# Lokale EAP-Authentifizierung auf dem Wireless LAN-Controller mit EAP-FAST und LDAP-Server - Konfigurationsbeispiel

# Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Hintergrundinformationen Konfigurieren Netzwerkdiagramm Konfigurationen Konfigurieren von EAP-FAST als lokale EAP-Authentifizierungsmethode auf dem WLC Generieren eines Gerätezertifikats für den WLC Herunterladen des Gerätezertifikats auf den WLC Installieren des Stammzertifikats von PKI im WLC Generieren eines Gerätezertifikats für den Client Generieren des Stammzertifizierungsstellenzertifikats für den Client Konfigurieren des lokalen EAP auf dem WLC LDAP-Server konfigurieren Erstellen von Benutzern auf dem Domänencontroller Konfigurieren des Benutzers für den LDAP-Zugriff Verwenden von LDP zum Identifizieren der Benutzerattribute Wireless-Client konfigurieren Überprüfung Fehlerbehebung Zugehörige Informationen

# **Einleitung**

In diesem Dokument wird erläutert, wie die lokale EAP-Authentifizierung (Extensible Authentication Protocol, EAP) - Flexible Authentication via Secure Tunneling (FAST) auf einem Wireless LAN Controller (WLC) konfiguriert wird. In diesem Dokument wird auch erläutert, wie der LDAP-Server (Lightweight Directory Access Protocol) als Backend-Datenbank für den lokalen EAP konfiguriert wird, um Benutzeranmeldeinformationen abzurufen und den Benutzer zu authentifizieren.

## Voraussetzungen

## **Anforderungen**

Es gibt keine spezifischen Anforderungen für dieses Dokument.

## Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco WLC der Serie 4400 mit Firmware 4.2
- Cisco Aironet Lightweight Access Point (LAP) der Serie 1232AG
- Microsoft Windows 2003 Server, der als Domänencontroller, LDAP-Server sowie als Zertifizierungsstellenserver konfiguriert ist.
- Cisco Aironet 802.11 a/b/g Client-Adapter für Firmware-Version 4.2
- Cisco Aironet Desktop Utility (ADU) mit Firmware-Version 4.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

## **Konventionen**

Weitere Informationen zu Dokumentkonventionen finden Sie unter <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps von Cisco zu Konventionen).

## **Hintergrundinformationen**

Die lokale EAP-Authentifizierung auf Wireless LAN-Controllern wurde mit Wireless LAN Controller Version 4.1.171.0 eingeführt.

Local EAP ist eine Authentifizierungsmethode, die es Benutzern und Wireless-Clients ermöglicht, sich lokal auf dem Controller zu authentifizieren. Es wurde für den Einsatz in Außenstellen entwickelt, die die Verbindung zu Wireless-Clients aufrechterhalten möchten, wenn das Backend-System ausfällt oder der externe Authentifizierungsserver ausfällt. Wenn Sie den lokalen EAP aktivieren, fungiert der Controller als Authentifizierungsserver und lokale Benutzerdatenbank, sodass die Abhängigkeit von einem externen Authentifizierungsserver entfällt. Lokales EAP ruft Benutzeranmeldeinformationen aus der lokalen Benutzerdatenbank oder der LDAP-Backend-Datenbank ab, um Benutzer zu authentifizieren. Lokales EAP unterstützt die LEAP-, EAP-FAST-, EAP-TLS-, P EAPv0/MSCHAPv2- und PEAPv1/GTC-Authentifizierung zwischen dem Controller und Wireless-Clients.

Der lokale EAP kann einen LDAP-Server als Backend-Datenbank verwenden, um Benutzeranmeldeinformationen abzurufen.

Eine LDAP-Backend-Datenbank ermöglicht es dem Controller, die Anmeldeinformationen (Benutzername und Kennwort) eines bestimmten Benutzers von einem LDAP-Server abzufragen. Diese Anmeldeinformationen werden dann zur Authentifizierung des Benutzers verwendet. Die LDAP-Backend-Datenbank unterstützt die folgenden lokalen EAP-Methoden:

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

LEAP, EAP-FAST/MSCHAPv2 und PEAPv0/MSCHAPv2 werden ebenfalls unterstützt, **allerdings nur, wenn der LDAP-Server so konfiguriert ist, dass er ein unverschlüsseltes Kennwort zurückgibt**. Microsoft Active Directory wird z. B. nicht unterstützt, da es kein Klartextkennwort zurückgibt. Wenn der LDAP-Server nicht für die Rückgabe eines unverschlüsselten Kennworts konfiguriert werden kann, werden LEAP, EAP-FAST/MSCHAPv2 und PEAPv0/MSCHAPv2 nicht unterstützt.

**Hinweis:** Wenn auf dem Controller RADIUS-Server konfiguriert sind, versucht der Controller zunächst, die Wireless-Clients mithilfe der RADIUS-Server zu authentifizieren. Lokaler EAP wird nur dann versucht, wenn keine RADIUS-Server gefunden werden, entweder weil die RADIUS-Server abgelaufen sind oder weil keine RADIUS-Server konfiguriert wurden. Wenn vier RADIUS-Server konfiguriert sind, versucht der Controller, den Client mithilfe des ersten RADIUS-Servers, des zweiten RADIUS-Servers und des lokalen EAP zu authentifizieren. Wenn der Client eine manuelle Neuauthentifizierung versucht, versucht der Controller zuerst den dritten RADIUS-Server, dann den vierten RADIUS-Server und dann den lokalen EAP.

In diesem Beispiel wird EAP-FAST als Local EAP-Methode auf dem WLC verwendet, der wiederum so konfiguriert ist, dass er die LDAP-Backend-Datenbank nach Benutzeranmeldeinformationen eines Wireless-Clients abfragt.

## **Konfigurieren**

In diesem Dokument wird EAP-FAST mit Zertifikaten sowohl auf Client- als auch auf Serverseite verwendet. Dazu verwendet das Setup den **Microsoft Certificate Authority (CA)**-Server, um die Client- und Serverzertifikate zu generieren.

Die Benutzeranmeldeinformationen werden im LDAP-Server gespeichert, sodass der Controller bei erfolgreicher Zertifikatsvalidierung den LDAP-Server abfragt, um die Benutzeranmeldeinformationen abzurufen, und den Wireless-Client authentifiziert.

In diesem Dokument wird davon ausgegangen, dass die folgenden Konfigurationen bereits vorhanden sind:

- Beim WLC ist ein LAP registriert. Weitere Informationen zum Registrierungsprozess finden Sie unter Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC).
- Ein DHCP-Server ist so konfiguriert, dass er den Wireless-Clients eine IP-Adresse zuweist.
- Der Microsoft Windows 2003 Server ist sowohl als Domänencontroller als auch als CA-Server konfiguriert. In diesem Beispiel wird wireless.com als Domäne verwendet.Weitere Informationen zum Konfigurieren eines Windows 2003-Servers als Domänencontroller finden Sie unter Konfigurieren von Windows 2003 als Domänencontroller.Weitere Informationen zur Konfiguration des Microsoft Windows 2003-Servers als CA-Server (Certificate Authority) finden Sie unter Installieren und Konfigurieren des Microsoft Windows 2003-Servers als CA-Server der Enterprise-Klasse.

## **Netzwerkdiagramm**

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



# Konfigurationen

Gehen Sie wie folgt vor, um diese Konfiguration zu implementieren:

- Konfigurieren von EAP-FAST als lokale EAP-Authentifizierungsmethode auf dem WLC
- LDAP-Server konfigurieren
- <u>Wireless-Client konfigurieren</u>

## Konfigurieren von EAP-FAST als lokale EAP-Authentifizierungsmethode auf dem WLC

Wie bereits erwähnt, verwendet dieses Dokument EAP-FAST mit Zertifikaten sowohl auf Clientals auch auf Serverseite als lokale EAP-Authentifizierungsmethode. Der erste Schritt besteht darin, die folgenden Zertifikate auf den Server (in diesem Fall WLC) und den Client herunterzuladen und zu installieren.

Der WLC und der Client benötigen jeweils diese Zertifikate, um vom CA-Server heruntergeladen zu werden:

- Gerätezertifikat (eines für den WLC und eines für den Client)
- Root-Zertifikat der Public Key Infrastructure (PKI) für den WLC und CA-Zertifikat für den Client

#### Generieren eines Gerätezertifikats für den WLC

Führen Sie diese Schritte aus, um ein Gerätezertifikat für den WLC vom CA-Server zu generieren. Dieses Gerätezertifikat wird vom WLC für die Authentifizierung beim Client verwendet.

 Gehen Sie zu http://<IP-Adresse des CA-Servers>/certsrv von Ihrem PC, der eine Netzwerkverbindung zum CA-Server hat. Melden Sie sich als Administrator des Zertifizierungsstellenservers

an.	
🕽 about:blank - Microsoft Internet Explorer	
File Edt Ver Pillortes Hor dep	
Address and Mtp://10.77.244.198/certsrv	💌 🛃 Ga
Connect to 10, 77, 244, 198 Connecting to 80.77, 244, 198 User name:  administrator Password: Remember my password OK	cel
Opening page http://10.72.244.199/partery	a linternet

2. Wählen Sie Zertifikat anfordern aus.

The Set Year Prevention Took ( Help ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (	
	4
Microsoft Certificate Services - wrease      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 you     identify to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you red     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), were 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     View the status of a pending certificate request     Download a CA certificate, certificate chain, or CRL	👻 🔁 Go
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 you identify to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you red 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), o 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	Heme
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 you 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 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	
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or 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 View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	our aquest,
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	, or to
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	

3. Klicken Sie auf der Seite Zertifikat anfordern auf Erweiterte

Zertifikatsanforderung.	
Microsoft Certificate Services - Microsoft Internet Explorer	N 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Pån Edit View Pavoritis Tools Help	
Address an http://10.77.244.198/certsrv/certraus.asp	💌 🛃 Go
Microsoft Certificate Services wireless	Home
Request a Certificate	
Select the certificate type:	
User Certificate	
Or submit an advanced certificate request.	
http://10.77.244.198/ceetsrv/ceetrgad.asp	Internet

 Klicken Sie auf der Seite "Erweiterte Zertifikatanforderung" auf Erstellen, und senden Sie eine Anforderung an diese Zertifizierungsstelle. Dadurch gelangen Sie zum Anforderungsformular f
ür Advanced-Zertifikate.

