

# PEAP unter Unified Wireless Networks mit Microsoft Internet Authentication Service (IAS)

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[PEAP-Übersicht](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Konfigurieren von Microsoft Windows 2003 Server](#)

[Konfigurieren von Microsoft Windows 2003 Server](#)

[Installieren und Konfigurieren der DHCP-Dienste auf dem Microsoft Windows 2003 Server](#)

[Installieren und Konfigurieren von Microsoft Windows 2003 Server als CA-Server \(Certificate Authority\)](#)

[Clients mit der Domäne verbinden](#)

[Installieren des Internetauthentifizierungsdiensts auf dem Microsoft Windows 2003-Server und Anfordern eines Zertifikats](#)

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

[Hinzufügen von Benutzern zum Active Directory](#)

[Wireless-Zugriff für Benutzer zulassen](#)

[Konfigurieren des Wireless LAN-Controllers und der Lightweight Access Points](#)

[Konfigurieren des WLC für die RADIUS-Authentifizierung über den MS IAS-RADIUS-Server](#)

[Konfigurieren eines WLAN für die Clients](#)

[Konfigurieren der Wireless-Clients](#)

[Konfigurieren der Wireless Clients für die PEAP-MS CHAPv2-Authentifizierung](#)

[Überprüfung und Fehlerbehebung](#)

[Zugehörige Informationen](#)

## Einleitung

Dieses Dokument enthält ein Konfigurationsbeispiel für die Einrichtung des Protected Extensible Authentication Protocol (PEAP) mit der MS-CHAP-Authentifizierung (Microsoft Challenge Handshake Authentication Protocol) Version 2 in einem Cisco Unified Wireless-Netzwerk mit dem Microsoft Internet Authentication Service (IAS) als RADIUS-Server.

## Voraussetzungen

## Anforderungen

Es wird davon ausgegangen, dass der Leser über Grundkenntnisse der Windows 2003-Installation und der Cisco Controller-Installation verfügt, da in diesem Dokument nur die spezifischen Konfigurationen behandelt werden, mit denen die Tests vereinfacht werden.

**Hinweis:** Dieses Dokument soll den Lesern ein Beispiel für die Konfiguration geben, die auf dem MS-Server für die PEAP - MS CHAP-Authentifizierung erforderlich ist. Die in diesem Abschnitt vorgestellte Microsoft-Serverkonfiguration wurde in der Übung getestet und hat sich als einwandfrei erwiesen. Wenn Sie Probleme bei der Konfiguration des Microsoft-Servers haben, wenden Sie sich an Microsoft. Cisco TAC unterstützt keine Microsoft Windows Server-Konfiguration.

Informationen zur Erstinstallation und -konfiguration der Cisco Controller der Serie 4400 finden Sie in der [Schnellstartanleitung: Cisco Wireless LAN Controller der Serie 4400](#).

Microsoft Windows 2003 Installations- und Konfigurationsanleitungen finden Sie unter [Installieren von Windows Server 2003 R2](#).

Bevor Sie beginnen, installieren Sie das Betriebssystem Microsoft Windows Server 2003 mit SP1 auf jedem der Server im Testlabor, und aktualisieren Sie alle Service Packs. Installieren Sie die Controller und Lightweight Access Points (LAPs), und stellen Sie sicher, dass die neuesten Software-Updates konfiguriert sind.

## Verwendete Komponenten

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

- Cisco Controller der Serie 4400 mit Firmware-Version 4.0
- Cisco 1131 LWAPP AP (Lightweight Access Point Protocol)
- Windows 2003 Enterprise Server (SP1) mit installierten Internetauthentifizierungsdiensten (IAS), Zertifizierungsstellen (Certificate Authority, CA), DHCP- und DNS-Diensten (Domain Name System)
- Windows XP Professional mit SP 2 (und aktualisierten Service Packs) und Cisco Aironet 802.11a/b/g Wireless Network Interface Card (NIC)
- Aironet Desktop Utility Version 4.0
- Cisco Switch 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 Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

## Konventionen

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

## PEAP-Übersicht

PEAP verwendet Transport Level Security (TLS), um einen verschlüsselten Kanal zwischen einem authentifizierenden PEAP-Client wie einem Wireless-Laptop und einem PEAP-Authentifizierer wie Microsoft Internet Authentication Service (IAS) oder einem beliebigen RADIUS-Server zu erstellen. PEAP gibt keine Authentifizierungsmethode an, bietet jedoch zusätzliche Sicherheit für andere EAP-Authentifizierungsprotokolle wie EAP-MSCHAPv2, die über den von PEAP bereitgestellten verschlüsselten TLS-Kanal betrieben werden können. Der PEAP-Authentifizierungsprozess umfasst zwei Hauptphasen:

### **PEAP Phase 1: TLS-verschlüsselter Kanal**

Der Wireless-Client ist mit dem Access Point verknüpft. Eine IEEE 802.11-basierte Zuordnung bietet eine Open System- oder Shared Key-Authentifizierung, bevor eine sichere Zuordnung zwischen dem Client und dem Access Point (LAP) 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 IAS-Server erfolgreich abgeschlossen wurde, wird die TLS-Sitzung zwischen den Clients ausgehandelt. Der in dieser Verhandlung abgeleitete Schlüssel wird zur Verschlüsselung der gesamten nachfolgenden Kommunikation verwendet.

### **PEAP Phase zwei: 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 IAS-Server authentifiziert den Wireless-Client mit EAP-MS-CHAP v2. Die LAP und der Controller leiten nur Meldungen zwischen dem Wireless-Client und dem RADIUS-Server weiter. Der WLC und der LAP können diese Nachrichten nicht entschlüsseln, da sie nicht der TLS-Endpunkt sind.

Nach der ersten PEAP-Phase und der Erstellung des TLS-Kanals zwischen dem IAS-Server und dem 802.1X Wireless-Client wird für einen erfolgreichen Authentifizierungsversuch, bei dem der Benutzer gültige kennwortbasierte Anmeldeinformationen mit PEAP-MS-CHAP v2 angegeben hat, folgende RADIUS-Nachrichtensequenz verwendet:

1. Der IAS-Server sendet eine Identitätsanforderungsnachricht an den Client: EAP-Request/Identity.
2. Der Client antwortet mit einer Identitätsantwort: EAP-Response/Identity.
3. Der IAS-Server sendet eine MS-CHAP v2-Challenge-Meldung: EAP-Request/EAP-Type=EAP MS-CHAP-V2 (Challenge).
4. Der Client antwortet mit einer MS-CHAP v2-Herausforderung und Antwort: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Antwort).
5. Der IAS-Server sendet ein MS-CHAP v2-Erfolgspaket zurück, wenn der Server den Client erfolgreich authentifiziert hat: EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (Success).
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 (Success).
7. Der IAS-Server sendet ein EAP-TLV, das eine erfolgreiche Authentifizierung anzeigt.
8. Der Client antwortet mit einer EAP-TLV-Statuserfolgsmeldung.
9. Der Server schließt die Authentifizierung ab und sendet eine EAP-Success-Nachricht im Klartext. Wenn VLANs für die Client-Isolierung bereitgestellt werden, sind die VLAN-Attribute in dieser Meldung enthalten.

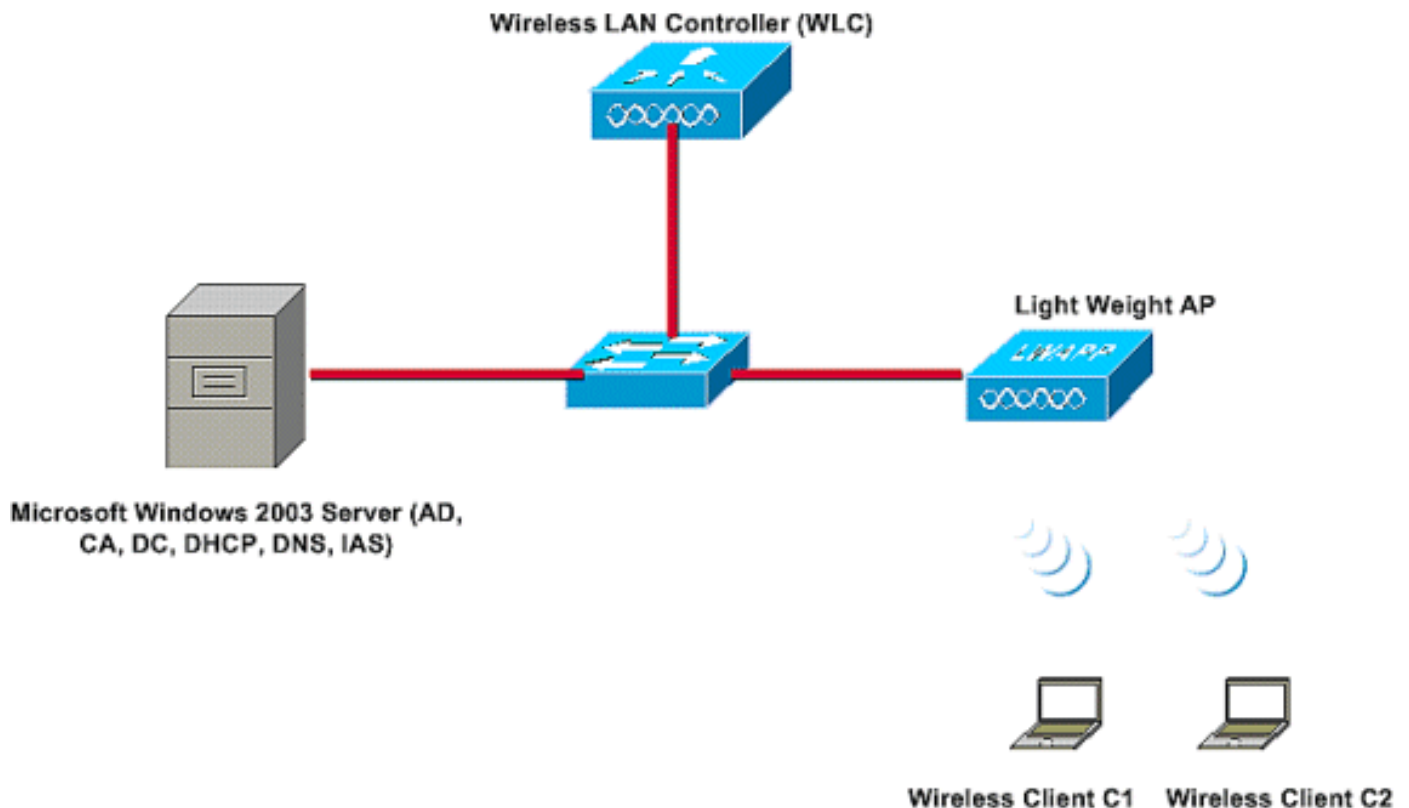
## **Konfigurieren**

Dieses Dokument enthält ein Beispiel für die Konfiguration von PEAP MS-CHAP v2.

**Hinweis:** Verwenden Sie das [Tool für die Suche nach Befehlen \(nur registrierte Kunden\)](#), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

## Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



In diesem Setup führt ein Microsoft Windows 2003-Server die folgenden Rollen aus:

- Domänencontroller für die Domäne **Wireless.com**
- DHCP/DNS-Server
- CA-Server (Certificate Authority)
- Active Directory - zur Verwaltung der Benutzerdatenbank
- Internet Authentication Service (IAS) - zur Authentifizierung der Wireless-Benutzer

Dieser Server ist wie dargestellt über einen Layer-2-Switch mit dem kabelgebundenen Netzwerk verbunden.

Der Wireless LAN Controller (WLC) und die registrierte LAP werden ebenfalls über den Layer-2-Switch mit dem Netzwerk verbunden.

Die Wireless-Clients C1 und C2 verwenden die PEAP MSCHAP v2-Authentifizierung (Wi-Fi Protected Access 2 (WPA2)), um eine Verbindung mit dem Wireless-Netzwerk herzustellen.

Ziel ist es, den Microsoft 2003-Server, den Wireless LAN Controller und den Lightweight Access Point so zu konfigurieren, dass die Wireless-Clients mit PEAP MSCHAP v2-Authentifizierung authentifiziert werden.

Im nächsten Abschnitt wird erläutert, wie Sie die Geräte für dieses Setup konfigurieren.

## Konfigurationen

In diesem Abschnitt wird die Konfiguration beschrieben, die für die Einrichtung der PEAP MS-CHAP v2-Authentifizierung in diesem WLAN erforderlich ist:

- Konfigurieren von Microsoft Windows 2003 Server
- Konfigurieren des Wireless LAN-Controllers (WLC) und der APs mit geringem Gewicht
- Konfigurieren der Wireless-Clients

Beginnen Sie mit der Konfiguration des Microsoft Windows 2003-Servers.

## Konfigurieren von Microsoft Windows 2003 Server

### Konfigurieren von Microsoft Windows 2003 Server

Verwenden Sie, wie im Abschnitt "Netzwerkeinrichtung" erwähnt, den Microsoft Windows 2003-Server im Netzwerk, um diese Funktionen auszuführen.

- **Domänencontroller** - für die Domäne "**Wireless**"
- **DHCP/DNS-Server**
- **CA-Server (Certificate Authority)**
- **Internet Authentication Service (IAS)** - zur Authentifizierung der Wireless-Benutzer
- **Active Directory** - zur Verwaltung der Benutzerdatenbank

Konfigurieren Sie den Microsoft Windows 2003-Server für diese Dienste. Beginnen Sie mit der Konfiguration des Microsoft Windows 2003-Servers als Domänencontroller.

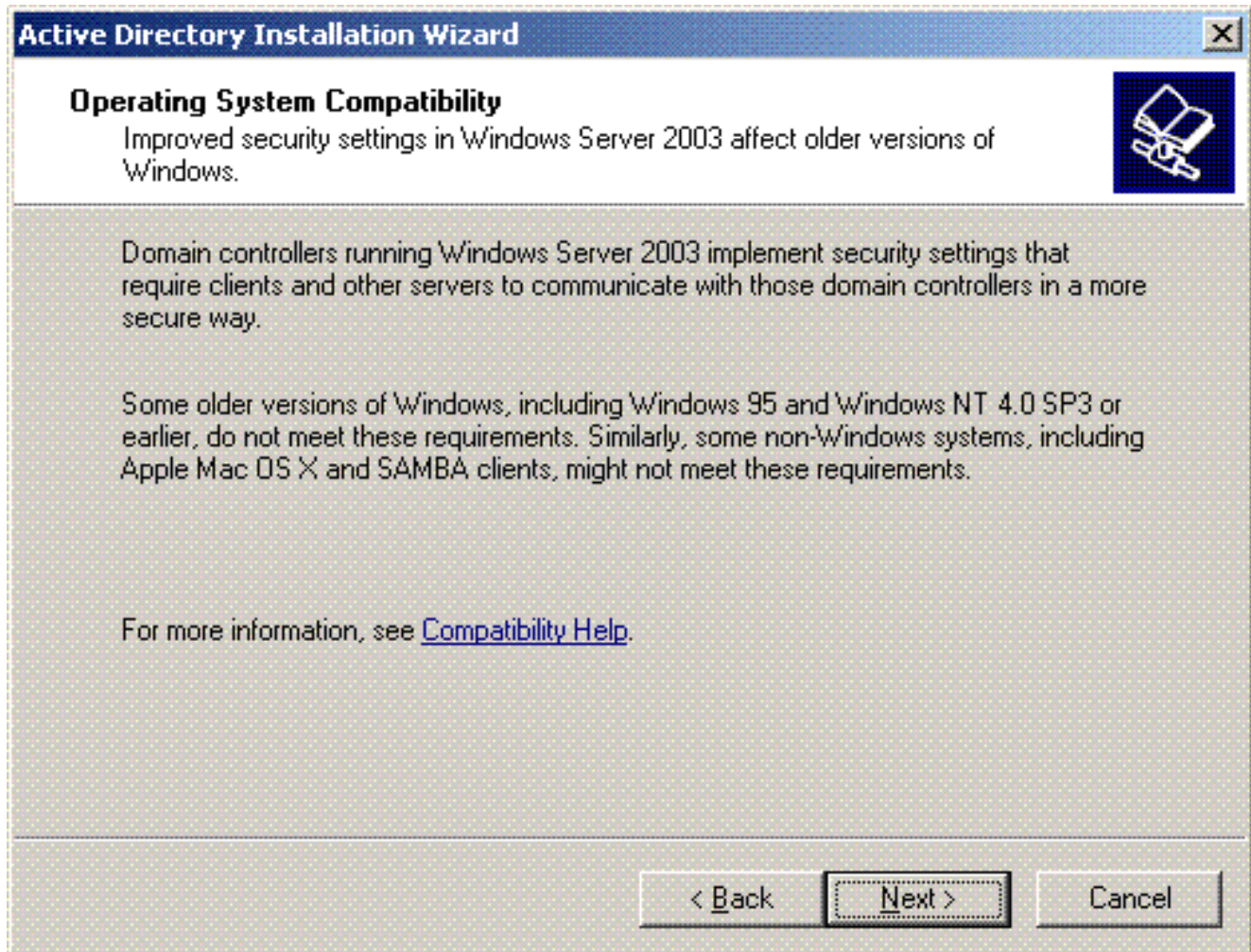
### **Konfigurieren des Microsoft Windows 2003-Servers als Domänencontroller**

Führen Sie die folgenden Schritte aus, um den Microsoft Windows 2003-Server als Domänencontroller zu konfigurieren:

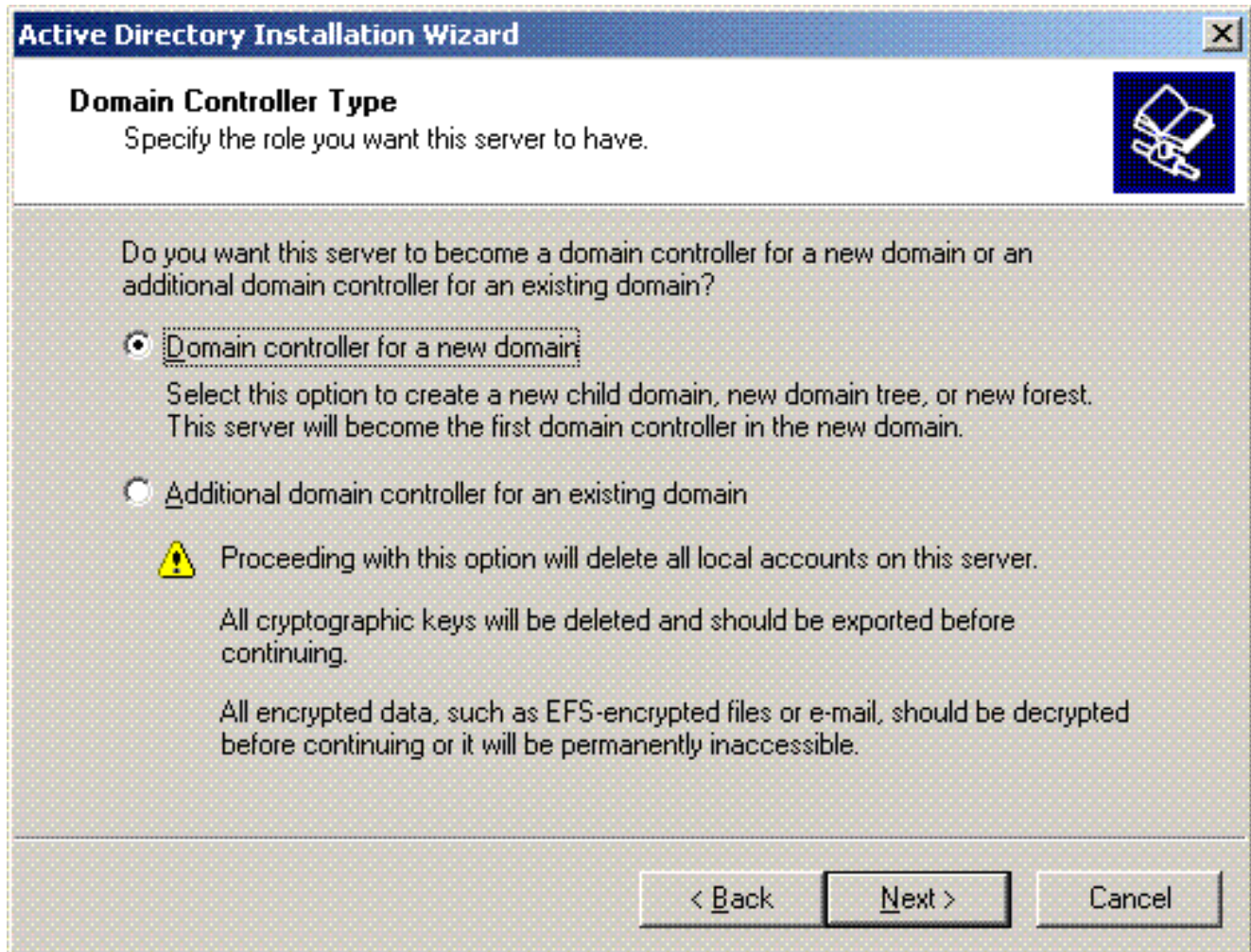
1. Klicken Sie auf **Start**, klicken Sie auf **Ausführen**, geben Sie **dcpromo.exe** ein, und klicken Sie dann auf **OK**, um den Active Directory-Installationsassistenten zu starten.



2. Klicken Sie auf **Weiter**, um den Active Directory-Installationsassistenten auszuführen.

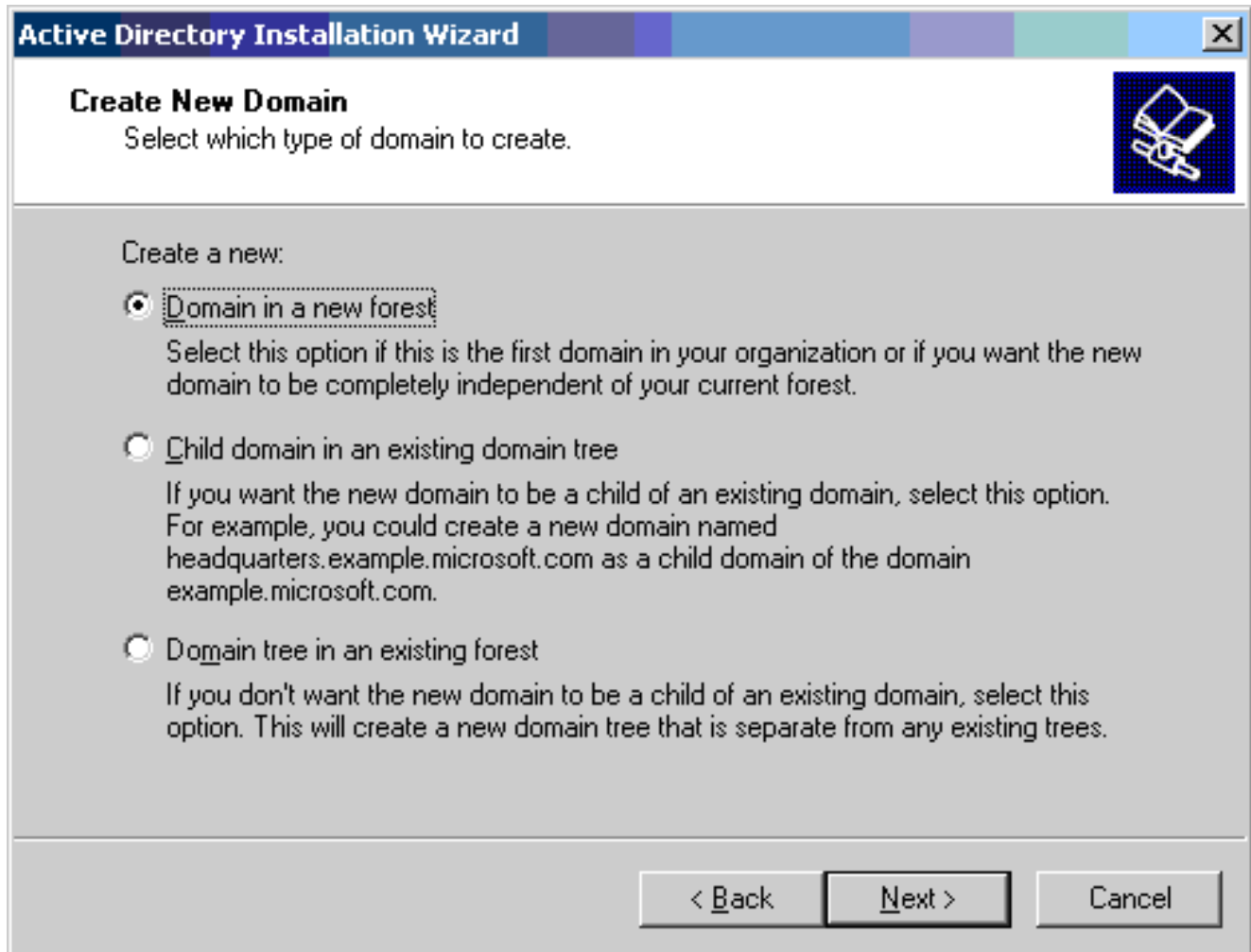


3. Um eine neue Domäne zu erstellen, wählen Sie die Option **Domänencontroller** für eine neue Domäne aus.

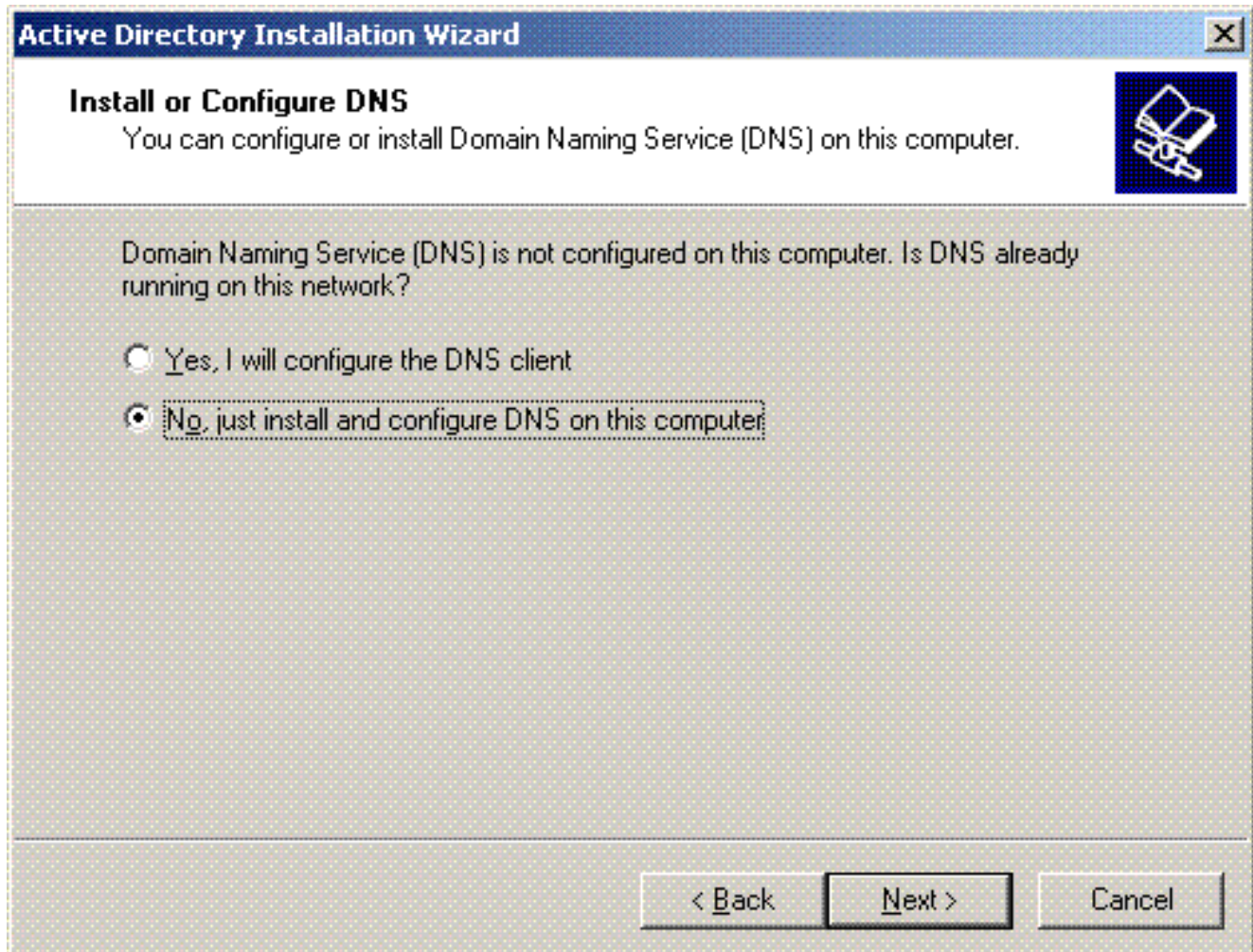


4. Klicken Sie auf **Weiter**, um eine neue Gesamtstruktur von Domänenstrukturen zu erstellen.






5. Wenn DNS nicht auf dem System installiert ist, bietet der Assistent Optionen zum Konfigurieren von DNS. Wählen Sie **Nein, nur DNS auf diesem Computer installieren und konfigurieren**. Klicken Sie auf **Next** (Weiter).



6. Geben Sie den vollständigen DNS-Namen für die neue Domäne ein. In diesem Beispiel wird **Wireless.com** verwendet, und klicken Sie auf **Weiter**.

