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

## Inhalt



## 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 Cisco Technical Tips Conventions (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.

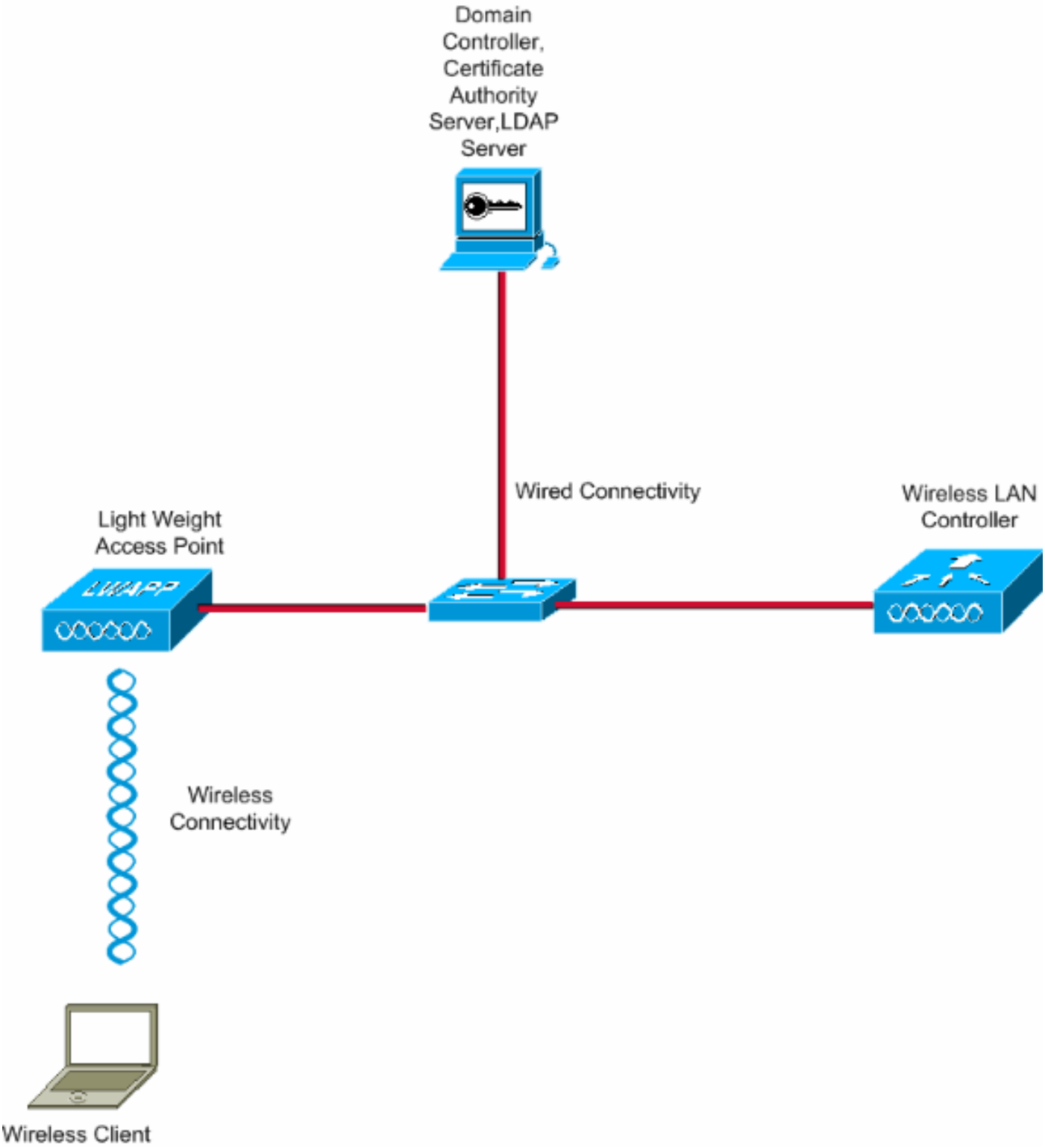
Die Benutzeranmeldeinformationen werden im LDAP-Server gespeichert, sodass der Controller bei erfolgreicher Zertifikatsvalidierung den LDAP-Server abfragt, um die Benutzeranmeldeinformationen abzurufen, und den Wireless-Client authentifiziert.

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
- Wireless-Client konfigurieren

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

Wie bereits erwähnt, verwendet dieses Dokument EAP-FAST mit Zertifikaten sowohl auf Client- als 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.

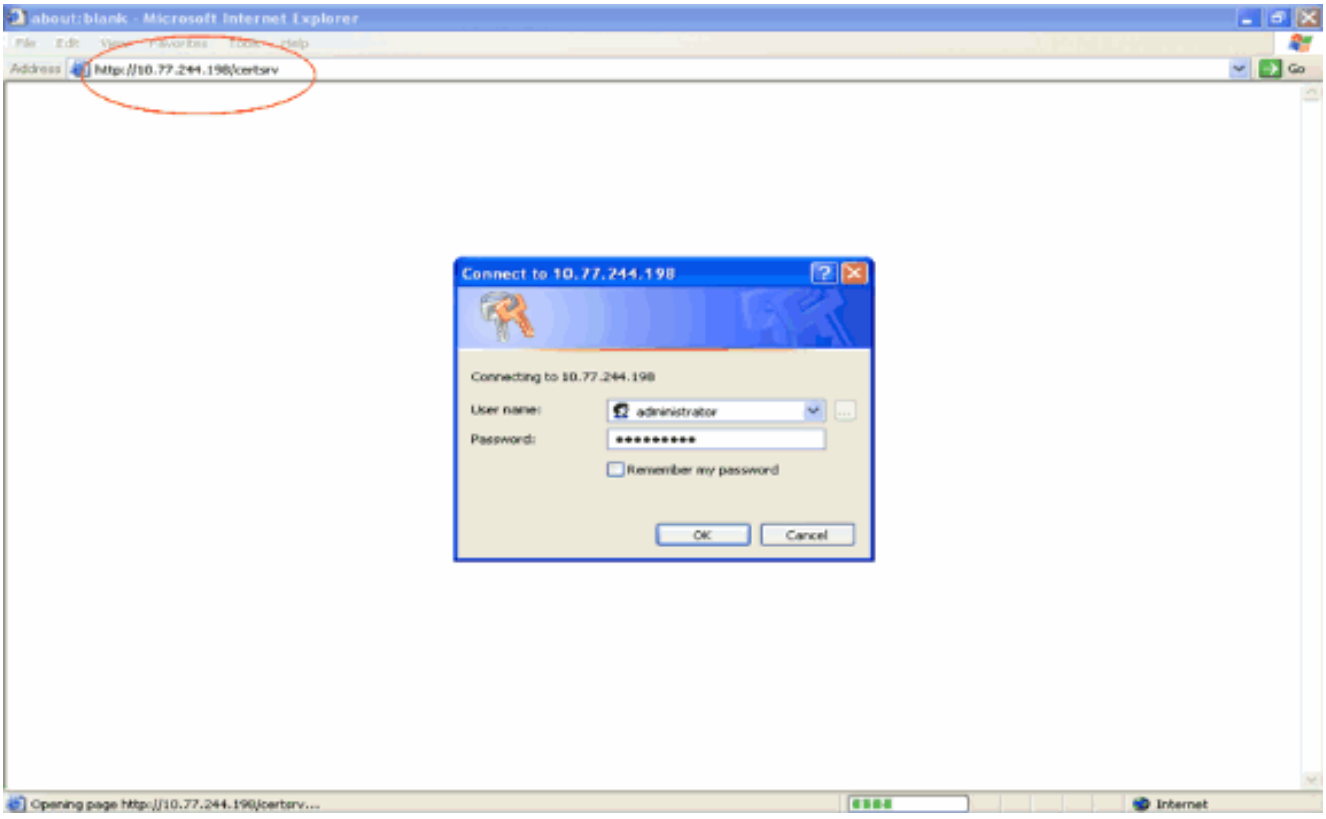
Der WLC und der Client benötigen jeweils diese Zertifikate, um vom CA-Server heruntergeladen zu werden:

- 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

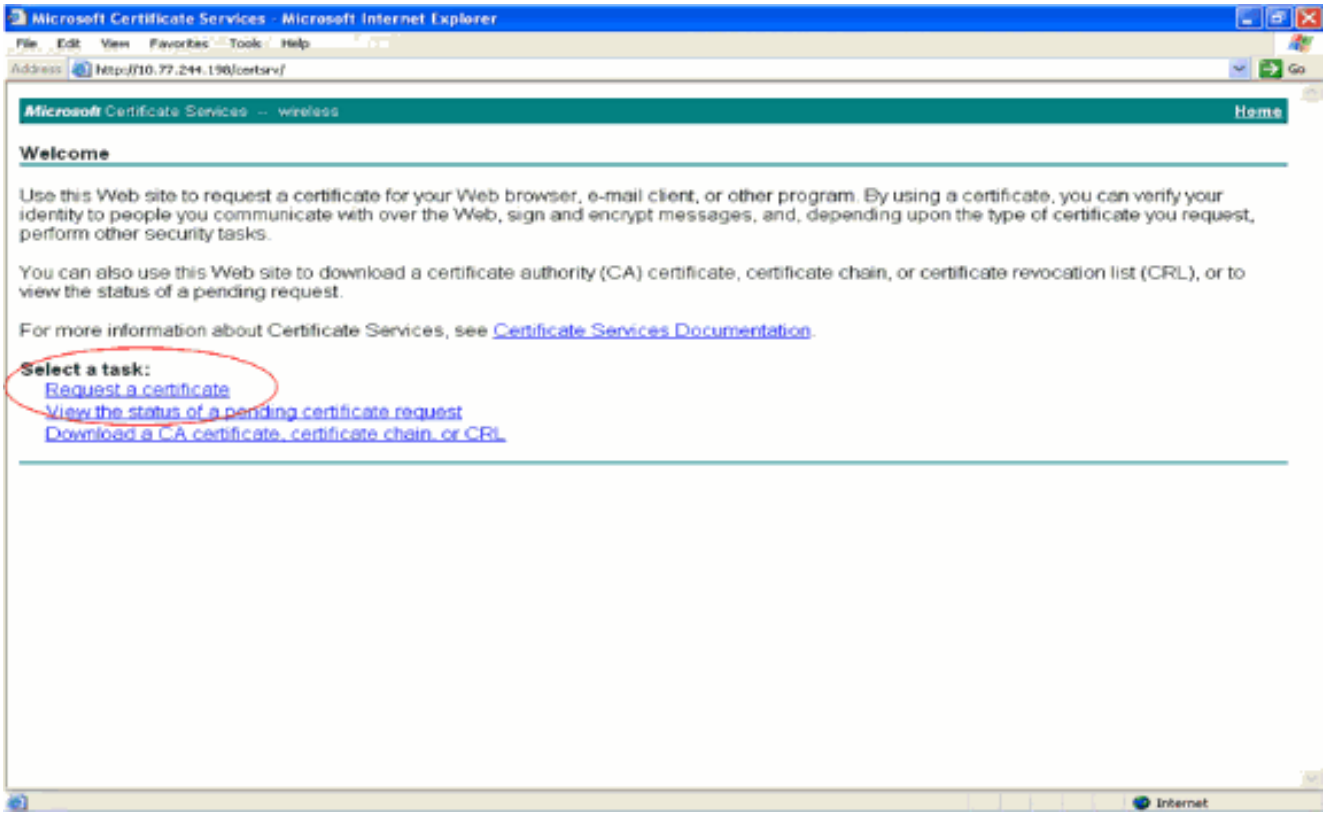
## Generieren eines Gerätezertifikats für den WLC

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.

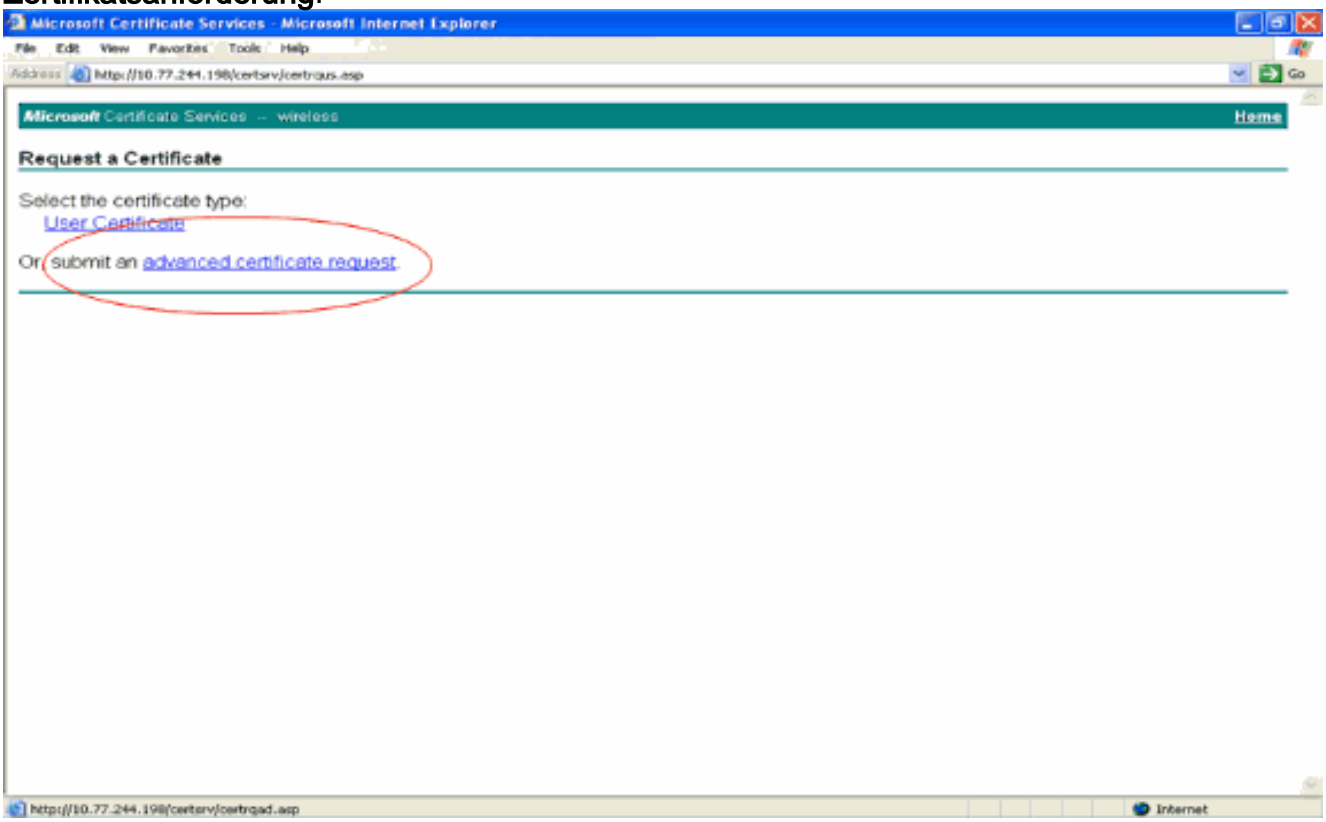
1. Gehen Sie zu **http://<IP-Adresse des CA-Servers>/certsrv** von Ihrem PC, der eine Netzwerkverbindung zum CA-Server hat. Melden Sie sich als Administrator des Zertifizierungsstellenservers an.



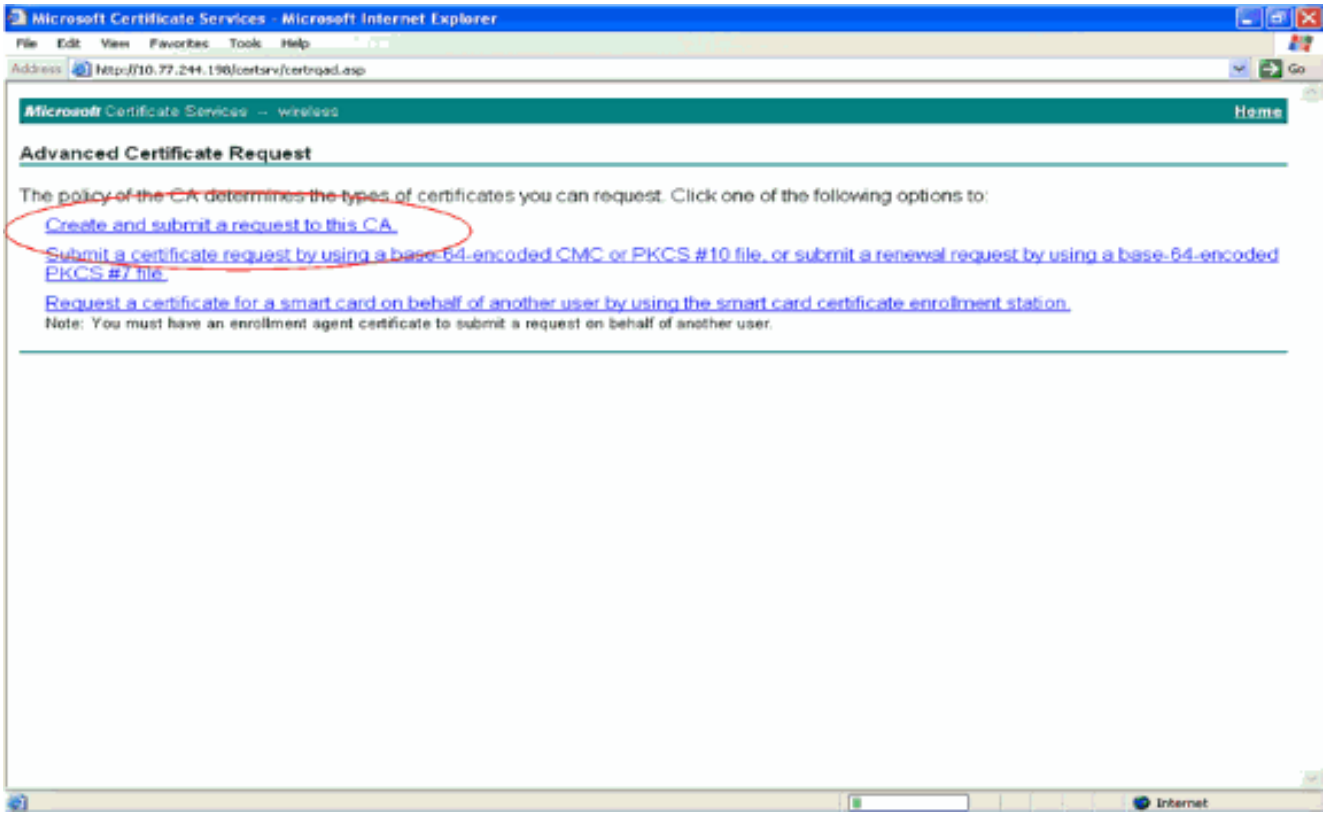

2. Wählen Sie **Zertifikat anfordern aus**.



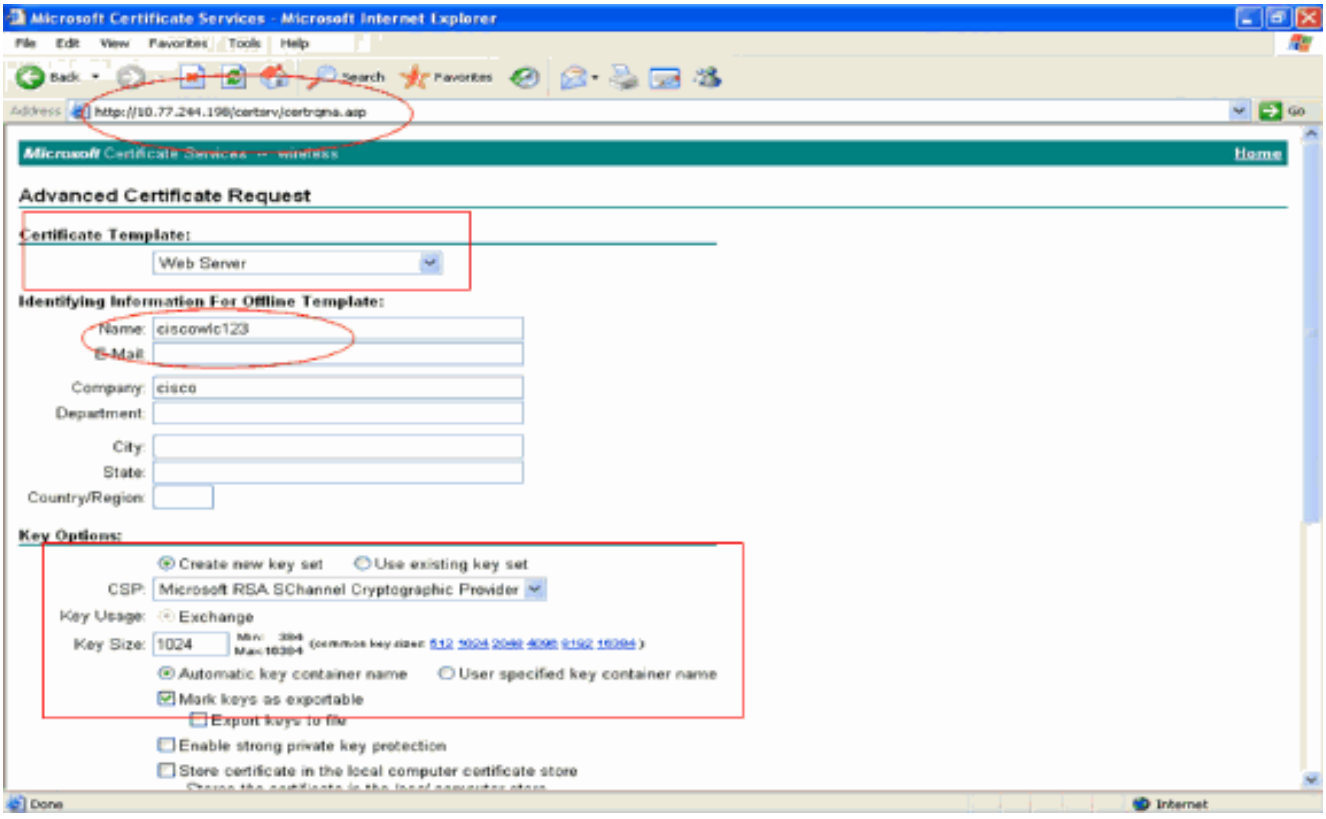

3. Klicken Sie auf der Seite Zertifikat anfordern auf **Erweiterte Zertifikatsanforderung**.



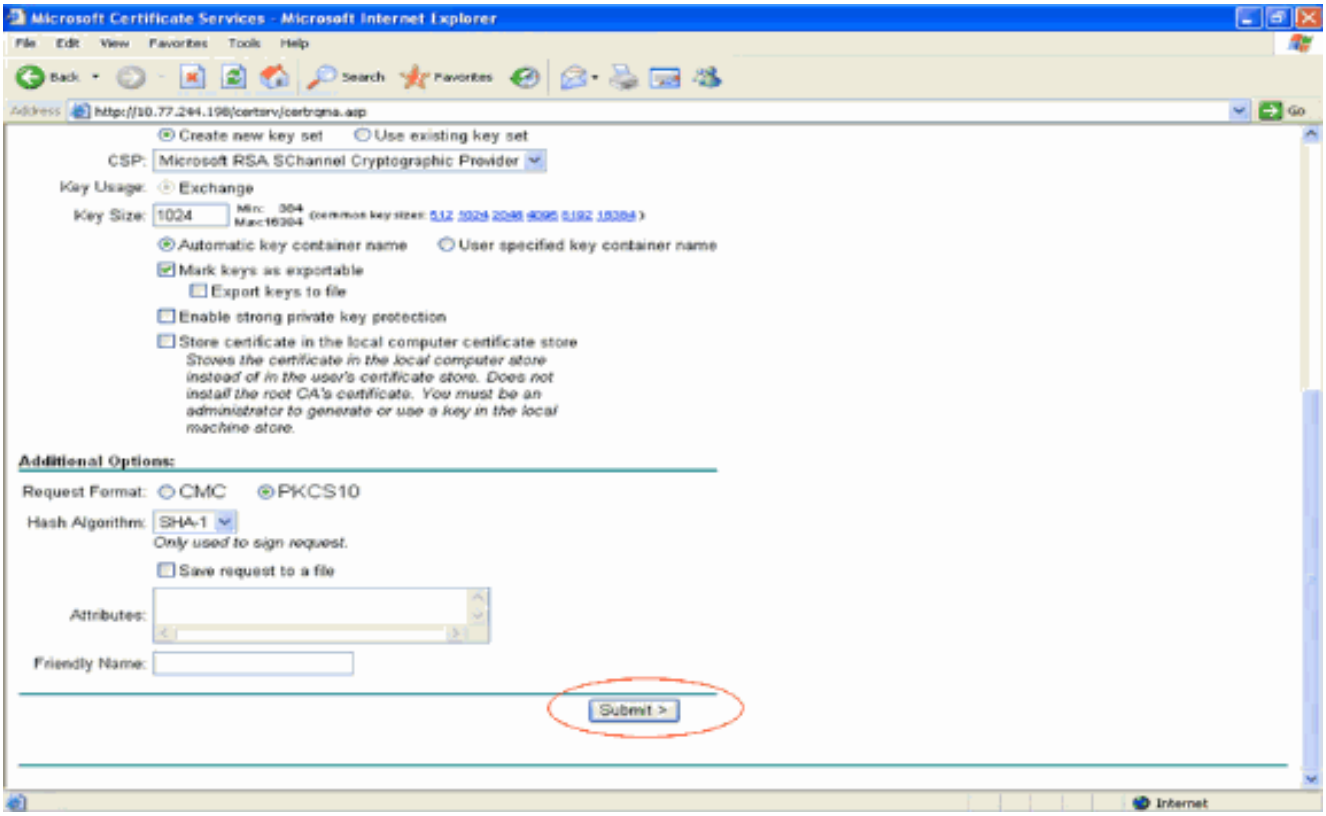

4. Klicken Sie auf der Seite "Erweiterte Zertifikatanforderung" auf **Erstellen, und senden Sie eine Anforderung an diese Zertifizierungsstelle**. Dadurch gelangen Sie zum Anforderungsformular für Advanced-Zertifikate.




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.

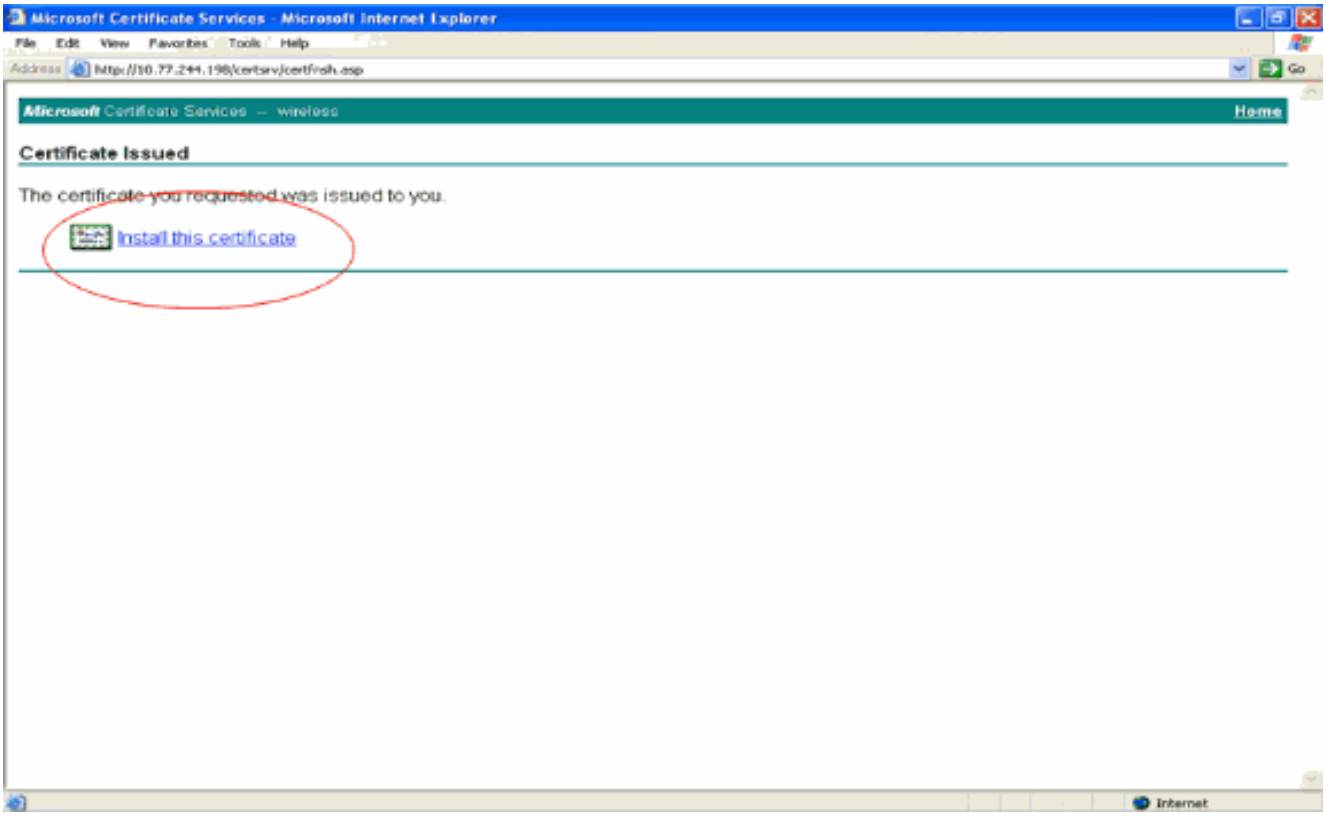


7. Konfigurieren Sie alle anderen erforderlichen Felder, und klicken Sie auf **Senden**.

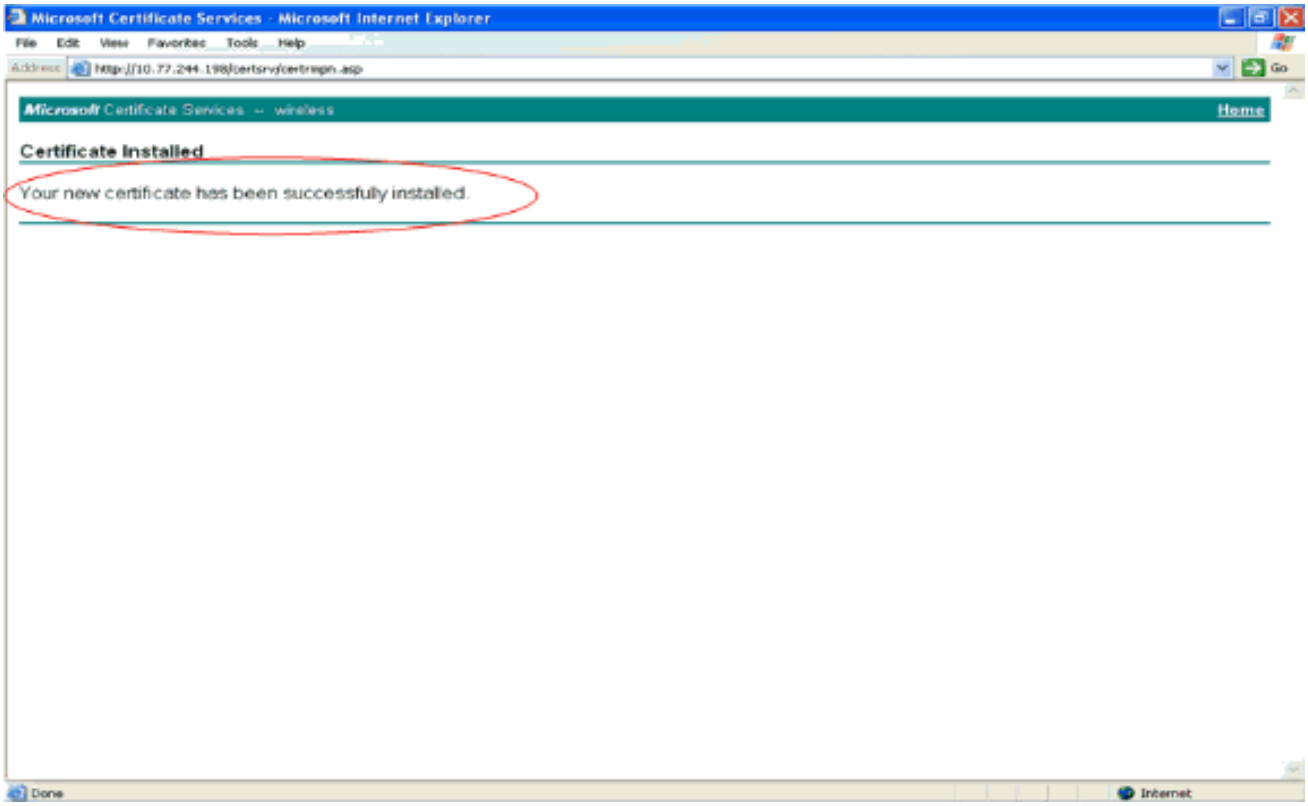



8. Klicken Sie im nächsten Fenster auf **Ja**, um den Zertifikatanforderungsprozess zu ermöglichen.

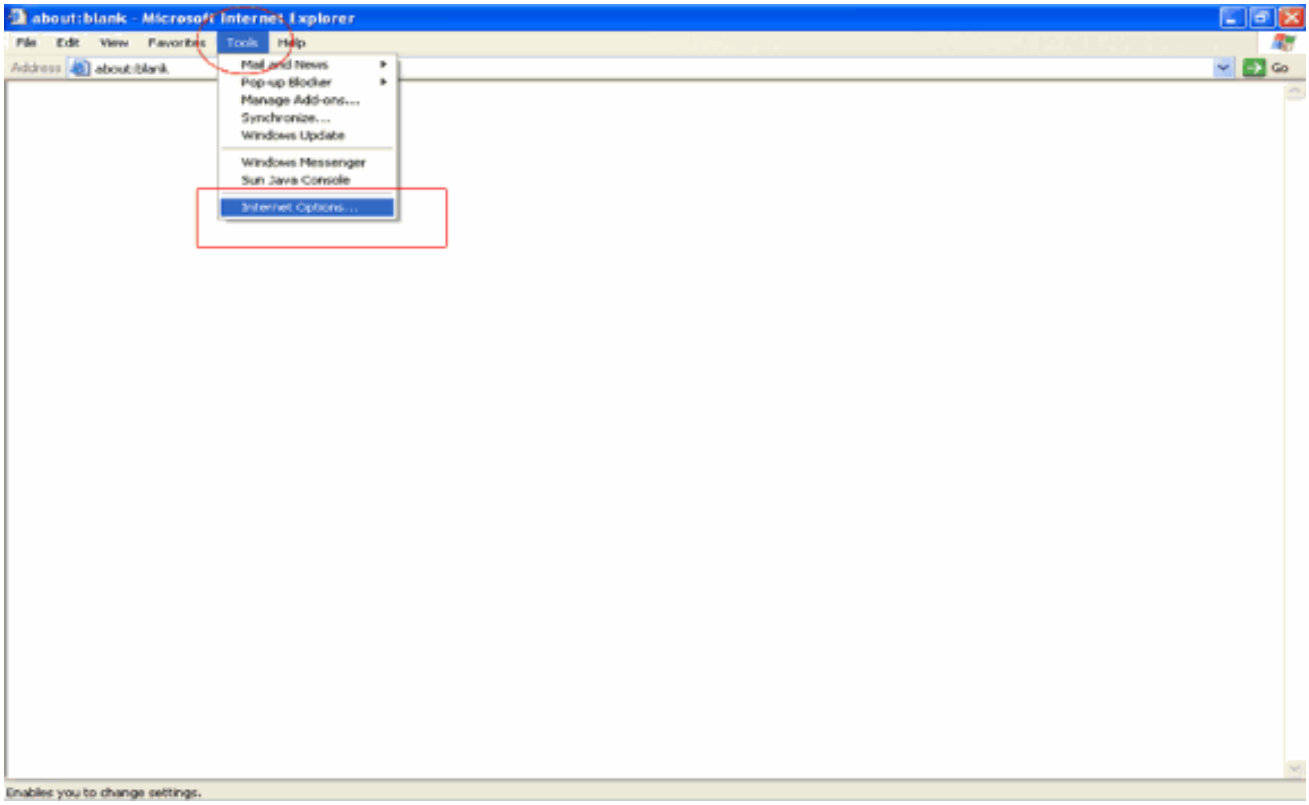

9. Das Fenster Certificate Issued (Von Zertifikat ausgestellt) wird angezeigt, das auf einen erfolgreichen Zertifikatanforderungsprozess hinweist. Der nächste Schritt besteht darin, das ausgestellte Zertifikat im Zertifikatspeicher dieses PCs zu installieren. Klicken Sie auf **Dieses Zertifikat installieren**.



