Exemple de configuration d'authentification EAP locale sur le contrôleur de réseau local sans fil avec un serveur EAP-FAST et LDAP

Table des matières

Introduction Conditions préalables Exigences Composants utilisés Conventions Informations générales Configurer Diagramme du réseau Configurations Configurer EAP-FAST en tant que méthode d'authentification EAP locale sur le WLC Générer un certificat de périphérique pour le WLC Téléchargement du certificat de périphérique sur le WLC Installer le certificat racine de PKI dans le WLC Générer un certificat de périphérique pour le client Générer le certificat CA racine pour le client Configurer le protocole EAP local sur le WLC Configurer le serveur LDAP Création d'utilisateurs sur le contrôleur de domaine Configurer l'utilisateur pour l'accès LDAP Utilisation du protocole LDP pour identifier les attributs utilisateur Configuration du client sans fil Vérifier **Dépannage** Informations connexes

Introduction

Ce document explique comment configurer l'authentification EAP (Extensible Authentication Protocol) - Flexible Authentication via Secure Tunneling (FAST) L'authentification EAP locale sur un contrôleur LAN sans fil (WLC). Ce document explique également comment configurer le serveur de protocole d'accès aux annuaires allégés (LDAP) comme base de données principale pour que l'EAP local récupère les identifiants utilisateurs et pour authentifier l'utilisateur.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

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

- Contrôleur de réseau sans fil de la gamme Cisco 4400 qui exécute le micrologiciel 4.2
- Point d'accès léger (LAP) de la gamme Cisco Aironet 1232AG
- Serveur Microsoft Windows 2003 configuré en tant que contrôleur de domaine, serveur LDAP et serveur d'autorité de certification.
- Adaptateur client Cisco Aironet 802.11 a/b/g qui exécute le micrologiciel 4.2
- Utilitaire de bureau Cisco Aironet (Aironet Desktop Utility ou ADU) qui exécute la version 4.2 du micrologiciel

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>

Informations générales

L'authentification EAP locale sur les contrôleurs LAN sans fil a été introduite avec la version 4.1.171.0 du contrôleur LAN sans fil.

L'EAP local est une méthode d'authentification qui permet aux utilisateurs et aux clients sans fil d'être authentifiés localement sur le contrôleur. Cette méthode est conçue pour une utilisation dans les bureaux distants qui veulent conserver la connectivité avec les clients sans fil lorsque le système principal est perturbé ou que le serveur d'authentification externe est en panne. Lorsque vous activez l'EAP local, le contrôleur sert de serveur d'authentification et de base de données d'utilisateurs locaux, de sorte qu'il supprime la dépendance vis-à-vis d'un serveur d'authentification externe. L'authentification EAP locale récupère les identifiants de l'utilisateur à partir de la base de données des utilisateurs locaux ou de la base de données LDAP principale pour authentifier les utilisateurs. Le protocole EAP local prend en charge l'authentification LEAP, EAP-FAST, EAP-TLS, P EAPv0/MSCHAPv2 et PEAPv1/GTC entre le contrôleur et les clients sans fil.

L'EAP local peut utiliser un serveur LDAP comme base de données principale pour récupérer les informations d'identification des utilisateurs.

Une base de données principale LDAP permet au contrôleur de demander à un serveur LDAP les informations d'identification (nom d'utilisateur et mot de passe) d'un utilisateur particulier. Ces informations d'identification sont ensuite utilisées pour authentifier l'utilisateur.

La base de données du serveur principal LDAP prend en charge les méthodes EAP locales suivantes :

- EAP-FAST/GTC
- EAP-TLS
- PEAPv1/GTC.

LEAP, EAP-FAST/MSCHAPv2 et PEAPv0/MSCHAPv2 sont également pris en charge, **mais uniquement si le serveur LDAP est configuré pour renvoyer un mot de passe en texte clair**. Par exemple, Microsoft Active Directory n'est pas pris en charge car il ne renvoie pas de mot de passe en texte clair. Si le serveur LDAP ne peut pas être configuré pour renvoyer un mot de passe en texte clair, LEAP, EAP-FAST/MSCHAPv2 et PEAPv0/MSCHAPv2 ne sont pas pris en charge.

Remarque : si des serveurs RADIUS sont configurés sur le contrôleur, celui-ci tente d'authentifier les clients sans fil à l'aide des serveurs RADIUS en premier. L'authentification EAP locale est utilisée uniquement si aucun serveur RADIUS n'est détecté, soit parce que les serveurs RADIUS ont expiré, soit parce qu'aucun serveur RADIUS n'a été configuré. Si quatre serveurs RADIUS sont configurés, le contrôleur tente d'authentifier le client avec le premier serveur RADIUS, puis avec le deuxième serveur RADIUS, puis avec le protocole EAP local. Si le client tente de s'authentifier à nouveau manuellement, le contrôleur tente le troisième serveur RADIUS, puis le quatrième serveur RADIUS, et enfin le protocole EAP local.

Cet exemple utilise EAP-FAST comme méthode EAP locale sur le WLC, qui à son tour est configuré pour interroger la base de données principale LDAP pour les informations d'identification d'utilisateur d'un client sans fil.

Configurer

Ce document utilise EAP-FAST avec des certificats à la fois du côté client et du côté serveur. Pour cela, le programme d'installation utilise le serveur **Microsoft Certificate Authority (CA)** pour générer les certificats client et serveur.

Les informations d'identification de l'utilisateur sont stockées dans le serveur LDAP de sorte qu'en cas de validation de certificat réussie, le contrôleur interroge le serveur LDAP afin de récupérer les informations d'identification de l'utilisateur et authentifie le client sans fil.

Ce document suppose que ces configurations sont déjà en place :

- Un LAP est enregistré auprès du WLC. Référez-vous à <u>Enregistrement d'un point d'accès</u> <u>léger (LAP) à un contrôleur de réseau local sans fil (WLC)</u> pour plus d'informations sur le processus d'enregistrement.
- Un serveur DHCP est configuré pour attribuer une adresse IP aux clients sans fil.
- Le serveur Microsoft Windows 2003 est configuré en tant que contrôleur de domaine et serveur AC. Cet exemple utilise wireless.com comme domaine.Référez-vous à <u>Configuration</u> <u>de Windows 2003 en tant que contrôleur de domaine</u> pour plus d'informations sur la configuration d'un serveur Windows 2003 en tant que contrôleur de domaine.Référez-vous à <u>Installer et configurer le serveur Microsoft Windows 2003 en tant que serveur d'autorité de</u> <u>certification (CA)</u> afin de configurer le serveur Windows 2003 en tant que serveur d'autorité de certification d'entreprise.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Complétez ces étapes afin d'implémenter cette configuration :

- Configurer EAP-FAST en tant que méthode d'authentification EAP locale sur le WLC
- <u>Configurer le serveur LDAP</u>
- Configuration du client sans fil

Configurer EAP-FAST en tant que méthode d'authentification EAP locale sur le WLC

Comme mentionné précédemment, ce document utilise EAP-FAST avec des certificats côté client et côté serveur comme méthode d'authentification EAP locale. La première étape consiste à télécharger et à installer les certificats suivants sur le serveur (WLC, dans ce cas) et le client.

Le WLC et le client ont chacun besoin de ces certificats pour être téléchargés à partir du serveur CA :

- Certificat de périphérique (un pour le WLC et un pour le client)
- Certificat racine de l'infrastructure à clé publique (PKI) pour le WLC et certificat CA pour le client

Générer un certificat de périphérique pour le WLC

Exécutez ces étapes afin de générer un certificat de périphérique pour le WLC à partir du serveur CA. Ce certificat de périphérique est utilisé par le WLC pour s'authentifier auprès du client.

1. Accédez à http://<adresse IP du serveur AC>/certsrv à partir de votre PC qui dispose d'une connexion réseau au serveur AC. Connectez-vous en tant qu'administrateur du serveur AC.

about:blank - Microsoft Internet Explorer		- e 🛛
File Edt View Filewrites Total Help		
Address Mtp://10.77.244.198/certsrv		🛩 💽 Go
	Connect to 10.77.244.198	
Opening page http://10.77.244.190/certsrv	(14)	S Internet
Célestienne Demender un		

2. Sélectionnez **Demander un** certificat.

File Edit Ven Feworitäs Tools / Help Tools / Help Address Image: Addres Image: Address Image: Address	forme
	- 🔁 😡
Microsoft Certificate Services wireless Microsoft Certificate Services wireless Welcome Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request perform other security tasks.	iome 🥖
Welcome Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request perform other security tasks.	it,
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request perform other security tasks.	st.
become a second research research	
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.	>
For more information about Certificate Services, see Certificate Services Documentation.	
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	

3. Dans la page Demander un certificat, cliquez sur Demande de certificat

avancee.	
Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Pavoritis' Tools' Help	A
Address 🕘 Ntp://10.77.241.198/certsrv/certraus.esp	🖂 🛃 Go
	<u>s</u>
Alicrosoff Certificate Services weeless	Heme
Request a Certificate	
Select the certificate type:	
User Contriccto	
Or submit an advanced certificate request.	
http://10.77.244.198/certsrv/certroad.asp	Internet

4. Dans la page Demande de certificat avancée, cliquez sur **Créer et envoyer une demande à** cette autorité de certification. Vous accédez alors au formulaire de demande de certificat avancé.

Microsoft Certificate Services - Microsoft Internet Explorer		
File Edit View Favorites Tools Help		
Address al http://10.77.244.198/certsrv/certrgad.asp		🛩 🔁 Go
Microsoft Certificate Services wireless		Heme
Advanced Certificate Request		
The policy of the CA determines the types of certificates you can request. Click o	ne of the following options to:	
Create and submit a request to this CA.		
Submit a certificate request by using a base 64-encoded CMC or PKCS #10 PKCS #7 file	file, or submit a renewal request by using a b	ase-64-encoded
Request a certificate for a smart card on behalf of another user by using the sr Note: You must have an enrollment agent certificate to submit a request on behalf of another	mart card certificate enrolment station. ruser.	
ภ		😳 Internet

- 5. Dans le formulaire de demande de certificat avancé, sélectionnez Serveur Web comme modèle de certificat. Spécifiez ensuite un nom pour ce certificat de périphérique.Cet exemple utilise le nom de certificat ciscowlc123. Complétez les autres informations d'identification selon vos besoins.
- 6. Dans la section Options de clé, sélectionnez l'option Marquer les clés comme exportables. Parfois, cette option particulière est grisée et ne peut pas être activée ou désactivée si vous choisissez un modèle de serveur Web. Dans ce cas, cliquez sur Back du menu du navigateur pour revenir à une page précédente et revenir à cette page. Cette fois, l'option Marquer les clés comme exportables doit être disponible

disponible.	
Alicrosoft Certificate Services - Microsoft Internet Explorer	
Me Edt Wew Pavorites Tools Help	40
Gask · D - 2 C - 2 centh of Parentes @ 2. 3 20 28	
Address a http://10.77.244.198/cartary/certrgna.aap	💌 🛃 GO
Microsoff Certificate Services Vinetess	Heme
Advanced Certificate Request	
Contribution Terror Later	
Certificate i empiate:	
Web Server	
Identifying Information For Offline Template:	
Name: ciscowlc123	
E-Mail	
Company: cisco	
Department	
Caw .	
State	
Country/Region	
Key Options:	
Create new key set Ouse existing key set	
CSP: Microsoft RSA SChannel Cryptographic Previder	
Key Usage: (*) Exchange	
Key Size: 1024 http://doi.org/10.000/1022/2008/4000-0162/10204/)	
Automatic key container name O User specified key container name	
Mark keys as exportable	
Export keys to file	
Lenable strong private key protection	
 Store certificate in the local computer certificate store Characterize additional is the local computer store 	
Done	Internet

