NPS, draadloze LAN-controllers en draadloze netwerken configureren

Inhoud

Inleiding

In dit document wordt beschreven hoe u de PEAP met MS-CHAP-verificatie configureert met de Microsoft NPS als de RADIUS-server.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van Windows 2008 installatie
- Kennis van installatie van Cisco-controller

Zorg ervoor dat aan deze vereisten is voldaan voordat u deze configuratie probeert:

- Installeer de Microsoft Windows Server 2008 op elk van de servers in het testlaboratorium.
- Alle servicepacks bijwerken.
- Installeer de controllers en lichtgewicht toegangspunten (LAP's).
- Configureer de nieuwste software-updates.

Raadpleeg de installatiehandleiding voor de draadloze controller uit de Cisco 5500-reeks voor informatie over de eerste installatie en configuratie van de Cisco 5508-reeks.

Opmerking: Dit document is bedoeld om de lezers een voorbeeld te geven van de configuratie die vereist is op een Microsoft-server voor PEAP-MS-CHAP-verificatie. De Microsoft Windows-serverconfiguratie die in dit document wordt weergegeven, is in het laboratorium getest en werkt naar verwachting. Als u problemen ondervindt met de configuratie, neemt u contact op met Microsoft voor hulp. Het Cisco Technical Assistance Center (TAC) biedt geen ondersteuning voor Microsoft Windows-serverconfiguratie.

Installatie- en configuratiehandleidingen voor Microsoft Windows 2008 zijn te vinden op Microsoft Tech Net.

Gebruikte componenten

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

- Cisco 5508 draadloze controller waarop firmware versie 7.4 wordt uitgevoerd
- Cisco Aironet 3602 Access Point (AP) met LWAPP (Lightweight Access Point Protocol)
- Windows 2008 Enterprise Server met NPS, Certificate Authority (CA), Dynamic Host Control Protocol (DHCP) en Domain Name System (DNS)-services geïnstalleerd
- Microsoft Windows 7-client-pc
- Cisco Catalyst 3560-serie 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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Conventies

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

Achtergrondinformatie

Dit document bevat een voorbeeldconfiguratie voor het Protected Extensible Authentication Protocol (PEAP) met Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) versie 2-verificatie in een Cisco Unified Wireless-netwerk met de Microsoft Network Policy Server (NPS) als RADIUS-server.

PEAP-overzicht

PEAP maakt gebruik van Transport Level Security (TLS) om een gecodeerd kanaal te maken tussen een geverifieerde PEAP-client, zoals een draadloze laptop, en een PEAP-verificator, zoals Microsoft NPS of een RADIUS-server. PEAP specificeert geen verificatiemethode, maar biedt extra beveiliging voor andere EAP's (Extensible Authentication Protocols), zoals EAP-MS-CHAP v2, die kunnen werken via het TLS-gecodeerde kanaal van PEAP. Het PEAP-authenticatieproces bestaat uit twee hoofdfasen.

PEAP fase één: TLS-gecodeerd kanaal

De draadloze client wordt aan het toegangspunt gekoppeld. Een op IEEE 802.11 gebaseerde koppeling biedt een open systeem of gedeelde sleutelverificatie voordat een beveiligde koppeling wordt gemaakt tussen de client en het toegangspunt. Nadat de op IEEE 802.11 gebaseerde koppeling tussen de client en het toegangspunt tot stand is gebracht, wordt met het toegangspunt onderhandeld over de TLS-sessie. Nadat de verificatie is voltooid tussen de draadloze client en NPS, wordt de TLS-sessie onderhandeld tussen de client en NPS. De sleutel die wordt afgeleid binnen deze onderhandeling wordt gebruikt om alle daaropvolgende communicatie te versleutelen.

PEAP fase twee: EAP-geauthentiseerde communicatie

EAP-communicatie, waaronder EAP-onderhandeling, vindt plaats binnen het TLS-kanaal dat door PEAP is gemaakt in de eerste fase van het PEAP-verificatieproces. De NPS 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 Wireless LAN Controller (WLC) en het LAP kunnen deze berichten niet decoderen omdat dit niet het TLS-eindpunt is.

De RADIUS-berichtenreeks voor een geslaagde verificatiepoging (waarbij de gebruiker geldige op een wachtwoord gebaseerde referenties heeft opgegeven bij PEAP-MS-CHAP v2) is:

1. De NPS stuurt een identiteitsaanvraagbericht naar de klant: EAP-Request/Identity.
2. De client reageert met een identiteitsreactie: EAP-Response/Identity.
3. De NPS verzendt een MS-CHAP v2 challenge bericht: EAP-Request/EAP-Type=EAP MS-CHAP-V2 (Challenge).
4. De client reageert met een MS-CHAP v2 challenge en respons: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response).
5. De NPS stuurt een MS-CHAP v2-succespakket terug wanneer de server de client met succes heeft geverifieerd: EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (Succes).

6. De client reageert met een MS-CHAP v2-succespakket wanneer de client de server met succes heeft geverifieerd: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Succes).
7. De NPS verzendt een EAP-type-length-value (TLV) die een succesvolle verificatie aangeeft.
8. De client reageert met een EAP-TLV-statussuccesbericht.
9. De server voltooit de verificatie en verzendt een EAP-succesbericht in platte tekst. Als VLAN's worden geïmplementeerd voor clientisolatie, worden de VLAN-kenmerken in dit bericht opgenomen.

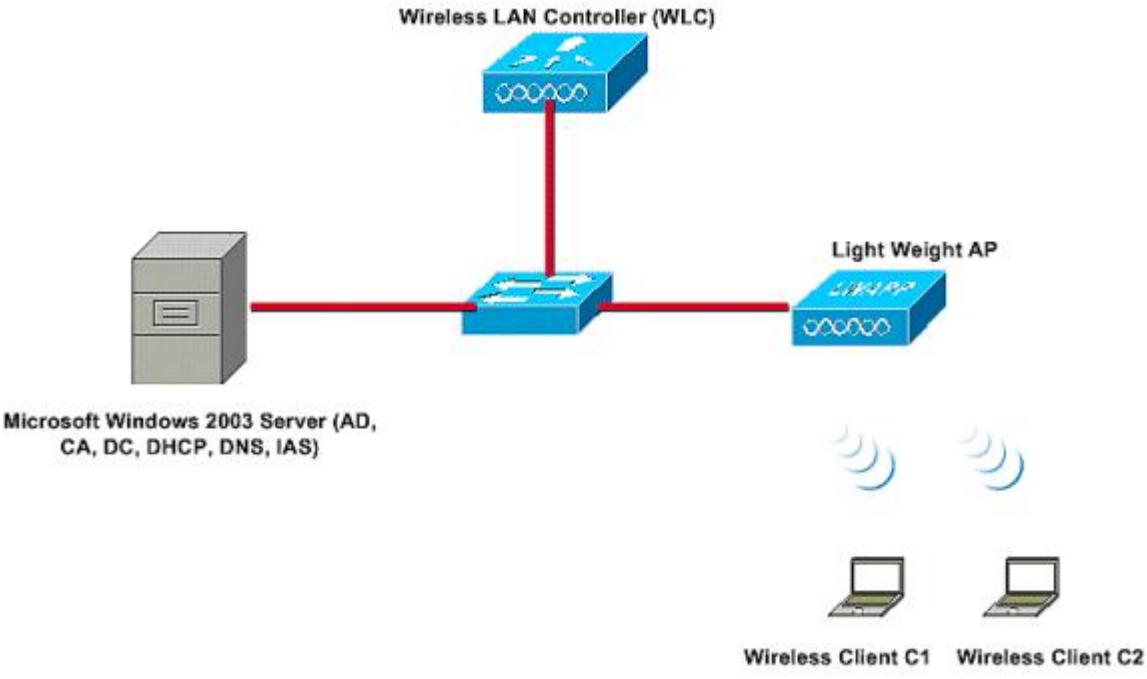
Configureren

In deze sectie vindt u de informatie voor het configureren van PEAP-MS-CHAP v2.

Opmerking: gebruik de Command Lookup Tool voor meer informatie over de commando's die in deze paragraaf worden gebruikt. Alleen geregistreerde Cisco-gebruikers hebben toegang tot interne Cisco-tools en -informatie.

Netwerkdiagram

Deze configuratie maakt gebruik van de volgende netwerkconfiguratie:



Netwerkdiagram

In deze configuratie voert een Microsoft Windows 2008-server de volgende rollen uit:

- Domeincontroller voor het domein
- DHCP/DNS-server
- CA-server
- NPS – voor verificatie van de draadloze gebruikers

- Active Directory – om de gebruikersdatabase te onderhouden

De server maakt verbinding met het bekabelde netwerk via een Layer 2-switch, zoals wordt weergegeven. De WLC en de geregistreerde LAP maken ook verbinding met het netwerk via de Layer 2-switch.

De draadloze clients maken gebruik van Wi-Fi Protected Access 2 (WPA2) - PEAP-MS-CHAP v2-verificatie om verbinding te maken met het draadloze netwerk.

Configuraties

Het doel van dit voorbeeld is de Microsoft 2008-server, draadloze LAN-controller en lichtgewicht toegangspunt te configureren om de draadloze clients te verifiëren met PEAP-MS-CHAP v2-verificatie. Er zijn drie belangrijke stappen in dit proces:

1. De Microsoft Windows 2008-server configureren.
2. Configureer de WLC en de lichtgewicht toegangspunten.
3. Configureer de draadloze clients.

De Microsoft Windows 2008-server configureren

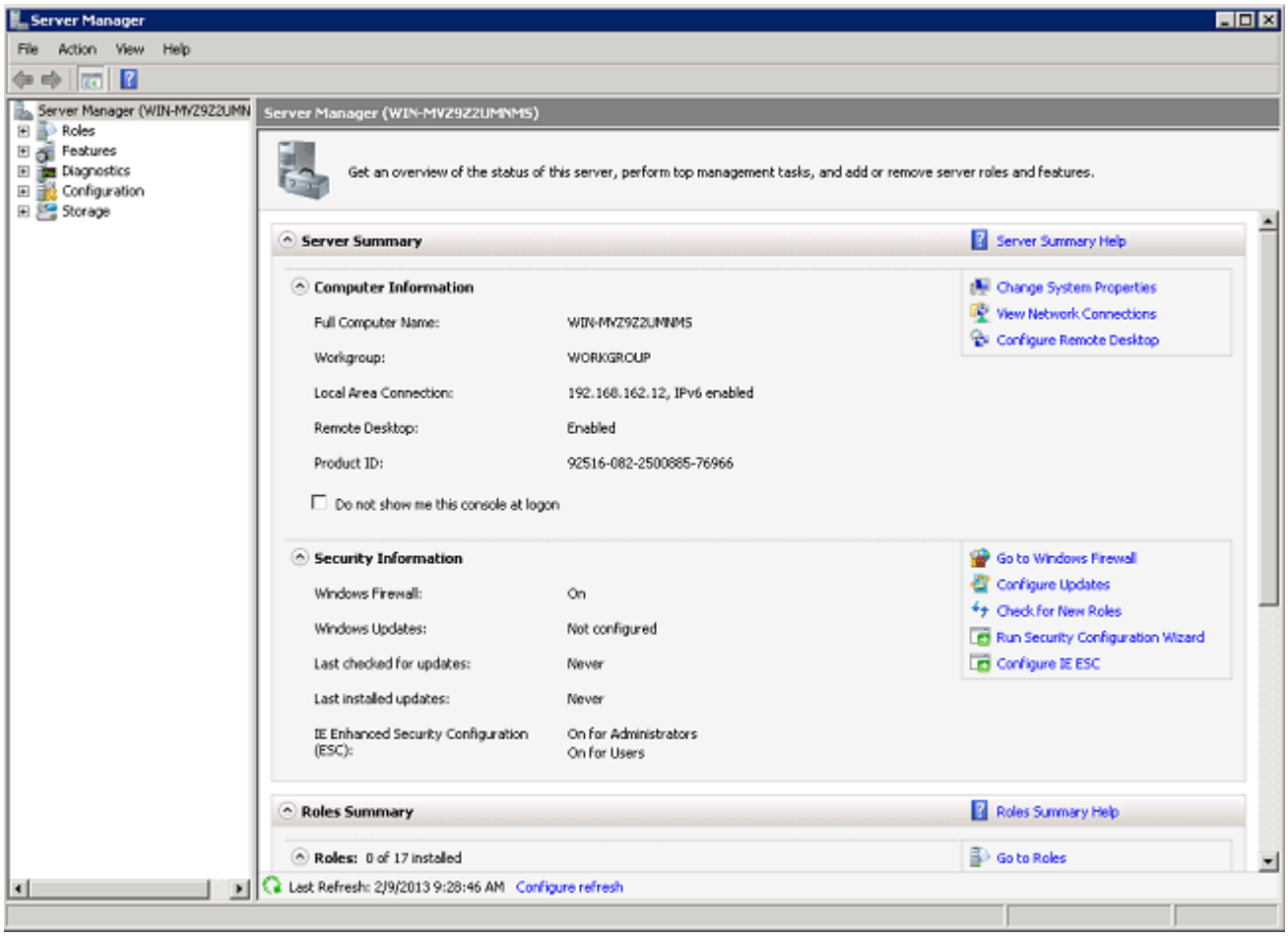
In dit voorbeeld bevat een volledige configuratie van de Microsoft Windows 2008-server de volgende stappen:

1. Configureer de server als een domeincontroller.
2. DHCP-services installeren en configureren.
3. de server installeren en configureren als een CA-server.
4. Klanten verbinden met het domein.
5. Installeer de NPS.
6. Een certificaat installeren.
7. Configureer de NPS voor PEAP-verificatie.
8. Gebruikers toevoegen aan de Active Directory.

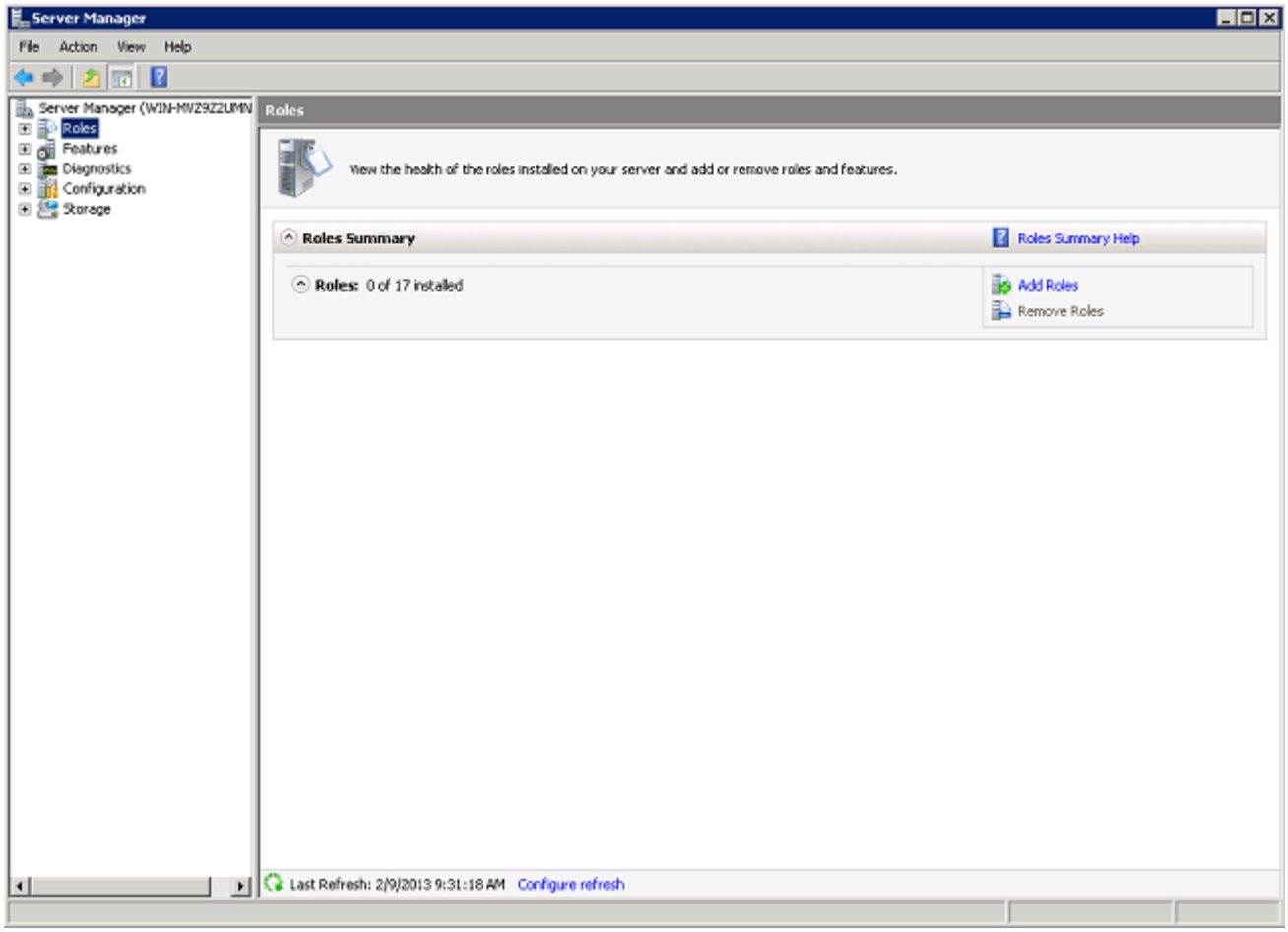
De Microsoft Windows 2008-server configureren als domeincontroller

Voer deze stappen uit om de Microsoft Windows 2008-server als domeincontroller te configureren:

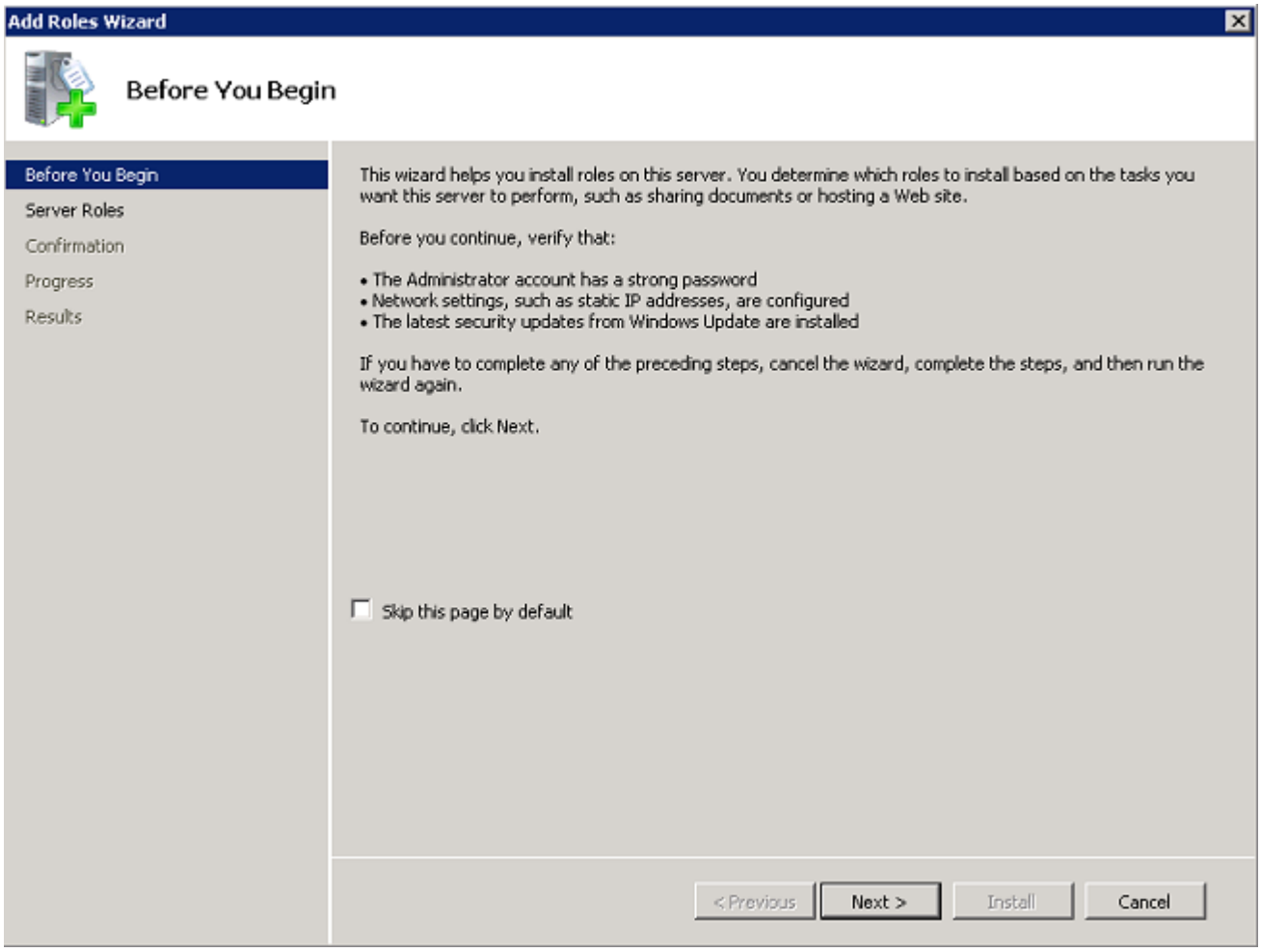
1. Klik op Start> Serverbeheer.



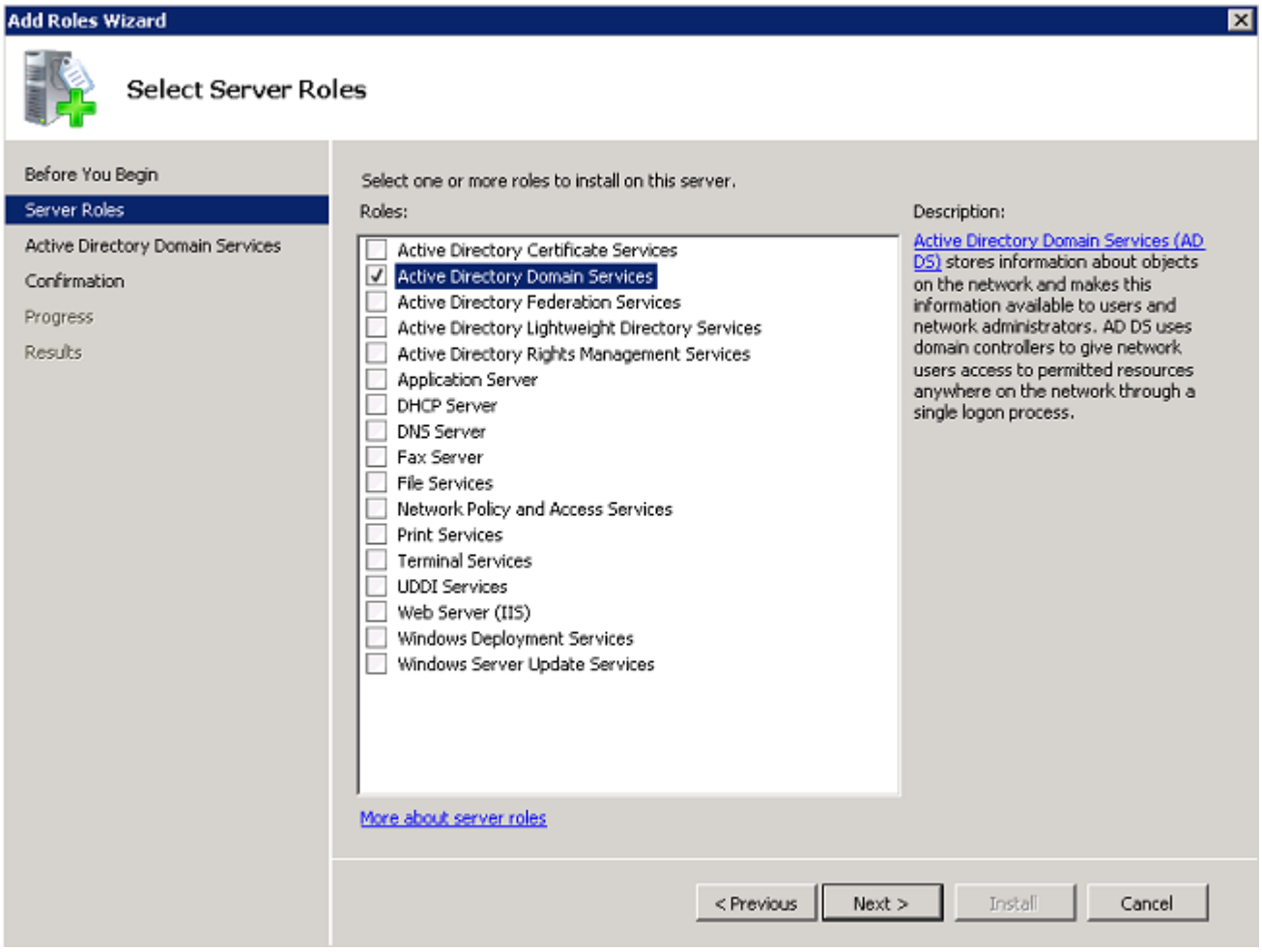
2. Klik op Rollen> Rollen toevoegen.



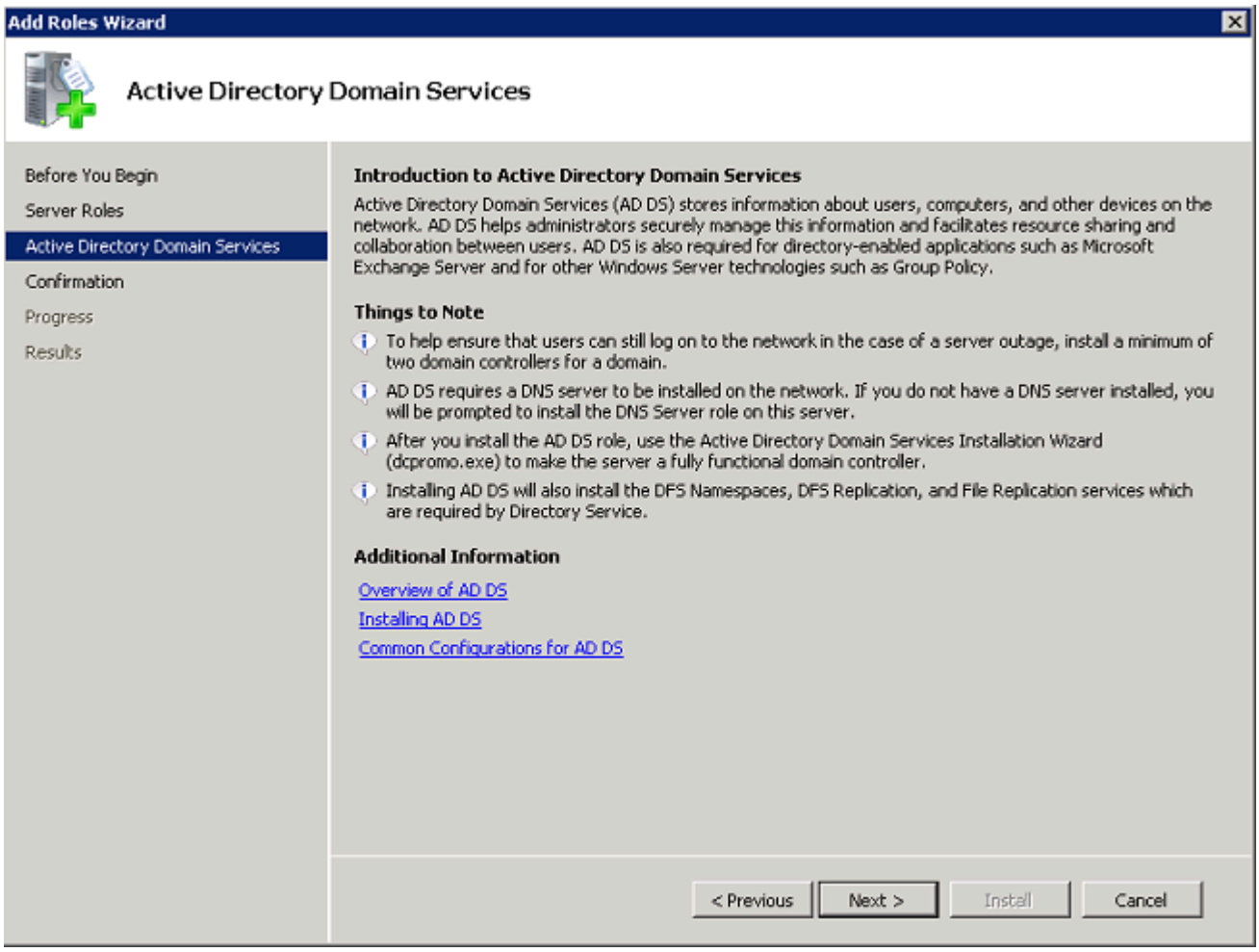
3. Klik op Next (Volgende).



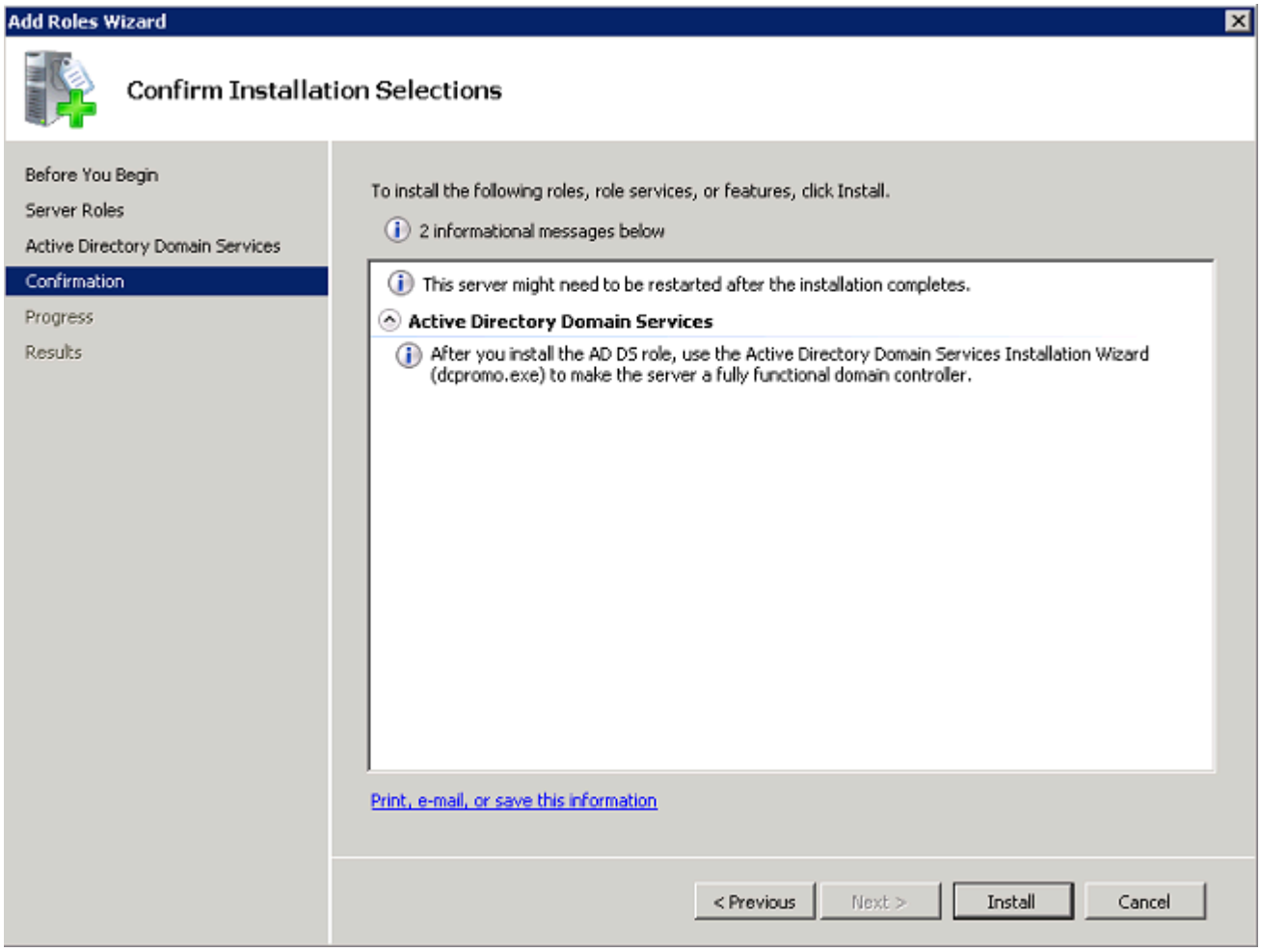
4. Selecteer de service Active Directory Domain Services en klik op Volgende.



5. Controleer de introductie van Active Directory Domain Services en klik op Volgende.

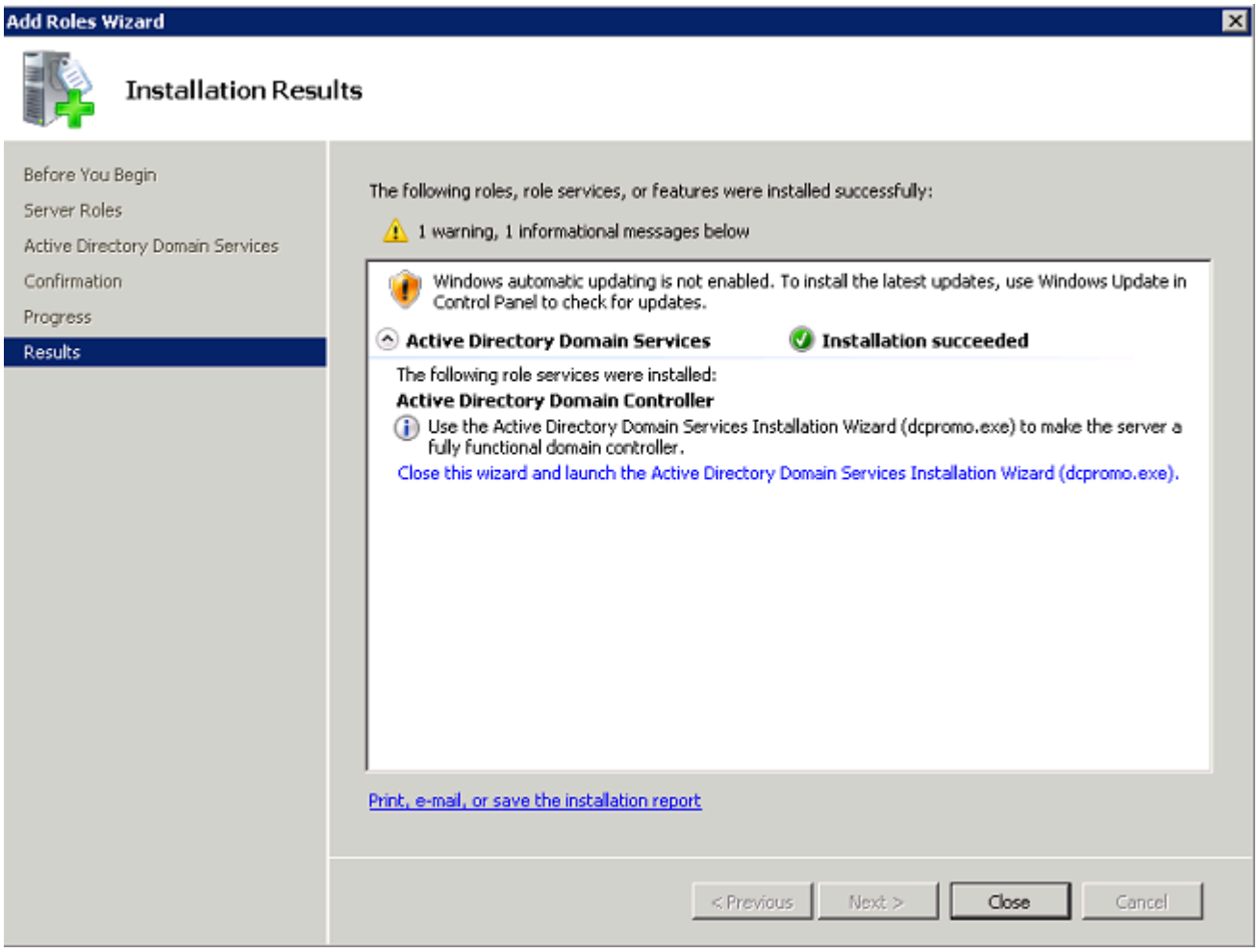


6. Klik op Installeren om het installatieproces te starten.

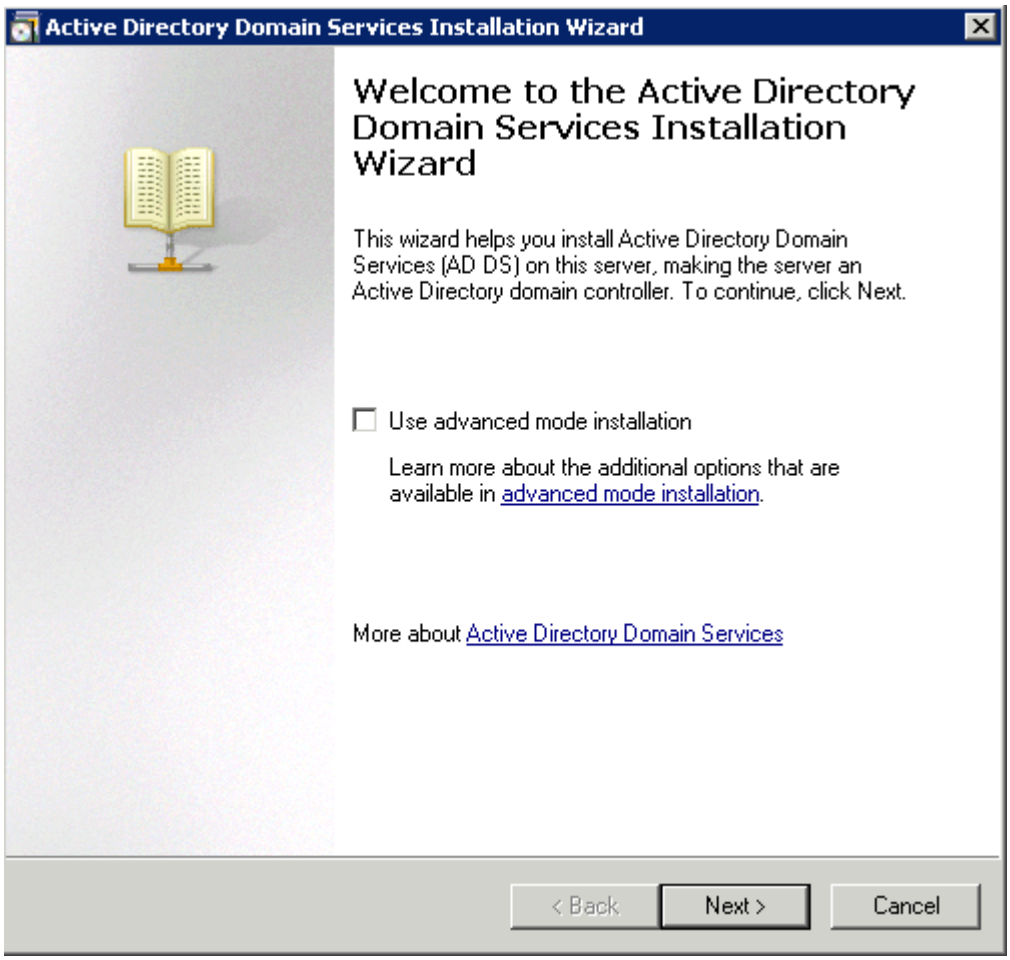


De installatie gaat door en wordt voltooid.

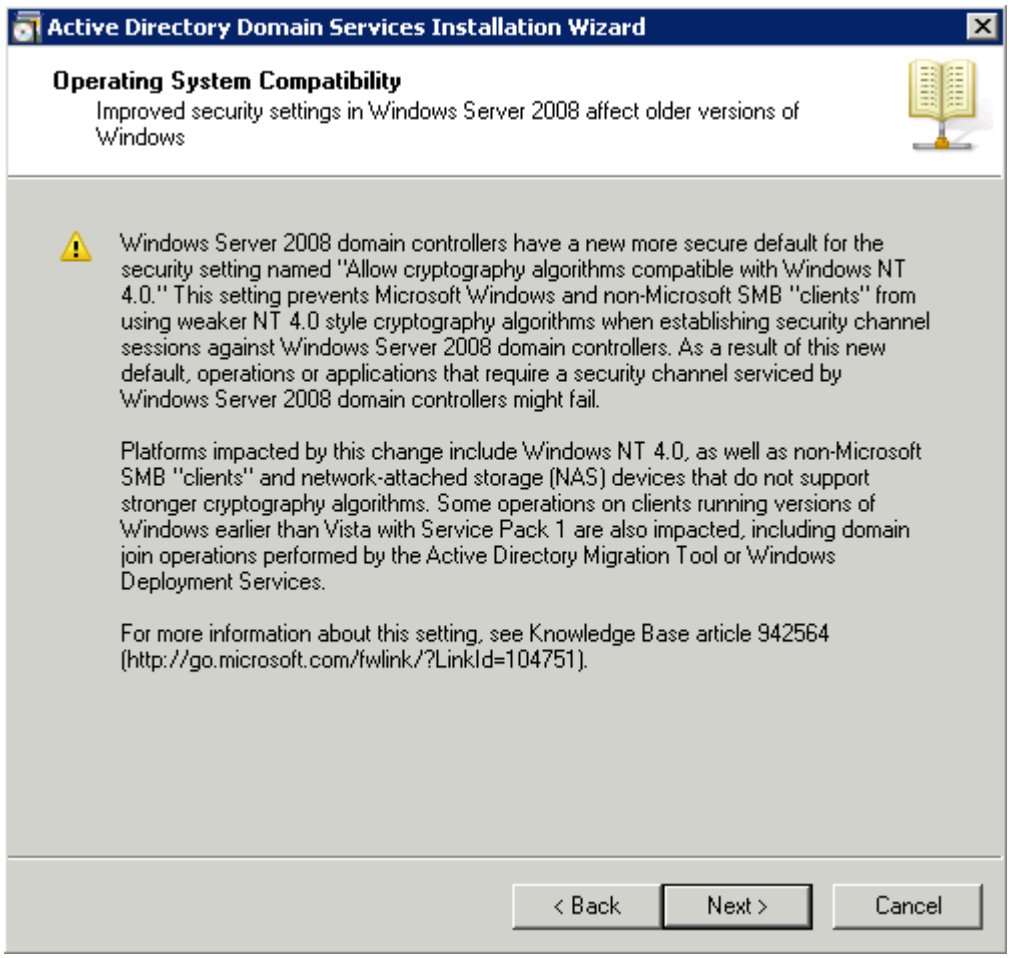
7. Klik op Deze wizard sluiten en start de installatiewizard voor Active Directory Domain Services (dcpromo.exe) om door te gaan met de installatie en configuratie van de Active Directory.



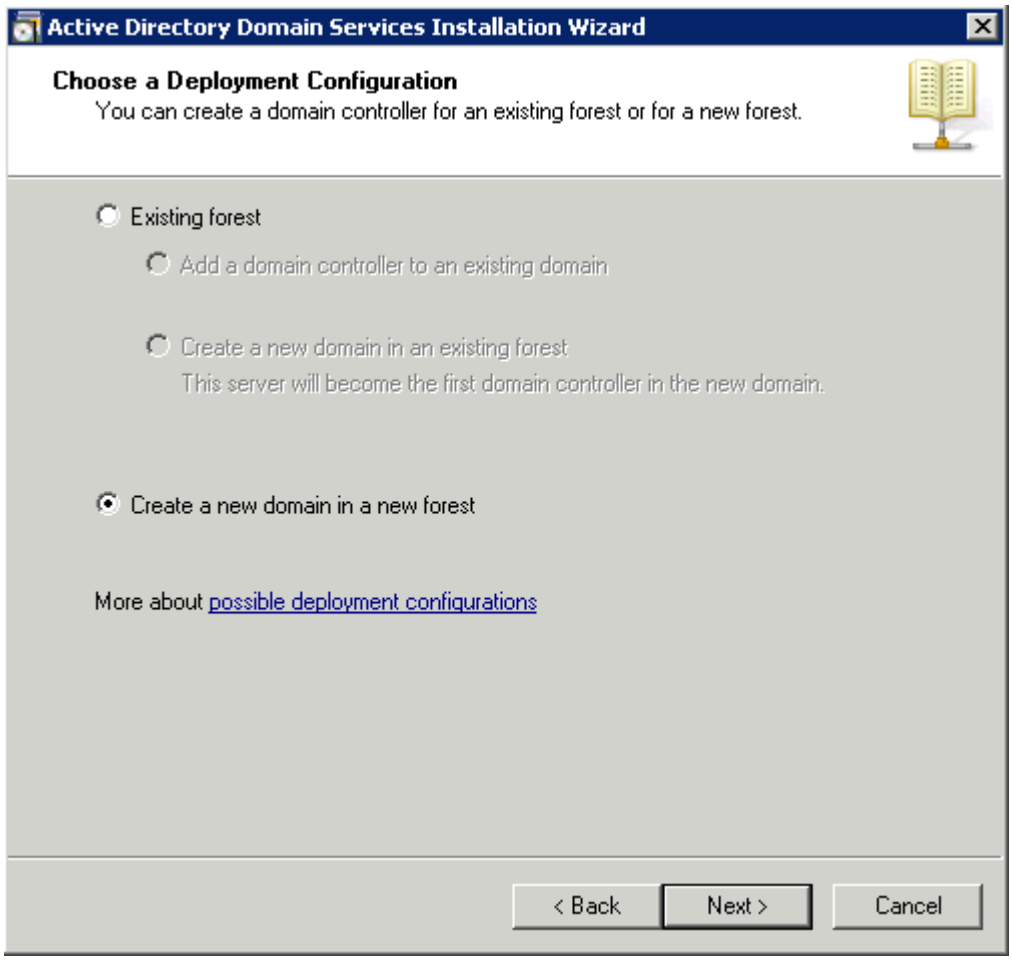
8. Klik op Volgende om de installatiewizard voor Active Directory Domain Services uit te voeren.



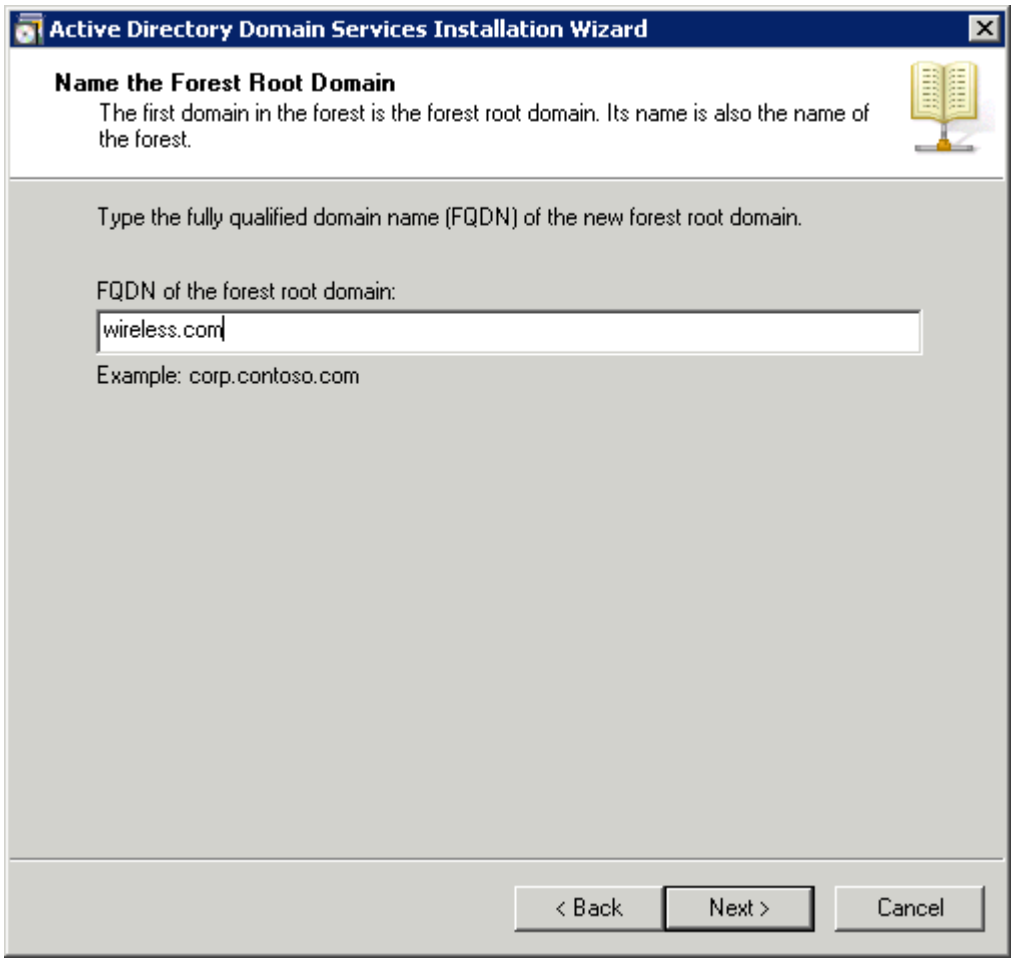
9. Controleer de informatie over de compatibiliteit van het besturingssysteem en klik op Volgende.



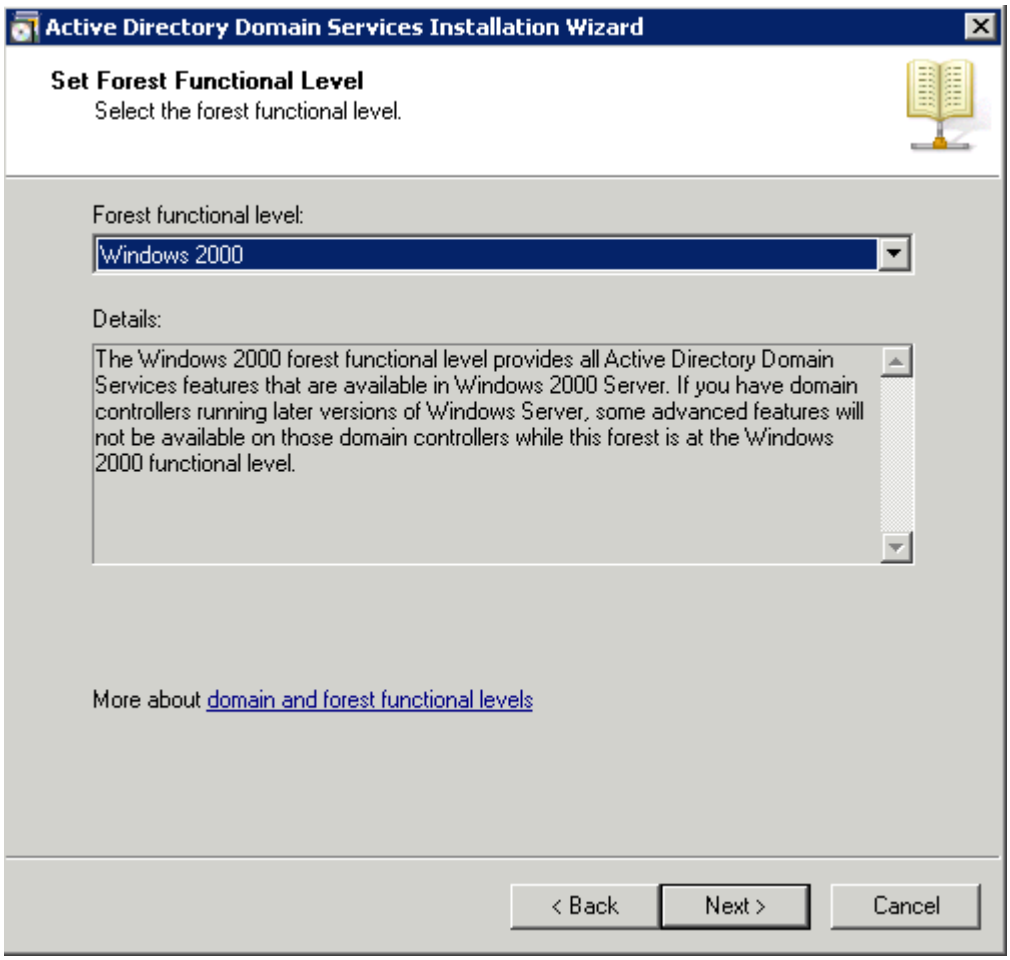
10. Klik op Een nieuw domein maken in een nieuw forest > Volgende om een nieuw domein te maken.



