

PEAP unter UWNs mit ACS 5.1 und Windows 2003 Server

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

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

[CA \(democa\)](#)

[Cisco 1121 Secure ACS 5.1](#)

[Installation mit der Appliance der Serie CSACS-1121](#)

[Installation des ACS Servers](#)

[Cisco WLC5508 Controller-Konfiguration](#)

[Erstellen der erforderlichen Konfiguration für WPAv2/WPA](#)

[PEAP-Authentifizierung](#)

[Zertifikatvorlagen-Snap-In installieren](#)

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

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

[Einrichtung des ACS 5.1-Zertifikats](#)

[Exportfähiges Zertifikat für ACS konfigurieren](#)

[Installieren des Zertifikats in der ACS 5.1-Software](#)

[Konfigurieren des ACS-Identitätsspeichers für Active Directory](#)

[Hinzufügen eines Controllers zum ACS als AAA-Client](#)

[Konfigurieren von ACS-Zugriffsrichtlinien für Wireless](#)

[Erstellen einer ACS-Zugriffsrichtlinie und einer Serviceregel](#)

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

[Durchführen einer einfachen Installation und Konfiguration](#)

[Installieren der Wireless-Netzwerkkarte](#)

[Konfigurieren der Wireless-Netzwerkverbindung](#)

[Fehlerbehebung bei der Wireless-Authentifizierung mit ACS](#)

[PEAP-Authentifizierung schlägt mit ACS-Server fehl](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie einen sicheren Wireless-Zugriff mithilfe von

Wireless LAN-Controllern, Microsoft Windows 2003 Software und Cisco Secure Access Control Server (ACS) 5.1 über Protected Extensible Authentication Protocol (PEAP) mit Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) Version 2 konfigurieren.

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

Voraussetzungen

Anforderungen

Es wird davon ausgegangen, dass der Techniker über Grundkenntnisse der Windows 2003-Installation und der Cisco Wireless LAN-Controller-Installation verfügt, da in diesem Dokument nur die spezifischen Konfigurationen behandelt werden, die für die Durchführung der Tests erforderlich sind.

Informationen zur Erstinstallation und -konfiguration der Cisco Controller der Serie 5508 finden Sie im [Installationshandbuch für Cisco Wireless Controller der Serie 5500](#). Informationen zur Erstinstallation und -konfiguration der Cisco Controller der Serie 2100 finden Sie in der [Schnellstartanleitung: Cisco Wireless LAN Controller der Serie 2100](#).

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.

Windows Server 2003 mit SP1, Enterprise Edition, wird verwendet, um die automatische Registrierung von Benutzer- und Workstation-Zertifikaten für die PEAP-Authentifizierung zu konfigurieren. Die automatische Zertifikatregistrierung und die automatische Erneuerung vereinfachen die Bereitstellung von Zertifikaten und erhöhen die Sicherheit, da Zertifikate automatisch ablaufen und erneuert werden.

Verwendete Komponenten

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

- Cisco Controller der Serien 2106 oder 5508 mit 7.0.98.0
- Cisco 1142 LWAPP AP (Lightweight Access Point Protocol)
- Windows 2003 Enterprise mit installiertem Internet Information Server (IIS), Certificate Authority (CA), DHCP und Domain Name System (DNS)
- Cisco Secure Access Control System Appliance (ACS) 5.1
- Windows XP Professional mit SP (und aktualisierten Service Packs) und Wireless-Netzwerkkarte (NIC) (mit CCX v3-Unterstützung) oder Drittanbieter-Komponente.
- Cisco Switch der Serie 3750

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).

Konfigurieren

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

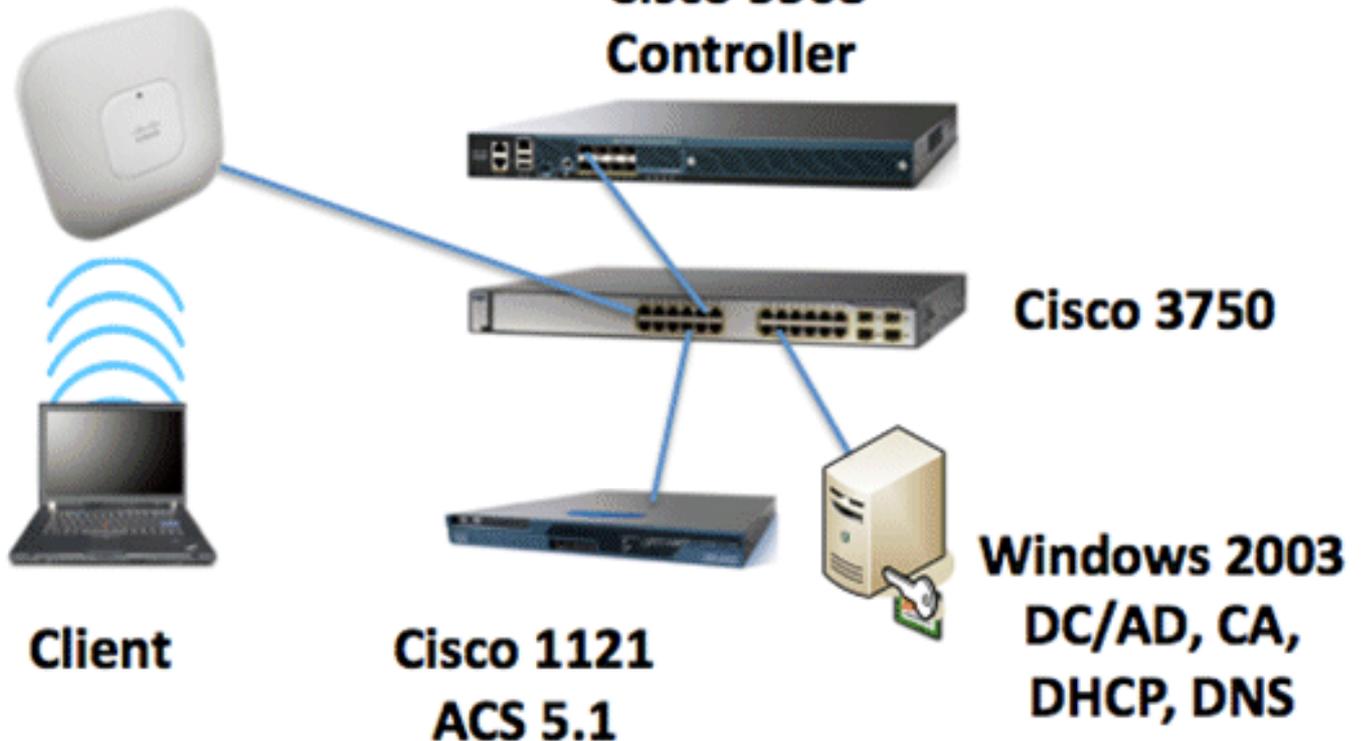
Hinweis: Verwenden Sie das [Tool für die Suche nach Befehlen \(nur registrierte Kunden\)](#), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:

Topologie des Cisco Secure Wireless Labs

Access Point



Dieses Dokument beschreibt in erster Linie die schrittweise Implementierung des PEAP unter Unified Wireless Networks mit ACS 5.1 und Windows 2003 Enterprise Server. Der Schwerpunkt liegt auf der automatischen Registrierung des Clients, sodass der Client sich automatisch registriert und das Zertifikat vom Server erhält.

Hinweis: Um Wi-Fi Protected Access (WPA)/WPA2 mit Temporal Key Integrity Protocol (TKIP)/Advanced Encryption Standard (AES) zu Windows XP Professional mit SP hinzuzufügen,

siehe [WPA2/Wireless Provisioning Services Information Element \(WPS IE\) update for Windows XP with Service Pack 2](#) .

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

[CA \(democa\)](#)

CA ist ein Computer, auf dem Windows Server 2003 mit SP2 Enterprise Edition ausgeführt wird und der folgende Rollen ausführt:

- Ein Domänencontroller für die **demo.local**-Domäne, auf der IIS ausgeführt wird
- Ein DNS-Server für die **demo.local** DNS-Domäne
- Ein DHCP-Server
- Enterprise-Stammzertifizierungsstelle für die **demo.local**-Domäne

Führen Sie die folgenden Schritte aus, um die Zertifizierungsstelle für diese Dienste zu konfigurieren:

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

[Grundlegende Installation und Konfiguration durchführen](#)

Gehen Sie folgendermaßen vor:

1. Installieren Sie Windows Server 2003 mit SP2, Enterprise Edition als Standalone-Server.
2. Konfigurieren Sie das TCP/IP-Protokoll mit der IP-Adresse *10.0.10.10* und der Subnetzmaske *255.255.255.0*.