**Active Directory Installation Wizard** [X]

**New Domain Name**  
Specify a name for the new domain.

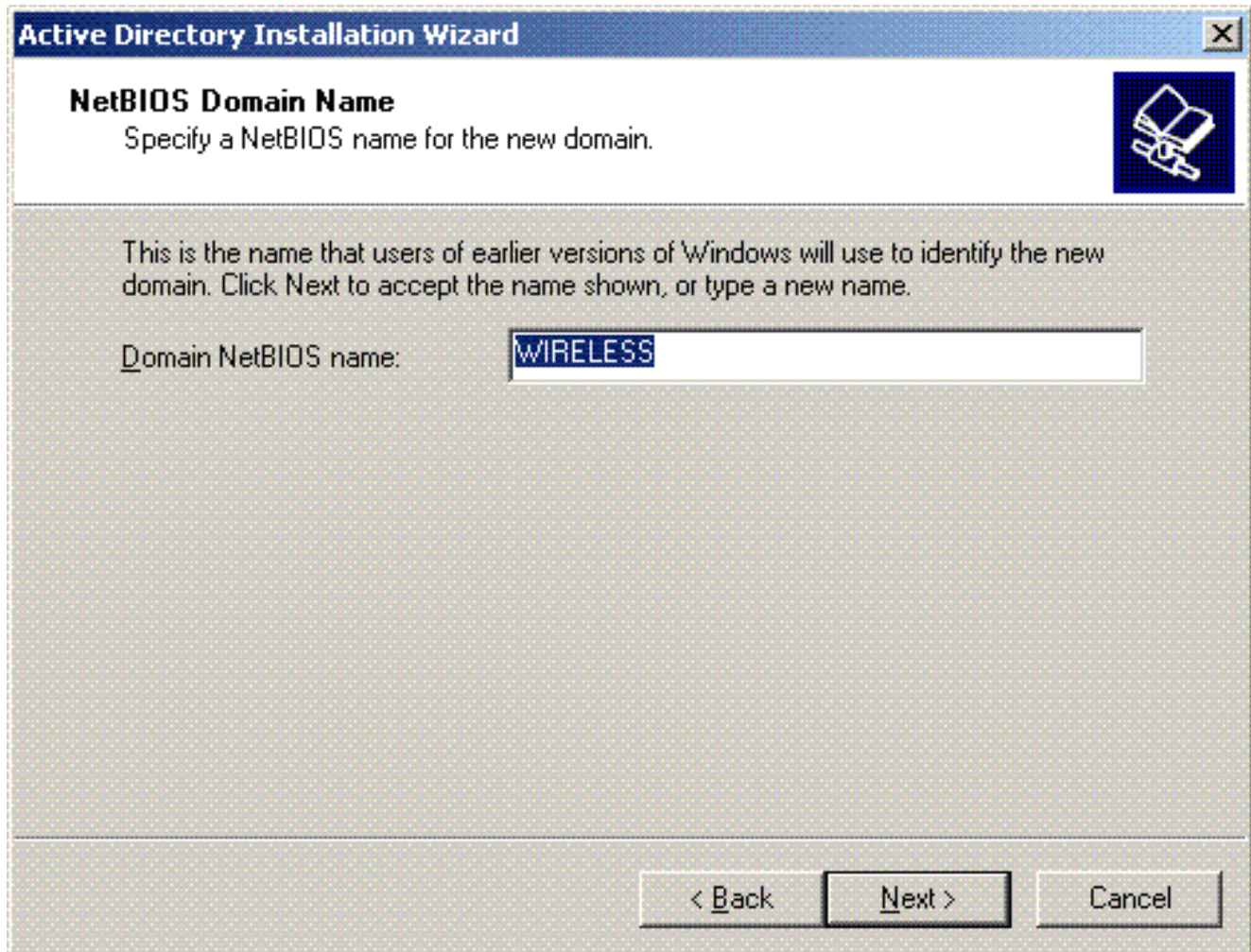


Type the full DNS name for the new domain  
(for example: headquarters.example.microsoft.com).

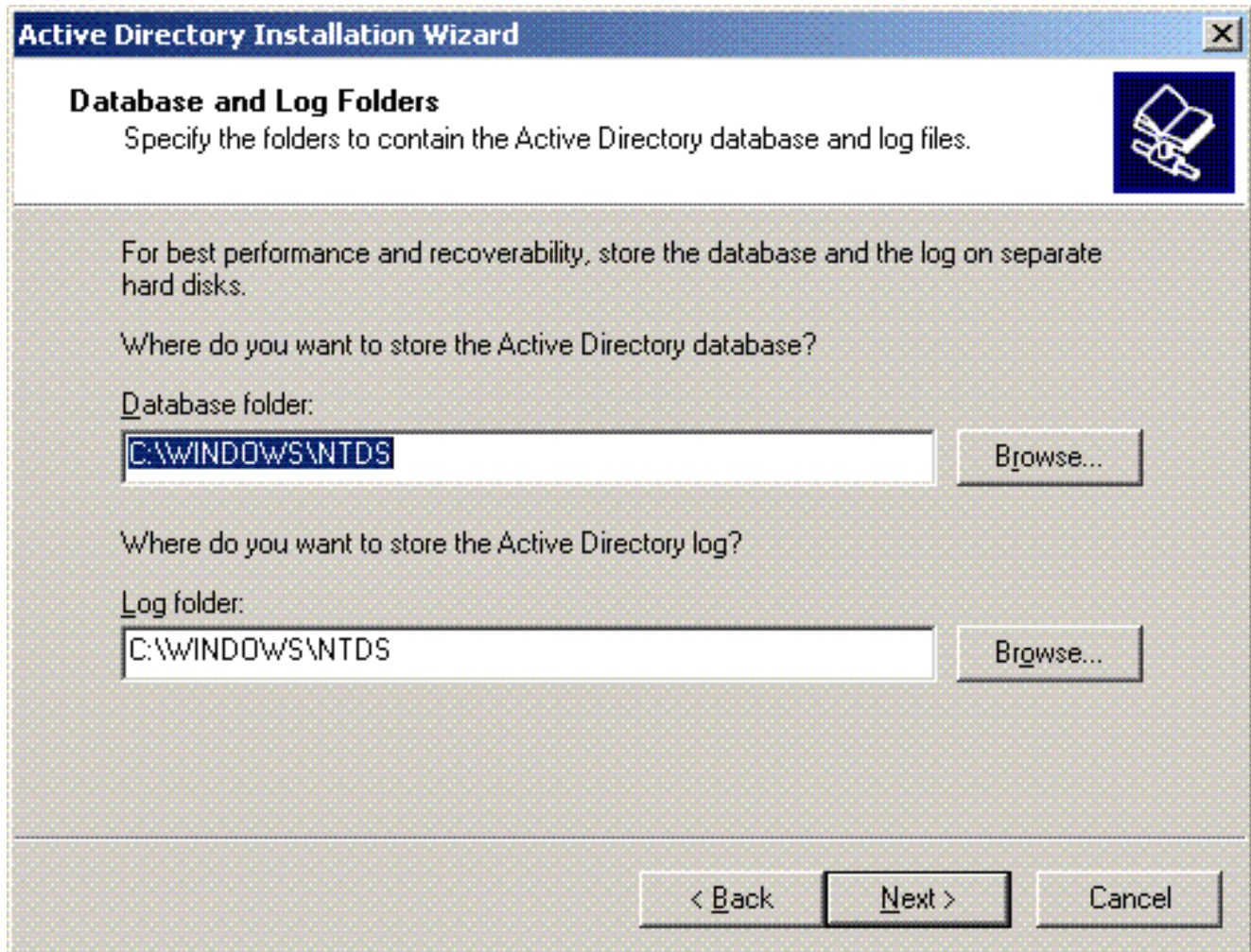
Full DNS name for new domain:

< Back   Next >   Cancel

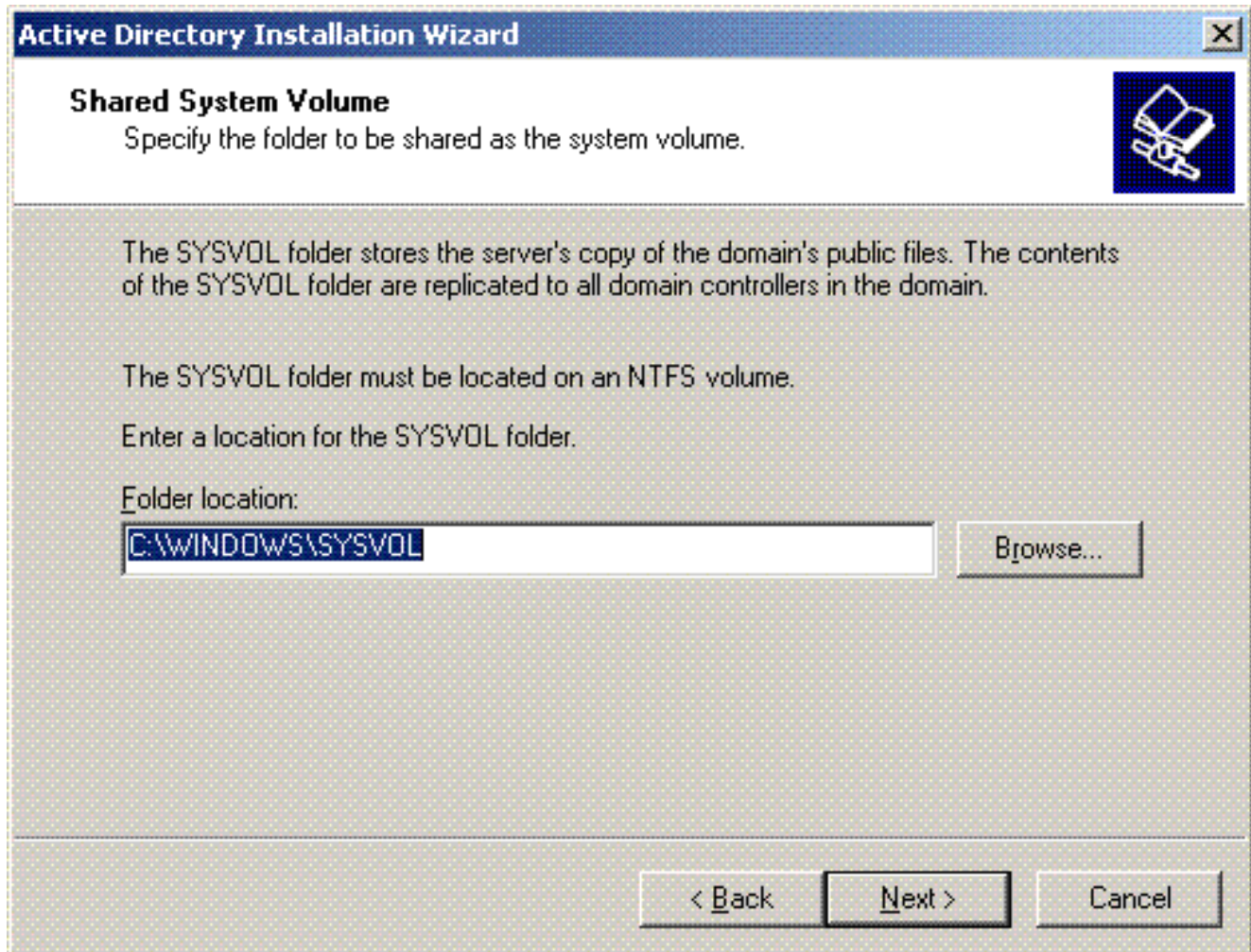
7. Geben Sie den NETBIOS-Namen für die Domäne ein, und klicken Sie auf **Weiter**. In diesem Beispiel wird **WIRELESS** verwendet.



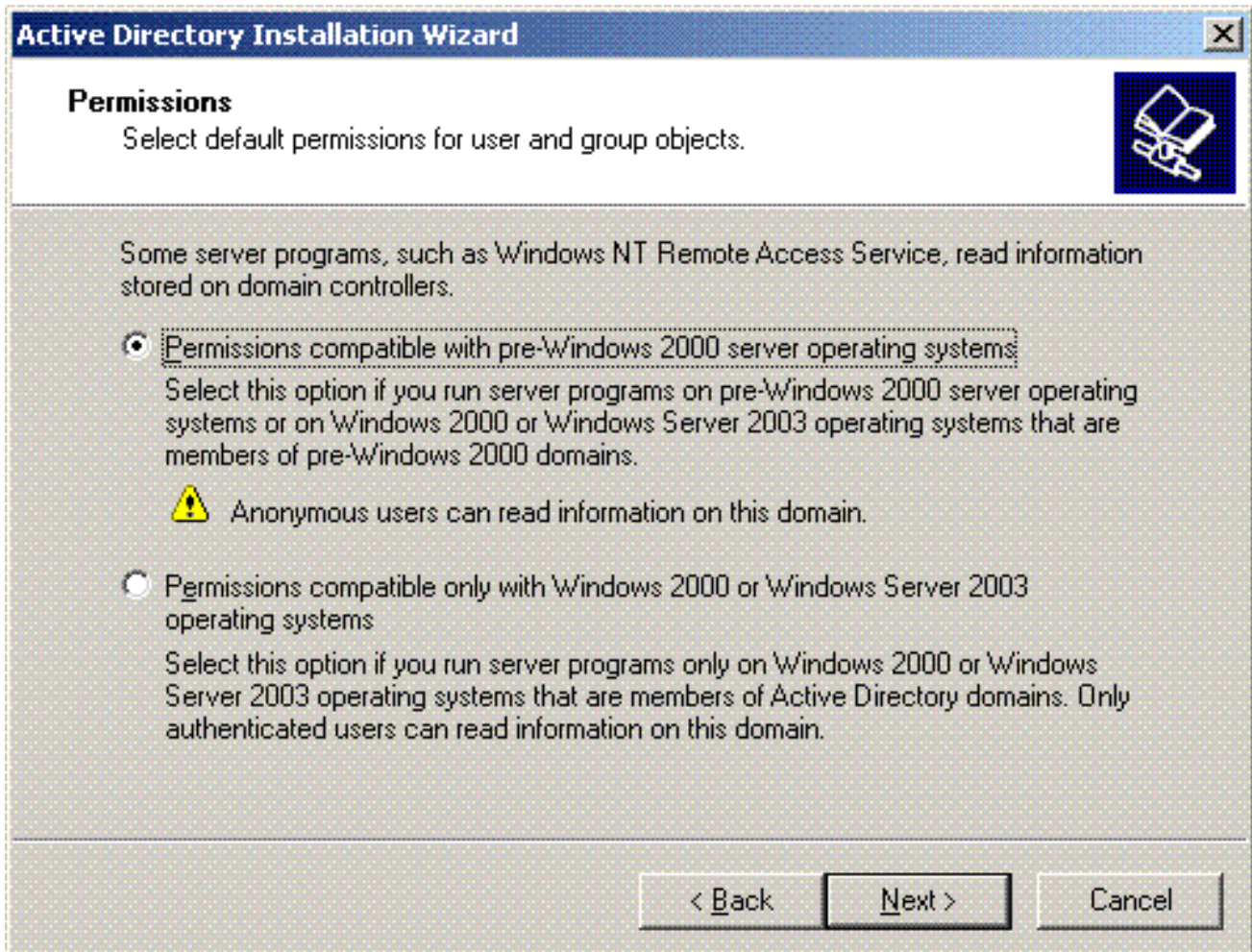
8. Wählen Sie die Datenbank- und Protokollspeicherorte für die Domäne aus. Klicken Sie auf **Next** (Weiter).



9. Wählen Sie einen Speicherort für den Sysvol-Ordner aus. Klicken Sie auf **Next** (Weiter).



10. Wählen Sie die Standardberechtigungen für die Benutzer und Gruppen aus. Klicken Sie auf **Next** (Weiter).



11. Legen Sie das Administratorkennwort fest, und klicken Sie auf **Weiter**.

**Active Directory Installation Wizard**

### Directory Services Restore Mode Administrator Password

This password is used when you start the computer in Directory Services Restore Mode.

Type and confirm the password you want to assign to the Administrator account used when this server is started in Directory Services Restore Mode.

The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both.

Restore Mode Password:

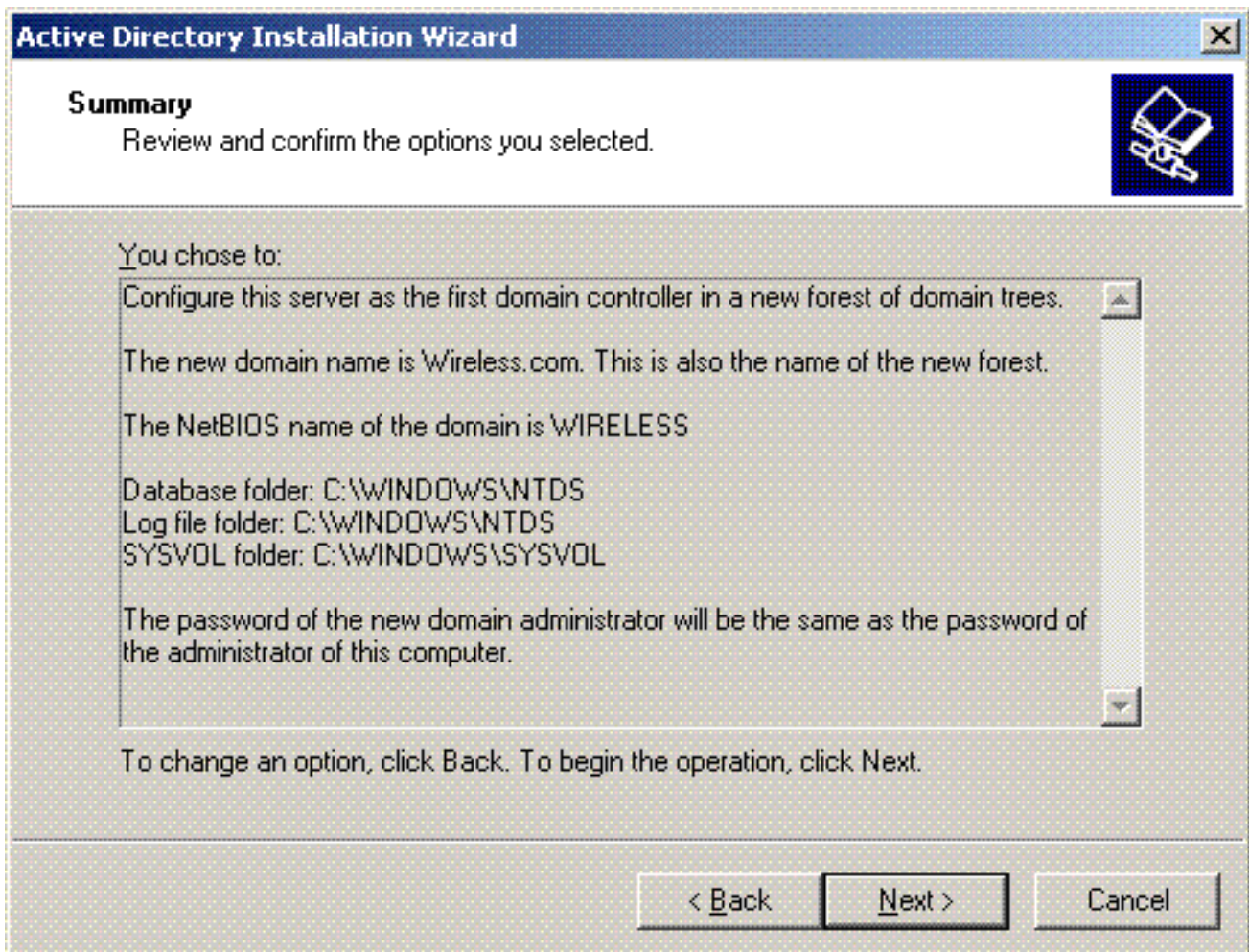
Confirm password:

For more information about Directory Services Restore Mode, see [Active Directory Help](#).

< Back   Next >   Cancel

12. Klicken Sie auf **Weiter**, um die zuvor festgelegten Domänenoptionen zu akzeptieren.

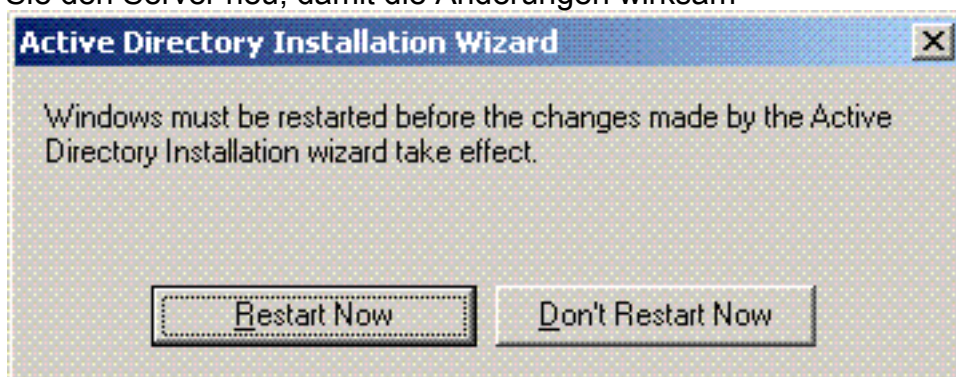




13. Klicken Sie auf **Fertig stellen**, um den Active Directory-Installationsassistenten zu schließen.



14. Starten Sie den Server neu, damit die Änderungen wirksam



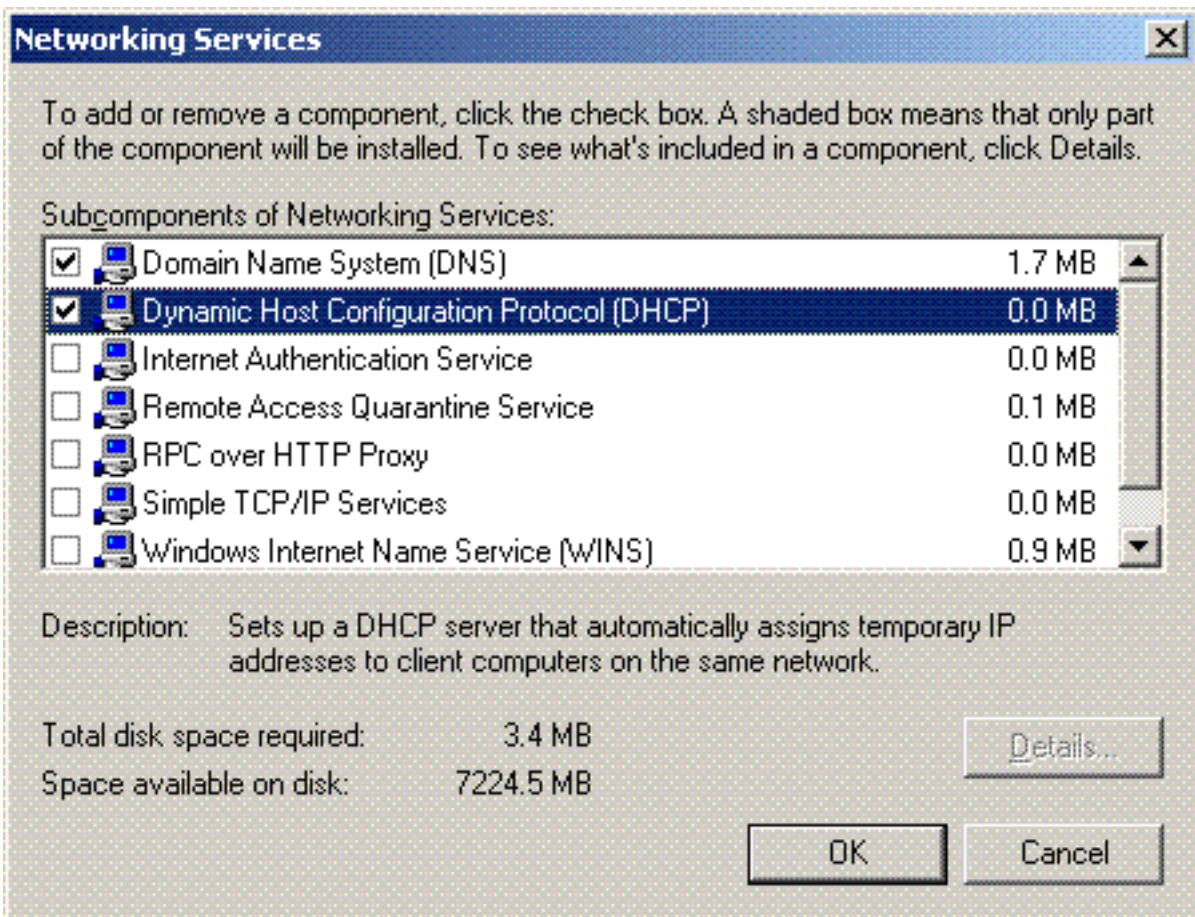
werden.

Mit diesem Schritt haben Sie den Microsoft Windows 2003-Server als Domänencontroller konfiguriert und eine neue Domäne **Wireless.com** erstellt. Konfigurieren Sie anschließend die DHCP-Dienste auf dem Server.

## [Installieren und Konfigurieren der DHCP-Dienste auf dem Microsoft Windows 2003 Server](#)

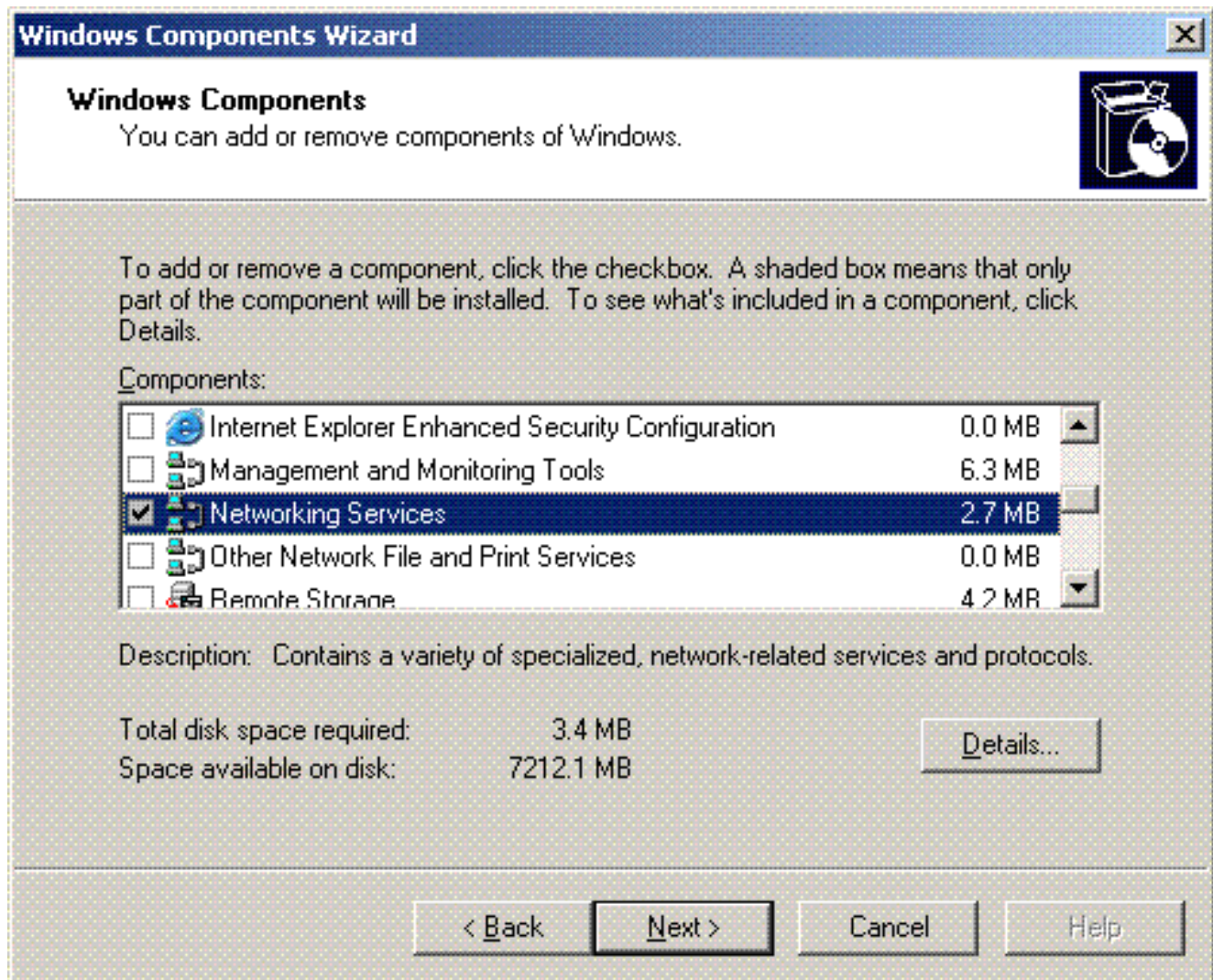
Der DHCP-Dienst auf dem Microsoft 2003-Server wird verwendet, um den Wireless-Clients IP-Adressen bereitzustellen. Führen Sie die folgenden Schritte aus, um DHCP-Dienste auf diesem Server zu installieren und zu konfigurieren:

1. Klicken Sie in der Systemsteuerung auf **Software**.
2. Klicken Sie auf **Windows-Komponenten hinzufügen/entfernen**.
3. Wählen Sie **Netzwerkdienste aus**, und klicken Sie auf **Details**.
4. Wählen Sie **Dynamic Host Configuration Protocol (DHCP) aus**, und klicken Sie auf



OK.

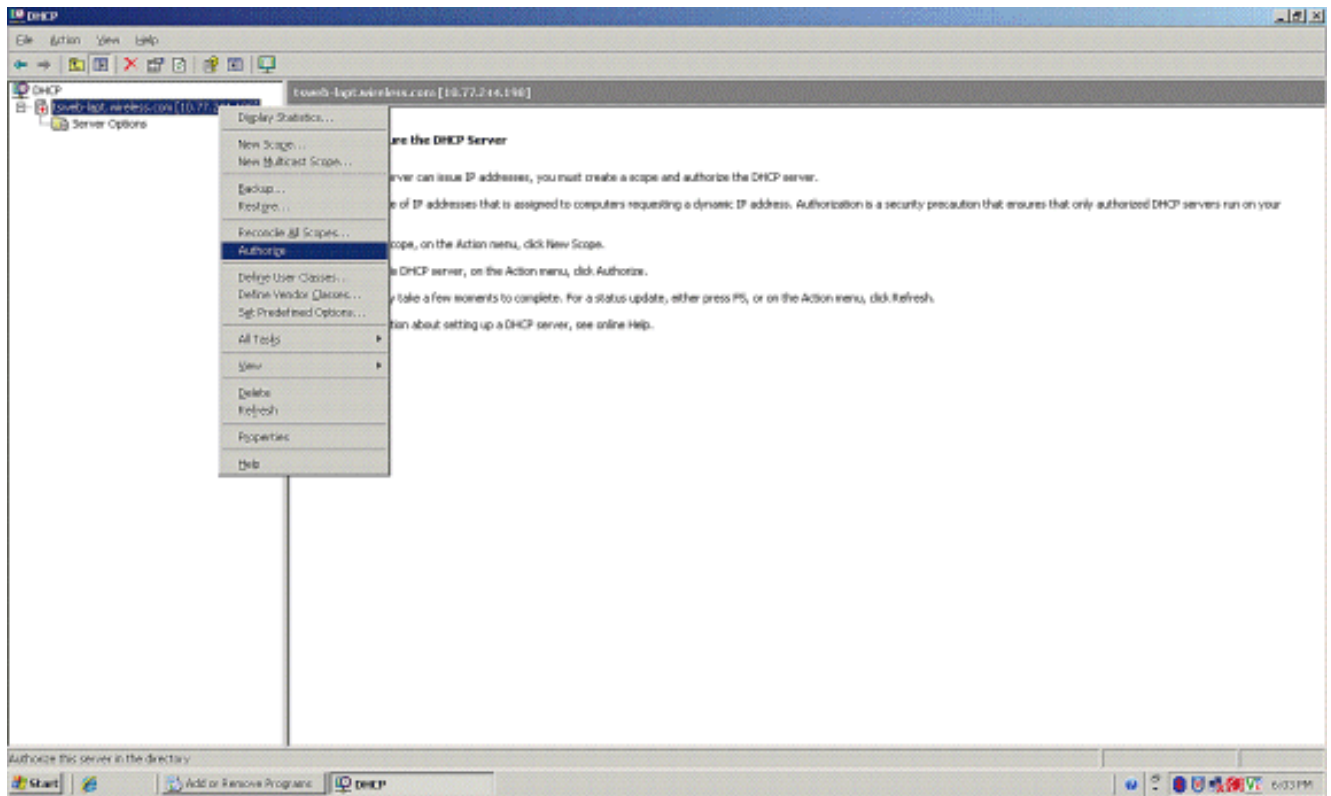
5. Klicken Sie auf **Weiter**, um den DHCP-Dienst zu installieren.