7. Configurez tous les autres champs nécessaires et cliquez sur **Submit**.

Microsoft Certificate Services - Microsoft Internet Explorer	
Pile Edit View Pavorites Tools Help	
🔇 bad. • 💿 - 🗟 😰 🐔 🔎 Search 🦅 Pavorites 🤣 😥 🖓 🦝 🦓	
ZdShess (a) http://10.77.244.198/certary/certrgna.asp	💌 🔁 😡 .
Create new key set	
CSP: Microsoft RSA SChannel Cryptographic Previder 🛩	
Key Usage: 🛞 Exchange	
Key Size: 1024 Min: 304 (common key sizes: 532 5029 2049 6085 5392 10009) Marc 16304	
Automatic key container name	
Mark keys as exportable	
Export keys to file	
Enable strong private key protection	
Store centicate in the local computer certificate store Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.	
Additional Options:	
Request Format: O CMC @ PKCS10	
Hash Algorithm: SHA-1 V	
Only used to sign request.	
Save request to a file	
Attributes:	
Friendly Name:	
Submit >	
	Internet

8. Cliquez sur **Yes** dans la fenêtre suivante afin d'autoriser le processus de demande de certificat.

Potentia	al Scripting Violation
⚠	This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?
	Yes No

 La fenêtre Certificate Issued (Certificat émis) s'affiche et indique que le processus de demande de certificat a réussi. L'étape suivante consiste à installer le certificat émis dans le magasin de certificats de ce PC. Cliquez sur Installer ce certificat.

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Pavorities' Tools Help	
Address all http://10.77.244.198/certsrv/certfinsh.asp	💌 🛃 Go
All second Carl Second Carl Second Second	· · · · · · · · · · · · · · · · · · ·
Microsoff Certificate Services - Wireless	Home
Certificate Issued	
The certificate you requested was issued to you.	
Install this certificate	
in the second	

10. Le nouveau certificat est correctement installé sur le PC à partir duquel la demande est générée vers le serveur

NC.	
Microsoft Certificate Services - Microsoft Internet Explorer	
Ve Edit Were Pavorites Tools Help	
ddrece 🕘 Mtgc//10.77.244.198/certsrvy/certrepn.asp	💌 🎒 Go
Microsoff Certificate Services wireless	Heme
Certificate Installed	
Your new certificate has been successfully installed.	
Q Hann	The second second
Tonu	Uncerner,

11. L'étape suivante consiste à exporter ce certificat du magasin de certificats vers le disque dur en tant que fichier. Ce fichier de certificat sera utilisé ultérieurement pour télécharger le certificat sur le WLC.Afin d'exporter le certificat à partir du magasin de certificats, ouvrez le navigateur Internet Explorer, puis cliquez sur **Outils > Options** Internet.

🔹 about:blank - Microsofi Internet Explorer	 IE	×
Pile Edit View Pavorbes Tools Help	1	r
Pie Citi Ver Pevorie Address a about Bark. Pop so Bloke Propos Bloke Undoes Resenger Son Zava Console Sterreet Citizets.	- G	
		Y
Enables you to change settings.		

12. Cliquez sur **Content > Certificates** afin d'accéder au magasin de certificats où les certificats sont installés par

défaut.

Internet Options 🔹 💽 🔀
General Security Privacy Content Connections Programs Advanced
Content Advisor Ratings help you control the Internet content that can be viewed on this computer. Enable Settings
Certificates
Use certificates to positively identify yourself, certification authorities, and publishers.
Clear SSL State Certificates Publishers
Personal information
AutoComplete stores previous entries and suggests matches for you. AutoComplete
Microsoft Profile Assistant stores your My Profile

 13. Les certificats de périphérique sont généralement installés dans la liste de certificats personnels. Ici, vous devriez voir le certificat nouvellement installé. Sélectionnez le certificat et cliquez sur Exporter.

ertificates			? 🏼
Intended purpose:	<all></all>		~
Personal Other Per	ople Intermediate Certification	Authorities Trusted Root Ce	tification < >
Issued To	Issued By	Expiratio Friendly Na	me
ciscowlc123	wireless	1/25/2010 <none></none>	
Import	port Remove		Advanced
-Certificate intended	DUIDOSOS		
Conver Authoriticatio	-		
Server Authenticatio	n		View
Server Authenticatio	n		View
Server Authenticatio	n		View

14. Cliquez sur **Next** dans les fenêtres suivantes. Sélectionnez l'option **Oui, exporter la clé privée** dans la fenêtre **Assistant Exportation de certificat**. Cliquez sur **Next**

(Suivant).	
Certificate Export Wizard	
Export Private Key You can choose to export the private key with the certificate.	
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.	
Do you want to export the private key with the certificate?	
Yes, export the private key	
No, do not export the private key	
< Back Next > Cancel	

 Choisissez le format de fichier d'exportation .PFX et choisissez l'option Enable strong protection. Cliquez sur Next (Suivant).

Select the format yo	u want to use:
	binary X.509 (.CER)
Base-64 enco	ded X.SU9 (.CER)
Cryptographi	c Message Syntax Standard - PKCS #7 Certificates (.P7B)
Personal Info	rmation Exchange - PKC5 #12 (.PFX)
Include al	certificates in the certification path if possible
🗹 Enable str	ong protection (requires IE 5.0, NT 4.0 SP4 or above)
Delete th	a private key if the export is successful

16. Dans la fenêtre Password, saisissez un mot de passe. Cet exemple utilise **cisco** comme mot de

passe.			
Certific	ate Export Wizard		
Pass T	word o maintain security, you must protect t	he private key by using a passwo	ord.
т	ype and confirm a password. Password:		

	Confirm password:		
		< <u>B</u> ack <u>N</u> ext >	Cancel

17. Enregistrez le fichier de certificat (fichier .PFX) sur votre disque dur. Cliquez sur **Next** et terminez le processus d'exportation avec



Téléchargement du certificat de périphérique sur le WLC

Maintenant que le certificat de périphérique WLC est disponible sous la forme d'un fichier .PFX, l'étape suivante consiste à télécharger le fichier sur le contrôleur. Les WLC Cisco acceptent les certificats uniquement au format .PEM. Par conséquent, vous devez d'abord convertir le fichier au format .PFX ou PKCS12 en fichier PEM à l'aide du programme openSSL.

Convertir le certificat au format PFX en PEM à l'aide du programme openSSL

Vous pouvez copier le certificat sur n'importe quel PC sur lequel vous avez installé openSSL pour le convertir au format PEM. Entrez ces commandes dans le fichier Openssl.exe du dossier bin du programme openSSL :

Remarque : vous pouvez télécharger openSSL à partir du site Web OpenSSL.

!--- ciscowlc123 is the name used in this example for the exported file. !--- You can specify
any name to your certificate file. Enter Import Password : cisco
!--- This is the same password that is mentioned in step 16 of the previous section. MAC
verified Ok Enter PEM Pass phrase : cisco
!--- Specify any passphrase here. This example uses the PEM passphrase as cisco. Verifying - PEM
pass phrase : cisco

Le fichier de certificat est converti au format PEM. L'étape suivante consiste à télécharger le certificat de périphérique au format PEM sur le WLC.

Remarque : avant cela, vous avez besoin d'un logiciel de serveur TFTP sur votre PC à partir duquel le fichier PEM va être téléchargé. Ce PC doit être connecté au WLC. Le répertoire courant et le répertoire de base du serveur TFTP doivent être spécifiés avec l'emplacement de stockage du fichier PEM.

Télécharger le certificat de périphérique au format PEM converti sur le WLC

Cet exemple explique le processus de téléchargement via l'interface de ligne de commande du WLC.

- 1. Connectez-vous à la CLI du contrôleur.
- 2. Entrez la commande transfer download datatype eapdevcert.
- 3. Entrez la commande **transfer download serverip** *10.77.244.196*.10.77.244.196 est l'adresse IP du serveur TFTP.
- 4. Entrez la commande **transfer download filename** *ciscowlc.pem*.ciscowlc123.pem est le nom de fichier utilisé dans cet exemple.
- 5. Entrez la commande **transfer download certpassword** pour définir le mot de passe du certificat.
- 6. Entrez la commande transfer download start pour afficher les paramètres mis à jour.Répondez ensuite y lorsque vous êtes invité à confirmer les paramètres actuels et à lancer le processus de téléchargement.Cet exemple montre le résultat de la commande download :

(Cisco Controller) >transfer download start

Mode.TFTPData Type.Vendor Dev CertTFTP Server IP.10.77.244.196TFTP Packet Timeout.6TFTP Max Retries.10TFTP Path.10TFTP Filename.ciscowlc.pem

This may take some time. Are you sure you want to start? (y/N) y TFTP EAP CA cert transfer starting. Certificate installed. Reboot the switch to use the new certificate. Enter the reset system command to reboot the controller. The controller is now loaded with the device certificate.

7. Entrez la commande **reset system** pour redémarrer le contrôleur. Le contrôleur est maintenant chargé avec le certificat du périphérique.

Installer le certificat racine de PKI dans le WLC

Maintenant que le certificat de périphérique est installé dans le WLC, l'étape suivante consiste à installer le certificat racine de l'ICP sur le WLC à partir du serveur AC. Effectuez les étapes suivantes :

1. Accédez à http://<adresse IP du serveur AC>/certsrv à partir de votre PC qui dispose d'une connexion réseau au serveur AC. Connectez-vous en tant qu'administrateur du serveur AC.

