

# EAP-TLS onder Unified Wireless Network met ACS 4.0 en Windows 2003

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Netwerkdigram](#)

[Conventies](#)

[Windows Enterprise 2003 instellen met IIS, certificaatinstantie, DNS, DHCP \(DC CA\)](#)

[DC CA \(draadloze democratie\)](#)

[Windows Standard 2003 Setup met Cisco Secure ACS 4.0](#)

[Basisinstallatie en -configuratie](#)

[Cisco beveiligde ACS 4.0 installatie](#)

[Configuratie van Cisco LWAPP-controllers](#)

[De gewenste configuratie voor WAP2/WAP maken](#)

[EAP-TLS-verificatie](#)

[Installeer de sjablonen van het certificaat magnetisch in](#)

[De certificaatsjabloon voor de ACS-webserver maken](#)

[De nieuwe ACS-webservercertificaatsjabloon inschakelen](#)

[ACS 4.0 certificaatinstelling](#)

[Exportcertificaat voor ACS configureren](#)

[Installeer het certificaat in de ACS 4.0-software](#)

[CLIENTconfiguratie voor MAP-TLS met behulp van Windows Zero Touch](#)

[Een basisinstallatie en -configuratie uitvoeren](#)

[De draadloze netwerkverbinding configureren](#)

[Gerelateerde informatie](#)

## [Inleiding](#)

Dit document beschrijft hoe u beveiligde draadloze toegang kunt configureren met behulp van draadloze LAN-controllers (WLC's), Microsoft Windows 2003-software en Cisco Secure Access Control Server (ACS) 4.0 via Extensible Authentication Protocol-Transport Layer Security (EAP-TLS).

**Opmerking:** Raadpleeg voor meer informatie over de implementatie van beveiligde draadloze verbindingen de [Microsoft Wi-Fi-website](#) en [Cisco SAFE Wireless Blueprint](#).

## [Voorwaarden](#)

## Vereisten

Er wordt aangenomen dat de installateur kennis heeft van de basisinstallatie van Windows 2003 en de installatie van Cisco-controllers, aangezien dit document alleen de specifieke configuraties bevat om de tests te vergemakkelijken.

Raadpleeg de [Snelle startgids](#) voor informatie over de installatie en de configuratie van de Cisco 4400 Series controllers: [Cisco 4400 Series draadloze LAN-controllers](#). Raadpleeg de [Snelle startgids](#) voor informatie over de installatie en de configuratie van de Cisco 2000 Series controllers: [Cisco 2000 Series draadloze LAN-controllers](#).

Voordat u begint, installeert u de Windows Server 2003 met Service Pack (SP)1 besturingssysteem op elk van de servers in het testlaboratorium en werkt u alle servicepakketten bij. Installeer de controllers en AP's en zorg ervoor dat de laatste softwareupdates worden geconfigureerd.

**Belangrijk:** Op het moment dat dit document is geschreven, is SP1 de nieuwste Windows Server 2003 update, en SP2 met update patches is de nieuwste software voor Windows XP Professional.

Windows Server 2003 met SP1, Enterprise Edition, wordt gebruikt zodat de automatische inschrijving van gebruikers- en werkstationcertificaten voor EAP-TLS-verificatie kan worden geconfigureerd. Dit wordt beschreven in het gedeelte [EAP-TLS-verificatie](#) van dit document. Automatische inschrijving en automatische vernieuwing van het certificaat maken het gemakkelijker om certificaten in te voeren en de veiligheid te verbeteren door automatisch certificaten te beëindigen en te verlengen.

## Gebruikte componenten

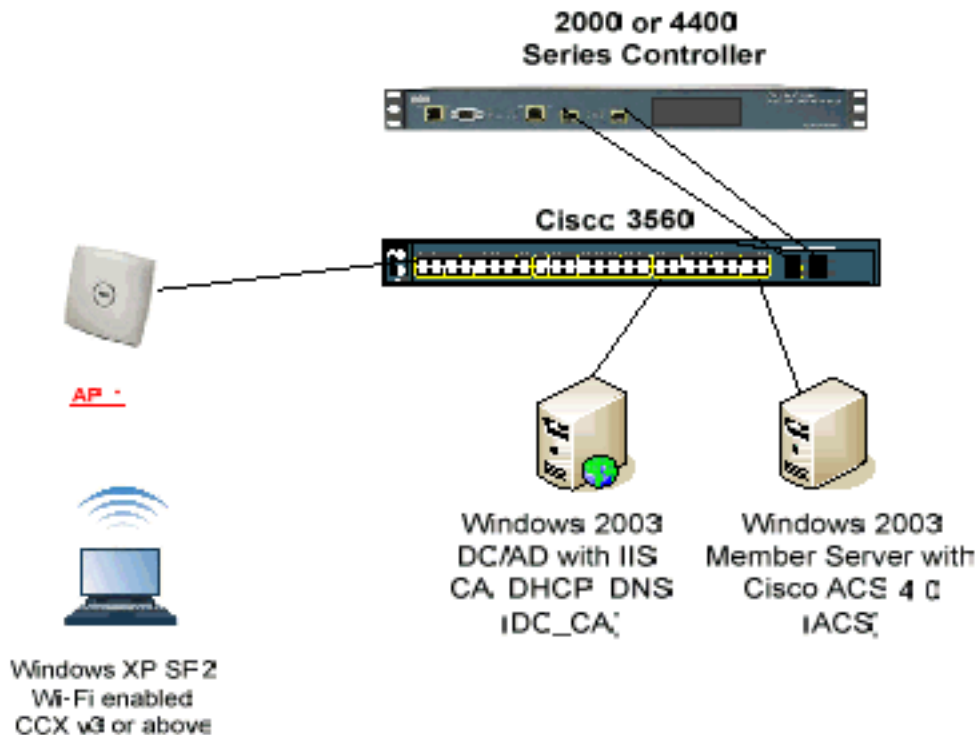
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 2006 of 4400 Series controller op 3.2.16.21
- Cisco Aironet 1131 lichtgewicht access point Protocol (LWAPP) AP
- Windows 2003 Enterprise met geïnstalleerde Internet Information Server (IS), certificaatautoriteit (CA), DHCP en Domain Name System (DNS)
- Windows 2003 Standard met Access Control Server (ACS) 4.0
- Windows XP Professional met SP (en bijgewerkte servicepakketten) en draadloze netwerkinterfacekaart (NIC) (met CCX v3-ondersteuning) of hardware van derden.
- Cisco 3560 Switch

## Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:

**Cisco beveiligde draadloze labourologie**



Het belangrijkste doel van dit document is u de stap-voor-stap procedure te bieden om het MAP-TLS onder Unified Wireless Networks te implementeren met ACS 4.0 en de Windows 2003 Enterprise-server. De belangrijkste nadruk is op het automatisch registreren van de client zodat de client automatisch inlogt en het certificaat van de server ontvangt.

**Opmerking:** Om Wi-Fi Protected Access (WAP)/WAP2 toe te voegen met Temperatuur Key Integrity Protocol (TKIP)/Advanced Encryption Standard (AES) aan Windows XP Professional met SP, raadpleeg [WAP2/Wireless Provisioning Services Information Element \(WPS IE\)-update voor Windows XP met SP2](#).

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 de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

## Windows Enterprise 2003 instellen met IIS, certificaatinstantie, DNS, DHCP (DC\_CA)

### DC\_CA (draadloze democratie)

DC\_CA is een computer die Windows Server 2003 met SP1, Enterprise Edition runt en deze rollen uitvoert:

- Een domeincontroller voor de draadloze demo.local-domein dat IS draait
- Een DNS-server voor het draadloze modem.lokale DNS-domein
- Een DHCP-server
- Enterprise root CA voor de draadloze demo.local

Voltooi deze stappen om DC\_CA voor deze services te configureren:

1. [Voer een basisinstallatie en -configuratie uit.](#)
2. [Configuratie van de computer als een domeincontroller.](#)
3. [Verhoog het functionele niveau van het domein.](#)
4. [Installeer en configureer DHCP.](#)
5. [Installeer de certificatediensten.](#)
6. [Controleer de Administrator-rechten voor certificaten.](#)
7. [Voeg computers toe aan het domein.](#)
8. [Draadloze toegang tot computers toestaan](#)
9. [Voeg gebruikers aan het domein toe.](#)
10. [Draadloze toegang voor gebruikers toestaan](#)
11. [Voeg groepen toe aan het domein.](#)
12. [Voeg gebruikers aan de groep Draadloze gebruikers toe.](#)
13. [Voeg clientcomputers toe aan de groep Wireless-Gebruikers.](#)

### Stap 1: Basis installatie en configuratie uitvoeren

Voer de volgende stappen uit:

1. Installeer Windows Server 2003 met SP1, Enterprise Edition, als een zelfstandige server.
2. Configureer het TCP/IP-protocol met het IP-adres van 172.16.100.26 en het subnetmasker van 255.255.255.0.

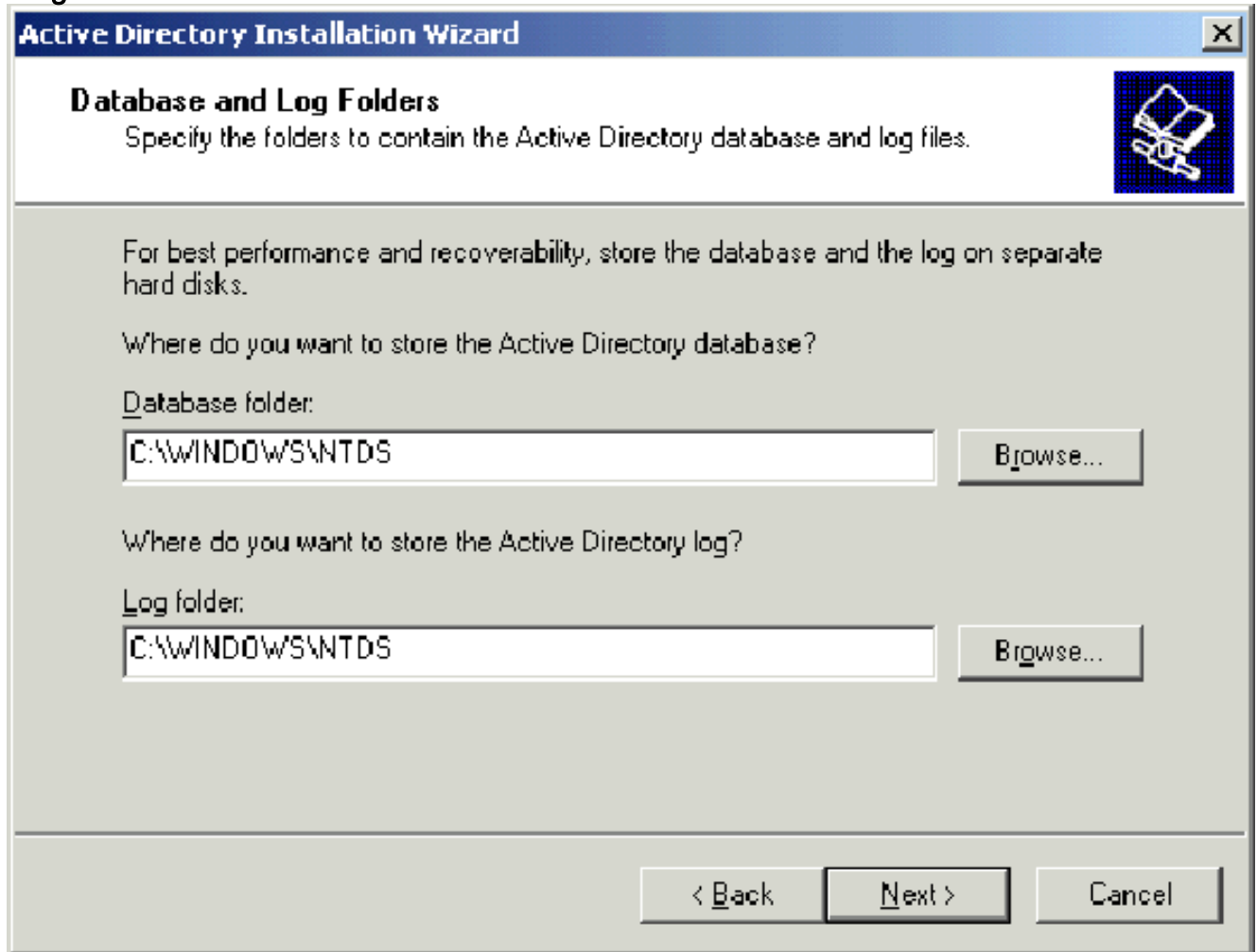
### Stap 2: De computer configureren als een Domain Controller

Voer de volgende stappen uit:

1. Om de wizard Actieve map installeren te starten, kiest u **Start > Start > Run**, typt u **dcpromo.exe** en klikt u op **OK**.
2. Klik in de pagina Welkom in de Active Directory Installatie Wizard op **Volgende**.
3. Klik op **Volgende** op de pagina Compatibiliteit met besturingssysteem.
4. Selecteer in de pagina Domain Controller Type de optie **Domain Controller voor een nieuw domein** en klik op **Volgende**.
5. Selecteer in de pagina Nieuw domein maken de optie **Domain in een nieuw bos** en klik op **Volgende**.
6. Selecteer in het gedeelte Installeer of Configureer de DNS-pagina **door Nee te selecteren en DNS op deze computer te configureren** en op **Volgende** te klikken.
7. Typ **Wireless-demo.local** op de pagina Nieuwe domeinnaam en klik op **Volgende**.
8. Voer op de pagina Domain Name <Domain Name>de Domeinnaam van **Netopgemerkt** in als **een draadloze** versie en klik op **Volgende**.

9. Op de pagina Database en Log Folders Locatie accepteert u de standaard database en logmappen en klikt u op

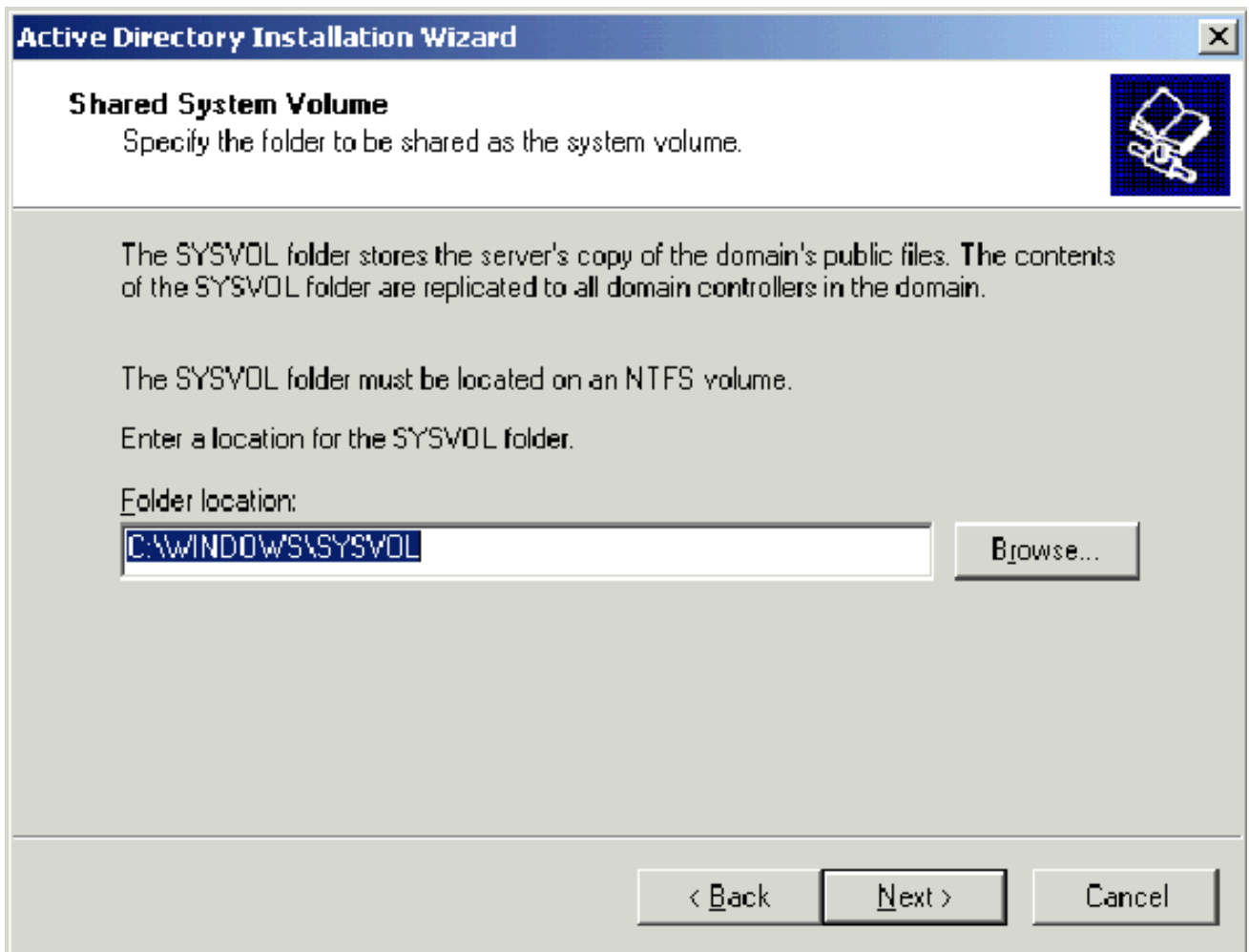
**Volgende.**



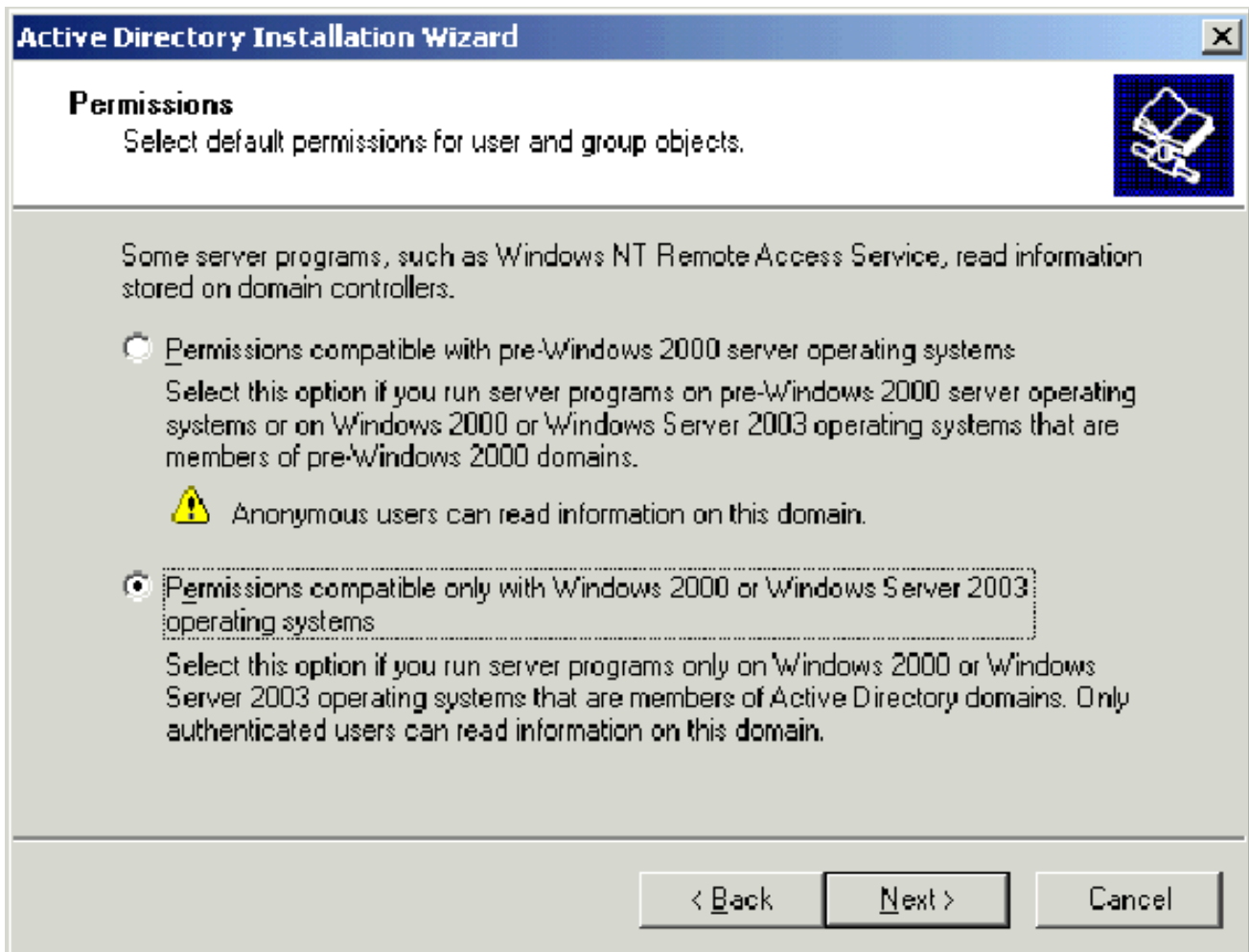
The screenshot shows a Windows dialog box titled "Active Directory Installation Wizard". The main heading is "Database and Log Folders" with a sub-instruction: "Specify the folders to contain the Active Directory database and log files." Below this, a note states: "For best performance and recoverability, store the database and the log on separate hard disks." The question "Where do you want to store the Active Directory database?" is followed by a text field labeled "Database folder:" containing "C:\WINDOWS\NTDS" and a "Browse..." button. A second question, "Where do you want to store the Active Directory log?", is followed by a text field labeled "Log folder:" also containing "C:\WINDOWS\NTDS" and a "Browse..." button. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

10. Controleer in het dialoogvenster Gedeeld systeemvolume of de standaardmaplocatie correct is en klik op

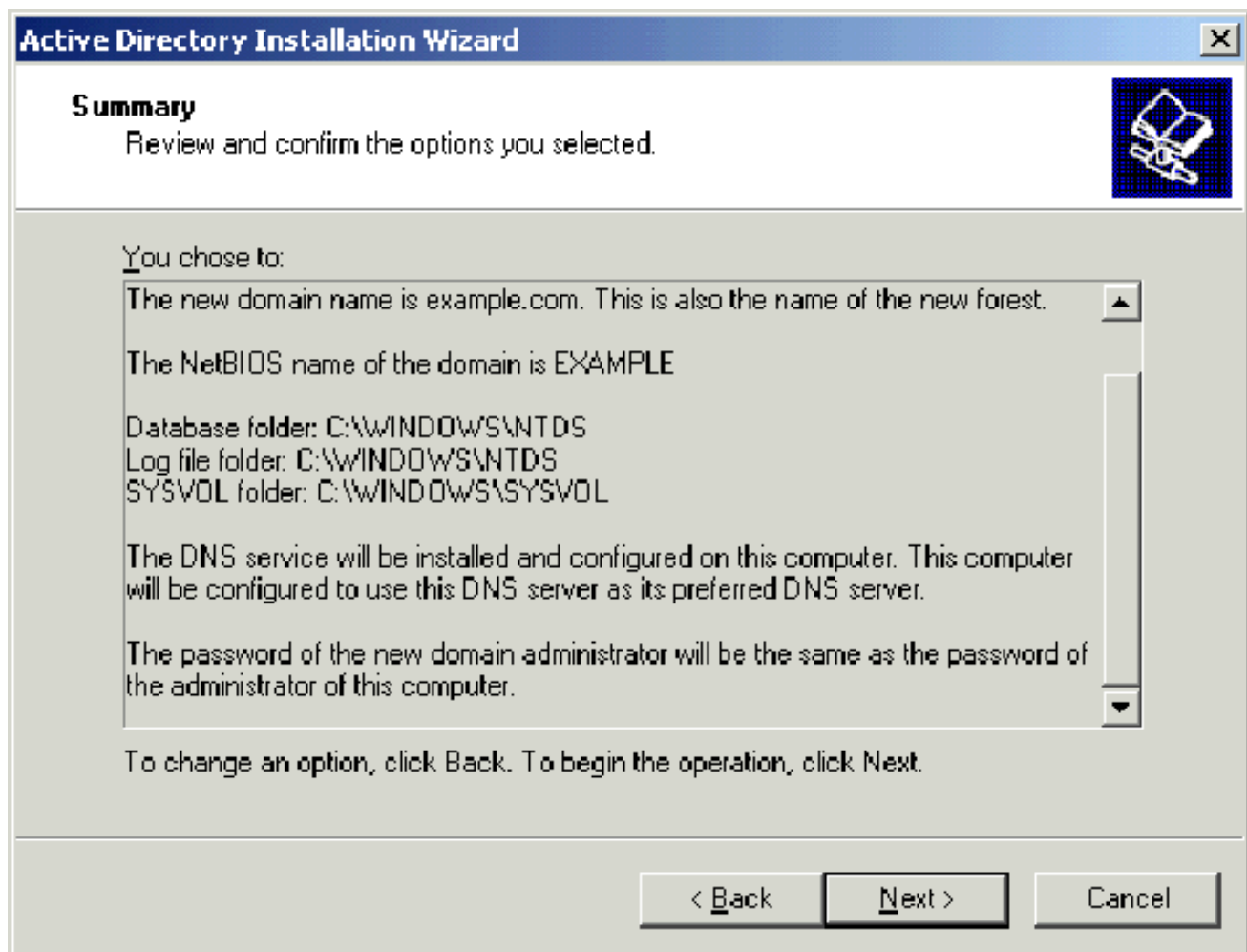
**Volgende.**



11. Controleer of toegangsrechten die alleen compatibel zijn met Windows 2000 of Windows Server 2003-besturingssysteem zijn geselecteerd en klik op Volgende.



12. Laat de wachtwoordvakjes leeg op de pagina Terugzetten van adresservices en klik op **Volgende**.
13. Bekijk de informatie op de overzichtspagina en klik op **Volgende**.



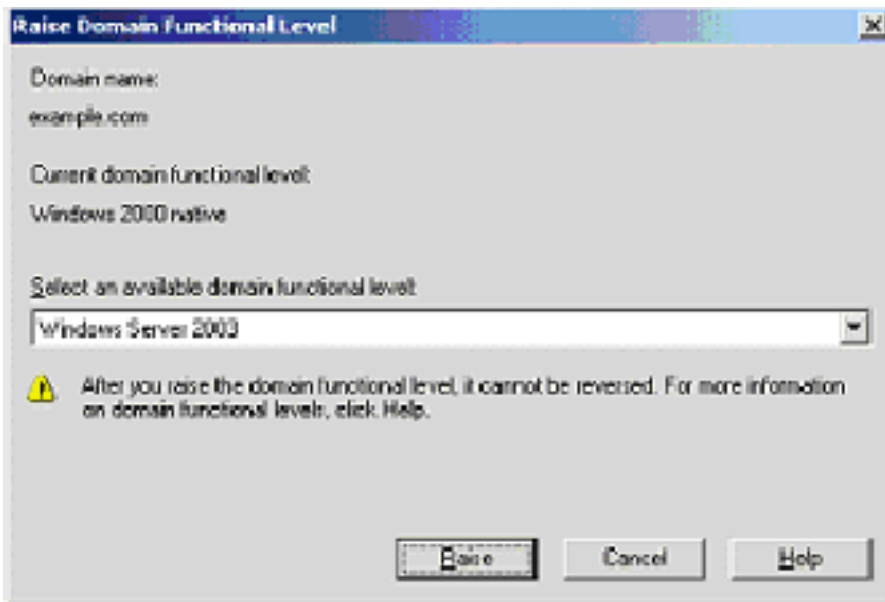
14. Klik op **Voltooien** van de pagina met de installatiewizard van de actieve map.
15. Klik na het opstarten van de computer op **Nu opnieuw starten**.

### [Stap 3: Het functionele niveau van het domein verhogen](#)

Voer de volgende stappen uit:

1. Open de map Active Directory Domain en Trusts magneet-inbeling uit de map beheertools (**Start > Beheertools > Active Directory Domain and Trusts**) en klik met de rechtermuisknop op de domeincomputer **DC\_CA.wirelessdemo.local**.
2. Klik op **Functioneel niveau** verhogen en selecteer vervolgens **Windows Server 2003** op de pagina Functioneel niveau





vergroten.

