# Lokale EAP-verificatie op de draadloze LAN-controller met EAP-FAST- en LDAP-serverconfiguratievoorbeeld

## Inhoud



## Inleiding

In dit document wordt uitgelegd hoe u EAP-verificatie (Extensible Verification Protocol) kunt configureren - flexibele verificatie via Secure Tunneling (FAST) lokale EAP-verificatie op een draadloze LAN-controller (WLC). Dit document legt ook uit hoe u de LDAP-server (Lichtgewicht Directory Access Protocol) kunt configureren als de back-end database voor Local EAP om gebruikersreferenties op te halen en de gebruiker te verifiëren.

## Voorwaarden

## Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 4400 Series WLC voor gebruik van firmware 4.2
- Cisco Aironet 1232AG Series lichtgewicht access point (LAP)
- Microsoft Windows 2003-server geconfigureerd als domeincontroller, LDAP-server en Certificate Authority-server.
- Cisco Aironet 802.11 a/b/g clientadapter waarop firmware-release 4.2 wordt uitgevoerd
- Cisco Aironet Desktop Utility (ADU) gebruikt firmware versie 4.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

# Achtergrondinformatie

Lokale EAP-verificatie op draadloze LAN-controllers is geïntroduceerd met versie 4.1.171.0 van de draadloze LAN-controller.

Local EAP is een verificatiemethode waarmee gebruikers en draadloze clients lokaal op de controller kunnen worden geverifieerd. Het is ontworpen voor gebruik in externe kantoren die de verbinding met draadloze clients willen behouden wanneer het backend-systeem verstoord raakt of de externe verificatieserver uitvalt. Wanneer u lokale EAP inschakelt, fungeert de controller als de verificatieserver en de lokale gebruikersdatabase, waardoor de afhankelijkheid van een externe verificatieserver wordt opgeheven. Lokale EAP wint gebruikersreferenties terug uit de lokale gebruikersdatabase of de LDAP-back-end database om gebruikers te verifiëren. Lokale EAP ondersteunt LEAP, EAP-FAST, EAP-TLS, P EAPv0/MSCHAPv2 en PEAPv1/GTC-verificatie tussen de controller en draadloze clients.

Lokale EAP kan een LDAP-server als back-end database gebruiken om gebruikersreferenties op te halen.

Een LDAP backend database stelt de controller in staat om een LDAP-server te bevragen voor de referenties (gebruikersnaam en wachtwoord) van een bepaalde gebruiker. Deze referenties worden vervolgens gebruikt voor de verificatie van de gebruiker.

De LDAP-back-end database ondersteunt deze lokale EAP-methoden:

- EAP-FAST/GTC

- EAP-TLS
- PEAPv1/GTC

LEAP, EAP-FAST/MSCHAPv2 en PEAPv0/MSCHAPv2 worden ook ondersteund, **maar alleen als de LDAP-server is ingesteld om een helder tekstwachtwoord te retourneren**. Microsoft Active Directory wordt bijvoorbeeld niet ondersteund omdat het geen clear-text wachtwoord teruggeeft. Als de LDAP-server niet kan worden geconfigureerd om een helder tekstwachtwoord te retourneren, worden LEAP, EAP-FAST/MSCHAPv2 en PEAPv0/MSCHAPv2 niet ondersteund.

**Opmerking:** als er RADIUS-servers zijn geconfigureerd op de controller, probeert de controller eerst de draadloze clients te verifiëren met behulp van de RADIUS-servers. Lokale EAP wordt alleen geprobeerd als er geen RADIUS-servers worden gevonden, ofwel omdat er een time-out is opgetreden voor de RADIUS-servers, ofwel omdat er geen RADIUS-servers zijn geconfigureerd. Als vier RADIUS-servers zijn geconfigureerd, probeert de controller de client te verifiëren met de eerste RADIUS-server, de tweede RADIUS-server en vervolgens lokale EAP. Als de client vervolgens handmatig opnieuw probeert te verifiëren, probeert de controller de derde RADIUS-server, vervolgens de vierde RADIUS-server en vervolgens lokale EAP.

In dit voorbeeld wordt EAP-FAST gebruikt als de lokale EAP-methode op de WLC, die op zijn beurt is geconfigureerd om de LDAP backend database te bevragen voor gebruikersreferenties van een draadloze client.

# Configureren

In dit document wordt EAP-FAST gebruikt met certificaten aan zowel de client- als de serverkant. Hiervoor gebruikt de setup een **Microsoft Certificate Authority (CA)**-server om de client- en servercertificaten te genereren.

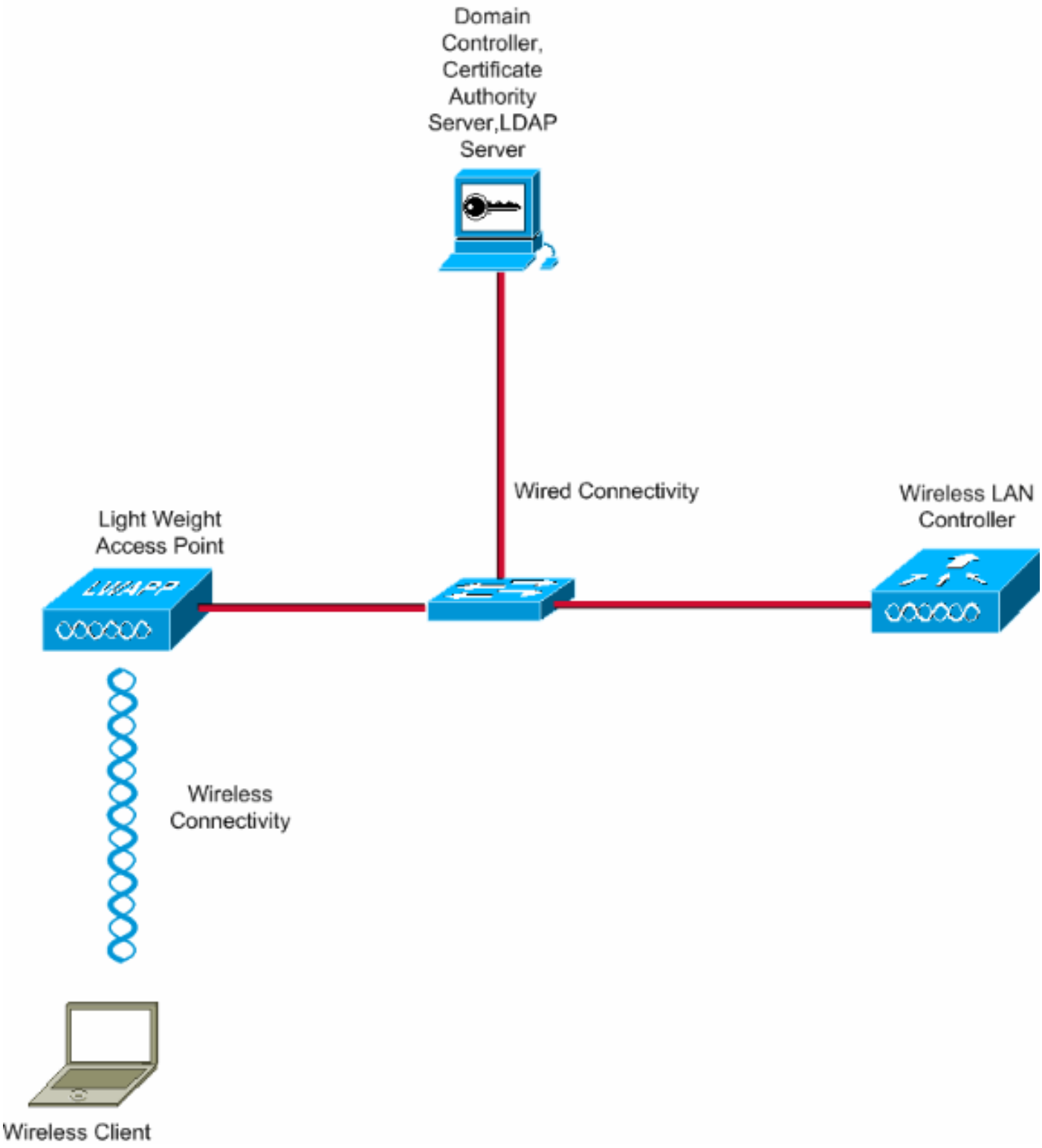
De gebruikersreferenties worden opgeslagen in de LDAP-server, zodat de controller bij een succesvolle certificaatherkenning de LDAP-server raadpleegt om de gebruikersreferenties op te halen en de draadloze client te verifiëren.

In dit document wordt ervan uitgegaan dat deze configuraties al zijn geïnstalleerd:

- Een LAP is geregistreerd bij de WLC. Raadpleeg Lichtgewicht AP (LAP)-registratie voor een draadloze LAN-controller (WLC) voor meer informatie over het registratieproces.
- Een DHCP-server is ingesteld om een IP-adres toe te wijzen aan de draadloze clients.
- Microsoft Windows 2003 server is geconfigureerd als domeincontroller en CA server. Dit voorbeeld gebruikt **wireless.com** als domein.Zie Windows 2003 configureren als domeincontroller voor meer informatie over het configureren van een Windows 2003-server als domeincontroller.Raadpleeg De Microsoft Windows 2003-server installeren en configureren als een CA-server (Certificate Authority) om de Windows 2003-server te configureren als een CA-server voor ondernemingen.

## Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:




## Configuraties

Voltooi de volgende stappen om deze configuratie te implementeren:

- EAP-FAST configureren als lokale EAP-verificatiemethode op de WLC
- LDAP-server configureren
- Draadloze client configureren

## EAP-FAST configureren als lokale EAP-verificatiemethode op de WLC

Zoals eerder vermeld, wordt in dit document EAP-FAST gebruikt met certificaten op zowel de client als de server als de lokale EAP-verificatiemethode. De eerste stap is het downloaden en installeren van de volgende certificaten naar de server (WLC, in dit geval) en de client.

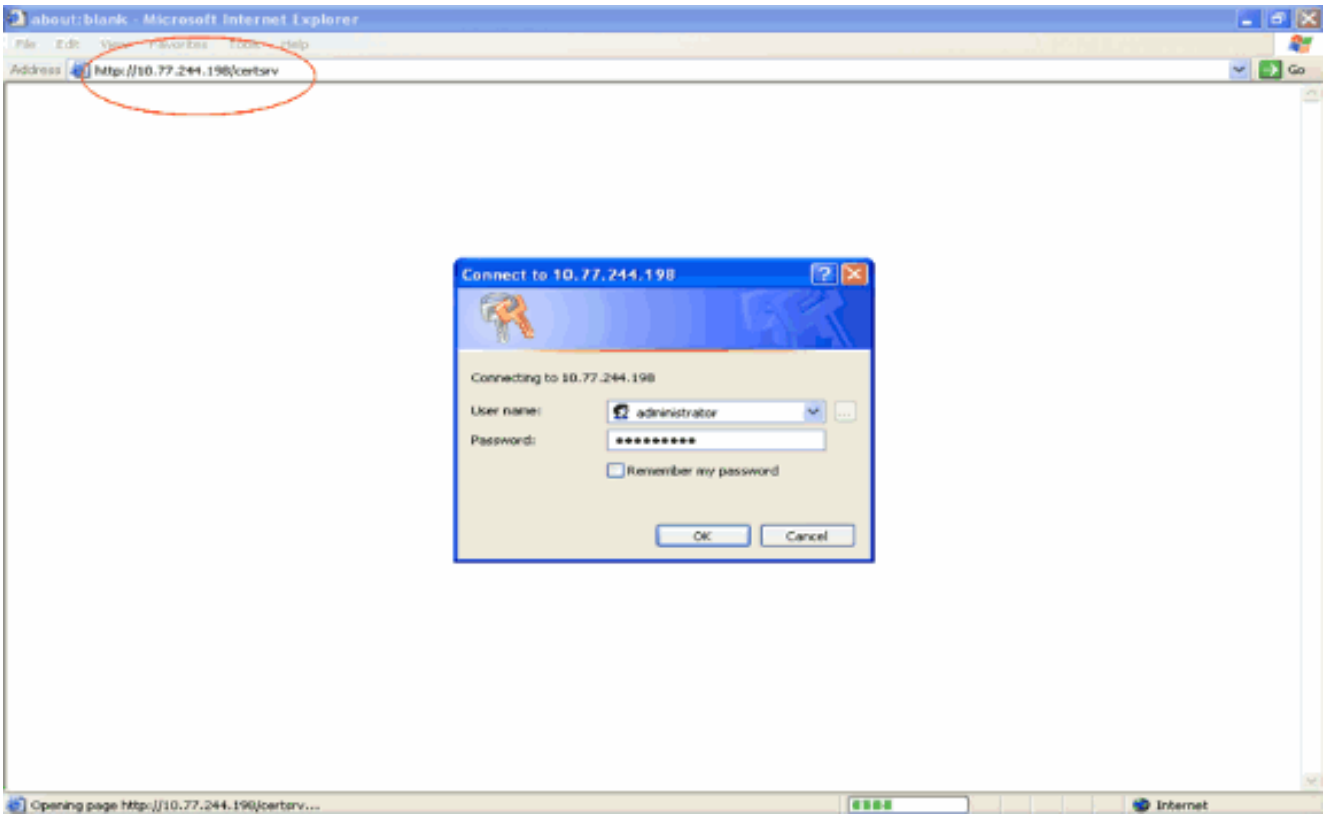
De WLC en de client hebben elk deze certificaten nodig om gedownload te worden van de CA-server:

- Apparaatcertificaat (één voor de WLC en één voor de client)
- basiscertificaat van de Public Key Infrastructure (PKI) voor de WLC en CA-certificaat voor de client

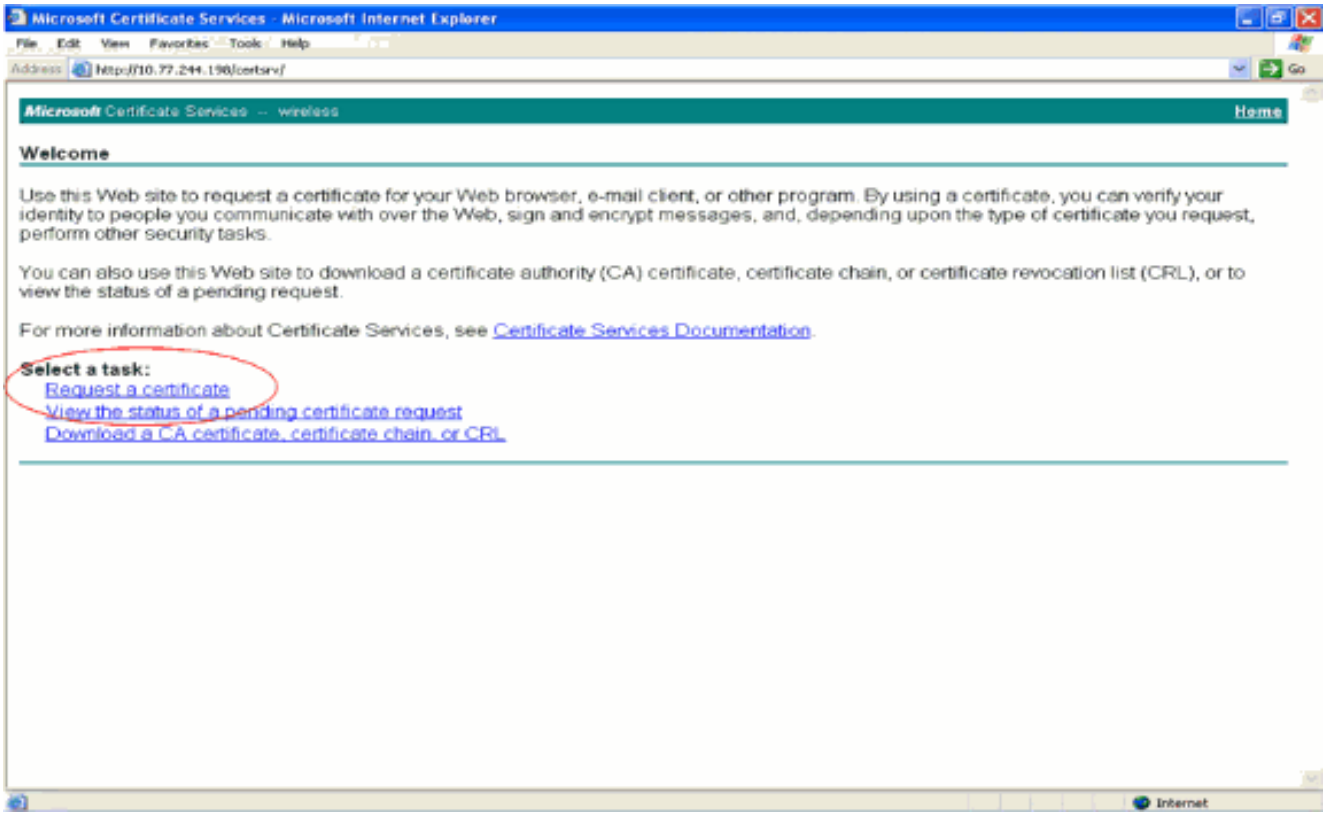
## Een apparaatcertificaat voor de WLC genereren

Voer deze stappen uit om een apparaatcertificaat voor de WLC te genereren vanaf de CA-server. Dit apparaatcertificaat wordt door de WLC gebruikt om te verifiëren bij de client.

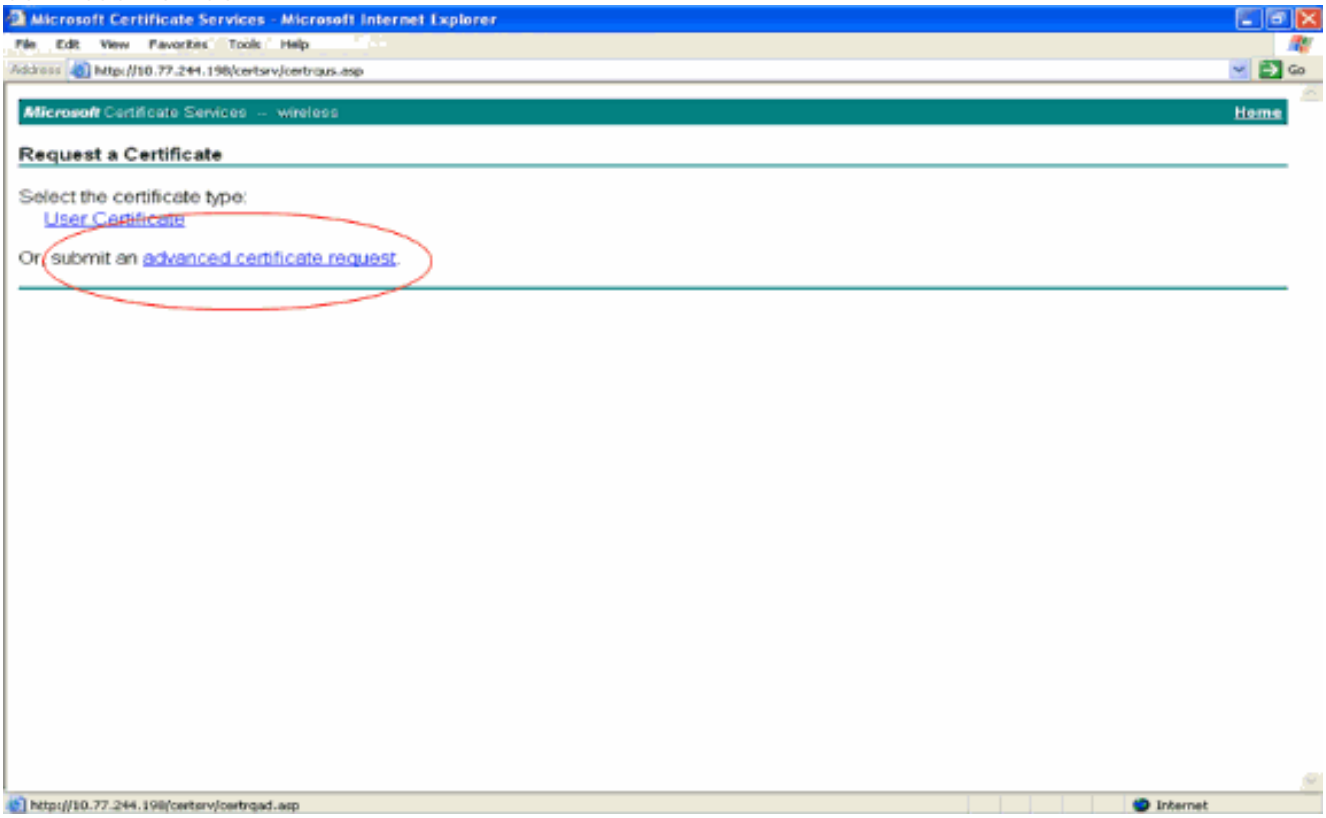
1. Ga naar **http://<IP-adres van CA-server>/certsrv** vanaf uw pc die een netwerkverbinding met de CA-server heeft. Log in als beheerder van de CA-server.



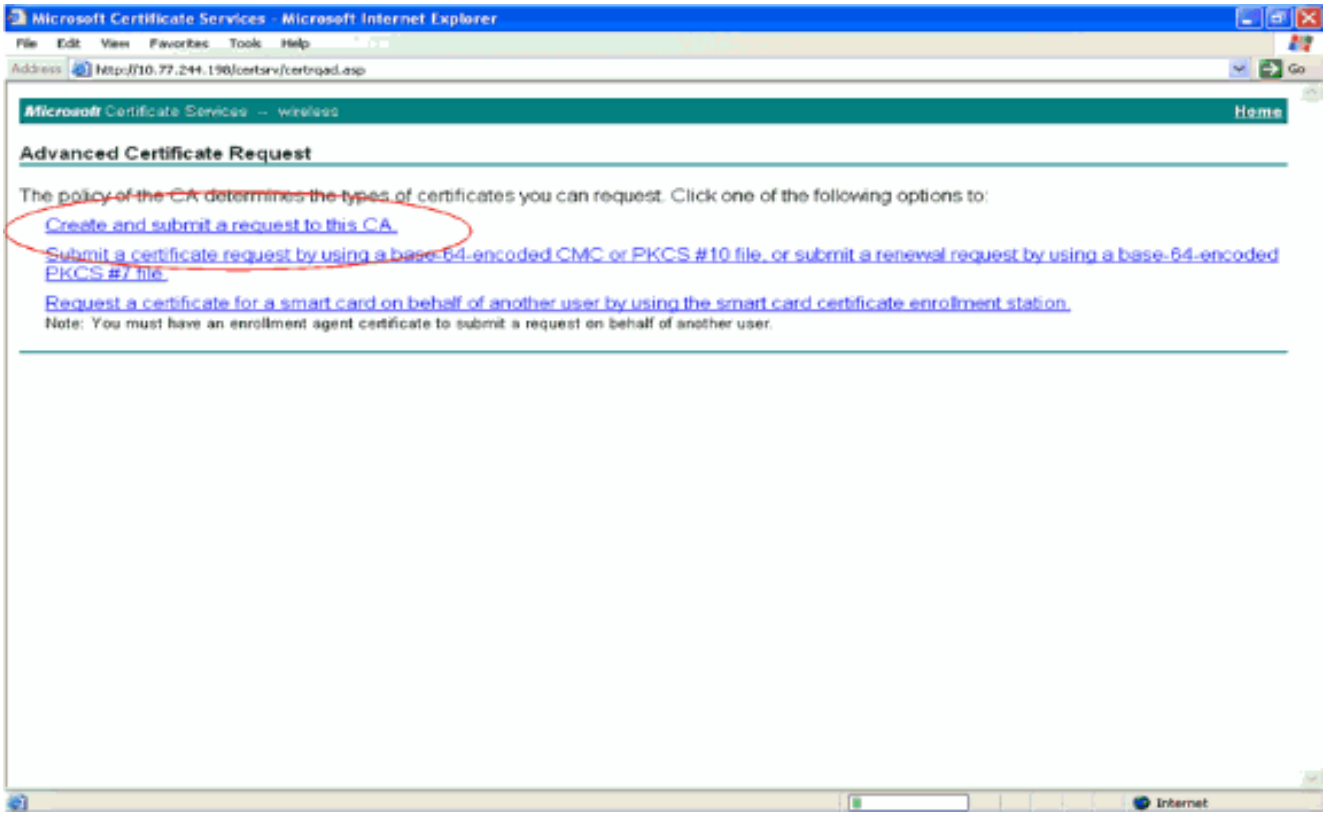

2. Selecteer **Certificaat aanvragen**.



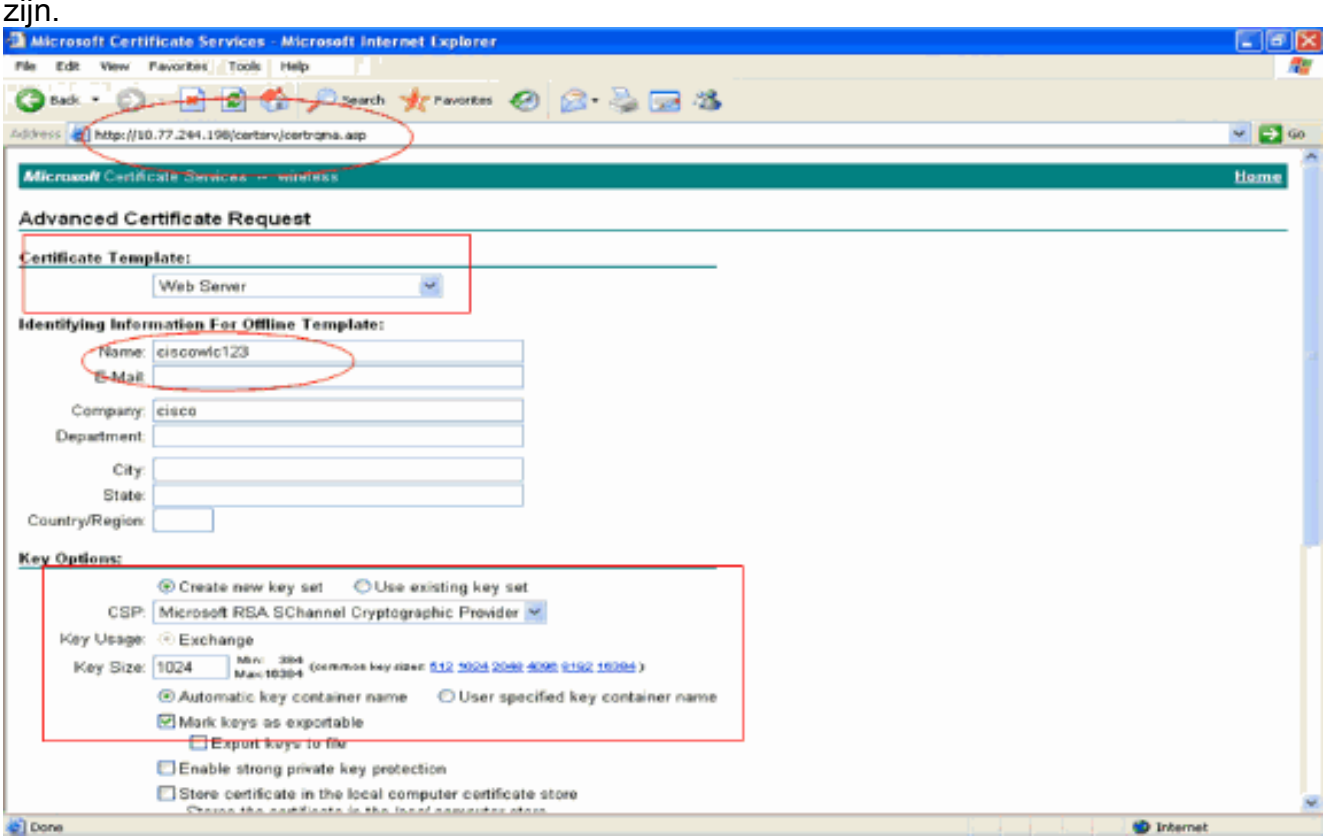

3. Klik op de pagina Certificaat aanvragen op **Geavanceerd certificaatverzoek**.




4. Klik op de pagina Geavanceerd certificaatverzoek op **Aanmaken en een aanvraag indienen bij deze certificeringsinstantie**. Dit brengt u naar het Geavanceerd certificaataanvraagformulier.

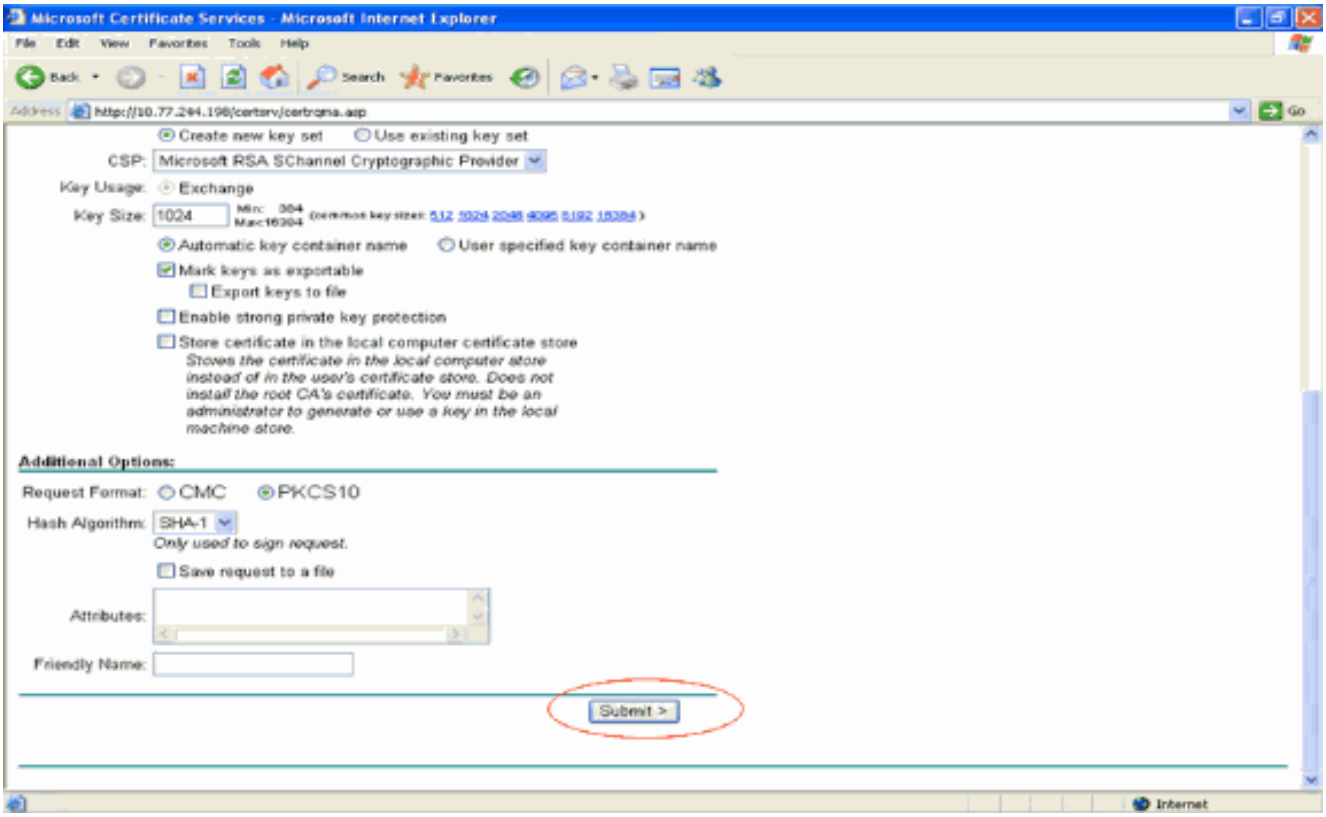



5. Kies in het formulier Geavanceerd certificaatverzoek **Web Server** als de certificaatsjabloon. Specificeer vervolgens een naam voor dit apparaatcertificaat.Dit voorbeeld gebruikt de certificaatnaam als ciscowlc123. Vul de andere identificatiegegevens in volgens uw vereiste.
6. Selecteer in het gedeelte **Belangrijkste opties** de optie **Toetsen markeren als exporteerbaar**. Soms wordt deze optie grijs weergegeven en kan deze niet worden ingeschakeld of uitgeschakeld als u een webserversjabloon kiest. In dergelijke gevallen, klik **terug** van het browser menu om één pagina terug te gaan en opnieuw terug te komen naar deze pagina. Ditmaal moeten de markeertoetsen als exporteerbare optie beschikbaar zijn.

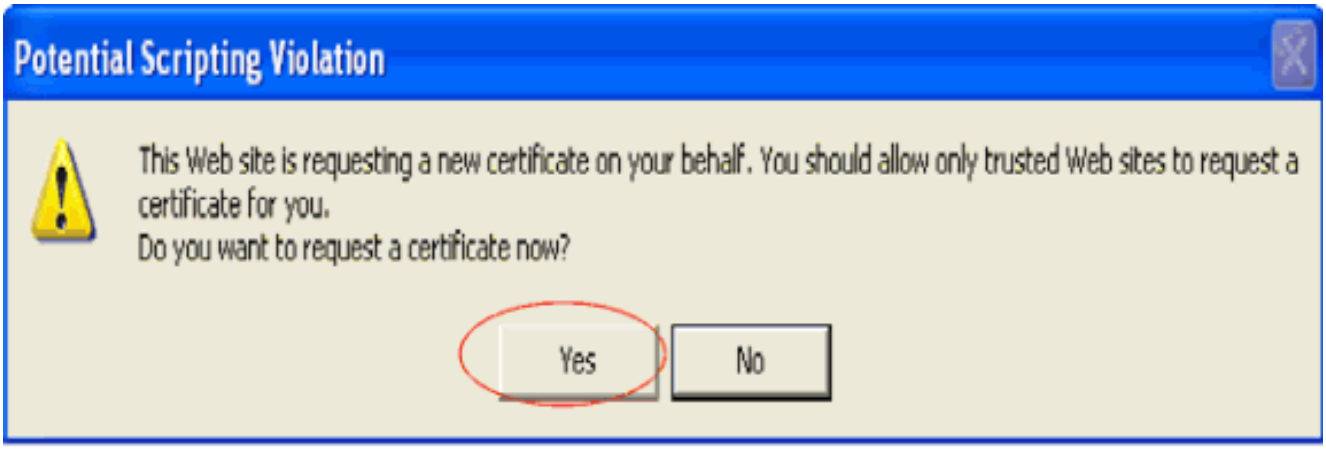



7. Configureer alle andere benodigde velden en klik op

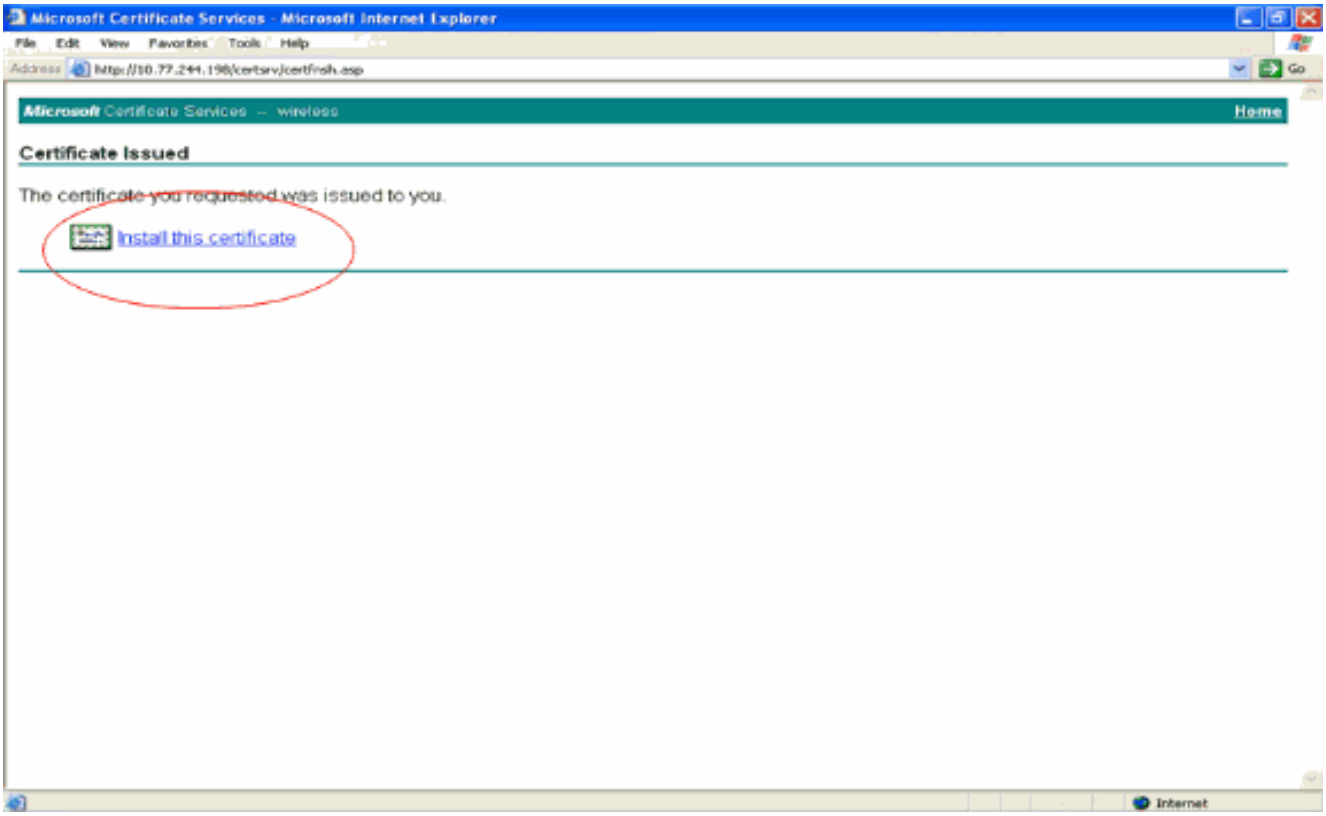
**Indienen**.