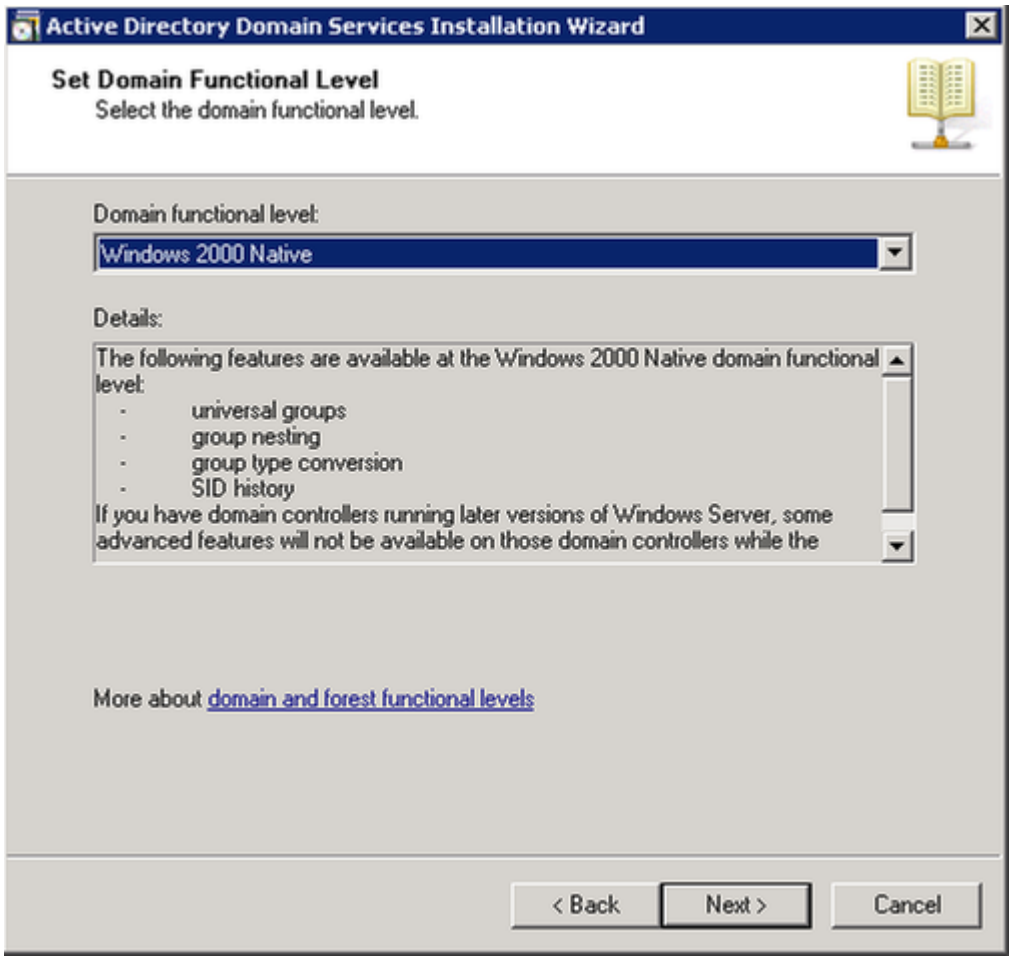
11. Voer de volledige DNS-naam in voor het nieuwe domein en klik op Volgende.



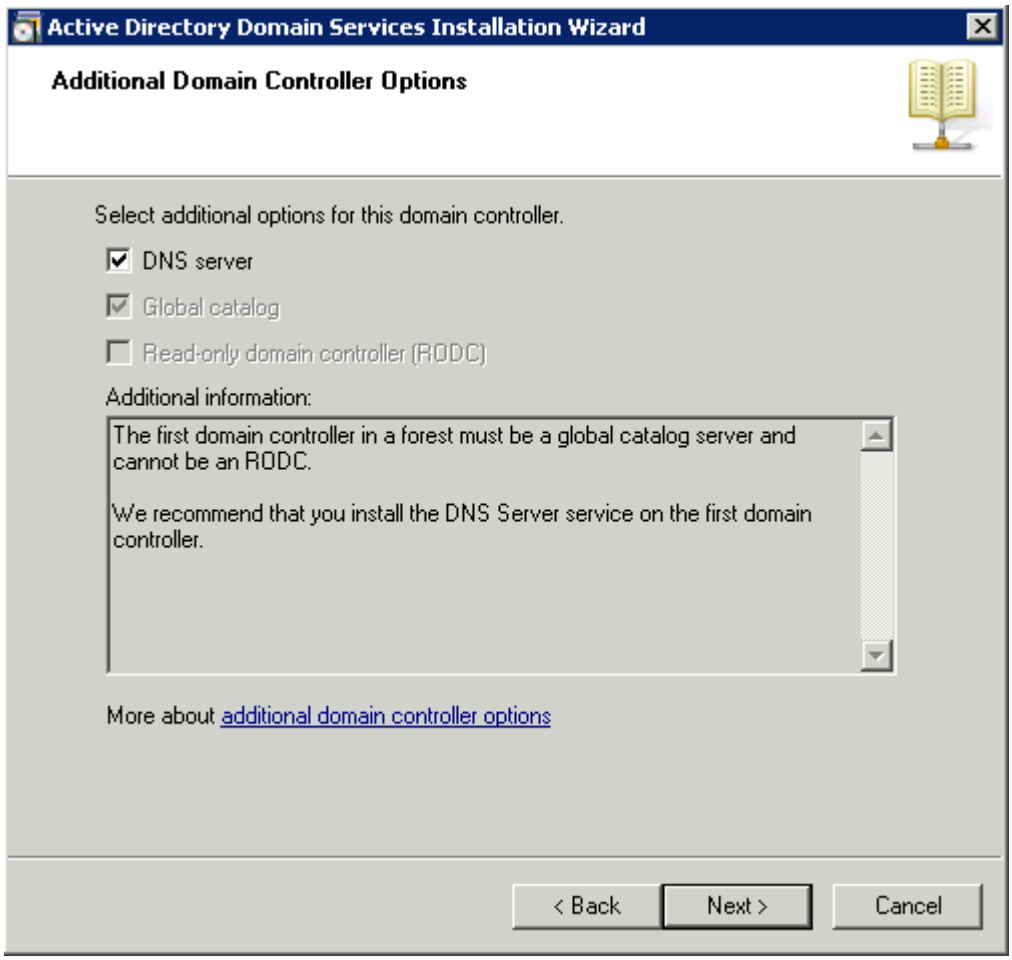
12. Selecteer het functionele niveau van het forest voor uw domein en klik op Volgende.



13. Selecteer het functionele domeinniveau voor uw domein en klik op Volgende.

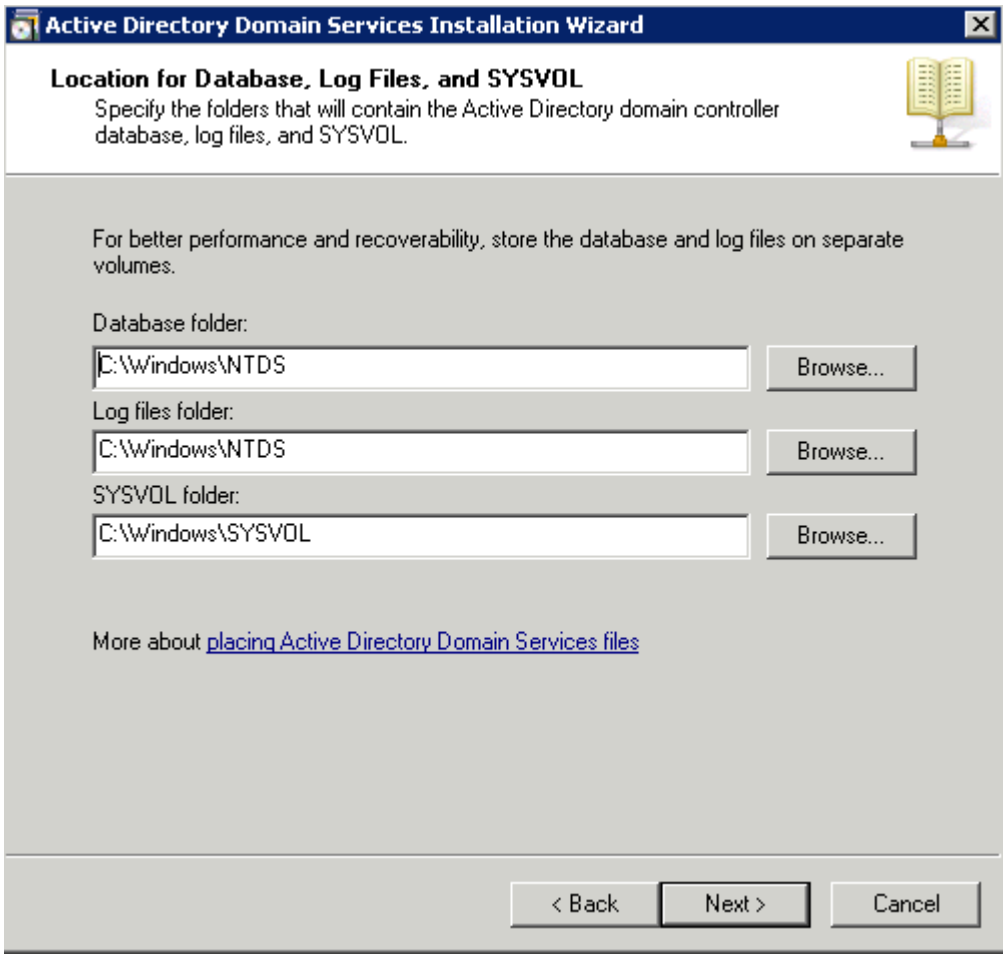


14. Controleer of DNS-server is geselecteerd en klik op Volgende.

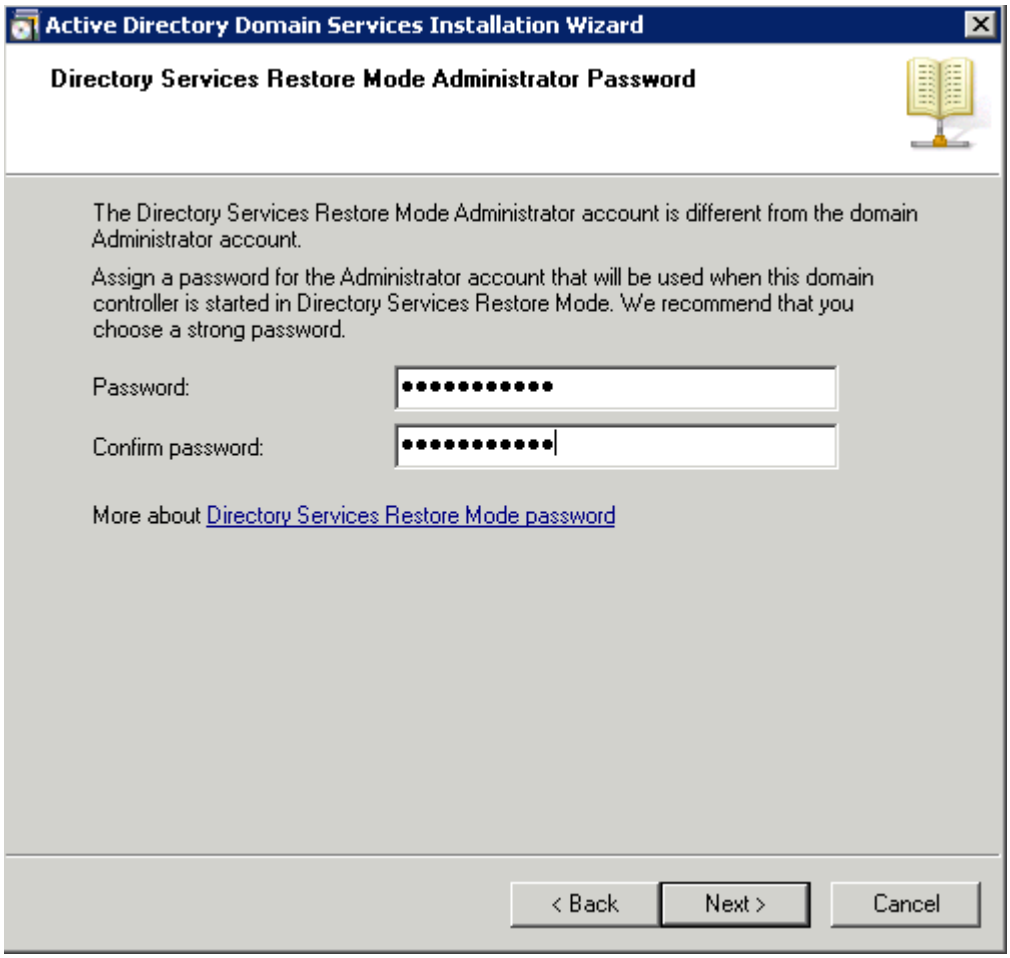


15. Klik op Ja voor de installatiewizard om een nieuwe zone in DNS voor het domein te maken.

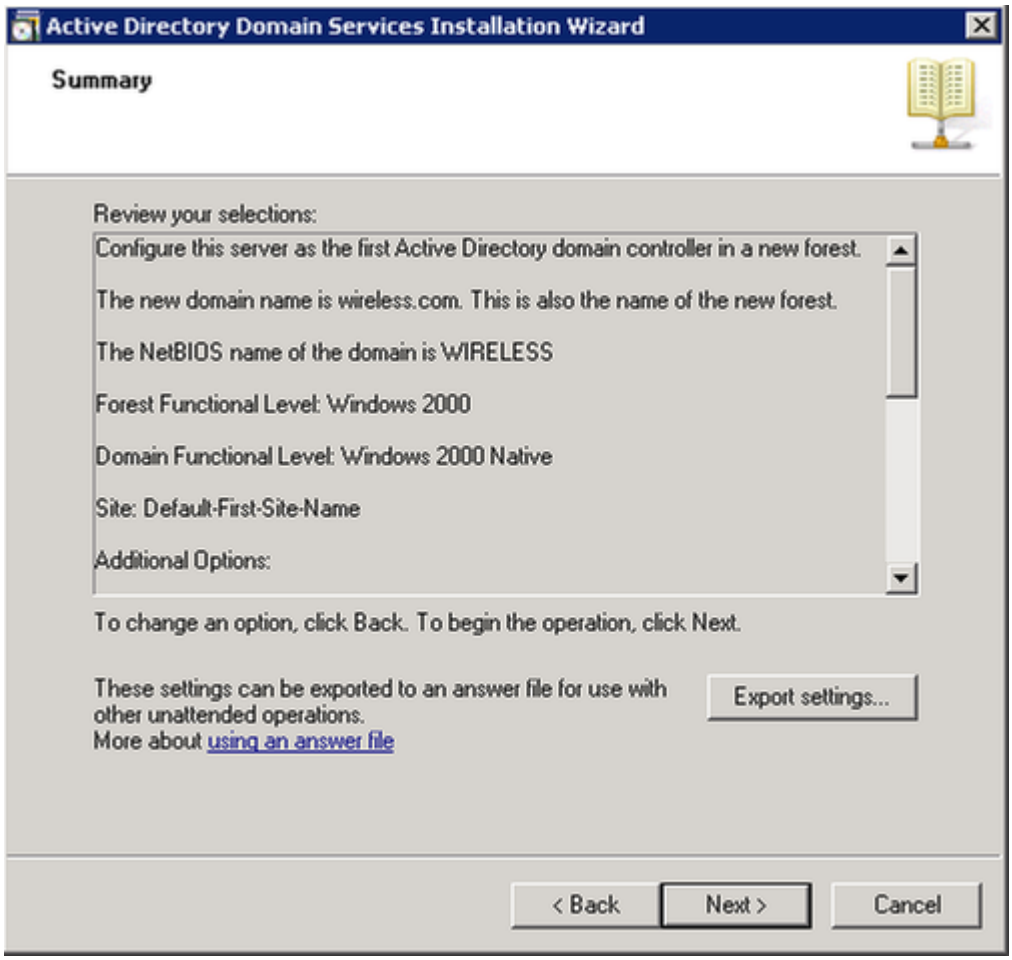
16. Selecteer de mappen die Active Directory voor de bestanden moet gebruiken en klik op Volgende.



17. Voer het beheerderswachtwoord in en klik op Volgende.

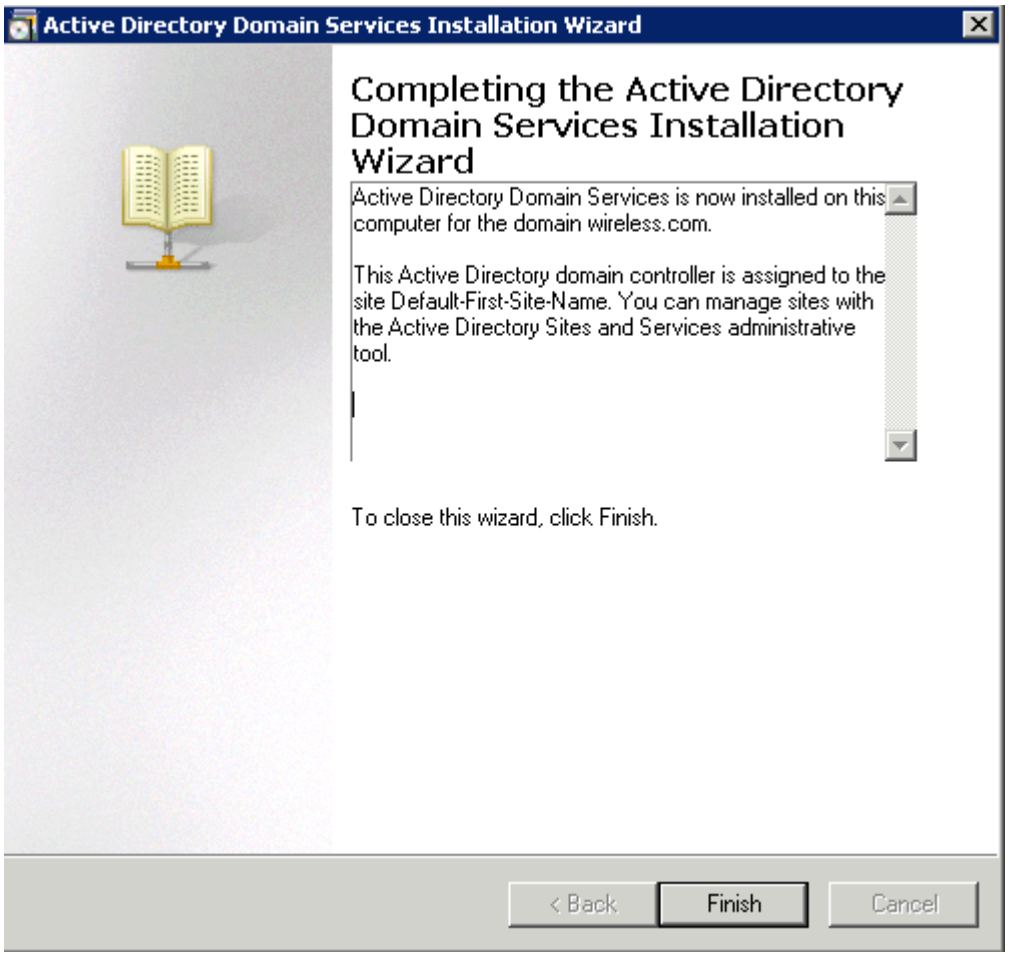


18. Controleer uw selecties en klik op Volgende.

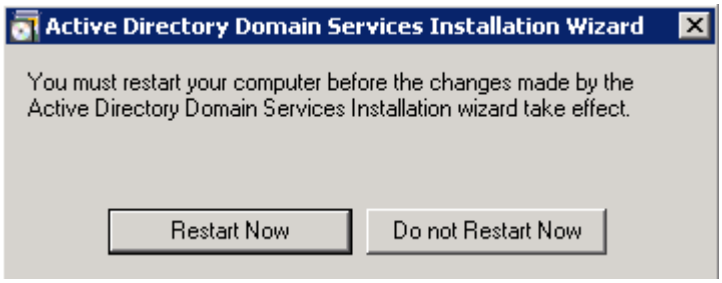


De installatie gaat door.

19. Klik op Voltooien om de wizard te sluiten.



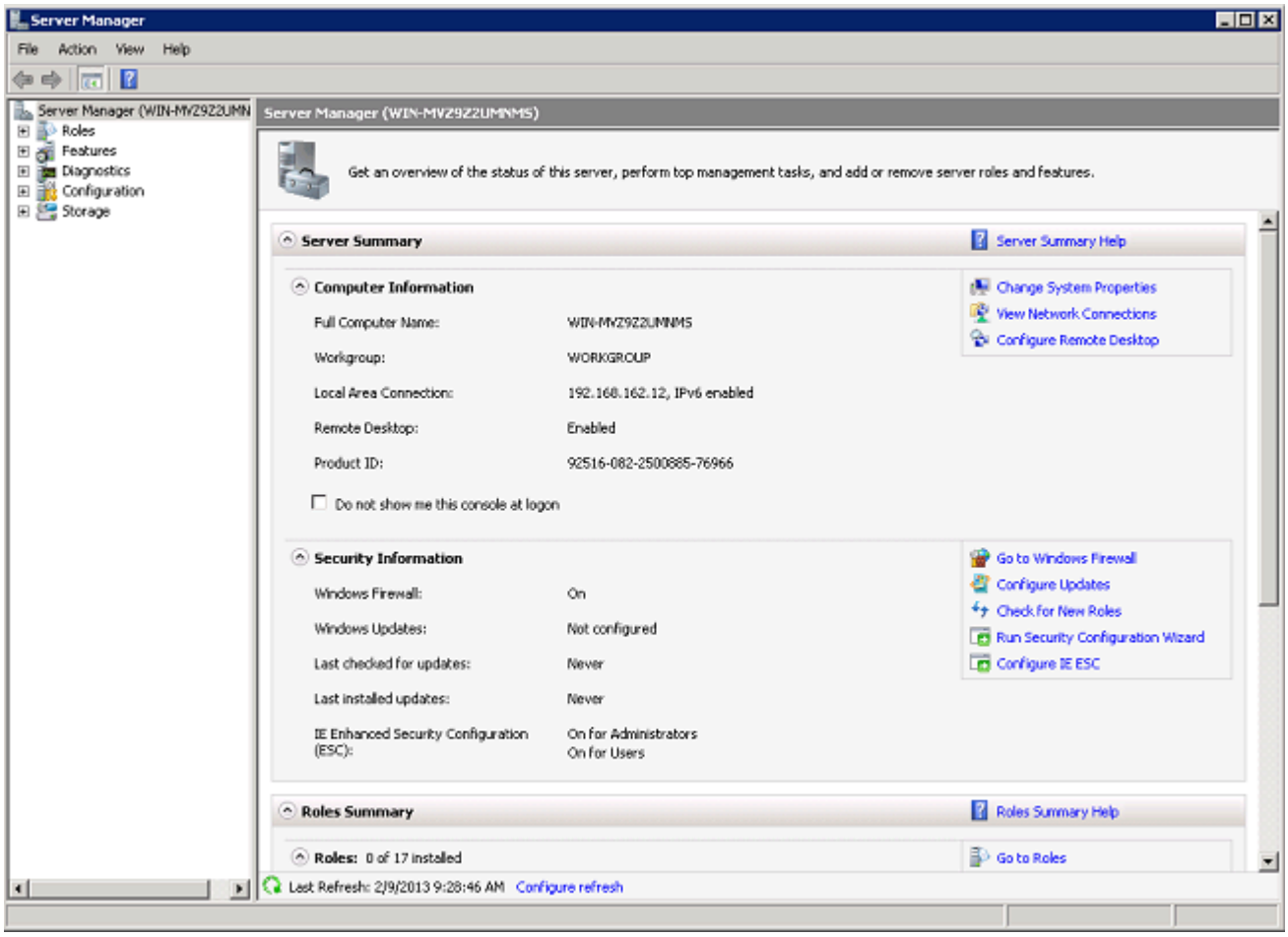
20. Start de server opnieuw op zodat de wijzigingen van kracht worden.



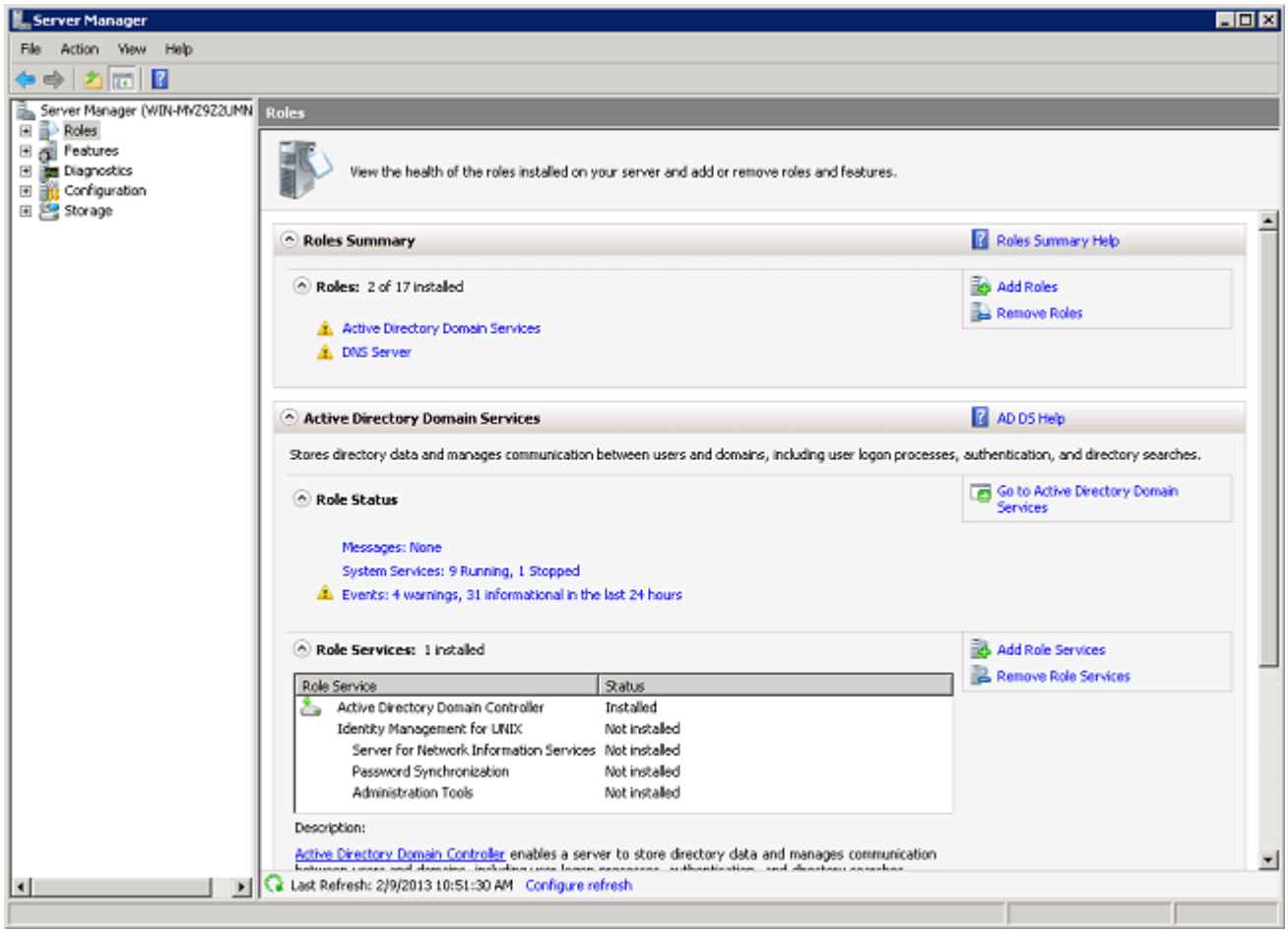
DHCP-services installeren en configureren op de Microsoft Windows 2008-server

De DHCP-service op de Microsoft 2008-server wordt gebruikt om IP-adressen te verstrekken aan de draadloze clients. Voer de volgende stappen uit om DHCP-services te installeren en configureren:

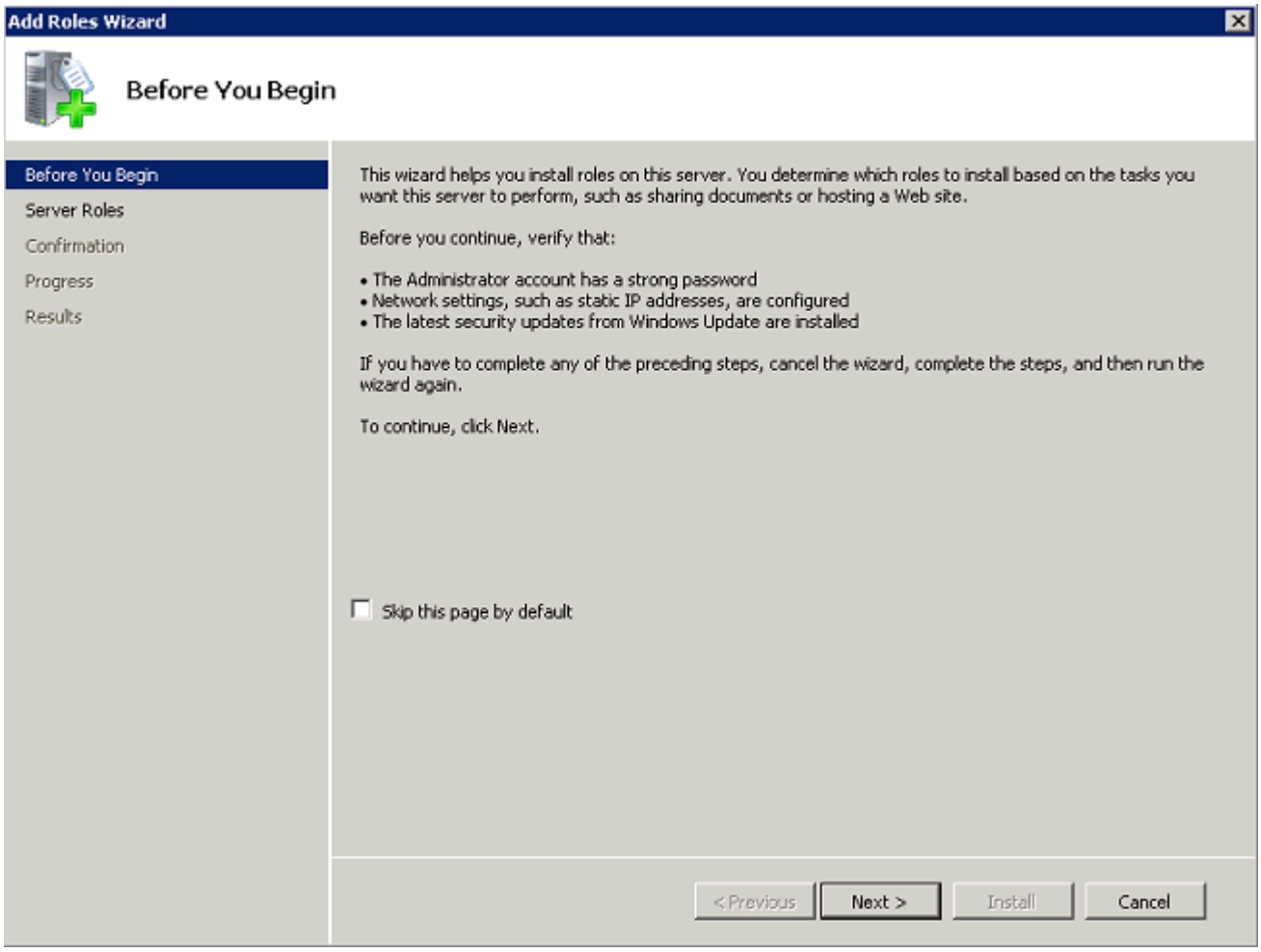
1. Klik op Start>Serverbeheer.



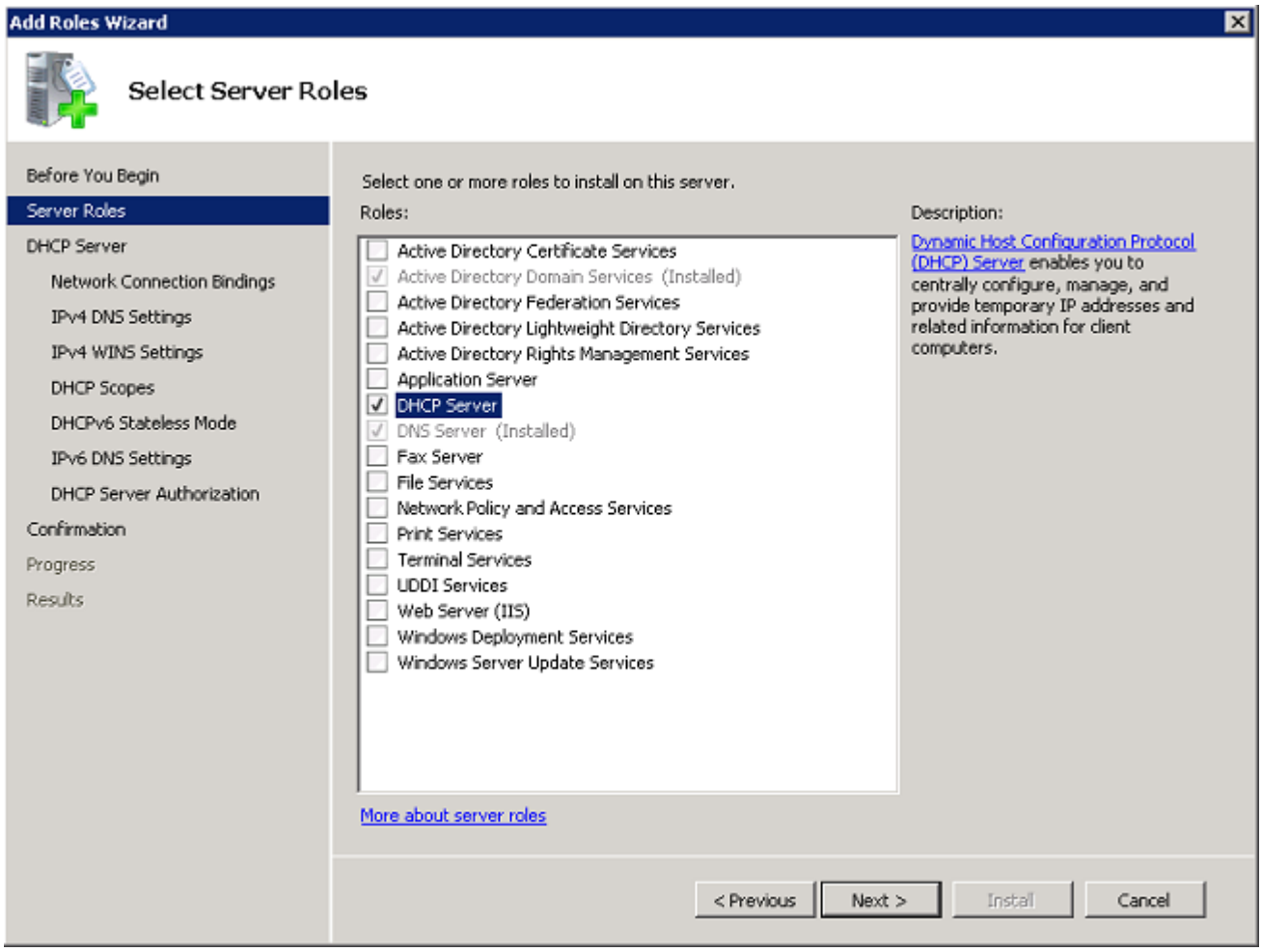
2. Klik op Rollen> Rollen toevoegen.



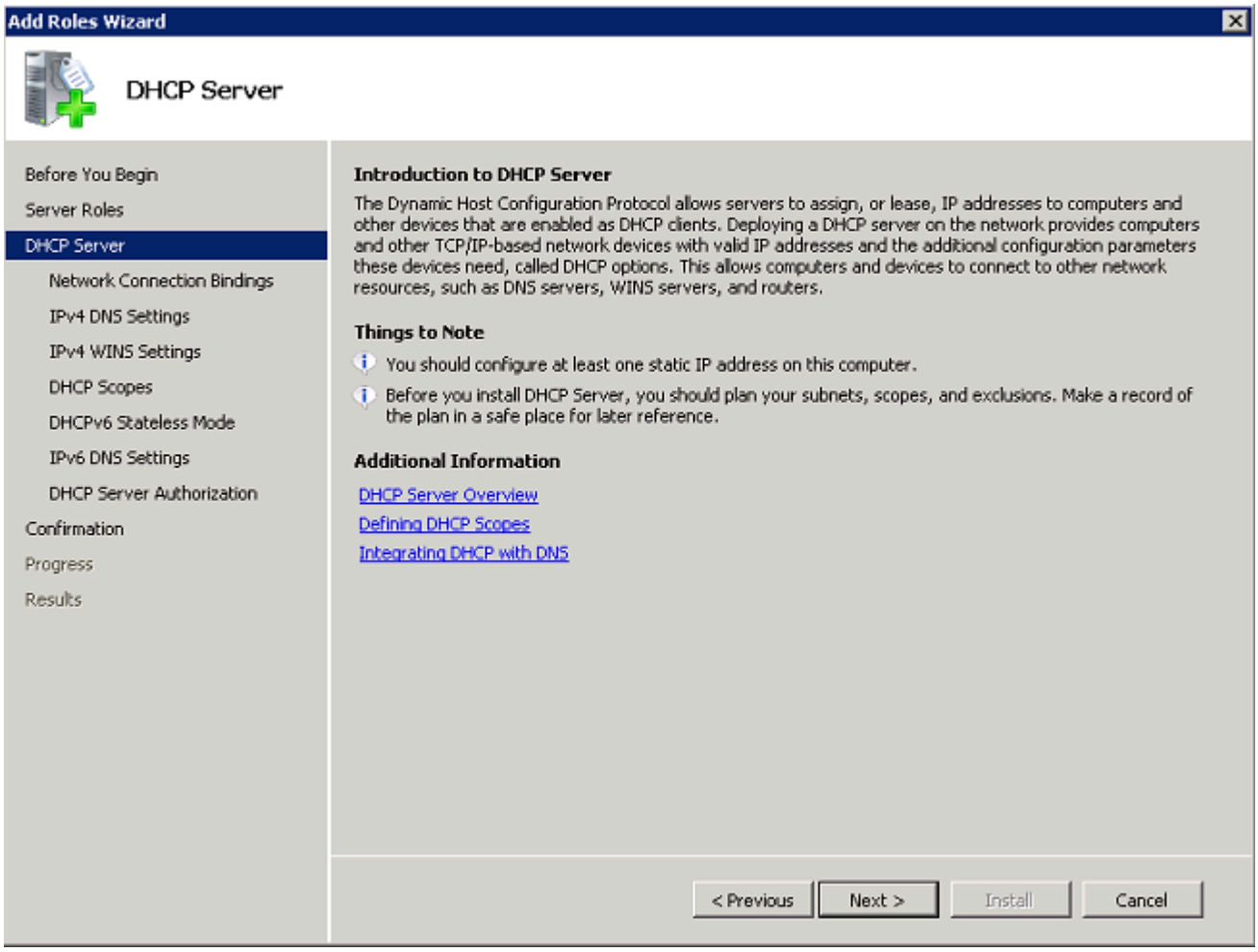
3. Klik op Next (Volgende).



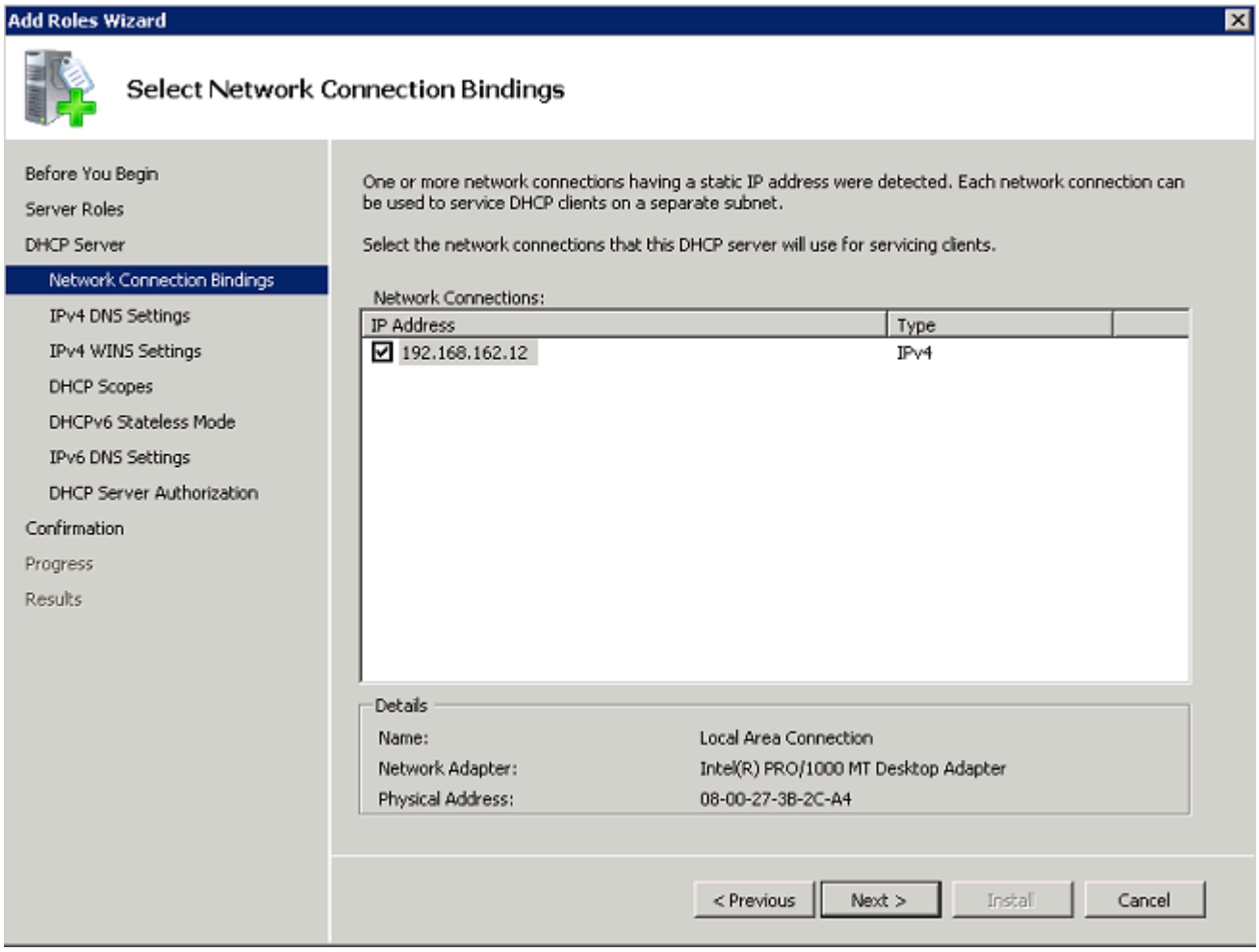
4. Selecteer de service DHCP Server en klik op Volgende.



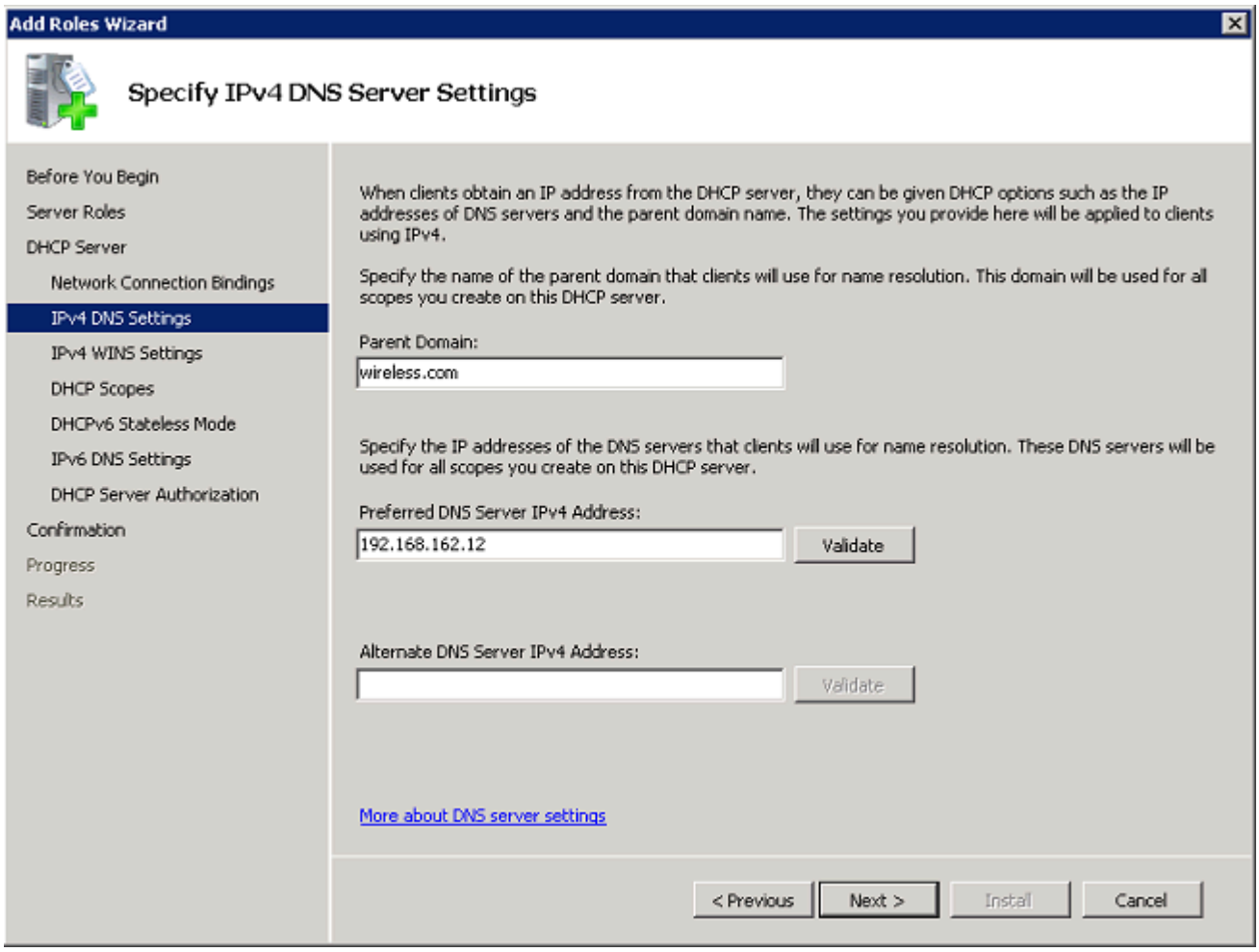
5. Controleer de introductie van DHCP Server en klik op Volgende.



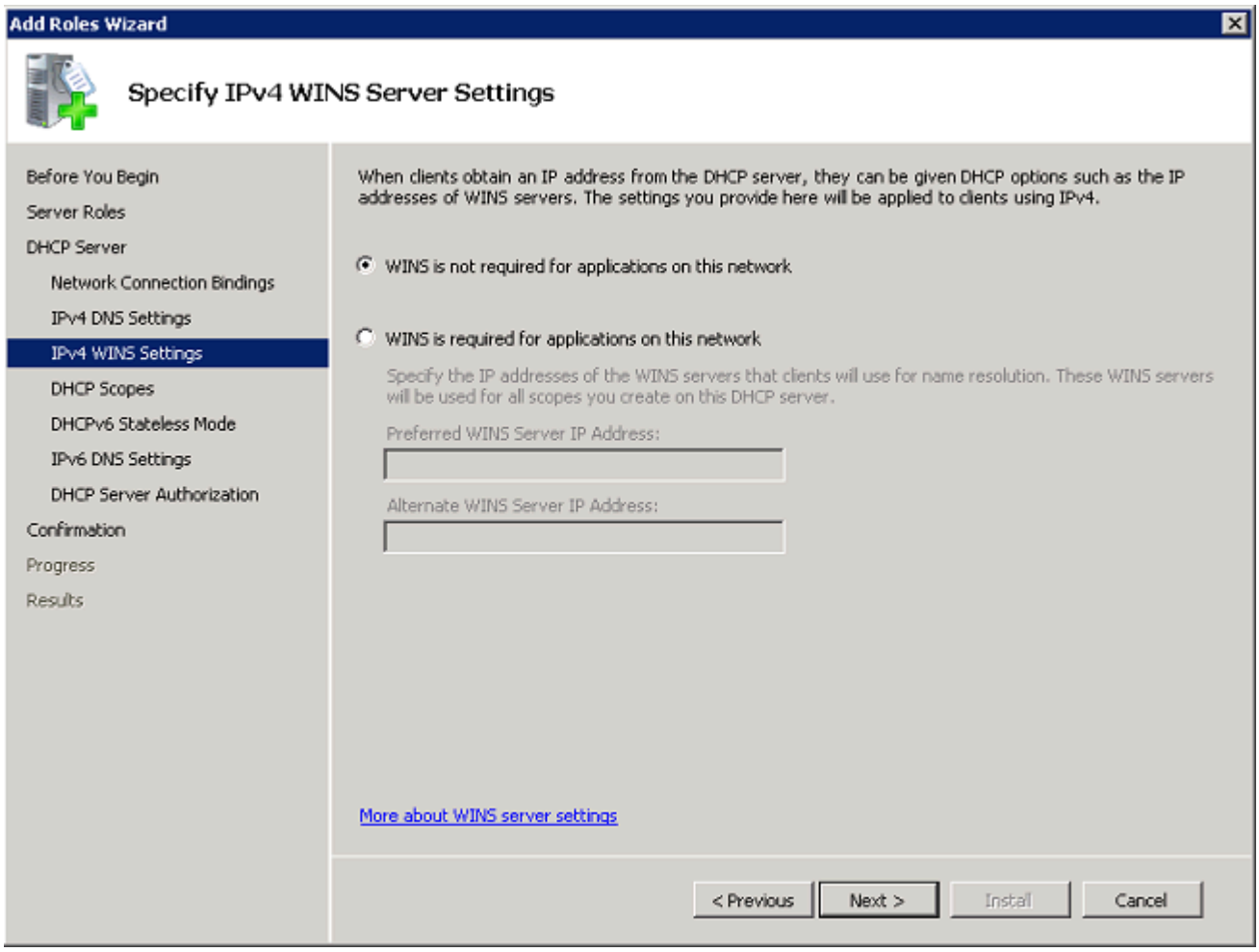
6. Selecteer de interface die de DHCP-server moet controleren op verzoeken en klik op Volgende.



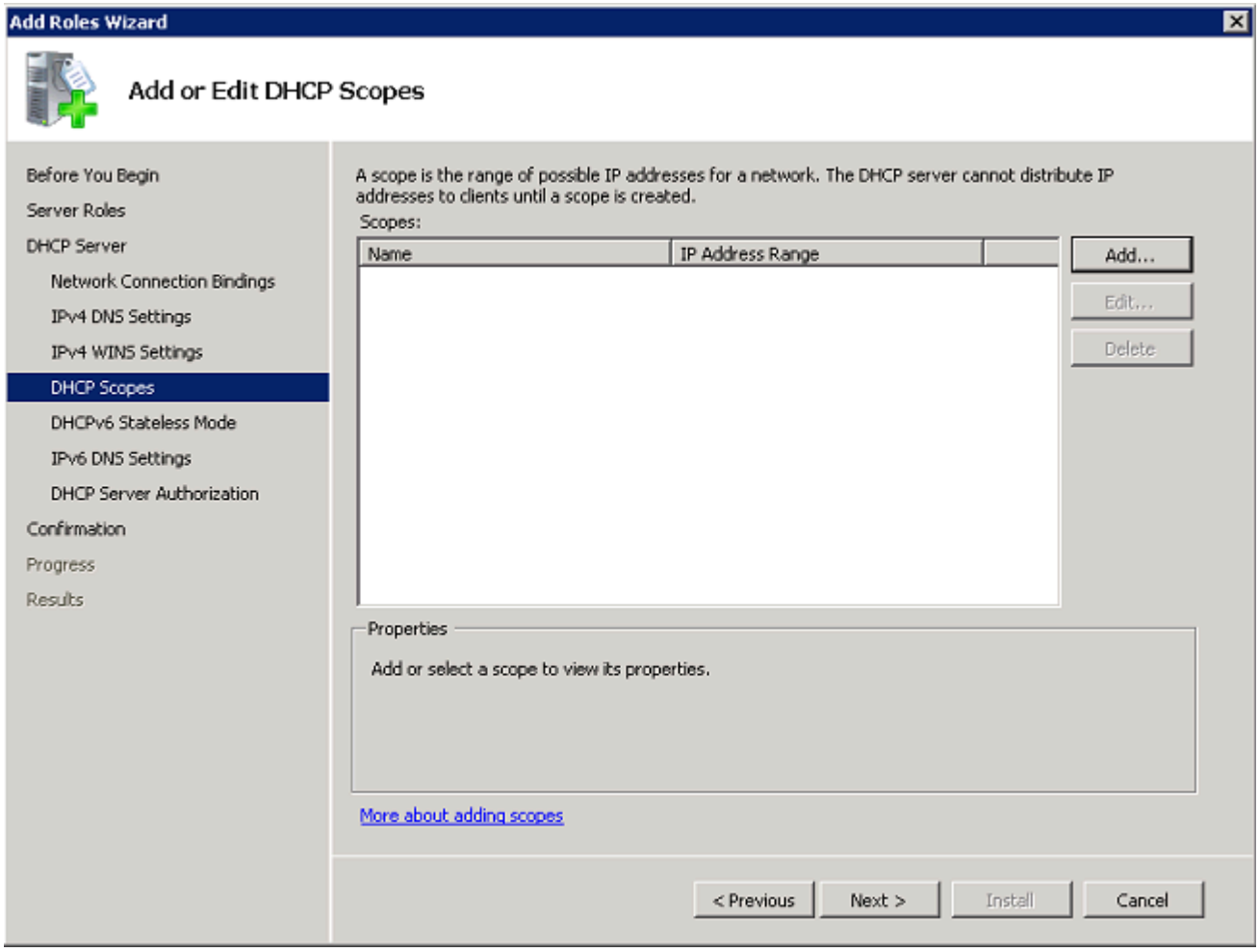
7. Configureer de standaard DNS-instellingen die de DHCP-server moet opgeven voor clients en klik op Volgende.