3. Klik op **Omhoog** , klik op **OK** en klik vervolgens nogmaals op **OK**.

#### [Stap 4: DHCP installeren en configureren](#)

Voer de volgende stappen uit:

1. Installeer Dynamic Host Configuration Protocol (DHCP) als onderdeel van de netwerkservice door **programma's toe te voegen of te verwijderen** in het Configuratiescherm.
2. Open de DHCP-connector van de map Administrator Gereedschappen (**Start > Programma's > Administratieve tools > DHCP**), en markeer vervolgens de DHCP-server, **DC\_CA.wirelessdemo.local**.
3. Klik op **Action** en vervolgens op **Authorized** om de DHCP-service te autoriseren.
4. Op de console boom, klik met de rechtermuisknop **DC\_CA.wirelessdemo.local** en klik vervolgens op **New Range**.
5. Klik op **Volgende** op de welkomspagina van de wizard Nieuw gebied.
6. Typ in het veld Naam in het veld Naam **CorpNet** het type **CorpNet**.

## New Scope Wizard

### Scope Name

You have to provide an identifying scope name. You also have the option of providing a description.



Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

< Back

Next >

Cancel

7. Klik op **Volgende** en vul deze parameters in: Start IP-adres—172.16.100.1 End-IP-adres—172.16.100.254 Lengte—24 Subnetmasker—255.255.255.0

## New Scope Wizard

### IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.



Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length:

Subnet mask:

< Back

Next >

Cancel

- Klik op **Next** en voer **172.16.100.1** in voor het Start IP-adres en **172.16.100.100** voor het uitsluiten van het End IP-adres. Klik op **Volgende**. Deze gereserveerde IP-adressen worden niet toegewezen door de DHCP-server.

## New Scope Wizard

### Add Exclusions

Exclusions are addresses or a range of addresses that are not distributed by the server.



Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:

End IP address:

Excluded address range:

9. Klik op **Volgende** op de pagina Lease Duration.

10. Kies op de pagina DHCP-opties configureren **ja, ik wil deze opties nu configureren** en op **Volgende** klikken.

## New Scope Wizard

### Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.



When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

- Yes, I want to configure these options now
- No, I will configure these options later

< Back

Next >

Cancel

11. Voeg op de pagina Router (Standaard gateway) het standaardrouteradres van **172.16.100.1 toe** en klik op **Volgende**.

### Router (Default Gateway)

You can specify the routers, or default gateways, to be distributed by this scope.



To add an IP address for a router used by clients, enter the address below.

IP address:

Add

172.16.100.1
--------------

Remove

Up

Down

< Back

Next >

Cancel

12. Op de pagina Domain Name and DNS Server, type **Wireless-demo.local** in het veld Parent-domein, type **172.16.100.26** in het veld IP-adres en klik vervolgens op **Add** en klik op **Next**.

## New Scope Wizard

### Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.



You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:

Resolve

IP address:

172.16.100.26

Add

Remove

Up

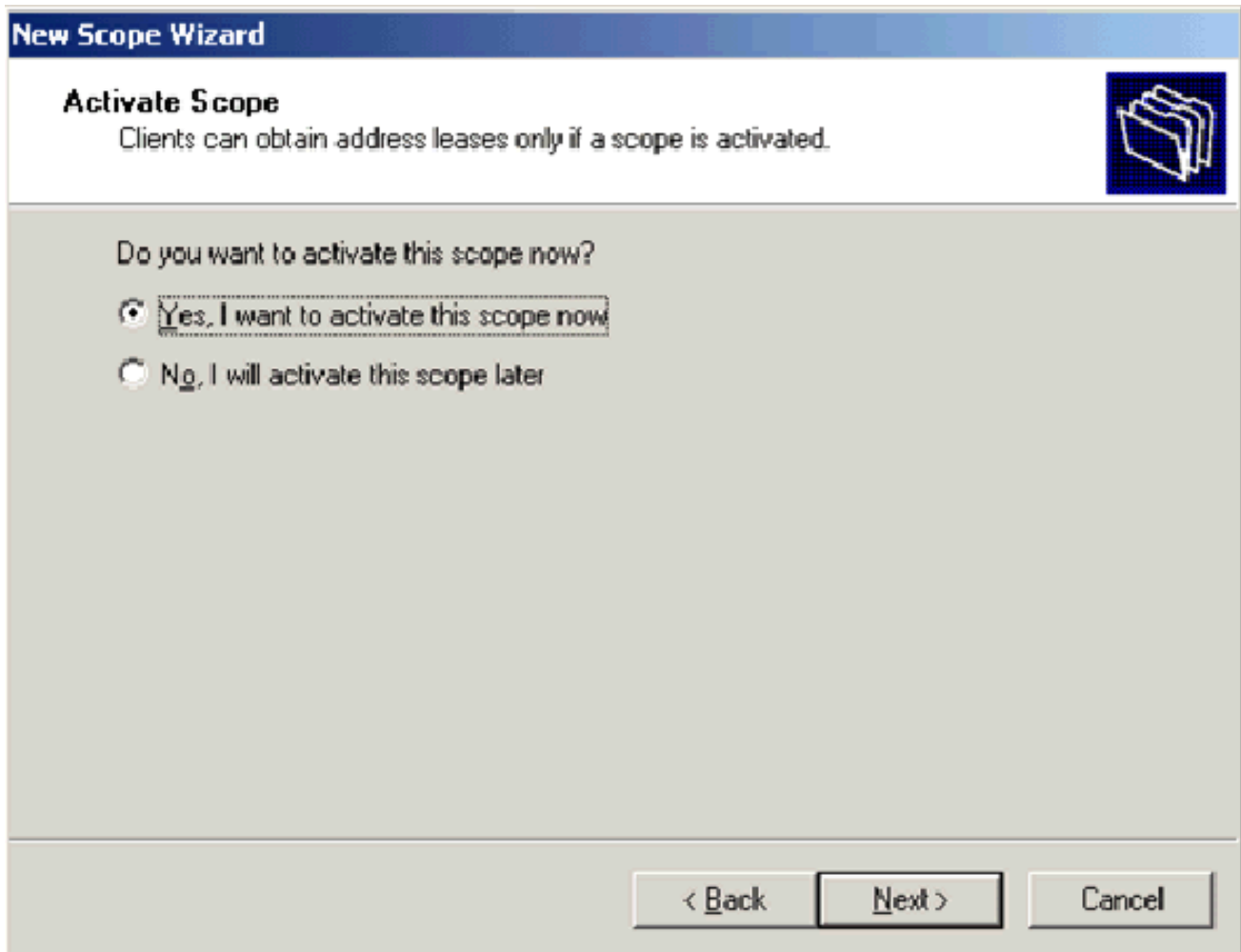
Down

< Back

Next >

Cancel

13. Klik op **Volgende** op de pagina WINS Server.
14. Kies op de pagina Toepassingsgebied activeren **ja, ik wil deze werkingsfeer nu activeren** en op **Volgende** klikken.



15. Klik op **Voltooien** van de **pagina** Nieuwe wizard.

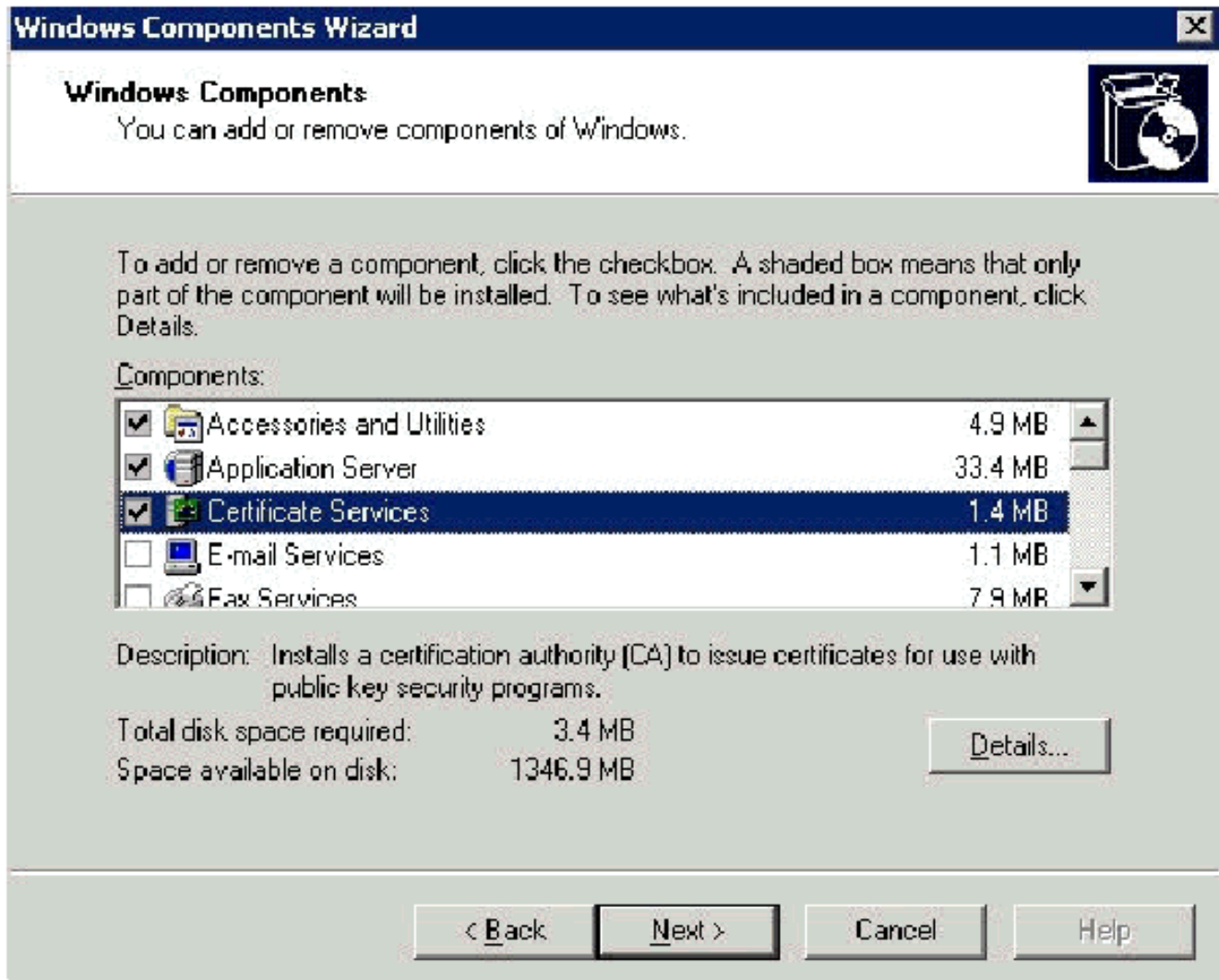
### [Stap 5: certificaatservices installeren](#)

Voer de volgende stappen uit:

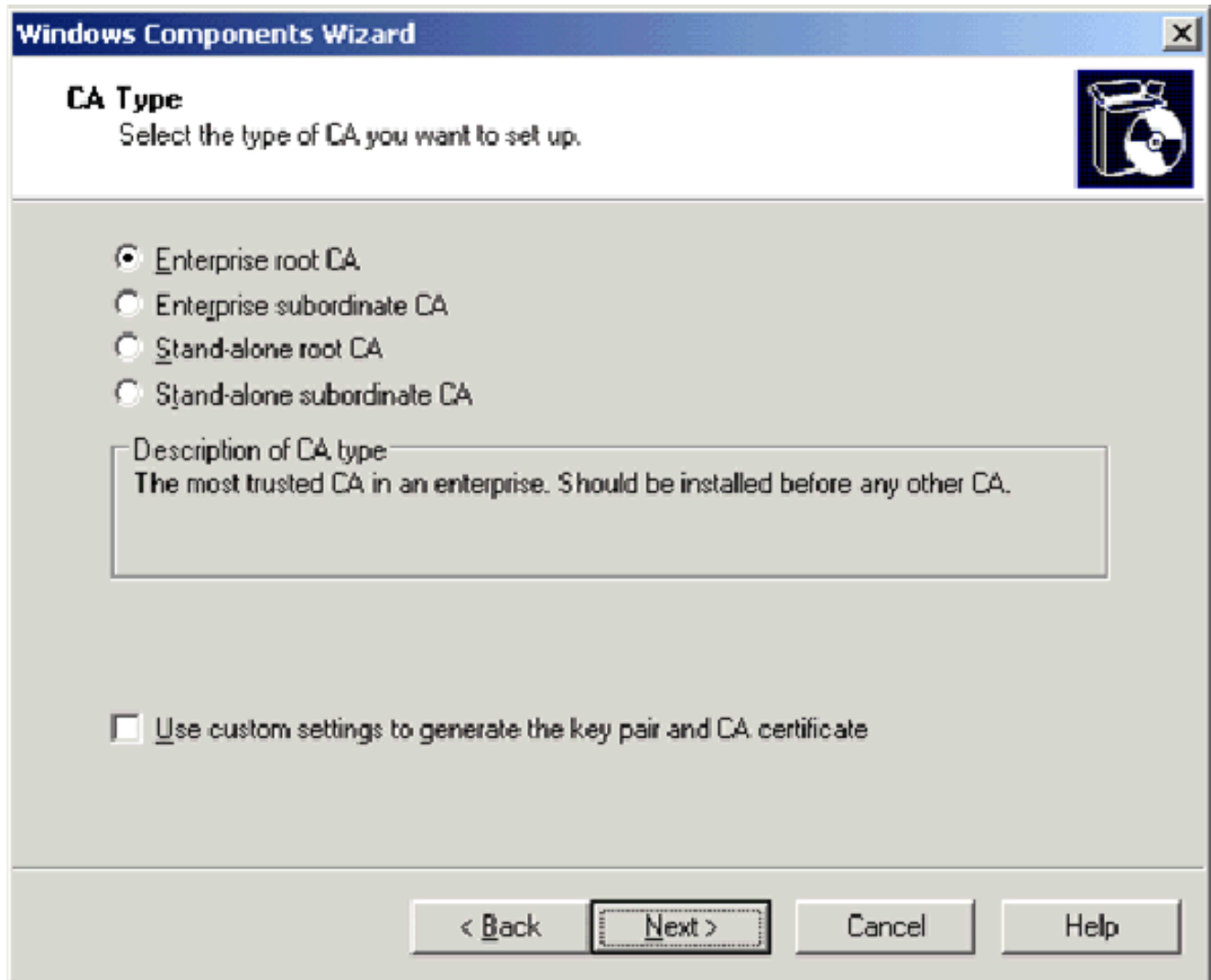
**Opmerking:** IS moet geïnstalleerd voordat u certificaatservices installeert en de gebruiker moet onderdeel uitmaken van de Enterprise Admin OU.

1. Open in het Configuratiescherm de **programma's toevoegen of verwijderen** en klik vervolgens op **Windows-onderdelen toevoegen of verwijderen**.
2. Selecteer in de Wizard Windows-onderdelen de optie **certificaatservices** en klik vervolgens op **Volgende**.

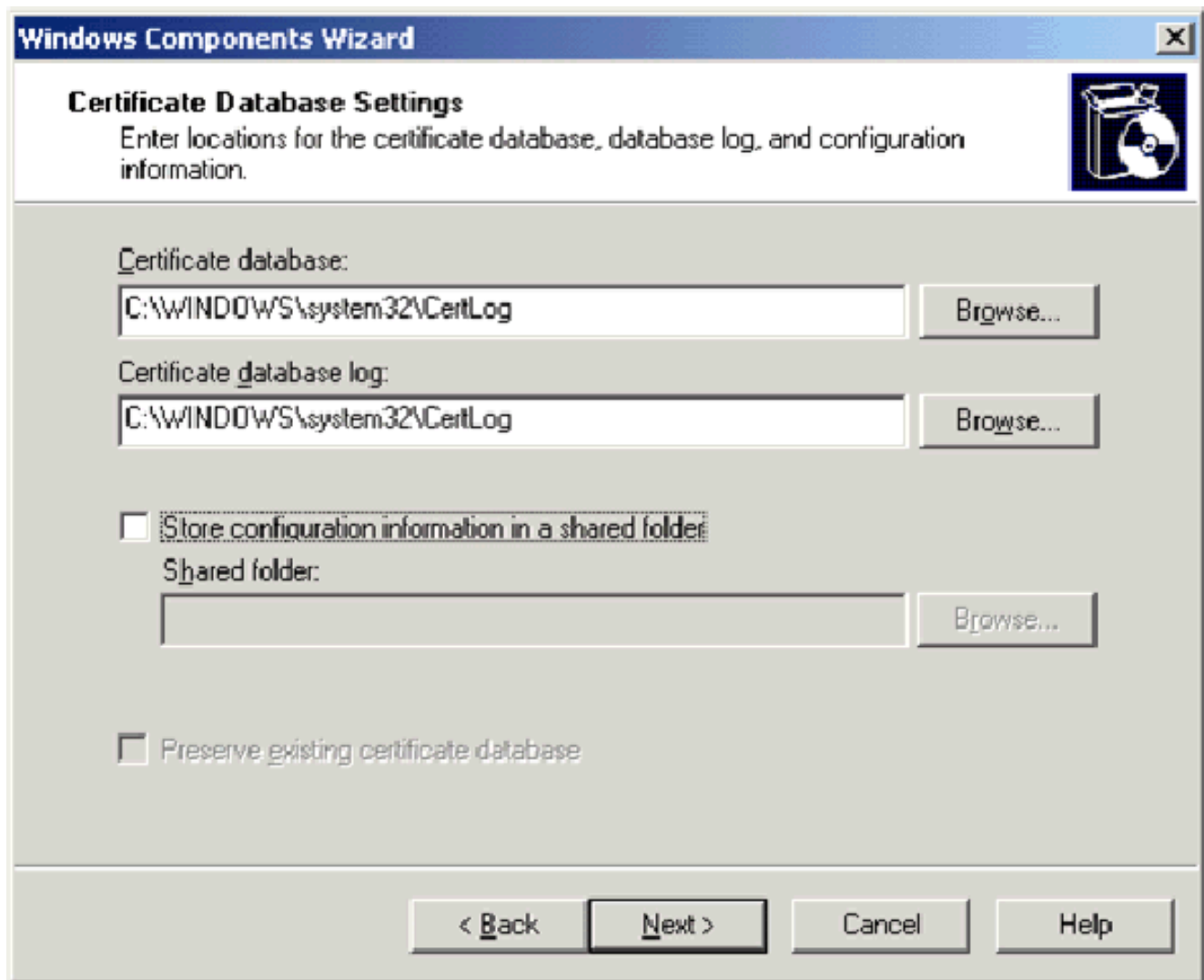




3. Kies op de CA-pagina type **CA-wortel** en klik op **Volgende**.



4. Op de CA Identificatie van de informatiepagina, type **draadloze democra** in de Gemeenschappelijke naam voor dit CA vakje. U kunt de andere optionele gegevens invoeren en vervolgens op **Volgende** klikken. Accepteer de standaardinstellingen op de pagina Instellingen van de certificaatdatabase.

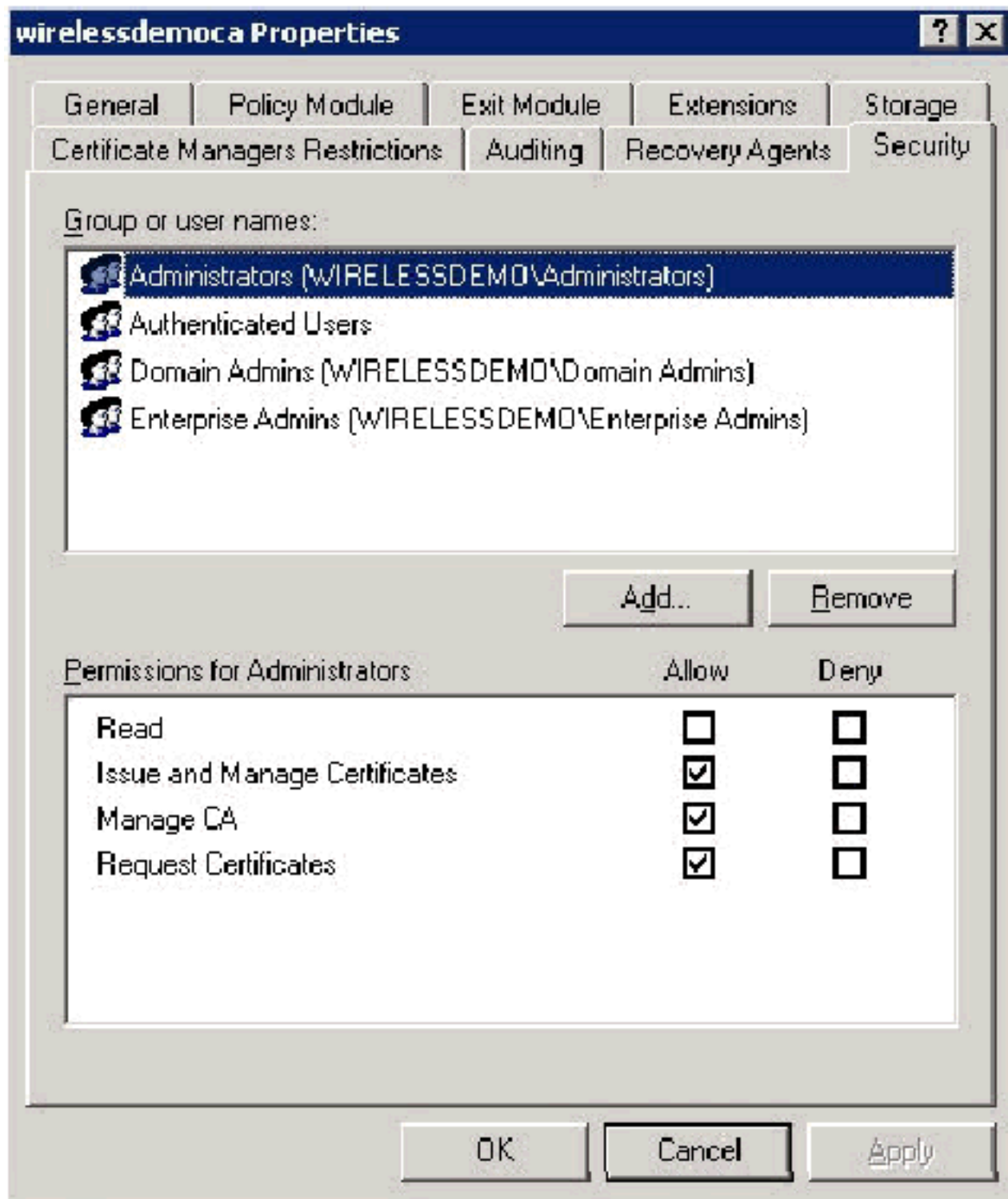


5. Klik op **Volgende**. Klik na voltooiing van de installatie op **Voltooien**.
6. Klik op **OK** nadat u de waarschuwing voor het installeren van IS hebt gelezen.

### [Stap 6: Controleer de Administrator-toegangsrechten voor certificaten](#)

Voer de volgende stappen uit:

1. Kies **Start > Administratieve hulpmiddelen > certificeringsinstantie**.
2. Klik met de rechtermuisknop op **draadloze democratie CA** en klik vervolgens op **Properties**.
3. Klik in het tabblad **Beveiliging** op **Beheerders** in de lijst **Groep of Gebruikersnaam**.
4. Controleer in de lijst met toegangsrechten of beheerders of deze opties zijn ingesteld op **Toestaan van: Certificaten afgeven en beheren** **CA beheren Certificaten aanvragen** Als een van deze instellingen op **Deny** is ingesteld of niet geselecteerd is, stelt u de toestemming in om **Staan toe** te staan.



5. Klik op **OK** om het dialoogvenster Wireless-democra CA-eigenschappen te sluiten en vervolgens de certificeringsinstantie te sluiten.

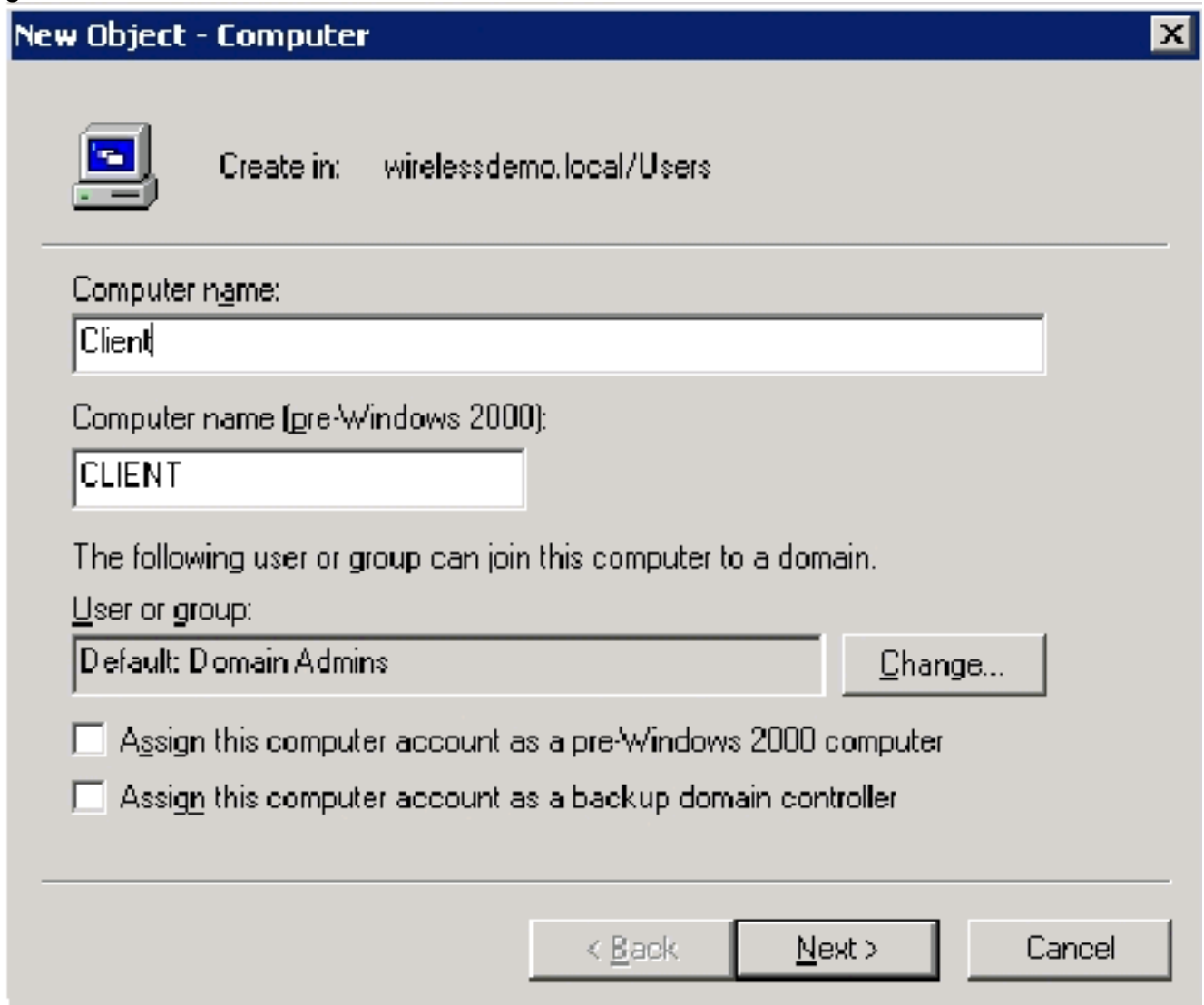
### [Stap 7: Computers aan het domein toevoegen](#)

Voer de volgende stappen uit:

**N.B.:** Als de computer al aan het domein is toegevoegd, gaat u naar [Gebruikers toevoegen aan het domein](#).

1. Open de optie Actieve gebruikers en computers in de map.
2. In de console boom, **breid draadloos demo.local uit**.
3. Klik met de rechtermuisknop op **Gebruikers**, klik op **Nieuw** en klik vervolgens op **Computer**.

4. Typ in het dialoogvenster Nieuw object - Computer de naam van de computer in het veld Naam van de computer en klik op **Volgende**. In dit voorbeeld wordt de computernaam **Client** gebruikt.



**New Object - Computer**

Create in: wirelessdemo.local/Users

Computer name:  
Client

Computer name (pre-Windows 2000):  
CLIENT

The following user or group can join this computer to a domain.  
User or group:  
Default: Domain Admins Change...