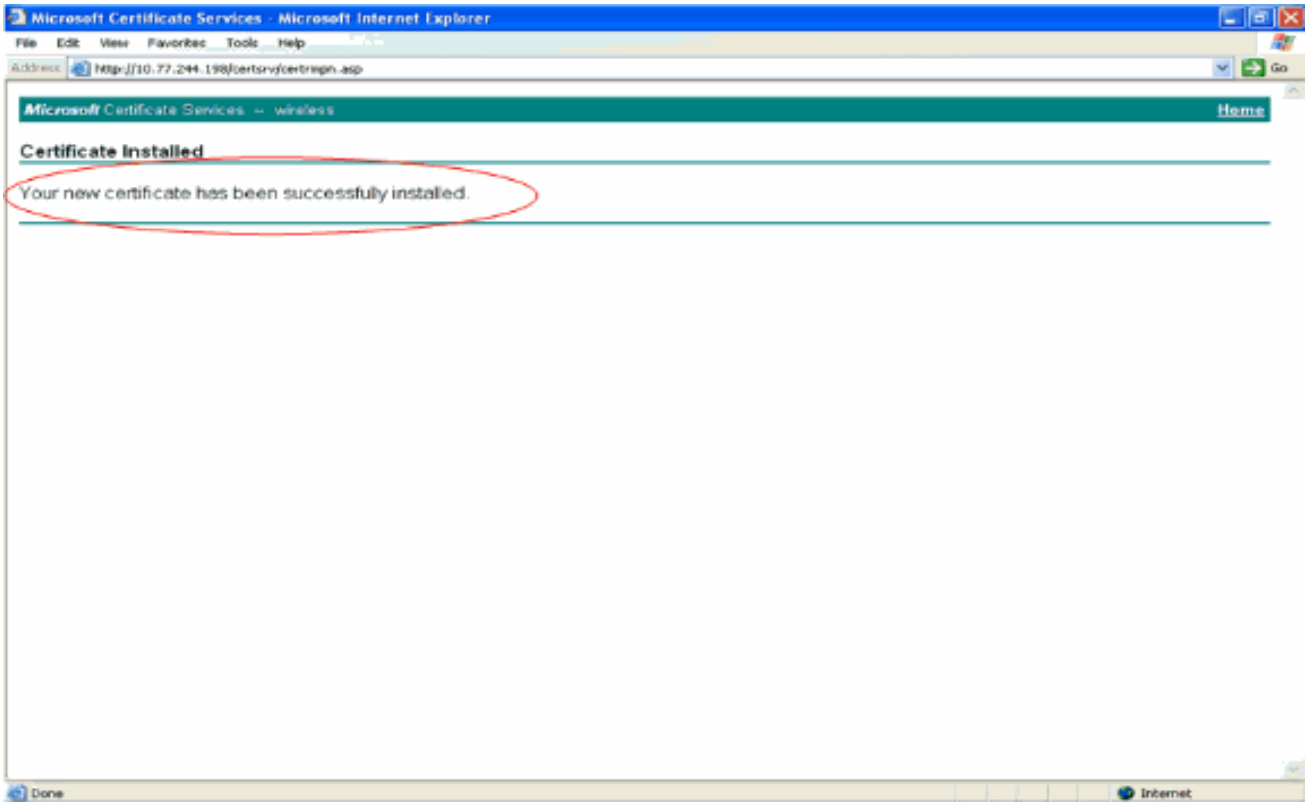

8. Klik in het volgende venster op **Ja** om het proces voor het aanvragen van certificaten toe te staan.



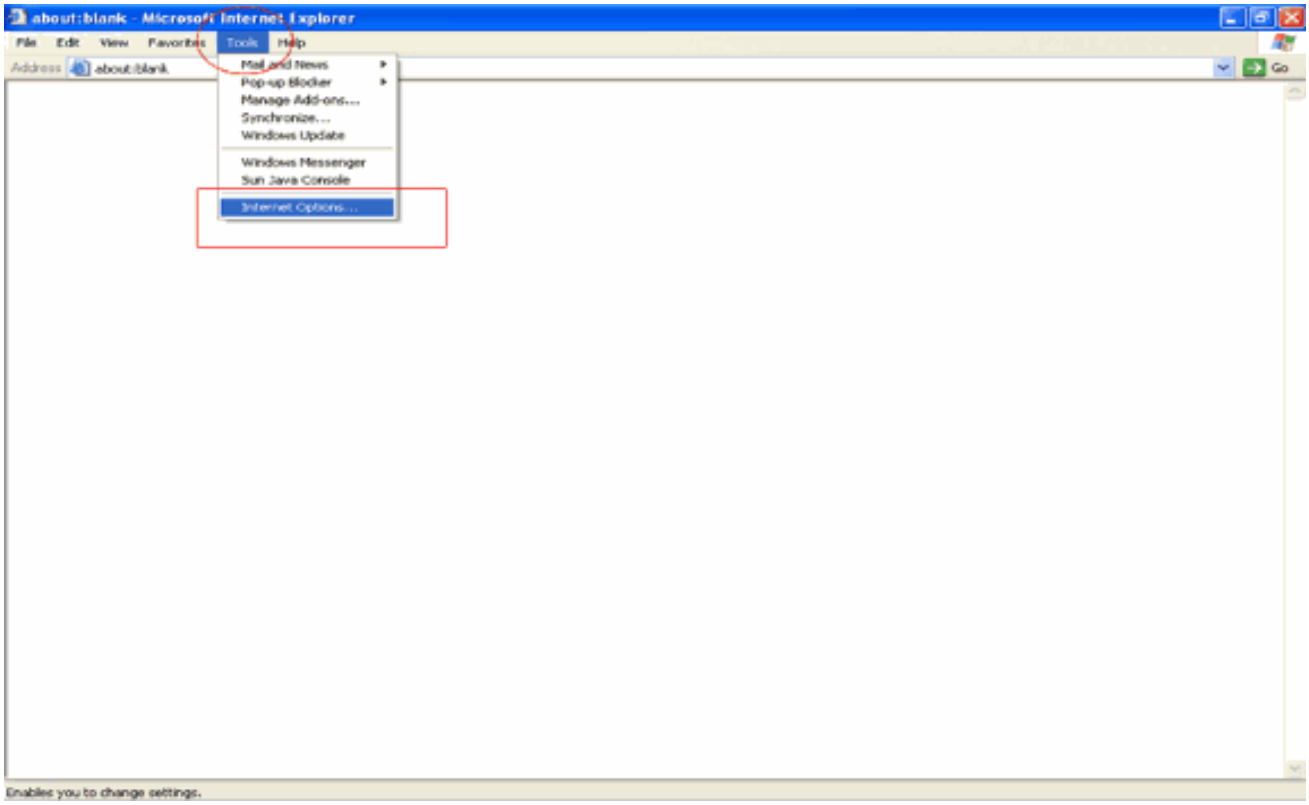

9. Het venster voor een certificaataanvraag wordt weergegeven. Dit duidt op een geslaagde procedure voor het aanvragen van een certificaat. De volgende stap is het afgegeven certificaat te installeren in het certificaatarchief van deze PC. Klik op **Dit certificaat installeren**.



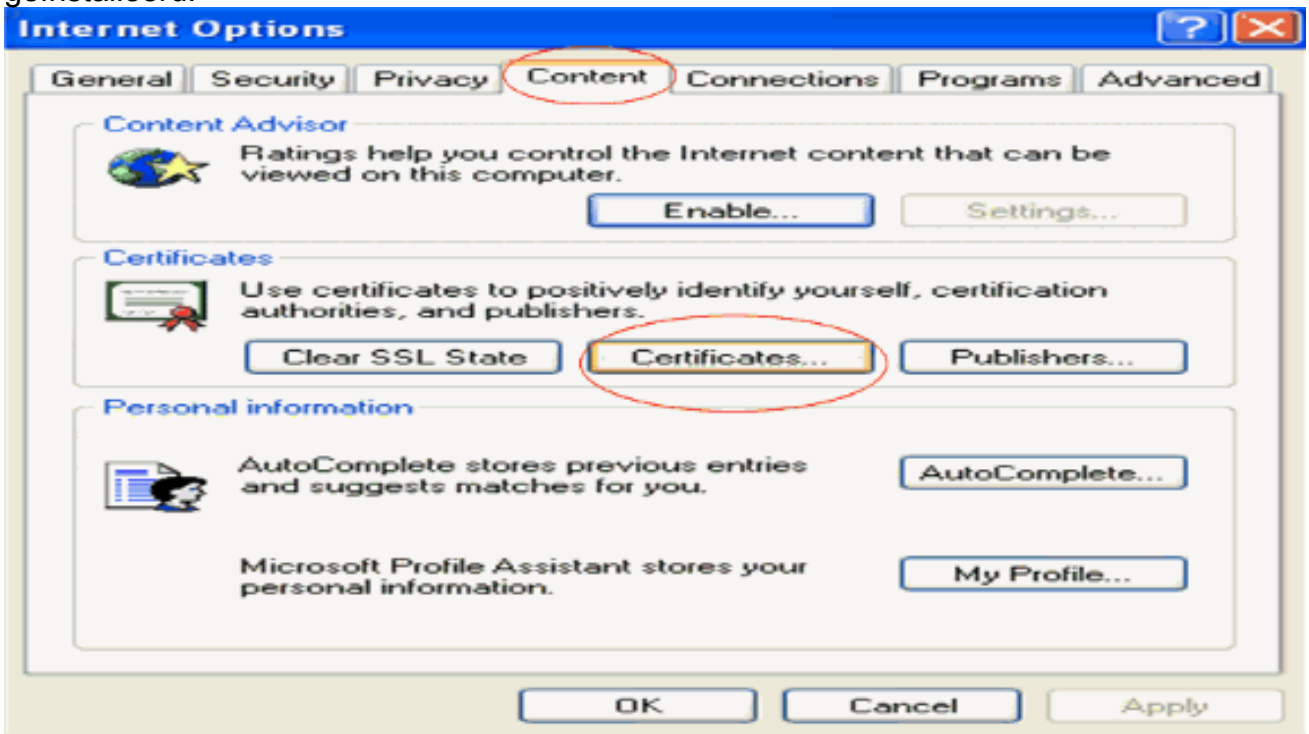

10. Het nieuwe certificaat wordt met succes geïnstalleerd op de pc van waar het verzoek wordt gegenereerd naar de CA-server.



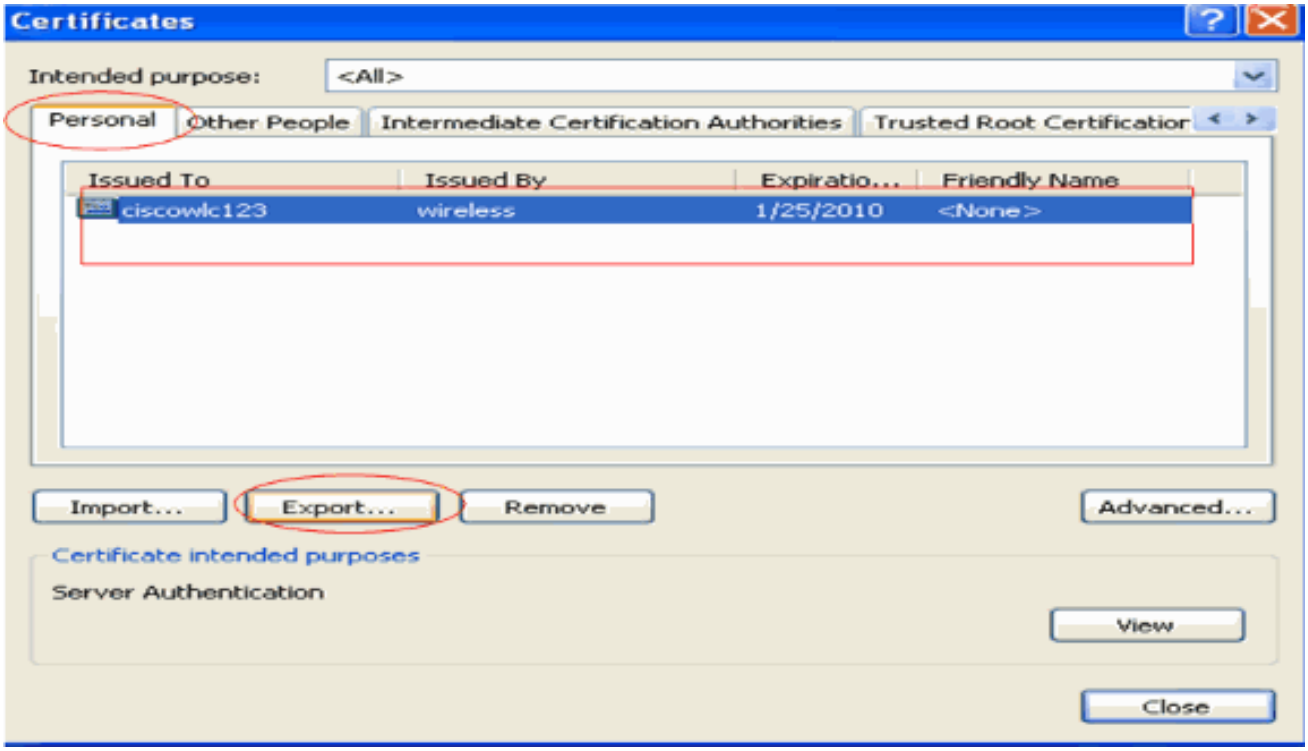

11. De volgende stap is om dit certificaat van het certificaatarchief naar de vaste schijf als bestand te exporteren. Dit certificaatbestand wordt later gebruikt om het certificaat naar de WLC te downloaden.Als u het certificaat uit het certificaatarchief wilt exporteren, opent u de Internet Explorer-browser en vervolgens klikt u op **Gereedschappen > Internet-opties**.




12. Klik op **Inhoud > Certificaten** om naar het certificaatarchief te gaan waar de certificaten standaard worden
geïnstalleerd.

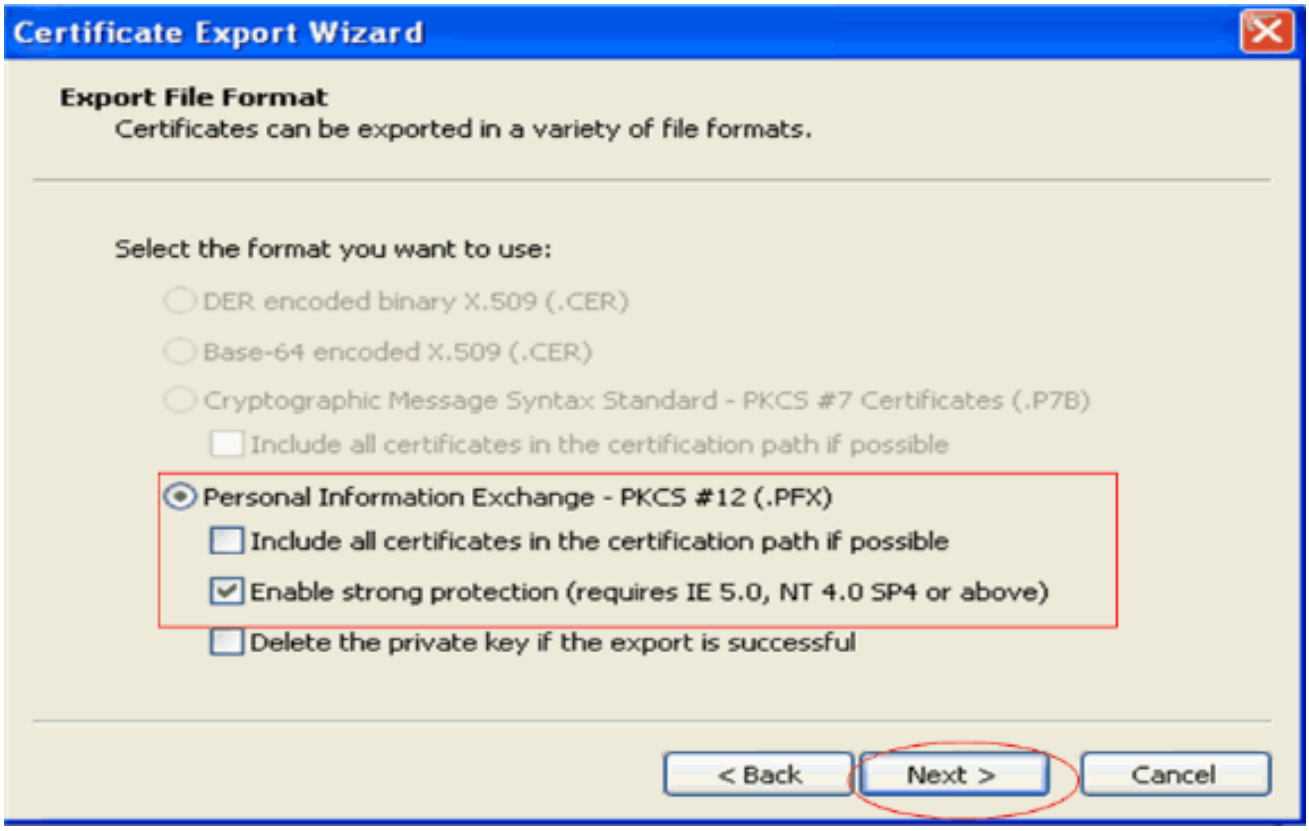



13. De apparaatcertificaten worden gewoonlijk geïnstalleerd onder de **Persoonlijke** certificaatlijst. Hier, zou u het onlangs geïnstalleerde certificaat moeten zien. Selecteer het certificaat en klik op
**Exporteren**.

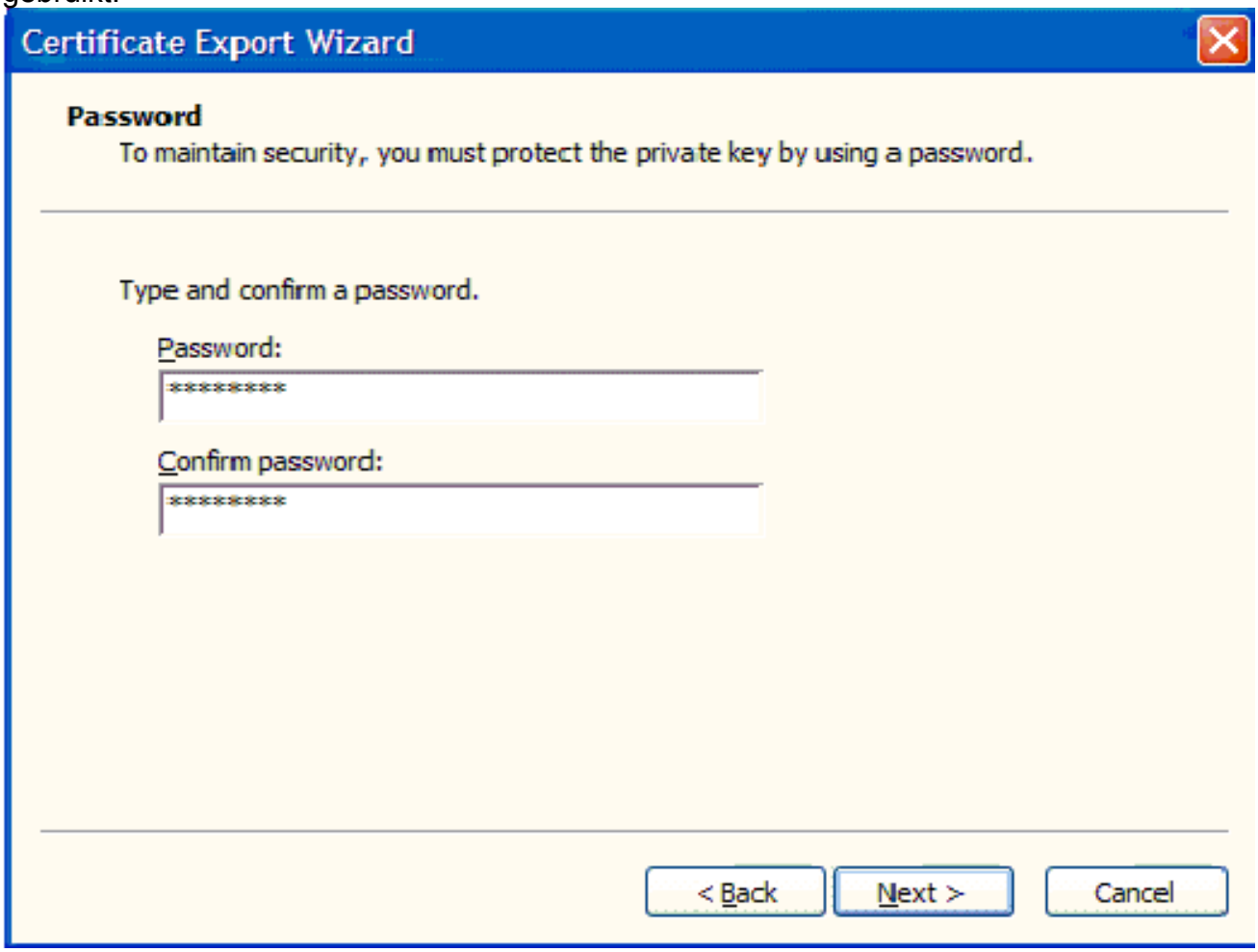



14. Klik op **Volgende** in de volgende vensters. Kies **Ja, exporteer de** optie **private sleutel** in het venster **Wizard Certificaat exporteren**. Klik op **Next**
(Volgende).


15. Kies de exportbestandsindeling als **.PFX** en kies de optie **Sterke bescherming inschakelen**. Klik op **Next**
(Volgende).

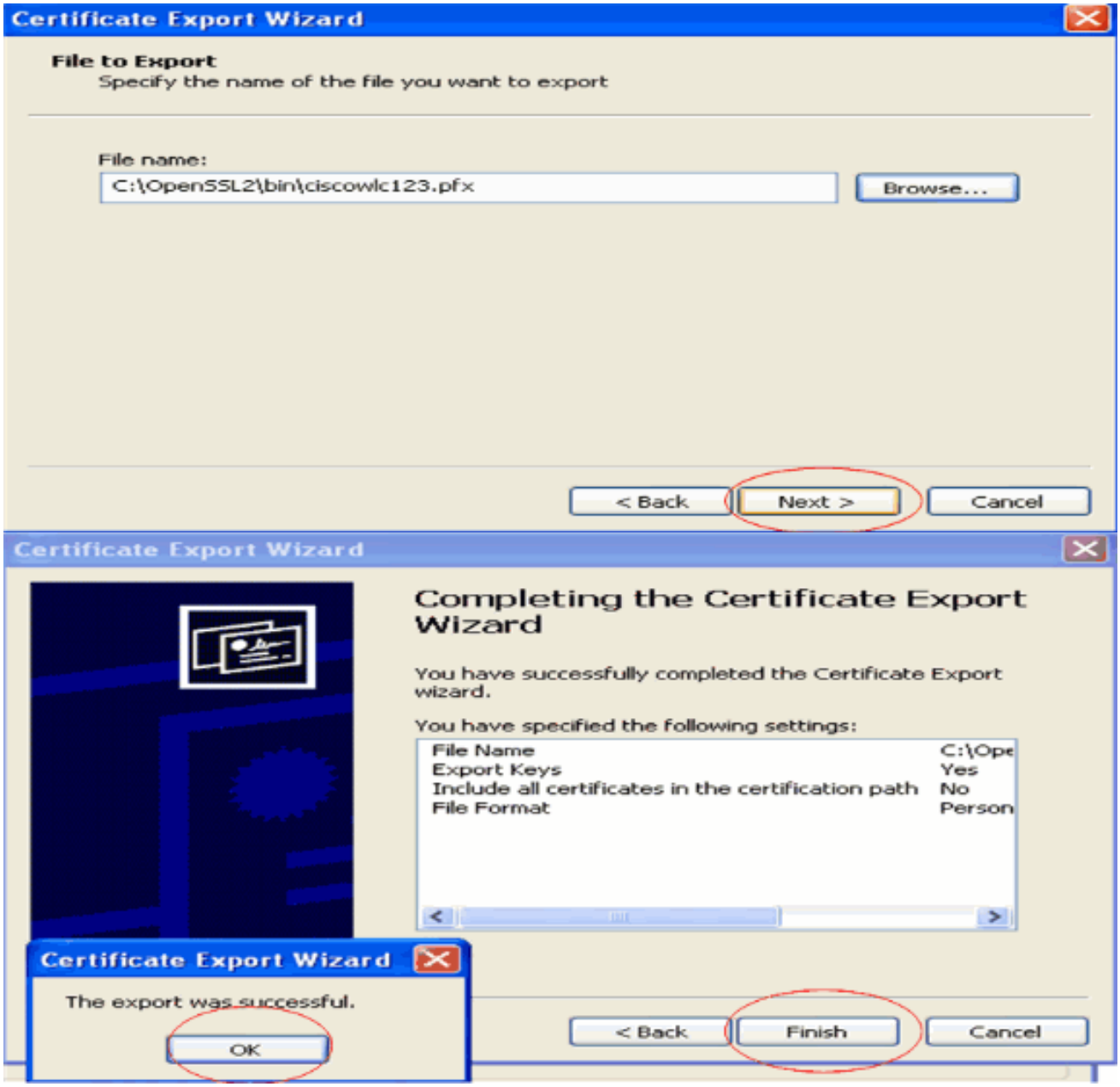



16. Voer in het wachtwoordvenster een wachtwoord in. In dit voorbeeld wordt **cisco** als het wachtwoord
gebruikt.




17. Sla het certificaatbestand (.PFX-bestand) op de vaste schijf op. Klik op **Volgende** en voer het exportproces met succes

uit.




## Het downloaden van het Apparaatcertificaat op WLC

Nu het WLC-apparaatcertificaat beschikbaar is als een .PFX-bestand, is de volgende stap om het bestand te downloaden naar de controller. Cisco WLC's accepteren certificaten alleen in .PEM-indeling. Daarom moet u eerst het bestand met de .PFX- of PKCS12-indeling naar een PEM-bestand converteren via het openSSL-programma.

### Het certificaat in PFX naar PEM-formaat converteren met het openSSL-programma

U kunt het certificaat kopiëren naar elke pc waarop u openSSL hebt geïnstalleerd om het naar PEM-indeling te converteren. Voer deze opdrachten in in het bestand Openssl.exe in de bin-map van het openSSL-programma:

**Opmerking:** u kunt openSSL downloaden van de OpenSSL website.

```
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
```

Het certificaatbestand wordt geconverteerd naar de PEM-indeling. De volgende stap is om het PEM-formaat apparaatcertificaat te downloaden naar de WLC.

**Opmerking:** Daarvoor hebt u een TFTP-serversoftware op uw pc nodig van waaruit het PEM-bestand wordt gedownload. Deze PC zou connectiviteit aan WLC moeten hebben. De TFTP-server moet zijn huidige en basismap hebben gespecificeerd met de locatie waar het PEM-bestand is opgeslagen.

## Download het geconverteerde PEM Format-apparaatcertificaat naar de WLC

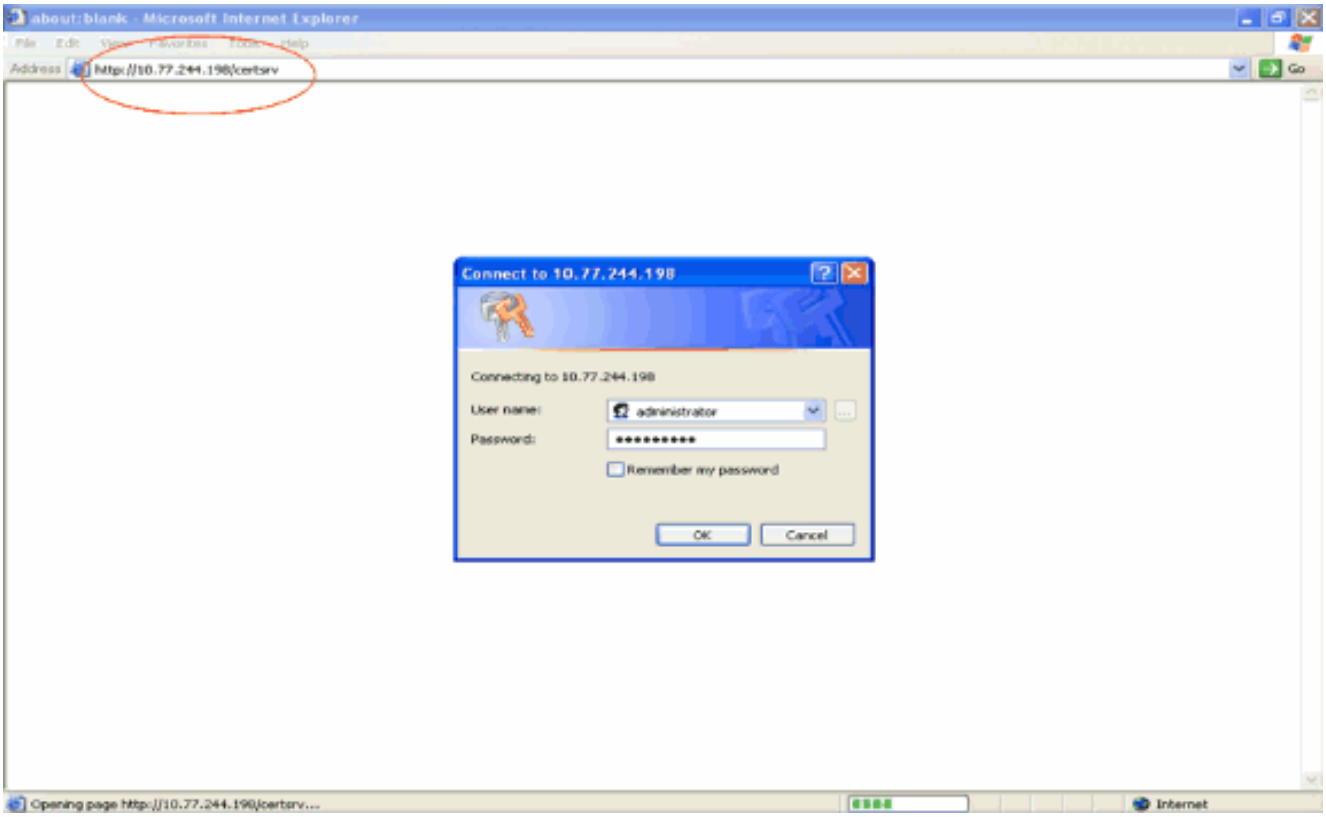
Dit voorbeeld verklaart het downloadproces door CLI van WLC.