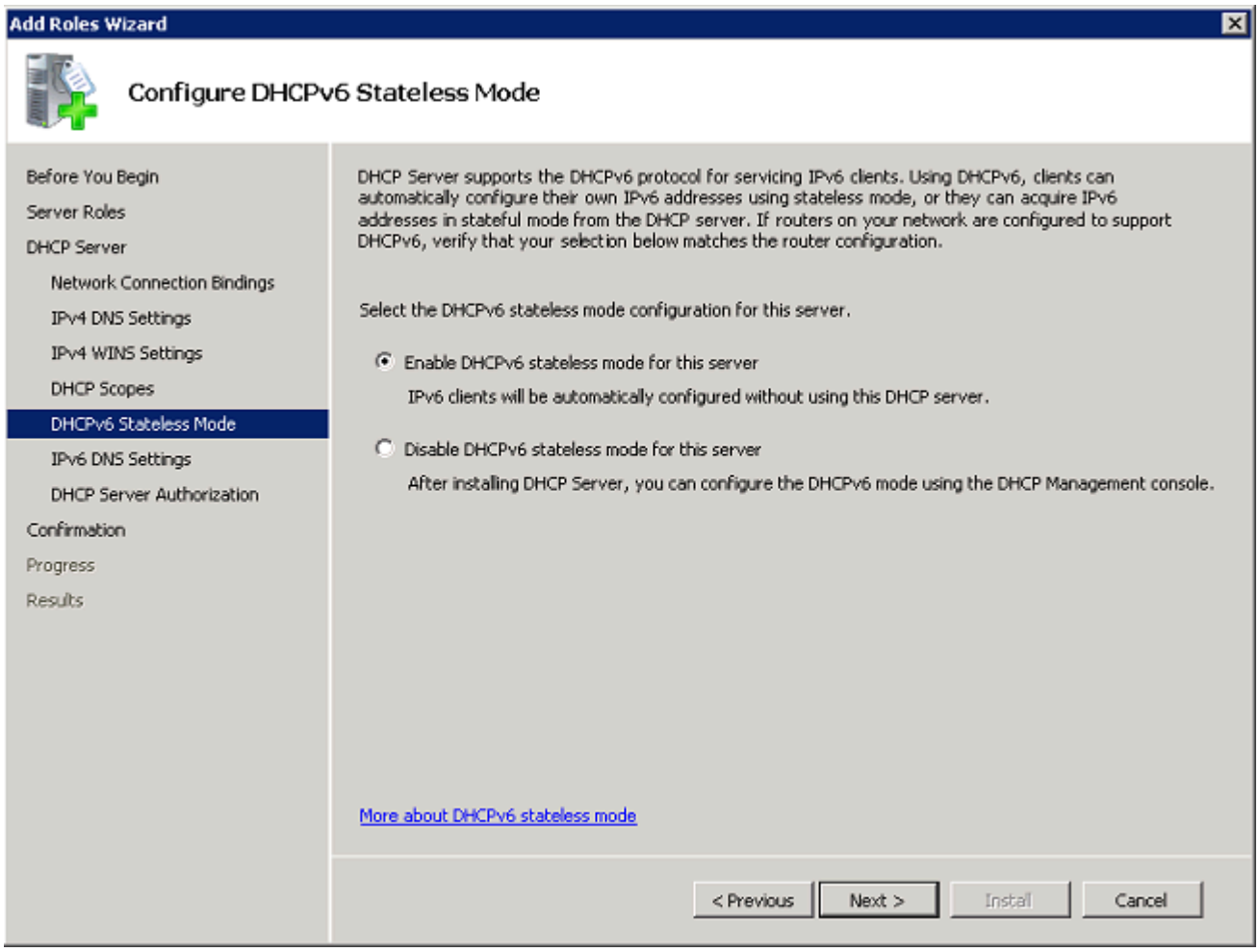
8. Configureren van WINS als het netwerk WINS ondersteunt.



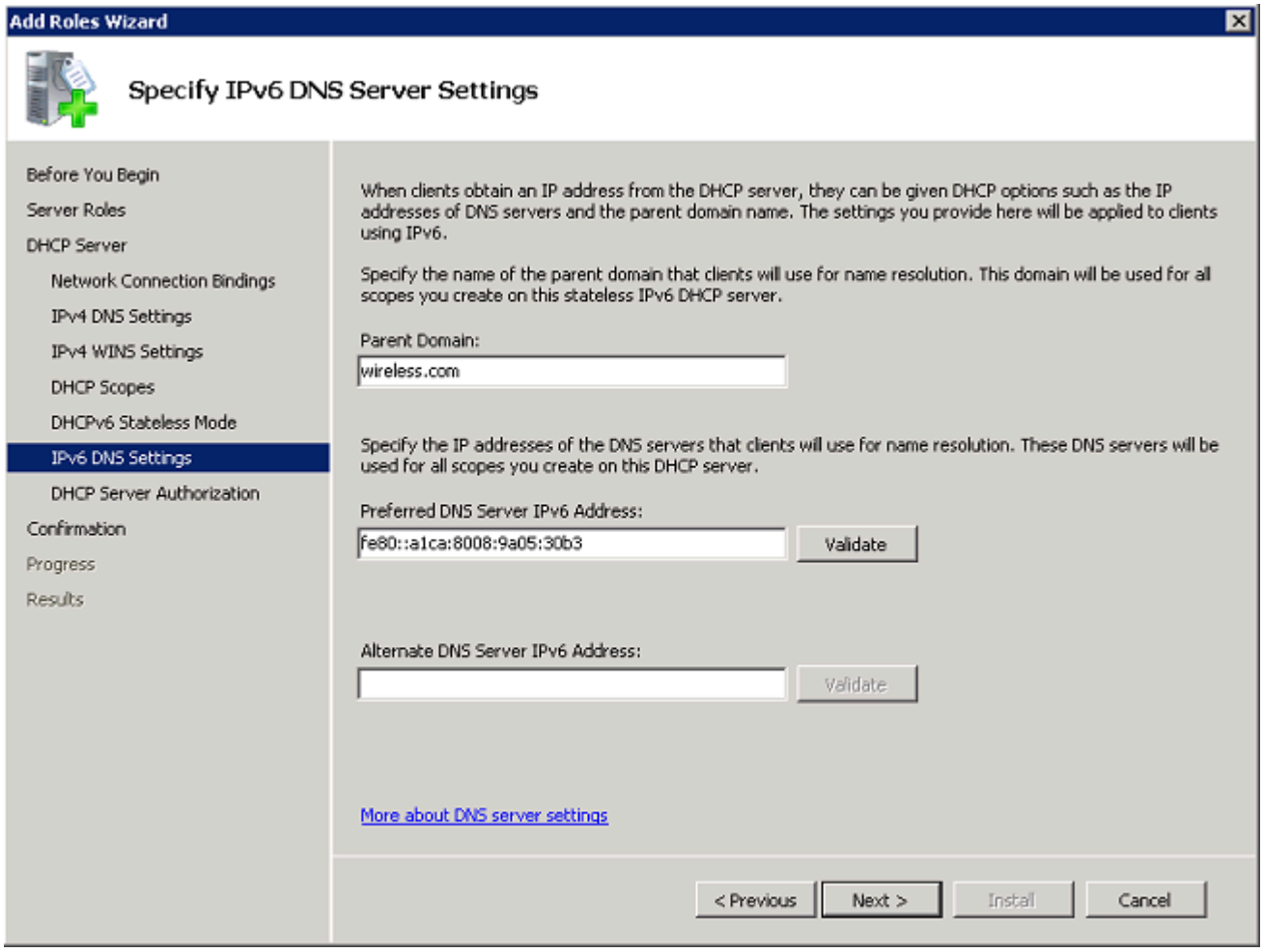
9. Klik op Toevoegen om de wizard te gebruiken om een DHCP-bereik te maken of klik op Volgende om later een DHCP-bereik te maken. Klik op Volgende om door te gaan.



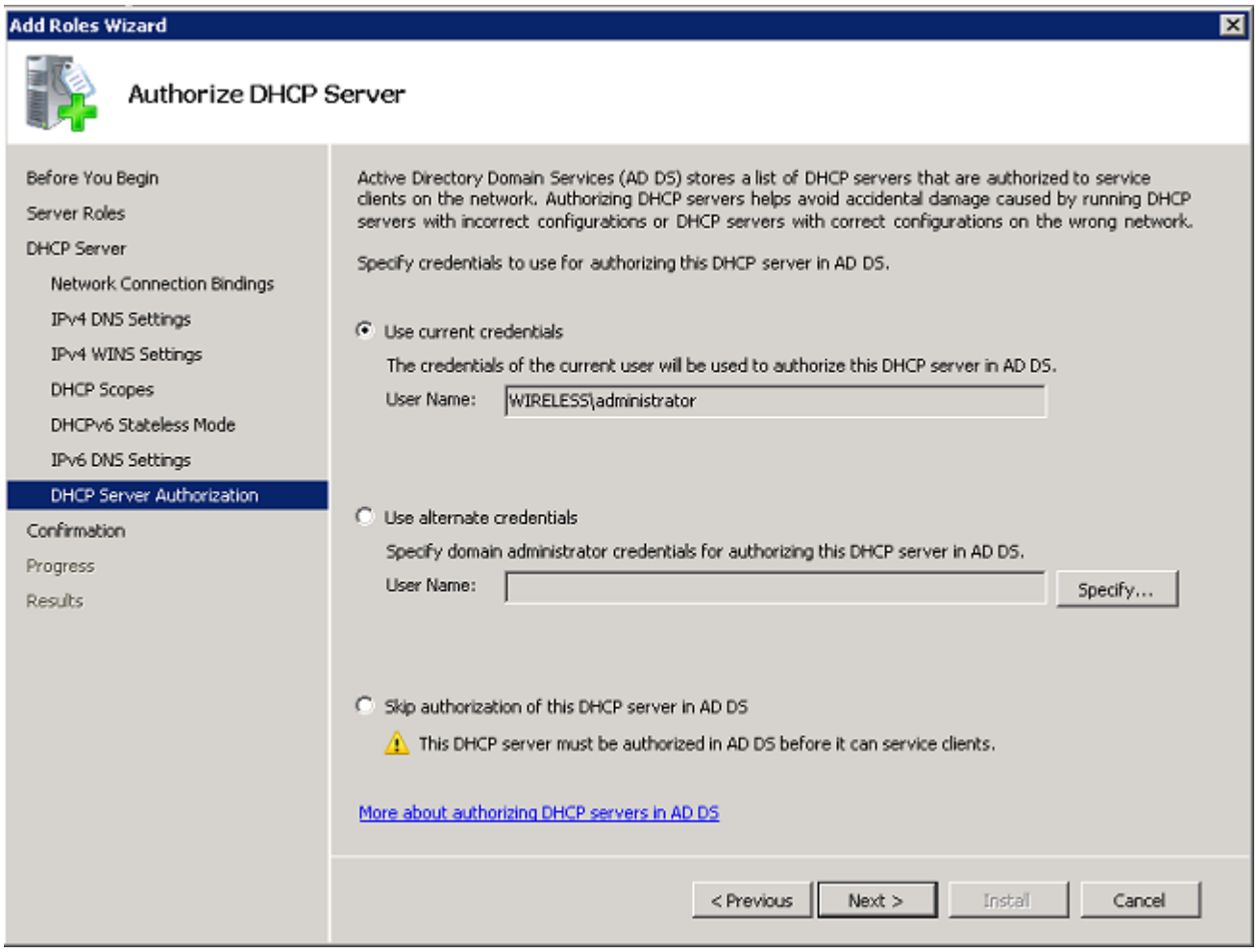
10. Schakel de DHCPv6-ondersteuning op de server in of uit en klik op Volgende.



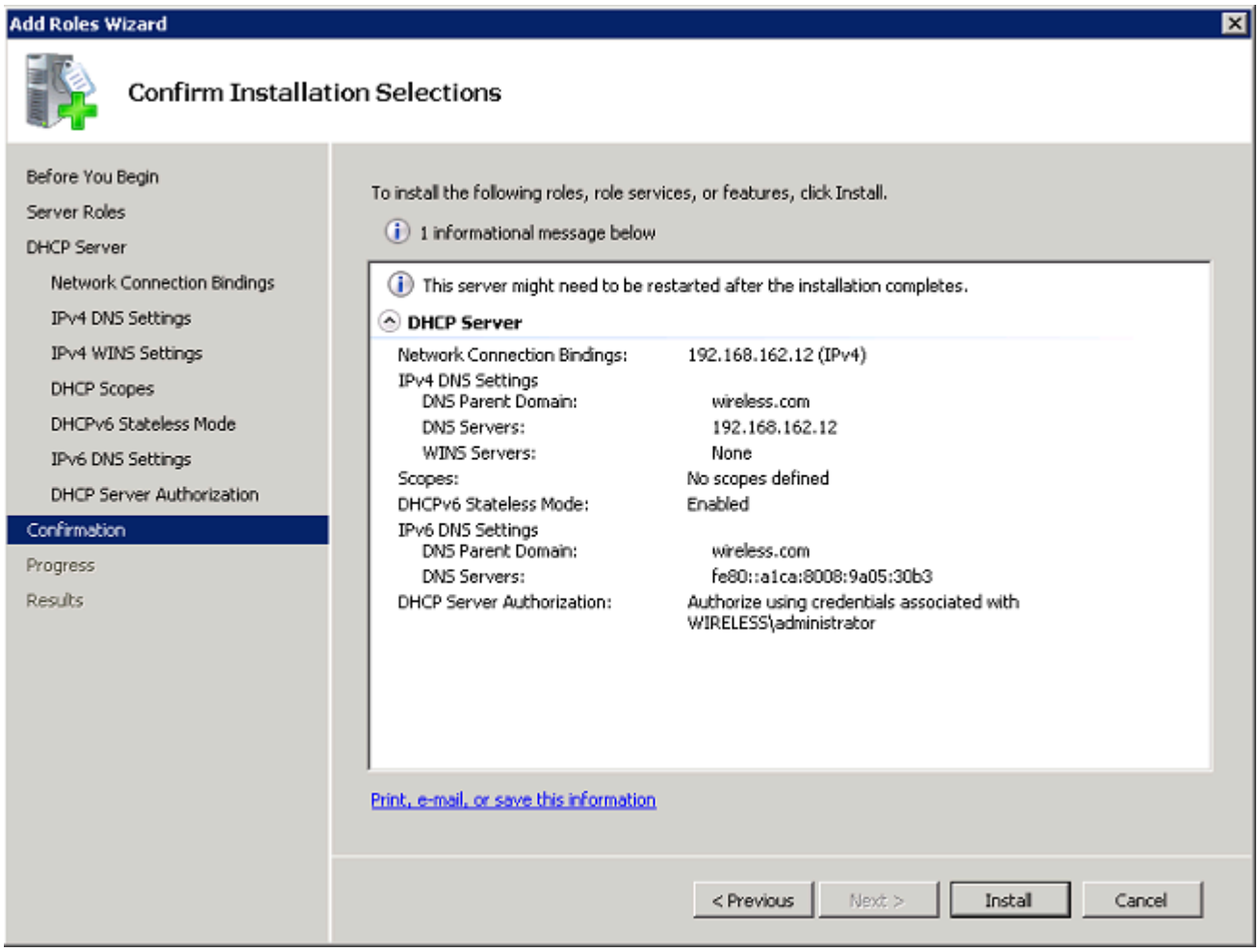
11. Configureer de IPv6 DNS-instellingen als DHCPv6 in de voorgaande stap is ingeschakeld. Klik op Volgende om door te gaan.



12. Geef de referenties van de domeinbeheerder op om de DHCP-server in Active Directory te autoriseren en klik op Volgende.

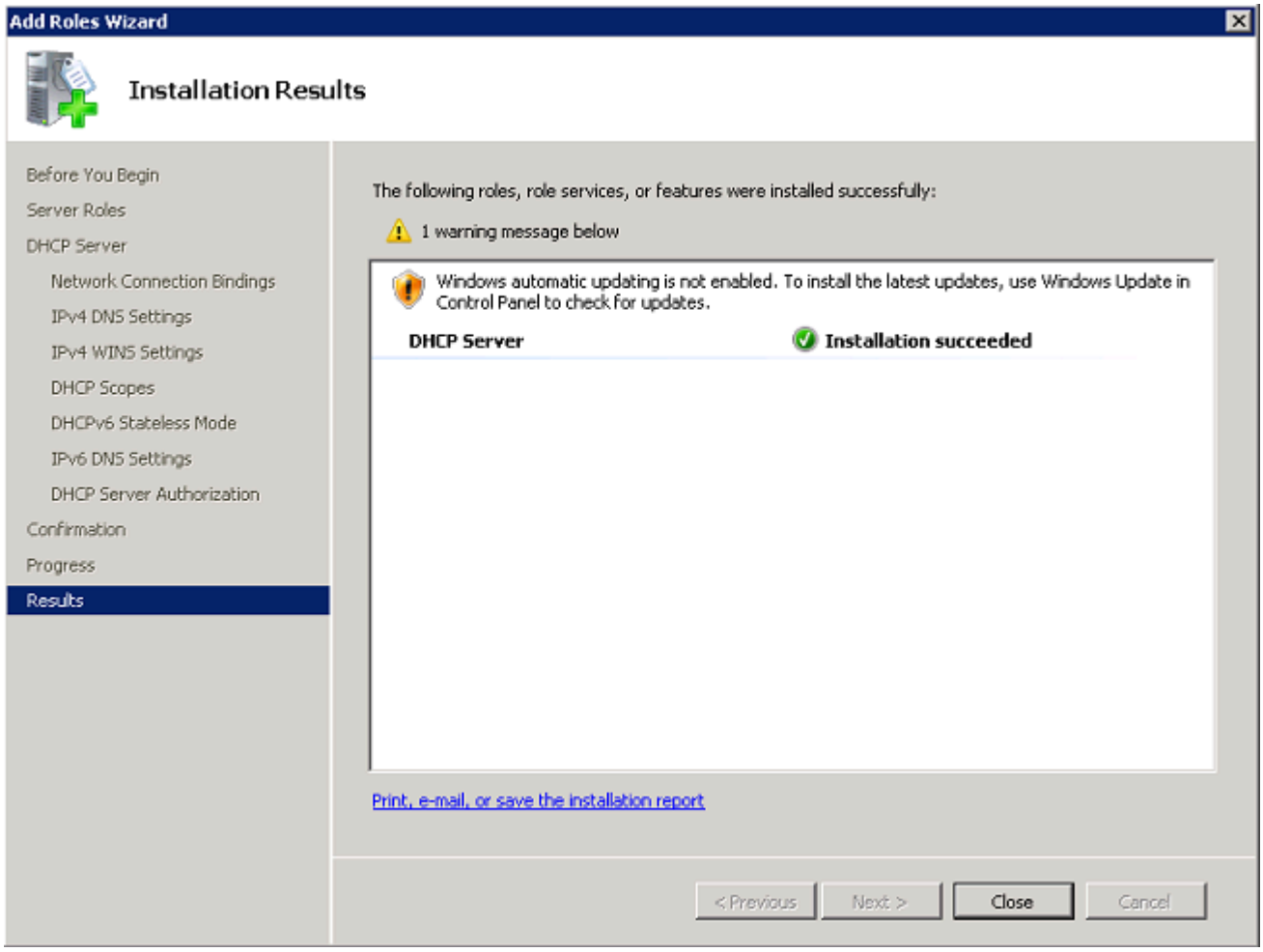


13. Controleer de configuratie op de bevestigingspagina en klik op Installeren om de installatie te voltooien.



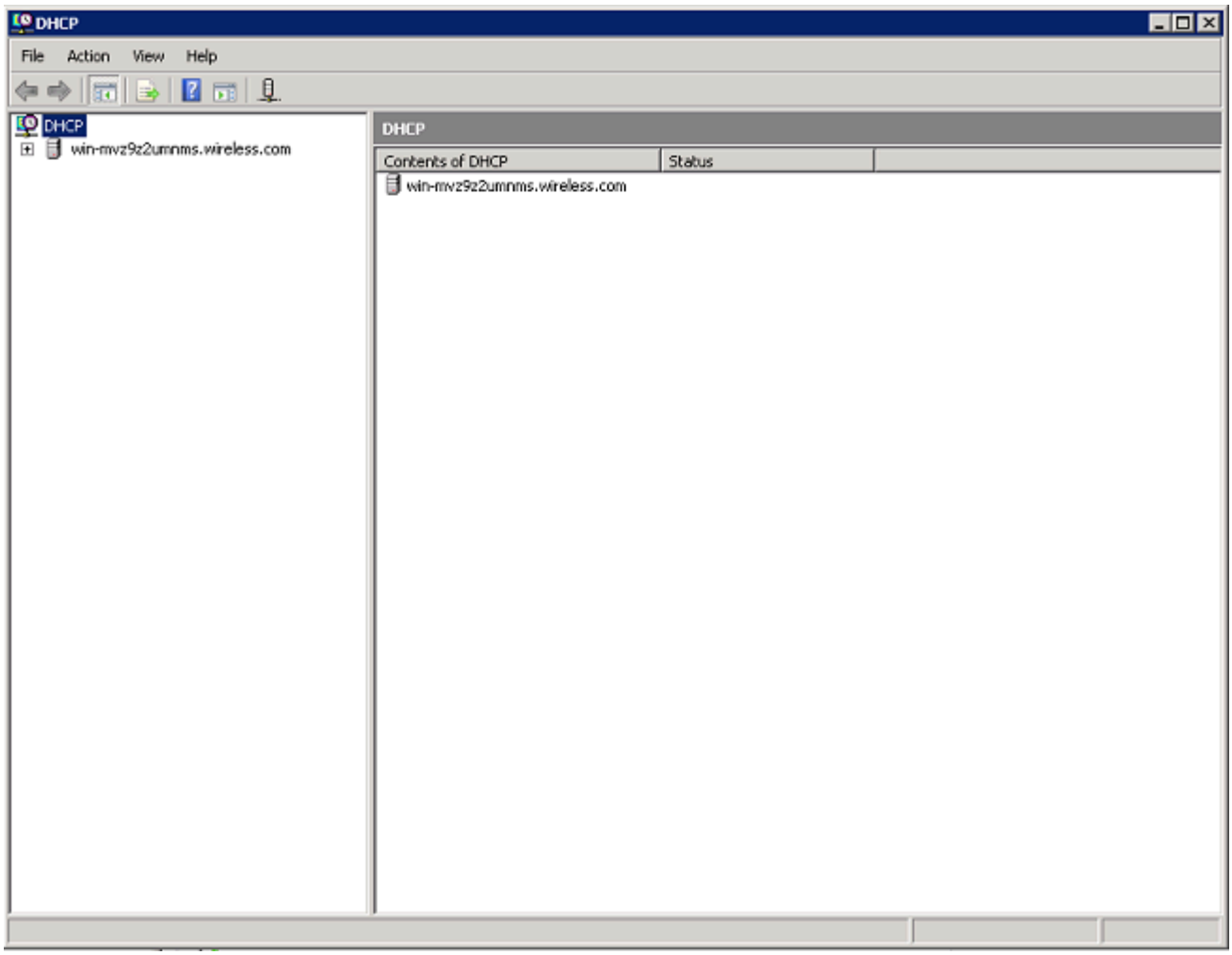
De installatie gaat door.

14. Klik op Sluiten om de wizard te sluiten.

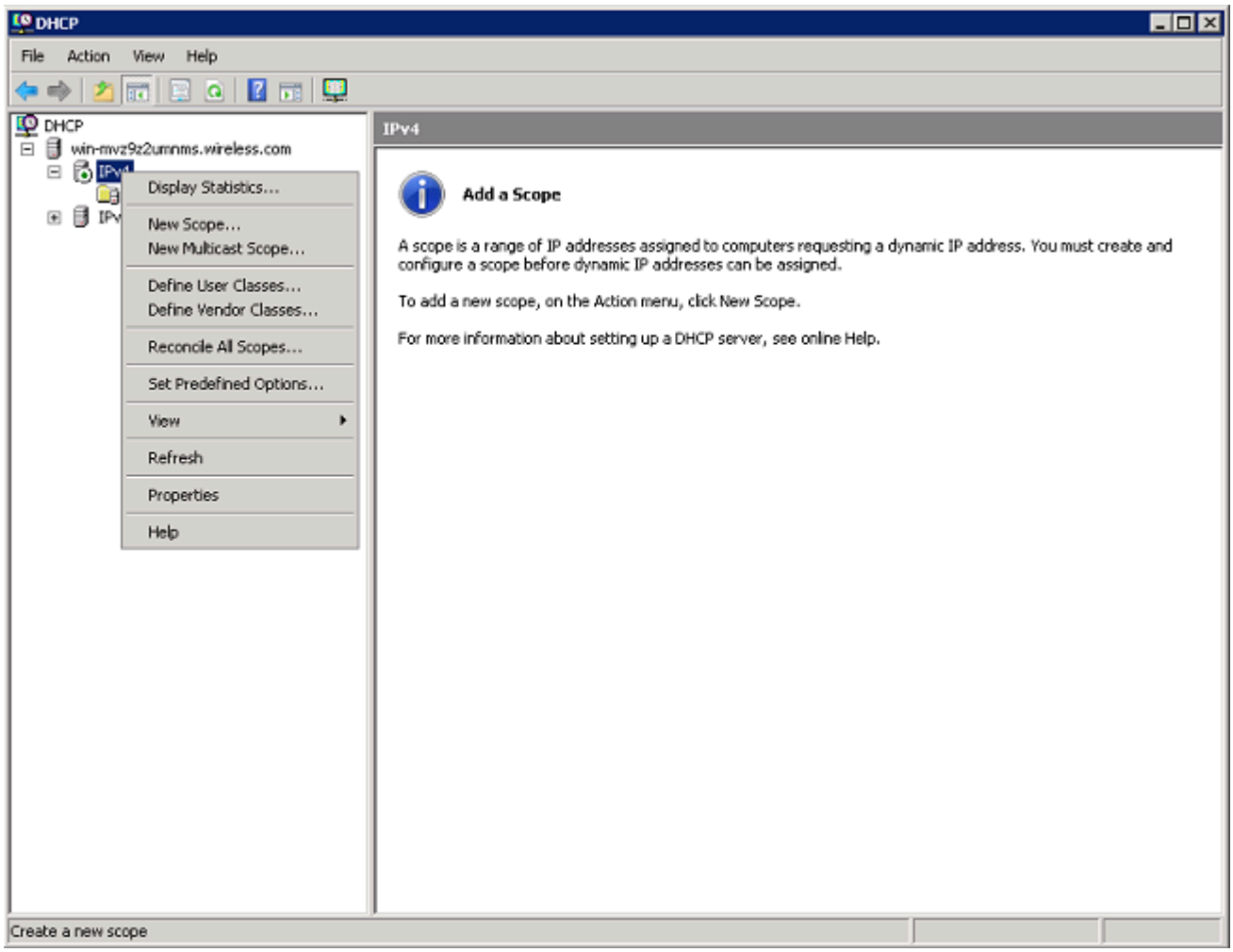


De DHCP-server is nu geïnstalleerd.

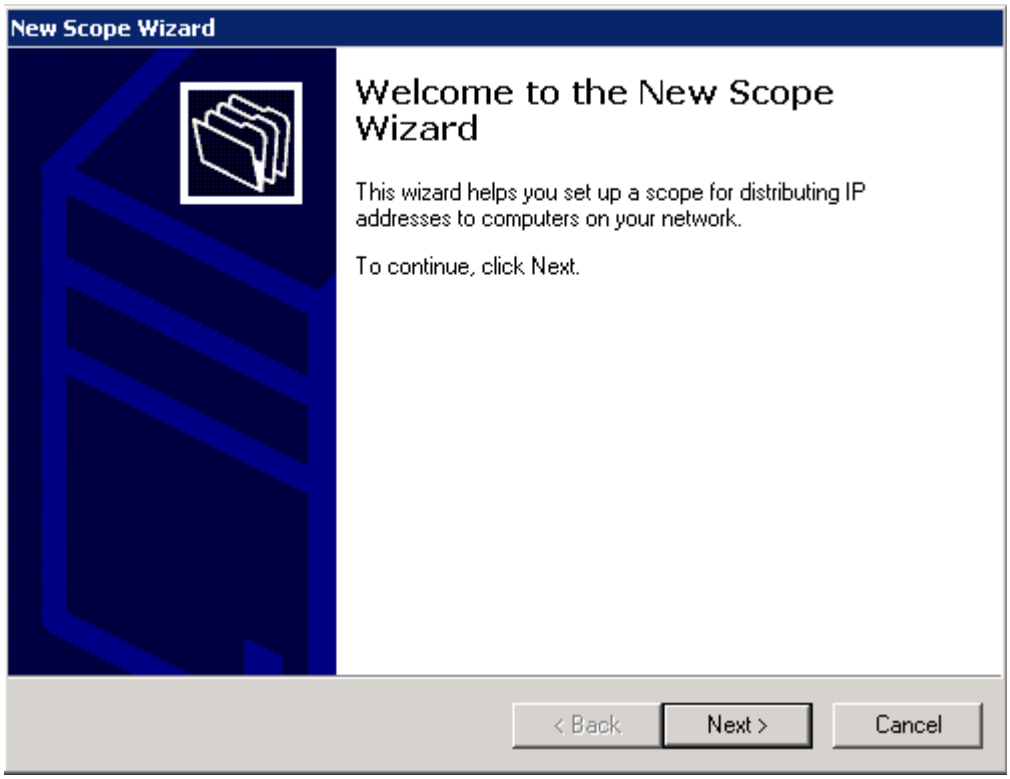
15. Klik op Start > Systeembeheer > DHCP om de DHCP-service te configureren.



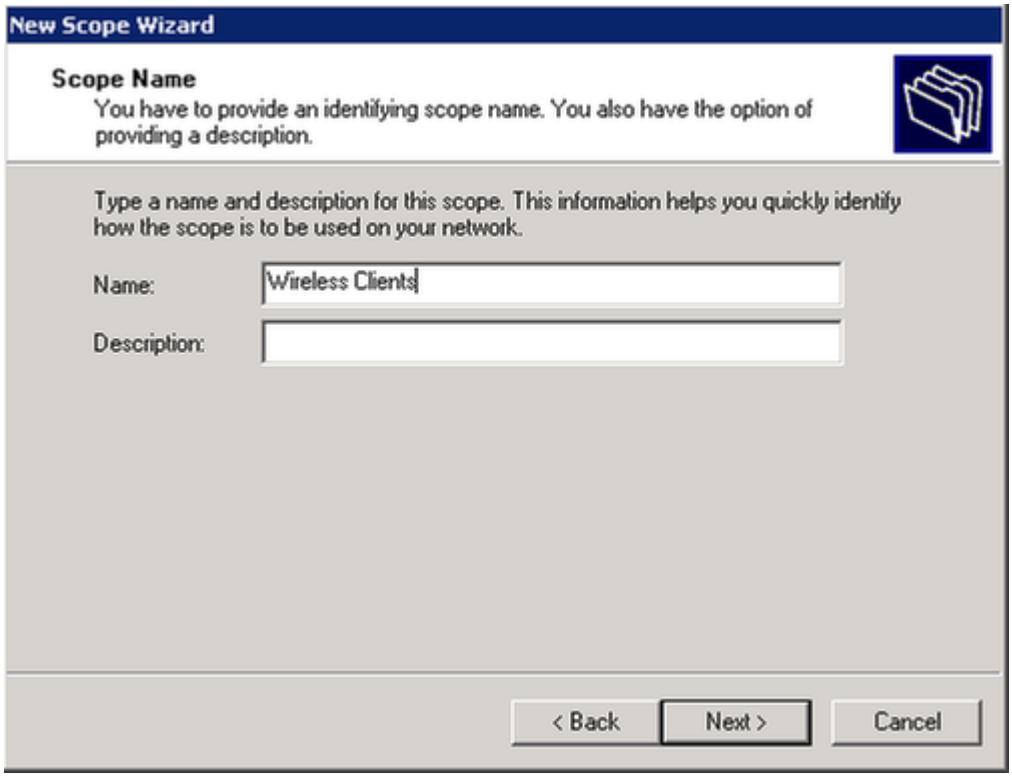
16. Vouw de DHCP-server uit (in de vorige afbeelding voor dit voorbeeld), klik met de rechtermuisknop op IPv4 en kies Nieuw bereik om een DHCP-bereik te maken.



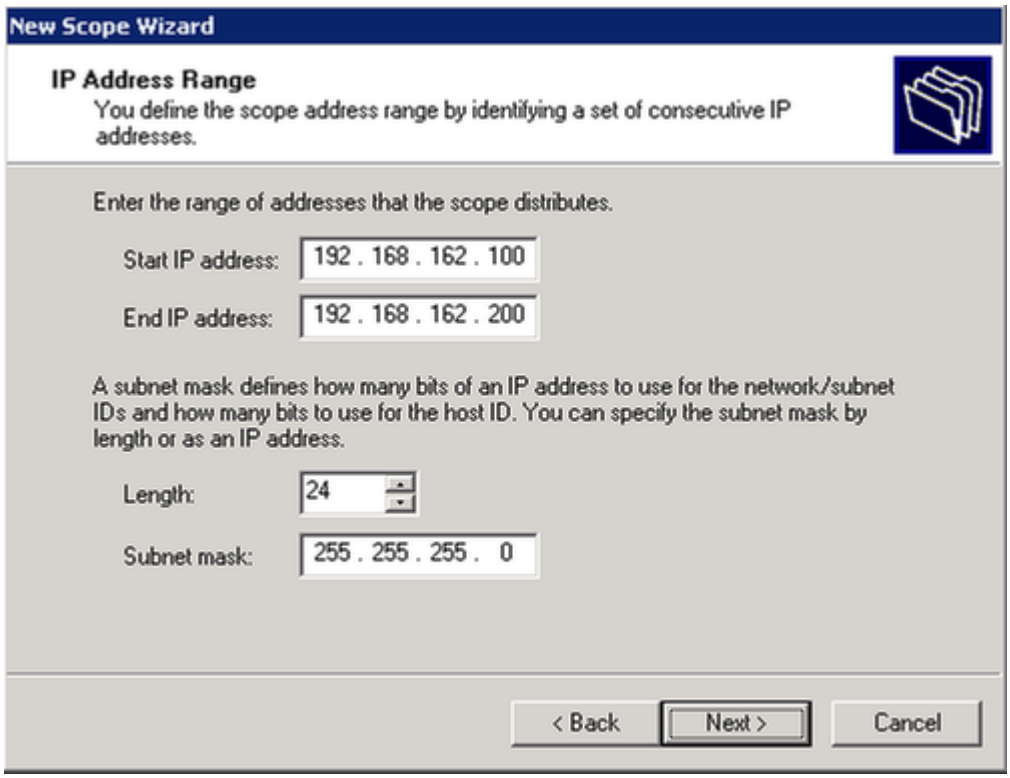
17. Klik op Volgende om het nieuwe bereik te configureren met de wizard Nieuwe reikwijdte.



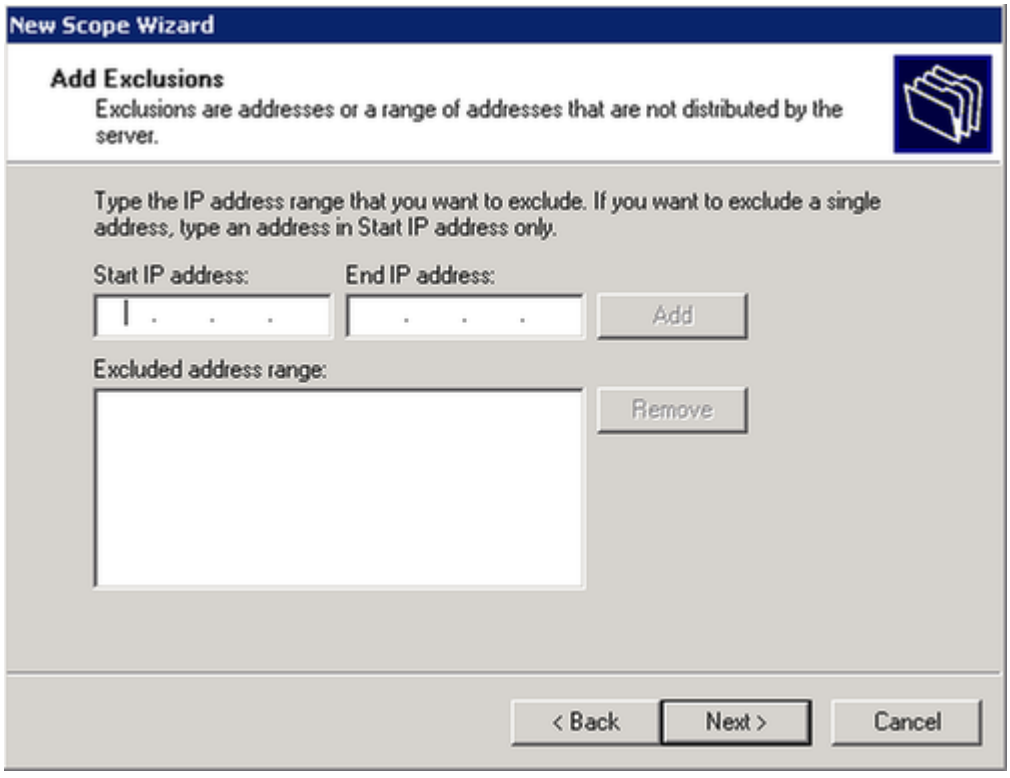
18. Geef een naam op voor het nieuwe bereik (Wireless Clients in dit voorbeeld) en klik op Volgende.



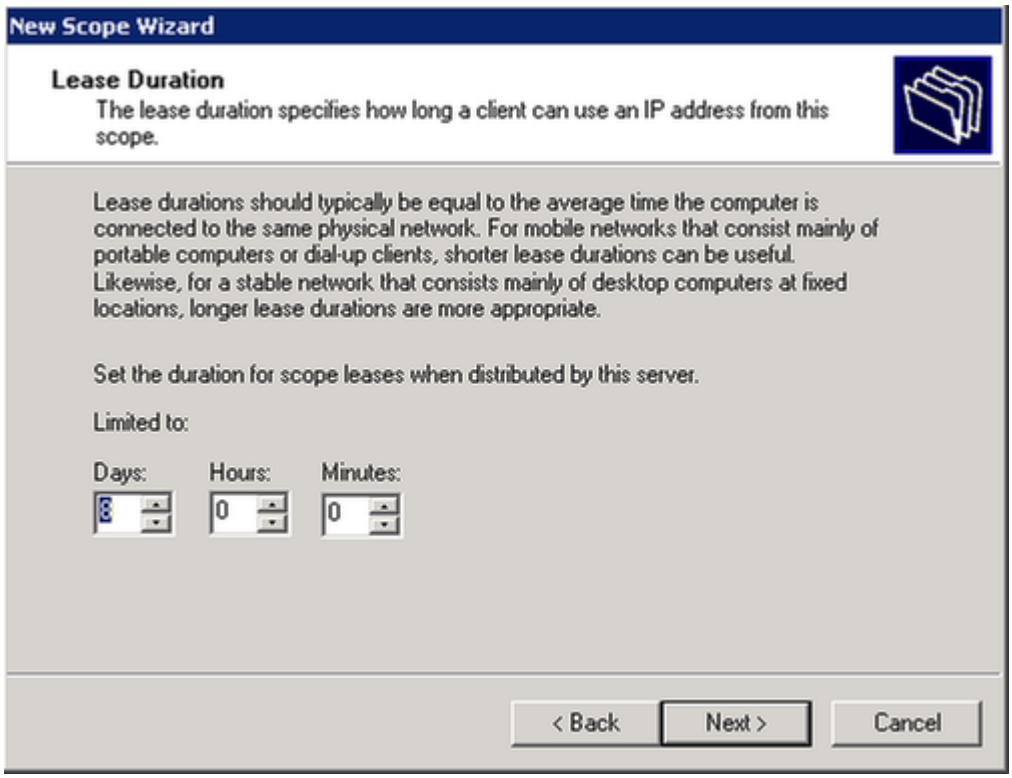
19. Geef het bereik op van beschikbare IP-adressen die kunnen worden gebruikt voor DHCP-leases. Klik op Volgende om door te gaan.



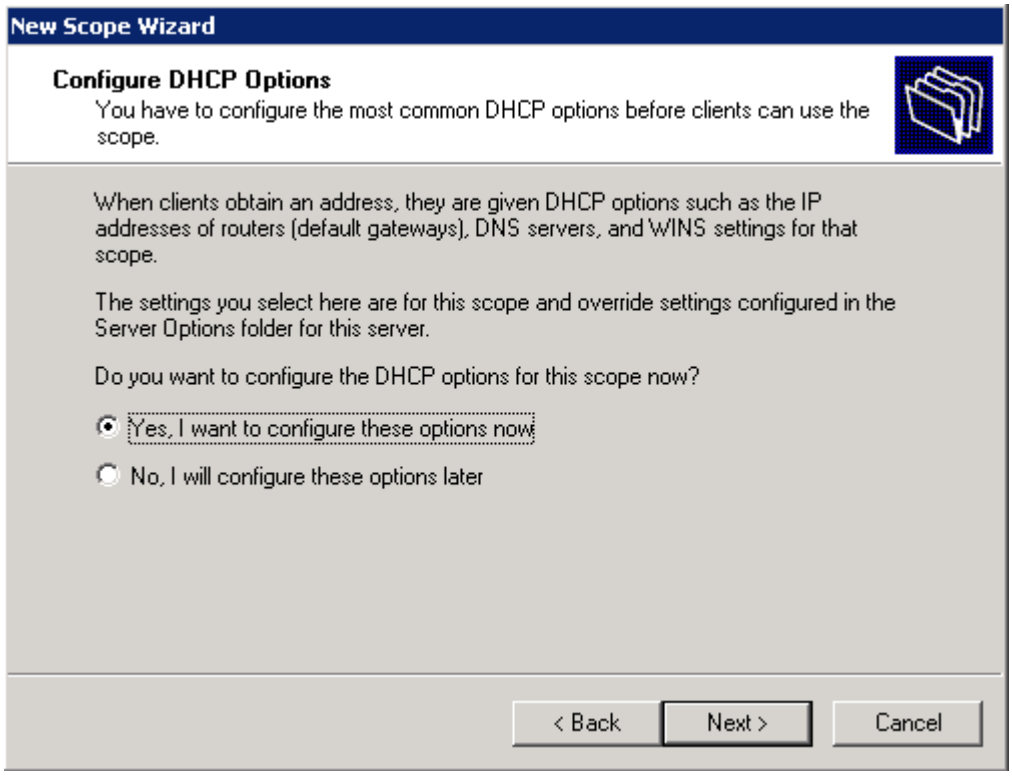
20. Maak een optionele lijst met uitgesloten adressen. Klik op Volgende om door te gaan.



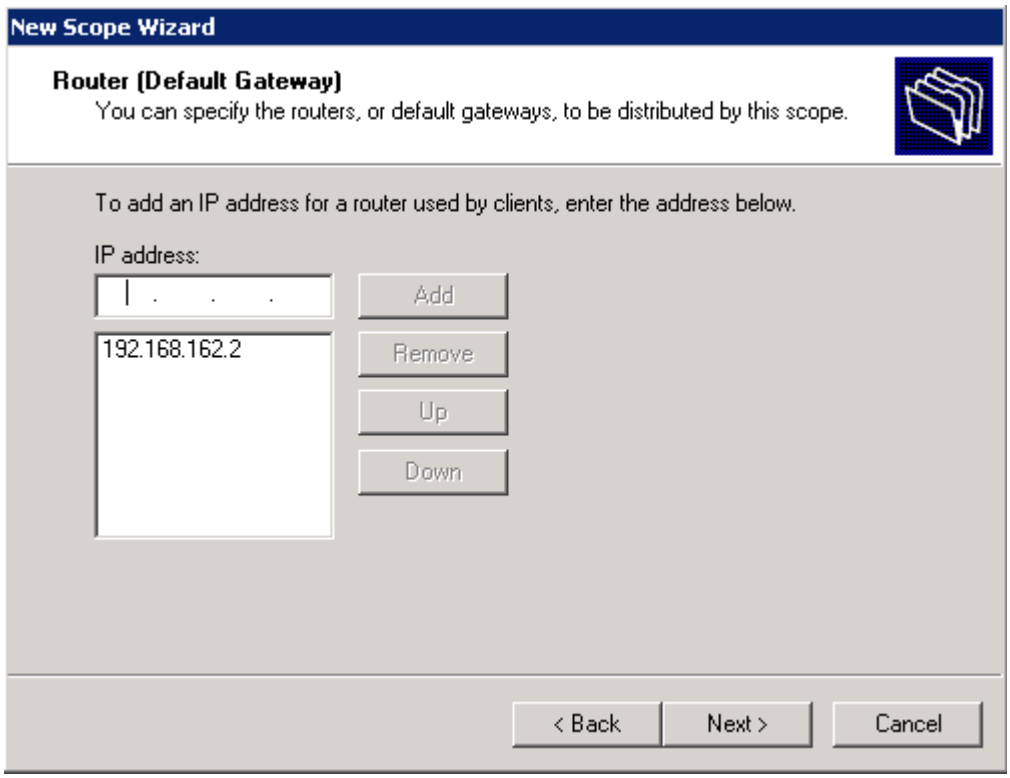
21. Configureer de leasetijd en klik op Volgende.



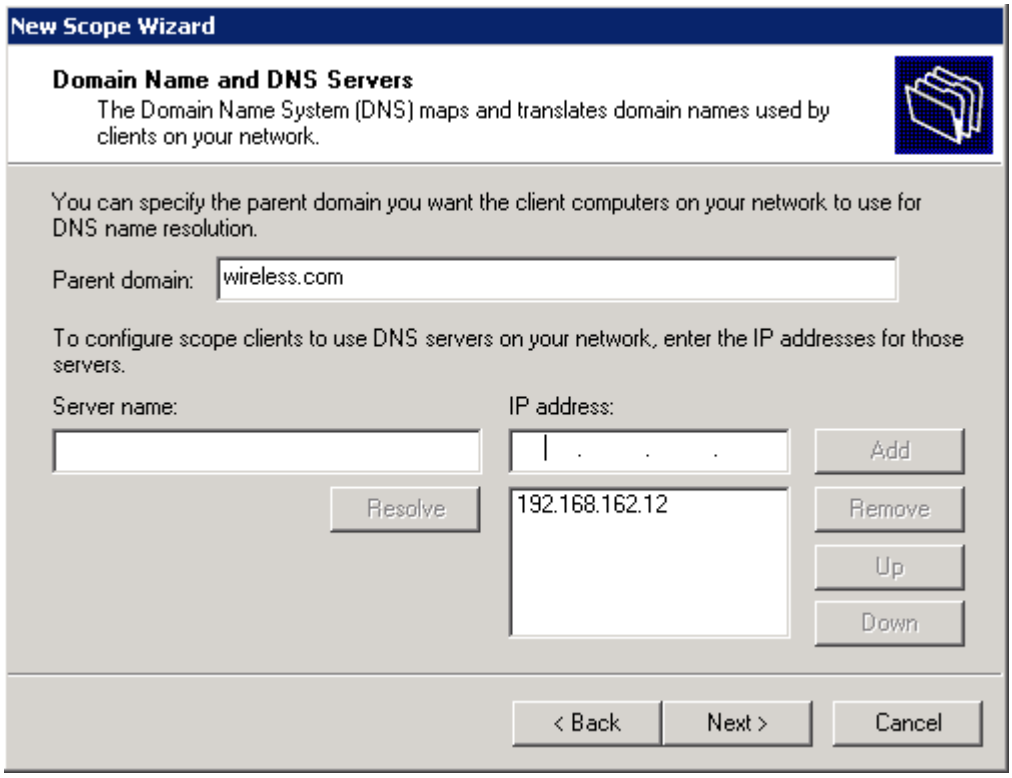
22. Klik op Ja, ik wil deze opties nu configureren en klik op Volgende.



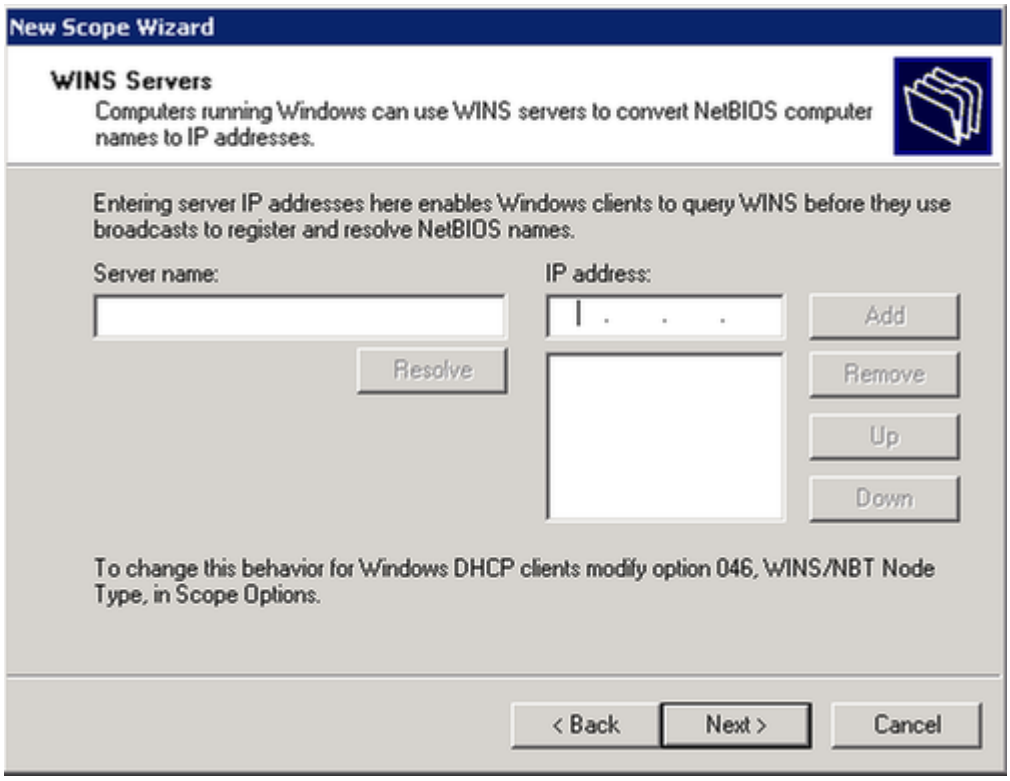
23. Voer het IP-adres van de standaardgateway voor dit bereik in en klik op Toevoegen > Volgende.



