Konfigurieren von NPS, Wireless LAN Controllern und drahtlosen Netzwerken

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie das PEAP mit MS-CHAP-Authentifizierung und Microsoft NPS als RADIUS-Server konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse der Windows 2008-Installation
- Kenntnisse der Cisco Controller-Installation

Stellen Sie vor der Konfiguration sicher, dass die folgenden Anforderungen erfüllt sind:

- Installieren Sie Microsoft Windows Server 2008 auf jedem der Server im Testlabor.
- Aktualisieren Sie alle Service Packs.
- Einbau der Controller und Lightweight Access Points (LAPs)
- Konfigurieren Sie die neuesten Software-Updates.

Informationen zur Erstinstallation und -konfiguration der Cisco Wireless Controller der Serie 5508 finden Sie im Installationshandbuch für Cisco Wireless Controller der Serie 5500.

Anmerkung: Dieses Dokument soll den Lesern ein Beispiel für die Konfiguration geben, die auf einem Microsoft-Server für die PEAP-MS-CHAP-Authentifizierung erforderlich ist. Die in diesem Dokument vorgestellte Microsoft Windows-Serverkonfiguration wurde in der Übung getestet und funktioniert wie erwartet. Wenn Sie Probleme mit der Konfiguration haben, wenden Sie sich an Microsoft. Das Cisco Technical Assistance Center (TAC) unterstützt keine Microsoft Windows-Serverkonfiguration.

Microsoft Windows 2008 Installations- und Konfigurationshandbücher finden Sie auf Microsoft Tech Net.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco 5508 Wireless Controller mit Firmware-Version 7.4
- Cisco Aironet 3602 Access Point (AP) mit LWAPP (Lightweight Access Point Protocol)
- Windows 2008 Enterprise Server mit installiertem NPS, CA (Certificate Authority), DHCP (Dynamic Host Control Protocol) und DNS (Domain Name System)
- Microsoft Windows 7-Client-PC
- Cisco Catalyst Switches der Serie 3560

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

Dieses Dokument enthält eine Beispielkonfiguration für das Protected Extensible Authentication Protocol (PEAP) mit dem Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) Version 2 für die Authentifizierung in einem Cisco Unified Wireless-Netzwerk mit dem Microsoft Network Policy Server (NPS) als RADIUS-Server.

PEAP-Übersicht

PEAP verwendet Transport Level Security (TLS), um einen verschlüsselten Kanal zwischen einem authentifizierten PEAP-Client, z. B. einem Wireless-Laptop, und einem PEAP-Authentifikator, z. B. Microsoft NPS oder einem beliebigen RADIUS-Server, zu erstellen. PEAP gibt keine Authentifizierungsmethode an, bietet jedoch zusätzliche Sicherheit für andere Extensible Authentication Protocols (EAPs) wie EAP-MS-CHAP v2, die über den von PEAP bereitgestellten TLS-verschlüsselten Kanal betrieben werden können. Der PEAP-Authentifizierungsprozess besteht aus zwei Hauptphasen.

PEAP Phase 1: TLS-verschlüsselter Kanal

Der Wireless-Client wird mit dem Access Point verknüpft. Eine IEEE 802.11-basierte Zuordnung bietet eine Authentifizierung mit offenem System oder gemeinsam genutztem Schlüssel, bevor eine sichere Zuordnung zwischen dem Client und dem Access Point erstellt wird. Nachdem die IEEE 802.11-basierte Verbindung zwischen dem Client und dem Access Point hergestellt wurde, wird die TLS-Sitzung mit dem Access Point ausgehandelt. Nachdem die Authentifizierung zwischen dem Wireless-Client und dem NPS erfolgreich abgeschlossen wurde, wird die TLS-Sitzung zwischen dem Client und dem NPS ausgehandelt. Der in dieser Verhandlung abgeleitete Schlüssel wird zur Verschlüsselung der gesamten nachfolgenden Kommunikation verwendet.

PEAP Phase 2: EAP-authentifizierte Kommunikation

Die EAP-Kommunikation, die auch die EAP-Verhandlung umfasst, findet innerhalb des von PEAP innerhalb der ersten Stufe des PEAP-Authentifizierungsprozesses erstellten TLS-Kanals statt. Der NPS authentifiziert den Wireless-Client mit EAP-MS-CHAP v2. Der LAP und der Controller leiten nur Nachrichten zwischen dem Wireless-Client und dem RADIUS-Server weiter. Der Wireless LAN Controller (WLC) und das LAP können diese Nachrichten nicht entschlüsseln, da sie nicht den TLS-Endpunkt bilden.

Die RADIUS-Nachrichtensequenz für einen erfolgreichen Authentifizierungsversuch (bei dem der Benutzer gültige kennwortbasierte Anmeldeinformationen mit PEAP-MS-CHAP v2 angegeben hat) ist:

1. Der NPS sendet eine Identitätsanforderungsnachricht an den Client: EAP-Anforderung/Identität.
2. Der Client antwortet mit einer Identitätsantwort: EAP-Antwort/Identität
3. Der NPS sendet eine MS-CHAP v2-Abfragenachricht: EAP-Request/EAP-Type=EAP MS-CHAP-V2 (Herausforderung).

4. Der Client antwortet mit einer MS-CHAP v2-Herausforderung und Antwort: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response).
5. Der NPS sendet ein MS-CHAP v2-Erfolgspaket zurück, wenn der Server den Client erfolgreich authentifiziert hat: EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (Erfolg).
6. Der Client antwortet mit einem MS-CHAP v2-Erfolgspaket, wenn der Client den Server erfolgreich authentifiziert hat: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Erfolgreich).
7. Der NPS sendet einen TLV (EAP-type-length-value), der auf eine erfolgreiche Authentifizierung hinweist.
8. Der Client antwortet mit einer EAP-TLV-Statuserfolgsmeldung.
9. Der Server schließt die Authentifizierung ab und sendet eine EAP-Success-Nachricht im Nur-Text-Format. Wenn VLANs für die Client-Isolierung bereitgestellt werden, sind die VLAN-Attribute in dieser Meldung enthalten.

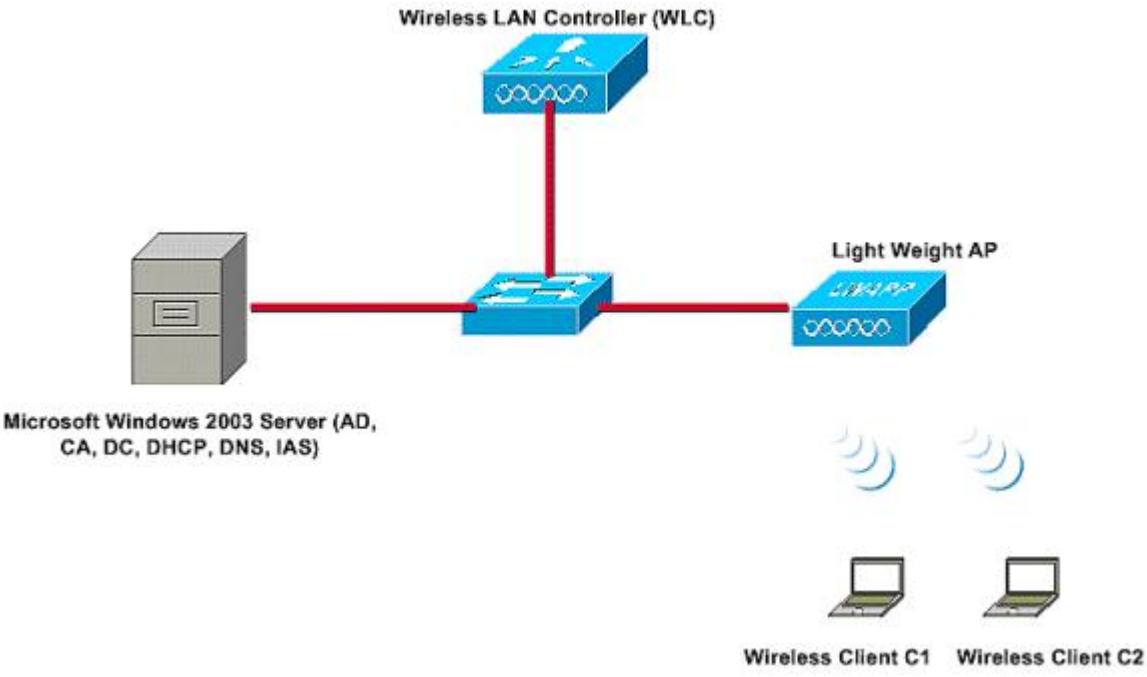
Konfigurieren

In diesem Abschnitt werden die Informationen zur Konfiguration von PEAP-MS-CHAP v2 angezeigt.

Anmerkung: Weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen erhalten Sie mit dem Befehlsnachschlachtool. Nur registrierte Cisco Benutzer können auf interne Tools und Informationen von Cisco zugreifen.

Netzwerkdiagramm

Bei dieser Konfiguration wird folgende Netzwerkkonfiguration verwendet:



Netzwerkdiagramm

In diesem Setup führt ein Microsoft Windows 2008-Server die folgenden Rollen aus:

- Domänencontroller für die Domäne
- DHCP/DNS-Server
- CA-Server
- NPS - zur Authentifizierung der Wireless-Benutzer
- Active Directory - zur Verwaltung der Benutzerdatenbank

Der Server stellt über einen Layer-2-Switch, wie dargestellt, eine Verbindung zum kabelgebundenen Netzwerk her. Der WLC und der registrierte LAP stellen ebenfalls über den Layer-2-Switch eine Verbindung zum Netzwerk her.

Die Wireless-Clients verwenden die Wi-Fi Protected Access 2 (WPA2) - PEAP-MS-CHAP v2-Authentifizierung, um eine Verbindung mit dem Wireless-Netzwerk herzustellen.

Konfigurationen

Das Ziel dieses Beispiels ist die Konfiguration des Microsoft 2008-Servers, des Wireless LAN Controllers und des Lightweight AP zur Authentifizierung der Wireless Clients mit PEAP-MS-CHAP v2-Authentifizierung. Dieser Prozess besteht aus drei Hauptschritten:

1. Konfigurieren Sie Microsoft Windows 2008 Server.
2. Konfigurieren des WLC und der APs mit geringem Gewicht
3. Konfigurieren der Wireless-Clients

Konfigurieren von Microsoft Windows 2008 Server

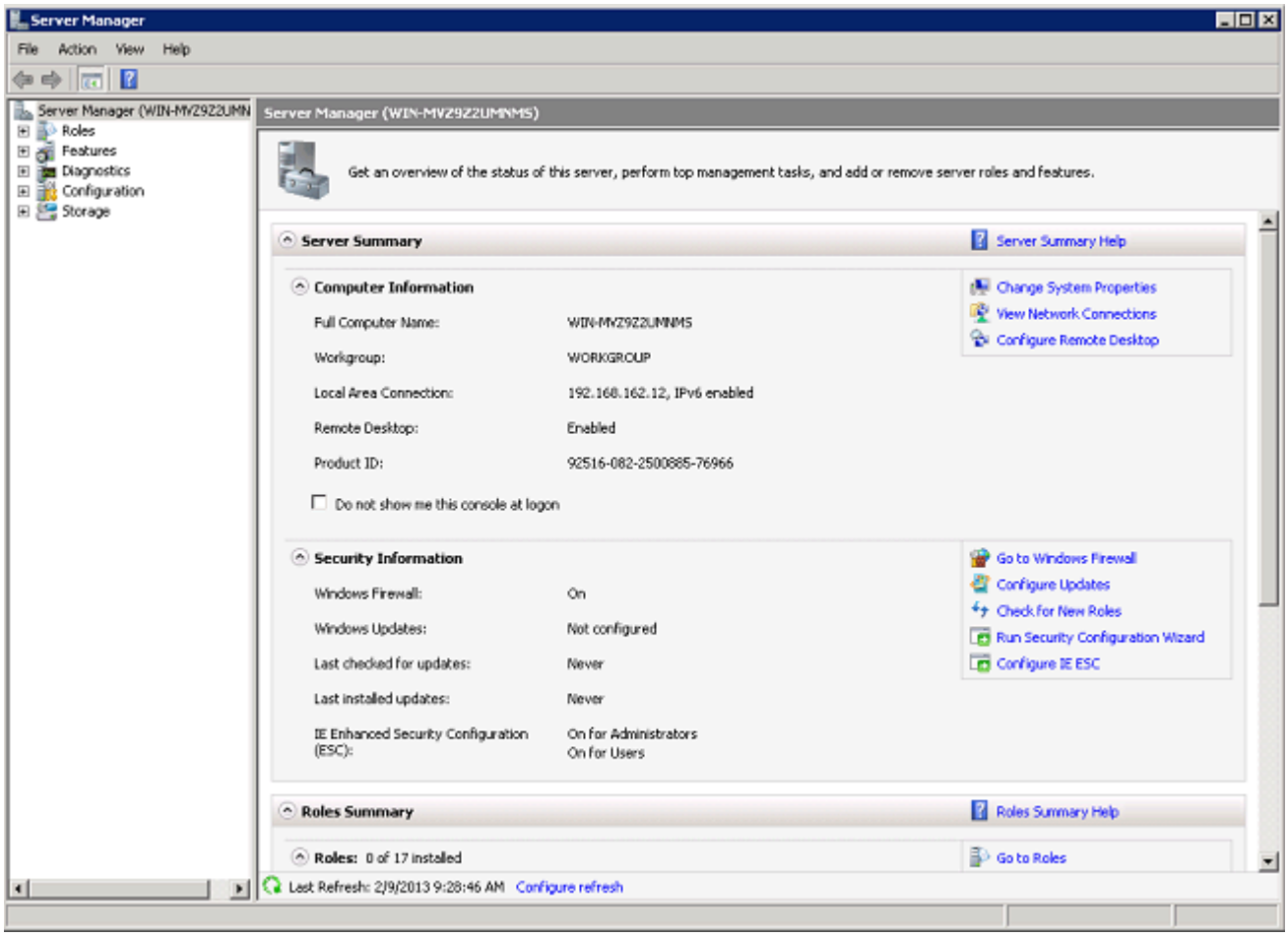
In diesem Beispiel umfasst eine vollständige Konfiguration des Microsoft Windows 2008-Servers die folgenden Schritte:

1. Konfigurieren Sie den Server als Domänencontroller.
2. Installieren und Konfigurieren von DHCP-Services
3. Installation und Konfiguration des Servers als CA-Server.
4. Verbinden Sie Clients mit der Domäne.
5. Installation des NPS
6. Installieren eines Zertifikats
7. Konfigurieren des NPS für die PEAP-Authentifizierung
8. Hinzufügen von Benutzern zum Active Directory

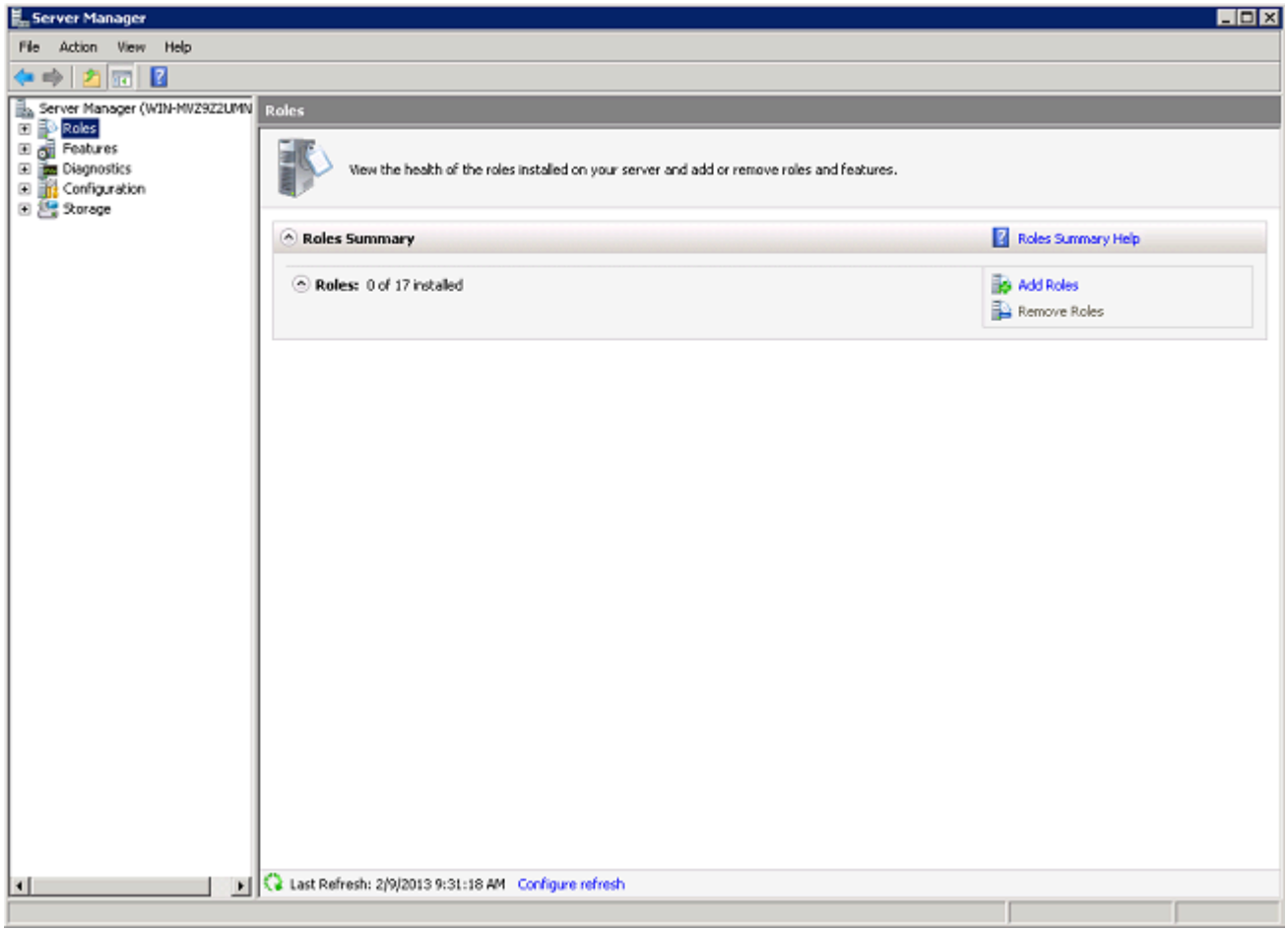
Konfigurieren von Microsoft Windows 2008 Server als Domänencontroller

Führen Sie die folgenden Schritte aus, um den Microsoft Windows 2008-Server als Domänencontroller zu konfigurieren:

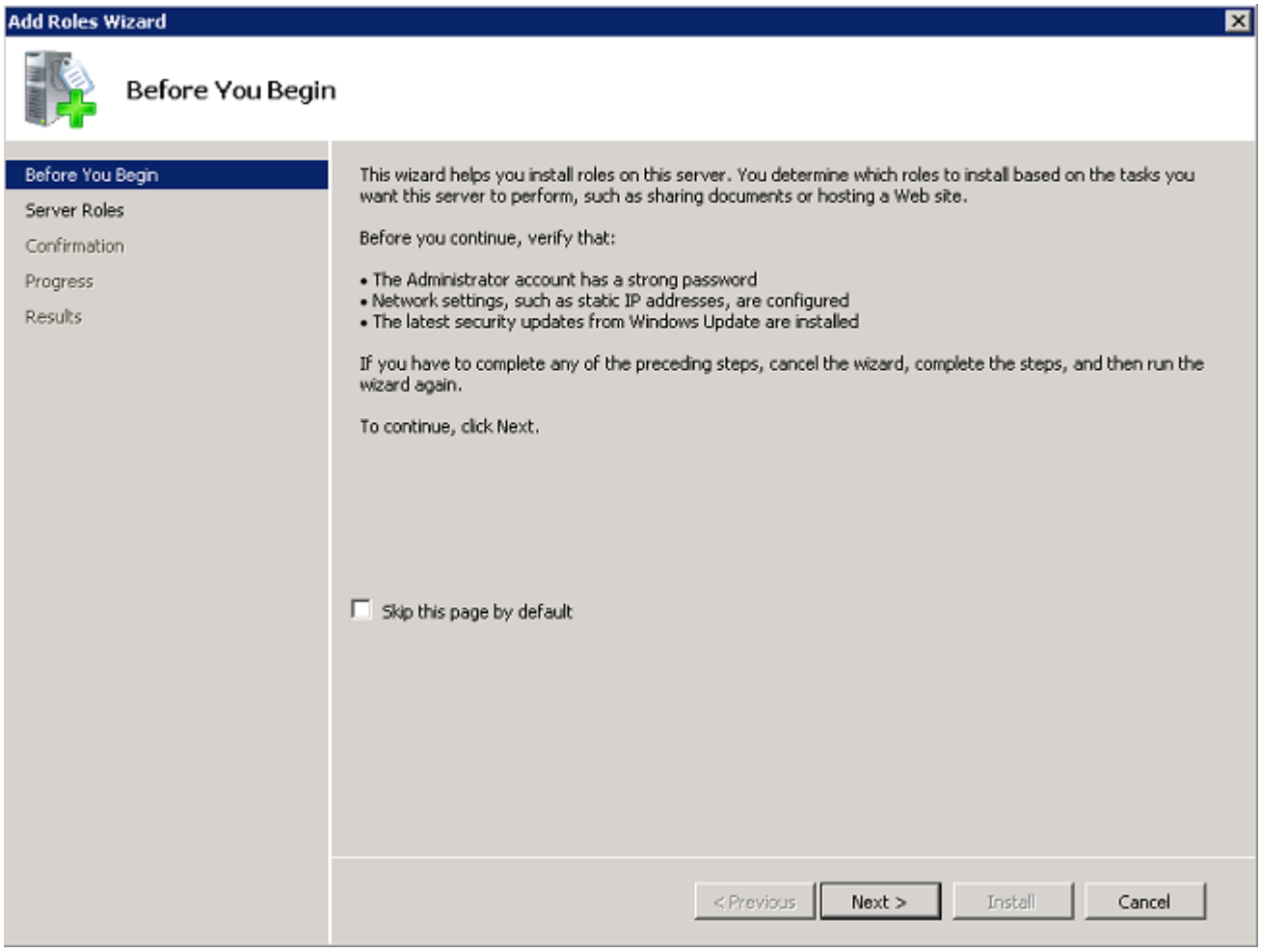
1. Klicken Sie auf Start> Server Manager.



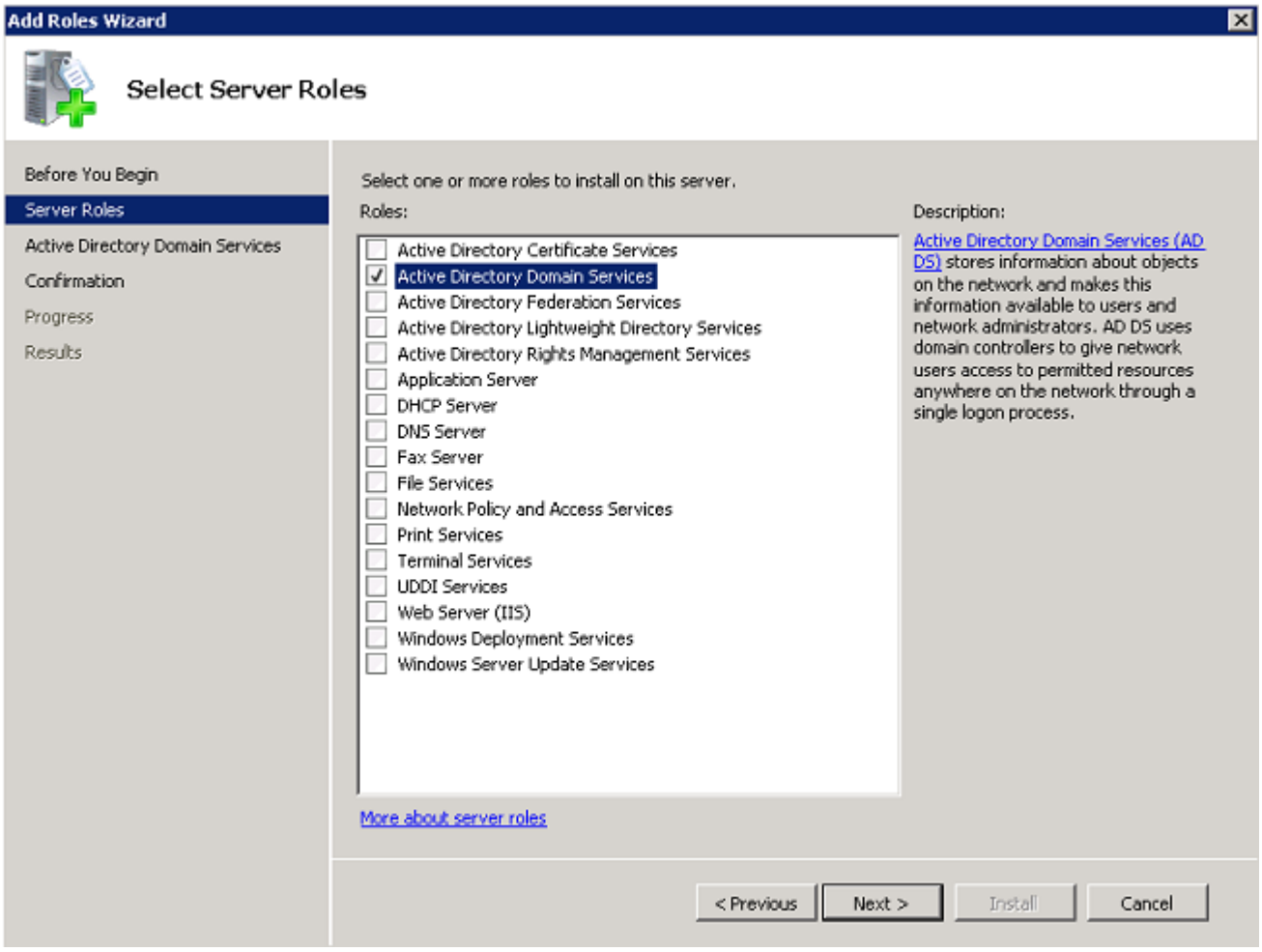
2. Klicken Sie auf Rollen > Rollen hinzufügen.



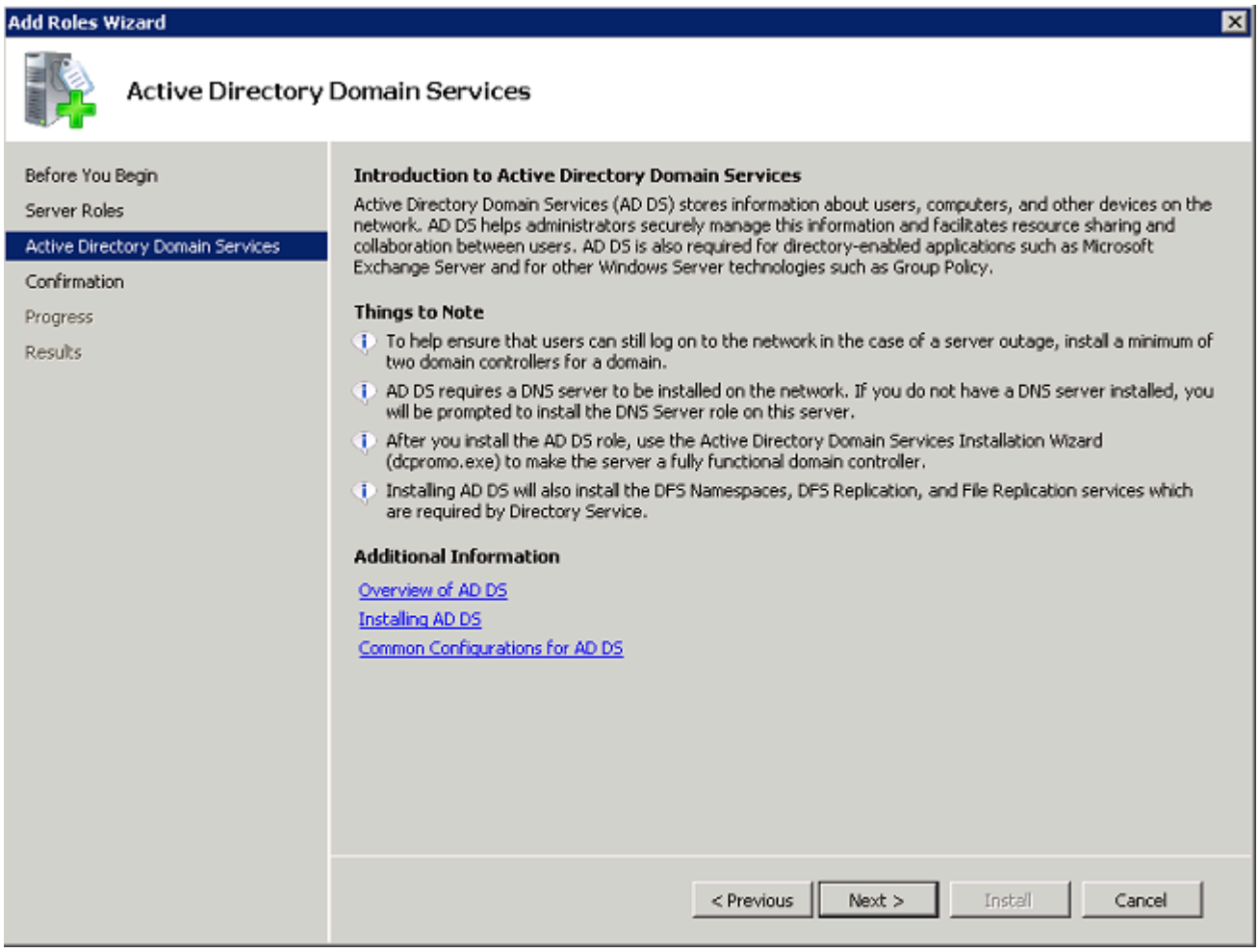
3. Klicken Sie auf Next (Weiter).



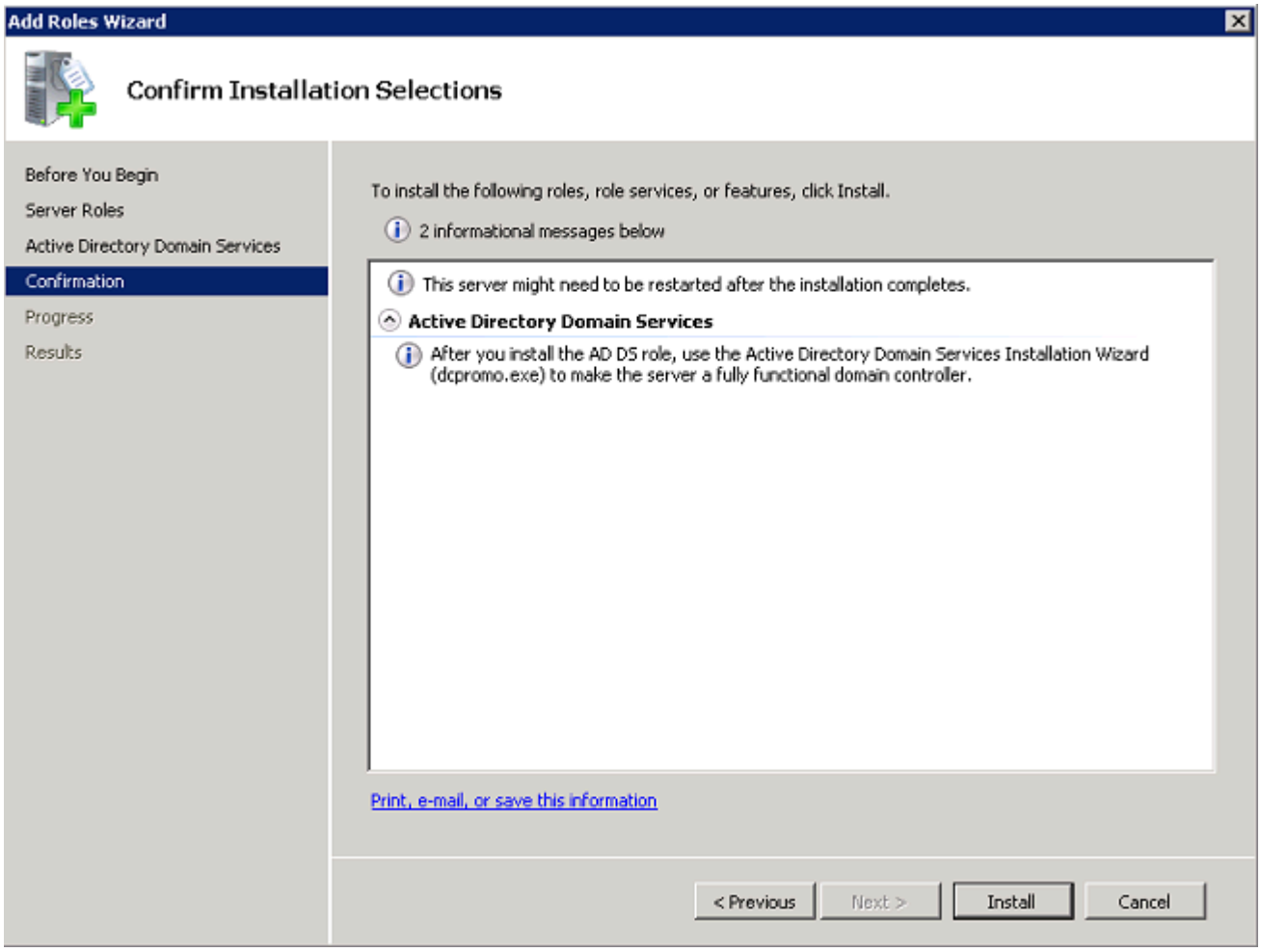
4. Wählen Sie den Dienst Active Directory-Domänendienste aus, und klicken Sie auf Weiter.



5. Überprüfen Sie die Einführung in die Active Directory-Domänendienste, und klicken Sie auf Weiter.

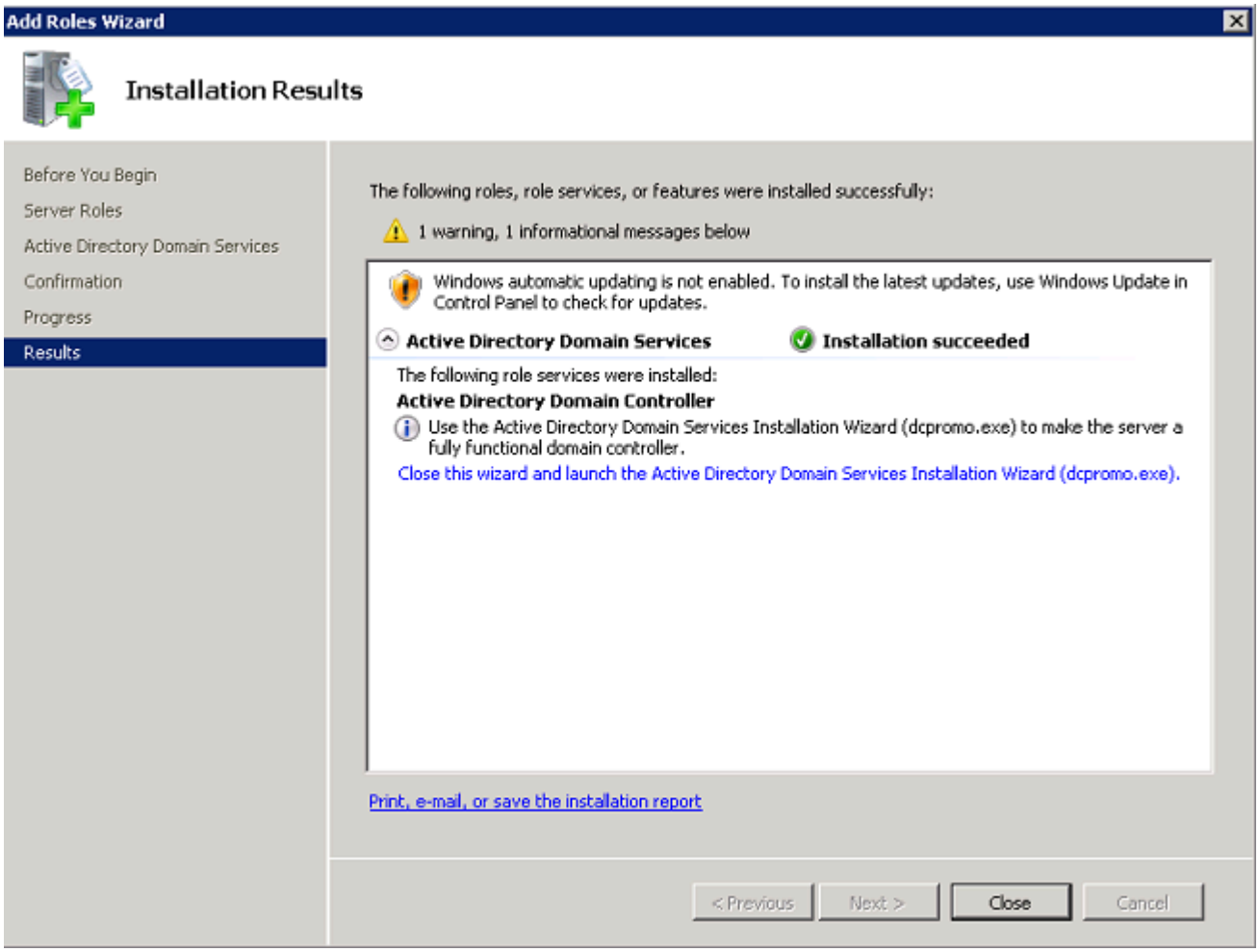


6. Klicken Sie auf Installieren, um die Installation zu starten.

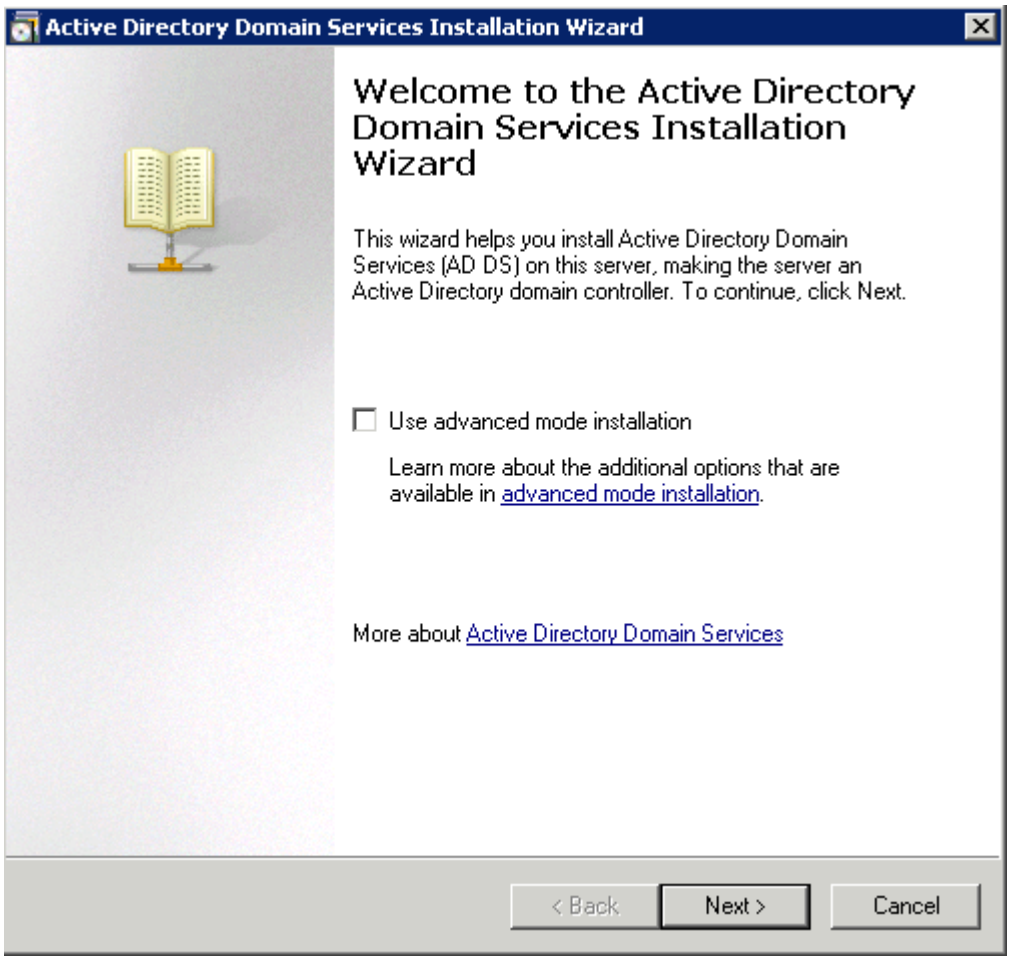


Die Installation wird fortgesetzt und abgeschlossen.

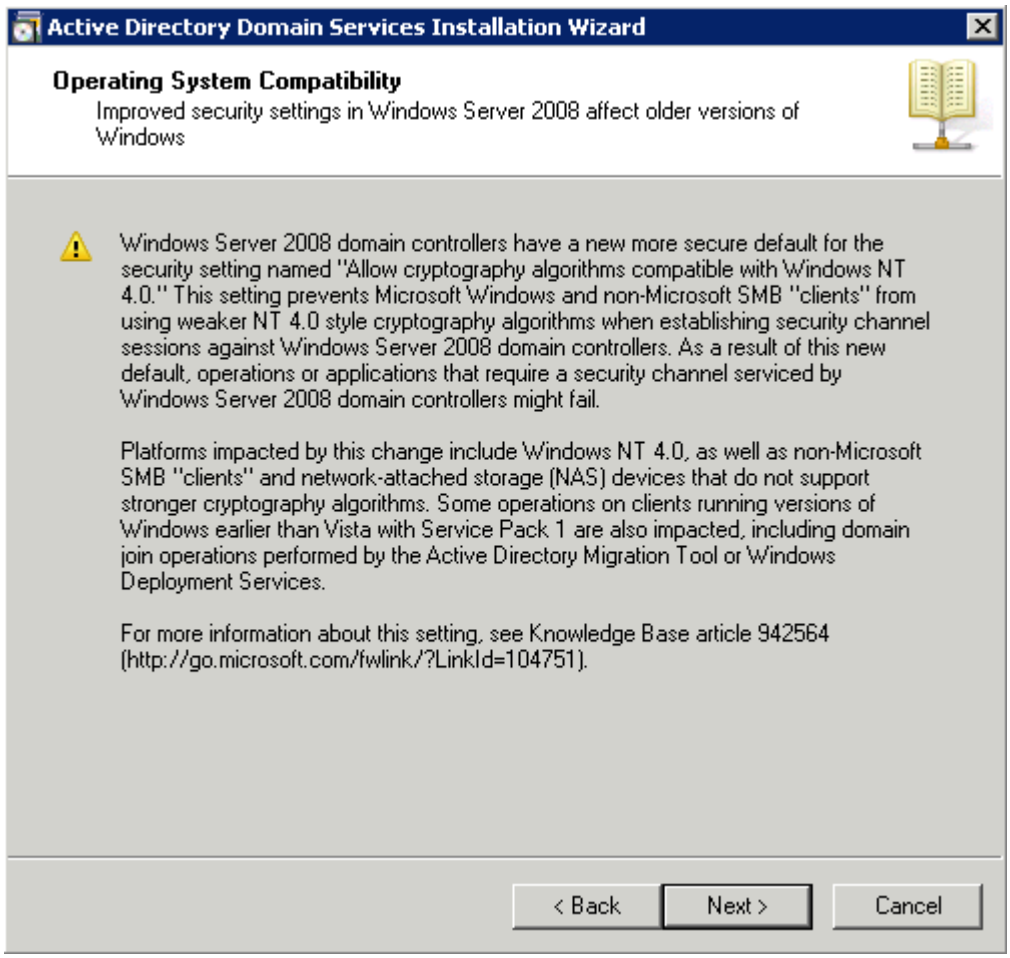
7. Klicken Sie auf Diesen Assistenten schließen, und starten Sie den Assistenten zum Installieren der Active Directory-Domänendienste (dcpromo.exe), um die Installation und Konfiguration von Active Directory fortzusetzen.



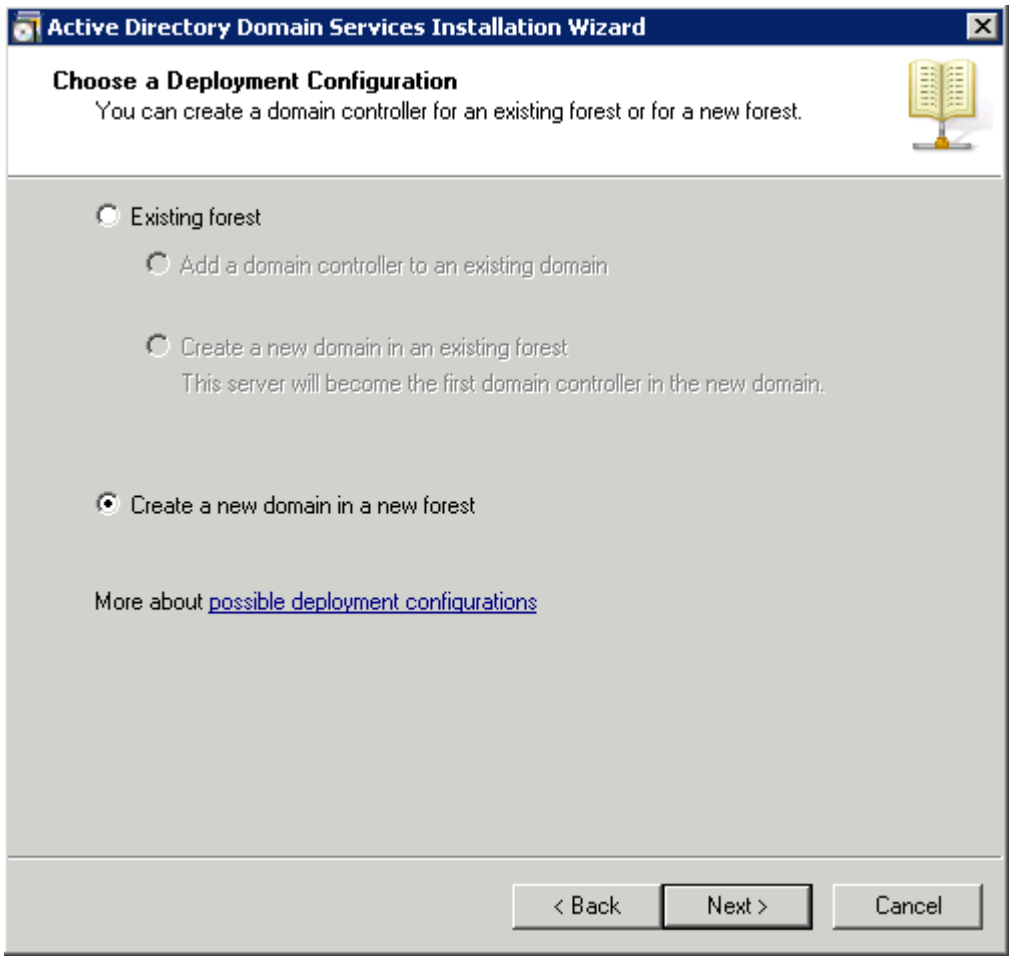
8. Klicken Sie auf Weiter, um den Assistenten zum Installieren der Active Directory-Domänendienste auszuführen.



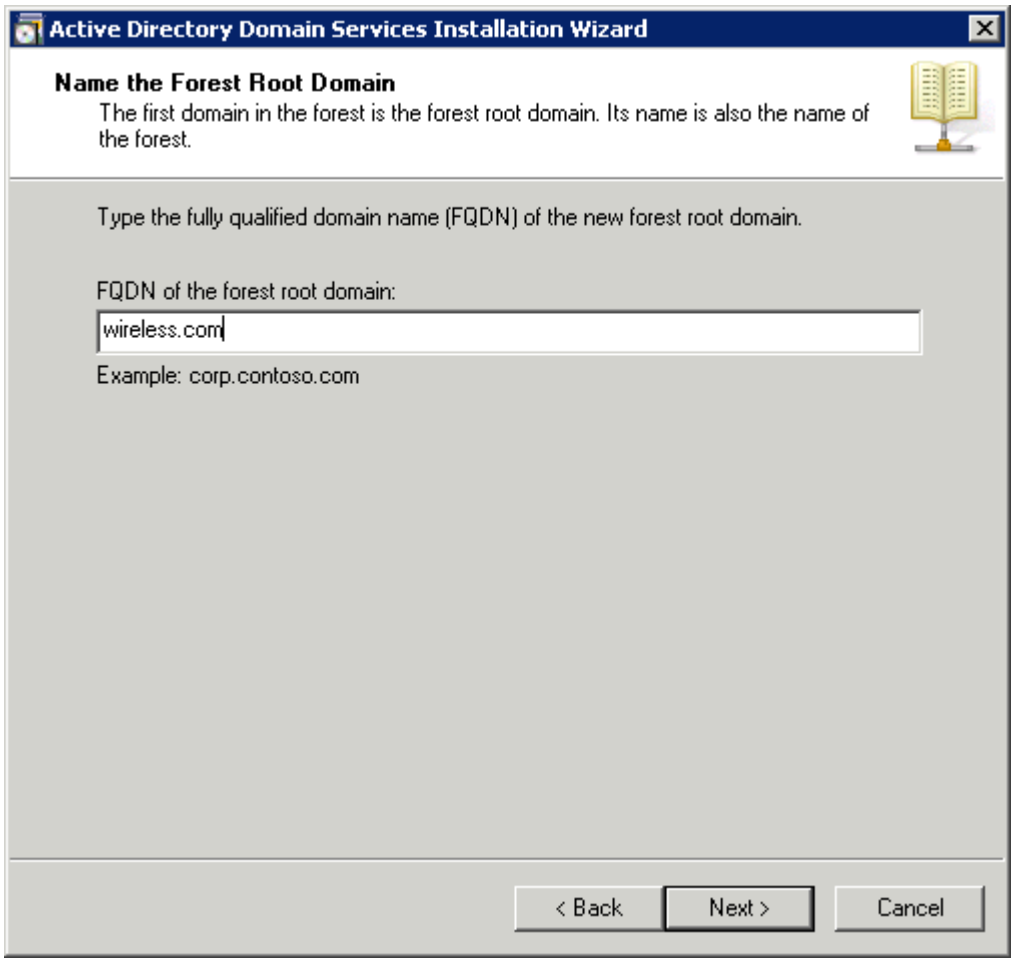
9. Überprüfen Sie die Informationen zur Betriebssystemkompatibilität, und klicken Sie auf Weiter.



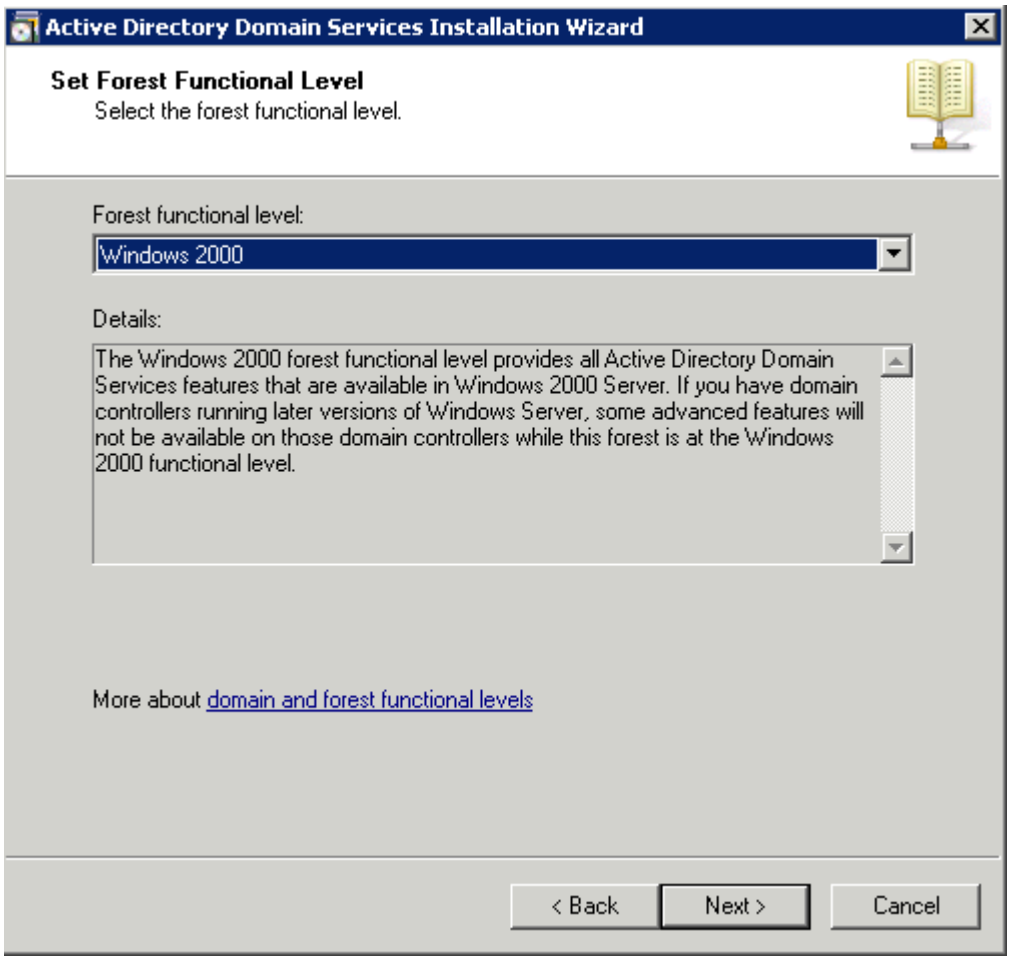
10. Klicken Sie auf Eine neue Domäne in einer neuen Gesamtstruktur erstellen > Weiter, um eine neue Domäne zu erstellen.



