

EAP-TLS unter Unified Wireless Network mit ACS 4.0 und Windows 2003

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Netzwerkdiagramm](#)

[Konventionen](#)

[Windows Enterprise 2003-Setup mit IIS, Certificate Authority, DNS, DHCP \(DC CA\)](#)

[DC CA \(Wireless-Demo\)](#)

[Windows Standard 2003-Setup mit Cisco Secure ACS 4.0](#)

[Grundlegende Installation und Konfiguration](#)

[Installation von Cisco Secure ACS 4.0](#)

[Konfiguration des Cisco LWAPP-Controllers](#)

[Erstellen der erforderlichen Konfiguration für WPA2/WPA](#)

[EAP-TLS-Authentifizierung](#)

[Installieren des Snap-Ins für Zertifikatsvorlagen](#)

[Erstellen der Zertifikatsvorlage für den ACS-Webserver](#)

[Aktivieren der Zertifikatsvorlage für den neuen ACS-Webserver](#)

[ACS 4.0 Zertifikateinrichtung](#)

[Exportfähiges Zertifikat für ACS konfigurieren](#)

[Installieren des Zertifikats in der ACS 4.0-Software](#)

[CLIENT-Konfiguration für EAP-TLS mit Windows Zero Touch](#)

[Durchführen einer grundlegenden Installation und Konfiguration](#)

[Konfigurieren der Wireless-Netzwerkverbindung](#)

[Zugehörige Informationen](#)

[Einführung](#)

In diesem Dokument wird beschrieben, wie Sie den sicheren Wireless-Zugriff mithilfe von Wireless LAN-Controllern (WLCs), der Microsoft Windows 2003-Software und dem Cisco Secure Access Control Server (ACS) 4.0 über Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) konfigurieren.

Hinweis: Weitere Informationen zur Bereitstellung sicherer Wireless-Netzwerke finden Sie auf der [Microsoft Wi-Fi-Website](#) und im [Cisco SAFE Wireless Blueprint](#).

[Voraussetzungen](#)

Anforderungen

Es wird davon ausgegangen, dass das Installationsprogramm über Kenntnisse der grundlegenden Installation von Windows 2003 und der Installation des Cisco Controllers verfügt, da dieses Dokument nur die spezifischen Konfigurationen behandelt, die die Tests erleichtern sollen.

Informationen zur Erstinstallation und Konfiguration der Cisco Controller der Serie 4400 finden Sie in der [Schnellstartanleitung: Cisco Wireless LAN Controller der Serie 4400](#). Informationen zur Erstinstallation und Konfiguration der Cisco Controller der Serie 2000 finden Sie in der [Schnellstartanleitung: Cisco Wireless LAN Controller der Serie 2000](#).

Bevor Sie beginnen, installieren Sie Windows Server 2003 mit Service Pack (SP)1 auf jedem Server im Testlabor und aktualisieren Sie alle Service Packs. Installieren Sie die Controller und APs, und stellen Sie sicher, dass die neuesten Software-Updates konfiguriert sind.

Wichtig: Zum Zeitpunkt der Erstellung dieses Dokuments war SP1 das neueste Windows Server 2003-Update und SP2 mit Update-Patches die neueste Software für Windows XP Professional.

Windows Server 2003 mit SP1, Enterprise Edition, wird verwendet, um die automatische Registrierung von Benutzer- und Workstation-Zertifikaten für die EAP-TLS-Authentifizierung zu konfigurieren. Dies wird im Abschnitt [EAP-TLS-Authentifizierung](#) dieses Dokuments beschrieben. Die automatische Registrierung von Zertifikaten und die automatische Verlängerung von Zertifikaten vereinfachen die Bereitstellung von Zertifikaten und erhöhen die Sicherheit, indem Zertifikate automatisch ablaufen und erneuert werden.

Verwendete Komponenten

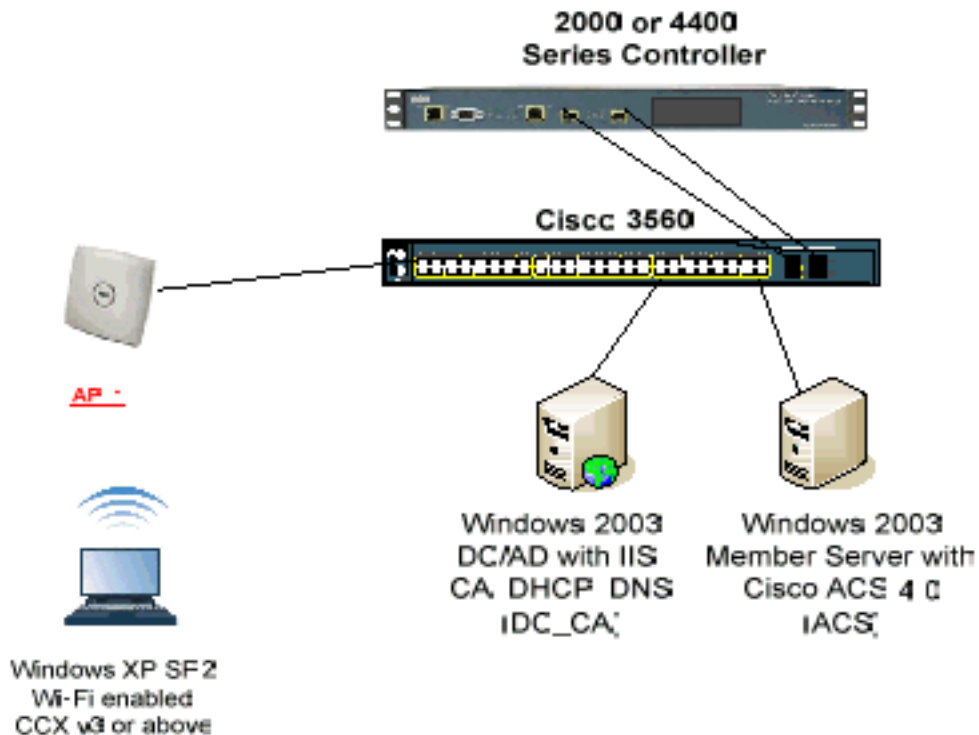
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Controller der Serie 2006 oder 4400 mit 3.2.116.21
- Cisco 1131 LWAPP AP (Lightweight Access Point Protocol)
- Windows 2003 Enterprise mit installiertem Internet Information Server (IIS), Certificate Authority (CA), DHCP und Domain Name System (DNS)
- Windows 2003 Standard mit Access Control Server (ACS) 4.0
- Windows XP Professional mit SP (und aktualisierten Service Packs) und Wireless-Netzwerkschnittstellenkarte (NIC) (mit CCX v3-Unterstützung) oder Drittanbieter-Komponente.
- Cisco 3560-Switch

Netzwerkdigramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:

Cisco Secure Wireless Lab-Topologie



Dieses Dokument enthält in erster Linie eine schrittweise Anleitung zur Implementierung des EAP-TLS unter Unified Wireless Networks mit ACS 4.0 und dem Windows 2003 Enterprise-Server. Der Schwerpunkt liegt auf der automatischen Registrierung des Clients, sodass der Client sich automatisch anmeldet und das Zertifikat vom Server bezieht.

Hinweis: Wenn Sie Windows XP Professional mit SP um WiFi Protected Access (WPA)/WPA2 mit Temporal Key Integrity Protocol (TKIP)/Advanced Encryption Standard (AES) erweitern möchten, lesen Sie das [WPA2/Wireless Provisioning Services Information Element \(WPS IE\)-Update für Windows XP mit SP2](#).

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 in den [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

Windows Enterprise 2003-Setup mit IIS, Certificate Authority, DNS, DHCP (DC_CA)

DC_CA (Wireless-Demo)

DC_CA ist ein Computer, der Windows Server 2003 mit SP1, Enterprise Edition ausführt und folgende Rollen ausführt:

- Ein Domänencontroller für die Wirelessdemo.local-Domäne, die IIS ausführt
- Ein DNS-Server für die Wirelessdemo.local DNS-Domäne
- Ein DHCP-Server
- Enterprise-Root-CA für die WirelessDemo.Local-Domäne

Gehen Sie wie folgt vor, um DC_CA für diese Services zu konfigurieren:

1. [Durchführen einer grundlegenden Installation und Konfiguration](#)
2. [Konfigurieren Sie den Computer als Domänen-Controller.](#)
3. [Heben Sie die Funktionsstufe der Domäne an.](#)
4. [Installieren und konfigurieren Sie DHCP.](#)
5. [Installieren Sie Zertifikatsdienste.](#)
6. [Überprüfen Sie die Administratorberechtigungen für Zertifikate.](#)
7. [Hinzufügen von Computern zur Domäne.](#)
8. [Ermöglichen Sie den Wireless-Zugriff auf Computer.](#)
9. [Fügen Sie der Domäne Benutzer hinzu.](#)
10. [Wireless-Zugriff für Benutzer zulassen.](#)
11. [Fügen Sie der Domäne Gruppen hinzu.](#)
12. [Fügen Sie Benutzer zur WirelessUsers-Gruppe hinzu.](#)
13. [Fügen Sie der WirelessUsers-Gruppe Clientcomputer hinzu.](#)

Schritt 1: Grundlegende Installation und Konfiguration

Führen Sie diese Schritte aus:

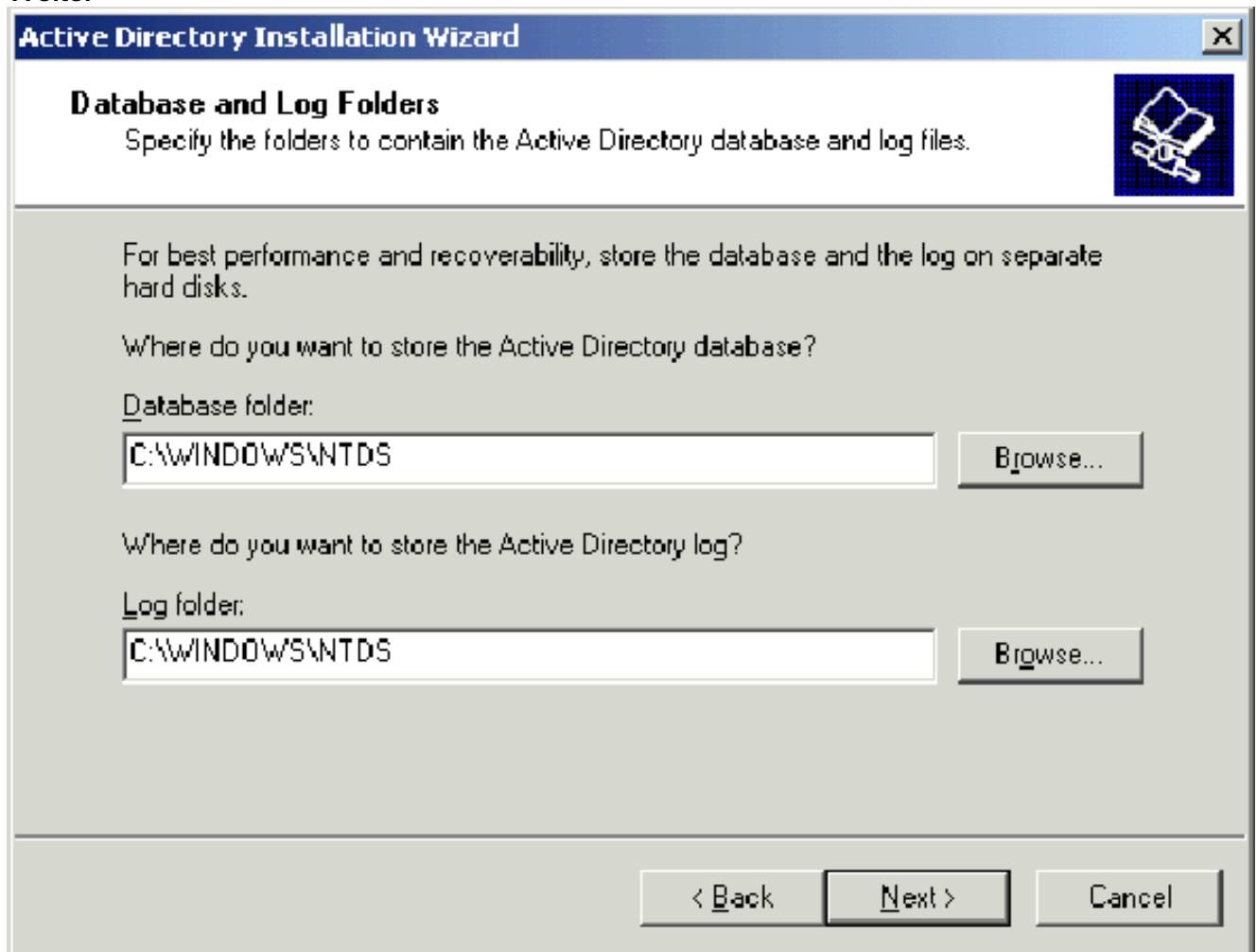
1. Installieren Sie Windows Server 2003 mit SP1, Enterprise Edition als eigenständiger Server.
2. Konfigurieren Sie das TCP/IP-Protokoll mit der IP-Adresse 172.16.100.26 und der Subnetzmaske 255.255.255.0.

Schritt 2: Konfigurieren des Computers als Domänen-Controller

Führen Sie diese Schritte aus:

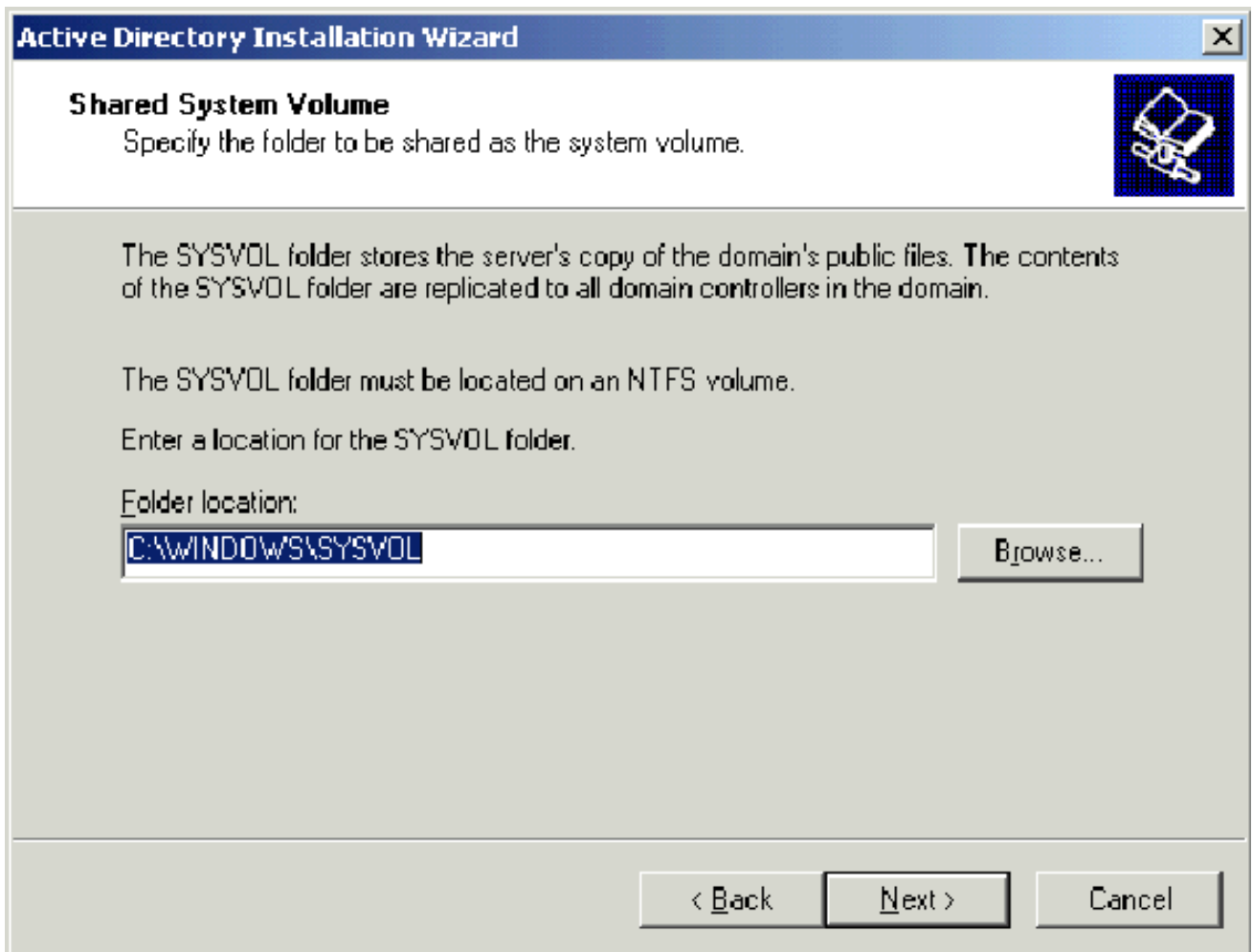
1. Um den Active Directory-Installationsassistenten zu starten, wählen Sie **Start > Ausführen**, geben Sie **dcpromo.exe ein**, und klicken Sie auf **OK**.
2. Klicken Sie auf der Seite Willkommen beim Assistenten zur Active Directory-Installation auf **Weiter**.
3. Klicken Sie auf der Seite Betriebssystemkompatibilität auf **Weiter**.
4. Wählen Sie auf der Seite Domain Controller Type (Domänencontrollertyp) die Option **Domain Controller (Domänencontroller) für eine neue Domäne aus**, und klicken Sie auf **Next (Weiter)**.
5. Wählen Sie auf der Seite Neue Domäne erstellen die Option **Domäne in einem neuen Wald aus**, und klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite DNS installieren oder konfigurieren die Option **Nein, installieren und konfigurieren Sie DNS auf diesem Computer** und klicken Sie auf **Weiter**.
7. Geben Sie auf der Seite Neuer Domänenname **wirelessDemo.local ein**, und klicken Sie auf **Weiter**.

8. Geben Sie auf der Seite NetBIOS Domain Name (NetBIOS-Domänenname) den Domain NetBIOS-Namen als **WirelessDemo ein**, und klicken Sie auf **Next (Weiter)**.
9. Akzeptieren Sie auf der Seite Speicherort von Datenbank- und Protokollordnern die Standardverzeichnisse für Datenbank- und Protokollordner, und klicken Sie auf **Weiter**.

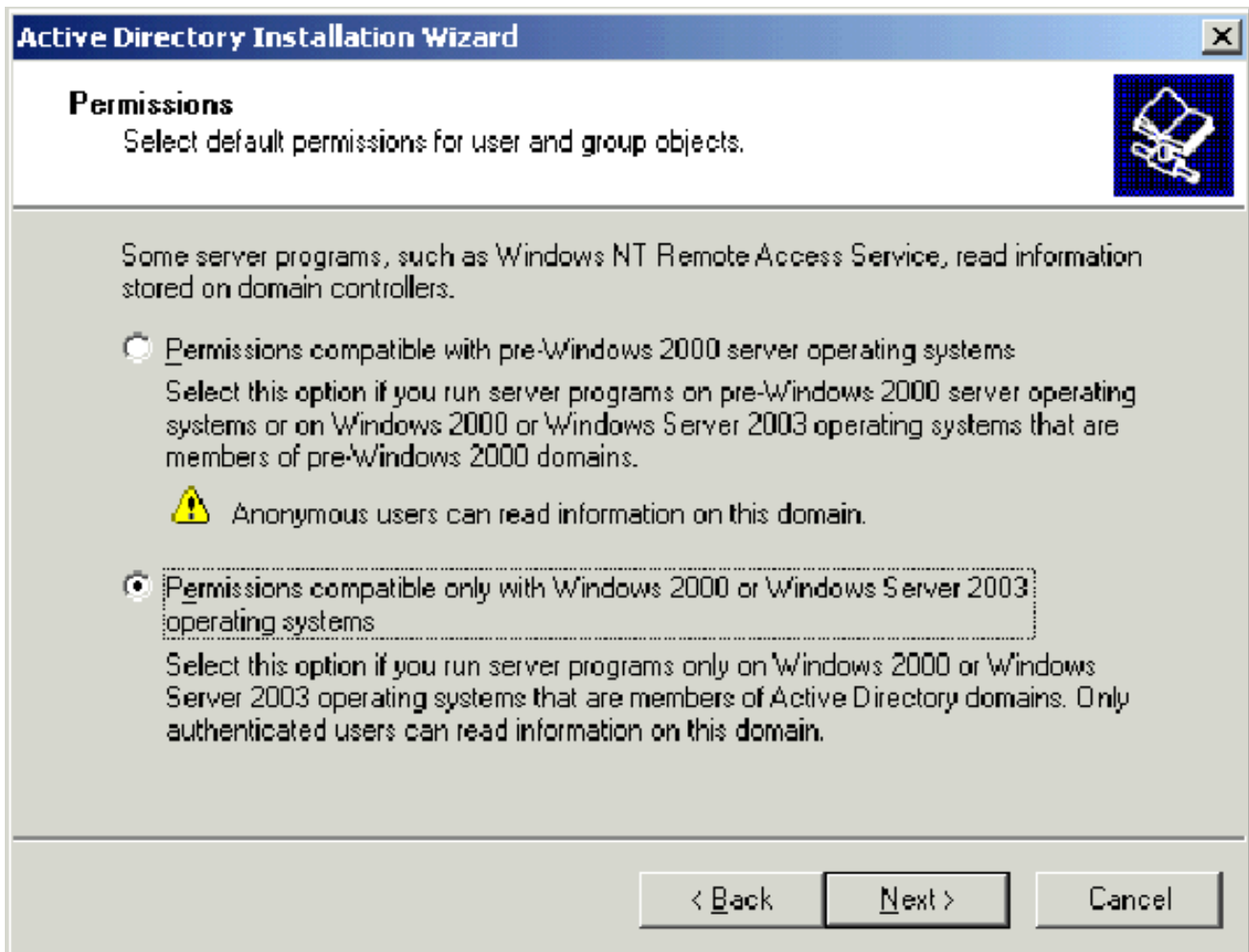


The screenshot shows a Windows dialog box titled "Active Directory Installation Wizard". The main heading is "Database and Log Folders" with a sub-instruction: "Specify the folders to contain the Active Directory database and log files." Below this, there is a note: "For best performance and recoverability, store the database and the log on separate hard disks." The first question is "Where do you want to store the Active Directory database?" with a text input field containing "C:\WINDOWS\NTDS" and a "Browse..." button. The second question is "Where do you want to store the Active Directory log?" with a text input field containing "C:\WINDOWS\NTDS" and a "Browse..." button. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

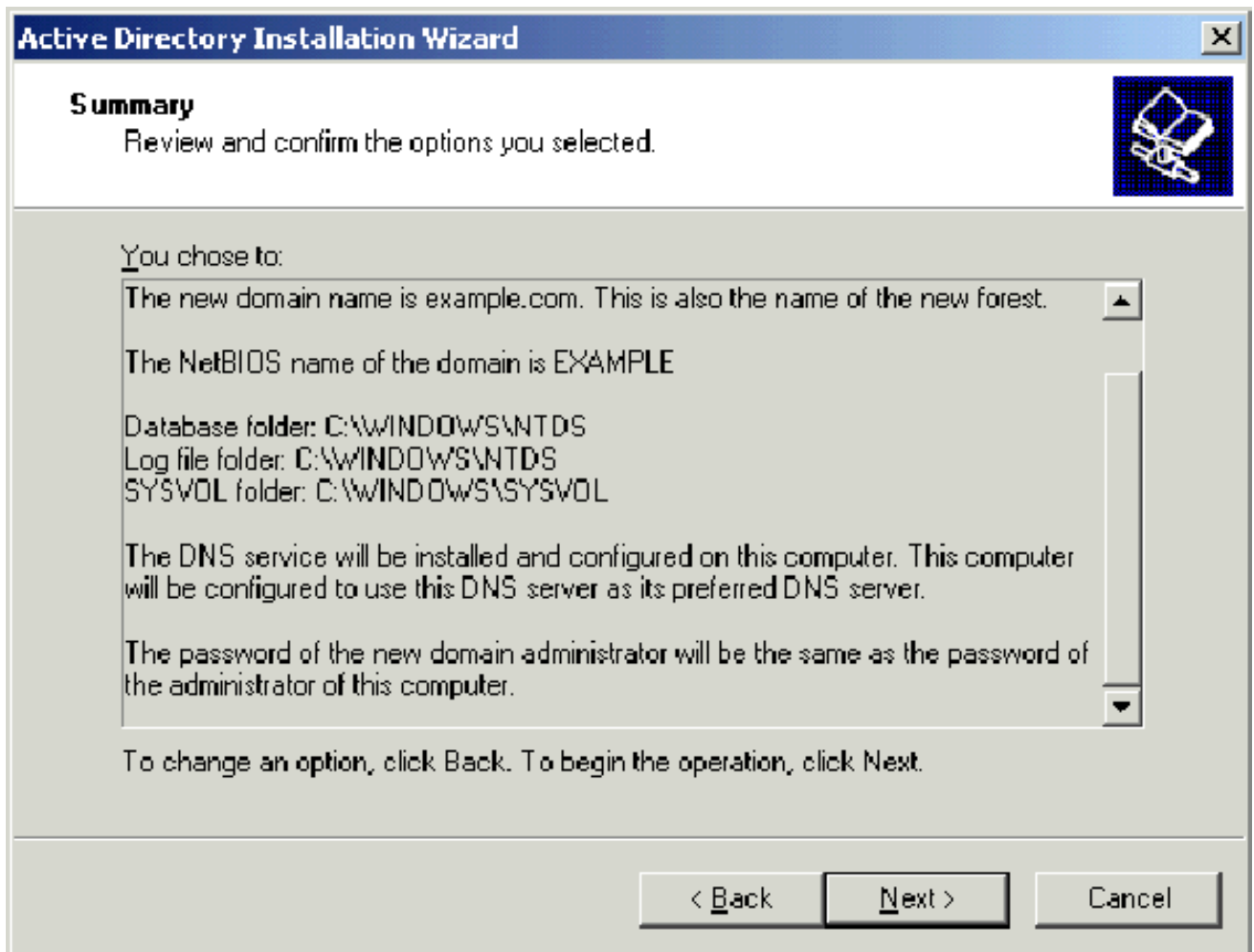
10. Überprüfen Sie im Dialogfeld Freigegebene Systemlautstärke, ob der Standardordner richtig ist, und klicken Sie auf **Weiter**.



11. Überprüfen Sie auf der Seite "Berechtigungen", ob **Berechtigungen, die nur mit Windows 2000- oder Windows Server 2003-Betriebssystemen kompatibel sind**, ausgewählt sind, und klicken Sie auf **Weiter**.



12. Lassen Sie auf der Seite Administratormodus-Administratorkennwort für die Verzeichnisdienste die Kennwortfelder leer, und klicken Sie auf **Weiter**.
13. Überprüfen Sie die Informationen auf der Seite Übersicht, und klicken Sie auf **Weiter**.

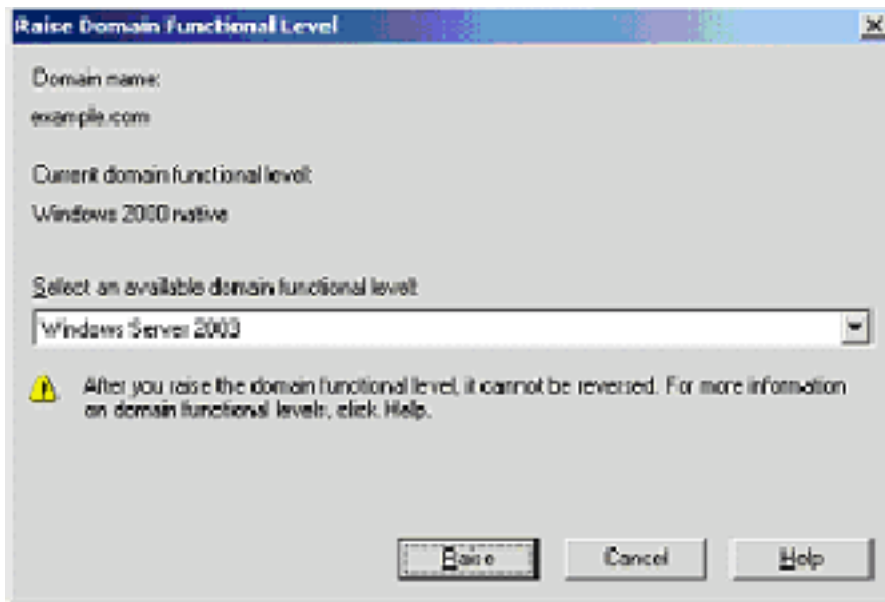


14. Klicken Sie auf der Seite Complete the Active Directory Installation Wizard (Assistent zur Durchführung der Active Directory-Installation) auf **Fertig stellen**.
15. Wenn Sie aufgefordert werden, den Computer neu zu starten, klicken Sie auf **Jetzt neu starten**.

Schritt 3: Erweitern der Domänenfunktionsebene

Führen Sie diese Schritte aus:

1. Öffnen Sie das Snap-In Active Directory Domains and Trusts im Ordner **Administrative Tools** (**Start > Verwaltung > Active Directory Domains and Trusts**), und klicken Sie dann mit der rechten Maustaste auf den Domänencomputer **DC_CA.wirelessdemo.local**.
2. Klicken Sie auf **Domänenfunktionsebene auslösen**, und wählen Sie dann **Windows Server 2003** auf der Seite Domänenfunktionsebene auslösen



aus.

3. Klicken Sie auf **Erhöhen**, klicken Sie auf **OK**, und klicken Sie dann erneut auf **OK**.

Schritt 4: Installieren und Konfigurieren von DHCP

Führen Sie diese Schritte aus:

1. Installieren Sie Dynamic Host Configuration Protocol (DHCP) als Netzwerkdienstkomponente, indem Sie in der Systemsteuerung **Software** verwenden.
2. Öffnen Sie das DHCP-Snap-In im Ordner Verwaltung (**Start > Programme > Verwaltung > DHCP**), und markieren Sie dann den DHCP-Server **DC_CA.wirelessdemo.local**.
3. Klicken Sie auf **Aktion** und dann auf **Autorisieren**, um den DHCP-Dienst zu autorisieren.
4. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **DC_CA.wirelessdemo.local**, und klicken Sie dann auf **Neuer Bereich**.
5. Klicken Sie auf der Willkommenseite des Assistenten für neue Bereiche auf **Weiter**.
6. Geben Sie auf der Seite Scope Name (Bereichsname) **CorpNet** im Feld Name ein.

