PEAP onder UWN's met ACS 5.1- en Windows 2003-server

Inhoud

Inleiding

Dit document beschrijft hoe u beveiligde draadloze toegang kunt configureren met behulp van

draadloze LAN-controllers, Microsoft Windows 2003-software en Cisco Secure Access Control Server (ACS) 5.1 via Protected Extensible Verification Protocol (PEAP) met Microsoft Challenge Handshake Verification Protocol (MS-CHAP) versie 2.

N.B.: Raadpleeg de Microsoft Wi-Fi-website en Cisco SAFE Wireless Blueprint voor informatie over de implementatie van beveiligde draadloze verbindingen.

Voorwaarden

Vereisten

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

Raadpleeg voor installatie- en configuratieinformatie voor de Cisco 5508 Series controllers de installatiehandleiding voor de Cisco 5500 Series draadloze controller. Raadpleeg voor installatie- en configuratieinformatie voor Cisco 2100 Series controllers de Quick Start Guide: Cisco 2100 Series draadloze LAN-controller.

U vindt de installatie- en configuratiehandleidingen voor Microsoft Windows 2003 op Installing Windows Server 2003 R2 .

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

Windows Server 2003 met SP1, Enterprise Edition, wordt gebruikt zodat automatische inschrijving van gebruikers- en werkstationcertificaten voor PEAP-verificatie kan worden geconfigureerd. Door certificaten automatisch in te schrijven en automatisch te vernieuwen, kunt u certificaten gemakkelijker implementeren en de beveiliging verbeteren door certificaten automatisch te verlopen en te vernieuwen.

Gebruikte componenten

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

- Cisco 2106 of 5508 Series controller waarop 7.0.98.0 wordt uitgevoerd
- Cisco 1142 lichtgewicht access point protocol (WAP) access point
- Windows 2003 Enterprise met Internet Information Server (IIS), certificaatinstantie (CA), DHCP en geïnstalleerd Domain Name System (DNS)
- Cisco 1121 Secure Access Control System-applicatie (ACS) 5.1
- Windows XP Professional met SP (en bijgewerkte Service Packs) en draadloze netwerkinterfacekaart (NIC) (met CCX v3-ondersteuning) of een externe leverancier.
- Cisco 3750 Switch

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

Conventies

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

Configureren

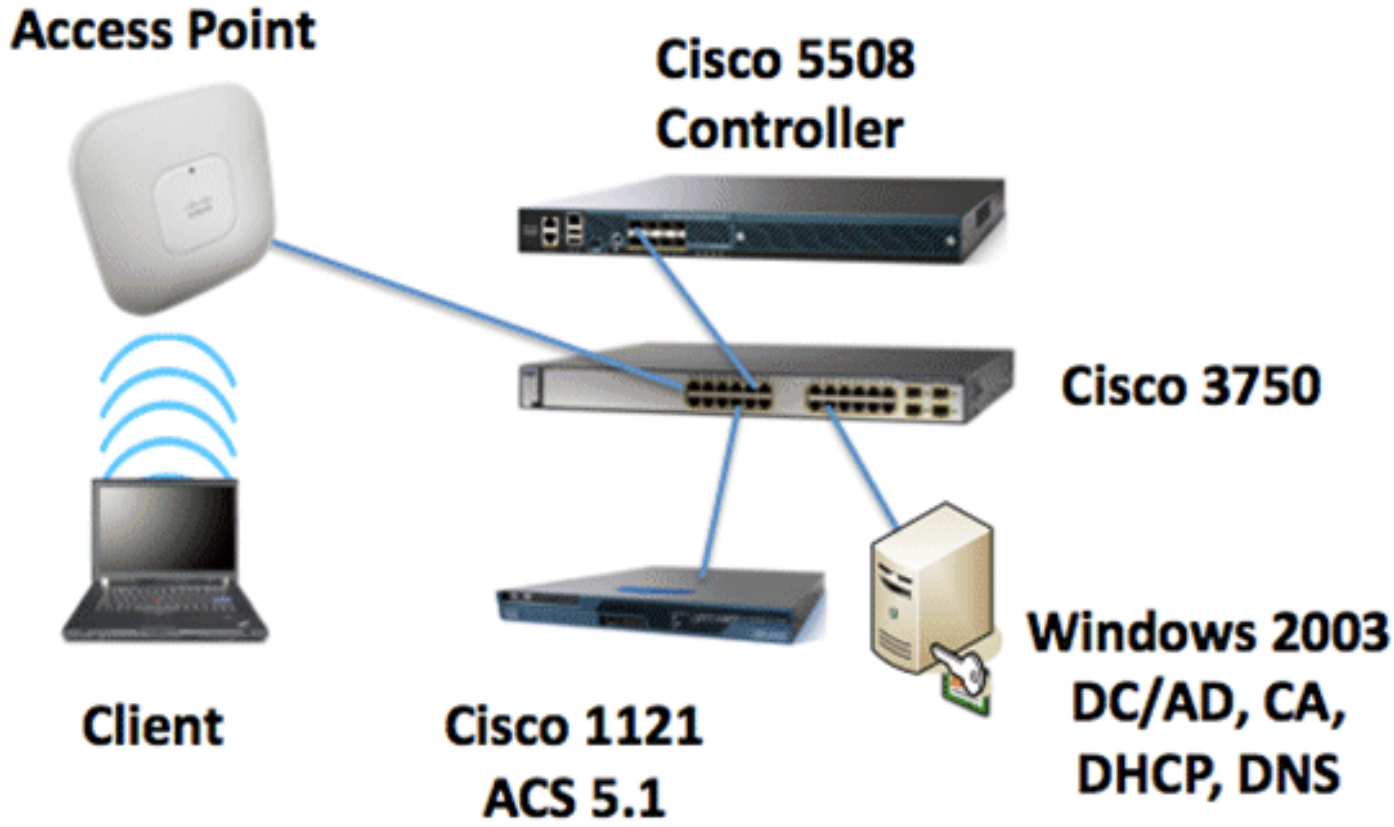
Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

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

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:

Cisco Secure Wireless Lab-topologie



Het belangrijkste doel van dit document is u de stapsgewijze procedure te bieden voor de implementatie van PEAP onder Unified Wireless Networks met ACS 5.1 en de Windows 2003 Enterprise-server. De belangrijkste nadruk ligt op automatische inschrijving van de client, zodat de client automatisch inschrijft en het certificaat van de server haalt.

Opmerking: Raadpleeg WPA2/Wireless Provisioning Services Information Element (WPS IE) update voor Windows XP met Service Pack 2 om Wi-Fi Protected Access (WPA)/WPA2 met Temporal Key Integrity Protocol (TKIP)/Advanced Encryption Standard (AES) toe te voegen aan Windows XP Professional met SP .

Windows Enterprise 2003 Setup met IIS, certificeringsinstantie, DNS, DHCP (CA)

CA (democratie)

CA is een computer die Windows Server 2003 met SP2, Enterprise Edition, draait en deze rollen uitvoert:

- Een domeincontroller voor het **demo.local** domein dat IIS uitvoert
- Een DNS-server voor het **demo.local** DNS-domein
- Een DHCP-server
- Enterprise root CA voor het **demo.local** domein

Voer de volgende stappen uit om CA voor deze services te configureren:

1. Voer een eenvoudige installatie en configuratie uit.
2. Configureer de computer als een domeincontroller.
3. Verhoog het functionele niveau van het domein.
4. DHCP installeren en configureren.
5. Installeer de certificaatservices.
6. Controleer de beheerdersrechten voor certificaten.
7. Voeg computers toe aan het domein.
8. Draadloze toegang tot computers toestaan.
9. Voeg gebruikers toe aan het domein.
10. Verleen draadloze toegang aan gebruikers.
11. Voeg groepen toe aan het domein.
12. Voeg gebruikers toe aan de groep draadloze gebruikers.
13. Voeg clientcomputers toe aan de groep draadloze gebruikers.

Basisinstallatie en -configuratie uitvoeren

Voer de volgende stappen uit:

1. Installeer Windows Server 2003 met SP2, Enterprise Edition, als een zelfstandige server.
2. Configureer het TCP/IP-protocol met het IP-adres van *10.0.10.10* en het subnetmasker van *255.255.255.0*.

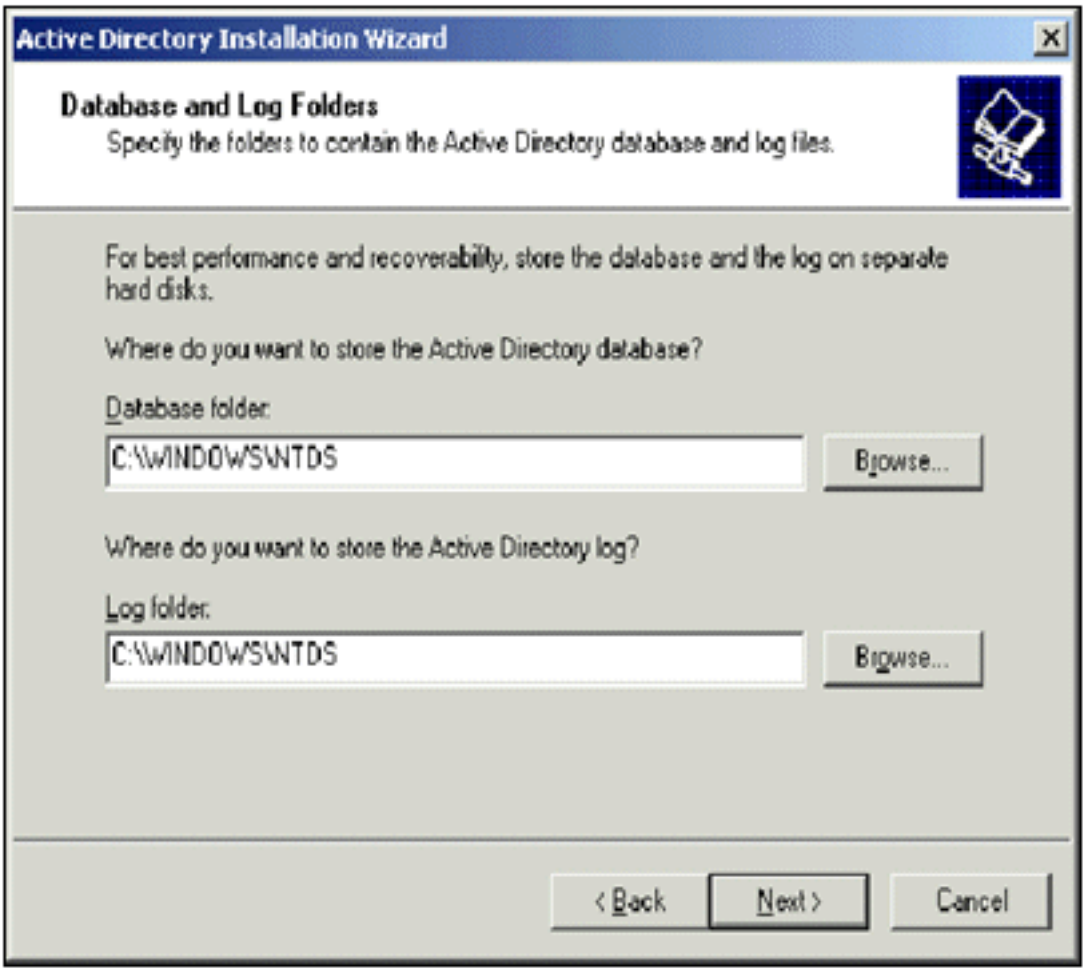
De computer configureren als een domeincontroller

Voer de volgende stappen uit:

1. Als u de installatiewizard van Active Directory wilt starten, kiest u **Start > Uitvoeren**, **typt u dcpromo.exe** en klikt u op **OK**.
2. Klik op de pagina Welkom bij de installatiewizard van Active Directory op **Volgende**.
3. Klik op de pagina Besturingssysteemcompatibiliteit op **Volgende**.
4. Selecteer op de pagina Domain Controller Type de optie **Domain Controller voor een nieuw domein** en klik op **Volgende**.
5. Selecteer op de pagina Nieuw domein maken de optie **Domein in een nieuw bos** en klik op

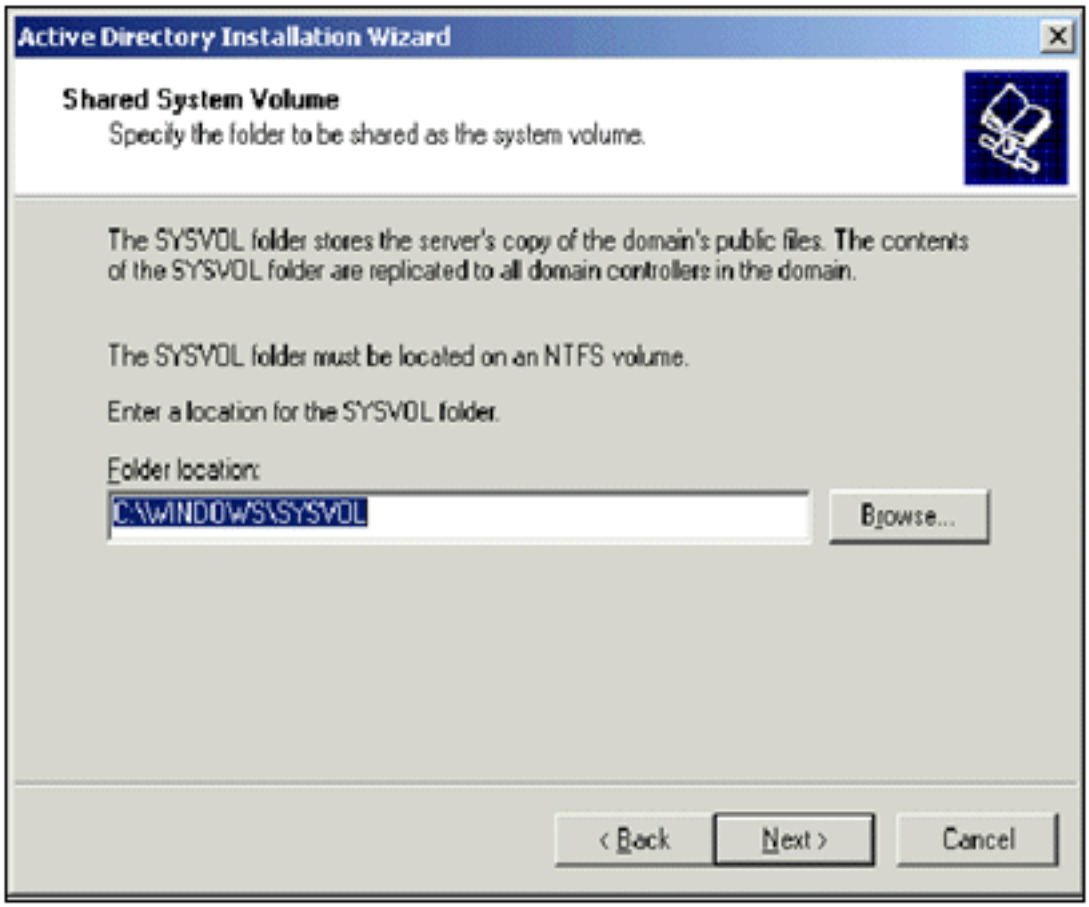
Volgende.

6. Op de pagina Installeer of stel DNS in, selecteer **Nee, installeer en configureer DNS op deze computer** en klik op **Volgende**.
7. Typ op de pagina Nieuwe domeinnaam **demo.local** en klik op **Volgende**.
8. Voer op de pagina Domain Name van NetBIOS de Domain NetBIOS-naam in als **demo** en klik op **Next**.
9. Accepteer op de pagina Locaties voor database- en logmappen de standaarddirectory's voor database- en logmappen en klik op



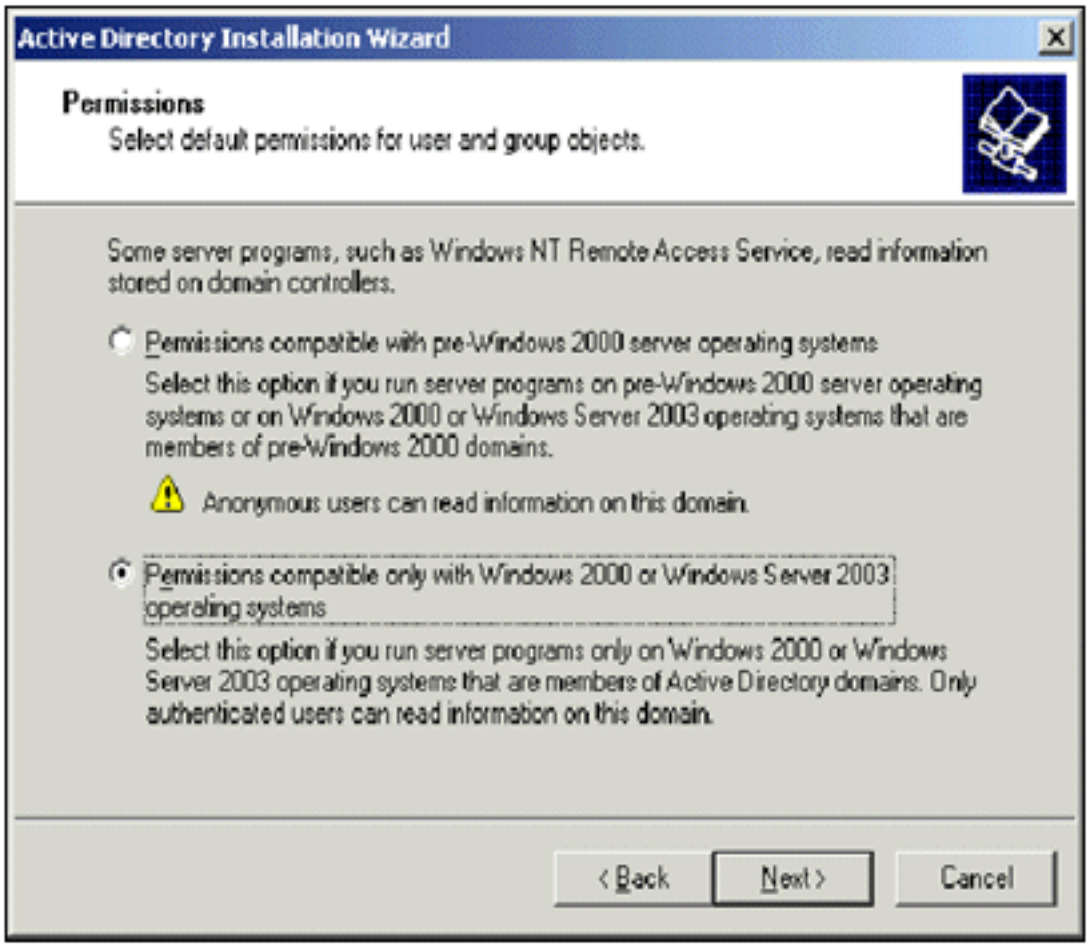
Volgende.

10. Controleer op de pagina Gedeeld systeemvolume of de standaardmaplocatie correct is en klik op



Volgende.

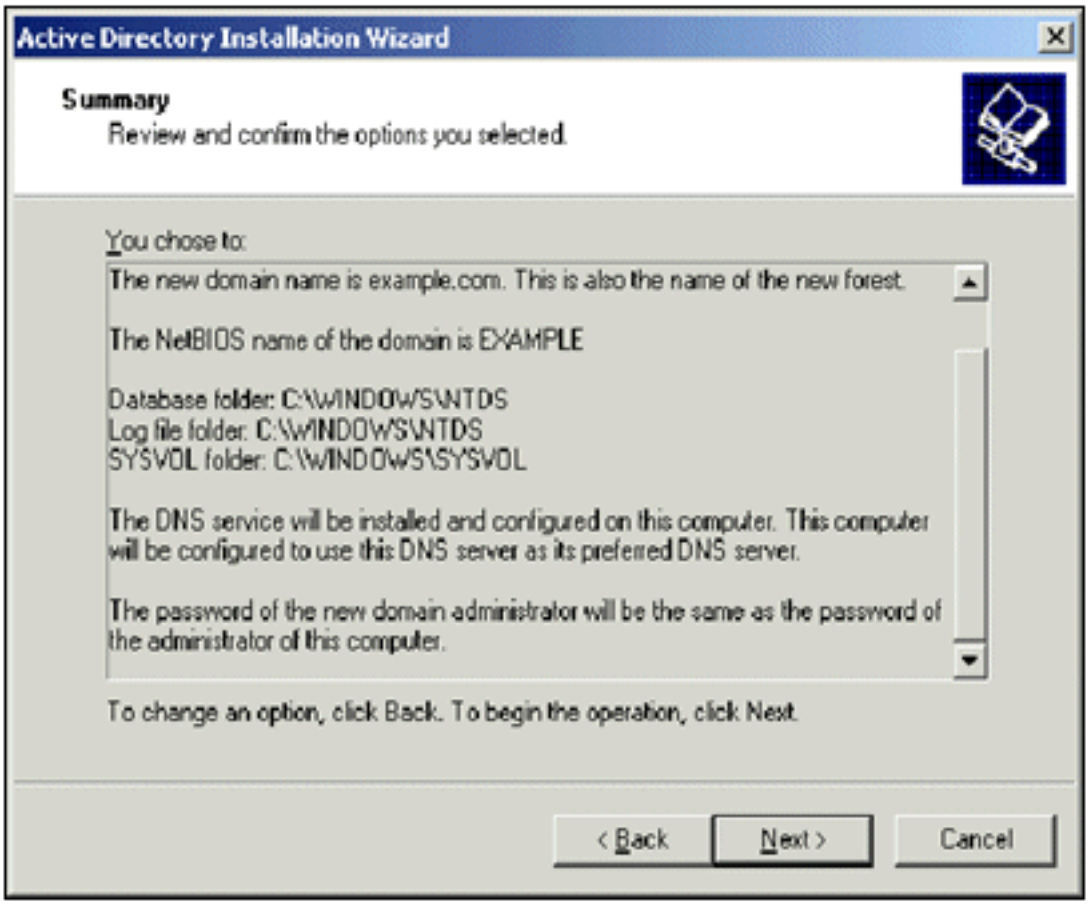
11. Controleer op de pagina **Rechten** of **alleen toegangsrechten die compatibel zijn met de besturingssystemen Windows 2000 of Windows Server 2003** zijn geselecteerd en klik op



Volgende.

12. Laat op de pagina Directory Services Recovery Mode Management Password de wachtwoordvakjes leeg en klik op **Volgende**.

13. Bekijk de informatie op de pagina Samenvatting en klik op **Volgende**.

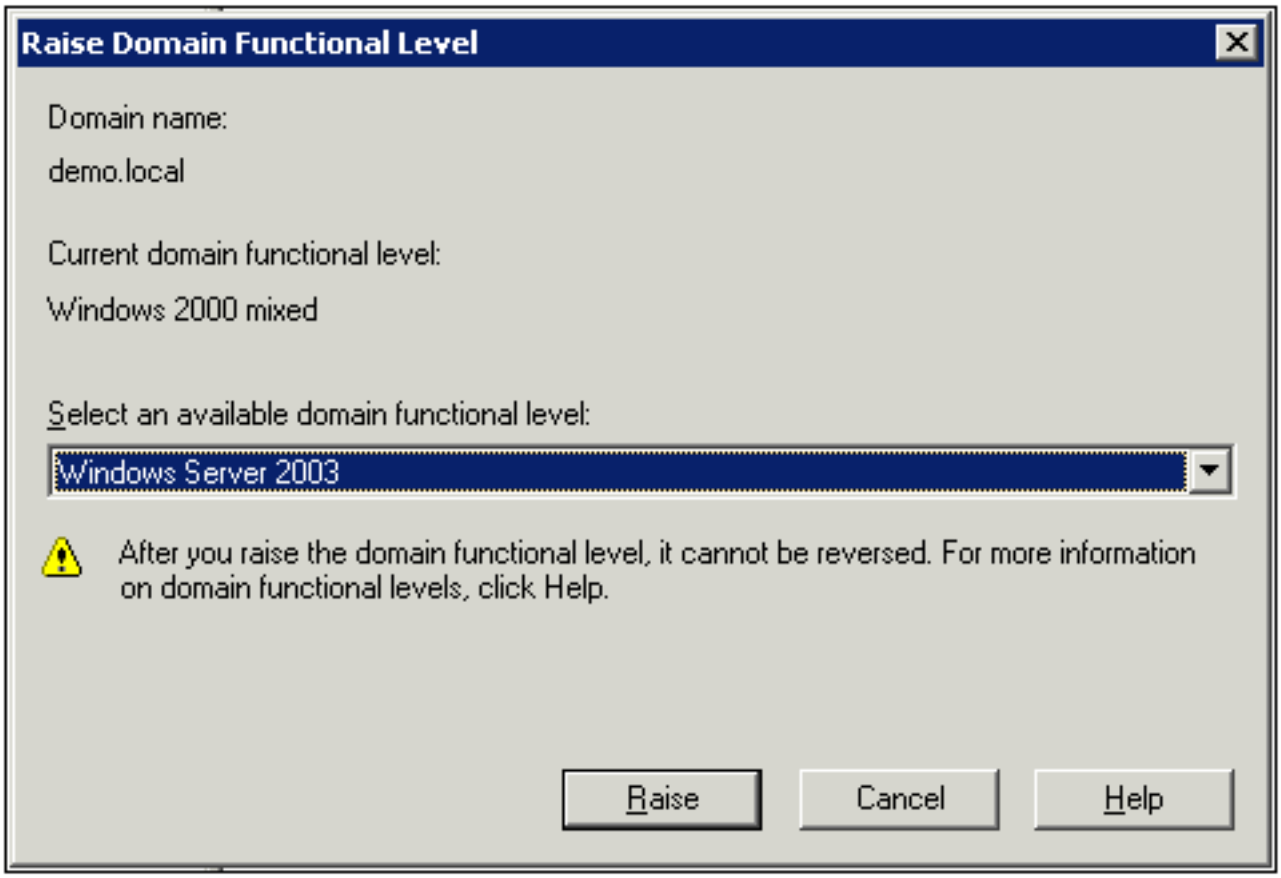


14. Wanneer u klaar bent met de installatie van Active Directory, klikt u op **Voltooien**.
15. Wanneer u wordt gevraagd de computer opnieuw op te starten, klikt u op **Nu opnieuw starten**.

Het functionele niveau van het domein verhogen

Voer de volgende stappen uit:

1. Open de invoegtoepassing Active Directory Domains and Trusts vanuit de map Administrative Tools (Start > Programma's > Administratieve tools > **Active Directory Domains and Trusts**) en klik vervolgens met de rechtermuisknop op de domeincomputer **CA.demo.local**.
2. Klik op **Functioneel niveau domein verhogen** en selecteer vervolgens **Windows Server 2003** op de pagina Functioneel niveau domein verhogen.

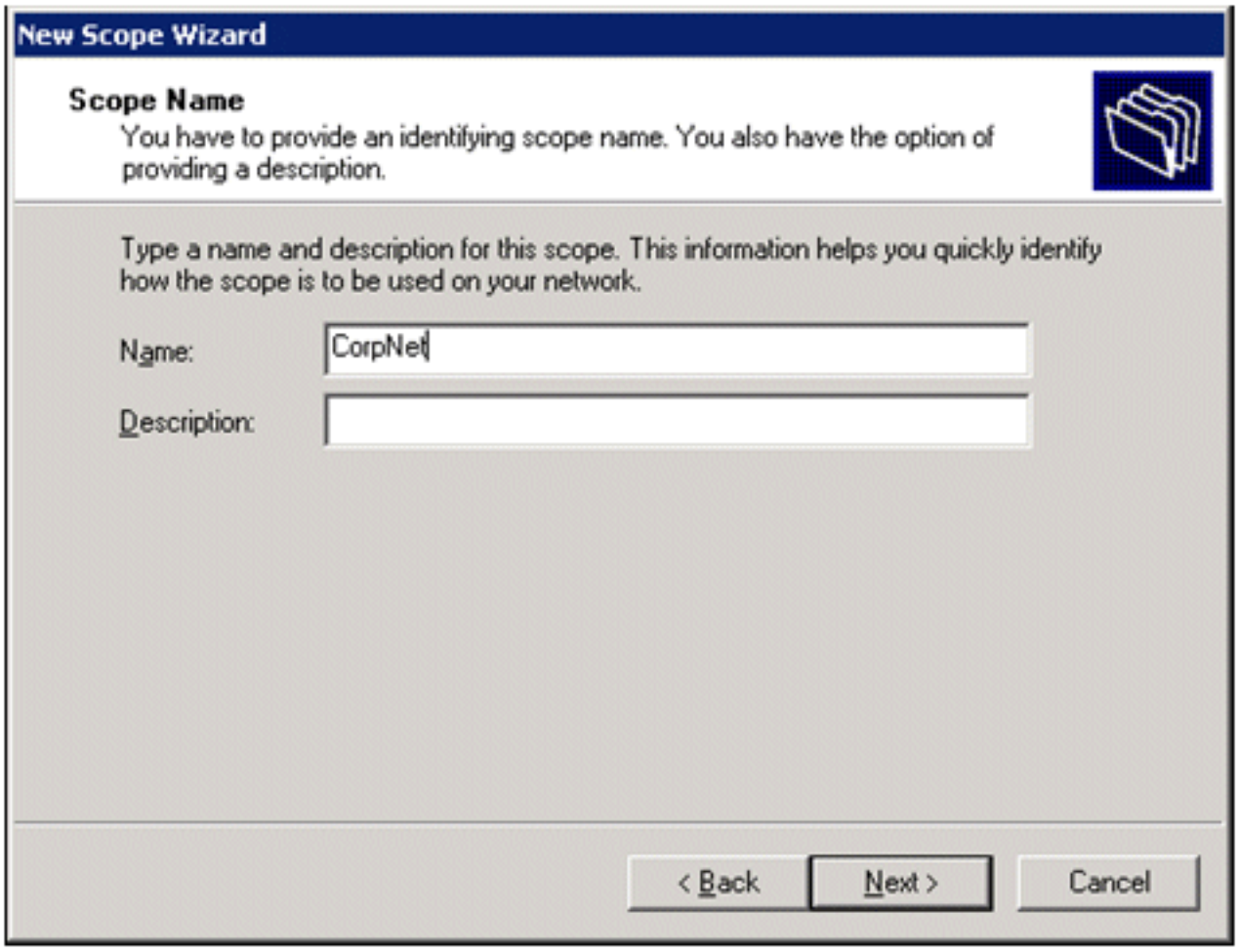


3. Klik op **Verhogen**, klik op **OK** en klik vervolgens nogmaals op **OK**.

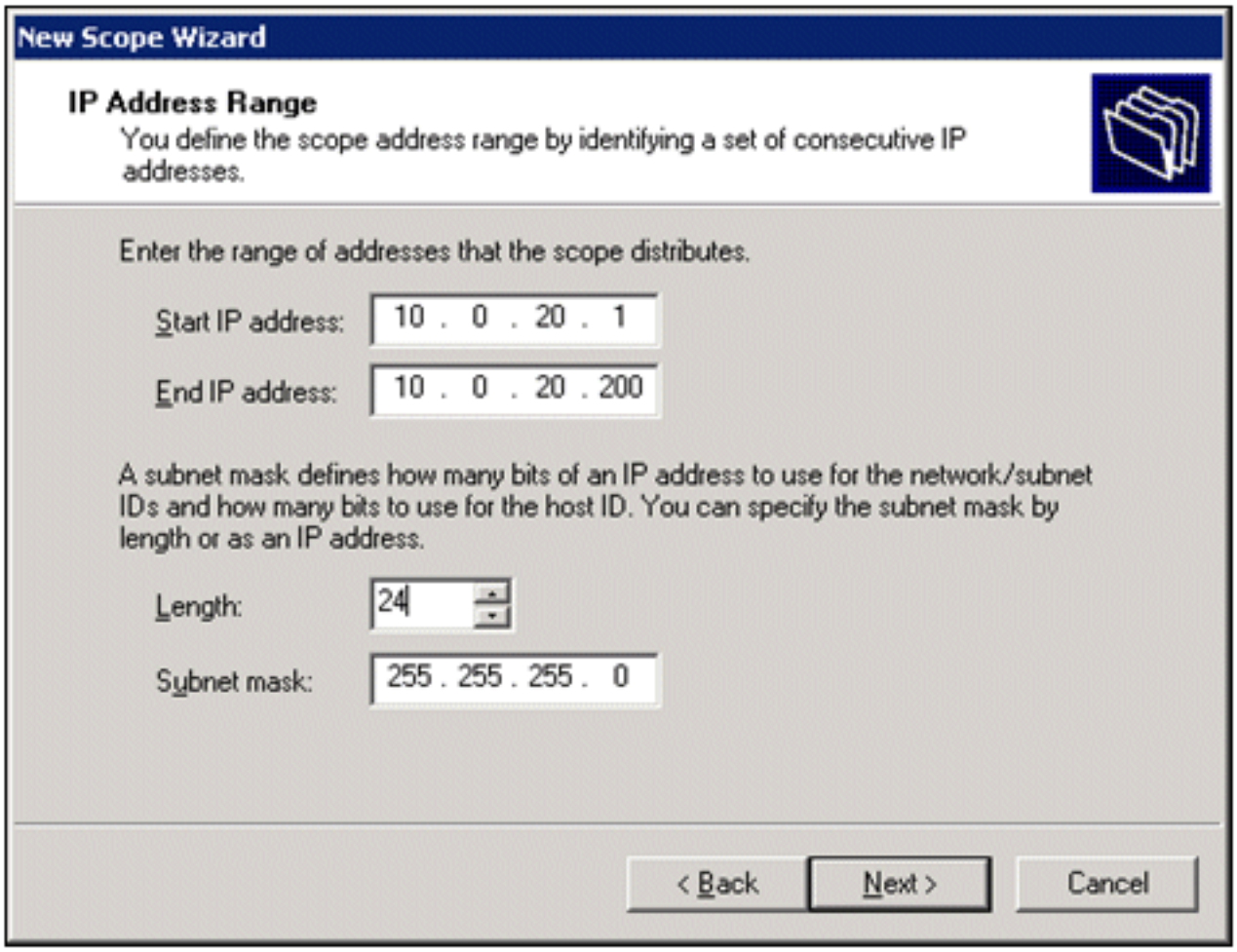
DHCP installeren en configureren

Voer de volgende stappen uit:

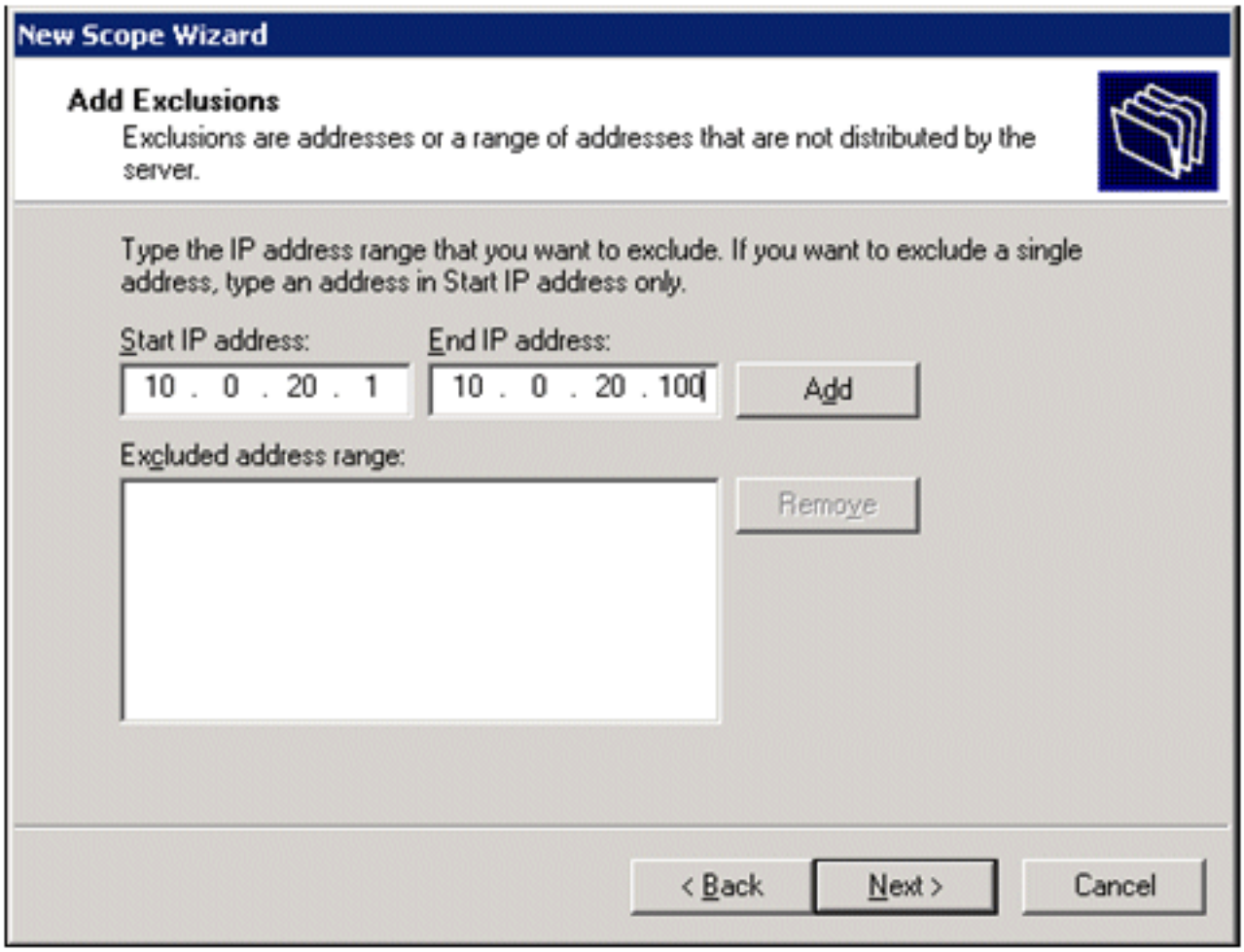
1. Installeer **Dynamic Host Configuration Protocol (DHCP)** als een **netwerkservicecomponent** met behulp van **Software** in het Configuratiescherm.
2. Open de invoegtoepassing DHCP vanuit de map Systeembeheer (Start > Programma's > Hulpprogramma's > **DHCP**) en markeer vervolgens de DHCP-server **CA.demo.local**.
3. Klik op **Action** en klik vervolgens op **Autoriseren** om de DHCP-service te autoriseren.
4. Klik in de consolestructuur met de rechtermuisknop op **CA.demo.local** en klik vervolgens op **Nieuw bereik**.
5. Klik op de welkomstpagina van de wizard Nieuw bereik op **Volgende**.
6. Typ op de pagina Naam bereik **CorpNet** in het veld Naam.