Microsoft Certificate Services - Microsoft Internet Explorer		
Ne Edit View Pavorites Took Help		
ddiress 🕘 http://10.77.244.190/certsrv/certroad.asp		👻 🔁 Go
Afficrosoft Certificate Services wireless		Home
Advanced Certificate Request		
The policy of the CA determines the types of certificates you can request. Click or	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 #101 PKCS #7 file.	file, or submit a renewal request by using a base-64-er	coded
Request a certificate for a smart card on behalf of another user by using the sm Note: You must have an enrollment agent certificate to submit a request on behalf of another	nart card certificate enrollment station, user.	
		1
	Internet	

- 5. Wählen Sie im Anforderungsformular für erweiterte Zertifikate als Zertifikatvorlage den Webserver aus. Geben Sie dann einen Namen für dieses Gerätezertifikat an. In diesem Beispiel wird der Zertifikatsname ciscowlc123 verwendet. Tragen Sie die sonstigen für Sie relevanten Informationen ein.
- 6. Wählen Sie im Abschnitt Schlüsseloptionen die Option Schlüssel als exportierbar markieren. Manchmal ist diese Option ausgegraut und kann nicht aktiviert oder deaktiviert werden, wenn Sie eine Webservervorlage auswählen. Klicken Sie in diesem Fall im Browser-Menü auf Zurück, um eine Seite zurückzukehren und zu dieser Seite zurückzukehren. Diesmal sollte die Option Schlüssel als exportierbar markieren verfügbar

sein.	
Microsoft Certificate Services - Microsoft Internet Explorer	
Me Edt View Pavorites Tools Help	
G tak · O	
Address Al http://10.77.244.198/cartery/centrone.am	v 🖾 😡
Microsoft Certificate Services - ministrat	Home
Advanced Certificate Request	
Cartificate Template:	
Cerimitate rempatei	
AABD Calvel.	
Identifying Information For Offline Template:	
Name: ciscowic123	
6-Mail	
Company: [cisco	
Department:	
City:	
State	
Country/Region:	
Key Onderse	
CSP Mission RVA SCharged Contempting RVA Set	
Key Litzer (* Exchange	
Key Size 1024 Marc 384 (compositive days 512 1004 2049 4099 9192 19044)	
Mac(1004     Mac(1004	
Southmatic key concerner name Coster specified key concerner name	
Export keys to file	
Enable strong private key protection	
Store certificate in the local computer certificate store	
Done	Dinternet

7. Konfigurieren Sie alle anderen erforderlichen Felder, und klicken Sie auf **Senden**.

🔿 Microsoft Certificate Services - Microsoft Internet Explorer	E 6 🛛
Fde Edit View Favorites Tools Help	14
🔇 tad. • 🕥 - 🖻 🖻 🐔 🔎 Search 🦅 Pavortes 🤣 🍙 - 😓 🖼 🦓	
Address at http://10.77.244.198/certary.certrona.asp	💌 🔁 Go
	^
CSP: Microsoft RSA SChannel Cryptographic Provider 🛩	
Key Usager. (Exchange	
Key Size: 1024 Min: 084 (common key size: 512 3024 2049 4085 5182 30364 )	
Automatic 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 instad 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: OCMC @PKCS10	
Hash Algorithm: SHA-1 M	
Only used to sign request.	
Save request to a file	
Attributes:	
Friendly Name:	
Submit >	
	*
🕘	lemet

8. Klicken Sie im nächsten Fenster auf **Ja**, um den Zertifikatanforderungsprozess zu ermöglichen.

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

 Das Fenster Certificate Issued (Von Zertifikat ausgestellt) wird angezeigt, das auf einen erfolgreichen Zertifikatanforderungsprozess hinweist. Der nächste Schritt besteht darin, das ausgestellte Zertifikat im Zertifikatspeicher dieses PCs zu installieren. Klicken Sie auf Dieses Zertifikat installieren.

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edt Wew Pavorties Tools Help	
Addinos 🕘 http://10.77.244.198/certsrv/certfrish.asp	🗹 🔁 Go
Microsoft Certificate Services - wireless	Home
Certificate Issued	
The certificate you requested was issued to you.	
Install this certificate	
Ø)	Internet

10. Das neue Zertifikat wird erfolgreich auf dem PC installiert, von dem aus die Anforderung an den Zertifizierungsstellenserver generiert

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	20
iddrece 🕘 Mtgr://10.77.244.198/certsrv/certrepn.asp	💌 🛃 Go
Microsoff Certificate Services wireless	Home
Certificate Installed	
Your new certificate has been successfully installed.	
Done	Internet
)or nächste Schritt hesteht darin, dieses Zertifikat aus dem Zerti	ifikatespaisher als Datai auf

11. Der nächste Schritt besteht darin, dieses Zertifikat aus dem Zertifikatsspeicher als Datei auf die Festplatte zu exportieren. Diese Zertifikatsdatei wird später verwendet, um das Zertifikat auf den WLC herunterzuladen.Um das Zertifikat aus dem Zertifikatspeicher zu exportieren, öffnen Sie den Internet Explorer-Browser, und klicken Sie dann auf Extras > Internetoptionen.

	<u> </u>
Pde Ede View Pavores Tools Pilip	12
Tele     Tele     Tele     Tele       Address     about blank     Marage Address       Synchronize     Windows Update       Windows Update     Windows Oracle       Subcord     Sinterree Coplarios	
	X

12. Klicken Sie auf **Inhalt > Zertifikate**, um zum Zertifikatspeicher zu wechseln, in dem die Zertifikate standardmäßig installiert

sind.
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
OK Cancel Apply

 Die Gerätezertifikate werden in der Regel in der Liste Persönliche Zertifikate installiert. Hier sollte das neu installierte Zertifikat angezeigt werden. Wählen Sie das Zertifikat aus, und klicken Sie auf Exportieren.

Certificates			? 🔀
Intended purpose:	<all></all>		~
Personal Other Peopl	e Intermediate Certification	Authorities Trusted Roo	t Certification
Issued To	Issued By	Expiratio Friendi	y Name
ciscowic123	wireless	1/25/2010 <none:< td=""><td>&gt;</td></none:<>	>
Import Exp	Remove		Advanced
- Certificate intended pu	rposes		
Server Authentication			
Server Addientication			Linu
			VIEW

14. Klicken Sie in den folgenden Fenstern auf Weiter. Wählen Sie im Fenster des Zertifikats-Export-Assistenten die Option Ja, privaten Schlüssel exportieren aus. Klicken Sie auf Next (Weiter).

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

 Wählen Sie als Exportdateiformat .PFX aus, und wählen Sie die Option Starken Schutz aktivieren. Klicken Sie auf Next (Weiter).

<ul> <li>DER encoded binary X.509 (.CER)</li> <li>Base-64 encoded X.509 (.CER)</li> <li>Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)</li> <li>Include all certificates in the certification path if possible</li> </ul>	Salact	the format you want to use
<ul> <li>Base-64 encoded X.509 (.CER)</li> <li>Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)</li> <li>Include all certificates in the certification path if possible</li> </ul>		DER encoded binary X.509 (.CER)
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)		Base-64 encoded X.509 (.CER)
Include all certificates in the certification path if possible		Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
		Include all certificates in the certification path if possible
		Include all certificates in the certification path if possible
Include all certificates in the certification path if possible		Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

16. Geben Sie im Fenster Password (Kennwort) ein Kennwort ein. In diesem Beispiel wird **cisco** als Kennwort

verwendet.	
Certificate Export Wizard	
Password To maintain security, you must protect th	he private key by using a password.
Type and confirm a password.	
Password:	
] <u>C</u> onfirm password:	
*****	
	< <u>B</u> ack <u>N</u> ext > Cancel

17. Speichern Sie die Zertifikatsdatei (.PFX-Datei) auf Ihrer Festplatte. Klicken Sie auf **Weiter**, und beenden Sie den Exportvorgang



## Herunterladen des Gerätezertifikats auf den WLC

Nachdem das WLC-Gerätezertifikat jetzt als PFX-Datei verfügbar ist, wird die Datei im nächsten Schritt auf den Controller heruntergeladen. Cisco WLCs akzeptieren Zertifikate nur im PEM-Format. Daher müssen Sie die Datei im .PFX- oder PKCS12-Format zunächst mithilfe des openSSL-Programms in eine PEM-Datei konvertieren.

Konvertieren des Zertifikats in PFX in PEM-Format mit dem openSSL-Programm

Sie können das Zertifikat auf jeden PC kopieren, auf dem Sie openSSL installiert haben, um es in das PEM-Format zu konvertieren. Geben Sie die folgenden Befehle in die Datei Openssl.exe im Ordner bin des OpenSSL-Programms ein:

Hinweis: Sie können openSSL von der OpenSSL- Website herunterladen.

!--- 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

Die Zertifikatsdatei wird in das PEM-Format konvertiert. Der nächste Schritt ist das Herunterladen des Gerätezertifikats im PEM-Format auf den WLC.

**Hinweis:** Zuvor benötigen Sie eine TFTP-Server-Software auf Ihrem PC, von der die PEM-Datei heruntergeladen werden soll. Dieser PC muss über eine Verbindung mit dem WLC verfügen. Auf dem TFTP-Server sollten das aktuelle Verzeichnis und das Basisverzeichnis mit dem Speicherort der PEM-Datei angegeben werden.

Laden Sie das Gerätezertifikat im konvertierten PEM-Format in den WLC herunter.

In diesem Beispiel wird der Downloadvorgang über die CLI des WLC erläutert.

- 1. Melden Sie sich an der CLI des Controllers an.
- 2. Geben Sie den Befehl transfer download datatype eapdevcert ein.
- 3. Geben Sie den Befehl **transfer download serverip** *10.77.244.196 ein*.10.77.244.196 ist die IP-Adresse des TFTP-Servers.
- 4. Geben Sie den Befehl **transfer download file name** *ciscowlc.pem ein*.ciscowlc123.pem ist der in diesem Beispiel verwendete Dateiname.
- 5. Geben Sie den Befehl **transfer download certpassword** ein, um das Kennwort für das Zertifikat festzulegen.
- 6. Geben Sie den Befehl transfer download start ein, um die aktualisierten Einstellungen anzuzeigen.Beantworten Sie dann y, wenn Sie aufgefordert werden, die aktuellen Einstellungen zu bestätigen und den Download-Vorgang zu starten.Dieses Beispiel zeigt die Ausgabe des Befehls 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. Geben Sie den Befehl **reset system** (**System zurücksetzen**) ein, um den Controller neu zu starten. Der Controller wird nun mit dem Gerätezertifikat geladen.

#### Installieren des Stammzertifikats von PKI im WLC

Nachdem nun das Gerätezertifikat im WLC installiert ist, besteht der nächste Schritt darin, das

Stammzertifikat der PKI vom CA-Server auf dem WLC zu installieren. Gehen Sie folgendermaßen vor:

 Gehen Sie zu http://<IP-Adresse des CA-Servers>/certsrv von Ihrem PC, der eine Netzwerkverbindung zum CA-Server hat. Melden Sie sich als Administrator des CA-Servers an.



2. Klicken Sie auf Zertifizierungsstellenzertifikat, Zertifikatskette oder Zertifikatsperrliste herunterladen.

File Edit Vers Excelate Took Help	-
Address at http://10.77.244.190/certsrv/	🔁 Go
	10
Microsoft Certificate Sentess He	me
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 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. Auf der Ergebnisseite werden die aktuellen Zertifizierungsstellenzertifikate angezeigt, die auf dem Zertifizierungsstellenserver im Feld für das **Zertifizierungsstellenzertifikat** verfügbar sind.

Wählen Sie **DER** als Verschlüsselungsmethode aus, und klicken Sie auf **CA-Zertifikat** herunterladen.