AU.		
about:blank - Microsoft Internet Explorer		- • 🔀
File Edit View Palvortes Totat Help		an 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 19
Address Mtp://10.77.244.198/certsrv		🛩 💽 Go
Cpening page http://10.77.244.190/certerv	Connect to 10.77.244.198	et

2. Cliquez sur Download a CA certificate, certificate chain ou

CRL.	
Microsoft Certificate Services - Microsoft Internet Explorer	
We Edit Vers Twortes Tools 1940	4
33ress a http://10.77.244.198/certary/	💌 🔁 😡
Allerande Collinson Stationers Includes	Uama
ANCTORE CENTRE AND A MEMORY	nome
Nelcome	
Use this Web site to request a certificate for your Web browser, e-mail client, or other identity to people you communicate with over the Web, sign and encrypt messages, an perform other security tasks.	program. By using a certificate, you can verify your nd, depending upon the type of certificate you request,
You can also use this Web site to download a certificate authority (CA) certificate, cert iew the status of a pending request.	ificate chain, or certificate revocation list (CRL), or to
For more information about Certificate Services, see Certificate Services Documental	tion.
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	
	Tobaccash
	La roter rees

3. Dans la page résultante, vous pouvez voir les certificats d'autorité de certification actuels

disponibles sur le serveur d'autorité de certification dans la zone **Certificat d'autorité de certification**. Choisissez **DER** comme méthode de codage et cliquez sur **Télécharger le certificat**

CA. Microsoft Certificate Services - Microsoft Internet Explorer File Edit View Pavorities Tools Help Address 🍓 http://10.77.244.198/certsrv/certcarc.asp Microsoft Certificate Services - wirele Download a CA Certificate, Certificate Chain, or CRL To trust certificates issued from this certification authority, install this CA certificate chain To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method CA certificate: Current (wireless) Encoding method: DER O Base 64 Download CA certificate Download CA certificate chain Download latest base CR Download latest delta CRL Internet

- 4. Enregistrez le certificat en tant que fichier **.cer**. Cet exemple utilise **certnew.cer** comme nom de fichier.
- 5. L'étape suivante consiste à convertir le fichier .cer au format PEM et à le télécharger sur le contrôleur. Afin d'effectuer ces étapes, répétez la même procédure expliquée dans la section <u>Téléchargement du certificat de périphérique vers le WLC</u> avec ces modifications :Les fichiers openSSL "-in" et "-out" sont certnew.cer et certnew.pem.En outre, aucune phrase de passe PEM ou aucun mot de passe d'importation n'est requis dans ce processus.En outre, la commande openSSL pour convertir le fichier .cer en fichier .pem est :x509 -in certnew.cer inform DER -out certnew.pem -outform PEMÀl'étape 2 de la section <u>Télécharger le certificat de périphérique au format PEM converti vers le WLC</u>, la commande pour télécharger le certificat de périphérique au format PEM converti vers le WLC, la commande pour télécharger le certificat vers le WLC est :(Cisco Controller)>transfer download datatype eapcacertLe fichier à télécharger sur le WLC est certnew.pem.

Vous pouvez vérifier si les certificats sont installés sur le WLC à partir de l'interface graphique utilisateur du contrôleur comme suit :

 Dans l'interface graphique utilisateur du WLC, cliquez sur Security. Dans la page Security, cliquez sur Advanced > IPSec Certs dans les tâches qui apparaissent sur la gauche. Cliquez sur CA Certificate afin d'afficher le certificat CA installé. Voici l'exemple :



 Afin de vérifier si le certificat de périphérique est installé sur le WLC, à partir de la GUI du WLC, cliquez sur Security. Dans la page Security, cliquez sur Advanced > IPSec Certs dans les tâches qui apparaissent sur la gauche. Cliquez sur ID Certificate afin d'afficher le certificat de périphérique installé. Voici

i exemple :										
wic2006 - Microsoft Inter	rnet Explorer									
File Edit View Favorites	Tools Help									<u></u>
ahaha									Eing	Logout <u>R</u> efresh
CISCO	MONITOR	WLANS	CONTROLLER	W1RELESS	SECURITY	MANAGEMENT	COMMANDS	HELP		
Security	ID Certific	cate			\bigcirc					New
T AAA	Name		Ya	lid Period						
General	bsnSslEapC)evCert	Fro	m 2008 Jan 24	th. 12:18:31 (GMT Until 2010 Jar	n 23rd, 12:18:31			
Authentication										
Accounting TACACS+										
LDAP.										
MAC Filtering										
Disabled Clients User Login Policies										
AP Policies										
E Local EAP										
F Priority Order										
E Access Control Lists										
Wireless Protection Policies										
F Web Auth										
- Advanced										
Sensors										
Shunned Clients										
1D Certificate										
8									🛆 🥥 Inte	ernet

Générer un certificat de périphérique pour le client

Maintenant que le certificat du périphérique et le certificat de l'autorité de certification sont installés sur le WLC, l'étape suivante consiste à générer ces certificats pour le client.

Exécutez ces étapes afin de générer le certificat de périphérique pour le client. Ce certificat sera utilisé par le client pour s'authentifier auprès du WLC. Ce document explique les étapes impliquées dans la génération de certificats pour le client professionnel Windows XP.

 Accédez à http://<adresse IP du serveur AC>/certsrv à partir du client qui nécessite l'installation du certificat. Connectez-vous au serveur AC en tant que nom de domaine\nom d'utilisateur. Le nom d'utilisateur doit correspondre au nom de l'utilisateur qui utilise cette machine XP et l'utilisateur doit déjà être configuré comme faisant partie du même domaine que le serveur

AC.	
Connect to 10.7	7.244.198 🔹 💽
Connecting to 10.7	7.244.198
User name:	🖸 wireless\user2
Password:	•••••
	Remember my password
	OK Cancel

2. Sélectionnez Demander un

certificat.

Microsoft Certificate Services - Microsoft Internet Explorer	X
The Edit View Favorities Tools Help	11
d3mm 👸 http://10.77.244.198/certsrv/	Go
Microsoft Certificate Services - wireless Hame Welcome Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your	
identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.	
For more information about Certificate Services, see <u>Certificate Services Documentation</u> . Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	
1 Diternet	

3. Dans la page Demander un certificat, cliquez sur Demande de certificat

avancée.

Microsoft Certificate Services - Microsoft Internet Explorer	
We Edit Wew Pavarties Tools Help	1
schoss 🖓 http://10.77.244.198/certsrv/certrous.asp	🚽 🛃 G
I Research Carlifords Carloss	Hama
MILCOSOF CENTILIES SERVICES - WHENESS	Home
Request a Certificate	
elect the certificate type:	
User Certificate	
Dr. submit an advanced certificate request	
A CARACTER OF BETTER COMPANY CONTRACTOR	
http://ID 77 244 108/weteps/pattered are	Tokarnak

4. Dans la page Demande de certificat avancée, cliquez sur **Créer et envoyer une demande à cette autorité de certification**. Vous accédez alors au formulaire de demande de certificat avancé

Microsoft Certificate Services - Microsoft Internet Explorer	🗖 🖻 🔀
Pile Edit View Pavorites Tools Help	
Address 🕘 Napol/10.77.244.190/certsrv/certrqad.asp	💌 🛃 Go
Mirmanii Cartificate Senitop wixilaat	Home
Michael Constant Servers - Maters	il sille
Advanced Certificate Request	
The policy of the CA determines the lupes of certificates you can request. Click one of the following options to:	
The party of the Crick of the termines the types of central terms you can request. Circk of the of the following options to:	
	- have be an end of
Subtrit a certificate request by using a base-b4-encoded CMC or PKCS #10 file, or submit a renewal request by using a PKCS #7 file.	a base-64-encoded
Request a certificate for a smart card on behalf of another user by using the smart card certificate enrolment station.	
Note: You must have an enrollment agent certificate to submit a request on behalf of another user.	
	C Internet
ans le formulaire de demande de certificat avancé. choisissez Utilisateur dar	າs le menu

5. Dans le formulaire de demande de certificat avancé, choisissez Utilisateur dans le menu déroulant Modèle de certificat.Dans la section Key options, choisissez les paramètres suivants :Saisissez la taille de la clé dans le champ Taille de la clé. Cet exemple utilise 1024.Cochez l'option Marquer les clés comme exportables.

Microsoft Certi	ficate Services - Microsoft Internet Explorer	
File Edit View	Favorites Tools Help	
Address 🔕 http://10	1.77.244.198/certsrv/certroma.asp	🗹 🔁 😡
Microsoft Certifi	tate Services wreless	Home
Advanced Ce	rtificate Dequest	
Haveneed de	Thireate Request	
Certificate Tem	date:	
	Basic EFS 💌	
	Basic EFS	
Key Options:	User	
	Create new key set OUse existing key set	
CSP:	Microsoft Enhanced Cryptographic Provider v1.0 💌	
Key Usage:	Exchange	
Key Size:	1024 Min: 394 (common key sizes: 512 3924 2049 9996 0192 16294.)	
	Automatic key container name OUser specified key container name	
	Mark keys as exportable	
	Export keys to file	
	Enable strong private key protection	
	Store certificate in the local computer certificate store	
	Stores the certificate in the local computer store instead of in the user's certificate store. Does not	
	install the root CA's certificate. You must be an	
	administrator to generate or use a key in the local machine store	
	mar name source.	
Additional Optic	05:	
Request Format:	©CMC OPKCS10	
Hash Algorithm.	SHA-1 👻	
-	Only used to sign request.	
	Save request to a file	
	<u> </u>	
Attributes:		
Done		Internet

6. Configurez tous les autres champs nécessaires et cliquez sur

Submit.	
3 Microsoft Certificate Services - Microsoft Internet Explorer	
Pile Edit View Pavoržes Tools Help	
🔇 Ball + 🜍 - 📧 🗟 🐔 🔎 Search 👷 Pavortes 🥝 🔗 😓 🖼 🦓	
Address 🕘 http://10.77.244.198/certsrv/certrgna.asp	💌 🔁 Go
Treate new key set Use existing key set	
CSP: Microsoft RSA SChannel Cryptographic Previder 👻	
Kay Usaga: 🐵 Exchange	
Key Size: 1024 Mic: 1034 (remmon key size: 512 5025 2045 6095 5192 10304)	
Automatic key container name O User specified key container name	
Mark keys as exportable	
Export keys to file	
Enable strong private key protection	
Stoves the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local mechine store.	
Additional Options: Request Format: O CMC	
Hash Algorithm SHA-1 ×	
Only used to sign request.	
Save request to a file	
Attributes:	
Friendly Name:	
Submit >	
	 Internet

7. Le certificat de périphérique du client est maintenant généré conformément à la demande. Cliquez sur **Installer le certificat** afin d'installer le certificat dans le magasin de certificats.

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	A¥
Address 🕘 http://10.77.244.190/certsrv/certfinsh.asp	🚽 🔁 ຜ
	<u>A</u>
Microsoff Certificate Services wireless	Home
Certificate Issued	
The certificate you requested was issued to you.	
Install this certificate	
e)	Internet

 Vous devriez pouvoir trouver le certificat de périphérique du client installé sous la liste de certificats personnels sous Outils > Options Internet > Contenu > Certificats sur le navigateur IE du

client.			
Certificates			<u>?</u> 🔀
Intended purpose: <	All>		~
Personal Other People	Intermediate Certification	n Authorities Trusted Root (Certification
Issued To	Issued By	Expiratio Eriendly (Name
E 1234	wireless	1/25/2009 <none></none>	
Import Export	Remove		Advanced
Certificate intended purp	oses		
Encrypting File System			
			View
			Close

Le certificat de périphérique du client est installé sur le client.