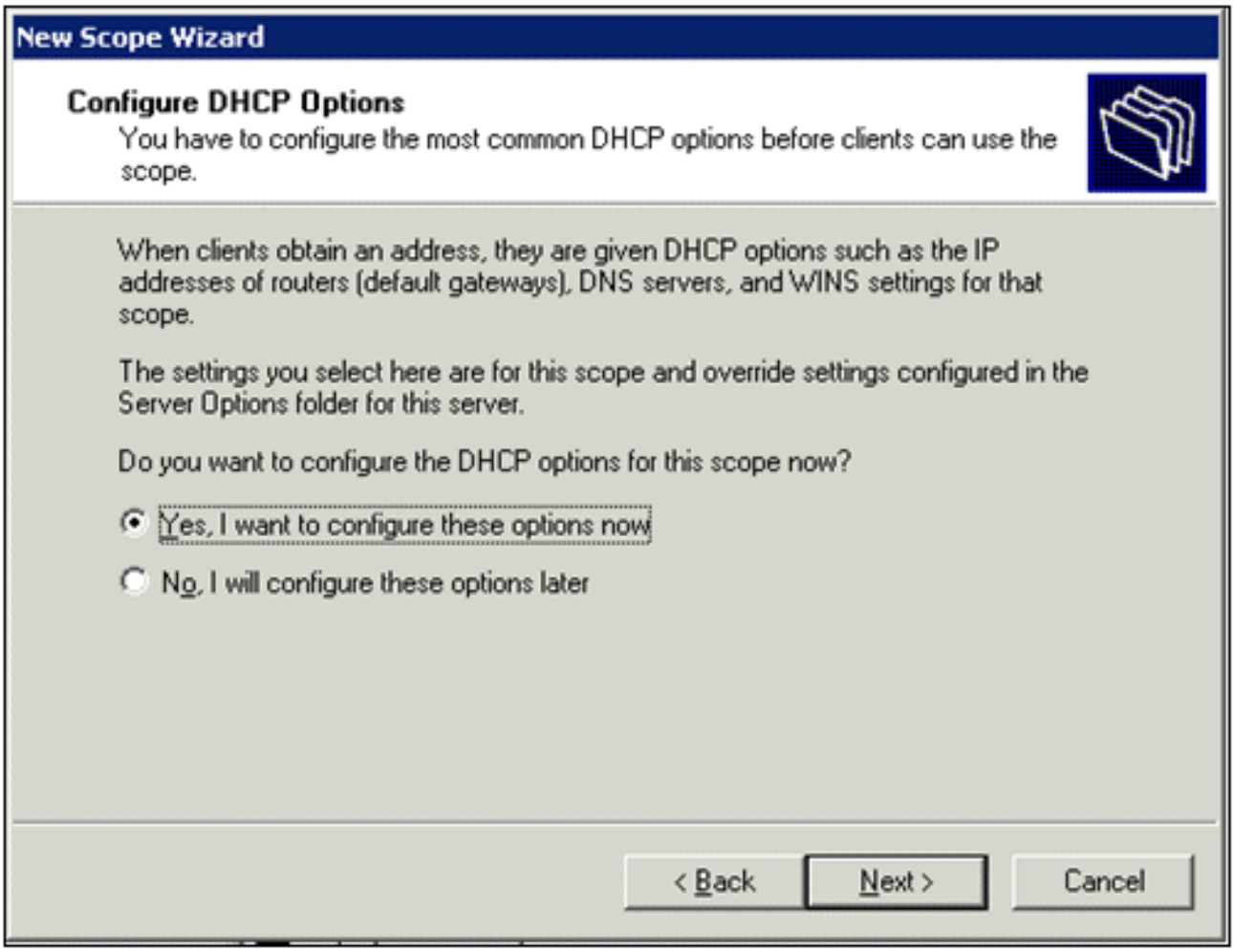
7. Klik op **Volgende** en vul deze parameters in:IP-adres starten - **10.0.20.1**Einde IP-adres - **10.0.20.2010**Lengte - **24**Subnetmasker - **255.255.255.0**



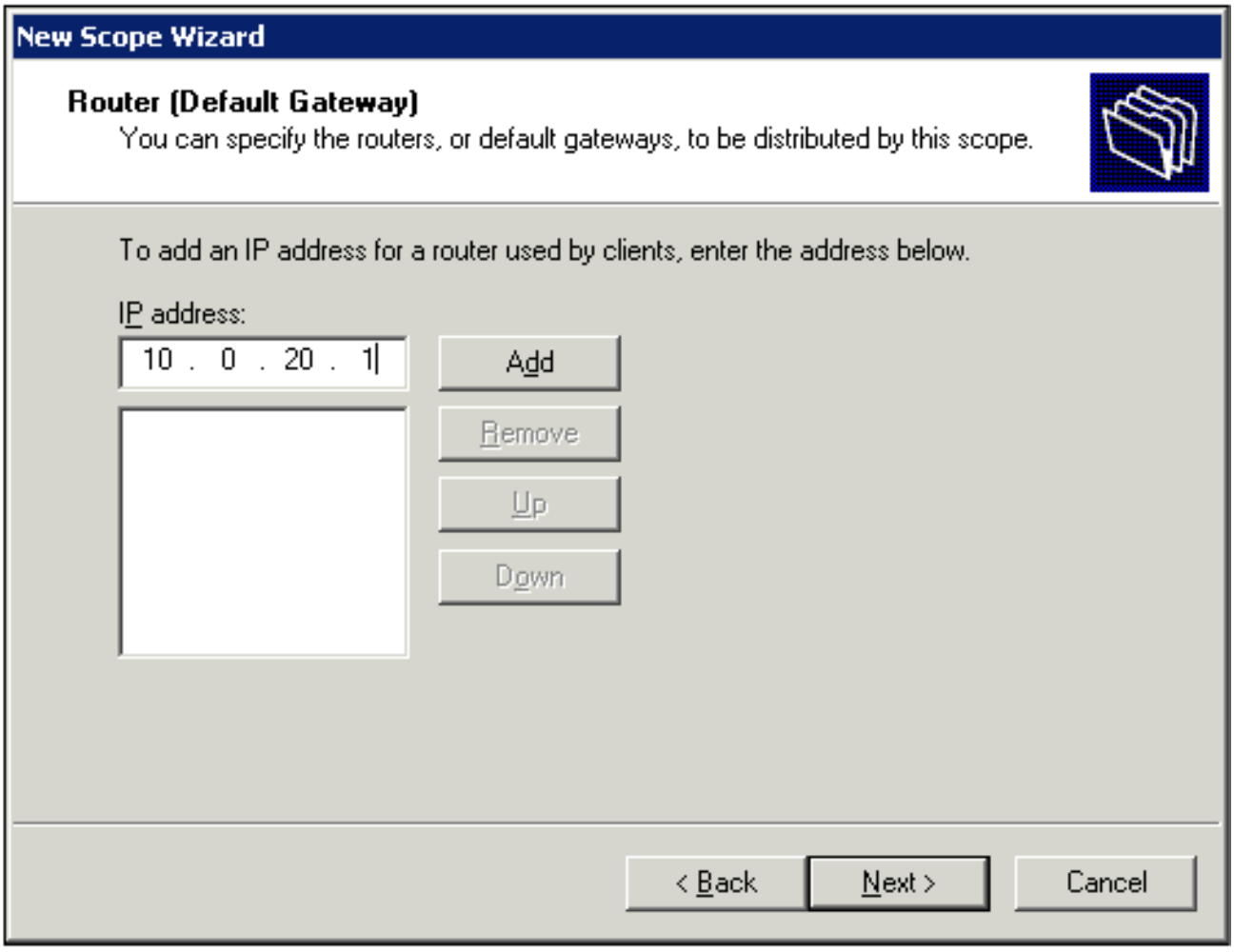
8. Klik op **Volgende** en voer *10.0.20.1 in* voor het IP-adres Start en *10.0.20.100* voor de uitsluiting van het IP-adres End. Klik vervolgens op **Volgende**. Hierbij worden de IP-adressen tussen 10.0.20.1 en 10.0.20.100 gereserveerd. Deze IP-adressen worden niet toegewezen door de DHCP-
server.



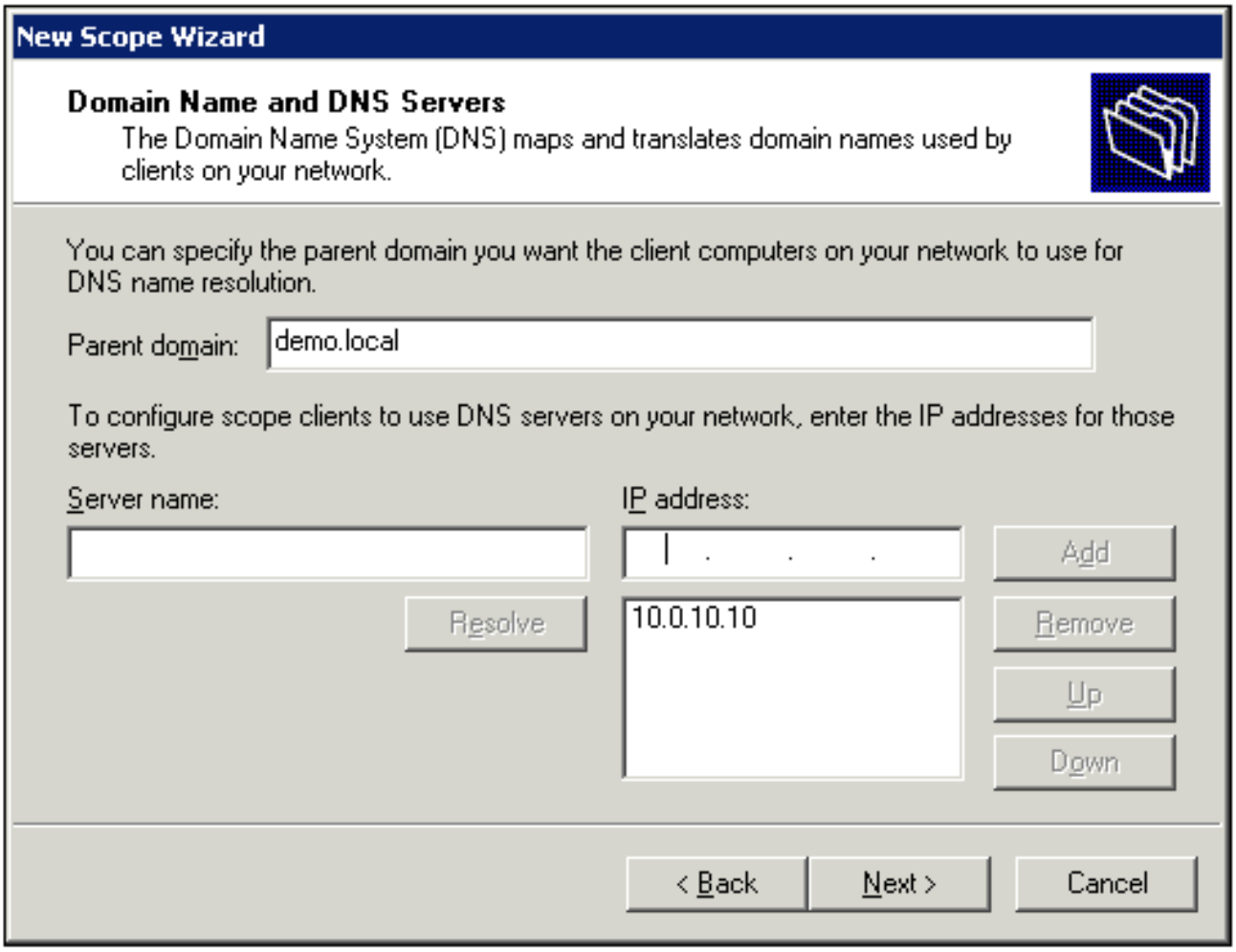
9. Klik op de pagina Looptijd op **Volgende**.
10. Kies op de pagina DHCP-opties configureren **Ja, ik wil deze opties nu configureren** en klik op
    Volgende.



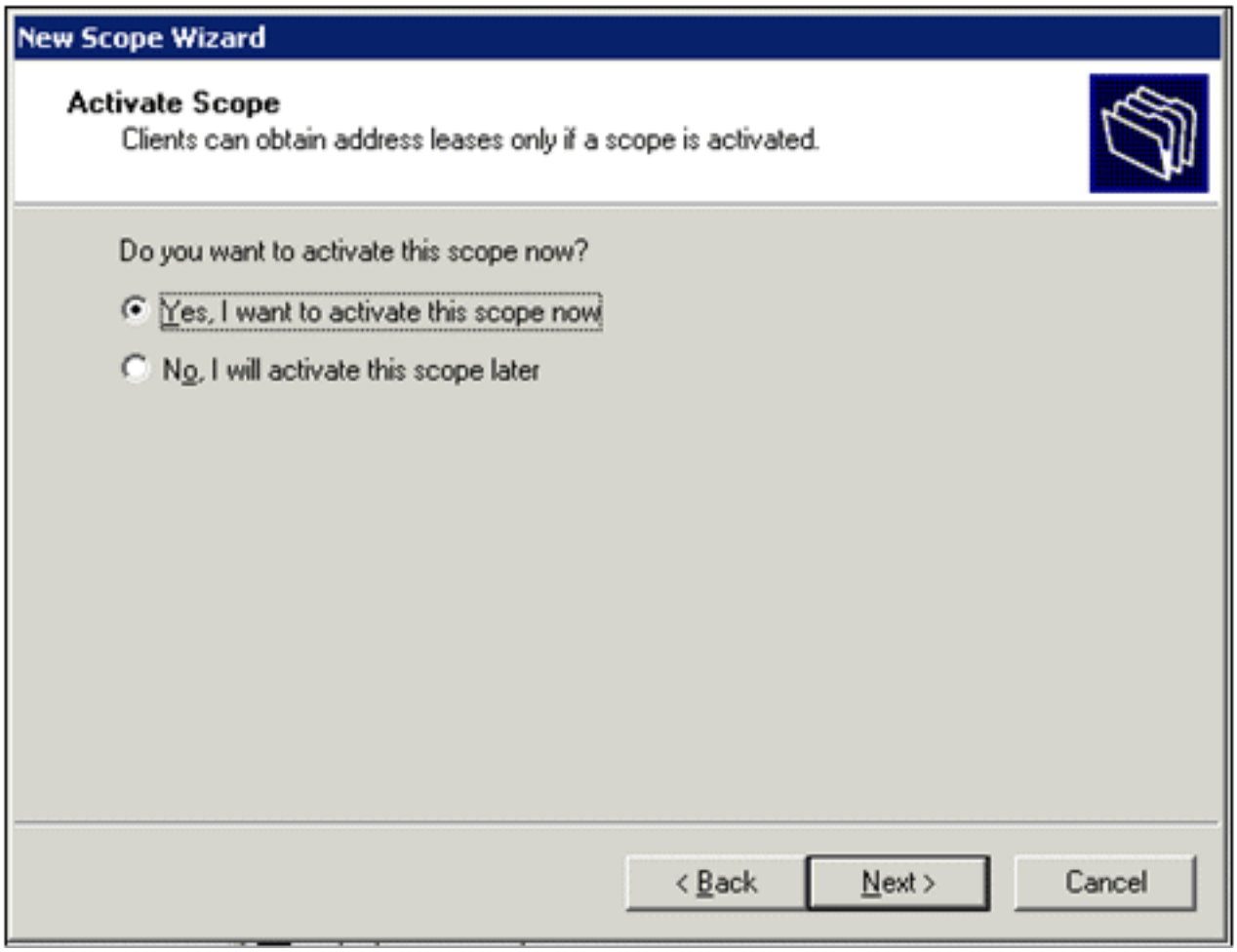
11. Op de pagina Router (Default Gateway) voegt u het standaardrouteradres van *10.0.20.1 toe* en klikt u op
Volgende.



12. Typ op de pagina Domeinnaam en DNS-servers *demo.local* in het veld Ouderdomein, type *10.0.10.10* in het veld IP-adres en klik vervolgens op **Toevoegen** en klik op **Volgende**.



13. Klik op de pagina WINS-servers op **Volgende**.
14. Kies **Ja** op de pagina Werkingsbereik activeren**, ik wil dit bereik nu activeren** en klik op **Volgende**.



15. Wanneer u klaar bent met de pagina New Scope Wizard, klikt u op **Finish**.

Certificaatservices installeren

Voer de volgende stappen uit:

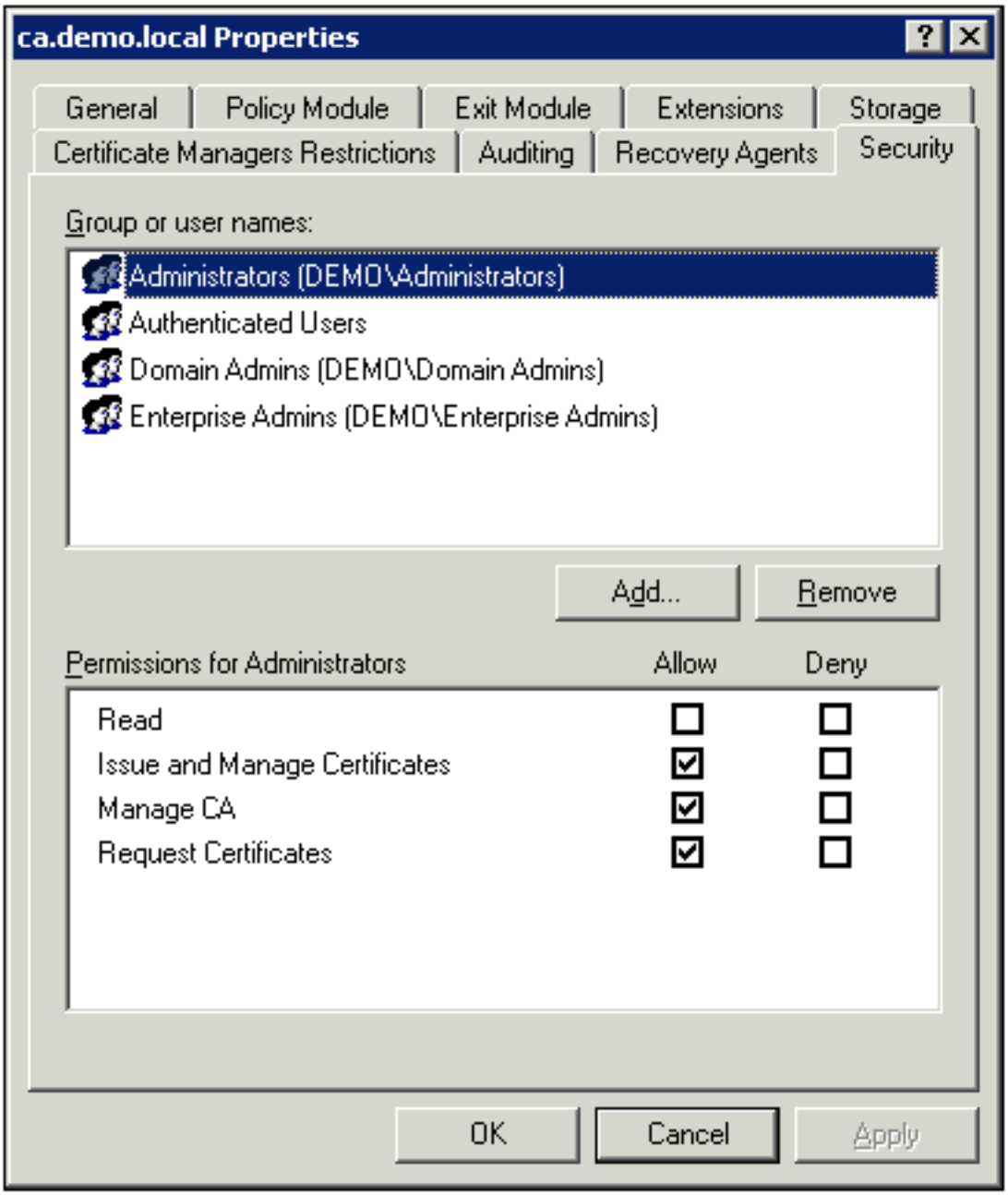
Opmerking: IIS moet worden geïnstalleerd voordat u de certificaatservices installeert en de gebruiker moet deel uitmaken van de Enterprise Admin OU.

1. Open in het Configuratiescherm de optie **Software** en klik vervolgens op **Windows-onderdelen toevoegen of verwijderen**.
2. Kies op de pagina Wizard Windows-onderdelen de optie Certificaatservices en klik vervolgens op Volgende.
3. Kies op de pagina CA Type de optie Enterprise root CA en klik op Volgende.
4. Typ op de pagina CA Identifying Information (CA-identificatiegegevens) *democratie* in de algemene naam voor dit CA-vak. U kunt ook de overige optionele details invoeren. Klik vervolgens op **Volgende** en accepteer de standaardwaarden op de pagina Certificaatdatabase-instellingen.
5. Klik op **Next** (Volgende). Klik op **Voltooien** als de installatie is voltooid.
6. Klik op **OK** nadat u het waarschuwingsbericht over het installeren van IIS hebt gelezen.

Controleer beheerderrechten voor certificaten

Voer de volgende stappen uit:

1. Kies **Start** > **Administratieve tools** > **Certificeringsinstantie**.
2. Klik met de rechtermuisknop op **democratische CA** en klik vervolgens op **Eigenschappen**.
3. Klik op het tabblad Beveiliging op **Beheerders** in de lijst met groepen of gebruikersnamen.
4. Controleer in de lijst met toegangsrechten voor beheerders of deze opties zijn ingesteld op **Toestaan**:Certificaten afgeven en beherenCA beherenCertificaten aanvragenAls om het even welk van deze worden geplaatst om te ontkennen of niet geselecteerd zijn, plaats de toestemmingen om toe te



staan.

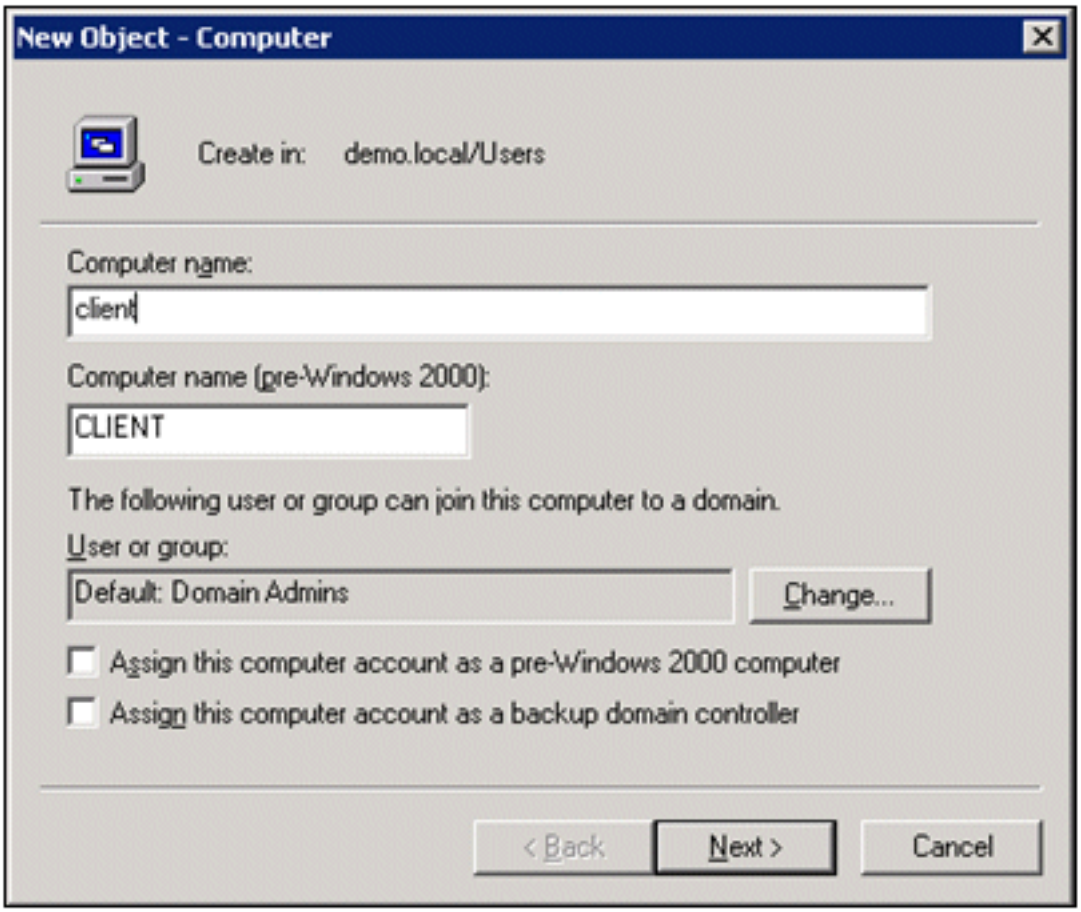
5. Klik op **OK** om het dialoogvenster democratische CA-eigenschappen te sluiten en sluit vervolgens de certificeringsinstantie.

Computers aan het domein toevoegen

Voer de volgende stappen uit:

Opmerking: Als de computer al is toegevoegd aan het domein, gaat u verder met Gebruikers toevoegen aan het domein.

1. Open de invoegtoepassing **Active Directory-gebruikers en -computers**.
2. In de consoleboom, breid **demo.local uit**.
3. Klik met de rechtermuisknop op **Computers**, klik op **Nieuw** en klik vervolgens op **Computer**.
4. Typ in het dialoogvenster Nieuw object - computer de naam van de computer in het veld Computer name en klik op **Volgende**. In dit voorbeeld wordt de computernaam *Client* gebruikt.



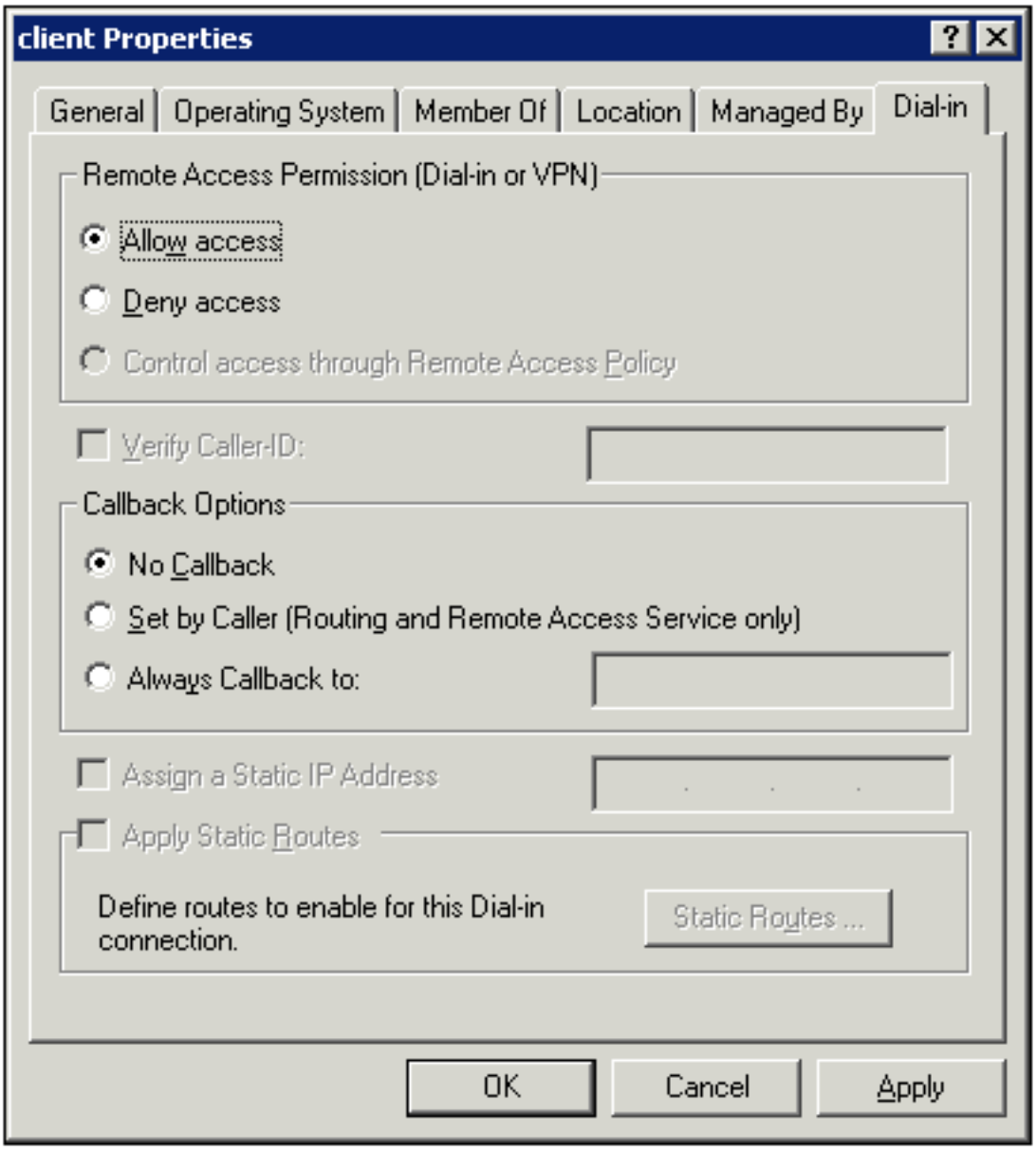
5. Klik in het dialoogvenster Beheerd op **Volgende**.
6. Klik in het dialoogvenster Nieuw object - computer op **Voltooien**.
7. Herhaal stap 3 tot en met 6 om extra computeraccounts te maken.

Draadloze toegang tot computers toestaan

Voer de volgende stappen uit:

1. Klik in de consolestructuur van Active Directory-gebruikers en -computers op de map **Computers** en klik met de rechtermuisknop op de computer waarvoor u draadloze toegang wilt toewijzen. Dit voorbeeld toont de procedure met Computer **Client** die u in stap 7 hebt toegevoegd. Klik op **Eigenschappen** en ga vervolgens naar het tabblad **Inbellen**.
2. In de Toestemming voor externe toegang kiest u **Toegang toestaan** en klikt u op

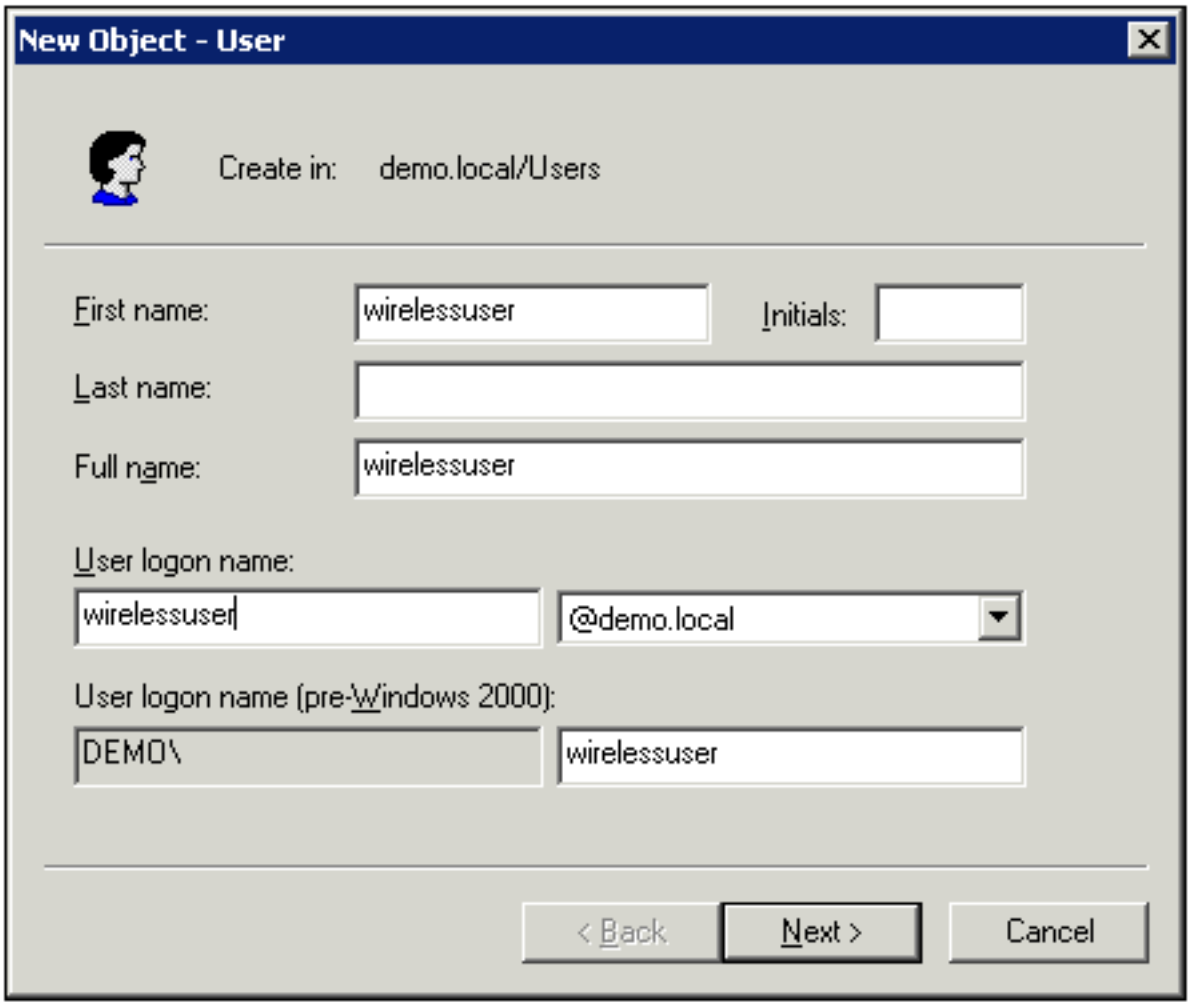
OK.



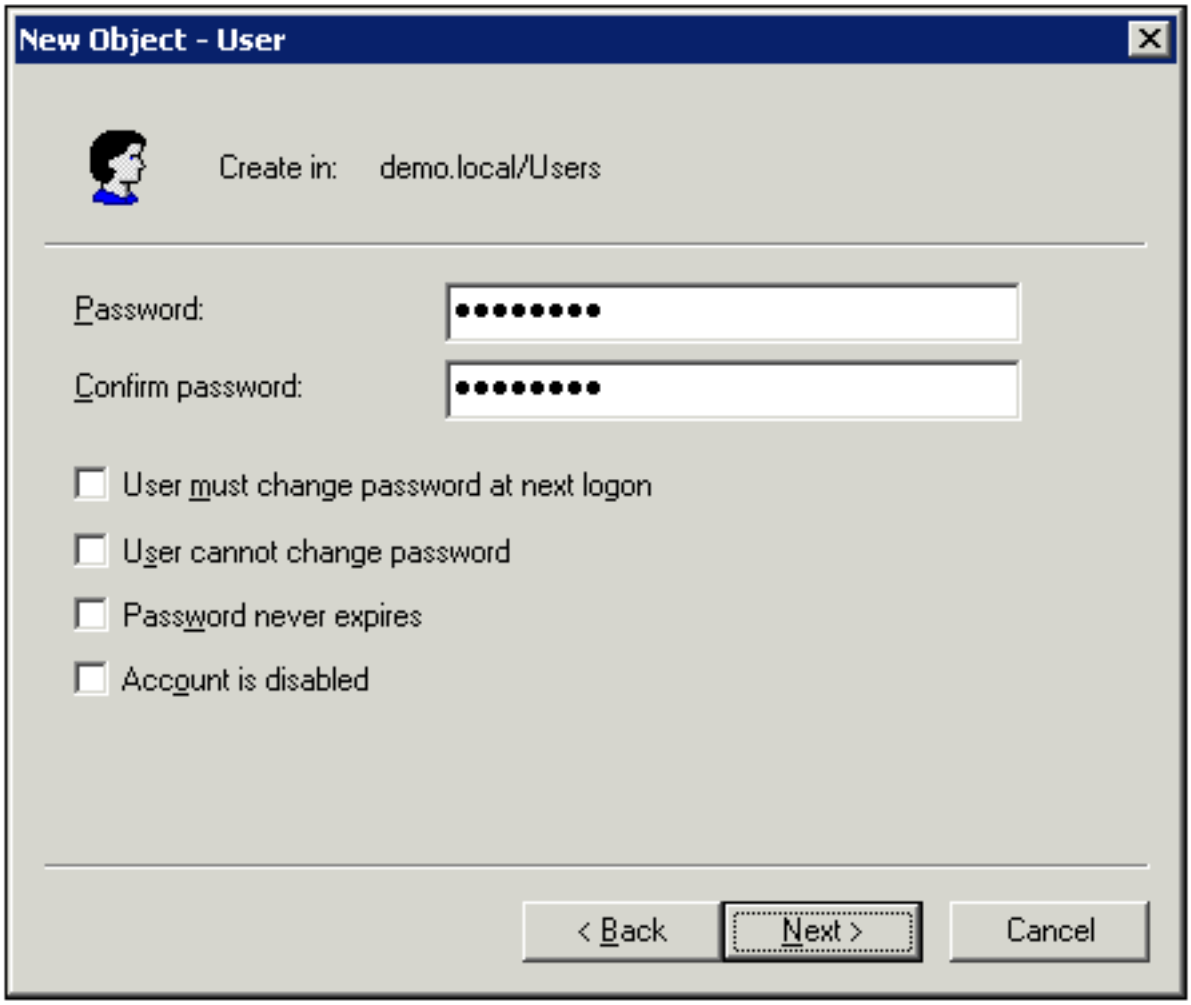
[Gebruikers aan het domein toevoegen]

Voer de volgende stappen uit:

1. In de Active Directory Gebruikers en Computers console boom, klik met de rechtermuisknop op **Gebruikers**, klik op **Nieuw**, en klik vervolgens op **Gebruiker**.
2. Typ in het dialoogvenster Nieuw object - gebruiker de naam van de draadloze gebruiker. In dit voorbeeld wordt de naam van de *draadloze gebruiker* in het veld Voornaam gebruikt en de naam van de *draadloze gebruiker* in het veld Gebruikersnaam voor aanmelding. Klik op **Next**
(Volgende).



