

PEAP onder Unified Wireless Networks met Microsoft Internet Verification Service (IAS)

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[PEAP - Overzicht](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[De Microsoft Windows 2003-server configureren](#)

[De Microsoft Windows 2003-server configureren](#)

[DHCP-services installeren en configureren op de Microsoft Windows 2003-server](#)

[De Microsoft Windows 2003-server installeren en configureren als een certificeringsinstantie \(CA\)-server](#)

[Clients met domein verbinden](#)

[Installeer de internetverificatieservice op de Microsoft Windows 2003-server en vraag een certificaat aan](#)

[De internetverificatieservice configureren voor PEAP-MS-CHAP v2-verificatie](#)

[Gebruikers toevoegen aan de actieve map](#)

[Draadloze toegang voor gebruikers toestaan](#)

[De draadloze LAN-controller en lichtgewicht AP's configureren](#)

[De WLC voor RADIUS-verificatie configureren via MS IAS RADIUS-server](#)

[WLAN's voor de clients configureren](#)

[De draadloze clients configureren](#)

[De draadloze clients voor PEAP-MS CHAPv2-verificatie configureren](#)

[Verifiëren en probleemoplossing](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document biedt een configuratievoorbeeld voor het instellen van een Protected Extensible Verification Protocol (PEAP) met Microsoft Challenge Handshake Verification Protocol (MS-CHAP), versie 2-verificatie in een Cisco Unified Wireless-netwerk met de Microsoft Internet Verification Service (IAS) als RADIUS-server.

[Voorwaarden](#)

Vereisten

Er wordt verondersteld dat de lezer kennis heeft van de basisinstallatie van Windows 2003 en de installatie van Cisco-controllers, aangezien dit document alleen betrekking heeft op de specifieke configuraties om de tests te vergemakkelijken.

Opmerking: Dit document is bedoeld om de lezers een voorbeeld te geven van de configuratie die vereist is op een MS-server voor PEAP - MS CHAP-verificatie. De Microsoft-serverconfiguratie die in deze sectie wordt gepresenteerd, is getest in het lab en blijkt te werken zoals verwacht. Als u problemen ondervindt bij het configureren van de Microsoft-server, neemt u contact op met Microsoft voor ondersteuning. Cisco TAC ondersteunt Microsoft Windows-serverconfiguratie niet.

Raadpleeg voor installatie- en configuratieinformatie voor Cisco 4400 Series controllers de [Quick Start Guide: Cisco 4400 Series draadloze LAN-controllers](#).

U vindt de installatie- en configuratiehandleidingen voor Microsoft Windows 2003 op [Installing Windows Server 2003 R2](#).

Voordat u begint, installeert u de Microsoft Windows Server 2003 met SP1-besturingssysteem op elk van de servers in het testlaboratorium en werkt u alle servicepakketten bij. Installeer de controllers en lichtgewicht access points en zorg ervoor dat de nieuwste software updates geconfigureerd zijn.

Gebruikte componenten

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

- Cisco 4400 Series controller voor de firmware versie 4.0
- Cisco 1131 lichtgewicht access point protocol (WAP) access point
- Windows 2003 Enterprise Server (SP1) met internetverificatieservice (IAS), certificeringsinstantie (CA), DHCP en geïnstalleerde DNS-services (Domain Name System)
- Windows XP Professional met SP2 (en bijgewerkte servicepakketten) en Cisco Aironet 802.11a/b/g draadloze netwerkinterfacekaart (NIC)
- Aironet Desktop Utility versie 4.0
- Cisco 3560 Switch

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.

PEAP - Overzicht

PEAP maakt gebruik van Transport Level Security (TLS) om een versleuteld kanaal te maken tussen een verificerende PEAP-client, zoals een draadloze laptop, en een PEAP-verificator, zoals Microsoft Internet Verification Service (IAS) of een RADIUS-server. PEAP specificeert geen

verificatiemethode, maar biedt aanvullende beveiliging voor andere EAP-verificatieprotocollen, zoals EAP-MSCHAPv2, die kunnen werken via het met TLS versleutelde kanaal dat door PEAP wordt geboden. Het PEAP-verificatieproces bestaat uit twee hoofdfasen:

PEAP fase één: TLS versleuteld kanaal

De draadloze client is gekoppeld aan het toegangspunt. Een op IEEE 802.11 gebaseerde associatie biedt een Open System of Shared Key-verificatie voordat een beveiligde associatie wordt gemaakt tussen de client en het access point (LAP). Nadat de op IEEE 802.11 gebaseerde verbinding tussen de client en het access point met succes is tot stand gebracht, wordt de TLS-sessie met het AP overeengekomen. Nadat de verificatie met succes is voltooid tussen de draadloze client en de IAS-server, wordt de TLS-sessie tussen de client en de IAS-server onderling overeengekomen. De sleutel die binnen deze onderhandeling wordt afgeleid wordt gebruikt om alle verdere communicatie te versleutelen.

PEAP fase twee: EAP-geverifieerde communicatie

EAP-communicatie, met inbegrip van EAP-onderhandeling, vindt plaats binnen het TLS-kanaal dat door PEAP in de eerste fase van het PEAP-verificatieproces is gecreëerd. De IAS-server verifieert de draadloze client met EAP-MS-CHAP v2. De LAP en de controller sturen alleen berichten door tussen de draadloze client en de RADIUS-server. De WLC en de LAP kunnen deze berichten niet decrypteren omdat het niet het TLS eindpunt is.

Nadat PEAP-fase één is opgetreden en het TLS-kanaal is gemaakt tussen de IAS-server en de 802.1X Wireless-client, is de RADIUS-berichtsequentie als volgt: voor een succesvolle verificatiepoging waarbij de gebruiker geldige, op een wachtwoord gebaseerde referenties heeft geleverd bij PEAP-MS-CHAP v2:

1. De IAS-server stuurt een identiteitsverzoekbericht naar de client: EAP-Verzoek/Identity.
2. De client reageert met een identiteitsresponsbericht: EAP-Response/Identity.
3. De IAS-server stuurt een MS-CHAP v2-provocatiebericht: EAP-request/EAP-Type=EAP MS-CHAP-V2 (Challenge).
4. De client reageert met een uitdaging en antwoord van MS-CHAP v2: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response).
5. De IAS-server stuurt een MS-CHAP v2-succespakket terug wanneer de server de client met succes heeft geverifieerd: EAP-request/EAP-Type=EAP-MS-CHAP-V2 (Success).
6. De client reageert met een succespakket van MS-CHAP v2 wanneer de client de server met succes heeft geverifieerd: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Success).
7. De IAS-server stuurt een EAP-TLV die een geslaagde verificatie aangeeft.
8. De client reageert met een EAP-TLV-statusbericht.
9. De server voltooit de verificatie en verstuurt een EAP-Success-bericht met behulp van plaintext. Als VLAN's worden geïmplementeerd voor client-isolatie, zijn de VLAN-kenmerken in dit bericht opgenomen.

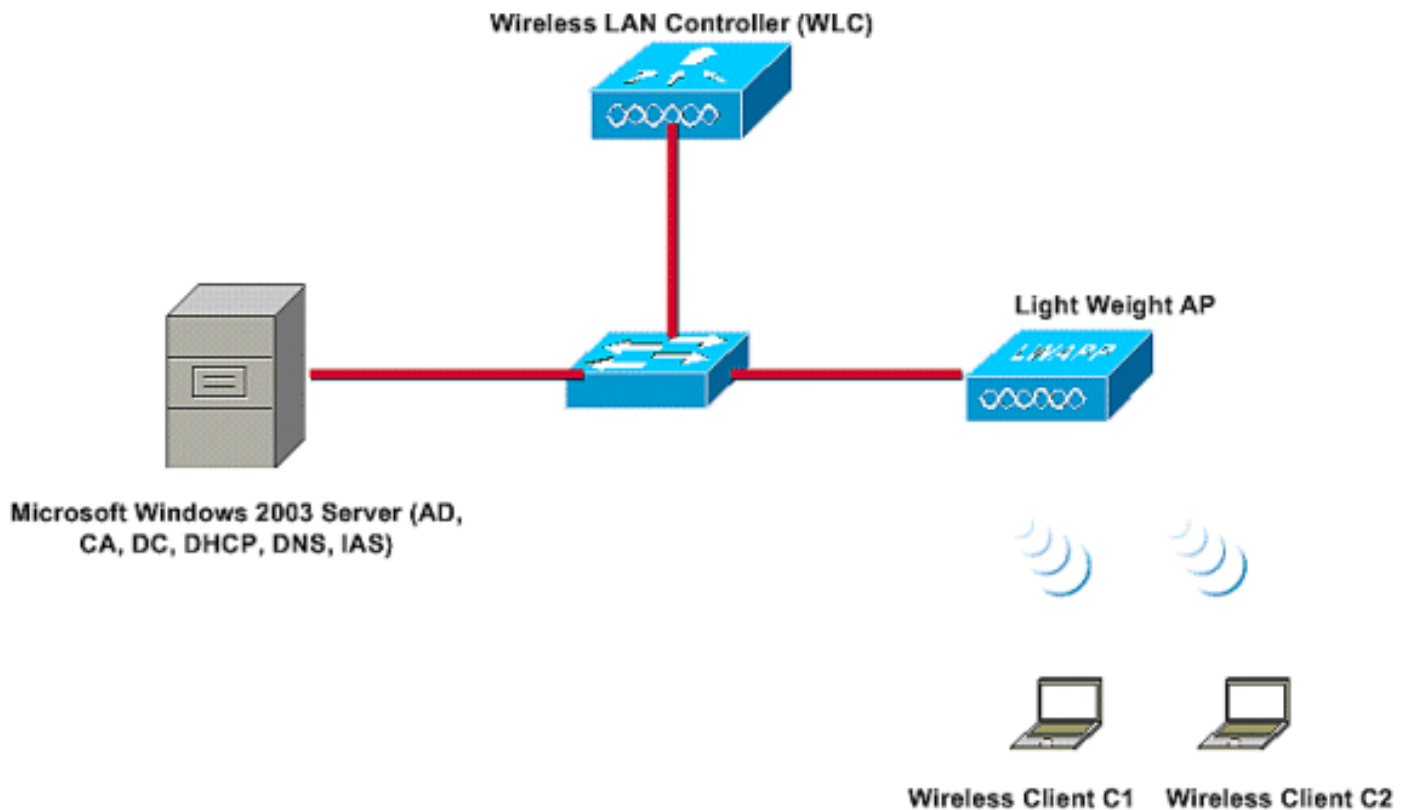
Configureren

Dit document biedt een voorbeeld voor de configuratie van PEAP MS-CHAP v2.

Opmerking: Gebruik de [Command Lookup Tool \(alleen voor geregistreerde klanten\)](#) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



In deze installatie worden deze rollen uitgevoerd door een Microsoft Windows 2003-server:

- Domeincontroller voor het domein **Wireless.com**
- DHCP-/DNS-server
- CA-server (Certificate Authority)
- Active Directory - voor het onderhouden van de gebruikersdatabase
- Internetverificatieservice (IAS) - voor het verifiëren van de draadloze gebruikers

Deze server verbindt met het bekabelde netwerk via een Layer 2 switch zoals getoond.

De draadloze LAN-controller (WLC) en de geregistreerde LAP maken ook verbinding met het netwerk via Layer 2 switch.

Draadloze clients C1 en C2 gebruiken Wi-Fi Protected Access 2 (WPA2) - PEAP MSCHAP v2-verificatie om verbinding te maken met het draadloze netwerk.

Het doel is om de Microsoft 2003-server, draadloze LAN-controller en Light Weight AP te configureren om de draadloze clients te verifiëren met PEAP MSCHAP v2-verificatie.

In het volgende gedeelte wordt uitgelegd hoe u de apparaten voor deze installatie kunt configureren.

Configuraties

In deze sectie wordt gekeken naar de configuratie die nodig is om PEAP MS-CHAP v2-verificatie in dit WLAN in te stellen:

- De Microsoft Windows 2003-server configureren
- Configureer de draadloze LAN-controller (WLC) en de lichtgewicht AP's
- De draadloze clients configureren

Start met de configuratie van de Microsoft Windows 2003-server.

[De Microsoft Windows 2003-server configureren](#)

[De Microsoft Windows 2003-server configureren](#)

Zoals in het gedeelte Network Setup is vermeld, gebruikt u de Microsoft Windows 2003-server in het netwerk om deze functies uit te voeren.

- **Domain Controller** - voor het domein **Wireless**
- **DHCP-/DNS-server**
- **CA-server (Certificate Authority)**
- **Internetverificatieservice (IAS)** - voor het verifiëren van de draadloze gebruikers
- **Active Directory** - voor het onderhouden van de gebruikersdatabase

Configureer de Microsoft Windows 2003-server voor deze services. Begin met de configuratie van de Microsoft Windows 2003-server als een Domain Controller.

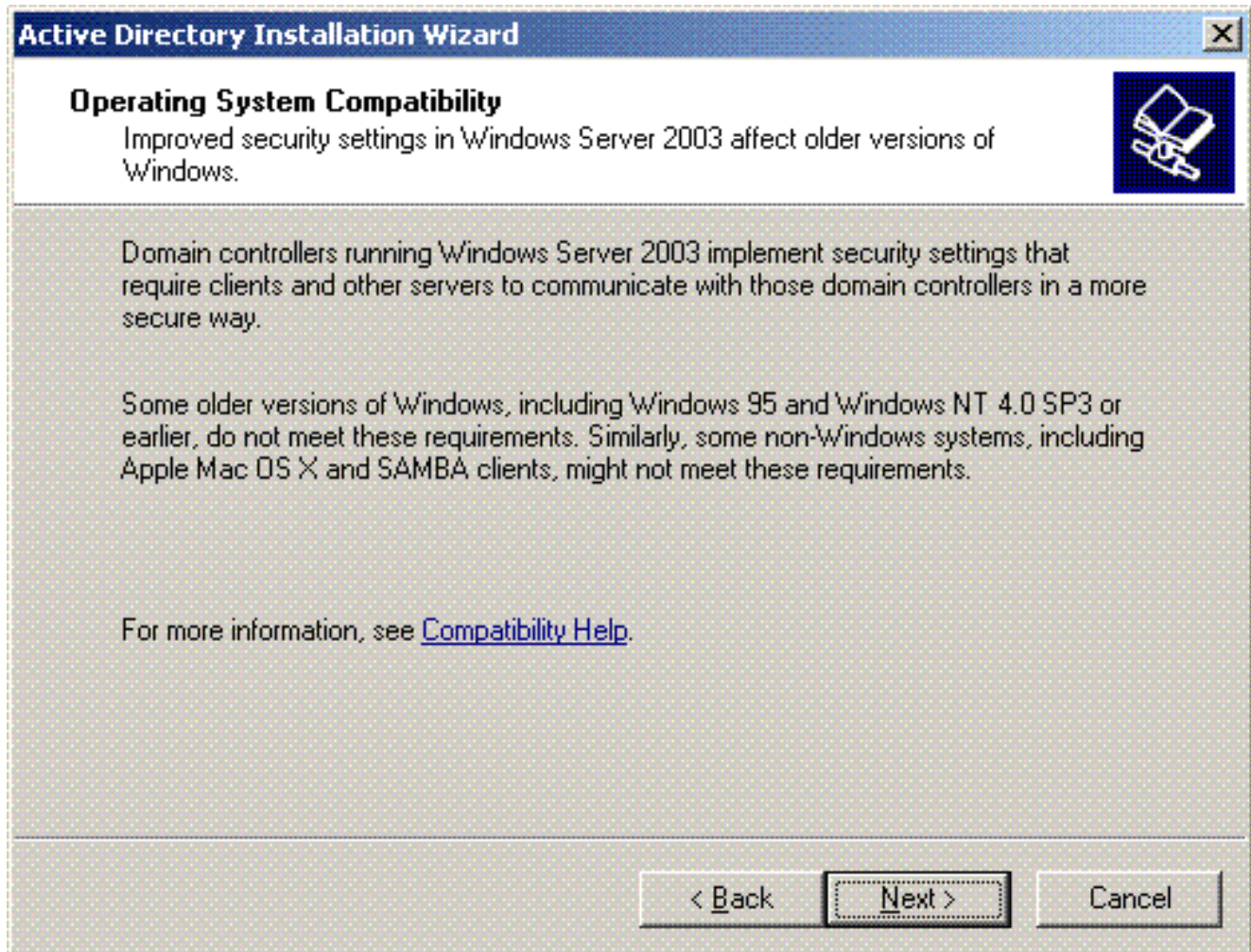
De Microsoft Windows 2003-server configureren als domeincontroller

Voltooi de volgende stappen om de Microsoft Windows 2003-server als een domeincontroller te configureren:

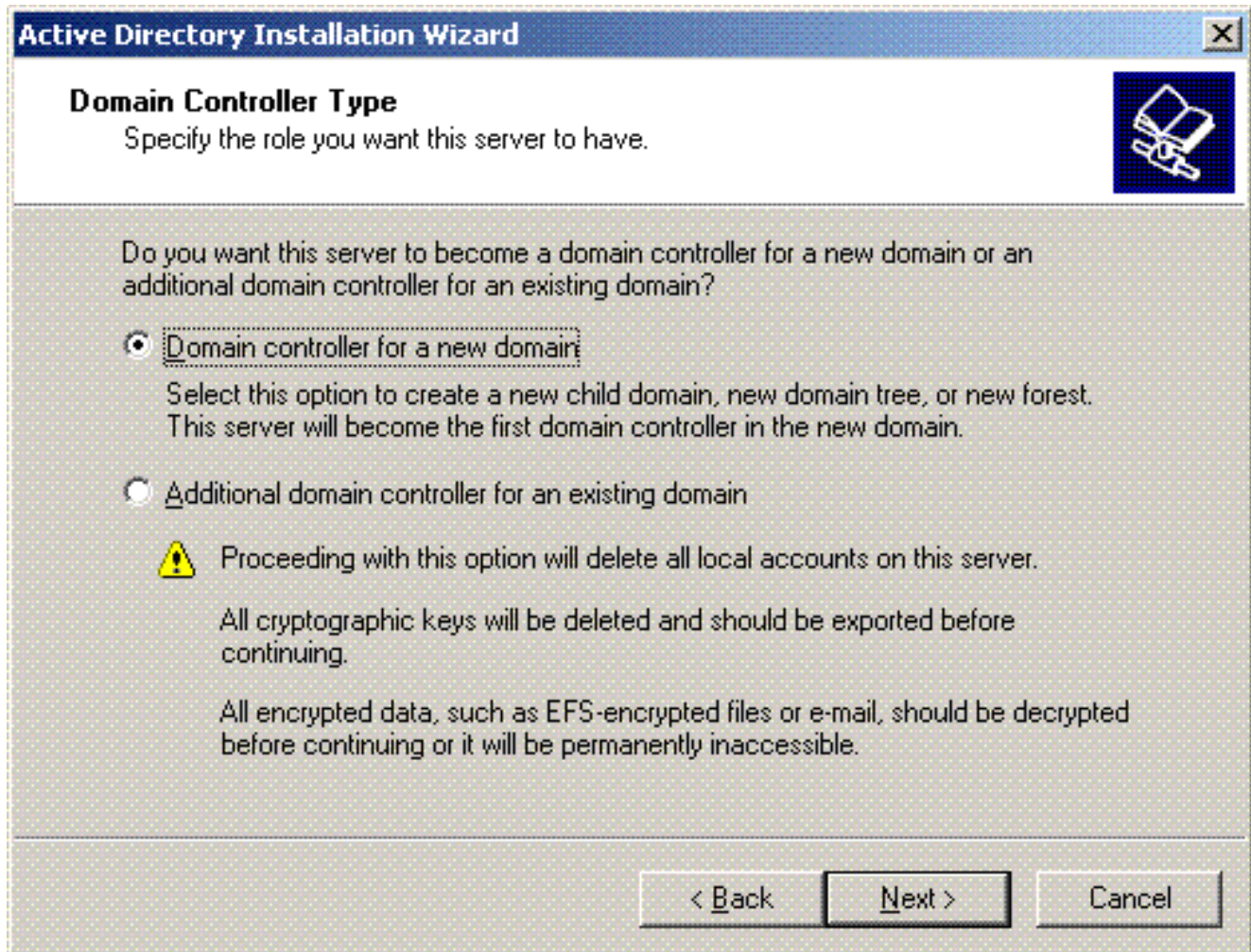
1. Klik op **Start**, klik op **Uitvoeren**, typ **dcpromo.exe**, en klik vervolgens op **OK** om de installatiewizard van Active Directory te starten.



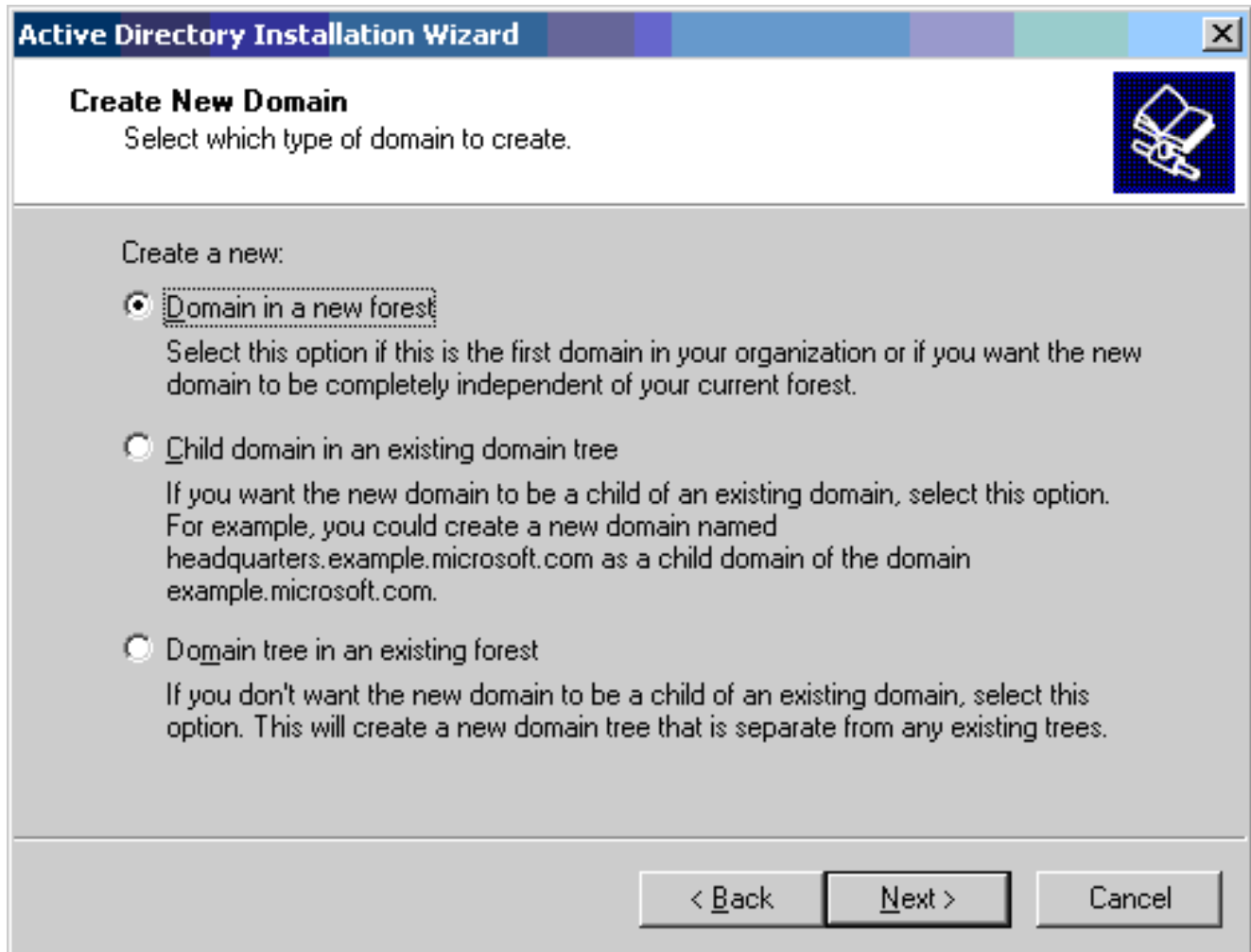
2. Klik op **Next** om de installatiewizard van Active Directory uit te voeren.



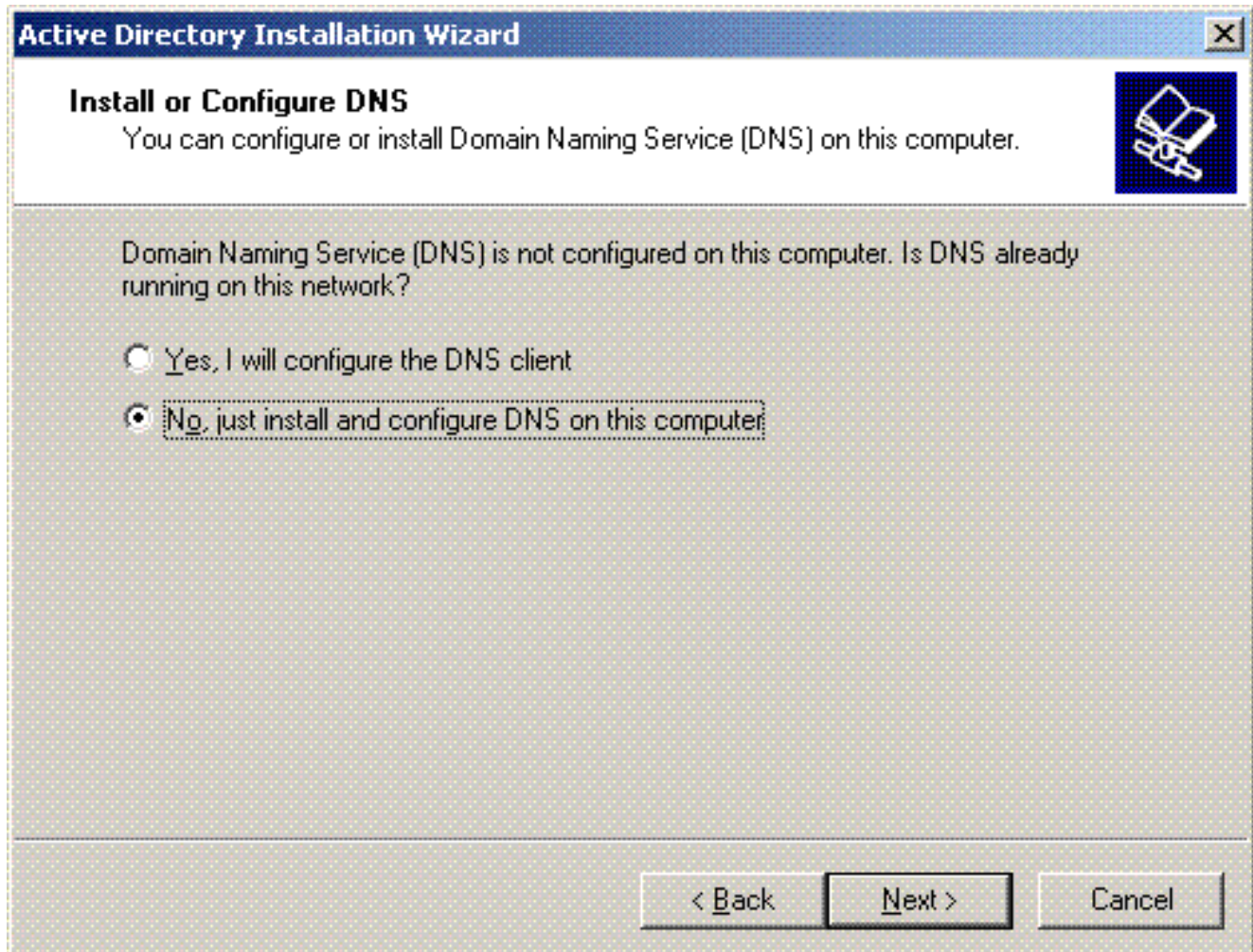
3. Kies de optie **Domeincontroller** voor een nieuw domein om een nieuw domein te maken.



4. Klik op **Volgende** om een nieuw bos met domeinbomen te maken.



5. Als DNS niet op het systeem is geïnstalleerd, biedt de wizard u opties om DNS te configureren. Kies **Nee, Installeer en configureer DNS op deze computer**. Klik op **Next (Volgende)**.



6. Typ de volledige DNS-naam voor het nieuwe domein. In dit voorbeeld wordt **Wireless.com** gebruikt en klikt u op **Volgende**.

Active Directory Installation Wizard [X]

New Domain Name
Specify a name for the new domain.

Type the full DNS name for the new domain
(for example: headquarters.example.microsoft.com).

Full DNS name for new domain:

< Back Next > Cancel

7. Voer de NETBIOS-naam in voor het domein en klik op **Volgende**. In dit voorbeeld wordt **DRAADLOOS** gebruikt.

Active Directory Installation Wizard

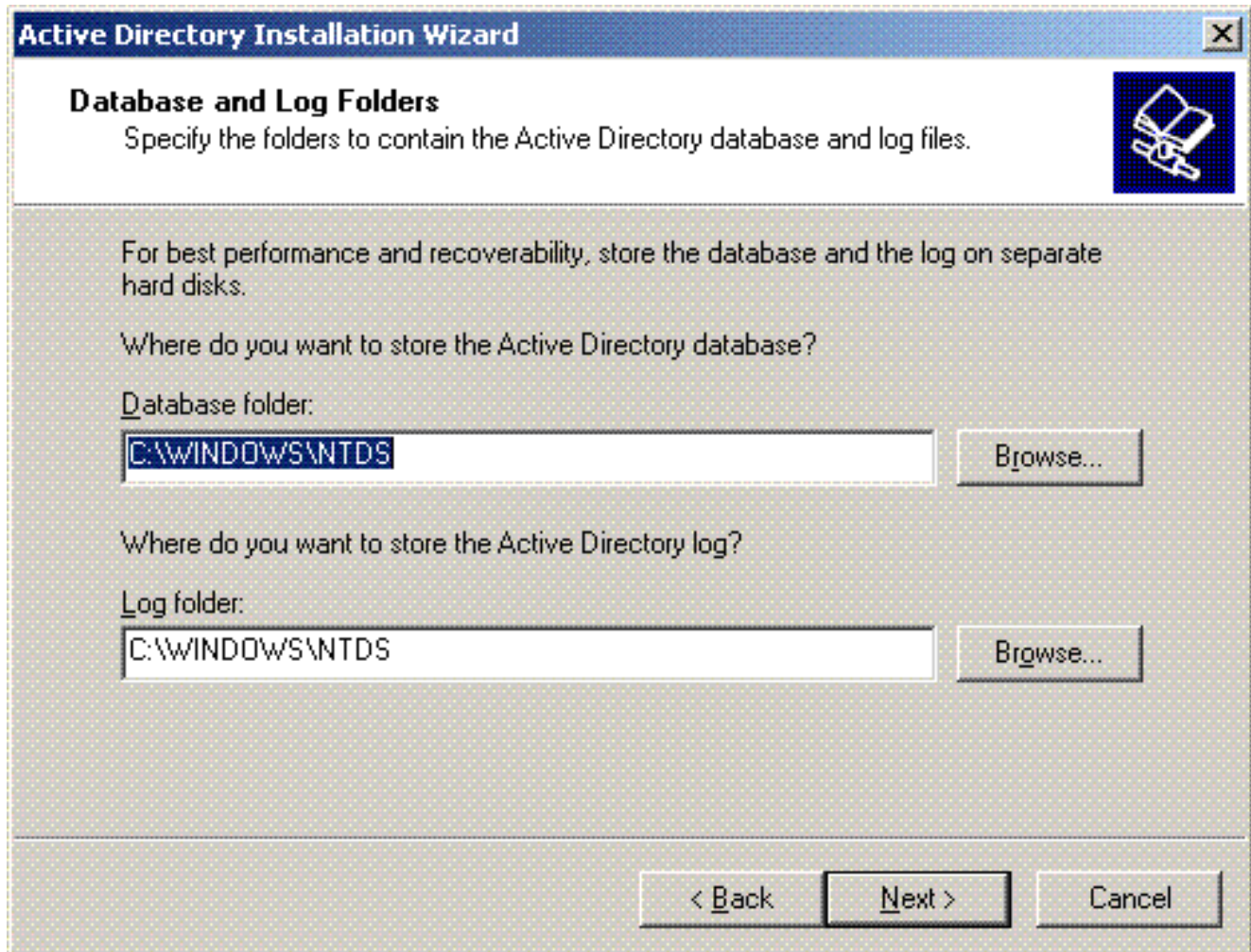
NetBIOS Domain Name
Specify a NetBIOS name for the new domain.