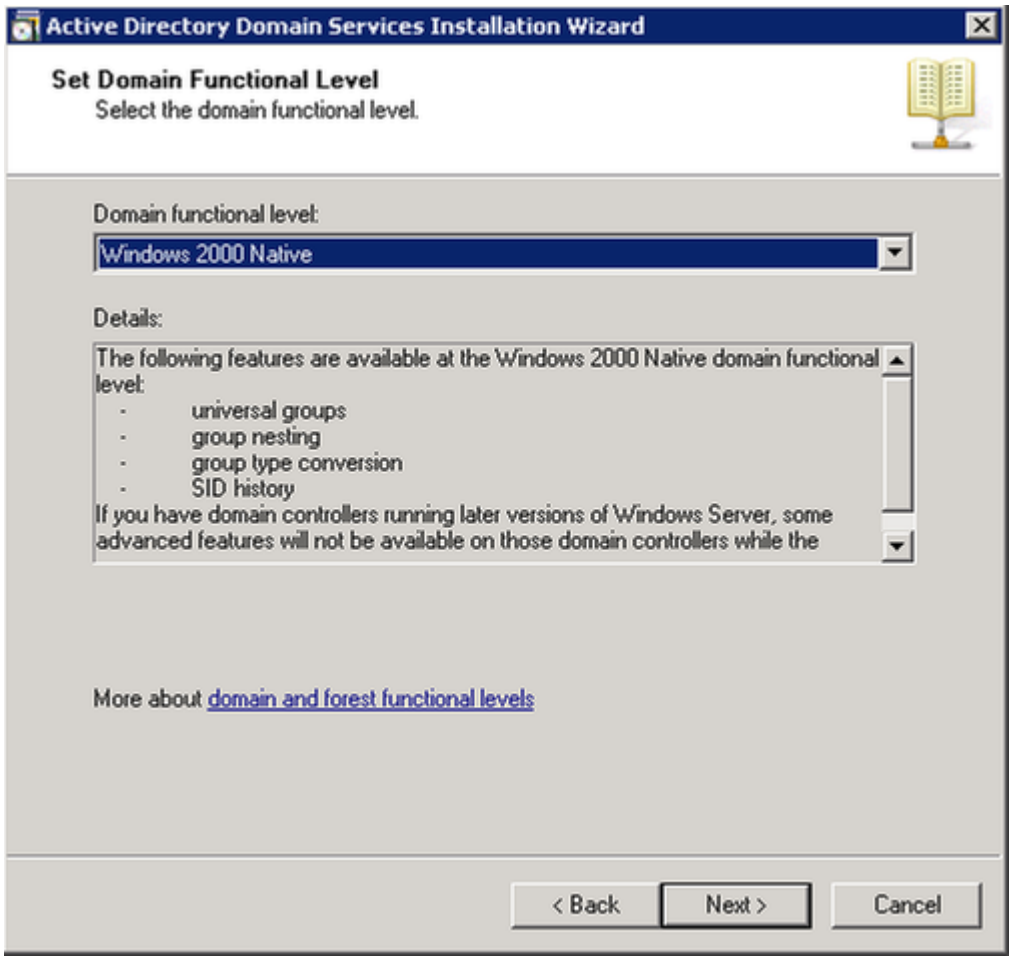
11. Geben Sie den vollständigen DNS-Namen für die neue Domäne ein, und klicken Sie auf Weiter.



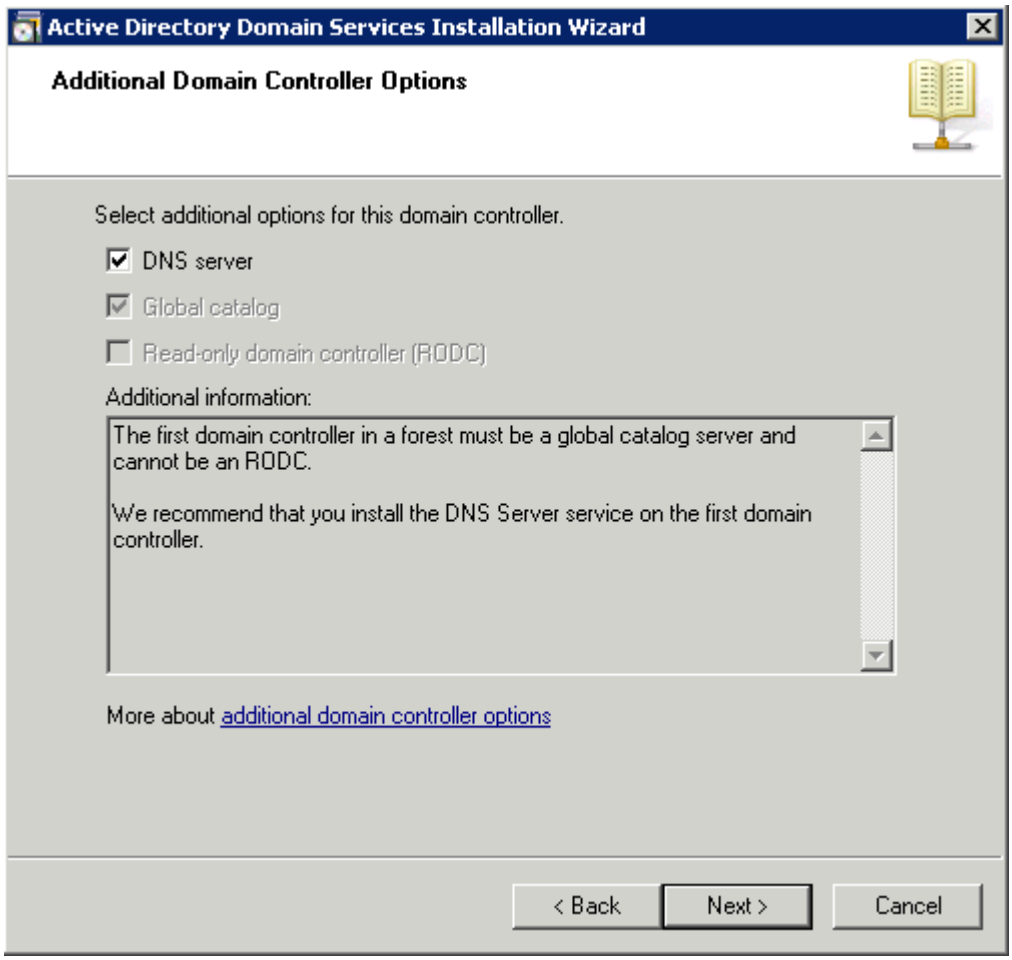
12. Wählen Sie die Gesamtstrukturfunktionsebene für Ihre Domäne aus, und klicken Sie auf Weiter.



13. Wählen Sie die funktionale Domänenebene für Ihre Domäne aus, und klicken Sie auf Weiter.

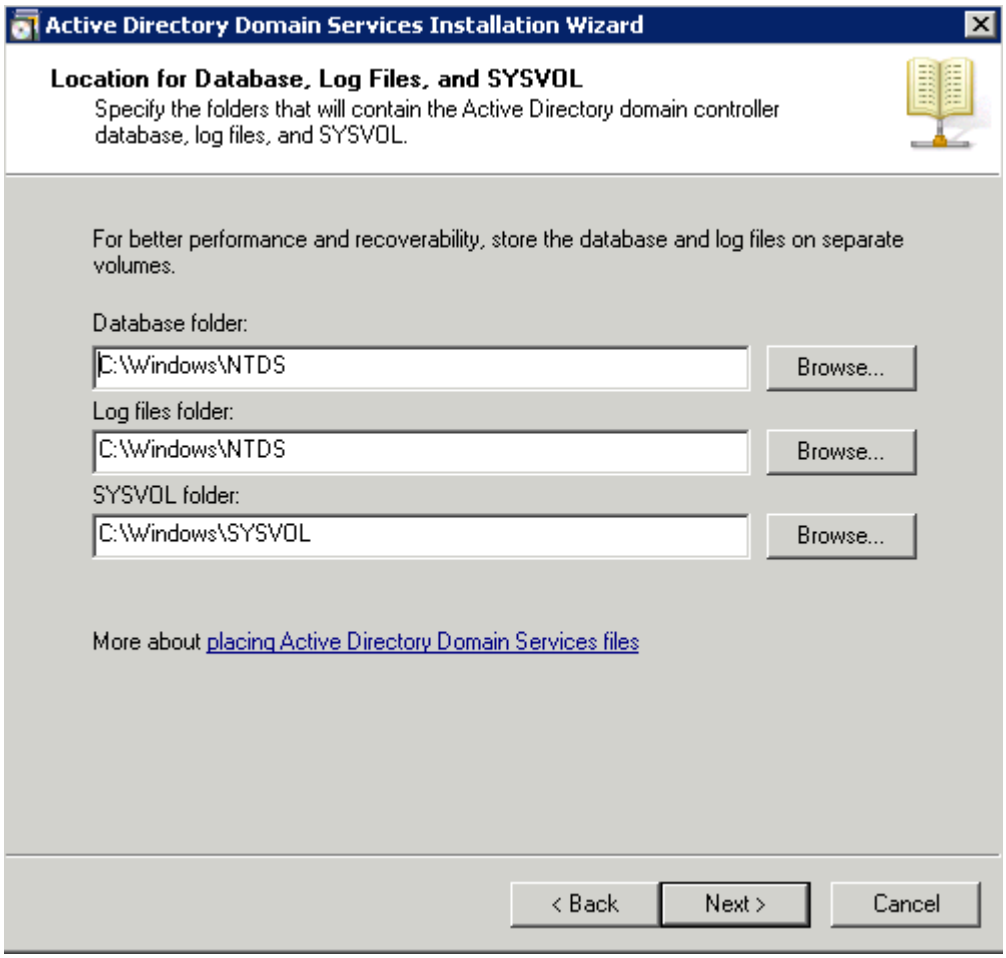


14. Vergewissern Sie sich, dass der DNS-Server ausgewählt ist, und klicken Sie auf Weiter.

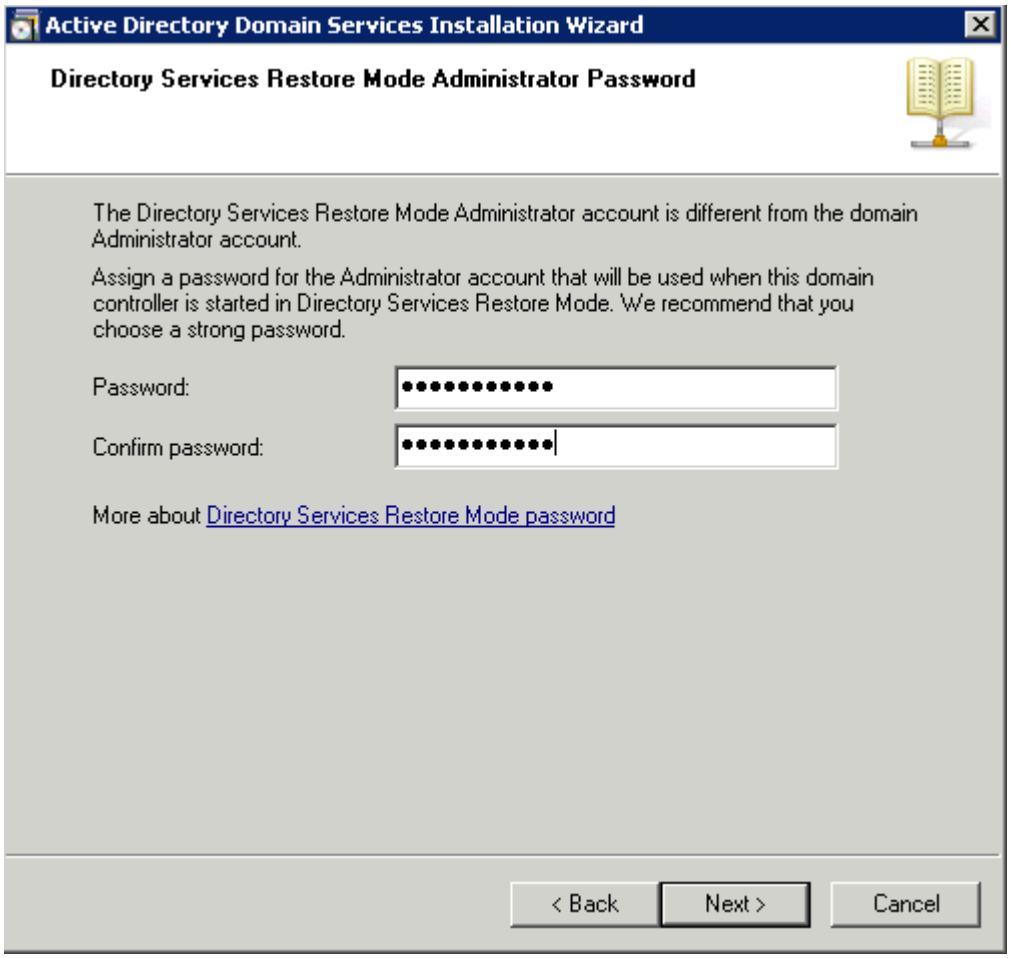


15. Klicken Sie auf Ja, um mit dem Installationsassistenten eine neue Zone in DNS für die Domäne zu erstellen.

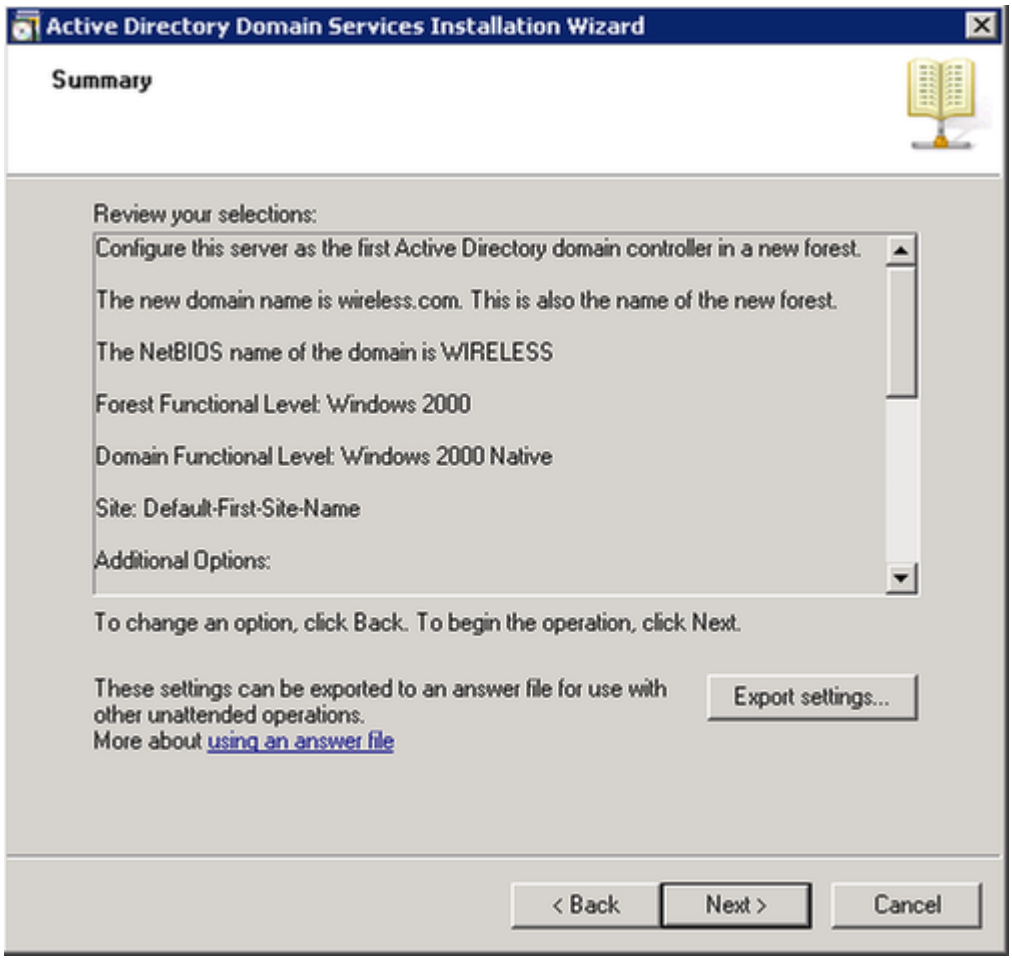
16. Wählen Sie die Ordner aus, die Active Directory für die Dateien verwenden muss, und klicken Sie auf Weiter.



17. Geben Sie das Administratorkennwort ein, und klicken Sie auf Weiter.

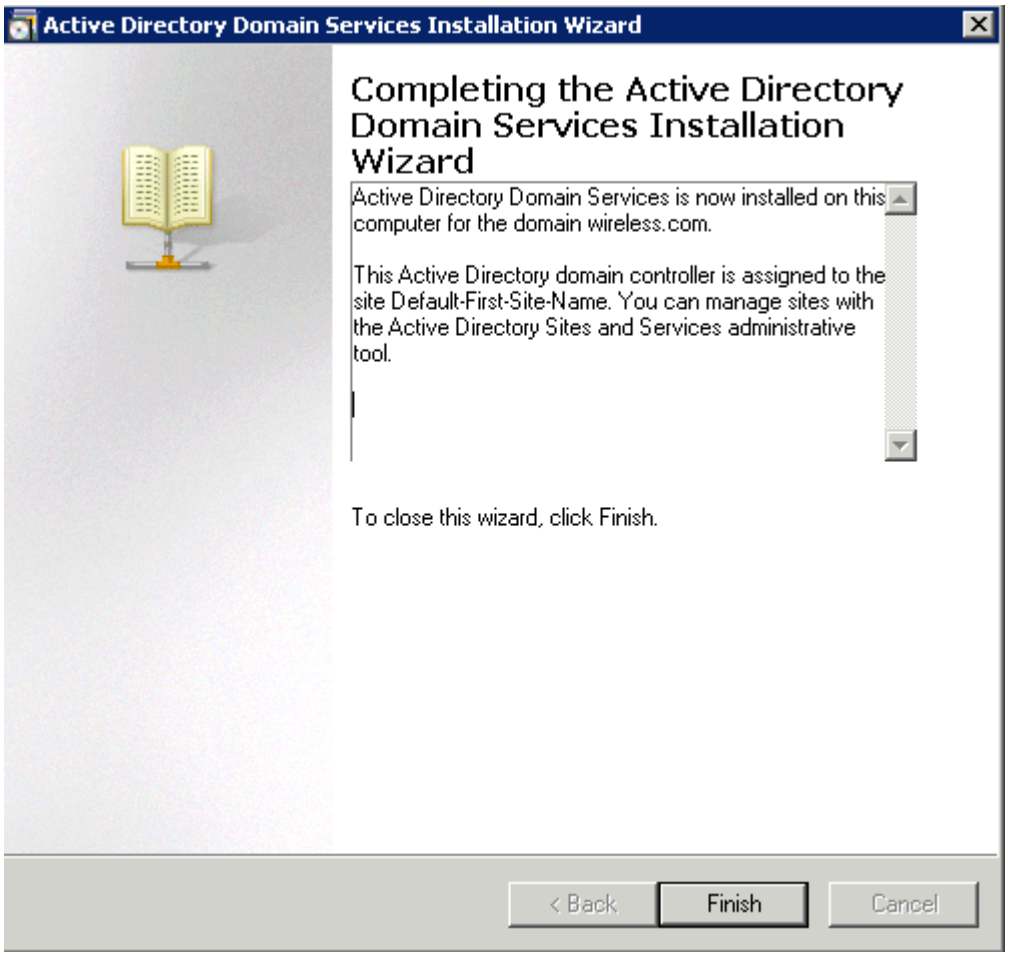


18. Überprüfen Sie Ihre Auswahl, und klicken Sie auf Weiter.

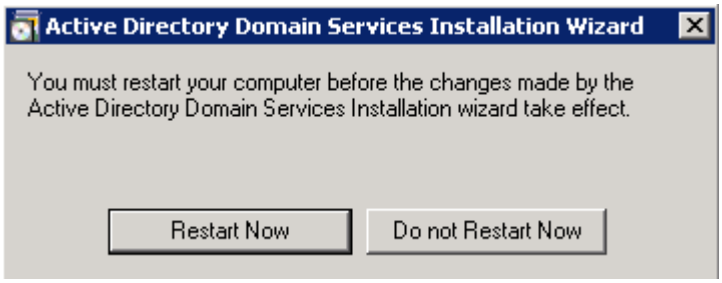


Die Installation wird fortgesetzt.

19. Klicken Sie auf Fertig stellen, um den Assistenten zu schließen.



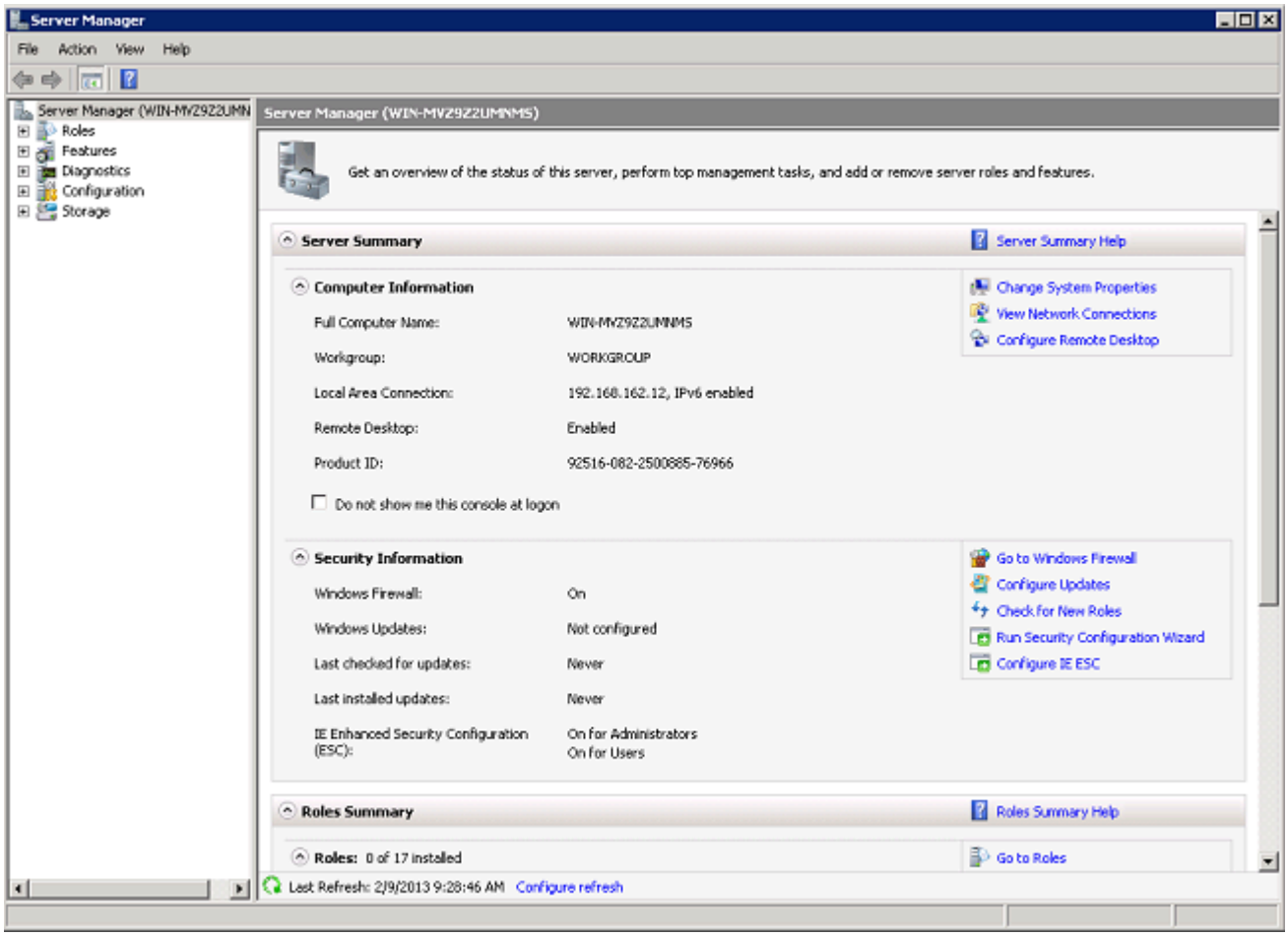
20. Starten Sie den Server neu, damit die Änderungen wirksam werden.



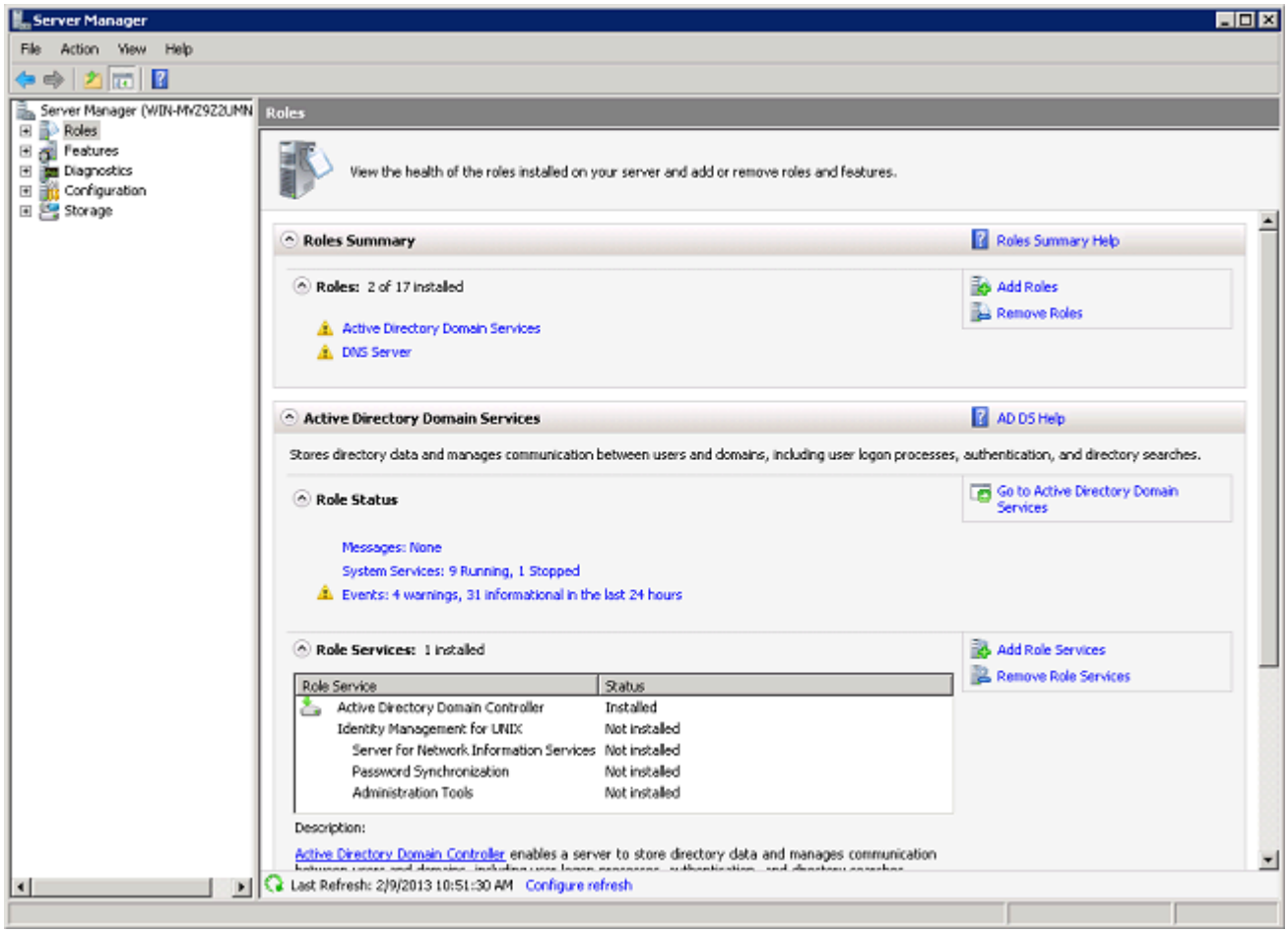
Installieren und Konfigurieren der DHCP-Dienste auf dem Microsoft Windows 2008 Server

Der DHCP-Dienst auf dem Microsoft 2008-Server wird verwendet, um den Wireless-Clients IP-Adressen bereitzustellen. Gehen Sie wie folgt vor, um DHCP-Dienste zu installieren und zu konfigurieren:

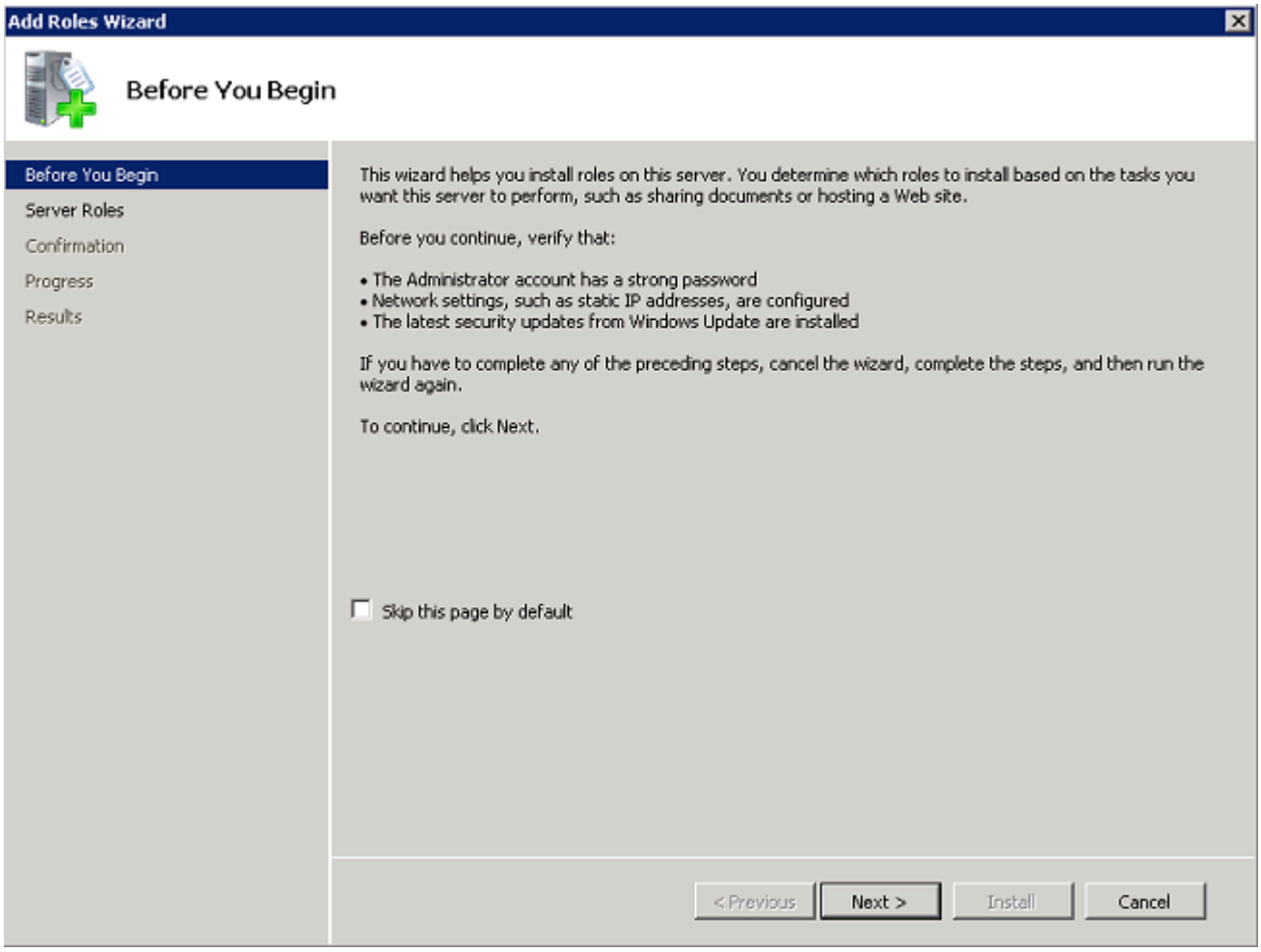
1. Klicken Sie auf Start>Server Manager.



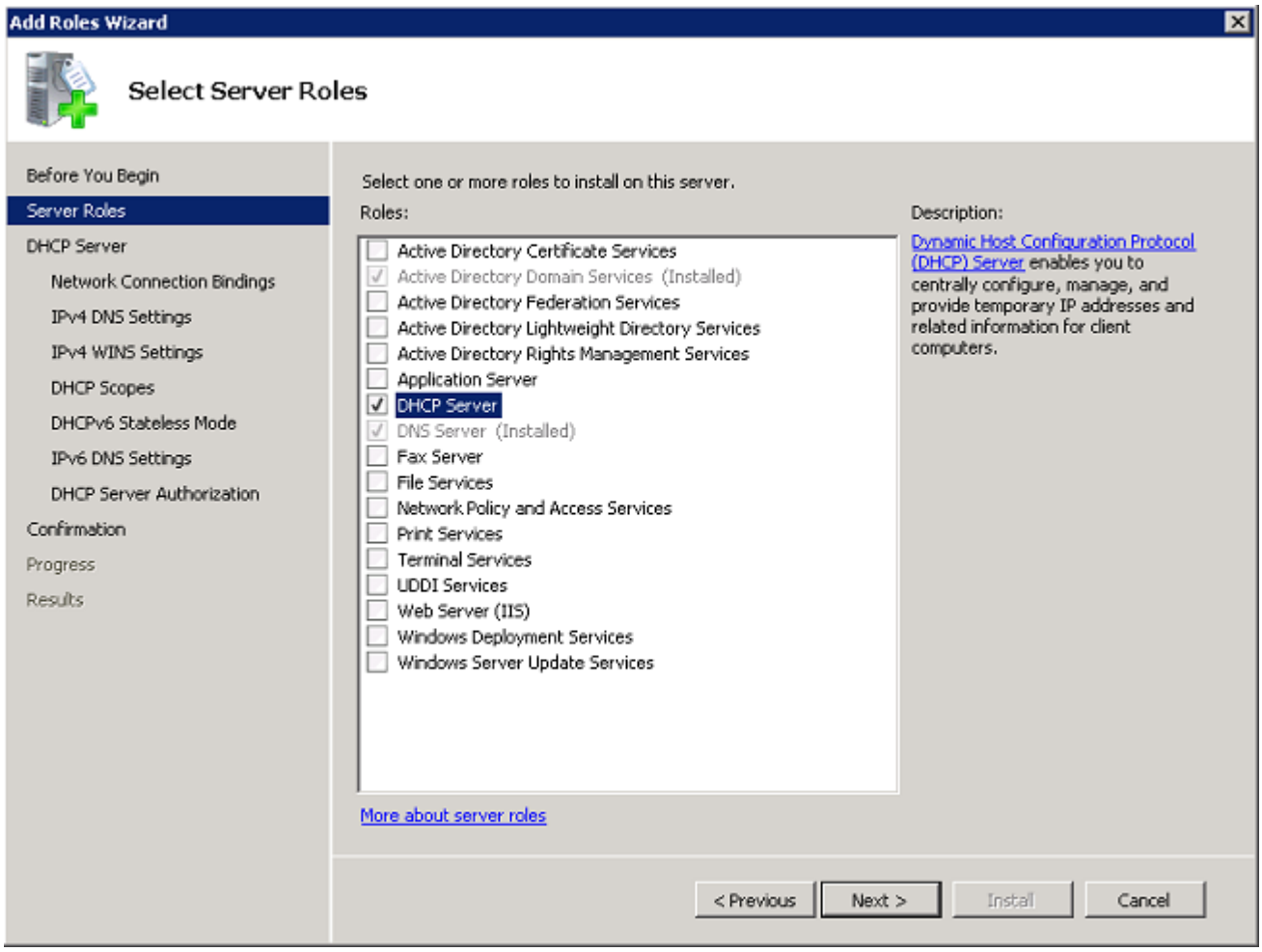
2. Klicken Sie auf Rollen > Rollen hinzufügen.



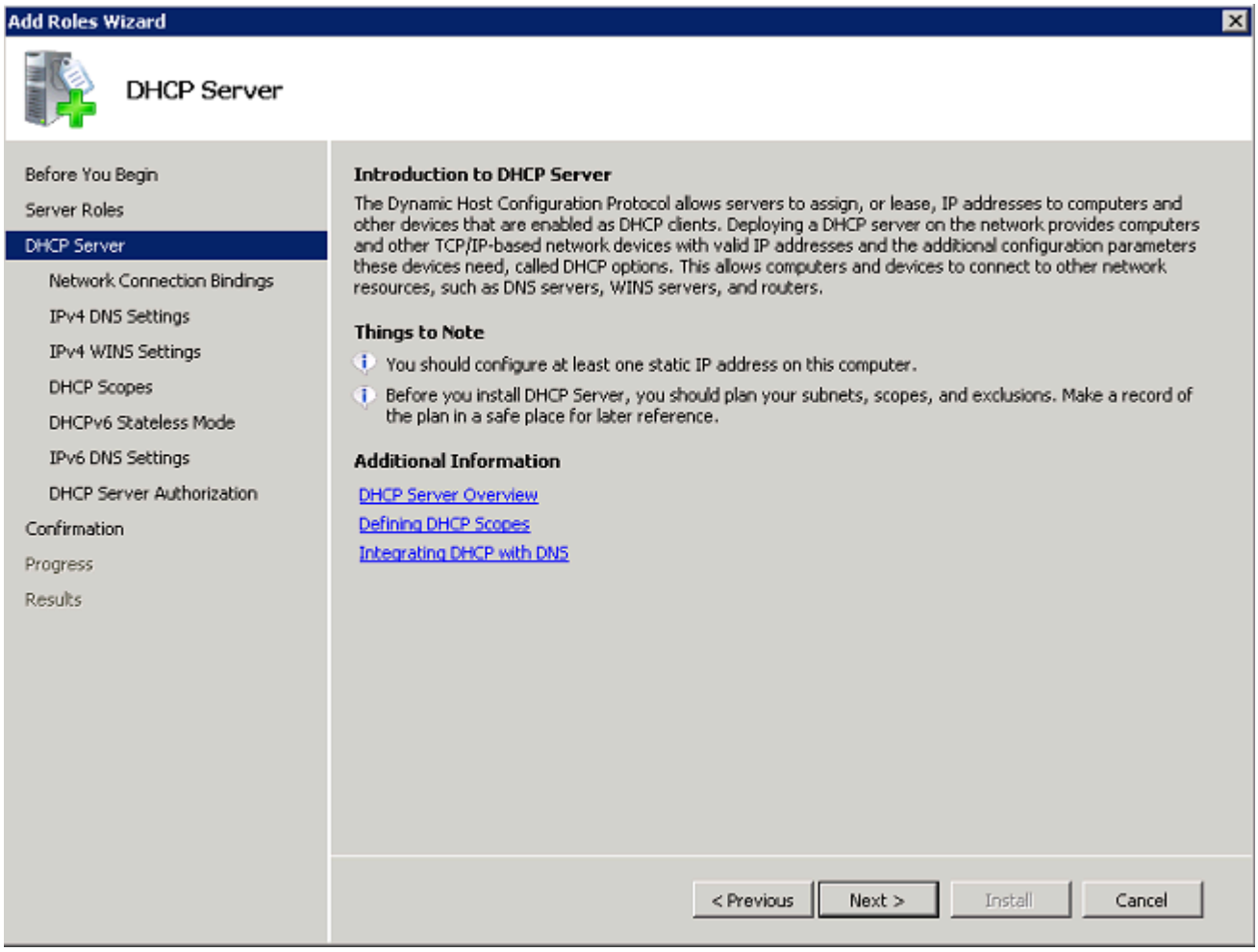
3. Klicken Sie auf Next (Weiter).



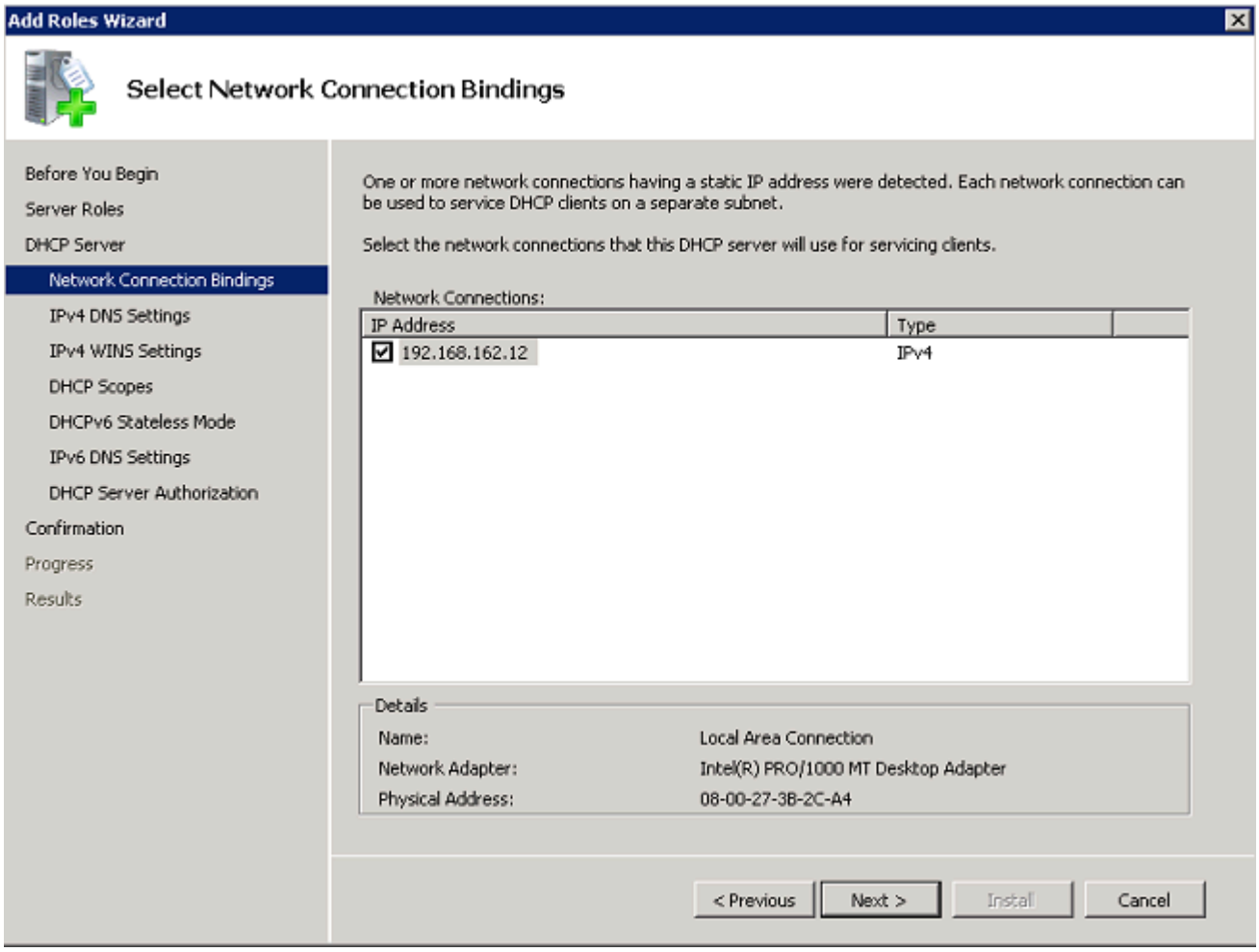
4. Wählen Sie den Service DHCP-Server aus, und klicken Sie auf Weiter.



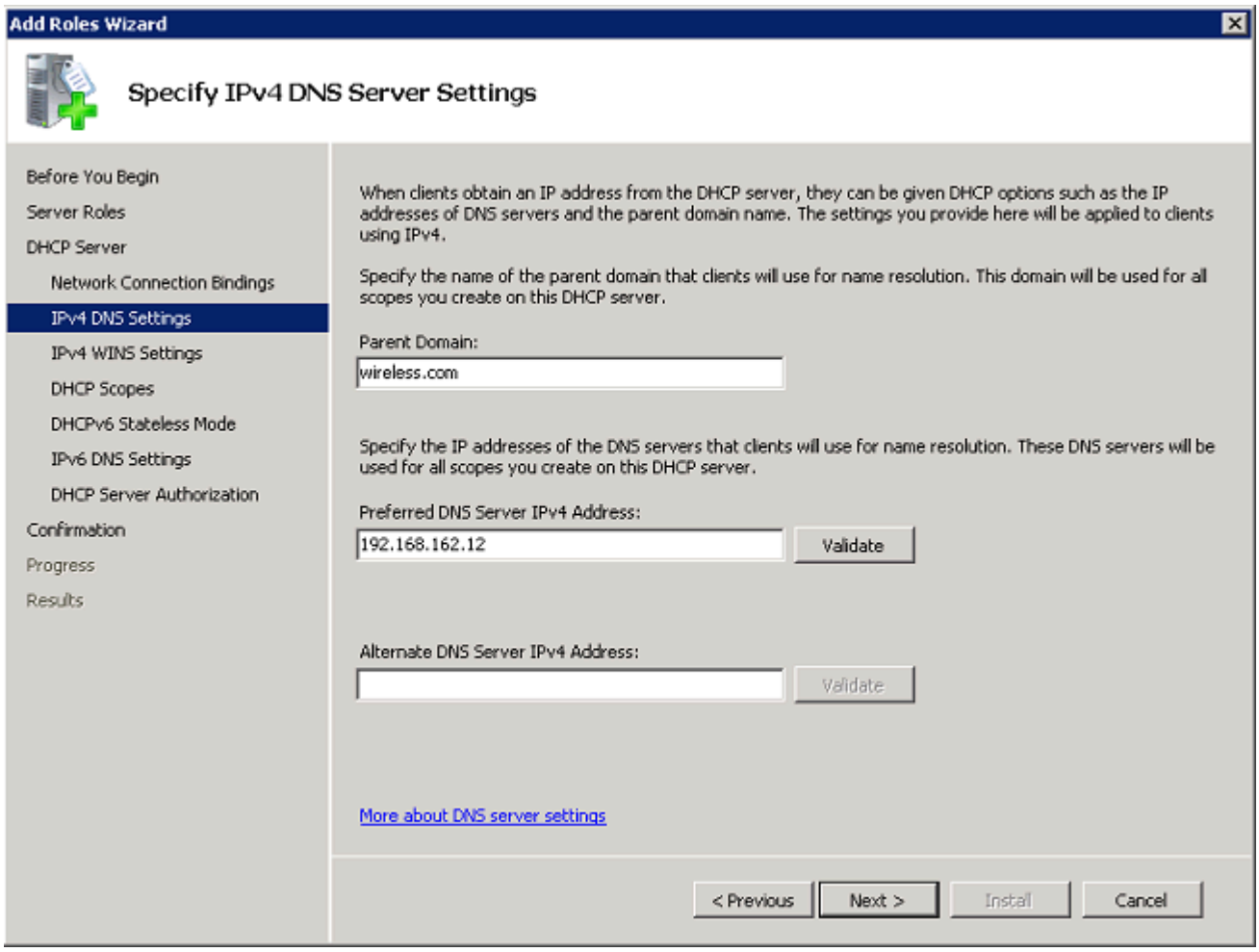
5. Lesen Sie den Abschnitt Einführung in den DHCP-Server, und klicken Sie auf Weiter.



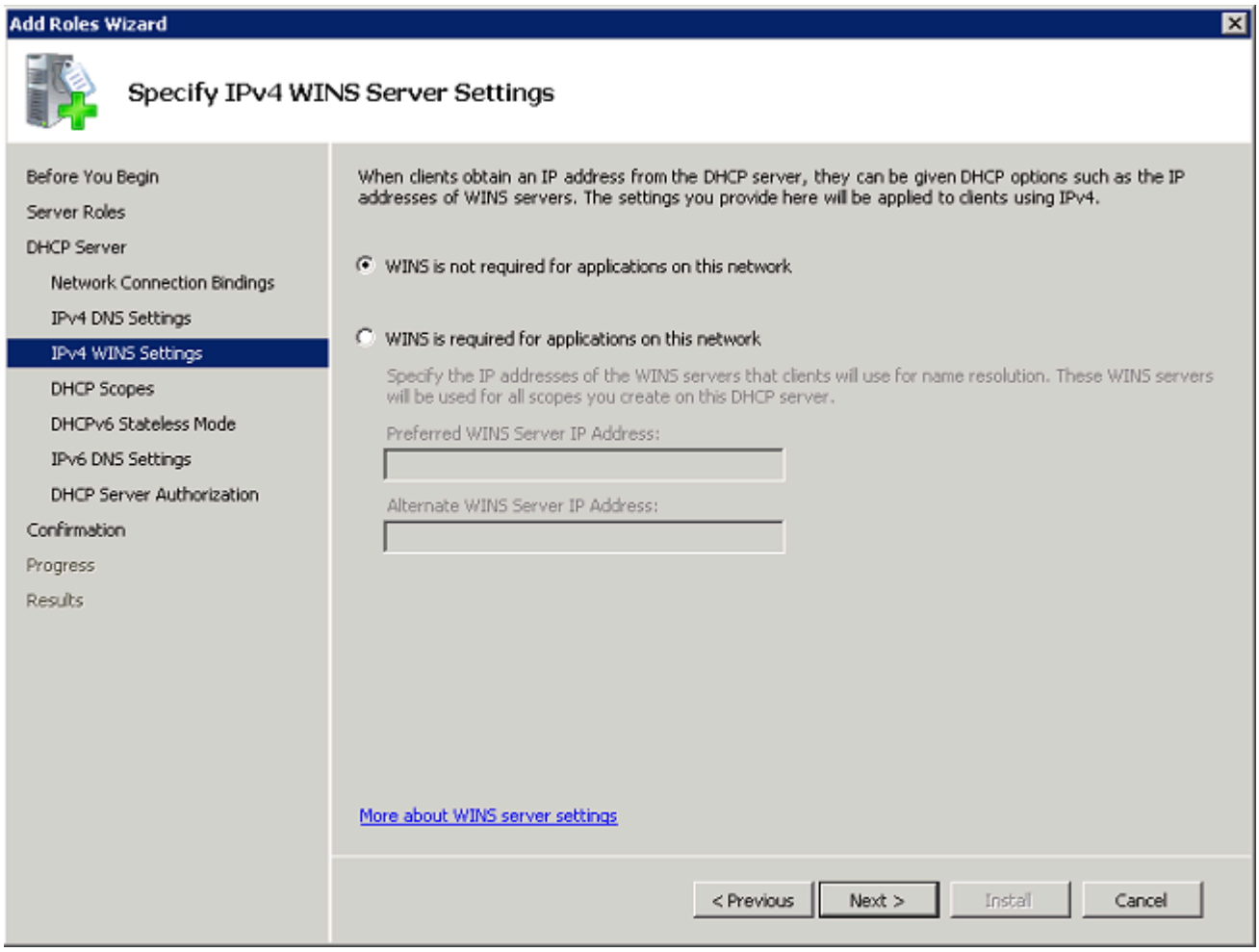
6. Wählen Sie die Schnittstelle aus, die der DHCP-Server auf Anfragen überwachen muss, und klicken Sie auf Weiter.