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



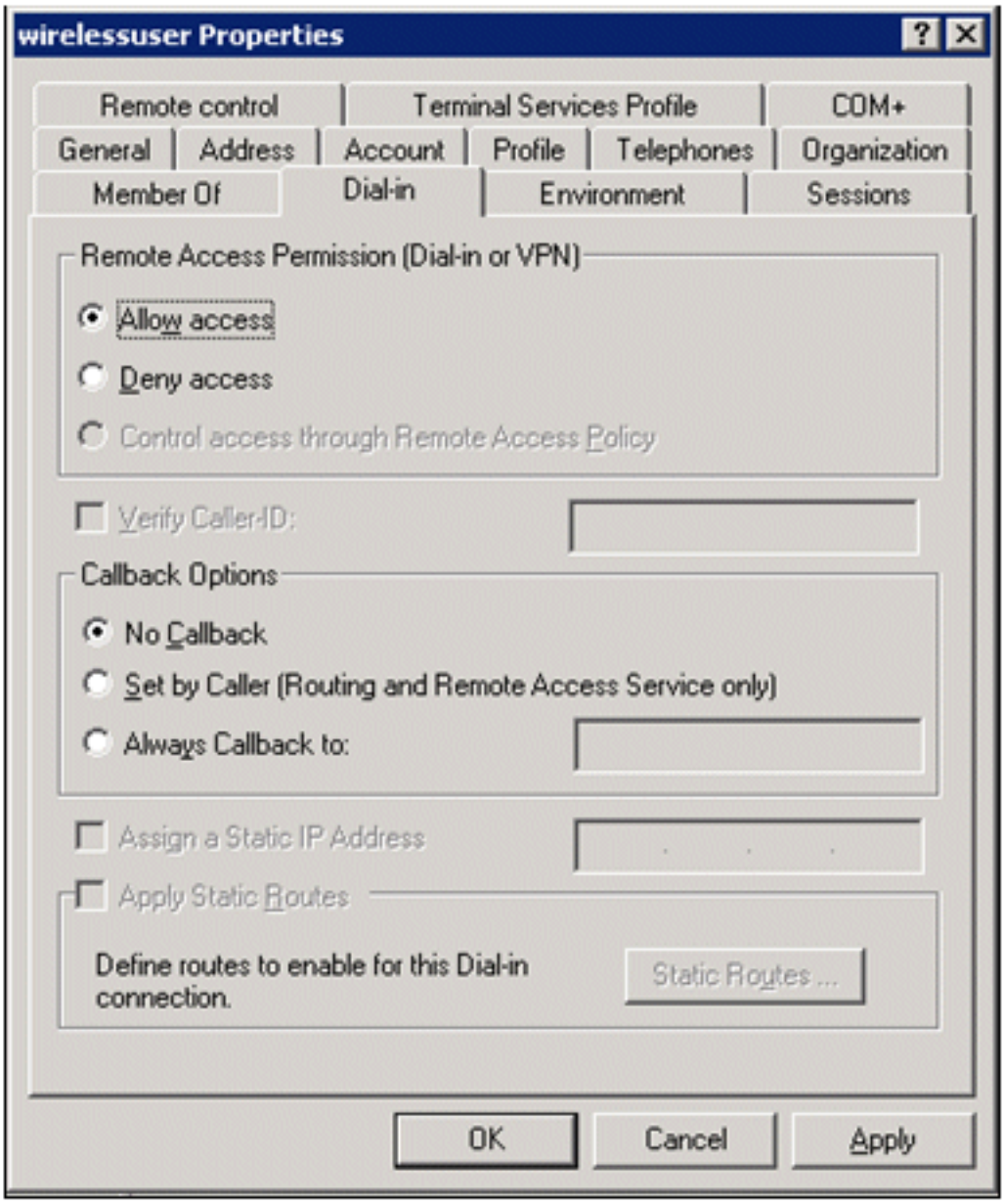
4. Klik in het dialoogvenster Nieuw object - gebruiker op **Voltooien**.
5. Herhaal stap 2 tot en met 4 om extra gebruikersaccounts te maken.

Draadloze toegang voor gebruikers toestaan

Voer de volgende stappen uit:

1. In de Active Directory Gebruikers en Computers console boom, klik op de **Gebruikers** map, klik met de rechtermuisknop op **draadloze gebruiker**, klik op **Eigenschappen**, en ga vervolgens naar het **inbel** tabblad.
2. In de Toestemming voor externe toegang kiest u **Toegang toestaan** en klikt u op

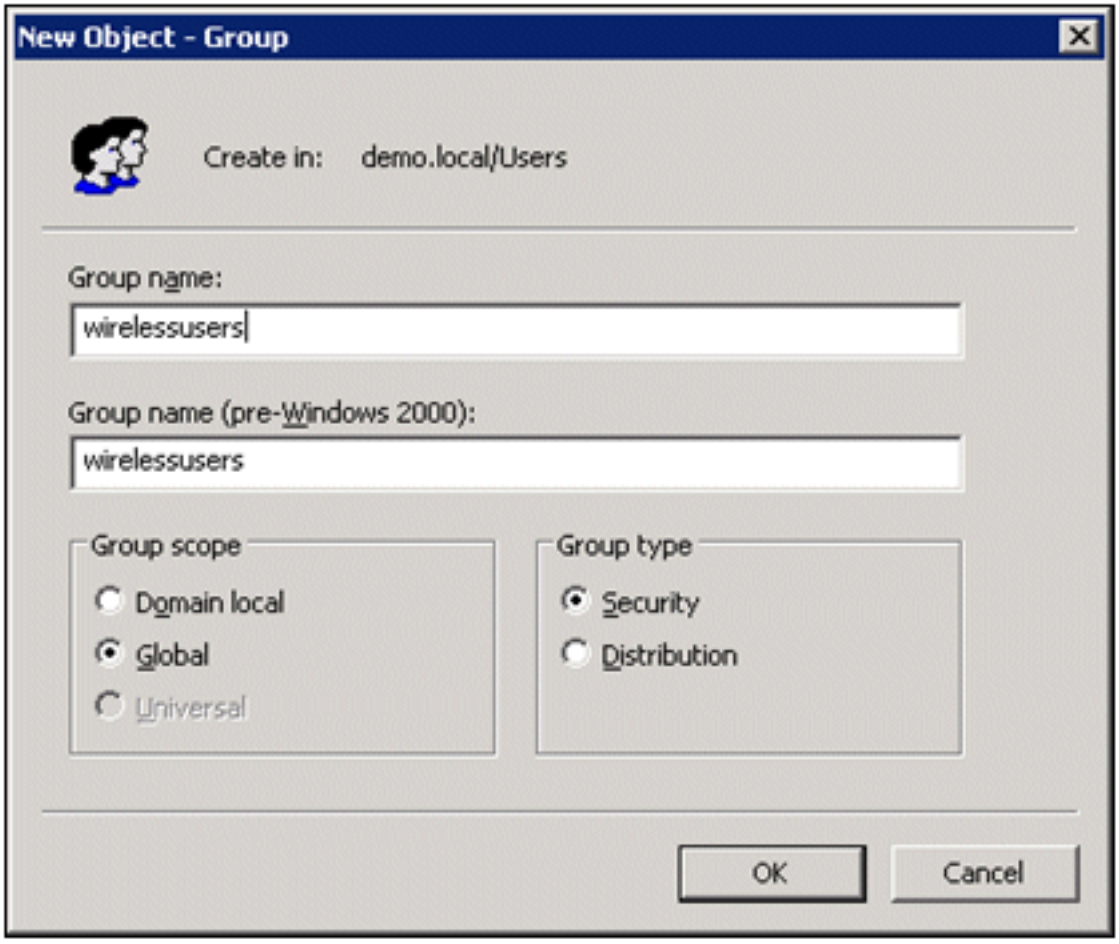
OK.



[Groepen aan het domein toevoegen]

Voer de volgende stappen uit:

1. In de Active Directory Gebruikers en Computers console boom, klik met de rechtermuisknop op **Gebruikers**, klik op **Nieuw** en klik vervolgens op **Groep**.
2. Typ in het dialoogvenster Nieuw object - groep de naam van de groep in het veld Groepsnaam en klik vervolgens op **OK**. In dit document wordt de naam van de groep *draadloze gebruikers*

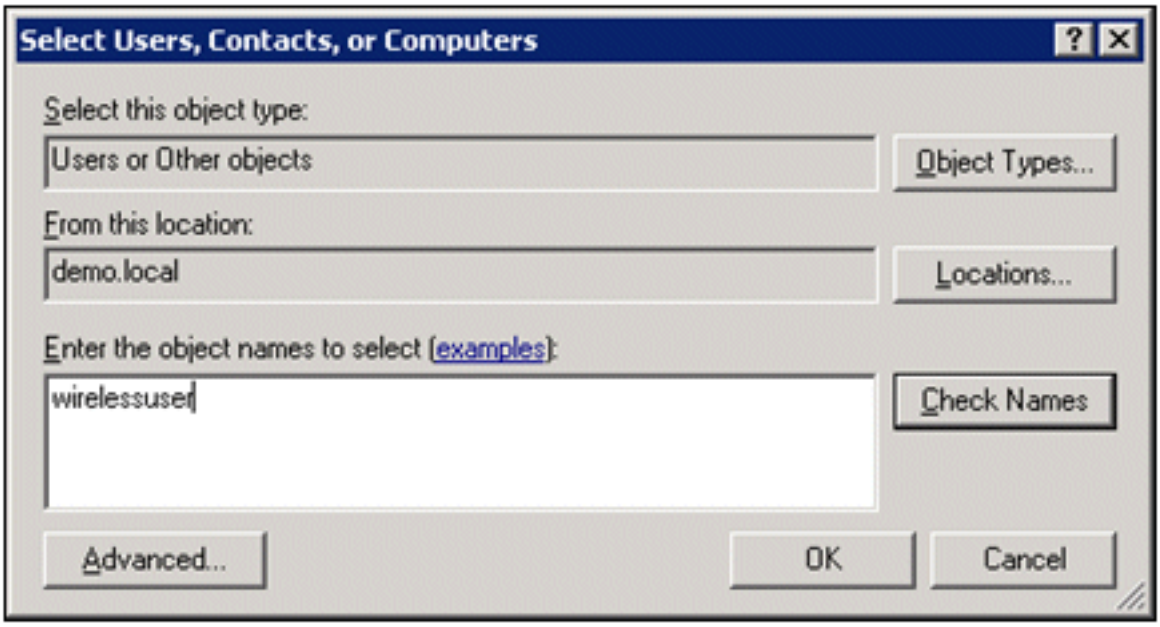


gebruikt.

[Gebruikers toevoegen aan de groep draadloze gebruikers]

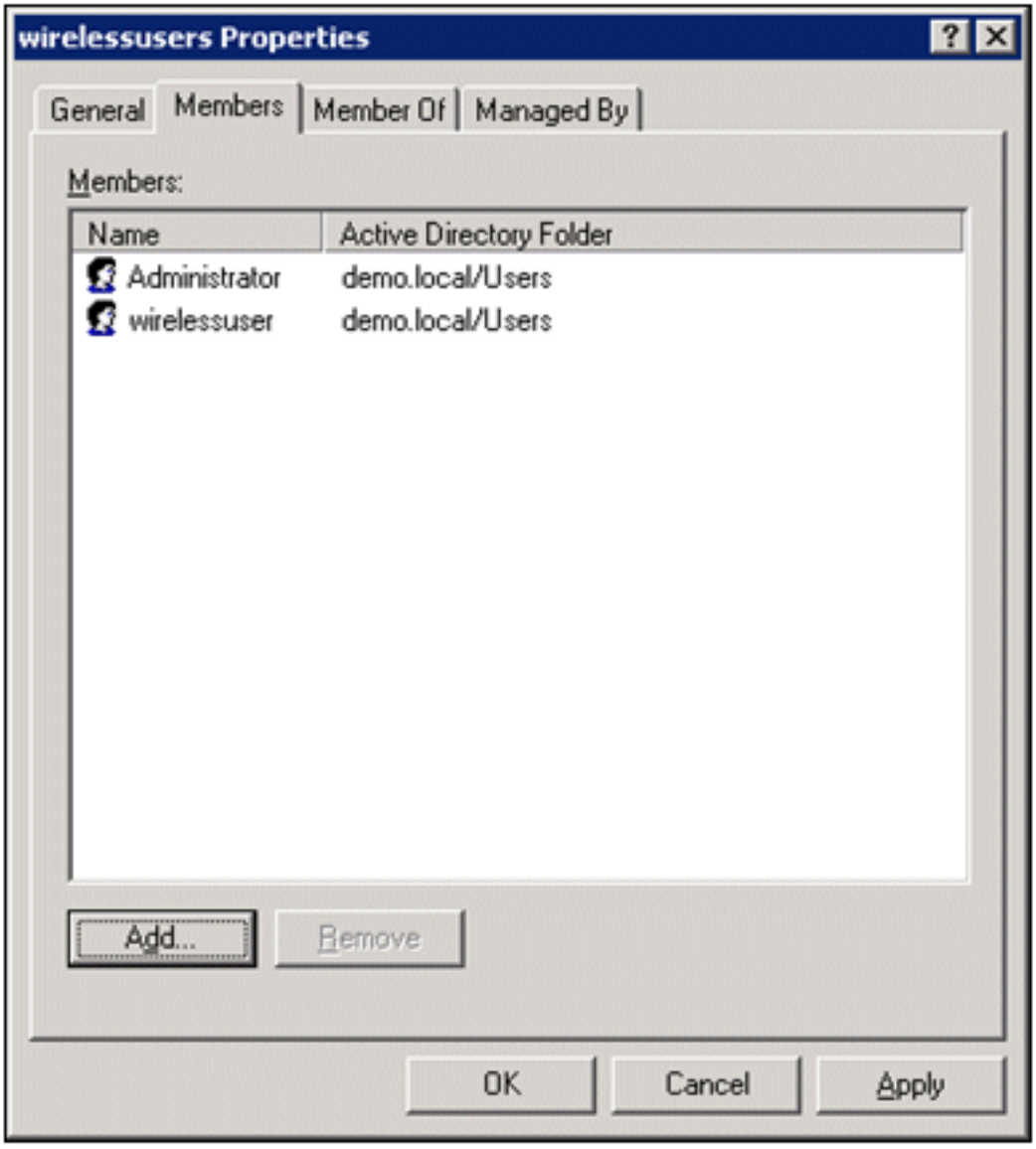
Voer de volgende stappen uit:

1. Dubbelklik in het detailvenster van Active Directory-gebruikers en -computers op de groep *draadloze gebruikers*.
2. Ga naar het tabblad Leden en klik op **Toevoegen**.
3. Typ in het dialoogvenster Gebruikers, contactpersonen, computers of groepen selecteren de naam van de gebruikers die u aan de groep wilt toevoegen. Dit voorbeeld laat zien hoe u de gebruiker *draadloze gebruiker* aan de groep kunt toevoegen. Klik op



OK.

4. Klik in het dialoogvenster Meervoudige namen op **OK**. De account voor draadloze gebruikers wordt toegevoegd aan de groep draadloze



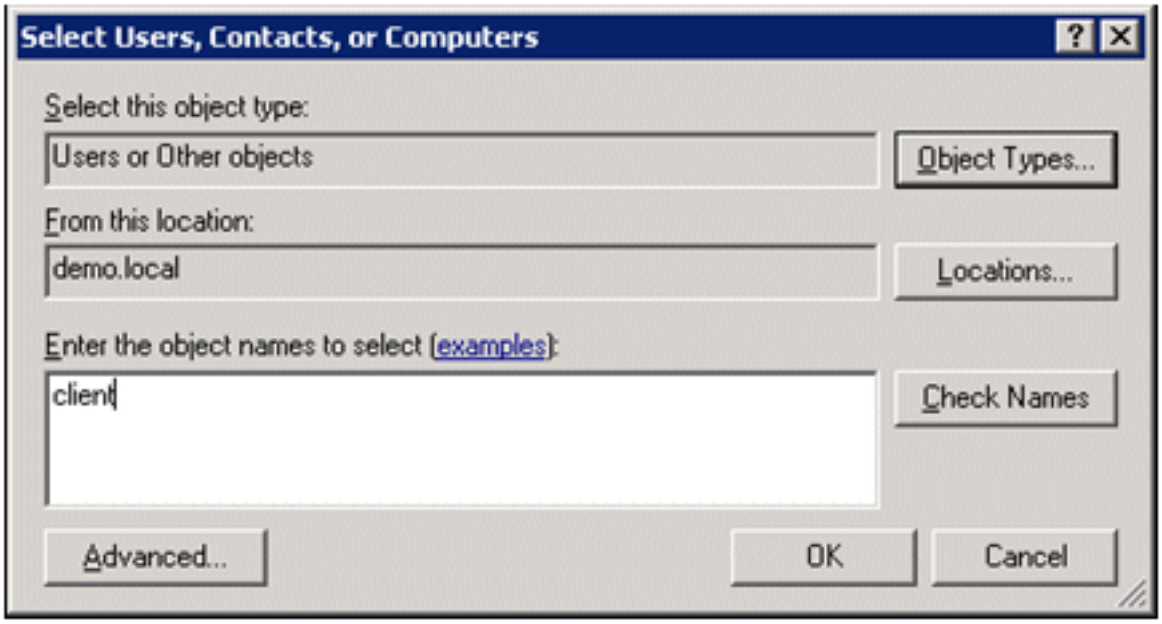
gebruikers.

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

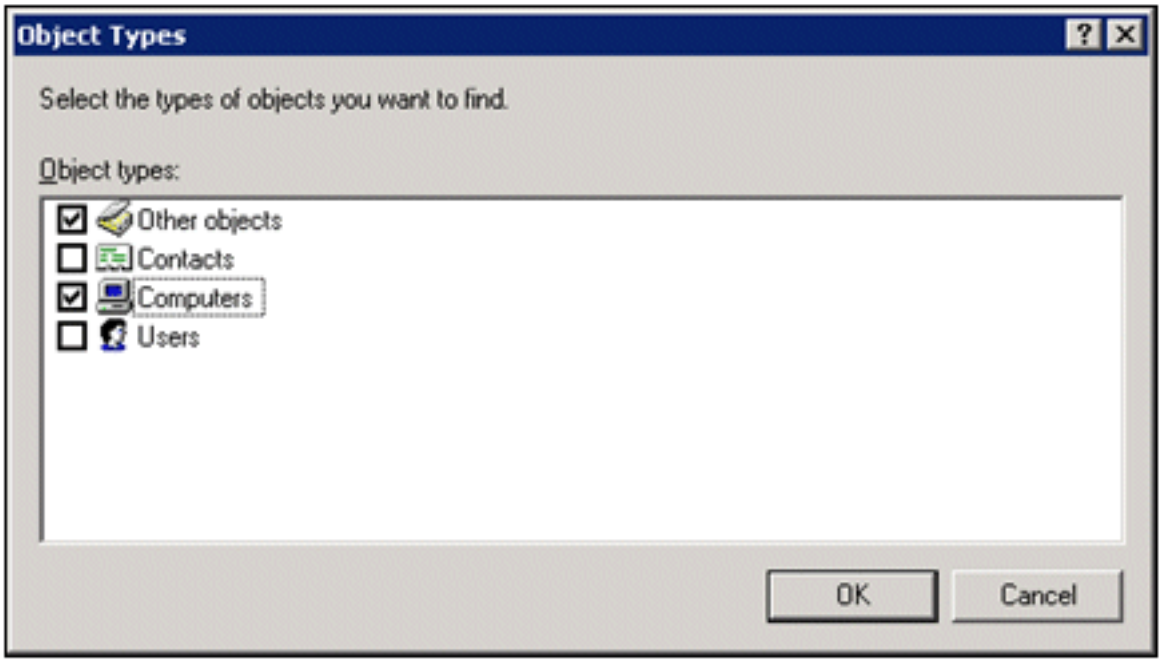
Voeg clientcomputers toe aan de groep draadloze gebruikers

Voer de volgende stappen uit:

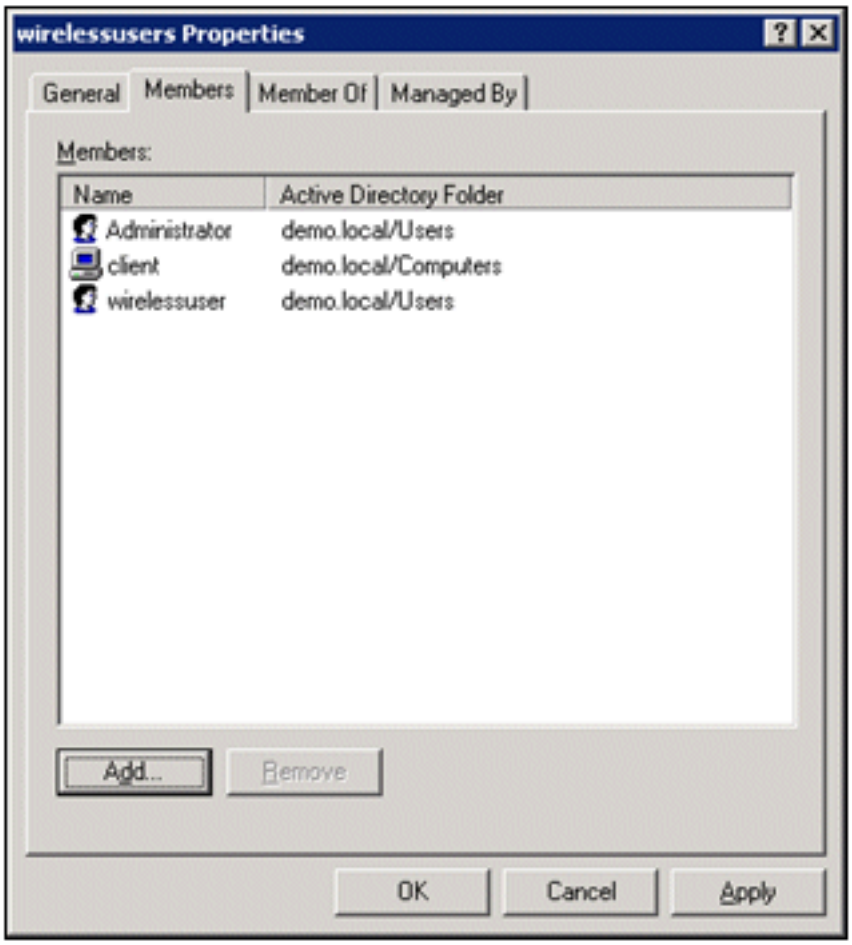
1. Herhaal stap 1 en 2 in het gedeelte Gebruikers toevoegen aan de sectie Draadloze gebruikersgroep van dit document.
2. Typ in het dialoogvenster Gebruikers, contactpersonen of computers selecteren de naam van de computer die u aan de groep wilt toevoegen. Dit voorbeeld toont hoe de computer met de naam *client* aan de groep kan worden toegevoegd.



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



4. Klik tweemaal op **OK**. De CLIENT-computeraccount wordt toegevoegd aan de groep



draadloze gebruikers.

5. Herhaal de procedure om meer computers aan de groep toe te voegen.

Cisco 1121 beveiligde ACS-module 5.1

Installatie met de CSACS-1121 Series applicatie

Het CSACS-1121 apparaat is voorgeïnstalleerd met de ACS 5.1 software. Dit hoofdstuk geeft u een overzicht van het installatieproces en de taken die u moet uitvoeren voordat u ACS installeert.

1. Sluit de CSACS-1121 aan op de netwerk- en apparaatconsole. Zie Hoofdstuk 4, "Kabels aansluiten."
2. Schakel het CSACS-1121 apparaat in. Zie Hoofdstuk 4 "De applicatie voor CSACS-1121 Series inschakelen".
3. Voer de **setup-**opdracht uit bij de CLI-prompt om de eerste instellingen voor de ACS-server te configureren. Zie Het installatieprogramma uitvoeren.

De ACS-server installeren

In dit gedeelte wordt het installatieproces voor de ACS-server op het CSACS-1121 Series-apparaat beschreven.

- Start het installatieprogramma
- Controleer het installatieproces
- Taken na de installatie

Raadpleeg voor gedetailleerde informatie over de installatie van de Cisco Secure ACS-server de

installatie- en upgrade-handleiding voor Cisco Secure Access Control System 5.1.

Cisco WLC508-controllerconfiguratie

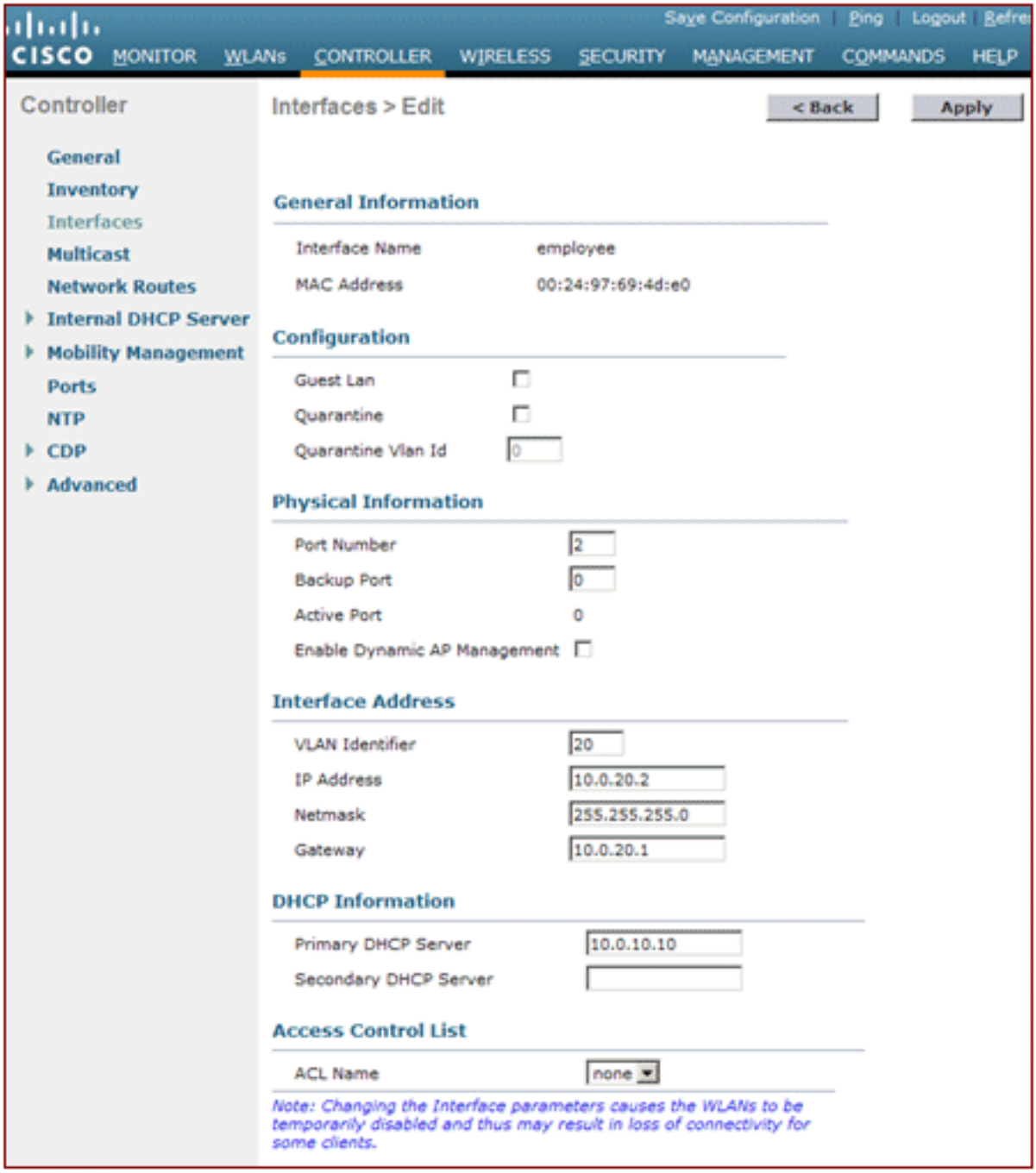
De benodigde configuratie voor WPAv2/WPA maken

Voer de volgende stappen uit:

Opmerking: De veronderstelling is dat de controller basisconnectiviteit met het netwerk heeft en dat IP bereikbaarheid naar de beheerinterface succesvol is.

1. Blader naar **https://10.0.1.10** om in te loggen op de controller.

2. Klik op **Aanmelden**.
3. Log in met de standaard gebruiker *beheerder* en standaard wachtwoord *beheerder*.
4. Maak een nieuwe interface voor VLAN-mapping onder het menu **Controller**.
5. Klik op **Interfaces**.
6. Klik op **New** (Nieuw).
7. Voer in het veld Interfacenaam *Werknemer in*. (Dit veld kan elke gewenste waarde hebben.)
8. Voer in het veld VLAN-id *20 in*. (Dit veld kan elk VLAN zijn dat in het netwerk wordt gedragen.)
9. Klik op **Apply** (Toepassen).
10. Configureer de informatie zoals dit venster Interfaces > Bewerken toont:IP-interfaceadres - **10.0.20.2**Netmasker - **255.255.255.0**Gateway - **10.0.10.1**Primaire DHCP - **10.0.10.10**

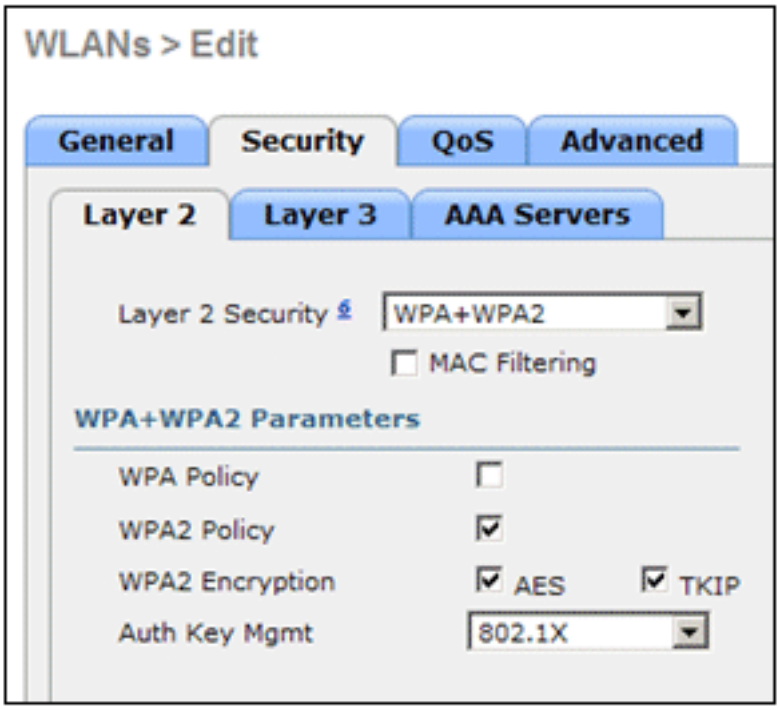


11. Klik op **Apply** (Toepassen).
12. Klik op het tabblad **WLAN's**.
13. Kies **Nieuw maken** en klik op **Ga**.
14. Voer een profielnaam in en voer in het veld WLAN SSID *Werknemer* in.

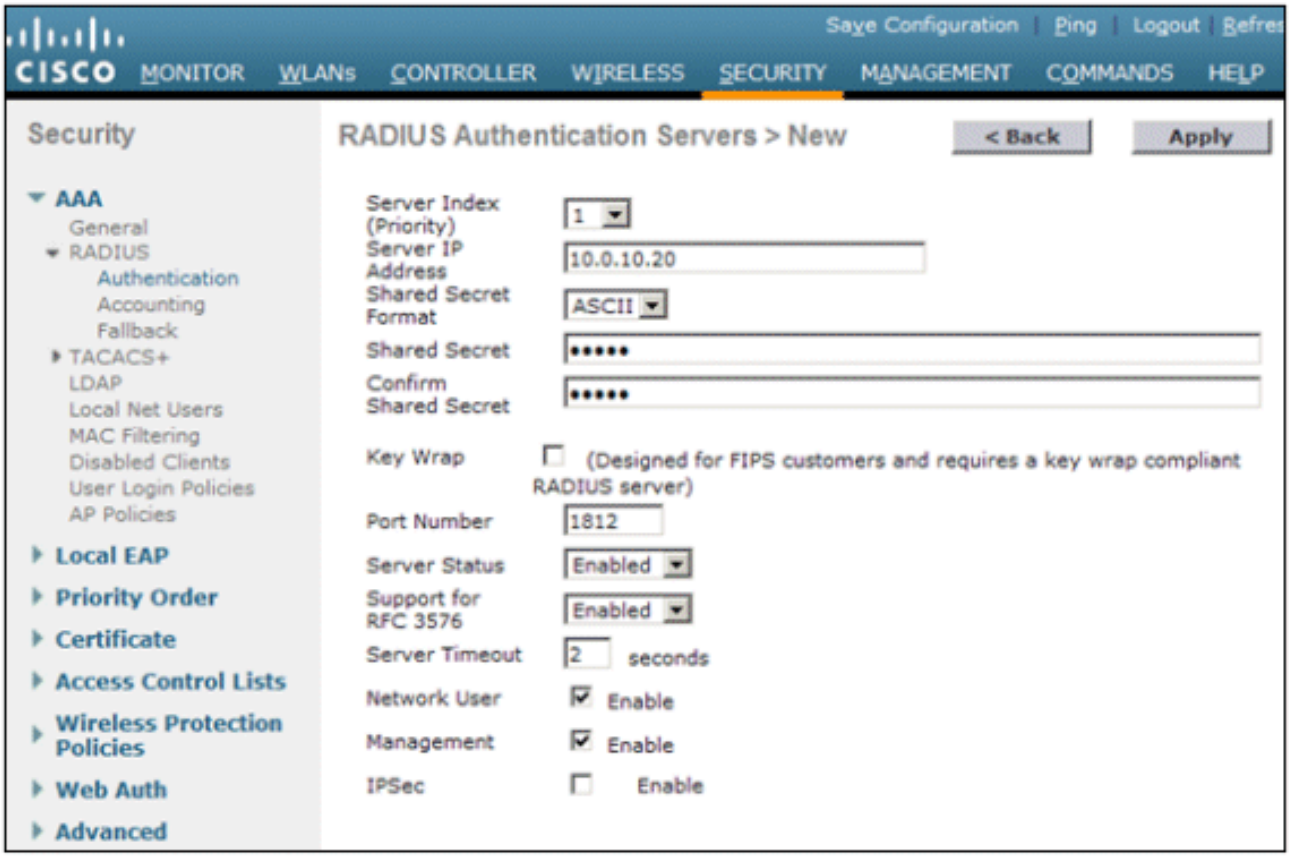
15. Kies een ID voor het WLAN en klik op **Toepassen**.

16. Configureer de informatie voor dit WLAN wanneer het venster WLAN's > Bewerken wordt weergegeven.**Opmerking:** WPAv2 is de gekozen Layer 2-coderingsmethode voor dit lab. Om WPA met TKIP-MIC-clients te kunnen koppelen aan deze SSID, kunt u ook de **WPA-compatibiliteitsmodus** controleren en **WPA2 TKIP Clients-**vakken **toestaan** of clients die de 802.11i AES-coderingsmethode niet ondersteunen.
17. Klik in het scherm WLAN's > Bewerken op het tabblad **Algemeen**.
18. Zorg dat het vakje Status is ingeschakeld en dat de juiste **interface** (medewerker) is geselecteerd. Controleer ook of het aanvinkvakje **Enabled (Ingeschakeld) is ingeschakeld** voor Broadcast
SSID.

19. Klik op het tabblad **Beveiliging**.
20. Selecteer onder het submenu Layer 2 **WPA + WPA2** voor Layer 2 Security. Controleer voor WPA2-encryptie **AES + TKIP** om TKIP-clients toe te staan.



21. Kies **802.1x** als verificatiemethode.
22. Sla Layer 3-submenu over omdat dit niet nodig is. Zodra de RADIUS-server is geconfigureerd, kan de juiste server worden gekozen in het Verificatiemenu.
23. De tabbladen **QoS** en **Advanced** kunnen standaard blijven staan, tenzij er speciale configuraties nodig zijn.
24. Klik op het menu **Beveiliging** om de RADIUS-server toe te voegen.
25. Klik onder het submenu RADIUS op **Verificatie**. Klik vervolgens op **Nieuw**.
26. Voeg het IP-adres van de RADIUS-server (10.0.10.20) toe; dit is de ACS-server die eerder is geconfigureerd.
27. Zorg dat de gedeelde sleutel overeenkomt met de AAA-client die in de ACS-server is geconfigureerd. Zorg dat het vakje **Netwerkgebruiker** is ingeschakeld en klik op **Toepassen**.