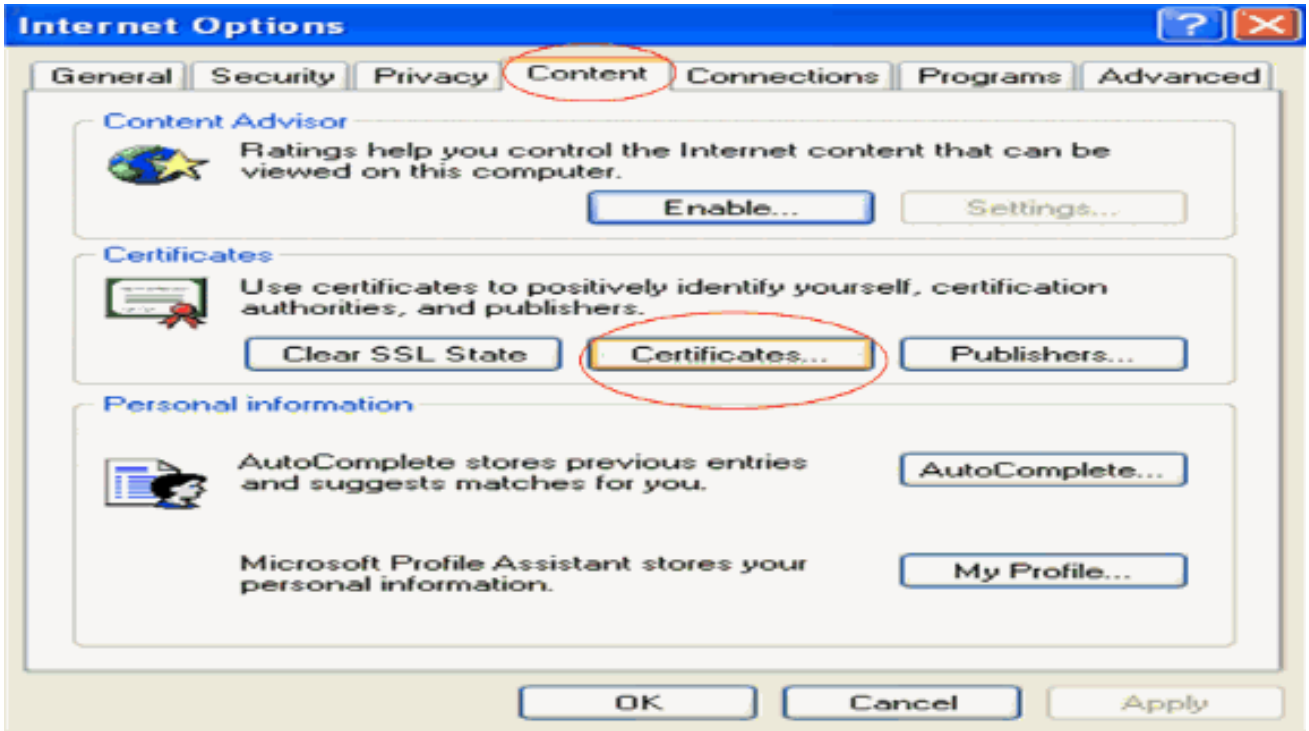

10. Das neue Zertifikat wird erfolgreich auf dem PC installiert, von dem aus die Anforderung an den Zertifizierungsstellenserver generiert wird.



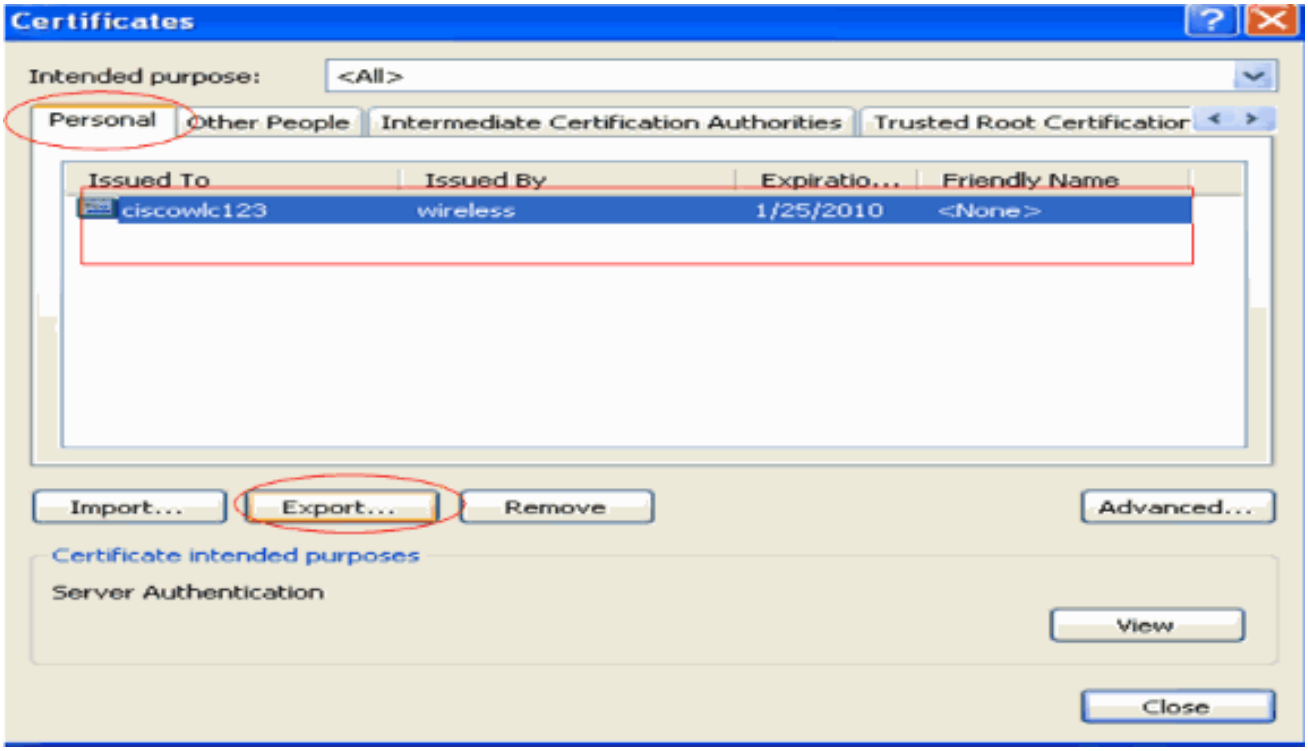

11. Der nächste Schritt besteht darin, dieses Zertifikat aus dem Zertifikatsspeicher als Datei auf die Festplatte zu exportieren. Diese Zertifikatsdatei wird später verwendet, um das Zertifikat auf den WLC herunterzuladen.Um das Zertifikat aus dem Zertifikatspeicher zu exportieren, öffnen Sie den Internet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




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

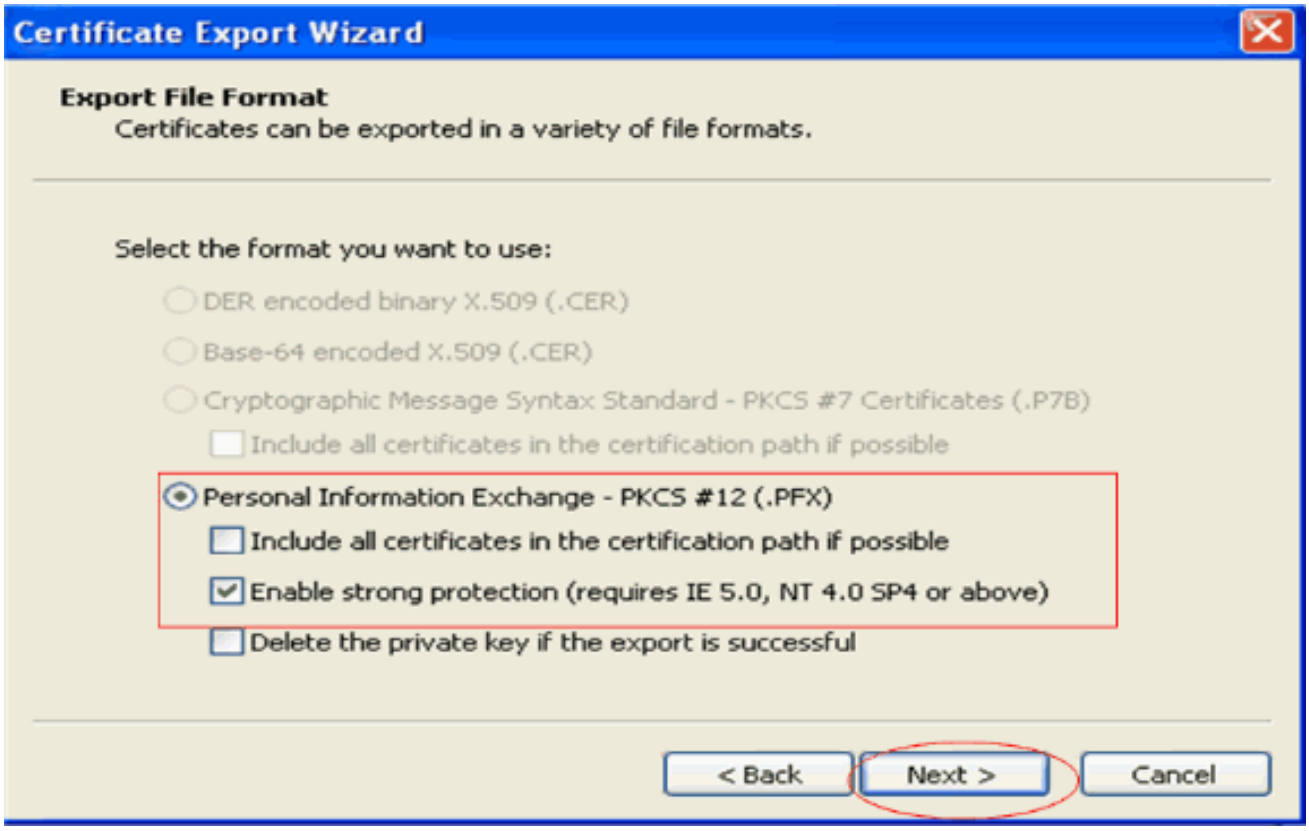



13. Die Gerätezertifikate werden in der Regel in der Liste **Persönliche** Zertifikate installiert. Hier sollte das neu installierte Zertifikat angezeigt werden. Wählen Sie das Zertifikat aus, und klicken Sie auf
**Exportieren**.

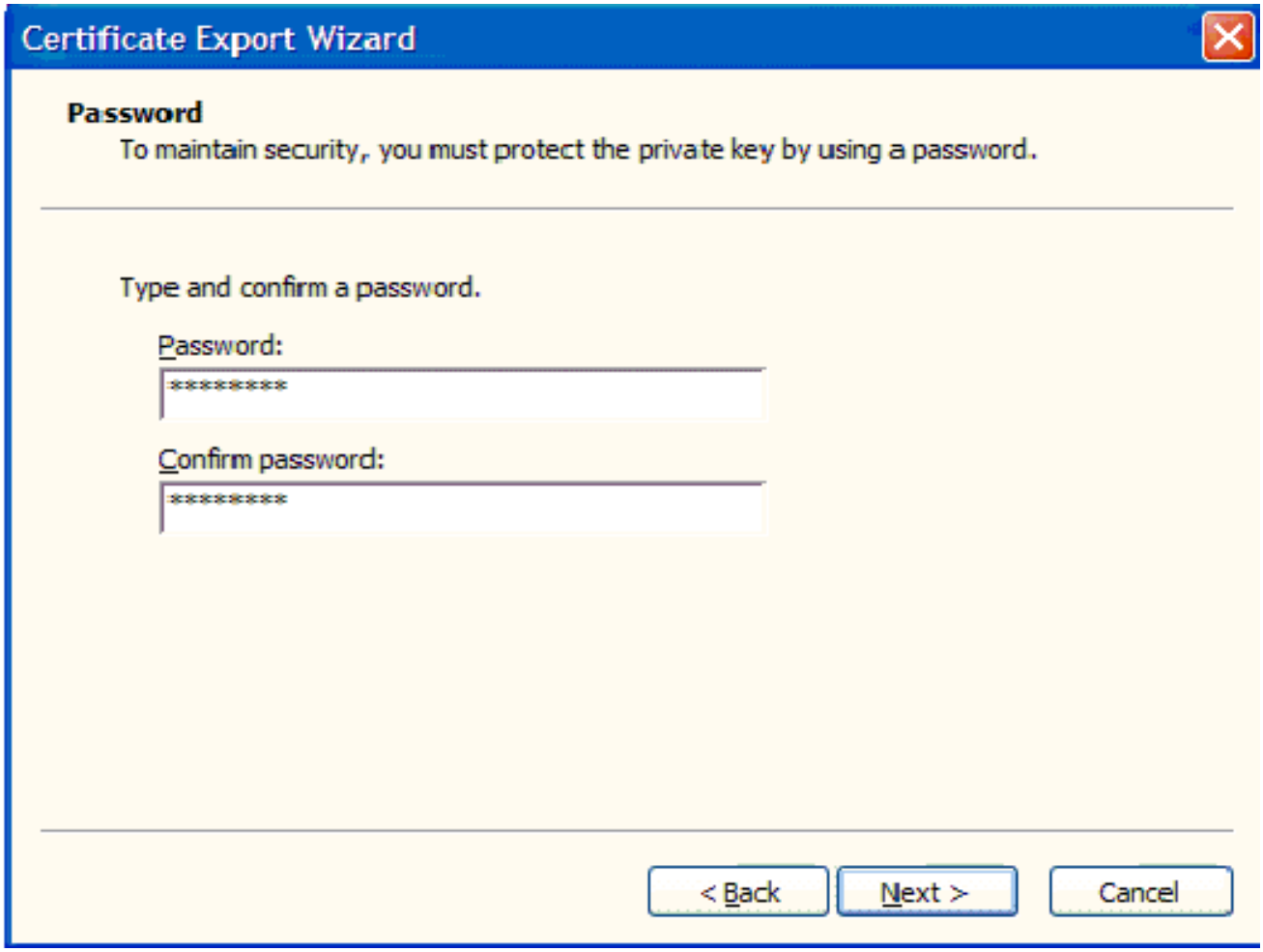



14. Klicken Sie in den folgenden Fenstern auf **Weiter**. Wählen Sie im Fenster des **Zertifikats-Export-Assistenten** die Option **Ja, privaten Schlüssel exportieren** aus. Klicken Sie auf **Next** (Weiter).


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

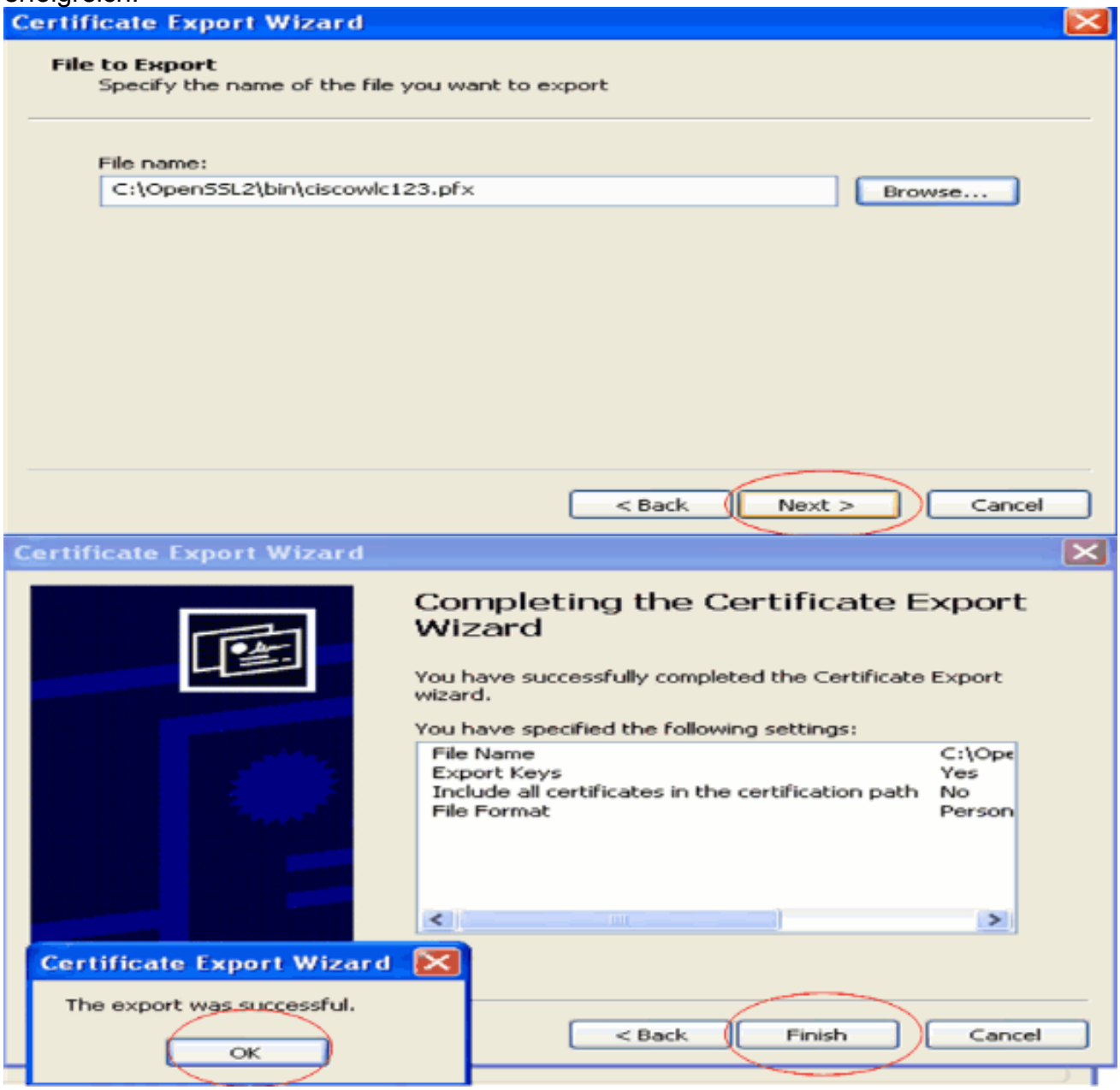



16. Geben Sie im Fenster Password (Kennwort) ein Kennwort ein. In diesem Beispiel wird **cisco** als Kennwort
verwendet.




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

erfolgreich.