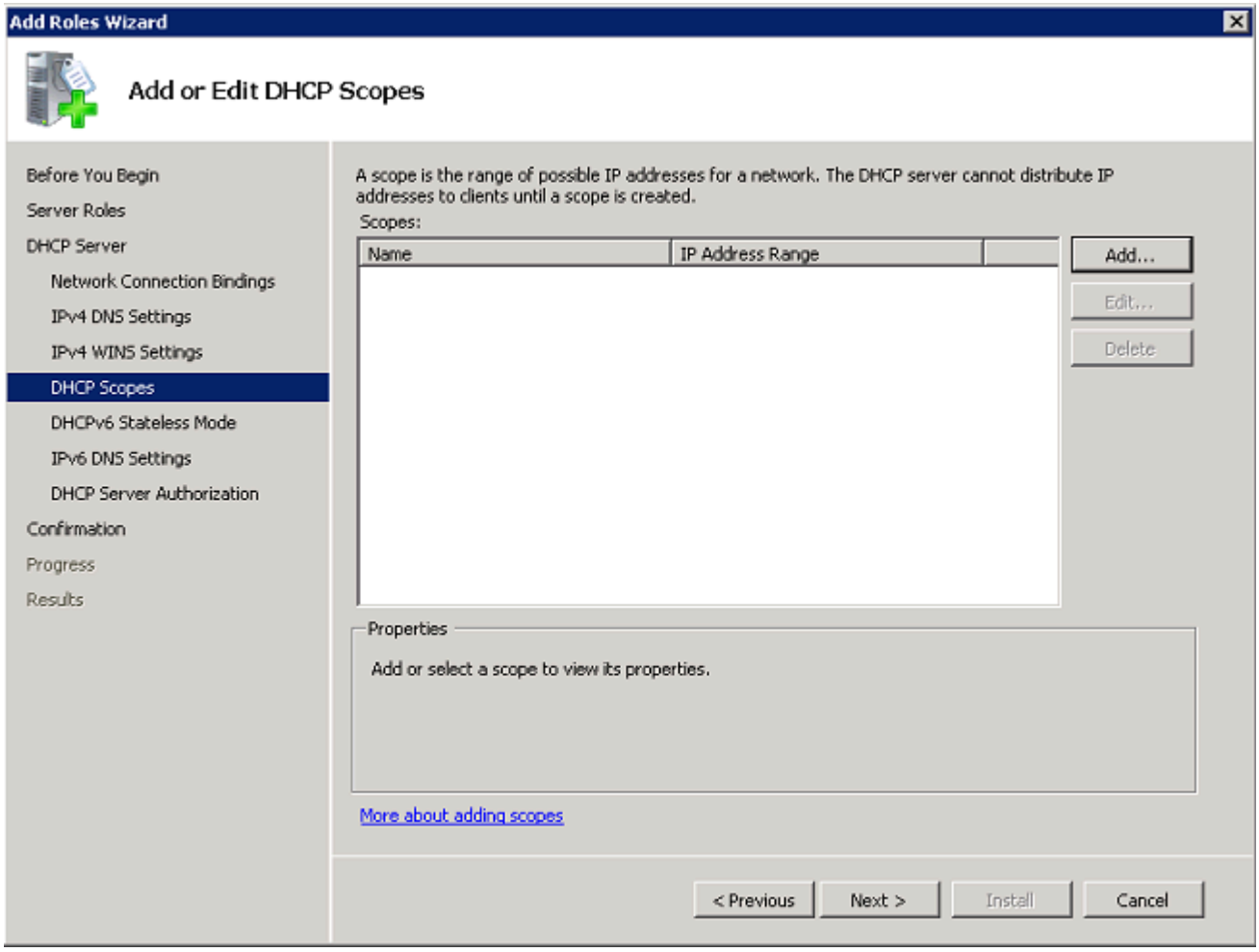
7. Konfigurieren Sie die DNS-Standardeinstellungen, die der DHCP-Server den Clients bereitstellen muss, und klicken Sie auf Weiter.



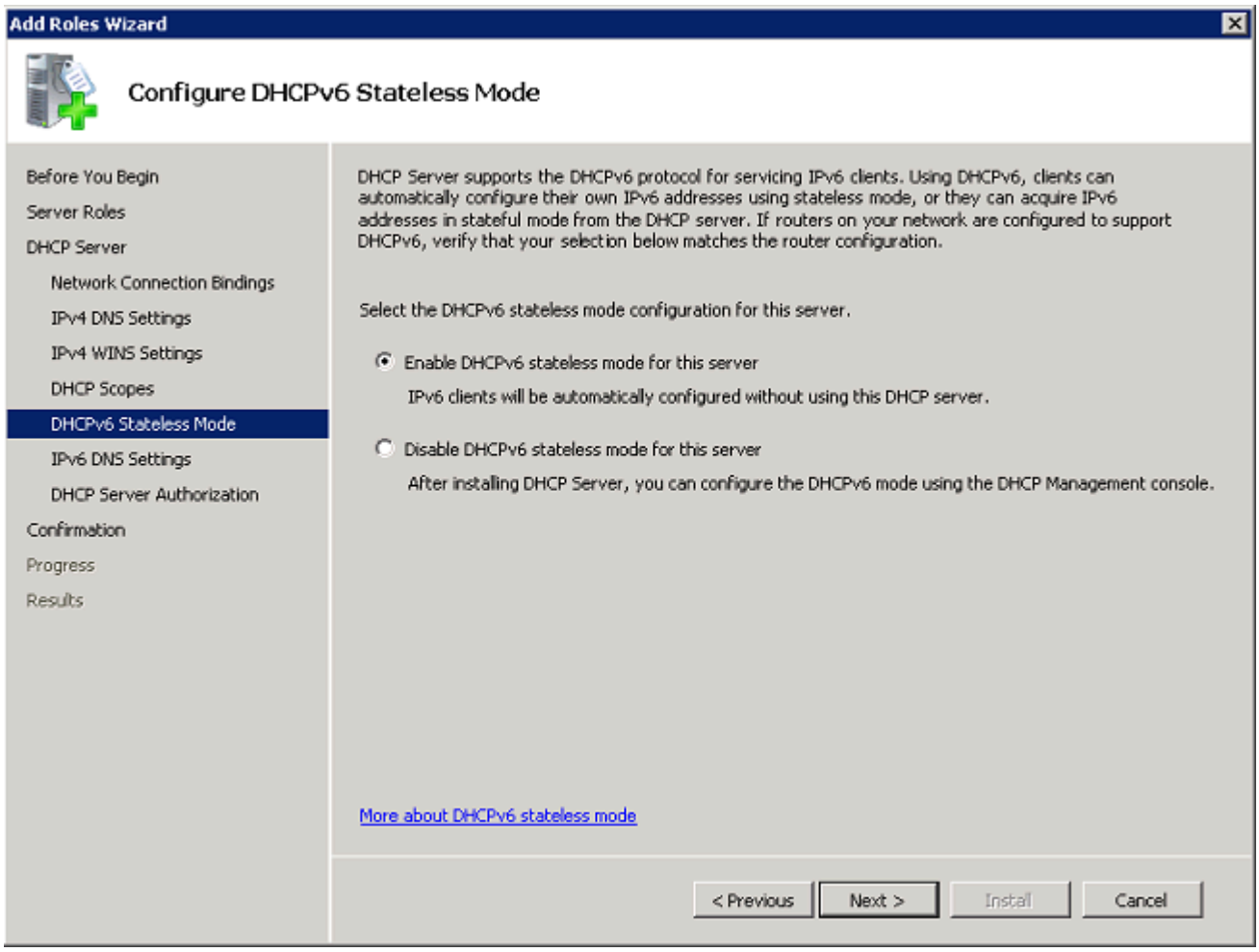
8. Konfigurieren Sie WINS, wenn das Netzwerk WINS unterstützt.



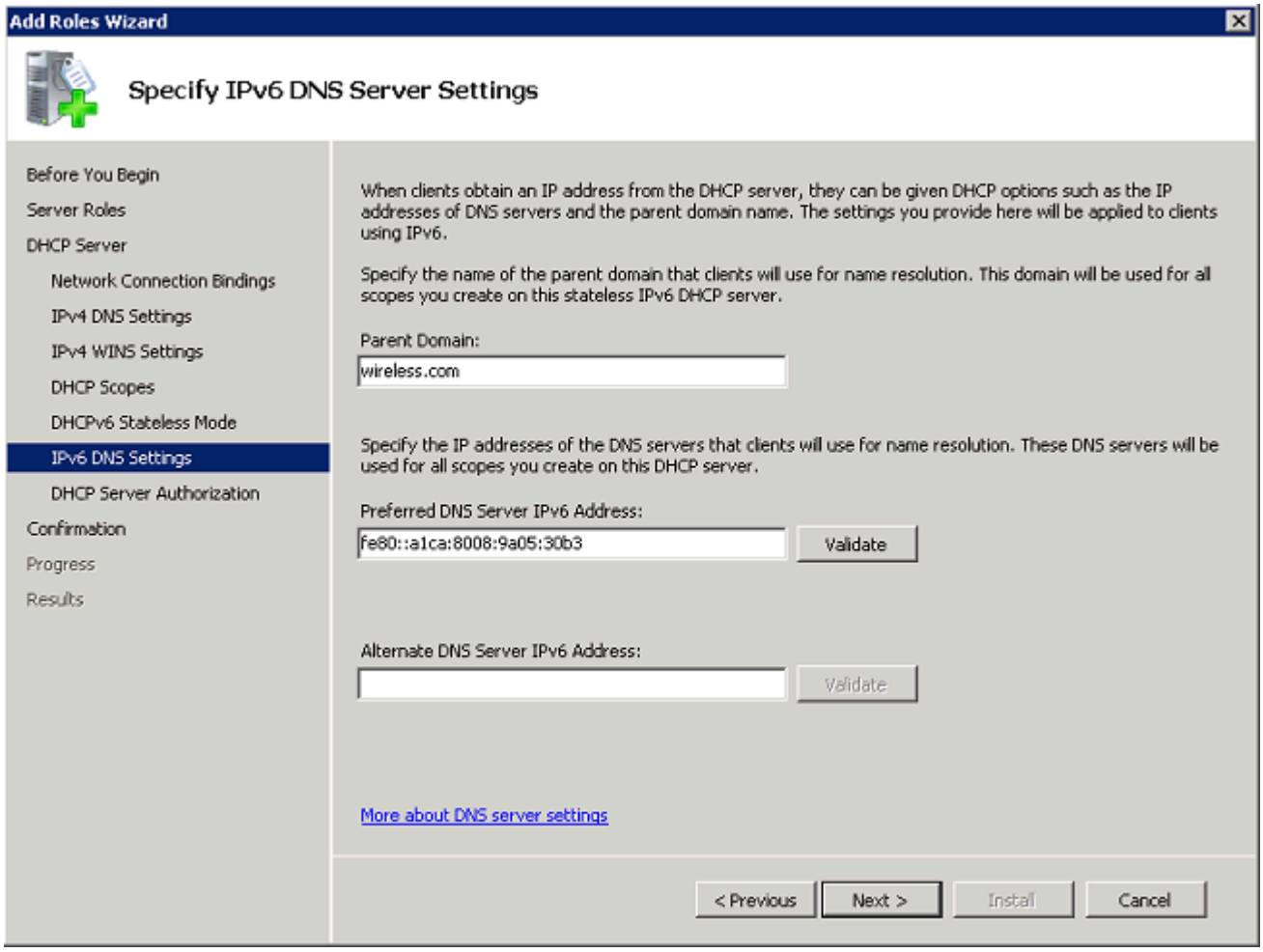
9. Klicken Sie auf Hinzufügen, um den Assistenten zum Erstellen eines DHCP-Bereichs zu verwenden, oder auf Weiter, um einen DHCP-Bereich zu einem späteren Zeitpunkt zu erstellen. Klicken Sie auf Weiter, um fortzufahren.



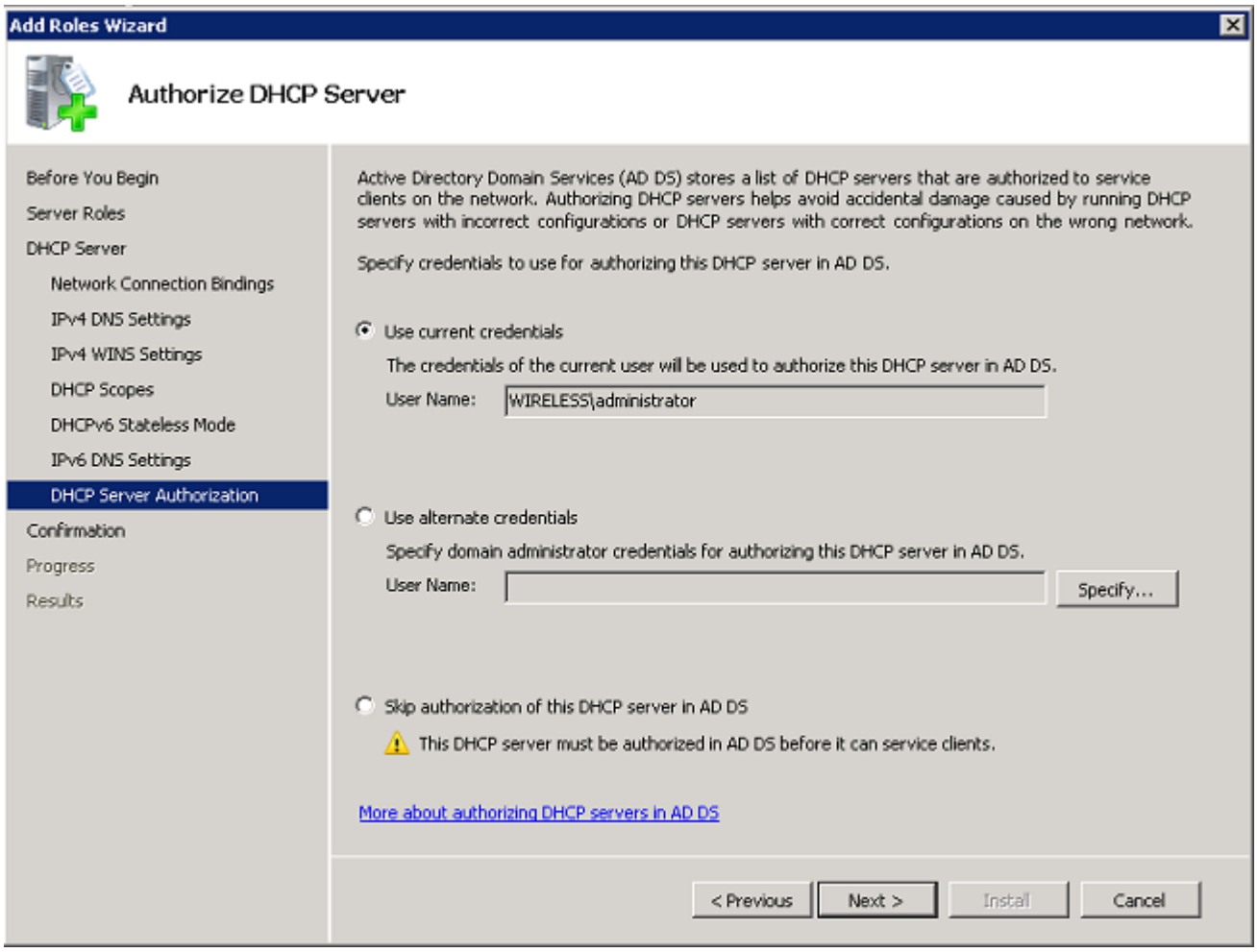
10. Aktivieren oder deaktivieren Sie die DHCPv6-Unterstützung auf dem Server, und klicken Sie auf Weiter.



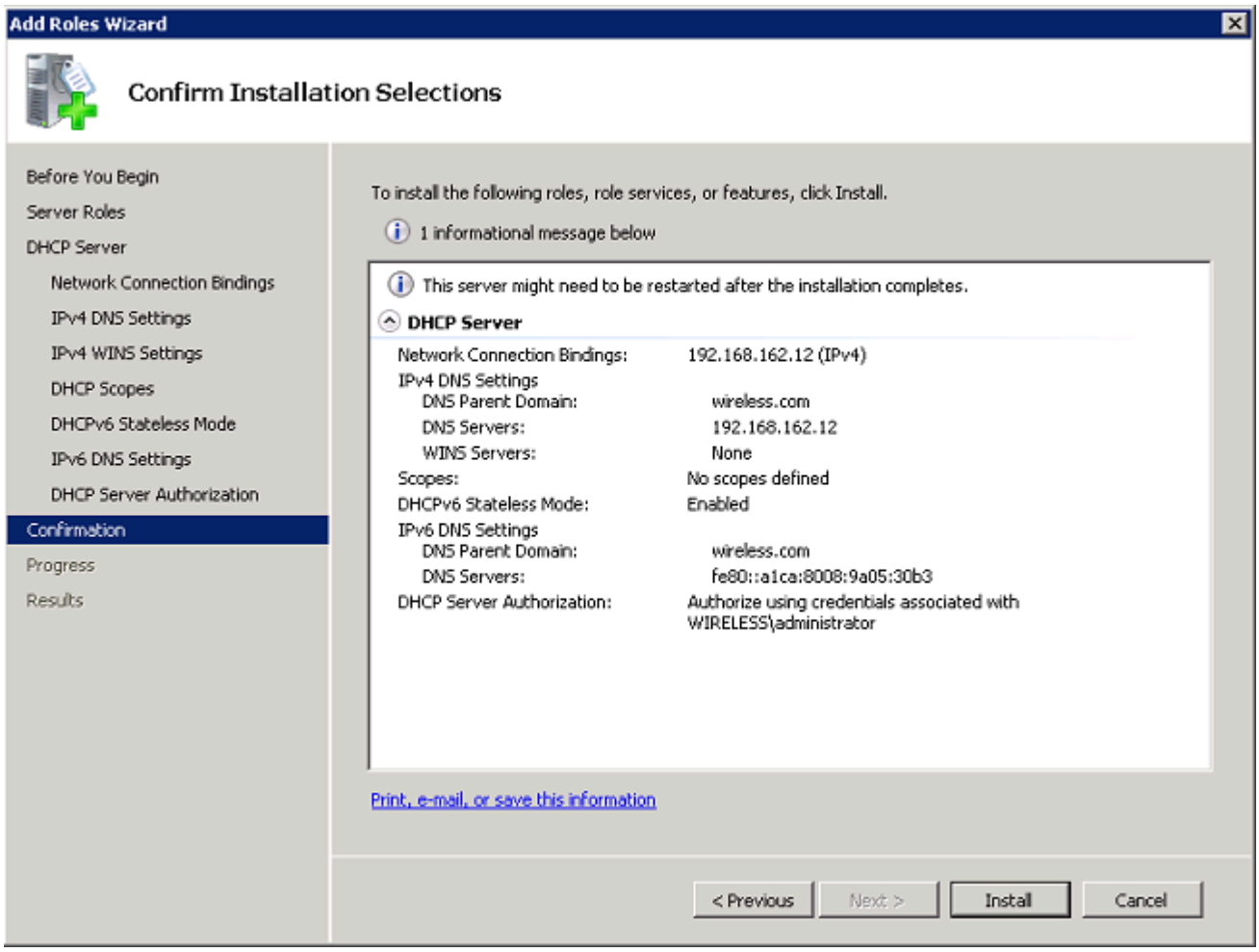
11. Konfigurieren Sie die IPv6-DNS-Einstellungen, wenn DHCPv6 im vorherigen Schritt aktiviert wurde. Klicken Sie auf Weiter, um fortzufahren.



12. Geben Sie Domänenadministratoranmeldeinformationen an, um den DHCP-Server in Active Directory zu autorisieren, und klicken Sie auf Weiter.

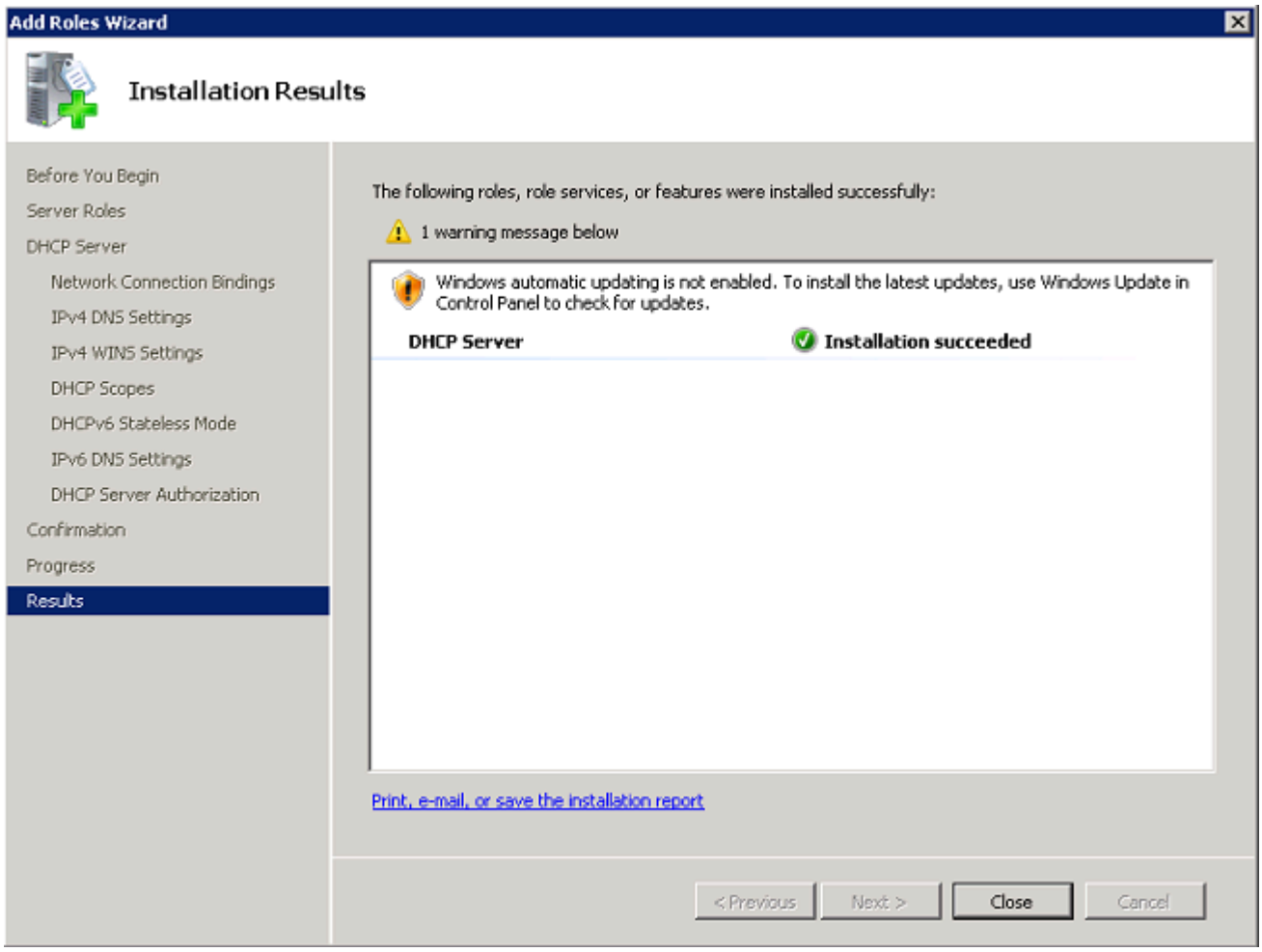


13. Überprüfen Sie die Konfiguration auf der Bestätigungsseite, und klicken Sie auf Installieren, um die Installation abzuschließen.



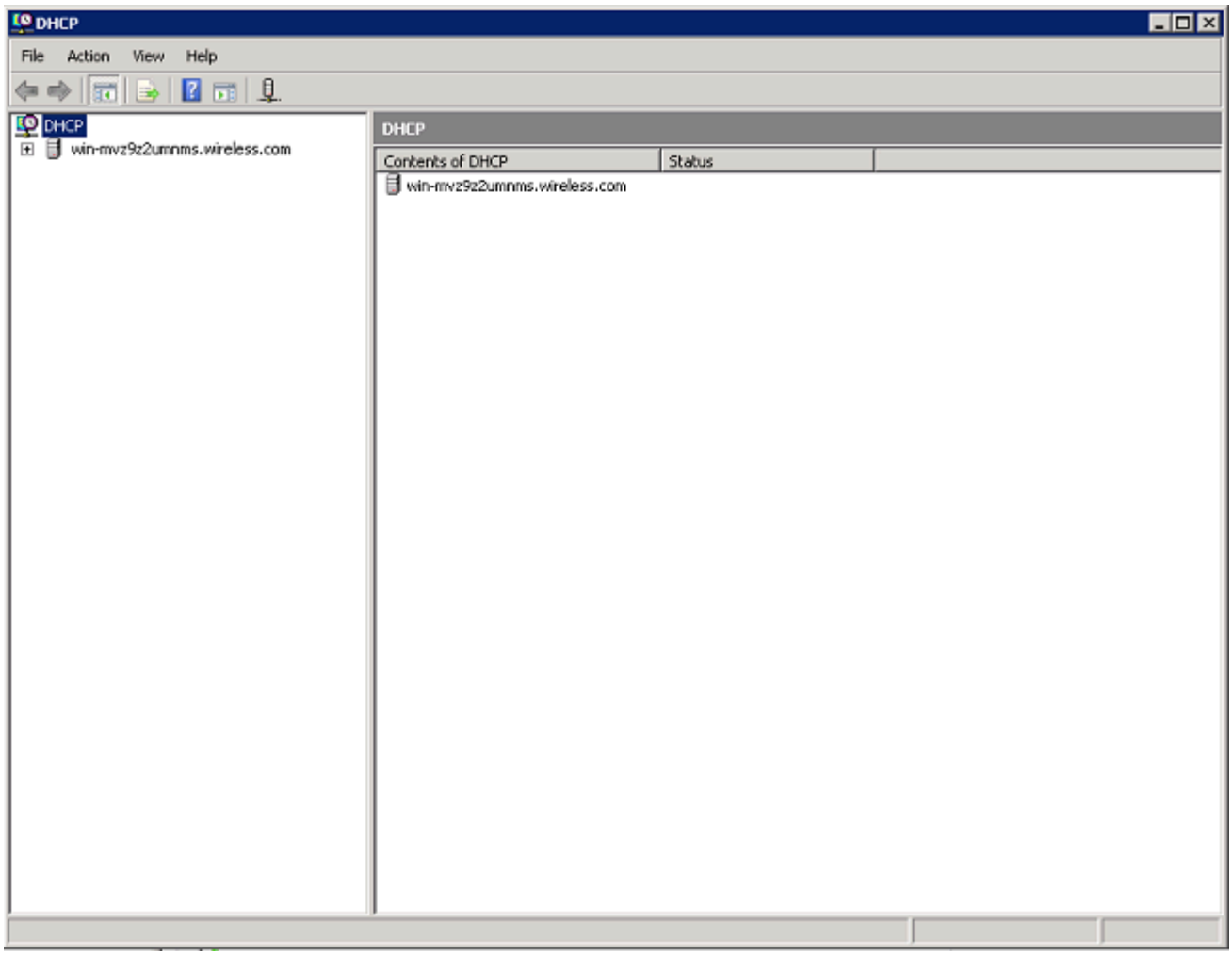
Die Installation wird fortgesetzt.

14. Klicken Sie auf Schließen, um den Assistenten zu schließen.

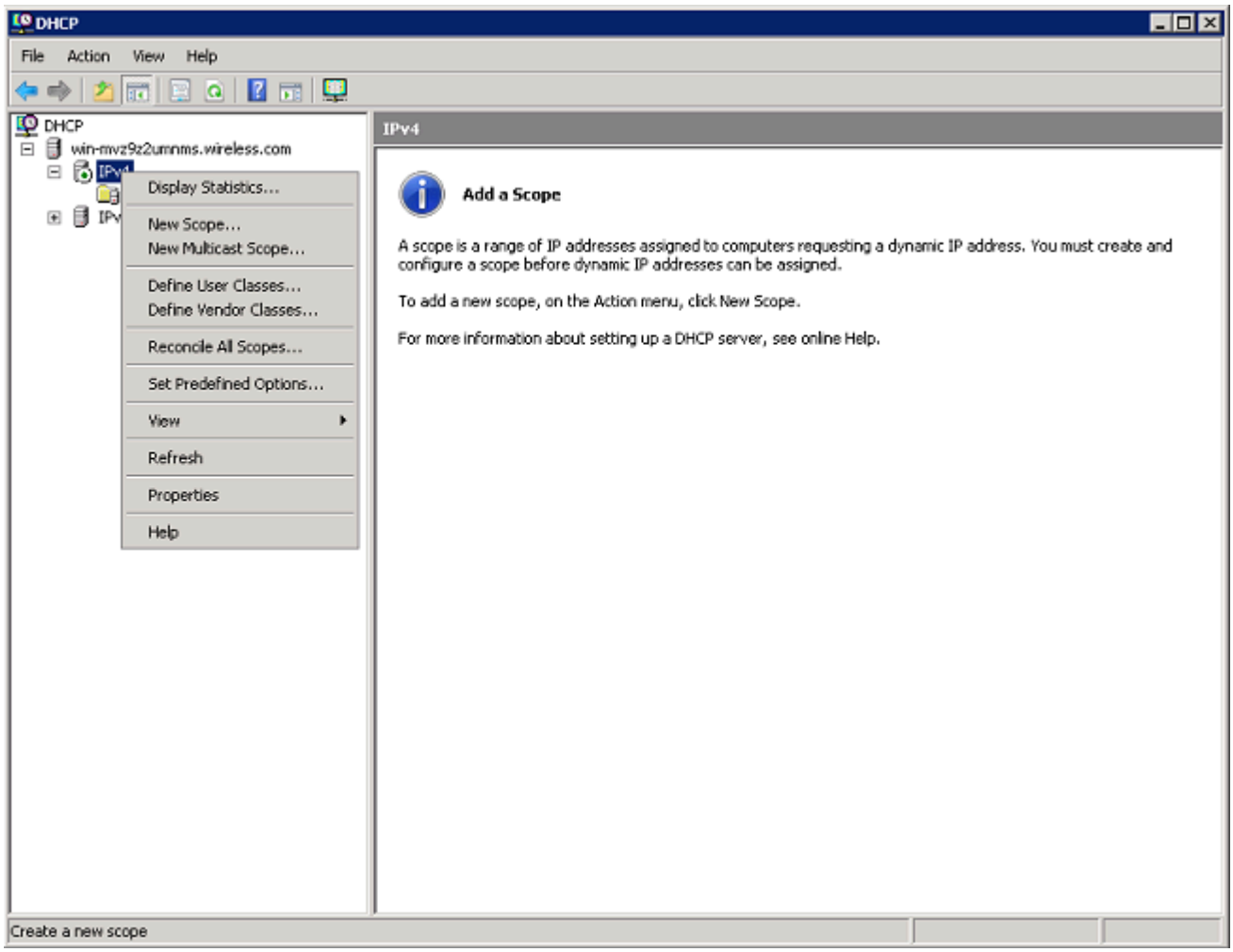


Der DHCP-Server ist nun installiert.

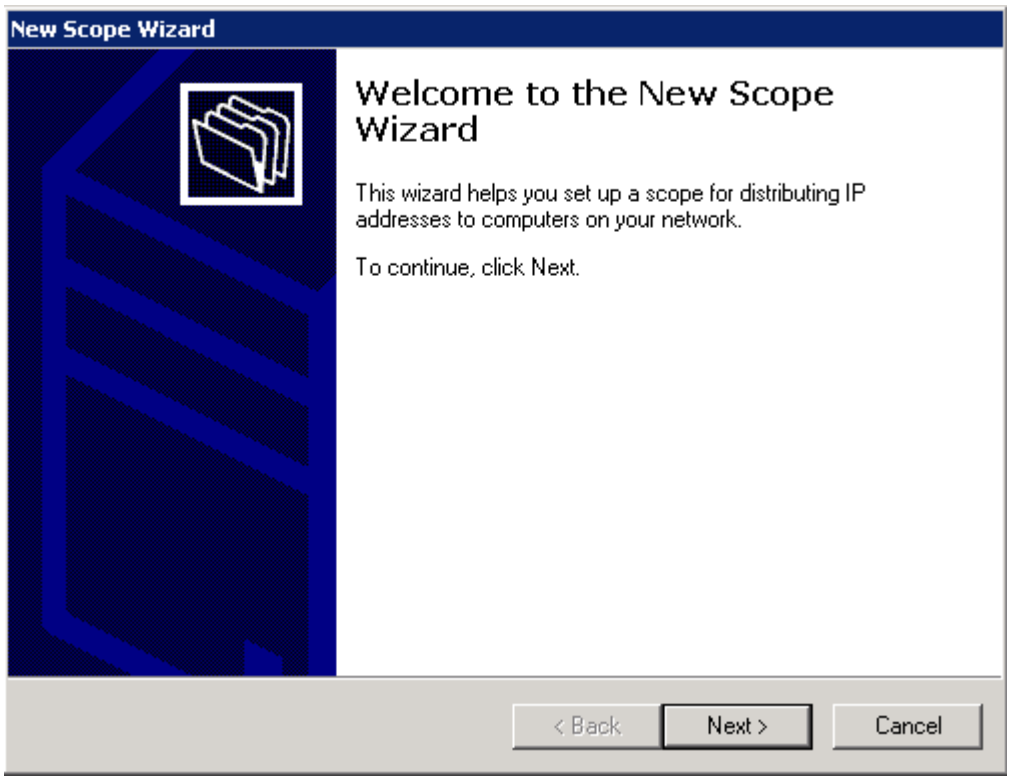
15. Klicken Sie auf Start > Verwaltung > DHCP, um den DHCP-Dienst zu konfigurieren.



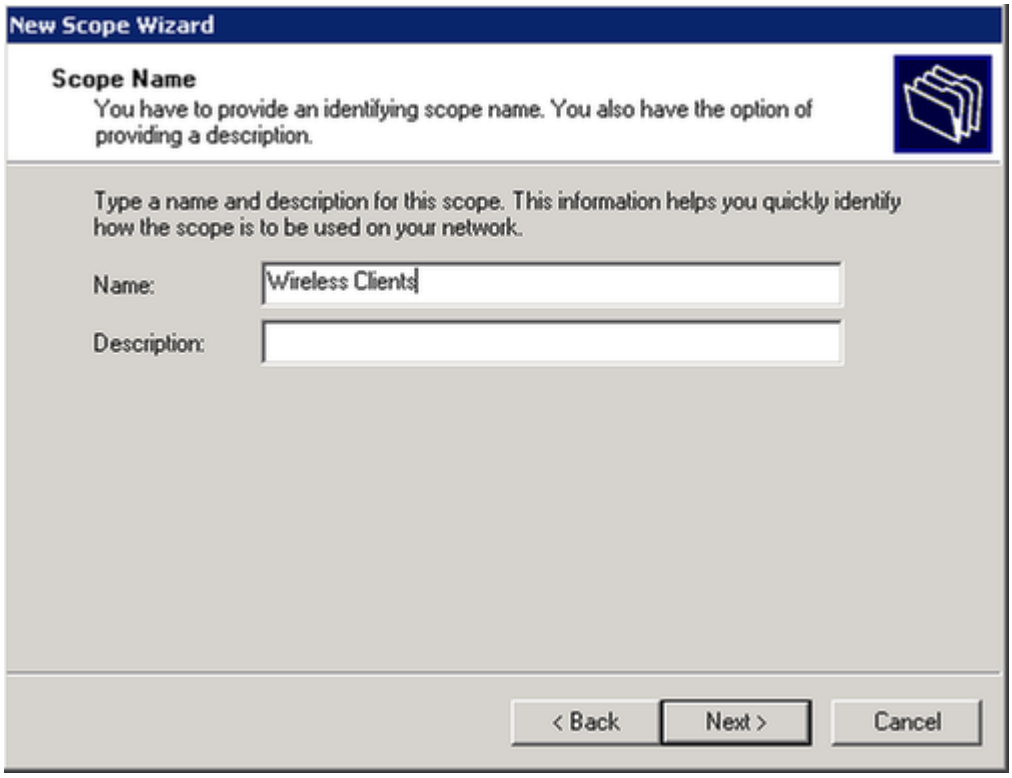
16. Erweitern Sie den DHCP-Server (im vorherigen Bild für dieses Beispiel dargestellt), klicken Sie mit der rechten Maustaste auf IPv4, und wählen Sie Neuer Bereich, um einen DHCP-Bereich zu erstellen.



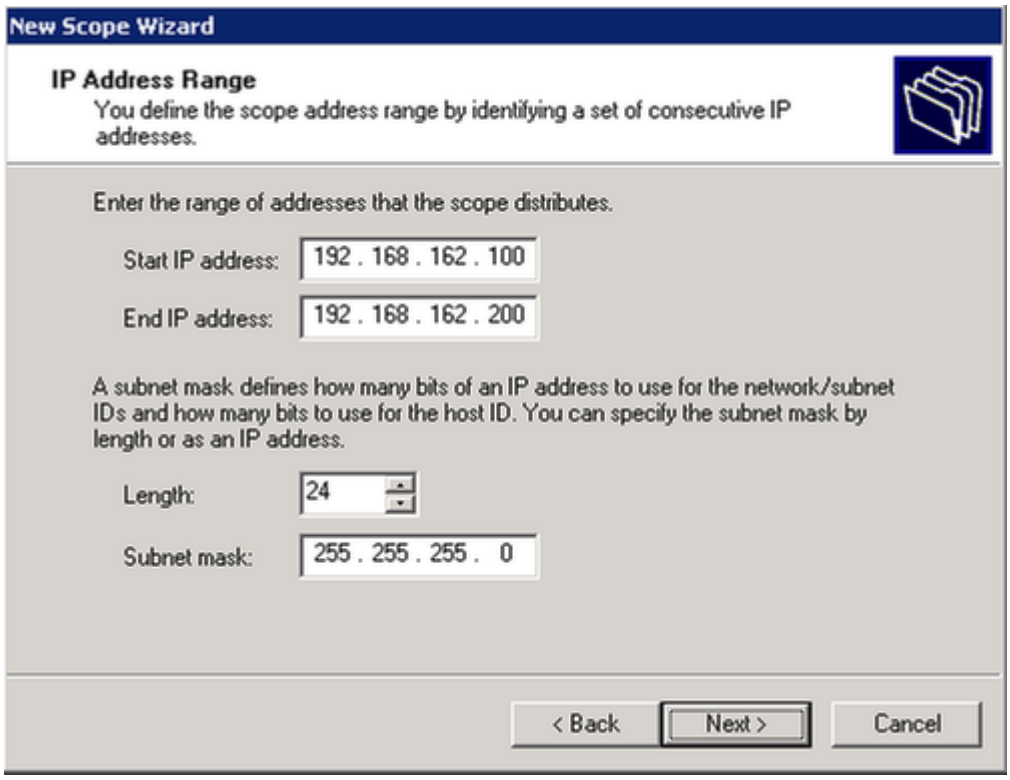
17. Klicken Sie auf Weiter, um den neuen Bereich mithilfe des Assistenten für neue Bereiche zu konfigurieren.



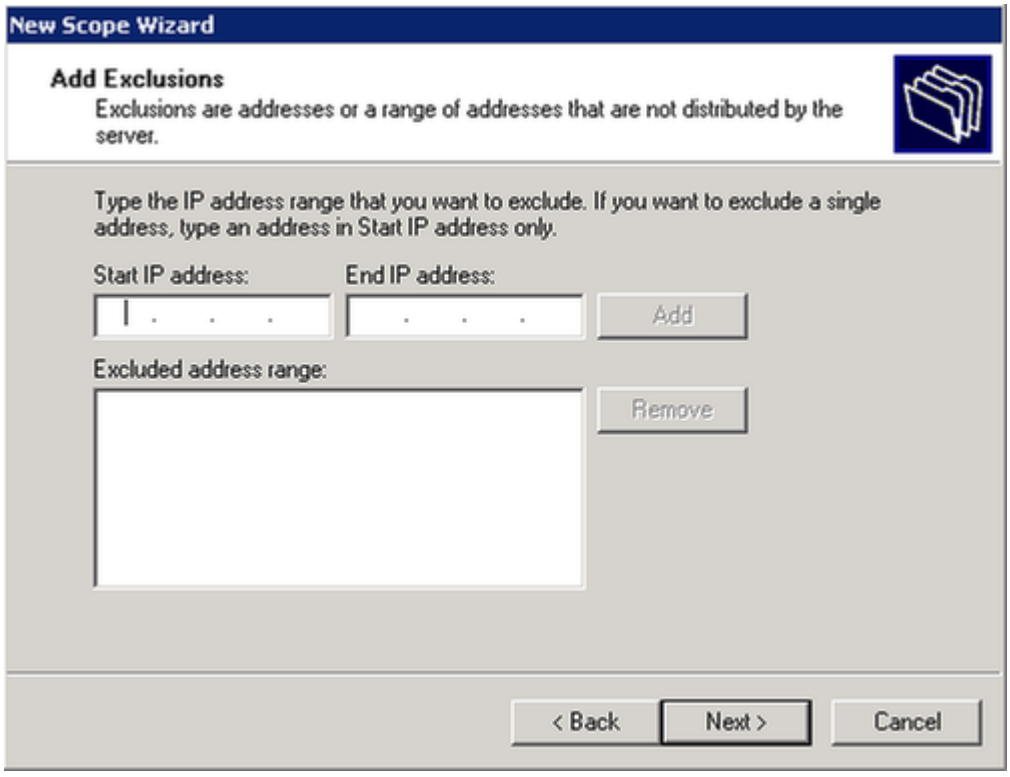
18. Geben Sie einen Namen für den neuen Bereich an (in diesem Beispiel Wireless Clients), und klicken Sie auf Weiter.



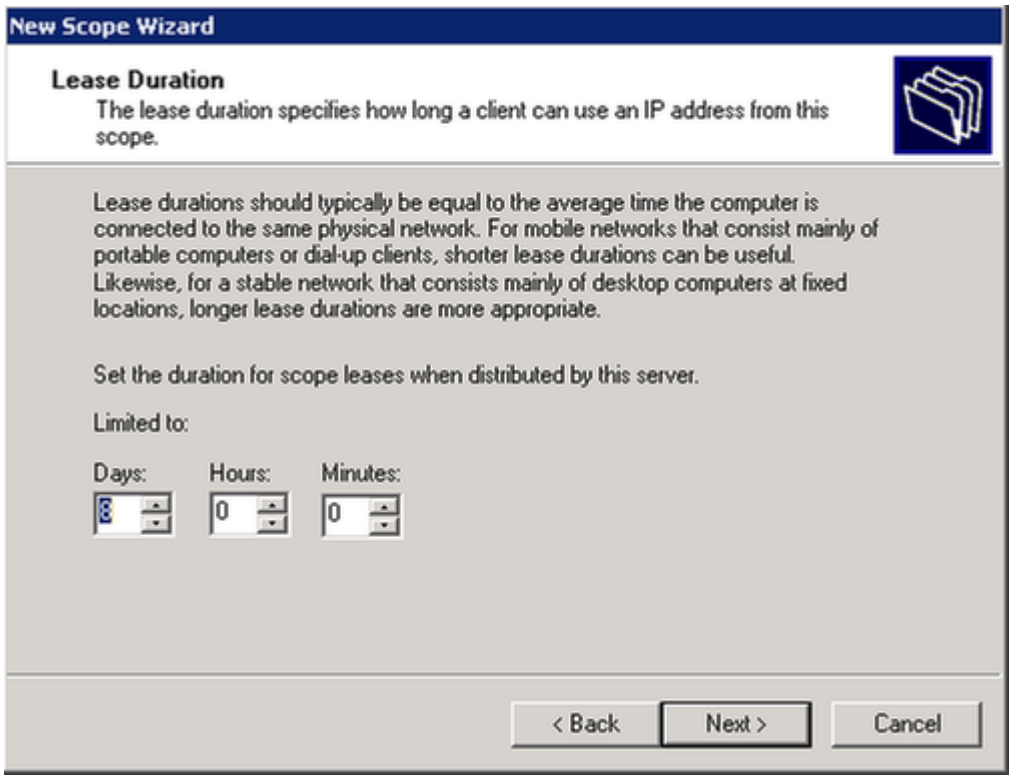
19. Geben Sie den Bereich der verfügbaren IP-Adressen ein, die für DHCP-Leases verwendet werden können. Klicken Sie auf Weiter, um fortzufahren.



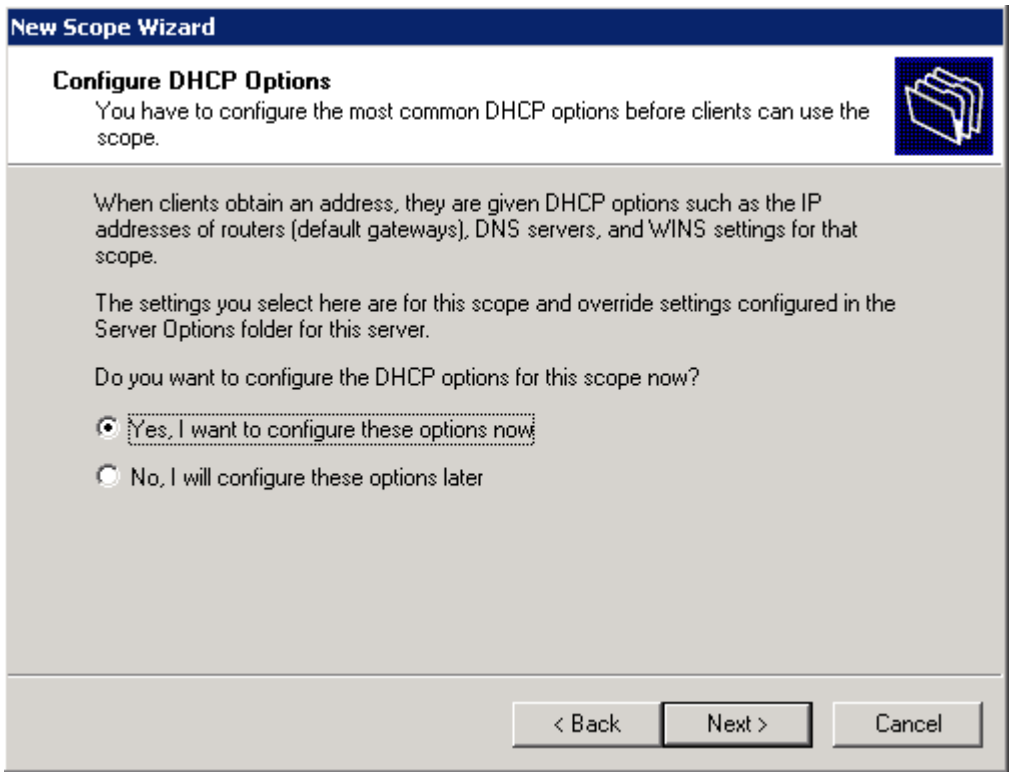
20. Erstellen Sie eine optionale Liste der ausgeschlossenen Adressen. Klicken Sie auf Weiter, um fortzufahren.



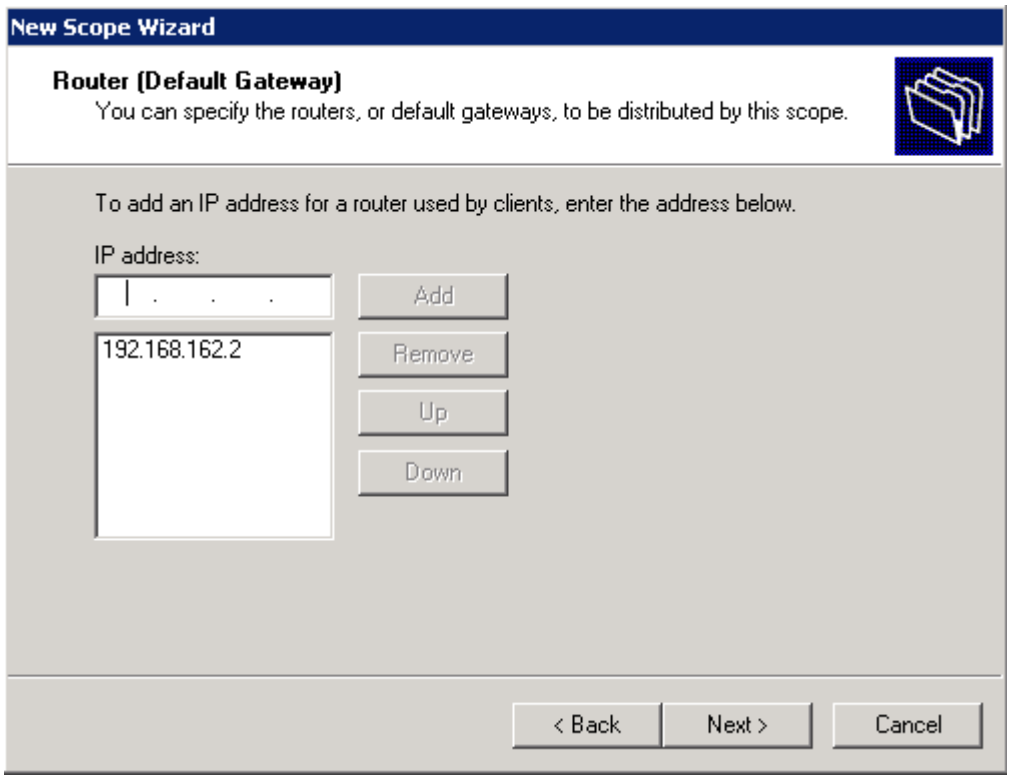
21. Konfigurieren Sie die Leasedauer, und klicken Sie auf Weiter.



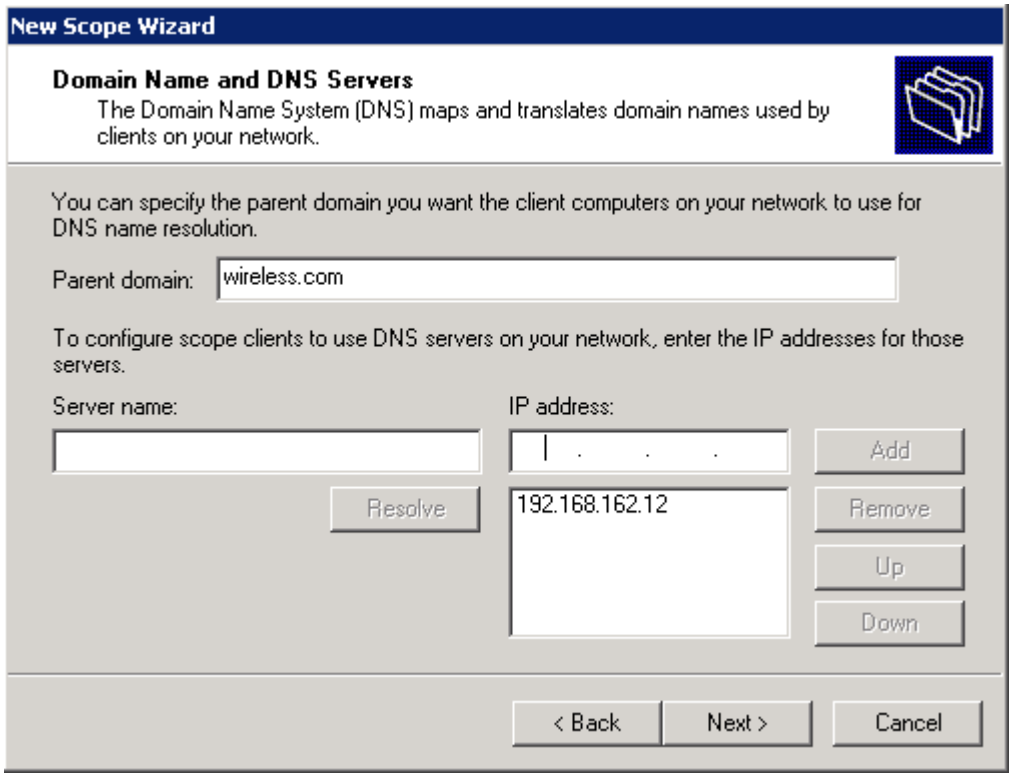
22. Klicken Sie auf Ja, ich möchte diese Optionen jetzt konfigurieren, und klicken Sie auf Weiter.