This is the name that users of earlier versions of Windows will use to identify the new domain. Click Next to accept the name shown, or type a new name.

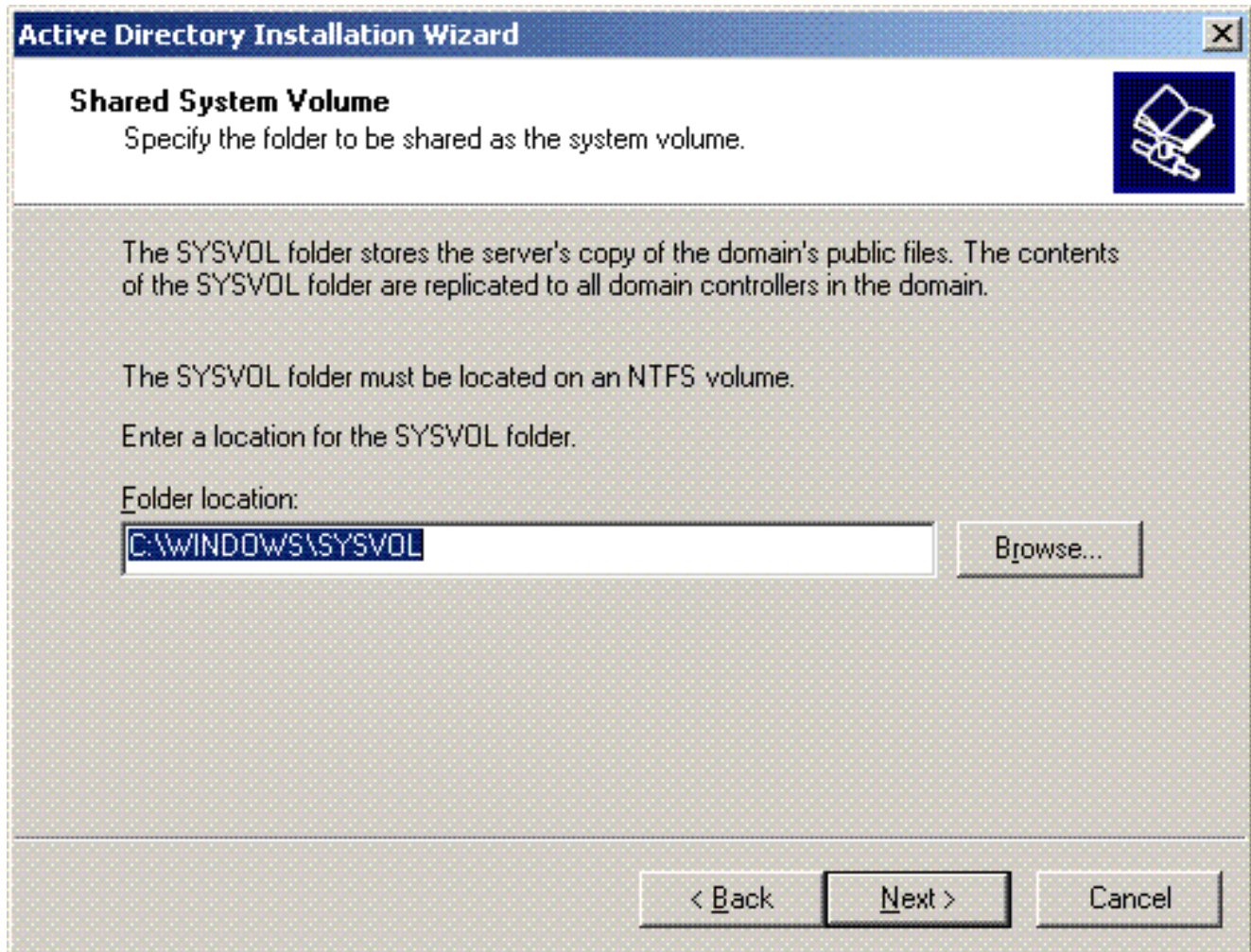
Domain NetBIOS name:

< Back Next > Cancel

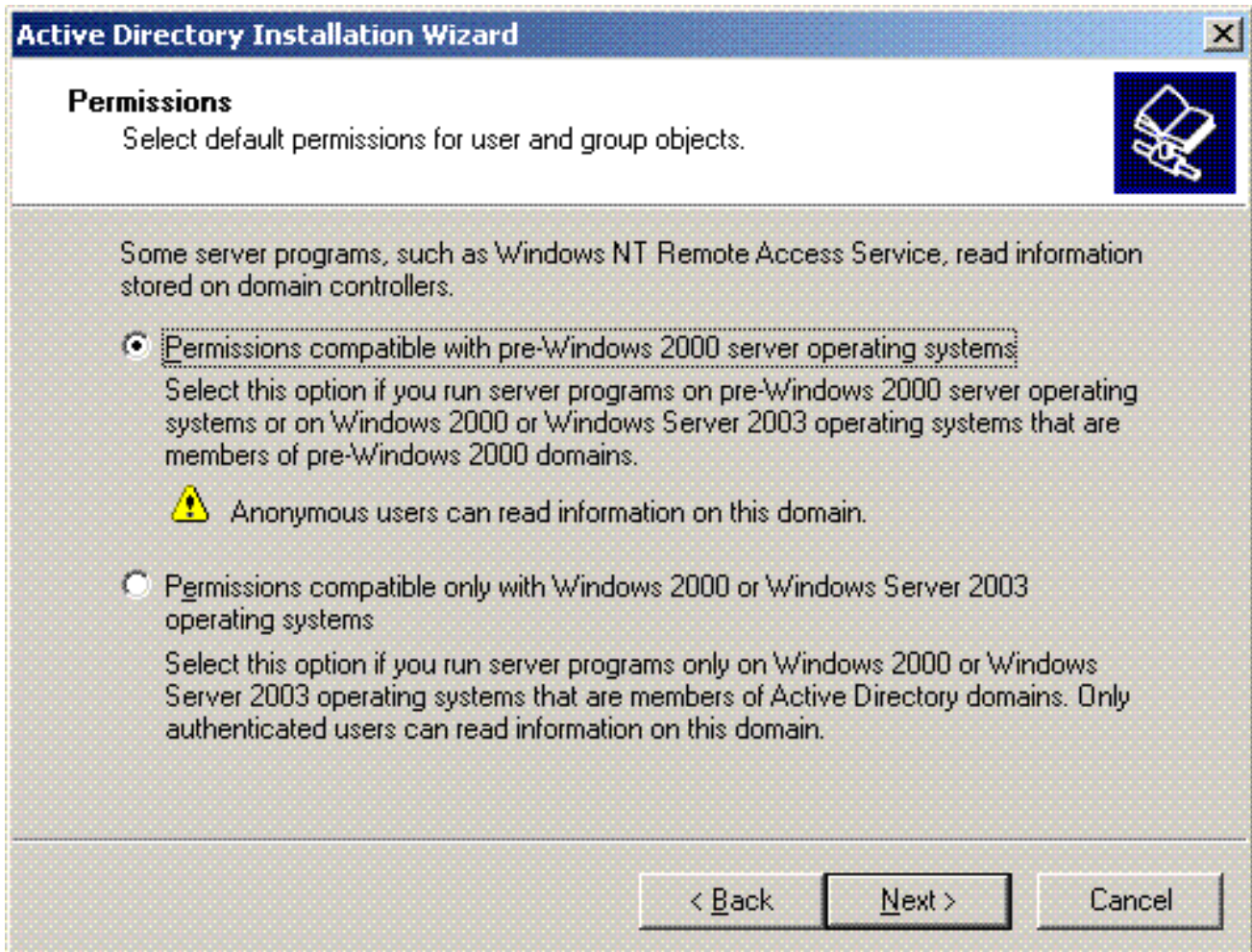
8. Kies de database en loglocaties voor het domein. Klik op **Next** (Volgende).



9. Kies een locatie voor de map Sysvol. Klik op **Next** (Volgende).



10. Kies de standaardrechten voor de gebruikers en groepen. Klik op **Next** (Volgende).



11. Stel het beheerderwachtwoord in en klik op **Volgende**.

Active Directory Installation Wizard

Directory Services Restore Mode Administrator Password

This password is used when you start the computer in Directory Services Restore Mode.

Type and confirm the password you want to assign to the Administrator account used when this server is started in Directory Services Restore Mode.

The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both.

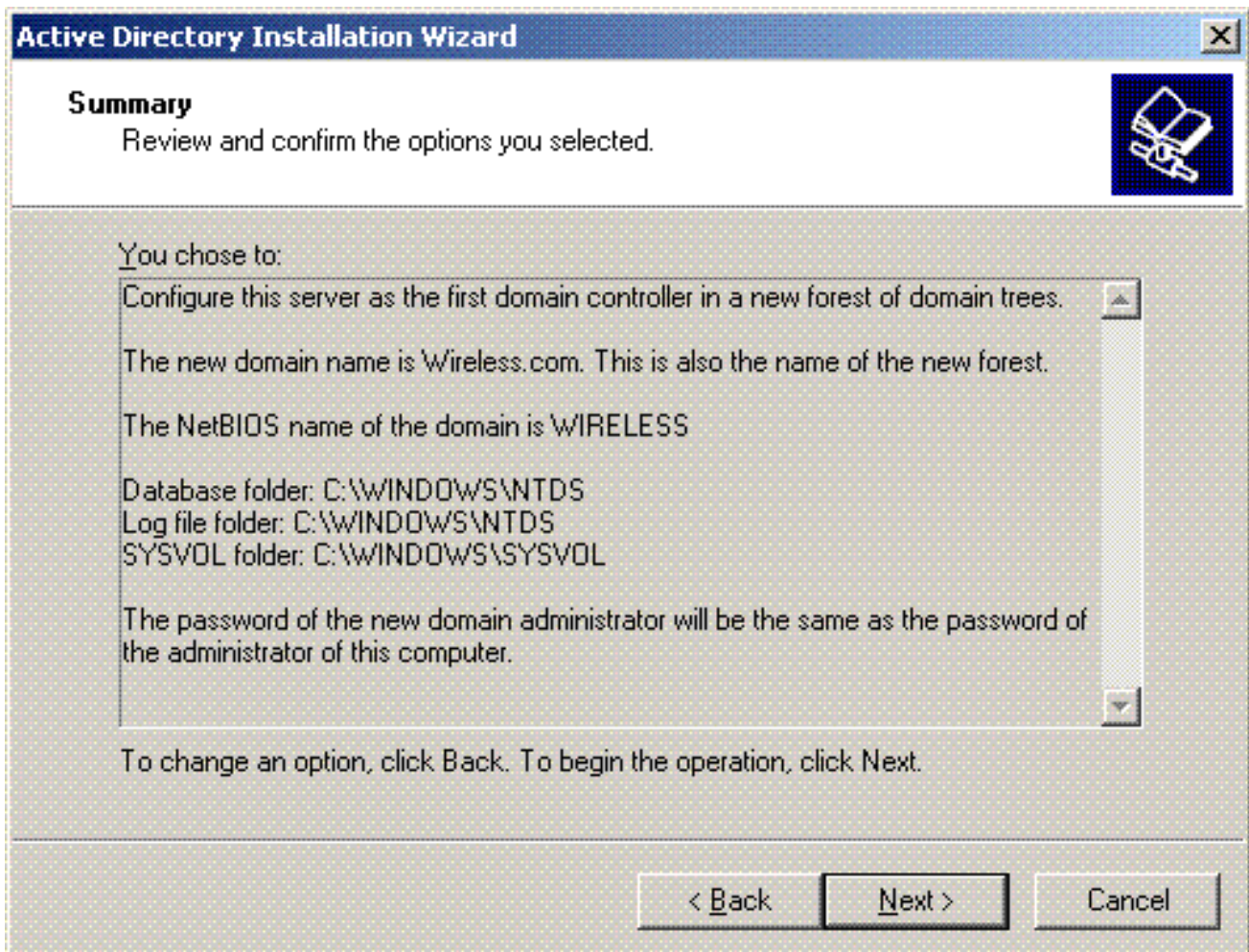
Restore Mode Password:

Confirm password:

For more information about Directory Services Restore Mode, see [Active Directory Help](#).

< Back Next > Cancel

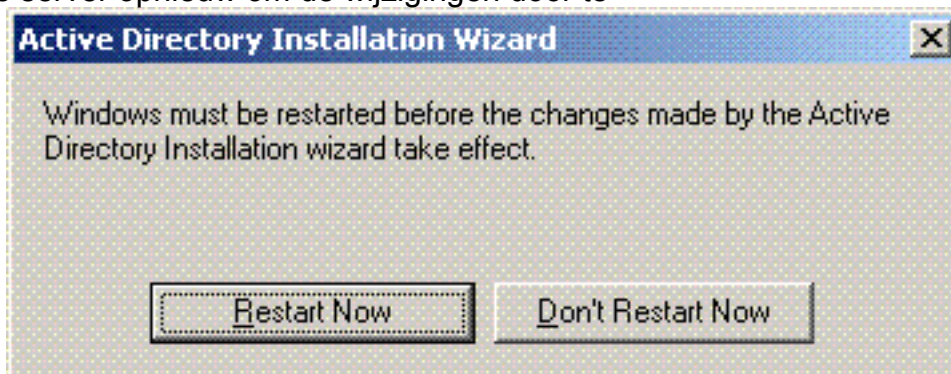
12. Klik op **Volgende** om de eerder ingestelde Domain Options te accepteren.



13. Klik op **Voltooien** om de installatiewizard van Active Directory te sluiten.



14. Start de server opnieuw om de wijzigingen door te



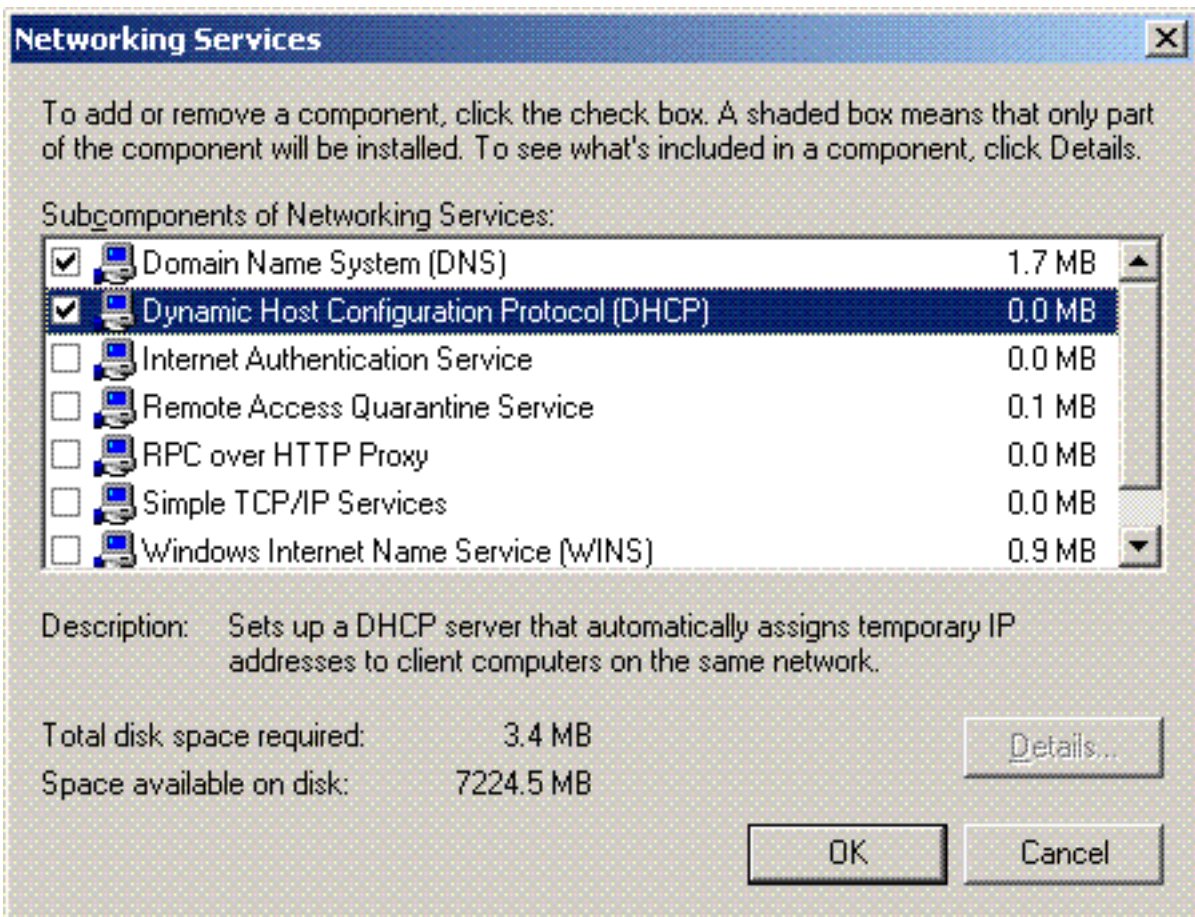
voeren.

Met deze stap hebt u de Microsoft Windows 2003-server geconfigureerd als een Domain Controller en een nieuw domein gemaakt voor **Wireless.com**. Configureer vervolgens DHCP-services op de server.

[DHCP-services installeren en configureren op de Microsoft Windows 2003-server](#)

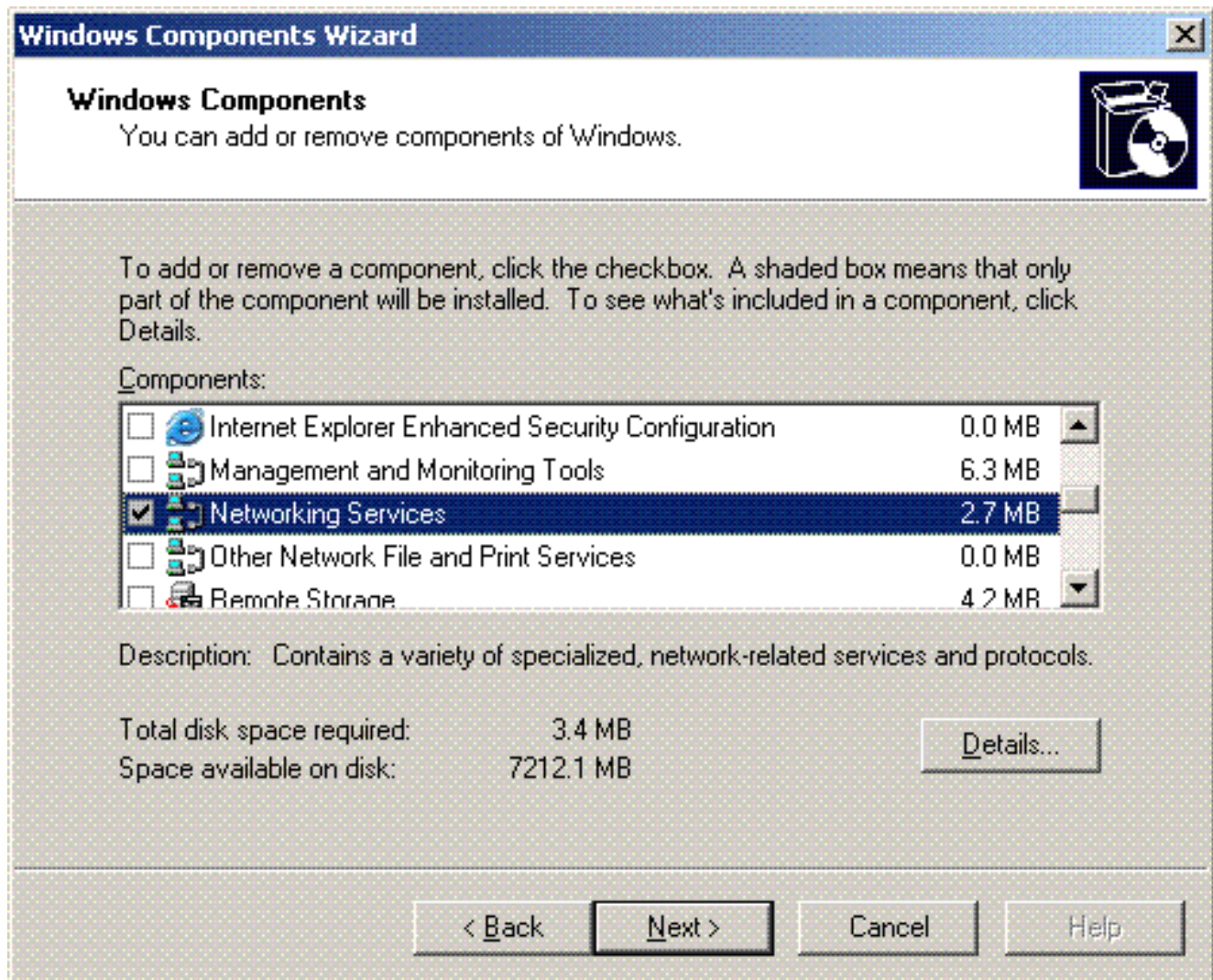
De DHCP-service op de Microsoft 2003-server wordt gebruikt om IP-adressen aan de draadloze clients te leveren. Voltooi de volgende stappen om de DHCP-services op deze server te installeren en te configureren:

1. Klik op **Software** in het Configuratiescherm.
2. Klik op **Windows-onderdelen toevoegen of verwijderen**.
3. Kies **Netwerkservices** en klik op **Details**.
4. Kies **Dynamic Host Configuration Protocol (DHCP)** en klik op



OK.

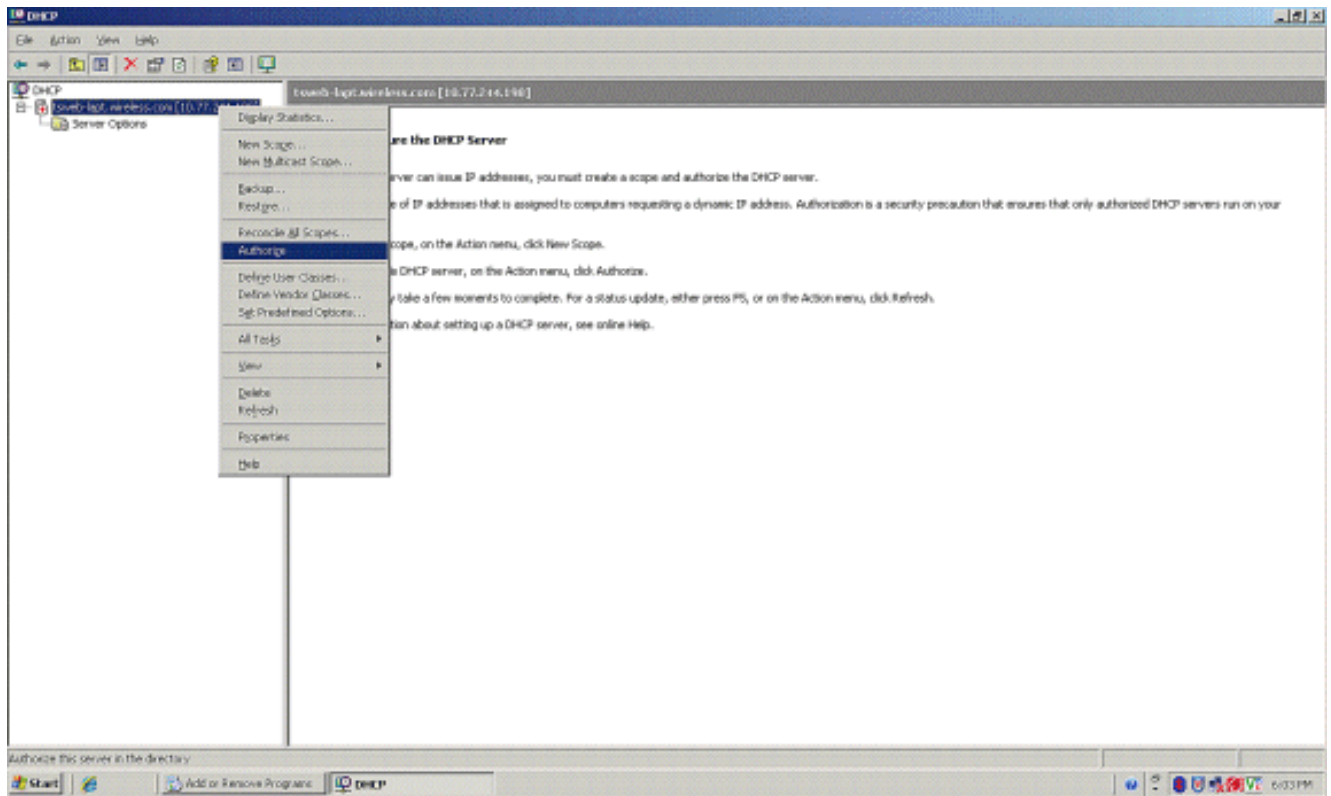
5. Klik op **Next** om de DHCP-service te installeren.



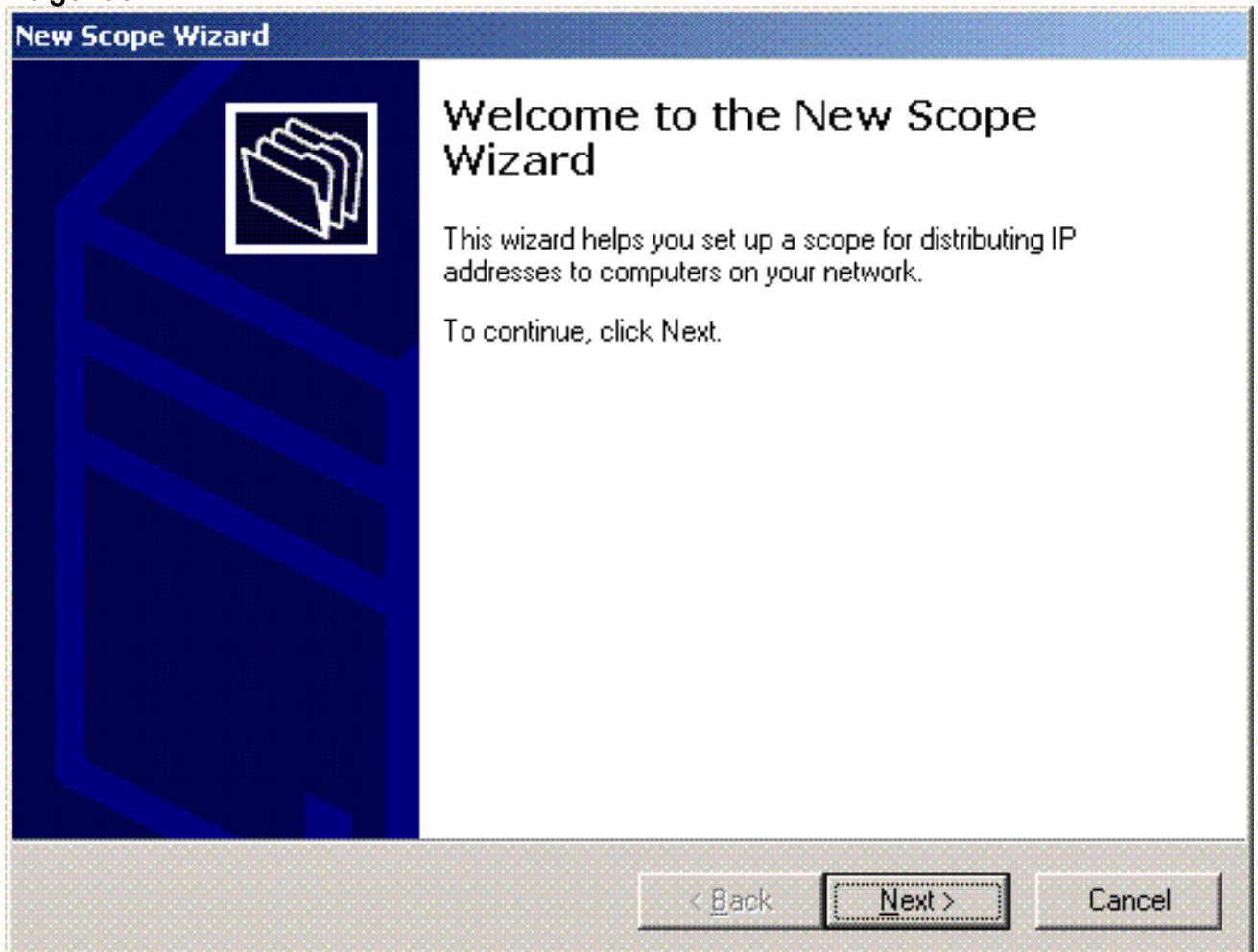
6. Klik op **Voltoeien** om de installatie te voltooien.



7. Om de DHCP-services te configureren klikt u op **Start > Programma's > Systeembeheer** en klikt u op de invoegtoepassing **DHCP**.
8. Kies de DHCP-server - **tsweb-lapt.wireless.com** (in dit voorbeeld).
9. Klik op **Actie** en klik vervolgens op **Autoriseren** om DHCP-service te autoriseren.