## 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.

```
openssl>pkcs12 -in ciscowlc123.pfx -out ciscowlc123.pem
```

```
!--- 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.

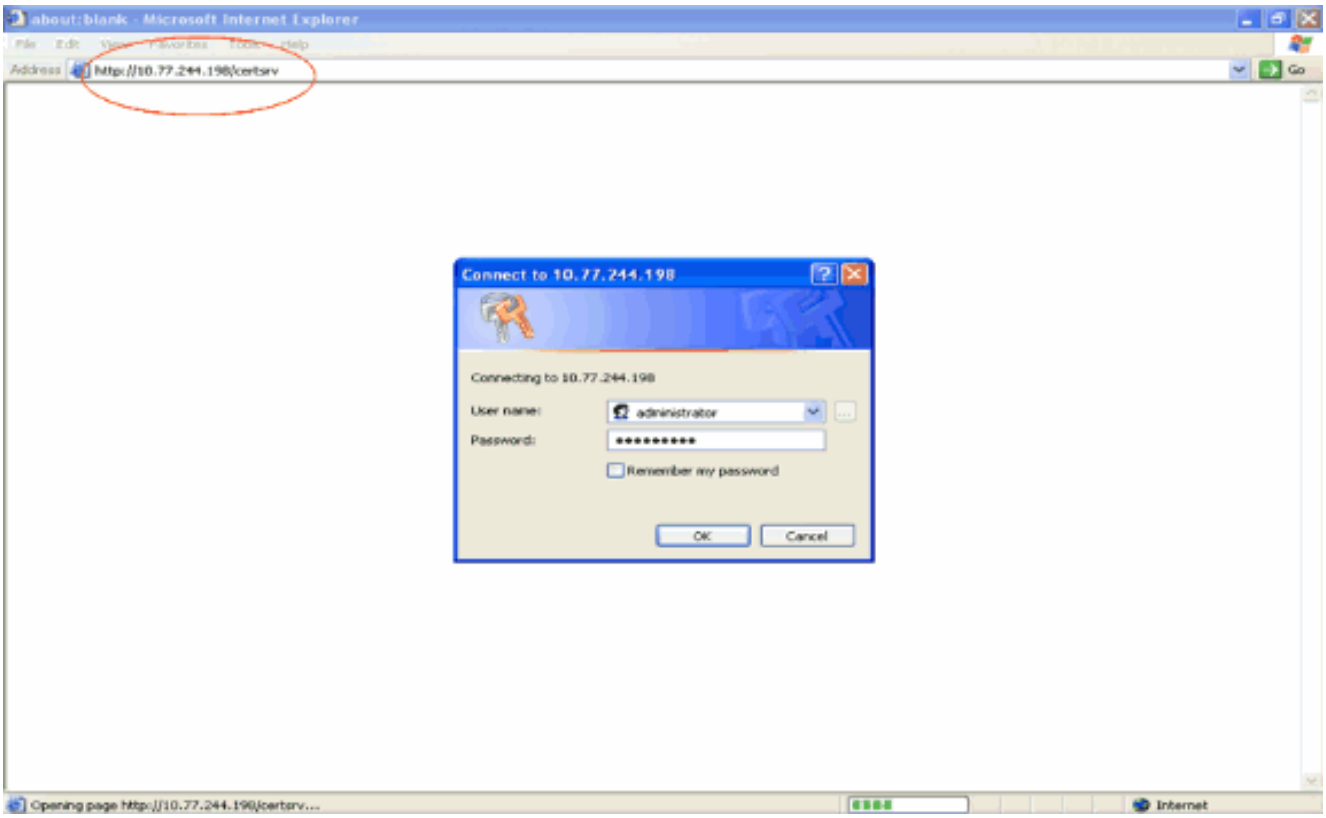
1. Melden Sie sich an der CLI des Controllers an.
2. Geben Sie den Befehl **transfer download datatype eapdevcert** ein.
3. Geben Sie den Befehl **transfer download serverip** ***10.77.244.196 ein***.10.77.244.196 ist die IP-Adresse des TFTP-Servers.
4. Geben Sie den Befehl **transfer download file name** ***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..................................... TFTP
   Data Type................................ Vendor Dev Cert
   TFTP Server IP........................... 10.77.244.196
   TFTP Packet Timeout...................... 6
   TFTP Max Retries......................... 10
   TFTP Path.....................................
   TFTP 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

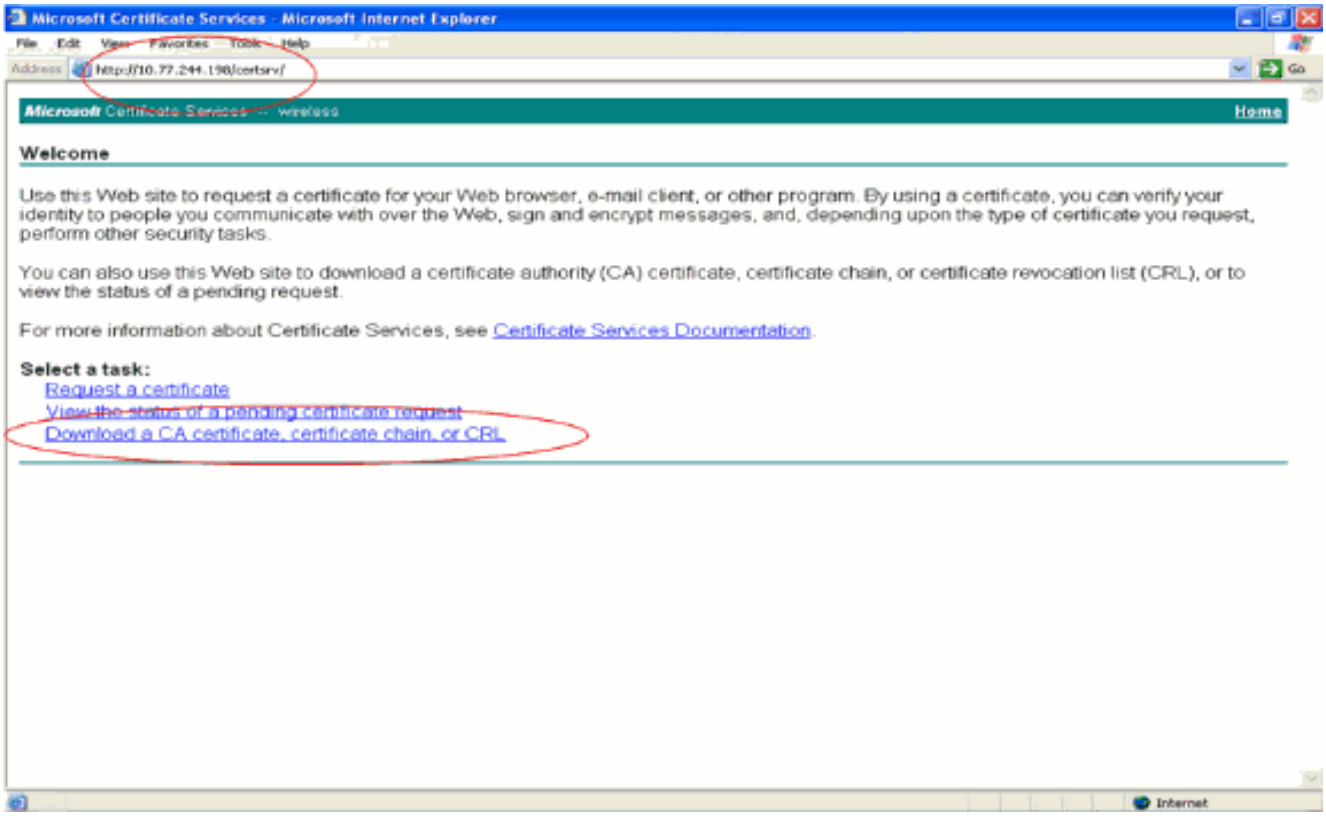
Nachdem nun das Gerätezertifikat im WLC installiert ist, besteht der nächste Schritt darin, das

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

1. 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.

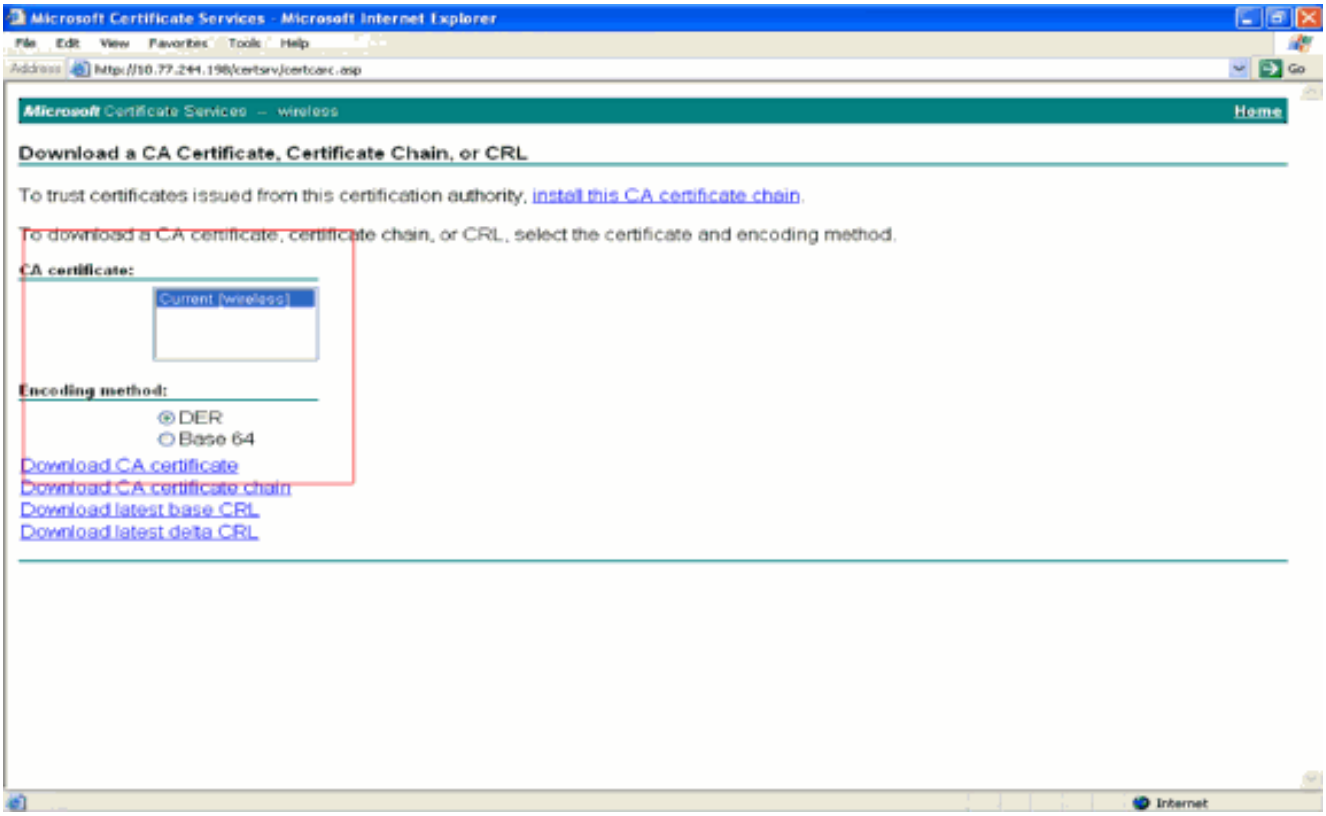



2. Klicken Sie auf **Zertifizierungsstellenzertifikat, Zertifikatskette oder Zertifikatsperrliste herunterladen**.




3. Auf der Ergebnisseite werden die aktuellen Zertifizierungsstellenzertifikate angezeigt, die auf dem Zertifizierungsstellenserver im Feld für das **Zertifizierungsstellenzertifikat** verfügbar sind.

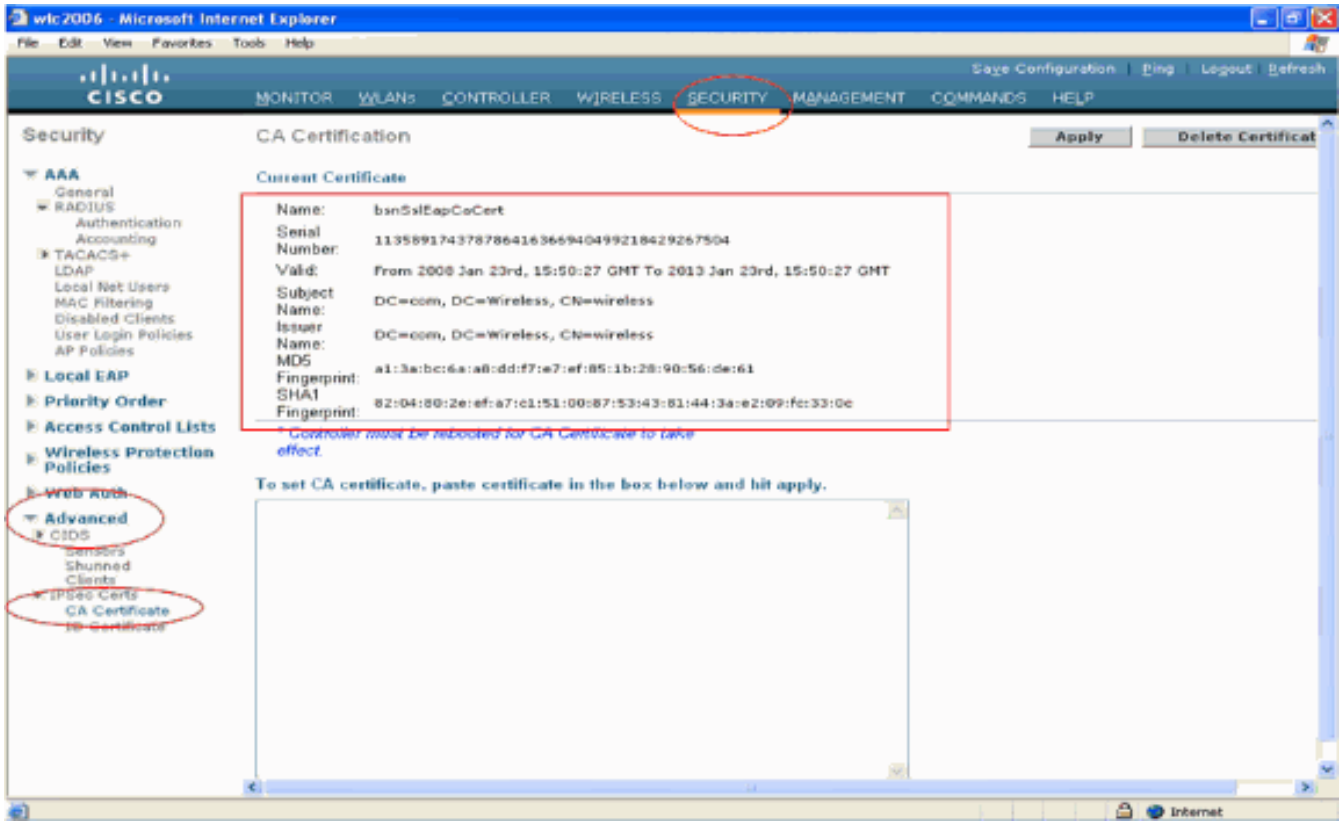
Wählen Sie **DER** als Verschlüsselungsmethode aus, und klicken Sie auf **CA-Zertifikat herunterladen**.



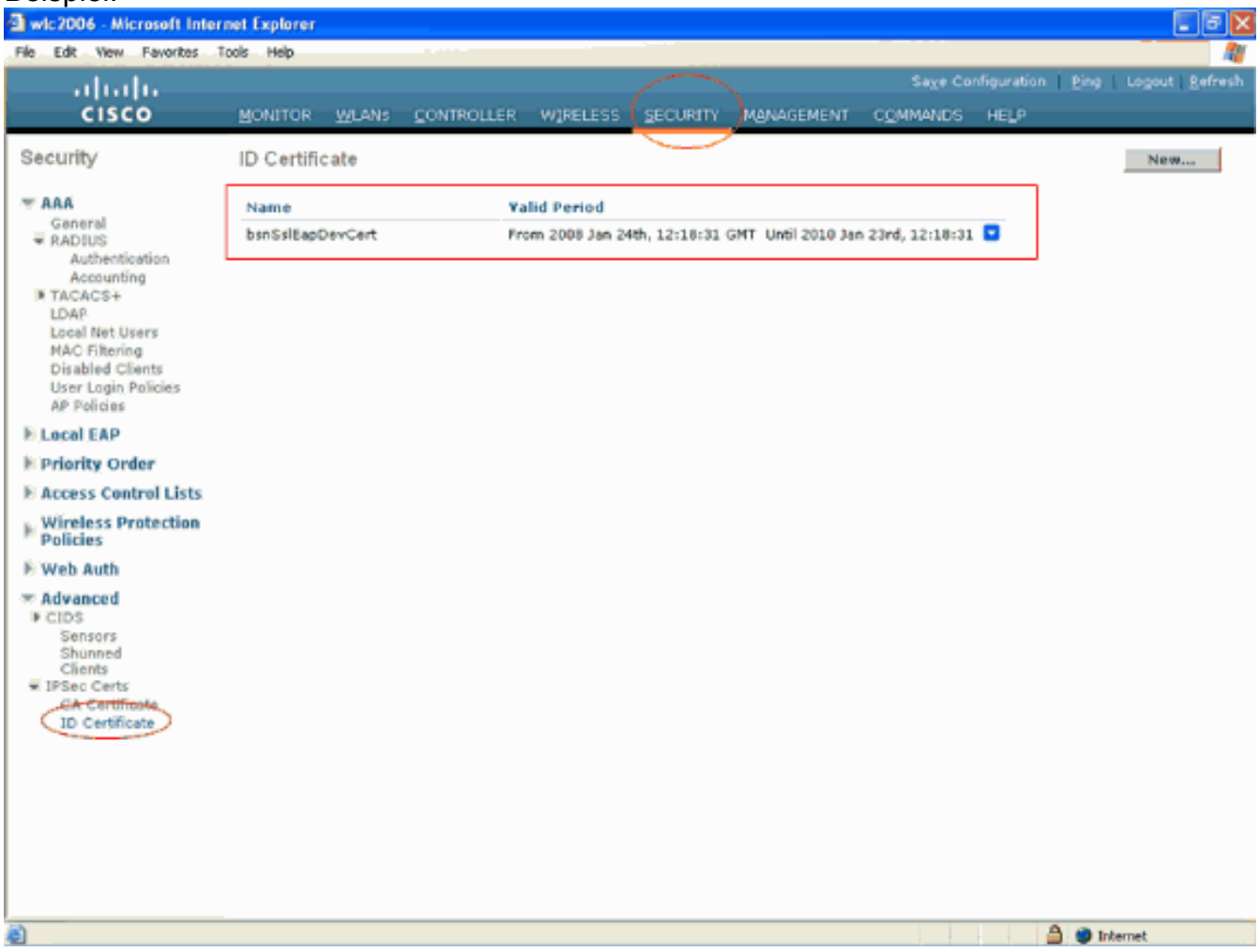

4. Speichern Sie das Zertifikat als .**cer**-Datei. In diesem Beispiel wird **certnew.cer** als Dateiname verwendet.
5. Im nächsten Schritt wird die CER-Datei in das PEM-Format konvertiert und auf den Controller heruntergeladen. Wiederholen Sie zum Durchführen dieser Schritte den gleichen Vorgang wie im Abschnitt Herunterladen des Gerätezertifikats auf den WLC 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 PEM**In Schritt 2 des Abschnitts Download the Converted PEM Format Device 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" eapcacert**Die 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:

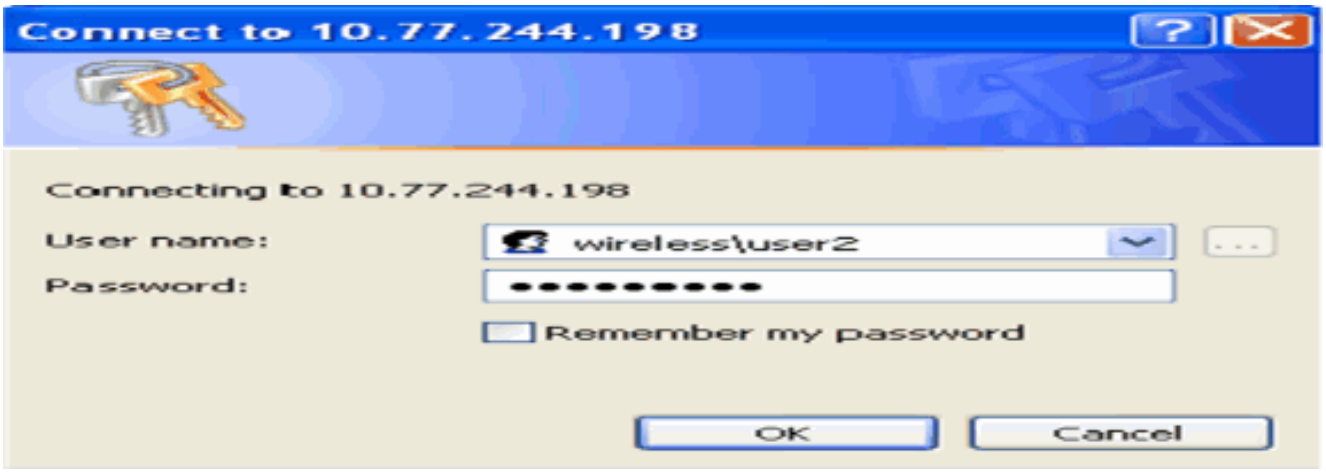


## Generieren eines Gerätezertifikats für den Client

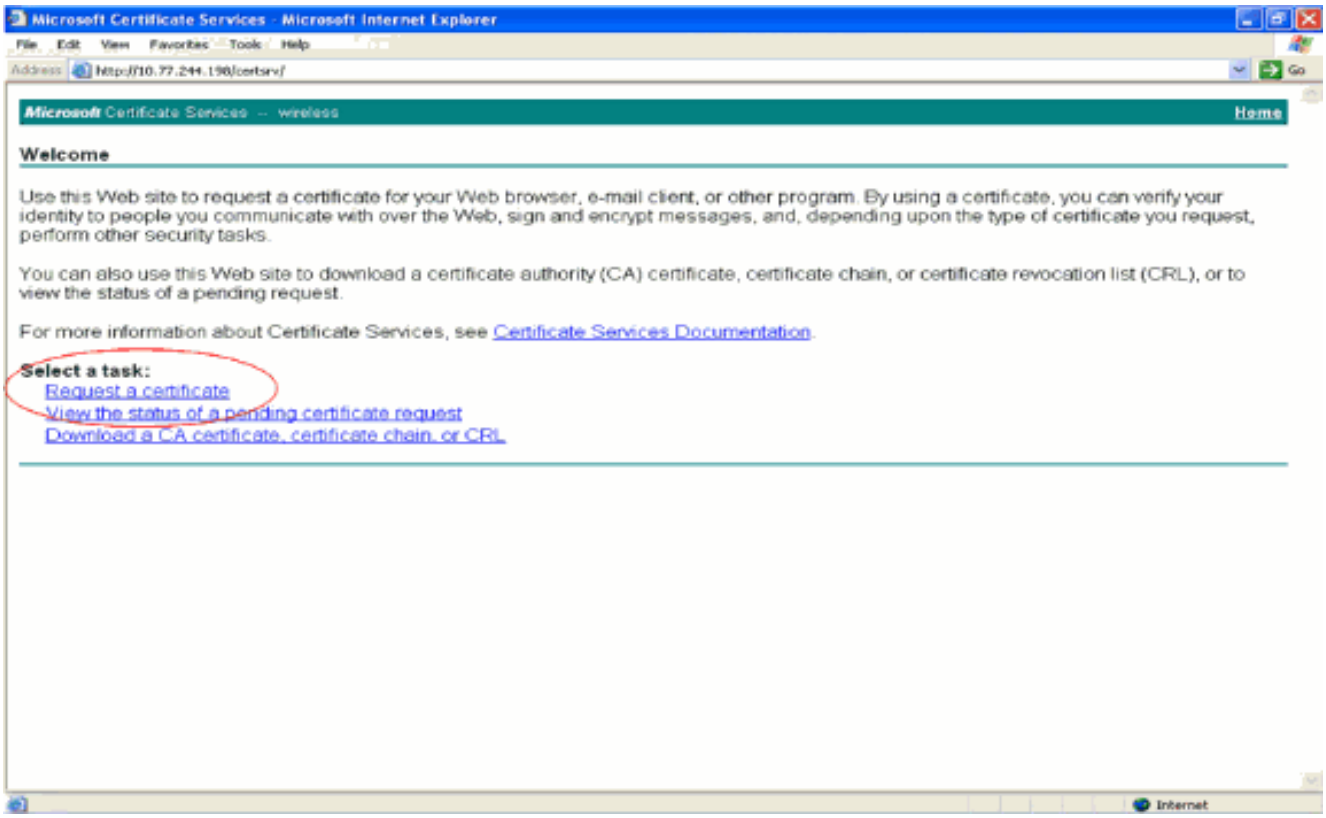
Nachdem das Gerätezertifikat und das Zertifizierungsstellenzertifikat auf dem WLC installiert sind, besteht der nächste Schritt darin, diese Zertifikate für den Client zu generieren.

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.

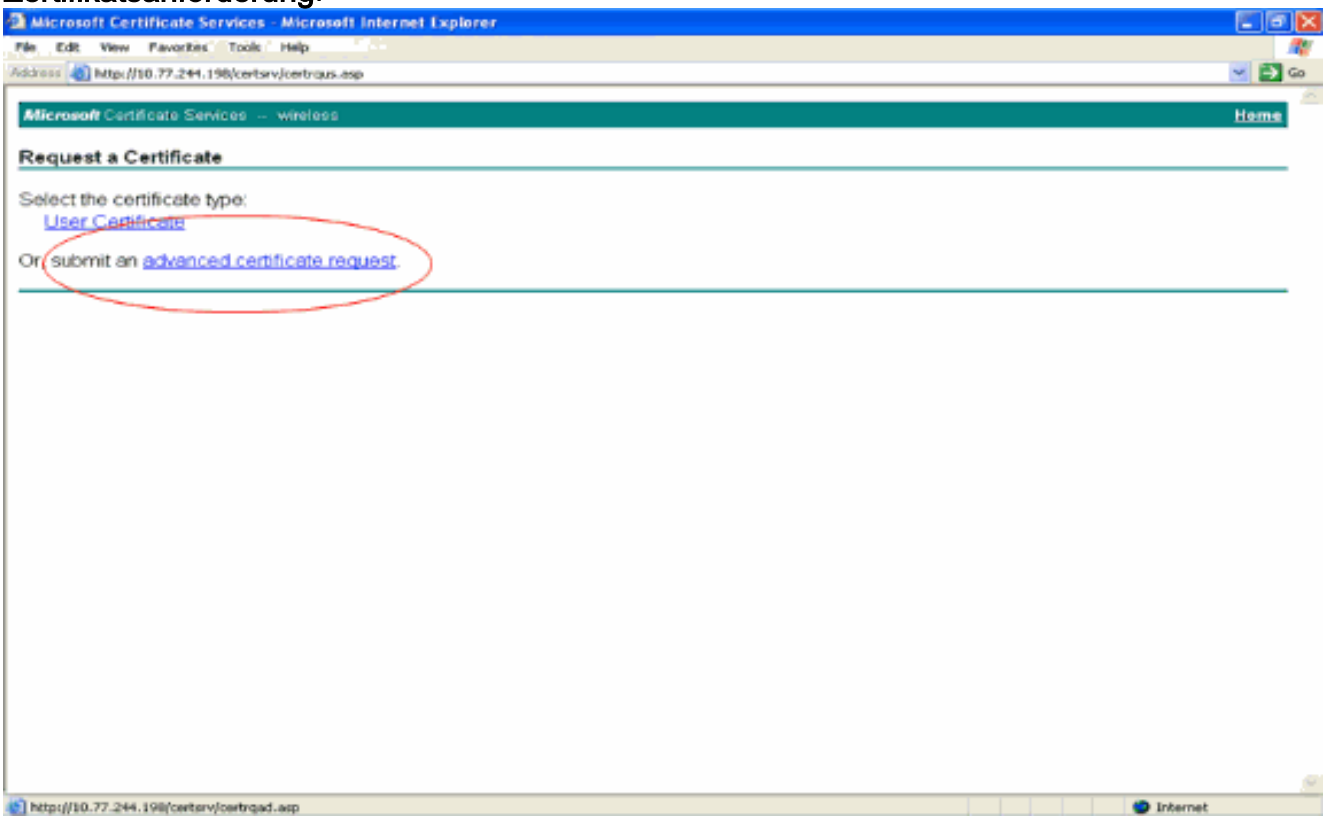
1. Gehen Sie zu **http://<IP-Adresse des CA-Servers>/certsrv** vom Client, auf dem das Zertifikat installiert werden muss. Melden Sie sich beim CA-Server als Domänenname\Benutzername an. Beim Benutzernamen sollte es sich um den Namen des Benutzers handeln, der diesen XP-Computer verwendet. Der Benutzer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



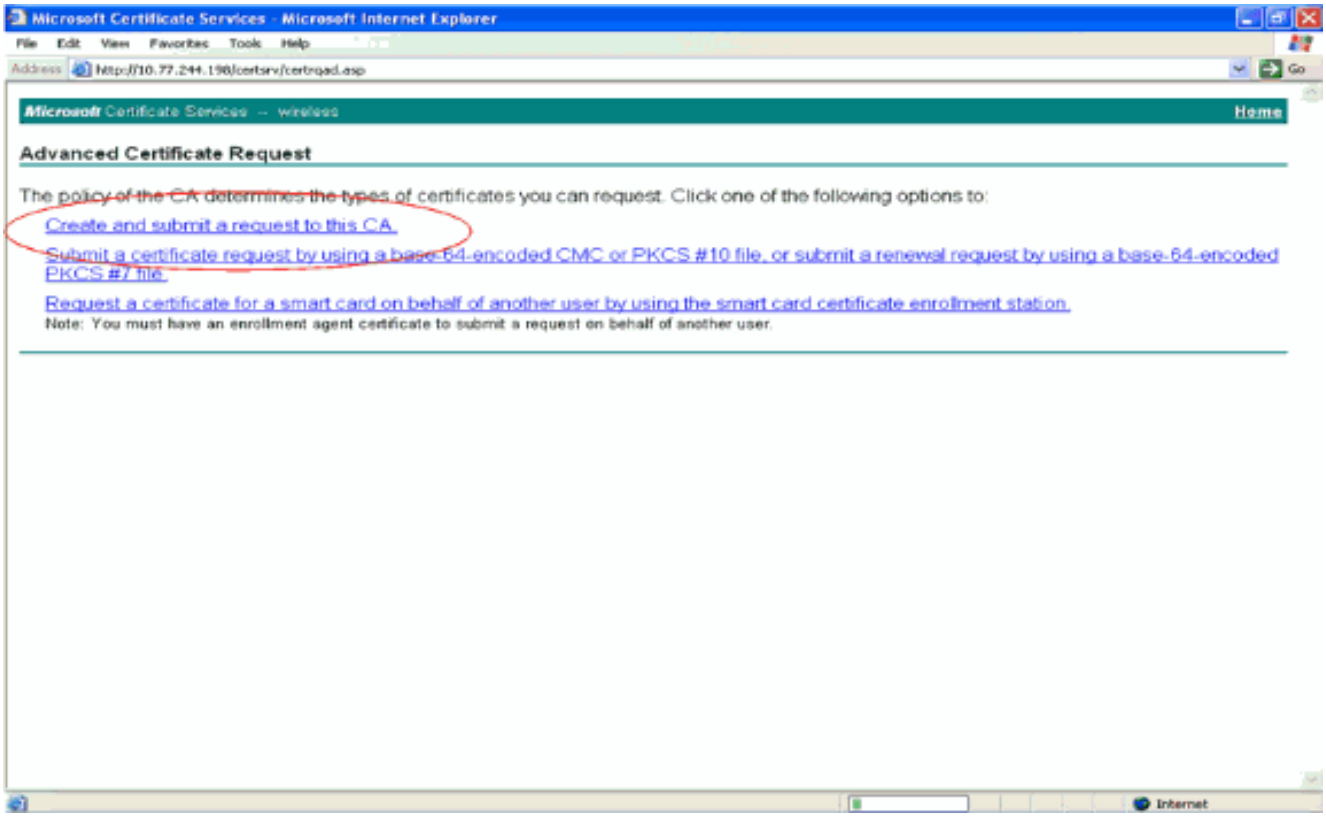

2. Wählen Sie **Zertifikat anfordern aus**.



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

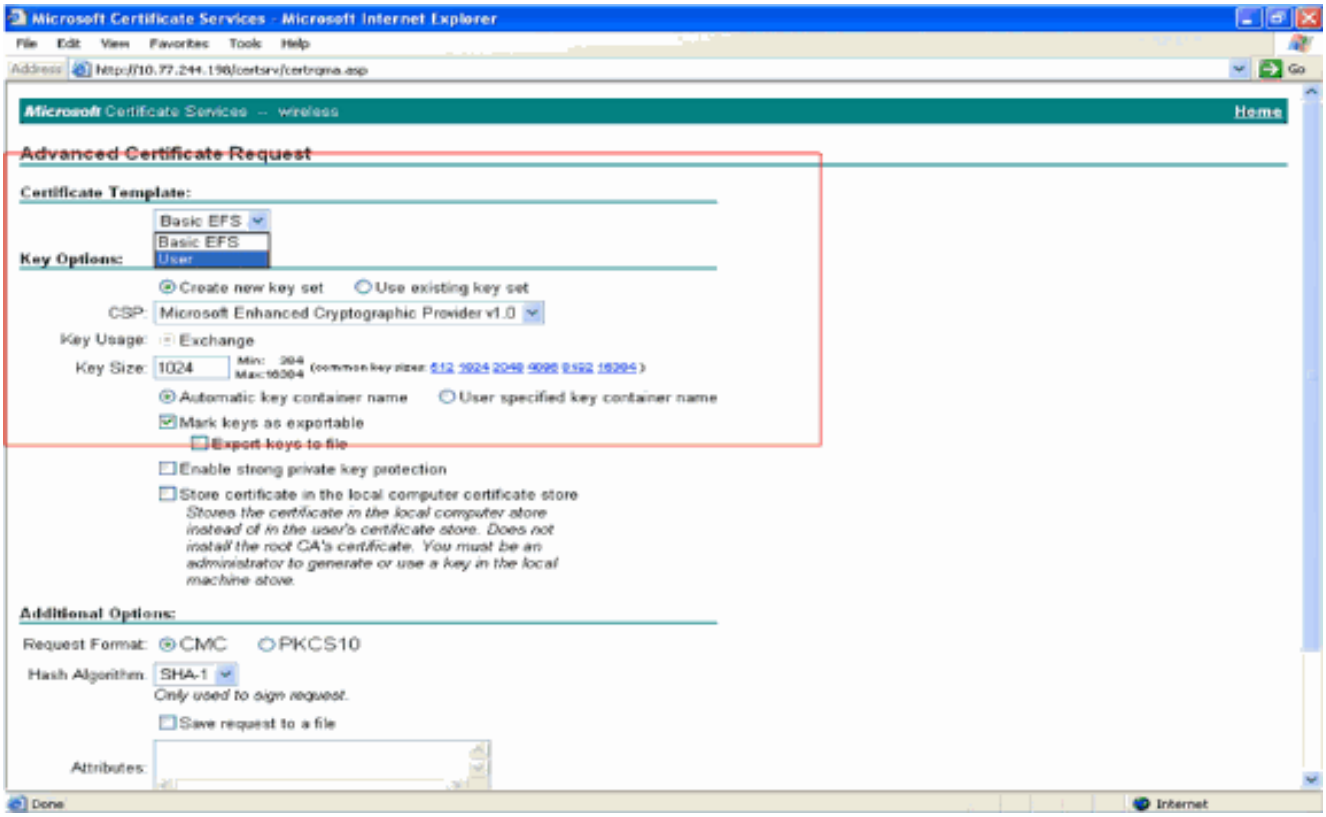



4. Klicken Sie auf der Seite "Erweiterte Zertifikatanforderung" auf **Erstellen, und senden Sie eine Anforderung an diese Zertifizierungsstelle**. Dadurch gelangen Sie zum Anforderungsformular für Advanced-Zertifikate.

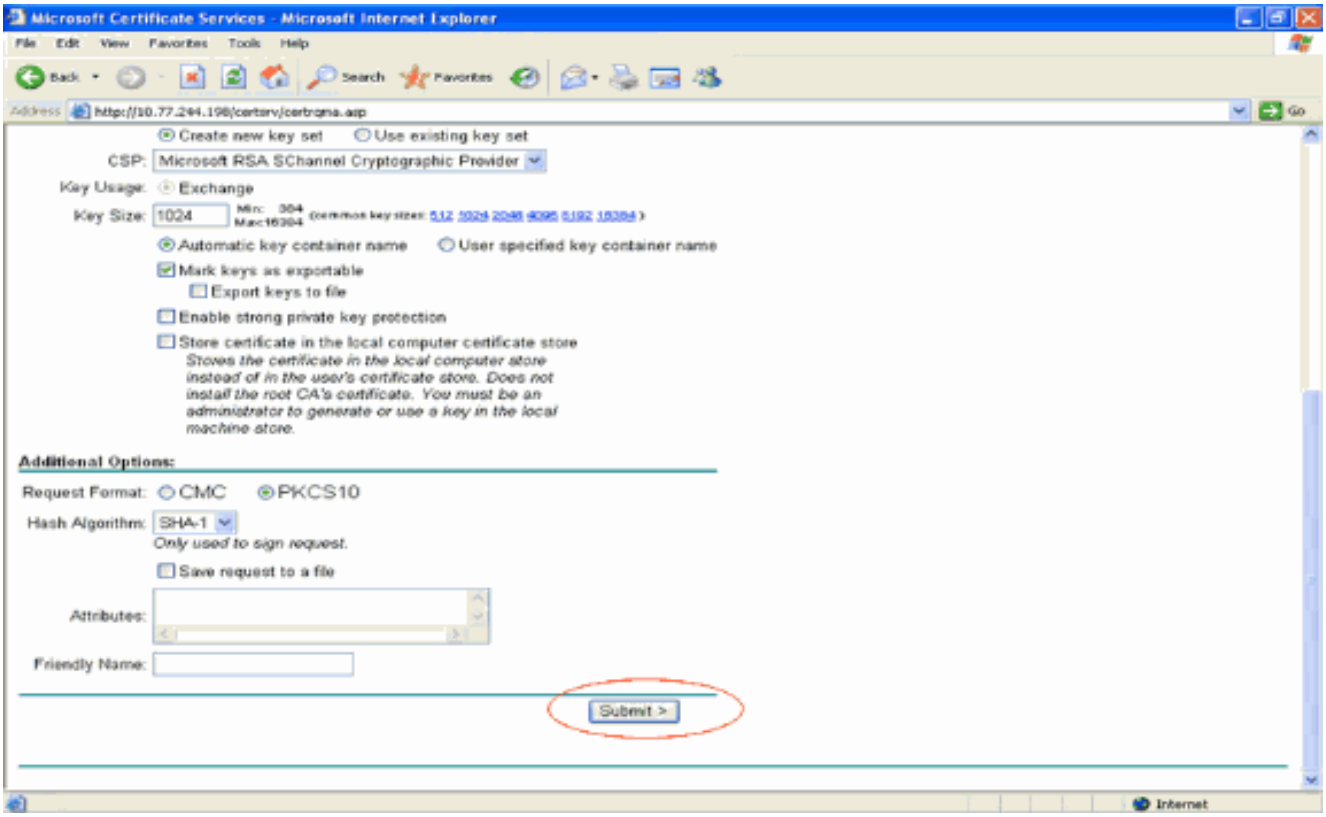