1. Meld u aan bij de controller CLI.
2. Voer de opdracht **download datatype edapdevice in**.
3. Voer de opdracht **download serverip** *10.77.244.196 in*.10.77.24.196 is het IP-adres van de TFTP-server.
4. Voer de opdracht **download bestandsnaam** *ciscowlc.pem*.ciscowlc123.pem is de bestandsnaam die in dit voorbeeld wordt gebruikt.
5. Voer de opdracht **Certpassword downloaden overdracht in** om het wachtwoord voor het certificaat in te stellen.
6. Voer de opdracht **Start** voor **downloaden** van **overdracht in** om de bijgewerkte instellingen te bekijken.Dan, antwoord **y** wanneer gevraagd om de huidige instellingen te bevestigen en het downloadproces te starten.Dit voorbeeld toont de output van het downloadbevel:
   ```
   (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. Voer de opdracht **Systeem opnieuw instellen in** om de controller te herstarten. De controller is nu geladen met het apparaatcertificaat.

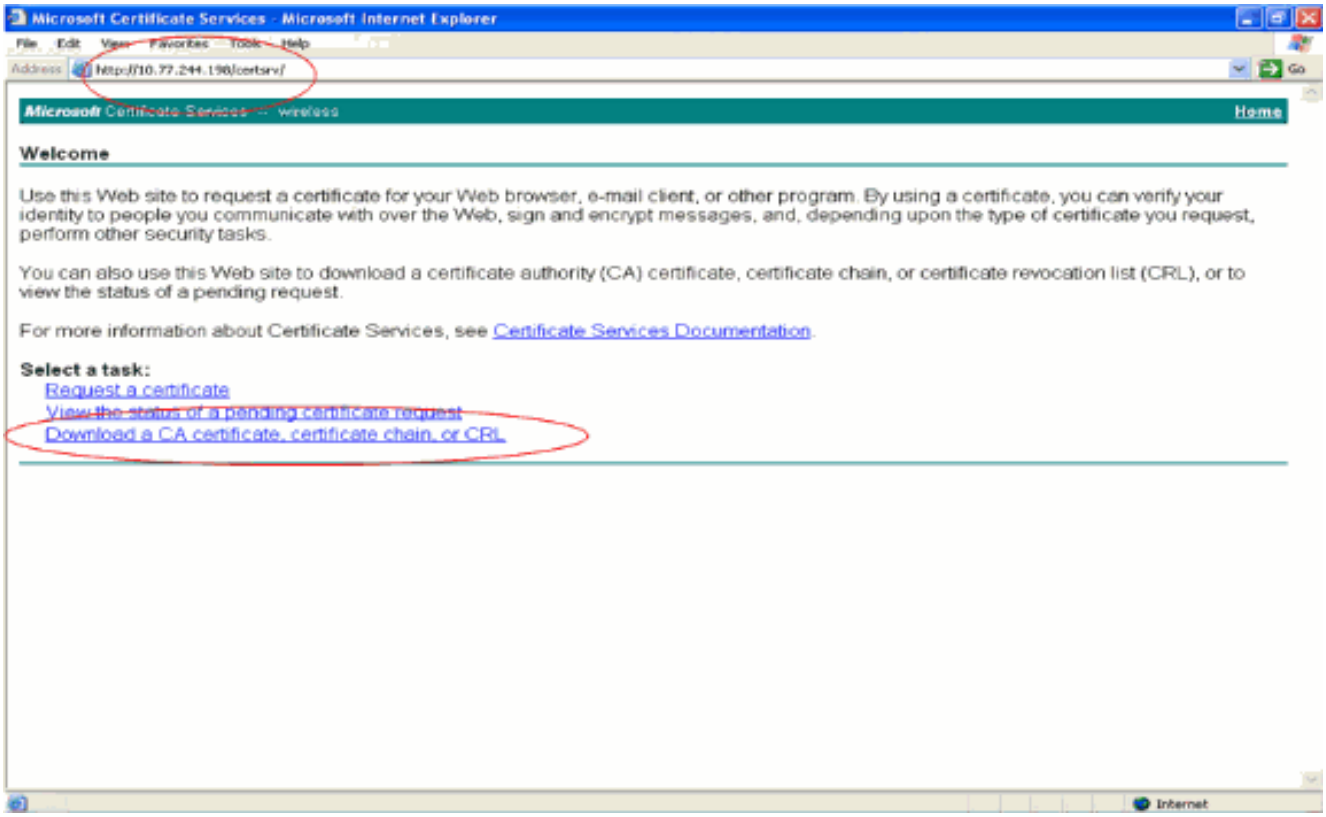
## Installeer het basiscertificaat van PKI in de WLC

Nu het apparaatcertificaat in de WLC is geïnstalleerd, is de volgende stap om het Root Certificate van de PKI naar de WLC te installeren vanaf de CA-server. Voer de volgende stappen uit:

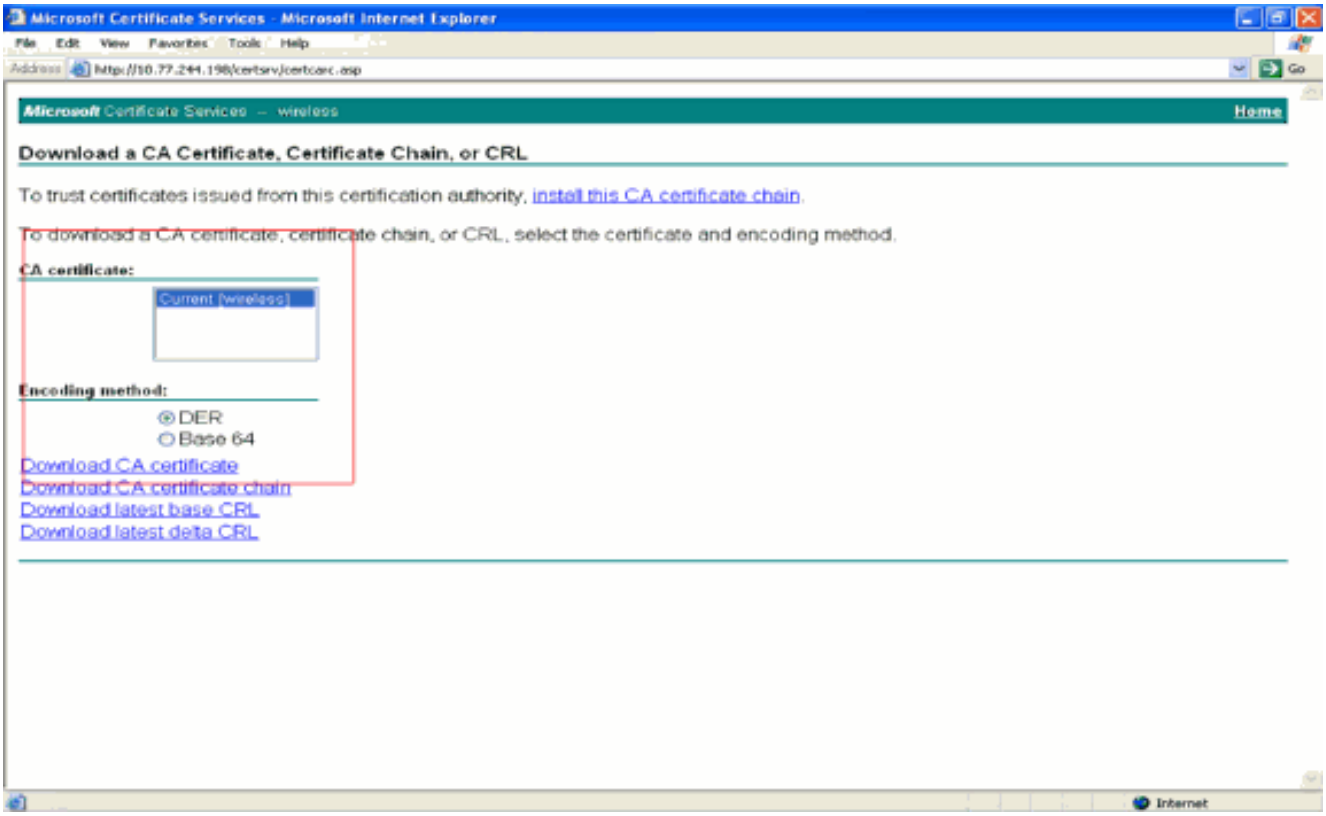
1. Ga naar **http://<IP-adres van CA-server>/certsrv** vanaf uw pc die een netwerkverbinding met de CA-server heeft. Login als beheerder van de CA-server.




2. Klik op **Een CA-certificaat, certificaatketen of CRL downloaden**.



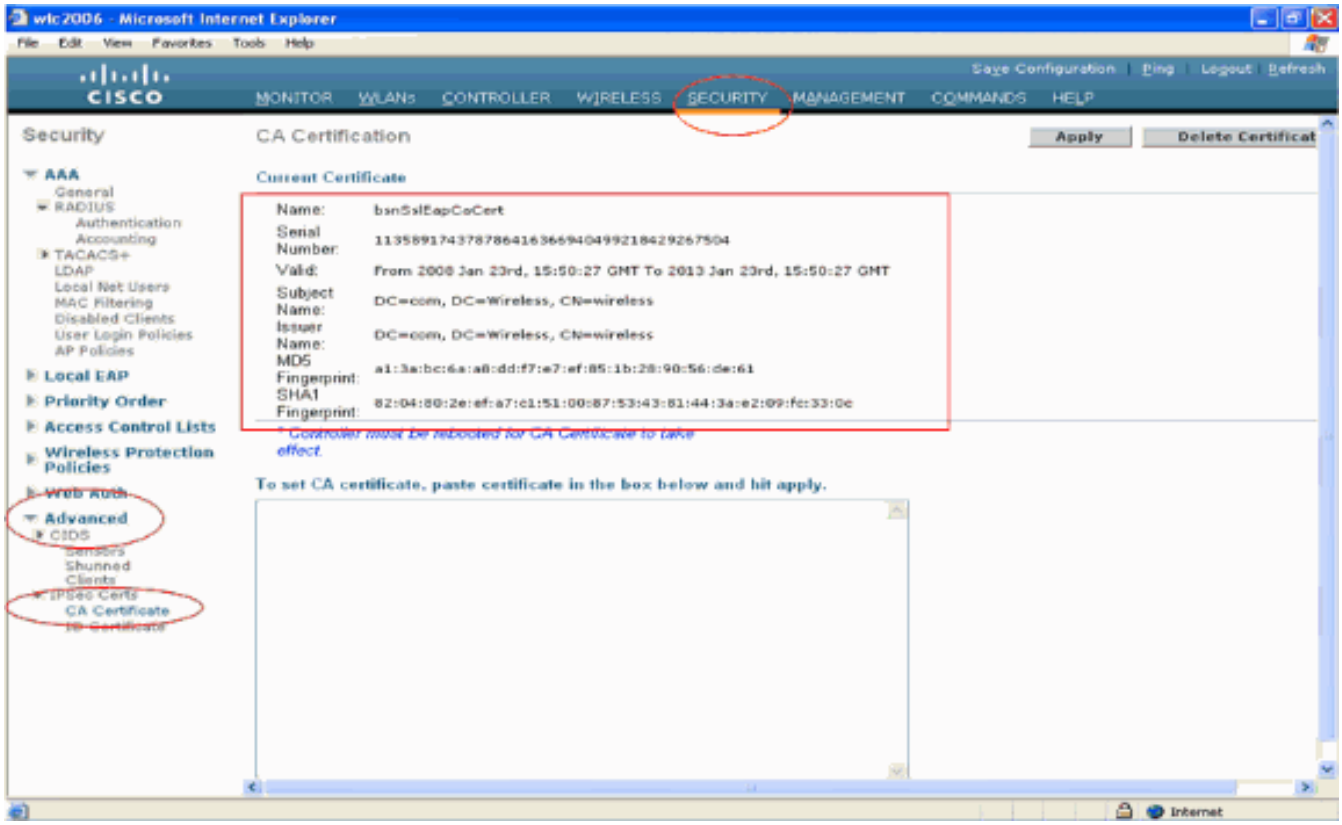

3. Op de resulterende pagina kunt u de huidige CA-certificaten zien die beschikbaar zijn op de CA-server onder het vakje **CA-certificaat**. Kies **DER** als de coderingsmethode en klik op **CA-certificaat downloaden**.



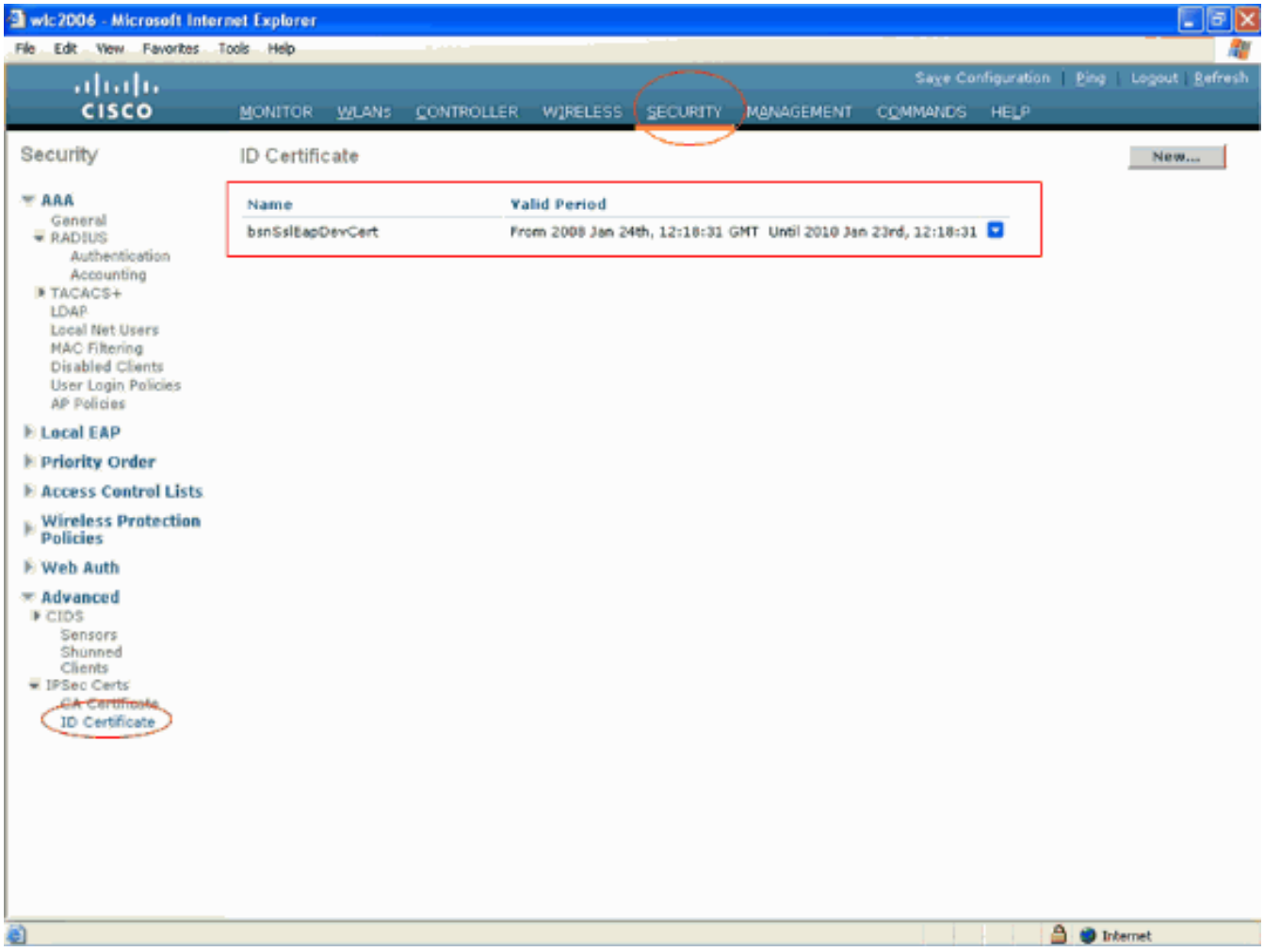

4. Sla het certificaat op als een **.cer-**bestand. Dit voorbeeld gebruikt **certnew.cer** als bestandsnaam.
5. De volgende stap is om het .cer-bestand naar PEM-formaat te converteren en het naar de controller te downloaden. Om deze stappen uit te voeren, herhaal dezelfde procedure die in het gedeelte Downloaden van het Apparaatcertificaat naar de WLC is uitgelegd met deze wijzigingen:De openSSL "-in" en "-out" bestanden zijn **certnew.cer** en **certnew.pem**.Hierbij zijn ook geen PEM-wachtwoorden of importwachtwoorden vereist.De opdracht openSSL om het **.cer-**bestand naar het **.pem-**bestand te converteren is ook:**x509 -in *certnew.cer* -information DER -out *certnew.pem* -outform PEM**In stap 2 van de Download het geconverteerde PEM Format Device Certificate naar de WLC-sectie, is de opdracht om het certificaat te downloaden naar de WLC:(Cisco Controller)**>download datatype Eapcacert**Het bestand dat gedownload moet worden naar de WLC is **certnew.pem**.

U kunt als volgt controleren of de certificaten op de WLC zijn geïnstalleerd vanaf de controller-GUI:

- Klik vanuit de WLC GUI op **Security**. Klik op de pagina Beveiliging op **Geavanceerd > IPSec-certs** vanuit de taken die aan de linkerkant worden weergegeven. Klik op **CA-certificaat** om het geïnstalleerde CA-certificaat te bekijken. Hier is het voorbeeld:




- Om te verifiëren of het apparaatcertificaat op de WLC is geïnstalleerd, klikt u vanuit de WLC GUI op **Security**. Klik op de pagina Beveiliging op **Geavanceerd > IPSec**-certs vanuit de taken die aan de linkerkant worden weergegeven. Klik op **ID-certificaat** om het geïnstalleerde apparaatcertificaat te bekijken. Hier is het voorbeeld:

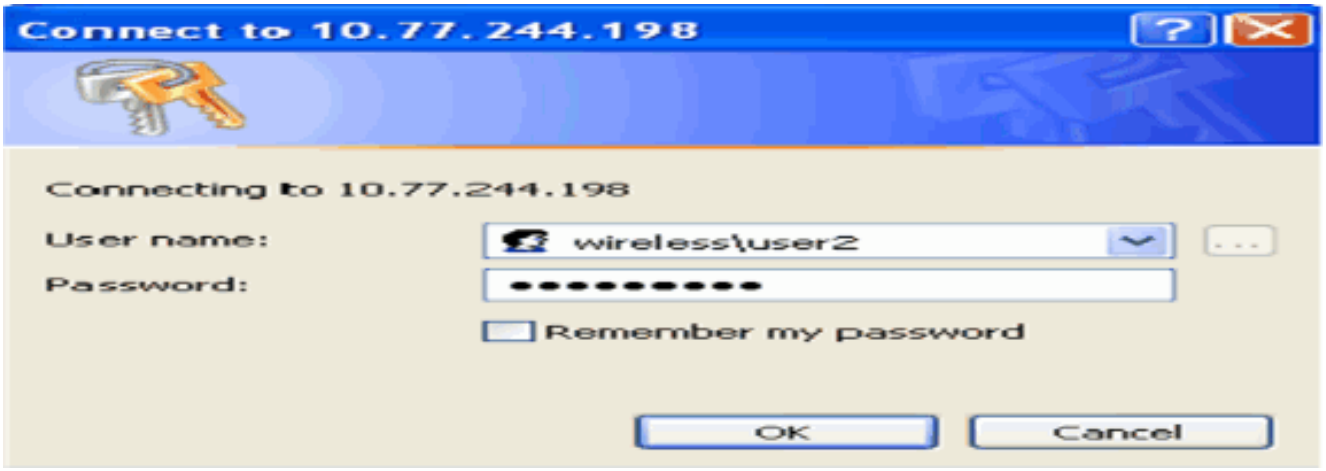


## Een apparaatcertificaat voor de client genereren

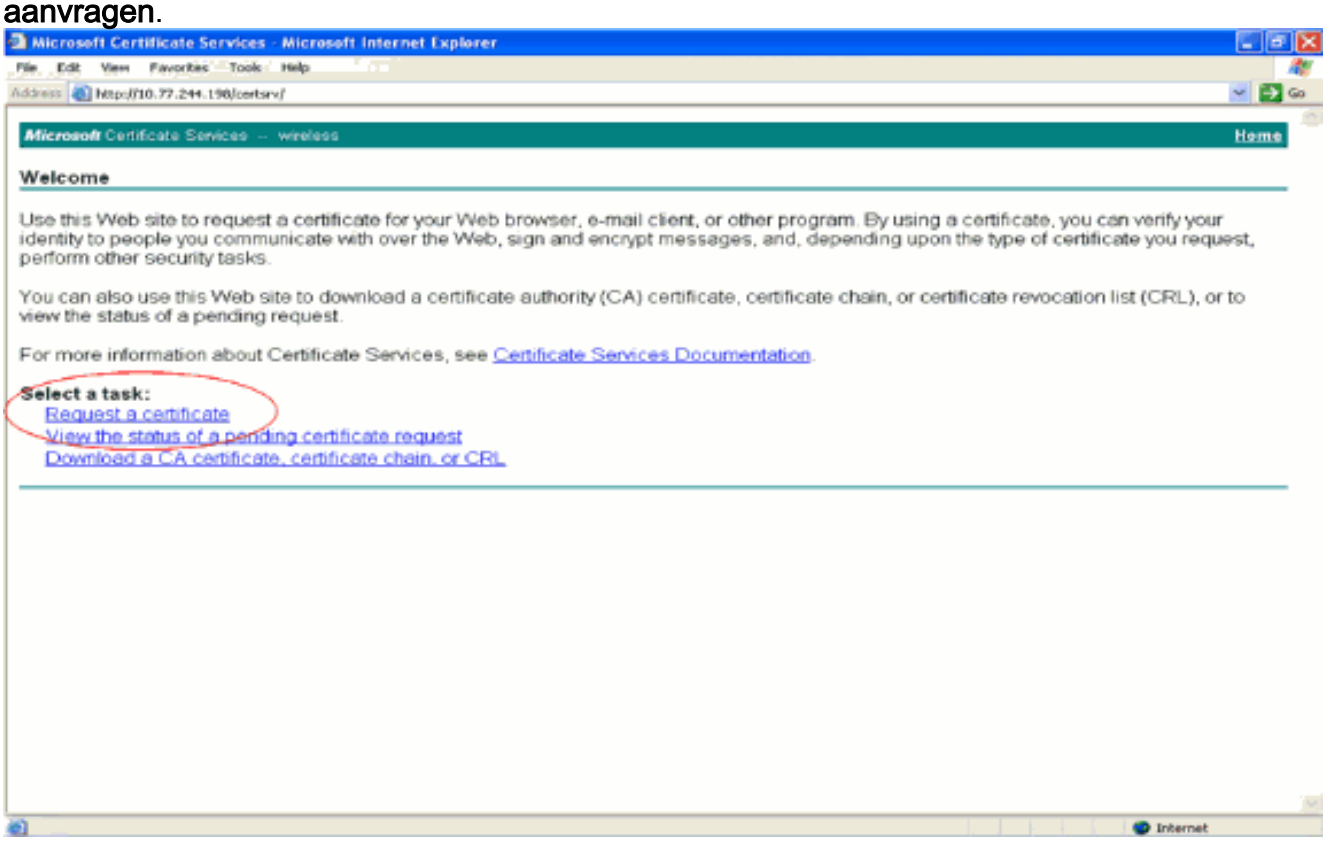
Nu het apparaatcertificaat en het CA-certificaat op de WLC zijn geïnstalleerd, is de volgende stap om deze certificaten voor de client te genereren.

Voer deze stappen uit om het apparaatcertificaat voor de client te genereren. Dit certificaat zal door de client worden gebruikt voor de verificatie van de WLC. In dit document worden de stappen uitgelegd die moeten worden uitgevoerd bij het genereren van certificaten voor de professionele client van Windows XP.

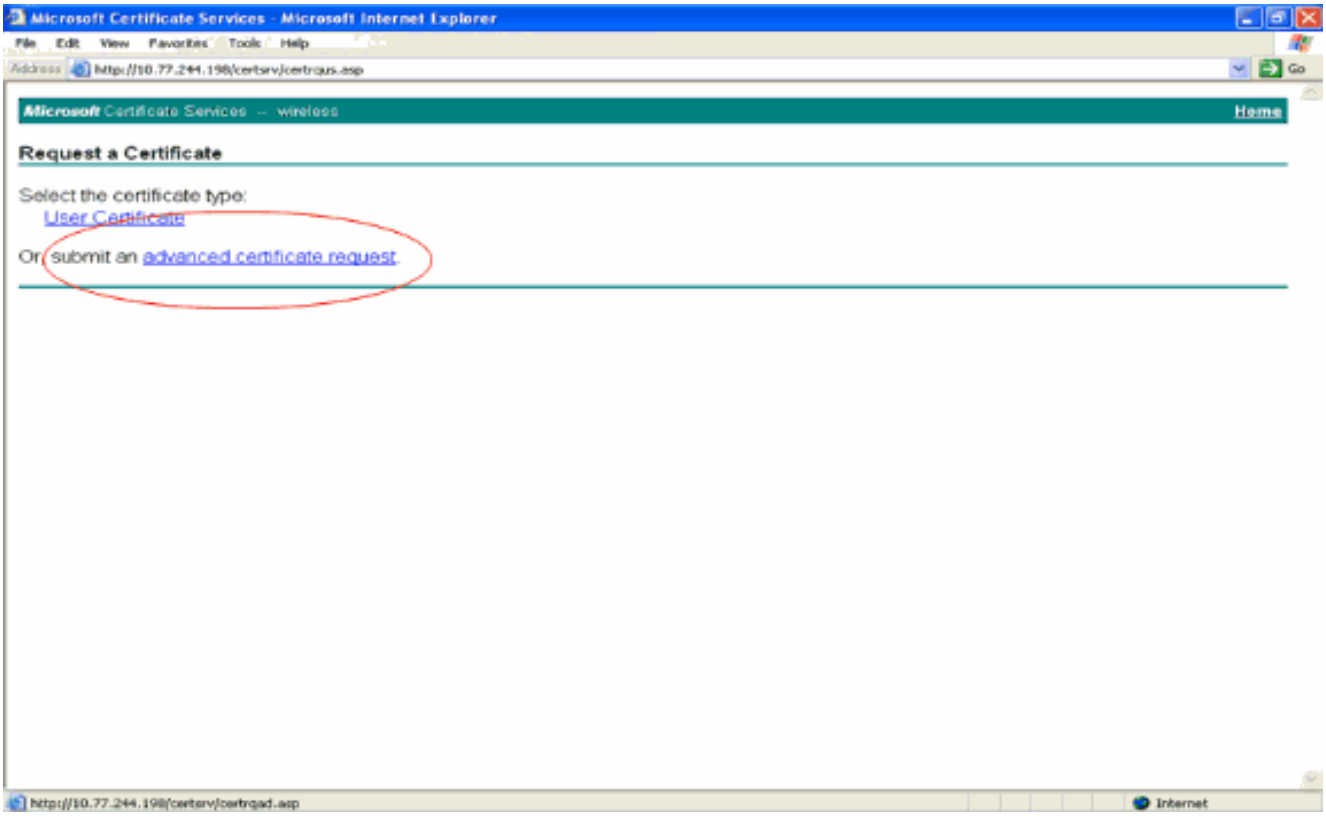
1. Ga naar **http://<IP-adres van CA-server>/certsrv** van de client waarvoor het certificaat moet worden geïnstalleerd. Aanmelden als domeinnaam\gebruikersnaam voor CA-server. De gebruikersnaam zou de naam moeten zijn van de gebruiker die deze XP machine gebruikt, en de gebruiker zou reeds moeten worden geconfigureerd als deel van hetzelfde domein als de CA-
server.



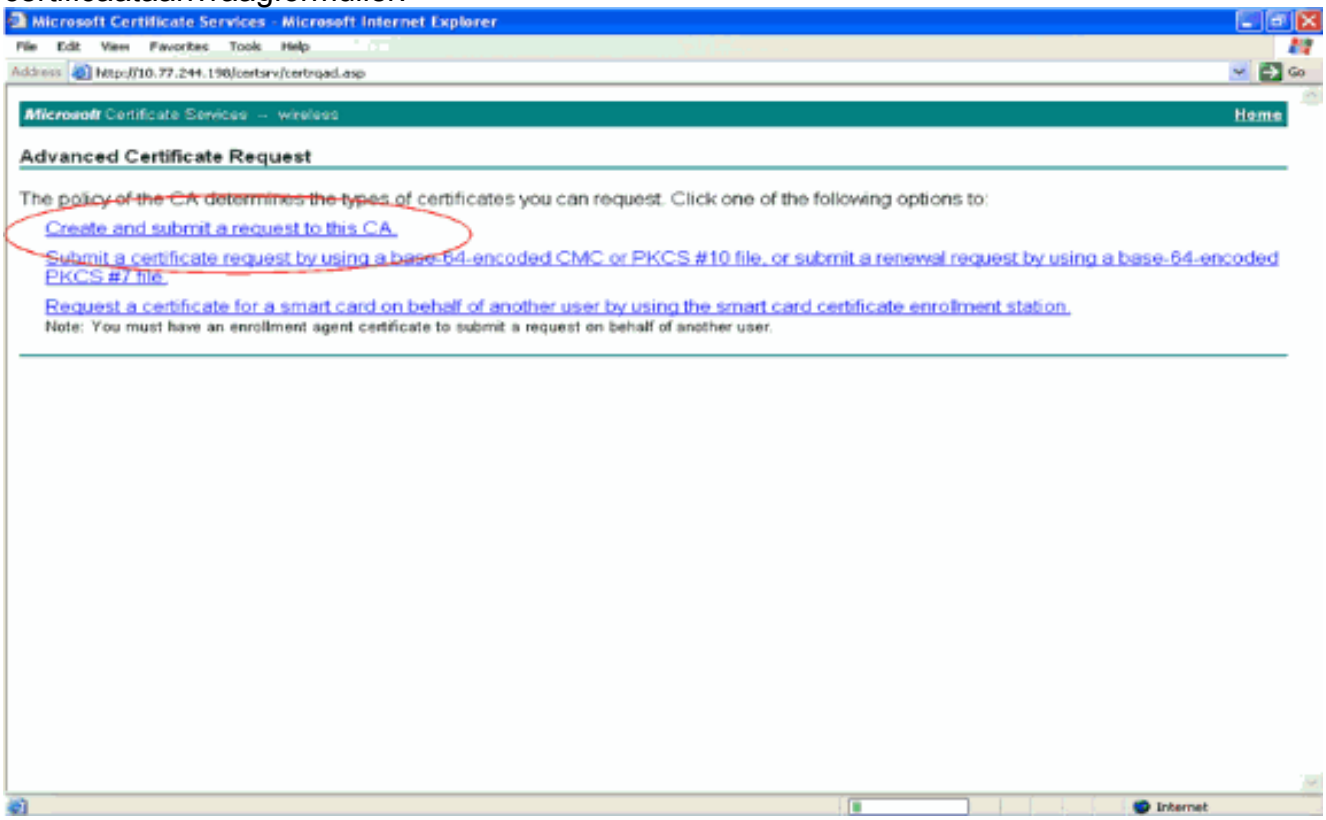

2. Selecteer **Certificaat aanvragen**.



3. Klik op de pagina Certificaat aanvragen op **Geavanceerd certificaatverzoek**.

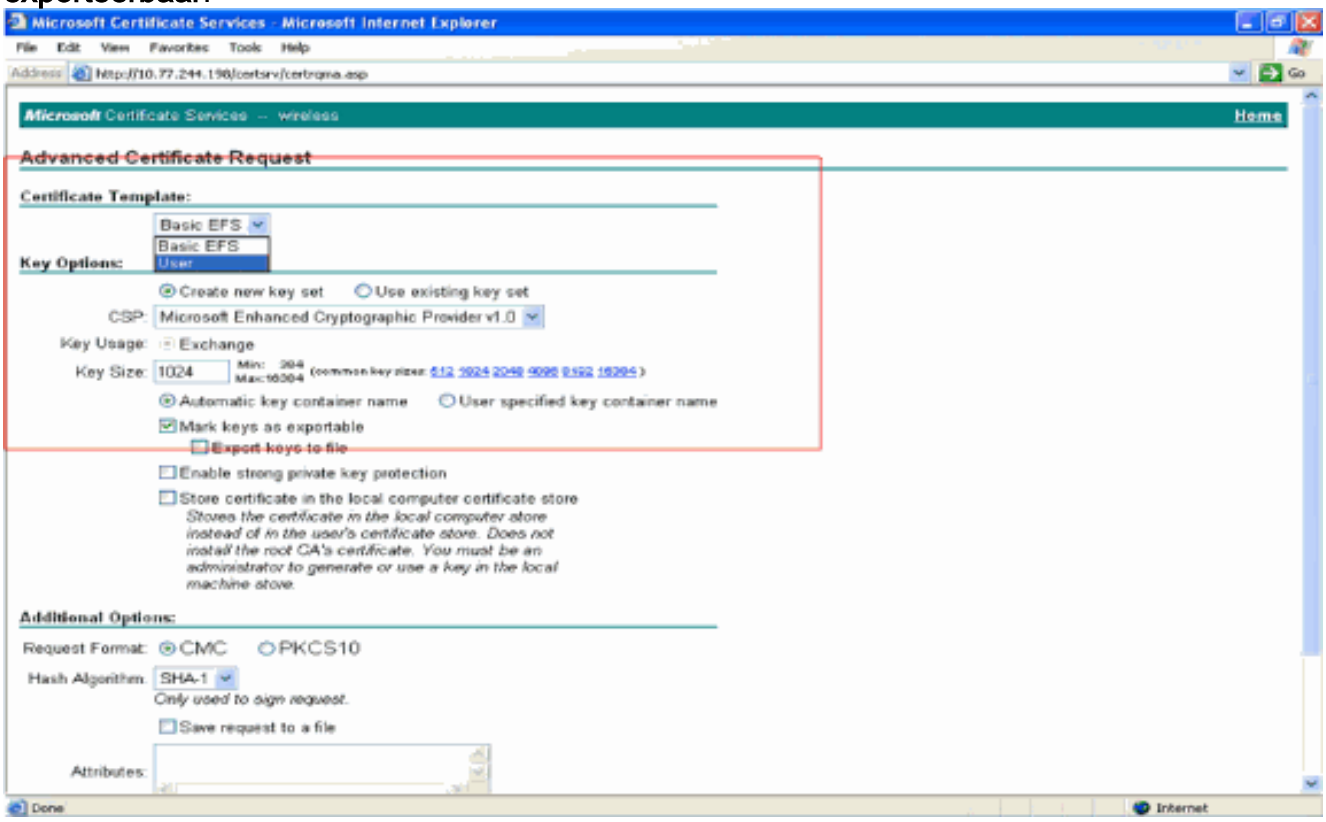



4. Klik op de pagina Geavanceerd certificaatverzoek op **Aanmaken en een aanvraag indienen bij deze certificeringsinstantie**. Dit brengt u naar het geavanceerde certificaataanvraagformulier.

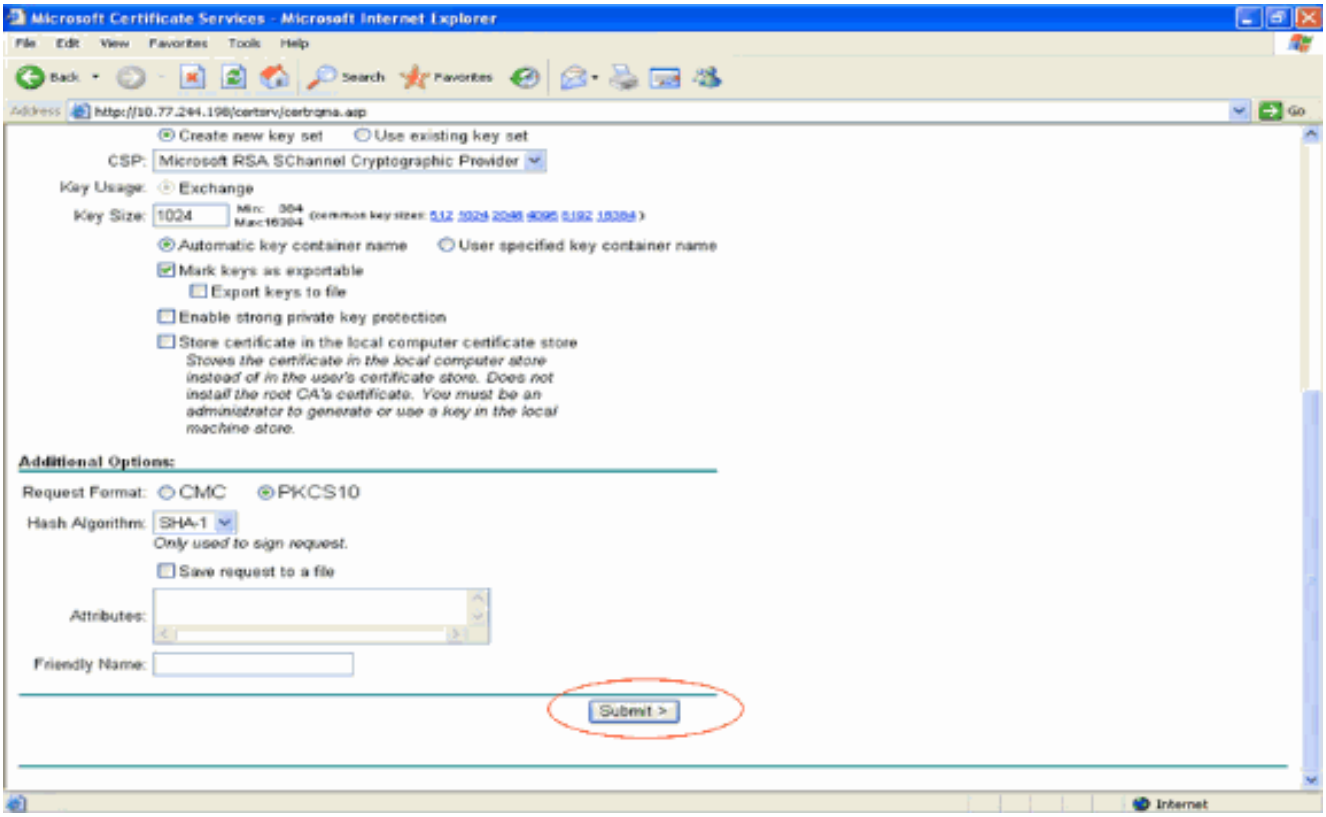



5. Kies in het aanvraagformulier voor Geavanceerd certificaat **Gebruiker** in het vervolgkeuzemenu Certificaatsjabloon.Kies in het gedeelte Belangrijkste opties deze parameters:Voer in het veld Sleutelgrootte de grootte in. In dit voorbeeld wordt **1024** gebruikt.Controleer de optie **Toetsen markeren als**

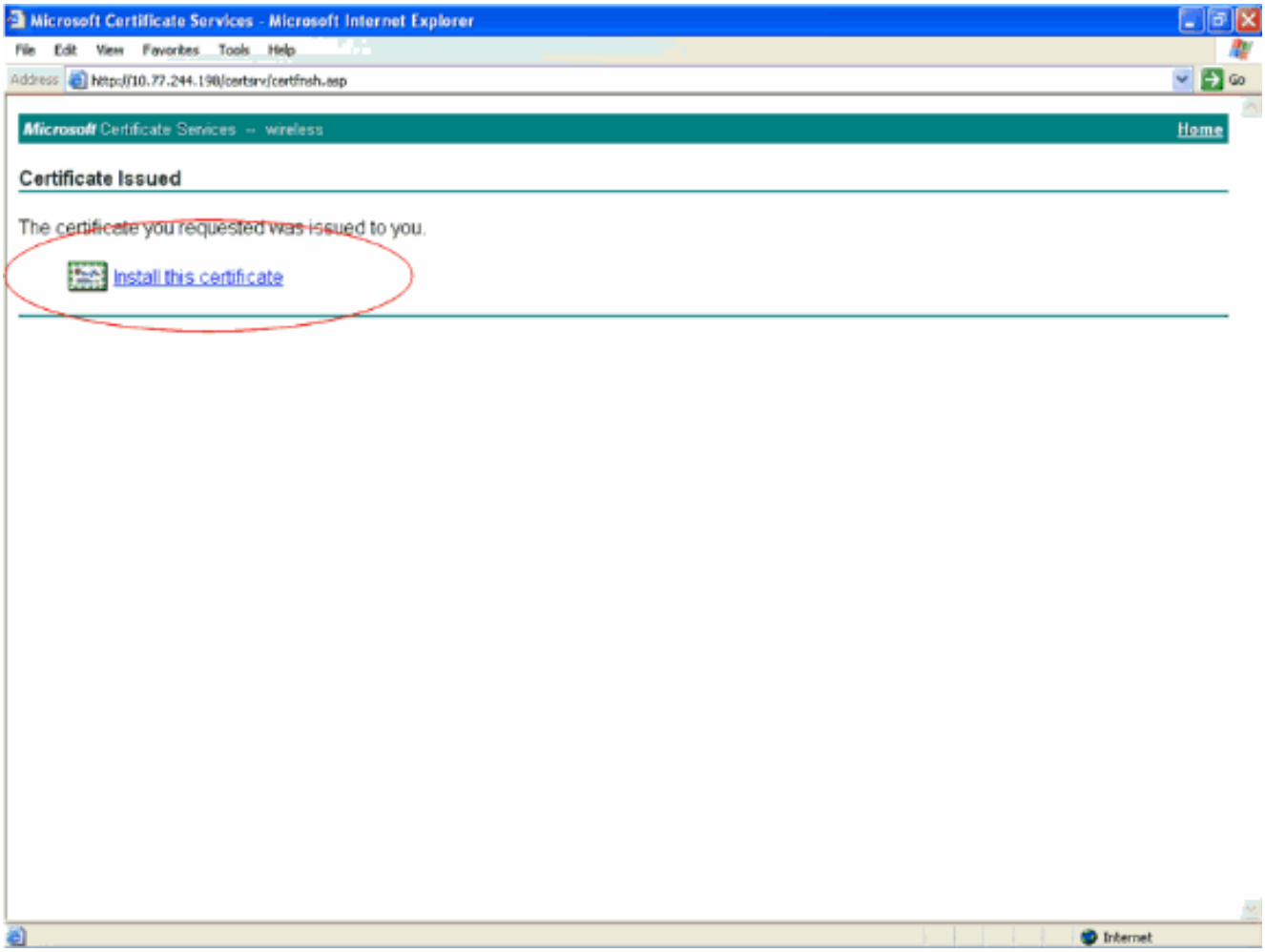
exporteerbaar.



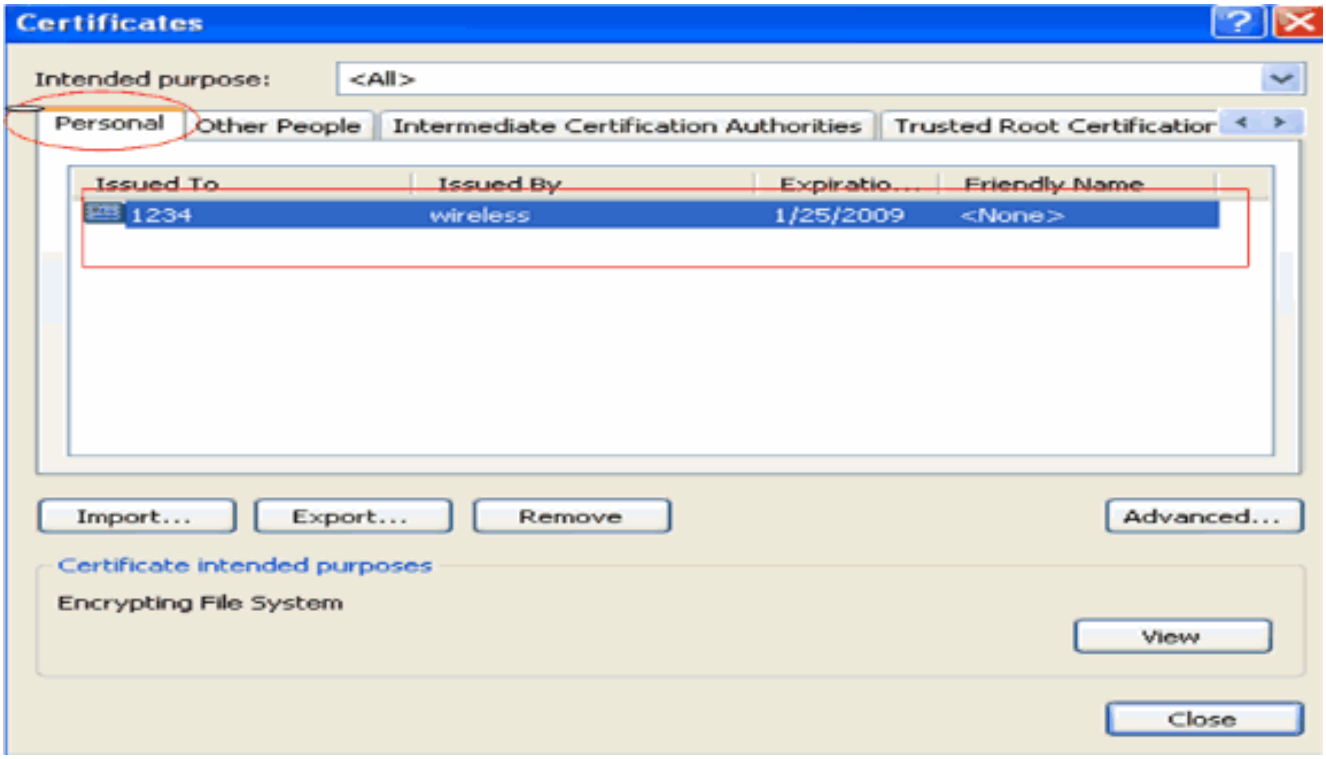

6. Configureer alle andere benodigde velden en klik op **Indienen**.




7. Het apparaatcertificaat van de client wordt nu gegenereerd op basis van de aanvraag. Klik op **Certificaat installeren** om het certificaat in het certificaatarchief te installeren.




8. U moet het apparaatcertificaat van de client kunnen vinden dat is geïnstalleerd onder de lijst met persoonlijke certificaten onder **Gereedschappen > Internet-opties > Inhoud > Certificaten** op de IE-browser van de client.

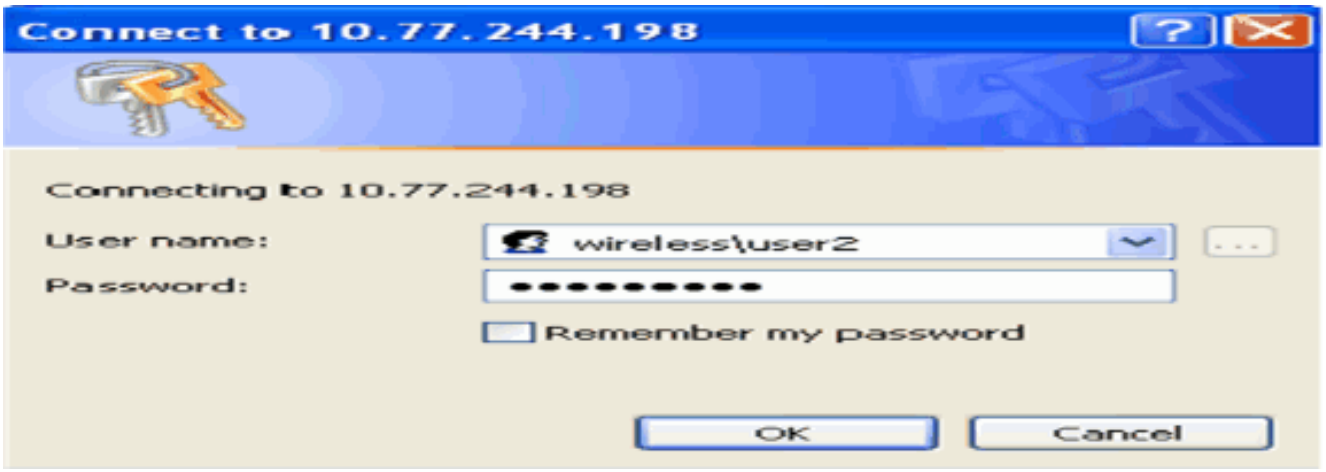



Het apparaatcertificaat voor de client is geïnstalleerd op de client.

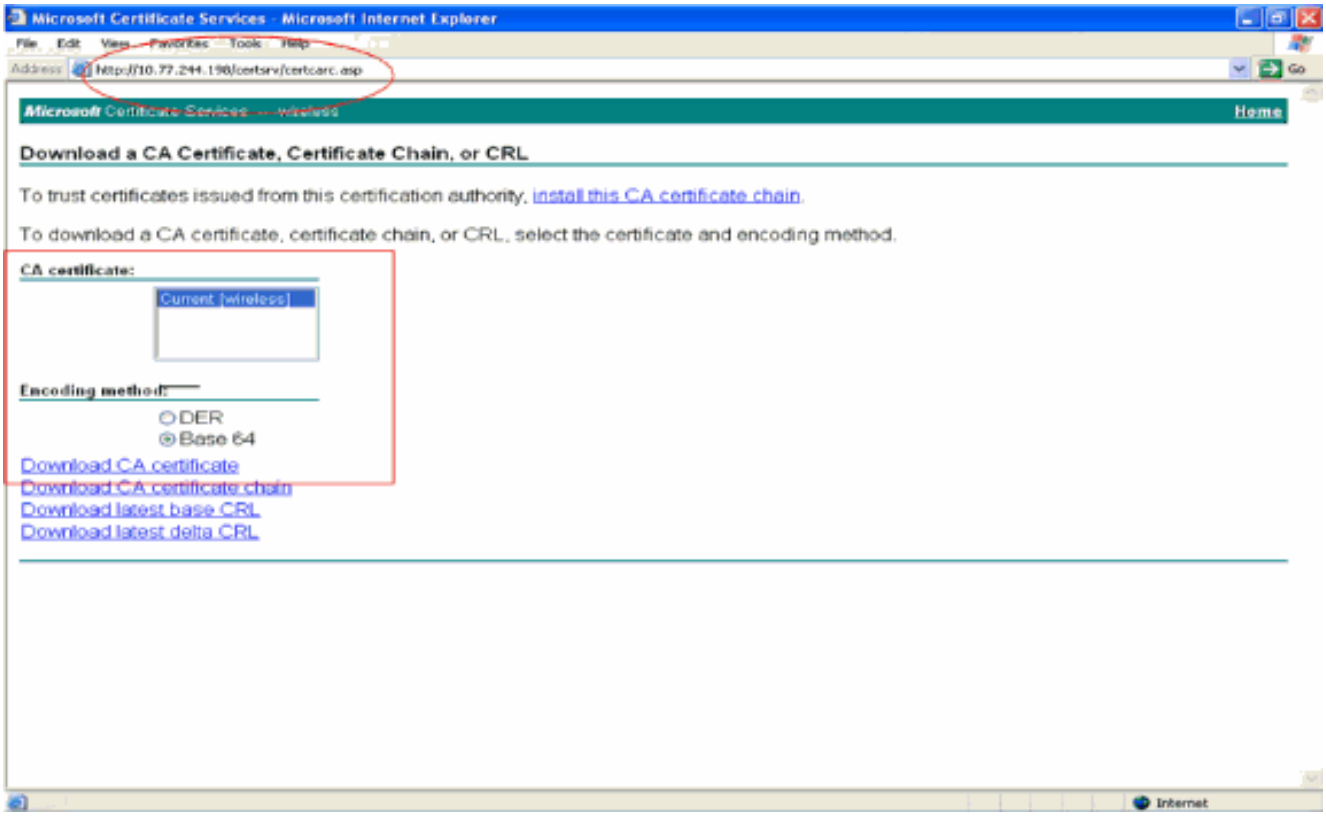
## Het CA-certificaat van de hoofdmap voor de client genereren

De volgende stap is het CA-certificaat voor de client te genereren. Voltooi de volgende stappen vanaf de client-pc:

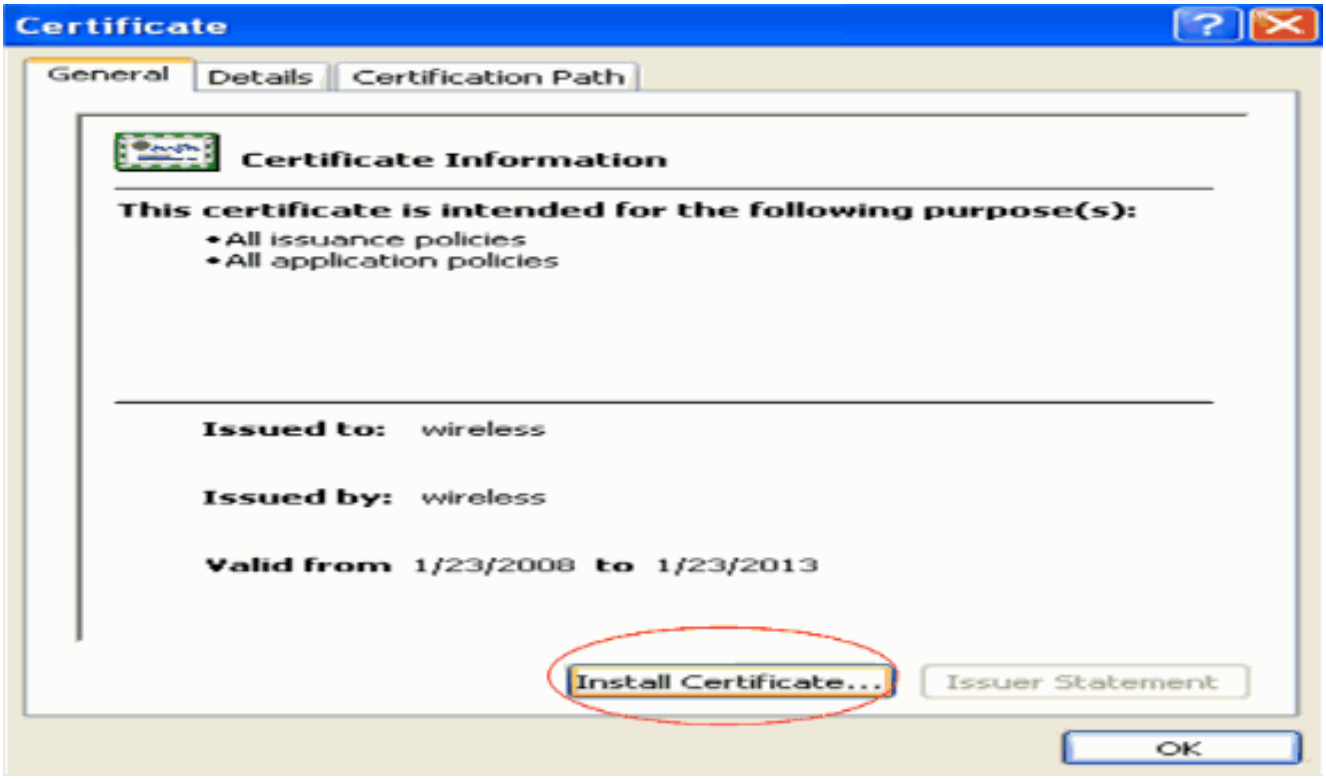
1. Ga naar **http://<IP-adres van CA-server>/certsrv** van de client waarvoor het certificaat moet worden geïnstalleerd. Aanmelden als domeinnaam\gebruikersnaam voor CA-server. De gebruikersnaam zou de naam moeten zijn van de gebruiker die deze XP machine gebruikt, en de gebruiker zou reeds moeten worden geconfigureerd als deel van hetzelfde domein als de CA-
server.



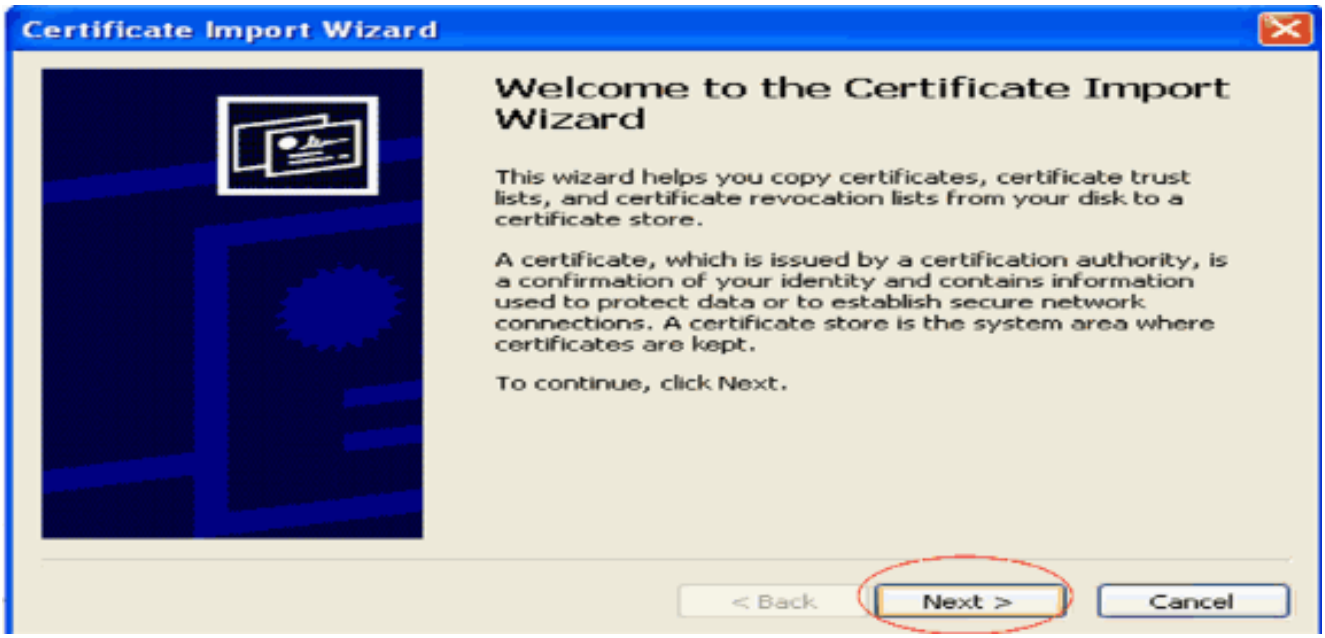

2. Op de resulterende pagina kunt u de huidige CA-certificaten zien die beschikbaar zijn op de CA-server onder het vakje **CA-certificaat**. Kies **Base 64** als de coderingsmethode. Klik vervolgens op **CA-certificaat downloaden** en sla het bestand op op de pc van de client als een **.cer**-bestand. Dit voorbeeld gebruikt **rootca.cer** als bestandsnaam.



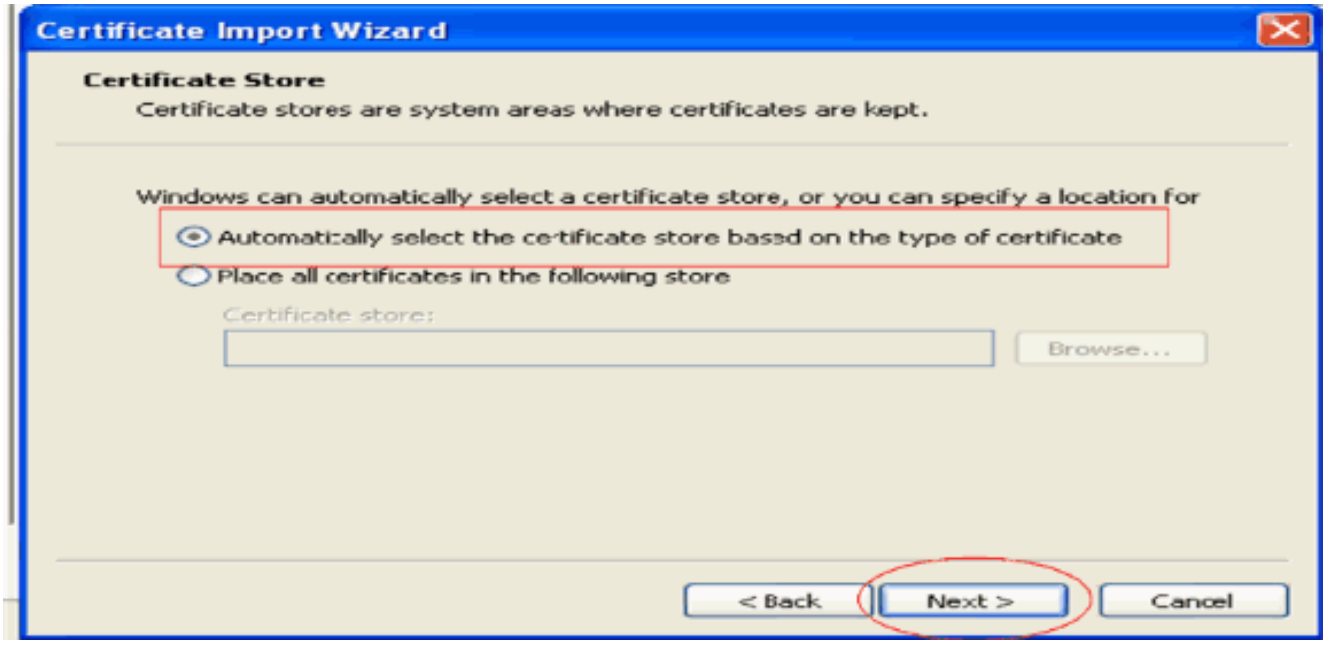

3. Installeer vervolgens het CA-certificaat dat is opgeslagen in .cer-indeling naar het certificaatarchief van de client. Dubbelklik op het bestand rootca.cer en klik op **Certificaat installeren**.



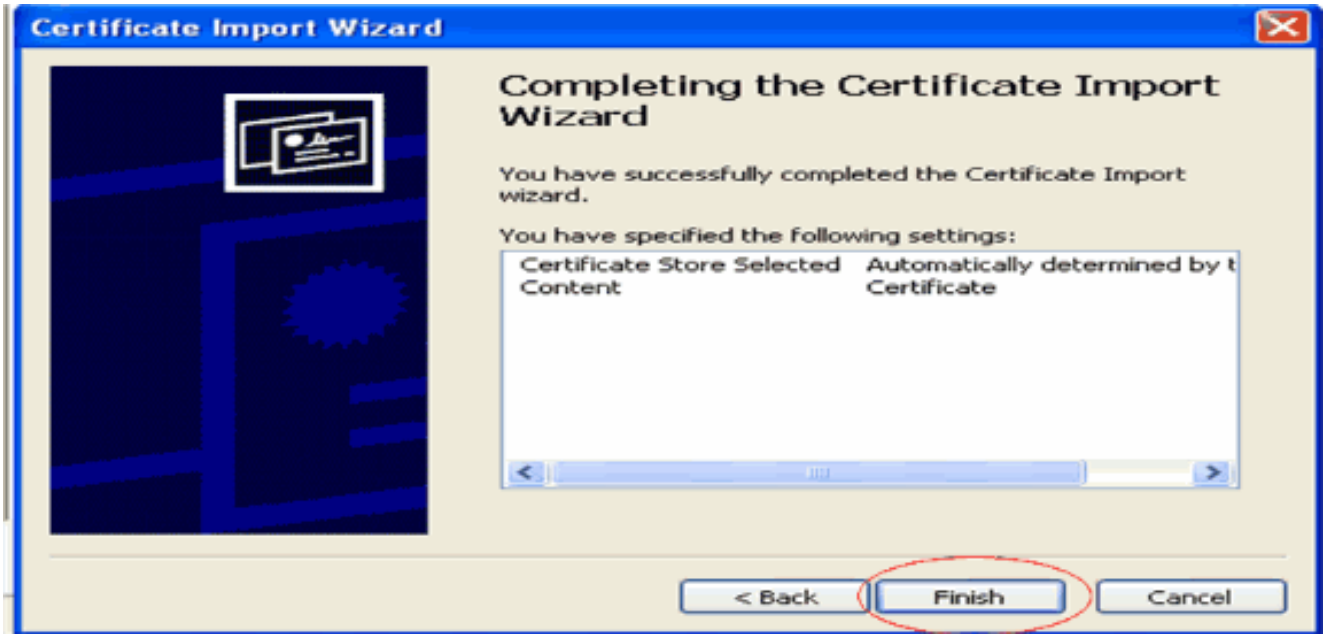

4. Klik op **Volgende** om het certificaat van de vaste schijf van de client te importeren in het certificaatarchief.



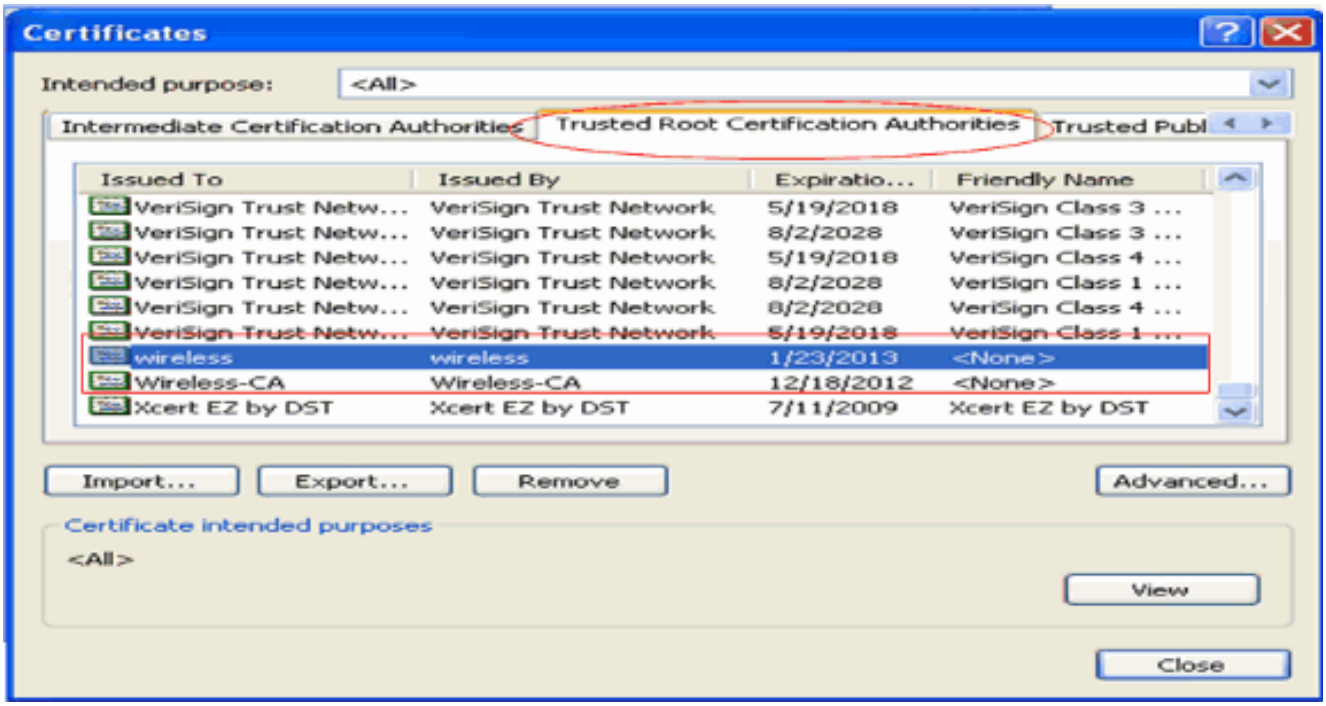

5. Kies **Automatisch het certificaatarchief selecteren op basis van het type certificaat** en klik op **Volgende**.




6. Klik op **Voltooien** om het importproces te voltooien.




7. CA-certificaten worden standaard geïnstalleerd onder de lijst met Trusted Root-certificeringsinstanties in de IE-browser van de client onder **Gereedschappen > Internet-opties > Inhoud > Certificaten**. Hier is het voorbeeld:

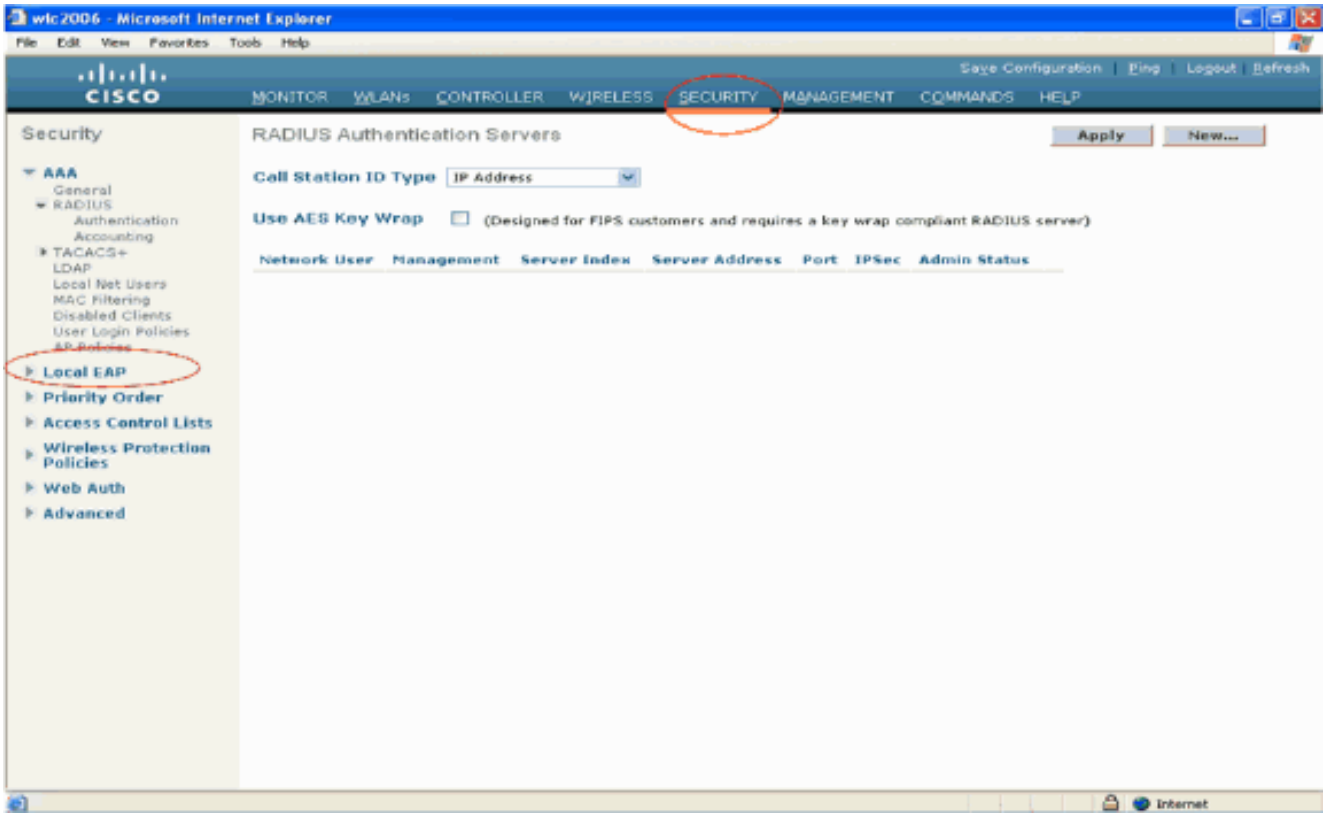



Alle vereiste certificaten zijn geïnstalleerd op de WLC en op de client voor EAP-FAST lokale EAP-verificatie. De volgende stap is de WLC te configureren voor lokale EAP-verificatie.

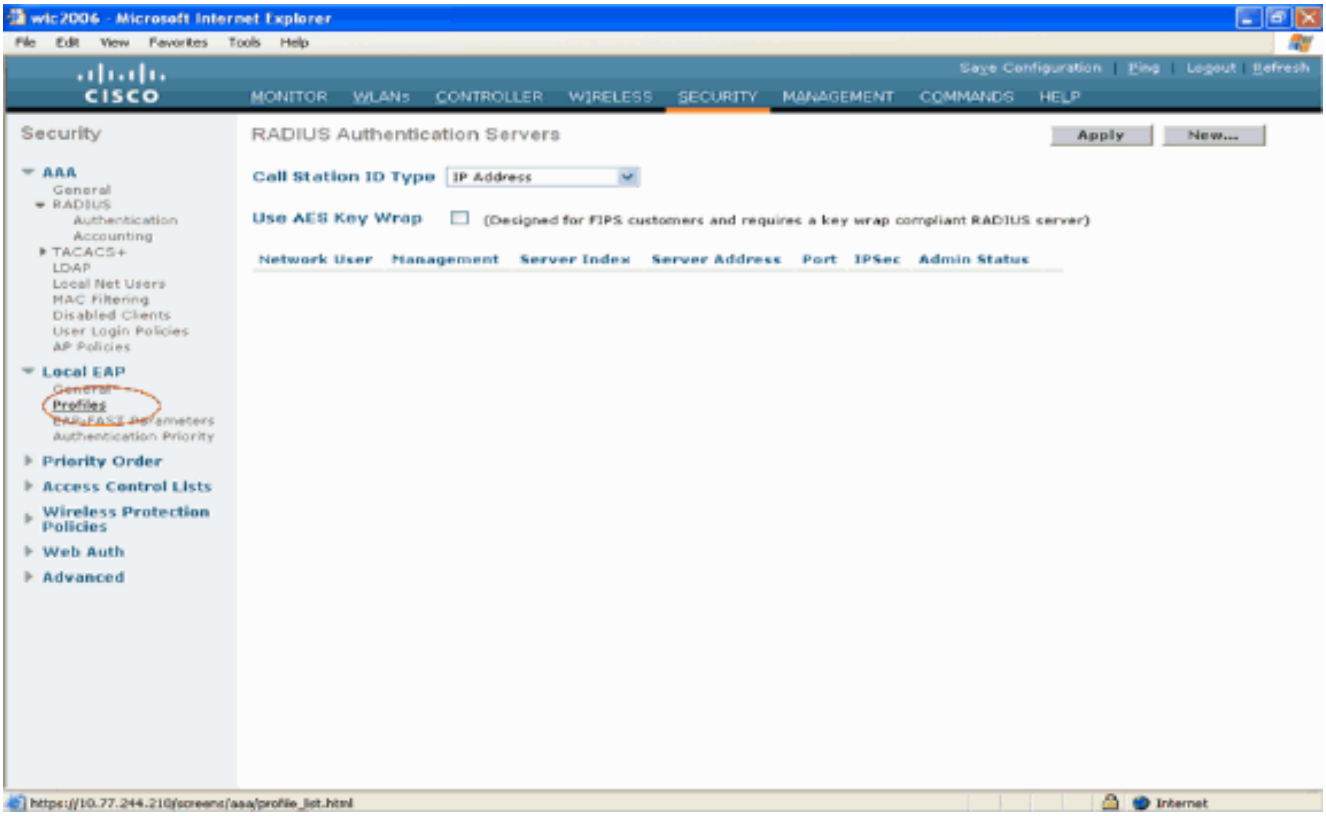
## Lokale EAP op de WLC configureren

Voltooi deze stappen van de **WLC GUI-modus** om Local EAP-verificatie op de WLC te configureren:

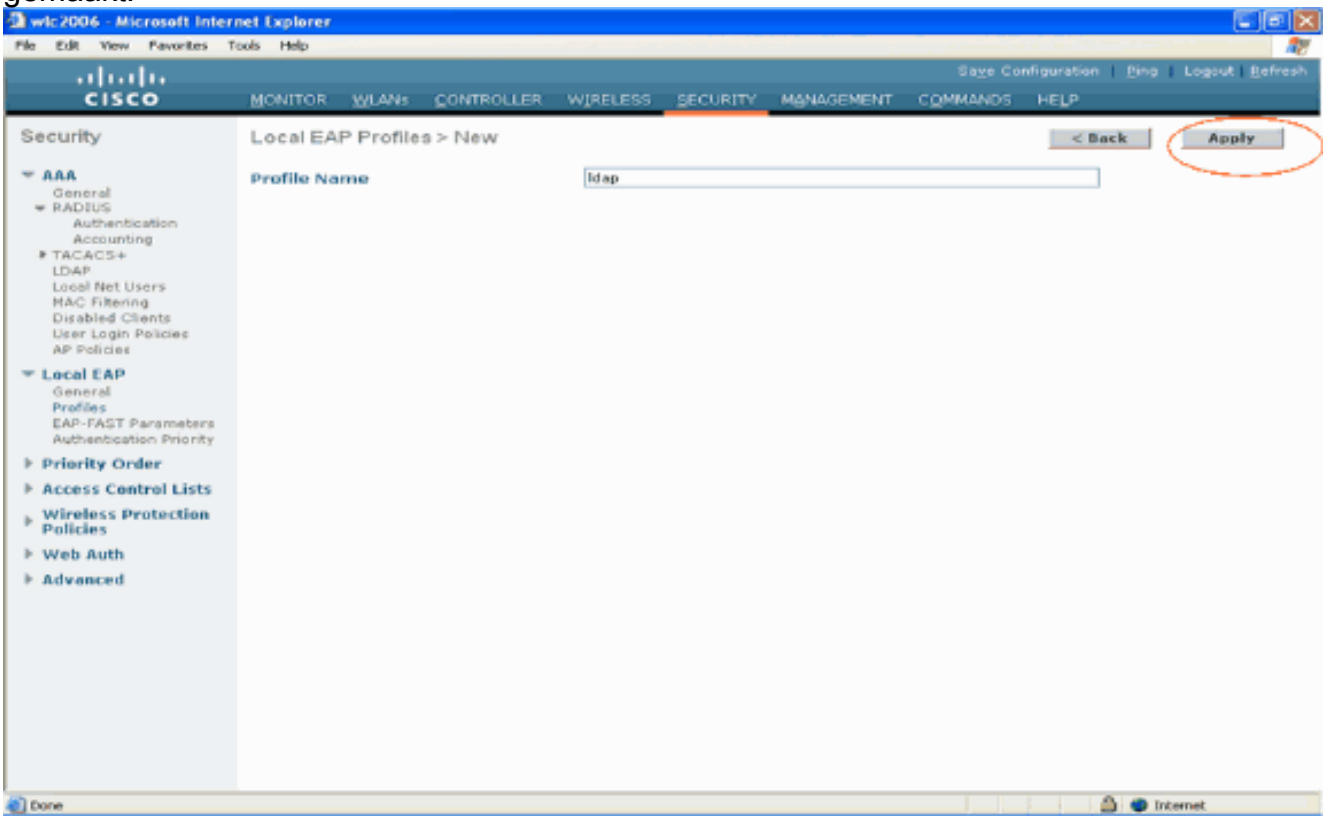
1. Klik op **Beveiliging > Lokale EAP**.



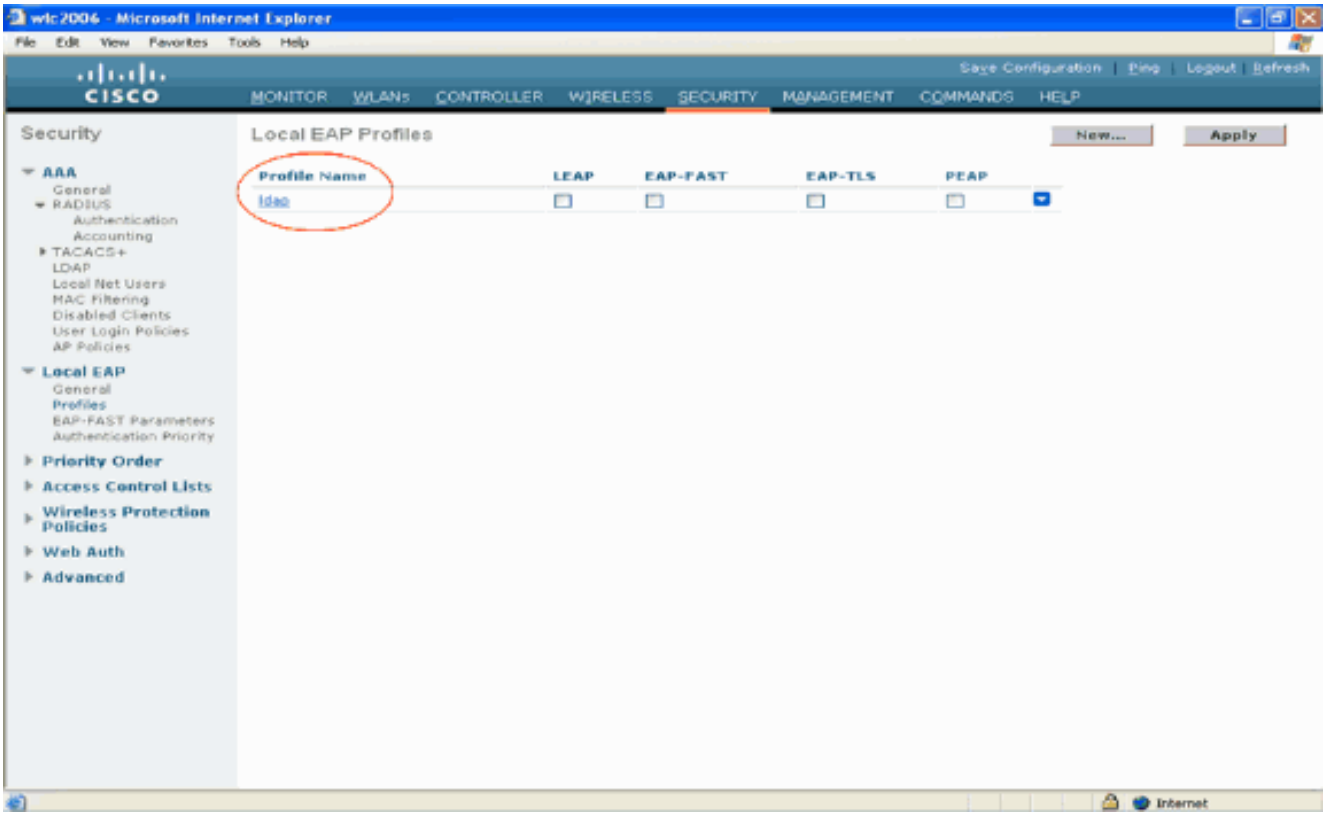

2. Klik onder Local EAP op **Profielen** om het lokale EAP-profiel te configureren.



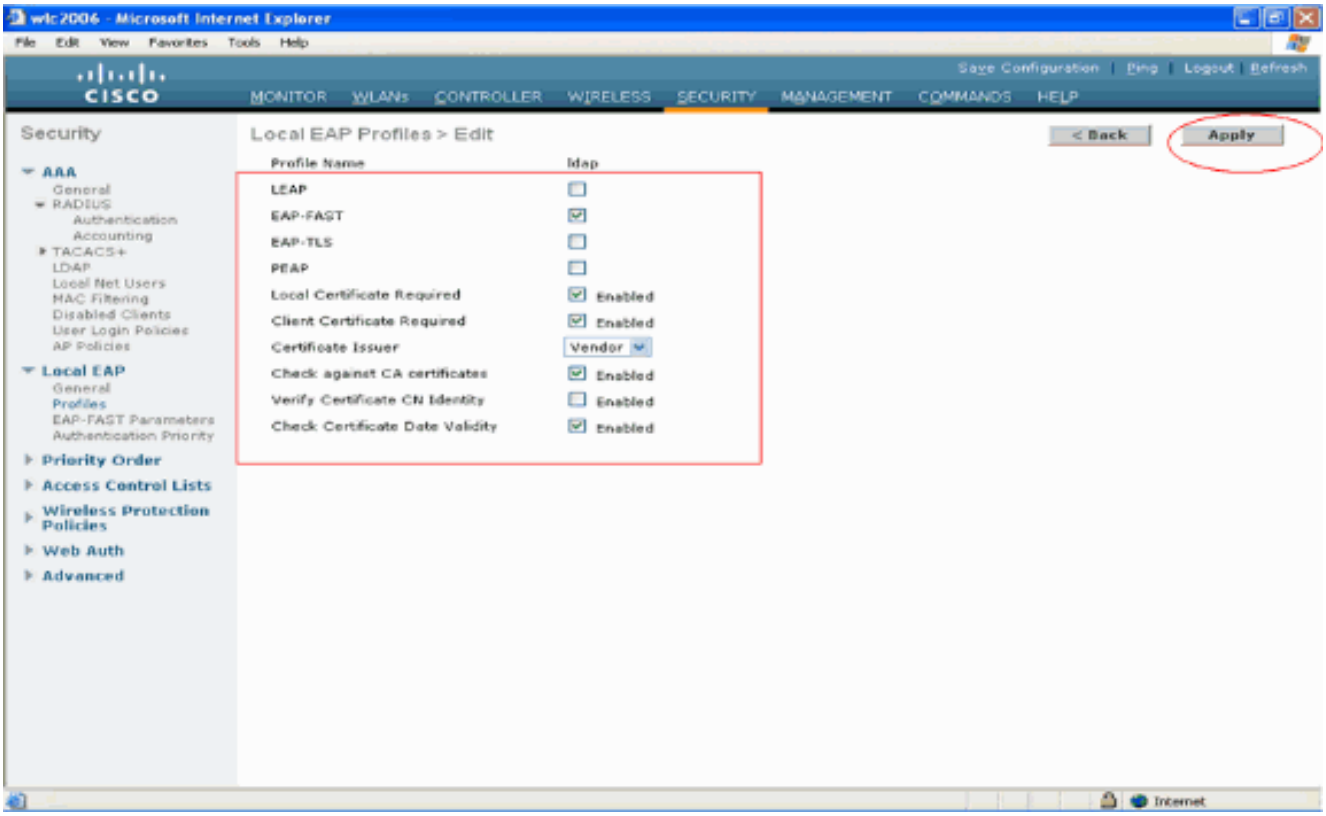

3. Klik op **Nieuw** om een nieuw lokaal EAP-profiel te maken.
4. Configureer een naam voor dit profiel en klik op **Toepassen**. In dit voorbeeld is de profielnaam **ldap**. Dit brengt u naar de lokale EAP-profielen die op de WLC zijn gemaakt.



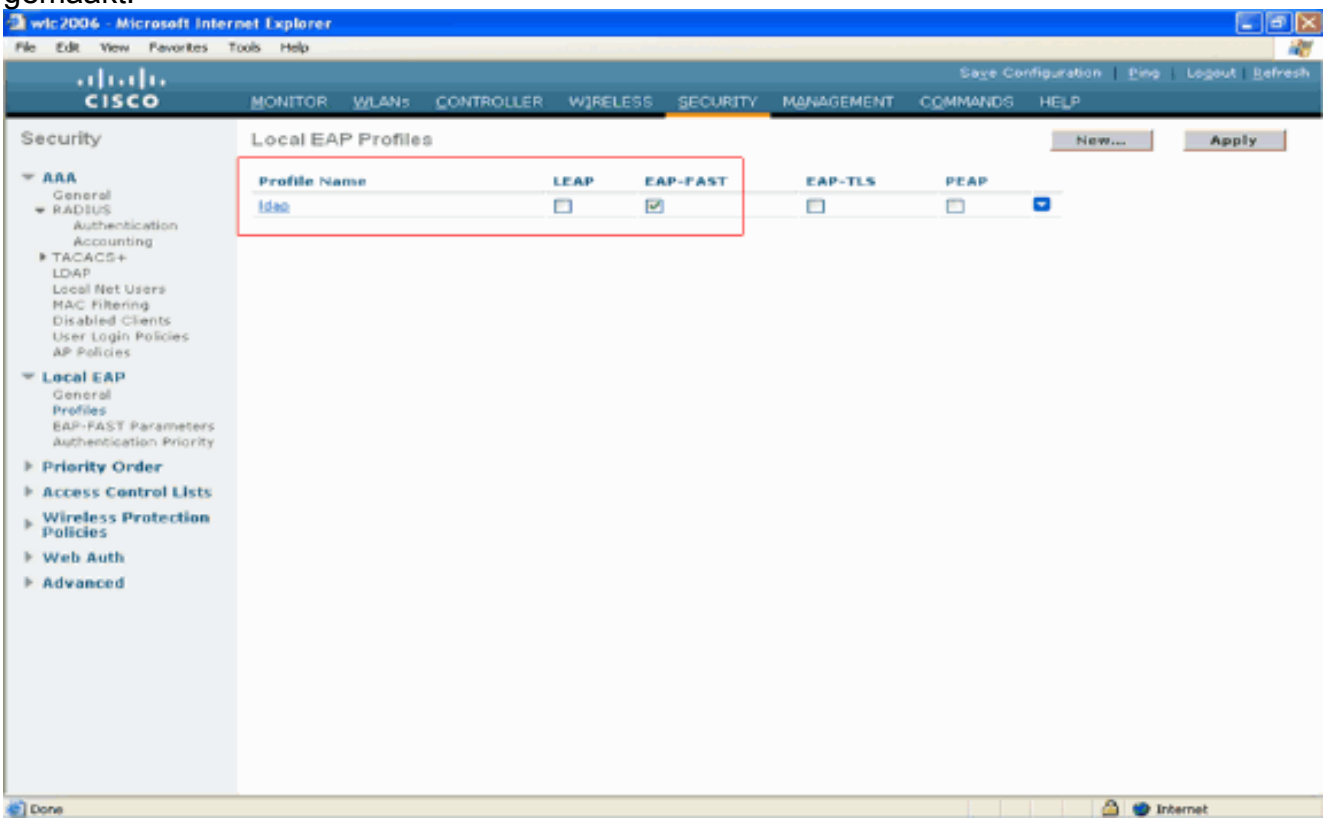

5. Klik op het **ladapprofiel** dat zojuist is gemaakt en dat wordt weergegeven onder het veld Profielnaam van de pagina Lokale EAP-profielen. Dit brengt u naar de **lokale EAP Profielen > Bewerken**
pagina.



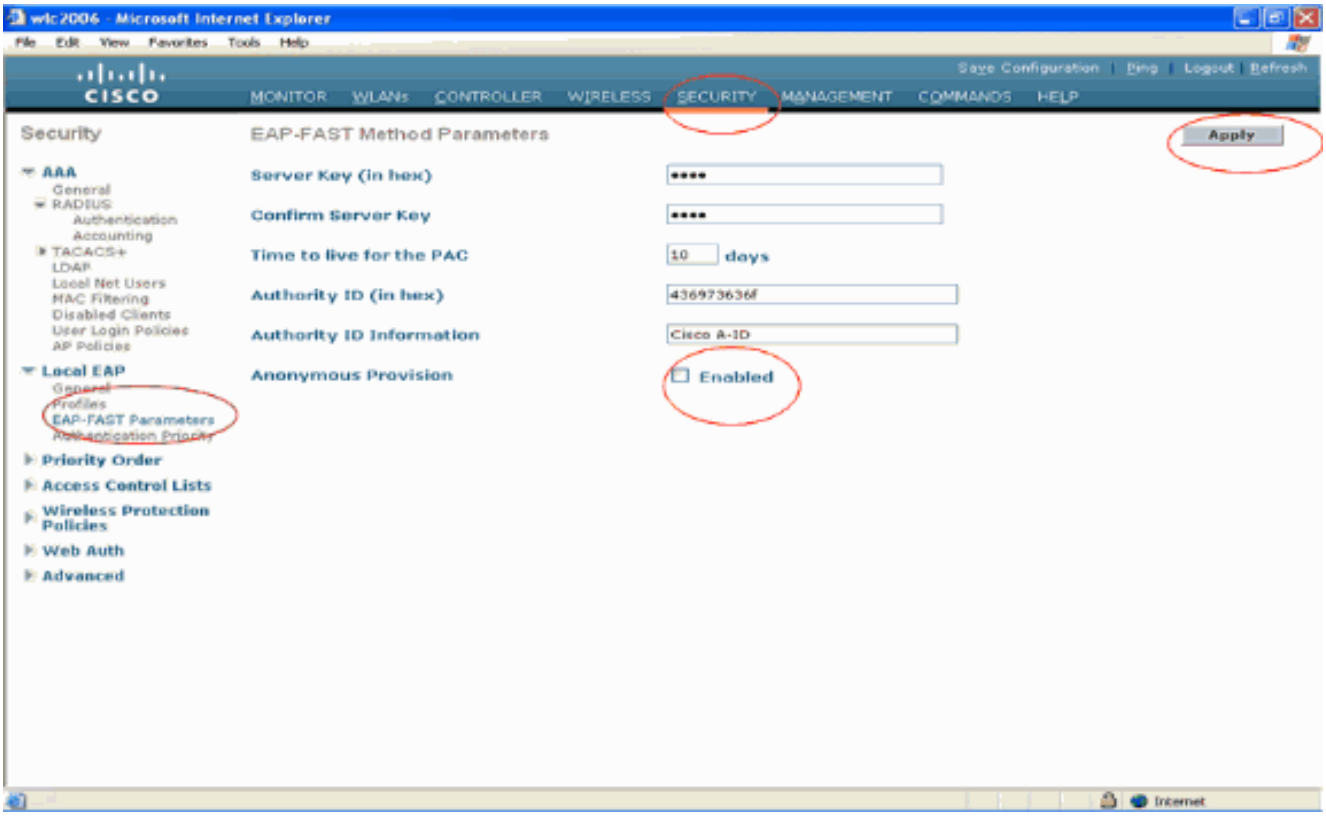

6. Configureer de parameters die specifiek zijn voor dit profiel op de pagina **Local EAP Profiles > Edit**.Kies **EAP-FAST** als de lokale EAP-verificatiemethode.Schakel de selectievakjes in naast **Lokaal certificaat vereist** en **Clientcertificaat vereist**.Kies **Verkoper** als Certificaatverlener omdat dit document gebruik maakt van een CA-server van derden.Schakel het aanvinkvakje naast **Controle op CA-certificaten** in om het inkomende certificaat van de client te laten valideren tegen de CA-certificaten op de controller.Als u wilt dat de gemeenschappelijke naam (GN) in het inkomende certificaat wordt gevalideerd tegen de CN van de CA-certificaten op de controller, kruis dan het aanvinkvakje **verify certificaat CN identity aan**. De standaardinstelling is uitgeschakeld. Om de controller in staat te stellen te controleren of het inkomende apparaatcertificaat nog steeds geldig is en niet is verlopen, kruist u het aanvinkvakje **Datum certificaat controleren en geldigheid controleren aan**.**Opmerking: de** geldigheid van de certificaatdatum wordt gecontroleerd aan de hand van de huidige UTC (GMT)-tijd die op de controller is ingesteld. Tijdzone offset wordt genegeerd.Klik op **Apply**
(Toepassen).




7. Het lokale EAP-profiel met EAP-FAST-verificatie wordt nu op de WLC gemaakt.



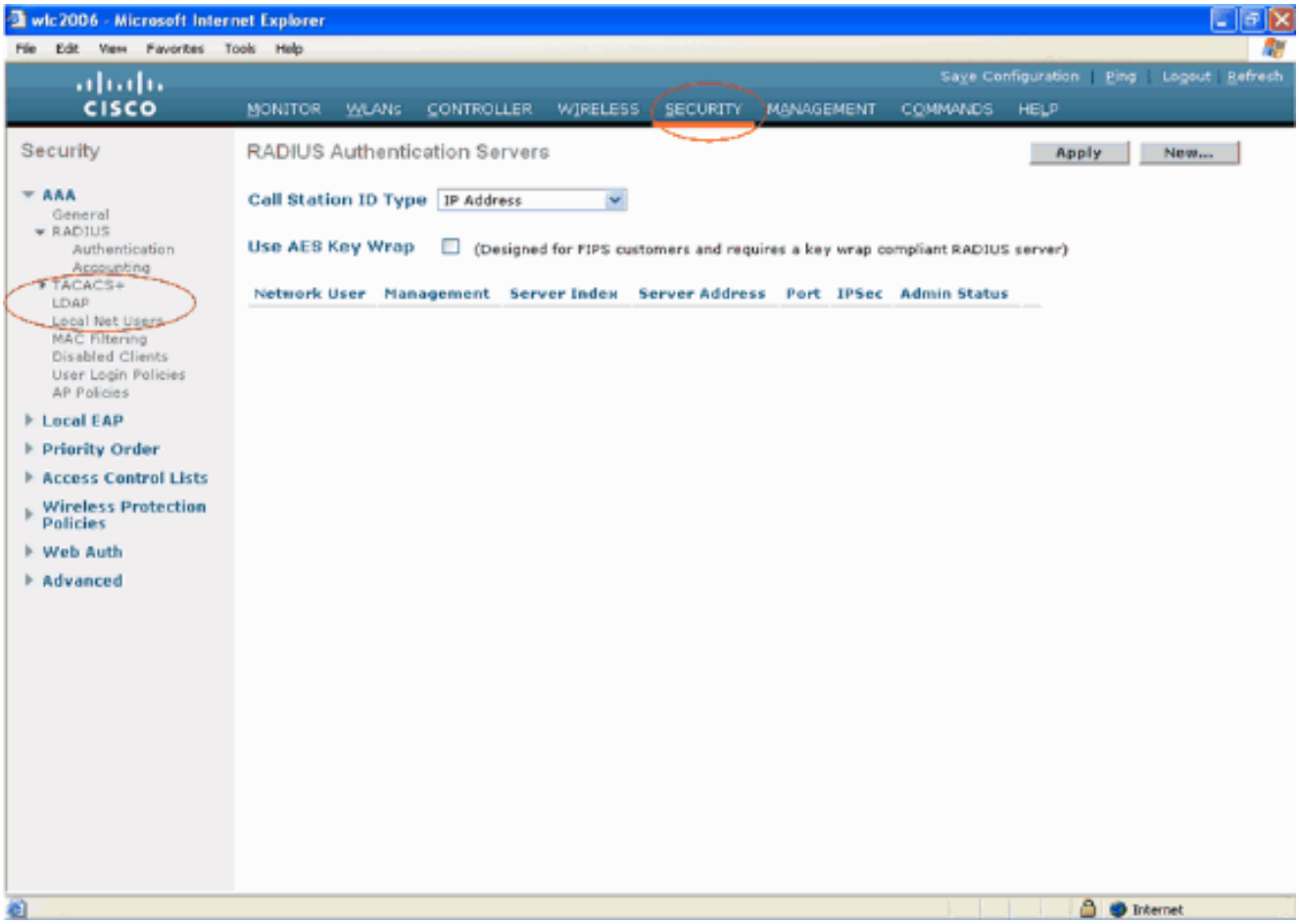

8. De volgende stap is EAP-FAST-specifieke parameters op de WLC te configureren. Klik op de pagina WLC Security op **Local EAP > EAP-FAST-parameters** om naar de pagina EAP-FAST-methodeparameters te gaan.Schakel het aanvinkvakje **Anonymous Provision uit** omdat dit voorbeeld EAP-FAST met certificaten verklaart. Laat alle andere parameters in gebreke. Klik op **Apply**
(Toepassen).




## WLC configureren met Details van LDAP Server

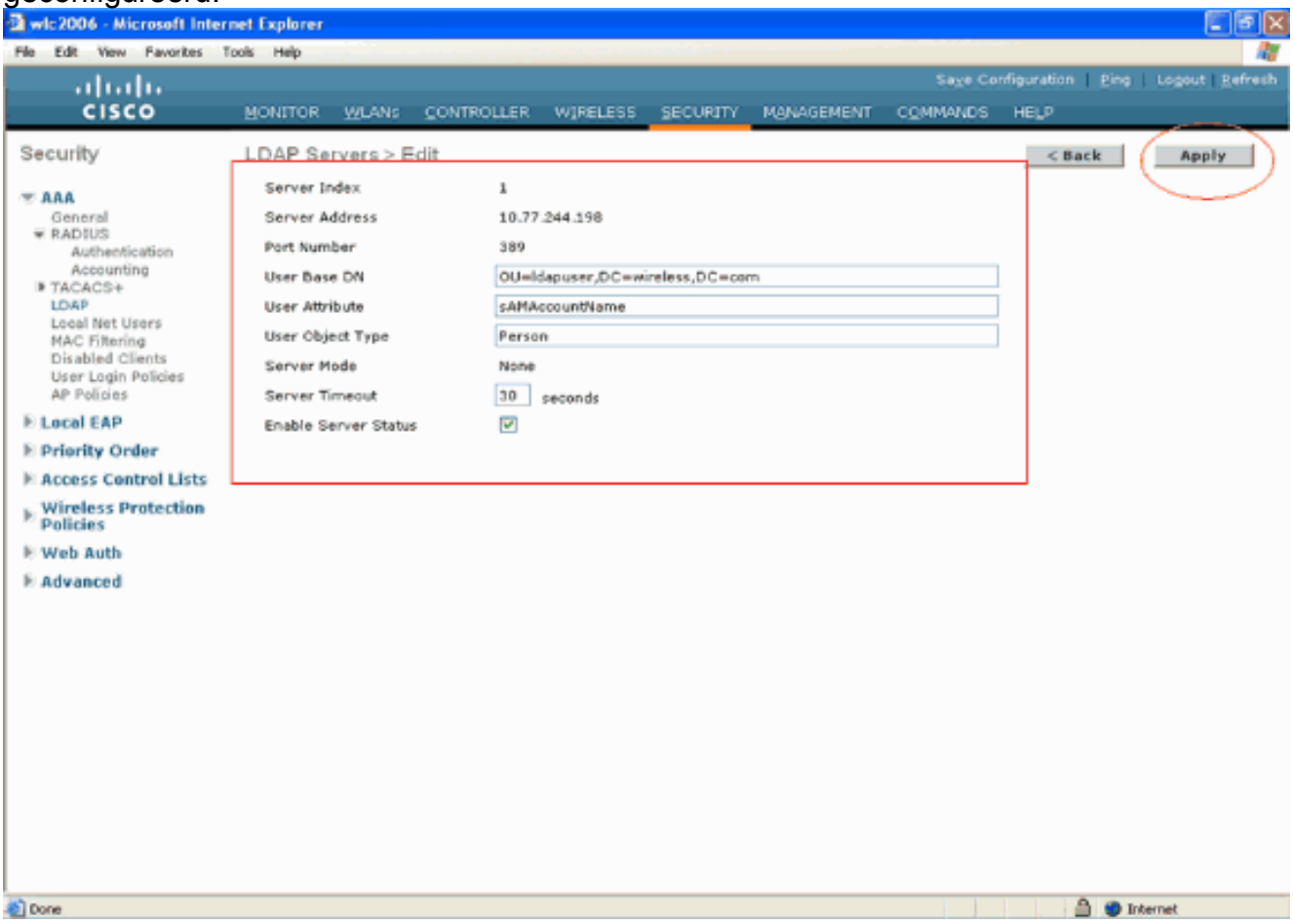
Nu de WLC is geconfigureerd met het Local EAP-profiel en de bijbehorende informatie, is de volgende stap om de WLC te configureren met details van de LDAP-server. Voltooi deze stappen op WLC:

1. Selecteer op de pagina **Security** van de WLC de optie **AAA > LDAP** in het taakvenster aan de linkerkant om naar de configuratiepagina van de LDAP-server te gaan. Klik op **Nieuw** om een LDAP-server toe te voegen. De pagina **LDAP Servers > New** verschijnt.




2. Geef in de pagina Bewerken LDAP-servers de gegevens op van de LDAP-server, zoals IP-adres van LDAP-server, poortnummer, serverstatus inschakelen enzovoort.Kies een nummer uit de vervolgkeuzelijst **Server Index (Prioriteit)** om de prioriteitsvolgorde van deze server te specificeren ten opzichte van alle andere geconfigureerde LDAP-servers. U kunt maximaal zeventien servers configureren. Als de controller de eerste server niet kan bereiken, probeert het de tweede server in de lijst enzovoort.Voer in het veld **IP-adres** van de LDAP-server het IP-adres van de **server in**.Voer het TCP-poortnummer van de LDAP-server in het veld **Poortnummer in**. Het geldige bereik loopt van 1 tot 65535 en de standaardwaarde is **389**.Voer in het veld **User Base DN** de voorname naam (DN) in van de substructuur in de LDAP-server die een lijst van alle gebruikers bevat. Bijvoorbeeld, ou=organisationele eenheid, .ou=volgende organisatorische eenheid, en o=corporation.com. Als de boom die gebruikers bevat