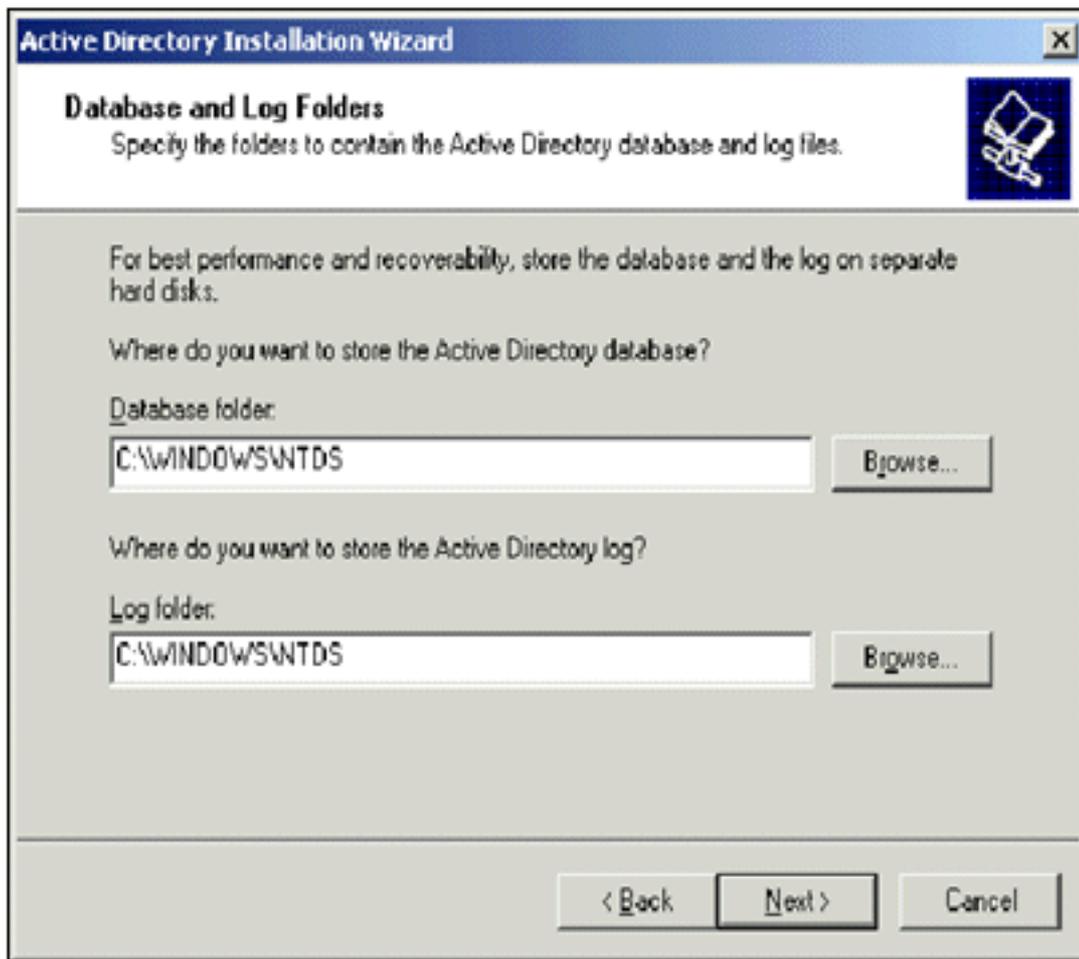
[Konfigurieren des Computers als Domänencontroller](#)

Gehen Sie folgendermaßen vor:

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 des Active Directory-Installationsassistenten auf

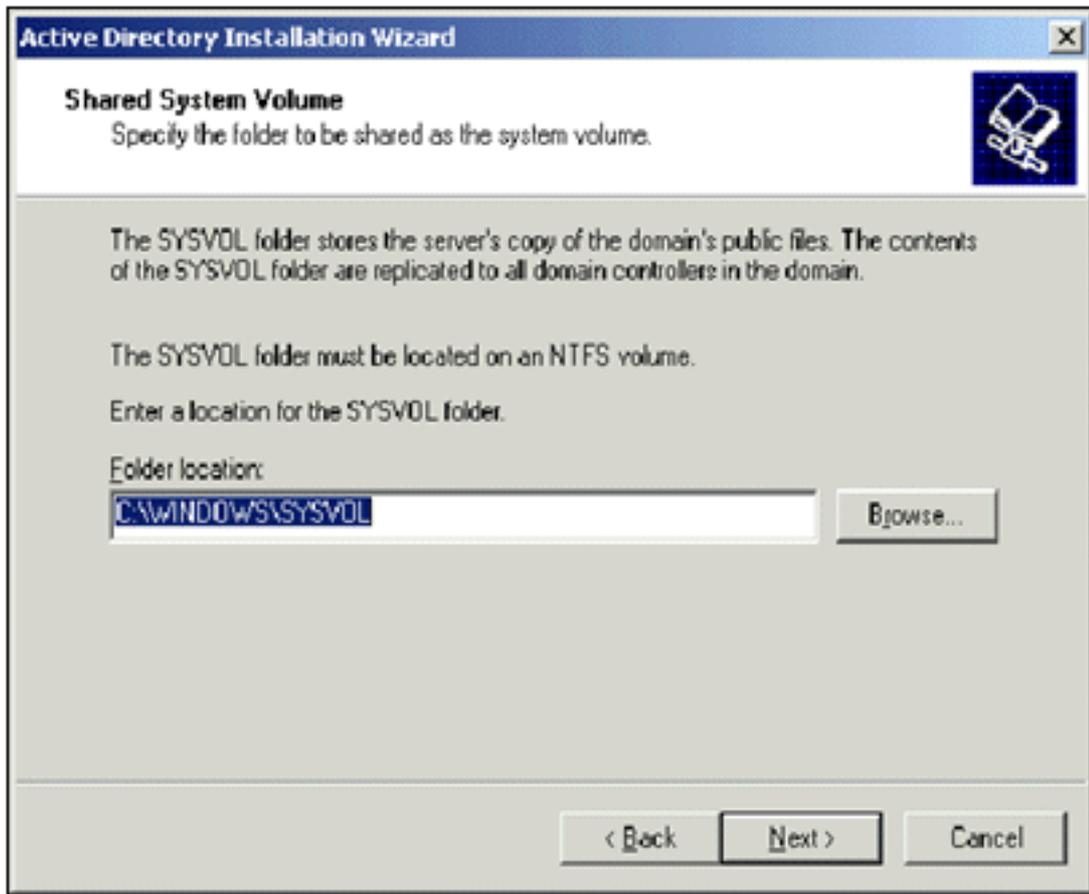
Weiter.