23. Geben Sie die IP-Adresse des Standardgateways für diesen Bereich ein, und klicken Sie auf Hinzufügen > Weiter.

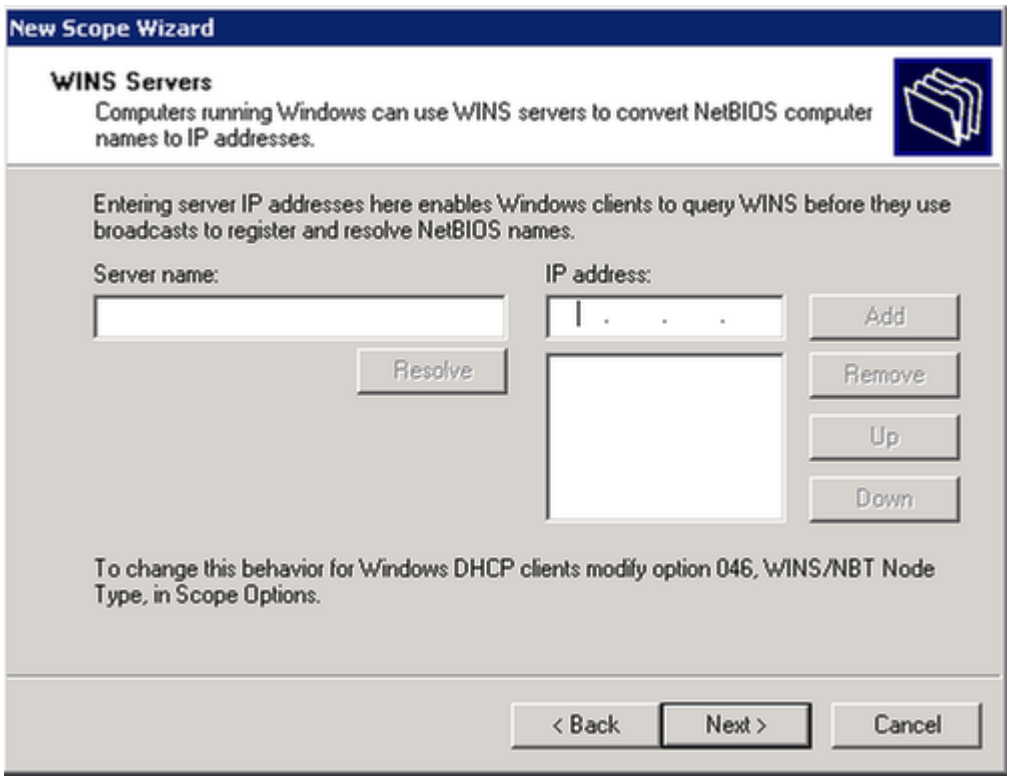


24. Konfigurieren Sie den DNS-Domänennamen und den DNS-Server für die Clients. Klicken Sie auf Weiter, um fortzufahren.

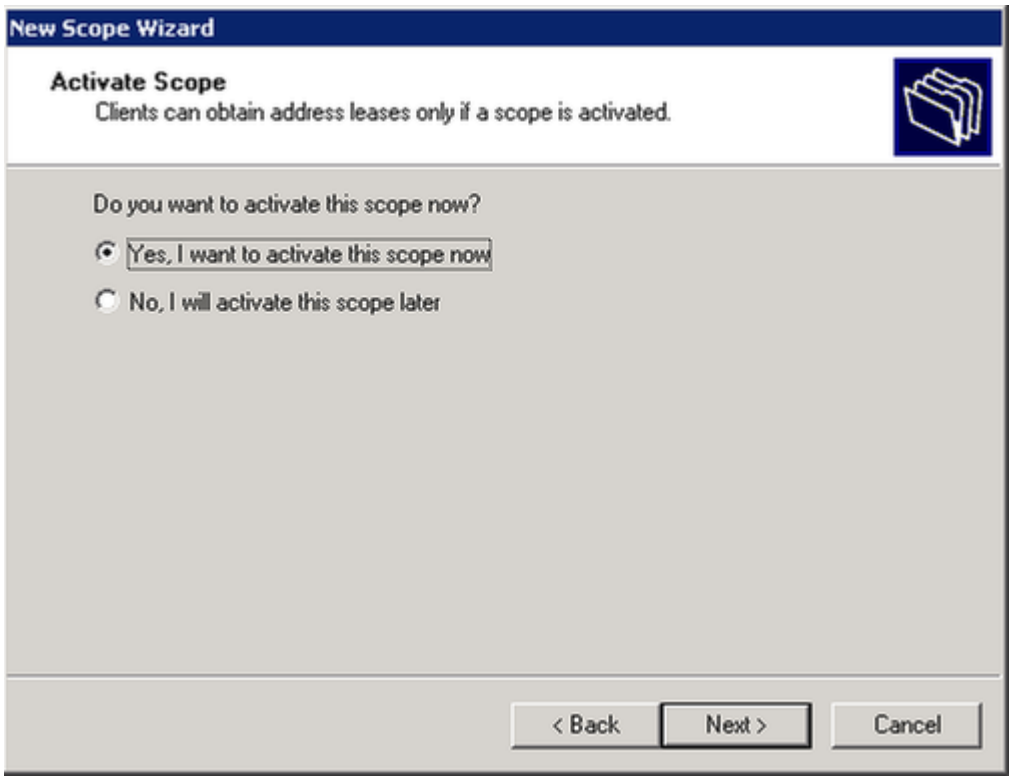


25. Geben Sie WINS-Informationen für diesen Bereich ein, wenn das Netzwerk WINS

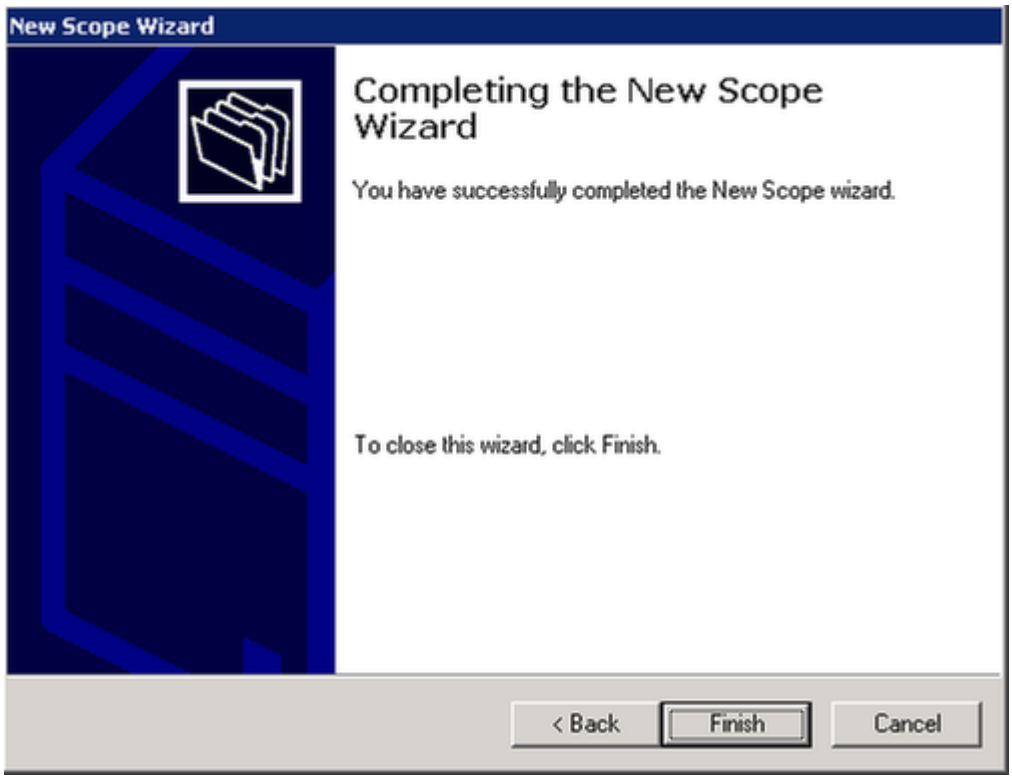
unterstützt. Klicken Sie auf Weiter, um fortzufahren.



26. Klicken Sie zum Aktivieren dieses Bereichs auf Ja, ich möchte diesen Bereich jetzt aktivieren> Weiter.



27. Klicken Sie auf Fertig stellen, um den Assistenten abzuschließen und zu schließen.

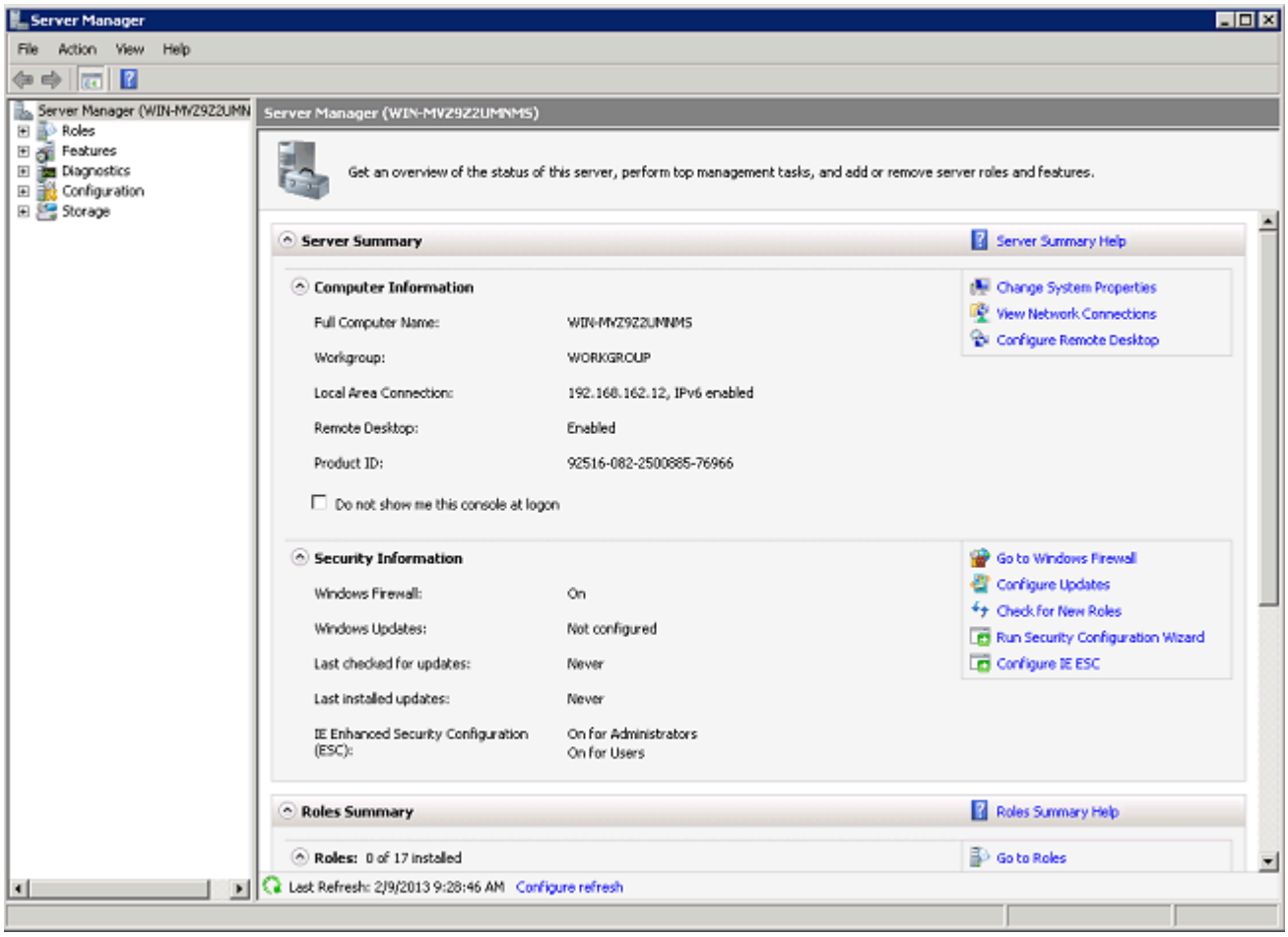


Installieren und Konfigurieren von Microsoft Windows 2008 Server als Zertifizierungsstellenserver

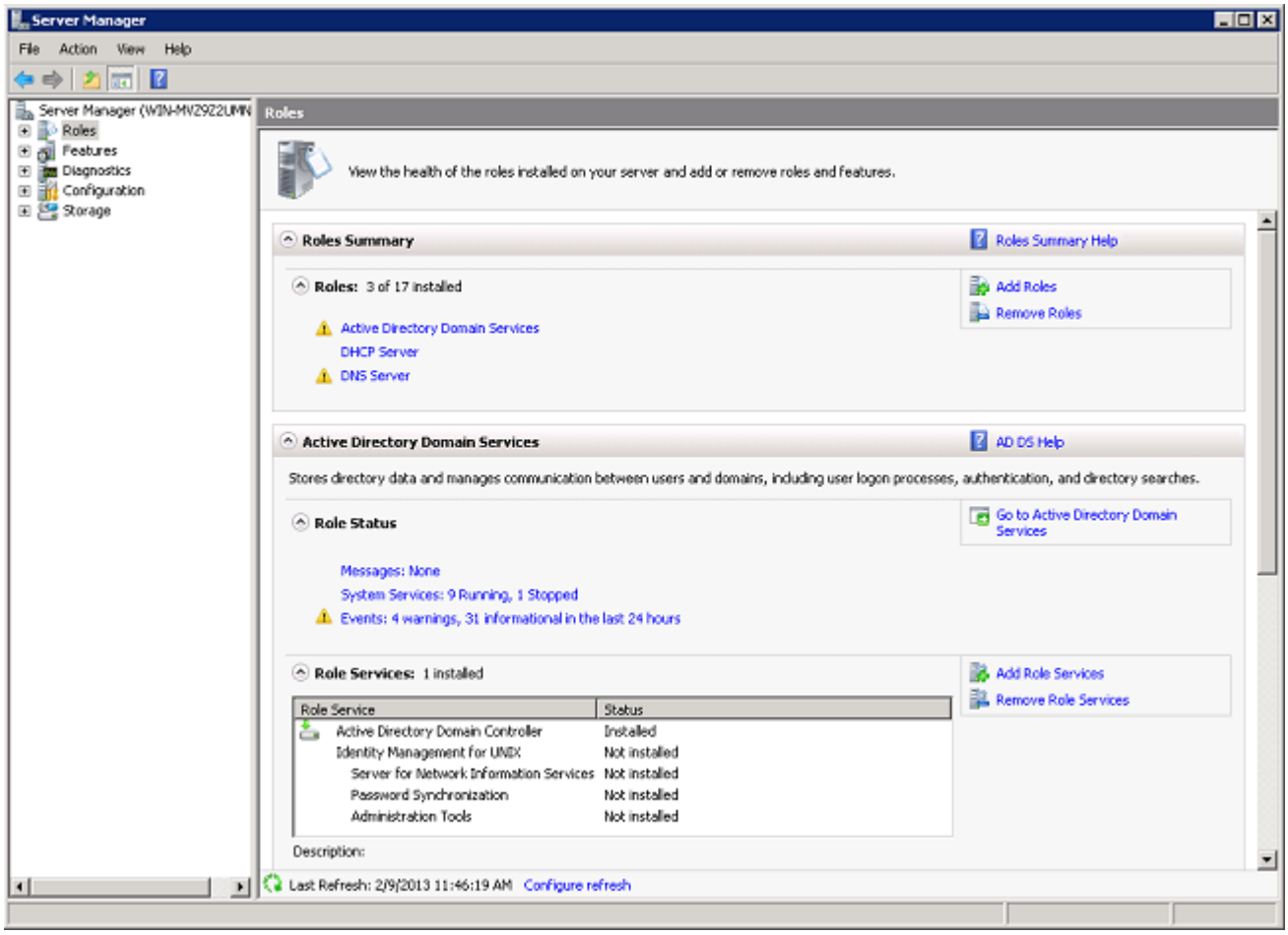
PEAP mit EAP-MS-CHAP v2 validiert den RADIUS-Server anhand des auf dem Server vorhandenen Zertifikats. Darüber hinaus muss das Serverzertifikat von einer öffentlichen Zertifizierungsstelle ausgestellt werden, die vom Clientcomputer als vertrauenswürdig eingestuft wird (d. h., das öffentliche Zertifizierungsstellenzertifikat ist bereits im Ordner der vertrauenswürdigen Stammzertifizierungsstelle im Zertifikatspeicher des Clientcomputers vorhanden).

Führen Sie die folgenden Schritte aus, um den Microsoft Windows 2008-Server als CA-Server zu konfigurieren, der das Zertifikat an den NPS ausstellt:

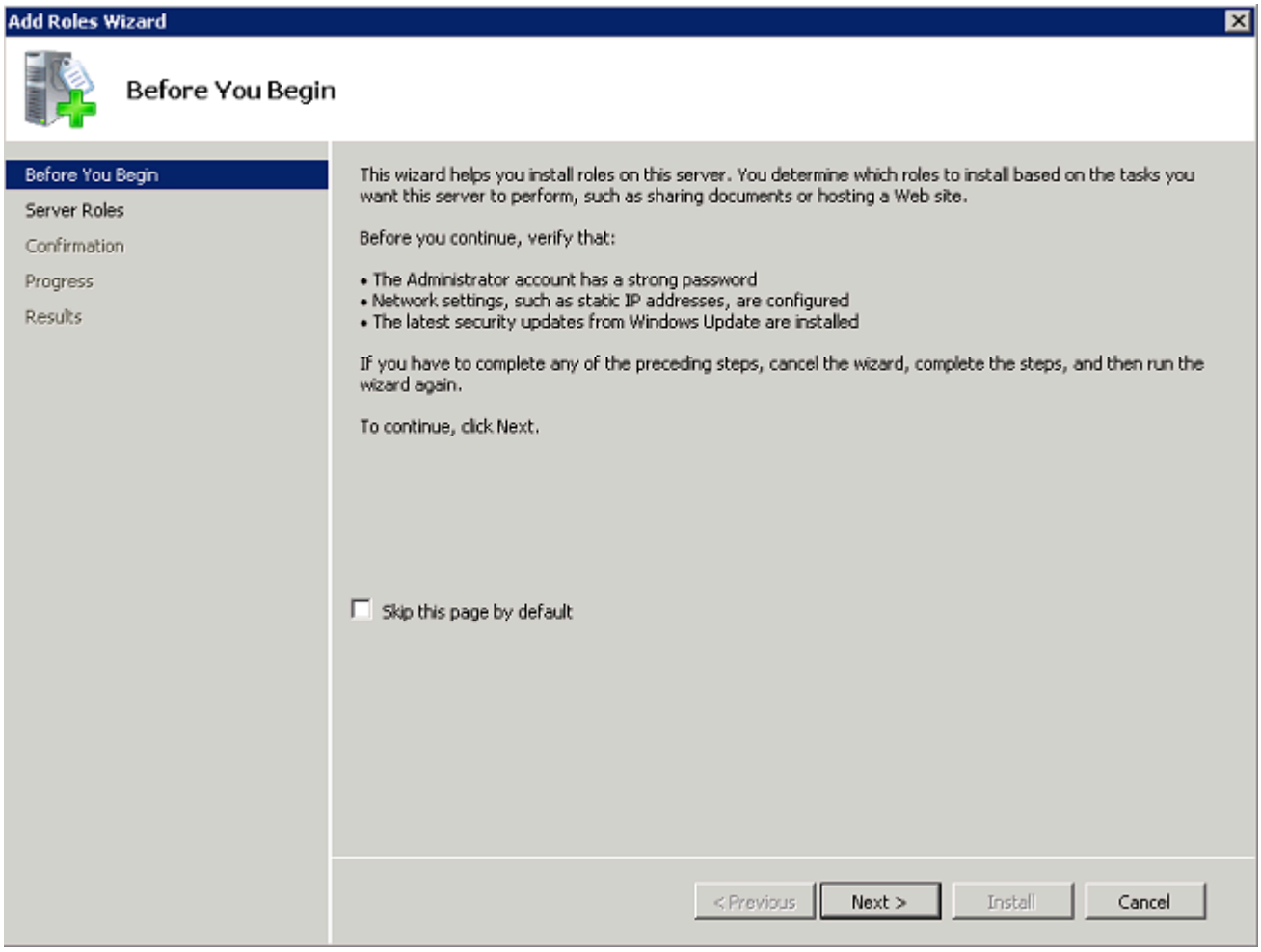
1. Klicken Sie auf Start> Server Manager.



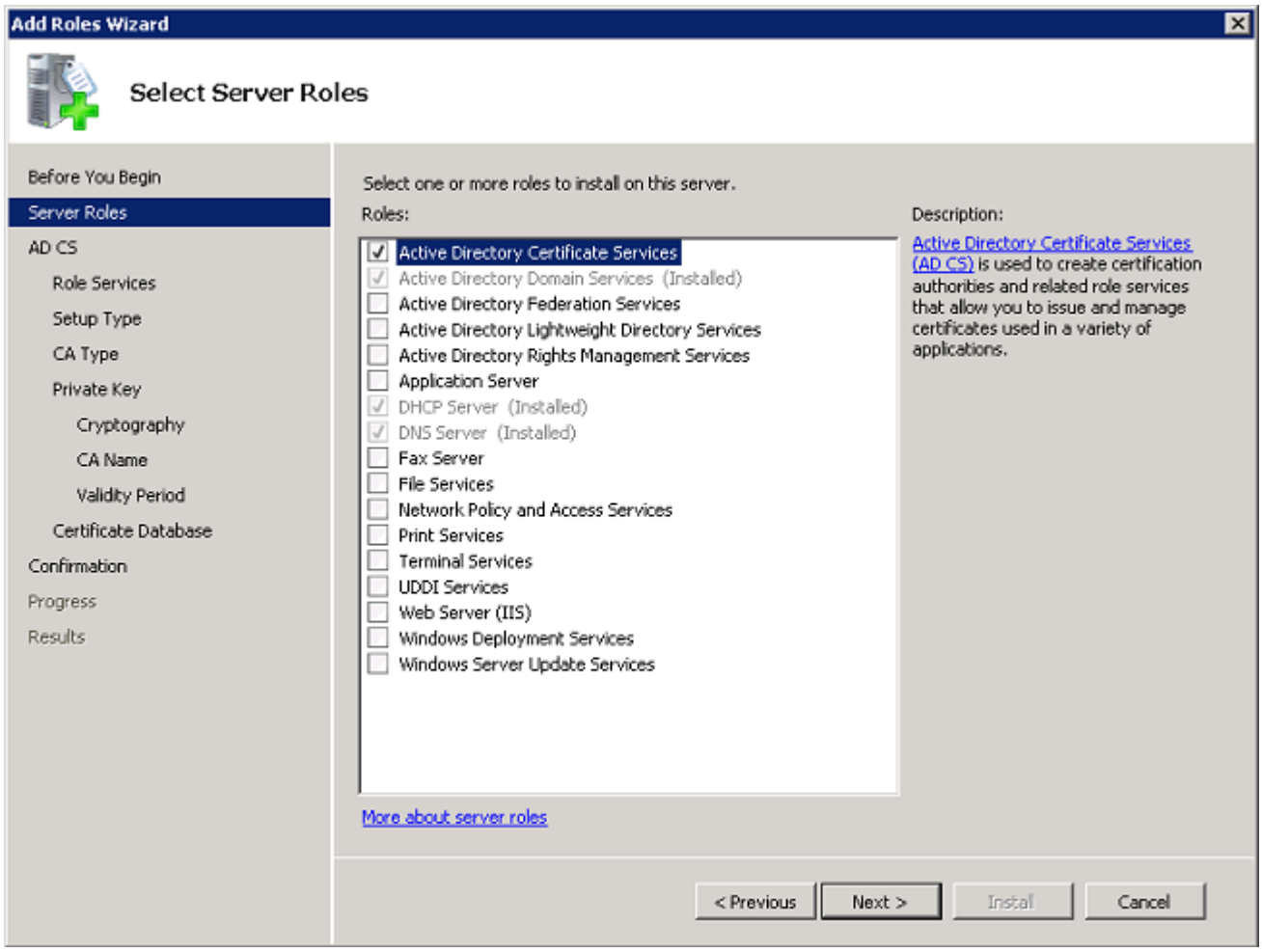
2. Klicken Sie auf Rollen > Rollen hinzufügen.



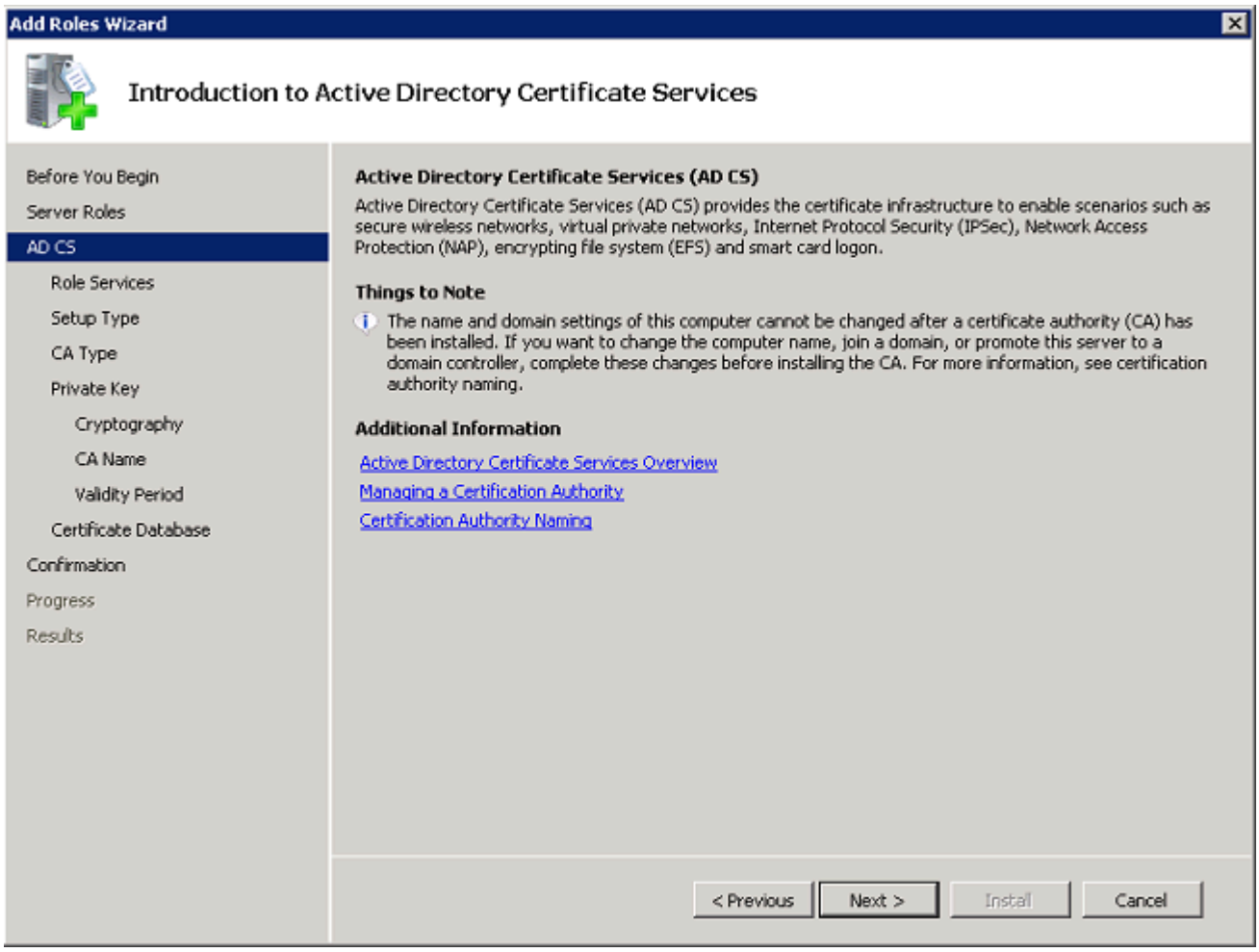
3. Klicken Sie auf Next (Weiter).



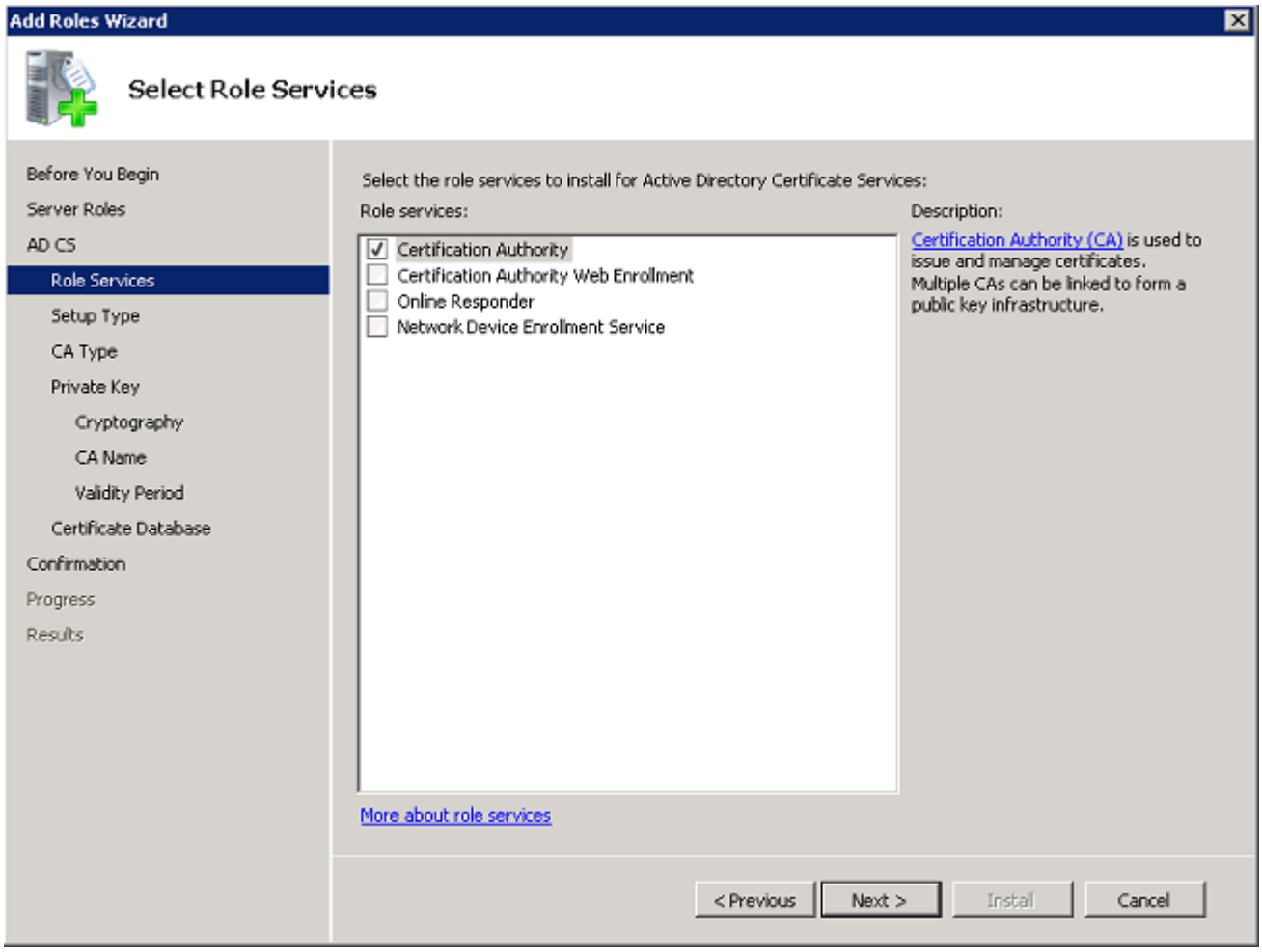
4. Wählen Sie den Dienst Active Directory-Zertifikatdienste aus, und klicken Sie auf Weiter.



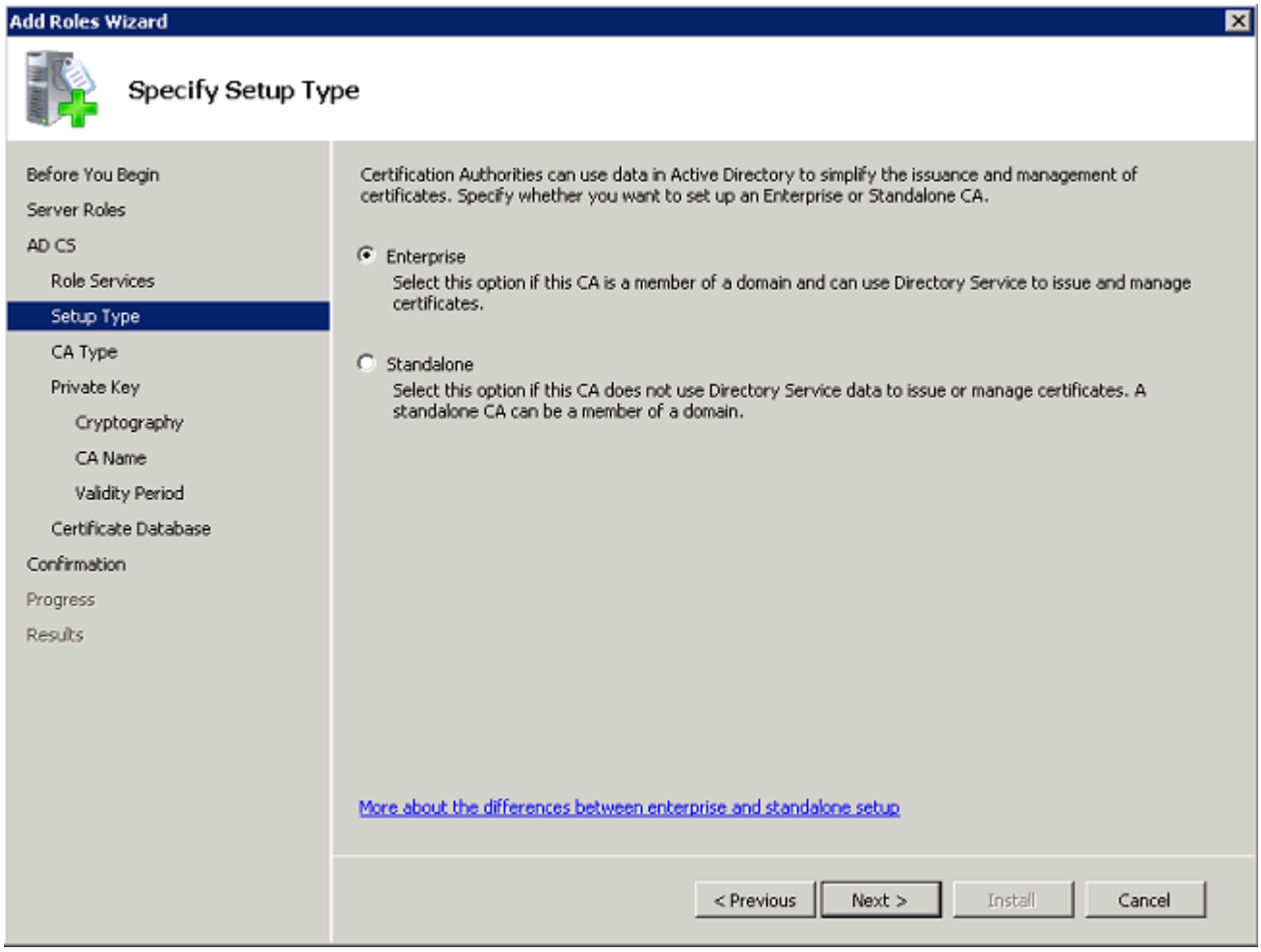
5. Überprüfen Sie die Einführung in die Active Directory-Zertifikatdienste, und klicken Sie auf Weiter.



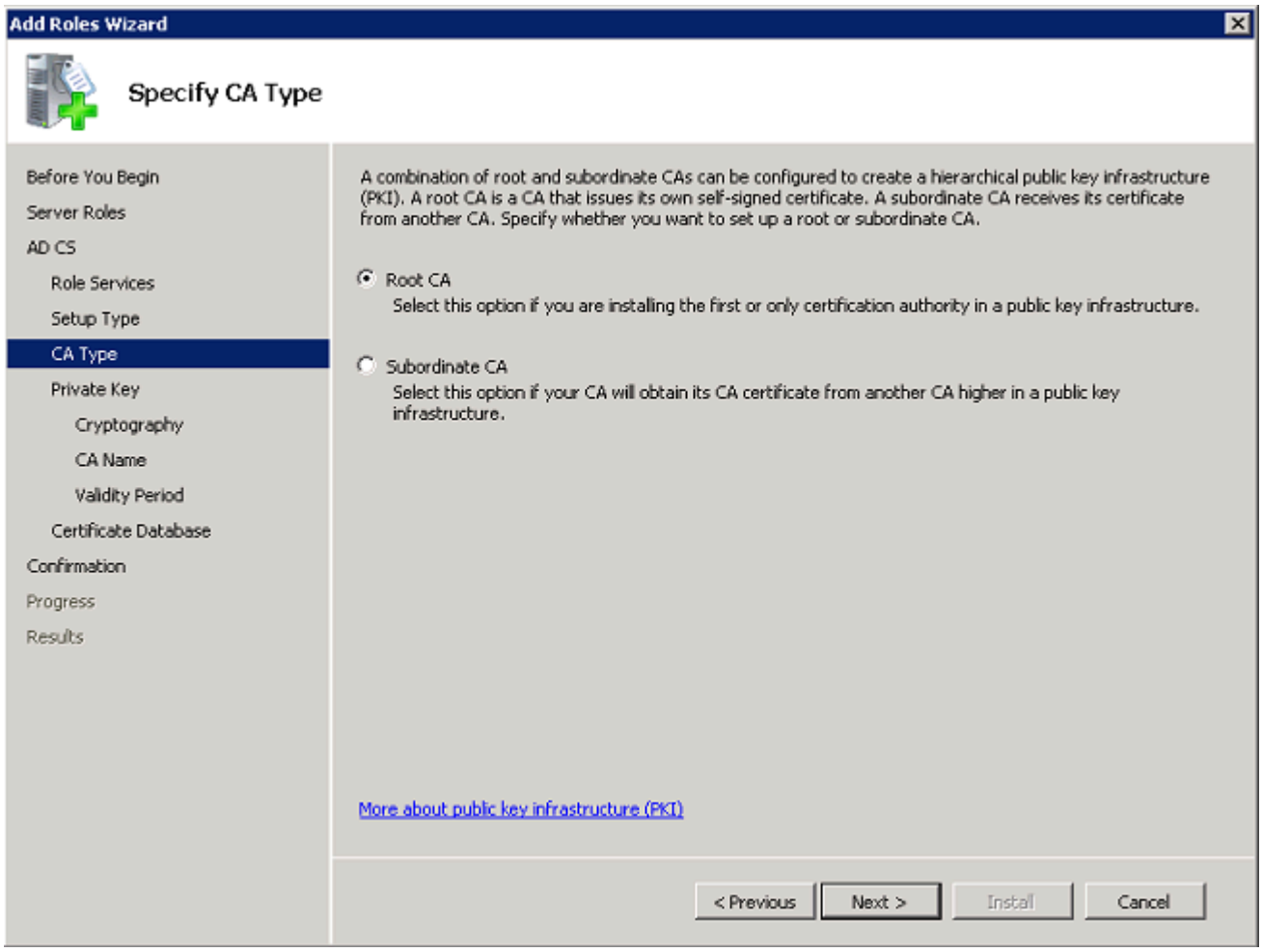
6. Wählen Sie die Zertifizierungsstelle aus, und klicken Sie auf Weiter.



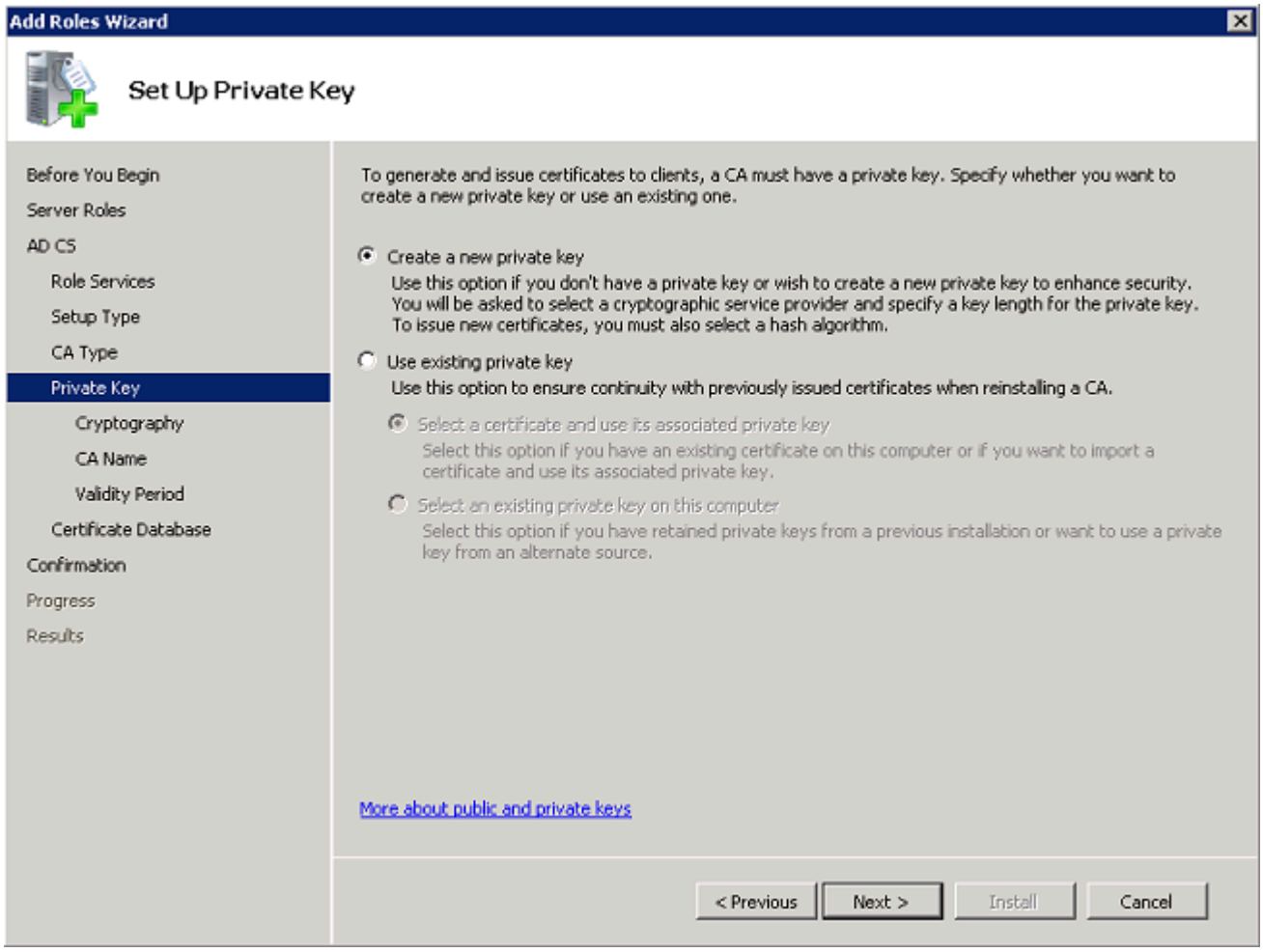
7. Wählen Sie Enterprise aus, und klicken Sie auf Weiter.



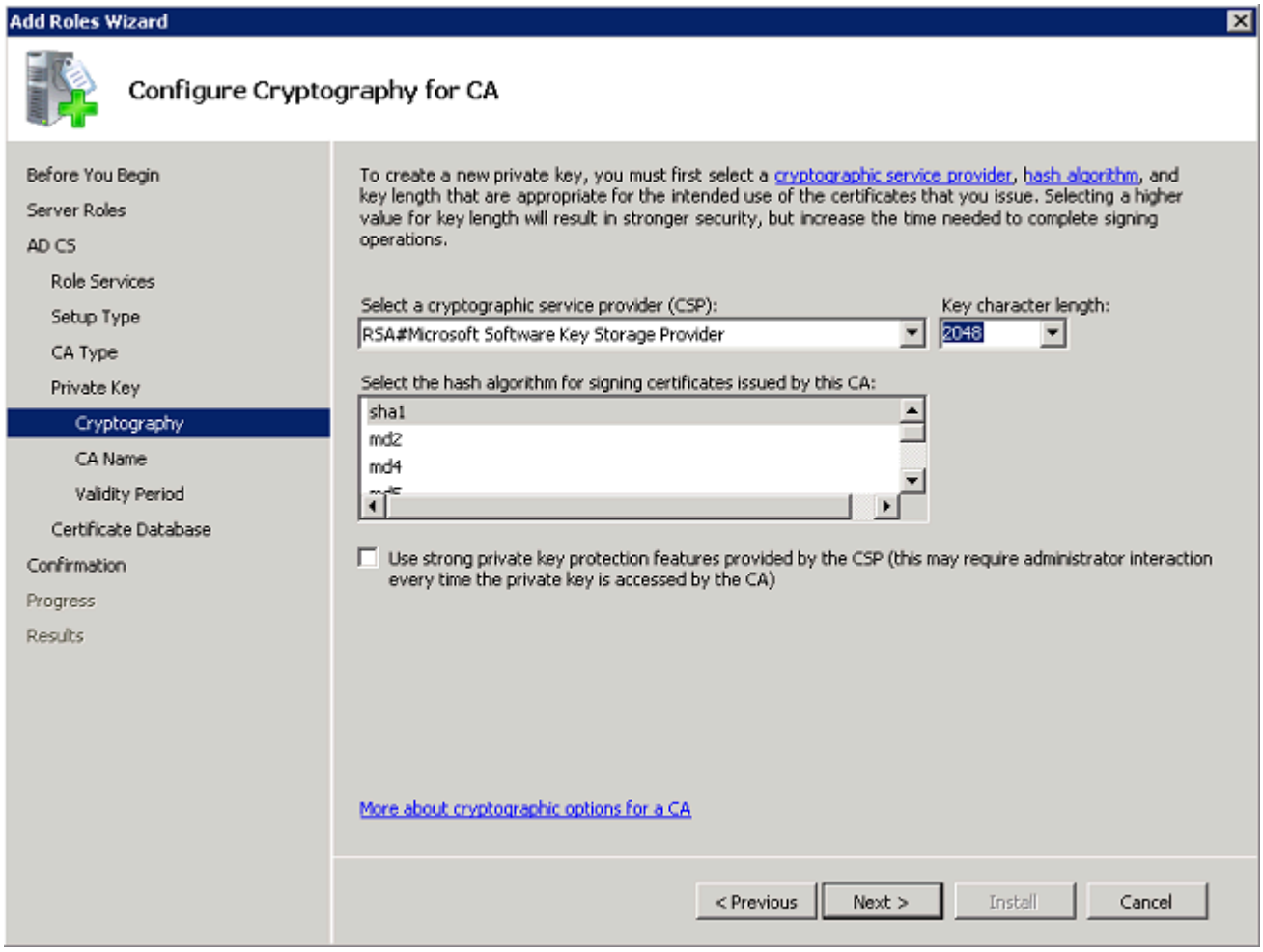
8. Wählen Sie Stammzertifizierungsstelle aus, und klicken Sie auf Weiter.



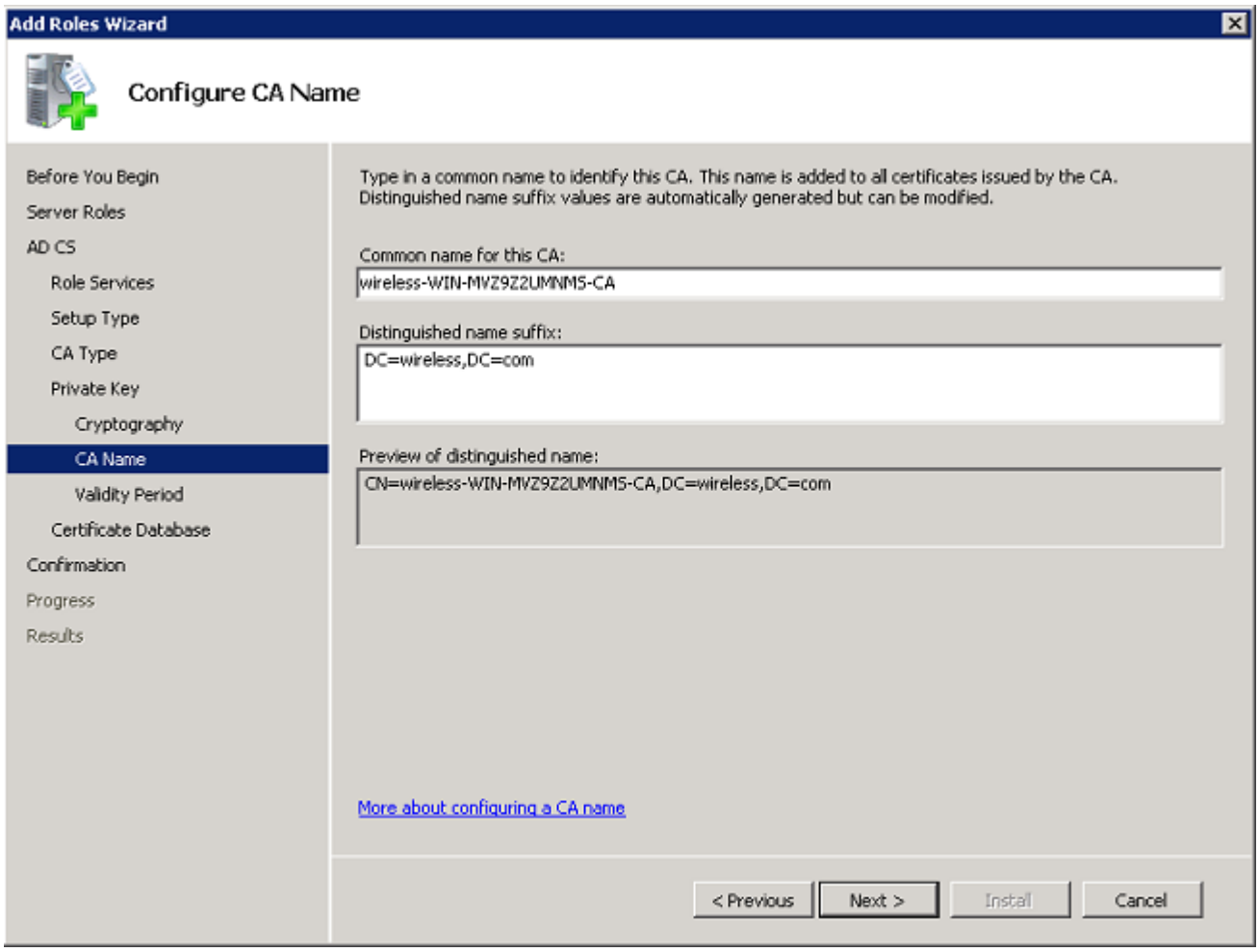
9. Wählen Sie Neuen privaten Schlüssel erstellen aus, und klicken Sie auf Weiter.



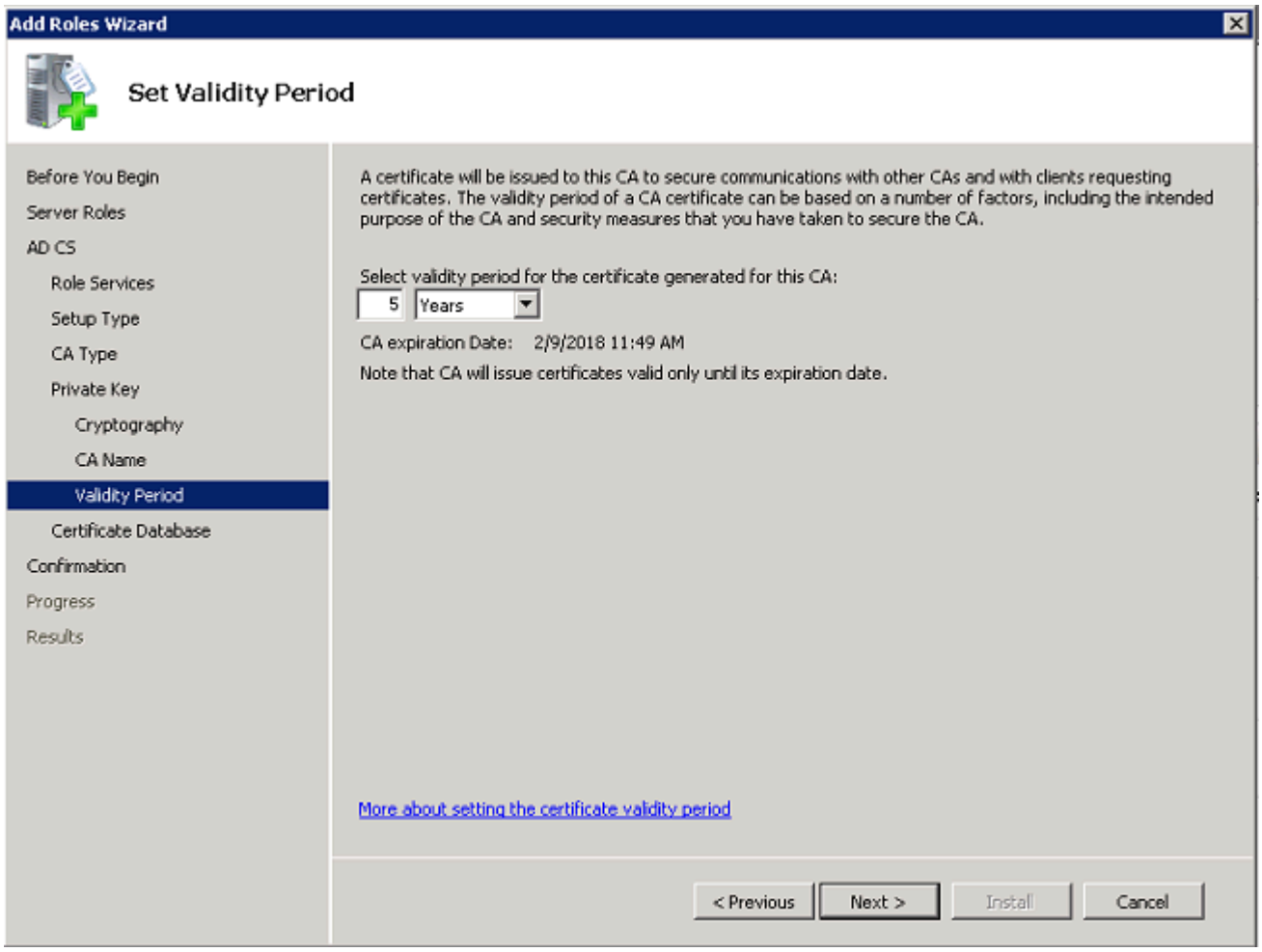
10. Klicken Sie unter "Verschlüsselung für CA konfigurieren" auf Weiter.