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

7. Klicken Sie auf **Weiter**, und füllen Sie die folgenden Parameter aus: Start-IP-Adresse - 172.16.100.1 End IP address (Endadresse): 172.16.100.254 Länge: 24 Subnetzmaske: 255.255.255.0

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:

End IP address:

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:

Subnet mask:

< Back

Next >

Cancel

8. Klicken Sie auf **Next**, und geben Sie als Start-IP-Adresse **172.16.100.1** und als **End-IP-Adresse 172.16.100.100 ein**. Klicken Sie anschließend auf **Weiter**. Damit werden die IP-Adressen im Bereich von 172.16.100.1 bis 172.16.100.100 reserviert. Diese reservierten IP-Adressen werden vom DHCP-Server nicht zugewiesen.

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:

Excluded address range:

9. Klicken Sie auf der Seite Leasingdauer auf **Weiter**.
10. Wählen Sie auf der Seite DHCP-Optionen konfigurieren die Option **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

11. Fügen Sie auf der Seite Router (Default Gateway) (Router (Standard-Gateway) die Standardadresse des Routers **172.16.100.1** hinzu, und klicken Sie auf **Weiter**.

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

12. Geben Sie auf der Seite Domain Name and DNS Servers (Domänenname und DNS-Server) **wirelessdemo.local** in das Feld Parent domain (Übergeordnete Domäne) ein, geben Sie **172.16.100.26** in das Feld IP-Adresse ein, und klicken Sie dann auf **Hinzufügen** und dann auf **Weiter**.

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

172.16.100.26

Remove

Up

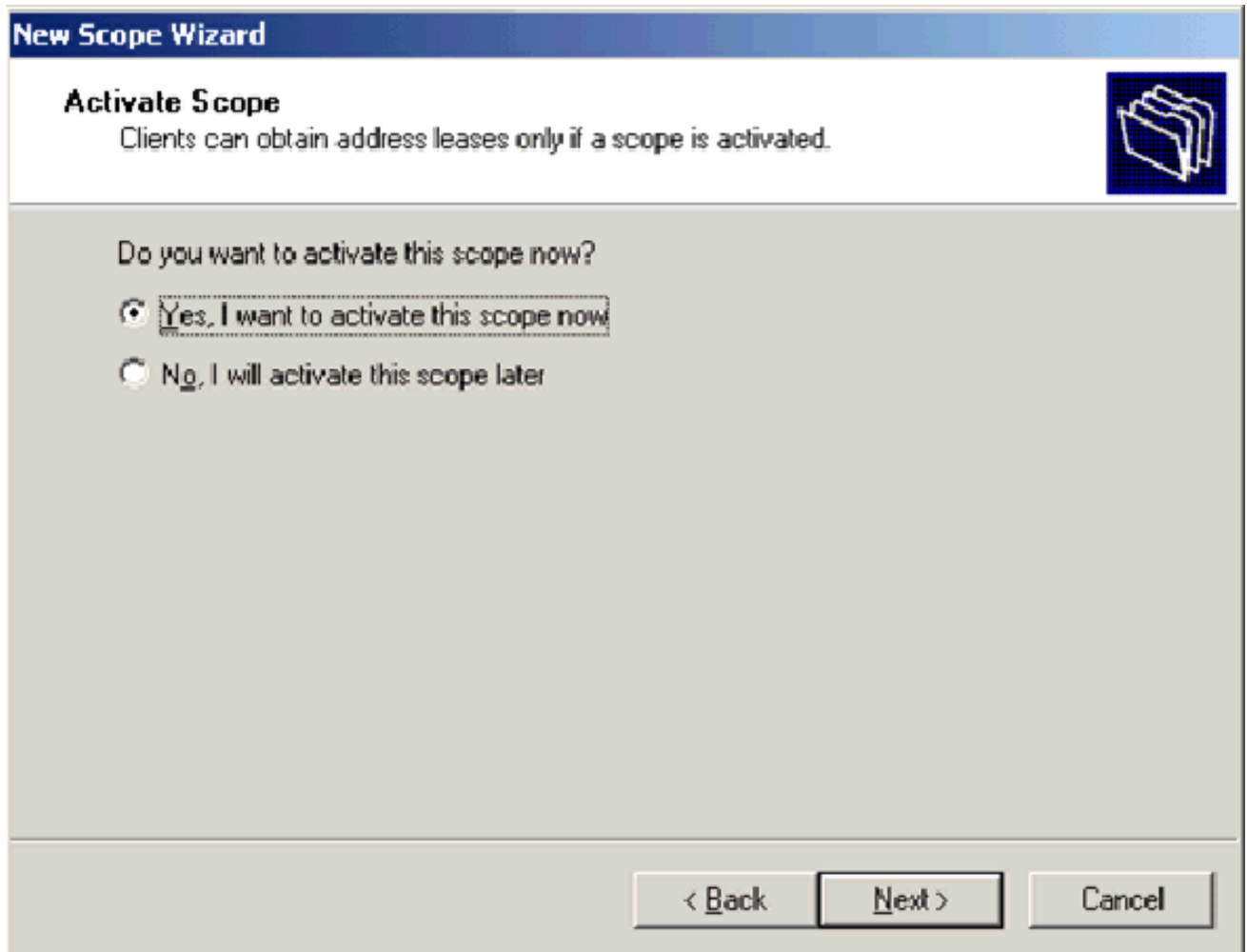
Down

< Back

Next >

Cancel

13. Klicken Sie auf der Seite WINS-Server auf **Weiter**.
14. Wählen Sie auf der Seite Scope (Bereich aktivieren) die Option **Yes (Ja)** aus. **Ich möchte diesen Bereich jetzt aktivieren** und klicken Sie auf **Next (Weiter)**.



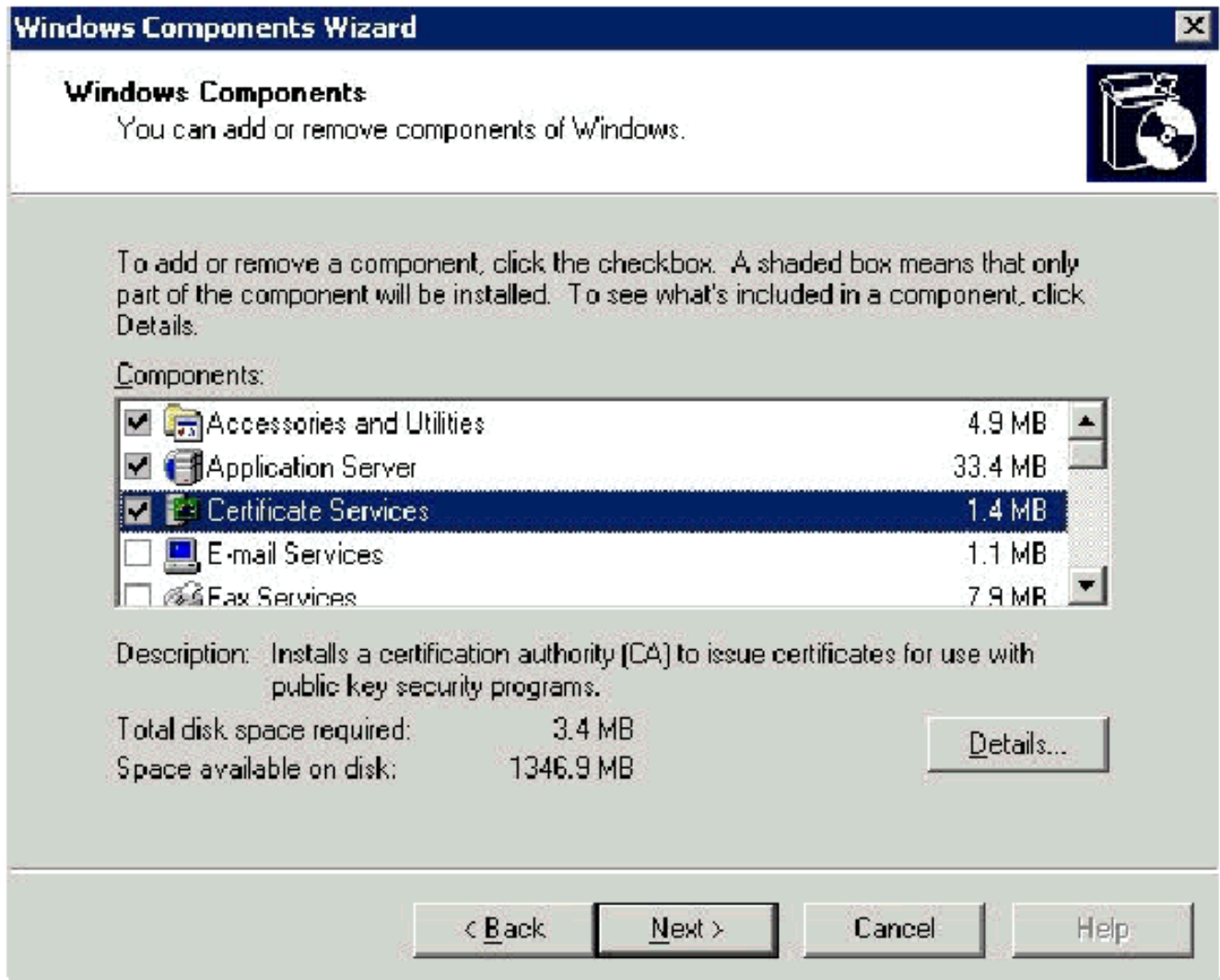
15. Klicken Sie auf der Seite Fertigstellen des Assistenten für neue Bereiche auf **Fertig stellen**.

[Schritt 5: Installieren von Zertifikatsdiensten](#)

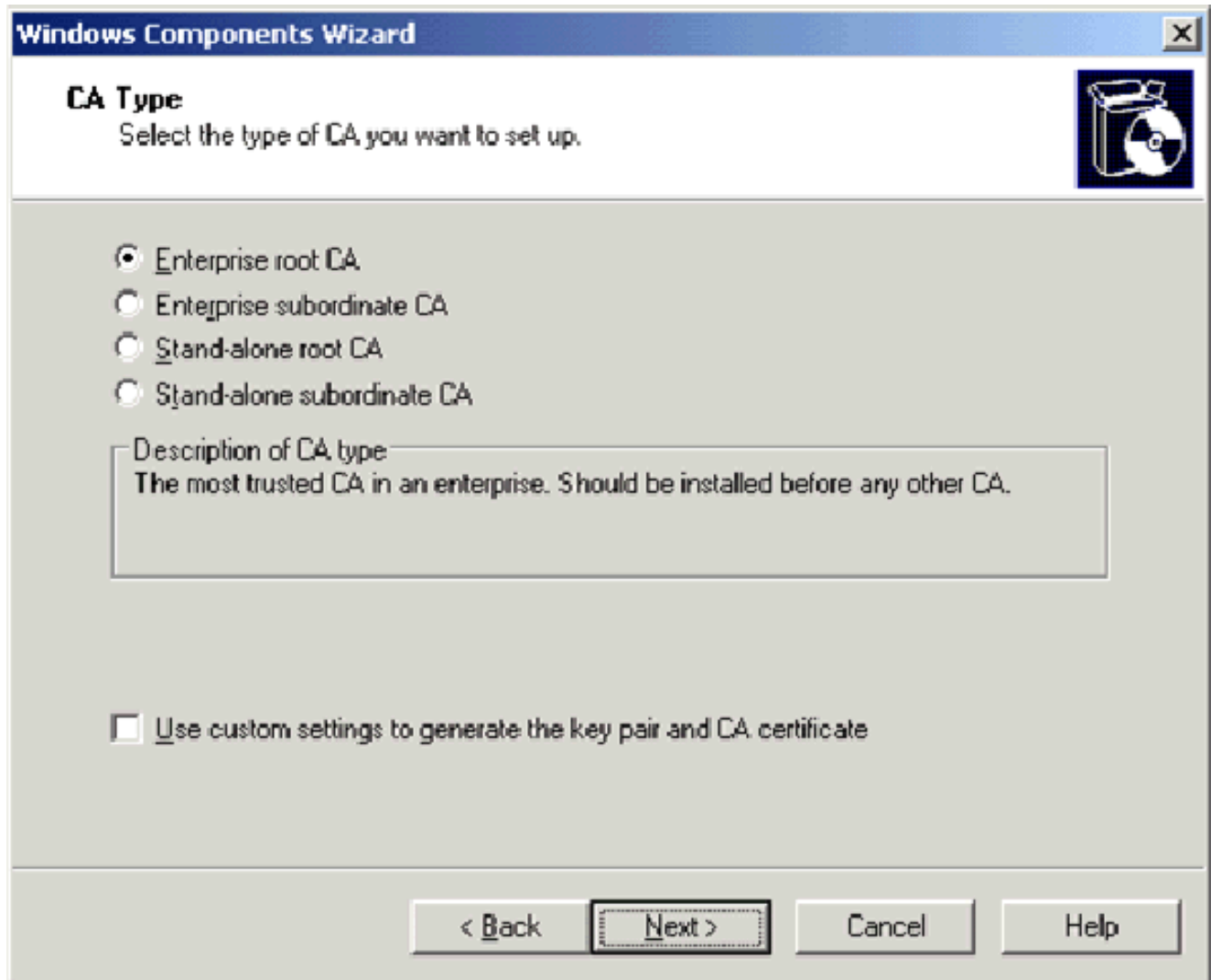
Führen Sie diese Schritte aus:

Hinweis: IIS muss installiert werden, bevor Sie Zertifikatsdienste installieren, und der Benutzer sollte Teil der Enterprise Admin-Organisationseinheit sein.

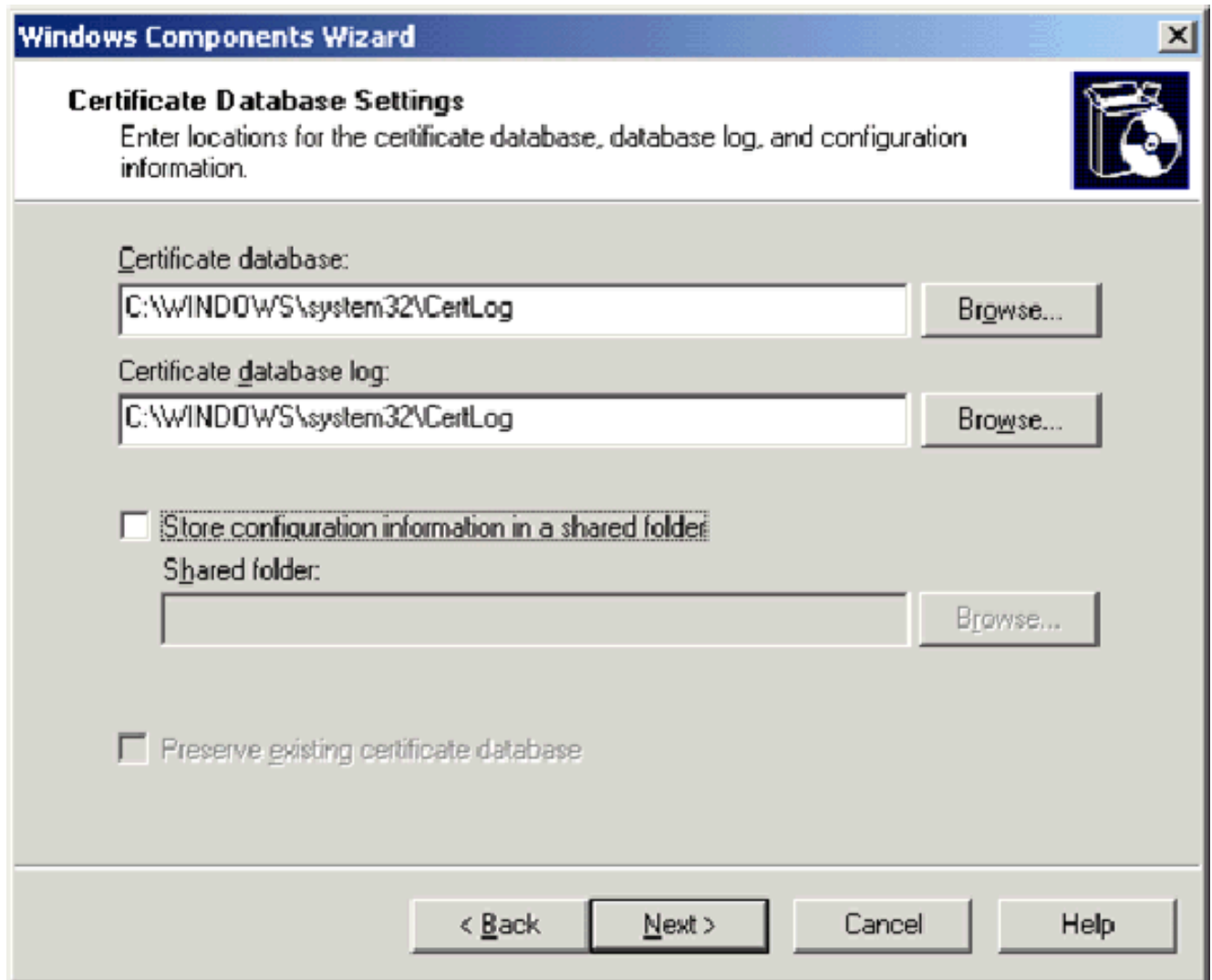
1. Öffnen Sie in der Systemsteuerung das **Applet Software** und klicken Sie dann auf **Windows-Komponenten hinzufügen/entfernen**.
2. Wählen Sie auf der Seite Assistent für Windows-Komponenten die Option **Zertifikatsdienste aus**, und klicken Sie dann auf **Weiter**.



3. Wählen Sie auf der Seite CA Type (CA-Typ) die **Enterprise Root CA** aus, und klicken Sie auf **Next (Weiter)**.



4. Geben Sie auf der Informationsseite zur CA-Identifizierung in das Feld Allgemeiner Name für diese CA Wireless **Demca** ein. Sie können die anderen optionalen Details eingeben und dann auf **Weiter** klicken. Akzeptieren Sie die Standardwerte auf der Seite Einstellungen für Zertifikatsdatenbank.

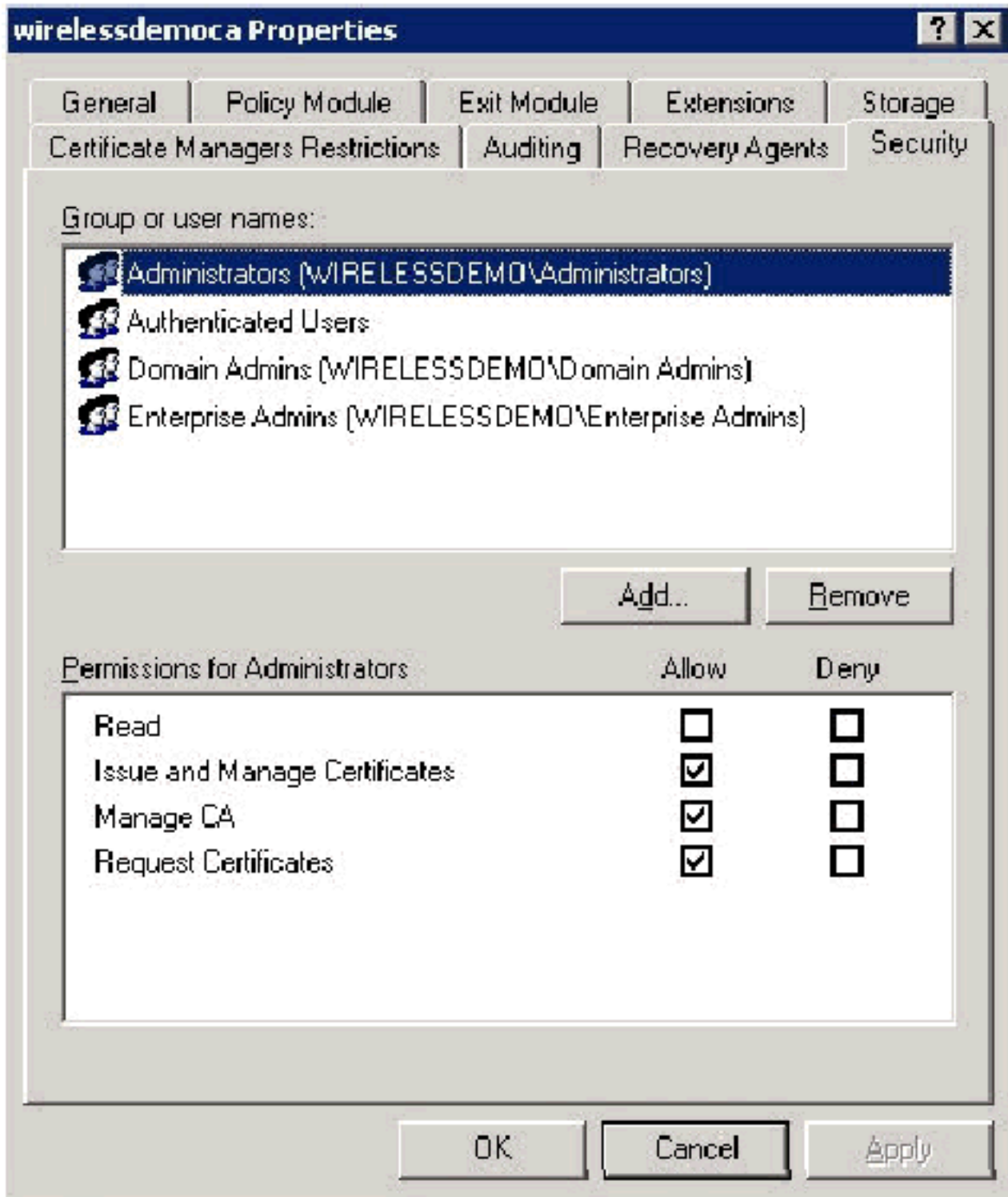


5. Klicken Sie auf **Weiter**. Klicken Sie nach Abschluss der Installation auf **Fertig stellen**.
6. Klicken Sie nach dem Lesen der Warnung über die Installation von IIS auf **OK**.

Schritt 6: Administratorberechtigungen für Zertifikate überprüfen

Führen Sie diese Schritte aus:

1. Wählen Sie **Start > Verwaltung > Zertifizierungsstelle** aus.
2. Klicken Sie mit der rechten Maustaste auf **WirelessDemo CA** und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf der Registerkarte Sicherheit in der Liste Gruppe oder Benutzernamen auf **Administratoren**.
4. Überprüfen Sie in der Liste Berechtigungen oder Administratoren, ob diese Optionen auf **Zulassen** festgelegt sind: Zertifikate ausstellen und verwalten, CA verwalten, Zertifikate anfordern. Wenn eine dieser Optionen auf Verweigern festgelegt ist oder nicht ausgewählt ist, legen Sie die Berechtigung auf **Zulassen** fest.



5. Klicken Sie auf **OK**, um das Dialogfeld Eigenschaften drahtloser democa CA zu schließen, und schließen Sie dann die Zertifizierungsstelle.

[Schritt 7: Hinzufügen von Computern zur Domäne](#)

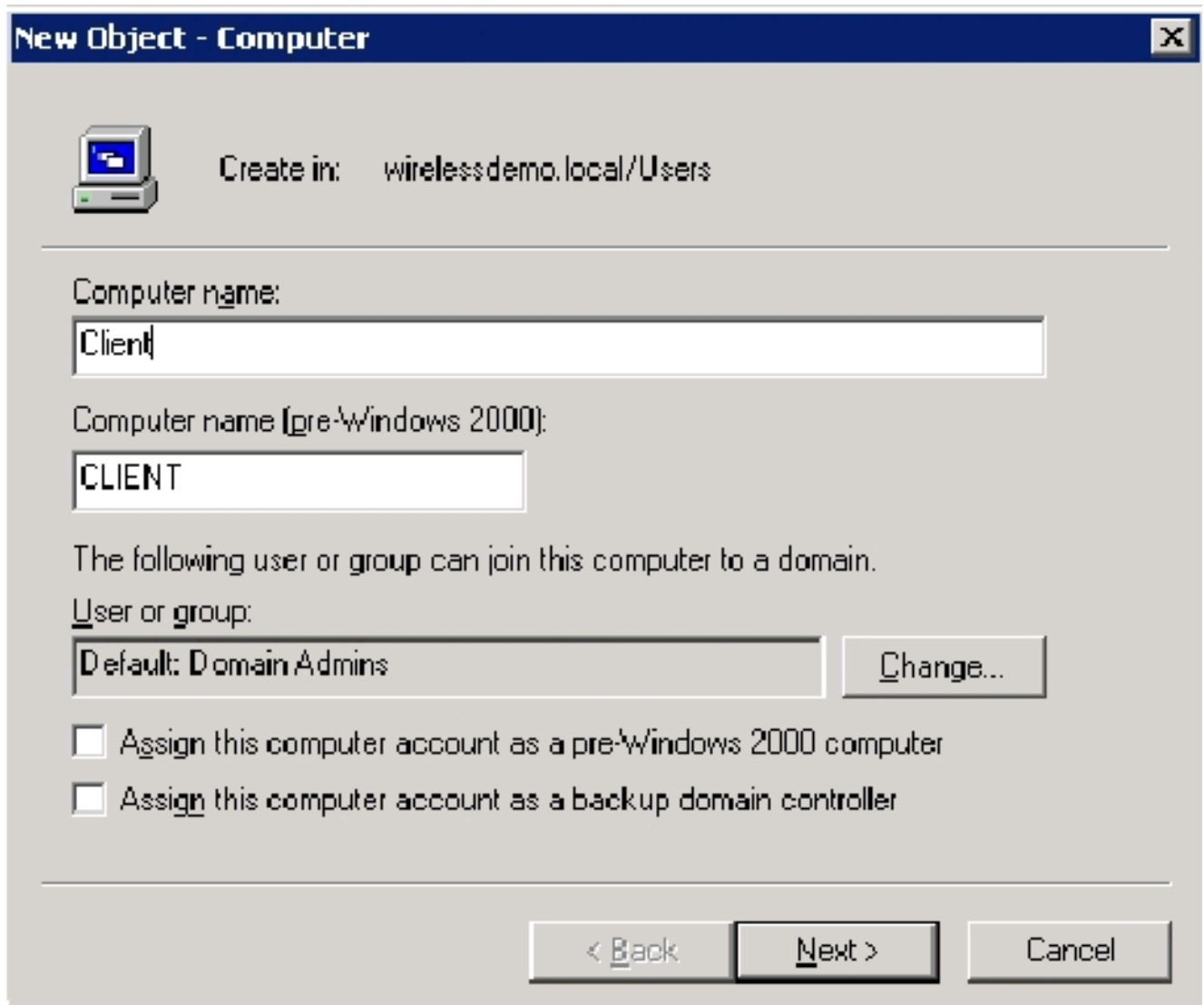
Führen Sie diese Schritte aus:

Hinweis: Wenn der Computer bereits zur Domäne hinzugefügt wurde, fahren Sie mit [Benutzer zur Domäne hinzufügen fort](#).

1. Öffnen Sie das Snap-In Active Directory-Benutzer und -Computer.
2. Erweitern Sie in der Konsolenstruktur die Option **wirelessDemo.local**.
3. Klicken Sie mit der rechten Maustaste auf **Benutzer**, klicken Sie auf **Neu**, und klicken Sie

dann auf **Computer**.

4. Geben Sie im Dialogfeld Neues Objekt - Computer den Namen des Computers in das Feld Computername ein, und klicken Sie auf **Weiter**. In diesem Beispiel wird der Computername **Client** verwendet.



5. Klicken Sie im Dialogfeld Verwaltete auf **Weiter**.
6. Klicken Sie im Dialogfeld Neuer Objektcomputer auf **Fertig stellen**.
7. Wiederholen Sie die Schritte 3 bis 6, um weitere Computerkonten zu erstellen.