Assign this computer account as a pre-Windows 2000 computer  
 Assign this computer account as a backup domain controller

< Back **Next >** Cancel

5. Klik in het dialoogvenster Beheerd op **Volgende**.  
6. Klik in het dialoogvenster Nieuwe object-computer op **Voltoeien**.  
7. Herhaal stap 3 tot en met 6 om extra computerrekeningen te maken.

### [Stap 8: Draadloze toegang tot computers toestaan](#)

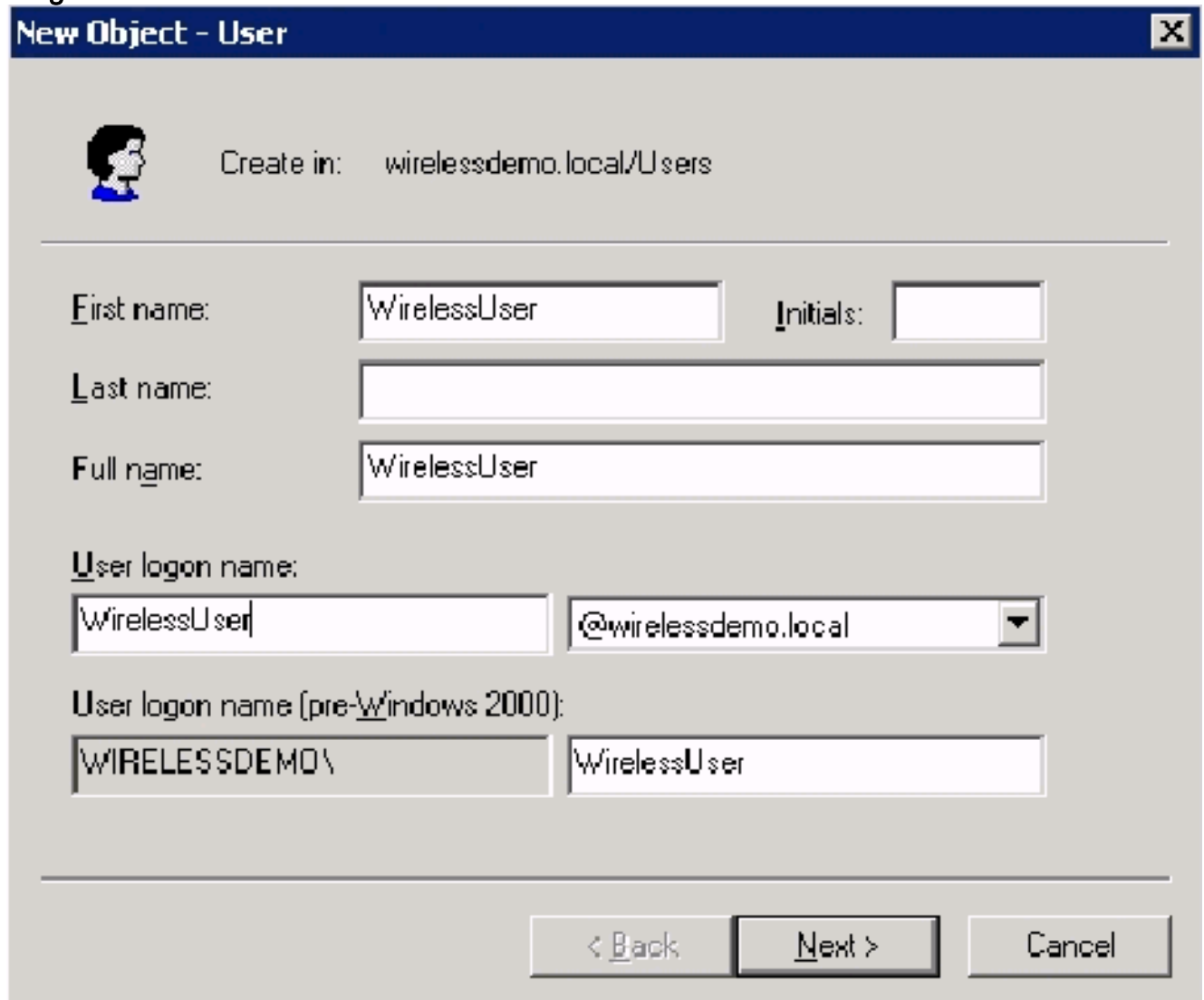
Voer de volgende stappen uit:

1. In de console van Actieve Gebruikers en Computers van de Map van de **Computers**, klik de map **Computers** en klik met de rechtermuisknop op de computer waarvoor u draadloze toegang wilt toewijzen. Dit voorbeeld toont de procedure met computer **CLIENT** die u in stap 7 hebt toegevoegd.
2. Klik op **Eigenschappen** en ga vervolgens naar het tabblad Inbellen.
3. Kies **Toegang toestaan** en klik op **OK**.

### [Stap 9: Gebruikers aan het domein toevoegen](#)

Voer de volgende stappen uit:

1. In de console van Actieve Gebruikers en Computers van de Map, klikt u met de rechtermuisknop op **Gebruikers**, klikt u op **Nieuw** en vervolgens klikt u op **Gebruiker**.
2. In het dialoogvenster Nieuw object - Gebruiker typt u **Draadloze** gebruiker in het veld Voornaam en typt u **draadloze** gebruiker in het veld Naam gebruiker en klikt u op **Volgende**.



**New Object - User**

Create in: wirelessdemo.local/Users

First name:  Initials:

Last name:

Full name:

User logon name:

User logon name (pre-Windows 2000):

< Back Next > Cancel

3. In het dialoogvenster Nieuw object - Gebruiker typt u een wachtwoord in het veld Wachtwoord en bevestigt u het wachtwoord. Schakel het **wachtwoord** uit door de gebruiker **bij de volgende** optie voor aanmelding te wijzigen en klik op **Volgende**.

New Object - User

Create in: wirelessdemo.local/Users

Password: [.....]

Confirm password: [.....]

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back    Next >    Cancel

4. Klik in het dialoogvenster Nieuw object - gebruiker op **Voltooien**.
5. Herhaal stap 2 tot en met 4 om extra gebruikersrekeningen te maken.

### [Stap 10: Draadloze toegang voor gebruikers toestaan](#)

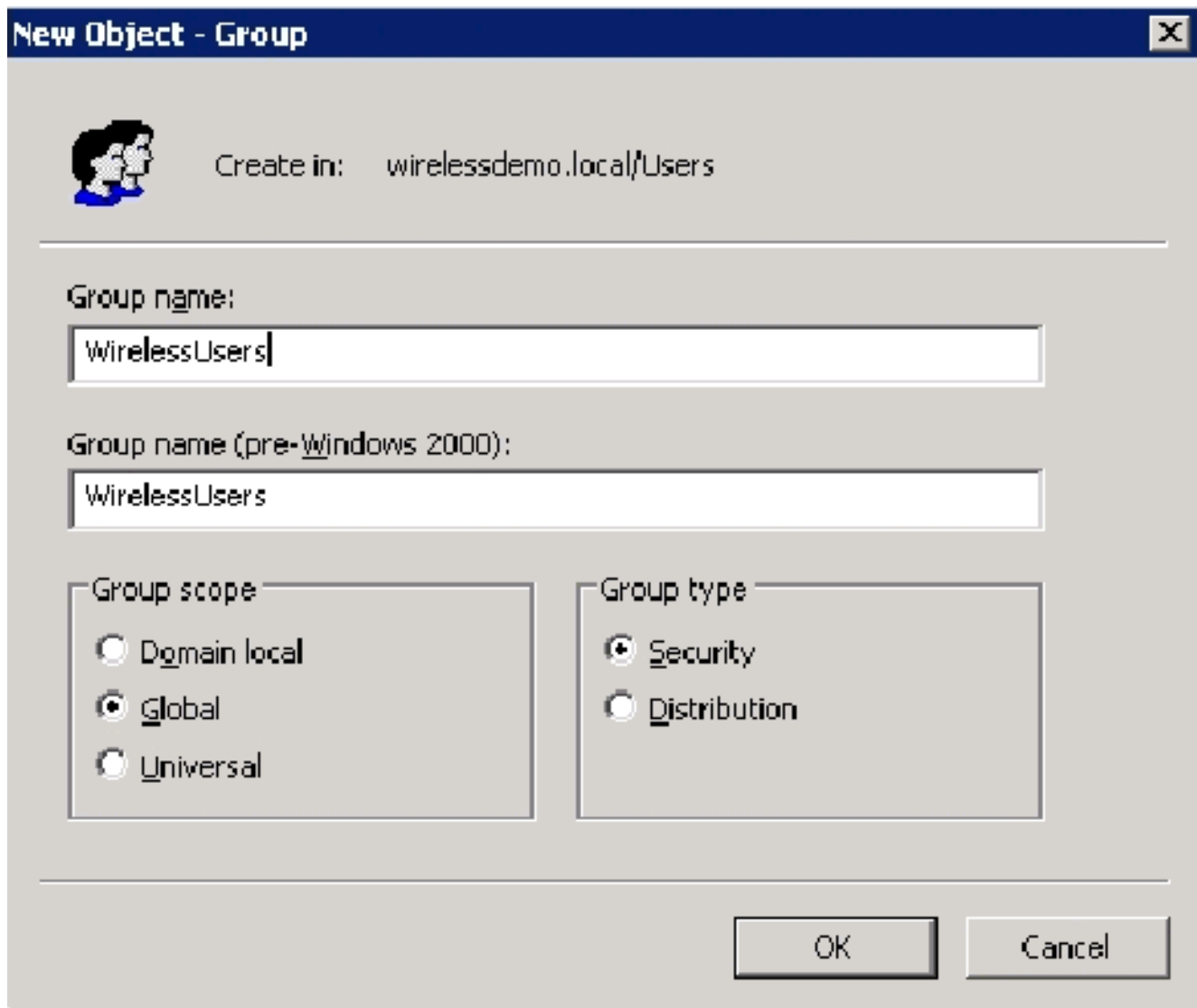
Voer de volgende stappen uit:

1. In de boom van de Gebruikers en computers van de Actieve Map van de **Gebruikers**, klik met de rechtermuisknop op **Draadloze** gebruiker, klik op **Eigenschappen** en ga dan naar het tabblad Inbelen.
2. Kies **Toegang toestaan** en klik op **OK**.

### [Stap 11: Groepen aan het domein toevoegen](#)

Voer de volgende stappen uit:

1. In de console van Actieve Gebruikers en Computers van de Map, klik met de rechtermuisknop op **Gebruikers**, klik op **Nieuw** en klik vervolgens op **Groep**.
2. Typ in het dialoogvenster Nieuwe object - groep de naam van de groep in het veld Naam van de groep en klik vervolgens op **OK**. Dit document gebruikt de groepsnaam **Draadloze gebruikers**.

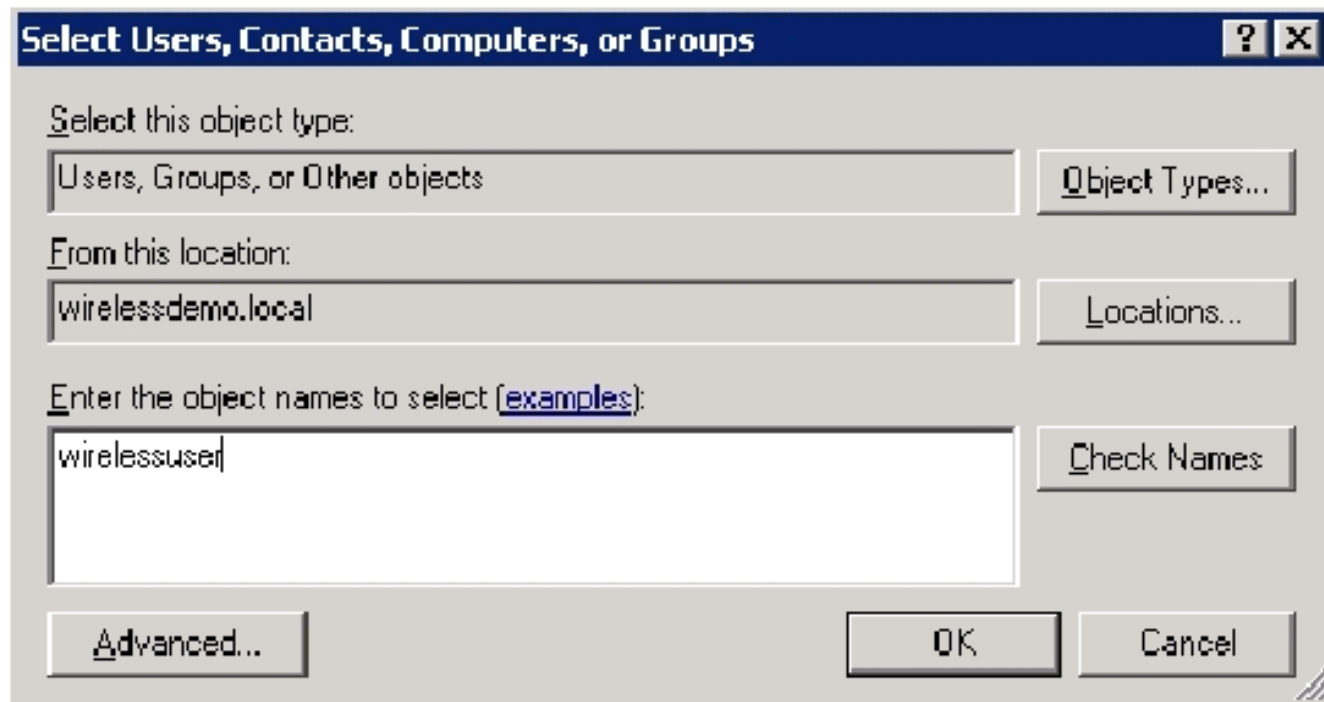


## [Stap 12: Gebruikers aan de groep draadloze gebruikers toevoegen](#)

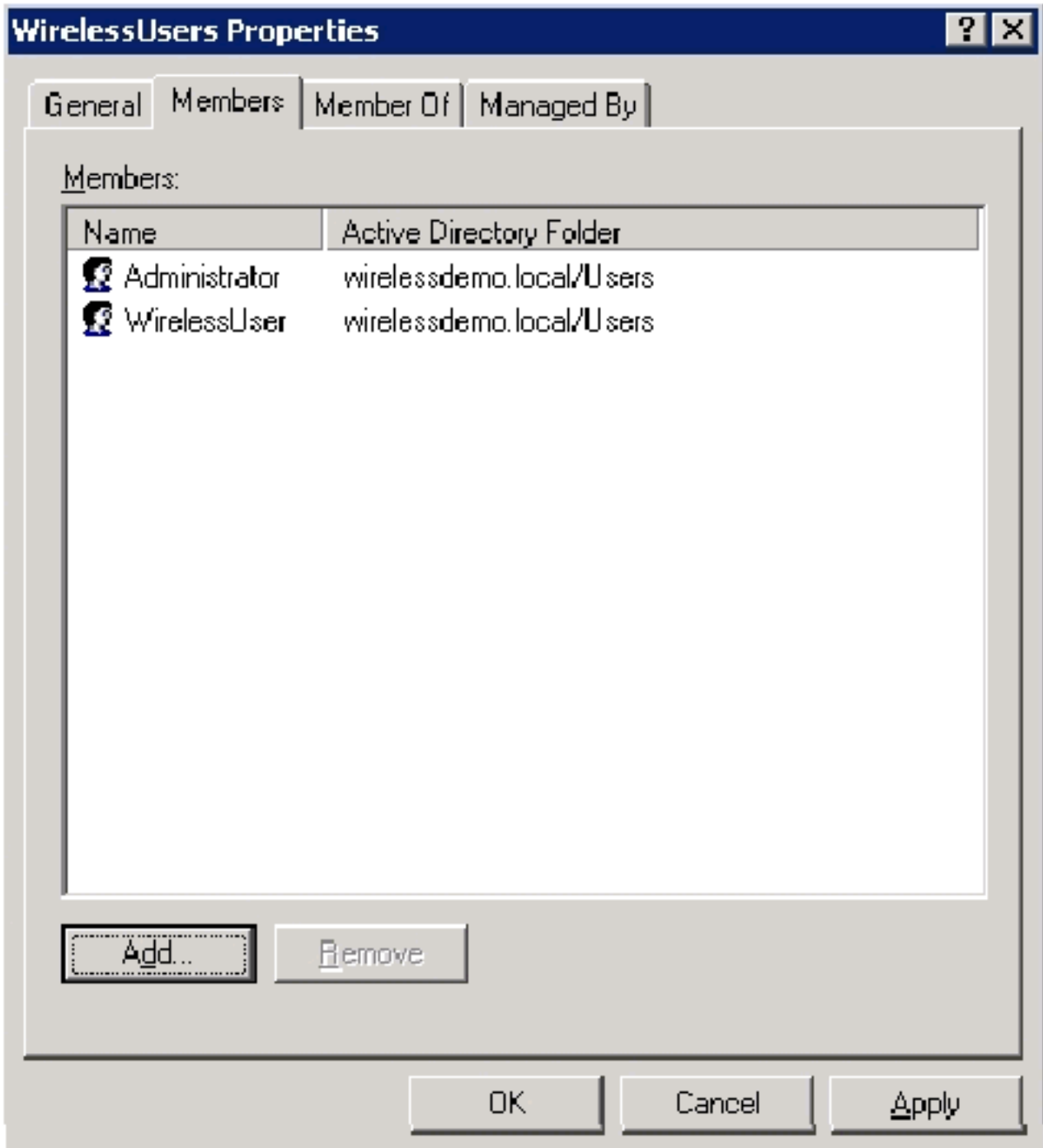
Voer de volgende stappen uit:

1. In het detailvenster van Actieve Gebruikers en Computers van de Map dubbelklik op de **Draadloze** groepgebruikers.
2. Ga naar het tabblad Leden en klik op **Toevoegen**.
3. In het dialoogvenster Gebruikers, contactgegevens, computers of groepen selecteren, typt u de naam van de gebruikers die u aan de groep wilt toevoegen. Dit voorbeeld toont hoe u de **draadloze gebruiker** aan de groep kunt toevoegen. Klik op **OK**.





4. Klik in het dialoogvenster Meerdere namen vinden op **OK**. De draadloze gebruikersaccount wordt toegevoegd aan de groep Draadloze gebruikers.

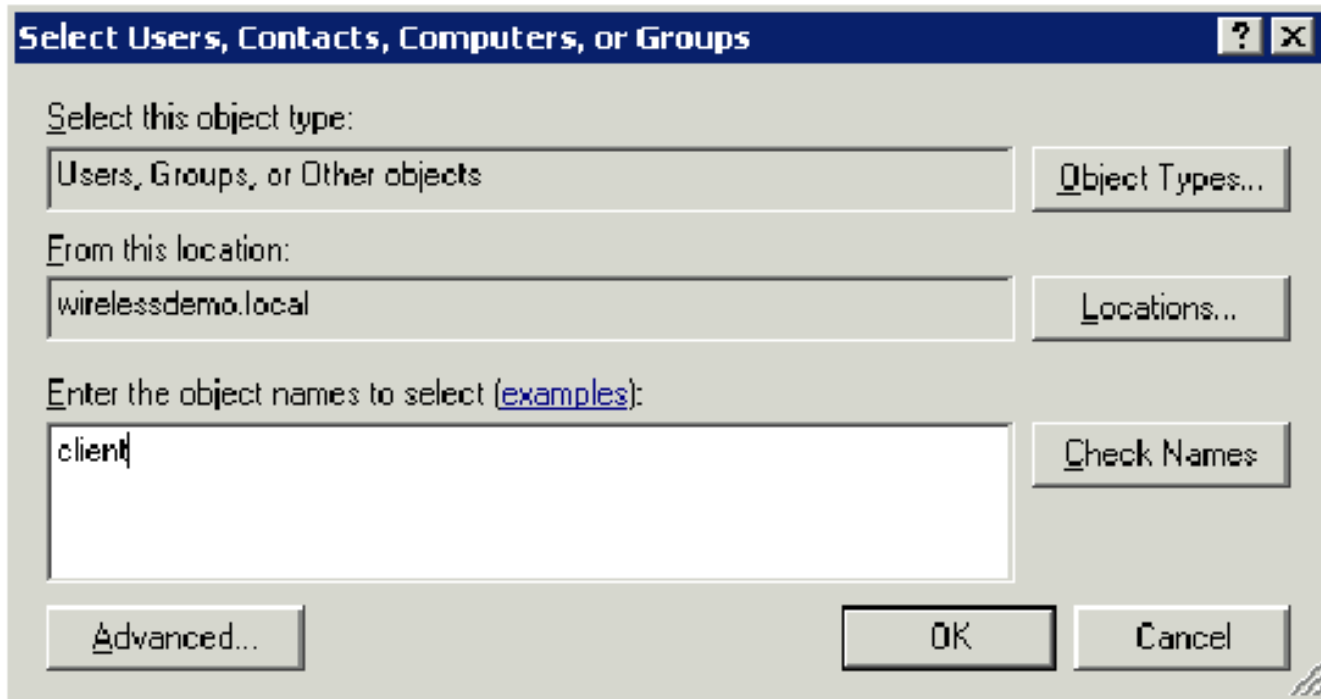


5. Klik op **OK** om wijzigingen in de groep Draadloze gebruikers op te slaan.
6. Herhaal deze procedure om meer gebruikers aan de groep toe te voegen.

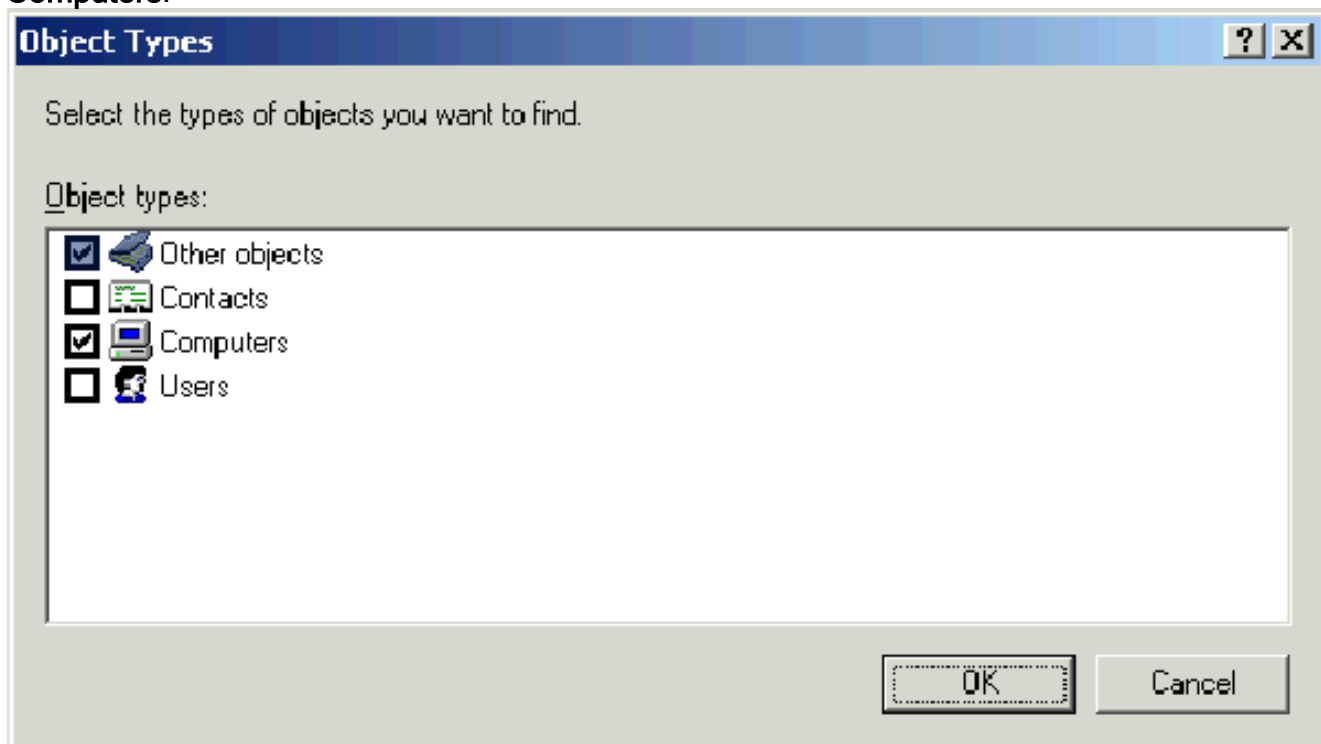
### [Stap 13: Clientcomputers aan de groep draadloze gebruikers toevoegen](#)

Voer de volgende stappen uit:

1. Herhaal stap 1 en 2 in het gedeelte [Gebruikers toevoegen aan het](#) gedeelte [Wireless-](#)gebruikersgroep van dit document
2. Typ in het dialoogvenster Gebruikers, contactgegevens of computers selecteren de naam van de computer die u aan de groep wilt toevoegen. Dit voorbeeld toont hoe de computer genoemd **client** aan de groep moet worden toegevoegd.



3. Klik op **Objecttypen**, wis het vakje **Gebruikers** en controleer **Computers**.



4. Klik twee keer op **OK**. De CLIENT-computeraccount wordt toegevoegd aan de groep draadloze gebruikers.
5. Herhaal de procedure om meer computers aan de groep toe te voegen.

## [Windows Standard 2003 Setup met Cisco Secure ACS 4.0](#)

Cisco Secure ACS is een computer waarop Windows Server 2003 met SP1, Standard Edition wordt uitgevoerd, die RADIUS-verificatie en -machtiging voor de controller biedt. Volg de procedures in deze sectie om ACS als een RADIUS-server te configureren:

### [Basisinstallatie en -configuratie](#)

Voer de volgende stappen uit:

1. Installeer Windows Server 2003 met SP1, Standard Edition, als een **ledenserver** die **ACS** in het **draadloze demo.local** domein heet. **Opmerking:** De ACS servernaam verschijnt als cisco\_w2003 in de resterende configuraties. Vervang ACS of cisco\_w2003 op de resterende labinstallatie.
2. Voor de lokale gebiedsverbinding, moet u het TCP/IP-protocol configureren met het IP-adres van **172.16.100.26**, het subnetmasker van **255.255.255.0** en het DNS-serverIP-adres van **127.0.1**.

## Cisco beveiligde ACS 4.0 installatie

**Opmerking:** Raadpleeg de [installatiehandleiding voor Cisco Secure ACS 4.0 voor Windows](#) voor meer informatie over de configuratie van Cisco Secure ACS 4.0 voor Windows.