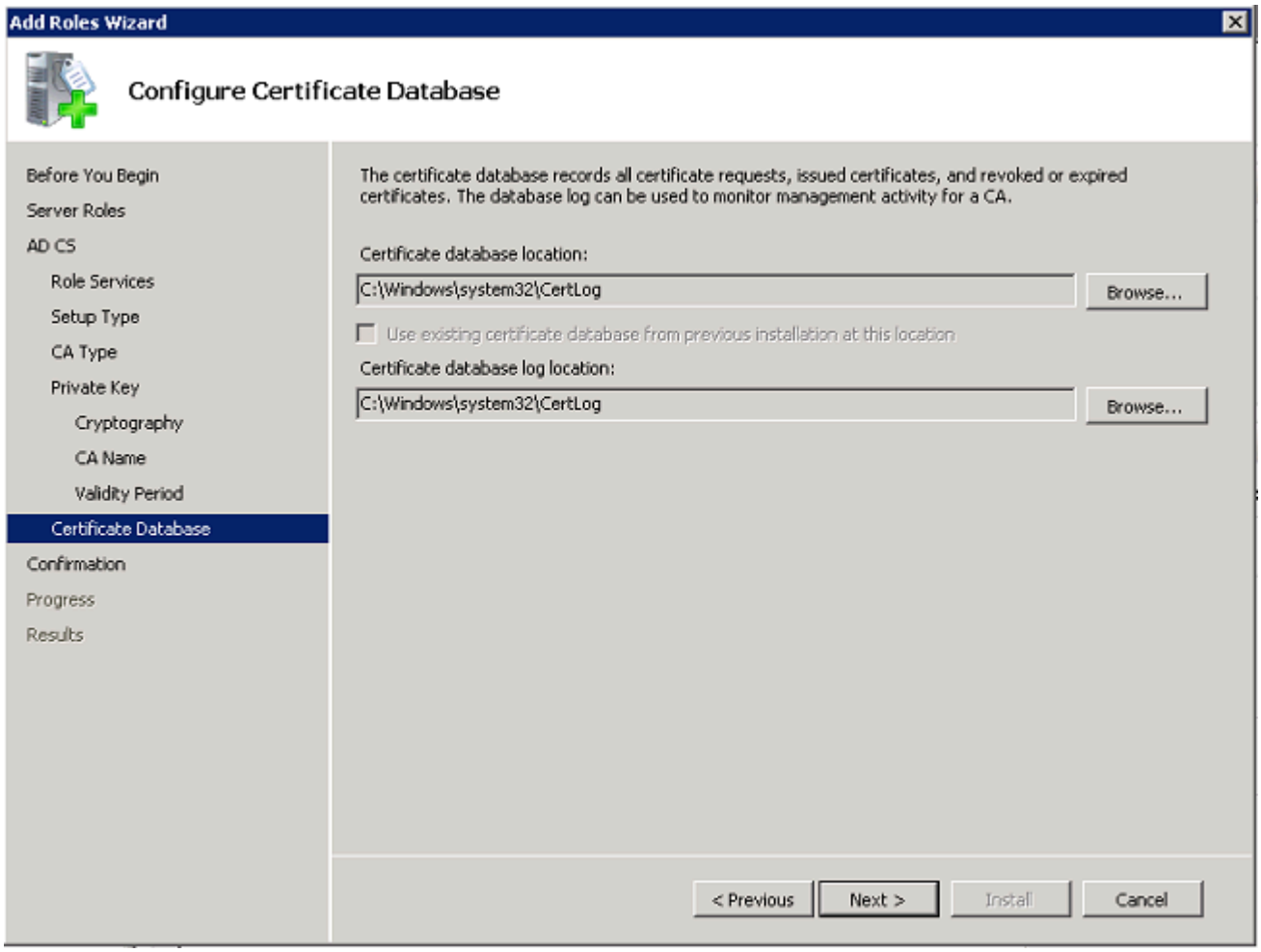
11. Klicken Sie auf Weiter, um den standardmäßigen allgemeinen Namen für diese Zertifizierungsstelle zu akzeptieren.



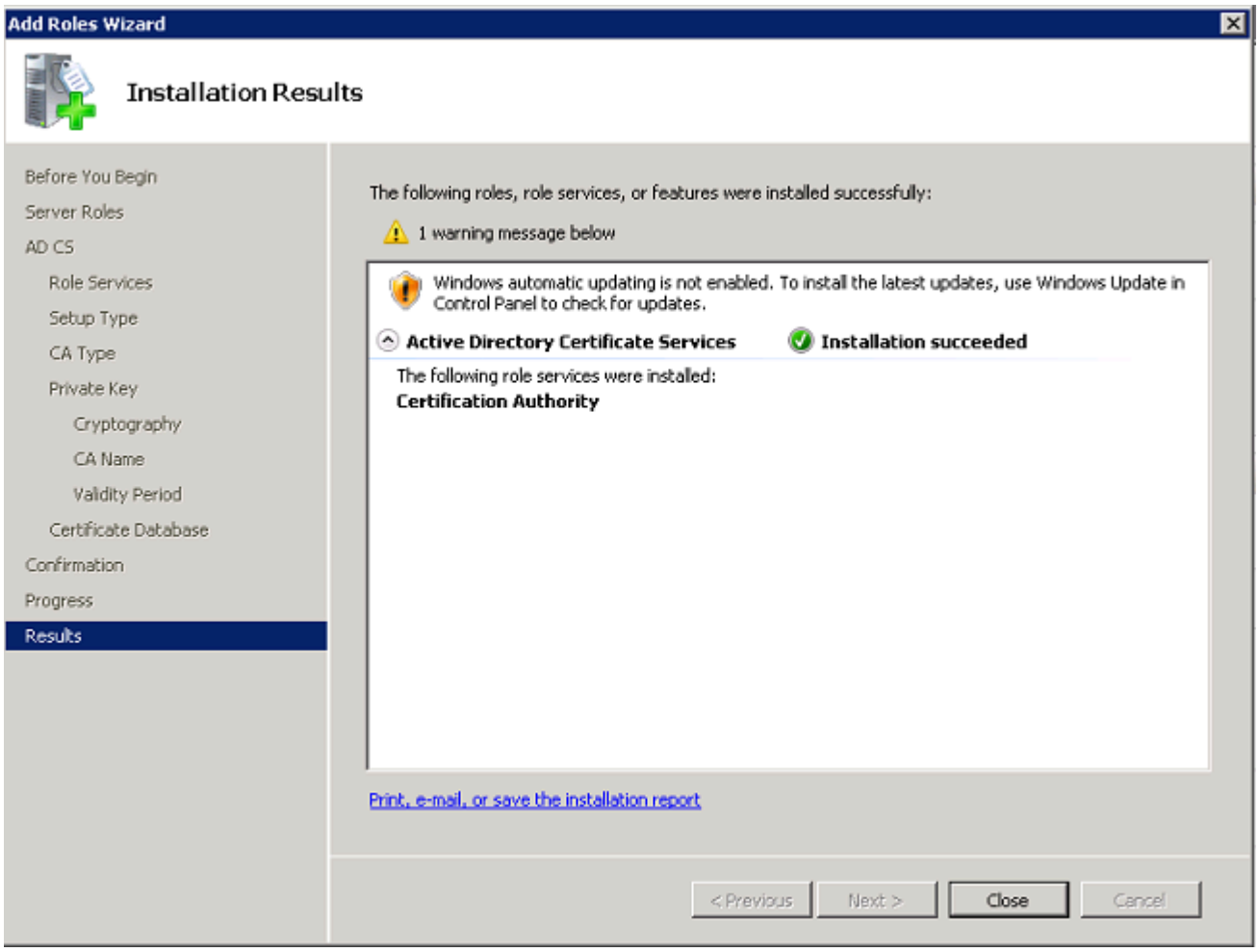
12. Wählen Sie den Zeitraum aus, für den dieses Zertifizierungsstellenzertifikat gültig ist, und klicken Sie auf Weiter.



13. Klicken Sie auf Weiter, um den Standardspeicherort für die Zertifikatsdatenbank zu übernehmen.



14. Überprüfen Sie die Konfiguration, und klicken Sie auf Installieren, um die Active Directory-Zertifikatdienste zu starten.

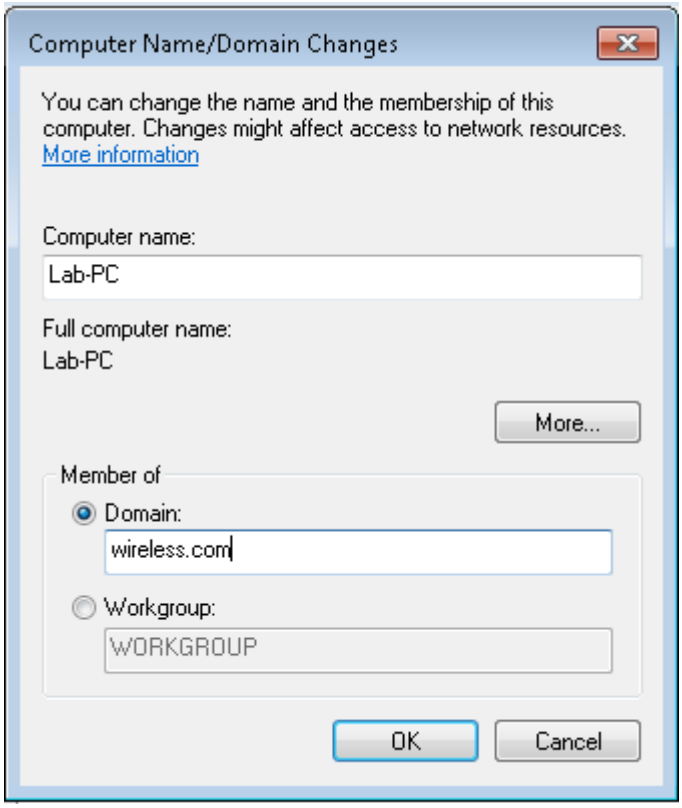


15. Klicken Sie nach Abschluss der Installation auf Schließen.

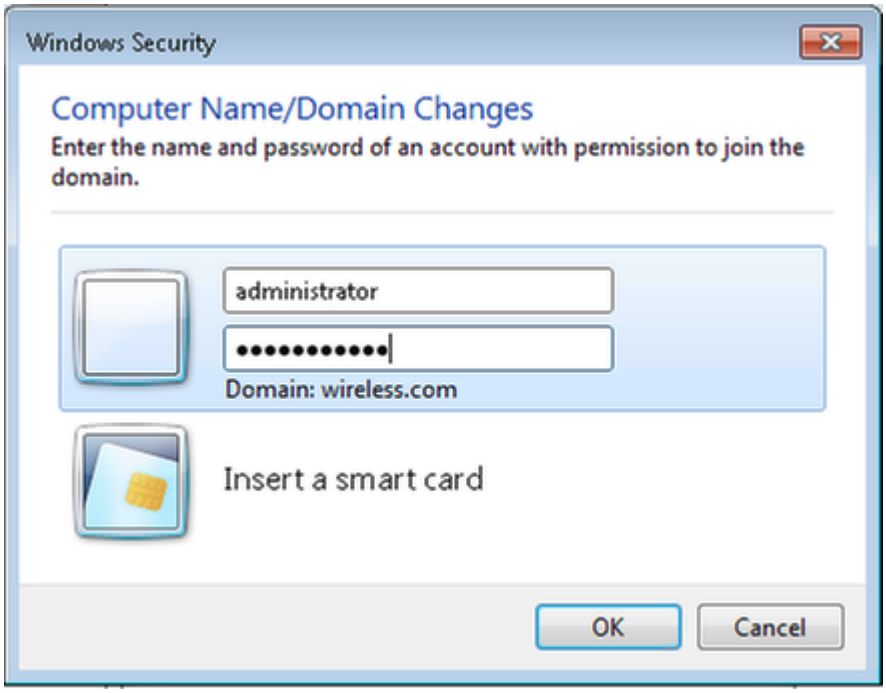
Clients mit der Domäne verbinden

Führen Sie die folgenden Schritte aus, um die Clients mit dem kabelgebundenen Netzwerk zu verbinden und die domänenspezifischen Informationen aus der neuen Domäne herunterzuladen:

1. Verbinden Sie die Clients über ein gerades Ethernetkabel mit dem kabelgebundenen Netzwerk.
2. Starten Sie den Client, und melden Sie sich mit dem Benutzernamen und dem Kennwort des Clients an.
3. Klicken Sie auf Start>Ausführen, geben Sie cmd ein, und klicken Sie auf OK.
4. Geben Sie an der Eingabeaufforderung ipconfig ein, und klicken Sie auf Enter, um zu überprüfen, ob DHCP korrekt funktioniert und ob der Client eine IP-Adresse vom DHCP-Server erhalten hat.
5. Um den Client mit der Domäne zu verbinden, klicken Sie auf Start, klicken Sie mit der rechten Maustaste auf Computer, wählen Sie Eigenschaften, und wählen Sie Einstellungen ändern unten rechts aus.
6. Klicken Sie auf Ändern.
7. Klicken Sie auf Domäne, geben Sie den Domänennamen (in diesem Beispiel Wireless) ein, und klicken Sie auf OK.

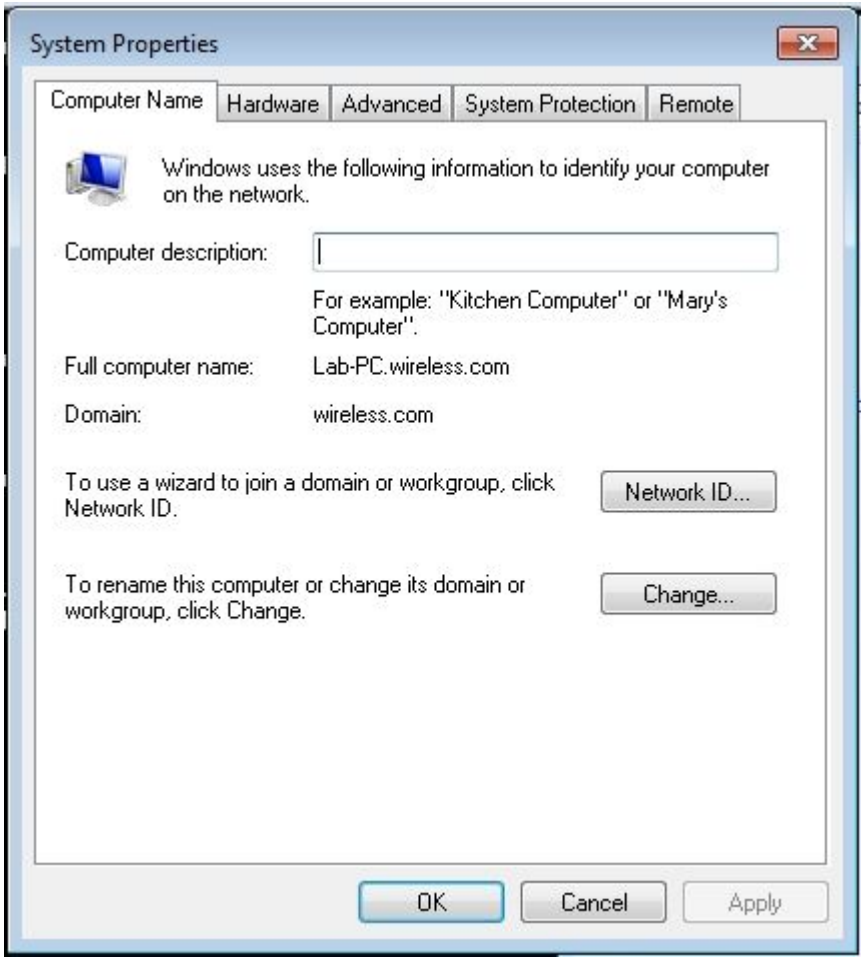


8. Geben Sie den Benutzernamen Administrator und das Kennwort für die Domäne ein, der der Client beitritt. Dies ist das Administratorkonto im Active Directory auf dem Server.

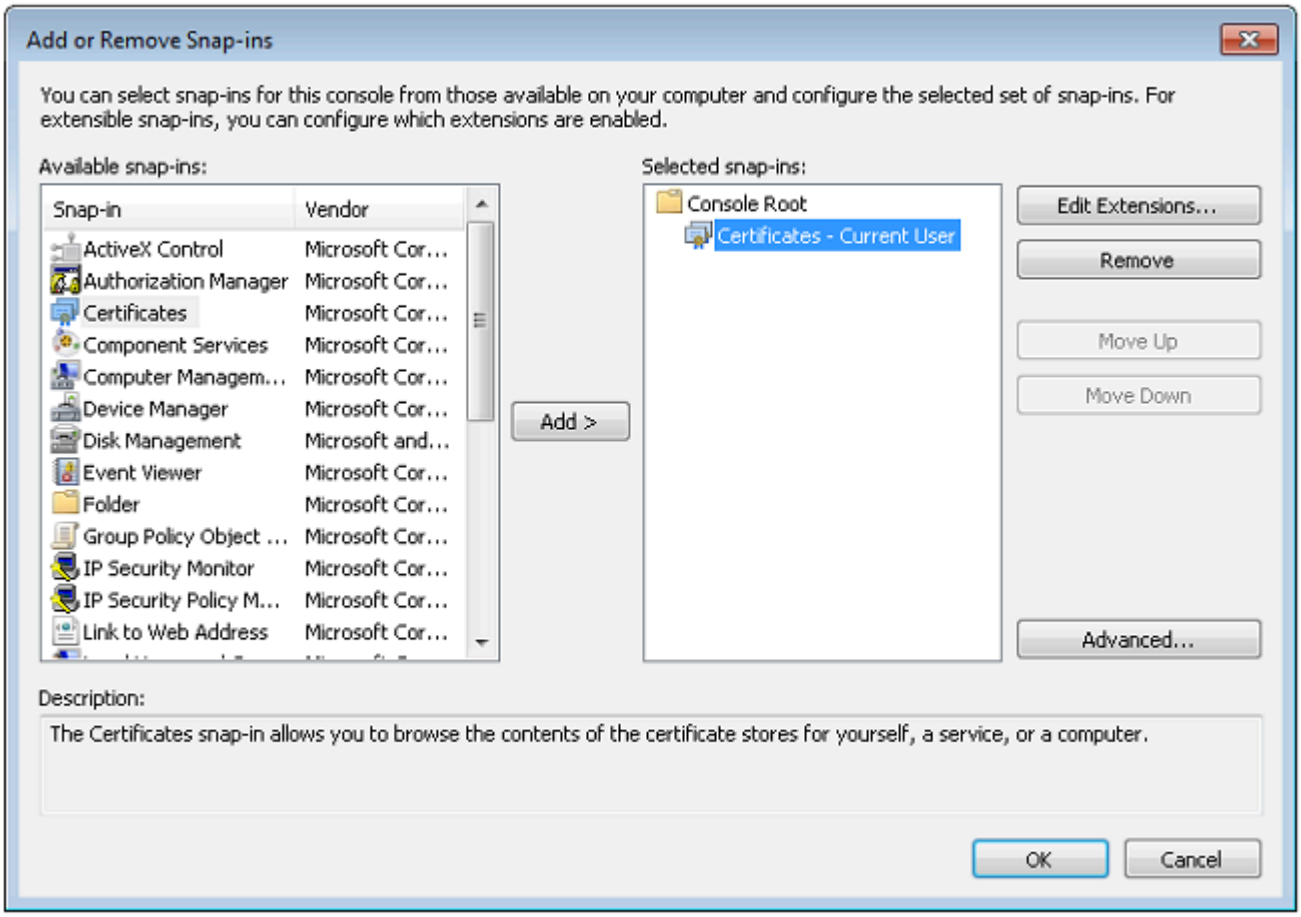


9. Klicken Sie auf OK, und klicken Sie erneut auf OK.

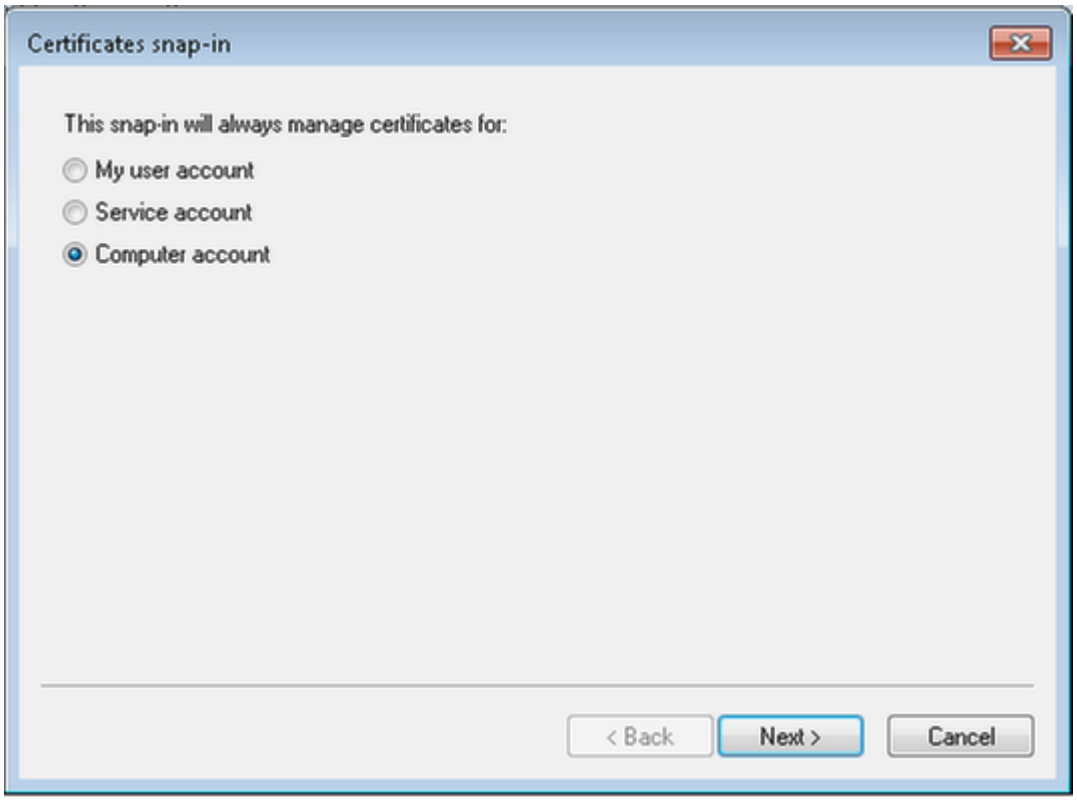
10. Klicken Sie auf Schließen>Jetzt neu starten, um den Computer neu zu starten.
11. Melden Sie sich nach dem Neustart des Computers mit folgenden Funktionen an: Benutzername = Administrator; Password = <Domänenkennwort>; Domäne = Wireless.
12. Klicken Sie auf Start, klicken Sie mit der rechten Maustaste auf Computer, wählen Sie Eigenschaften, und wählen Sie Einstellungen ändern unten rechts aus, um zu überprüfen, ob Sie sich in der Wireless-Domäne befinden.
13. Der nächste Schritt besteht darin, zu überprüfen, ob der Client das Zertifizierungsstellenzertifikat (trust) vom Server erhalten hat.



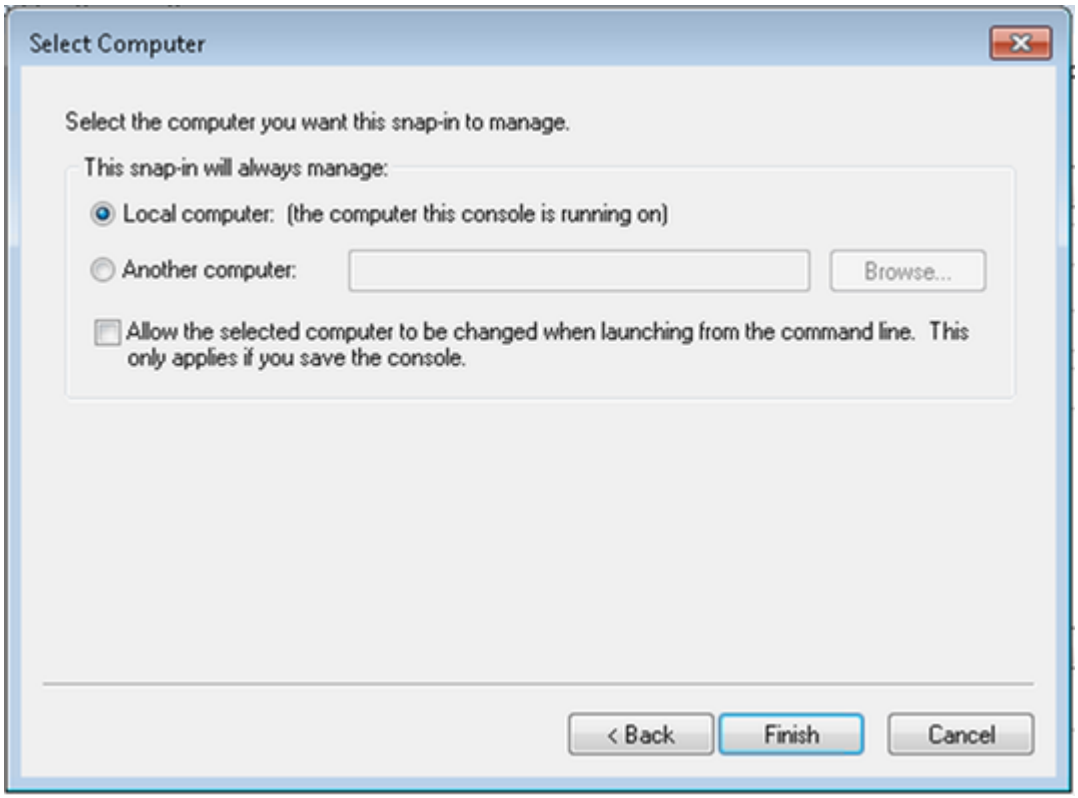
14. Klicken Sie auf Start, geben Sie mmc ein, und drücken Sie die Eingabetaste.
15. Klicken Sie auf Datei, und klicken Sie auf Snap-In hinzufügen/entfernen.
16. Wählen Sie Zertifikate aus, und klicken Sie auf Hinzufügen.



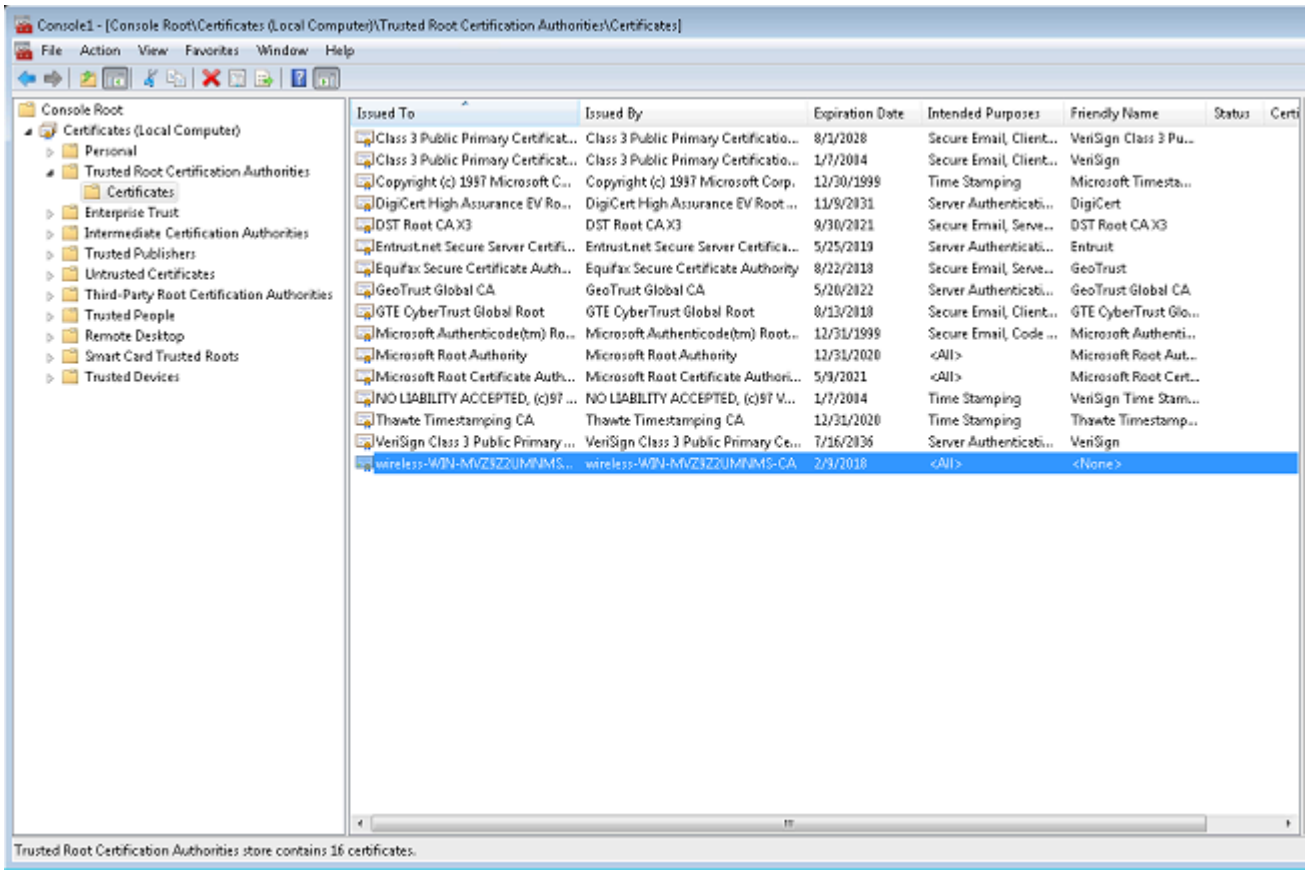
17. Klicken Sie auf Computerkonto, und klicken Sie auf Weiter.



18. Klicken Sie auf Lokaler Computer, und klicken Sie auf Weiter.



19. Klicken Sie auf OK.
20. Erweitern Sie die Ordner Zertifikate (Lokaler Computer) und Vertrauenswürdige Stammzertifizierungsstellen, und klicken Sie auf Zertifikate. Suchen Sie in der Liste nach einem Zertifikat für die Wireless-Domäne-CA. In diesem Beispiel heißt das Zertifizierungsstellenzertifikat wireless-WIN-MVZ9Z2UMNMS-CA.

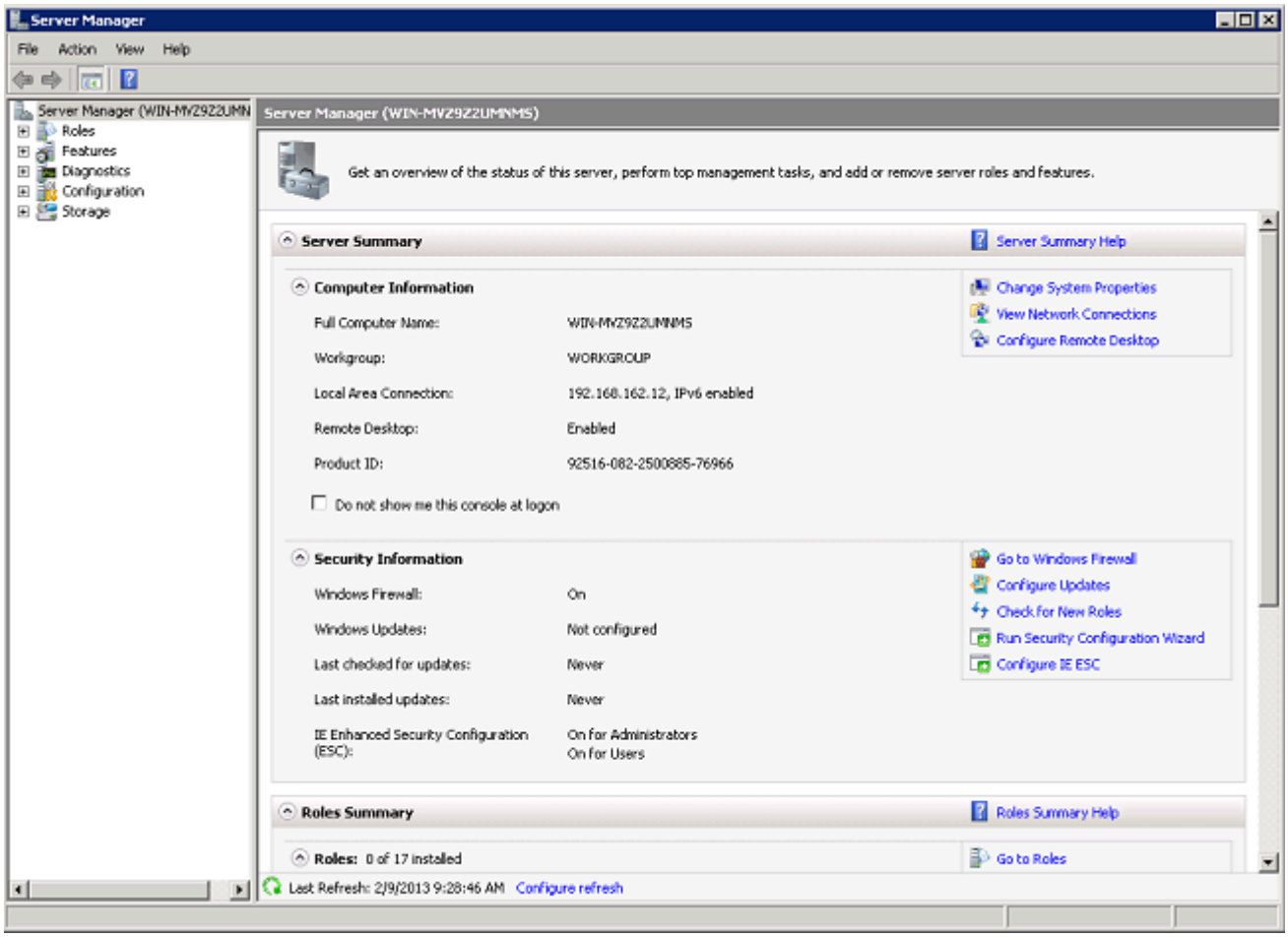


21. Wiederholen Sie dieses Verfahren, um der Domäne weitere Clients hinzuzufügen.

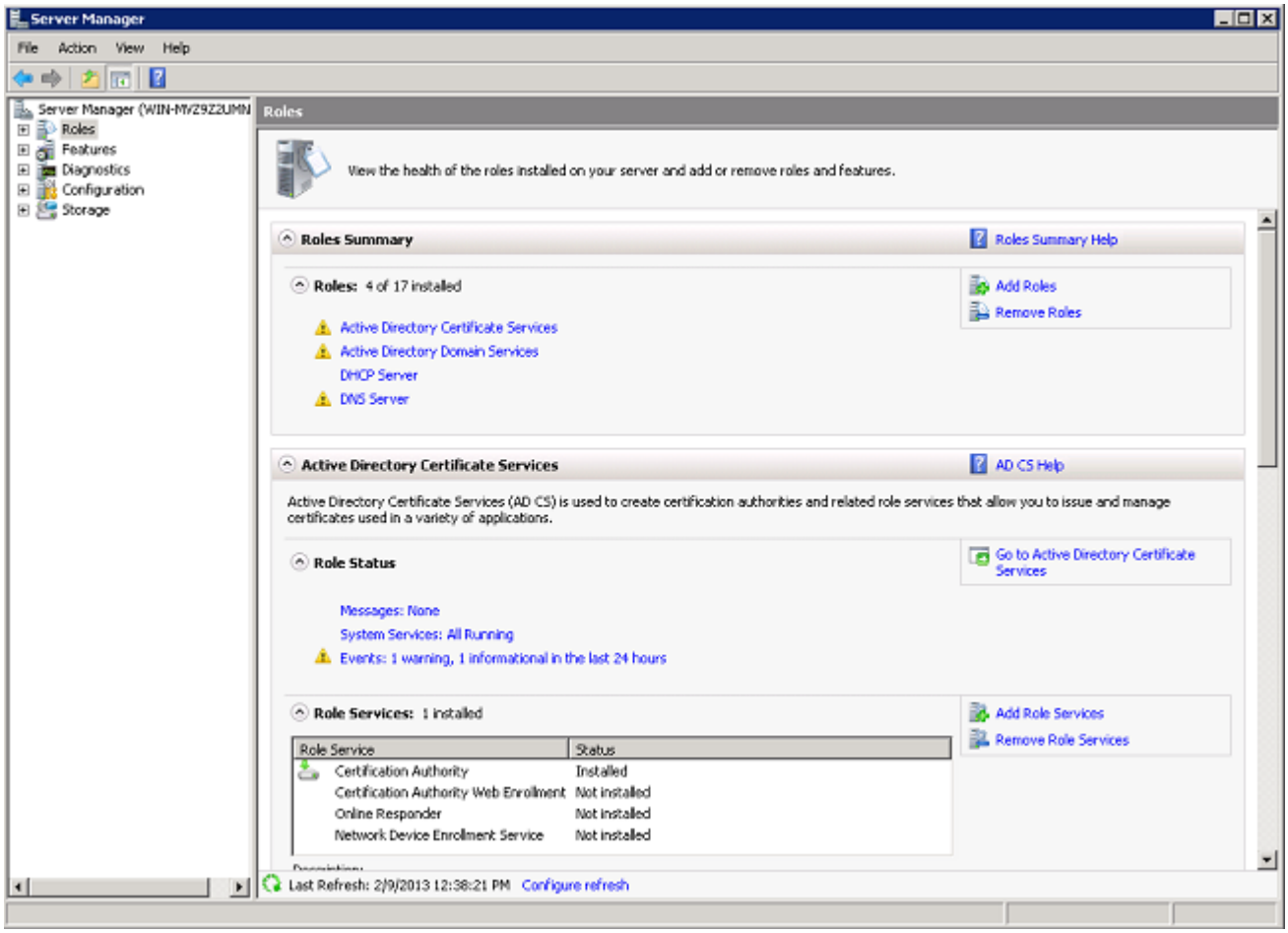
Installieren des Netzwerkrichtlinienservers auf dem Microsoft Windows 2008 Server

In dieser Konfiguration wird der NPS als RADIUS-Server verwendet, um Wireless-Clients mit PEAP-Authentifizierung zu authentifizieren. Führen Sie die folgenden Schritte aus, um NPS auf dem Microsoft Windows 2008-Server zu installieren und zu konfigurieren:

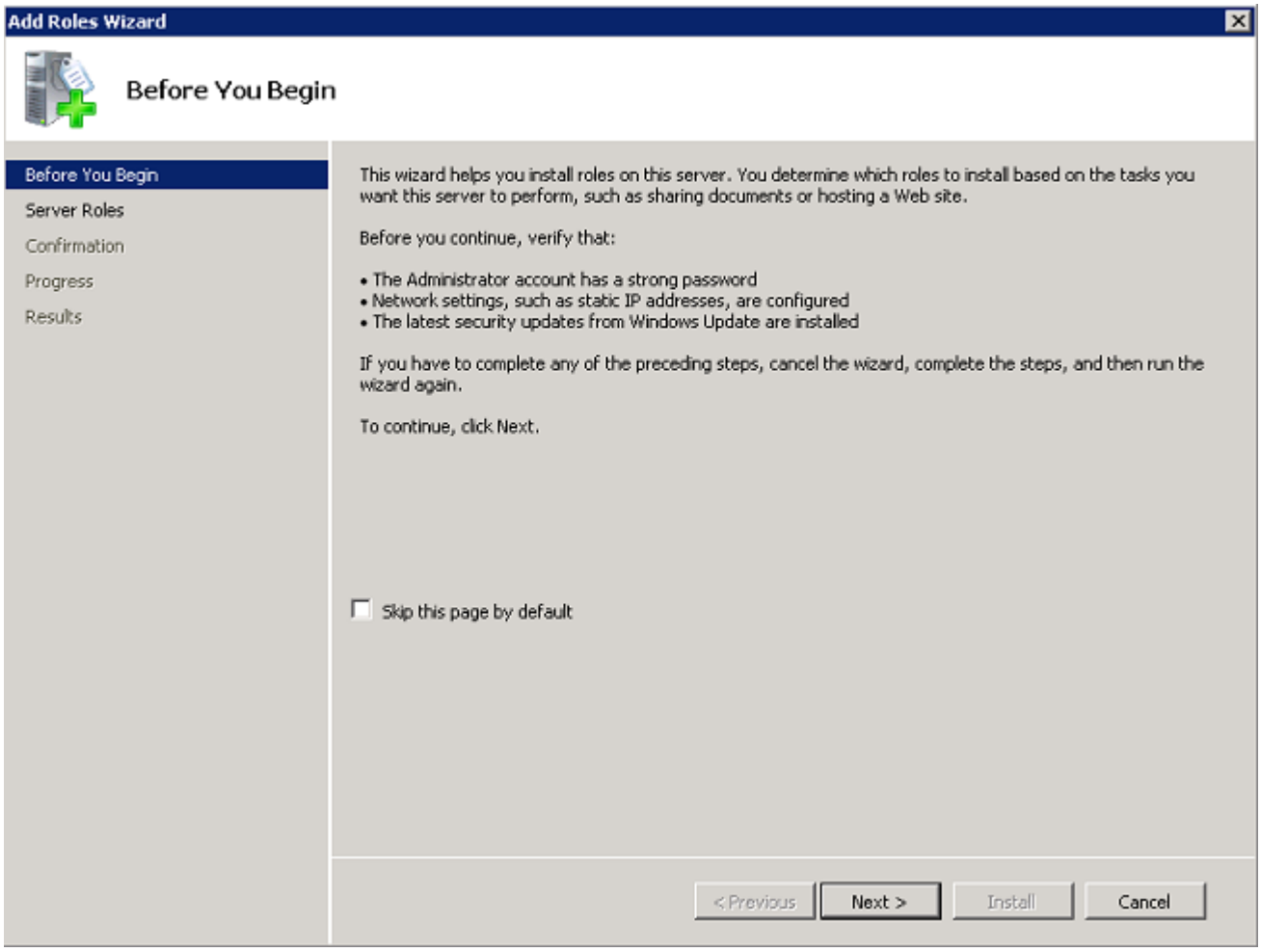
1. Klicken Sie auf Start> Server Manager.



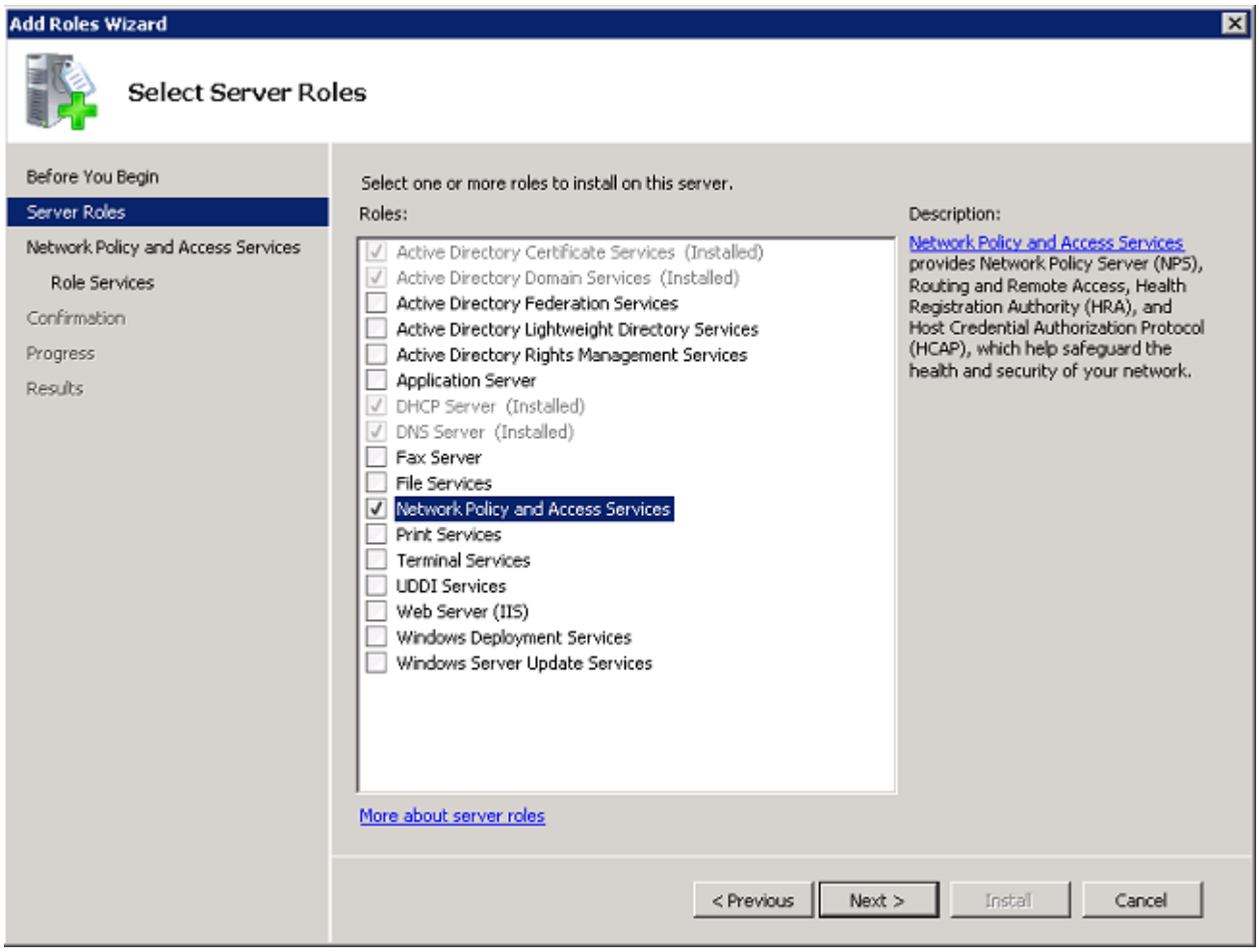
2. Klicken Sie auf Rollen > Rollen hinzufügen.



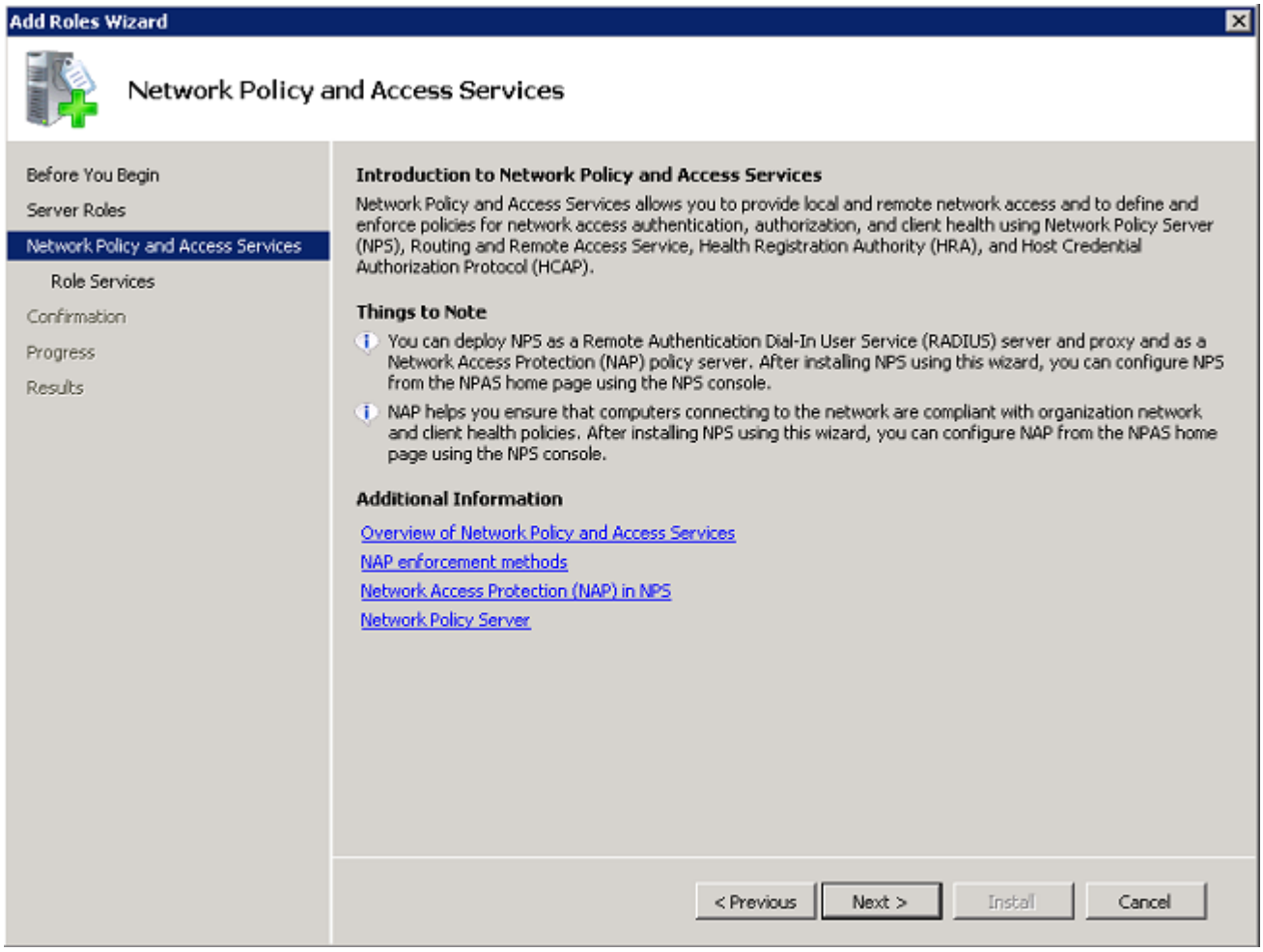
3. Klicken Sie auf Next (Weiter).



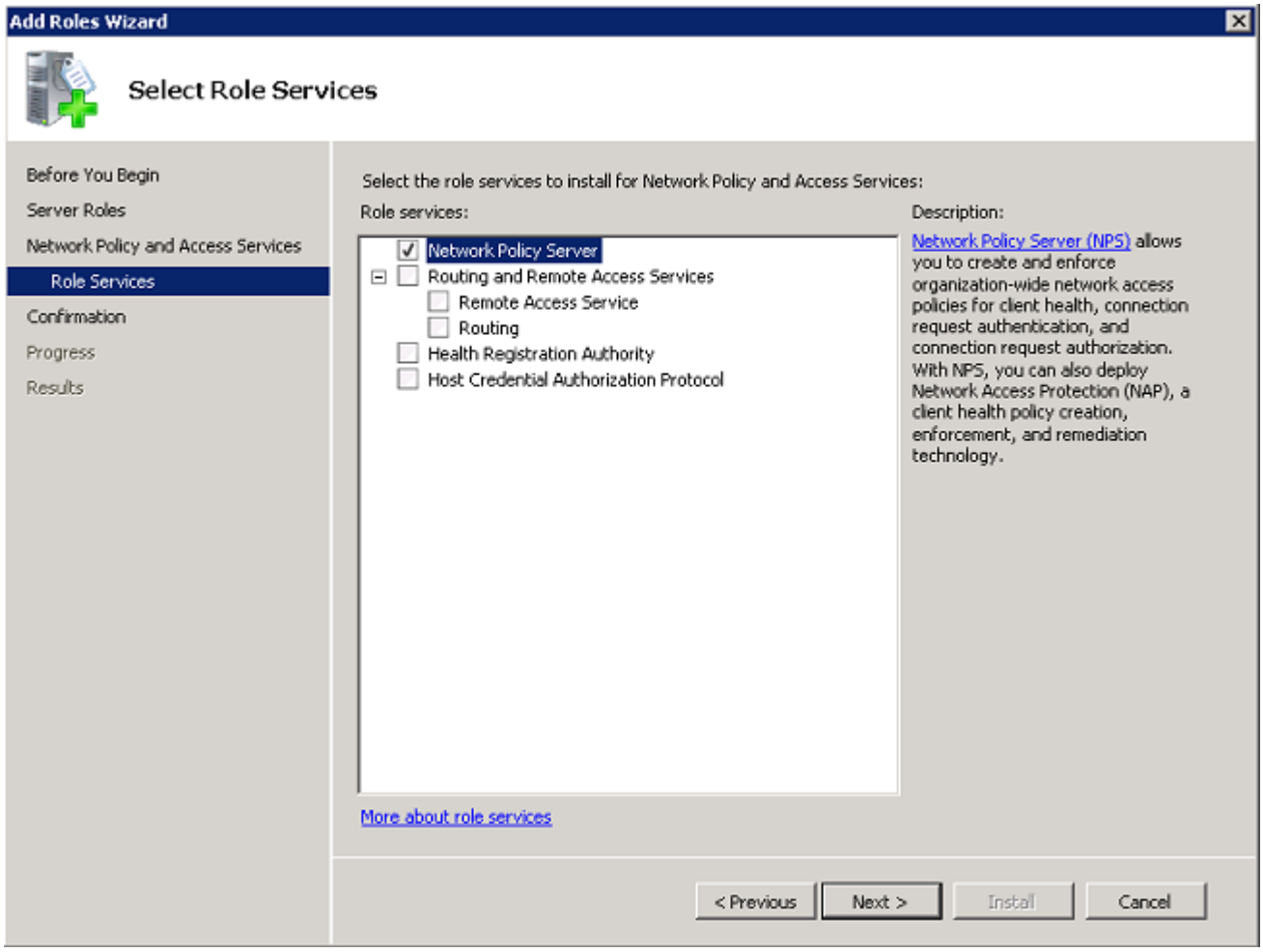
4. Wählen Sie den Dienst Netzwerkrichtlinie und Zugriffsdienste aus, und klicken Sie auf Weiter.