6. Klicken Sie auf **Fertig stellen**, um die Installation abzuschließen.



7. Um DHCP-Dienste zu konfigurieren, klicken Sie auf **Start > Programme > Verwaltung** und dann auf das **DHCP-Snap-In**.
8. Wählen Sie den DHCP-Server - **tsweb-lapt.wireless.com** (in diesem Beispiel).
9. Klicken Sie auf **Aktion** und dann auf **Autorisieren**, um den DHCP-Dienst zu autorisieren.



10. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **tsweb-lapt.wireless.com**, und klicken Sie dann auf **Neuer Bereich**, um einen IP-Adressbereich für die Wireless-Clients zu definieren.
11. Klicken Sie auf der Seite Willkommen des Assistenten für neue Bereiche des Assistenten für neue Bereiche auf **Weiter**.



12. Geben Sie auf der Seite Scope Name (Bereichsname) den Namen des DHCP-Bereichs ein. Verwenden Sie in diesem Beispiel **DHCP-Clients** als Bereichsname. Klicken Sie auf **Next** (Weiter).

**New Scope Wizard**

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

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

Name:

Description:

< Back    Next >    Cancel

13. Geben Sie auf der Seite IP-Adressbereich die Start- und End-IP-Adressen für den Bereich ein, und klicken Sie auf **Weiter**.

## 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: 10 . 77 . 244 . 218

End IP address: 10 . 77 . 244 . 219

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: 8

Subnet mask: 255 . 0 . 0 . 0

< Back

Next >

Cancel

14. Geben Sie auf der Seite "Add Exclusions" (Ausschlüsse hinzufügen) die IP-Adresse an, die Sie im DHCP-Bereich reservieren/ausschließen möchten. Klicken Sie auf **Next** (Weiter).



## 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

15. Geben Sie auf der Seite "Leasingdauer" die Leasingdauer an, 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:
<input type="text" value="8"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

< Back

Next >

Cancel

16. Wählen Sie auf der Seite Configure DHCP options (DHCP-Optionen konfigurieren) die Option **Yes, I want to configure DHCP Option now (Ja, DHCP-Option jetzt konfigurieren)** aus, und klicken Sie auf **Next (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

17. Wenn ein Standard-Gateway-Router vorhanden ist, geben Sie die IP-Adresse des Gateway-Routers auf der Seite Router (Standard-Gateway) an, und klicken Sie auf **Next (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

Remove

Up

Down

< Back

Next >

Cancel

18. Geben Sie auf der Seite Domain Name and DNS servers (Domänenname und DNS-Server) den Namen der zuvor konfigurierten Domäne ein. Verwenden Sie im Beispiel **Wireless.com**. Geben Sie die IP-Adresse des Servers ein. Klicken Sie auf **Hinzufügen**.

## 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

Resolve

10.77.244.217

Remove

Up

Down

< Back

Next >

Cancel

19. Klicken Sie auf **Next** (Weiter).
20. Klicken Sie auf der Seite "WINS-Server" auf **Weiter**.
21. Wählen Sie auf der Seite "Bereich aktivieren" die Option **Ja, ich möchte den Bereich jetzt aktivieren**, und klicken Sie auf **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

< Back

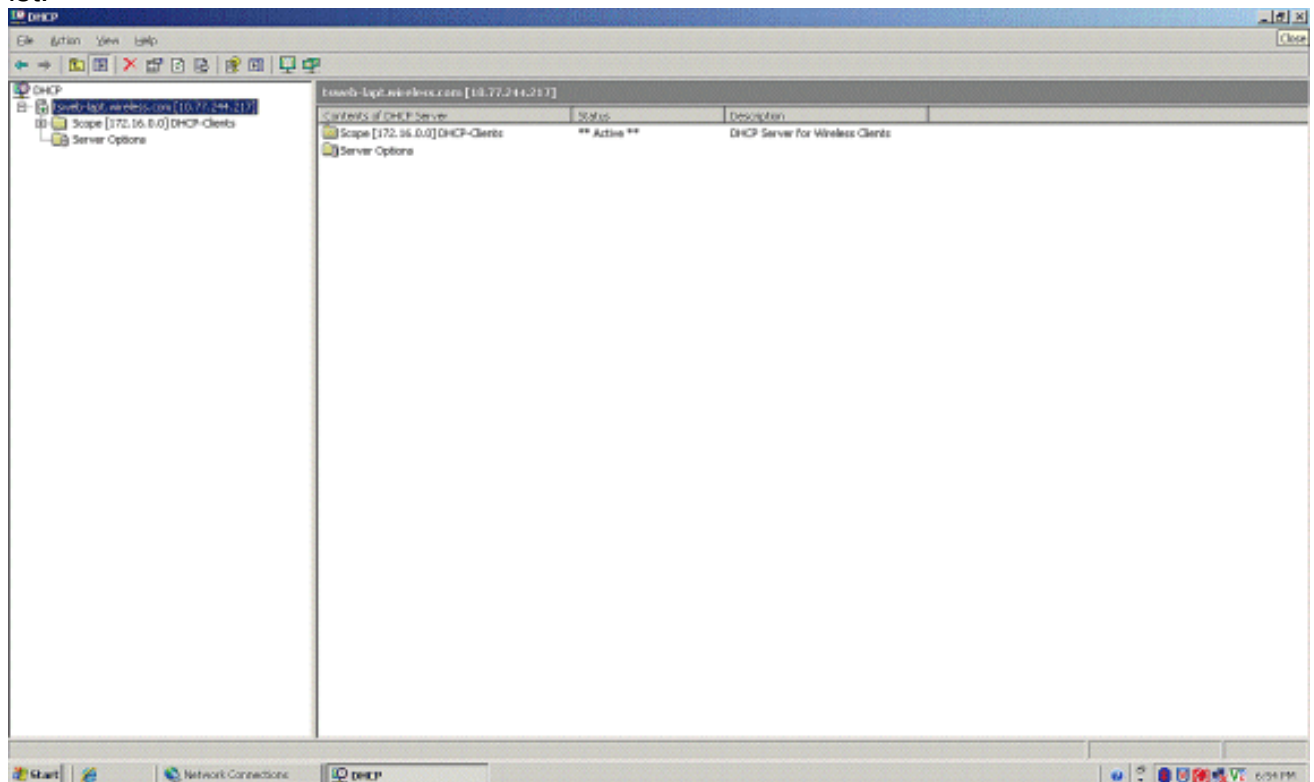
Next >

Cancel

22. Wenn Sie den Assistenten für neue Bereiche abschließen, klicken Sie auf **Fertig stellen**.



23. Überprüfen Sie im Fenster DHCP-Snapin (DHCP-Snapin), ob der erstellte DHCP-Bereich aktiv ist.



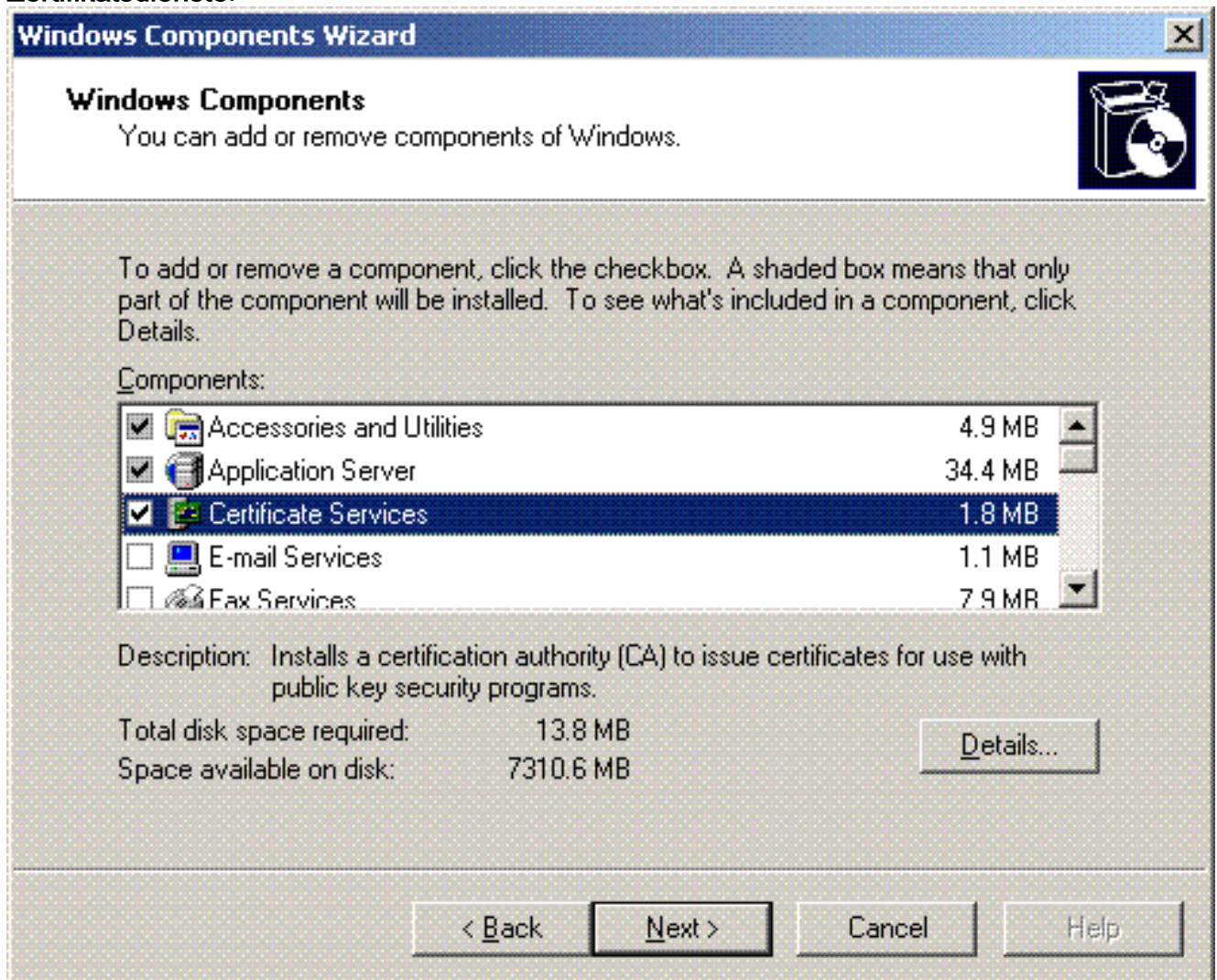
Nachdem DHCP/DNS auf dem Server aktiviert wurde, konfigurieren Sie den Server als CA-Server (Enterprise Certificate Authority).

## Installieren und Konfigurieren von Microsoft Windows 2003 Server als CA-Server (Certificate Authority)

PEAP mit EAP-MS-CHAPv2 validiert den RADIUS-Server anhand des auf dem Server vorhandenen Zertifikats. Darüber hinaus muss das Serverzertifikat von einer öffentlichen Zertifizierungsstelle ausgestellt werden, der der Clientcomputer vertraut (d. h. das öffentliche Zertifizierungsstellenzertifikat ist bereits im Ordner der vertrauenswürdigen Stammzertifizierungsstelle im Zertifikatspeicher des Clientcomputers vorhanden). Konfigurieren Sie in diesem Beispiel den Microsoft Windows 2003-Server als Zertifizierungsstelle, die das Zertifikat an den Internetauthentifizierungsdienst (IAS) ausstellt.

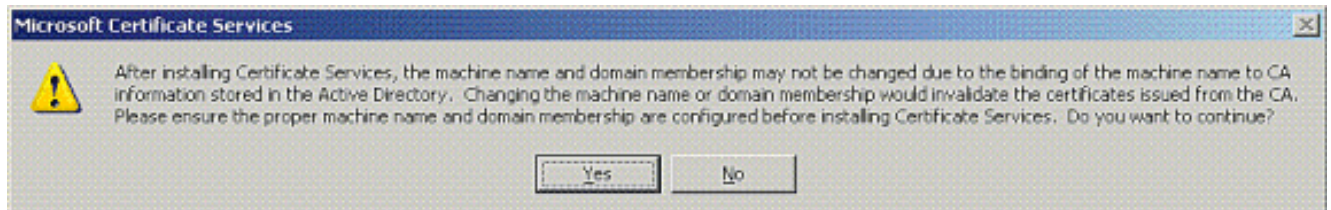
Führen Sie die folgenden Schritte aus, um die Zertifikatdienste auf dem Server zu installieren und zu konfigurieren:

1. Klicken Sie in der Systemsteuerung auf **Programme hinzufügen oder entfernen**.
2. Klicken Sie auf **Windows-Komponenten hinzufügen/entfernen**.
3. Klicken Sie auf **Zertifikatsdienste**.

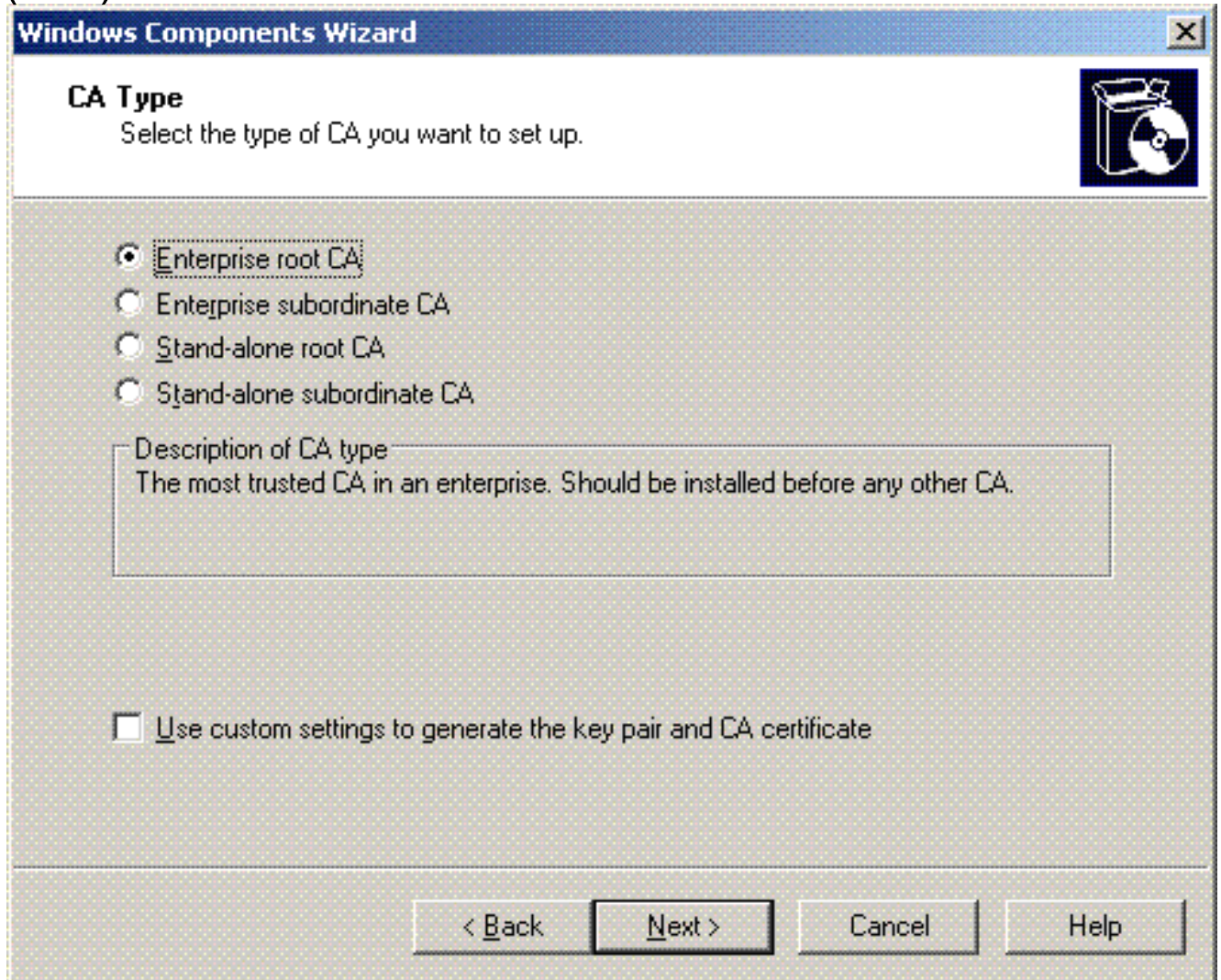


4. Klicken Sie auf **Ja**, um die Warnmeldung anzuzeigen. **Nach der Installation der Zertifikatsdienste kann der Computer nicht umbenannt werden, und der Computer kann einer Domäne nicht beitreten oder daraus entfernt werden. Möchten Sie fortfahren?**






5. Wählen Sie unter Certificate Authority Type (Zertifizierungsstellentyp) die Option **Enterprise root CA** aus, und klicken Sie auf **Next** (Weiter).



6. Geben Sie einen Namen zur Identifizierung der Zertifizierungsstelle ein. In diesem Beispiel wird **Wireless-CA** verwendet. Klicken Sie auf **Next** (Weiter).

**Windows Components Wizard** X

**CA Identifying Information**   
Enter information to identify this CA.

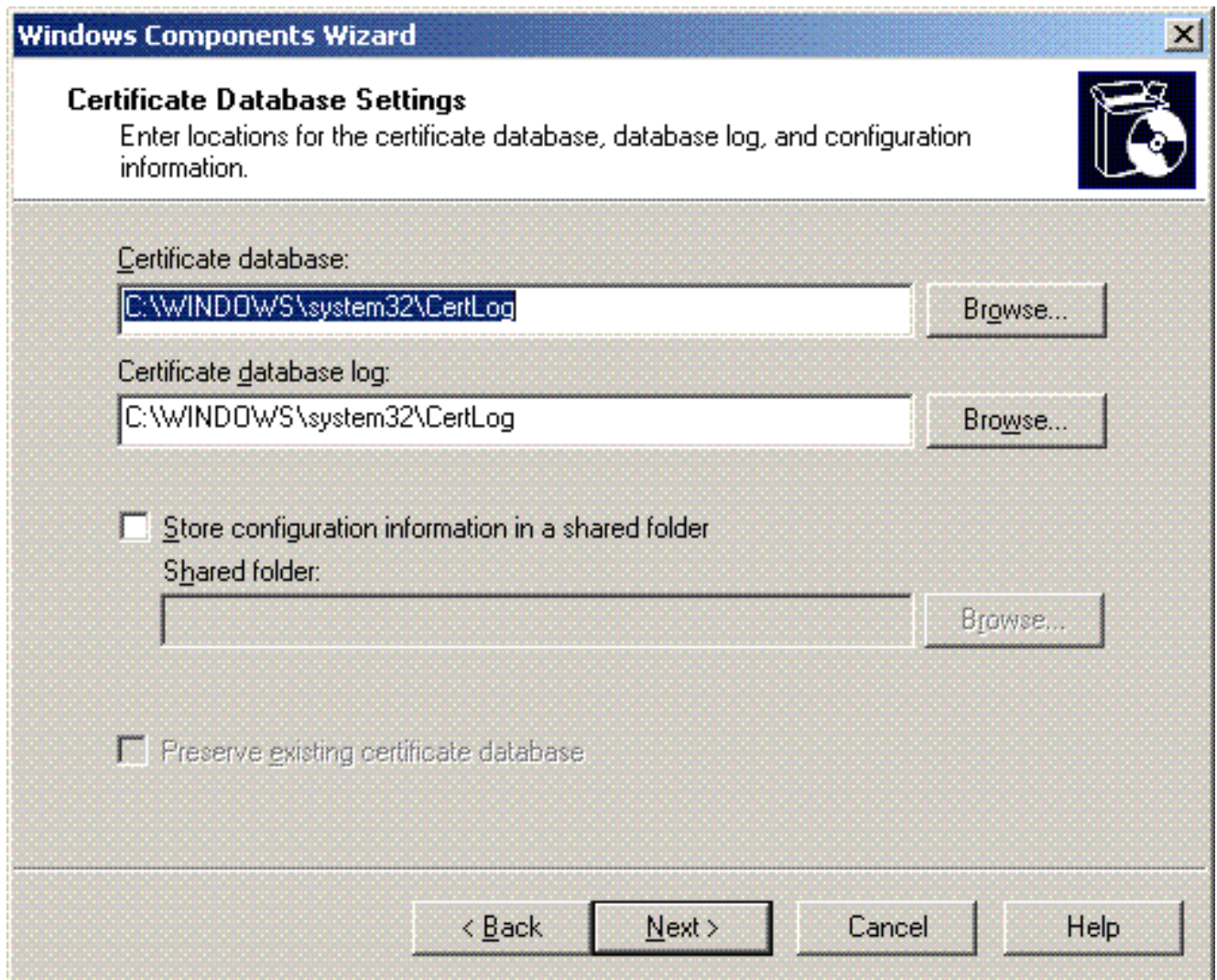
Common name for this CA:

Distinguished name suffix:

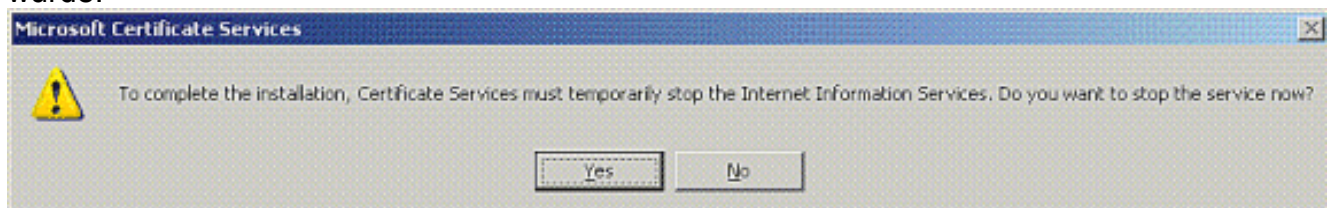
Preview of distinguished name:

Validity period:     
Expiration date: 12/12/2012 7:01 PM

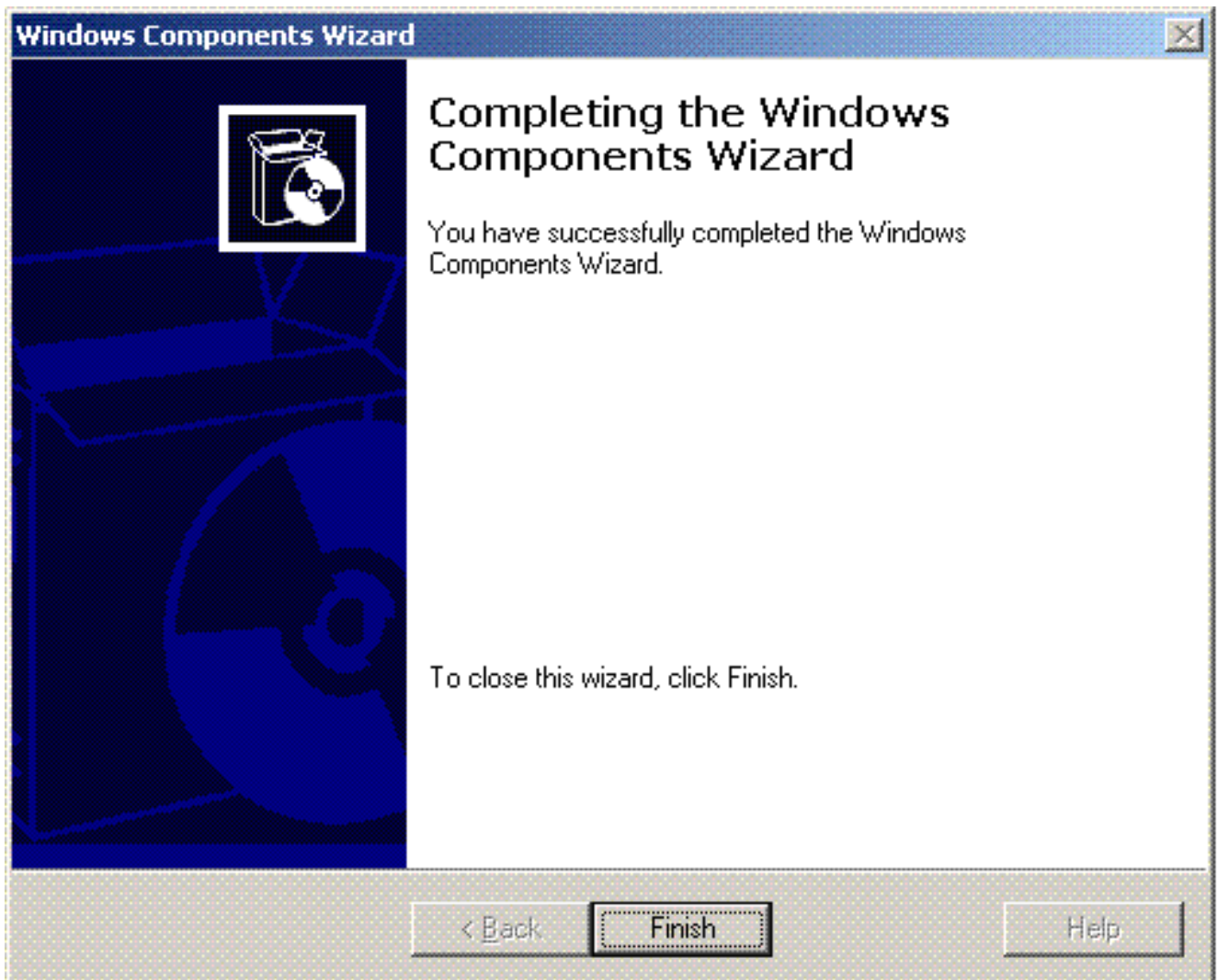
7. Für die Zertifikatdatenbankspeicherung wird ein Verzeichnis "Zertifikatprotokoll" erstellt.  
Klicken Sie auf **Next**  
(Weiter).



8. Wenn IIS aktiviert ist, muss es beendet werden, bevor Sie fortfahren. Klicken Sie auf **OK**, um die Warnmeldung anzuzeigen, dass IIS beendet werden muss. Er wird automatisch neu gestartet, nachdem die Zertifizierungsstelle installiert wurde.



9. Klicken Sie auf **Fertig stellen**, um die Installation der Zertifizierungsstellen-Services abzuschließen.

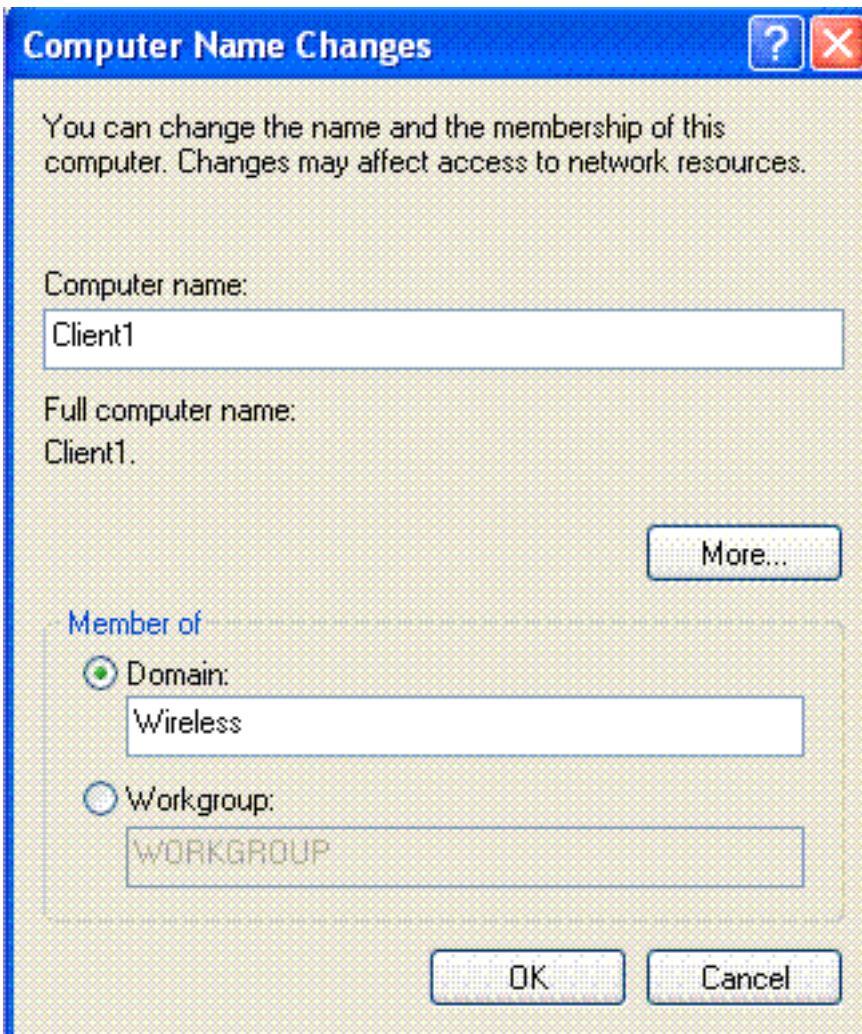


Der nächste Schritt besteht darin, den Internetauthentifizierungsdienst auf dem Microsoft Windows 2003-Server zu installieren und zu konfigurieren.