Générer le certificat CA racine pour le client

L'étape suivante consiste à générer le certificat CA pour le client. Exécutez les étapes suivantes à partir du PC client :

 Accédez à http://<adresse IP du serveur AC>/certsrv à partir du client qui nécessite l'installation du certificat. Connectez-vous au serveur AC en tant que nom de domaine\nom d'utilisateur. Le nom d'utilisateur doit correspondre au nom de l'utilisateur qui utilise cette machine XP et l'utilisateur doit déjà être configuré comme faisant partie du même domaine que le serveur

AC.		
Connect to 10.	77.244.198 🛛 😨 📔	×
Connecting to 10.	77.244.198	
User name:	🛃 wireless\user2	
Password:	•••••	
	Remember my password	
	OK Cancel	ו

 Dans la page résultante, vous pouvez voir les certificats d'autorité de certification actuels disponibles sur le serveur d'autorité de certification dans la zone Certificat d'autorité de certification. Sélectionnez Base 64 comme méthode de codage. Cliquez ensuite sur Download CA certificate et enregistrez le fichier sur le PC du client en tant que fichier .cer. Cet exemple utilise rootca.cer comme nom de fichier

Microsoft Certificate Services - Microsoft Internet Explorer	
Pier Edit Vers Parliffes Took Pielo	
Address Mhtp://10.77.244.190/certsrv/certcarc.asp	💌 🔁 😡
Mission Conference Sections - windows	Hama
ARCHART CONTRACTOR AND A	noms
Download a CA Certificate, Certificate Chain, or CRL	
To trust certificates issued from this certification authority, install this CA certificate chain.	
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.	
CA certificate:	
Current (wireless)	
Encoding method:	
ODER	
Base 64	
Download CA certificate	
Download CA certificate chain	
Download latest base CRL	
Download latest deta CHL	
	Internet

3. Ensuite, installez le certificat CA enregistré au format .cer dans le magasin de certificats du client. Double-cliquez sur le fichier rootca.cer et cliquez sur **Install Certificate**.

Certificate	? 🗙
General Details Certification Path	
Certificate Information	_
This certificate is intended for the following purpose(s): • All issuance policies • All application policies	
Issued to: wireless	-
Issued by: wireless	
Valid from 1/23/2008 to 1/23/2013	
Install Certificate Issuer Stateme	nt K

4. Cliquez sur **Next** afin d'importer le certificat du disque dur du client vers le magasin de certificats.

Certificate Import Wizard		$\mathbf{\times}$
	Welcome to the Certificate Import Wizard This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store. A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept. To continue, click Next.	
	< Back Next > Cancel	

5. Choisissez Automatically select the certificate store based on the type of certificate et cliquez sur

Next.

r tificate Store Certificate stores are system a	areas where certificates are kept.
Windows can automatically sel	ect a certificate store, or you can specify a location fo
 Automatically select the 	certificate store based on the type of certificate
O Place all certificates in the second se	he following store
Certificate store:	
	Browse

6. Cliquez sur **Finish** afin de terminer le processus d'importation

Completing the Certificate Impo Wizard You have successfully completed the Certificate Impo wizard. You have specified the following settings: Certificate Store Selected Automatically determine Content Certificate	ort ^{rt} d by t
< Back Finish C	ancel
	Completing the Certificate Impo Wizard You have successfully completed the Certificate Impo wizard. You have specified the following settings: Certificate Store Selected Automatically determine Content Certificate

7. Par défaut, les certificats CA sont installés sous la liste Autorités de certification racine de confiance sur le navigateur IE du client sous Outils > Options Internet > Contenu > Certificats. Voici l'exemple :

termediate Certification Au	thorities Trusted Root C	ertification Aut	Trusted Publ	4
Issued to	Issued By	Expiratio	Friendly Name	-
VeriSign Trust Netw	VeriSign Trust Network	5/19/2018	VeriSign Class 3	
VeriSign Trust Netw	VeriSign Trust Network	8/2/2028	VeriSign Class 3	
VeriSign Trust Netw	Verisign Trust Network	5/19/2018	VeriSign Class 4	
VeriSign Trust Netw	Verisign Trust Network	8/2/2028	VeriSign Class 1	
VeriSign Trust Netw	verisign Trust Network	8/2/2028	Verisign Class 4	
Verisign Trust Netw	Verisign Trust Network	6/19/2018	Verisign Class 1	
No Wreless	Wireless	1/23/2013	<none></none>	
End Wireless-CA	Wireless-CA	7/11/2012	<none></none>	
	Near CE by Dor	7711/2009	ACCIT 22 07 031	~
Import Export Certificate intended purpose	Remove		Advanc	ed.
<all></all>			View	

Tous les certificats requis sont installés sur le WLC ainsi que sur le client pour l'authentification EAP-FAST Local EAP. L'étape suivante consiste à configurer le WLC pour l'authentification EAP locale.

Configurer le protocole EAP local sur le WLC

Complétez ces étapes à partir du **mode GUI** du WLC afin de configurer l'authentification EAP locale sur le WLC :

1. Cliquez sur **Security > Local**

EAP. wic2006 - Microsoft Inter	rnet Explorer
File Edit View Pavorites	Tools Help
ululu cisco	Saye Configuration Eing Logout Befresh MONITOR WLANS CONTROLLER WIRELESS BECURITY MANAGEMENT COMMANDS HELP
Security	RADIUS Authentication Servers Apply New
 AAA General RACIUS Authentication Accounting TACAC3+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies Priority Order Access Control Lists Wireless Protection Policies Web Auth Advanced 	Call Station ID Type IP Address S Use AES Key Wrop C (Designed for FIPS customers and requires a key wrap compliant RADIUS server) Network User Management Server Index Server Address Port IPSec Admin Status
6	A Pitternet

 Sous Local EAP, cliquez sur **Profiles** afin de configurer le profil EAP local.



- 3. Cliquez sur **New** afin de créer un nouveau profil EAP local.
- Configurez un nom pour ce profil et cliquez sur Apply. Dans cet exemple, le nom du profil est Idap. Vous accédez ainsi aux profils EAP locaux créés sur le
 WLC

Wic2006 - Microsoft Inter	net Explorer								
File Edit View Pevorites T	ools Help								27
ahaha							Sa⊻e Co	nfiguration <u>P</u> in	g Logout Befresh
CISCO	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Local EAF	P Profile	s > New					< Back	Apply
 AAA General RADIUS Authentication Accounting TACACS+ LDAP LDAP Load Net Users MAC Filtering Disabled Clients User Login Policies AP Policies 	Profile Nar	me		Idap					
 Local EAP General Profiles EAP-FAST Parameters Authentication Priority 									
▶ Priority Order									
Access Control Lists									
Wireless Protection Policies									
▶ Web Auth									
▶ Advanced									
(i) Done								A •	Internet

 Cliquez sur le profil Idap qui vient d'être créé, qui apparaît sous le champ Nom du profil de la page Profils EAP locaux. Vous accédez à la page Profils EAP locaux > Modifier.

wic2006 - Microsoft Inter	rnet Explorer								
File Edit View Pavorites	Tools Help	_							
ahaha								nfiguration Ping	Logout Refresh
CISCO	MONITOR	<u>WLAN5</u>	CONTROLLER	W]RELES	S SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Local EA	P Profile	0		_			New	Apply
- AAA	Profile Na	me		LEAP	EAP-PAST	EAP-TLS	PEAP		
General * RADIUS Authentication Accounting * TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Idea							0	
 Local EAP General Profiles EAP-FAST Parameters Authentication Priority 									
▶ Priority Order									
▶ Access Control Lists									
Wireless Protection Policies									
▶ Web Auth									
Advanced									
(4)								🛆 🙂 Ir	ternet

6. Configurez les paramètres spécifiques à ce profil sur la page Profils EAP locaux > Modifier.Sélectionnez EAP-FAST comme méthode d'authentification EAP locale.Activez les cases à cocher en regard de Certificat local requis et Certificat client requis.Choisissez Vendor comme émetteur de certificat car ce document utilise un serveur d'autorité de certification tiers.Activez la case à cocher en regard de Check against CA certificates afin de permettre au certificat entrant du client d'être validé par rapport aux certificats CA sur le contrôleur.Si vous voulez que le nom commun (CN) dans le certificat entrant soit validé par rapport au CN des certificats CA sur le contrôleur, cochez la case Vérifier l'identité CN du certificat. Le paramètre par défaut est désactivé. Afin de permettre au contrôleur de vérifier que le certificat du périphérique entrant est toujours valide et n'a pas expiré, cochez la case Vérifier la validité de la date du certificat.Remarque : la validité de la date du certificat est comparée à l'heure UTC (GMT) actuelle configurée sur le contrôleur. Le décalage du fuseau horaire est ignoré.Cliquez sur Apply.



7. Le profil EAP local avec authentification EAP-FAST est maintenant créé sur le

VVLC.								
wic2006 - Microsoft Inter	net Explorer							
File Edit View Pavorites 1	fools Help							
ahaha							nfiguration <u>P</u> ing	Logout Befresh
CISCO	MONITOR WLA	N5 CONTROLLER	W]RELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Local EAP Pro	files					New	Apply
- AAA	Profile Name		LEAP E	AP-PAST	EAP-TLS	PEAP		
General RADIUS	Ideo			0				
Authentication								
▶ TACACS+								
LOAP Local Net Users								
MAC Filtering Disabled Clients								
User Login Policies								
T Local FAP								
General								
EAP-FAST Parameters								
Authentication Priority								
Priority Order								
Wireless Control Lists								
Policies								
Web Auth								
Advanced								
Cone							🛆 🙂 14	vternet

8. L'étape suivante consiste à configurer les paramètres spécifiques d'EAP-FAST sur le WLC. Dans la page WLC Security, cliquez sur Local EAP > EAP-FAST Parameters afin de passer à la page EAP-FAST Method Parameters.Désactivez la case à cocher Approvisionnement anonyme car cet exemple explique EAP-FAST à l'aide de certificats. Conservez tous les autres paramètres par défaut. Cliquez sur Apply.

wic2006 - Microsoft Inter	net Explorer svis Help			
uluilu cisco	MONITOR WLANS CONTROLLER WIRELES		Sage Configuration	I Ping Logout Befresi
Security	EAP-FAST Method Parameters	\bigcirc		Appty
Constal	Server Key (in hex)	••••		
RADIUS Authentication	Confirm Server Key	••••		
IN TACACS+	Time to live for the PAC	10 doys		
MAC Filtering Disabled Clients	Authority ID (in hex)	436973636f		
User Login Policies AP Policies	Authority ID Information	Cieco A-ID		
* Local EAP Gonard Profiles EAP-FAST Parameters Advisation Prince	Anonymous Provision	Enabled		
Priority Order				
Access Control Lists Wireless Protection Policies				
F Web Auth				
F Advanced				
n				🛆 👄 Internet

Configurer le WLC avec les détails du serveur LDAP

Maintenant que le WLC est configuré avec le profil EAP local et les informations associées, l'étape suivante consiste à configurer le WLC avec les détails du serveur LDAP. Complétez ces étapes sur le WLC :

 Dans la page Security du WLC, sélectionnez AAA > LDAP dans le volet de tâches de gauche afin de passer à la page de configuration du serveur LDAP. Afin d'ajouter un serveur LDAP, cliquez sur New. La page LDAP Servers > New apparaît.