28. De basisconfiguratie is nu voltooid en u kunt beginnen met het testen van PEAP.

PEAP-verificatie

Voor PEAP met MS-CHAP versie 2 zijn certificaten vereist op de ACS-servers, maar niet op de draadloze clients. Automatische inschrijving van computercertificaten voor de ACS-servers kan worden gebruikt om een implementatie te vereenvoudigen.

Voltooi de procedures in deze sectie om CA-server zo te configureren dat automatische inschrijving mogelijk is voor computer- en gebruikerscertificaten.

Opmerking: Microsoft heeft de Web Server-sjabloon gewijzigd met de release van de Windows 2003 Enterprise CA, zodat sleutels niet langer exporteerbaar zijn en de optie grijs is. Er zijn geen andere certificaatsjablonen die worden geleverd met certificaatservices die bedoeld zijn voor serververificatie en die de mogelijkheid bieden om sleutels als exporteerbaar te markeren die beschikbaar zijn in de vervolgkeuzelijst, zodat u een nieuwe sjabloon moet maken die dit doet.

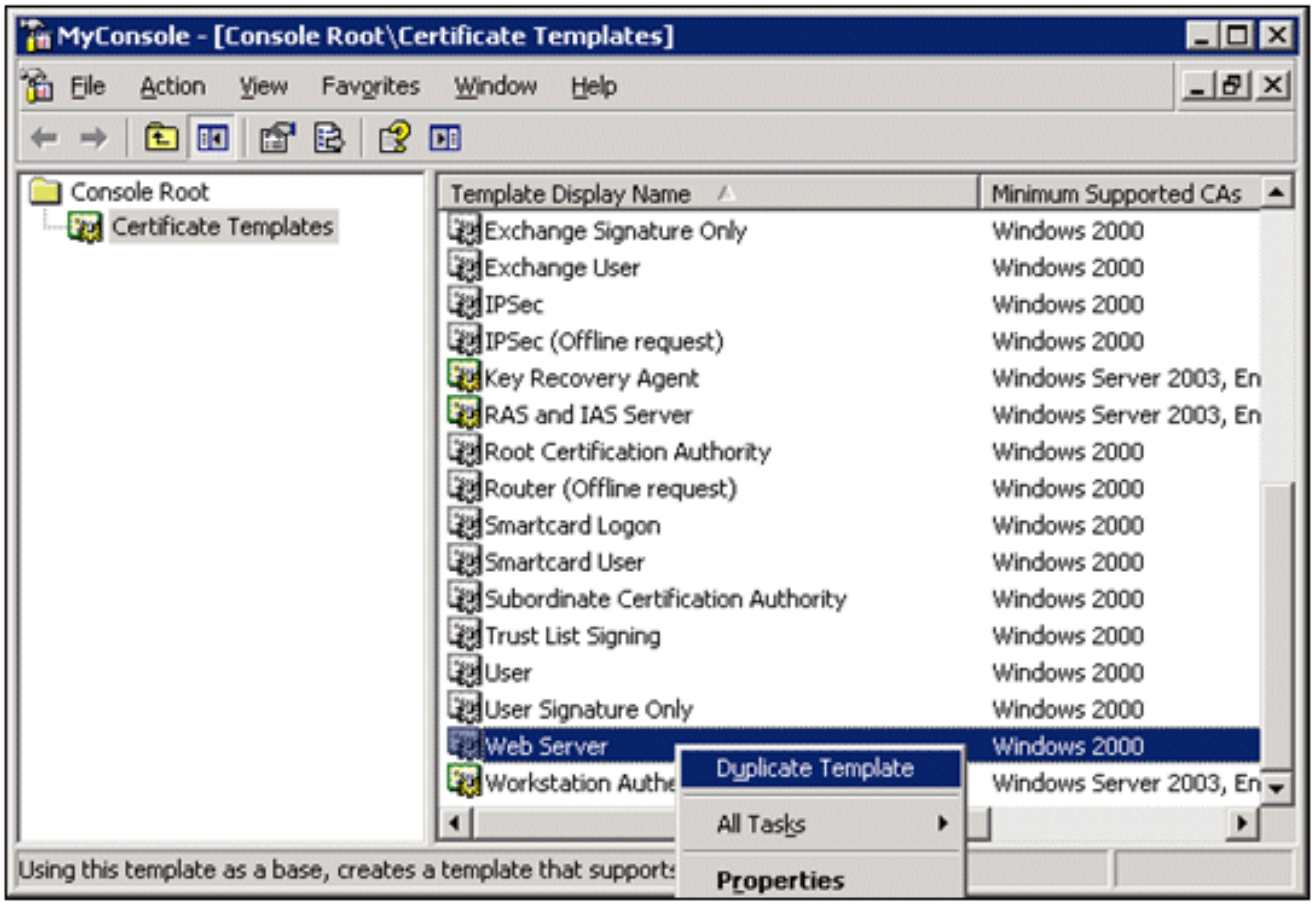
Opmerking: Windows 2000 biedt exporteerbare sleutels en deze procedures hoeven niet te worden gevolgd als u Windows 2000 gebruikt.

Installeer de tijdelijke sjablonen voor het certificaat.

Voer de volgende stappen uit:

1. Kies **Start** > **Uitvoeren**, voer *mmc in* en klik op **OK**.
2. Klik in het menu Bestand op **Magnetisch toevoegen/verwijderen** en klik vervolgens op **Toevoegen**.
3. Dubbelklik onder Snap-in op **Certificaatsjablonen**, klik op **Sluiten** en klik vervolgens op **OK**.

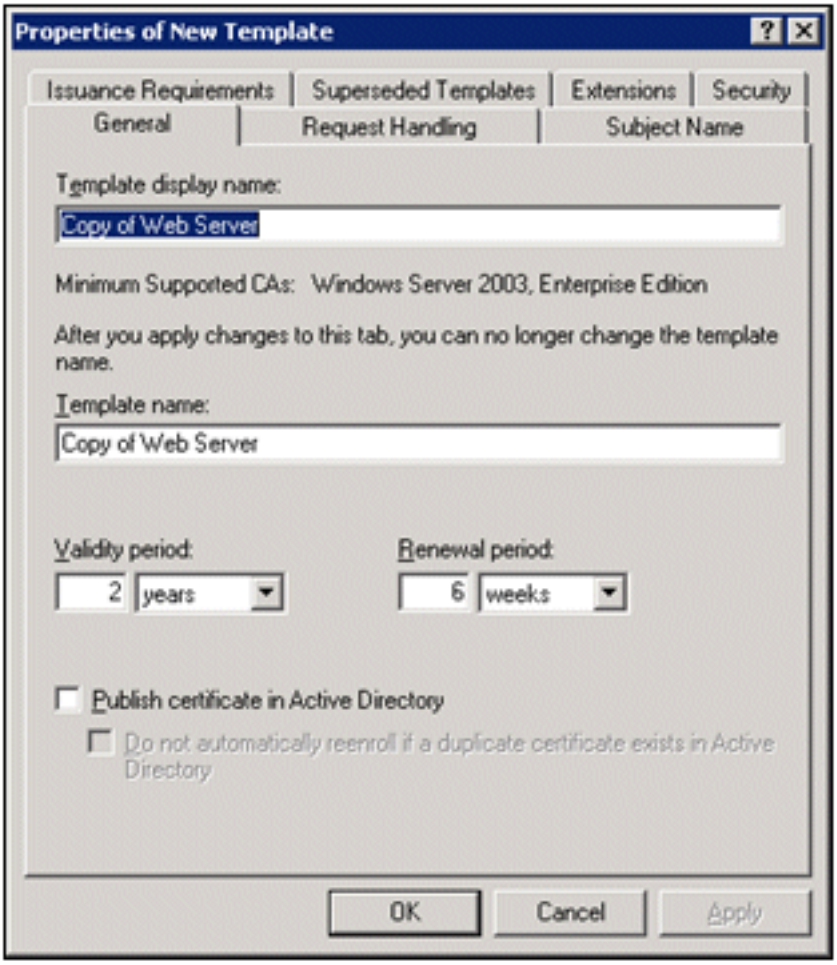
4. Klik in de consolestructuur op **Certificaatsjablonen**. Alle certificaatsjablonen worden weergegeven in het Detailvenster.
5. Om stap 2 tot en met 4 te omzeilen, voert u *certmpl.msc in*, dat de sjablonen van het certificaat onverwacht
   opent.



De certificaatsjabloon voor de ACS-webserver maken

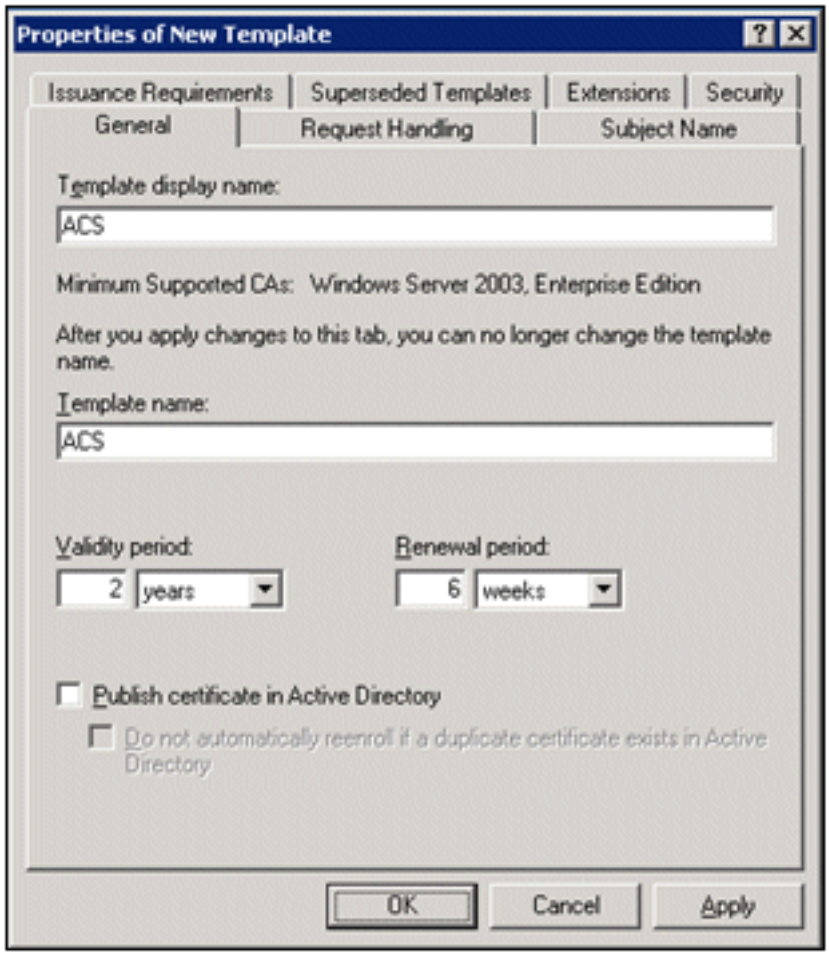
Voer de volgende stappen uit:

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



dupliceren.

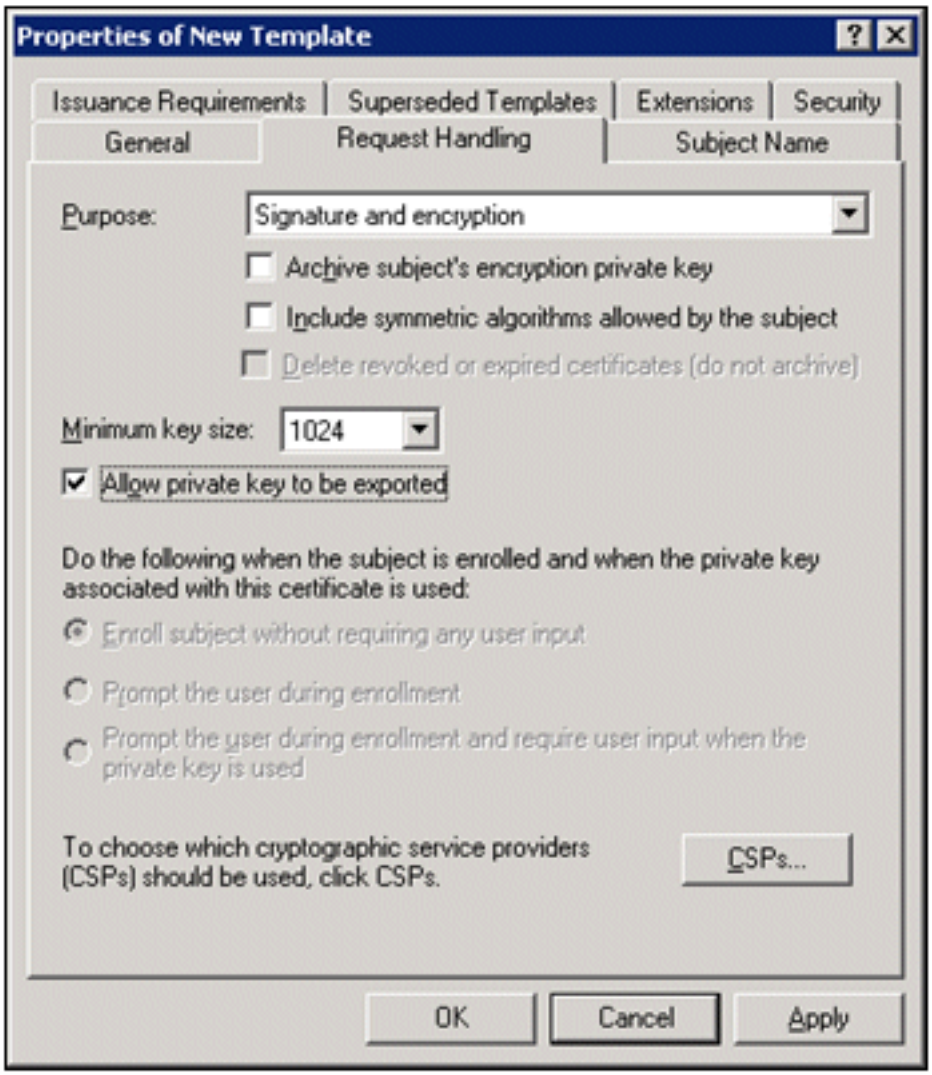
3. Typ *ACS* in het veld Weergavenaam



sjabloon.

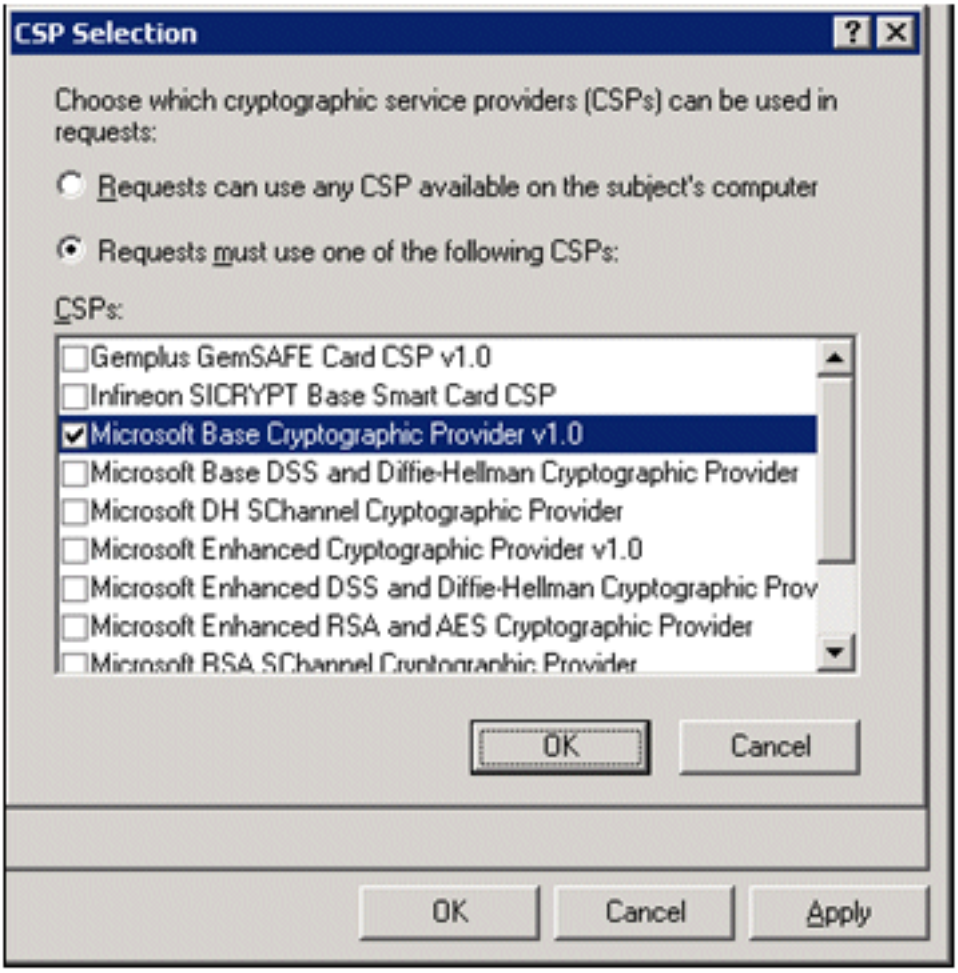
4. Ga naar het tabblad **Aanvraag behandelen** en controleer **private sleutel toestaan om**

geëxporteerd te worden. Zorg er ook voor dat **Handtekening en versleuteling** is geselecteerd in het vervolgkeuzemenu



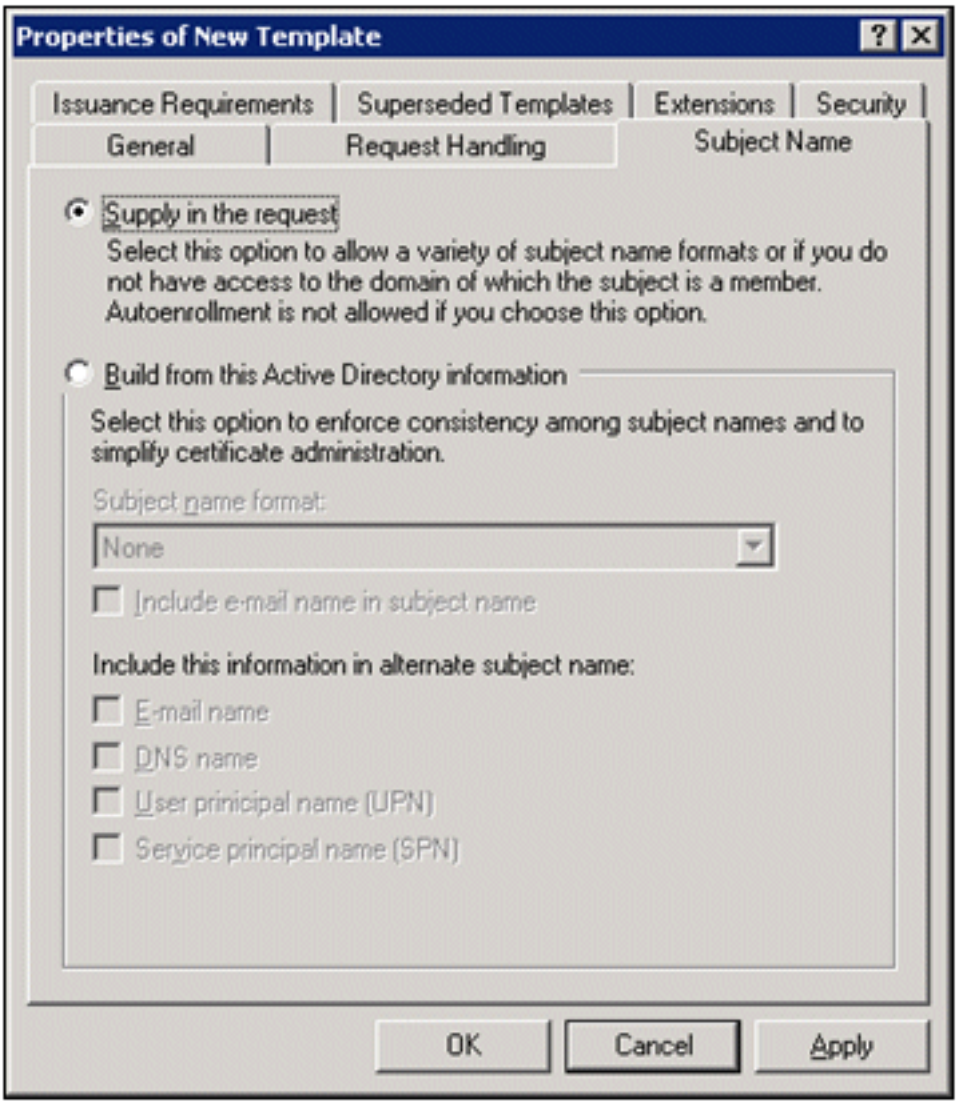
Doel.

5. Kies **Verzoeken moet een van de volgende CSP's gebruiken** en controleer **Microsoft Base Cryptographic Provider v1.0**. Schakel een andere CDV uit die zijn geselecteerd en klik op



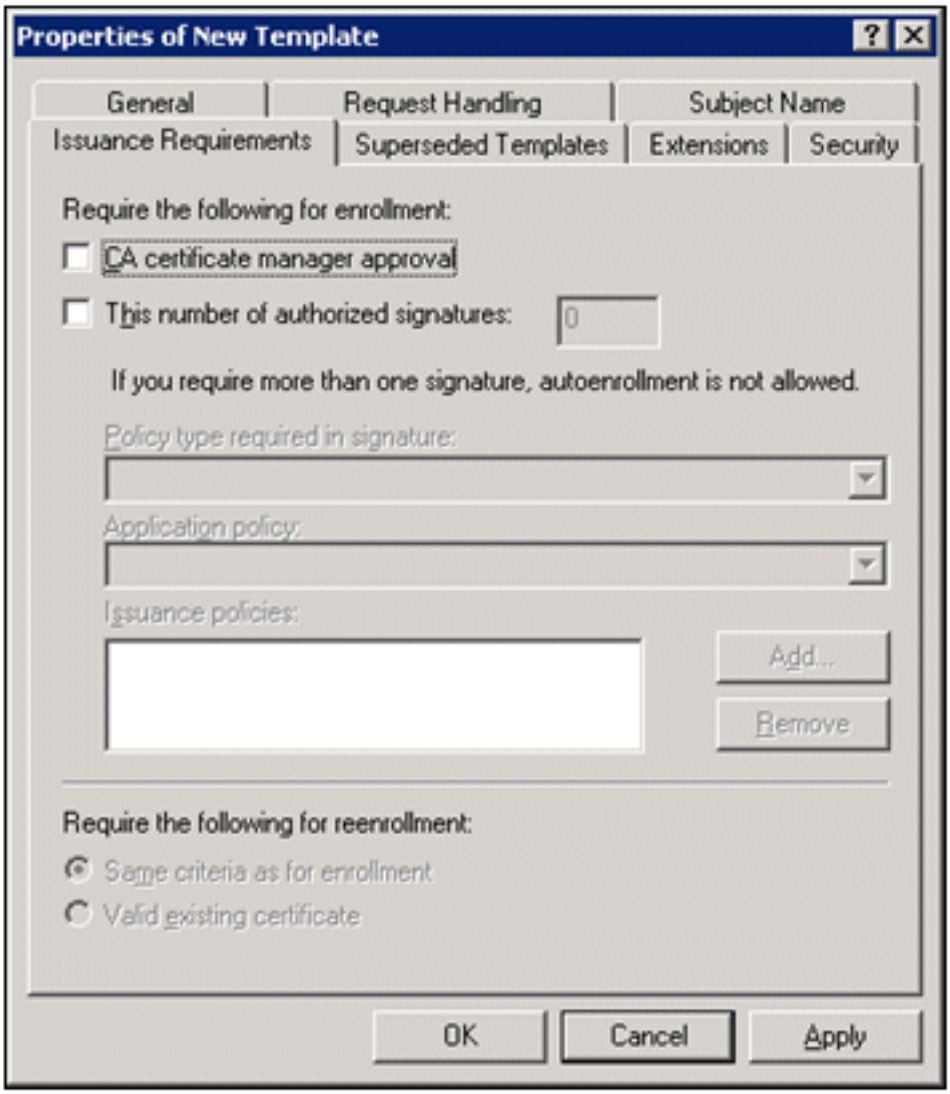
OK.

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



OK.

7. Ga naar het tabblad **Beveiliging**, markeer de **groep Domain Admins** en controleer of de optie **Enroll** is ingeschakeld.**Opmerking:** Als u ervoor kiest om uit deze Active Directory-informatie te bouwen, controleer dan alleen de **hoofdnaam van de gebruiker (UPN)** en verwijder de **naam** in onderwerpnaam en e-mailnaam omdat er geen e-mailnaam is ingevoerd voor de account van de draadloze gebruiker in de invoegtoepassing Gebruikers en computers van de Active Directory. Als u deze twee opties niet uitschakelt, probeert automatische inschrijving om e-mail te gebruiken, wat resulteert in een fout met automatische inschrijving.
8. Indien nodig zijn er extra veiligheidsmaatregelen om te voorkomen dat certificaten automatisch worden weggeduwd. Deze vindt u onder het tabblad Uitgiftevereisten. Dit wordt in dit document niet verder



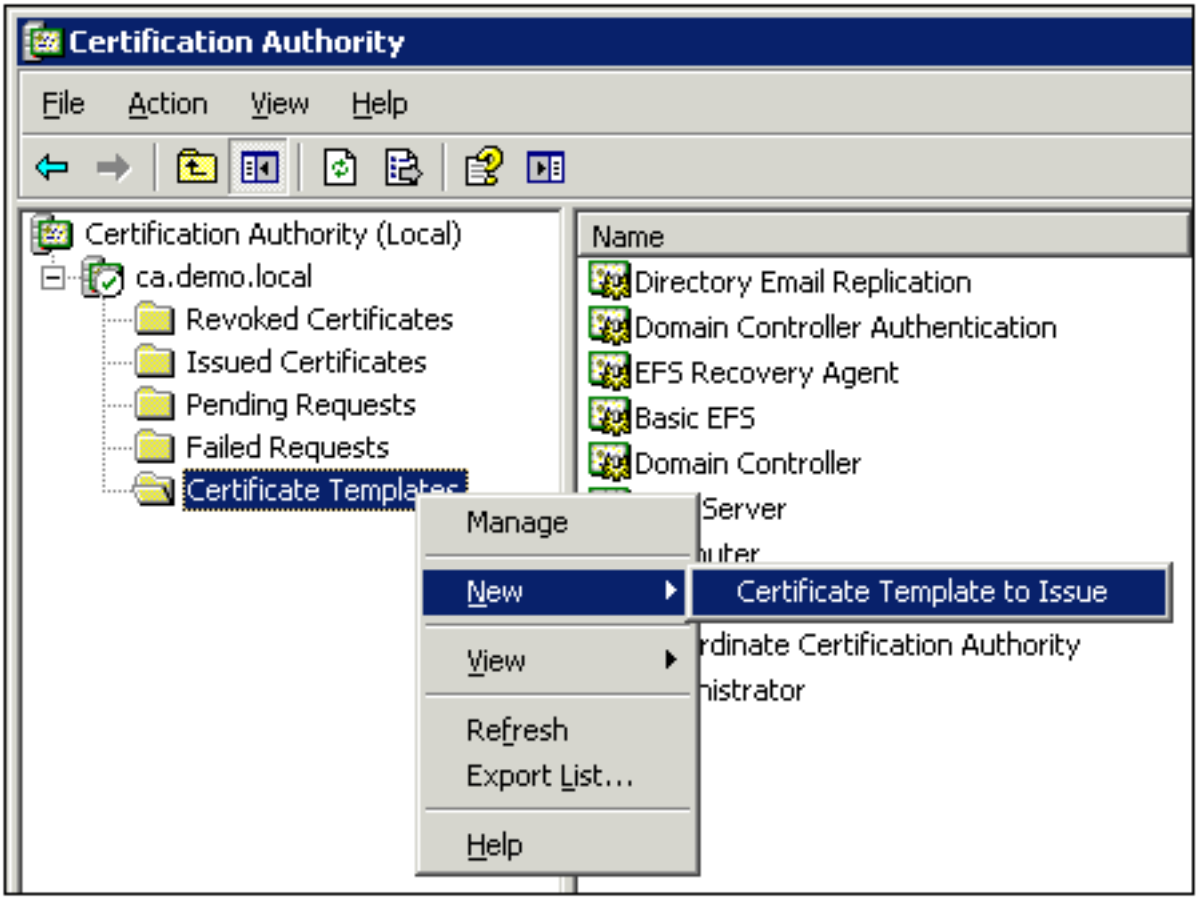
besproken.

9. Klik op **OK** om de sjabloon op te slaan en deze sjabloon vanaf de invoegtoepassing Certificaatinstantie te gebruiken.

De nieuwe ACS-webservercertificaatsjabloon inschakelen

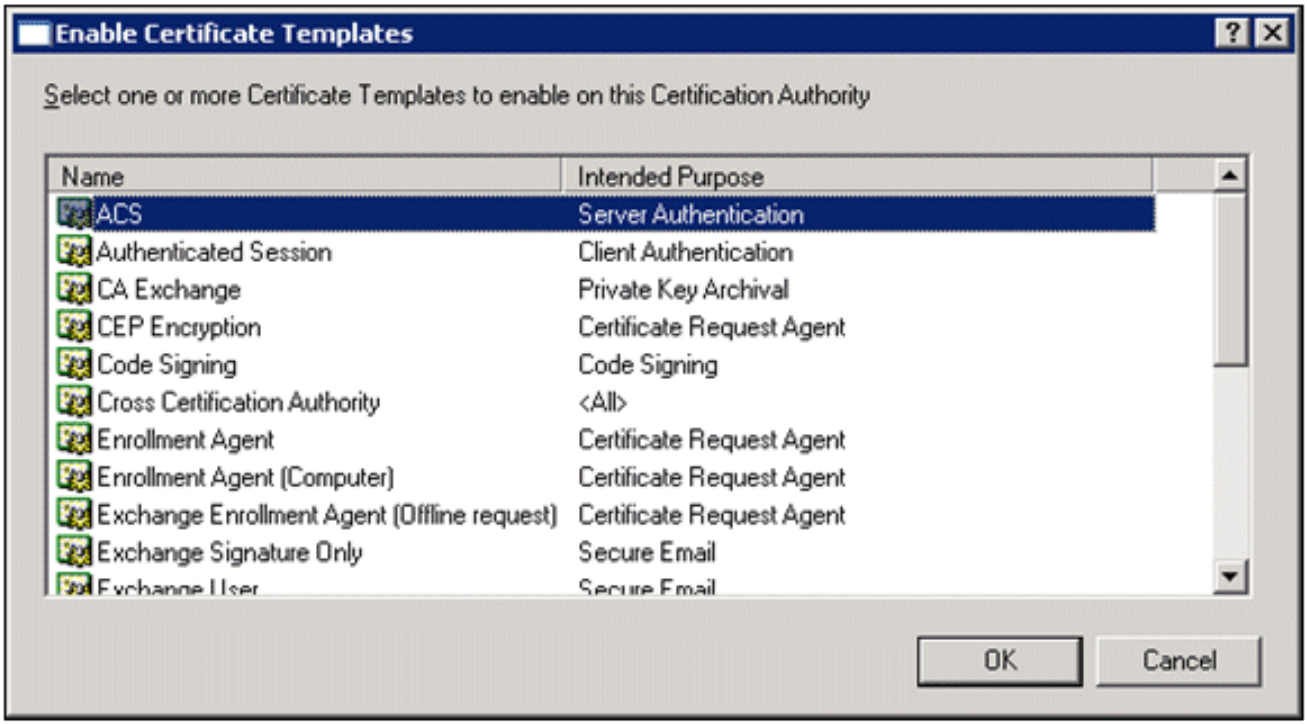
Voer de volgende stappen uit:

1. Open de module van de certificeringsinstantie. Voer stap 1 tot en met 3 uit in het gedeelte Certificaatsjabloon maken voor de ACS-webserver, kies de optie **Certificaatinstantie**, kies **Lokale computer** en klik op **Voltooien**.
2. Vouw **ca.demo.local** in de consolestructuur van de certificeringsinstantie uit en klik met de rechtermuisknop op **certificaatsjablonen**.
3. Ga naar **Nieuw > Certificaatsjabloon voor**

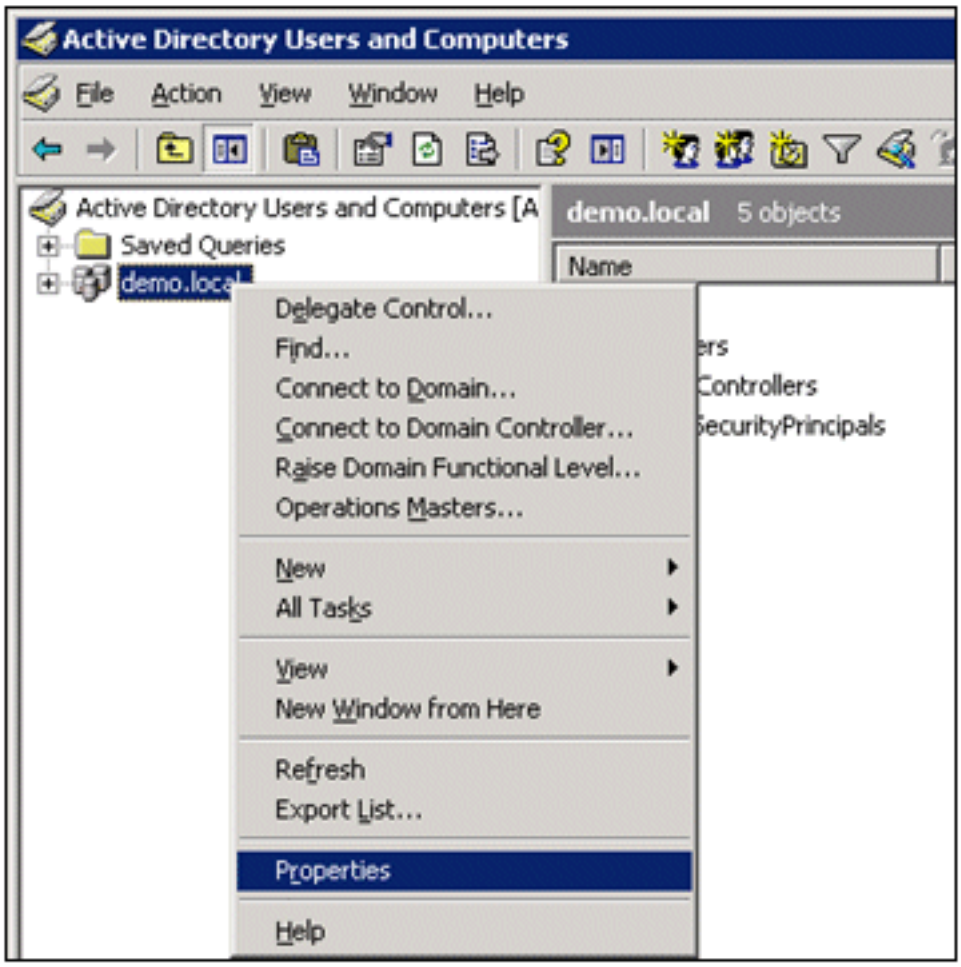


afgifte.

