# 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, reportezvous au <u>site Web Microsoft Wi-Fi</u> et au <u>Cisco SAFE Wireless Blueprint</u>.

## **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 <u>Guide d'installation des contrôleurs sans fil de la gamme</u> <u>Cisco 5500</u>. Pour obtenir des informations sur l'installation et la configuration initiales des contrôleurs de la gamme Cisco 2100, reportez-vous au <u>Guide de démarrage rapide : Contrôleur</u> <u>LAN sans fil de la gamme Cisco 2100</u>.

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 <u>Conventions relatives aux conseils techniques Cisco.</u>

## **Configurer**

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

**Remarque :** utilisez l'<u>outil de recherche de commandes</u> (clients <u>enregistrés</u> 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



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

## 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

- 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

Active Directory Installation Wizard	×
Database and Log Folders Specify the folders to contain the Active Directory database and log fil	•• 👻
For best performance and recoverability, store the database and the lo hard disks.	g on separate
Where do you want to store the Active Directory database?	
Database folder:	
C:\WINDOWS\NTDS	Bjowse
Where do you want to store the Active Directory log?	
C:\WINDOWSWITDS	Br <u>o</u> wse
< <u>B</u> ack <u>N</u> ext	> Cancel

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

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 Bjowse
<u>⟨B</u> ack <u>N</u> ext> Cancel

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

Active Directo	ry Installation Wizard		
Permission Select d	s lefault permissions for user and group objects.		
Some se stored o	erver programs, such as Windows NT Remote Access Service, read information n domain controllers.		
C Perr	nissions compatible with pre-Windows 2000 server operating systems		
Sele syste mem	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.		
Permission	nissions compatible only with Windows 2000 or Windows Server 2003 aling systems		
Sele Serv auth	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		

Suivant

de mot de passe vides et cliquez sur Next.

13. Vérifiez les informations sur la page Summary et cliquez sur

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. To change an option, click Back, To begin the operation, click Nest	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\SYSVDL SYSVDL folder: C:\WINDOWS\SYSVDL The DNS can be used by installed and configured on this corrector. This corrector	
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 Nest	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 SYSVDL folder: C:\WINDOWS\SYSVDL The DNS session will be installed and configured on this computer. This computer	
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 Nest	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 session will be installed and configured on this computer. This computer	*
Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVDL 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\SYSVDL The DNS service will be installed and configured on this computer. This computer	
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 DNS service will be installed and configured on this computer. This computer	
The password of the new domain administrator will be the same as the password of the administrator of this computer.	will be configured to use this DNS server as its preferred DNS server.	
To change an option, click Back, To begin the operation, click Next	The password of the new domain administrator will be the same as the password of the administrator of this computer.	-
and a second s	To change an option, click Back. To begin the operation, click 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

- 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.
- 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

- 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.
- 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 p providing a de	rovide an identifying scope name. You also have the option of scription.
Type a name a how the scope	and description for this scope. This information helps you quickly identify is to be used on your network.
Name:	CorpNet
Description:	
	< <u>B</u> ack <u>N</u> ext > Cancel

 Cliquez sur Next et renseignez ces paramètres :Adresse IP de début - 10.0.20.1Adresse IP de fin - 10.0.20.200Longueur - 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.
Start IP address: 10 . 0 . 20 . 1
End IP address: 10 . 0 . 20 . 200
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
Sybnet mask: 255 . 255 . 0
< <u>B</u> ack <u>N</u> ext> 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.

w 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:           10 . 0 . 20 . 1         10 . 0 . 20 . 100         Add
Excluded address range:
Remo <u>v</u> e
< <u>B</u> ack <u>N</u> ext > Cancel

- 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.

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>B</u> ack <u>N</u> ext > Cancel		

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.
I <u>P</u> address:
10.0.20.1 A <u>d</u> d
<u>R</u> emove
Шр
D <u>o</u> wn
< <u>B</u> ack <u>N</u> ext > 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	
<b>Domain Name and DNS Servers</b> The Domain Name System (DNS) maps a clients on your network.	and translates domain names used by
You can specify the parent domain you want the DNS name resolution.	he client computers on your network to use for
Parent do <u>m</u> ain: demo.local	
To configure scope clients to use DNS servers servers.	s on your network, enter the IP addresses for those
<u>S</u> erver name:	I <u>P</u> address:
	Add
Resolve	10.0.10.10 <u>B</u> emove
	Цр
	Down
	< <u>B</u> ack <u>N</u> ext > Cancel

- 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.

