

# Konfigurieren von NPS, Wireless LAN Controllern und drahtlosen Netzwerken

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[PEAP-Übersicht](#)

[PEAP Phase 1: TLS-verschlüsselter Kanal](#)

[PEAP Phase 2: EAP-authentifizierte Kommunikation](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Konfigurieren von Microsoft Windows 2008 Server](#)

[Konfigurieren von Microsoft Windows 2008 Server als Domänencontroller](#)

[Installieren und Konfigurieren der DHCP-Dienste auf dem Microsoft Windows 2008 Server](#)

[Installieren und Konfigurieren von Microsoft Windows 2008 Server als Zertifikatsstellenserver](#)

[Clients mit der Domäne verbinden](#)

[Installieren des Netzwerkrichtlinienservers auf dem Microsoft Windows 2008 Server](#)

[Installieren eines Zertifikats](#)

[Konfigurieren des Netzwerkrichtlinienserver-Diensts für die PEAP-MS-CHAP v2-Authentifizierung](#)

[Hinzufügen von Benutzern zum Active Directory](#)

[Konfigurieren des Wireless LAN-Controllers und der LAPs](#)

[Konfigurieren des WLC für die RADIUS-Authentifizierung](#)

[Konfigurieren eines WLAN für die Clients](#)

[Konfigurieren der Wireless Clients für die PEAP-MS-CHAP v2-Authentifizierung](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

---

## 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

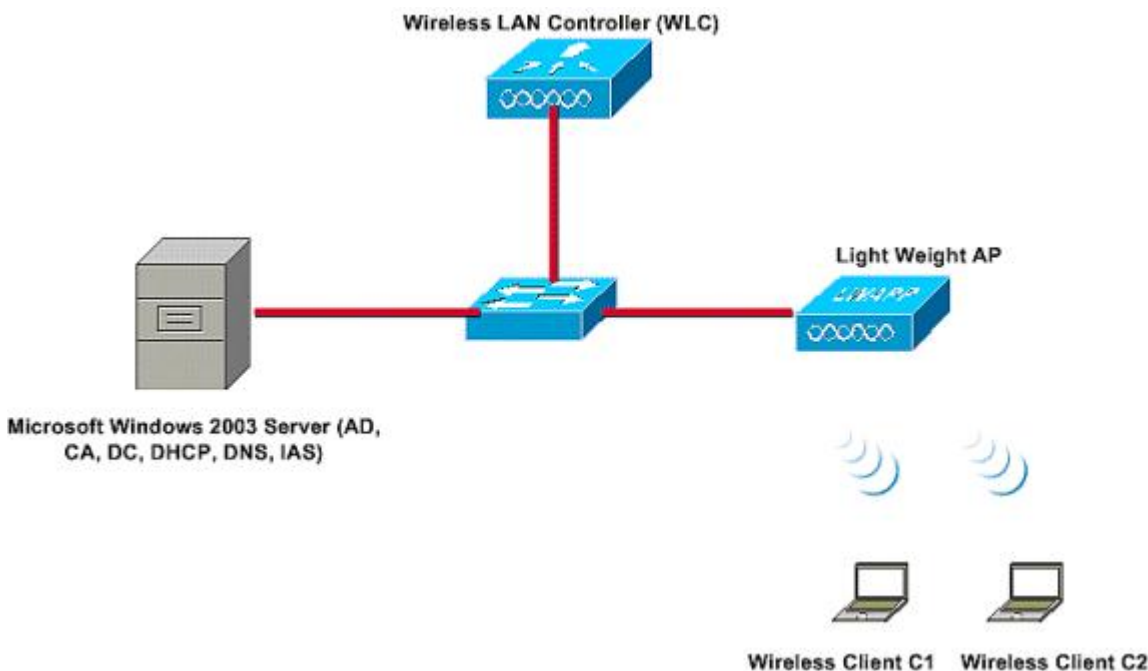
In diesem Abschnitt werden die Informationen zur Konfiguration von PEAP-MS-CHAP v2 angezeigt.



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

## Netzwerkdiagramm

Bei dieser Konfiguration wird folgende Netzwerkkonfiguration verwendet:



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

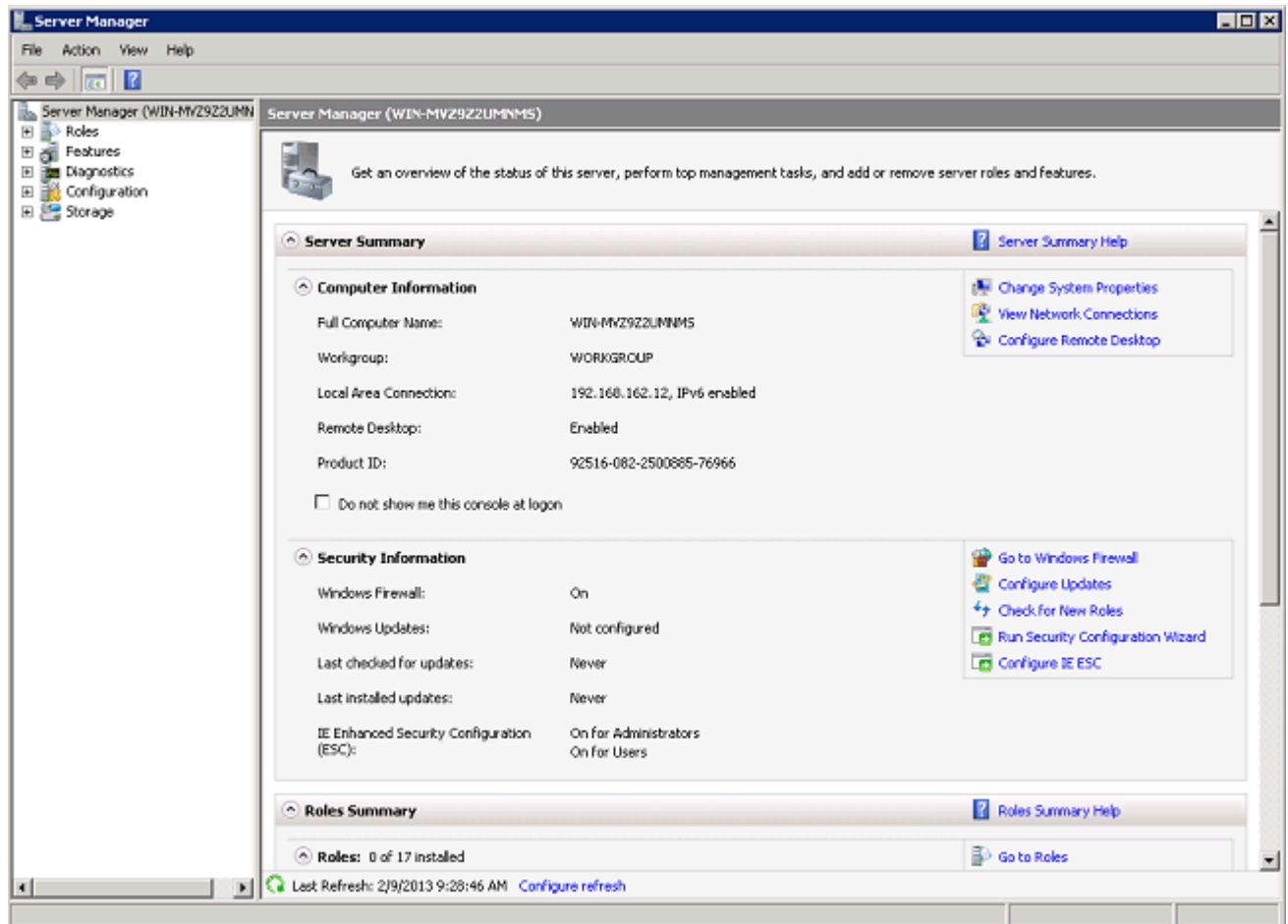
In diesem Beispiel umfasst eine vollständige Konfiguration des Microsoft Windows 2008-Servers die folgenden Schritte:

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

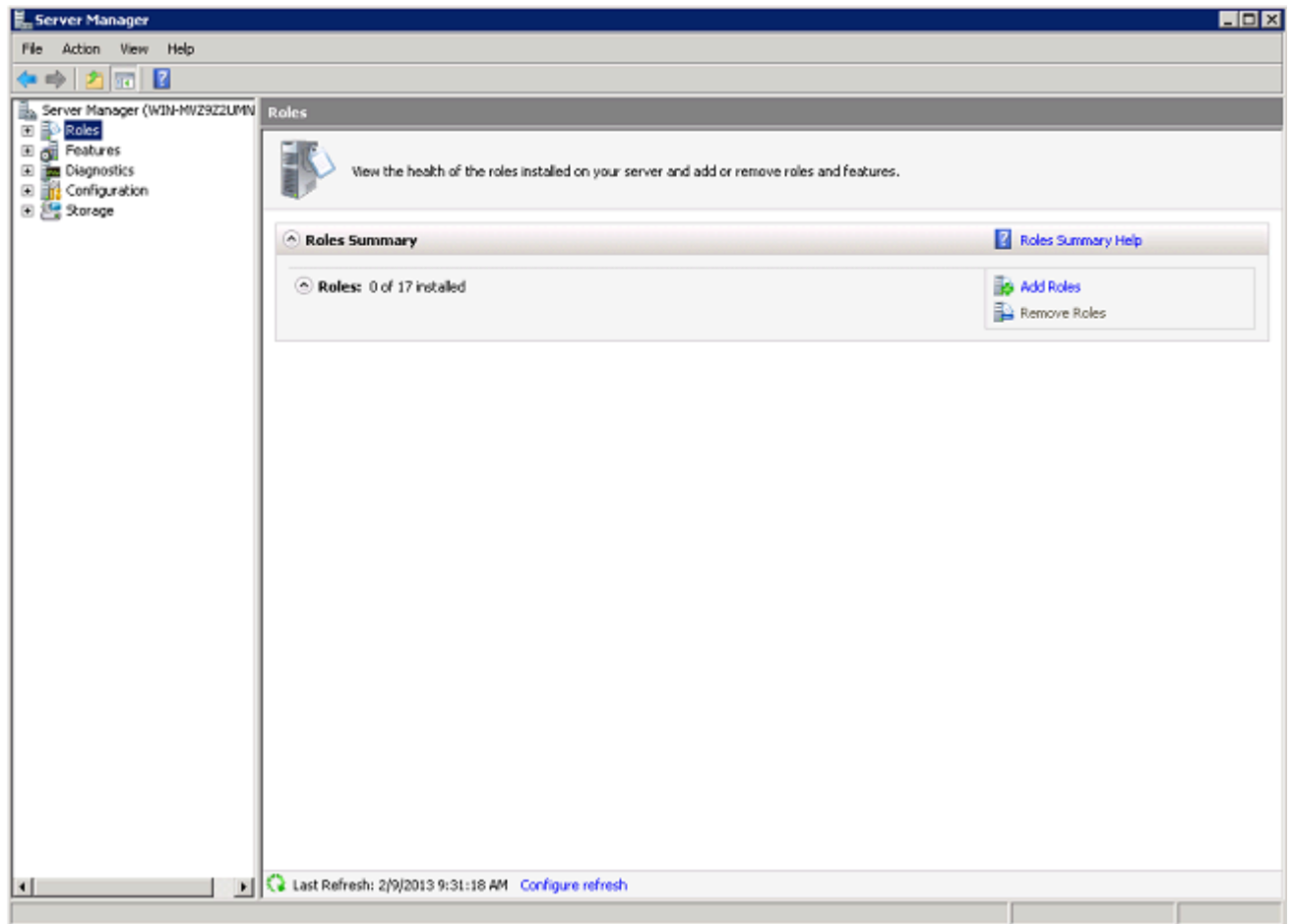
### Konfigurieren von Microsoft Windows 2008 Server als Domänencontroller

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).

**Add Roles Wizard**

 **Before You Begin**

**Before You Begin**

Server Roles

Confirmation

Progress

Results

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

Before you continue, verify that:

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

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

To continue, click Next.


☐ Skip this page by default

< Previous   **Next >**   Install   Cancel

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



**Add Roles Wizard**

 **Select Server Roles**

**Before You Begin**

**Server Roles**

Active Directory Domain Services

Confirmation

Progress

Results

Select one or more roles to install on this server.

Roles:

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

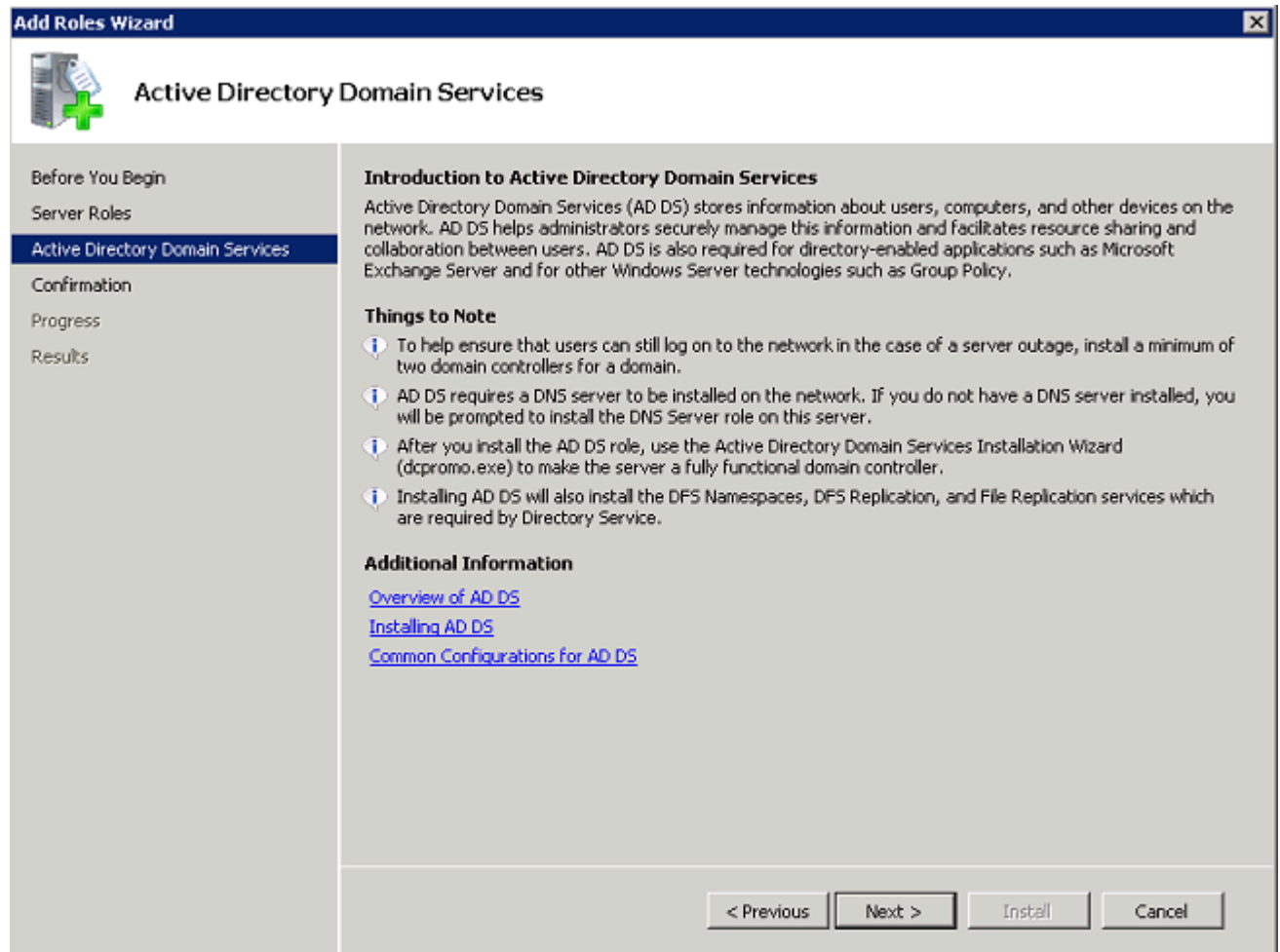
[More about server roles](#)

Description:

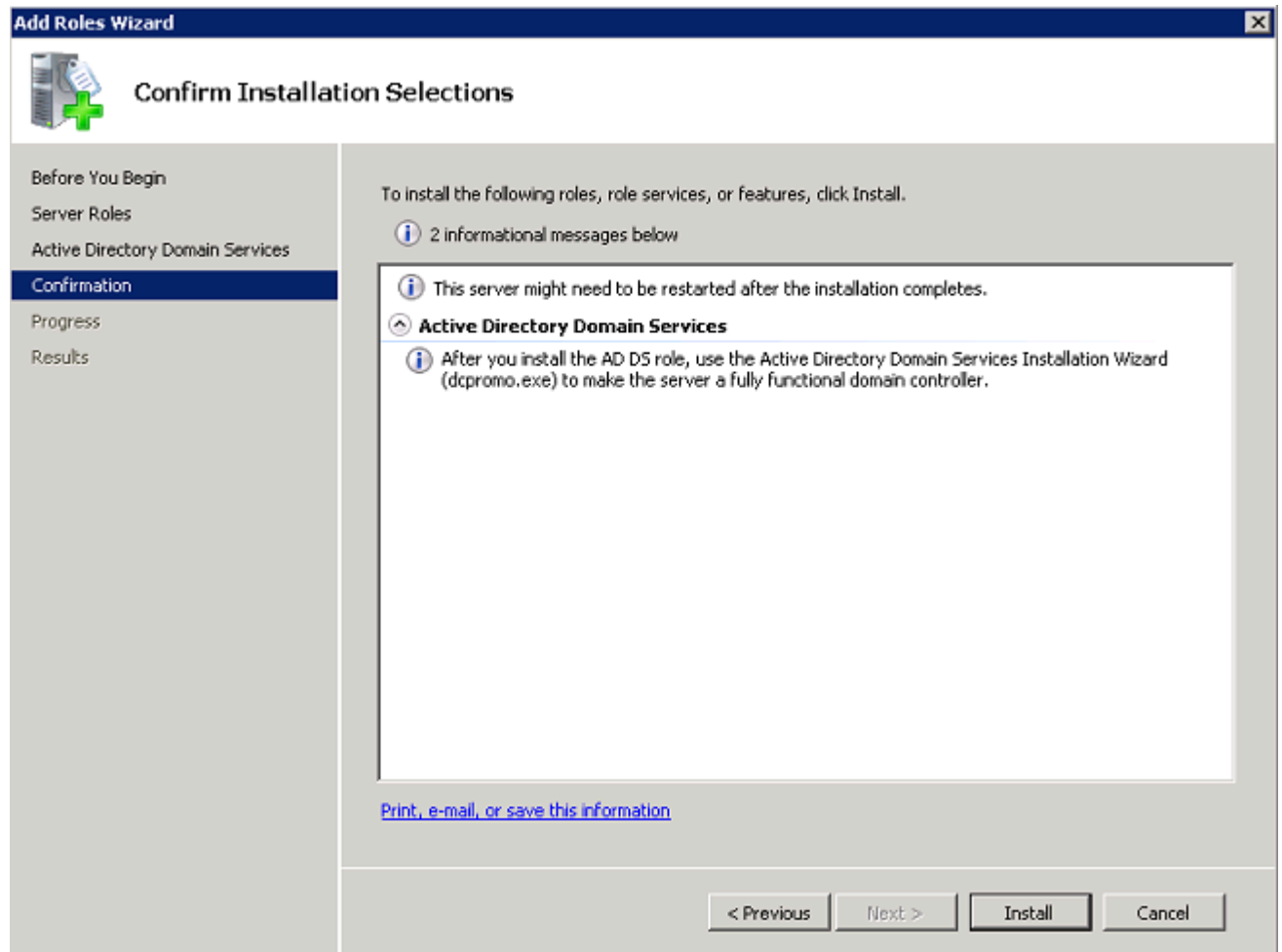
[Active Directory Domain Services \(AD DS\)](#) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

< Previous   Next >   Install   Cancel

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

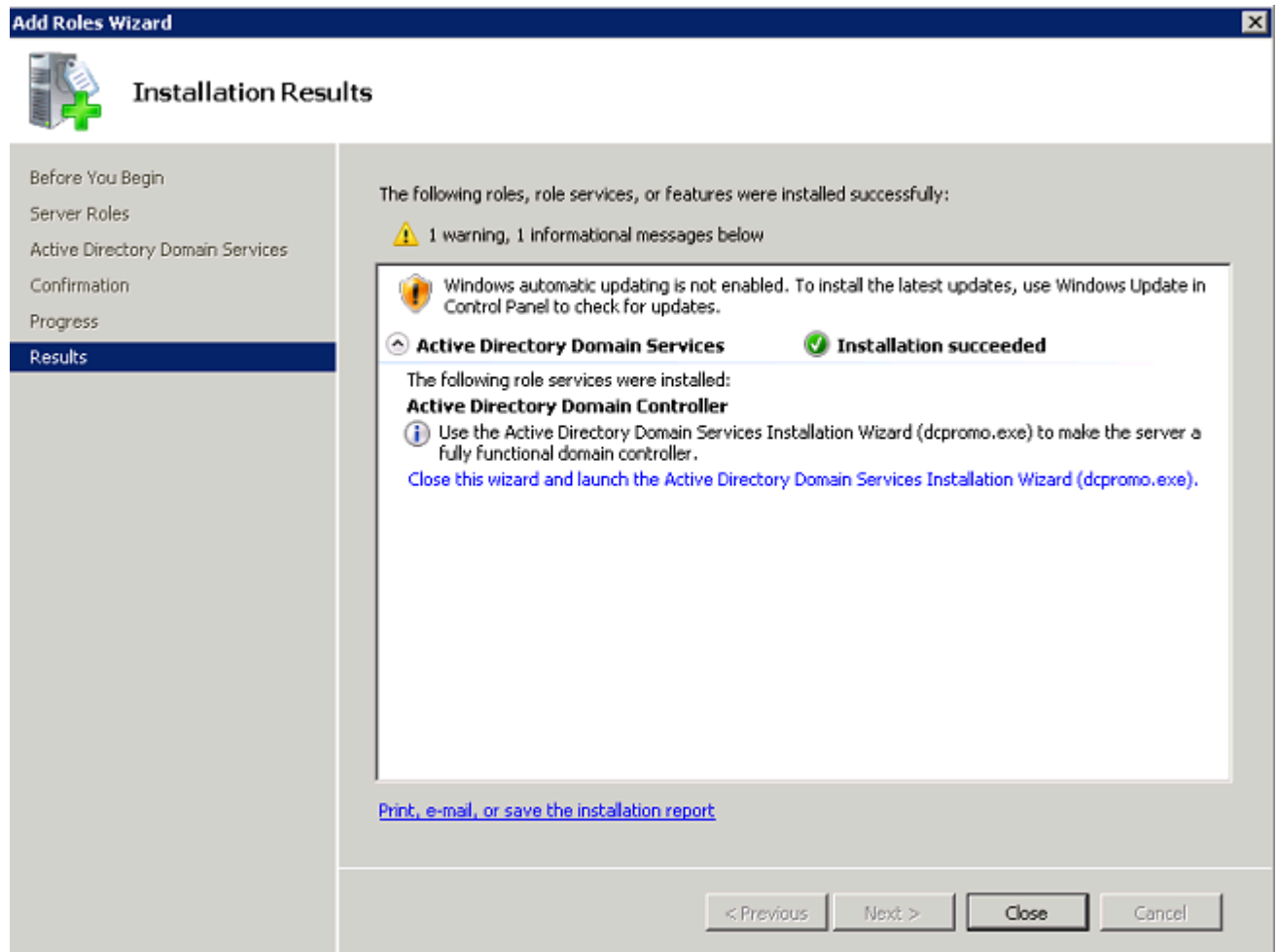


6. Klicken Sie auf Installieren, um die Installation zu starten.



Die Installation wird fortgesetzt und abgeschlossen.

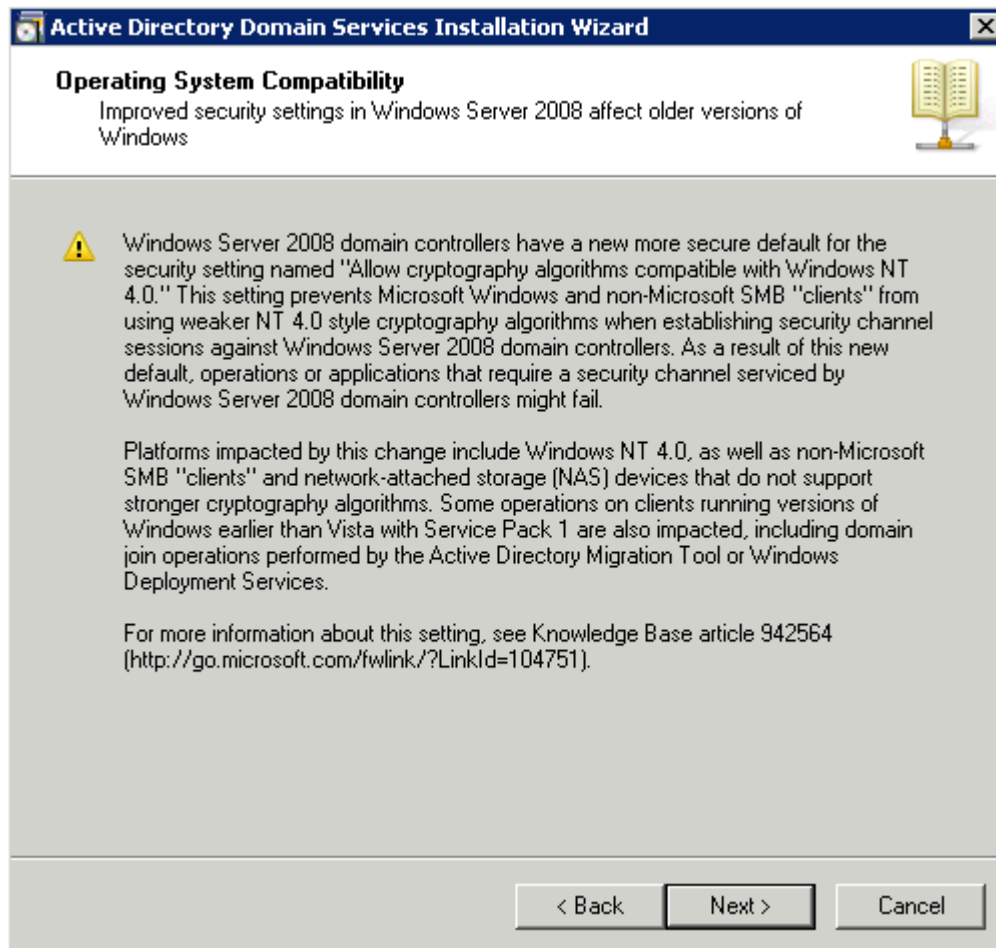
7. Klicken Sie auf Diesen Assistenten schließen, und starten Sie den Assistenten zum Installieren der Active Directory-Domänendienste (dcpromo.exe), um die Installation und Konfiguration von Active Directory fortzusetzen.



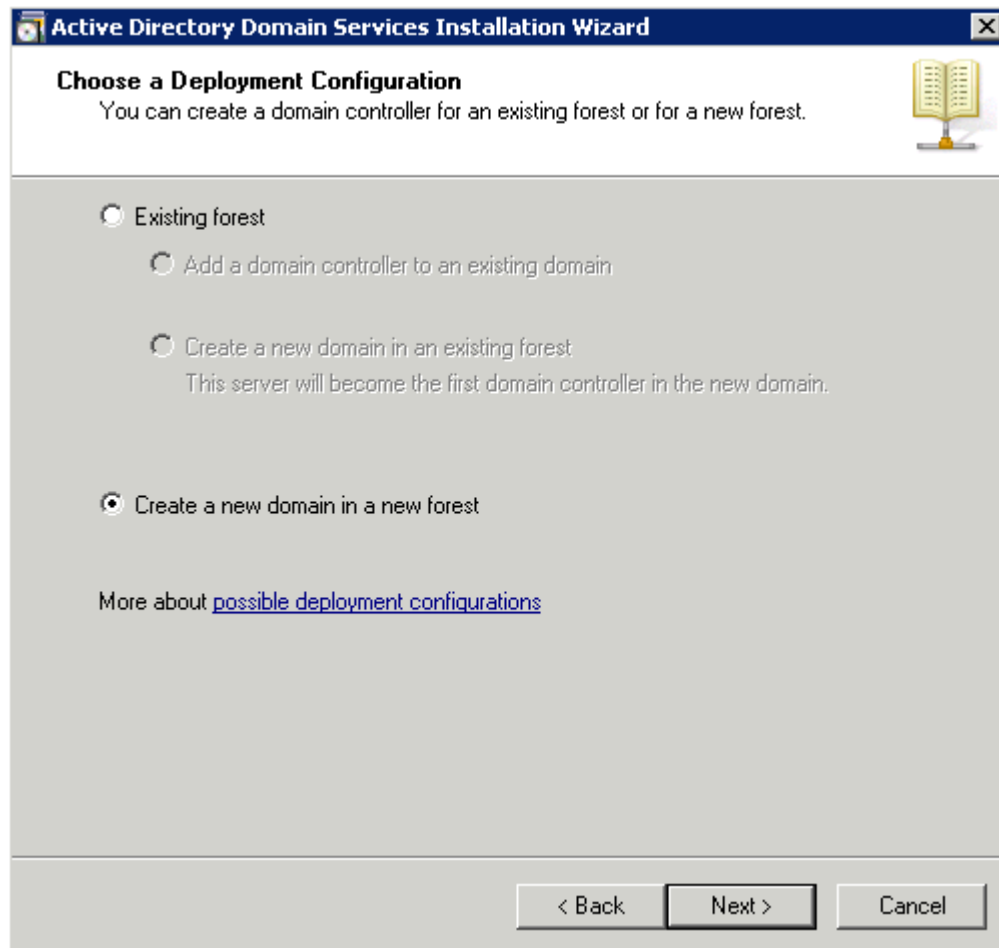
8. Klicken Sie auf Weiter, um den Assistenten zum Installieren der Active Directory-Domänendienste auszuführen.