Microsoft Certificate Services - Microsoft Internet Explorer	
Ple Edit View Pavertist Tools Help	A.
Addimus 🚯 http://10.77.244.198/certsrv/certcarc.asp	🚽 🔁 Go
	10
Microsoft Certificate Services - wretees	Home
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:	
Encoding method: © DER © Base 64 Download CA certificate Download latest base CRL Download latest data CRL	
	ernet

- 4. Speichern Sie das Zertifikat als .cer-Datei. In diesem Beispiel wird certnew.cer als Dateiname verwendet.
- 5. Im nächsten Schritt wird die CER-Datei in das PEM-Format konvertiert und auf den Controller heruntergeladen. Wiederholen Sie zum Durchführen dieser Schritte den gleichen Vorgang wie im Abschnitt <u>Herunterladen des Gerätezertifikats auf den WLC</u> mit den folgenden Änderungen:Die openSSL-Dateien "-in" und "-out" sind certnew.cer und certnew.pem.Außerdem sind bei diesem Prozess keine PEM-Kennzeichenfolgen oder Import-Kennwörter erforderlich.Der Befehl openSSL zur Konvertierung der Datei .cer in die Datei .pem lautet ebenfalls wie folgt:x509 -in certnew.cer -information DER -out certnew.pem -outform PEMIn Schritt 2 des Abschnitts <u>Download the Converted PEM Format Device</u> Certificate to the WLC (Konvertiertes PEM-Format-Gerätezertifikat in den WLC herunterladen) lautet der Befehl zum Herunterladen des Zertifikats in den WLC:(Cisco Controller)>Datentyp "Transfer Download" eapcacertDie Datei, die auf den WLC heruntergeladen werden soll, ist certnew.pem.

Sie können über die grafische Benutzeroberfläche des Controllers wie folgt überprüfen, ob die Zertifikate auf dem WLC installiert sind:

 Klicken Sie in der WLC-GUI auf Sicherheit. Klicken Sie auf der Seite Sicherheit auf Erweitert > IPSec-Zertifikate aus den links angezeigten Aufgaben. Klicken Sie auf CA Certificate (Zertifizierungsstellenzertifikat), um das installierte Zertifizierungsstellenzertifikat anzuzeigen. Hier ein Beispiel:



 Um zu überprüfen, ob das Gerätezertifikat auf dem WLC installiert ist, klicken Sie in der WLC-GUI auf Security (Sicherheit). Klicken Sie auf der Seite Sicherheit auf Erweitert > IPSec-Zertifikate aus den links angezeigten Aufgaben. Klicken Sie auf ID Certificate, um das installierte Gerätezertifikat anzuzeigen. Hier ein Beispiel:

Deispiei.										
🗿 wic2006 - Microsoft Inter	rnet Explorer									
File Edit View Favorites	Tools Help									
ababa									i <u>B</u> ing   L	ogout <u>R</u> efresh
CISCO	MONITOR	WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP		
Security	ID Certifica	ate			)	-			1	New
<ul> <li>AAA General RADIUS Authentication Accounting</li> <li>TACACS+ LOAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies</li> <li>Local EAP</li> <li>Priority Order</li> <li>Access Control Lists</li> <li>Wireless Protection Policies</li> <li>Web Auth</li> <li>Advanced</li> <li>CIDS Sensors Shunned Clients</li> <li>IPSec Certs GA Cardinose ID Certificate</li> </ul>	Name bsnSslEapDe	wCert	From the second	lid Period om 2008 Jan 24	eh, 12:18:31 (	GMT Un6i 2010 Ja	n 23rd, 12:18:31			
ē)								1	🔵 Interr	et.
-										

#### Generieren eines Gerätezertifikats für den Client

Nachdem das Gerätezertifikat und das Zertifizierungsstellenzertifikat auf dem WLC installiert sind, besteht der nächste Schritt darin, diese Zertifikate für den Client zu generieren.

Führen Sie diese Schritte aus, um das Gerätezertifikat für den Client zu generieren. Dieses Zertifikat wird vom Client für die Authentifizierung beim WLC verwendet. In diesem Dokument werden die Schritte zum Generieren von Zertifikaten für den professionellen Windows XP-Client erläutert.

 Gehen Sie zu http://<IP-Adresse des CA-Servers>/certsrv vom Client, auf dem das Zertifikat installiert werden muss. Melden Sie sich beim CA-Server als Domänenname\Benutzername an. Beim Benutzernamen sollte es sich um den Namen des Benutzers handeln, der diesen XP-Computer verwendet. Der Benutzer sollte bereits als Teil derselben Domäne wie der Zertifizierungsstellenserver konfiguriert

sein.	
Connect to 10.77.	244.198 🔹 🔁 🔀
Connecting to 10.77.	244.198
User name:	🛃 wireless\user2
Password:	
	Remember my password
	OK Cancel

2. Wählen Sie Zertifikat anfordern

Microsoft Certificate Services - Microsoft Internet Explorer	
e Edit View Favorites Tools Help	
ansi a Mapu/10.77.244.190/certarv/	Sec. 10
ficrosoft Certificate Services wireless	Home
/elcome	
Ise this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certific dentity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type erform other security tasks.	ate, you can verify your of certificate you request,
ou can also use this web site to download a certificate authority (CA) certificate, certificate chain, or certificate re ew the status of a pending request.	evocation list (CRL), or to
or more information about Certificate Services, see Certificate Services Documentation.	
elect a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	

3. Klicken Sie auf der Seite Zertifikat anfordern auf **Erweiterte** 

Zertifikatsanforderung.	
Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Pavorities Tools Help	A1
Address 🕘 http://10.77.244.198/certsrv/certraus.esp	🚽 🛃 Go
Silement Carificato Sanicaa viiniaa	Home
And the second contracts of the second	A DETINE
Request a Certificate	
Calact the certificate type:	
User Certificate	
Or(submit an <u>advanced certificate request</u> .	
http://10.77.244.198/certsrv/certrgad.asp	Internet

4. Klicken Sie auf der Seite "Erweiterte Zertifikatanforderung" auf **Erstellen, und senden Sie** eine Anforderung an diese Zertifizierungsstelle. Dadurch gelangen Sie zum Anforderungsformular für Advanced-

-			
∠e	rtifi	kate.	

e Edit View Pavorites Tools Help	
Inss and Napul/10.77.244.198/certsrv/certroad.asp	<u>×</u> 🔁
ficroad/ Certificate Services - wireless	Heme
Avanced Certificate Resused	
Ivanced Certificate Request	
e policy of the CA determines the types of certificates you can request. Click one of the	e 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 file, or s	submit a renewal request by using a base-64-encoded
PRCS #7 file	
Request a certificate for a smart card on behalf of another user by using the smart car. Note: You must have an enrollment agent cartificate to submit a request on behalf of another user.	d certificate enrolment station.

5. Wählen Sie im Anforderungsformular für erweiterte Zertifikate im Dropdown-Menü Zertifikatvorlage die Option **Benutzer** aus.Wählen Sie im Abschnitt "Key options" (Schlüsseloptionen) folgende Parameter aus:Geben Sie die Schlüssellänge in das Feld Schlüssellänge ein. In diesem Beispiel wird **1024** verwendet.Aktivieren Sie die Option **Schlüssel als exportierbar** 

#### markieren.

Microsoft Certi	licate Services - Microsoft Internet Explorer	
File Edit View	Favorités Tools Help	
Address 🚳 Nttp://10	.77.244.196/certsrv/certrgma.esp	💌 🔁 Go
	ante Manufano - Vintera	· · · · · · · · · · · · · · · · · · ·
Microsoff Centre	ate Services wreless	Heme
Advanced Ce	rtificate Request	1
Certificate Temp	date:	
	Basic EFS Y	
Key Options:	Basic EFS User	
	© Create new key set	
CSP:	Microsoft Enhanced Cryptographic Provider v1.0	
Key Usage:	Exchange	
Key Size	1024 Min: 394 (common key pizer: 612 1924 2049 4096 0.922 16394 )	
	Actomatic law container name     Other specified law container name	
	Mark keys as exportable	
	Export koyo to file	
	Enable strong private key protection	
	Store certificate in the local computer certificate store	
	Stores the centricate in the local computer alore instead of in the user's centificate store. Does not	
	install the root CA's certificate. You must be an	
	auministrator to generate or use a vey in the local machine store.	
Additional Optio	06	
Request Format:	©CMC OPKCS10	
Hash Algorithm	SHA.1 V	
	Only used to sign request.	
	Save request to a file	
Attributes:		
Done Done		Internet