### [Clients mit der Domäne verbinden](#)

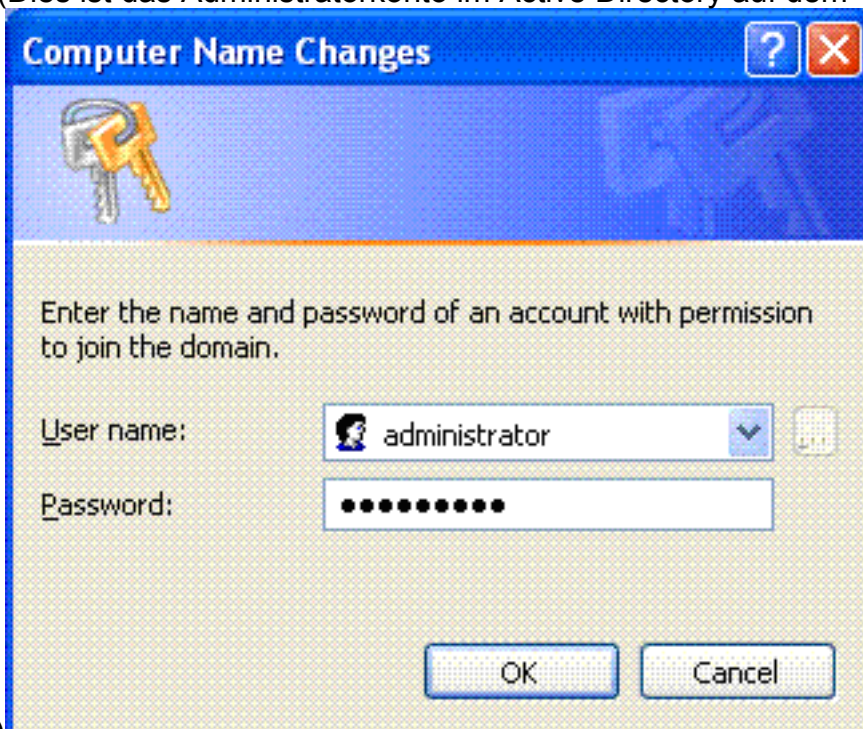
Der nächste Schritt besteht darin, die Clients mit dem kabelgebundenen Netzwerk zu verbinden und die domänenspezifischen Informationen aus der neuen Domäne herunterzuladen. Mit anderen Worten: Verbinden Sie die Clients mit der Domäne. Führen Sie hierzu die folgenden Schritte aus:

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/Kennwort des Clients an.
3. Klicken Sie auf **Start**, klicken Sie auf **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 der Client eine IP-Adresse vom DHCP-Server erhalten hat.
5. Um den Client mit der Domäne zu verbinden, klicken Sie mit der rechten Maustaste auf **Arbeitsplatz**, und wählen Sie **Eigenschaften**.
6. Klicken Sie auf die Registerkarte **Computername**.
7. Klicken Sie auf **Ändern**.
8. Klicken Sie auf **Domäne**, geben Sie **wireless.com ein**, und klicken Sie auf



OK.

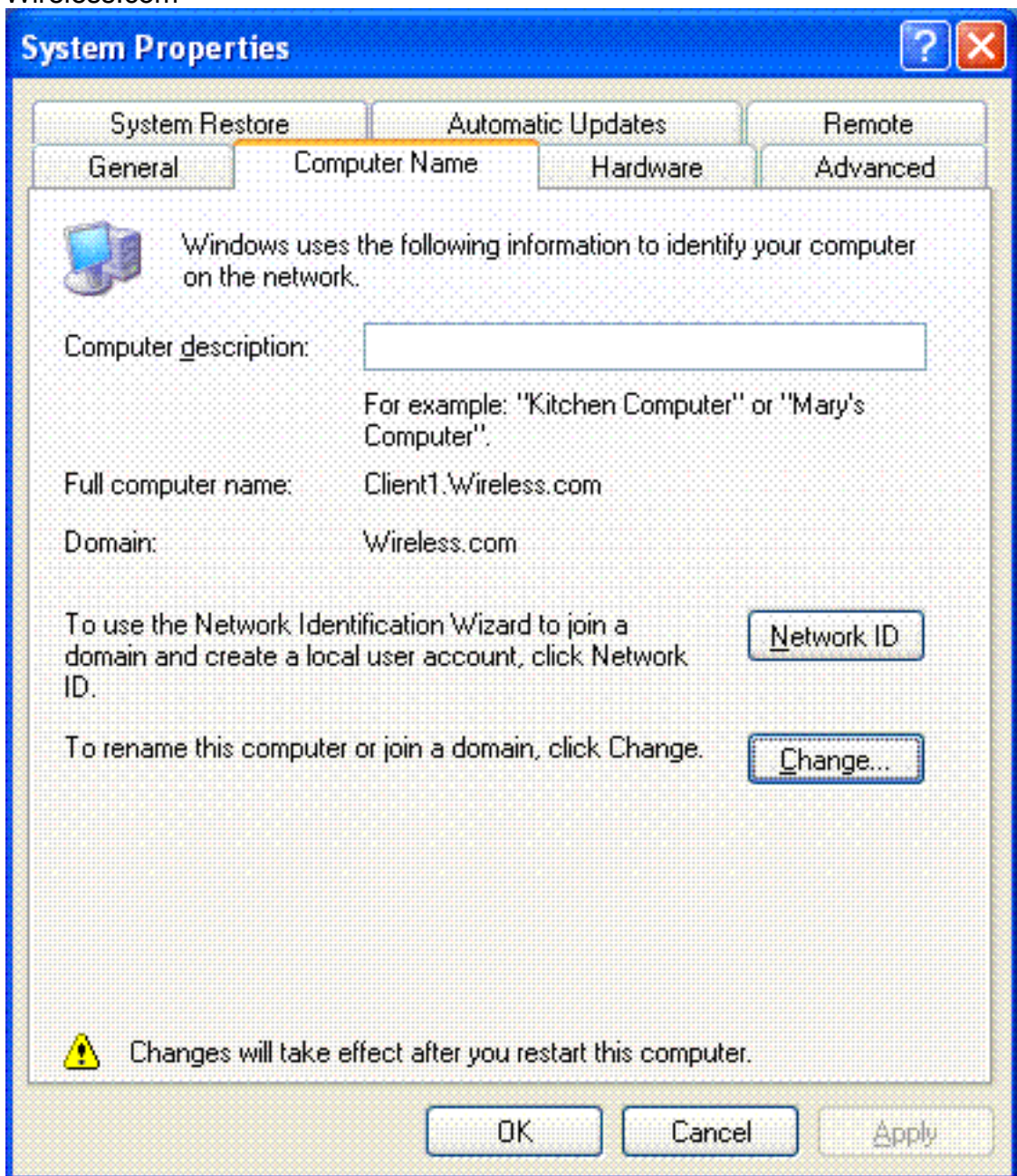
9. Geben Sie **Username Administrator** und das Kennwort für die Domäne ein, der der Client beitrifft. (Dies ist das Administratorkonto im Active Directory auf dem



Server.)



10. Klicken Sie auf **OK**.
11. Klicken Sie auf **Ja**, um den Computer neu zu starten.
12. Melden Sie sich nach dem Neustart des Computers mit folgenden Informationen an:  
Benutzername = **Administrator**; Kennwort = **<Domänenkennwort>**; Domäne = **Wireless**.
13. Klicken Sie mit der rechten Maustaste auf **Arbeitsplatz**, und klicken Sie auf **Eigenschaften**.
14. Klicken Sie auf die Registerkarte **Computername**, um sicherzustellen, dass Sie sich in der Domäne Wireless.com

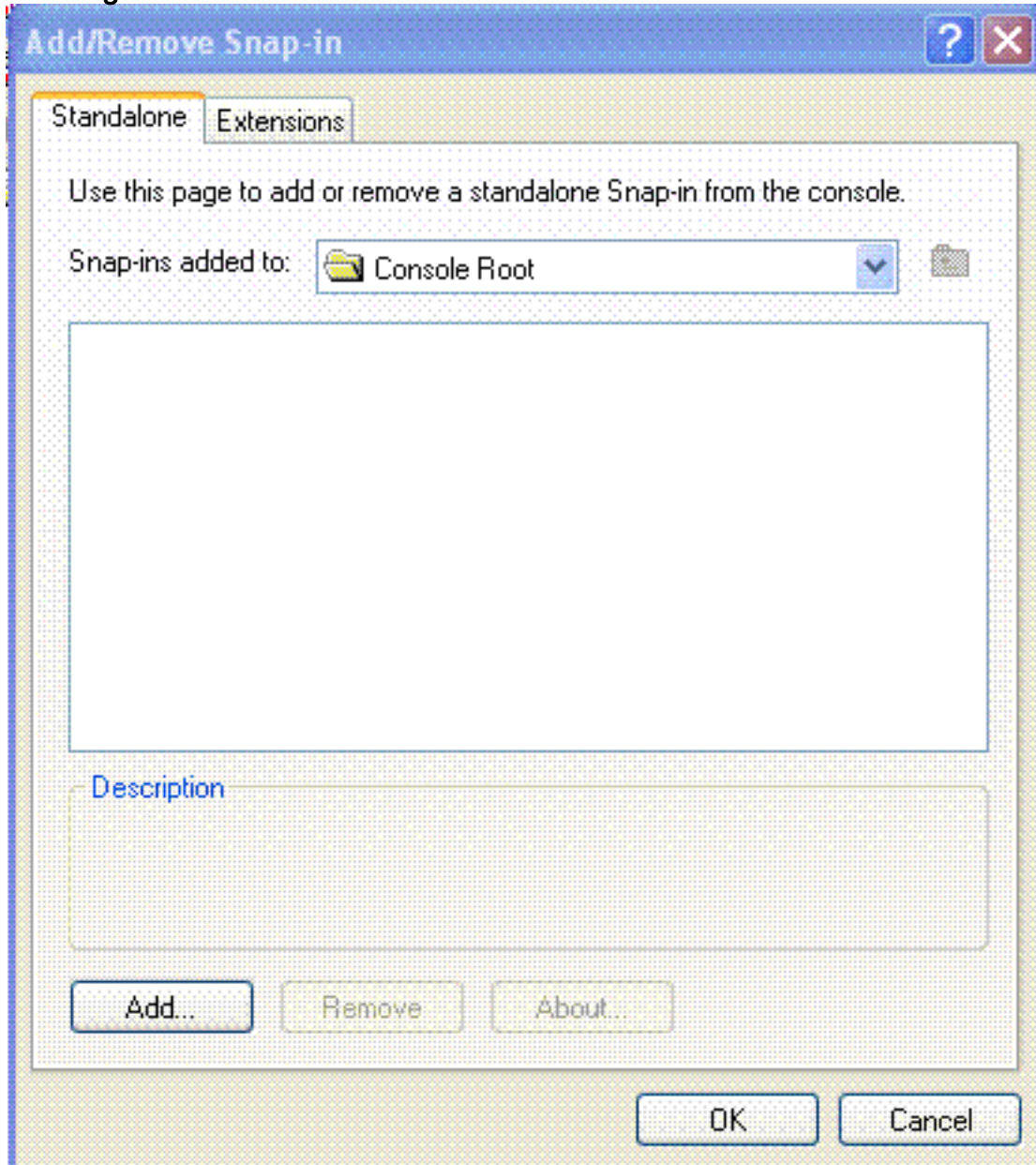


befinden.

15. Der nächste Schritt besteht darin, zu überprüfen, ob der Client das Zertifizierungsstellenzertifikat (trust) vom Server erhalten hat.
16. Klicken Sie auf **Start**, klicken Sie auf **Ausführen**, geben Sie **mmc ein**, und klicken Sie auf

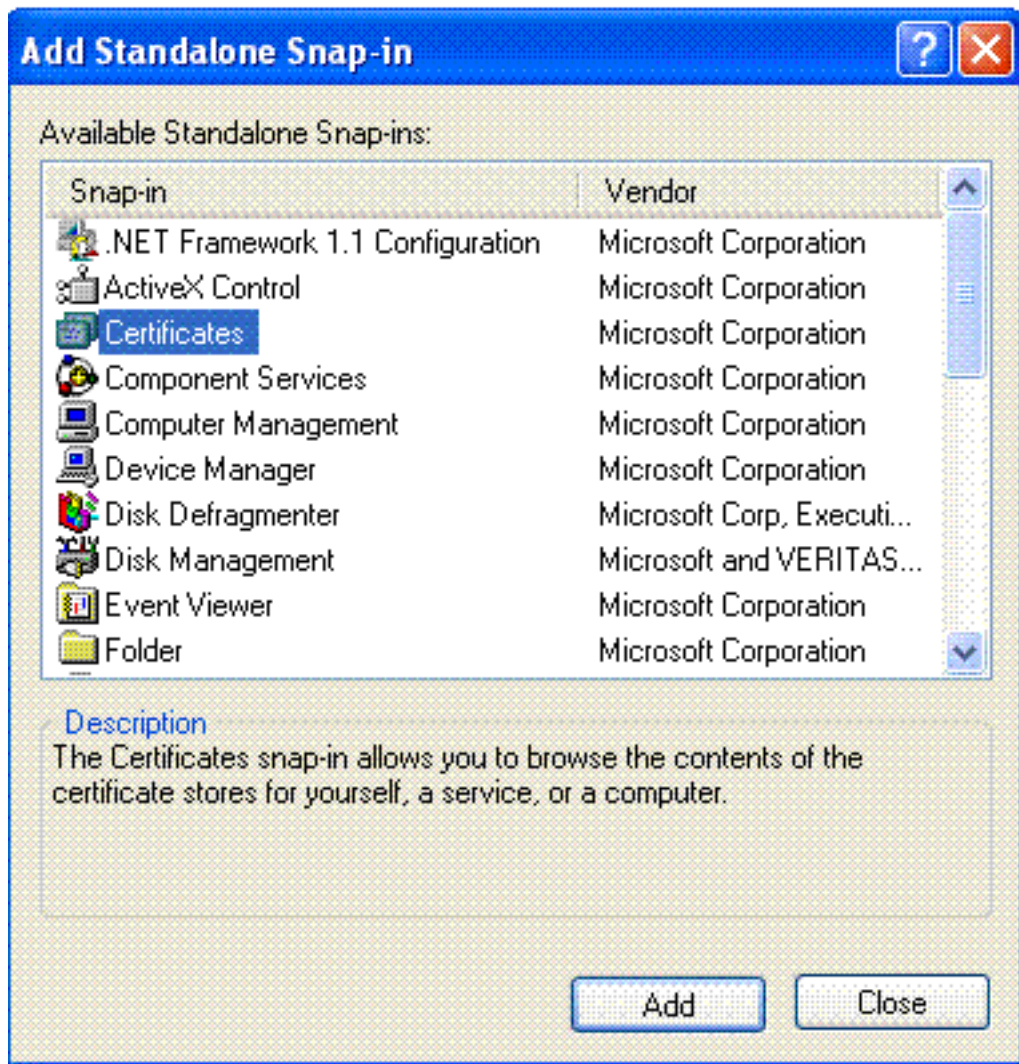
OK.

17. Klicken Sie auf **Datei**, und klicken Sie auf Snap-In hinzufügen/entfernen.



18. Klicken Sie auf **Hinzufügen**.

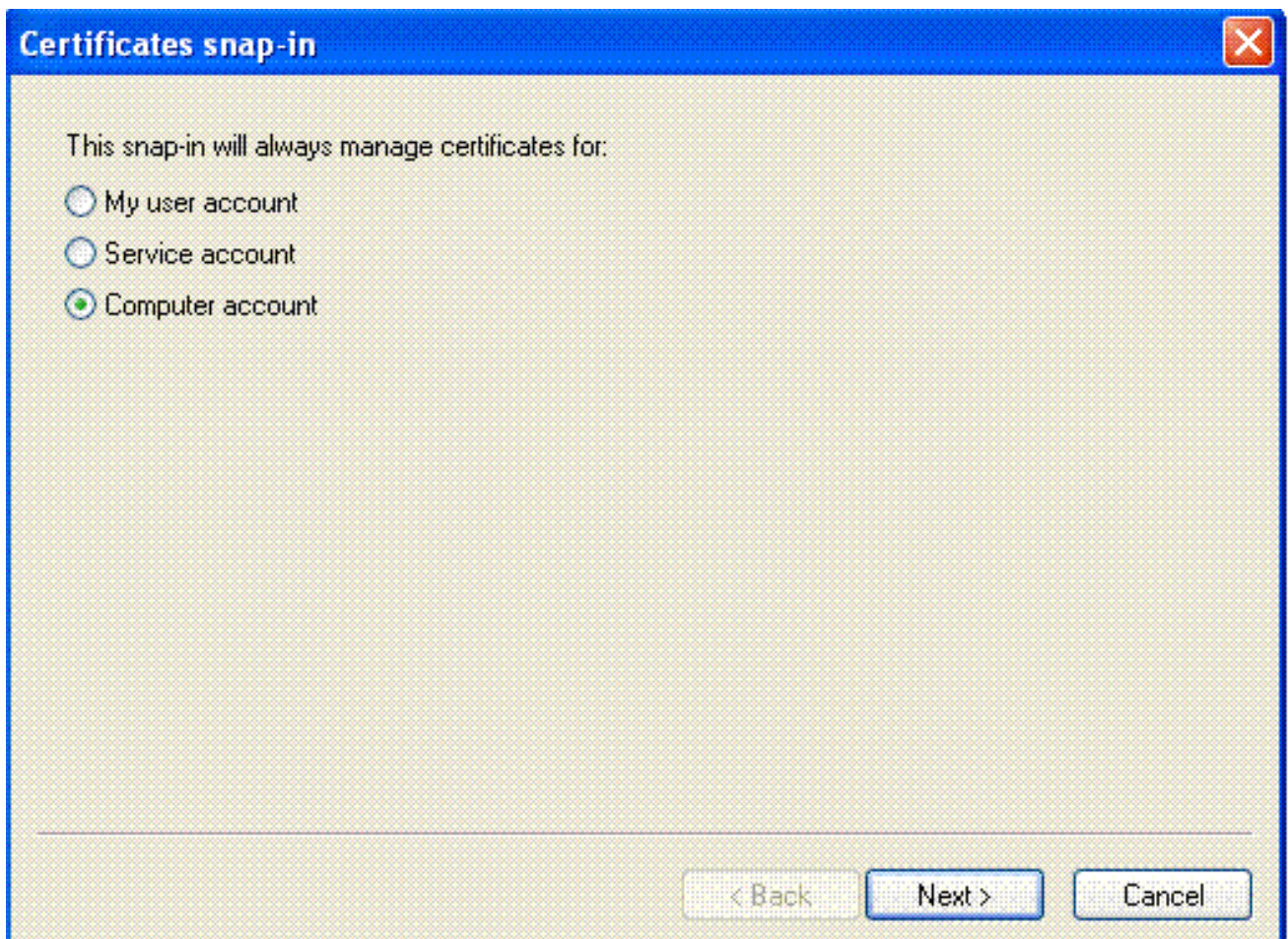
19. Wählen Sie **Zertifikat aus**, und klicken Sie auf



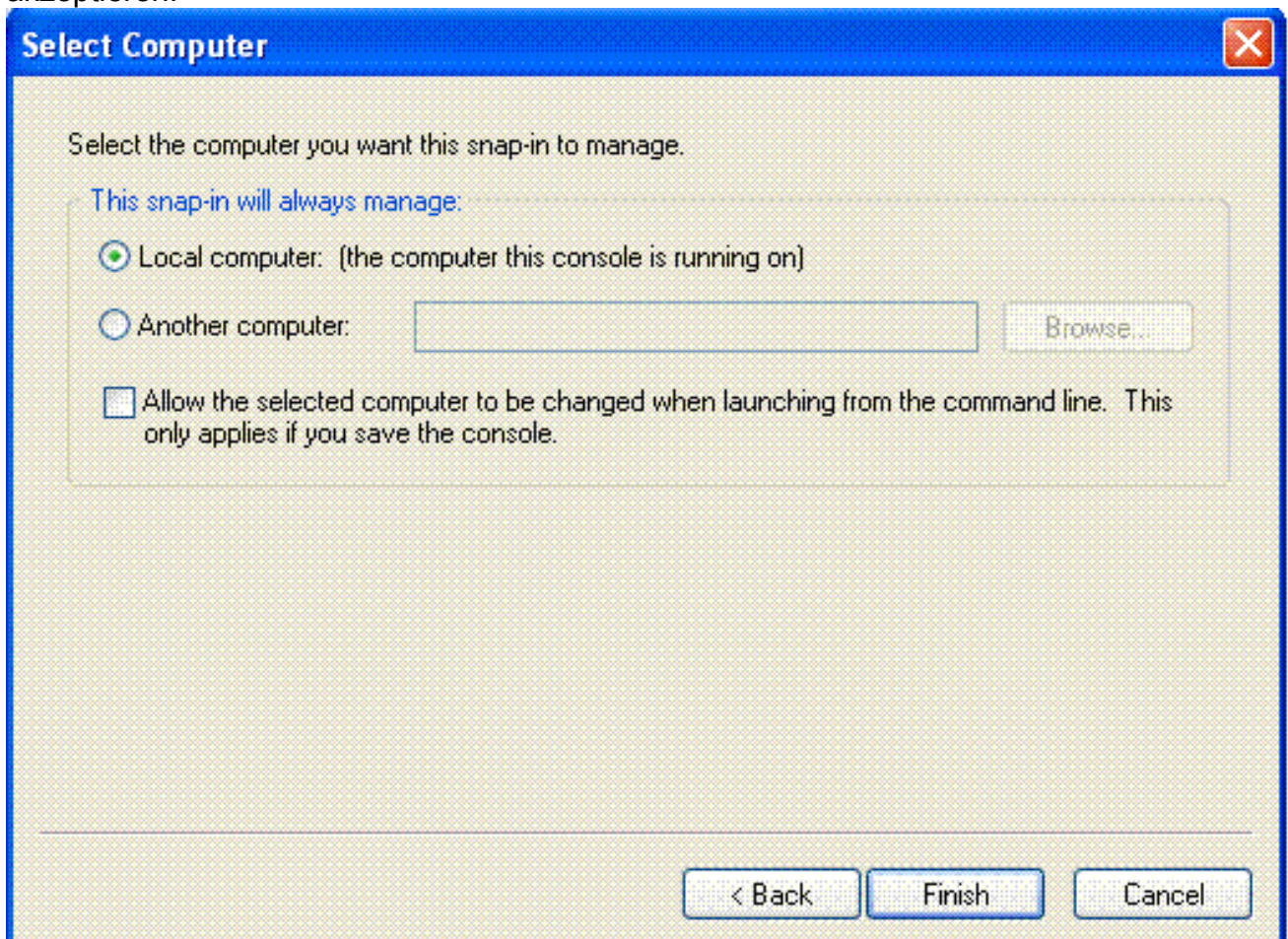
**Hinzufügen.**

20. Wählen Sie **Computerkonto aus**, und klicken Sie auf **Weiter**.



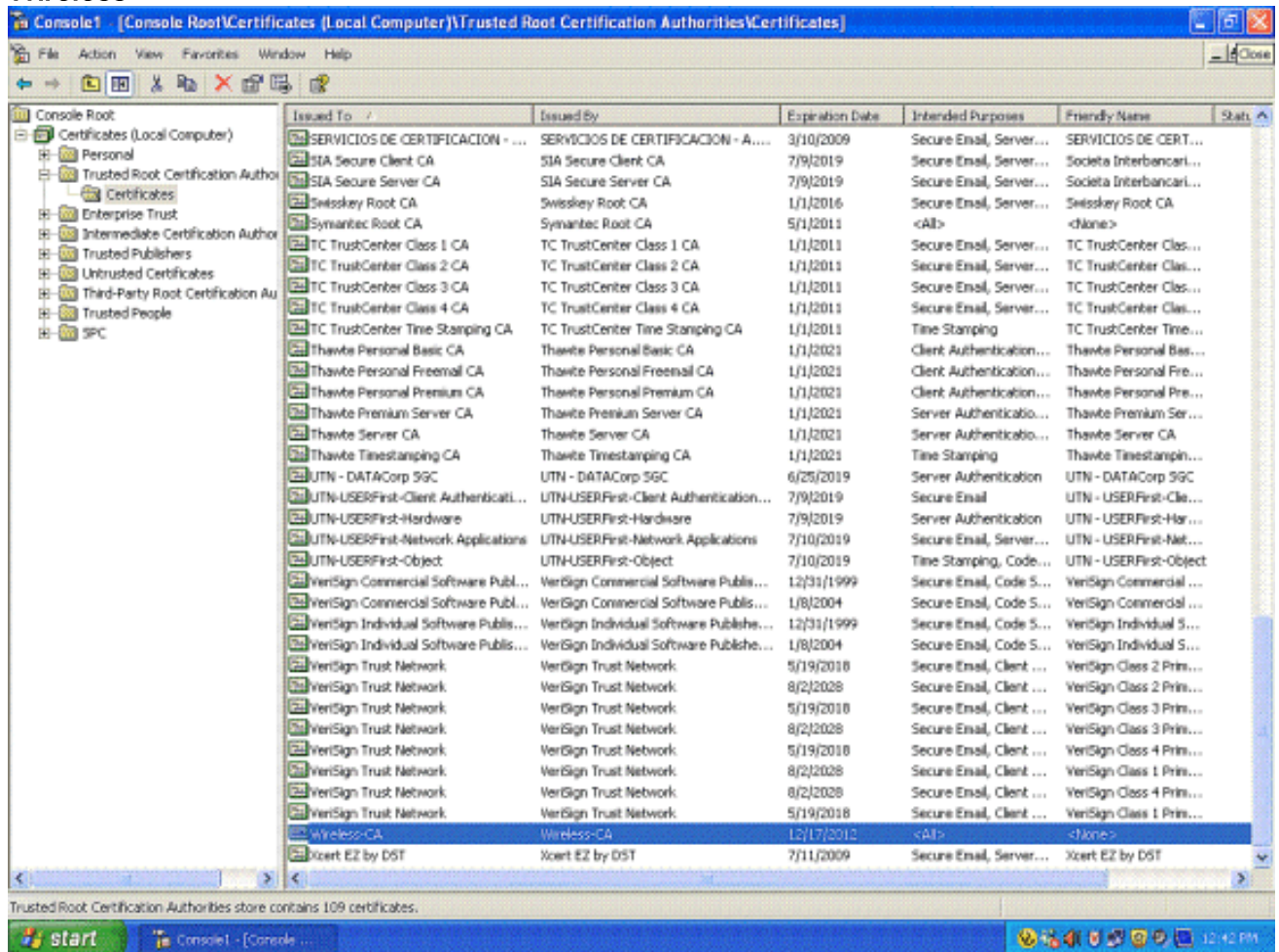


21. Klicken Sie auf **Fertig stellen**, um den lokalen Standardcomputer zu akzeptieren.



22. Klicken Sie auf **Schließen** und dann auf **OK**.

23. Erweitern Sie **Zertifikate (Lokaler Computer)**, erweitern Sie **Vertrauenswürdige Stammzertifizierungsstellen**, und klicken Sie auf **Zertifikate**. Suchen Sie in der Liste nach **Wireless**.



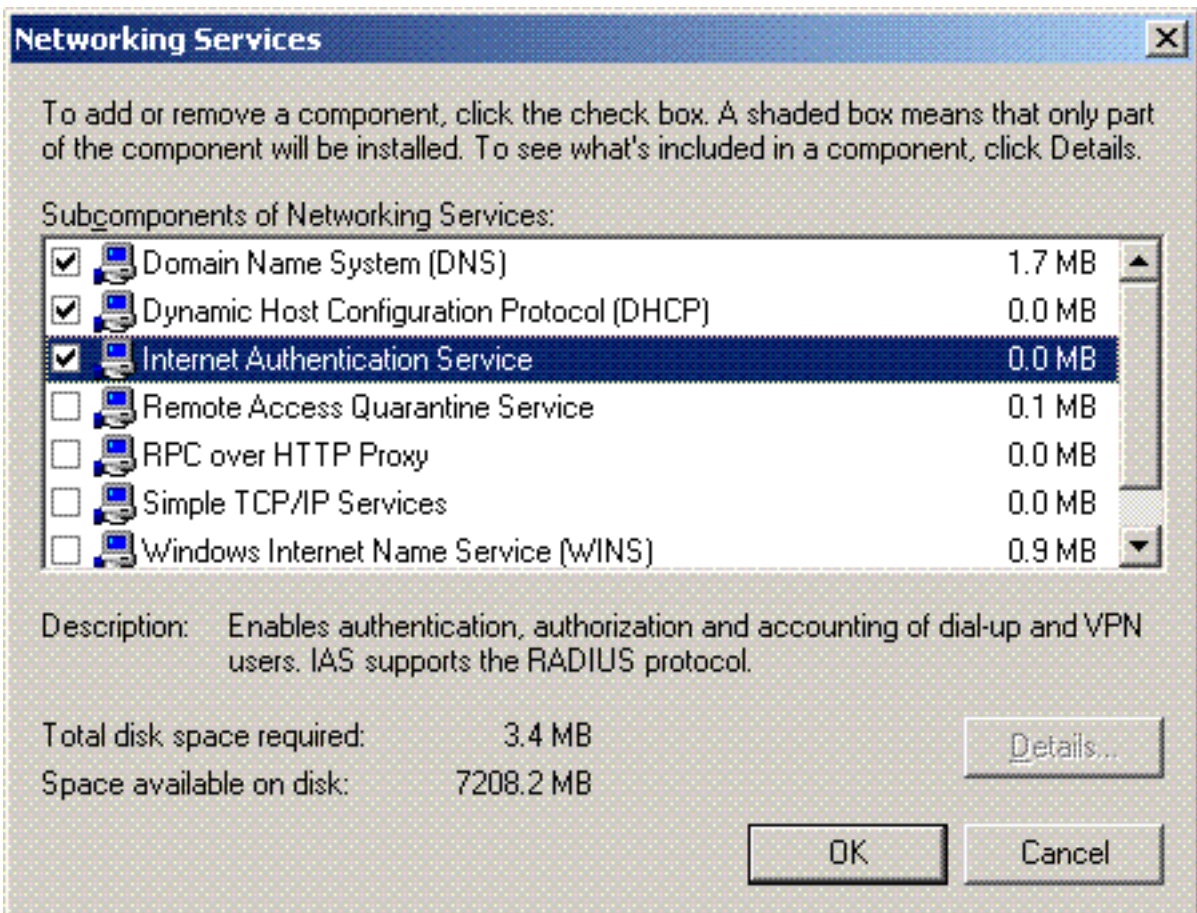
24. Wiederholen Sie dieses Verfahren, um der Domäne weitere Clients hinzuzufügen.