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

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

- 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 certificatsGérer CADemander des certificatsSi l'une de ces options est définie sur Refuser ou n'est pas sélectionnée, définissez les autorisations sur

ca.demo.local Properties		? ×	
General   Policy Module   Exit Mod Certificate Managers Restrictions   Auditin	ule   Extensio g   RecoveryA	ns Storage gents Security	
Group or user names: Administrators (DEMO\Administrators) Authenticated Users Domain Admins (DEMO\Domain Admins) Enterprise Admins (DEMO\Enterprise Admins)			
Permissions for Administrators Read Issue and Manage Certificates Manage CA Request Certificates	A <u>d</u> d Allow I I I I I I I I I	<u>R</u> emove Deny	
ОК	Cancel	Apply	

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 <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 **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

ew Object - Computer	×
Create in: demo.local/Users	
Computer name:	
client	
Computer name (pre-Windows 2000):	
CLIENT	
The following user or group can join this computer to a domain.	
Default: Domain Admins Change	
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	

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

- 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

clier	nt Properties ?
G	eneral Operating System Member Of Location Managed By Dial-in
Г	Remote Access Permission (Dial-in or VPN)
	Allow access
	© <u>D</u> eny access
	C Control access through Remote Access Policy
Г	Callback Options
	No <u>C</u> allback
	Set by Caller (Routing and Remote Access Service only)
	C Always Callback to:
-	Assign a Static IP Address
Γ	Apply Static Boutes
	Define routes to enable for this Dial-in Static Routes
	OK Cancel <u>A</u> pply

#### 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 cliquez sur **Utilisateur**.
- 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		×
Create in:	demo.local/Users	
<u>F</u> irst name:	wirelessuser <u>I</u> nitials:	
Last name:		
Full n <u>a</u> me:	wirelessuser	-
User logon name:		_
wirelessuser	@demo.local	<b>▼</b>
User logon name (pre	<u>W</u> indows 2000):	
DEMO\	wirelessuser	
	·	
	< <u>B</u> ack <u>N</u> ext >	Cancel

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

Create in:	demo.local/Users
Password:	•••••
<u>C</u> onfirm password:	•••••
User <u>m</u> ust change p	assword at next logon
🔲 U <u>s</u> er cannot change	e password
🔲 Pass <u>w</u> ord never exp	ires
Account is disabled	

- 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

- 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

Remote control Termin	al Services Profile	COM+
General Address Account	Profile Telephones	Organizatio
Member Of Dial-in	Environment	Sessions
- Remote Access Permission (Dial-in (	or VPN)	
Allow access		
C Denv access		
C. Castral second through Remote	Assess Reliev	
C Control access through Hemote	Access Folicy	
Callback Options	,	
No Callback		
C Set by Caller (Routing and Rem	ote Access Service on	y)
C Always Callback to:		
•	1	
🗖 Assign a Static IP Address		
Apply Static Routes	,	
Define motes to enable (exitin Die	15	
connection.	Static Ro	ytes

#### 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 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*.

ew Object - Group	×
Create in: demo.	ocal/Users
Group name:	
wirelessusers	
,	
Group name (pre- <u>W</u> indows 200	0):
wirelessusers	
Group scope	Group type
C Domain local	Security
Global	C Distribution
C Universal	
	OK Cancel

#### Ajouter des utilisateurs au groupe d'utilisateurs sans fil

- 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

Select this object type.		
Users or Other objects	Objec	ct Type
From this location:		
demo.local	Loc	ations
Enter the object names to select (examples):		
Enter the object names to select ( <u>examples</u> ): wirelessuser		ck Nan

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

wirelessusers Proper	ties	? ×
General Members	Member Of Managed By	
Members:		
Name	Active Directory Folder	
🖸 Administrator	demo.local/Users	
🖸 😡 wirelessuser	demo.local/Users	
bha	Bemove	
	Hemory	
	OK Cancel	Applu
		OPPY

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 :

fil.

- 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.
- 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

Users or Other objects	Dbject Types
, Erom this location:	
demo.local	Locations
Enter the object names to select (examples):	
client	<u>C</u> heck Name

groupe.

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

Ordinateurs.

Select the types of objects you want to find.	
Object types:	
🗹 🐳 Other objects	
EE Contacts	
OK Cancel	

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

wirelessusers Proper	ties	? ×
General Members	Member Of Managed By	
Members:		
Name Administrator	Active Directory Folder	
E client	demo.local/Computers	
🖸 wirelessuser	demo.local/Users	
	- 1	
Add	Bemove	
	OK Cancel	Apply

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 <u>Chapitre 4, Connexion des câbles.</u>
- 2. Mettez le périphérique CSACS-1121 sous tension. Reportez-vous au <u>chapitre 4, « Mise sous</u> <u>tension de l'appliance de la gamme CSACS-1121 ».</u>
- 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
- <u>Tâches post-installation</u>

Pour obtenir des informations détaillées sur l'installation du serveur Cisco Secure ACS, reportezvous au <u>Guide d'installation et de mise à niveau de Cisco Secure Access Control System 5.1</u>.