3. Klicken Sie auf der Seite "Betriebssystemkompatibilität" auf **Weiter**.
4. Wählen Sie auf der Seite Domain Controller Type (Domänencontrollertyp) die Option **Domain Controller für eine neue Domäne aus**, und klicken Sie auf **Next (Weiter)**.
5. Wählen Sie auf der Seite Neue Domäne erstellen die Option **Domäne in einer neuen Gesamtstruktur aus**, und klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite "DNS installieren oder konfigurieren" die Option **Nein, nur DNS auf diesem Computer installieren und konfigurieren**, und klicken Sie auf **Weiter**.
7. Geben Sie auf der Seite Neuer Domänenname **demo.local ein**, und klicken Sie auf **Weiter**.
8. Geben Sie auf der Seite NetBIOS Domain Name (NetBIOS-Domänenname) den NetBIOS-Domännennamen als **Demo ein**, und klicken Sie auf **Next (Weiter)**.
9. Akzeptieren Sie auf der Seite "Datenbank- und Protokollordner - Speicherorte" die Standardverzeichnisse für Datenbank- und Protokollordner, und klicken Sie auf



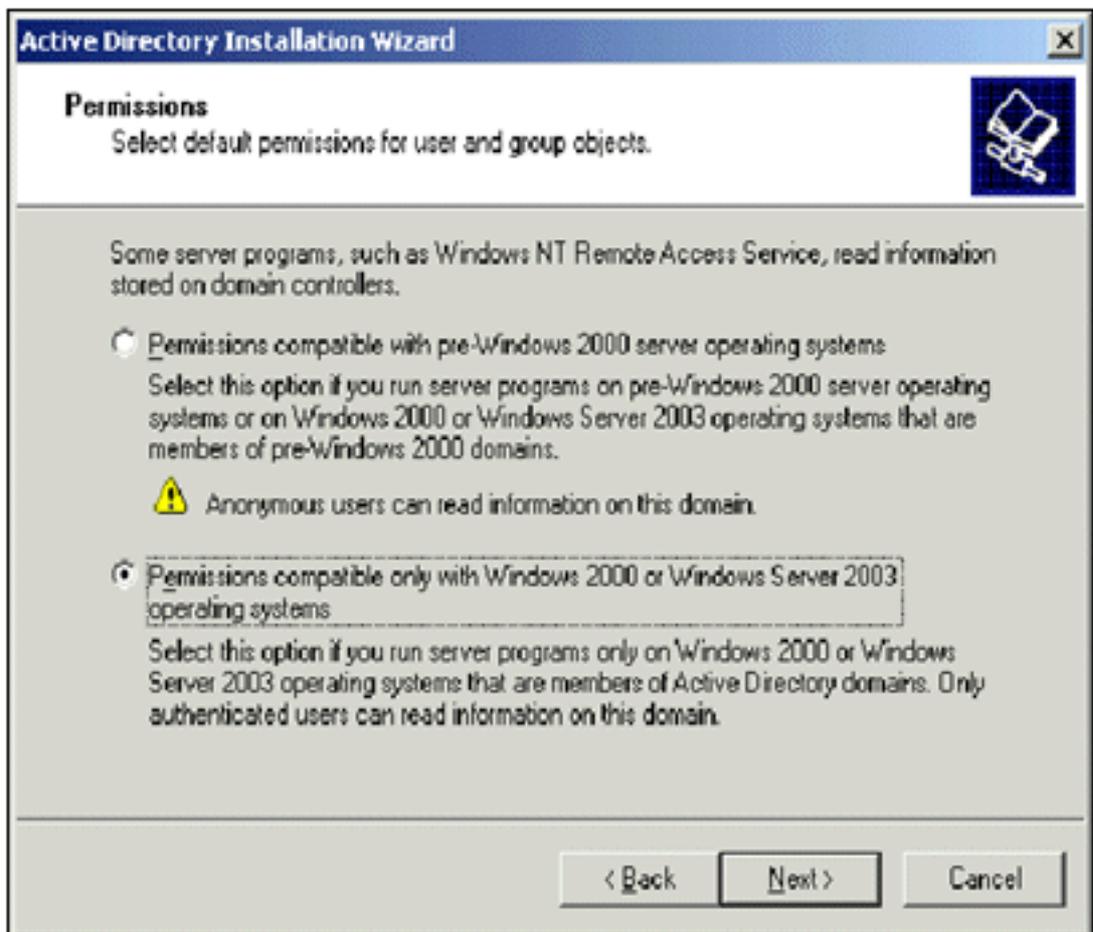
Weiter.

10. Überprüfen Sie auf der Seite Freigegebenes Systemvolume, ob der Standardspeicherort des Ordners korrekt ist, und klicken Sie auf



Weiter.

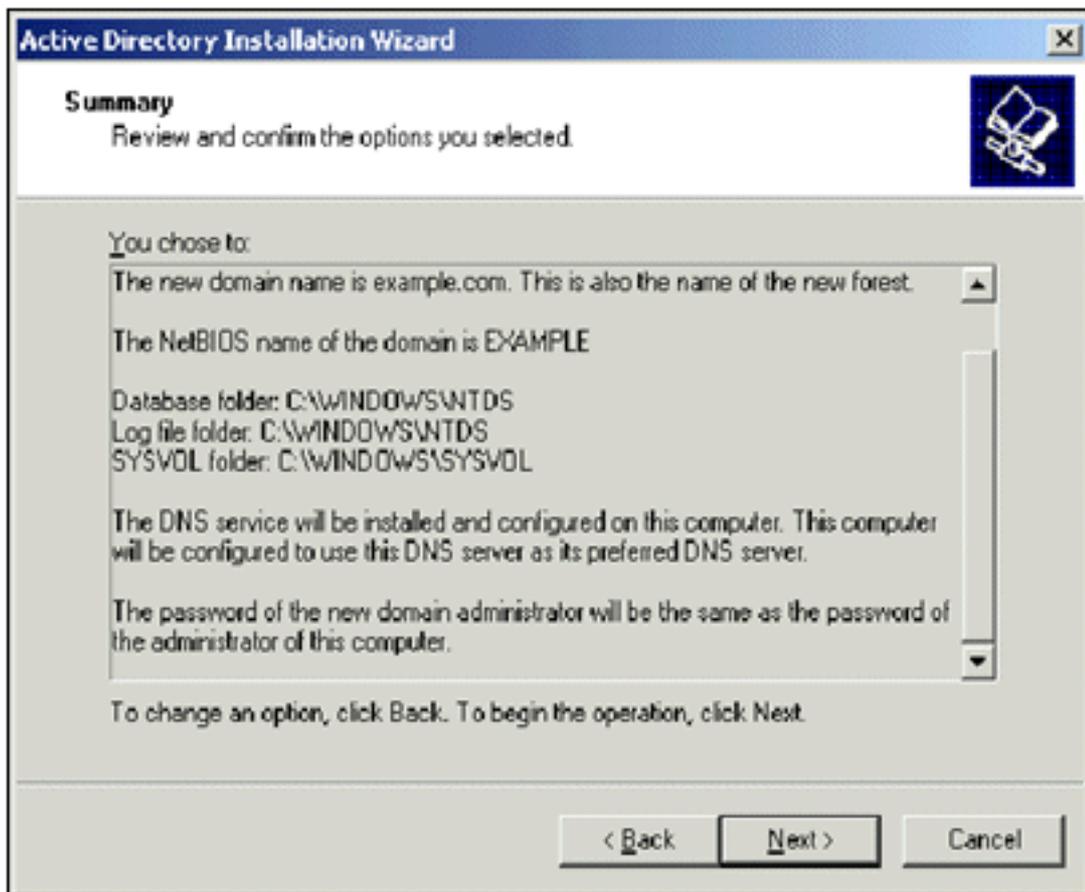
11. Überprüfen Sie auf der Seite Berechtigungen, ob **Nur mit Windows 2000- oder Windows Server 2003-Betriebssystemen kompatible Berechtigungen** ausgewählt ist, und klicken Sie



auf Weiter.

12. Lassen Sie auf der Seite "Administratorkennwort für Wiederherstellungsmodus der Verzeichnisdienste" die Kennwortfelder leer, und klicken Sie auf "**Weiter**".

