

NPS, draadloze LAN-controllers en draadloze netwerken configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[PEAP-overzicht](#)

[PEAP fase één: TLS-gecodeerd kanaal](#)

[PEAP fase twee: EAP-geauthentiseerde communicatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[De Microsoft Windows 2008-server configureren](#)

[De Microsoft Windows 2008-server configureren als domeincontroller](#)

[DHCP-services installeren en configureren op de Microsoft Windows 2008-server](#)

[De Microsoft Windows 2008-server als CA-server installeren en configureren](#)

[Cliënten verbinden met het domein](#)

[De netwerkbeleidserver installeren op de Microsoft Windows 2008-server](#)

[Een certificaat installeren](#)

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

[Gebruikers toevoegen aan de Active Directory](#)

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

[De WLC configureren voor RADIUS-verificatie](#)

[Een WLAN configureren voor de clients](#)

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

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

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

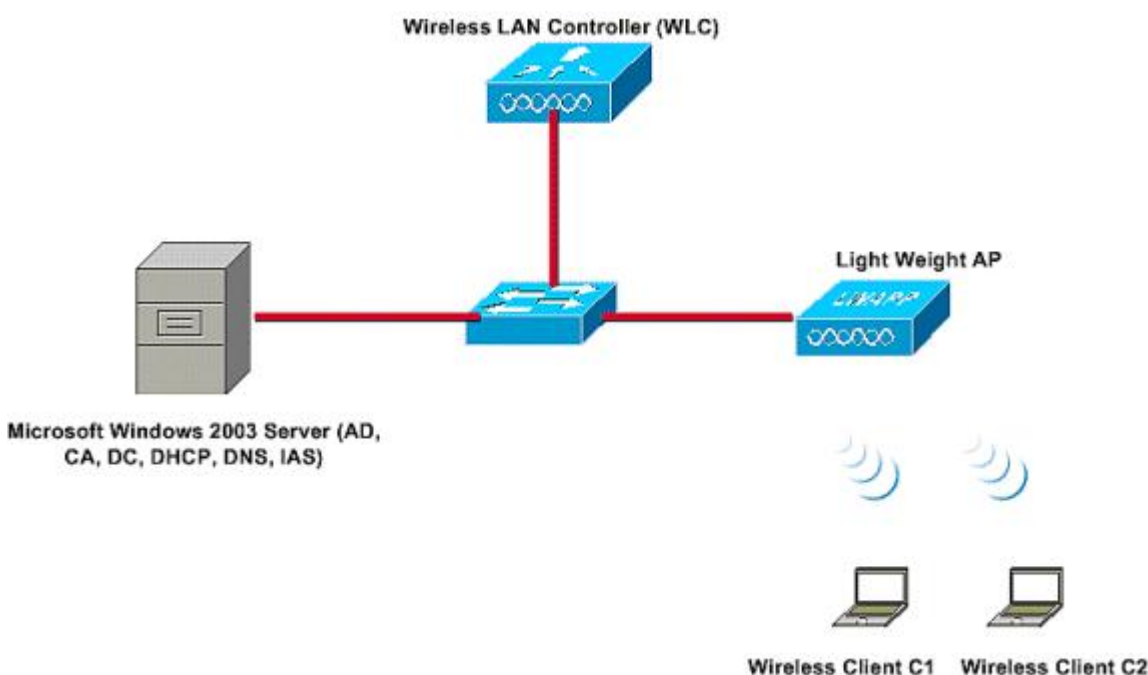
In deze sectie vindt u de informatie voor het configureren van PEAP-MS-CHAP v2.



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.

Netwerkdigram

Deze configuratie maakt gebruik van de volgende netwerkconfiguratie:



Netwerkdigram

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

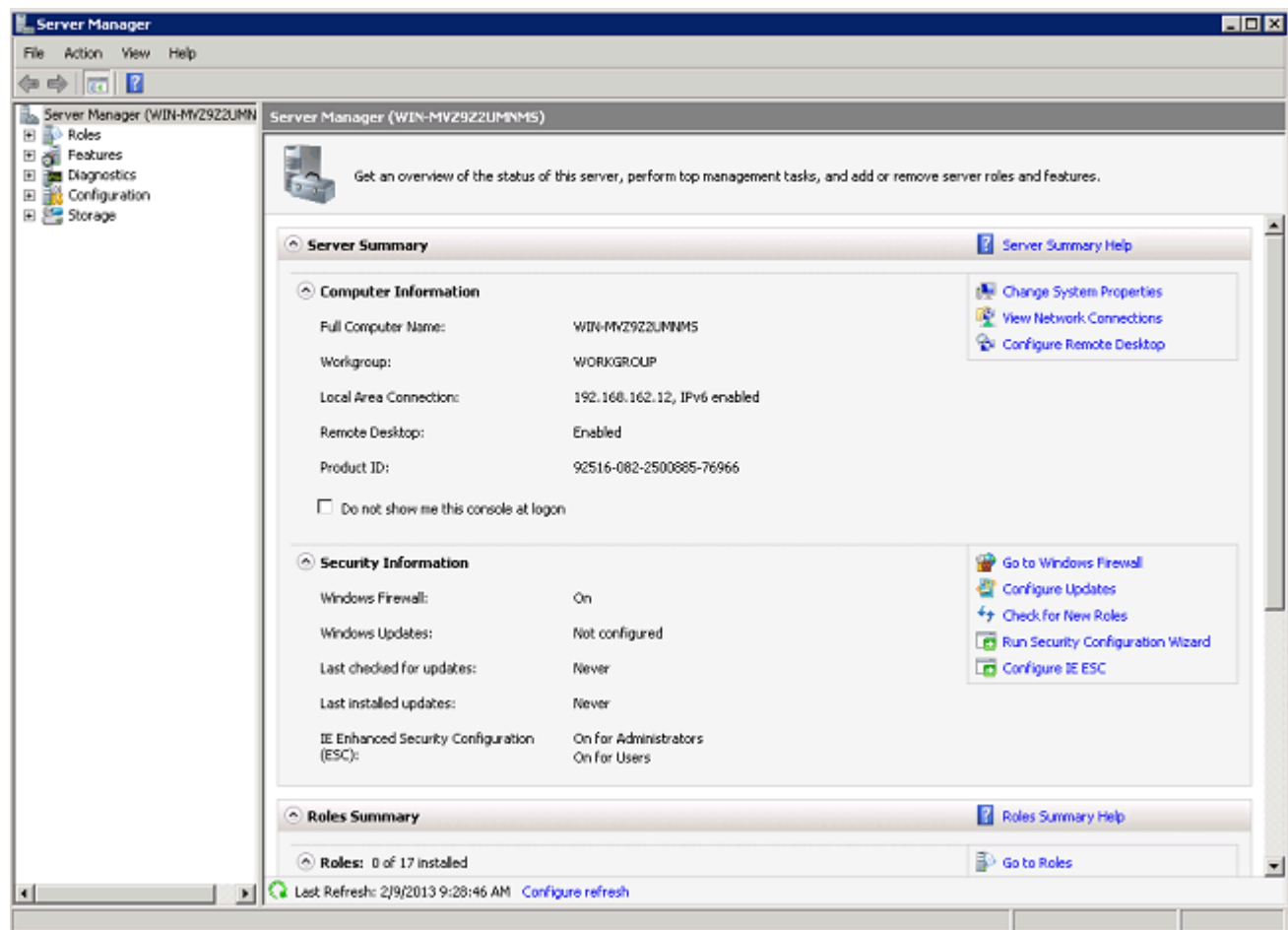
In dit voorbeeld bevat een volledige configuratie van de Microsoft Windows 2008-server de volgende stappen:

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.

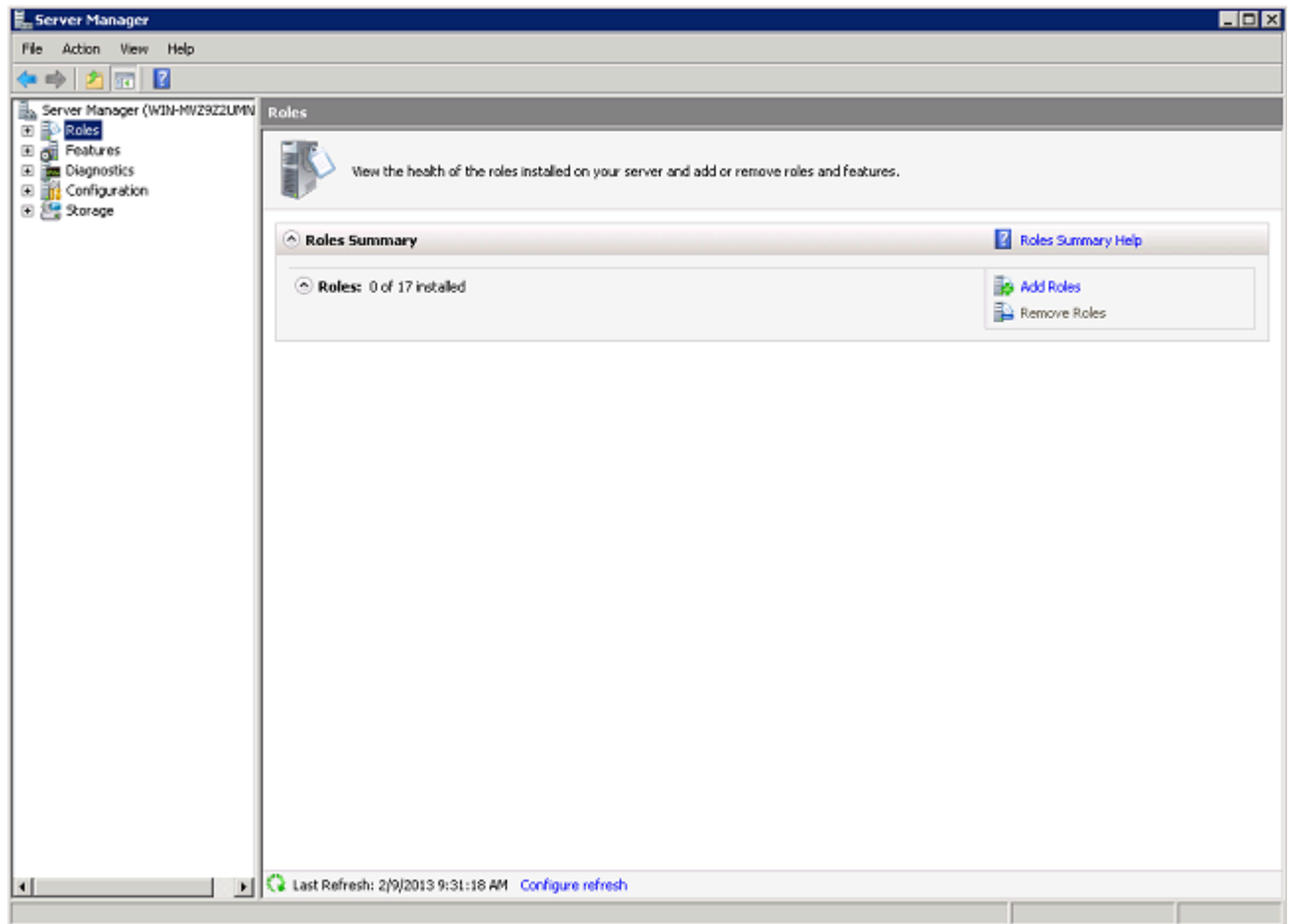
De Microsoft Windows 2008-server configureren als domeincontroller

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).

Add Roles Wizard

 **Before You Begin**

Before You Begin

Server Roles

Confirmation

Progress

Results

This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.

Before you continue, verify that:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

☐ Skip this page by default

< Previous **Next >** Install Cancel

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

Add Roles Wizard

 **Select Server Roles**

Before You Begin

Server Roles

Active Directory Domain Services

Confirmation

Progress

Results

Select one or more roles to install on this server.

Roles:

- ☐ Active Directory Certificate Services
- ☒ **Active Directory Domain Services**
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ☐ File Services
- ☐ Network Policy and Access Services
- ☐ Print Services
- ☐ Terminal Services
- ☐ UDDI Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

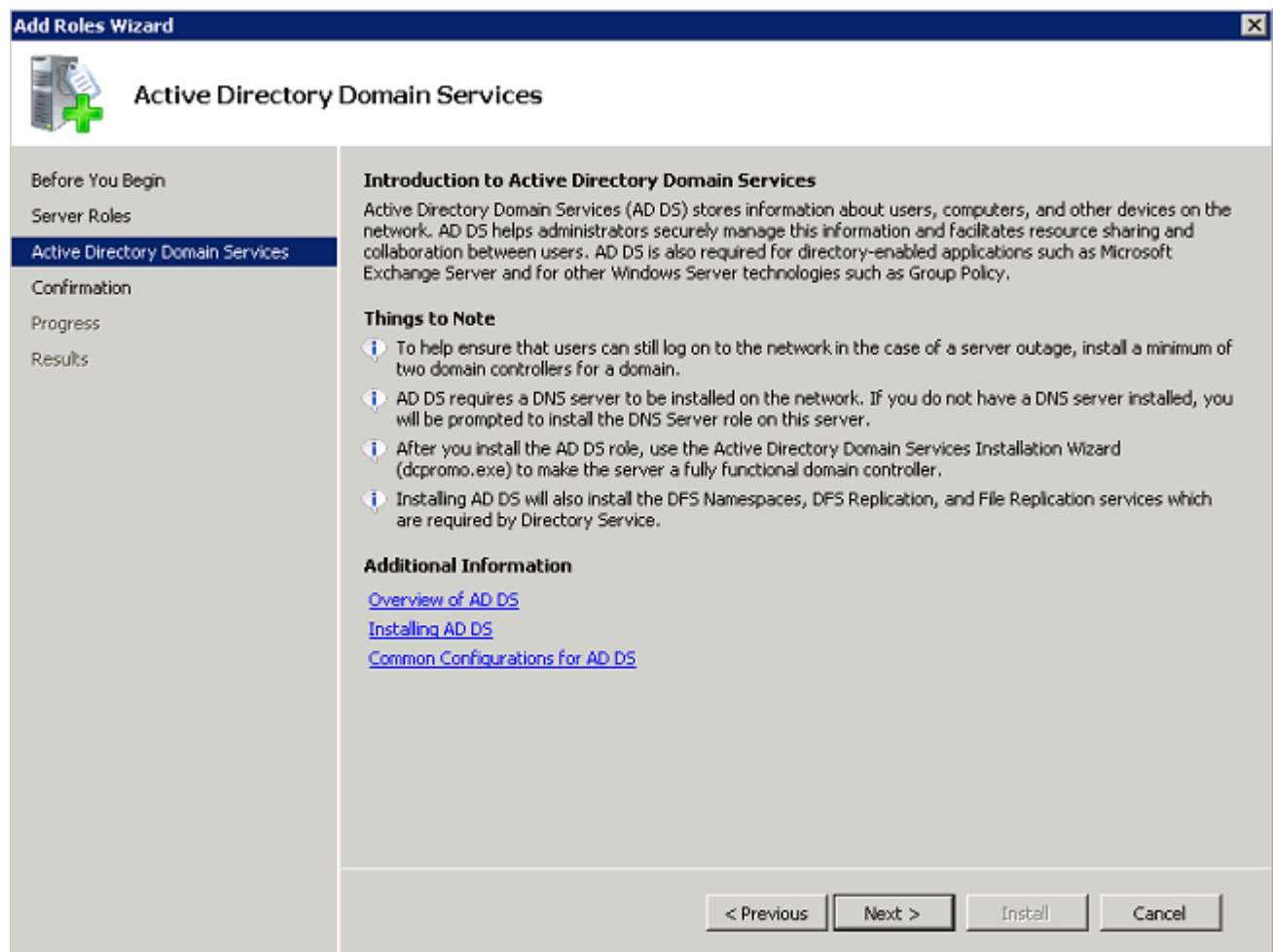
[More about server roles](#)

Description:

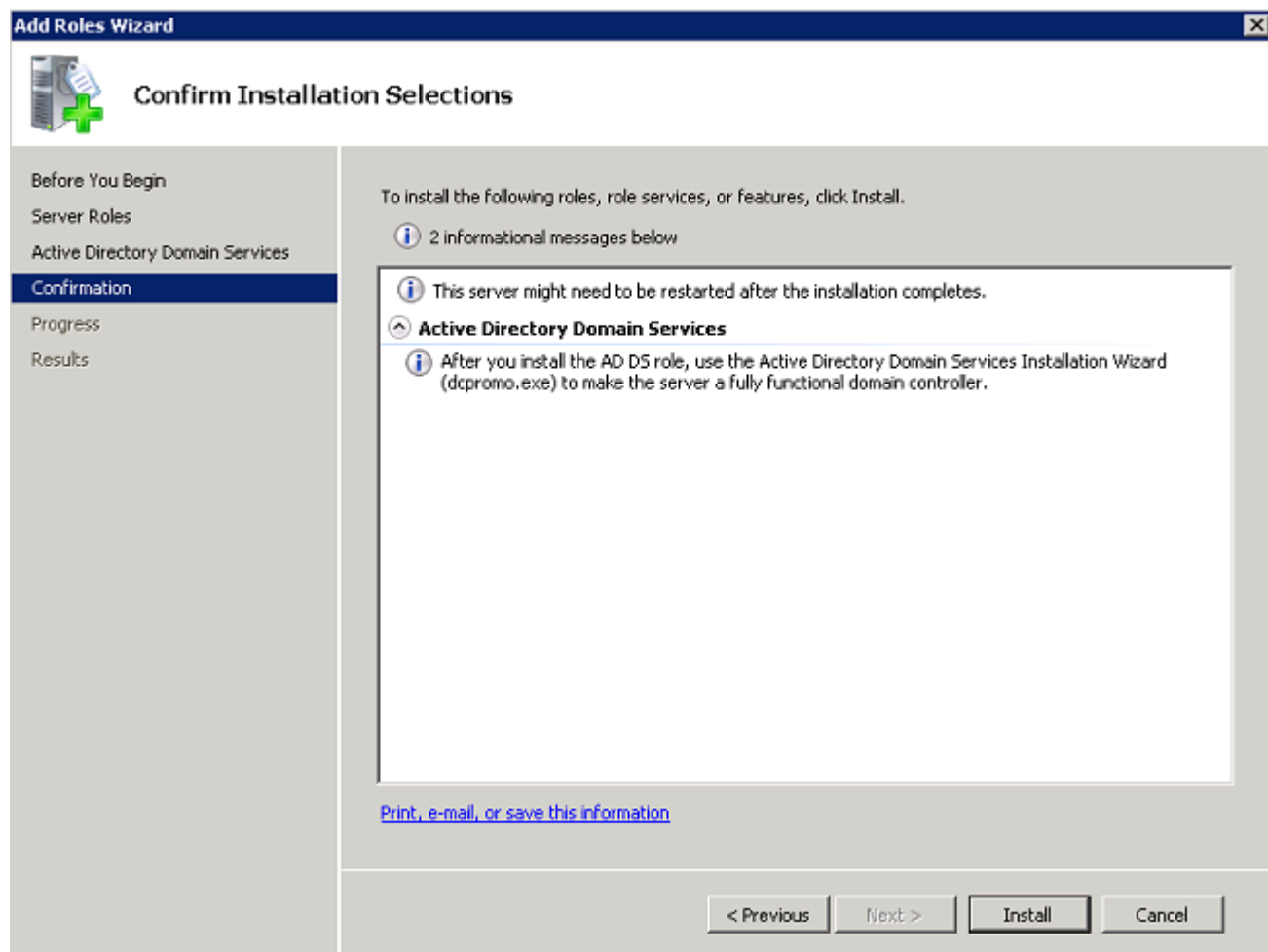
[Active Directory Domain Services \(AD DS\)](#) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

< Previous Next > Install Cancel

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

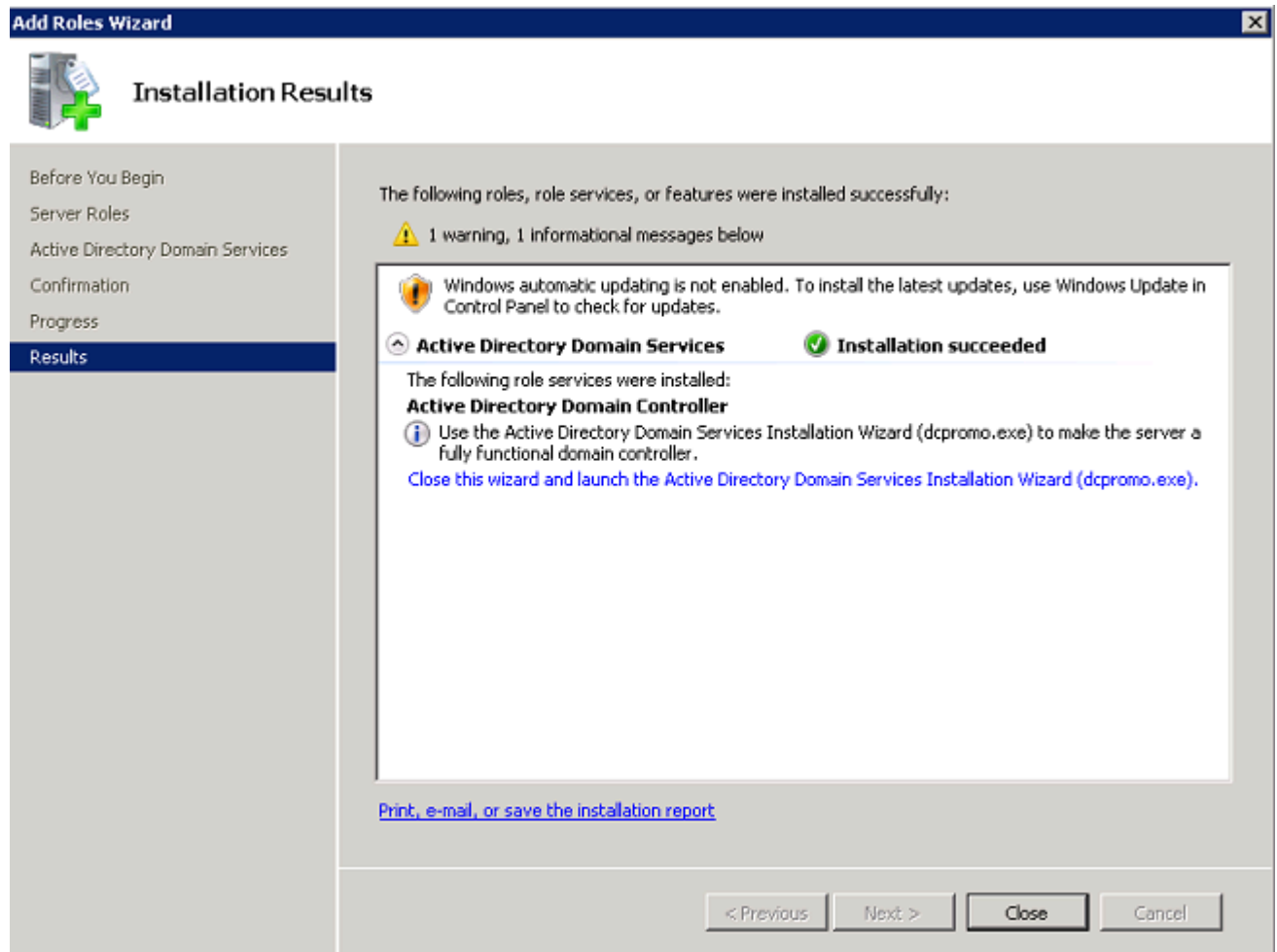


6. Klik op Installeren om het installatieproces te starten.



De installatie gaat door en wordt voltooid.

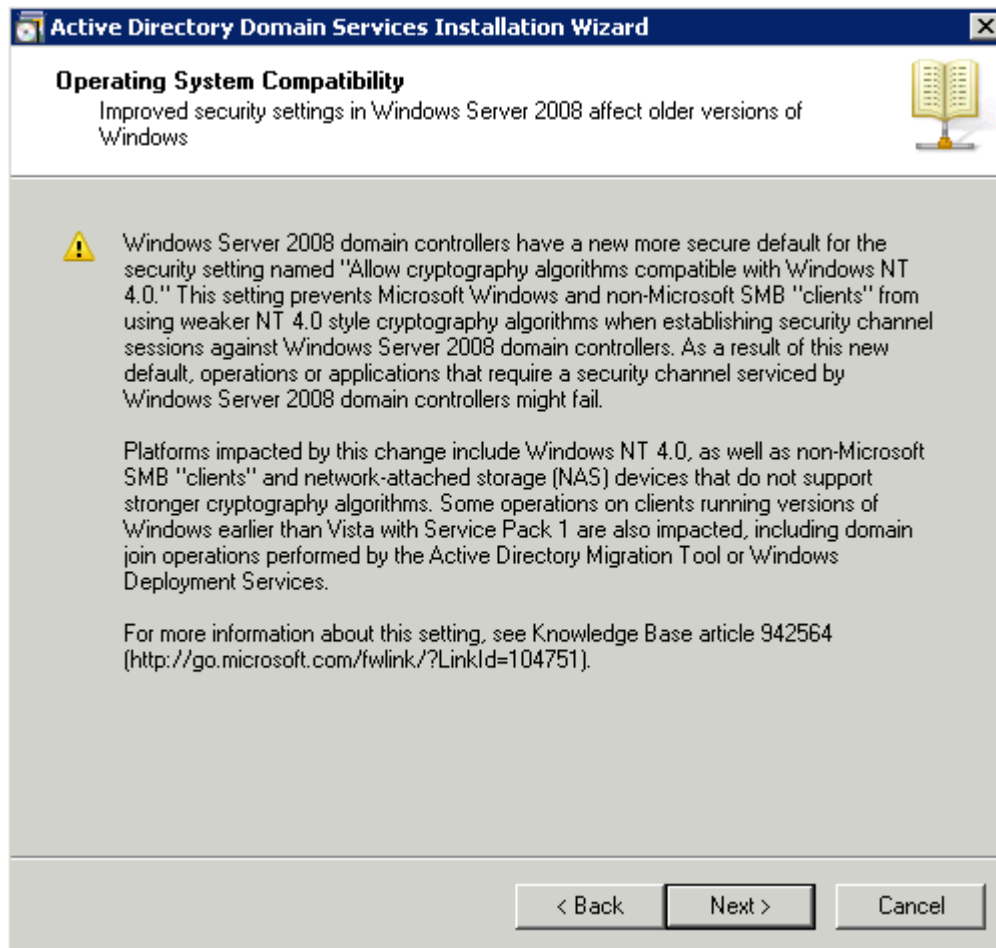
7. Klik op Deze wizard sluiten en start de installatiewizard voor Active Directory Domain Services (dcpromo.exe) om door te gaan met de installatie en configuratie van de Active Directory.



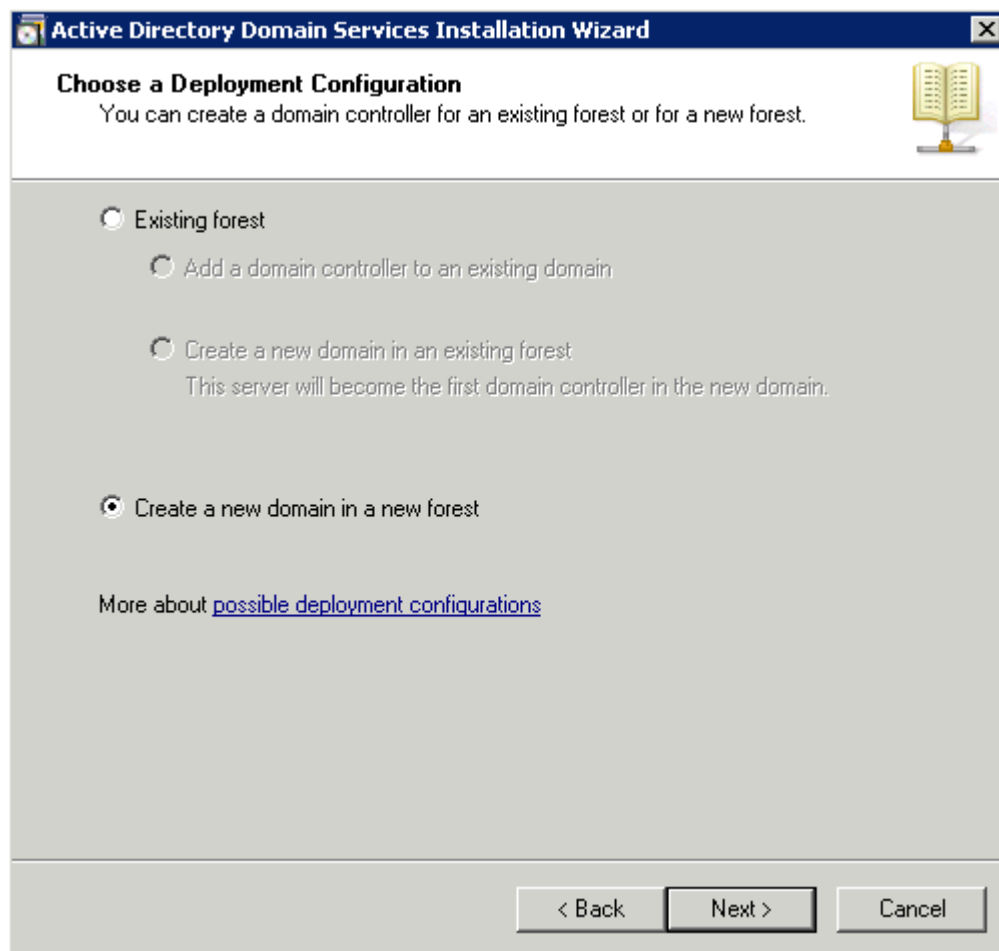
8. Klik op Volgende om de installatiewizard voor Active Directory Domain Services uit te voeren.



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.

Active Directory Domain Services Installation Wizard

Name the Forest Root Domain

The first domain in the forest is the forest root domain. Its name is also the name of the forest.

Type the fully qualified domain name (FQDN) of the new forest root domain.