## 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.
- Configurez les informations comme le montre la fenêtre Interfaces > Edit :Adresse IP de l'interface - 10.0.20.2Masque réseau - 255.255.255.0Passerelle - 10.0.10.1DHCP principal : 10.0.10.10

միսիս			s	a <u>v</u> e Configuration	Ping   Loge	out   <u>B</u> efrei
CISCO MONITOR WI	ANS CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Controller	Interfaces > Edit			< 84	ack /	Apply
General Inventory Interfaces	General Informat	ion				
Multicast	Interface Name	em; 00:	ployee 24:97:69:4d:e	0		
Internal DHCP Server	Configuration					
<ul> <li>Mobility Management</li> <li>Ports</li> </ul>	Guest Lan					
NTP CDP	Quarantine Quarantine Vlan Id	0				
Advanced	Physical Informat	tion				
	Port Number Backup Port		2			
	Active Port		0			
	Enable Dynamic AF	9 Management S				
	VLAN Identifier		20			
	IP Address Netmask		255.255.255	0		
	Gateway		10.0.20.1			
	DHCP Information	n				
	Primary DHCP Sen Secondary DHCP S	ver Ierver	10.0.10.10			
	Access Control Li	st				
	ACL Name		none 💌			
	Note: Changing the In temporarily disabled a some clients.	terface param and thus may r	eters causes t esult in loss of	he WLANs to be f connectivity for		

- 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*.

CISCO MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	Sa <u>v</u> e Configuration M <u>A</u> NAGEMENT	Eing C <u>O</u> MMA	Logout <u>R</u> efree
WLANs	WI	_ANs > New			< B	ack	Apply
<ul> <li>WLANS</li> <li>WLANS</li> <li>Advanced</li> </ul>	1	l'ype Profile Name SSID ID	[ [ [ [ [	WLAN Employee Employee			

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**.
- 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

55ID.						
վերին				S	ave Configuration	Ping Logout Refre
CISCO MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS HELP
WLANs	WI	_ANs > Edit			< Ba	ack Apply
WLANs WLANs	•	General Se	curity Qos	6 Advanc	ed	
Advanced		Profile Name	Employee			
		Туре	WLAN			
		SSID	Employee			
		Status	Enabled			
		Security Policies	[WPA2][Auth( Modifications do changes.)	802.1X)] ne under secu	rity tab will appear	r after applying the
		Radio Policy Interface Broadcast SSID	All employee 💌 💌 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

WLANs > E	dit		
General	Security	QoS	Advanced
Layer 2	Layer 3	AAA S	ervers
Layer 2 WPA+WPA	Security 🤨 🛛 🗸 F 2 Parameter	VPA+WPA2 MAC Filto	2 💌
WPA Po	licy		
WPA2 P	WPA2 Policy		
WPA2 E	WPA2 Encryption		ES 🔽 TKIP
Auth Ke	y Mgmt	802.	1X 💌

d'authentification. L

- 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**.

սիսիս		Saye Configuration Ping Logout Befree
CISCO MONITOR WL	ANS <u>C</u> ONTROLLER	WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security	RADIUS Auther	ntication Servers > New < Back Apply
<ul> <li>AAA         General         <ul> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> </ul> </li> <li>TACACS+         <ul> <li>LDAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> <li>AP Policies</li> </ul> </li> </ul>	Server Index (Priority) Server IP Address Shared Secret Format Shared Secret Confirm Shared Secret Key Wrap Port Number	1         10.0.10.20         ASCII         •••••         •••••         •••••         (Designed for FIPS customers and requires a key wrap compliant ADIUS server)         1812
Local EAP	Server Status	Enabled 💌
Priority Order	Support for	Enabled 💌
Certificate	Server Timeout	2 seconds
Access Control Lists	Network User	Enable
<ul> <li>Wireless Protection</li> <li>Policies</li> </ul>	Management	Enable
▶ Web Auth	IPSec	Enable
Advanced		

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

- 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.

MyConsole - [Console Root\Cer	tificate Templates]	
Ele Action Yew Favorites ← → E E E 20 20 20 20 100 100 100 100 100 100 100	<u>W</u> indow <u>H</u> elp	<u>_8×</u>
Console Root	Template Display Name Exchange Signature Only Exchange User File IPSec IPSec (Offline request) Key Recovery Agent RAS and IAS Server Root Certification Authority Router (Offline request) Smartcard Logon Smartcard User Subordinate Certification Authority Trust List Signing User User Signature Only	Minimum Supported CAs Windows 2000 Windows 2000 Windows 2000 Windows 2000 Windows Server 2003, En Windows Server 2003, En Windows 2000 Windows 2000
Using this template as a base, creates a	Workstation Authe     Duplicate Template       Image: Workstation Authe     All Tasks	Windows Server 2003, En

#### 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 Dupliquer le

Properties of New Template
Issuance Requirements   Superseded Templates   Extensions   Security General   Request Handling   Subject Name
Template display name:
Copy of Web Server
Minimum Supported CAs: Windows Server 2003, Enterprise Edition
After you apply changes to this tab, you can no longer change the template name.
Template name:
Copy of Web Server
Validity period: <u>R</u> enewal period:
2 years 💌 6 weeks 💌
Publish certificate in Active Directory
Do not automatically reenrol if a duplicate certificate exists in Active Directory
OK Cancel Apply