[Schritt 8: Wireless-Zugriff auf Computer zulassen](#)

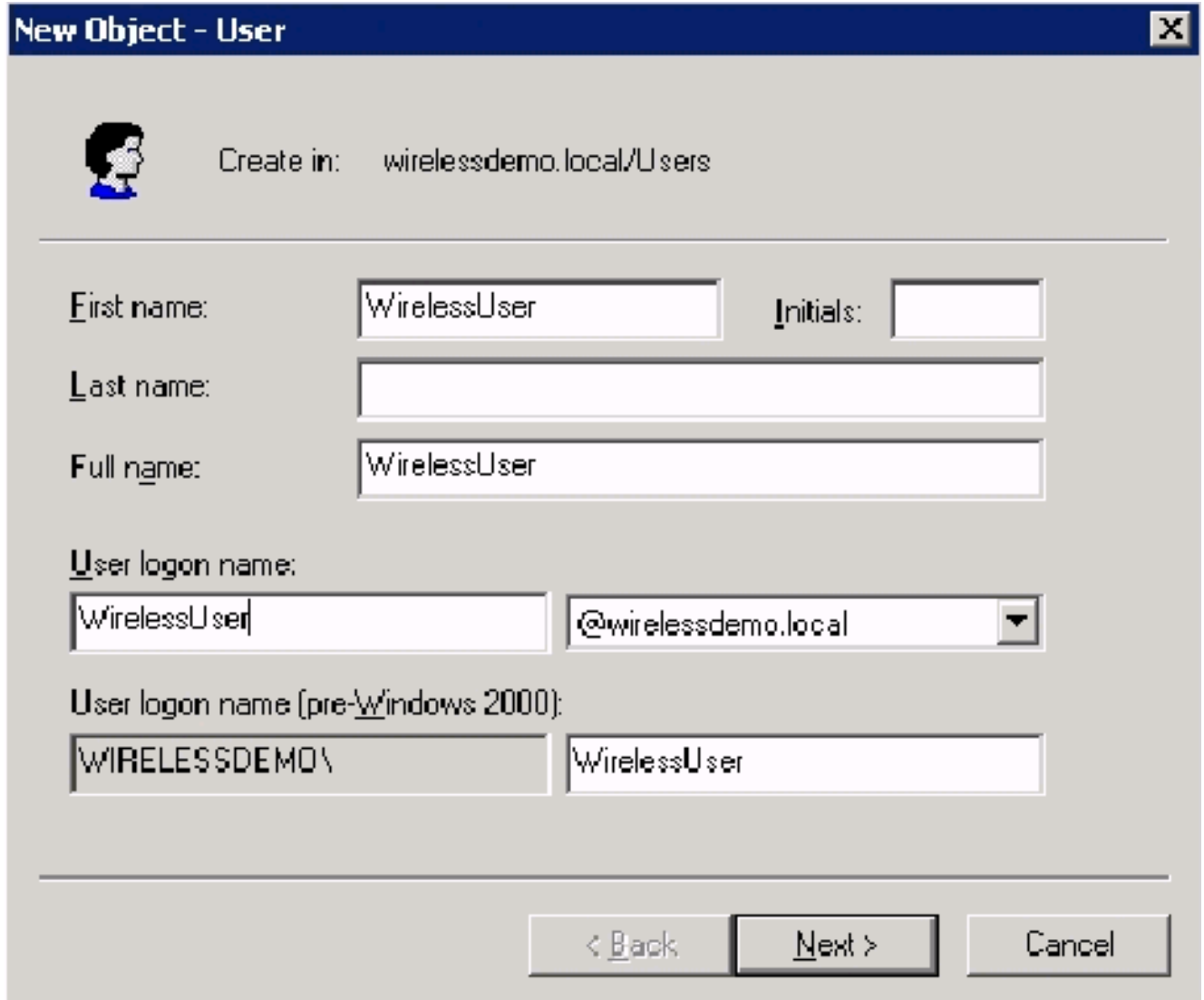
Führen Sie diese Schritte aus:

1. Klicken Sie in der Konsolenstruktur Active Directory Users and Computers (Active Directory-Benutzer und -Computer) auf den Ordner **Computers** und klicken Sie mit der rechten Maustaste auf den Computer, für den Sie den Wireless-Zugriff zuweisen möchten. In diesem Beispiel wird die Prozedur mit Computer **CLIENT** veranschaulicht, die Sie in Schritt 7 hinzugefügt haben.
2. Klicken Sie auf **Eigenschaften**, und wechseln Sie dann zur Registerkarte **Einwählen**.
3. Wählen Sie **Zugriff zulassen aus**, und klicken Sie auf **OK**.

Schritt 9: Hinzufügen von Benutzern zur Domäne

Führen Sie diese Schritte aus:

1. Klicken Sie in der Konsolenansicht 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 **WirelessUser** in das Feld Vorname ein, und geben Sie **WirelessUser** in das Feld Benutzername ein, und klicken Sie auf **Weiter**.



New Object - User

Create in: wirelessdemo.local/Users

First name: Initials:

Last name:

Full name:

User logon name:

User logon name (pre-Windows 2000):

< Back Next > Cancel

3. Geben Sie im Dialogfeld Neues Objekt - Benutzer in die Felder Kennwort und Kennwort bestätigen ein beliebiges Kennwort ein. Deaktivieren Sie das Kontrollkästchen **Benutzer muss Kennwort bei der nächsten Anmeldung ändern**, und klicken Sie auf **Weiter**.

New Object - User

Create in: wirelessdemo.local/Users

Password: [.....]

Confirm password: [.....|]

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back Next > Cancel

4. Klicken Sie im Dialogfeld Neues Objekt - Benutzer auf **Fertig stellen**.
5. Wiederholen Sie die Schritte 2 bis 4, um weitere Benutzerkonten zu erstellen.

[Schritt 10: Wireless-Zugriff für Benutzer zulassen](#)

Führen Sie diese Schritte aus:

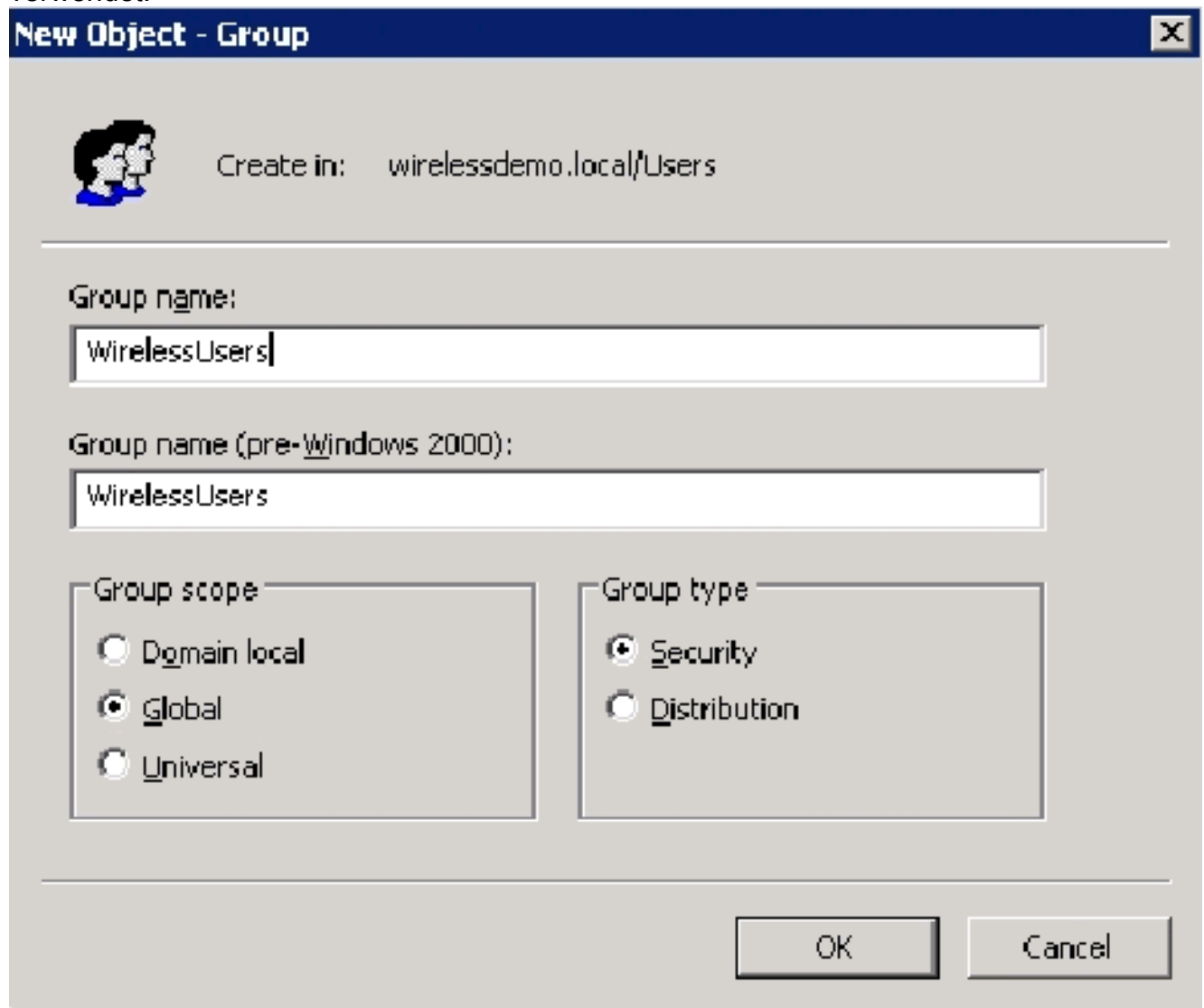
1. Klicken Sie in der Konsolenansicht von Active Directory Users and Computers auf den Ordner **Users**, klicken Sie mit der rechten Maustaste auf **WirelessUser**, klicken Sie auf **Eigenschaften**, und wechseln Sie dann zur Registerkarte Dial-in (Einwählen).
2. Wählen Sie **Zugriff zulassen aus**,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

[Schritt 11: Hinzufügen von Gruppen zur Domäne](#)

Führen Sie diese Schritte aus:

1. Klicken Sie in der Konsolenstruktur von Active Directory-Benutzern und -Computern mit der rechten Maustaste auf **Benutzer**, klicken Sie auf **Neu**, und klicken Sie dann auf **Gruppe**.
2. Geben Sie im Dialogfeld Neues Objekt - Gruppe im Feld Gruppenname den Namen der Gruppe ein, und klicken Sie auf **OK**. In diesem Dokument wird der Gruppenname **WirelessUsers**

verwendet.



New Object - Group

Create in: wirelessdemo.local/Users

Group name:
WirelessUsers

Group name (pre-Windows 2000):
WirelessUsers

Group scope

- Domain local
- Global
- Universal

Group type

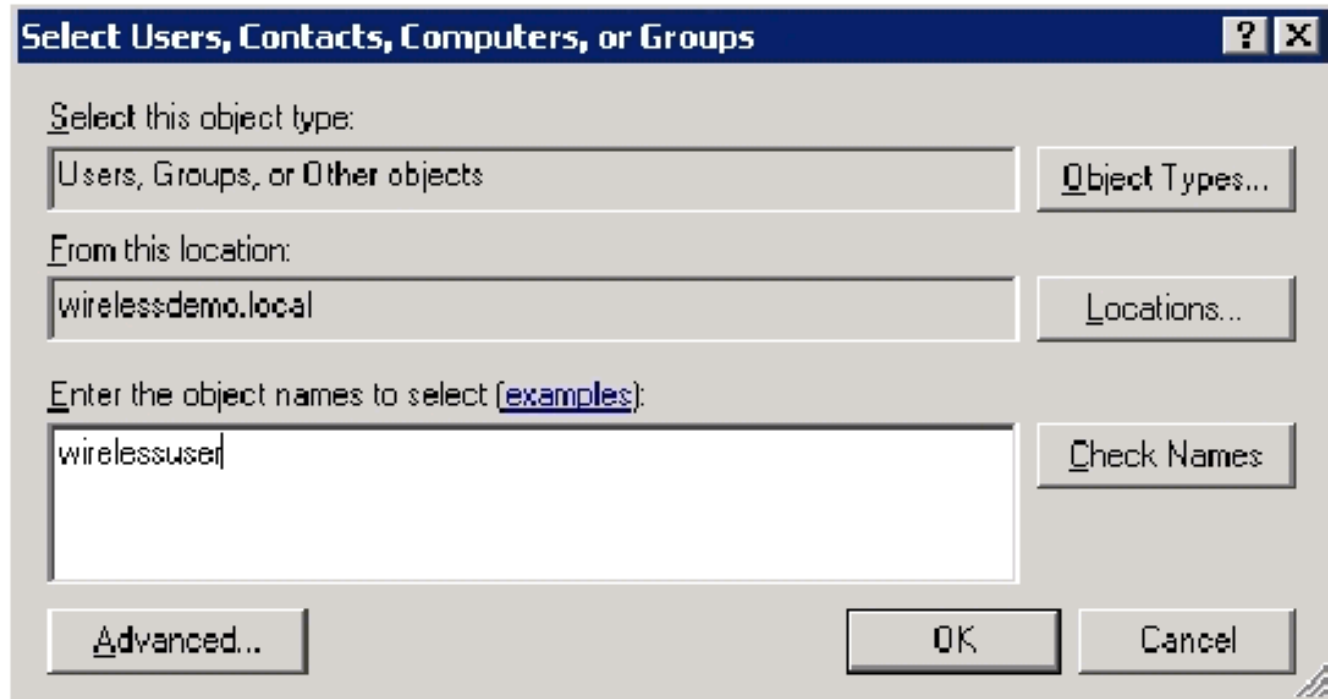
- Security
- Distribution

OK Cancel

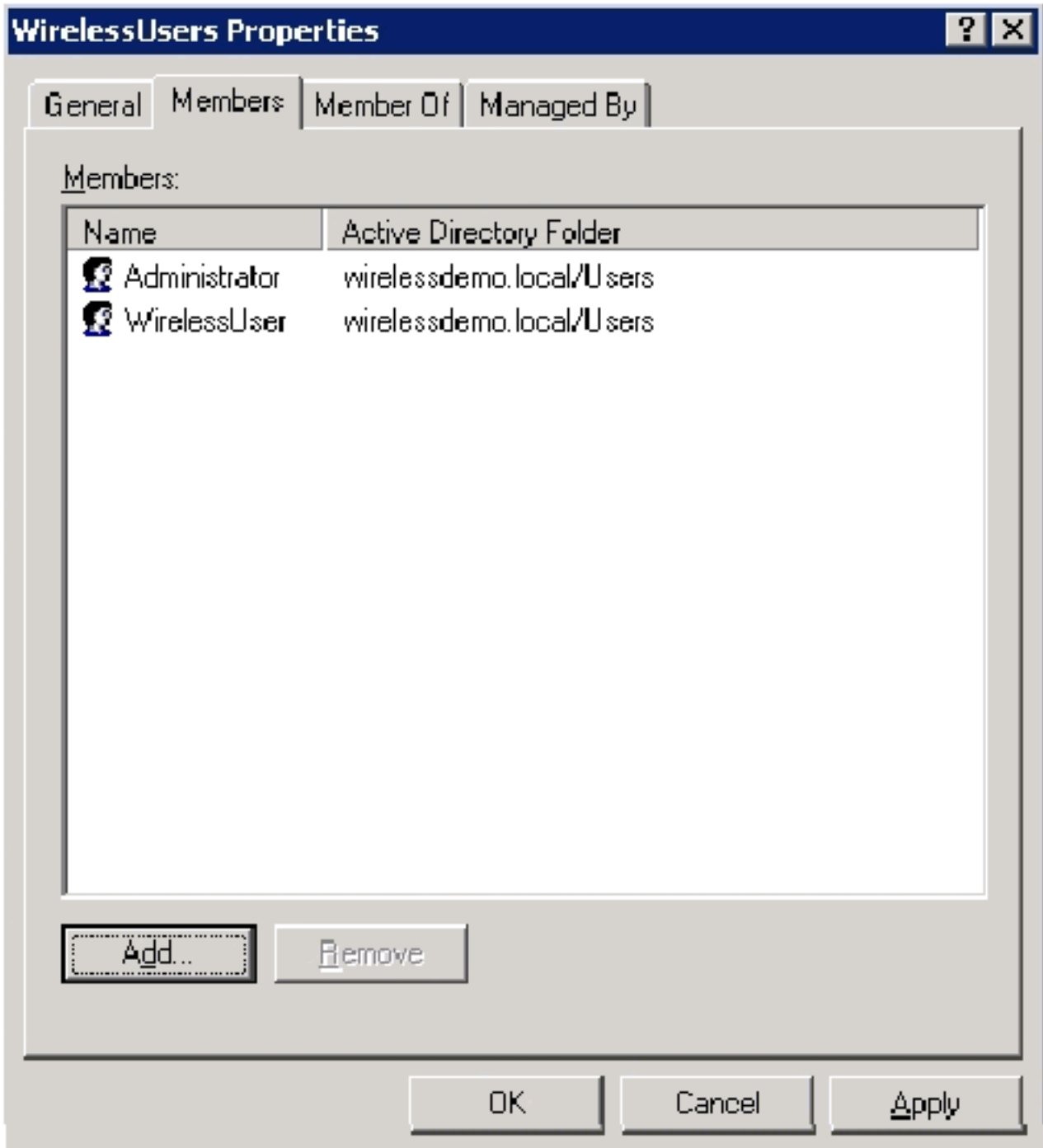
[Schritt 12: Hinzufügen von Benutzern zur Wireless-Benutzergruppe](#)

Führen Sie diese Schritte aus:

1. Doppelklicken Sie im Detailbereich von Active Directory-Benutzern und -Computern auf Group **WirelessUsers**.
2. Öffnen Sie die Registerkarte Mitglieder, und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Dialogfeld Benutzer, Kontakte, Computer oder Gruppen auswählen den Namen der Benutzer ein, die Sie der Gruppe hinzufügen möchten. In diesem Beispiel wird veranschaulicht, wie der Benutzer **WirelessUser** der Gruppe hinzugefügt wird. Klicken Sie auf **OK**.



4. Klicken Sie im Dialogfeld Mehrere Namen gefunden auf **OK**. Das WirelessUser-Benutzerkonto wird der WirelessUsers-Gruppe hinzugefügt.

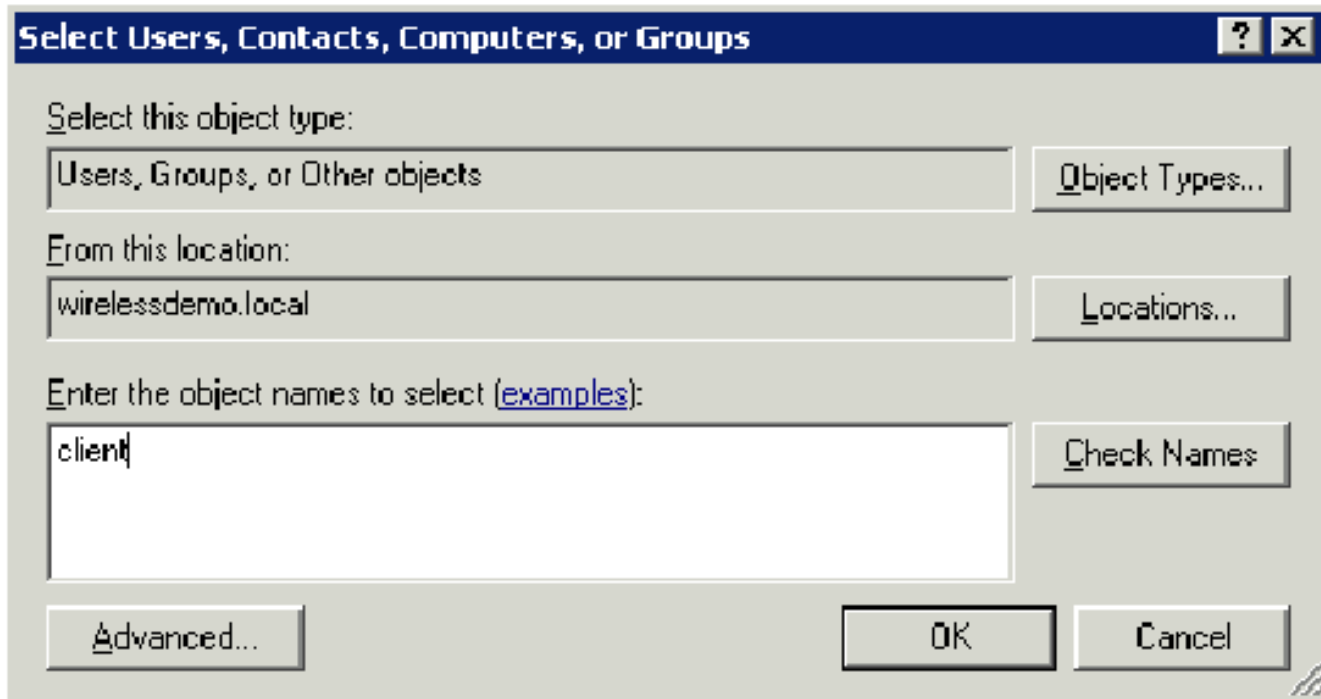


5. Klicken Sie auf **OK**, um die Änderungen in der Gruppe Wireless-Benutzer zu speichern.
6. Wiederholen Sie diese Prozedur, um der Gruppe weitere Benutzer hinzuzufügen.

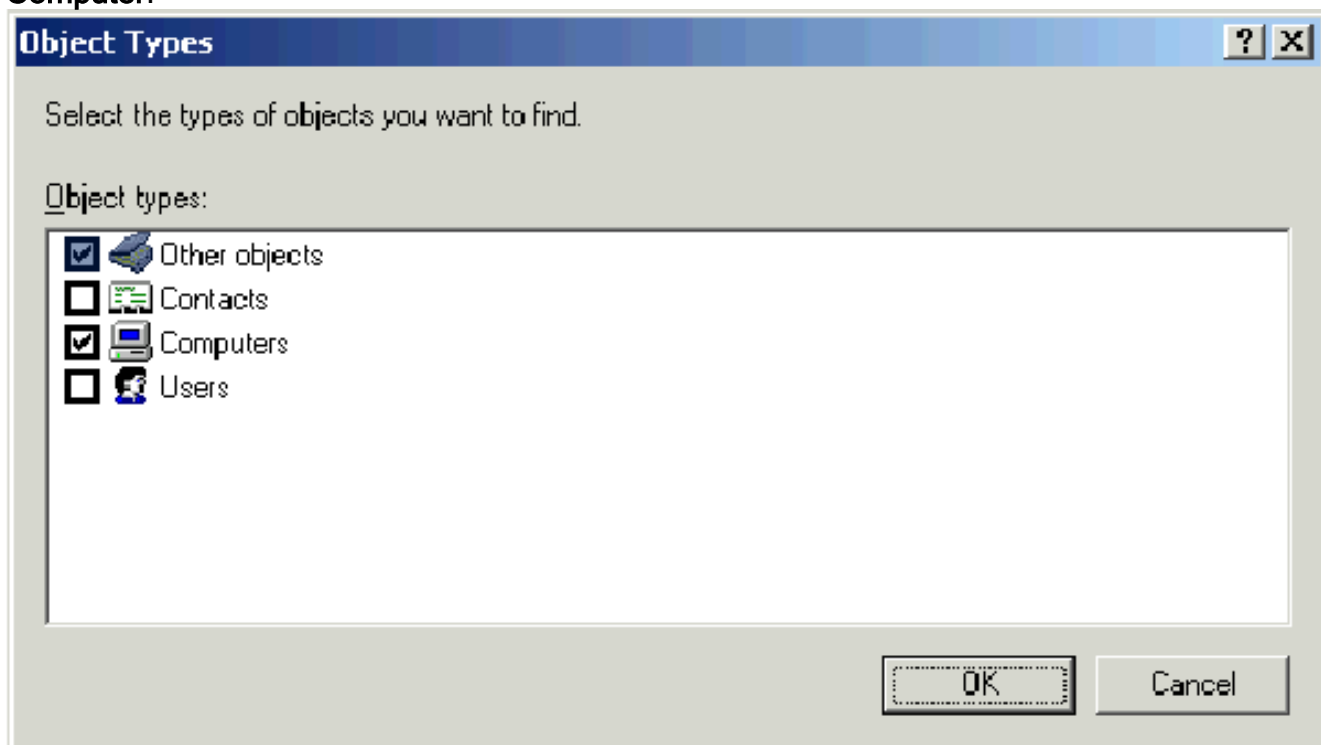
[Schritt 13: Hinzufügen von Clientcomputern zur Wireless-Benutzergruppe](#)

Führen Sie diese Schritte aus:

1. Wiederholen Sie die Schritte 1 und 2 im Abschnitt [Benutzer zur Wireless-Benutzergruppe hinzufügen](#) in diesem Dokument.
2. Geben Sie im Dialogfeld Benutzer, Kontakte oder Computer auswählen den Namen des Computers ein, den Sie der Gruppe hinzufügen möchten. In diesem Beispiel wird veranschaulicht, wie der Computer **client** der Gruppe hinzugefügt wird.



3. Klicken Sie auf **Objekttypen**, deaktivieren Sie das Kontrollkästchen **Benutzer**, und aktivieren Sie dann **Computer**.



4. Klicken Sie zweimal auf **OK**. Das CLIENT-Computerkonto wird der WirelessUsers-Gruppe hinzugefügt.
5. Wiederholen Sie die Prozedur, um der Gruppe weitere Computer hinzuzufügen.

[Windows Standard 2003-Setup mit Cisco Secure ACS 4.0](#)

Cisco Secure ACS ist ein Computer, auf dem Windows Server 2003 mit SP1, Standard Edition, ausgeführt wird. Dieser Computer bietet RADIUS-Authentifizierung und -Autorisierung für den Controller. Gehen Sie wie in diesem Abschnitt beschrieben vor, um ACS als RADIUS-Server zu konfigurieren:

Grundlegende Installation und Konfiguration

Führen Sie diese Schritte aus:

1. Installieren Sie Windows Server 2003 mit SP1, Standard Edition, als **Mitgliedsserver** mit dem Namen **ACS** in der **Domäne "wirelessdemo.local"**. **Hinweis:** Der ACS-Servername wird in den verbleibenden Konfigurationen als cisco_w2003 angezeigt. Ersetzen Sie ACS oder cisco_w2003 in der verbleibenden Laboreinrichtung.
2. Konfigurieren Sie für die LAN-Verbindung das TCP/IP-Protokoll mit der IP-Adresse **172.16.100.26**, der Subnetzmaske **255.255.255.0** und der IP-Adresse des DNS-Servers **127.0.0.1**.

Installation von Cisco Secure ACS 4.0

Hinweis: Weitere Informationen zur Konfiguration von Cisco Secure ACS 4.0 für Windows finden Sie im [Installationshandbuch für Cisco Secure ACS 4.0 für Windows](#).

Führen Sie diese Schritte aus:

1. Melden Sie sich mit einem Domänenadministrator-Konto beim Computer mit dem Namen ACS für Cisco Secure ACS an. **Hinweis:** Es werden nur Installationen unterstützt, die auf dem Computer ausgeführt werden, auf dem Cisco Secure ACS installiert wird. Remote-Installationen, die mit Windows Terminal Services oder Produkten wie Virtual Network Computing (VNC) durchgeführt werden, werden nicht getestet und werden nicht unterstützt.
2. Legen Sie die Cisco Secure ACS-CD in ein CD-ROM-Laufwerk am Computer ein.
3. Wenn das CD-ROM-Laufwerk die Windows-Automatisierungsfunktion unterstützt, wird das Dialogfeld "Cisco Secure ACS for Windows Server" angezeigt. **Hinweis:** Wenn auf dem Computer kein erforderliches Service Pack installiert ist, wird ein Dialogfeld angezeigt. Windows Service Packs können entweder vor oder nach der Installation von Cisco Secure ACS angewendet werden. Sie können mit der Installation fortfahren, aber das erforderliche Service Pack muss nach Abschluss der Installation angewendet werden. Andernfalls funktioniert Cisco Secure ACS möglicherweise nicht zuverlässig.
4. Führen Sie eine der folgenden Aufgaben aus: Wenn das Dialogfeld Cisco Secure ACS für Windows Server angezeigt wird, klicken Sie auf **Installieren**. Wenn das Dialogfeld Cisco Secure ACS für Windows Server nicht angezeigt wird, führen Sie **setup.exe** aus, das sich im Stammverzeichnis der Cisco Secure ACS-CD befindet.
5. Das Dialogfeld "Cisco Secure ACS Setup" zeigt den Softwarelizenzvertrag an.
6. Lesen Sie die Software-Lizenzvereinbarung. Wenn Sie der Softwarelizenzvereinbarung zustimmen, klicken Sie auf **Akzeptieren**. Das Dialogfeld Willkommen zeigt grundlegende Informationen zum Installationsprogramm an.
7. Wenn Sie die Informationen im Dialogfeld Willkommen gelesen haben, klicken Sie auf **Weiter**.
8. Im Dialogfeld Bevor Sie beginnen können werden Elemente aufgelistet, die Sie abschließen müssen, bevor Sie mit der Installation fortfahren. Wenn Sie alle im Dialogfeld Vor dem Start aufgeführten Elemente abgeschlossen haben, aktivieren Sie für jedes Element das entsprechende Kontrollkästchen, und klicken Sie auf **Weiter**. **Hinweis:** Wenn Sie nicht alle im Feld Bevor Sie beginnen aufgelisteten Elemente abgeschlossen haben, klicken Sie auf **Abbrechen** und klicken Sie anschließend auf **Setup beenden**. Nachdem Sie alle im Dialogfeld

"Vor dem Start" aufgeführten Elemente abgeschlossen haben, starten Sie die Installation neu.

9. Das Dialogfeld Speicherort für Ziel auswählen wird angezeigt. Unter Zielordner wird der Installationsort angezeigt. Dies ist das Laufwerk und der Pfad, auf dem das Installationsprogramm Cisco Secure ACS installiert.
10. Wenn Sie den Installationsstandort ändern möchten, führen Sie die folgenden Schritte aus: Klicken Sie auf **Durchsuchen**. Das Dialogfeld Ordner auswählen wird angezeigt. Das Feld Pfad enthält den Installationsspeicherort. Ändern Sie den Installationsstandort. Sie können den neuen Speicherort entweder in das Feld Pfad eingeben oder mithilfe der Verzeichnisse Laufwerke und Verzeichnisse ein neues Laufwerk und Verzeichnis auswählen. Der Installationsort muss sich auf einem lokalen Laufwerk des Computers befinden. **Hinweis:** Geben Sie keinen Pfad an, der das Prozentzeichen "%" enthält. Wenn Sie dies tun, wird die Installation möglicherweise ordnungsgemäß fortgesetzt, schlägt aber fehl, bevor sie abgeschlossen wird. Klicken Sie auf **OK**. **Hinweis:** Wenn Sie einen Ordner angegeben haben, der nicht vorhanden ist, wird im Installationsprogramm ein Dialogfeld angezeigt, in dem die Erstellung des Ordners bestätigt wird. Klicken Sie zum Fortfahren auf **Ja**.
11. Im Dialogfeld Zielort auswählen wird der neue Installationsspeicherort unter Zielordner angezeigt.
12. Klicken Sie auf **Weiter**.
13. Das Dialogfeld Konfiguration der Authentifizierungsdatenbank enthält Optionen zum Authentifizieren von Benutzern. Sie können sich nur mit der Cisco Secure User-Datenbank oder auch mit einer Windows-Benutzerdatenbank authentifizieren. **Hinweis:** Nach der Installation von Cisco Secure ACS können Sie zusätzlich zu Windows-Benutzerdatenbanken die Authentifizierungsunterstützung für alle externen Benutzerdatenbanktypen konfigurieren.
14. Wenn Benutzer nur mit der Cisco Secure User-Datenbank authentifiziert werden sollen, wählen Sie die Option **Nur Cisco Secure ACS-Datenbank überprüfen aus**.
15. Wenn Sie Benutzer mit einer Windows Security Access Manager (SAM)-Benutzerdatenbank oder einer Active Directory-Benutzerdatenbank zusätzlich zur Cisco Secure-Benutzerdatenbank authentifizieren möchten, führen Sie die folgenden Schritte aus: Wählen Sie **auch die Option Windows-Benutzerdatenbank aus**. Das Kontrollkästchen **Yes, see "Grant Dialin Permission to User" (Ja, Einwahlberechtigung für Benutzer gewähren)** wird aktiviert. **Hinweis:** Das Kontrollkästchen **"Grant Dialin Permission to User" (Wahlberechtigung für Benutzer gewähren)** gilt für alle Zugriffsarten, die von Cisco Secure ACS gesteuert werden, und nicht nur für den Einwahlzugang. Ein Benutzer, der über einen VPN-Tunnel auf das Netzwerk zugreift, wählt beispielsweise nicht in einen Netzwerkzugriffsserver. Wenn jedoch das Kontrollkästchen **Yes (Ja) aktiviert** ist, **verwenden Sie die Einstellung "Grant Dialin Permission to User" (Einwahlberechtigung für Benutzer gewähren), wendet Cisco Secure ACS die Windows-Benutzereinwahlberechtigungen an, um zu bestimmen, ob dem Benutzer Zugriff auf das Netzwerk gewährt werden soll.** Wenn Sie Benutzern, die von einer Windows-Domänenbenutzerdatenbank authentifiziert wurden, nur dann Zugriff gewähren möchten, wenn sie über eine Einwahlberechtigung in ihrem Windows-Konto verfügen, aktivieren Sie das **Kontrollkästchen Yes (Ja)**, und **lesen Sie die Option "Grant Dialin Permission to User" (Wahlberechtigung für Benutzer gewähren).**
16. Klicken Sie auf **Weiter**.
17. Das Installationsprogramm installiert Cisco Secure ACS und aktualisiert die Windows-Registrierung.