6. Konfigurieren Sie alle anderen erforderlichen Felder, und klicken Sie auf

Aldronoff Certificate Services - Microsoft Internet Leptorer Face voir Pacieta Tool Page Face voir Pacieta Page Face voir Page voir Page Face voir Page v	Senden.	
Reguest Format:     Childrend Options:     Request Format:     Childrend Value     Childrend Value     Childrend Value     Chil	Microsoft Certificate Services - Microsoft Internet Explorer	
Image: Start + Image: Sta	Pås Edit View Pavortes Tools Help	
Additional Options:	🔾 Back + 🕥 - 🖹 📓 🐔 🔎 Search 🦅 Pavortes 🤣 🎯 + 🌺 🔜 🖄	
Oreste new key set     Oreste new key set     Oreste new key set     Oreste mew key set     Oreste mew key set     Oreste mew key set     Oreste new key s	Addshess and http://b0.77.244.198/certary.jcertrgna.asp	🛩 🛃 ຍາ
CSP: Microsoft RSA SChannel Cryptographic Provider V Key Size D2A Microsoft (rememon key street 512 5024 5024 6026 5182 10004) @ Automatic key container name @ User specified key container name @ Mark keys as exportable @ Export keys 10 fe @ Table strong private key protection @ Store certificate in the local computer certificate store Stores the certificate in the local computer store instal Derived CAS certificate. You must be an administratic to generate or use a key in the local machine ato: Additional Options: Privedly Name: Privedly Name:	Create new key set     Ouse existing key set	^
Key Usage:       Exchange         Key Size:       1024       Mar. 1694       Common key state 132 1024 2084 4000 (102 1004)         Automatic kay container name       User specified key container name       User specified key container name         Export keys to file       Export keys to file       Export keys to file         Enable strong private key protection       Store certificate in the local computer actificate store         Stores the certificate in the local computer actificate store       Stores the certificate. You must be an administrator to generate or use a key in the local machine atore.         Additional Optione:	CSP: Microsoft RSA SChannel Cryptographic Previder 🍟	
Wey Size:       1024       Min: 804 Mark 1097         © Automatic key container name       User specified key container name         © Mark keys as expontable       Expont keys to file         Expont keys to file       Expont keys to file         Store certificate in the local computer datre instead of in the user's certificate store Stores the certificate in the local computer datre instead of a the user's certificate store. Does not instal the not CA's certificate to use a key in the local machine date.         Additional Options:       Request Format:         Request Format:       CMC         Only used to sign request.         Same request to a file         Attributes:         Priendly Name:	Kay Usage: ③ Exchange	
Automatic key container name     Mark keys as exportable     Equat keys to file     Enable strong private key protection     Store certificate in the local computer certificate store     Storea the certificate in the local computer attace     instalf the nool CA's certificate. You must be an     administrator to generate or use a key in the local     machine atore.  Additional Options:  Request Format:     Ordy used to eign request.     Store request to a file  Attributes:  Friendly Name:  Dubmit >	Key Size: 1024 Mic: 1024 40 (ceremon key sizer: 512 1024 2048 606 5192 15364 )	
Mark keys as exportable Export keys to fie Export keys to fie The board computer certificate store Stores the certificate in the local computer store Stores the certificate in the local computer store and star the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.  Additional Options:  Request Format: CMC OPKCS10 Hash Algorithm Orly used to a fie Attributes: Friendly Name:  Dubmit >	Automatic key container name     Ouser specified key container name	
■ Export keys to fie ■ Export keys to field ■ Export	I Mark keys as exportable	
■ Internet in the local computer certificate store Stores Stores the certificate in the local computer atore instead of in the use's certificate atore. Does not install the root CA's certificate. You must be an adminiatizator to generate or use a key in the local machine atore.          Additional Options:         Request Format:       CMC       OPKCS10         Hash Algorithm:       SHA1       Only used to sign request.         Size request to a file       Size request to a file         Attributes:       Size request to a file         Friendly Name:       Sizemation	Export keys to file	
Store certificate in the local computer certificate store instead of in the local computer store instead 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:       OMC         ONLY used to sign request.         Sine request to a file         Attributes:         Friendly Name:	Enable strong private key protection	
Additional Options: Request Format: CMC @PKCS10 Hash Algorithm: SHA1 @ Only used to sign request. Save request to a file Attributes: Friendly Name: Submit >	Store certificate in the local computer certificate store Stores the certificate in the local computer store install the root GA's certificate store. Does not install the root GA's certificate, You must be an administrator to generate or use a key in the local machine store.	
Request Format: ○CMC ●PKCS10 Hash Algorithm: □HA1 ♥ Colly used to sign request. □ Save request to a file Attributes: Friendly Name: Submit >	Additional Options:	
Hash Algorithm: SHA1 Only used to sign request. Save request to a file Attributes: Friendly Name: Submit >	Request Format: OCMC @PKCS10	
Only used to sign request.  Save request to a file  Attributes:  Friendly Name:  Submit >	Hash Algorithm: SHA-1 V	
Save request to a file  Attributes:  Friendly Name:  Submit >	Only used to sign request.	
Attributes:	Save request to a file	
Friendly Name:	Attributes:	
Submit >	Friendly Name:	
Submit >		
a) a Internet	Submit >	
a) 🕒 Diternat		
		Internet

7. Das Gerätezertifikat des Clients wird jetzt entsprechend der Anforderung generiert. Klicken Sie auf **Zertifikat installieren**, um das Zertifikat im Zertifikatspeicher zu installieren.

A Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	47
Address al http://10.77.244.190/certsrv/certfinsh.asp	🚽 🛃 Go
	8
Microsoff Certificate Services wireless	Home
Certificate Issued	
The certificate you requested was issued to you.	
Install this certificate	
	M.
	Unternet

 Sie sollten das Gerätezertifikat des Clients in der Liste Persönliches Zertifikat unter Extras > Internetoptionen > Inhalt > Zertifikate im IE-Browser des Clients finden können.

rtificates				- 12
tended purpose:	<all></all>	A the line True	ted Product at Kingh	1.00
Other Peo	pple Intermediate Certification	Auchonicies	sted Root Certificat	lor
Issued To 1234	Ussued By wireless	Expiratio 1/25/2009	<pre>Eriendly.Name <none></none></pre>	
Import Ex	port Remove		Adva	anced
Import E>	purposes		Adva	anced
Import Ex Certificate intended Encrypting File Syste	port Remove		Adva	anced
Import Ex Certificate intended Encrypting File Syste	purposes		Adva	anced

Das Gerätezertifikat für den Client wird auf dem Client installiert.

Generieren des Stammzertifizierungsstellenzertifikats für den Client

Im nächsten Schritt wird das Zertifizierungsstellenzertifikat für den Client generiert. Führen Sie die folgenden Schritte vom Client-PC aus:

 Gehen Sie zu http://<IP-Adresse des CA-Servers>/certsrv vom Client, auf dem das Zertifikat installiert werden muss. Melden Sie sich beim CA-Server als Domänenname\Benutzername an. Beim Benutzernamen sollte es sich um den Namen des Benutzers handeln, der diesen XP-Computer verwendet. Der Benutzer sollte bereits als Teil derselben Domäne wie der Zertifizierungsstellenserver konfiguriert sein

Selli.		
Connect to 10.7	77.244.198	? 🔀
Connecting to 10.3	77.244.198	
User name:	🛃 wireless\user2	💌
Password:		
	Remember my password	
		Cancel

2. Auf der Ergebnisseite werden die aktuellen Zertifizierungsstellenzertifikate angezeigt, die auf dem Zertifizierungsstellenserver im Feld f
ür das Zertifizierungsstellenzertifikat verf
ügbar sind. W
ählen Sie Base 64 als Encoding-Methode aus. Klicken Sie dann auf CA-Zertifikat herunterladen und speichern Sie die Datei auf dem Client-PC als .cer-Datei. In diesem Beispiel wird rootca.cer als Dateiname

Microsoft Certificate Services - Microsoft Internet Explorer      Microsoft Certificate Services - Microsoft Internet Explorer      Microsoft Certificate Services      Microsoft Certificate Services      Microsoft Certificate Services      Microsoft Certificate Services      Microsoft Certificate Services	2 X 2 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3
Microsoft Conflicture Services     Microsoft Conflicture Services	දී ග ි
Address AMerceff Certificate Services - versions Home	60 ()
Microsoft Confidence Services	
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 chain	
Download latest base CRL	
Download latest delta CRL	
	-
	1

 Installieren Sie anschließend das CA-Zertifikat, das im CER-Format gespeichert ist, im Zertifikatspeicher des Clients. Doppelklicken Sie auf die Datei rootca.cer, und klicken Sie auf Zertifikat

#### installieren.

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	ient OK

4. Klicken Sie auf **Weiter**, um das Zertifikat von der Festplatte des Clients in den Zertifikatspeicher zu

# Certificate Import Wizard Image: Certificate Import Vizard Image: Certificate Import Wizard Image: Certificate Import Vizard Image: Certificate

5. Wählen Sie **den Zertifikatspeicher basierend auf dem Zertifikatstyp automatisch aus,** und klicken Sie auf **Weiter**.

icate Import Wizard	Ð
tificate Store Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a location for	
Automatically select the certificate store based on the type of certificate	
O Place all certificates in the following store	
Browse	
< Back Next > Cancel	
	cate Import Wizard         tificate Store         Certificate stores are system areas where certificates are kept.         Windows can automatically select a certificate store, or you can specify a location for         Image: Automatically select the certificate store based on the type of certificate         Image: Place all certificates in the following store         Certificate store:         Image: Place store:

6. Klicken Sie auf **Beenden**, um den Importvorgang abzuschließen.

Certificate Import Wizard			X
	Completing the C Wizard You have successfully complexized. You have specified the follow Certificate Store Selected Content	Certificate Import leted the Certificate Import wing settings: Automatically determined by t Certificate	
	< Back	Finish Cancel	

7. In der Standardeinstellung werden Zertifizierungsstellenzertifikate im IE-Browser des Clients unter Extras > Internetoptionen > Inhalt > Zertifikate in der Liste Vertrauenswürdige Stammzertifizierungsstellen installiert. Hier ein Beispiel:

rtificates				?
tended purpose: <a>All&gt;</a>	×			
Intermediate Certification Au	thorities Trusted Root C	ertification Aut	norities Trusted Put	a <
Issued To	Issued By	Expiratio	Friendly Name	1
VeriSign Trust Netw	VeriSign Trust Network	5/19/2018	VeriSign Class 3	
WeriSign 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	5/19/2018	VeriSign Class 1	
E wireless	wireless	1/23/2013	<none></none>	
Wireless-CA	Wireless-CA	12/18/2012	<none></none>	
Xcert EZ by DST	Xcert EZ by DST	7/11/2009	Xcert EZ by DST	~
Import Export	Remove		Advan	ced
Cashificanta interneted as service				
certificate interficed purpose				
<all></all>			View	
				se

Alle erforderlichen Zertifikate werden sowohl auf dem WLC als auch auf dem Client für die EAP-FAST Local-EAP-Authentifizierung installiert. Im nächsten Schritt wird der WLC für die lokale EAP-Authentifizierung konfiguriert.

## Konfigurieren des lokalen EAP auf dem WLC

Führen Sie im **WLC-GUI-Modus** die folgenden Schritte aus, um die lokale EAP-Authentifizierung auf dem WLC zu konfigurieren:

1. Klicken Sie auf **Sicherheit > Lokaler** 

ie Edit View Pavorites	Tools Help							
uludu cisco	MONITOR MLANS	CONTROLLER	WIRELESS (	SECURITY	MANAGEMENT	Saya Ca C <u>O</u> MMANDS	nfiguration   P HELP	ing i Logout i <u>B</u> efre
Security	RADIUS Authentie	ation Servers		$\bigcirc$			Apply	New
AAA General RADUUS Automication Accounting TACACS+ LDAP Local Net Users MAC Pittering Disabled Clients User Login Policies AP.Polose Local EAP Priority Order Access Control Lists Wireless Protection Policies Web Auth Advanced	Call Station ID Typ Use AES Key Wrap Network User Man	e IP Address  (Designed fr agement Server)	or FIPS custo	mers and requ	iires a key wrap o s <u>Port</u> IPSec	ampliant RADIU:	š server)	
							A	. Internet

2. Klicken Sie unter Local EAP (Lokales EAP) auf **Profiles** (Profile), um das Profil Local EAP (Lokales EAP) zu

#### konfigurieren.

Wic2006 - Microsoft Interne	t Explorer	
	Save Config MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS H	guration   Eing   Logout   Befresh IELP
Security AAA General RADIUS Authentication Accounting TACACS+ LOAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Control Policies Control Priority Order Access Control Lists Wireless Protection Policies Wireless Protection Policies Wireless Protection Policies	RADIUS Authentication Servers Call Station ID Type IP Address  USe AES Key Wrap  (Designed for FIPS customers and requires a key wrap compliant RADIUS or Network User Planagement Server Index Server Address Port IPSec Admin Status	Apply New