#### modèle.

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

operties of New 1	Template 🛛
Issuance Requirem General	nents   Superseded Templates   Extensions   Secur Request Handling   Subject Name
T <u>e</u> mplate display r	name:
ACS	
Minimum Supporte	ed CAs: Windows Server 2003, Enterprise Edition
After you apply ch	anges to this tab, you can no longer change the templat
name.	
Iemplate name:	
ACS	
Validitu neriod	Renewal period
I ~ Iyears	• I o weeks
Publish certific	ate in Active Directory
Do not aut	omatically reenroll if a duplicate certificate exists in Active
Directory	
Directory	
Directory	
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

roperties of Ne	w Template 🔹 👔
Issuance Requi General	rements   Superseded Templates   Extensions   Security Request Handling   Subject Name
Purpose:	Signature and encryption         Archive subject's encryption private key         Include symmetric algorithms allowed by the subject         Delete revoked or expired certificates (do not archive)
Minimum key si Minimum key si Allow privat Do the followin associated with C Enroll subject	ze: 1024 te key to be exported g when the subject is enrolled and when the private key this certificate is used: ct without requiring any user input
C Prompt the C Prompt the private key	user during enrollment user during enrollment and require user input when the is used
To choose whi (CSPs) should I	Ch cryptographic service providers <u>C</u> SPs be used, click CSPs. OK Cancel <u>Apply</u>

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

SP Selection			? 2
Choose which cryptograph requests:	ic service providers	(CSPs) can be	used in
C Requests can use any	CSP available on th	ne subject's con	nputer
• Requests must use on	e of the following CS	Ps:	
<u>C</u> SPs:			
Gemplus GemSAFE Ca	rd CSP v1.0 e Smart Card CSP		-
Microsoft Base Cryptog	raphic Provider v1.0		
Microsoft Base DSS an	d Diffie-Hellman Cry I Cruptographic Prov	ptographic Prov ider	vider
Microsoft Enhanced Cr	vptographic Provide	rv1.0	
Microsoft Enhanced DS	S and Diffie-Hellma	n Cryptographic	Prov
Microsoft Enhanced RS	SA and AES Cryptog	raphic Provider	-1
ILIMICIOSOIT ISSA SLIbann	eu uvotodrannic. Pto	MINE	_
	OK	C	ancel
	<u>.</u>		
		-	

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

perties of New To	emplate	
Issuance Requireme	nts Superseded Templates	Extensions Security
General	Request Handling	Subject Name
Supply in the re Select this option not have access Autoenrollment	quest in to allow a variety of subject is is to the domain of which the s is not allowed if you choose thi	name formats or if you do ubject is a member. is option.
C Build from this A	ctive Directory information	subject names and to
simplify certificate	administration.	) subject names and to
Subject name for	mat	
None		<b>Y</b>
Include e-ma	i name in subject name	
Include this infor	mation in alternate subject nam	ie:
E-mail name		
DNS name		
Luser prinicip	al name (UPN)	
Service princ	ipal name (SPN)	
	ar 1	
	UK II	Cancel Apply

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.
- 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

roperties of New Template
General         Request Handling         Subject Name           Issuance Requirements         Superseded Templates         Extensions         Security
Require the following for enrollment:
This number of authorized signatures:
If you require more than one signature, autoenrollment is not allowed. Relicy type required in signature:
Application policy:
ssuance policies:
Add
Bemove
Require the following for reenrollment: Same criteria as for enrollment
C Valid existing certificate
OK Cancel Apply

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

- 1. Ouvrez le composant logiciel enfichable Autorité de certification. Effectuez les étapes 1 à 3 dans 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**.
- 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.
| 🔯 Certification Authority       |              |          |                                 |
|---------------------------------|--------------|----------|---------------------------------|
| <u>File Action View H</u> elp   |              |          |                                 |
| ← → 🗈 🖬 🖻 😫                     | 1 😫 💵        |          |                                 |
| in Certification Authority (Loc | :al)         | Name     |                                 |
| 🖻 👩 ca.demo.local               |              | 🔯 Direc  | tory Email Replication          |
| Revoked Certificat              | es           | Dom 💱    | ain Controller Authentication   |
| Issued Certificates             | ;            | EFS 🔯    | Recovery Agent                  |
| Pending Requests                |              | 🔯 Basio  | : EFS                           |
| Failed Requests                 |              | Dom      | ain Controller                  |
|                                 | Manage       |          | Server                          |
|                                 |              |          | huter                           |
|                                 | <u>N</u> ew  | <u> </u> | Certificate Template to Issue   |
|                                 | View         | •        | rdinate Certification Authority |
|                                 |              |          | histrator                       |
|                                 | Refresh      |          |                                 |
|                                 | Export L     | jst      |                                 |
|                                 | <u>H</u> elp |          |                                 |
| -                               |              |          |                                 |