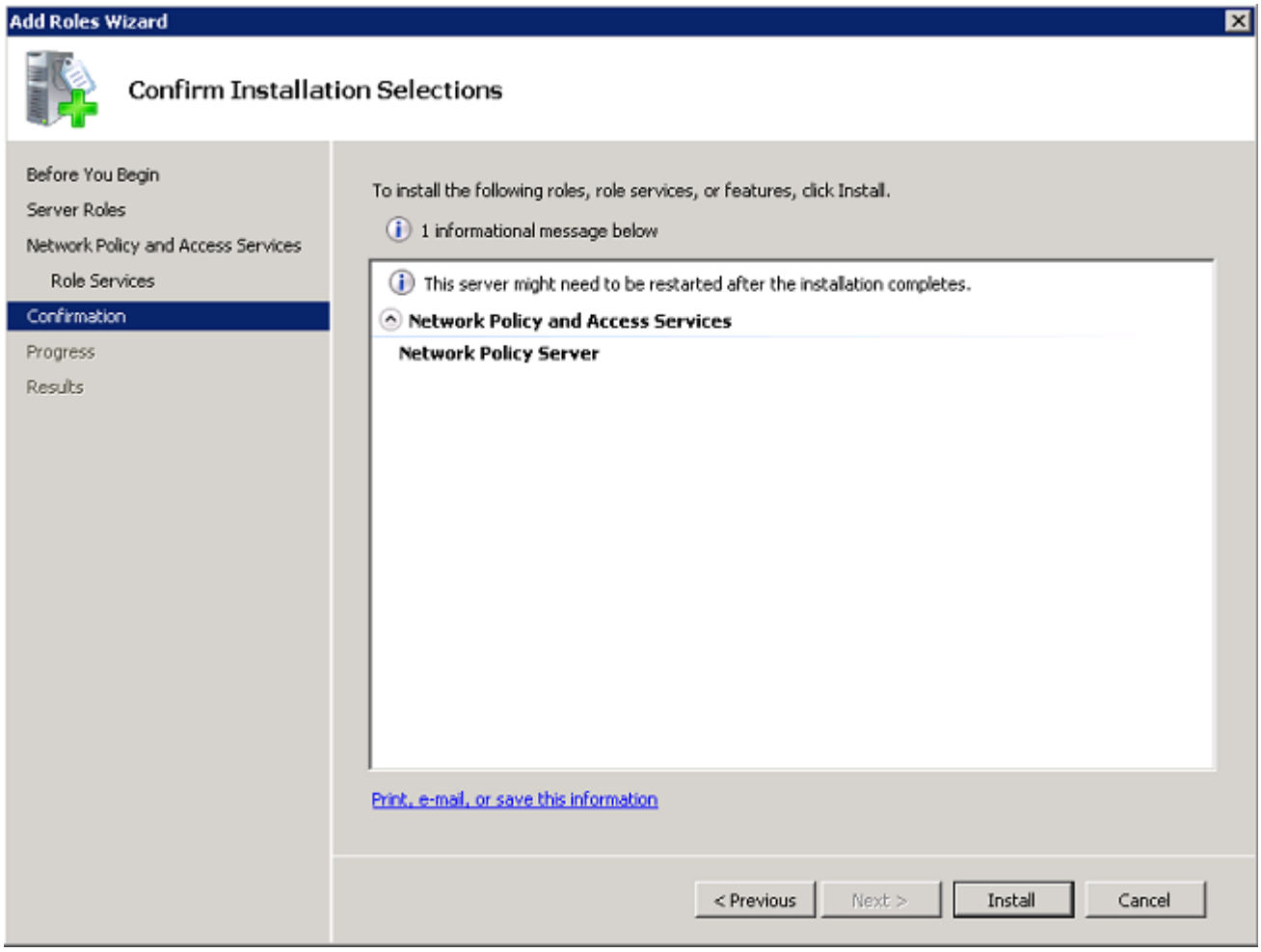
5. Lesen Sie die Einführung in Netzwerkrichtlinien und Zugriffsservices, und klicken Sie auf Weiter.



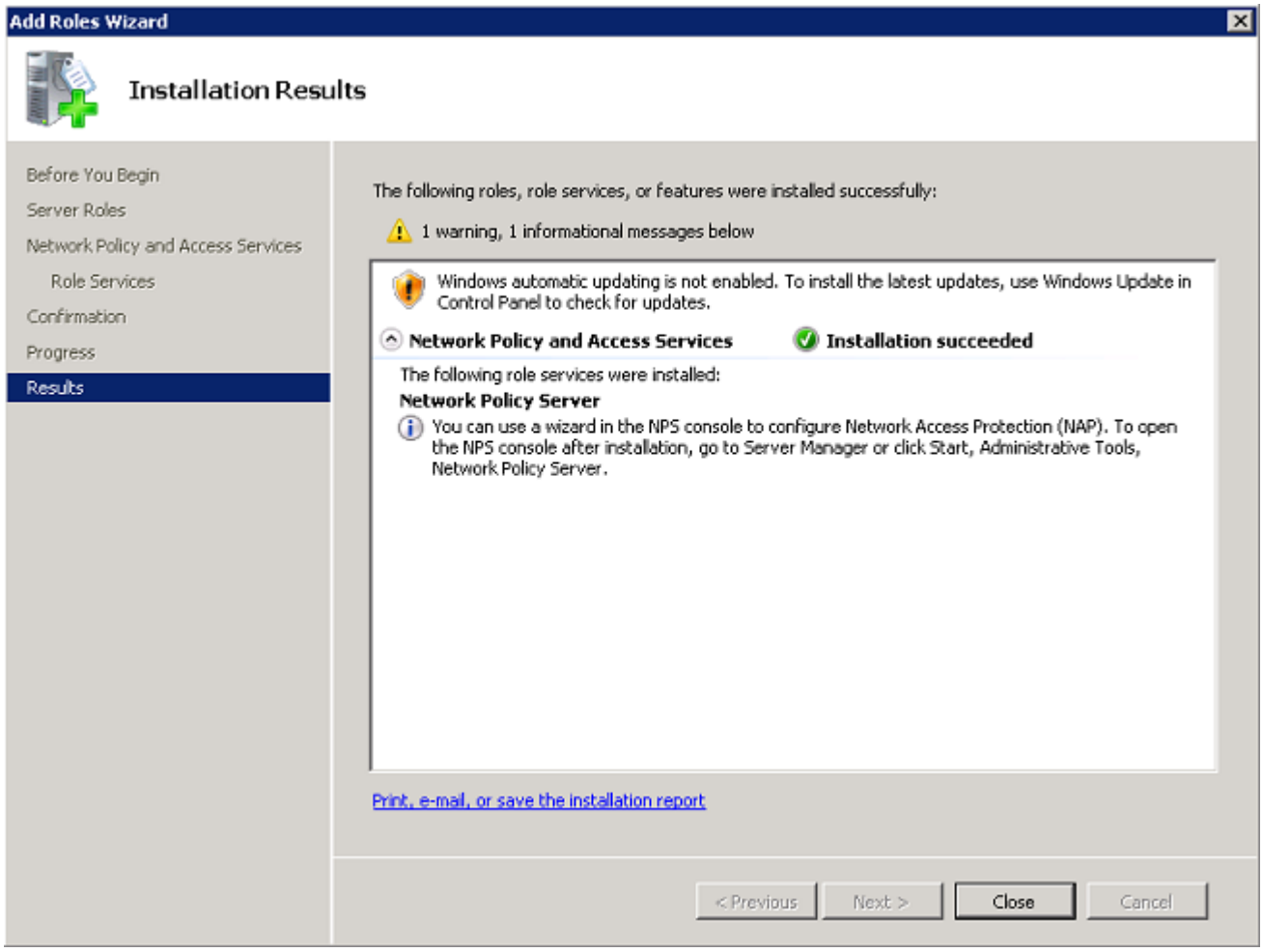
6. Wählen Sie Netzwerkrichtlinienserver aus, und klicken Sie auf Weiter.



7. Überprüfen Sie die Bestätigung, und klicken Sie auf Installieren.



Nach Abschluss der Installation wird ein ähnlicher Bildschirm angezeigt.

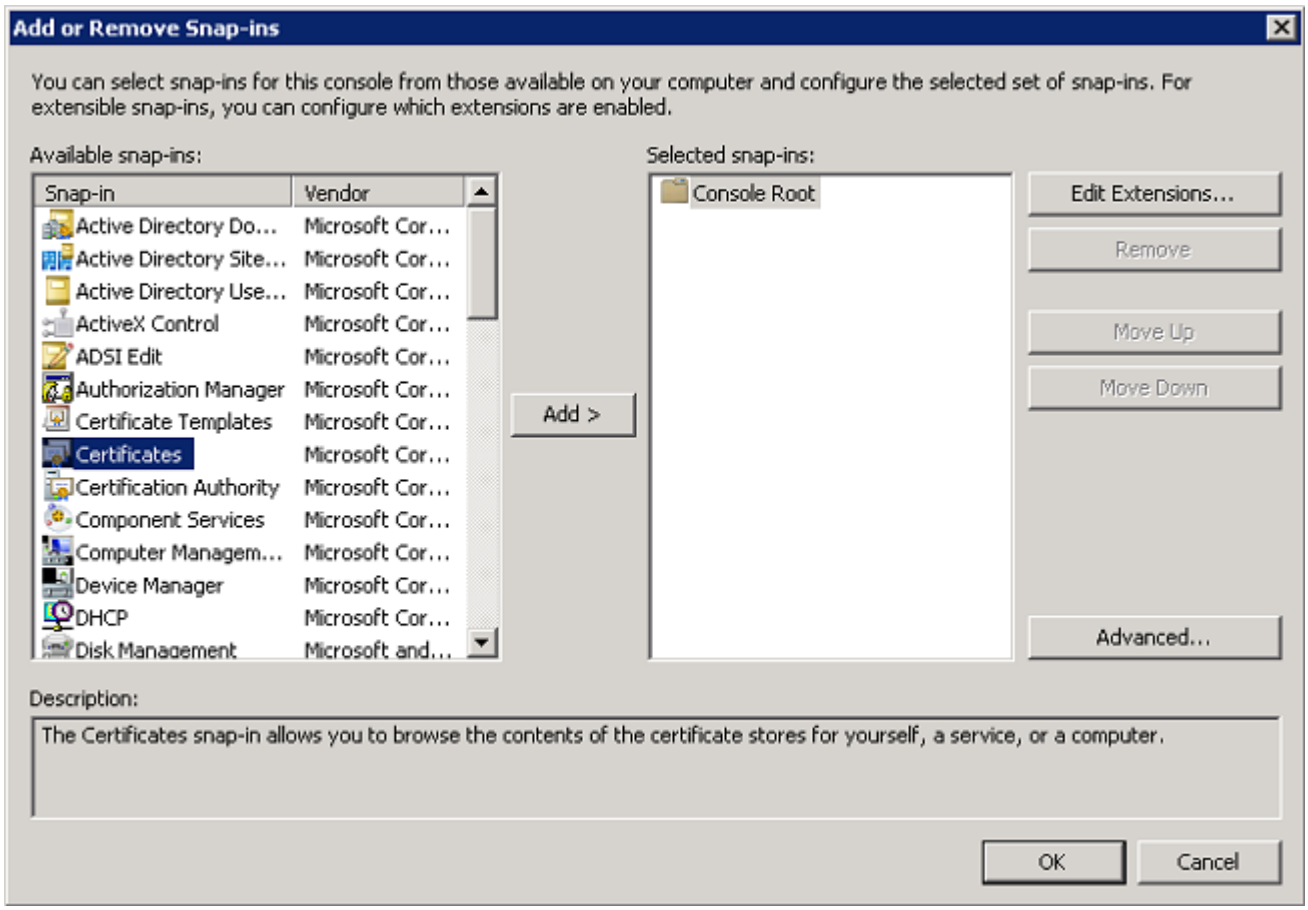


8. Klicken Sie auf Close (Schließen).

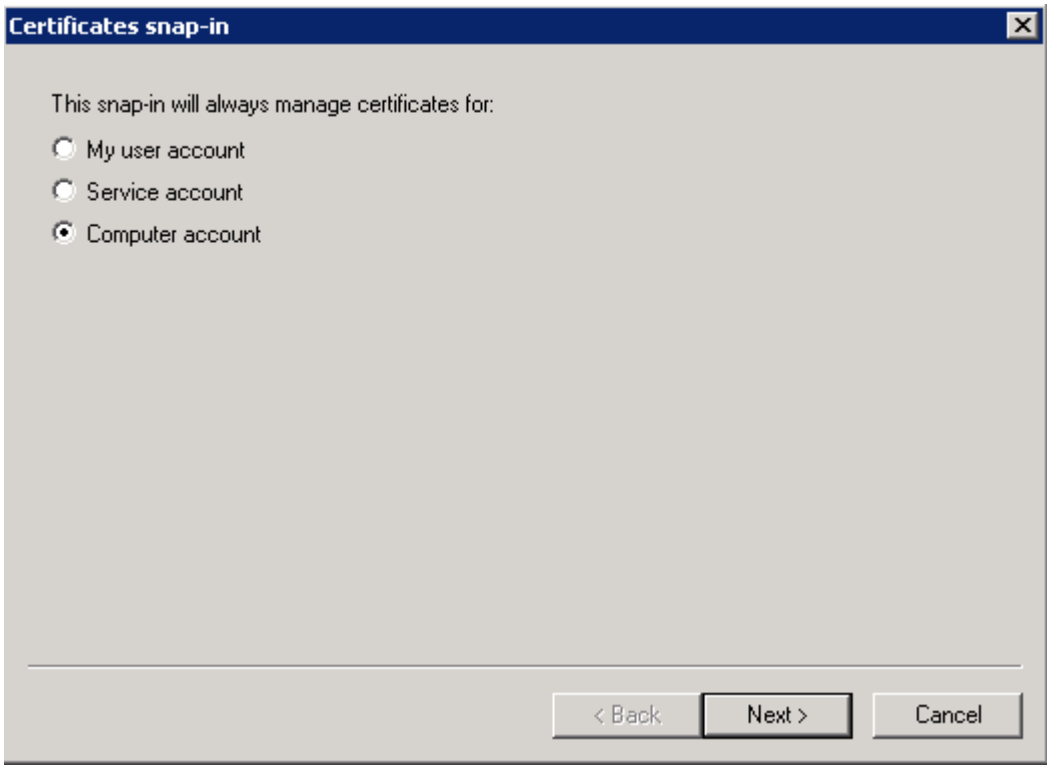
Installieren eines Zertifikats

Führen Sie die folgenden Schritte aus, um das Computerzertifikat für den NPS zu installieren:

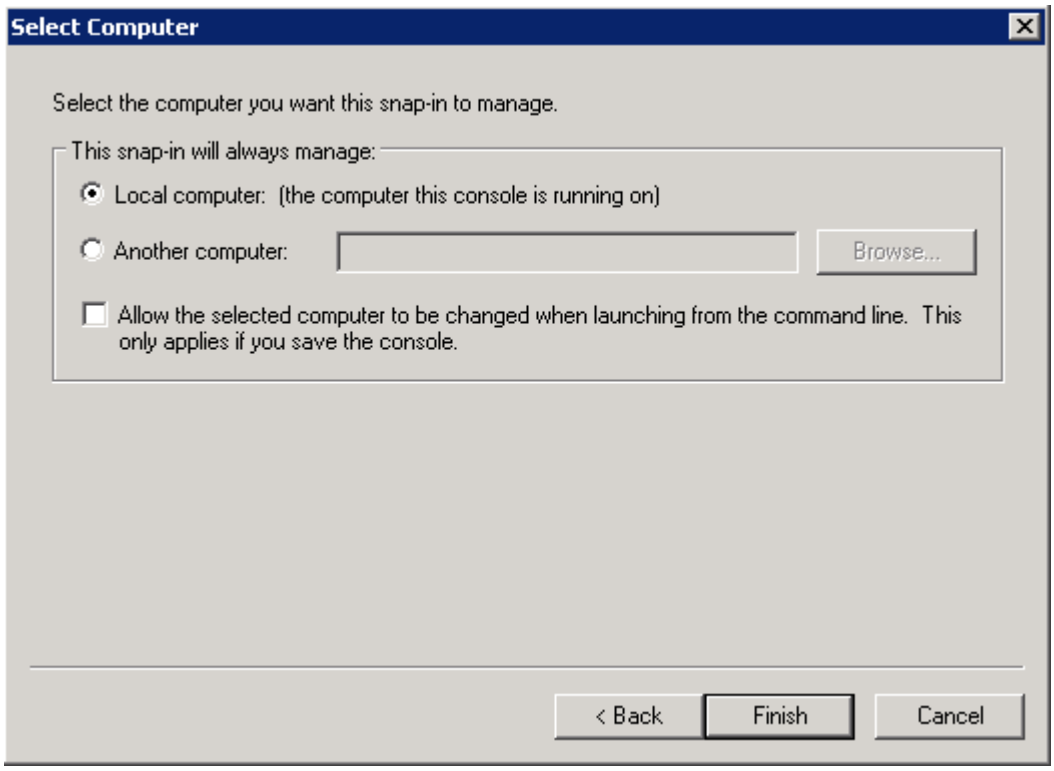
1. Klicken Sie auf Start, geben Sie mmc ein, und drücken Sie die Eingabetaste.
2. Klicken Sie auf Datei > Snap-In hinzufügen/entfernen.
3. Wählen Sie Zertifikate aus, und klicken Sie auf Hinzufügen.



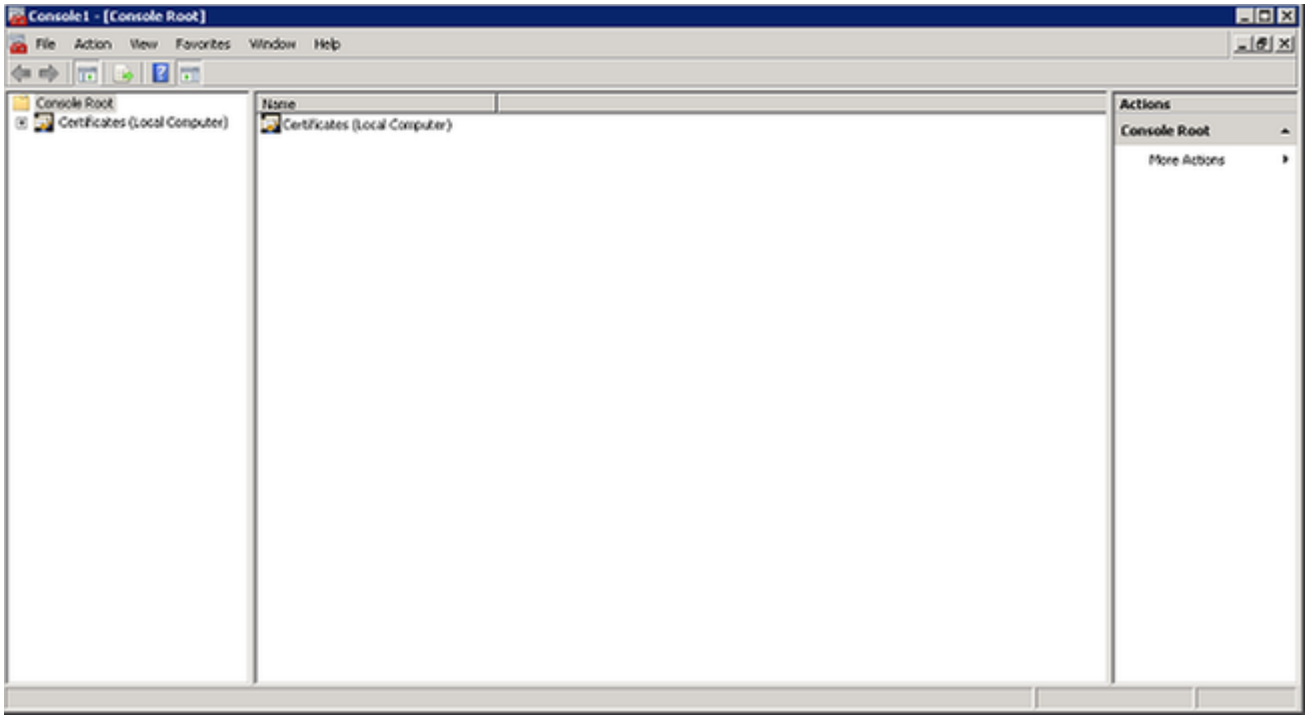
4. Wählen Sie Computerkonto aus, und klicken Sie auf Weiter.



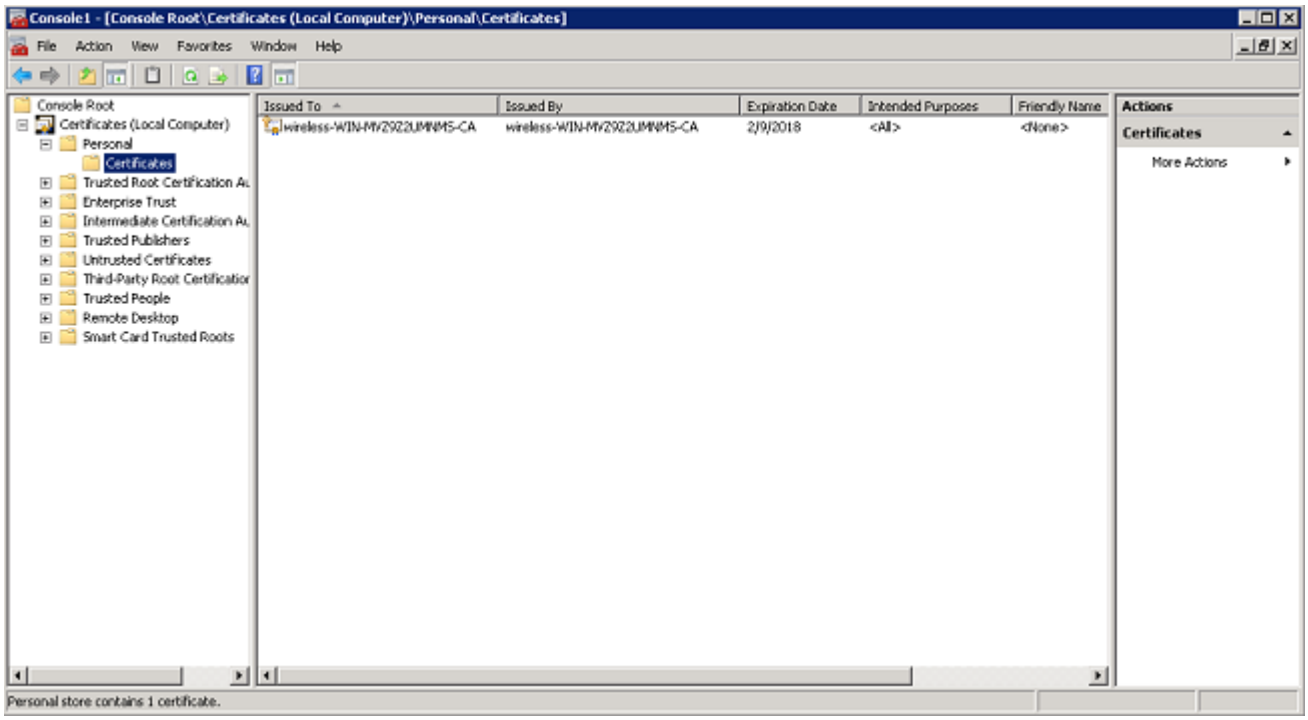
5. Wählen Sie Lokaler Computer aus, und klicken Sie auf Fertig stellen.



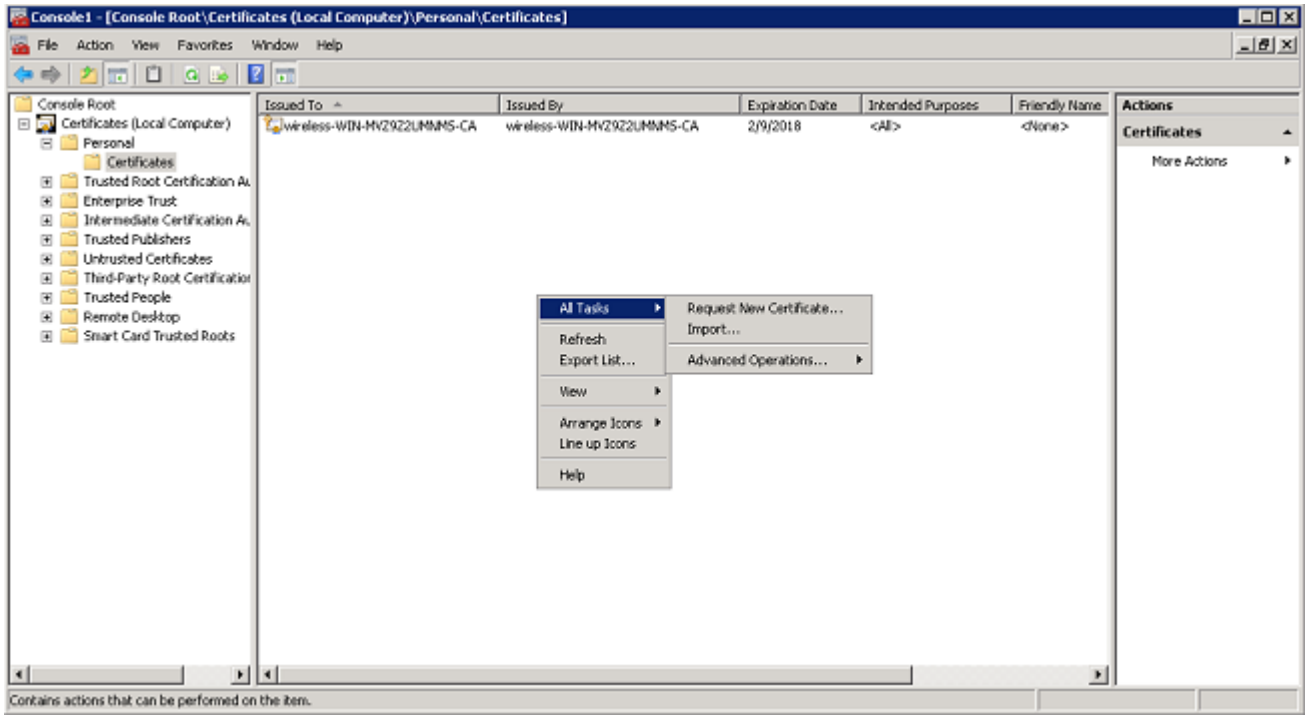
6. Klicken Sie auf OK, um zur Microsoft Management Console (MMC) zurückzukehren.



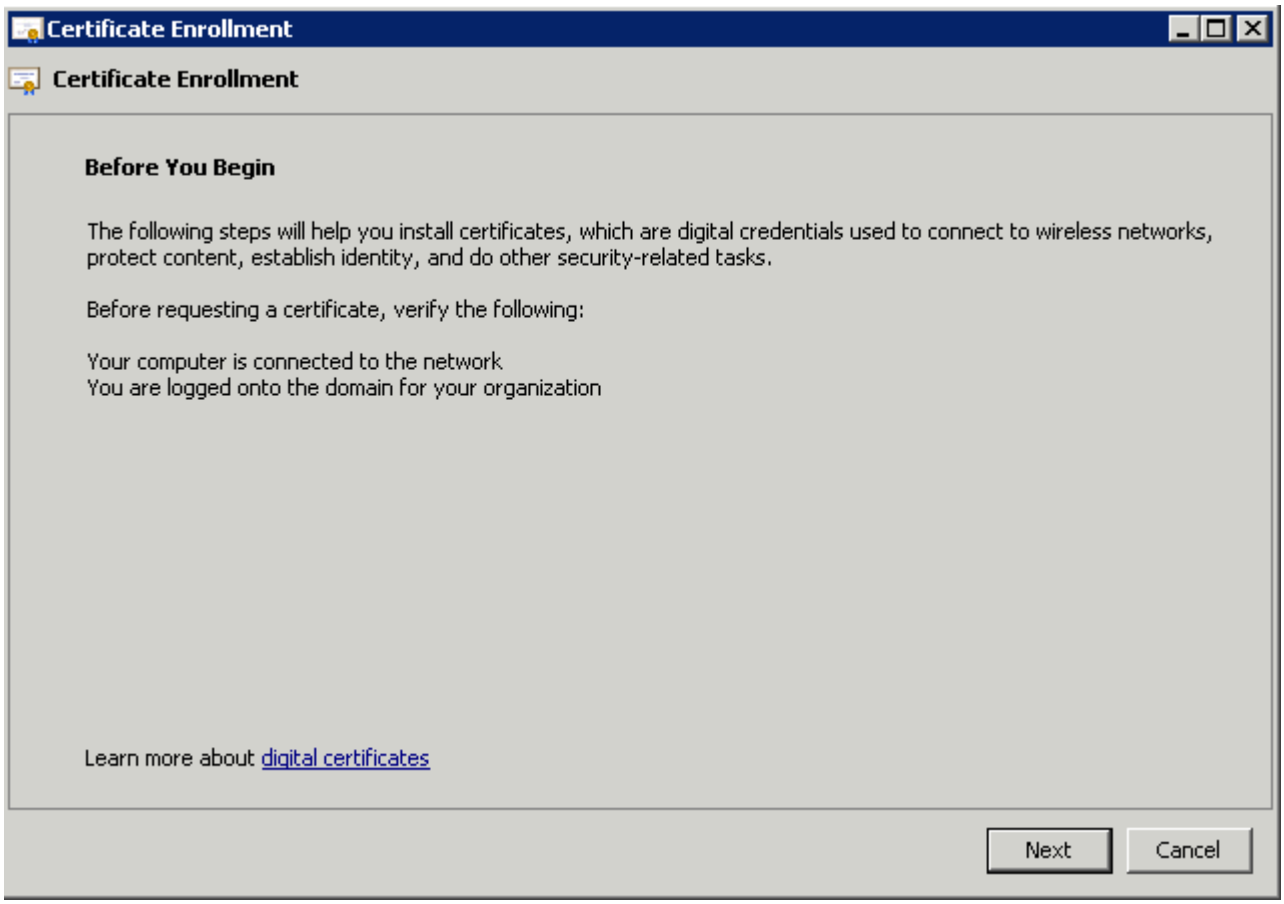
7. Erweitern Sie die Ordner Zertifikate (Lokaler Computer) und Persönliche Ordner, und klicken Sie auf Zertifikate.



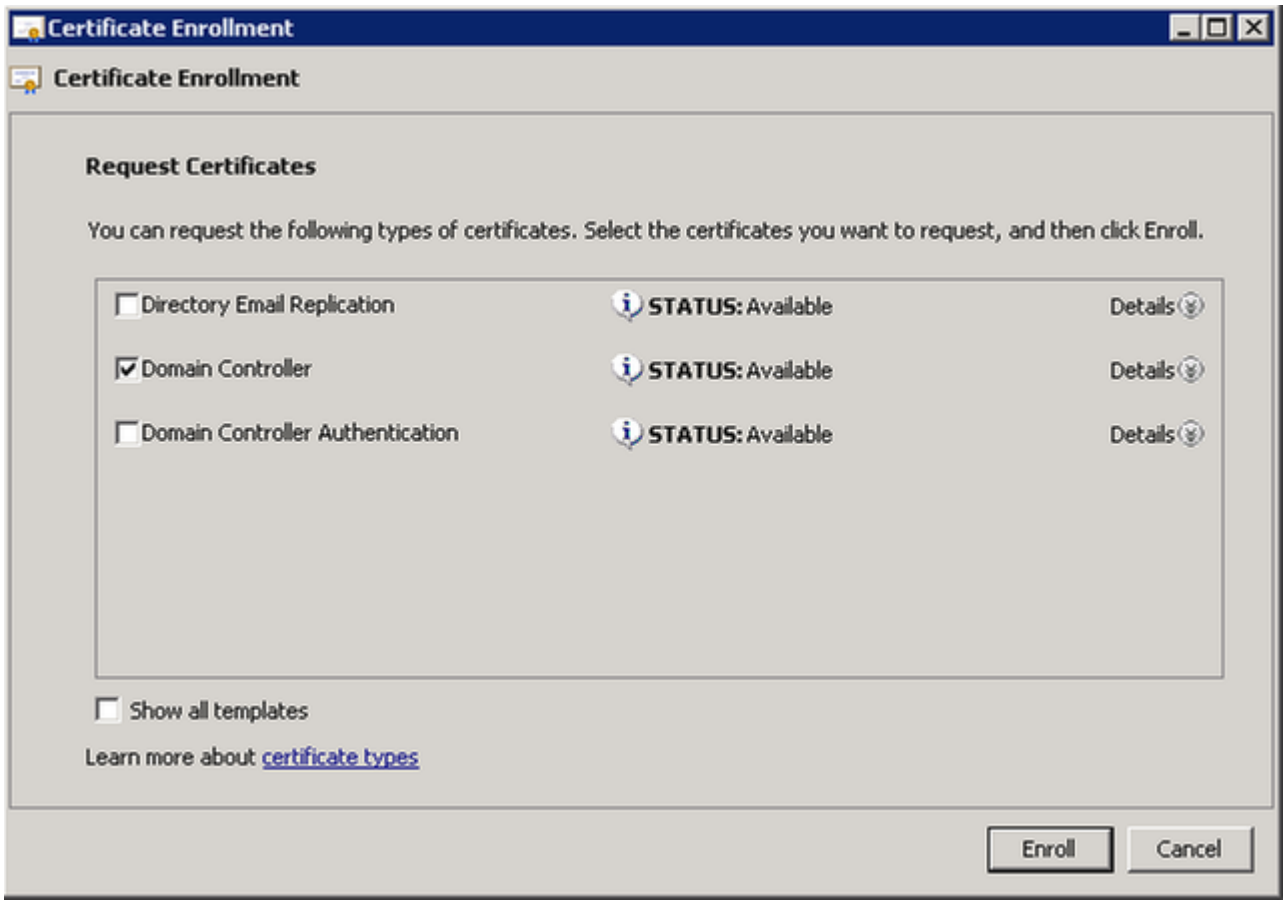
8. Klicken Sie mit der rechten Maustaste in den leeren Bereich unterhalb des Zertifizierungsstellenzertifikats, und wählen Sie Alle Aufgaben > Neues Zertifikat anfordern aus.



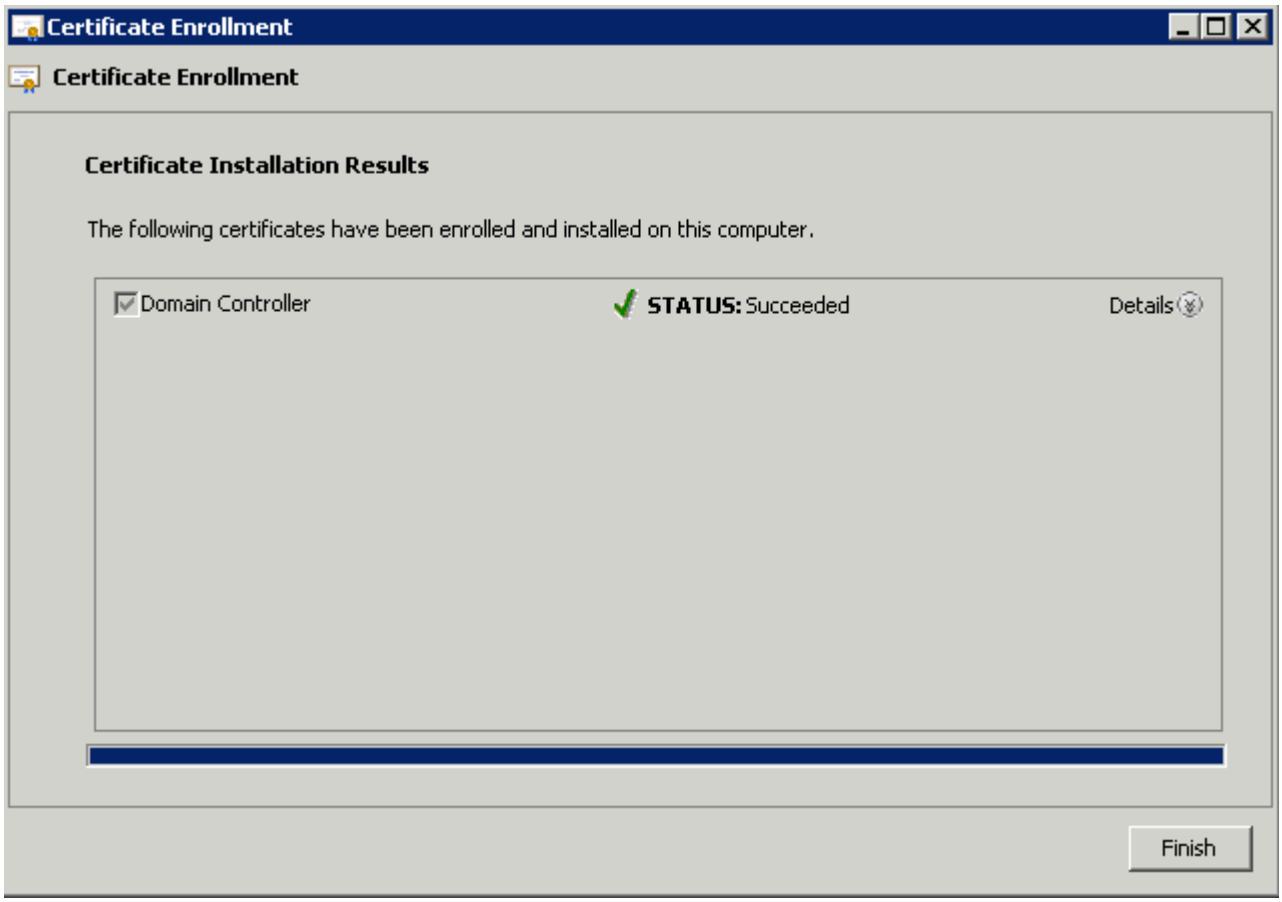
9. Klicken Sie auf Next (Weiter).



10. Wählen Sie Domain Controller aus, und klicken Sie auf Registrieren.

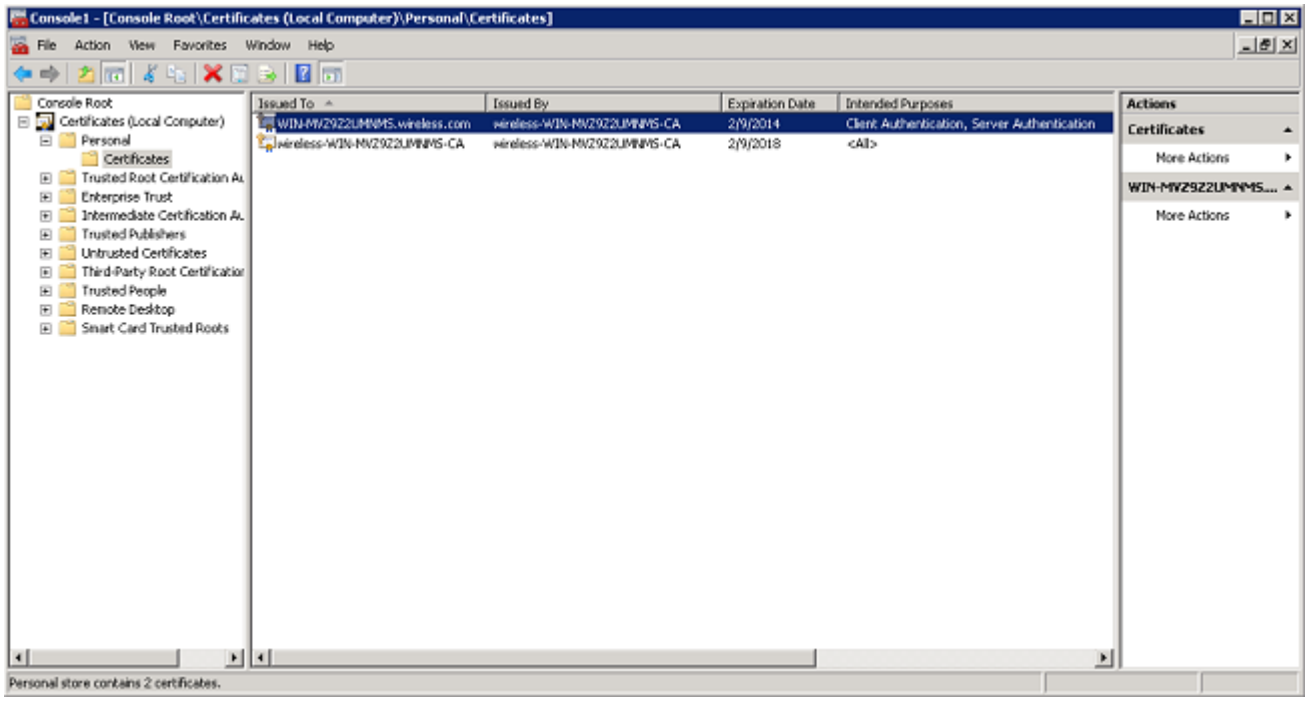


11. Klicken Sie nach der Installation des Zertifikats auf Fertig stellen.



Das NPS-Zertifikat ist jetzt installiert.

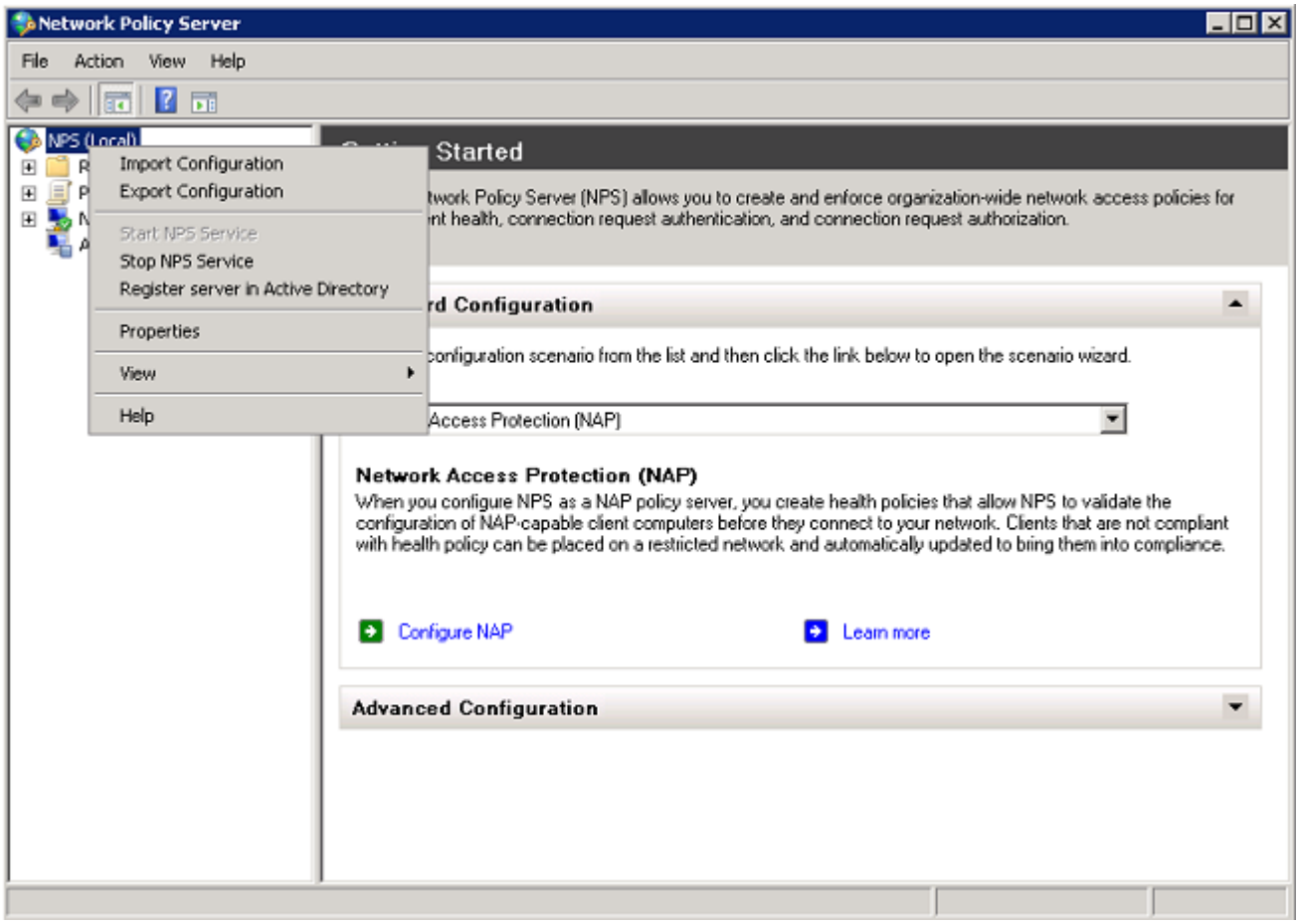
12. Stellen Sie sicher, dass der beabsichtigte Zweck des Zertifikats "Client Authentication, Server Authentication" lautet.



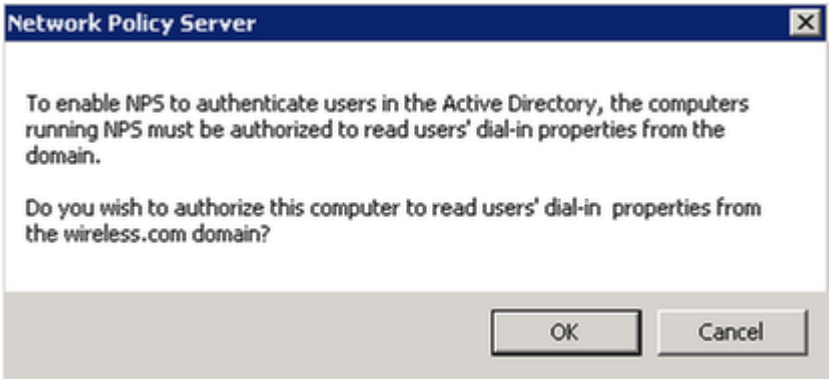
Konfigurieren des Netzwerkrichtlinienserver-Diensts für die PEAP-MS-CHAP v2-Authentifizierung

Führen Sie die folgenden Schritte aus, um den NPS für die Authentifizierung zu konfigurieren:

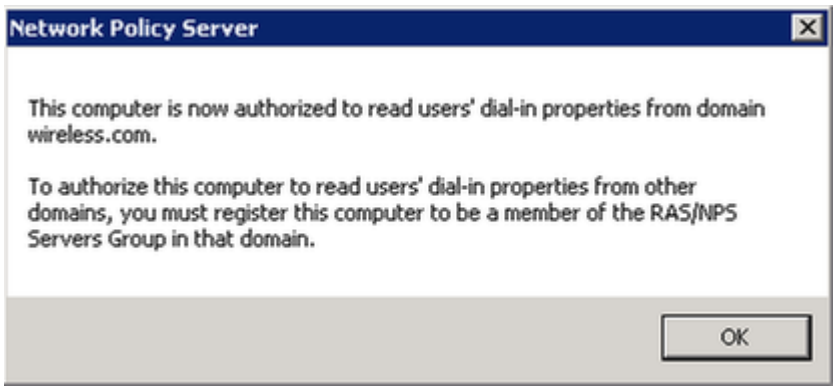
1. Klicken Sie auf Start > Verwaltung> Netzwerkrichtlinienserver.
2. Klicken Sie mit der rechten Maustaste auf NPS (Lokal), und wählen Sie Server in Active Directory registrieren aus.



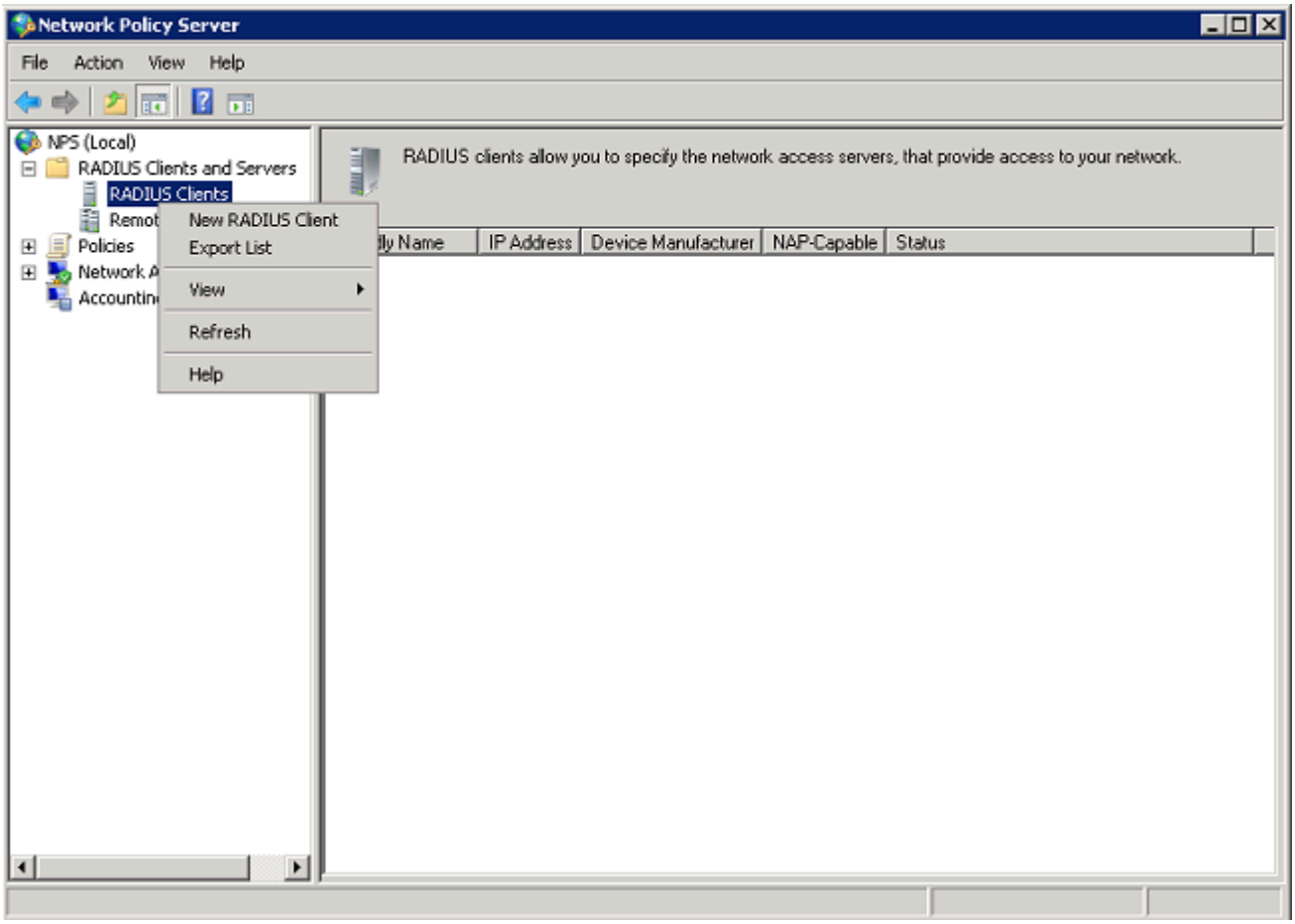
3. Klicken Sie auf OK.



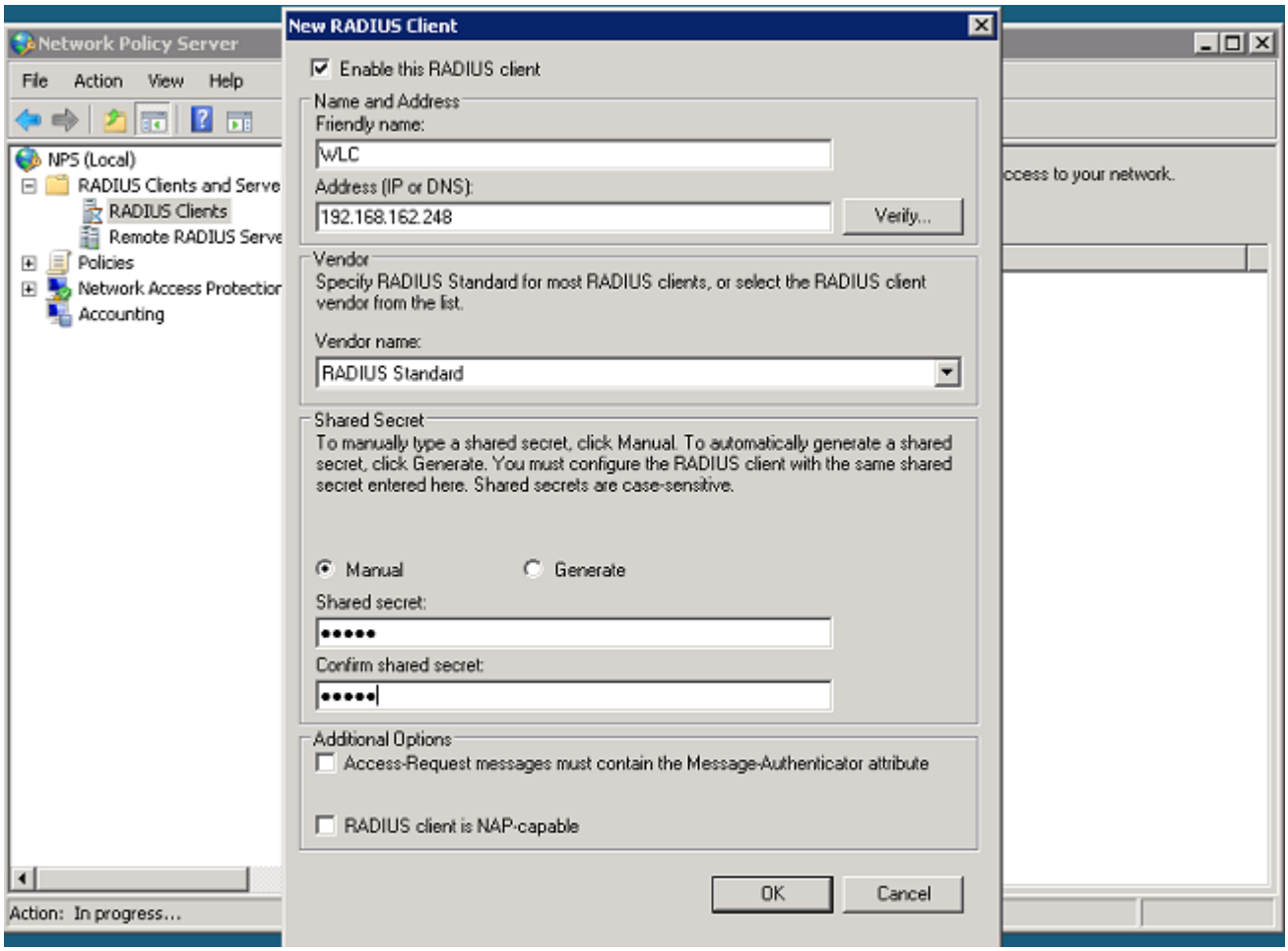
4. Klicken Sie auf OK.



