certificate	
O R	lead certificate from file	
	Certificate file	
ΘU	Ise certificate from storage	
	Certificate CN cisco_w2003.wirelessde	
	Private key file	
	Private key password	

11. Cliquez sur

Submit.

System Configuration

Edit

Install ACS Certificate

?

Installed Certificate Information

Issued to:cisco_w2003.wirelessdemo.localIssued by:wirelessdemocaValid from:March 17 2006 at 08:33:25Valid to:March 16 2008 at 08:33:25Validity: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
C None
CiFull
Generate New File
Every day
C Every week
C Every month
○ When size is greater than 2048 KB
Manage Directory
\circ Keep only the last 7 files
Delete files older than 7 days
Back to Helm

- 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 Configuratio	in 🧖
PEAP	
□ Allow EAP-MSCHAPV2	
□ Allow EAP-GTC	
Allow Posture Validation	
Cisco client initial message:	
PEAP session timeout (minutes):	120
Enable Fast Reconnect:	\checkmark
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):	120

- 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

-	<u>ې</u>
	<u>?</u>
te is successully added into storage.	the global system certi
common name	wirelessdemoca
	ate is successully added into storage. common name

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



- 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

	wireless Networks	Advanced	
🗹 Use	Windows to configure	my wireless n	etwork settings
Avail	hle <u>n</u> elworks:		
To co abou	nnect :o, disconnec! f wiieless retworks in r	rom, or find ou arge. click th	ut more information e button below.
		View	Wireless Network:
			Moveun
			Move <u>up</u> Move <u>d</u> ow
	Add	e Pror	Move <u>up</u> Move <u>down</u>
	<u>dd</u> emov	e Prop	Move <u>up</u> Move <u>d</u> own

- 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

Association	Authentication	Connection	
Network na	me (SSID): network key —	Enployee	
This hetw	uork reguires a ko	ey for the following:	
Network	Authentication:	Open	•
Data ens	ryption:	WEP	
Network	key:		
Confirm n	etwork key:		
Key index	(edvariced);	1	
🔽 The k	ey is provided fo	rme auromatically	
This is a access	i computei-to-coi points are not us	mpu:er (ad noc) network ed	<; wireless

- 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

	Wireless ne	twork proper	ties	? 🛛	
	Association	Authenlica:ion	Connection		
	Select this wireless Eth	option to provide nemel networks	authenticated retwork	access for	
I	💌 Enable	IEEE 802.1x au:ł	nentication for this netwo	urk	
	EA ^D type:	Smart Card or o	ther Certhicate	~	
	Aulhent Aulhent unavala	icate as compule icate as guest wh abe	er when computer inform	Propeities ation s available ormation is	
			OK	Cancel)

- 10. Cliquez sur **Properties**.
- 11. Vérifiez que les cases de cette fenêtre sont

Si	mart Card or o	ther Certi	ficate Pr	operties		? 🔀
4	When connectin	g				
	🔘 Jse my smar	t pard				
	💿 Jse a certfic	ate on this c	omputer			
	🔽 Jse simp	e certificate :	selection (R	ecommend	ed)	
200	Validate serve	er certificate				
	Connect to t	hese servers.	a			2.
	Trusted Root Ce	ertification Au	thorities:			
	ABA.ECOM	Root CA				~
	ACS333					-
	ACS40				an an a	S
	Autordad L	Jertificadora o	ie la Asocia	conNacio	rai cel Nol	taria
	E Paltimore E	.eminanora r 7 ku D.ST	ieu .negin i	Nacional de	er olden in	aru
	Belgacom I	Zingitzan E.Trust Prima	nu Δ			
	C C WHKT	SecureNet C	A Class A			~
	<		101		4	>
	- Lenier -		-	Vi	iew Certfic	ate
1	Use a different	user name fo	r the conne	clion		
			1	OK.		Cancel
1.0						

- 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