4. Klik op de **ACS-certificaatsjabloon**.

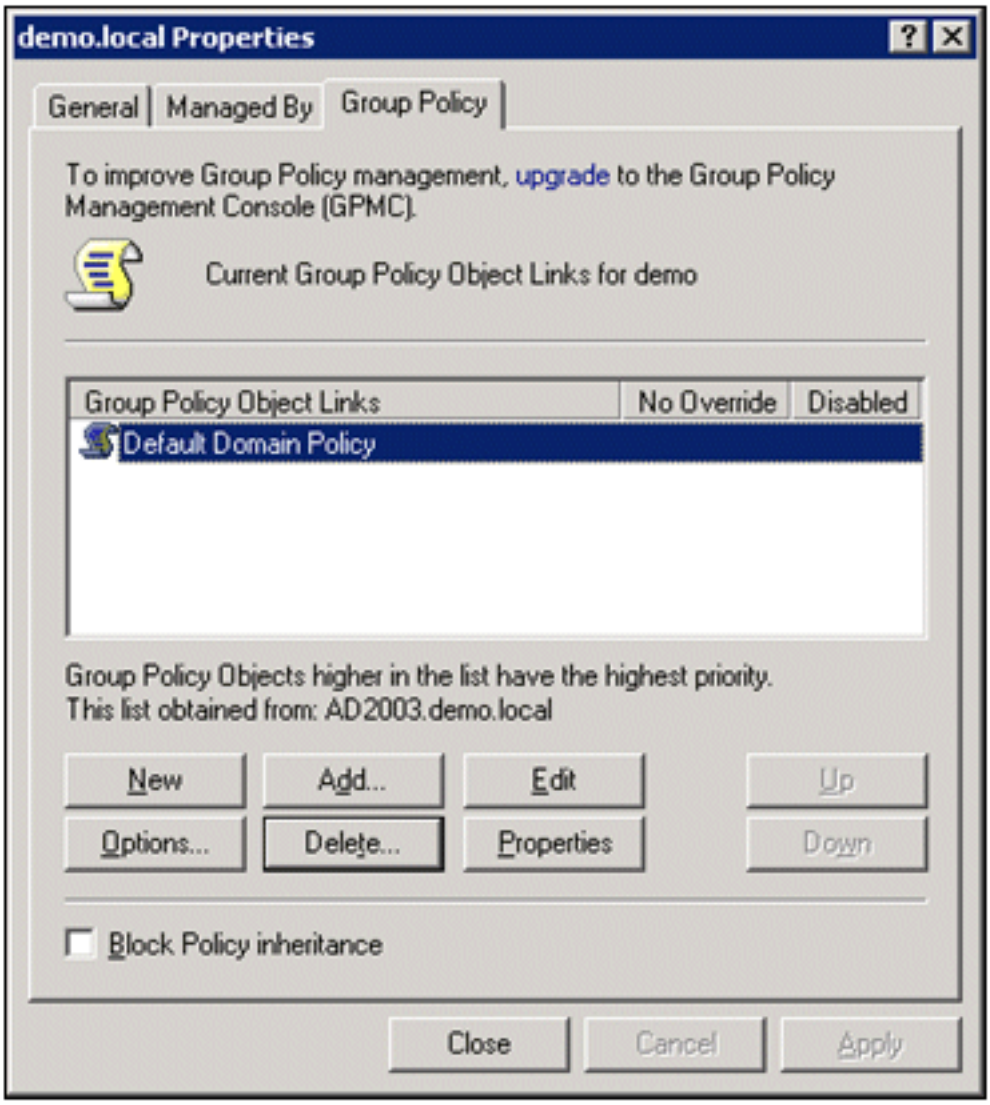


5. Klik op **OK** en open de **invoegtoepassing Active Directory Gebruikers en Computers**.
6. Dubbelklik in de consolestructuur op **Active Directory-gebruikers en -computers**, klik met de rechtermuisknop op **demo.local** en klik vervolgens op



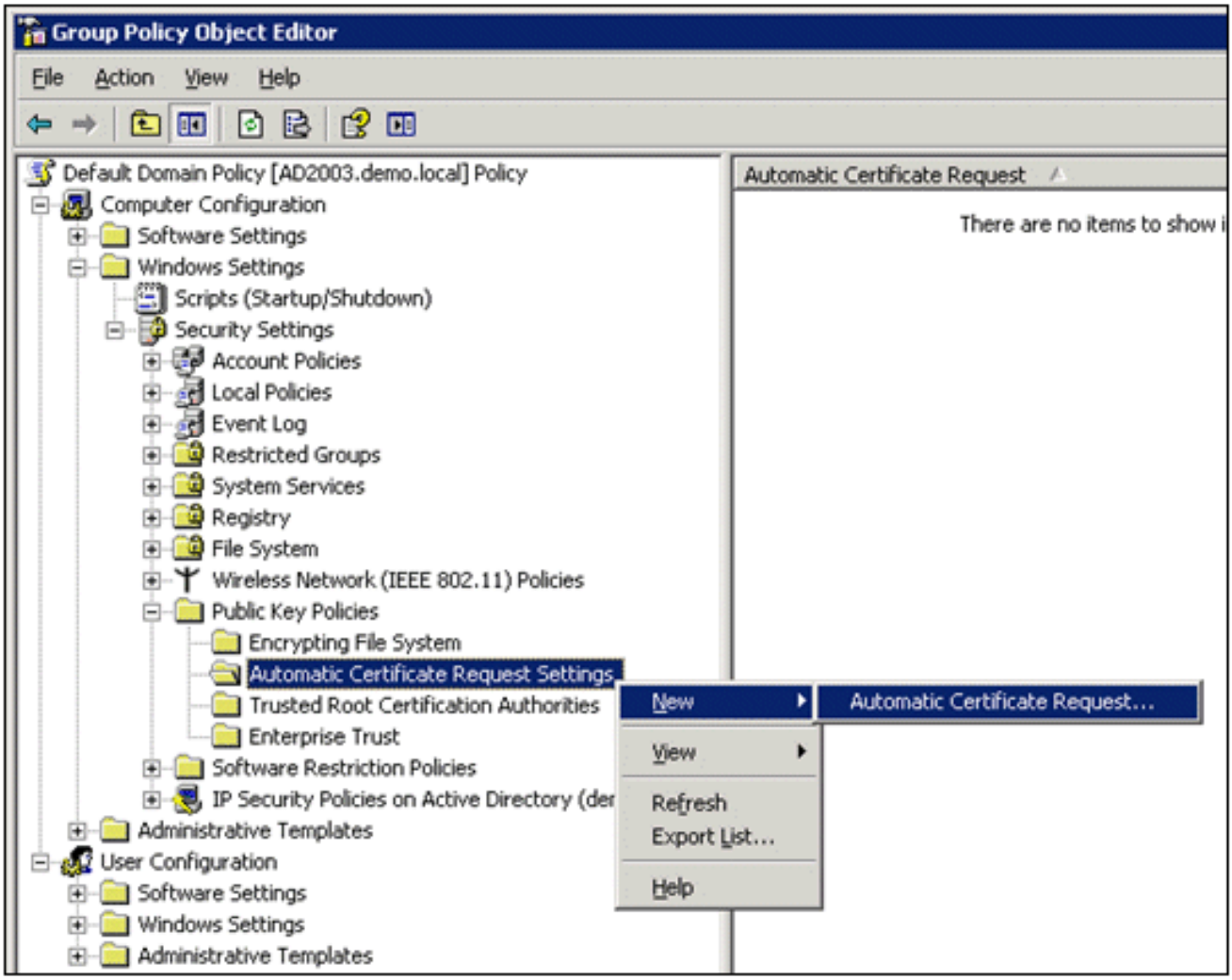
Eigenschappen.

7. Klik op het tabblad Groepsbeleid op **Standaarddomeinbeleid** en klik vervolgens op **Bewerken**. Hiermee wordt de invoegtoepassing Group Policy Object Editor



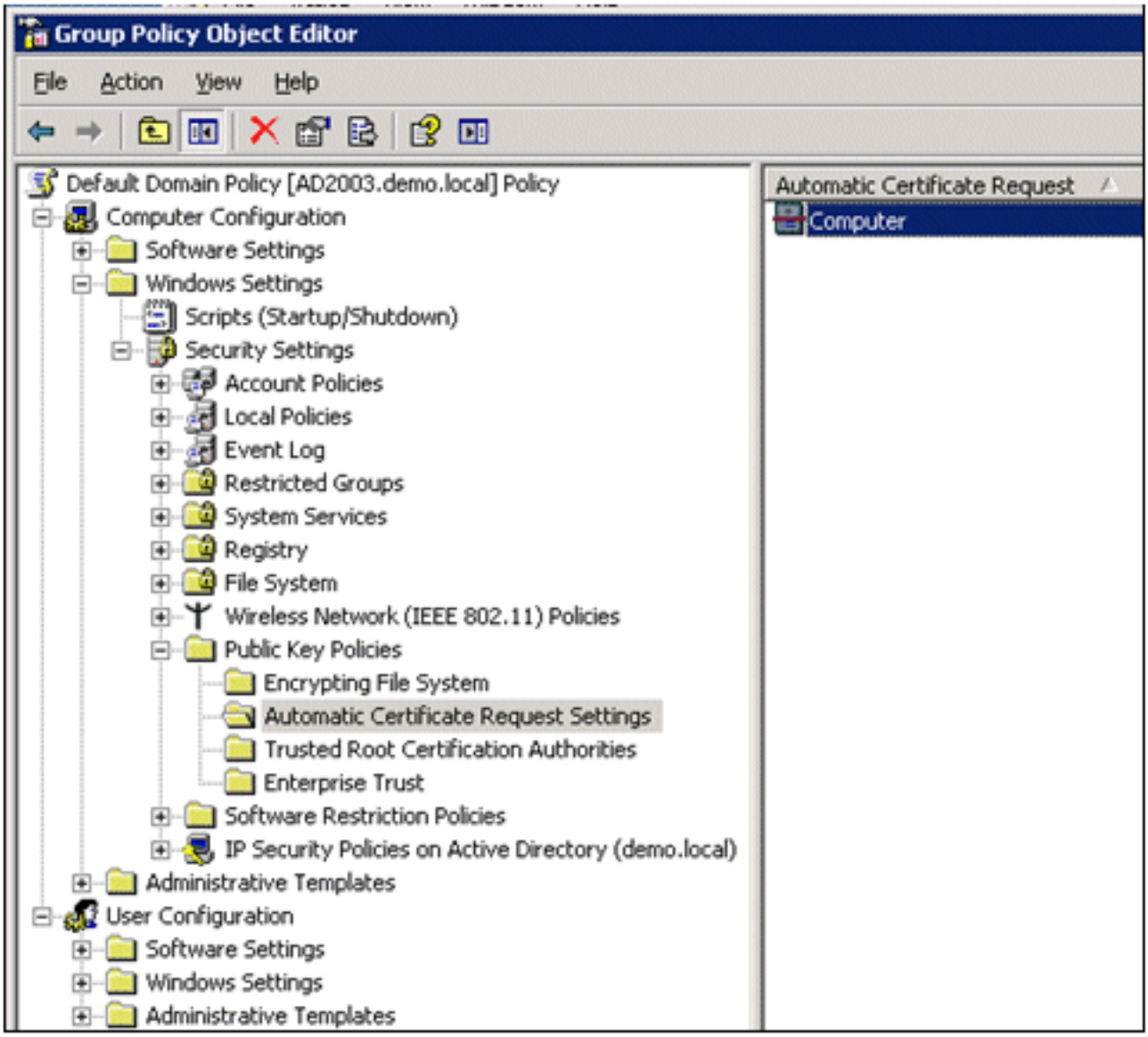
geopend.

8. In de consoleboom, breid Computer Configuration > **Windows-instellingen** > **Beveiligingsinstellingen** > **Public Key Policies uit**, en kies dan **Automatische certificaataanvraag-instellingen**.

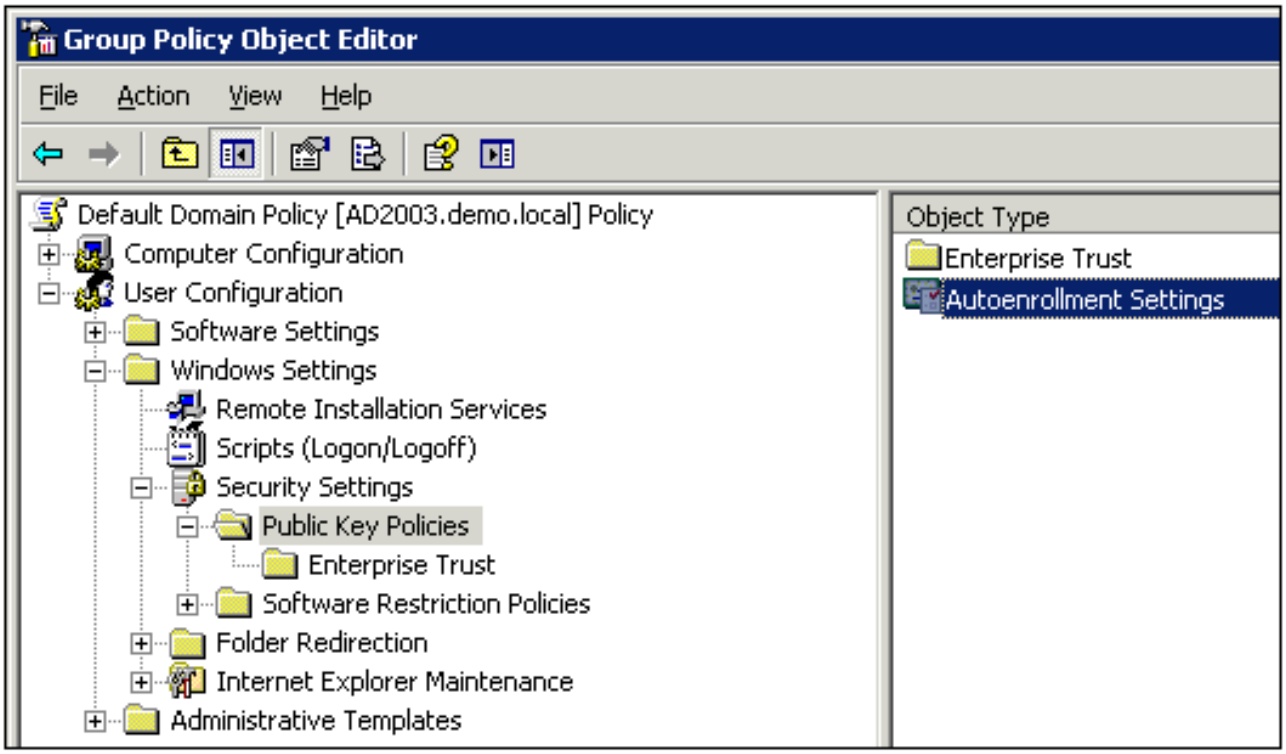


9. Klik met de rechtermuisknop op **Instellingen voor automatische certificaataanvraag** en kies **Nieuw > Automatisch certificaatverzoek**.
10. Klik op de pagina Welkom bij de wizard Automatische certificaataanvraag instellen op **Volgende**.
11. Op de pagina Certificaatsjabloon klikt u op **Computer** en vervolgens klikt u op **Volgende**.

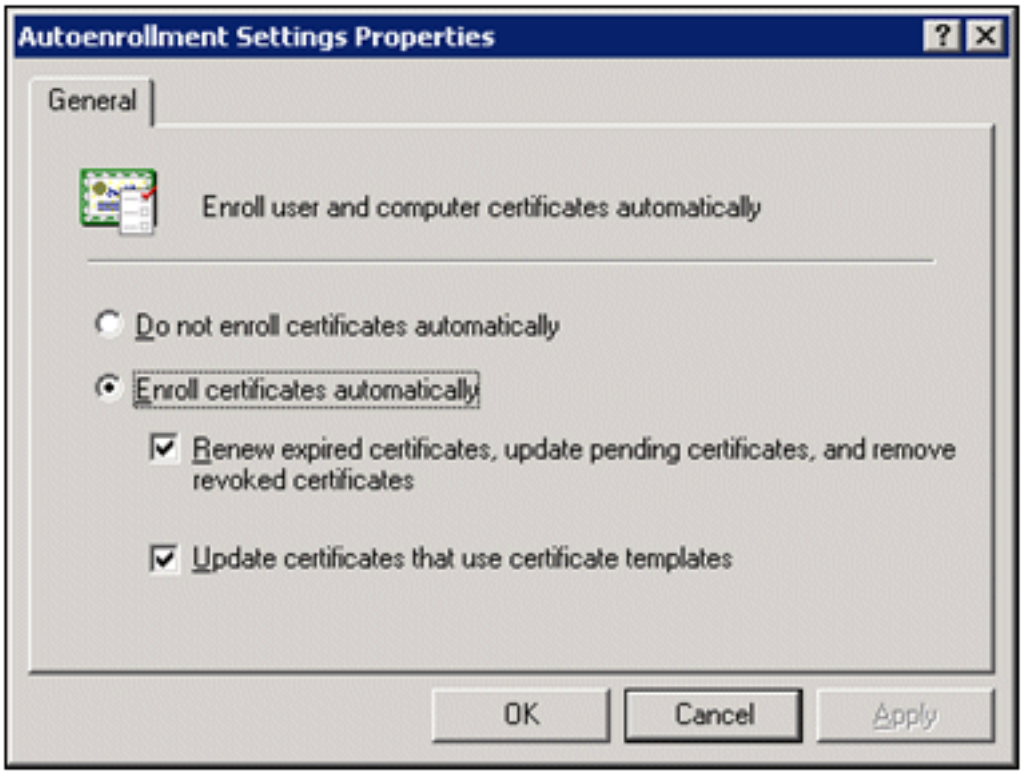
12. Klik op **Voltooien** wanneer u de pagina Wizard Automatisch certificaataanvraag instellen hebt voltooid. Het certificaattype Computer verschijnt nu in het detailvenster van de invoegtoepassing Group Policy Object
    Editor.



13. In de consoleboom, breid **Gebruikersconfiguratie > Windows-instellingen > Beveiligingsinstellingen > Public Key Policies uit**.
14. Dubbelklik in het detailvenster op **Instellingen voor automatische inschrijving**.



15. Kies **Certificaten automatisch inschrijven** en controleer **Verlengen van verlopen certificaten, update hangende certificaten en verwijder ingetrokken certificaten** en **update certificaten die certificaatsjablonen**



gebruiken.
16. Klik op **OK**.

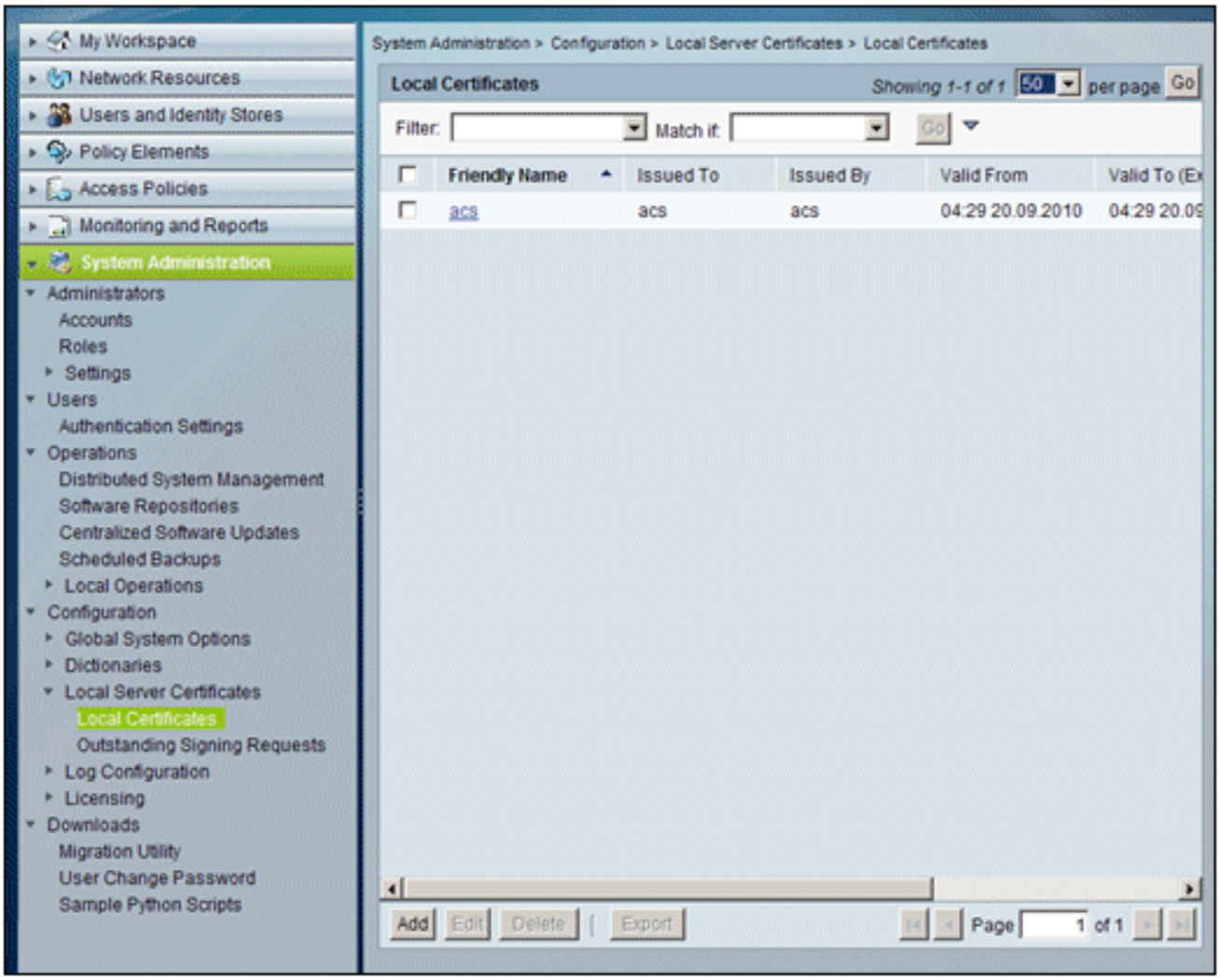
ACS 5.1 Certificaat instellen

Exporteerbaar certificaat configureren voor ACS

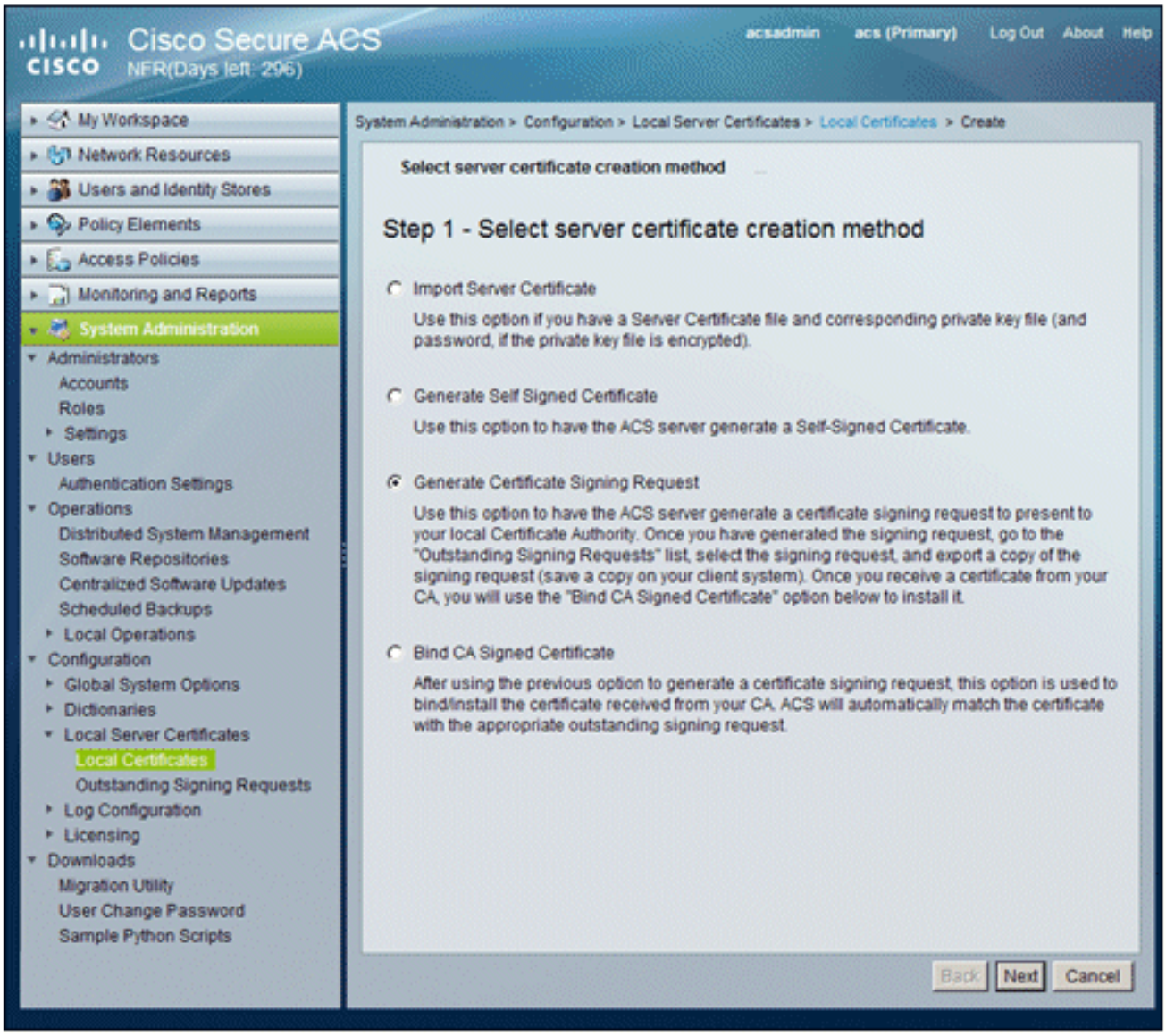
Opmerking: de ACS-server moet een servercertificaat verkrijgen van de ECA-server van de bedrijfsroot om een WLAN PEAP-client te kunnen verifiëren.

Opmerking: Zorg ervoor dat IIS Manager niet geopend is tijdens het proces voor het instellen van het certificaat, omdat dit problemen veroorzaakt met gecachede informatie.

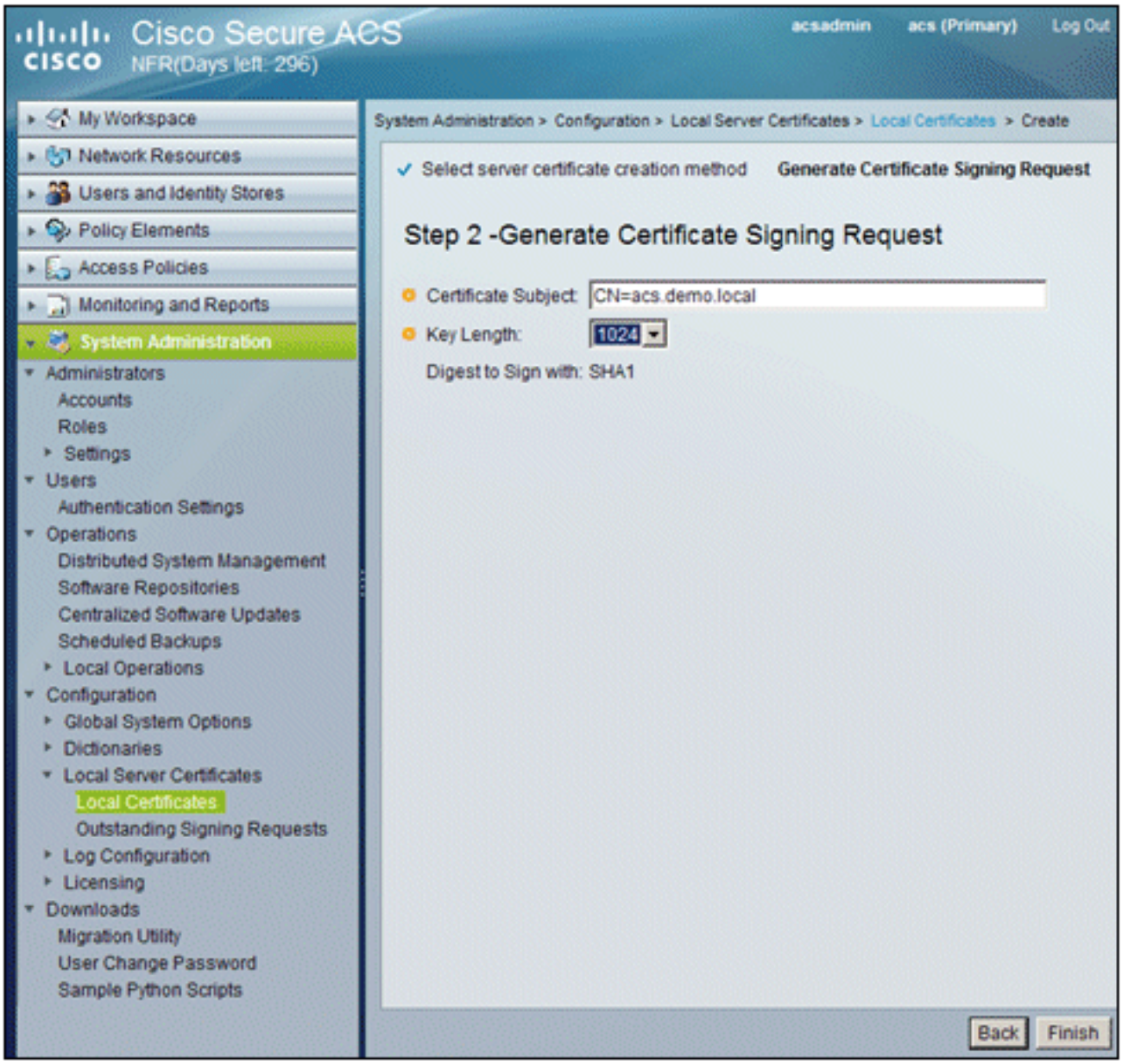
1. Meld u aan bij de ACS-server met de rechten van een accountbeheerder.
2. Ga naar **Systeembeheer > Configuratie > Lokale servercertificaten**. Klik op **Add** (Toevoegen).



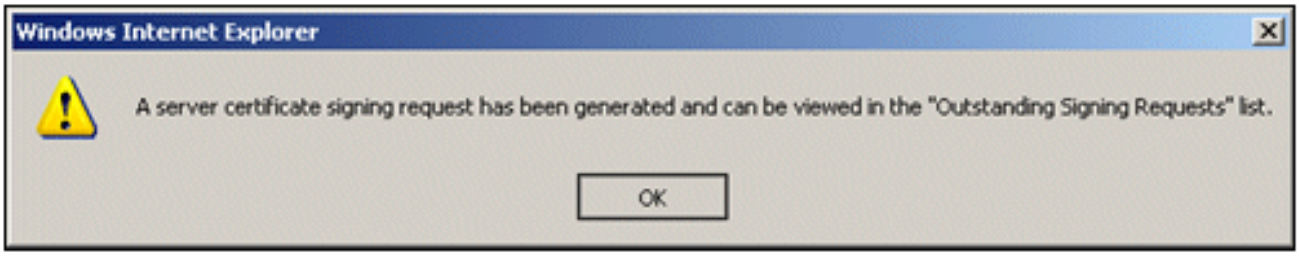
3. Wanneer u een methode voor het genereren van een servercertificaat kiest, kiest u **Aanvraag voor het genereren van een certificaat**. Klik op **Next** (Volgende).



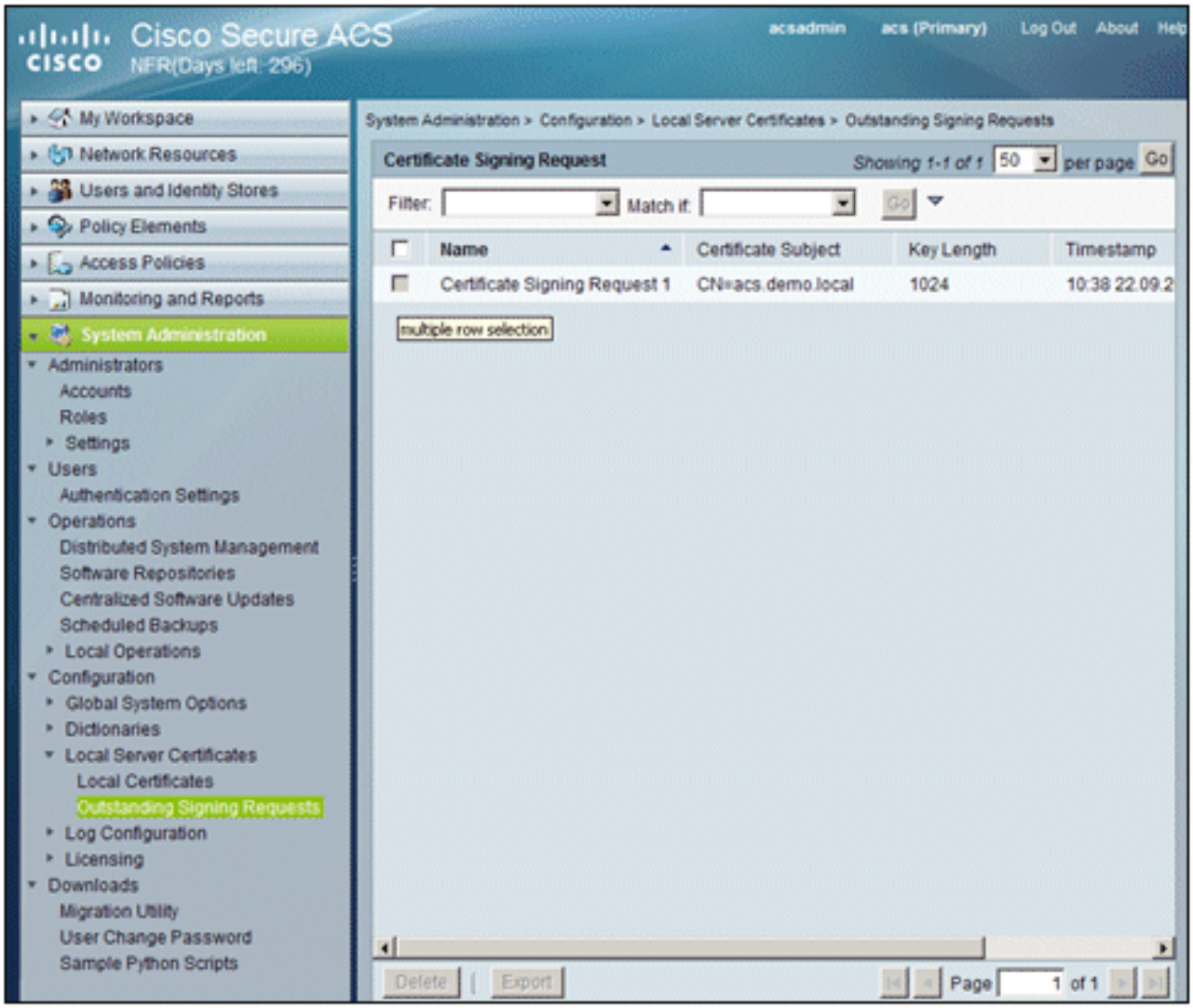
4. Voer een certificaatonderwerp en een sleutellengte in als voorbeeld en klik op **Voltooien**:Certificaat Onderwerp - **CN=acs.demo.local**Sleutellengte - **1024**



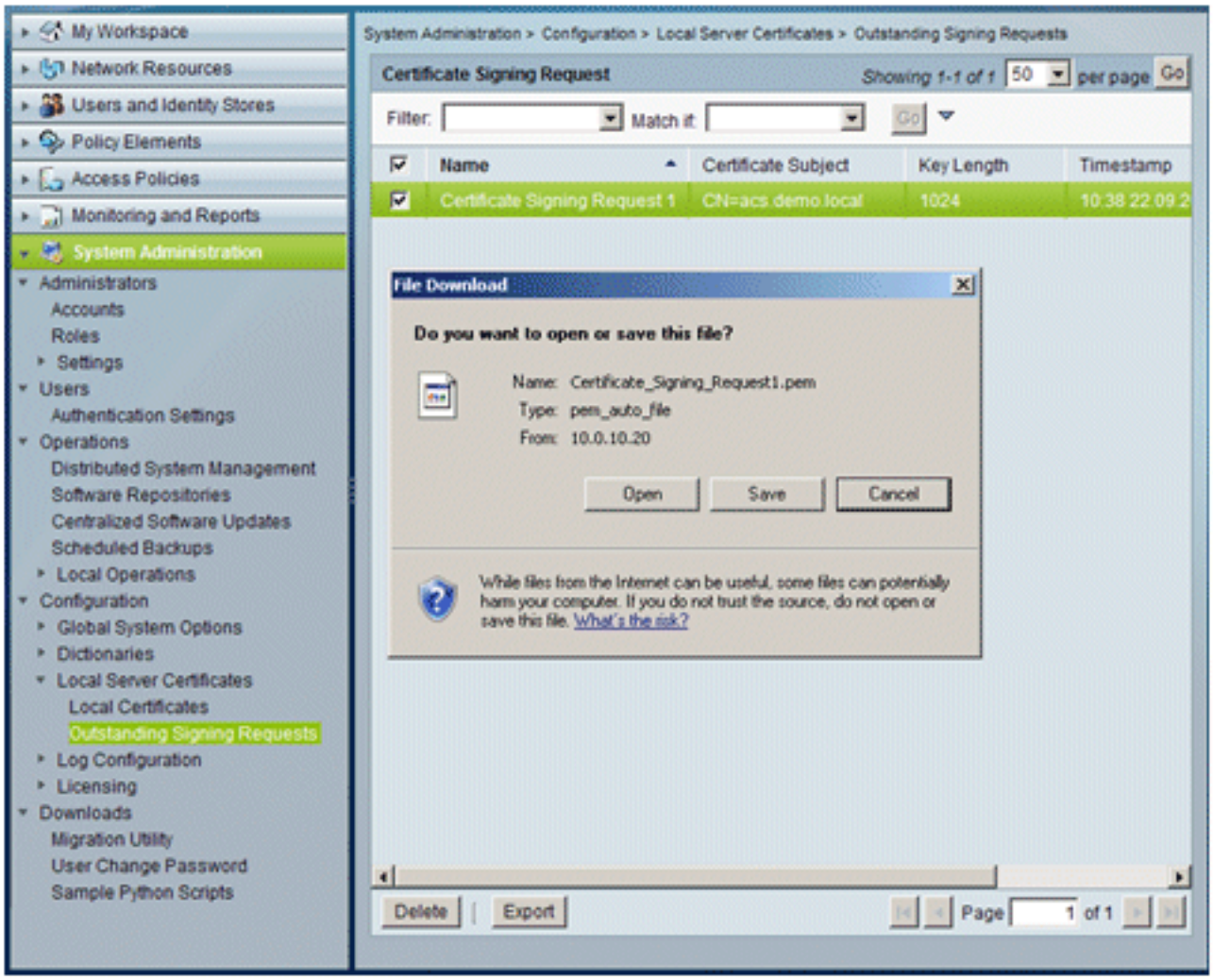
5. ACS zal vragen dat een certificaat ondertekeningsverzoek is gegenereerd. Klik op **OK**.



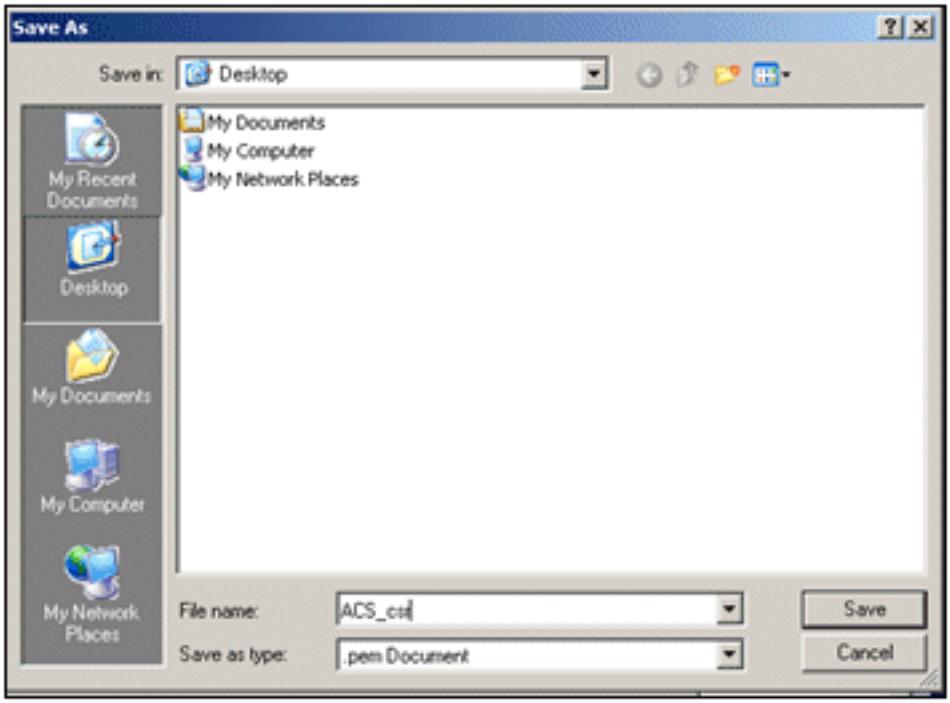
6. Ga onder Systeembeheer naar **Configuratie > Lokale servercertificaten > Openstaande ondertekeningsaanvragen**.**Opmerking:** de reden voor deze stap is dat Windows 2003 niet geschikt is voor exporteerbare sleutels en dat u een certificaataanvraag moet genereren op basis van het ACS-certificaat dat u eerder hebt gemaakt.