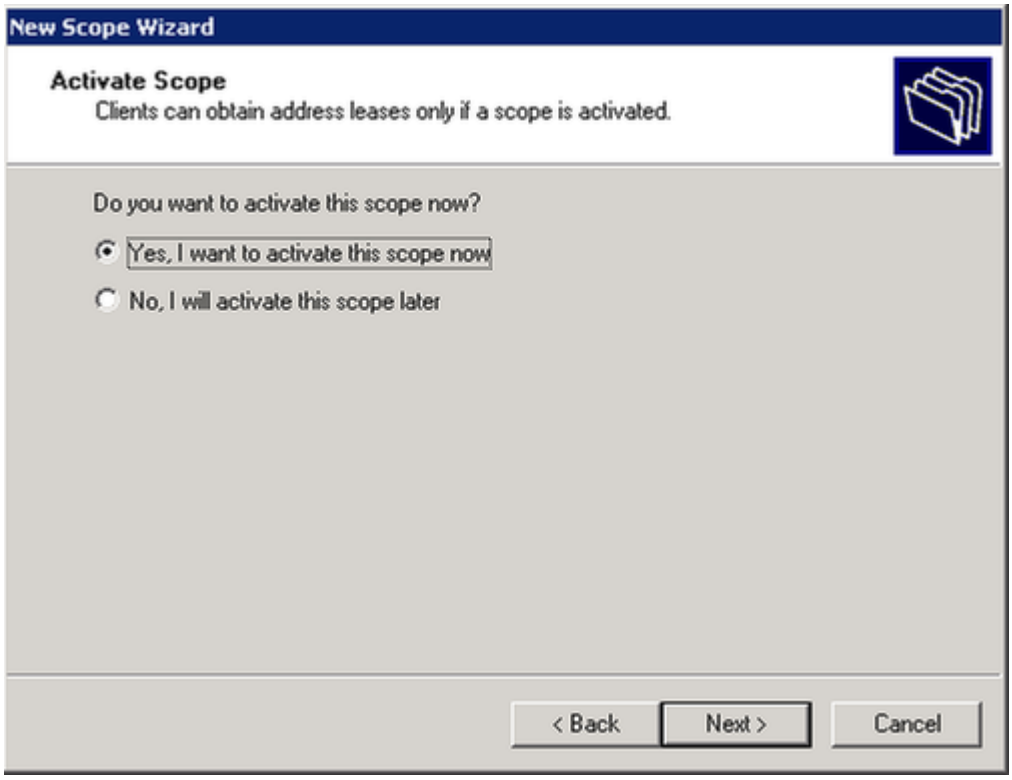
24. Configureer de DNS-domeinnaam en de DNS-server die door de clients moeten worden gebruikt. Klik op Volgende om door te gaan.



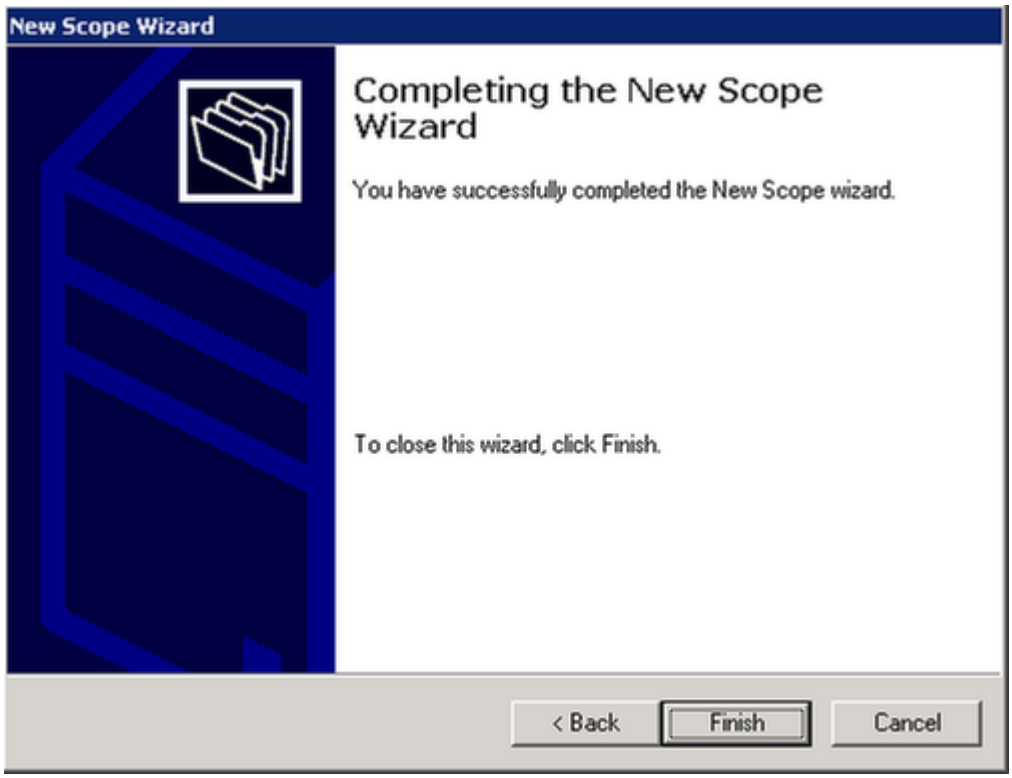
25. Voer WINS-gegevens voor dit bereik in als het netwerk WINS ondersteunt. Klik op Volgende om door te gaan.



26. Om dit bereik te activeren, klikt u op Ja, ik wil dit bereik nu activeren> Volgende.



27. Klik op Voltooien om de wizard te voltooien en te sluiten.

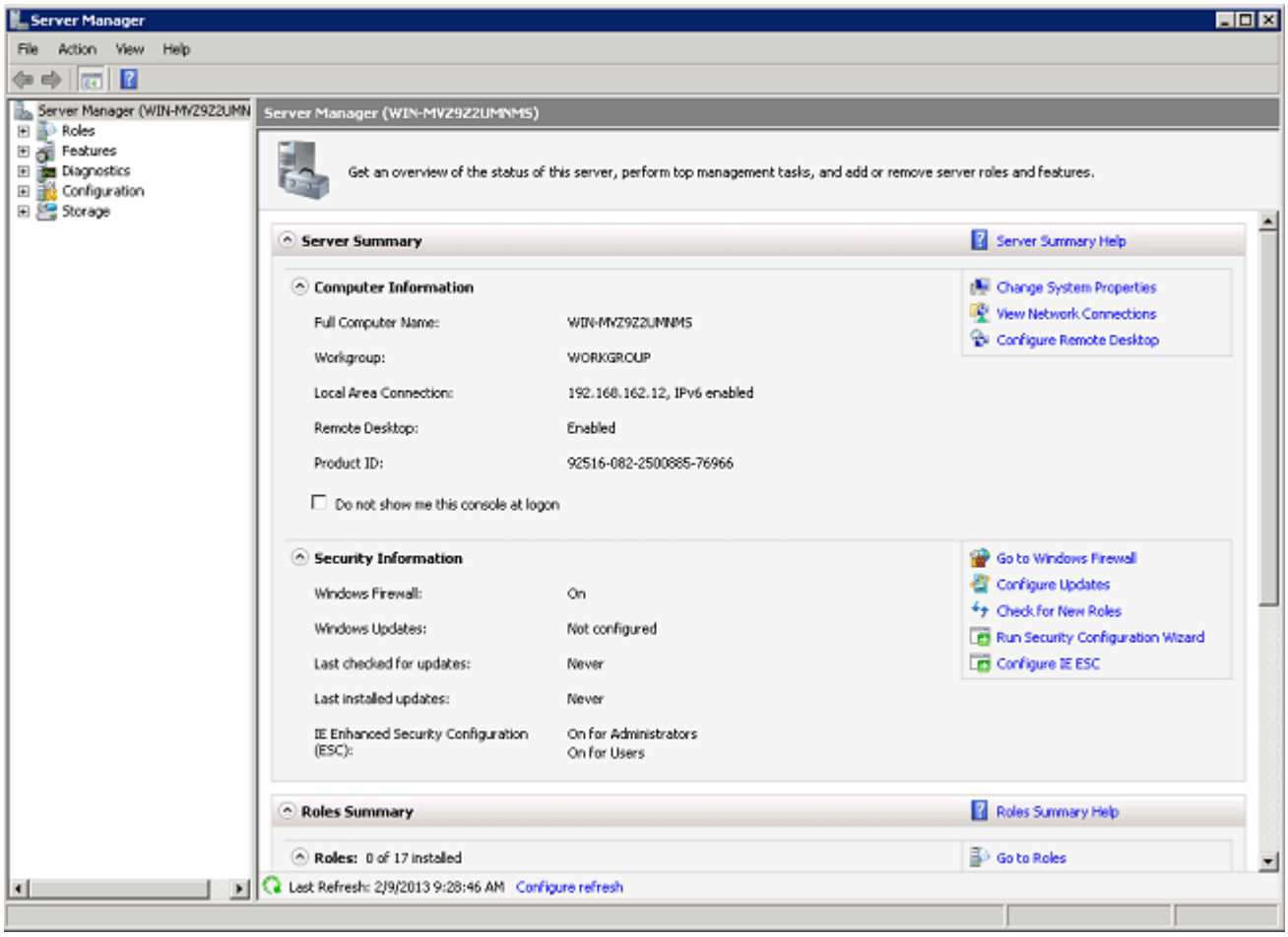


De Microsoft Windows 2008-server als CA-server installeren en configureren

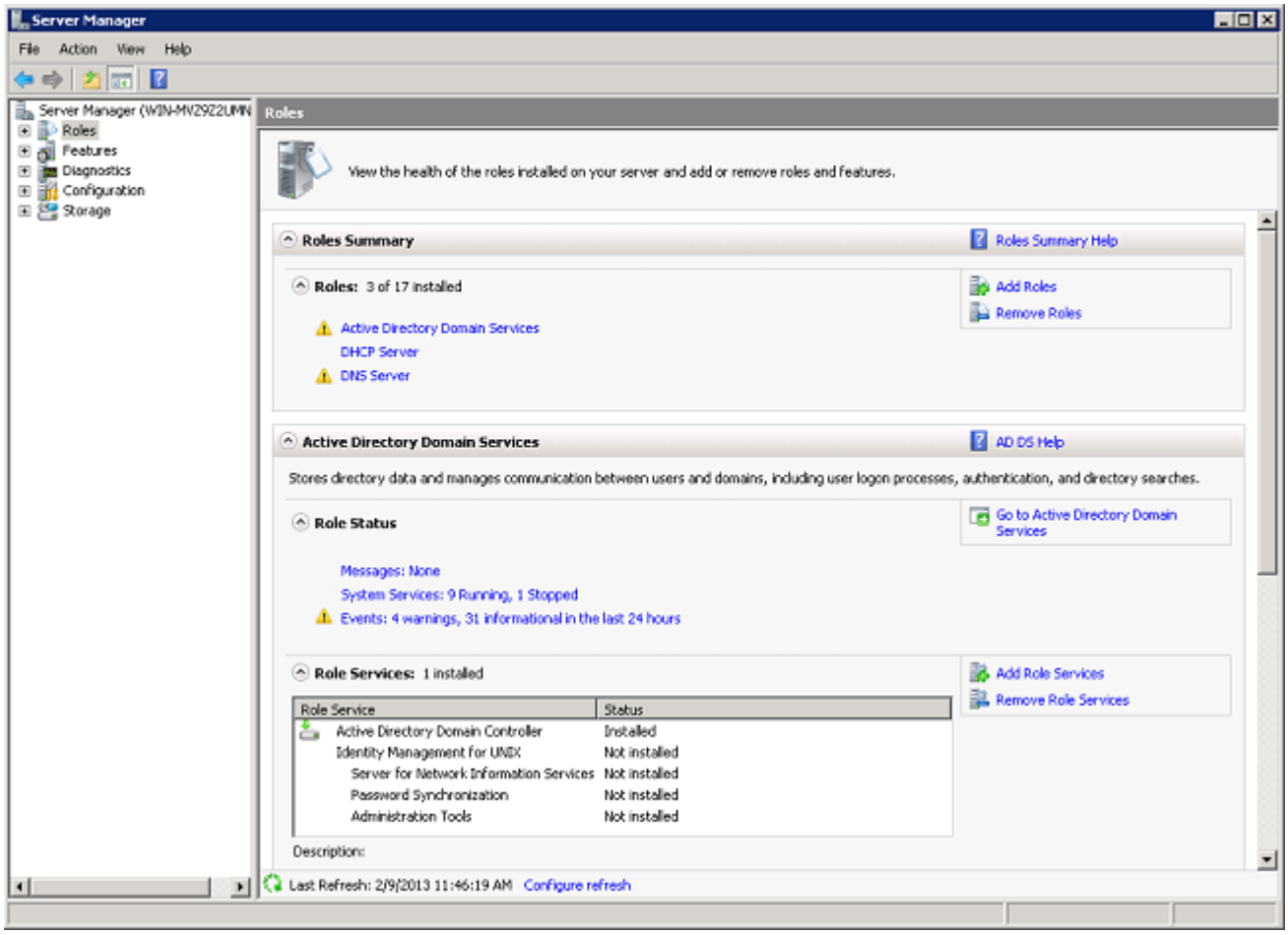
PEAP met EAP-MS-CHAP v2 valideert de RADIUS-server op basis van het certificaat dat op de server aanwezig is. Bovendien moet het servercertificaat worden uitgegeven door een openbare CA die wordt vertrouwd door de clientcomputer (dat wil zeggen dat het openbare CA-certificaat al bestaat in de map Trusted Root Certification Authority op het clientcomputercertificaatarchief).

Voer deze stappen uit om de Microsoft Windows 2008-server te configureren als een CA-server die het certificaat aan de NPS afgeeft:

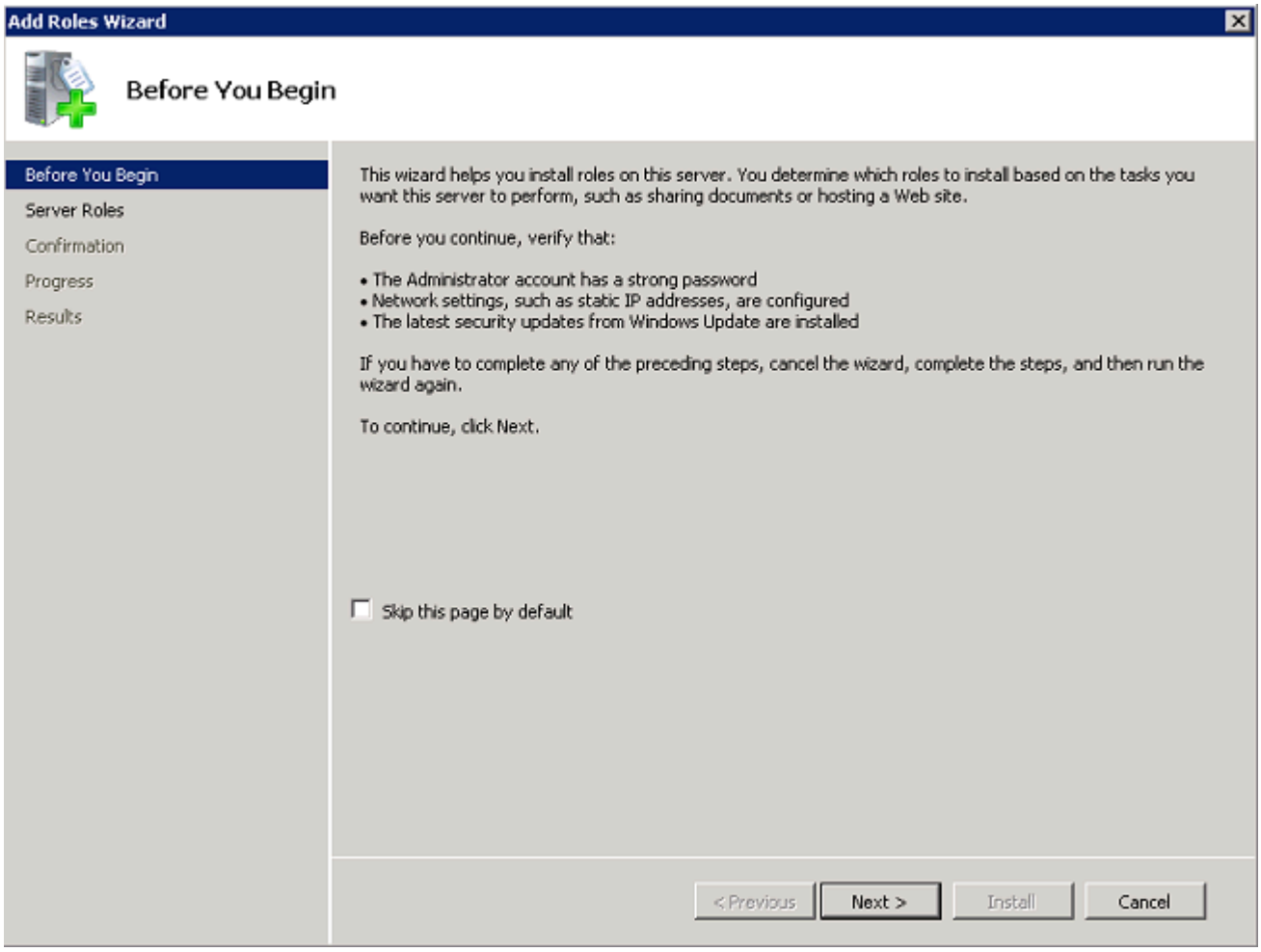
1. Klik op Start> Serverbeheer.



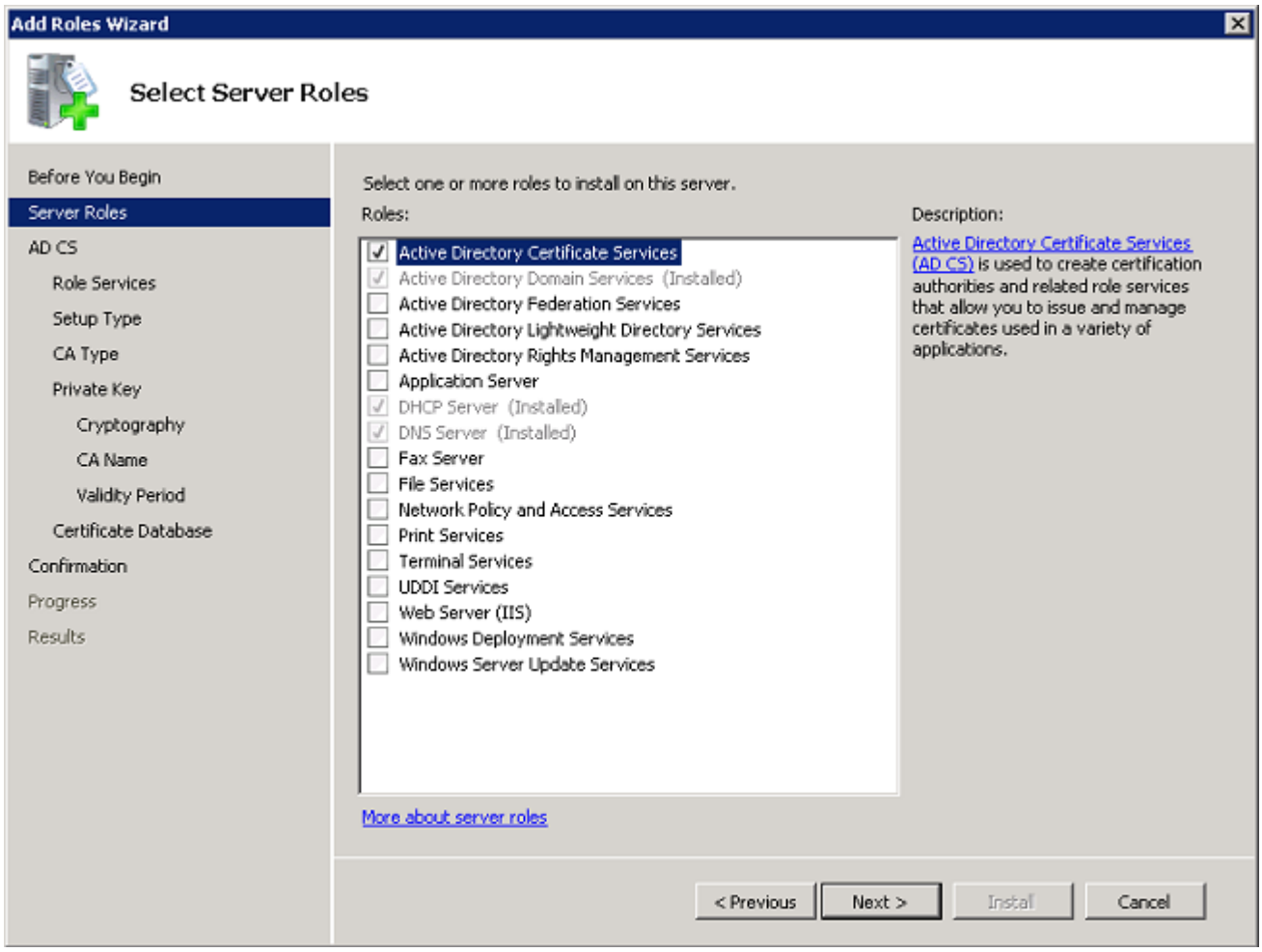
2. Klik op Rollen> Rollen toevoegen.



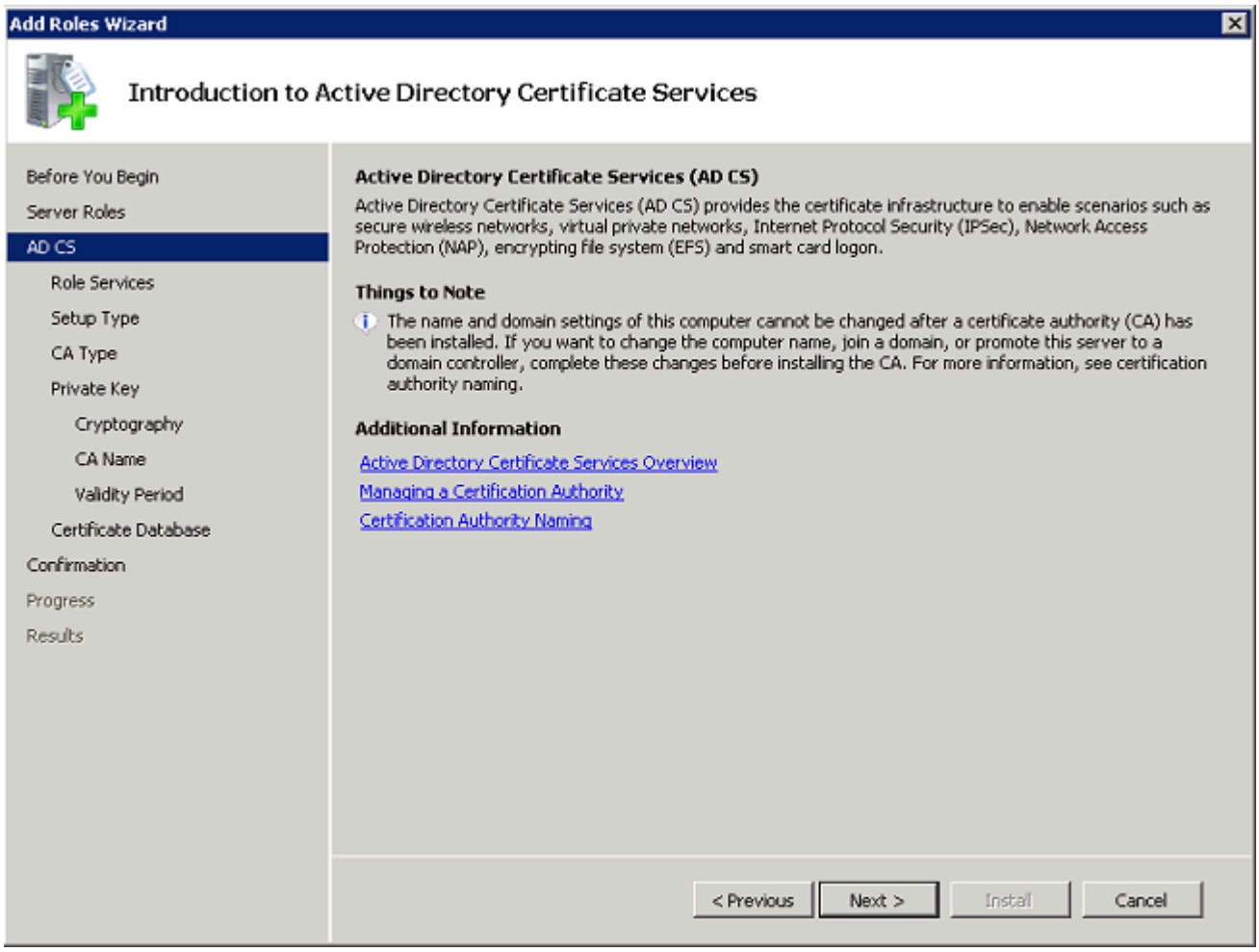
3. Klik op Next (Volgende).



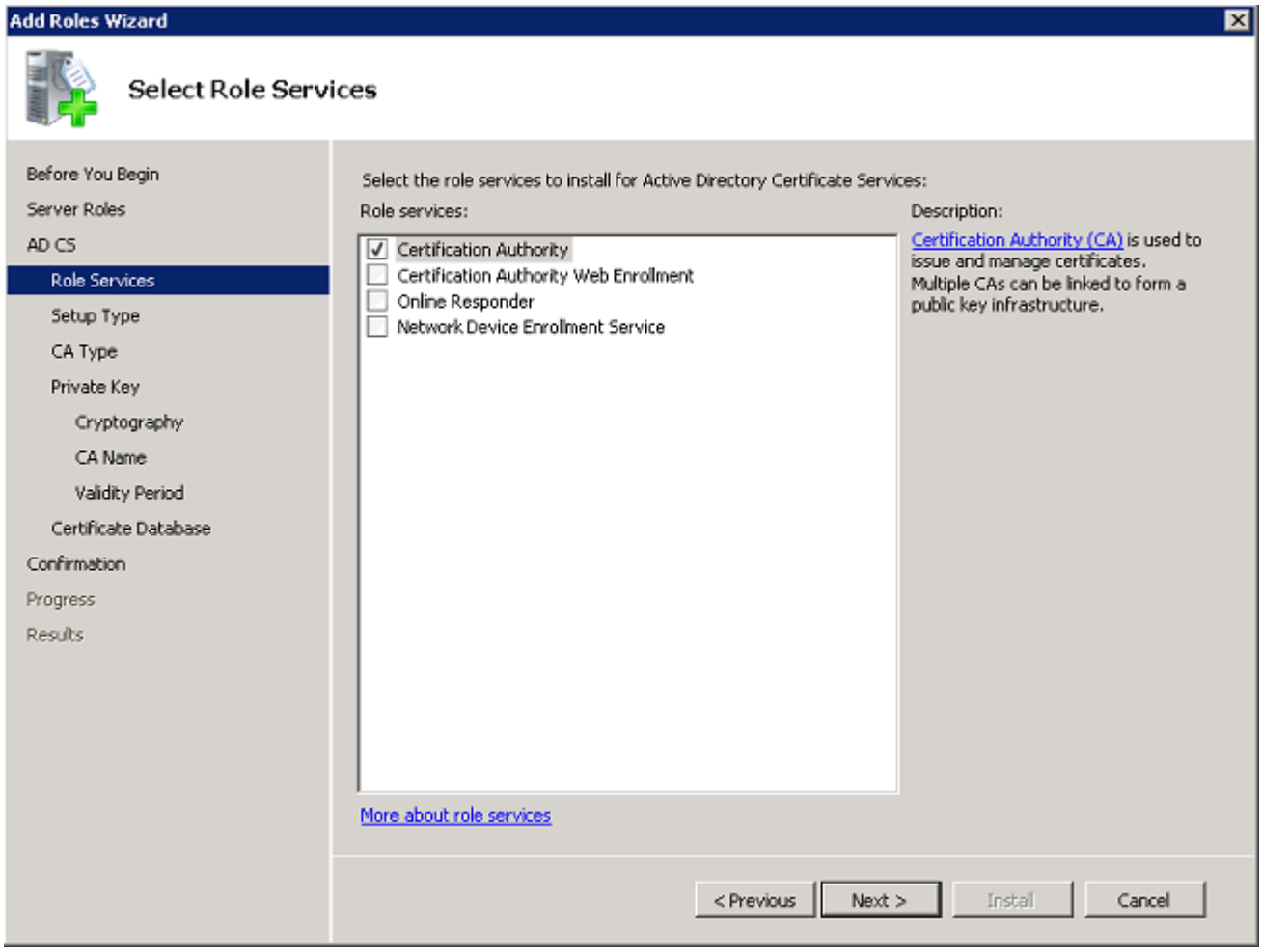
4. Selecteer de service Active Directory Certificate Services en klik op Volgende.



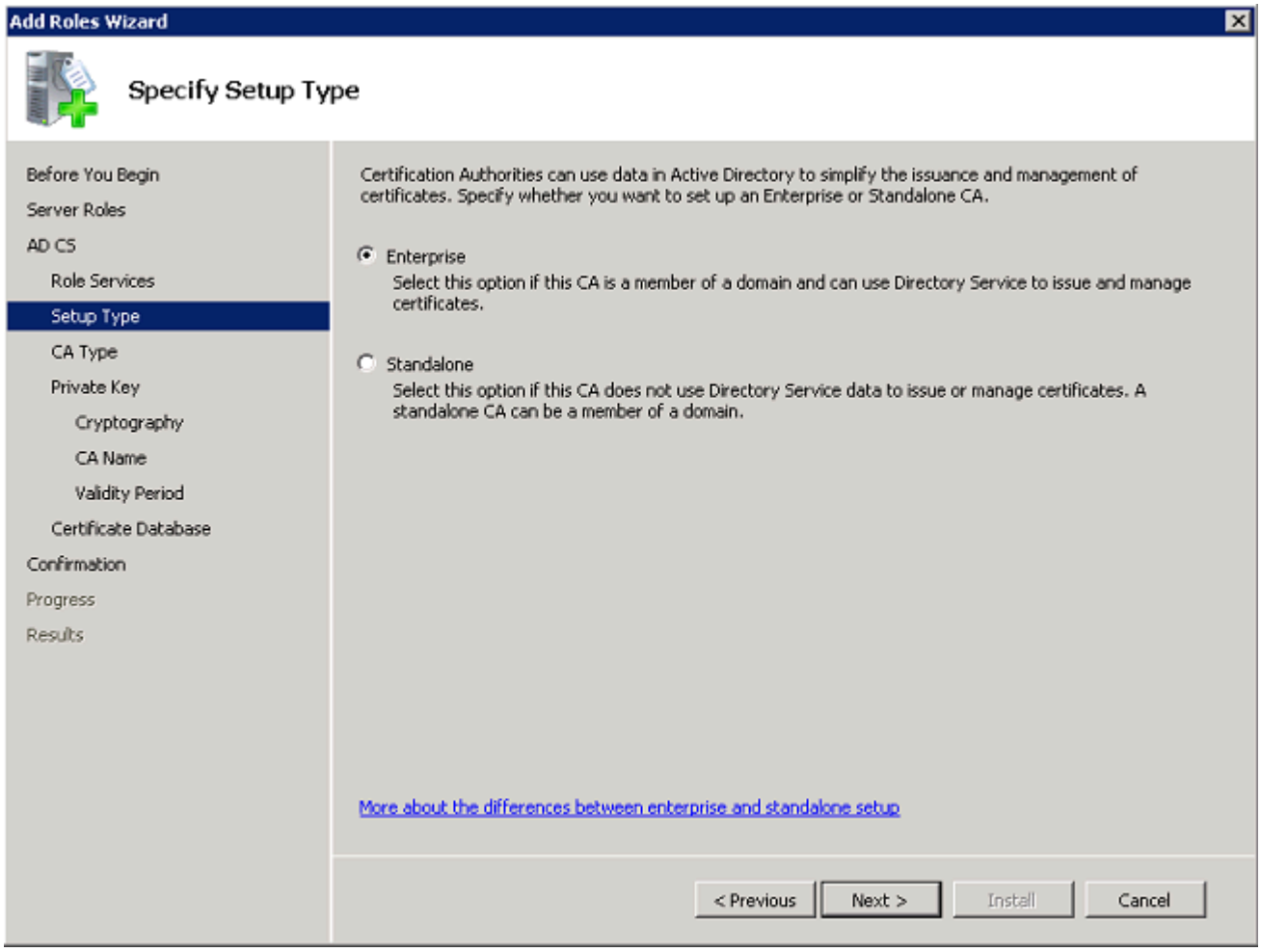
5. Controleer de introductie van Active Directory Certificate Services en klik op Volgende.



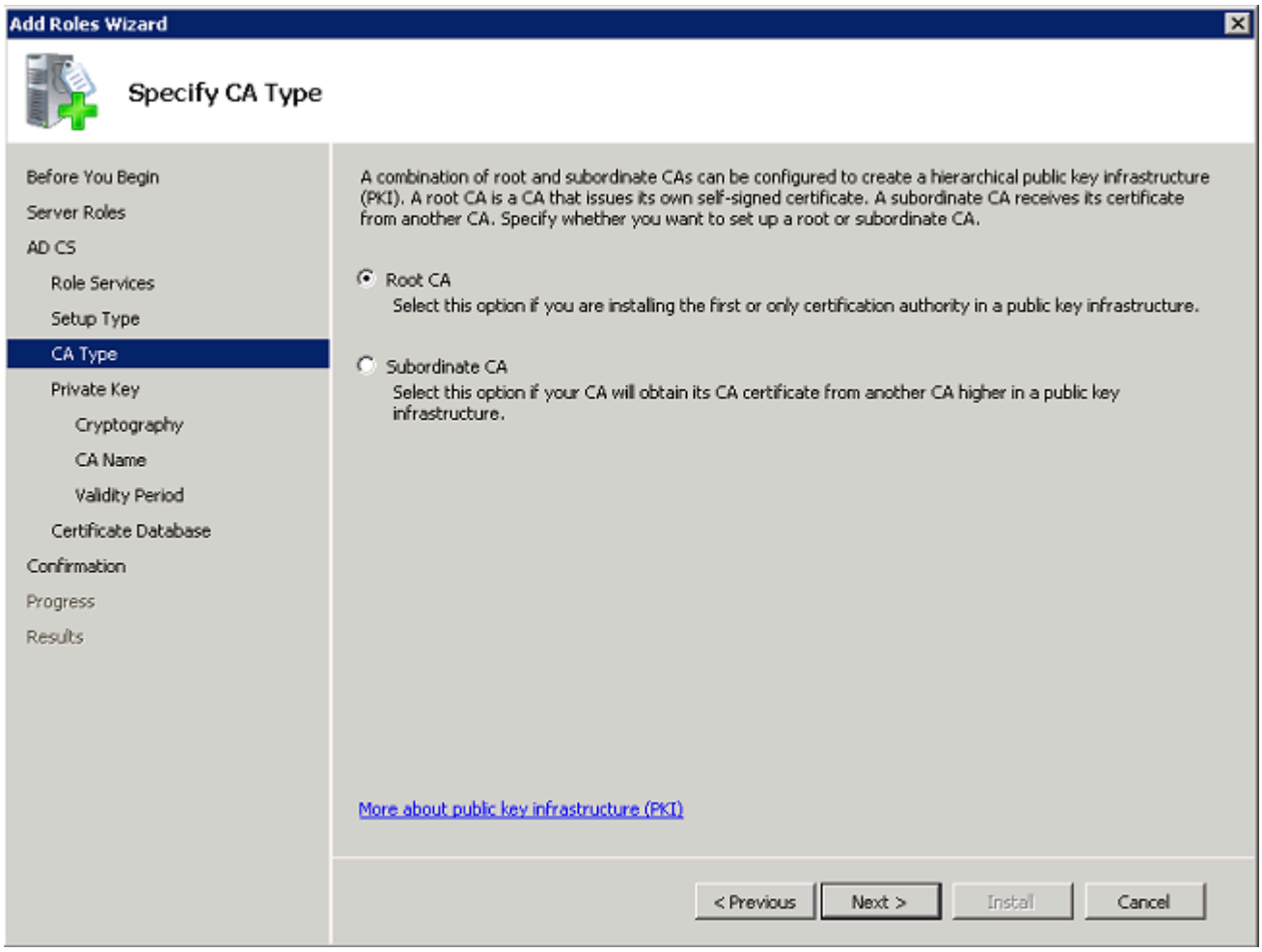
6. Selecteer de certificeringsinstantie en klik op Volgende.



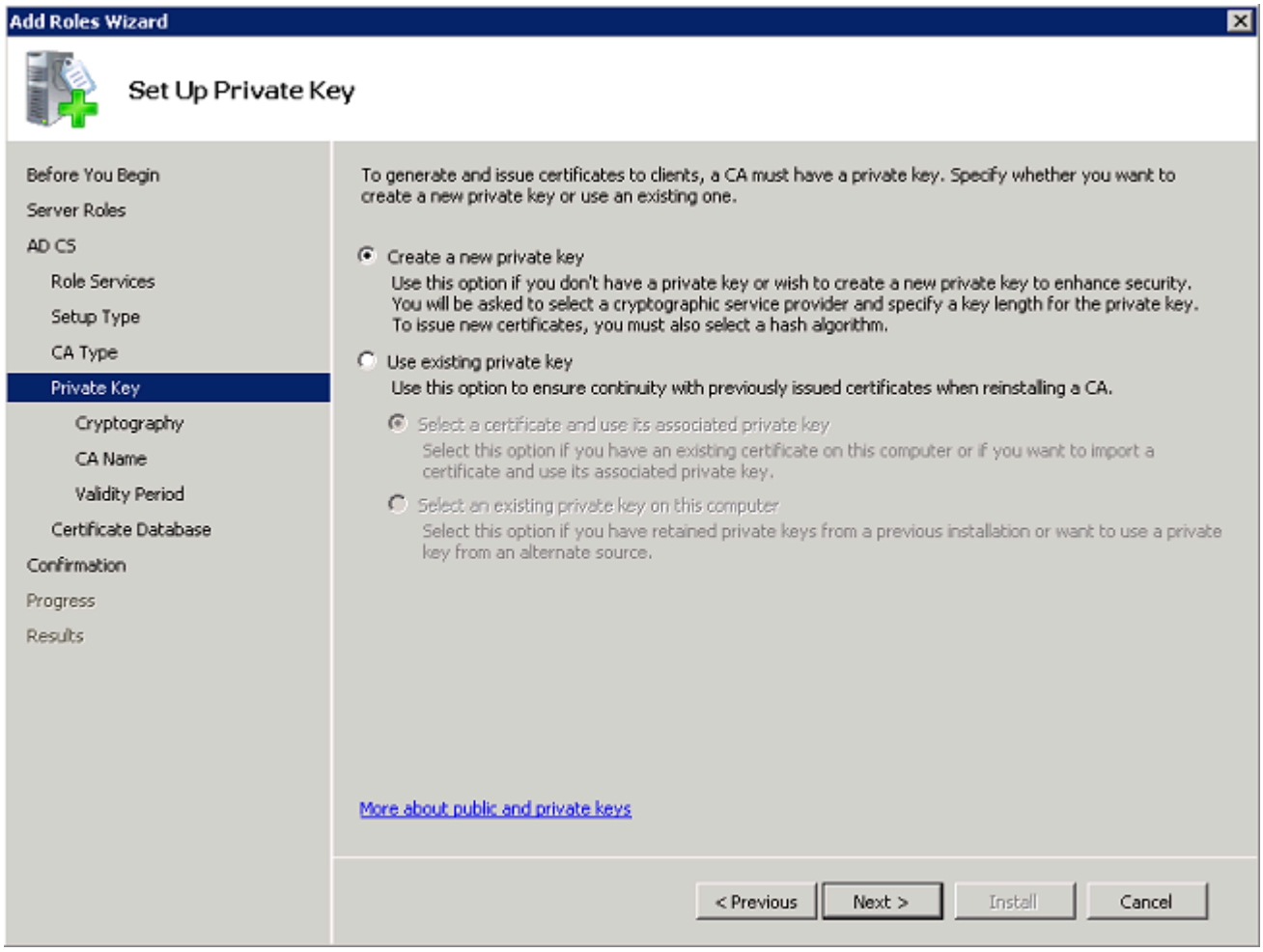
7. Selecteer Enterprise en klik op Volgende.



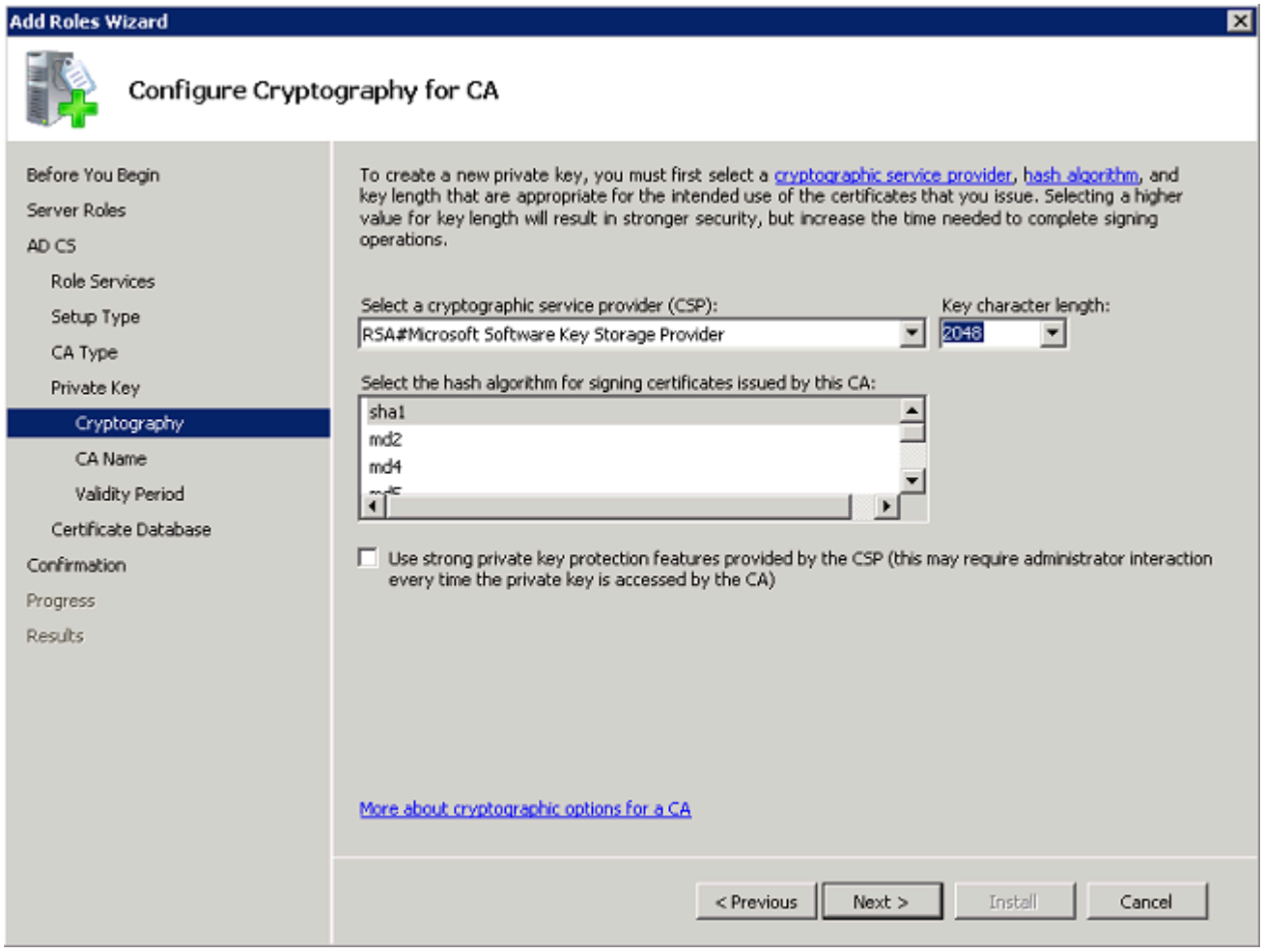
8. Selecteer CA starten en klik op Volgende.



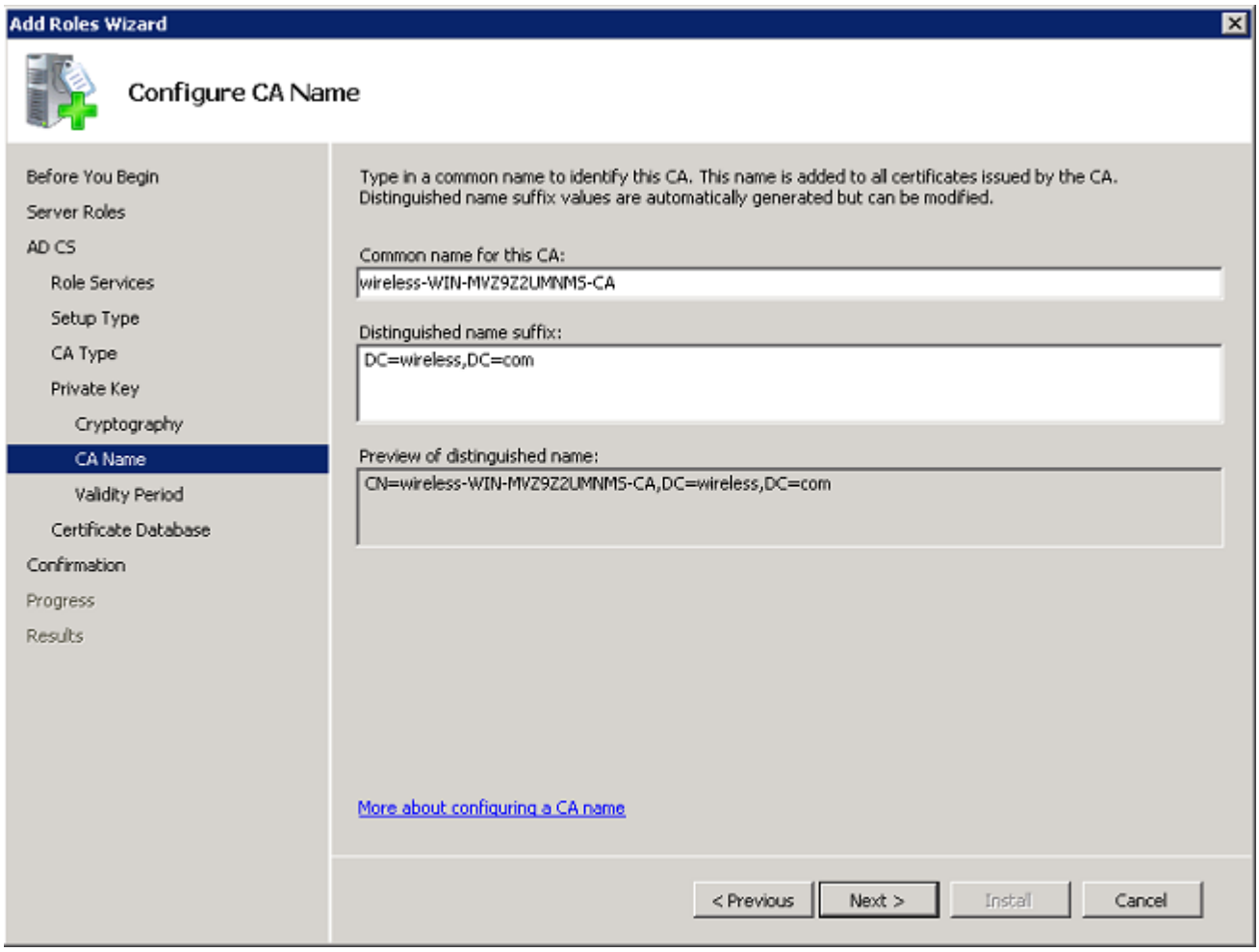
9. Selecteer Een nieuwe privésleutel maken en klik op Volgende.



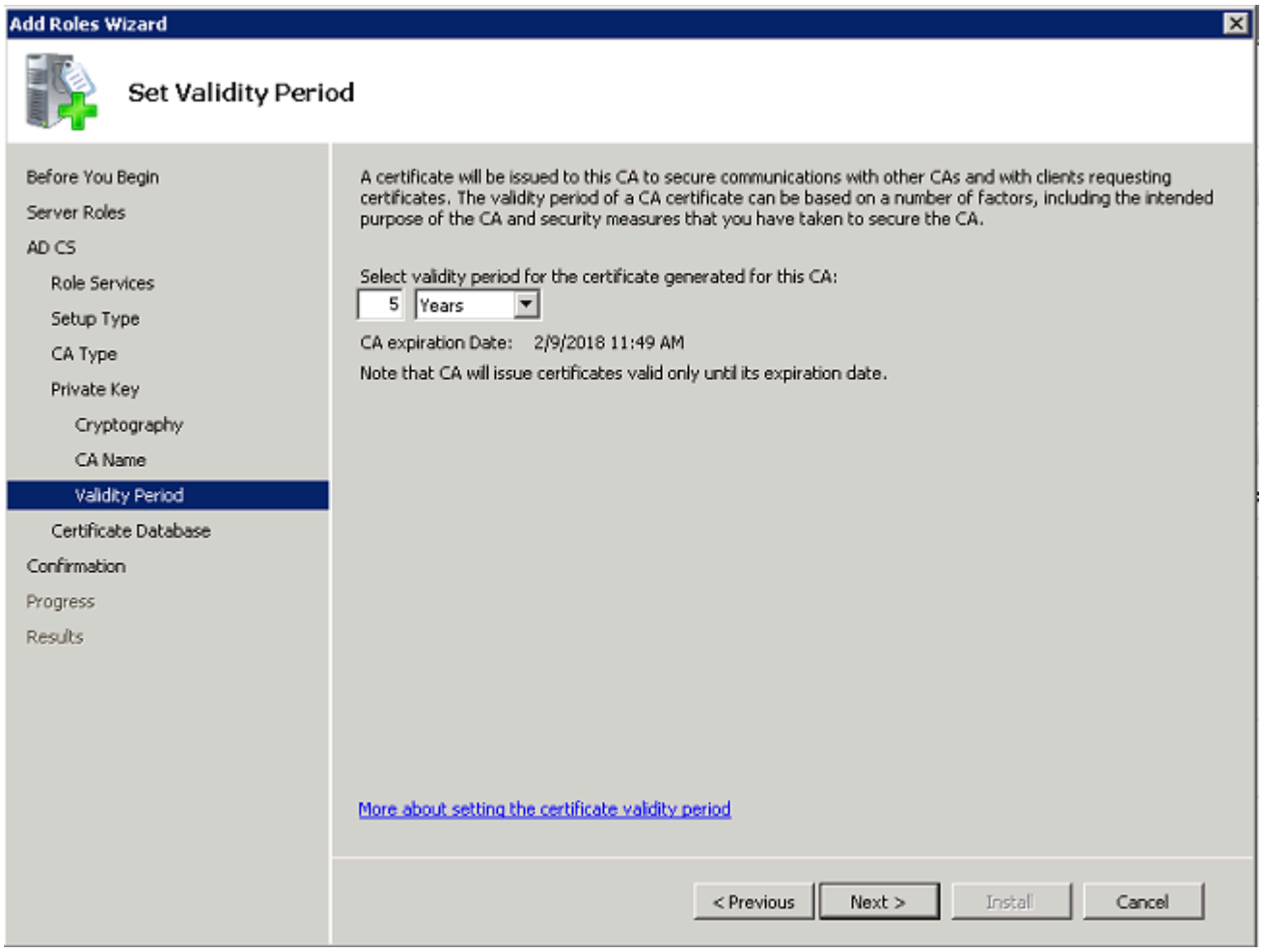
10. Klik op Volgende op Cryptografie configureren voor CA.