de basis DN is, ga o=corporation.com of dc=corporation, dc=com in.In dit voorbeeld, wordt de gebruiker gevestigd onder de Organisatorische Eenheid (OU) **ldapuser** die beurtelings als deel van het domein van **Wireless.com** wordt gecreëerd.De gebruikersbasis-DN moet het volledige pad aangeven waar de gebruikersinformatie (gebruikersreferenties volgens de EAP-FAST-verificatiemethode) zich bevindt. In dit voorbeeld bevindt de gebruiker zich onder de basis DN OU=ldapuser, DC=Wireless, DC=com.Meer informatie over OE en de configuratie van de gebruiker vindt u in het gedeelte Gebruikers maken op de domeincontroller van dit document.Voer in het veld **Gebruikerskenmerken** de naam van het kenmerk in in de gebruikersrecord die de gebruikersnaam bevat.Voer in het veld **User Object Type** de waarde in van het kenmerk LDAP objectType dat de record als gebruiker identificeert. Vaak hebben gebruikersrecords verschillende waarden voor het objectType-kenmerk, waarvan sommige uniek zijn voor de gebruiker en sommige met andere objecttypes worden gedeeld.**Opmerking:** U kunt de waarde van deze twee velden uit uw directory server verkrijgen met de LDAP browser utility, die wordt geleverd als onderdeel van de Windows 2003 support tools. **Deze Microsoft LDAP**

**browser tool wordt LDP genoemd.** Met behulp van deze tool kunt u de velden Gebruikersbasis-DN, Gebruikerskenmerk en Gebruikersobjecttype van deze specifieke gebruiker kennen. Gedetailleerde informatie over het gebruik van LDP om deze gebruikerspecifieke kenmerken te kennen, wordt besproken in het gedeelte Gebruikerskenmerken gebruiken om de sectie Gebruikerskenmerken van dit document te identificeren.Kies **Secure** uit de vervolgkeuzelijst Servermodus als u wilt dat alle LDAP-transacties een beveiligde TLS-tunnel gebruiken. Anders kiest u **Geen**, wat de standaardinstelling is.Voer in het veld **Server Time-out** het aantal seconden in tussen hertransmissies. Het geldige bereik is 2 tot 30 seconden en de standaardwaarde is 2 seconden.Schakel het selectievakje **Serverstatus inschakelen in** om deze LDAP-server in te schakelen of uit om deze uit te schakelen. De standaardwaarde is uitgeschakeld.Klik op **Toepassen** om de wijzigingen te doorvoeren.Hier is een voorbeeld dat al met deze informatie is
geconfigureerd:



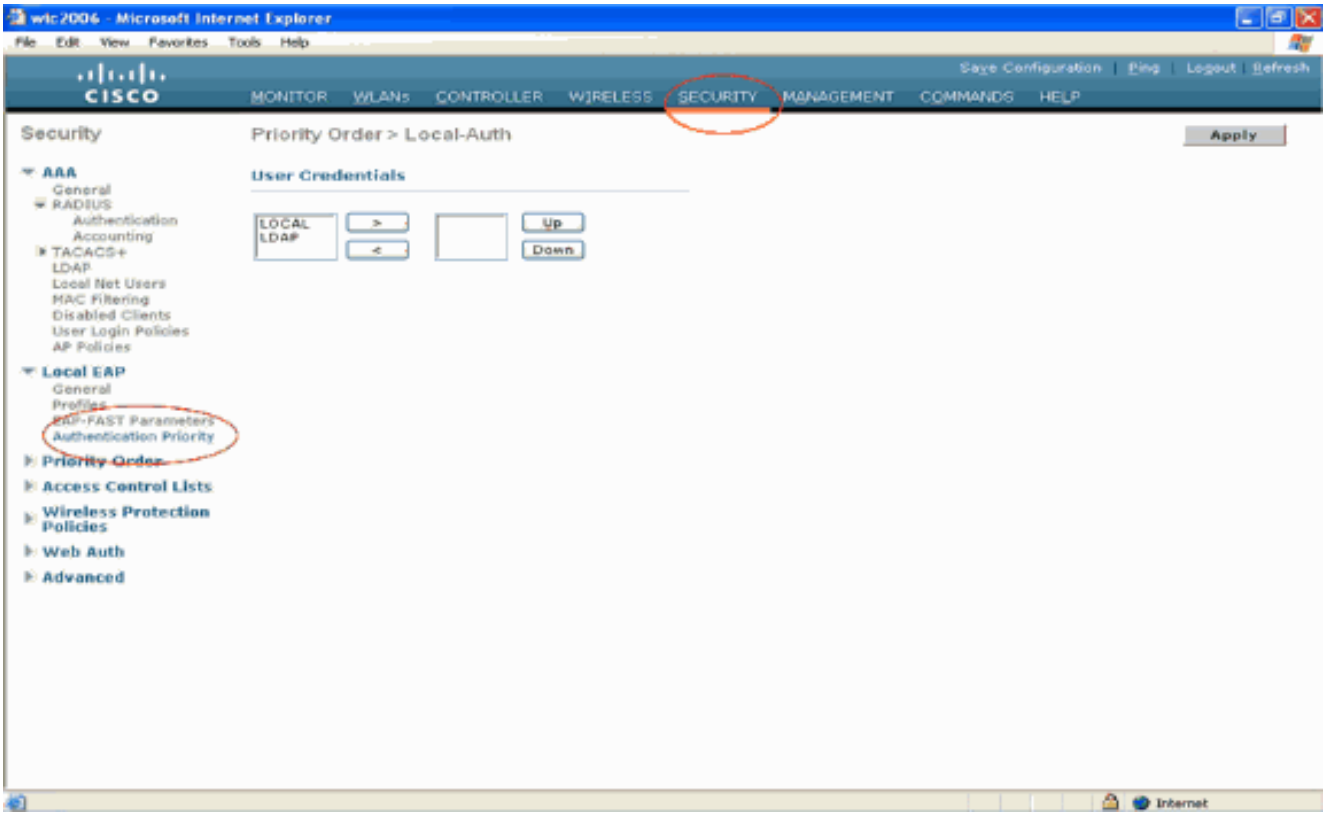

Nu de details over de LDAP server op de WLC zijn geconfigureerd, is de volgende stap om LDAP te configureren als de prioriteitsback-end database, zodat de WLC eerst naar de LDAP database kijkt voor gebruikersreferenties in plaats van naar andere databases.

## LDAP configureren als de prioriteitsdatabase voor backend

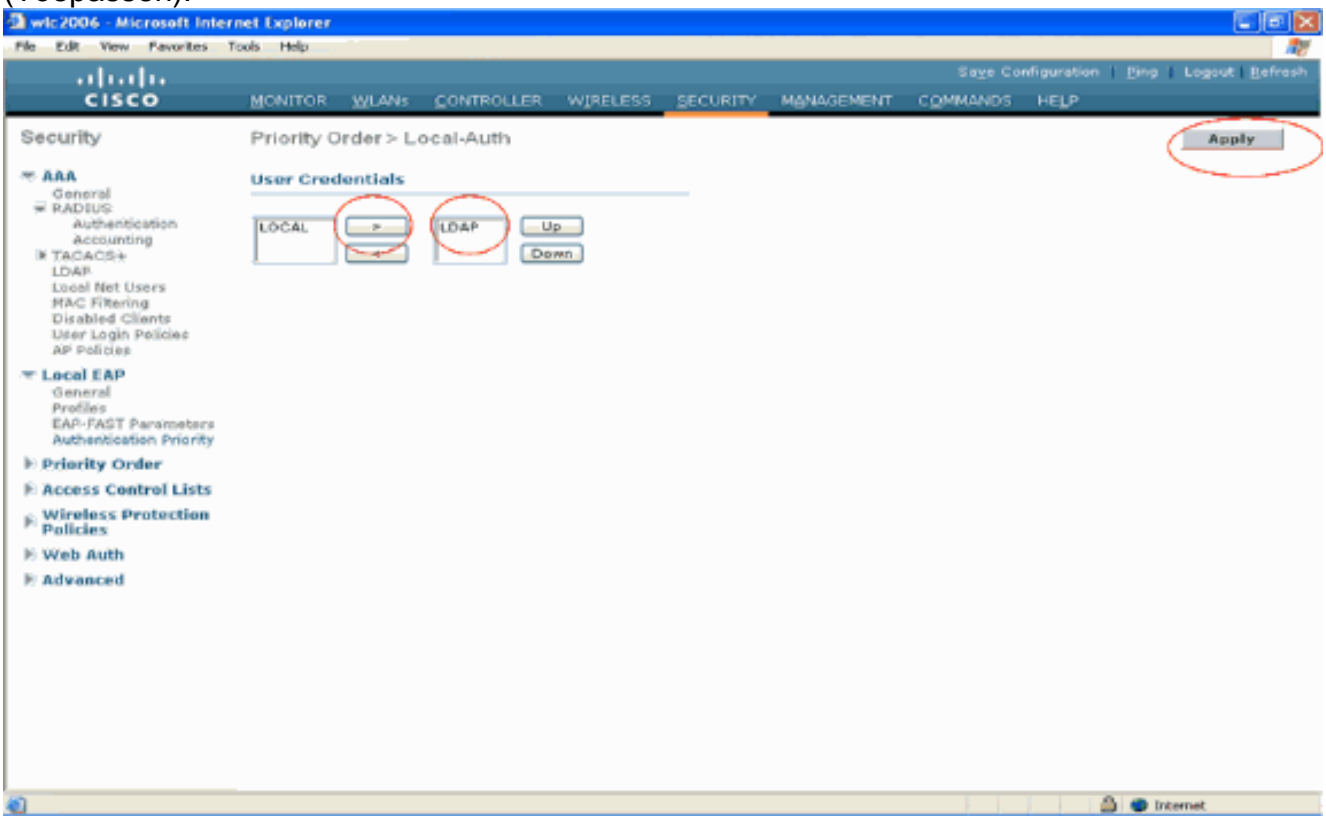
Voltooi deze stappen op de WLC om LDAP te configureren als de prioritaire backend database:

1. Klik op de pagina Beveiliging op **Lokale EAP > Verificatieprioriteit**. In de pagina Prioriteitsvolgorde > Local-Auth kunt u twee databases (Local en LDAP) vinden die de gebruikersreferenties kunnen opslaan.Als u LDAP als prioriteitsdatabase wilt maken, kiest u **LDAP** uit het veld Gebruikersreferenties links en klikt u op de knop **>** om LDAP te

verplaatsen naar het veld Prioriteitsvolgorde aan de rechterkant.




2. Dit voorbeeld laat duidelijk zien dat LDAP in het linkervak is gekozen en dat de **>**toets is geselecteerd. Hierdoor wordt LDAP verplaatst naar het vak aan de rechterkant dat de prioriteit bepaalt. De LDAP-database wordt gekozen als de verificatie-prioriteitsdatabase.Klik op **Apply** (Toepassen).



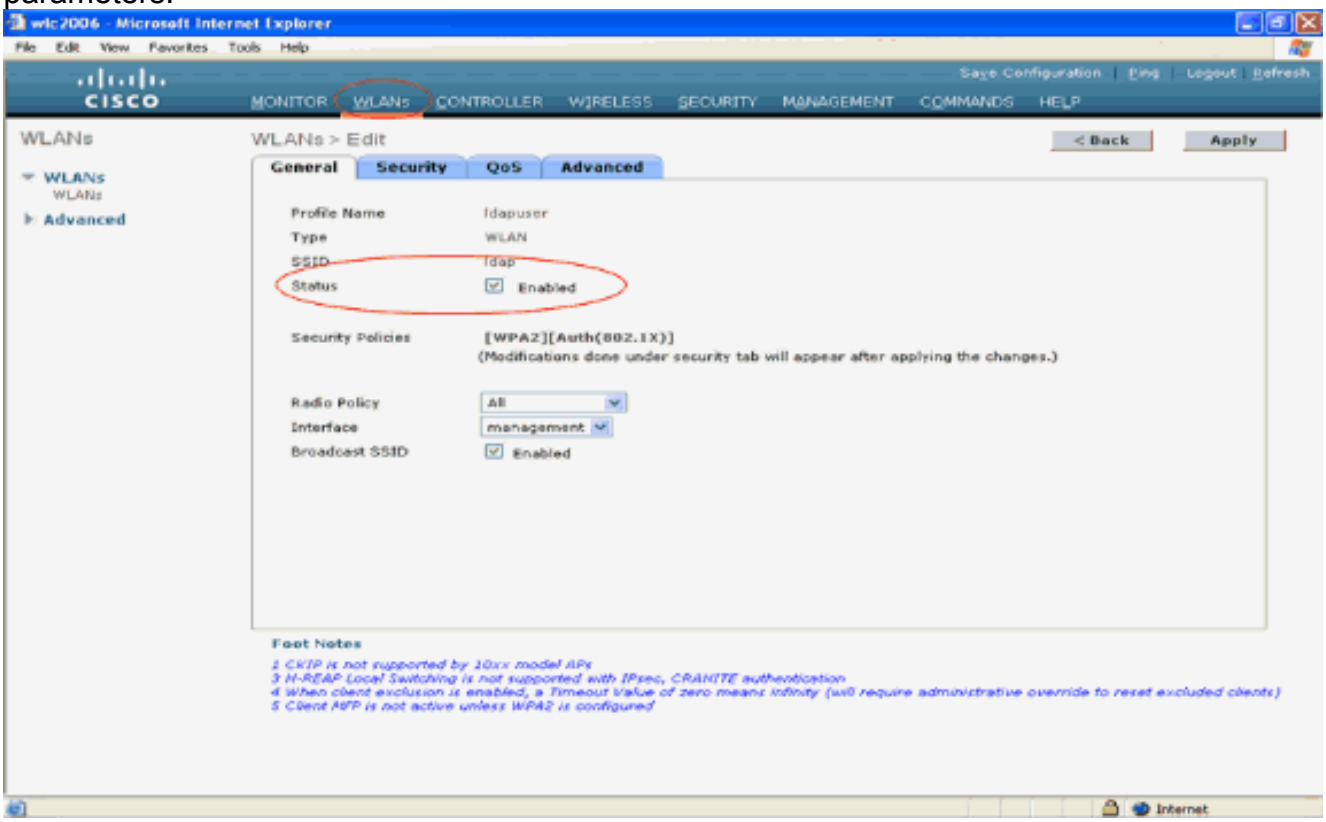

**Opmerking:** Als zowel LDAP als LOCAL in het rechtervak User Credentials met LDAP bovenaan en LOCAL onderaan verschijnen, probeert Local EAP om clients te verifiëren met

behulp van de LDAP-back-end database en faalt over naar de lokale gebruikersdatabase als de LDAP-servers niet bereikbaar zijn. Als de gebruiker niet wordt gevonden, wordt de verificatiepoging geweigerd. Als LOCAL zich bovenaan bevindt, probeert Local EAP alleen met de lokale gebruikersdatabase te verifiëren. Het faalt niet over naar de LDAP backend database.

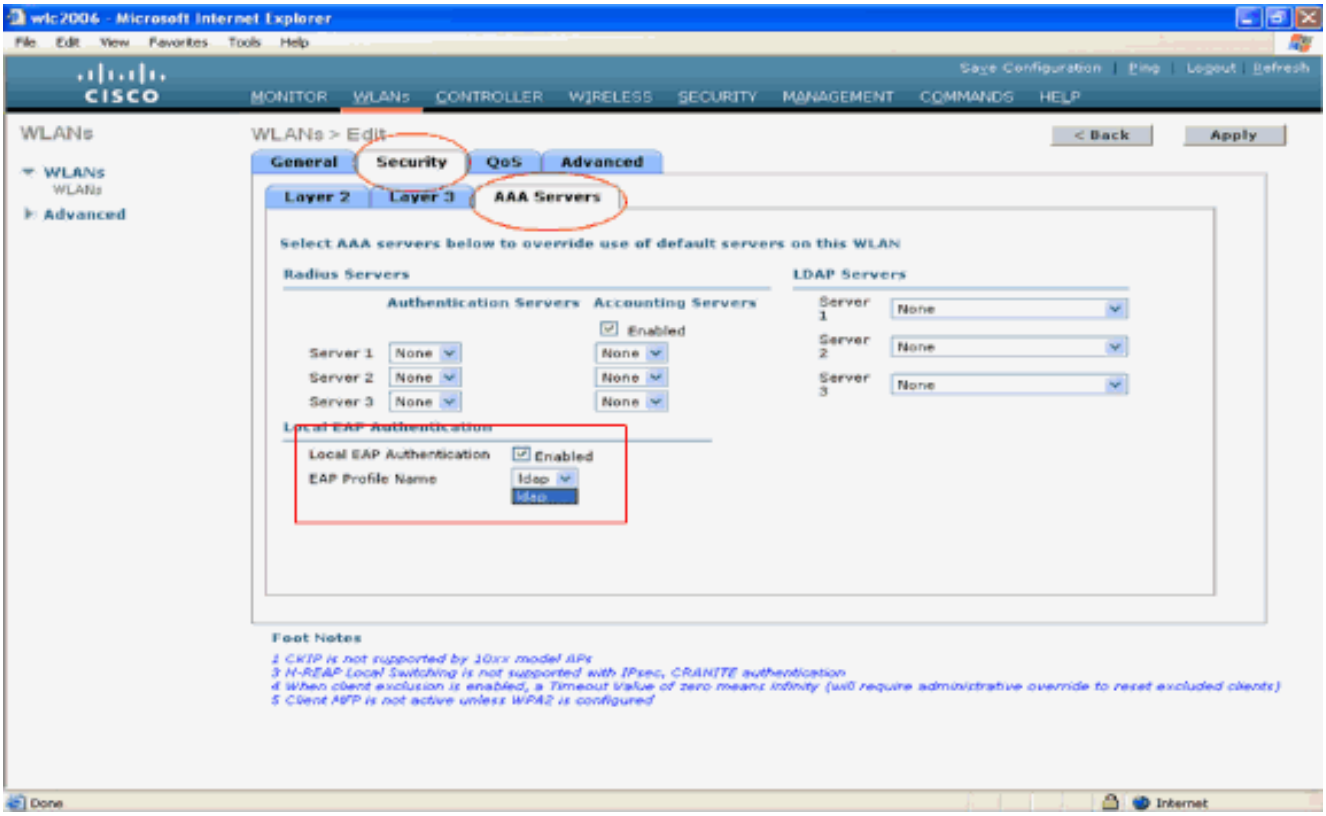
## WLAN's op de WLC configureren met lokale EAP-verificatie

De laatste stap in de WLC is om een WLAN te configureren die Local EAP als verificatiemethode gebruikt met LDAP als back-end database. Voer de volgende stappen uit:

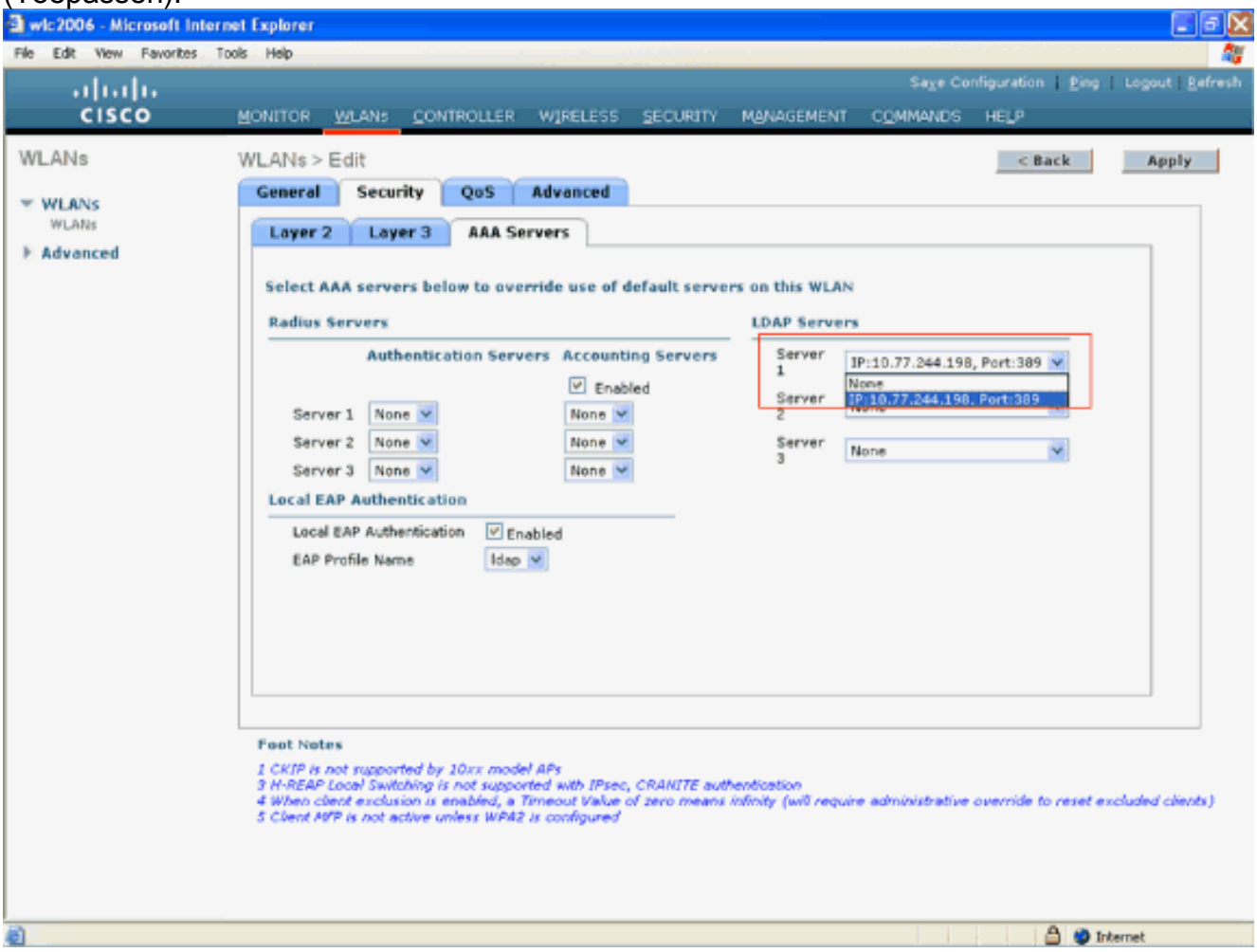
1. Klik in het hoofdmenu van de controller op **WLAN's** om naar de configuratiepagina van WLAN's te gaan. In de pagina WLAN's klikt u op **Nieuw** om een nieuw WLAN te maken. Dit voorbeeld maakt een nieuwe WLAN-**map**.Klik op **Toepassen** De volgende stap is het configureren van de WLAN-parameters in de WLAN's > pagina Bewerken.
2. In de WLAN-bewerkingspagina schakelt u de status van dit WLAN in. Configureer alle andere noodzakelijke
parameters.




3. Klik op **Beveiliging** om de beveiligingsgerelateerde parameters voor dit WLAN te configureren. In dit voorbeeld wordt Layer 2-beveiliging gebruikt als 802.1x met 104-bits dynamisch WEP.**N.B.:** In dit document wordt 802.1x met dynamisch WEP als voorbeeld gebruikt. Het wordt aanbevolen om veiligere verificatiemethoden te gebruiken, zoals WPA/ WPA2.
4. Klik op de configuratiepagina van WLAN security op **het** tabblad **AAA-servers**. Schakel op de pagina AAA-servers de lokale EAP-verificatiemethode in en kies **ladp** in het vervolgkeuzevenster dat overeenkomt met de parameter EAP Profile Name. Dit is het lokale EAP-profiel dat in dit voorbeeld is
gemaakt.

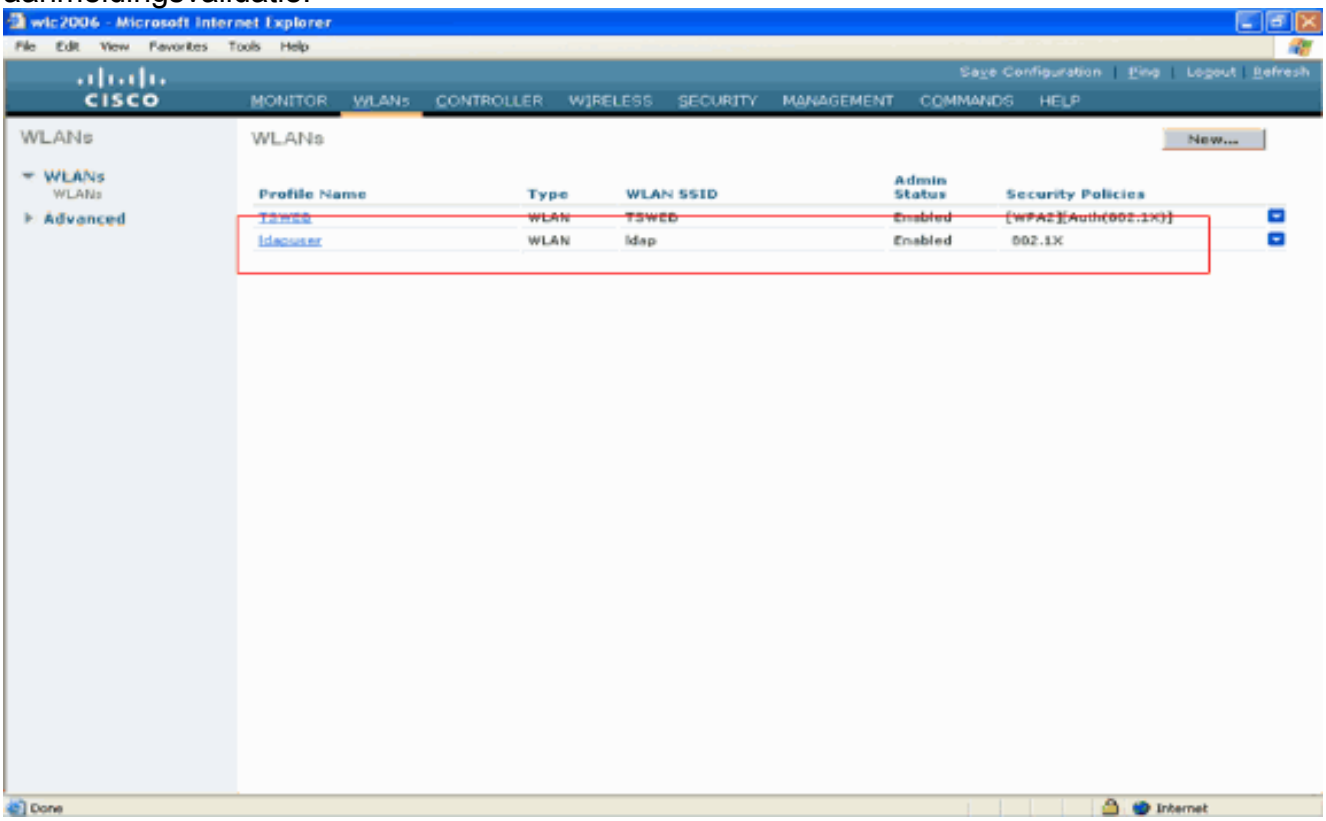



5. Kies de LDAP-server (die eerder op de WLC is geconfigureerd) uit de vervolgkeuzelijst. Zorg ervoor dat de LDAP-server bereikbaar is via de WLC.Klik op **Apply** (Toepassen).




6. Het nieuwe WLAN ldapis op de WLC geconfigureerd. Dit WLAN verifieert clients met lokale EAP-verificatie (in dit geval EAP-FAST) en vraagt een LDAP-back-end database voor client-

aanmeldingsvalidatie.




# LDAP-server configureren

Nu Local EAP is geconfigureerd op de WLC, is de volgende stap om de LDAP-server te configureren die fungeert als een back-end database voor het verifiëren van de draadloze clients na een succesvolle certificaatvalidatie.