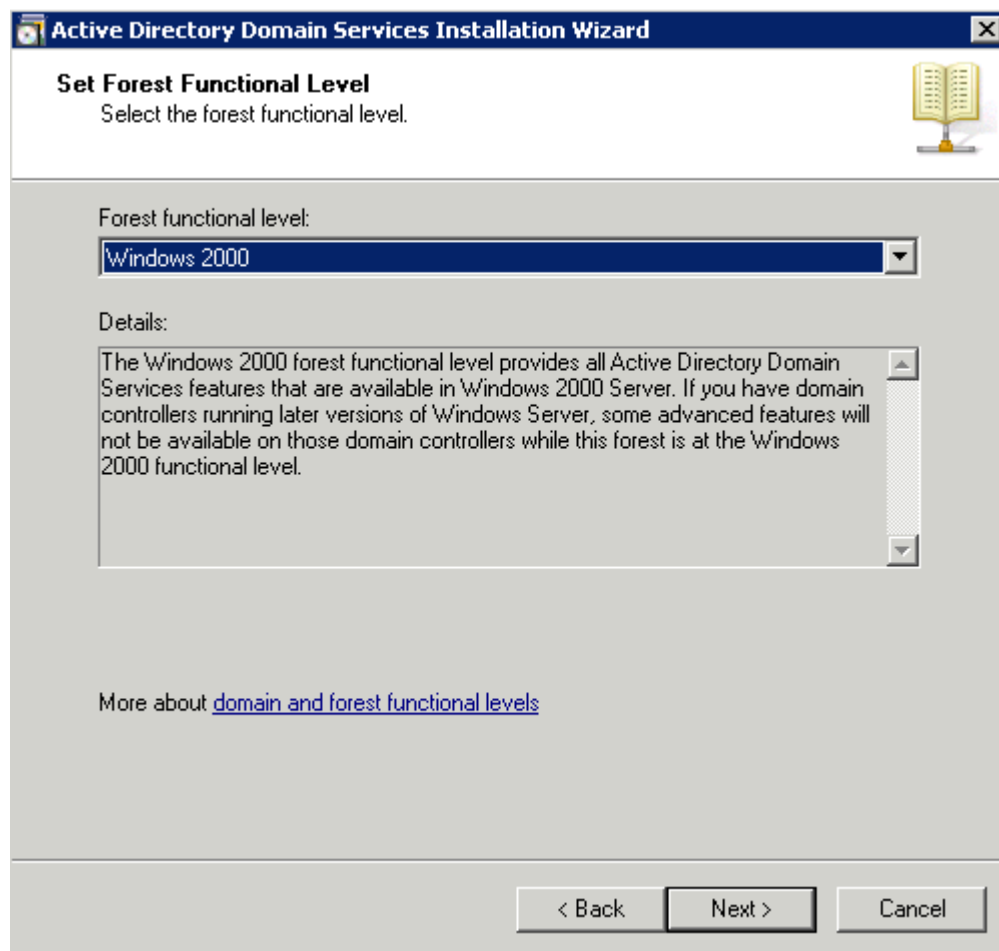
FQDN of the forest root domain:

wireless.com

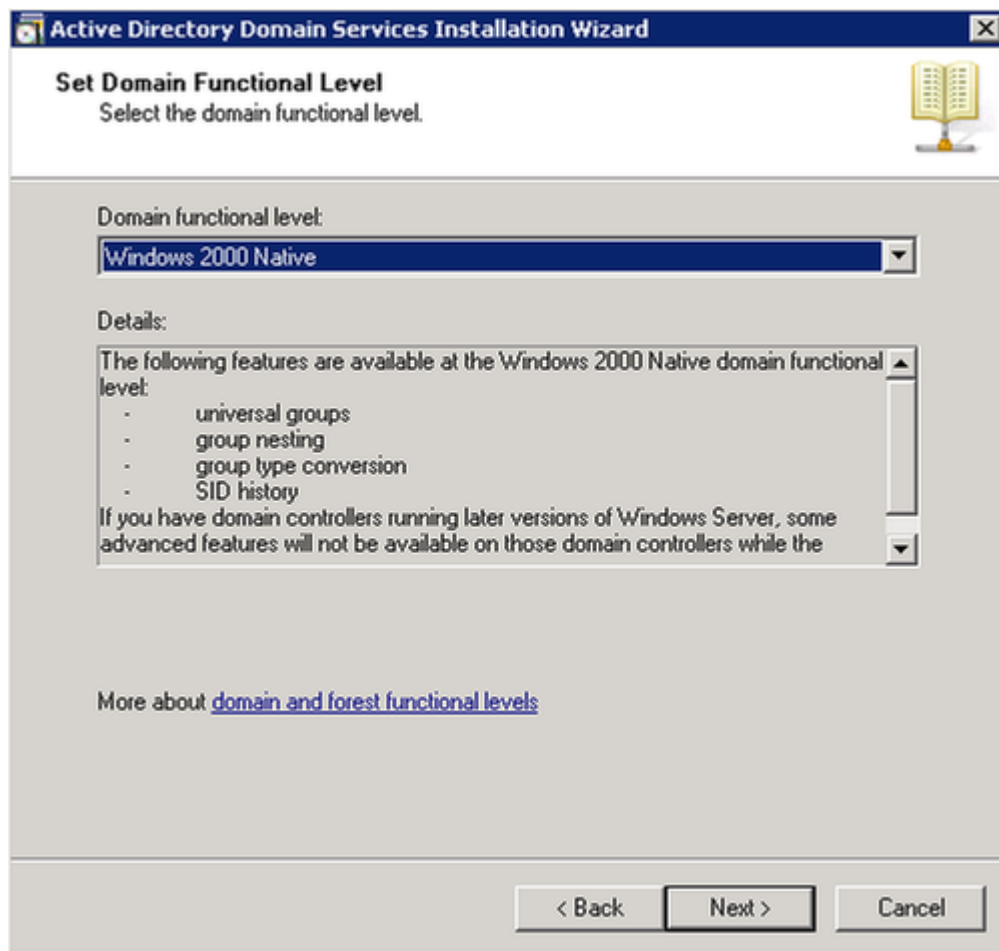
Example: corp.contoso.com

< Back Next > Cancel

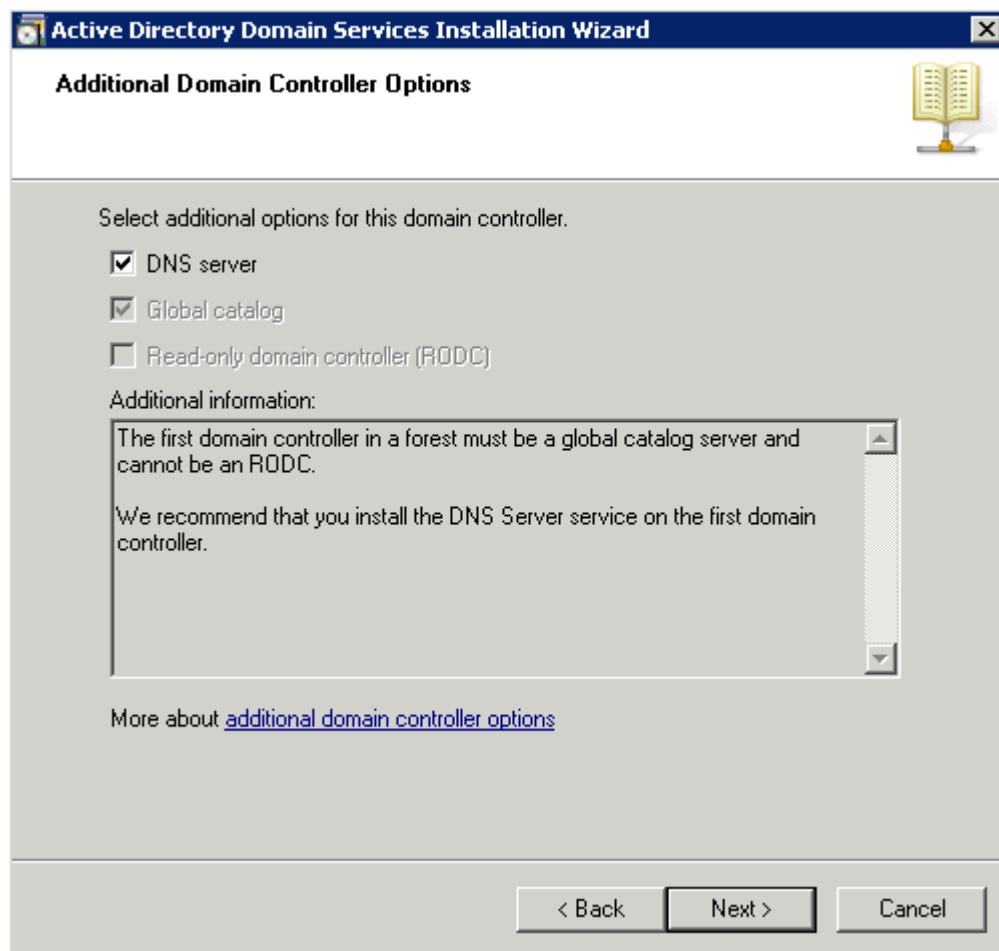
12. Selecteer het functionele niveau van het forest voor uw domein en klik op Volgende.



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.

Active Directory Domain Services Installation Wizard

Location for Database, Log Files, and SYSVOL
Specify the folders that will contain the Active Directory domain controller database, log files, and SYSVOL.

For better performance and recoverability, store the database and log files on separate volumes.

Database folder:

Log files folder:

SYSVOL folder:

More about [placing Active Directory Domain Services files](#)

17. Voer het beheerderswachtwoord in en klik op Volgende.

Active Directory Domain Services Installation Wizard

Directory Services Restore Mode Administrator Password

The Directory Services Restore Mode Administrator account is different from the domain Administrator account.

Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.

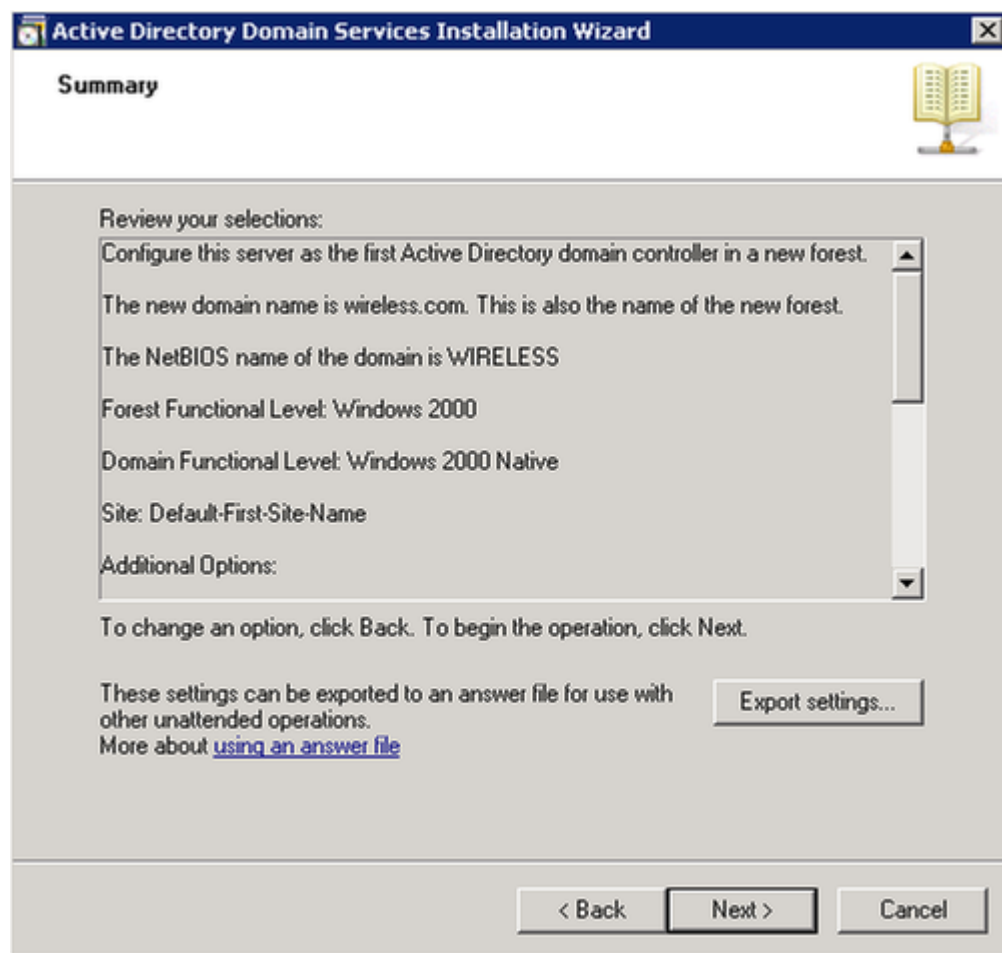
Password:

Confirm password:

More about [Directory Services Restore Mode password](#)

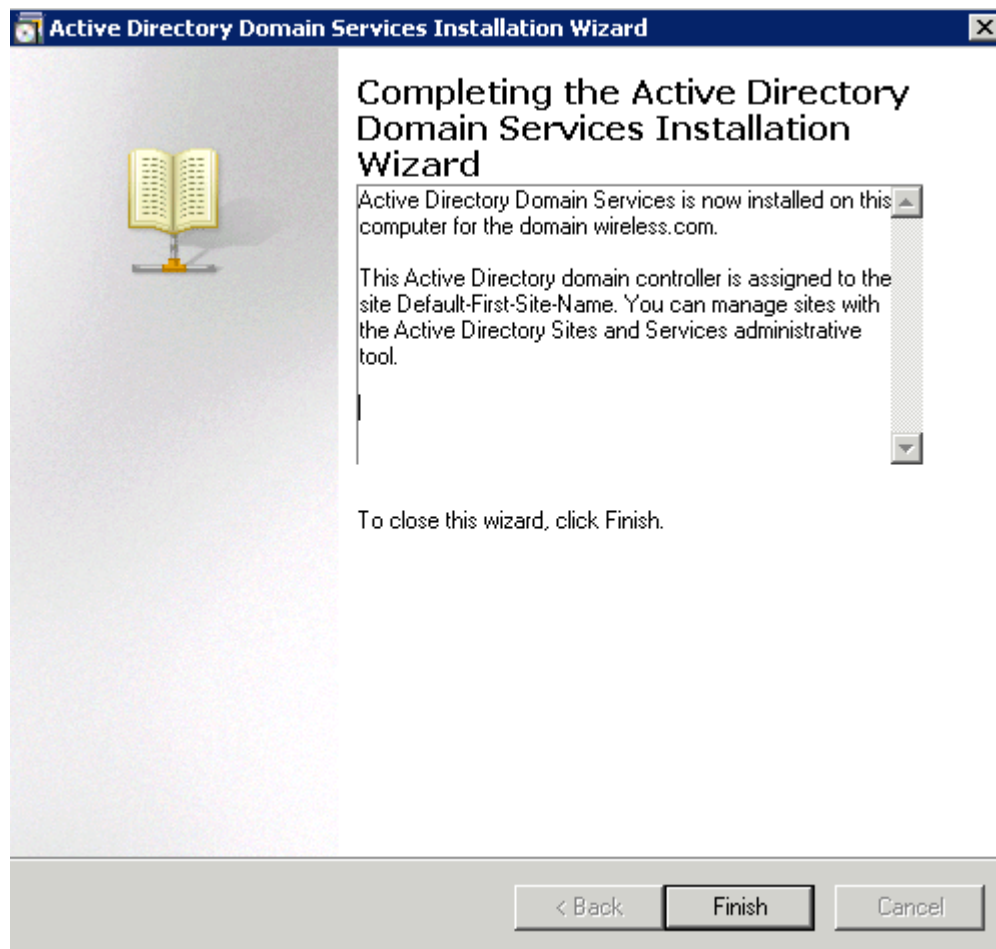
< Back Next > Cancel

18. Controleer uw selecties en klik op Volgende.

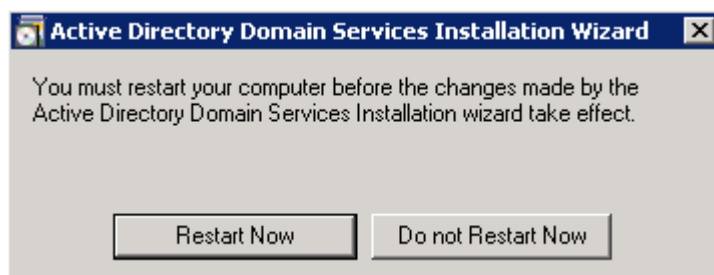


De installatie gaat door.

19. Klik op Voltooien om de wizard te sluiten.



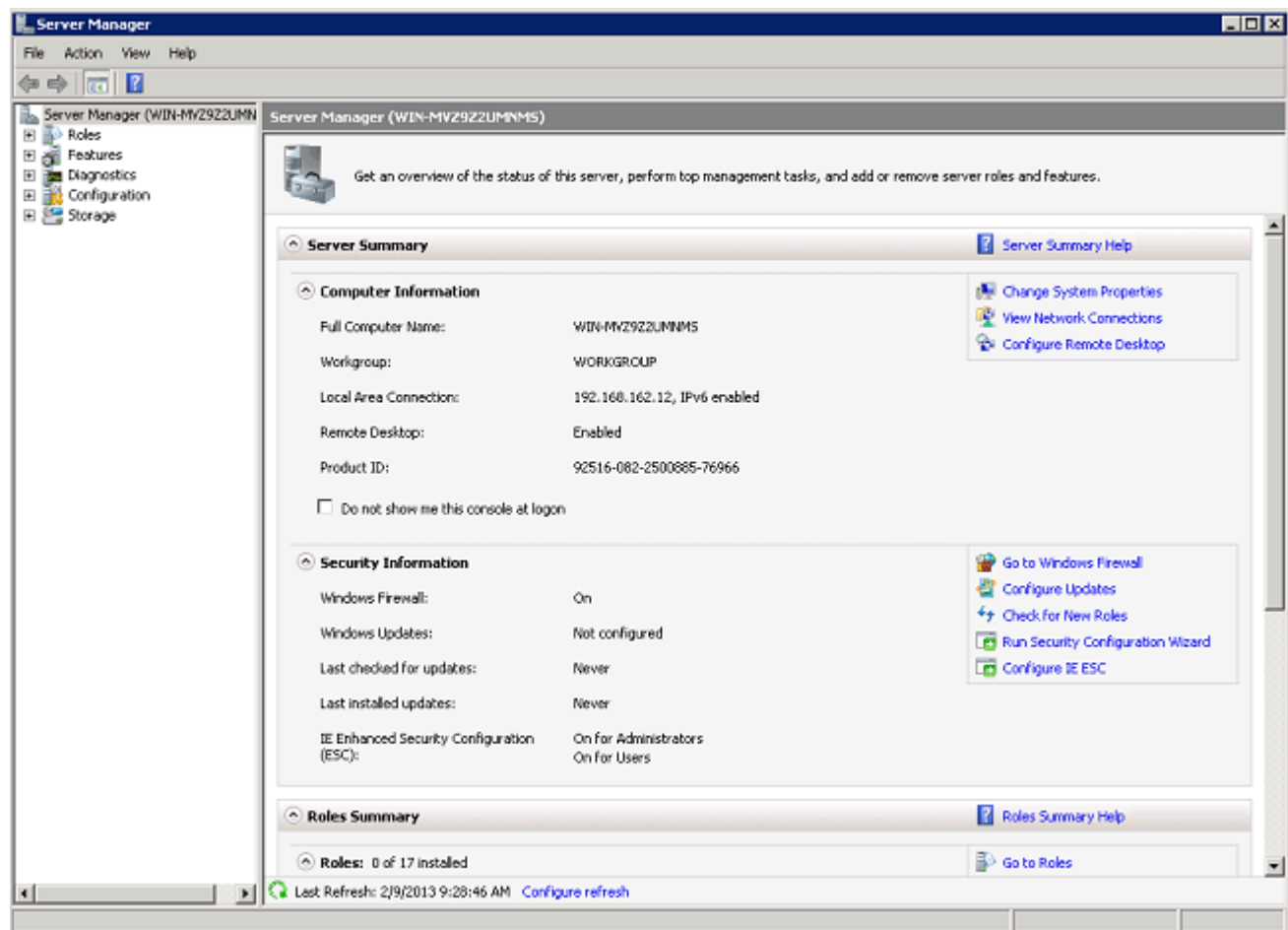
20. Start de server opnieuw op zodat de wijzigingen van kracht worden.



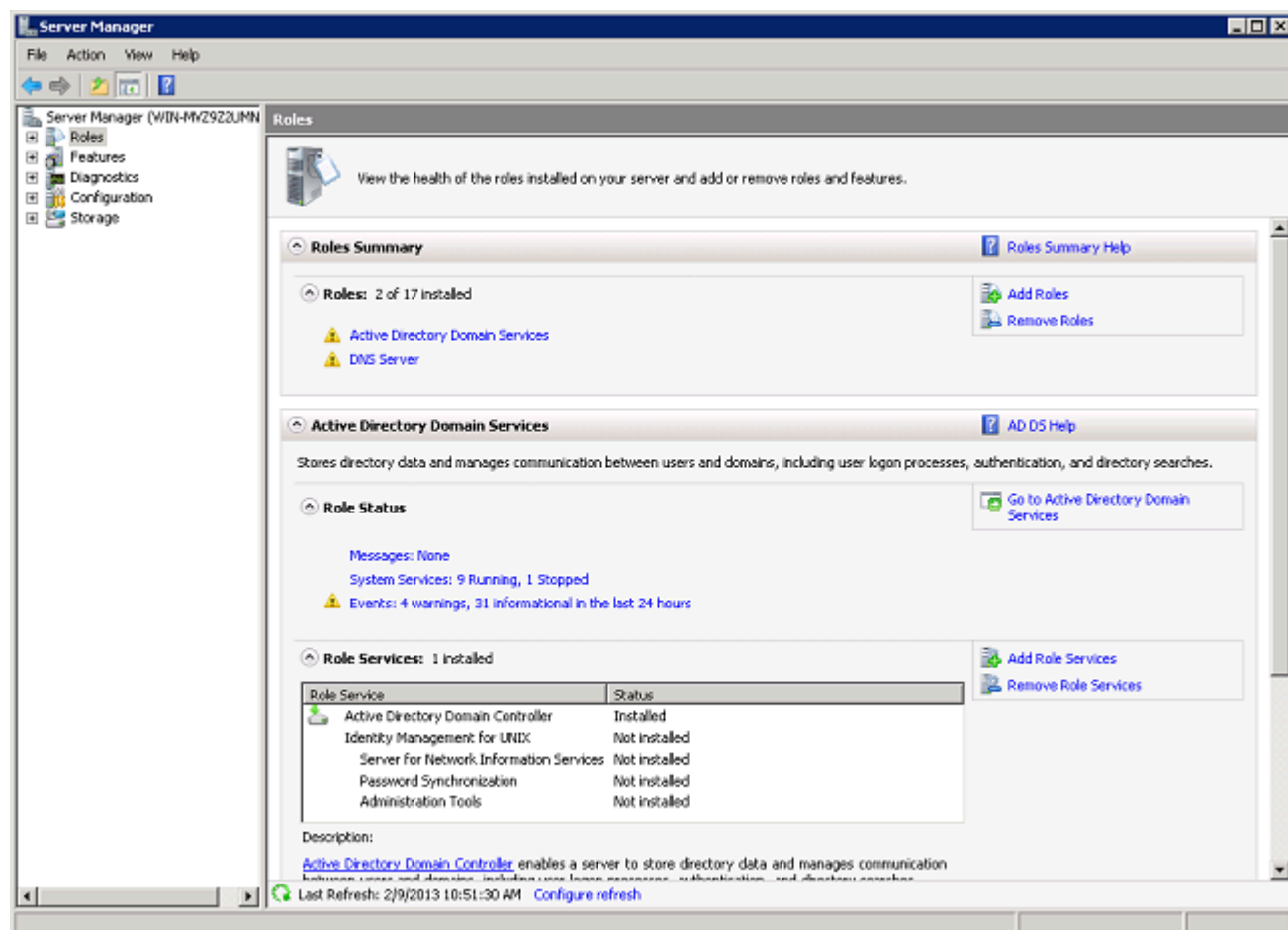
DHCP-services installeren en configureren op de Microsoft Windows 2008-server

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).

Add Roles Wizard

 **Before You Begin**

Before You Begin

Server Roles

Confirmation

Progress

Results

This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.

Before you continue, verify that:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

☐ Skip this page by default

< Previous **Next >** Install Cancel

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

Add Roles Wizard

 **Select Server Roles**

Before You Begin

Server Roles

- DHCP Server
 - Network Connection Bindings
 - IPv4 DNS Settings
 - IPv4 WINS Settings
 - DHCP Scopes
 - DHCPv6 Stateless Mode
 - IPv6 DNS Settings
 - DHCP Server Authorization
- Confirmation
- Progress
- Results

Select one or more roles to install on this server.

Roles:

- ☐ Active Directory Certificate Services
- ☒ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☒ **DHCP Server**
- ☒ DNS Server (Installed)
- ☐ Fax Server
- ☐ File Services
- ☐ Network Policy and Access Services
- ☐ Print Services
- ☐ Terminal Services
- ☐ UDDI Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

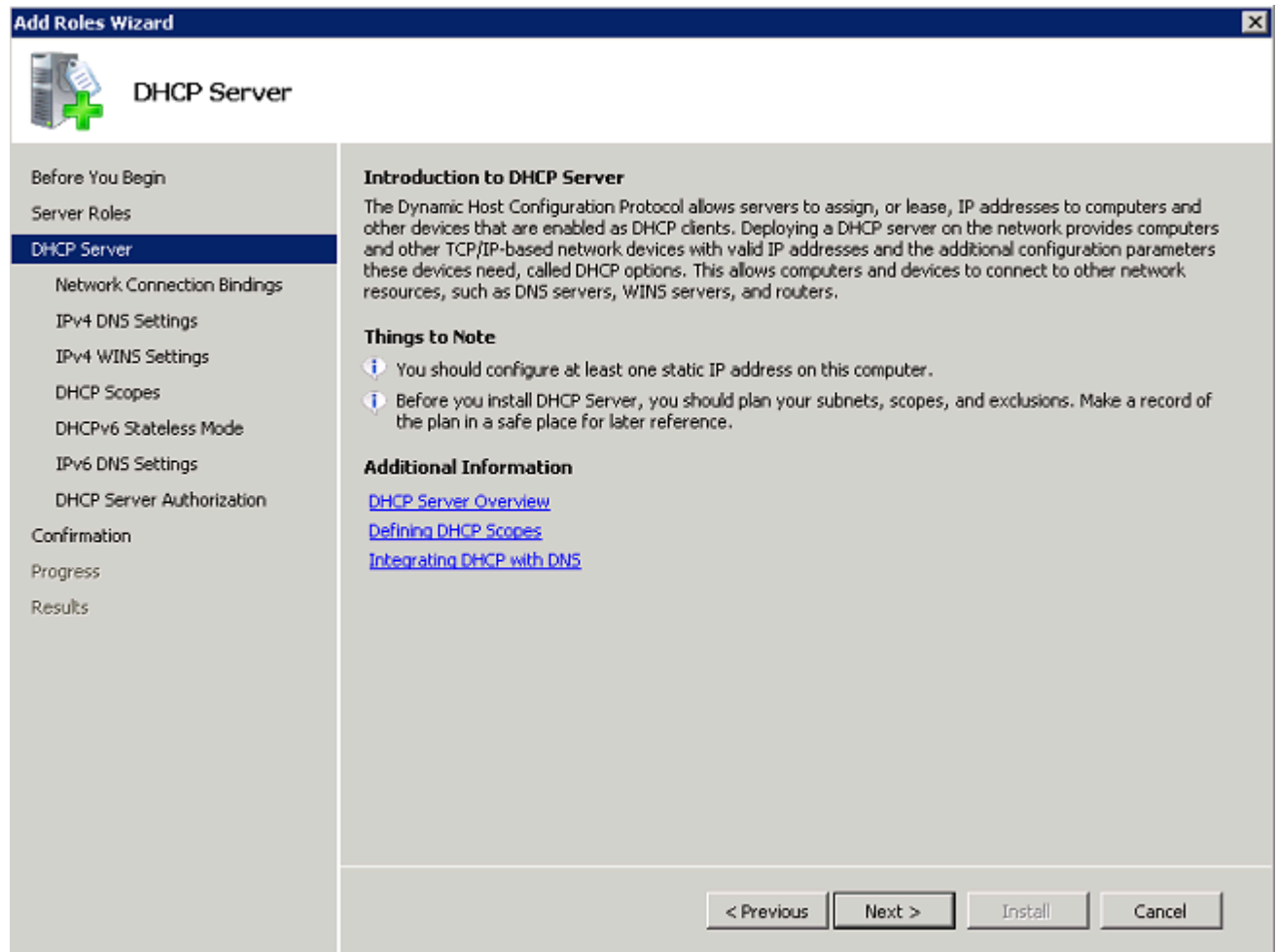
Description:

[Dynamic Host Configuration Protocol \(DHCP\) Server](#) enables you to centrally configure, manage, and provide temporary IP addresses and related information for client computers.

[More about server roles](#)

< Previous Next > Install Cancel

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.

Add Roles Wizard

 **Select Network Connection Bindings**

Before You Begin
Server Roles
DHCP Server
Network Connection Bindings
IPv4 DNS Settings
IPv4 WINS Settings
DHCP Scopes
DHCPv6 Stateless Mode
IPv6 DNS Settings
DHCP Server Authorization
Confirmation
Progress
Results

One or more network connections having a static IP address were detected. Each network connection can be used to service DHCP clients on a separate subnet.

Select the network connections that this DHCP server will use for servicing clients.

Network Connections:

IP Address	Type
☒ 192.168.162.12	IPv4

Details

Name: Local Area Connection
Network Adapter: Intel(R) PRO/1000 MT Desktop Adapter
Physical Address: 08-00-27-3B-2C-A4

< Previous Next > Install Cancel

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

Add Roles Wizard

 **Specify IPv4 DNS Server Settings**

Before You Begin

Server Roles

DHCP Server

Network Connection Bindings

IPv4 DNS Settings

IPv4 WINS Settings

DHCP Scopes

DHCPv6 Stateless Mode

IPv6 DNS Settings

DHCP Server Authorization

Confirmation

Progress

Results

When clients obtain an IP address from the DHCP server, they can be given DHCP options such as the IP addresses of DNS servers and the parent domain name. The settings you provide here will be applied to clients using IPv4.

Specify the name of the parent domain that clients will use for name resolution. This domain will be used for all scopes you create on this DHCP server.

Parent Domain:

Specify the IP addresses of the DNS servers that clients will use for name resolution. These DNS servers will be used for all scopes you create on this DHCP server.

Preferred DNS Server IPv4 Address:

Alternate DNS Server IPv4 Address:

[More about DNS server settings](#)

8. Configureren van WINS als het netwerk WINS ondersteunt.

Add Roles Wizard

 **Specify IPv4 WINS Server Settings**

Before You Begin

Server Roles

DHCP Server

Network Connection Bindings

IPv4 DNS Settings

IPv4 WINS Settings

DHCP Scopes

DHCPv6 Stateless Mode

IPv6 DNS Settings

DHCP Server Authorization

Confirmation

Progress

Results

When clients obtain an IP address from the DHCP server, they can be given DHCP options such as the IP addresses of WINS servers. The settings you provide here will be applied to clients using IPv4.

☒ WINS is not required for applications on this network

☐ WINS is required for applications on this network

Specify the IP addresses of the WINS servers that clients will use for name resolution. These WINS servers will be used for all scopes you create on this DHCP server.

Preferred WINS Server IP Address:

Alternate WINS Server IP Address:

[More about WINS server settings](#)

< Previous Next > Install Cancel

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.

Add Roles Wizard

 **Add or Edit DHCP Scopes**

Before You Begin
Server Roles
DHCP Server
 Network Connection Bindings
 IPv4 DNS Settings
 IPv4 WINS Settings
DHCP Scopes
 DHCPv6 Stateless Mode
 IPv6 DNS Settings
 DHCP Server Authorization
Confirmation
Progress
Results

A scope is the range of possible IP addresses for a network. The DHCP server cannot distribute IP addresses to clients until a scope is created.

Scopes:

Name	IP Address Range
------	------------------

Add...
Edit...
Delete

Properties
Add or select a scope to view its properties.