Voer de volgende stappen uit:

1. Met behulp van een Domain Administrator-account kunt u inloggen op de computer genaamd ACS naar Cisco Secure ACS. **Opmerking:** Alleen installaties die op de computer worden uitgevoerd waar u Cisco Secure ACS installeert, worden ondersteund. Afstandsinstallaties die worden uitgevoerd met Windows Terminal Services of producten zoals Virtual Network Computing (VPN) worden niet getest en worden niet ondersteund.
2. Plaats de Cisco Secure ACS CD in een CD-ROM station op de computer.
3. Als het CD-ROM station de automatische optie van Windows ondersteunt, verschijnt Cisco Secure ACS voor Windows Server. **N.B.:** Als de computer niet het vereiste servicepakket is geïnstalleerd, verschijnt er een dialoogvenster. Windows-servicepakketten kunnen worden toegepast voor of na het installeren van Cisco Secure ACS. U kunt doorgaan met de installatie, maar het vereiste servicepakket moet worden toegepast nadat de installatie is voltooid. Anders werkt Cisco Secure ACS mogelijk niet goed.
4. Voer een van deze taken uit: Als het dialoogvenster Cisco Secure ACS voor Windows Server verschijnt, klikt u op **Installeer**. Als het dialoogvenster Cisco Secure ACS voor Windows Server niet wordt weergegeven, voert u **Setup.exe** uit, dat zich bevindt in de hoofdmap van de Cisco Secure ACS-cd.
5. Het dialoogvenster Cisco Secure ACS Setup geeft de softwarelicentieovereenkomst weer.
6. Lees de softwarelicentieovereenkomst. Als u de softwarelicentieovereenkomst accepteert, klikt u op **Accepteren**. Het dialoogvenster Welkom geeft basisinformatie over het setup-programma weer.
7. Nadat u de informatie in het dialoogvenster Welkom hebt gelezen, klikt u op **Volgende**.
8. Het dialoogvenster Voordat u met de installatie begint, toont de items die u moet voltooien voordat u doorgaat. Als u alle items hebt ingevuld die zijn opgesomd in het dialoogvenster Voordat u begint, schakelt u het bijbehorende vakje voor elk item in en klikt u op **Volgende**. **N.B.:** Als u niet alle items hebt ingevuld die in het vakje Voordat u begint, klikt u op **Annuleren** en vervolgens klikt u op **Setup**. Nadat u alle items hebt voltooid die in het dialoogvenster Voordat u begint, moet u de installatie opnieuw opstarten.
9. Het dialoogvenster Doellocatie kiezen verschijnt. Onder Destination Folder verschijnt de installatielocatie. Dit is het station en het pad waarop het setup-programma Cisco Secure ACS installeert.
10. Als u de installatielocatie wilt wijzigen, voert u de volgende stappen uit: Klik op **Bladeren**. Het

dialogoogvenster Map kiezen verschijnt. Het vakje Pad bevat de installatielocatie. Verander de installatielocatie. U kunt de nieuwe locatie in het Pad-vak typen of de lijsten Drives en Directories gebruiken om een nieuw station en een nieuwe map te selecteren. De installatielocatie moet zich op een lokaal station naar de computer bevinden. **Opmerking:** specificeer geen pad dat een procent teken bevat, "%". Als u dit wel doet, verschijnt de installatie mogelijk op de juiste manier maar niet goed voordat deze voltooid is. Klik op **OK**. **N.B.:** Als u een map hebt opgegeven die niet bestaat, wordt in het setup-programma een dialogoogvenster weergegeven om te bevestigen dat de map is gemaakt. Klik op **Ja** om verder te gaan.

11. In het dialogoogvenster Doellocatie kiezen verschijnt de nieuwe installatielocatie onder Map doelmap.
12. Klik op **Volgende**.
13. Het dialogoogvenster Configuration van de verificatiedatabase bevat opties voor het authenticeren van gebruikers. U kunt alleen authenticeren met de Cisco Secure-gebruikersdatabase, of ook met een Windows-gebruikersdatabase. **Opmerking:** Nadat u Cisco Secure ACS hebt geïnstalleerd, kunt u de authenticatie ondersteuning configureren voor alle externe gebruikers database types naast Windows gebruikersdatabases.
14. Als u gebruikers alleen met de Cisco Secure-gebruikersdatabase wilt authenticeren, kiest u de **optie Alleen Cisco Secure ACS-database controleren**.
15. Als u gebruikers wilt authenticeren met een Windows Security Access Manager (SAM) gebruikersdatabase of een Active Directory-gebruikersdatabase naast de Cisco Secure-gebruikersdatabase, Voltooi de volgende stappen: Kies de optie **Ook de Windows-gebruikersdatabase controleren**. Het aanvinkvakje "Toekenning van de toestemming aan gebruiker" wordt aangevinkt. **Opmerking:** Ja, raadpleeg de instellingsoptie "Toekenning van inbeltoestemming aan gebruiker" is van toepassing op alle vormen van toegang die worden gecontroleerd door Cisco Secure ACS, niet alleen inbeltoegang. Een gebruiker die het netwerk via een VPN-tunnel opzoekt, voert bijvoorbeeld geen netwerktoegangsserver in. Als **Ja** echter, verwijst u naar het instellingsvenster "Toekenning van inbeltoestemming aan gebruiker", dan past Cisco Secure ACS de inbelrechten van Windows toe om te bepalen of de gebruiker toegang tot het netwerk kan worden verleend. Als u toegang tot gebruikers wilt toestaan die voor authentiek zijn verklaard door een gegevensbestand van de domeingebruiker van Windows slechts wanneer zij inbeltoestemming in hun rekening van Windows hebben, zie **Ja**, "Toekenning de instelvenster van de "Toekenning aan gebruiker" controleren.
16. Klik op **Volgende**.
17. Het setup-programma installeert Cisco Secure ACS en werkt de Windows-registratie bij.
18. Het dialogoogvenster Geavanceerde opties toont verschillende functies van Cisco Secure ACS die standaard niet ingeschakeld zijn. Raadpleeg de [gebruikersgids](#) voor [Cisco Secure ACS voor Windows Server, versie 4.0](#) voor meer informatie over deze functies. **Opmerking:** de vermelde functies verschijnen alleen in de Cisco Secure ACS HTML-interface als u ze toestaat. Na de installatie kunt u deze optie in- of uitschakelen op de pagina Geavanceerde opties in het gedeelte Interface Configuration.
19. Schakel het bijbehorende vakje in voor elke optie die u wilt inschakelen.
20. Klik op **Volgende**.
21. Het dialogoogvenster Active Service Monitoring verschijnt. **N.B.:** Na de installatie kunt u de actieve functies voor servicecontrole configureren op de pagina Active Service Management in het vak Systeemconfiguratie.
22. Als u wilt dat Cisco Secure ACS de gebruikersverificatieservices controleert, controleert u

het vakje **Aanmelden** inschakelen. Kies in de lijst Script de optie die u wilt toepassen in het geval van een fout in de verificatieservice: **Geen eenvoudige Actie**-Cisco Secure ACS voert geen script uit. **N.B.:** Deze optie is handig als u berichten per gebeurtenis activeert. **Herstart**-Cisco Secure ACS voert een script uit dat de computer herstart die Cisco Secure ACS runt. **Start alle**-Cisco Secure ACS opnieuw op alle Cisco beveiligde ACS-services. **Start RADIUS/TACACS+**—Cisco Secure ACS opnieuw start alleen de RADIUS- en TACACS+-services.

23. Als u wilt dat Cisco Secure ACS een e-mailbericht verzenden wanneer service-controle een gebeurtenis detecteert, schakelt u het vakje **Mail** notification in.
24. Klik op **Volgende**.
25. Het dialoogvenster Wachtwoord voor encryptie van database verschijnt. **Opmerking:** Het Wachtwoord voor encryptie van databases is versleuteld en opgeslagen in het ACS-register. Mogelijk moet u dit wachtwoord opnieuw gebruiken wanneer er zich kritieke problemen voordoen en de database handmatig moet worden geopend. Houd dit wachtwoord ter beschikking zodat Technische ondersteuning toegang tot de database kan krijgen. Het wachtwoord kan worden gewijzigd tijdens elke verloopperiode.
26. Voer een wachtwoord in voor gegevenscodering. Het wachtwoord moet minimaal acht tekens lang zijn en moet zowel tekens als cijfers bevatten. Er zijn geen ongeldige tekens. Klik op **Volgende**.
27. Het setup-programma is voltooid en het dialoogvenster Cisco Secure ACS-service initiatie verschijnt.
28. Voor elke gewenste optie van Cisco Secure ACS Services Initiation controleert u het bijbehorende vakje. De acties die met de opties zijn verbonden, worden uitgevoerd nadat het setup-programma is voltooid. **Ja, ik wil de Cisco Secure ACS Service nu starten** - Start de Windows services die Cisco Secure ACS vormen. Als u deze optie niet selecteert, is de Cisco Secure ACS HTML-interface niet beschikbaar tenzij u de computer opnieuw start of de CSAdmin-service start. **Ja, ik wil dat de instelling de Cisco Secure ACS-beheerder vanuit mijn browser start na installatie** - opent de Cisco Secure ACS HTML-interface in de standaard webbrowser voor de huidige Windows-gebruikersaccount. **Ja, ik wil het leesmij bestand bekijken** - opent het README.TXT-bestand in Windows-toetsenbord.
29. Klik op **Volgende**.
30. Als u een optie hebt geselecteerd, wordt de Cisco Secure ACS-services gestart. Het dialoogvenster Complete installatie toont informatie over de Cisco Secure ACS HTML-interface.
31. Klik op **Voltooien**. **Opmerking:** de rest van de configuratie is gedocumenteerd onder het hoofdstuk voor het MAP-type dat is ingesteld.

## [Configuratie van Cisco LWAPP-controllers](#)

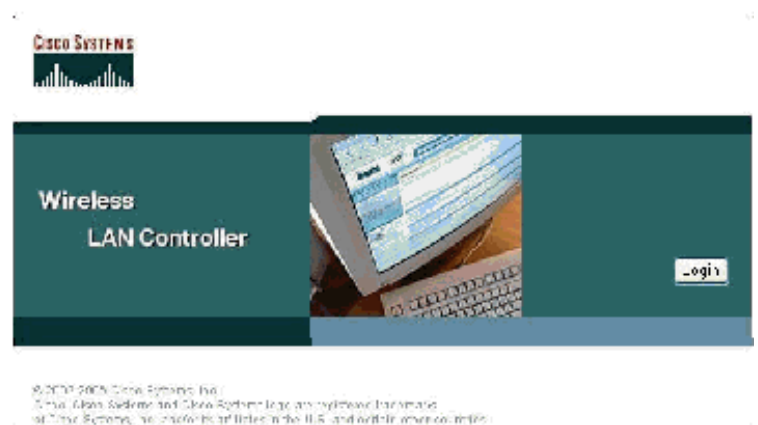
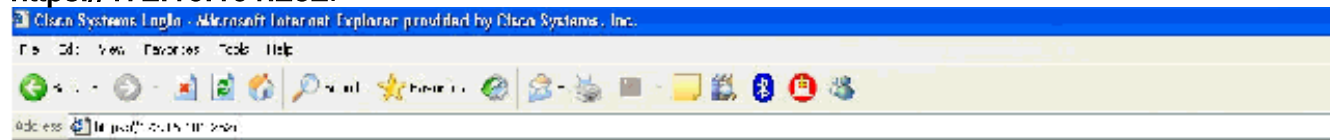
### [De gewenste configuratie voor WAP2/WAP maken](#)

Voer de volgende stappen uit:

**Opmerking:** De veronderstelling is dat de controller een basisverbinding heeft met het netwerk en IP bereikbaarheid op de beheerinterface.

1. Meld u aan bij de controller door te bladeren naar

<https://172.16.101.252>



2. Klik op **Aanmelden**.
3. Aanmelden met de standaardinstelling van de **gebruikershandleiding** en de standaardinstelling van het wachtwoord.
4. Maak de interface-VLAN-afbeelding onder het menu Controller.
5. Klik op **Interfaces**.
6. Klik op **New** (Nieuw).
7. In het veld Interfacenaam type **werknemer**. (Dit veld kan elke waarde zijn die u wilt.)
8. In het veldtype VLAN ID **20**. (Dit veld kan elk VLAN zijn dat in het netwerk wordt meegevoerd.)
9. Klik op **Apply** (Toepassen).
10. Configuratie van de informatie zoals deze interfaces > venster Bewerken toont.

Back Search Favorites

Address: https://172.16.101.252/screens/frameset.html

CISCO SYSTEMS

MONITOR WLANs CONTROLLER WIRELESS SECURITY

Controller

General

Inventory

Interfaces

Internal DHCP Server

Mobility Management

Mobility Groups

Mobility Statistics

Ports

Master Controller Mode

Network Time Protocol

QoS Profiles

Interfaces > Edit

General Information

Interface Name employee

Interface Address

VLAN Identifier 20

IP Address 172.16.100.1

Netmask 255.255.255.0

Gateway 172.16.100.1

Physical Information

Port Number 1

DHCP Information

Primary DHCP Server 172.16.100.25

Secondary DHCP Server 0.0.0.0

Access Control List

ACL Name none

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

11. Klik op **Apply** (Toepassen).
12. Klik op **WLAN**.
13. Klik op **New** (Nieuw).
14. In het WLAN SSID veldtype **werknemer**.
15. Klik op **Apply** (Toepassen).
16. Configureer de informatie zoals dit WLAN's > venster Bewerken toont. **Opmerking:** WAP2 is de gekozen Layer 2 encryptie methode voor dit lab. Om WAP met TKIP-MIC klanten toe te staan om aan deze SSID te associëren, kunt u ook de **compatibiliteitsmodus** voor WPP controleren en **WAP2 TKIP-clients toestaan** of de clients die de 802.11i AES-encryptie niet ondersteunen.



## WLANs > Edit

<b>WLAN ID</b>	1
<b>WLAN SSID</b>	Employee

### General Policies

Radius Policy	All
Admin Status	<input checked="" type="checkbox"/> Enabled
Session Timeout (secs)	1800
Quality of Services (QoS)	Silver (best effort)
WMM Policy	Disabled
7920 Pkts Support	<input type="checkbox"/> Client CAC Limit <input type="checkbox"/> AP CAC Limit
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
Allow PPP Override	<input type="checkbox"/> Enabled
Client Exclusion	<input checked="" type="checkbox"/> Enabled ** 60 Timeout Value (secs)
DHCP Server	<input type="checkbox"/> Override
DHCP Addr. Assignment	<input checked="" type="checkbox"/> Required
Interface Name	employee

### Security Policies

Layer 2 Security	WPA2
	<input type="checkbox"/> MAC Filtering
Layer 3 Security	None
	<input type="checkbox"/> Web Policy **

\* Web Policy cannot be used in combination with IPsec and L2TP.

\*\* When client exclusion is enabled, a timeout value of zero means infinity (will require administrative override to reset excluded clients)

### Radius Servers

	Authentication Servers	Accounting Servers
Server 1	IP:172.16.100.25, Port:1812	none
Server 2	none	none
Server 3	none	none

### WPA2 Parameters

WPA Compatibility Mode	<input checked="" type="checkbox"/> Enable
Allow WPA2 TKIP Clients	<input checked="" type="checkbox"/> Enable
Pre-Shared Key	<input type="checkbox"/> Enabled (WPA2 passphrase has been set)

17. Klik op **Apply** (Toepassen).
18. Klik op het menu **Beveiliging** en voeg de RADIUS-server toe.
19. Klik op **New** (Nieuw).
20. Voeg het IP-adres van de RADIUS-server (172.16.100.25) toe, dat de ACS-server eerder is geconfigureerd.
21. Zorg ervoor dat de gedeelde toets overeenkomt met de AAA-client die in de ACS-server is ingesteld.
22. Klik op **Apply** (Toepassen).



## Security

### AAA

- General
- RADIUS Authentication
- RADIUS Accounting
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies

### Access Control Lists

### Web Auth Certificate

### Wireless Protection Policies

- Trusted AP Policies
- Rogue Policies
- Standard Signatures
- Custom Signatures
- Client Exclusion Policies
- AP Authentication

## RADIUS Authentication Servers > New

<b>Server Index (Priority)</b>	1 <input type="button" value="v"/>
<b>Server IP Address</b>	<input type="text" value="172.16.100.25"/>
<b>Keys Format</b>	ASCII <input type="button" value="v"/>
<b>Shared Secret</b>	<input type="password" value="••••••"/>
<b>Confirm Shared Secret</b>	<input type="password" value="••••••"/>
<b>Key Wrap</b>	<input type="checkbox"/>
<b>Port Number</b>	<input type="text" value="1812"/>
<b>Server Status</b>	Enabled <input type="button" value="v"/>
<b>Support for RFC 3576</b>	Enabled <input type="button" value="v"/>
<b>Retransmit Timeout</b>	<input type="text" value="2"/> seconds
<b>Network User</b>	<input checked="" type="checkbox"/> Enable
<b>Management</b>	<input type="checkbox"/> Enable

23. De basisconfiguratie is nu voltooid en u kunt beginnen met het testen van de EAP-TLS.

## [EAP-TLS-verificatie](#)

Voor de verificatie van het MAP-TLS zijn computercertificaten en gebruikerscertificaten op de draadloze client nodig, de toevoeging van EAP-TLS als een MAP-type aan het toegangsbeleid op afstand voor draadloze toegang, en een herconfiguratie van de draadloze netwerkverbinding.

Om DC\_CA te vormen om auto-inschrijving voor computer en gebruikerscertificaten te verstrekken, vul de procedures in deze sectie in.

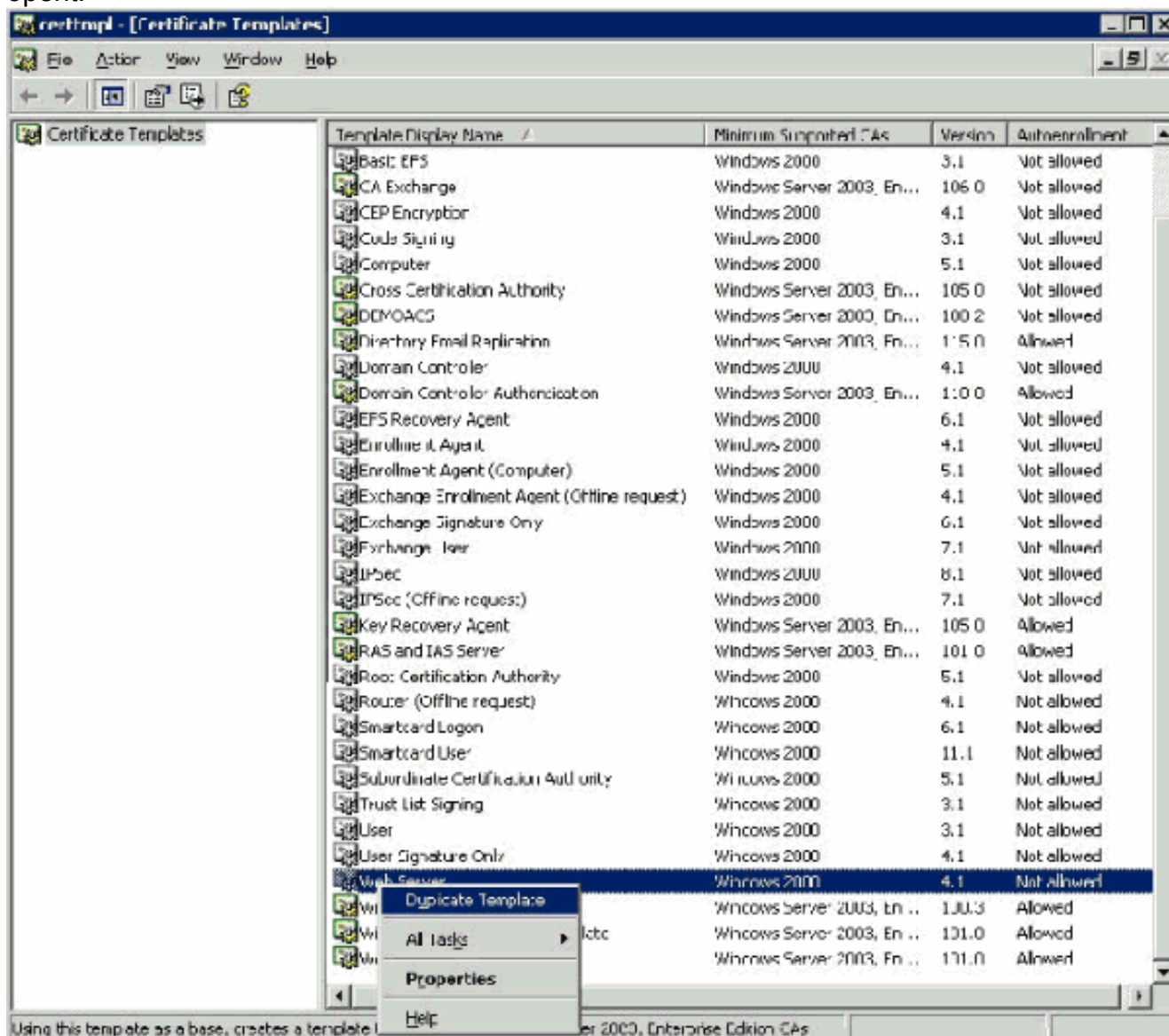
**Opmerking:** Microsoft heeft de sjabloon voor web servers gewijzigd met de release van Windows 2003 Enterprise CA, zodat de toetsen niet langer geëxporteerd kunnen worden en de optie uitgerijnd is. Er zijn geen andere certificaatsjablonen die bij certificatie diensten worden geleverd en die bedoeld zijn voor serververificatie en de mogelijkheid bieden om sleutels als exportbaar te markeren die in de vervolkeuzelijst beschikbaar zijn, zodat u een nieuwe sjabloon moet maken die dit wel doet.

**Opmerking:** Windows 2000 maakt het mogelijk om voor export geschikte toetsen in te schakelen en deze procedures hoeven niet te worden gevolgd als u Windows 2000 gebruikt.

## [Installeer de sjablonen van het certificaat magnetisch in](#)

Voer de volgende stappen uit:

1. Kies **Start > Uitvoeren**, type **mmc** en klik op **OK**.
2. Klik in het menu Bestand op **Toevoegen/verwijderen Magnetisch-in** en klik vervolgens op **Toevoegen**.
3. Dubbelklik onder Magnetisch in op **certificaatsjablonen**, klik op **Sluiten** en klik vervolgens op **OK**.
4. Klik in de console-boom op **certificaatsjablonen**. Alle certificaatsjablonen verschijnen in het deelvenster met details.
5. Om stap 2 door 4 te omzeilen, typt **certtmpl.msc**, die de sjablonen van het certificaat magnetisch-in opent.



## [De certificaatsjabloon voor de ACS-webserver maken](#)

Voer de volgende stappen uit:

1. Klik in het deelvenster Details van de sjablonen voor certificaten op de sjabloon van de **webserver**.
2. Klik in het menu Actie op **Dubbele sjabloon**.

**Properties of New Template** [?] [X]

Issuance Requirements | Superseded Templates | Extensions | Security

General | Request Handling | Subject Name

Template display name:  
Copy of Web Server

Minimum Supported CAs: Windows Server 2003, Enterprise Edition

After you apply changes to this tab, you can no longer change the template name.

Template name:  
Copy of Web Server

Validity period: 2 years  
Renewal period: 6 weeks

Publish certificate in Active Directory  
 Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply

3. Typ in het veld Naam van de sjabloon de **naam**

**Properties of New Template** [?] [X]

Issuance Requirements | Superseded Templates | Extensions | Security

General | **Request Handling** | Subject Name

Template display name:  
[ACS]

Minimum Supported CAs: Windows Server 2003, Enterprise Edition

After you apply changes to this tab, you can no longer change the template name.

Template name:  
[ACS]

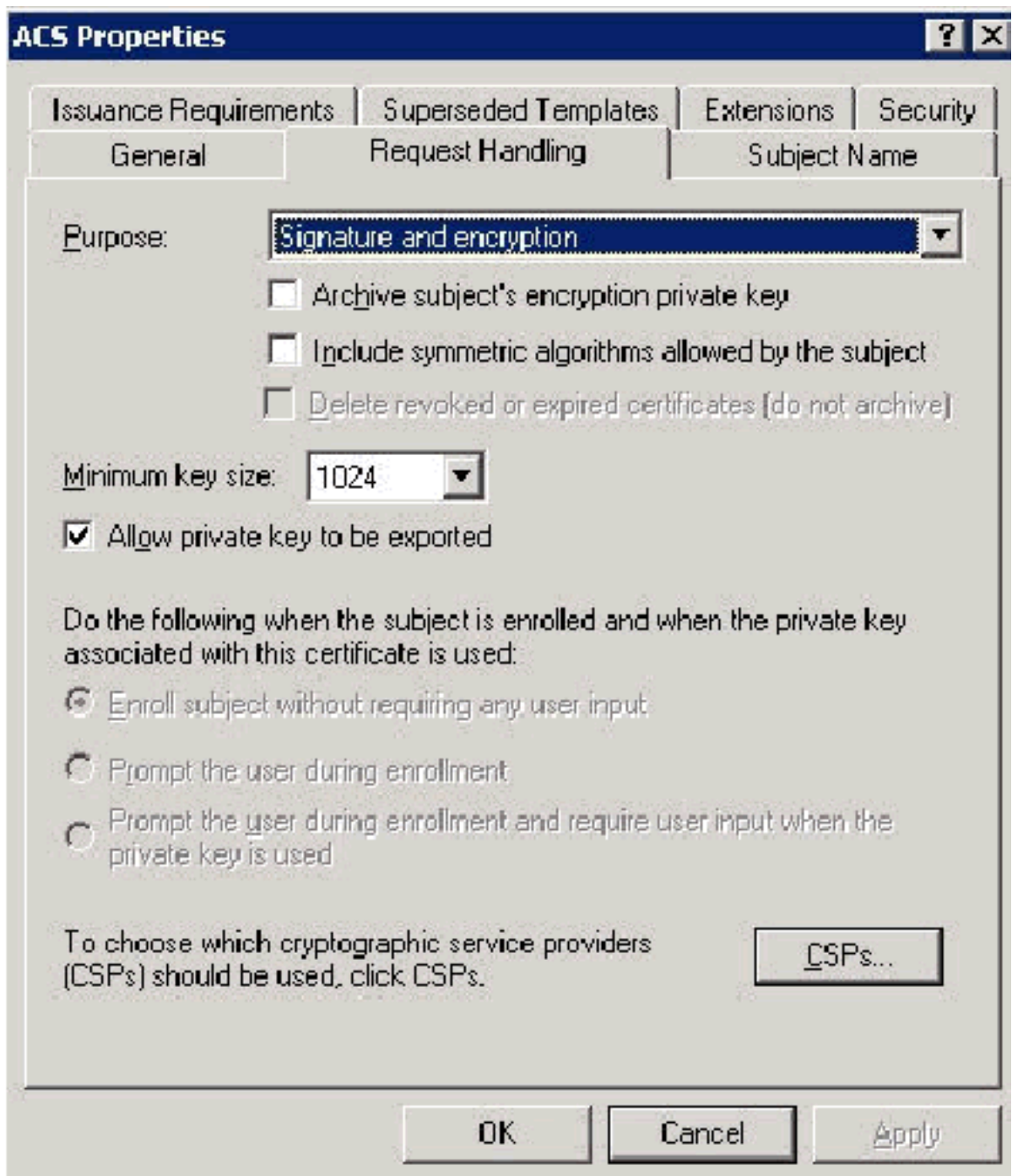
Validity period: [ 2 ] years [▼]      Renewal period: [ 6 ] weeks [▼]

Publish certificate in Active Directory  
     Do not automatically reenroll if a duplicate certificate exists in Active Directory

[ OK ] [ Cancel ] [ Apply ]

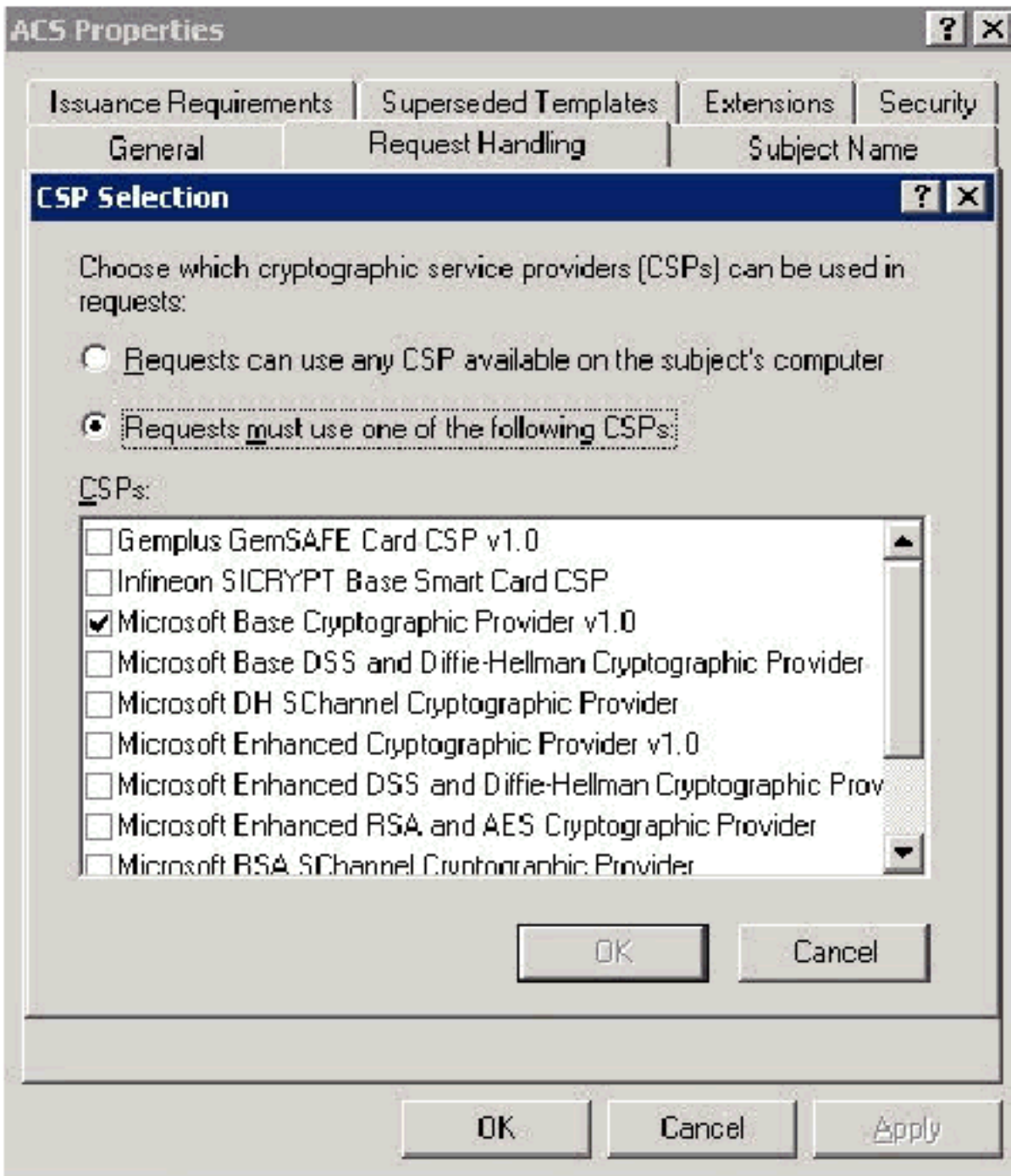
ACS.