5. Wählen Sie im Anforderungsformular für erweiterte Zertifikate im Dropdown-Menü Zertifikatvorlage die Option **Benutzer** aus.Wählen Sie im Abschnitt "Key options" (Schlüsseloptionen) folgende Parameter aus:Geben Sie die Schlüssellänge in das Feld

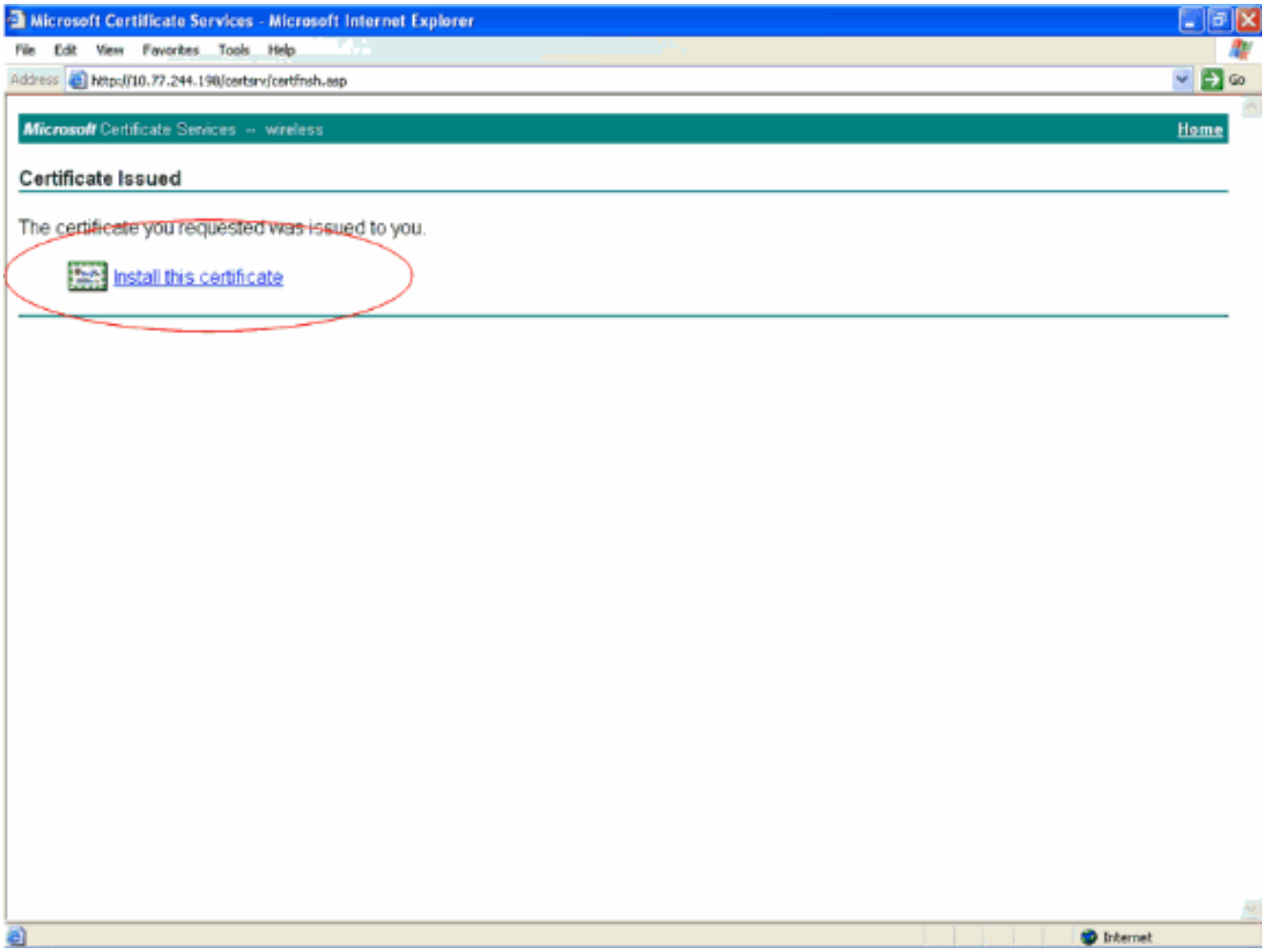
Schlüssellänge ein. In diesem Beispiel wird **1024** verwendet.Aktivieren Sie die Option **Schlüssel als exportierbar markieren**.



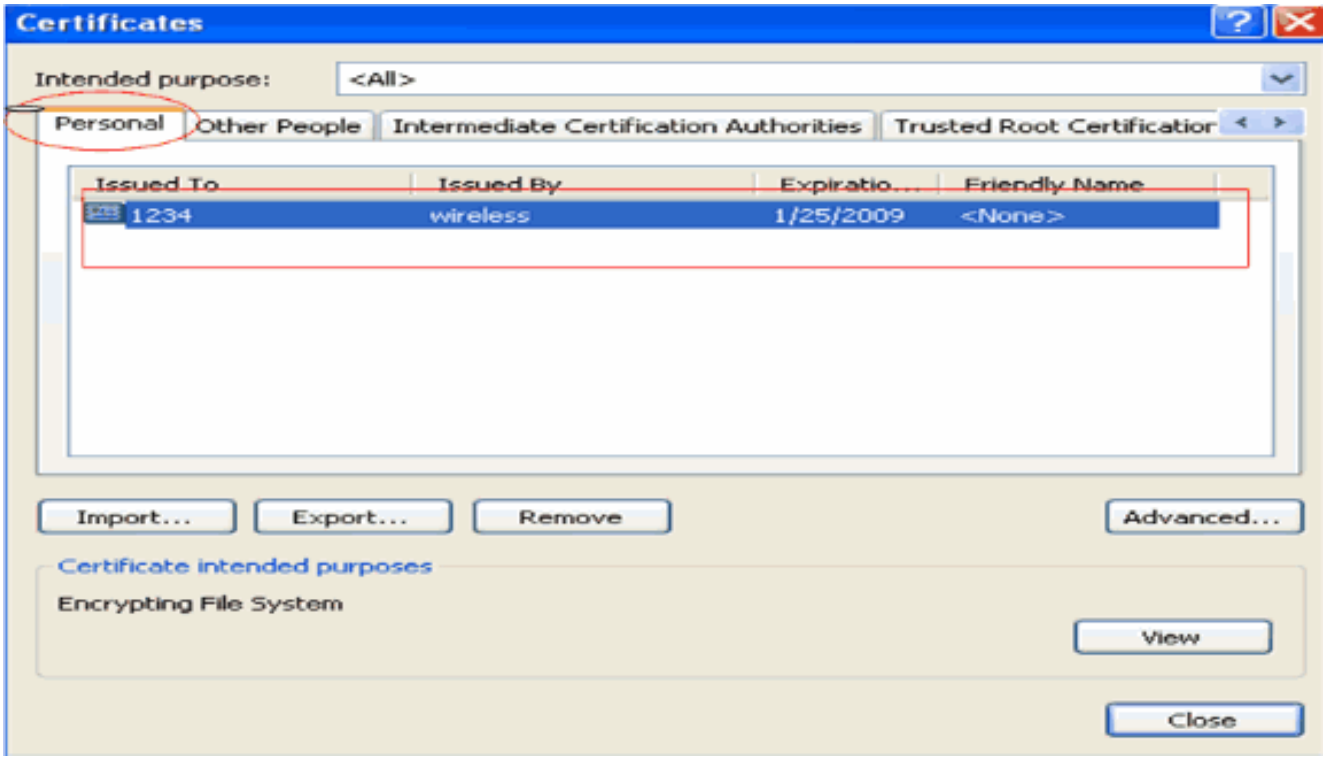

6. Konfigurieren Sie alle anderen erforderlichen Felder, und klicken Sie auf **Senden**.




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




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

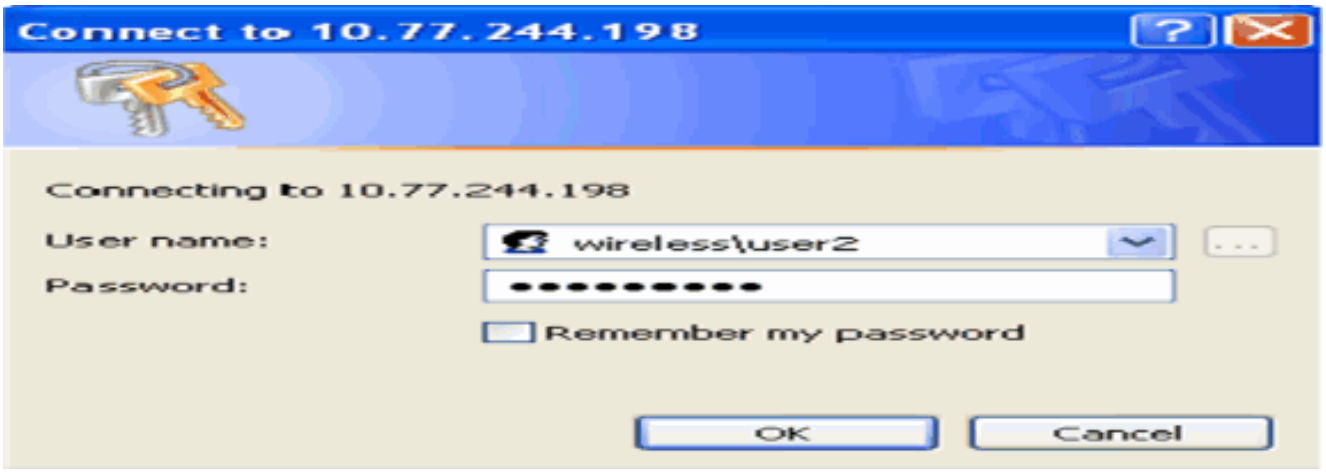



Das Gerätezertifikat für den Client wird auf dem Client installiert.

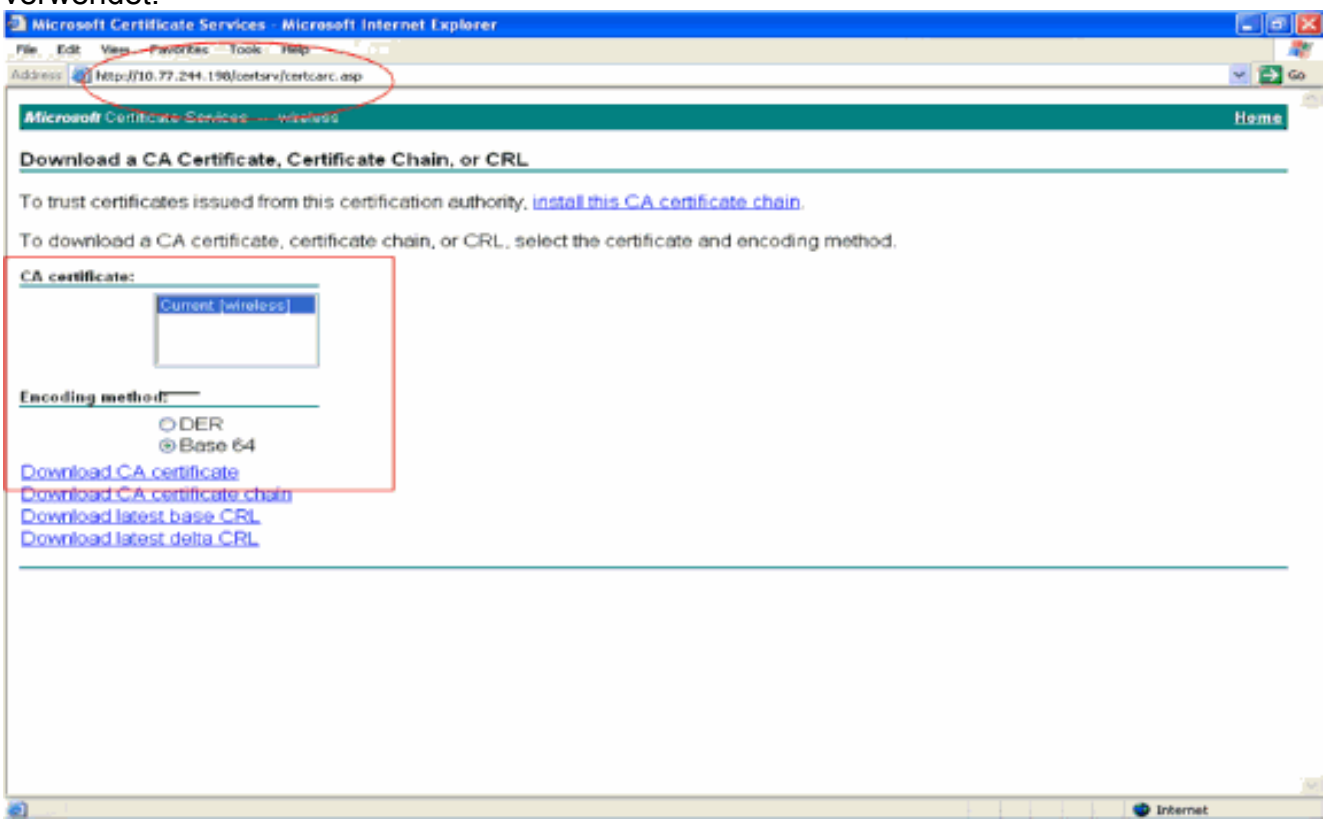
## Generieren des Stammzertifizierungsstellenzertifikats für den Client

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

1. 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.

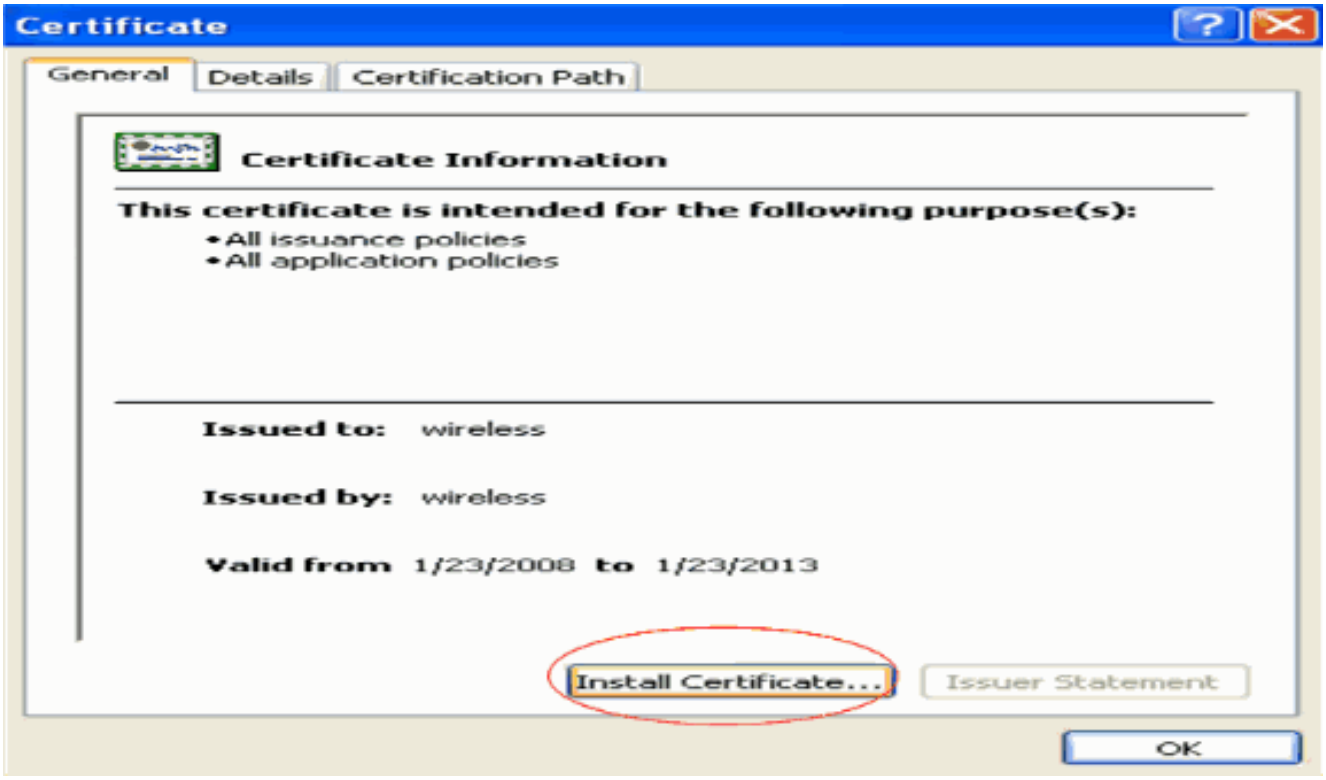



2. Auf der Ergebnisseite werden die aktuellen Zertifizierungsstellenzertifikate angezeigt, die auf dem Zertifizierungsstellenserver im Feld für das **Zertifizierungsstellenzertifikat** verfügbar sind. Wählen Sie **Base 64** als Encoding-Methode aus. Klicken Sie dann auf **CA-Zertifikat herunterladen**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

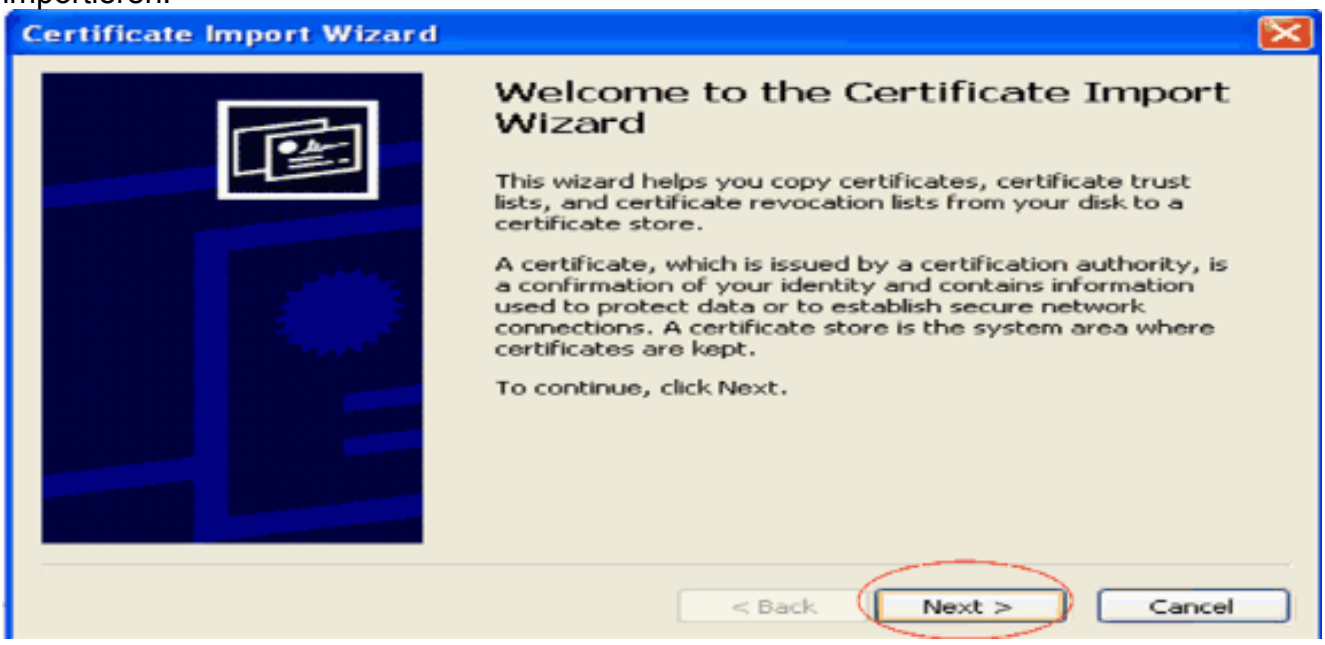



3. Installieren Sie anschließend das CA-Zertifikat, das im CER-Format gespeichert ist, im Zertifikatspeicher des Clients. Doppelklicken Sie auf die Datei rootca.cer, und klicken Sie auf **Zertifikat**

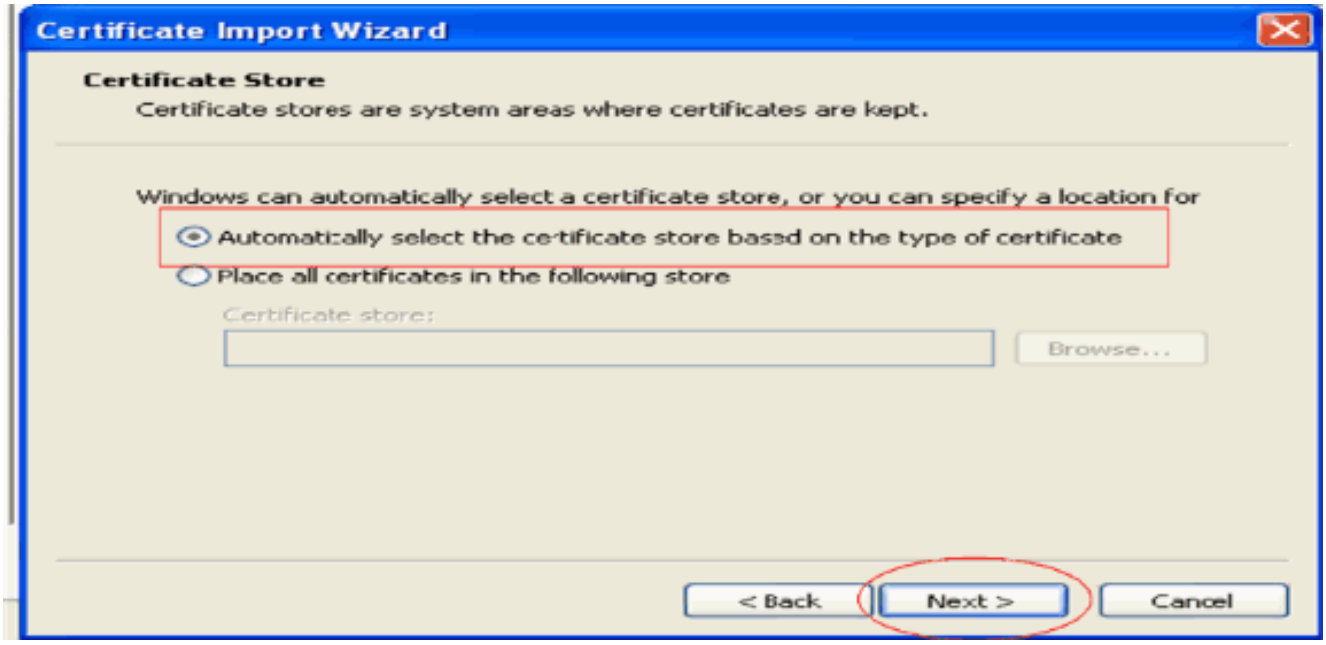
installieren.



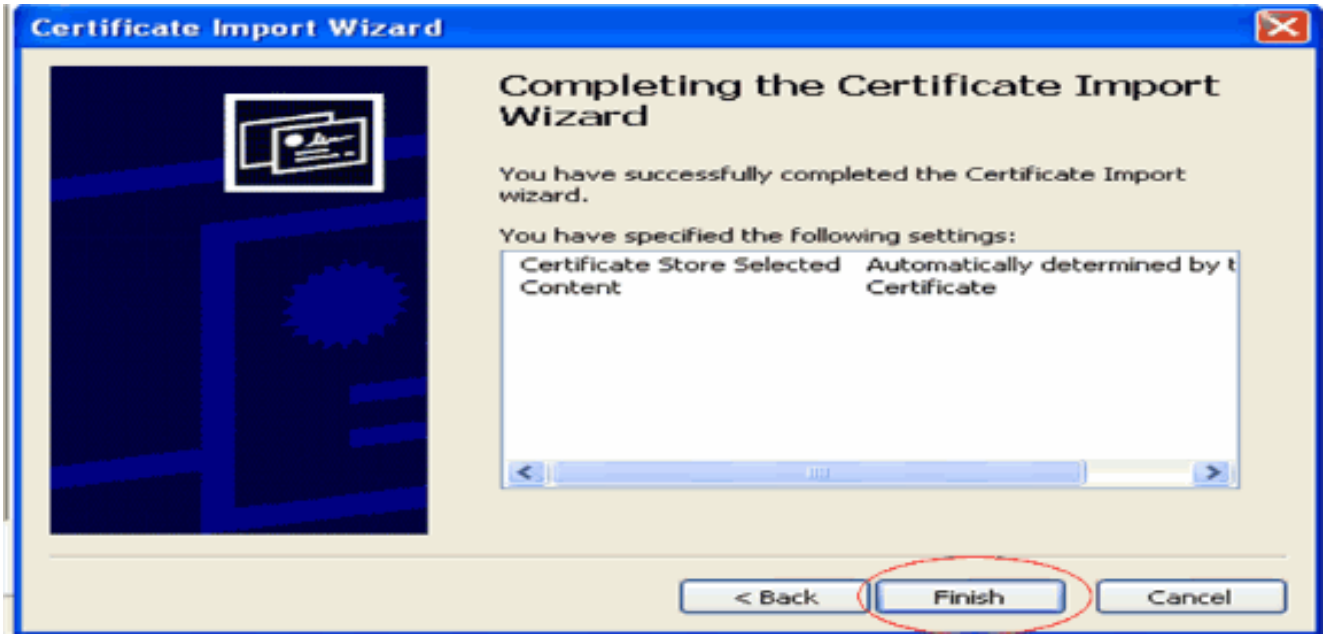

4. Klicken Sie auf **Weiter**, um das Zertifikat von der Festplatte des Clients in den Zertifikatspeicher zu importieren.



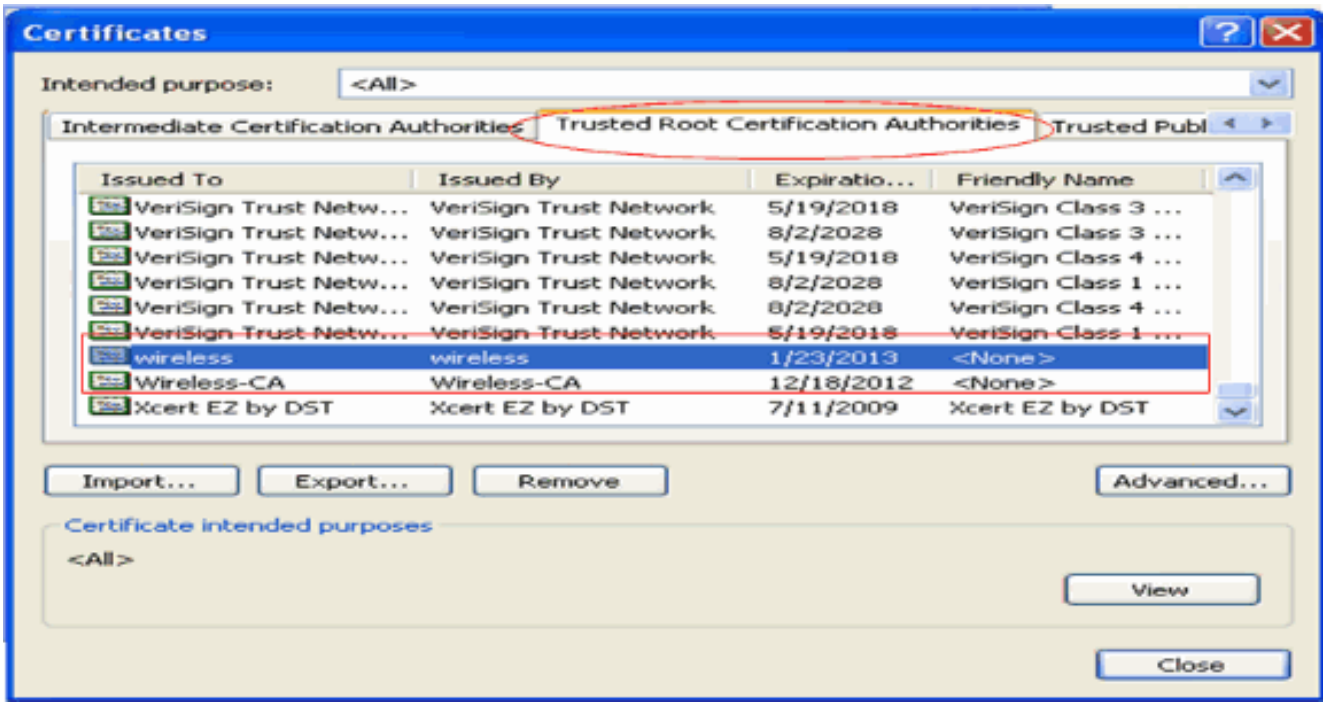

5. Wählen Sie **den Zertifikatspeicher basierend auf dem Zertifikatstyp automatisch aus,** und klicken Sie auf **Weiter**.




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




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:

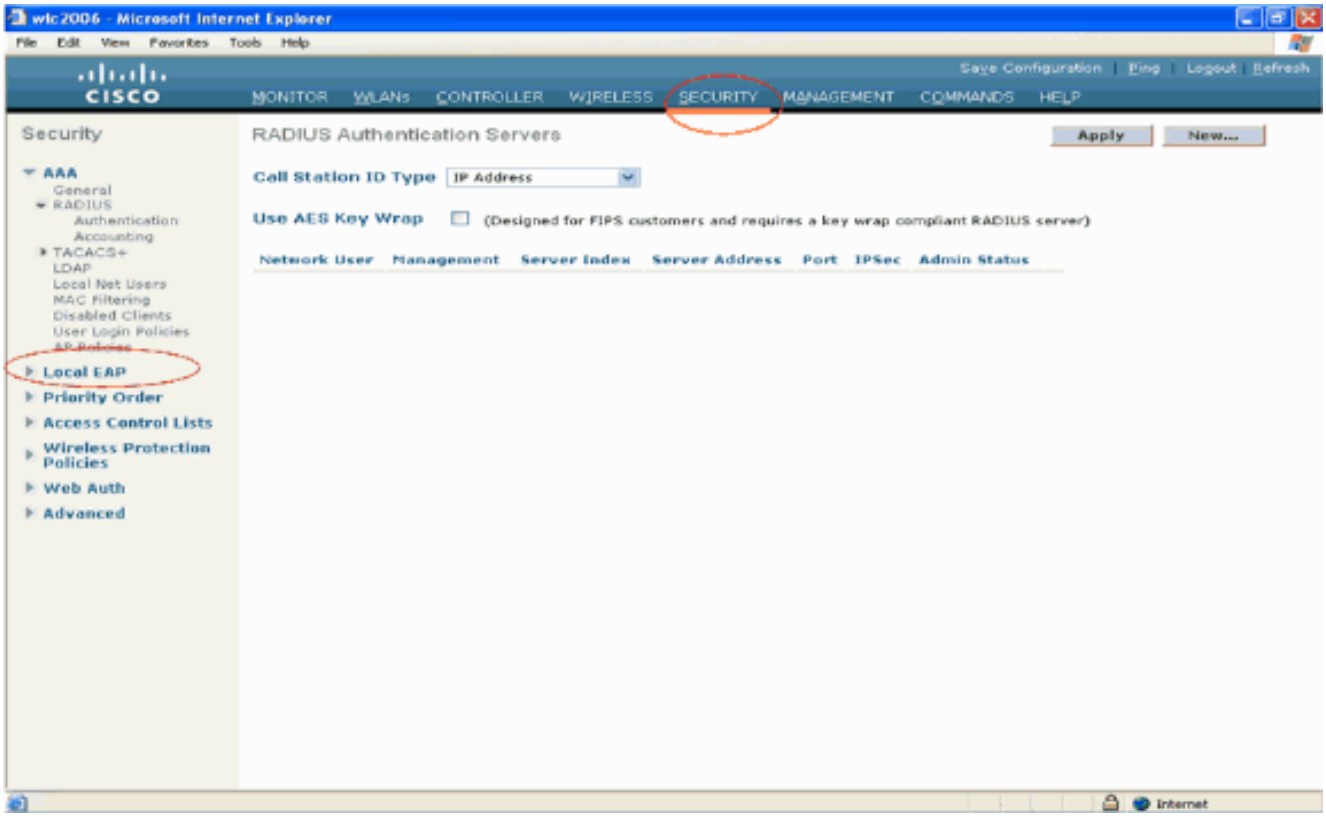



Alle erforderlichen Zertifikate werden sowohl auf dem WLC als auch auf dem Client für die EAP-FAST Local-EAP-Authentifizierung installiert. Im nächsten Schritt wird der WLC für die lokale EAP-Authentifizierung konfiguriert.

## Konfigurieren des lokalen EAP auf dem WLC

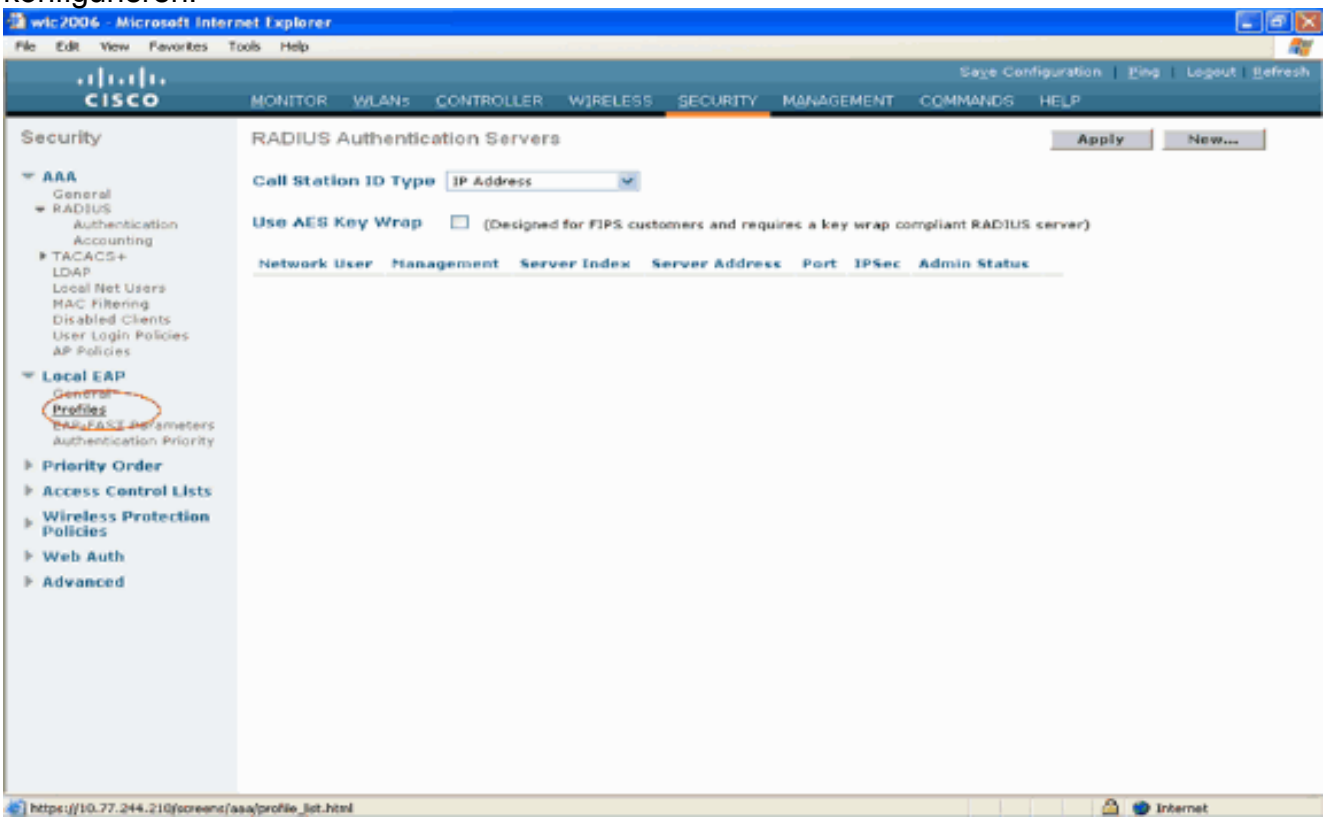
Führen Sie im **WLC-GUI-Modus** die folgenden Schritte aus, um die lokale EAP-Authentifizierung auf dem WLC zu konfigurieren:

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

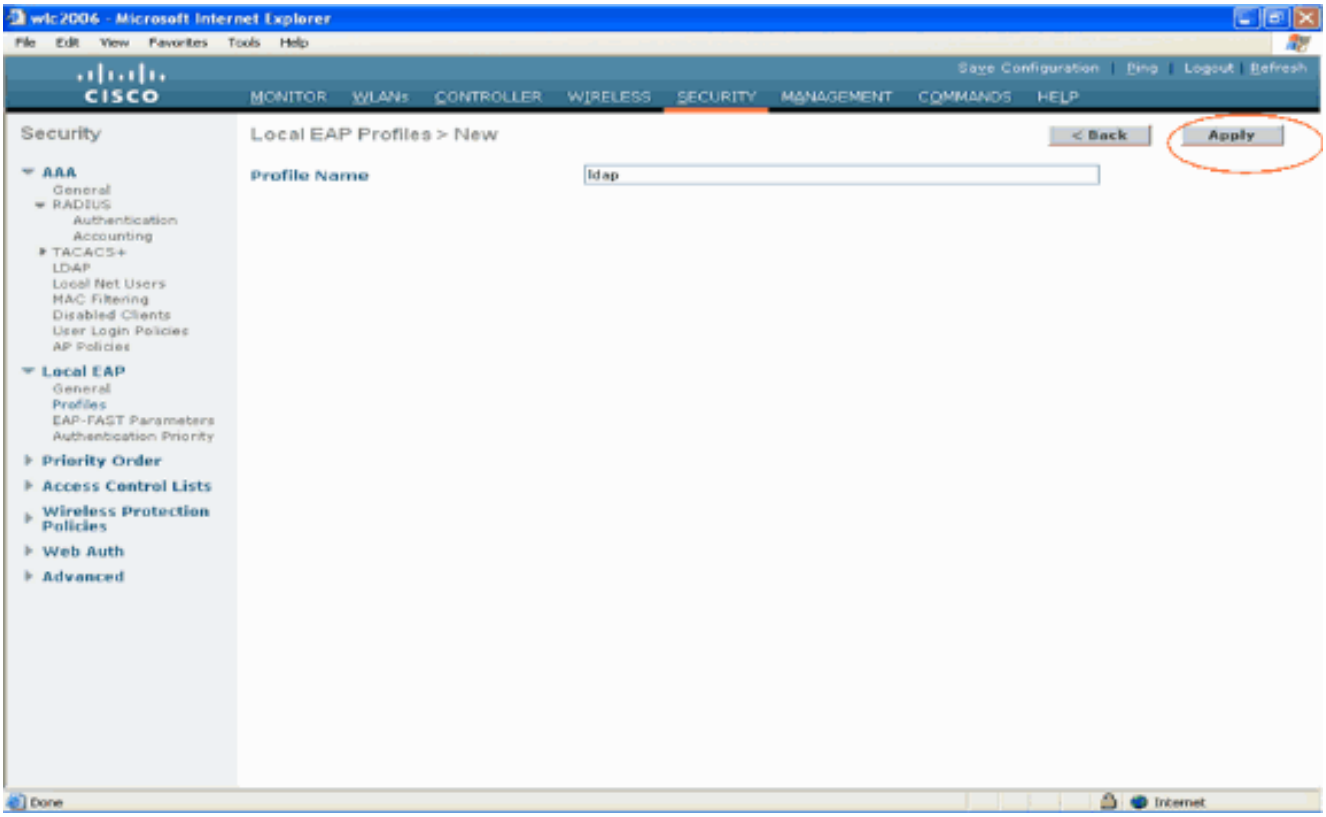



2. Klicken Sie unter Local EAP (Lokales EAP) auf **Profiles** (Profile), um das Profil Local EAP (Lokales EAP) zu

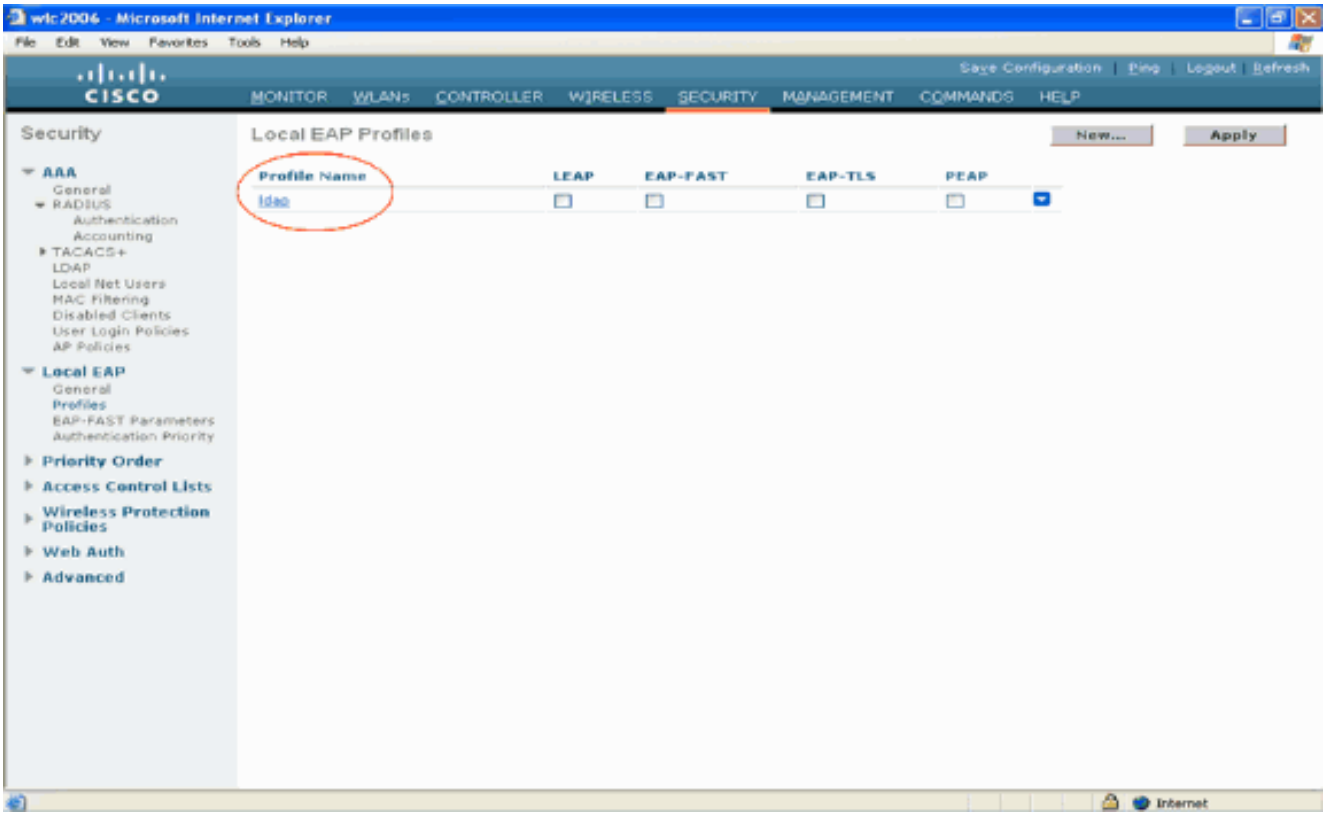
konfigurieren.



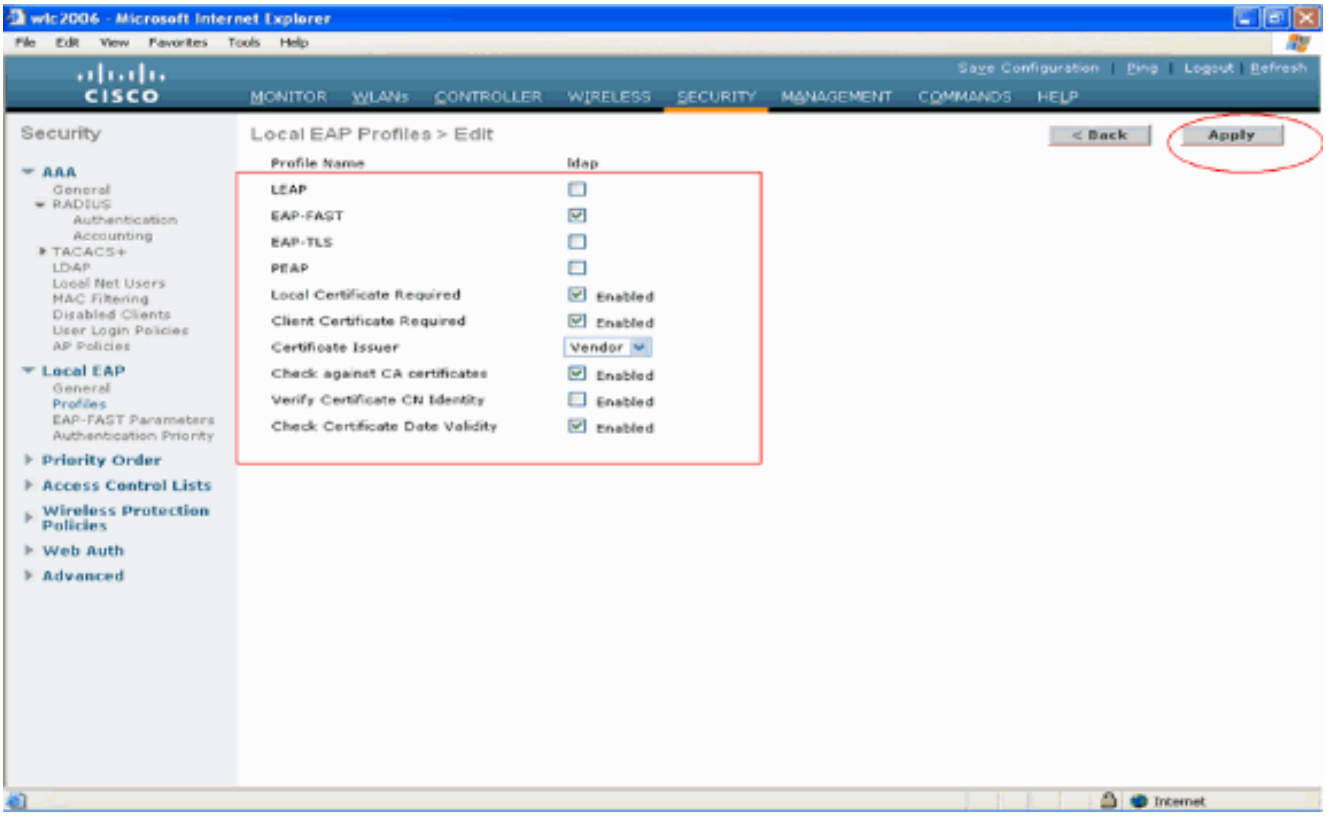

3. Klicken Sie auf **Neu**, um ein neues lokales EAP-Profil zu erstellen.
4. Konfigurieren Sie einen Namen für dieses Profil, und klicken Sie auf **Apply**. In diesem Beispiel lautet der Profilname **ldap**. Dadurch gelangen Sie zu den lokalen EAP-Profilen, die auf dem WLC erstellt
wurden.



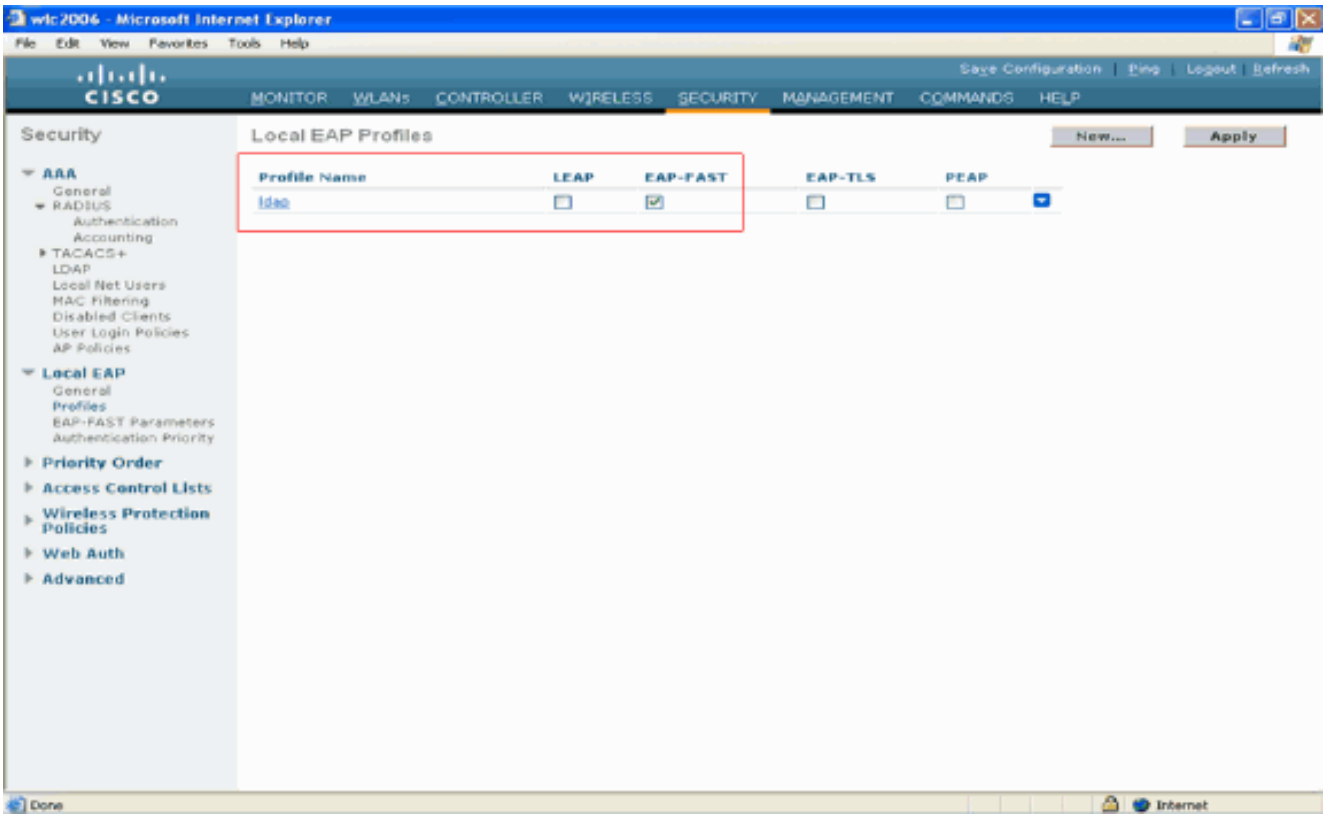

5. Klicken Sie auf das gerade erstellte **LDAP**-Profil, das im Feld Profilname der Seite Lokale EAP-Profile angezeigt wird. Dadurch gelangen Sie zur Seite **Lokale EAP-Profile > Bearbeiten**.



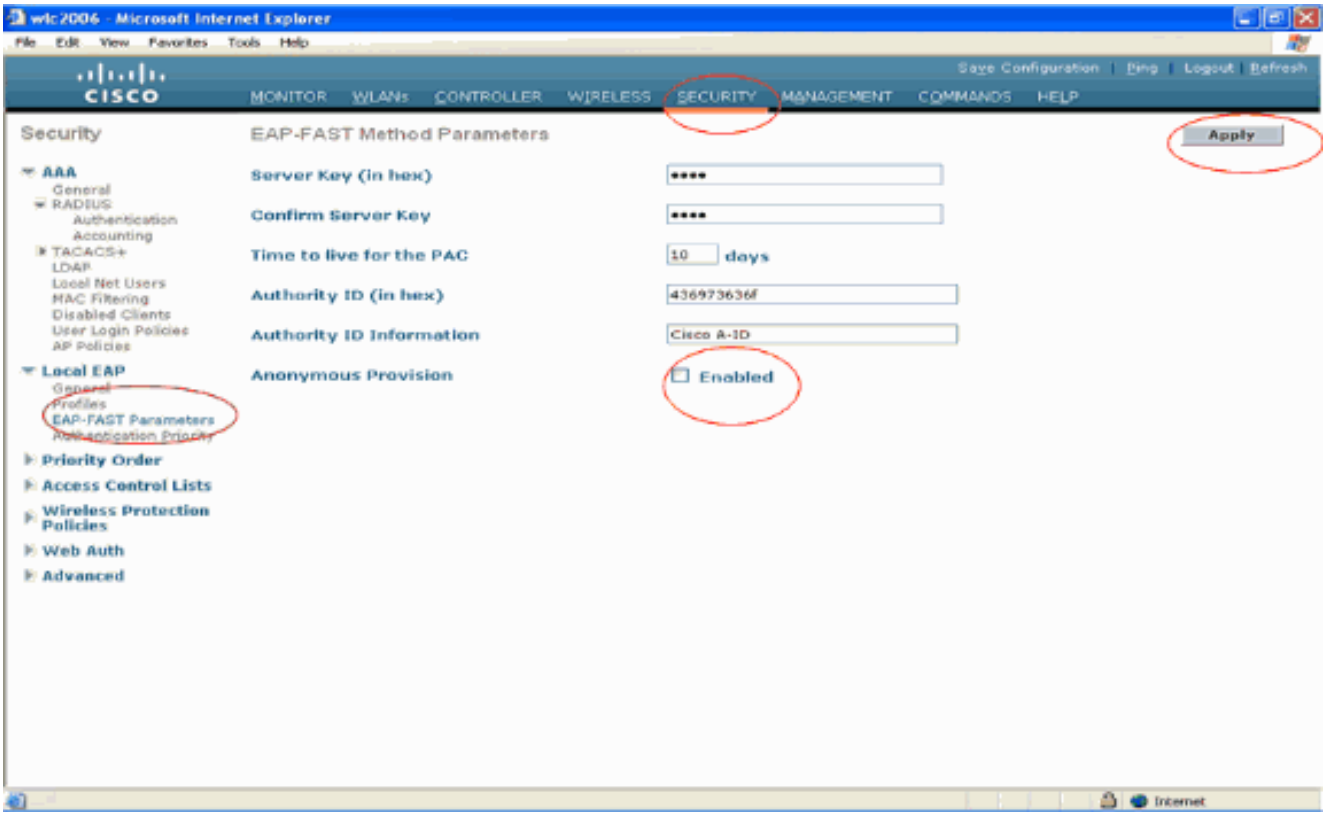

6. Konfigurieren Sie die für dieses Profil spezifischen Parameter auf der Seite **Lokale EAP-Profile > Bearbeiten**.Wählen Sie **EAP-FAST** als lokale EAP-Authentifizierungsmethode aus.Aktivieren Sie die Kontrollkästchen neben **Lokales Zertifikat erforderlich** und **Clientzertifikat erforderlich**.Wählen 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.