[More about adding scopes](#)

< Previous Next > Install Cancel

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

Add Roles Wizard

 **Configure DHCPv6 Stateless Mode**

Before You Begin

Server Roles

DHCP Server

Network Connection Bindings

IPv4 DNS Settings

IPv4 WINS Settings

DHCP Scopes

DHCPv6 Stateless Mode

IPv6 DNS Settings

DHCP Server Authorization

Confirmation

Progress

Results

DHCP Server supports the DHCPv6 protocol for servicing IPv6 clients. Using DHCPv6, clients can automatically configure their own IPv6 addresses using stateless mode, or they can acquire IPv6 addresses in stateful mode from the DHCP server. If routers on your network are configured to support DHCPv6, verify that your selection below matches the router configuration.

Select the DHCPv6 stateless mode configuration for this server.

☒ Enable DHCPv6 stateless mode for this server
IPv6 clients will be automatically configured without using this DHCP server.

☐ Disable DHCPv6 stateless mode for this server
After installing DHCP Server, you can configure the DHCPv6 mode using the DHCP Management console.

[More about DHCPv6 stateless mode](#)

< Previous Next > Install Cancel

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

Add Roles Wizard

Specify IPv6 DNS Server Settings



Before You Begin

Server Roles

DHCP Server

- Network Connection Bindings
- IPv4 DNS Settings
- IPv4 WINS Settings
- DHCP Scopes
- DHCPv6 Stateless Mode
- IPv6 DNS Settings**
- DHCP Server Authorization

Confirmation

Progress

Results

When clients obtain an IP address from the DHCP server, they can be given DHCP options such as the IP addresses of DNS servers and the parent domain name. The settings you provide here will be applied to clients using IPv6.

Specify the name of the parent domain that clients will use for name resolution. This domain will be used for all scopes you create on this stateless IPv6 DHCP server.

Parent Domain:

Specify the IP addresses of the DNS servers that clients will use for name resolution. These DNS servers will be used for all scopes you create on this DHCP server.

Preferred DNS Server IPv6 Address:

Alternate DNS Server IPv6 Address:

[More about DNS server settings](#)

< Previous Next > Install Cancel

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

Add Roles Wizard

Authorize DHCP Server



Before You Begin

Server Roles

DHCP Server

- Network Connection Bindings
- IPv4 DNS Settings
- IPv4 WINS Settings
- DHCP Scopes
- DHCPv6 Stateless Mode
- IPv6 DNS Settings
- DHCP Server Authorization**

Confirmation

Progress

Results

Active Directory Domain Services (AD DS) stores a list of DHCP servers that are authorized to service clients on the network. Authorizing DHCP servers helps avoid accidental damage caused by running DHCP servers with incorrect configurations or DHCP servers with correct configurations on the wrong network.

Specify credentials to use for authorizing this DHCP server in AD DS.

☒ Use current credentials

The credentials of the current user will be used to authorize this DHCP server in AD DS.

User Name:

☐ Use alternate credentials

Specify domain administrator credentials for authorizing this DHCP server in AD DS.

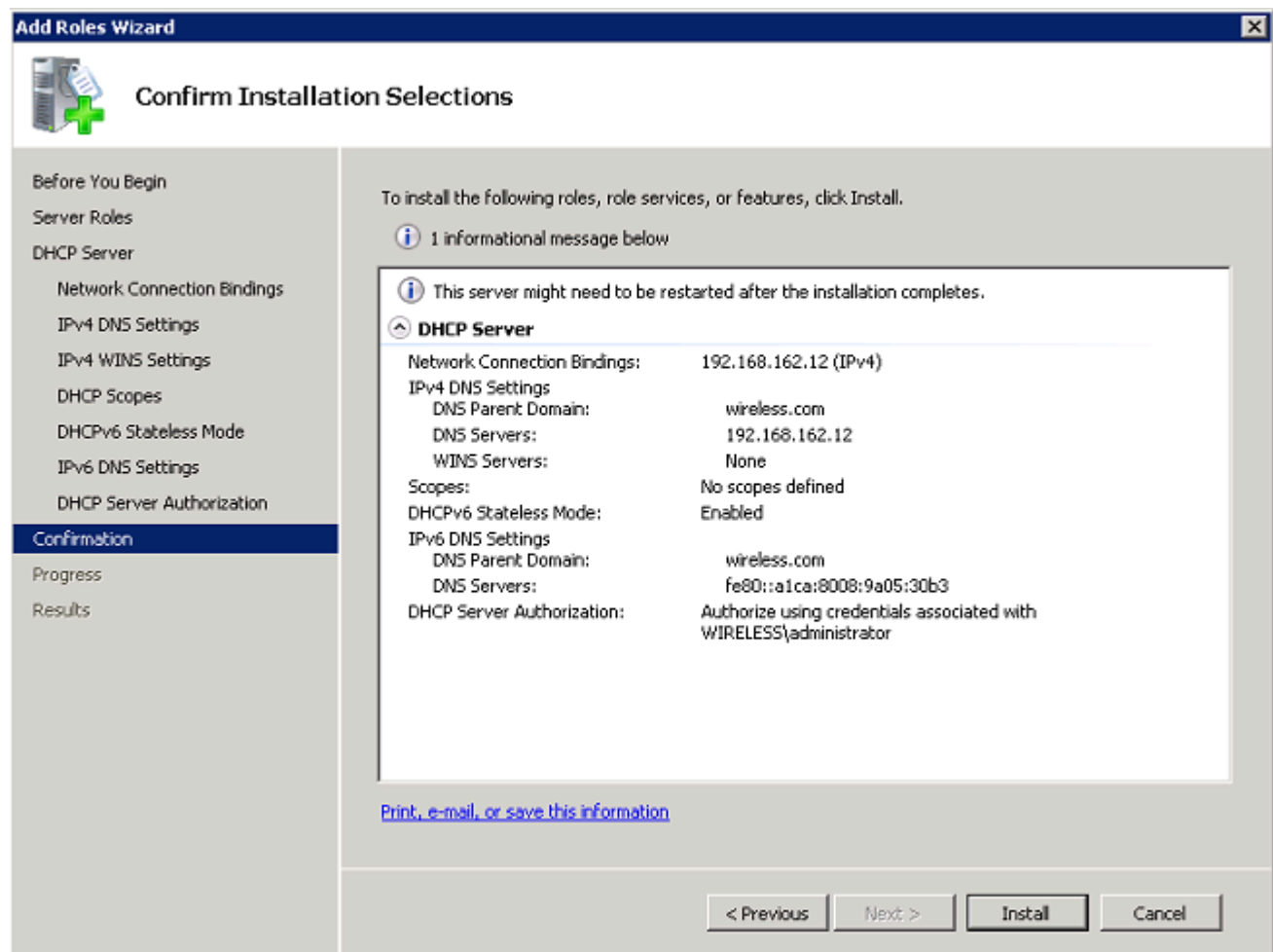
User Name:

☐ Skip authorization of this DHCP server in AD DS

 This DHCP server must be authorized in AD DS before it can service clients.

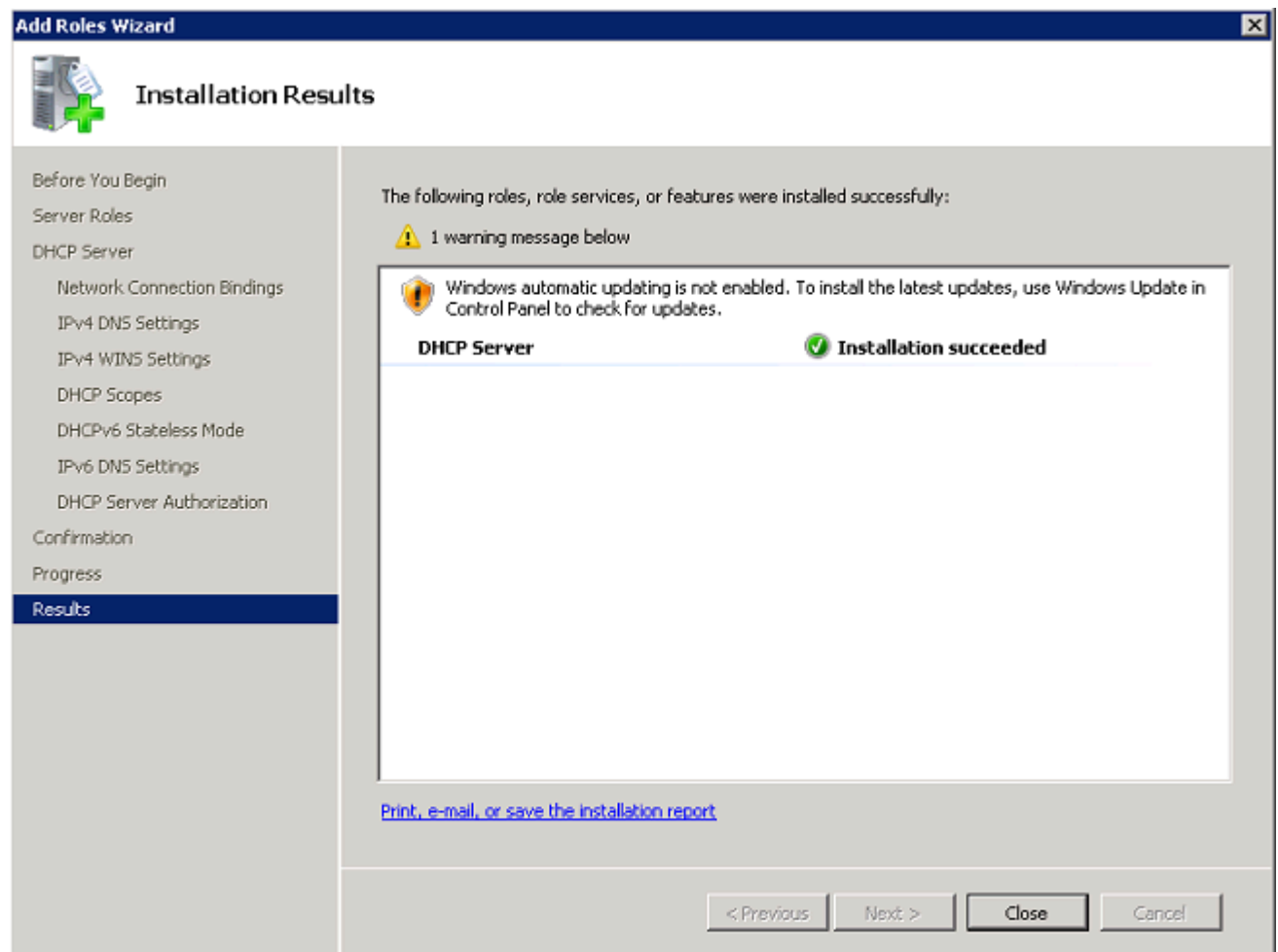
[More about authorizing DHCP servers in AD DS](#)

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



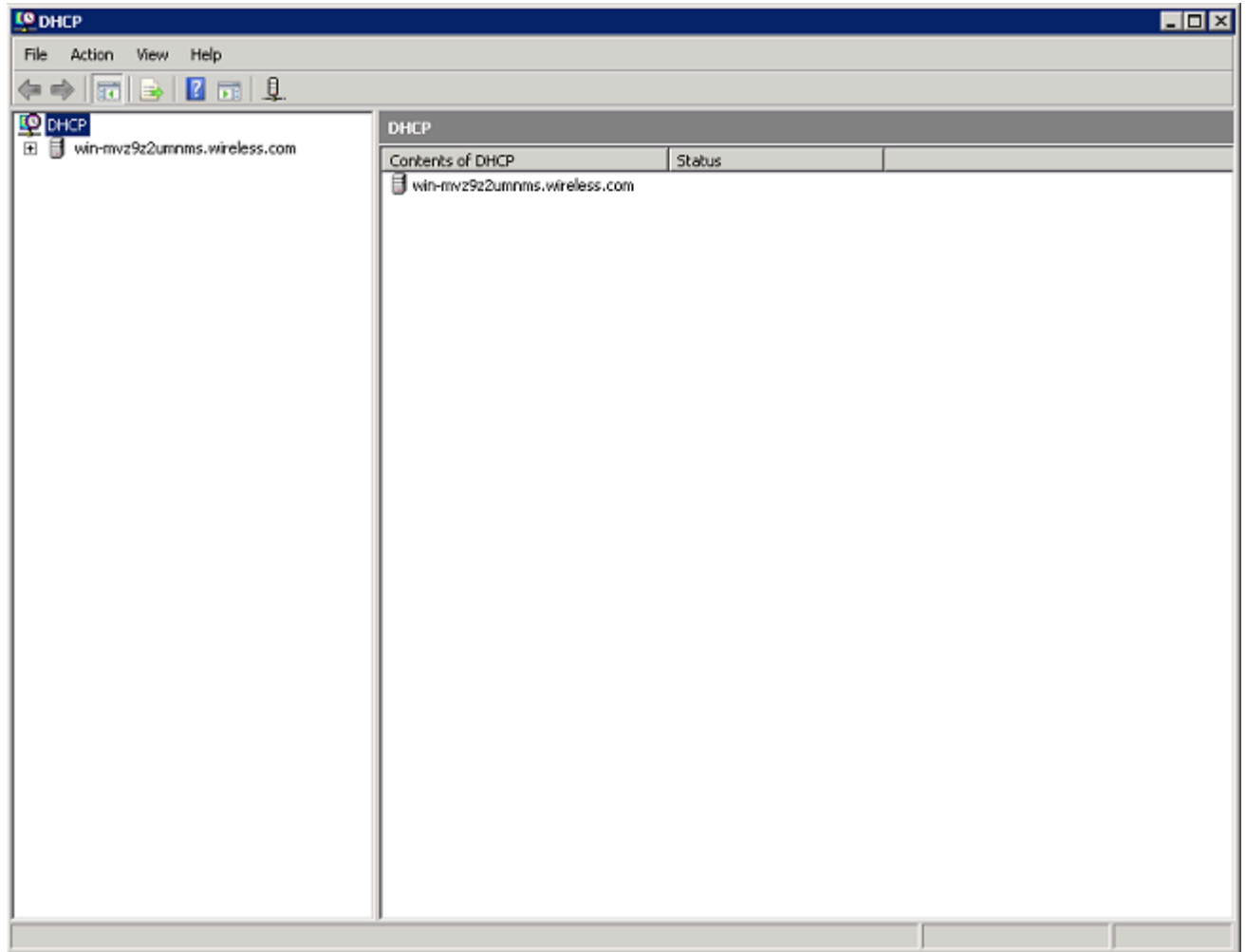
De installatie gaat door.

14. Klik op Sluiten om de wizard te sluiten.

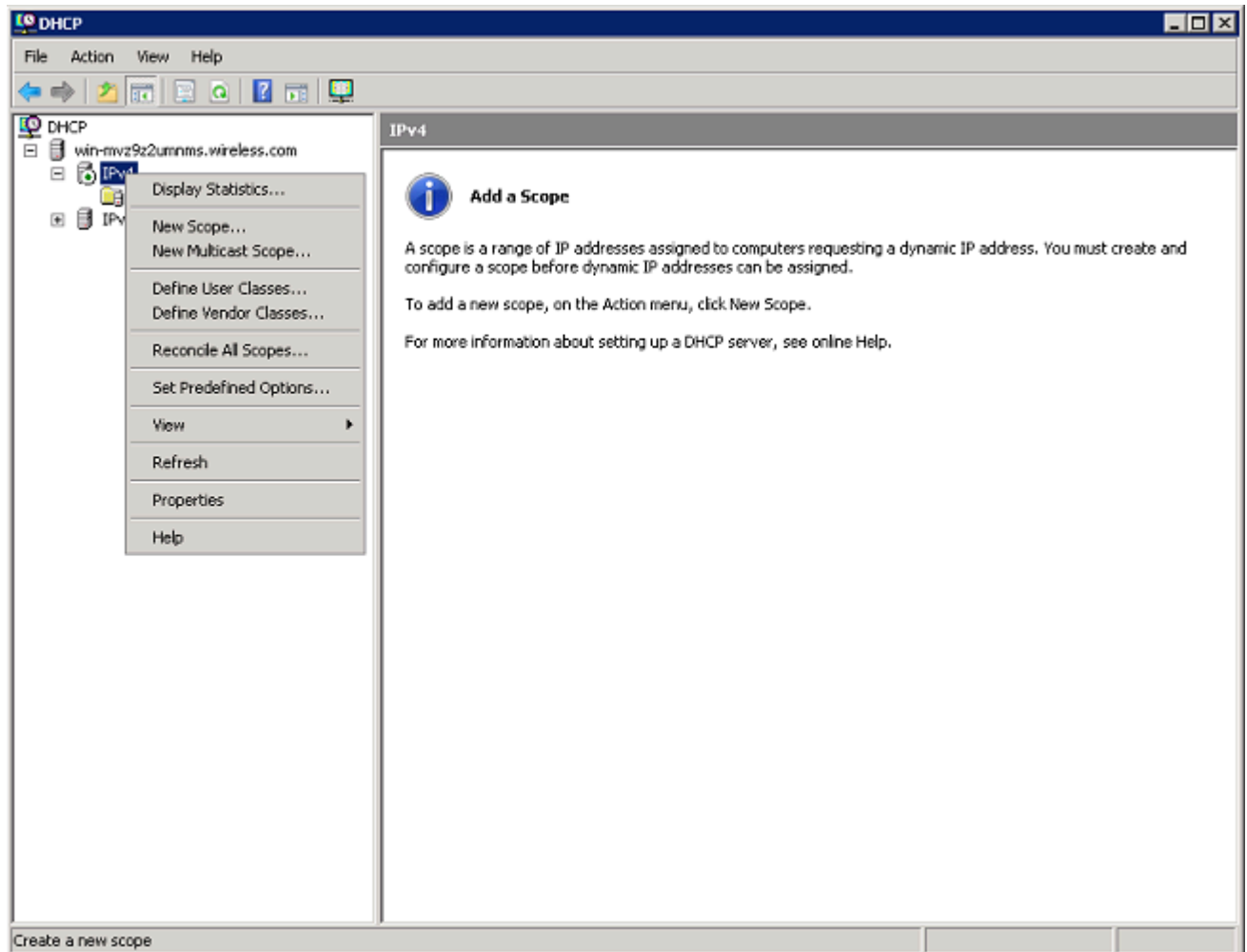


De DHCP-server is nu geïnstalleerd.

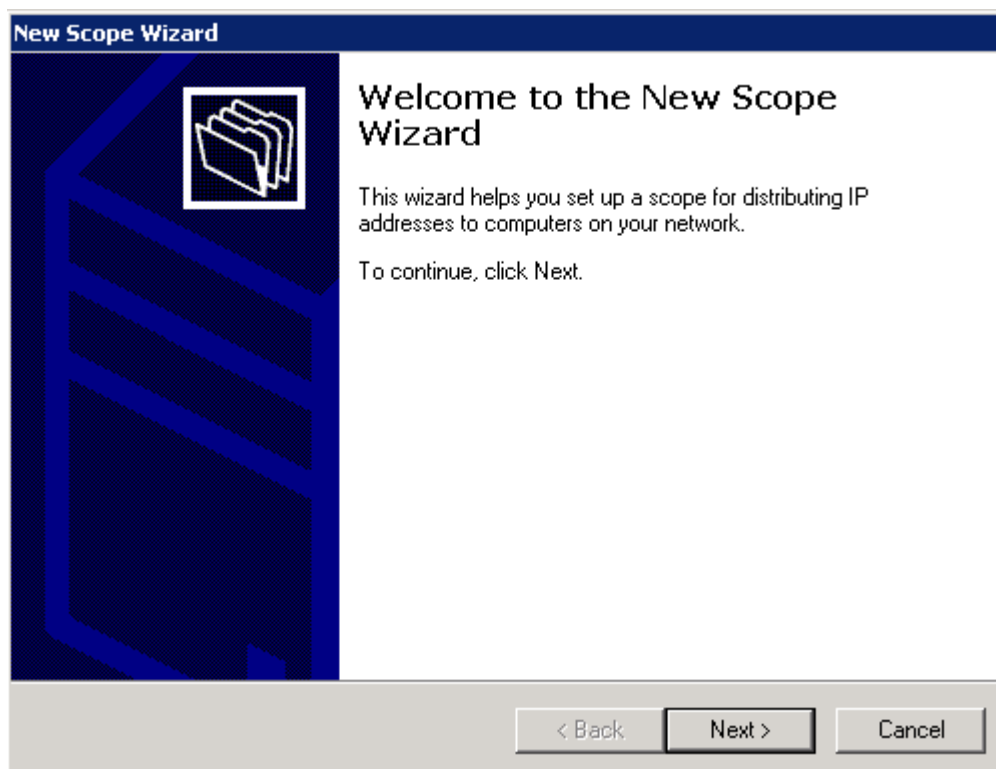
15. Klik op Start > Systeembeheer > DHCP om de DHCP-service te configureren.



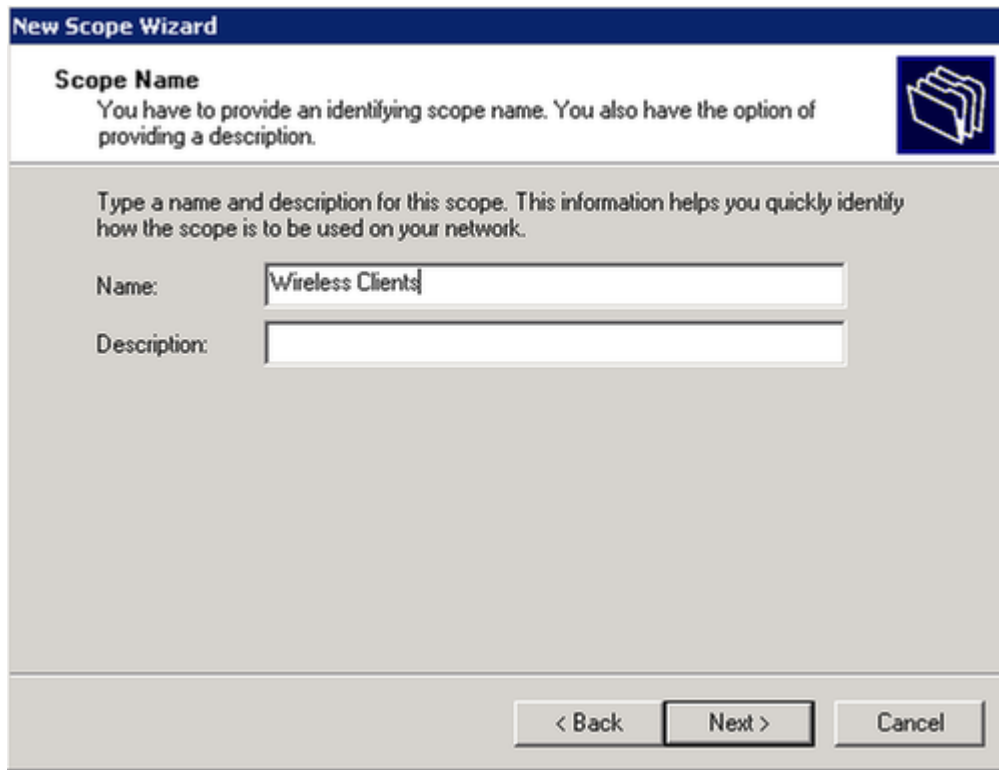
16. Vouw de DHCP-server uit (in de vorige afbeelding voor dit voorbeeld), klik met de rechtermuisknop op IPv4 en kies Nieuw bereik om een DHCP-bereik te maken.



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.



The image shows a 'New Scope Wizard' dialog box. The title bar is dark blue with the text 'New Scope Wizard' in white. The main area has a light gray background. At the top, there is a section titled 'Scope Name' in bold, followed by the text 'You have to provide an identifying scope name. You also have the option of providing a description.' To the right of this text is a small icon of a folder with a document. Below this, there is a paragraph of text: 'Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.' Underneath this text are two input fields. The first is labeled 'Name:' and contains the text 'Wireless Clients'. The second is labeled 'Description:' and is empty. At the bottom of the dialog box, there are three buttons: '< Back', 'Next >', and 'Cancel'.

New Scope Wizard

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

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

Name:

Description:

< Back Next > Cancel

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

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: 192 . 168 . 162 . 100

End IP address: 192 . 168 . 162 . 200

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: 24

Subnet mask: 255 . 255 . 255 . 0

< Back Next > Cancel

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

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.

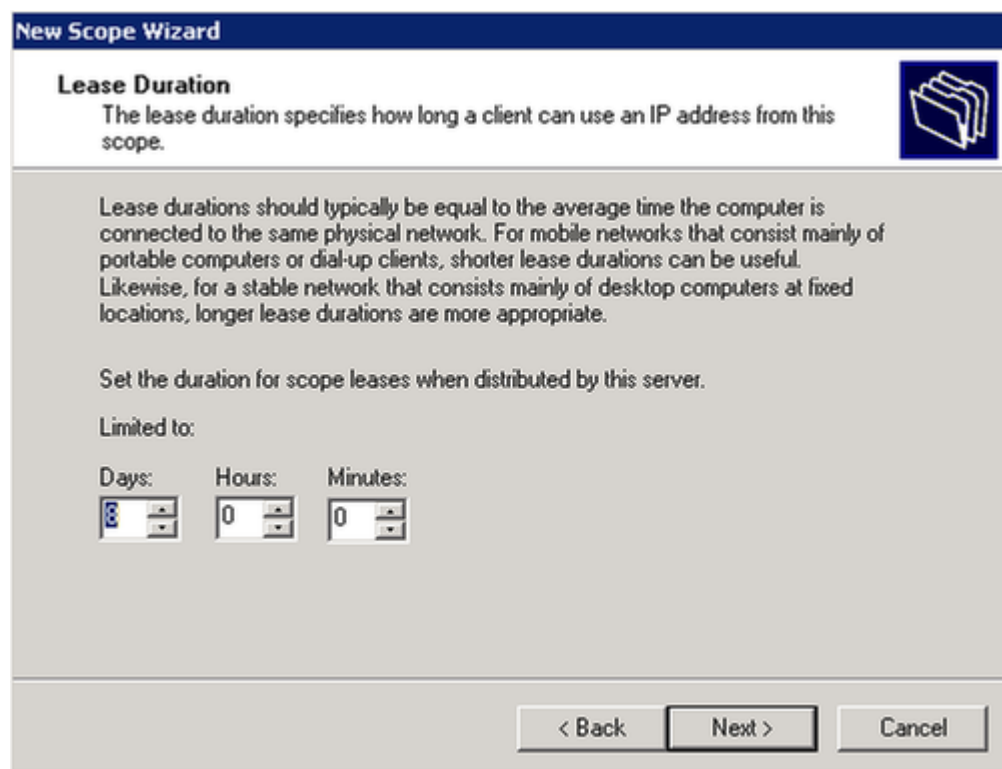
Start IP address: . . . End IP address: . . . Add

Excluded address range:

Remove

< Back Next > Cancel

21. Configureer de leasetijd 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.

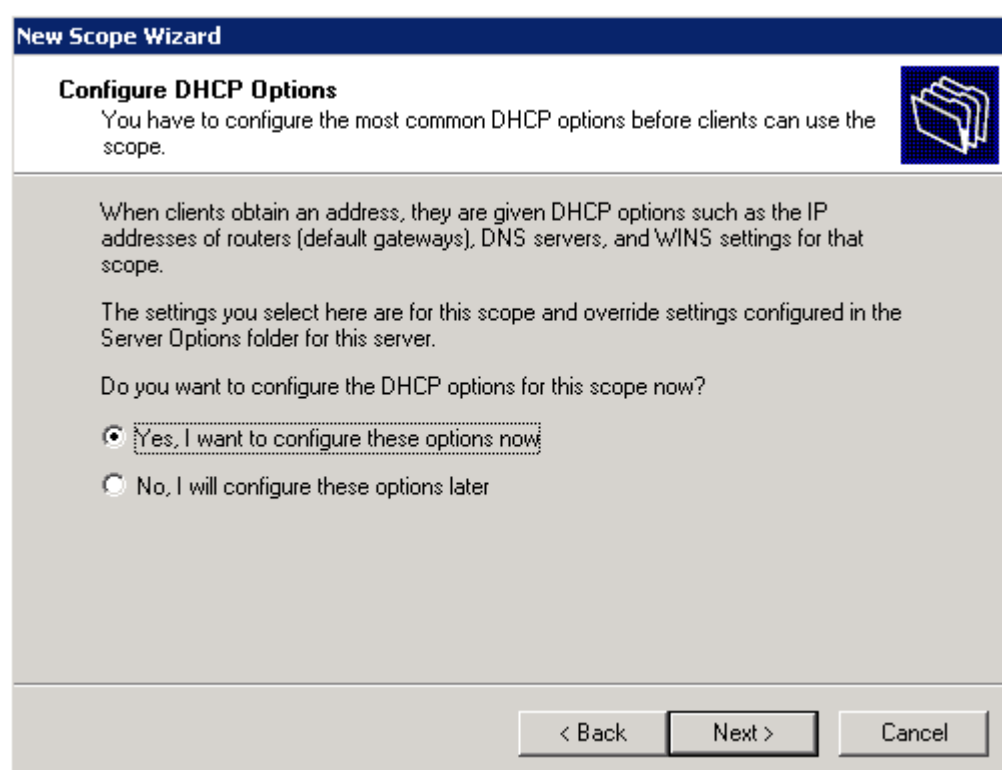
Set the duration for scope leases when distributed by this server.

Limited to:

Days: Hours: Minutes:

< Back Next > Cancel

22. Klik op Ja, ik wil deze opties 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

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

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:

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

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:

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

New Scope Wizard

WINS Servers
Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.

Entering server IP addresses here enables Windows clients to query WINS before they use broadcasts to register and resolve NetBIOS names.

Server name: IP address:

To change this behavior for Windows DHCP clients modify option 046, WINS/NBT Node Type, in Scope Options.

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

New Scope Wizard

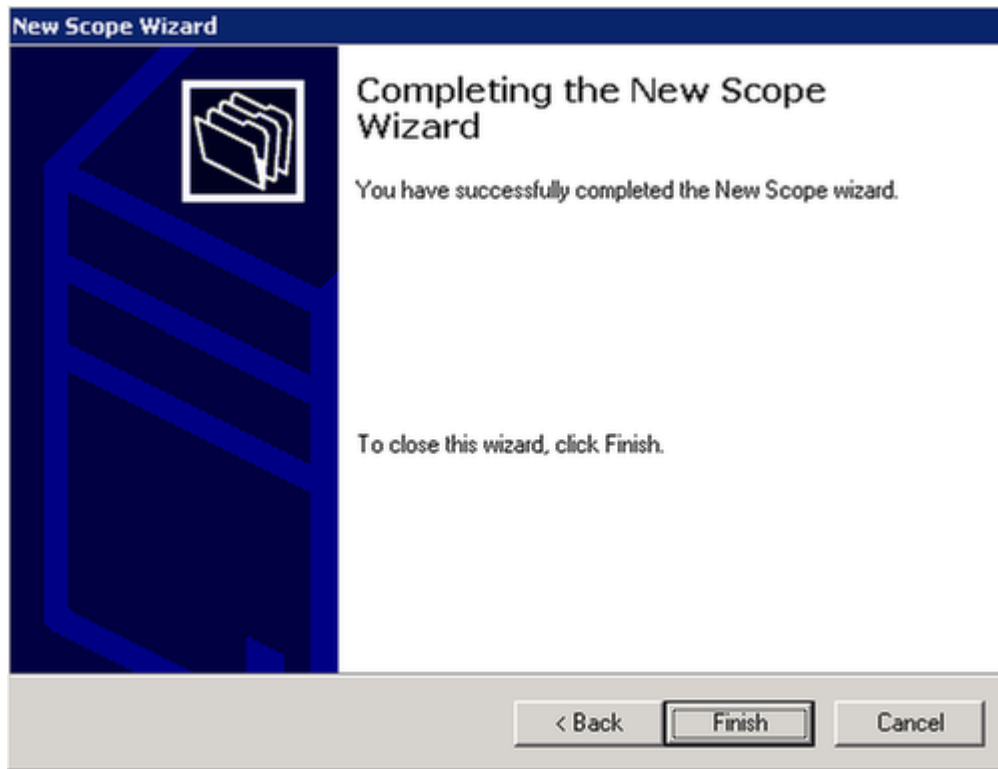
Activate Scope
Clients can obtain address leases only if a scope is activated.