10. Klik in de consolestructuur met de rechtermuisknop op **tsweb-lapt.wireless.com** en klik vervolgens op **New Scope** om een IP-adresbereik voor de draadloze clients te definiëren.
11. Klik op de pagina Welkom bij de wizard Nieuw bereik van de wizard Nieuw bereik op **Volgende**.



12. Typ op de pagina Naam bereik de naam van de DHCP-scope. In dit voorbeeld, gebruik **DHCP-Clients** als de scope naam. Klik op **Next**

(Volgende).

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: DHCP-Clients

Description: DHCP Server for Wireless Clients

< Back Next > Cancel

13. Voer op de pagina IP-adresbereik de begin- en eindadressen voor de scope in en klik op **Volgende**.

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: 10 . 77 . 244 . 218

End IP address: 10 . 77 . 244 . 219

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: 8

Subnet mask: 255 . 0 . 0 . 0

< Back

Next >

Cancel

14. Vermeld op de pagina Uitsluitingen toevoegen het IP-adres dat u wilt reserveren/uitsluiten van het DHCP-bereik. Klik op **Next** (Volgende).

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:

Add

Excluded address range:

Remove

< Back

Next >

Cancel

15. Vermeld de leasduur op de pagina Leaseduur en klik op **Volgende**.

New Scope Wizard

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.



Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days:	Hours:	Minutes:
<input type="text" value="8"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

< Back

Next >

Cancel

16. Kies op de pagina DHCP-opties configureren **Ja, ik wil DHCP-optie nu configureren** en klik op **Volgende**.

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

17. Als er een standaardgatewayrouter is, vermeld dan het IP-adres van de gatewayrouter op de pagina Router (Default Gateway) en klik op **Next**.

New Scope Wizard

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

Remove

Up

Down

< Back

Next >

Cancel

18. Typ op de pagina Domain Name en DNS servers de naam van het domein dat eerder is geconfigureerd. Gebruik in het voorbeeld **Wireless.com**. Voer het IP-adres van de server in. Klik op **Add** (Toevoegen).

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:

IP address:

Add

Resolve

Remove

Up

Down

< Back

Next >

Cancel

19. Klik op **Next** (Volgende).
20. Klik op de pagina WINS Server op **Volgende**.
21. Kies **Ja** op de pagina Werkingsgebied activeren, **ik wil het bereik nu activeren** en klik op **Volgende**.

New Scope Wizard

Activate Scope

Clients can obtain address leases only if a scope is activated.



Do you want to activate this scope now?

- Yes, I want to activate this scope now
- No, I will activate this scope later

< Back

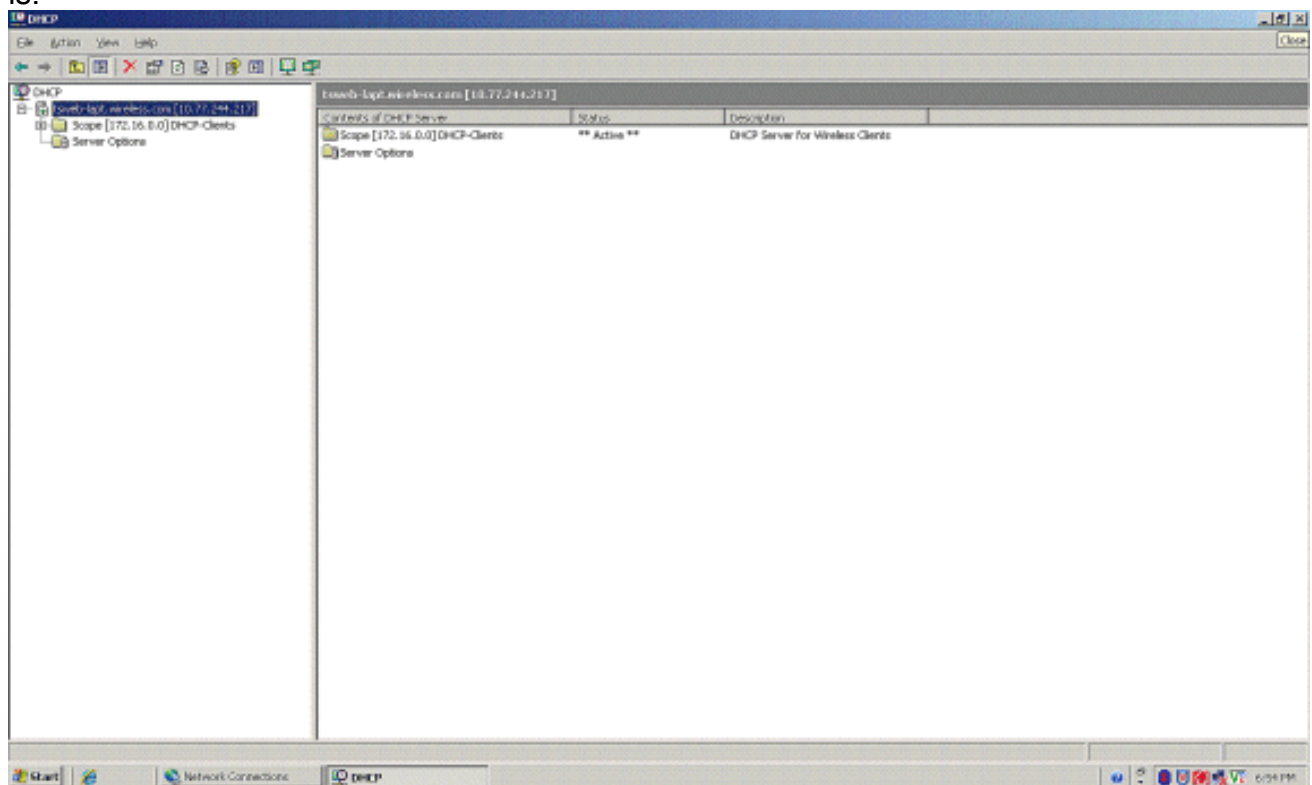
Next >

Cancel

22. Klik op **Voltooien** om de wizard Nieuw bereik te voltooien.



23. Controleer in het venster DHCP Snapin of het DHCP-bereik dat is gemaakt actief is.



Nu DHCP/ DNS is ingeschakeld op de server, moet u de server configureren als een ECA-server (Enterprise Certificate Authority).

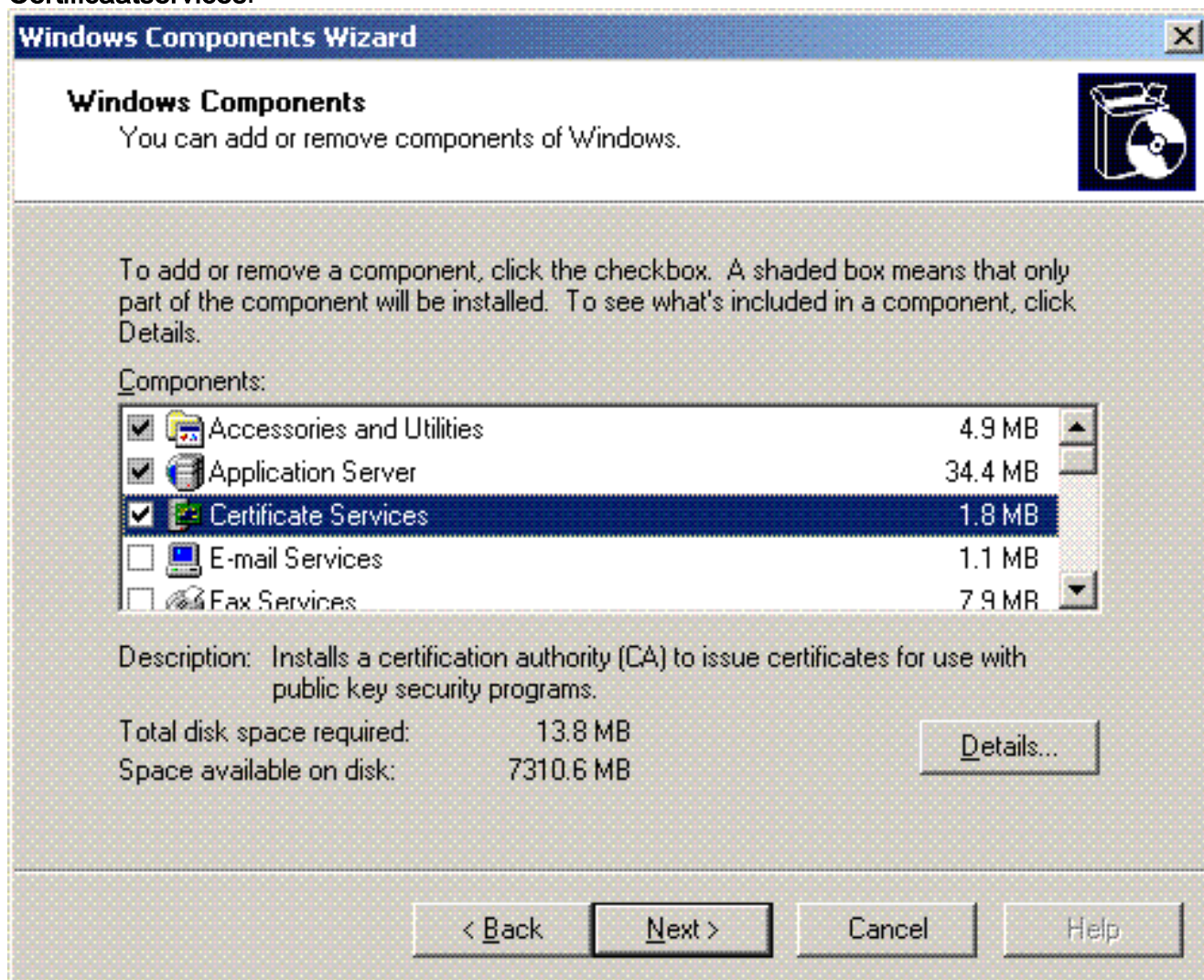
[De Microsoft Windows 2003-server installeren en configureren als een](#)

certificeringsinstantie (CA)-server

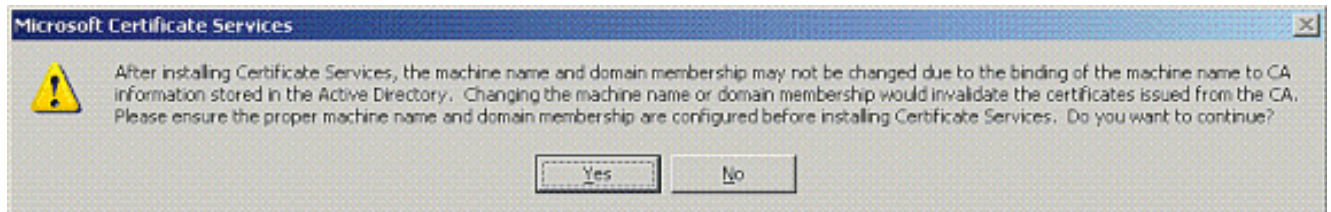
PEAP met EAP-MS-CHAPv2 valideert de RADIUS-server op basis van het certificaat dat op de server aanwezig is. Bovendien moet het servercertificaat worden afgegeven door een openbare certificeringsinstantie (CA) die wordt vertrouwd door de clientcomputer (dat wil zeggen dat het openbare CA-certificaat al bestaat in de map Trusted Root Certification Authority op het certificaatarchief van de clientcomputer). In dit voorbeeld moet u de Microsoft Windows 2003-server configureren als een certificeringsinstantie (CA) die het certificaat afgeeft aan de Internet Verification Service (IAS).

Voltooi de volgende stappen om de certificaatservices op de server te installeren en te configureren:

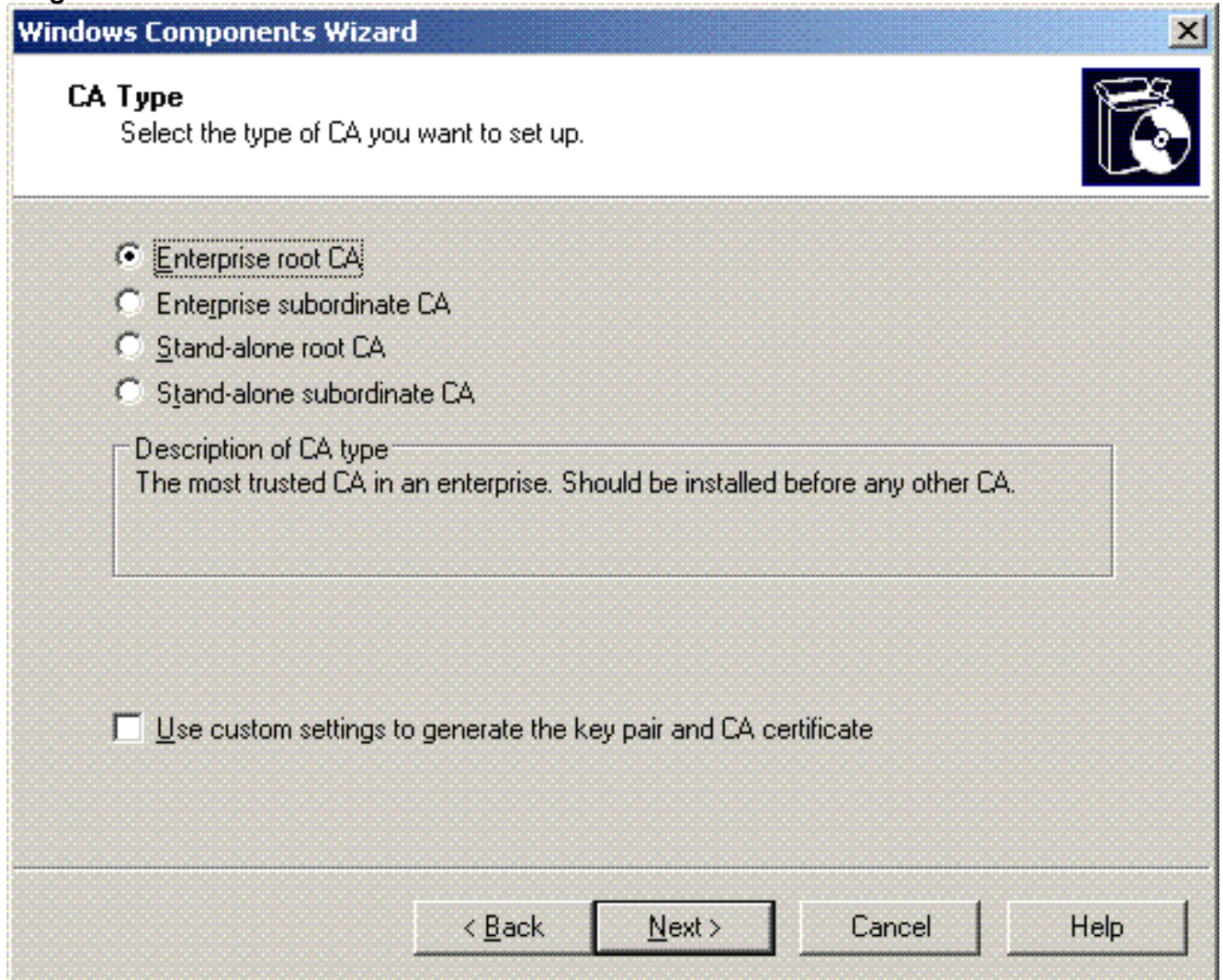
1. Klik op **Software** in het Configuratiescherm.
2. Klik op **Windows-onderdelen toevoegen of verwijderen**.
3. Klik op **Certificaatservices**.



4. Klik op **Ja** om het waarschuwingsbericht te **waarschuwen**. Na het installeren van **certificaatservices** kan de computer niet hernoemd worden en kan de computer niet worden toegevoegd aan of verwijderd worden uit een domein. Wilt u doorgaan?



5. Kies onder Certificate Authority Type de **Enterprise root CA**, en klik op **Volgende**.



6. Voer een naam in om de CA te identificeren. In dit voorbeeld wordt **Wireless-AC** gebruikt. Klik op **Next** (Volgende).

Windows Components Wizard

CA Identifying Information
Enter information to identify this CA.

Common name for this CA:
Wireless-CA

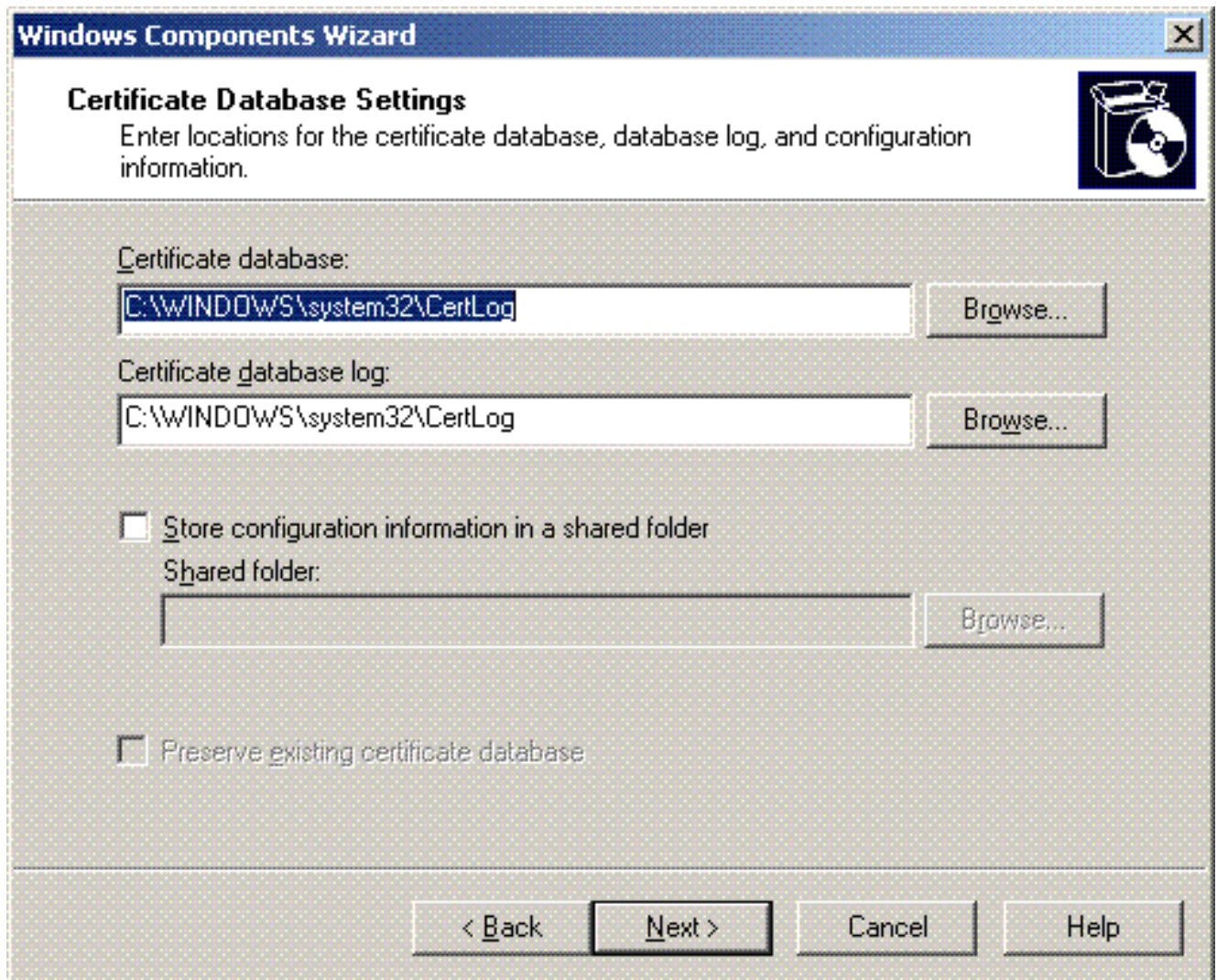
Distinguished name suffix:
DC=Wireless,DC=com

Preview of distinguished name:
CN=Wireless-CA,DC=Wireless,DC=com

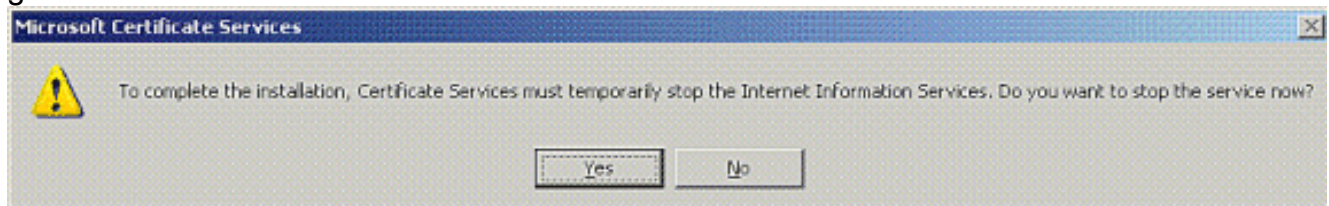
Validity period: 5 Years Expiration date: 12/12/2012 7:01 PM

< Back Next > Cancel Help

7. Er wordt een directory "Cert Log" aangemaakt voor de opslag van de certificaatdatabase.
Klik op **Next**
(Volgende).



8. Als IIS is ingeschakeld, moet dit worden gestopt voordat u doorgaat. Klik op **OK** om te waarschuwen dat IIS moet worden gestopt. Het start automatisch opnieuw nadat CA is geïnstalleerd.



9. Klik op **Voltoeien** om de installatie van de CA-diensten (Certificate Authority) te voltooien.

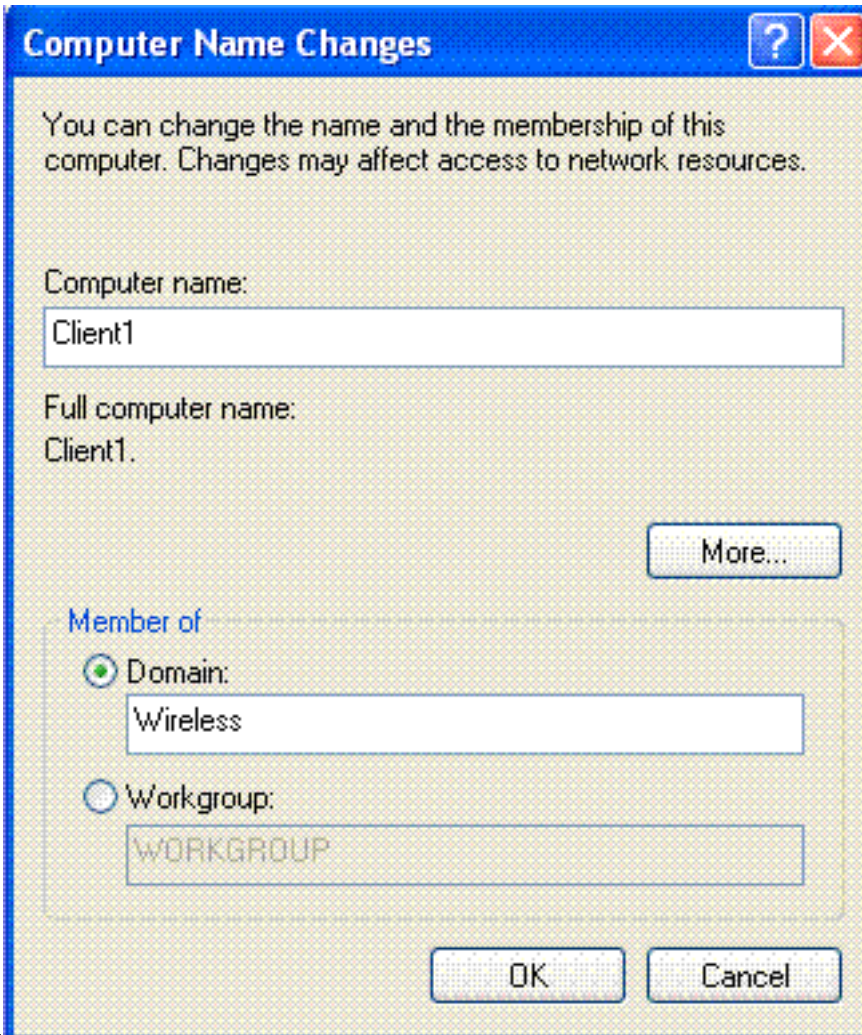


De volgende stap is het installeren en configureren van de Internet-verificatieservice op de Microsoft Windows 2003-server.

[Clients met domein verbinden](#)

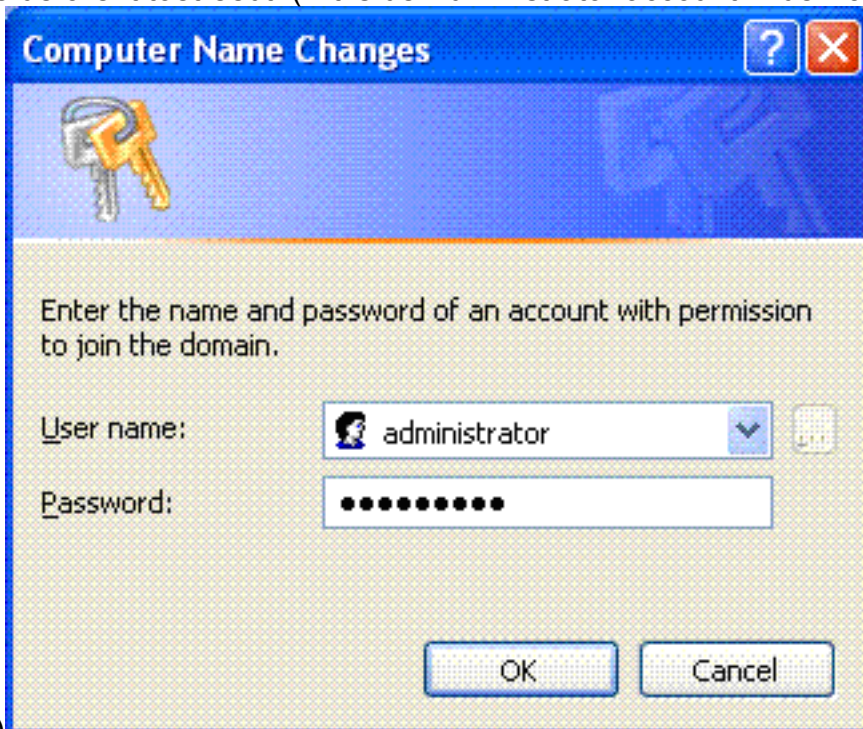
De volgende stap is om de clients te verbinden met het bekabelde netwerk en de domeinspecifieke informatie van het nieuwe domein te downloaden. Met andere woorden, verbind de cliënten met het domein. Voltooi de volgende stappen om dit te doen:

1. Sluit de clients aan op het bekabelde netwerk met een rechtstreekse Ethernet-kabel.
2. Start de client op en log in met de gebruikersnaam/ het wachtwoord van de client.
3. Klik op **Start**; klik op **Uitvoeren**; type **cmd**; en klik op **OK**.
4. Typ **ipconfig** bij de opdrachtprompt en klik op **Enter** om te verifiëren dat DHCP correct werkt en dat de client een IP-adres van de DHCP-server heeft ontvangen.
5. Om zich bij de cliënt aan het domein aan te sluiten, klik **Mijn Computer met de** rechtermuisknop aan, en kies **Eigenschappen**.
6. Klik op het tabblad **Computer Name**.
7. Klik op **Wijzigen**.
8. Klik op **Domain**; typ **wireless.com**; en klik op



OK.

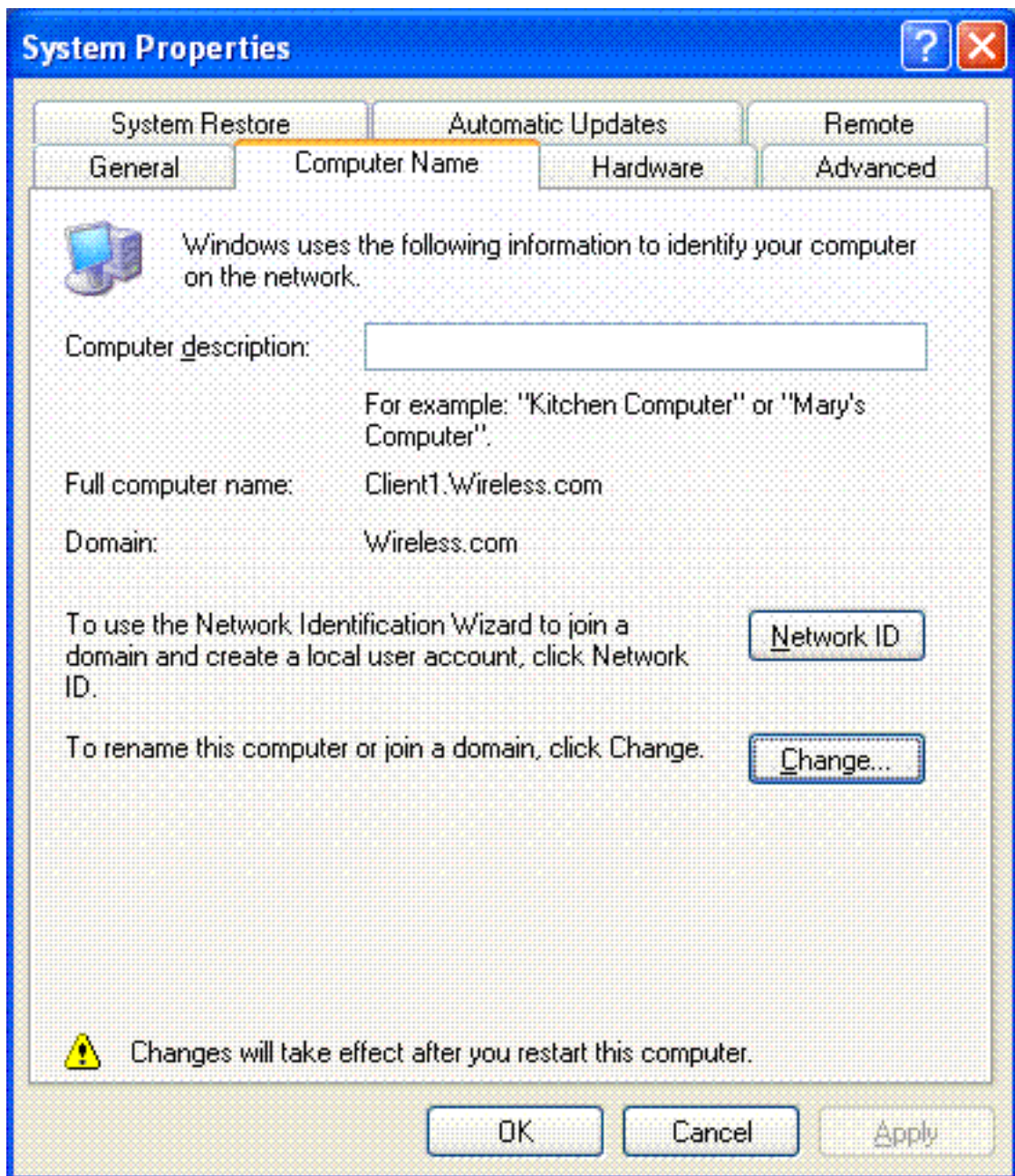
9. Typ **Gebruikersnaam Administrator** en het wachtwoord dat specifiek is voor het domein waartoe de client toetreedt. (Dit is de Administrator-account in de Active Directory op de



server.)