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.

**Active Directory Domain Services Installation Wizard**

**Name the Forest Root Domain**

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

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

FQDN of the forest root domain:

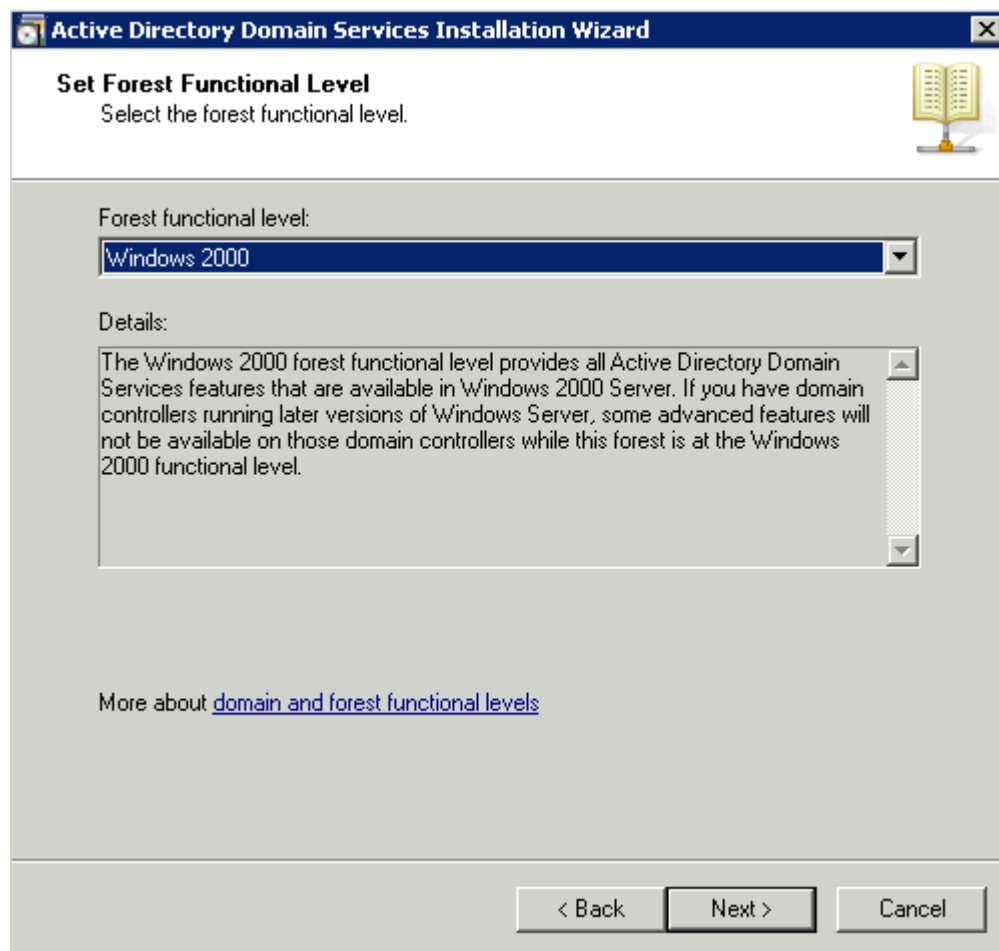
wireless.com

Example: corp.contoso.com

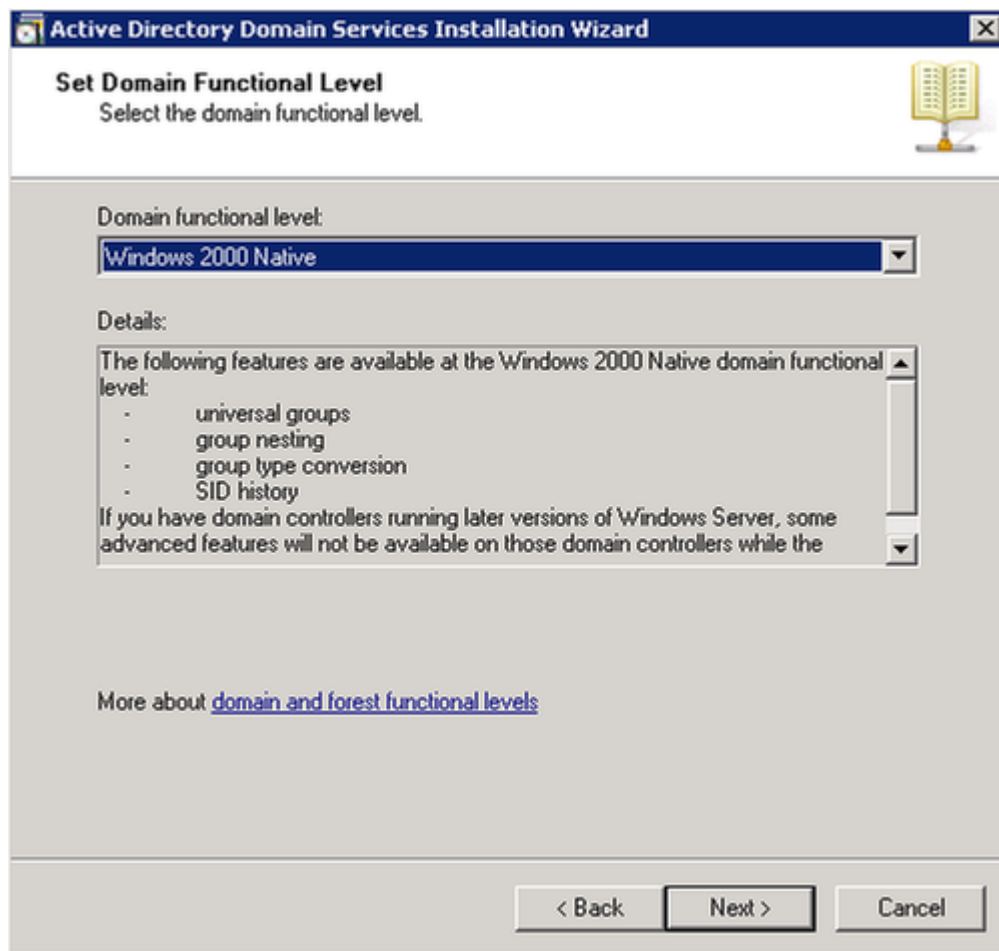
< Back   Next >   Cancel

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

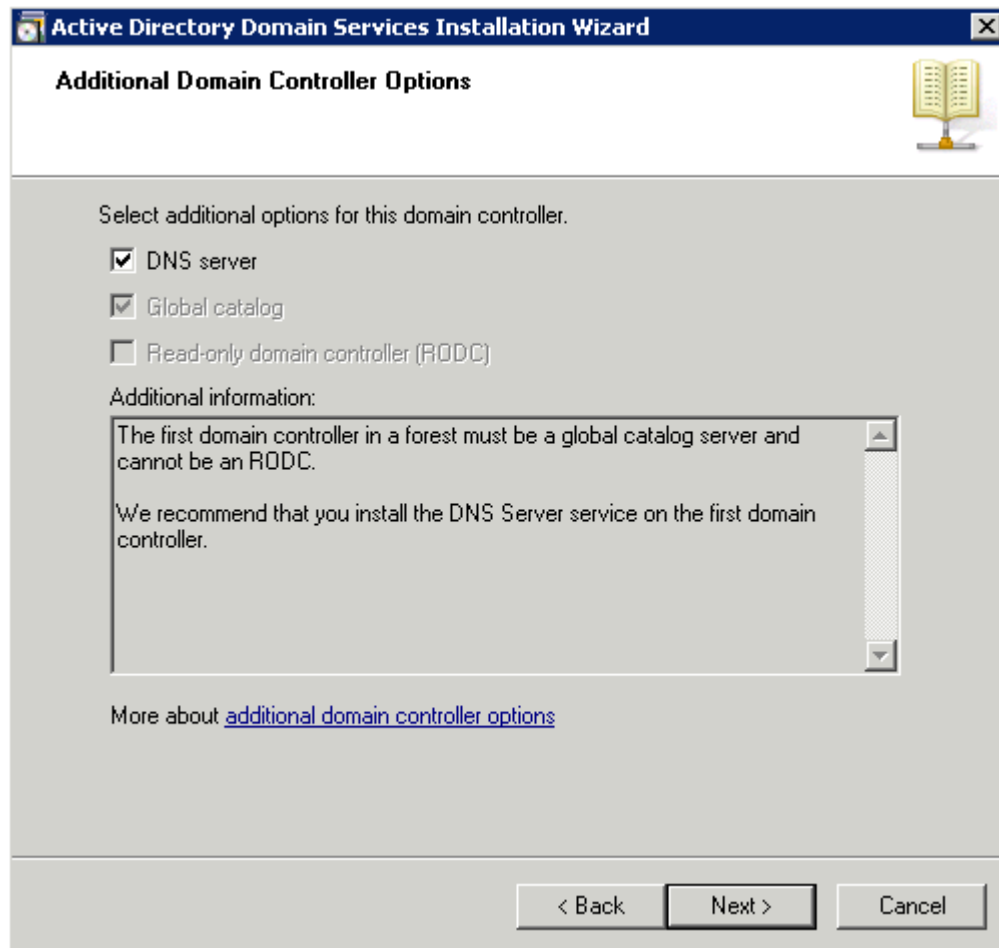




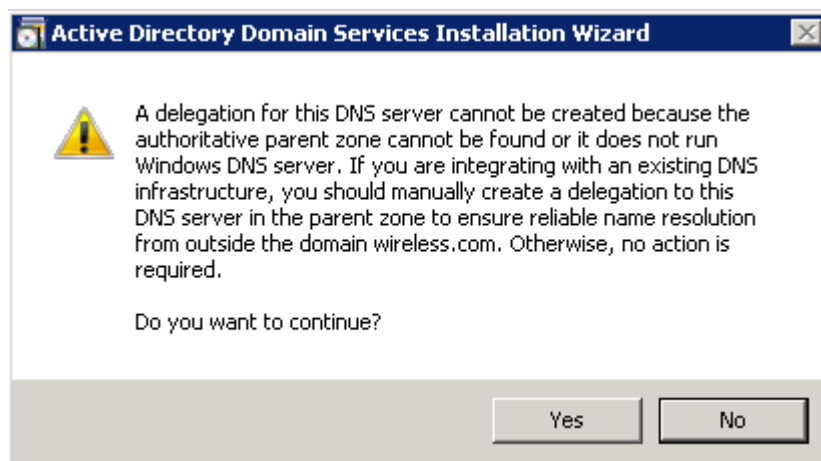
13. Wählen Sie die funktionale Domänenebene für Ihre Domäne aus, und klicken Sie auf Weiter.



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.

**Active Directory Domain Services Installation Wizard**

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

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

Database folder:

Log files folder:

SYSVOL folder:

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

< Back   Next >   Cancel

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

**Active Directory Domain Services Installation Wizard**

**Directory Services Restore Mode Administrator Password**

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

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

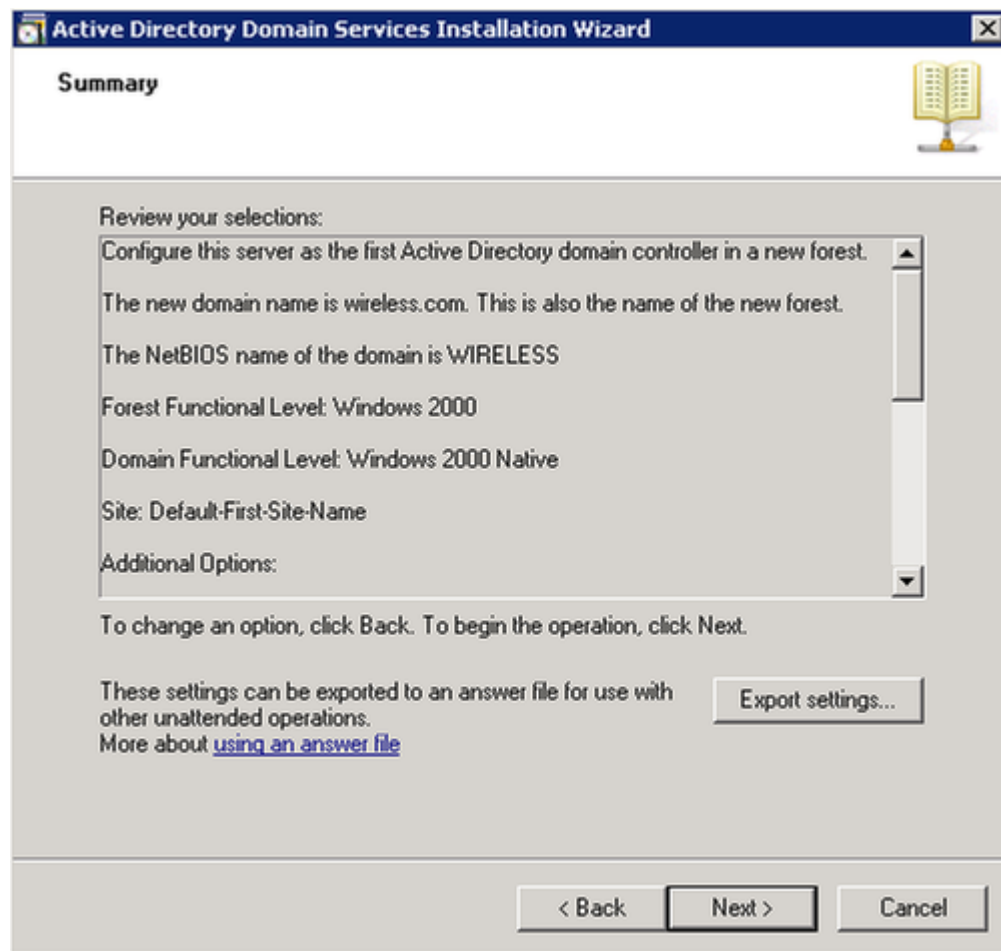
Password:

Confirm password:

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

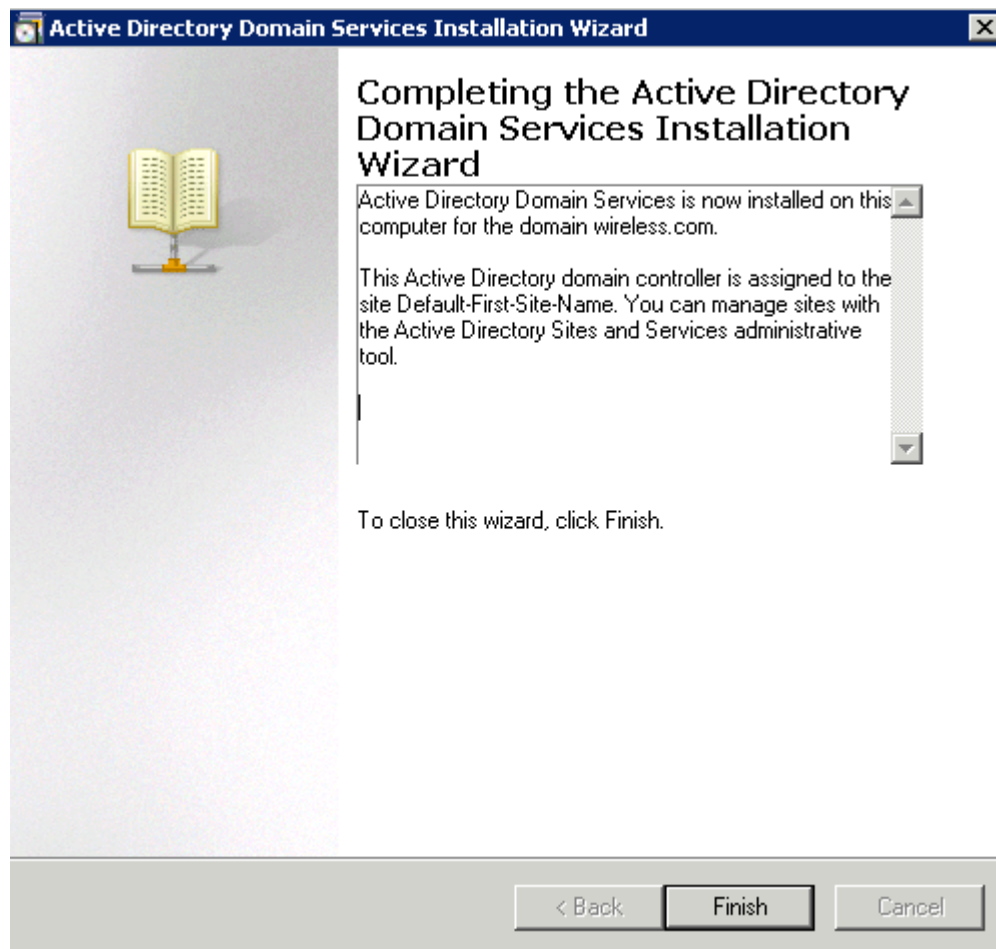
< Back   Next >   Cancel

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

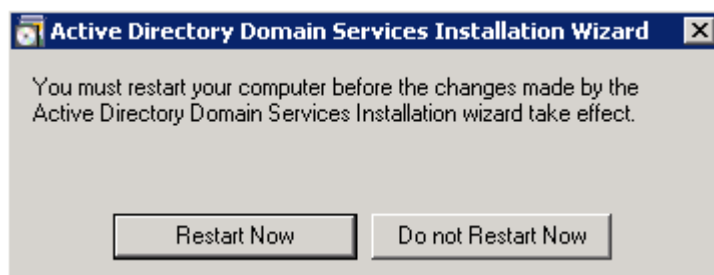


Die Installation wird fortgesetzt.

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



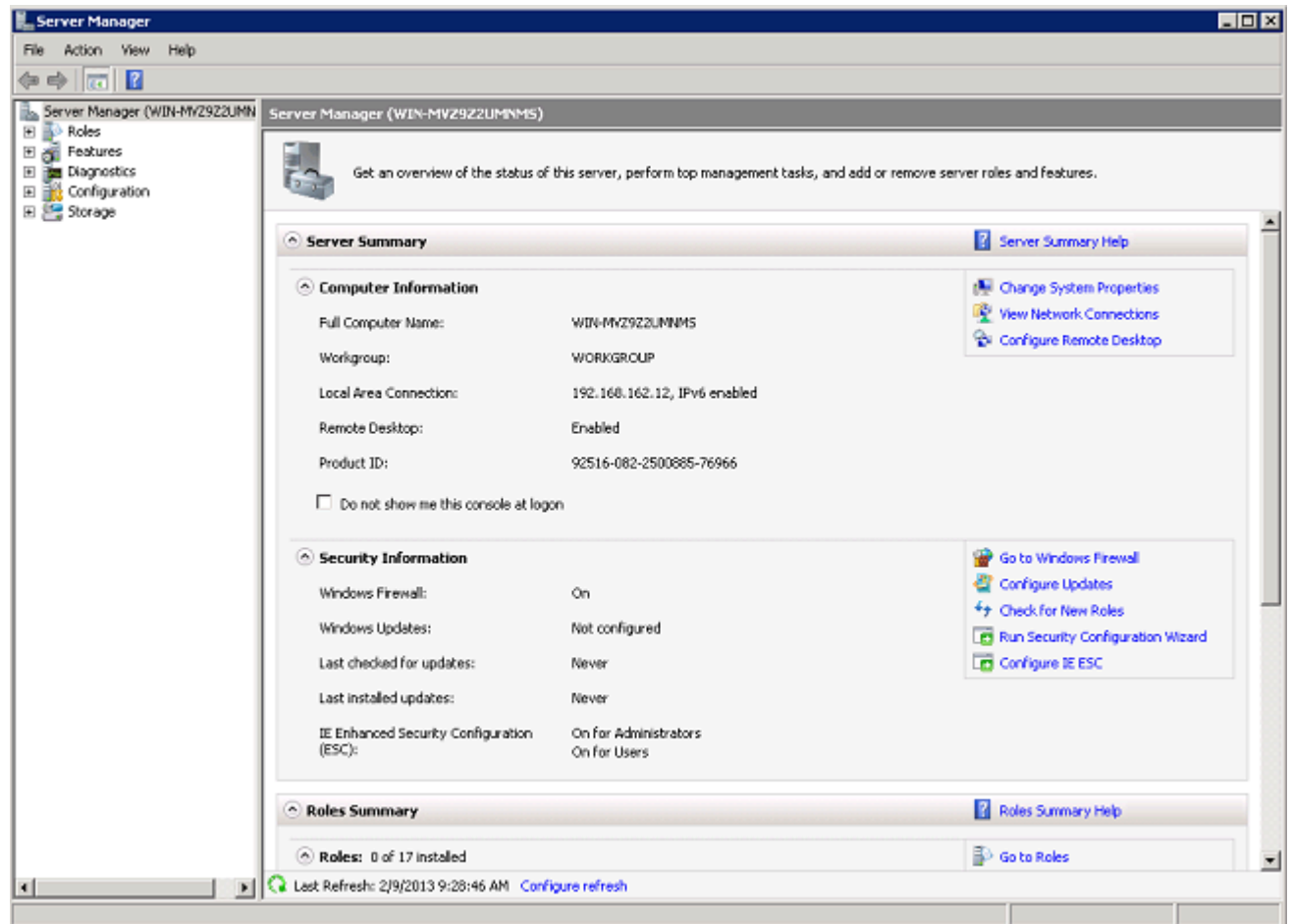
20. Starten Sie den Server neu, damit die Änderungen wirksam werden.



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

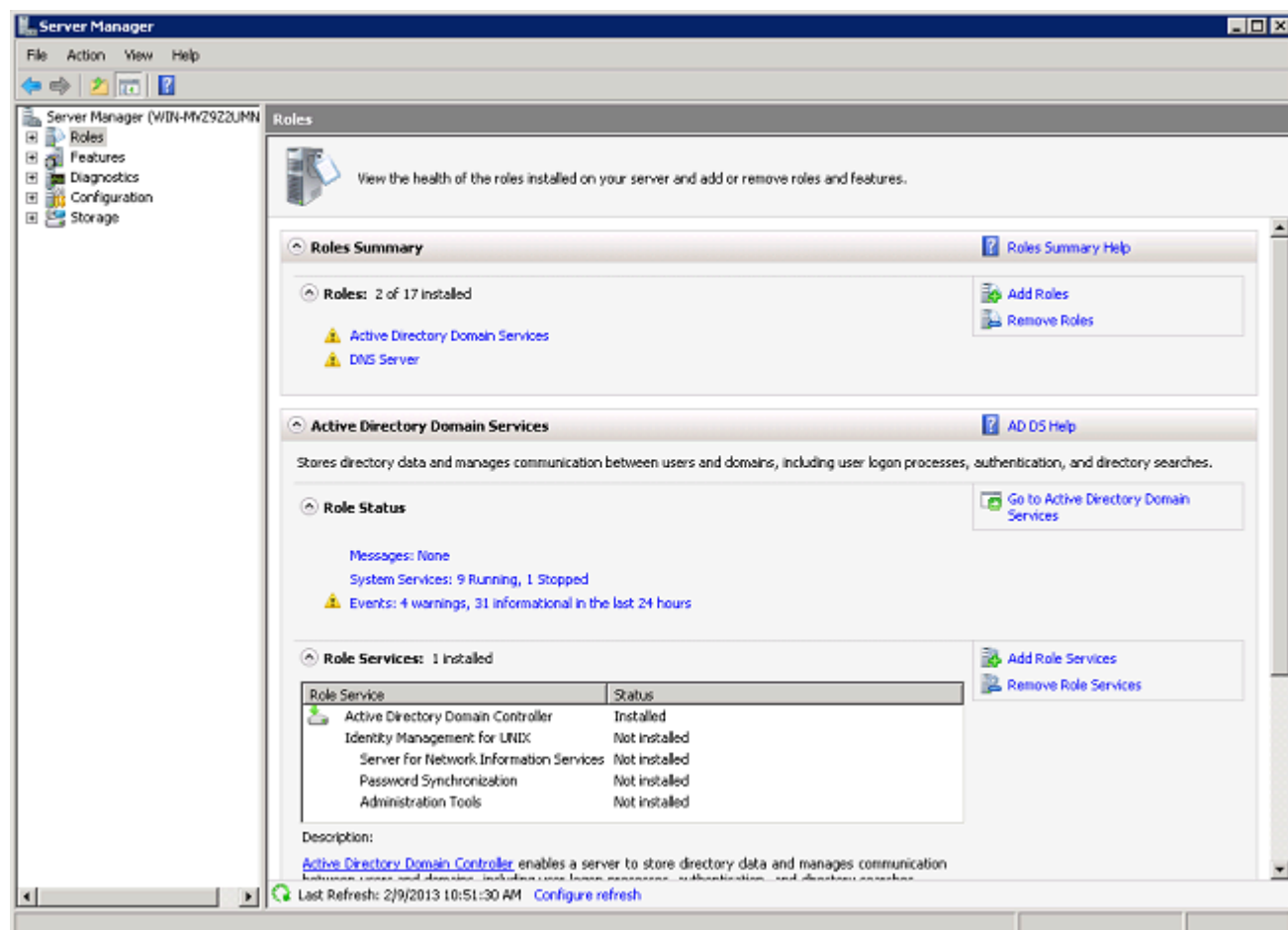
Der DHCP-Dienst auf dem Microsoft 2008-Server wird verwendet, um den Wireless-Clients IP-Adressen bereitzustellen. Gehen Sie wie folgt vor, um DHCP-Dienste zu installieren und zu konfigurieren:

1. Klicken Sie auf Start>Server Manager.




2. Klicken Sie auf Rollen > Rollen hinzufügen.





3. Klicken Sie auf Next (Weiter).

**Add Roles Wizard**

 **Before You Begin**

**Before You Begin**

Server Roles

Confirmation

Progress

Results

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

Before you continue, verify that:

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

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


To continue, click Next.

☐ Skip this page by default

< Previous   **Next >**   Install   Cancel

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

**Add Roles Wizard**

 **Select Server Roles**

**Before You Begin**

**Server Roles**

DHCP Server

Network Connection Bindings

IPv4 DNS Settings

IPv4 WINS Settings

DHCP Scopes

DHCPv6 Stateless Mode

IPv6 DNS Settings

DHCP Server Authorization

Confirmation

Progress

Results

Select one or more roles to install on this server.

Roles:

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

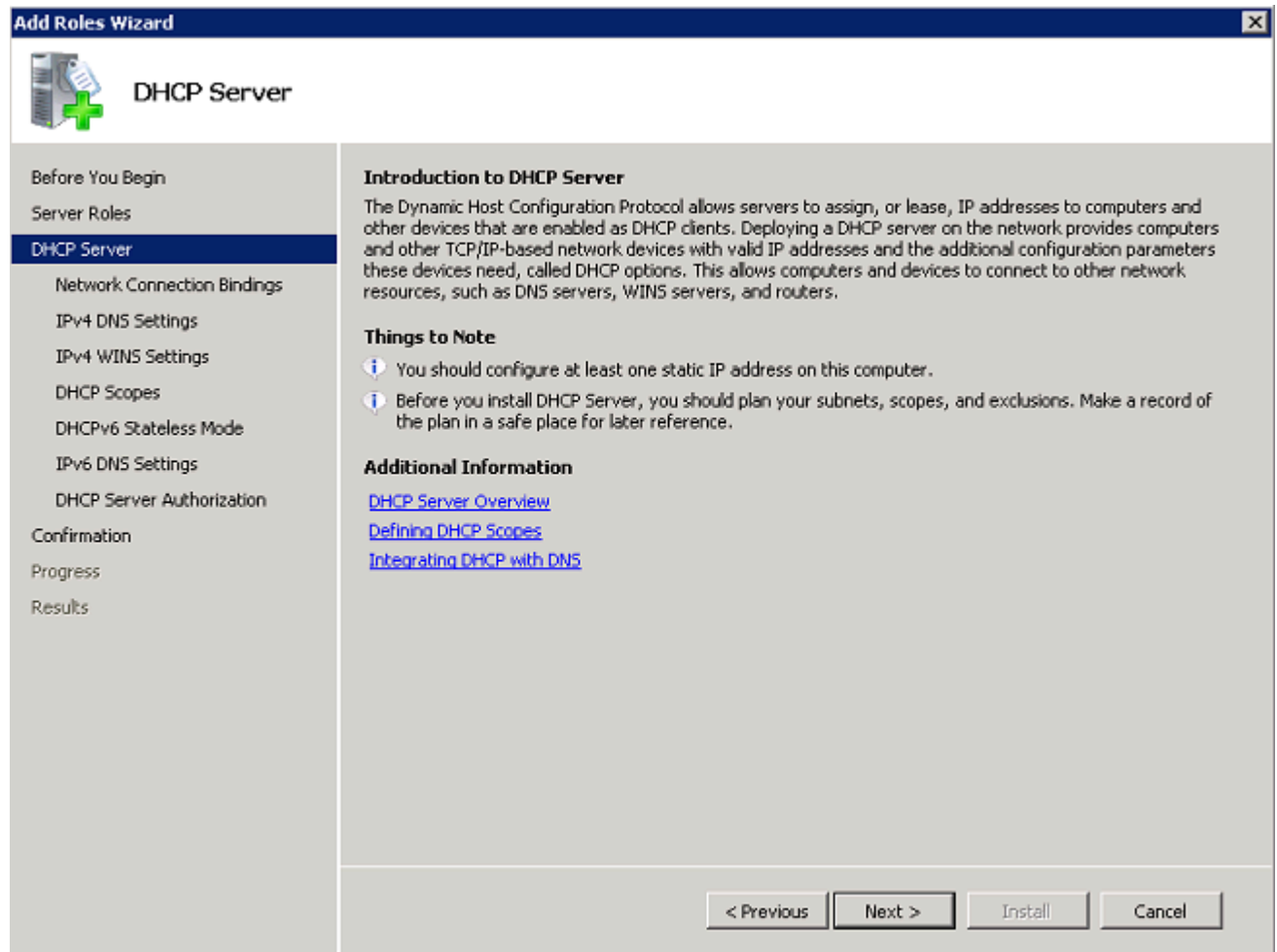
Description:

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

[More about server roles](#)


< Previous    Next >    Install    Cancel

5. 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.