2. Dans la page LDAP Servers Edit, spécifiez les détails du serveur LDAP tels que l'adresse IP du serveur LDAP, le numéro de port, l'état Enable Server, etc.Choisissez un numéro dans la liste déroulante Server Index (Priority) pour spécifier l'ordre de priorité de ce serveur par rapport à tout autre serveur LDAP configuré. Vous pouvez configurer jusqu'à dix-sept serveurs. Si le contrôleur ne peut pas atteindre le premier serveur, il essaie le second dans la liste, etc.Saisissez l'adresse IP du serveur LDAP dans le champ Server IP Address. Saisissez le numéro de port TCP du serveur LDAP dans le champ Port Number. La plage valide s'étend de 1 à 65535, et la valeur par défaut est 389. Dans le champ User Base DN, entrez le nom distinctif (DN) du sous-arbre dans le serveur LDAP qui contient une liste de tous les utilisateurs. Par exemple, ou=unité organisationnelle, .ou=unité organisationnelle suivante et o=corporation.com. Si l'arborescence contenant les utilisateurs est le DN de base, entrez o=corporation.com ou dc=corporation, dc=com.Dans cet exemple, l'utilisateur se trouve sous l'unité d'organisation (OU) **Idapuser** qui, à son tour, est créé dans le domaine Wireless.com.Le DN de base d'utilisateur doit pointer vers le chemin complet où se trouvent les informations d'utilisateur (informations d'identification d'utilisateur selon la méthode d'authentification EAP-FAST). Dans cet exemple, l'utilisateur se trouve sous le DN de base OU=Idapuser, DC=Wireless, DC=com.Pour plus d'informations sur l'unité d'organisation, ainsi que sur la configuration utilisateur, reportez-vous à la section Création d'utilisateurs sur le contrôleur de domaine de ce document. Dans le champ User Attribute, entrez le nom de l'attribut dans l'enregistrement utilisateur contenant le nom d'utilisateur. Dans le champ User Object Type, entrez la valeur de l'attribut LDAP objectType qui identifie l'enregistrement comme utilisateur. Souvent, les enregistrements utilisateur ont plusieurs valeurs pour l'attribut objectType, certains étant propres à l'utilisateur et certains étant partagés avec d'autres types d'objet. Remarque : vous pouvez obtenir la valeur de ces deux champs à partir de votre serveur d'annuaire à l'aide de l'utilitaire de navigation LDAP, fourni avec les outils de support de Windows 2003. Cet outil de navigateur LDAP Microsoft est appelé LDP. À l'aide

de cet outil, vous pouvez connaître les champs DN de base utilisateur, Attribut utilisateur et Type d'objet utilisateur de cet utilisateur particulier. Des informations détaillées sur l'utilisation du protocole LDP pour connaître ces attributs spécifiques à l'utilisateur sont présentées dans la section <u>Utilisation du protocole LDP pour identifier les attributs utilisateur</u> de ce document. Choisissez **Secure** dans la liste déroulante Server Mode si vous souhaitez que toutes les transactions LDAP utilisent un tunnel TLS sécurisé. Sinon, choisissez **None**, qui est le paramètre par défaut. Dans le champ **Server Timeout**, saisissez le nombre de secondes entre les retransmissions. La plage valide s'étend de 2 à 30 secondes, et la valeur par défaut est de 2 secondes. Cochez la case **Enable Server Status** pour activer ce serveur LDAP ou décochez-la pour le désactiver. Par défaut, cette option est désactivée. Cliquez sur Apply pour valider les modifications. Voici un exemple déjà configuré avec ces informations

Wic2006 - Microsoft Intern File Edt. Vew Pavortes To	net Explorer cols Help									
abab								Sa <u>v</u> e Co	nfiguration	Ping Logout Refresh
CISCO	MONITOR	WLANS	CONTROL	LER WIRE	LESS SEC	CURITY	MANAGEMENT	COMMANDS	HELP	
Security TAAA General TAAA General TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies F Local EAP Priority Order Access Control Lists Wireless Protection Policies Wireless Protection Policies	MONITOR L DAP Server In Server Ad Port Numil User Base User Attri User Obje Server Mo Server Til Enable Se	WLANS vers > E dex ldress ber DN bute ext Type ade meout river Status	CONTROL dit 3 3 4 4 5	LER WIRE LI.0.77.244.19 LI.0.77.244.19 S89 DU-Idapuser APAccountly Person Vone 10 second:	LESS SEC	s,DC=cer	n		HE_P < Ba	ck Apply
Done Done									1.10	🕽 🖤 Internet

Maintenant que les détails sur le serveur LDAP sont configurés sur le WLC, l'étape suivante consiste à configurer LDAP comme base de données principale prioritaire afin que le WLC recherche d'abord dans la base de données LDAP les identifiants utilisateur plutôt que toute autre base de données.

Configurer LDAP comme base de données principale prioritaire

Complétez ces étapes sur le WLC afin de configurer LDAP comme base de données principale prioritaire :

 Dans la page Security, cliquez sur Local EAP > Authentication Priority. Dans la page Ordre de priorité > Authentification locale, vous trouverez deux bases de données (Local et LDAP) qui peuvent stocker les informations d'identification et de connexion de l'utilisateur. Afin de faire de LDAP la base de données de priorité, choisissez LDAP dans la zone d'informations d'identification de l'utilisateur du côté gauche et cliquez sur le bouton > afin de déplacer LDAP dans la zone d'ordre de priorité sur le côté

droit

😫 wic2006 - Microsoft Intern	et Explorer								
He Edit View Pavorites To	xols Help						Sa <u>v</u> e Cor	nfiguration Ping	Logout Befresh
cisco	MONITOR	<u>WLAN5</u>	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Priority 0	rder > Lo	ocal-Auth		\smile				Apply
 AAA General RADIUS Authentication Accounting TACACG+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Local EAP General Profile StD-FAST Parameters Authentication Priority Priority Order Access Control Lists Wireless Protection Policies Web Auth Advanced 	LOCAL LDAP	lentials		₽ ₩n					
Ø								🛆 🌒 1	nternet

2. Cet exemple montre clairement que LDAP est sélectionné dans la zone de gauche et que le bouton > est sélectionné. Par conséquent, LDAP est déplacé vers la zone située sur le côté droit qui détermine la priorité. La base de données LDAP est choisie comme base de données de priorité d'authentification.Cliquez sur



Remarque : si LDAP et LOCAL apparaissent dans la zone de droite Informations

d'identification et de connexion de l'utilisateur avec LDAP en haut et LOCAL en bas, Local EAP tente d'authentifier les clients à l'aide de la base de données principale LDAP et bascule vers la base de données utilisateur locale si les serveurs LDAP ne sont pas accessibles. Si l'utilisateur est introuvable, la tentative d'authentification est rejetée. Si LOCAL figure en haut de la liste, Local EAP tente de s'authentifier en utilisant uniquement la base de données des utilisateurs locaux. Il ne bascule pas sur la base de données principale LDAP.

Configurer le WLAN sur le WLC avec l'authentification EAP locale

La dernière étape dans le WLC consiste à configurer un WLAN qui utilise Local EAP comme méthode d'authentification avec LDAP comme base de données principale. Effectuez les étapes suivantes :

- Dans le menu principal du contrôleur, cliquez sur WLANs afin de passer à la page de configuration WLANs. Dans la page WLANs, cliquez sur New afin de créer un nouveau WLAN. Cet exemple crée un nouveau Idap WLAN.Cliquez sur Apply. L'étape suivante consiste à configurer les paramètres WLAN dans la page WLANs > Edit.
- 2. Dans la page WLAN edit, activez l'état de ce WLAN. Configurez tous les autres paramètres nécessaires.



- 3. Cliquez sur Security afin de configurer les paramètres liés à la sécurité pour ce WLAN. Cet exemple utilise la sécurité de couche 2 comme 802.1x avec WEP dynamique 104 bits. Remarque : ce document utilise 802.1x avec le WEP dynamique comme exemple. Il est recommandé d'utiliser des méthodes d'authentification plus sécurisées, telles que WPA/WPA2.
- 4. Dans la page de configuration de la sécurité WLAN, cliquez sur l'onglet AAA servers. Dans la page AAA servers, activez la méthode d'authentification EAP locale et choisissez ldap dans la liste déroulante qui correspond au paramètre EAP Profile Name. Il s'agit du profil EAP local créé dans cet exemple.

3 wic2006 - Microsoft Internet Explorer	E)	- X
Ne Edit View Pavorites Tools Help	Sage Configuration Pine Legeut Be	afresh
CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY	MANAGEMENT COMMANDS HELP	
WLANS WLANS WLANS Advanced Select AAA servers below to override use of default server Radius Servers Authentication Servers Accounting Servers Server 1 None × Server 2 None × Server 3 None × Local EAP Authentication Enabled EAP Profile Name Mone × Server 3 None × Local EAP Authentication Enabled EAP Profile Name Mone × Server 3 None × Server 4 None × Server 5 None × Server 6 None × Server 7 None × None × None × Server 3 None × Local EAP Authentication Enabled Base Server 3 Server 4 Server 4 Server 5 Server 3 Server 6 Server 4 Server 7 None × Server 8 Server 9 Server 9 Server 9 Server 9 Server 9 <td< th=""><th>< Back Apply rs on this WLAN LDAP Servers Server None Server None None None</th><th></th></td<>	< Back Apply rs on this WLAN LDAP Servers Server None Server None None None	

5. Sélectionnez le serveur LDAP (qui a été précédemment configuré sur le WLC) dans la liste déroulante . Assurez-vous que le serveur LDAP est accessible depuis le WLC.Cliquez sur **Apply**.

a wic2006 - Microsoft Inter	rnet Explorer	- 6 🛛
File Edit View Pavorites T	Tools Help	
cisco	Saye Configuration Bing Lo MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	gout <u>R</u> efresh
WLANS WLANS WLANS Advanced	WLANS > Edit C Back Ceneral Security QoS Advanced Layer 2 Layer 3 AAA Servers Layer 2 Layer 3 AAA Servers Select AAA servers below to override use of default servers on this WLAN Radius Servers Ceneral Security Provided Server 1 None X Enabled Server 2 None X Enabled Server 3 None X None X Cocal EAP Authentication Enabled BAP Profile Name Eda X	Apply

6. Le nouveau LDAP WLAN a été configuré sur le WLC. Ce WLAN authentifie les clients avec l'authentification EAP locale (EAP-FAST dans ce cas) et interroge une base de données

principale LDAP pour la validation des informations d'identification du client.

wic2006 - Microsoft Int	ernet Explorer						
File Edit View Fevorites	Tools Help						
ababa					54	ge Configuration Fing Lo	gout <u>R</u> efresh
CISCO	MONITOR WLANS	CONTROLLER WIR	RELESS SECURITY	MANAGEMENT	COMMA	NDS HELP	
WLANs	WLANs					N	
- WLANS WLANS	Profile Name	Туре	WLAN SSID		Admin Status	Security Policies	
Advanced	Tawee	WLAN	TSWED		Enabled	[WFA2][Auth(002.1%)]	ا ا
	Ideouser	WLAN	Idap		Enabled	002.1X	
Done						💁 🗶 Internet	t

Configurer le serveur LDAP

Maintenant que Local EAP est configuré sur le WLC, l'étape suivante consiste à configurer le serveur LDAP qui sert de base de données back-end pour authentifier les clients sans fil lors de la validation de certificat réussie.