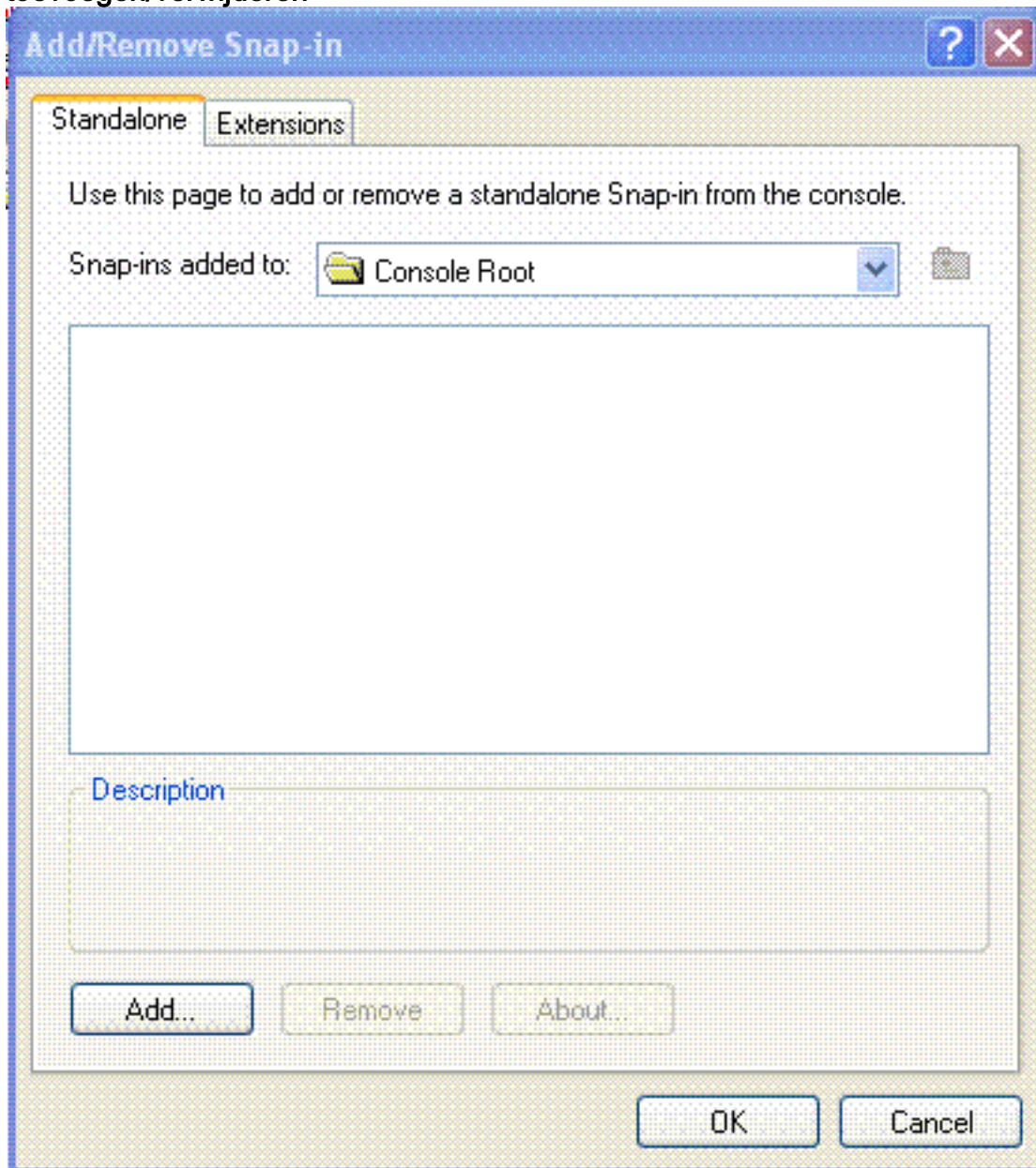
10. Klik op **OK**.
11. Klik op **Ja** om de computer opnieuw op te starten.
12. Log na het opstarten van de computer in met de volgende informatie: Gebruikersnaam = **Beheerder**; Wachtwoord = **<domeinwachtwoord>**; Domein = **Draadloos**.
13. Klik met de rechtermuisknop op **Deze computer** en klik op **Eigenschappen**.
14. Klik op het tabblad **Computer Name** om te controleren of u zich op het Wireless.com-domein



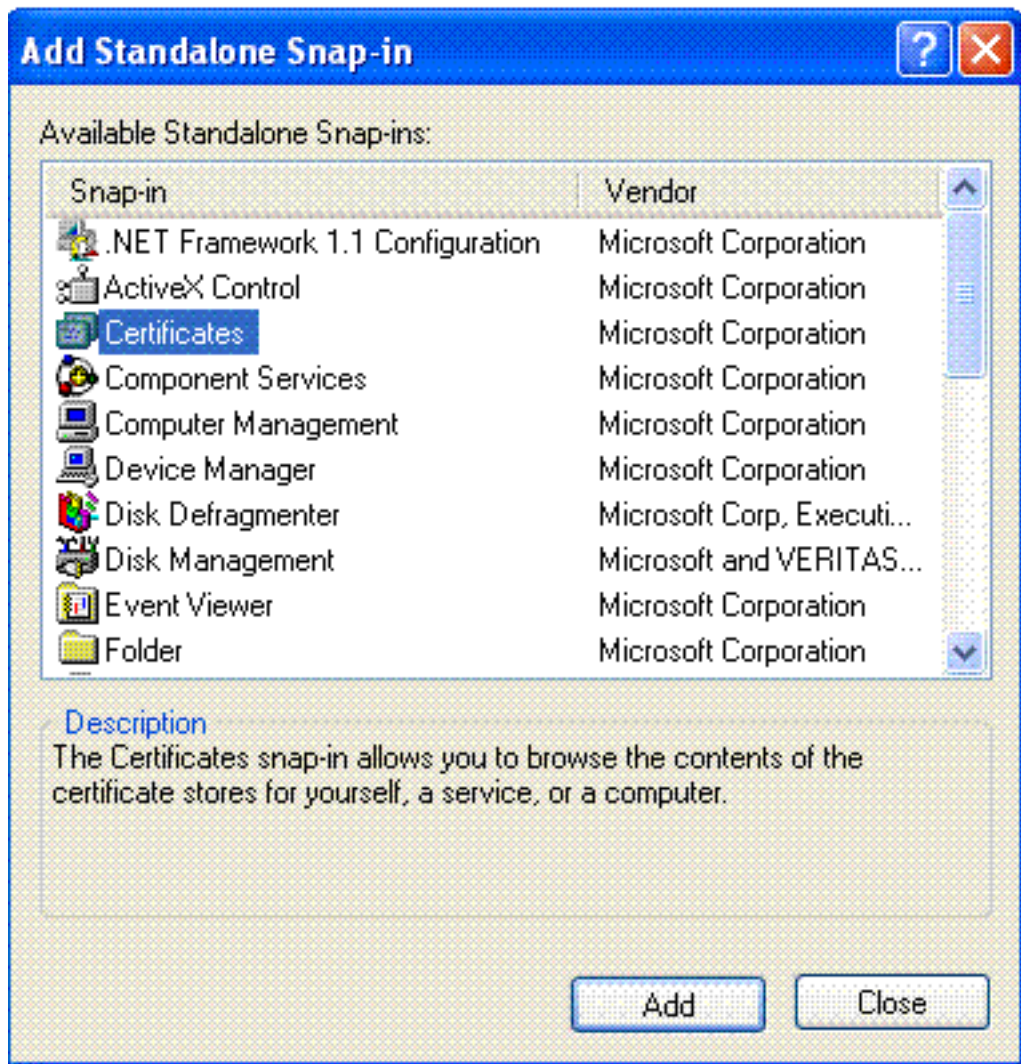
bevindt.

15. De volgende stap is te verifiëren dat de client het CA-certificaat (vertrouwen) van de server heeft ontvangen.
16. Klik op **Start**; klik op **Uitvoeren**; typ **mmc** en klik op **OK**.

17. Klik op **Bestand** en klik op Onverwacht-in toevoegen/verwijderen.

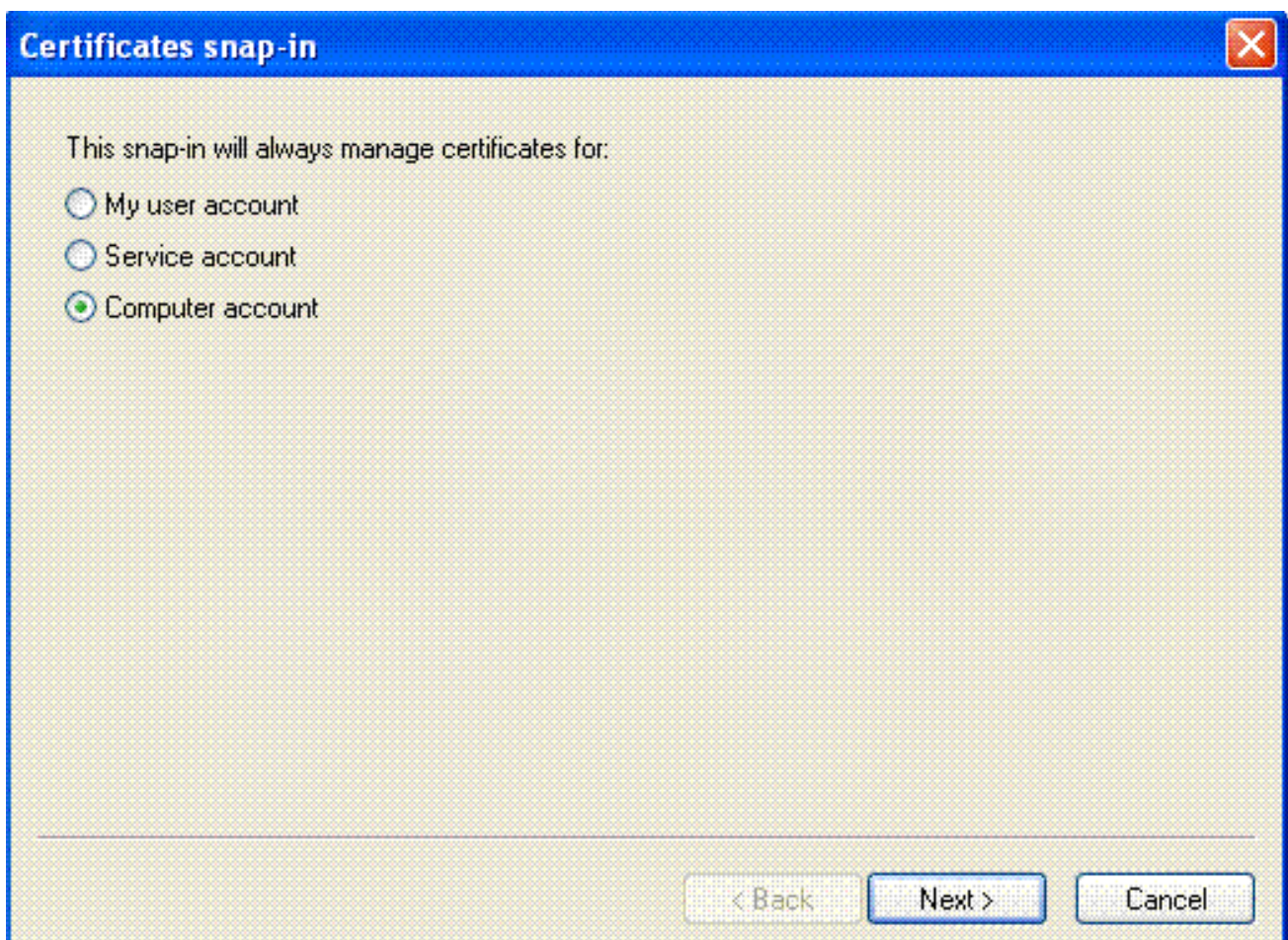


18. Klik op **Add** (Toevoegen).
19. Kies **Certificaat** en klik op

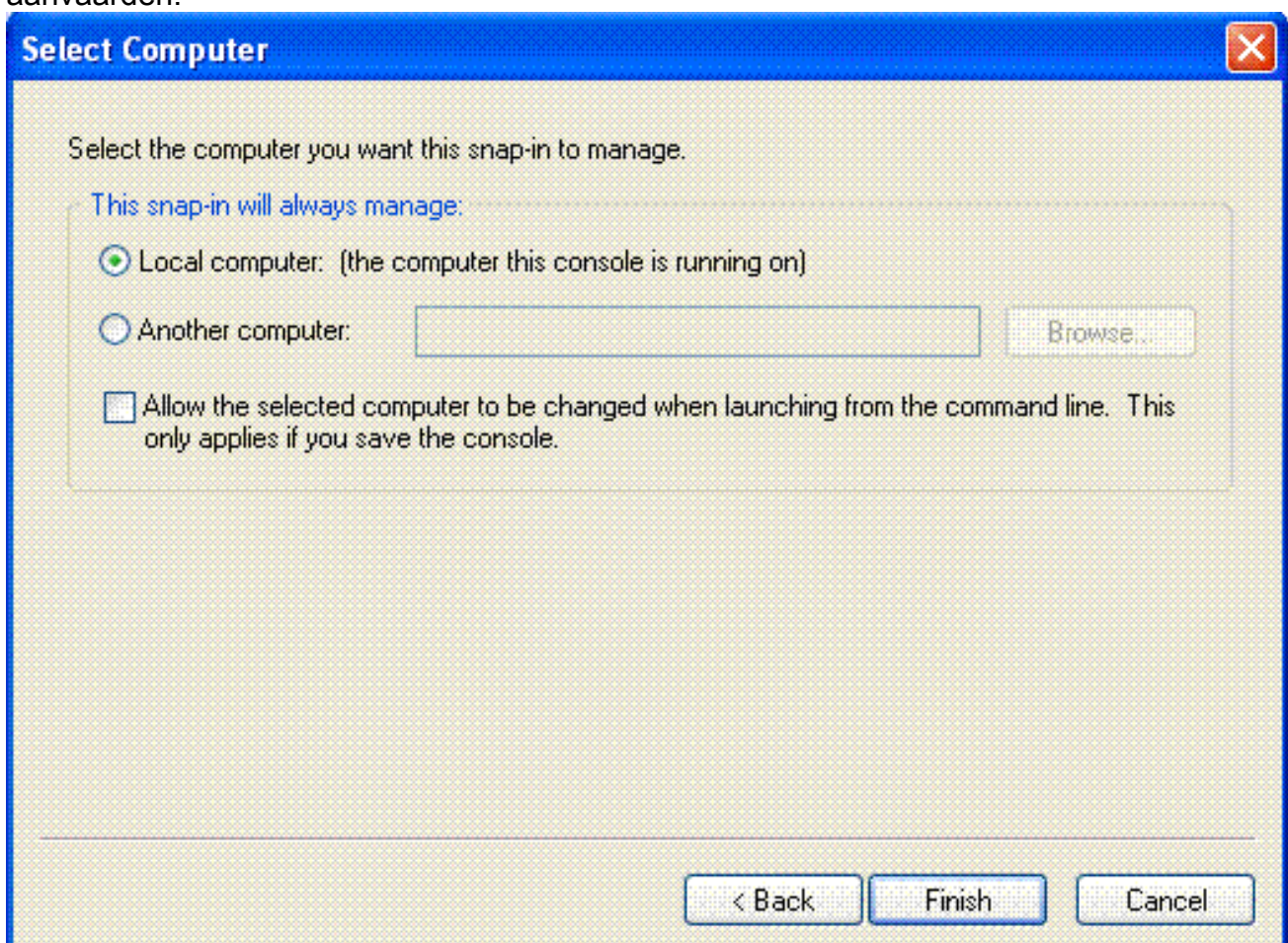


Toevoegen.

20. Kies Computeraccount en klik op Volgende.

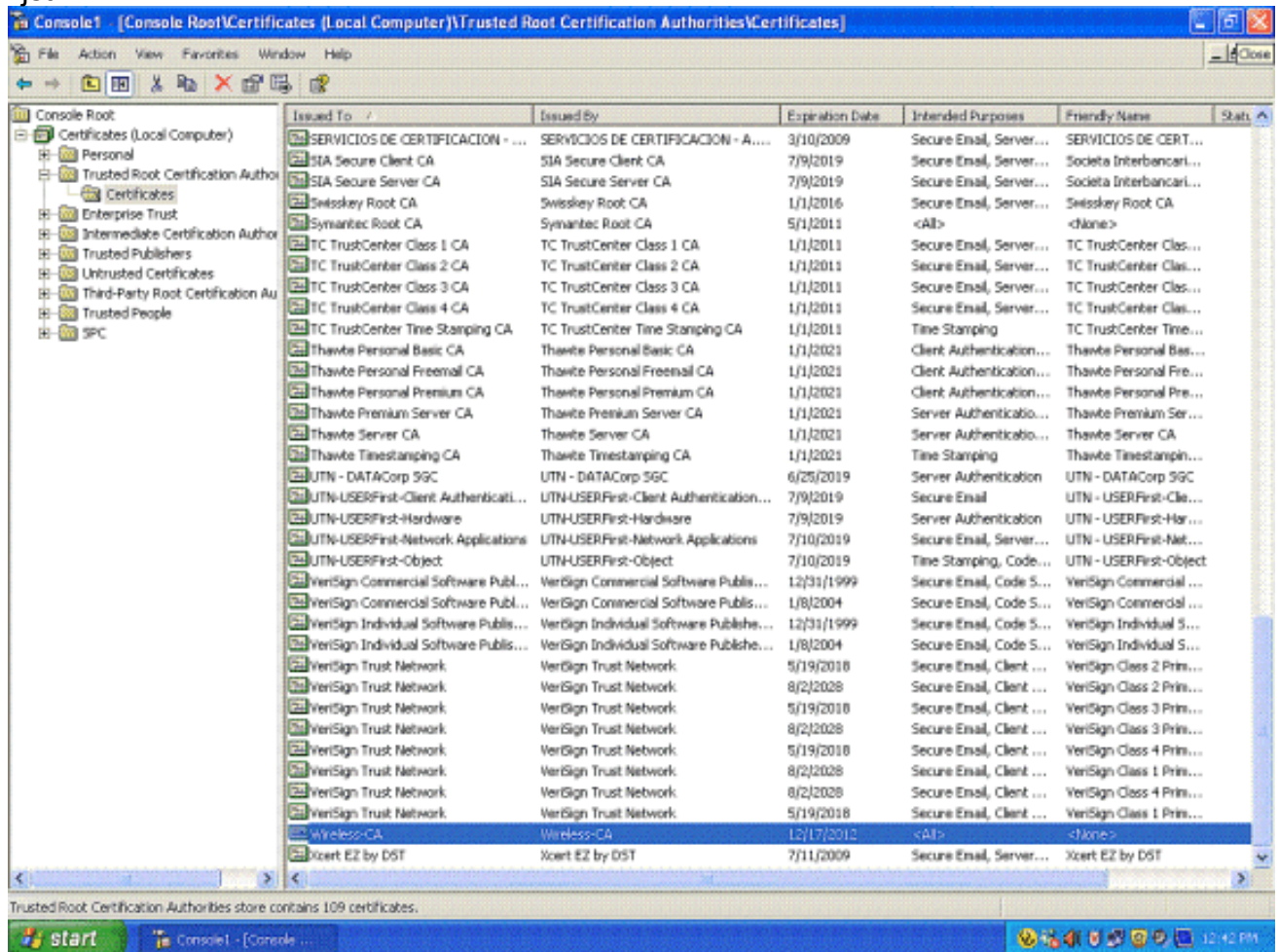


21. Klik op **Voltoeien** om de standaard lokale computer te aanvaarden.



22. Klik op **Sluiten** en klik op **OK**.

23. Breid **Certificaten uit (Local Computer)**; breid **Trusted Root-certificeringsinstanties** uit en klik op **Certificaten**. Zoek draadloos in de lijst.



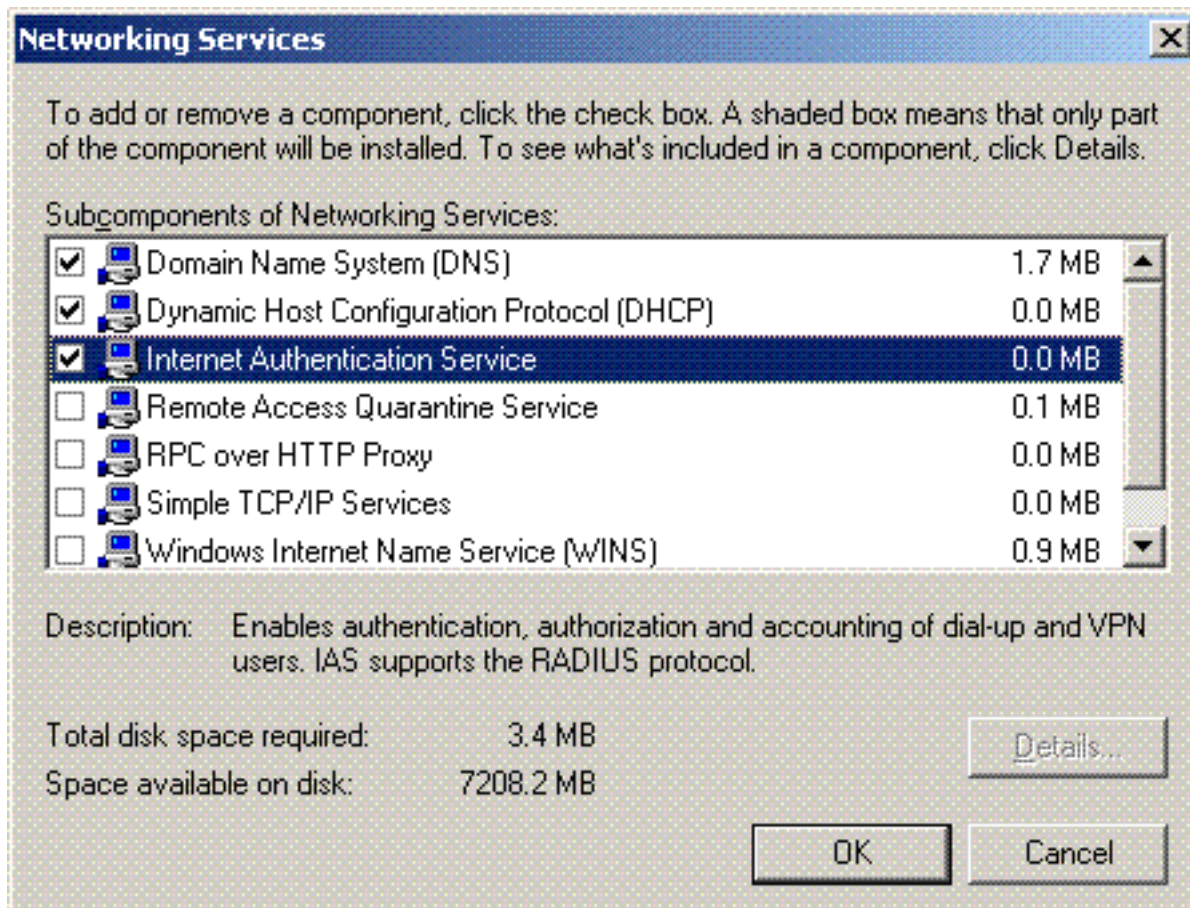
24. Herhaal deze procedure om meer clients aan het domein toe te voegen.

[Installeer de internetverificatieservice op de Microsoft Windows 2003-server en vraag een certificaat aan](#)

In deze setup wordt de Internet Authenticatieservice (IAS) gebruikt als een RADIUS-server voor het verifiëren van draadloze clients met PEAP-verificatie.

Voltooi deze stappen om IAS op de server te installeren en te configureren.

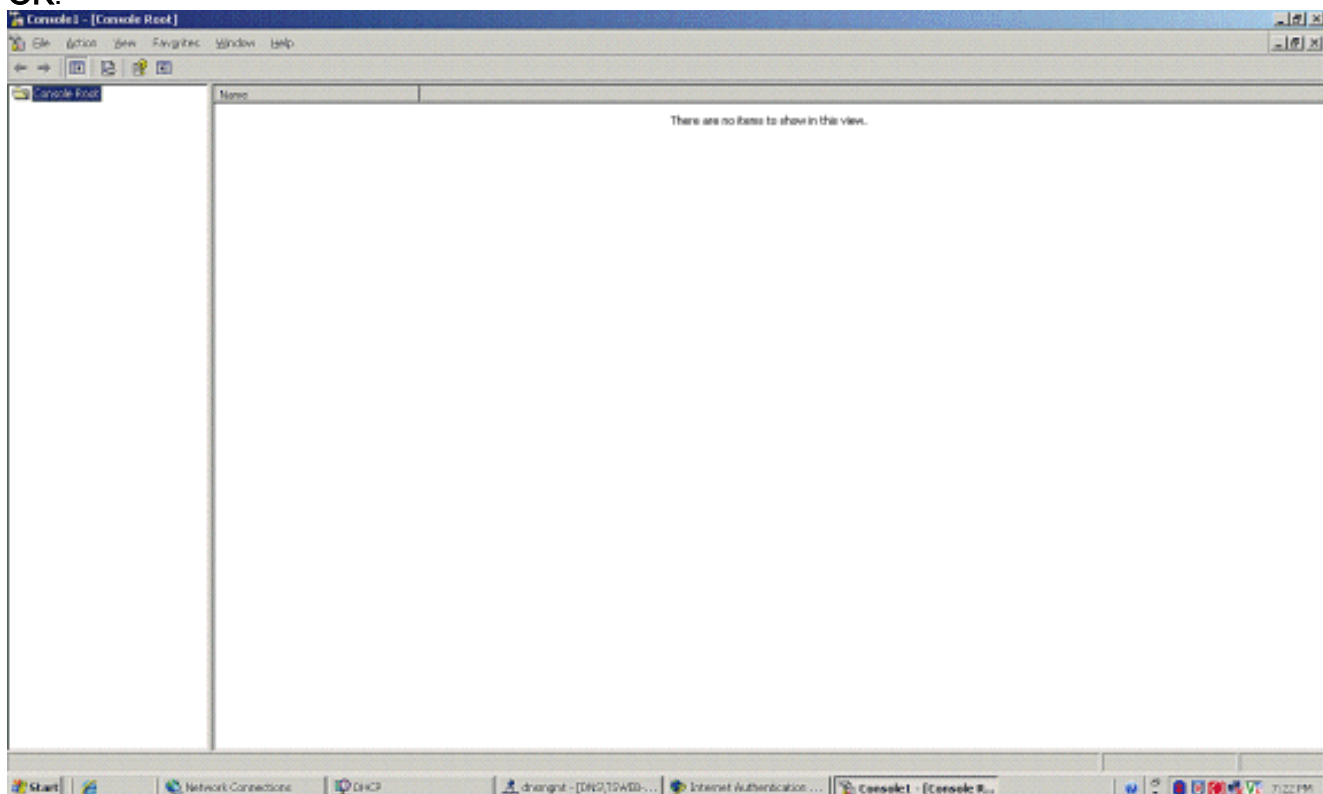
1. Klik op **Software** in het Configuratiescherm.
2. Klik op **Windows-onderdelen toevoegen of verwijderen**.
3. Kies **Netwerkservices** en klik op **Details**.
4. Kies **Internet-verificatieservice**; klik op **OK**; en klik op **Volgende**.



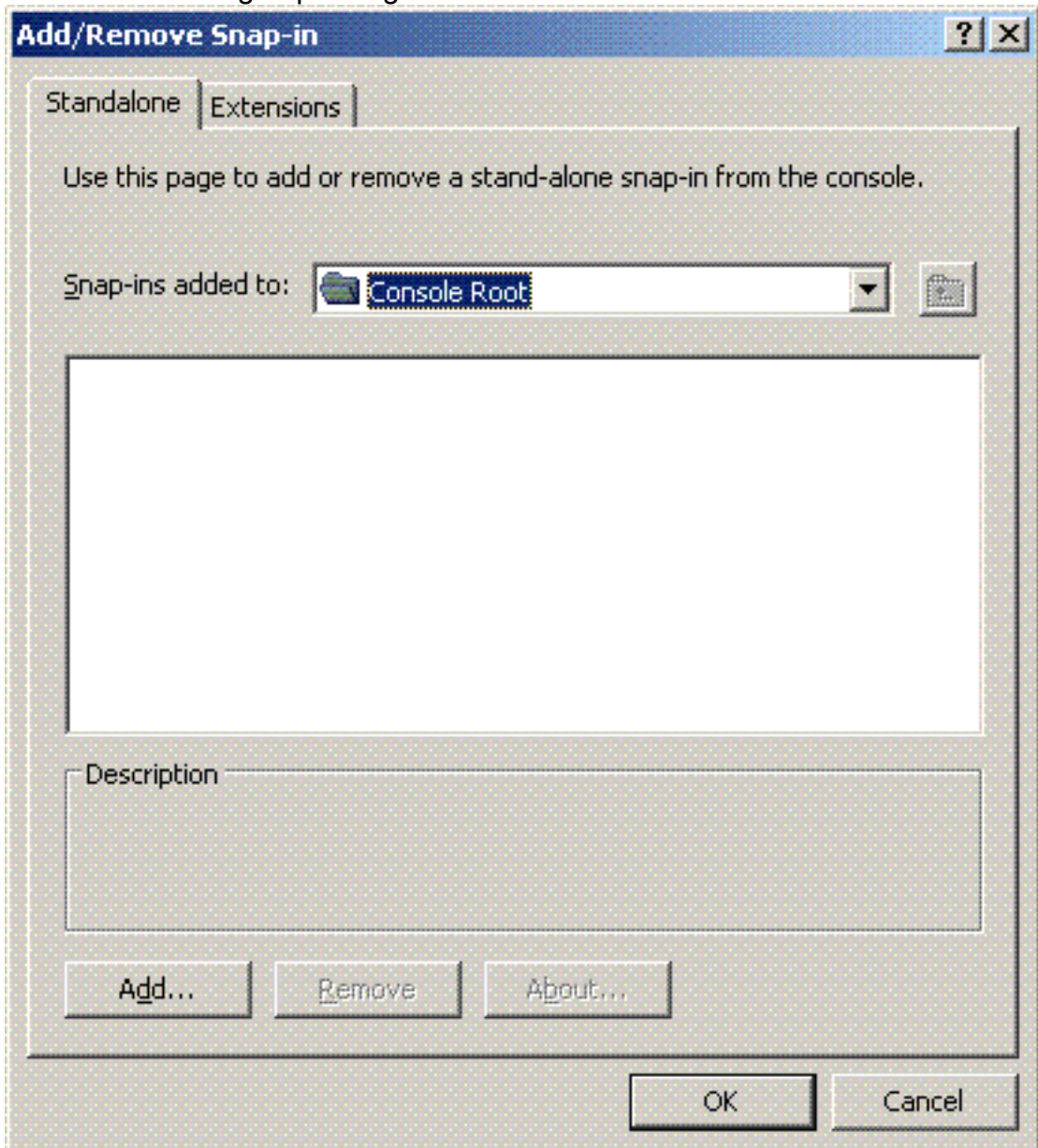
5. Klik op **Voltooien** om de IAS-installatie te voltooien.