- 3. Klicken Sie auf **Neu**, um ein neues lokales EAP-Profil zu erstellen.
- 4. Konfigurieren Sie einen Namen f
  ür dieses Profil, und klicken Sie auf Apply. In diesem Beispiel lautet der Profilname Idap. Dadurch gelangen Sie zu den lokalen EAP-Profilen, die auf dem WLC erstellt

wurden.									
Wic2006 - Microsoft Inter	net Explorer								
File Edit View Pavorites	Tools Help								27
ահանո								nfiguration <u>P</u> in	9 Logout Befresh
CISCO	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Local EAF	Profile	s≻New					< Back	Apply
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>TACACS+</li> <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>	Profile Nar	ne		ldap					
<ul> <li>Local EAP General Profiles EAP-FAST Parameters Authentication Priority</li> </ul>									
▶ Priority Order									
▶ Access Control Lists									
Wireless Protection Policies									
F Web Auth									
Advanced									
() Done								A .	Internet

 Klicken Sie auf das gerade erstellte LDAP-Profil, das im Feld Profilname der Seite Lokale EAP-Profile angezeigt wird. Dadurch gelangen Sie zur Seite Lokale EAP-Profile > Bearbeiten.

wic2006 - Microsoft Inte	rnet Explorer								
File Edit View Pevorites	Tools Help	_							
ահանո								nfiguration   Ping	Logout Refresh
CISCO	MONITOR	<u>WLAN5</u>	CONTROLLER	W]RELES!	S SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Local EA	P Profile	8					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	Ideo							0	
<ul> <li>Local EAP General Profiles EAP-FAST Parameters Authentication Priority</li> </ul>									
▶ Priority Order									
▶ Access Control Lists									
Wireless Protection Policies									
Web Auth									
▶ Advanced									

6. Konfigurieren Sie die für dieses Profil spezifischen Parameter auf der Seite Lokale EAP-Profile > Bearbeiten.Wählen Sie EAP-FAST als lokale EAP-Authentifizierungsmethode aus. Aktivieren Sie die Kontrollkästchen neben Lokales Zertifikat erforderlich und Clientzertifikat erforderlich. Wählen Sie als Zertifikataussteller den Anbieter aus, da in diesem Dokument ein Zertifizierungsstellenserver eines Drittanbieters verwendet wird. Aktivieren Sie das Kontrollkästchen neben Prüfung auf Zertifizierungsstellenzertifikate, damit das vom Client eingehende Zertifikat anhand der Zertifizierungsstellenzertifikate auf dem Controller validiert werden kann. Wenn der allgemeine Name (CN) im eingehenden Zertifikat mit der CN der Zertifizierungsstellenzertifikate auf dem Controller überprüft werden soll, aktivieren Sie das Kontrollkästchen Zertifikat-CN-Identität überprüfen. Standardmäßig ist diese Option deaktiviert. Damit der Controller überprüfen kann, ob das eingehende Gerätezertifikat noch gültig und nicht abgelaufen ist, aktivieren Sie das Kontrollkästchen Check Certificate Date Validity (Zertifikatsdatumvalidität überprüfen). Hinweis: Die Gültigkeit des Zertifikatsdatums wird mit der aktuellen UTC (GMT)-Zeit verglichen, die auf dem Controller konfiguriert ist. Der Zeitzonenoffset wird ignoriert.Klicken Sie auf Apply (Anwenden).



7. Das lokale EAP-Profil mit EAP-FAST-Authentifizierung wird jetzt auf dem WLC

erstellt.	net Explorer								
File Edit View Fevorites T	tools Help								
ahaha							Saye Co	nfiguration thing	Logout Befresh
CISCO	MONITOR	<u>W</u> LANS	CONTROLLER	W]RELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Local EAP	Profiles						New	Apply
<ul> <li>ARA General</li> <li>RADIUS Authentication Accounting</li> <li>TACACS+ LOAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies</li> <li>Local EAP General Profiles EAP-FAST Parameters Authentication Priority</li> <li>Priority Order</li> <li>Access Control Lists</li> <li>Wireless Protection Policies</li> <li>Web Auth</li> <li>Advanced</li> </ul>	Profile Nan Idao				J	EAP-TLS	PEAP		
Cone								🛆 🔵 1/	nternet

8. Im nächsten Schritt werden EAP-FAST-spezifische Parameter auf dem WLC konfiguriert. Klicken Sie auf der Seite "WLC Security" auf Local EAP > EAP-FAST Parameters, um zur Seite "EAP-FAST Method Parameters" zu wechseln.Deaktivieren Sie das Kontrollkästchen Anonyme Bereitstellung, da in diesem Beispiel EAP-FAST unter Verwendung von Zertifikaten erläutert wird. Lassen Sie alle anderen Parameter auf ihren Standardwerten. Klicken Sie auf Apply (Anwenden).

wic2006 - Microsoft Inter	net Explorer			
uluilu cisco	MONITOR WLANS CONTROLLER WIRELES		Saye Confi COMMANDS	guration   <u>P</u> ing   Logaut Befreal HELP
Security	EAP-FAST Method Parameters	$\bigcirc$		Apply
The AAA General	Server Key (in hex)	****		
RADIUS Authentication	Confirm Server Key	••••		
IN TACACS+	Time to live for the PAC	10 doys		
Local Net Users MAC Filtering Disabled Clients	Authority ID (in hex)	436973636f		
User Login Policies AP Policies	Authority ID Information	Citco A-ID		
T Local EAP Gonard Profiles EAP-FAST Parameters Interference Princip	Anonymous Provision	Enabled		
E Priority Order				
Access Control Lists     Wireless Protection     Policies				
H Web Auth				
E Advanced				
0				A Privat

Konfigurieren des WLC mit LDAP-Serverdetails

Nachdem der WLC mit dem lokalen EAP-Profil und den zugehörigen Informationen konfiguriert wurde, besteht der nächste Schritt darin, den WLC mit Details des LDAP-Servers zu konfigurieren. Führen Sie am WLC die folgenden Schritte aus:

 Wählen Sie auf der Seite Sicherheit des WLC im Aufgabenbereich auf der linken Seite AAA
 LDAP aus, um zur LDAP-Serverkonfigurationsseite zu wechseln. Um einen LDAP-Server hinzuzufügen, klicken Sie auf Neu. Die Seite LDAP-Server > Neu wird angezeigt.



2. Geben Sie auf der Seite "LDAP Servers Edit" (LDAP-Server bearbeiten) Details zum LDAP-Server an, z. B. IP-Adresse des LDAP-Servers, Portnummer, Serverstatus aktivieren usw.Wählen Sie eine Zahl aus dem Dropdown-Feld Serverindex (Priorität) aus, um die Prioritätsreihenfolge dieses Servers in Bezug auf andere konfigurierte LDAP-Server anzugeben. Sie können bis zu siebzehn Server konfigurieren. Wenn der Controller den ersten Server nicht erreichen kann, versucht er den zweiten Server in der Liste und so weiter. Geben Sie die IP-Adresse des LDAP-Servers in das Feld Server-IP-Adresse ein.Geben Sie die TCP-Portnummer des LDAP-Servers in das Feld Portnummer ein. Der gültige Bereich liegt zwischen 1 und 65535, und der Standardwert ist 389.Geben Sie im Feld User Base DN (Benutzerbasis-DN) den Distinguished Name (DN) der Unterstruktur des LDAP-Servers ein, der eine Liste aller Benutzer enthält. Beispielsweise ou=Organisationseinheit, .ou=nächste Organisationseinheit und o=corporation.com. Wenn es sich bei der Struktur mit den Benutzern um die Basis-DN handelt, geben Sie o=corporation.com oder dc=corporation, dc=com ein.In diesem Beispiel befindet sich der Benutzer unter der Organisationseinheit Idapuser (OU), die wiederum als Teil der Wireless.com-Domäne erstellt wird.Der Benutzerbasis-DN sollte auf den vollständigen Pfad verweisen, in dem sich die Benutzerinformationen (Benutzeranmeldeinformationen gemäß der EAP-FAST-Authentifizierungsmethode) befinden. In diesem Beispiel befindet sich der Benutzer unter der Basis-DN OU=Idapuser, DC=Wireless, DC=com.Weitere Einzelheiten zur OU sowie zur Benutzerkonfiguration werden im Abschnitt Erstellen von Benutzern auf dem Domänencontroller dieses Dokuments erläutert. Geben Sie im Feld Benutzerattribut den Namen des Attributs in den Benutzerdatensatz ein, der den Benutzernamen enthält.Geben Sie im Feld User Object Type (Benutzerobjekttyp) den Wert des LDAP objectType-Attributs ein, das den Datensatz als Benutzer identifiziert. Benutzerdatensätze verfügen häufig über mehrere Werte für das objectType-Attribut, von denen einige für den Benutzer eindeutig sind und von denen einige für andere Objekttypen freigegeben sind. Hinweis: Sie können den

Wert dieser beiden Felder von Ihrem Verzeichnisserver mit dem LDAP-Browserdienstprogramm abrufen, das Teil der Windows 2003-Supporttools ist. Dieses Microsoft LDAP-Browsertool heißt LDP. Mithilfe dieses Tools können Sie die Felder Benutzerbasis-DN, Benutzerattribut und Benutzerobjekttyp dieses Benutzers kennen. Detaillierte Informationen zur Verwendung von LDP zum Kennzeichnen dieser benutzerspezifischen Attribute finden Sie im Abschnitt Verwenden von LDP zum Identifizieren von Benutzerattributen dieses Dokuments.Wählen Sie im Dropdown-Feld "Servermodus" die Option Sicher aus, wenn alle LDAP-Transaktionen einen sicheren TLS-Tunnel verwenden sollen. Andernfalls wählen Sie None (Keine), die Standardeinstellung.Geben Sie im Feld Server Timeout (Serverzeitüberschreitung) die Anzahl der Sekunden zwischen erneuten Übertragungen ein. Der gültige Bereich liegt zwischen 2 und 30 Sekunden, und der Standardwert ist 2 Sekunden. Aktivieren Sie das Kontrollkästchen Serverstatus aktivieren, um diesen LDAP-Server zu aktivieren, oder deaktivieren Sie ihn, um ihn zu deaktivieren. Der Standardwert ist deaktiviert.Klicken Sie auf Anwenden, um die Änderungen zu übernehmen. Hier ist ein Beispiel, das bereits mit diesen Informationen konfiguriert

wurde:								
🔁 wic2006 - Microsoft Inter	net Explorer							
File Edit View Favorites T	lools Help							Ay
abab							nfiguration <u>P</u> ir	ng   Logout   <u>R</u> efresh
cisco	MONITOR WLANS	CONTROLLER	W]RELESS	SECURITY	MANAGEMENT	COMMANDS	неџр	
CISCO Security * AAA General * RADIUS Authentication Accounting TACACS+ LOAF Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies E Local EAP F Priority Order F Access Control Lists Wireless Protection Policies W Web Auth Advanced	MONITOR WLANS LDAP Servers > E Server Index Server Address Port Number User Base DN User Attribute User Object Type Server Mode Server Timeout Enable Server Status	CONTROLLER dit 1 10.77 389 OU=5 SAMA Perso None 30 : V	W]RELESS 7.244.198 dapuser,DC+mi iccountName in seconds	SECURITY	m	COMMANDS	HELP < Back	Apply
Done								Internet

Nachdem nun die Details zum LDAP-Server auf dem WLC konfiguriert sind, besteht der nächste Schritt darin, LDAP als Backend-Datenbank mit Priorität zu konfigurieren, sodass der WLC zunächst in der LDAP-Datenbank nach Benutzeranmeldeinformationen und nicht nach anderen Datenbanken sucht.