Add Roles Wizard



## Select Network Connection Bindings

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

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

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

Network Connections:

IP Address	Type
<input checked="" type="checkbox"/> 192.168.162.12	IPv4

Details

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

< Previous


Next >

Install

Cancel

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

**Add Roles Wizard**

 **Specify IPv4 DNS Server Settings**

**Before You Begin**

Server Roles

DHCP Server

Network Connection Bindings

**IPv4 DNS Settings**

IPv4 WINS Settings

DHCP Scopes

DHCPv6 Stateless Mode

IPv6 DNS Settings

DHCP Server Authorization

Confirmation

Progress

Results

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

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

Parent Domain:

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

Preferred DNS Server IPv4 Address:


Alternate DNS Server IPv4 Address:

[More about DNS server settings](#)

< Previous   Next >   Install   Cancel

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

**Add Roles Wizard**

 **Specify IPv4 WINS Server Settings**

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

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

☒ WINS is not required for applications on this network

☐ WINS is required for applications on this network

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

Preferred WINS Server IP Address:


Alternate WINS Server IP Address:

[More about WINS server settings](#)

< Previous    Next >    Install    Cancel

9. 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.

**Add Roles Wizard**

 **Add or Edit DHCP Scopes**

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

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

Scopes:

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

**Add...**  
**Edit...**  
**Delete**

Properties  
Add or select a scope to view its properties.


[More about adding scopes](#)

< Previous    Next >    Install    Cancel

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



**Add Roles Wizard**

 **Configure DHCPv6 Stateless Mode**

**Before You Begin**

Server Roles

DHCP Server

Network Connection Bindings

IPv4 DNS Settings

IPv4 WINS Settings

DHCP Scopes

**DHCPv6 Stateless Mode**

IPv6 DNS Settings

DHCP Server Authorization

Confirmation

Progress

Results

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

Select the DHCPv6 stateless mode configuration for this server.

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


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

[More about DHCPv6 stateless mode](#)

< Previous   Next >   Install   Cancel

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

**Add Roles Wizard**

 **Specify IPv6 DNS Server Settings**

**Before You Begin**

Server Roles

DHCP Server

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

Confirmation

Progress

Results

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

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

Parent Domain:

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

Preferred DNS Server IPv6 Address:

Alternate DNS Server IPv6 Address:


[More about DNS server settings](#)

< Previous   Next >   Install   Cancel

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

**Add Roles Wizard**

## Authorize DHCP Server



**Before You Begin**

**Server Roles**

DHCP Server

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

**Confirmation**

Progress

Results

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

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

☒ Use current credentials

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


User Name:

☐ Use alternate credentials

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

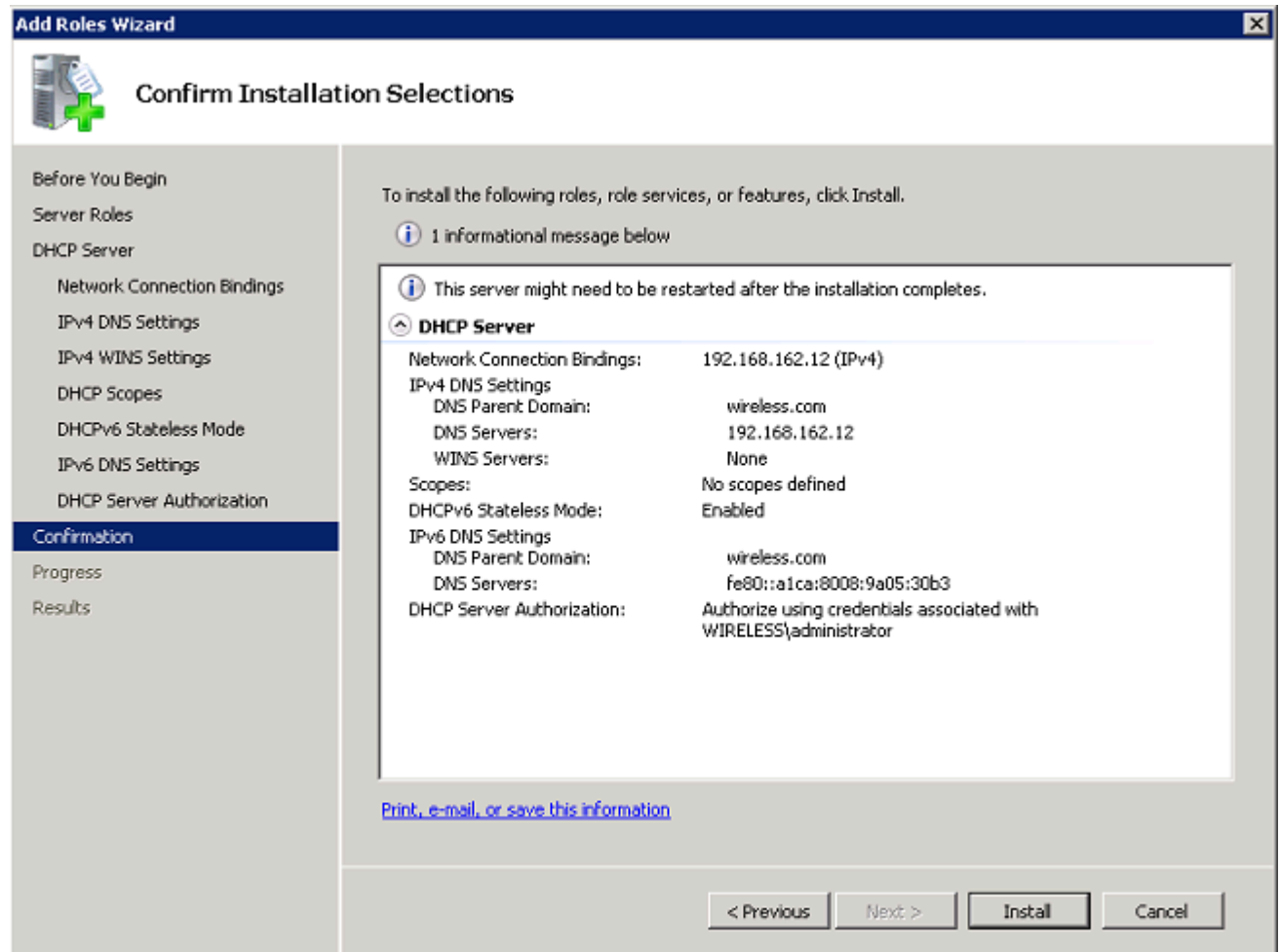
User Name:

☐ Skip authorization of this DHCP server in AD DS

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

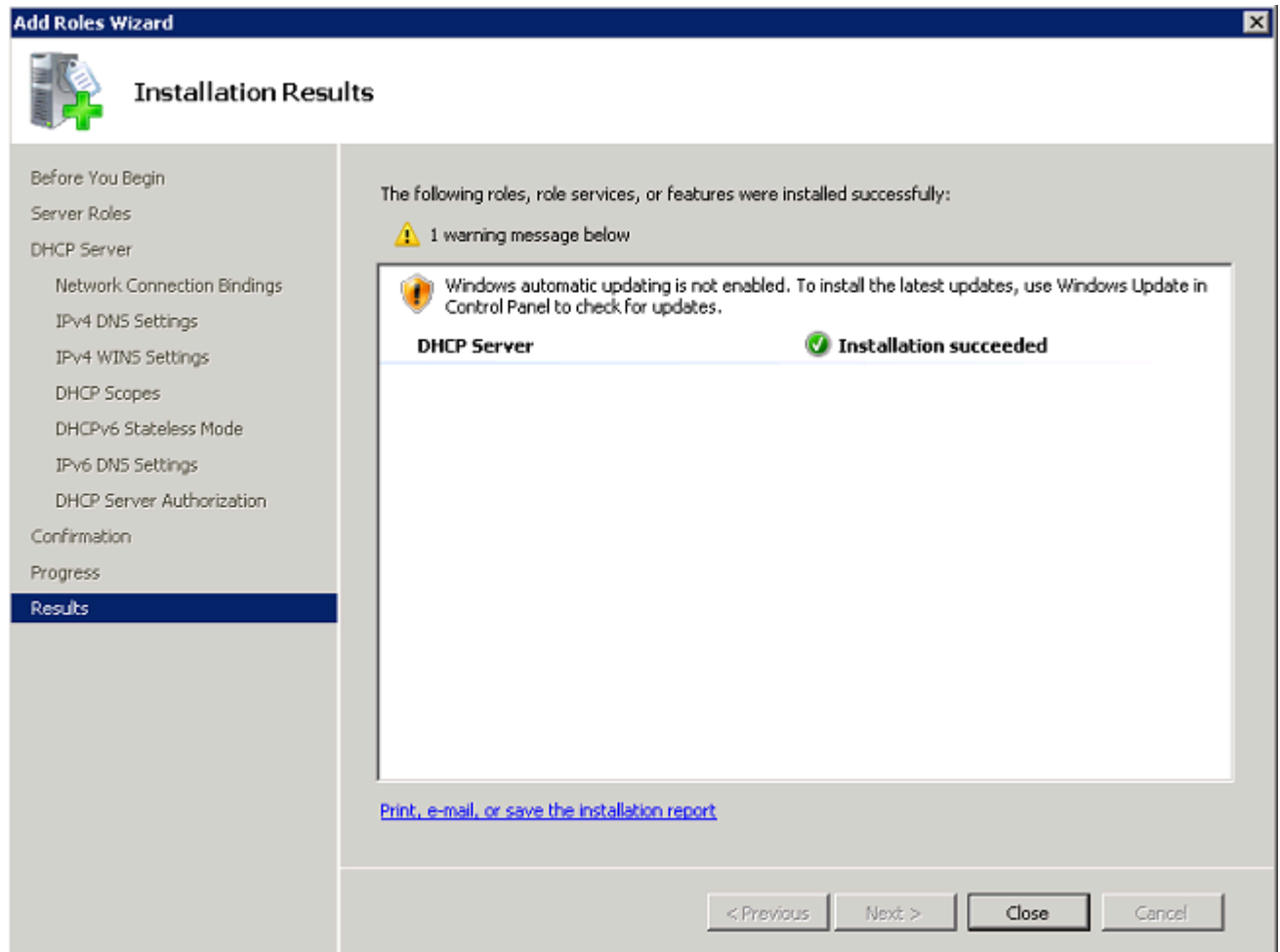
[More about authorizing DHCP servers in AD DS](#)

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



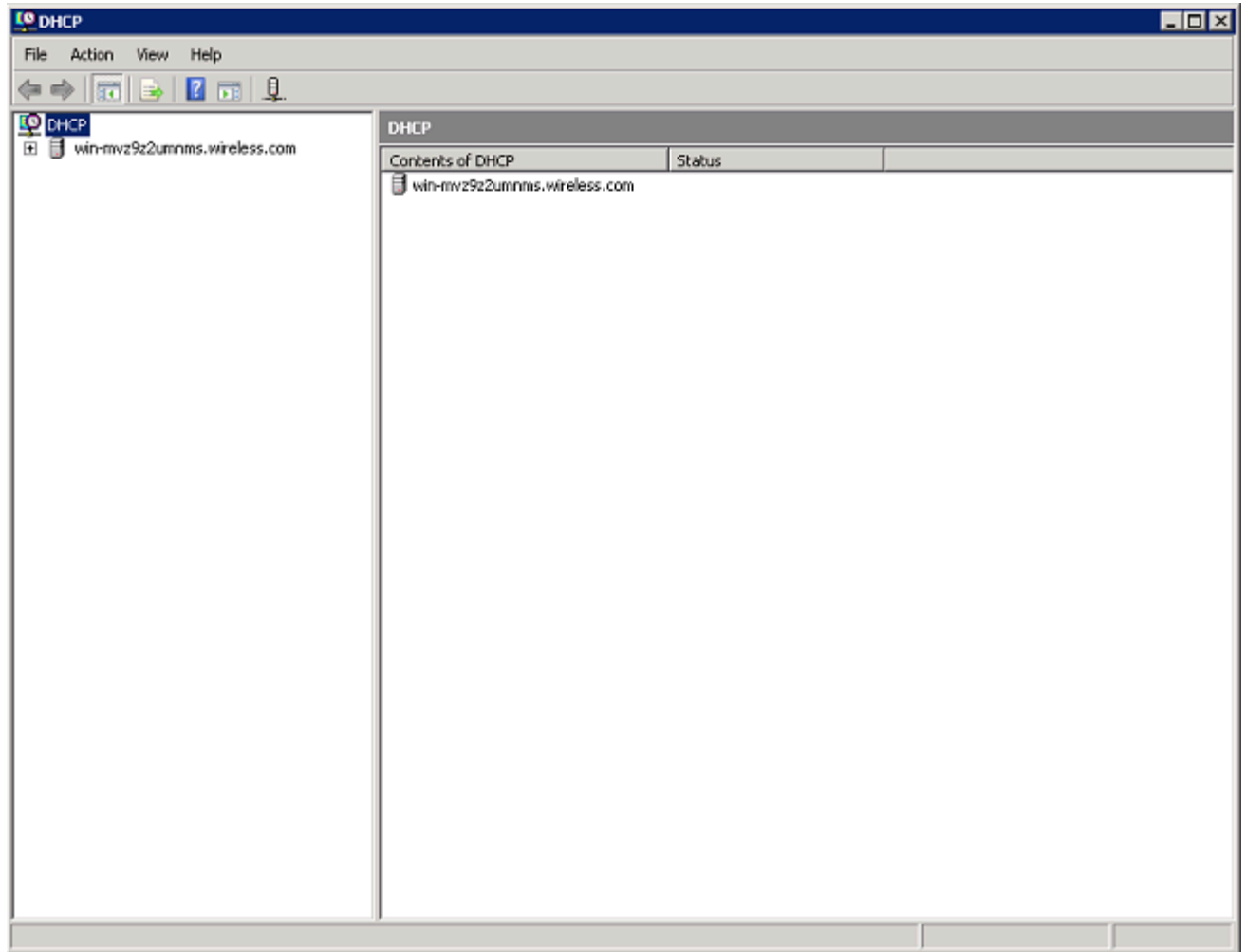
Die Installation wird fortgesetzt.

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

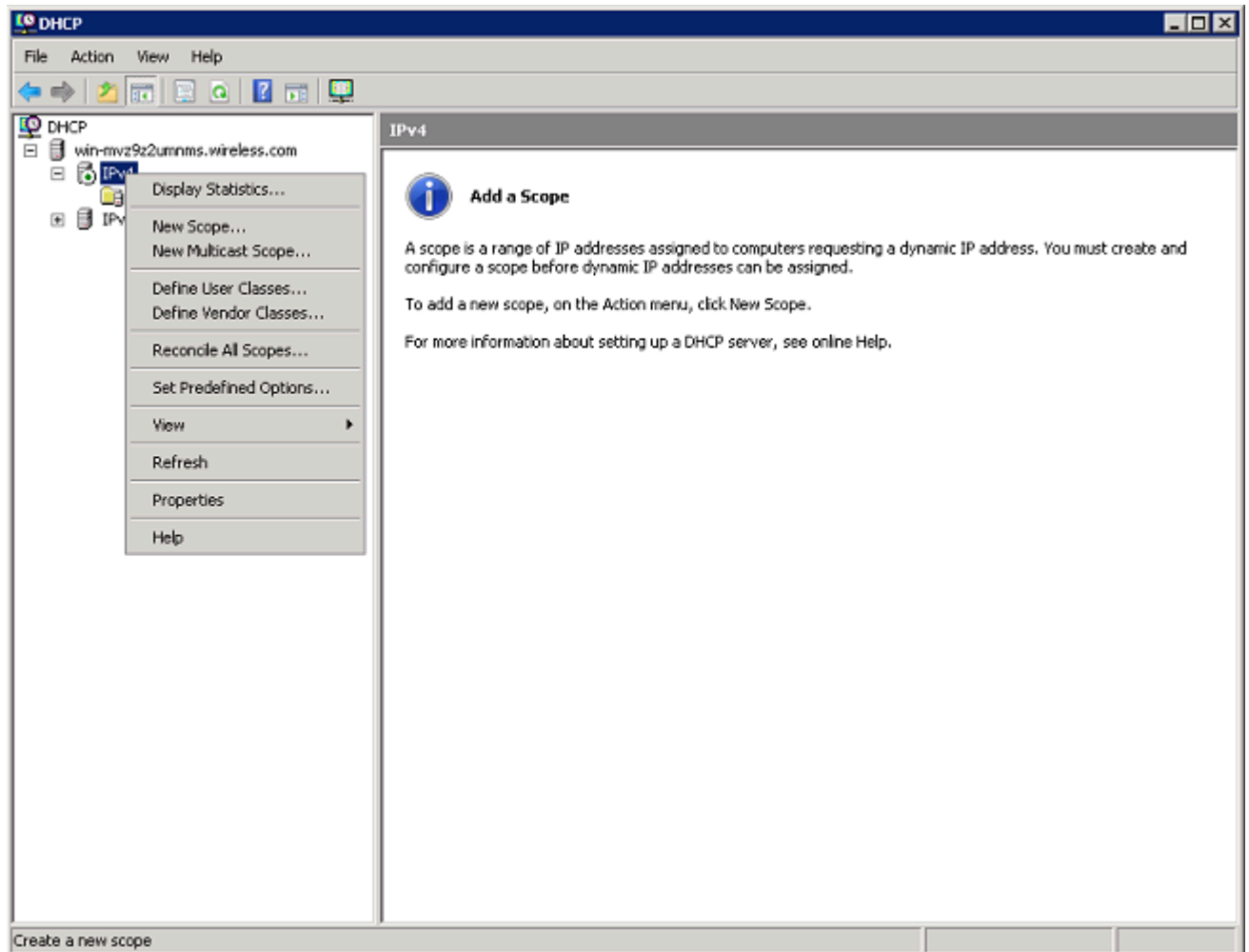


Der DHCP-Server ist nun installiert.

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



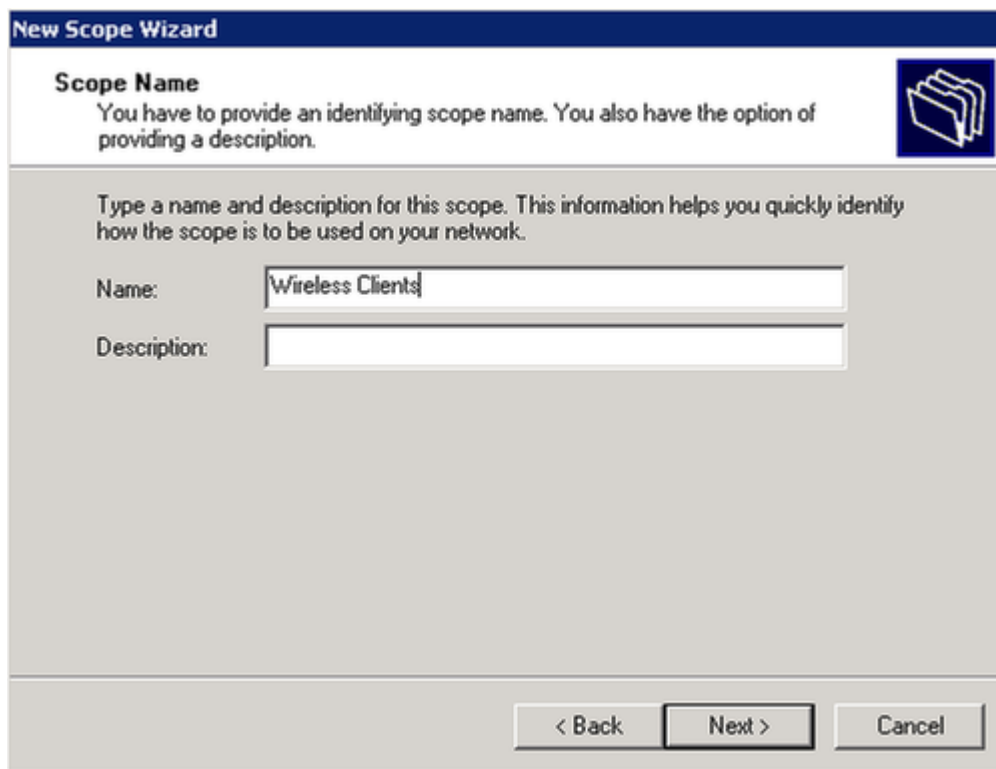
16. Erweitern Sie den DHCP-Server (im vorherigen Bild für dieses Beispiel dargestellt), klicken Sie mit der rechten Maustaste auf IPv4, und wählen Sie Neuer Bereich, um einen DHCP-Bereich zu erstellen.



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.

The image shows the 'New Scope Wizard' window at the 'Scope Name' step. The title bar is dark blue with the text 'New Scope Wizard' in white. The main area has a light gray background. At the top left, the text reads: 'Scope Name', 'You have to provide an identifying scope name. You also have the option of providing a description.' At the top right, there is a dark blue icon of a folder with three sub-folders. Below this, the text reads: 'Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.' There are two input fields: 'Name:' with the text 'Wireless Clients' and 'Description:' which is empty. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

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



**New Scope Wizard**

**IP Address Range**  
You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 162 . 100

End IP address: 192 . 168 . 162 . 200

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length: 24

Subnet mask: 255 . 255 . 255 . 0

< Back Next > Cancel

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

**New Scope Wizard**

**Add Exclusions**  
Exclusions are addresses or a range of addresses that are not distributed by the server.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

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

Excluded address range:

Remove

< Back Next > Cancel

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

**New Scope Wizard**

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

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

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

Limited to:

Days:  Hours:  Minutes:

< Back   Next >   Cancel

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

**New Scope Wizard**

**Configure DHCP Options**  
You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

☒ Yes, I want to configure these options now

☐ No, I will configure these options later

< Back   Next >   Cancel

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

**New Scope Wizard**

**Router (Default Gateway)**  
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

. . .	Add
192.168.162.2	Remove
	Up
	Down

< Back   Next >   Cancel

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

**New Scope Wizard**

**Domain Name and DNS Servers**  
The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

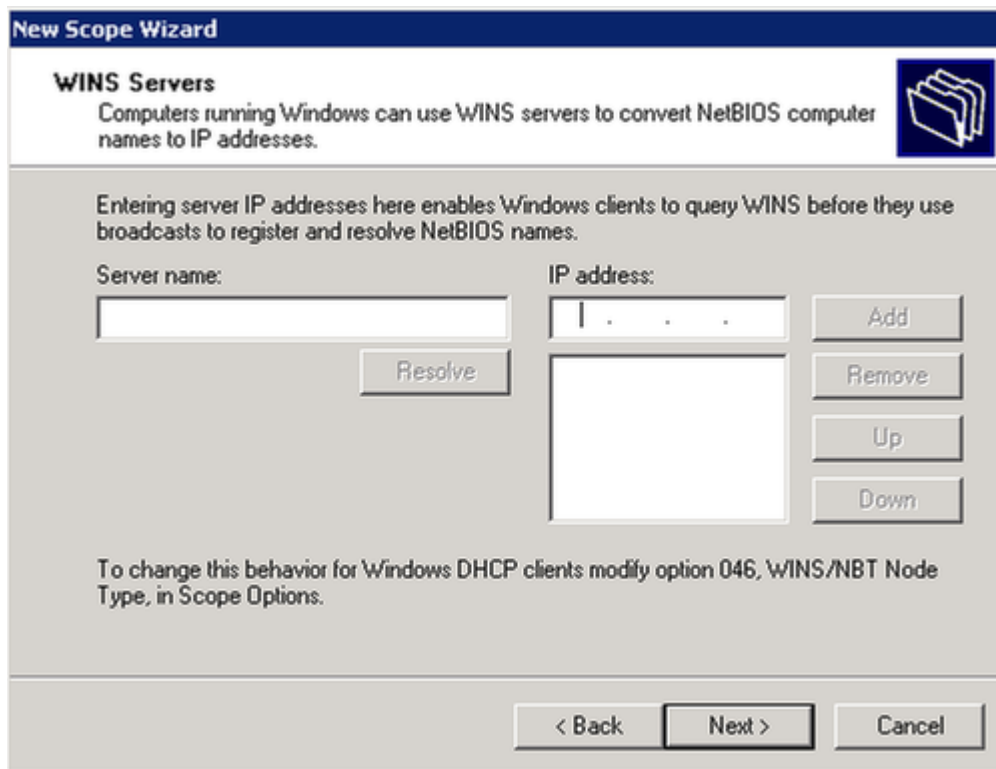
To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:	IP address:	Add
<input type="text"/>	. . .	Remove Up Down
Resolve	192.168.162.12	

< Back   Next >   Cancel

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

unterstützt. Klicken Sie auf Weiter, um fortzufahren.



**New Scope Wizard**

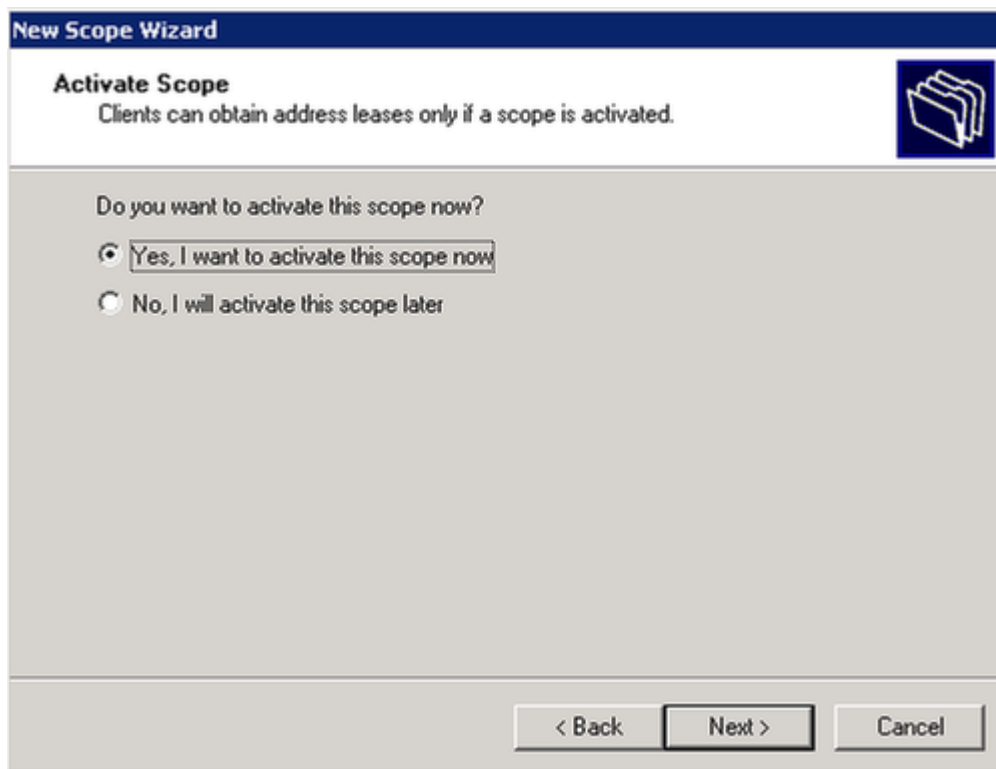
**WINS Servers**  
Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.