## [Installieren des Internetauthentifizierungsdiensts auf dem Microsoft Windows 2003-Server und Anfordern eines Zertifikats](#)

In dieser Konfiguration wird der Internetauthentifizierungsdienst (Internet Authentication Service, IAS) als RADIUS-Server zur Authentifizierung von Wireless-Clients mit PEAP-Authentifizierung verwendet.

Führen Sie diese Schritte aus, um IAS auf dem Server zu installieren und zu konfigurieren.

1. Klicken Sie in der Systemsteuerung auf **Software**.
2. Klicken Sie auf **Windows-Komponenten hinzufügen/entfernen**.
3. Wählen Sie **Networking Services** aus, und klicken Sie auf **Details**.
4. Wählen Sie **Internetauthentifizierungsdienst** aus, klicken Sie auf **OK**, und klicken Sie auf



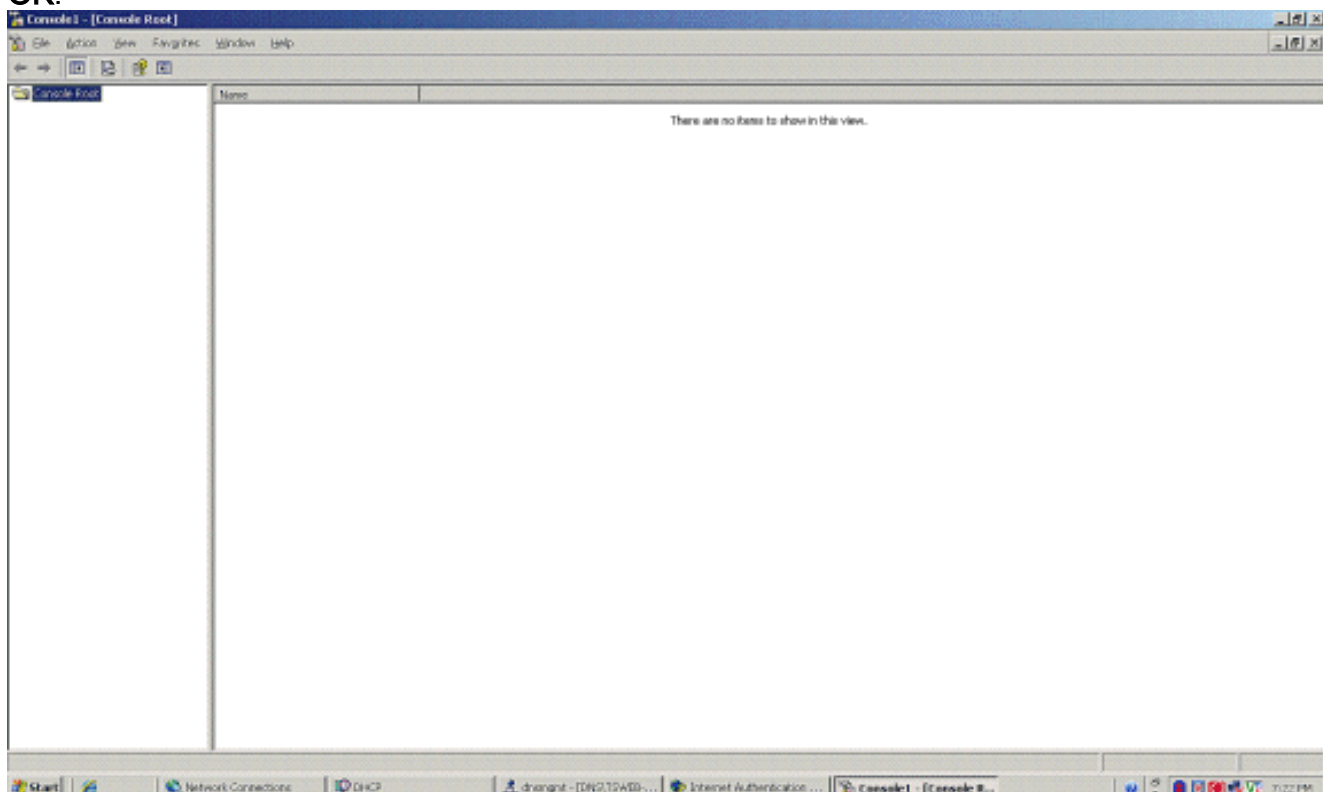
Weiter.

5. Klicken Sie auf **Fertig stellen**, um die IAS-Installation abzuschließen.

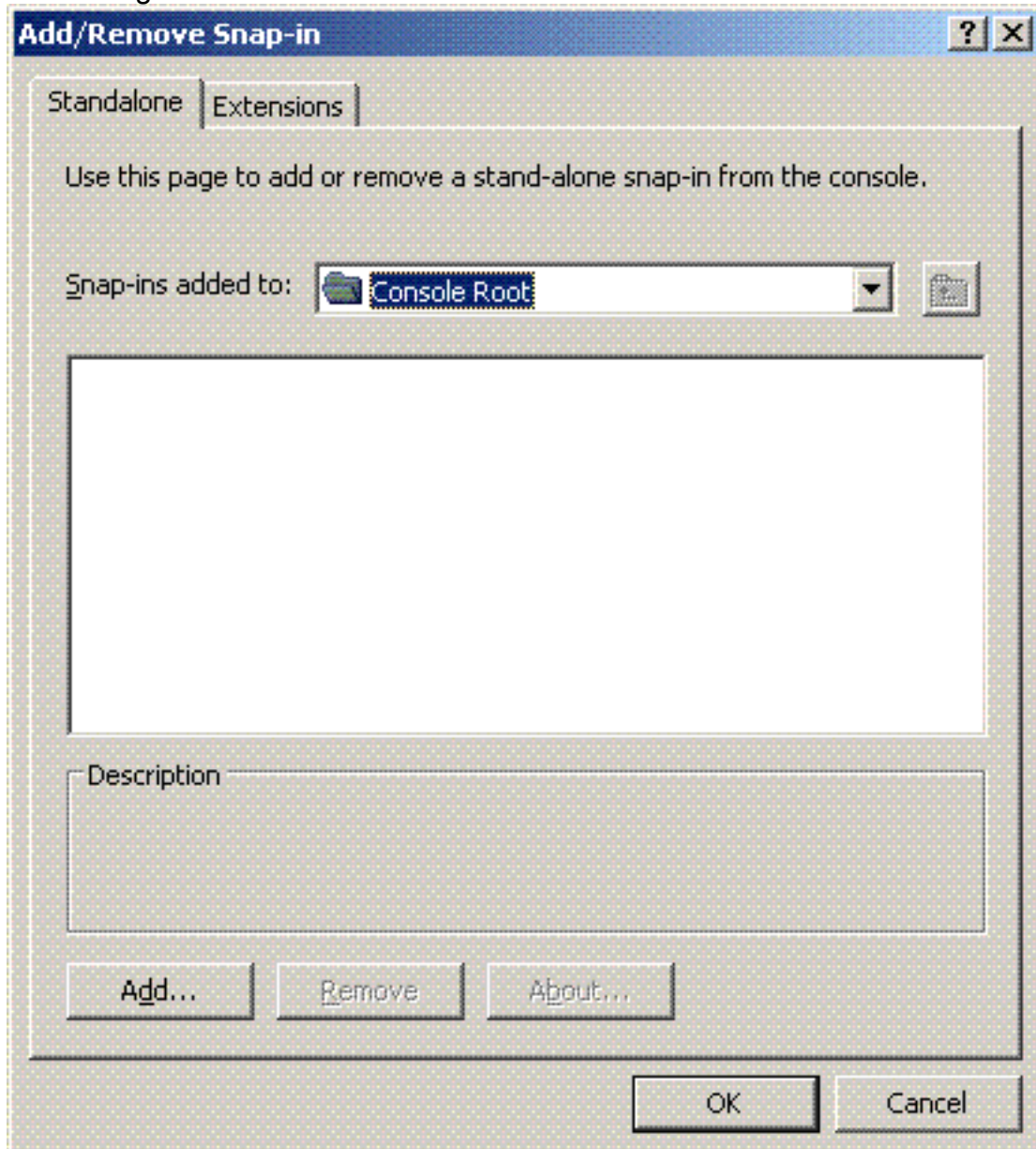


6. Der nächste Schritt ist die Installation des Computerzertifikats für den Internetauthentifizierungsdienst (IAS).

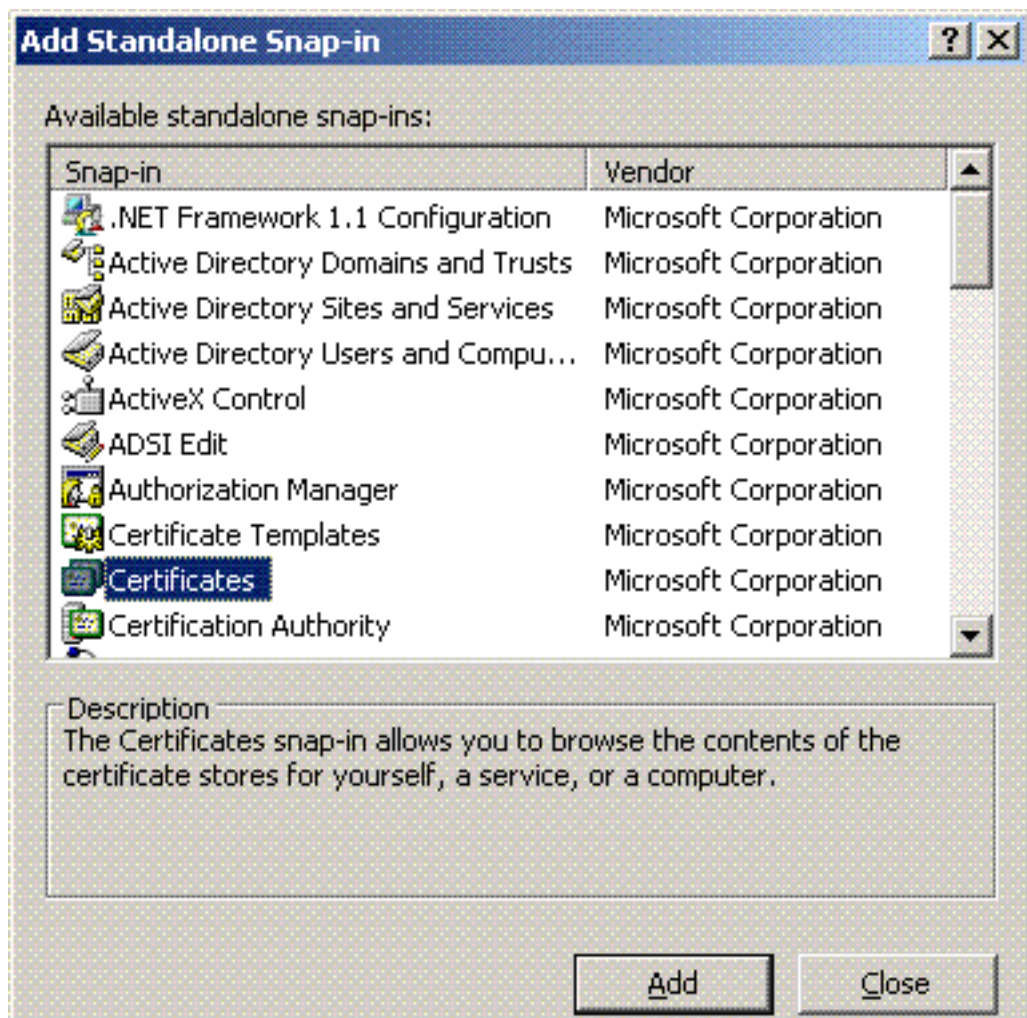
7. Klicken Sie auf **Start**, klicken Sie auf **Ausführen**, geben Sie **mmc ein**, und klicken Sie auf **OK**.



8. Klicken Sie im Dateimenü auf **Konsole**, und wählen Sie dann Snap-In **hinzufügen/entfernen**.
9. Klicken Sie auf **Hinzufügen**, um ein Snap-In hinzuzufügen.

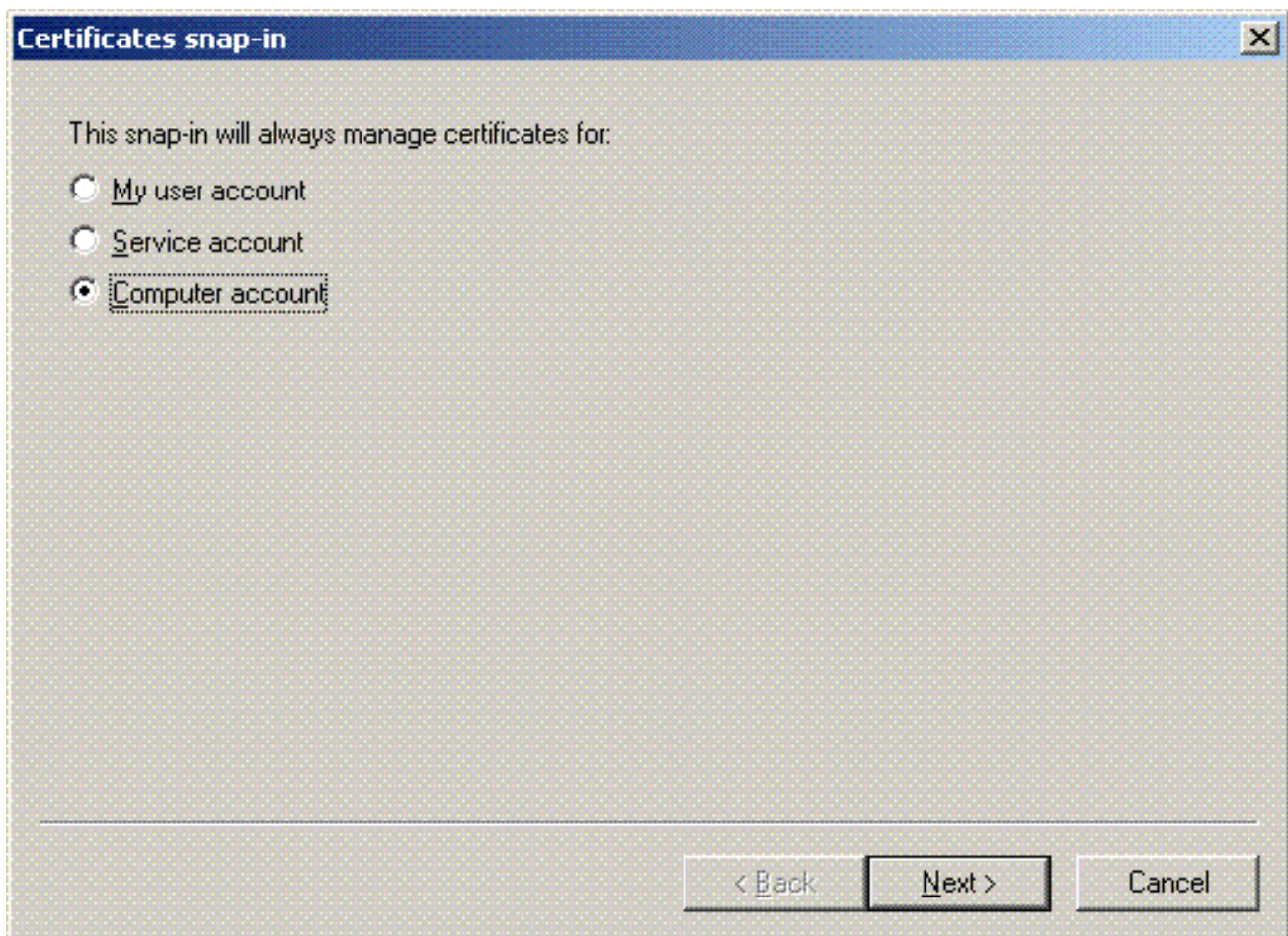


10. Wählen Sie **Zertifikate** aus der Liste der Snap-Ins aus, und klicken Sie auf

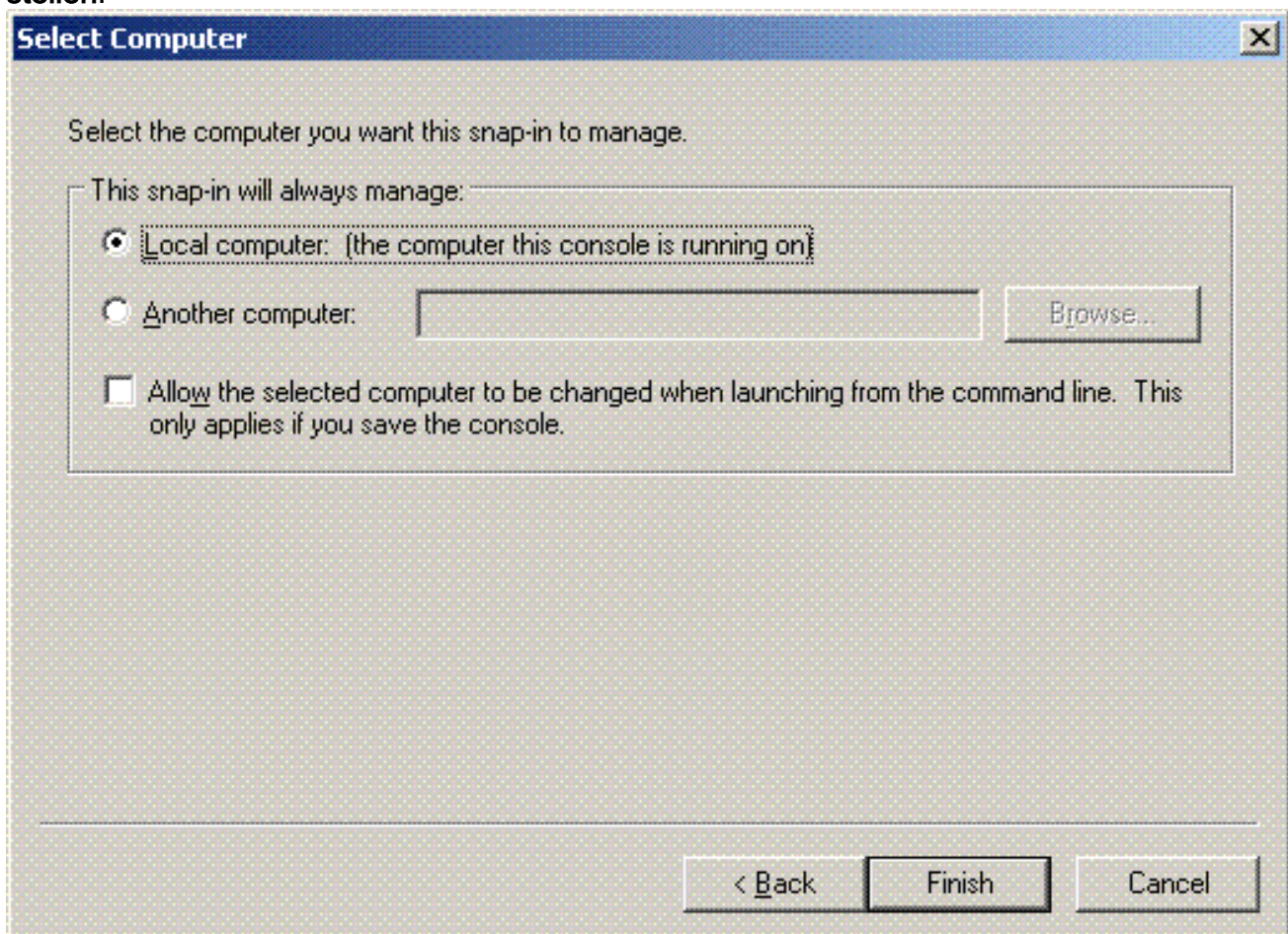


**Hinzufügen.**

11. Wählen Sie **Computerkonto aus**, und klicken Sie auf **Weiter**.

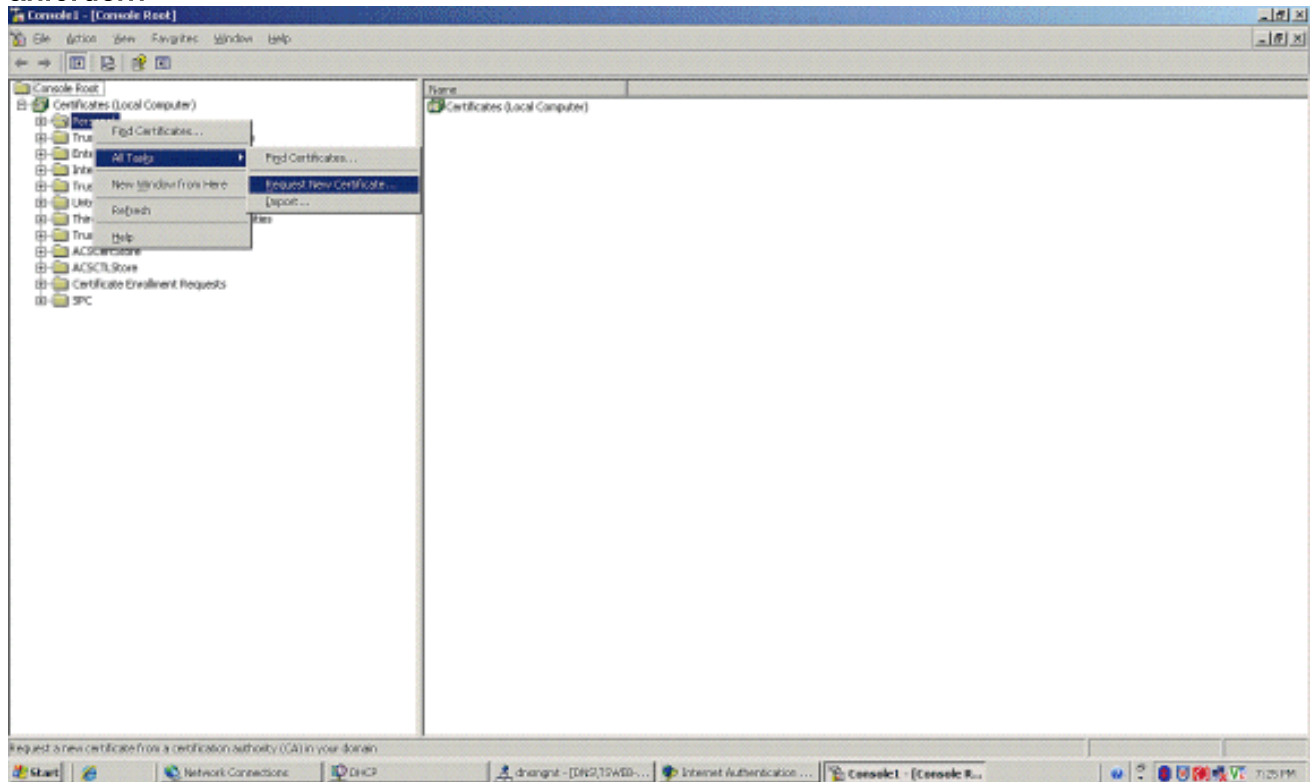


12. Wählen Sie **Lokaler Computer** aus, und klicken Sie auf **Fertig stellen**.



13. Klicken Sie auf **Schließen** und dann auf **OK**.

14. Erweitern Sie **Zertifikate (Lokaler Computer)**, klicken Sie mit der rechten Maustaste auf **Persönlicher Ordner**, wählen Sie **Alle Aufgaben** und dann **Neues Zertifikat anfordern**.



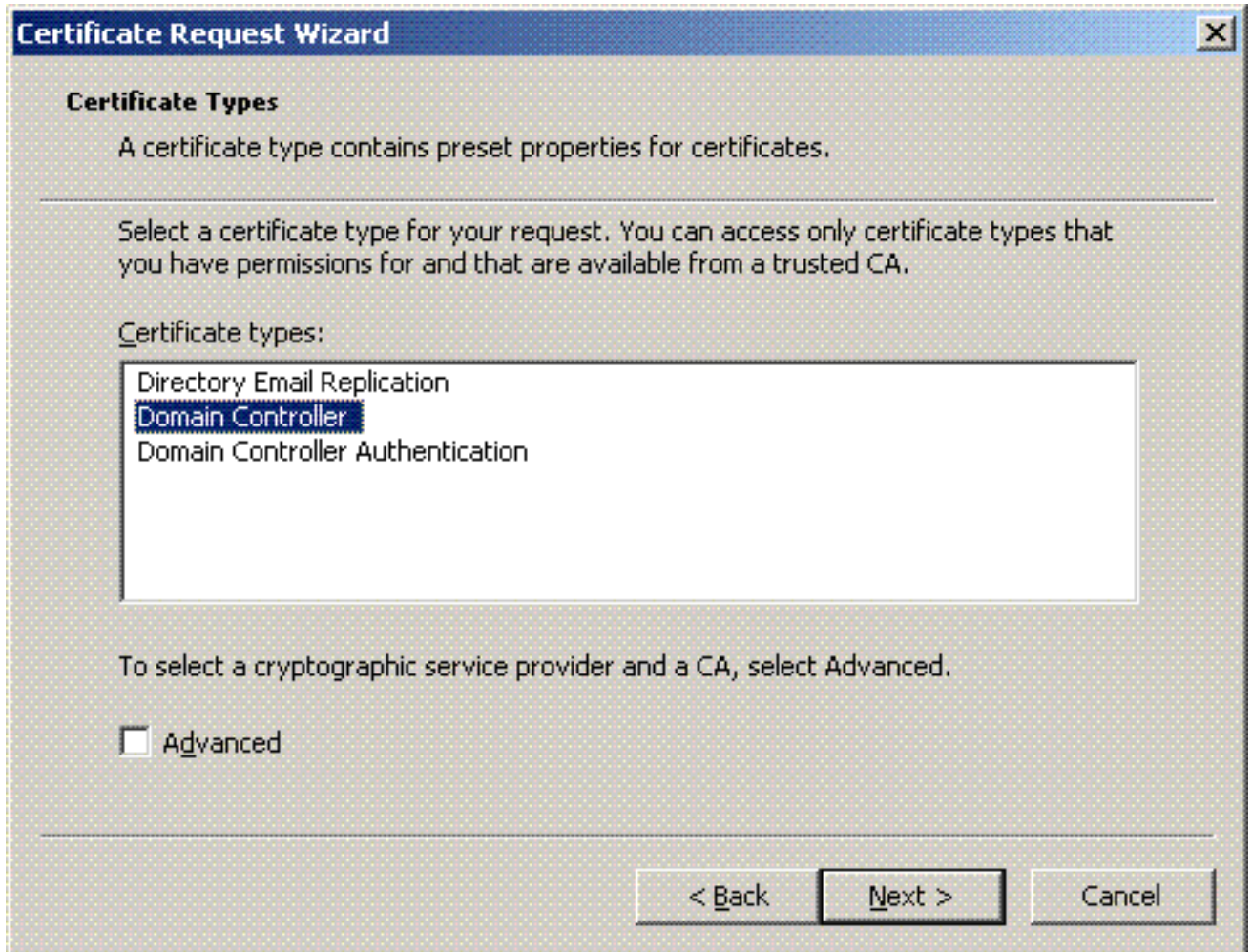
15. Klicken Sie auf **Weiter** im *Assistenten für Zertifikatsanforderungen*



16. Wählen Sie die Zertifikatvorlage **Domänencontroller aus** (wenn Sie ein Computerzertifikat



auf einem anderen Server als dem Domänencontroller anfordern, wählen Sie eine Zertifikatvorlage **Computer**), und klicken Sie auf **Weiter**.



17. Geben Sie einen Namen und eine Beschreibung für das Zertifikat ein.

**Certificate Request Wizard** [X]

**Certificate Friendly Name and Description**

You can provide a name and description that help you quickly identify a specific certificate.

---

Type a friendly name and description for the new certificate.