6. De volgende stap is het installeren van het computercertificaat voor de Internet-verificatieservice (IAS).
7. Klik op **Start**; klik op **Uitvoeren**; typ **mmc**; en klik op **OK**.

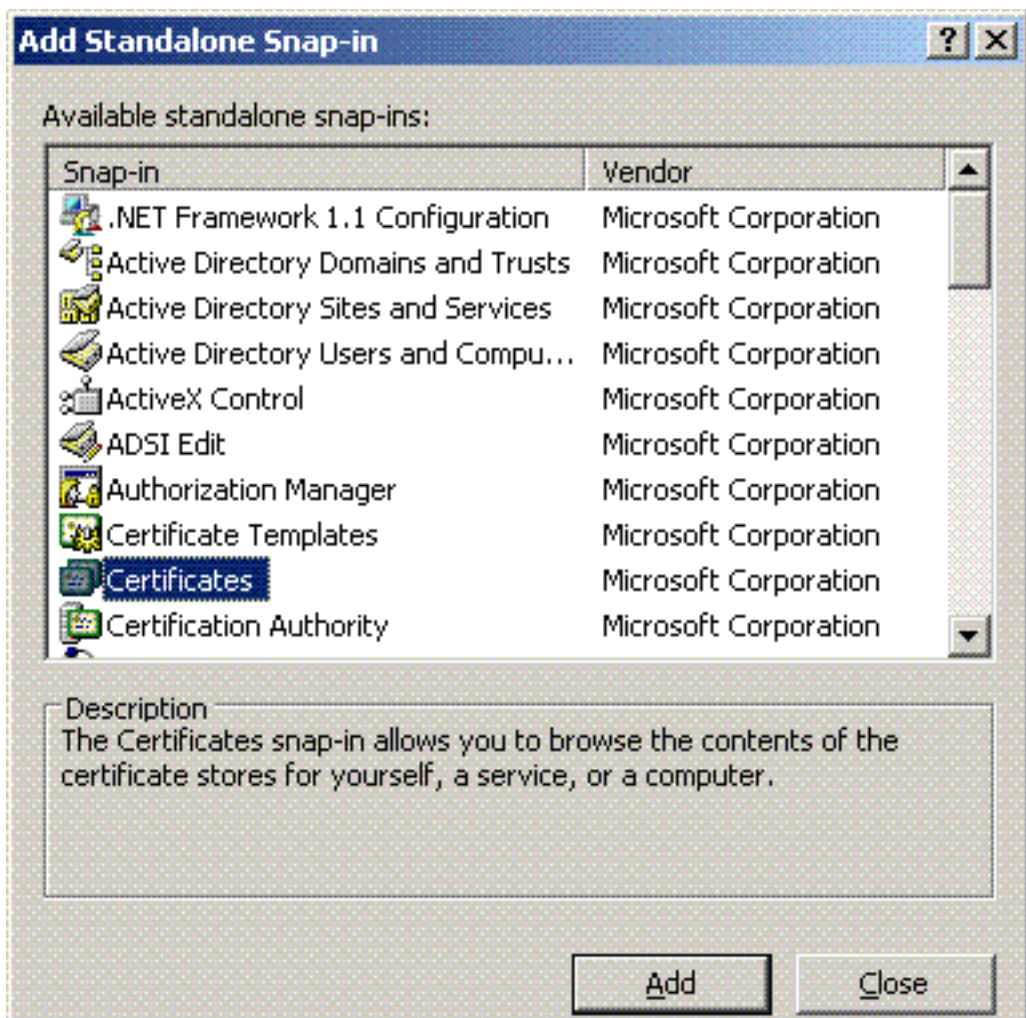


8. Klik op **Console** in het menu Bestand en kies vervolgens module **toevoegen/verwijderen**.
9. Klik op **Add** om een invoegtoepassing toe te



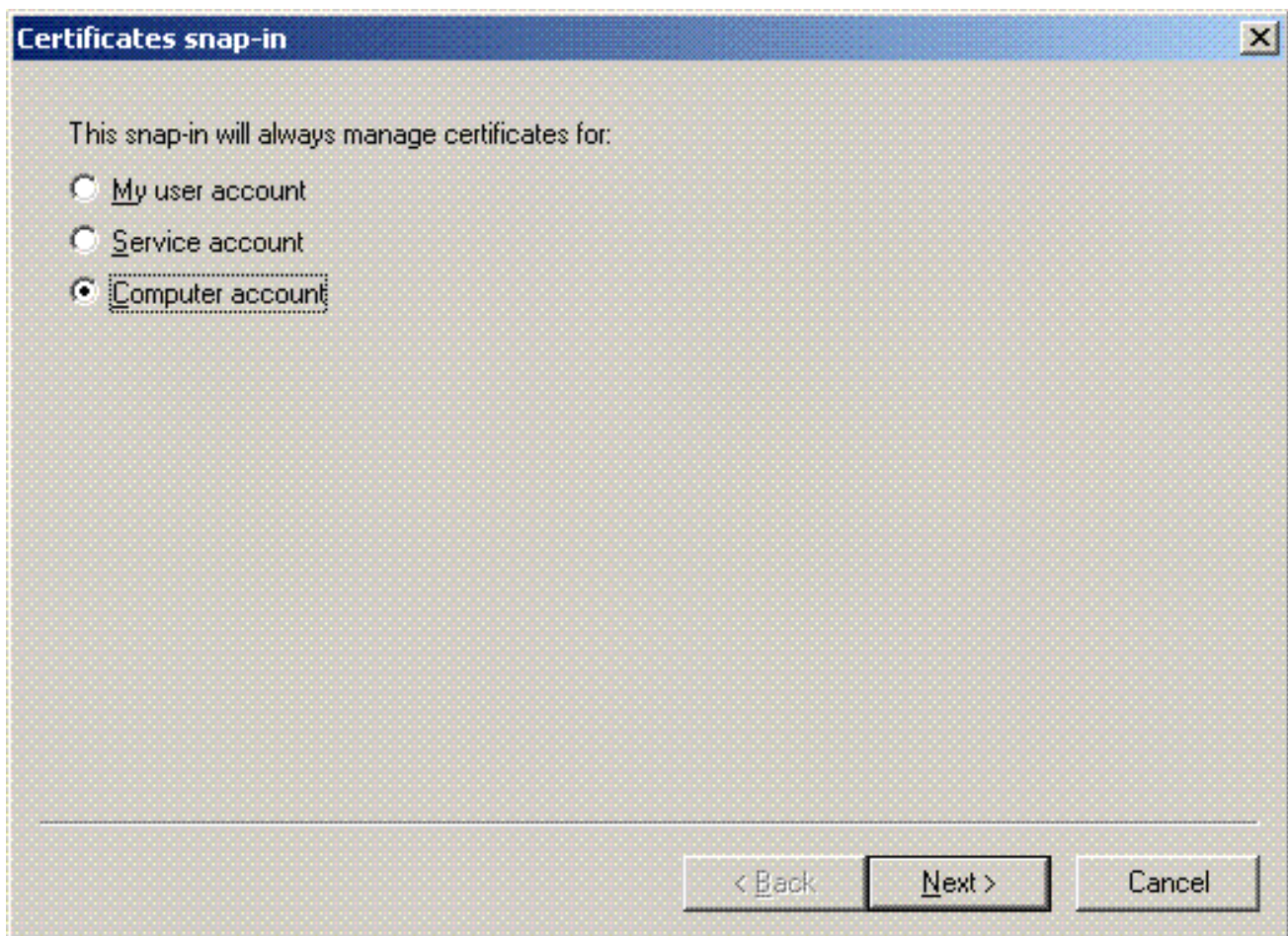
voegen.

10. Kies **Certificaten** uit de lijst met invoegtoepassingen en klik op

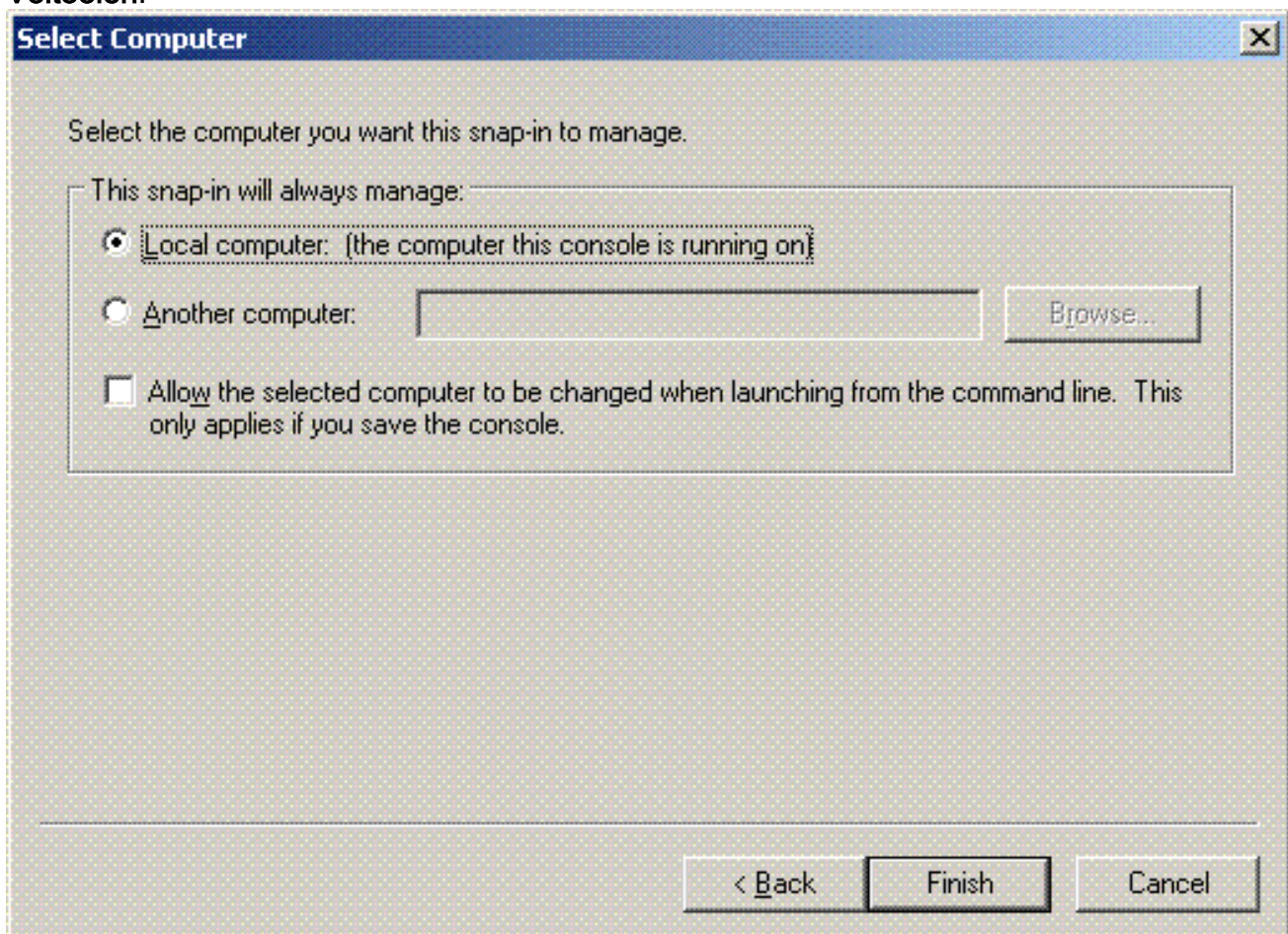


Toevoegen.

11. Kies **Computer-account** en klik op **Volgende**.

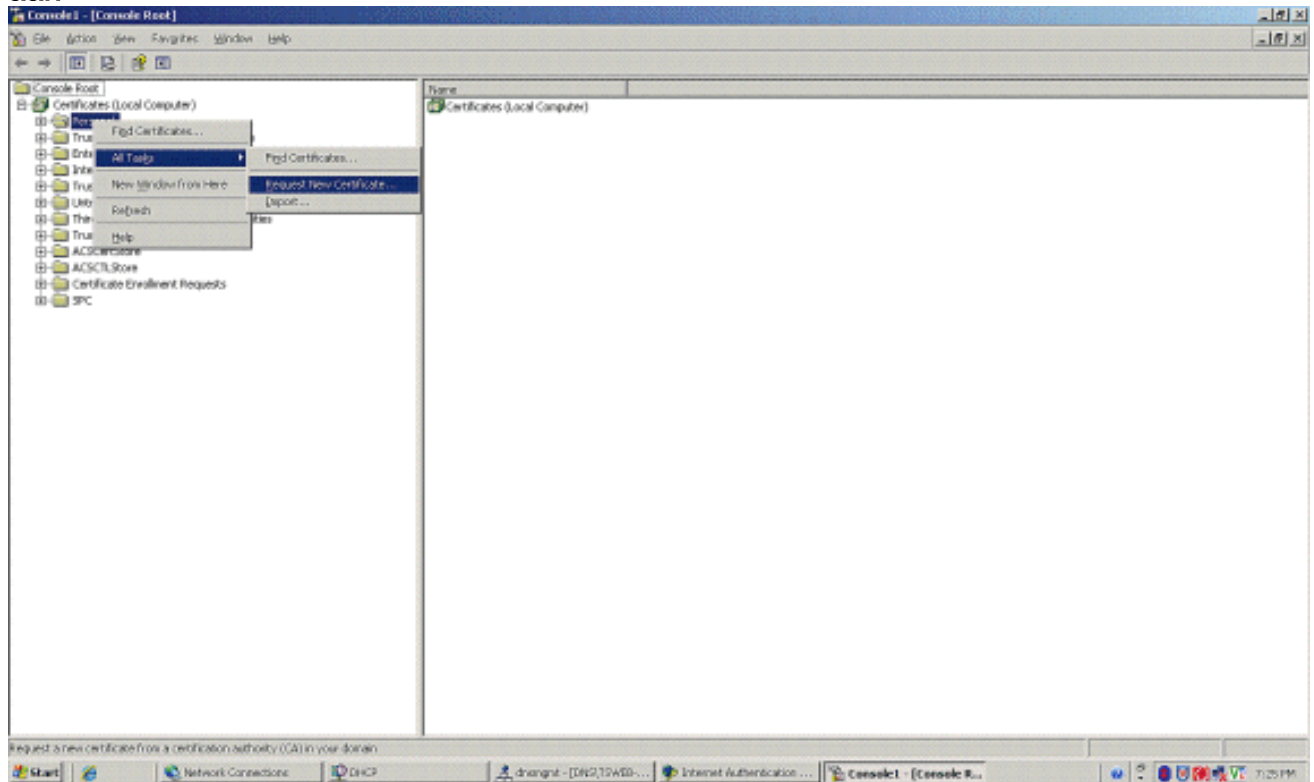


12. Kies **Lokale computer** en klik op **Voltooien**.



13. Klik op **Sluiten** en klik op **OK**.

14. Breid **Certificaten uit (Local Computer)**; klik met de rechtermuisknop op **Persoonlijke map**; kies **Alle taken** en vraag vervolgens **Nieuw certificaat aan**.

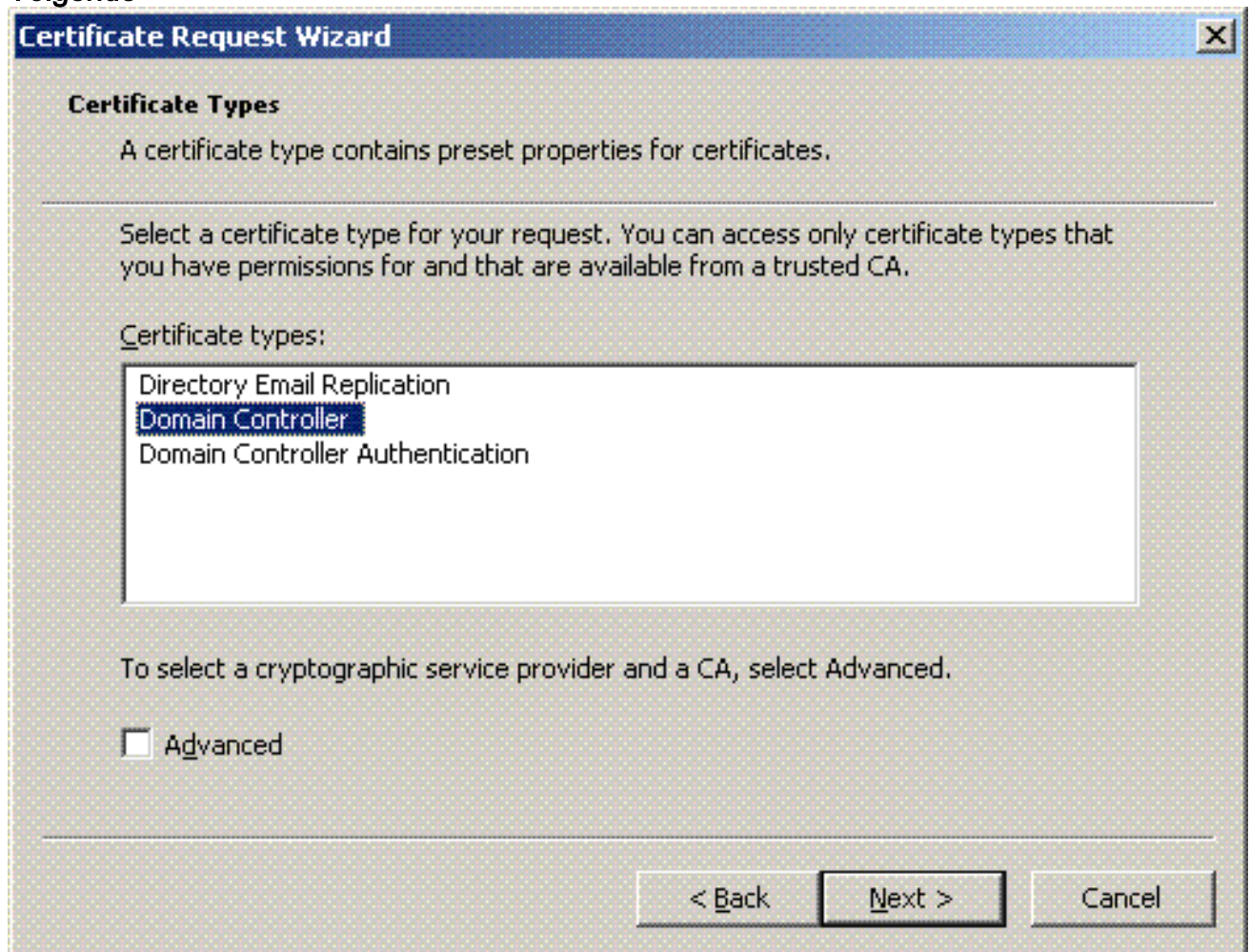


15. Klik op **Volgende** in *de wizard Certificaataanvraag*



16. Kies de **Domain Controller**-certificaatsjabloon (als u een computercertificaat aanvraagt op

een andere server dan de DC, kies een **Computer** certificaatsjabloon) en klik op **Volgende**.



17. Typ een naam en een beschrijving voor het certificaat.

Certificate Request Wizard [X]

Certificate Friendly Name and Description

You can provide a name and description that help you quickly identify a specific certificate.

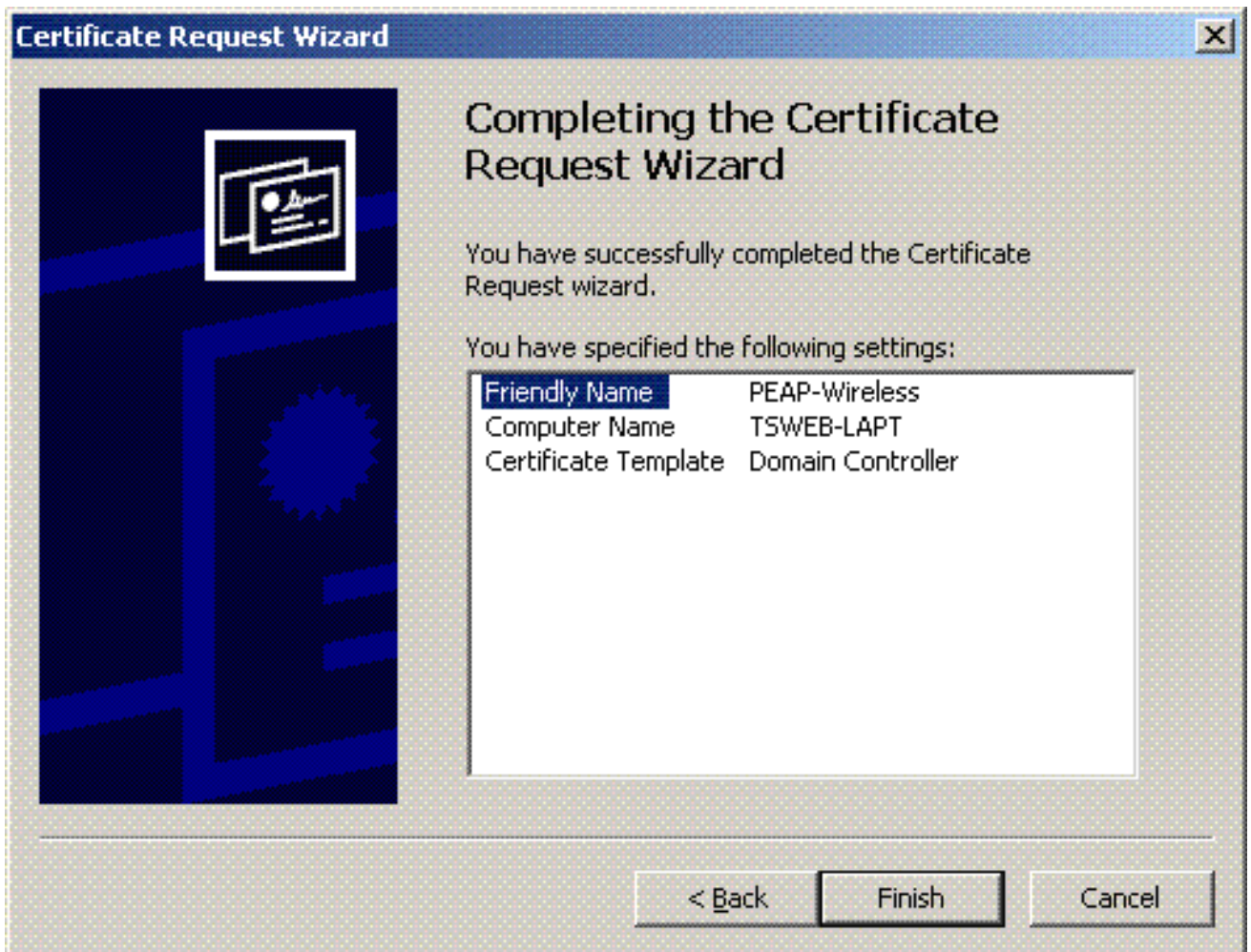
Type a friendly name and description for the new certificate.

Friendly name:

Description:

< Back Next > Cancel

18. Klik op **Voltoeien** om de wizard voor certificeringsaanvragen te voltooien.

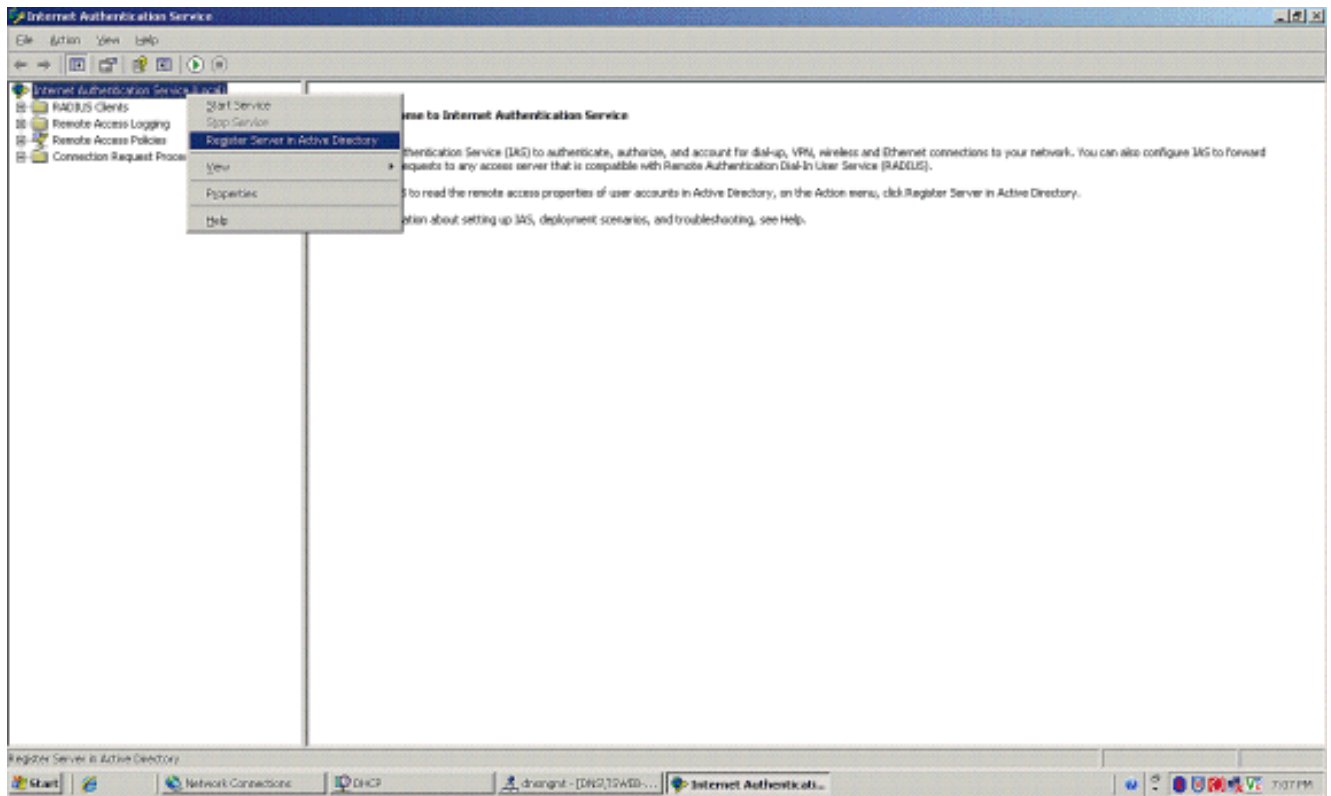


[De internetverificatieservice configureren voor PEAP-MS-CHAP v2-verificatie](#)

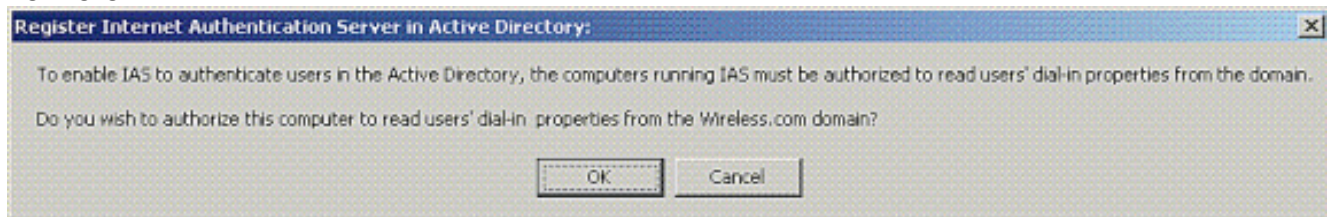
Nu u een certificaat voor de IAS hebt geïnstalleerd en aangevraagd, moet u de IAS configureren voor verificatie.

Voer de volgende stappen uit:

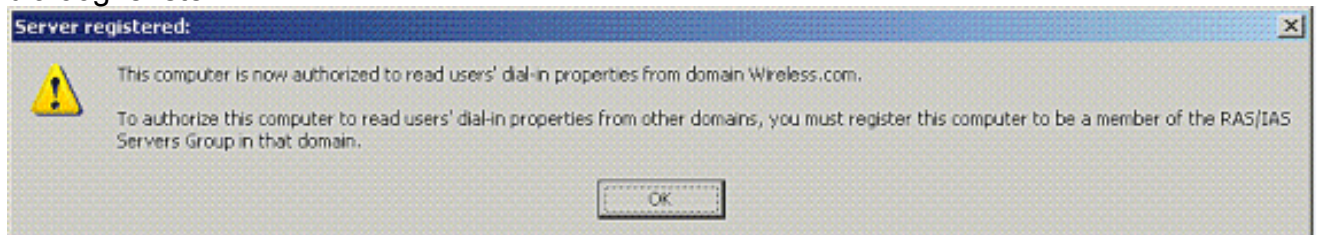
1. Klik op **Start > Programma's > Systeembeheer** en klik op Inloggen voor **internetverificatie**.
2. Klik met de rechtermuisknop op **Internet Authenticatieservice (IAS)** en klik vervolgens op **Service registreren in Active Directory**.