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

Server name:  IP address:

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

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



**New Scope Wizard**

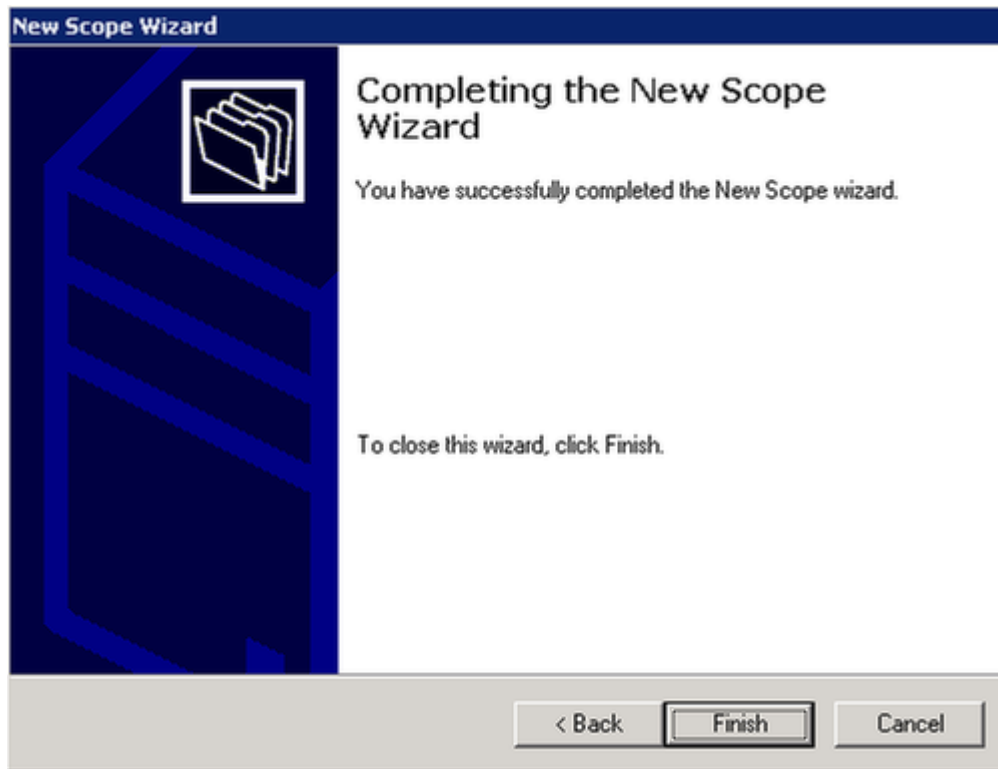
**Activate Scope**  
Clients can obtain address leases only if a scope is activated.

Do you want to activate this scope now?

☒ Yes, I want to activate this scope now

☐ No, I will activate this scope later

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

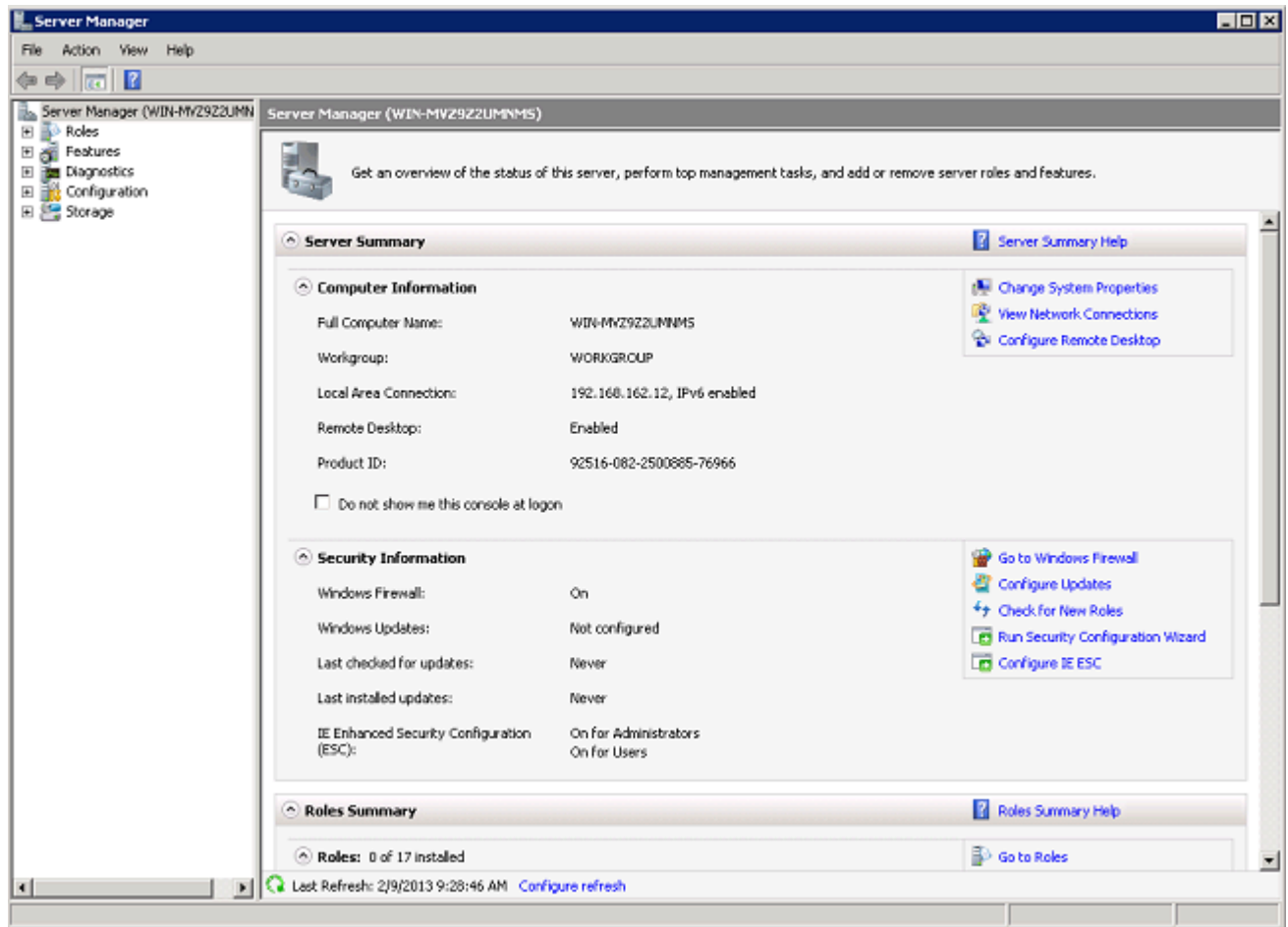


Installieren und Konfigurieren von Microsoft Windows 2008 Server als Zertifizierungsstellenserver

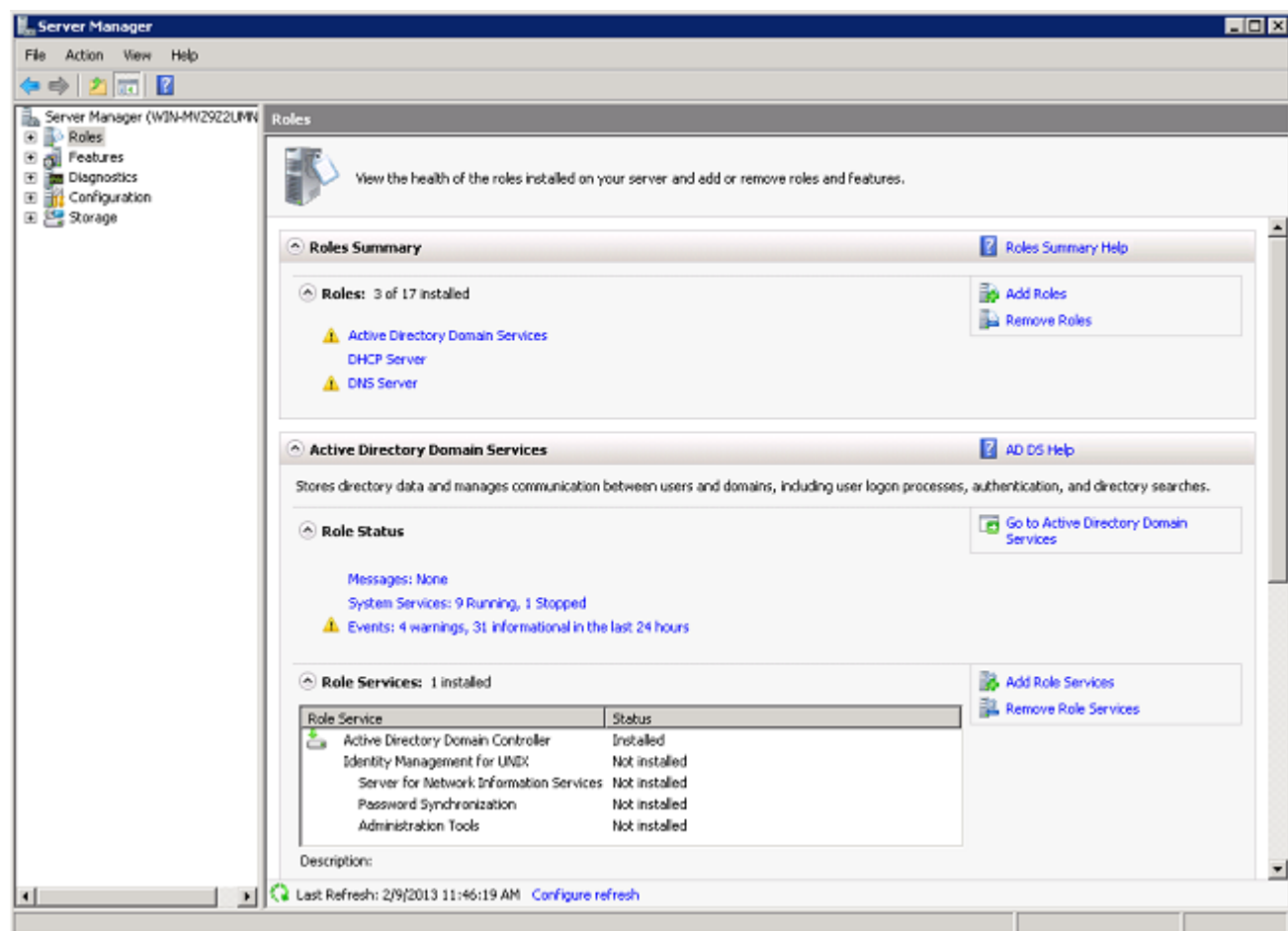
PEAP mit EAP-MS-CHAP v2 validiert den RADIUS-Server anhand des auf dem Server vorhandenen Zertifikats. Darüber hinaus muss das Serverzertifikat von einer öffentlichen Zertifizierungsstelle ausgestellt werden, die vom Clientcomputer als vertrauenswürdig eingestuft wird (d. h., das öffentliche Zertifizierungsstellenzertifikat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

**Add Roles Wizard**

 **Before You Begin**

**Before You Begin**

Server Roles

Confirmation

Progress

Results

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

Before you continue, verify that:

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

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

To continue, click Next.


☐ Skip this page by default

< Previous   **Next >**   Install   Cancel

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



**Add Roles Wizard**

 **Select Server Roles**

**Before You Begin**

**Server Roles**

AD CS  
Role Services  
Setup Type  
CA Type  
Private Key  
Cryptography  
CA Name  
Validity Period  
Certificate Database  
Confirmation  
Progress  
Results

Select one or more roles to install on this server.

Roles:

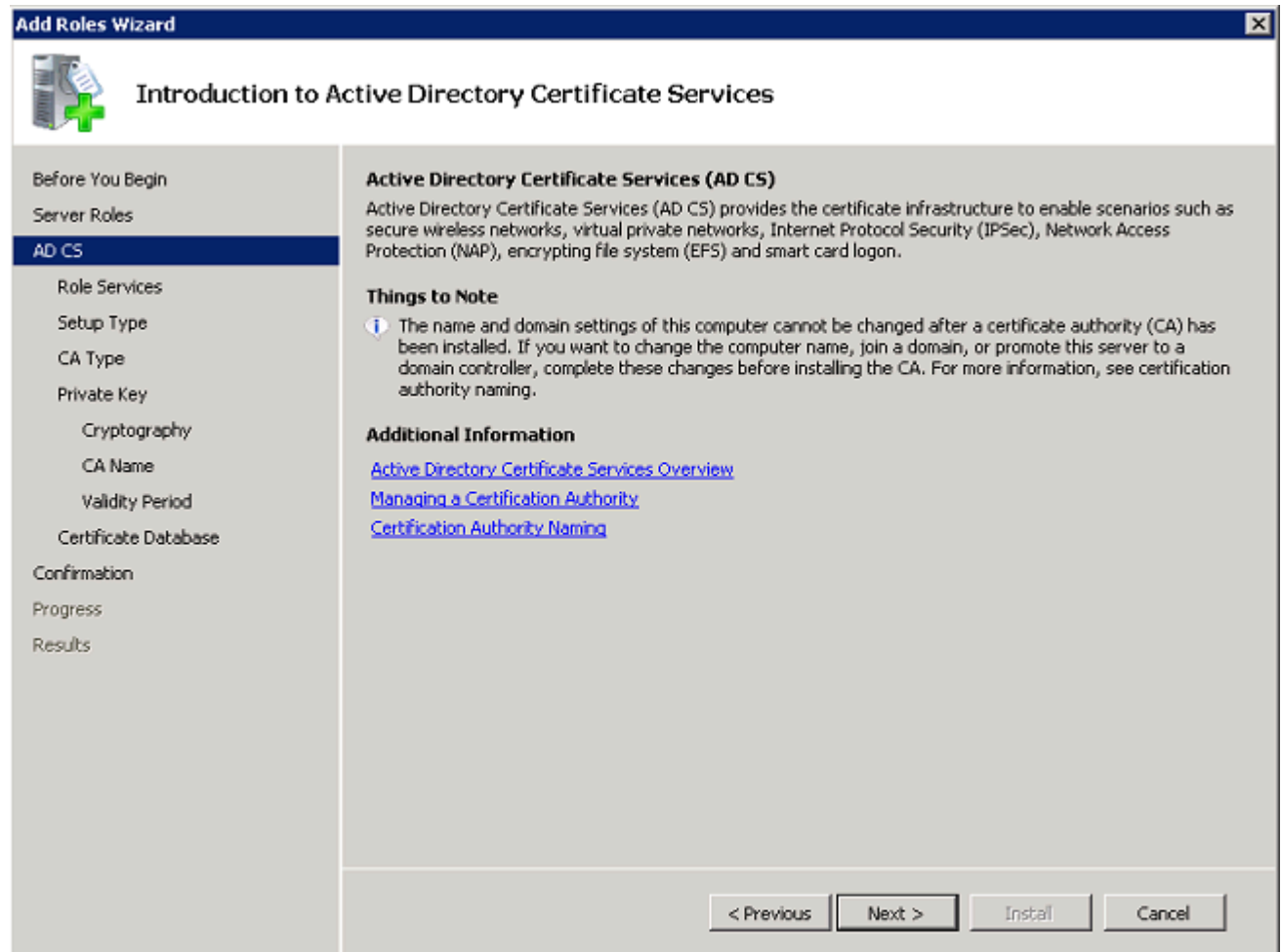
- ☒ **Active Directory Certificate Services**
- ☒ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☒ DHCP Server (Installed)
- ☒ DNS Server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

Description:  
[Active Directory Certificate Services \(AD CS\)](#) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

[More about server roles](#)


< Previous   Next >   Install   Cancel

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.

**Add Roles Wizard**

 **Select Role Services**

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

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

Role services:

<input checked="" type="checkbox"/>	Certification Authority
<input type="checkbox"/>	Certification Authority Web Enrollment
<input type="checkbox"/>	Online Responder
<input type="checkbox"/>	Network Device Enrollment Service


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

[More about role services](#)

< Previous    Next >    Install    Cancel

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

**Add Roles Wizard**

 **Specify Setup Type**

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

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

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


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

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

< Previous   Next >   Install   Cancel

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

**Add Roles Wizard**

 **Specify CA Type**

**Before You Begin**

Server Roles

AD CS

Role Services

Setup Type

**CA Type**

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

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

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


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

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

< Previous   Next >   Install   Cancel

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

**Add Roles Wizard**

 **Set Up Private Key**

**Before You Begin**

**Server Roles**

**AD CS**

Role Services

Setup Type

CA Type

**Private Key**

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

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

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

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

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


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

[More about public and private keys](#)

< Previous   Next >   Install   Cancel

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

**Add Roles Wizard**

 **Configure Cryptography for CA**

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

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

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

Key character length:  
2048

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


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

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

< Previous   Next >   Install   Cancel

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

**Add Roles Wizard**

 **Configure CA Name**

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

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

Common name for this CA:  
wireless-WIN-MVZ9Z2UMNMS-CA

Distinguished name suffix:  
DC=wireless,DC=com

Preview of distinguished name:  
CN=wireless-WIN-MVZ9Z2UMNMS-CA,DC=wireless,DC=com


[More about configuring a CA name](#)

< Previous    Next >    Install    Cancel

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



**Add Roles Wizard**

 **Set Validity Period**

**Before You Begin**

**Server Roles**

**AD CS**

- Role Services
- Setup Type
- CA Type
- Private Key
  - Cryptography
  - CA Name
- Validity Period**
- Certificate Database
- Confirmation
- Progress
- Results

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

Select validity period for the certificate generated for this CA:

**Years**

CA expiration Date: 2/9/2018 11:49 AM


Note that CA will issue certificates valid only until its expiration date.

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

< Previous   Next >   Install   Cancel

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

**Add Roles Wizard**

 **Configure Certificate Database**

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

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

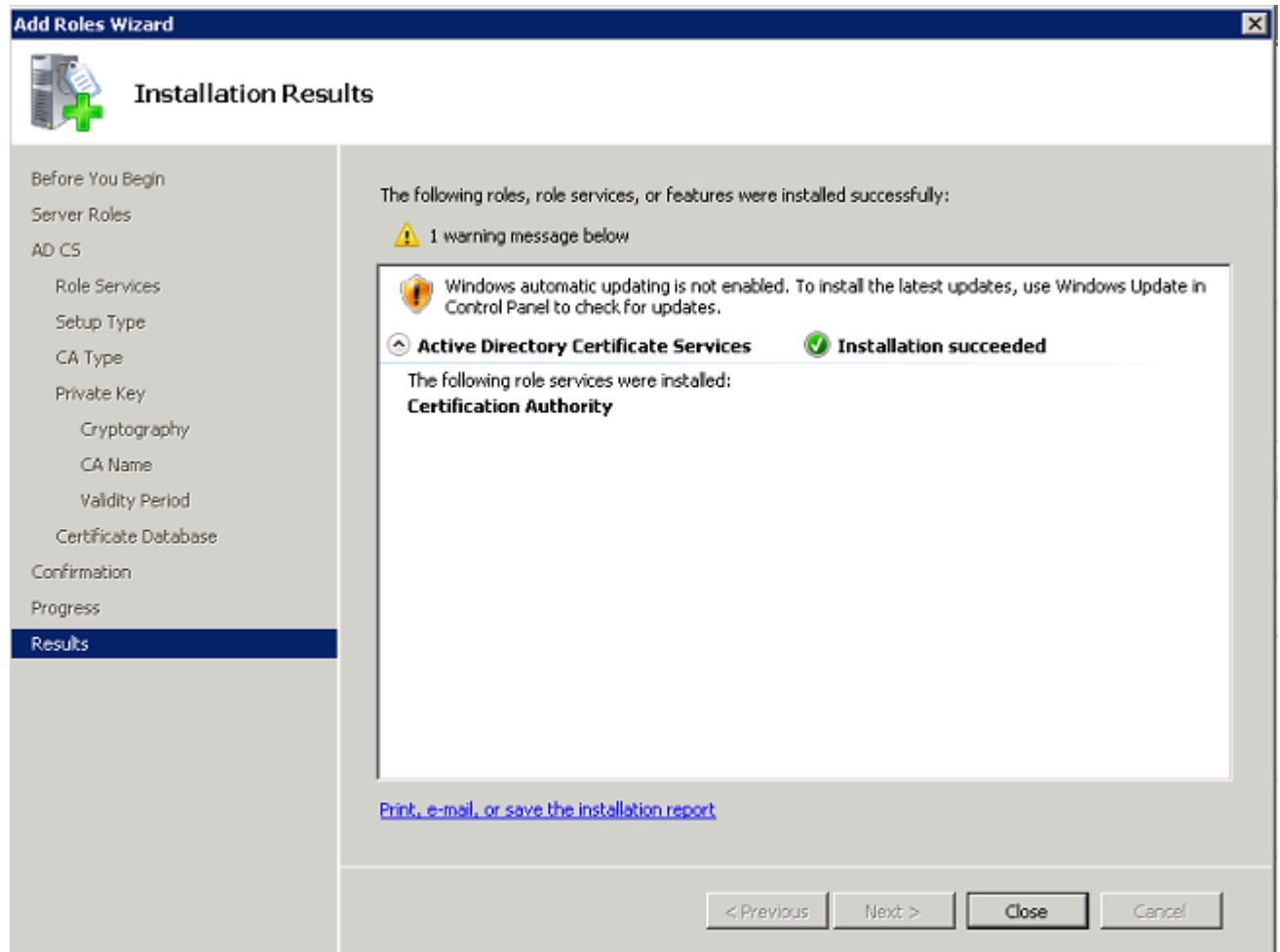
Certificate database location:

☐ Use existing certificate database from previous installation at this location

Certificate database log location:

< Previous    Next >    Install    Cancel

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

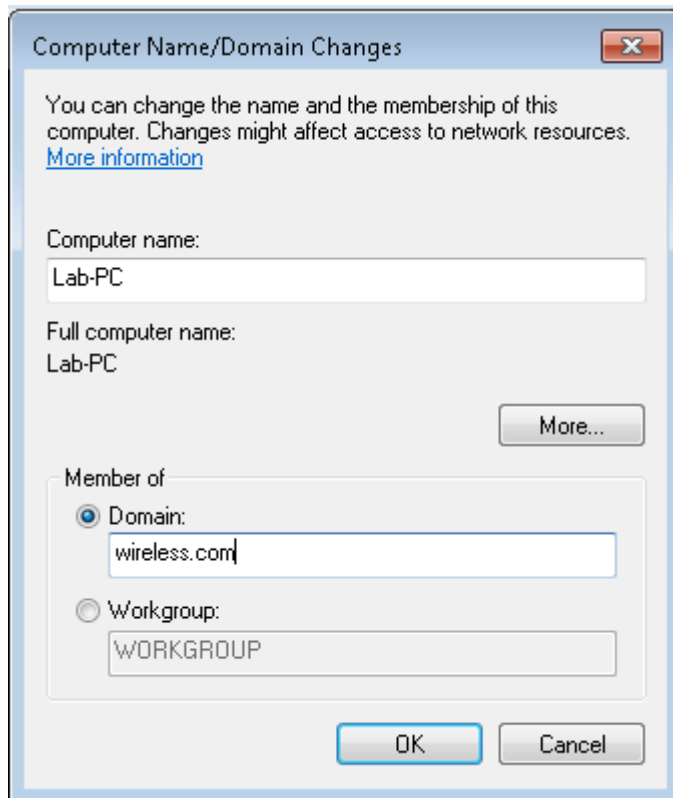


15. Klicken Sie nach Abschluss der Installation auf Schließen.

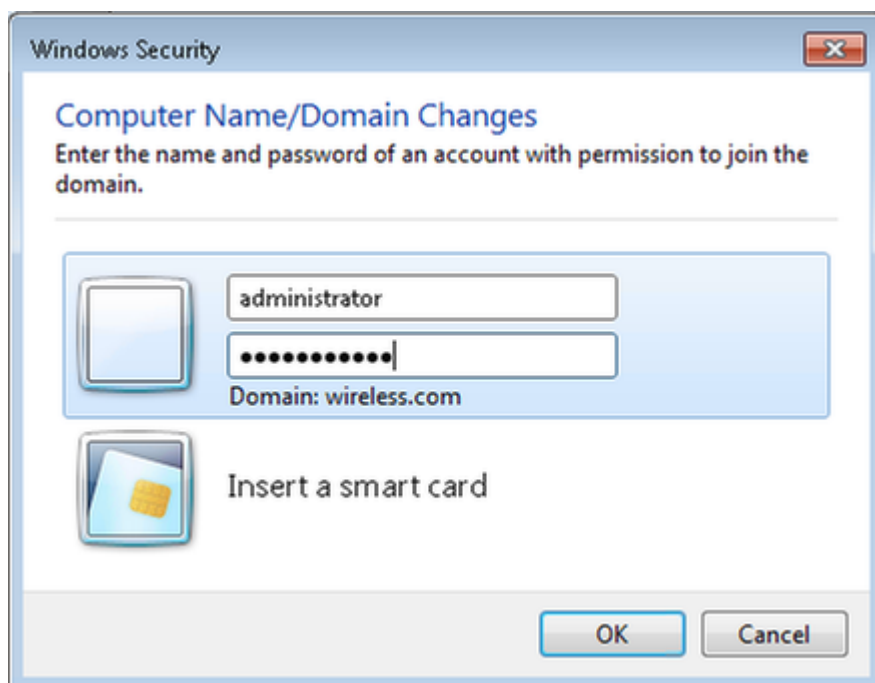
#### Clients mit der Domäne verbinden

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.



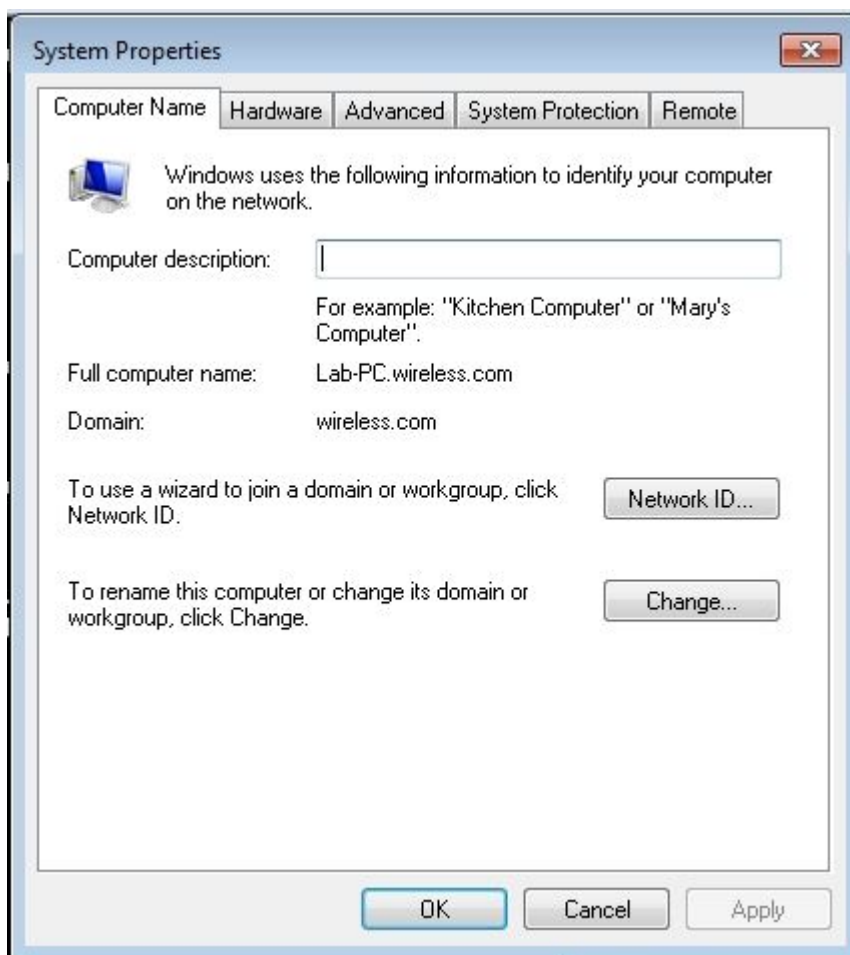
8. Geben Sie den Benutzernamen Administrator und das Kennwort für die Domäne ein, der der Client beitrifft. Dies ist das Administratorkonto im Active Directory auf dem Server.