4. Ga naar het tabblad Handling aanvragen en controle **Laat privé-toets geëxporteerd**



worden.

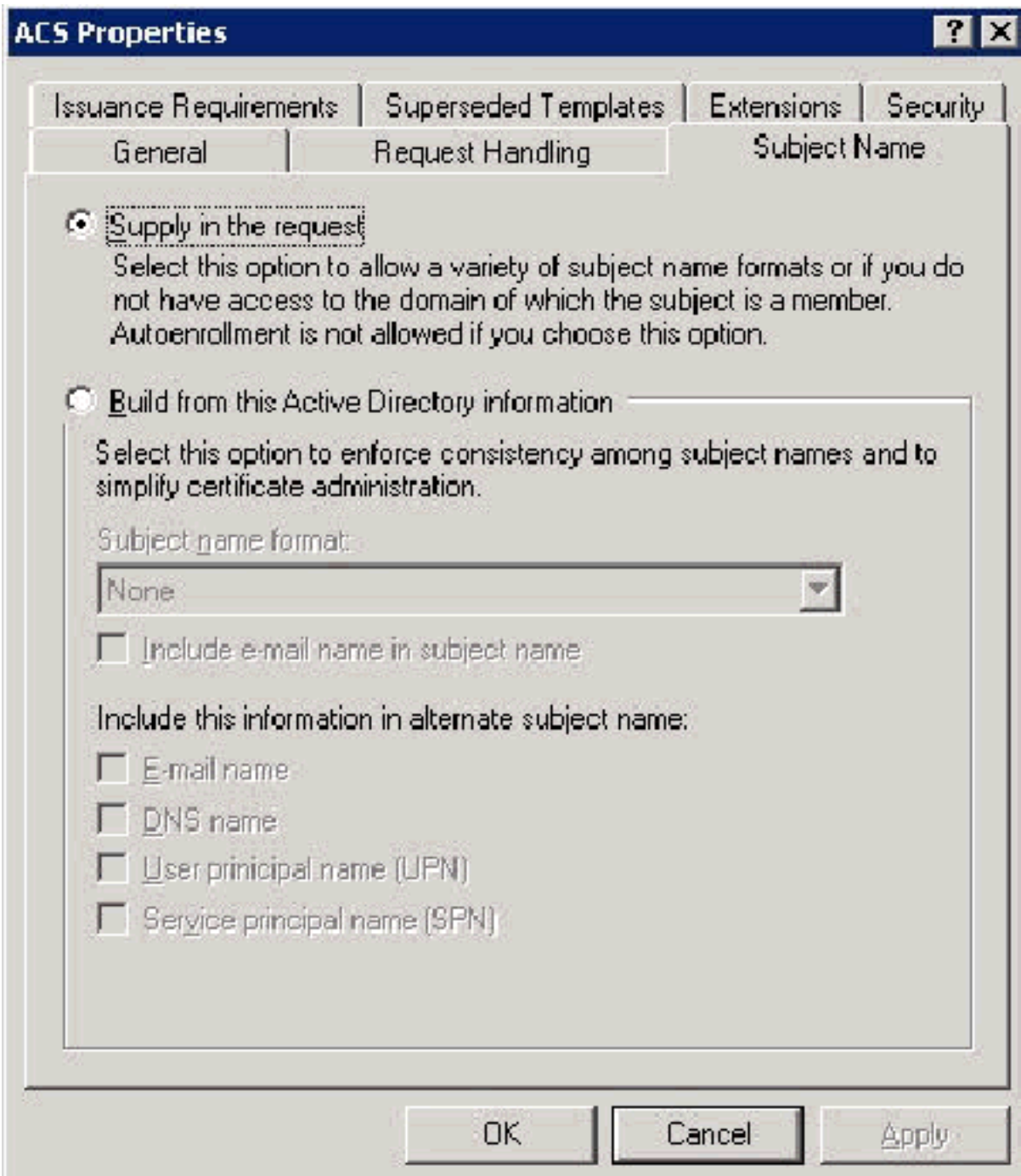
5. Kies de aanvragen moeten een van de volgende CSP's gebruiken en Microsoft Base Cryptographic Provider v1.0 controleren. Controleer alle andere CSP's die zijn afgevinkt en klik vervolgens op



OK.

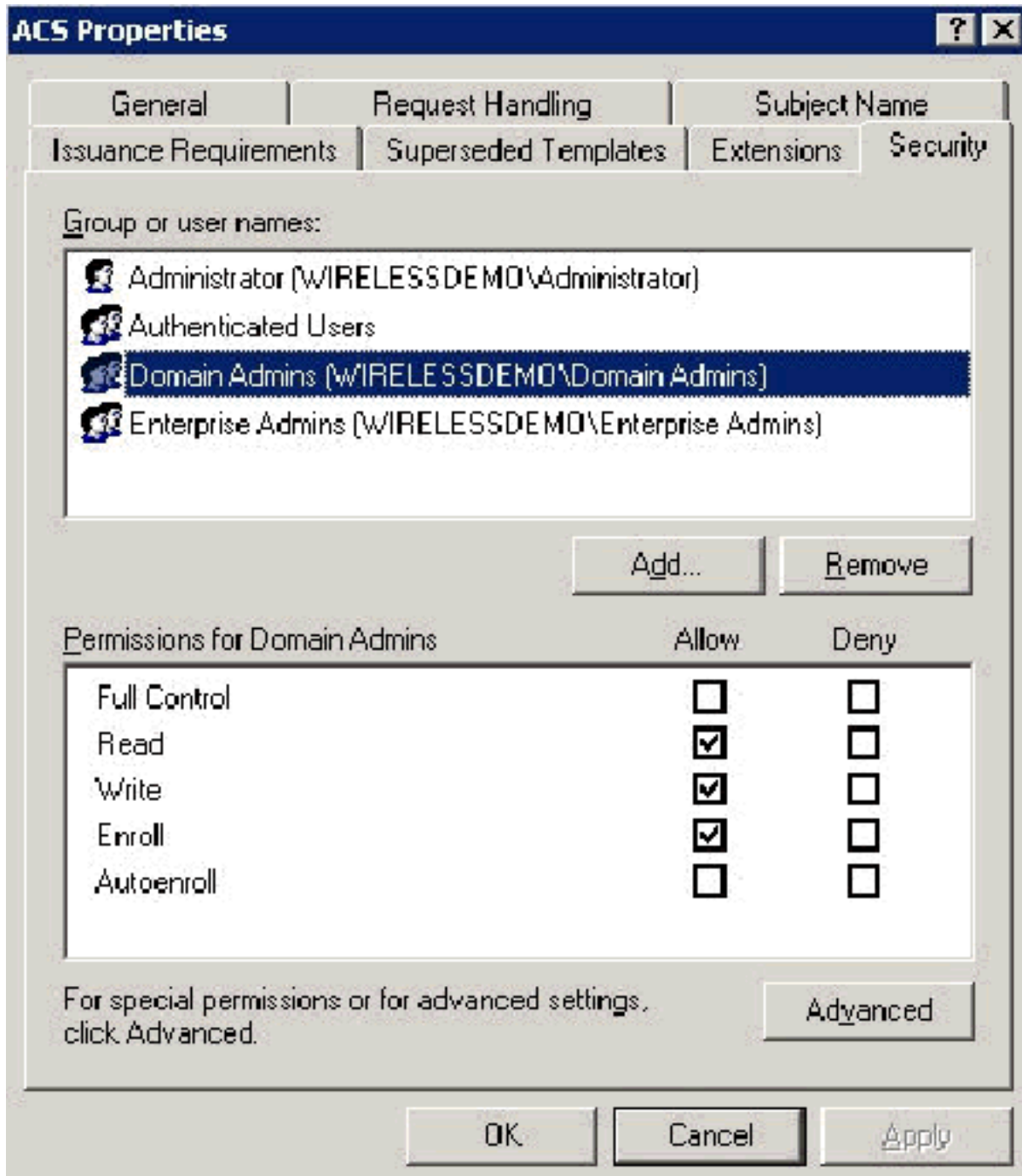
6. Ga naar het tabblad Onderwerp, kies **Levering in het verzoek** en klik op





OK.

7. Ga naar het tabblad Security om de groep **Domain Admins** te markeren en zorg ervoor dat de optie **Enroll** onder Toegestaan controle is. **Belangrijk:** Als u ervoor kiest om alleen van deze Active Directory-informatie te maken, controleert u de naam van de gebruiker (UPN) en verwijdert u de naam van e-mail in de naam Onderwerp en e-mailnaam omdat er geen e-mailnaam is ingevoerd voor de account van de draadloze gebruiker in de actieve map Gebruikers en computers. Als u deze twee opties niet uitschakelt, probeert u automatisch e-mail te gebruiken, wat leidt tot een fout in de automatische inschrijving.



8. Indien nodig zijn er aanvullende veiligheidsmaatregelen om te voorkomen dat certificaten automatisch worden uitgewezen. Deze zijn te vinden op het tabblad Uitgifte-vereisten. Dit wordt in dit document niet verder besproken.

**ACS Properties** [?] [X]

General | Request Handling | Subject Name  
 Issuance Requirements | Superseded Templates | Extensions | Security

Require the following for enrollment:

CA certificate manager approval

This number of authorized signatures:

If you require more than one signature, autoenrollment is not allowed.

Policy type required in signature:

Application policy:

Issuance policies:  
 Add... Remove

Require the following for reenrollment:

Same criteria as for enrollment

Valid existing certificate

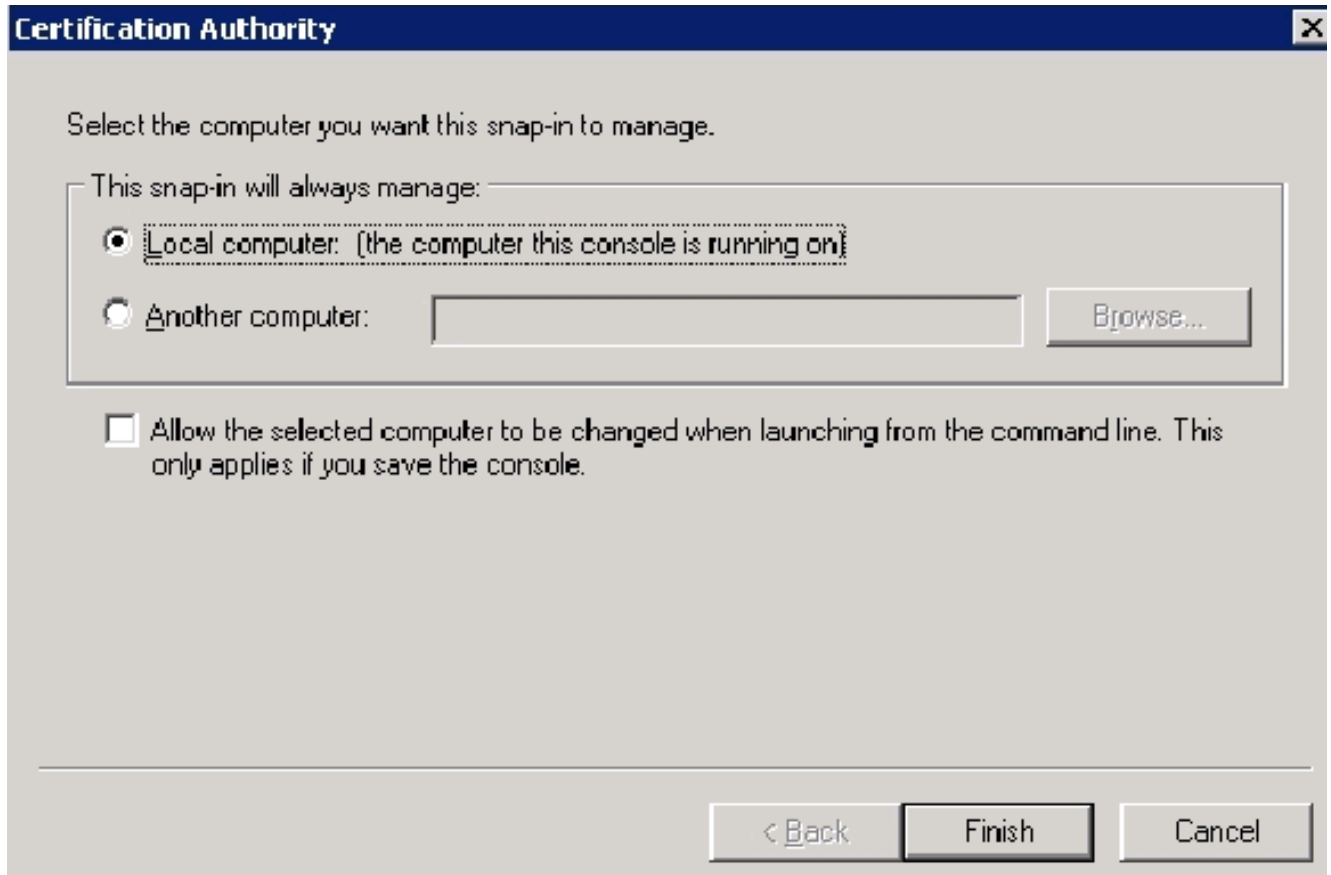
OK Cancel Apply

9. Klik op **OK** om de sjabloon op te slaan en deze sjabloon uit te geven door de certificaatinstantie ingebroken.

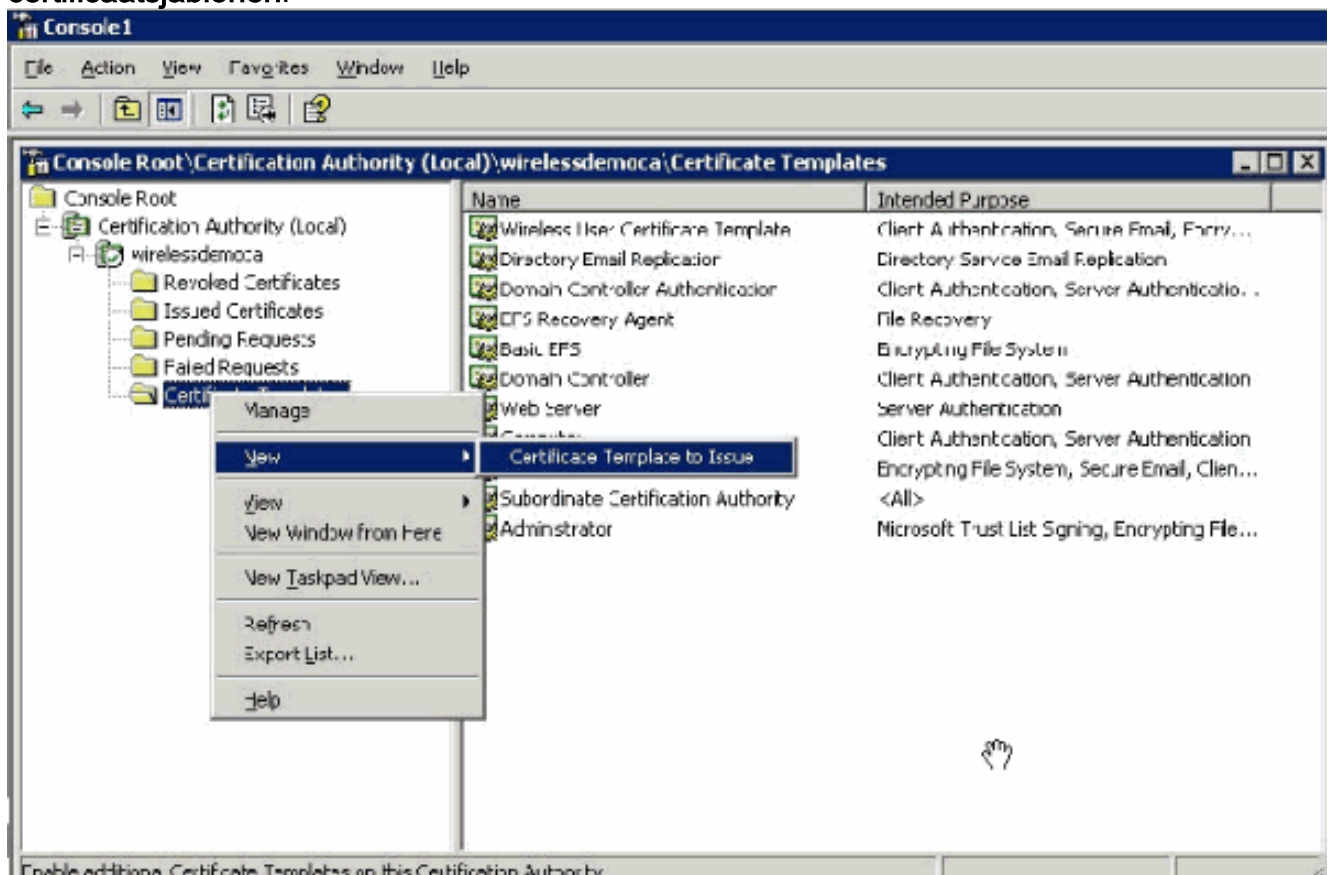
## [De nieuwe ACS-webservercertificaatsjabloon inschakelen](#)

Voer de volgende stappen uit:

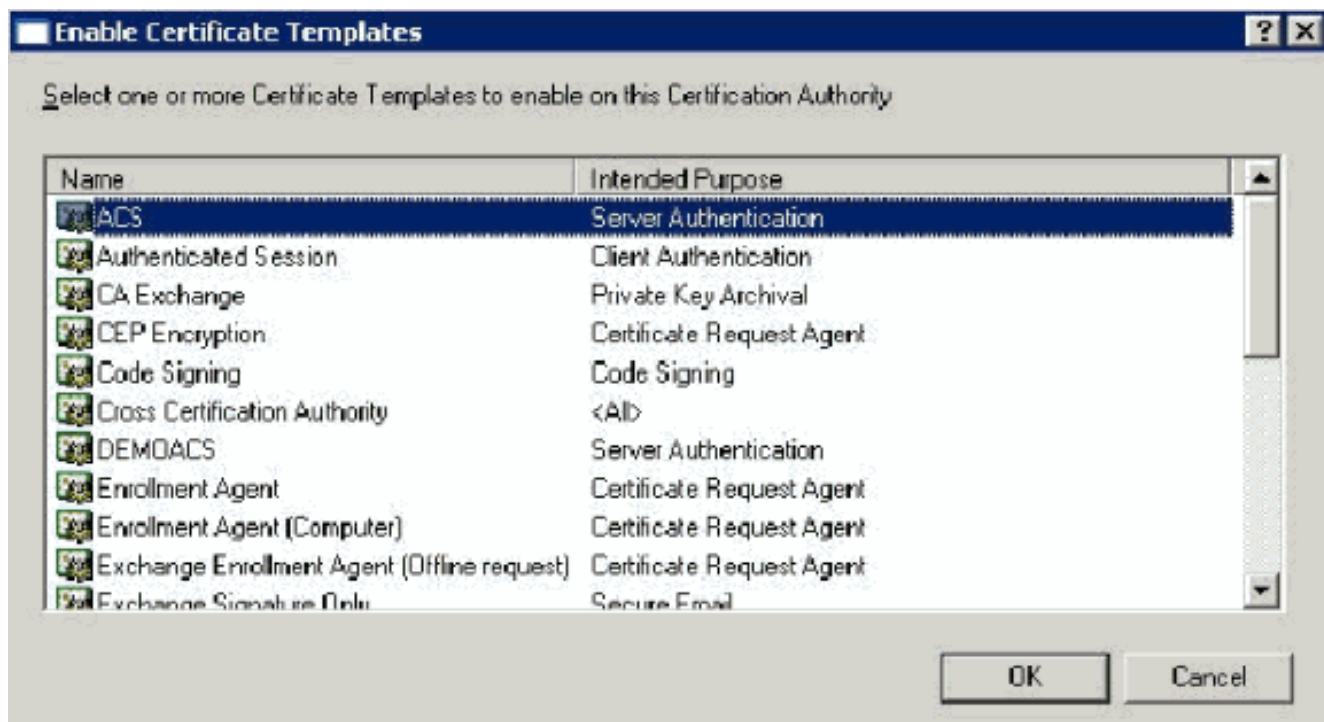
1. Open de ingebouwde **certificeringsinstantie**. Volg stap 1-3 in het gedeelte [Certificaatsjabloon maken voor de](#) sectie [ACS-webserver](#), kies de optie **certificaatinstantie**, kies **lokale computer** en klik op **Voltooien**.



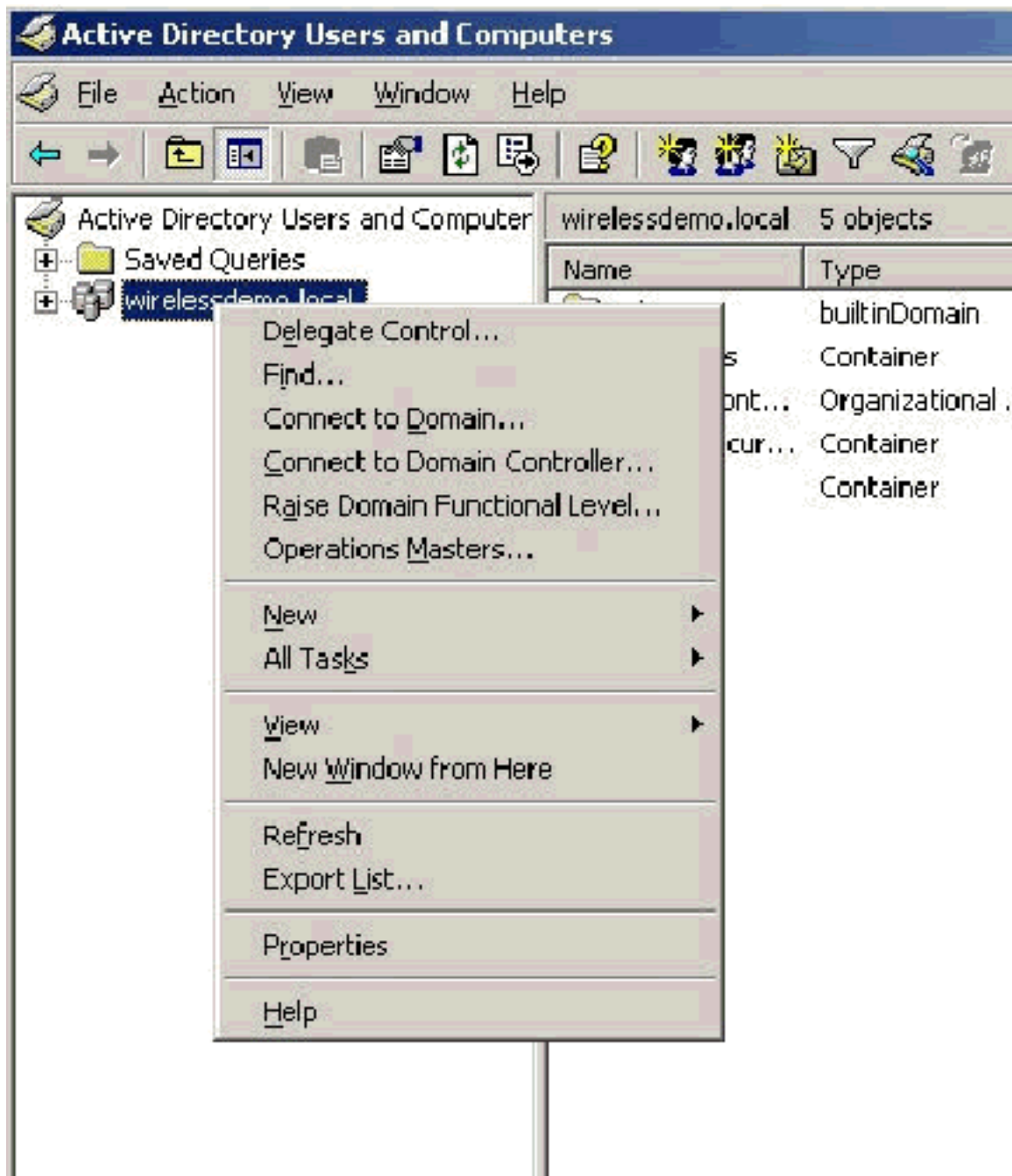
- In de console boom, **breid draadloze democra uit**, en klik dan met de rechtermuisknop **certificaatsjablonen**.



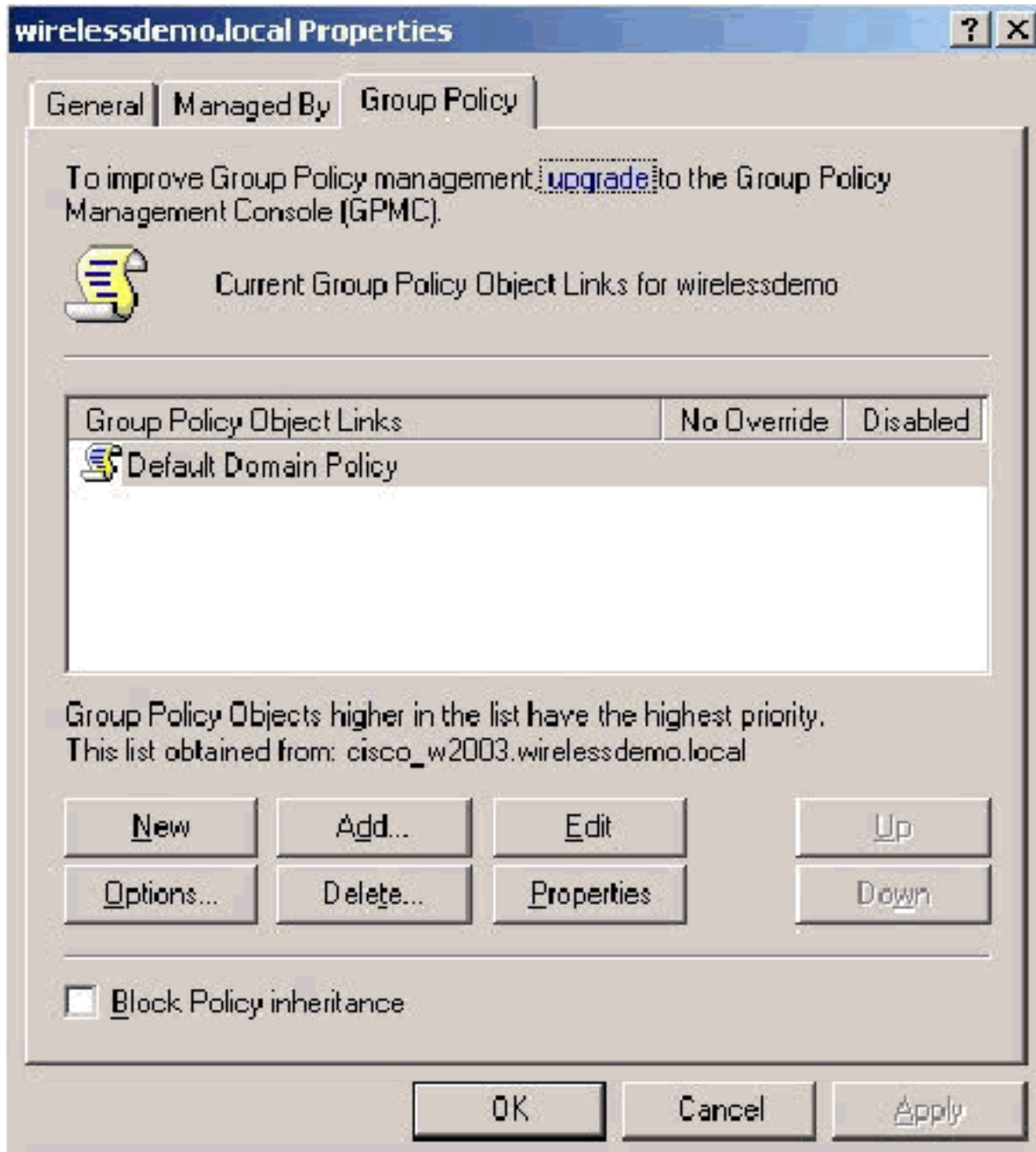
- Kies **Nieuw > certificaatsjabloon voor afgifte**.
- Klik op de **ACS-**certificaatsjabloon.