## LDAP als primäre Backend-Datenbank konfigurieren

Führen Sie auf dem WLC die folgenden Schritte aus, um LDAP als bevorzugte Backend-Datenbank zu konfigurieren:  Klicken Sie auf der Seite Sicherheit auf Lokaler EAP > Authentifizierungspriorität. Auf der Seite "Priority Order" (Prioritätsreihenfolge) > "Local-Auth" (Lokale Authentifizierung) finden Sie zwei Datenbanken (Lokal und LDAP), in denen die Benutzeranmeldeinformationen gespeichert werden können.Um LDAP als Prioritätsdatenbank festzulegen, wählen Sie LDAP aus dem Feld für die Anmeldeinformationen des Benutzers auf der linken Seite aus, und klicken Sie auf die > Schaltfläche, um LDAP in das Feld für die Prioritätsreihenfolge auf der rechten Seite zu

verschieben.								
🚰 wic2006 - Microsoft Intern	et Explorer							
File Edit View Pavorites To	ols Help							. 🦓
սիսիս							figuration	Ping   Logout   <u>R</u> efresh
CISCO	MONITOR WLAN	5 CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Priority Order >	Local-Auth		$\frown$				Apply
<ul> <li>Constal</li> <li>General</li> <li>RADIUS</li> <li>Autheotication</li> <li>Accounting</li> <li>TACACS+</li> <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> <li>AP Policies</li> </ul>	User Credential		P wn					
General Profiles RDP-FAST Parameters Authentication Priority Priority Ocdes Process Control Lists Wireless Protection								
* Policies								
P Web Auth								
<b>Ø</b> ]								Internet

 Dieses Beispiel zeigt deutlich, dass LDAP im linken Kästchen ausgewählt und die Schaltfläche > ausgewählt wurde. Als Ergebnis wird LDAP in das Feld rechts verschoben, das die Priorität festlegt. Die LDAP-Datenbank wird als Authentifizierungsprioritäts-Datenbank ausgewählt.Klicken Sie auf **Apply** (Anwenden).



**Hinweis:** Wenn sowohl LDAP als auch LOCAL im rechten Feld mit den Benutzeranmeldeinformationen angezeigt werden, wobei LDAP oben und LOCAL unten angezeigt wird, versucht Local EAP, Clients mithilfe der LDAP-Backend-Datenbank zu authentifizieren. Wenn die LDAP-Server nicht erreichbar sind, wird ein Failover zur lokalen Benutzerdatenbank durchgeführt. Wenn der Benutzer nicht gefunden wird, wird der Authentifizierungsversuch abgelehnt. Wenn LOCAL oben ist, versucht Local EAP, sich nur mithilfe der lokalen Benutzerdatenbank zu authentifizieren. Es findet kein Failover zur LDAP-Backend-Datenbank statt.

#### WLAN auf dem WLC mit lokaler EAP-Authentifizierung konfigurieren

Der letzte Schritt des WLC besteht in der Konfiguration eines WLAN, das Local EAP als Authentifizierungsmethode verwendet, wobei LDAP als Backend-Datenbank verwendet wird. Gehen Sie folgendermaßen vor:

- Klicken Sie im Hauptmenü des Controllers auf WLANs, um zur Konfigurationsseite für WLANs zu wechseln. Klicken Sie auf der Seite "WLANs" auf Neu, um ein neues WLAN zu erstellen. In diesem Beispiel wird ein neuer WLAN-LDAP erstellt.Klicken Sie auf Apply. Der nächste Schritt besteht darin, die WLAN-Parameter auf der Seite WLANs > Edit (WLANs > Bearbeiten) zu konfigurieren.
- Aktivieren Sie auf der Seite zur Bearbeitung des WLAN den Status dieses WLAN. Konfigurieren Sie alle weiteren erforderlichen Parameter.



- 3. Klicken Sie auf Sicherheit, um die sicherheitsrelevanten Parameter f
  ür dieses WLAN zu konfigurieren. In diesem Beispiel wird Layer-2-Sicherheit als 802.1x mit 104 Bit dynamischem WEP verwendet. Hinweis: In diesem Dokument wird 802.1x mit dynamischem WEP als Beispiel verwendet. Es wird empfohlen, sicherere Authentifizierungsmethoden wie WPA/WPA2 zu verwenden.
- 4. Klicken Sie auf der Seite "WLAN Security Configuration" auf die Registerkarte AAA Servers. Aktivieren Sie auf der Seite AAA-Server die Methode zur lokalen EAP-Authentifizierung, und wählen Sie Idap aus dem Dropdown-Feld aus, das dem Parameter EAP Profile Name (EAP-Profilname) entspricht. Dies ist das lokale EAP-Profil, das in diesem Beispiel erstellt wurde.

wic2006 - Microsoft Inte	rnet Explorer
 cisco	Sage Configuration   Eing   Logout   Befresh MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANS WLANS H Advanced	<form><form><form></form></form></form>
Done .	🛆 🌚 Internet

5. Wählen Sie den LDAP-Server (der zuvor auf dem WLC konfiguriert wurde) aus dem Dropdown-Feld aus. Stellen Sie sicher, dass der LDAP-Server vom WLC erreichbar ist.Klicken Sie auf **Apply** 

(Anwenden).		
a wic2006 - Microsoft Inter	ernet Explorer	🛛
File Edit View Favorites 1	Tools Help	- 47
սիսիս	Sage Configuration Bing Logout	l <u>R</u> efresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
WLANs	WLANs > Edit App	ily
* WLANS	General Security QoS Advanced	
WLANS	Layer 2 Layer 3 AAA Servers	
P Advanced	Select AAA servers below to override use of default servers on this WI AN	
	Radius Servers LDAP Servers	
	Authentication Servers Accounting Servers Server 10:10.77.244.198 Part: 389	
	✓ Enabled           ✓         Enabled	
	Server 1 None V 2	
	Server 2 None V None V Server 3 None V	
	Local EAP Authentication	
	Local EAP Authentication V Enabled	
	EAP Profile Name Idap 🛩	
	Foot Notes	
	1 CRIP is not supported by 10xx model APs 3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication	
	4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded cl 5 Client MPP is not active unless WPA2 is configured	lievots (
<b>a</b>	A a taunat	
	ainteritet.	

 Die neue WLAN-Idapwurde auf dem WLC konfiguriert. Dieses WLAN authentifiziert Clients mit lokaler EAP-Authentifizierung (in diesem Fall EAP-FAST) und fragt eine LDAP-Backend-Datenbank zur Überprüfung der Client-Anmeldeinformationen ab.

Sage Certiguration Engl Legel CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP WLANS WLANS IN THE CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	ut   <u>R</u> efresh
WLANS WLANS New	
WLANs         Profile Name         Type         WLAN SSID         Admin Status         Security Policies           > Advanced         Tawas         WLAN         Tawas         Enabled         (wFA2)(Auth(002.1X))	
Idaguser WLAN Idap Enabled 002.1X	

## **LDAP-Server konfigurieren**

Nach der Konfiguration des lokalen EAP auf dem WLC besteht der nächste Schritt in der Konfiguration des LDAP-Servers, der als Backend-Datenbank dient, um die Wireless-Clients nach erfolgreicher Zertifikatsvalidierung zu authentifizieren.

Der erste Schritt bei der Konfiguration des LDAP-Servers besteht darin, eine Benutzerdatenbank auf dem LDAP-Server zu erstellen, sodass der WLC diese Datenbank abfragen kann, um den Benutzer zu authentifizieren.

## Erstellen von Benutzern auf dem Domänencontroller

In diesem Beispiel wird ein neuer OU **Idapuser** erstellt, und **user2** wird unter dieser OU erstellt. Wenn dieser Benutzer für den LDAP-Zugriff konfiguriert wird, kann der WLC diese LDAP-Datenbank zur Benutzerauthentifizierung abfragen.

Die in diesem Beispiel verwendete Domäne ist wireless.com.

#### Erstellen einer Benutzerdatenbank unter einer Organisationseinheit

In diesem Abschnitt wird erläutert, wie Sie eine neue OU in Ihrer Domäne erstellen und einen neuen Benutzer auf dieser OU erstellen.

- 1. Klicken Sie auf dem Domänencontroller auf Start > Programme > Verwaltung > Active Directory-Benutzer und -Computer, um die Verwaltungskonsole Active Directory-Benutzer und -Computer zu starten.
- 2. Klicken Sie mit der rechten Maustaste auf Ihren Domänennamen (in diesem Beispiel wireless.com), und wählen Sie dann im Kontextmenü die Option **Neu > Organisationseinheit**,

um eine neue Organisationseinheit zu erstellen.



 Weisen Sie dieser OU einen Namen zu, und klicken Sie auf OK.

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

Nachdem nun der neue OU **Idapuser** auf dem LDAP-Server erstellt wurde, besteht der nächste Schritt darin, user **user2** unter dieser OU zu erstellen. Gehen Sie wie folgt vor, um dieses Ziel zu erreichen:

 Klicken Sie mit der rechten Maustaste auf die neu erstellte Organisationseinheit. Wählen Sie Neu > Benutzer aus den sich ergebenden Kontextmenüs, um einen neuen Benutzer zu erstellen.



2. Füllen Sie auf der Seite für die Benutzereinrichtung die erforderlichen Felder aus, wie in diesem Beispiel gezeigt. In diesem Beispiel ist **user2** der Benutzername.Dies ist der Benutzername, der in der LDAP-Datenbank für die Authentifizierung des Clients überprüft wird. In diesem Beispiel wird **abcd** als Vorname und Nachname verwendet. Klicken Sie auf **Next** 

(Weiter).

New Object - User	×
Create in: Wireless.com/Idapuser	
Eirst name: abcd Initials:	
Last name:	
Full ngme: abcd	
Liser logon name:	
user2 @Wireless.com	
User logon name (pre- <u>W</u> indows 2000):	
WIRELESS\ user2	
< Back Next > Canc	el

3. Geben Sie ein Kennwort ein, und bestätigen Sie es. Wählen Sie die Option Kennwort läuft nie ab, und klicken Sie auf

Password:					
<u>C</u> onfirm pa	ssword:				_
□ User <u>m</u> □ U <u>s</u> erca	ust change annot chang	password a ge passwor	at next logon d		
Passwe	ord never ex	pires			

 Klicken Sie auf Beenden.Ein neuer Benutzer user2 wird unter der OU Idapuser erstellt. Die Benutzeranmeldeinformationen sind:Benutzername: user2Kennwort: Laptop123



Nachdem der Benutzer in einer Organisationseinheit erstellt wurde, besteht der nächste Schritt darin, diesen Benutzer für den LDAP-Zugriff zu konfigurieren.

## Konfigurieren des Benutzers für den LDAP-Zugriff

Führen Sie die Schritte in diesem Abschnitt aus, um einen Benutzer für den LDAP-Zugriff zu konfigurieren.