18. Im Dialogfeld Erweiterte Optionen sind mehrere Funktionen von Cisco Secure ACS aufgeführt, die standardmäßig nicht aktiviert sind. Weitere Informationen zu diesen Funktionen finden Sie im [Benutzerhandbuch für Cisco Secure ACS für Windows Server, Version 4.0](#). **Hinweis:** Die aufgeführten Funktionen werden in der HTML-Schnittstelle von Cisco Secure ACS nur angezeigt, wenn Sie sie aktivieren. Nach der Installation können Sie sie auf der Seite Erweiterte Optionen im Abschnitt Schnittstellenkonfiguration aktivieren oder deaktivieren.
19. Aktivieren Sie für jede Funktion, die Sie aktivieren möchten, das entsprechende Kontrollkästchen.
20. Klicken Sie auf **Weiter**.
21. Das Dialogfeld "Active Service Monitoring" wird angezeigt. **Hinweis:** Nach der Installation können Sie aktive Service-Überwachungsfunktionen auf der Seite Active Service Management (Aktives Service-Management) im Abschnitt System Configuration (Systemkonfiguration) konfigurieren.
22. Wenn Sie möchten, dass Cisco Secure ACS Benutzerauthentifizierungsdienste überwacht, aktivieren Sie das Kontrollkästchen **Enable Login Monitoring (Anmeldungsüberwachung aktivieren)**. Wählen Sie in der Liste Skript zu Ausführung die Option aus, die Sie bei einem Ausfall eines Authentifizierungsdiensts anwenden möchten: **No Remedial Action** (Keine Problembehebung) - Cisco Secure ACS führt kein Skript aus. **Hinweis:** Diese Option ist nützlich, wenn Sie E-Mail-Benachrichtigungen für Ereignisse aktivieren. **Neustart** - Cisco Secure ACS führt ein Skript aus, das den Computer neu startet, auf dem Cisco Secure ACS ausgeführt wird. **Alle neu starten** - Cisco Secure ACS startet alle Cisco Secure ACS-Services neu. **Neustart von RADIUS/TACACS+**: Cisco Secure ACS startet nur die RADIUS- und TACACS+-Dienste neu.
23. Wenn Cisco Secure ACS eine E-Mail-Nachricht senden soll, wenn die Service-Überwachung ein Ereignis erkennt, aktivieren Sie das Kontrollkästchen **Mail Notification**.
24. Klicken Sie auf **Weiter**.
25. Das Dialogfeld Datenbankverschlüsselungskennwort wird angezeigt. **Hinweis:** Das Datenbankverschlüsselungskennwort wird verschlüsselt und in der ACS-Registrierung gespeichert. Möglicherweise müssen Sie dieses Kennwort erneut verwenden, wenn kritische Probleme auftreten und der Zugriff auf die Datenbank manuell erfolgen muss. Halten Sie dieses Kennwort bereit, damit der technische Support Zugriff auf die Datenbank erhält. Das Kennwort kann bei jedem Ablaufzeitraum geändert werden.
26. Geben Sie ein Kennwort für die Datenbankverschlüsselung ein. Das Kennwort muss mindestens acht Zeichen lang sein und sowohl Zeichen als auch Ziffern enthalten. Es sind keine ungültigen Zeichen vorhanden. Klicken Sie auf **Weiter**.
27. Das Setup-Programm wird abgeschlossen, und das Dialogfeld "Cisco Secure ACS Service Initiation" wird angezeigt.
28. Aktivieren Sie für jede Cisco Secure ACS Services Initiation-Option das entsprechende Kontrollkästchen. Die den Optionen zugeordneten Aktionen treten nach Abschluss des Installationsprogramms auf. **Ja, ich möchte jetzt den Cisco Secure ACS Service starten** - Startet die Windows-Dienste, die Cisco Secure ACS bilden. Wenn Sie diese Option nicht auswählen, ist die HTML-Schnittstelle für Cisco Secure ACS nur verfügbar, wenn Sie den Computer neu starten oder den CSAdmin-Dienst starten. **Ja, nach der Installation möchte ich den Cisco Secure ACS Administrator vom Browser aus starten** - Öffnet die Cisco Secure ACS HTML-Schnittstelle im Standard-Webbrowser für das aktuelle Windows-Benutzerkonto. **Ja, ich möchte die Readme-Datei anzeigen** - Öffnet die Datei README.TXT in Windows Notepad.

29. Klicken Sie auf **Weiter**.
30. Wenn Sie eine Option ausgewählt haben, werden die Cisco Secure ACS-Services gestartet. Das Dialogfeld Setup Complete (Setup abgeschlossen) enthält Informationen zur HTML-Schnittstelle von Cisco Secure ACS.
31. Klicken Sie auf **Fertig stellen**. **Hinweis:** Die restliche Konfiguration ist im Abschnitt für den konfigurierten EAP-Typ dokumentiert.

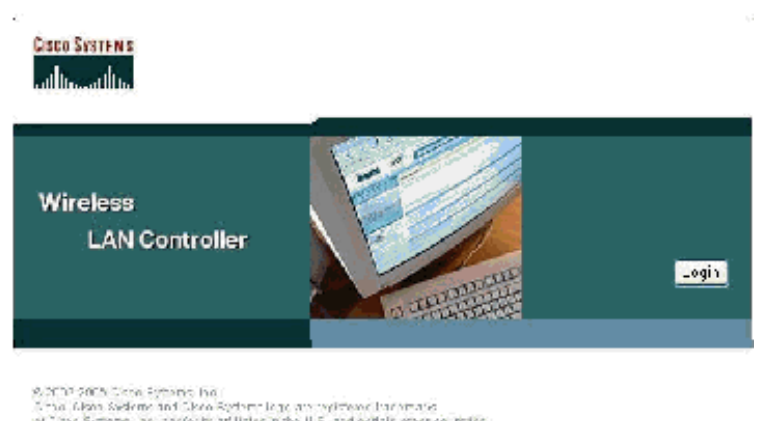
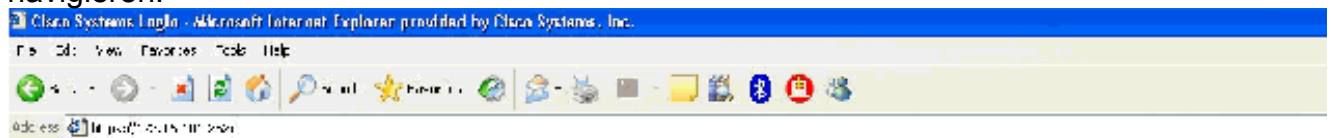
Konfiguration des Cisco LWAPP-Controllers

Erstellen der erforderlichen Konfiguration für WPA2/WPA

Führen Sie diese Schritte aus:

Hinweis: Es wird davon ausgegangen, dass der Controller über eine grundlegende Verbindung zum Netzwerk verfügt und die IP-Erreichbarkeit zur Verwaltungsschnittstelle erfolgreich ist.

1. Melden Sie sich beim Controller an, indem Sie zu **https://172.16.101.252** navigieren.



2. Klicken Sie auf **Anmelden**.
3. Melden Sie sich mit dem Standardbenutzer-**Admin** und dem Standardkennwort **admin an**.
4. Erstellen Sie die VLAN-Zuordnung für die Schnittstelle im Menü Controller.
5. Klicken Sie auf **Schnittstellen**.
6. Klicken Sie auf **Neu**.
7. Geben Sie im Feld Schnittstellenname **Employee** ein. (Dieses Feld kann beliebig sein.)

8. Geben Sie im Feld "VLAN ID" **20 ein**. (Dieses Feld kann jedes VLAN sein, das im Netzwerk übertragen wird.)
9. Klicken Sie auf **Apply** (Anwenden).
10. Konfigurieren Sie die Informationen so, wie diese Schnittstellen > Fenster Bearbeiten angezeigt werden.

The screenshot shows the Cisco Systems web interface for configuring an interface. The browser address bar shows `https://172.16.101.252/screens/frameset.html`. The interface is titled "Interfaces > Edit" and is part of the "CONTROLLER" section. The left sidebar lists various configuration categories, with "Interfaces" selected. The main content area is divided into several sections:

- General Information:** Interface Name: employee
- Interface Address:**
 - VLAN Identifier: 20
 - IP Address: 172.16.100.1
 - Netmask: 255.255.255.0
 - Gateway: 172.16.100.1
- Physical Information:**
 - Port Number: 1
- DHCP Information:**
 - Primary DHCP Server: 172.16.100.25
 - Secondary DHCP Server: 0.0.0.0
- Access Control List:**
 - ACL Name: none

A red note at the bottom of the page reads: "Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients."

11. Klicken Sie auf **Apply** (Anwenden).
12. Klicken Sie auf **WLAN**.
13. Klicken Sie auf **Neu**.
14. Geben Sie im Feld WLAN SSID **Employee ein**.
15. Klicken Sie auf **Apply** (Anwenden).
16. Konfigurieren Sie die Informationen so, wie diese WLANs angezeigt werden. > Fenster "Bearbeiten". **Hinweis:** WPA2 ist die gewählte Layer-2-Verschlüsselungsmethode für diese Übung. Damit WPA mit TKIP-MIC-Clients eine Verbindung zu dieser SSID herstellen kann,

können Sie auch die Kontrollkästchen **WPA-Kompatibilitätsmodus** aktivieren und **WPA2 TKIP-Clients** oder Clients **zulassen**, die die 802.11i AES-Verschlüsselungsmethode nicht unterstützen.

WLANs > Edit

WLAN ID	1
WLAN SSID	Employee

General Policies

Radius Policy	All
Admin Status	<input checked="" type="checkbox"/> Enabled
Session Timeout (secs)	1800
Quality of Service (QoS)	Silver (best effort)
WMM Policy	Disabled
7920 Profile Support	<input type="checkbox"/> Client CAC Limit <input type="checkbox"/> AP CAC Limit
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
Allow AAA Override	<input type="checkbox"/> Enabled
Client Exclusion	<input checked="" type="checkbox"/> Enabled ** 60 Timeout Value (secs)
DHCP Server	<input type="checkbox"/> Override
DHCP Addr. Assignment	<input checked="" type="checkbox"/> Required
Interface Name	employee

Security Policies

Layer 2 Security	WPA2
	<input type="checkbox"/> MAC Filtering
Layer 3 Security	None
	<input type="checkbox"/> Web Policy **

* Web Policy cannot be used in combination with IPsec and L2TP.

** When client exclusion is enabled, a timeout value of zero means infinity (will require administrative override to reset excluded clients)

Radius Servers

	Authentication Servers	Accounting Servers
Server 1	IP:172.16.100.25, Port:1812	none
Server 2	none	none
Server 3	none	none

WPA2 Parameters

WPA Compatibility Mode	<input checked="" type="checkbox"/> Enable
Allow WPA2 TKIP Clients	<input checked="" type="checkbox"/> Enable
Pre-Shared Key	<input type="checkbox"/> Enabled (WPA2 passphrase has been set)

17. Klicken Sie auf **Apply** (Anwenden).
18. Klicken Sie auf das Menü **Security**, und fügen Sie den RADIUS-Server hinzu.
19. Klicken Sie auf **Neu**.
20. Fügen Sie die IP-Adresse des RADIUS-Servers (172.16.100.25) hinzu, die der zuvor konfigurierte ACS-Server ist.
21. Stellen Sie sicher, dass der gemeinsam genutzte Schlüssel mit dem im ACS-Server konfigurierten AAA-Client übereinstimmt.
22. Klicken Sie auf **Apply** (Anwenden).



Security

AAA

- General
- RADIUS Authentication
- RADIUS Accounting
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies

Access Control Lists

Web Auth Certificate

Wireless Protection Policies

- Trusted AP Policies
- Rogue Policies
- Standard Signatures
- Custom Signatures
- Client Exclusion Policies
- AP Authentication

RADIUS Authentication Servers > New

Server Index (Priority)	1 <input type="button" value="v"/>
Server IP Address	<input type="text" value="172.16.100.25"/>
Keys Format	ASCII <input type="button" value="v"/>
Shared Secret	<input type="password" value="••••••"/>
Confirm Shared Secret	<input type="password" value="••••••"/>
Key Wrap	<input type="checkbox"/>
Port Number	<input type="text" value="1812"/>
Server Status	Enabled <input type="button" value="v"/>
Support for RFC 3576	Enabled <input type="button" value="v"/>
Retransmit Timeout	<input type="text" value="2"/> seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input type="checkbox"/> Enable

The screenshot shows the CiscoSecure ACS web interface in Microsoft Internet Explorer. The browser title is "CiscoSecure ACS - Microsoft Internet Explorer provided by Cisco Systems, Inc." and the address bar shows "http://172.16.100.25:3052/index2.htm". The page title is "Network Configuration" and the sub-page is "Edit". The main heading is "AAA Client Setup For DEMO_2006_1". The configuration fields are:

- AAA Client IP Address: 173.16.101.253
- Key: shared secret
- Authentication Using: RADIUS (Cisco Aires-GT)

There are also several checkboxes for configuration options:

- Single Connect TACACS+ AAA Client (Record step in accounting on failure).
- Log Update/Watchdog Packets from this AAA Client.
- Log RADIUS Tunneling Packets from this AAA Client.
- Replace RADIUS Port info with Username from this AAA Client.

23. Die Basiskonfiguration ist nun abgeschlossen, und Sie können mit dem Testen des EAP-TLS beginnen.

EAP-TLS-Authentifizierung

Für die EAP-TLS-Authentifizierung sind Computer- und Benutzerzertifikate auf dem Wireless-Client erforderlich, die Ergänzung der Remote-Zugriffsrichtlinie für den Wireless-Zugriff um EAP-TLS als EAP-Typ sowie eine Neukonfiguration der Wireless-Netzwerkverbindung.

Führen Sie die in diesem Abschnitt beschriebenen Schritte aus, um DC_CA für die automatische Registrierung von Computer- und Benutzerzertifikaten zu konfigurieren.

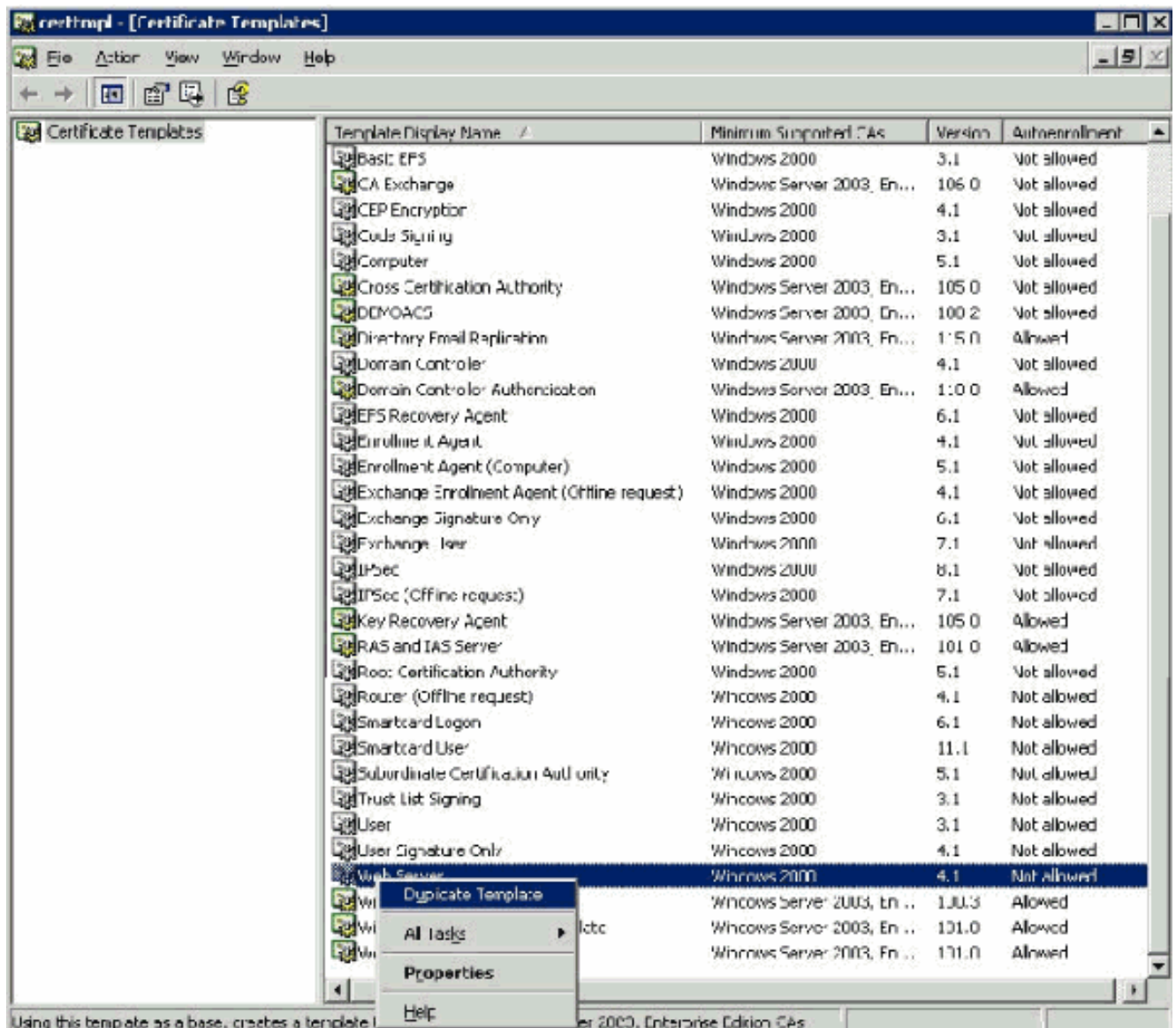
Hinweis: Microsoft hat die Webserver-Vorlage mit der Veröffentlichung der Windows 2003 Enterprise CA so geändert, dass Schlüssel nicht mehr exportierbar sind und die Option deaktiviert ist. Es gibt keine anderen Zertifikatsvorlagen, die mit Zertifikatsdiensten für die Serverauthentifizierung bereitgestellt werden und die die Möglichkeit bieten, Schlüssel als exportierbar zu markieren, die im Dropdown-Menü verfügbar sind. Daher müssen Sie eine neue Vorlage erstellen, die dies tut.

Hinweis: Windows 2000 ermöglicht das Exportieren von Schlüsseln, und diese Verfahren müssen bei Verwendung von Windows 2000 nicht befolgt werden.

Installieren des Snap-Ins für Zertifikatsvorlagen

Führen Sie diese Schritte aus:

1. Wählen Sie **Start > Ausführen**, geben Sie **mmc ein**, und klicken Sie auf **OK**.
2. Klicken Sie im Menü Datei auf **Snap-In hinzufügen/entfernen** und klicken Sie anschließend auf **Hinzufügen**.
3. Doppelklicken Sie unter Snap-In auf **Zertifikatsvorlagen**, klicken Sie auf **Schließen** und dann auf **OK**.
4. Klicken Sie in der Konsolenstruktur auf **Zertifikatsvorlagen**. Alle Zertifikatsvorlagen werden im Bereich Details angezeigt.
5. Um die Schritte 2 bis 4 zu umgehen, geben Sie **certtmpl.msc ein**, wodurch das Snap-In für Zertifikatsvorlagen geöffnet wird.



[Erstellen der Zertifikatsvorlage für den ACS-Webserver](#)

Führen Sie diese Schritte aus:

1. Klicken Sie im Detailbereich des Snap-Ins Zertifikatsvorlagen auf die **Webserver**-Vorlage.
2. Klicken Sie im Menü Aktion auf **Vorlage duplizieren**.

Properties of New Template [?] [X]

Issuance Requirements | Superseded Templates | Extensions | Security

General | Request Handling | Subject Name

Template display name:

Minimum Supported CAs: Windows Server 2003, Enterprise Edition

After you apply changes to this tab, you can no longer change the template name.

Template name:

Validity period: years weeks

Renewal period: weeks

Publish certificate in Active Directory

Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply

3. Geben Sie im Feld Name der Vorlagenanzeige **ACS**

Properties of New Template [?] [X]

Issuance Requirements | Superseded Templates | Extensions | Security

General | **Request Handling** | Subject Name

Template display name:
ACS

Minimum Supported CAs: Windows Server 2003, Enterprise Edition

After you apply changes to this tab, you can no longer change the template name.

Template name:
ACS

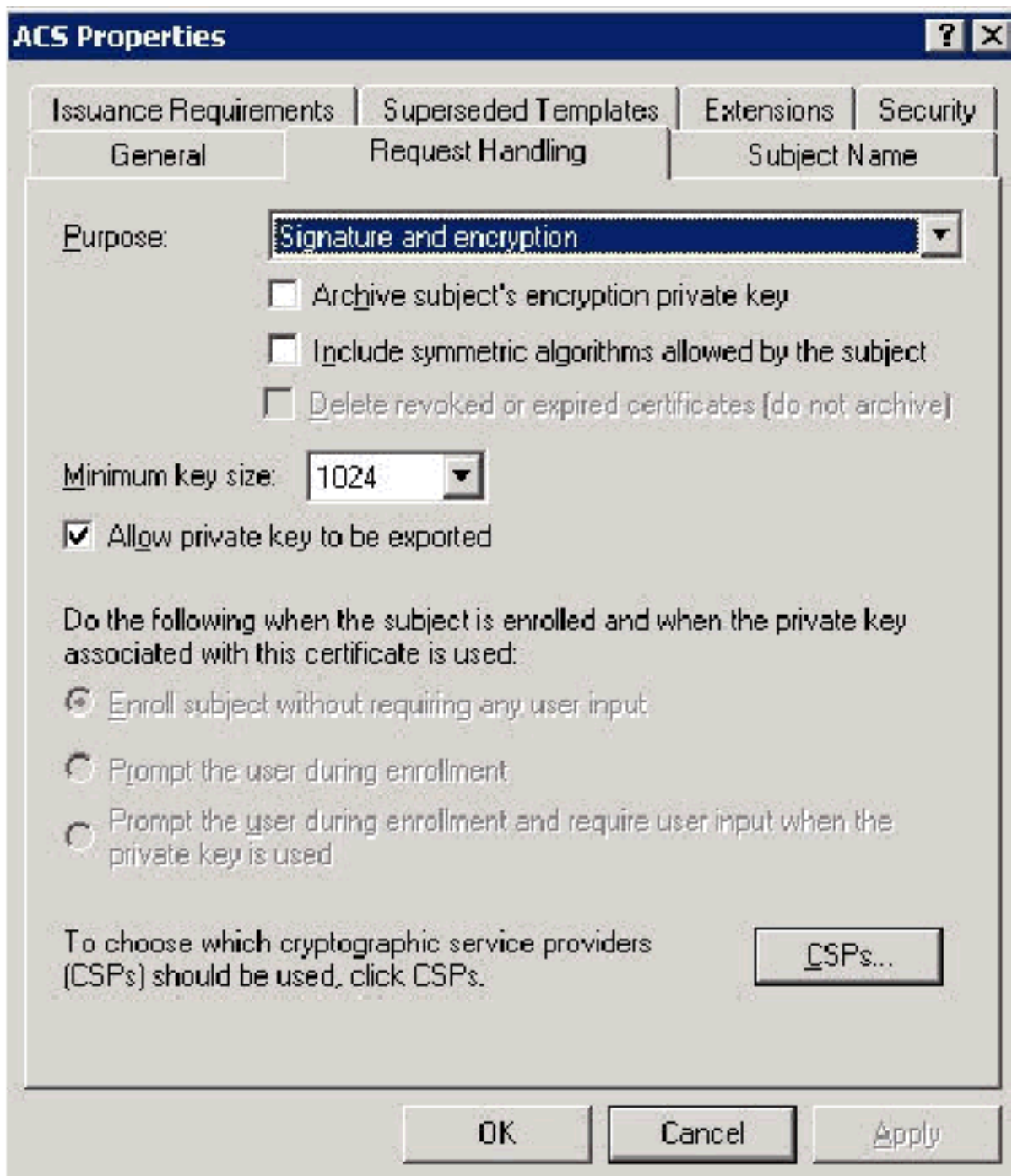
Validity period: 2 years
Renewal period: 6 weeks

Publish certificate in Active Directory
 Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply

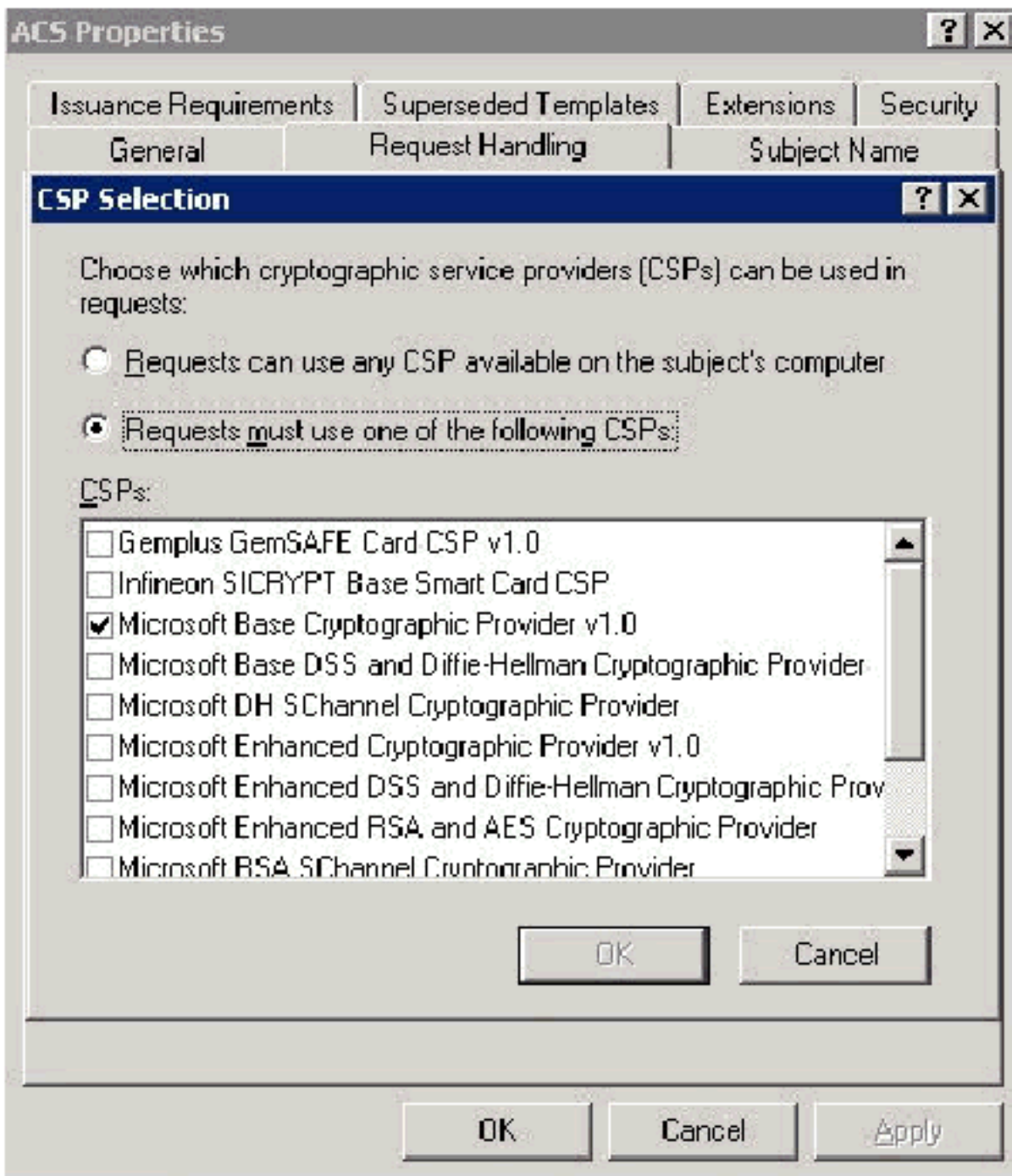
ein.