Do you want to activate this scope now?

☒ Yes, I want to activate this scope now

☐ No, I will activate this scope later

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

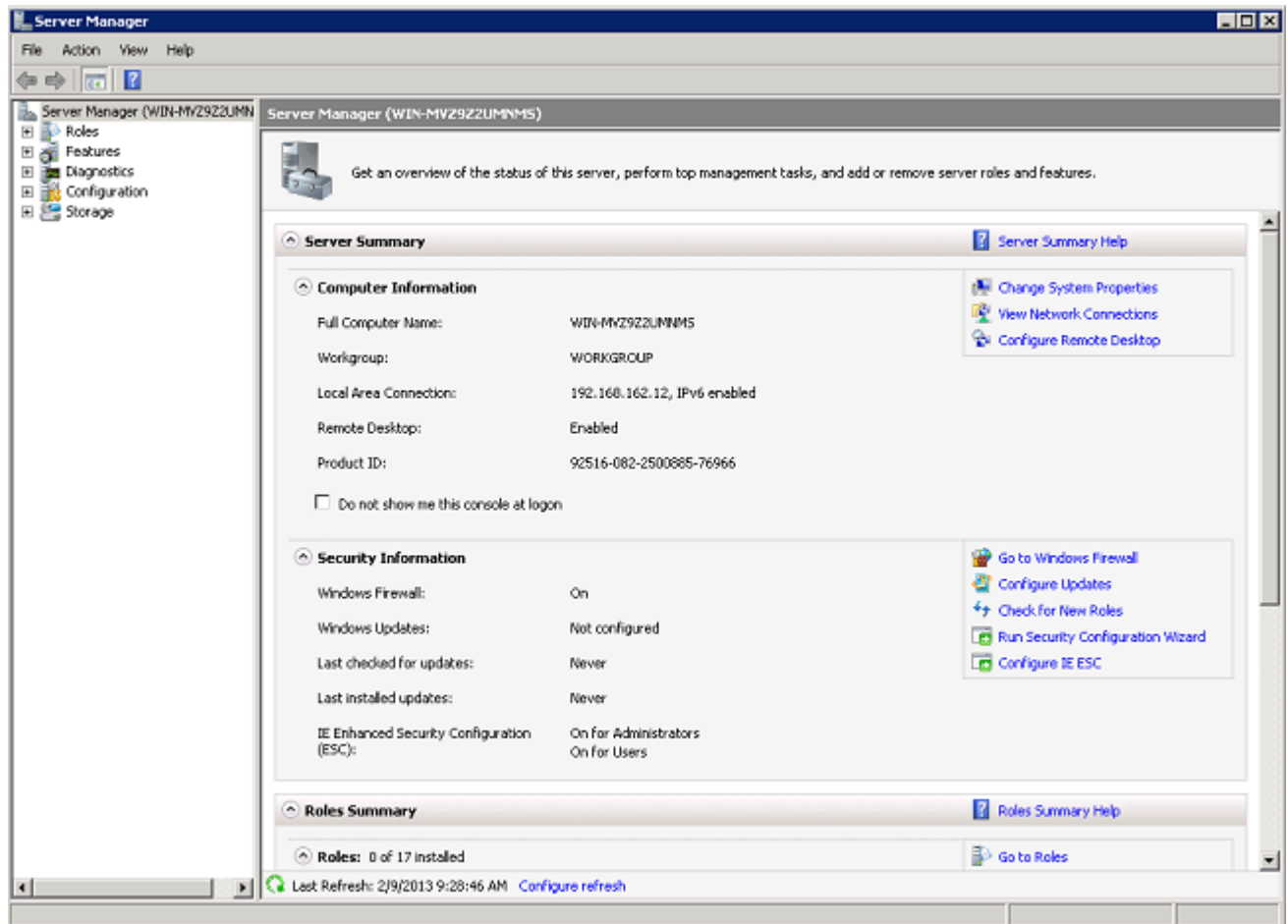


De Microsoft Windows 2008-server als CA-server installeren en configureren

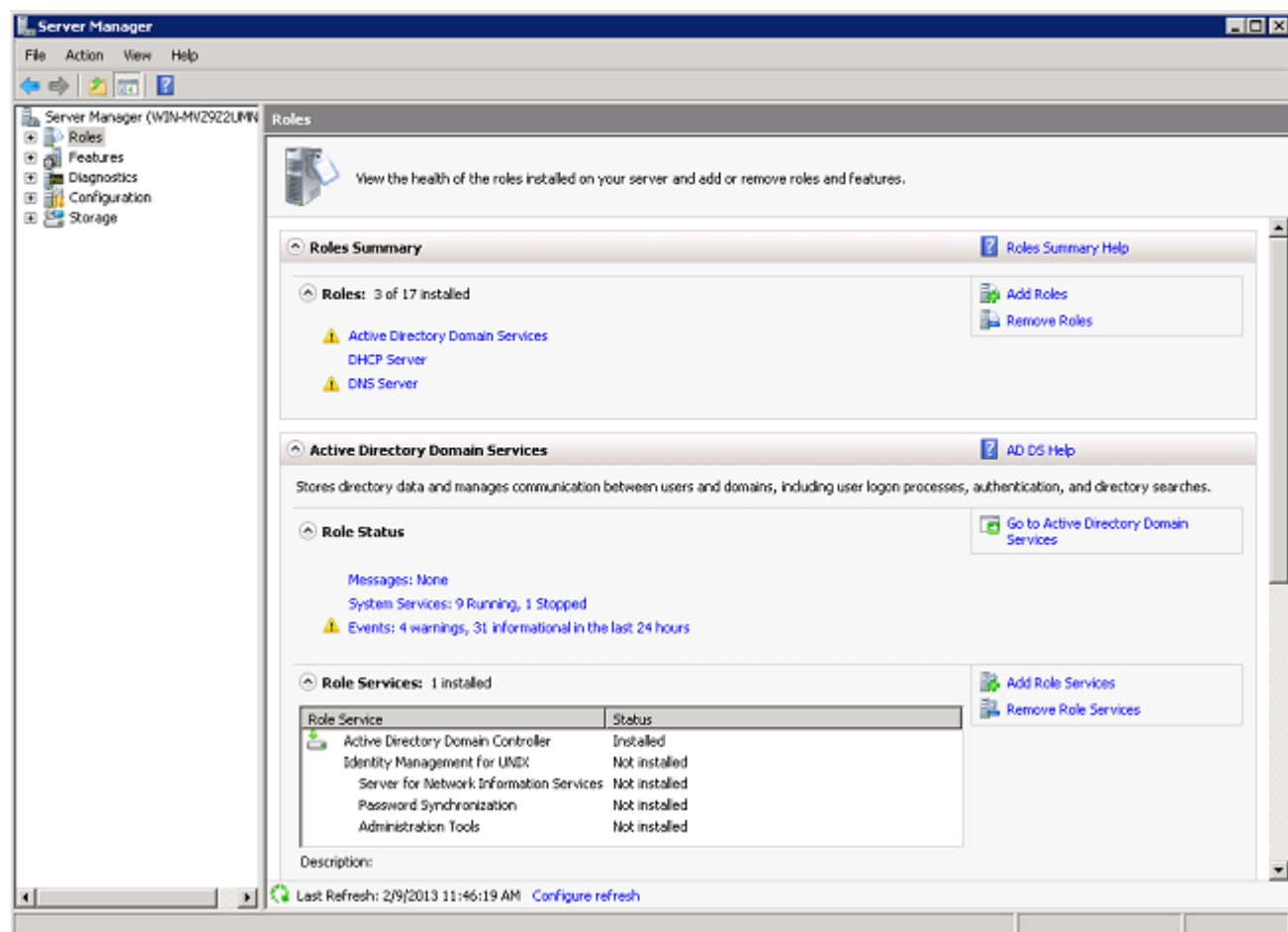
PEAP met EAP-MS-CHAP v2 valideert de RADIUS-server op basis van het certificaat dat op de server aanwezig is. Bovendien moet het servercertificaat worden uitgegeven door een openbare CA die wordt vertrouwd door de clientcomputer (dat wil zeggen dat het openbare CA-certificaat al bestaat in de map Trusted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

Add Roles Wizard

 **Before You Begin**

Before You Begin

Server Roles

Confirmation

Progress

Results

This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.

Before you continue, verify that:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

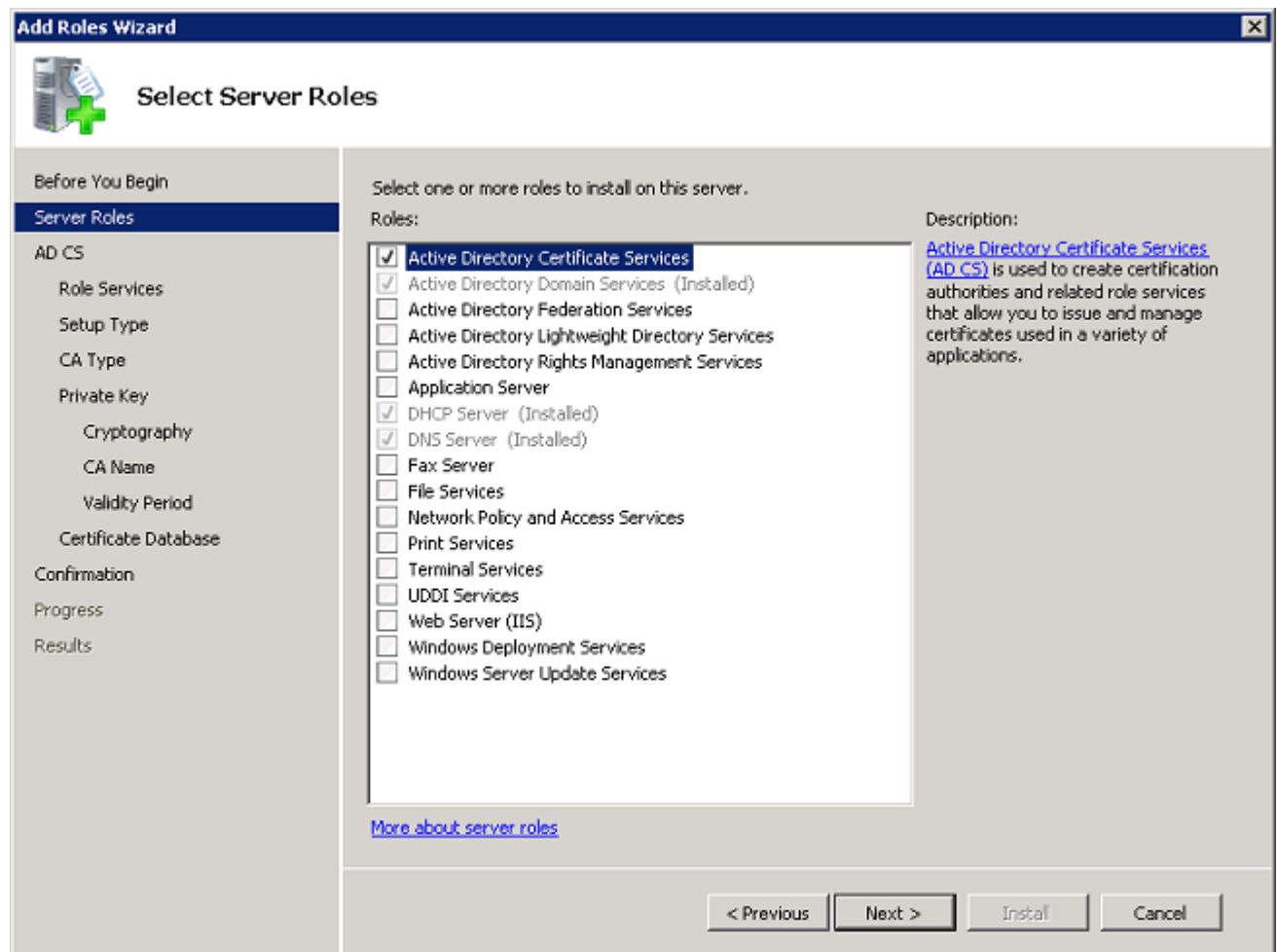
If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

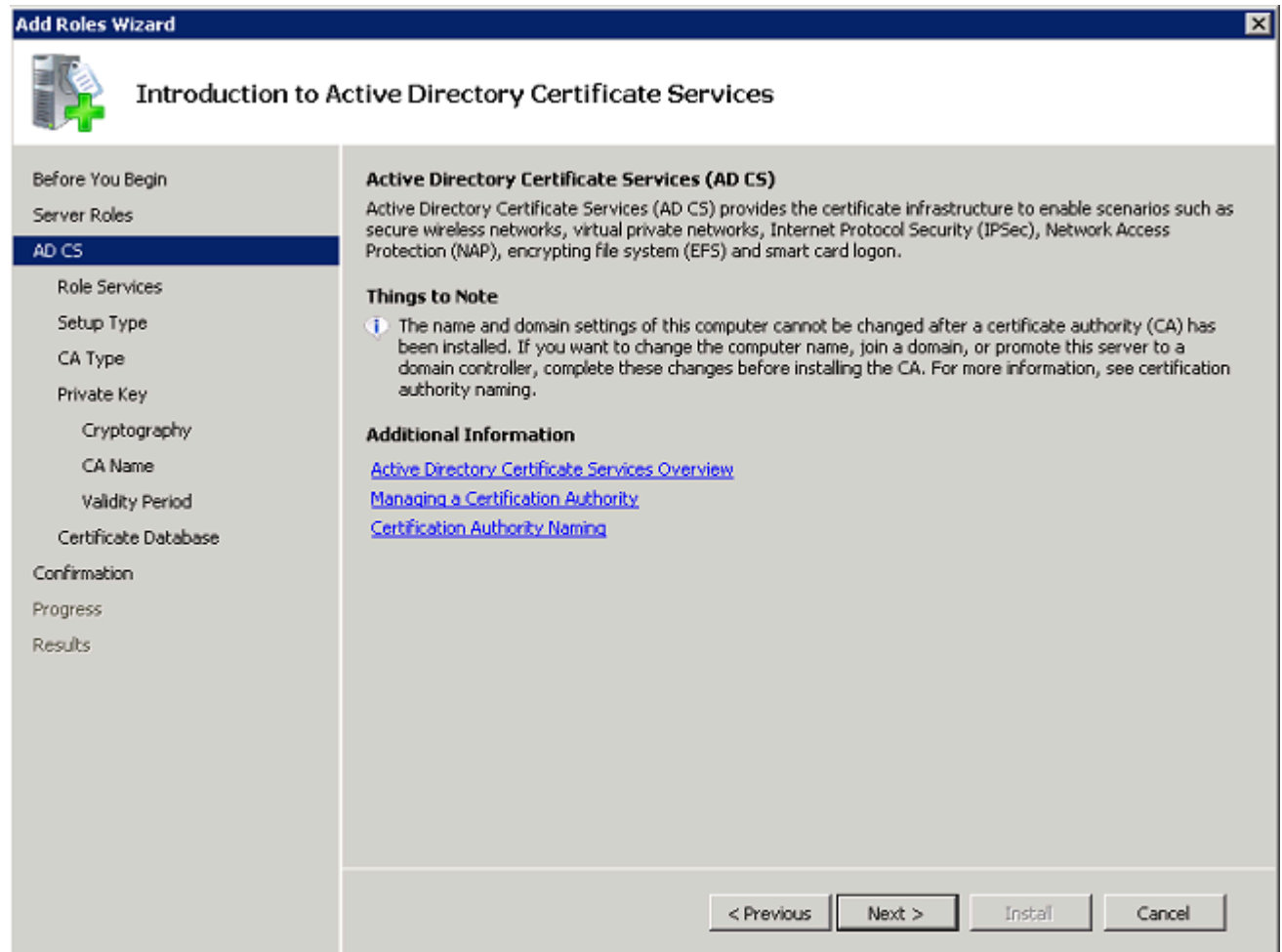
☐ Skip this page by default

< Previous **Next >** Install Cancel

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.

Add Roles Wizard

 **Select Role Services**

Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
 Cryptography
 CA Name
 Validity Period
Certificate Database
Confirmation
Progress
Results

Select the role services to install for Active Directory Certificate Services:

Role services:

☒	Certification Authority
☐	Certification Authority Web Enrollment
☐	Online Responder
☐	Network Device Enrollment Service

Description:
[Certification Authority \(CA\)](#) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.

[More about role services](#)

< Previous Next > Install Cancel

7. Selecteer Enterprise en klik op Volgende.

Add Roles Wizard

 **Specify Setup Type**

Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.

☒ Enterprise
Select this option if this CA is a member of a domain and can use Directory Service to issue and manage certificates.

☐ Standalone
Select this option if this CA does not use Directory Service data to issue or manage certificates. A standalone CA can be a member of a domain.

[More about the differences between enterprise and standalone setup](#)

< Previous Next > Install Cancel

8. Selecteer CA starten en klik op Volgende.

Add Roles Wizard

 **Specify CA Type**

Before You Begin
Server Roles
AD CS
 Role Services
 Setup Type
CA Type
 Private Key
 Cryptography
 CA Name
 Validity Period
 Certificate Database
Confirmation
Progress
Results

A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA.

☒ **Root CA**
Select this option if you are installing the first or only certification authority in a public key infrastructure.

☐ **Subordinate CA**
Select this option if your CA will obtain its CA certificate from another CA higher in a public key infrastructure.

[More about public key infrastructure \(PKI\)](#)

< Previous Next > Install Cancel

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

Add Roles Wizard

 **Set Up Private Key**

Before You Begin

Server Roles

AD CS

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

To generate and issue certificates to clients, a CA must have a private key. Specify whether you want to create a new private key or use an existing one.

☒ **Create a new private key**
Use this option if you don't have a private key or wish to create a new private key to enhance security. You will be asked to select a cryptographic service provider and specify a key length for the private key. To issue new certificates, you must also select a hash algorithm.

☐ **Use existing private key**
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

☒ **Select a certificate and use its associated private key**
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

☐ **Select an existing private key on this computer**
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

[More about public and private keys](#)

< Previous Next > Install Cancel

10. Klik op Volgende op Cryptografie configureren voor CA.

Add Roles Wizard

 **Configure Cryptography for CA**

Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

To create a new private key, you must first select a [cryptographic service provider](#), [hash algorithm](#), and key length that are appropriate for the intended use of the certificates that you issue. Selecting a higher value for key length will result in stronger security, but increase the time needed to complete signing operations.

Select a cryptographic service provider (CSP):
RSA#Microsoft Software Key Storage Provider

Key character length:
2048

Select the hash algorithm for signing certificates issued by this CA:
sha1
md2
md4
sha256

☐ Use strong private key protection features provided by the CSP (this may require administrator interaction every time the private key is accessed by the CA)

[More about cryptographic options for a CA](#)

< Previous Next > Install Cancel

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

Add Roles Wizard

 **Configure CA Name**

Before You Begin
Server Roles
AD CS
 Role Services
 Setup Type
 CA Type
 Private Key
 Cryptography
 CA Name
 Validity Period
 Certificate Database
Confirmation
Progress
Results

Type in a common name to identify this CA. This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA:

Distinguished name suffix:

Preview of distinguished name:

[More about configuring a CA name](#)

< Previous Next > Install Cancel

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

Add Roles Wizard

 **Set Validity Period**

Before You Begin
Server Roles
AD CS
 Role Services
 Setup Type
 CA Type
 Private Key
 Cryptography
 CA Name
Validity Period
 Certificate Database
Confirmation
Progress
Results

A certificate will be issued to this CA to secure communications with other CAs and with clients requesting certificates. The validity period of a CA certificate can be based on a number of factors, including the intended purpose of the CA and security measures that you have taken to secure the CA.

Select validity period for the certificate generated for this CA:
 Years

CA expiration Date: 2/9/2018 11:49 AM
Note that CA will issue certificates valid only until its expiration date.

[More about setting the certificate validity period](#)

< Previous Next > Install Cancel

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

Add Roles Wizard

 **Configure Certificate Database**

Before You Begin

Server Roles

AD CS

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

The certificate database records all certificate requests, issued certificates, and revoked or expired certificates. The database log can be used to monitor management activity for a CA.

Certificate database location:

C:\Windows\system32\CertLog Browse...

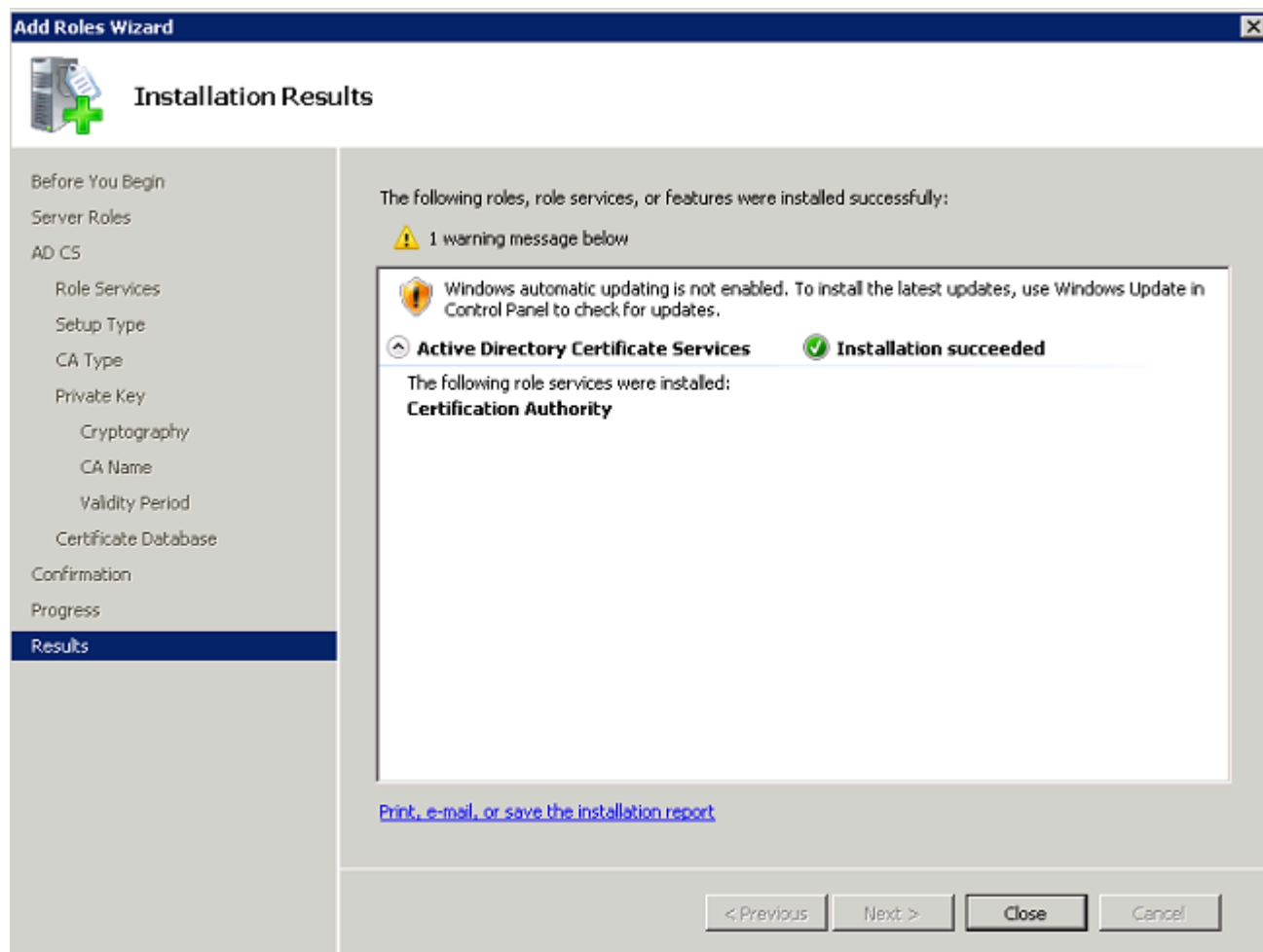
☐ Use existing certificate database from previous installation at this location

Certificate database log location:

C:\Windows\system32\CertLog Browse...

< Previous Next > Install Cancel

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

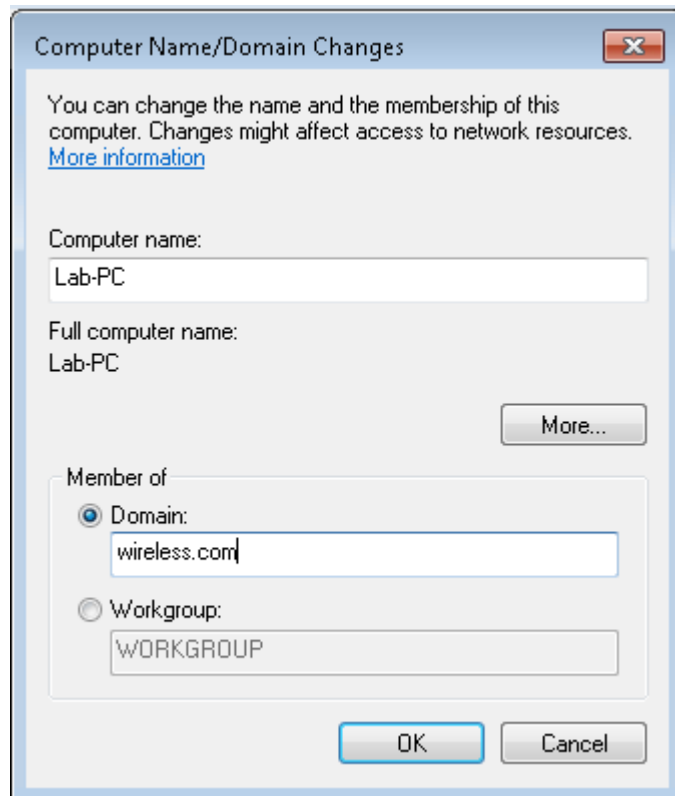


15. Nadat de installatie is voltooid, klikt u op Sluiten.

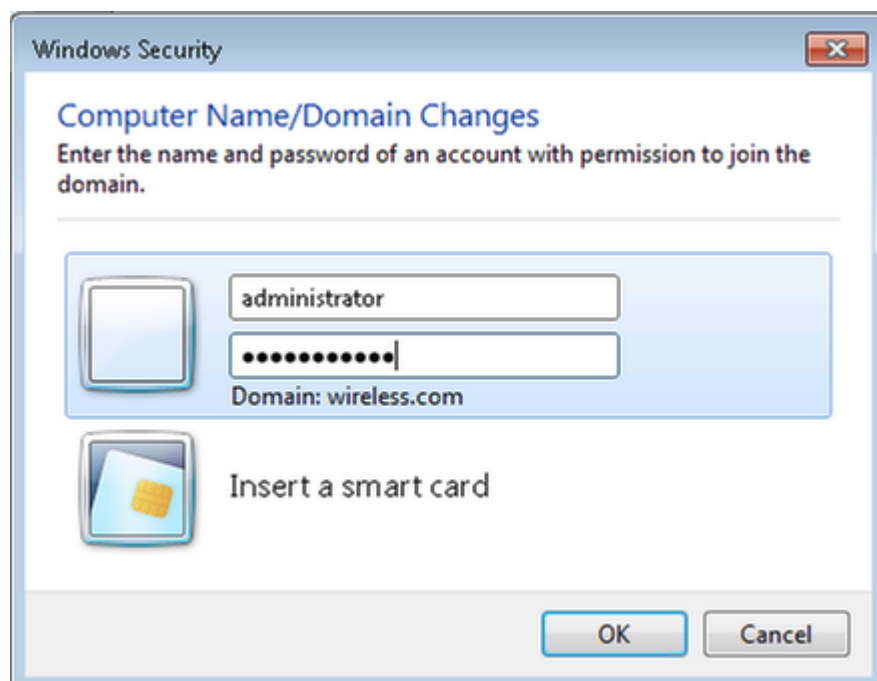
Clënten verbinden met het domein

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.



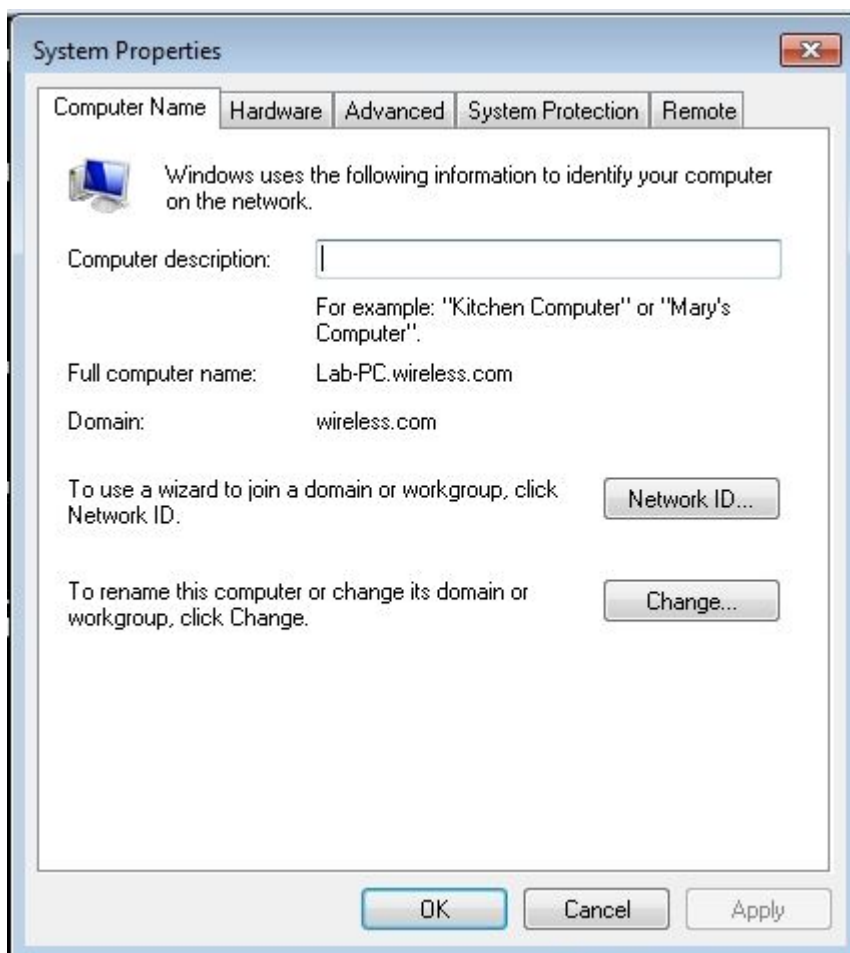
8. Voer de beheerder van de gebruikersnaam en het wachtwoord in dat specifiek is voor het domein waaraan de client deelneemt. Dit is de beheerdersaccount in de Active Directory op de server.