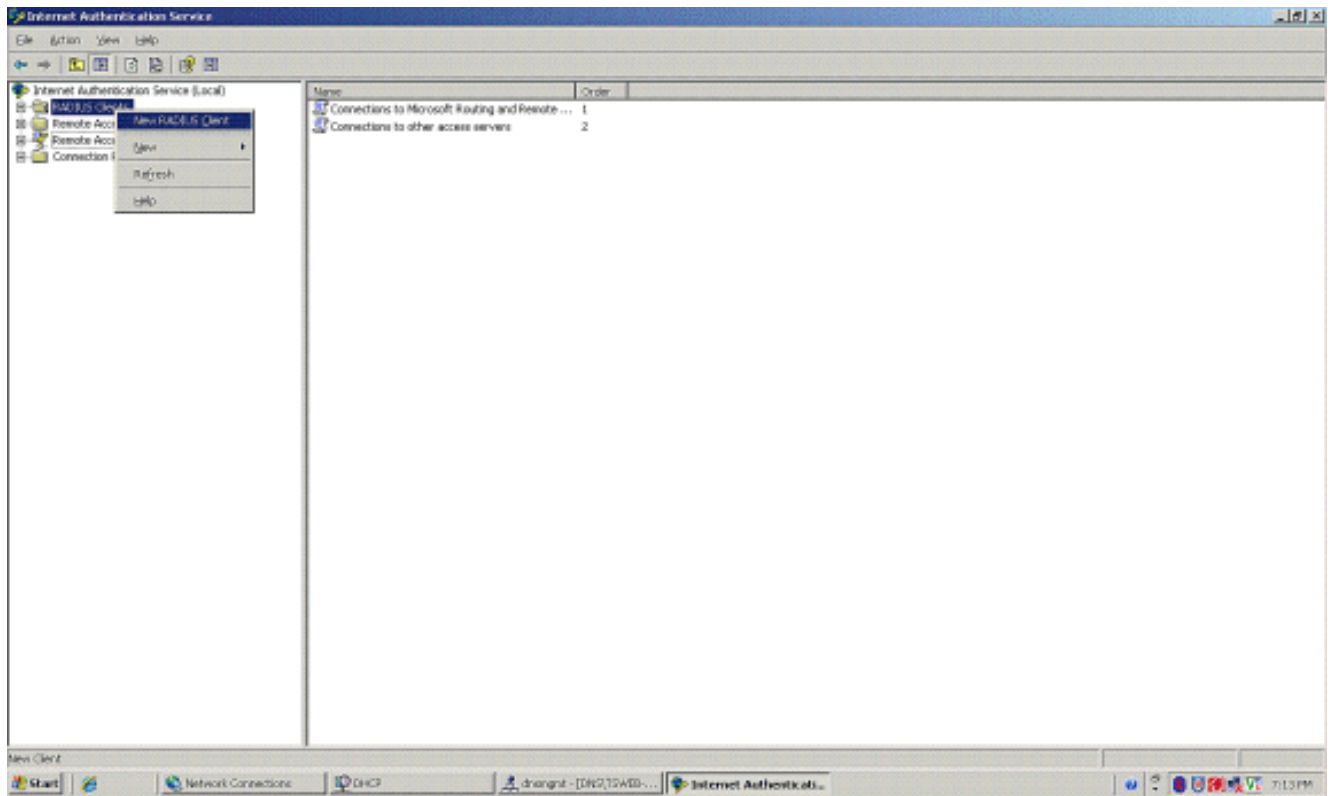
3. De internetverificatieservice registreren in actieve map wordt weergegeven. Klik op OK. Hierdoor kan IAS gebruikers in de Active Directory verifiëren.



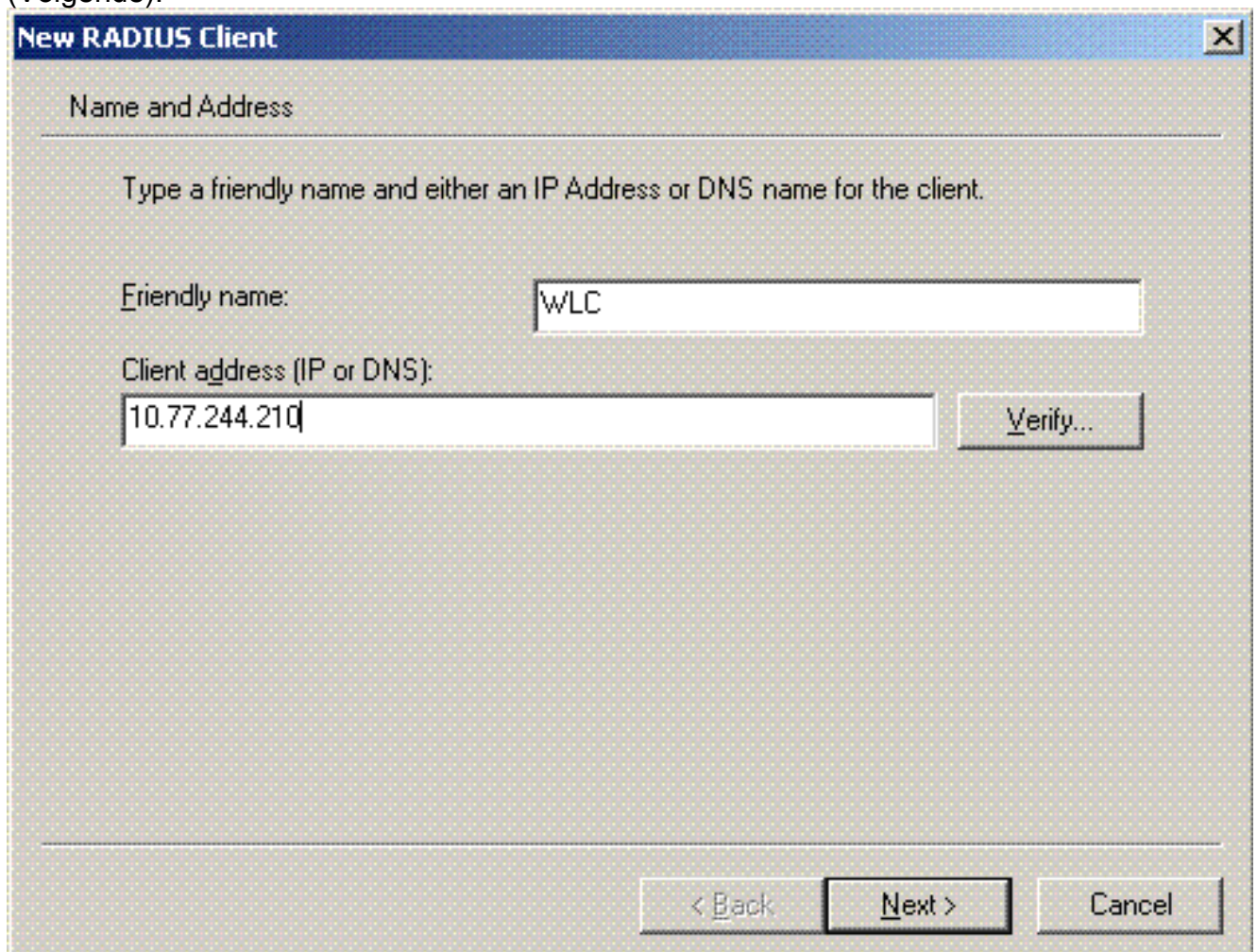
4. Klik op OK in het volgende dialoogvenster.



5. Voeg de draadloze LAN-controller toe als AAA-client op de MS IAS-server.
6. Klik met de rechtermuisknop op **RADIUS-clients** en kies **Nieuwe RADIUS-client**.

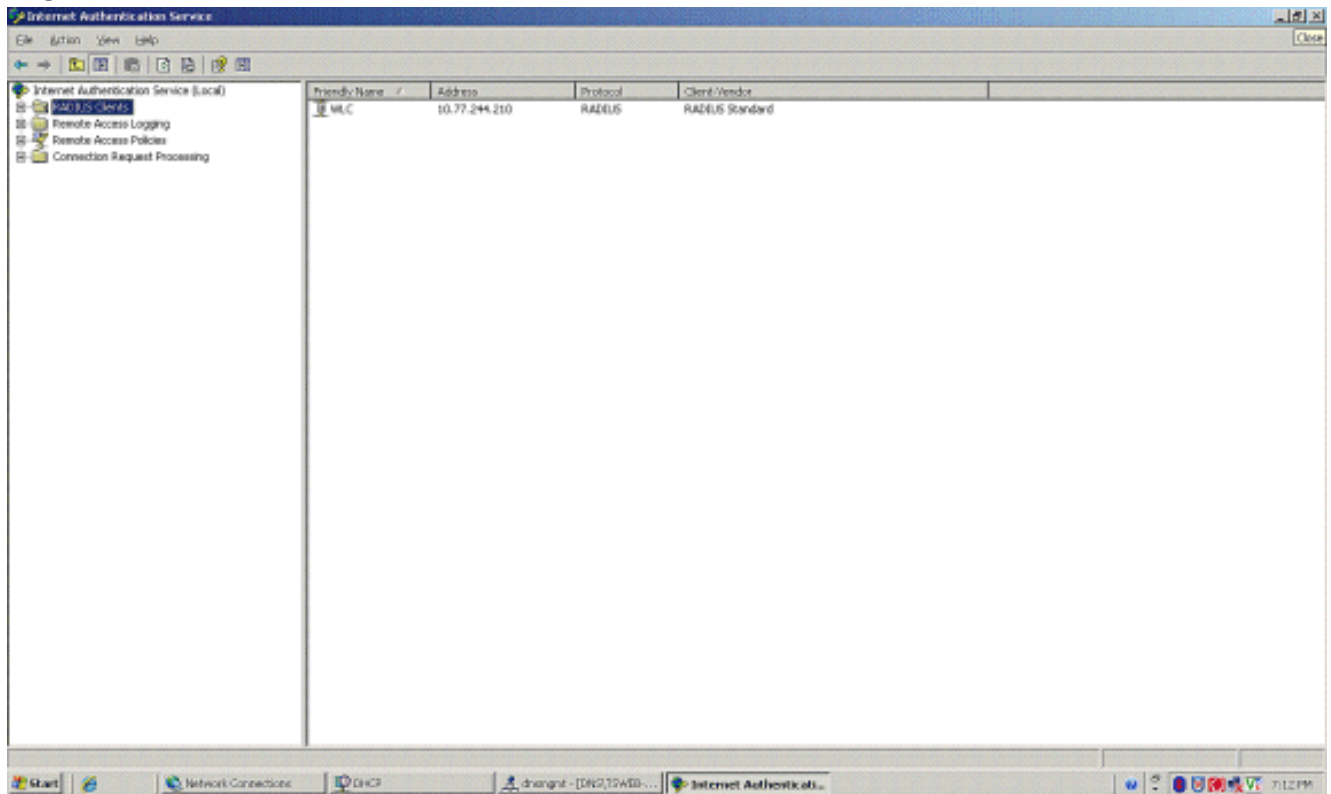


7. Typ de naam van de client (in dit geval WLC) en voer het IP-adres van de WLC in. Klik op **Next** (Volgende).



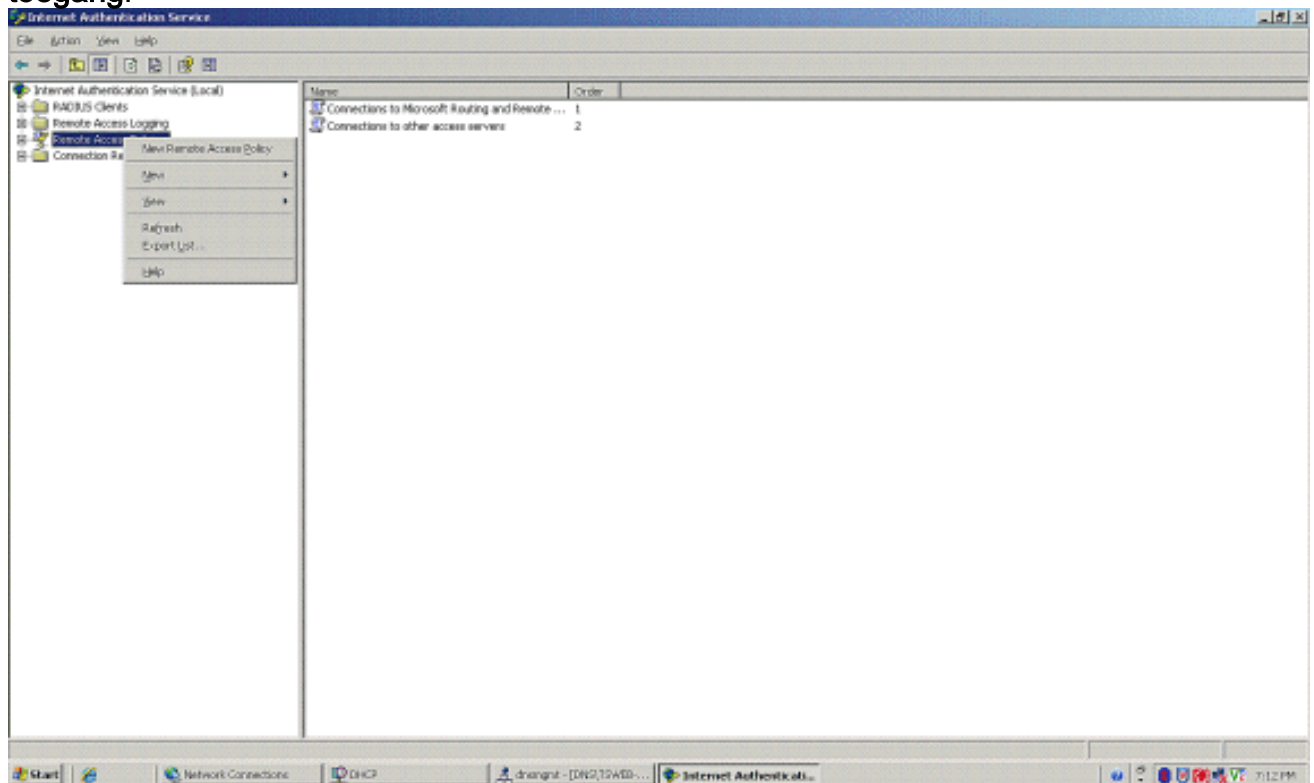
8. Kies op de volgende pagina onder Client-Verkoper **RADIUS-standaard**, voer het gedeelde geheim in en klik op **Voltoeien**.

9. Bericht dat WLC als AAA-client wordt toegevoegd op de IAS.



10. Creëer een beleid voor externe toegang voor de clients.

11. Om dit te doen, klik je met de rechtermuisknop op **het beleid voor externe toegang** en kies je het **nieuwe beleid voor externe toegang**.




12. Typ een naam voor het beleid voor externe toegang. Gebruik in dit voorbeeld de naam **PEAP**. Klik vervolgens op **Volgende**.

New Remote Access Policy Wizard [X]

Policy Configuration Method

The wizard can create a typical policy, or you can create a custom policy.



How do you want to set up this policy?

Use the wizard to set up a typical policy for a common scenario

Set up a custom policy

Type a name that describes this policy.

Policy name:


Example: Authenticate all VPN connections.

< Back Next > Cancel

13. Kies de beleidskenmerken op basis van uw vereisten. Kies in dit voorbeeld **Draadloos**.

New Remote Access Policy Wizard [X]

Access Method
Policy conditions are based on the method used to gain access to the network.

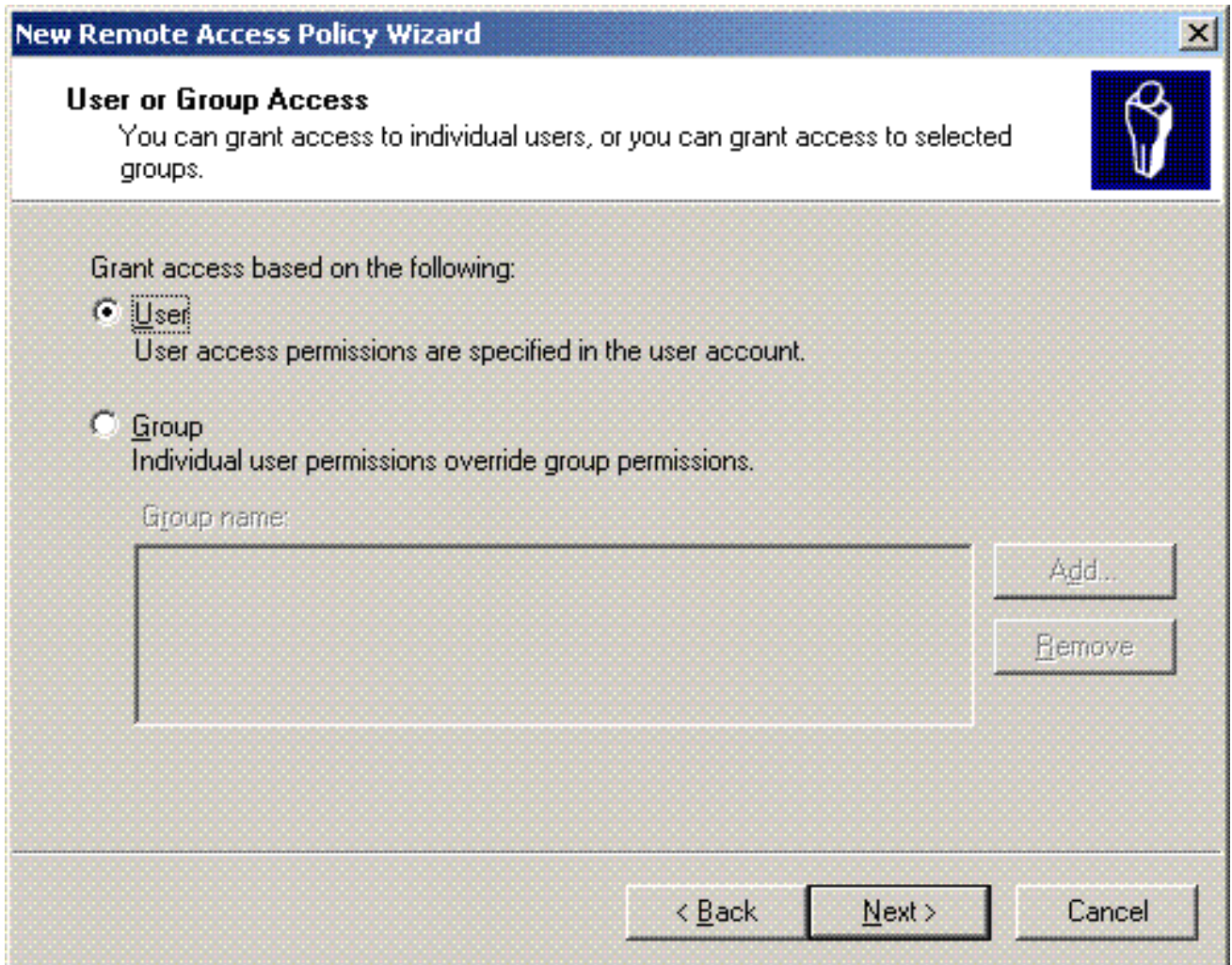


Select the method of access for which you want to create a policy.

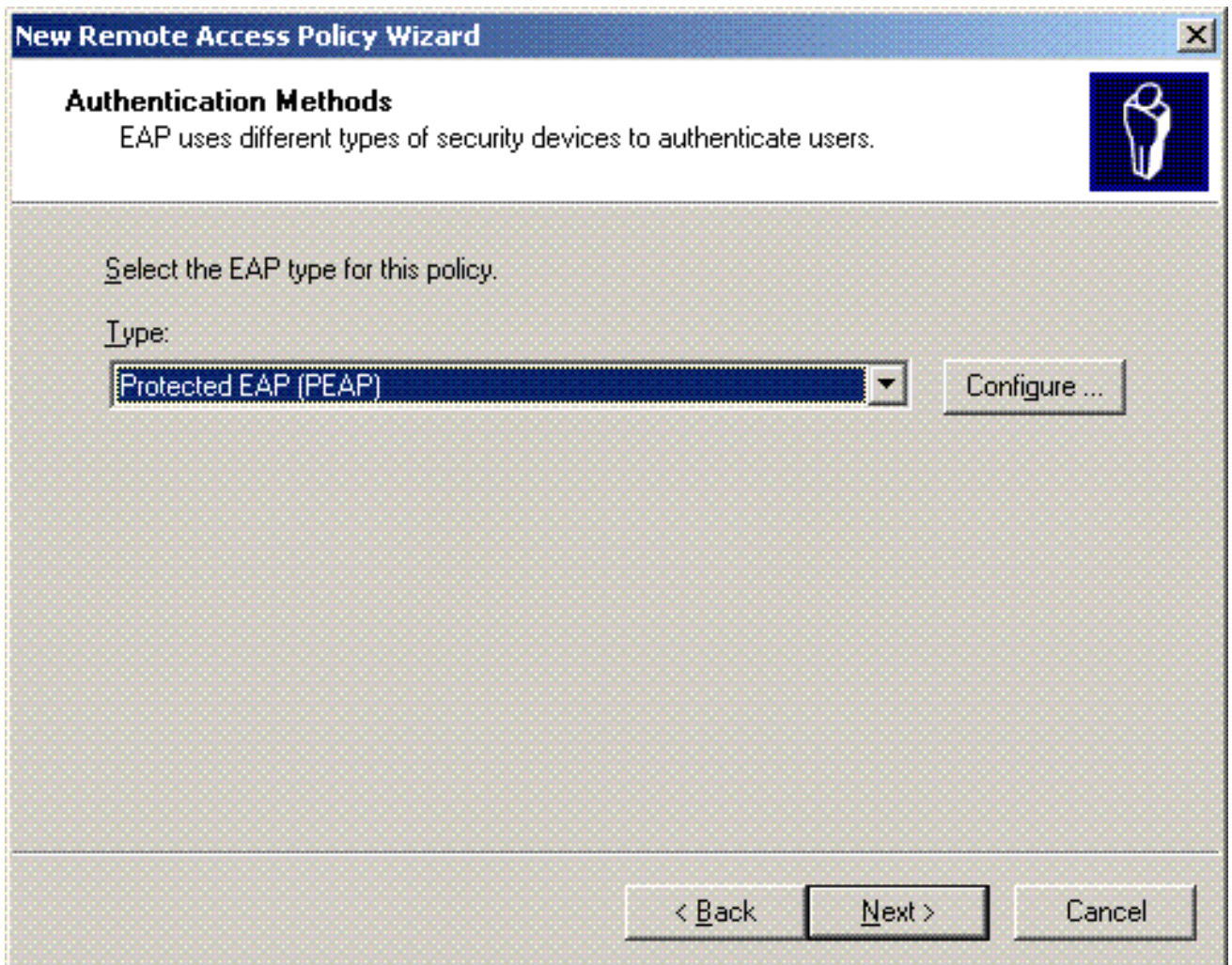
- V**PN
Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.
- D**ial-up
Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.
- W**ireless
Use for wireless LAN connections only.
- E**thernet
Use for Ethernet connections, such as connections that use a switch.

< **B**ack **N**ext > Cancel

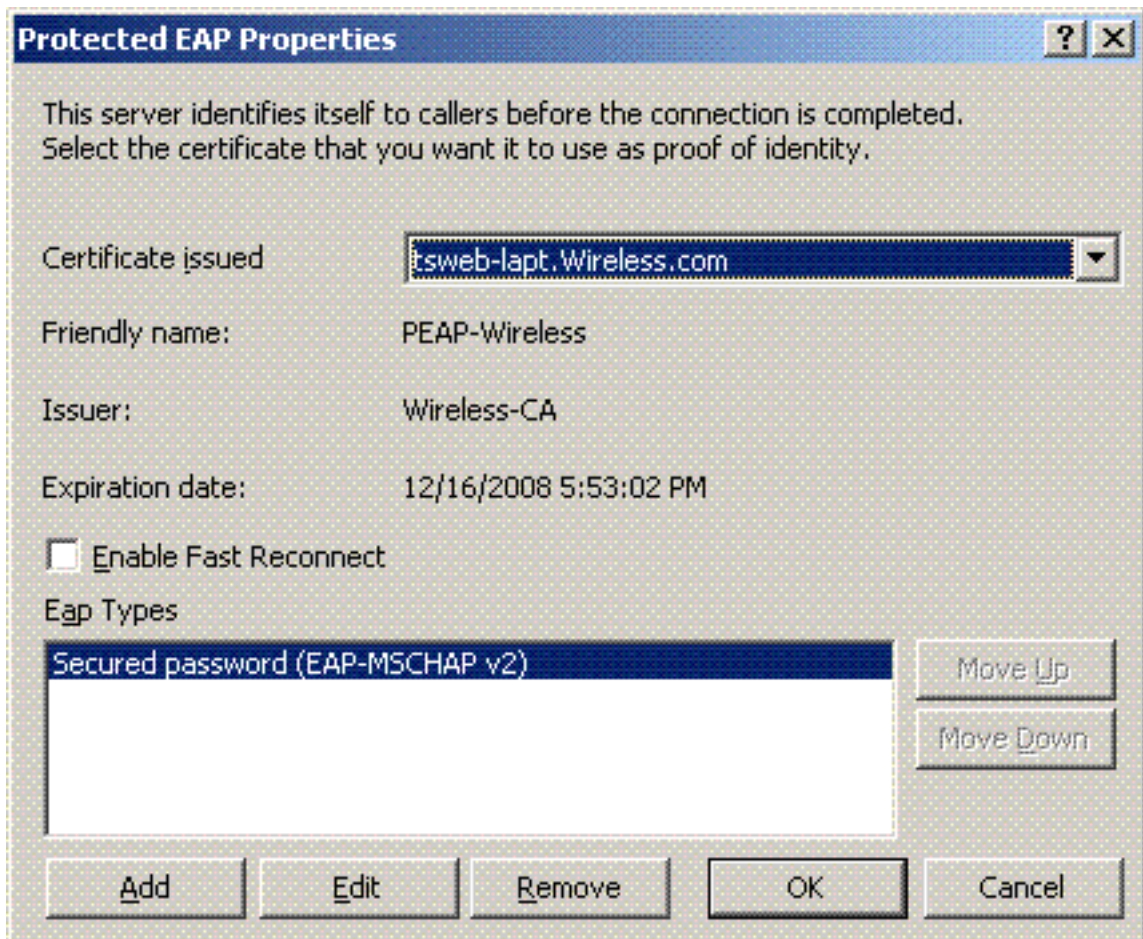
14. Kies op de volgende pagina **Gebruiker** om dit beleid voor externe toegang toe te passen op de lijst met gebruikers.



15. Kies onder Verificatiemethoden de optie **Protected EAP (PEAP)** en klik op **Configureren**.

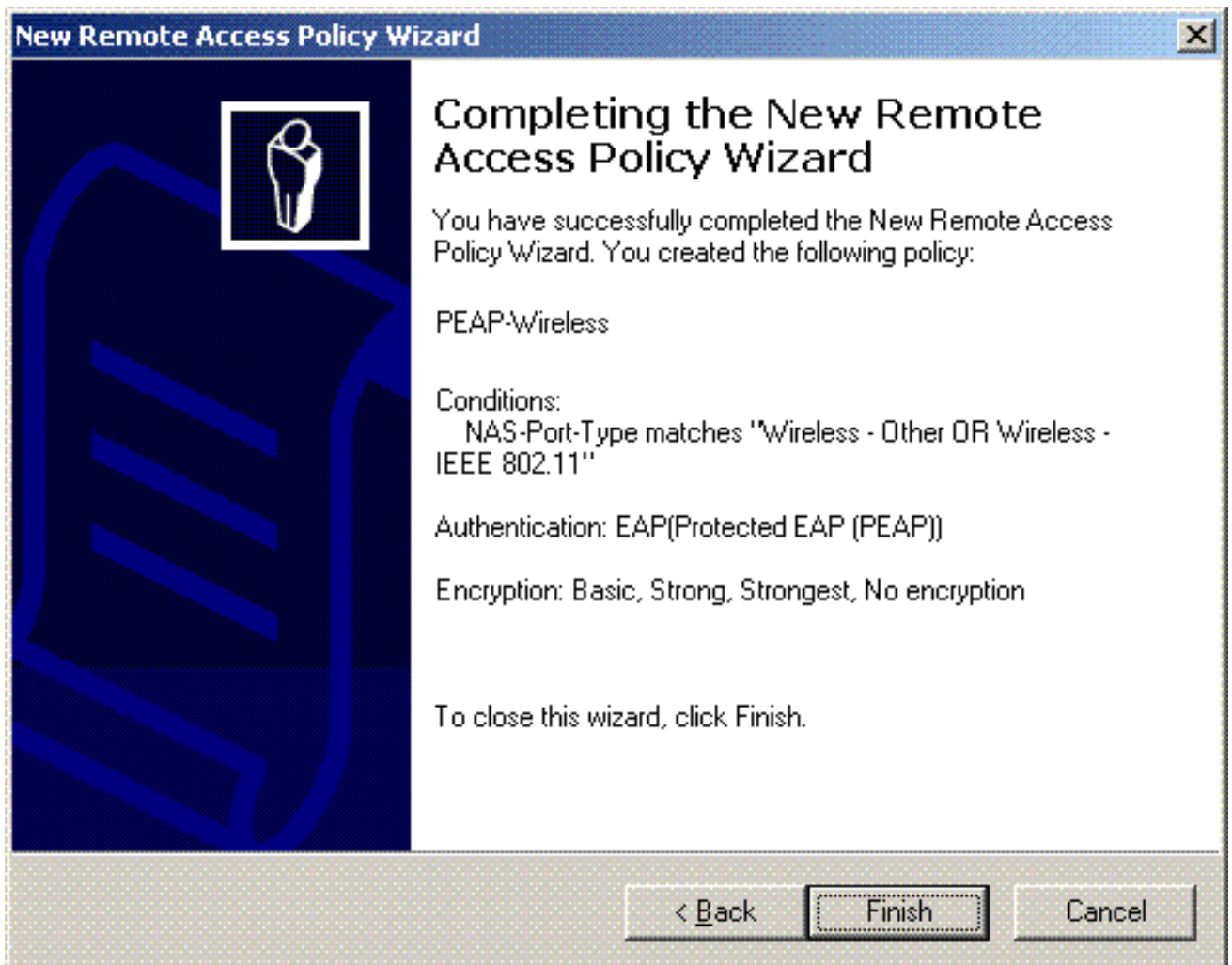


16. Kies op de pagina **Beschermd EAP-eigenschappen** het juiste certificaat in het vervolgkeuzemenu Certificaat afgeven en klik op

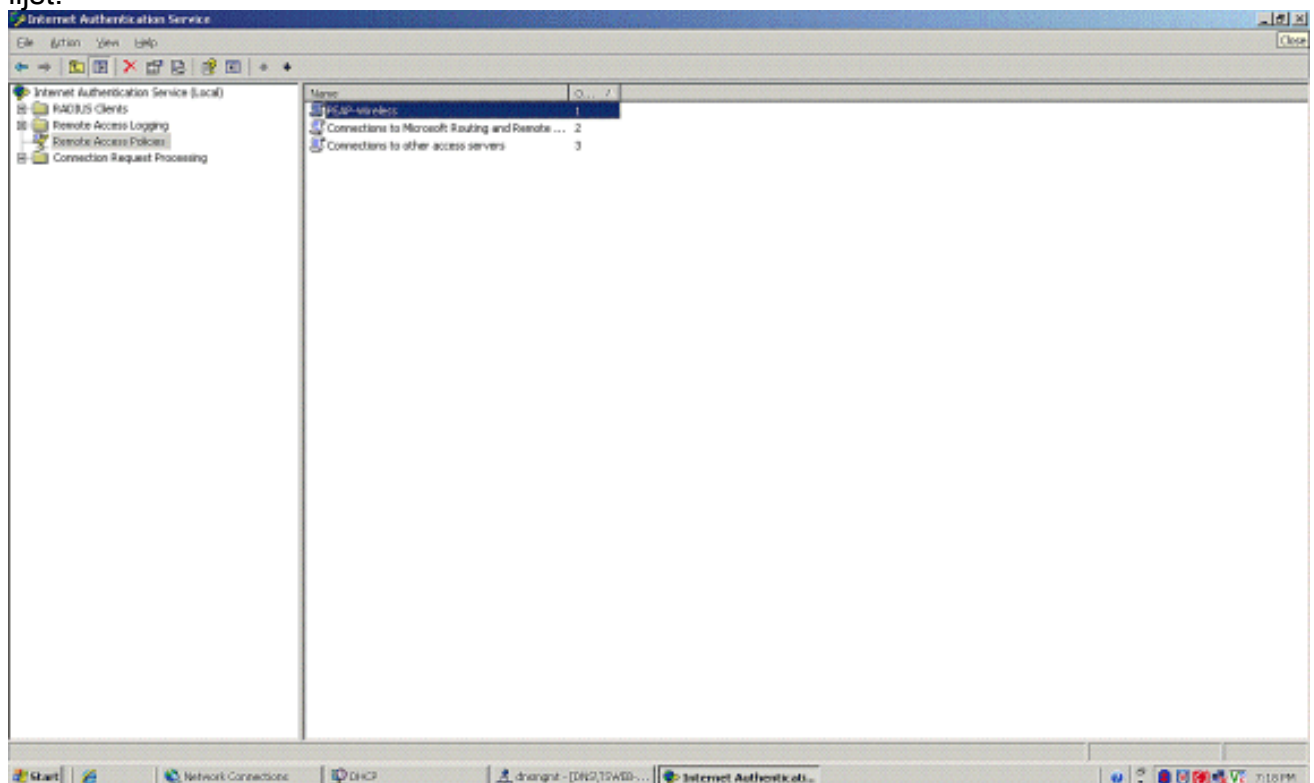


OK.