7. Kies de vermelding **Certificaat-ondertekeningsaanvraag** en klik op **Exporteren**.



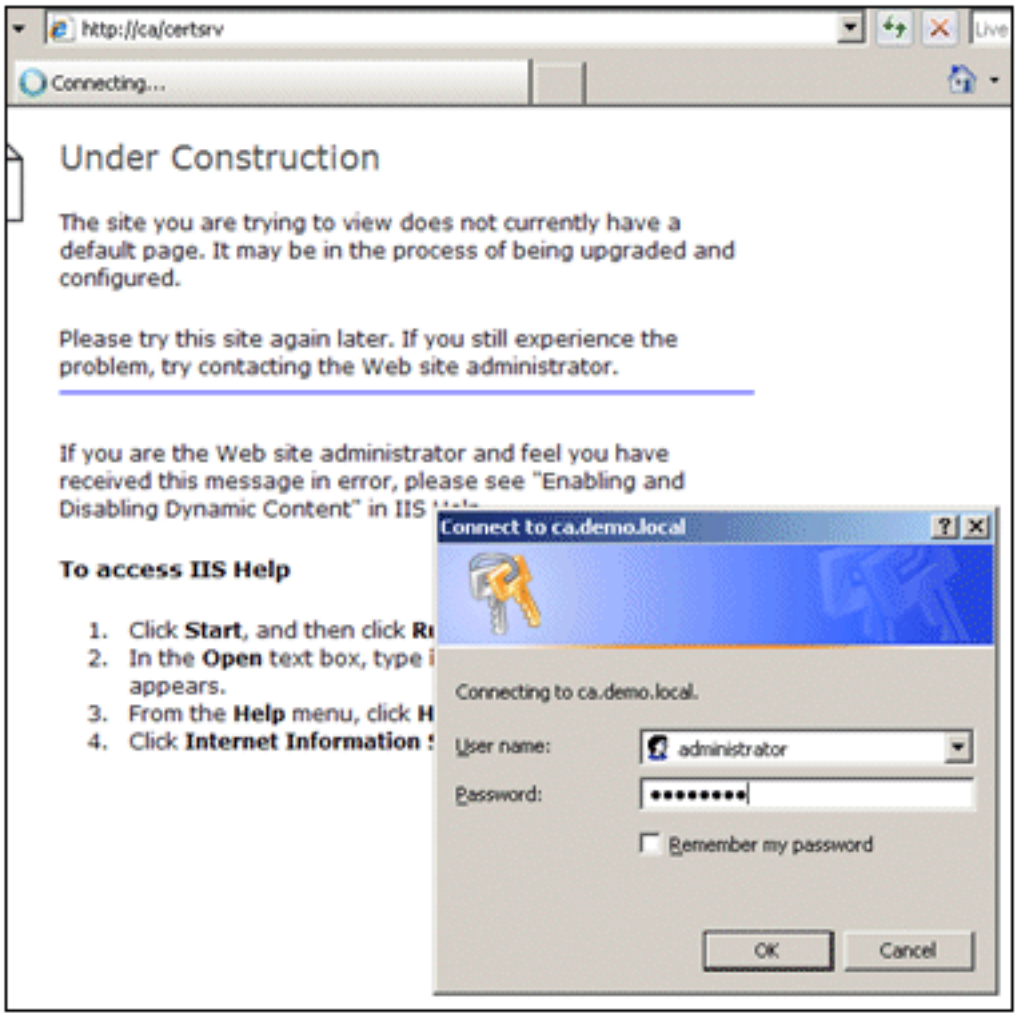
8. Sla het ACS-certificaat **.pem**-bestand op het bureaublad op.



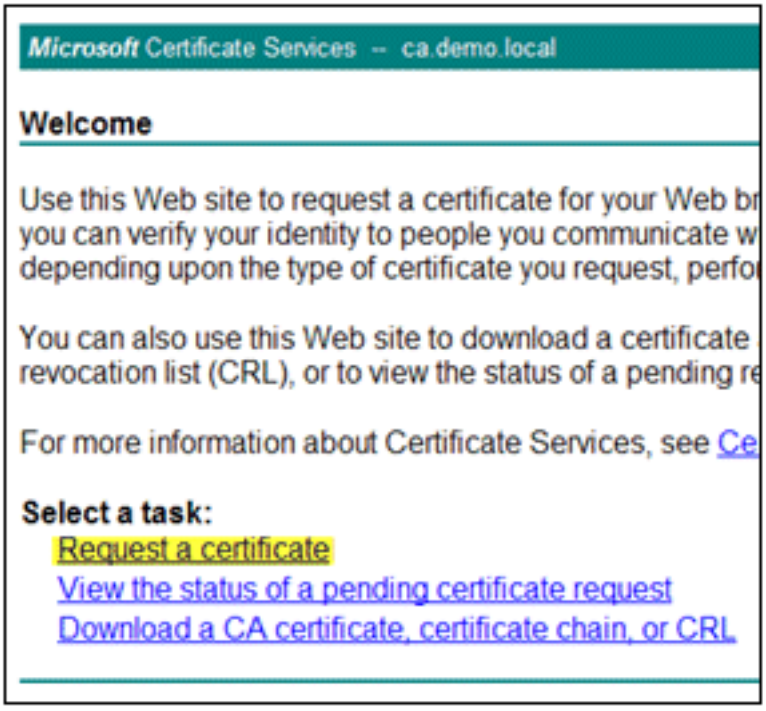
Installeer het certificaat in ACS 5.1-software

Voer de volgende stappen uit:

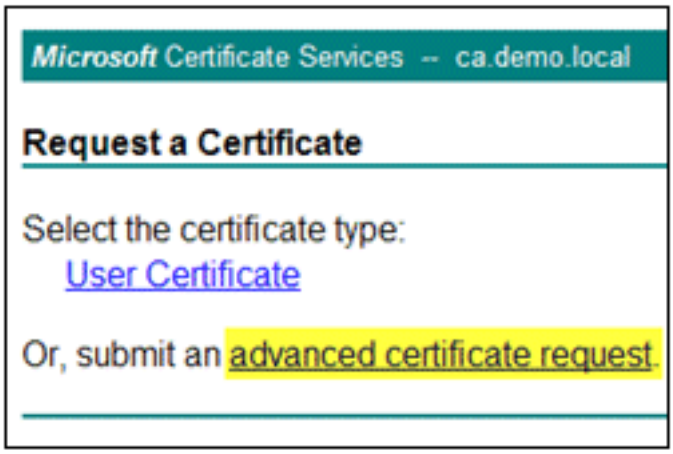
1. Open een browser en maak verbinding met CA server URL **http://10.0.10.10/certsrv**.



2. Het venster Microsoft Certificate Services verschijnt. Kies **Certificaat aanvragen**.

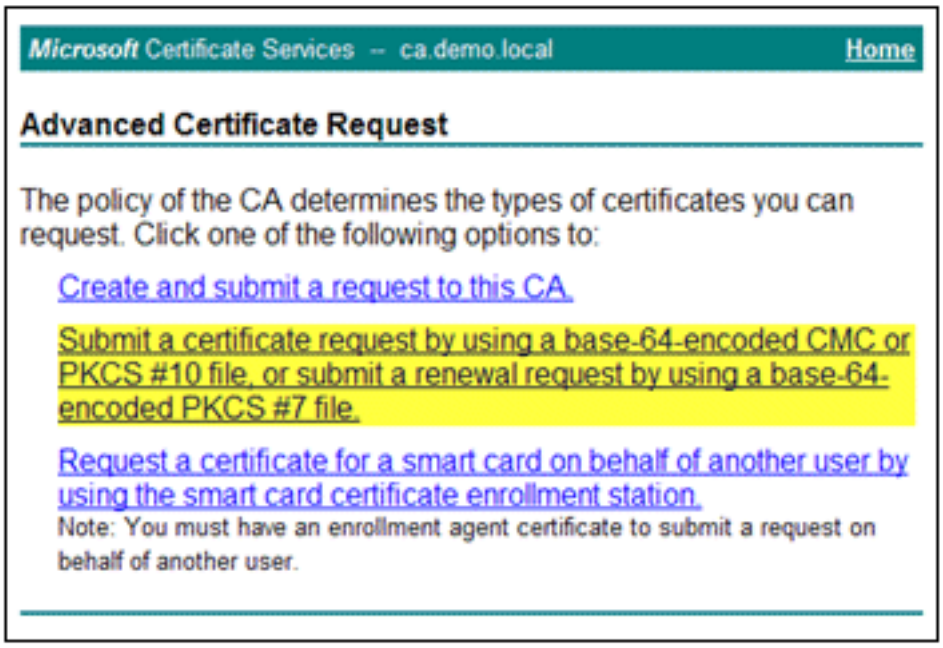


3. Klik om een **geavanceerde certificaataanvraag in** te



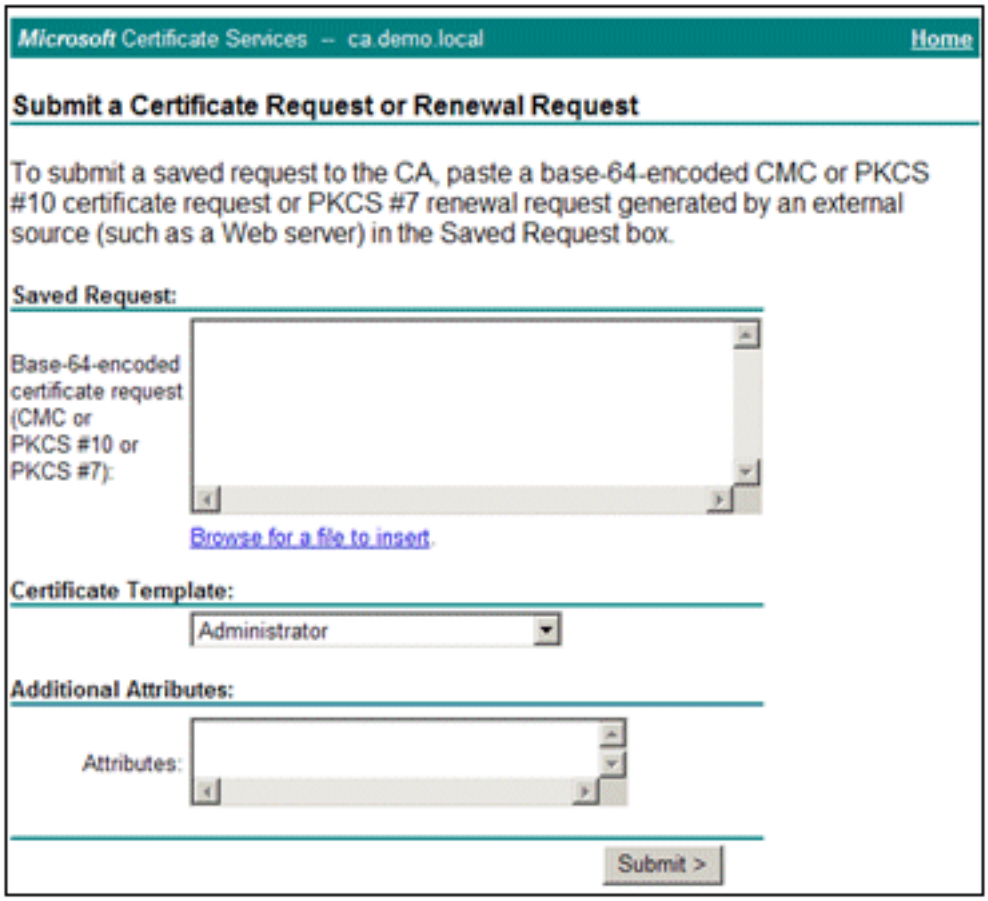
dienen.

4. In het geavanceerde verzoek, klik **Submit een certificaatverzoek dat basis-64-**



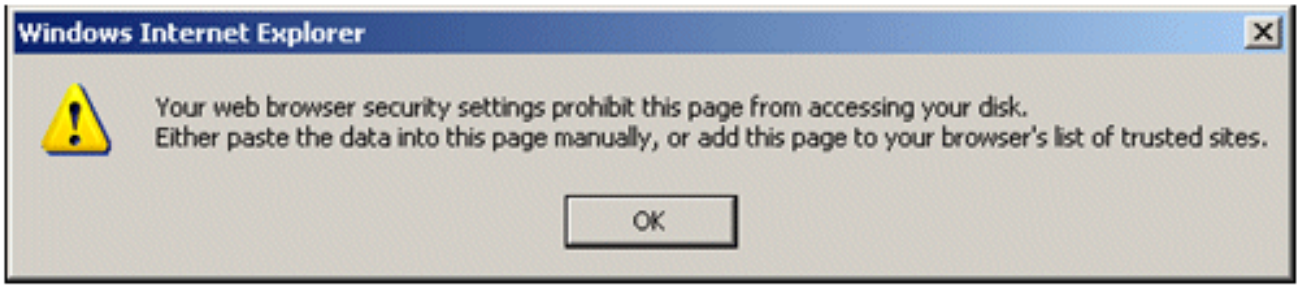
gecodeerd...

5. Blader in het veld Opgeslagen aanvraag naar het vorige ACS-certificaat aanvraagbestand en voer dit in als de beveiligingsrechten van de browser dit

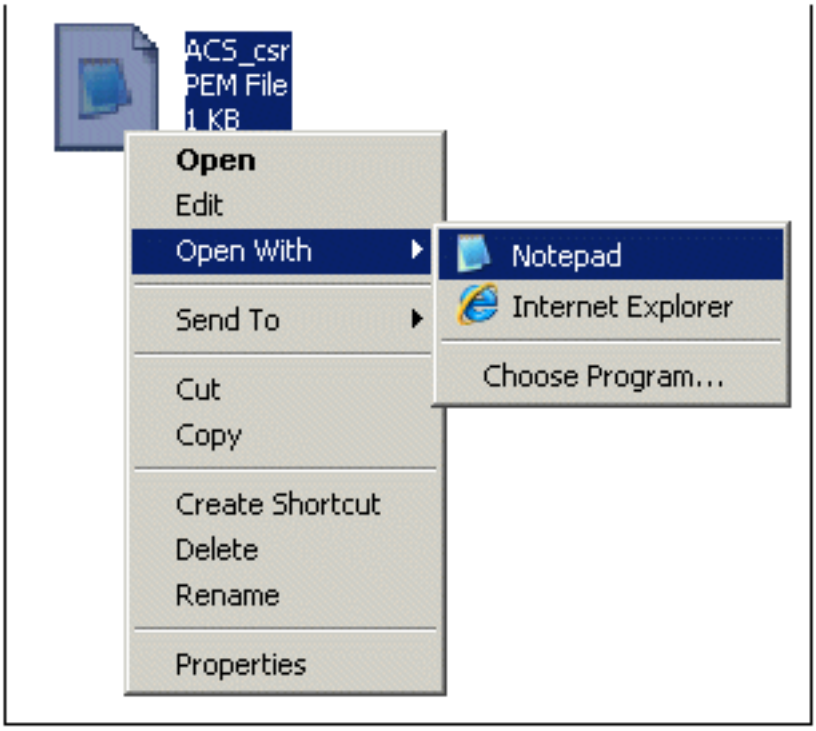


toestaan.

6. De beveiligingsinstellingen van de browser staan mogelijk geen toegang tot het bestand op een schijf toe. Als dit het geval is, klikt u op **OK** om een handmatige plak uit te voeren.

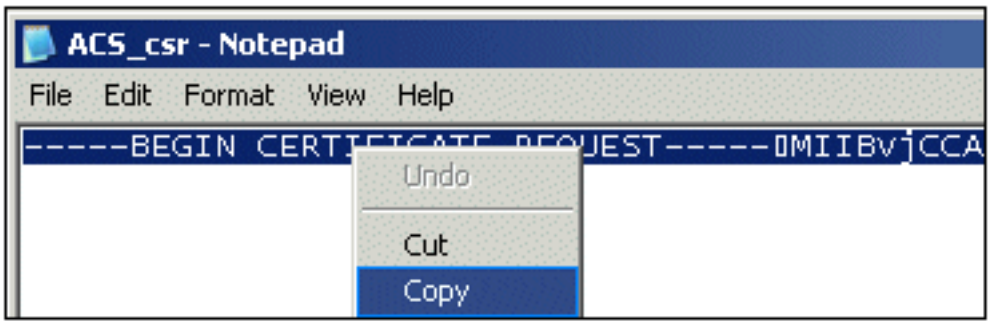


7. Zoek het ACS *.pem-bestand uit de vorige ACS-export. Open het bestand met een teksteditor (bijvoorbeeld



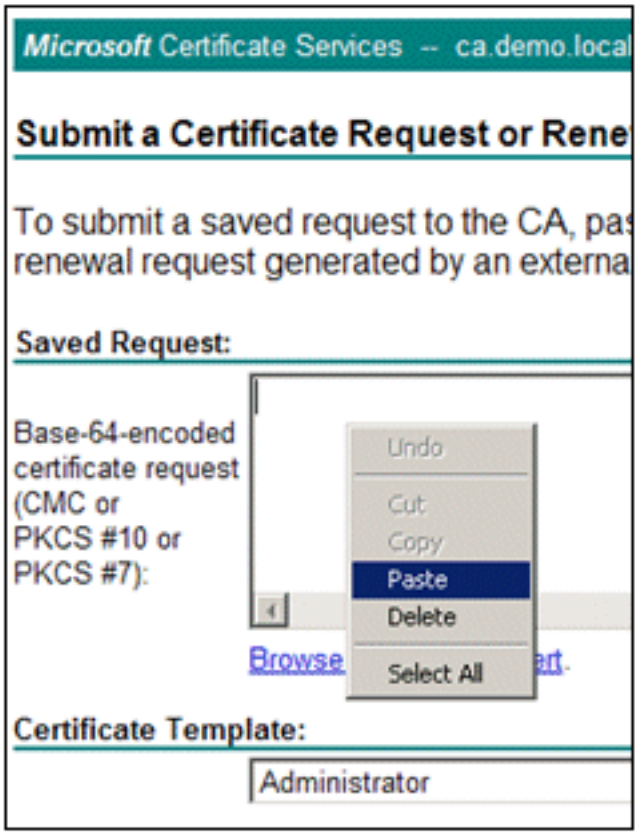
Kladblok).

8. Markeer de gehele inhoud van het bestand en klik op



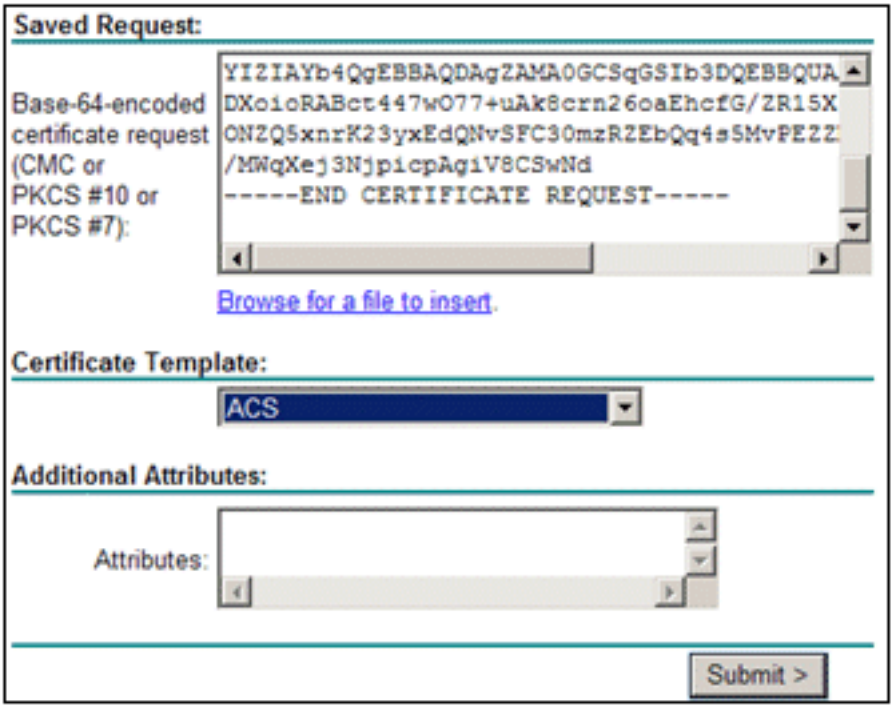
Kopiëren.

9. Ga terug naar het venster voor Microsoft-certificaataanvraag. **Plakt** de gekopieerde inhoud in

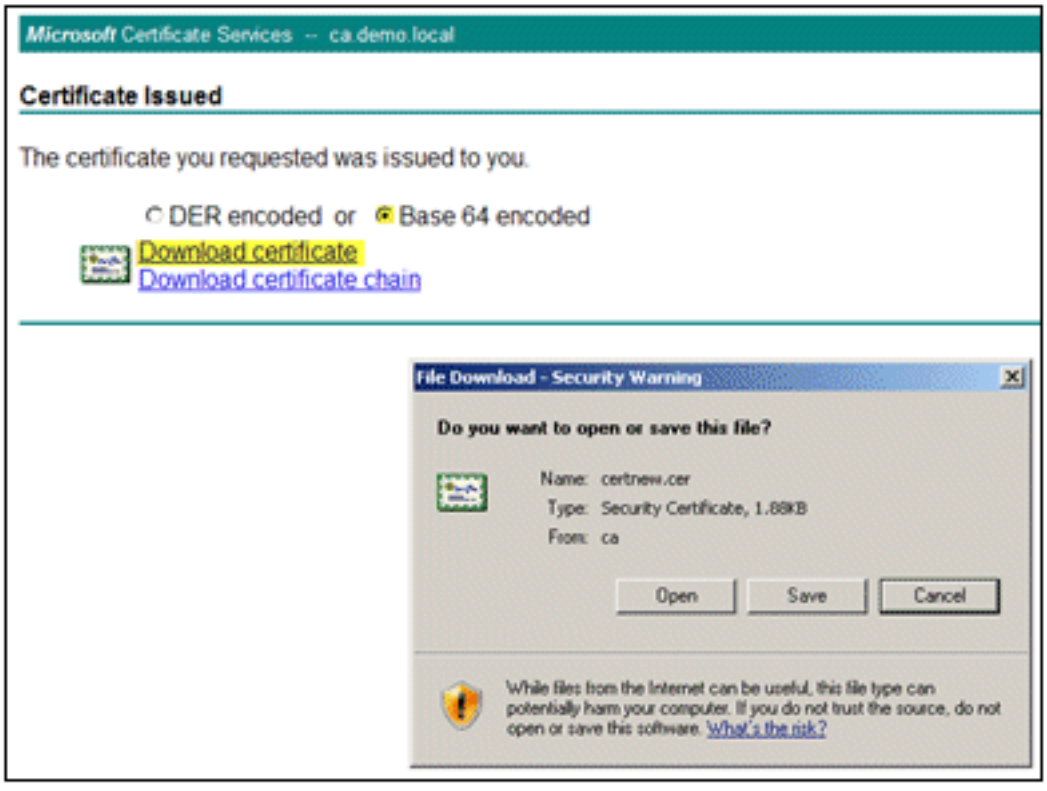


het veld Opgeslagen aanvraag.

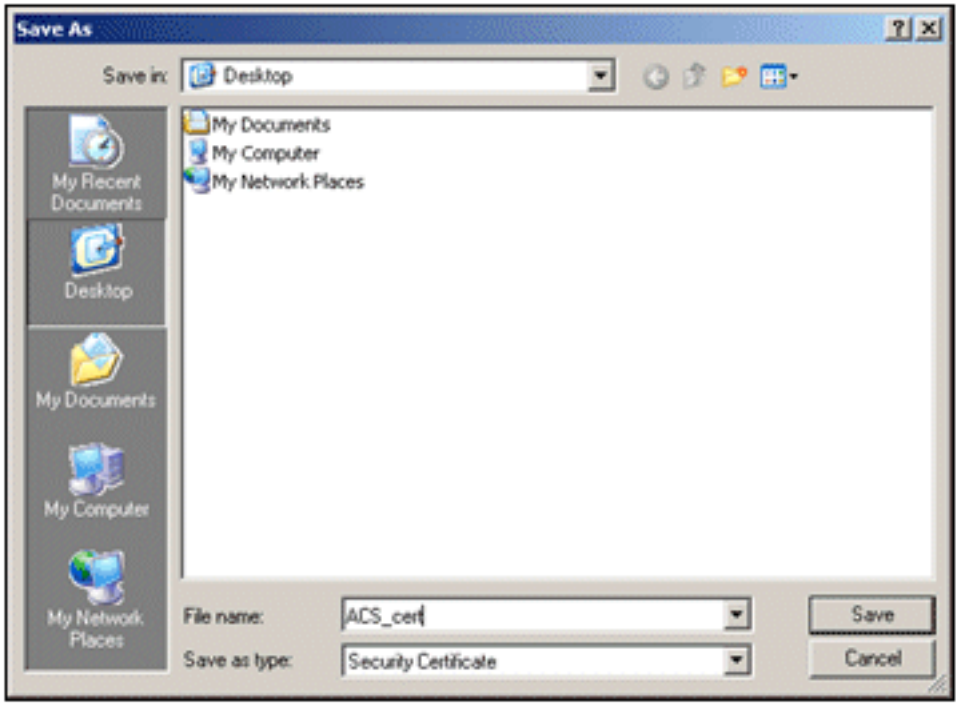
10. Kies **ACS** als de certificaatsjabloon en klik op **Indienen**.



11. Zodra het certificaat is afgegeven, kiest u **Base 64 gecodeerd** en klikt u op **Certificaat downloaden**.

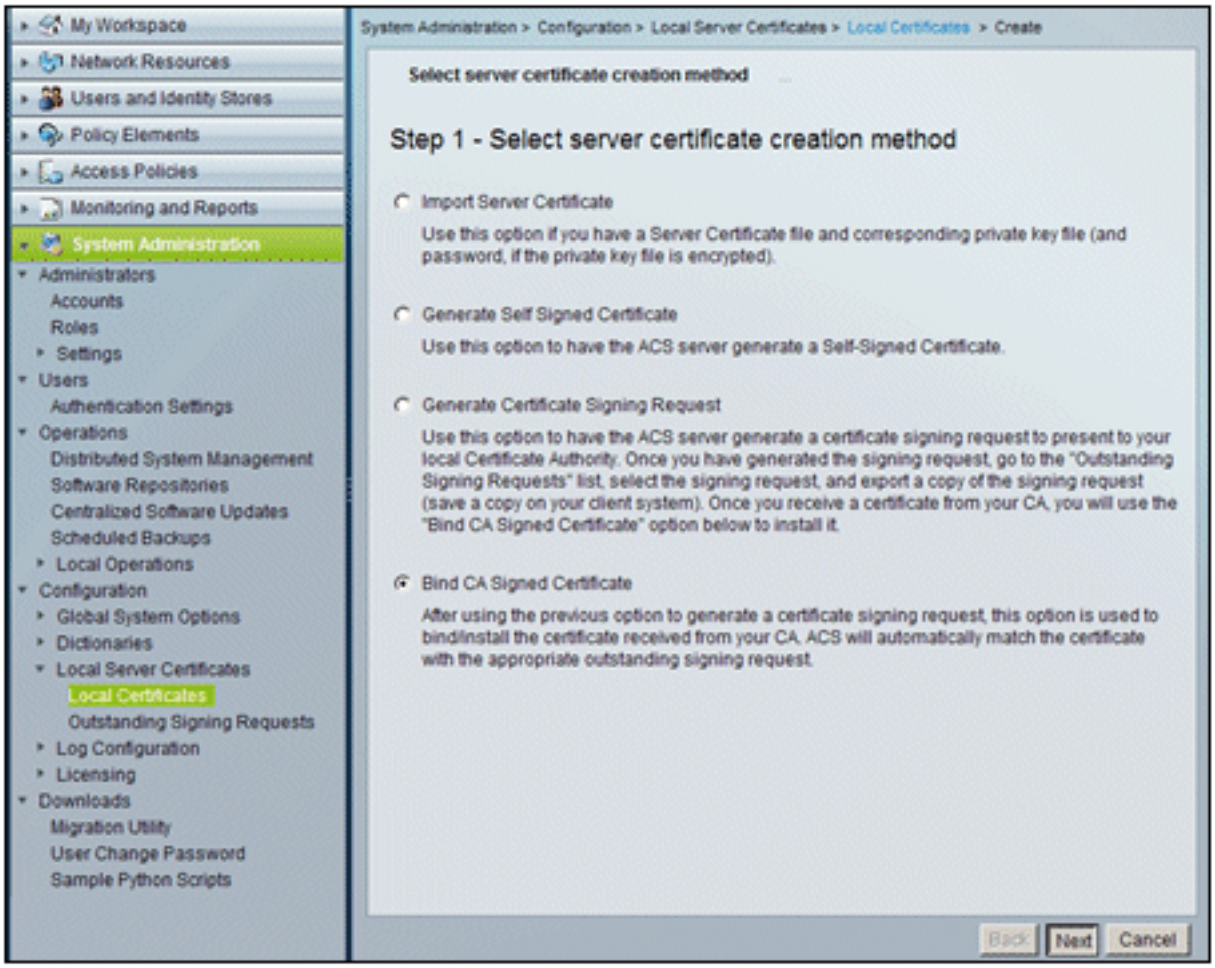


12. Klik op **Opslaan** om het certificaat op te slaan op het

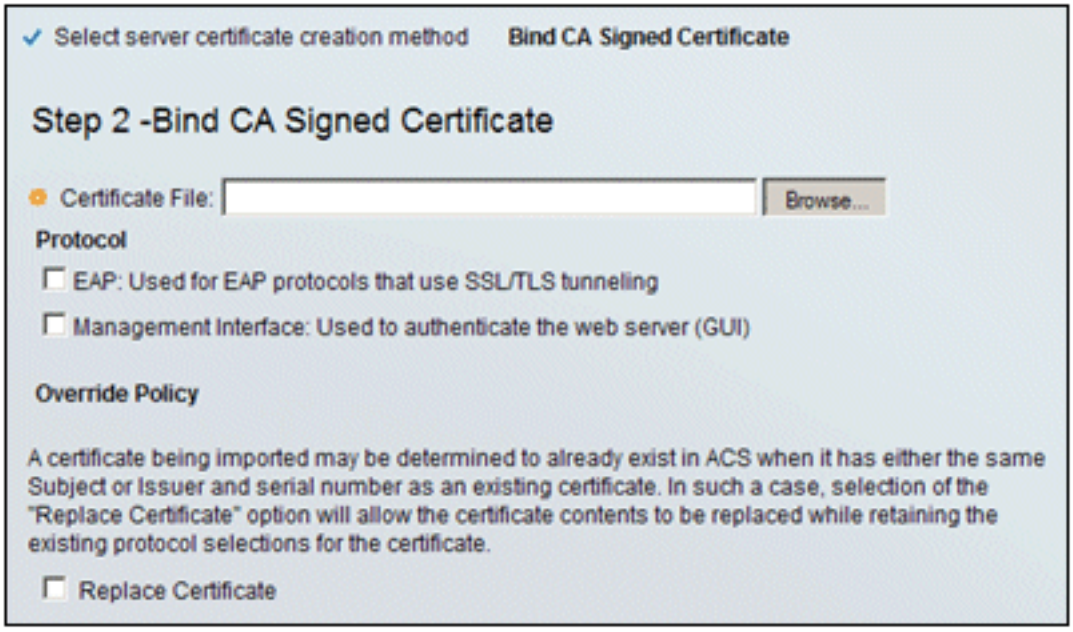


bureaublad.

13. Ga naar **ACS > Systeembeheer > Configuratie > Lokale servercertificaten**. Kies **Bind CA Ondertekend certificaat** en klik op **Volgende**.

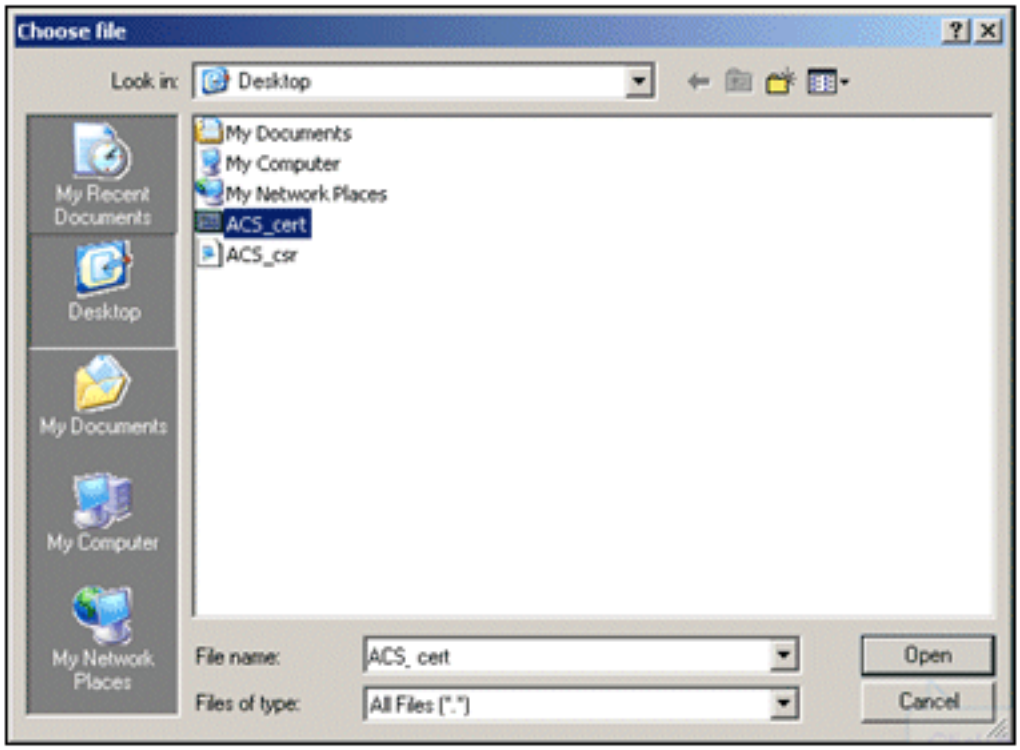


14. Klik op **Bladeren** en lokaliseer het opgeslagen



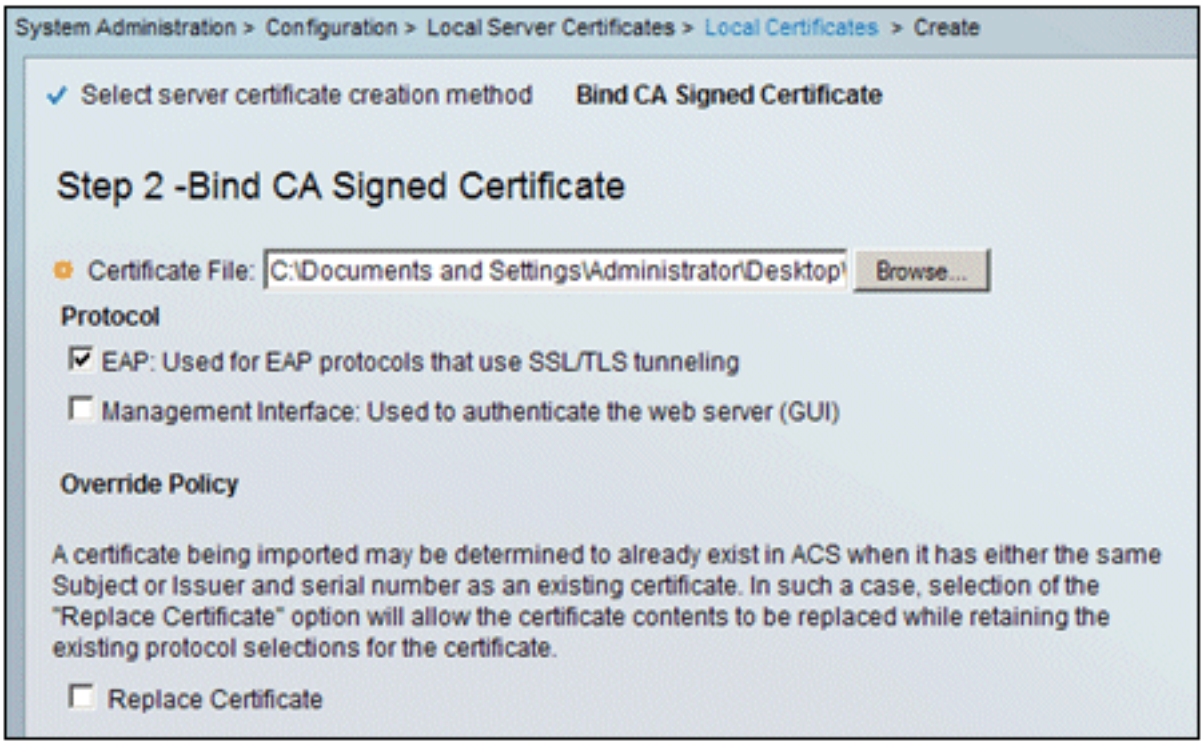
certificaat.