De eerste stap in het configureren van de LDAP-server is het maken van een gebruikersdatabase op de LDAP-server, zodat de WLC deze database kan bevragen om de gebruiker te verifiëren.

## Gebruikers maken op de domeincontroller

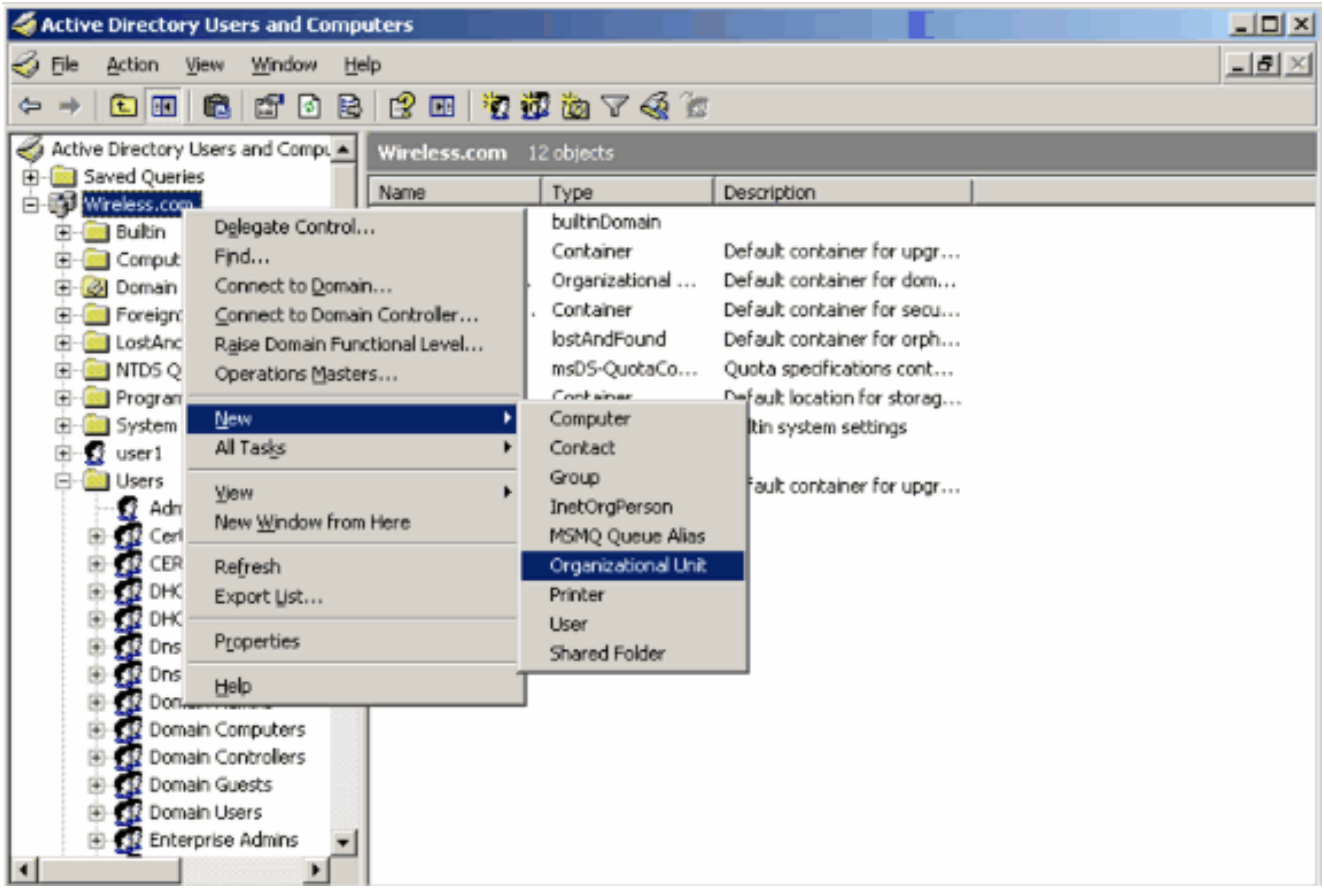
In dit voorbeeld wordt een nieuwe OU **ldapuser** gemaakt en de gebruiker **user2** wordt gemaakt onder deze OU. Door deze gebruiker voor LDAP-toegang te configureren, kan de WLC deze LDAP-database bevragen voor gebruikersverificatie.

Het domein dat in dit voorbeeld wordt gebruikt is **wireless.com**.

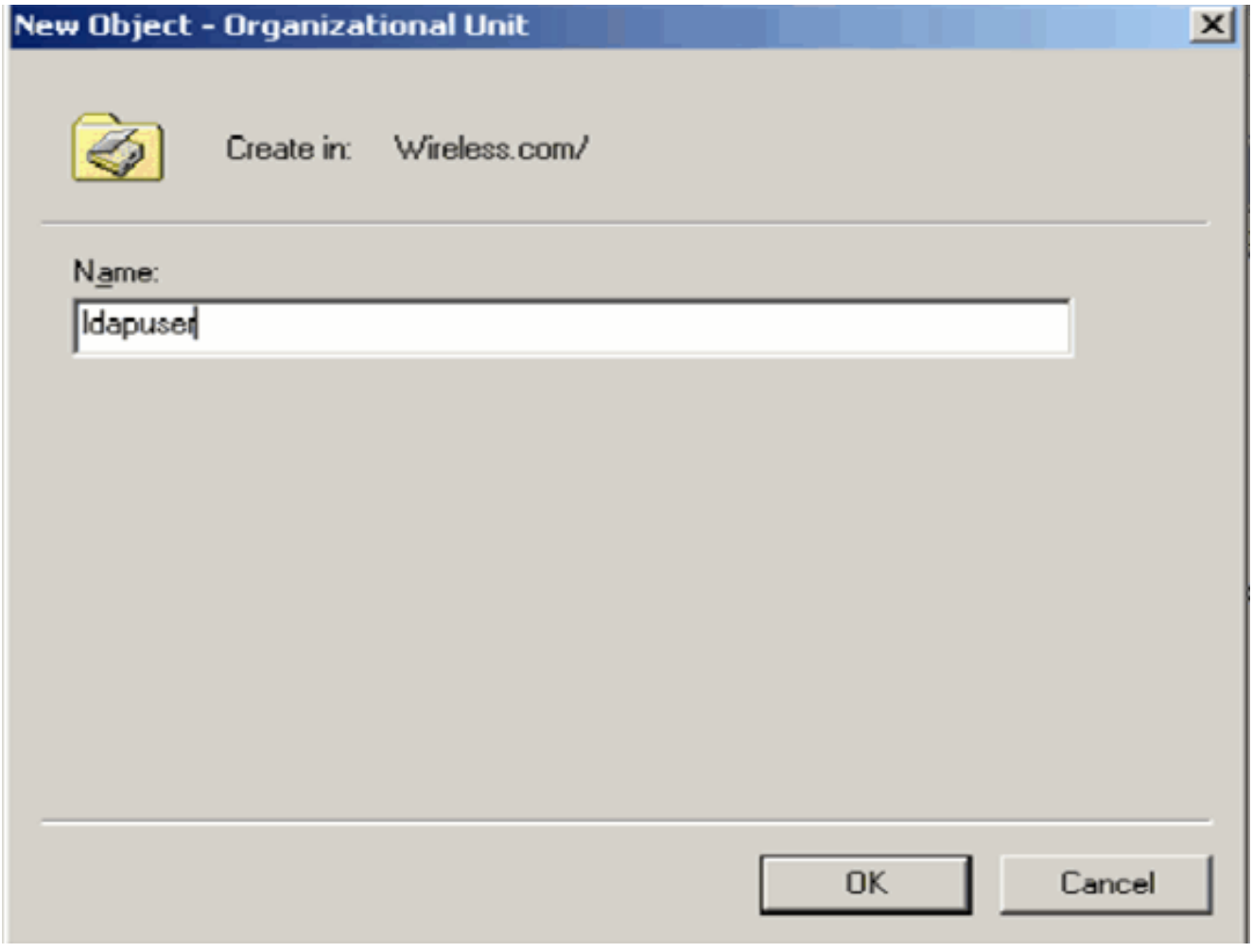
### Een gebruikersdatabase maken onder een OE

In deze paragraaf wordt uitgelegd hoe u een nieuwe OU in uw domein maakt en een nieuwe gebruiker maakt op deze OE.

1. Klik in de domeincontroller op **Start > Programma's > Administratieve tools > Active Directory-gebruikers en -computers** om de **Active Directory**-beheerconsole te starten.
2. Klik met de rechtermuisknop op uw domeinnaam (wireless.com, in dit voorbeeld) en selecteer **Nieuw > Organisatorische eenheid** in het contextmenu om een nieuwe OU te maken.

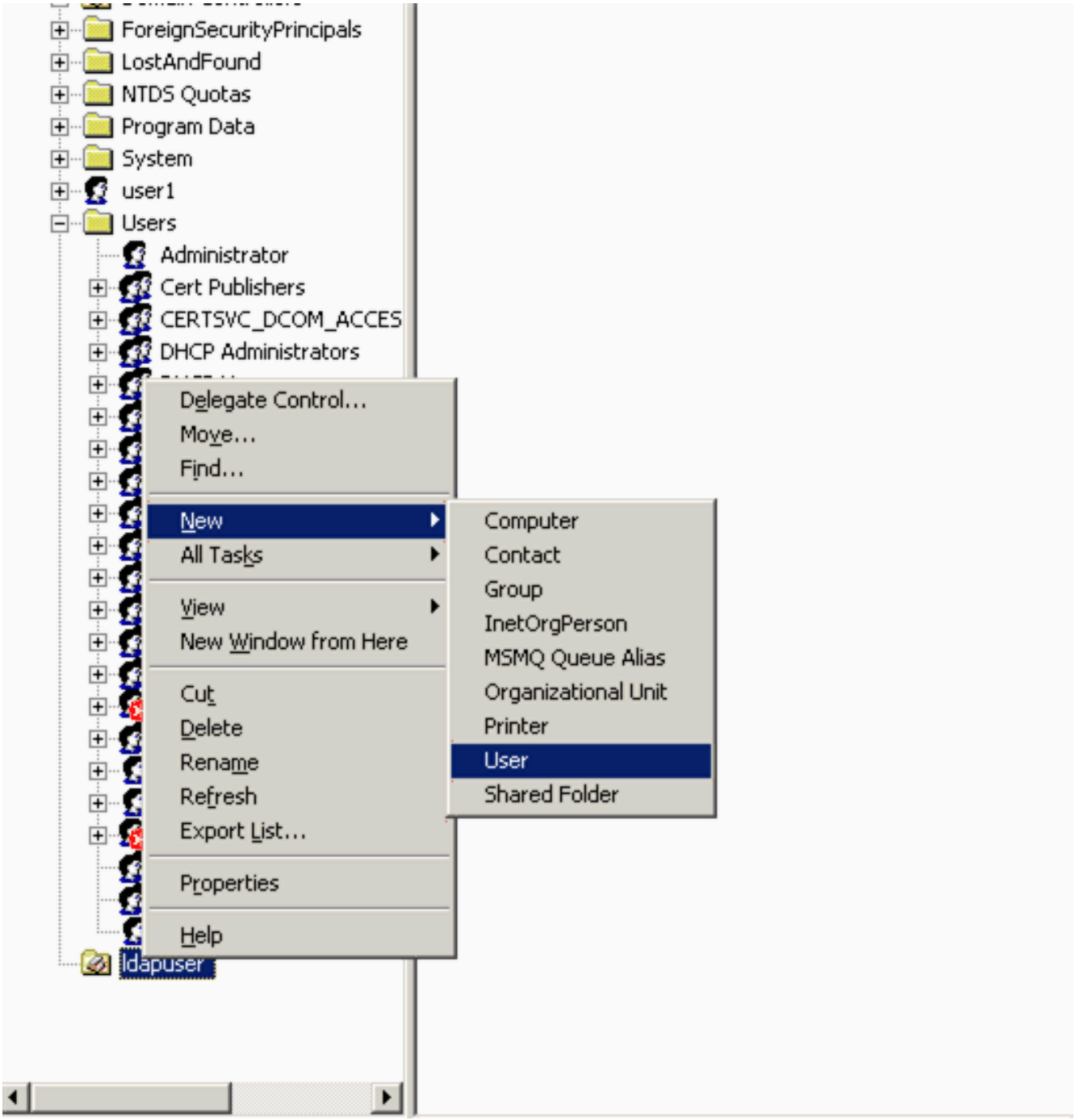



3. Wijs een naam toe aan deze OE en klik op **OK**.

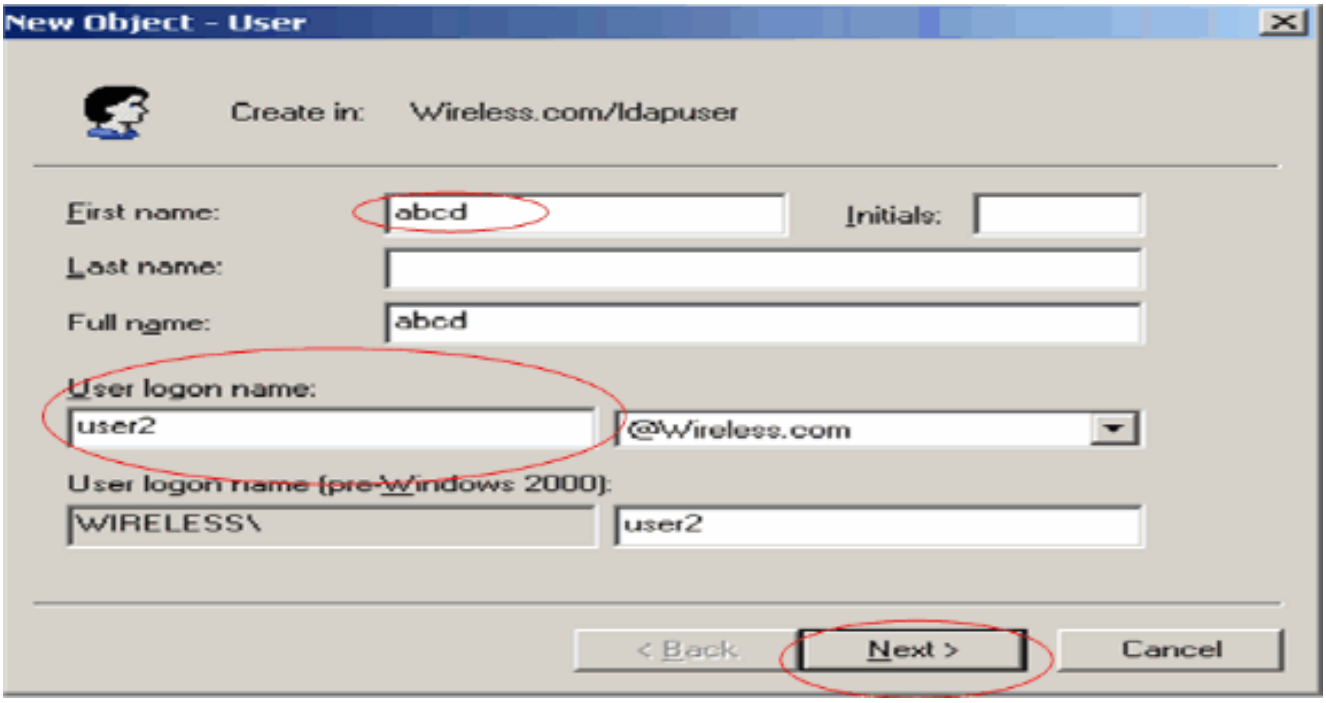



Nu de nieuwe OU **ldapuser** op de LDAP server wordt gemaakt, is de volgende stap om user **user2** onder deze OU te maken. Voltooi de volgende stappen om dit te bereiken:

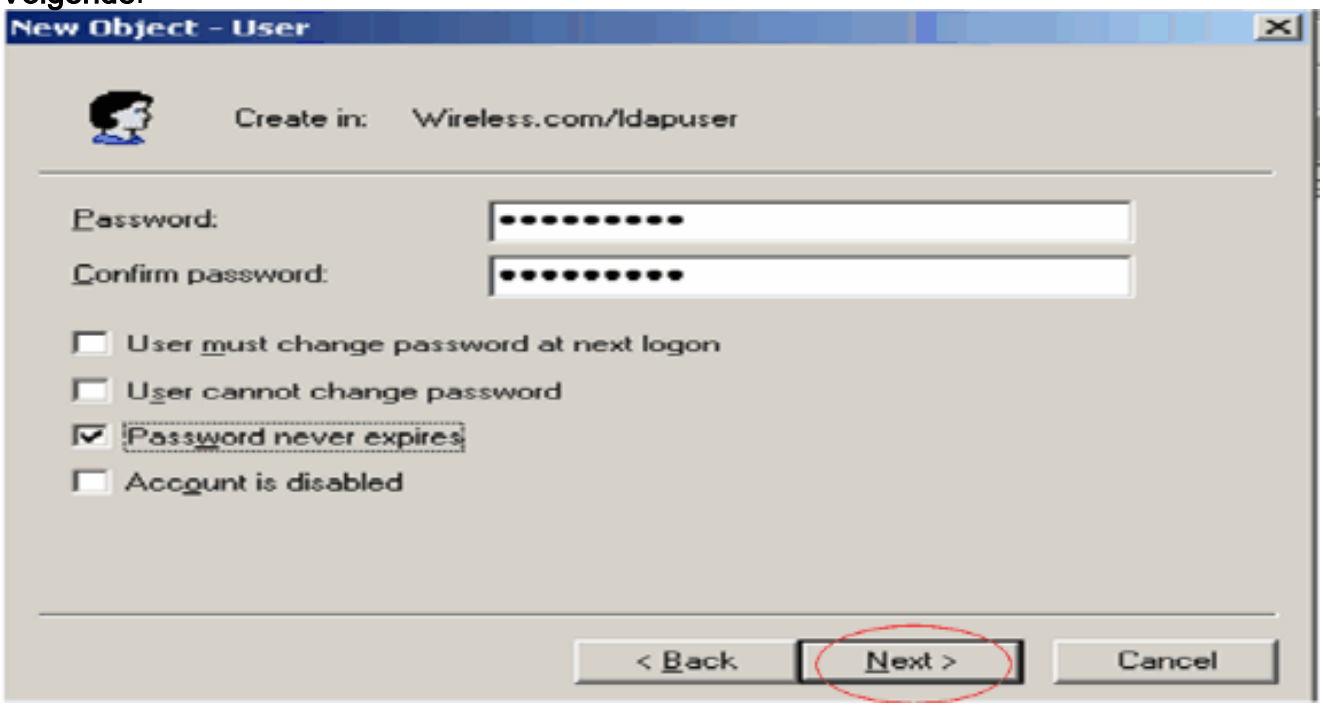
1. Klik met de rechtermuisknop op de nieuwe OE. Selecteer **Nieuw > Gebruiker** in de resulterende contextmenu's om een nieuwe gebruiker te maken.



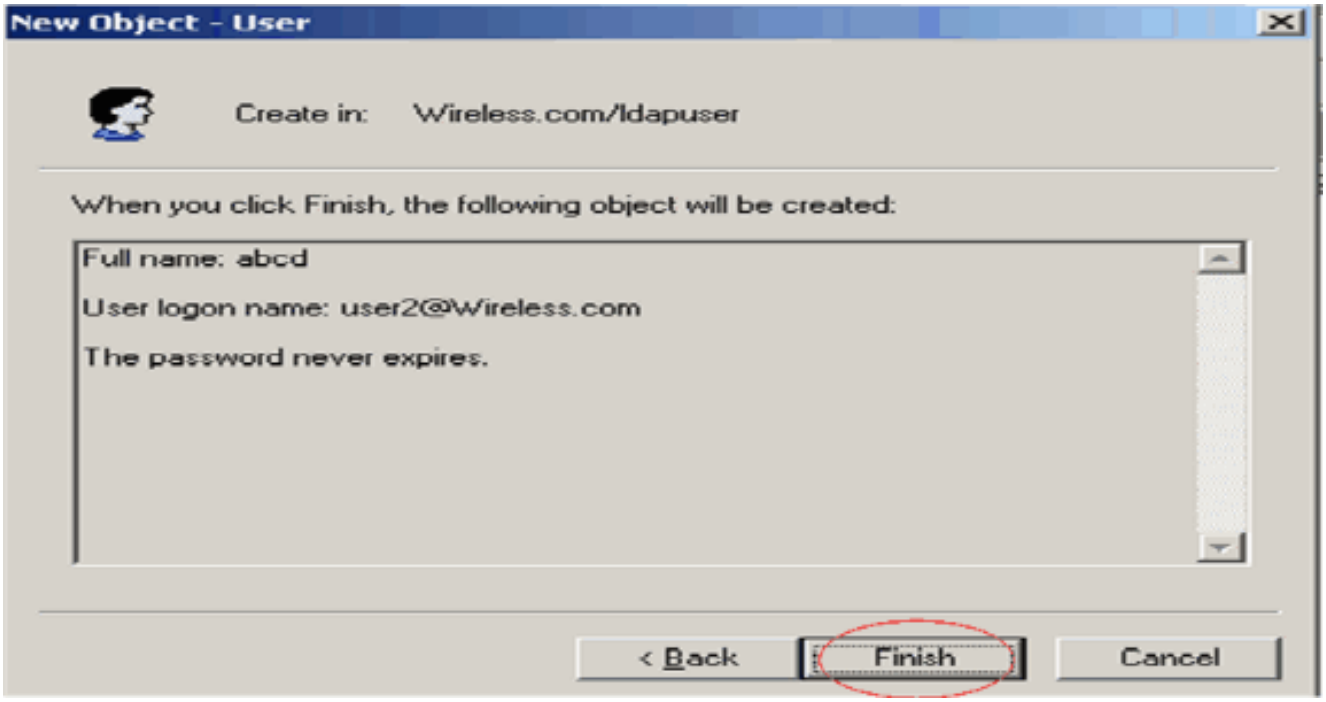

2. Vul op de pagina Instellen gebruiker de gewenste velden in zoals in dit voorbeeld. In dit voorbeeld is **user2** de gebruikersnaam voor aanmelding.Dit is de gebruikersnaam die wordt geverifieerd in de LDAP-database voor het authenticeren van de client. In dit voorbeeld wordt **abcd** gebruikt als de voor- en achternaam. Klik op **Next** (Volgende).




3. Voer een wachtwoord in en bevestig het wachtwoord. Kies de optie **Wachtwoord verloopt nooit** en klik op **Volgende**.




4. Klik op Finish (Voltooien).Een nieuwe gebruiker **user2** wordt aangemaakt onder de OU **ldapuser**. De gebruikersreferenties zijn:gebruikersnaam: **user2**wachtwoord: **Laptop123**




Nu de gebruiker onder een OE wordt gecreëerd, is de volgende stap om deze gebruiker te configureren voor LDAP-toegang.

## De gebruiker voor LDAP-toegang configureren

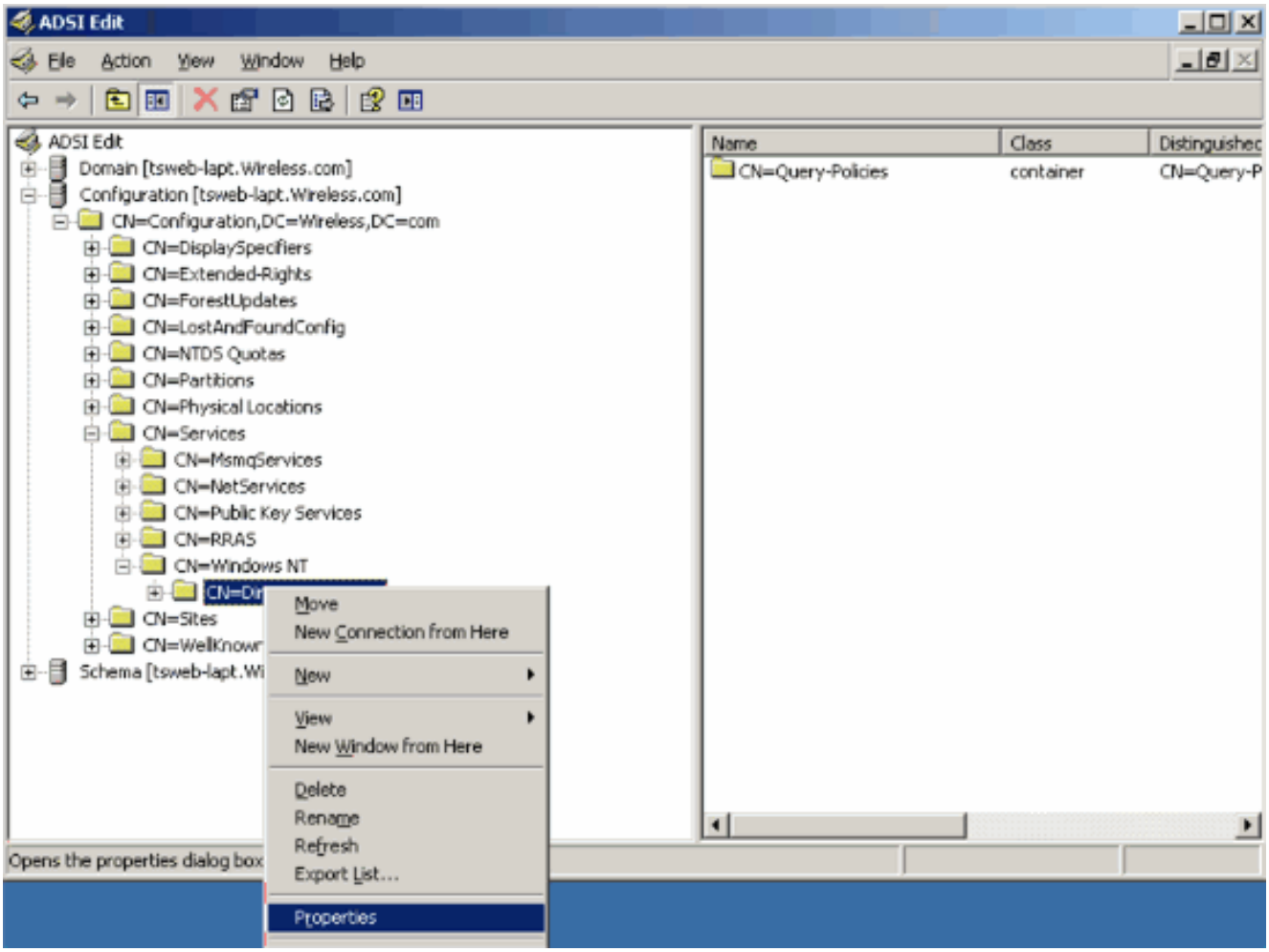
Voer de stappen in deze sectie uit om een gebruiker voor LDAP-toegang te configureren.

### Anonieme bindfunctie inschakelen op de Windows 2003-server

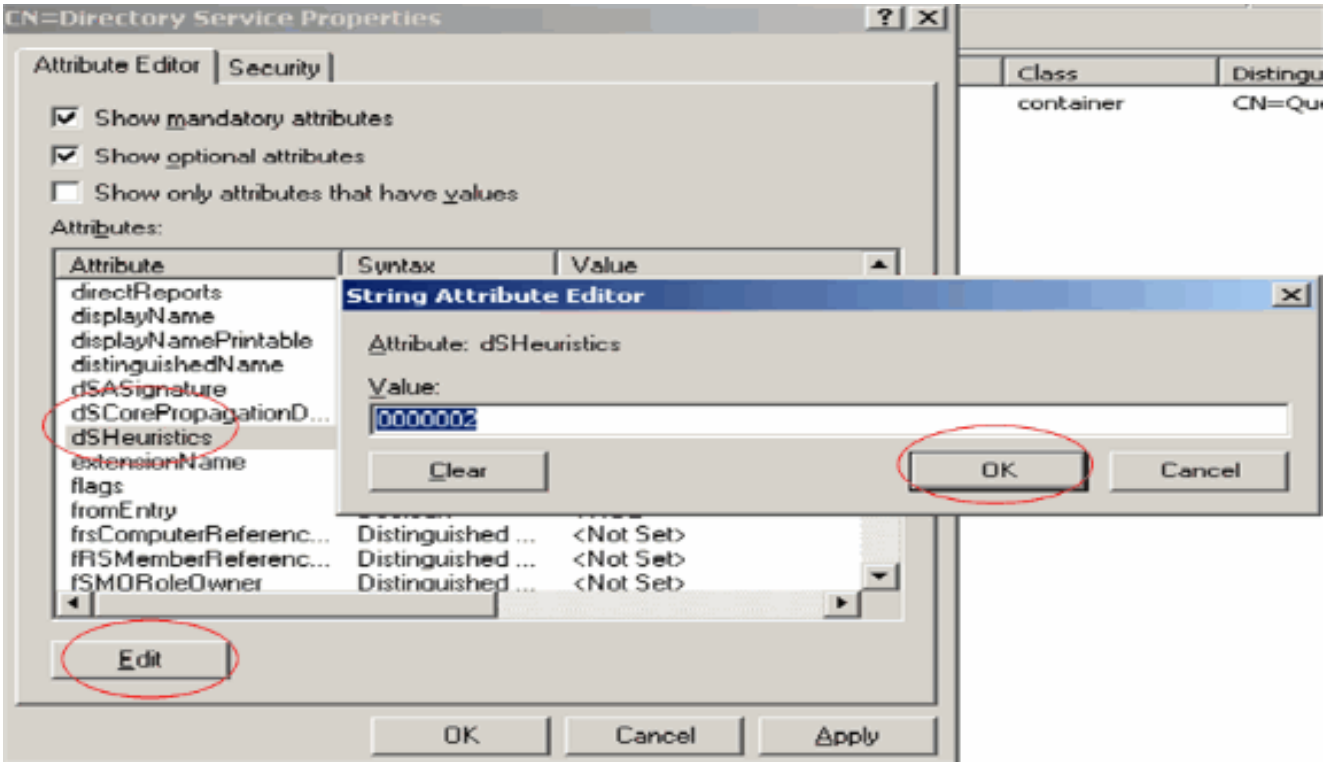
Voor toepassingen van derden om toegang te krijgen tot Windows 2003 AD op de LDAP, moet de functie Anonymous Bind zijn ingeschakeld op Windows 2003. Standaard zijn anonieme LDAP-bewerkingen niet toegestaan op Windows 2003 domeincontrollers.

Voer deze stappen uit om de functie Anonymous Bind in te schakelen:

1. Start het gereedschap **Bewerken ADSI** vanaf de locatie Start > Uitvoeren > Type: **ADSI Edit.msc**. Deze tool maakt deel uit van Windows 2003-ondersteuningstools.
2. Breid in het venster ADSI Edit het hoofddomein uit (Configuration [tsweb-lapt.Wireless.com]).Breid **CN=Services > CN=Windows NT > CN=Directory Service uit**. Klik met de rechtermuisknop op de container **CN=Directory Service** en selecteer **eigenschappen** in het
contextmenu.




3. Klik in het venster **CN=Directory Service Properties** op het kenmerk **dsHeuristics** onder het veld Attribute en kies **Bewerken**. Voer in het venster **String Attribute Editor** van deze eigenschap de waarde **000002 in** en klik op **Toepassen** en **OK**. De functie Anonymous Bind is ingeschakeld op Windows 2003-server.**Opmerking:** het laatste (zevende) teken is het teken dat bepaalt hoe u zich kunt binden aan LDAP-dienst. "0" of geen zevende teken betekent dat anonieme LDAP-bewerkingen zijn uitgeschakeld. **Door het zevende teken op "2" in te stellen, wordt de functie Anonymous Bind ingeschakeld.**

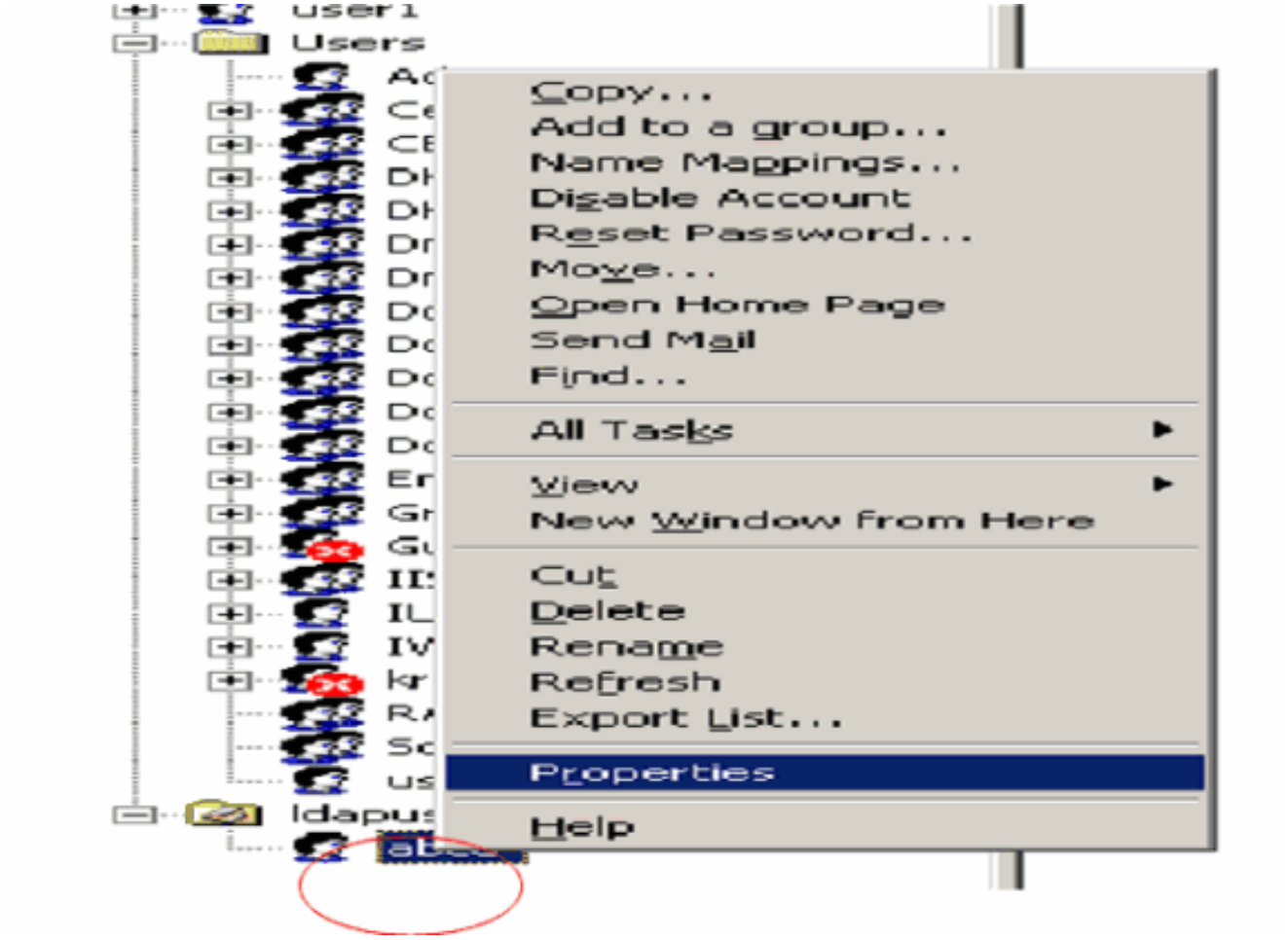



**N.B.:** Als deze eigenschap al een waarde bevat, controleert u of u alleen het zevende teken aan de linkerkant wijzigt. Dit is het enige teken dat gewijzigd moet worden om anonieme bindingen mogelijk te maken. Als de huidige waarde bijvoorbeeld "0010000" is, moet u deze wijzigen in "0010002". Als de huidige waarde minder dan zeven tekens bedraagt, moet u nullen op de niet gebruikte plaatsen zetten: "001" wordt "0010002".

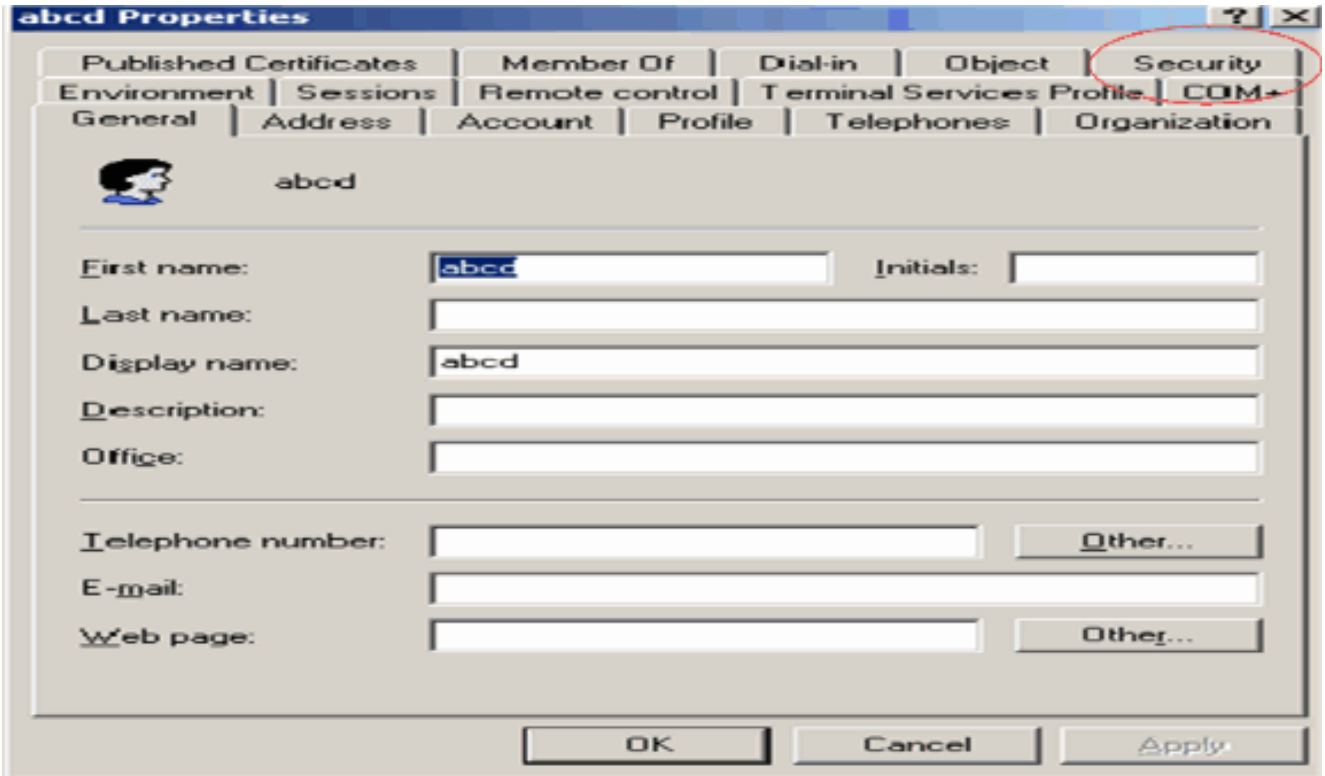
## ANONIEME AANMELDTOEGANG verlenen aan de gebruiker "user2"

De volgende stap is om **ANONYMOUS LOGON** toegang tot de gebruiker **user2** te verlenen. Voltooi de volgende stappen om dit te bereiken:

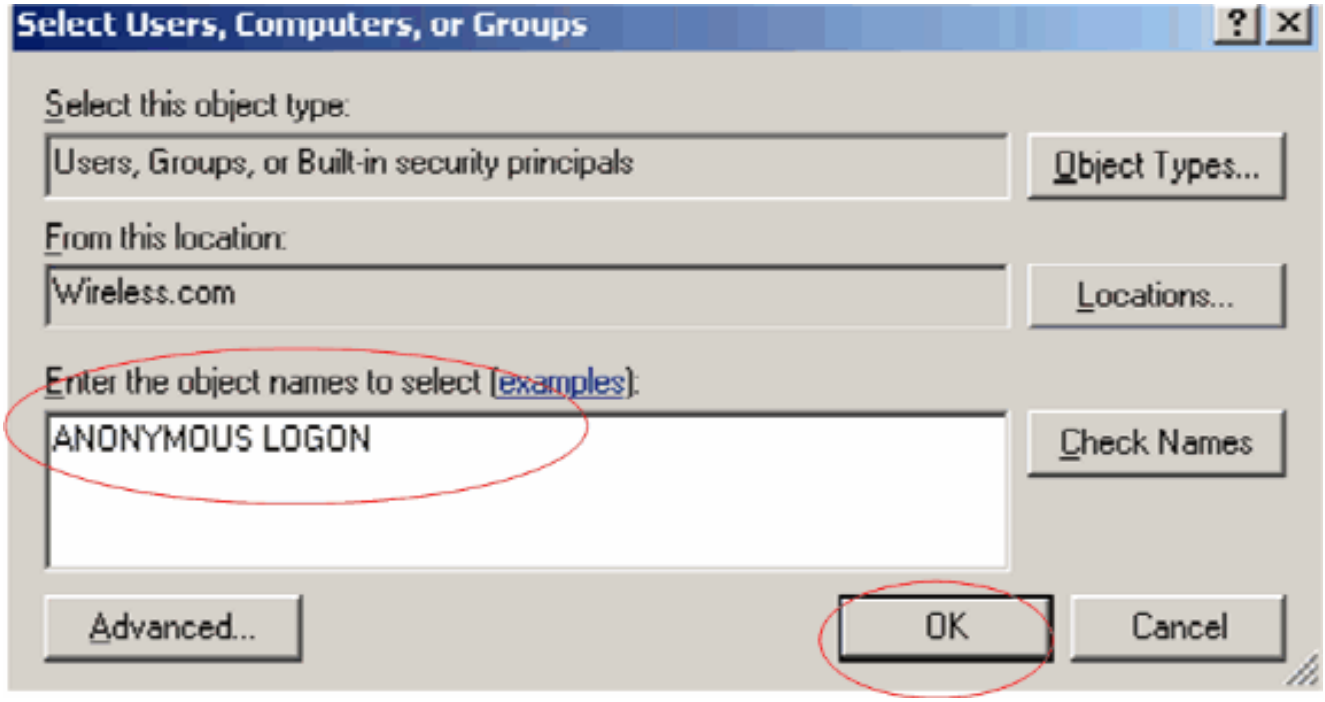
1. Open **Active Directory-gebruikers** en -**computers**.
2. Controleer of **Geavanceerde functies bekijken** is ingeschakeld.
3. Navigeer naar de gebruiker **user2** en klik er met de rechtermuisknop op. Selecteer **Eigenschappen** in het contextmenu. Deze gebruiker wordt geïdentificeerd met de voornaam "abcd".



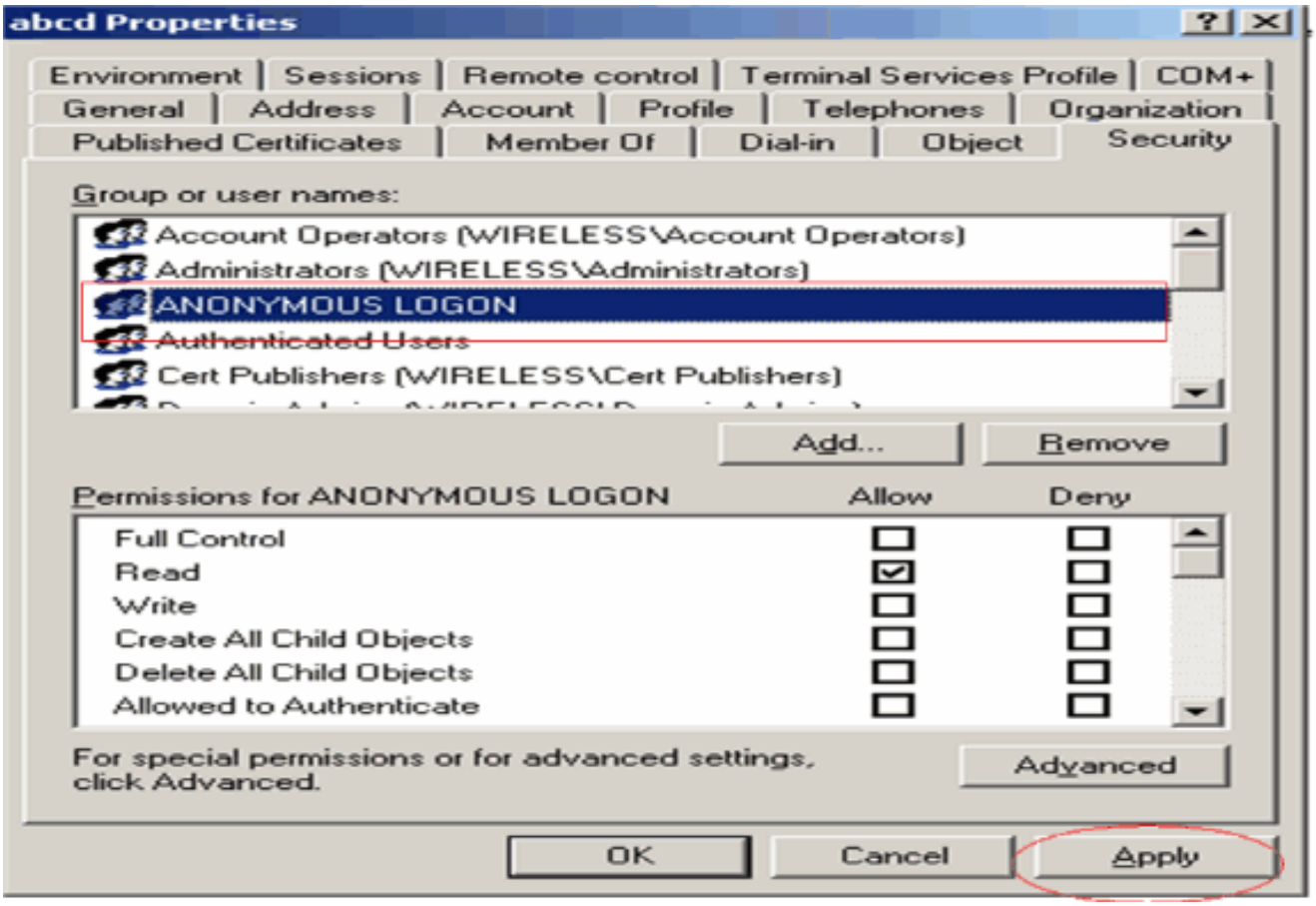

4. Ga naar **Beveiliging** in het venster Eigenschappen van ABCD.




5. Klik op **Add** in het resulterende venster.
6. Typ **ANONIEME AANMELDING** onder het kopje **Voer de objectnamen in om het** vakje **te selecteren** en bevestig het dialoogvenster.



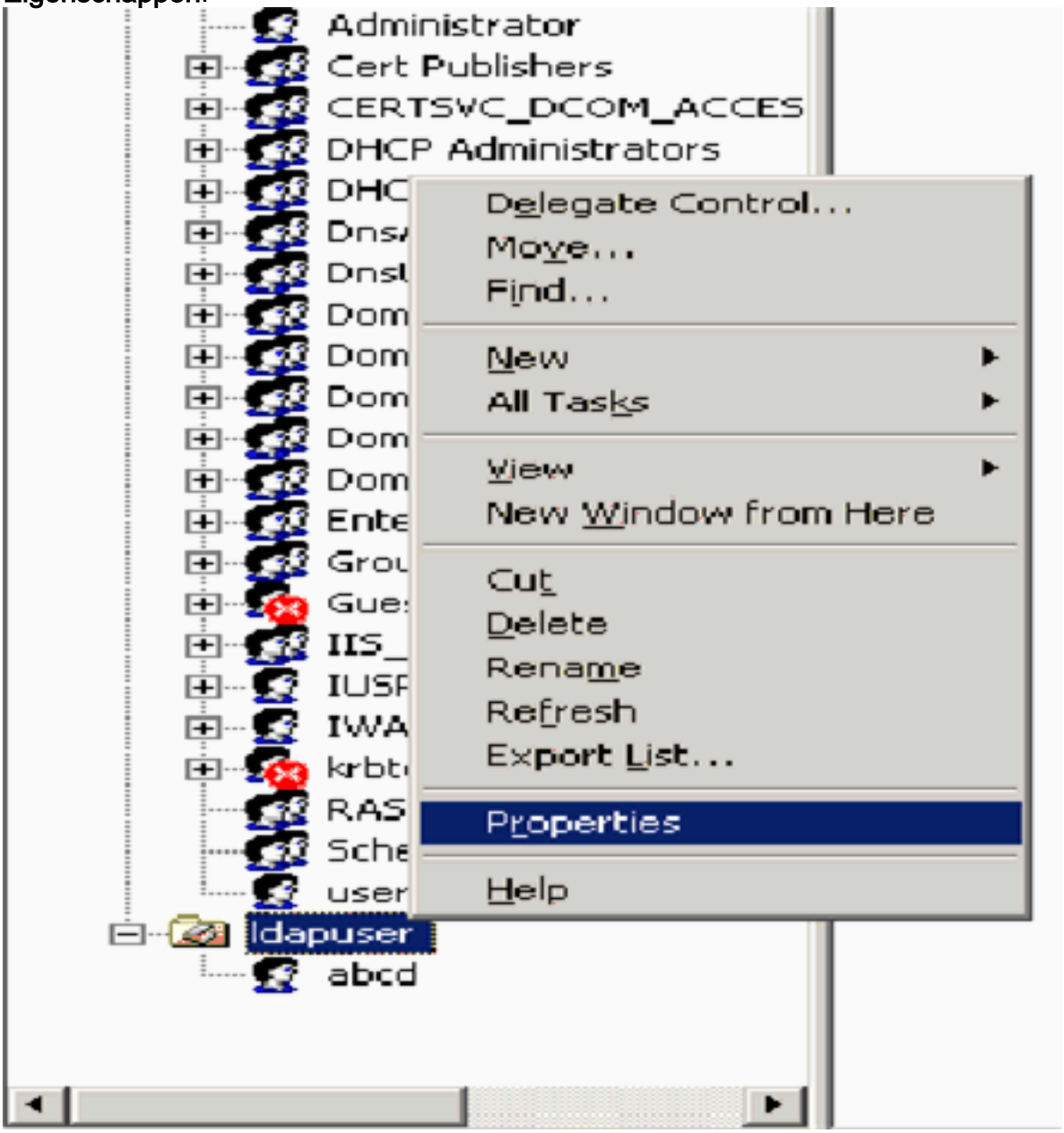

7. In de ACL, zult u opmerken dat **ANONYMOUS LOGON** toegang tot sommige bezitsreeksen van de gebruiker heeft. Klik op **OK**. De ANONYMOUS LOGON-toegang wordt aan deze gebruiker
verleend.



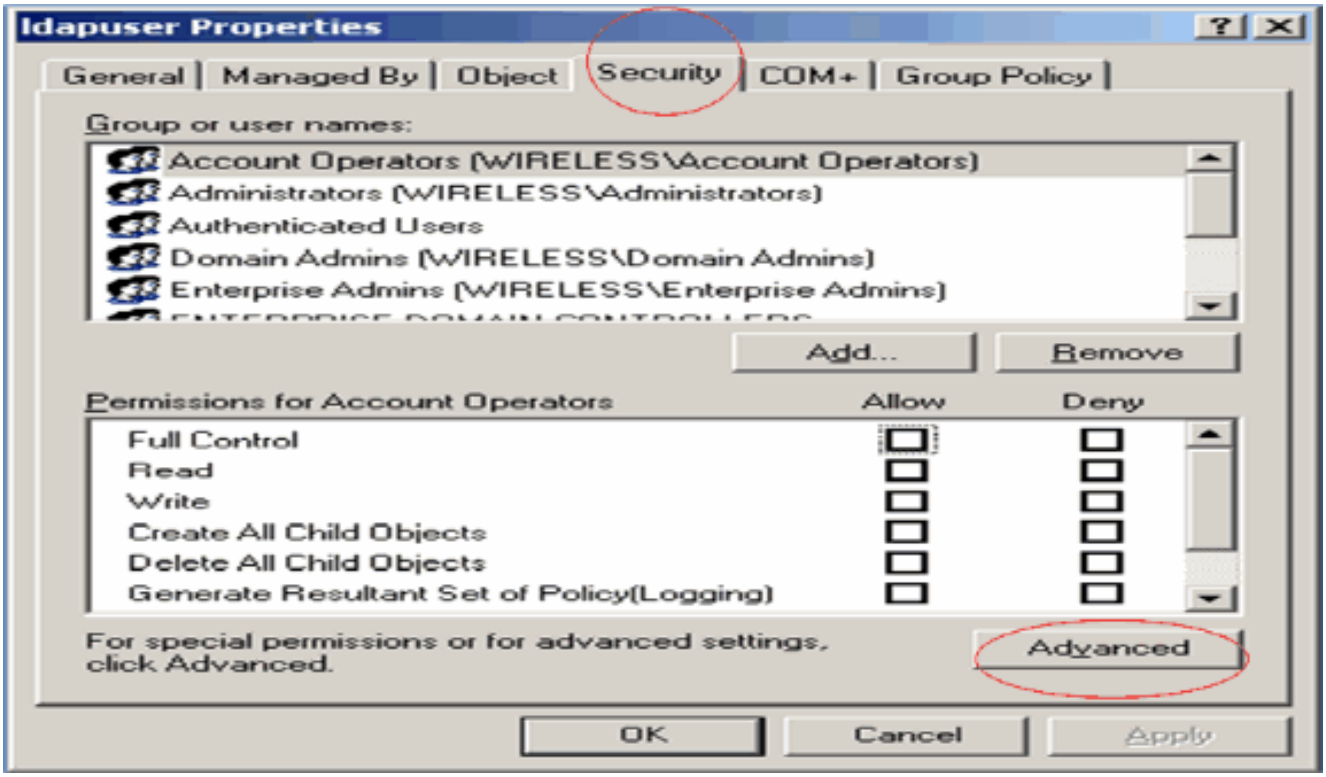

## Toestemming voor lijst met inhoud verlenen aan de OE

De volgende stap is om ten minste toestemming voor **Lijstinhoud** te verlenen aan de **ANONIEME LOGON** op de OE dat de gebruiker zich bevindt. In dit voorbeeld staat "user2" op de OU "ldapuser". Voltooi de volgende stappen om dit te bereiken:

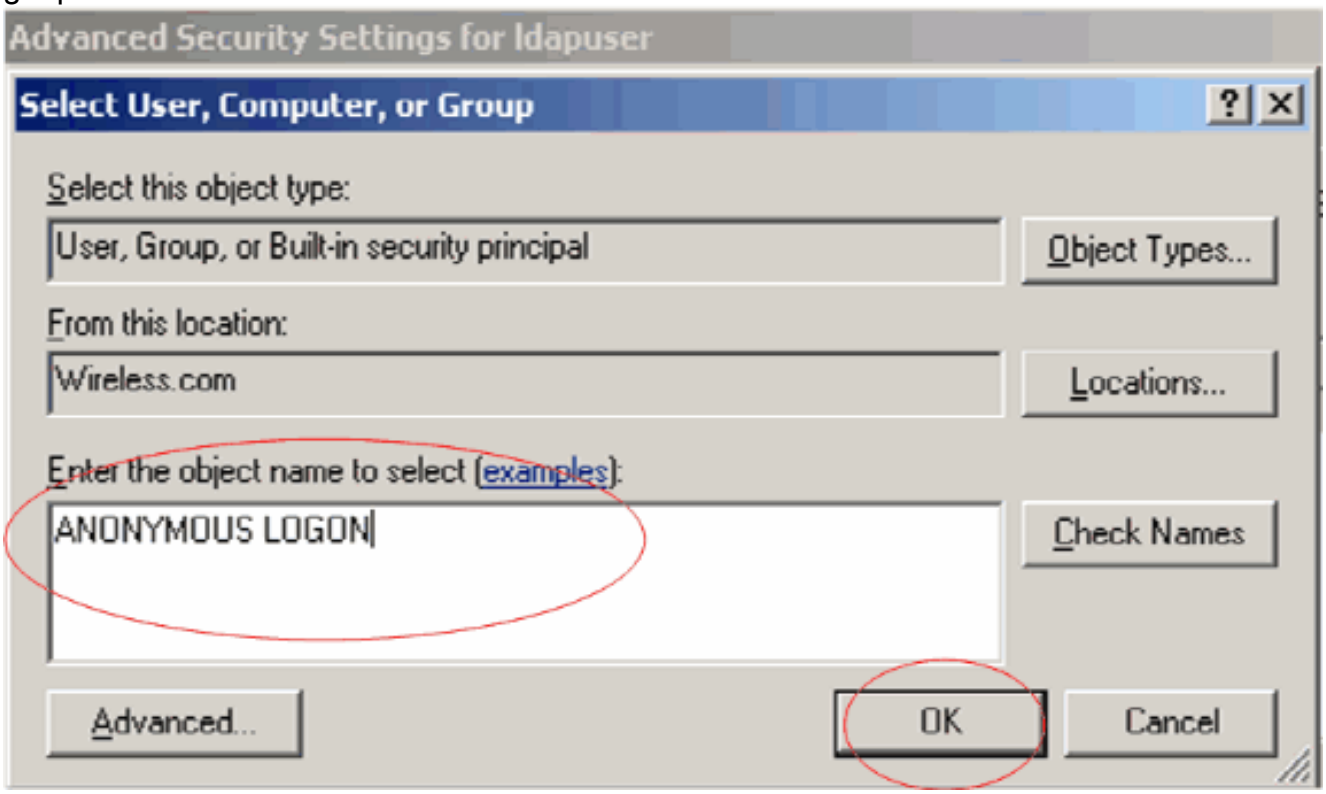