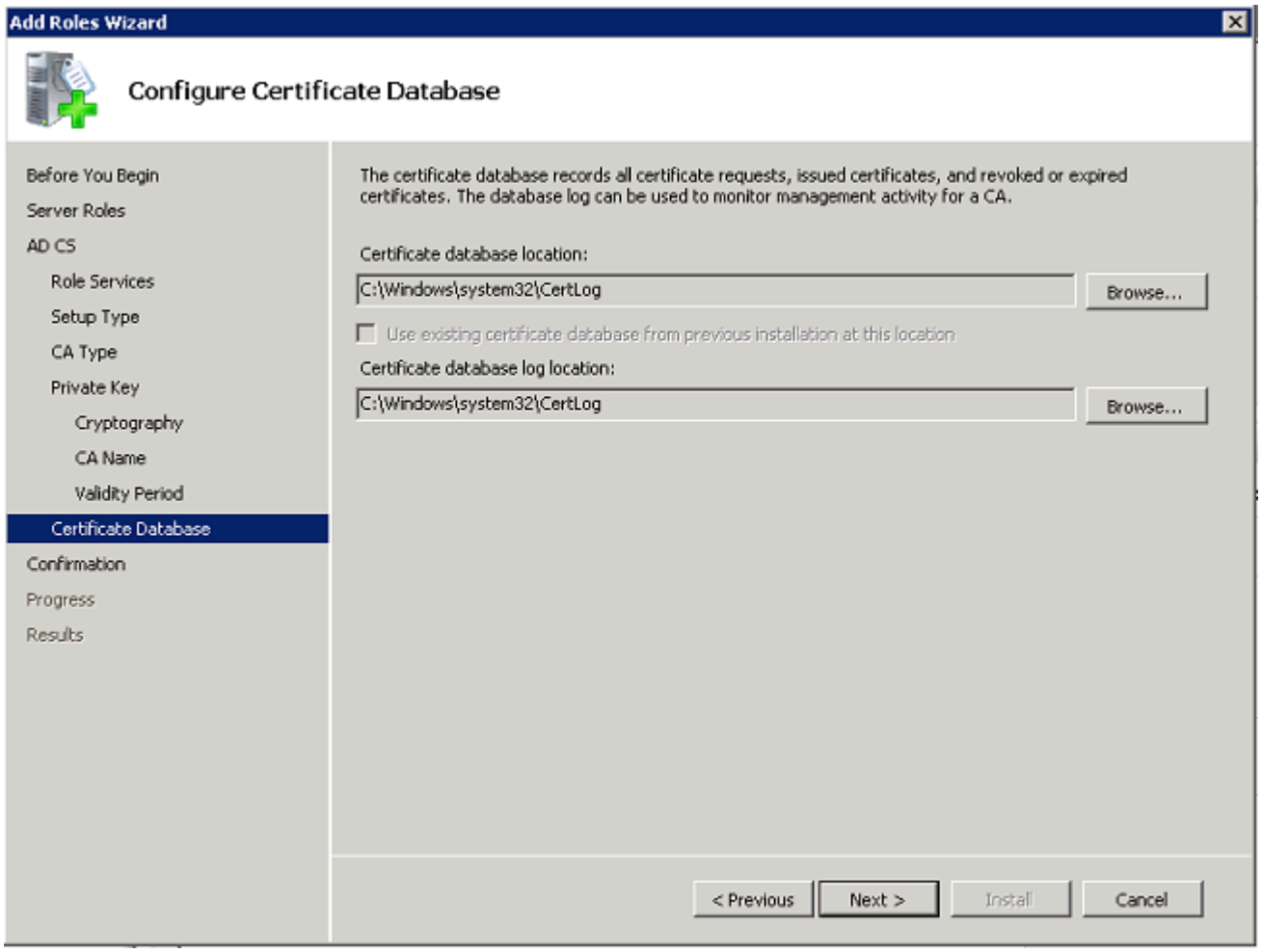
11. Klik op Volgende om de standaard gemeenschappelijke naam voor deze CA te accepteren.



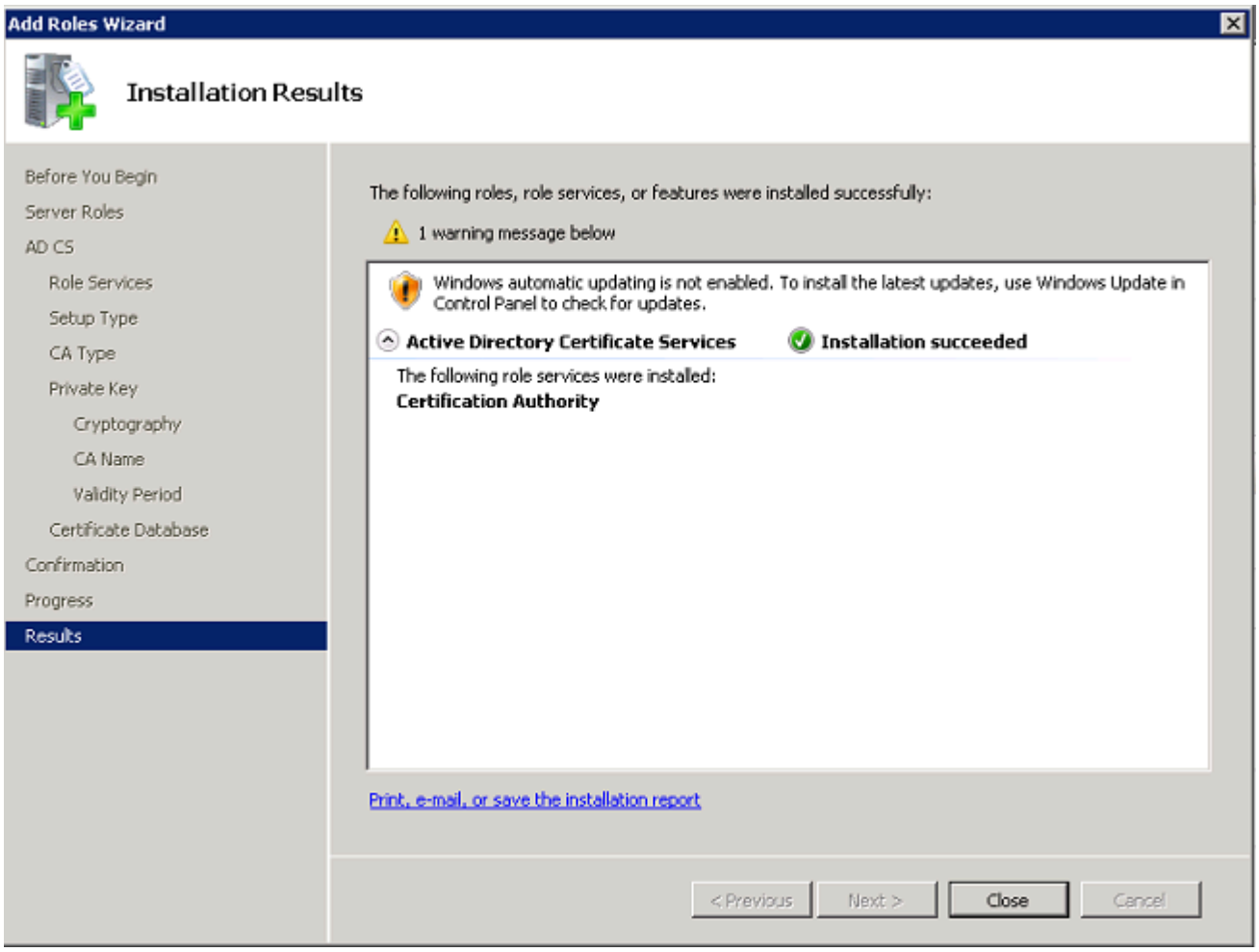
12. Selecteer de geldigheidsduur van dit CA-certificaat en klik op Volgende.



13. Klik op Volgende om de standaardlocatie voor de certificaatdatabase te accepteren.



14. Controleer de configuratie en klik op Installeren om de Active Directory Certificate Services te starten.

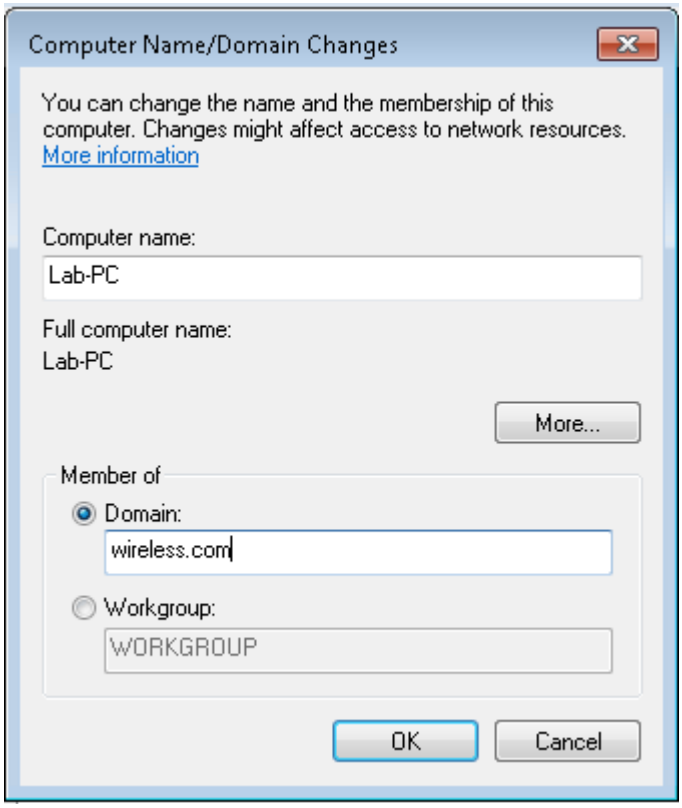


15. Nadat de installatie is voltooid, klikt u op Sluiten.

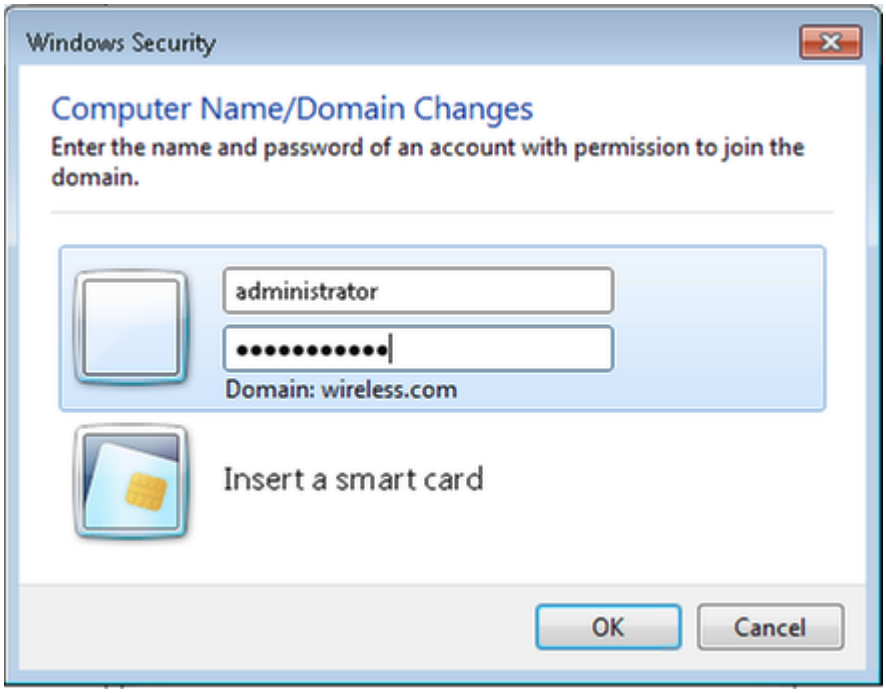
Cliënten verbinden met het domein

Voer deze stappen uit om de clients te verbinden met het bekabelde netwerk en om de domeinspecifieke informatie van het nieuwe domein te downloaden:

1. Sluit de clients aan op het bekabelde netwerk met een straight through Ethernet-kabel.
2. Start de client op en log in met de gebruikersnaam en het wachtwoord van de client.
3. Klik op Start>Uitvoeren, voer cmd in en klik op OK.
4. Voer bij de opdrachtprompt ipconfig in en klik op Enter om te controleren of DHCP correct werkt en of de client een IP-adres van de DHCP-server heeft ontvangen.
5. Als u de client wilt toevoegen aan het domein, klikt u op Start, klikt u met de rechtermuisknop op Computer, kiest u Eigenschappen en kiest u Instellingen wijzigen rechtsonder.
6. Klik op Wijzigen.
7. Klik op Domein, voer de domeinnaam Wireless in voor dit voorbeeld en klik op OK.

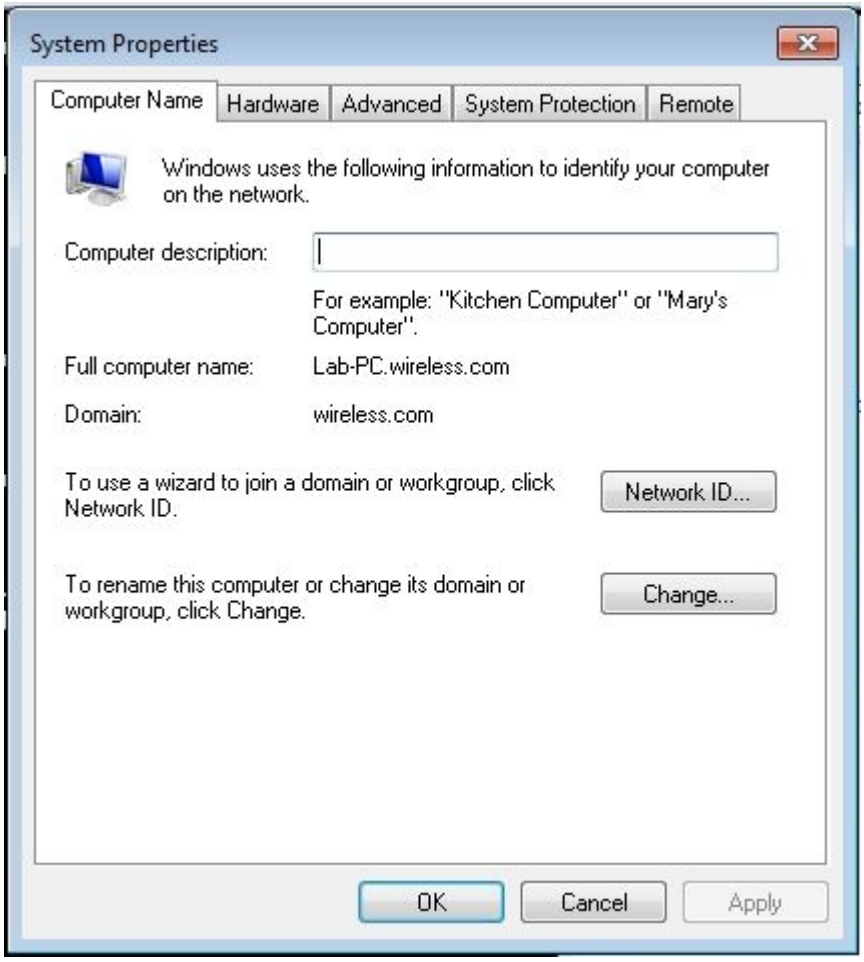


8. Voer de beheerder van de gebruikersnaam en het wachtwoord in dat specifiek is voor het domein waaraan de client deelneemt. Dit is de beheerdersaccount in de Active Directory op de server.

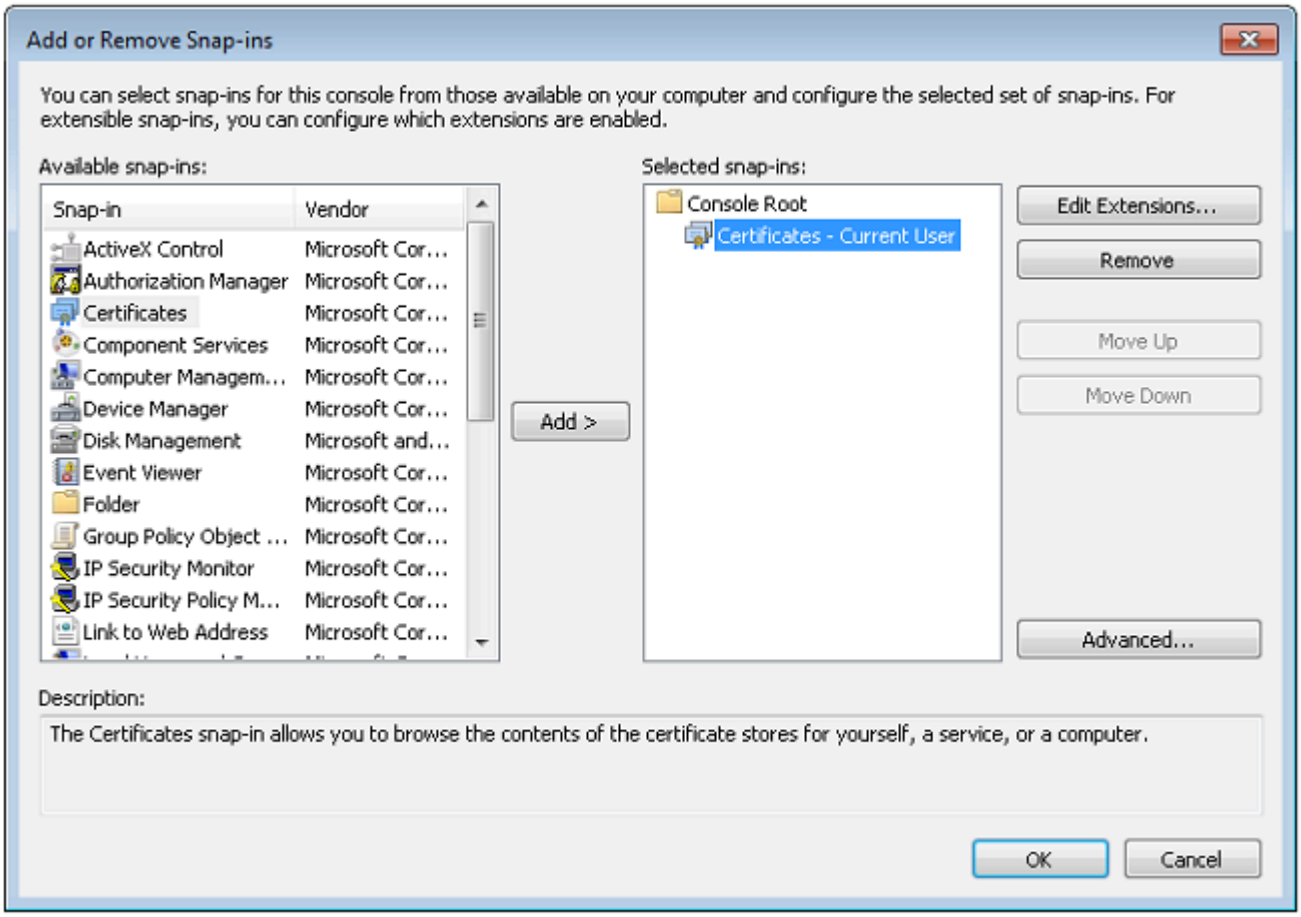


9. Klik op OK en klik nogmaals op OK.

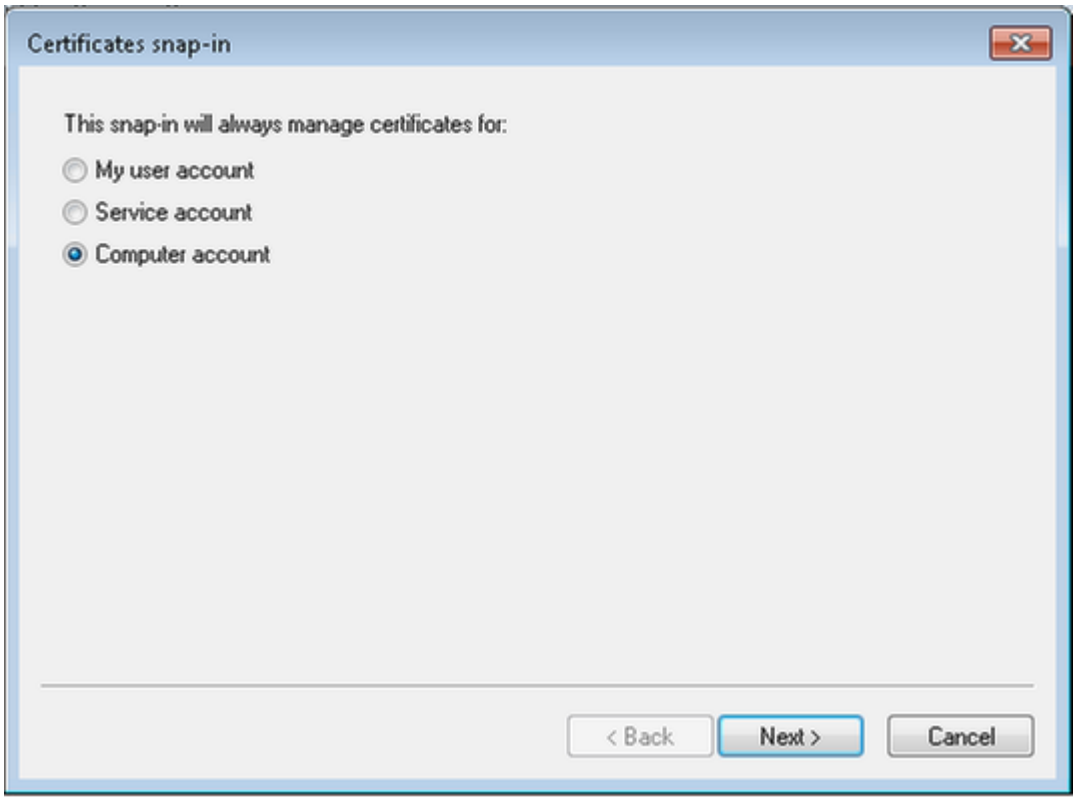
10. Klik op Sluiten>Nu opnieuw starten om de computer opnieuw op te starten.
11. Wanneer de computer opnieuw is opgestart, meldt u zich aan met: Gebruikersnaam = Beheerder; Wachtwoord = <domeinwachtwoord>; Domein = draadloos.
12. Klik op Start, klik met de rechtermuisknop op Computer, kies Eigenschappen en kies Instellingen wijzigen rechtsonder om te controleren of u zich in het draadloze domein bevindt.
13. De volgende stap is om te controleren of de client het CA-certificaat (vertrouwen) van de server heeft ontvangen.



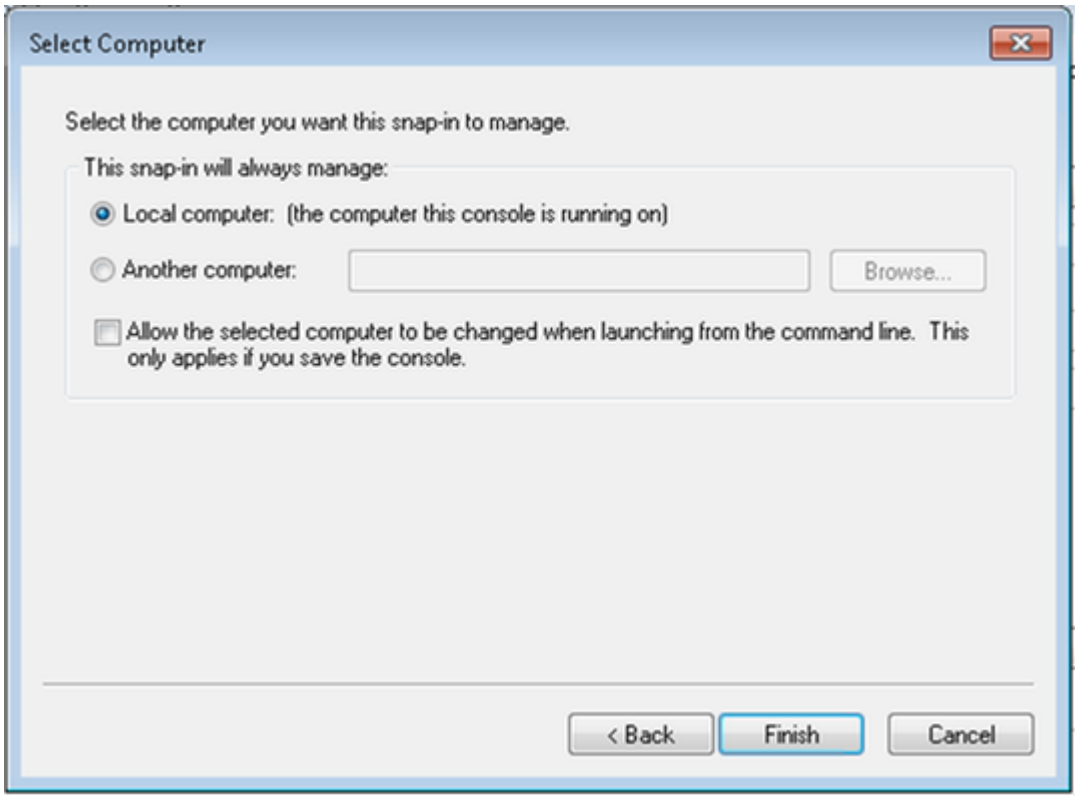
14. Klik op Start, voer mmc in en druk op Enter.
15. Klik op Bestand en klik op Add/Remove snap-in.
16. Kies Certificaten en klik op Toevoegen.



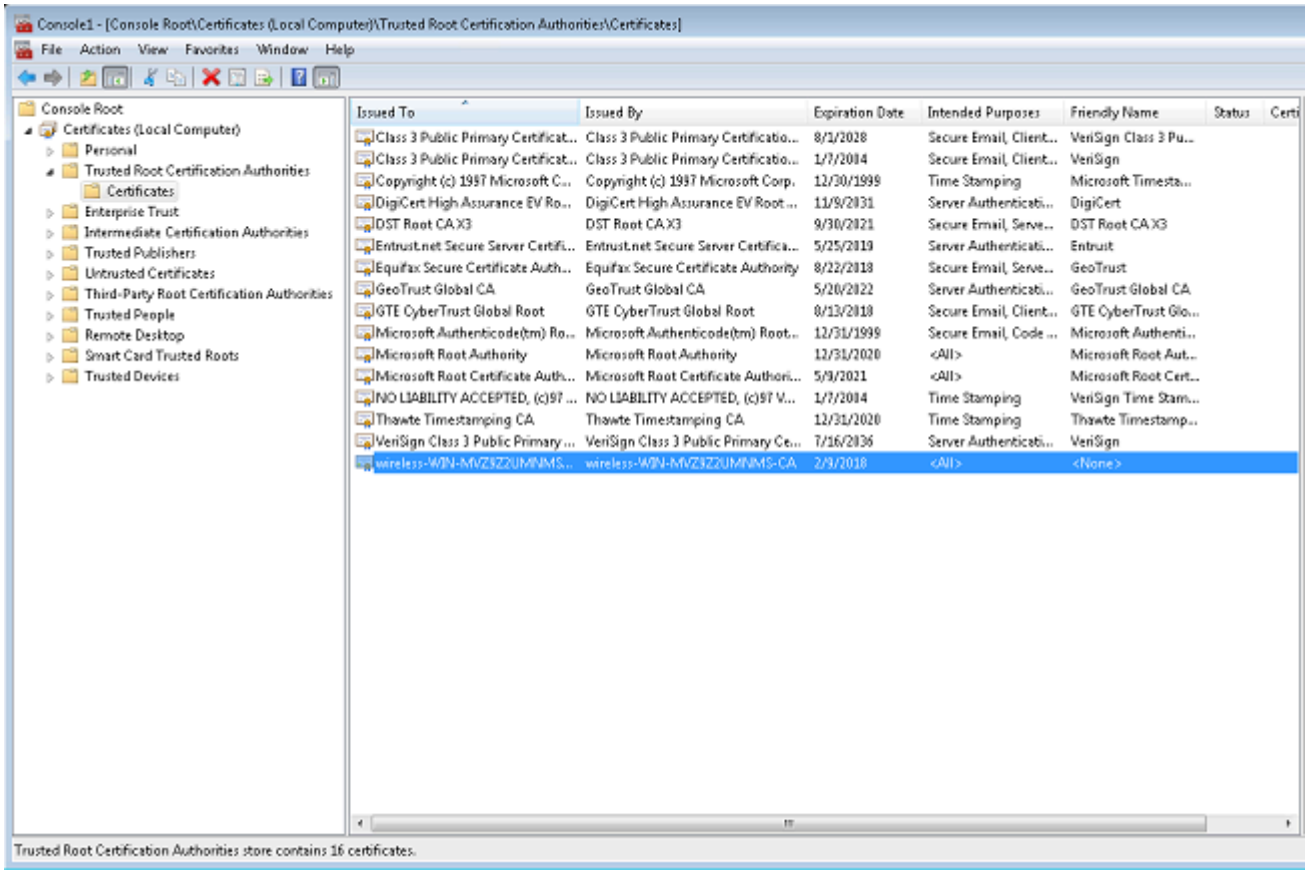
17. Klik op Computeraccount en klik op Volgende.



18. Klik op Lokale computer en klik op Volgende.



19. Klik op OK.
20. Vouw de mappen Certificaten (Lokale computer) en Vertrouwde basiscertificeringsinstanties uit en klik op Certificaten. Zoek Wireless Domain CA cert in de lijst. In dit voorbeeld wordt de CA cert wireless-WIN-MVZ9Z2UMNMS-CA genoemd.

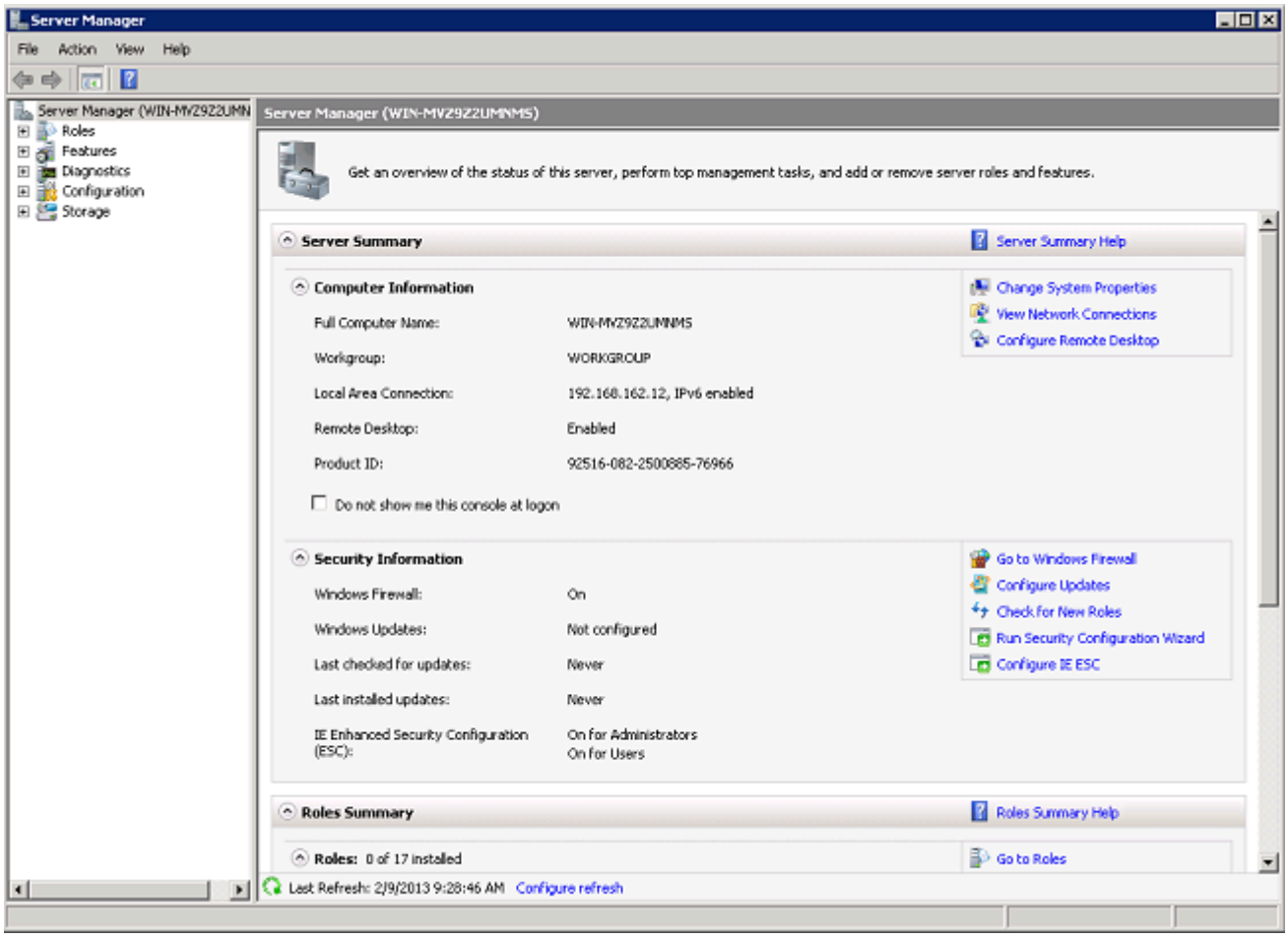


21. Herhaal deze procedure om meer clients aan het domein toe te voegen.

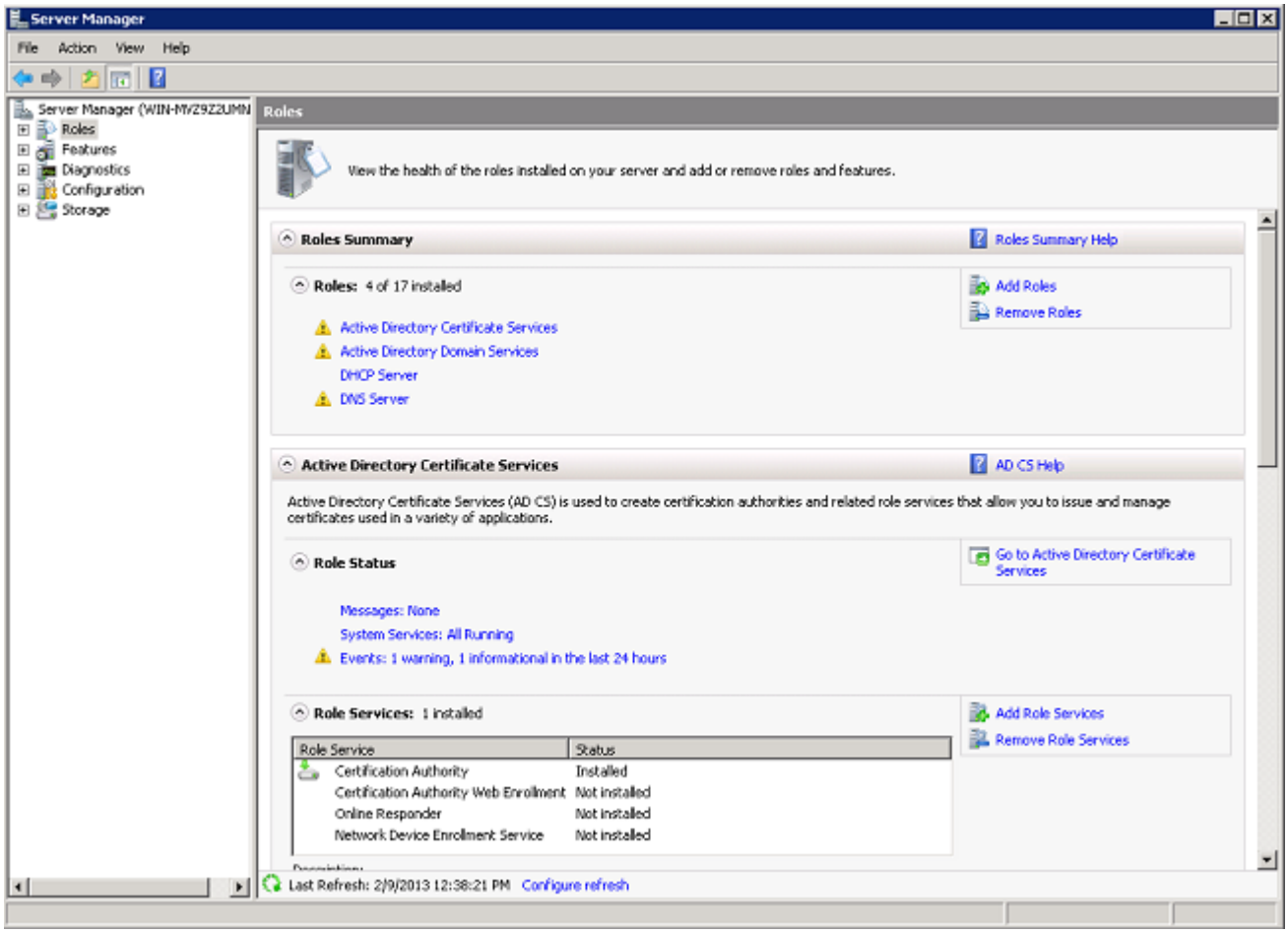
De netwerkbeleidsserver installeren op de Microsoft Windows 2008-server

In deze configuratie wordt de NPS gebruikt als een RADIUS-server voor de verificatie van draadloze clients met PEAP-verificatie. Voer de volgende stappen uit om NPS te installeren en configureren op de Microsoft Windows 2008-server:

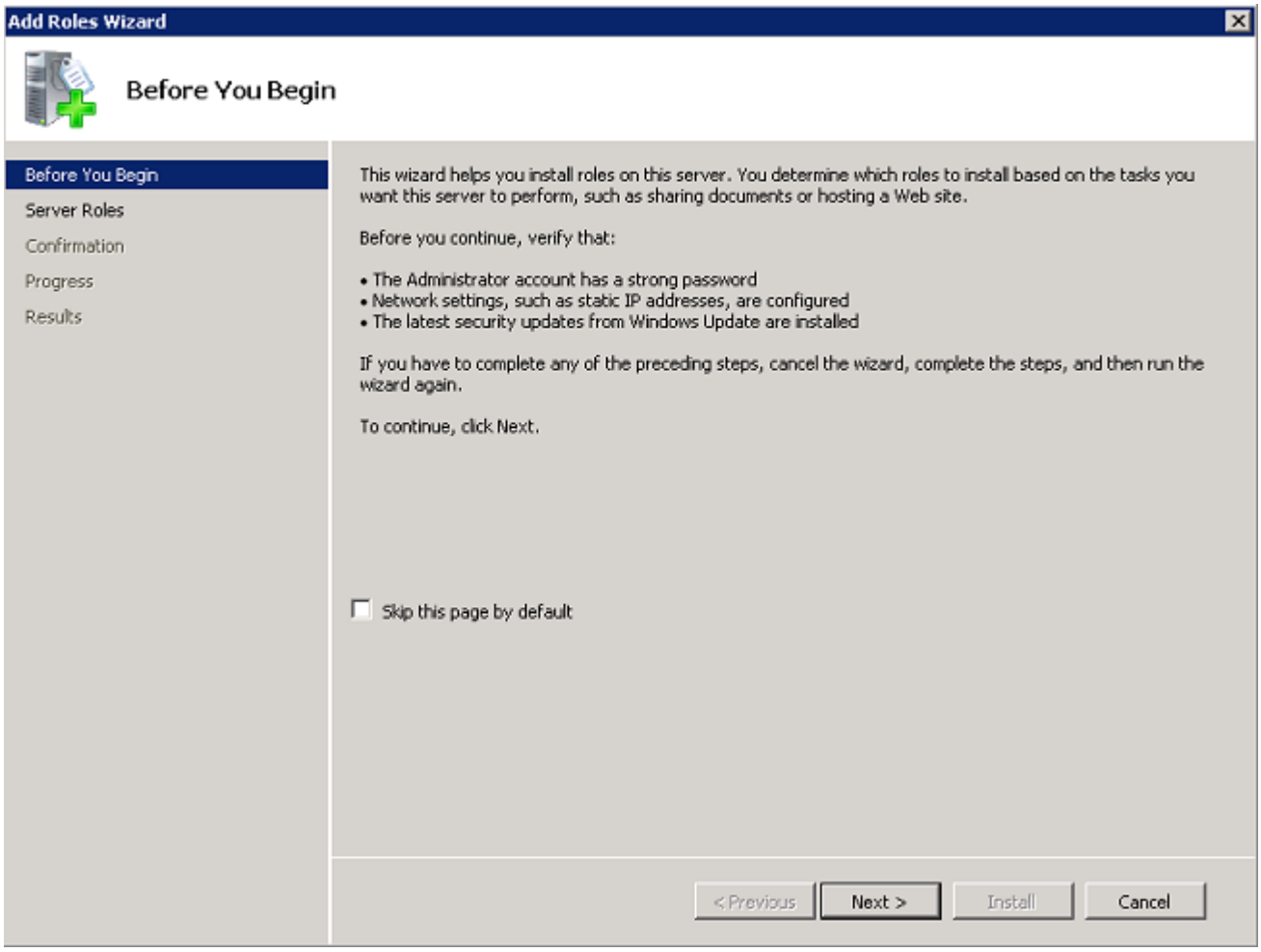
1. Klik op Start> Serverbeheer.



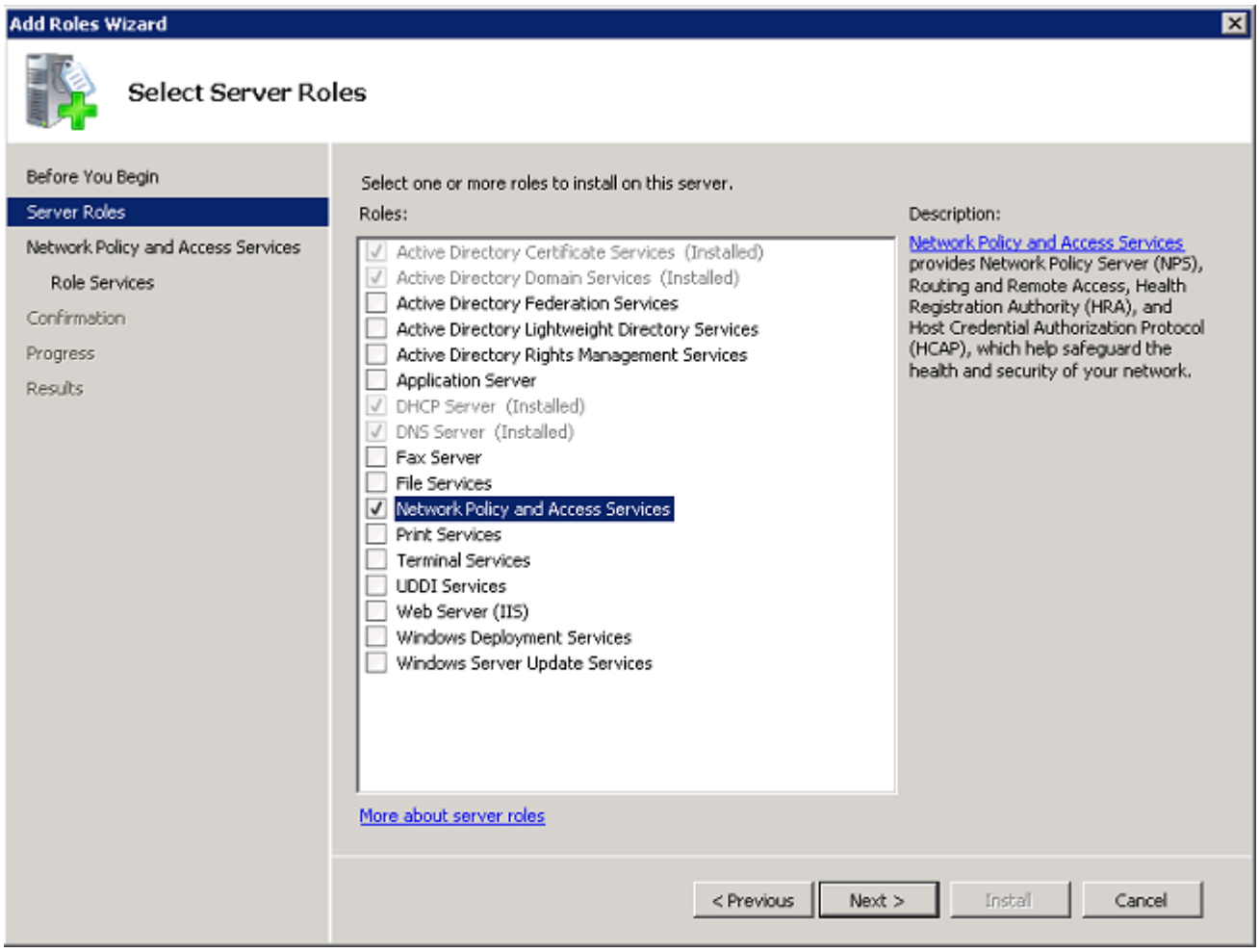
2. Klik op Rollen> Rollen toevoegen.



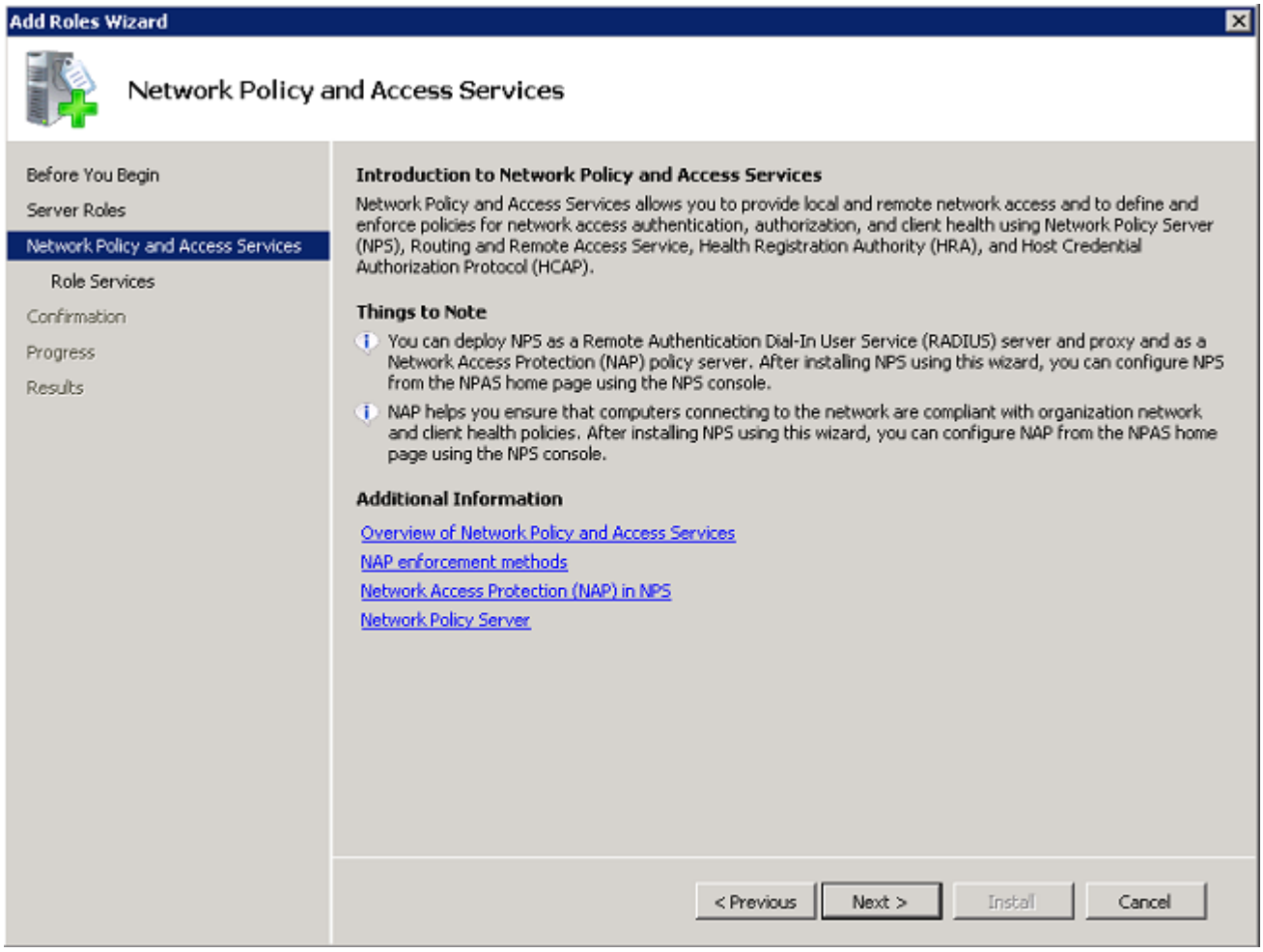
3. Klik op Next (Volgende).



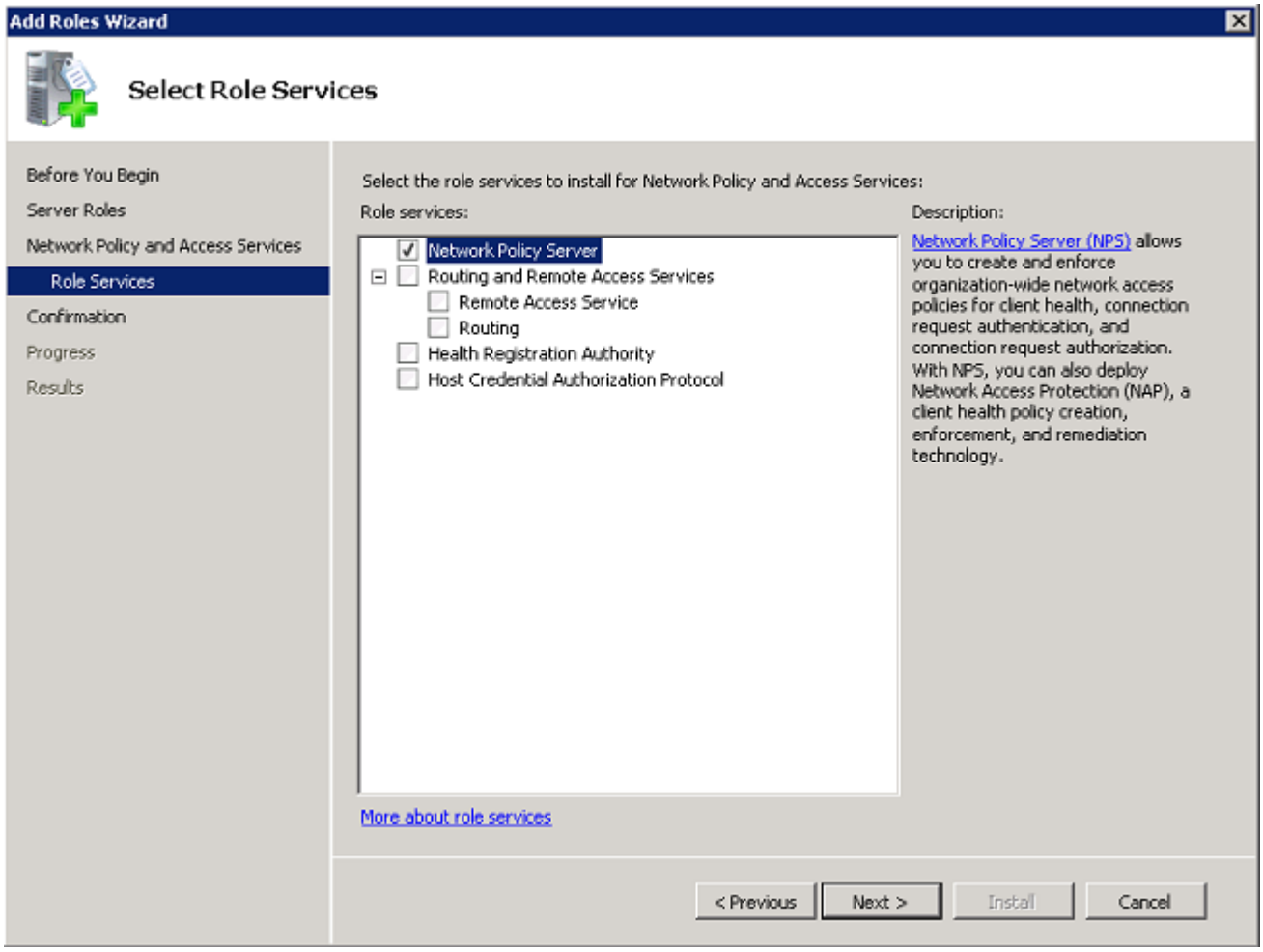
4. Selecteer de service Netwerkbeleid en toegangsservices en klik op Volgende.



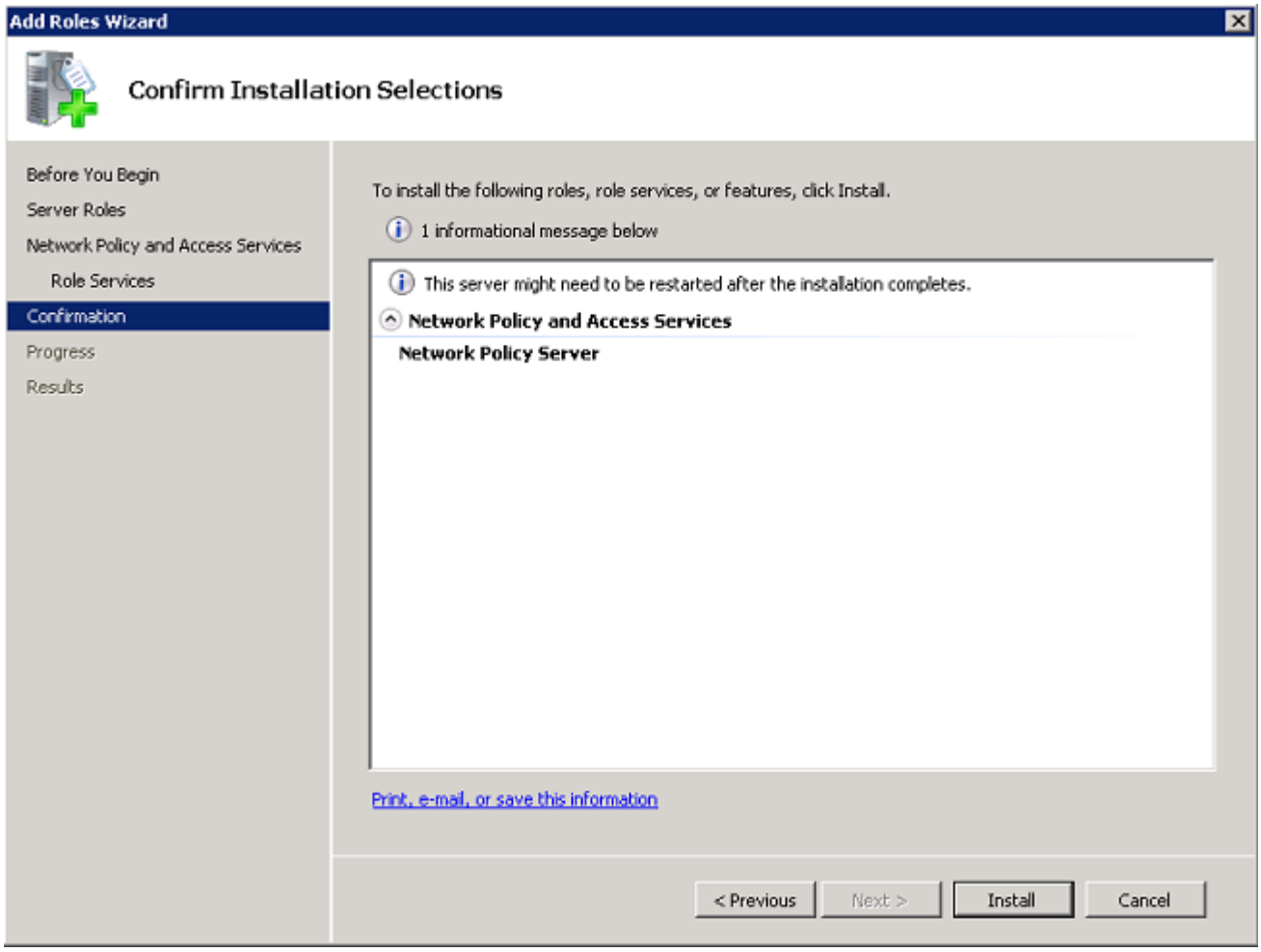
5. Bekijk de Inleiding tot netwerkbeleid en toegangsservices en klik op Volgende.