La première étape de la configuration du serveur LDAP consiste à créer une base de données utilisateur sur le serveur LDAP afin que le WLC puisse interroger cette base de données pour authentifier l'utilisateur.

Création d'utilisateurs sur le contrôleur de domaine

Dans cet exemple, une nouvelle unité d'organisation **Idapuser** est créée et l'utilisateur **user2** est créé sous cette unité d'organisation. En configurant cet utilisateur pour l'accès LDAP, le WLC peut interroger cette base de données LDAP pour l'authentification des utilisateurs.

Le domaine utilisé dans cet exemple est wireless.com.

Créer une base de données utilisateur sous une unité organisationnelle

Cette section explique comment créer une nouvelle unité d'organisation dans votre domaine et créer un nouvel utilisateur sur cette unité d'organisation.

 Dans le contrôleur de domaine, cliquez sur Démarrer > Programmes > Outils d'administration > Utilisateurs et ordinateurs Active Directory afin de lancer la console de gestion Utilisateurs et ordinateurs Active Directory. Cliquez avec le bouton droit sur votre nom de domaine (wireless.com, dans cet exemple), puis sélectionnez Nouveau > Unité d'organisation dans le menu contextuel afin de créer une nouvelle unité



3. Attribuez un nom à cette unité d'organisation et cliquez sur **OK**.

New Object	- Organiza	tional Unit		X
S	Create in:	Wireless.com/		
N <u>a</u> me:				
Idapuser				
			OK	Cancel

Maintenant que la nouvelle unité d'organisation **Idapuser** est créée sur le serveur LDAP, l'étape suivante consiste à créer l'utilisateur **user2** sous cette unité d'organisation. Pour ce faire, procédez comme suit :

 Cliquez avec le bouton droit sur la nouvelle unité d'organisation créée. Sélectionnez New > User dans les menus contextuels résultants afin de créer un nouvel utilisateur.



 Dans la page User setup, renseignez les champs obligatoires comme indiqué dans cet exemple. Cet exemple a user2 comme nom de connexion de l'utilisateur. Il s'agit du nom d'utilisateur qui sera vérifié dans la base de données LDAP pour l'authentification du client. Cet exemple utilise abcd comme prénom et nom. Cliquez sur Next (Suivant).

New Object - User	×
Create in: Wireless.com/Idapuser	
Eirst name: abcd Initials:	
Last name:	
Full name: abcd	
User2	
User logon riame (pre-Windows 2000):	
WIRELESS\ user2	
< <u>B</u> ack <u>N</u> ext > Cance	4

3. Entrez un mot de passe et confirmez-le. Sélectionnez l'option **Password never expires** et cliquez sur

Password:		•••••	-		
<u>C</u> onfirm passwe	ord:	•••••	•		
User <u>m</u> ust o	change pass	word at next lo	ogon		
U <u>s</u> er canno	ot change pa	ssword			
Password r	never expires				
Account is	disabled				

 Cliquez sur Finish (Terminer).Un nouvel utilisateur user2 est créé sous l'unité d'organisation Idapuser. Les informations d'identification utilisateur sont :nom d'utilisateur : user2password : Laptop123



Maintenant que l'utilisateur sous une unité d'organisation est créé, l'étape suivante consiste à configurer cet utilisateur pour l'accès LDAP.

Configurer l'utilisateur pour l'accès LDAP

Suivez les étapes de cette section afin de configurer un utilisateur pour l'accès LDAP.

Activer la fonctionnalité de liaison anonyme sur Windows 2003 Server

Pour que les applications tierces puissent accéder à Windows 2003 AD sur le serveur LDAP, la fonctionnalité de liaison anonyme doit être activée sur Windows 2003. Par défaut, les opérations LDAP anonymes ne sont pas autorisées sur les contrôleurs de domaine Windows 2003.

Effectuez ces étapes afin d'activer la fonctionnalité de liaison anonyme :

- 1. Lancez l'outil **ADSI Edit** à partir de l'emplacement Démarrer > Exécuter > Tapez : **ADSI Edit.msc**. Cet outil fait partie des outils de support de Windows 2003.
- Dans la fenêtre Édition ADSI, développez le domaine racine (Configuration [tsweblapt.Wireless.com]).Développez CN=Services > CN=Windows NT > CN=Directory Service. Cliquez avec le bouton droit sur le conteneur CN=Directory Service et sélectionnez properties dans le menu contextuel.



3. Dans la fenêtre CN=Directory Service Properties, cliquez sur l'attribut dsHeuristics sous le champ Attribute et choisissez Edit. Dans la fenêtre Éditeur d'attributs de chaîne de cet attribut, entrez la valeur 000002 et cliquez sur Appliquer et sur OK. La fonctionnalité de liaison anonyme est activée sur le serveur Windows 2003.Remarque : le dernier (septième) caractère est celui qui contrôle la façon dont vous pouvez établir une liaison avec le service LDAP. « 0 » ou aucun septième caractère signifie que les opérations LDAP anonymes sont désactivées. La définition du septième caractère sur "2" active la fonctionnalité de liaison anonyme.

EN=Directory Service Pr	operties		? X		
Attribute Editor Security			1	Class container	Distingu CN=Qu
 Show mandatory attributes Show only attributes Attributes: 	butes tes that have <u>v</u> alues				
Attribute	Syntax	Value	_		
directReports displayName displayNamePrintable distinguishedName dSASignature dSCorePropagationD dSHeuristics extensionName flags	String Attribu Attribute: dSH Value: 0000002 lear	te Editor euristics	Ć	ОК	Cancel
frsComputerReferenc fRSMemberReferenc fSMORoleOwner	Distinguished Distinguished Distinguished	<not set=""> <not set=""> <not set=""></not></not></not>	-		
	OK	Cancel	Apply		

Remarque : si cet attribut contient déjà une valeur, veillez à ne modifier que le septième caractère à partir de la gauche. C'est le seul caractère qui doit être modifié afin d'activer les liaisons anonymes. Par exemple, si la valeur actuelle est "0010000", vous devrez la remplacer par "0010002". Si la valeur actuelle est inférieure à sept caractères, vous devrez mettre des zéros aux endroits non utilisés : "001" deviendra "0010002".

Octroi de l'accès ANONYMOUS LOGON à l'utilisateur « user2 »

L'étape suivante consiste à accorder l'accès **ANONYMOUS LOGON** à l'utilisateur **user2**. Complétez ces étapes afin d'atteindre ceci :

- 1. Ouvrez Utilisateurs et ordinateurs Active Directory.
- 2. Assurez-vous que Afficher les fonctionnalités avancées est coché.
- 3. Accédez à l'utilisateur **user2** et cliquez dessus avec le bouton droit. Sélectionnez **Propriétés** dans le menu contextuel. Cet utilisateur est identifié par le prénom « abcd
 - ».

哇 🗠 🌄 useri		
🖃 🛄 Users		
	⊆opy Add to a group Name Mappings	
	Reset Password Move	
	Open Home Page	
🖻 🛣 Da	Send Mail	
	Find	
	All Tas <u>k</u> s	•
🖻 🗠 🚮 Er	View	F.
	New <u>W</u> indow from Here	
😐 🥳 II:	Cut	
	Delete	
🖭 🚮 kr	Refresh	
- 🕵 R/	Export List	
	Properties	
	Help	

4. Accédez à Sécurité dans la fenêtre Propriétés

Published Certificates		Dial-in Diae	t Securi
nvironment Session	Bemote control	Terminal Services	Profile COI
General Address	Account Profile	Telephones	Organizatio
— ·			
abcd			
<u>F</u> irst name:	abcd	Initials:	
Last name:			
Display name:	abcd		
Descriptions			
Description	1		
Offi <u>c</u> e:			
<u>T</u> elephone number:	[<u>O</u> ther
E- <u>m</u> ail:			
Web page:	-		Other
Ttop page.	1		
	OK	Cancal	Applu

- 5. Cliquez sur Add dans la fenêtre résultante.
- 6. Entrez ANONYMOUS LOGON dans la zone Entrez les noms des objets à sélectionner et accédez à la boîte de dialogue.

Select Users, Computers, or Groups	<u>?×</u>
Select this object type:	
Users, Groups, or Built-in security principals	<u>O</u> bject Types
From this location:	
Wireless.com	Locations
Enter the object names to select (examples):	
ANONYMOUS LOGON	<u>C</u> heck Names
<u>A</u> dvanced	OK Cancel

7. Dans la liste de contrôle d'accès, vous remarquerez que **ANONYMOUS LOGON** a accès à certains ensembles de propriétés de l'utilisateur. Click OK. L'accès OUVERTURE DE SESSION ANONYME est accordé à cet

utilisateur.		
abcd Properties		? ×
Environment Sessions Remote control T General Address Account Profile Published Certificates Member Of D	erminal Service: Telephones ial-in Objec	s Profile COM+ Organization ot Security
<u>G</u> roup or user names:		
Account Operators (WIRELESS Accou Administrators (WIRELESS Administrators	int Operators) ors)	
ANONYMOUS LOGON		
Cert Publishers (WIRELESS\Cert Publis	hers)	-
	A <u>d</u> d	<u>R</u> emove
Permissions for ANONYMOUS LOGON	Allow	Deny
Full Control Read Write Create All Child Objects Delete All Child Objects Allowed to Authenticate		
For special permissions or for advanced settin click Advanced.	ngs,	Advanced
ОК	Cancel	

Octroi d'une autorisation de contenu de liste sur l'unité organisationnelle

L'étape suivante consiste à accorder au moins l'autorisation List Contents à l'OUVERTURE DE SESSION ANONYME sur l'unité d'organisation où se trouve l'utilisateur. Dans cet exemple, « user2 » se trouve sur l'unité d'organisation « ldapuser ». Complétez ces étapes afin d'atteindre ceci :

 Dans Utilisateurs et ordinateurs Active Directory, cliquez avec le bouton droit sur l'unité d'organisation Idapuser et choisissez
 Propriétée



2. Cliquez sur **Security**, puis sur **Advanced**.

apuser Properties		?
General Managed By Object Security C	OM+ Group F	Policy
Group or user names:		
Account Operators (WIRELESS Account	nt Operators)	^
Administrators (WIRELESS \Administrato	rs)	
🚮 Authenticated Users		
🗾 👧 Domain Admins (WIRELESS\Domain Ad	dmins)	
Enterprise Admins (WIRELESS\Enterprise)	se Admins)	-1
	10 A	
	Add	<u>Remove</u>
Permissions for Account Operators	Allow	Deny
Full Control		
Read		
Write		
Create All Child Objects		
Delete All Child Objects		
Generate Resultant Set of Policy(Logging)		
For special permissions or for advanced setting click Advanced.	gs, 🧲	Advanced
ОК	Cancel	Apply

3. Cliquez sur Add. Dans la boîte de dialogue qui s'ouvre, entrez ANONYMOUS LOGON.

Advanced Security Settings for Idapuser	
Select User, Computer, or Group	<u>? ×</u>
Select this object type:	
User, Group, or Built-in security principal	Object Types
From this location:	
Wireless.com	Locations
Enter the object name to select (examples):	
ANONYMOUS LOGON	<u>C</u> heck Names
Advanced OK	Cancel

- 4. Acceptez le dialogue. Une nouvelle boîte de dialogue s'ouvre.
- 5. Dans la liste déroulante **Appliquer à**, sélectionnez **Cet objet uniquement** et activez la case à cocher Autoriser le contenu de la **liste**.