13. Überprüfen Sie die Informationen auf der Seite "Übersicht", und klicken Sie auf



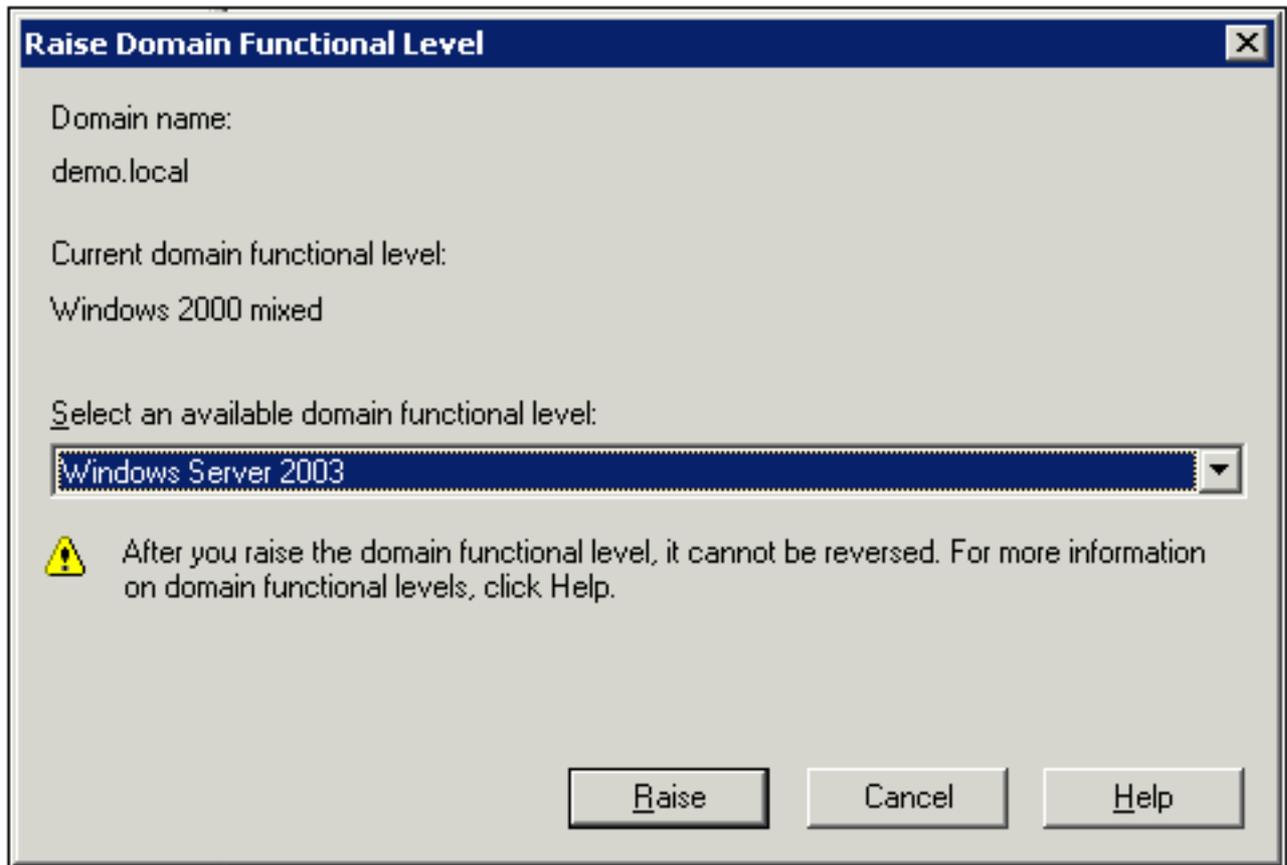
Weiter.

14. Wenn Sie die Installation von Active Directory abgeschlossen haben, klicken Sie auf **Fertig stellen**.
15. Wenn Sie aufgefordert werden, den Computer neu zu starten, klicken Sie auf **Jetzt neu starten**.

[Erhöhen der Domänenfunktionsebene](#)

Gehen Sie folgendermaßen vor:

1. Öffnen Sie das Snap-In Active Directory-Domänen und -Vertrauensstellungen im Ordner Verwaltung (Start > Programme > Verwaltung > **Active Directory-Domänen und -Vertrauensstellungen**), und klicken Sie dann mit der rechten Maustaste auf den Domänencomputer **CA.demo.local**.
2. Klicken Sie auf **Domänenfunktionsebene heraufstufen**, und wählen Sie dann auf der Seite Domänenfunktionsebene die Option **Windows Server 2003 aus**.



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

[Installieren und Konfigurieren von DHCP](#)

Gehen Sie folgendermaßen vor:

1. Installieren Sie **Dynamic Host Configuration Protocol (DHCP)** als **Netzwerkdienst-Komponente**, indem Sie in der Systemsteuerung die Option **Software** verwenden.
2. Öffnen Sie das DHCP-Snap-In im Ordner Verwaltung (Start > Programme > Verwaltung > **DHCP**), und markieren Sie dann den DHCP-Server, **CA.demo.local** (**CA.demo.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 **CA.demo.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 Bereichsname im Feld Name **CorpNet** 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 geben Sie die folgenden Parameter ein: Start-IP-Adresse - 10.0.20.1 End-IP-Adresse - 10.0.20.200 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 **Weiter**, und geben Sie *10.0.20.1* als Start-IP-Adresse und *10.0.20.100* als End-IP-Adresse ein, die ausgeschlossen werden soll. Klicken Sie dann auf **Weiter**. Dadurch werden die IP-Adressen im Bereich von 10.0.20.1 bis 10.0.20.100 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 "Leasedauer" 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 (Standard-Gateway) die Standard-Routeradresse *10.0.20.1* hinzu, und klicken Sie auf **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:

10 . 0 . 20 . 1	Add
	Remove
	Up
	Down

< Back Next > Cancel

12. Geben Sie auf der Seite Domain Name and DNS Servers (Domänenname und DNS-Server) *demo.local* in das Feld Parent domain (Übergeordnete Domäne) ein, geben Sie *10.0.10.10* in das Feld IP address (IP-Adresse) ein, und klicken Sie dann auf **Add** (Hinzufügen) und dann auf **Next** (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.

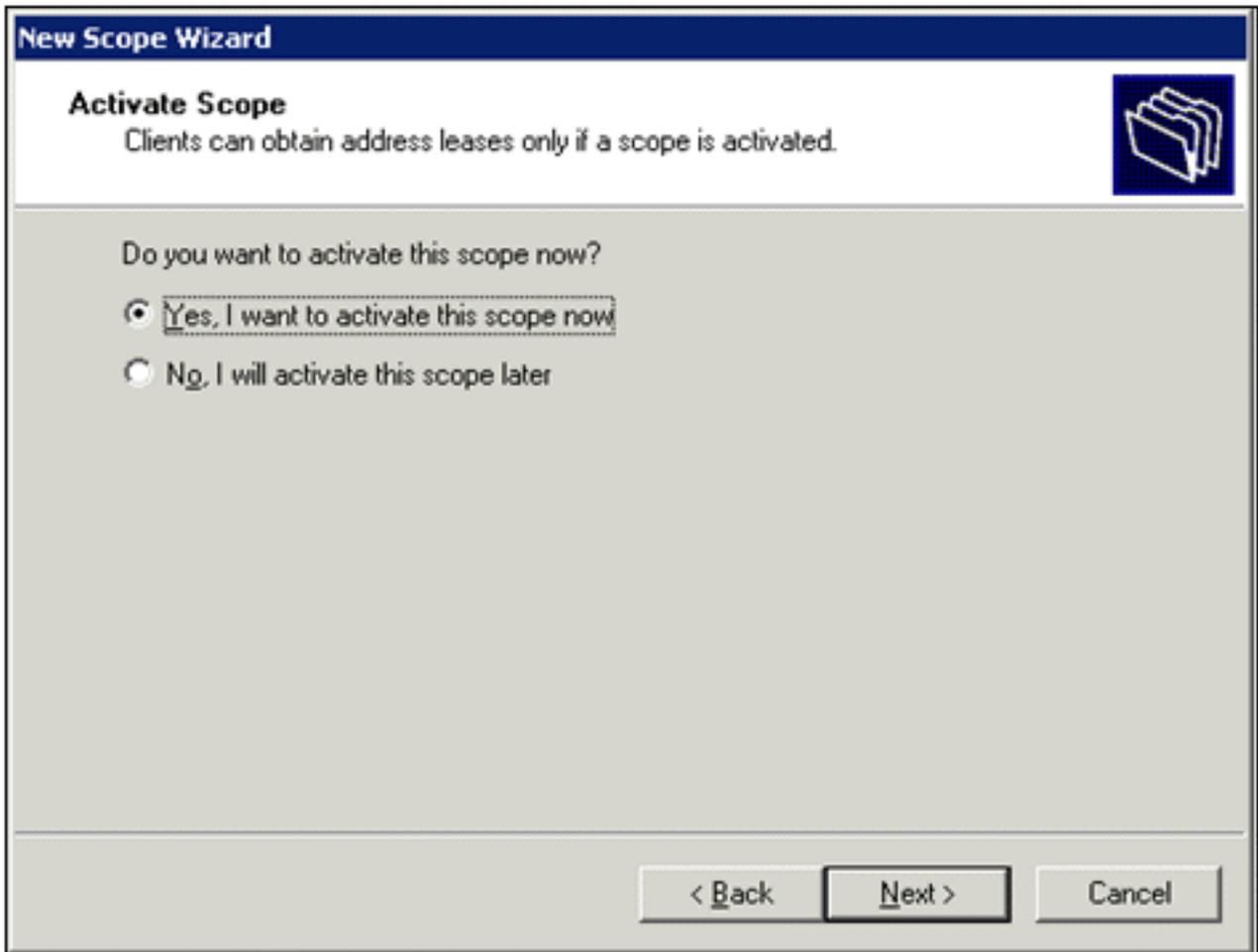
Parent domain:

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

Server name:	IP address:	
<input type="text"/>	<input type="text" value=" . . ."/>	<input type="button" value="Add"/>
<input type="button" value="Resolve"/>	<input type="text" value="10.0.10.10"/>	<input type="button" value="Remove"/>
		<input type="button" value="Up"/>
		<input type="button" value="Down"/>

13. Klicken Sie auf der Seite "WINS-Server" auf **Weiter**.

14. Wählen Sie auf der Seite "Bereich aktivieren" die Option **Ja, ich möchte diesen Bereich jetzt aktivieren**, und klicken Sie auf **Weiter**.