#### Aktivieren der Funktion für anonyme Bindung auf Windows 2003 Server

Damit Anwendungen von Drittanbietern über LDAP auf Windows 2003 AD zugreifen können, muss die Funktion "Anonyme Bindung" unter Windows 2003 aktiviert sein. Standardmäßig sind anonyme LDAP-Vorgänge auf Windows 2003-Domänencontrollern nicht zulässig.

Führen Sie die folgenden Schritte aus, um die Funktion für anonyme Bindung zu aktivieren:

- Starten Sie das ADSI Edit-Tool über Start > Ausführen > Typ: ADSI Edit.msc. Dieses Tool ist Teil der Windows 2003-Supporttools.
- Erweitern Sie im Fenster "ADSI Edit" die Stammdomäne (Configuration [tsweblapt.Wireless.com]).Erweitern Sie CN=Services > CN=Windows NT > CN=Directory Service. Klicken Sie mit der rechten Maustaste auf den Container CN=Directory Service, und wählen Sie Eigenschaften aus dem Kontextmenü aus.



3. Klicken Sie im Fenster CN=Directory Service Properties auf das dsHeuristics-Attribut im Feld Attribute, und wählen Sie Edit aus. Geben Sie im Fenster Zeichenfolgenattribut-Editor dieses Attributs den Wert 000002 ein, und klicken Sie auf Anwenden und OK. Die Funktion "Anonyme Bindung" ist auf dem Windows 2003-Server aktiviert.Hinweis: Das letzte (siebte) Zeichen steuert die Art der Anbindung an den LDAP-Dienst. "0" oder kein siebtes Zeichen bedeutet, dass anonyme LDAP-Vorgänge deaktiviert sind. Durch Festlegen des siebten Zeichens auf "2" wird die Funktion "Anonyme Bindung" aktiviert.

EN=Directory Service Pr	operties		? X		
Attribute Editor Security				Class	Distingu
Show mandatory attri	butes			container	CN=Qu
Show optional attribut	tes				
Show only attributes I	that have <u>v</u> alues				
Attributes:	_				
Attribute	Syntax	Value	▲		
directReports	String Attribut	e Editor			×
displayNamePrintable	Attribute: dSHe	euristics			
distinguishedName	Value				
dSCorePropagationD					
dSHeuristics	100000000		6		
extensionName flags	<u>C</u> lear			ок 丿	Cancel
fromEntry					
frsComputerReferenc	Distinguished	<not set=""></not>			
fSM0Bole0wper	Distinguished	<not set<="" td=""><td>-1</td><td></td><td></td></not>	-1		
1. Internet	Distinguished	the set			
Ean					
	ОК	Cancel	Apply		
				1	

**Hinweis:** Wenn dieses Attribut bereits einen Wert enthält, stellen Sie sicher, dass Sie nur das siebte Zeichen von links ändern. Dies ist das einzige Zeichen, das geändert werden muss, um anonyme Bindungen zu aktivieren. Wenn der aktuelle Wert beispielsweise "0010000" ist, müssen Sie ihn in "0010002" ändern. Wenn der aktuelle Wert weniger als sieben Zeichen enthält, müssen Sie an den nicht verwendeten Stellen Nullen eingeben: "001" wird zu "0010002".

#### ANONYMER ANMELDEZUGRIFF für Benutzer "user2"

Der nächste Schritt besteht darin, dem Benutzer **user2 ANONYME LOGON**-Zugriff zu gewähren. Gehen Sie wie folgt vor, um dieses Ziel zu erreichen:

- 1. Öffnen Sie Active Directory-Benutzer und -Computer.
- 2. Vergewissern Sie sich, dass Erweiterte Funktionen anzeigen aktiviert ist.
- 3. Navigieren Sie zum Benutzer user2, und klicken Sie mit der rechten Maustaste darauf. Wählen Sie im Kontextmenü die Option Eigenschaften aus. Dieser Benutzer ist mit dem Vornamen "abcd" gekennzeichnet.

🔄 🛛 🎫 🖬 Useri		
😑 📖 Users		
😰 Aqî	Conv	
⊂ ∈	Add to a group	
i i i i i i i i i i i i i i i i i i i	Modito a group	
😐 🚮 🔂 🖬	Name Mappings	
	Disable Account	
Dr 🛐 🕞	R <u>e</u> set Password	
Dr	Mo <u>v</u> e	
	<u>O</u> pen Home Page	
	Send M <u>a</u> il	
	Find	
	oll Talelia	
	All Tasks	-
E E E	View	•
🔅 🗇 🚮 🖓	New Window from Here	
📋 🗇 🌆 Gu		
	Cu <u>t</u>	
😐 🗠 🚾 🛛 🗠	Delete	
🕀 🖸 🔁 🖬	Rena <u>m</u> e	
🐑 💑 kr	Refresh	
🕵 R/	Export <u>L</u> ist	
🚮 Sd		
🛃 us	Properties	
	Help	
(	)	

4. Gehen Sie zu Sicherheit im abcd-

ca propercies			
Published Certificates	Member Of	Dial-in Obj	ject 🕻 Securit
Environment Session	is Remote control	Terminal Servic	es Profile CON
General Address	Account Prof	ile   Telephone:	Organization
🛃 abcd			
First name:	abed	Initials:	
Last name:			
Display name:	abcd		
Description:			
Office:	I		
<u>I</u> elephone number:	[		Other
E- <u>m</u> ail:			
∭eb page:			Othe <u>r</u>
	οκ	Cancel	Apply

- 5. Klicken Sie im resultierenden Fenster auf Hinzufügen.
- Geben Sie im Feld Geben Sie die zu verwendenden Objektnamen ein und bestätigen Sie den Dialog mit ANONYMER ANMELDUNG.

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	Check Names
La Advanced and	
Advanced	

7. In der ACL werden Sie feststellen, dass **ANONYME LOGON** Zugriff auf einige Eigenschaftensätze des Benutzers hat. Klicken Sie auf **OK**. Der ANONYME LOGON-Zugriff wird diesem Benutzer

gewährt. abcd Properties	2×
Environment   Sessions   Remote control   Terminal Servi General   Address   Account   Profile   Telephone Published Certificates   Member Of   Dial-in   Ot	ices Profile   COM+   es   Organization   bject Security
Group or user names:	
Account Operators (WIRELESS Account Operators Administrators (WIRELESS Administrators)	
ANONYMOUS LOGON	
Cert Publishers (WIRELESS\Cert Publishers)	-
A <u>d</u> d	<u>Remove</u>
Permissions for ANONYMOUS LOGON Allow	Deny
Full Control     Image: Control       Read     Image: Control       Write     Image: Control       Create All Child Objects     Image: Control       Delete All Child Objects     Image: Control       Allowed to Authenticate     Image: Control	
For special permissions or for advanced settings, click Advanced.	Adyanced
OK Cancel	

#### Erteilen der Inhaltsberechtigung für die Organisationseinheit

Der nächste Schritt besteht darin, der **ANONYMEN ANMELDUNG** in der Organisationseinheit, in der sich der Benutzer befindet, mindestens die Berechtigung **Inhalt** auflisten zu gewähren. In diesem Beispiel befindet sich "user2" in der OU "Idapuser". Gehen Sie wie folgt vor, um dieses Ziel zu erreichen:

1. Klicken Sie in Active Directory-Benutzer und -Computer mit der rechten Maustaste auf **OU** Idapuser, und wählen Sie Eigenschaften



2. Klicken Sie auf **Sicherheit** und dann auf **Erweitert**.

lapuser Properties			?>
General   Managed By   Object   Security   C	OM+ Group	Policy	
Group or user names:			
Account Operators (WIRELESS Accou	int Operators)		-
Administrators (WIRELESS Administrato	ors)		
Authenticated Users			
🗾 👧 Domain Admins (WIRELESS\Domain A	dmins)		
Enterprise Admins (WIRELESS\Enterpri	ise Admins)		-1
			<u> </u>
	Add	Bemove	•
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 settin click Advanced.	igs,	Advance	a
ОК	Cancel	Ap	ele

3. Klicken Sie auf **Hinzufügen**. Geben Sie im daraufhin angezeigten Dialogfeld **ANONYME LOGON** (ANONYME **ANMELDUNG**) ein.

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. Bestätigen Sie den Dialog. Daraufhin wird ein neues Dialogfeld geöffnet.
- 5. Wählen Sie im Dropdown-Feld **Übernehmen auf** die Option **Nur dieses Objekt aus,** und aktivieren Sie das Kontrollkästchen **Inhalt** zulassen.

Permission Entry for Idapuser		<u>?</u> ×	1
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 Create All Child Objects			
	οк	Cancel	1

## Verwenden von LDP zum Identifizieren der Benutzerattribute

Bei diesem GUI-Tool handelt es sich um einen LDAP-Client, mit dem Benutzer Vorgänge (z. B. Verbinden, Binden, Suchen, Ändern, Hinzufügen, Löschen) in einem beliebigen LDAPkompatiblen Verzeichnis (z. B. Active Directory) durchführen können. LDP wird verwendet, um in Active Directory gespeicherte Objekte zusammen mit deren Metadaten anzuzeigen, z. B. Sicherheitsbeschreibungen und Replikationsmetadaten.

Das LDP GUI-Tool ist enthalten, wenn Sie die Windows Server 2003 Support Tools von der Produkt-CD installieren. In diesem Abschnitt wird erläutert, wie Sie mit dem LDP-Dienstprogramm die spezifischen Attribute identifizieren, die dem Benutzer **user2** zugeordnet sind. Einige dieser Attribute werden verwendet, um die LDAP-Serverkonfigurationsparameter für den WLC auszufüllen, z. B. Benutzerattribut-Typ und Benutzerobjekttyp.

- 1. Klicken Sie auf dem Windows 2003-Server (selbst auf demselben LDAP-Server) auf **Start > Ausführen**, und geben Sie **LDP ein**, um auf den LDP-Browser zuzugreifen.
- Klicken Sie im LDP-Hauptfenster auf Connection > Connect (Verbindung > Verbinden), und stellen Sie eine Verbindung mit dem LDAP-Server her, indem Sie die IP-Adresse des LDAP-Servers eingeben.