4. Öffnen Sie die Registerkarte Request Handling (Anforderungsverarbeitung), und aktivieren Sie **Allow private key to be**



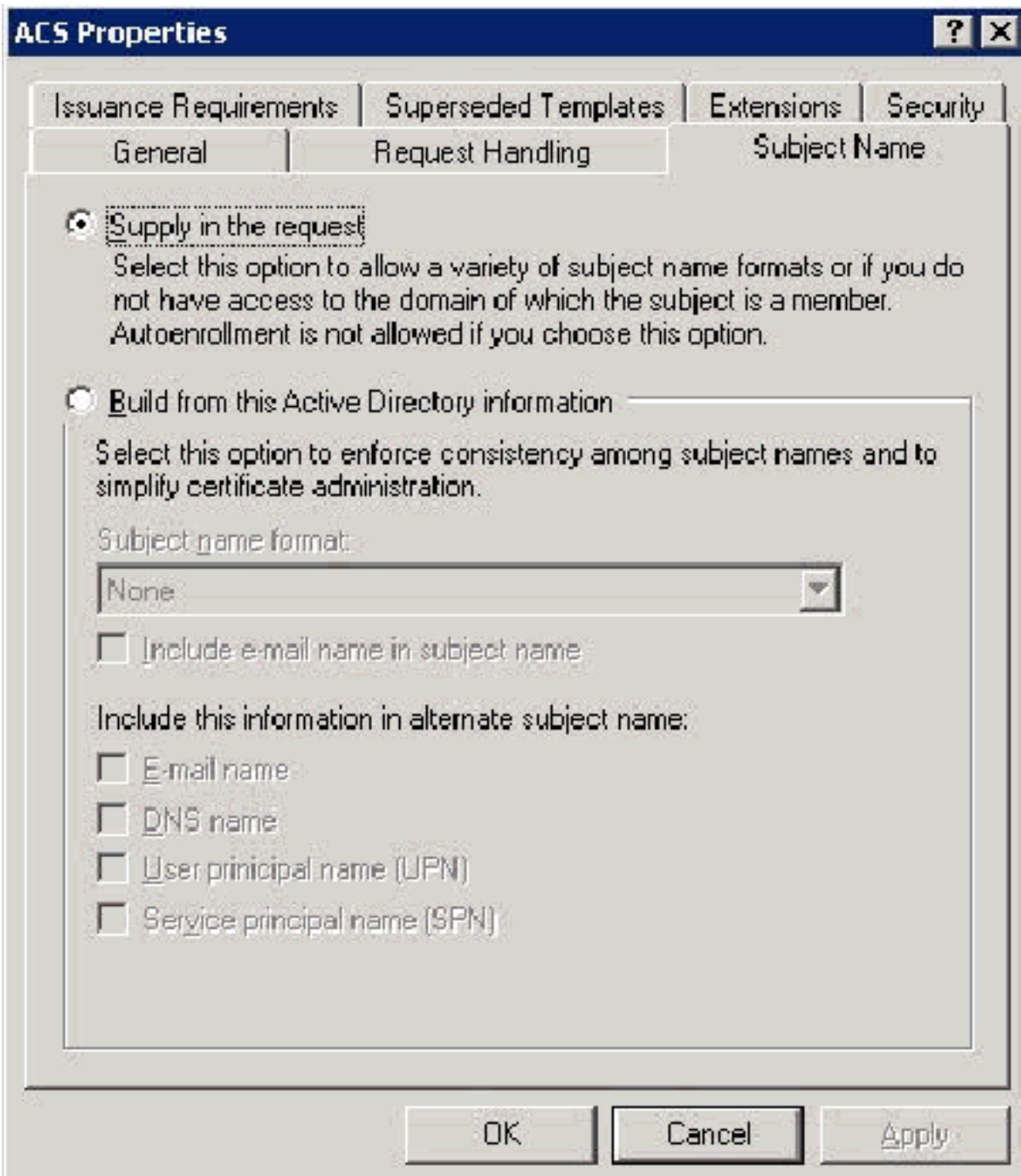
export.

5. Wählen Sie Anforderungen aus, müssen Sie einen der folgenden CSPs verwenden und **Microsoft Base Cryptographic Provider v1.0** aktivieren. Deaktivieren Sie alle anderen CSPs, die aktiviert sind, und klicken Sie dann auf



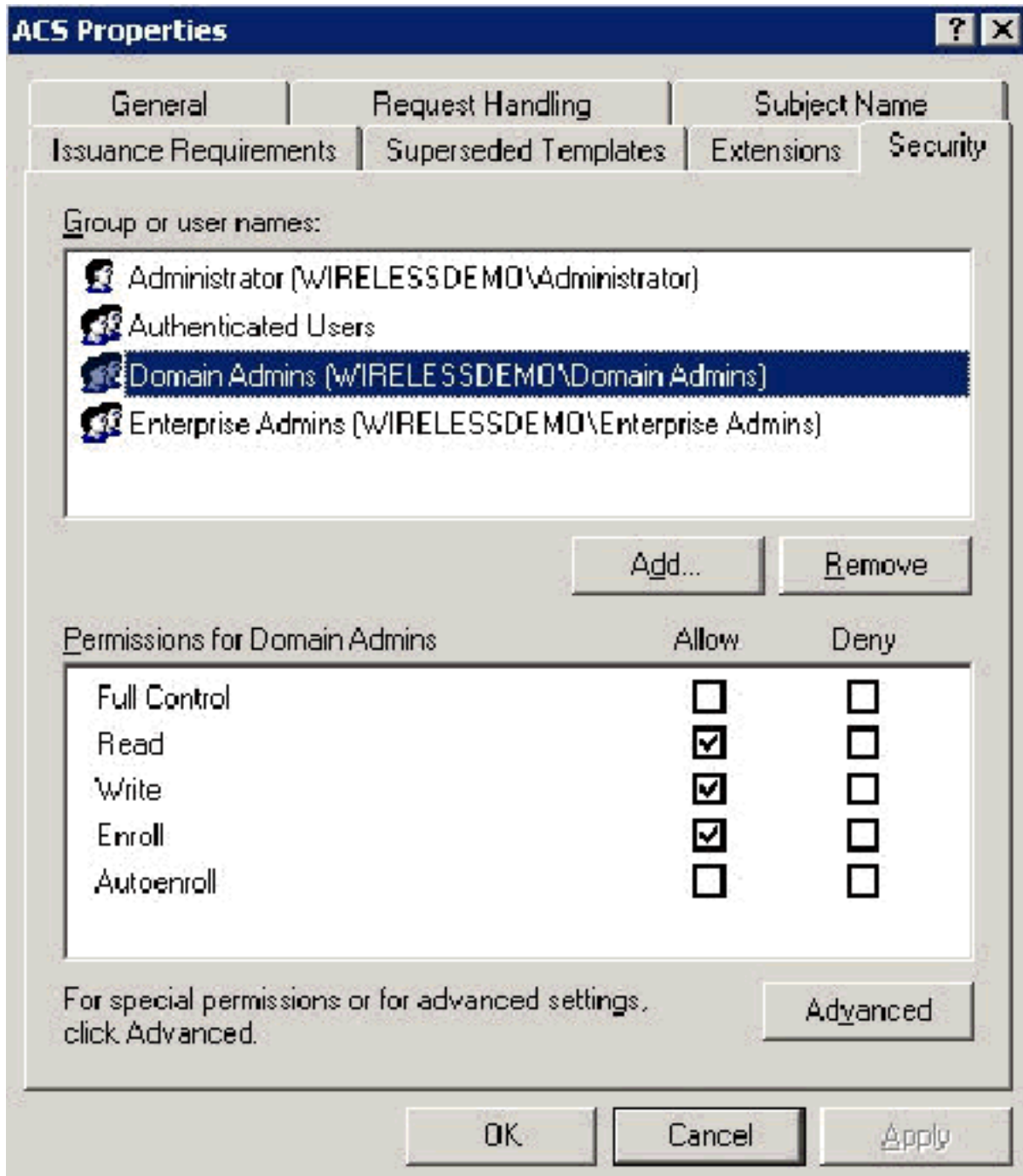
OK.

6. Öffnen Sie die Registerkarte **Betreffname**, wählen Sie **in der Anfrage** die Option **Angebot aus**, und klicken Sie auf



OK.

7. Gehen Sie zur Registerkarte Sicherheit, markieren Sie die **Domänen-Administratorgruppe**, und stellen Sie sicher, dass die Option **Registrieren** unter Zulassen aktiviert ist. **Wichtig:** Wenn Sie sich dazu entscheiden, nur aus diesen Active Directory-Informationen zu erstellen, aktivieren Sie **User Principal Name (UPN)** und deaktivieren Sie **Include email name in Subject name (Betreffname und E-Mail-Name)**, da im Snap-In Active Directory Users (Active Directory-Benutzer und -Computer) kein E-Mail-Name für das Wireless-Benutzerkonto eingegeben wurde. Wenn Sie diese beiden Optionen nicht deaktivieren, wird bei der automatischen Registrierung versucht, E-Mails zu verwenden. Dies führt zu einem Fehler bei der automatischen Registrierung.



8. Falls erforderlich, gibt es zusätzliche Sicherheitsmaßnahmen, um zu verhindern, dass Zertifikate automatisch entfernt werden. Diese finden Sie auf der Registerkarte "Issuance Requirements" (Ausgabeanforderungen). Dies wird in diesem Dokument nicht weiter erläutert.

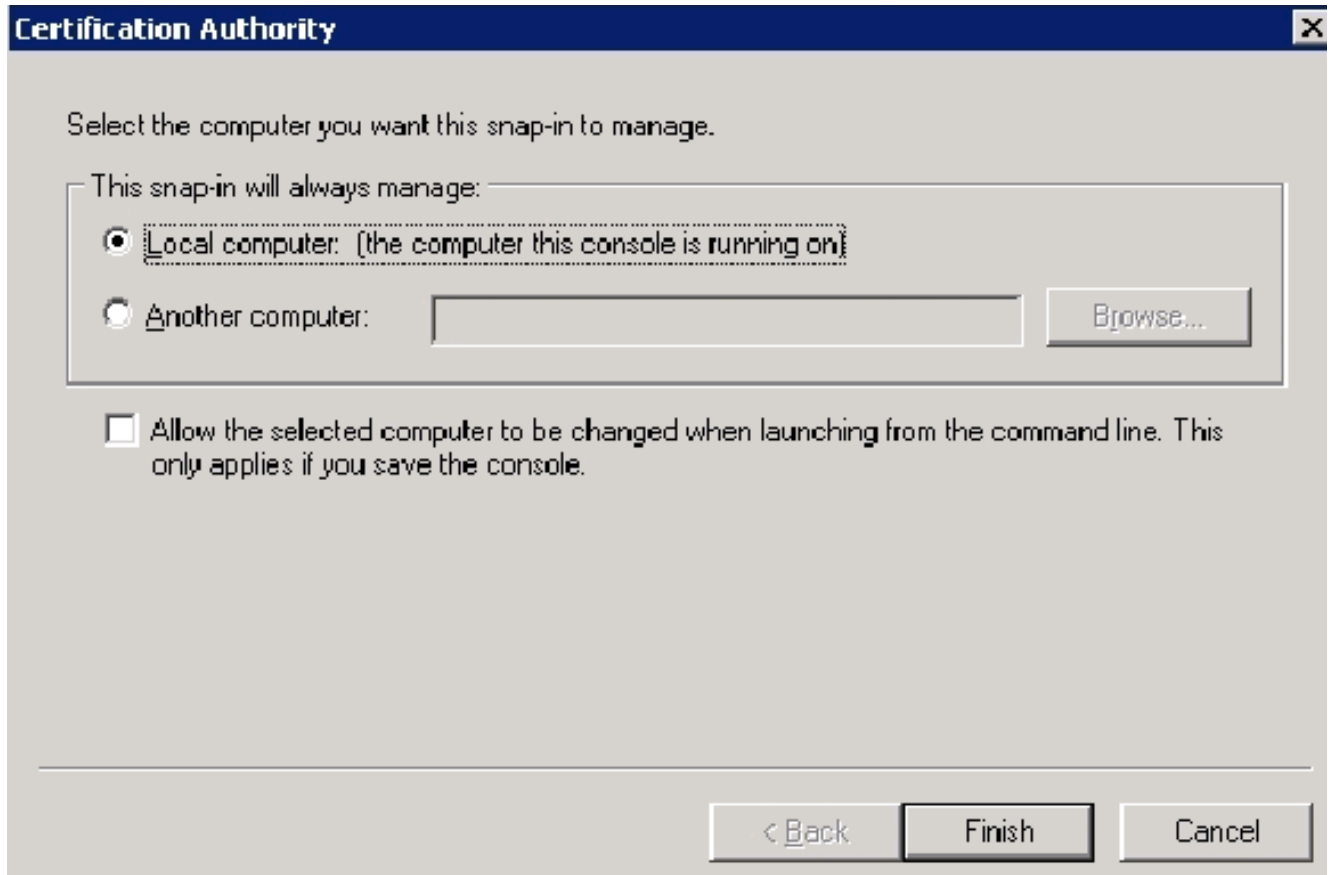
The screenshot shows the 'ACS Properties' dialog box with the 'Request Handling' tab selected. The 'Issuance Requirements' section is active, showing options for enrollment and reenrollment. The 'CA certificate manager approval' checkbox is checked. The 'This number of authorized signatures' is set to 0. The 'Policy type required in signature', 'Application policy', and 'Issuance policies' fields are empty. The 'Require the following for reenrollment' section has 'Same criteria as for enrollment' selected. The 'OK', 'Cancel', and 'Apply' buttons are visible at the bottom.

9. Klicken Sie auf **OK**, um die Vorlage zu speichern und im Snap-In der Zertifizierungsstelle mit der Ausgabe dieser Vorlage fortzufahren.

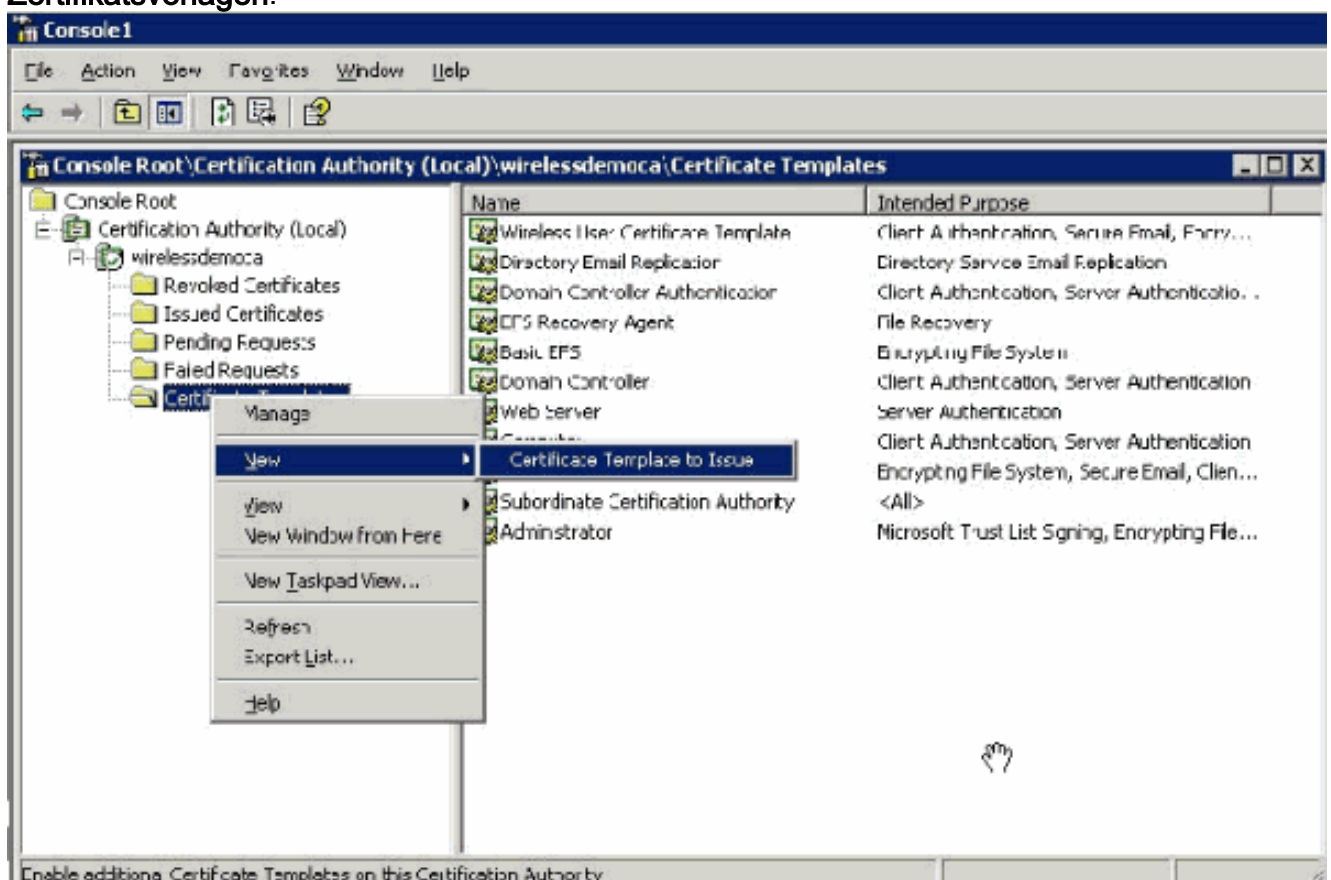
[Aktivieren der Zertifikatsvorlage für den neuen ACS-Webserver](#)

Führen Sie diese Schritte aus:

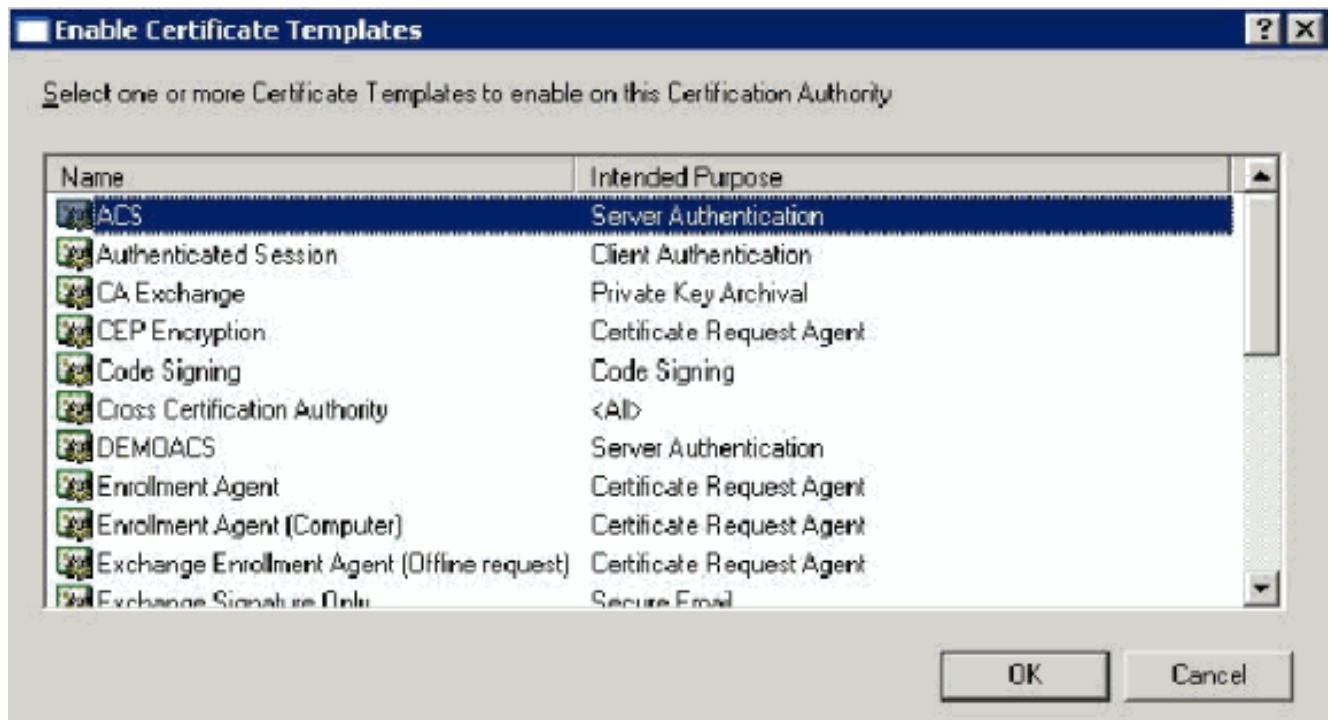
1. Öffnen Sie das Snap-In der **Zertifizierungsstelle**. Befolgen Sie die Schritte 1-3 im Abschnitt [Erstellen der Zertifikatsvorlage für den ACS-Webserver](#), wählen Sie die Option **Certificate Authority (Zertifizierungsstelle)** aus, wählen Sie **Local Computer (Lokaler Computer)** aus, und klicken Sie auf **Beenden**.



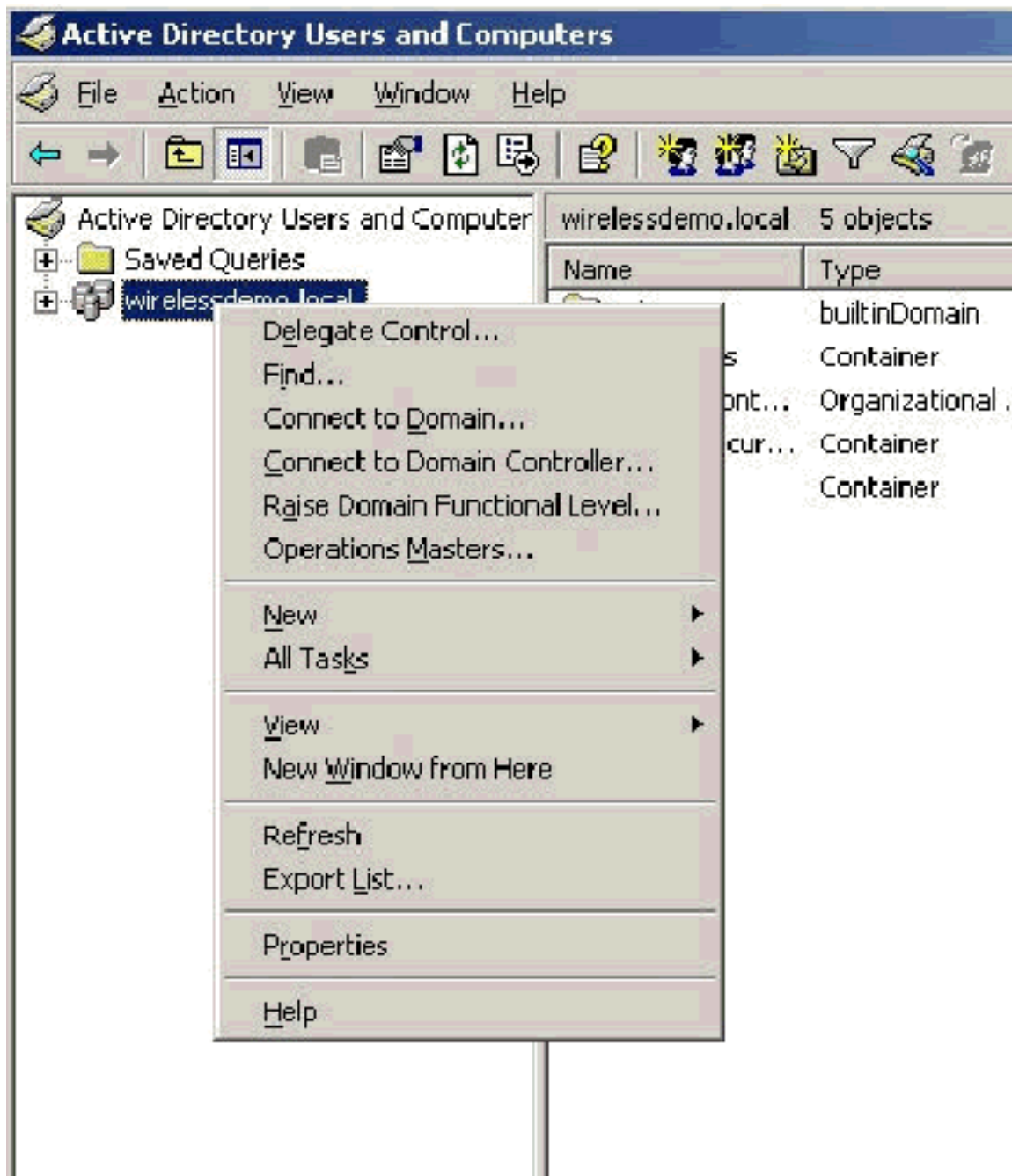
2. Erweitern Sie in der Konsolenstruktur die Option **wirelessdemoca**, und klicken Sie dann mit der rechten Maustaste auf **Zertifikatsvorlagen**.



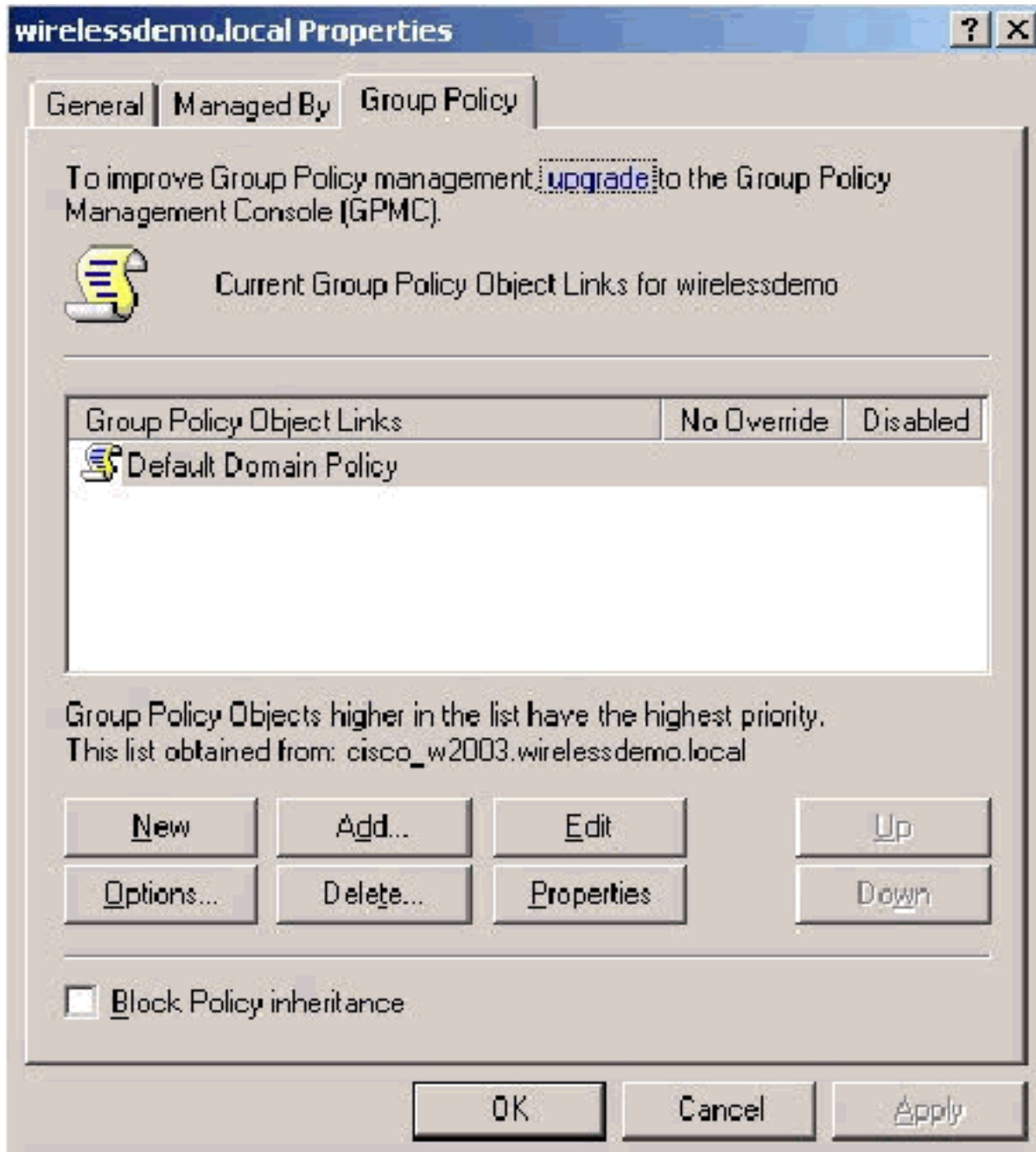
3. Wählen Sie **Neu > Zu erteilende Zertifikatsvorlage** aus.
4. Klicken Sie auf die **ACS-**Zertifikatsvorlage.