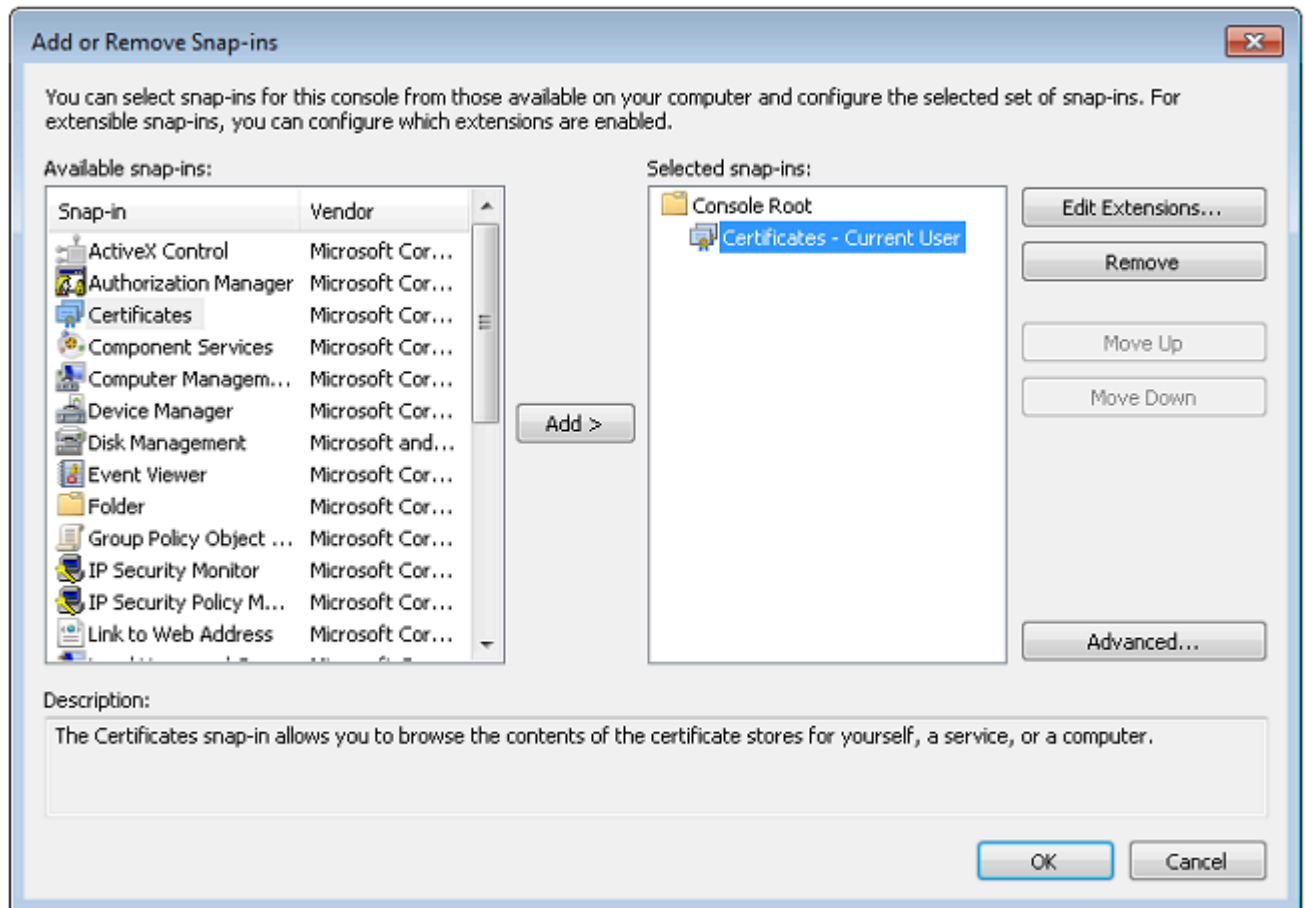
9. Klicken Sie auf OK, und klicken Sie erneut auf OK.



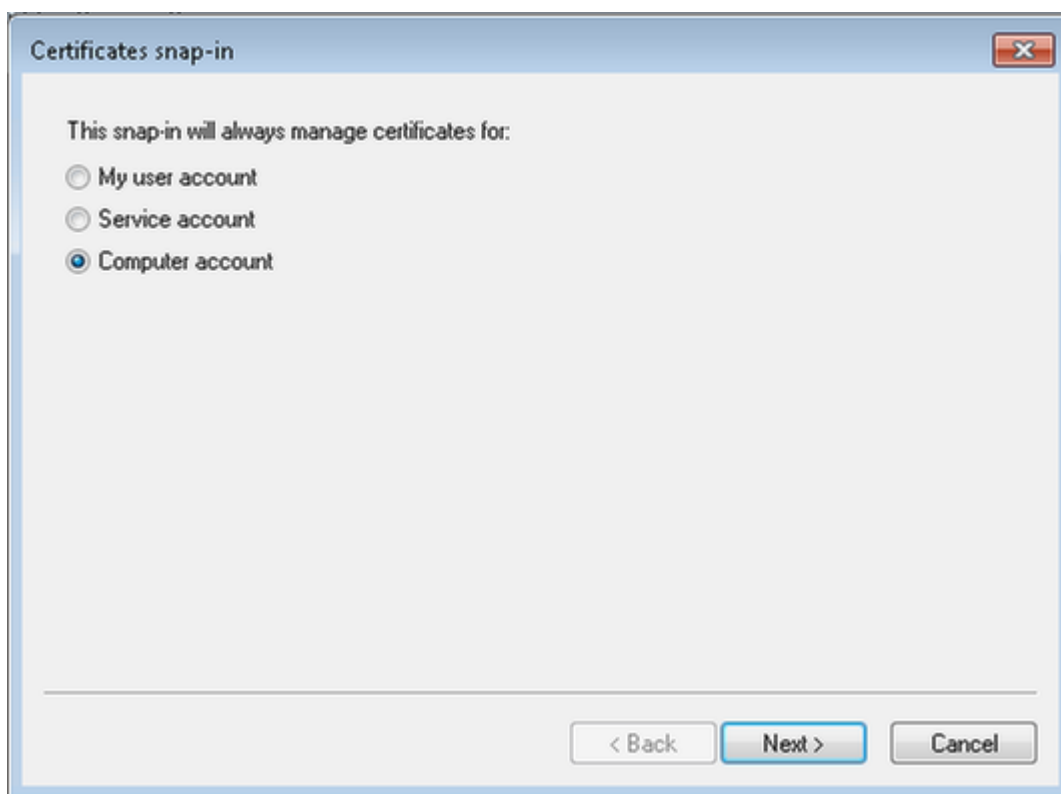
10. Klicken Sie auf Schließen>Jetzt neu starten, um den Computer neu zu starten.
11. Melden Sie sich nach dem Neustart des Computers mit folgenden Funktionen an:  
Benutzername = Administrator; Password = <Domänenkennwort>; Domäne = Wireless.
12. Klicken Sie auf Start, klicken Sie mit der rechten Maustaste 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.



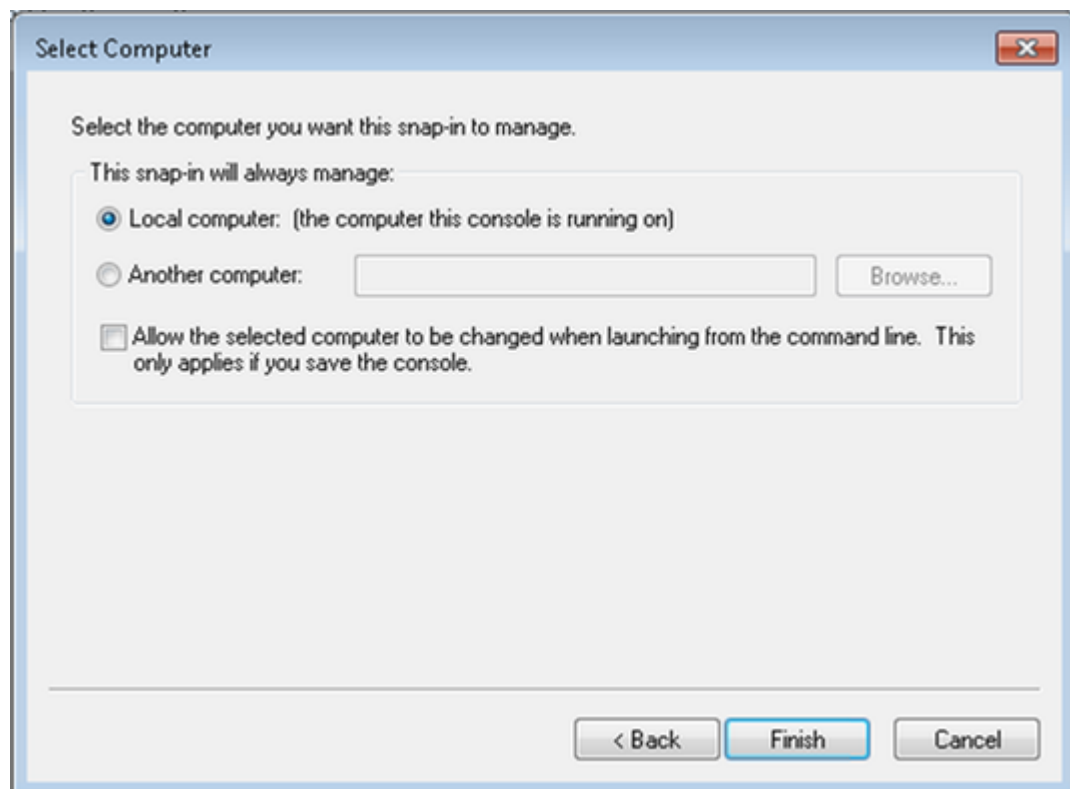
14. Klicken Sie auf Start, geben Sie mmc ein, und drücken Sie die Eingabetaste.
15. Klicken Sie auf Datei, und klicken Sie auf Snap-In hinzufügen/entfernen.
16. Wählen Sie Zertifikate aus, und klicken Sie auf Hinzufügen.



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

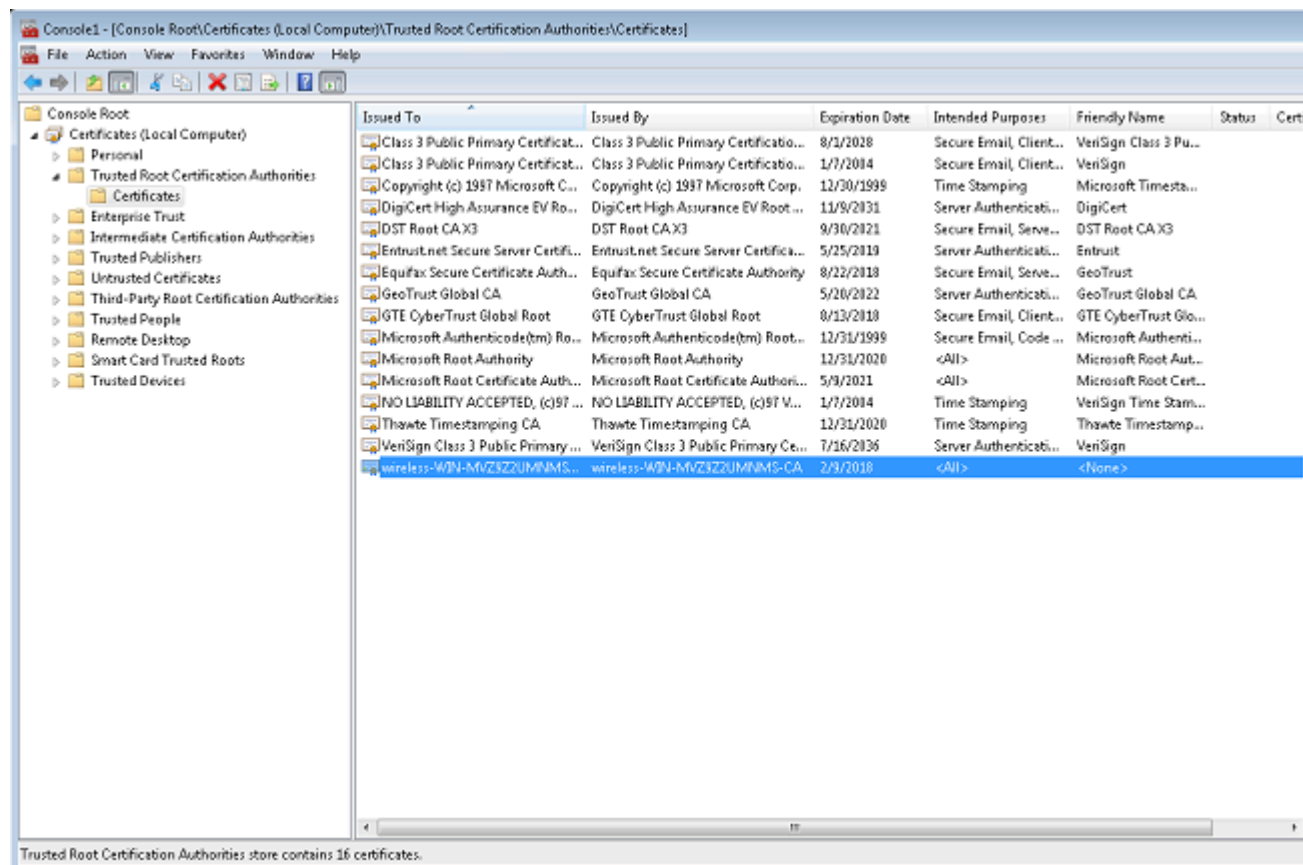


18. Klicken Sie auf Lokaler Computer, und klicken Sie auf Weiter.



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.

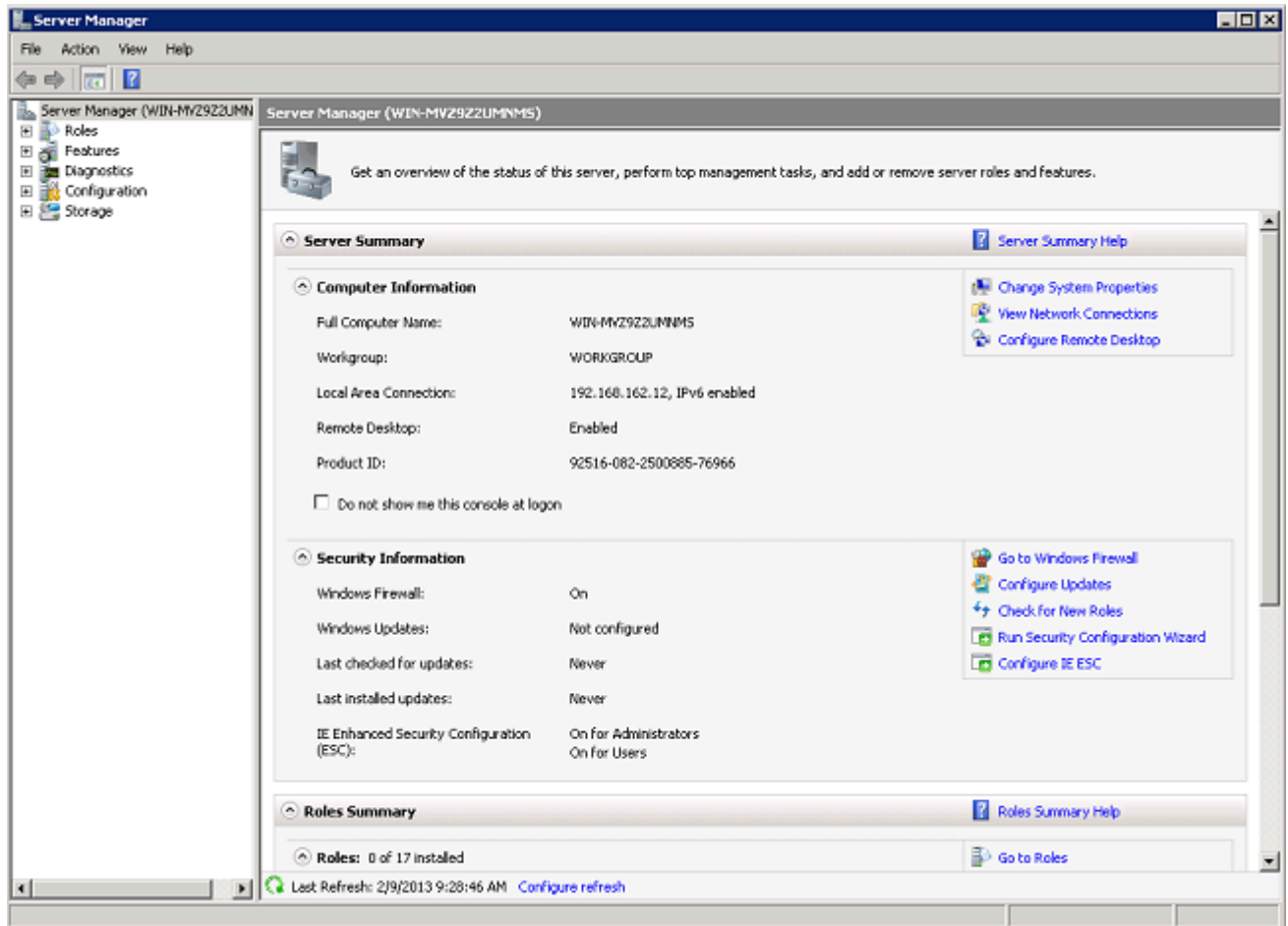


21. Wiederholen Sie dieses Verfahren, um der Domäne weitere Clients hinzuzufügen.

Installieren des Netzwerkrichtlinienservers auf dem Microsoft Windows 2008 Server

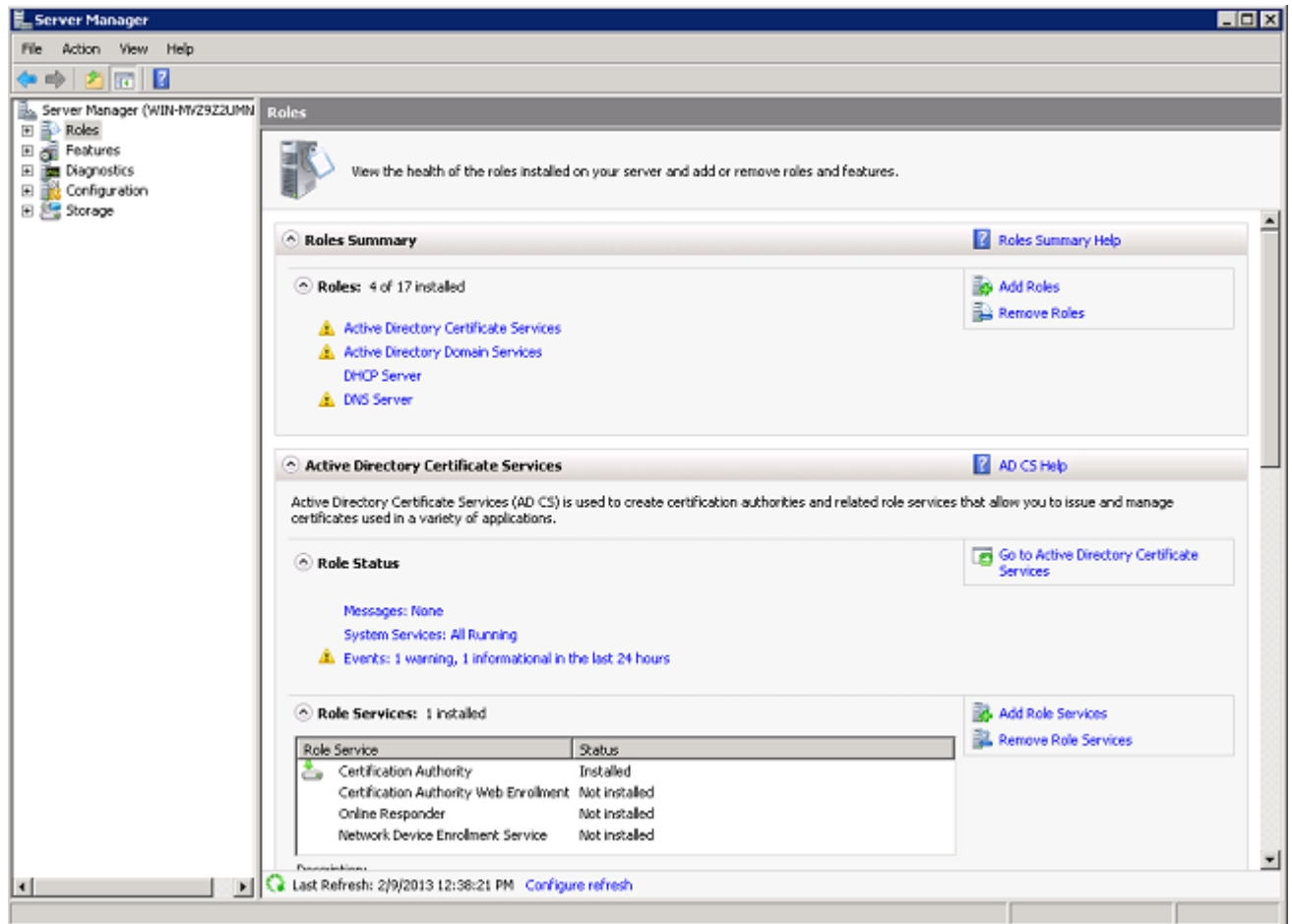
In dieser Konfiguration wird der NPS als RADIUS-Server verwendet, um Wireless-Clients mit PEAP-Authentifizierung zu authentifizieren. Führen Sie die folgenden Schritte aus, um NPS auf dem Microsoft Windows 2008-Server zu installieren und zu konfigurieren:

1. Klicken Sie auf Start> Server Manager.




2. Klicken Sie auf Rollen > Rollen hinzufügen.





3. Klicken Sie auf Next (Weiter).

**Add Roles Wizard**

 **Before You Begin**

**Before You Begin**

Server Roles

Confirmation

Progress

Results

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

Before you continue, verify that:

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

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


To continue, click Next.

☐ Skip this page by default

< Previous   **Next >**   Install   Cancel

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

**Add Roles Wizard**

 **Select Server Roles**

**Before You Begin**

**Server Roles**

Network Policy and Access Services

Role Services

Confirmation

Progress

Results

Select one or more roles to install on this server.

Roles:

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

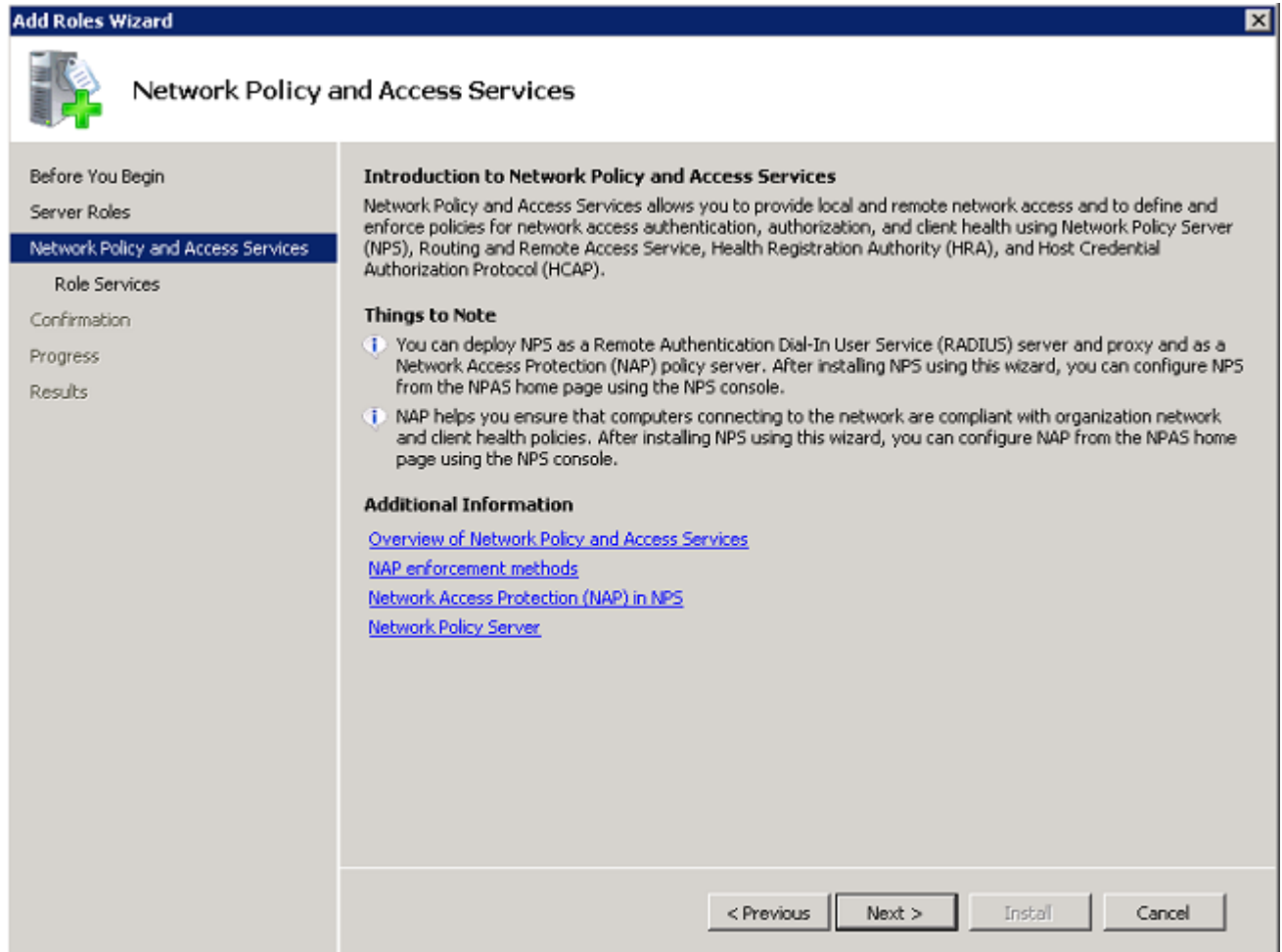
Description:

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

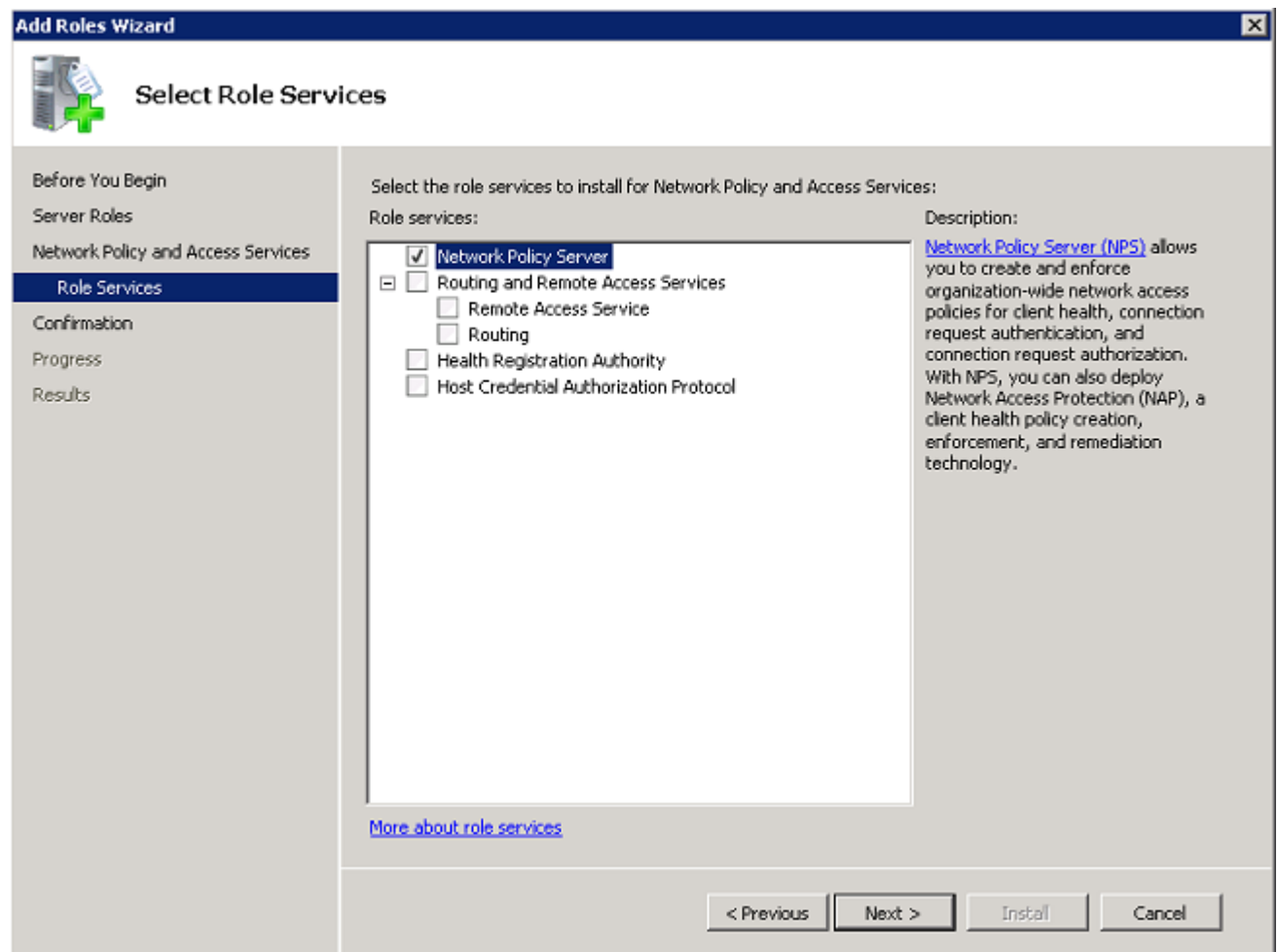
[More about server roles](#)

< Previous   Next >   Install   Cancel

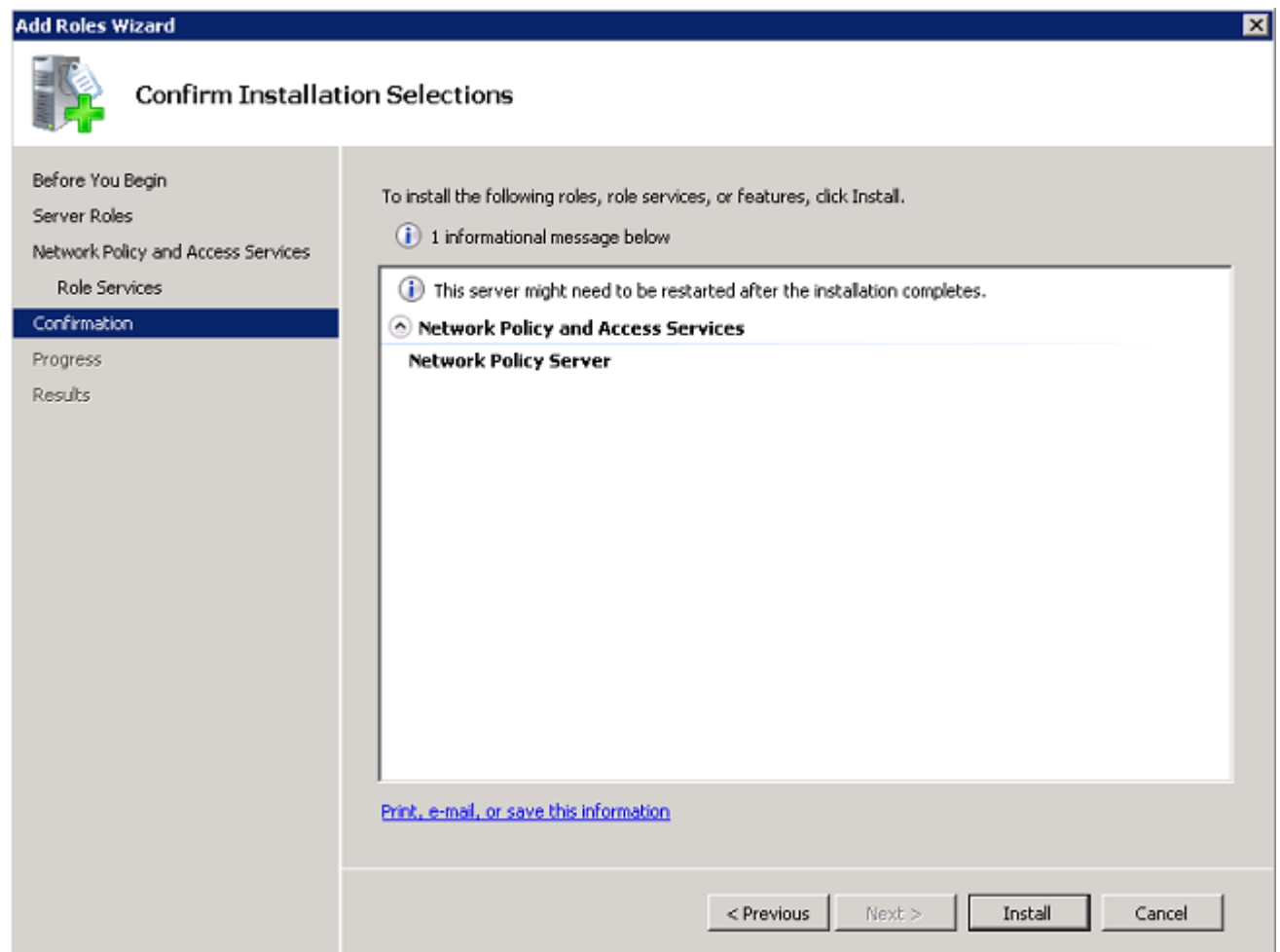
5. Lesen Sie die Einführung in Netzwerkrichtlinien und Zugriffsservices, und klicken Sie auf Weiter.