15. Wenn Sie den Assistenten für neue Bereiche beendet haben, klicken Sie auf **Fertig stellen**.

[Zertifikatsdienste installieren](#)

Gehen Sie folgendermaßen vor:

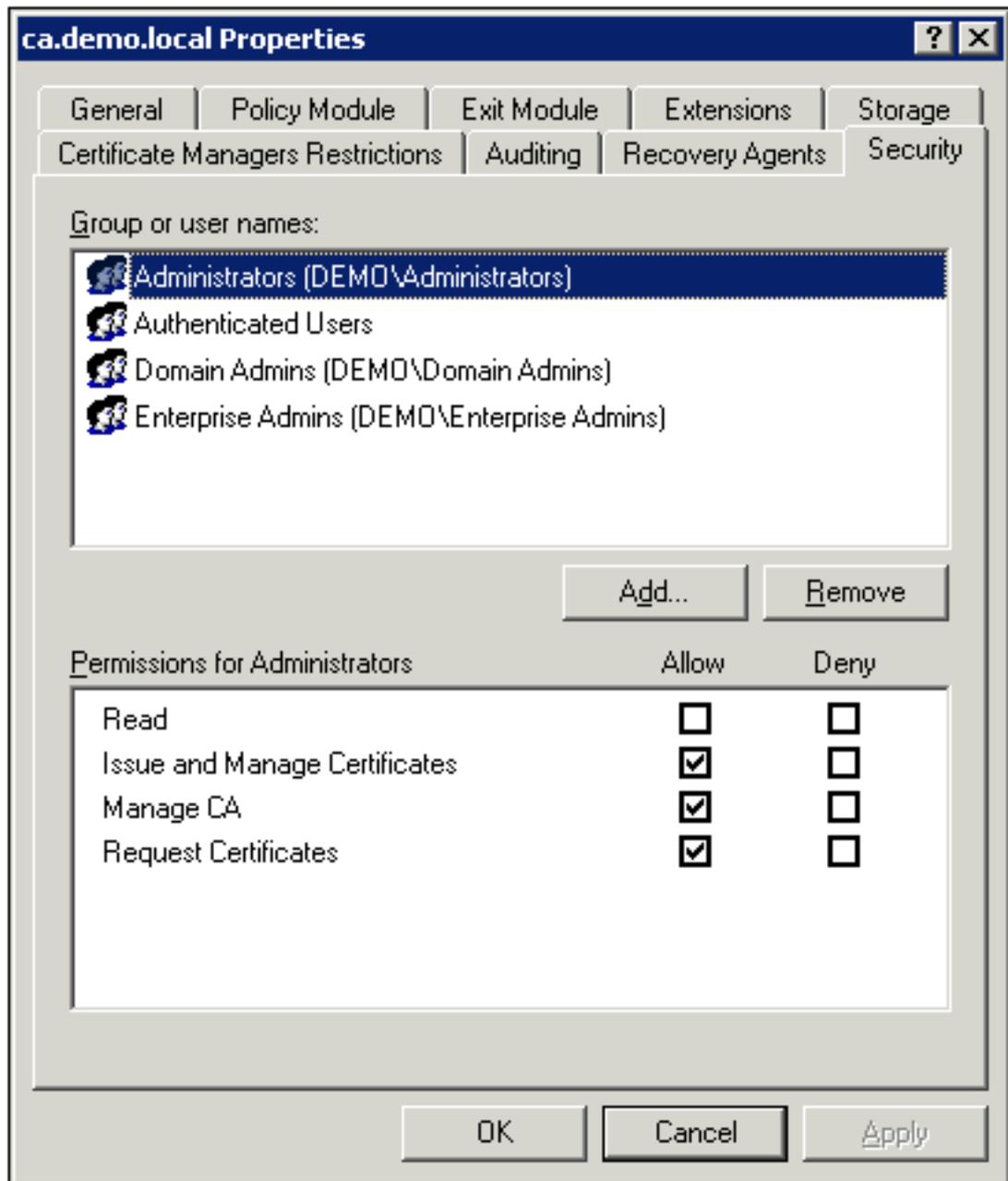
Hinweis: IIS muss vor der Installation der Zertifikatsdienste installiert werden, und der Benutzer muss Teil der Enterprise Admin-OU sein.

1. Öffnen Sie in der Systemsteuerung **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 Option Enterprise root CA aus, und klicken Sie auf Next (Weiter).
4. Geben Sie auf der Seite CA Identifying Information (CA-Identifizierungsinformationen) *democa* in das Feld Common Name (Allgemeiner Name für diese CA) ein. Sie können auch die anderen optionalen Details eingeben. Klicken Sie dann auf **Weiter**, und übernehmen Sie die Standardeinstellungen auf der Seite Zertifikatdatenbank-Einstellungen.
5. Klicken Sie auf **Next** (Weiter). Klicken Sie nach Abschluss der Installation auf **Fertig stellen**.
6. Klicken Sie nach dem Lesen der Warnmeldung zur Installation von IIS auf **OK**.

[Administratorberechtigungen für Zertifikate überprüfen](#)

Gehen Sie folgendermaßen vor:

1. Wählen Sie **Start > Verwaltung > Zertifizierungsstelle**.
2. Klicken Sie mit der rechten Maustaste auf die **Demo-CA**, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf der Registerkarte Sicherheit in der Liste Gruppen- oder Benutzernamen auf **Administratoren**.
4. Überprüfen Sie in der Liste Berechtigungen für Administratoren, ob die folgenden Optionen auf **Zulassen** eingestellt sind:
 - Zertifikate ausstellen und verwalten
 - CA verwalten
 - Zertifikate anfordern
 Wenn eine dieser Optionen auf Verweigern festgelegt ist oder nicht ausgewählt ist, setzen Sie die Berechtigungen auf



Zulassen.

5. Klicken Sie auf **OK**, um das Dialogfeld Eigenschaften der Demo-CA zu schließen, und schließen Sie dann die Zertifizierungsstelle.