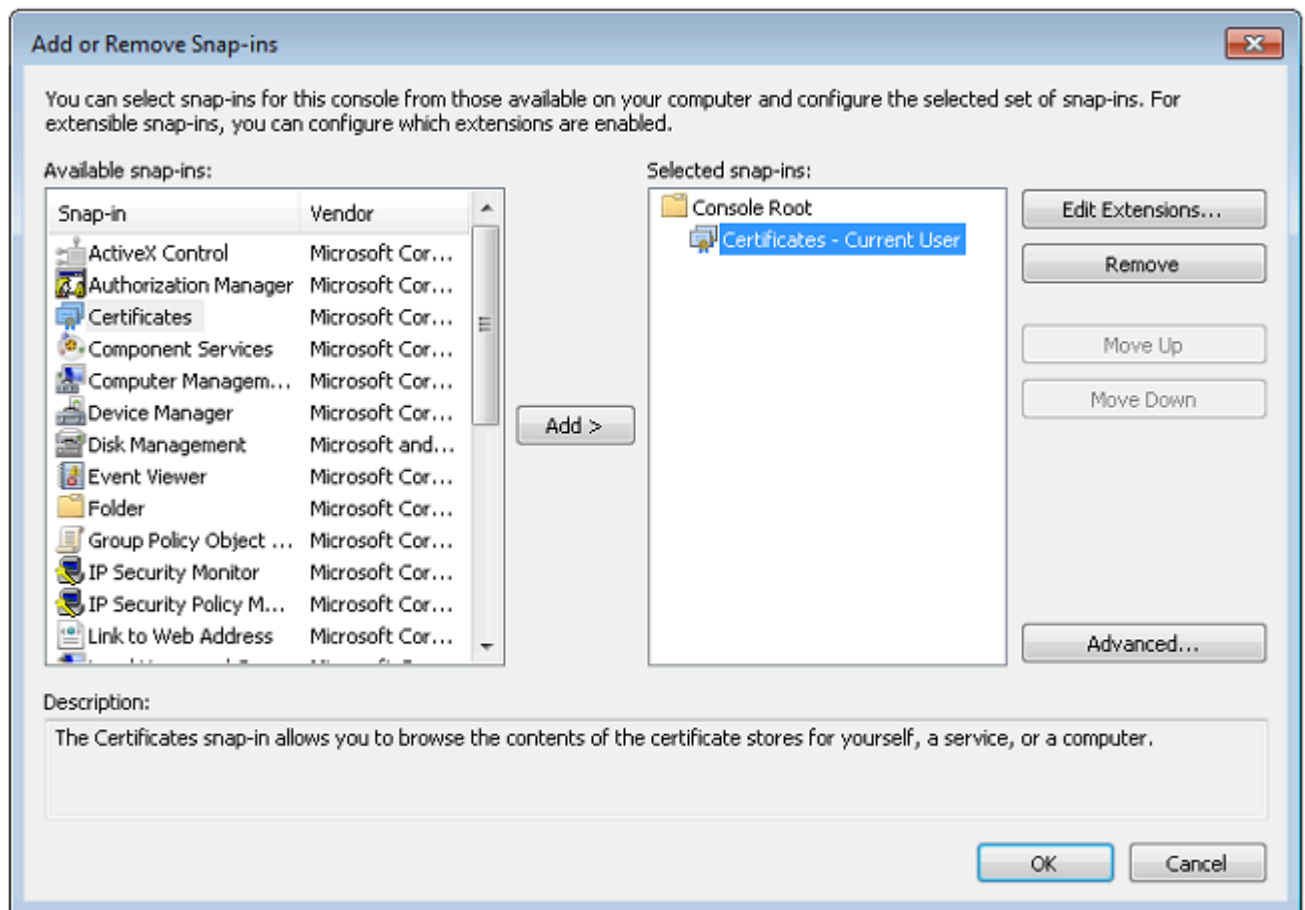
9. Klik op OK en klik nogmaals op OK.



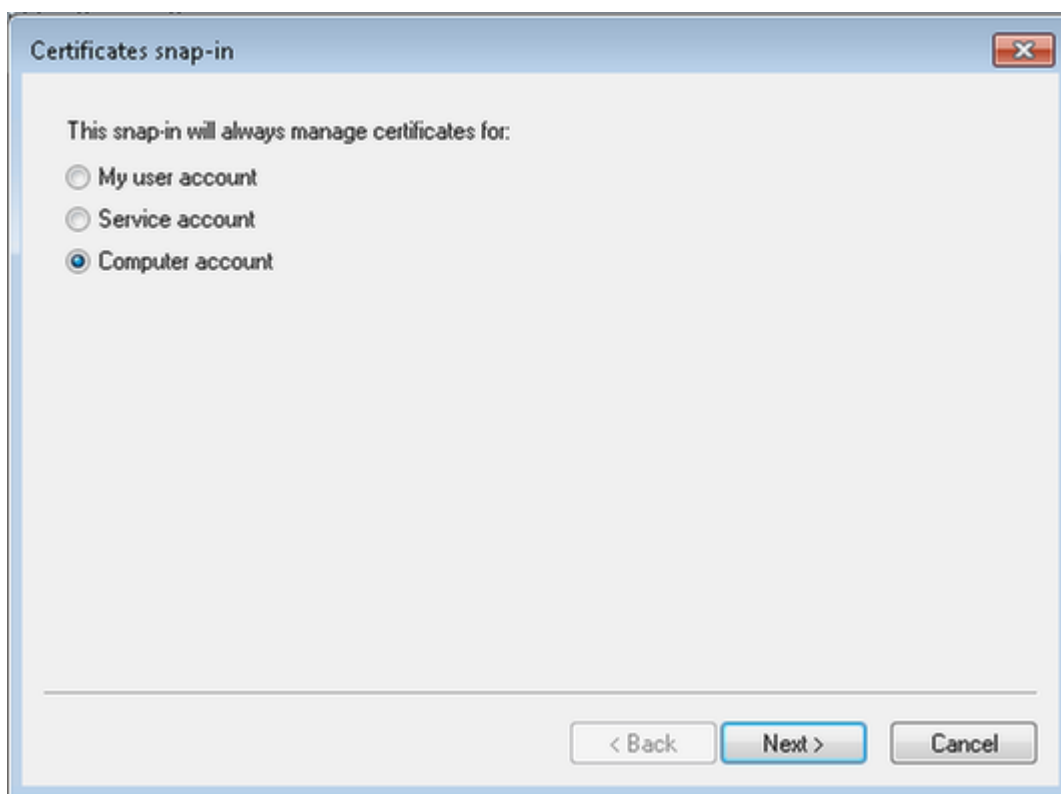
10. Klik op Sluiten>Nu opnieuw starten om de computer opnieuw op te starten.
11. Wanneer de computer opnieuw is opgestart, meldt u zich aan met: Gebruikersnaam = Beheerder; Wachtwoord = <domeinwachtwoord>; Domein = draadloos.
12. Klik op Start, klik met de rechtermuisknop op Computer, kies Eigenschappen 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.



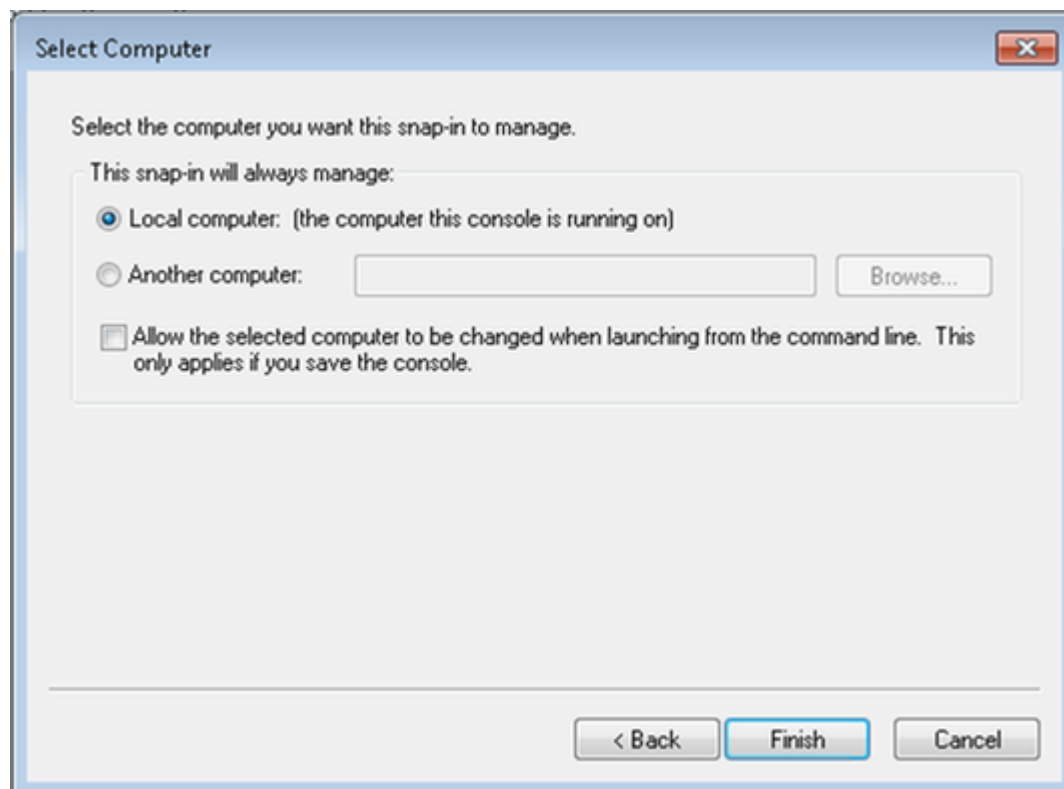
14. Klik op Start, voer mmc in en druk op Enter.
15. Klik op Bestand en klik op Add/Remove snap-in.
16. Kies Certificaten en klik op Toevoegen.



17. Klik op Computeraccount en klik op Volgende.

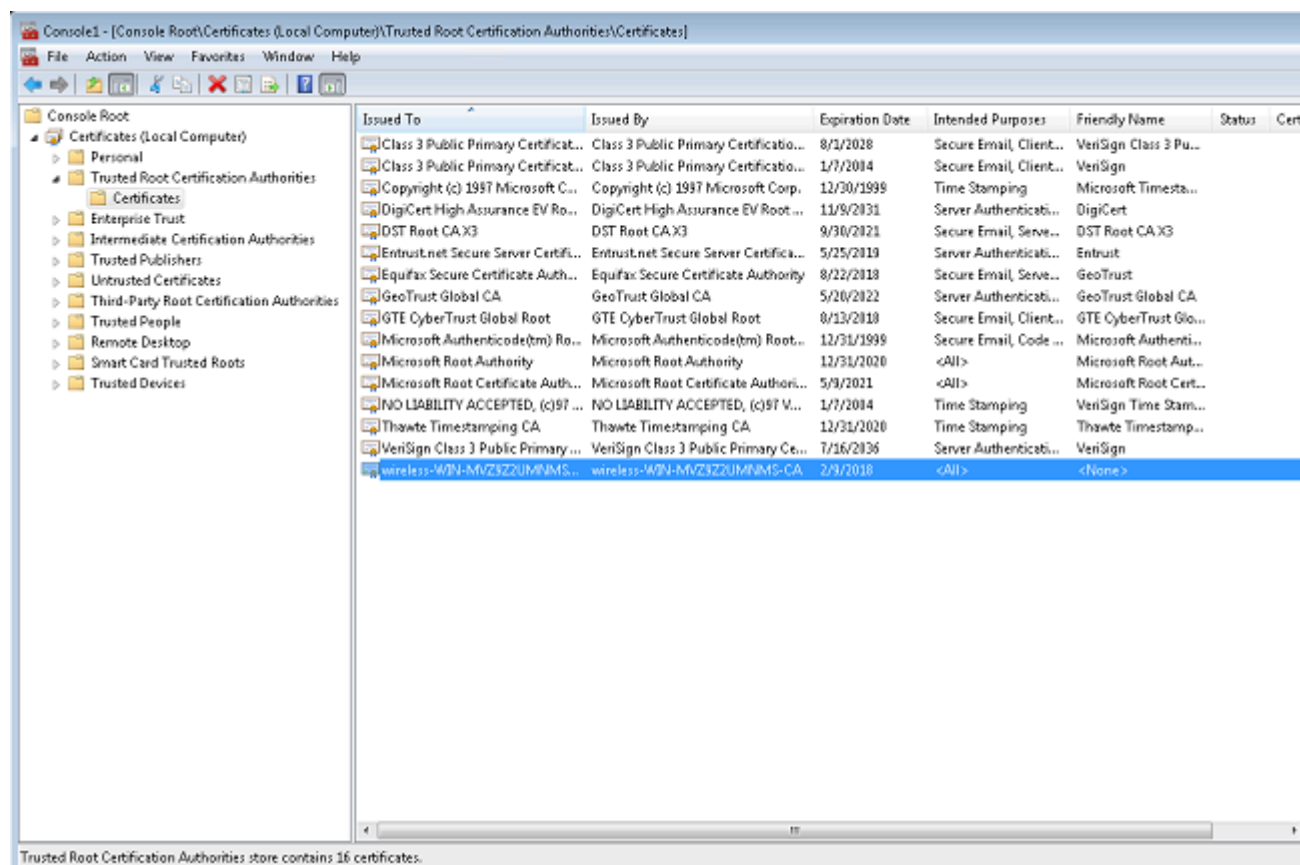


18. Klik op Lokale computer en klik op Volgende.



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.

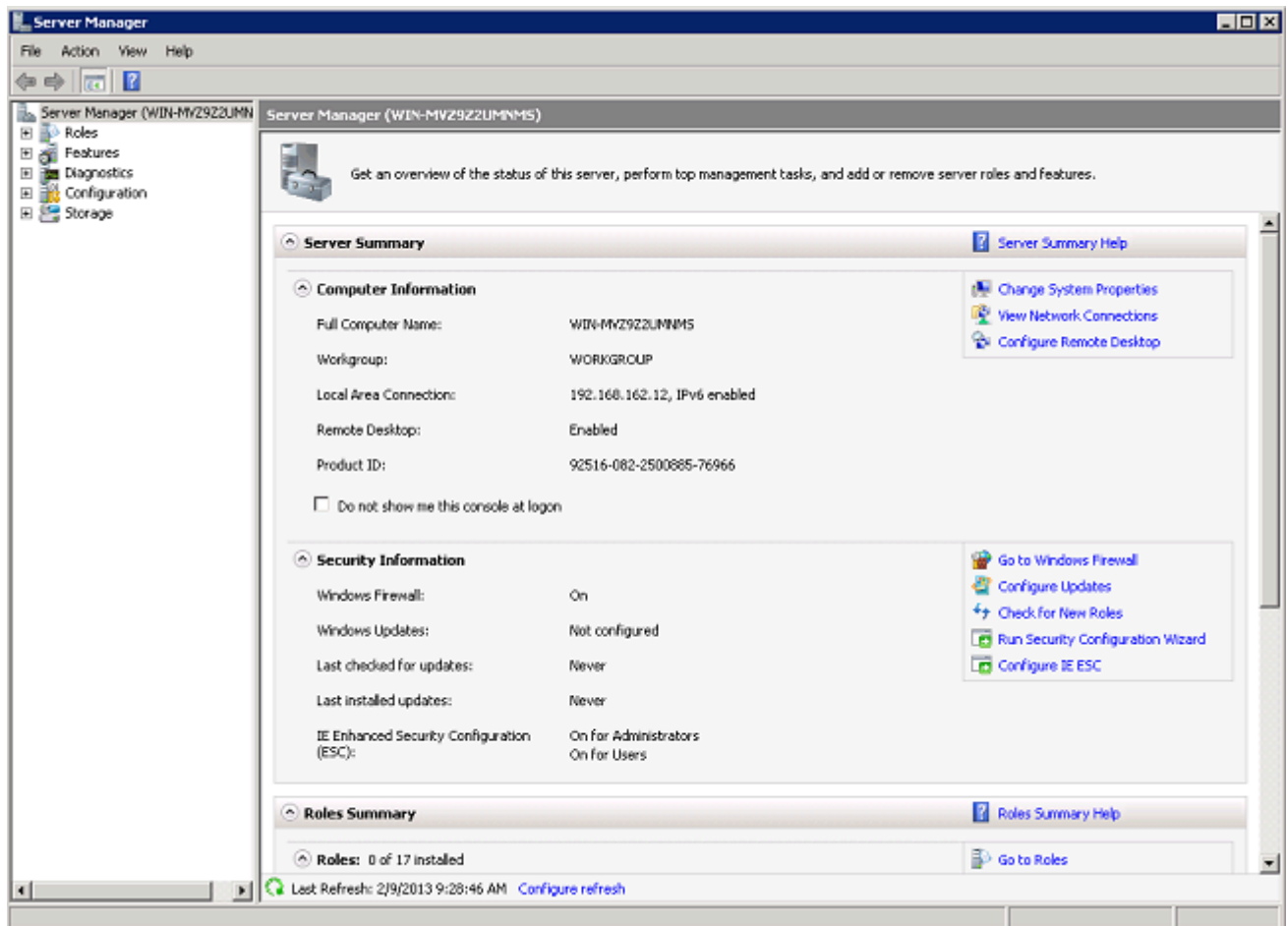


21. Herhaal deze procedure om meer clients aan het domein toe te voegen.

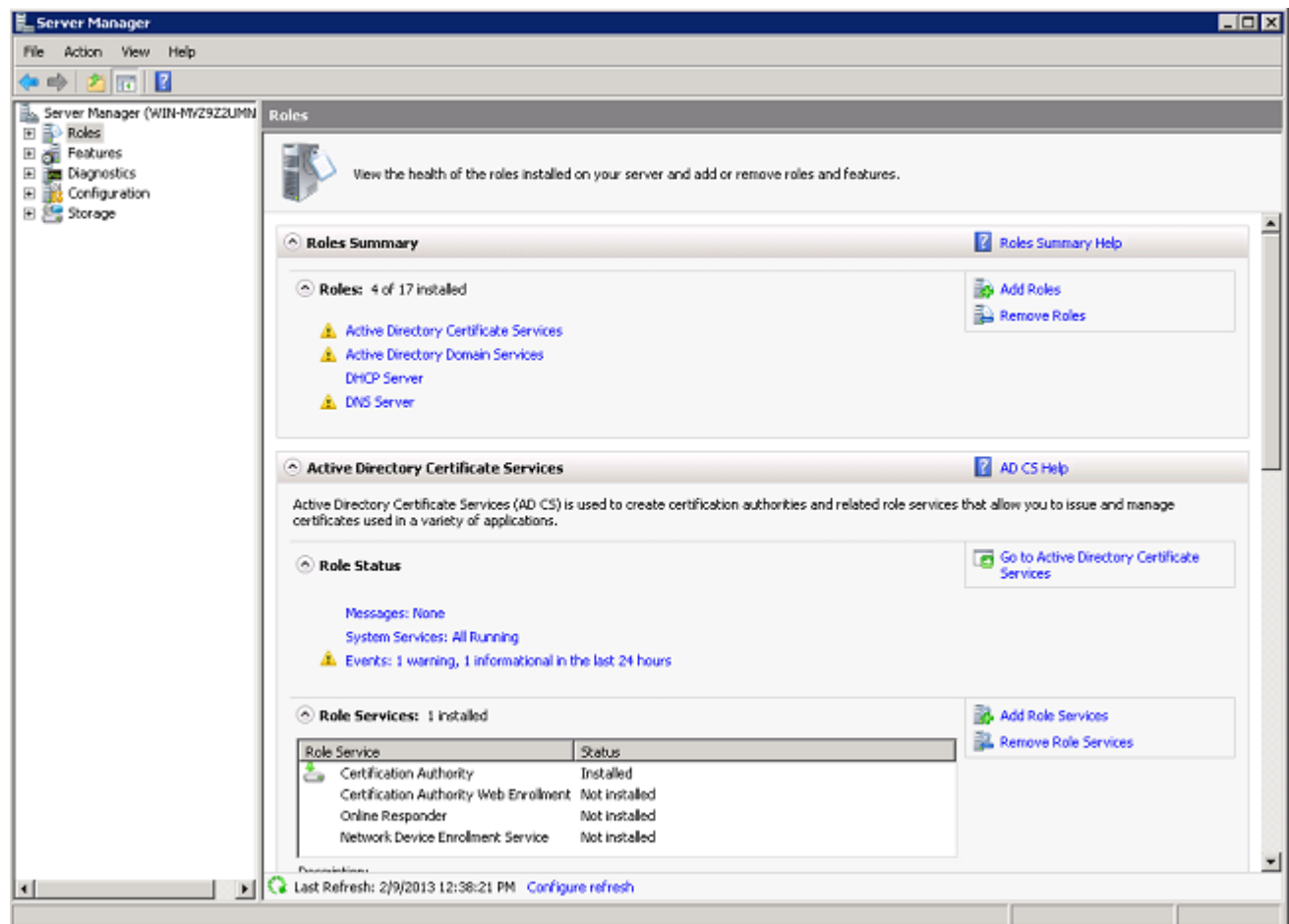
De netwerkbeleidserver installeren op de Microsoft Windows 2008-server

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).

Add Roles Wizard

 **Before You Begin**

Before You Begin

Server Roles

Confirmation

Progress

Results

This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.

Before you continue, verify that:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

☐ Skip this page by default

< Previous **Next >** Install Cancel

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

Add Roles Wizard

 **Select Server Roles**

Before You Begin

Server Roles

Network Policy and Access Services

Role Services

Confirmation

Progress

Results

Select one or more roles to install on this server.

Roles:

- ☒ Active Directory Certificate Services (Installed)
- ☒ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☒ DHCP Server (Installed)
- ☒ DNS Server (Installed)
- ☐ Fax Server
- ☐ File Services
- ☒ Network Policy and Access Services
- ☐ Print Services
- ☐ Terminal Services
- ☐ UDDI Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

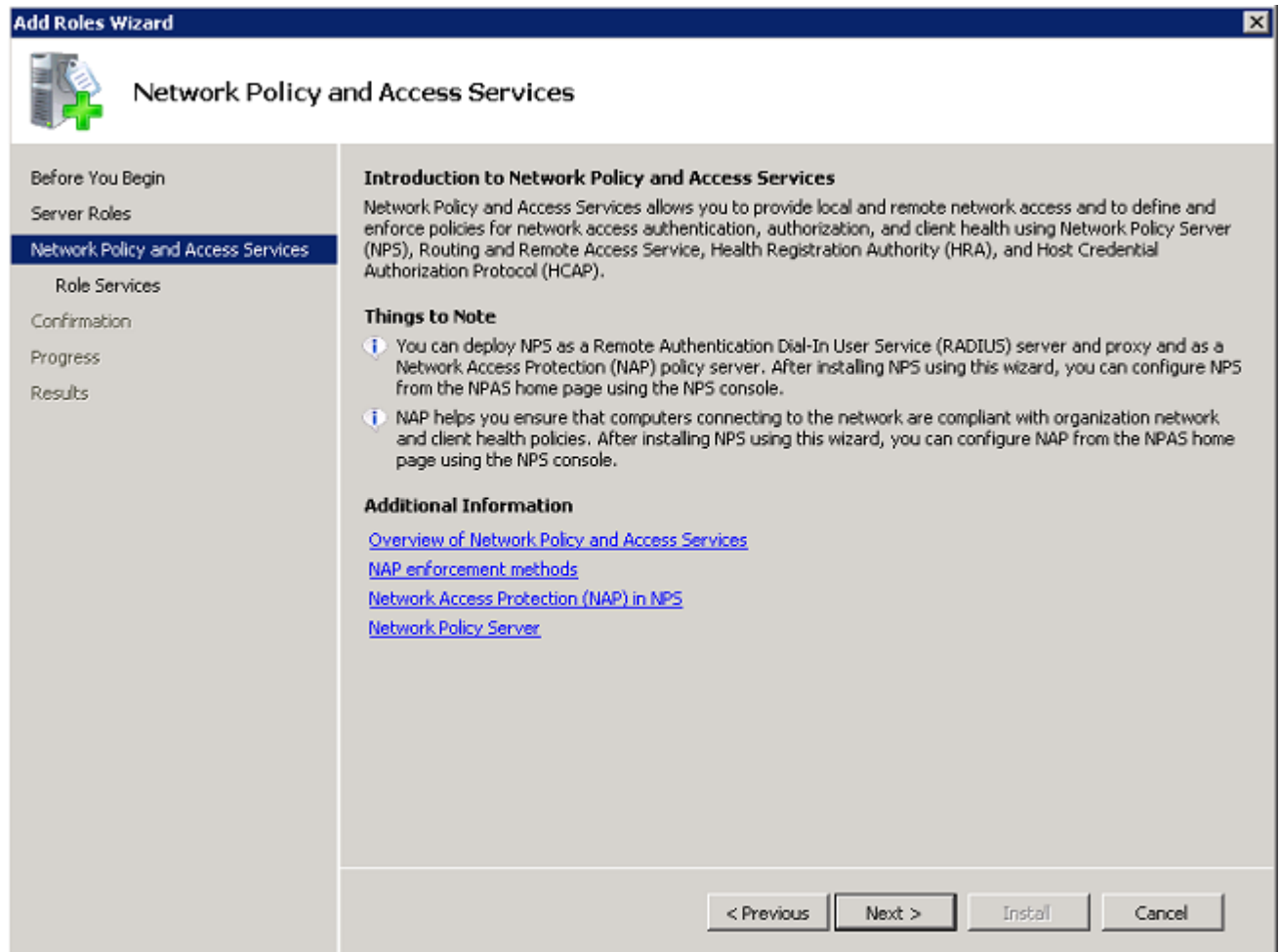
[More about server roles](#)

Description:

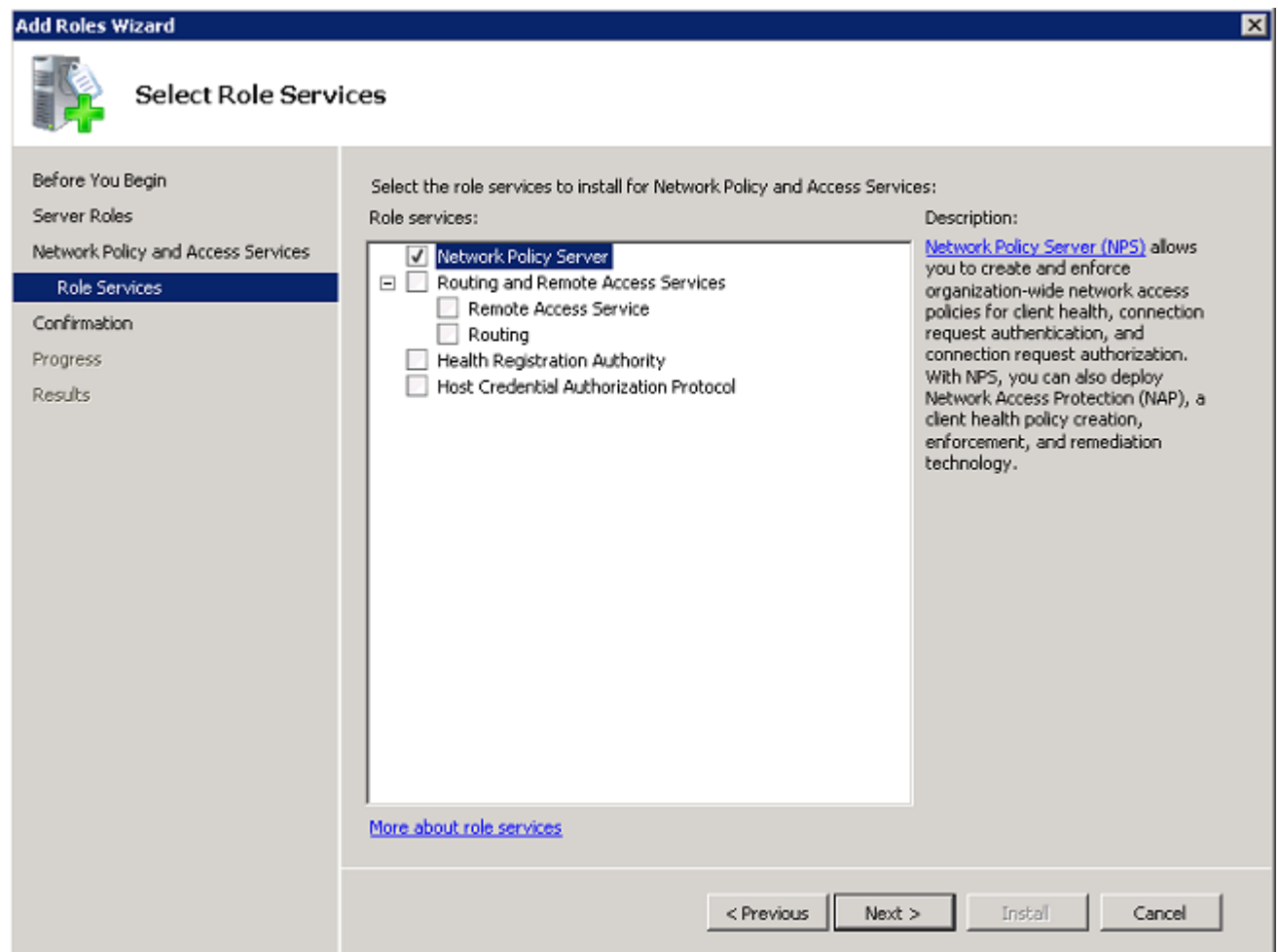
[Network Policy and Access Services](#) provides Network Policy Server (NPS), Routing and Remote Access, Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP), which help safeguard the health and security of your network.