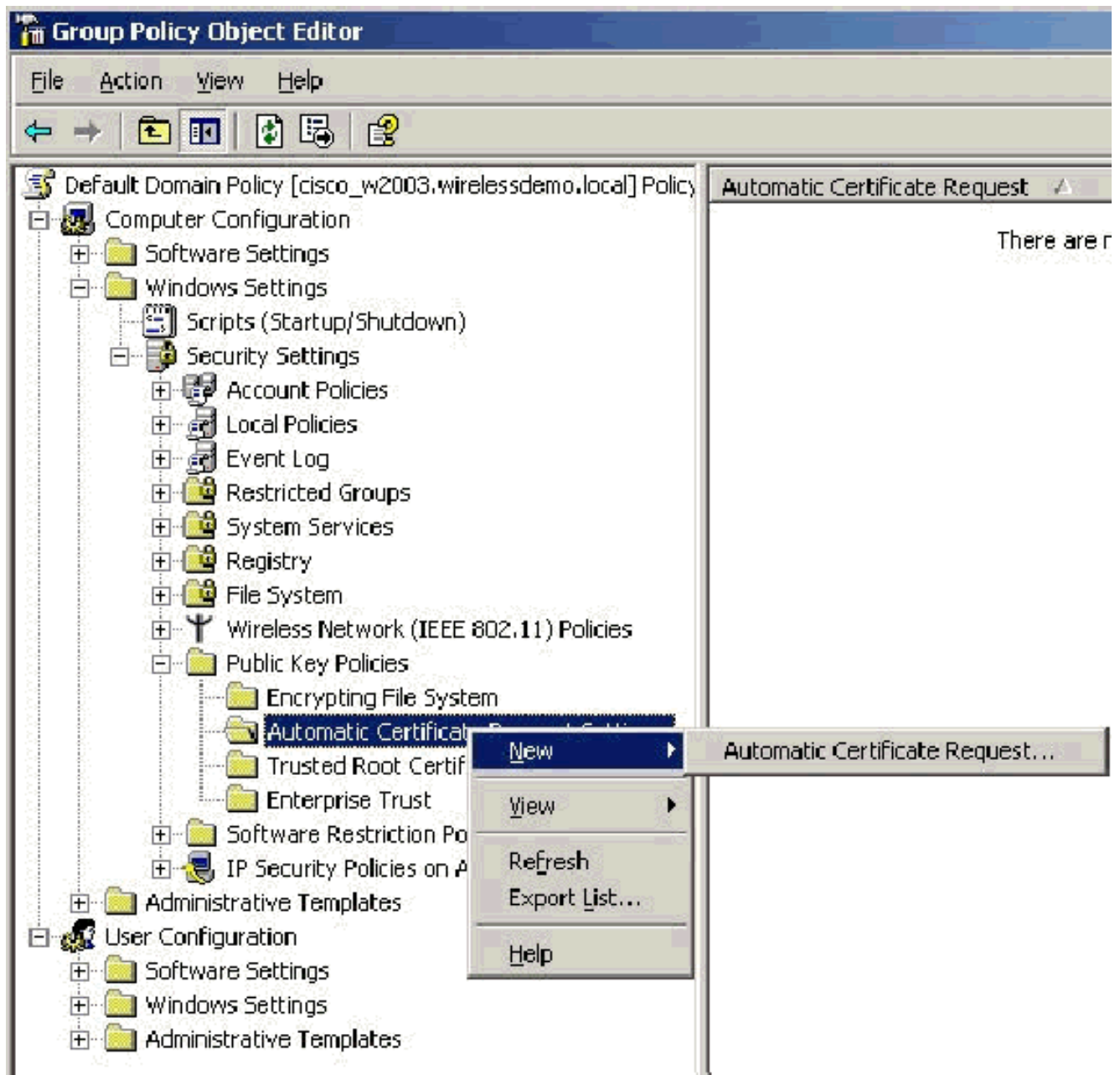
5. Klik op **OK** en open de optie **Actieve gebruikers en computers** in de map.
6. In de console boom, dubbelklik op **Actieve Gebruikers en Computers** van de **Map**, klik met de rechtermuisknop op het lokale domein **Wireless.demo** en klik vervolgens op **Eigenschappen**.



7. Klik in het tabblad Groepsbeleid op **Standaardbeleid voor domein** en vervolgens op **Bewerken**. Dit opent de editor voor groepsbeleid.

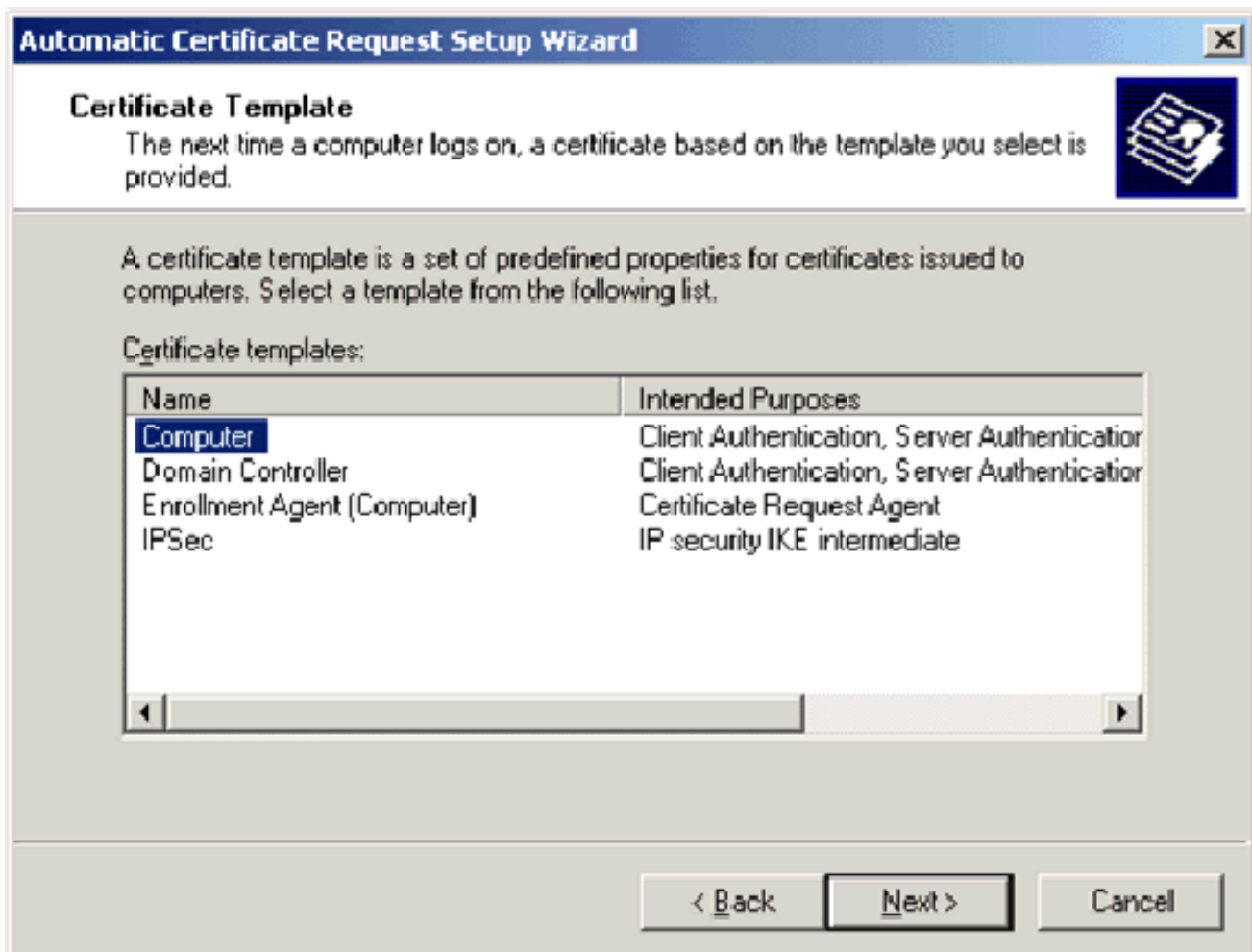


8. Wilt u in de console-boom **Computer Configuration > Windows Settings > Security Settings > Public Key Policies** uitvouwen, en vervolgens de optie **Automatisch certificaataanvraag** selecteren.

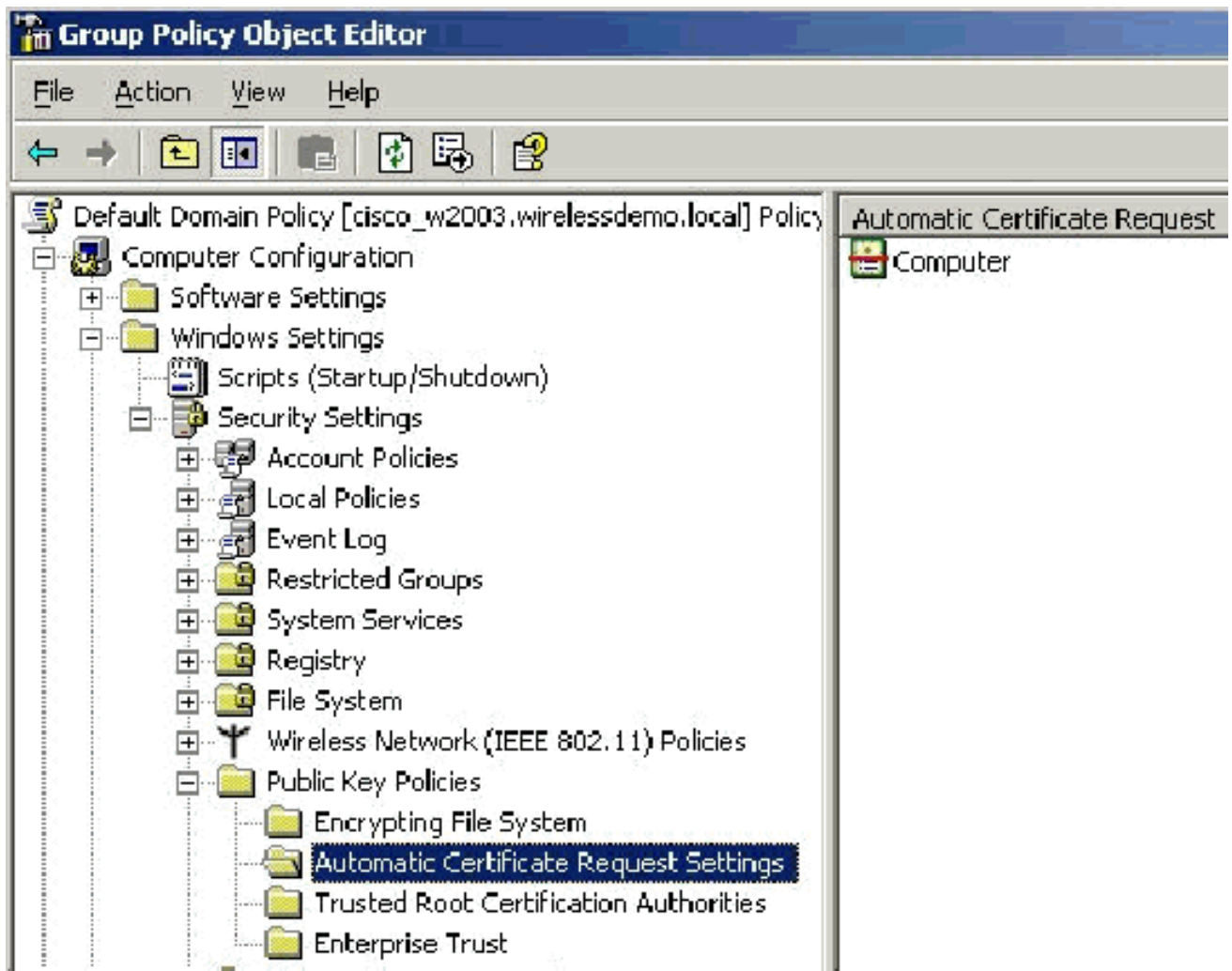


9. Klik met de rechtermuisknop op **Instellingen automatische certificaataanvraag** en kies **Nieuw > Automatisch certificaataanvraag**.
10. Klik op **Volgende** op de pagina Welkom bij de wizard Automatisch certificaataanvraag instellen.
11. Klik in de pagina certificaatsjabloon op **Computer** en klik op **Volgende**.

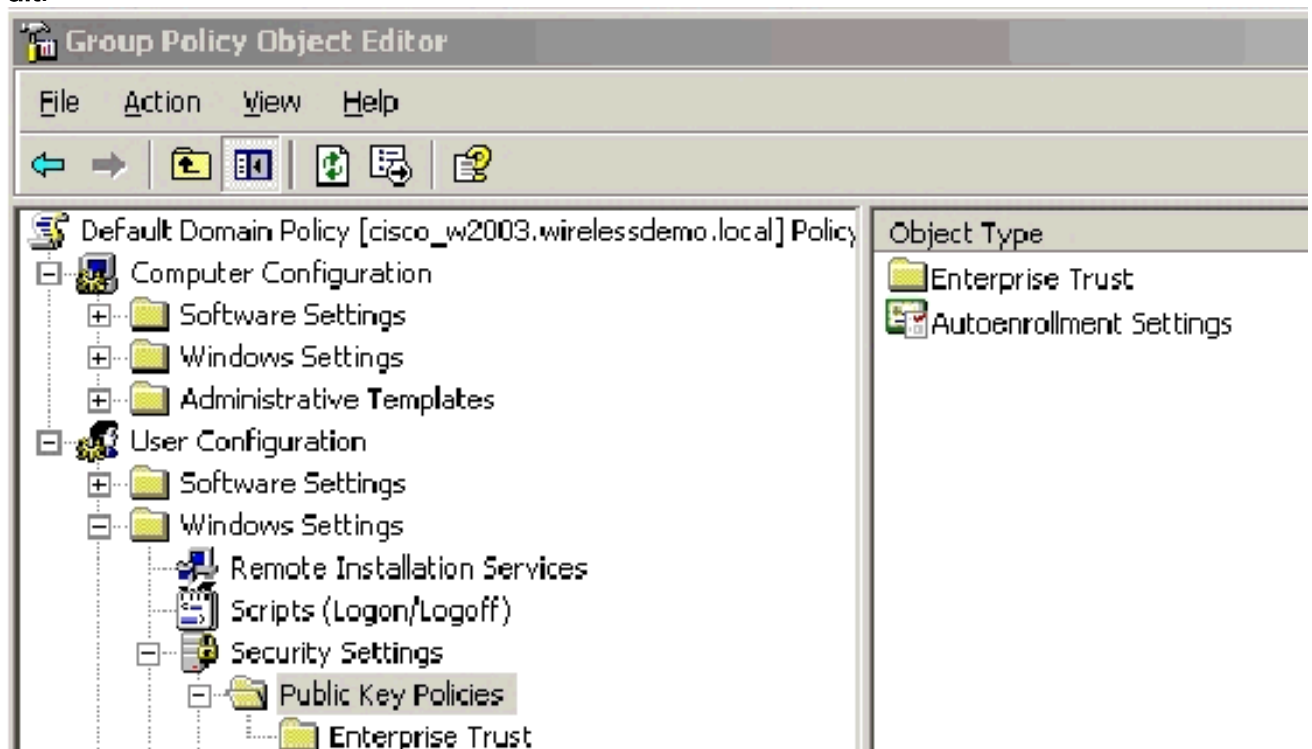




12. Klik op **Voltooien** van de pagina Wizard certificaataanvraag **invullen**. Het type Computer-certificaat verschijnt nu in het detailvenster van de editor voor groepsbeleid.

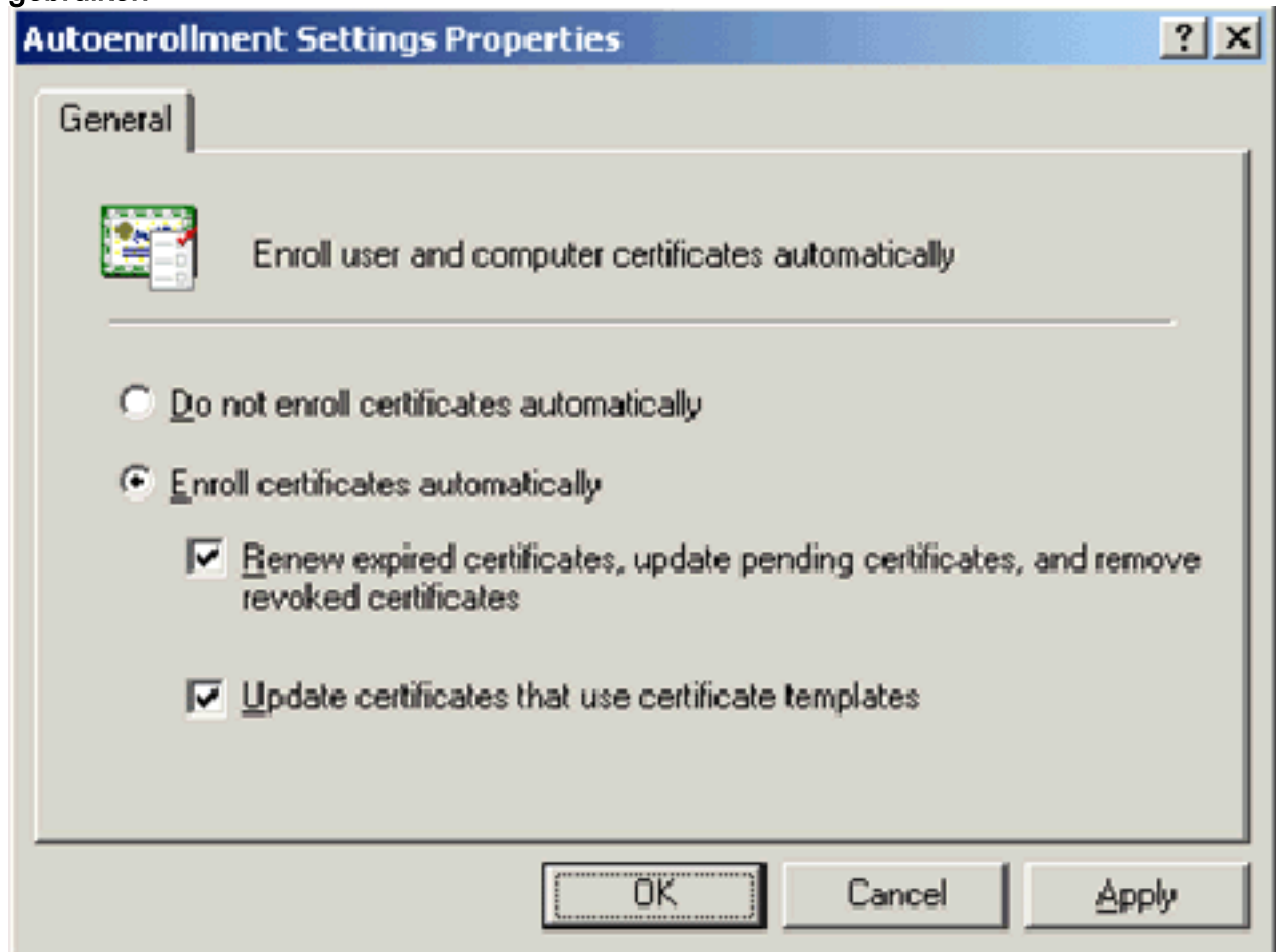


13. In de console boom, breid **Gebruiker Configuration > Windows Instellingen > Security Instellingen > Openbare Belangrijkste beleid** uit.



14. Dubbelklik in het deelvenster met details op **Instellingen voor automatische inschrijving**.  
 15. Kies **automatisch inlogcertificaten** en controleer **Verleng verlopen certificaten, update**

hangende certificaten en verwijder ingetrokken certificaten en update certificaten die certificaatsjablonen gebruiken.



16. Klik op OK.

## [ACS 4.0 certificaatinstelling](#)

### [Exportcertificaat voor ACS configureren](#)

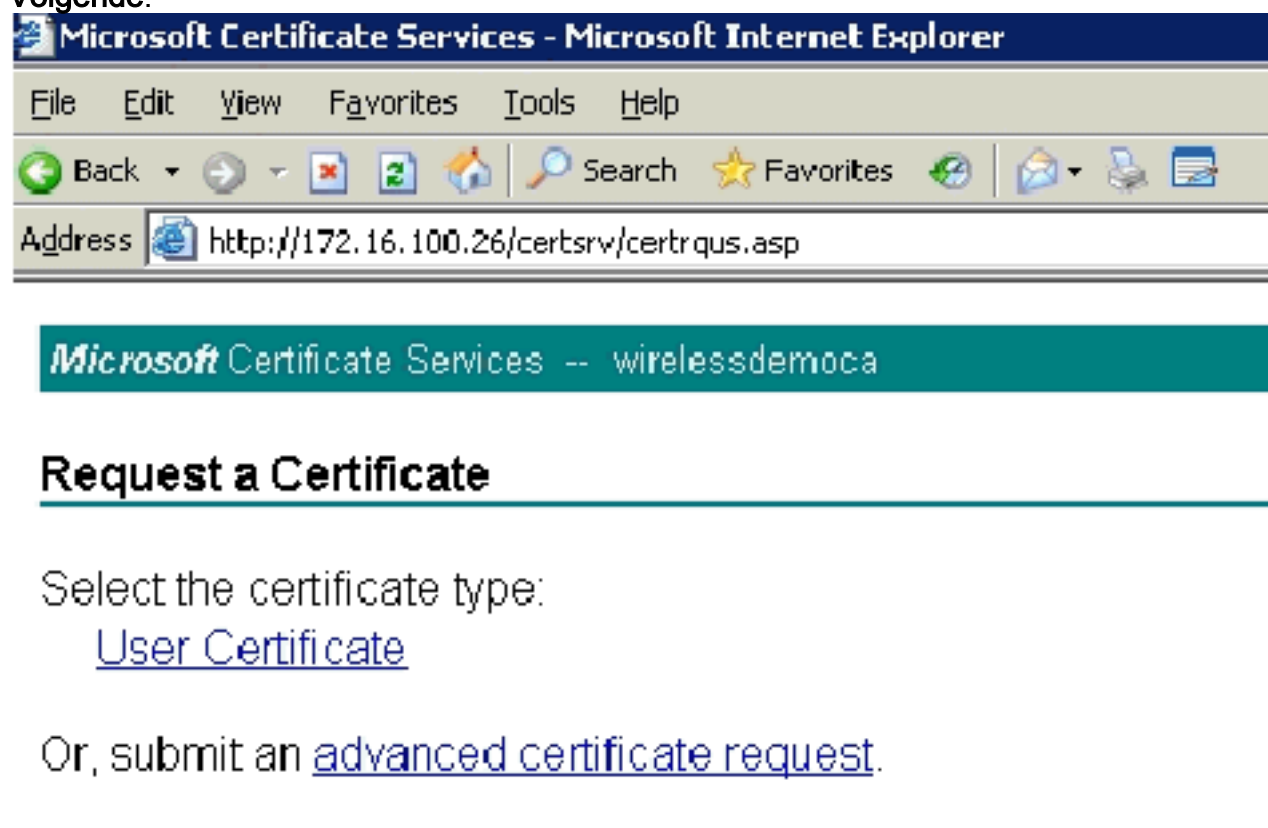
**Belangrijk:** De ACS-server moet een servercertificaat van de Enterprise root CA-server verkrijgen om een WLAN EAP-TLS-client te authentifieren.

**Belangrijk:** Zorg ervoor dat de IIS Manager niet tijdens het proces van de certificaatopstelling wordt geopend aangezien het problemen met gecached informatie veroorzaakt.

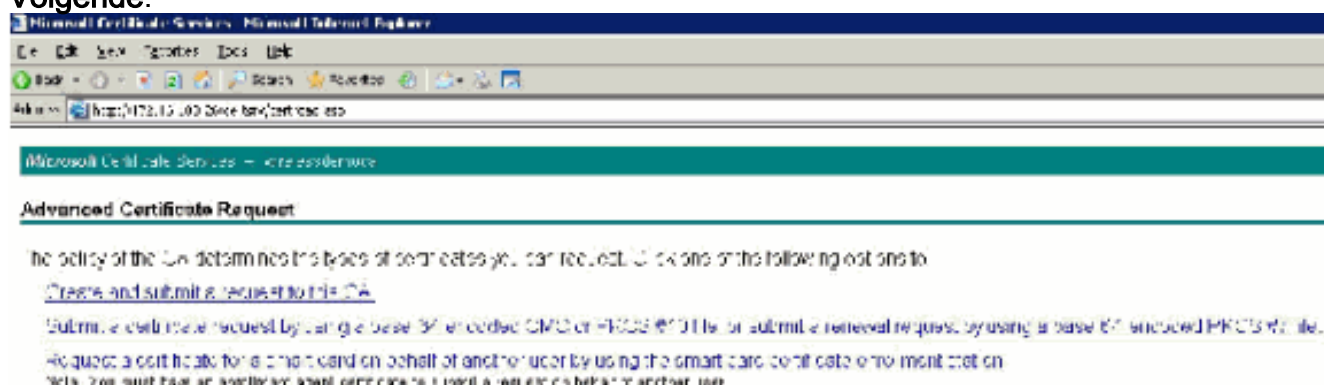
1. Meld u aan op de ACS-server met een account met de rechten van de Enterprise Admin.
2. Richt de browser op de server van de Microsoft certificeringsinstantie op <http://IP-address-of-Root-CA/certsrv>. In dit geval is het IP-adres **172.16.100.26**.
3. Log in als beheerder.



4. Kies een certificaat aanvragen en klik op **Volgende.**



5. Klik op **Geavanceerde aanvraag** en klik op **Volgende.**



6. Klik op **Maken en dien een verzoek in bij deze CA** en klik op **Volgende.** **Belangrijk:** De reden voor deze stap is vanwege het feit dat Windows 2003 geen exportbare sleutels toestaat en u moet een certificaataanvraag genereren gebaseerd op het ACS-certificaat dat u eerder creëerde.

sock - [Icons] Secret - Favorites [Icons] [Icons]

Address <https://172.16.1.10:2544/verif/ima.asp>

**Microsoft Certificate Services** - wirelessdemo.local

## Advanced Certificate Request

---

**Certificate Template:**

Administrator

Administrator

Basic EFS

Enhanced Recovery Agent

User

CSP: Wireless User Certificate Template

Key Usage: S\_Lordine Certification Authority

Key Store: Web Server  
My: 15384: 1024 2048 4096 8192 16384

Automatic key container name  User specified key container name

Mark keys as exportable  
 Export keys to file

Enable storing private key protection

Store certificate in the local computer certificate store  
*Saves the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.*

---

**Additional Options:**

Request Format:  CMC  PKCS10

Hash Algorithm:   
Only used to sign request.