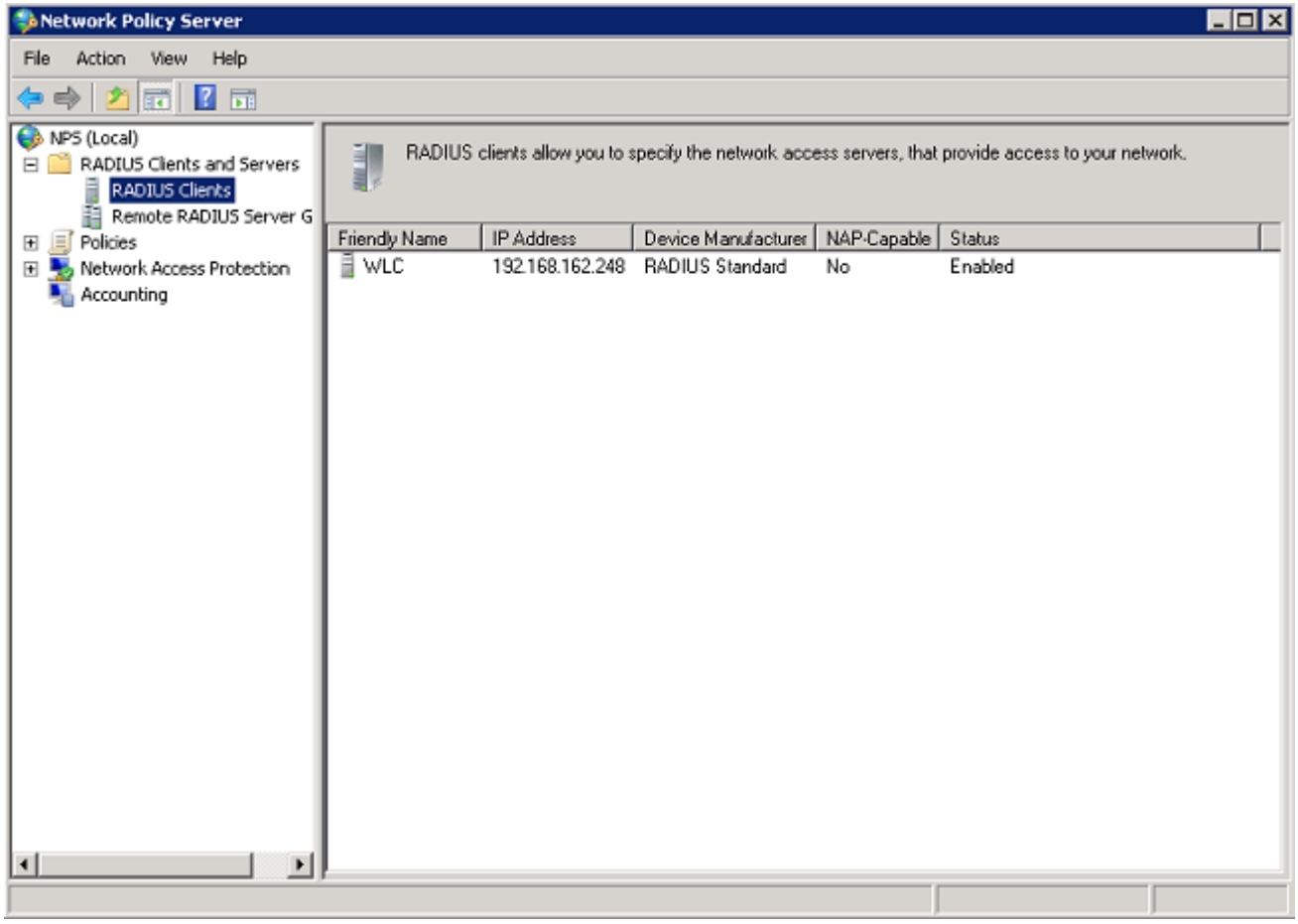
5. Fügen Sie den Wireless LAN Controller als AAA-Client (Authentication, Authorization, Accounting) auf dem NPS hinzu.
6. Erweitern Sie RADIUS-Clients und -Server. Klicken Sie mit der rechten Maustaste auf RADIUS Clients, und wählen Sie New RADIUS Client (Neuer RADIUS-Client).



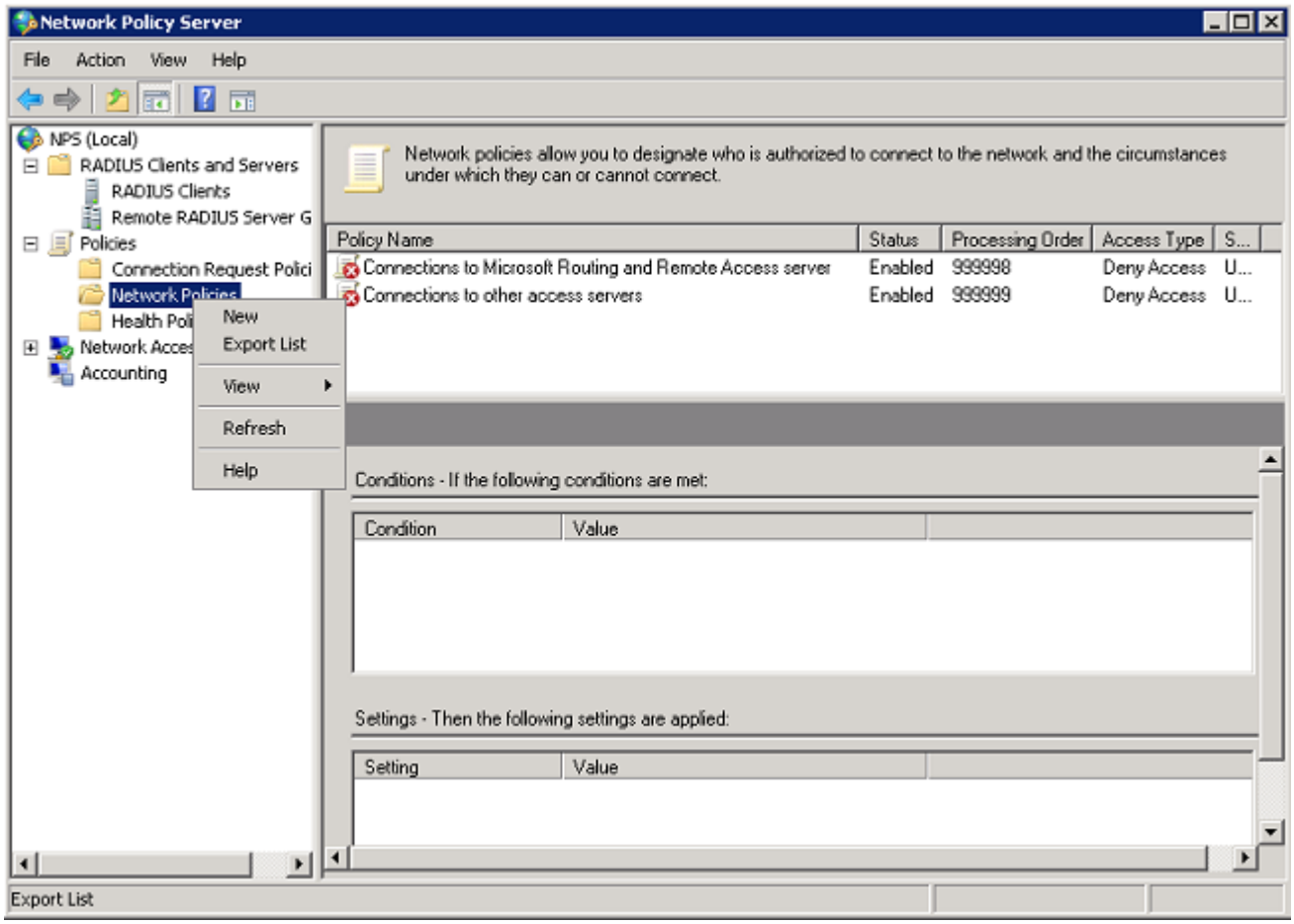
7. Geben Sie einen Anzeigenamen (in diesem Beispiel WLC), die Verwaltungs-IP-Adresse des WLC (in diesem Beispiel 192.168.162.248) und einen gemeinsamen geheimen Schlüssel ein. Derselbe geheime Schlüssel wird für die Konfiguration des WLC verwendet.



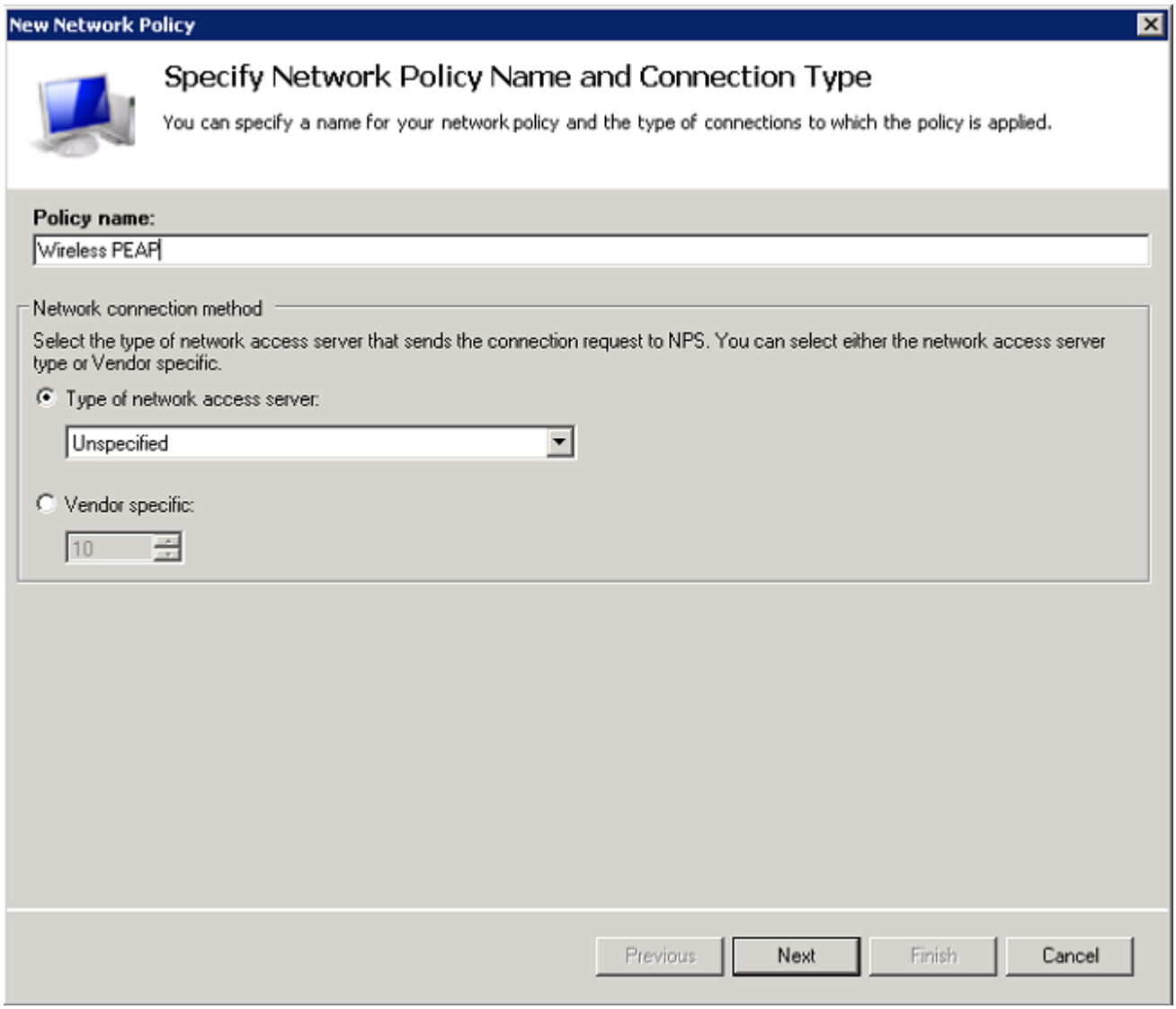
8. Klicken Sie auf OK, um zum vorherigen Bildschirm zurückzukehren.



9. Erstellen einer neuen Netzwerkrichtlinie für Wireless-Benutzer Erweitern Sie Richtlinien, klicken Sie mit der rechten Maustaste auf Netzwerkrichtlinien, und wählen Sie Neu.

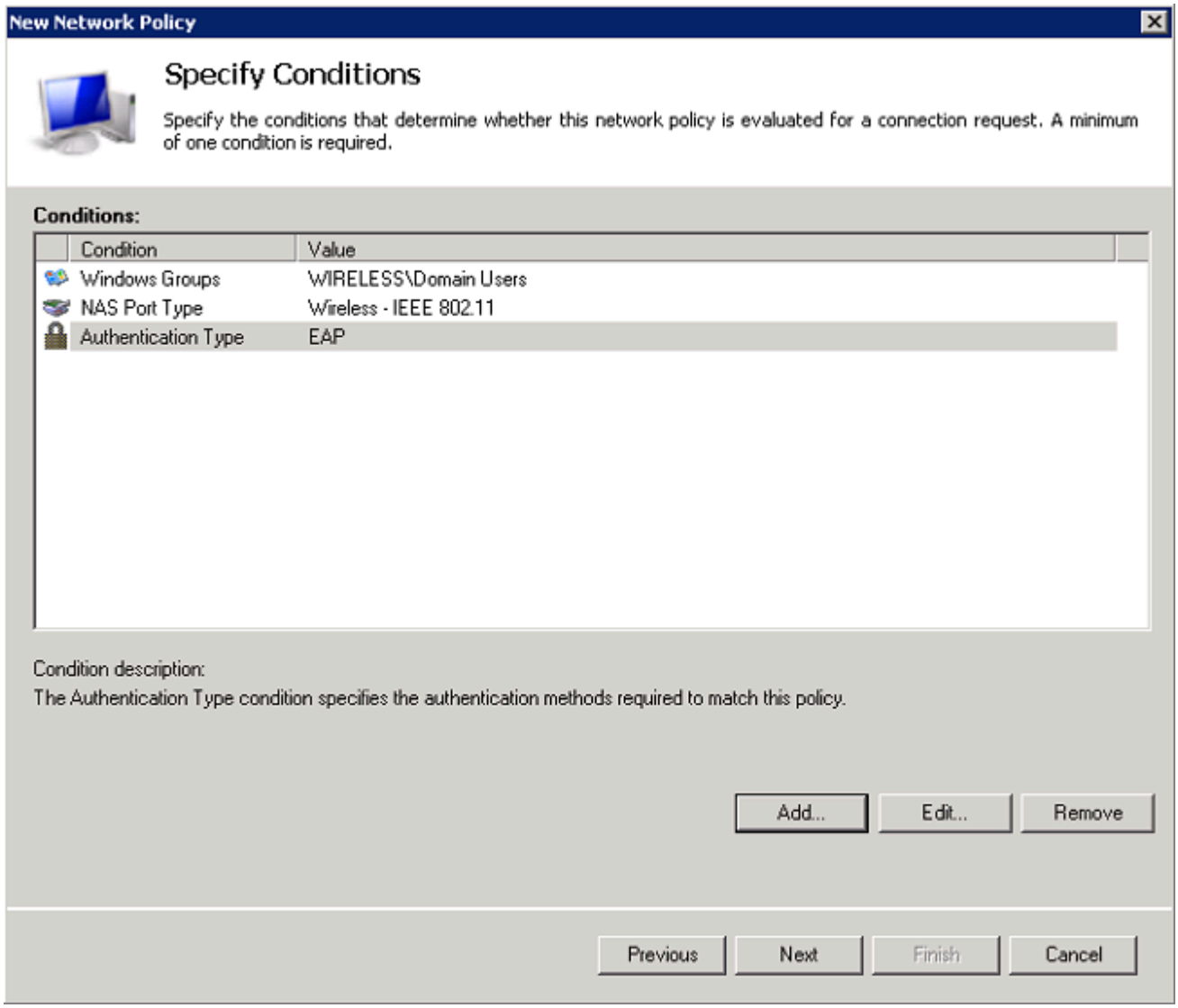


10. Geben Sie einen Richtliniennamen für diese Regel ein (in diesem Beispiel Wireless PEAP), und klicken Sie auf Weiter.

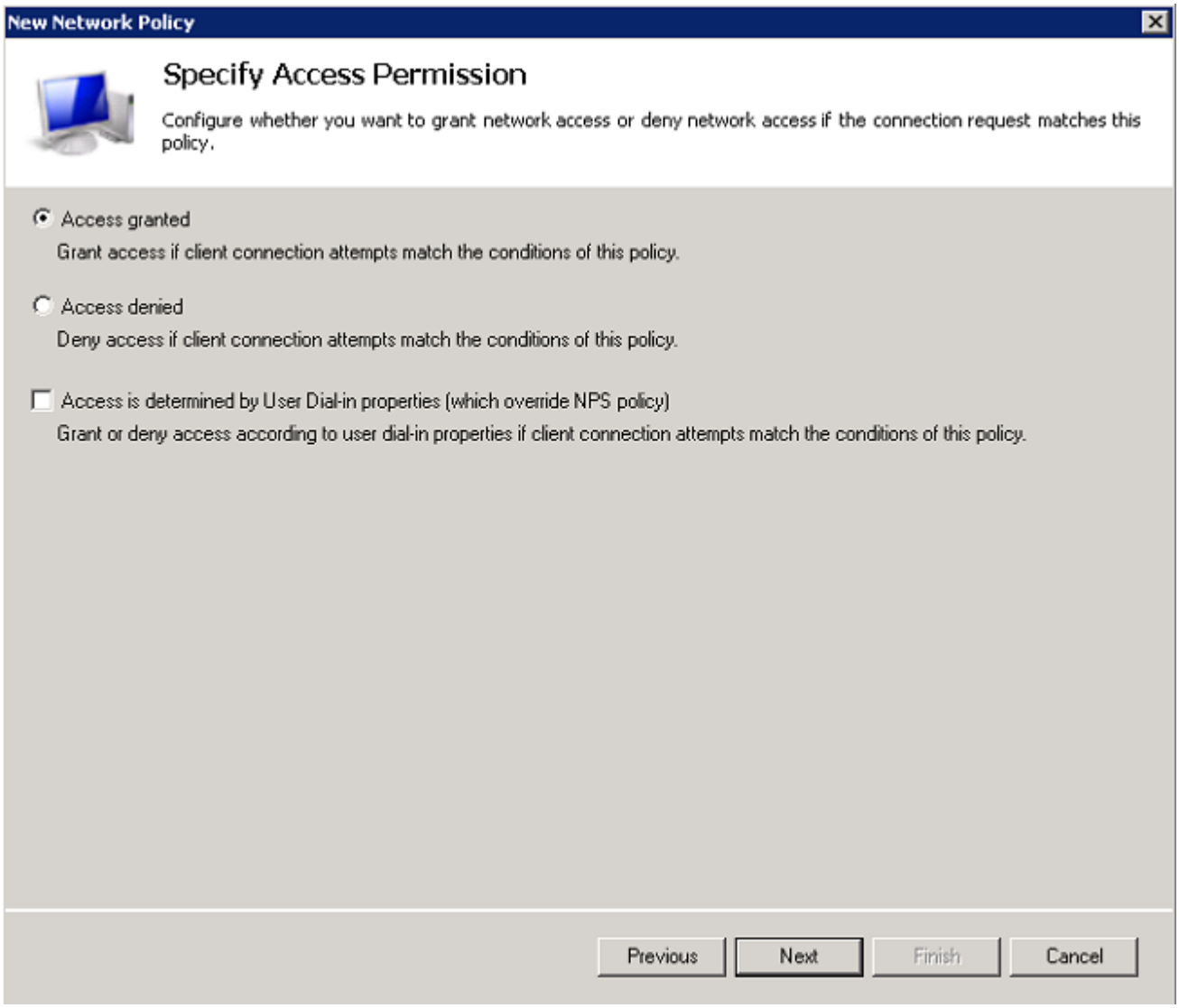


11. Wenn diese Richtlinie nur Wireless-Domänenbenutzer zulässt, fügen Sie die folgenden drei Bedingungen hinzu, und klicken Sie auf Weiter:

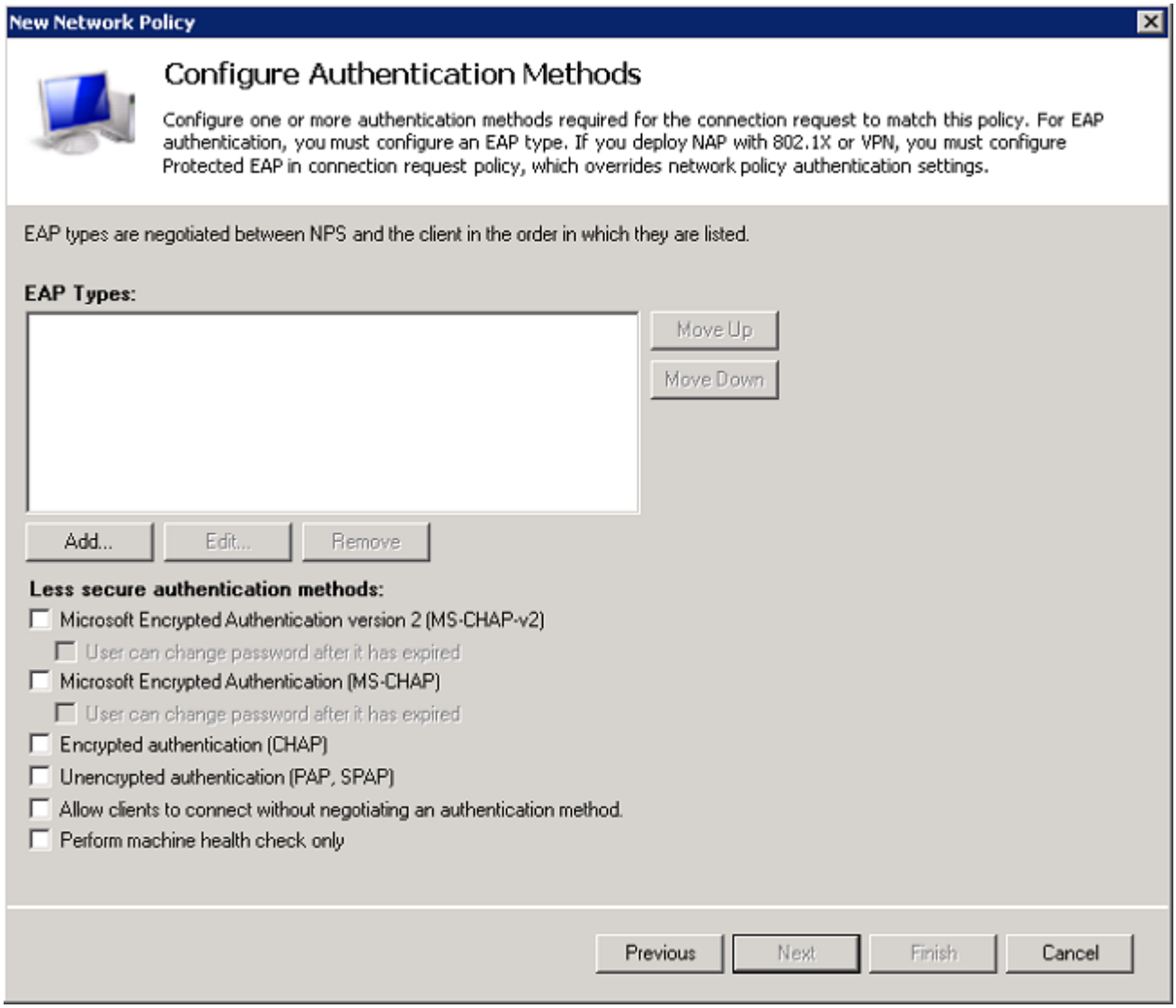
    - Windows-Gruppen - Domänenbenutzer
    - NAS-Porttyp - Wireless - IEEE 802.11
    - Authentifizierungstyp - EAP



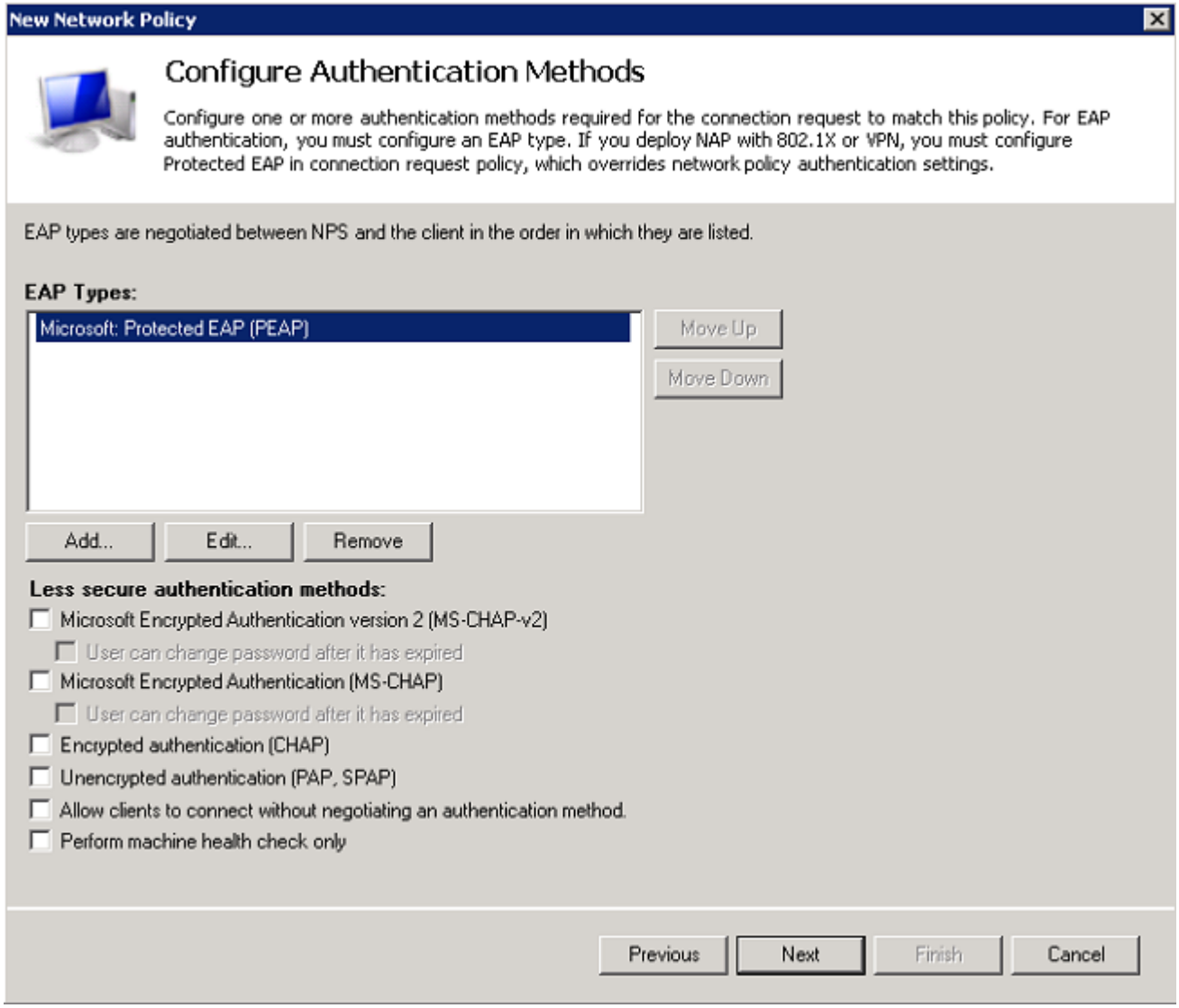
12. Klicken Sie auf Zugriff gewährt, um Verbindungsversuche zu gewähren, die dieser Richtlinie entsprechen, und klicken Sie auf Weiter.



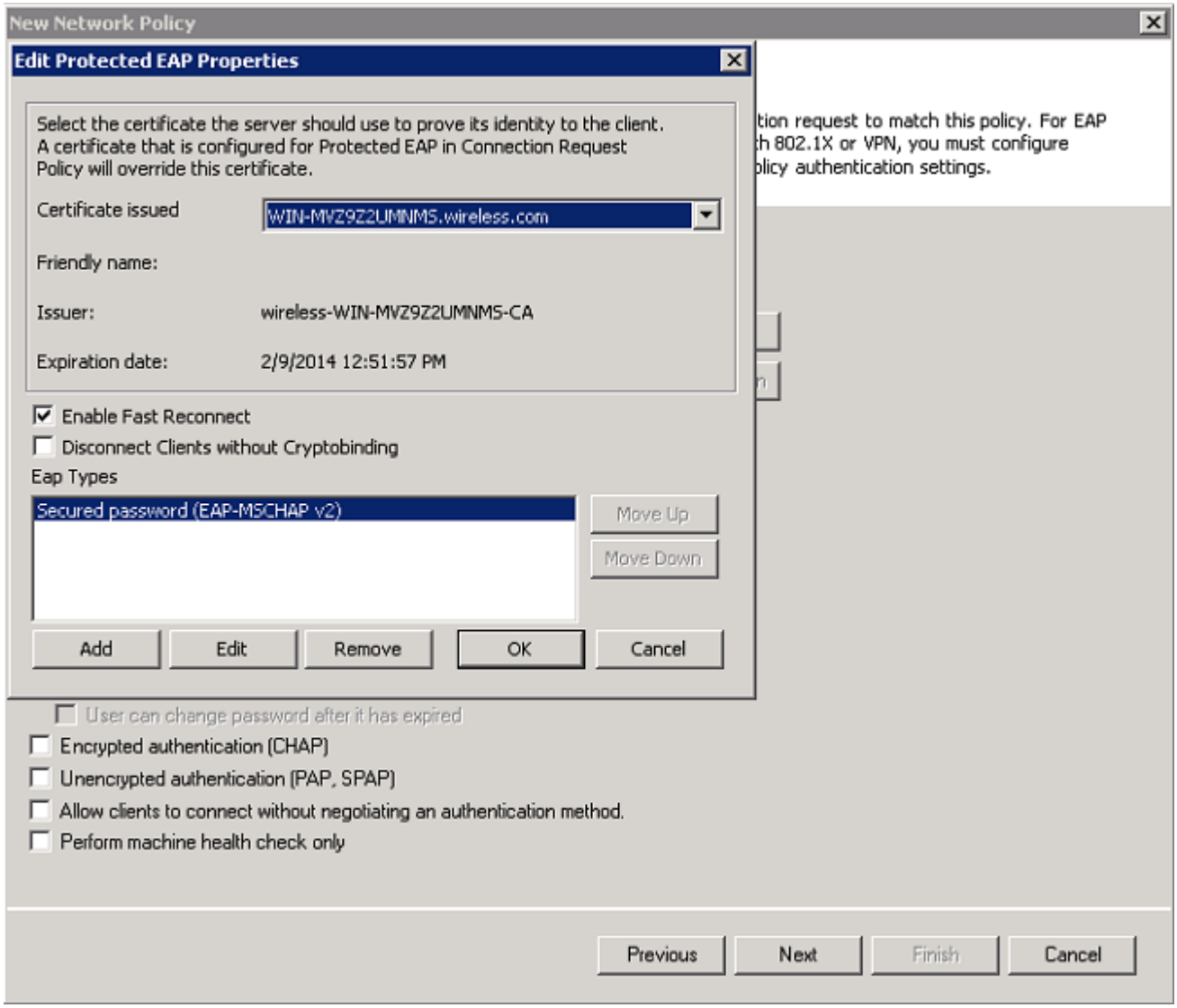
13. Deaktivieren Sie alle Authentifizierungsmethoden unter Weniger sichere Authentifizierungsmethoden.



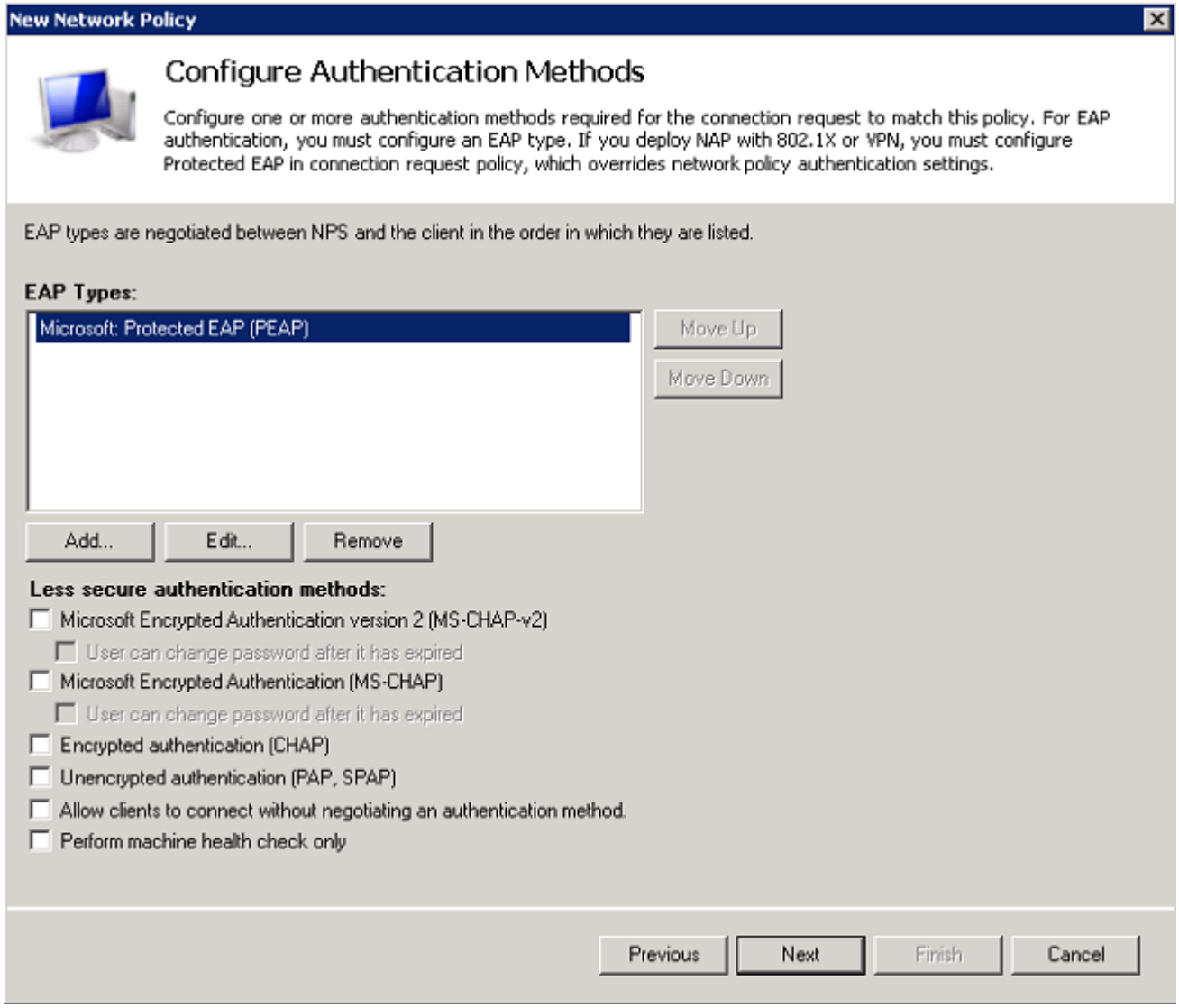
14. Klicken Sie auf Hinzufügen, wählen Sie PEAP aus, und klicken Sie auf OK, um PEAP zu aktivieren.



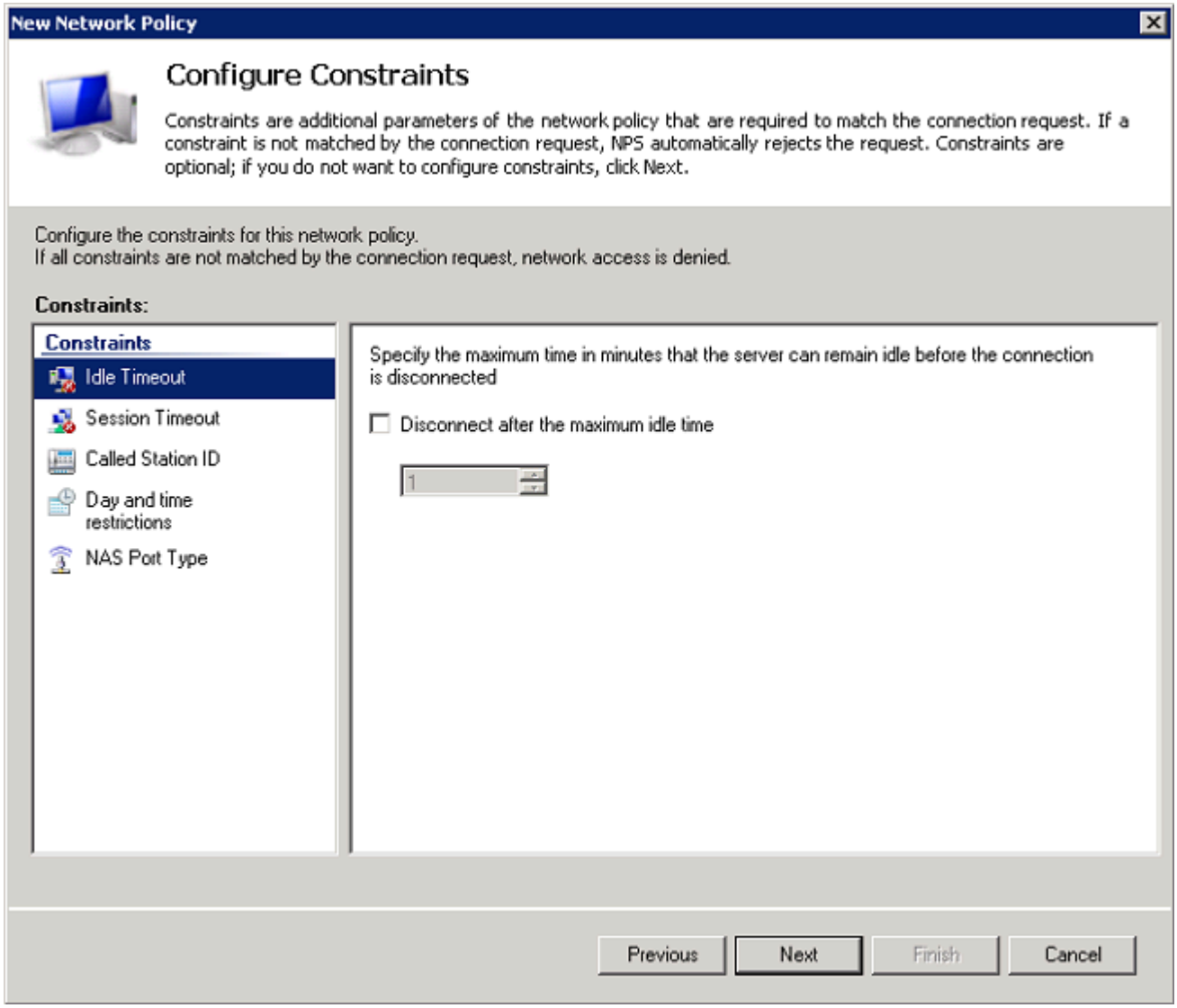
15. Microsoft auswählen: Protected EAP (PEAP), und klicken Sie auf Edit. Stellen Sie sicher, dass das zuvor erstellte Domänencontrollerzertifikat in der Dropdown-Liste "Zertifikat ausgestellt" ausgewählt ist, und klicken Sie auf OK.



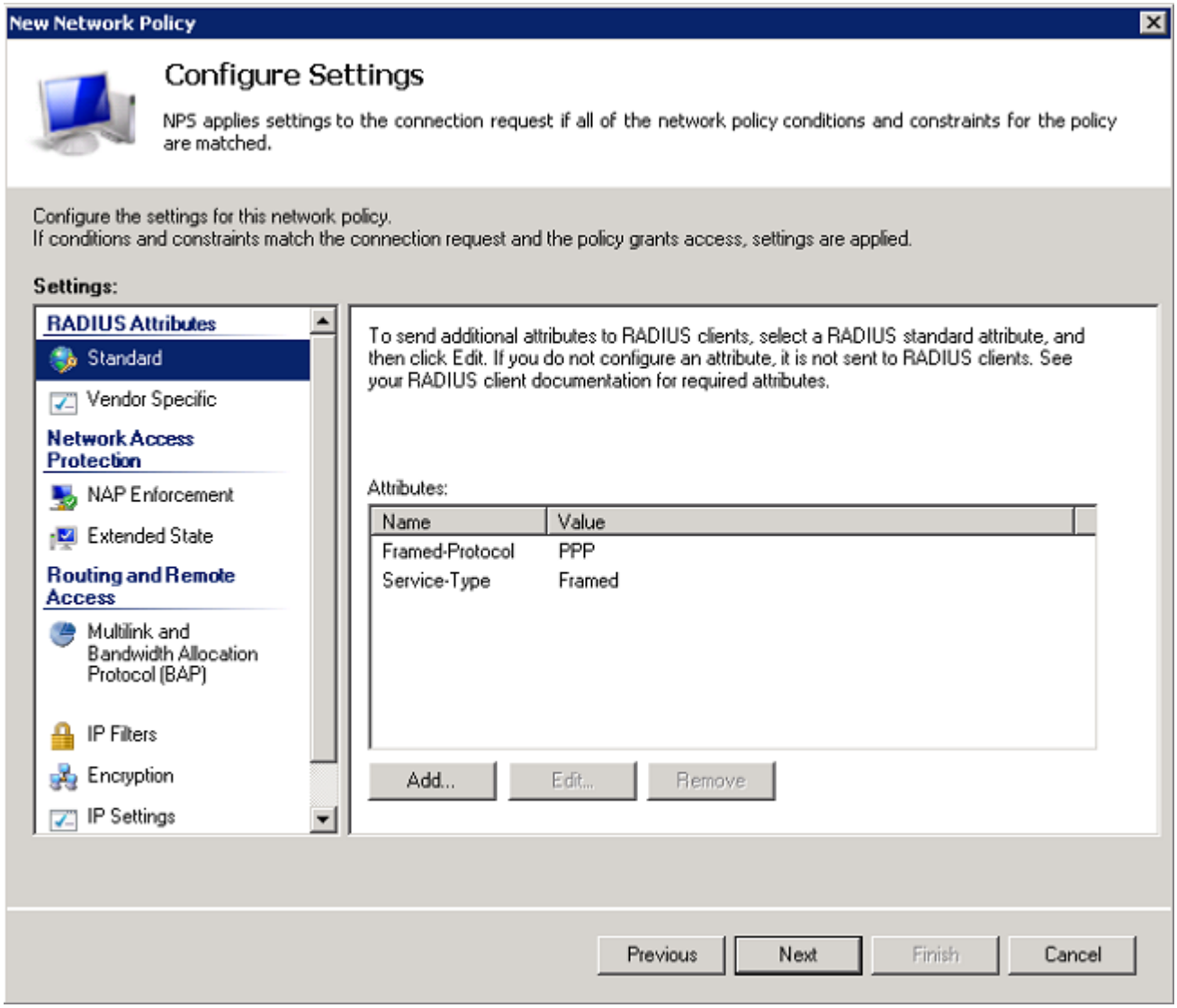
16. Klicken Sie auf Next (Weiter).



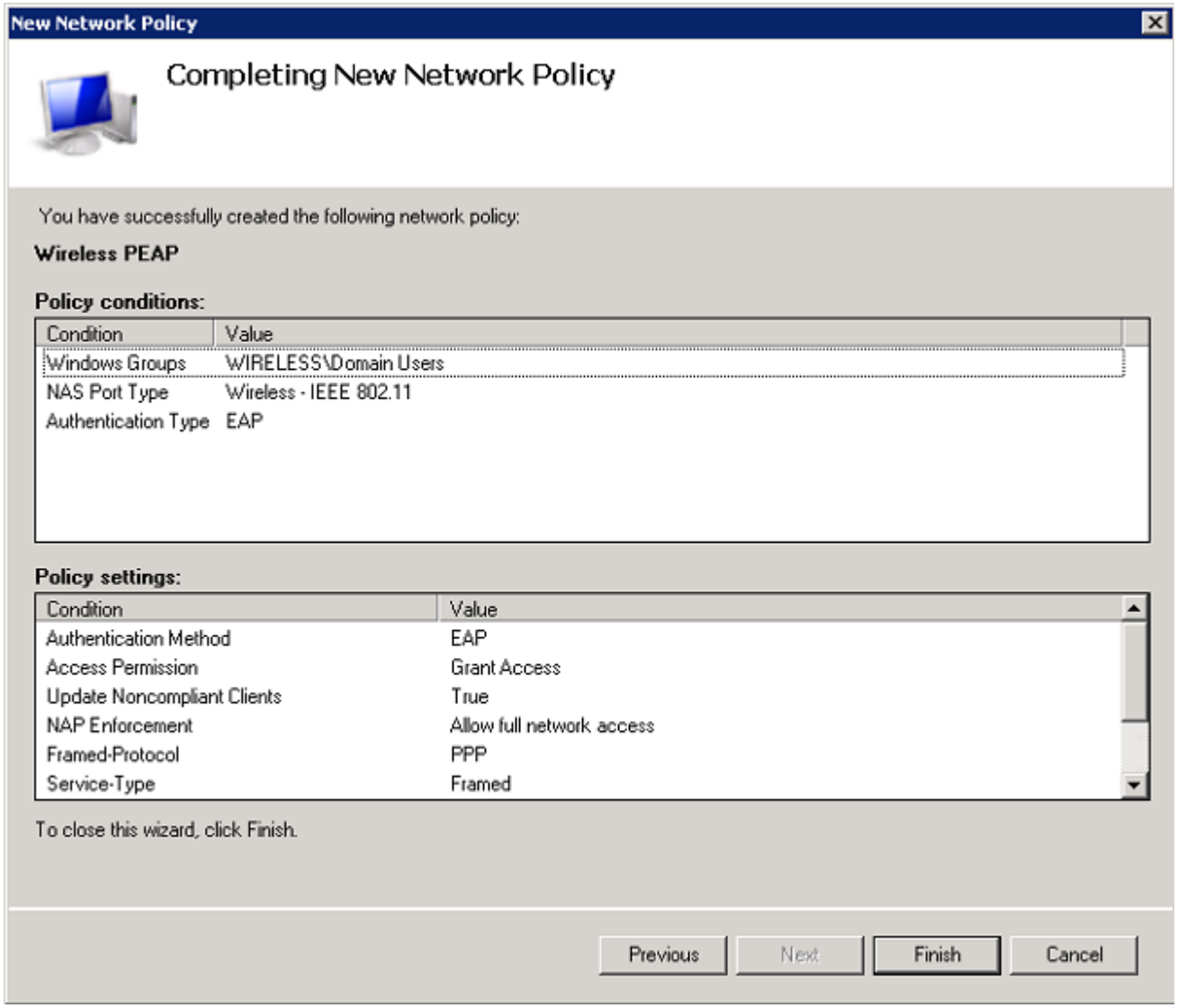
17. Klicken Sie auf Next (Weiter).



18. Klicken Sie auf Next (Weiter).



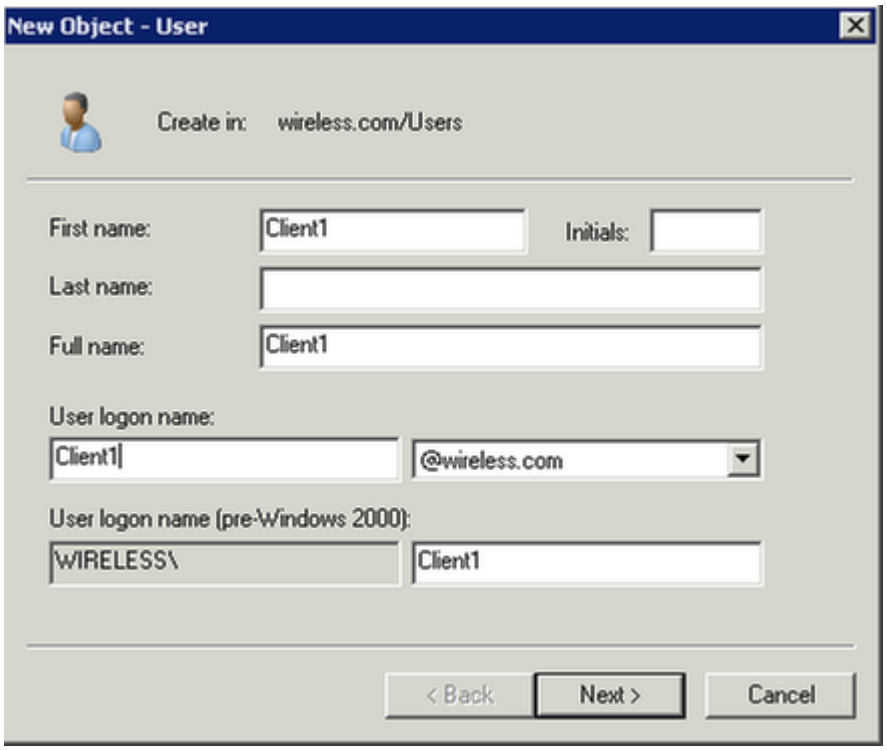
19. Klicken Sie auf Beenden.



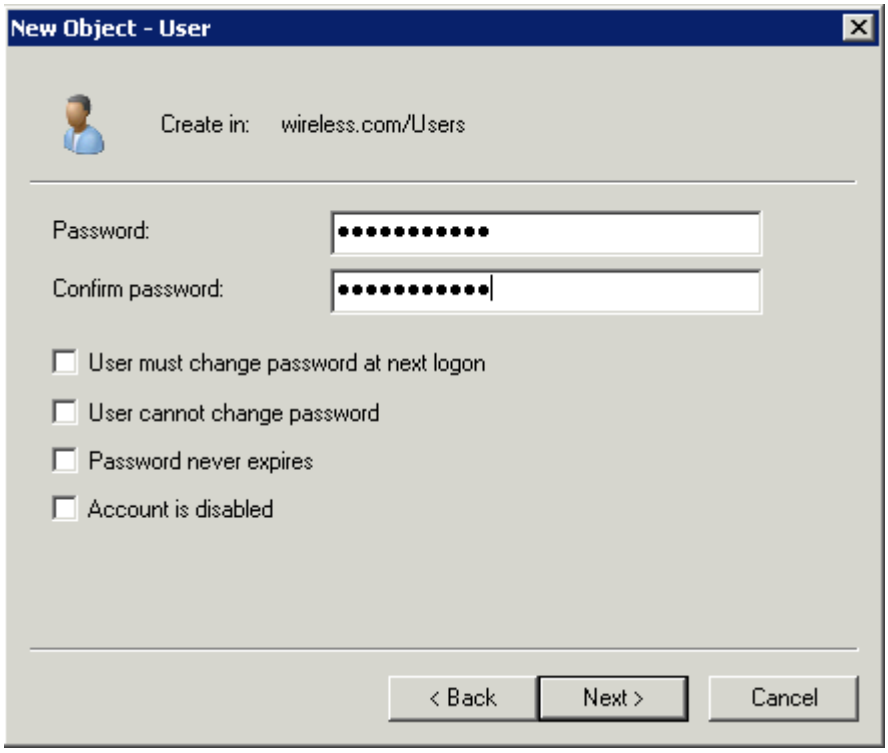
Hinzufügen von Benutzern zum Active Directory

In diesem Beispiel wird die Benutzerdatenbank in Active Directory verwaltet. Führen Sie die folgenden Schritte aus, um der Active Directory-Datenbank Benutzer hinzuzufügen:

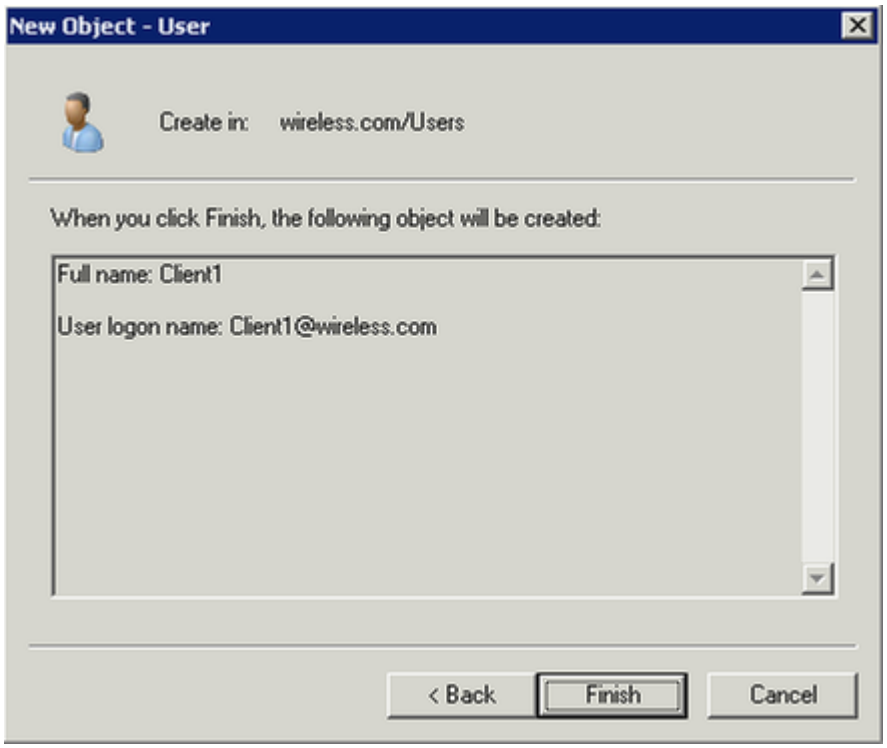
1. Öffnen Sie Active Directory-Benutzer und -Computer. Klicken Sie auf Start> Verwaltung >> Active Directory-Benutzer und -Computer.
2. Erweitern Sie in der Konsolenstruktur von Active Directory-Benutzer und -Computer die Domäne, klicken Sie mit der rechten Maustaste auf Benutzer> Neu, und wählen Sie Benutzer aus.
3. Geben Sie im Dialogfeld Neues Objekt - Benutzer den Namen des Wireless-Benutzers ein. In diesem Beispiel wird der Name Client1 im Feld Vorname und Client1 im Feld Benutzername verwendet. Klicken Sie auf Next (Weiter).