< Previous Next > Install Cancel

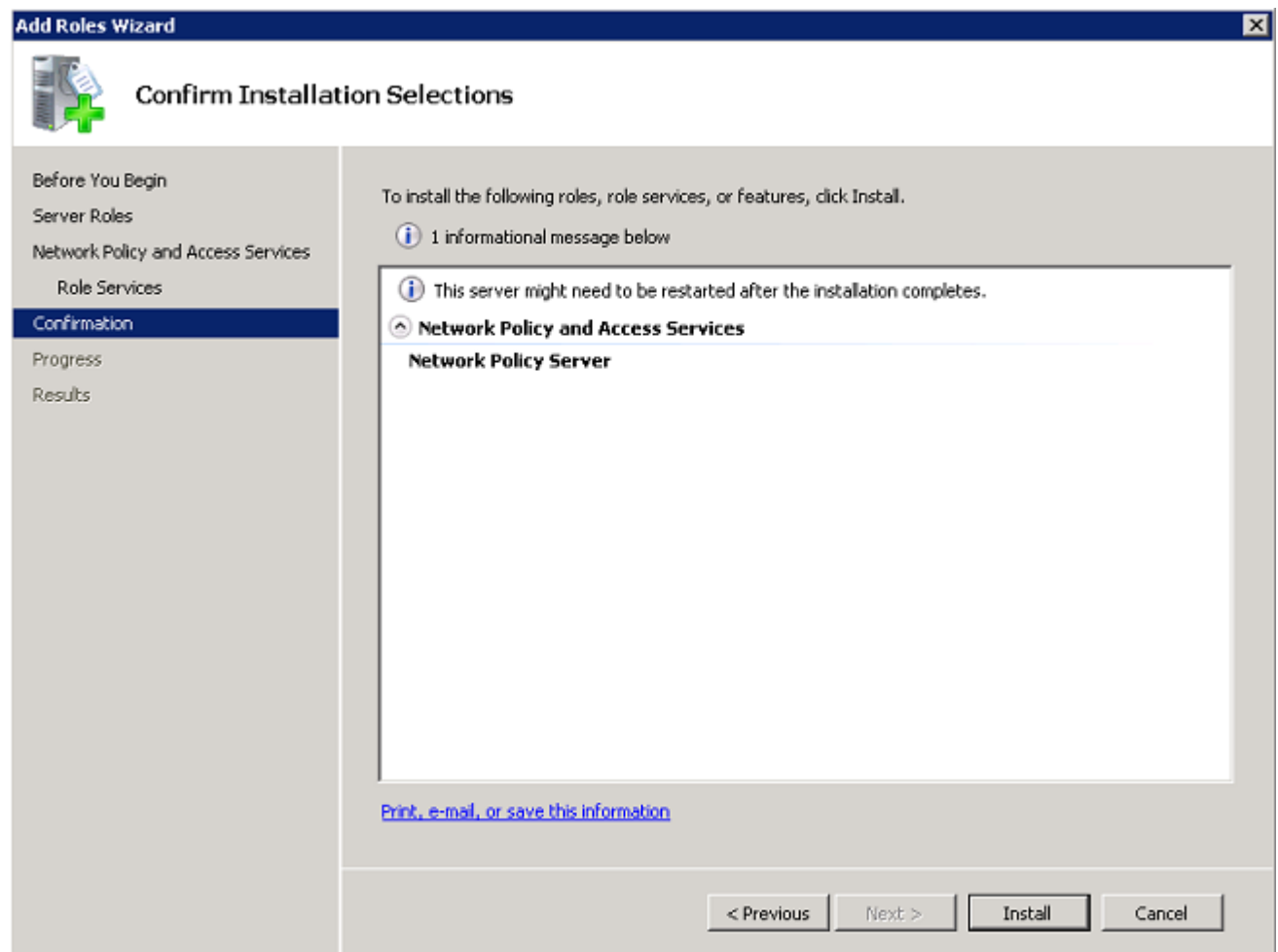
5. Bekijk de Inleiding tot netwerkbeleid en toegangsservices en klik op Volgende.



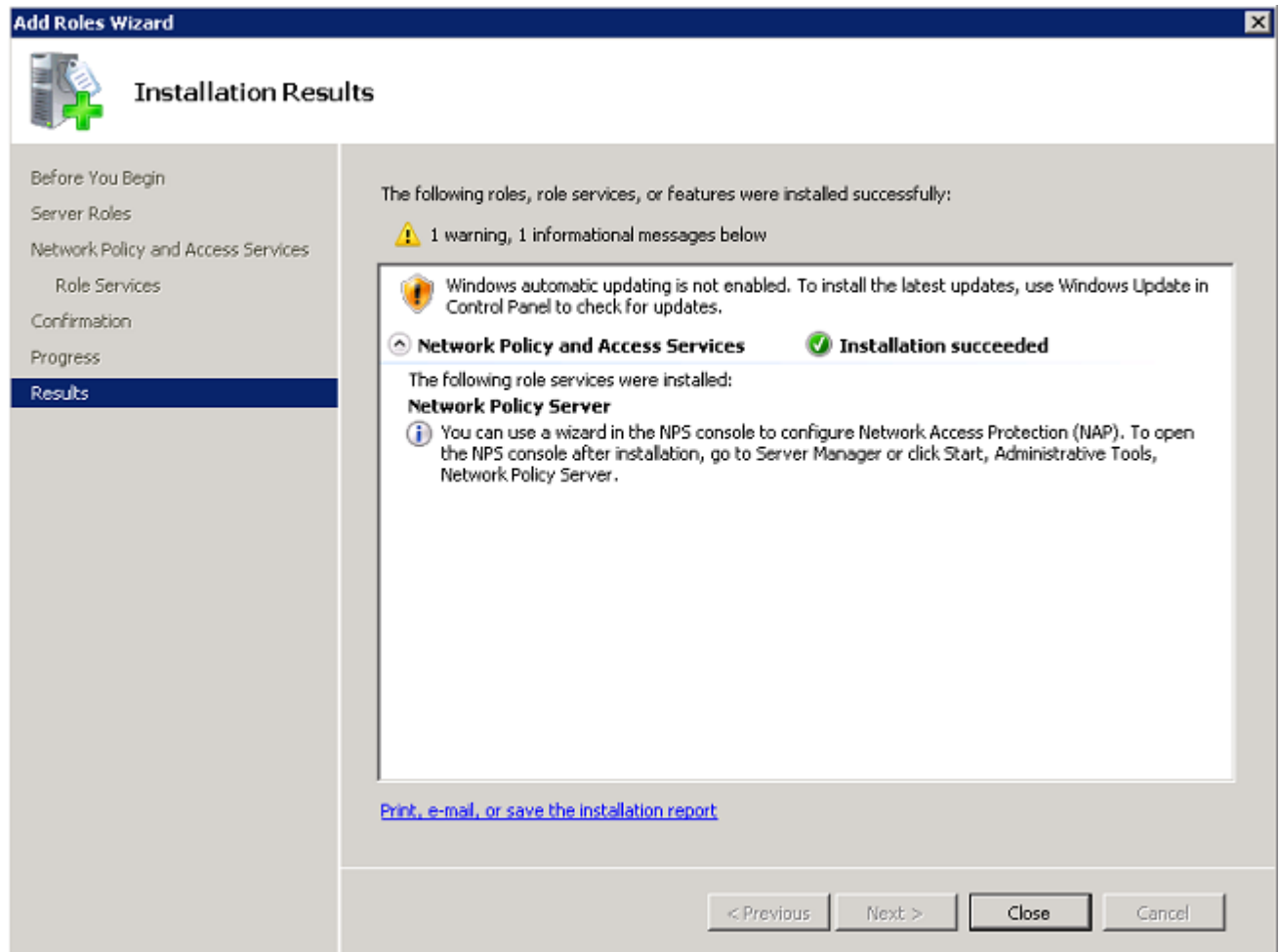
6. Selecteer Netwerkkeleidsserver en klik op Volgende.



7. Controleer de bevestiging en klik op Installeren.



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

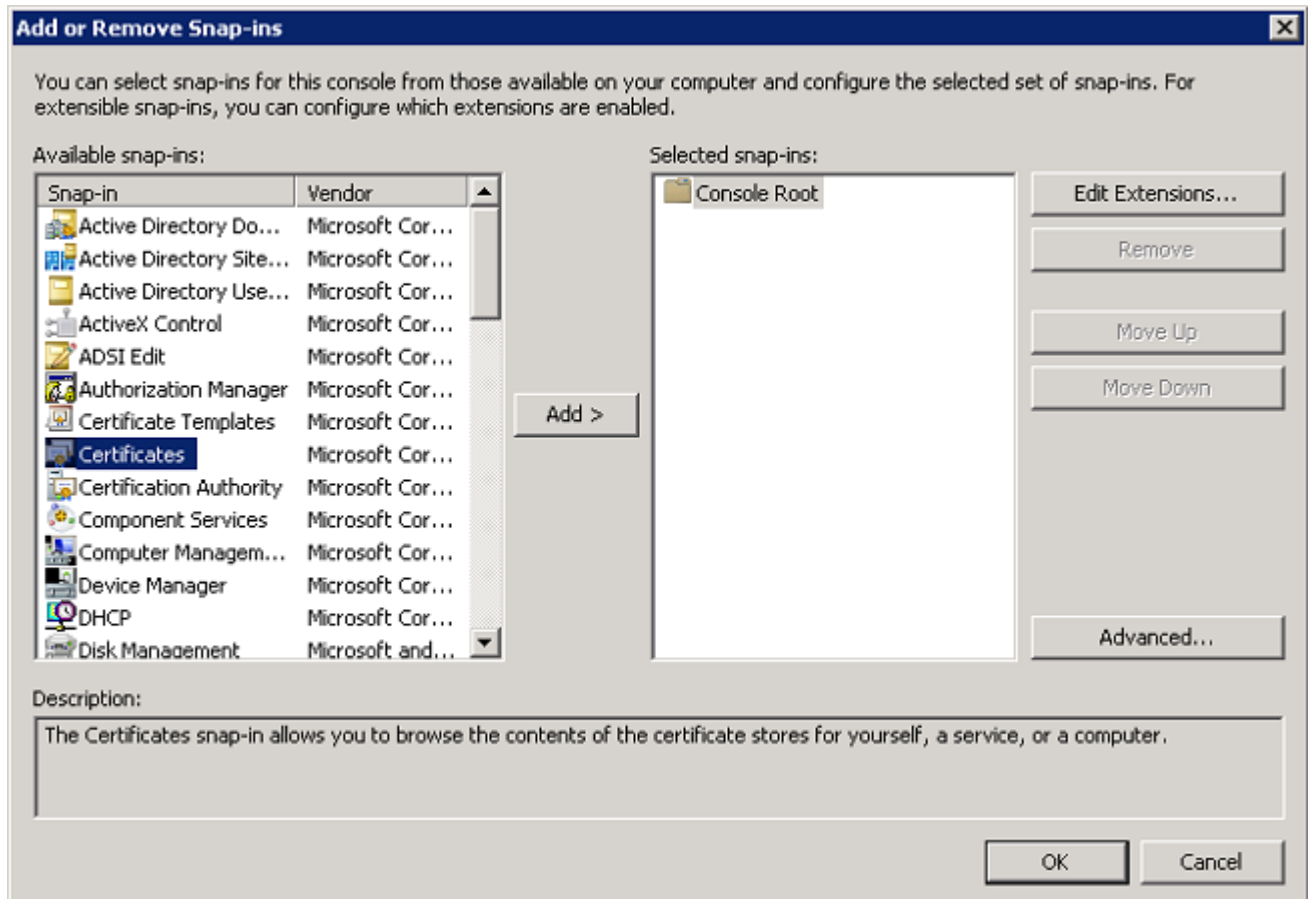


8. Klik op Close (Sluiten).

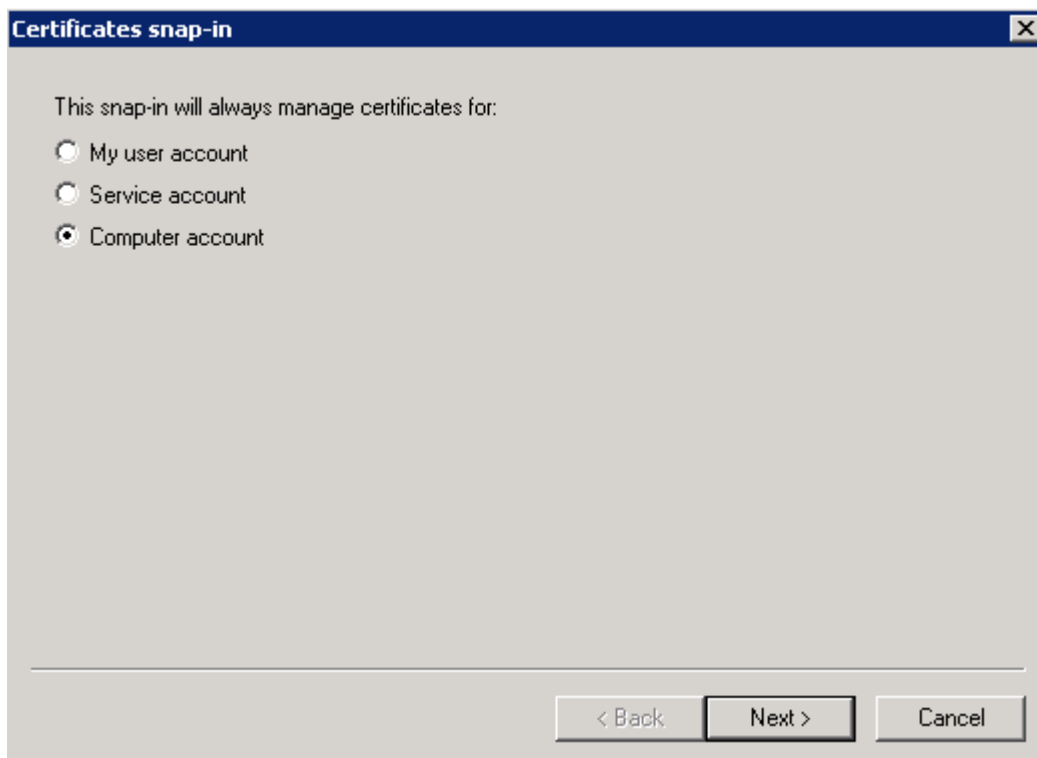
Een certificaat installeren

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

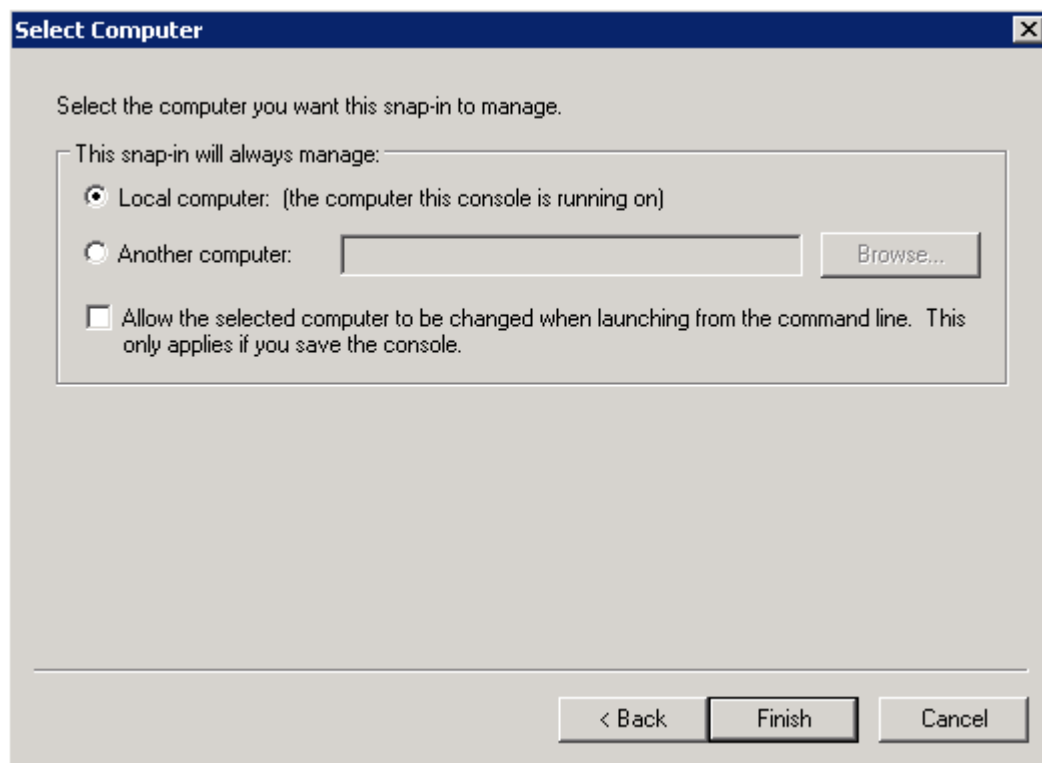
1. Klik op Start, voer mmc in en druk op Enter.
2. Klik op Bestand > Module toevoegen/verwijderen.
3. Kies Certificaten en klik op Toevoegen.



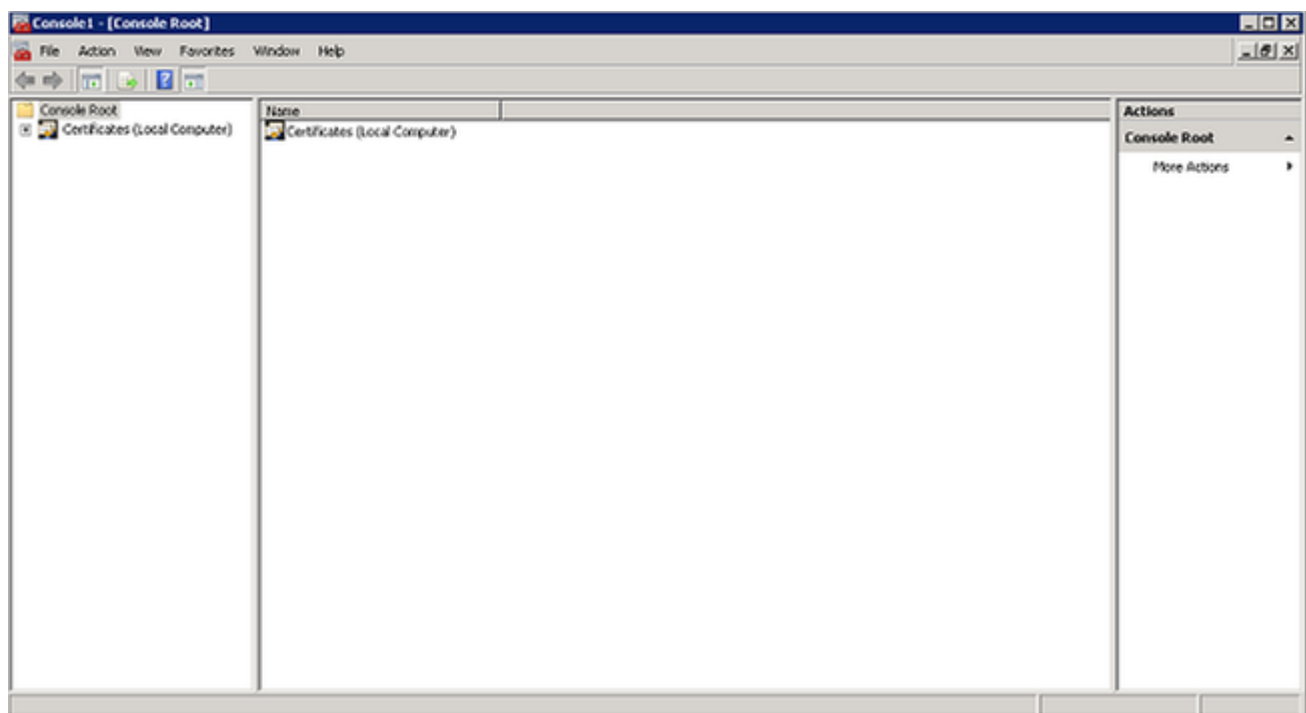
4. Kies Computeraccount en klik op Volgende.



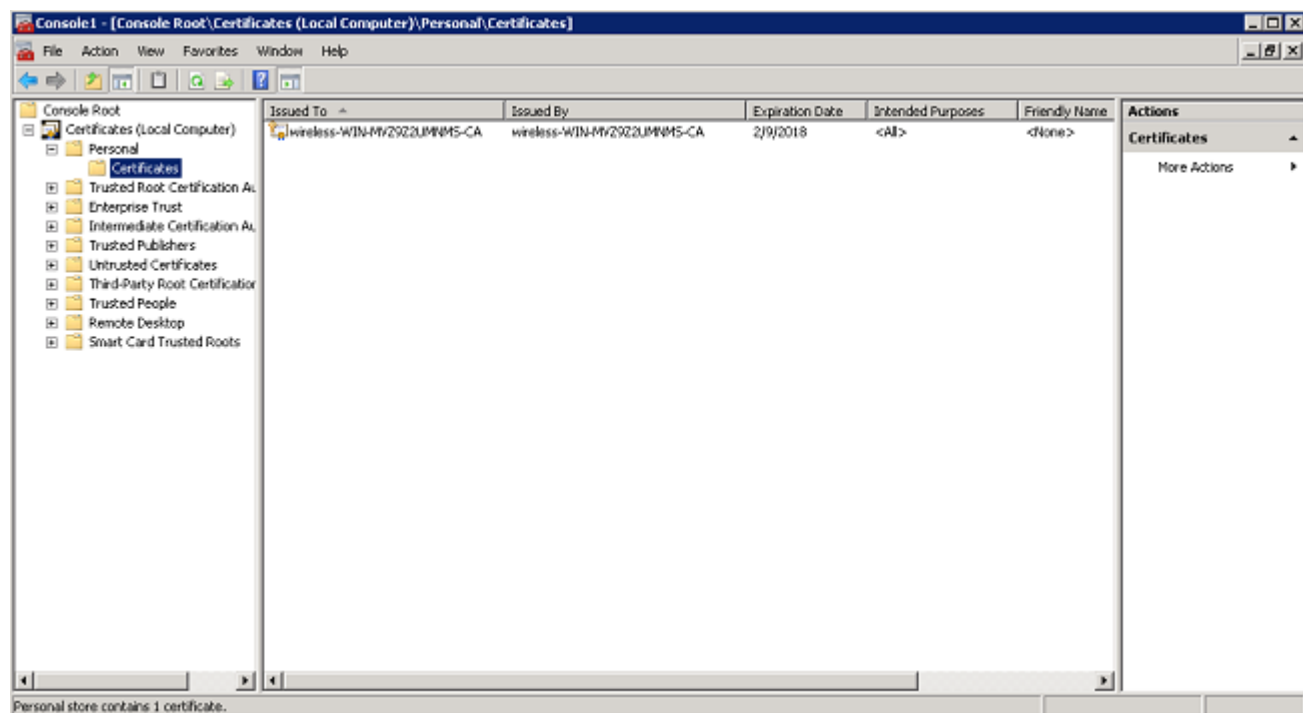
5. Selecteer Lokale computer en klik op Voltooien.



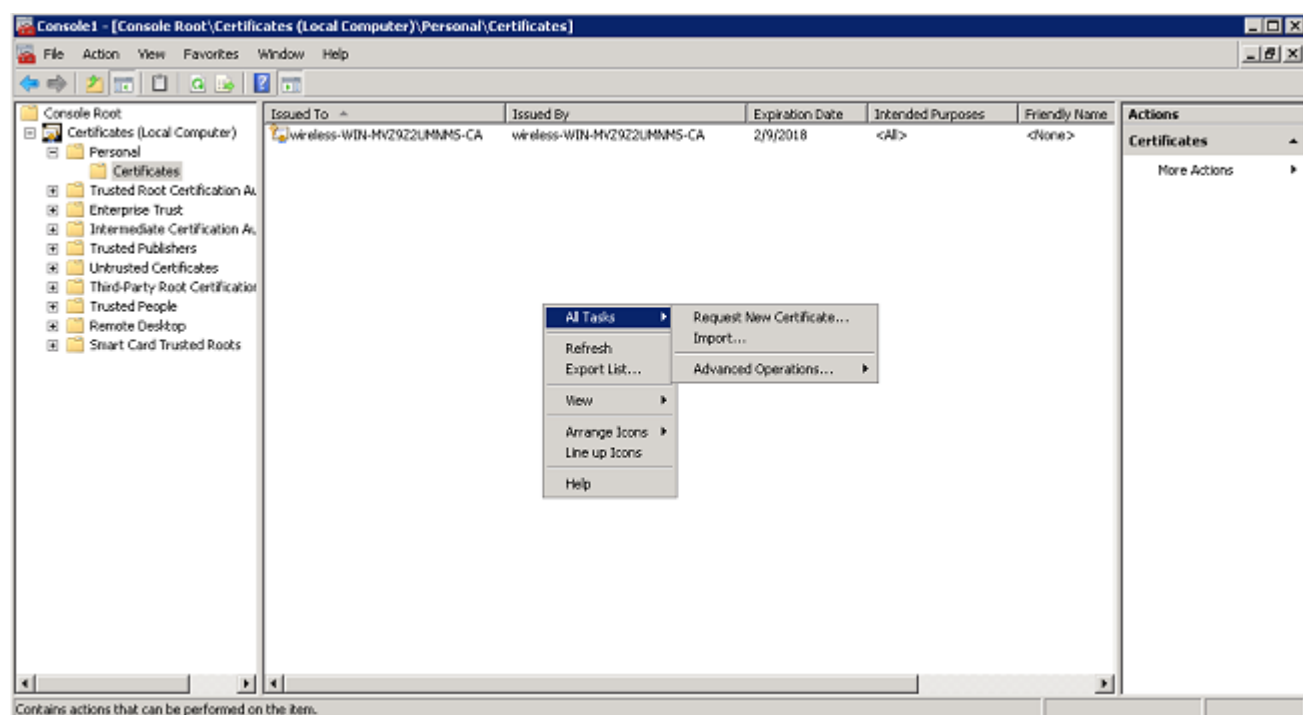
6. Klik op OK om terug te keren naar de Microsoft Management Console (MMC).



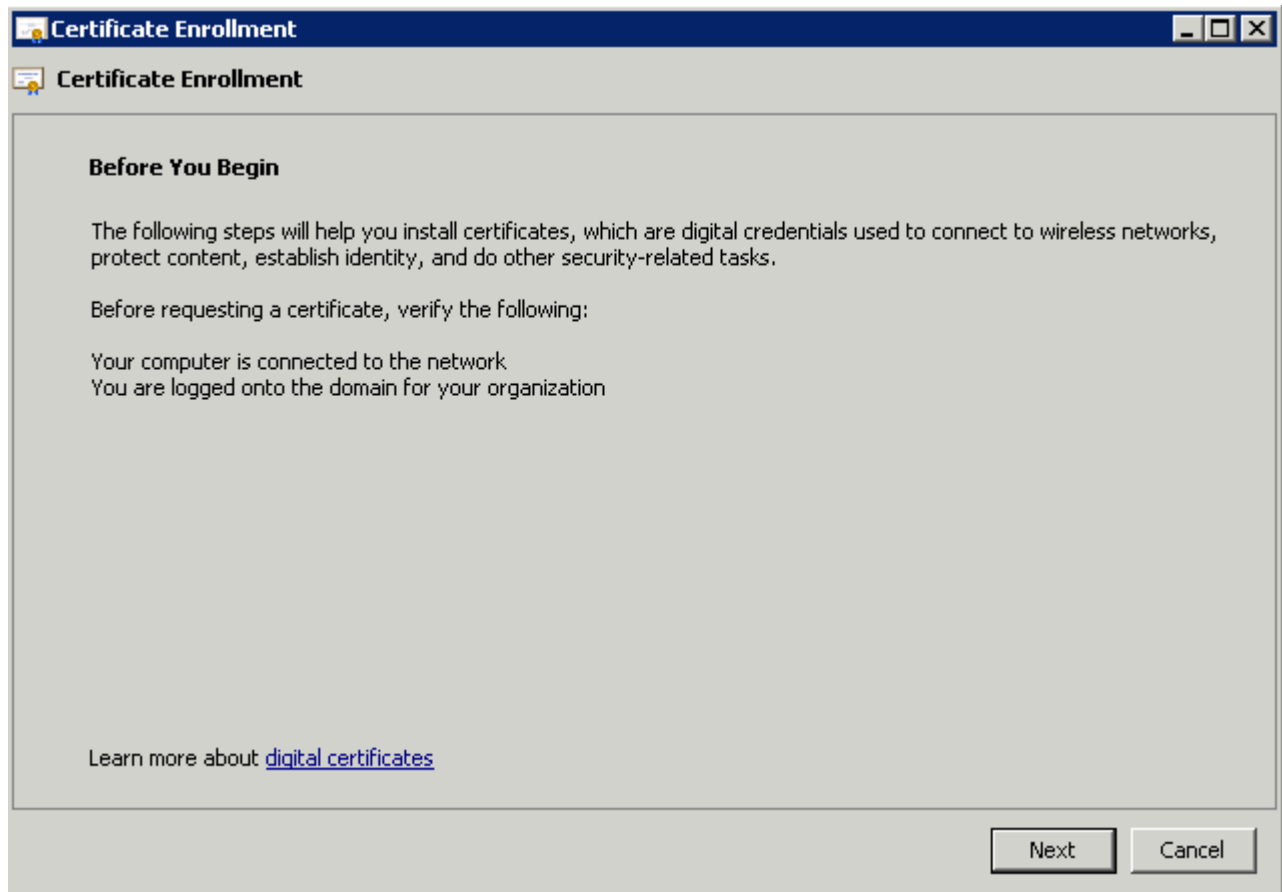
7. Vouw de mappen Certificaten (Lokale computer) en Persoonlijke gegevens uit en klik op Certificaten.



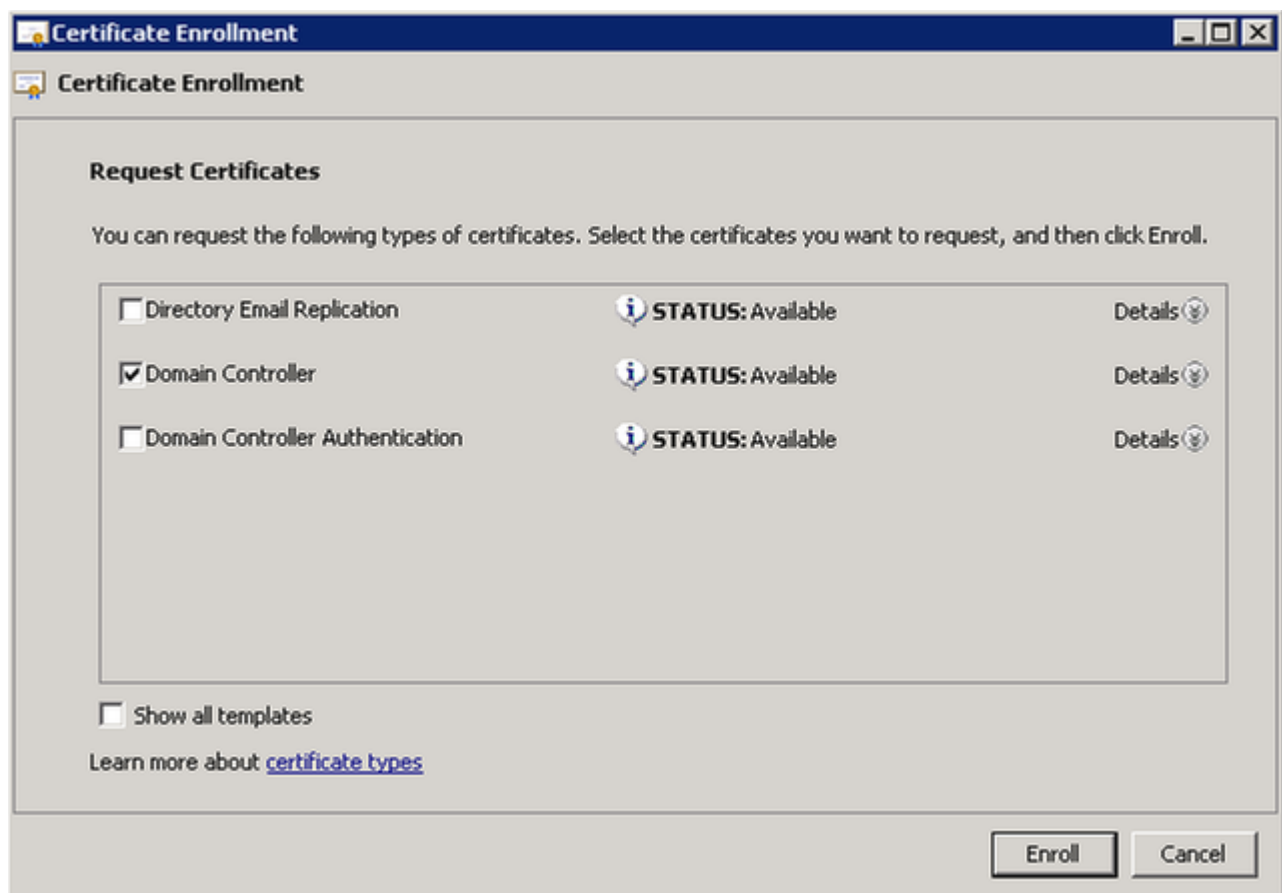
8. Klik met de rechtermuisknop in de witte ruimte onder het CA-certificaat en kies Alle taken > Nieuw certificaat aanvragen.