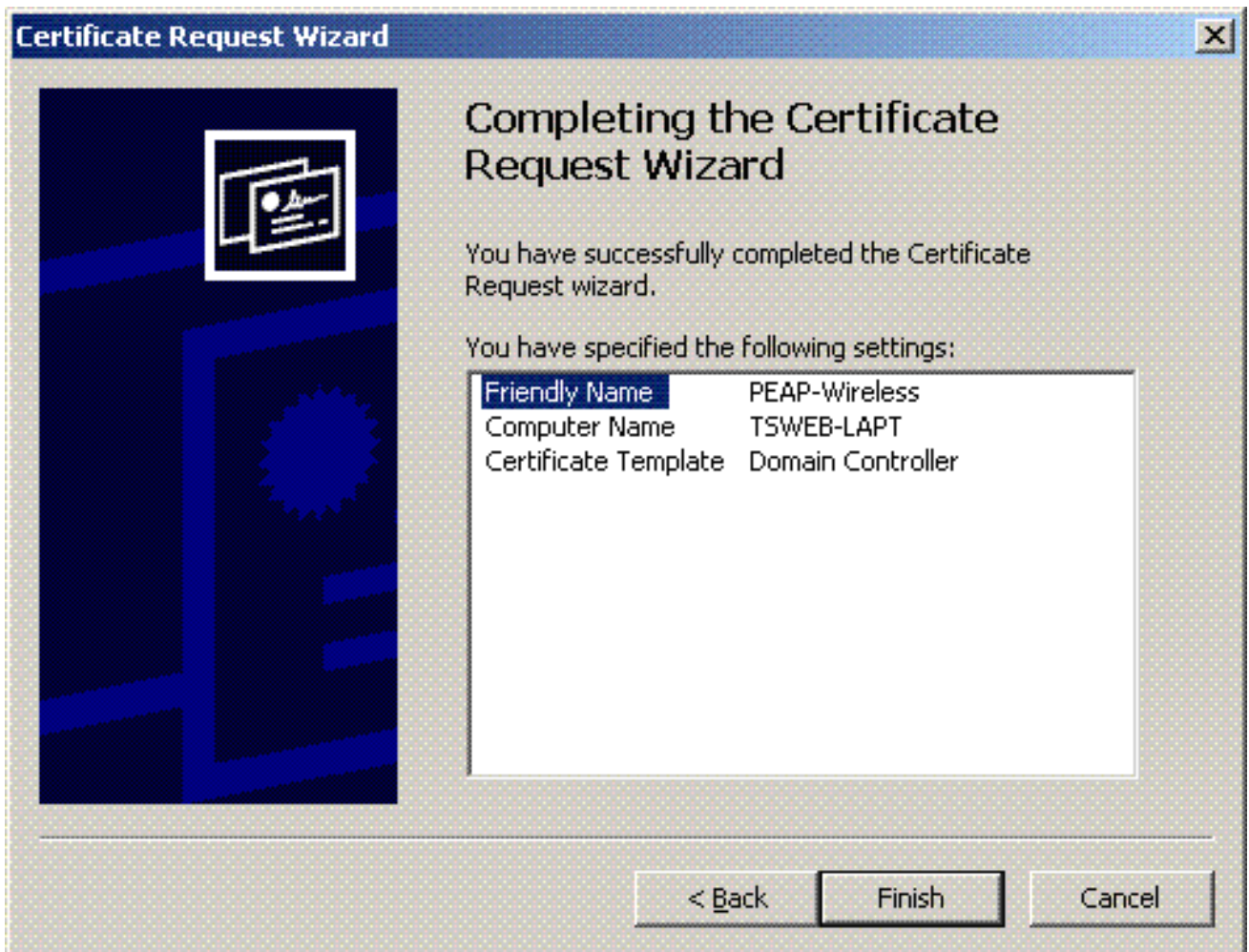
Friendly name:

Description:

---

< Back   Next >   Cancel

18. Klicken Sie auf **Fertig stellen**, um den Assistenten für Zertifizierungsanforderungen abzuschließen.

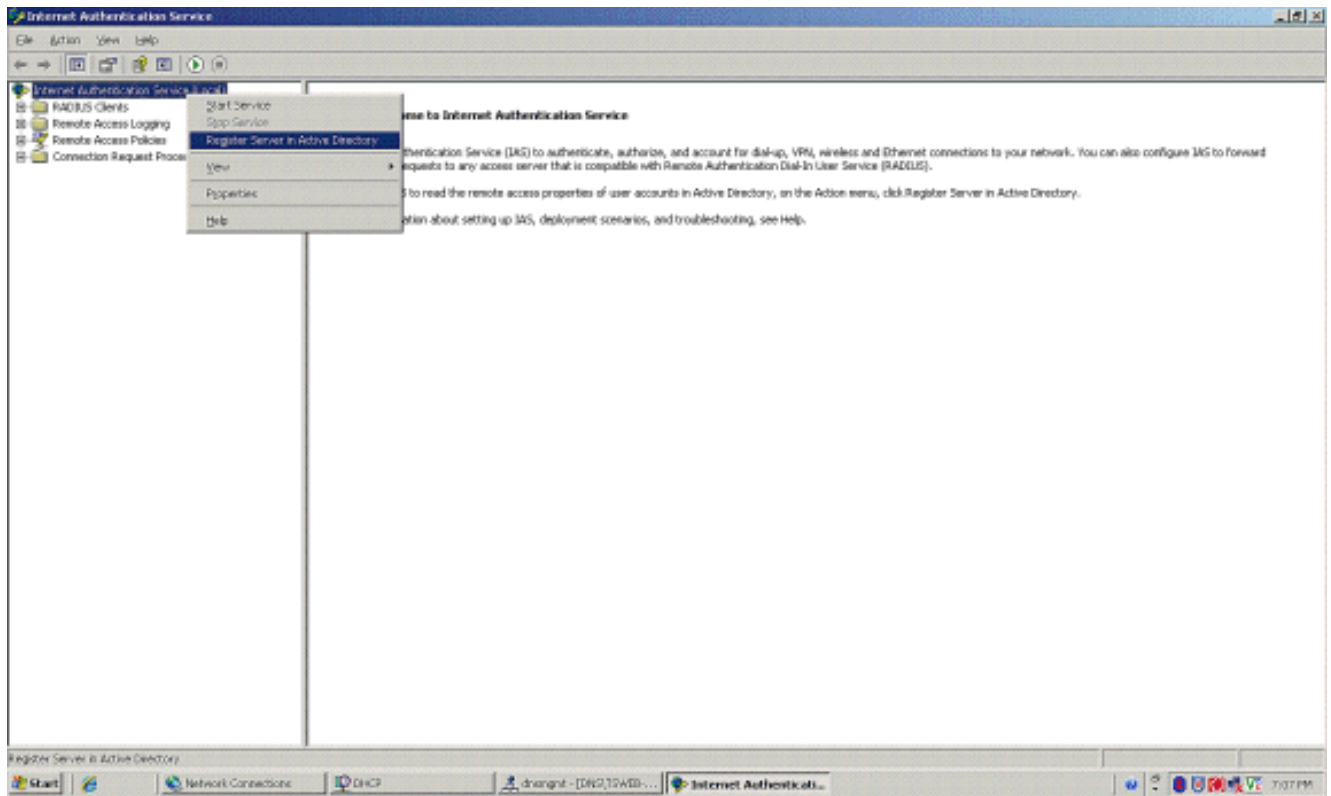


## [Konfigurieren des Internetauthentifizierungsdiensts für die PEAP-MS-CHAP v2-Authentifizierung](#)

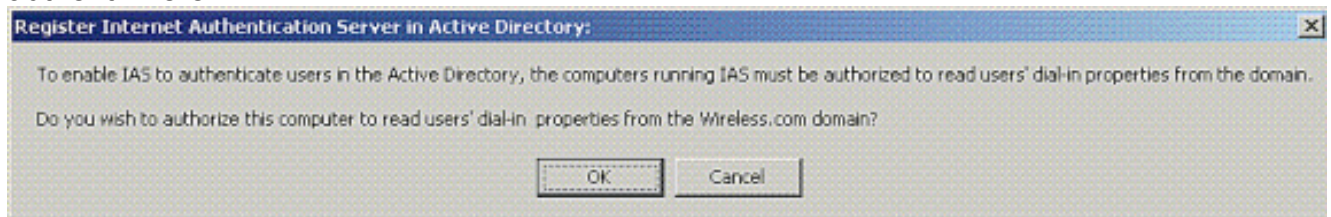
Nachdem Sie ein Zertifikat für den IAS installiert und angefordert haben, konfigurieren Sie den IAS für die Authentifizierung.

Führen Sie diese Schritte aus:

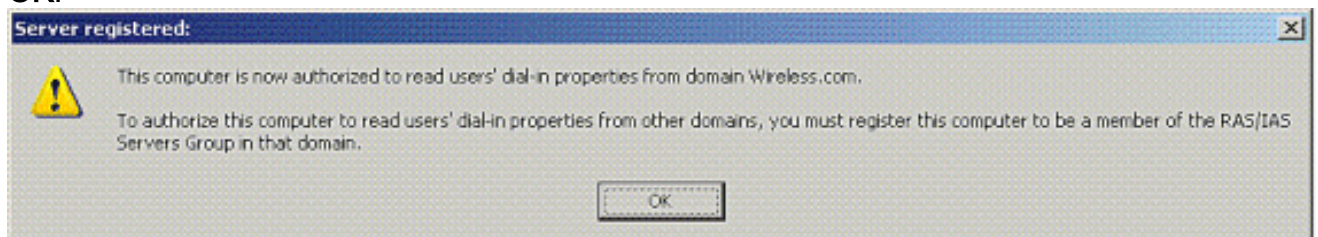
1. Klicken Sie auf **Start > Programme > Verwaltung**, und klicken Sie auf **Internet Authentication Service** Snap-in.
2. Klicken Sie mit der rechten Maustaste auf **Internetauthentifizierungsdienst (IAS)**, und klicken Sie dann auf **Dienst in Active Directory registrieren**.



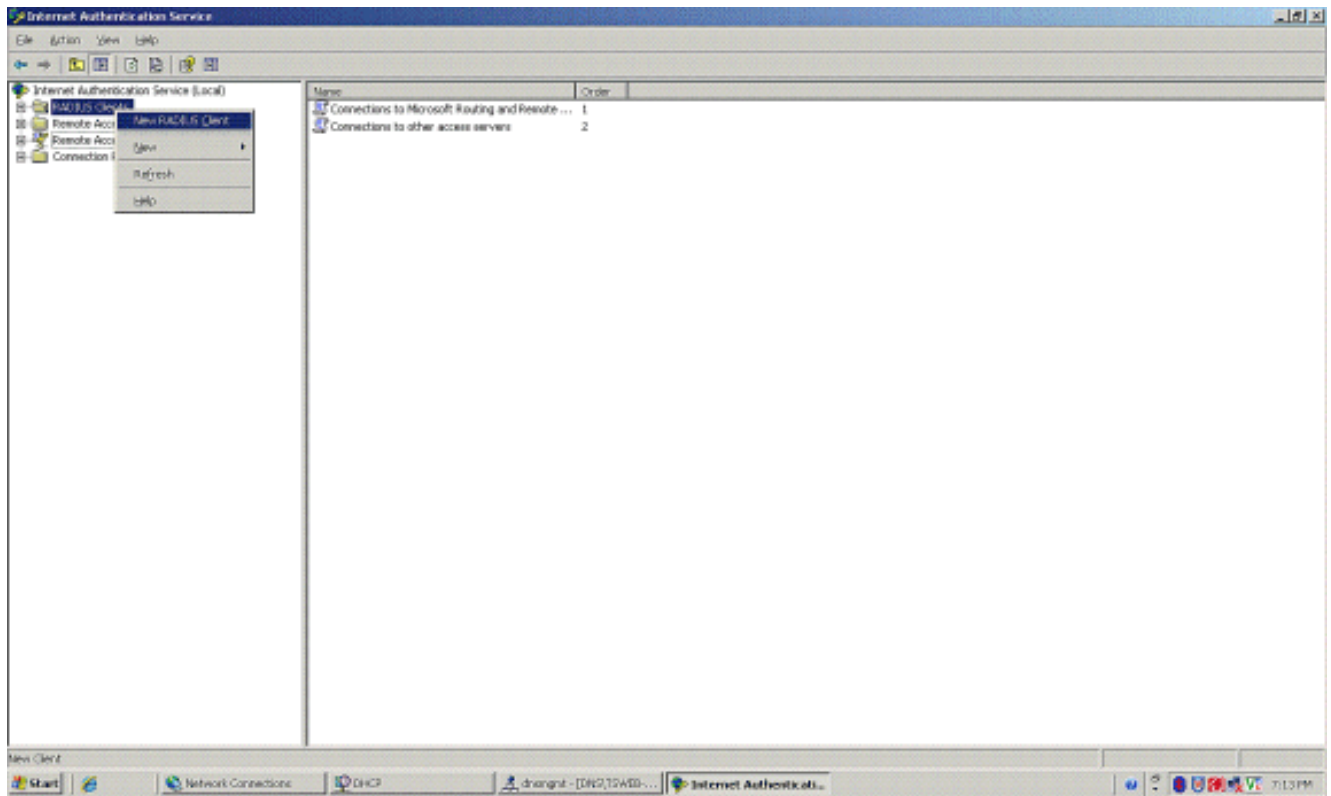
3. Das Dialogfeld **Internetauthentifizierungsdienst in Active Directory registrieren** wird angezeigt. Klicken Sie auf **OK**. Dadurch kann IAS Benutzer im Active Directory authentifizieren.



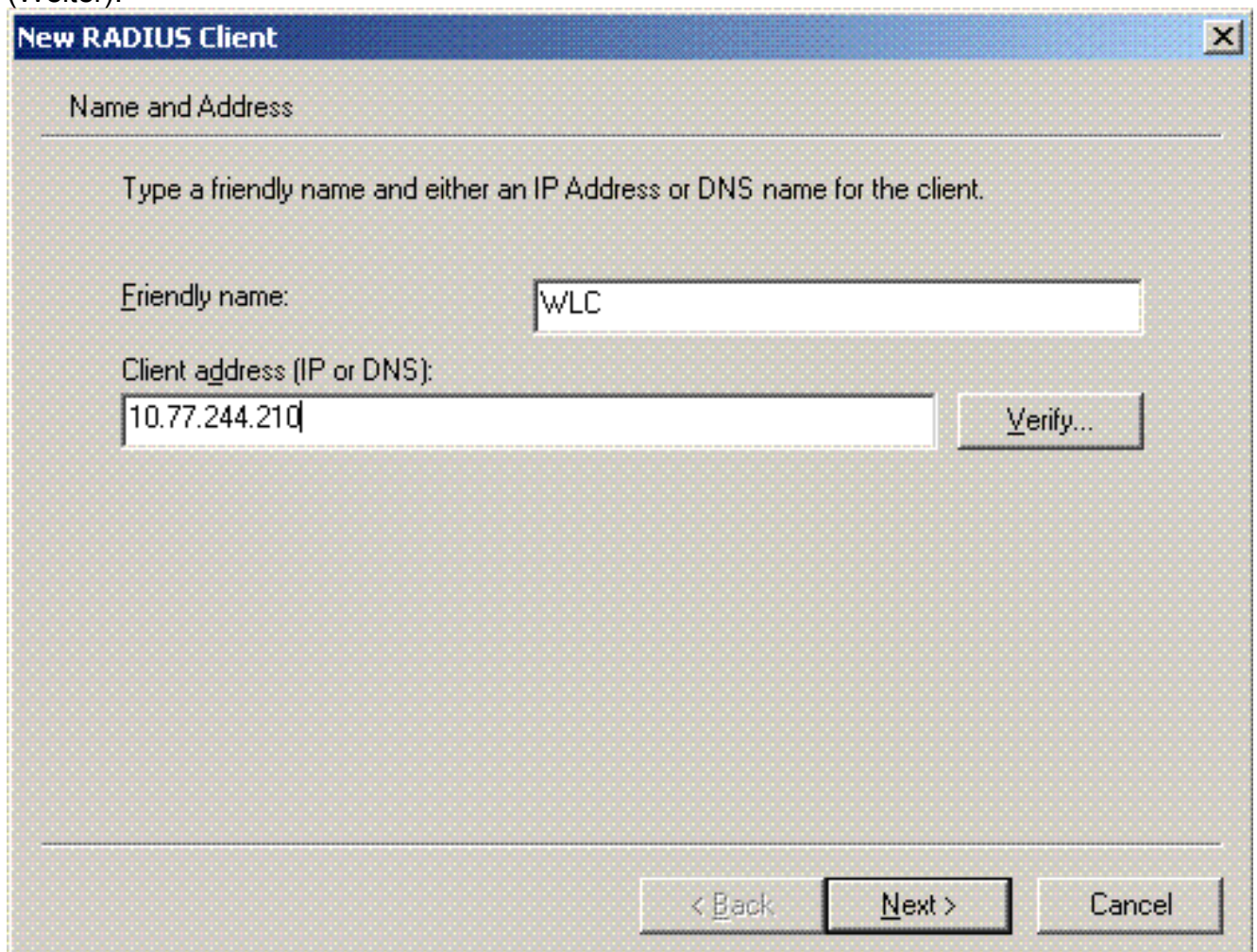
4. Klicken Sie im nächsten Dialogfeld auf **OK**.



5. Fügen Sie den Wireless LAN Controller als AAA-Client auf dem MS IAS-Server hinzu.
6. Klicken Sie mit der rechten Maustaste auf **RADIUS Clients**, und wählen Sie **New RADIUS Client (Neuer RADIUS-Client)**.



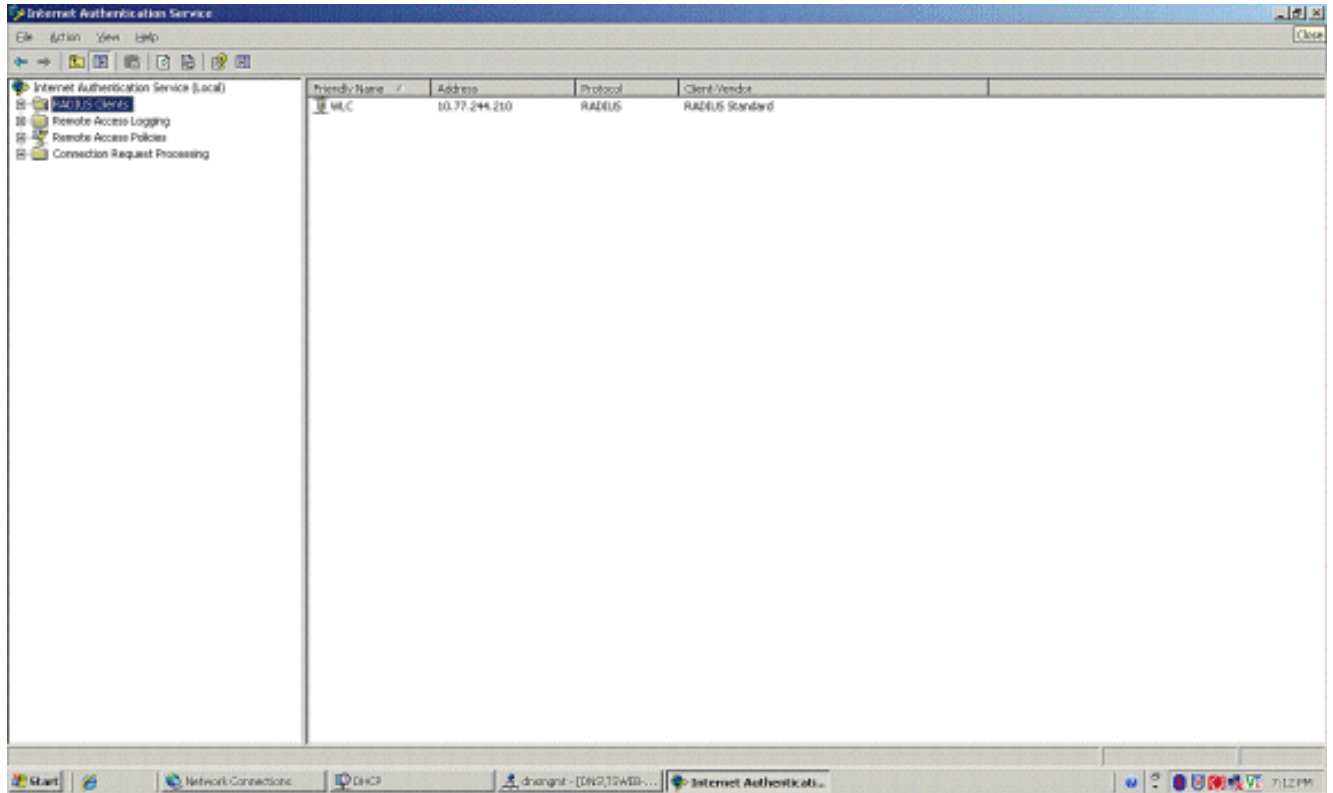
7. Geben Sie den Namen des Clients (in diesem Fall WLC) und die IP-Adresse des WLC ein. Klicken Sie auf **Next** (Weiter).



8. Wählen Sie auf der nächsten Seite unter "Client-Vendor" den Eintrag "**RADIUS Standard**" aus, geben Sie den gemeinsamen geheimen Schlüssel ein, und klicken Sie auf "**Fertig**"

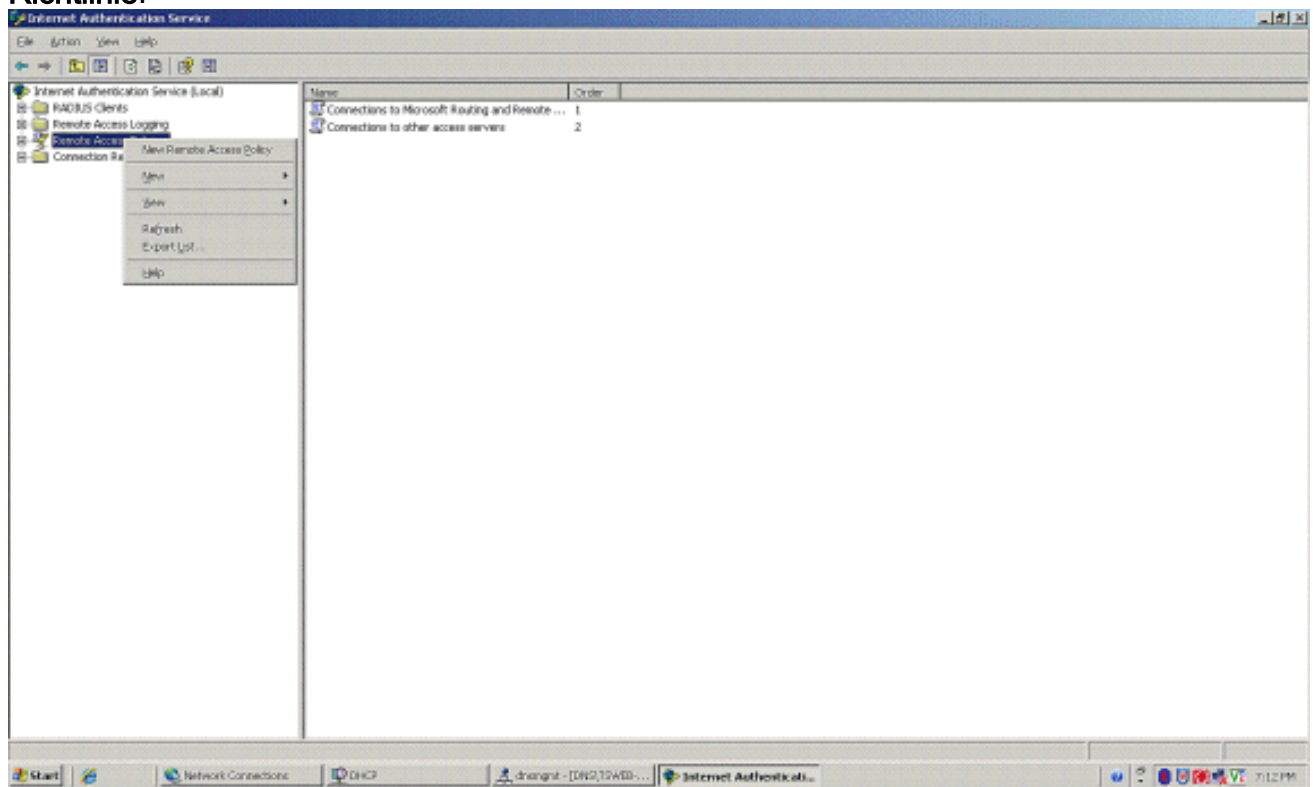
stellen".

9. Beachten Sie, dass der WLC dem IAS als AAA-Client hinzugefügt wird.



10. Erstellen Sie eine Remote-Zugriffsrichtlinie für die Clients.

11. Klicken Sie dazu mit der rechten Maustaste auf **RAS-Richtlinien**, und wählen Sie **Neue RAS-Richtlinie**.




12. Geben Sie einen Namen für die RAS-Richtlinie ein. Verwenden Sie in diesem Beispiel den Namen **PEAP**. Klicken Sie dann auf **Weiter**.

**New Remote Access Policy Wizard** [X]

**Policy Configuration Method**

The wizard can create a typical policy, or you can create a custom policy.



How do you want to set up this policy?

Use the wizard to set up a typical policy for a common scenario

Set up a custom policy

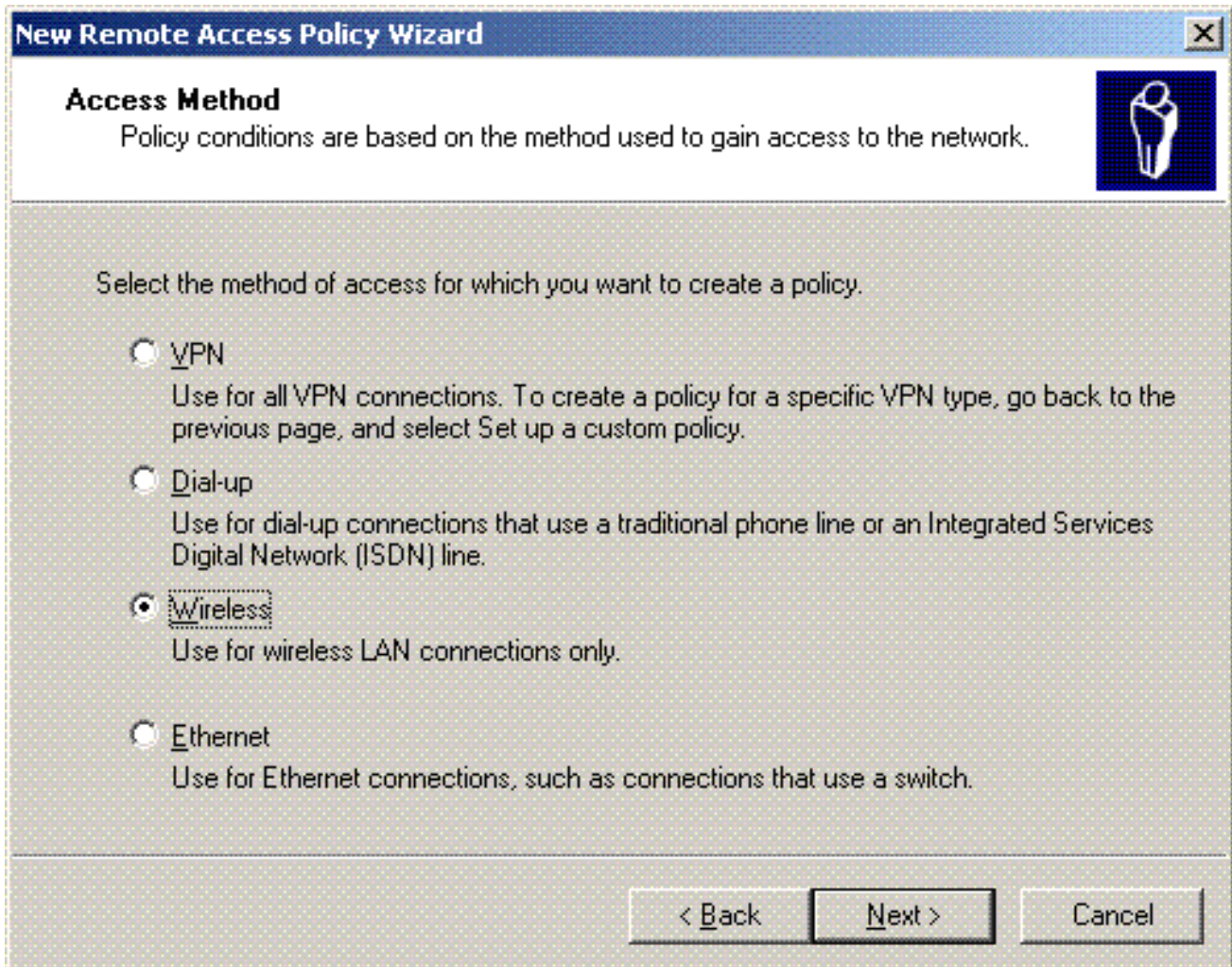
Type a name that describes this policy.

Policy name:

Example: Authenticate all VPN connections.

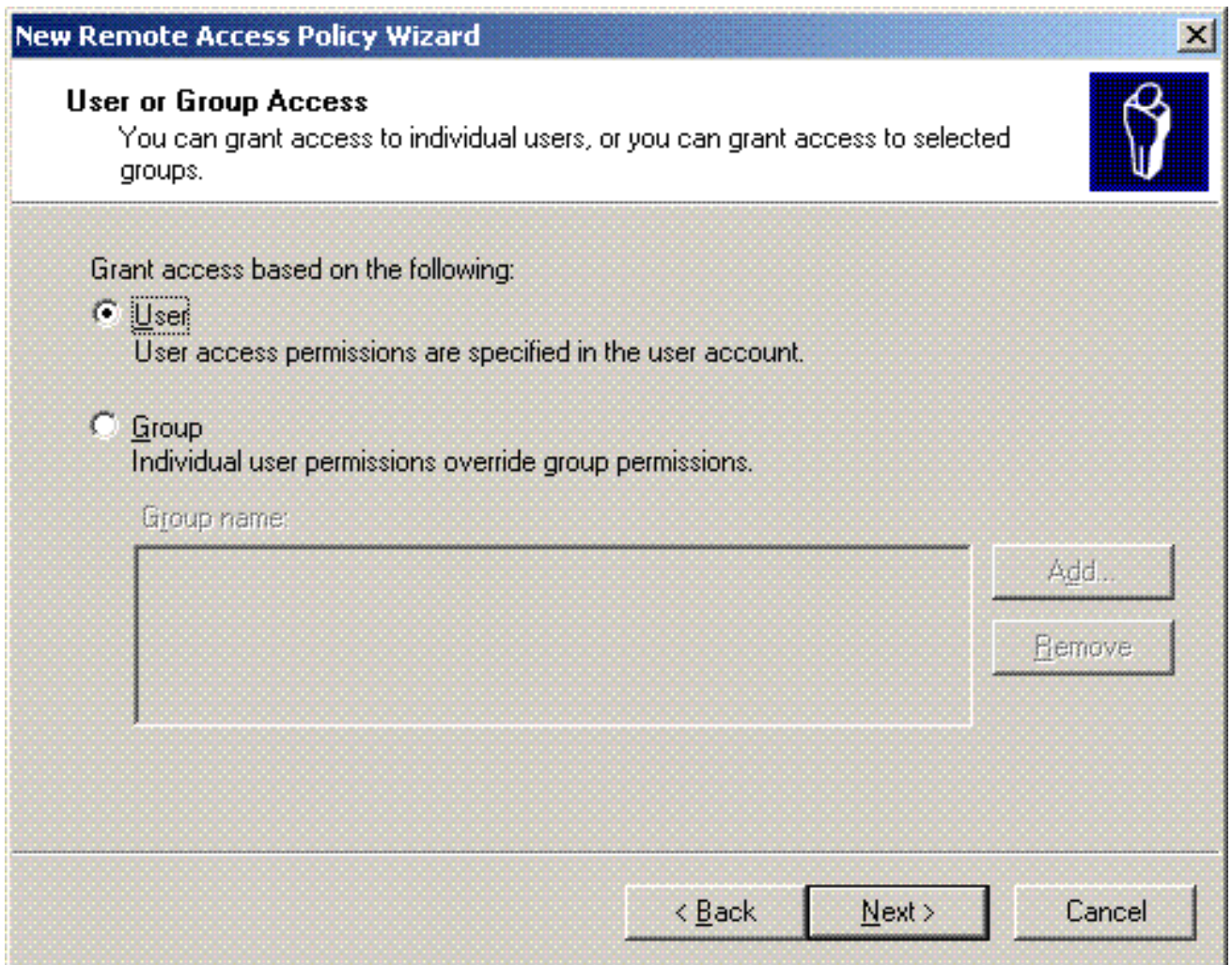
< Back   Next >   Cancel

13. Wählen Sie die Richtlinienattribute basierend auf Ihren Anforderungen aus. Wählen Sie in diesem Beispiel **Wireless** aus.