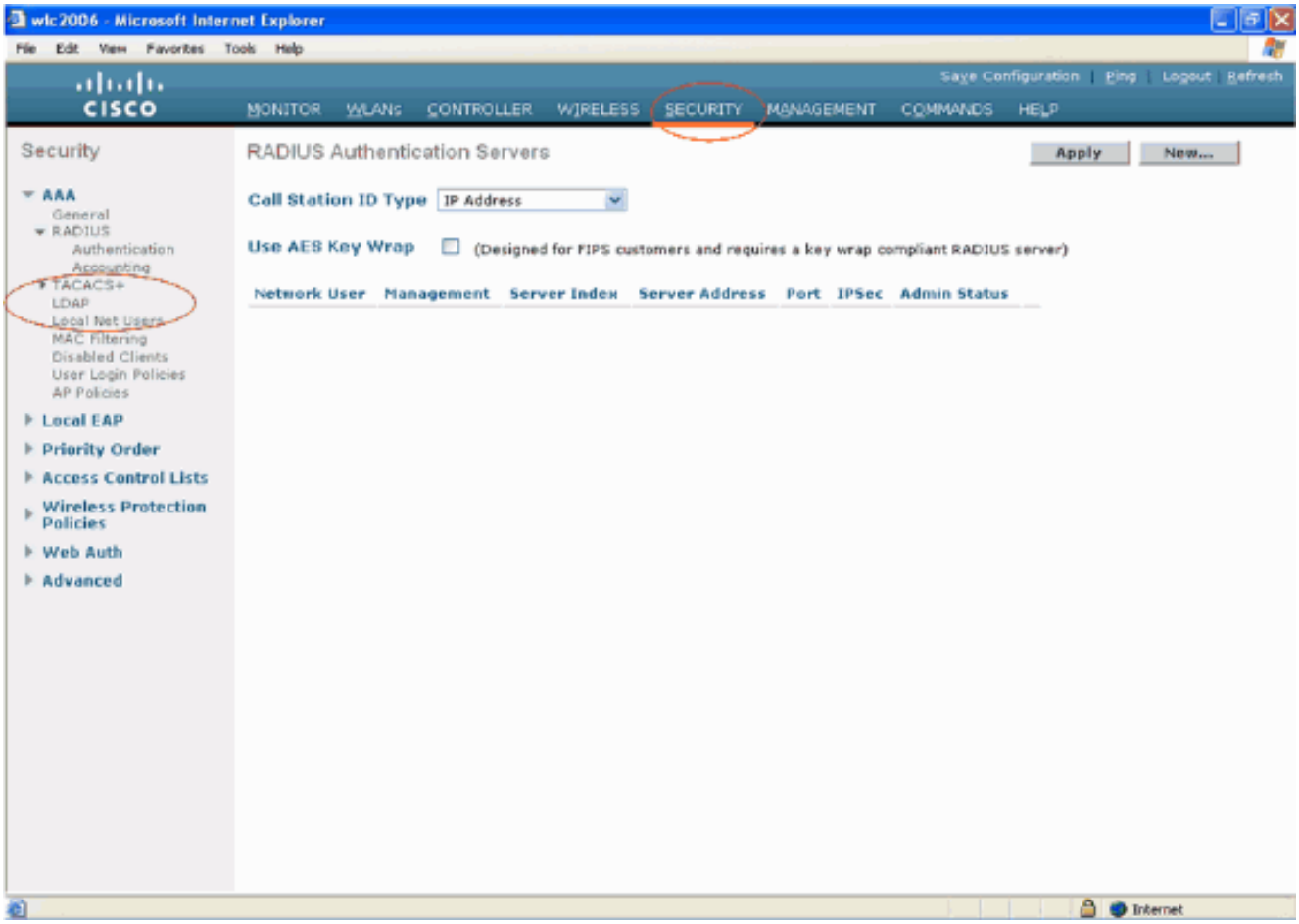

8. Im nächsten Schritt werden EAP-FAST-spezifische Parameter auf dem WLC konfiguriert. Klicken Sie auf der Seite "WLC Security" auf **Local EAP > EAP-FAST Parameters,** um zur Seite "EAP-FAST Method Parameters" zu wechseln.Deaktivieren Sie das Kontrollkästchen **Anonyme Bereitstellung**, da in diesem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




## Konfigurieren des WLC mit LDAP-Serverdetails

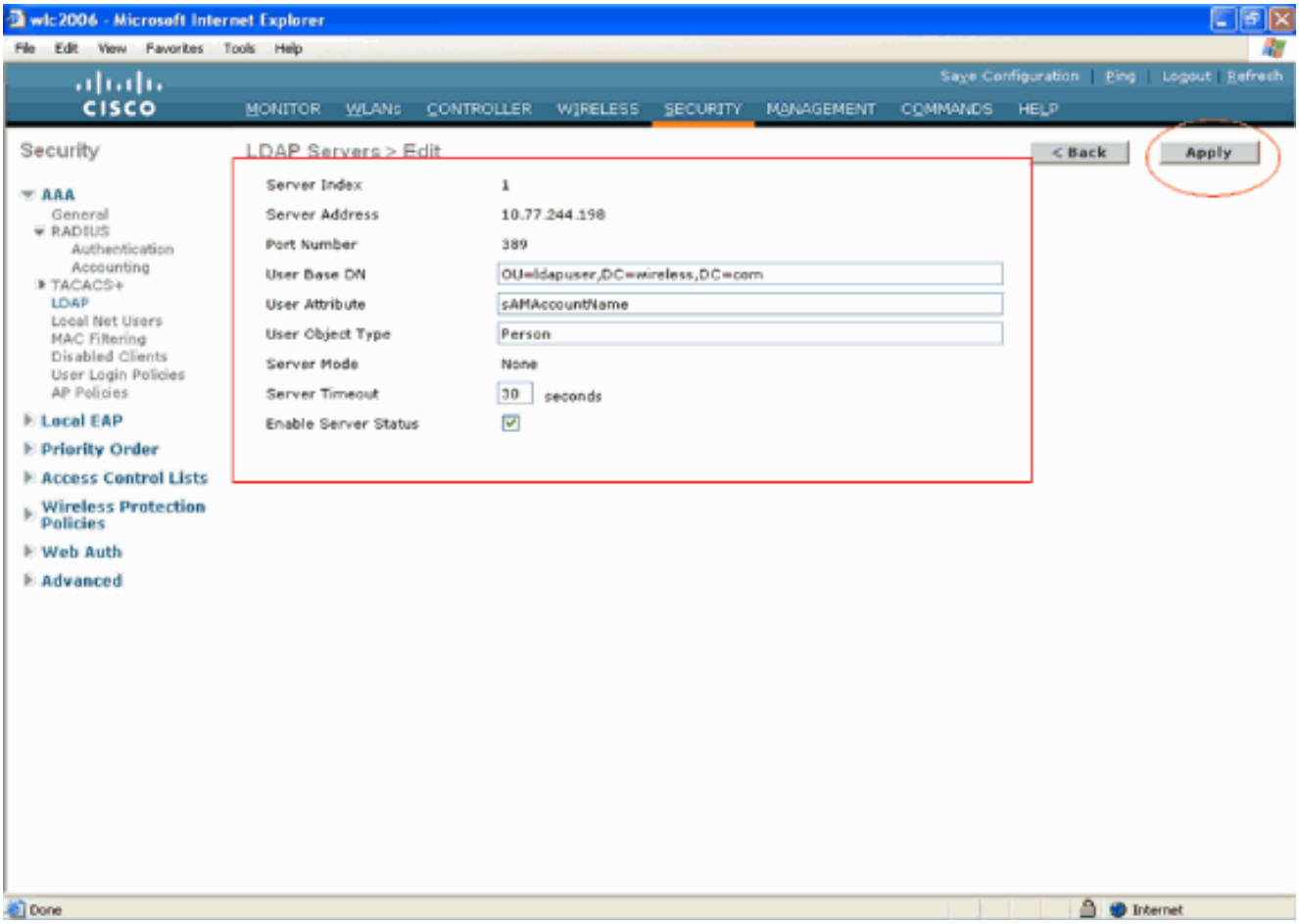
Nachdem der WLC mit dem lokalen EAP-Profil und den zugehörigen Informationen konfiguriert wurde, besteht der nächste Schritt darin, den WLC mit Details des LDAP-Servers zu konfigurieren. Führen Sie am WLC die folgenden Schritte aus:

1. 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 ldapuser (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=ldapuser, 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:

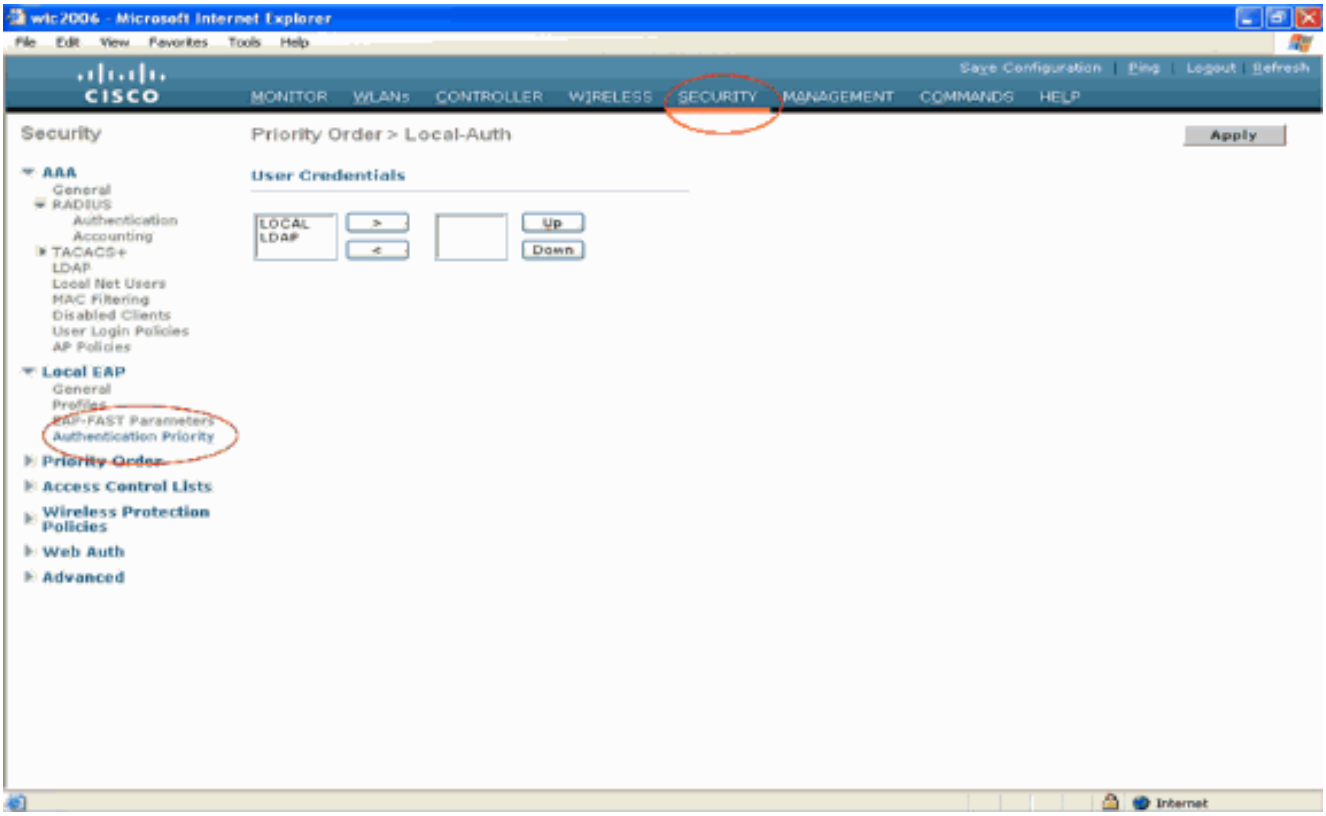



Nachdem nun die Details zum LDAP-Server auf dem WLC konfiguriert sind, besteht der nächste Schritt darin, LDAP als Backend-Datenbank mit Priorität zu konfigurieren, sodass der WLC zunächst in der LDAP-Datenbank nach Benutzeranmeldeinformationen und nicht nach anderen Datenbanken sucht.

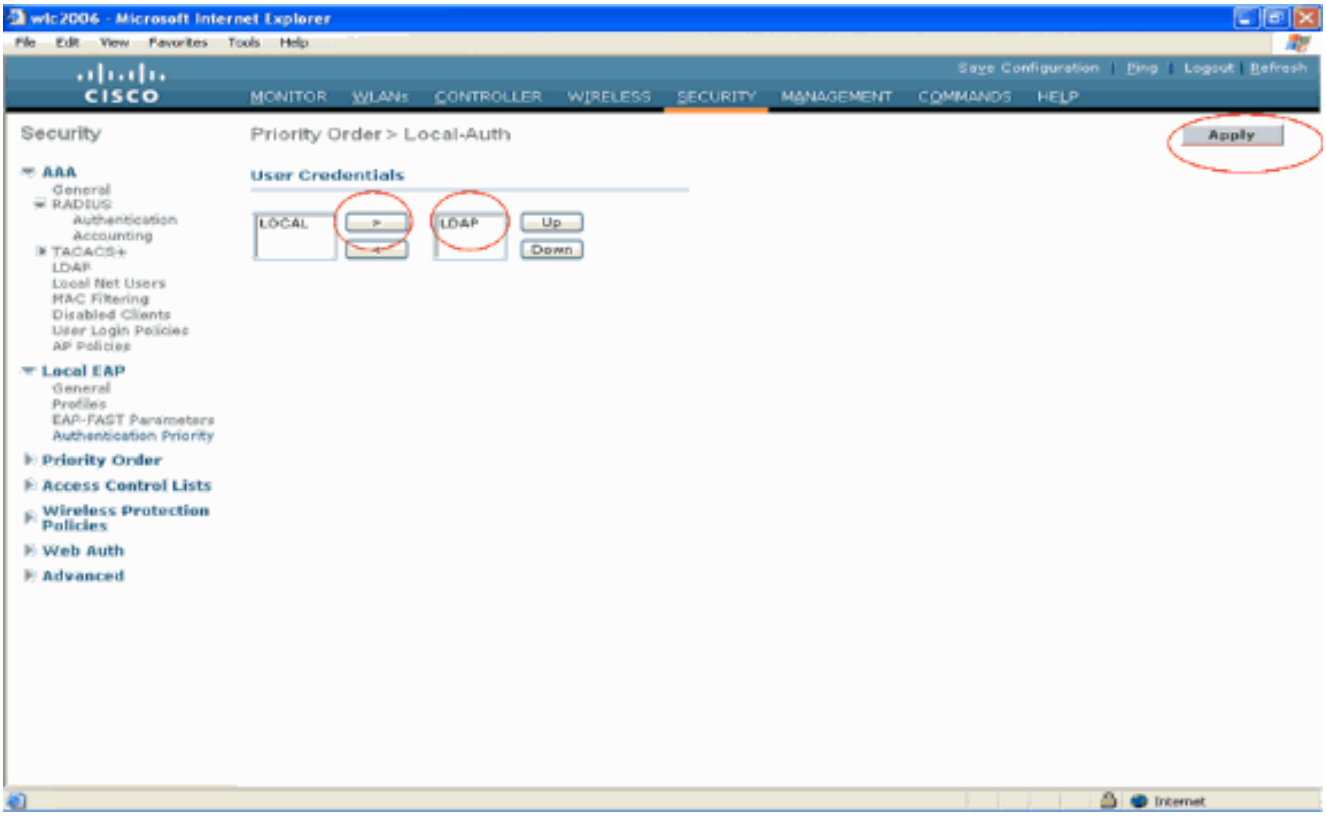
## LDAP als primäre Backend-Datenbank konfigurieren

Führen Sie auf dem WLC die folgenden Schritte aus, um LDAP als bevorzugte Backend-Datenbank zu konfigurieren:

1. 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.




2. 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).

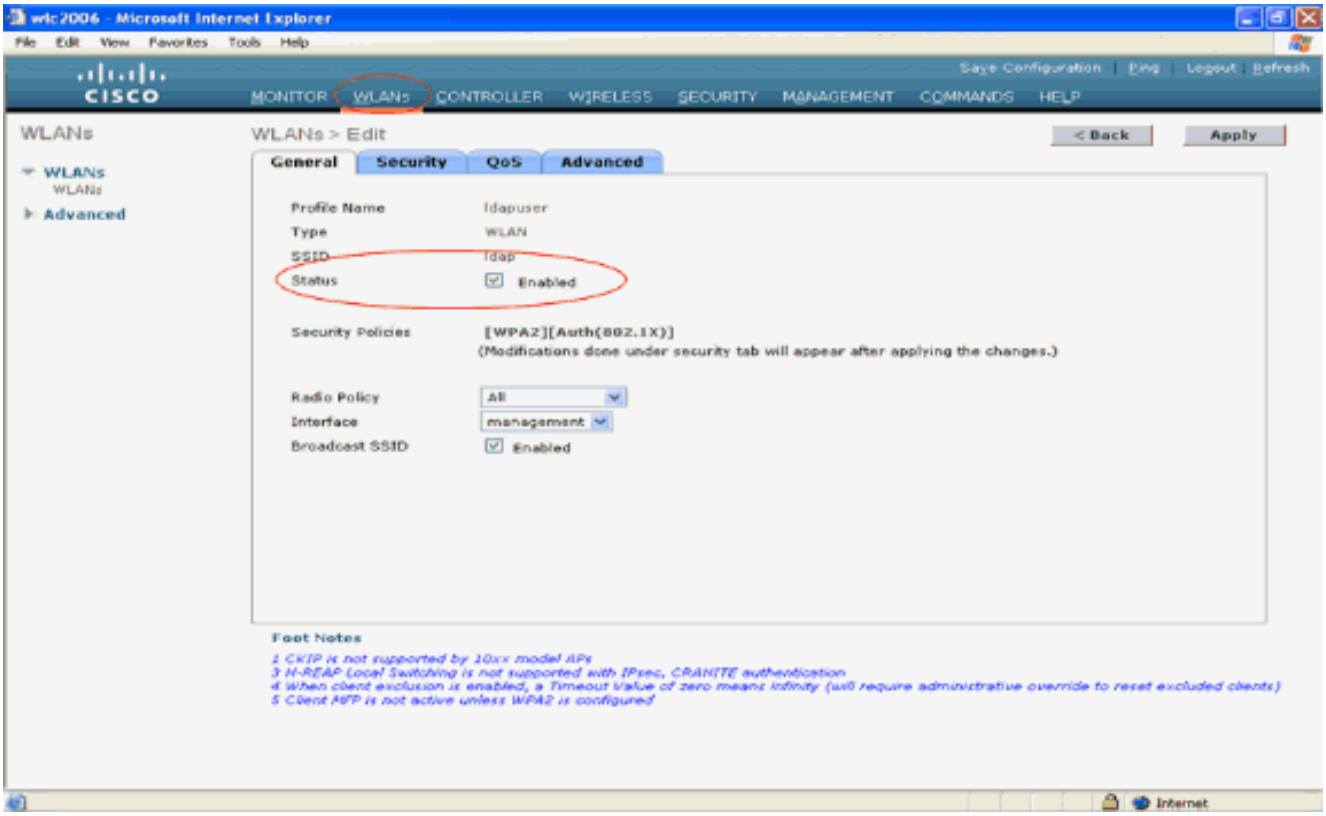



**Hinweis:** Wenn sowohl LDAP als auch LOCAL im rechten Feld mit den Benutzeranmeldeinformationen angezeigt werden, wobei LDAP oben und LOCAL unten angezeigt wird, versucht Local EAP, Clients mithilfe der LDAP-Backend-Datenbank zu authentifizieren. Wenn die LDAP-Server nicht erreichbar sind, wird ein 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.

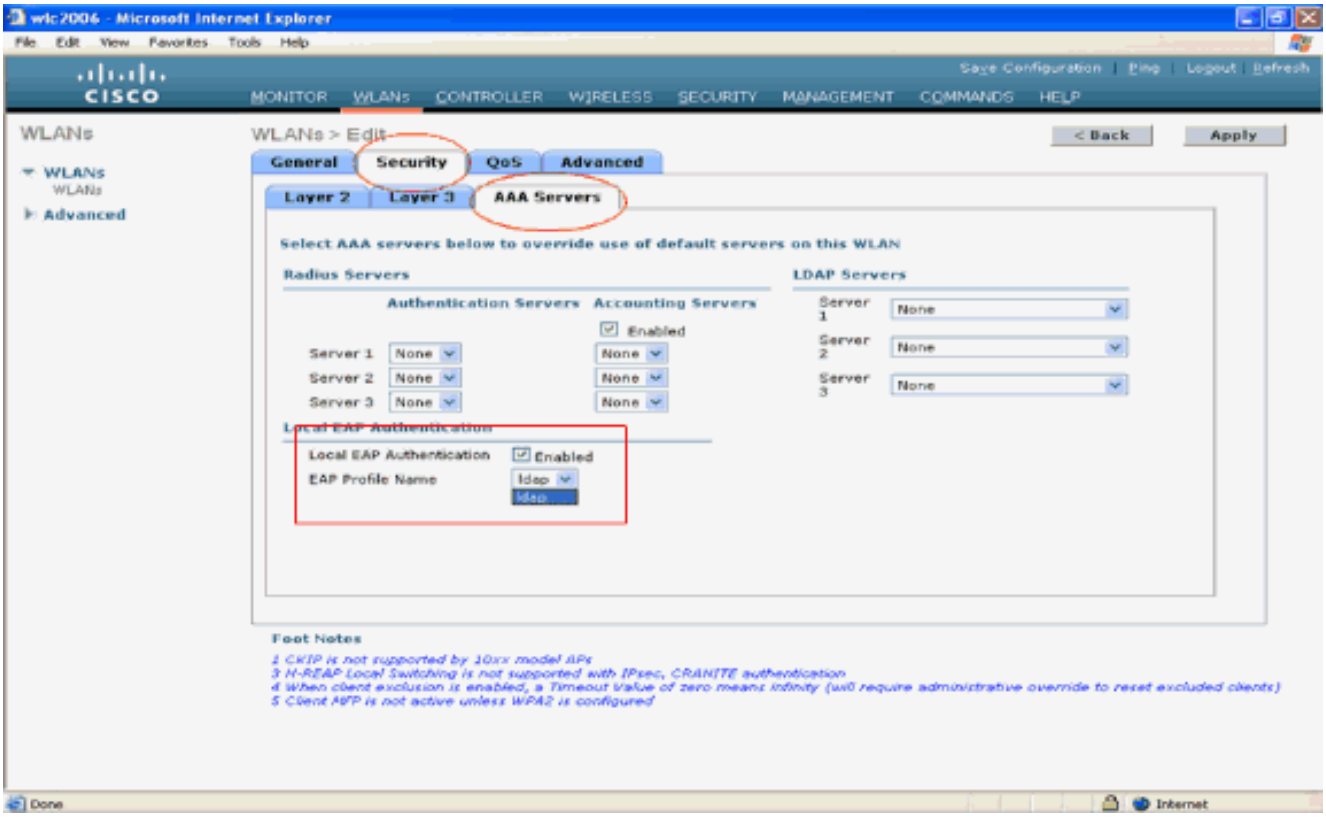
## WLAN auf dem WLC mit lokaler EAP-Authentifizierung konfigurieren

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:

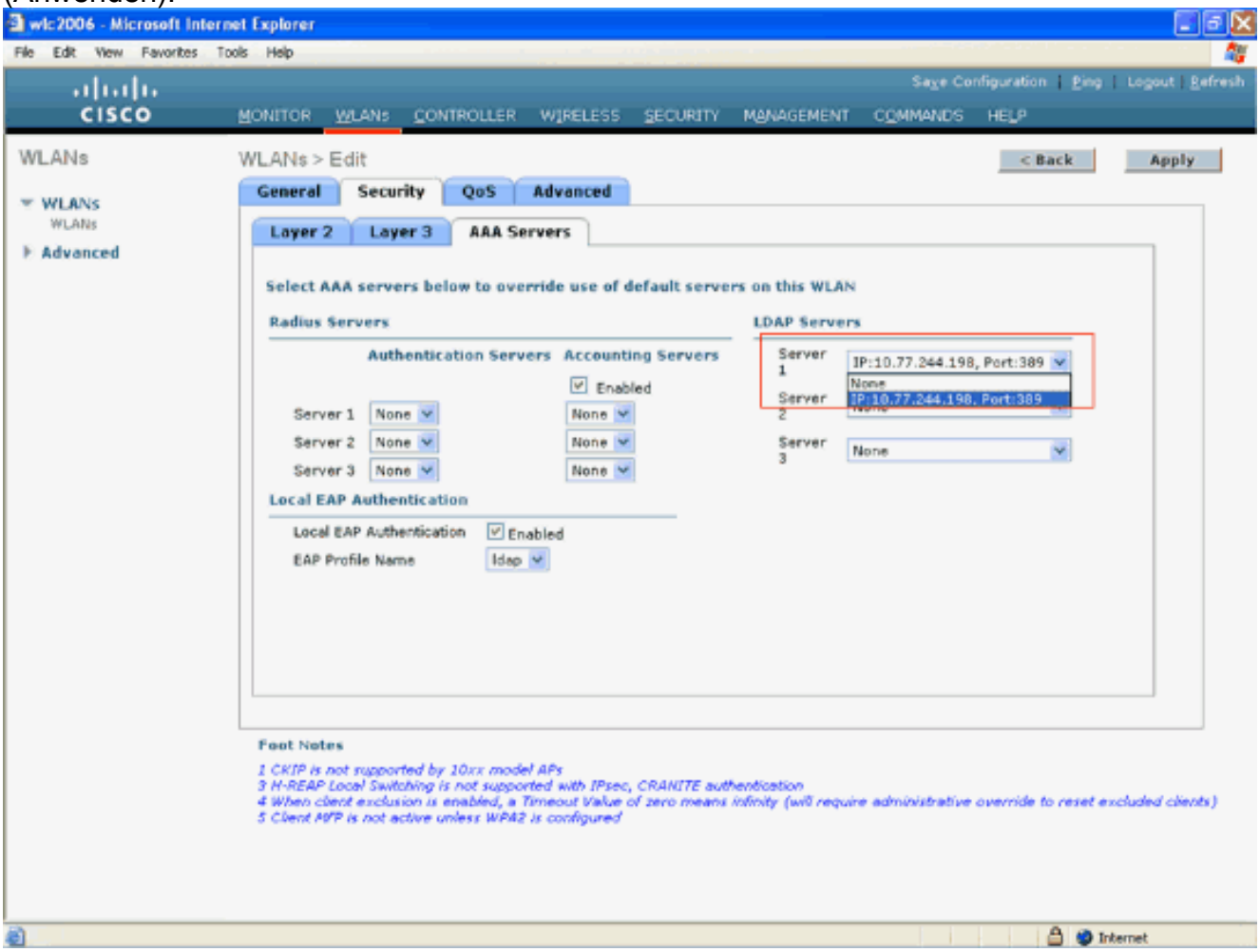
1. Klicken Sie im Hauptmenü des Controllers auf **WLANs**, um zur Konfigurationsseite für WLANs zu wechseln. Klicken Sie auf der Seite "WLANs" auf **Neu**, um ein neues WLAN zu erstellen. In diesem Beispiel wird ein neuer WLAN-**LDAP** erstellt.Klicken Sie auf **Apply**. Der nächste Schritt besteht darin,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



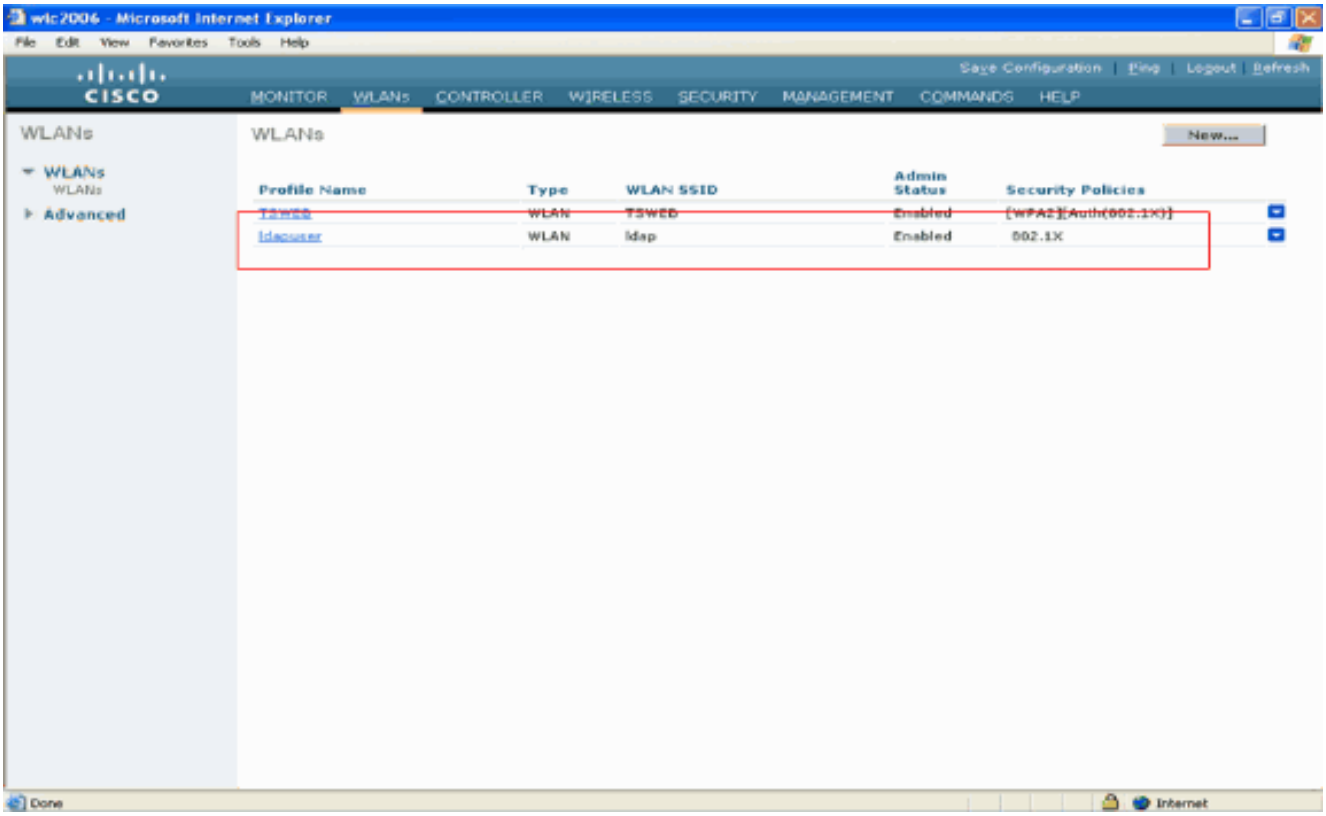

3. Klicken Sie auf **Sicherheit**, um die sicherheitsrelevanten Parameter für dieses WLAN zu konfigurieren. In diesem Beispiel wird Layer-2-Sicherheit als 802.1x mit 104 Bit dynamischem WEP verwendet.**Hinweis:** In diesem Dokument wird 802.1x mit dynamischem WEP als Beispiel verwendet. Es wird empfohlen, 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 **ldap** 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.



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).




6. Die neue WLAN-ldapwurde 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.




# 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 **ldapuser** 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.

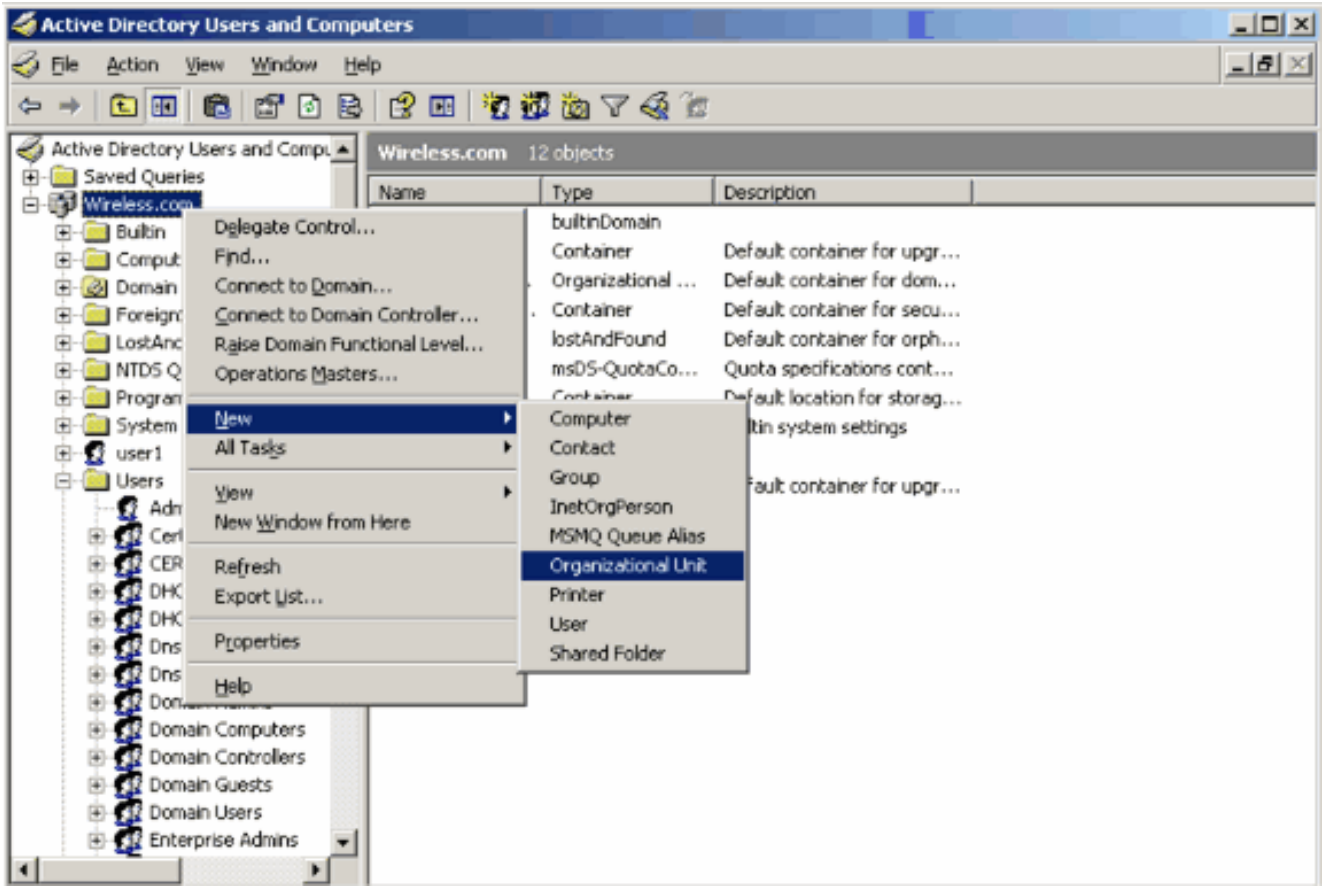
Die in diesem Beispiel verwendete Domäne ist **wireless.com**.

### Erstellen einer Benutzerdatenbank unter einer Organisationseinheit

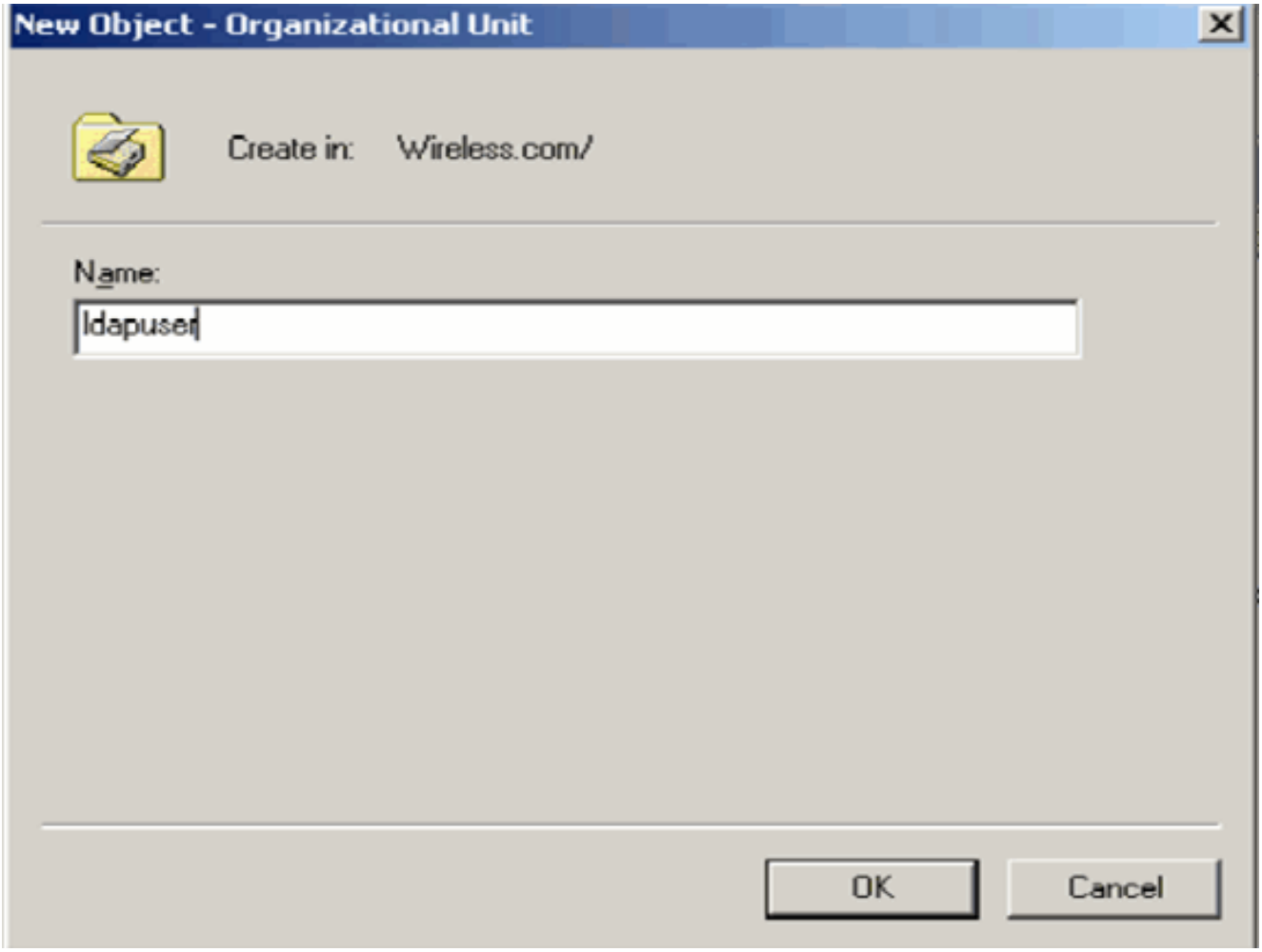
In diesem Abschnitt wird erläutert, wie Sie eine neue OU in Ihrer Domäne erstellen und einen neuen Benutzer auf dieser OU erstellen.