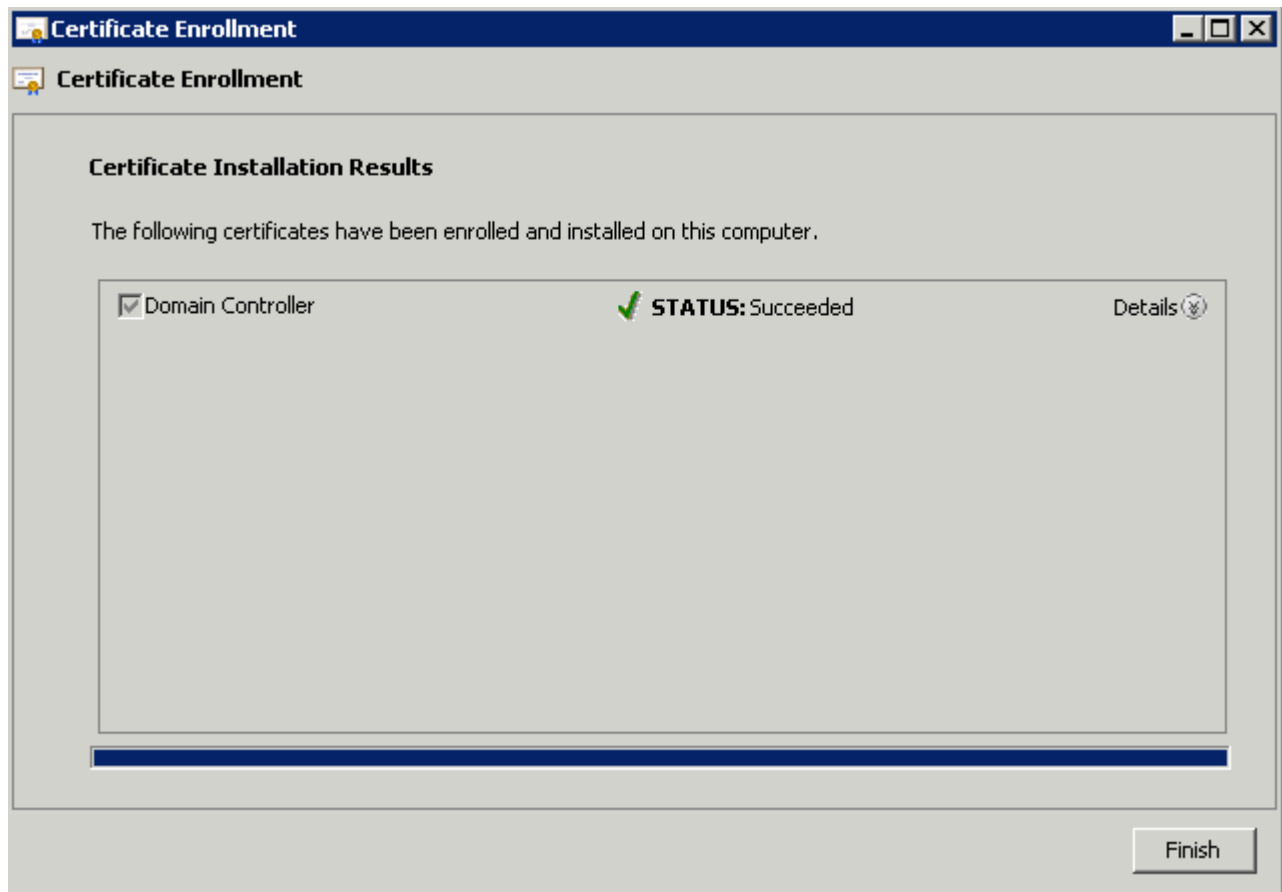
9. Klik op Next (Volgende).



10. Selecteer Domeincontroller en klik op Inschrijven.

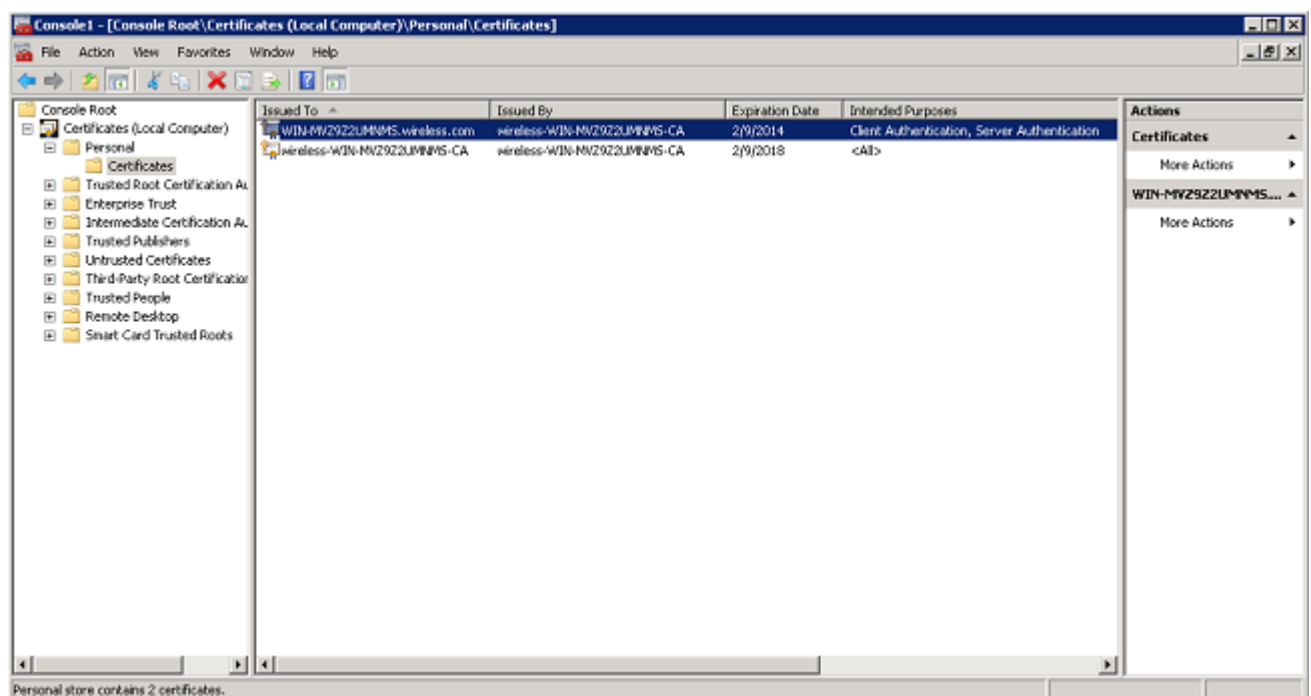


11. Klik op Voltooien zodra het certificaat is geïnstalleerd.



Het NPS-certificaat is nu geïnstalleerd.

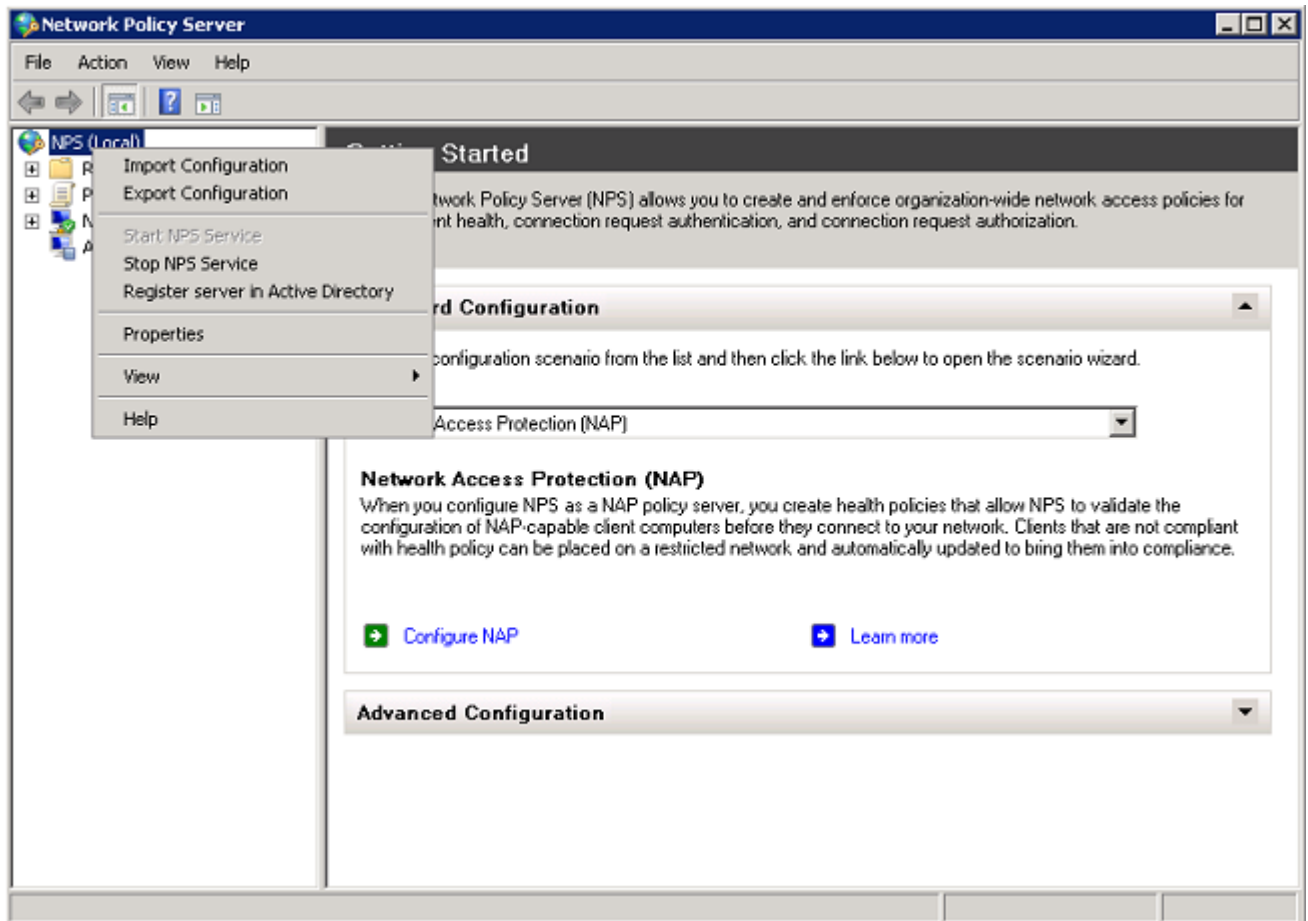
12. Zorg ervoor dat het beoogde doel van het certificaat clientverificatie, serververificatie leest.



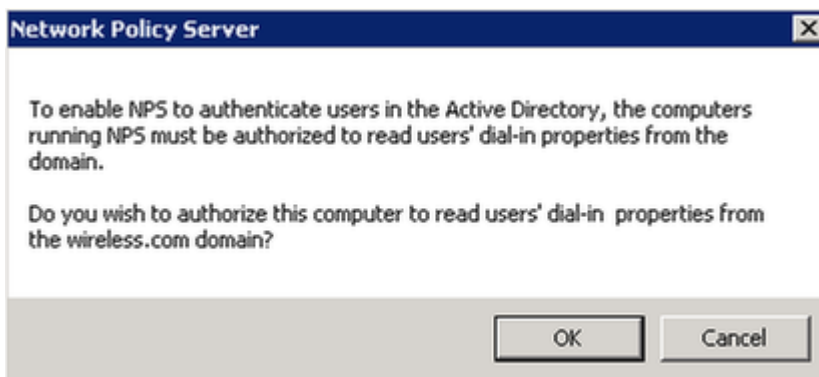
De netwerkbeleidsserverservice configureren voor PEAP-MS-CHAP v2-verificatie

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

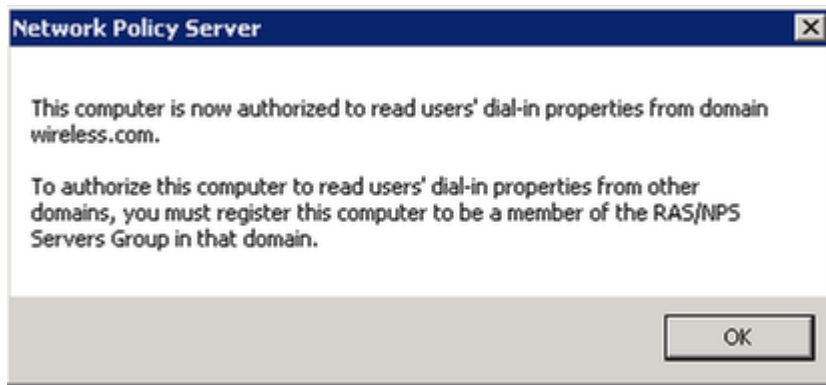
1. Klik op Start > Systeembeheer> Netwerkbeleidsserver.
2. Klik met de rechtermuisknop op NPS (Lokaal) en kies Server registreren in Active Directory.



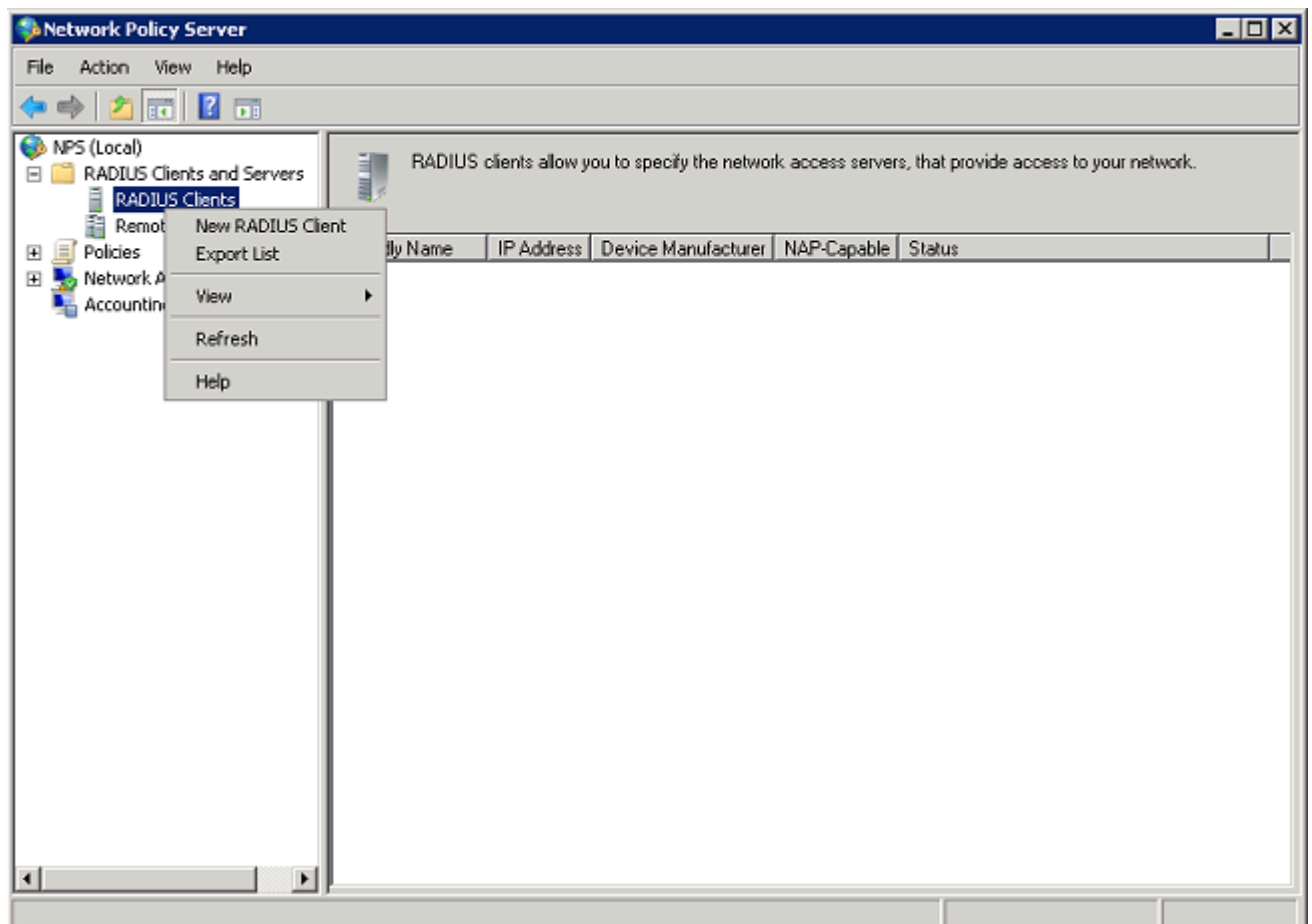
3. Klik op OK.



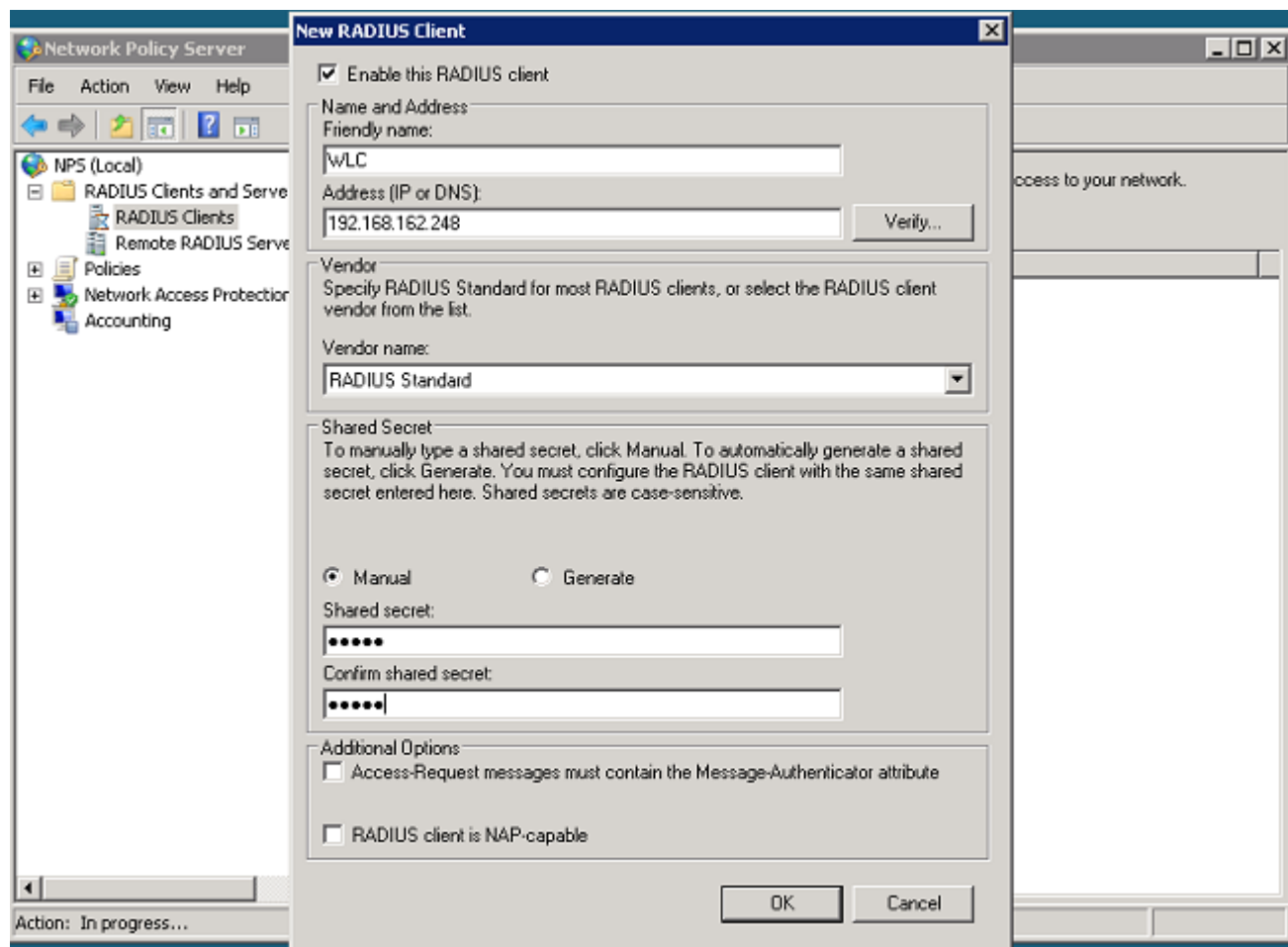
4. Klik op OK.



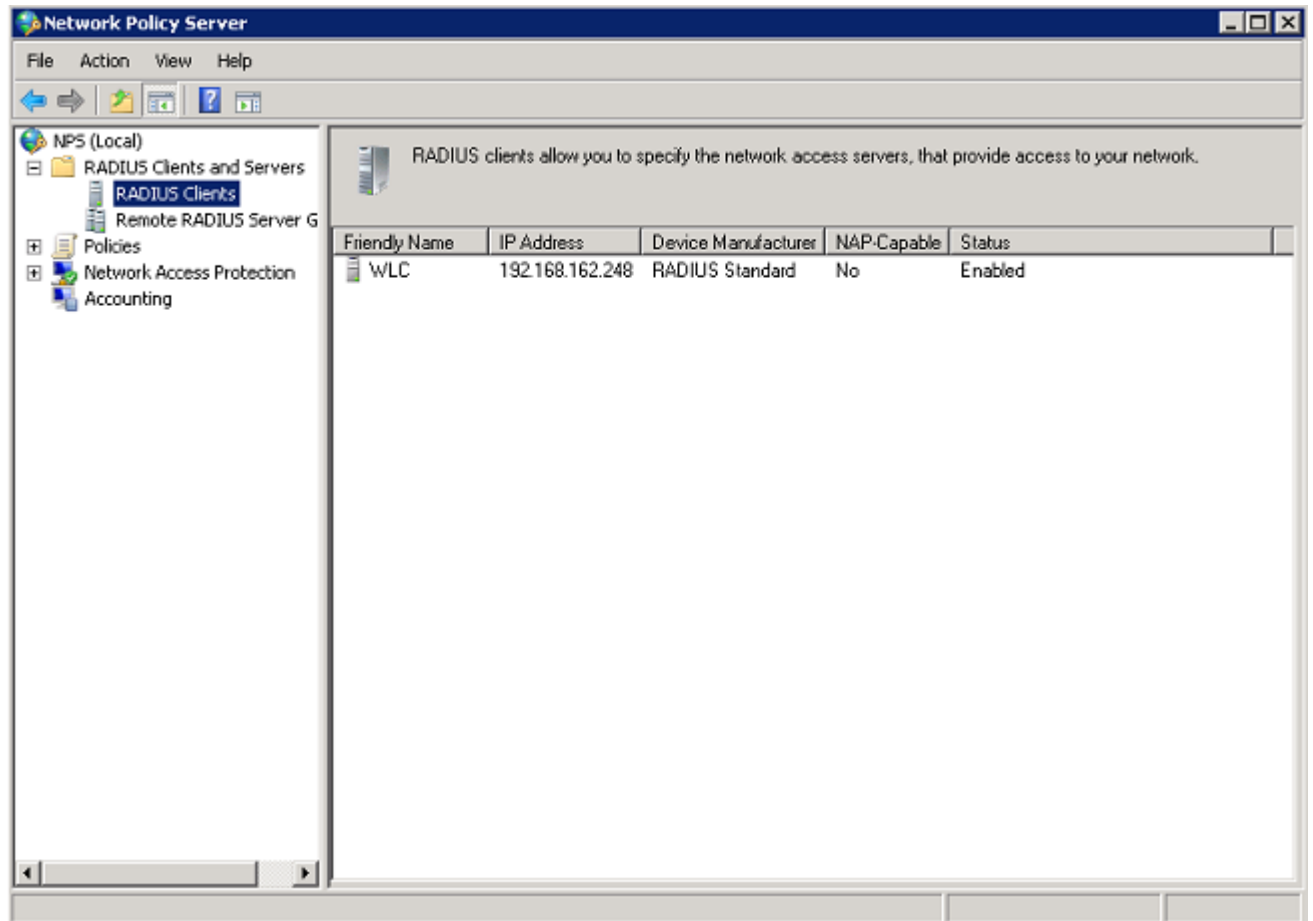
5. Voeg de draadloze LAN-controller toe als een verificatie-, autorisatie- en boekhoudclient (AAA) op de NPS.
6. RADIUS-clients en -servers uitbreiden. Klik met de rechtermuisknop op RADIUS-clients en kies Nieuwe RADIUS-client.



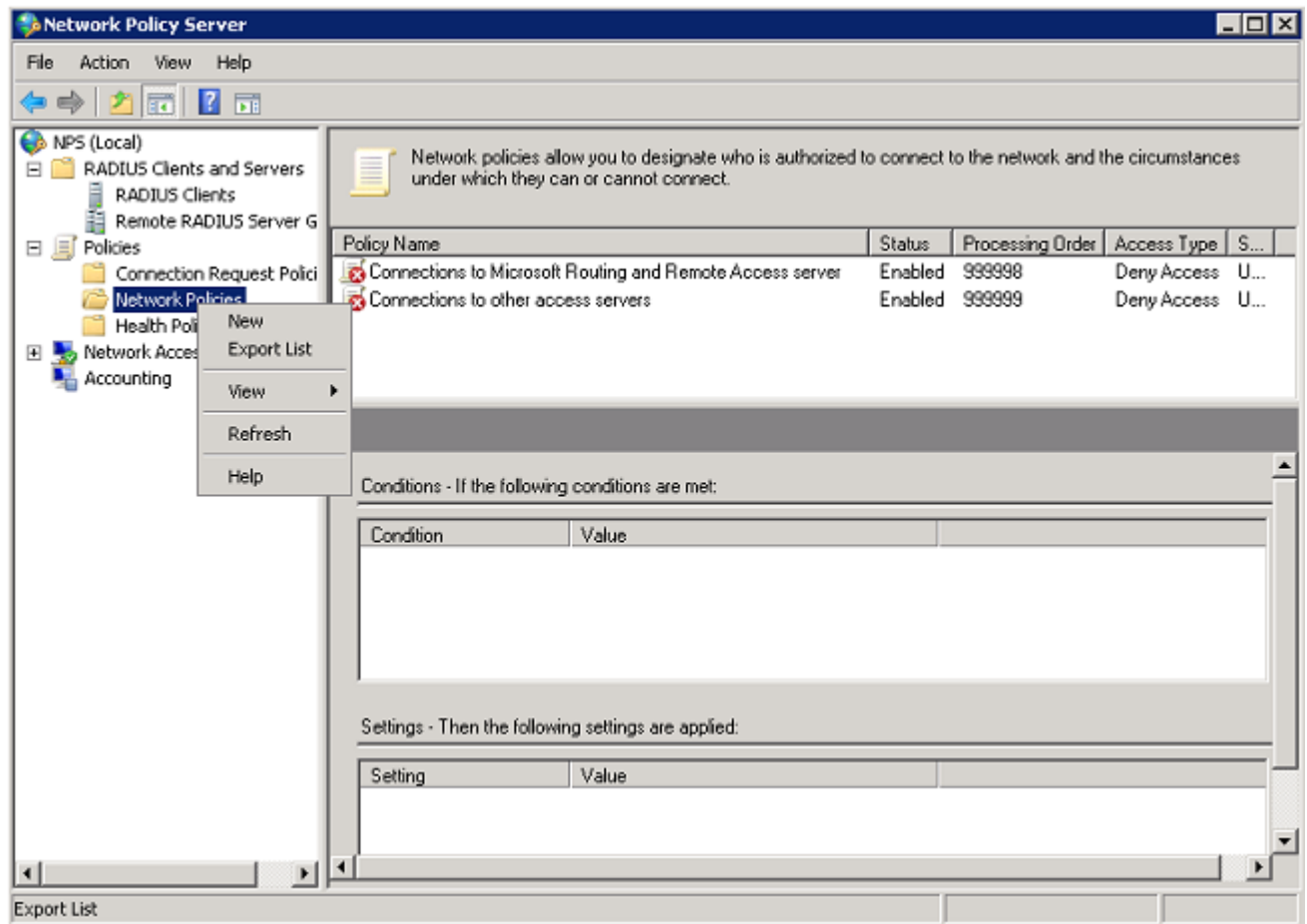
7. Voer een vriendelijke naam (WLC in dit voorbeeld), het IP-adres van het beheer van de WLC (192.168.162.248 in dit voorbeeld) en een gedeeld geheim in. Hetzelfde gedeelde geheim wordt gebruikt om de WLC te configureren.



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.



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

New Network Policy

Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name:

Wireless PEAP

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific.

☒ Type of network access server:

Unspecified

☐ Vendor specific:

10

Previous Next Finish Cancel

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

New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
Windows Groups	WIRELESS\Domain Users
NAS Port Type	Wireless - IEEE 802.11
Authentication Type	EAP

Condition description:
The Authentication Type condition specifies the authentication methods required to match this policy.

Add... Edit... Remove

Previous Next Finish Cancel

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

New Network Policy ✕



Specify Access Permission

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

☒ Access granted
Grant access if client connection attempts match the conditions of this policy.

☐ Access denied
Deny access if client connection attempts match the conditions of this policy.

☐ Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Previous Next Finish Cancel

13. Schakel alle verificatiemethoden uit onder Minder veilige verificatiemethoden.

New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Move Up
Move Down

Add... Edit... Remove

Less secure authentication methods:

- ☐ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
 - ☐ User can change password after it has expired
- ☐ Microsoft Encrypted Authentication (MS-CHAP)
 - ☐ User can change password after it has expired
- ☐ Encrypted authentication (CHAP)
- ☐ Unencrypted authentication (PAP, SPAP)
- ☐ Allow clients to connect without negotiating an authentication method.
- ☐ Perform machine health check only

Previous Next Finish Cancel

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

New Network Policy [X]

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Microsoft: Protected EAP (PEAP)

Move Up

Move Down

Add...