Here Ldp	
Connection Browse View Options Utilities	Help
Connect       Bind       Opsconnect       New       Corl+N       Save       Save &s	*
Brint Print Prevjew Print Setup	
Connect to specified server	

3. Wenn Sie mit dem LDAP-Server verbunden sind, wählen Sie im Hauptmenü die Option **Ansicht** aus, und klicken Sie auf

Daum.		
Lap://tsweb-lapt.Wireless.com/CC=Wireless,DC=com		_ 🗆 X
Connection Browse View Options Utilities		Help
Iree     Ctrl+T       Enterprise Configuration       ✓ Status Bar       Set Font	<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; 1.2.840.113556.1.4.1339; 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; 1.2.840.113556.1.4.1504; 1.2.840.113556.1.4.1948; 2.2.840.113556.1.4.802; 1.2.840.113556.1.4.1907; 1.2.840.113556.1.4.1948; 2.2.8upportedLDAPVersion; 3; 2; 1.2.840.113556.1.4.802; 1.2.840.113556.1.4.1907; 1.2.840.113556.1.4.1948; 2.2.8upportedLDAPVersion; 3; 2; 1.2.8upportedLDAPVersion; MaxConnections; MaxConnldleTime; MaxPageSize; MaxQueryOuration; MaxTempTableSize; MaxResultSetSize; MaxNotificationPerConn; MaxValRange; 1.2.8upportedSASLMechanisms: GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5; 1.2.8upportedSASLMechanisms: GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5; 1.2.8upportedSASLMechanisms: GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5; 1.2.8upportedSasLMechanisms: GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5; 1.3.8upportedCapabilities: 1.2.840.113556.1.4.800; 1.2.840.113556.1.4. 1.2.840.113556.1.4.1791; 1.3.8upportedCapabilities: 1.2.840.113556.1.4.800; 1.2.840.113556.1.4. 1.2.840.113556.1.4.1791; 1.3.8iglobalCatalogReady; TRUE; 1.3.8iglobalCatalogReady; TRUE; 1.4.8iglobalCa</pre>	*ation 1670;
		1

 Geben Sie im resultierenden Fenster Baumansicht die Basis-DN des Benutzers ein. In diesem Beispiel befindet sich user2 unter der OU "Idapuser" unter der Domäne Wireless.com. Daher ist die BaseDN für Benutzer2 OU=Idapuser, dc=wireless, dc=com. Klicken Sie auf OK.

Midap://tsweb-lapt.Wireless.com/DE=Wireless.DE=com		. 0 ×
Connection Browse View Options Utilities		Help
Tree View BaseDN: DU-Idaguser.do-wireless.do-com Cancel	X I3556.1.4.473; 1.2.840.113556.1.4.528; 1.2.840.113556.1.4.417; I3556.1.4.619; 1.2.840.113556.1.4.521; 1.2.840.113556.1.4.970; I3556.1.4.805; 1.2.840.113556.1.4.521; 1.2.840.113556.1.4.1339; I3556.1.4.1338; 1.2.840.113556.1.4.1413; 2.16.840.1.113556.1.4.1339; I3556.1.4.1340; 1.2.840.113556.1.4.1413; 2.16.840.1.13556.1.4.1852; I3556.1.4.802; 1.2.840.113556.1.4.1907; 1.2.840.113556.1.4.1948; 2> supportedLDAPVersion: 3; 2; I2> supportedLDAPVersion: 3, 2; I2> supportedCommittedUSN: 16926; I2> domsinState: 5, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,	uration 1.1670;
Ready		1.

5. Auf der linken Seite des LDP-Browsers wird der gesamte Tree angezeigt, der unter der angegebenen BaseDN angezeigt wird (OU=Idapuser, dc=wireless, dc=com). Erweitern Sie die Struktur, um den Benutzer user2 zu suchen. Dieser Benutzer kann mit dem CN-Wert identifiziert werden, der den Vornamen des Benutzers darstellt. In diesem Beispiel ist es CN=abcd. Doppelklicken Sie auf CN=abcd. Im rechten Fensterbereich des LDP-Browsers zeigt LDP alle mit user2 verknüpften Attribute an. In diesem Beispiel wird dieser Schritt erläutert:



Beachten Sie in diesem Beispiel die eingekreisten Felder rechts.

- 6. Wie im Abschnitt <u>WLC mit LDAP-Serverdetails konfigurieren</u> dieses Dokuments erwähnt, geben Sie im Feld **Benutzerattribut** den Namen des Attributs in den Benutzerdatensatz ein, der den Benutzernamen enthält. Aus dieser LDP-Ausgabe geht hervor, dass **sAMAccountName** ein Attribut ist, das den Benutzernamen "user2" enthält. Geben Sie daher das **sAMAccountName**-Attribut ein, das dem Feld **User Attribute** des WLC entspricht.
- 7. Geben Sie im Feld User Object Type (Benutzerobjekttyp) den Wert des LDAP objectType-Attributs ein, das den Datensatz als Benutzer identifiziert. Benutzerdatensätze verfügen häufig über mehrere Werte für das objectType-Attribut, von denen einige für den Benutzer eindeutig sind und von denen einige für andere Objekttypen freigegeben sind. In der LDP-Ausgabe ist CN=Person ein Wert, der den Datensatz als Benutzer identifiziert. Geben Sie daher Person als Attribut User Object Type auf dem WLC an.

## Wireless-Client konfigurieren

Der letzte Schritt besteht darin, den Wireless-Client für die EAP-FAST-Authentifizierung mit Clientund Serverzertifikaten zu konfigurieren. Gehen Sie wie folgt vor, um dieses Ziel zu erreichen:

 Starten Sie das Cisco Aironet Desktop Utility (ADU). Klicken Sie im ADU-Hauptfenster auf Profile Management > New (Profilverwaltung > Neu), um ein neues Wireless-Clientprofil zu erstellen.

🗃 Cisco Aironet Desktop Uti	lity - Current Profile: sdreteretet	? 🛛
Action Options Help		
Current Status Profile Manageme	ent 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>	Soon
Network Name 3 (SSID3):	<empty></empty>	Scart
Auto Select Profiles		Order Profiles

2. Geben Sie einen Profilnamen an, und weisen Sie diesem Profil einen SSID-Namen zu. Dieser SSID-Name muss mit dem Namen identisch sein, der auf dem WLC konfiguriert wurde. In diesem Beispiel lautet der SSID-Name

eneral Security Advance	ed	
Profile Settings		
Profile Name:	Idapuser	
Client Name:	CLIENT1	]
Network Names		
SSIDT	Idap	S. S. S. S. S. S.
SSID2:		
SSID3:		
		,

- 3. Klicken Sie auf die Registerkarte **"Sicherheit**", und wählen Sie **802.1x/EAP** als Layer-2-Sicherheit aus. Wählen Sie **EAP-FAST** als EAP-Methode aus, und klicken Sie auf **Konfigurieren**.
- 4. Wählen Sie auf der EAP-FAST-Konfigurationsseite im Dropdown-Feld "EAP-FAST Authentication Method" die Option **TLS Client Certificate** aus, und klicken Sie auf **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	_
	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	
	DK Cancel

5. Im Konfigurationsfenster für das TLS-Client-Zertifikat:Aktivieren Sie das Kontrollkästchen Serveridentität validieren, und wählen Sie das auf dem Client installierte Zertifizierungsstellenzertifikat (wie im Abschnitt <u>Generate the Root CA certificate for the</u> <u>Client</u> in diesem Dokument erläutert) als vertrauenswürdige Stammzertifizierungsstelle aus.Wählen Sie das auf dem Client installierte Gerätezertifikat (wie im Abschnitt <u>Generate a</u> <u>Device Certificate for the Client (Gerätezertifikat für den Client generieren) in</u> diesem Dokument erläutert) als Clientzertifikat aus.Klicken Sie auf OK.In diesem Beispiel wird dieser Schritt erläutert<sup>-</sup>

onfigure TLS Client Certificate	? D
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	
	UK Cancel

Das Profil des Wireless-Clients wird erstellt.

# <u>Überprüfung</u>

Führen Sie diese Schritte aus, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

- 1. Aktivieren Sie die LDAP-SSID auf der ADU.
- Klicken Sie in den nächsten Fenstern auf Ja oder OK. Sie sollten in der Lage sein, alle Schritte der Client-Authentifizierung sowie die Zuordnung zu sehen, um erfolgreich auf der ADU zu sein.

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert. Verwenden des WLC-CLI-Modus

 Um zu überprüfen, ob WLC mit dem LDAP-Server kommunizieren und den Benutzer finden kann, geben Sie den Befehl debug aaap Idap enable in der WLC-CLI ein. In diesem Beispiel wird ein erfolgreicher Kommunikations-LDAP-Prozess beschrieben:Hinweis: Einige der Ausgaben in diesem Abschnitt wurden aus Platzgründen in zweite Zeilen verschoben.(Cisco Controller) >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
```

Aus den hervorgehobenen Informationen in dieser Debugausgabe geht eindeutig hervor, dass der LDAP-Server vom WLC mit den auf dem WLC angegebenen Benutzerattributen abgefragt wird und der LDAP-Prozess erfolgreich ist.

 Um zu überprüfen, ob die lokale EAP-Authentifizierung erfolgreich ist, geben Sie den Befehl debug aaa local-auth eap method events enable aus der WLC-CLI an. Hier ein Beispiel:(Cisco Controller) >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
```

(436973636£00000000000000000000)

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) • Der Befehl debug aaa local-auth db enable ist ebenfalls sehr nützlich. Hier ein Beispiel:(Cisco Controller) >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

 Um die im WLC installierten Zertifikate anzuzeigen, die f
ür die lokale Authentifizierung verwendet werden sollen, geben Sie den Befehl show local-auth Certificates (Zertifikate f
ür lokale Authentifizierung anzeigen) in der WLC-CLI ein. Hier ein Beispiel:(Cisco Controller)
 >Zertifikate f
ür lokale Authentifizierung anzeigen

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: 0=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: 0=Cisco Systems, CN=Cisco Manufacturing CA Issuer: 0=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.

 Um die Konfiguration der lokalen Authentifizierung auf dem WLC über den CLI-Modus anzuzeigen, geben Sie den Befehl show local-auth config ein. Hier ein Beispiel:(Cisco

#### Controller) >Konfiguration für lokale Authentifizierung anzeigen

User credentials database search order:

Primary ..... LDAP

#### Timer:

Active timeou	t	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

## **Fehlerbehebung**

Sie können die folgenden Befehle verwenden, um Probleme mit Ihrer Konfiguration zu beheben:

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

# Zugehörige Informationen

- EAP-FAST-Authentifizierung mit Wireless LAN-Controllern und Konfigurationsbeispiel eines externen RADIUS-Servers
- PEAP unter Unified Wireless Networks mit Microsoft Internet Authentication Service (IAS)
- Dynamische VLAN-Zuordnung mit WLCs basierend auf ACS zu Active Directory -Konfigurationsbeispiel für die Gruppenzuordnung
- <u>Konfigurationsanleitung für den Cisco Wireless LAN Controller Konfigurieren von</u> <u>Sicherheitslösungen</u>
- Konfigurationsanleitung für den Cisco Wireless LAN Controller Verwalten von Controller-Software und -Konfigurationen
- EAP-Authentifizierung mit WLAN-Controllern (WLC) Konfigurationsbeispiel
- Wireless LAN Controller (WLC) Design und Funktionen Häufig gestellte Fragen
- <u>Cisco Secure Services Client mit EAP-FAST-Authentifizierung</u>
- <u>Wireless LAN Controller (WLC) Häufig gestellte Fragen</u>
- <u>Controller Wireless LAN Controller (WLC) Fehler und Systemmeldungen FAQ</u>
- <u>Technischer Support und Dokumentation für Cisco Systeme</u>

#### Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.