4. Geben Sie im Dialogfeld Neues Objekt - Benutzer in den Feldern Kennwort und Kennwort bestätigen ein Kennwort Ihrer Wahl ein. Stellen Sie sicher, dass das Kontrollkästchen Benutzer muss Kennwort bei der nächsten Anmeldung ändern nicht aktiviert ist, und klicken Sie auf Weiter.



5. Klicken Sie im Dialogfeld Neues Objekt - Benutzer auf Fertig stellen.



6. Wiederholen Sie die Schritte 2 bis 4, um weitere Benutzerkonten zu erstellen.

Konfigurieren des Wireless LAN-Controllers und der LAPs

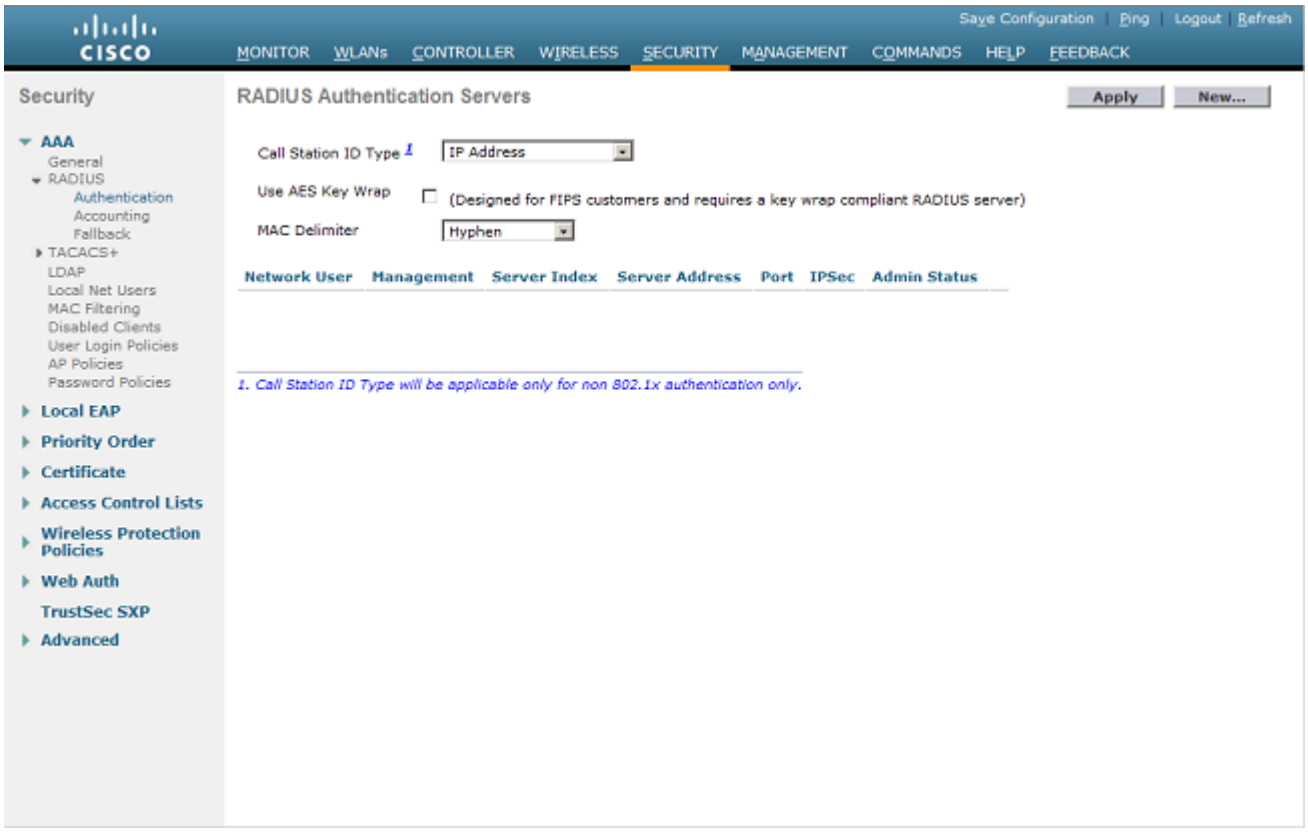
Konfigurieren Sie die Wireless-Geräte (Wireless LAN-Controller und LAPs) für diese Einrichtung.

Konfigurieren des WLC für die RADIUS-Authentifizierung

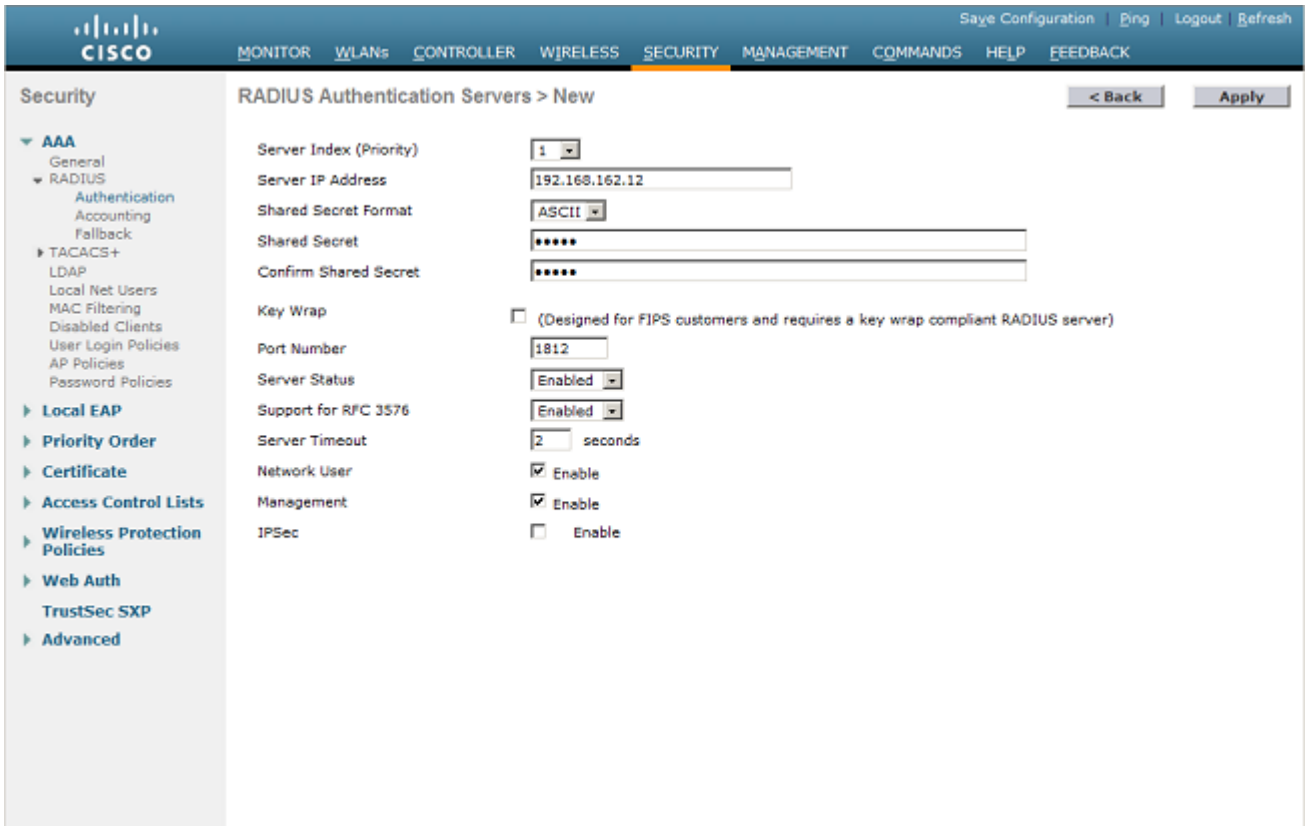
Konfigurieren Sie den WLC so, dass der NPS als Authentifizierungsserver verwendet wird. Der WLC muss konfiguriert werden, um die Benutzeranmeldeinformationen an einen externen RADIUS-Server weiterzuleiten. Der externe RADIUS-Server überprüft dann die Anmeldeinformationen des Benutzers und ermöglicht den Zugriff auf die Wireless-Clients.

Führen Sie die folgenden Schritte aus, um den NPS als RADIUS-Server auf der Seite Security > RADIUS Authentication (Sicherheit > RADIUS-Authentifizierung) hinzuzufügen:

1. Wählen Sie Security > RADIUS > Authentication (Sicherheit > RADIUS > Authentifizierung) in der Controllerschnittstelle, um die Seite RADIUS Authentication Servers (RADIUS-Authentifizierungsserver) anzuzeigen. Klicken Sie auf Neu, um einen RADIUS-Server zu definieren.



2. Definieren Sie die RADIUS-Serverparameter. Zu diesen Parametern gehören die RADIUS-Server-IP-Adresse, der gemeinsame geheime Schlüssel, die Portnummer und der Serverstatus. Die Kontrollkästchen "Network User and Management" (Netzwerkbenutzer und -verwaltung) legen fest, ob die RADIUS-basierte Authentifizierung für Verwaltungs- und Netzwerkbenutzer (Wireless-Benutzer) gilt. In diesem Beispiel wird der NPS als RADIUS-Server mit der IP-Adresse 192.168.162.12 verwendet. Klicken Sie auf Apply.



Konfigurieren eines WLAN für die Clients

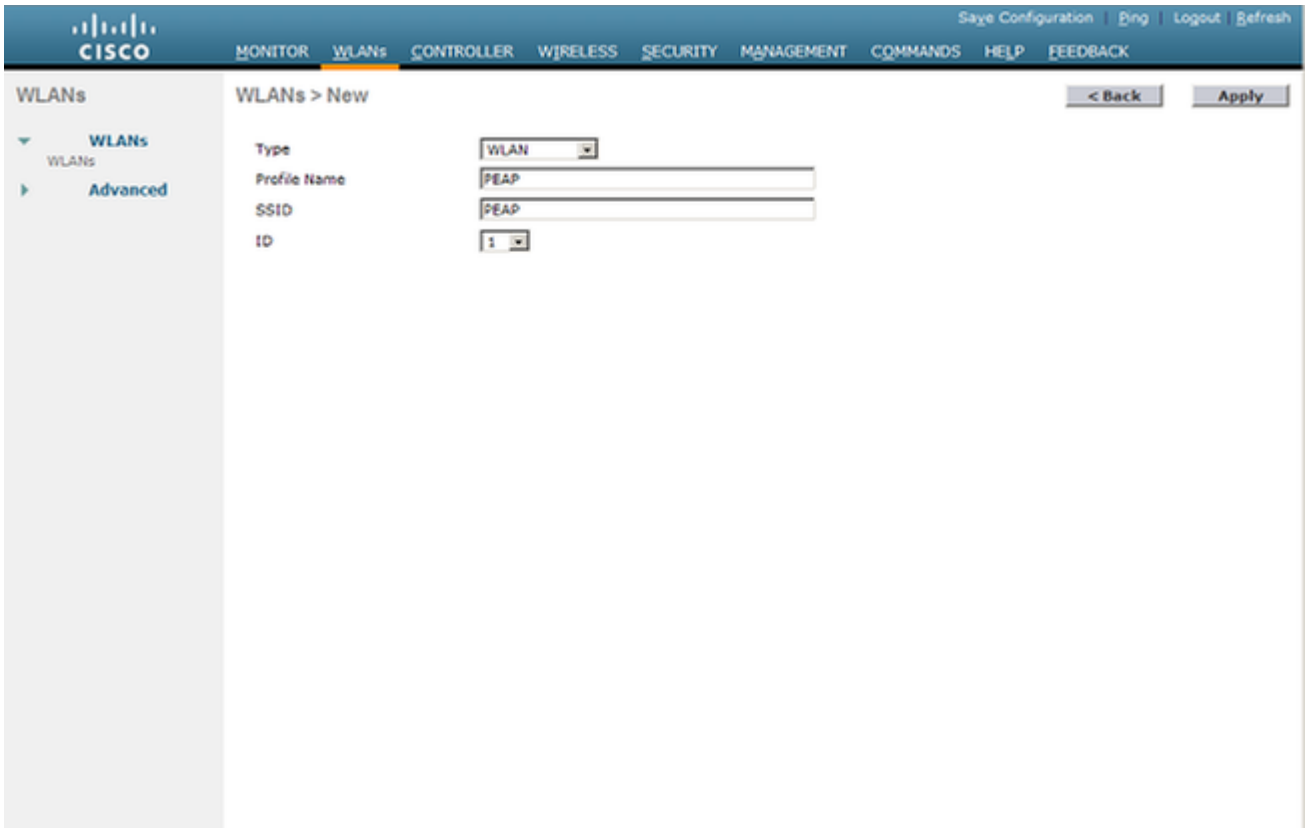
Konfigurieren Sie den Service Set Identifier (SSID) (WLAN), mit dem die Wireless-Clients eine Verbindung herstellen. In diesem Beispiel erstellen Sie die SSID und nennen sie PEAP.

Definieren Sie die Layer-2-Authentifizierung als WPA2, sodass die Clients eine EAP-basierte Authentifizierung (in diesem Beispiel PEAP-MS-CHAP v2) durchführen und den erweiterten Verschlüsselungsstandard (AES) als Verschlüsselungsmechanismus verwenden. Lassen Sie alle anderen Werte unverändert.

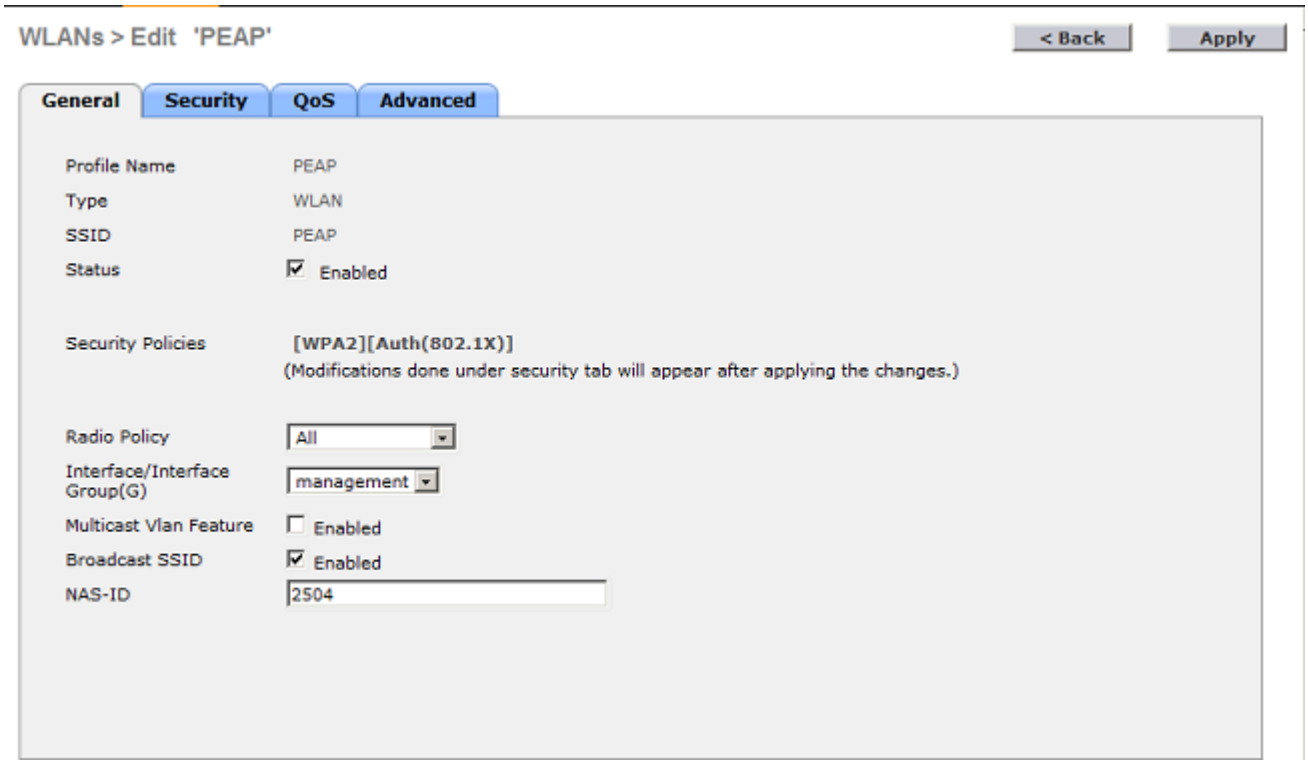
Anmerkung: Dieses Dokument bindet das WLAN an die Verwaltungsschnittstellen. Wenn Sie mehrere VLANs in Ihrem Netzwerk haben, können Sie ein separates VLAN erstellen und dieses an die SSID binden. Weitere Informationen zum Konfigurieren von VLANs auf WLCs finden Sie unter VLANs auf Wireless LAN Controllern - Konfigurationsbeispiel.

Gehen Sie wie folgt vor, um ein WLAN auf dem WLC zu konfigurieren:

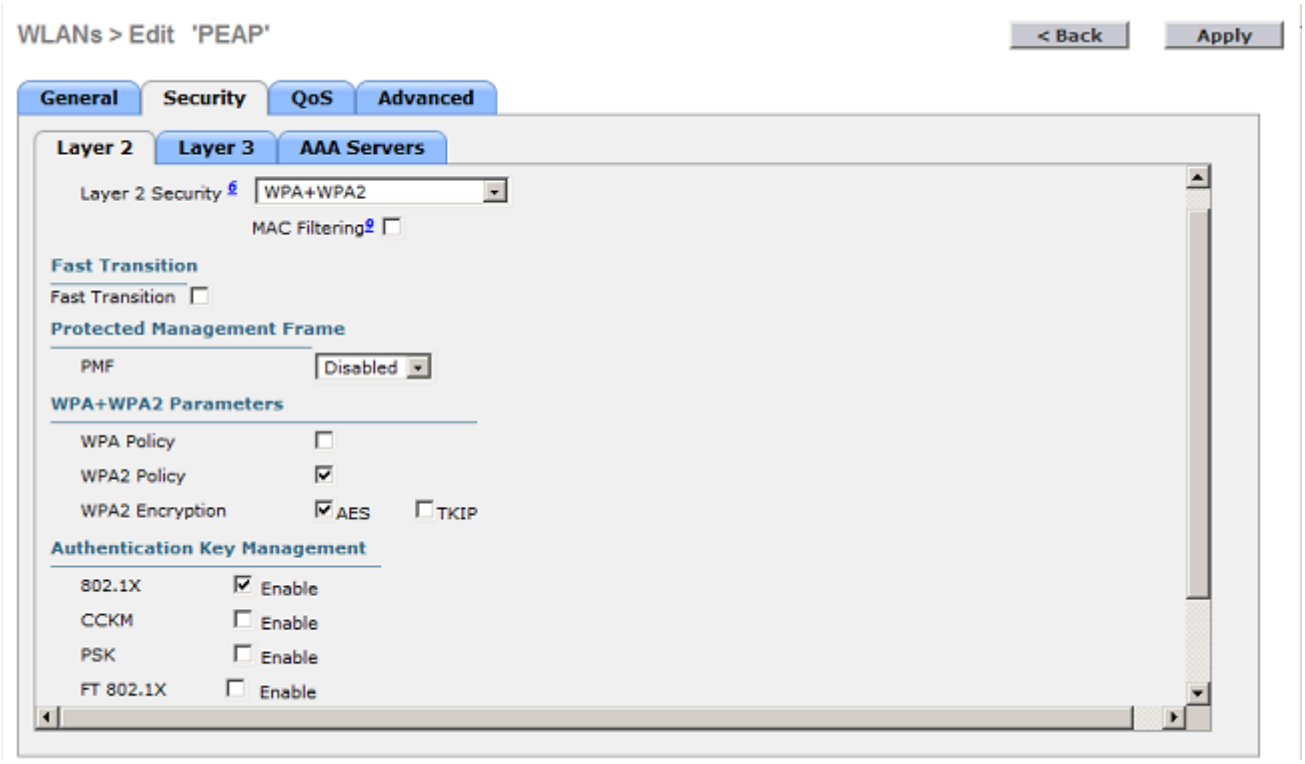
1. Klicken Sie auf WLANs in der Controller-Schnittstelle, um die Seite "WLANs" anzuzeigen. Auf dieser Seite werden die WLANs aufgelistet, die auf dem Controller vorhanden sind.
2. Wählen Sie Neu aus, um ein neues WLAN zu erstellen. Geben Sie die WLAN-ID und die WLAN-SSID für das WLAN ein, und klicken Sie auf Apply.



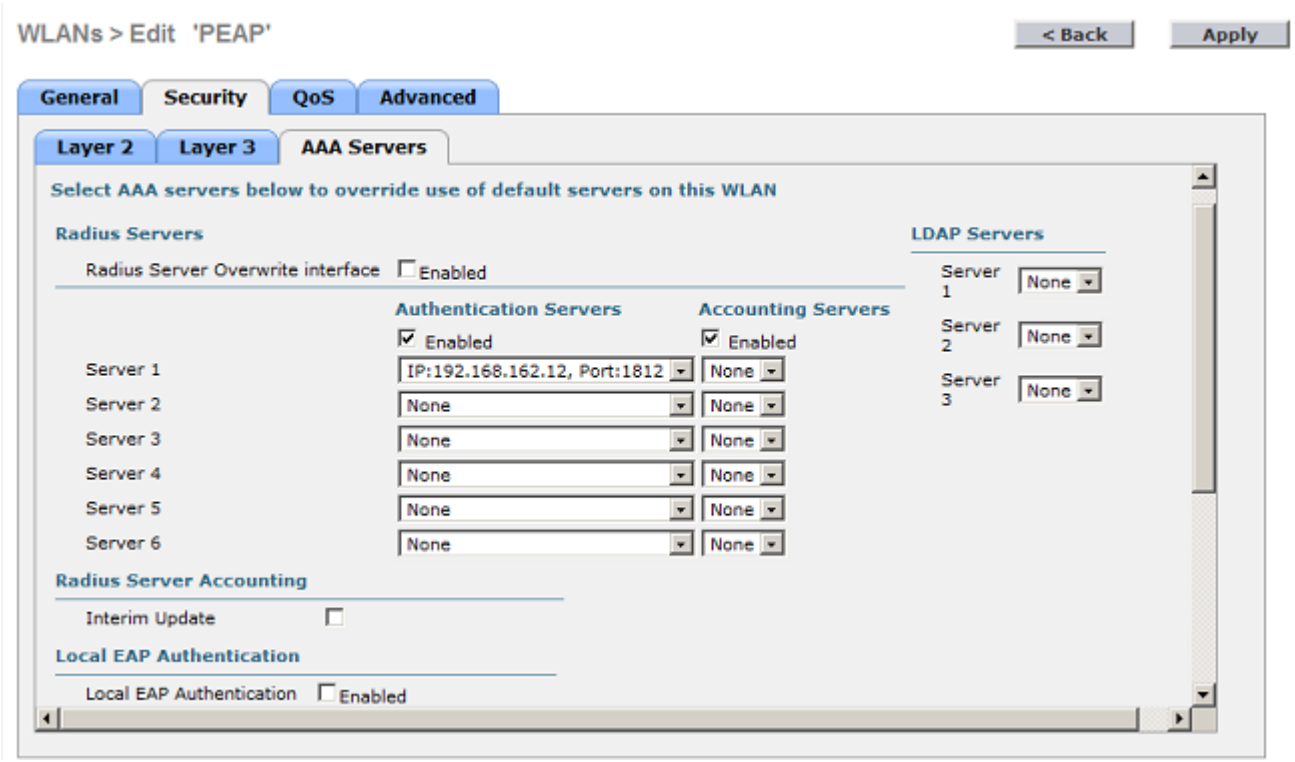
3. Führen Sie die folgenden Schritte aus, um die SSID für 802.1x zu konfigurieren:
    1. Klicken Sie auf die Registerkarte Allgemein, und aktivieren Sie das WLAN.



    2. Klicken Sie auf die Registerkarten Sicherheit > Layer 2, legen Sie die Layer-2-Sicherheit auf WPA + WPA2 fest, aktivieren Sie die Kontrollkästchen WPA + WPA2-Parameter (z. B. WPA2 AES) nach Bedarf, und klicken Sie auf 802.1x als Authentifizierungsschlüsselverwaltung.



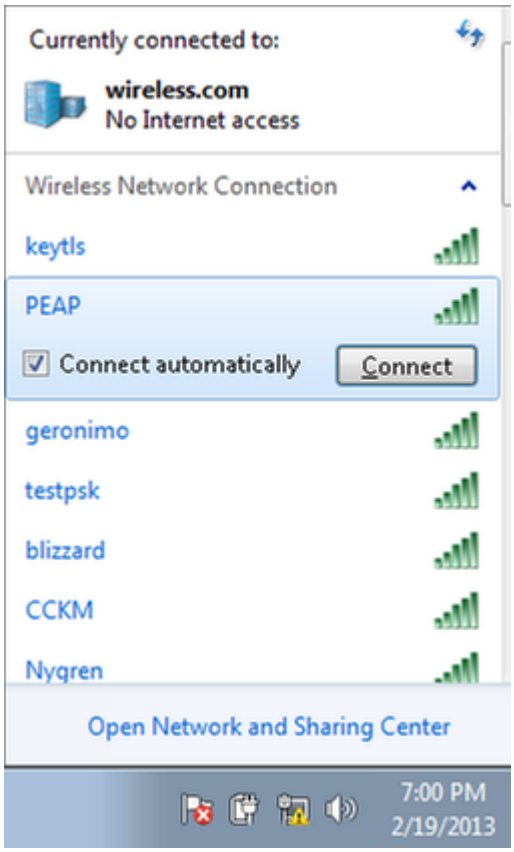
3. Klicken Sie auf die Registerkarten Sicherheit > AAA-Server, wählen Sie die IP-Adresse des NPS aus der Dropdown-Liste Server 1 aus, und klicken Sie auf Anwenden.



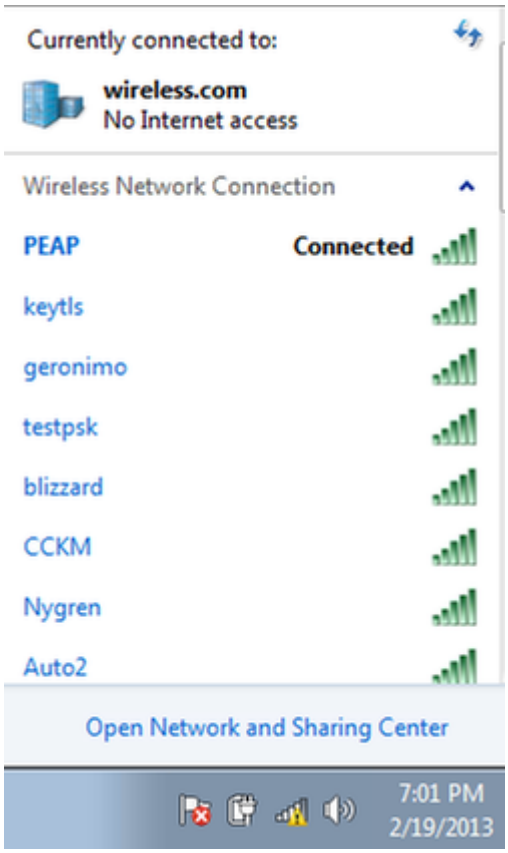
Konfigurieren der Wireless Clients für die PEAP-MS-CHAP v2-Authentifizierung

Führen Sie diese Schritte aus, um den Wireless-Client mit dem Windows Zero Config Tool für die Verbindung mit dem PEAP-WLAN zu konfigurieren.

1. Klicken Sie in der Taskleiste auf das Symbol Netzwerk. Klicken Sie auf die PEAP-SSID und dann auf Verbinden.



2. Der Client muss nun mit dem Netzwerk verbunden sein.



3. Wenn die Verbindung ausfällt, versuchen Sie, erneut eine Verbindung zum WLAN herzustellen. Wenn das Problem weiterhin besteht, lesen Sie den Abschnitt Fehlerbehebung.

Überprüfung

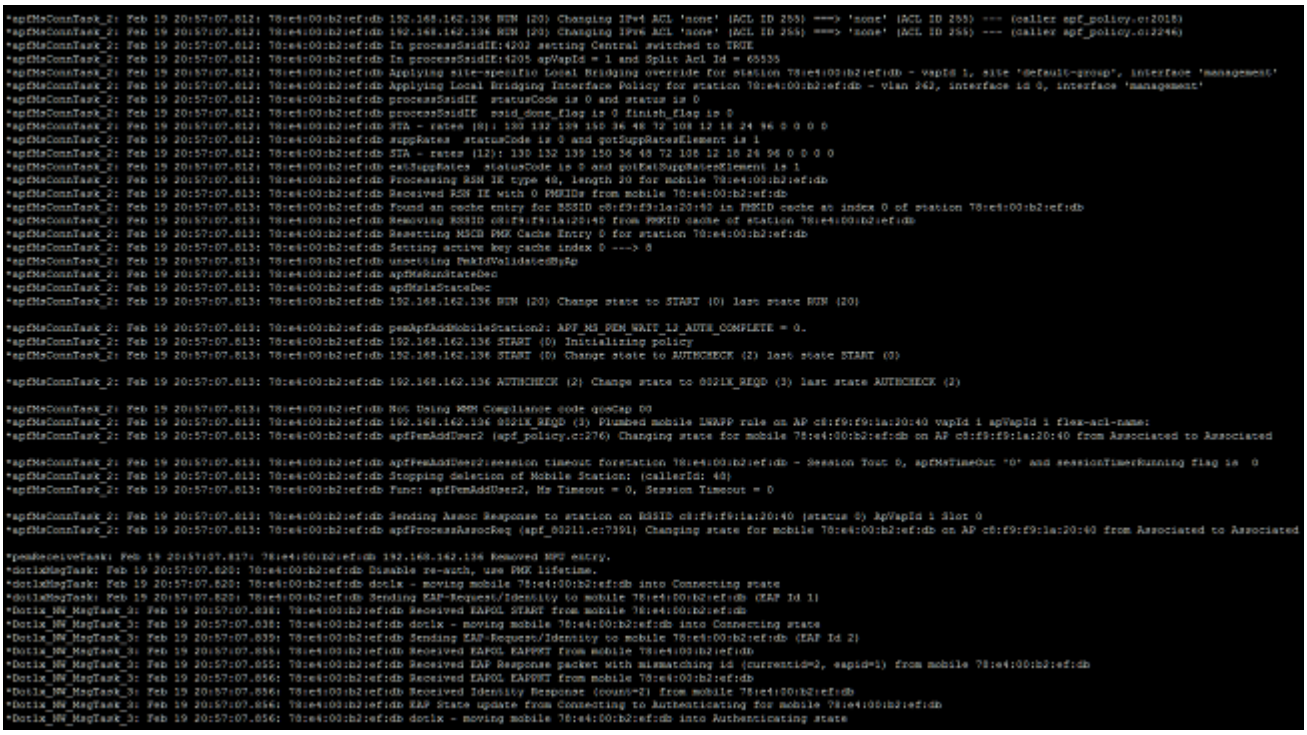
Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Wenn Ihr Client keine Verbindung mit dem WLAN hergestellt hat, finden Sie in diesem Abschnitt Informationen, die Sie zur Fehlerbehebung bei der Konfiguration verwenden können.

Es gibt zwei Tools, mit denen 802.1x-Authentifizierungsfehler diagnostiziert werden können: den Befehl debug client und die Ereignisanzeige in Windows.

Wenn Sie ein Client-Debugging vom WLC aus durchführen, ist dies nicht ressourcenintensiv und hat keine Auswirkungen auf den Service. Um eine Debugsitzung zu starten, öffnen Sie die Befehlszeilenschnittstelle (CLI) des WLC, und geben Sie die MAC-Adresse des Debugclients ein, wobei die MAC-Adresse die MAC-Adresse des Wireless-Clients ist, der keine Verbindung herstellen kann. Versuchen Sie, während dieses Debugs eine Verbindung mit dem Client herzustellen. Für die CLI des WLC muss eine Ausgabe vorhanden sein, die ähnlich wie in diesem Beispiel aussieht:



Dies ist ein Beispiel für ein Problem, das bei einer fehlerhaften Konfiguration auftreten kann. Hier zeigt das WLC-Debugging an, dass der WLC in den Authentifizierungsstatus gewechselt ist, was

bedeutet, dass der WLC auf eine Antwort vom NPS wartet. Dies ist in der Regel auf einen falschen gemeinsamen geheimen Schlüssel auf dem WLC oder dem NPS zurückzuführen. Sie können dies über die Windows Server-Ereignisanzeige bestätigen. Wenn Sie kein Protokoll finden, hat die Anforderung es nie an den NPS geschafft.

Ein weiteres Beispiel aus dem WLC-Debugging ist ein Access-Reject. Eine Zugriffszurückweisung zeigt an, dass der NPS die Client-Anmeldeinformationen empfangen und zurückgewiesen hat. Dies ist ein Beispiel für einen Client, der eine Zugriffsablehnung empfängt:

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

Wenn eine Zugriffszurückweisung angezeigt wird, überprüfen Sie die Protokolle in den Windows Server-Ereignisprotokollen, um zu ermitteln, warum der NPS auf den Client mit einer Zugriffszurückweisung reagiert hat.

Bei einer erfolgreichen Authentifizierung wird im Client-Debugging der Status "access-accept" (Akzeptieren) verwendet, wie in diesem Beispiel gezeigt:

```
*dot1xMsgTask: Feb 19 21:33:14.576: 78:e4:00:b2:ef:db Sending EAP-Request/Identity to mobile 78:e4:00:b2:ef:db (EAP Id 1)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.596: 78:e4:00:b2:ef:db Received EAPOL START from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.596: 78:e4:00:b2:ef:db dot1x - moving mobile 78:e4:00:b2:ef:db into Connecting state
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.596: 78:e4:00:b2:ef:db Sending EAP-Request/Identity to mobile 78:e4:00:b2:ef:db (EAP Id 2)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.601: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.601: 78:e4:00:b2:ef:db Received EAP Response packet with mismatching id (currentid=2, eapid=1) from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.611: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.611: 78:e4:00:b2:ef:db Received Identity Response (count=2) from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.611: 78:e4:00:b2:ef:db EAP State update from Connecting to Authenticating for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.611: 78:e4:00:b2:ef:db dot1x - moving mobile 78:e4:00:b2:ef:db into Authenticating state
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.611: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.663: 78:e4:00:b2:ef:db Processing Access-Challenge for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.663: 78:e4:00:b2:ef:db Entering Backend Auth Req state (id=3) for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.663: 78:e4:00:b2:ef:db Sending EAP Request from AAA to mobile 78:e4:00:b2:ef:db (EAP Id 3)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.661: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.661: 78:e4:00:b2:ef:db Received EAP Response from mobile 78:e4:00:b2:ef:db (EAP Id 3, EAP Type 25)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.661: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.665: 78:e4:00:b2:ef:db Processing Access-Challenge for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.665: 78:e4:00:b2:ef:db Entering Backend Auth Req state (id=4) for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.665: 78:e4:00:b2:ef:db Sending EAP Request from AAA to mobile 78:e4:00:b2:ef:db (EAP Id 4)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.674: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.674: 78:e4:00:b2:ef:db Received EAP Response from mobile 78:e4:00:b2:ef:db (EAP Id 4, EAP Type 25)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.674: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.685: 78:e4:00:b2:ef:db Processing Access-Challenge for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.685: 78:e4:00:b2:ef:db Entering Backend Auth Req state (id=7) for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.685: 78:e4:00:b2:ef:db WARNING: updated EAP-Identifier 4 ===> 7 for STA 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.685: 78:e4:00:b2:ef:db Sending EAP Request from AAA to mobile 78:e4:00:b2:ef:db (EAP Id 7)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.706: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.706: 78:e4:00:b2:ef:db Received EAP Response from mobile 78:e4:00:b2:ef:db (EAP Id 7, EAP Type 25)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.706: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.709: 78:e4:00:b2:ef:db Processing Access-Challenge for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.709: 78:e4:00:b2:ef:db Entering Backend Auth Req state (id=8) for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.709: 78:e4:00:b2:ef:db Sending EAP Request from AAA to mobile 78:e4:00:b2:ef:db (EAP Id 8)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.721: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.721: 78:e4:00:b2:ef:db Received EAP Response from mobile 78:e4:00:b2:ef:db (EAP Id 8, EAP Type 25)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.721: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.726: 78:e4:00:b2:ef:db Processing Access-Challenge for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.726: 78:e4:00:b2:ef:db Entering Backend Auth Req state (id=9) for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.726: 78:e4:00:b2:ef:db Sending EAP Request from AAA to mobile 78:e4:00:b2:ef:db (EAP Id 9)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.738: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.738: 78:e4:00:b2:ef:db Received EAP Response from mobile 78:e4:00:b2:ef:db (EAP Id 9, EAP Type 25)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.738: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.745: 78:e4:00:b2:ef:db Processing Access-Challenge for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.746: 78:e4:00:b2:ef:db Entering Backend Auth Req state (id=10) for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.746: 78:e4:00:b2:ef:db Sending EAP Request from AAA to mobile 78:e4:00:b2:ef:db (EAP Id 10)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.752: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.752: 78:e4:00:b2:ef:db Received EAP Response from mobile 78:e4:00:b2:ef:db (EAP Id 10, EAP Type 25)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.752: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.758: 78:e4:00:b2:ef:db Processing Access-Challenge for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.758: 78:e4:00:b2:ef:db Entering Backend Auth Req state (id=11) for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.758: 78:e4:00:b2:ef:db Sending EAP Request from AAA to mobile 78:e4:00:b2:ef:db (EAP Id 11)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.770: 78:e4:00:b2:ef:db Received EAPOL EAPPKT from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.770: 78:e4:00:b2:ef:db Received EAP Response from mobile 78:e4:00:b2:ef:db (EAP Id 11, EAP Type 25)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.770: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.781: 78:e4:00:b2:ef:db Processing Access-Accept for mobile 78:e4:00:b2:ef:db
```

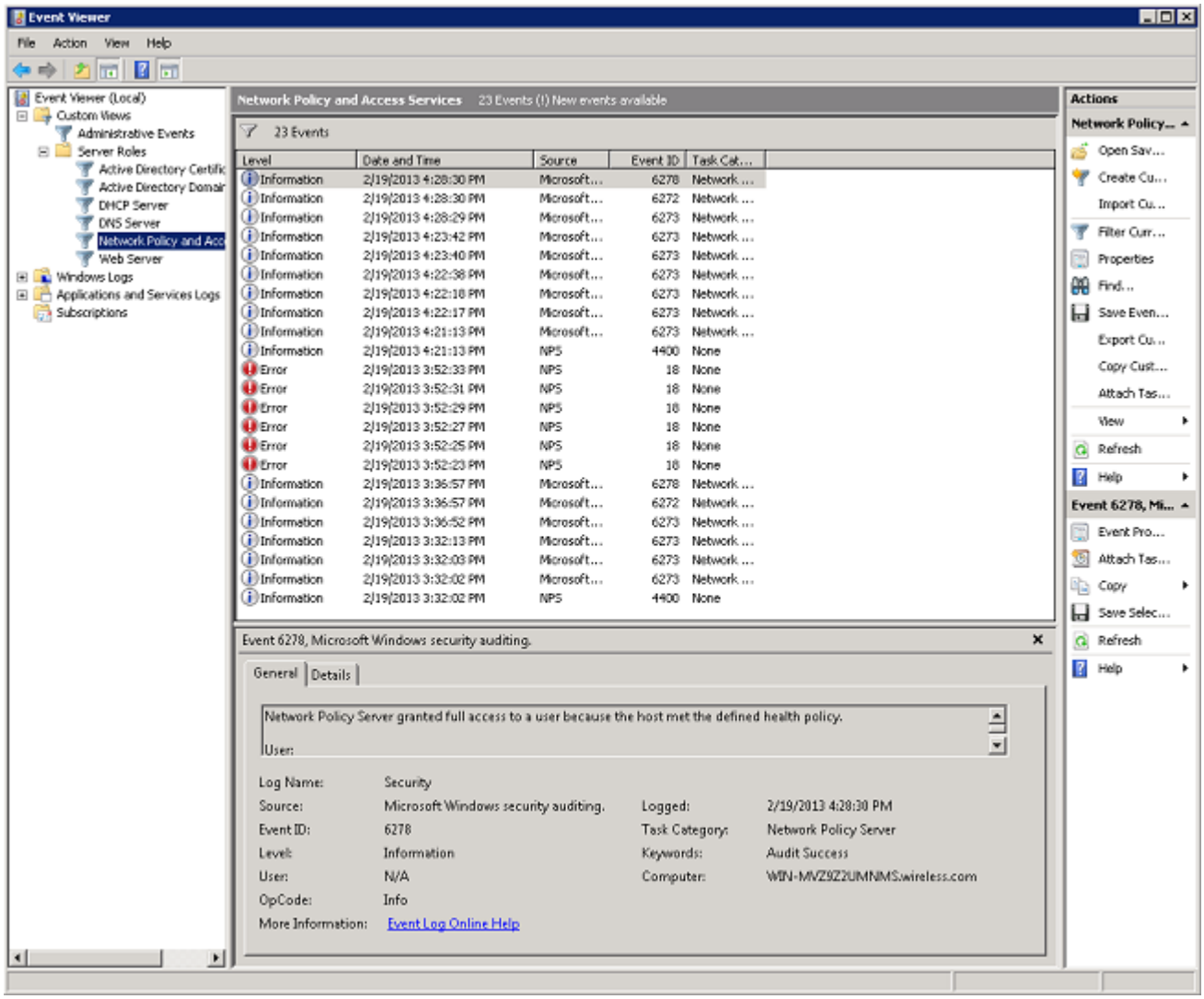
Wenn Sie Probleme mit Zugriffsverweigerungen und Zeitüberschreitungen bei Antworten beheben möchten, ist der Zugriff auf den RADIUS-Server erforderlich. Der WLC fungiert als Authentifizierer, der EAP-Nachrichten zwischen dem Client und dem RADIUS-Server weiterleitet. Ein RADIUS-

Server, der mit einem Timeout bei Ablehnung oder Antwort antwortet, muss vom Hersteller des RADIUS-Dienstes überprüft und diagnostiziert werden.

Anmerkung: TAC bietet keinen technischen Support für RADIUS-Server von Drittanbietern. In den Protokollen auf dem RADIUS-Server wird jedoch im Allgemeinen erläutert, warum eine Clientanforderung abgelehnt oder ignoriert wurde.

Um Probleme mit Zugriffsverweigerungen und Timeouts für Antworten vom NPS zu beheben, überprüfen Sie die NPS-Protokolle in der Windows-Ereignisanzeige auf dem Server.

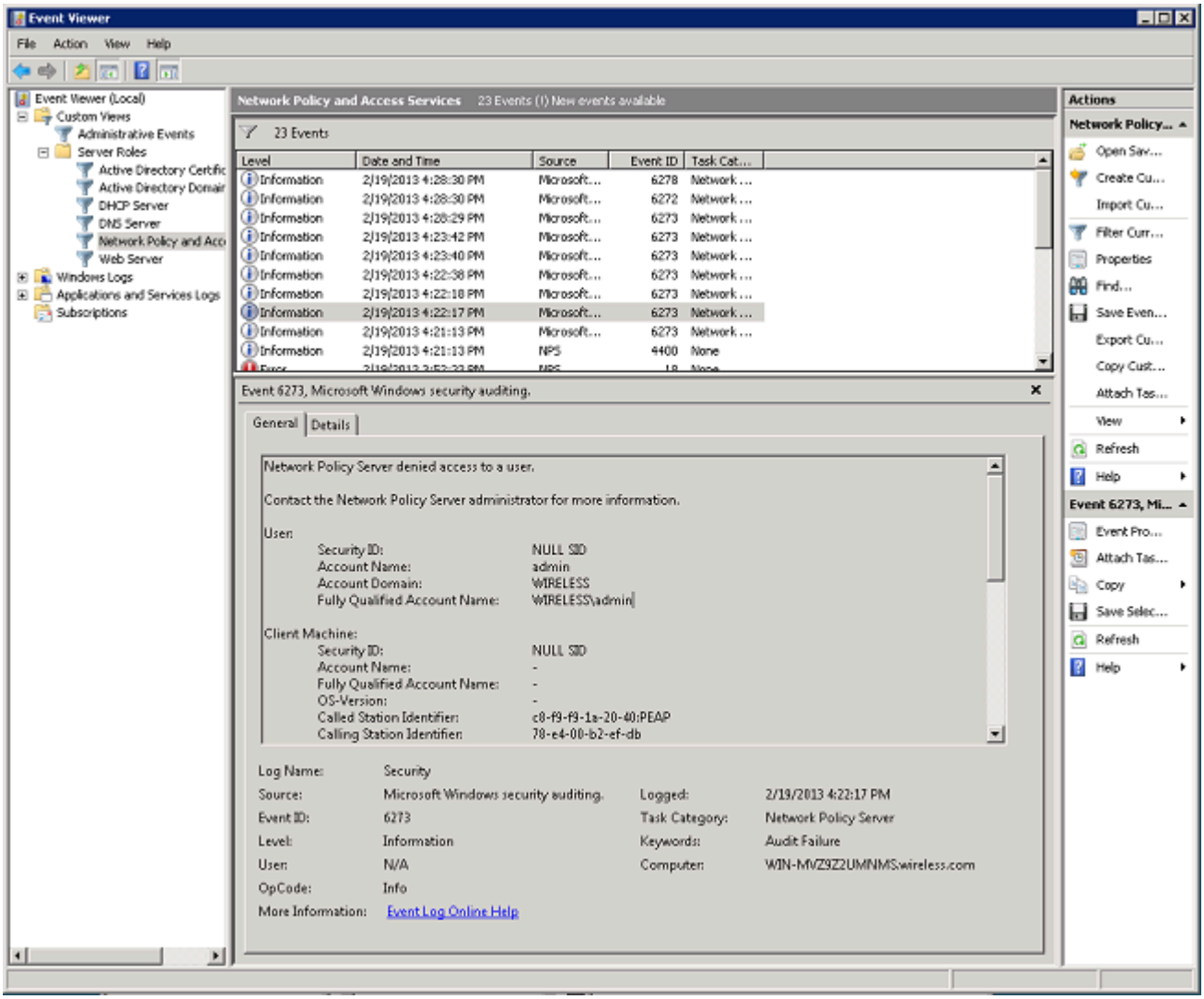
1. Klicken Sie auf Start > Administrator-Tools > Ereignisanzeige, um die Ereignisanzeige zu starten und die NPS-Protokolle zu überprüfen.
2. Erweitern Sie Benutzerdefinierte Ansichten > Serverrollen > Netzwerkrichtlinie und Zugriff.



In diesem Abschnitt der Ereignisansicht werden Protokolle der übergebenen und fehlgeschlagenen Authentifizierungen angezeigt. Untersuchen Sie diese Protokolle, um zu ermitteln, warum ein Client die Authentifizierung nicht weitergibt. Sowohl erfolgreiche als auch fehlgeschlagene Authentifizierungen werden als informativ angezeigt. Scrollen Sie durch die

Protokolle, um den Benutzernamen zu finden, der nicht authentifiziert werden konnte und der eine Zugriffsablehnung erhalten hat, die auf den WLC-Debugs basiert.

Dies ist ein Beispiel für einen NPS, wenn einem Benutzer der Zugriff verweigert wird:

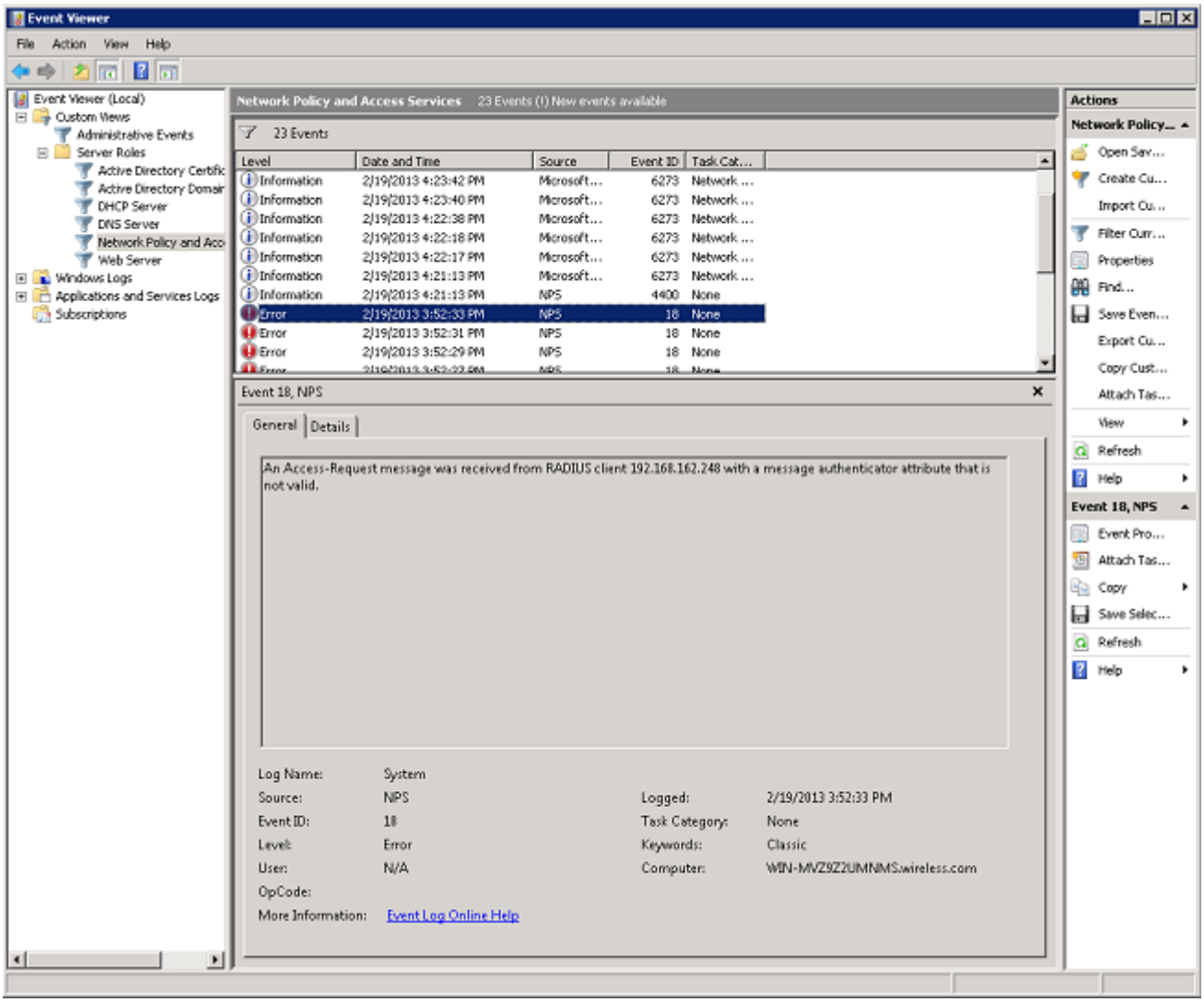


Wenn Sie eine deny-Anweisung in der Ereignisanzeige überprüfen, überprüfen Sie den Abschnitt Authentifizierungsdetails. In diesem Beispiel können Sie sehen, dass der NPS dem Benutzer den Zugriff aufgrund eines falschen Benutzernamens verweigert hat:

```
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.
```

Die Ereignisansicht auf dem NPS hilft Ihnen auch, wenn Sie eine Fehlerbehebung durchführen müssen, wenn der WLC keine Antwort vom NPS erhält. Dies wird in der Regel durch einen falschen gemeinsamen geheimen Schlüssel zwischen dem NPS und dem WLC verursacht.

In diesem Beispiel verwirft der NPS die Anforderung vom WLC aufgrund eines falschen gemeinsamen geheimen Schlüssels:



Zugehörige Informationen

- [Technischer Support und Downloads von Cisco]

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.