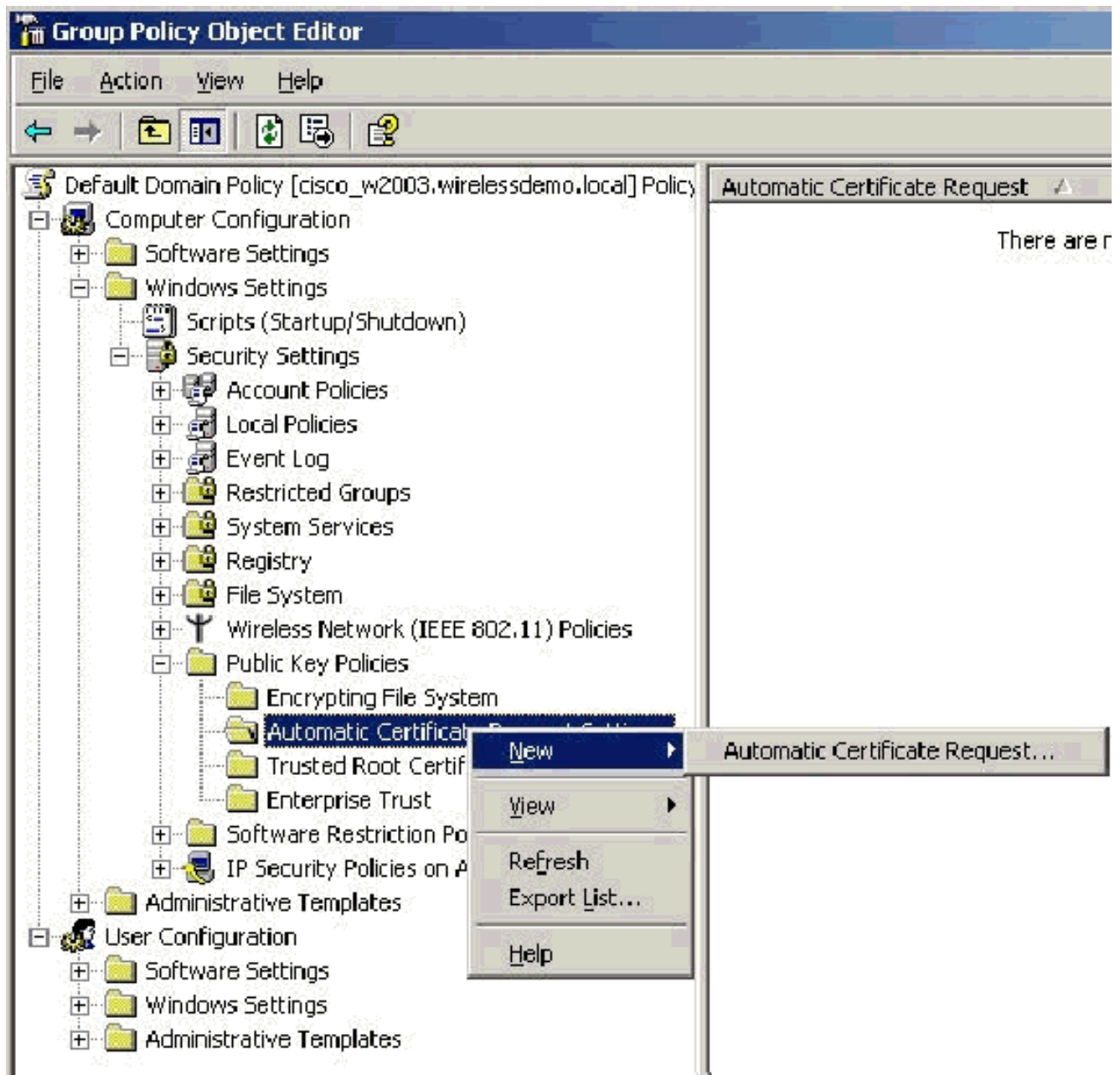
5. Klicken Sie auf **OK**, und öffnen Sie das **Snap-In Active Directory-Benutzer und -Computer**.
6. Doppelklicken Sie in der Konsolenstruktur auf **Active Directory-Benutzer und -Computer**, klicken Sie mit der rechten Maustaste auf die **Domäne WirelessDemo.local**, und klicken Sie dann auf **Eigenschaften**.



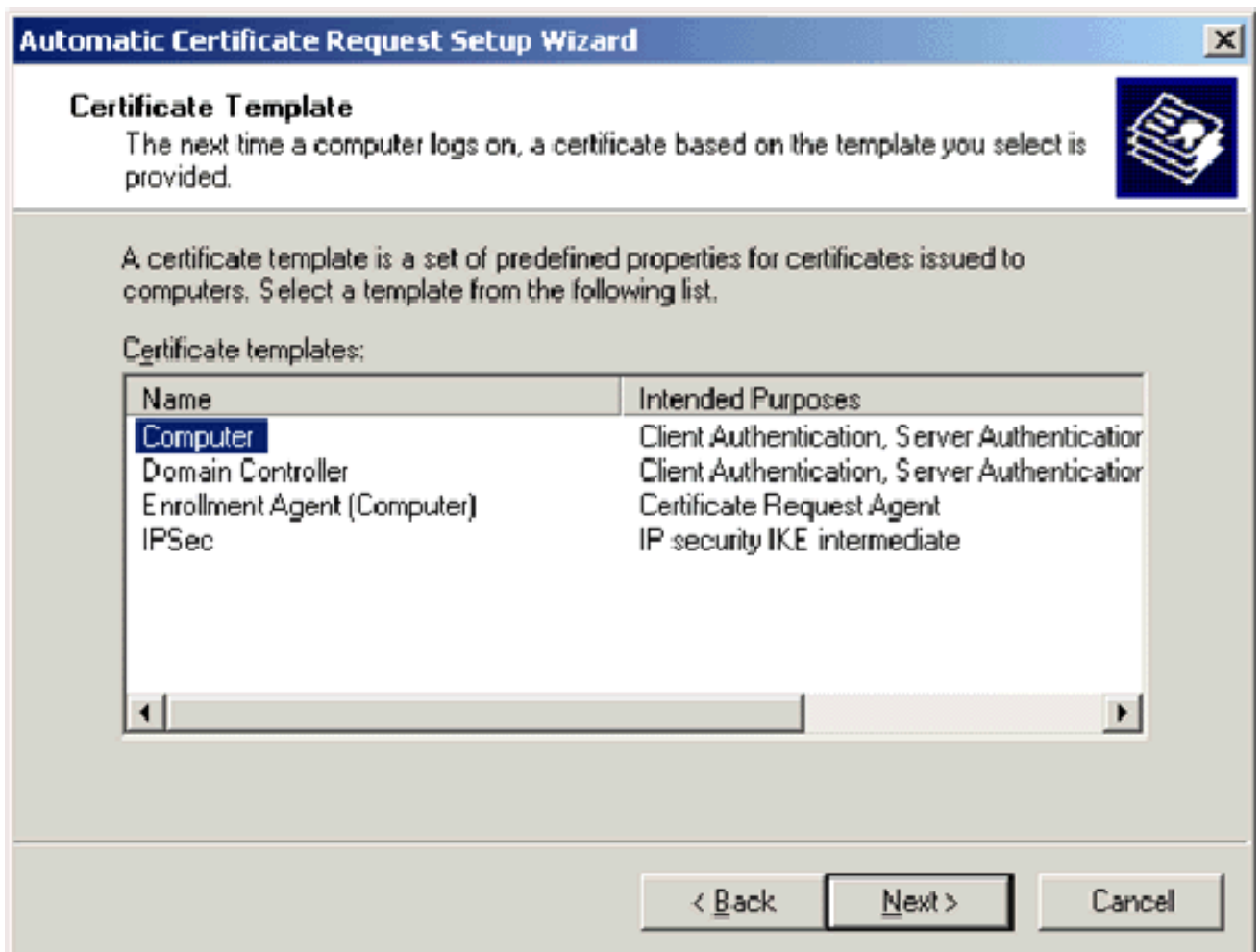
7. Klicken Sie auf der Registerkarte Gruppenrichtlinie auf **Standard-Domänenrichtlinie** und klicken Sie dann auf **Bearbeiten**. Dadurch wird das Snap-In Gruppenrichtlinienobjekteditor geöffnet.



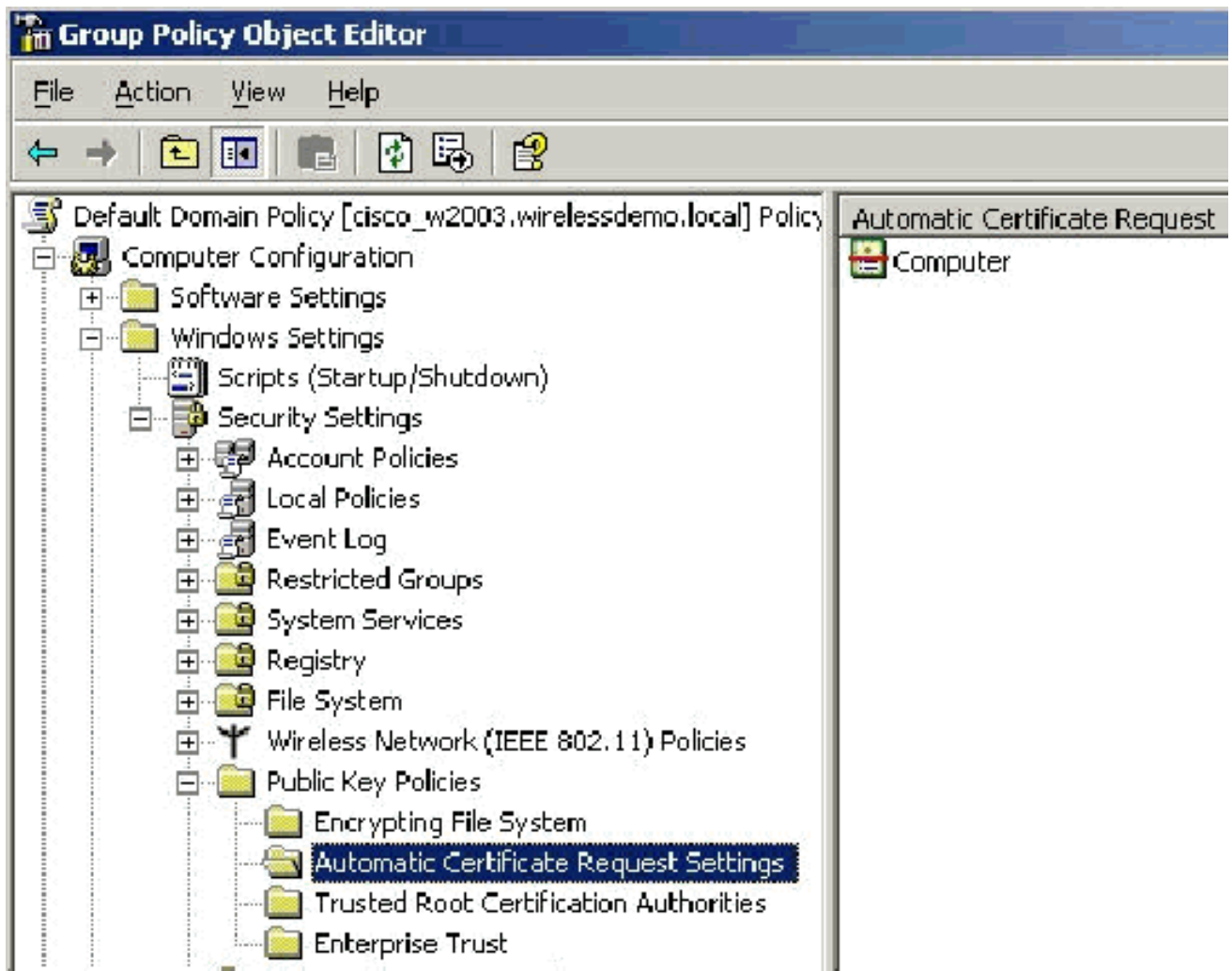
8. Erweitern Sie in der Konsolenstruktur **Computer Configuration > Windows Settings > Security Settings > Public Key Policies (Computerkonfiguration > Windows-Einstellungen > Sicherheitseinstellungen > Öffentliche Schlüsselrichtlinien)**, und wählen Sie **Automatic Certificate Request Settings (Automatische Zertifikatsanforderungseinstellungen)** aus.



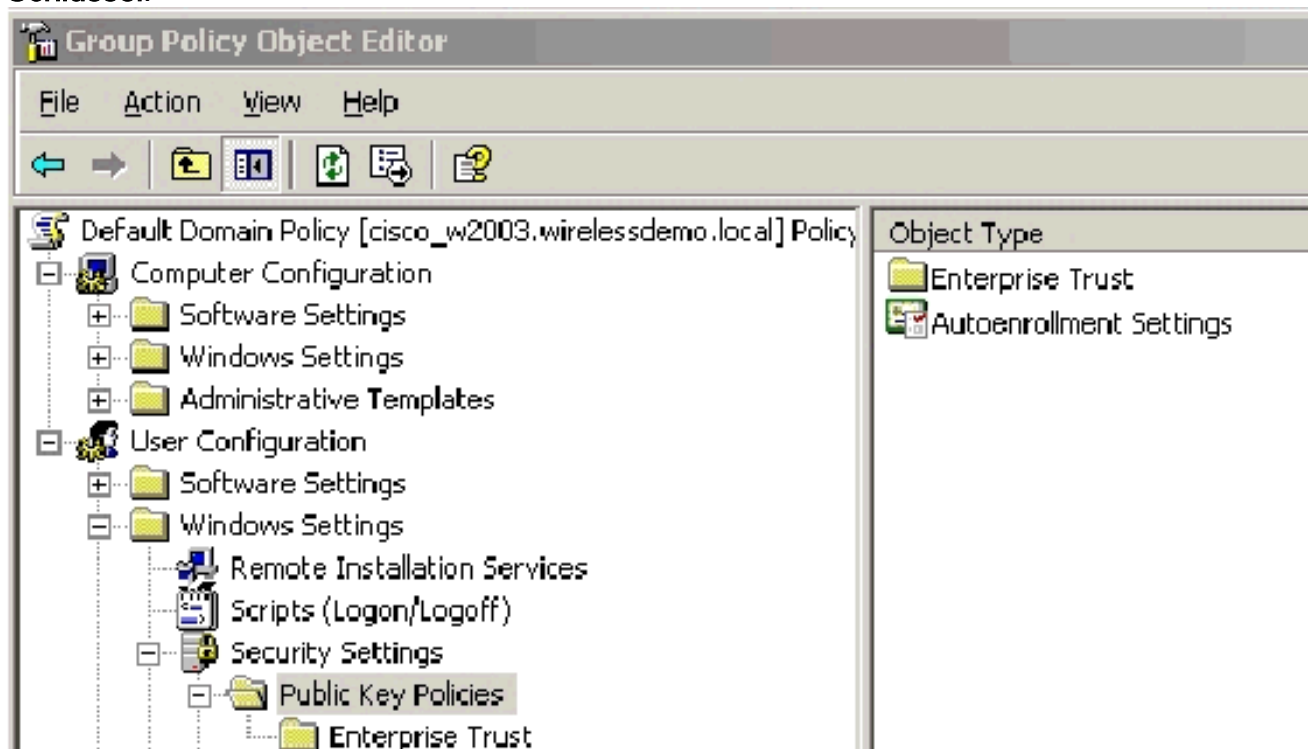
9. Klicken Sie mit der rechten Maustaste auf **Einstellungen für automatische Zertifikatsanforderung** und wählen Sie **Neu > Automatische Zertifikatsanforderung**.
10. Klicken Sie auf der Seite Willkommen beim Assistenten für die automatische Zertifikatsanforderung auf **Weiter**.
11. Klicken Sie auf der Seite Zertifikatvorlage auf **Computer** und dann auf **Weiter**.



12. Klicken Sie auf der Seite Abschließen des Assistenten für die automatische Zertifikatsanforderung auf **Fertig stellen**. Der Computerzertifikattyp wird nun im Detailbereich des Snap-Ins "Gruppenrichtlinienobjekteditor" angezeigt.



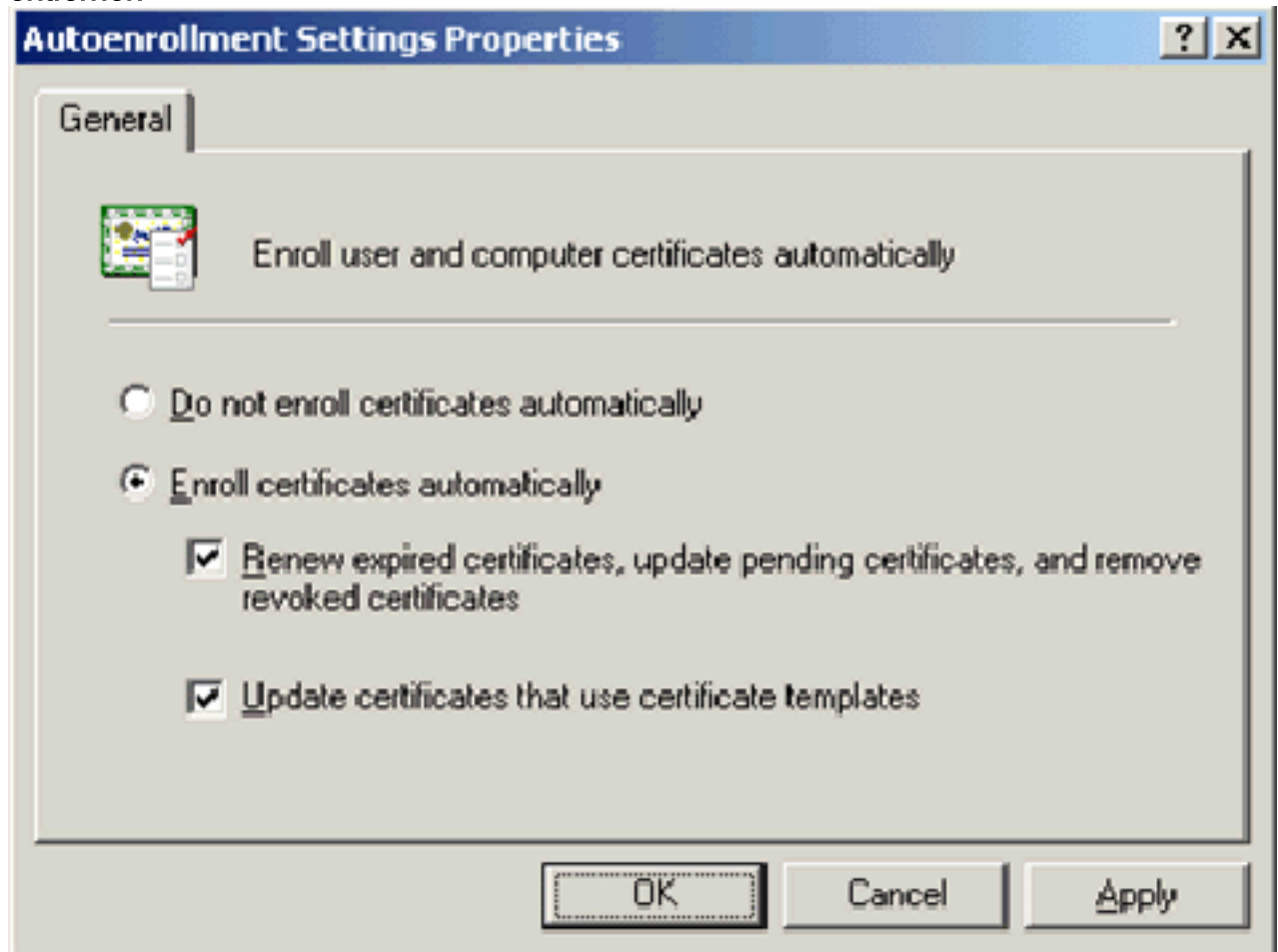
13. Erweitern Sie in der Konsolenstruktur **Benutzerkonfiguration** > **Windows-Einstellungen** > **Sicherheitseinstellungen** > **Richtlinien für öffentlichen Schlüssel**.



14. Doppelklicken Sie im Detailbereich auf **Einstellungen für die automatische Registrierung**.

15. Wählen Sie **Zertifikate automatisch registrieren** und aktivieren Sie die Option **Ausgelaufene**

Zertifikate verlängern, ausstehende Zertifikate aktualisieren sowie widerrufen Zertifikate und Zertifikate mit Zertifikatsvorlagen entfernen.



16. Klicken Sie auf OK.

[ACS 4.0 Zertifikateinrichtung](#)

[Exportfähiges Zertifikat für ACS konfigurieren](#)

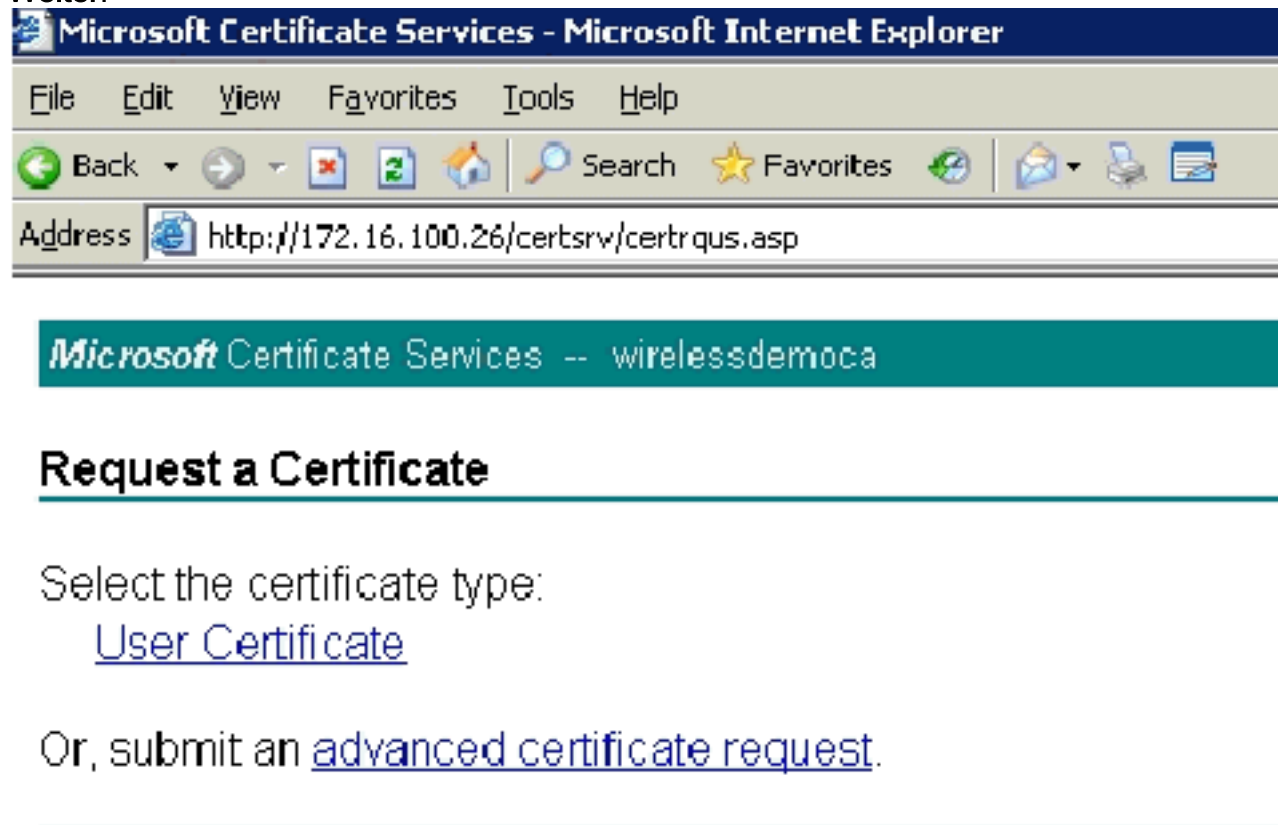
Wichtig: Der ACS-Server muss ein Serverzertifikat vom Enterprise-Root-CA-Server beziehen, um einen WLAN-EAP-TLS-Client zu authentifizieren.

Wichtig: Stellen Sie sicher, dass der IIS-Manager während des Zertifikateinrichtungsprozesses nicht geöffnet ist, da er Probleme mit zwischengespeicherten Informationen verursacht.

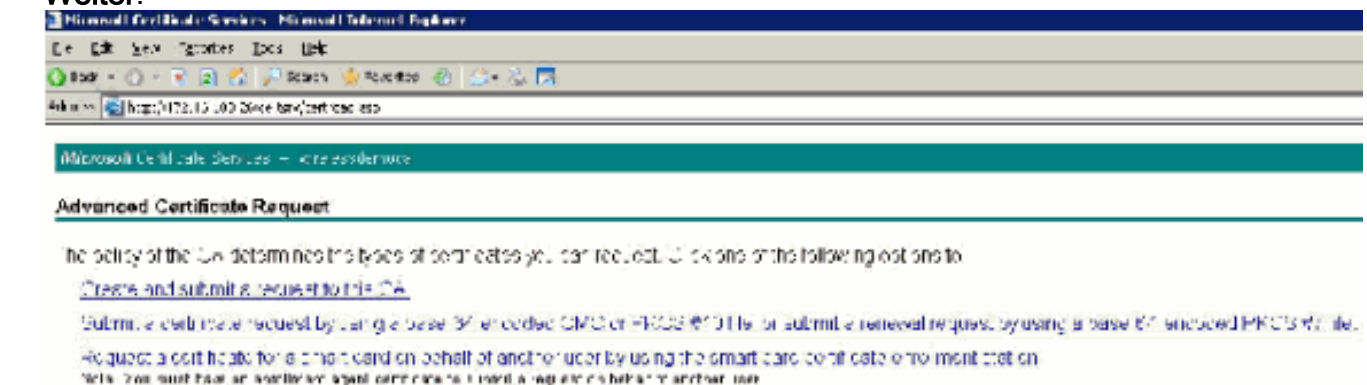
1. Melden Sie sich mit einem Konto mit Enterprise Admin-Rechten beim ACS-Server an.
2. Zeigen Sie auf dem lokalen ACS-Rechner den Browser auf den Microsoft-Zertifizierungsstellen-Server unter **<http://IP-address-of-Root-CA/certsrv>**. In diesem Fall lautet die IP-Adresse **172.16.100.26**.
3. Melden Sie sich als Administrator an.



4. Wählen Sie **Zertifikat anfordern** aus, und klicken Sie auf **Weiter**.



5. Wählen Sie **Erweiterte Anforderung** aus, und klicken Sie auf **Weiter**.



6. Wählen Sie **Erstellen** aus, und senden Sie eine Anfrage an diese CA, und klicken Sie auf **Weiter**. **Wichtig:** Der Grund für diesen Schritt liegt darin, dass Windows 2003 keine exportierbaren Schlüssel zulässt und dass Sie eine Zertifikatsanforderung auf der Grundlage des zuvor erstellten ACS-Zertifikats generieren müssen, das Sie zuvor erstellt

haben.

Microsoft Certificate Services - wirelessdemo.local

Advanced Certificate Request

Certificate Template:

Administrator

Key Options:

Administrator
Basic EFS
EFS Recovery Agent
User
my key set

CSP: Wireless User Certificate Template
Microsoft Base Cryptographic Services

Key Usage: S.Ordinary Certification Authority

Key Store: Web Server
Max: 15384
1024 2048 4096 8192 16384

Automatic key container name User specified key container name

Mark keys as exportable
 Export keys to file

Enable strong private key protection

Store certificate in the local computer certificate store
Saves the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

Request Format: CER PKCS10

Hash Algorithm: SHA-1
Only used to sign request.

Save request to file

Attributes:

Friendly Name:

7. Wählen Sie aus den Zertifikatsvorlagen die Zertifikatsvorlage aus, die zuvor mit dem Namen **ACS** erstellt wurde. Die Optionen ändern sich nach der Auswahl der Vorlage.
8. Konfigurieren Sie den Namen so, dass er der vollqualifizierte Domänenname des ACS-Servers ist. In diesem Fall lautet der ACS-Servername `cisco_w2003.wirelessdemo.local`. Stellen Sie sicher, dass **Zertifikat im Zertifikatsspeicher des lokalen Computers speichern** aktiviert ist, und klicken Sie auf

Microsoft Certificate Services - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://172.16.100.25/certsrv/certreqna.asp

Certificate Template:

ACS

Identifying Information For Offline Template:

Name: cisco_w2000_wirelessdemo.local

E-Mail:

Company:

Department:

City:

State:

Country/Region:

Key Options:

Create new key set Use existing key set

CSP: Microsoft Base Cryptographic Provider v1.0

Key Usage: Exchange

Key Size: 1024 Min:1024 Max:1024 (common key sizes: 3072)

Automatic key container name User specified key container name

Mark keys as exportable

Export keys to file

Store certificate in the local computer certificate store
Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

Request Format: CMC PKCS#10

Hash Algorithm: SHA-1
Only used to sign request.

Save request to a file

Attributes:

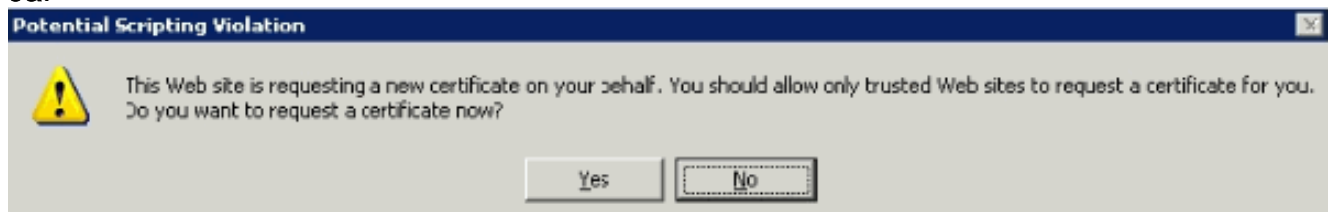
Friendly Name:

Submit >

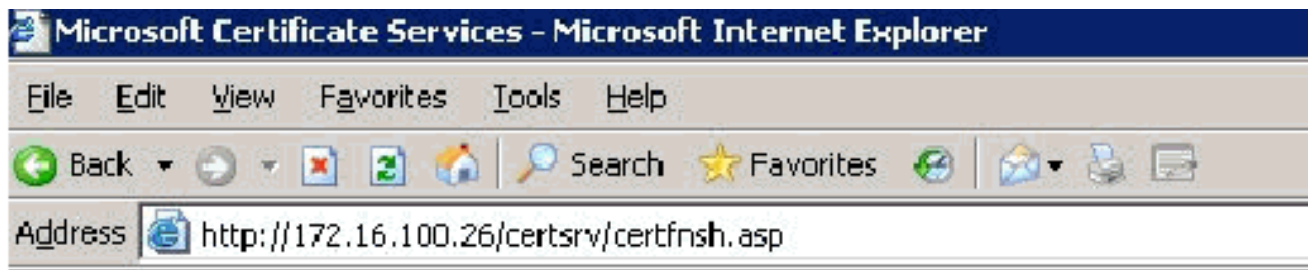
Senden.

9. Ein Popup-Fenster wird angezeigt, das vor einer möglichen Skriptverletzung warnt. Klicken Sie auf

Ja.



10. Klicken Sie auf **Zertifikat installieren**.



Microsoft Certificate Services -- wirelessdemoca

Certificate Issued

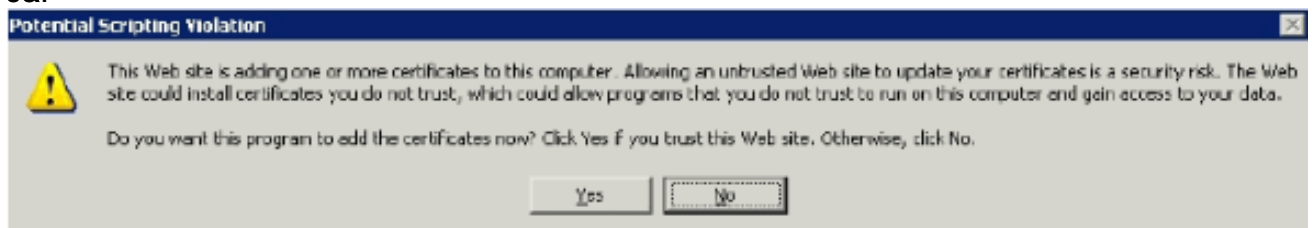
The certificate you requested was issued to you.