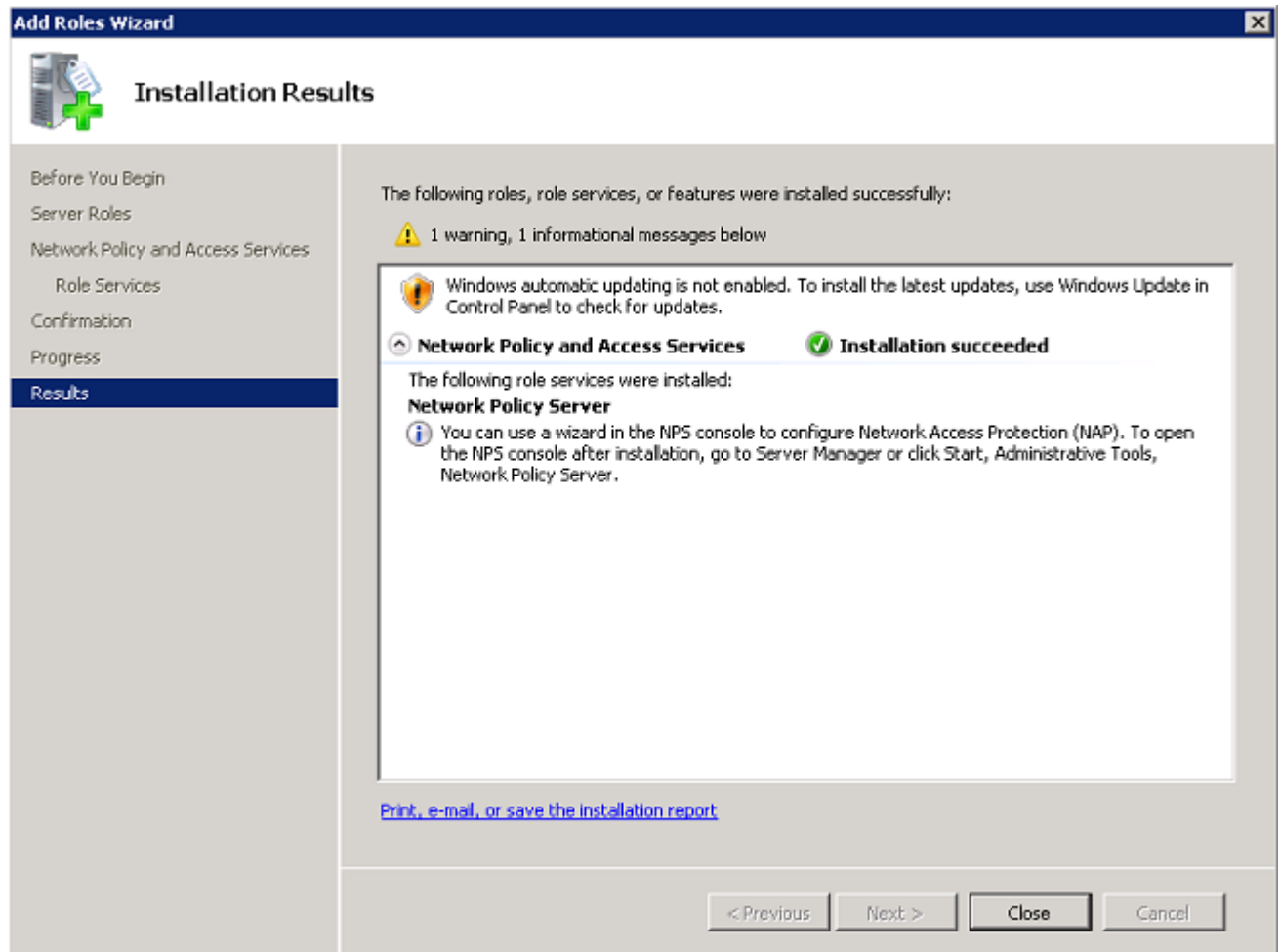
6. Wählen Sie Netzwerkrichtlinienserver aus, und klicken Sie auf Weiter.



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



Nach Abschluss der Installation wird ein ähnlicher Bildschirm angezeigt.

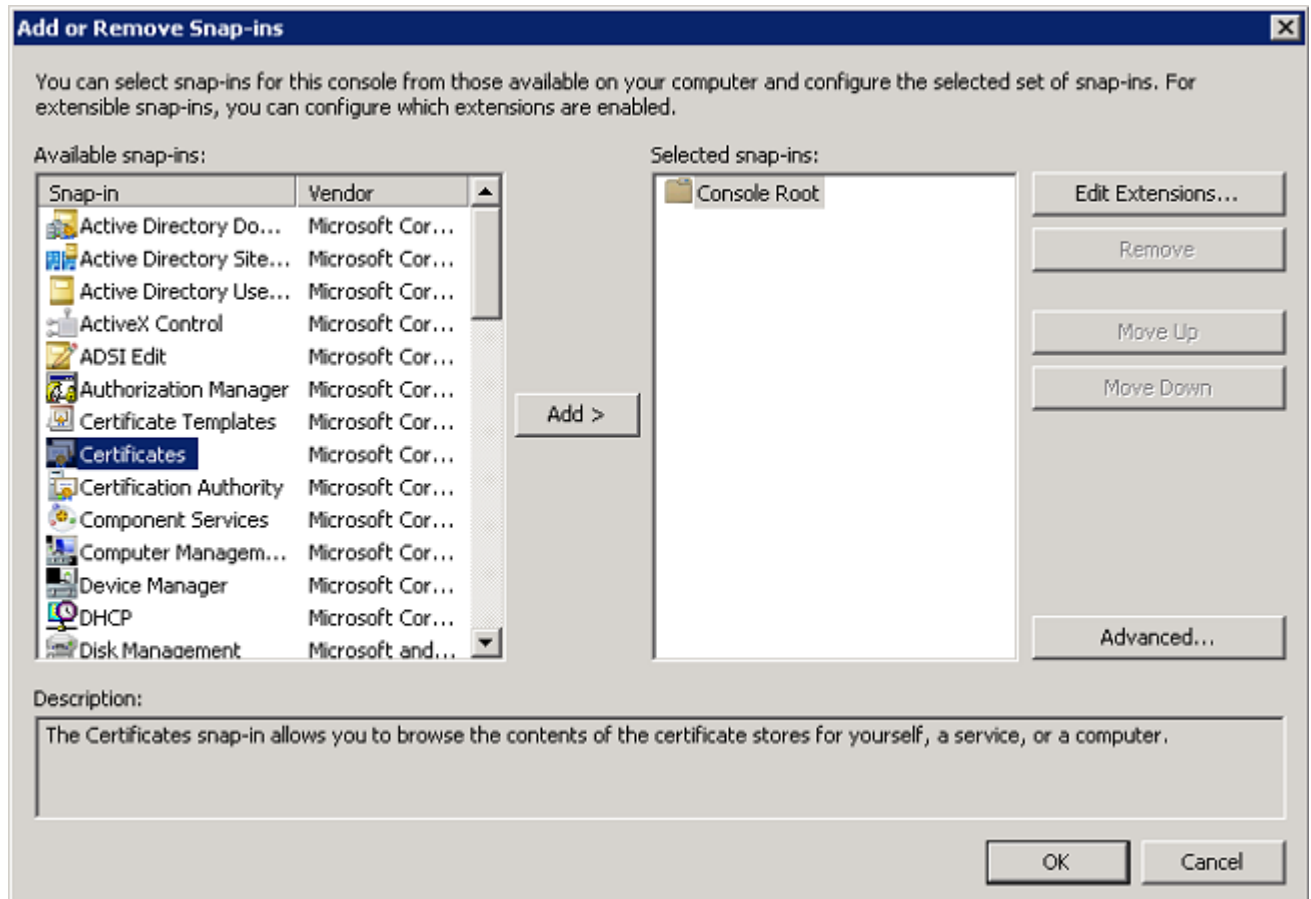


8. Klicken Sie auf Close (Schließen).

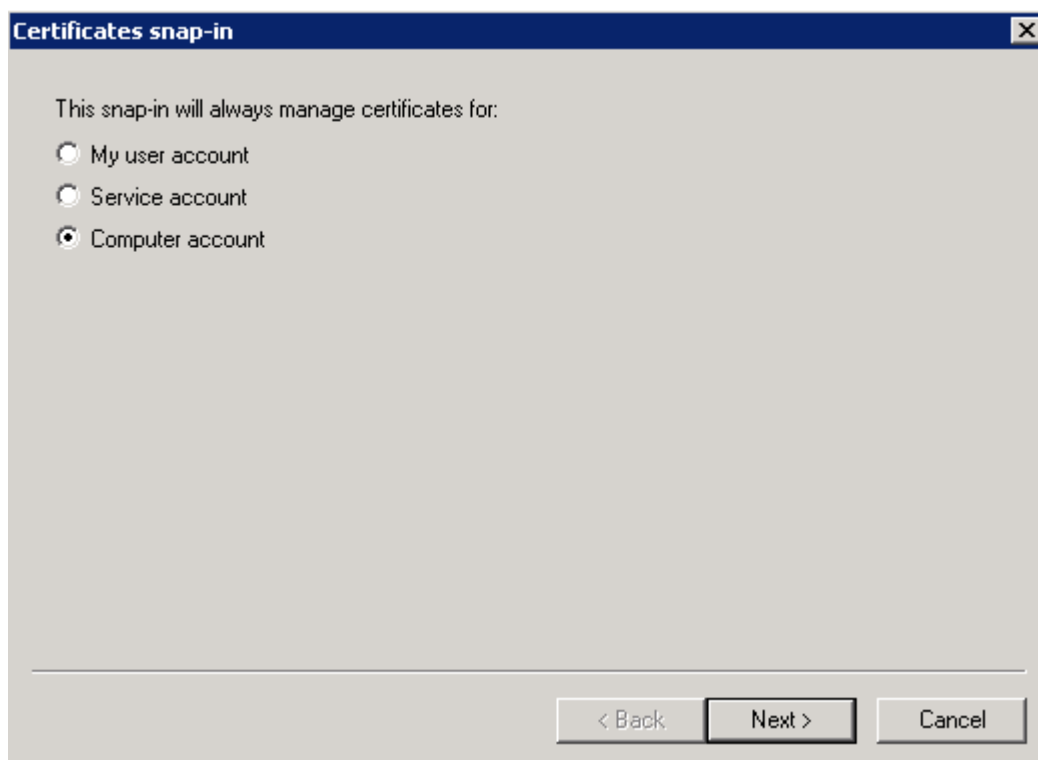
## Installieren eines Zertifikats

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.

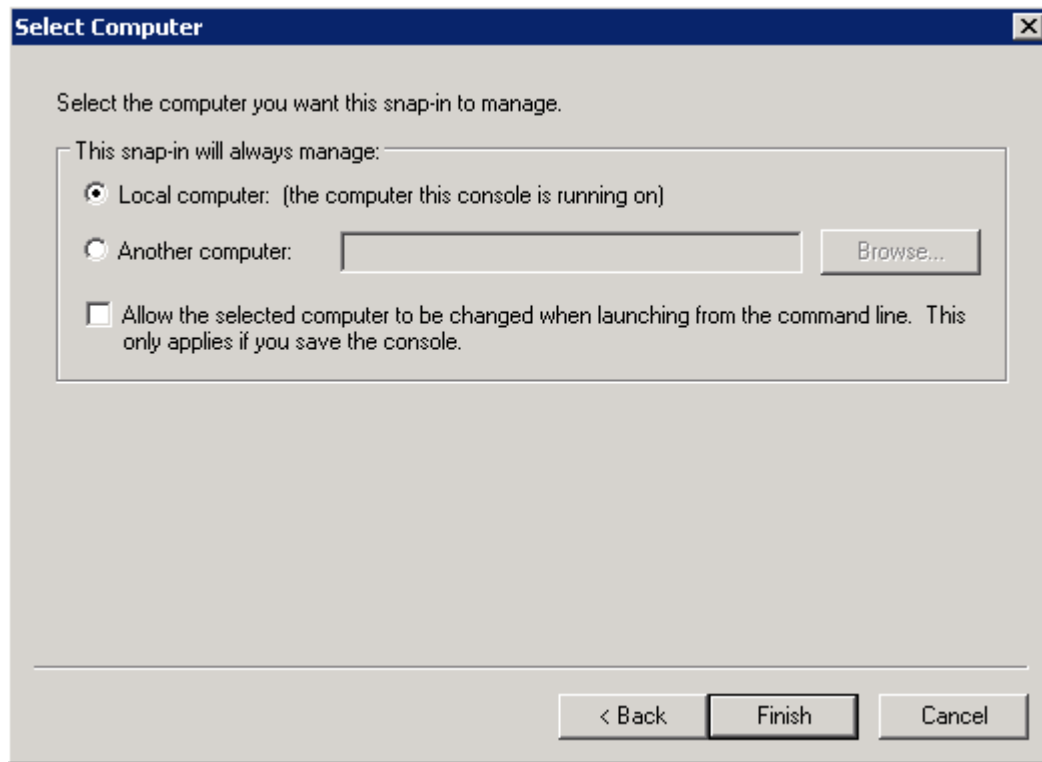


4. Wählen Sie Computerkonto aus, und klicken Sie auf Weiter.

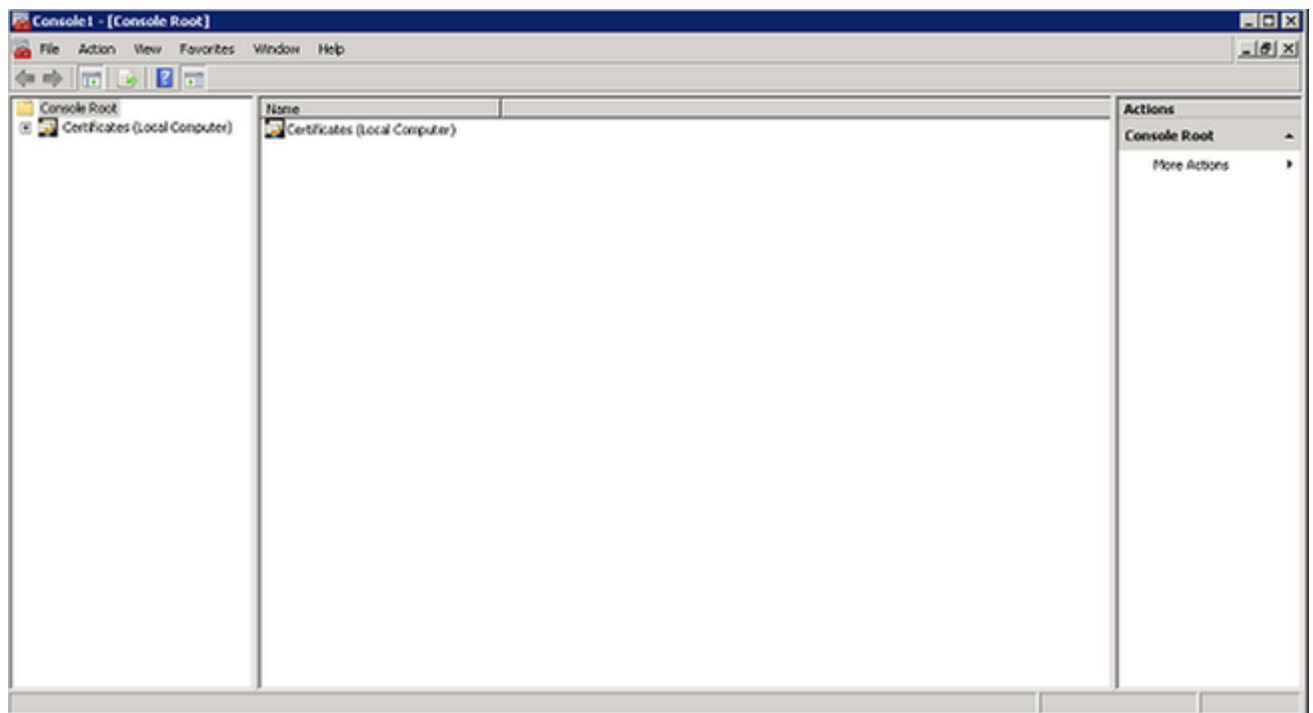


5. Wählen Sie Lokaler Computer aus, und klicken Sie auf Fertig stellen.

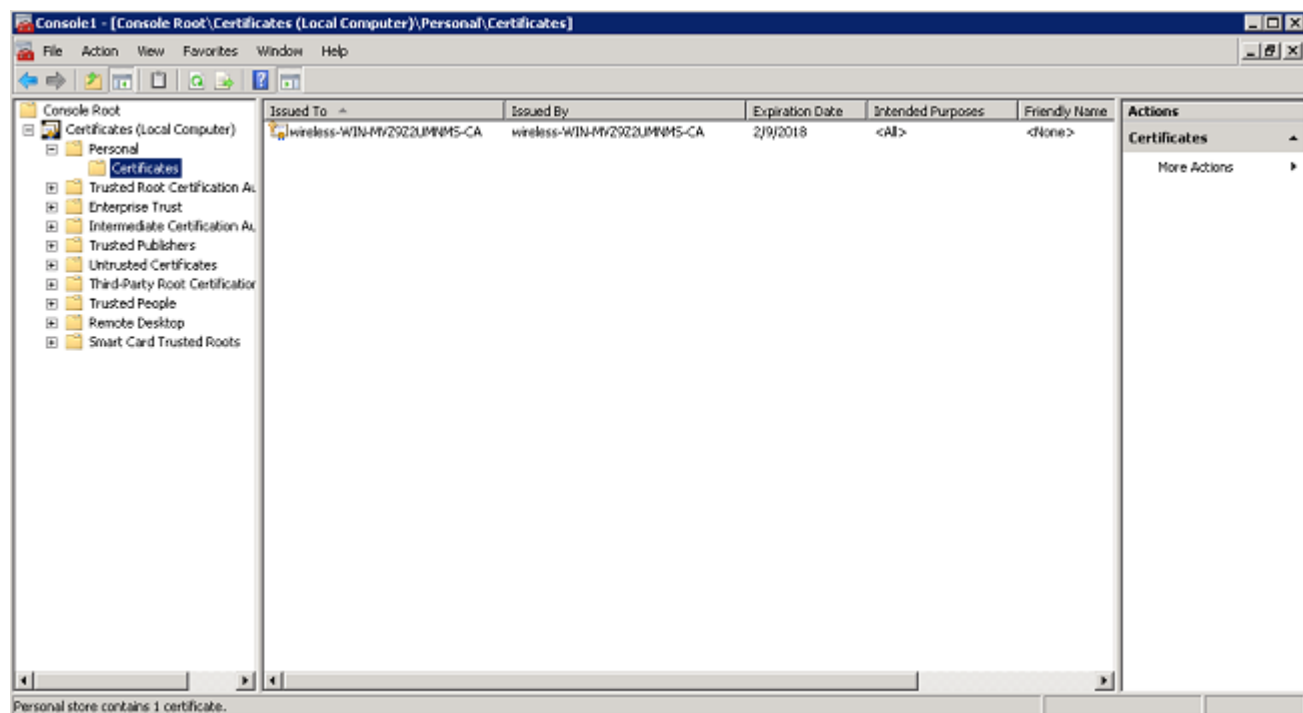




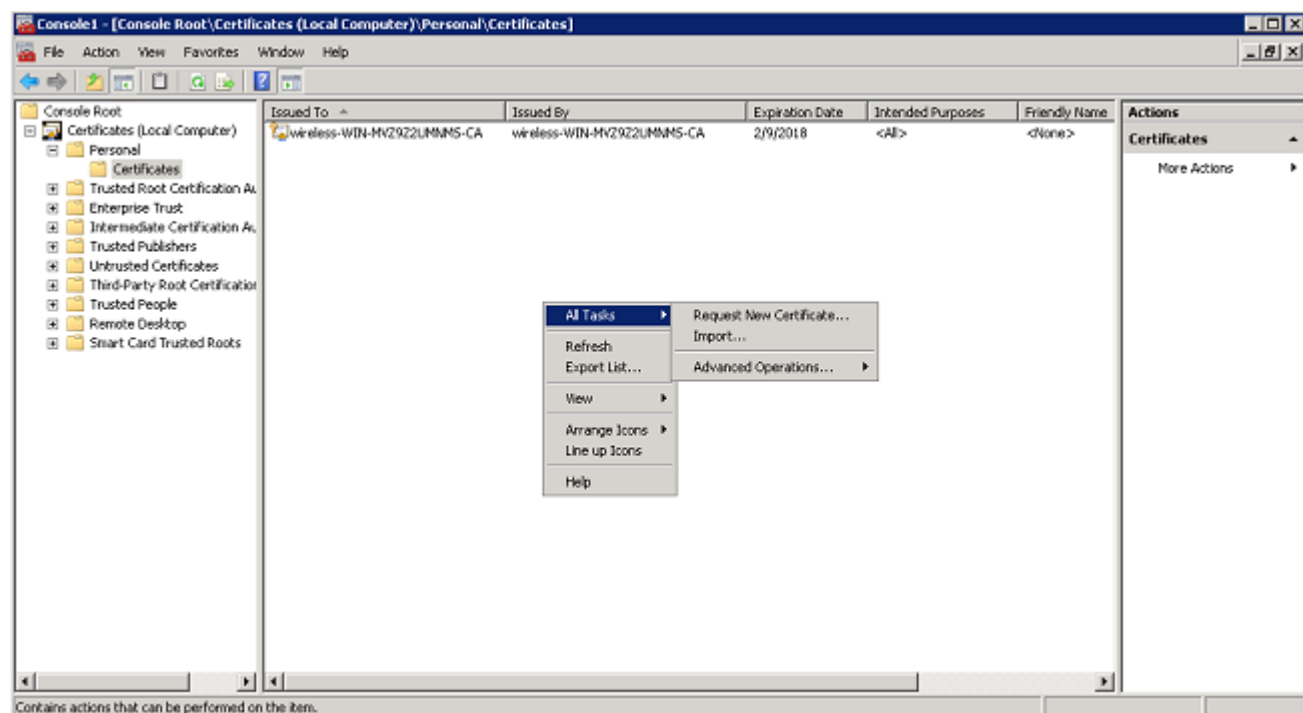
6. Klicken Sie auf OK, um zur Microsoft Management Console (MMC) zurückzukehren.



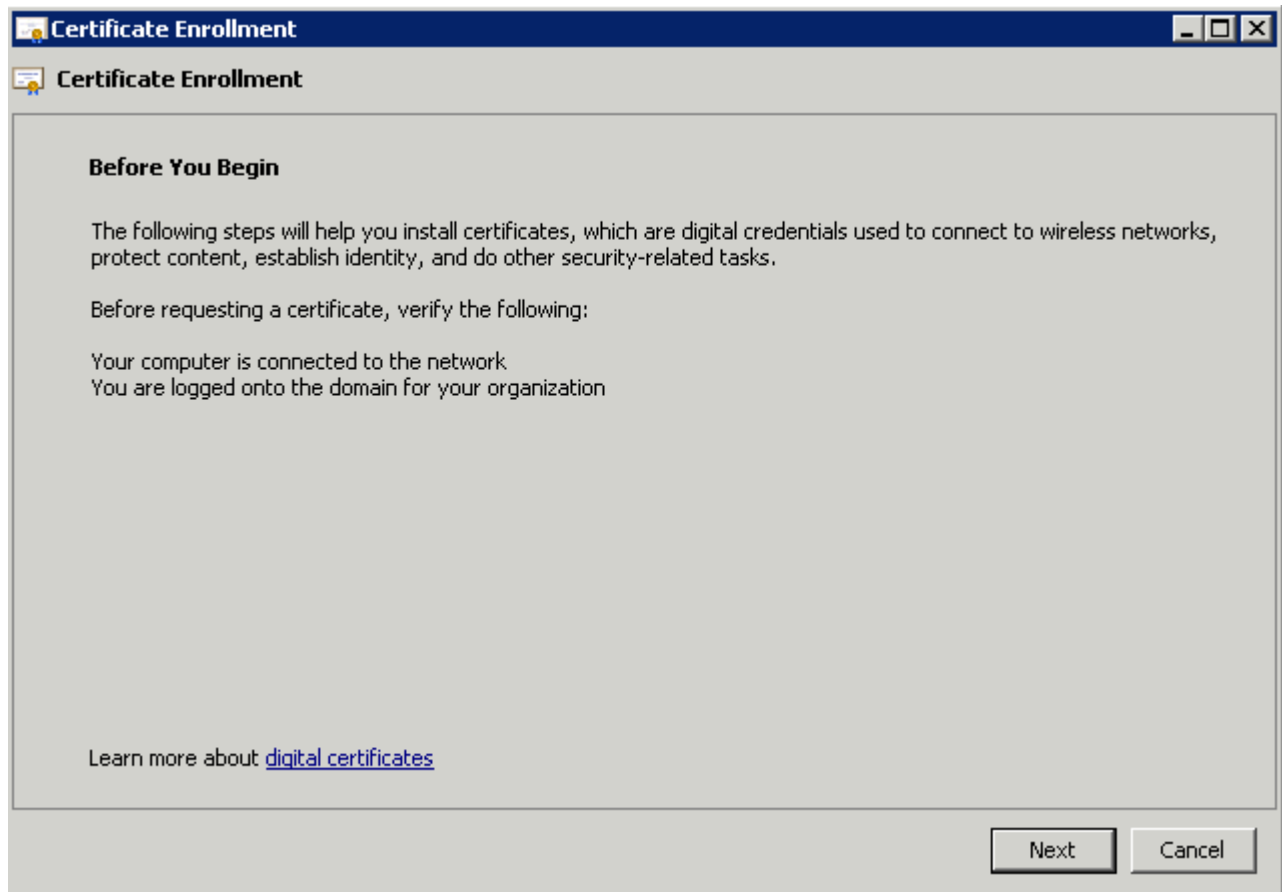
7. Erweitern Sie die Ordner Zertifikate (Lokaler Computer) und Persönliche Ordner, und klicken Sie auf Zertifikate.