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.

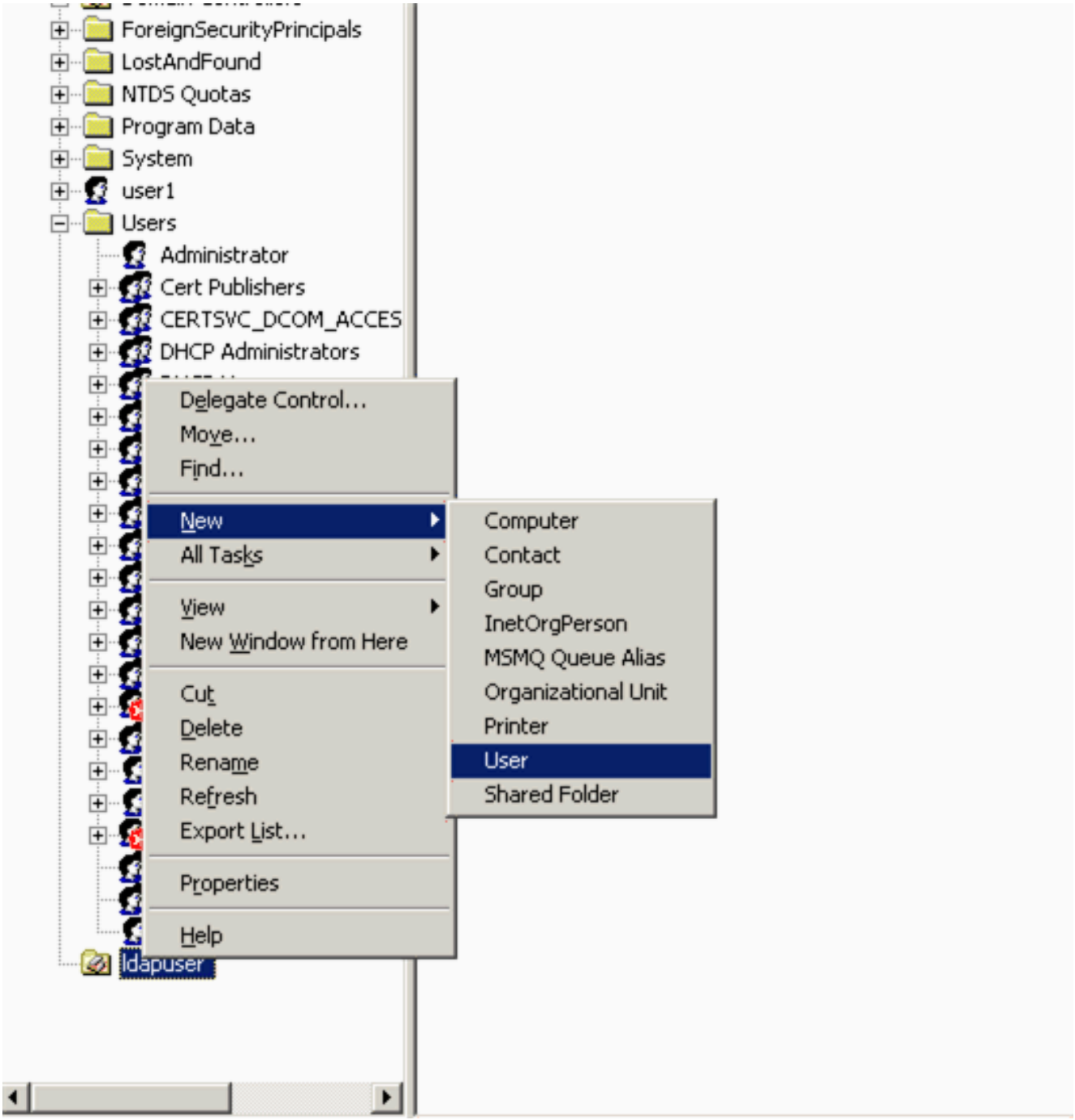



3. Weisen Sie dieser OU einen Namen zu, und klicken Sie auf **OK**.

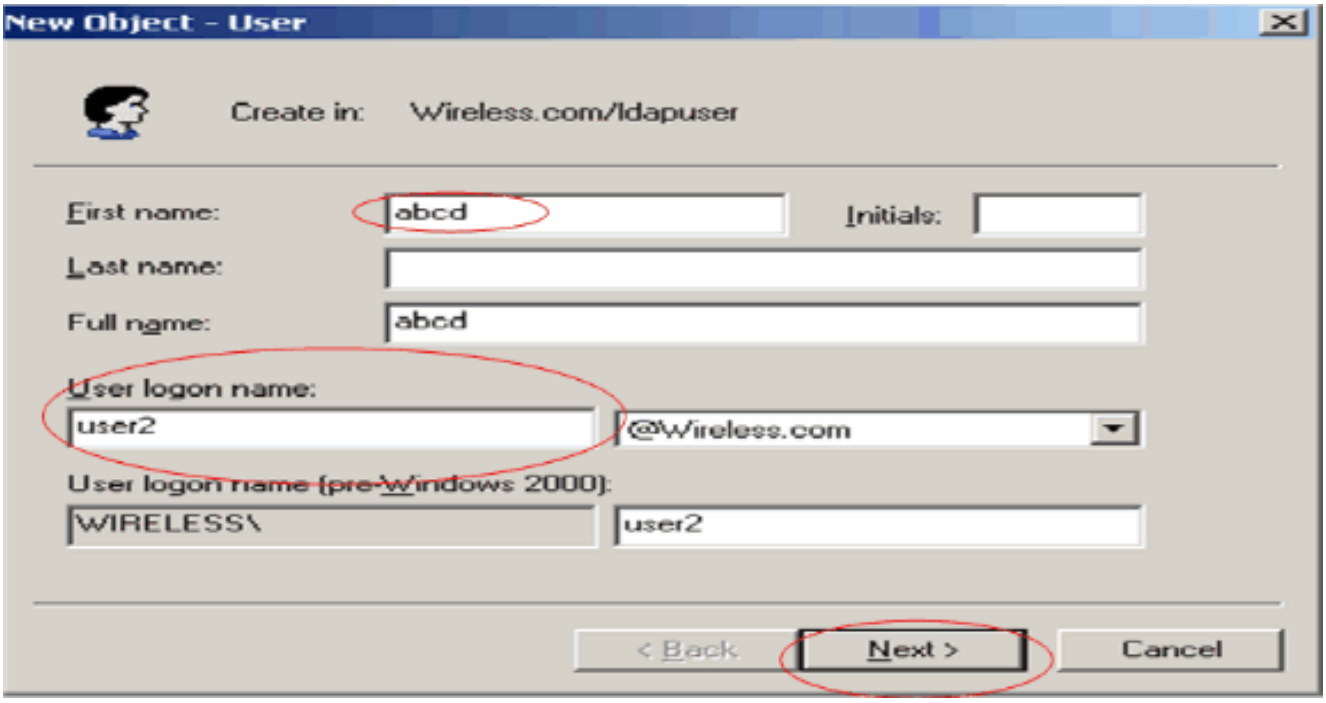



Nachdem nun der neue OU **ldapuser** auf dem LDAP-Server erstellt wurde, besteht der nächste Schritt darin, user **user2** unter dieser OU zu erstellen. Gehen Sie wie folgt vor, um dieses Ziel zu erreichen:

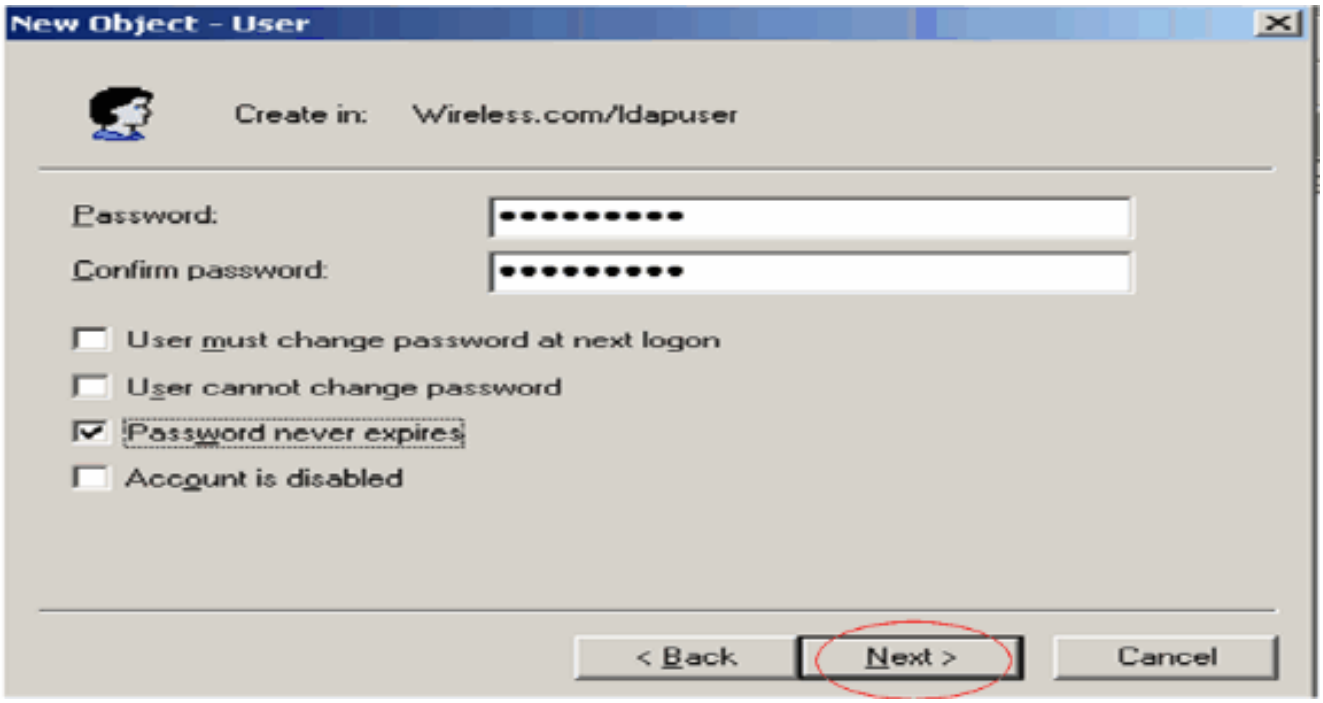
1. Klicken Sie mit der rechten Maustaste auf die neu erstellte Organisationseinheit. Wählen Sie **Neu > Benutzer** aus den sich ergebenden Kontextmenüs, um einen neuen Benutzer zu erstellen.



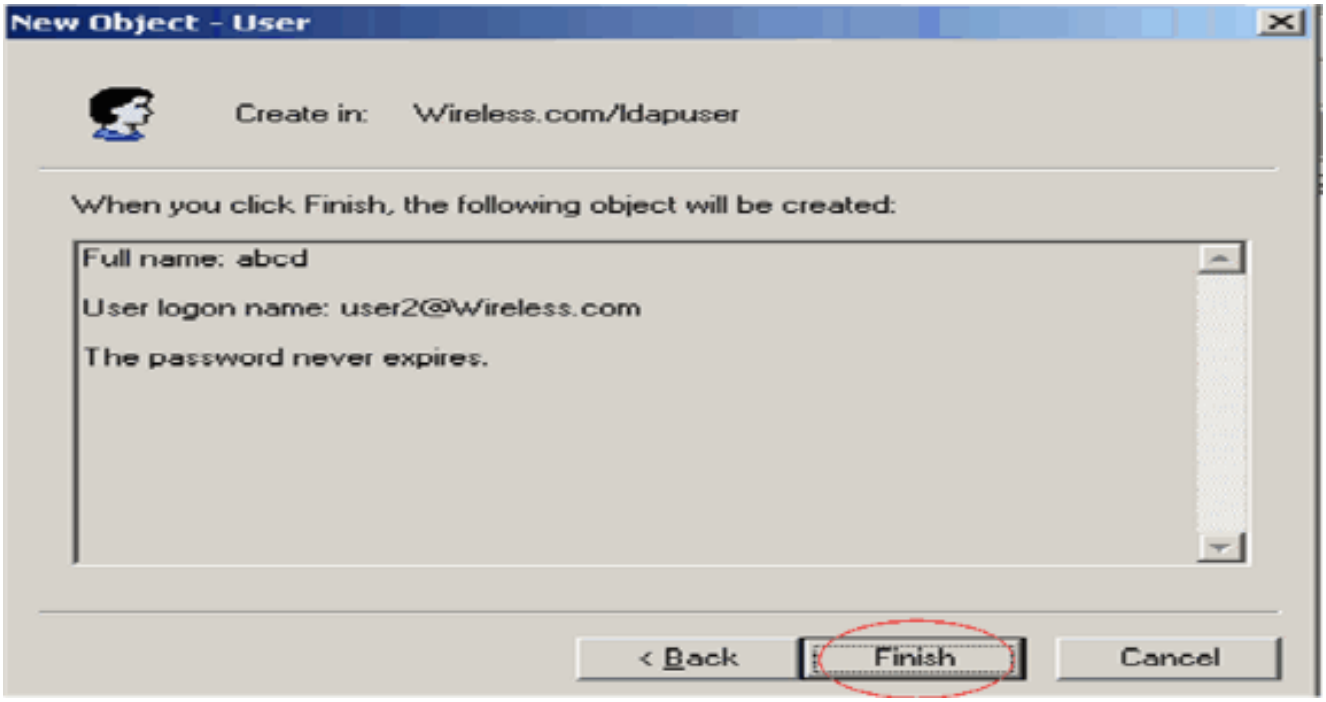

2. Füllen Sie auf der Seite für die Benutzereinrichtung die erforderlichen Felder aus, wie in diesem Beispiel gezeigt. In diesem Beispiel ist **user2** der Benutzername.Dies ist der Benutzername, der in der LDAP-Datenbank für die Authentifizierung des Clients überprüft wird. In diesem Beispiel wird **abcd**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




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




4. Klicken Sie auf Beenden.Ein neuer Benutzer **user2** wird unter der OU ldapuser **erstellt**. Die Benutzeranmeldeinformationen sind:Benutzername: **user2**Kennwort: **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

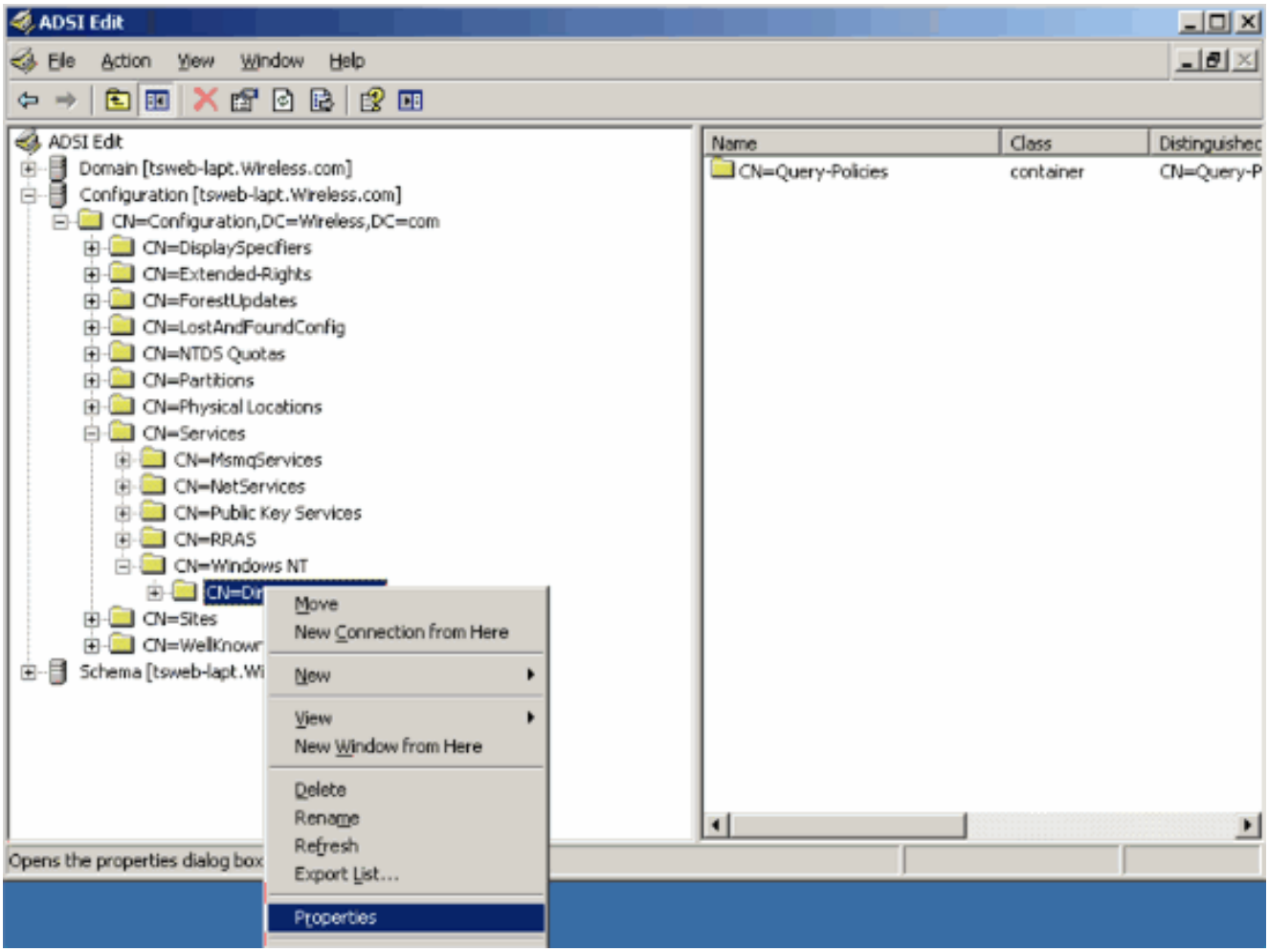
Führen Sie die Schritte in diesem Abschnitt aus, um einen Benutzer für den LDAP-Zugriff zu konfigurieren.

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

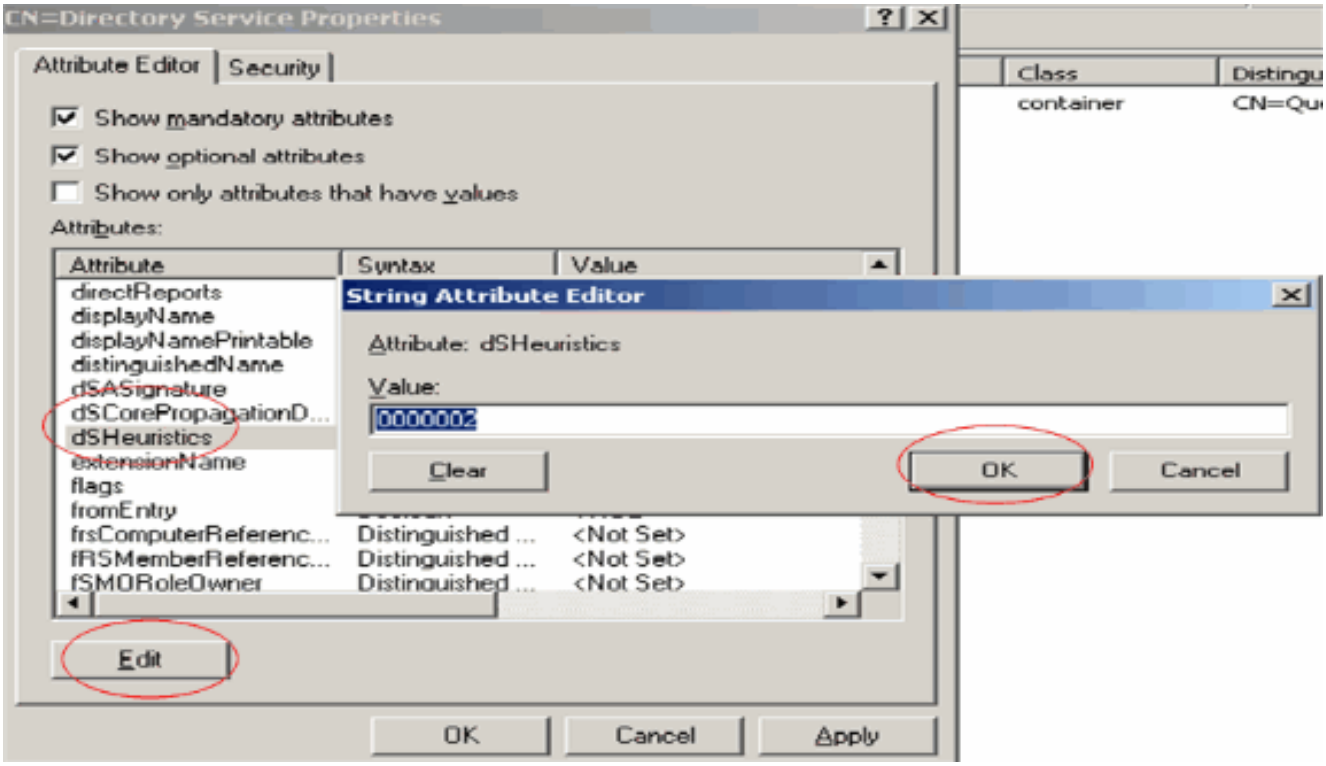
Damit Anwendungen von Drittanbietern über LDAP auf Windows 2003 AD zugreifen können, muss die Funktion "Anonyme Bindung" unter Windows 2003 aktiviert sein. Standardmäßig sind anonyme LDAP-Vorgänge auf Windows 2003-Domänencontrollern nicht zulässig.

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

1. Starten Sie das **ADSI Edit**-Tool über Start > Ausführen > Typ: **ADSI Edit.msc**. Dieses Tool ist Teil der Windows 2003-Supporttools.
2. Erweitern Sie im Fenster "ADSI Edit" die Stammdomäne (Configuration [tsweb-lapt.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.**

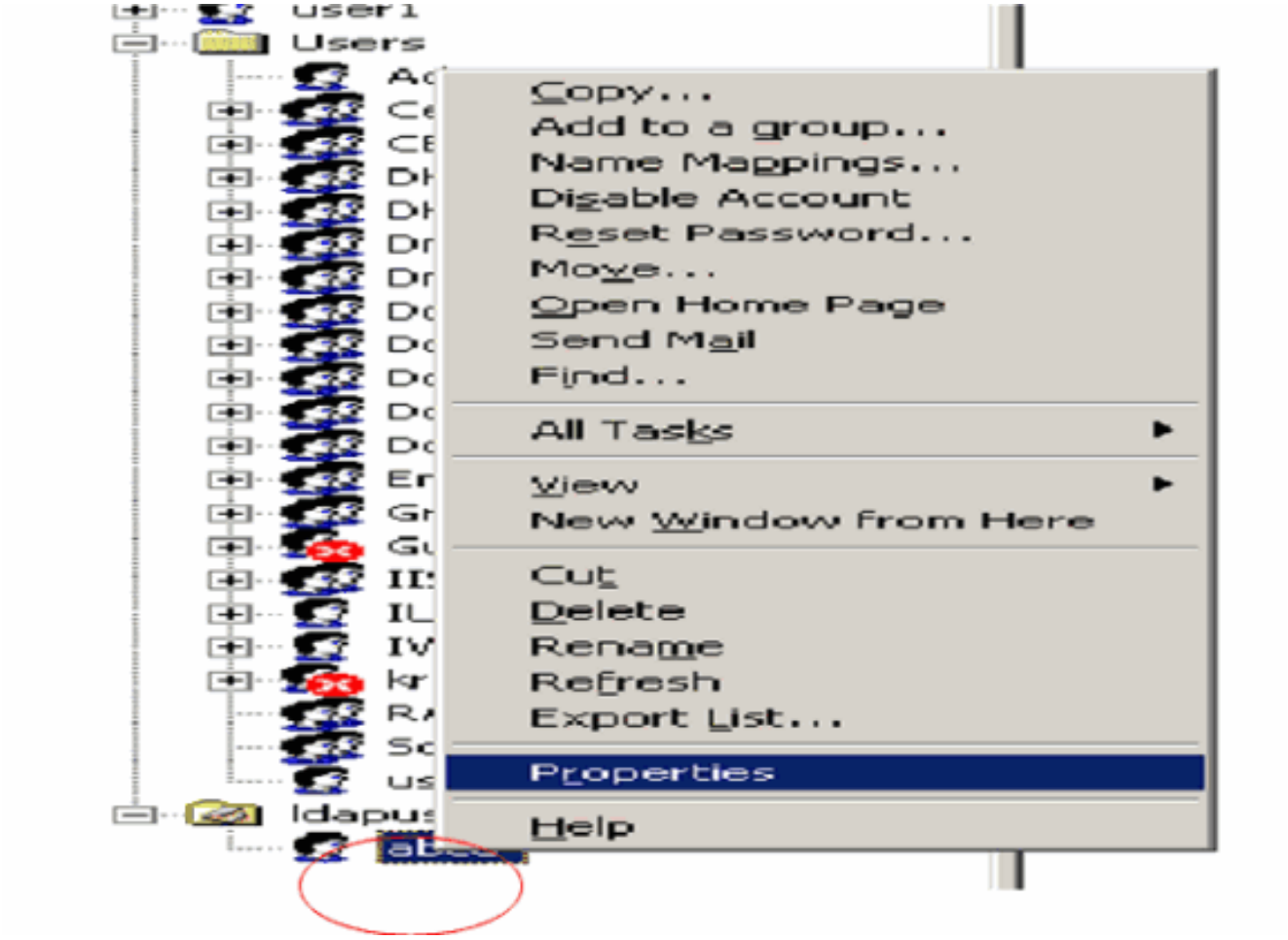



**Hinweis:** Wenn dieses Attribut bereits einen Wert enthält, stellen Sie sicher, dass Sie nur das siebte Zeichen von links ändern. Dies ist das einzige Zeichen, das geändert werden muss, um anonyme Bindungen zu aktivieren. Wenn der aktuelle Wert beispielsweise "0010000" ist, müssen Sie ihn in "0010002"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

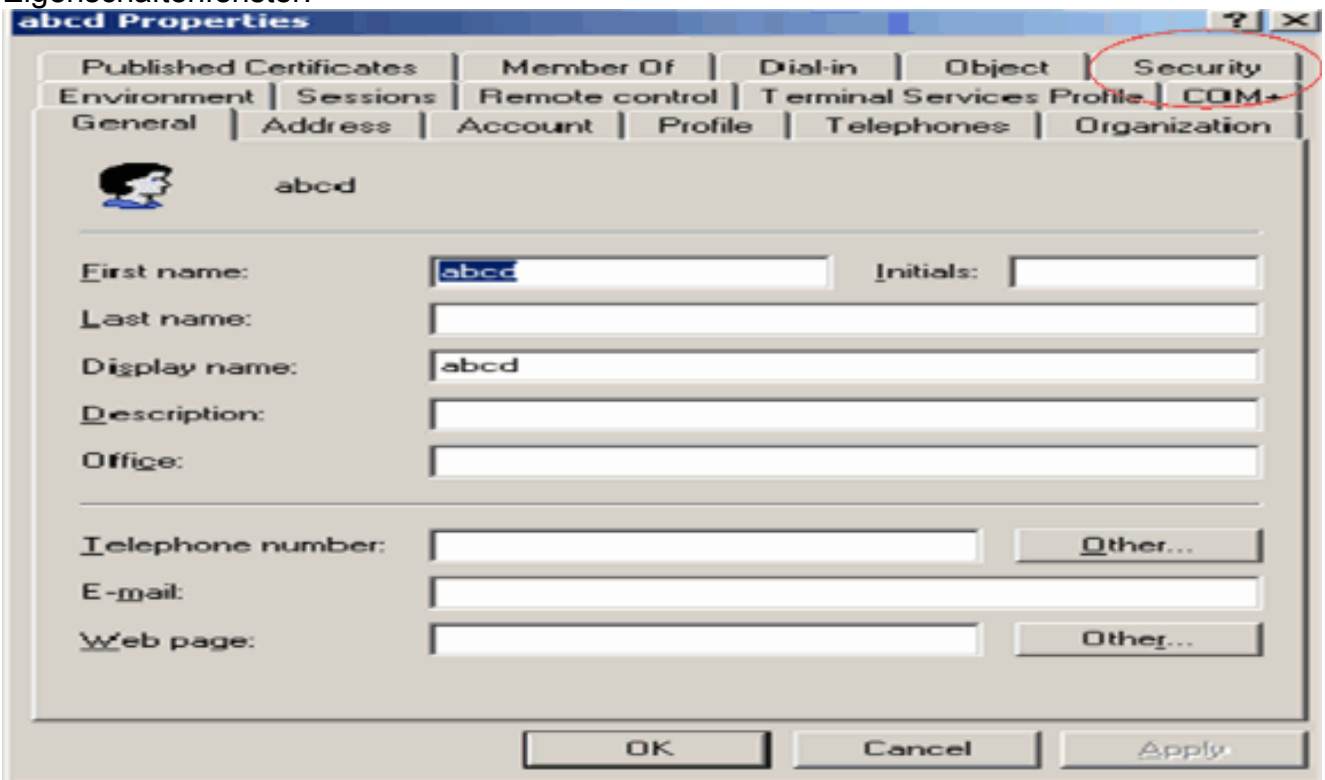
## ANONYMER ANMELDEZUGRIFF für Benutzer "user2"

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

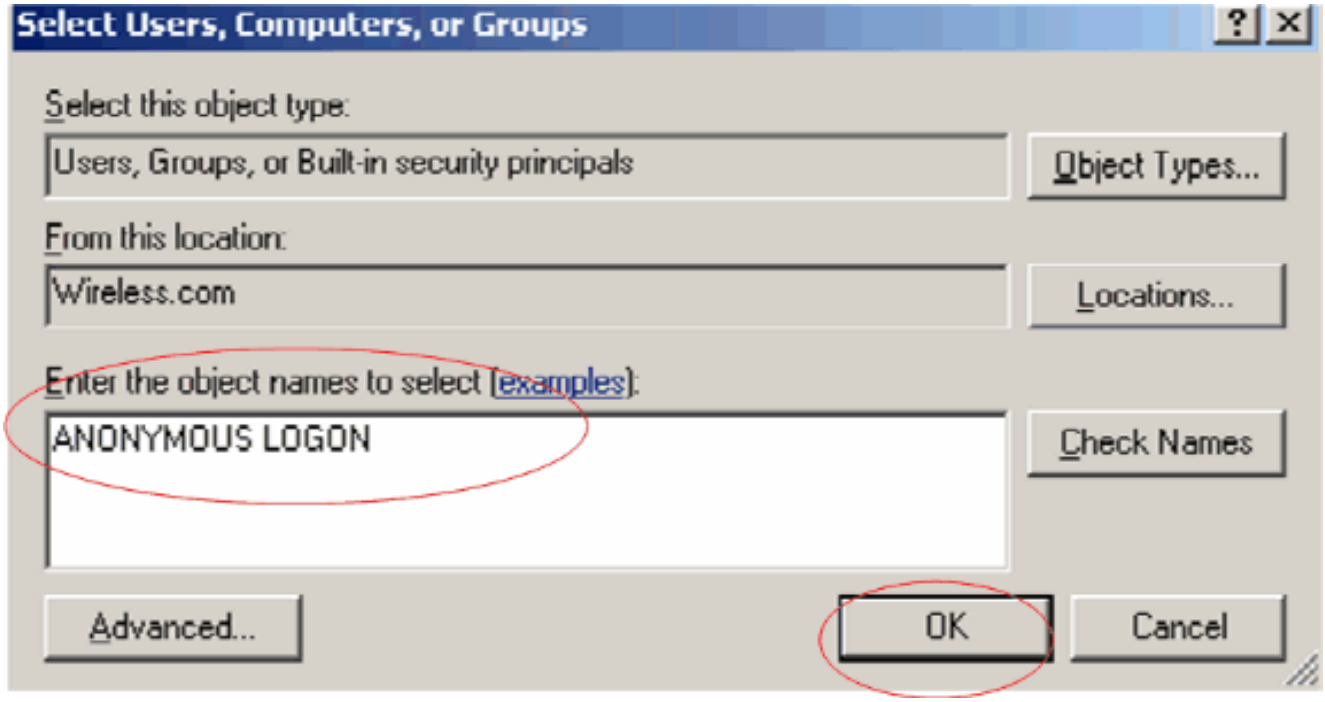
1. Öffnen Sie **Active Directory-Benutzer** und -**Computer**.
2. Vergewissern Sie sich, dass **Erweiterte Funktionen anzeigen** aktiviert ist.
3. Navigieren Sie zum Benutzer **user2**, und klicken Sie mit der rechten Maustaste darauf. Wählen Sie im Kontextmenü die Option **Eigenschaften** aus. Dieser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



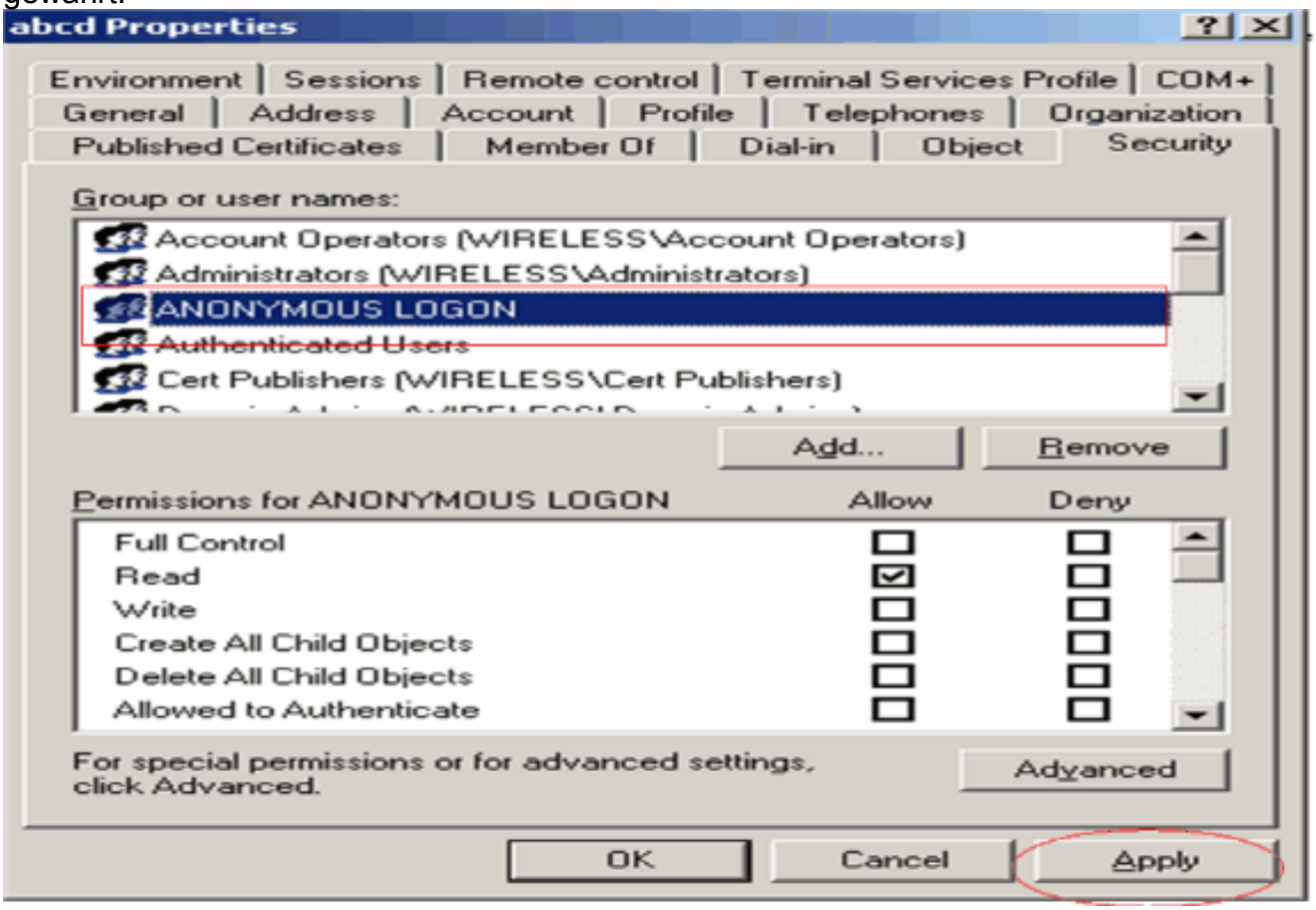

4. Gehen Sie zu **Sicherheit** im abcd-Eigenschaftenfenster.




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



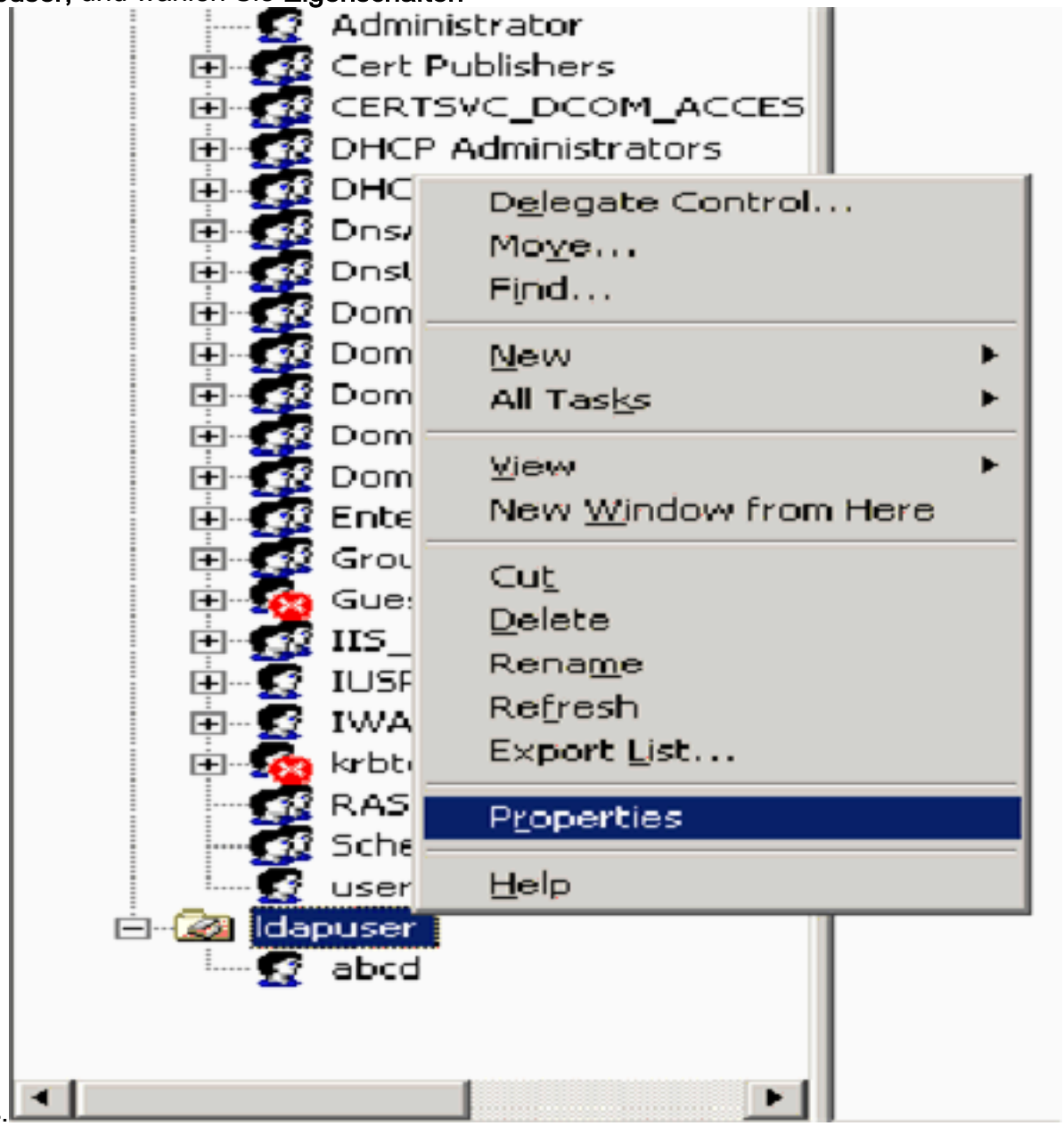

7. In der ACL werden Sie feststellen, dass **ANONYME LOGON** Zugriff auf einige Eigenschaftensätze des Benutzers hat. Klicken Sie auf **OK**. Der ANONYME LOGON-Zugriff wird diesem Benutzer
gewährt.




## Erteilen der Inhaltsberechtigung für die Organisationseinheit

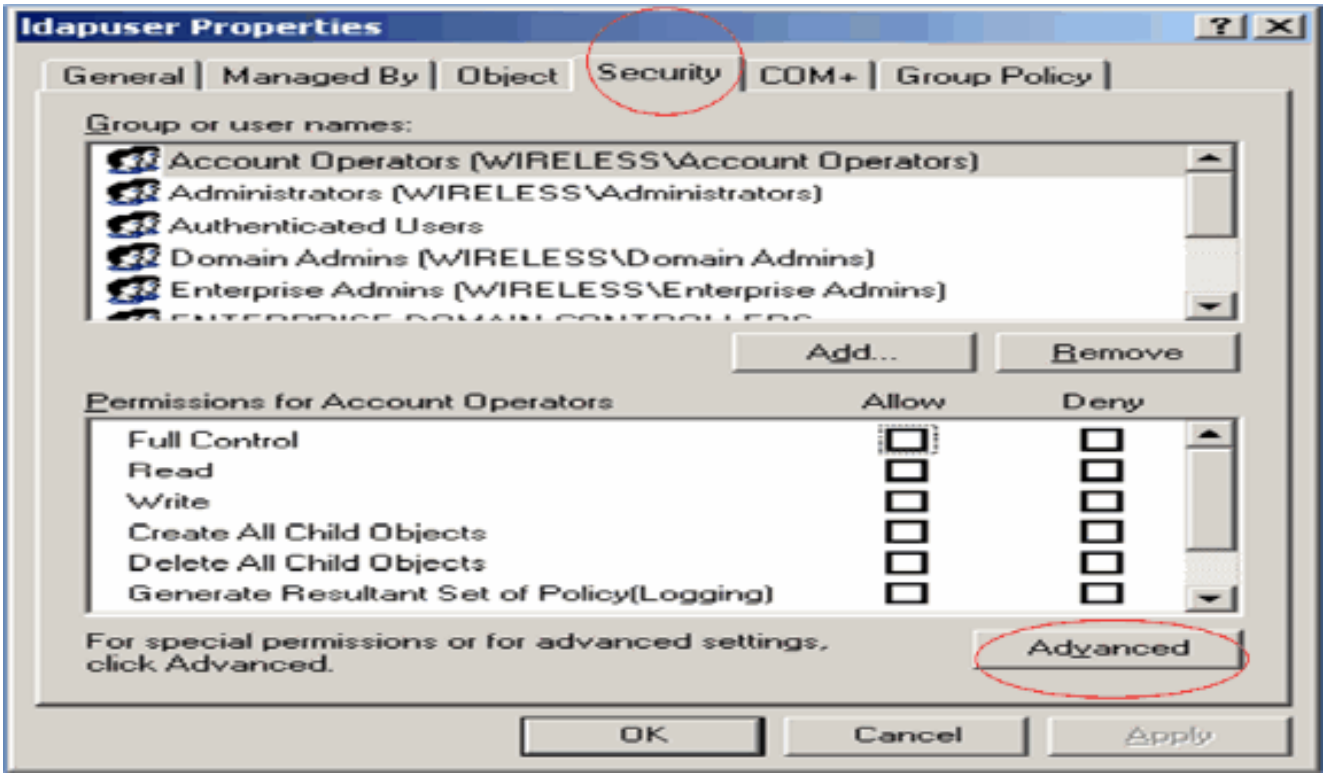