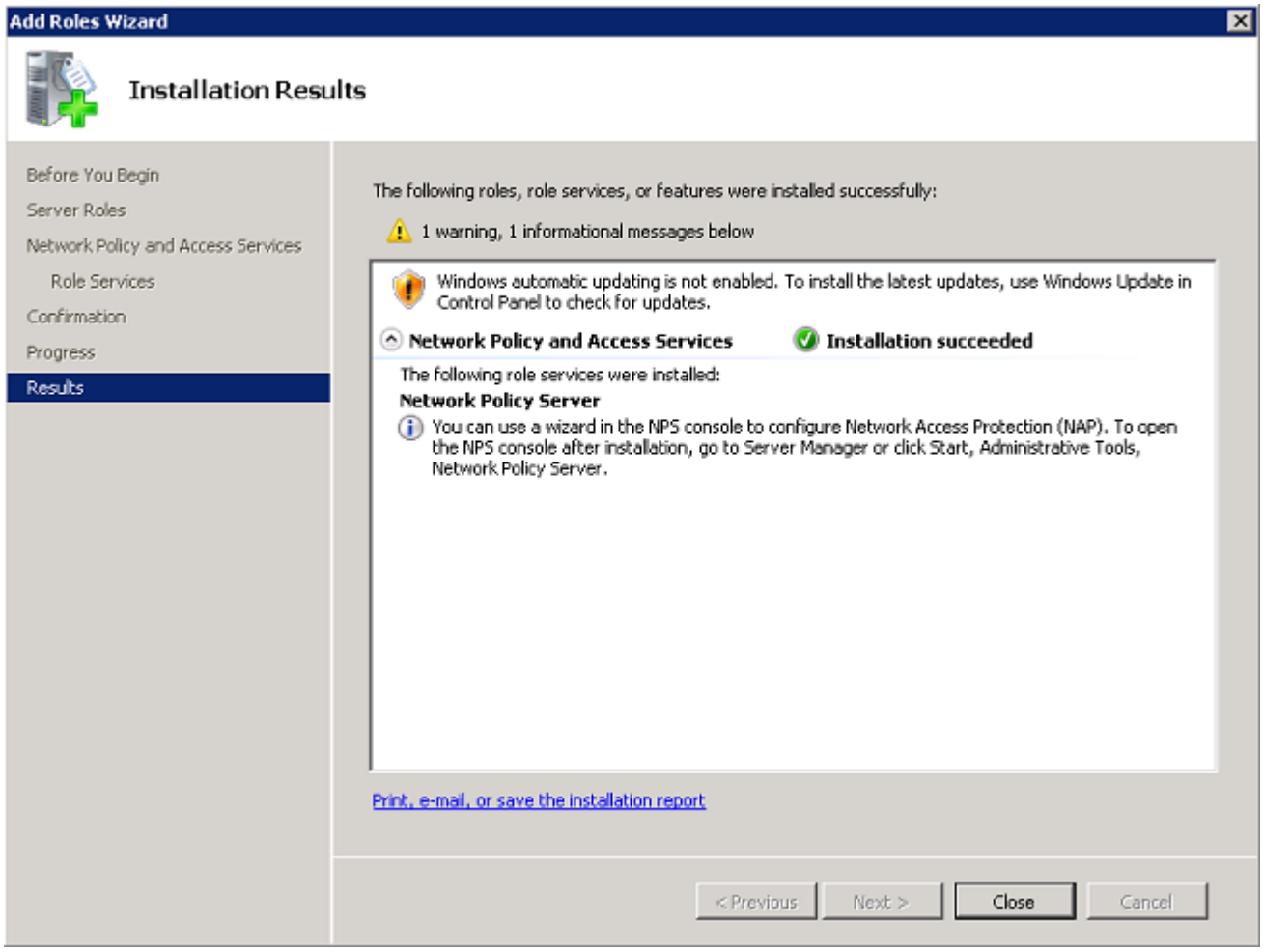
6. Selecteer Netwerkbeleidsserver en klik op Volgende.



7. Controleer de bevestiging en klik op Installeren.



Nadat de installatie is voltooid, wordt een scherm weergegeven dat vergelijkbaar is met dit scherm.

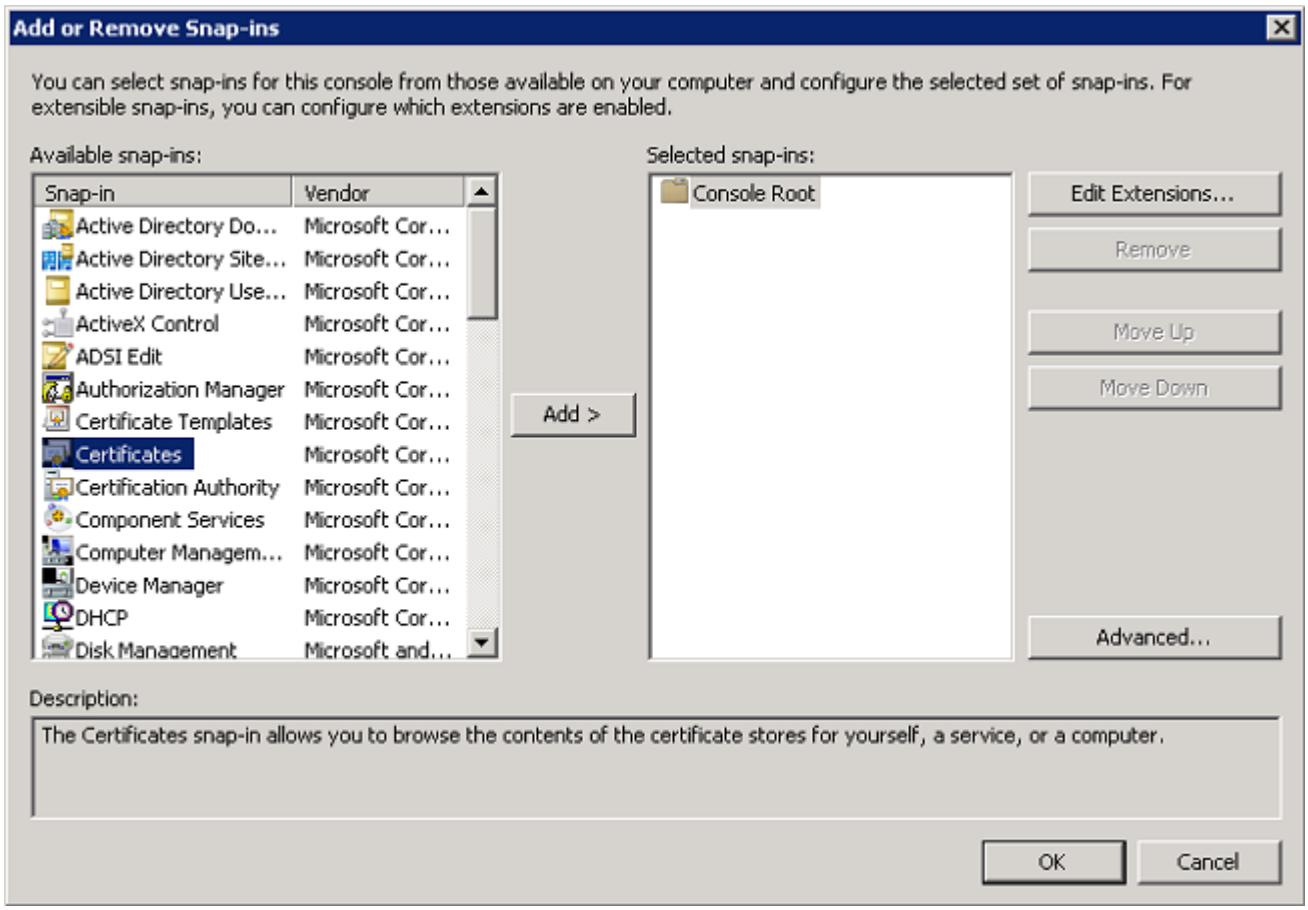


8. Klik op Close (Sluiten).

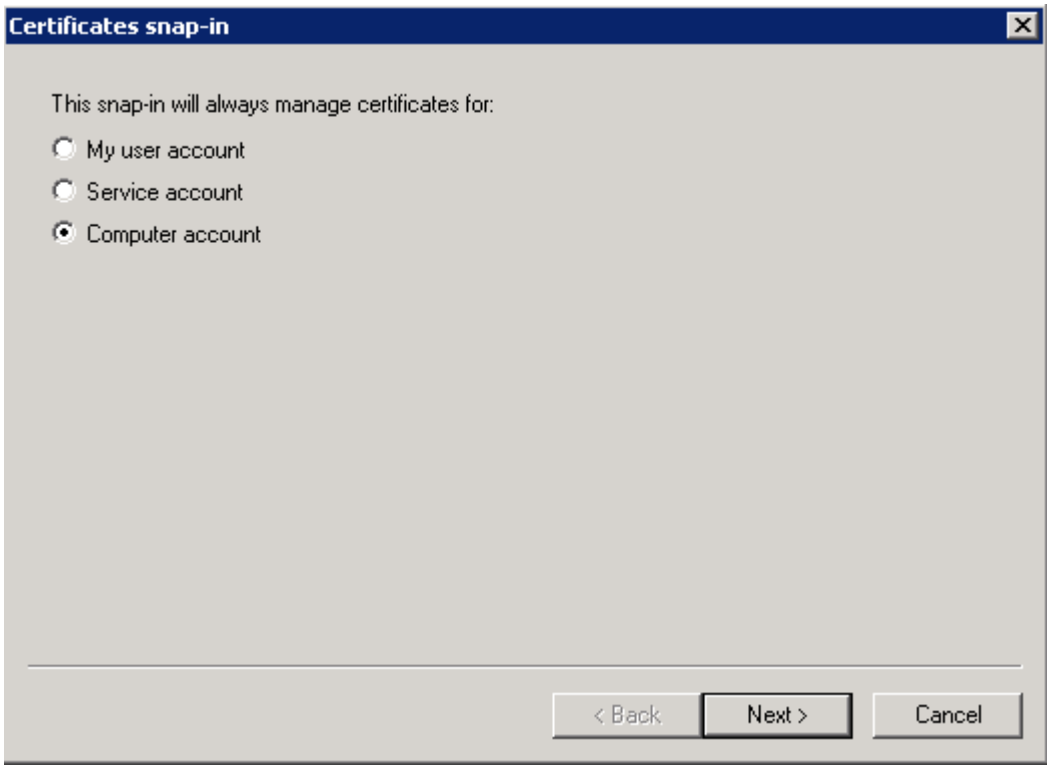
Een certificaat installeren

Voer de volgende stappen uit om het computercertificaat voor de NPS te installeren:

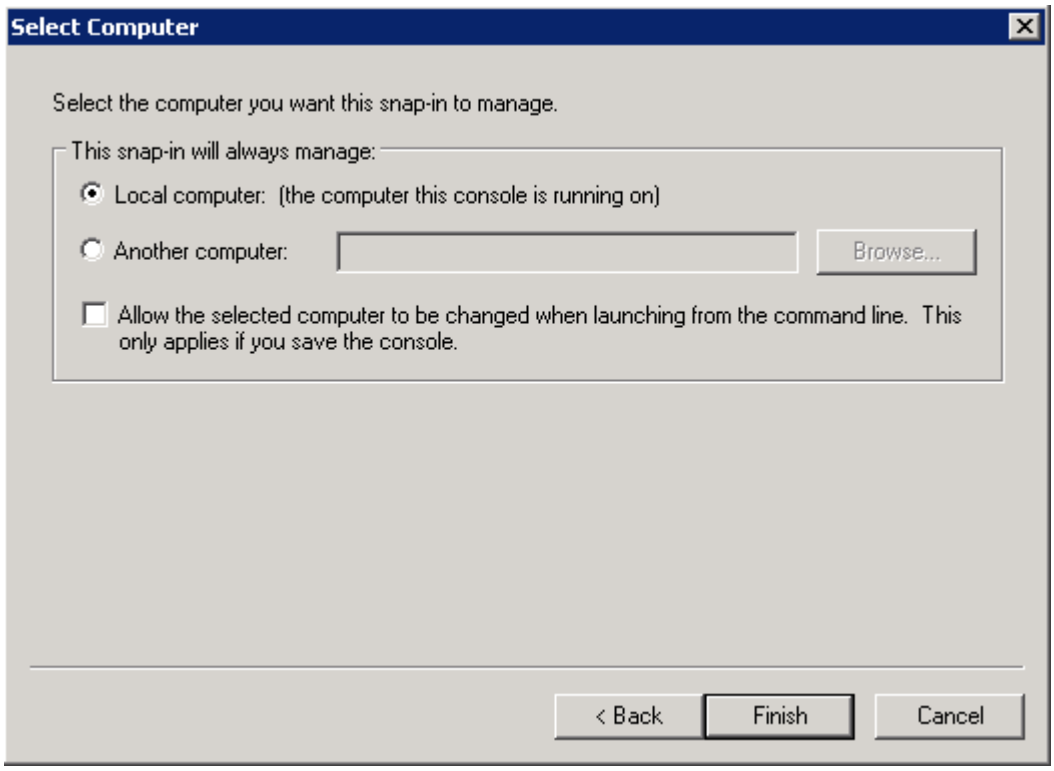
1. Klik op Start, voer mmc in en druk op Enter.
2. Klik op Bestand > Module toevoegen/verwijderen.
3. Kies Certificaten en klik op Toevoegen.



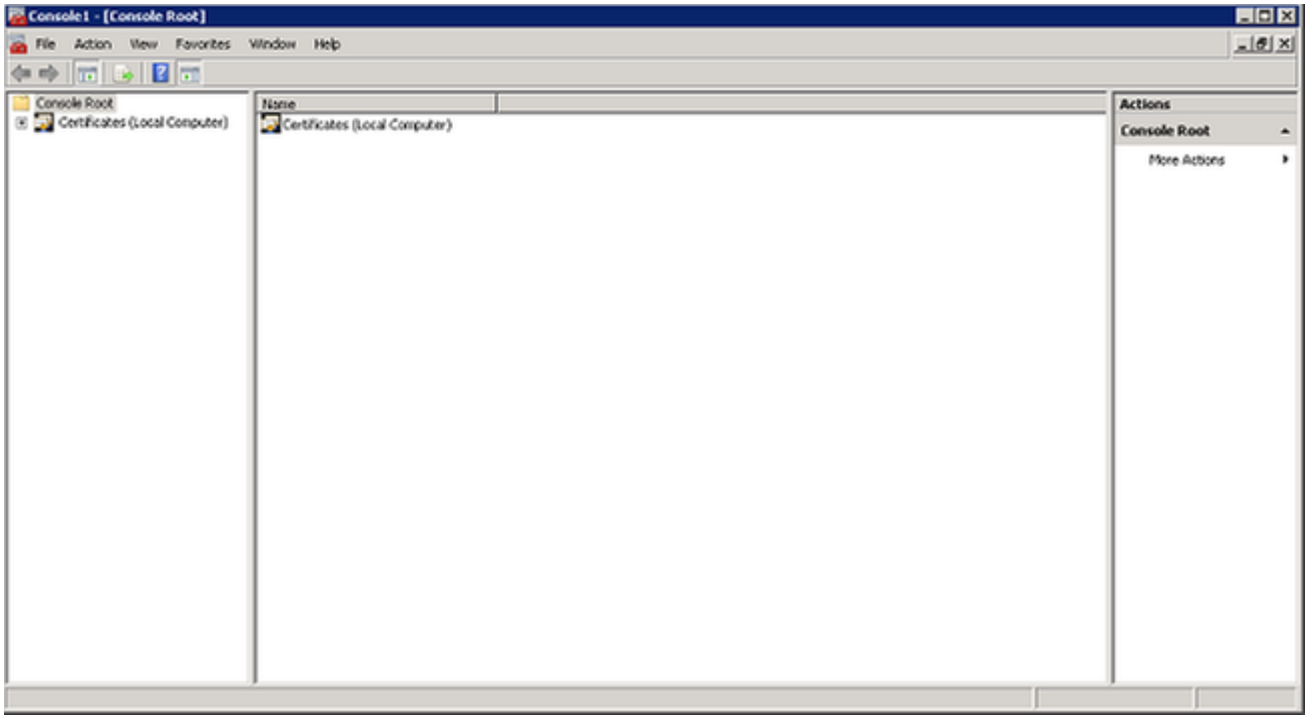
4. Kies Computeraccount en klik op Volgende.



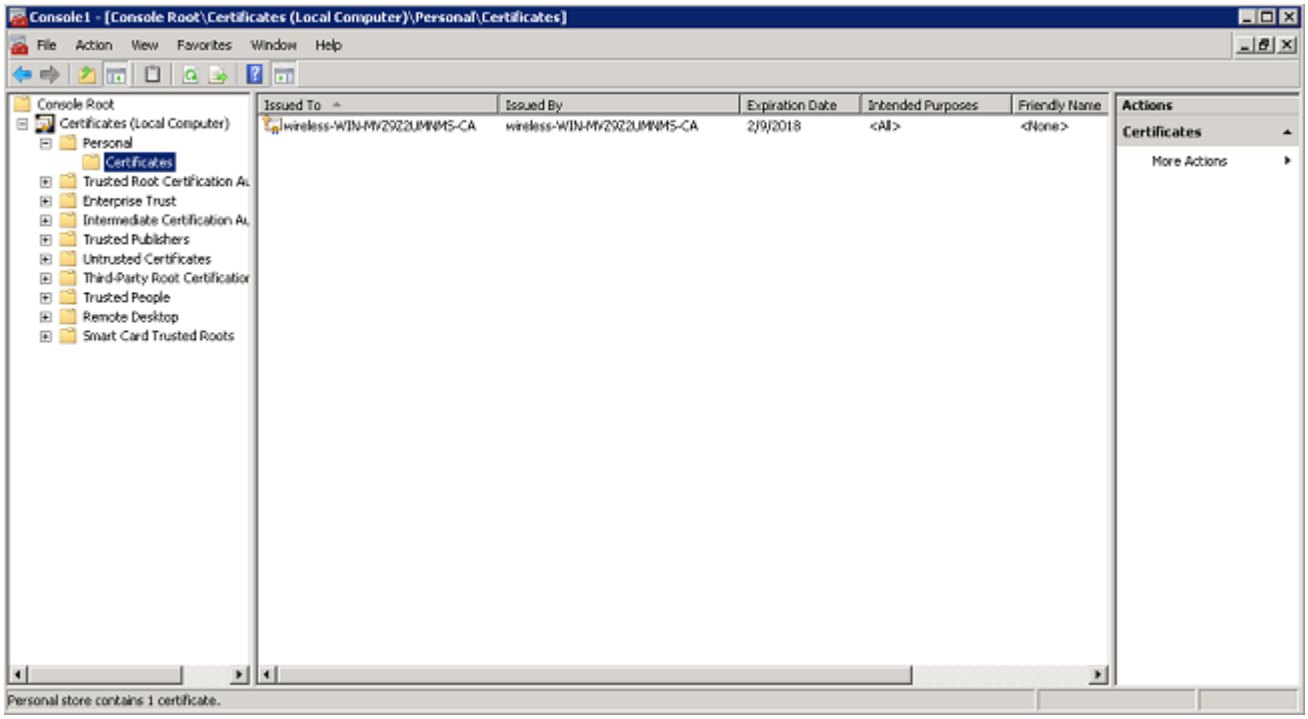
5. Selecteer Lokale computer en klik op Voltooien.



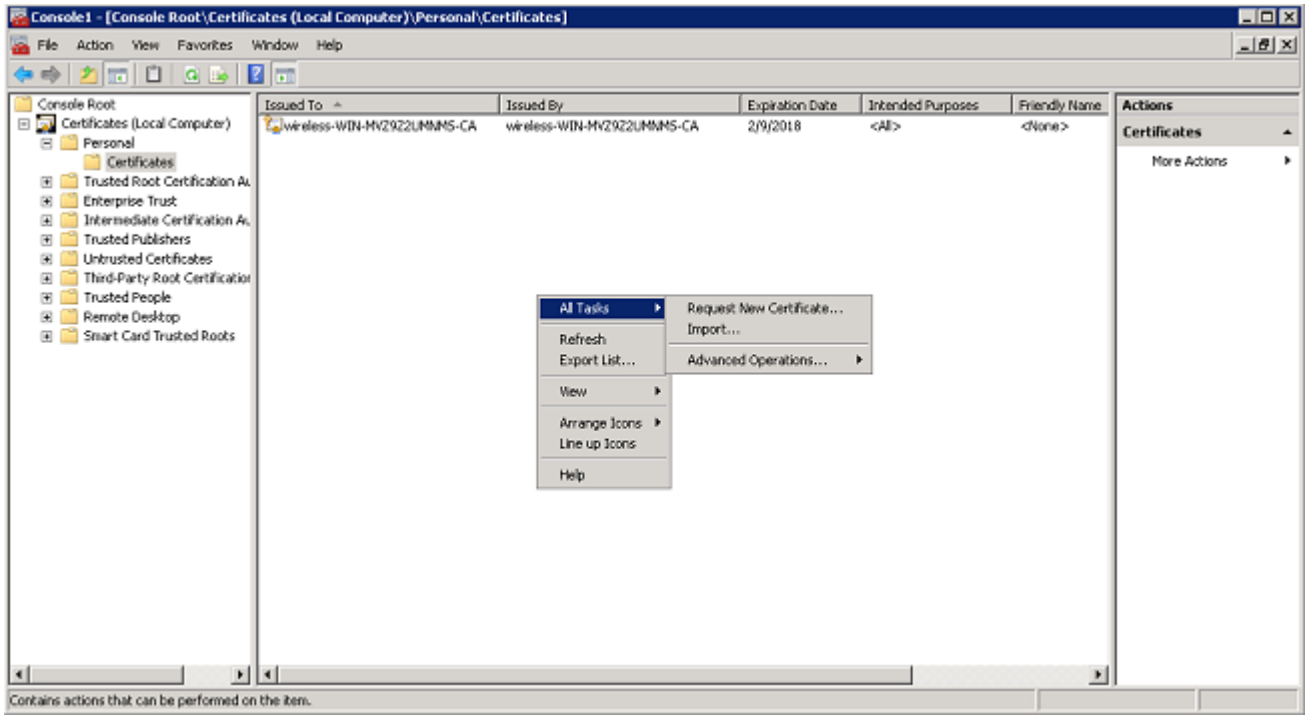
6. Klik op OK om terug te keren naar de Microsoft Management Console (MMC).



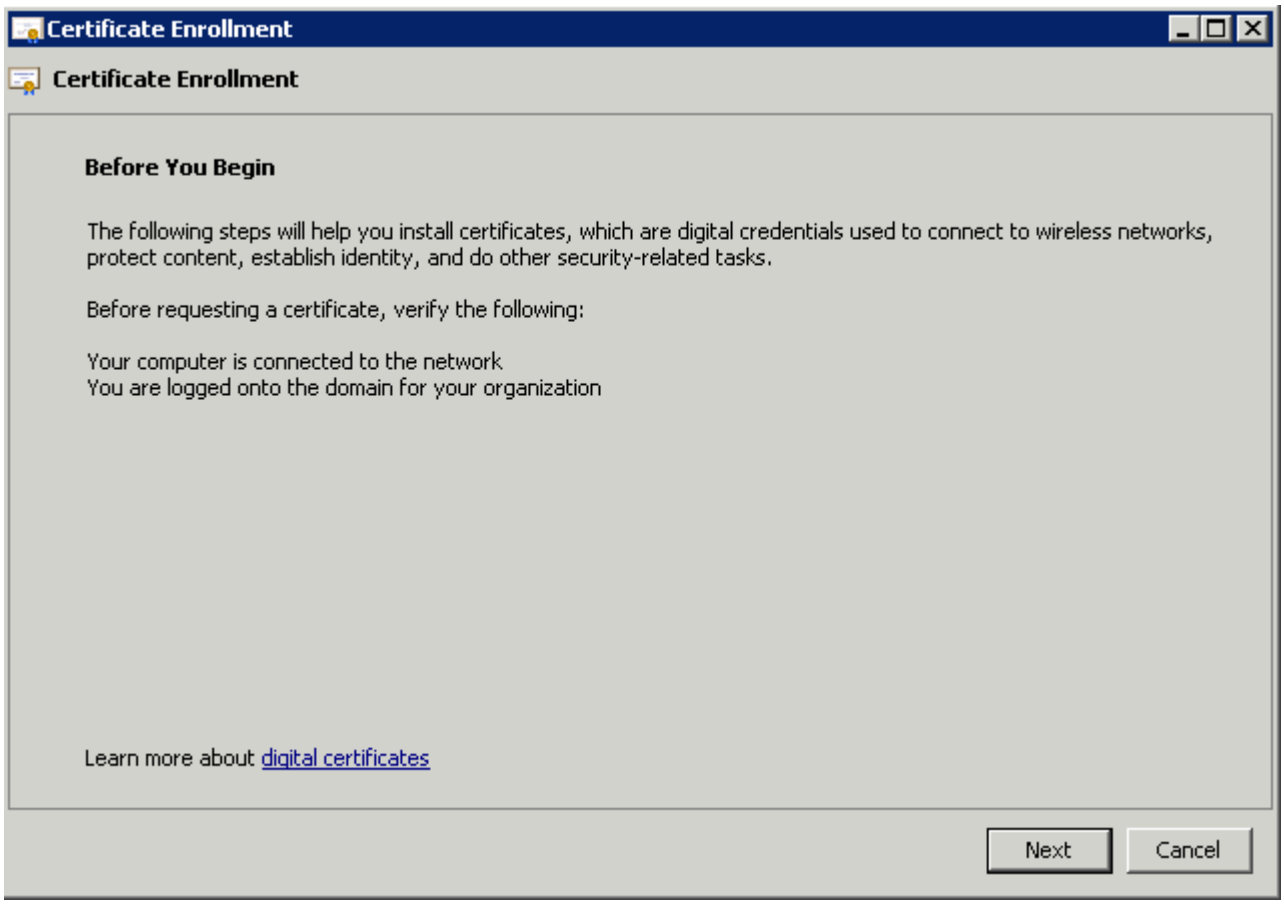
7. Vouw de mappen Certificaten (Lokale computer) en Persoonlijke gegevens uit en klik op Certificaten.



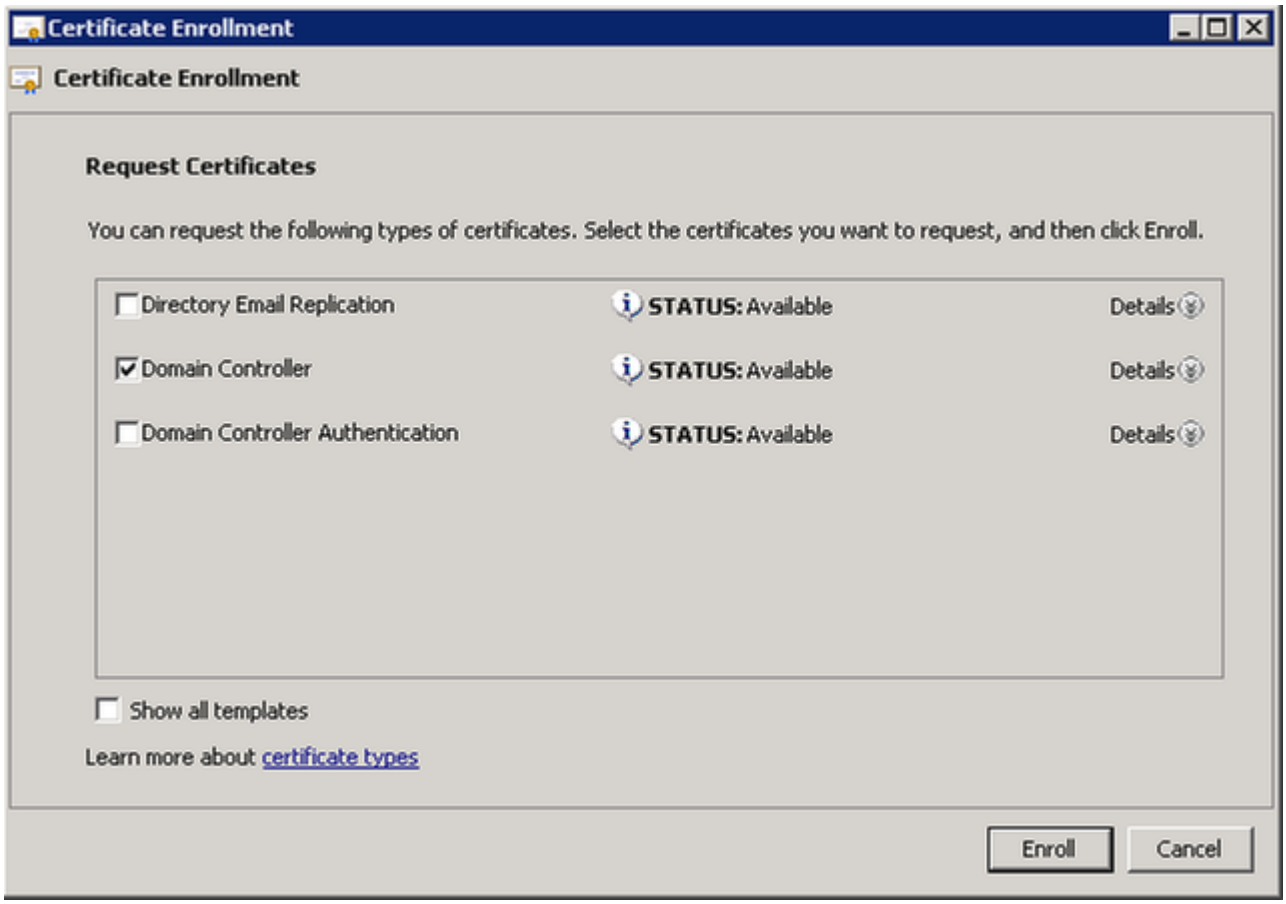
8. Klik met de rechtermuisknop in de witte ruimte onder het CA-certificaat en kies Alle taken > Nieuw certificaat aanvragen.



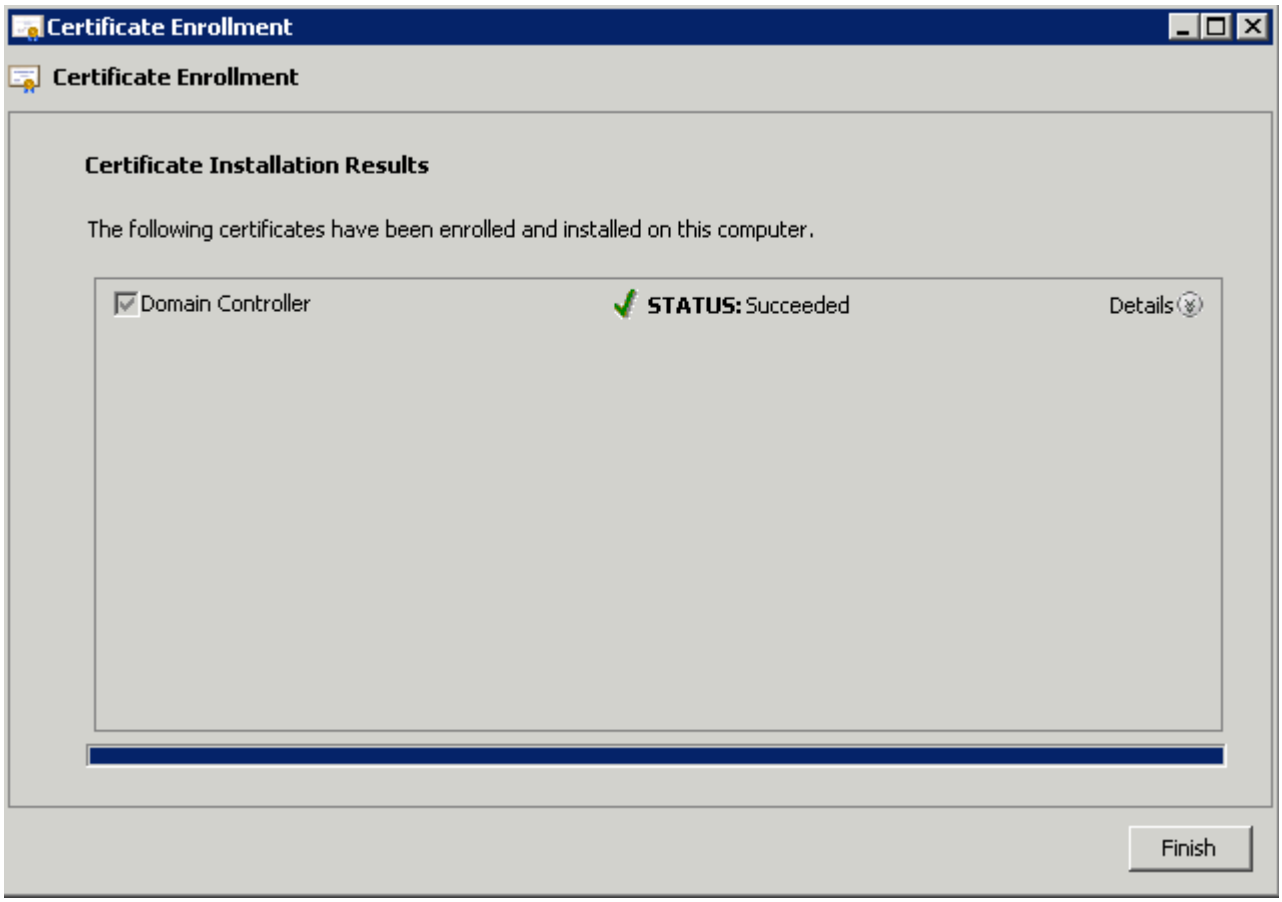
9. Klik op Next (Volgende).



10. Selecteer Domeincontroller en klik op Inschrijven.

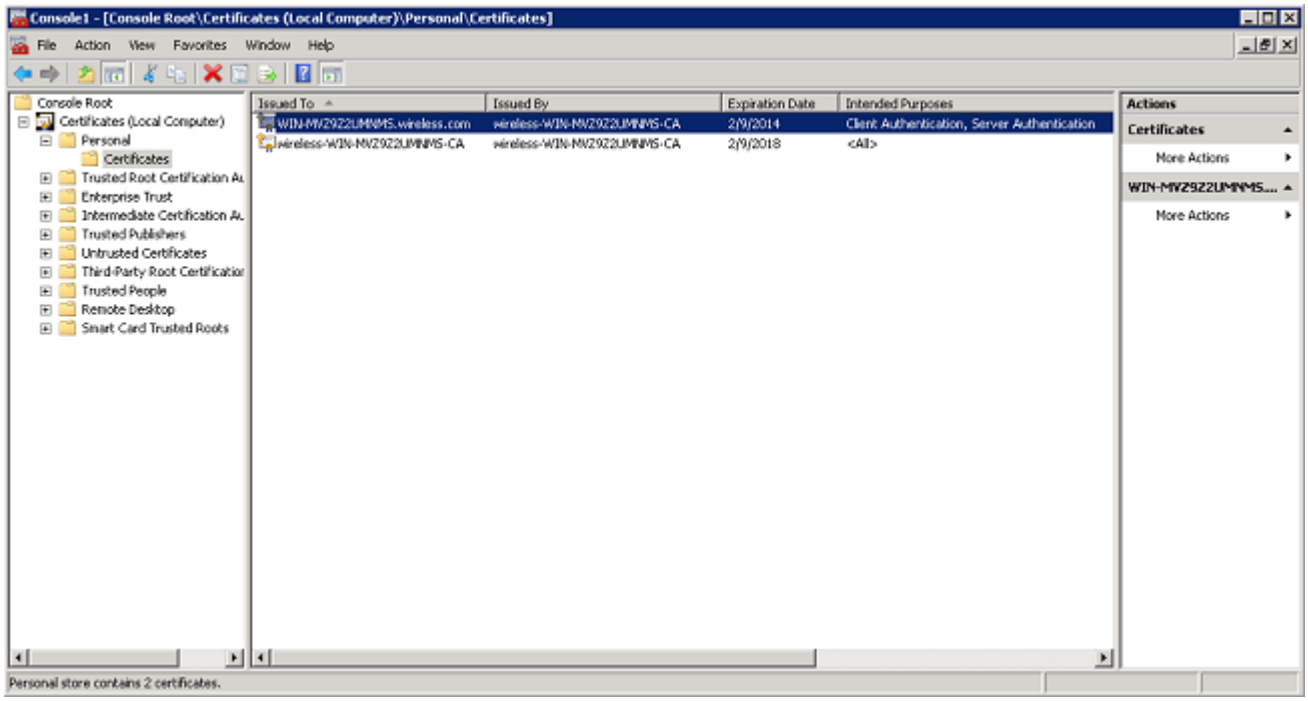


11. Klik op Voltooien zodra het certificaat is geïnstalleerd.



Het NPS-certificaat is nu geïnstalleerd.

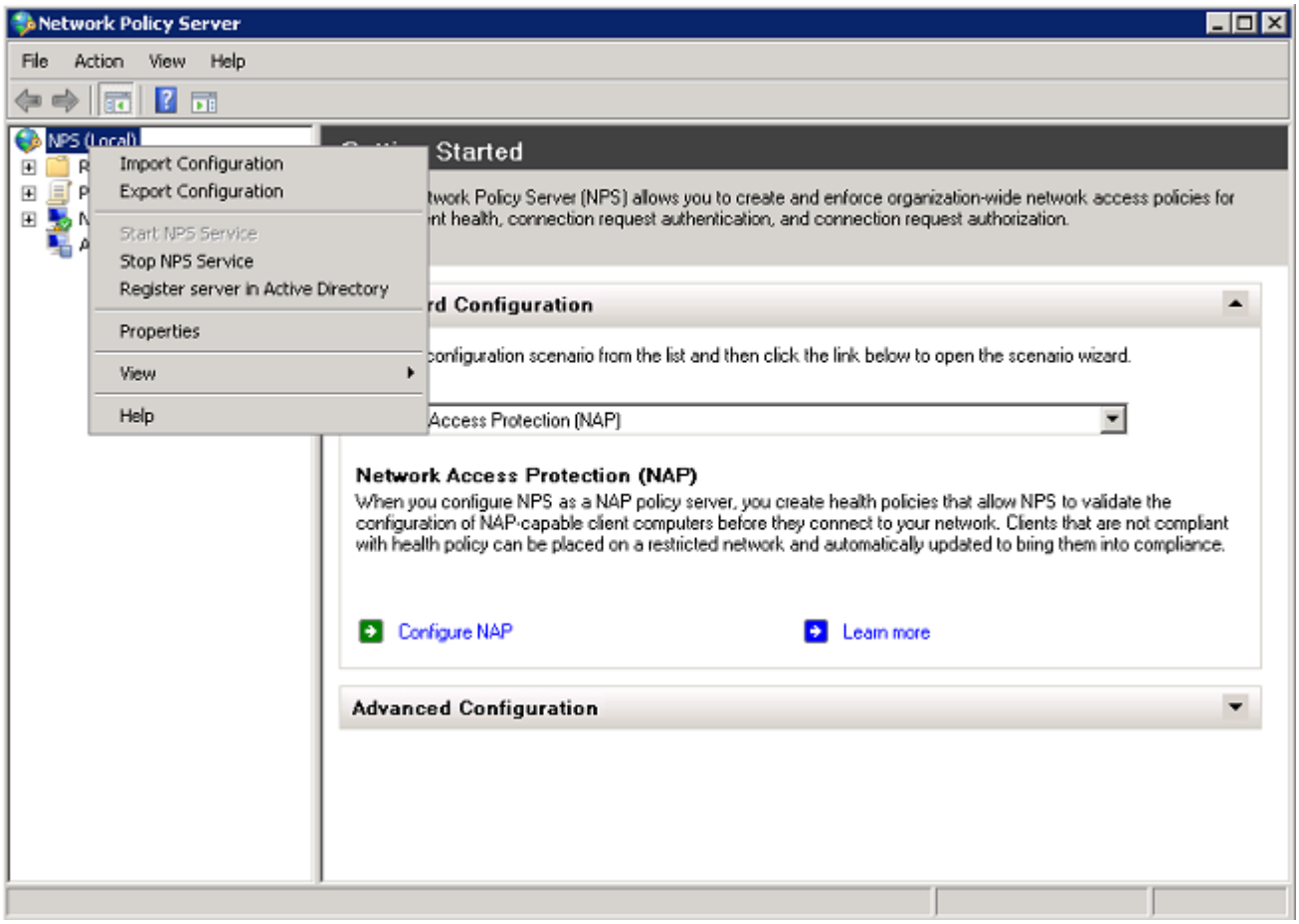
12. Zorg ervoor dat het beoogde doel van het certificaat clientverificatie, serververificatie leest.



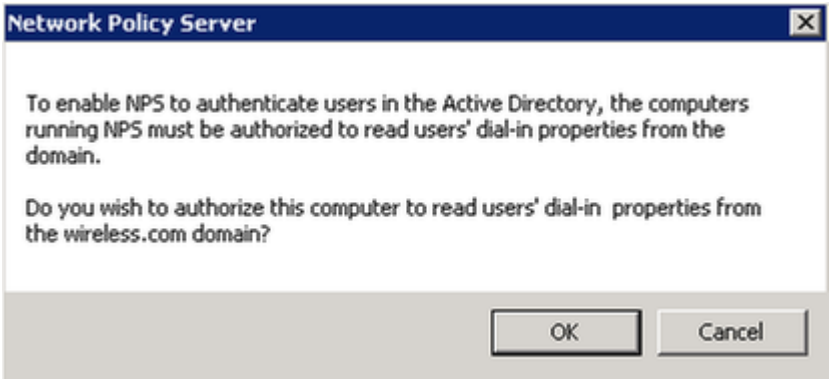
De netwerkbeleidsserverservice configureren voor PEAP-MS-CHAP v2-verificatie

Voer de volgende stappen uit om de NPS voor verificatie te configureren:

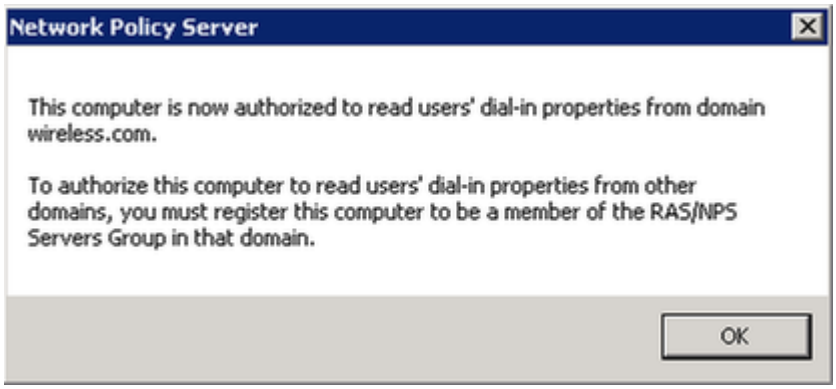
1. Klik op Start > Systeembeheer> Netwerkbeleidsserver.
2. Klik met de rechtermuisknop op NPS (Lokaal) en kies Server registreren in Active Directory.



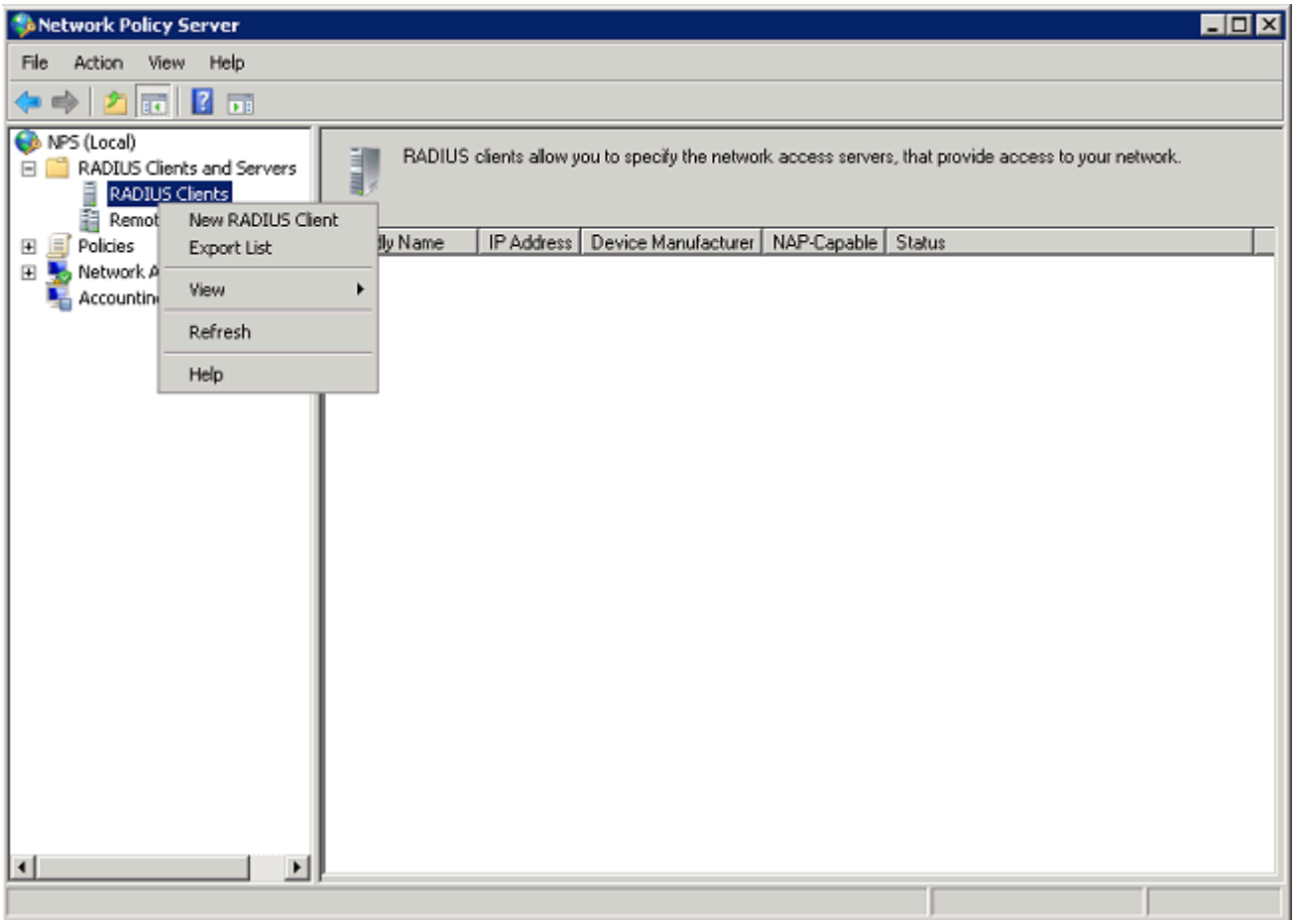
3. Klik op OK.



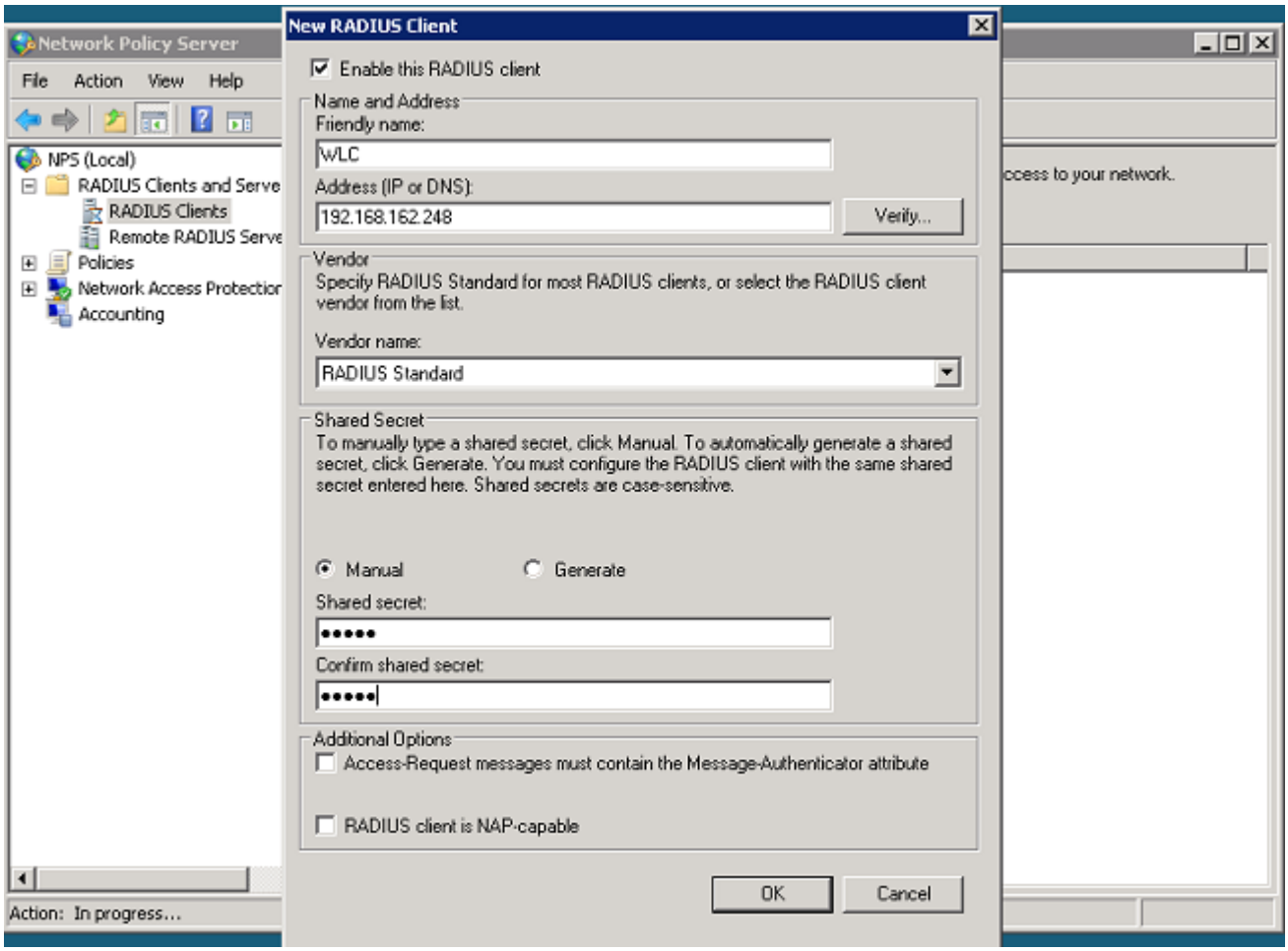
4. Klik op OK.