Permission Entry for Idapuser			<u> </u>
Object Properties			
Name: ANONYMOUS LOGON		<u>C</u> hange	
Apply onto: This object only			-
Permissions:	Allow	Deny	_
Full Control List Contents Bead All Properties Write All Properties Delete Delete Subtree Read Permissions Modify Permissions Modify Owner All Validated Writes All Extended Rights Create All Child Objects Delete Subtree Read Permissions to object	s and/or		
	ок	Cance	я

Utilisation du protocole LDP pour identifier les attributs utilisateur

Cet outil GUI est un client LDAP qui permet aux utilisateurs d'effectuer des opérations (telles que la connexion, la liaison, la recherche, la modification, l'ajout, la suppression) sur n'importe quel répertoire compatible LDAP, tel qu'Active Directory. Le protocole LDP permet d'afficher les objets stockés dans Active Directory, ainsi que leurs métadonnées, telles que les descripteurs de sécurité et les métadonnées de réplication.

L'outil LDP GUI est inclus lorsque vous installez les outils de support de Windows Server 2003 à partir du CD du produit. Cette section explique comment utiliser l'utilitaire LDP pour identifier les attributs spécifiques associés à l'utilisateur **user2**. Certains de ces attributs sont utilisés pour remplir les paramètres de configuration du serveur LDAP sur le WLC, tels que le type d'attribut d'utilisateur et le type d'objet d'utilisateur.

- 1. Sur le serveur Windows 2003 (même sur le même serveur LDAP), cliquez sur **Démarrer > Exécuter** et entrez **LDP** afin d'accéder au navigateur LDP.
- Dans la fenêtre principale de LDP, cliquez sur Connection > Connect et connectez-vous au serveur LDAP en entrant l'adresse IP du serveur LDAP.

i Ldp	_ 🗆 🗵
Connection Browse View Options Utilities	Help
Connect Bind Cbrl+B Disconnect Disconnect <td>*</td>	*
Save As	
Print Print Pregiew Pgint Setup	
Egt	
	X
Connect to specified server	

3. Une fois connecté au serveur LDAP, sélectionnez **View** dans le menu principal et cliquez sur **Tree**.

Yew Options U	tilities		Help
Tree Enterprise Confi ✓ Status Bar Set Font	Ctrl+T guration	<pre>1.2.840.113556.1.4.473; 1.2.840.113556.1.4.528; 1.2.840.113556.1.4.417; 1.2.840.113556.1.4.619; 1.2.840.113556.1.4.841; 1.2.840.113556.1.4.529; 1.2.840.113556.1.4.805; 1.2.840.113556.1.4.521; 1.2.840.113556.1.4.970; 1.2.840.113556.1.4.1338; 1.2.840.113556.1.4.474; 1.2.840.113556.1.4.1339; 1.2.840.113556.1.4.1340; 1.2.840.113556.1.4.1504; 1.2.840.113556.1.4.1852; 1.2.840.113556.1.4.802; 1.2.840.113556.1.4.1907; 1.2.840.113556.1.4.1948; 2.> supportedLDAPVersion: 3; 2; 12> supportedLDAPVersion: 3; 2; 12> supportedLDAPVersion: 3; 2; 12> supportedLDAPVersion: 3; 2; 12> supportedLDAPVersion: MaxConnections; MaxDatagramRecv; MaxReceiveBuffer; InitRecvTimeout; MaxConnections; MaxConnIdleTime; MaxPageSize; MaxOueryDuration; MaxTempTableSize; MaxResultSetSize; MaxNotificationPerConn; MaxValRange; 1> highestCommittedUSN: 16926; 4> supportedSASLMechanisms: GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5; 1> dnsHostName: tsweb-lapt.Wireless.com; 1> ldapServiceName: Wireless.com; 1> ldapServiceName: Wireless.com; 1> serverName: CN=TSWEB-LAPT,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Config; DC=Wireless,DC=com; 3> supportedCapabilities: 1.2.840.113556.1.4.800; 1.2.840.113556.1.4 1.2.840.113556.1.4.1791; 1> isSynchronized: TRUE; 1> isGlobalCatalogReady: TRUE; 1> domainFunctionality: 0 = [DS_BEHAVIOR_WIN2000]; 1> forestFunctionality: 0 = [DS_BEHAVIOR_WIN2000]; 1> domainControllerFunctionality: 2 = [DS_BEHAVIOR_WIN2003];</pre>	uration 4.1670;
	yew ⊊poors <u>Iree</u> Enterprise Conf ✓ Status Bar Set Font	Yee Chri+T Enterprise Configuration ✓ Status Bar Set Font	Year Content Inconstruct Content Enterprise Confloaration 1.2.840.113556.1.4.473; 1.2.840.113556.1.4.528; 1.2.840.113556.1.4.529; 1.2.840.113556.1.4.521; 1.2.840.113556.1.4.521; 1.2.840.113556.1.4.521; 1.2.840.113556.1.4.521; 1.2.840.113556.1.4.521; 1.2.840.113556.1.4.521; 1.2.840.113556.1.4.521; 1.2.840.113556.1.4.1521; 1.2.840.113556.1.4.1521; 1.2.840.113556.1.4.1521; 1.2.840.113556.1.4.1521; 1.2.840.113556.1.4.1521; 1.2.840.113556.1.4.1521; 1.2.840.113556.1.4.1521; 1.2.840.113556.1.4.1521; 1.2.840.113556.1.4.1523; 1.2.840.113556.1.4.1525; 1.2.840.1135555.1.4.1525; 1.2.840.1135555.1.4.1525; 1.2.840.1135555.1.4.1525

4. Dans la fenêtre Arborescence résultante, entrez le nom de domaine de base de l'utilisateur. Dans cet exemple, user2 se trouve sous l'unité d'organisation « ldapuser » sous le domaine Wireless.com. Par conséquent, le nom de domaine de base de l'utilisateur user2 est OU=ldapuser, dc=wireless, dc=com. Click OK.

Midap://tsweb-lapt.Wireless.com/DE=Wireless,DE=com		- 🗆 🗵
Connection Browse View Options Utilities		Help
Tree View BaseDN: DU-Idaguser.do-wireless.do-com Cancel	X 3556.1.4.473; 1.2.840.113556.1.4.528; 1.2.840.113556.1.4.417; 3556.1.4.619; 1.2.840.113556.1.4.841; 1.2.840.113556.1.4.529; 3556.1.4.805; 1.2.840.113556.1.4.521; 1.2.840.113556.1.4.970; 3556.1.4.1338; 1.2.840.113556.1.4.474; 1.2.840.113556.1.4.1339; 3556.1.4.1340; 1.2.840.113556.1.4.1413; 2.16.840.1.113730.3.4.9; 1.113730.3.4.10; 1.2.840.113556.1.4.1504; 1.2.840.113556.1.4.1852; 3556.1.4.802; 1.2.840.113556.1.4.1907; 1.2.840.113556.1.4.1852; 3556.1.4.802; 1.2.840.113556.1.4.1907; 1.2.840.113556.1.4.1948; 2> supportedLDAPVersion: 3; 2; 2> supportedLDAPVersion: 3; 2; 1> supportedLDAPVersion; 3; 2; 1> supportedLDAPVersion; 3; 2; 1> supportedLDAPVersion; 3; 2; 1> supportedLDAPVersion; 3; 2; 1> supportedLSASLMechanisms: GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5; 1> dnsHostName: tsweb-lapt.Wireless.com; 1> ldapServiceName: Wireless.com; 1> ldapServiceName: Wireless.com; 1> ldapServiceName: Wireless.com; 2: supportedCapabilities: 1.2.840.113556.1.4.800; 1.2.840.113556.1.4. 1.2.840.113556.1.4.1791; 1> isSynchronized: TRUE; 1> isSynchronized: TRUE; 1> isSynchronized: TRUE; 1> domainControllerFunctionality: 0 = [DS_BEHAVIOR_WIN2000]; 1> domainControllerFunctionality: 2 = [DS_BEHAVIOR_WIN2003];	ration .1670;
Ready		1.

5. Le côté gauche du navigateur LDP affiche l'arborescence complète qui apparaît sous le nom de domaine de base spécifié (OU=Idapuser, dc=wireless, dc=com). Développez l'arborescence pour localiser l'utilisateur user2. Cet utilisateur peut être identifié par la valeur CN qui représente le prénom de l'utilisateur. Dans cet exemple, c'est CN=abcd. Double-cliquez sur CN=abcd. Dans le volet de droite du navigateur LDP, LDP affiche tous les attributs associés à user2. Cet exemple explique cette étape :



Dans cet exemple, observez les champs entourés à droite.

- 6. Comme mentionné dans la section <u>Configurer le WLC avec les détails du serveur LDAP</u> de ce document, dans le champ Attribut d'utilisateur, entrez le nom de l'attribut dans l'enregistrement d'utilisateur qui contient le nom d'utilisateur.Àpartir de cette sortie LDP, vous pouvez voir que sAMAccountName est un attribut qui contient le nom d'utilisateur « user2 ». Par conséquent, entrez l'attribut sAMAccountName qui correspond au champ User Attribute sur le WLC.
- 7. Dans le champ User Object Type, entrez la valeur de l'attribut LDAP objectType qui identifie l'enregistrement comme utilisateur. Souvent, les enregistrements utilisateur ont plusieurs valeurs pour l'attribut objectType, certains étant propres à l'utilisateur et certains étant partagés avec d'autres types d'objet.Dans la sortie LDP, CN=Person est une valeur qui identifie l'enregistrement en tant qu'utilisateur. Par conséquent, spécifiez Person comme l'attribut User Object Type sur le WLC.

Configuration du client sans fil

La dernière étape consiste à configurer le client sans fil pour l'authentification EAP-FAST avec des certificats client et serveur. Complétez ces étapes afin d'atteindre ceci :

 Lancez l'utilitaire Cisco Aironet Desktop Utility (ADU). Dans la fenêtre principale de l'ADU, cliquez sur Profile Management > New afin de créer un nouveau profil de client sans fil.