Save request to file

Attributes:

Friendly Name:

7. Selecteer in de certificaatsjablonen de certificeringssjabloon die eerder met de naam **ACS** is gemaakt. De opties wijzigen nadat u de sjabloon hebt geselecteerd.
8. Configuratie van de Naam om de volledig gekwalificeerde domeinnaam van de ACS server te zijn. In dit geval is de ACS servernaam `cisco_w2003.wirelessdemo.local`. Zorg ervoor dat **het opslagcertificaat in de lokale computer certificatenwinkel** is ingeschakeld en klik vervolgens op

Microsoft Certificate Services - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites

Address http://172.16.100.25/certsrv/certreqns.asp

**Certificate Template:**

ACS

**Identifying Information For Offline Template:**

Name: cisco\_w2003\_wirelessdemo.local

E-Mail:

Company:

Department:

City:

State:

Country/Region:

**Key Options:**

Create new key set  Use existing key set

CSP: Microsoft Base Cryptographic Provider v1.0

Key Usage:  Exchange

Key Size: 1024 Min:1024 Max:1024 (common key sizes: 1024)

Automatic key container name  User specified key container name

Mark keys as exportable

Export keys to file

Store certificate in the local computer certificate store  
Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

**Additional Options:**

Request Format:  CMC  PKCS10

Hash Algorithm: SHA-1  
Only used to sign request.

Save request to a file

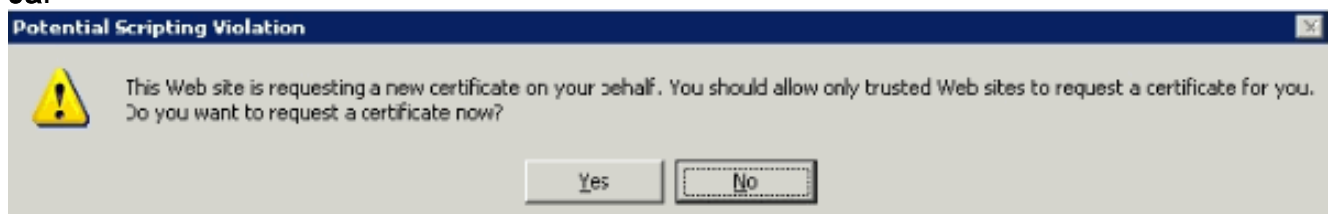
Attributes:

Friendly Name:

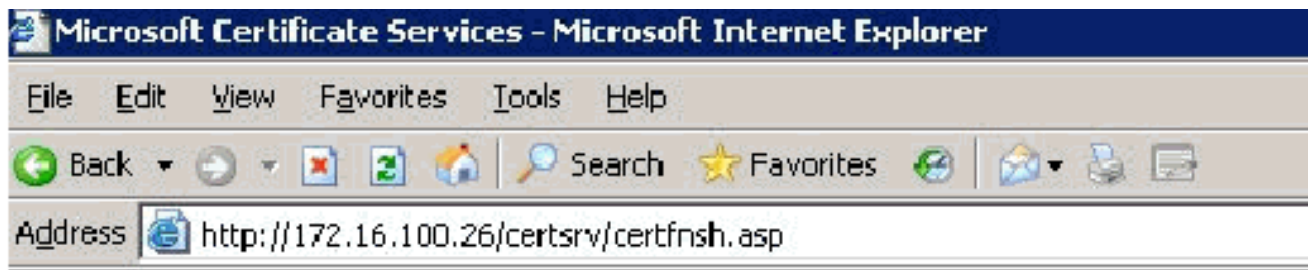
Submit >

Inzenden.

9. Een pop-upvenster verschijnt dat waarschuwt voor een mogelijke schending van het schrift. Klik op Ja.



10. Klik op Installeer dit certificaat.



Microsoft Certificate Services -- wirelessdemoca

## Certificate Issued

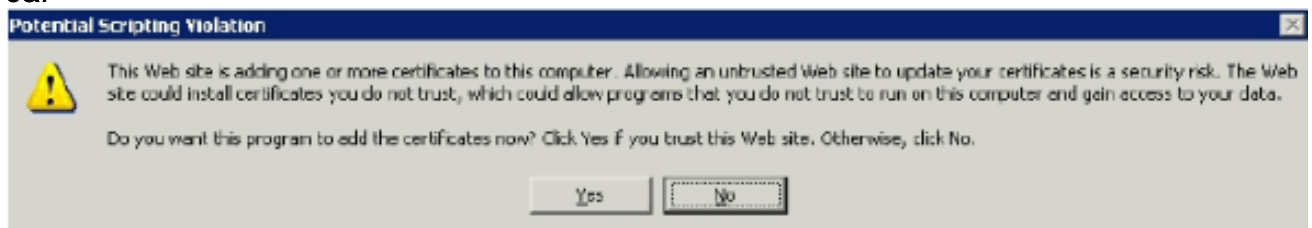
The certificate you requested was issued to you.



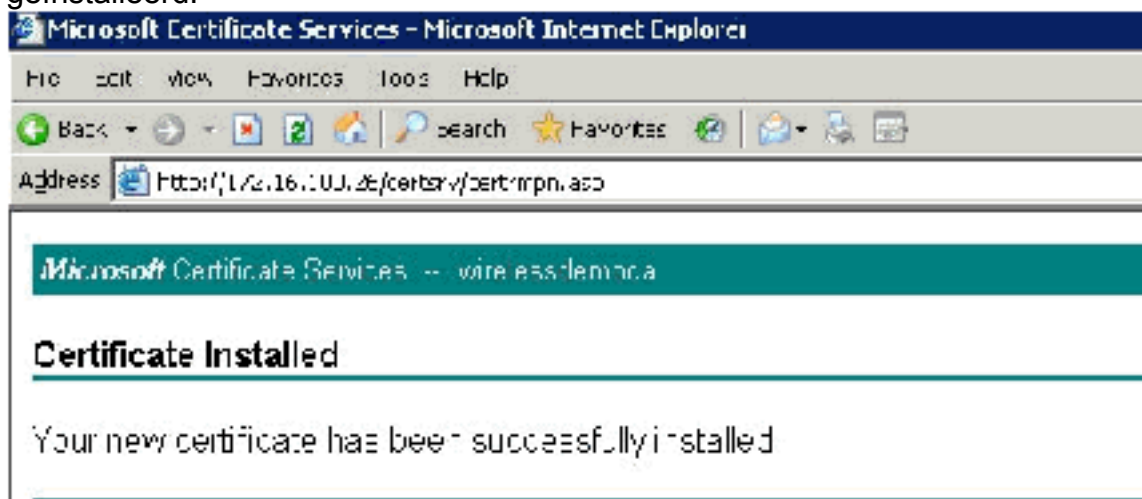
[Install this certificate](#)

11. Er verschijnt opnieuw een pop-upvenster en waarschuwt voor een mogelijke overtreding van het scripting. Klik op

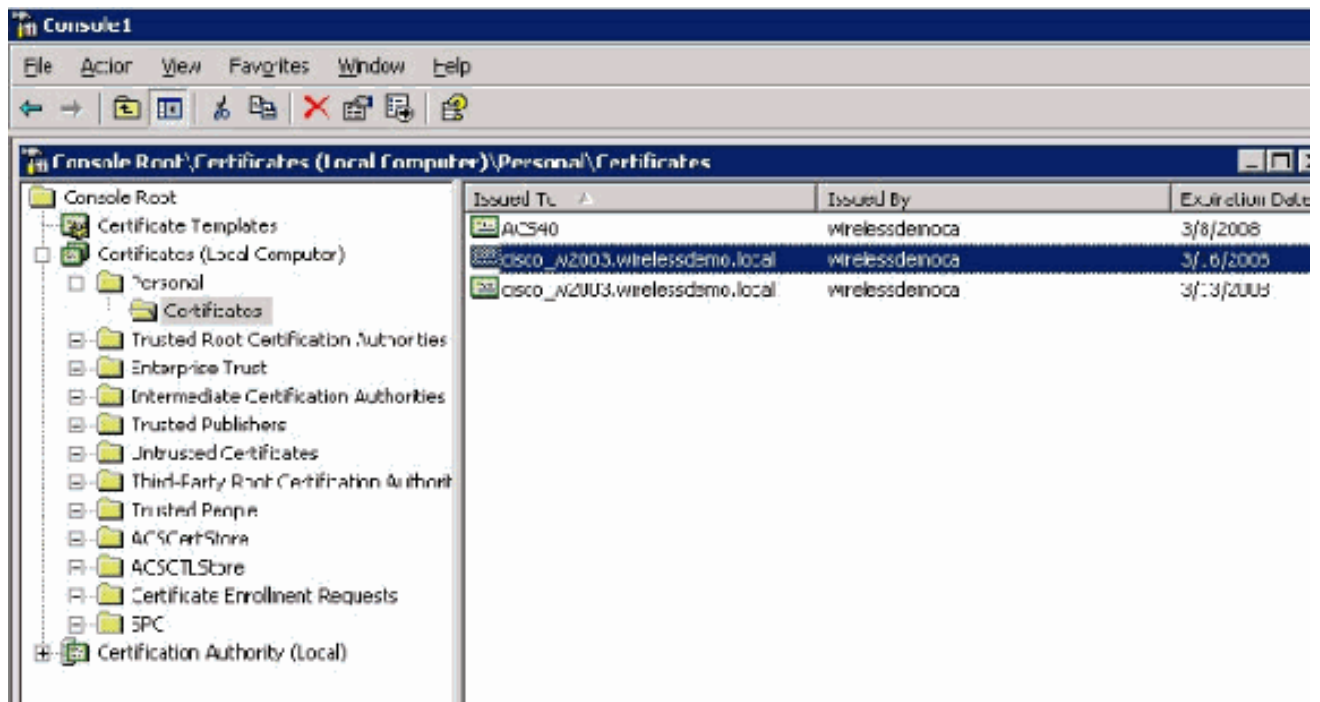
**Ja.**



12. Nadat u op **Ja** hebt geklikt, wordt het certificaat geïnstalleerd.



13. Op dit moment is het certificaat geïnstalleerd in de map Certificaten. Kies **Start > Start > Start**, type **mmc**, druk op **Voer in** en kies **Persoonlijk > Certificaten**.



14. Nu het certificaat op de lokale computer geïnstalleerd is (ACS of cisco\_w2003 in dit voorbeeld) moet u een certificaatbestand (.cer) genereren voor de configuratie van het ACS 4.0-certificaatbestand.
15. Richt op de ACS server (cisco\_w2003 in dit voorbeeld) de browser op de server van de Microsoft Certified Authority op <http://172.16.100.26/certsrv>.

### [Installeer het certificaat in de ACS 4.0-software](#)

Voer de volgende stappen uit:

1. Richt op de ACS server (cisco\_w2003 in dit voorbeeld) de browser op de Microsoft CA server op <http://172.16.100.26/certsrv>.
2. Selecteer in de optie Selecteren een taak en kies **een CA-certificaat, certificeringsketen of CRL**.
3. Kies de **Base64**-radiocoderingsmethode en klik op **Download CA**.



Microsoft Certificate Services - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address http://172.16.100.26/certs/v/certbcard.asp

---

Microsoft Certificate Services -- wirelessdemora

### Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority [install this CA certificate chain](#).

To download a CA certificate, certificate chain, or CRL, select the certificate encoding method:

**CA certificate:**

Current (wirelessdemora)

**Encoding method:**

DER

Base 64

[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

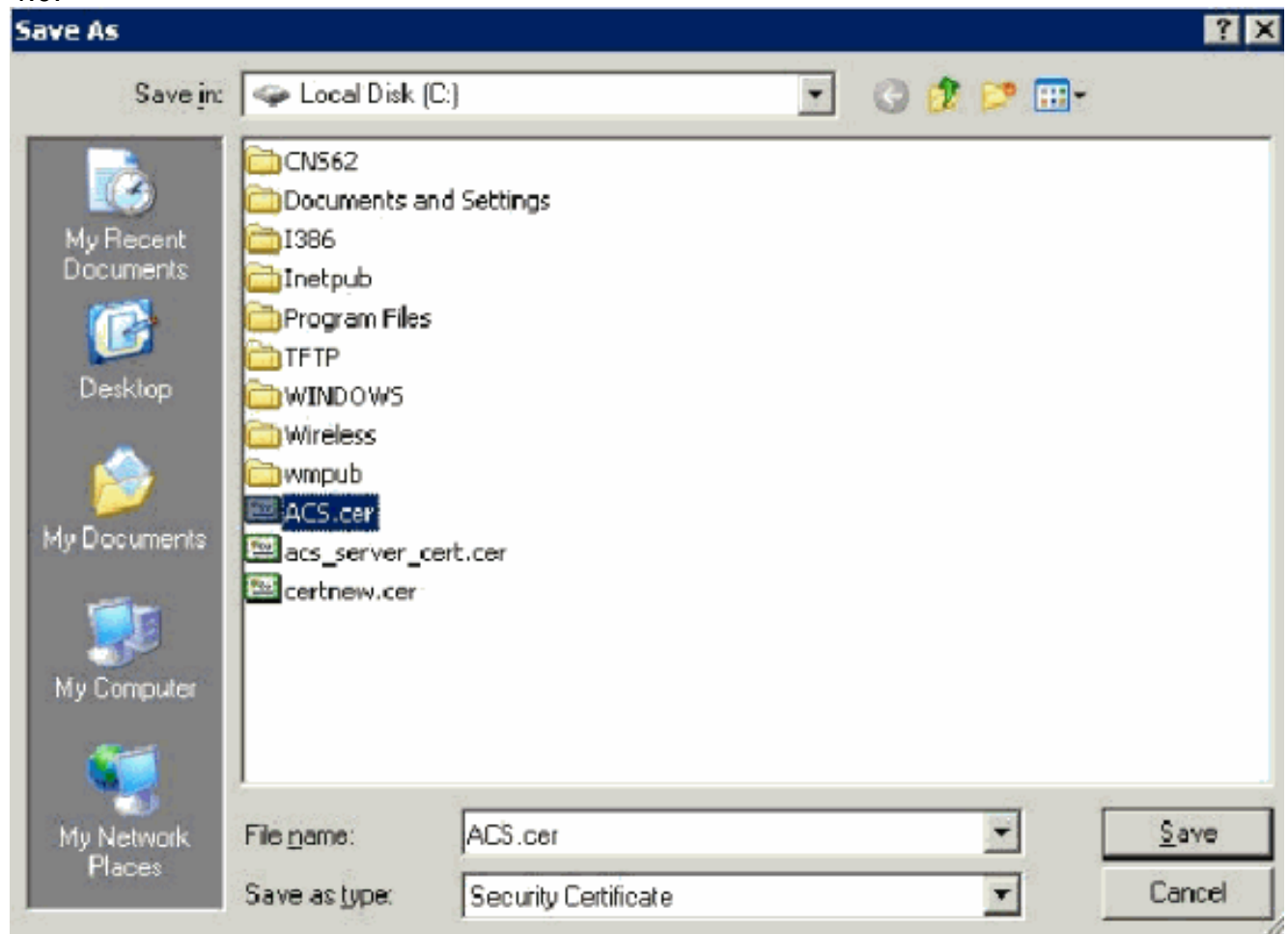
[Download latest delta CRL](#)

4. Er verschijnt een waarschuwingsvenster voor het downloaden van bestanden. Klik op Opslaan.



5. Sla het bestand op met een naam zoals ACS.cer of een naam die u wilt. Onthoud deze naam omdat u deze gebruikt tijdens de ACS-instelling van de certificaatinstantie in ACS

4.0.

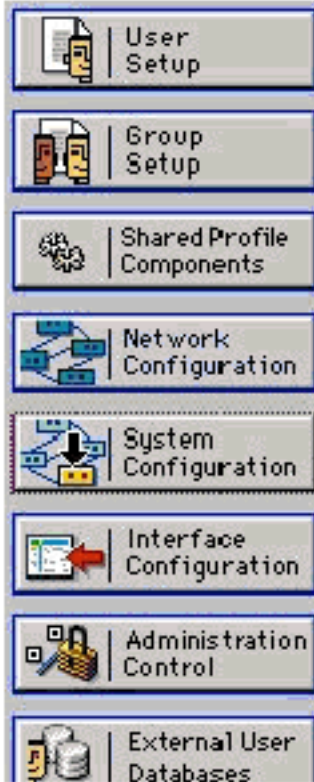



6. Open **ACS Admin** van de desktop sneltoets die tijdens de installatie is gemaakt.
7. Klik op **stelselconfiguratie**.



## System Configuration

### Select



-  [Service Control](#)
-  [Logging](#)
-  [Date Format Control](#)
-  [Local Password Management](#)
-  [ACS Internal Database Replication](#)
-  [ACS Backup](#)
-  [ACS Restore](#)
-  [ACS Service Management](#)
-  [VoIP Accounting Configuration](#)
-  [ACS Certificate Setup](#)
-  [Global Authentication Setup](#)

8. Klik op ACS certificaatinstelling.

# System Configuration

Select

## ACS Certificate Setup

-  [Install ACS Certificate](#)
-  [ACS Certification Authority Setup](#)
-  [Edit Certificate Trust List](#)
-  [Certificate Revocation Lists](#)
-  [Generate Certificate Signing Request](#)
-  [Generate Self-Signed Certificate](#)

Cancel

9. Klik op ACS-certificaat installeren.

# System Configuration

Edit

## Install ACS Certificate

Install new certificate 	
<input type="radio"/> Read certificate from file	
<b>Certificate file</b>	<input type="text"/>
<input checked="" type="radio"/> Use certificate from storage	
<b>Certificate CN</b>	<input type="text"/>
<b>Private key file</b>	<input type="text"/>
<b>Private key password</b>	<input type="text"/>

10. Kies het certificaat van opslag en type in de volledig gekwalificeerde domeinnaam van `cisco_w2003.wirelessdemo.local` (of `ACS.wirelessdemo.local` als u ACS als naam gebruikte).

## System Configuration

Edit

### Install ACS Certificate


Install new certificate 	
<input type="radio"/> Read certificate from file	
<b>Certificate file</b>	<input type="text"/>
<input checked="" type="radio"/> Use certificate from storage	
<b>Certificate CN</b>	<input type="text" value="cisco_w2003.wirelessdemo.local"/>
<b>Private key file</b>	<input type="text"/>
<b>Private key password</b>	<input type="text"/>

11. Klik op Inzenden.

## System Configuration

Edit

### Install ACS Certificate

Installed Certificate Information 	
<b>Issued to:</b>	cisco_w2003.wirelessdemo.local
<b>Issued by:</b>	wirelessdemoca
<b>Valid from:</b>	March 17 2006 at 08:33:25
<b>Valid to:</b>	March 16 2008 at 08:33:25
<b>Validity:</b>	OK


**The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.**

12. Klik op systeemconfiguratie.
13. Klik op Service Control en vervolgens op


Start.

## System Configuration

Select

CiscoSecure ACS on cisco\_w2003 

### Is Currently Running

Services Log File Configuration 

Level of detail

None

Low

Full

Generate New File

Every day

Every week


Every month

When size is greater than  KB

Manage Directory

Keep only the last  files

Delete files older than  days

 [Back to Help](#)

14. Klik op **stysteemconfiguratie**.
15. Klik op **Global Authentication Setup**.
16. Controleer **MAP-TLS** en alle bijbehorende vakjes.

# System Configuration

## Global Authentication Setup

### EAP Configuration

**PEAP**

Allow EAP-MSCHAPv2

Allow EAP-GTC

Allow Posture Validation

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

---

**EAP-FAST**

[EAP-FAST Configuration](#)

---

**EAP-TLS**

Allow EAP-TLS

Select one or more of the following options:

- Certificate SAN comparison
- Certificate CN comparison
- Certificate Binary comparison

EAP-TLS session timeout (minutes):

17. Klik op **Inzenden + opnieuw starten**.

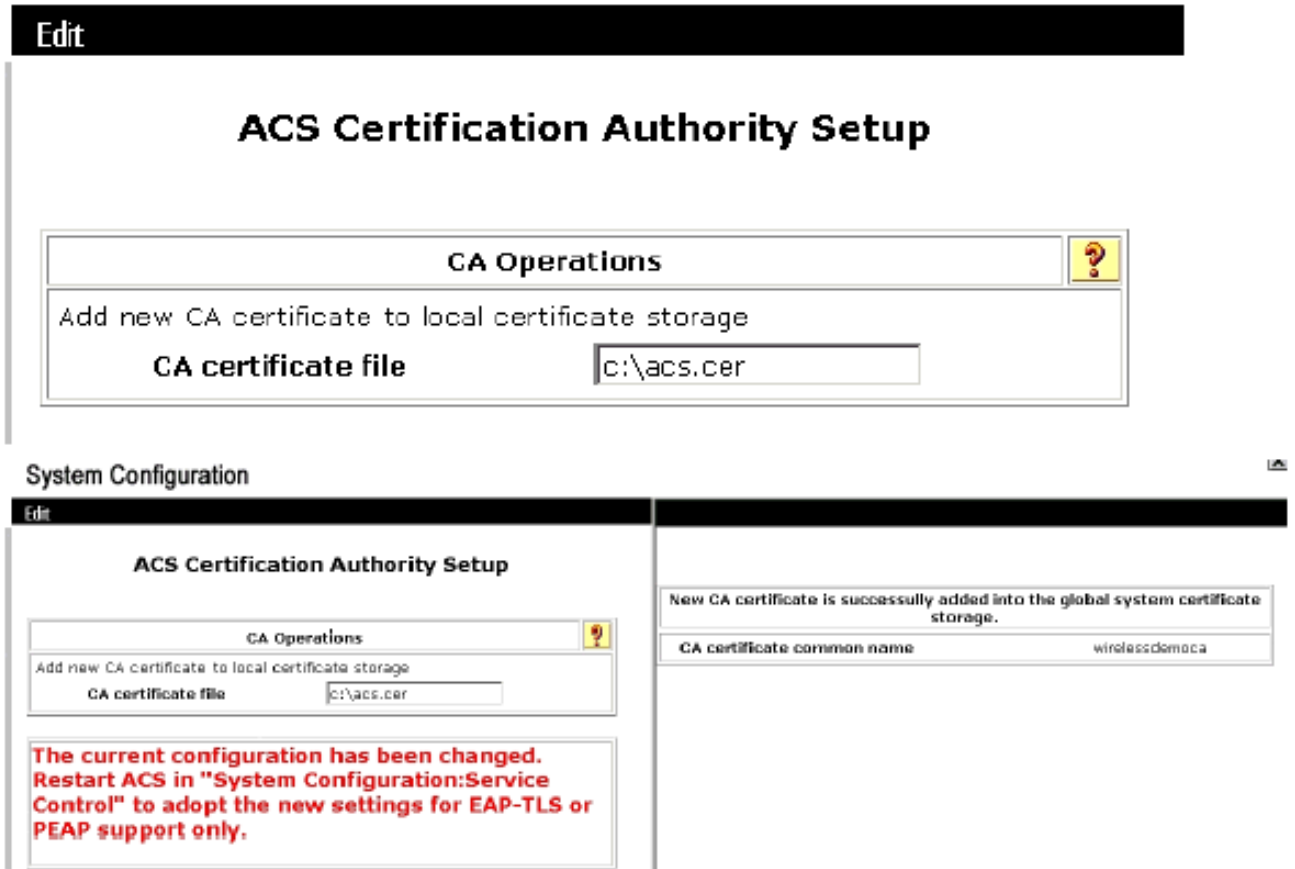
18. Klik op **stelsysteemconfiguratie**.

19. Klik op **ACS-certificeringsinstantie**.

20. Typ onder het venster Instellingen certificeringsinstantie ACS de naam en lokatie van het eerder gemaakte bestand. In dit voorbeeld is het \*.cer-bestand dat is gemaakt **ACS.cer** in de folder van de wortel c:\.

21. Typ **c:\acs.cer** in het veld CA-certificaatbestand en klik op **Inzenden**.

# System Configuration



**ACS Certification Authority Setup**

CA Operations

Add new CA certificate to local certificate storage

CA certificate file

New CA certificate is successfully added into the global system certificate storage.

CA certificate common name	wirelessdemo.ca
----------------------------	-----------------

**The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.**

22. Start de ACS-service opnieuw.

## [CLIENTconfiguratie voor MAP-TLS met behulp van Windows Zero Touch](#)

CLIENT is een computer die Windows XP Professional met SP2 runt die als draadloze client handelt en toegang tot Intranet bronnen via de draadloze AP verkrijgt. Volg de procedures in dit gedeelte om CLIENT als draadloze client te configureren.

### [Een basisinstallatie en -configuratie uitvoeren](#)

Voer de volgende stappen uit:

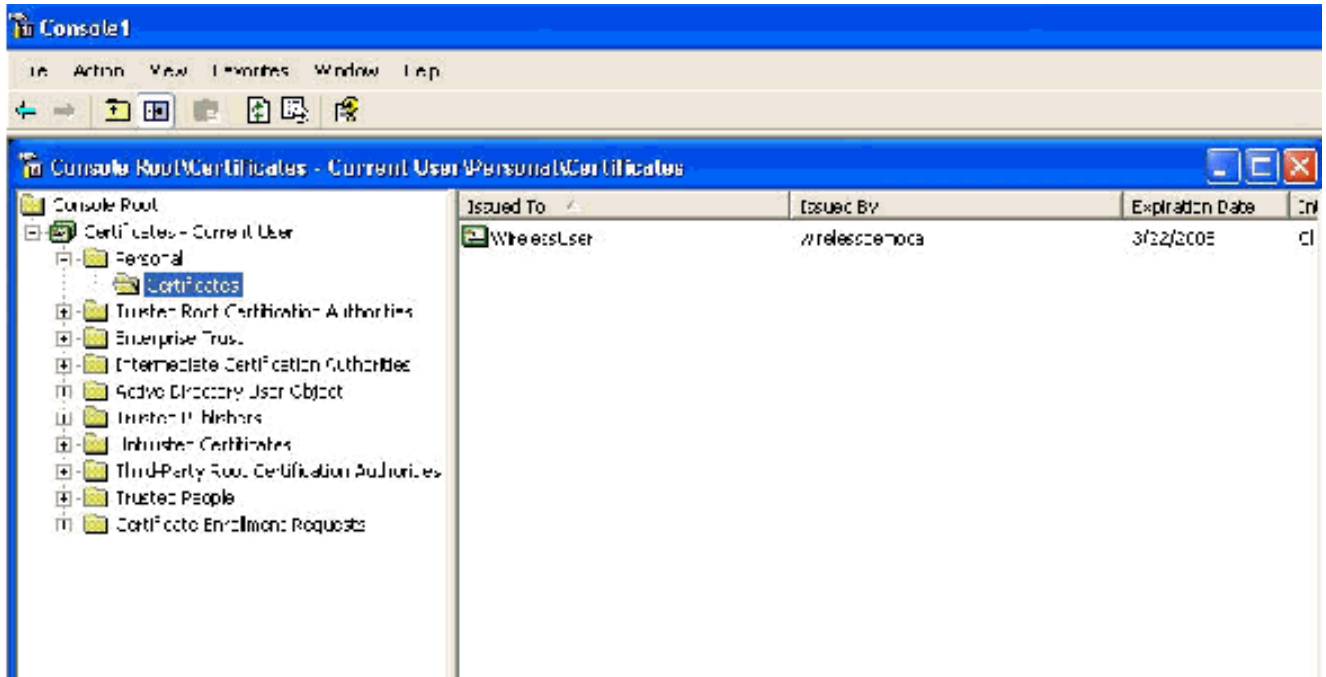
1. Sluit CLIENT aan op het intranet van het netwerk met behulp van een Ethernet-kabel die op de switch is aangesloten.
2. Installeer op CLIENT Windows XP Professional met SP2 als een lid-computer die **CLIENT** heet op het lokale domein Wireless-demo.com.
3. Installeer Windows XP Professional met SP2. Dit moet worden geïnstalleerd om EAP-TLS- en PEAP-ondersteuning te hebben. **Opmerking:** Windows Firewall is automatisch ingeschakeld in Windows XP Professional met SP2. Schakel de firewall niet uit.