4. Cliquez sur le modèle de certificat

#### ACS.

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	<alb< td=""><td></td></alb<>	
😥 Enrollment Agent	Certificate Request Agent	
🙀 Enrollment Agent (Computer)	Certificate Request Agent	
Exchange Enrollment Agent (Offline request)	Certificate Request Agent	
🐹 Exchange Signature Only	Secure Email	_
Exchange Liver	Secure Email	<b>•</b>

- 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

🐗 Active Directo	ory Users and Computers	
Sile Action	<u>Y</u> iew <u>W</u> indow <u>H</u> elp	
⇔ ⇒ 🗈 💽	1 🛍 🖆 🖻 🗟 😭 💷	🐮 🖉 🖄 🖓 🍕 ]
Active Director	y Users and Computers [A demo.]	ocal 5 objects
Saved Que	Name	
E G Canone	Delegate Control	
	Find	ers
	Connect to Domain	Controllers
	Connect to Domain Controller	SecurityPrincipals
	Raise Domain Functional Level	
	Operations Masters	
	New	•
	All Tasks	•
	⊻iew	•
	New Window from Here	
	Refresh	
	Export List	
	P <u>r</u> operties	
	Help	

# 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

demo.local Properties		? ×
General Managed By Group Policy		
To improve Group Policy management, upgrade Management Console (GPMC). Current Group Policy Object Links for	to the Group Po or demo	licy
Group Policy Object Links	No Override	Disabled
Group Policy Objects higher in the list have the h This list obtained from: AD2003.demo.local	ighest priority.	
New         Add         Edit           Options         Delete         Properties		<u>U</u> р Do <u>w</u> n
Block Policy inheritance		
Close	Cancel	Apply

s'ouvre. 🛏

 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

matic Certificate Request Setup W Certificate Template The next time a computer logs on, a c provided.	rizard certificate based on the template you select is
A certificate template is a set of prede computers. Select a template from the Certificate templates:	fined properties for certificates issued to following list.
Name	Intended Purposes
Computer Domain Controller Enrollment Agent (Computer) IPSec	Client Authentication, Server Authentication Client Authentication, Server Authentication Certificate Request Agent IP security IKE intermediate
•	<b>&gt;</b>
	< <u>B</u> ack <u>N</u> ext > Cance

#### 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.

🚡 Group Policy Object Editor				
Elle Action View Help				
S Default Domain Policy [AD2003.demo.local] Policy	Automatic Certificate Request			
E- 🛃 Computer Configuration	Computer			
Software Settings				
😑 🦳 Windows Settings				
- Scripts (Startup/Shutdown)				
E-B Security Settings				
Account Policies				
Local Policies				
🖲 🛃 Event Log				
Restricted Groups				
System Services				
🖲 🧰 Registry				
🕖 🛄 File System				
Wireless Network (IEEE 802.11) Policies				
E- Public Key Policies				
Encrypting File System				
Automatic Certificate Request Settings				
Enterprise Trust				
Software Restriction Policies				
IP Security Policies on Active Directory (demo.local)				
Administrative Templates				
E- 🕵 User Configuration				
Software Settings				
Windows Settings				
Administrative Templates				

- 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

Autoenrollm	ent Settings Properties	? X
General		
	Enroll user and computer certificates automatically	
© <u>D</u> or ⊙ <u>Enro</u>	iot enroll certificates automatically Il certificates automatically	
ঘ	Benew expired certificates, update pending certificates, and re revoked certificates	nove
<b>V</b>	Update certificates that use certificate templates	
	OK Cancel As	oply

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.

►	Sustam.	Administration > Cont	laural	ion > Local Secure	Certificates > Lo	cal Ca	rtificates	
Network Resources	System	Contractor - Cont	yura	ion > coolarderver	Cerunicates > Co	- Car Ce		0.1
Ilears and identity Stores	Loca	Certificates			5	showi	ng 1-1 of 1 🖼 🛄	per page Go
Delle: Clements	Filter	c		Match if:			Go 🔻	
Qy Policy Elements		Friendly Name		Issued To	Issued By		Valid From	Valid To (Ex
Access Policies		305		305	908		04:29 20 09 2010	04:29:20:05
<ul> <li>Monitoring and Reports</li> </ul>		Mar.						
🔹 💐 System Administration								
<ul> <li>Administrators         Accounts         Roles         Settings</li> <li>Users         Authentication Settings</li> <li>Operations         Distributed System Management         Software Repositories         Centralized Software Updates         Scheduled Backups         Local Operations</li> <li>Clobal System Options         Dictionaries         Local Server Certificates         Dustanding Signing Requests         Log Configuration         Licensing         Downloads         Migration Utility         Server Certificates         Server Certificates</li></ul>								
Sample Python Scripts	Add	Edit Delete	[]	Export		14	Page 1	of 1 🗾

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



 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



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.