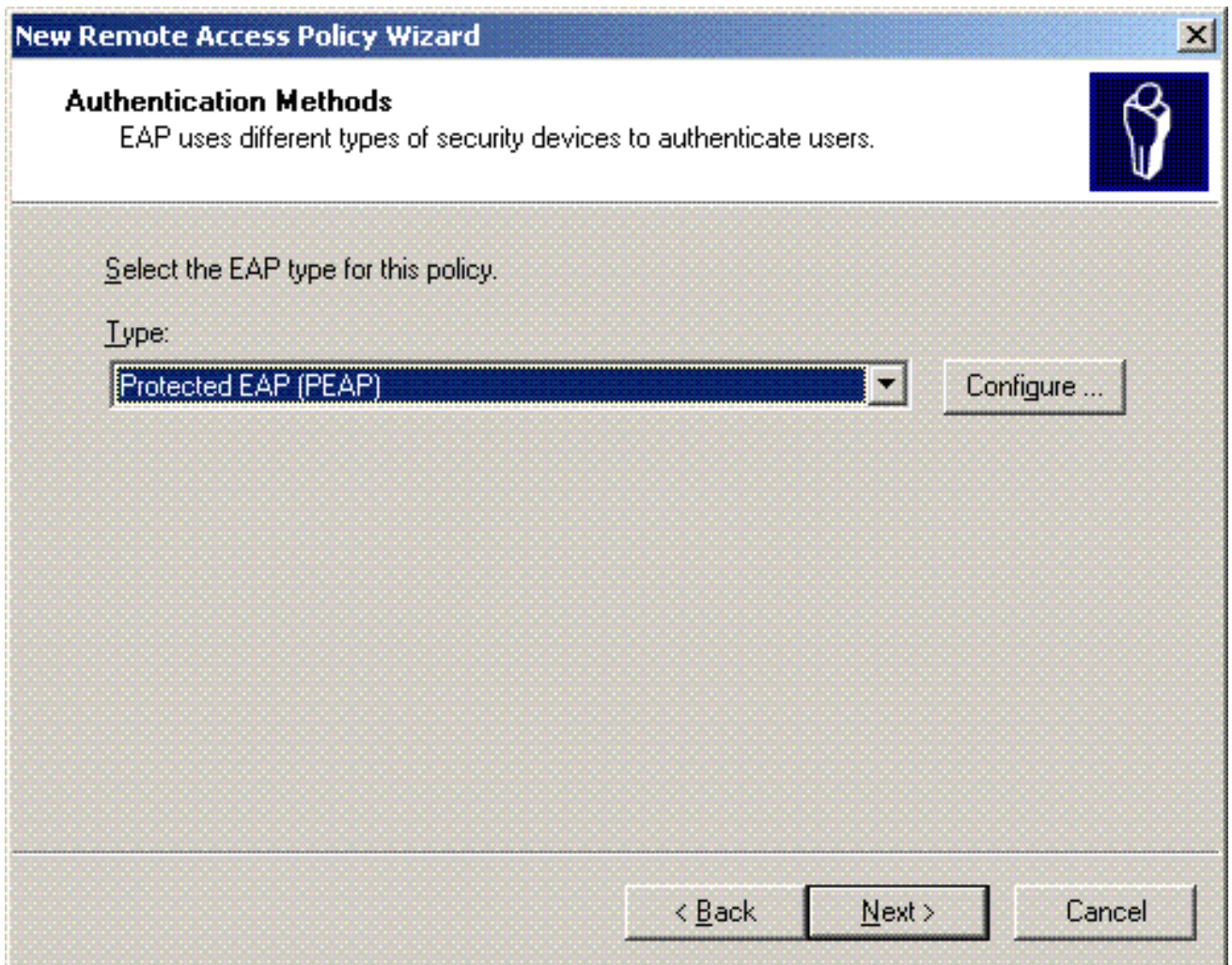


14. Wählen Sie auf der nächsten Seite **Benutzer** aus, um diese RAS-Richtlinie auf eine Liste von Benutzern anzuwenden.

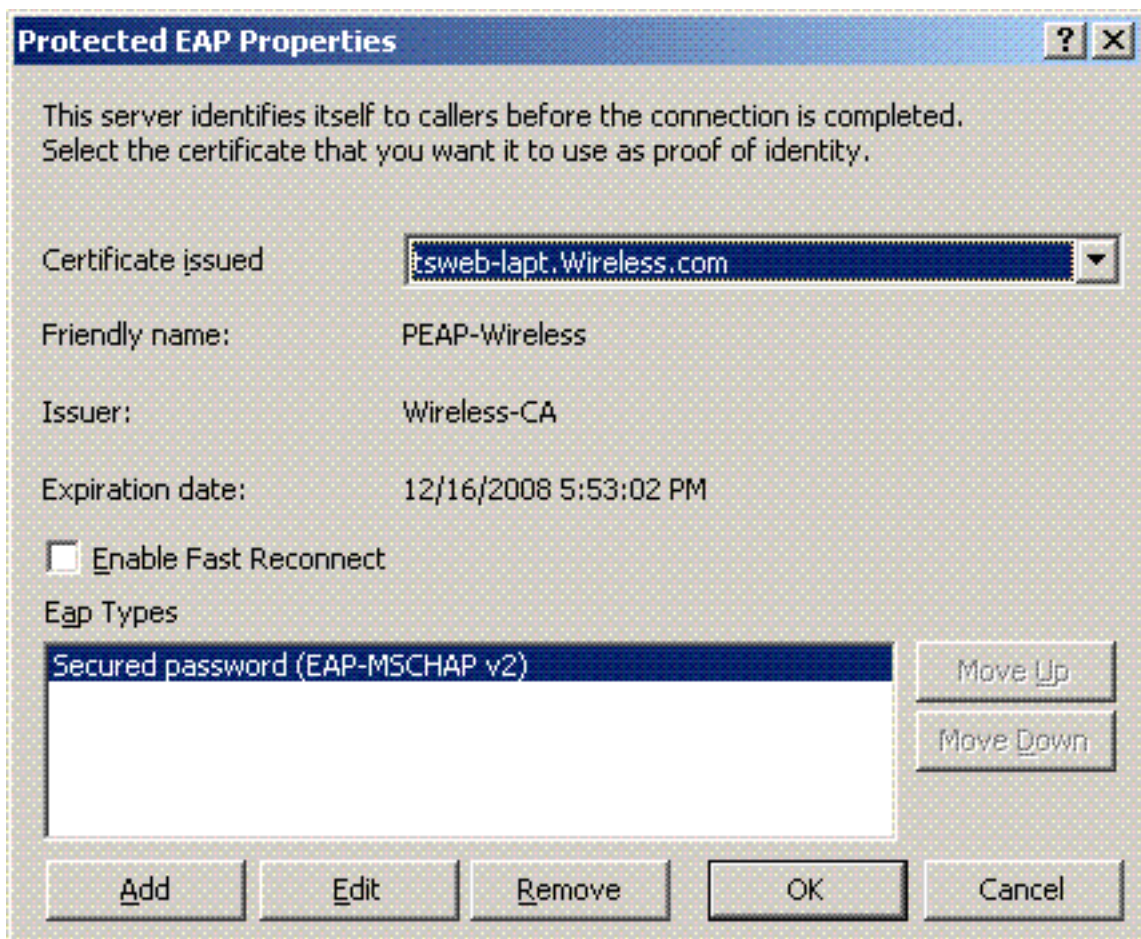




15. Wählen Sie unter Authentication Methods die Option **Protected EAP (PEAP)** aus, und klicken Sie auf **Configure**.

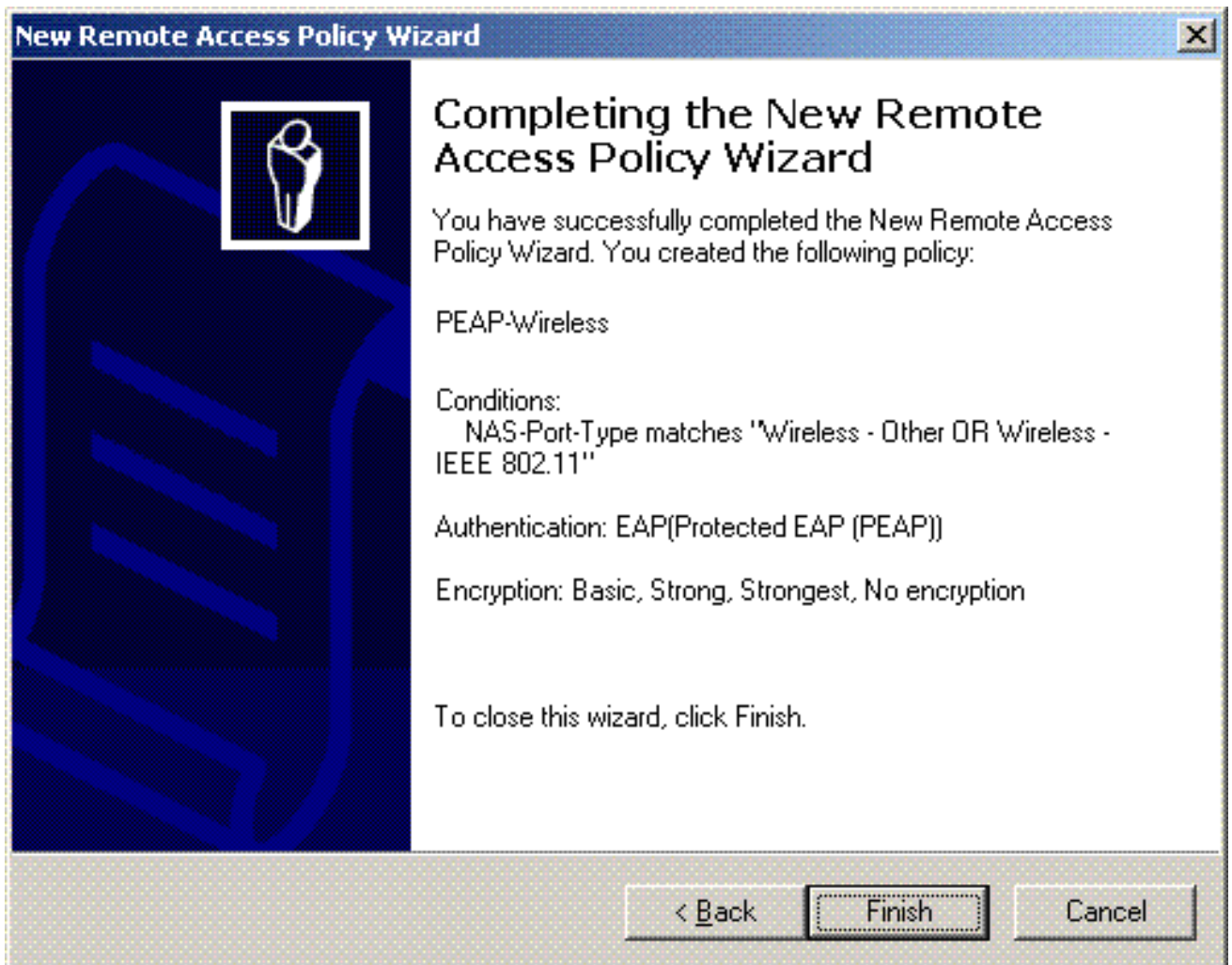


16. Wählen Sie auf der Seite **Protected EAP Properties (Geschützte EAP-Eigenschaften)** aus dem Dropdown-Menü Certificate Issued (Von Zertifikat ausgestellt) das entsprechende Zertifikat aus, und klicken Sie auf

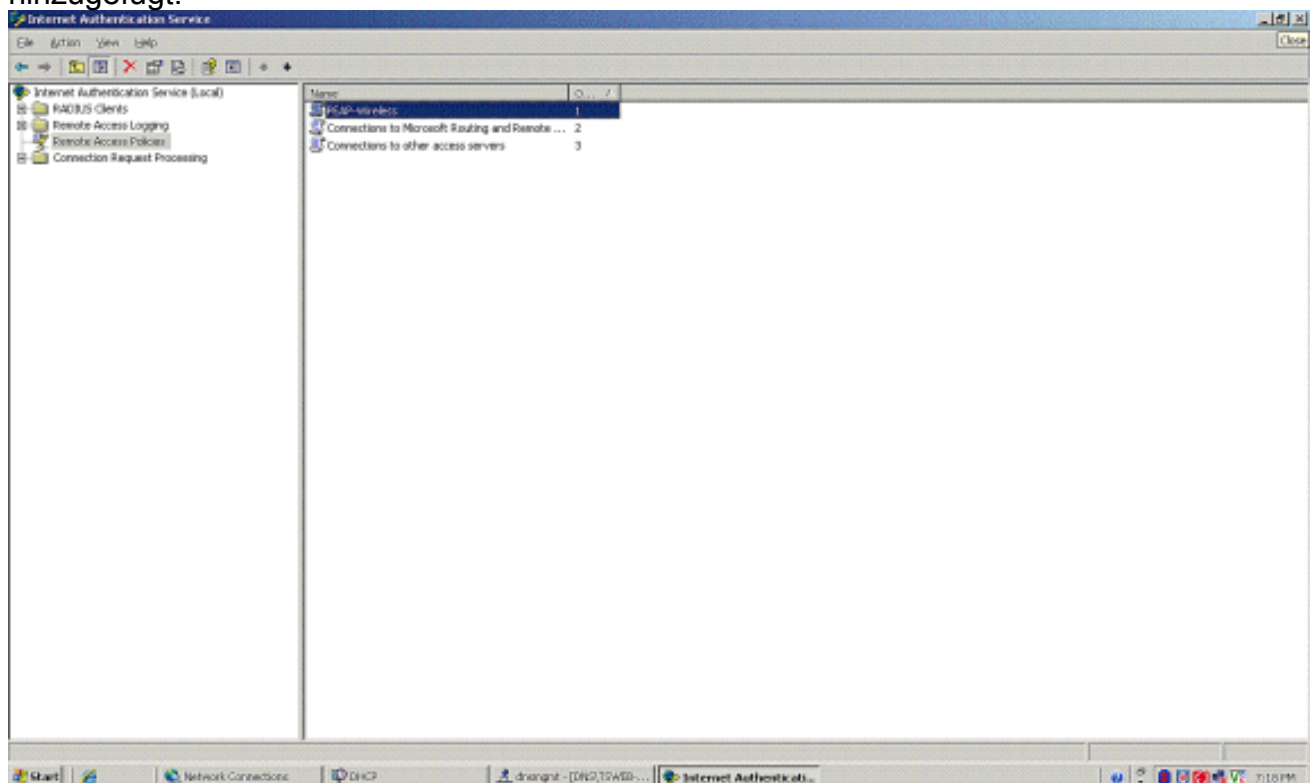


OK.

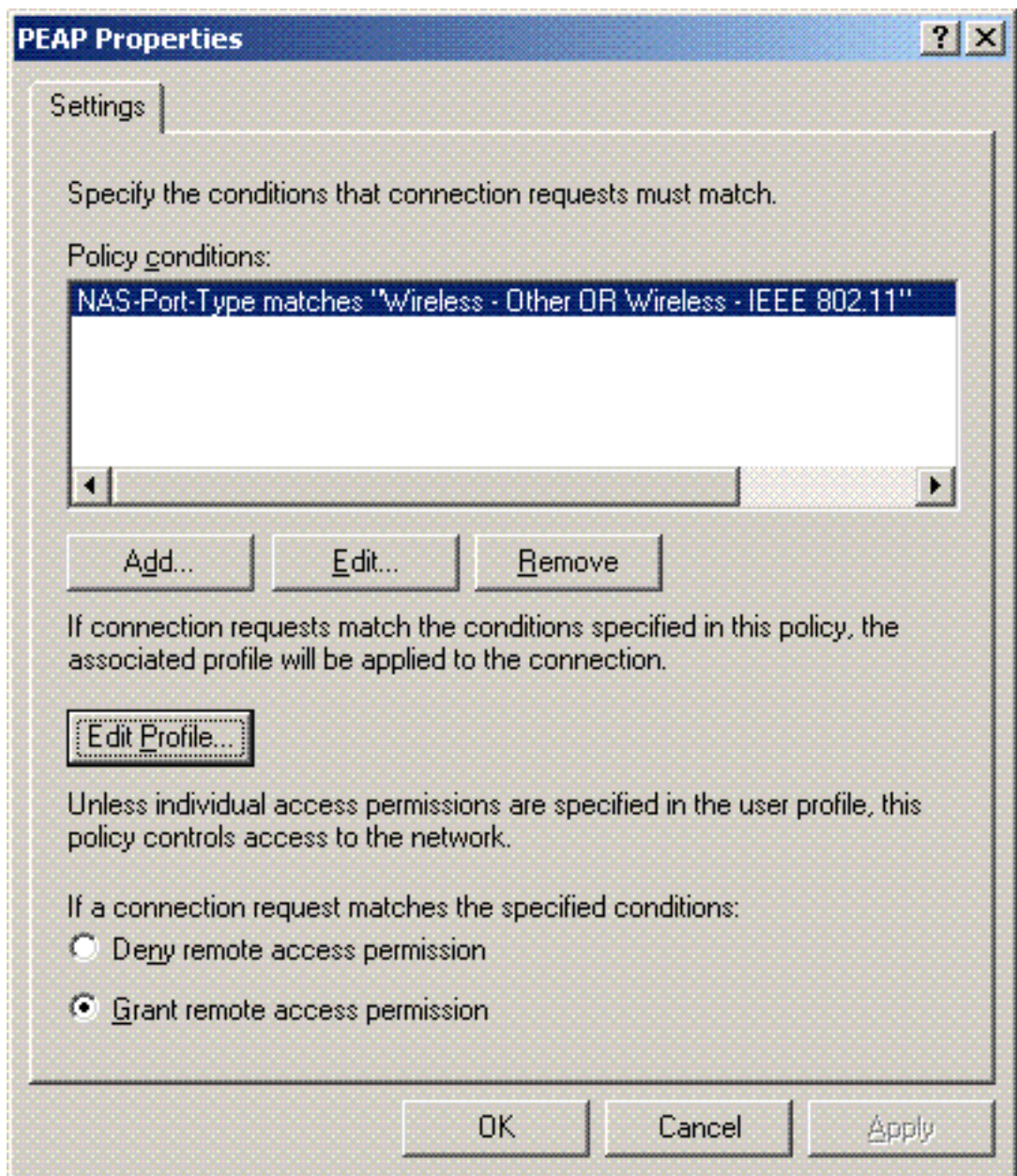
17. Überprüfen Sie die Details der Richtlinie für den Remote-Zugriff, und klicken Sie auf **Fertig stellen**.



18. Die RAS-Richtlinie wurde der Liste hinzugefügt.



19. Klicken Sie mit der rechten Maustaste auf die Richtlinie, und klicken Sie auf **Eigenschaften**. Wählen Sie **"RAS-Berechtigung erteilen"** unter **"Wenn eine Verbindungsanforderung den angegebenen Bedingungen"**



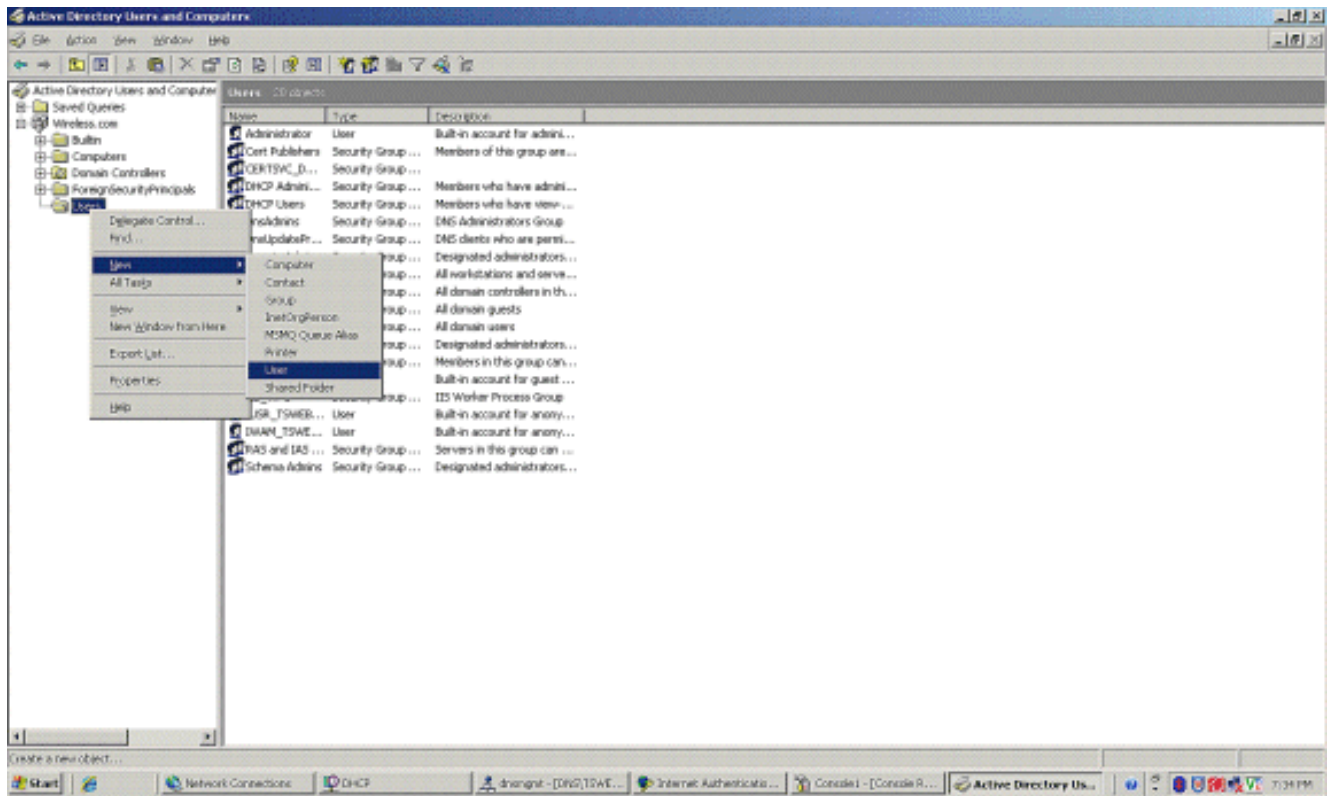
entspricht."

## [Hinzufügen von Benutzern zum Active Directory](#)

In dieser Konfiguration wird die Benutzerdatenbank im Active Directory verwaltet.

Führen Sie die folgenden Schritte aus, um der Active Directory-Datenbank Benutzer hinzuzufügen:

1. Klicken Sie in der Konsolenstruktur von Active Directory-Benutzer und -Computer mit der rechten Maustaste auf **Benutzer**, klicken Sie auf **Neu**, und klicken Sie dann auf **Benutzer**.




2. Geben Sie im Dialogfeld Neues Objekt - Benutzer den Namen des Wireless-Benutzers ein. In diesem Beispiel wird der Name **WirelessUser** im Feld Vorname und **WirelessUser** im Feld Benutzername verwendet. Klicken Sie auf **Next**

The 'New Object - User' dialog box is shown. The 'Create in' field is set to 'Wireless.com/Users'. The 'First name' field contains 'Client 1' and the 'Initials' field is empty. The 'Last name' field is empty. The 'Full name' field contains 'Client 1'. The 'User logon name' field contains 'Client1' and the domain dropdown is set to '@Wireless.com'. The 'User logon name (pre-Windows 2000)' field contains 'WIRELESS\'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

(Weiter).

3. Geben Sie im Dialogfeld Neues Objekt - Benutzer in den Feldern Kennwort und Kennwort bestätigen ein Kennwort Ihrer Wahl ein. Deaktivieren Sie das Kontrollkästchen **Benutzer muss Kennwort bei der nächsten Anmeldung ändern**, und klicken Sie auf

**New Object - User** [X]

 Create in: Wireless.com/Users

---

Password:

Confirm password:

User must change password at next login

User cannot change password

Password never expires

Account is disabled


---

< Back   Next >   Cancel

Weiter.

4. Klicken Sie im Dialogfeld Neues Objekt - Benutzer auf **Fertig**

**New Object - User** [X]

 Create in: Wireless.com/Users

---

When you click Finish, the following object will be created:

Full name: Client 1

User logon name: Client1@Wireless.com

---

< Back   Finish   Cancel

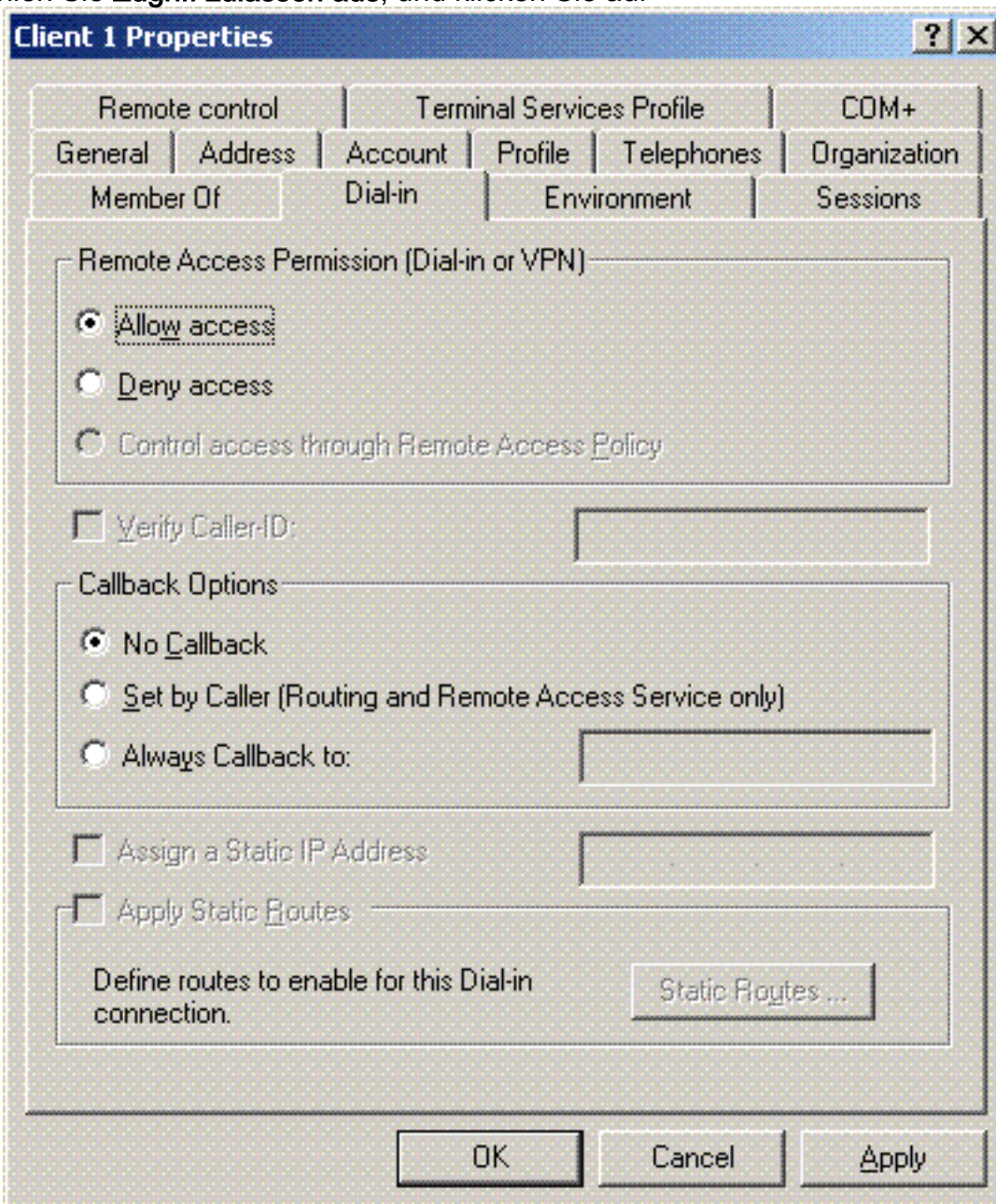
stellen.

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

## Wireless-Zugriff für Benutzer zulassen

Führen Sie diese Schritte aus:

1. Klicken Sie in der Konsolenstruktur von Active Directory-Benutzer und -Computer auf den Ordner **Benutzer**, klicken Sie mit der rechten Maustaste auf **WirelessUser**, klicken Sie auf **Eigenschaften**, und wechseln Sie dann zur **Registerkarte Einwählen (Dial-in)**.
2. Wählen Sie **Zugriff zulassen aus**, und klicken Sie auf



OK.

## Konfigurieren des Wireless LAN-Controllers und der Lightweight Access Points

Konfigurieren Sie nun die Wireless-Geräte für diese Konfiguration. Dazu gehört die Konfiguration der Wireless LAN Controller, Lightweight APs und Wireless Clients.



## Konfigurieren des WLC für die RADIUS-Authentifizierung über den MS IAS-RADIUS-Server

Konfigurieren Sie zunächst den WLC so, dass der MS IAS 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. Fügen Sie dazu den MS IAS-Server auf der Seite **Sicherheit > RADIUS-Authentifizierung** als RADIUS-Server hinzu.