Edit...

Remove

Less secure authentication methods:

- ☐ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
 - ☐ User can change password after it has expired
- ☐ Microsoft Encrypted Authentication (MS-CHAP)
 - ☐ User can change password after it has expired
- ☐ Encrypted authentication (CHAP)
- ☐ Unencrypted authentication (PAP, SPAP)
- ☐ Allow clients to connect without negotiating an authentication method.
- ☐ Perform machine health check only

Previous

Next

Finish

Cancel

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.

New Network Policy

Edit Protected EAP Properties

Select the certificate the server should use to prove its identity to the client. A certificate that is configured for Protected EAP in Connection Request Policy will override this certificate.

Certificate issued: WIN-MVZ9Z2UMNMS.wireless.com

Friendly name:

Issuer: wireless-WIN-MVZ9Z2UMNMS-CA

Expiration date: 2/9/2014 12:51:57 PM

☒ Enable Fast Reconnect

☐ Disconnect Clients without Cryptobinding

Eap Types

Secured password (EAP-MSCHAP v2)

Move Up

Move Down

Add Edit Remove OK Cancel

☐ User can change password after it has expired

☐ Encrypted authentication (CHAP)

☐ Unencrypted authentication (PAP, SPAP)

☐ Allow clients to connect without negotiating an authentication method.

☐ Perform machine health check only

Previous Next Finish Cancel

16. Klik op Next (Volgende).

New Network Policy [X]

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Microsoft: Protected EAP (PEAP)

Move Up

Move Down

Add...

Edit...

Remove

Less secure authentication methods:

- ☐ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
 - ☐ User can change password after it has expired
- ☐ Microsoft Encrypted Authentication (MS-CHAP)
 - ☐ User can change password after it has expired
- ☐ Encrypted authentication (CHAP)
- ☐ Unencrypted authentication (PAP, SPAP)
- ☐ Allow clients to connect without negotiating an authentication method.
- ☐ Perform machine health check only

Previous

Next

Finish

Cancel

17. Klik op Next (Volgende).

New Network Policy

Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Constraints

- Idle Timeout
- Session Timeout
- Called Station ID
- Day and time restrictions
- NAS Port Type

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

☐ Disconnect after the maximum idle time

1

Previous Next Finish Cancel

18. Klik op Next (Volgende).

New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

RADIUS Attributes

- ☒ Standard
- ☐ Vendor Specific

Network Access Protection

- ☒ NAP Enforcement
- ☒ Extended State

Routing and Remote Access

- ☐ Multilink and Bandwidth Allocation Protocol (BAP)
- ☐ IP Filters
- ☐ Encryption
- ☒ IP Settings

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

Add... Edit... Remove

Previous Next Finish Cancel

19. Klik op Finish (Voltooien).

New Network Policy

Completing New Network Policy

You have successfully created the following network policy:

Wireless PEAP

Policy conditions:

Condition	Value
Windows Groups	WIRELESS\Domain Users
NAS Port Type	Wireless - IEEE 802.11
Authentication Type	EAP

Policy settings:

Condition	Value
Authentication Method	EAP
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.

Previous Next Finish Cancel

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).

New Object - User

Create in: wireless.com/Users

First name: Client1 Initials:

Last name:

Full name: Client1

User logon name: Client1 @wireless.com

User logon name (pre-Windows 2000): WIRELESS\ Client1

< Back Next > Cancel

- 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.

New Object - User

Create in: wireless.com/Users

Password:

Confirm password:

☐ User must change password at next logon

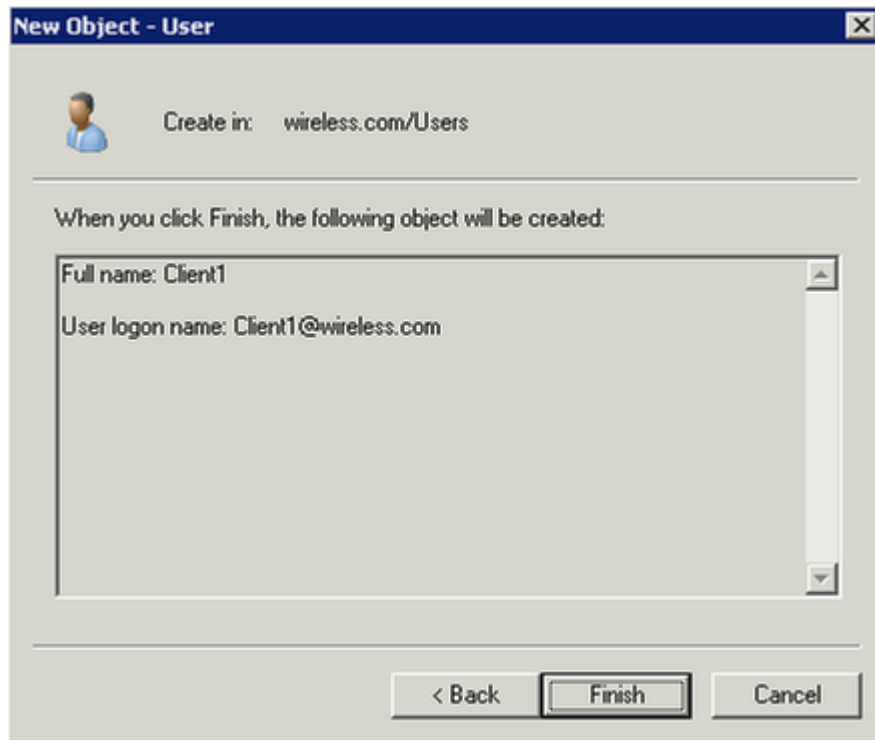
☐ User cannot change password

☐ Password never expires

☐ Account is disabled

< Back Next > Cancel

- 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.

[MONITOR](#)
[WLANs](#)
[CONTROLLER](#)
[WIRELESS](#)
[SECURITY](#)
[MANAGEMENT](#)
[COMMANDS](#)
[HELP](#)
[FEEDBACK](#)

[Save Configuration](#)
[Ping](#)
[Logout](#)
[Refresh](#)

Security

AAA

General

RADIUS

Authentication
Accounting
Fallback

TACACS+

LDAP
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Password Policies

Local EAP

Priority Order

Certificate

Access Control Lists

Wireless Protection Policies

Web Auth

TrustSec SXP

Advanced

RADIUS Authentication Servers

Apply

New...

Call Station ID Type

IP Address

Use AES Key Wrap

☐
 (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter

Hyphen

Network User

Management

Server Index

Server Address

Port

IPSec

Admin Status

1. Call Station ID Type will be applicable only for non 802.1x authentication only.

- 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).

The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes links for Save Configuration, Ping, Logout, and Refresh. The main menu on the left lists various security and management options. The central pane is titled 'RADIUS Authentication Servers > New' and contains the following configuration fields:

Field	Value
Server Index (Priority)	1
Server IP Address	192.168.162.12
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Key Wrap	☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	☒ Enable
Management	☒ Enable
IPSec	☐ Enable

Buttons for '< Back' and 'Apply' are located at the top right of the configuration area.

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.

WLANs > New

Type: WLAN
 Profile Name: PEAP
 SSID: PEAP
 ID: 1

< Back Apply

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.

WLANs > Edit 'PEAP'

General Security QoS Advanced

Profile Name: PEAP
 Type: WLAN
 SSID: PEAP
 Status: ☒ Enabled
 Security Policies: [WPA2][Auth(802.1X)]
 (Modifications done under security tab will appear after applying the changes.)
 Radio Policy: All
 Interface/Interface Group(G): management
 Multicast Vlan Feature: ☐ Enabled
 Broadcast SSID: ☒ Enabled
 NAS-ID: 2504

< Back Apply

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.

WLANs > Edit 'PEAP' < Back Apply

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security **6** WPA+WPA2
 MAC Filtering **9** ☐

Fast Transition
 Fast Transition ☐

Protected Management Frame
 PMF Disabled

WPA+WPA2 Parameters

WPA Policy ☐
 WPA2 Policy ☒
 WPA2 Encryption ☒ AES ☐ TKIP

Authentication Key Management

802.1X ☒ Enable
 CCKM ☐ Enable
 PSK ☐ Enable
 FT 802.1X ☐ Enable

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

WLANs > Edit 'PEAP' < Back Apply

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

Radius Server Overwrite interface ☐ Enabled

	Authentication Servers	Accounting Servers
Server 1	☒ Enabled IP:192.168.162.12, Port:1812	☒ Enabled None
Server 2	☐ None	☐ None
Server 3	☐ None	☐ None
Server 4	☐ None	☐ None
Server 5	☐ None	☐ None
Server 6	☐ None	☐ None

Radius Server Accounting
 Interim Update ☐

Local EAP Authentication
 Local EAP Authentication ☐ Enabled

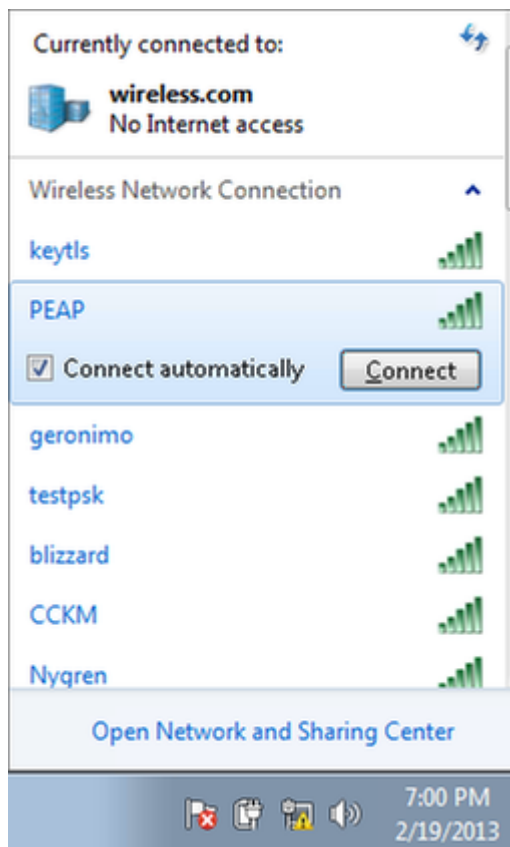
LDAP Servers

Server 1 None
 Server 2 None
 Server 3 None

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:

```
*apMgmtConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db 192.168.162.136 RUN (20) Changing IP4 ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2018)
*apMgmtConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db 192.168.162.136 RUN (20) Changing IP6 ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2246)
*apMgmtConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db In processSaidIE:4203 setting Central switched to TRUE
*apMgmtConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db In processSaidIE:4205 apVapId = 1 and Split Acl Id = 65535
*apMgmtConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db Applying site-specific Local Bridging override for station 78:e4:00:b2:ef:db - vapId 1, site "default-group", interface "management"
*apMgmtConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db Applying Local Bridging Interface Policy for station 78:e4:00:b2:ef:db - vlan 363, interface id 0, interface "management"
*apMgmtConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db processSaidIE statusCode is 0 and status is 0
*apMgmtConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db processSaidIE said_done_flag is 0 finish_flag is 0
*apMgmtConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db WTA - rates (8): 130 132 139 150 150 36 48 72 108 12 18 24 36 0 0 0 0
*apMgmtConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db suppRates statusCode is 0 and getSuppRatesElement is 1
*apMgmtConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db STA - rates (12): 130 132 139 150 150 36 48 72 108 12 18 24 36 0 0 0 0
*apMgmtConnTask_2: Feb 19 20:57:07.812: 78:e4:00:b2:ef:db callSuppRates statusCode is 0 and getSuppRatesElement is 1
*apMgmtConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db Processing RSN IE type 48, length 30 for mobile 78:e4:00:b2:ef:db
*apMgmtConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db Received RSN IE with 0 PMKIDs from mobile 78:e4:00:b2:ef:db
*apMgmtConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db Found an cache entry for SSID c8:f9:f9:1a:20:40 in PMKID cache at index 0 of station 78:e4:00:b2:ef:db
*apMgmtConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db Removing RSNID c8:f9:f9:1a:20:40 from PMKID cache of station 78:e4:00:b2:ef:db
*apMgmtConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db Reinserting RSNID PMK Cache Entry 0 for station 78:e4:00:b2:ef:db
*apMgmtConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db Setting active key cache index 0 --> 0
*apMgmtConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db updating RsnIdValidatedCbSp
*apMgmtConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db apMgmtStateDec
*apMgmtConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db apMgmtStateDec
*apMgmtConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db 192.168.162.136 RUN (20) Change state to START (0) last state RUN (20)
*apMgmtConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db pmkApMgmtMobileStation: AP_MGMT_WAIT_13 AUTH COMPLETE = 0.
*apMgmtConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db 192.168.162.136 START (0) Initialising policy
*apMgmtConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db 192.168.162.136 START (0) Change state to AUTHCHECK (2) last state START (0)
*apMgmtConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db 192.168.162.136 AUTHCHECK (2) Change state to 0021X_REQD (3) last state AUTHCHECK (2)
*apMgmtConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db Not Using RSN Compliance mode qoSMap 00
*apMgmtConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db 192.168.162.136 0021X_REQD (3) Plumbbed mobile LWAPP rule on AP c8:f9:f9:1a:20:40 vapId 1 apVapId 1 flex-acl-name:
*apMgmtConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db apfMgmtAddUser2 (apf_policy.c:276) Changing state for mobile 78:e4:00:b2:ef:db on AP c8:f9:f9:1a:20:40 from Associated to Associated
*apMgmtConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db apfMgmtAddUser2: session timeout for station 78:e4:00:b2:ef:db - Session Toot 0, apfMgmtTimeOut "0" and sessionTimerRunning flag is 0
*apMgmtConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db Stopping deletion of Mobile Station: (callerId: 40)
*apMgmtConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db Func: apfMgmtAddUser2, Ms Timeout = 0, Session Timeout = 0
*apMgmtConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db Sending Assoc Response to station on RSNID c8:f9:f9:1a:20:40 (status 0) ApVapId 1 Slot 0
*apMgmtConnTask_2: Feb 19 20:57:07.813: 78:e4:00:b2:ef:db apfProcessAssocReq (apf_00211.c:7391) Changing state for mobile 78:e4:00:b2:ef:db on AP c8:f9:f9:1a:20:40 from Associated to Associated
*pmkReclaimTask: Feb 19 20:57:07.817: 78:e4:00:b2:ef:db 192.168.162.136 Removed PMT entry.
*dot1dmgTask: Feb 19 20:57:07.820: 78:e4:00:b2:ef:db Disable w-auth, use PMK lifetime.
*dot1dmgTask: Feb 19 20:57:07.820: 78:e4:00:b2:ef:db dot1d - moving mobile 78:e4:00:b2:ef:db into Connecting state
*dot1dmgTask: Feb 19 20:57:07.820: 78:e4:00:b2:ef:db Sending EAP-Request/Identity to mobile 78:e4:00:b2:ef:db (EAP Id 1)
*dot1d_mgTask: Feb 19 20:57:07.838: 78:e4:00:b2:ef:db Received EAPOL START from mobile 78:e4:00:b2:ef:db
*dot1d_mgTask: Feb 19 20:57:07.839: 78:e4:00:b2:ef:db dot1d - moving mobile 78:e4:00:b2:ef:db into Connecting state
*dot1d_mgTask: Feb 19 20:57:07.839: 78:e4:00:b2:ef:db Sending EAP-Request/Identity to mobile 78:e4:00:b2:ef:db (EAP Id 2)
*dot1d_mgTask: Feb 19 20:57:07.858: 78:e4:00:b2:ef:db Received EAPOL EAP-Request from mobile 78:e4:00:b2:ef:db
*dot1d_mgTask: Feb 19 20:57:07.858: 78:e4:00:b2:ef:db Received EAP Response packet with mismatching id (currentId=2, apid=2) from mobile 78:e4:00:b2:ef:db
*dot1d_mgTask: Feb 19 20:57:07.858: 78:e4:00:b2:ef:db Received EAPOL EAP-Request from mobile 78:e4:00:b2:ef:db
*dot1d_mgTask: Feb 19 20:57:07.858: 78:e4:00:b2:ef:db Received Identity Response (count=2) from mobile 78:e4:00:b2:ef:db
*dot1d_mgTask: Feb 19 20:57:07.858: 78:e4:00:b2:ef:db EAP State update from Connecting to Authenticating for mobile 78:e4:00:b2:ef:db
*dot1d_mgTask: Feb 19 20:57:07.858: 78:e4:00:b2:ef:db dot1d - moving mobile 78:e4:00:b2:ef:db into Authenticating state
```

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_MagTask_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_MagTask_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_MagTask_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_MagTask_3: Feb 19 21:28:24.508: 78:e4:00:b2:ef:db Received EAPOL EAPFRT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MagTask_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_MagTask_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_MagTask_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_MagTask_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_MagTask_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_MagTask_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_MagTask_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_MagTask_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_MagTask_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_MagTask_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_MagTask_3: Feb 19 21:33:14.601: 78:e4:00:b2:ef:db Received EAPOL EAPFRT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MagTask_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_MagTask_3: Feb 19 21:33:14.611: 78:e4:00:b2:ef:db Received EAPOL EAPFRT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MagTask_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_MagTask_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_MagTask_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_MagTask_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_MagTask_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_MagTask_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_MagTask_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_MagTask_3: Feb 19 21:33:14.661: 78:e4:00:b2:ef:db Received EAPOL EAPFRT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MagTask_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_MagTask_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_MagTask_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_MagTask_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_MagTask_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_MagTask_3: Feb 19 21:33:14.674: 78:e4:00:b2:ef:db Received EAPOL EAPFRT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MagTask_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_MagTask_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_MagTask_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_MagTask_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_MagTask_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_MagTask_3: Feb 19 21:33:14.706: 78:e4:00:b2:ef:db Received EAPOL EAPFRT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MagTask_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_MagTask_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_MagTask_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_MagTask_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_MagTask_3: Feb 19 21:33:14.721: 78:e4:00:b2:ef:db Sending EAP Request from AAA to mobile 78:e4:00:b2:ef:db (EAP Id 8)
*Dot1x_NW_MagTask_3: Feb 19 21:33:14.721: 78:e4:00:b2:ef:db Received EAPOL EAPFRT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MagTask_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_MagTask_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_MagTask_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_MagTask_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_MagTask_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_MagTask_3: Feb 19 21:33:14.738: 78:e4:00:b2:ef:db Received EAPOL EAPFRT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MagTask_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_MagTask_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_MagTask_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_MagTask_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_MagTask_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_MagTask_3: Feb 19 21:33:14.752: 78:e4:00:b2:ef:db Received EAPOL EAPFRT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MagTask_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_MagTask_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_MagTask_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_MagTask_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_MagTask_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_MagTask_3: Feb 19 21:33:14.770: 78:e4:00:b2:ef:db Received EAPOL EAPFRT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MagTask_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_MagTask_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_MagTask_3: Feb 19 21:33:14.781: 78:e4:00:b2:ef:db Processing Access-Accept for mobile 78:e4:00:b2:ef:db
```

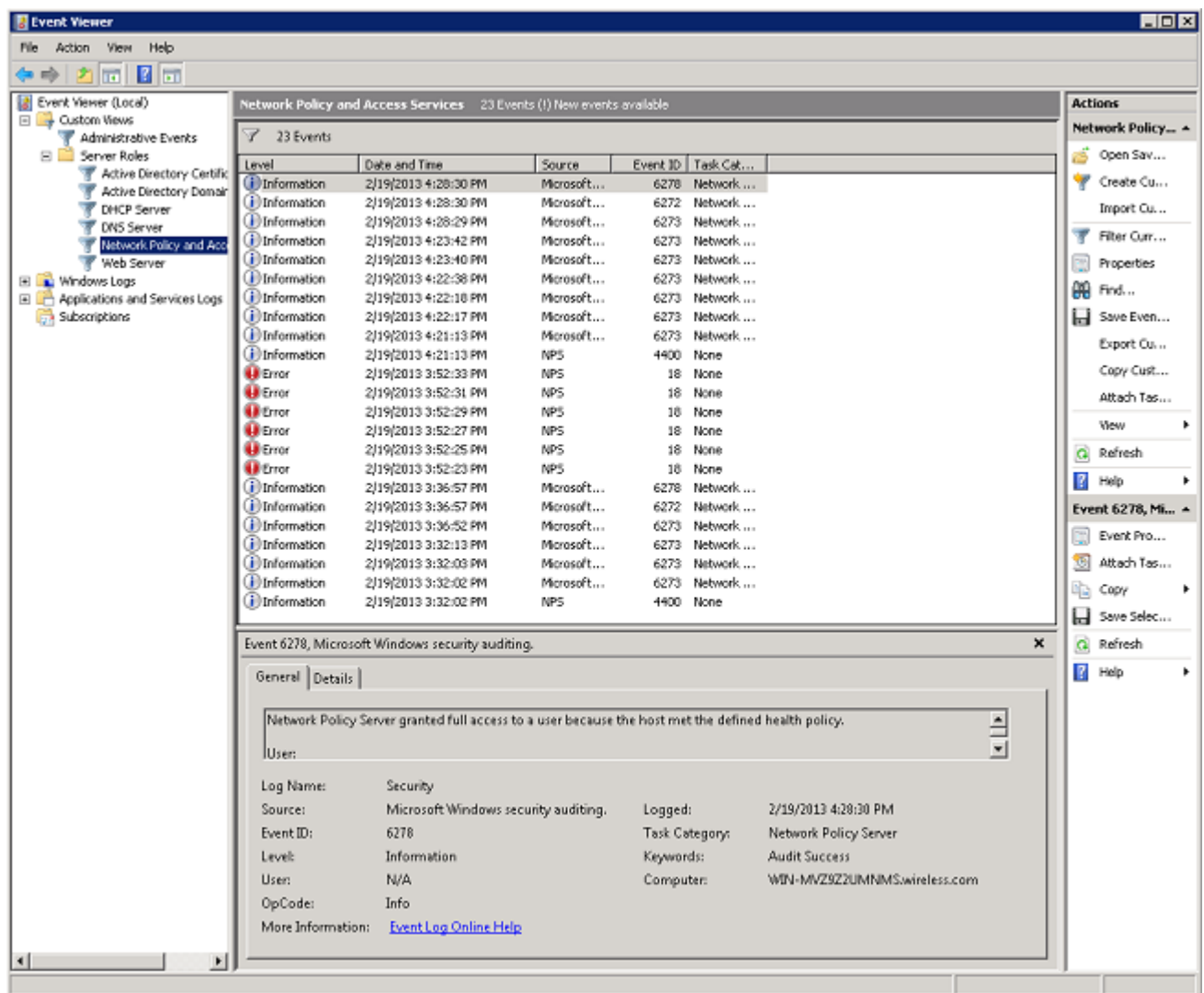
Als u problemen wilt oplossen met het afwijzen van toegang en het uitvoeren van reactietijden, hebt u toegang nodig tot de RADIUS-server. De WLC fungeert als een verificateur die EAP-berichten doorgeeft tussen de client en de RADIUS-server. Een RADIUS-server die reageert met een time-out voor weigering 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.

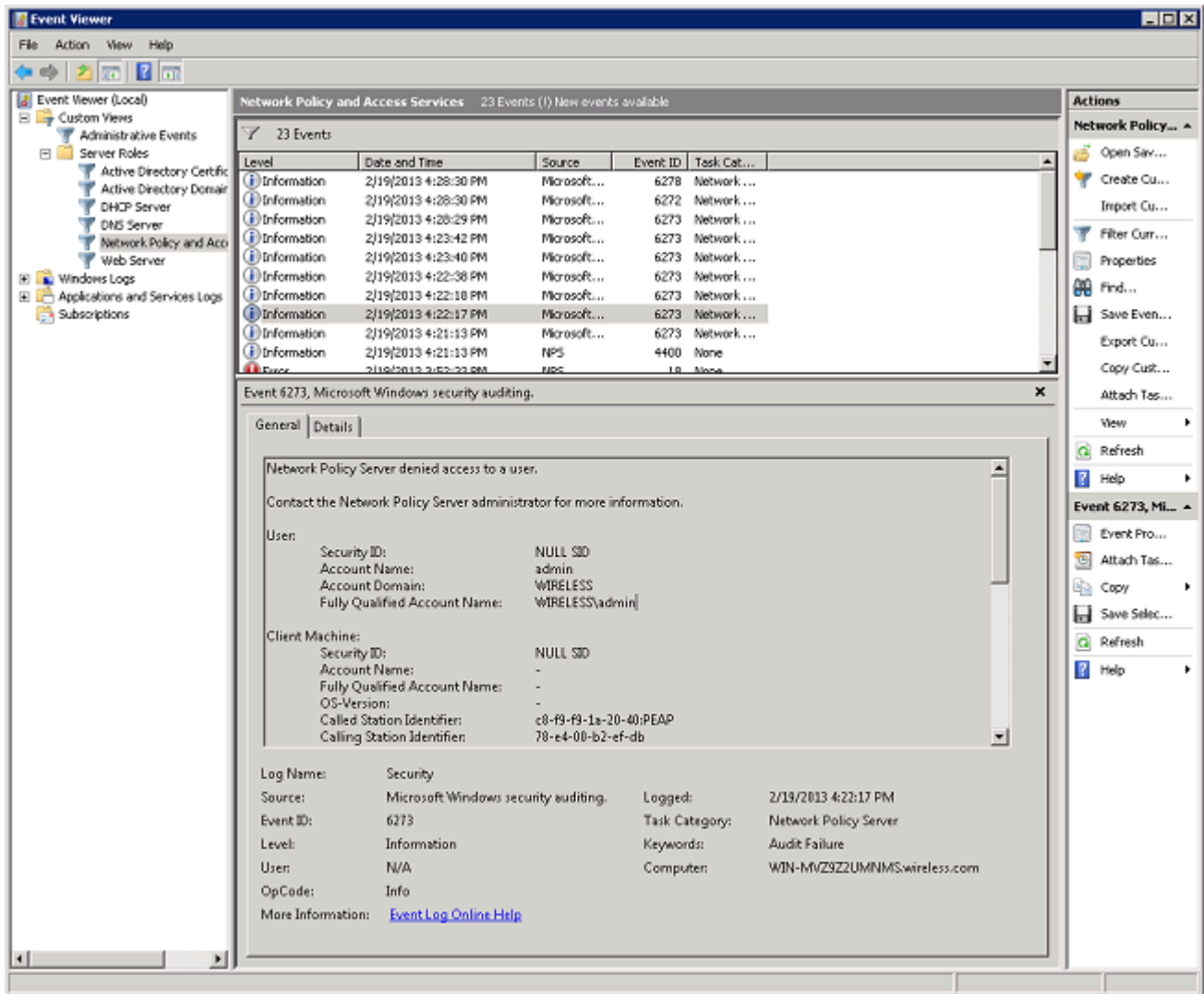
Als u problemen wilt oplossen met toegangsafwijzingen en reactietime-outs vanuit de NPS, bekijkt u de NPS-logs in de Windows Event Viewer op de server.

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-debuggs.

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:

Authentication Details:

Proxy Policy Name: Use Windows authentication for all users

Network Policy Name: -

Authentication Provider: Windows

Authentication Server: WIN-MVZ9Z2UMNMS.wireless.com

Authentication Type: EAP

EAP Type: -

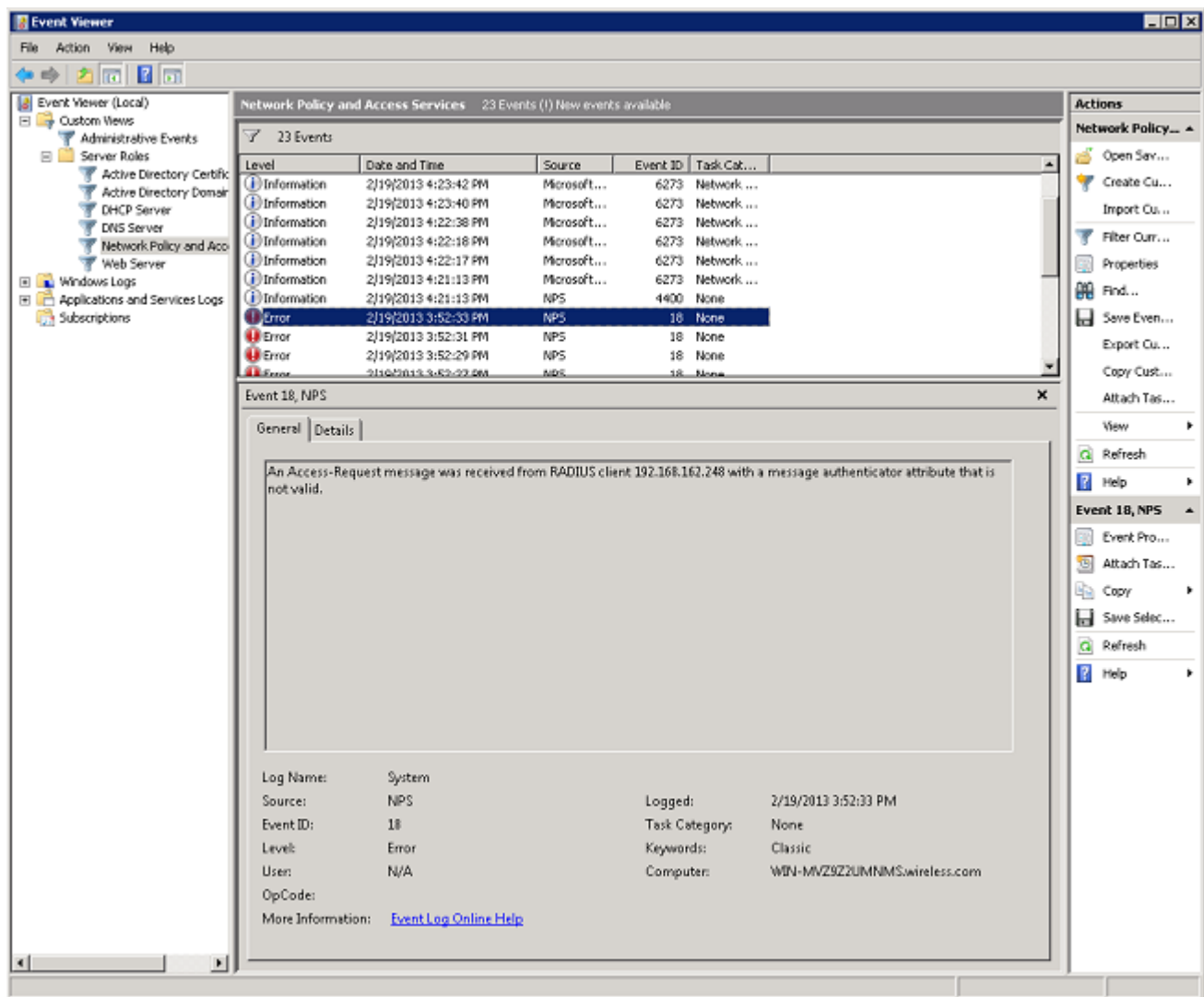
Account Session Identifier: -

Reason Code: 8

Reason: The specified user account does not exist.

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.