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



8. Enregistrez le fichier certificat .pem ACS sur le

Save As					<u>?×</u>
Save in:	Desktop		• 0	1 📂 🖽 -	
My Recent Documents Desktop My Documents My Computer	My Documents My Computer	ces			
My Network	File name:	ACS_ctd			Save
Places	Cause as honor	[			

### 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

Microsoft Certificate Services - ca.demo.local	<u>Home</u>
Advanced Certificate Request	
The policy of the CA determines the types of certificates you ca request. Click one of the following options to:	an
Create and submit a request to this CA.	
Submit a certificate request by using a base-64-encoded C PKCS #10 file, or submit a renewal request by using a base encoded PKCS #7 file.	<u>MC or</u> 2-64-
Request a certificate for a smart card on behalf of another using the smart card certificate enrollment station. Note: You must have an enrollment agent certificate to submit a request behalf of another user.	ser by at on

#### 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-

To submit a sav #10 certificate r source (such as	red request to the CA, paste a base-64-encoded CMC or PKCS request or PKCS #7 renewal request generated by an external 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 Temp	late:
	Administrator
Additional Attribu	ites:
Attributes:	× ×

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.

Windows	Internet Explorer
⚠	Your web browser security settings prohibit this page from accessing your disk. Either paste the data into this page manually, or add this page to your browser's list of trusted sites.
	ок

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

📕 ACS_csr - Notepad	
File Edit Format Vie	w Help
BEGIN CERT	Undo
	Cut
	Сору

Copier.

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

Microsoft Certificate Services ca.demo.local							
Submit a Cert	ificate I	Requesto	or Rene				
To submit a sav renewal reques	ved req t gener	uest to the ated by an	CA, pa externa				
Saved Request:	6						
Base-64-encoded certificate request		Undo					
(CMC or PKCS #10 or		Gut Copy					
PKCS #7):	4	Paste Delete					
	Browse	Select All	517-				
Certificate Temp	late:						
	Adminis	strator					

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):	YIZIAYb4QgEBBAQDAgZAMA0GCSqGSIb3DQEBBQUA DXoioRABct447w077+uAk8crn26oaEhcfG/ZR15X ONZQ5xnrK23yxEdQNvSFC30mzR2EbQq4s5MvPE22 /MWqXej3NjpicpAgiV8CSwNd END CERTIFICATE REQUEST
	Certificate Temp	late:
		ACS
	Additional Attribu	utes:
	Attributes:	x Y F
Submit.		Submit >

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

Certificate Issued	
The certificate you requeste	ed was issued to you.
C DER encode	d or Rase 64 encoded
Download certifi	cate chain
	File Download - Security Warning
	Do you want to open or save this Ne?
	Name: certnew.cer Type: Security Certificate, 1,88X8
	From: ca
	Open Save Ca
	While files from the Internet can be useful this file tune can
	notentially been your commuter. If you do not tout the source

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



14. Cliquez sur Browse, et localisez le certificat

<ul> <li>Select server certificate creation method</li> </ul>	Bind CA Signed Certificate
Step 2 -Bind CA Signed Certific	ate
O Certificate File:	Browse
Protocol	
EAP: Used for EAP protocols that use SSL	/TLS tunneling
Management Interface: Used to authentica	ate the web server (GUI)
Override Policy	
A certificate being imported may be determine Subject or Issuer and serial number as an exis "Replace Certificate" option will allow the certifi existing protocol selections for the certificate.	d to already exist in ACS when it has either the same sting certificate. In such a case, selection of the loate contents to be replaced while retaining the
Replace Certificate	

### enregistré.

Open.

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

Choose file					<u>?×</u>
Look in:	Desktop		+ 🖻	- 🖬 📩	
My Recent Documents Desktop My Documents My Computer	My Documents My Computer My Network Pl ACS_cert ACS_csr	sces			
My Network	File name:	ACS, cert		-	Open
Piaces	Files of type:	All Files (".")		•	Cancel

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.

System /	system Administration > Configuration > Local Server Certificates > Local Certificates								
Local Certificates Showing 1-2 of 2 50 💌									
Filter	Filter: Match if: Go 🗢								
	Friendly Name	•	Issued To	Issued By	Valid From				
	acs		acs	acs	04:29 20.09.2010				
	acs.demo.local		acs.demo.local	ca.demo.local	10:39 22.09.2010				