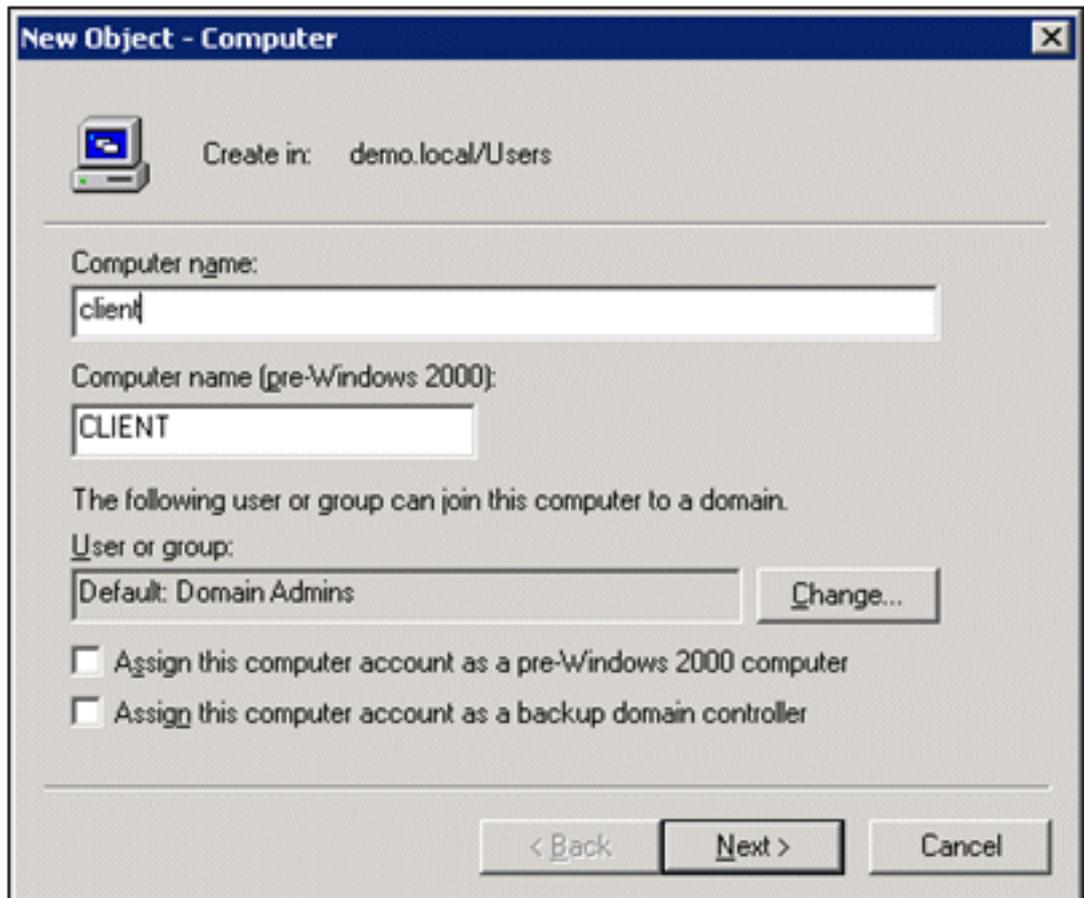
[Hinzufügen von Computern zur Domäne](#)

Gehen Sie folgendermaßen vor:

Hinweis: Wenn der Computer der Domäne bereits 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 **demo.local**.
3. Klicken Sie mit der rechten Maustaste auf **Computer**, 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 Computernamen ein, und klicken Sie auf **Weiter**. In diesem Beispiel wird der Computername *Client*



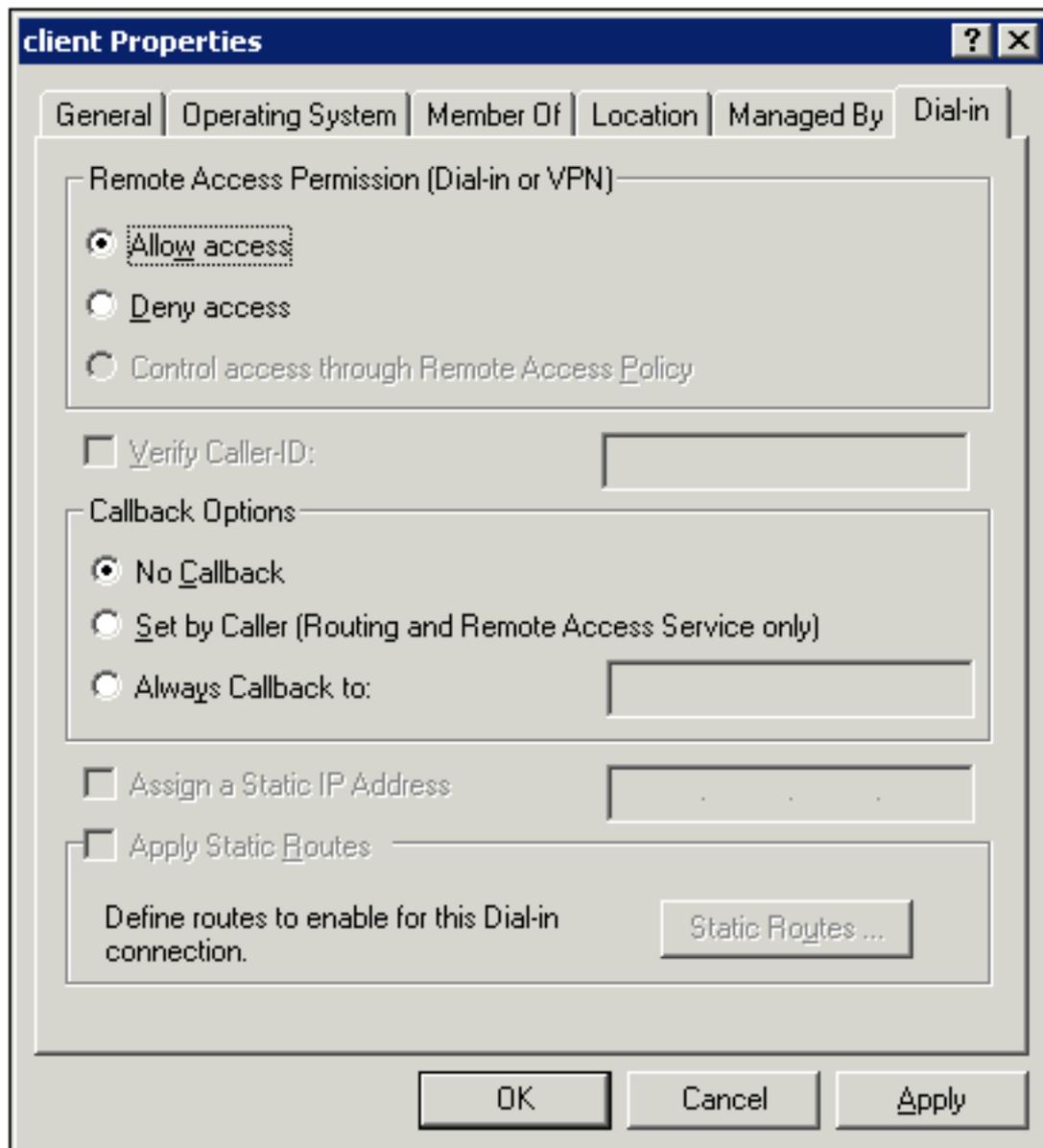
verwendet.

5. Klicken Sie im Dialogfeld Verwaltet auf **Weiter**.
6. Klicken Sie im Dialogfeld Neues Objekt - Computer auf **Fertig stellen**.
7. Wiederholen Sie die Schritte 3 bis 6, um weitere Computerkonten zu erstellen.

[Wireless-Zugriff auf Computer zulassen](#)

Gehen Sie folgendermaßen vor:

1. Klicken Sie in der Konsolenstruktur von Active Directory-Benutzer und -Computer auf den Ordner **Computer**, und klicken Sie mit der rechten Maustaste auf den Computer, dem Sie den Wireless-Zugriff zuweisen möchten. Dieses Beispiel zeigt die Vorgehensweise mit Computer **Client**, die Sie in Schritt 7 hinzugefügt haben. Klicken Sie auf **Eigenschaften**, und gehen Sie dann zur Registerkarte **Einwählen**.
2. Wählen Sie in Remote Access Permission (RAS-Berechtigung) die Option **Allow access (Zugriff zulassen)** aus, und klicken Sie auf



OK.

[Hinzufügen von Benutzern zur Domäne](#)

Gehen Sie folgendermaßen vor:

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** (Weiter).