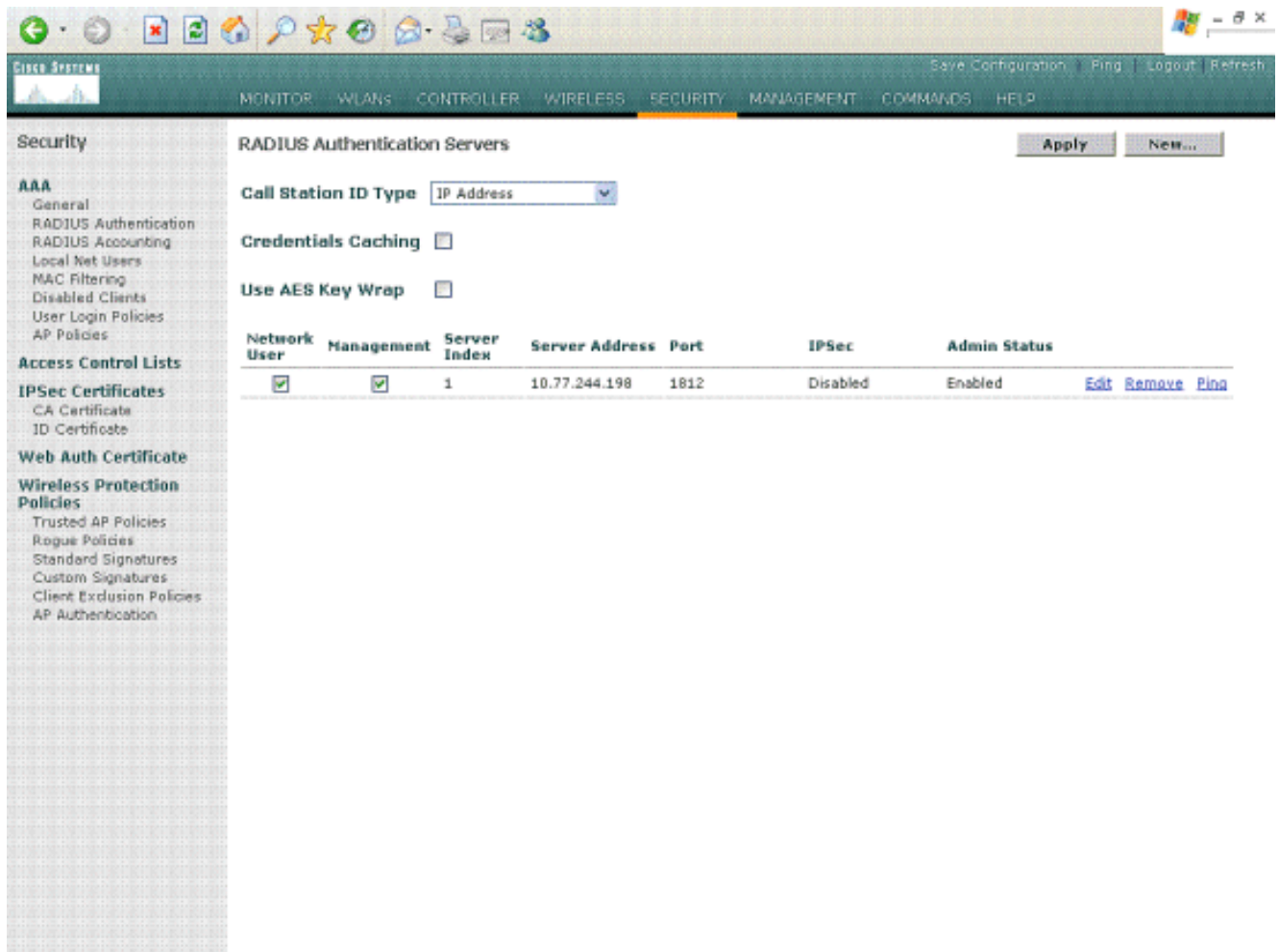
Führen Sie diese Schritte aus:

1. Wählen Sie **Sicherheit** und **RADIUS-Authentifizierung** in der Benutzeroberfläche des Controllers aus, um die Seite RADIUS-Authentifizierungsserver anzuzeigen. Klicken Sie anschließend auf **Neu**, um einen RADIUS-Server zu definieren.

The screenshot shows the Cisco WLC configuration interface. The left sidebar is expanded to 'Security' > 'RADIUS Authentication Servers'. The main area is titled 'RADIUS Authentication Servers > New'. The configuration fields are as follows:

Server Index (Priority)	1
Server IP Address	10.77.244.198
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Key Wrap	<input type="checkbox"/>
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Retransmit Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

2. Definieren Sie die RADIUS-Serverparameter auf der Seite **RADIUS Authentication Servers > New (RADIUS-Authentifizierungsserver > Neu)**. 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 gilt. In diesem Beispiel wird der MS IAS als RADIUS-Server mit der IP-Adresse 10.77.244.198 verwendet.



3. Klicken Sie auf **Apply** (Anwenden).
4. Der MS IAS-Server wurde dem WLC als Radius-Server hinzugefügt und kann zur Authentifizierung von Wireless Clients verwendet werden.

## Konfigurieren eines WLAN für die Clients

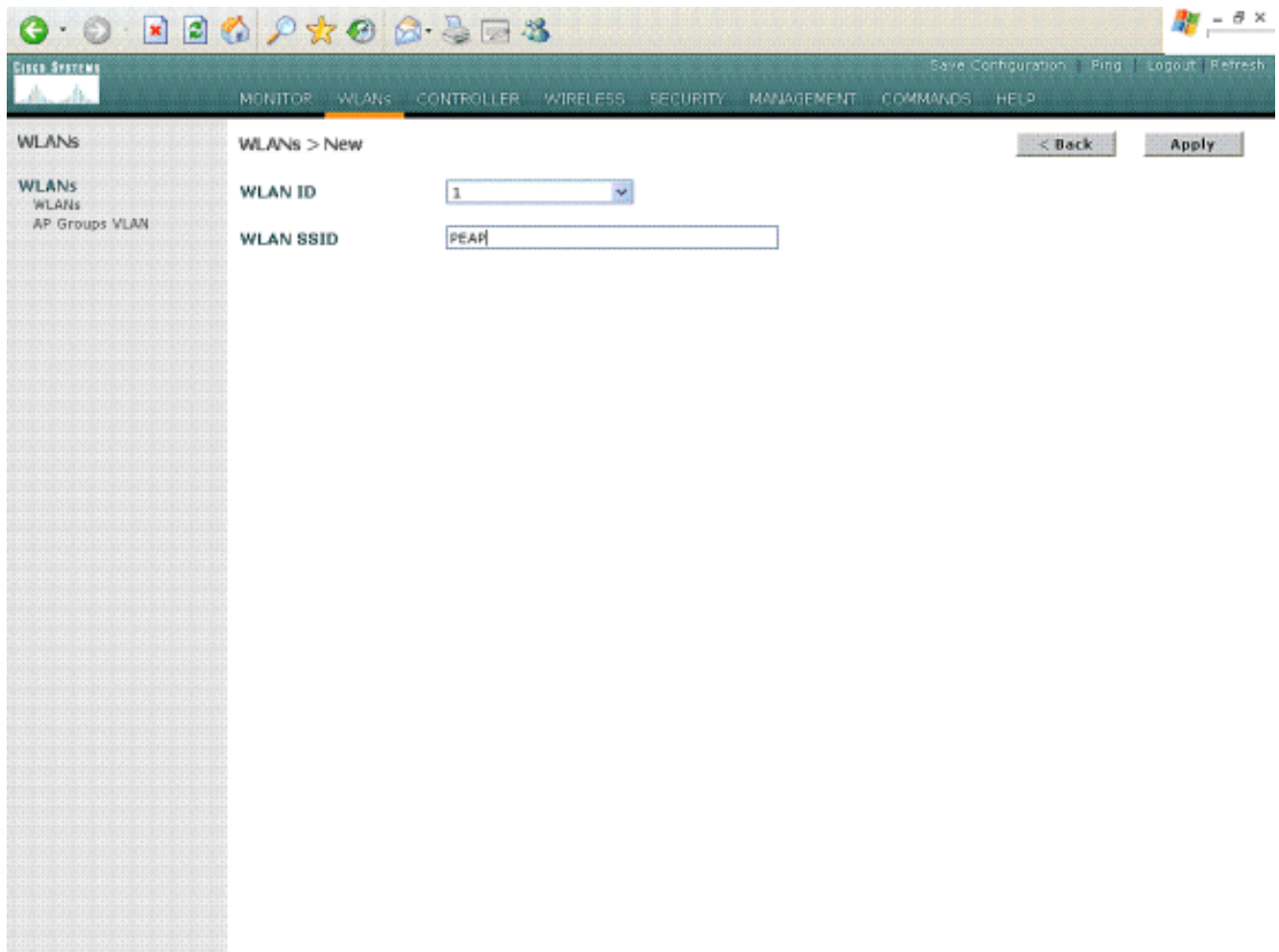
Konfigurieren Sie die SSID (WLAN), mit der die Wireless-Clients verbunden sind. Erstellen Sie in diesem Beispiel die SSID, und nennen Sie sie **PEAP**.

Definieren Sie die Layer-2-Authentifizierung als WPA2, sodass die Clients eine EAP-basierte Authentifizierung durchführen (in diesem Fall PEAP-MSCHAPv2) und AES als Verschlüsselungsmechanismus verwenden. Lassen Sie alle anderen Werte unverändert.

**Hinweis:** 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](#).

Um ein WLAN auf dem WLC zu konfigurieren, führen Sie die folgenden Schritte aus:

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



3. Nachdem Sie ein neues WLAN erstellt haben, wird die Seite **WLAN > Edit** (WLAN > Bearbeiten) für das neue WLAN angezeigt. Auf dieser Seite können Sie verschiedene spezifische Parameter für dieses WLAN definieren, z. B. Allgemeine Richtlinien, RADIUS-Server, Sicherheitsrichtlinien und 802.1x-Parameter.

WLANs > Edit

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

**General Policies**

Radio Policy: All  
Admin Status:  Enabled  
Session Timeout (secs): 0  
Quality of Service (QoS): Silver (best effort)  
WMM Policy: Disabled  
7920 Phone Support:  Client CAC Limit  AP CAC Limit  
Broadcast SSID:  Enabled  
Aironet IE:  Enabled  
Allow AAA Override:  Enabled  
Client Exclusion:  Enabled \*\* 60 Timeout Value (secs)  
DHCP Server:  Override  
DHCP Addr. Assignment:  Required  
Interface Name: management  
MFP Version Required: 1  
MFP Signature Generation:  (Global MFP Disabled)  
H-REAP Local Switching:   
\* H-REAP Local Switching not supported with IPSEC, CRANITE and FORTRESS authentications.

**Security Policies**

IPv6 Enable:   
Layer 2 Security: WPA1+WPA2  
 MAC Filtering  
Layer 3 Security: None  
 Web Policy \*

\*\* When client exclusion is enabled, a timeout value of zero means infinity (will require administrative override to reset excluded clients)  
\*\*\* CKIP is not supported by 10xx APs

4. Aktivieren Sie **Admin Status** unter General Policies (Allgemeine Richtlinien), um das WLAN zu aktivieren. Wenn der WAP die SSID in den Beacon-Frames übertragen soll, aktivieren Sie **Broadcast SSID**.
5. Wählen Sie unter Layer 2 Security (Layer 2-Sicherheit) **WPA1 + WPA2 aus**. Dadurch wird WPA im WLAN aktiviert. Blättern Sie auf der Seite nach unten, und wählen Sie die WPA-Richtlinie aus. In diesem Beispiel wird die WPA2- und AES-Verschlüsselung verwendet. Wählen Sie den entsprechenden RADIUS-Server aus dem Dropdown-Menü unter RADIUS Servers (RADIUS-Server) aus. Verwenden Sie in diesem Beispiel **10.77.244.198** (die IP-Adresse des MS IAS-Servers). Die übrigen Parameter können je nach Anforderung des WLAN-Netzwerks geändert werden.

WPA1+WPA2 Parameters

WPA1 Policy:   
WPA2 Policy:   
WPA2 Encryption:  AES  TKIP  
Auth Key Mgmt: 802.1x

6. Klicken Sie auf **Apply** (Anwenden).

Profile Name	WLAN ID	WLAN SSID	Admin Status	Security Policies
PEAP	1	PEAP	Enabled	[WPA2][Auth(802.1x)]

\* WLAN IDs 9-16 will not be pushed to 1130,1200 and 1240 AP models.

## Konfigurieren der Wireless-Clients

### Konfigurieren der Wireless Clients für die PEAP-MS CHAPv2-Authentifizierung

Dieses Beispiel enthält Informationen zur Konfiguration des Wireless-Clients mit dem Cisco Aironet Desktop Utility. Stellen Sie vor der Konfiguration des Client-Adapters sicher, dass die neueste Version der Firmware und des Dienstprogramms verwendet wird. Die aktuelle Version der Firmware und Dienstprogramme finden Sie auf der Seite für Wireless-Downloads unter Cisco.com.

Führen Sie die folgenden Schritte aus, um den Cisco Aironet 802.11 a/b/g Wireless-Client-Adapter mit der ADU zu konfigurieren:

1. Öffnen Sie das Aironet Desktop Utility.
2. Klicken Sie auf **Profilverwaltung**, und klicken Sie auf **Neu**, um ein Profil zu definieren.
3. Geben Sie auf der Registerkarte Allgemein den Profilnamen und die SSID ein. Verwenden Sie in diesem Beispiel die SSID, die Sie auf dem WLC (PEAP) konfiguriert haben.

The image shows a Windows-style dialog box titled "Profile Management". It has three tabs: "General", "Security", and "Advanced". The "Security" tab is selected. The dialog is divided into two main sections: "Profile Settings" and "Network Names".

**Profile Settings:**

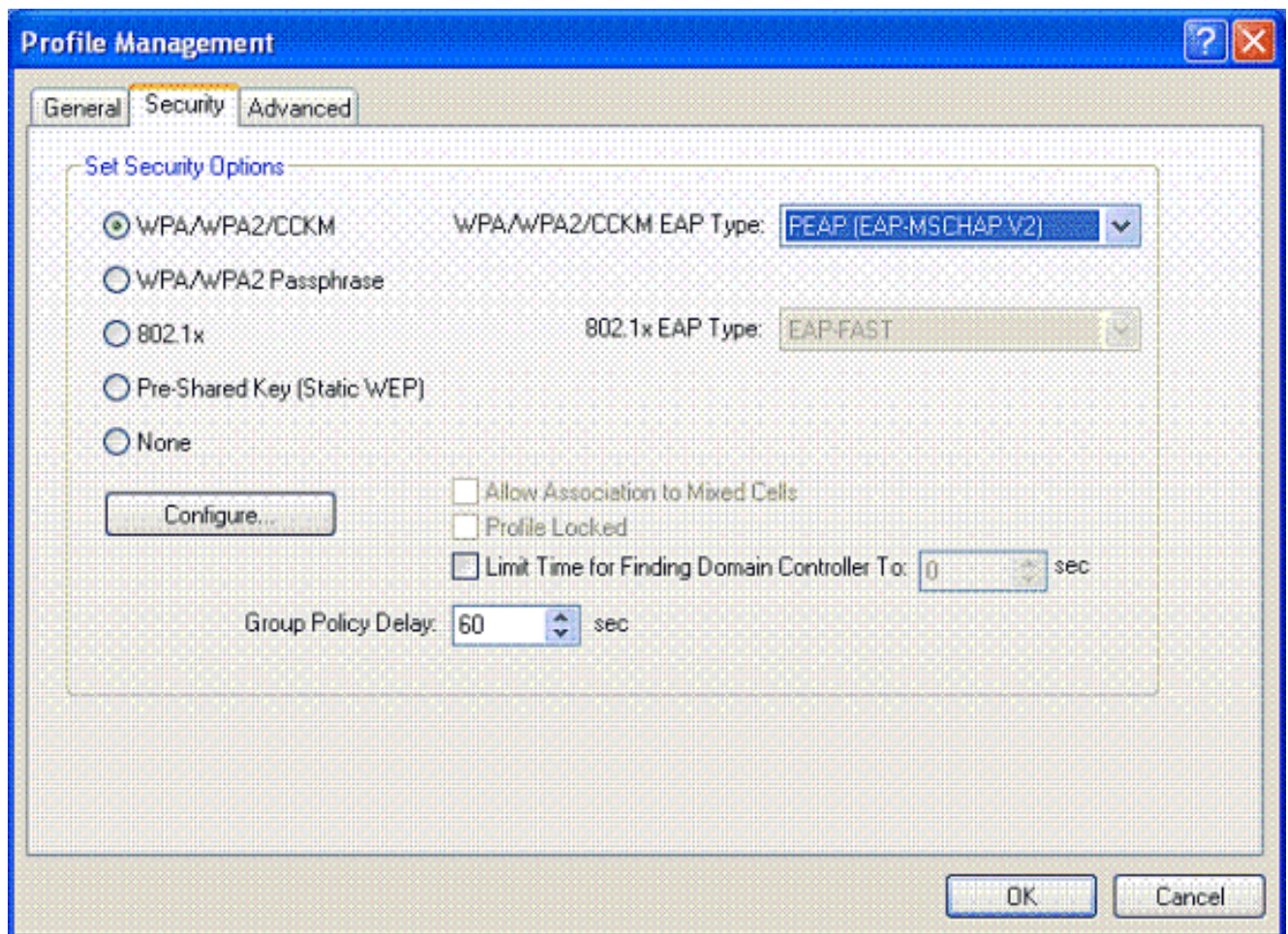
- Profile Name: PEAP-MSCHAPv2
- Client Name: CLIENT1

**Network Names:**

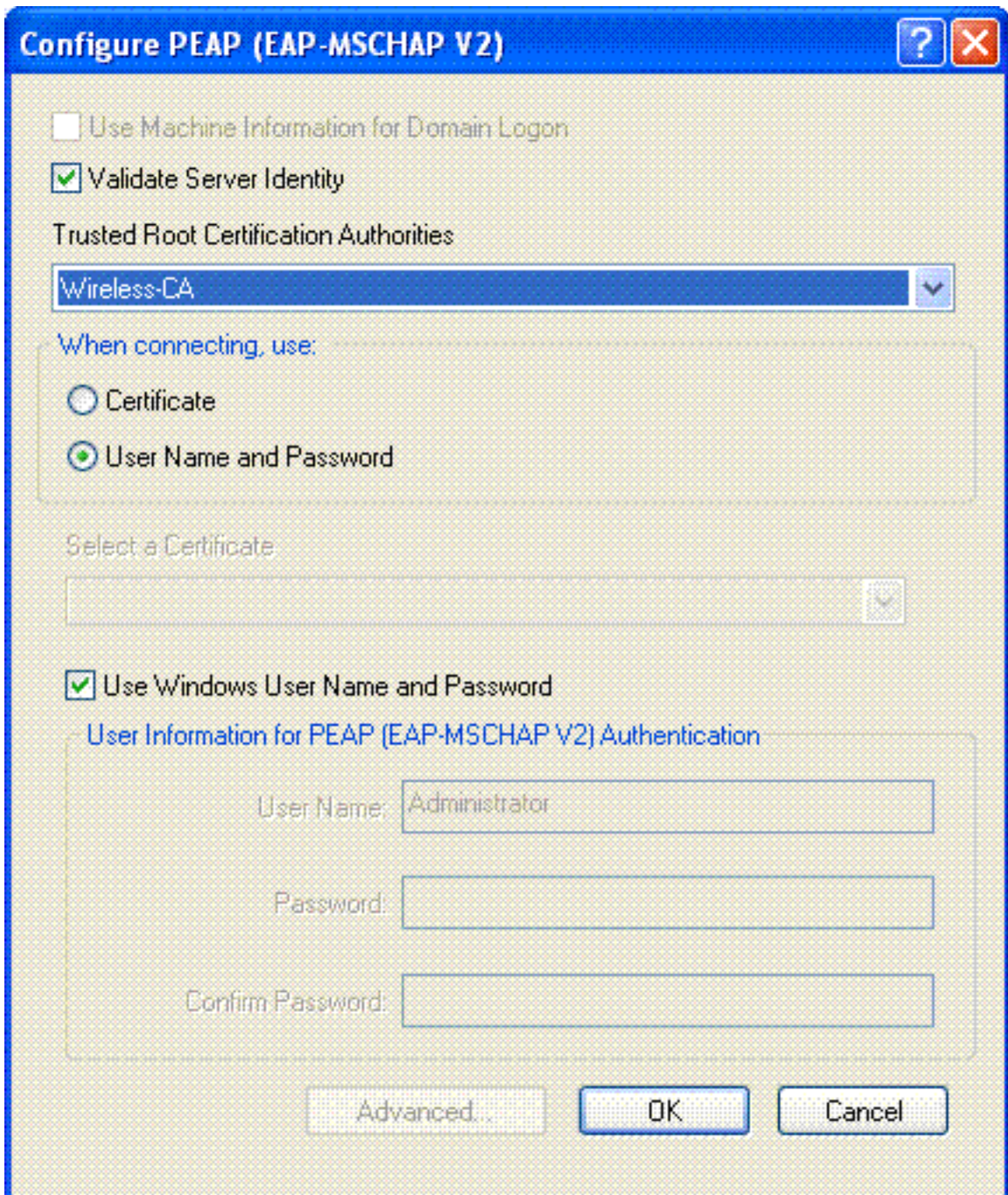
- SSID1: PEAP
- SSID2: (empty)
- SSID3: (empty)

At the bottom right, there are "OK" and "Cancel" buttons.

4. Wählen Sie die Registerkarte Sicherheit aus, wählen Sie **WPA/WPA2/CCKM aus**, geben Sie unter WPA/WPA2/CCKM EAP select **PEAP [EAP-MSCHAPv2]** ein, und klicken Sie auf **Konfigurieren**.



5. Wählen Sie **Serverzertifikat validieren** und dann **Wireless-CA** im Dropdown-Menü Vertrauenswürdige Stammzertifizierungsstellen



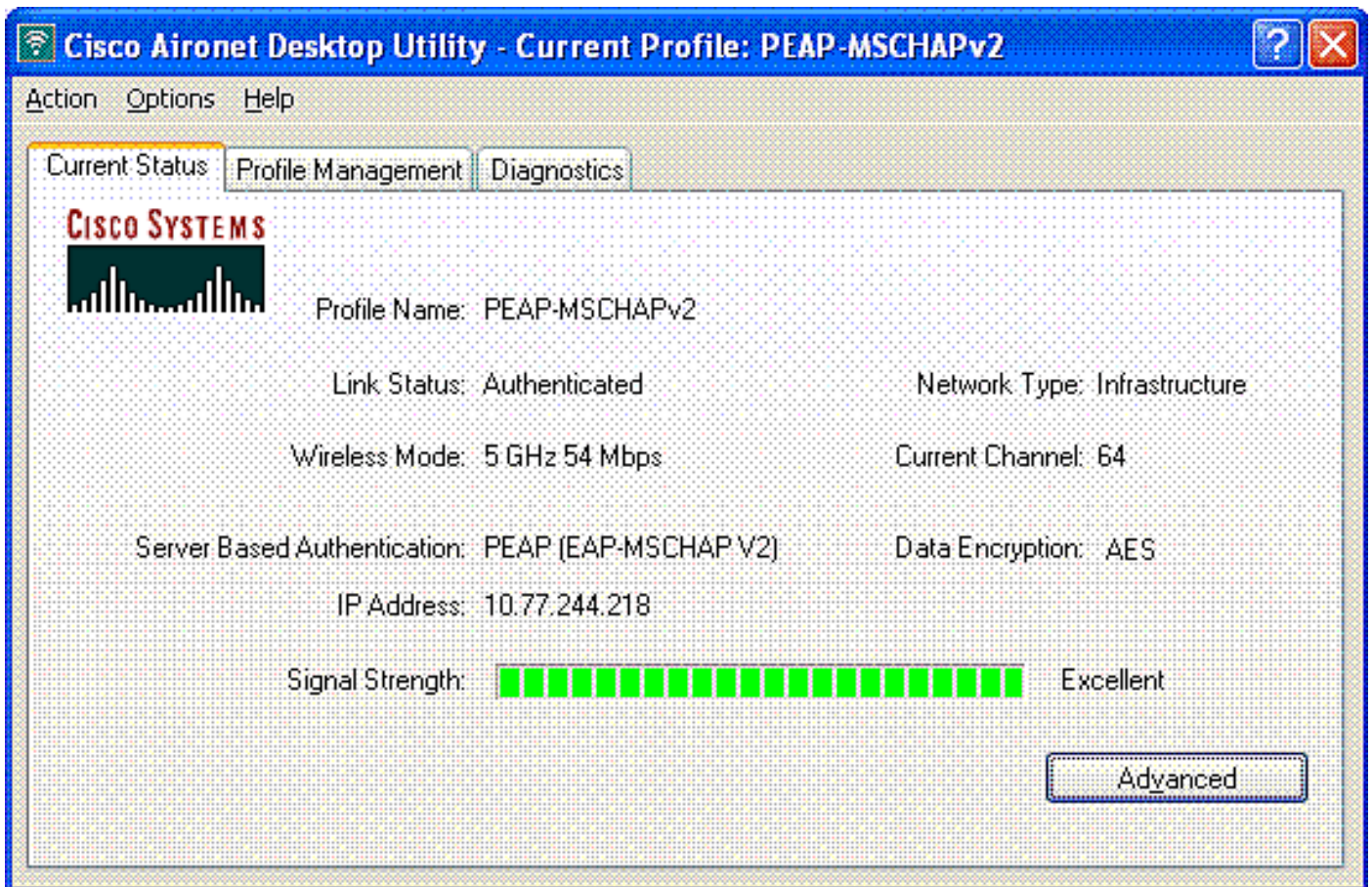
aus.

6. Klicken Sie auf **OK**, und aktivieren Sie das Profil. **Hinweis:** Wenn Sie das Protected EAP-Microsoft Challenge Handshake Authentication Protocol Version 2 (PEAP-MSCHAPv2) mit Microsoft XP SP2 verwenden und die Wireless-Karte von Microsoft Wireless Zero Configuration (WZC) verwaltet wird, müssen Sie den Microsoft Hotfix KB885453 anwenden. Dadurch werden mehrere Authentifizierungsprobleme im Zusammenhang mit PEAP Fast Resume vermieden.

## Überprüfung und Fehlerbehebung

Um zu überprüfen, ob die Konfiguration wie erwartet funktioniert, aktivieren Sie das Profil PEAP-MSCHAPv2 auf dem Wireless-Client Client1.





Sobald das Profil PEAP-MSCHAPv2 auf der ADU aktiviert ist, führt der Client die offene 802.11-Authentifizierung durch und führt dann die PEAP-MSCHAPv2-Authentifizierung durch. Hier ist ein Beispiel für eine erfolgreiche PEAP-MSCHAPv2-Authentifizierung.

Verwenden Sie die Befehle `debug`, um die Reihenfolge der auftretenden Ereignisse zu ermitteln.

Das [Output Interpreter-Tool](#) (OIT) ([nur](#) registrierte Kunden) unterstützt bestimmte `show`-Befehle. Verwenden Sie das OIT, um eine Analyse der `show`-Befehlsausgabe anzuzeigen.

Diese Befehle zum Debuggen auf dem Wireless LAN Controller sind nützlich.

- **debug dot1x events enable** - Zum Konfigurieren des Debuggens von 802.1x-Ereignissen
- **debug aaa events enable** - Konfigurieren des Debuggens von AAA-Ereignissen
- **debug mac addr <mac-Adresse>** - Um das MAC-Debugging zu konfigurieren, verwenden Sie den Befehl `debug mac`.
- **debug dhcp message enable** - Um das Debugging von DHCP-Fehlermeldungen zu konfigurieren

Dies sind die Beispielausgaben des Befehls `debug dot1x events enable` und des Befehls `debug client <mac address>`.

**debug dot1x events enable:**

```
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received EAPOL START from
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Sending EAP-Request/Identity to
mobile 00:40:96:ac:e6:57 (EAP Id 2)
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received Identity Response (count=2) from
mobile 00:40:96:ac:e6:57
```



Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending EAP-Success to mobile 00:40:96:ac:e6:57 (EAP Id 13)**  
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending default RC4 key to mobile 00:40:96:ac:e6:57**  
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending Key-Mapping RC4 key to mobile 00:40:96:ac:e6:57**  
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Received Auth Success while in Authenticating state for mobile 00:40:96:ac:e6:57**

**debug mac addr <MAC-Adresse>:**

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Association received from mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0**  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 STA: 00:40:96:ac:e6:57 - rates (8): 12 18 24 36 48 72 96 108 0 0 0 0 0 0  
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 RUN (20) Change state to START (0)**  
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0) Initializing policy**  
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0) Change state to AUTHCHECK (2)**  
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 AUTHCHECK (2) Change state to 8021X\_REQD (3)**  
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 8021X\_REQD (3)**  
Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Changing state for mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated**  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Stopping deletion of Mobile Station: 00:40:96:ac:e6:57 (callerId: 48)  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending Assoc Response to station 00:40:96:ac:e6:57 on BSSID 00:0b:85:51:5a:e0 (status 0)  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Changing state for mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 Removed NPU entry.  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 dot1x - moving mobile 00:40:96:ac:e6:57 into Connecting state  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Sending EAP-Request/Identity to mobile 00:40:96:ac:e6:57 (EAP Id 1)**  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Received EAPOL START from mobile 00:40:96:ac:e6:57**  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **EAP State update from Connecting to Authenticating for mobile 00:40:96:ac:e6:57**  
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 dot1x - moving mobile 00:40:96:ac:e6:57 into Authenticating state**  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Processing Access-Challenge for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Req state (id=3) for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
**Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 3)**  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
**Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25)**  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Processing Access-Challenge for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Req state (id=4) for mobile 00:40:96:ac:e6:57  
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 4)

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25)

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Req state (id=5) for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 5)

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25)

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Req state (id=6) for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57  
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6)

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25)

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Req state (id=10) for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10)

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25)

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Req state (id=11) for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
**Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 11)**

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
**Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25)**

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
**Processing Access-Accept for mobile 00:40:96:ac:e6:57**

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
**Creating a new PMK Cache Entry for station 00:40:96:ac:e6:57 (RSN 0)**

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
**Sending EAP-Success to mobile 00:40:96:ac:e6:57 (EAP Id 12)**

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
**Sending default RC4 key to mobile 00:40:96:ac:e6:57**

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57  
**Sending Key-Mapping RC4 key to mobile 00:40:96:ac:e6:57**

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218  
8021X\_REQD (3) **Change state to L2AUTHCOMPLETE (4)**

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218  
L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218  
L2AUTHCOMPLETE (4) Change state to RUN (20)

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN  
(20) Reached PLUMBFASPATH: from line 4041

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN  
(20) Replacing Fast Path rule

```
type = Airespace AP Client
on AP 00:0b:85:51:5a:e0, slot 0, interface = 2
ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20)
Card = 0 (slot 0), InHandle = 0x00000000,
OutHandle = 0x00000000, npuCryptoFlag = 0x0000
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Successfully plumbed mobile rule (ACL ID 255)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Reached RETURN: from line 4041
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend
Auth Success state (id=12) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Received Auth Success
while in Authenticating state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 dot1x -
moving mobile 00:40:96:ac:e6:57 into Authenticated state
```

**Hinweis:** Wenn Sie die Microsoft-Komponente zur Authentifizierung mit einem Cisco Secure ACS für die PEAP-Authentifizierung verwenden, führt der Client möglicherweise keine erfolgreiche Authentifizierung durch. Manchmal kann sich die erste Verbindung erfolgreich authentifizieren, aber spätere Fast-Connect-Authentifizierungsversuche führen nicht zu einer erfolgreichen Verbindung. Dies ist ein bekanntes Problem. Die Details zu diesem Problem und die entsprechende Behebung finden Sie [hier](#) .

## Zugehörige Informationen

- [PEAP unter Unified Wireless Networks mit ACS 4.0 und Windows 2003](#)
- [EAP-Authentifizierung mit WLAN-Controllern \(WLC\) - Konfigurationsbeispiel](#)
- [Wireless LAN Controller \(WLC\) Software-Upgrade auf die Versionen 3.2, 4.0 und 4.1](#)
- [Konfigurationsleitfäden für Cisco Wireless LAN Controller der Serie 4400](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

## 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.