#### 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

General	Directory Groups	B Directory Attributes	
Connect	on Details		
Active D Name:	Directory Domain	demo.local	
Diageo er	acify the credentic	le used to join this machin	to the Artise Directory Domain
C Licems	me.	administrator	
• Oseina	ine.		
Passw	ord:		
reachable	use the Test Conne	Test Connection	fentials are correct and Active Directory Domain
reachable	use the Test Conne ).	Test Connection	fentials are correct and Active Directory Domain
Click on %	use the Test Conne Save Changes' to c	Test Connection	tentials are correct and Active Directory Domain
Click on 3 have succ	use the Test Conne b. Save Changes' to c cessfully connected lable for use in pol	Test Connection Test Connection Connect to the Active Directo to the Domain, yr Window ico nules	tentials are correct and Active Directory Domain v Domain and save this configuration. Once yo
Click on 3 have succ to be avail	use the Test Conne Save Changes' to c cessfully connected lable for use in pol	Test Connection Test Connection connect to the Active Directo d to the Domain, yr Window icy rules.	tentials are correct and Active Directory Domain ty Domain and save this configuration. Once yo Internet Explorer
Click on 'S have succ to be avail	save Changes' to c save Changes' to c cessfully connected lable for use in pol	Test Connection Test Connection Connect to the Active Directo to the Domain, yo Window icy rules.	tentials are correct and Active Directory Domain ty Domain and save this configuration. Once yo <b>Internet Explorer</b> Connection test to 'demo.local' succeeded.
Click on % have succ to be avail	use the Test Connector Save Changes' to c cessfully connected lable for use in pol	Test Connection Test Connection Connect to the Active Directo to the Domain, yt Window icy rules.  ettings anoe	tentials are correct and Active Directory Domain ty Domain and save this configuration. Once yo <b>Internet Explorer</b> Connection test to 'demo.local' succeeded.
Click on % have succ to be avai End User I En:	ase the Test Connector Save Changes' to c pessfully connected lable for use in pol r Authentication Se able password cha	Test Connection Test Connection Connect to the Active Directo to the Domain, yr Window icy rules. ettings ange estication	tentials are correct and Active Directory Domain ny Domain and save this configuration. Once yo <b>Internet Explorer</b> Connection test to 'demo.local' succeeded. OK
Click on S have succ to be avail End User F En: En:	ase the Test Connector Save Changes' to c cessfully connected lable for use in pol r Authentication Se able password cha able machine auth	ection Button to ensure creation Test Connection connect to the Active Director d to the Domain, your window icy rules. ettings ange entication	tentials are correct and Active Directory Domain or Domain and save this configuration. Once yo <b>Internet Explorer</b> Connection test to 'demo.local' succeeded. OK
Click on S have succ to be avail End User IF En: IF En:	ase the Test Connector Save Changes' to c cessfully connected lable for use in pol r Authentication Se able password cha able machine auth able Machine Acce	ection Button to ensure creation Test Connection connect to the Active Directo d to the Domain, yo window icy rules. ettings ange entication ss Restrictions	tentials are correct and Active Directory Domain ty Domain and save this configuration. Once yo to Internet Explorer Connection test to 'demo.local' succeeded. OK

continuer.

4. Cliquez sur Enregistrer les



#### modifications.

pour plus d'informations sur la procédure d'intégration d'ACS 5.x, reportez-vous à <u>ACS 5.x et</u> <u>versions ultérieures : Exemple de configuration de l'intégration avec Microsoft Active</u> <u>Directory</u>.

#### 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

+ 🛠 My Workspace	Network	Resource	is > Net	work Device	15 an
Initial Resources	Netw	ork Devi	ces		
Network Device Groups     Network Devices and AAA Clients	Filter			× 1	latch
Default Network Device External RADIUS Servers	Г	Name	-	IP / Mask	N
3     3     3     3     3     4	-	No dat	a to dis	play	
Policy Elements					
Access Policies					
<ul> <li>Monitoring and Reports</li> </ul>					
	Cres	ste (	Juplica	te Edit	1

Clients. Cliquez sur Create.

2. Renseignez les champs suivants :Nom - wlcIP - 10.0.1.10Case à cocher RADIUS - CochéeSecret partagé -

Network Device Gro	ups		
Location	All Locations		Select
Device Type	All Device Types		Select
IP Address Single IP Address IP: 10.0.1.10	(s)	Authentication Options TACACS+ Shared Secret Single Connect Device C Legacy TACACS+ Sing TACACS+ Draft Compl Support RADIUS RADIUS Shared Secret Cisco TrustSec Device ID for TrustS Device ID: Password: TrustSec Advanced Setti	le Connect S liant Single C lec identificat

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

► St My Workspace	Network	Resources	i > Ne	twork Devices an	d AAA Clients		
* 😺 Network Resources	Network Devices Showing 1-1 of 1						
<ul> <li>Network Device Groups Network Devices and AAA Clients</li> </ul>	Filter: Match if:					٣	Go 💌
Default Network Device External RADIUS Servers		Name	•	IP / Mask	NDG:Location		NDG:Device Type
Busers and Identity Stores     Store		wic		10.0.1.10/32	All Locations		All Device Types
Policy Elements							
Access Policies							
Monitoring and Reports							