Der nächste Schritt besteht darin, der **ANONYMEN ANMELDUNG** in der Organisationseinheit, in der sich der Benutzer befindet, mindestens die Berechtigung **Inhalt** auflisten zu gewähren. In diesem Beispiel befindet sich "user2" in der OU "ldapuser". Gehen Sie wie folgt vor, um dieses Ziel zu erreichen:

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

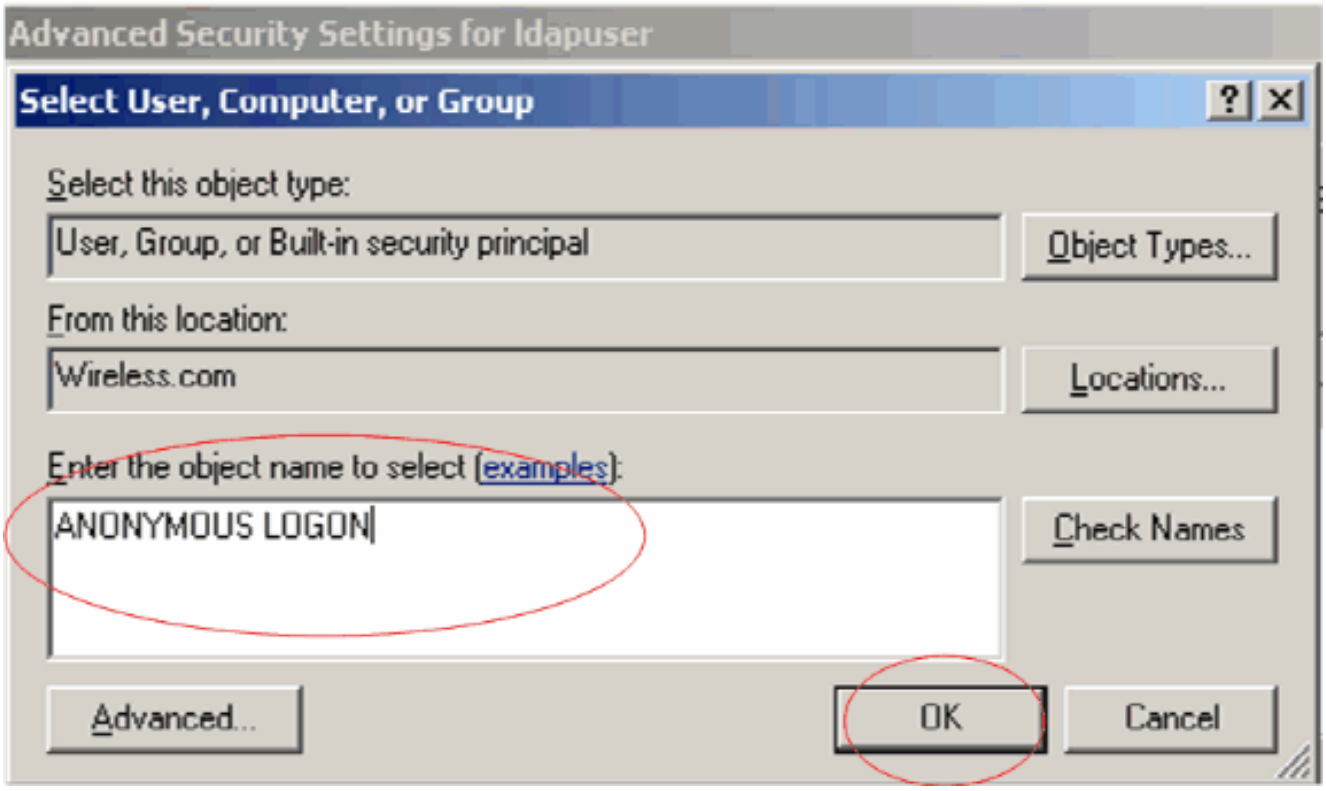



**aus**.

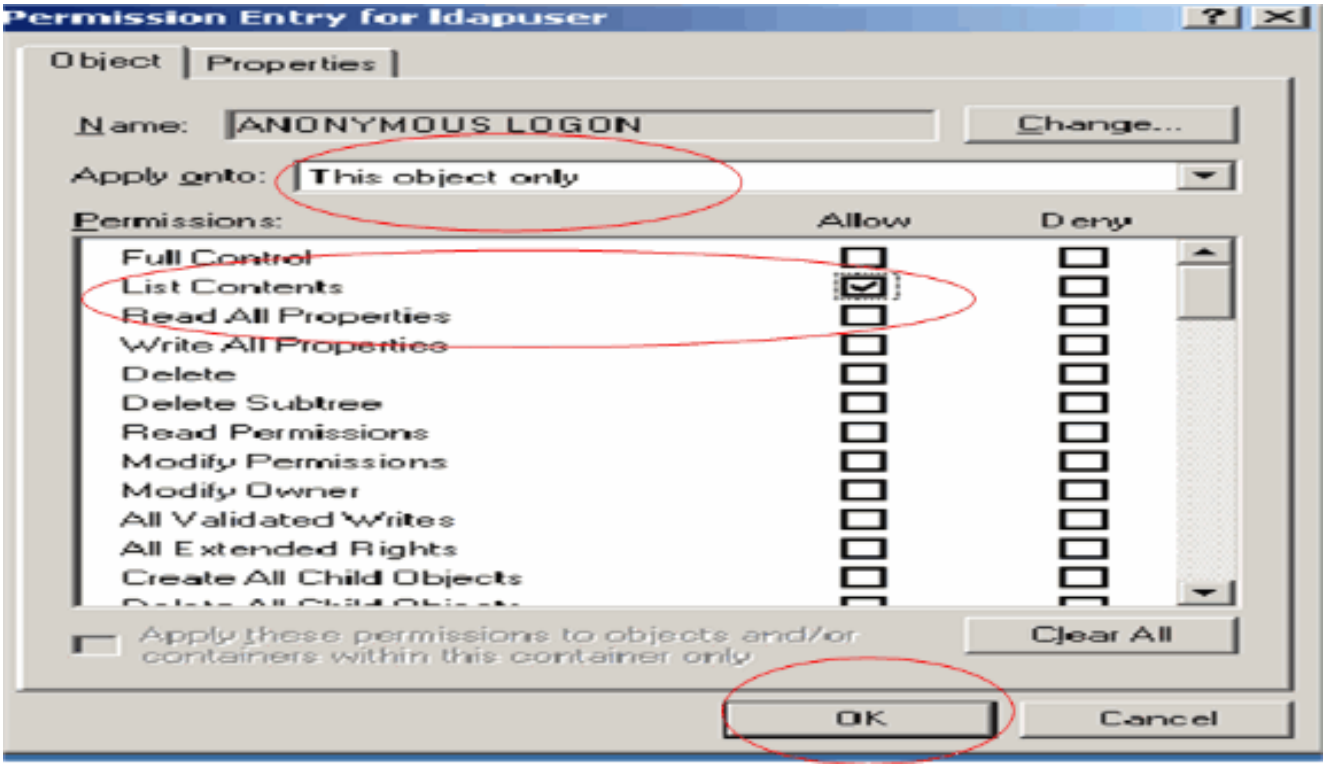
2. Klicken Sie auf **Sicherheit** und dann auf **Erweitert**.




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




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.

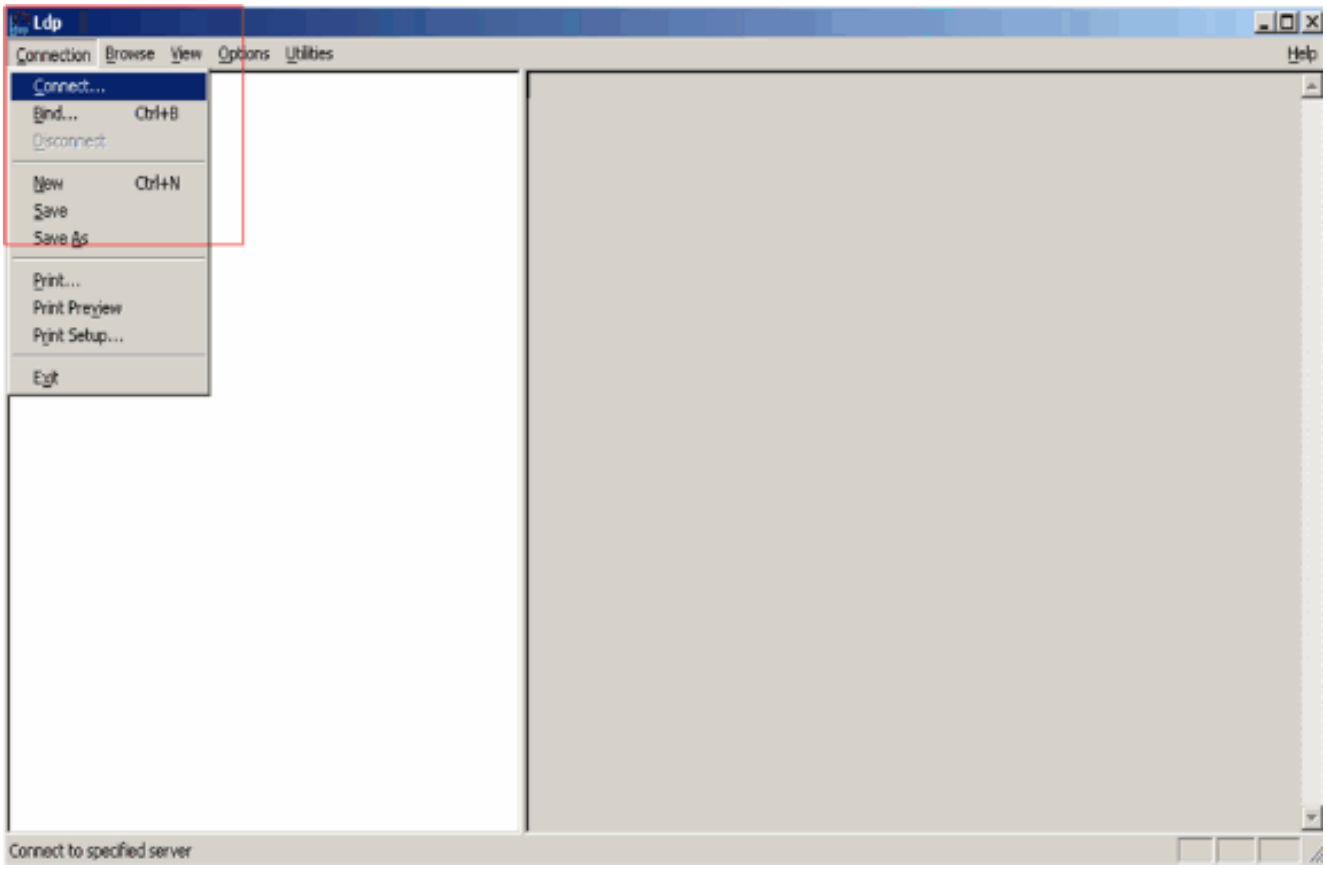



## Verwenden von LDP zum Identifizieren der Benutzerattribute

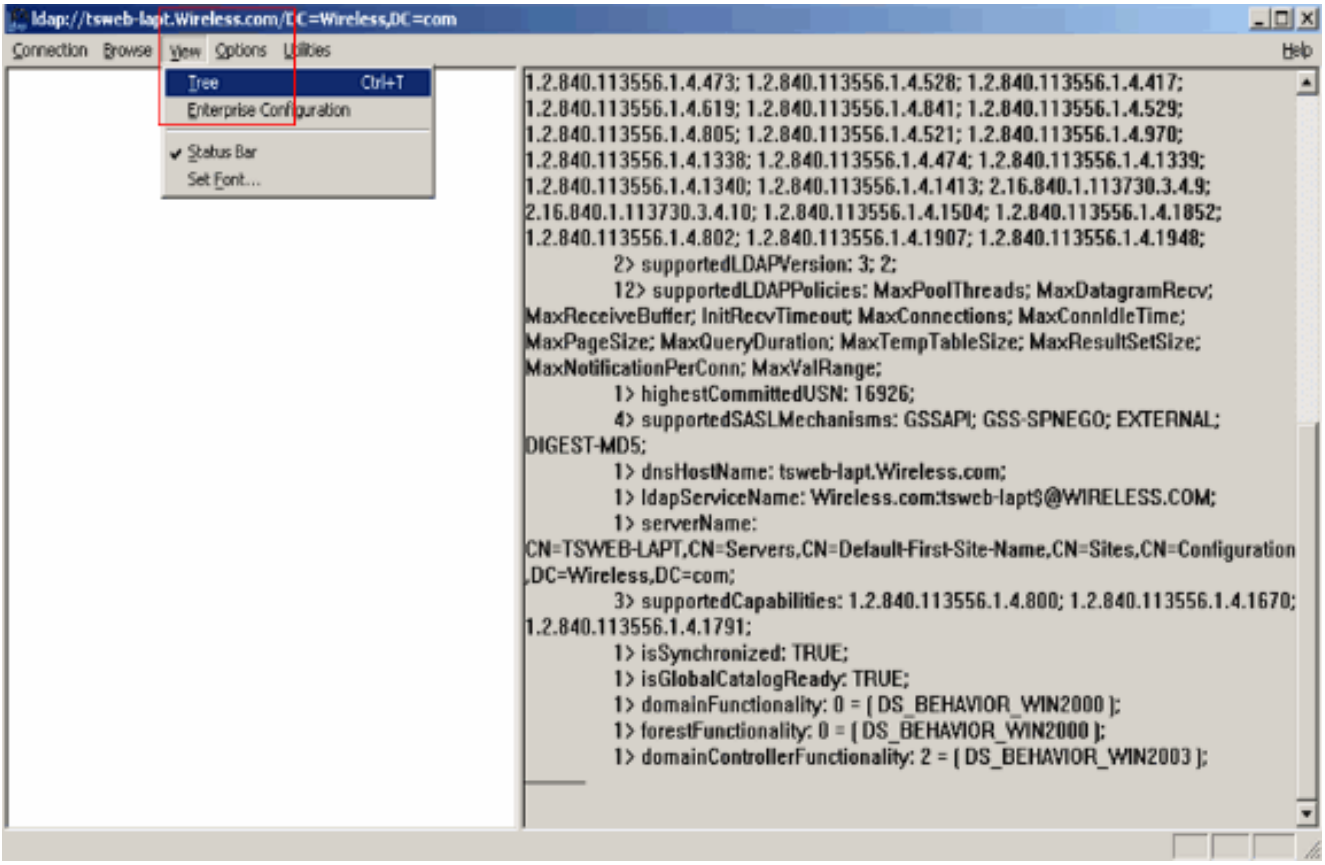
Bei diesem GUI-Tool handelt es sich um einen LDAP-Client, mit dem Benutzer Vorgänge (z. B. Verbinden, Binden, Suchen, Ändern, Hinzufügen, Löschen) in einem beliebigen LDAP-kompatiblen Verzeichnis (z. B. Active Directory) durchführen können. LDP wird verwendet, um in Active Directory gespeicherte Objekte 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.
2. 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.

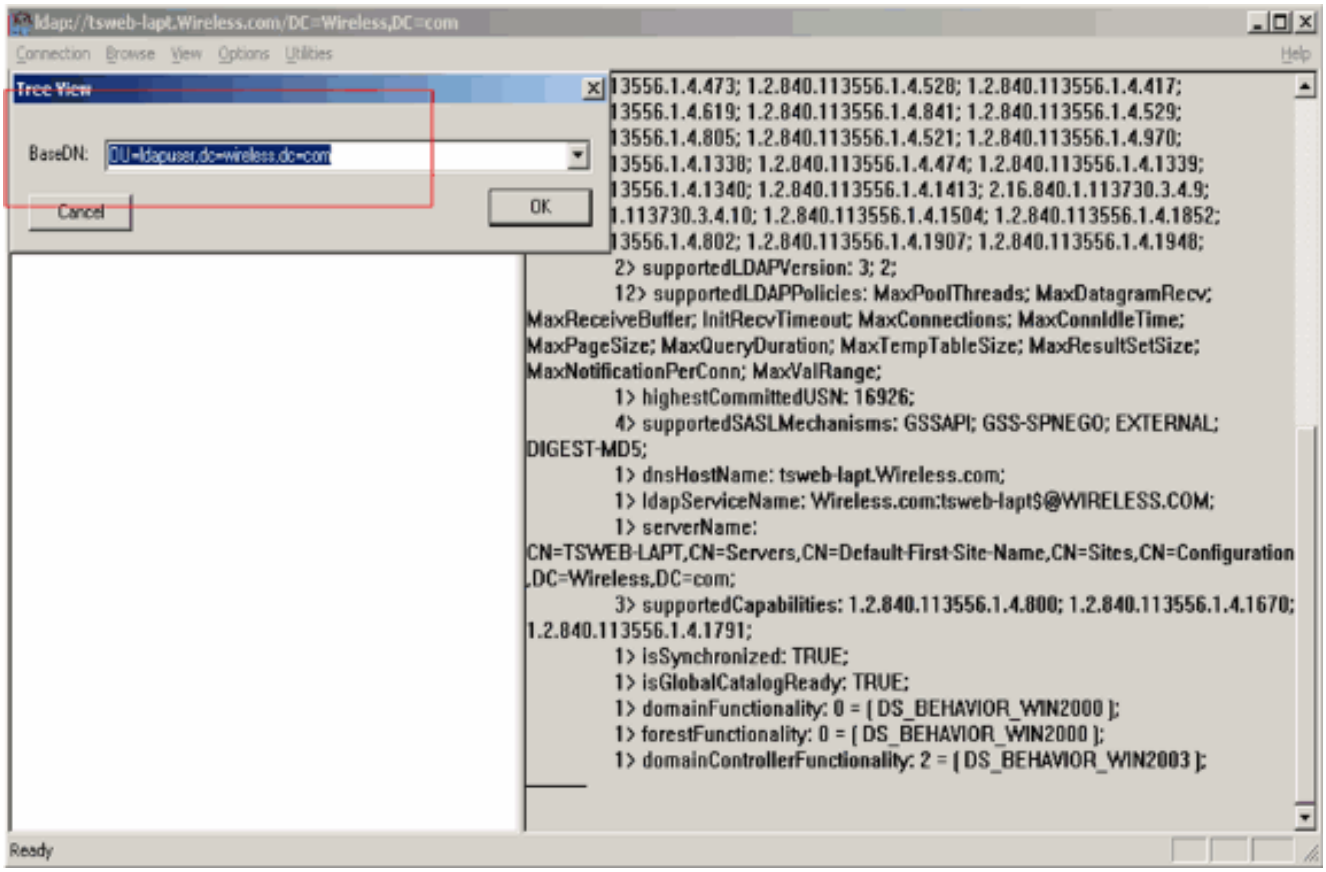



3. Wenn Sie mit dem LDAP-Server verbunden sind, wählen Sie im Hauptmenü die Option **Ansicht** aus, und klicken Sie auf **Baum**.

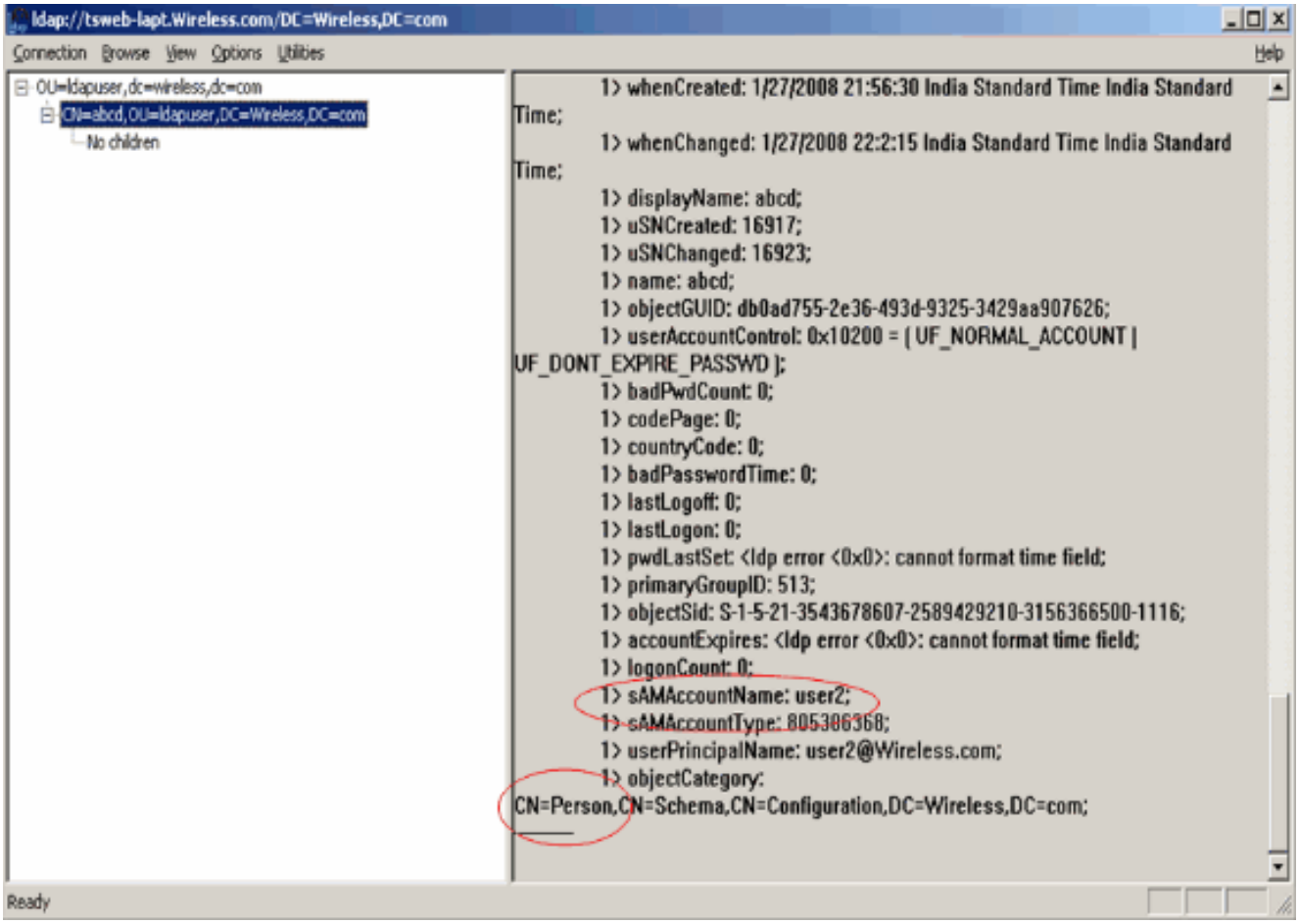



4. Geben Sie im resultierenden Fenster Baumansicht die Basis-DN des Benutzers ein. In diesem Beispiel **befindet sich user2 unter der OU "ldapuser" unter der Domäne Wireless.com**. Daher ist die BaseDN für **Benutzer**2 **OU=ldapuser, dc=wireless, dc=com**. Klicken Sie auf

OK.




5. Auf der linken Seite des LDP-Browsers wird der gesamte Tree angezeigt, der unter der angegebenen BaseDN angezeigt wird (**OU=ldapuser, 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:



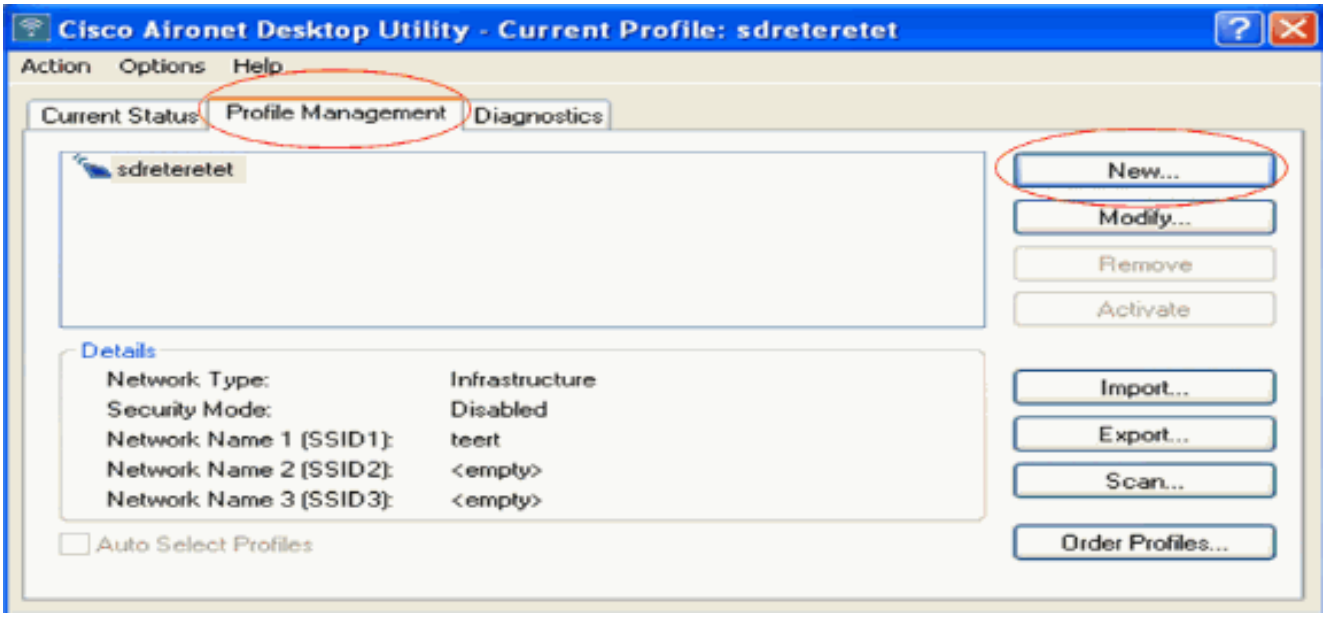

Beachten Sie in diesem Beispiel die eingekreisten Felder rechts.

6. Wie im Abschnitt WLC mit LDAP-Serverdetails konfigurieren 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.

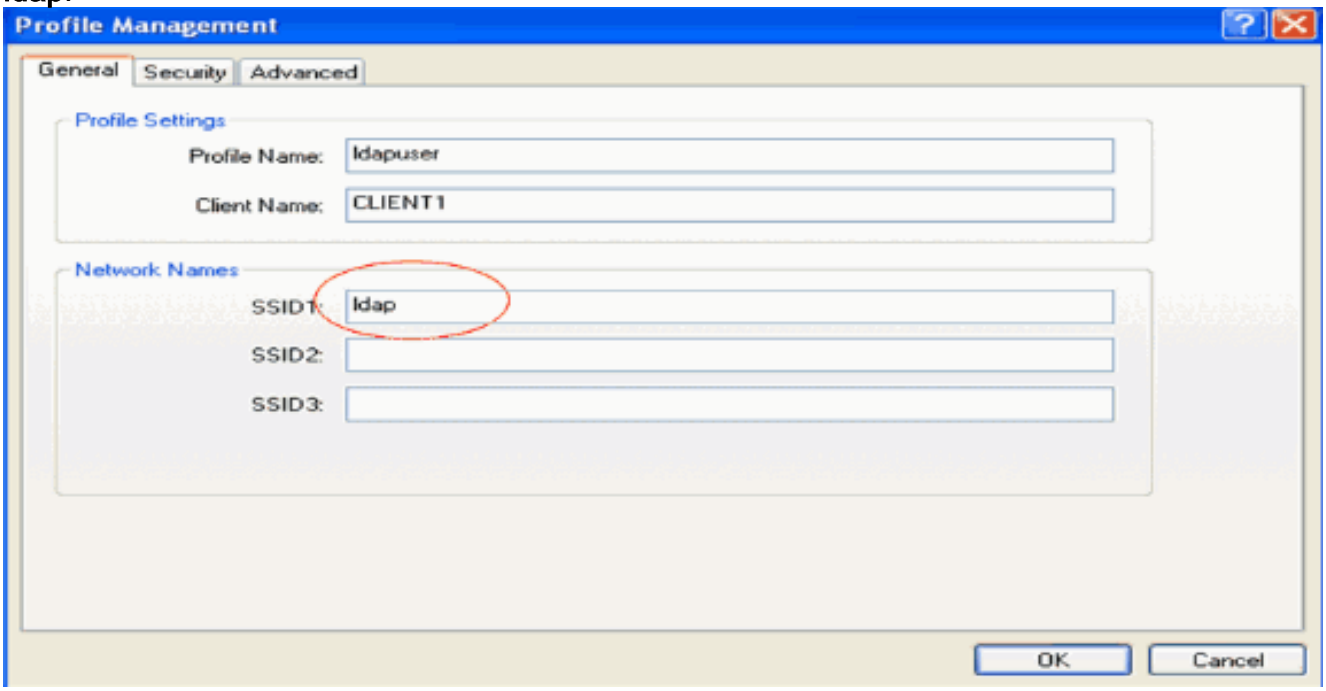
## Wireless-Client konfigurieren

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

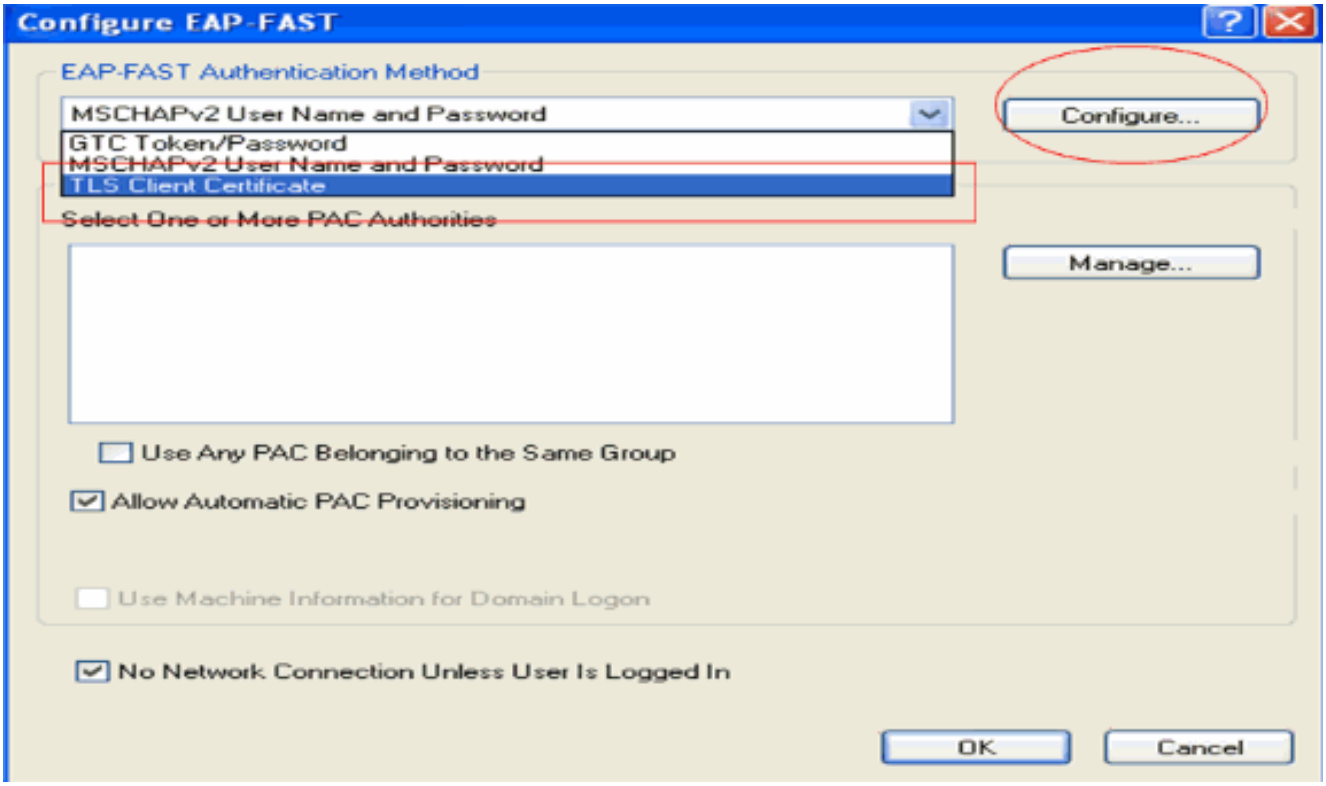
1. Starten Sie das **Cisco Aironet Desktop Utility** (ADU). Klicken Sie im ADU-Hauptfenster auf **Profile Management > New** (Profilverwaltung > Neu), um ein neues Wireless-Clientprofil zu erstellen.



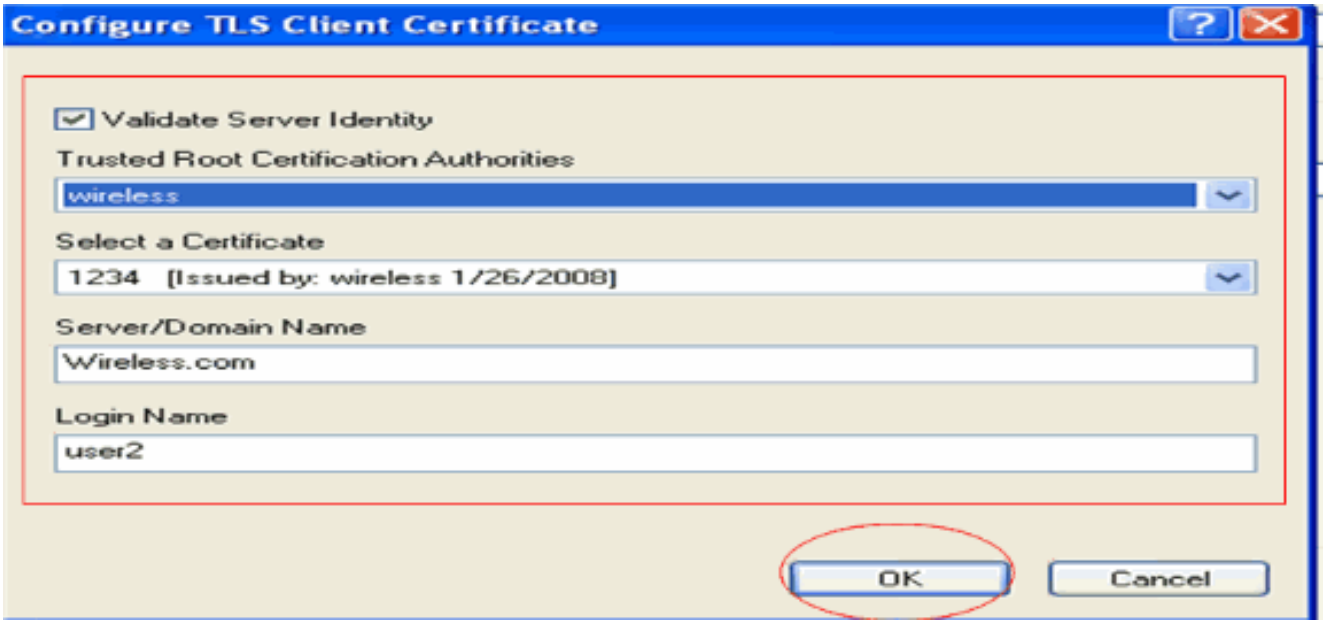

2. Geben Sie einen Profilnamen an, und weisen Sie diesem Profil einen SSID-Namen zu. Dieser SSID-Name muss mit dem Namen identisch sein, der auf dem WLC konfiguriert wurde. In diesem Beispiel lautet der SSID-Name **ldap**.




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**.




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 Generate the Root CA certificate for the Client in diesem Dokument erläutert) als vertrauenswürdige Stammzertifizierungsstelle aus.Wählen Sie das auf dem Client installierte Gerätezertifikat (wie im Abschnitt Generate a Device Certificate for the Client (Gerätezertifikat für den Client generieren) in diesem Dokument erläutert) als Clientzertifikat aus.Klicken Sie auf **OK**.In diesem Beispiel wird dieser Schritt
erläutert:




Das Profil des Wireless-Clients wird erstellt.

## Überprüfung

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

1. Aktivieren Sie die **LDAP**-SSID auf der ADU.
2. 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 ldap 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 ldap 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
(436973636f000000000000000000000)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Sending Start
```