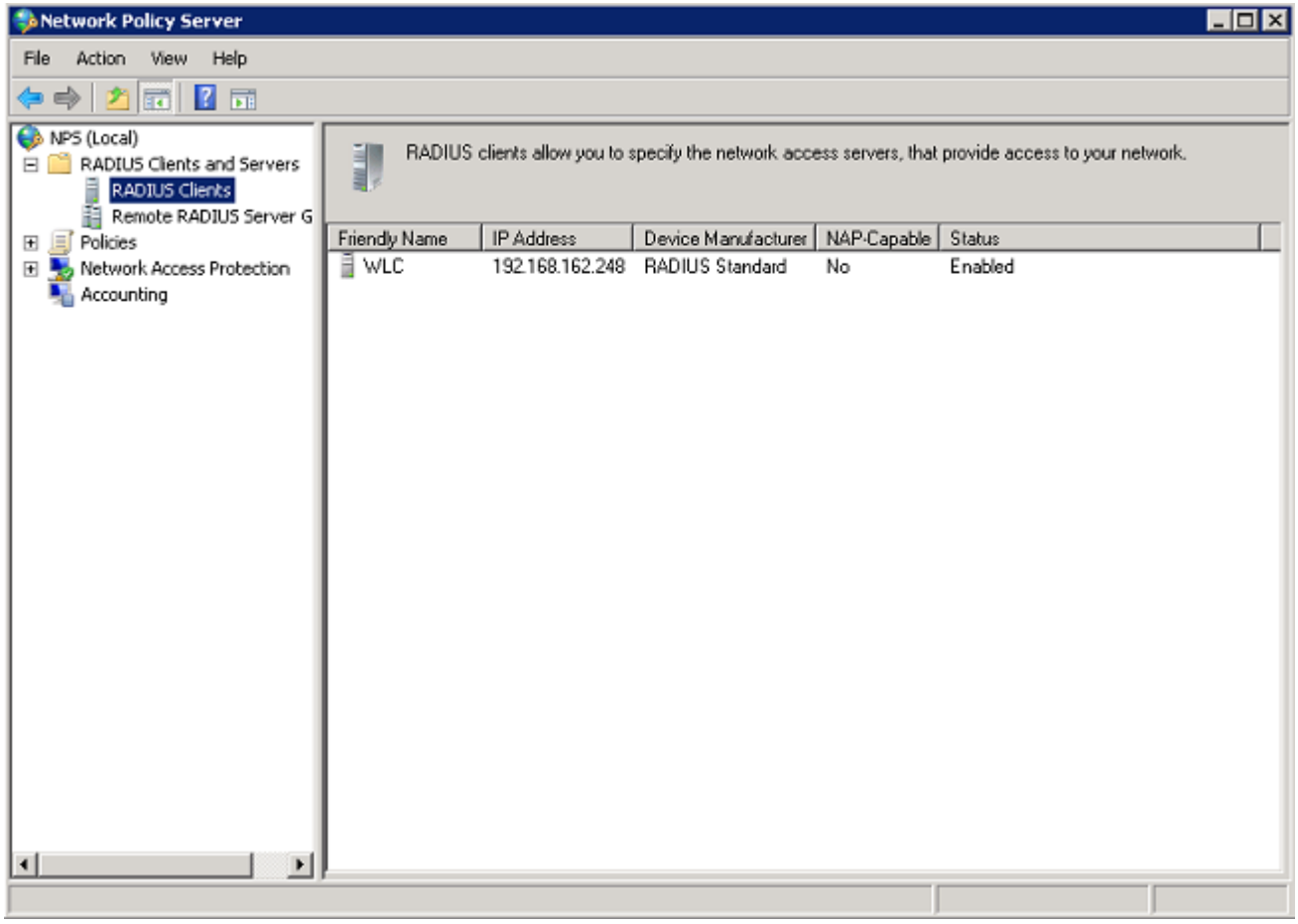
5. Voeg de draadloze LAN-controller toe als een verificatie-, autorisatie- en boekhoudclient (AAA) op de NPS.
6. RADIUS-clients en -servers uitbreiden. Klik met de rechtermuisknop op RADIUS-clients en kies Nieuwe RADIUS-client.



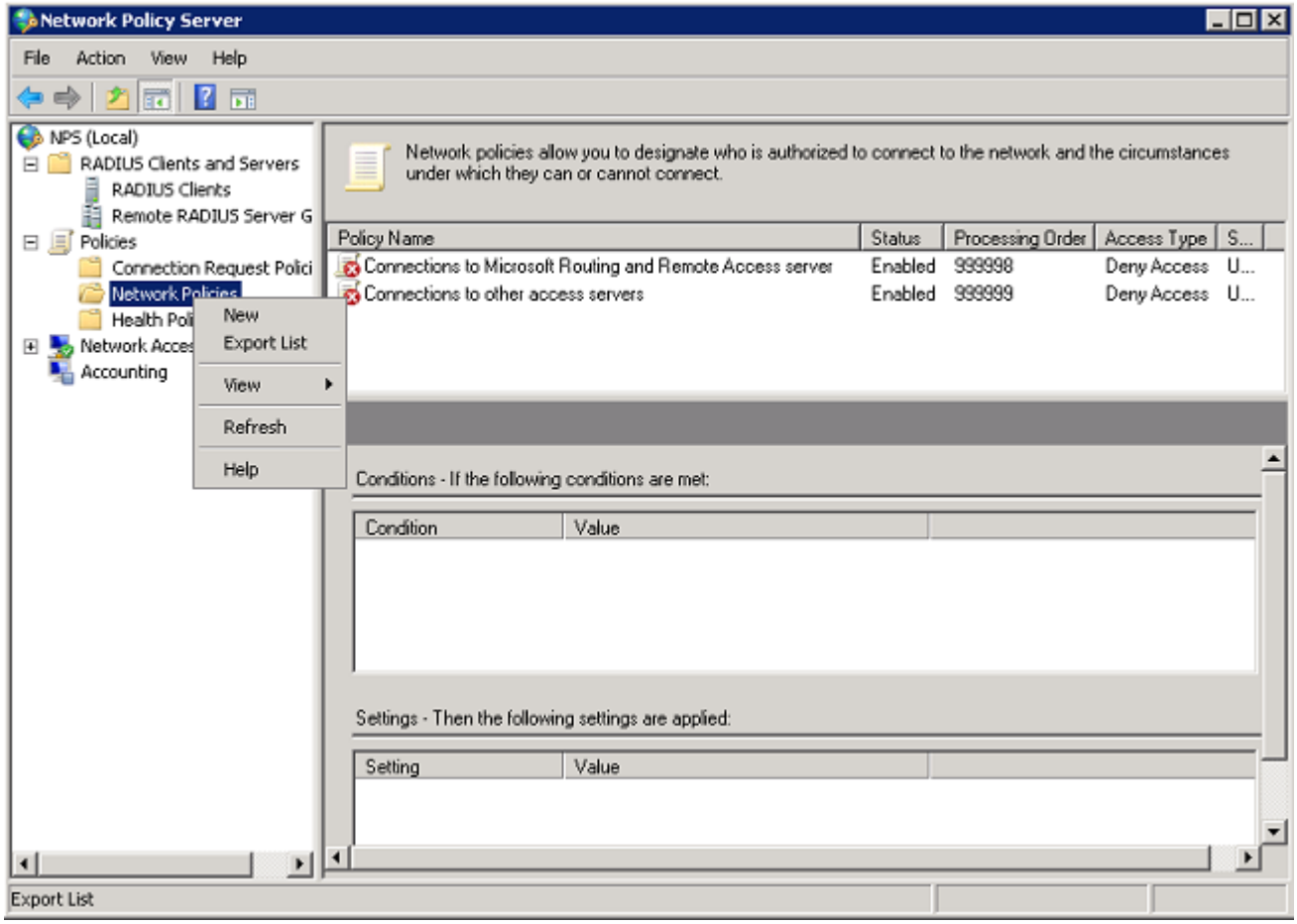
7. Voer een vriendelijke naam (WLC in dit voorbeeld), het IP-adres van het beheer van de WLC (192.168.162.248 in dit voorbeeld) en een gedeeld geheim in. Hetzelfde gedeelde geheim wordt gebruikt om de WLC te configureren.



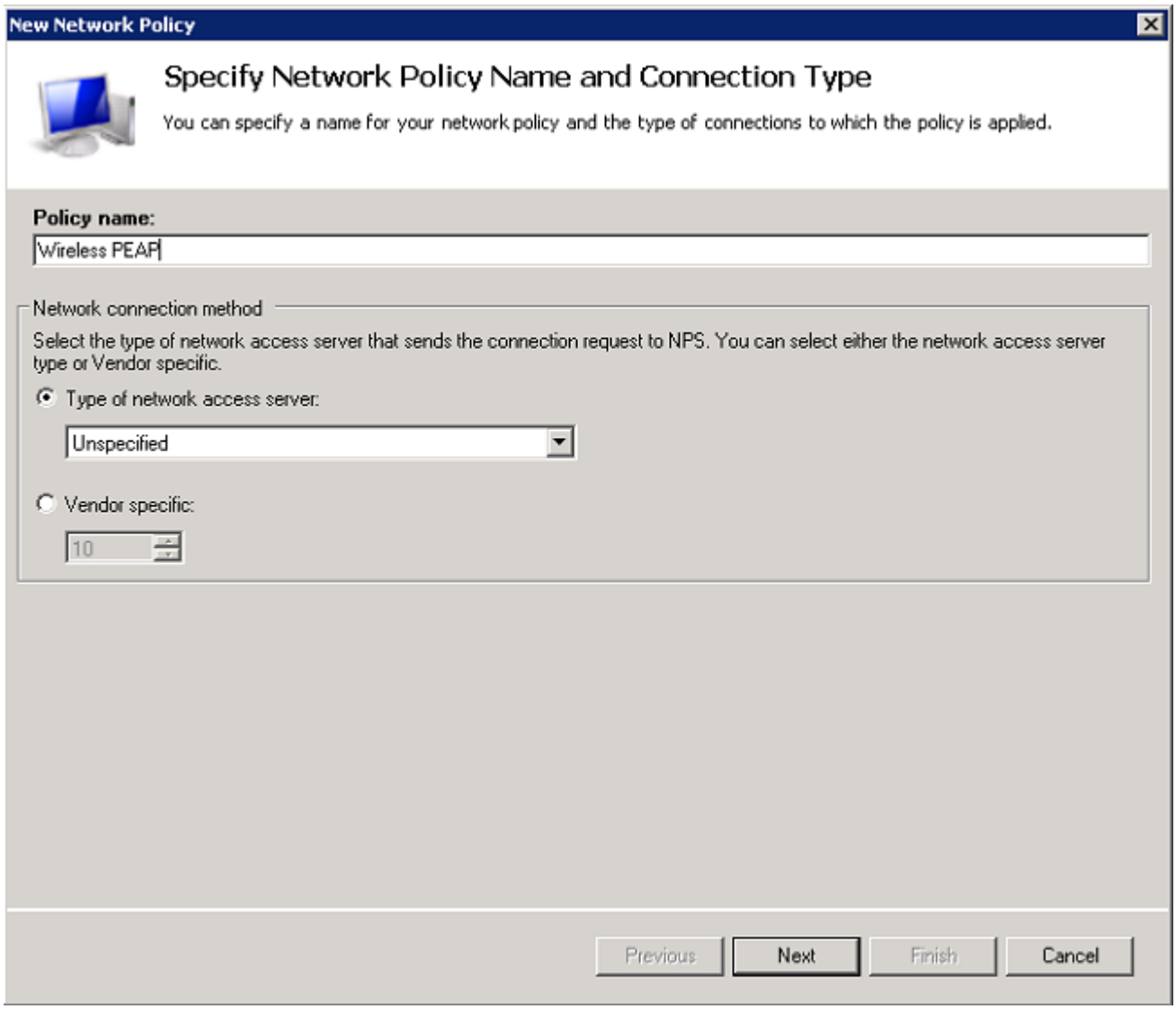
8. Klik op OK om terug te keren naar het vorige scherm.



9. Maak een nieuw netwerkbeleid voor draadloze gebruikers. Vouw Beleid uit, klik met de rechtermuisknop op Netwerkbeleid en kies Nieuw.

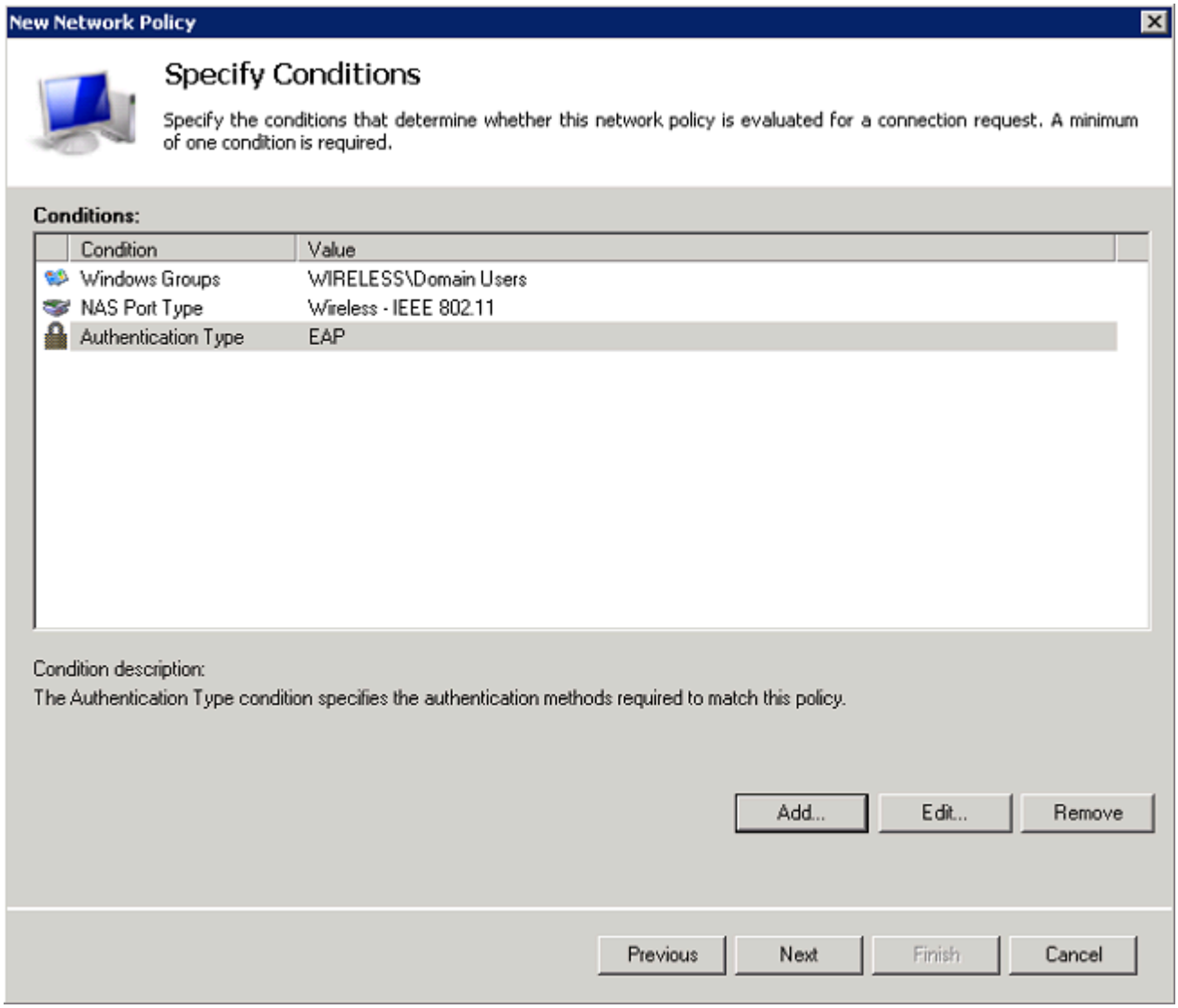


10. Voer een beleidsnaam in voor deze regel (Wireless PEAP, in dit voorbeeld) en klik op Volgende.

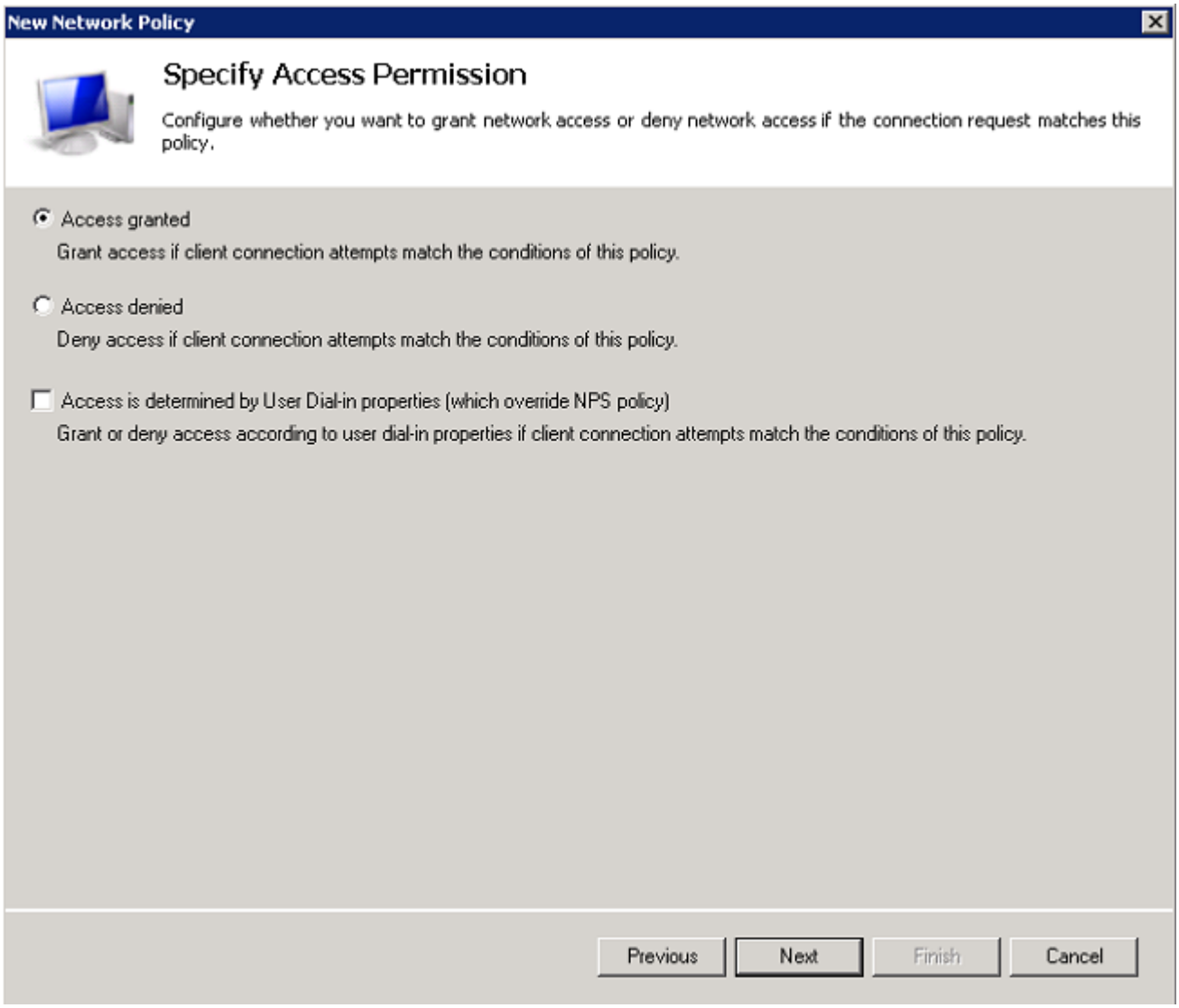


11. Als u met dit beleid alleen gebruikers van draadloze domeinen wilt toestaan, voegt u deze drie voorwaarden toe en klikt u op Volgende:

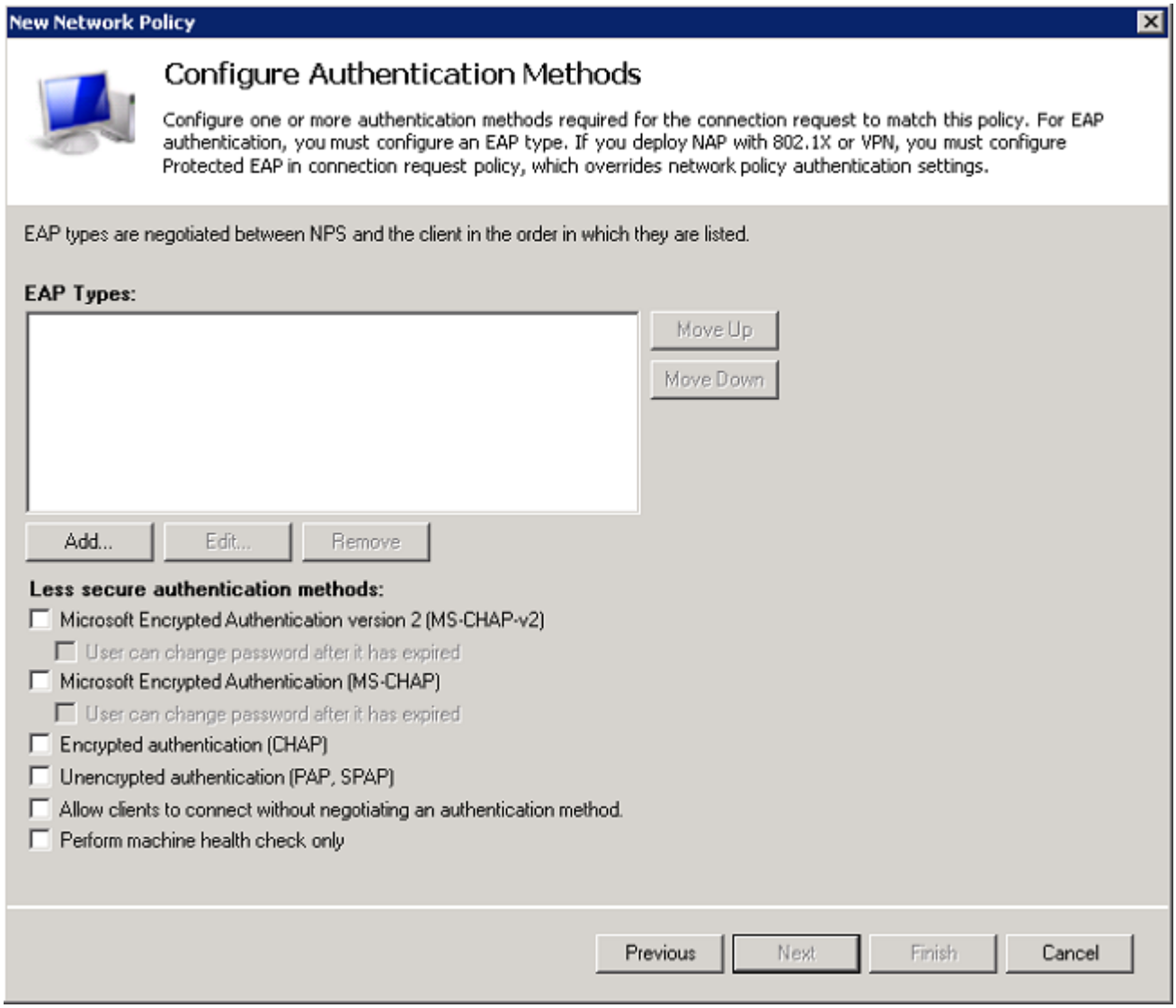
    - Windows-groepen - Domeingebruikers
    - Type NAS-poort - draadloos - IEEE 802.11
    - Verificatietype - EAP



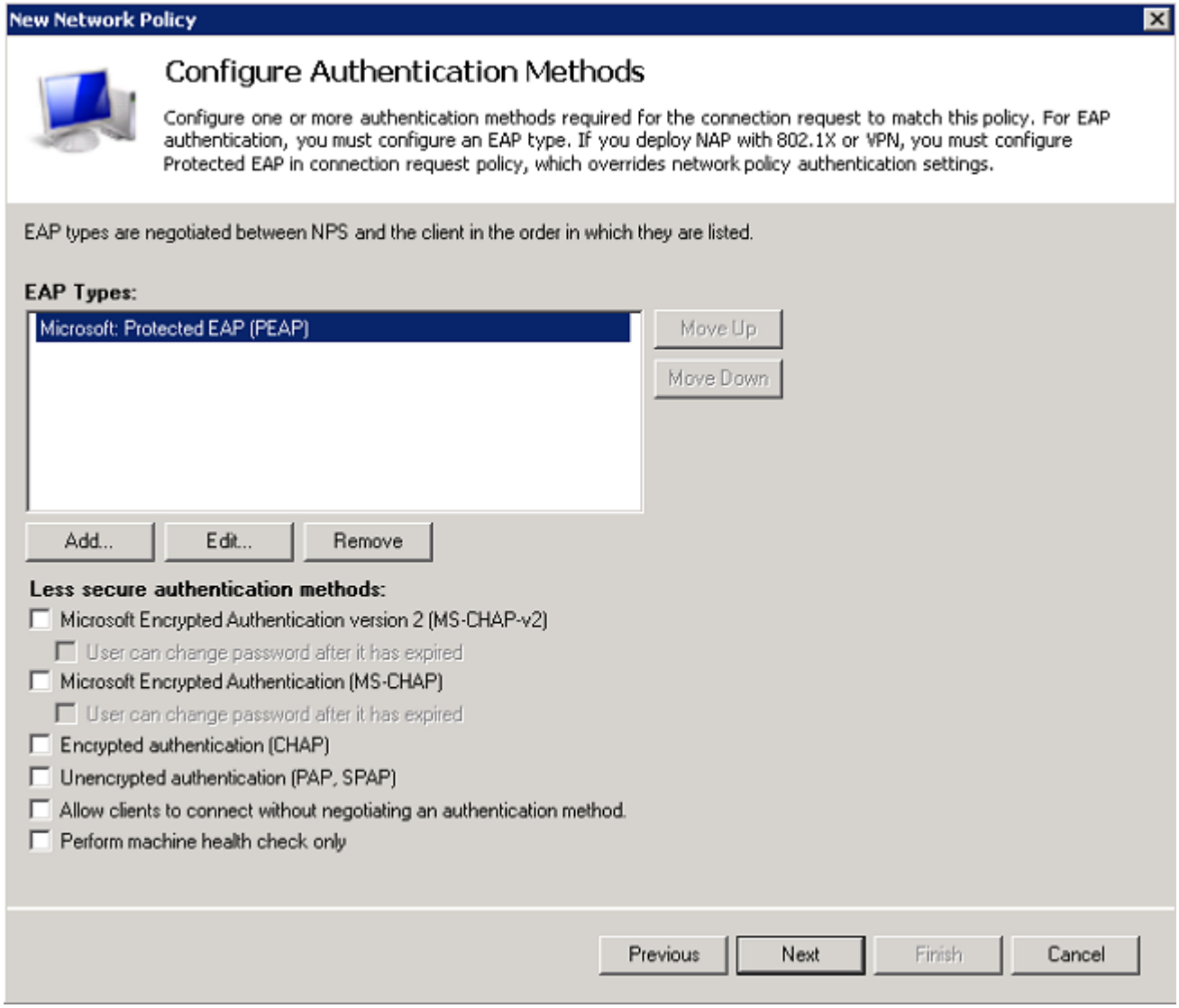
12. Klik op Toegang verleend om verbindingspogingen toe te staan die overeenkomen met dit beleid en klik op Volgende.



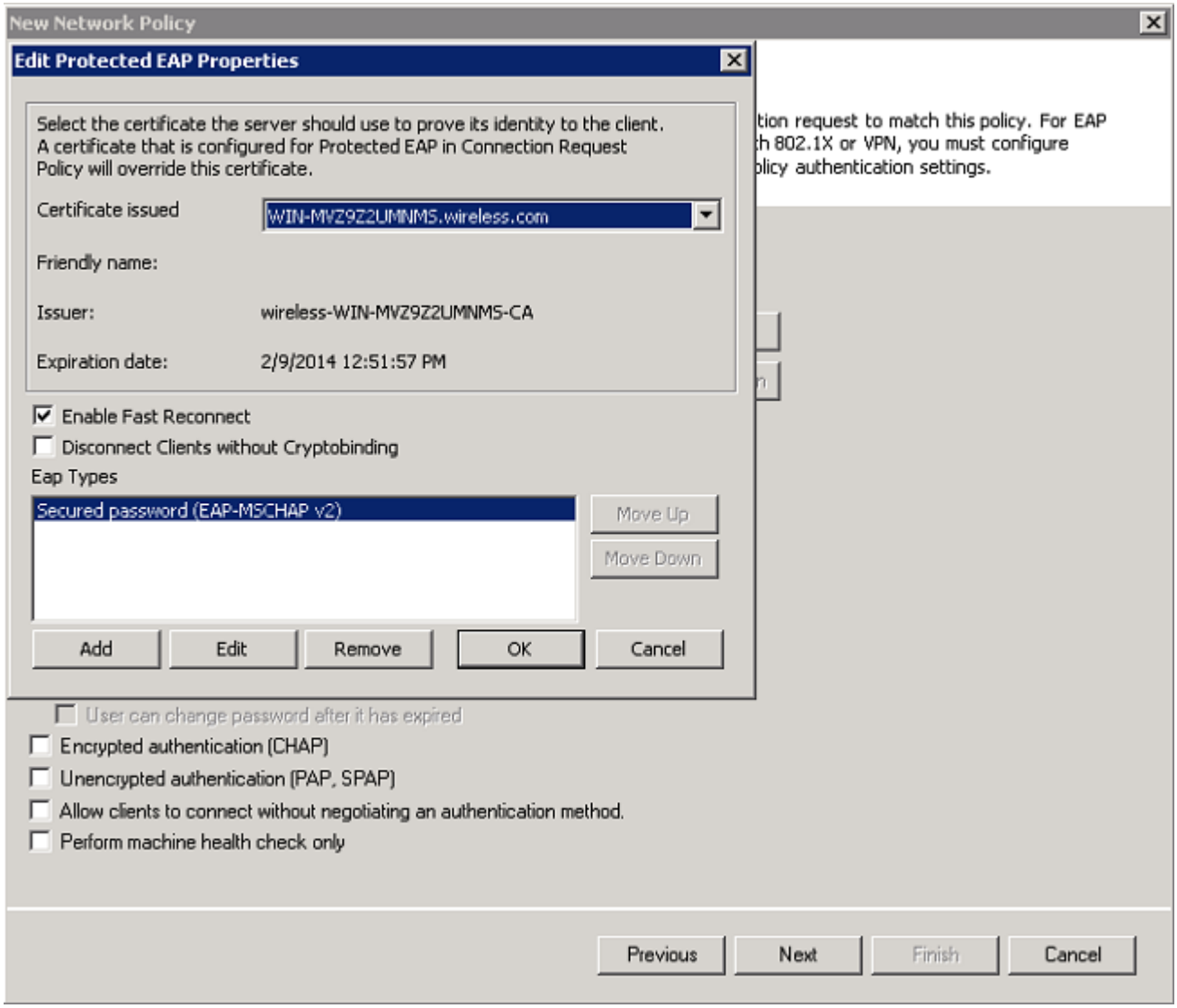
13. Schakel alle verificatiemethoden uit onder Minder veilige verificatiemethoden.



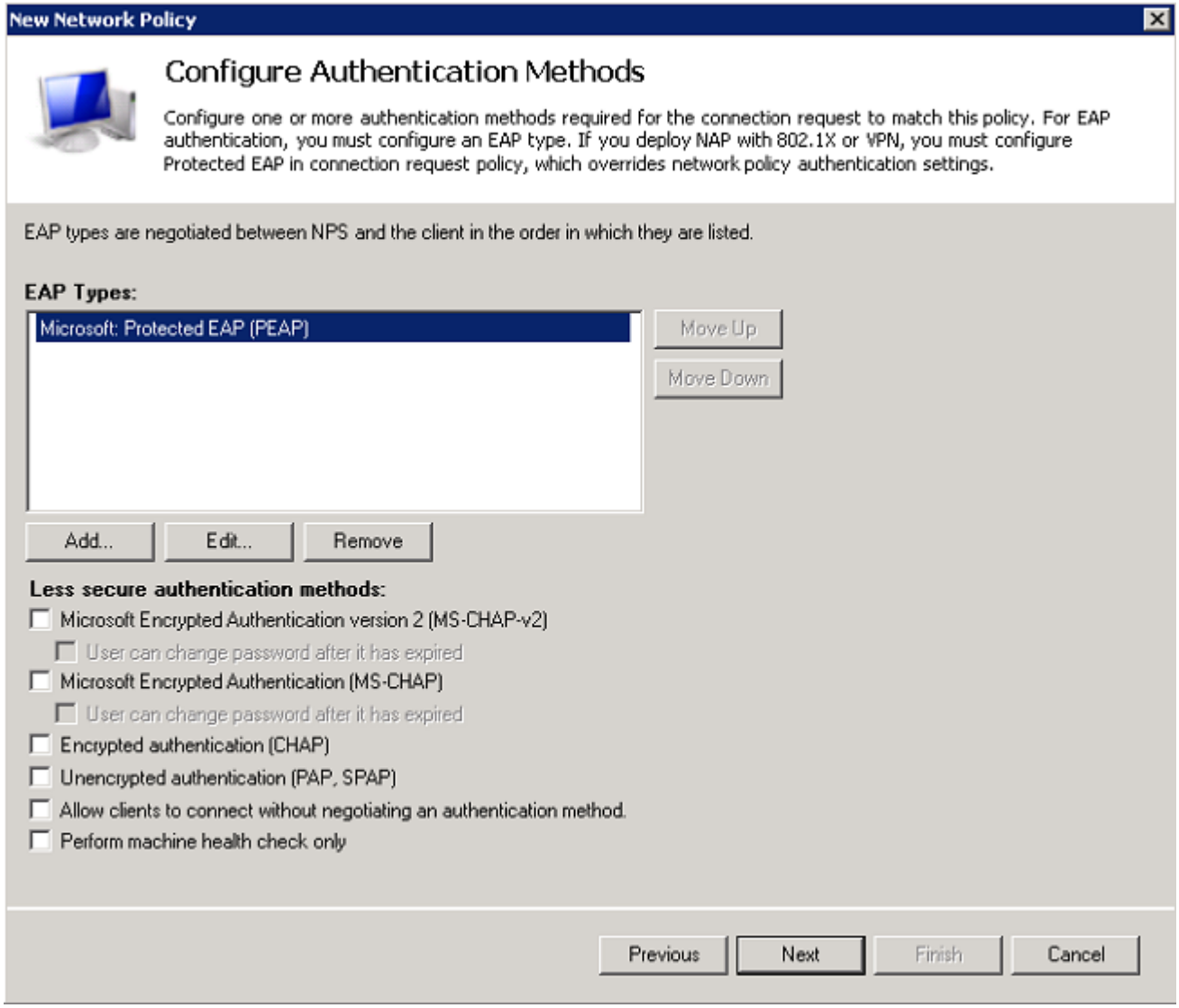
14. Klik op Toevoegen, selecteer PEAP en klik op OK om PEAP in te schakelen.



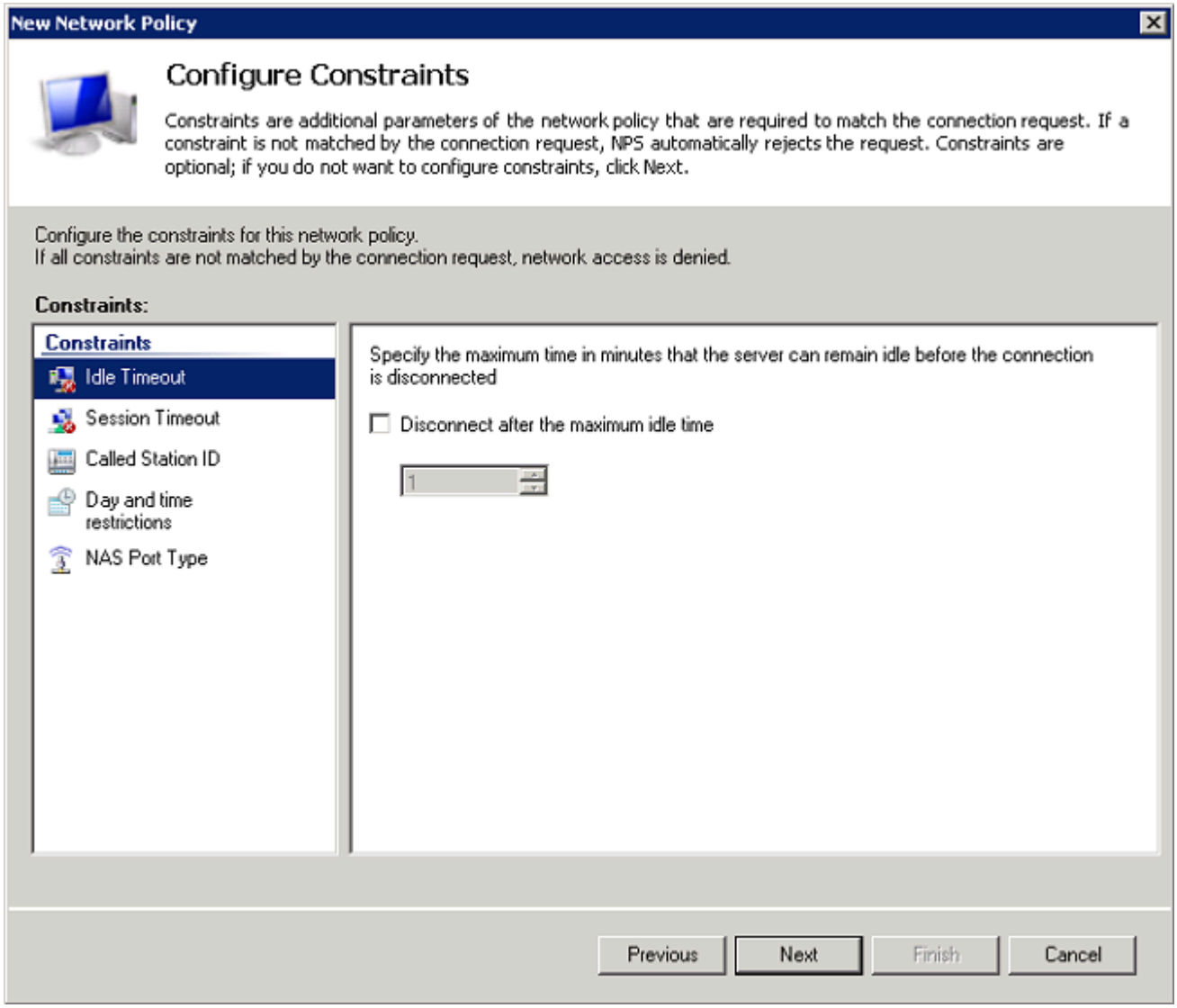
15. Selecteer Microsoft: Protected EAP (PEAP) en klik op Bewerken. Controleer of het eerder gemaakte domeincontrollercertificaat is geselecteerd in de vervolgkeuzelijst Certificaat verleend en klik op OK.



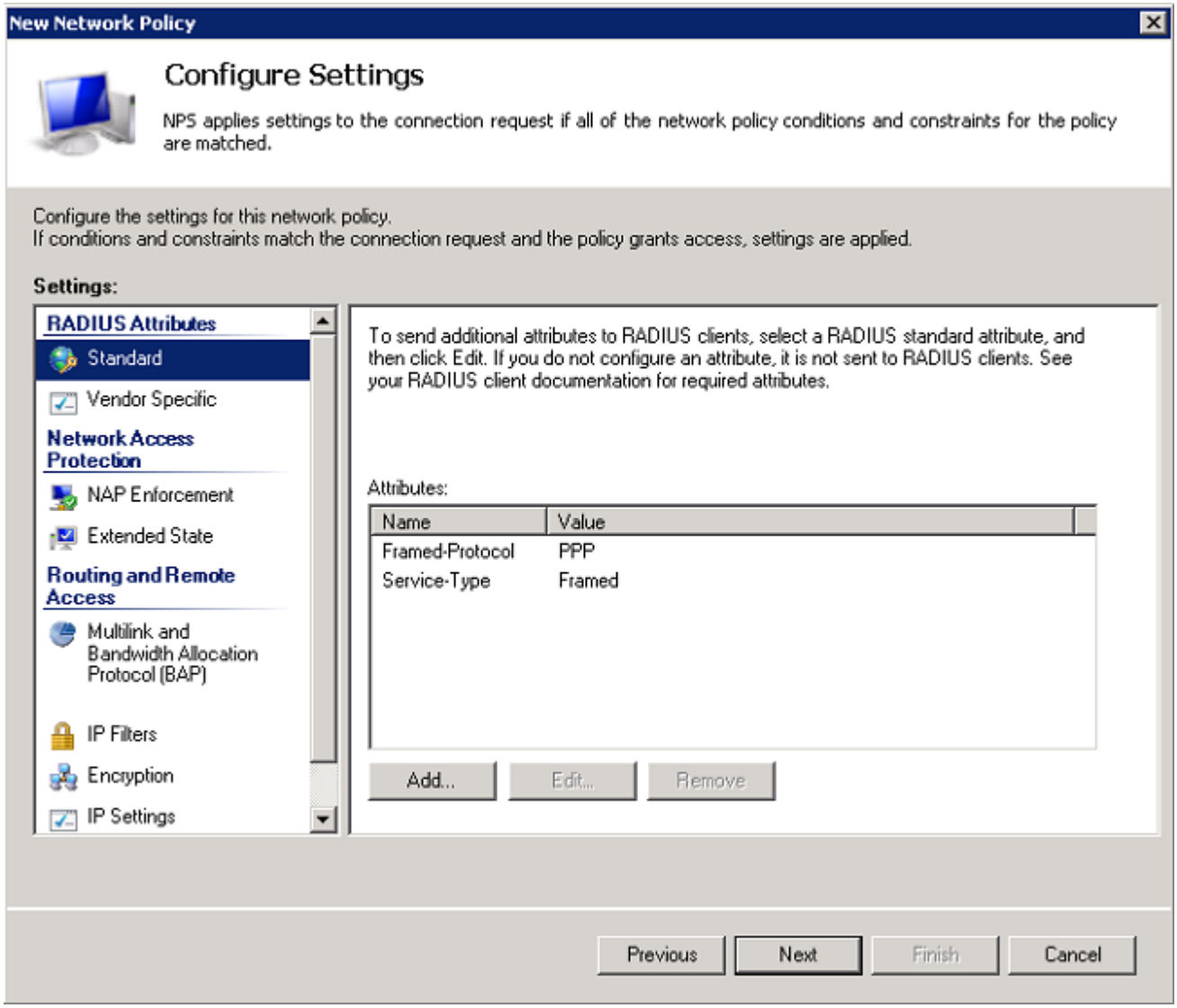
16. Klik op Next (Volgende).



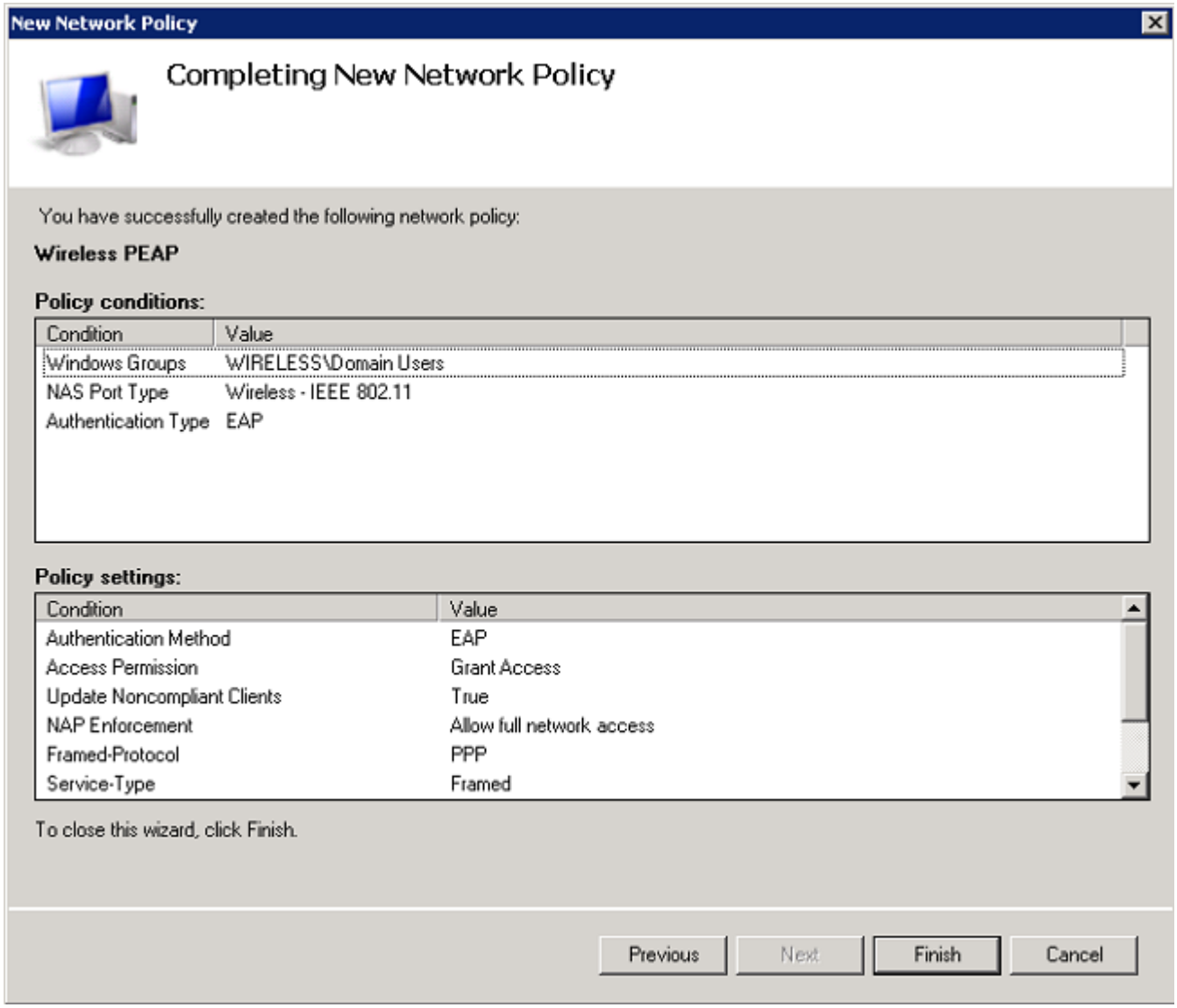
17. Klik op Next (Volgende).



18. Klik op Next (Volgende).



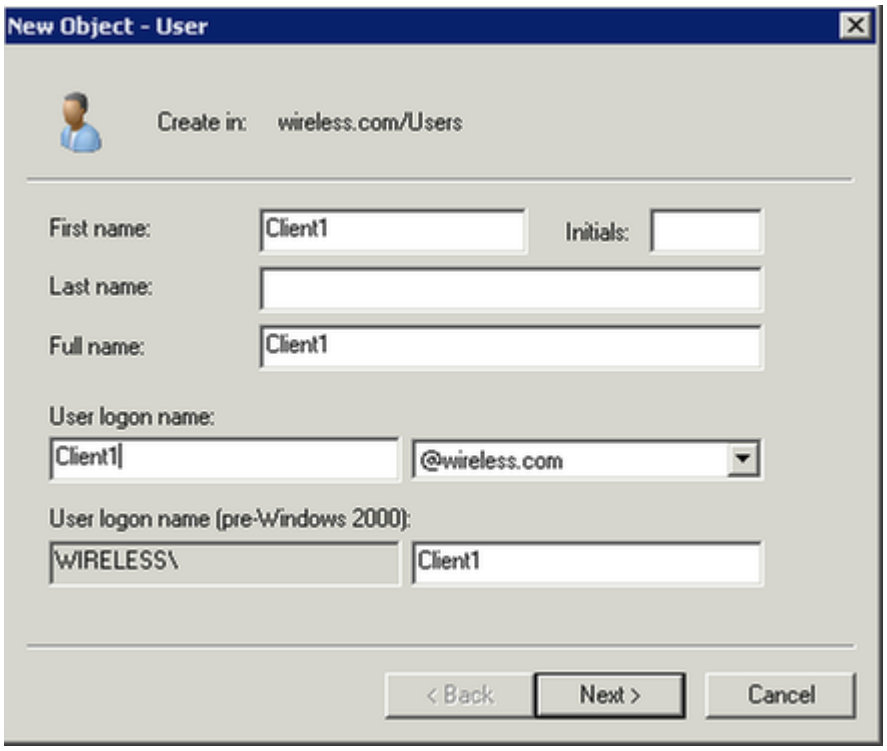
19. Klik op Finish (Voltooien).



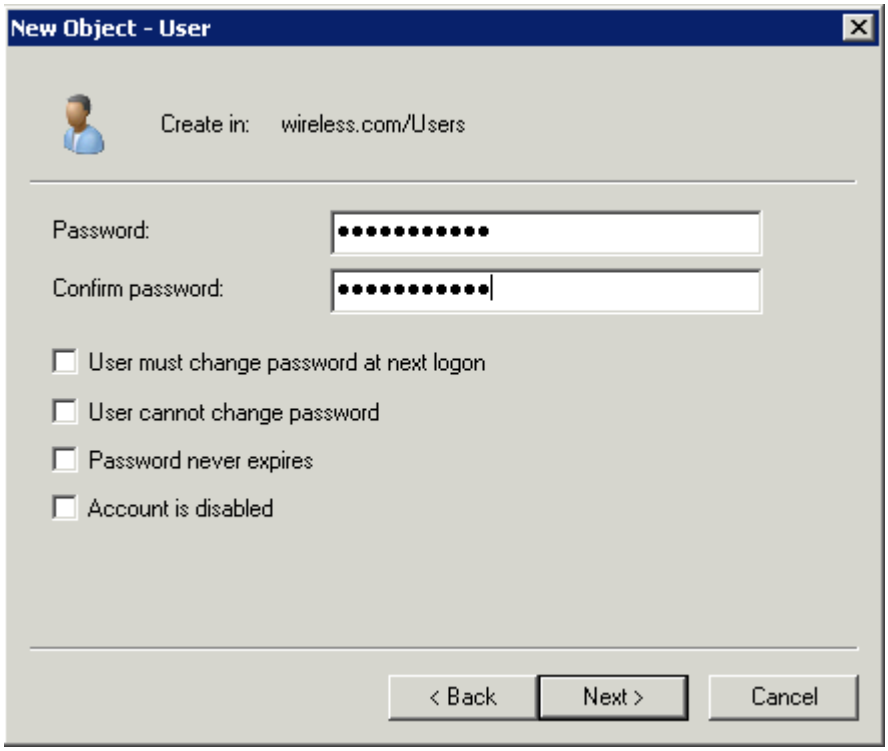
Gebruikers toevoegen aan de Active Directory

In dit voorbeeld wordt de gebruikersdatabase onderhouden in de Active Directory. Voer de volgende stappen uit om gebruikers aan de Active Directory-database toe te voegen:

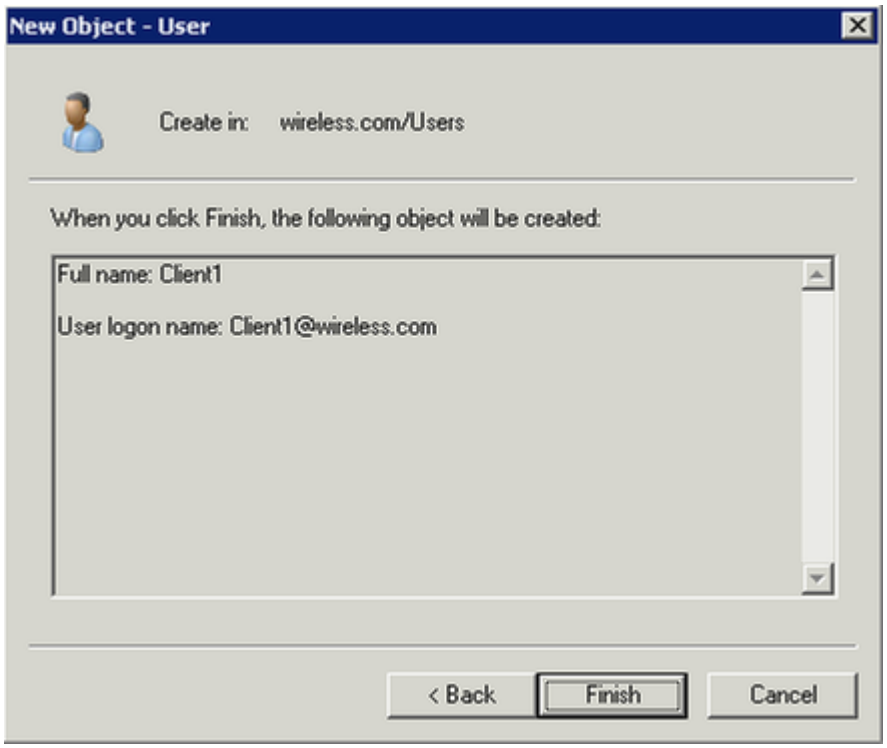
1. Open Active Directory-gebruikers en -computers. Klik op Start> Administratieve hulpmiddelen> Active Directory-gebruikers en -computers.
2. Vouw het domein uit in de consolestructuur van Active Directory Gebruikers en computers, klik met de rechtermuisknop op Gebruikers> Nieuw en kies Gebruiker.
3. Voer in het dialoogvenster Nieuw object – gebruiker de naam van de draadloze gebruiker in. In dit voorbeeld wordt de naam Client1 gebruikt in het veld Voornaam en Client1 in het veld Aanmeldingsnaam gebruiker. Klik op Next (Volgende).