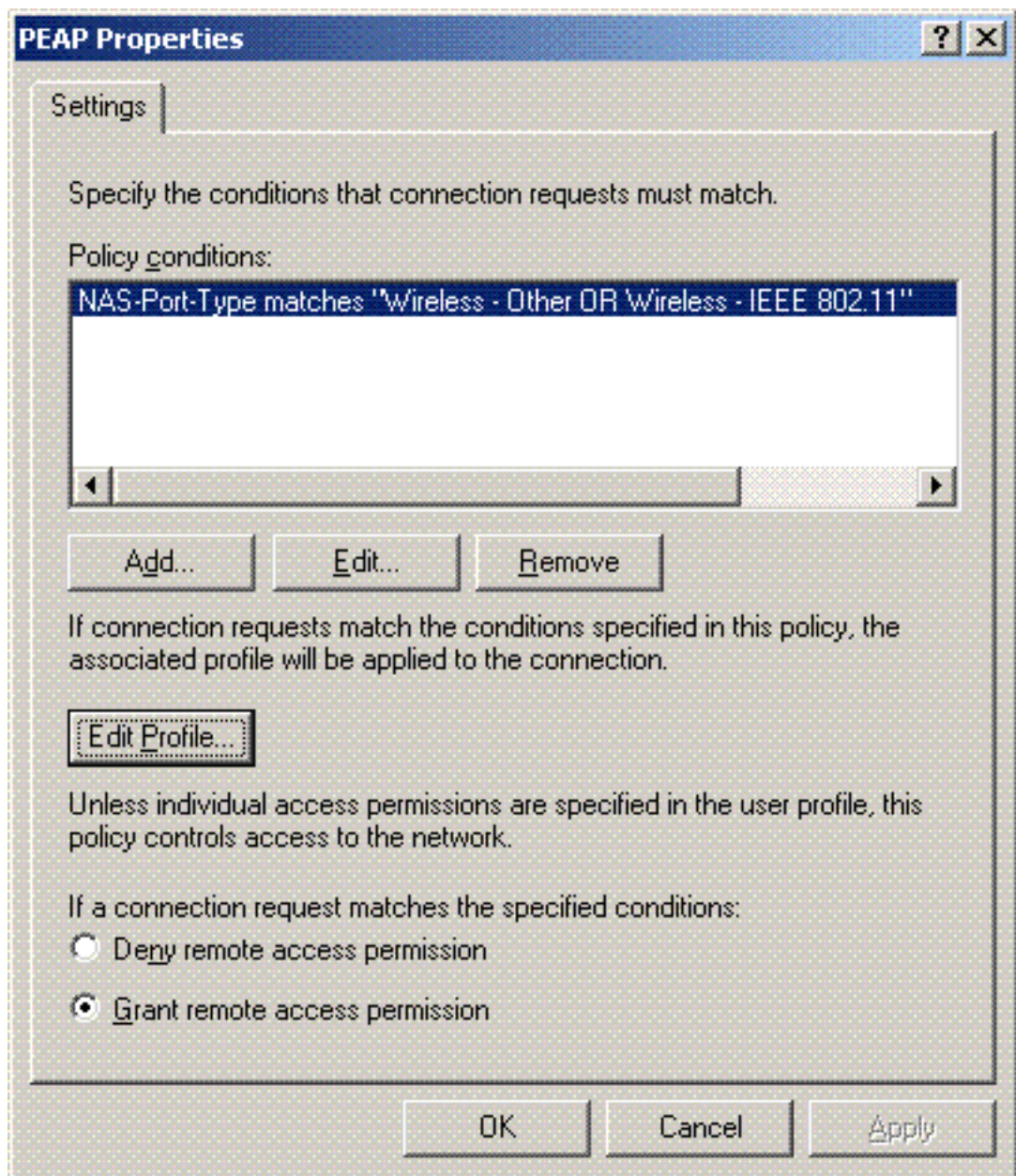
17. Controleer de details van het beleid voor externe toegang en klik op **Voltoeien**.



18. Het beleid voor externe toegang is toegevoegd aan de lijst.



19. Klik met de rechtermuisknop op het beleid en klik op **Eigenschappen**. Kies **"Toestemming voor externe toegang verlenen"** onder **"Als een verbindingsverzoek aan de opgegeven voorwaarden"**



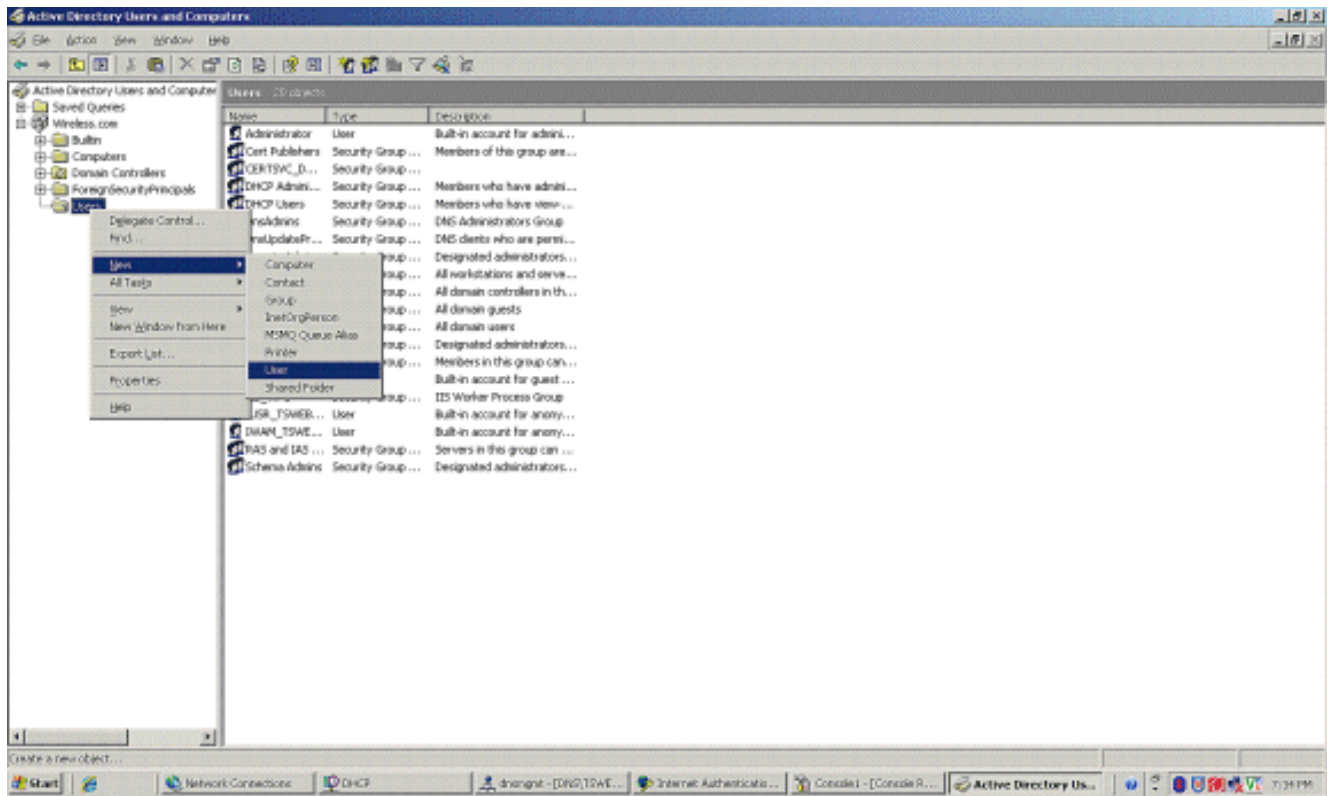
voldoet".

[Gebruikers toevoegen aan de actieve map](#)

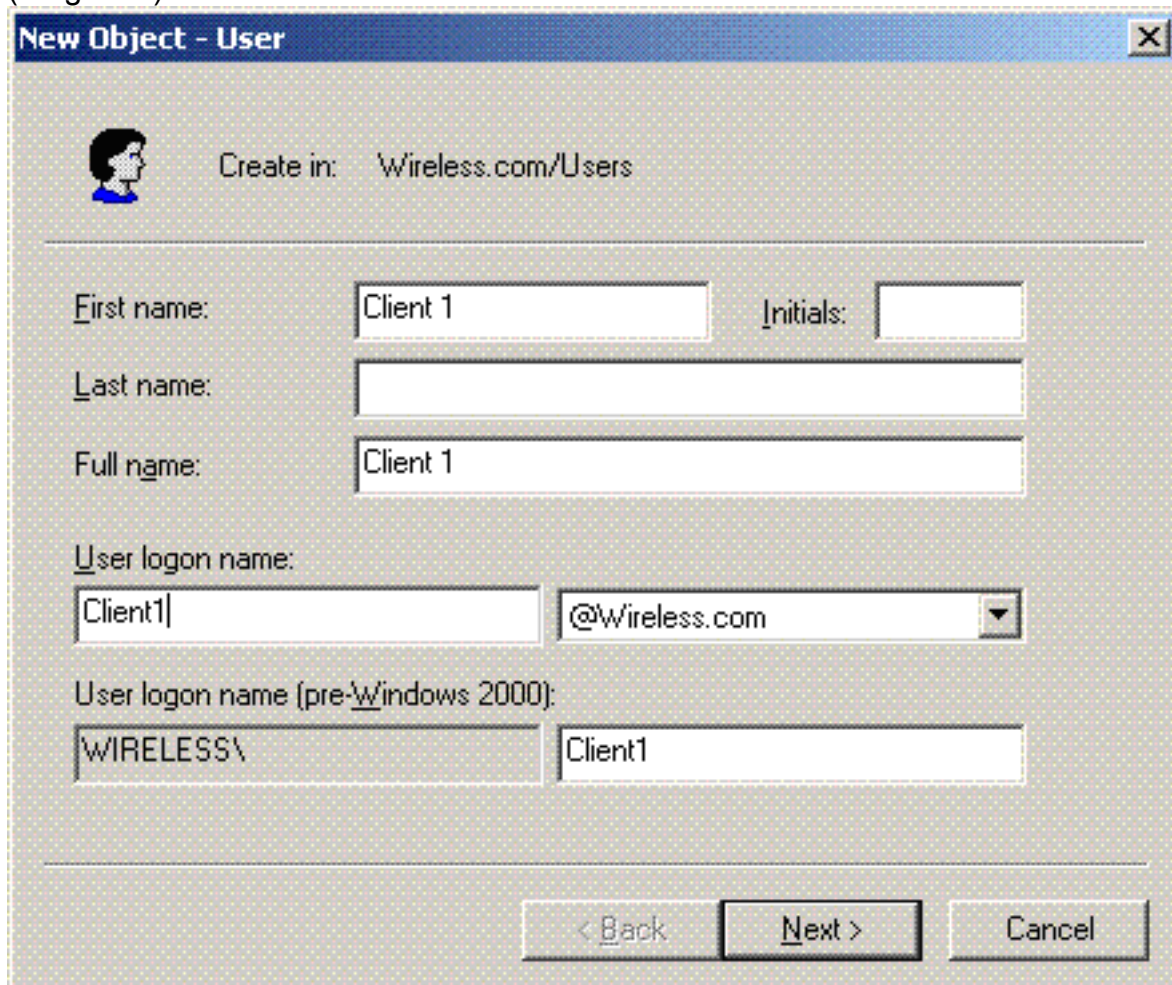
In deze instelling wordt de gebruikersdatabase onderhouden in de Active Directory.

Voltooi de volgende stappen om gebruikers aan de Active Directory-database toe te voegen:

1. In de Active Directory-console-structuur Gebruikers en Computers klikt u met de rechtermuisknop op **Gebruikers**, klikt u op **Nieuw** en klikt u vervolgens op **Gebruiker**.



2. Typ in het dialoogvenster Nieuw object - gebruiker de naam van de draadloze gebruiker. In dit voorbeeld wordt de naam **Draadloze gebruiker** gebruikt in het veld Voornaam en **Draadloze gebruiker** in het veld Gebruikersnaam. Klik op **Next** (Volgende).



3. Typ in het dialoogvenster Nieuw object - gebruiker een wachtwoord naar keuze in de velden Wachtwoord en Wachtwoord bevestigen. Wis het **wachtwoord** van de **gebruiker bij de**

volgende aanmelding en klik op Volgende.

New Object - User

Create in: Wireless.com/Users

Password: [masked]

Confirm password: [masked]

User must change password at next logon

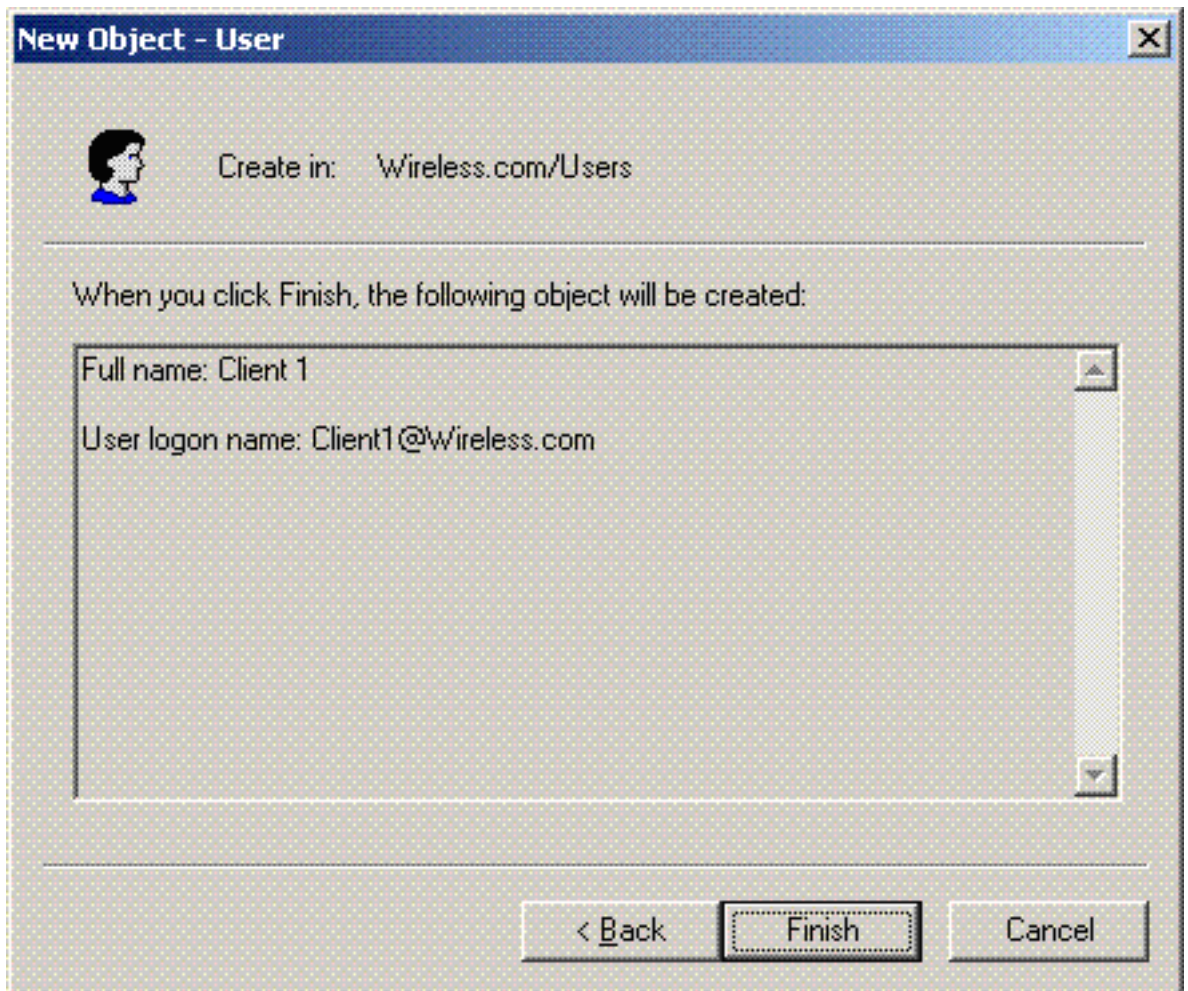
User cannot change password

Password never expires

Account is disabled

< Back Next > Cancel

4. Klik in het dialoogvenster Nieuw object - gebruiker op



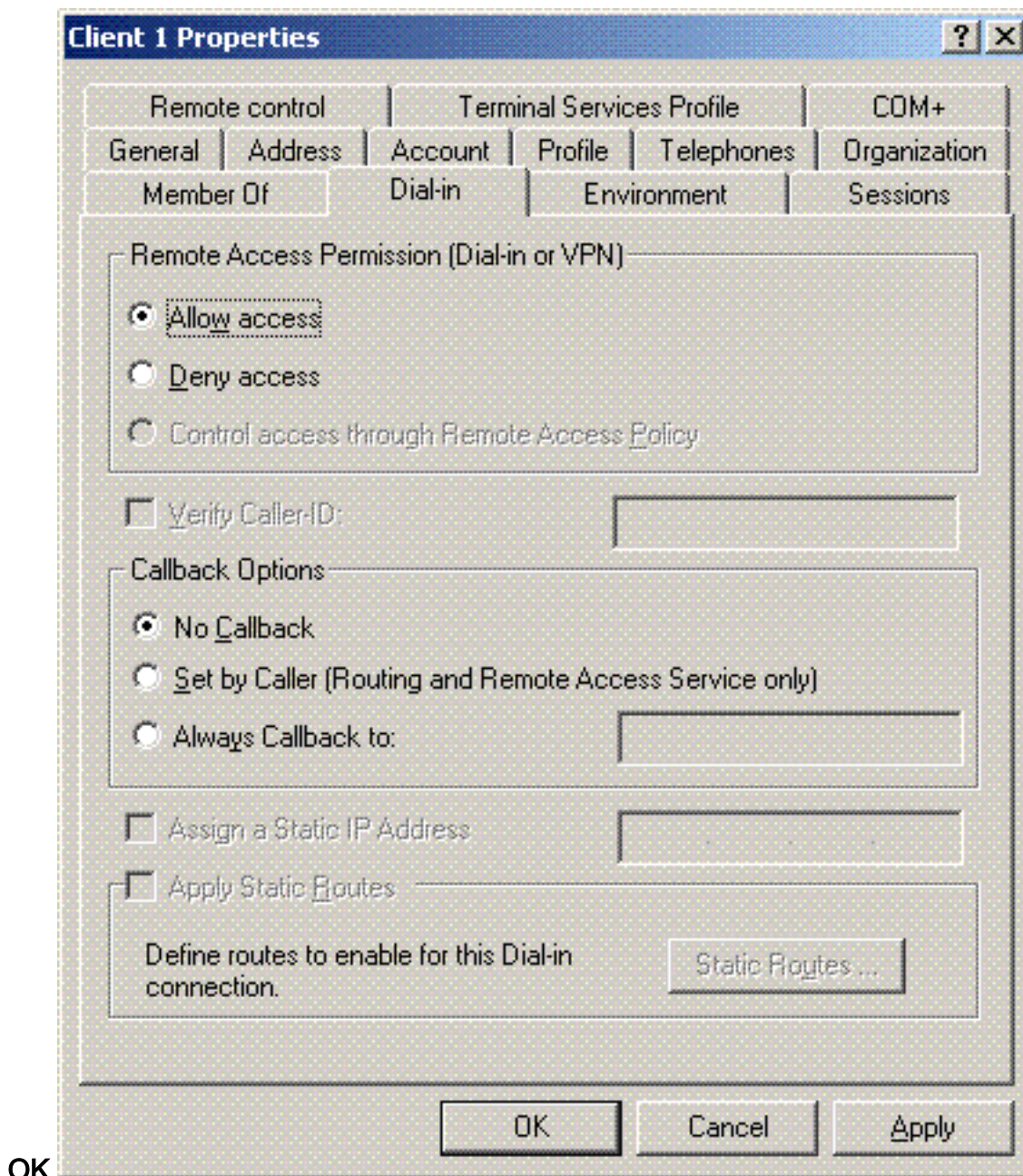
Voltoeien.

5. Herhaal stap 2 tot en met 4 om extra gebruikersaccounts te maken.

[Draadloze toegang voor gebruikers toestaan](#)

Voer de volgende stappen uit:

1. Klik in de structuur van de Active Directory-console op de **gebruikersmap**, klik met de rechtermuisknop op **Draadloze gebruiker**, klik op **Eigenschappen** en ga vervolgens naar het **tabblad Inbellen**.
2. Kies **Toegang toestaan** en klik op



OK.

[De draadloze LAN-controller en lichtgewicht AP's configureren](#)

Configureer nu de draadloze apparaten voor deze installatie. Dit omvat de configuratie van de draadloze LAN-controllers, lichtgewicht AP's en draadloze clients.

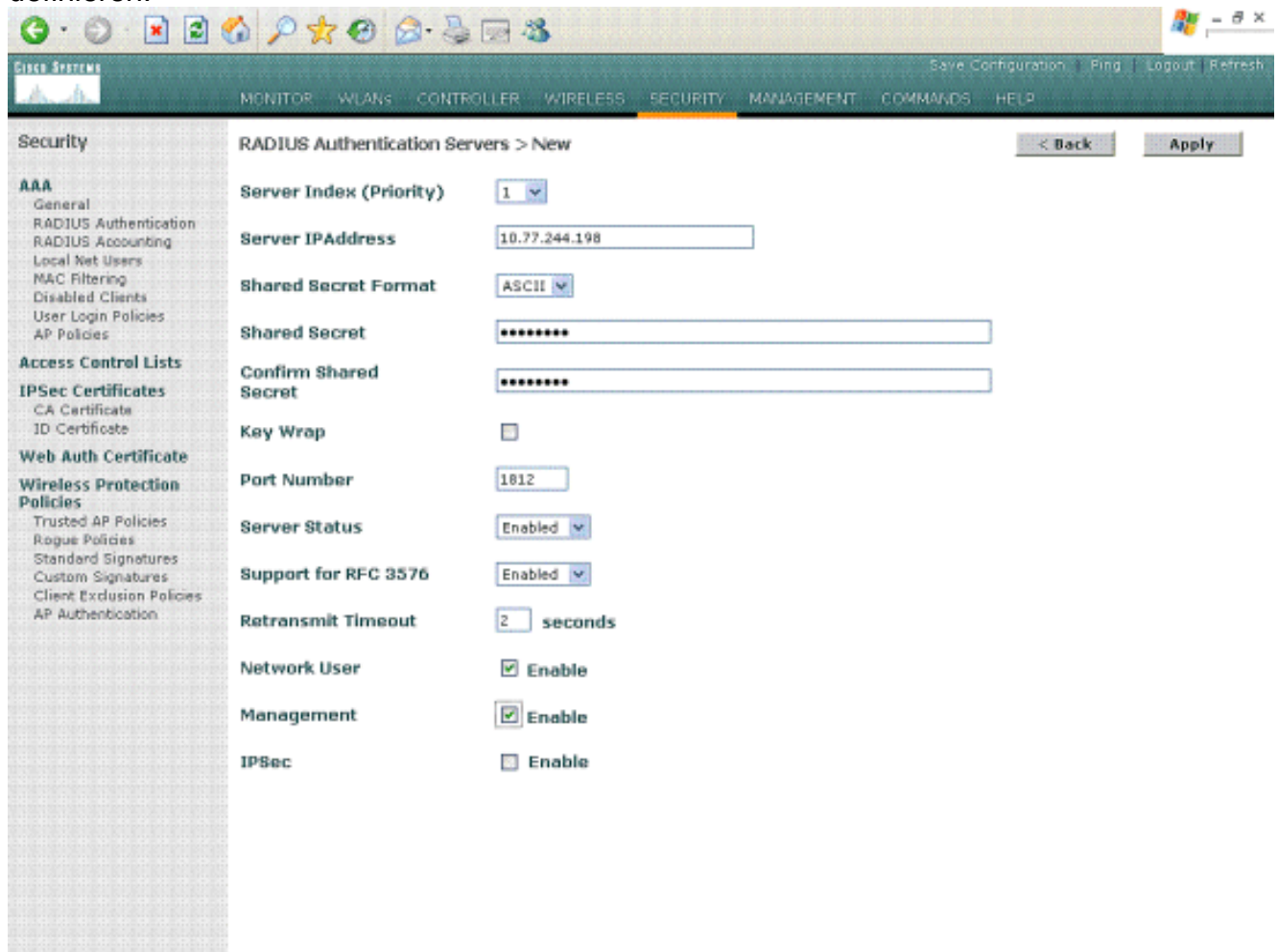
[De WLC voor RADIUS-verificatie configureren via MS IAS RADIUS-server](#)

Configureer eerst de WLC om de MS IAS als verificatieserver te gebruiken. De WLC moet worden geconfigureerd om de gebruikersreferenties te kunnen doorsturen naar een externe RADIUS-server. De externe RADIUS-server valideert vervolgens de gebruikersreferenties en biedt toegang tot de draadloze clients. Hiertoe voegt u de MS IAS-server als een RADIUS-server toe op de pagina **Security > RADIUS-verificatie**.

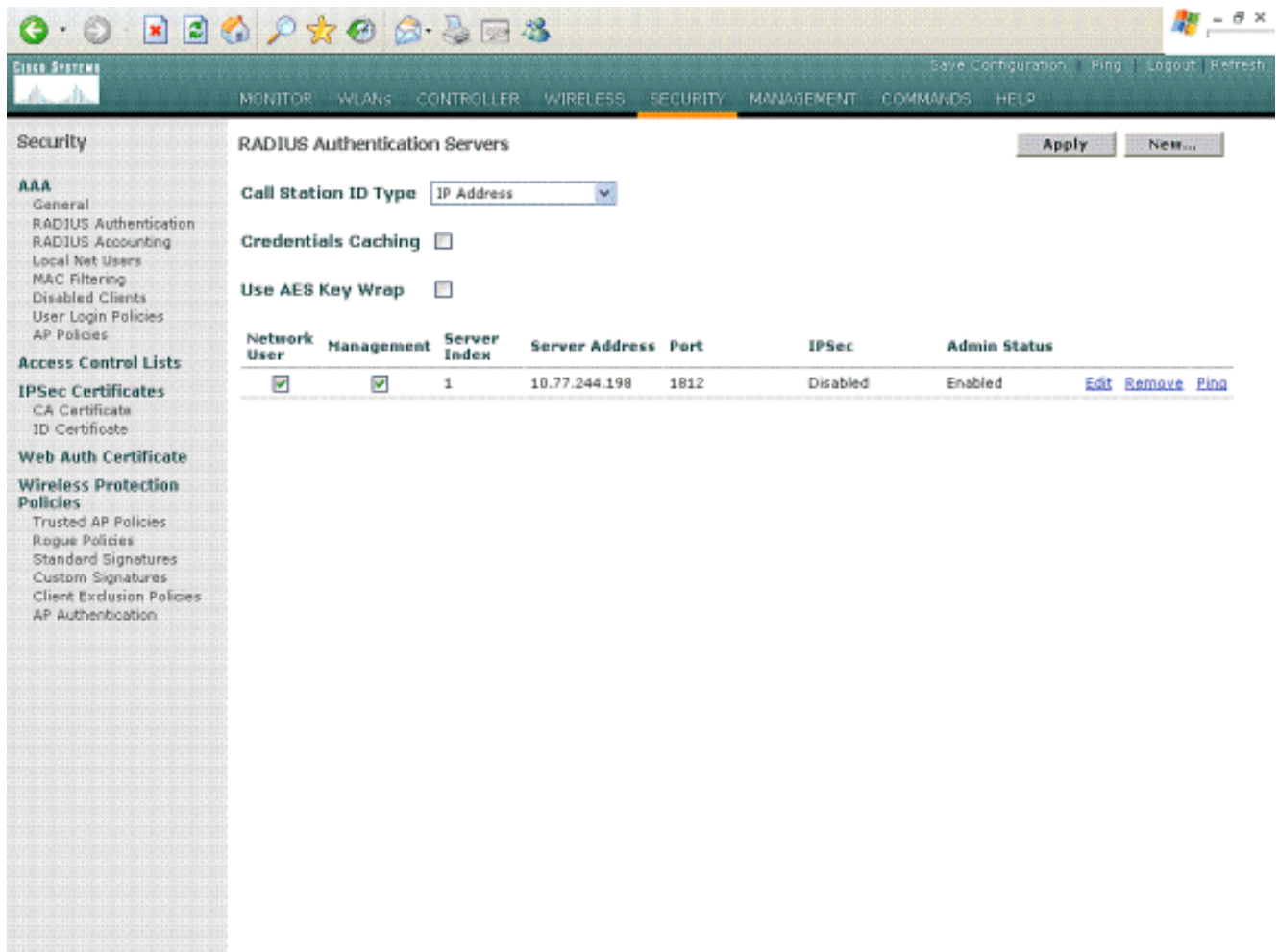
Voer de volgende stappen uit:

1. Kies **Beveiliging** en **RADIUS-verificatie** in de GUI van de controller om de pagina RADIUS-verificatieservers weer te geven. Klik vervolgens op **Nieuw** om een RADIUS-server te

definiëren.