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

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Process Response
(EAP handle = 0x1B000009)

**Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT:**
**Received TLS record type: Handshake in state: Start**

**Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Local certificate found**

**Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Hello handshake**

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT:
TLS_DHE_RSA_AES_128_CBC_SHA proposed...

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Proposed ciphersuite(s):

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_RSA_WITH_RC4_128_SHA

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Selected ciphersuite:

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Building Provisioning Server Hello

**Sun Jan 27 09:38:29 2008: eap_fast_crypto.c-EVENT:**
**Starting Diffie Hellman phase 1 ...**

**Sun Jan 27 09:38:30 2008: eap_fast_crypto.c-EVENT:**
**Diffie Hellman phase 1 complete**

Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: DH signature length = 128

Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: Sending Provisioning Serving Hello

Sun Jan 27 09:38:30 2008: eap_fast.c-EVENT: Tx packet fragmentation required

Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet():
EAP Fast NoData (0x2b)

Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet():
EAP Fast NoData (0x2b)

Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet():
EAP Fast NoData (0x2b)

Sun Jan 27 09:38:32 2008: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Reassembling TLS record

**Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Sending EAP-FAST Ack**

.....

.....

.....

**Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:**
**Received TLS record type: Handshake in state: Sent provisioning Server Hello**

**Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:**
**Reading Client Certificate handshake**

**Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 1 to chain**

**Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 2 to chain**

**Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Successfully validated received certificate**

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Rx'd I-ID:
"EAP-FAST I-ID" from Peer Cert

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:
Reading Client Key Exchange handshake

**Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT:**
**Starting Diffie Hellman phase 2 ...**

**Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT:**
**Diffie Hellman phase 2 complete.**

Sun **Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:**
**Reading Client Certificate Verify handshake**

**Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT:**
**Sign certificate verify succeeded (compare)**

.....

.....

.....

.....
.

- 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) Processing keys success
```

- Um die im WLC installierten Zertifikate anzuzeigen, die für die lokale Authentifizierung verwendet werden sollen, geben Sie den Befehl **show local-auth Certificates (Zertifikate für lokale Authentifizierung anzeigen**) in der WLC-CLI ein. Hier ein Beispiel:(Cisco Controller) **>Zertifikate für 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: O=cisco, CN=ciscowlc123

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

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


Certificate issuer ............................. cisco

  CA certificate:

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

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

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

   Device certificate:

            Not installed.
```

- 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 timeout .............................. 300


Configured EAP profiles:

    Name ........................................ ldapuser

      Certificate issuer ........................ vendor

      Peer verification options:

        Check against CA certificates ........... Enabled

        Verify certificate CN identity .......... Disabled

        Check certificate date validity ......... Disabled

      EAP-FAST configuration:

        Local certificate required .............. Yes

        Client certificate required ............. Yes

      Enabled methods ........................... fast

      Configured on WLANs ....................... 2


EAP Method configuration:

    EAP-FAST:

--More-- or (q)uit

      Server key ................................ <hidden>

      TTL for the PAC ........................... 10

      Anonymous provision allowed ............... No

      ..........................................

      ..........................................

      Authority Information ..................... Cisco A-ID
```

# 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
- Konfigurationsanleitung für den Cisco Wireless LAN Controller - Konfigurieren von Sicherheitslösungen
- 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
- Cisco Secure Services Client mit EAP-FAST-Authentifizierung
- Wireless LAN Controller (WLC) – Häufig gestellte Fragen
- Controller Wireless LAN Controller (WLC) Fehler und Systemmeldungen FAQ
- Technischer Support und Dokumentation für Cisco Systeme

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.