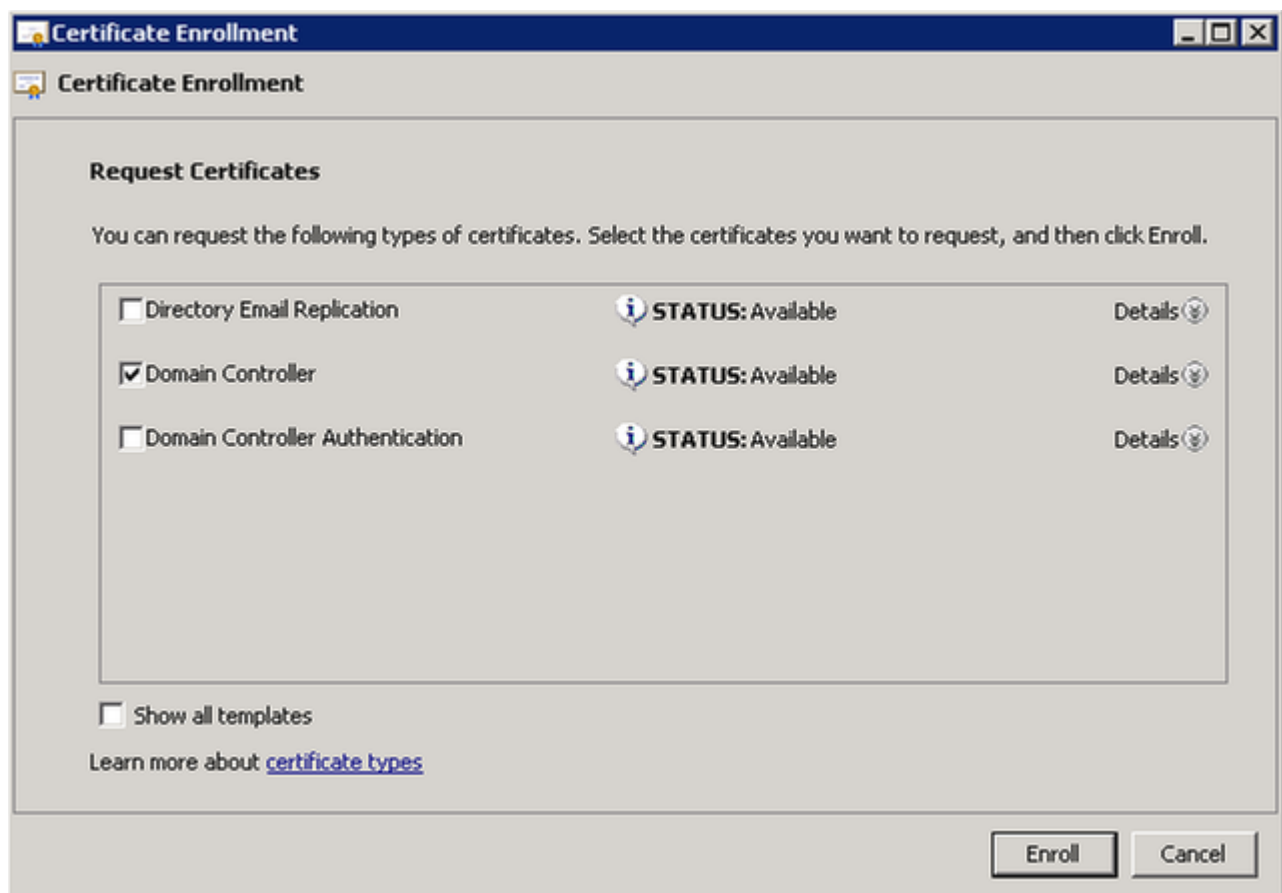
8. Klicken Sie mit der rechten Maustaste in den leeren Bereich unterhalb des Zertifizierungsstellenzertifikats, und wählen Sie Alle Aufgaben > Neues Zertifikat anfordern aus.



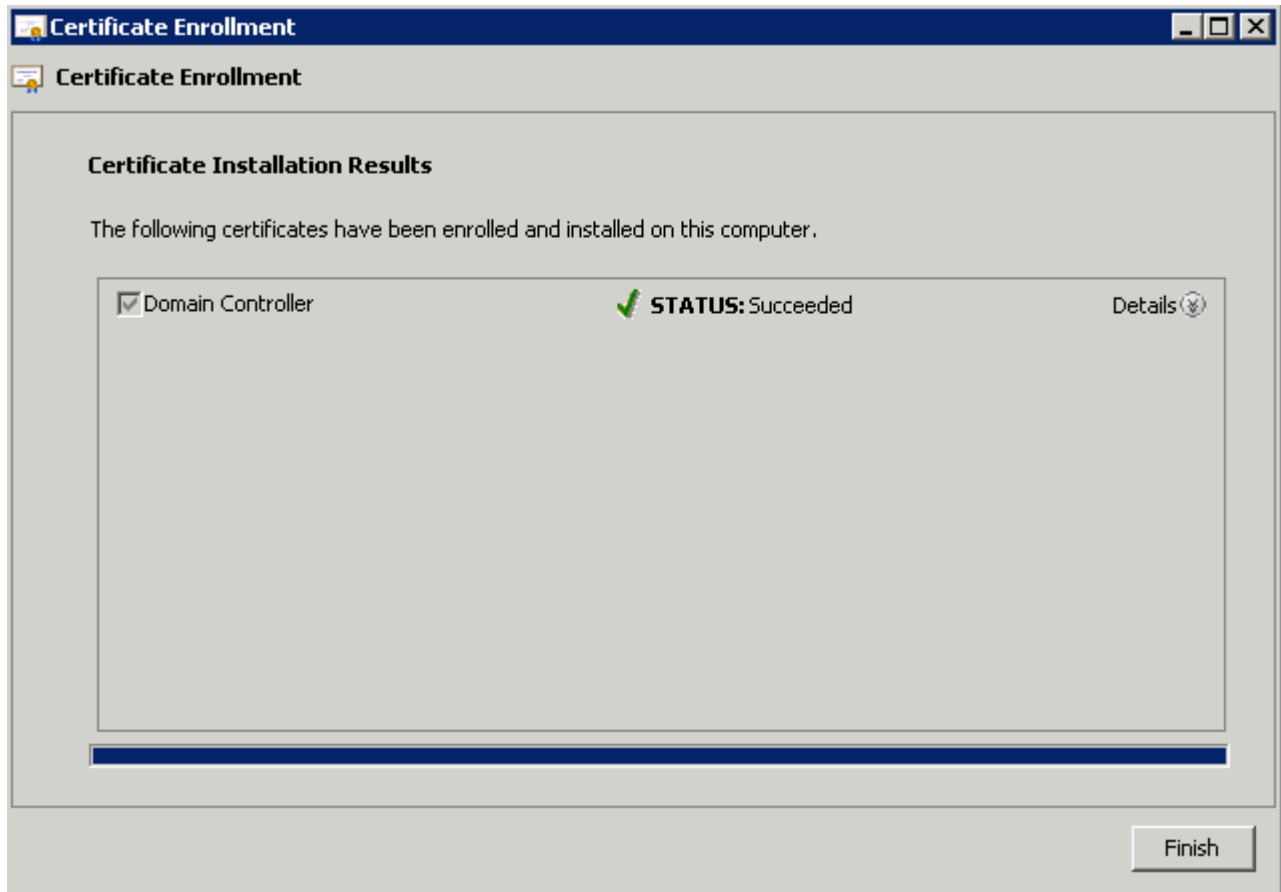
9. Klicken Sie auf Next (Weiter).



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

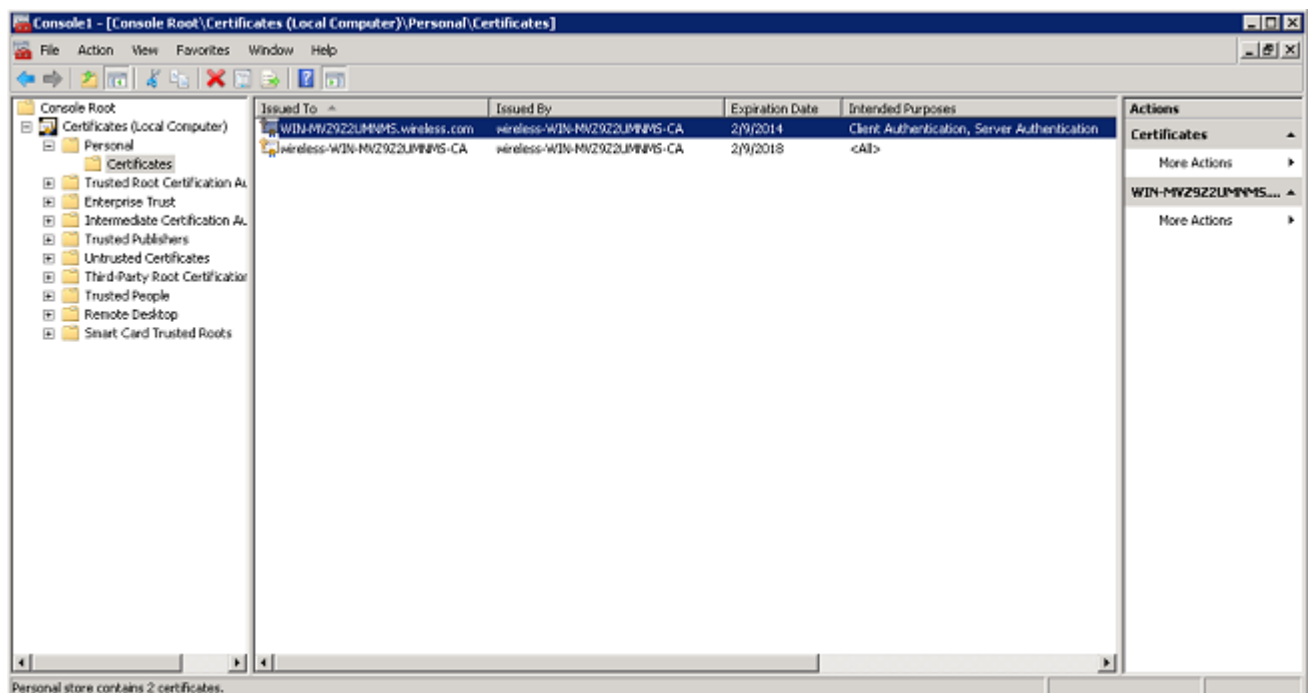


11. Klicken Sie nach der Installation des Zertifikats auf Fertig stellen.



Das NPS-Zertifikat ist jetzt installiert.

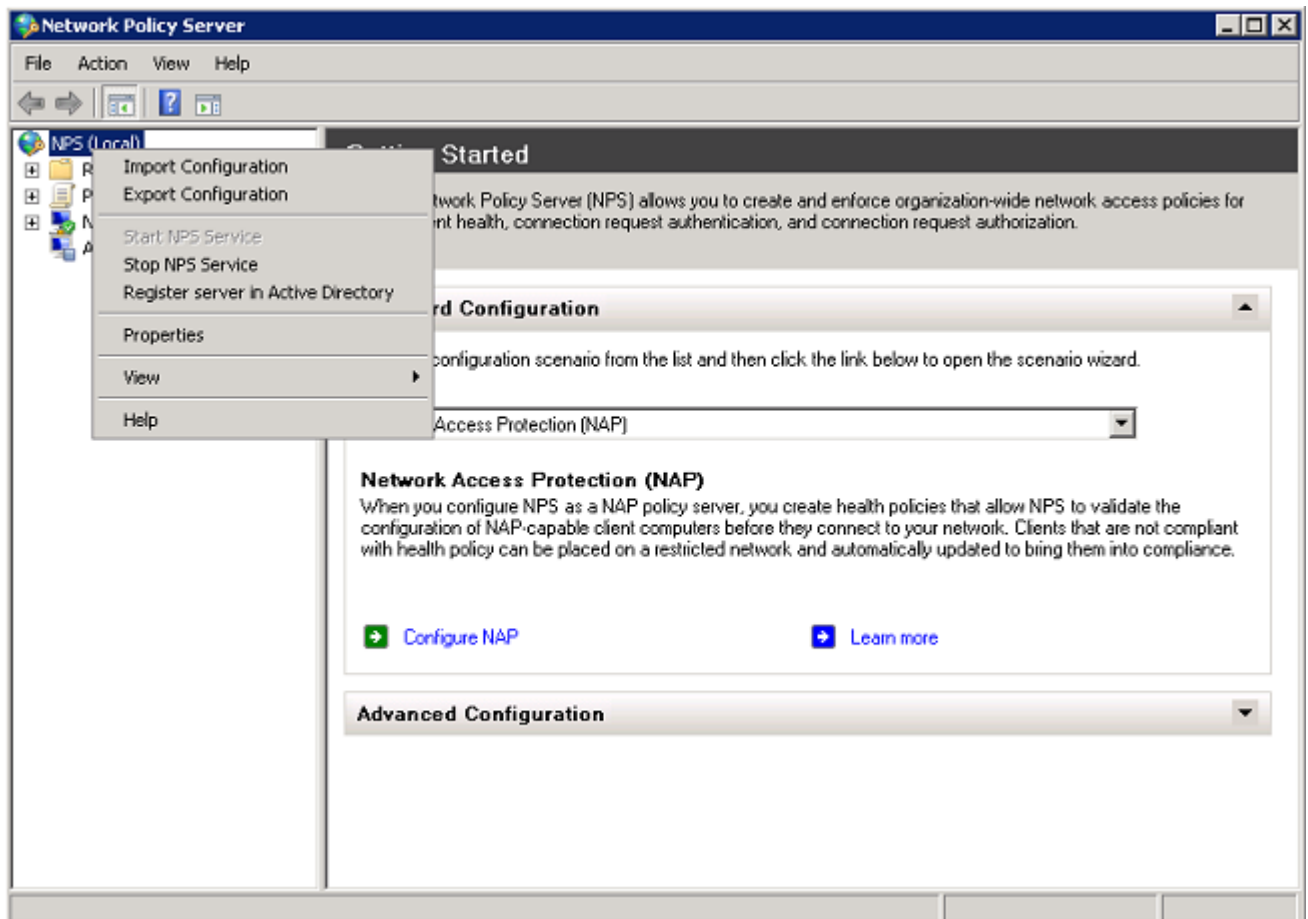
12. Stellen Sie sicher, dass der beabsichtigte Zweck des Zertifikats "Client Authentication, Server Authentication" lautet.



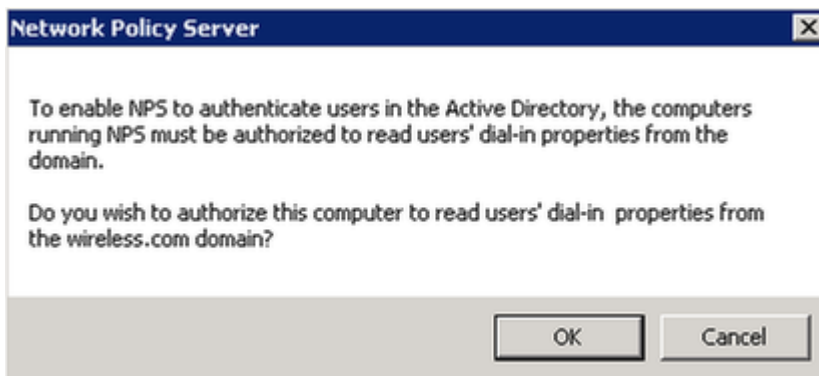
## Konfigurieren des Netzwerkrichtlinienserver-Diensts für die PEAP-MS-CHAP v2-Authentifizierung

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

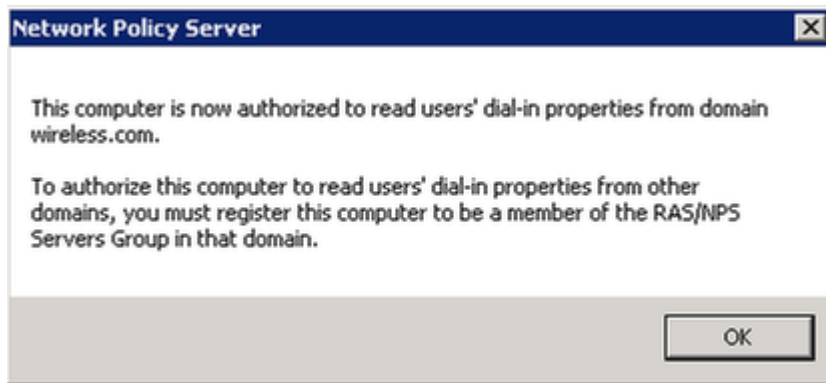
1. Klicken Sie auf Start > Verwaltung> Netzwerkrichtlinienserver.
2. Klicken Sie mit der rechten Maustaste auf NPS (Lokal), und wählen Sie Server in Active Directory registrieren aus.



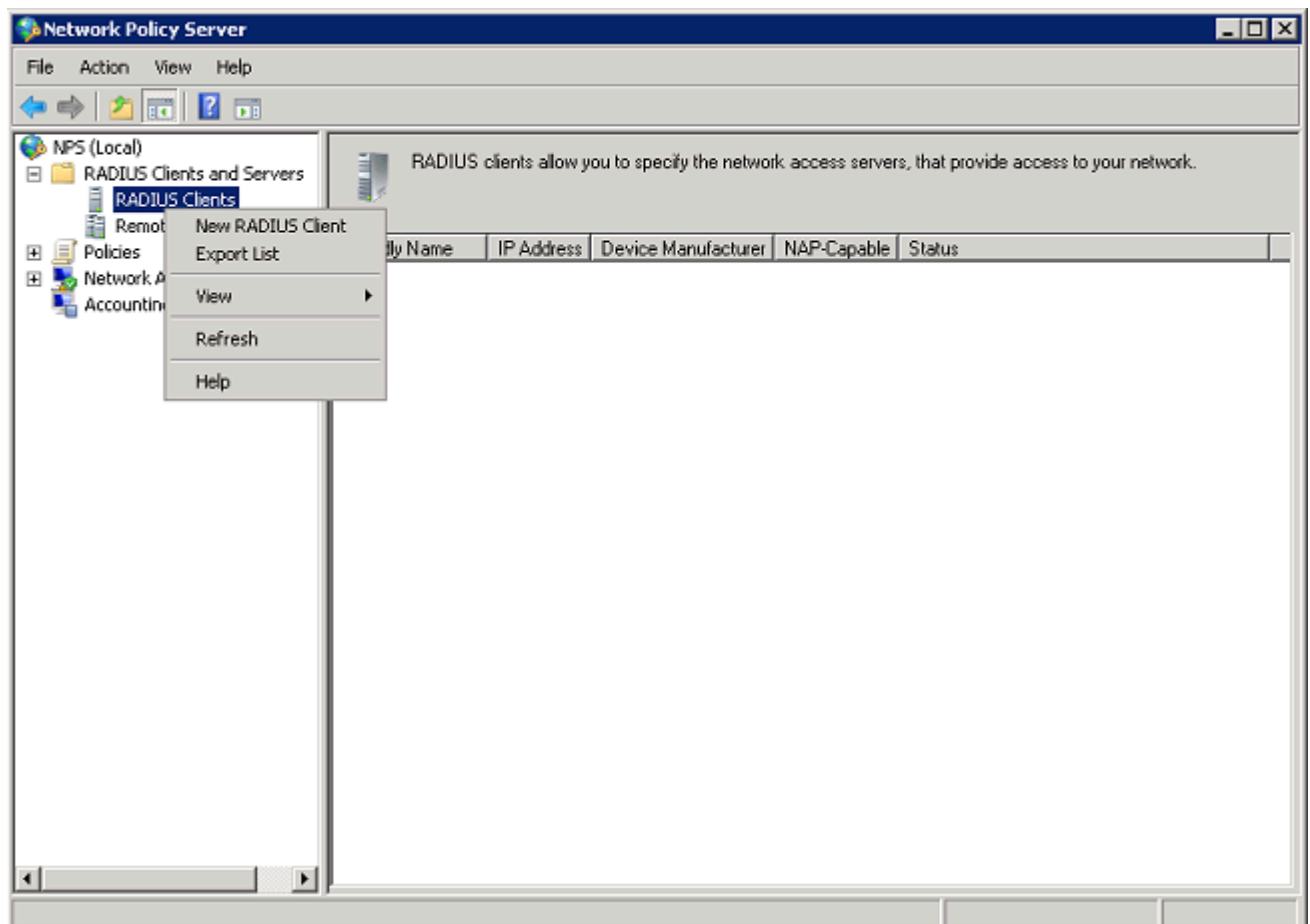
3. Klicken Sie auf OK.



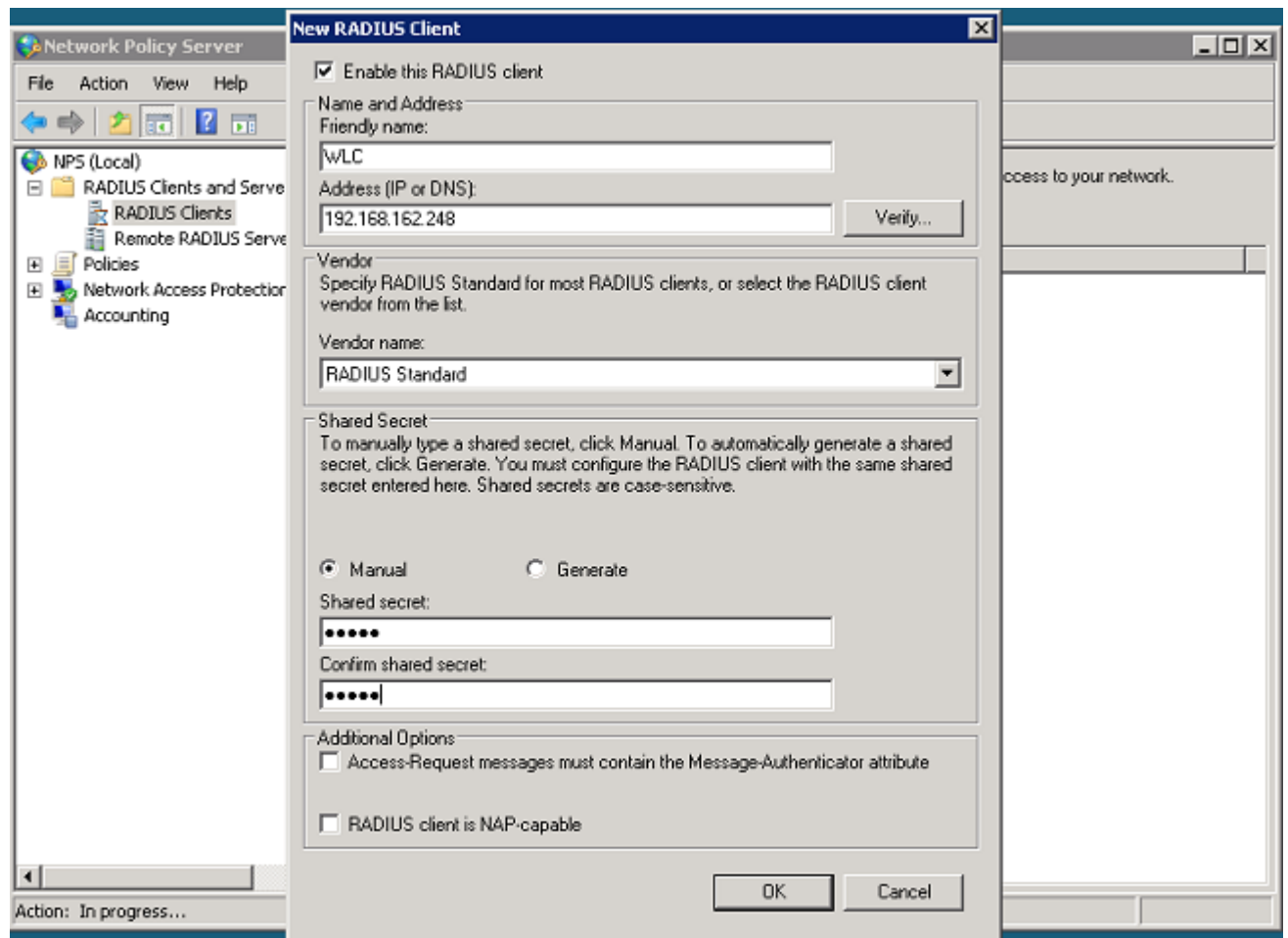
4. Klicken Sie auf OK.



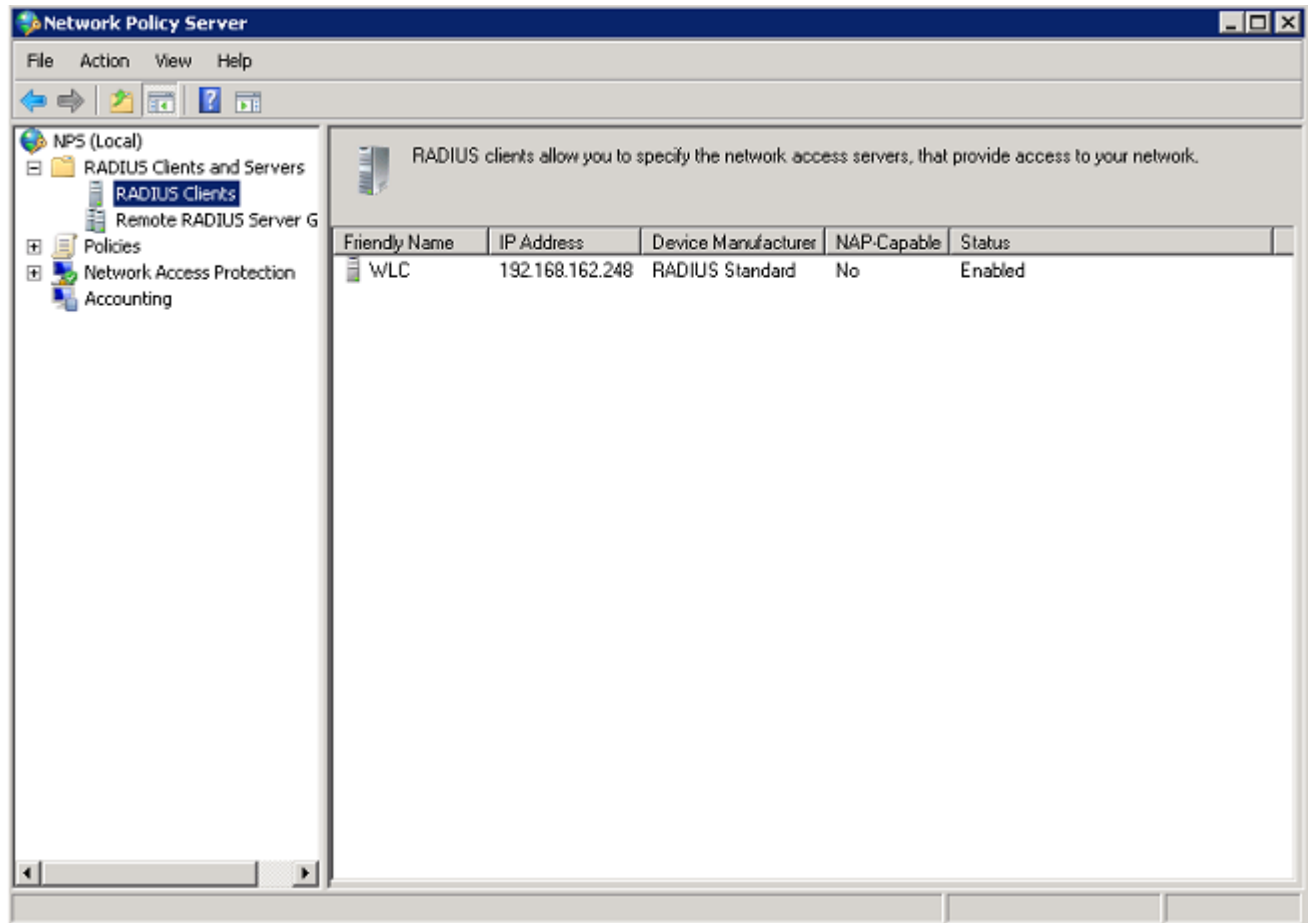
5. Fügen Sie den Wireless LAN Controller als AAA-Client (Authentication, Authorization, Accounting) auf dem NPS hinzu.
6. Erweitern Sie RADIUS-Clients und -Server. Klicken Sie mit der rechten Maustaste auf RADIUS Clients, und wählen Sie New RADIUS Client (Neuer RADIUS-Client).



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.