15. Kies het ACS-certificaat dat is afgegeven door de CA-server en klik op

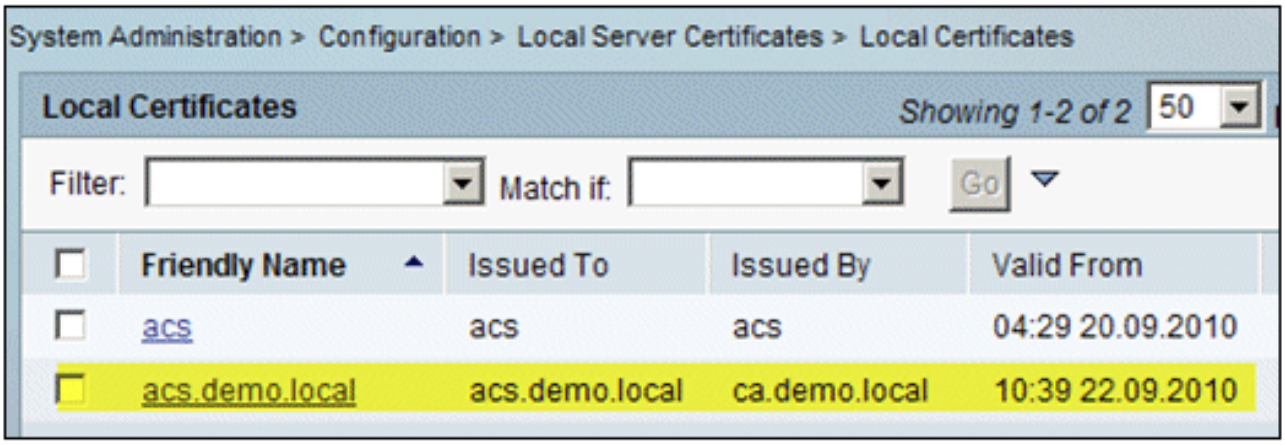


Openen.

16. Selecteer ook het vakje Protocol voor **EAP** en klik op **Voltooien**.



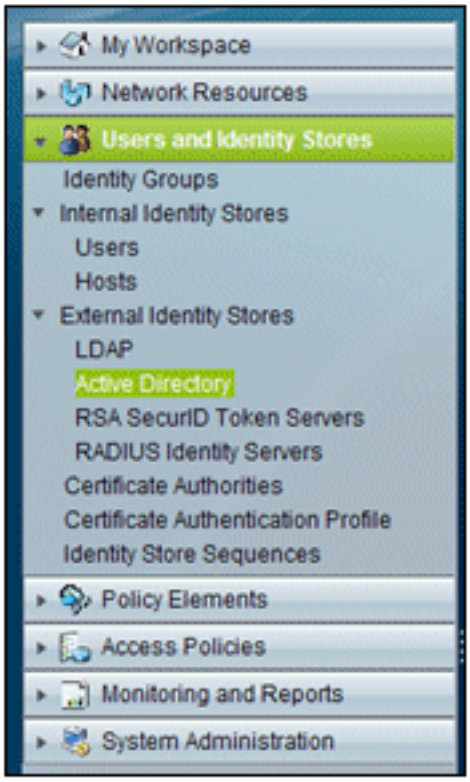
17. Het door CA afgegeven ACS-certificaat wordt weergegeven in het lokale ACS-certificaat.



ACS Identity Store configureren voor Active Directory

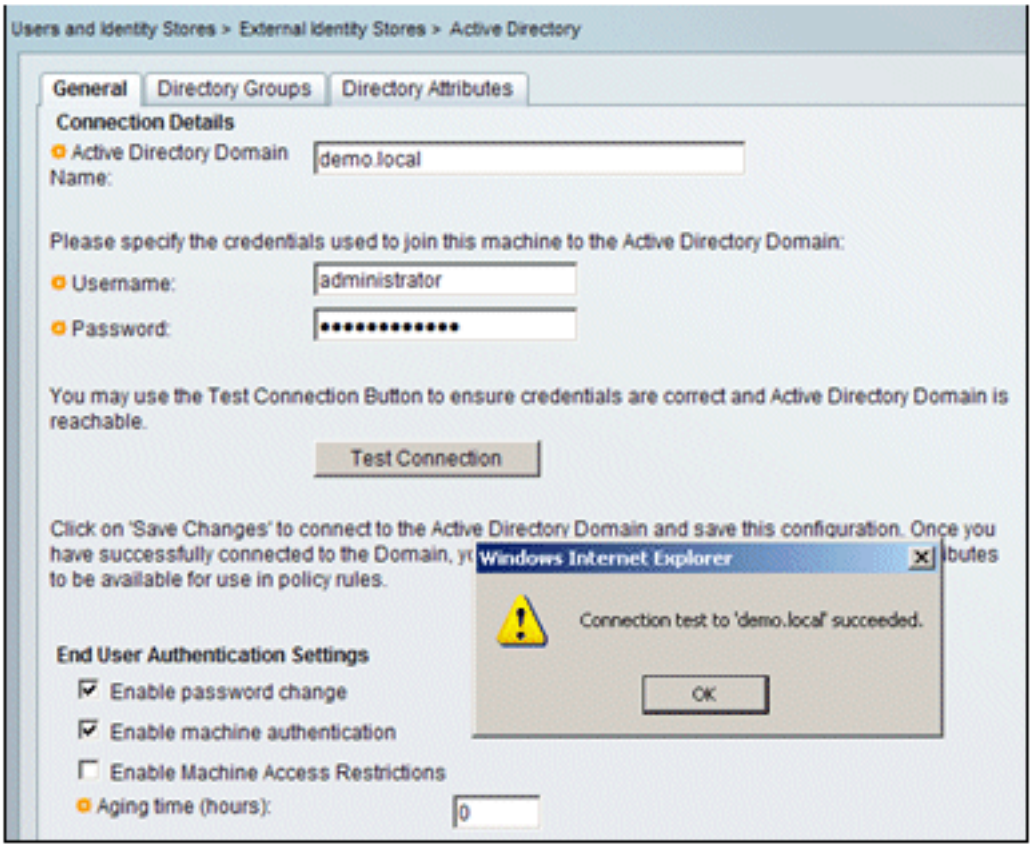
Voer de volgende stappen uit:

1. Maak verbinding met ACS en log in met Admin account.
2. Ga naar **Gebruikers en Identity Stores > Externe Identity Stores > Active**



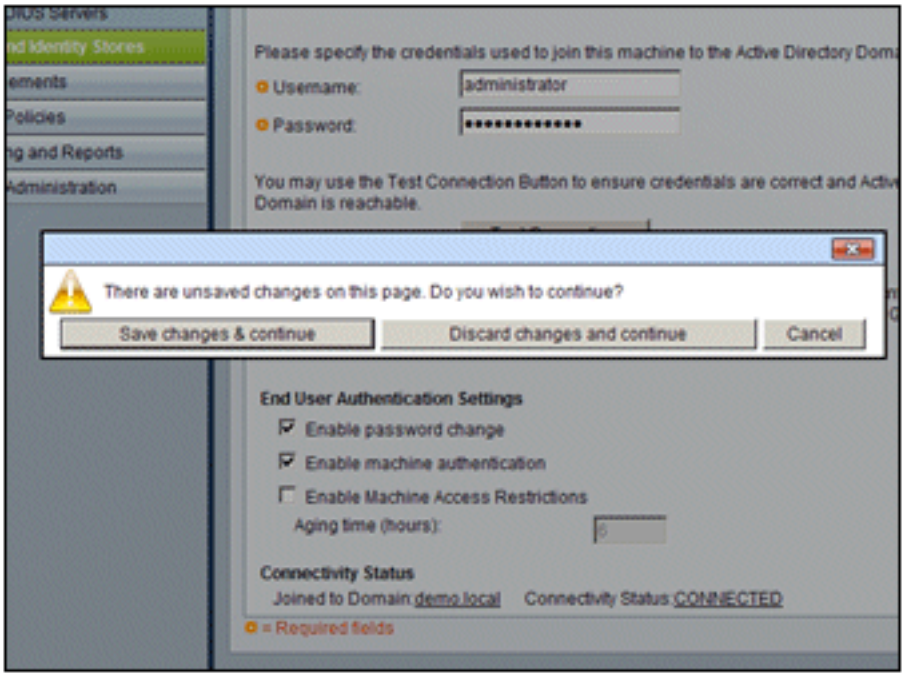
Directory.

3. Voer het Active Directory Domain *demo.local in*, voer het wachtwoord van de server in en klik op **Test Connection**. Klik op **OK** om verder te



gaan.

4. Klik op **Wijzigingen**

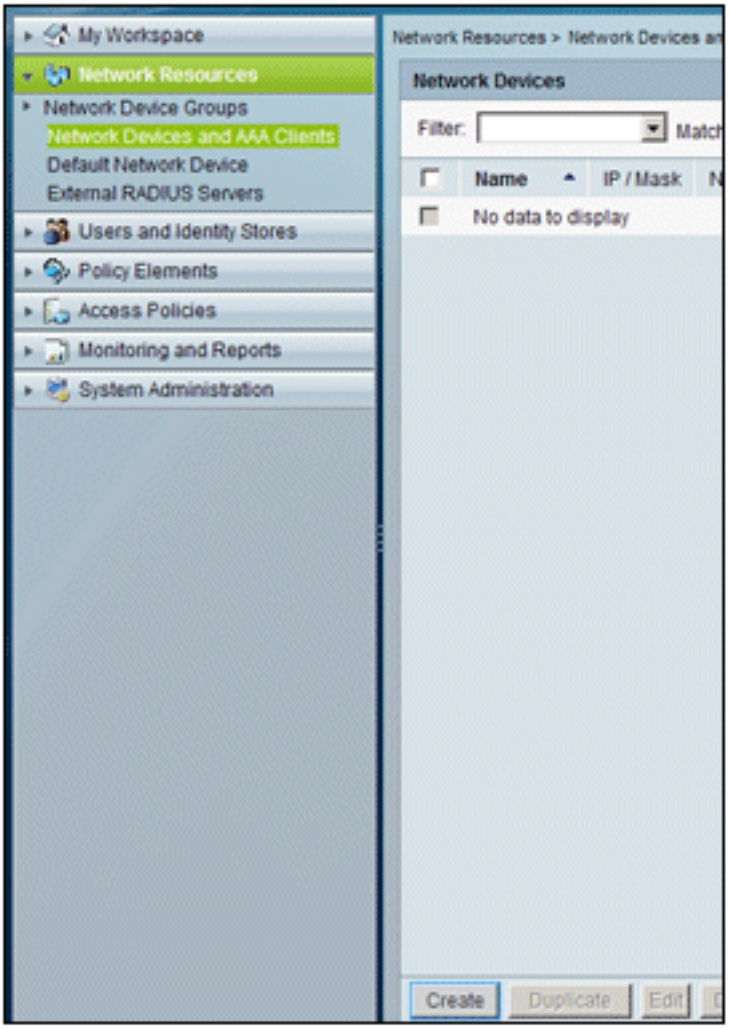


opslaan. **Opmerking:** Voor meer informatie over de integratieprocedure ACS 5.x, zie [ACS 5.x en later: Integratie met Microsoft Active Directory Configuration Voorbeeld](#).

Een controller toevoegen aan ACS als AAA-client

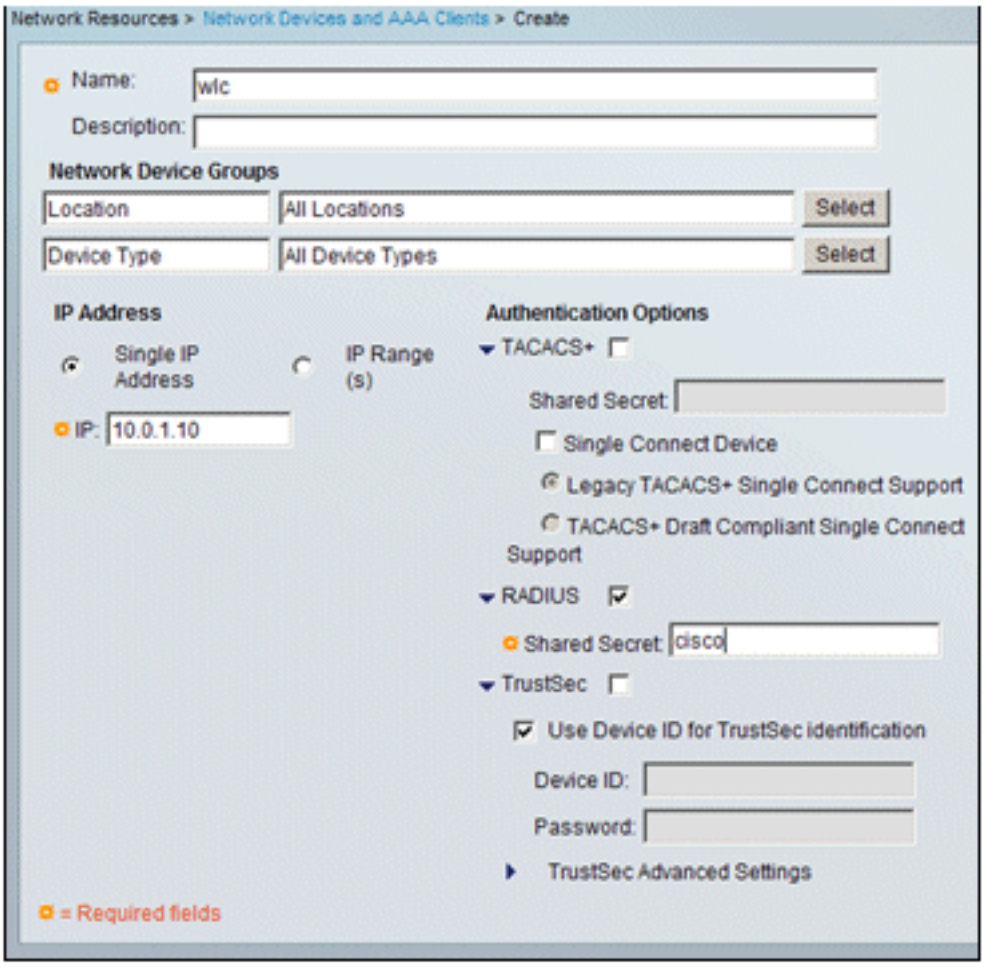
Voer de volgende stappen uit:

1. Maak verbinding met ACS en ga naar **Network Resources > Network Devices en AAA**



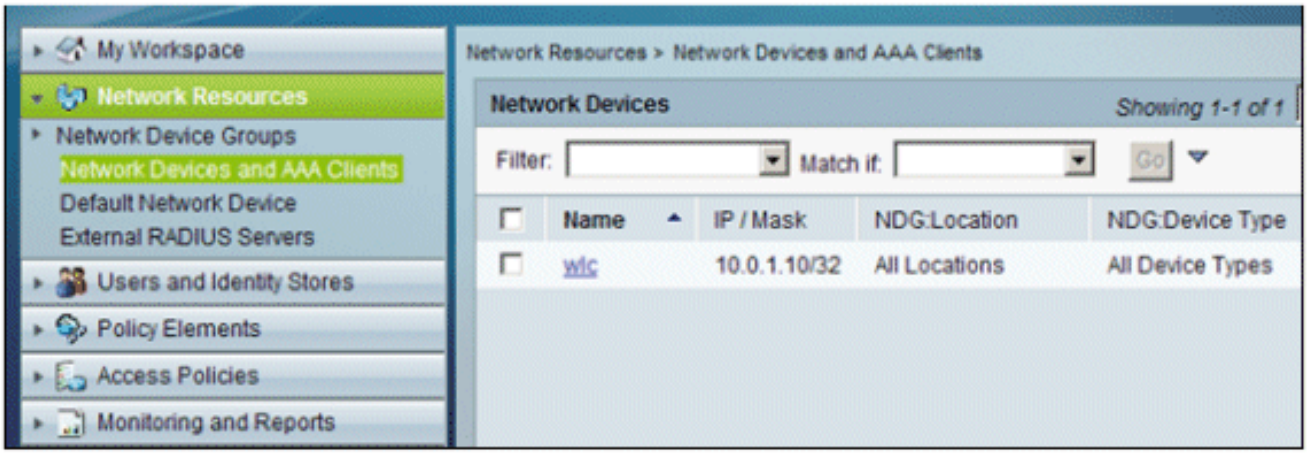
Clients. Klik op **Aanmaken**.

2. Voer in deze velden een van de volgende handelingen uit:Naam - **wlc**IP - **10.0.1.10**Selectievakje RADIUS - **ingeschakeld**Gedeeld geheim -



Cisco

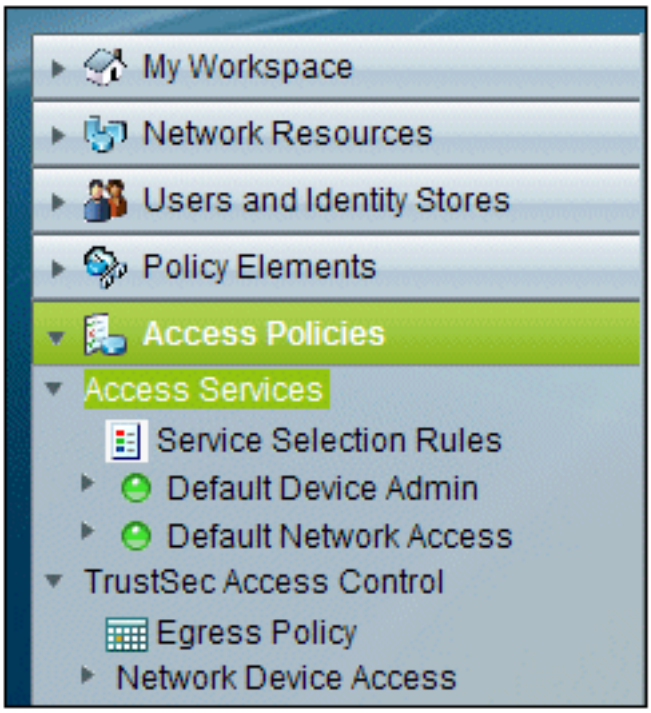
3. Klik op **Indienen** als u klaar bent. De controller wordt als een ingang weergegeven in de ACS Network Devices-
   lijst.



ACS-toegangsbeleid configureren voor draadloos

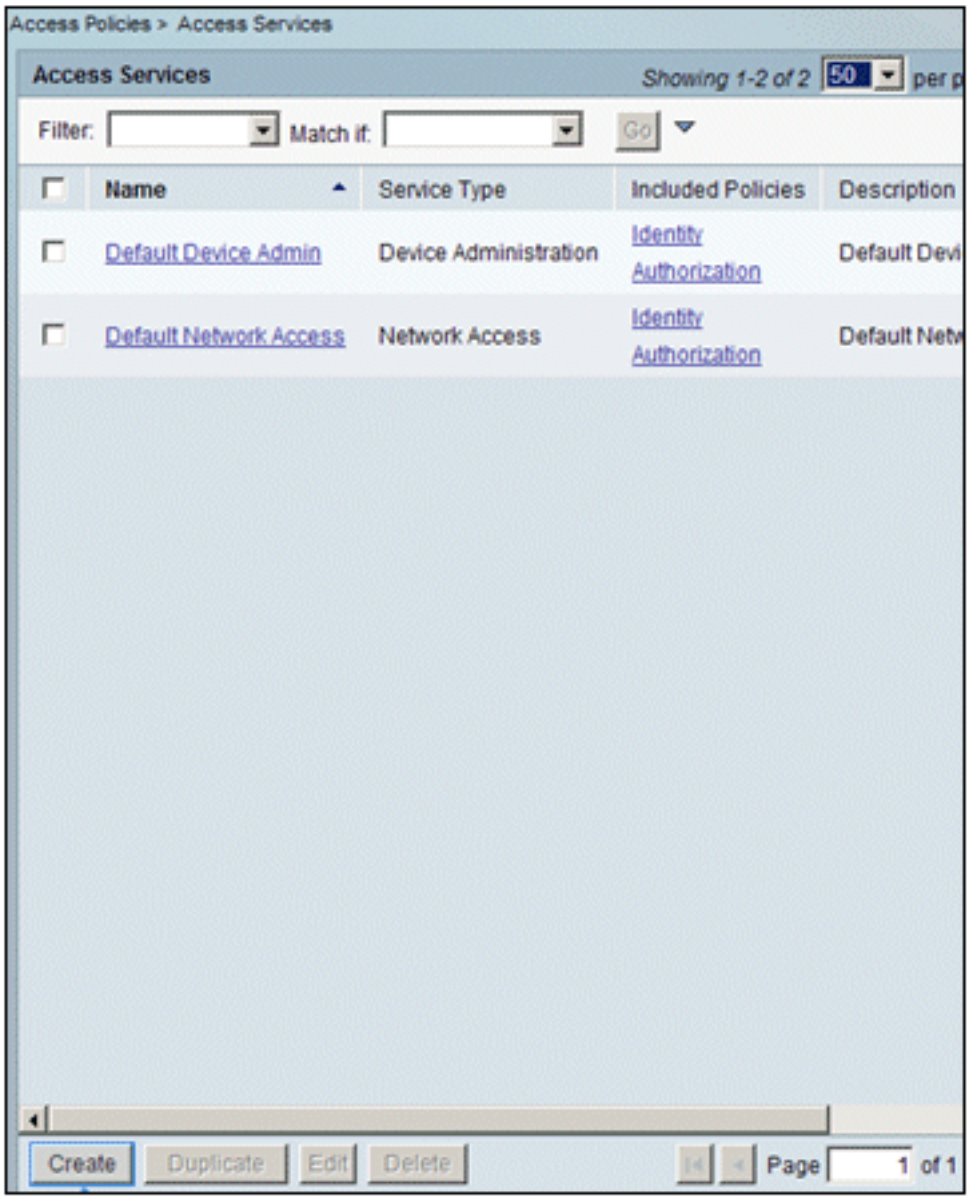
Voer de volgende stappen uit:

1. In ACS, ga naar **Toegangsbeleid >**



Toegangsdiensten.

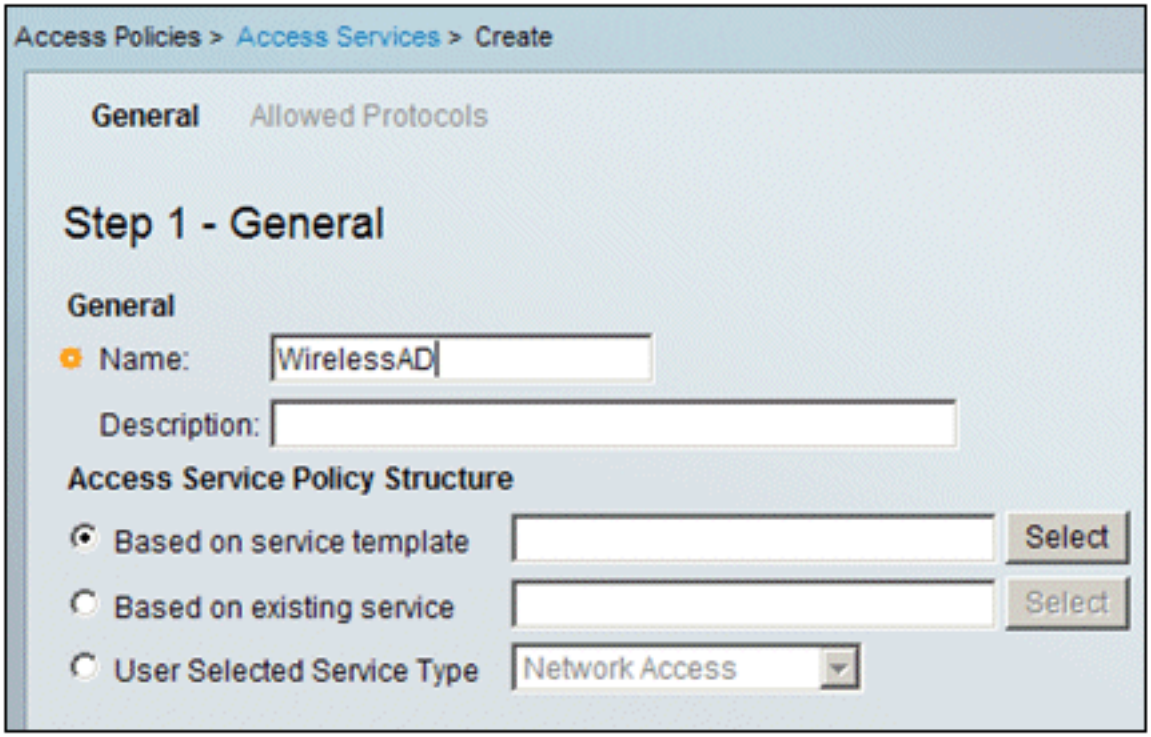
2. Klik in het venster Toegangsservices op



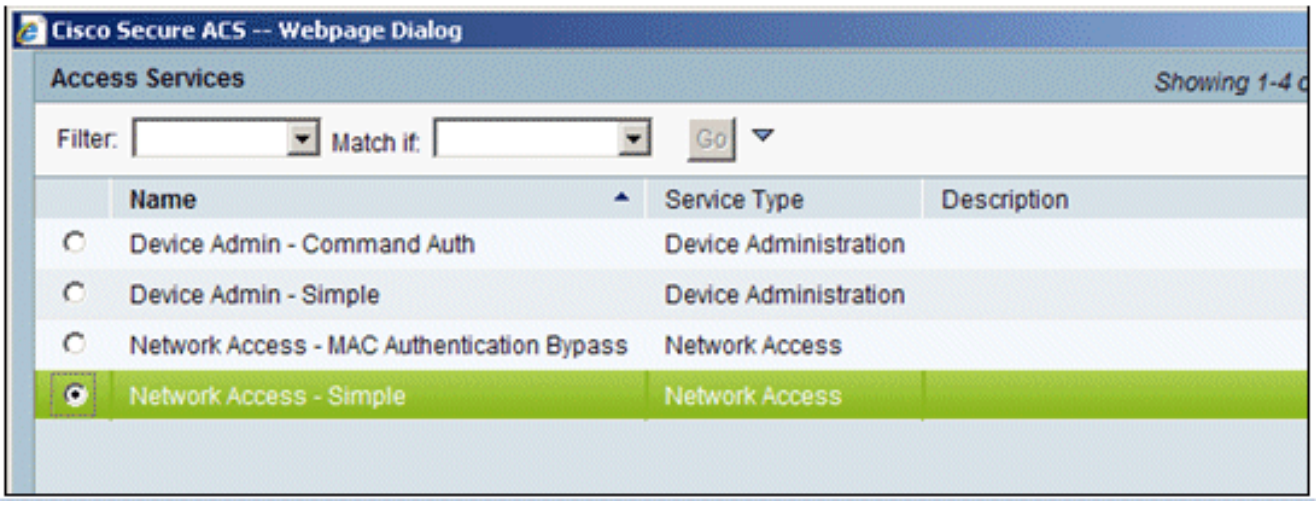
Maken.

3. Maak een toegangsservice en voer een naam in (bijvoorbeeld WirelessAD). Kies **Gebaseerd**

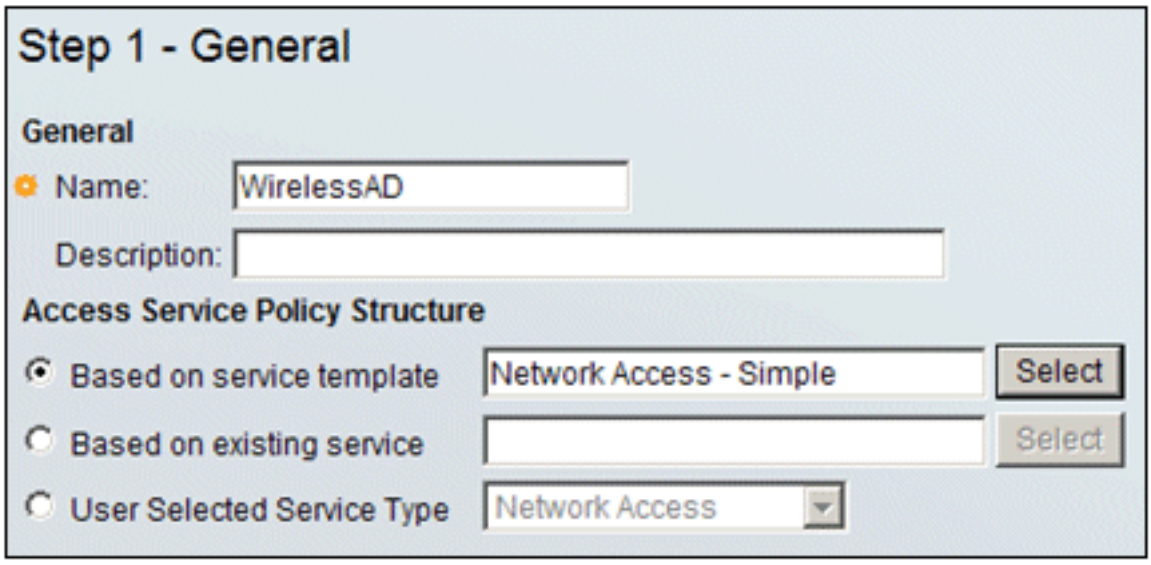
op servicesjabloon en klik op Selecteren.



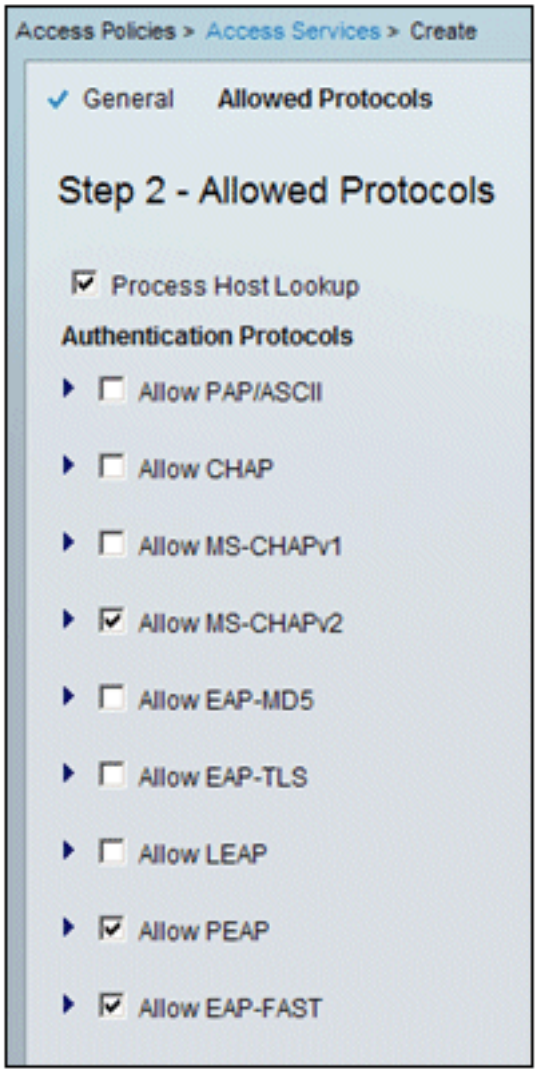
4. Kies in het dialoogvenster Webpagina de optie **Netwerktoegang - Eenvoudig**. Klik op **OK**.



5. Kies in het dialoogvenster Webpagina de optie **Netwerktoegang - Eenvoudig**. Klik op **OK**. Klik op **Volgende** als de sjabloon is geselecteerd.

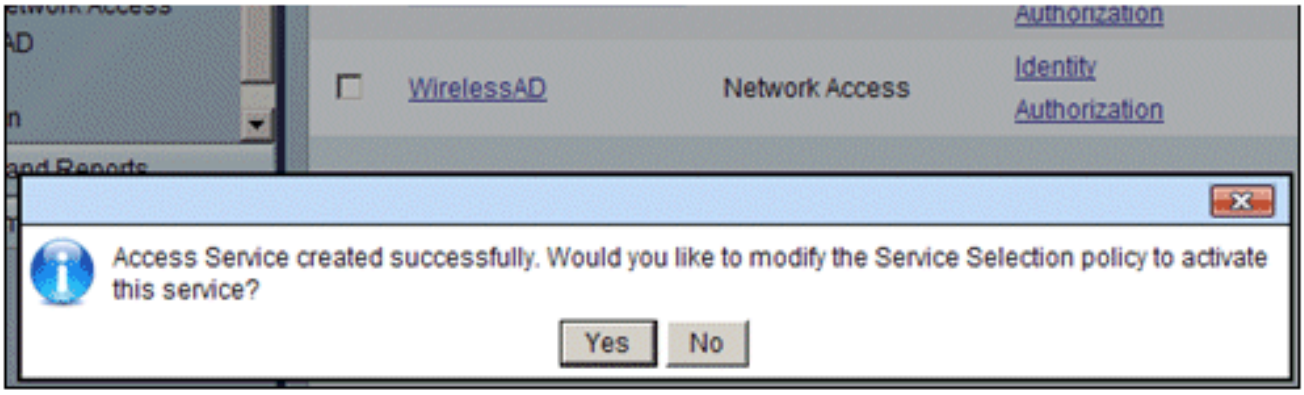


6. Schakel onder Toegestane protocollen de selectievakjes **Allow MS-CHAPv2** and **Allow PEAP**

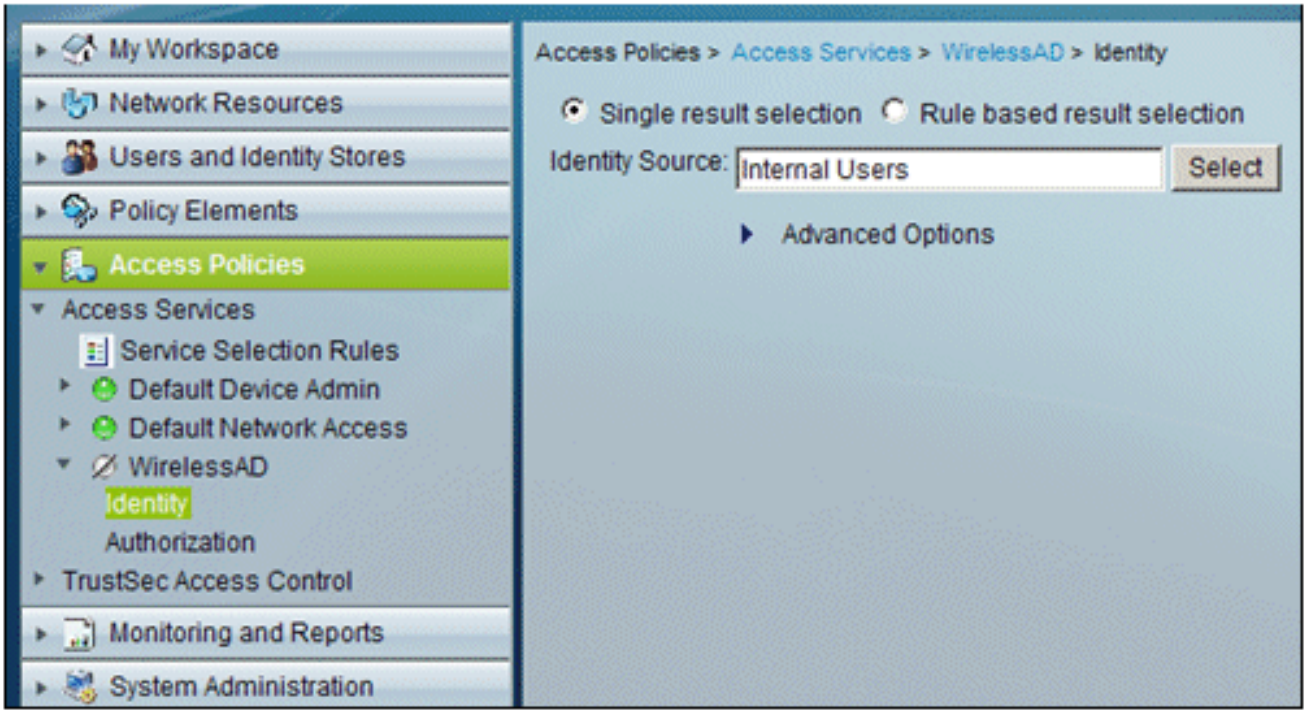


in. Klik op **Finish** (Voltooien).

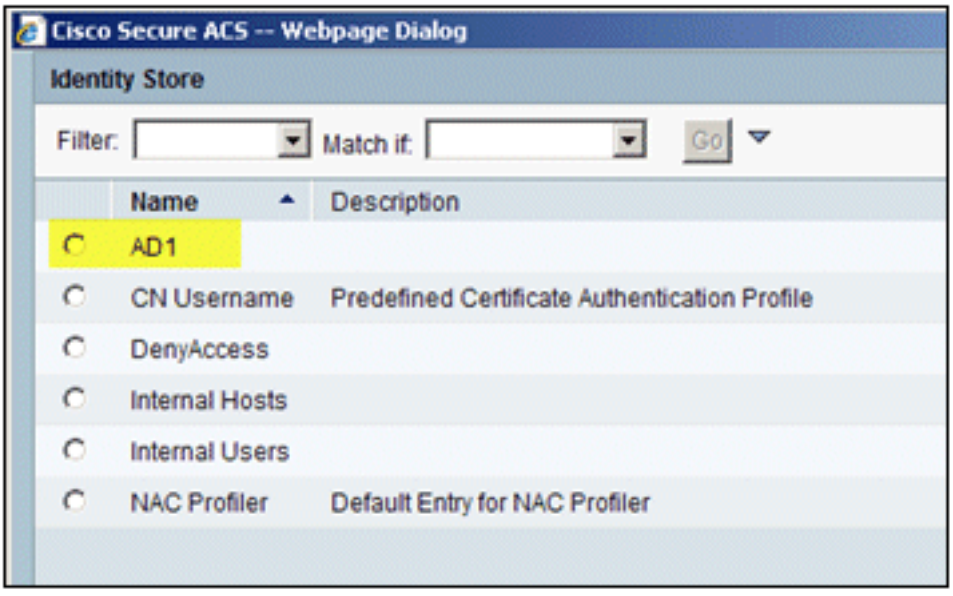
7. Wanneer ACS u vraagt om de nieuwe service te activeren, klikt u op **Ja**.