2. Definieer de RADIUS-serverparameters in de **RADIUS-verificatieservers > Nieuwe** pagina. Deze parameters omvatten het IP-adres van de RADIUS-server, gedeeld geheim, poortnummer en serverstatus. Met de selectievakjes Netwerkgebruiker en Netwerkbeheer wordt bepaald of de op RADIUS gebaseerde verificatie van toepassing is op beheer- en netwerkgebruikers. In dit voorbeeld wordt de MS IAS gebruikt als de RADIUS-server met IP-adres 10.77.244.198.



3. Klik op **Apply** (Toepassen).
4. MS IAS server is toegevoegd aan de WLC als een Radius server en kan worden gebruikt om draadloze clients te verifiëren.

WLAN's voor de clients configureren

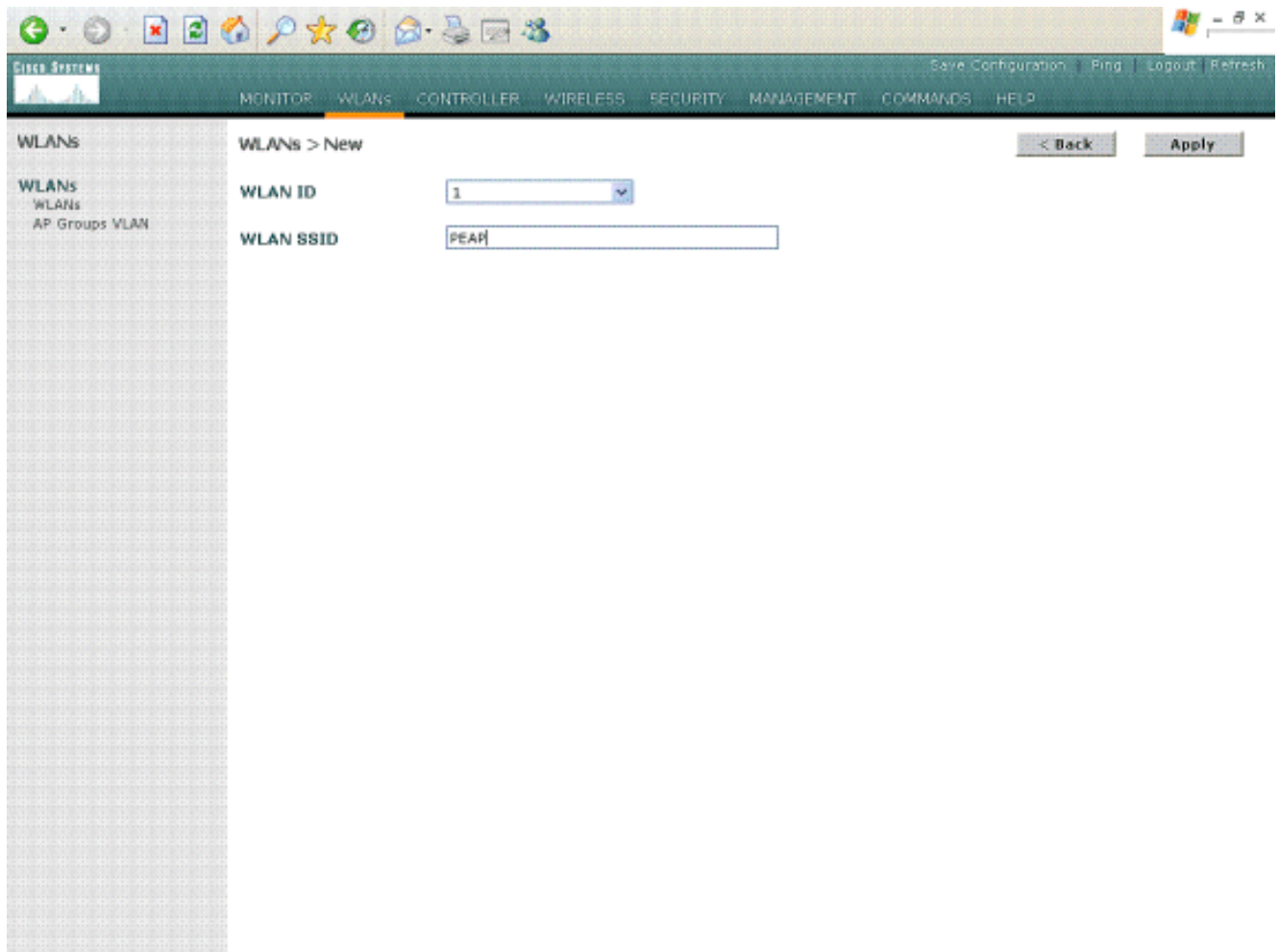
Configureer de SSID (WLAN) waarmee de draadloze clients verbinding maken. Maak in dit voorbeeld de SSID en noem het **PEAP**.

Definieer Layer 2-verificatie als WPA2, zodat de clients EAP-gebaseerde verificatie (in dit geval PEAP-MSCHAPv2) uitvoeren en AES als coderingsmechanisme gebruiken. Laat alle andere waarden op hun defaults staan.

Opmerking: dit document bindt het WLAN aan de beheerinterfaces. Wanneer u meerdere VLAN's in uw netwerk hebt, kunt u een afzonderlijk VLAN maken en het aan de SSID binden. Raadpleeg [VLAN's op Wireless LAN Controllers](#) Configuratie [Voorbeeld voor](#) informatie [over het configureren van](#) VLAN's [op](#) WLC's.

Voltooi de volgende stappen om een WLAN op de WLC te configureren:

1. Klik op **WLAN's** vanuit de GUI van de controller om de WLAN-pagina weer te geven. Deze pagina maakt een lijst van de WLAN's die op de controller bestaan.
2. Kies **Nieuw** om een nieuw WLAN te maken. Voer de WLAN-id en de WLAN-SSID voor het WLAN in en klik op **Toepassen**.



3. Zodra u een nieuw WLAN maakt, wordt de pagina **WLAN > Bewerken** voor het nieuwe WLAN weergegeven. Op deze pagina kunt u verschillende parameters definiëren die specifiek zijn voor dit WLAN, zoals Algemeen beleid, RADIUS-servers, beveiligingsbeleid en 802.1x-parameters.

The screenshot shows the Cisco Systems WLAN configuration interface. The main configuration area is titled 'WLAN ID 1' and 'Profile Name PEAP'. Under 'General Policies', 'Admin Status' is checked. Under 'Security Policies', 'Layer 2 Security' is set to 'WPA1+WPA2'. Other settings include 'Radio Policy' set to 'All', 'Session Timeout' set to '0', and 'Client Exclusion' set to 'Enabled' with a timeout value of '60'.

4. Controleer **Admin Status** onder Algemeen beleid om het WLAN in te schakelen. Als u wilt dat het toegangspunt de SSID uitzendt in zijn beacon-frames, controleer dan **Broadcast SSID**.
5. Kies onder Layer 2-beveiliging **WPA1+WPA2**. Dit schakelt WPA in op het WLAN. Blader naar beneden op de pagina en kies het WPA-beleid. In dit voorbeeld worden WPA2 en AES-encryptie gebruikt. Kies de juiste RADIUS-server in het keuzemenu onder RADIUS-servers. Gebruik in dit voorbeeld **10.77.244.198** (IP-adres van de MS IAS-server). De andere parameters kunnen worden aangepast op basis van de behoefte van het WLAN-netwerk.

The screenshot shows the 'WPA1+WPA2 Parameters' section of the configuration page. 'WPA2 Policy' is checked, and 'WPA2 Encryption' is set to 'AES'. The 'Auth Key Mgmt' is set to '802.1x'.

6. Klik op **Apply** (Toepassen).

The screenshot shows the 'WLANs' summary page. A table lists the configured WLANs:

Profile Name	WLAN ID	WLAN SSID	Admin Status	Security Policies
PEAP	1	PEAP	Enabled	[WPA2][Auth(802.1x)]

Below the table, a note states: '* WLAN IDs 9-16 will not be pushed to 1130,1200 and 1240 AP models.'

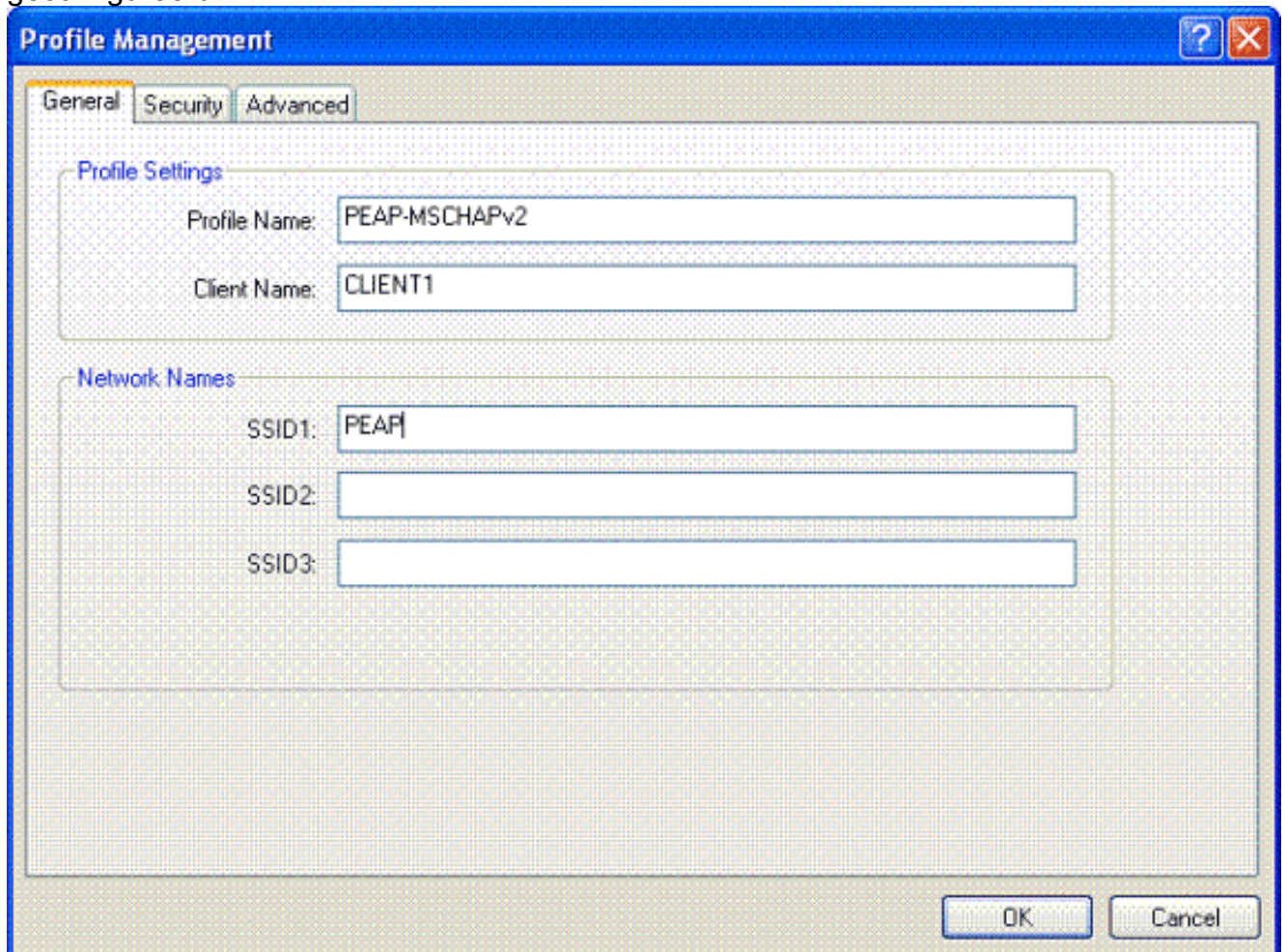
De draadloze clients configureren

De draadloze clients voor PEAP-MS CHAPv2-verificatie configureren

Dit voorbeeld bevat informatie over de manier waarop u de draadloze client kunt configureren met het Cisco Aironet Desktop Utility. Zorg ervoor dat de nieuwste versie van de firmware en het hulpprogramma wordt gebruikt voordat u de clientadapter configureert. Vind de nieuwste versie van de firmware en hulpprogramma's op de pagina Draadloze downloads op Cisco.com.

Voltooi de volgende stappen om de Cisco Aironet 802.11 a/b/g draadloze clientadapter met de ADU te configureren:

1. Open het Aironet-desktoophulpprogramma.
2. Klik op **Profielbeheer** en klik op **Nieuw** om een profiel te definiëren.
3. Voer op het tabblad Algemeen de naam van het profiel en de SSID in. Gebruik in dit voorbeeld de SSID die u op de WLC (PEAP) hebt geconfigureerd.

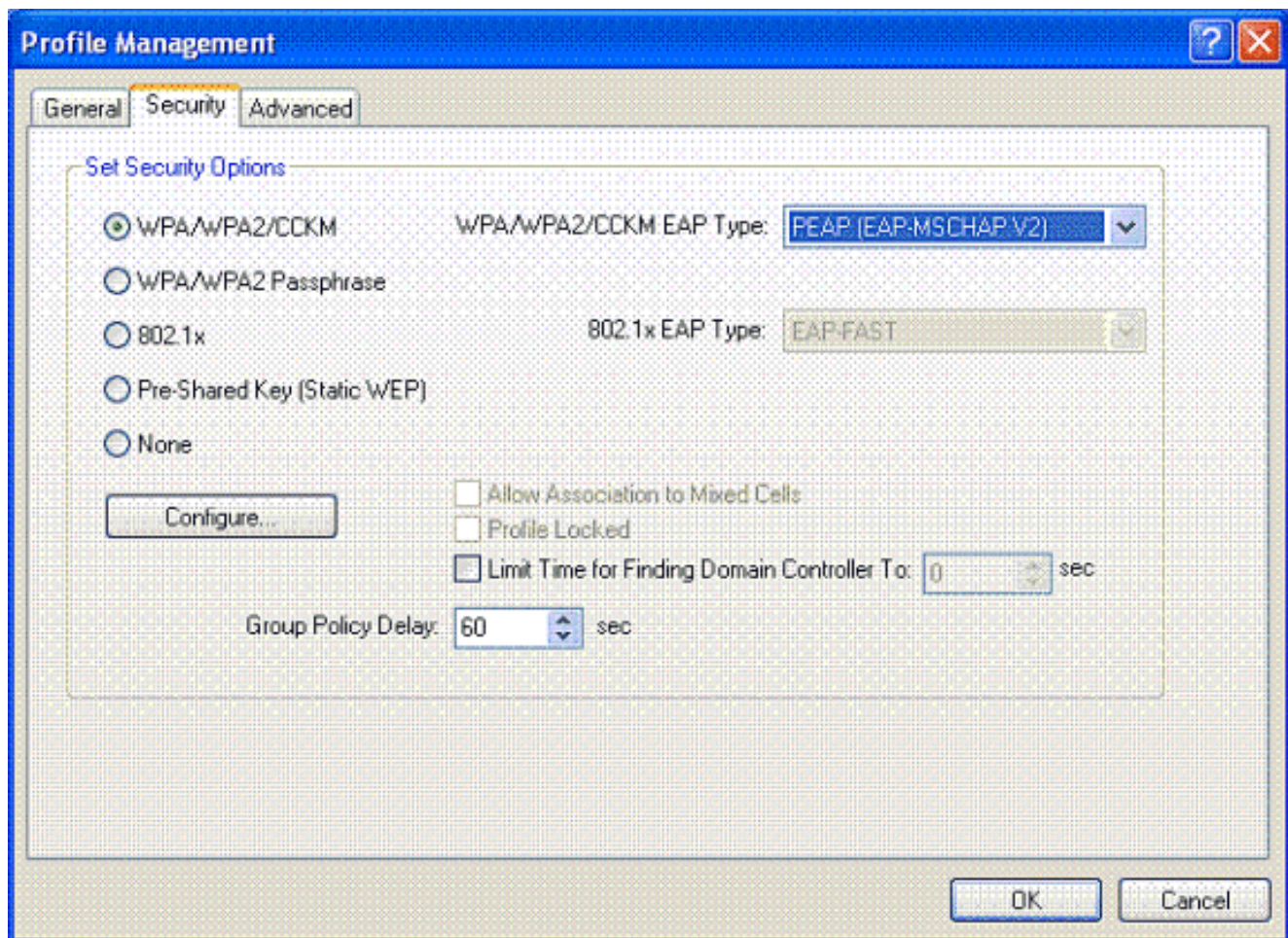


The screenshot shows the 'Profile Management' dialog box with the following fields:

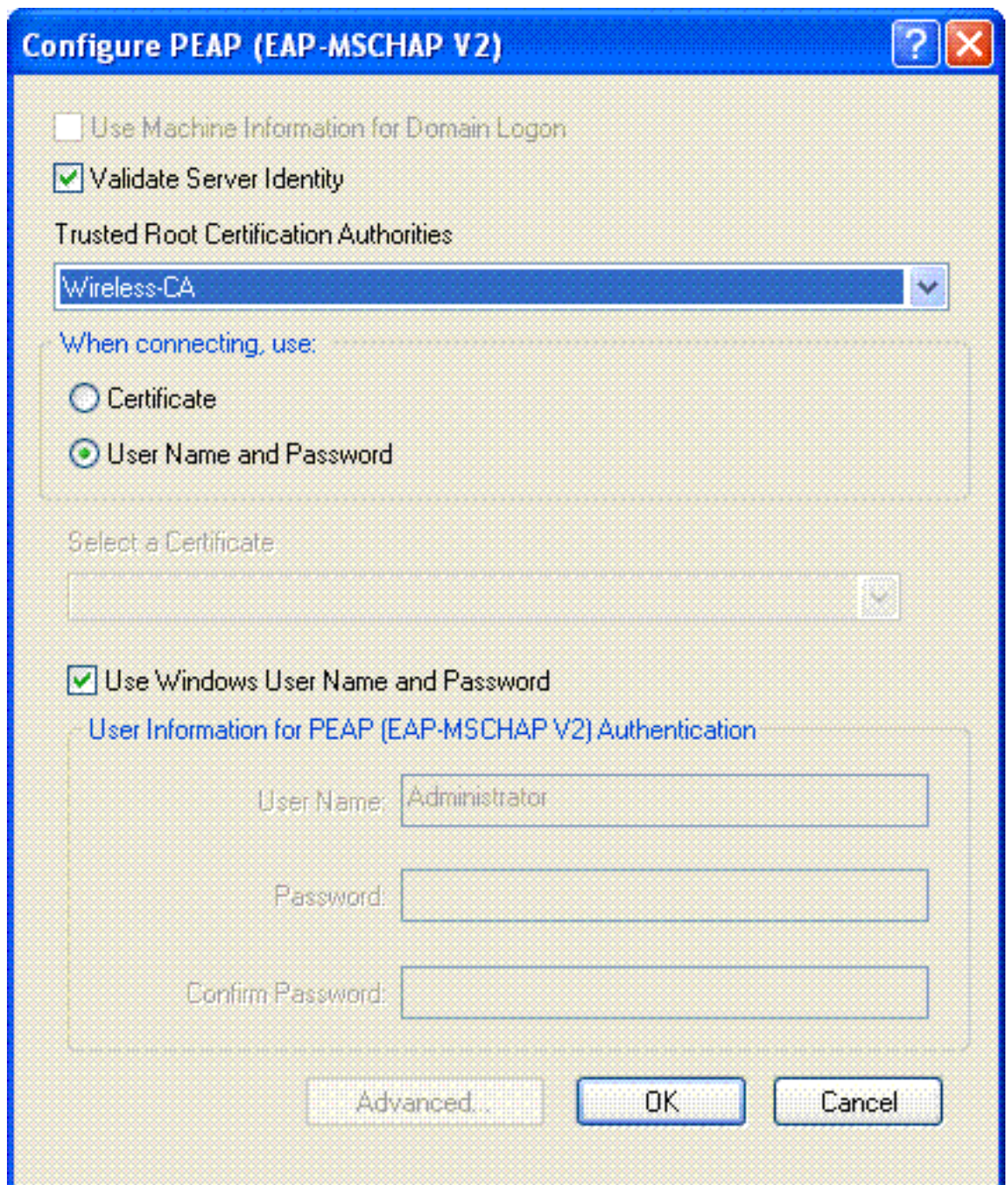
- Profile Name: PEAP-MSCHAPv2
- Client Name: CLIENT1
- SSID1: PEAP
- SSID2: (empty)
- SSID3: (empty)

Buttons: OK, Cancel

4. Kies het tabblad Beveiliging; kies **WPA/WPA2/CCKM**; typ onder WPA/WPA2/CCKM EAP de optie **PEAP [EAP-MSCHAPv2]** en klik op **Configureren**.



5. Kies **Servercertificaat valideren** en kies **Wireless-AC** onder het vervolgkeuzemenu Trusted Root Certificate

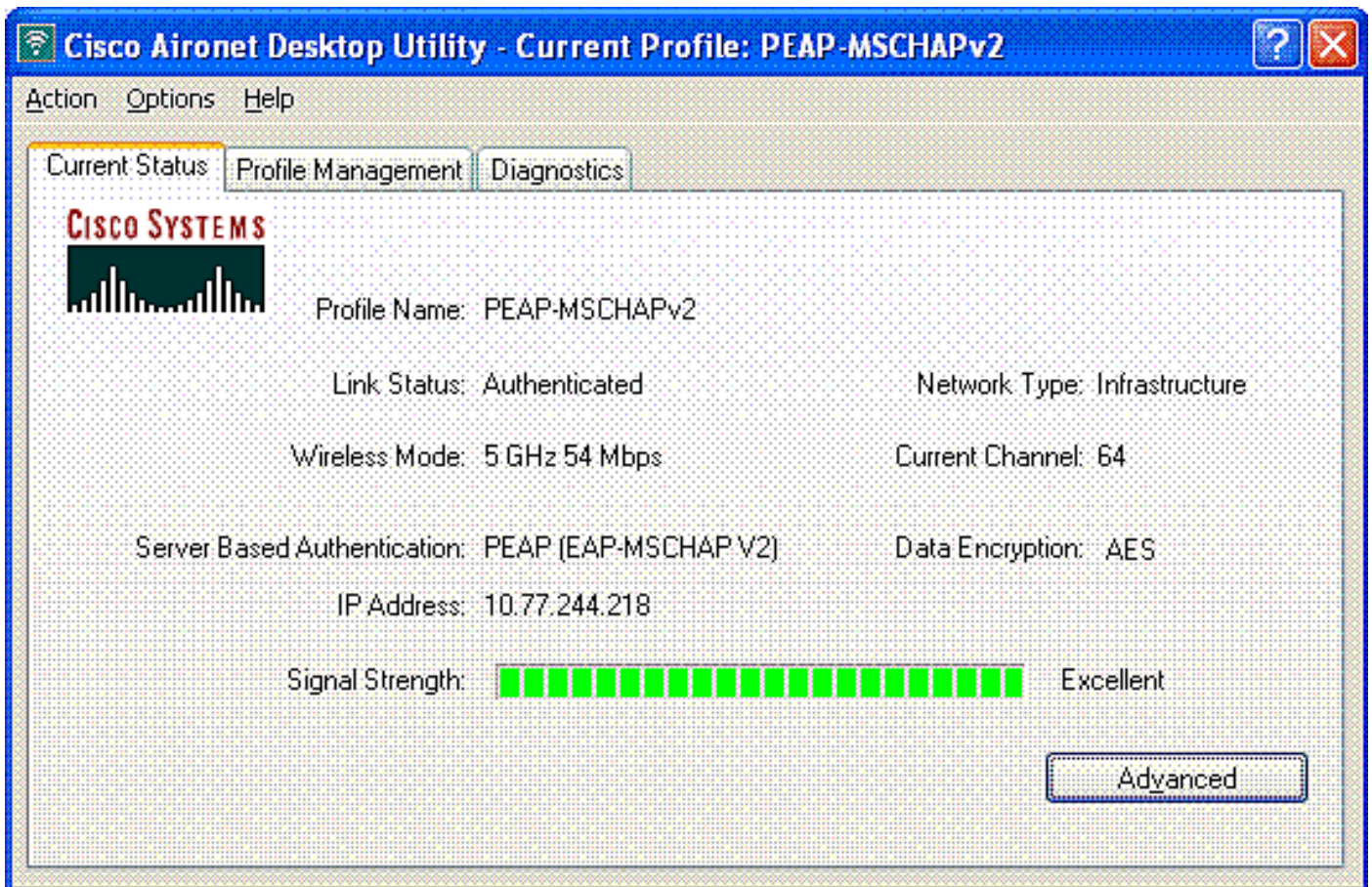


Authorities.

6. Klik op **OK** en activeer het profiel. **Opmerking:** wanneer u het Protected EAP-Microsoft Challenge Handshake Verificatieprotocol versie 2 (PEAP-MSCHAPv2) met Microsoft XP SP2 gebruikt en de draadloze kaart wordt beheerd door Microsoft Wireless Zero Configuration (WZC), moet u de Microsoft hotfix KB885453 toepassen. Dit voorkomt verschillende problemen met de verificatie in verband met PEAP Fast Resume.

Verifiëren en probleemoplossing

Om te controleren of de configuratie werkt zoals verwacht, activeert u het profiel PEAP-MSCHAPv2 op de draadloze client Client1.



Nadat het profiel PEAP-MSCHAPv2 op de ADU is geactiveerd, voert de client 802.11 open verificatie uit en voert vervolgens PEAP-MSCHAPv2-verificatie uit. Hier is een voorbeeld van succesvolle PEAP-MSCHAPv2-verificatie.

Gebruik de debug commando's om de volgorde van de gebeurtenissen te begrijpen die voorkomen.

De [Output Interpreter Tool](#) (OIT) (alleen voor [geregistreerde](#) klanten) ondersteunt bepaalde opdrachten met **show**. Gebruik de OIT om een analyse te bekijken van de output van de opdracht **show**.

Deze debug-opdrachten op de draadloze LAN-controller zijn handig.

- **debug dot1x gebeurtenissen inschakelen** —om het debuggen van 802.1x gebeurtenissen te configureren
- **debug aaa gebeurtenissen enable**-om het zuiveren van gebeurtenissen te vormen AAA
- **debug mac addr <mac address>** —om MAC-debugging te configureren gebruikt u de opdracht **debug mac**
- **debug dhcp bericht inschakelen** —om debug van DHCP-foutmeldingen te configureren

Dit zijn de voorbeelduitgangen van de **debug dot1x gebeurtenissen toelaten** bevel en **zuiveren client <mac address>** bevel.

debug dot1x gebeurtenissen inschakelen:

```
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received EAPOL START from
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Sending EAP-Request/Identity to
```


mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Creating a new PMK Cache**
Entry for station 00:40:96:ac:e6:57 (RSN 0)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending EAP-Success to**
mobile 00:40:96:ac:e6:57 (EAP Id 13)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending default RC4 key to**
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending Key-Mapping RC4 key to**
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Received Auth Success while in**
Authenticating state for mobile 00:40:96:ac:e6:57

debug mac addr <MAC Address>:

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Association received from**
mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 STA: 00:40:96:ac:e6:57 -
rates (8): 12 18 24 36 48 72 96 108 0 0 0 0 0 0
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 RUN (20)**
Change state to START (0)
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0)**
Initializing policy
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0)**
Change state to AUTHCHECK (2)
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 AUTHCHECK (2)**
Change state to 8021X_REQD (3)
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 8021X_REQD (3)**
Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Changing state for**
mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Stopping deletion of
Mobile Station: 00:40:96:ac:e6:57 (callerId: 48)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending Assoc Response to
station 00:40:96:ac:e6:57 on BSSID 00:0b:85:51:5a:e0 (status 0)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Changing state for
mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 Removed NPU entry.
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 dot1x - moving
mobile 00:40:96:ac:e6:57 into Connecting state
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Sending EAP-**
Request/Identity to mobile 00:40:96:ac:e6:57 (EAP Id 1)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Received EAPOL START from**
mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **EAP State update from**
Connecting to Authenticating for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 dot1x -**
moving mobile 00:40:96:ac:e6:57 into Authenticating state
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Req state (id=3) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 3)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57

Entering Backend Auth Req state (id=4) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 4)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Req state (id=5) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 5)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Req state (id=6) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Entering Backend Auth Req state (id=10) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Entering Backend Auth Req state (id=11) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 11)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Processing Access-Accept for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Creating a new PMK Cache Entry for station 00:40:96:ac:e6:57 (RSN 0)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Sending EAP-Success to mobile 00:40:96:ac:e6:57 (EAP Id 12)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Sending default RC4 key to mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Sending Key-Mapping RC4 key to mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
8021X_REQD (3) **Change state to L2AUTHCOMPLETE (4)**
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
L2AUTHCOMPLETE (4) Change state to RUN (20)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN

```
(20) Reached PLUMBFASPATH: from line 4041
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Replacing Fast Path rule
type = Airespace AP Client
on AP 00:0b:85:51:5a:e0, slot 0, interface = 2
ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20)
Card = 0 (slot 0), InHandle = 0x00000000,
OutHandle = 0x00000000, npuCryptoFlag = 0x0000
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Successfully plumbed mobile rule (ACL ID 255)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Reached RETURN: from line 4041
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend
Auth Success state (id=12) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Received Auth Success
while in Authenticating state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 dot1x -
moving mobile 00:40:96:ac:e6:57 into Authenticated state
```

Opmerking: als u de Microsoft Supplicant gebruikt voor verificatie met een Cisco Secure ACS voor PEAP-verificatie, wordt de client mogelijk niet geverifieerd. Soms kan de eerste verbinding met succes worden geverifieerd, maar latere pogingen voor snelle verificatie maken geen verbinding met succes. Dit is een bekende kwestie. De details van dit probleem en de oplossing voor hetzelfde zijn [hier](#) beschikbaar.

[Gerelateerde informatie](#)

- [PEAP onder Unified Wireless Networks met ACS 4.0 en Windows 2003](#)
- [Configuratie-voorbeeld van EAP-verificatie met WLAN-controllen \(WLC\)](#)
- [Software-upgrade voor draadloze LAN-controllen \(WLC\) naar versies 3.2, 4.0 en 4.1](#)
- [Cisco 4400 Series configuratiehandleidingen voor draadloze LAN-controllen](#)
- [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.