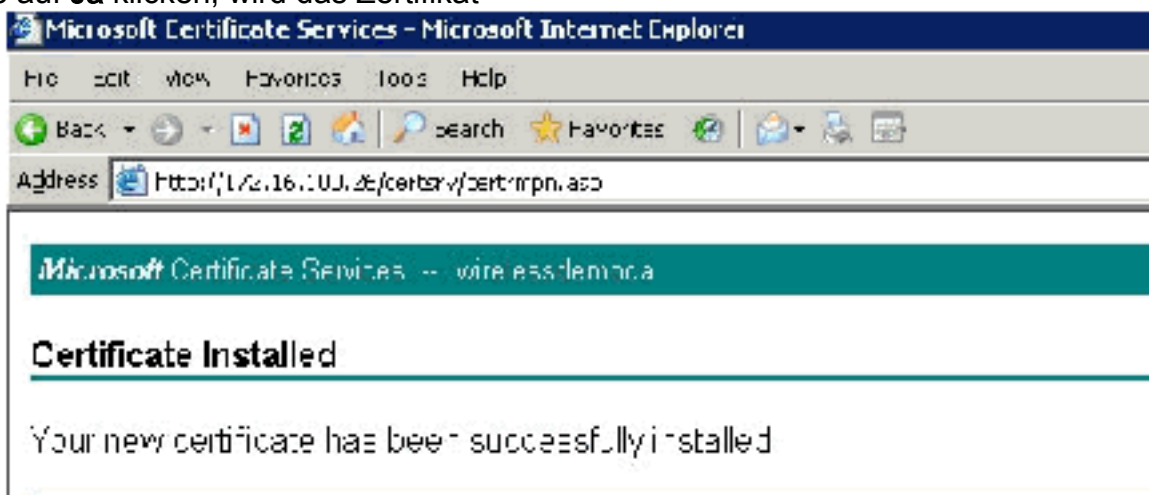
[Install this certificate](#)

11. Ein Popup-Fenster wird erneut angezeigt und warnt vor einer möglichen Skriptverletzung. Klicken Sie auf

Ja.

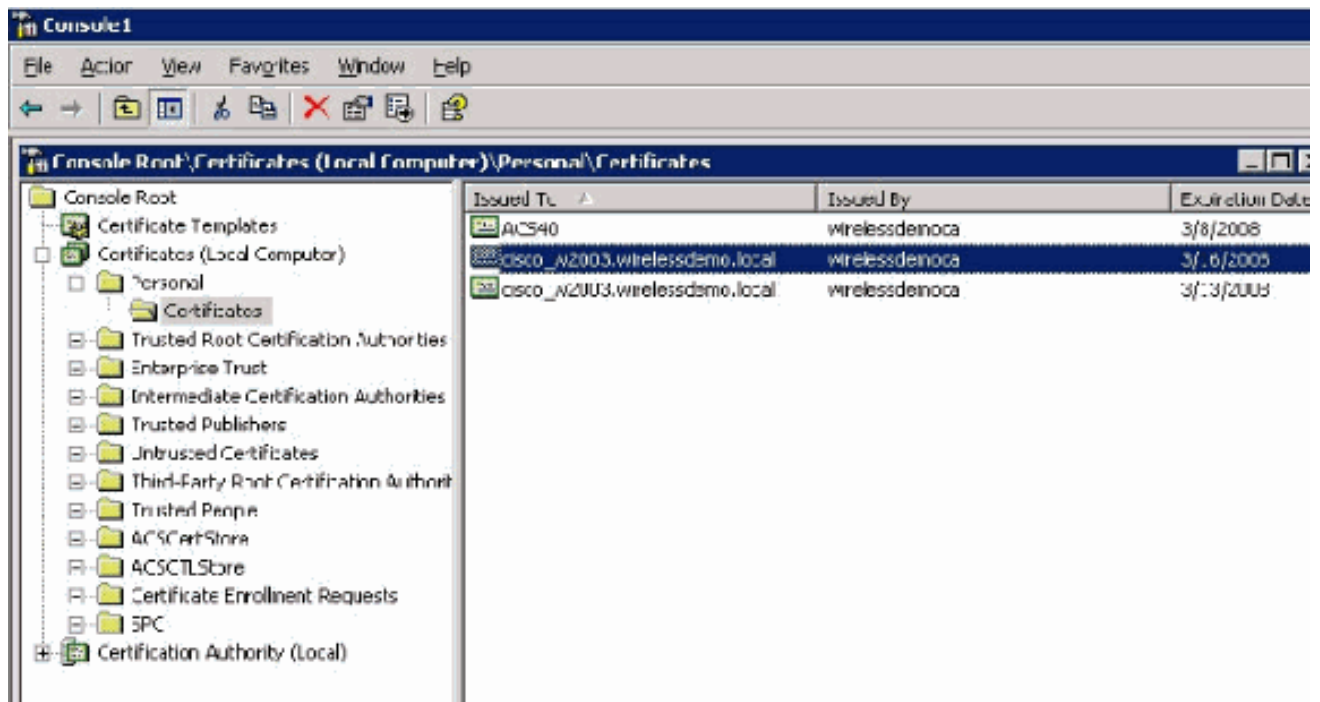


12. Wenn Sie auf **Ja** klicken, wird das Zertifikat



installiert.

13. An diesem Punkt wird das Zertifikat im Ordner Zertifikate installiert. Um auf diesen Ordner zuzugreifen, wählen Sie **Start > Ausführen**, geben Sie **mmc** ein, drücken Sie die **Eingabetaste**, und wählen Sie **Personal > Certificates** aus.



14. Nachdem das Zertifikat nun auf dem lokalen Computer installiert ist (in diesem Beispiel ACS oder cisco_w2003), müssen Sie eine Zertifikatsdatei (.cer) für die ACS 4.0-Zertifikatsdateikonfiguration generieren.
15. Zeigen Sie auf dem ACS-Server (in diesem Beispiel cisco_w2003) im Browser des Microsoft Certification Authority-Servers auf <http://172.16.100.26/certsrv>.

[Installieren des Zertifikats in der ACS 4.0-Software](#)

Führen Sie diese Schritte aus:

1. Zeigen Sie auf dem ACS-Server (in diesem Beispiel cisco_w2003) im Browser des Microsoft CA-Servers auf <http://172.16.100.26/certsrv>.
2. Wählen Sie aus der Option Task auswählen die Option **Zertifikat, Zertifikatskette oder CRL herunterladen aus**.
3. Wählen Sie das Optionskodierungsverfahren **Base 64** aus, und klicken Sie auf **CA-Zertifikat herunterladen**.

Microsoft Certificate Services - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address http://172.16.100.26/certs/v/certbase.asp

Microsoft Certificate Services -- wirelessdemora

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority [install this CA certificate chain](#).

To download a CA certificate, certificate chain, or CRL, select the certificate encoding method:

CA certificate:

Current (wirelessdemora)

Encoding method:

DER

Base 64

[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

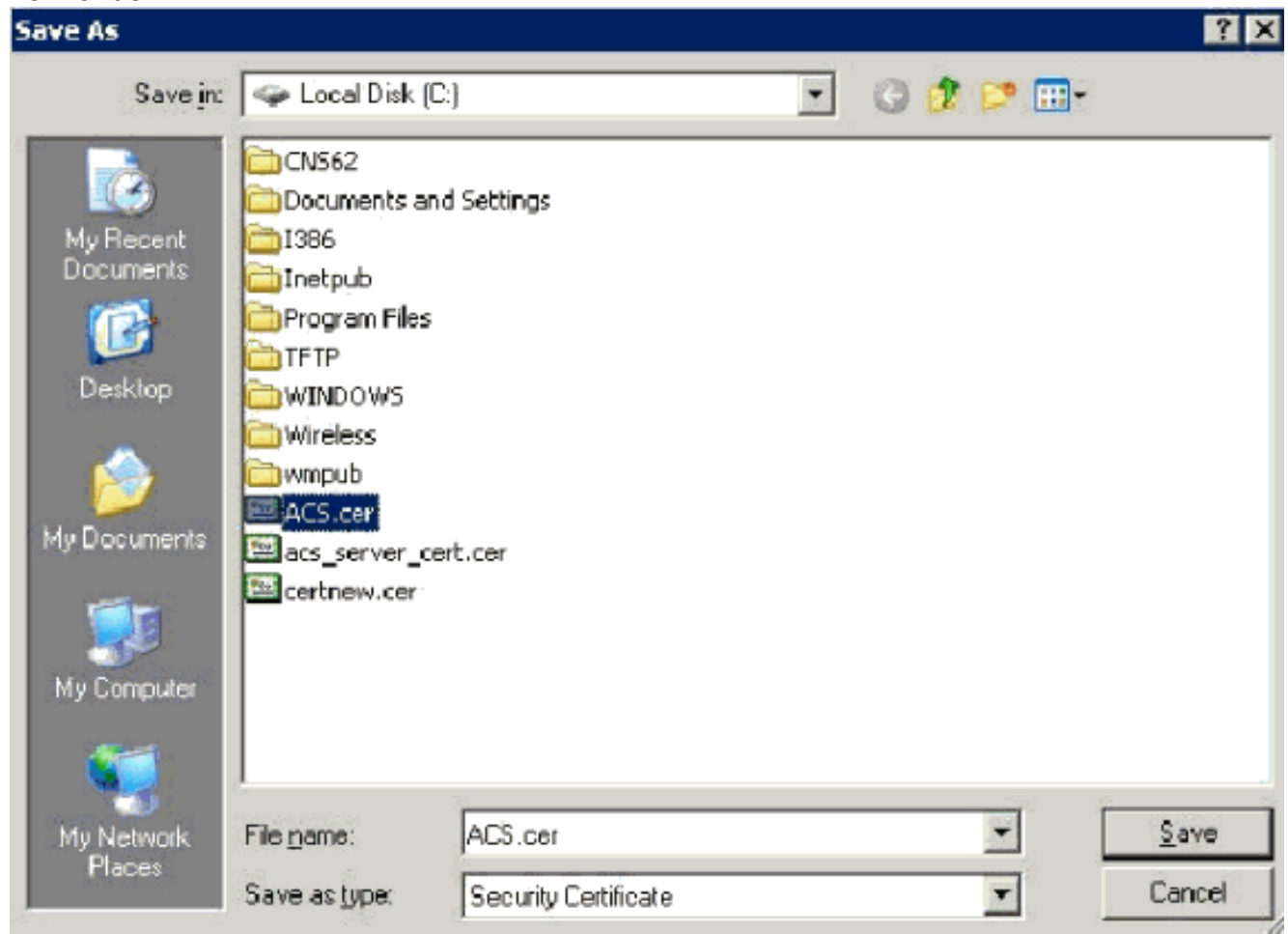
[Download latest delta CRL](#)

4. Ein Fenster mit einer Sicherheitswarnung für Dateidownload wird angezeigt. Klicken Sie auf **Speichern**.



5. Speichern Sie die Datei mit einem Namen wie ACS.cer oder einem beliebigen Namen, den Sie wünschen. Beachten Sie diesen Namen, da Sie ihn während der ACS Certificate

Authority-Einrichtung in ACS 4.0 verwenden.

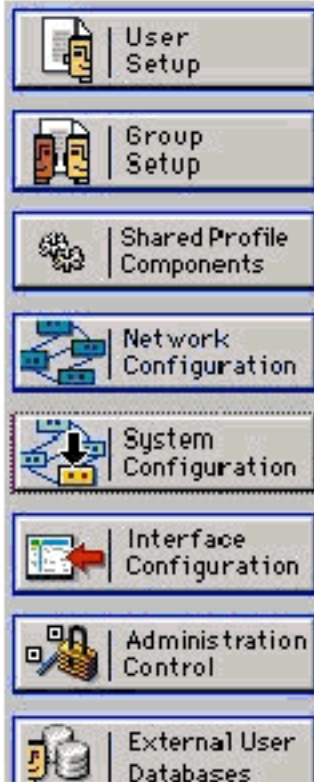


6. Öffnen Sie **ACS Admin** über die Desktop-Verknüpfung, die während der Installation erstellt wurde.
7. Klicken Sie auf **Systemkonfiguration**.



System Configuration

Select



-  [Service Control](#)
-  [Logging](#)
-  [Date Format Control](#)
-  [Local Password Management](#)
-  [ACS Internal Database Replication](#)
-  [ACS Backup](#)
-  [ACS Restore](#)
-  [ACS Service Management](#)
-  [VoIP Accounting Configuration](#)
-  [ACS Certificate Setup](#)
-  [Global Authentication Setup](#)

8. Klicken Sie auf **ACS Certificate Setup**.

System Configuration

Select

ACS Certificate Setup

-  [Install ACS Certificate](#)
-  [ACS Certification Authority Setup](#)
-  [Edit Certificate Trust List](#)
-  [Certificate Revocation Lists](#)
-  [Generate Certificate Signing Request](#)
-  [Generate Self-Signed Certificate](#)

Cancel

9. Klicken Sie auf **ACS-Zertifikat** installieren.

System Configuration

Edit

Install ACS Certificate

Install new certificate 	
<input type="radio"/> Read certificate from file	
Certificate file	<input type="text"/>
<input checked="" type="radio"/> Use certificate from storage	
Certificate CN	<input type="text"/>
Private key file	<input type="text"/>
Private key password	<input type="text"/>

10. Wählen Sie **Zertifikat aus Speicher verwenden** aus, und geben Sie den vollqualifizierten Domännennamen von **cisco_w2003.wirelessdemo.local** (oder **ACS.wirelessdemo.local**, wenn Sie ACS als Namen verwenden)

ein.

System Configuration

Edit

Install ACS Certificate

Install new certificate 

Read certificate from file

Certificate file

Use certificate from storage

Certificate CN

Private key file


Private key password

11. Klicken Sie auf
Senden.

System Configuration

Edit

Install ACS Certificate

Installed Certificate Information 

Issued to:	cisco_w2003.wirelessdemo.local
Issued by:	wirelessdemoca
Valid from:	March 17 2006 at 08:33:25
Valid to:	March 16 2008 at 08:33:25
Validity:	OK


**The current configuration has been changed.
Restart ACS in "System Configuration:Service
Control" to adopt the new settings for EAP-TLS or
PEAP support only.**

12. Klicken Sie auf Systemkonfiguration.


13. Klicken Sie auf **Dienststeuerung** und dann auf **Neu starten**.

System Configuration

Select

CiscoSecure ACS on cisco_w2003 

Is Currently Running

Services Log File Configuration 

Level of detail

None

Low

Full

Generate New File

Every day

Every week


Every month

When size is greater than KB

Manage Directory

Keep only the last files


Delete files older than days

 [Back to Help](#)

14. Klicken Sie auf **Systemkonfiguration**.
15. Klicken Sie auf **Global Authentication Setup**.
16. Aktivieren Sie **EAP-TLS** und alle darunter befindlichen Felder **zulassen**.

System Configuration

Global Authentication Setup

EAP Configuration 

PEAP

Allow EAP-MSCHAPv2

Allow EAP-GTC

Allow Posture Validation

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

EAP-FAST

[EAP-FAST Configuration](#)

EAP-TLS

Allow EAP-TLS

Select one or more of the following options:

- Certificate SAN comparison
- Certificate CN comparison
- Certificate Binary comparison

EAP-TLS session timeout (minutes):

17. Klicken Sie auf **Senden + Neu starten**.

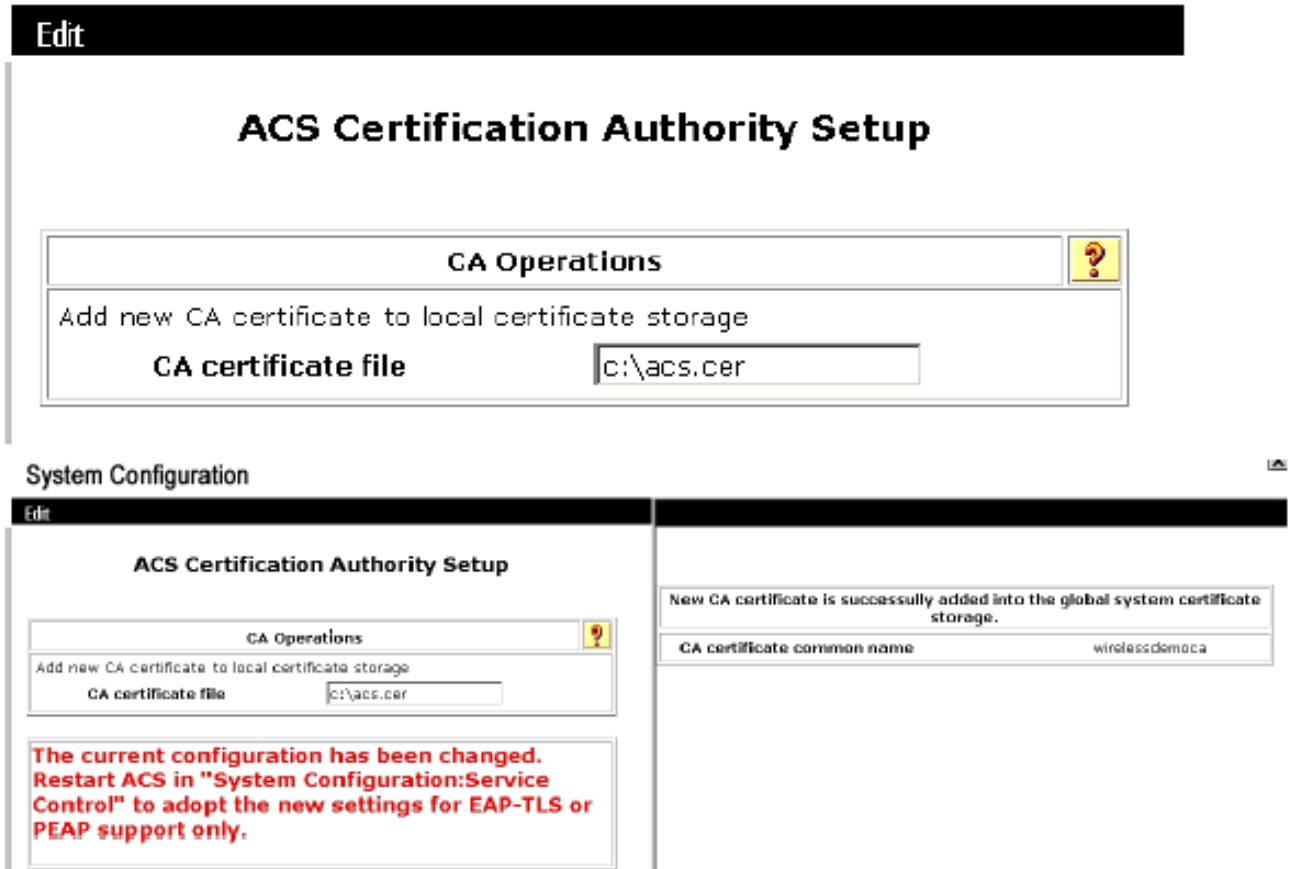
18. Klicken Sie auf **Systemkonfiguration**.

19. Klicken Sie auf **ACS Certification Authority Setup**.

20. Geben Sie im Fenster ACS Certification Authority Setup (Einrichtung der ACS-Zertifizierungsstelle) den Namen und den Speicherort der zuvor erstellten *.cer-Datei ein. In diesem Beispiel ist die erstellte Datei *.cer **ACS.cer** im Stammverzeichnis c:\.

21. Geben Sie **c:\acs.cer** in das Feld Zertifizierungsstellen-Datei ein, und klicken Sie auf **Senden**.

System Configuration



ACS Certification Authority Setup

CA Operations

Add new CA certificate to local certificate storage

CA certificate file

New CA certificate is successfully added into the global system certificate storage.

CA certificate common name wirelessdemo.ca

The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.

22. Starten Sie den ACS-Dienst neu.

[CLIENT-Konfiguration für EAP-TLS mit Windows Zero Touch](#)

CLIENT ist ein Computer, auf dem Windows XP Professional mit SP2 ausgeführt wird, der als Wireless-Client fungiert und über den Wireless Access Point Zugriff auf Intranet-Ressourcen erhält. Führen Sie die in diesem Abschnitt beschriebenen Schritte aus, um CLIENT als Wireless-Client zu konfigurieren.

[Durchführen einer grundlegenden Installation und Konfiguration](#)

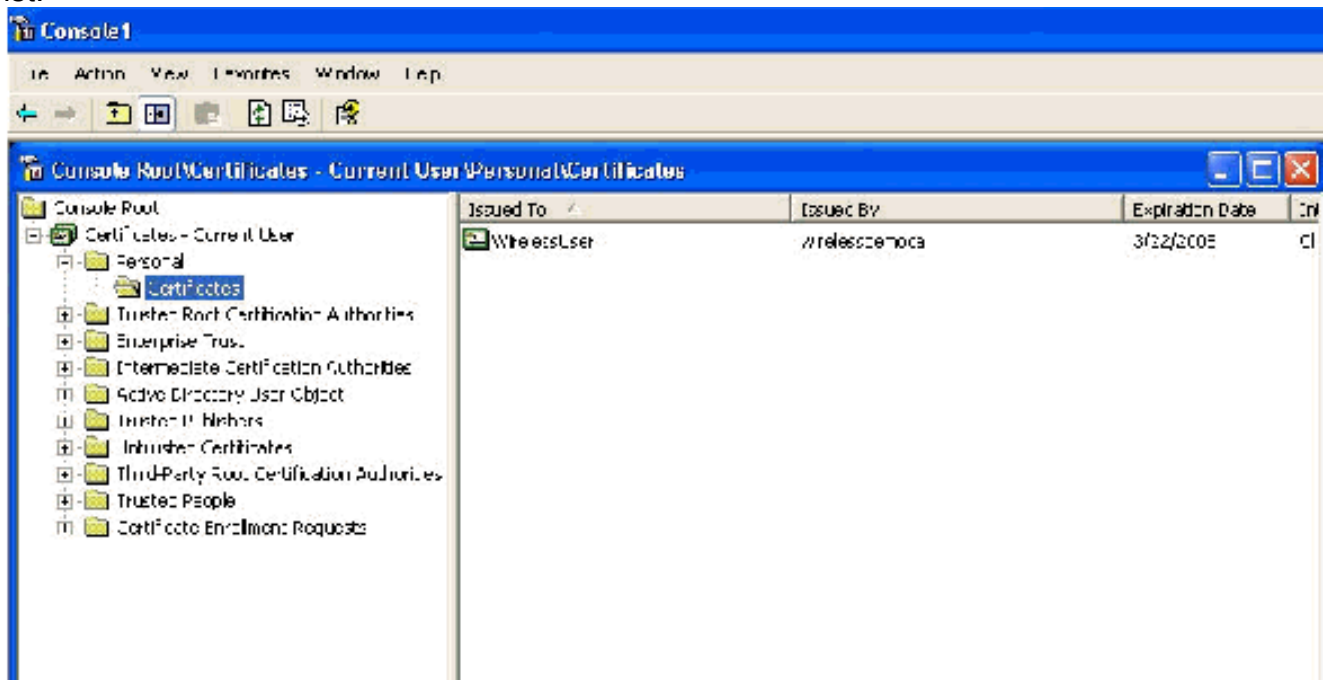
Führen Sie diese Schritte aus:

1. Verbinden Sie CLIENT mithilfe eines mit dem Switch verbundenen Ethernetkabels mit dem Intranet-Netzwerksegment.
2. Installieren Sie auf CLIENT Windows XP Professional mit SP2 als Mitgliedscomputer mit dem Namen **CLIENT** in der Domäne "wirelessdemo.local".
3. Installieren Sie Windows XP Professional mit SP2. Diese muss installiert werden, damit EAP-TLS und PEAP unterstützt werden. **Hinweis:** Windows-Firewall wird automatisch in Windows XP Professional mit SP2 aktiviert. Schalten Sie die Firewall nicht aus.

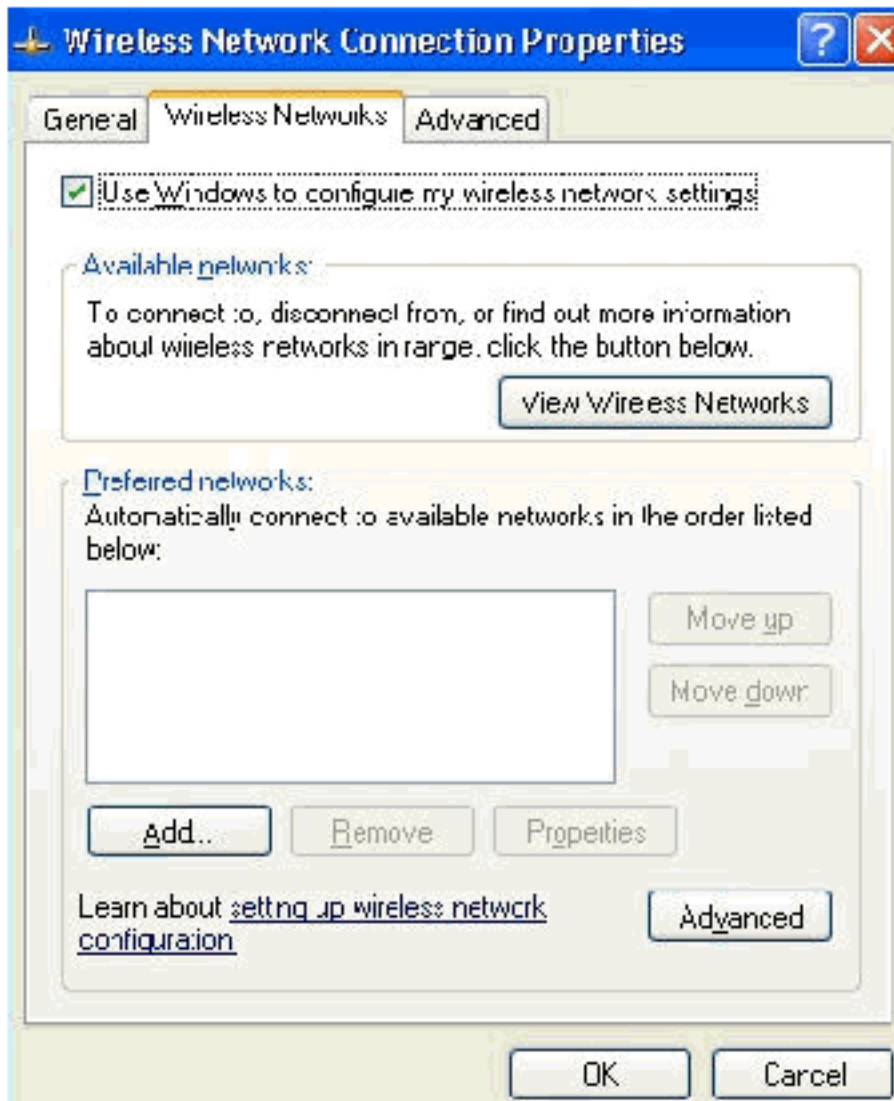
[Konfigurieren der Wireless-Netzwerkverbindung](#)

Führen Sie diese Schritte aus:

1. Melden Sie sich ab, und melden Sie sich dann mit dem WirelessUser-Konto in der Domäne "wirelessDemo.local" an.**Hinweis:** Aktualisieren Sie die Richtlinieneinstellungen für Computer- und Benutzergruppen, und rufen Sie sofort ein Computer- und Benutzerzertifikat für den Wireless-Client-Computer ab, indem Sie an der Eingabeaufforderung **gpupdate** eingeben. Andernfalls wird bei der Abmeldung und anschließenden Anmeldung dieselbe Funktion wie **gpupdate** ausgeführt. Sie müssen über das Kabel bei der Domäne angemeldet sein.**Hinweis:** Um zu überprüfen, ob das Zertifikat automatisch auf dem Client installiert ist, öffnen Sie das MMC-Zertifikat und überprüfen Sie, ob das WirelessUser-Zertifikat im Ordner Persönliche Zertifikate verfügbar ist.