New Object - User [X]

 Create in: demo.local/Users

First name: Initials:

Last name:

Full name:

User logon name:

User logon name (pre-Windows 2000):

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

Create in: demo.local/Users

Password: [masked]

Confirm password: [masked]

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back Next > Cancel

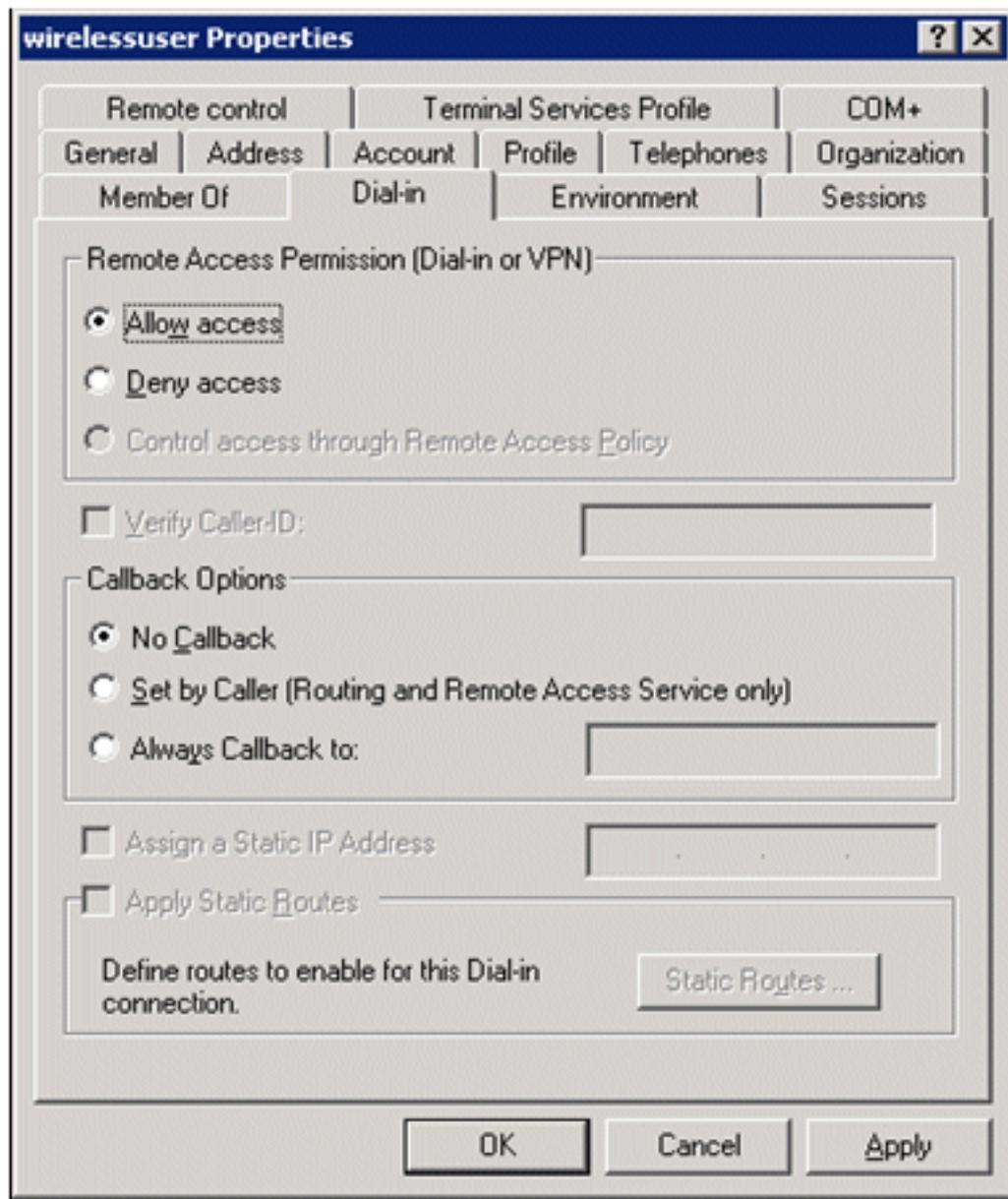
Weiter.

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

[Wireless-Zugriff für Benutzer zulassen](#)

Gehen Sie folgendermaßen vor:

1. Klicken Sie in der Konsolenstruktur von Active Directory-Benutzer und -Computer auf den Ordner **Benutzer**, klicken Sie mit der rechten Maustaste auf **Wireless-Benutzer**, klicken Sie auf **Eigenschaften**, und wechseln Sie dann zur Registerkarte **Einwählen**.
2. Wählen Sie in Remote Access Permission (RAS-Berechtigung) die Option **Allow access (Zugriff zulassen)** aus, und klicken Sie auf



OK.

[Hinzufügen von Gruppen zur Domäne](#)

Gehen Sie folgendermaßen vor:

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 **Gruppe**.
2. Geben Sie im Dialogfeld Neues Objekt - Gruppe den Namen der Gruppe in das Feld Gruppenname ein, und klicken Sie auf **OK**. In diesem Dokument wird der Gruppenname *Wireless-Benutzer*

New Object - Group

Create in: demo.local/Users

Group name:
wirelessusers

Group name (pre-Windows 2000):
wirelessusers

Group scope

- Domain local
- Global
- Universal

Group type

- Security
- Distribution

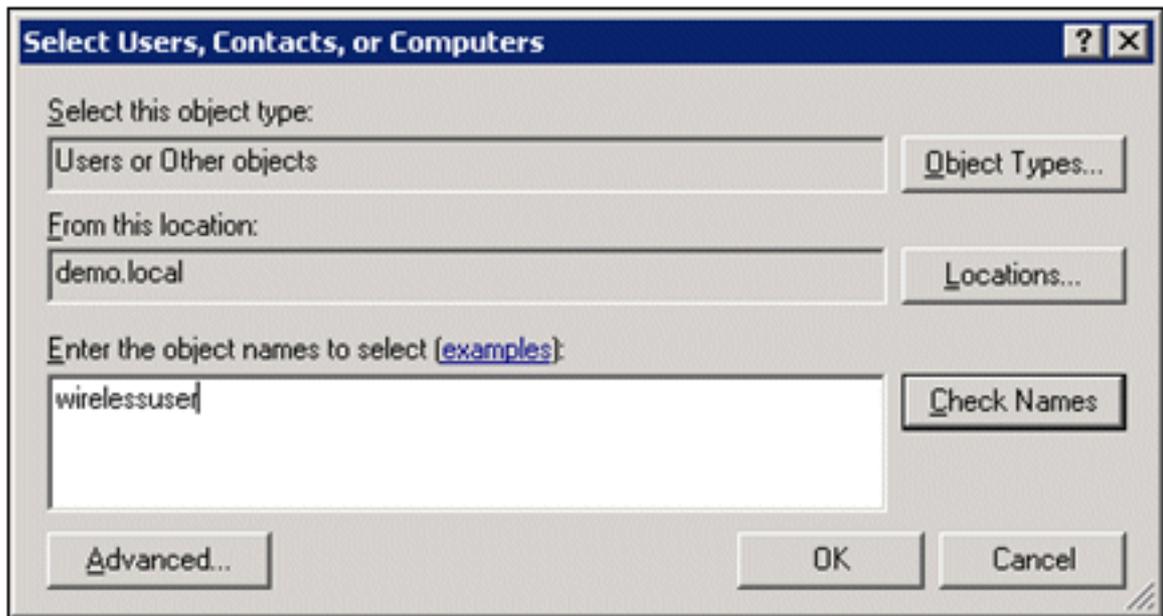
OK Cancel

verwendet.