4. Voer in het dialoogvenster Nieuw object – gebruiker een wachtwoord naar keuze in de velden Wachtwoord en wachtwoord bevestigen in. Controleer of het selectievakje Gebruiker moet wachtwoord wijzigen bij volgende aanmelding niet is ingeschakeld en klik op Volgende.



5. Klik in het dialoogvenster Nieuw object – gebruiker op Voltooien.



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

De draadloze LAN-controller en LAP's configureren

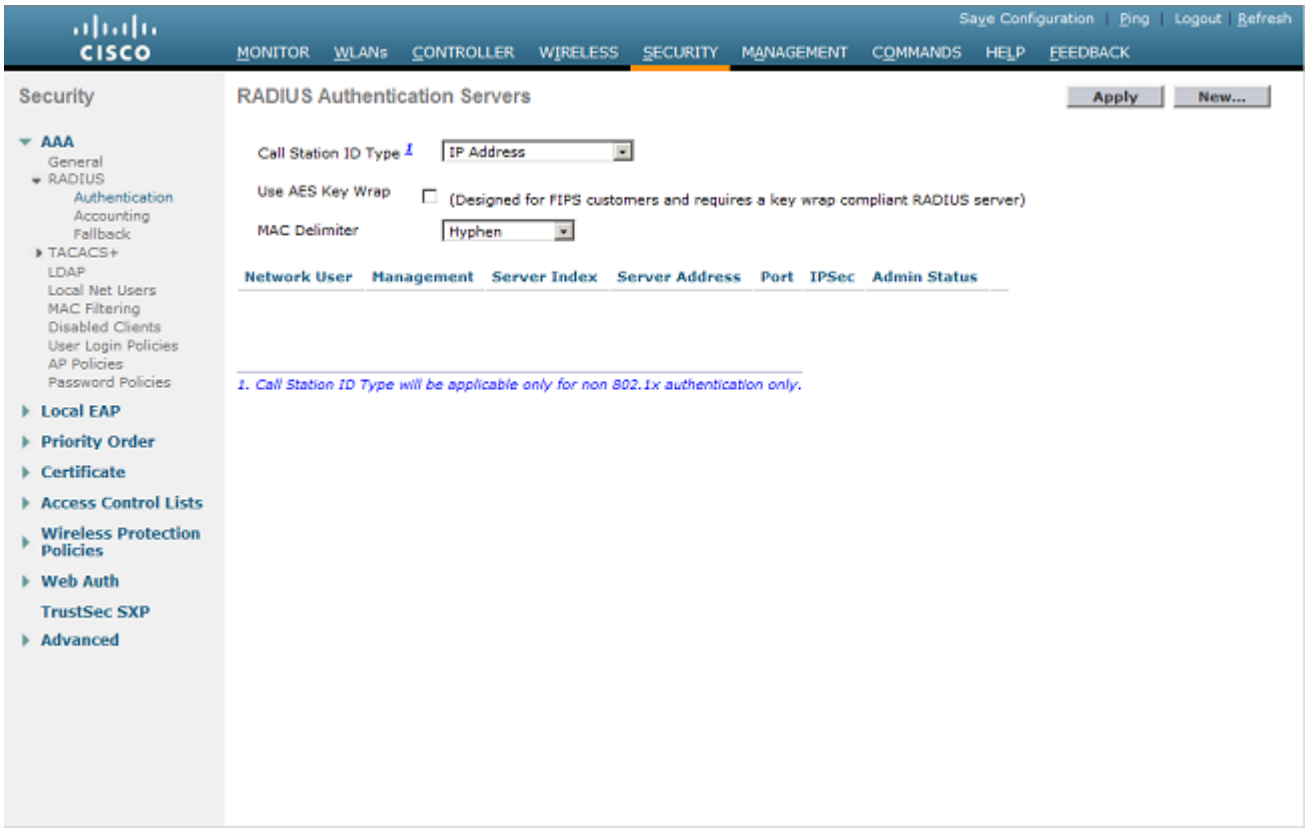
Configureer de draadloze apparaten (de draadloze LAN-controllers en LAP's) voor deze installatie.

De WLC configureren voor RADIUS-verificatie

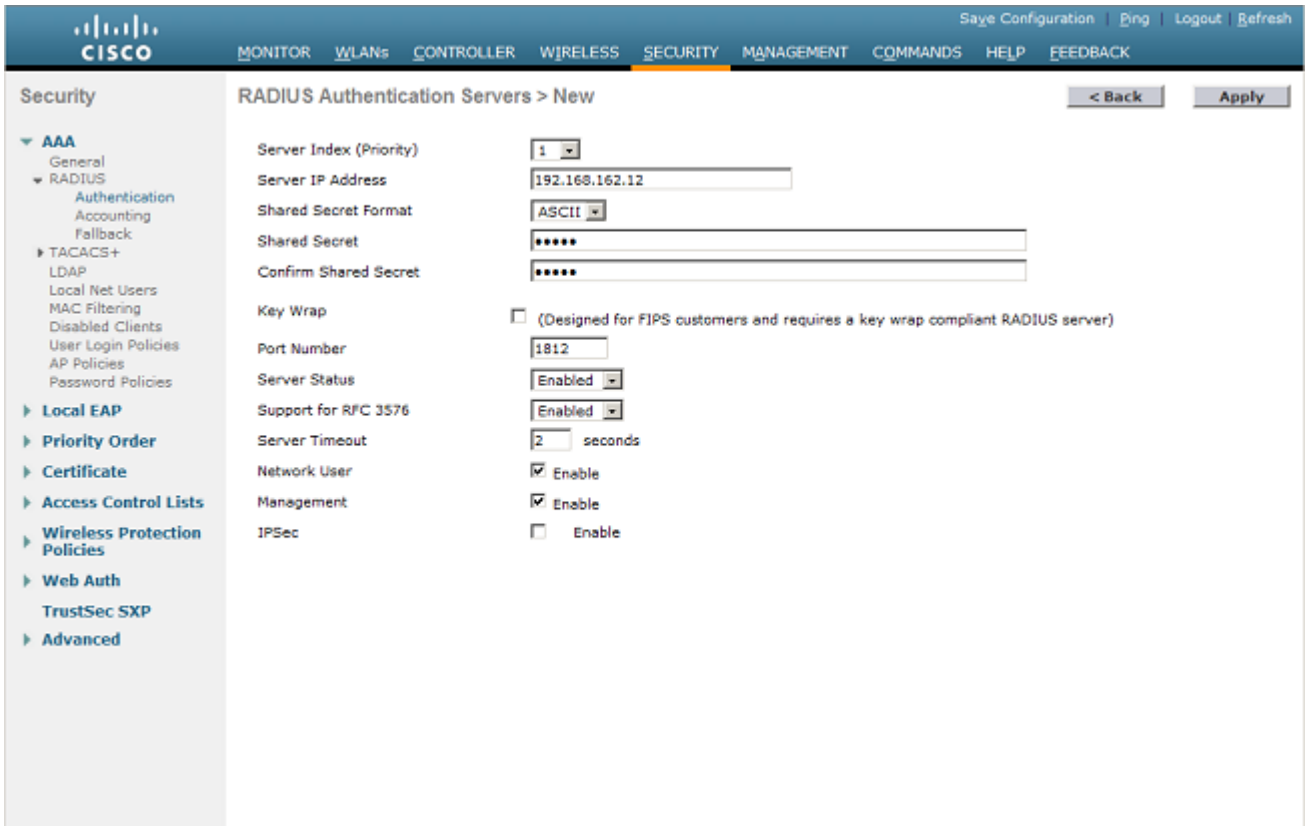
Configureer de WLC om de NPS als verificatieserver te gebruiken. De WLC moet worden geconfigureerd om de gebruikersreferenties door te sturen naar een externe RADIUS-server. De externe RADIUS-server valideert vervolgens de gebruikersreferenties en biedt toegang tot de draadloze clients.

Voer deze stappen uit om de NPS als RADIUS-server toe te voegen op de pagina Beveiliging > RADIUS-verificatie:

1. Kies Beveiliging> RADIUS > Verificatie in de controllerinterface om de pagina RADIUS-verificatieservers weer te geven. Klik op Nieuw om een RADIUS-server te definiëren.



2. De RADIUS-serverparameters definiëren. Deze parameters omvatten het IP-adres van de RADIUS-server, het gedeelde geheim, het poortnummer en de serverstatus. Met de selectievakjes Netwerkgebruiker en -beheer wordt bepaald of op RADIUS gebaseerde verificatie van toepassing is op beheer- en netwerkgebruikers (draadloze gebruikers). In dit voorbeeld wordt de NPS gebruikt als de RADIUS-server met een IP-adres van 192.168.162.12. Klik op Apply (Toepassen).



Een WLAN configureren voor de clients

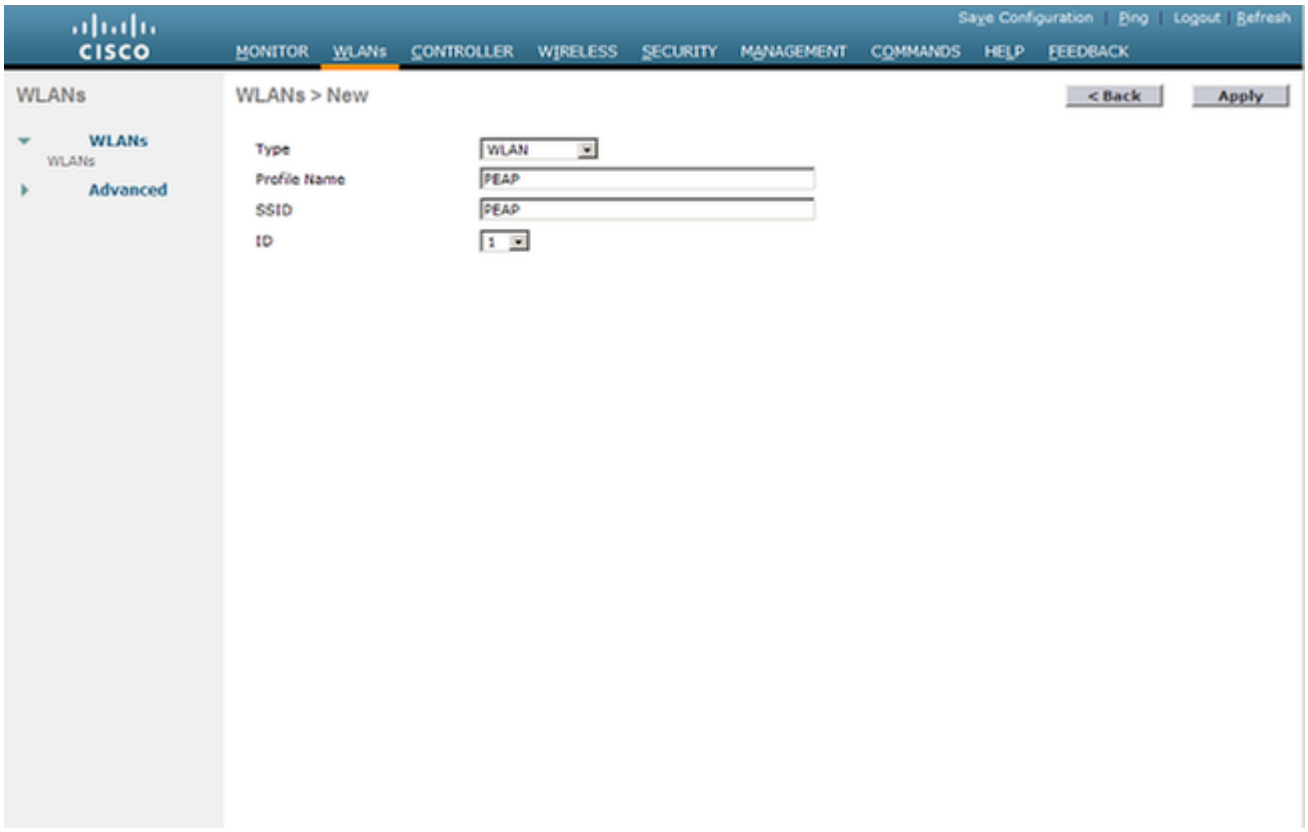
Configureer de Service Set Identifier (SSID) (WLAN) waarmee de draadloze clients verbinding maken. Maak in dit voorbeeld de SSID en noem deze PEAP.

Definieer Layer 2-verificatie als WPA2 zodat de clients EAP-gebaseerde verificatie uitvoeren (PEAP-MS-CHAP v2 in dit voorbeeld) en de geavanceerde coderingsstandaard (AES) als coderingsmechanisme gebruiken. Laat alle andere waarden op hun standaardwaarden.

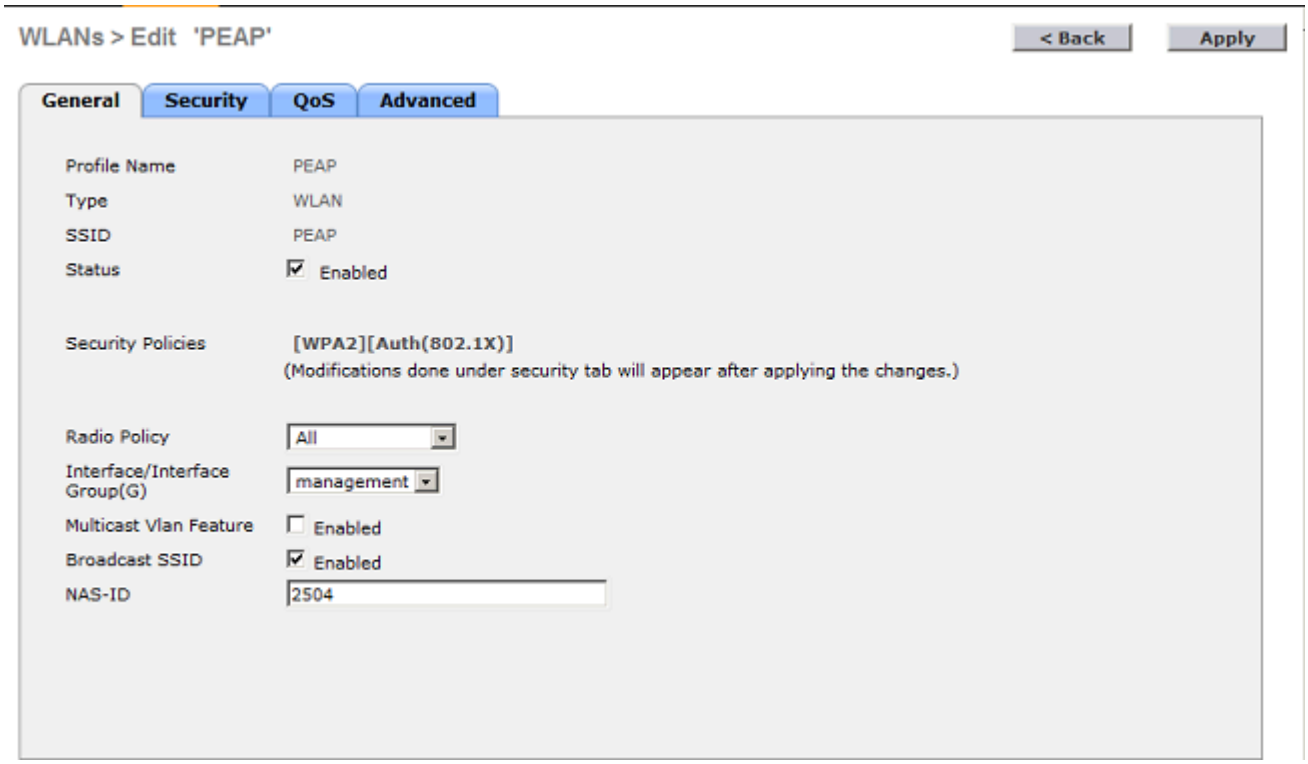
Opmerking: Dit document verbindt het WLAN met de beheerinterfaces. Wanneer u meerdere VLAN's in uw netwerk hebt, kunt u een apart VLAN maken en dit aan de SSID koppelen. Zie Voorbeeld van configuratie van VLAN's op draadloze LAN-controllers voor informatie over het configureren van VLAN's op WLC's.

Voer de volgende stappen uit om een WLAN op de WLC te configureren:

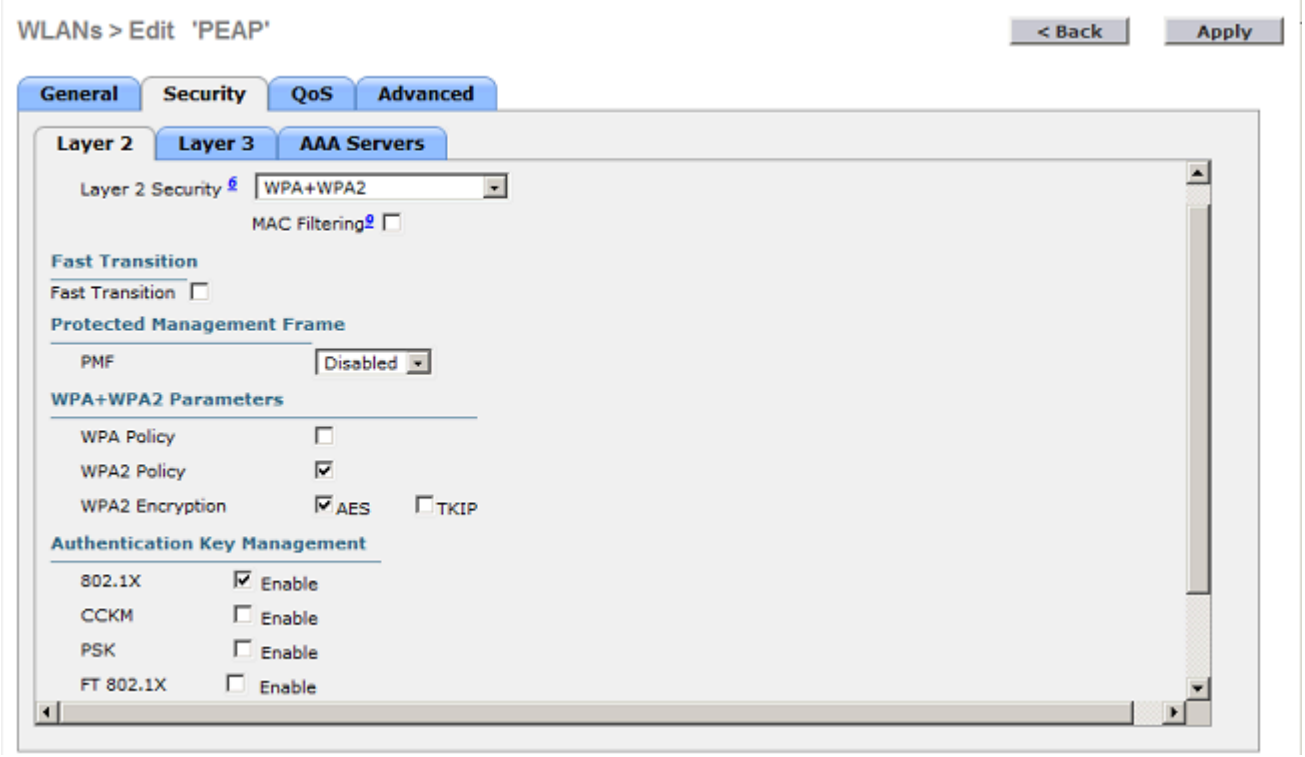
1. Klik op WLAN's in de controllerinterface om de WLAN-pagina weer te geven. Deze pagina geeft een overzicht van de WLAN's op de controller.
2. Kies Nieuw om een nieuw WLAN te maken. Voer de WLAN-ID en de WLAN-SSID voor het WLAN in en klik op Toepassen.



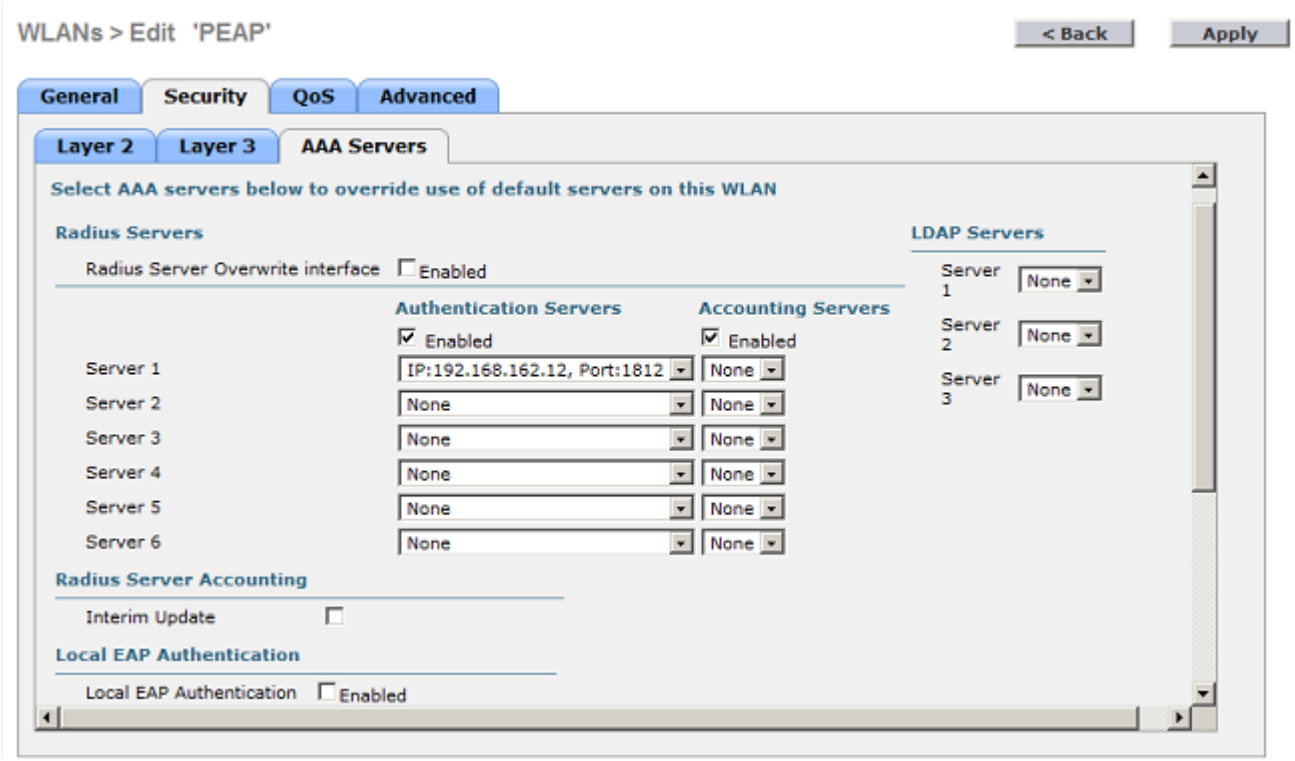
3. Voer de volgende stappen uit om de SSID voor 802.1x te configureren:
    1. Klik op het tabblad Algemeen en schakel het WLAN in.



    2. Klik op de tabbladen Beveiliging > Laag 2, stel Layer 2-beveiliging in op WPA + WPA2, schakel de selectievakjes WPA+WPA2 Parameters (bijvoorbeeld WPA2 AES) in als dat nodig is en klik op 802.1x als beheer van de verificatiesleutel.



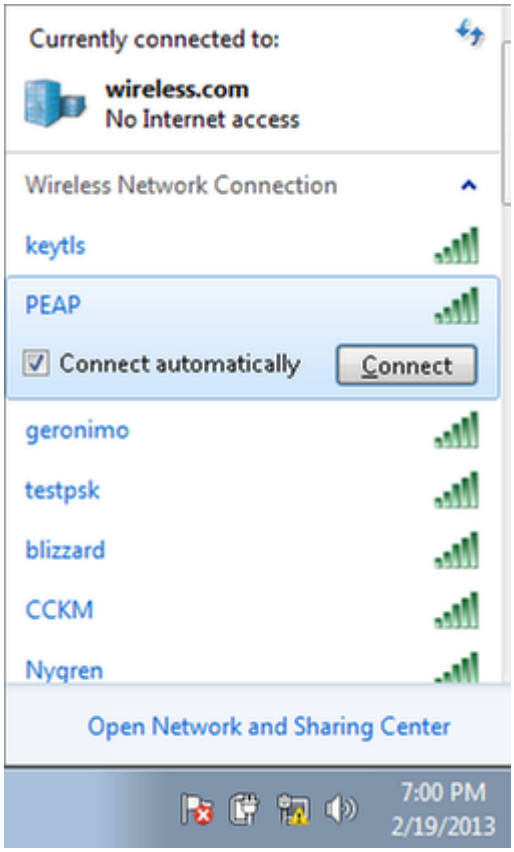
3. Klik op de tabbladen Beveiliging > AAA-servers, kies het IP-adres van de NPS in de vervolgkeuzelijst Server 1 en klik op Toepassen.



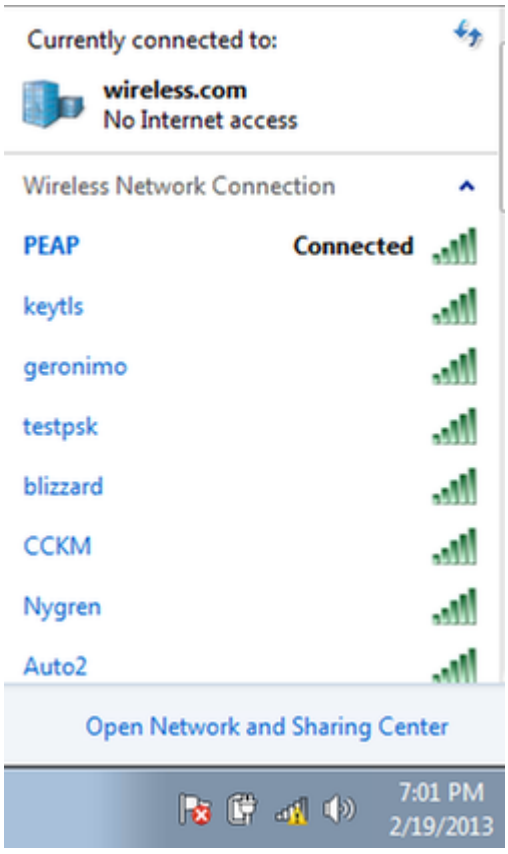
De draadloze clients configureren voor PEAP-MS-CHAP v2-verificatie

Voer deze stappen uit om de draadloze client met het hulpprogramma Windows Zero Config te configureren voor verbinding met het PEAP-WLAN.

1. Klik op het pictogram Netwerk op de taakbalk. Klik op de PEAP-SSID en klik op Verbinden.



2. De client moet nu verbonden zijn met het netwerk.



3. Als de verbinding mislukt, probeert u opnieuw verbinding te maken met het WLAN. Als het

probleem zich blijft voordoen, raadpleegt u het gedeelte Problemen oplossen.

Verifiëren

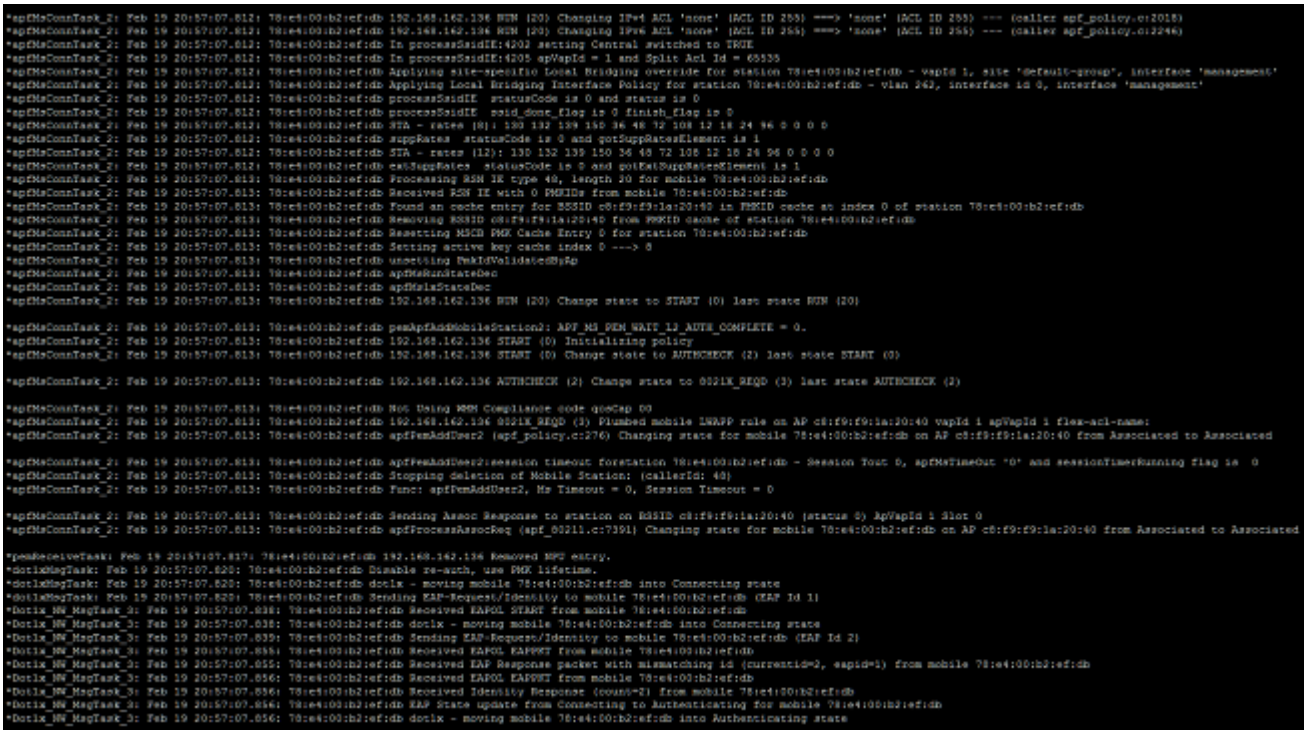
Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Als uw client geen verbinding heeft gemaakt met het WLAN, bevat dit gedeelte informatie die u kunt gebruiken om problemen met de configuratie op te lossen.

Er zijn twee hulpprogramma's die kunnen worden gebruikt om 802.1x-verificatiefouten te diagnosticeren: de opdracht Client debuggen en de Event Viewer in Windows.

Als u een clientfoutopsporing uitvoert vanuit de WLC, is dit niet arbeidsintensief en heeft dit geen invloed op de service. Als u een foutopsporingssessie wilt starten, opent u de opdrachtregelinterface (CLI) van de WLC en voert u het MAC-adres van de foutopsporingsclient in, waarbij het MAC-adres het draadloze MAC-adres is van de draadloze client die geen verbinding kan maken. Terwijl deze foutopsporing wordt uitgevoerd, probeert u de client te verbinden; er moet uitvoer zijn op de CLI van de WLC die lijkt op dit voorbeeld:



Dit is een voorbeeld van een probleem dat zich kan voordoen bij een verkeerde configuratie. Hier toont het WLC-debug dat de WLC is verplaatst naar de authenticatiestatus, wat betekent dat de WLC wacht op een reactie van de NPS. Dit is meestal te wijten aan een onjuist gedeeld geheim op de WLC of de NPS. U kunt dit bevestigen via de Windows Server Event Viewer. Als u geen logboek vindt, is het verzoek nooit bij de NPS terechtgekomen.

Een ander voorbeeld dat wordt gevonden van het WLC-debug is een access-reject. Een toegangsweigering toont aan dat de NPS de clientreferenties heeft ontvangen en afgewezen. Dit is een voorbeeld van een client die een toegangsweigering ontvangt:

```
*dot1xMsgTask: Feb 19 21:28:20.689: 78:e4:00:b2:ef:db Sending EAP-Request/Identity to mobile 78:e4:00:b2:ef:db (EAP Id 1)
*Dot1x_NW_MsgTask_3: Feb 19 21:28:20.699: 78:e4:00:b2:ef:db Received EAPOL START from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:28:20.699: 78:e4:00:b2:ef:db dot1x - moving mobile 78:e4:00:b2:ef:db into Connecting state
*Dot1x_NW_MsgTask_3: Feb 19 21:28:20.699: 78:e4:00:b2:ef:db Sending EAP-Request/Identity to mobile 78:e4:00:b2:ef:db (EAP Id 2)
*Dot1x_NW_MsgTask_3: Feb 19 21:28:24.508: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:28:24.508: 78:e4:00:b2:ef:db Received Identity Response (count=2) from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:28:24.508: 78:e4:00:b2:ef:db EAP State update from Connecting to Authenticating for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:28:24.508: 78:e4:00:b2:ef:db dot1x - moving mobile 78:e4:00:b2:ef:db into Authenticating state
*Dot1x_NW_MsgTask_3: Feb 19 21:28:24.508: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:28:24.519: 78:e4:00:b2:ef:db Processing Access-Reject for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:28:24.520: 78:e4:00:b2:ef:db Removing PMK cache due to EAP-Failure for mobile 78:e4:00:b2:ef:db (EAP Id -1)
*Dot1x_NW_MsgTask_3: Feb 19 21:28:24.520: 78:e4:00:b2:ef:db Sending EAP-Failure to mobile 78:e4:00:b2:ef:db (EAP Id -1)
```

Wanneer u een toegangsweigering ziet, controleert u de logs in de Windows Server-gebeurtenislogboeken om te bepalen waarom de NPS op de client heeft gereageerd met een toegangsweigering.

Een succesvolle authenticatie heeft een access-accept in het client debug, zoals te zien is in dit voorbeeld:

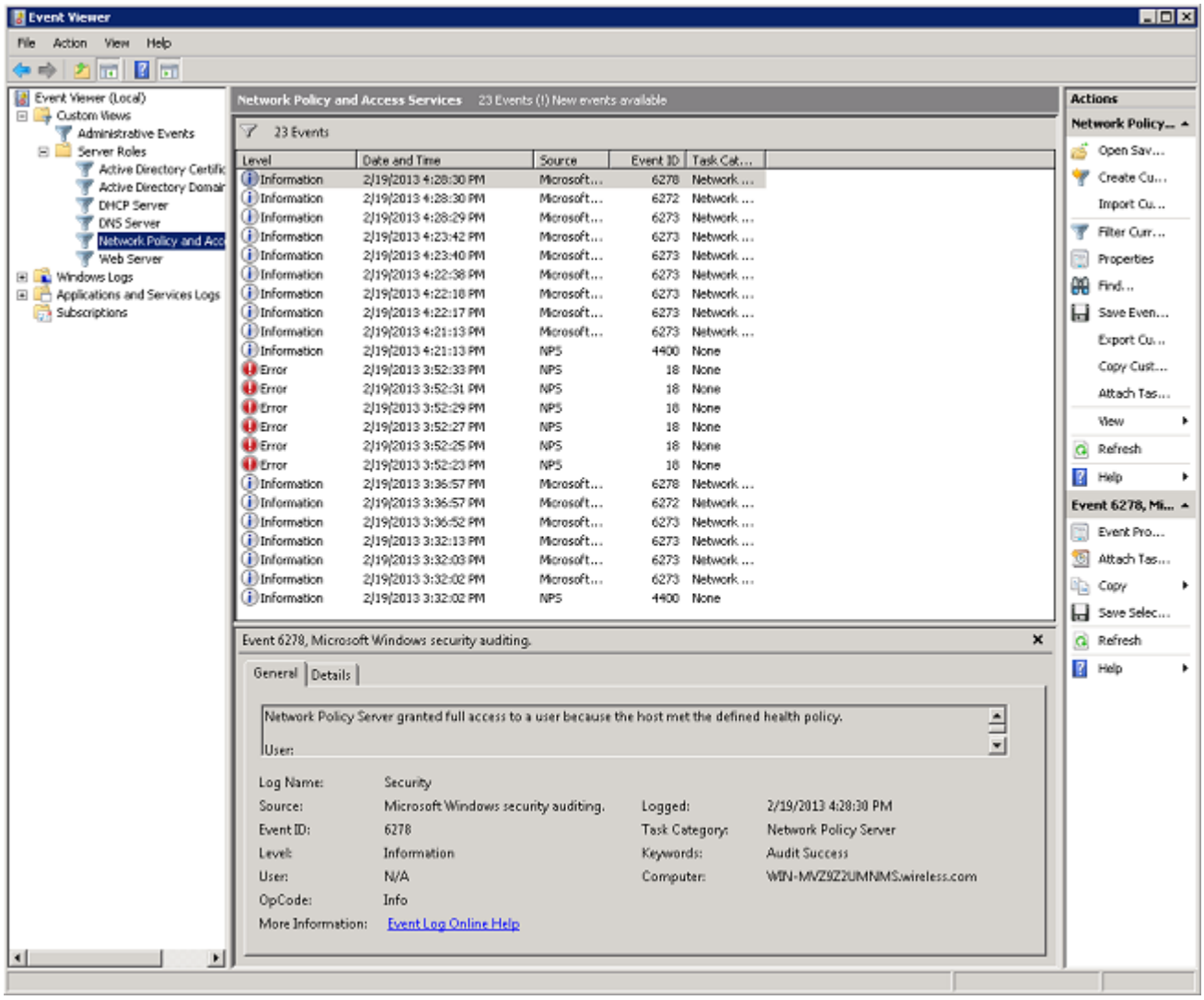
```
*dot1xMsgTask: Feb 19 21:33:14.576: 78:e4:00:b2:ef:db Sending EAP-Request/Identity to mobile 78:e4:00:b2:ef:db (EAP Id 1)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.596: 78:e4:00:b2:ef:db Received EAPOL START from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.596: 78:e4:00:b2:ef:db dot1x - moving mobile 78:e4:00:b2:ef:db into Connecting state
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.596: 78:e4:00:b2:ef:db Sending EAP-Request/Identity to mobile 78:e4:00:b2:ef:db (EAP Id 2)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.601: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.601: 78:e4:00:b2:ef:db Received EAP Response packet with mismatching id (currentid=2, eapid=1) from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.611: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.611: 78:e4:00:b2:ef:db Received Identity Response (count=2) from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.611: 78:e4:00:b2:ef:db EAP State update from Connecting to Authenticating for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.611: 78:e4:00:b2:ef:db dot1x - moving mobile 78:e4:00:b2:ef:db into Authenticating state
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.611: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.643: 78:e4:00:b2:ef:db Processing Access-Challenge for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.643: 78:e4:00:b2:ef:db Entering Backend Auth Req state (id=3) for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.643: 78:e4:00:b2:ef:db Sending EAP Request from AAA to mobile 78:e4:00:b2:ef:db (EAP Id 3)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.661: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.661: 78:e4:00:b2:ef:db Received EAP Response from mobile 78:e4:00:b2:ef:db (EAP Id 3, EAP Type 25)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.661: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.665: 78:e4:00:b2:ef:db Processing Access-Challenge for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.665: 78:e4:00:b2:ef:db Entering Backend Auth Req state (id=4) for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.665: 78:e4:00:b2:ef:db Sending EAP Request from AAA to mobile 78:e4:00:b2:ef:db (EAP Id 4)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.674: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.674: 78:e4:00:b2:ef:db Received EAP Response from mobile 78:e4:00:b2:ef:db (EAP Id 4, EAP Type 25)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.674: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.685: 78:e4:00:b2:ef:db Processing Access-Challenge for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.685: 78:e4:00:b2:ef:db Entering Backend Auth Req state (id=7) for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.685: 78:e4:00:b2:ef:db WARNING: updated EAP-Identifier 4 ===> 7 for STA 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.685: 78:e4:00:b2:ef:db Sending EAP Request from AAA to mobile 78:e4:00:b2:ef:db (EAP Id 7)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.706: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.706: 78:e4:00:b2:ef:db Received EAP Response from mobile 78:e4:00:b2:ef:db (EAP Id 7, EAP Type 25)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.706: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.709: 78:e4:00:b2:ef:db Processing Access-Challenge for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.709: 78:e4:00:b2:ef:db Entering Backend Auth Req state (id=8) for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.709: 78:e4:00:b2:ef:db Sending EAP Request from AAA to mobile 78:e4:00:b2:ef:db (EAP Id 8)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.721: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.721: 78:e4:00:b2:ef:db Received EAP Response from mobile 78:e4:00:b2:ef:db (EAP Id 8, EAP Type 25)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.721: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.726: 78:e4:00:b2:ef:db Processing Access-Challenge for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.726: 78:e4:00:b2:ef:db Entering Backend Auth Req state (id=9) for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.726: 78:e4:00:b2:ef:db Sending EAP Request from AAA to mobile 78:e4:00:b2:ef:db (EAP Id 9)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.738: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.738: 78:e4:00:b2:ef:db Received EAP Response from mobile 78:e4:00:b2:ef:db (EAP Id 9, EAP Type 25)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.738: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.745: 78:e4:00:b2:ef:db Processing Access-Challenge for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.746: 78:e4:00:b2:ef:db Entering Backend Auth Req state (id=10) for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.746: 78:e4:00:b2:ef:db Sending EAP Request from AAA to mobile 78:e4:00:b2:ef:db (EAP Id 10)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.752: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.752: 78:e4:00:b2:ef:db Received EAP Response from mobile 78:e4:00:b2:ef:db (EAP Id 10, EAP Type 25)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.752: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.758: 78:e4:00:b2:ef:db Processing Access-Challenge for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.758: 78:e4:00:b2:ef:db Entering Backend Auth Req state (id=11) for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.758: 78:e4:00:b2:ef:db Sending EAP Request from AAA to mobile 78:e4:00:b2:ef:db (EAP Id 11)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.770: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.770: 78:e4:00:b2:ef:db Received EAP Response from mobile 78:e4:00:b2:ef:db (EAP Id 11, EAP Type 25)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.770: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.781: 78:e4:00:b2:ef:db Processing Access-Accept for mobile 78:e4:00:b2:ef:db
```

Als u problemen wilt oplossen met het afwijzen van toegang en het uitvoeren van reactietijden, hebt u toegang nodig tot de RADIUS-server. De WLC fungeert als een verificator die EAP-berichten doorgeeft tussen de client en de RADIUS-server. Een RADIUS-server die reageert met een time-out voor weigering van toegang of respons moet worden onderzocht en gediagnosticeerd door de fabrikant van de RADIUS-service.

Opmerking: TAC biedt geen technische ondersteuning voor RADIUS-servers van derden; de logs op de RADIUS-server verklaren echter over het algemeen waarom een clientverzoek is afgewezen of genegeerd.

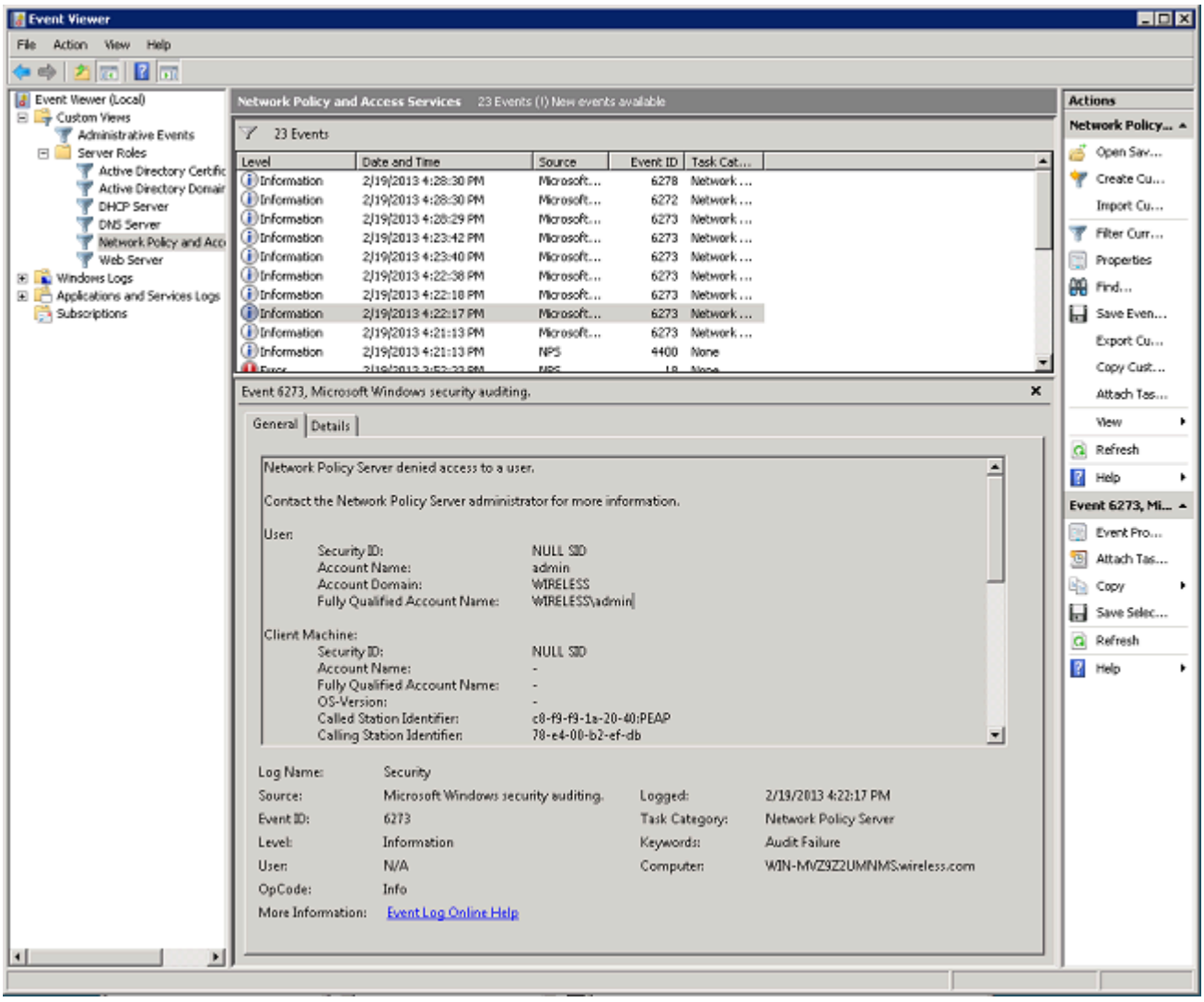
Als u problemen wilt oplossen met toegangsafwijzingen en reactietime-outs vanuit de NPS, bekijkt u de NPS-logs in de Windows Event Viewer op de server.

1. Klik op Start > Hulpmiddelen voor beheerders > Event Viewer om de Event Viewer te starten en de NPS-logs te bekijken.
2. Aangepaste weergaven uitbreiden > Serverrollen > Netwerkbeleid en toegang.

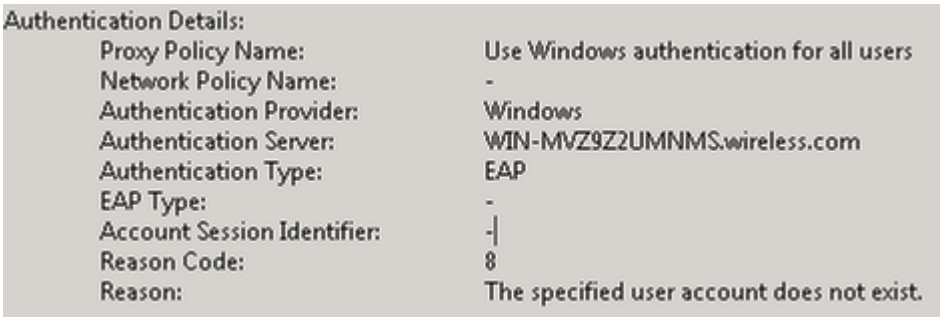


In dit gedeelte van de Gebeurtenisweergave vindt u logbestanden van doorgegeven en mislukte verificaties. Bekijk deze logs om problemen op te lossen waarom een client geen verificatie doorgeeft. Zowel goedgekeurde als mislukte verificaties worden weergegeven als informatief. Blader door de logs om de gebruikersnaam te vinden die niet is geverifieerd en die een toegangsweigering heeft ontvangen op basis van de WLC-debugs.

Dit is een voorbeeld van de NPS wanneer het een gebruiker toegang ontzegt:

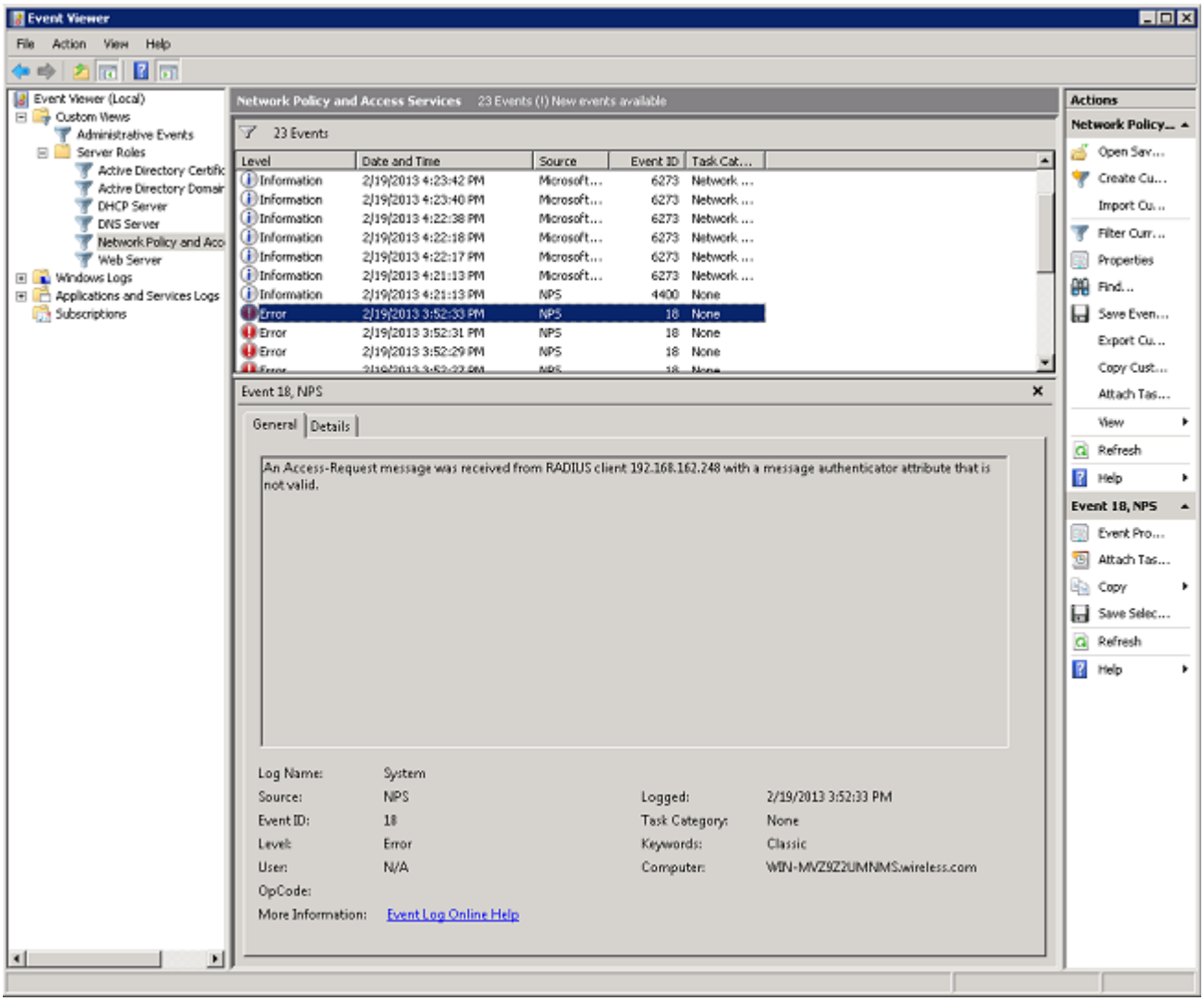


Wanneer u een weigeringsinstructie bekijkt in de Event Viewer, raadpleegt u de sectie Verificatiedetails. In dit voorbeeld ziet u dat de NPS de gebruiker de toegang heeft geweigerd vanwege een onjuiste gebruikersnaam:



De Gebeurtenisweergave op de NPS helpt ook wanneer u problemen moet oplossen als de WLC geen reactie van de NPS ontvangt. Dit wordt meestal veroorzaakt door een onjuist gedeeld geheim tussen de NPS en de WLC.

In dit voorbeeld wijst de NPS het verzoek van de WLC af vanwege een onjuist gedeeld geheim:



Gerelateerde informatie

- [Cisco Technical Support en downloads]

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.