🛜 Cisco Aironet Desktop U	Itility - Current Profile: sdreteretet	? 🛛
Action Options Help		
Current Status Profile Manage	ment Diagnostics	
Sdreteretet		New
		Modify
		Remove
		Activate
⊂ Details		
Network Type:	Infrastructure	Import
Security Mode:	Disabled	
Network Name 1 (SSID1):	teert	Export
Network Name 2 (SSID2):	<empty></empty>	Scan
Network Name 3 (SSID3):	<empty></empty>	
Auto Select Profiles		Order Profiles

2. Spécifiez un nom de profil et attribuez un nom SSID à ce profil. Ce nom SSID doit être le même que celui configuré sur le WLC. Dans cet exemple, le nom SSID est

Profile Settings Profile Na Client Na	me: Idapuser me: CLIENT1	
Network Names SSI SSI	D1 Idap D2:	

- 3. Cliquez sur l'onglet **Security** et choisissez **802.1x/EAP** comme niveau de sécurité de la couche 2. Choisissez **EAP-FAST** comme méthode EAP et cliquez sur **Configure**.
- 4. Dans la page de configuration EAP-FAST, choisissez **TLS Client Certificate** dans la liste déroulante EAP-FAST Authentication Method et cliquez sur **Configure**.

Configure EAP-FAST	? 🔀
EAP-FAST Authentication Method	
MSCHAPv2 User Name and Password	Configure
GTC Token/Password	
TLS Client Certificate	
Select One or More PAC Authorities	1
	Manage
Use Any PAC Belonging to the Same Group	
Allow Automatic PAC Provisioning	
Use Machine Information for Domain Logon	
No Network Connection Unless User Is Logged In	
	IK Cancel

5. Dans la fenêtre de configuration du certificat du client TLS :Activez la case à cocher Valider l'identité du serveur et sélectionnez le certificat d'autorité de certification installé sur le client (expliqué dans la section <u>Générer le certificat d'autorité de certification racine pour le client</u> de ce document) comme autorité de certification racine de confiance.Sélectionnez le certificat de périphérique installé sur le client (expliqué dans la section <u>Générer un certificat</u> de périphérique pour le client de ce document) en tant que certificat client.Click OK.Cet exemple explique cette étape

✓ Validate Server Identity	
Trusted Root Certification Authorities	
wireless	~
Select a Certificate	
1234 [Issued by: wireless 1/26/2008]	~
Server/Domain Name	
Wireless.com	
Login Name	
user2	

Le profil client sans fil est créé.

Vérifier

Suivez ces étapes afin de vérifier si votre configuration fonctionne correctement.

1. Activez le SSID **Idap** sur l'ADU.

 Cliquez sur Yes ou OK dans les fenêtres suivantes. Vous devriez être en mesure de voir toutes les étapes de l'authentification du client ainsi que l'association pour réussir sur l'ADU.

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration. Utilisez le mode CLI du WLC.

 Afin de vérifier si le WLC est capable de communiquer avec le serveur LDAP et de localiser l'utilisateur, spécifiez la commande debug aaa Idap enable à partir de l'ILC du WLC. Cet exemple explique un processus LDAP de communication réussi :Remarque : certains résultats de cette section ont été déplacés vers les secondes lignes pour des raisons d'espace.(Contrôleur Cisco) >debug aaa Idap enable

Sun Jan 27 09:23:46 2008: AuthenticationRequest: 0xba96514 Sun Jan 27 09:23:46 2008: Callback.....0x8 344900 Sun Jan 27 09:23:46 2008: protocolType.....0x0 0100002 Sun Jan 27 09:23:46 2008: proxyState.....00: 40:96:AC:E6:57-00:00 Sun Jan 27 09:23:46 2008: Packet contains 2 AVPs (not shown) Sun Jan 27 09:23:46 2008: ldapTask [1] received msg 'REQUEST' (2) in state 'IDLE' (1) Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to INIT Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_init (rc = 0 - Success) Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_bind (rc = 0 - Success) Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to CONNECTED Sun Jan 27 09:23:46 2008: LDAP server 1 now active Sun Jan 27 09:23:46 2008: LDAP_CLIENT: UID Search (base=OU=ldapuser, DC=wireless, DC=com, pattern=(&(objectclass=Person)(sAMAccountName=user2))) Sun Jan 27 09:23:46 2008: LDAP_CLIENT: Returned msg type 0x64 Sun Jan 27 09:23:46 2008: ldapAuthRequest [1] called lcapi_query base="OU=ldapus er,DC=wireless,DC=com" type="Person" attr="sAMAccountName" user="user2" (rc = 0 - Success) Sun Jan 27 09:23:46 2008: LDAP ATTR> dn = CN=abcd,OU=ldapuser,DC=Wireless,DC=com (size 38) Sun Jan 27 09:23:46 2008: Handling LDAP response Success

D'après les informations mises en surbrillance dans cette sortie de débogage, il est clair que le serveur LDAP est interrogé par le WLC avec les attributs d'utilisateur spécifiés sur le WLC et le processus LDAP est réussi.

Afin de vérifier si l'authentification EAP locale est réussie, spécifiez la commande debug aaa local-auth eap method events enable à partir de l'interface de ligne de commande WLC. Voici un exemple :(Contrôleur Cisco) >debug aaa local-auth eap method events enable Sun Jan 27 09:38:28 2008: eap_fast.c-EVENT: New context

(EAP handle = 0x1B000009) Sun Jan 27 09:38:28 2008: eap_fast.c-EVENT: Allocated new EAP-FAST context (handle = 0x22000009) Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Process Response (EAP handle = 0x1B000009) Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Received Identity Sun Jan 27 09:38:28 2008: eap_fast_tlv.c-AUTH-EVENT: Adding PAC A-ID TLV (436973636f000000000000000000000) Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Sending Start

Sun Jan 27 09:38:29 2008: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Process Response (EAP handle = 0x1B000009)Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Received TLS record type: Handshake in state: Start Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Local certificate found Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Hello handshake Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: TLS_DHE_RSA_AES_128_CBC_SHA proposed... Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Proposed ciphersuite(s): Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_RSA_WITH_AES_128_CBC_SHA Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_RSA_WITH_RC4_128_SHA Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Selected ciphersuite: Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Building Provisioning Server Hello Sun Jan 27 09:38:29 2008: eap_fast_crypto.c-EVENT: Starting Diffie Hellman phase 1 ... Sun Jan 27 09:38:30 2008: eap_fast_crypto.c-EVENT: Diffie Hellman phase 1 complete Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: DH signature length = 128 Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: Sending Provisioning Serving Hello Sun Jan 27 09:38:30 2008: eap_fast.c-EVENT: Tx packet fragmentation required Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet(): EAP Fast NoData (0x2b) Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet(): EAP Fast NoData (0x2b) Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet(): EAP Fast NoData (0x2b) Sun Jan 27 09:38:32 2008: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Reassembling TLS record Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Sending EAP-FAST Ack Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Received TLS record type: Handshake in state: Sent provisioning Server Hello

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:

Reading Client Certificate handshake Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 1 to chain Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 2 to chain Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Successfully validated received certificate Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Rx'd I-ID: "EAP-FAST I-ID" from Peer Cert Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Key Exchange handshake Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT: Starting Diffie Hellman phase 2 ... Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT: Diffie Hellman phase 2 complete. Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Certificate Verify handshake Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT: Sign certificate verify succeeded (compare) • La commande debug aaa local-auth db enable est également très utile. Voici un exemple :(Contrôleur Cisco) >debug aaa local-auth db enable Sun Jan 27 09:35:32 2008: LOCAL_AUTH: EAP: Received an auth request Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Creating new context Sun Jan 27 09:35:32 2008: LOCAL AUTH: Local auth profile name for context 'ldapuser' Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Created new context eap session handle fb000007 Sun Jan 27 09:35:32 2008: LOCAL_AUTH: (EAP:8) Sending the Rxd EAP packet (id 2) to EAP subsys Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Found matching context for id - 8 Sun Jan 27 09:35:32 2008: LOCAL_AUTH: (EAP) Sending user credential request username 'user2' to LDAP Sun Jan 27 09:35:32 2008: LOCAL AUTH: Found context matching MAC address - 8

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Sending the Rxd EAP packet (id 12) to EAP subsys
Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8
Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) ---> [KEY AVAIL] send_len 64, recv_len 0
Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) received keys waiting for success
Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8
Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Received success event
Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Received success event
Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Received success event

 Afin d'afficher les certificats installés dans le WLC à utiliser pour l'authentification locale, émettez la commande show local-auth certificates à partir de l'ILC du WLC. Voici un exemple :(Contrôleur Cisco) >show local-auth certificates

Certificates available for Local EAP authentication:

Certificate issuer vendor

CA certificate:

Subject: DC=com, DC=Wireless, CN=wireless

Issuer: DC=com, DC=Wireless, CN=wireless

Valid: 2008 Jan 23rd, 15:50:27 GMT to 2013 Jan 23rd, 15:50:27 GMT

Device certificate:

Subject: O=cisco, CN=ciscowlc123

Issuer: DC=com, DC=Wireless, CN=wireless

Valid: 2008 Jan 24th, 12:18:31 GMT to 2010 Jan 23rd, 12:18:31 GMT

Certificate issuer cisco

CA certificate:

Subject: O=Cisco Systems, CN=Cisco Manufacturing CA

Issuer: O=Cisco Systems, CN=Cisco Root CA 2048

Valid: 2005 Jun 10th, 22:16:01 GMT to 2029 May 14th, 20:25:42 GMT

Device certificate:

Not installed.

 Afin d'afficher la configuration d'authentification locale sur le WLC à partir du mode CLI, émettez la commande show local-auth config. Voici un exemple :(Contrôleur Cisco) >show local-auth config

User credentials database search order:

Timer:	
Active timeout	300
Configured EAP profiles:	
Name	ldapuser
Certificate issuer	vendor
Peer verification options:	
Check against CA certificates	Enabled
Verify certificate CN identity	Disabled
Check certificate date validity	Disabled
EAP-FAST configuration:	
Local certificate required	Yes
Client certificate required	Yes
Enabled methods	fast
Configured on WLANs	2
EAP Method configuration:	
EAP-FAST:	
More or (q)uit	
Server key	<hidden></hidden>
TTL for the PAC	10
Anonymous provision allowed	No
Authority Information	Cisco A-ID

Dépannage

Vous pouvez utiliser ces commandes pour dépanner votre configuration :

- debug aaa local-auth eap method events enable
- debug aaa all enable
- debug dot1x packet enable

Informations connexes

- Exemple de configuration d'authentification EAP-FAST avec des contrôleurs de réseau local sans fil et un serveur RADIUS externe
- PEAP sous des réseaux sans fil unifiés avec Microsoft Internet Authentication Service (IAS)
- Exemple de configuration d'une affectation de VLAN dynamique avec des contrôleurs de réseau local sans fil en fonction du mappage du groupe ACS au groupe Active Directory
- <u>Guide de configuration du contrôleur LAN sans fil Cisco Configuration des solutions de</u> <u>sécurité</u>
- <u>Guide de configuration du contrôleur LAN sans fil Cisco Gestion des logiciels et des</u> <u>configurations du contrôleur</u>
- Exemple de configuration de l'authentification EAP avec des contrôleurs de réseau local sans fil (WLC)
- Conception et fonctionnalités du contrôleur de réseau local sans fil Forum Aux Questions
- <u>Cisco Secure Services Client avec authentification EAP-FAST</u>
- <u>Contrôleur de réseau local sans fil (WLC) Forum Aux Questions</u>
- Contrôleurs Erreur du contrôleur LAN sans fil (WLC) et messages système FAQ
- Assistance et documentation techniques Cisco Systems

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.