1. In Active Directory Gebruikers en Computers, klik met de rechtermuisknop op de OU **ldapuser** en kies **Eigenschappen**.



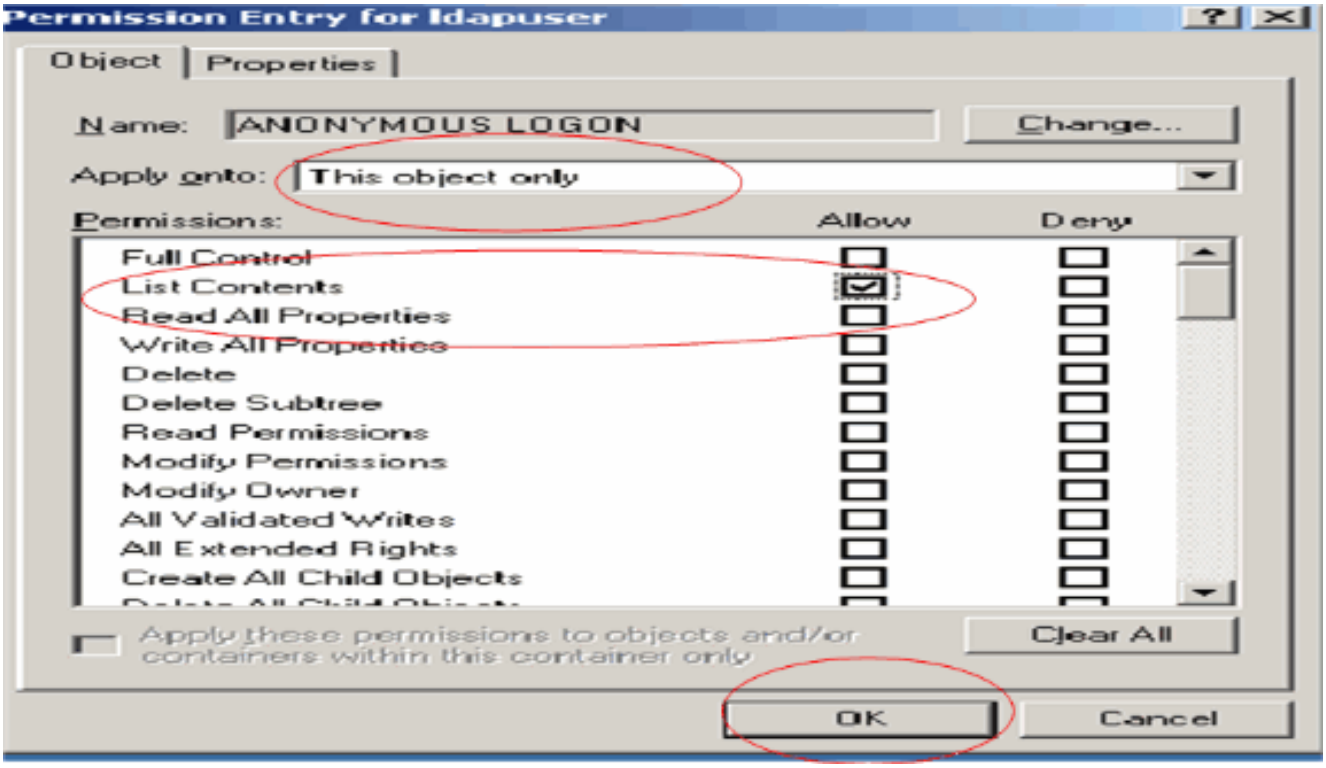

2. Klik op **Beveiliging** en vervolgens op **Geavanceerd**.




3. Klik op **Add** (Toevoegen). Typ **ANONIEME AANMELDING** in het dialoogvenster dat nu wordt geopend.




4. Bevestig de dialoog. Hierdoor wordt een nieuw dialoogvenster geopend.
5. Selecteer in het vervolgkeuzevenster **Toepassen op dit object alleen** en schakel het selectievakje **Inhoud lijst** toestaan
   in.

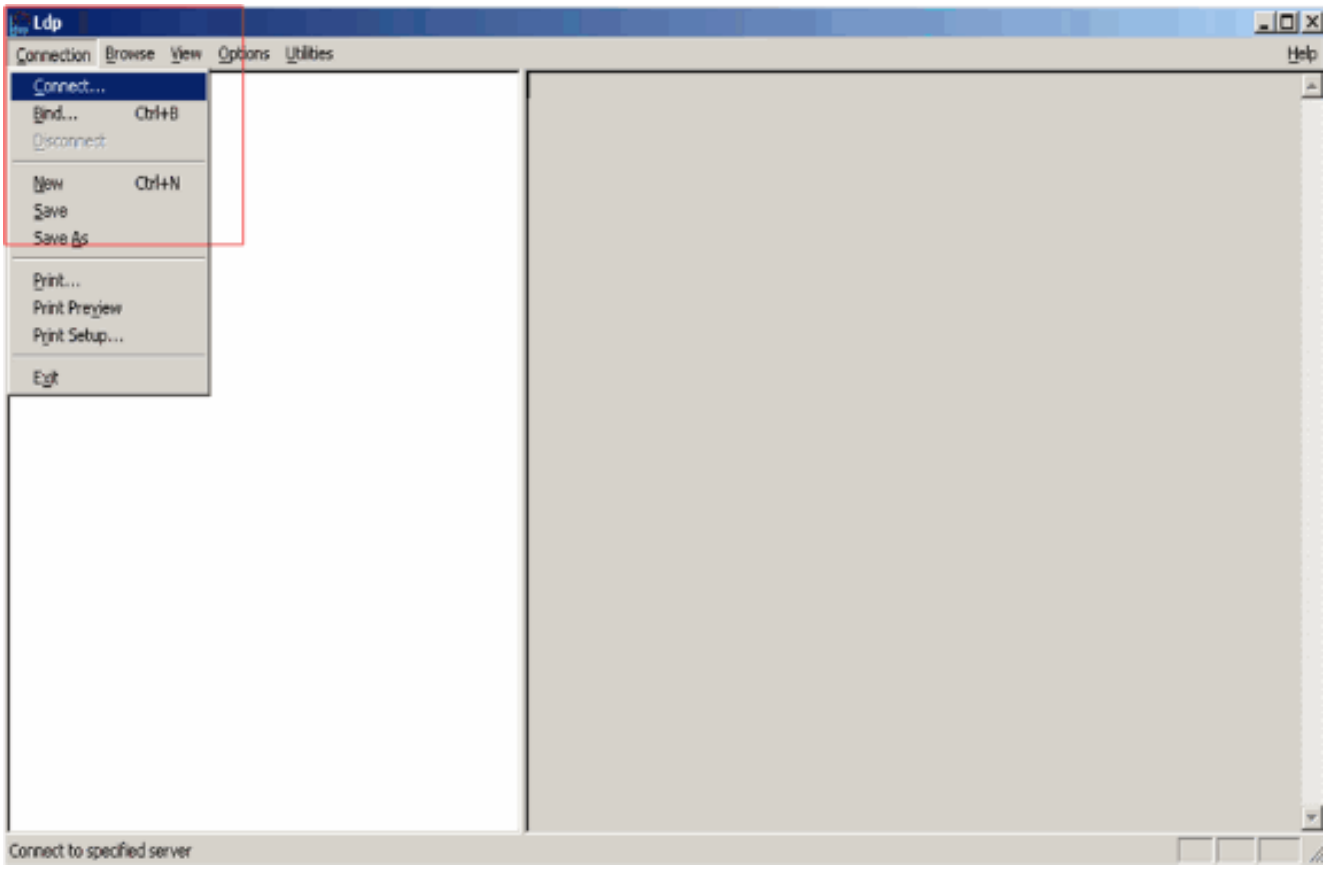



## LDP gebruiken om de gebruikerskenmerken te identificeren

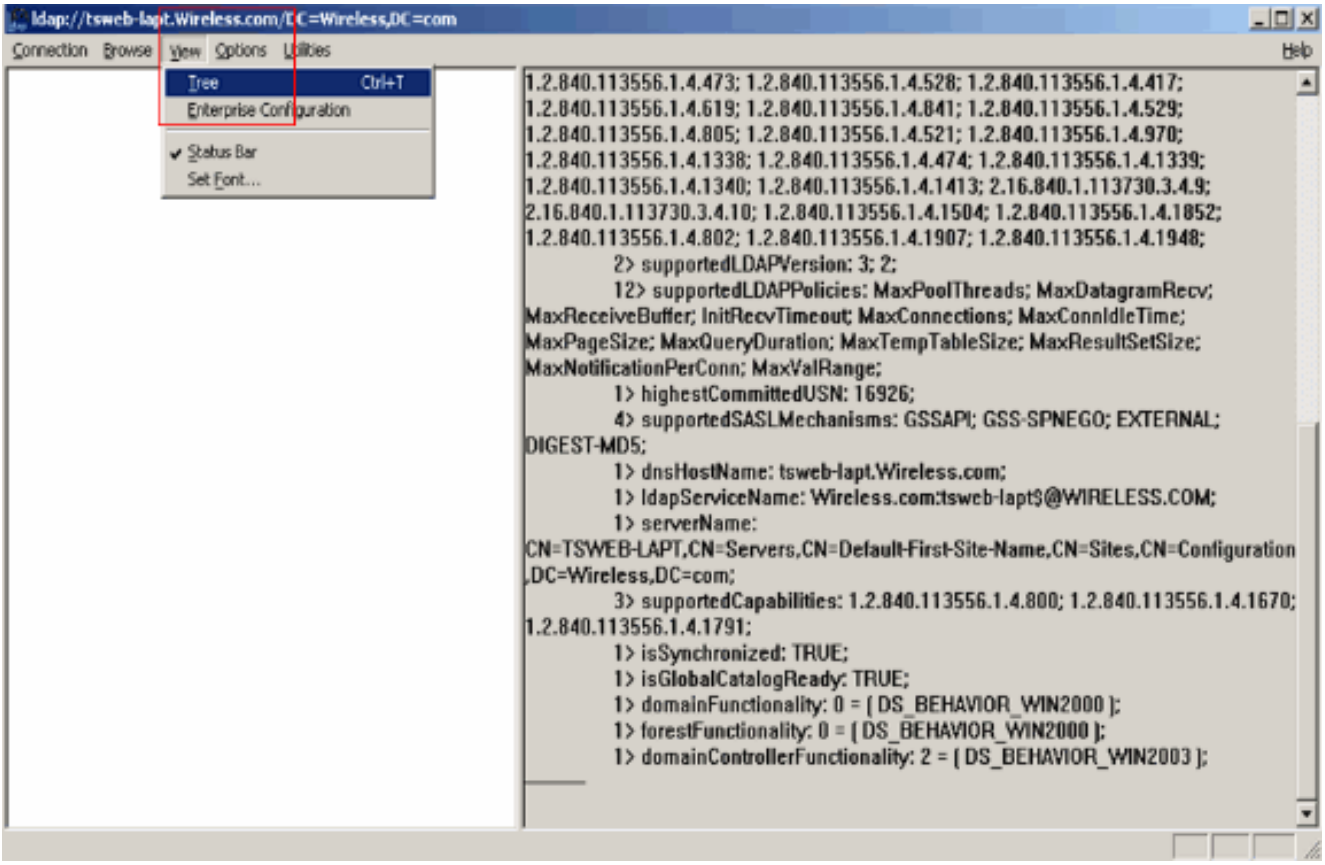
Dit GUI-gereedschap is een LDAP-client waarmee gebruikers bewerkingen kunnen uitvoeren (zoals verbinden, binden, zoeken, wijzigen, toevoegen, verwijderen) tegen elke LDAP-compatibele map, zoals Active Directory. LDP wordt gebruikt om objecten te bekijken die zijn opgeslagen in Active Directory, samen met hun metagegevens, zoals security descriptoren en replicatie metagegevens.

De LDP GUI-tool is inbegrepen wanneer u Windows Server 2003 Support Tools van de product-CD installeert. In deze paragraaf wordt uitgelegd hoe u met het LDP-hulpprogramma de specifieke kenmerken van de gebruiker **user2 kunt** identificeren. Sommige van deze eigenschappen worden gebruikt om de LDAP-serverconfiguratieparameters in de WLC in te vullen, zoals het type Gebruikerskenmerk en het type Gebruikersobject.

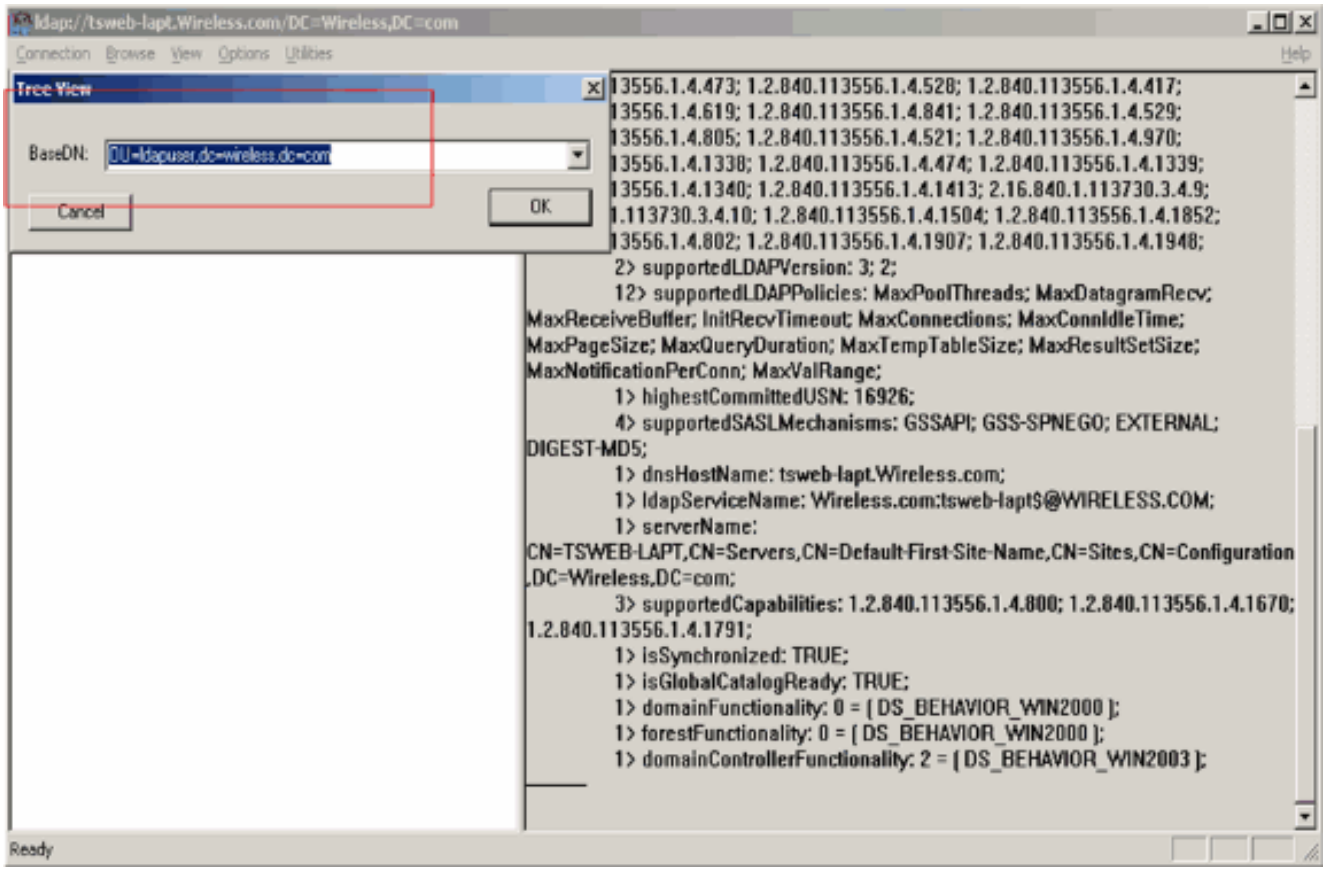
1. Klik op de Windows 2003-server (zelfs op dezelfde LDAP-server) op **Start > Uitvoeren** en voer **LDP** in om toegang te krijgen tot de LDP-browser.
2. Klik in het hoofdvenster van de LDP op **Verbinding > Verbinden** en verbinding maken met de LDAP-server door het IP-adres van de LDAP-server in te voeren.



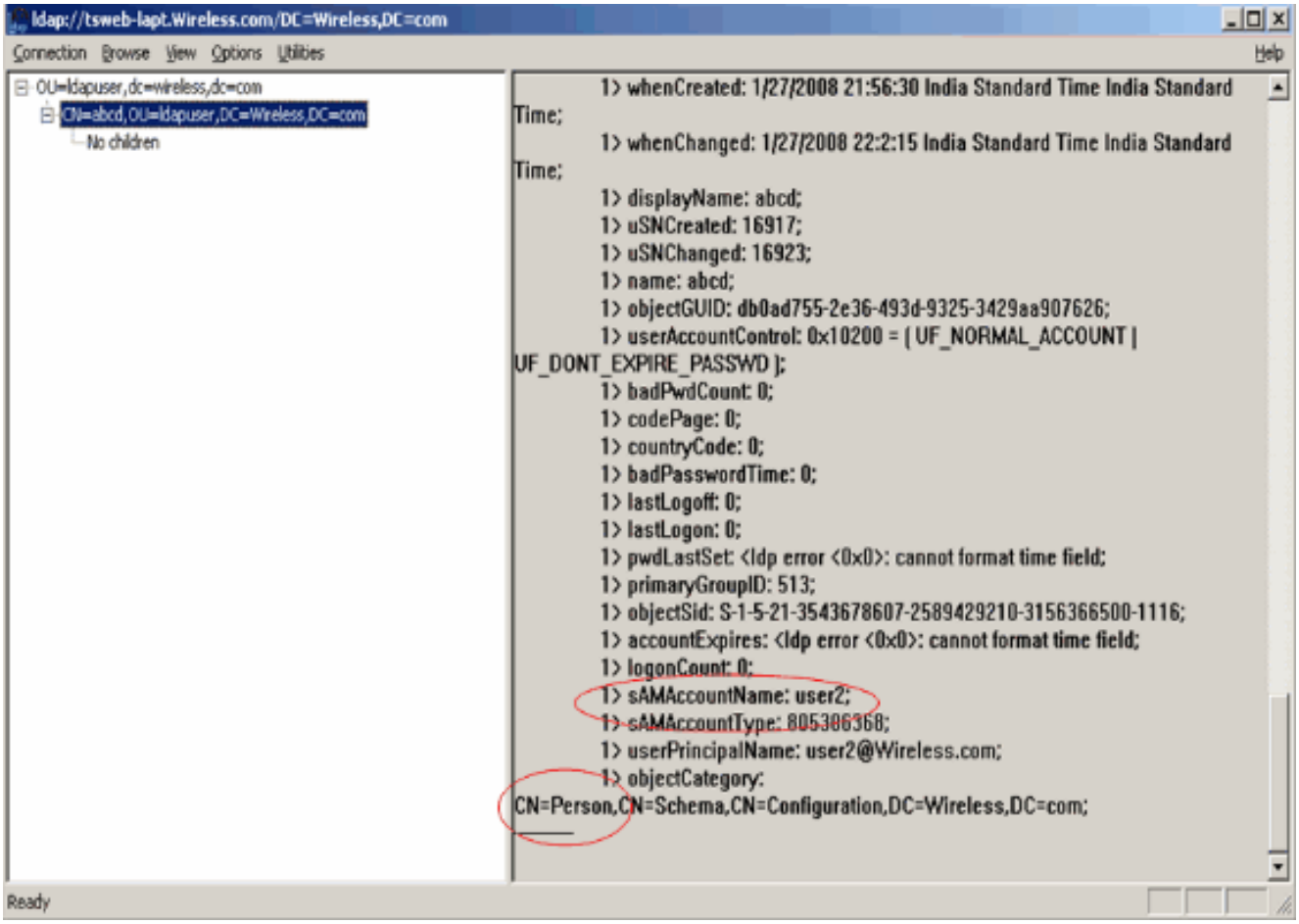

3. Na verbinding met de LDAP-server selecteert u **Weergave** in het hoofdmenu en klikt u op **Boom**.




4. Voer in het venster met de resulterende boomweergave het BaseDN van de gebruiker in. In dit voorbeeld **bevindt user2 zich onder de OU "ldapuser" onder het domein Wireless.com**. Daarom is de BaseDN voor gebruiker **user2 OU=ldapuser, dc=wireless, dc=com**. Klik op **OK**.




5. De linkerkant van de LDP browser toont de gehele boom die onder de gespecificeerde BaseDN verschijnt (**OU=ldapuser, dc=wireless, dc=com**). Breid de structuur uit om de gebruiker **user2** te vinden. Deze gebruiker kan worden geïdentificeerd met de GN-waarde die de voornaam van de gebruiker vertegenwoordigt. In dit voorbeeld is het **CN=abcd**. Dubbelklik op **CN=abcd**. In het rechterdeelvenster van de LDP-browser **worden alle kenmerken van gebruiker2 weergegeven**. Dit voorbeeld verklaart deze stap:



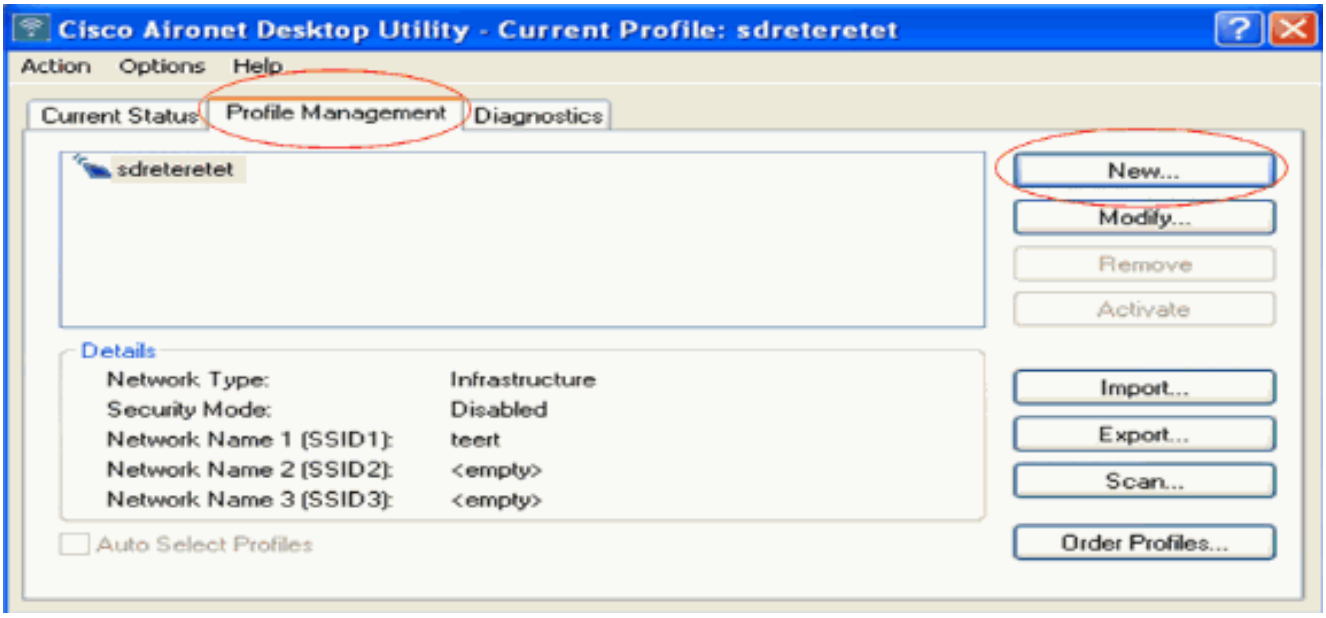

Neem in dit voorbeeld de omcirkelde velden rechts in acht.

6. Zoals vermeld in de sectie Configure WLC with Details of LDAP Server van dit document, voert u in het veld **User Attribute** de naam van het attribuut in in de gebruikersrecord die de gebruikersnaam bevat.Van deze LDP-uitvoer kunt u zien dat **sAMAaccountName** één kenmerk is dat de gebruikersnaam "user2" bevat. Voer daarom de eigenschap **sAMAaccountName in** die overeenkomt met het veld **Gebruikerskenmerken** in de WLC.
7. Voer in het veld **User Object Type** de waarde in van het kenmerk LDAP objectType dat de record als gebruiker identificeert. Vaak hebben gebruikersrecords verschillende waarden voor het objectType-kenmerk, waarvan sommige uniek zijn voor de gebruiker en sommige met andere objecttypes worden gedeeld.In de LDP-uitvoer is **CN=Person** één waarde die de record als gebruiker identificeert. Daarom specificeer **Persoon** als het attribuut **User Object Type** op WLC.

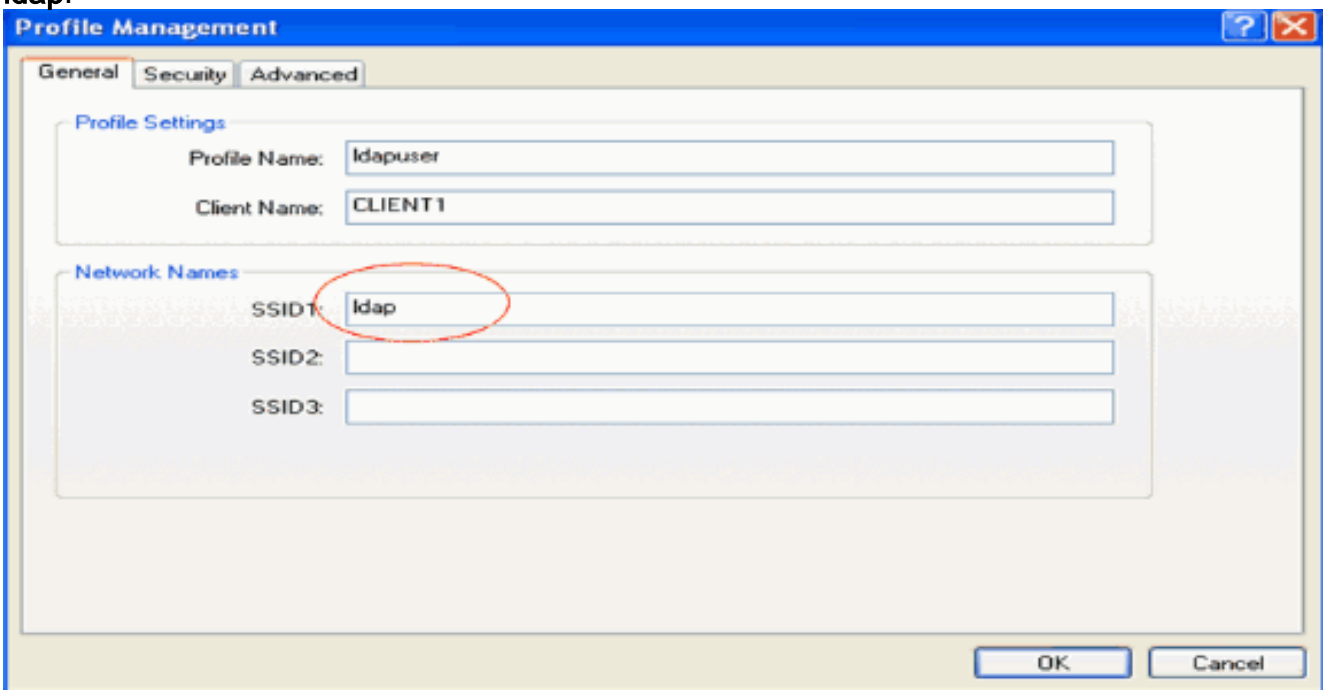
## Draadloze client configureren

De laatste stap is om de draadloze client te configureren voor EAP-FAST-verificatie met client- en servercertificaten. Voltooi de volgende stappen om dit te bereiken:

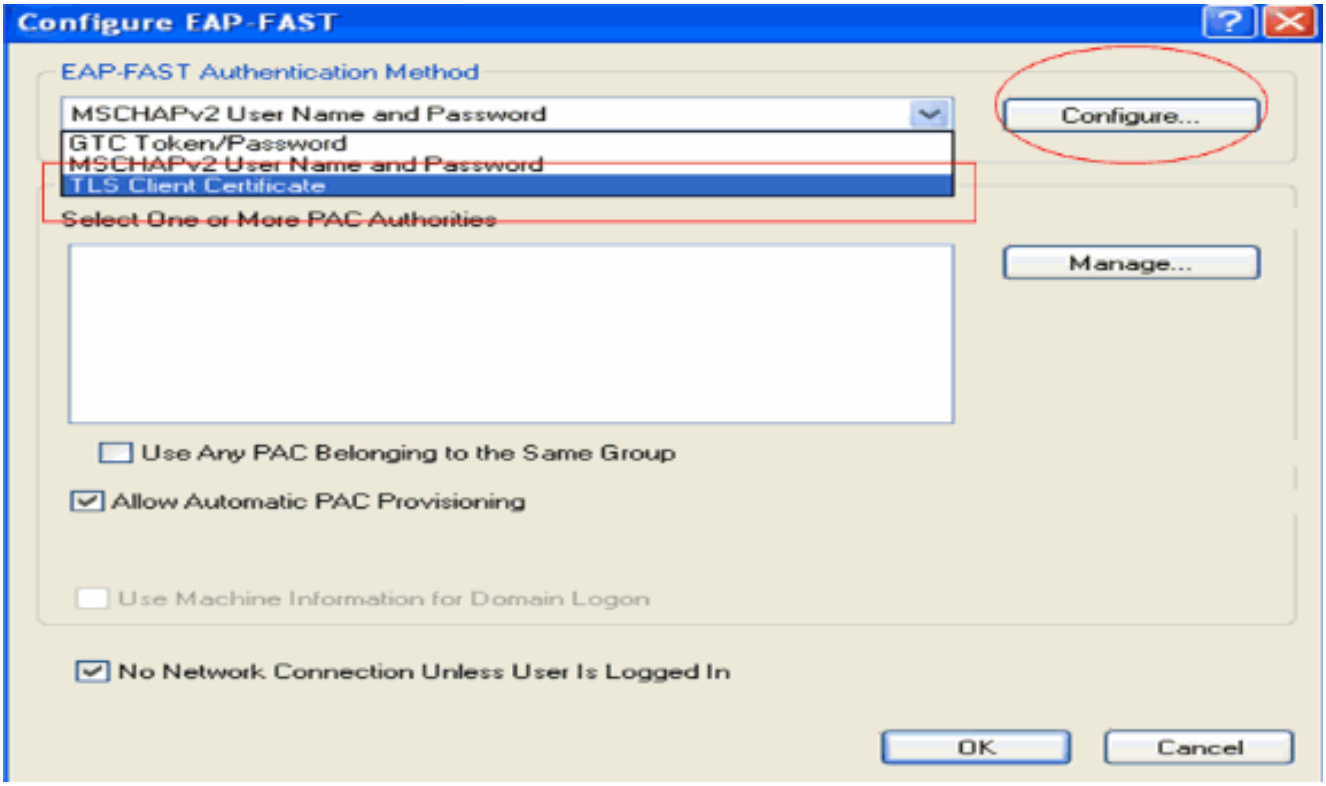
1. Start het **Cisco Aironet Desktop Utility** (ADU). Klik in het hoofdvenster van de ADU op **Profielbeheer > Nieuw** om een nieuw profiel voor de draadloze client te maken.



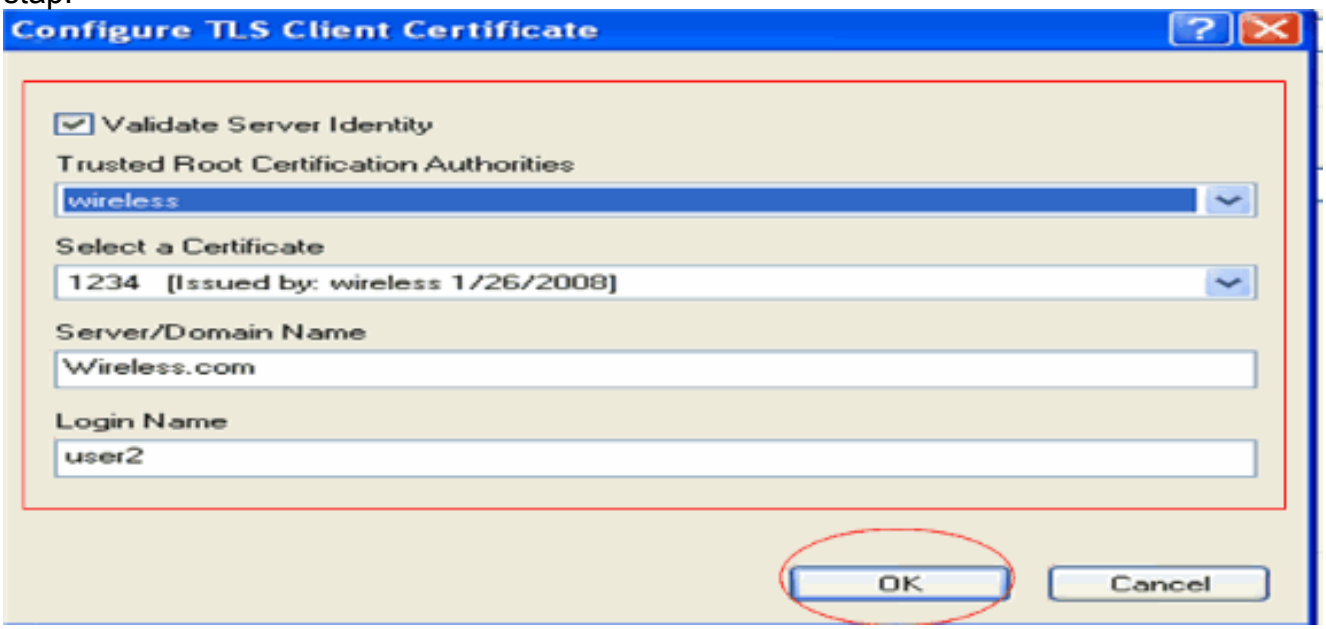

2. Geef een profielnaam op en wijs een SSID-naam toe aan dit profiel. Deze SSID naam zou het zelfde moeten zijn geconfigureerd op de WLC. In dit voorbeeld is de naam van de SSID **ldap**.




3. Klik op het tabblad **Beveiliging** en kies **802.1x/EAP** als Layer 2-beveiliging. Kies **EAP-FAST** als de EAP-methode en klik op **Configureren**.
4. Kies op de configuratiepagina EAP-FAST het **TLS-clientcertificaat** in de vervolgkeuzelijst EAP-FAST-verificatiemethode en klik op **Configureren**.




5. In het configuratievenster van het TLS-clientcertificaat:Schakel het aanvinkvakje **Validate Server Identity in** en selecteer het CA-certificaat dat op de client is geïnstalleerd (uitgelegd in het gedeelte Generate the Root CA certificate for the Client sectie of this document) als de Trusted Root-certificeringsinstantie.Selecteer het apparaatcertificaat dat op de client is geïnstalleerd (uitgelegd in het gedeelte Apparaatcertificaat genereren voor het gedeelte Cliënt van dit document) als clientcertificaat.Klik op **OK**.Dit voorbeeld verklaart deze stap:




Het profiel voor de draadloze client wordt gemaakt.

## Verifiëren

Voer deze stappen uit om te verifiëren of uw configuratie correct werkt.

1. Activeer de **ldap** SSID op de ADU.
2. Klik op **Ja** of op **OK** zoals vereist in de volgende vensters. U moet alle stappen van client-

verificatie en associatie kunnen zien om succesvol te zijn op de ADU.

Gebruik deze sectie om te controleren of uw configuratie goed werkt. Gebruik de WLC CLI-modus.

- Om te verifiëren of WLC met de LDAP server kan communiceren en de gebruiker vinden, specificeer **debug aaa ldap inschakelen** opdracht van de WLC CLI. Dit voorbeeld verklaart een succesvol communicatie LDAP proces:**N.B.: Een** deel van de uitvoer in deze sectie is verplaatst naar de tweede regel vanwege de ruimteoverweging.(Cisco Controller) **>debug aaa ladp activeren**