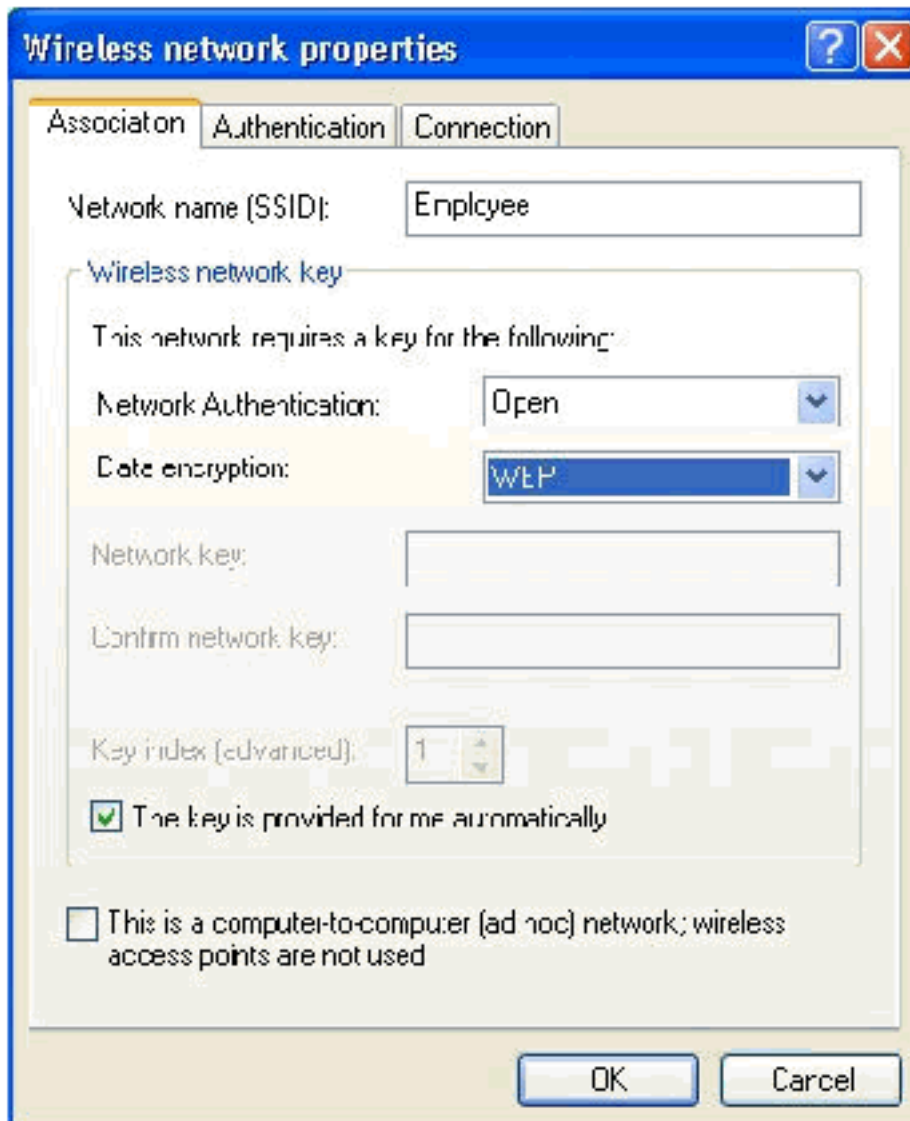


2. Wählen Sie **Start > Systemsteuerung**, doppelklicken Sie auf **Netzwerkverbindungen**, und klicken Sie dann mit der rechten Maustaste auf **Drahtlose Netzwerkverbindung**.
3. Klicken Sie auf **Eigenschaften**, gehen Sie zur Registerkarte Wireless Networks (Wireless-Netzwerke), und stellen Sie sicher, dass **Benutzer Windows zum Konfigurieren der Einstellungen meiner Wireless-Netzwerke** aktiviert



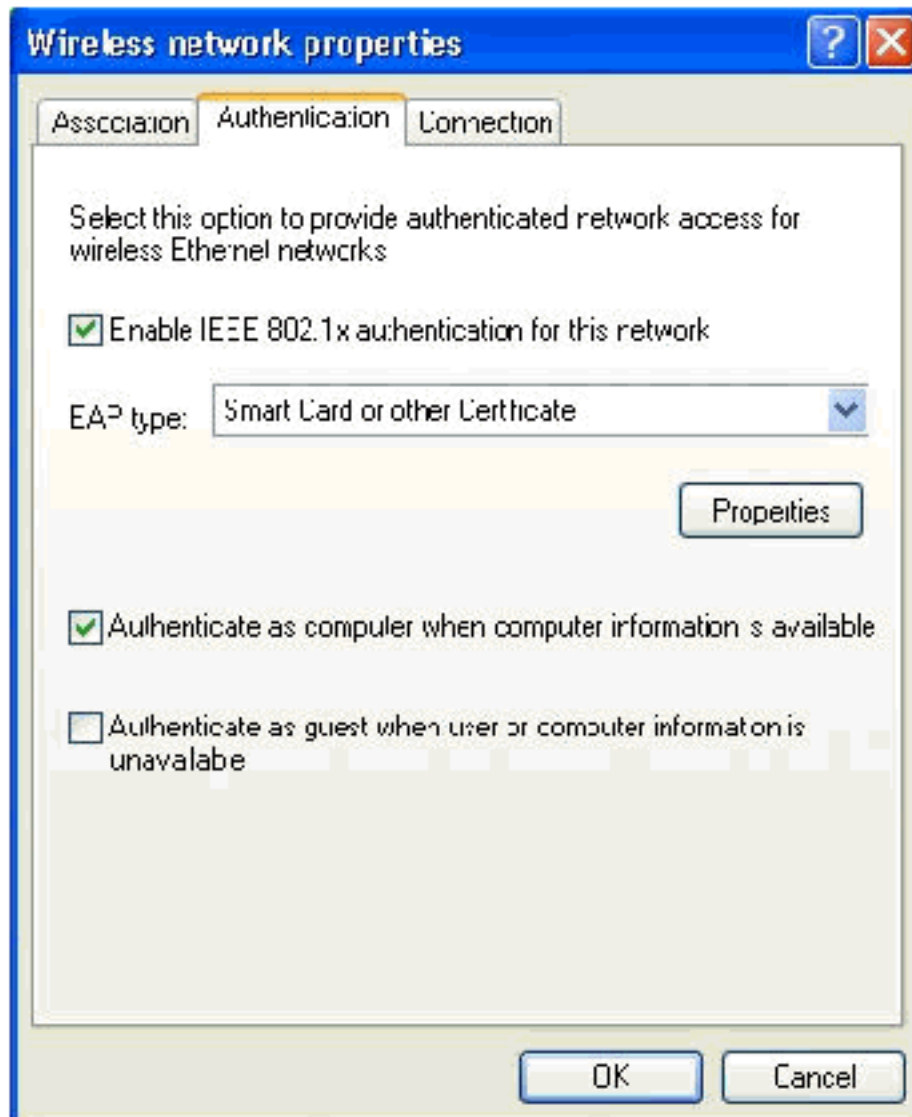
ist.

4. Klicken Sie auf **Hinzufügen**.
5. Öffnen Sie die Registerkarte Association (Zuordnung), und geben Sie **Employee** im Feld Netzwerkname (SSID) ein.
6. Stellen Sie sicher, dass die Datenverschlüsselung auf **WEP** eingestellt ist und **der Schlüssel für mich automatisch** aktiviert



ist.

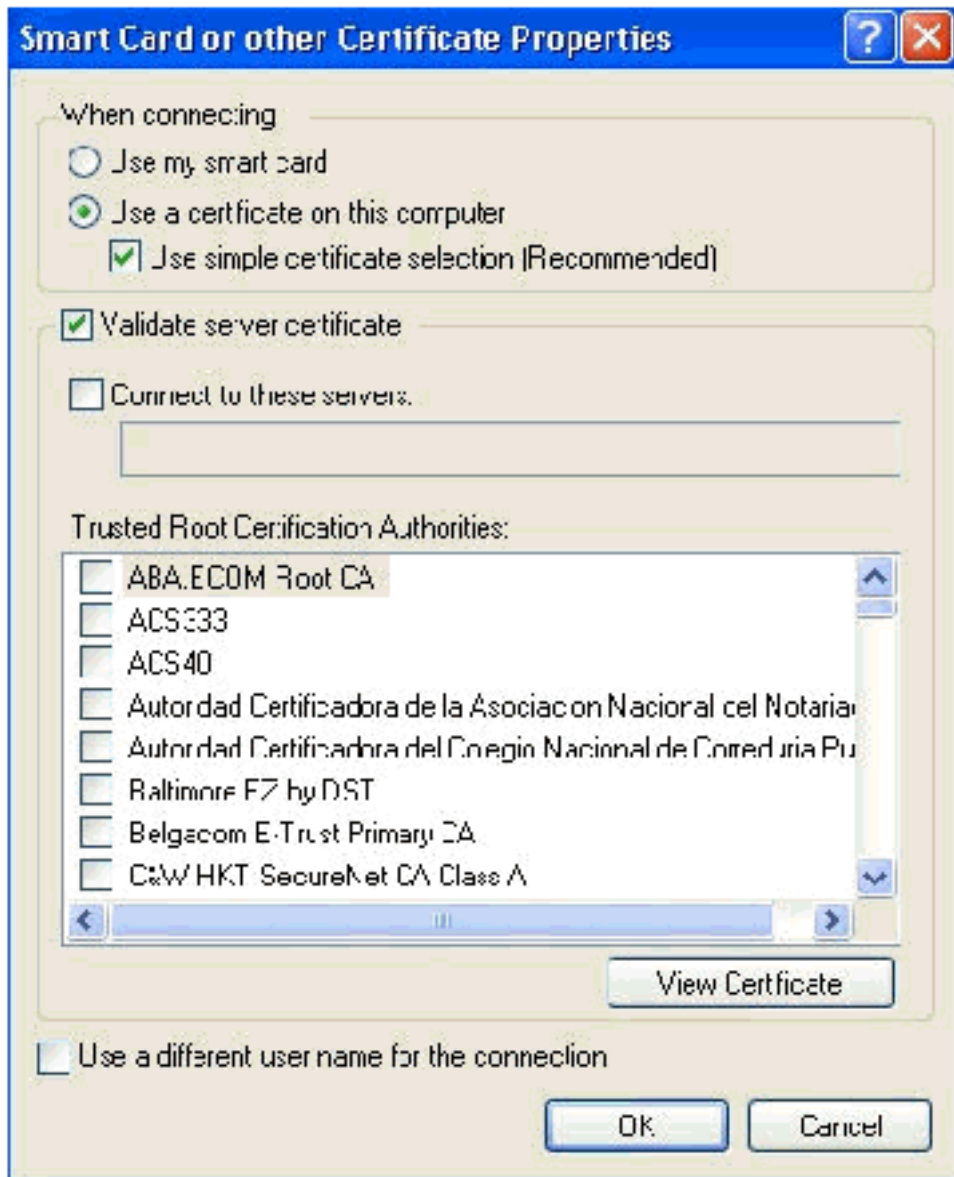
7. Öffnen Sie die Registerkarte Authentifizierung.
8. Überprüfen Sie, ob der EAP-Typ für die Verwendung von **Smart Card oder einem anderen Zertifikat** konfiguriert ist. Ist dies nicht der Fall, wählen Sie es aus dem Dropdown-Menü aus.
9. Wenn Sie möchten, dass der Computer vor der Anmeldung authentifiziert wird (was die Anwendung von Anmeldeskripten oder Gruppenrichtlinien ermöglicht), wählen Sie die Option **Als Computer authentifizieren, wenn Computerinformationen verfügbar**



sind.

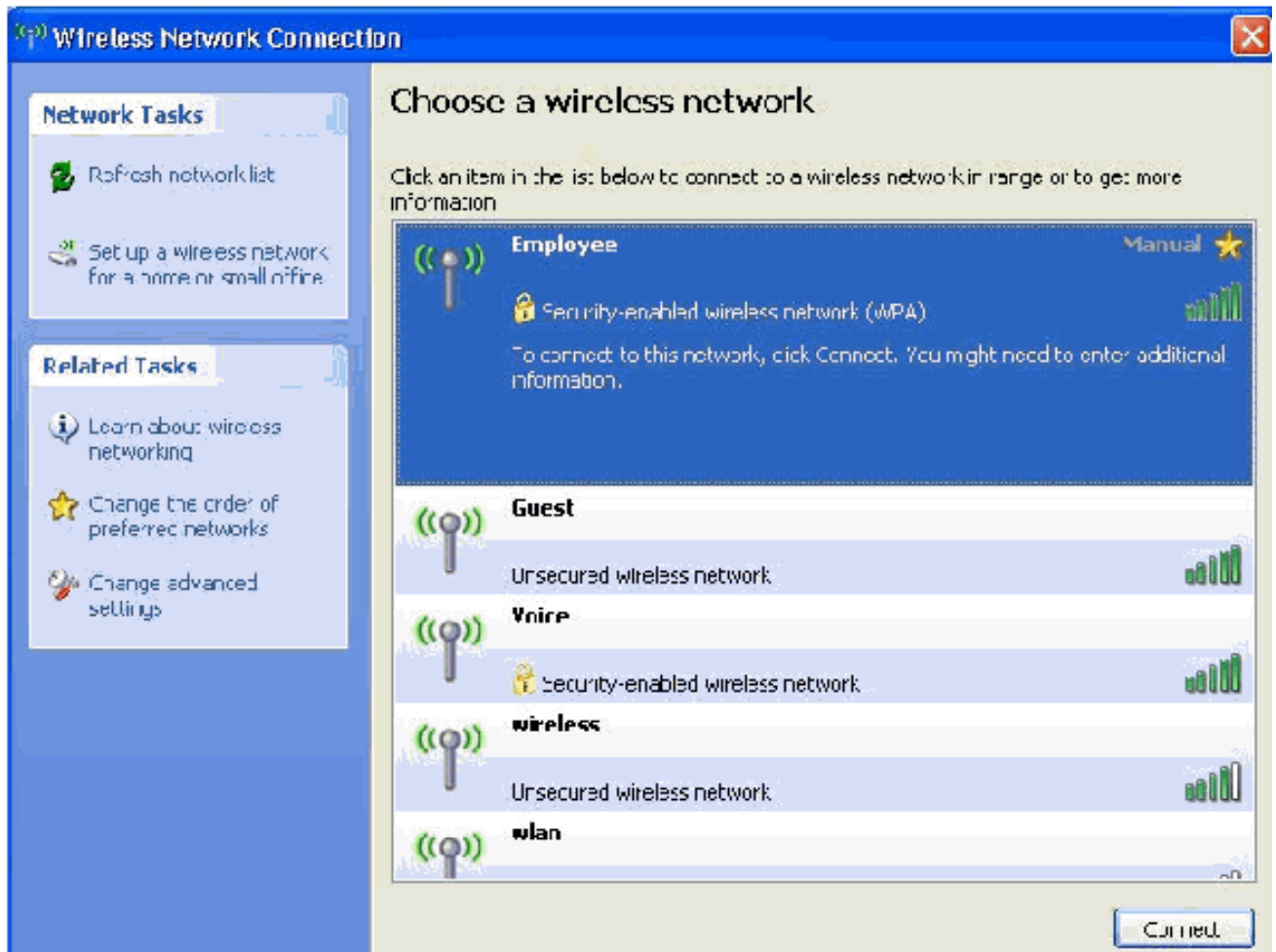
10. Klicken Sie auf **Eigenschaften**.

11. Stellen Sie sicher, dass die Kontrollkästchen in diesem Fenster aktiviert

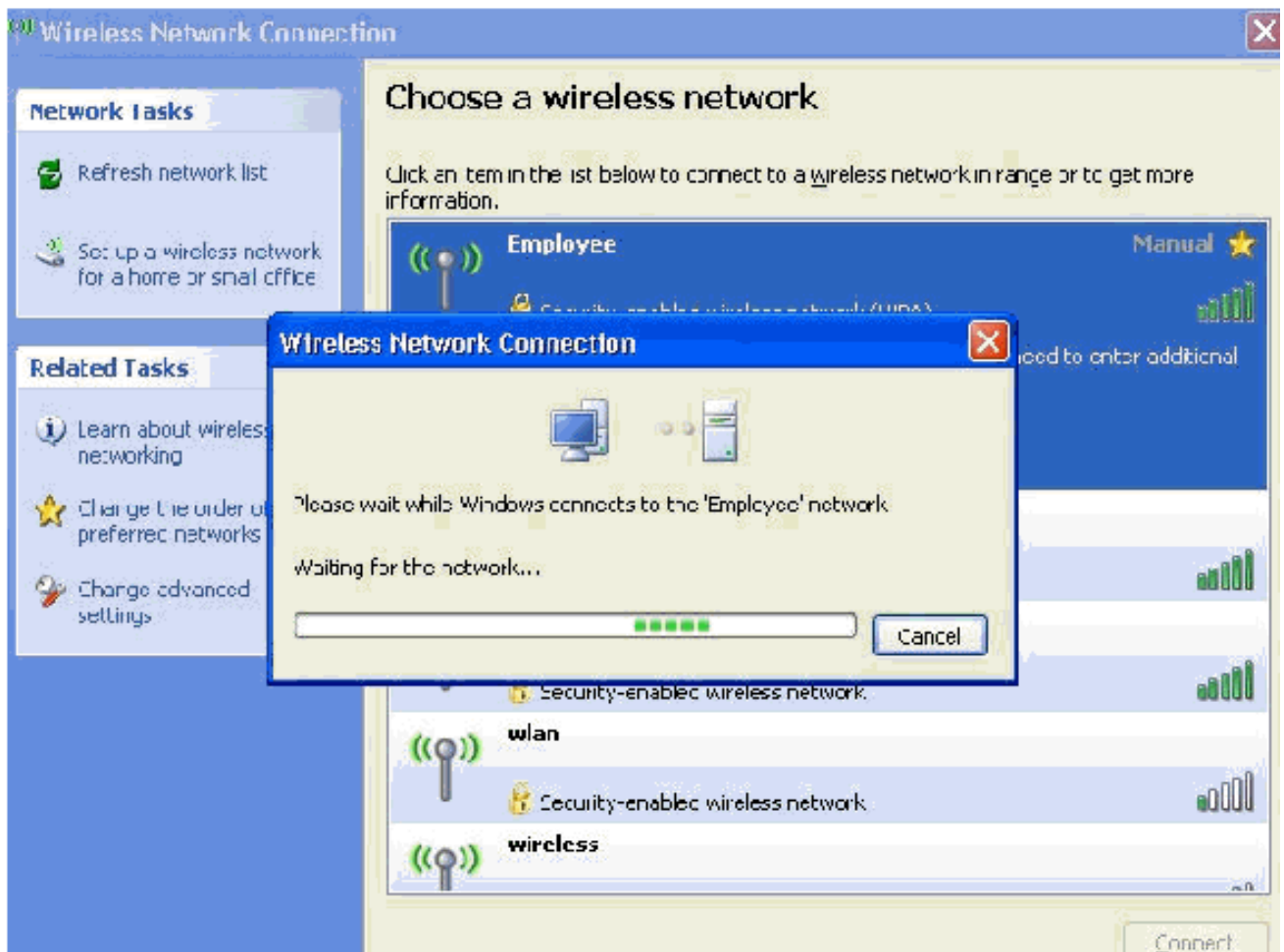


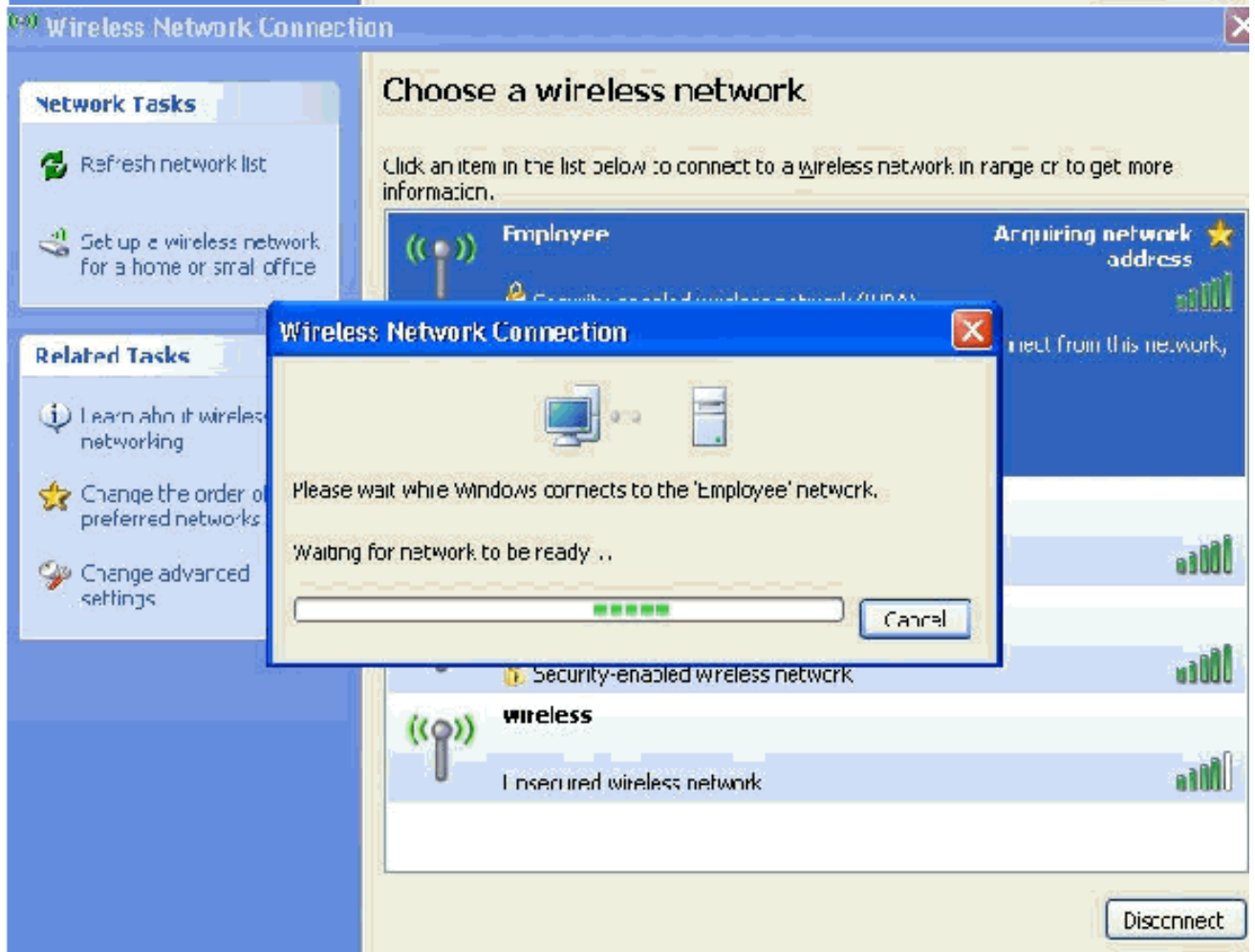
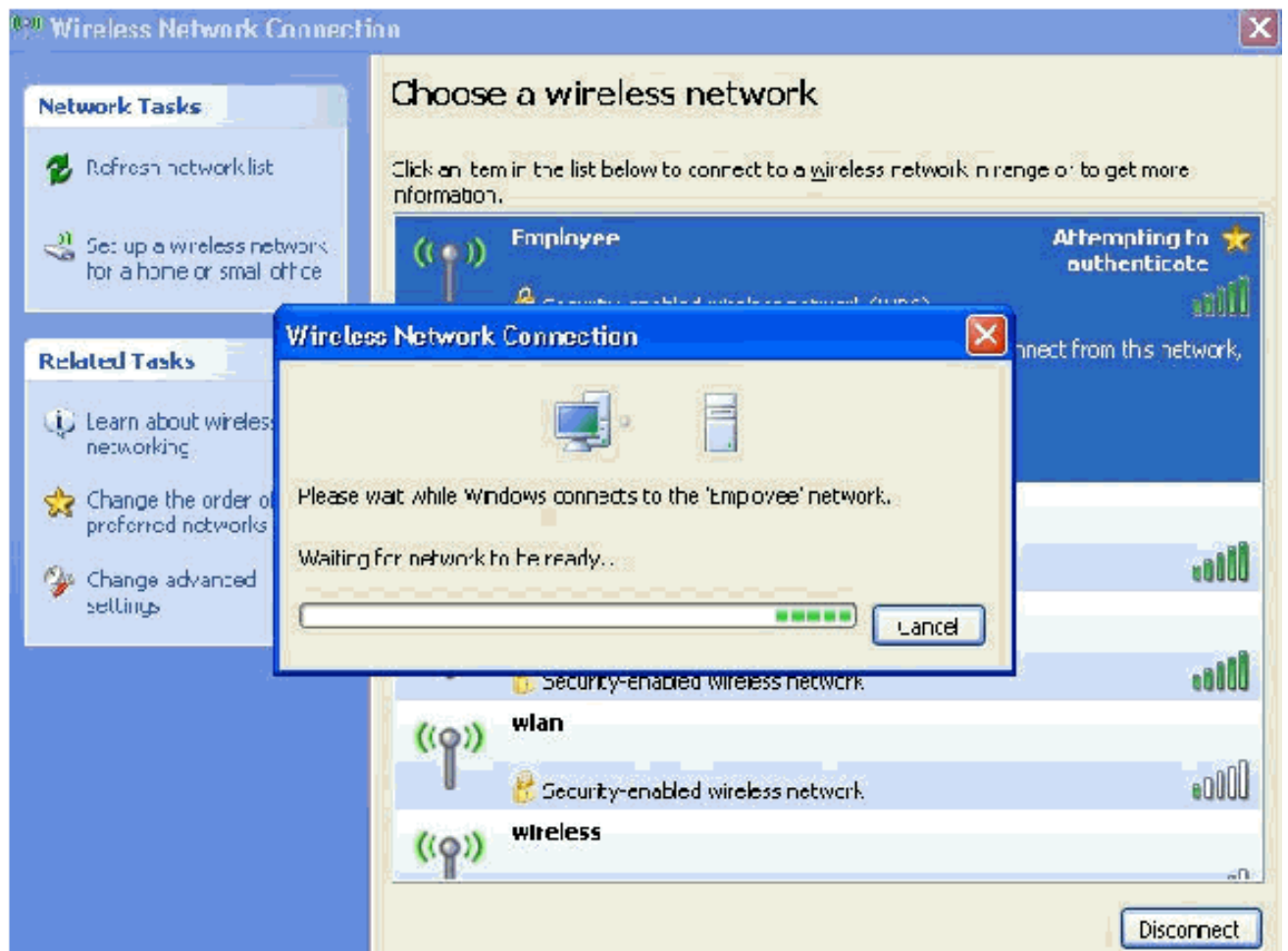
sind.

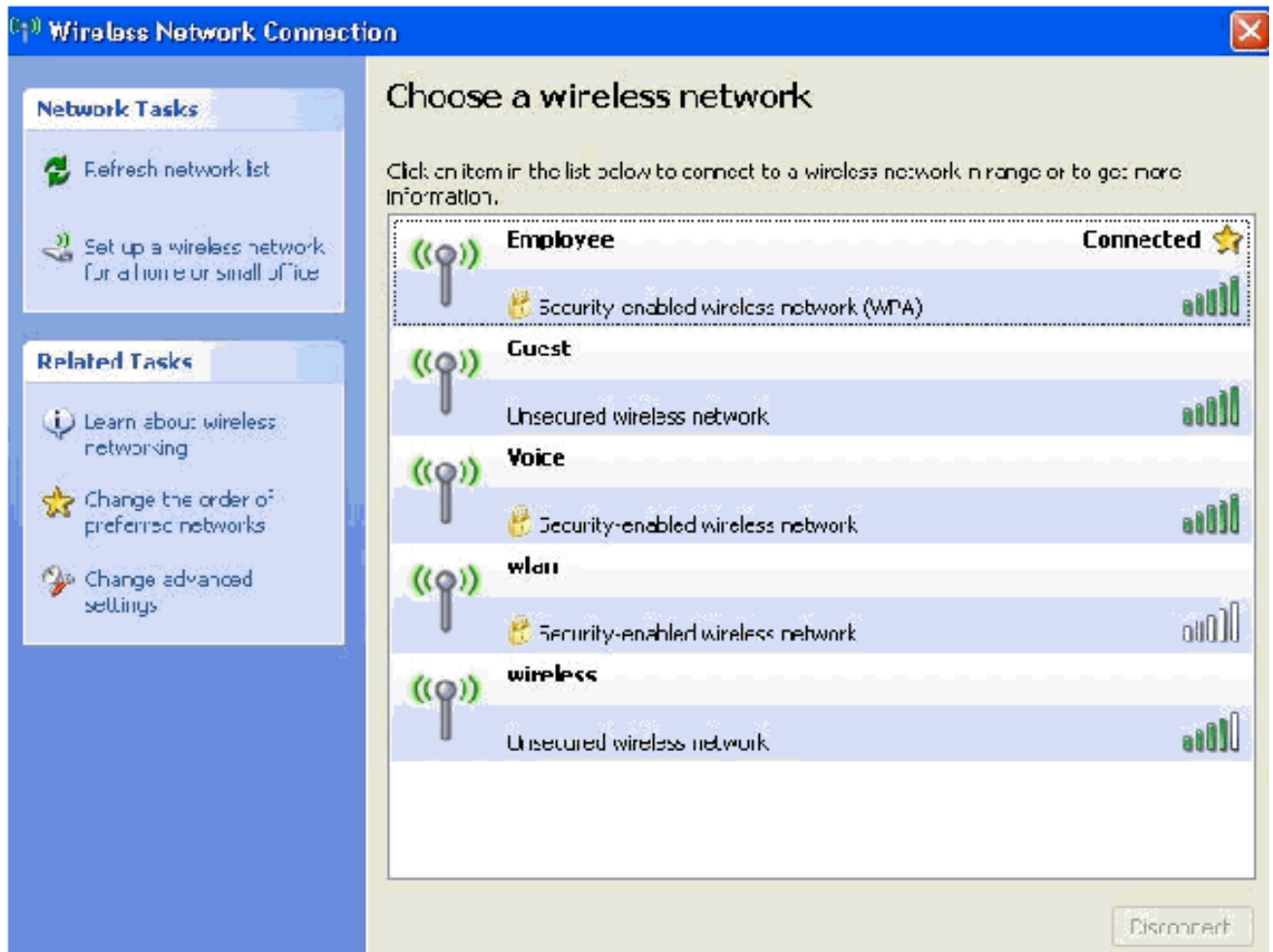
12. Klicken Sie dreimal **auf OK**.
13. Klicken Sie im System mit der rechten Maustaste auf das Symbol für die Wireless-Netzwerkverbindung, und klicken Sie dann auf **Verfügbare Wireless-Netzwerke anzeigen**.
14. Klicken Sie auf das Wireless-Netzwerk **Mitarbeiter** und dann auf **Verbinden**.



Diese Screenshots zeigen an, ob die Verbindung erfolgreich abgeschlossen wurde.







15. Nachdem die Authentifizierung erfolgreich war, überprüfen Sie die TCP/IP-Konfiguration für den Wireless-Adapter mithilfe von Netzwerkverbindungen. Der Adressbereich des DHCP-Bereichs bzw. des für die Wireless-Clients erstellten Bereichs sollte 172.16.100.100-172.16.100.254 betragen.
16. Öffnen Sie zum Testen der Funktionalität einen Browser, und rufen Sie <http://wirelessdemoca> (oder die IP-Adresse des Enterprise CA-Servers) auf.

Zugehörige Informationen

- [Konfigurationsbeispiel für EAP-Authentifizierung mit WLAN-Controllern \(WLC\)](#)
- [Konfigurationsleitfaden für Wireless LAN-Controller](#)
- [Grundlegende Konfigurationsbeispiel für Wireless LAN Controller und Lightweight Access Point](#)
- [Konfigurationsbeispiel für VLANs auf Wireless LAN-Controllern](#)
- [Konfigurationsbeispiel für AP-Gruppen-VLANs mit WLAN-Controllern](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)