### [De draadloze netwerkverbinding configureren](#)

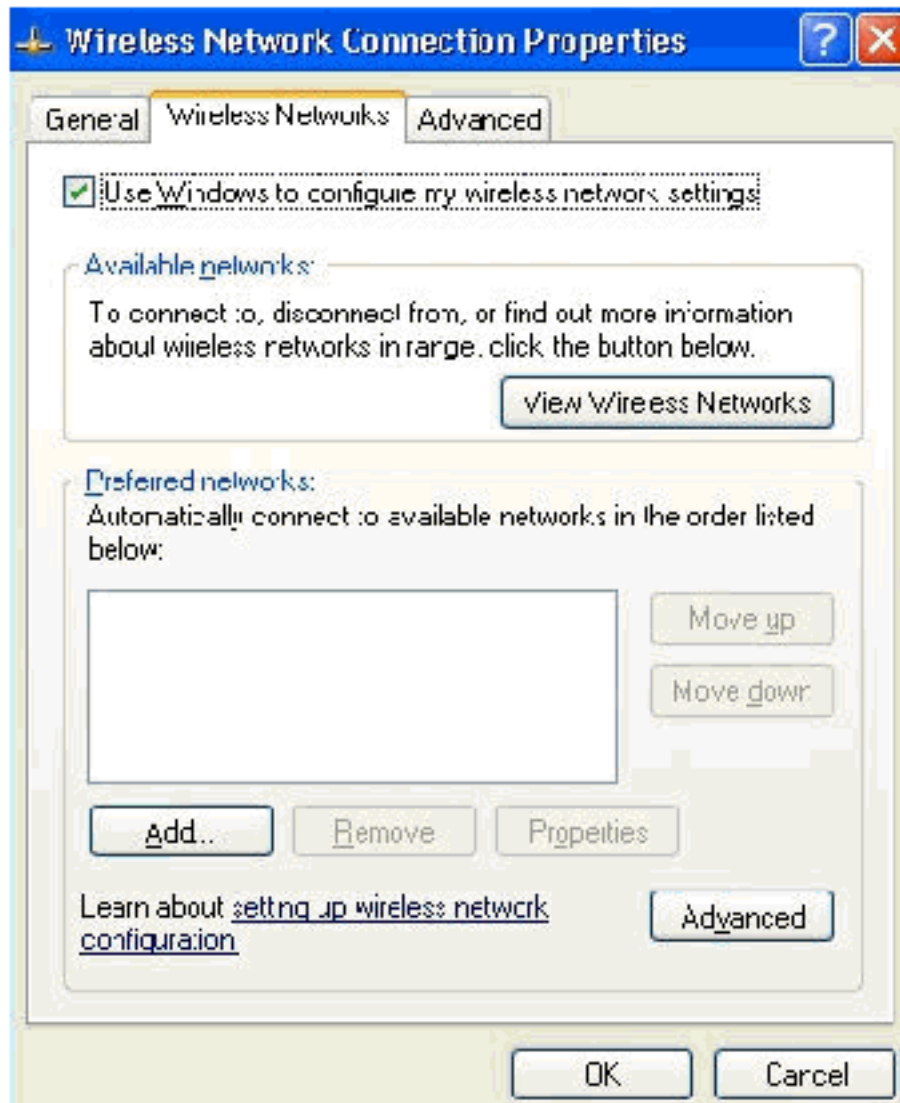
Voer de volgende stappen uit:



1. Log uit en log in door de WirelessUser-account in het lokale domein van de draadloze demo.com te gebruiken. **Opmerking:** update de beleidsinstellingen van de computer en de gebruikersgroep en verkrijg direct een computer en gebruikerscertificaat voor de draadloze clientcomputer door **gpupdate** te typen in een opdrachtmelding. Anders, wanneer u uitlogt en dan inlogt, voert het de zelfde functie uit als **gpupdate**. U moet via de bedrading op het domein zijn aangemeld. **Opmerking:** Om te valideren dat het certificaat automatisch op de client wordt geïnstalleerd, opent u de certificering-MMC en verklaart u dat het Wireless User-certificaat beschikbaar is in de map Mobile Certificates.

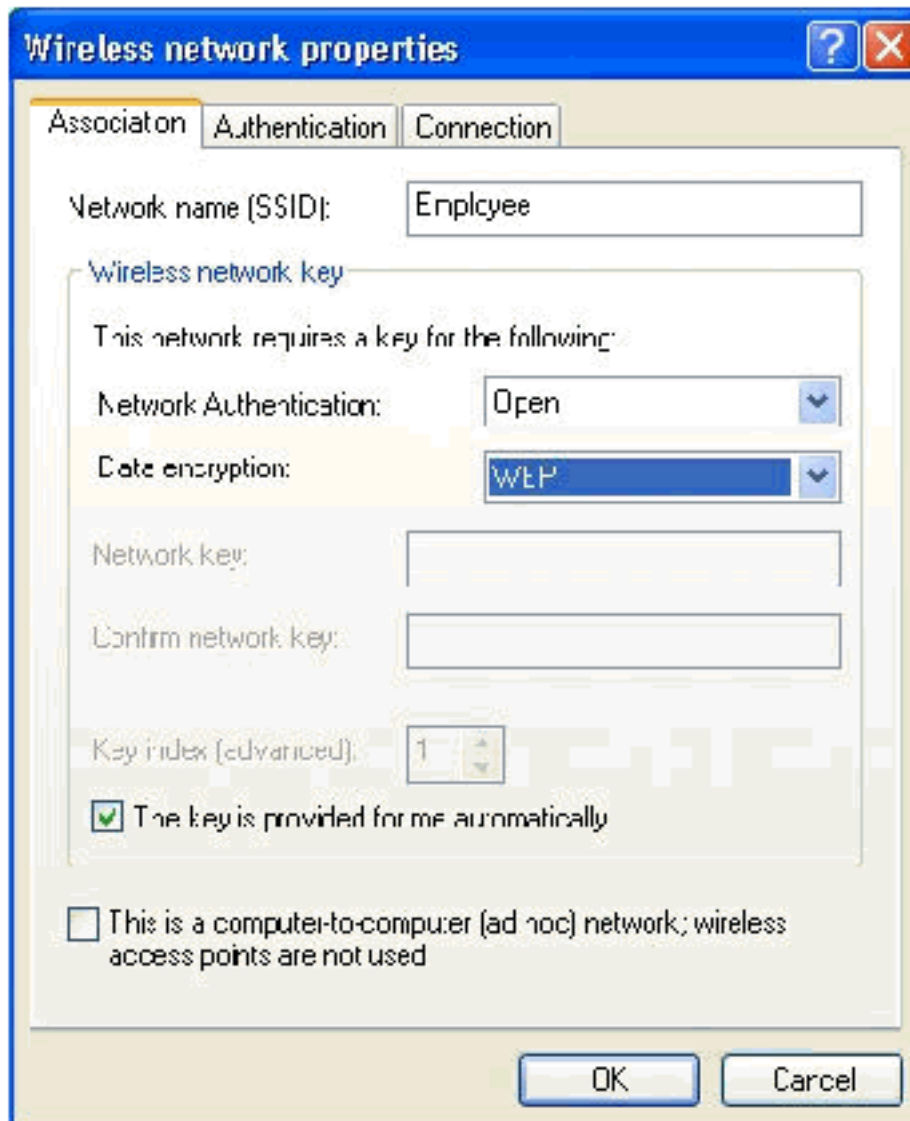


2. Kies **Start > Configuratiescherm**, dubbelklik op **Netwerkverbindingen** en klik met de rechtermuisknop op **Draadloze netwerkverbinding**.
3. Klik op **Eigenschappen**, ga naar het tabblad **Draadloze netwerken** en zorg ervoor dat **Gebruiker Windows om mijn draadloze netwerkinstellingen te configureren** is



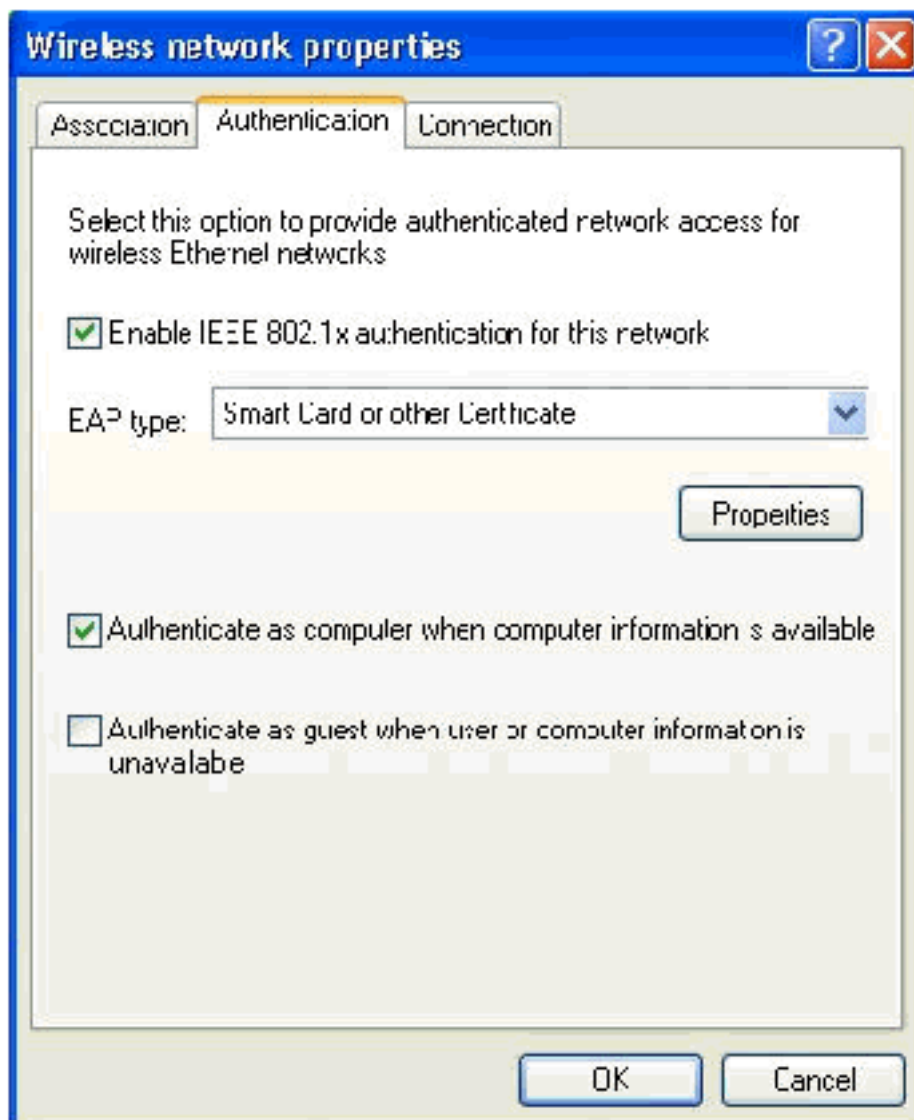
ingeschakeld.

4. Klik op **Add** (Toevoegen).
5. Ga naar het tabblad Associatie en type **Werknemer** in het veld Netwerknamen (SSID).
6. Zorg ervoor dat Data Encryption is ingesteld op en **de toets wordt automatisch**



gecontroleerd.

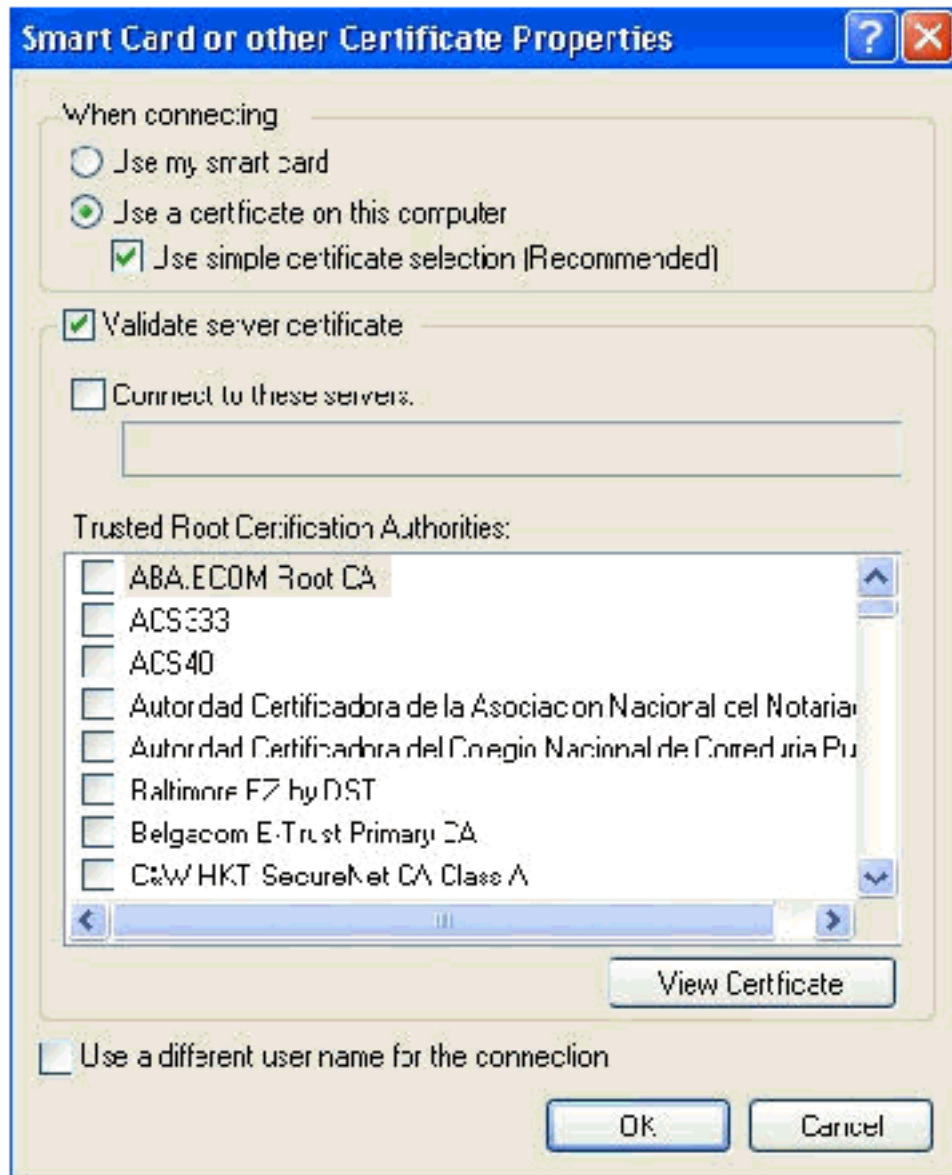
7. Ga naar het tabblad Verificatie.
8. Bevestig dat EAP type is ingesteld om **Smart Card of ander certificaat** te gebruiken. Als dit niet het geval is, selecteert u de optie in het uitrolmenu.
9. Als u wilt dat de machine voor de inlognaam wordt geauthentiseerd (dit maakt het mogelijk om inlogscripts of groepsbeleid toe te passen) kies de optie **Authenticate as computer wanneer computerinformatie beschikbaar**



is.

10. Klik op **Eigenschappen**.

11. Zorg ervoor dat de vakjes in dit venster zijn

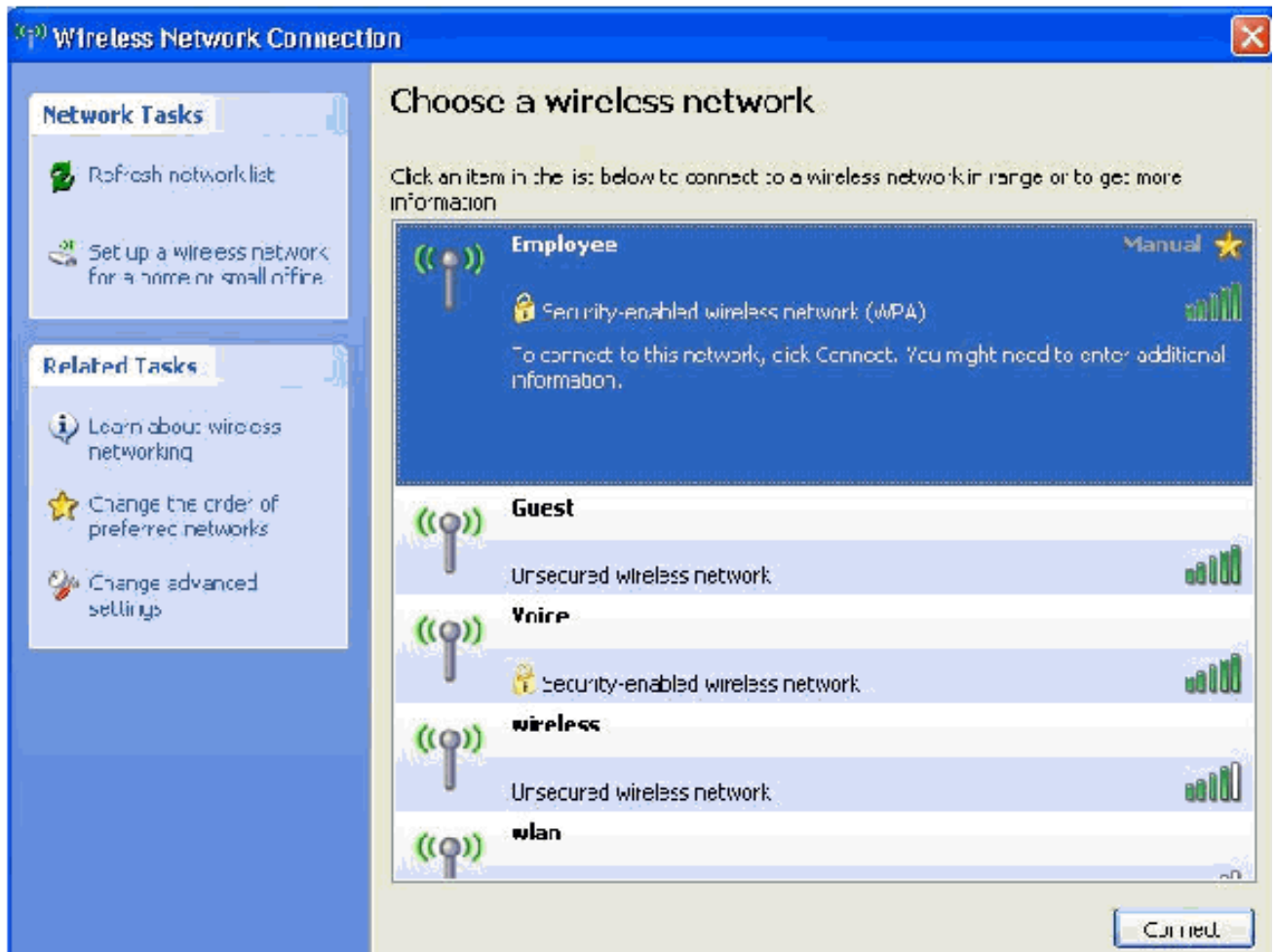


ingeschakeld.

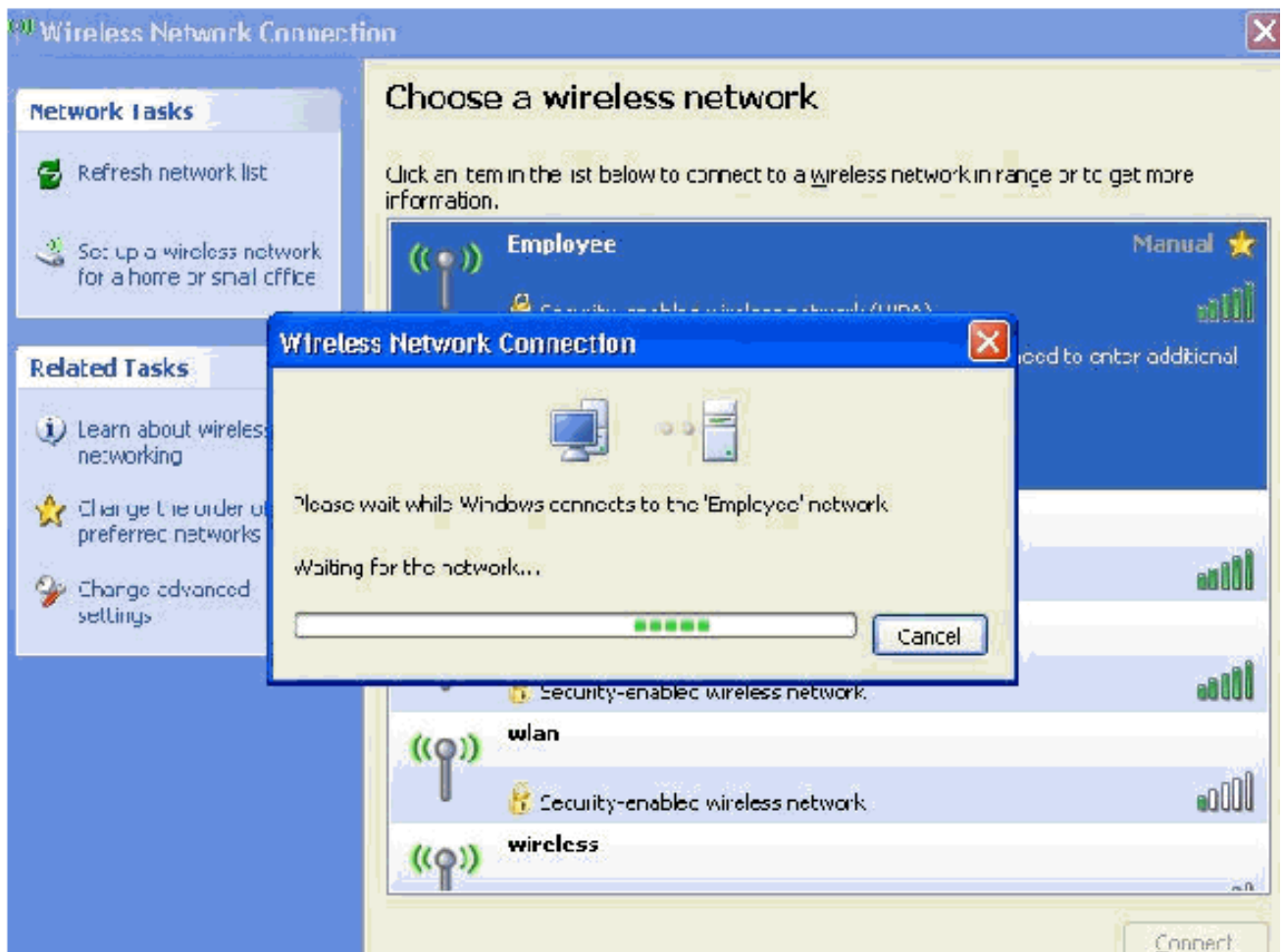
12. Klik drie keer op **OK**.

13. Klik met de rechtermuisknop op het pictogram voor draadloze netwerkverbinding in het systeem en klik vervolgens op **Beschikbare draadloze netwerken bekijken**.

14. Klik op het draadloze netwerk van de **Werknemer** en klik op **Connect**.



Deze screenshots geven aan of de verbinding met succes voltooid is.



Wireless Network Connection

### Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

**Employee** Attempting to authenticate

Security-enabled wireless network

Connect from this network

**wlan** Security-enabled wireless network

**wireless** Security-enabled wireless network

Disconnect

Wireless Network Connection

Please wait while Windows connects to the 'Employee' network.

Waiting for network to be ready...

Cancel

Wireless Network Connection

### Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

**Employee** Acquiring network address

Security-enabled wireless network (WPA)

Connect from this network

**wireless** Security-enabled wireless network

Security-enabled wireless network

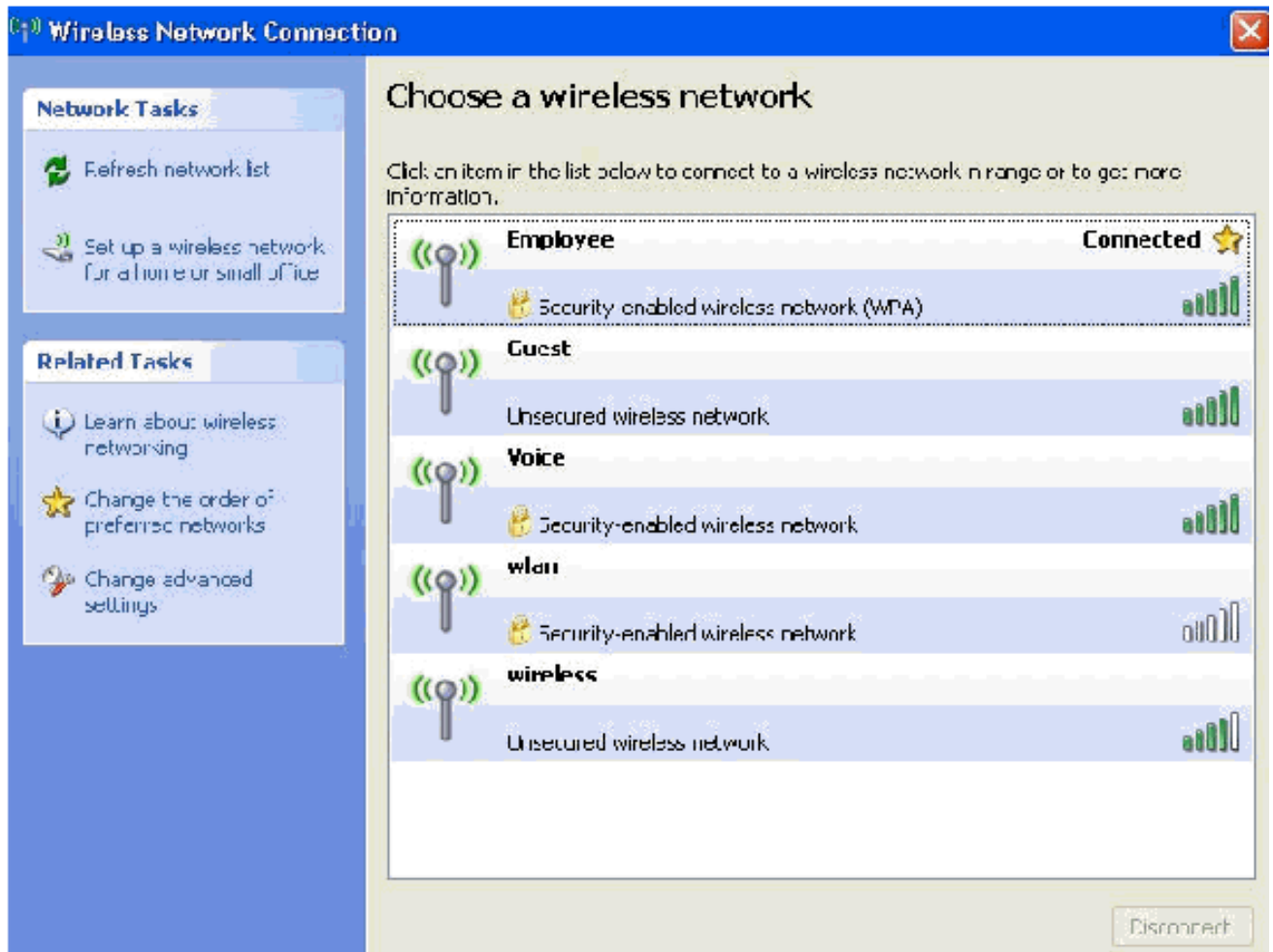
Disconnect

Wireless Network Connection

Please wait while Windows connects to the 'Employee' network.

Waiting for network to be ready...

Cancel



15. Nadat de authenticatie succesvol is, controleer de TCP/IP configuratie voor de draadloze adapter door Network Connections te gebruiken. Het moet een adresbereik hebben van 172.16.100.100-172.16.100.254 van het DHCP-bereik of het bereik dat wordt gecreëerd voor de draadloze klanten.
16. Om functionaliteit te testen, opent u een browser en bladert naar <http://wirelessdemoca> (of het IP adres van de Enterprise CA server).

## Gerelateerde informatie

- [PPP-verificatie met WLAN-controllers \(WLC\) - configuratievoorbeeld](#)
- [Configuratiehandleiding voor draadloze LAN-controllers](#)
- [Configuratievoorbeeld voor draadloos LAN-controller en lichtgewicht access point](#)
- [Configuratievoorbeeld van VLAN's voor draadloze LAN-controllers](#)
- [Configuratievoorbeeld van AP Group VLAN's met draadloze LAN-controllers](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)