```
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
```

Uit de gemarkeerde informatie in deze debug-uitvoer is duidelijk dat de LDAP-server door de WLC wordt bevraagd met de Gebruikerskenmerken die op de WLC zijn gespecificeerd en dat het LDAP-proces succesvol is.

- Om te verifiëren of lokale EAP-verificatie succesvol is, specificeert u de **debug aaa Local-auth eap method events** van de WLC CLI. Hierna volgt een voorbeeld:(Cisco Controller) **>debug aaa local-auth eap method events inschakelen**

```
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)**

.....

.....

.....

.....
.

- De opdracht **debug aaa local-auth** is ook erg handig. Hierna volgt een voorbeeld:(Cisco Controller) **>debug aaa local-auth dB inschakelen**

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
```

- Om de certificaten te bekijken die in WLC worden geïnstalleerd om voor lokale authentificatie worden gebruikt, geef het bevel van **show** de **certificaten van de lokale autoriteit** van CLI uit. Hierna volgt een voorbeeld:(Cisco Controller) **>certificaten van lokale autoriteiten weergeven**

```
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.
```

- Om de lokale authentificatieconfiguratie op WLC van de CLI wijze te bekijken, geef het bevel **show local-auth** Config uit. Hierna volgt een voorbeeld:(Cisco Controller) **>configuratie lokale status tonen**

```
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
```

# Problemen oplossen

U kunt deze opdrachten gebruiken om problemen met uw configuratie op te lossen:

- **debug aaa local-auth eap method gebeurtenissen activeren**
- **debug aaa all enable**
- **debug dot1x-pakket inschakelen**

## Gerelateerde informatie

- EAP-FAST-verificatie met draadloze LAN-controllers en externe RADIUS-serverconfiguratievoorbeeld
- PEAP onder Unified Wireless Networks met Microsoft Internet Verification Service (IAS)
- Dynamische VLAN-toewijzing met WLC's op basis van ACS naar Active Directory Group Mapping Configuration Voorbeeld
- Configuratiehandleiding voor Cisco draadloze LAN-controllers - Security oplossingen configureren
- Configuratiehandleiding voor Cisco draadloze LAN-controllers - Software en configuraties voor beheercontrollers
- Configuratie-voorbeeld van EAP-verificatie met WLAN-controllers (WLC)
- Draadloos LAN-controller (WLC) ontwerp en functies Veelgestelde vragen
- Cisco Secure Services-client met EAP-FAST-verificatie
- Veelgestelde vragen over wireless LAN-controller (WLC)
- Controllers draadloze LAN-controller (WLC) fout- en systeemmeldingen Veelgestelde vragen
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.