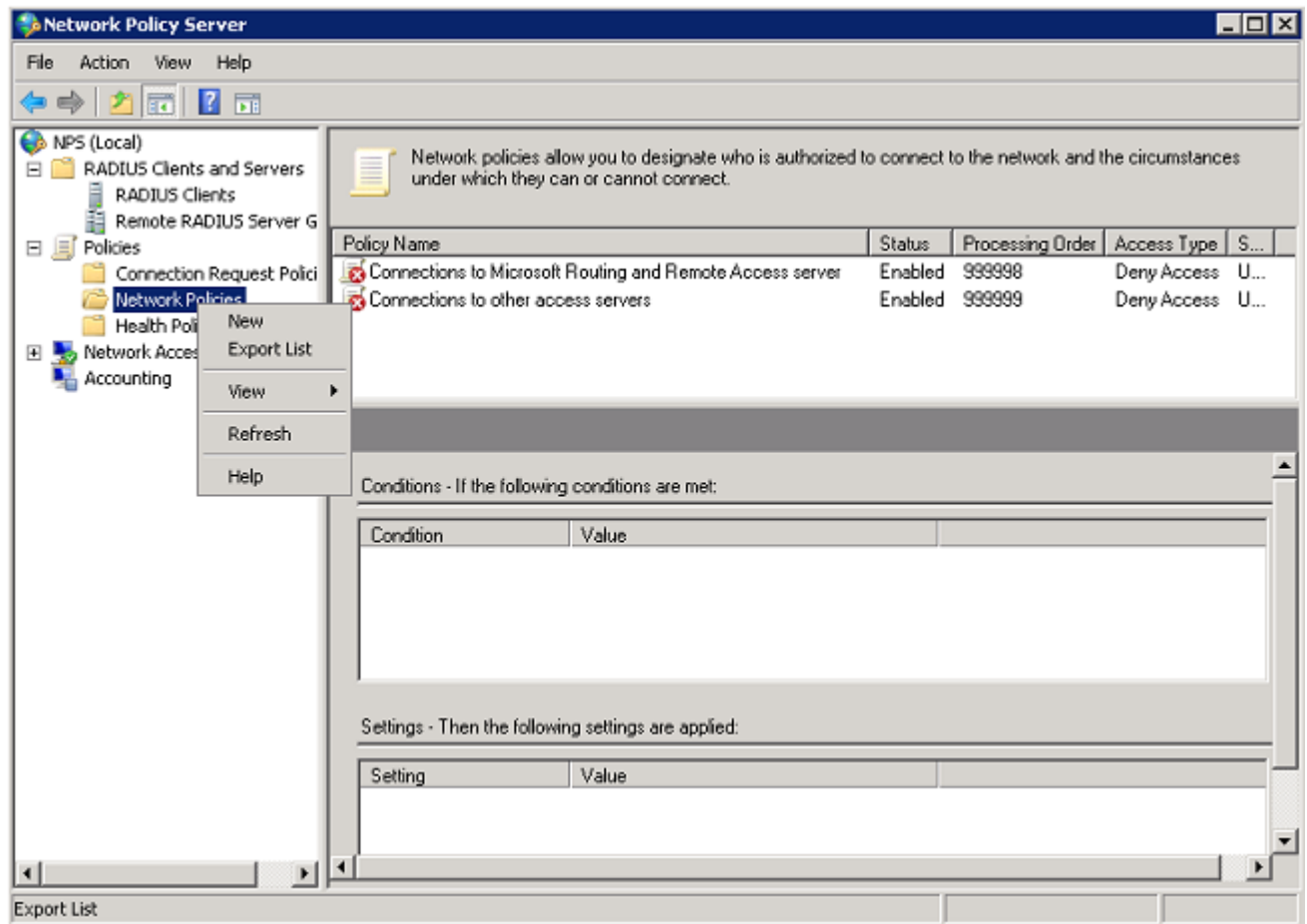


8. Klicken Sie auf OK, um zum vorherigen Bildschirm zurückzukehren.



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.

**New Network Policy**

### Specify Network Policy Name and Connection Type

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

**Policy name:**  
Wireless PEAP

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

☒ Type of network access server:  
Unspecified

☐ Vendor specific:  
10

Previous Next Finish Cancel

11. 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

New Network Policy

## Specify Conditions

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

**Conditions:**

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

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


Add... Edit... Remove

Previous Next Finish Cancel

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

New Network Policy ✕

---



## Specify Access Permission

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

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

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

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

Previous

Next

Finish

Cancel

13. Deaktivieren Sie alle Authentifizierungsmethoden unter Weniger sichere Authentifizierungsmethoden.

**New Network Policy**

## Configure Authentication Methods

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

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

**EAP Types:**

Move Up  
Move Down

Add... Edit... Remove

**Less secure authentication methods:**

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

Previous Next Finish Cancel

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

**New Network Policy**

## Configure Authentication Methods

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

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

**EAP Types:**

Microsoft: Protected EAP (PEAP)

Move Up

Move Down

Add...

Edit...

Remove

**Less secure authentication methods:**

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

Previous

Next

Finish

Cancel

15. 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.

New Network Policy

**Edit Protected EAP Properties**

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

Certificate issued: WIN-MVZ9Z2UMNMS.wireless.com

Friendly name:

Issuer: wireless-WIN-MVZ9Z2UMNMS-CA

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

☒ Enable Fast Reconnect

☐ Disconnect Clients without Cryptobinding

Eap Types

Secured password (EAP-MSCHAP v2)

Move Up

Move Down

Add Edit Remove OK Cancel

☐ User can change password after it has expired

☐ Encrypted authentication (CHAP)

☐ Unencrypted authentication (PAP, SPAP)

☐ Allow clients to connect without negotiating an authentication method.

☐ Perform machine health check only

Previous Next Finish Cancel

16. Klicken Sie auf Next (Weiter).

**New Network Policy** [X]

## Configure Authentication Methods

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

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

**EAP Types:**

Microsoft: Protected EAP (PEAP)

Move Up

Move Down

Add...

Edit...

Remove

**Less secure authentication methods:**

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

Previous

Next

Finish

Cancel

17. Klicken Sie auf Next (Weiter).



New Network Policy

## Configure Constraints

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

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

**Constraints:**

**Constraints**

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

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

☐ Disconnect after the maximum idle time

1

Previous Next Finish Cancel

18. Klicken Sie auf Next (Weiter).

**New Network Policy**

## Configure Settings

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

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

**Settings:**

**RADIUS Attributes**

- ☒ Standard
- ☐ Vendor Specific

**Network Access Protection**

- ☒ NAP Enforcement
- ☒ Extended State

**Routing and Remote Access**

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

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

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

Add... Edit... Remove

Previous Next Finish Cancel

19. Klicken Sie auf Beenden.

**New Network Policy**

## Completing New Network Policy

You have successfully created the following network policy:

**Wireless PEAP**

**Policy conditions:**

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

**Policy settings:**

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

To close this wizard, click Finish.

Previous Next Finish Cancel

### 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).

**New Object - User**

Create in: wireless.com/Users

First name: Client1 Initials:

Last name:

Full name: Client1

User logon name: Client1 @wireless.com

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

< Back Next > Cancel

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.

**New Object - User**

Create in: wireless.com/Users

Password:

Confirm password:

☐ User must change password at next logon

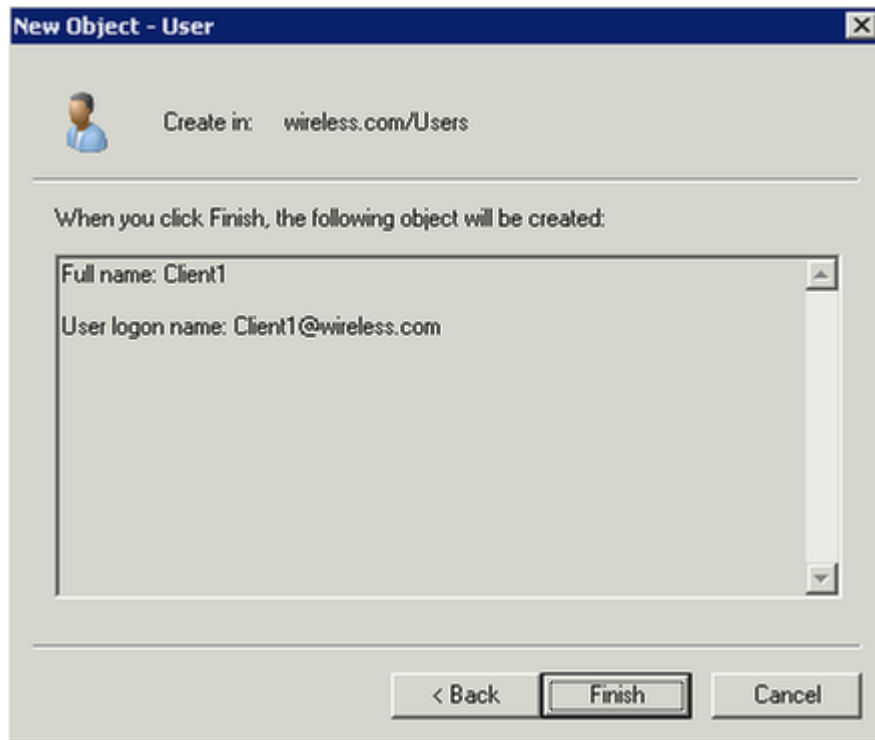
☐ User cannot change password

☐ Password never expires

☐ Account is disabled

< Back Next > Cancel

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.

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

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

Security

AAA

General

RADIUS
 

Authentication
 Accounting
 Fallback

TACACS+
 

LDAP

Local Net Users

MAC Filtering

Disabled Clients

User Login Policies

AP Policies

Password Policies

Local EAP

Priority Order

Certificate

Access Control Lists

Wireless Protection Policies

Web Auth

TrustSec SXP

Advanced

RADIUS Authentication Servers

Apply

New...

Cell Station ID Type

IP Address

Use AES Key Wrap

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

MAC Delimiter

Hyphen

Network User

Management

Server Index

Server Address

Port

IPSec

Admin Status

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

- 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.

The screenshot shows the Cisco Wireless LAN Controller (WLC) configuration interface. The top navigation bar includes links for 'Save Configuration', 'Ping', 'Logout', and 'Refresh'. The main menu on the left is under 'Security' and includes options like 'AAA', 'RADIUS', 'TACACS+', 'Local EAP', 'Priority Order', 'Certificate', 'Access Control Lists', 'Wireless Protection Policies', 'Web Auth', 'TrustSec SXP', and 'Advanced'. The right pane is titled 'RADIUS Authentication Servers > New' and contains the following configuration fields:

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

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

## 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.

WLANs > New

Type: WLAN

Profile Name: PEAP

SSID: PEAP

ID: 1

< Back 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.

WLANs > Edit 'PEAP'

< Back Apply

General Security QoS Advanced

Profile Name: PEAP

Type: WLAN

SSID: PEAP

Status: ☒ Enabled

Security Policies: [WPA2][Auth(802.1X)]  
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All

Interface/Interface Group(G): management

Multicast Vlan Feature: ☐ Enabled

Broadcast SSID: ☒ Enabled

NAS-ID: 2504

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.



WLANs > Edit 'PEAP' < Back Apply

**General Security QoS Advanced**

**Layer 2 Layer 3 AAA Servers**

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

**Fast Transition**  
 Fast Transition ☐

**Protected Management Frame**  
 PMF **Disabled**

**WPA+WPA2 Parameters**

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

**Authentication Key Management**

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

3. 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.

WLANs > Edit 'PEAP' < Back Apply

**General Security QoS Advanced**

**Layer 2 Layer 3 AAA Servers**

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

**Radius Servers**

Radius Server Overwrite interface ☐ Enabled

	Authentication Servers	Accounting Servers
Server 1	<input checked="" type="checkbox"/> Enabled IP:192.168.162.12, Port:1812	<input checked="" type="checkbox"/> Enabled None
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

**LDAP Servers**

Server 1 **None**  
 Server 2 **None**  
 Server 3 **None**

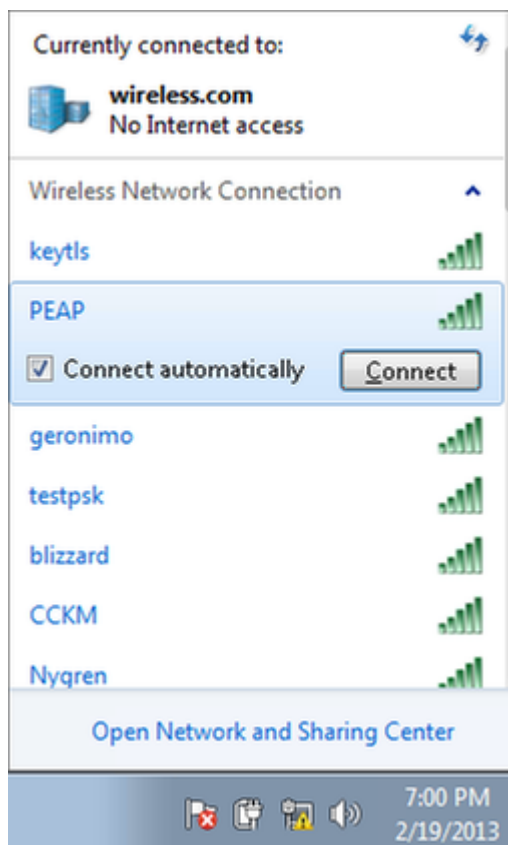
**Radius Server Accounting**  
 Interim Update ☐

**Local EAP Authentication**  
 Local EAP Authentication ☐ Enabled

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:

```
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db 192.168.162.136 RUN (20) Changing IPw4 ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2018)
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db 192.168.162.136 RUN (20) Changing IPw4 ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2246)
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db In processAddID:4202 setting Central switched to TRUE
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db In processAddID:4202 apVapId = 1 and Split Acl Id = 63355
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db Applying site-specific Local Bridging override for station 78:e4:00:b2:ef:db - vapId 1, site 'default-group', interface 'management'
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db Applying Local Bridging Interface Policy for station 78:e4:00:b2:ef:db - vlan 243, interface id 0, interface 'management'
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db processSsidIE statusCode is 0 and status is 0
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db processSsidIE ssid_done_flag is 0 finish_flag is 0
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db STA - rates [0]: 130 132 133 135 36 48 72 108 12 18 24 36 0 0 0 0
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db suppRates statusCode is 0 and gotSuppRatesElement is 1
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db STA - rates [12]: 130 132 133 135 36 48 72 108 12 18 24 36 0 0 0 0
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db csiSuppRates statusCode is 0 and gotCsiSuppRatesElement is 1
*apMgmtConnTask_2: Feb 19 20:57:07.612: 78:e4:00:b2:ef:db Processing RSN IE type 48, length 20 for mobile 78:e4:00:b2:ef:db
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db Received RSN IE with 0 PMKIDs from mobile 78:e4:00:b2:ef:db
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db Found an cache entry for SSID c0:f9:f9:1a:20:40 in PMKID cache at index 0 of station 78:e4:00:b2:ef:db
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db Removing SSID c0:f9:f9:1a:20:40 from PMKID cache of station 78:e4:00:b2:ef:db
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db Reinserting MSD PMG Cache Entry 5 for station 78:e4:00:b2:ef:db
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db Setting active key cache index 0 ----> 0
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db unsetting PmkIdValidatedMsg
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db apMgmtStateDec
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db apMgmtStateDec
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db 192.168.162.136 RUN (20) Change state to START (0) last state RUN (20)
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db pmcApMgmtMobileStation2: APF MS PMG WAIT 13 AUTH COMPLETE = 0.
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db 192.168.162.136 START (0) Initializing policy
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db 192.168.162.136 START (0) Change state to AUTHCHECK (2) last state START (0)
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db 192.168.162.136 AUTHCHECK (2) Change state to 8021K_REQD (3) last state AUTHCHECK (2)
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db MSG Using MPM Compliance code: qoeCap 00
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db 192.168.162.136 8021K_REQD (3) Plumbed mobile LWAPP role on AP c0:f9:f9:1a:20:40 vapId 1 file-acl-name:
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db apfMgmtTask2: apfMgmtTask2: Changing state for mobile 78:e4:00:b2:ef:db on AP c0:f9:f9:1a:20:40 from Associated to Associated
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db apfMgmtTask2: session timeout formation: 78:e4:00:b2:ef:db - Session Timeout 0, apMgmtTask2 "0" and sessionTimerRunning flag is 0
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db Stopping detection of Mobile Station: (callerId: 48)
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db Func: apfMgmtTask2, Ms Timeout = 0, Session Timeout = 0
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db Sending Assoc Response to station on SSID c0:f9:f9:1a:20:40 (status 0) ApVapId 1 Slot 0
*apMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db apfProcessAssocReq (apf_03211.c:7391) Changing state for mobile 78:e4:00:b2:ef:db on AP c0:f9:f9:1a:20:40 from Associated to Associated
*pmcMgmtConnTask_2: Feb 19 20:57:07.613: 78:e4:00:b2:ef:db 192.168.162.136 Removed MPM entry.
*dot1xMgmtTask_2: Feb 19 20:57:07.620: 78:e4:00:b2:ef:db Disable re-auth, use PMK lifetime.
*dot1xMgmtTask_2: Feb 19 20:57:07.620: 78:e4:00:b2:ef:db dot1x - moving mobile 78:e4:00:b2:ef:db into Connecting state
*dot1xMgmtTask_2: Feb 19 20:57:07.620: 78:e4:00:b2:ef:db Sending EAP-Request/Identity to mobile 78:e4:00:b2:ef:db (EAP Id 1)
*dot1xMgmtTask_2: Feb 19 20:57:07.638: 78:e4:00:b2:ef:db Received EAPOL START from mobile 78:e4:00:b2:ef:db
*dot1xMgmtTask_2: Feb 19 20:57:07.638: 78:e4:00:b2:ef:db dot1x - moving mobile 78:e4:00:b2:ef:db into Connecting state
*dot1xMgmtTask_2: Feb 19 20:57:07.639: 78:e4:00:b2:ef:db Sending EAP-Request/Identity to mobile 78:e4:00:b2:ef:db (EAP Id 2)
*dot1xMgmtTask_2: Feb 19 20:57:07.639: 78:e4:00:b2:ef:db Received EAPOL EAPREQ from mobile 78:e4:00:b2:ef:db
*dot1xMgmtTask_2: Feb 19 20:57:07.655: 78:e4:00:b2:ef:db Received EAP Response packet with mismatching id (currentid=2, apid=1) from mobile 78:e4:00:b2:ef:db
*dot1xMgmtTask_2: Feb 19 20:57:07.656: 78:e4:00:b2:ef:db Received EAPOL EAPREQ from mobile 78:e4:00:b2:ef:db
*dot1xMgmtTask_2: Feb 19 20:57:07.656: 78:e4:00:b2:ef:db Received Identity Response (currentid=2) from mobile 78:e4:00:b2:ef:db
*dot1xMgmtTask_2: Feb 19 20:57:07.656: 78:e4:00:b2:ef:db EAP State update from Connecting to Authenticating for mobile 78:e4:00:b2:ef:db
*dot1xMgmtTask_2: Feb 19 20:57:07.656: 78:e4:00:b2:ef:db dot1x - moving mobile 78:e4:00:b2:ef:db into Authenticating state
```

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 EAPFRM 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 EAPFRM 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 EAPFRM from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.611: 78:e4:00:b2:ef:db Received Identity Response (count=2) from mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.611: 78:e4:00:b2:ef:db EAP State update from Connecting to Authenticating for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.611: 78:e4:00:b2:ef:db dot1x - moving mobile 78:e4:00:b2:ef:db into Authenticating state
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.611: 78:e4:00:b2:ef:db Entering Backend Auth Response state for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.643: 78:e4:00:b2:ef:db Processing Access-Challenge for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.643: 78:e4:00:b2:ef:db Entering Backend Auth Req state (id=3) for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.643: 78:e4:00:b2:ef:db Sending EAP Request from AAA to mobile 78:e4:00:b2:ef:db (EAP Id 3)
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.661: 78:e4:00:b2:ef:db Received EAPOL EAPFRM 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 EAPFRM 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 EAPFRM 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 EAPFRM 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 EAPFRM 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 EAPFRM 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 21:33:14.759: 78:e4:00:b2:ef:db Processing Access-Challenge for mobile 78:e4:00:b2:ef:db
*Dot1x_NW_MsgTask_3: Feb 19 21:33:14.759: 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 21:33:14.759: 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 EAPFRM 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.

The screenshot shows the Windows Event Viewer window. The left pane shows the tree structure with 'Network Policy and Access Services' expanded. The main pane displays a list of 23 events. The bottom pane shows the details for Event 6278, Microsoft Windows security auditing.

Level	Date and Time	Source	Event ID	Task Cat...
Information	2/19/2013 4:28:30 PM	Microsoft...	6278	Network ...
Information	2/19/2013 4:28:30 PM	Microsoft...	6272	Network ...
Information	2/19/2013 4:28:29 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:23:42 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:23:40 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:22:58 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:22:18 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:22:17 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:21:13 PM	Microsoft...	6273	Network ...
Information	2/19/2013 4:21:13 PM	NPS	4400	None
Error	2/19/2013 3:52:33 PM	NPS	18	None
Error	2/19/2013 3:52:31 PM	NPS	18	None
Error	2/19/2013 3:52:29 PM	NPS	18	None
Error	2/19/2013 3:52:27 PM	NPS	18	None
Error	2/19/2013 3:52:25 PM	NPS	18	None
Error	2/19/2013 3:52:23 PM	NPS	18	None
Information	2/19/2013 3:36:57 PM	Microsoft...	6278	Network ...
Information	2/19/2013 3:36:57 PM	Microsoft...	6272	Network ...
Information	2/19/2013 3:36:52 PM	Microsoft...	6273	Network ...
Information	2/19/2013 3:32:13 PM	Microsoft...	6273	Network ...
Information	2/19/2013 3:32:03 PM	Microsoft...	6273	Network ...
Information	2/19/2013 3:32:02 PM	Microsoft...	6273	Network ...
Information	2/19/2013 3:32:02 PM	NPS	4400	None

Event 6278, Microsoft Windows security auditing.

General Details

Network Policy Server granted full access to a user because the host met the defined health policy.

User:

Log Name: Security

Source: Microsoft Windows security auditing. Logged: 2/19/2013 4:28:30 PM

Event ID: 6278 Task Category: Network Policy Server

Level: Information Keywords: Audit Success

User: N/A Computer: WIN-MVZ92UMNMS.wireless.com

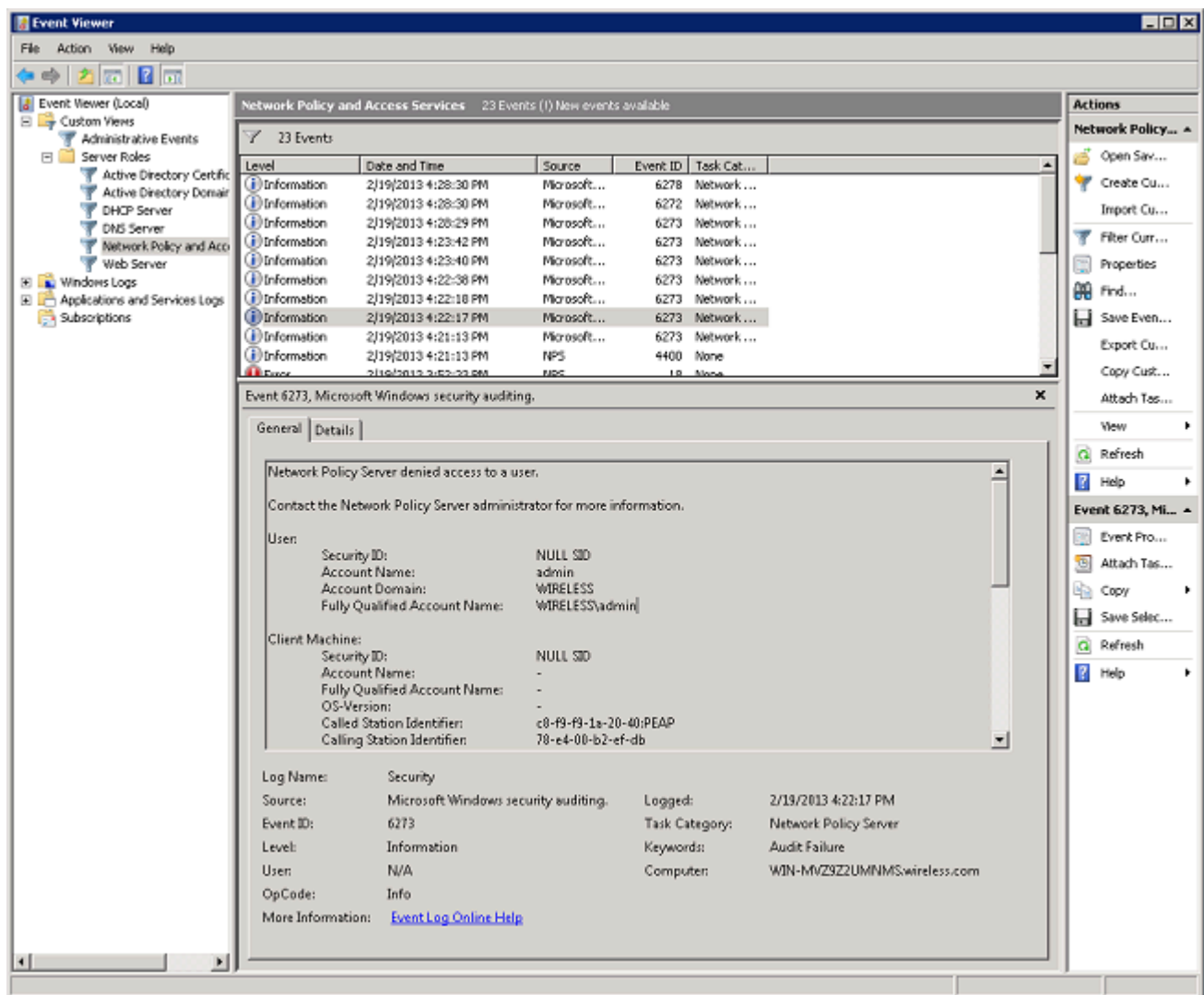
OpCode: Info

More Information: [Event Log Online Help](#)

In diesem Abschnitt der Ereignisanzeige 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: -

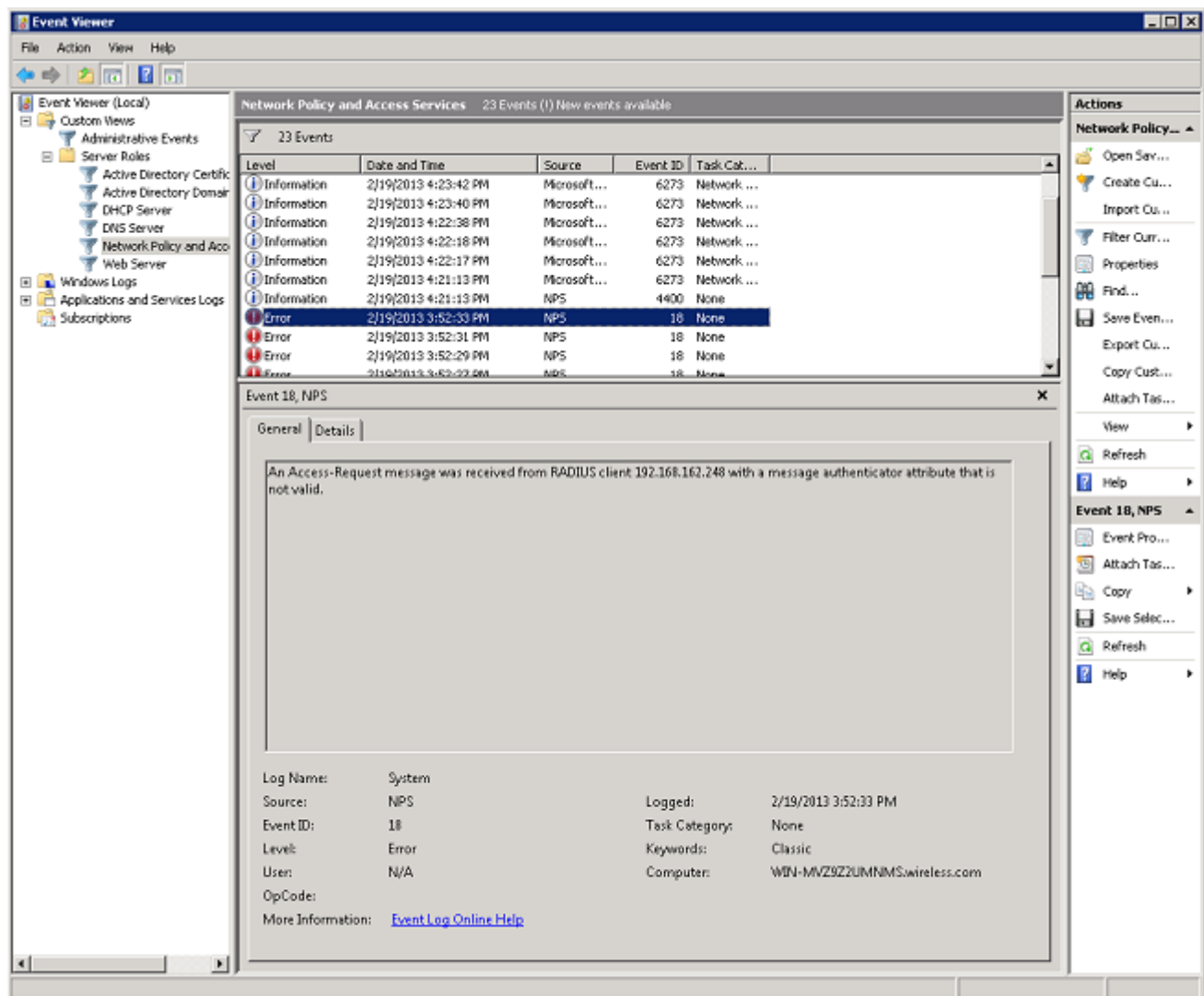
Account Session Identifier: -

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.