#### 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

Access F	Policies > Access Services			
Acces	ss Services		Showing 1-2 of 2	50 💌 per p
Filter	Match if		Go 🔻	
	Name 🔺	Service Type	Included Policies	Description
	Default Device Admin	Device Administration	Identity Authorization	Default Devi
	Default Network Access	Network Access	Identity Authorization	Default Netv
-				
Crea	te Duplicate Edit	Delete	Page	1 of 1

#### 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: WirelessAD	
Description:	
Access Service Policy Structure	
Based on service template	Select
C Based on existing service	Select
C User Selected Service Type Network Access	

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

Acces	ss Services		Showing 1-4
Filter:	Match if:	G0 🔻	
	Name *	Service Type	Description
0	Device Admin - Command Auth	Device Administration	
0	Device Admin - Simple	Device Administration	
0	Network Access - MAC Authentication Bypass	Network Access	
•	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

Sele
Sele
]

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**.



 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

Cisco Secure ACS Webpage Dialog						
Identit	y Store					
Filter:		Match if: Go 🔻				
	Name 🔺	Description				
C	AD1					
0	CN Username	Predefined Certificate Authentication Profile				
0	DenyAccess					
0	Internal Hosts					
0	Internal Users					
0	NAC Profiler	Default Entry for NAC Profiler				

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

OK.

Access Policies > Access Services > WirelessAD > Identity	
Single result selection C Rule based result selection	1
Identity Source: AD1 Sele	ct
Advanced Options	

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

Effectuez les étapes suivantes :

1. Accédez à Access Policies > Service Selection Rules.



 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.

e	Cisco Secure ACS Webpage Dialog
	General Name: WirelessRule Status: Enabled 💌 😂
	The Customize button in the lower right area of the policy rules scree conditions and results are available here for use in policy rules.
	Conditions       Protocol:     match     Select
	Results

C	🖉 Cisco Secure ACS Webpage Di						
	Enun	Definition					
		Enum Na	Enum Name				
	C	Radius		0			
	С	Tacacs		1			

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

Conditions		
Conditions		
Protocol: match	<ul> <li>Radius</li> </ul>	Sele
Doculto		
Results		

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

Ser	vice Se	election P	olicy			
Filt	er: Sta	itus 🔄	Match if: Equa	uls 💌	•	Clear
		Status	Name	Protocol	Conditions	
3		•	WirelessRule	match Radius	V2201220122017	682680
1		0	Rule-1	match Radius		
2		Θ	Rule-2	match Tacacs		
-						
••	Г	Default		If no rules define	ed or no enabl	led rule
C	reate	-  D	uplicate   • E	dit Delete	Move to	V

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

Use Windows to configure	my wireless network settings
Available networks: To connect to, disconnect fr about wireless networks in ra	om, or find out more information nge, click the button below.
	View Wireless Networks
Preferred networks: Automatically connect to available.	ilable networks in the order listed
Preferred networks: Automatically connect to available	ilable networks in the order listed Move up Move down
Preferred networks: Automatically connect to available below: Add	ilable networks in the order listed Move up Move down

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

Wireless network properties		<u>? ×</u>
Association Authentication	Connection	
Network name (SSID):	Employee	
Wireless network key		
This network requires a key	for the following:	
Network Authentication:	WPA	•
Data encryption:	TKIP	•
Network key:		
Confirm network key:		
Key index (advanced):		
The key is provided for r	ne automatically	
This is a computer-to-comp access points are not used	outer (ad hoc) network; v d	vireless
	OK	Cancel

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

Wireless network properties				
Association	Authentication Connection			
Select this wireless Et	option to provide authenticated network access for hemet networks.			
🗵 Enable	IEEE 802.1x authentication for this network			
EAP type:	Protected EAP (PEAP)			
	Propertie	:5		
Authenticate as computer when computer information is available				
Authenticate as guest when user or computer information is unavailable				
	OK Car	ncel		

#### 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

Protected EAP Properties				
When connecting:				
Validate server certificate				
Connect to these servers:				
Trusted Root Certification Authorities:				
C&W HKT SecureNet CA Root CA 1 Ca.demo.local Certiposte Classe A Personne Certiposte Serveur Certisign - Autoridade Certificadora - AC2 Certisign - Autoridade Certificadora - AC4				
Do not prompt user to authorize new servers or trusted certification authorities.				
Select Authentication Method:				
Secured password (EAP-MSCHAP v2)				
Enable Fast Reconnect				
OK Cancel				

- 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.

interne.



- 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 **Authentifications - RADIUS - Aujourd'hui**.

ly 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						
Logged At	RADIUS NAS Status Failure	Details	Username	MAC/IP Address	Access Service	Authentication Method
Sep 22,10 5:51:17.843 F	M 🖌	9	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)				
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

## 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'<u>authentification PEAP échoue</u> <u>lorsque vous vous connectez à un serveur RADIUS tiers</u>. 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
- <u>Assistance et documentation techniques Cisco Systems</u>

## 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.