8. In de nieuwe toegangsservice die net is gemaakt/geactiveerd, kunt u **Identity** uitvouwen en kiezen. Klik voor de identiteitsbron op **Selecteren**.



9. Kies **AD1** voor Active Directory die is geconfigureerd in ACS, klik op **OK**.



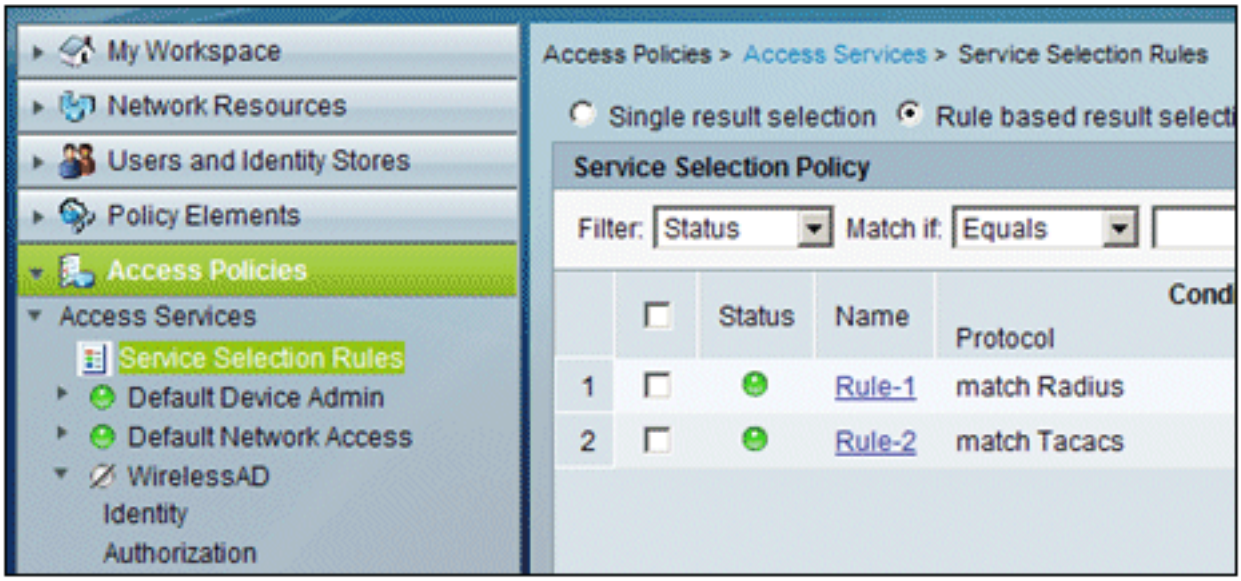
10. Bevestig dat de Identiteitsbron AD1 is en klik op **Wijzigingen**

opslaan.

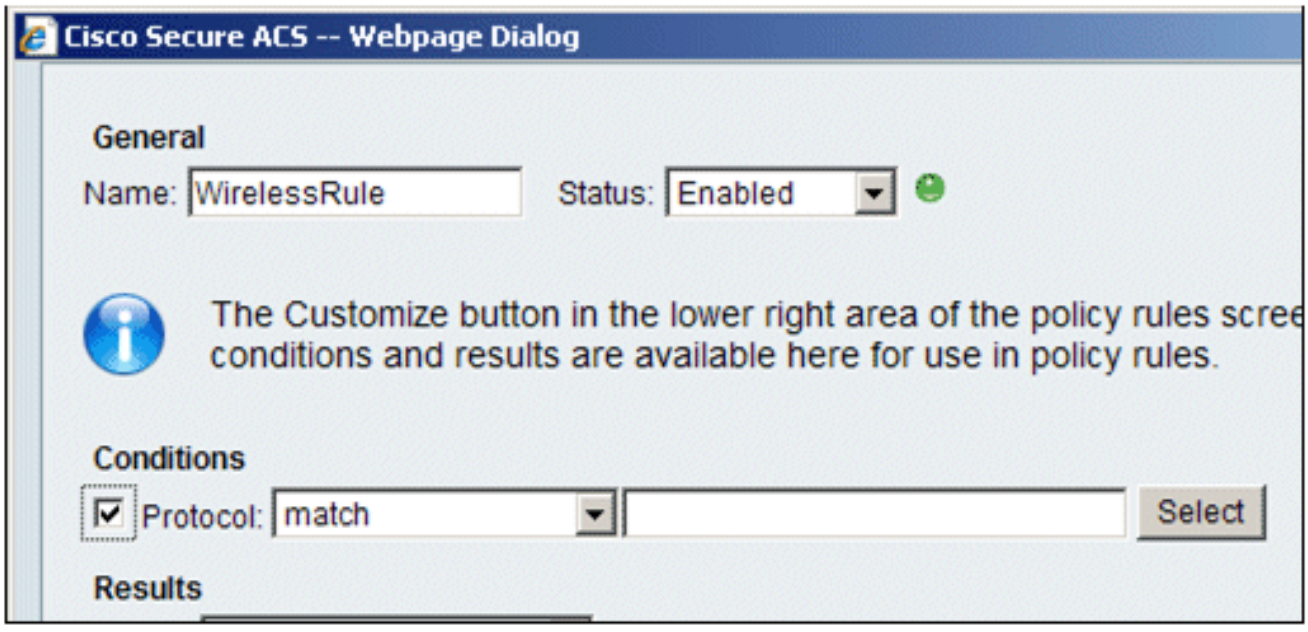
ACS-toegangsbeleid en -serviceregel maken

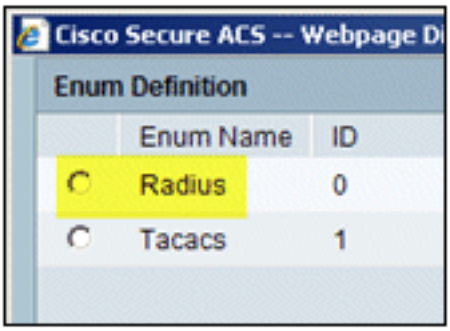
Voer de volgende stappen uit:

1. Ga naar **Toegangsbeleid > Regels voor servicesselectie**.

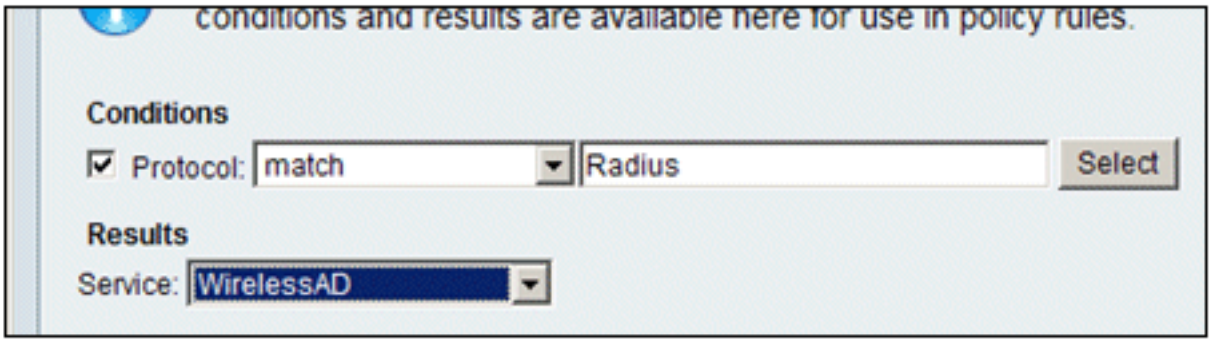


2. Klik op **Maken** in het venster Servicesselectiebeleid. Geef de nieuwe regel een naam (bijvoorbeeld *WirelessRule*). Vink het vakje **Protocol** aan om **Radius** aan te passen.

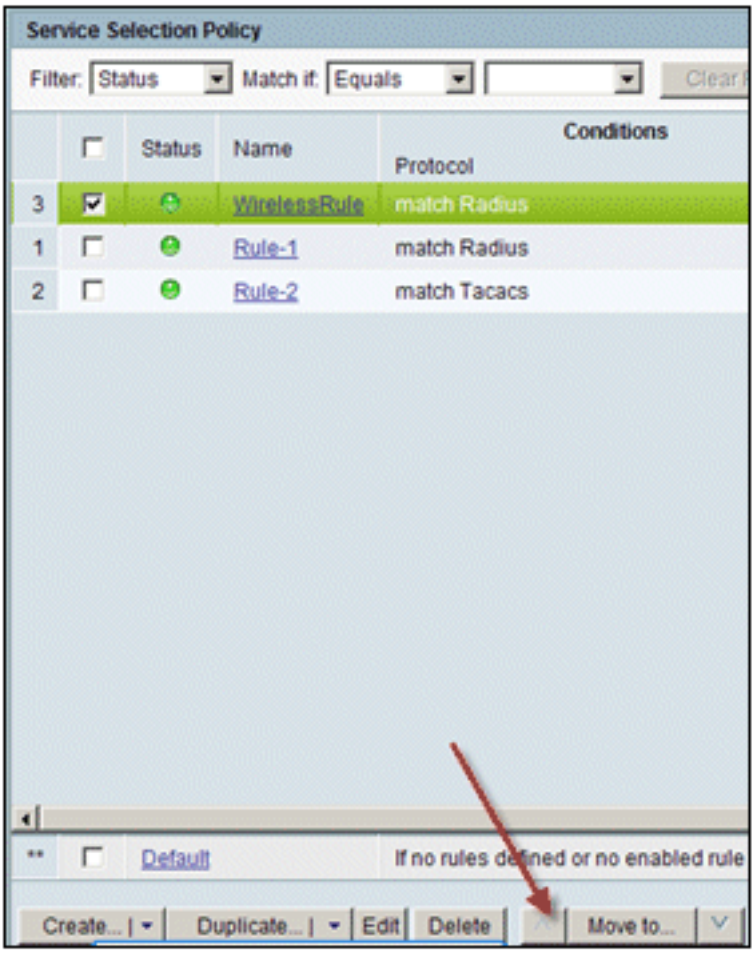




3. Kies **Straal** en klik op **OK**.
4. Kies onder Resultaten **WirelessAD** voor service (gemaakt in de vorige



stap).
5. Zodra de nieuwe draadloze regel is gemaakt, kiest u deze regel en **verplaatst u** deze naar de bovenkant, die de eerste regel zal zijn om draadloze radiusverificatie te identificeren met



Active Directory.

CLIENTconfiguratie voor PEAP met Windows Zero Touch

In ons voorbeeld, CLIENT is een computer die Windows XP Professional met SP in werking stelt die als draadloze cliënt dienst doet en toegang tot Intranet middelen door draadloze AP verkrijgt.

Voltooi de procedures in deze sectie om CLIENT als draadloze client te configureren.

Een basisinstallatie en -configuratie uitvoeren

Voer de volgende stappen uit:

1. Sluit de CLIENT aan op het Intranet-netwerksegment met behulp van een Ethernet-kabel die is aangesloten op de hub.
2. Installeer op CLIENT Windows XP Professional met SP2 als een lid computer met de naam CLIENT van het domein demo.local.
3. Installeer Windows XP Professional met SP2. Dit moet worden geïnstalleerd om PEAP-ondersteuning te hebben.**Opmerking:** Windows Firewall wordt automatisch ingeschakeld in Windows XP Professional met SP2. Schakel de firewall niet uit.

De draadloze netwerkadapter installeren

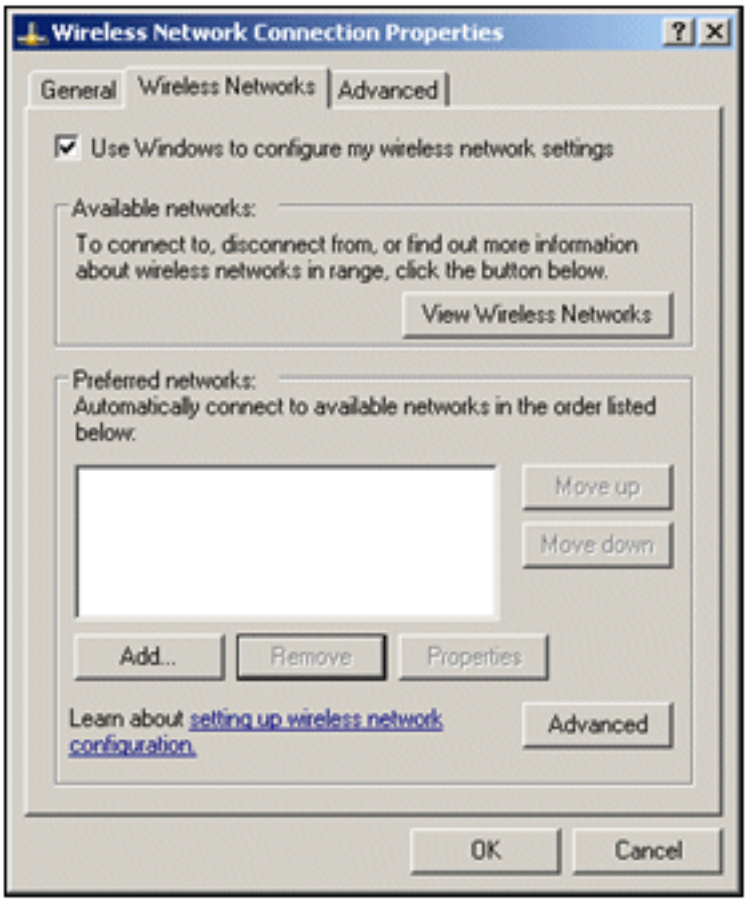
Voer de volgende stappen uit:

1. Sluit de CLIENTcomputer af.
2. Koppel de CLIENT-computer los van het intranet-netwerksegment.
3. Start de CLIENT-computer opnieuw en log vervolgens in met de lokale beheerdersaccount.
4. Installeer de draadloze netwerkadapter.**N.B.:** Installeer de configuratiesoftware van de fabrikant voor de draadloze adapter niet. Installeer de stuurprogramma's voor de draadloze netwerkadapter met de Wizard Hardware toevoegen. Ook, wanneer gevraagd, de CD voorzien door de fabrikant of een schijf met bijgewerkte stuurprogramma's voor gebruik met Windows XP Professional met SP2.

De draadloze netwerkverbinding configureren

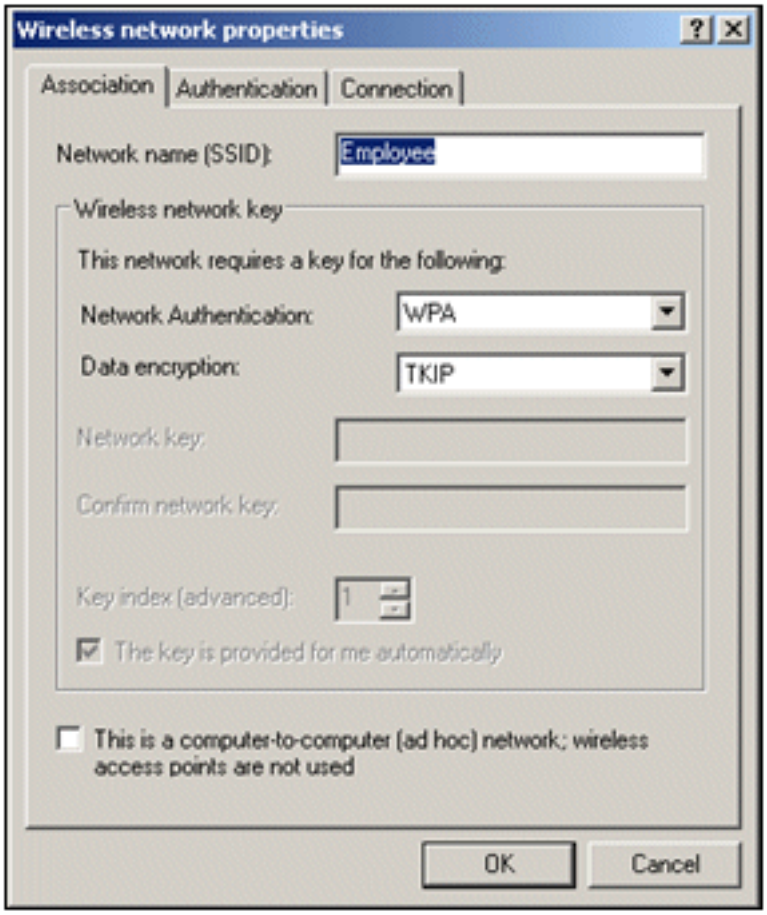
Voer de volgende stappen uit:

1. Log uit en log vervolgens in met de **WirelessUser**-account in het domein **demo.local**.
2. Kies **Start** > **Configuratiescherm**, dubbelklik op **Netwerkverbindingen** en klik met de rechtermuisknop op **Draadloze netwerkverbinding**.
3. Klik op **Eigenschappen**, ga naar het tabblad **Draadloze netwerken** en controleer of **Windows gebruiken om mijn draadloze netwerkinstellingen te configureren** is



ingeschakeld.

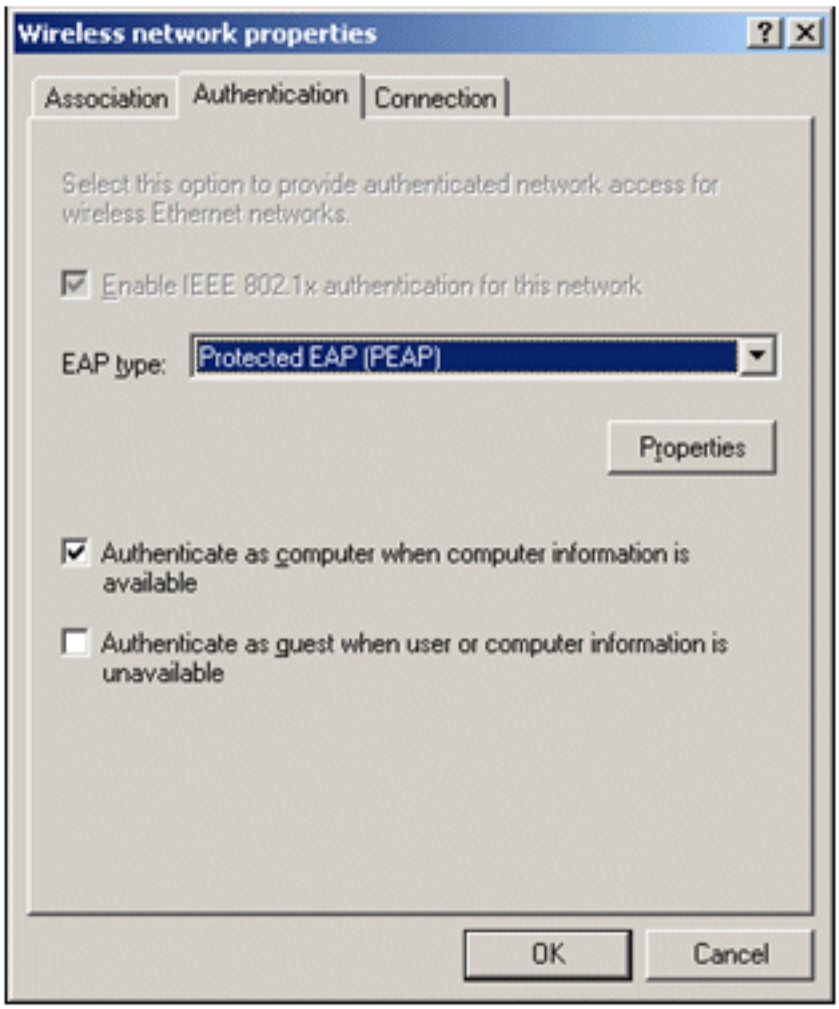
4. Klik op **Add** (Toevoegen).
5. Voer op het tabblad Koppeling *Werknemer* in het veld Netwerknaam (SSID) in.
6. Kies **WPA** voor de netwerkverificatie en zorg ervoor dat de gegevenscodering is ingesteld op



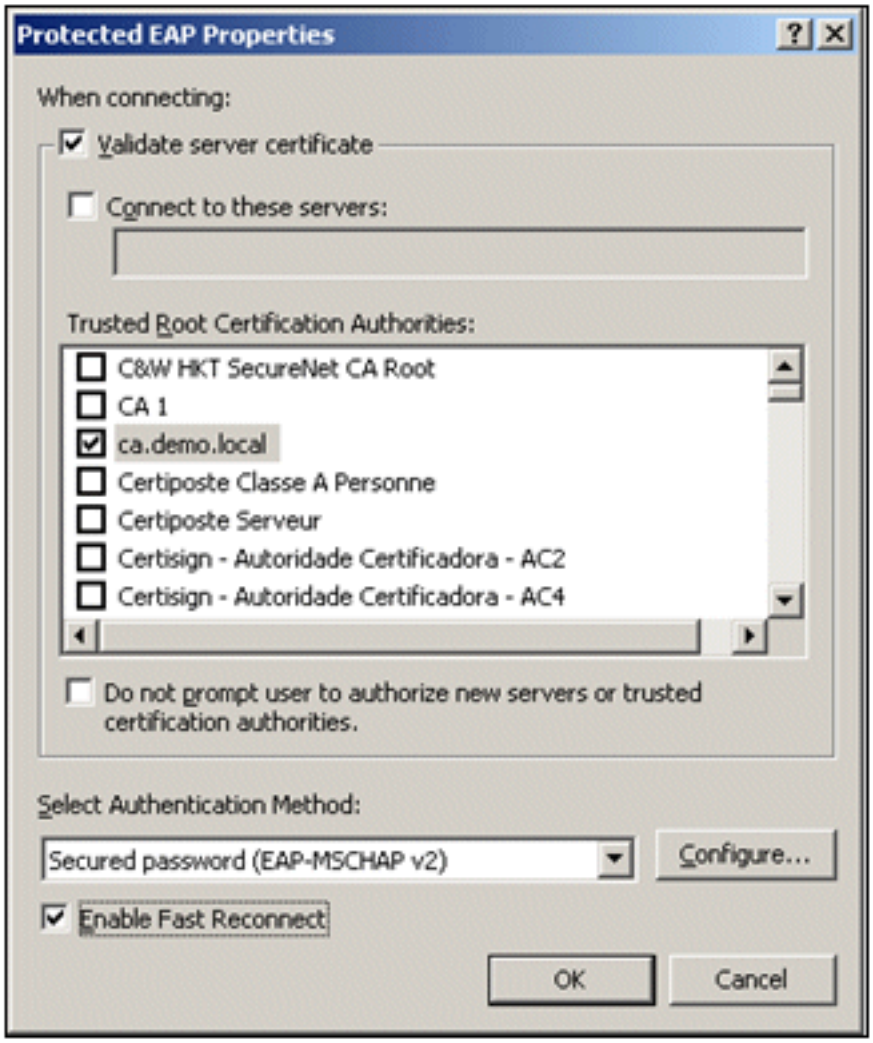
TKIP.

7. Klik op het tabblad **verificatie**.

8. Valideren dat het EAP-type is geconfigureerd voor het gebruik van **Protected EAP (PEAP)**. Als dit niet het geval is, kiest u de optie in het vervolgkeuzemenu.
9. Als u wilt dat de machine wordt geverifieerd voorafgaand aan de aanmelding (waardoor inlogscripts of groepsbeleiddrukken kunnen worden toegepast), controleer dan **Verifiëren als computer wanneer computerinformatie beschikbaar**



is.
10. Klik op **Eigenschappen**.
11. Aangezien PEAP verificatie van de server door de client omvat, moet u ervoor zorgen dat het **servercertificaat valideren** is gecontroleerd. Zorg er ook voor dat de CA die het ACS-certificaat heeft afgegeven, is gecontroleerd in het menu Trusted Root Certification Authorities.
12. Kies **beveiligd wachtwoord (EAP-MSCHAP v2)** onder Verificatiemethode omdat het voor interne verificatie wordt



gebruikt.

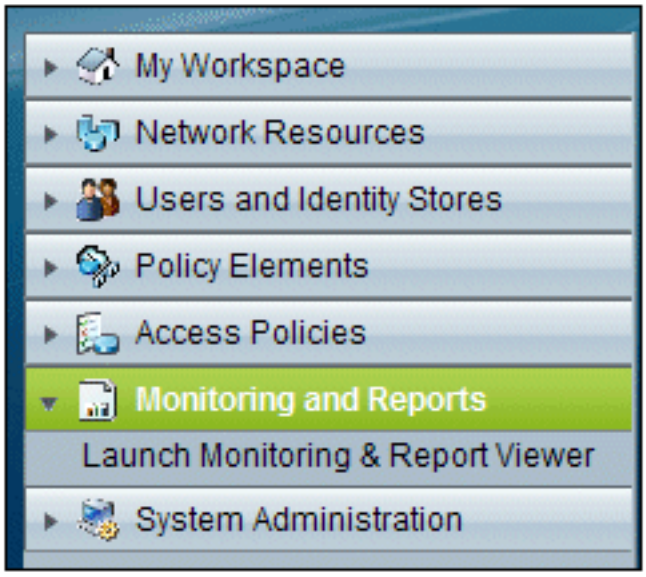
13. Zorg dat het selectievakje **Snel opnieuw verbinden inschakelen** is ingeschakeld. Klik vervolgens driemaal op **OK**.
14. Klik met de rechtermuisknop op het pictogram voor de draadloze netwerkverbinding in het systeemvak en klik vervolgens op **Beschikbare draadloze netwerken weergeven**.
15. Klik op het draadloze netwerk van de werknemer en klik vervolgens op **Verbinden**. De draadloze client toont **Connected** (**Verbonden)** als de verbinding succesvol is uitgevoerd.

16. Controleer, nadat de verificatie is geslaagd, de TCP/IP-configuratie voor de draadloze adapter met behulp van Network Connections. Het moet een adresbereik hebben van 10.0.20.100-10.0.20.200 van de DHCP-scope of de scope die is gecreëerd voor de draadloze CorpNet-clients.
17. Om de functionaliteit te testen, opent u een browser en bladert u naar **http://10.0.10.10** (of het IP-adres van de CA-server).

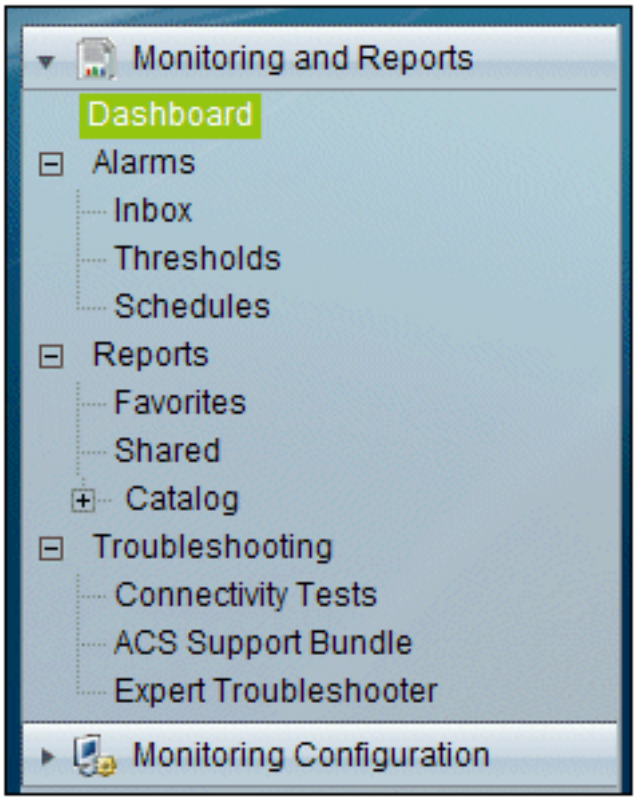
Probleemoplossing voor draadloze verificatie met ACS

Voer de volgende stappen uit:

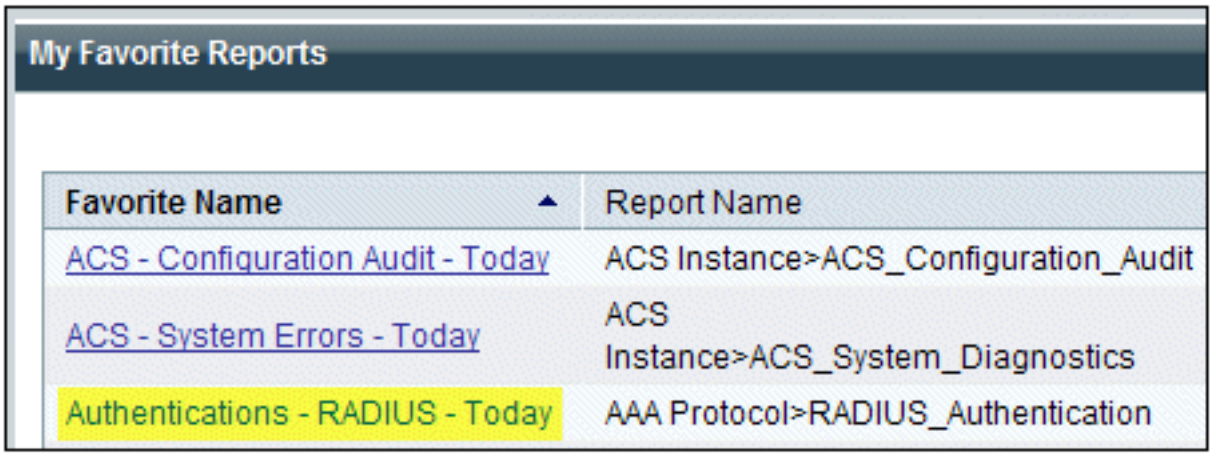
1. Ga naar **ACS > Monitoring and Reports**, en klik op **Start Monitoring & Report Viewer**.



2. Er wordt nu een apart ACS-venster geopend. Klik op **Dashboard**.

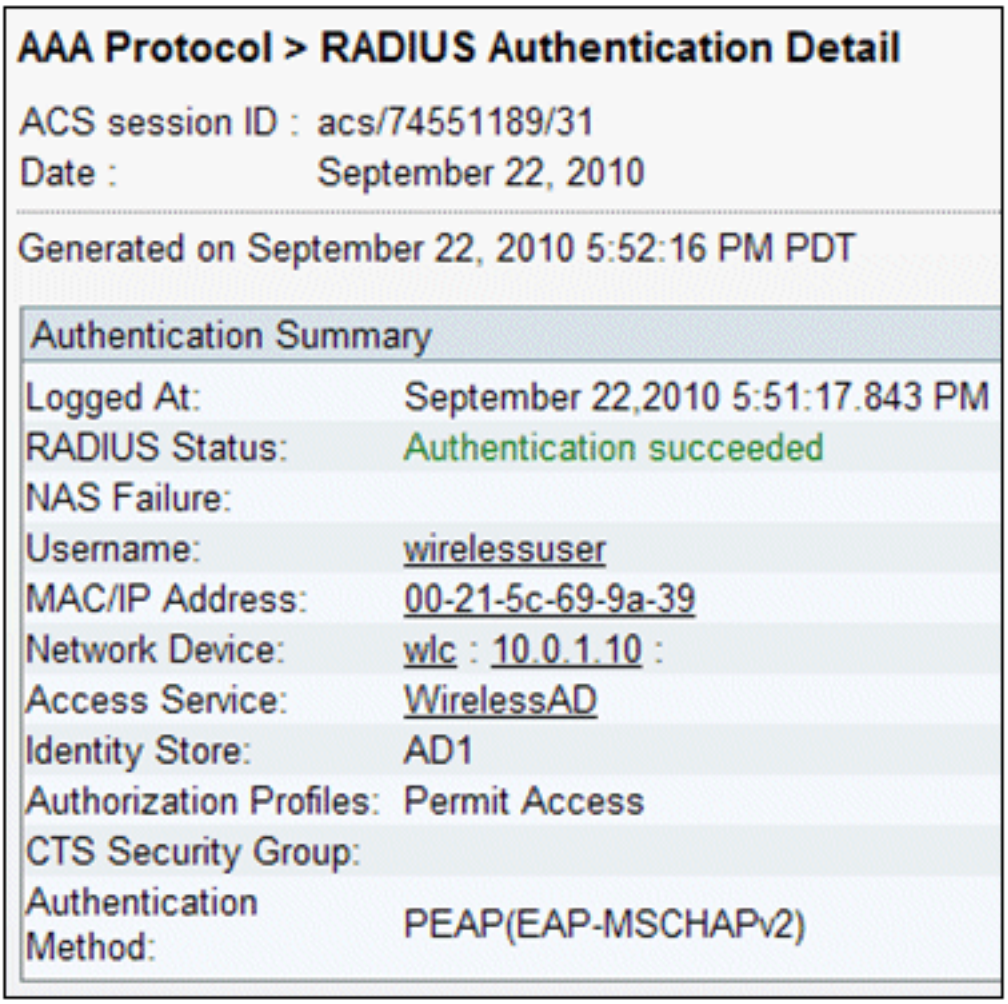


3. Klik in het gedeelte Mijn favoriete rapporten op **Verificaties - RADIUS - vandaag**.

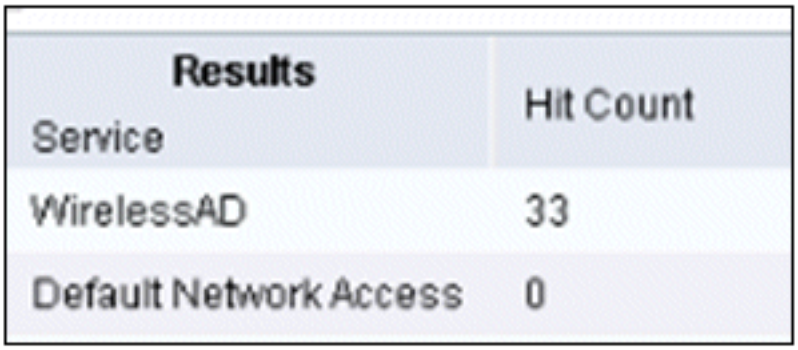


4. Een logbestand toont alle RADIUS-verificaties als Pass of Fail. Klik binnen een gelogd item op het **vergrootglaspictogram** in de kolom Details.

5. Het RADIUS-verificatiedetail biedt veel informatie over de geregistreerde pogingen.



6. ACS Service Hit Count kan een overzicht geven van pogingen die overeenkomen met de regel(s) die in ACS worden gemaakt. Ga naar **ACS > Toegangsbeleid > Toegangsservices** en klik op **Regels voor servicesselectie**.



Results Service	Hit Count
WirelessAD	33
Default Network Access	0

PEAP-verificatie mislukt met ACS-server

Wanneer uw client PEAP-verificatie met een ACS-server mislukt, controleert u of u de foutmelding van de `NAS-gedupliceerde verificatiepoging` vindt in de optie **Mislukte pogingen** onder het menu **Rapport en Activiteit** van de ACS.

U ontvangt deze foutmelding wanneer Microsoft Windows XP SP2 op de clientcomputer is geïnstalleerd en Windows XP SP2 verificeert tegen een server van een derde partij die geen Microsoft IAS-server is. Met name Cisco RADIUS-server (ACS) gebruikt een andere methode om het type Extensible Authentication Protocol Type:Length:Value-indeling (EAP-TLV) te berekenen dan de methode die Windows XP gebruikt. Microsoft heeft dit als een defect in de XP SP2-supplicant geïdentificeerd.

Neem voor een Hotfix contact op met Microsoft en raadpleeg het artikel PEAP-verificatie niet succesvol is wanneer u verbinding maakt met een RADIUS-server van derden . Het onderliggende probleem is dat aan de clientzijde, met het Windows-hulpprogramma, de optie Fast Reconconnect standaard is uitgeschakeld voor PEAP. Deze optie is standaard ingeschakeld aan de serverkant (ACS). Om dit probleem op te lossen, deselecteert u de optie Fast Reconconnect op de ACS-server (onder Globale systeemopties). U kunt ook de optie Fast Reconconnect aan de clientzijde inschakelen om het probleem op te lossen.

Voer deze stappen uit om Fast Recconnect in te schakelen op de client die Windows XP uitvoert met behulp van Windows Utility:

1. Kies **Start > Instellingen > Configuratiescherm**.
2. Dubbelklik op het pictogram **Network Connections**.
3. Klik met de rechtermuisknop op het pictogram **Draadloze netwerkverbinding** en klik vervolgens op **Eigenschappen**.
4. Klik op het tabblad **Draadloze netwerken**.
5. Kies de optie **Windows gebruiken om mijn draadloze netwerkinstellingen te configureren** om Windows in staat te stellen de clientadapter te configureren.
6. Als u al een SSID hebt geconfigureerd, kies dan de SSID en klik op **Eigenschappen**. Als dit niet het geval is, klikt u op **Nieuw** om een nieuw WLAN toe te voegen.
7. Voer de SSID in onder het tabblad Koppeling. Zorg ervoor dat de Netwerkverificatie **Open** is en dat de Gegevenscodering is ingesteld op **WEP**.
8. Klik op **Verificatie**.
9. Kies de **optie IEEE 802.1x-verificatie inschakelen voor deze** netwerkoptie.

10. Kies **PEAP** als EAP-type en klik op **Eigenschappen**.
11. Kies de optie **Snel opnieuw verbinden inschakelen** onder aan de pagina.

Gerelateerde informatie

- PEAP onder Unified Wireless Networks met ACS 4.0 en Windows 2003
- Configuratie-voorbeeld van Cisco draadloze LAN-controller (WLC) en Cisco ACS 5.x (TACACS+) voor webverificatie
- Installatie- en upgrade-handleiding voor Cisco Secure Access Control System 5.1
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

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