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

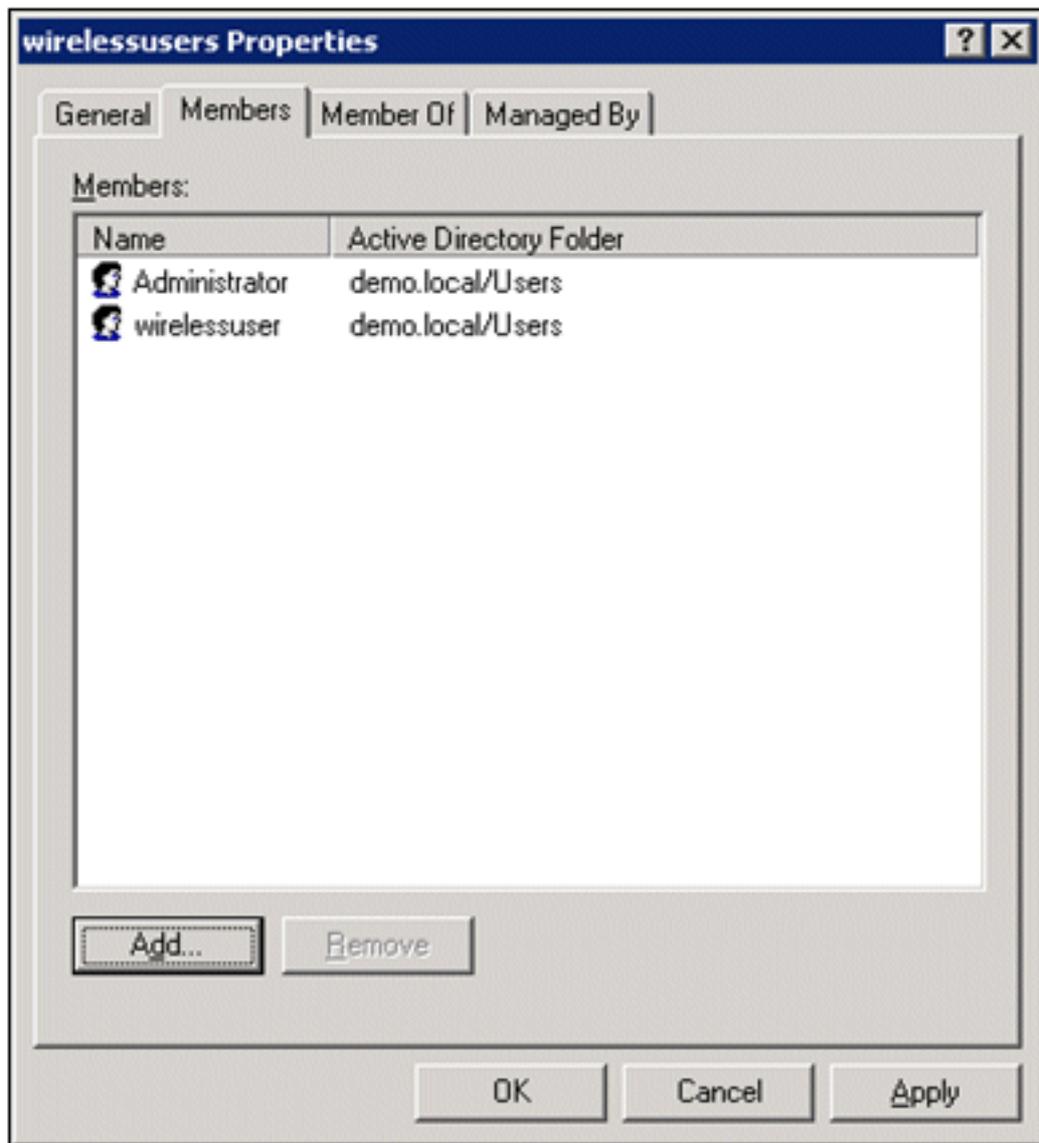
Gehen Sie folgendermaßen vor:

1. Doppelklicken Sie im Detailbereich von Active Directory-Benutzer und -Computer auf die Gruppe *WirelessUsers*.
2. Wechseln Sie zur 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* zur Gruppe hinzugefügt wird. Klicken Sie auf



OK.

4. Klicken Sie im Dialogfeld Mehrere gefundene Namen auf OK. Das Wireless-Benutzerkonto wird der Wireless-Benutzergruppe



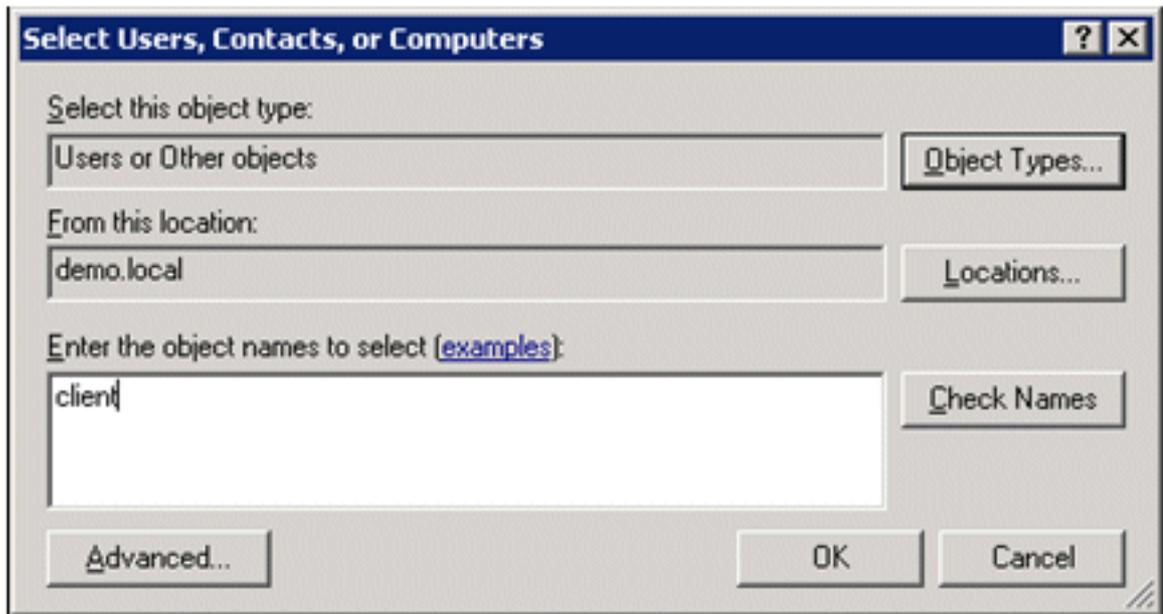
hinzugefügt.

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

Hinzufügen von Clientcomputern zur Gruppe der Wireless-Benutzer

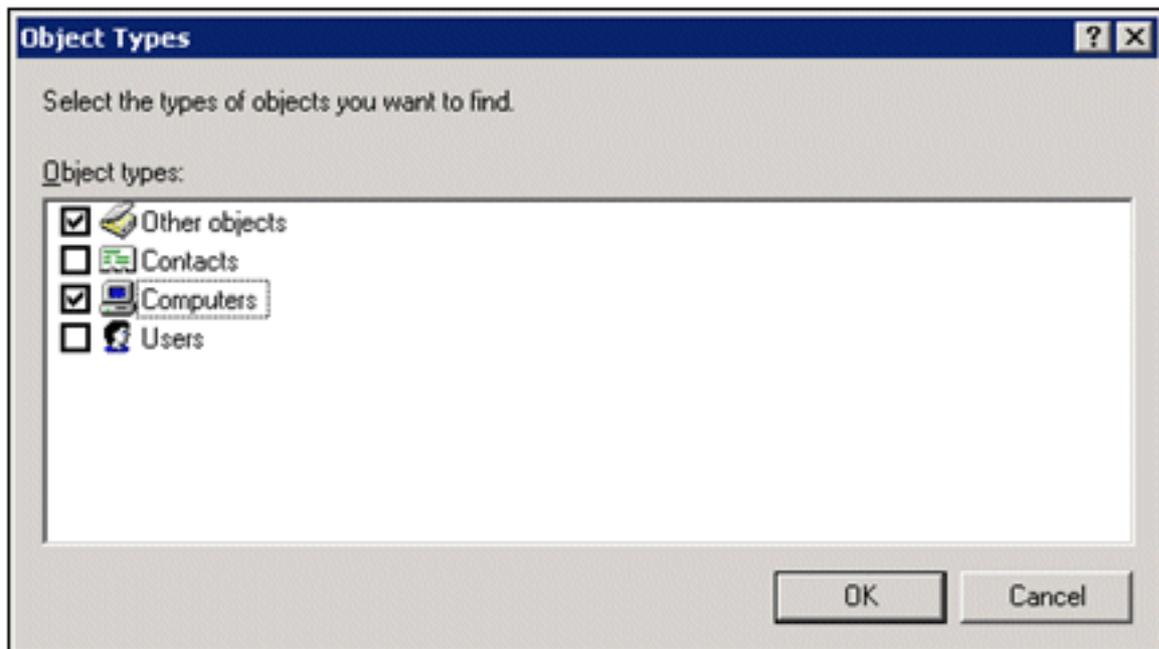
Gehen Sie folgendermaßen vor:

1. Wiederholen Sie die Schritte 1 und 2 im Abschnitt [Benutzer zur Gruppe der Wireless-Benutzer hinzufügen](#) dieses Dokuments.
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 mit dem Namen *client* zur Gruppe hinzugefügt

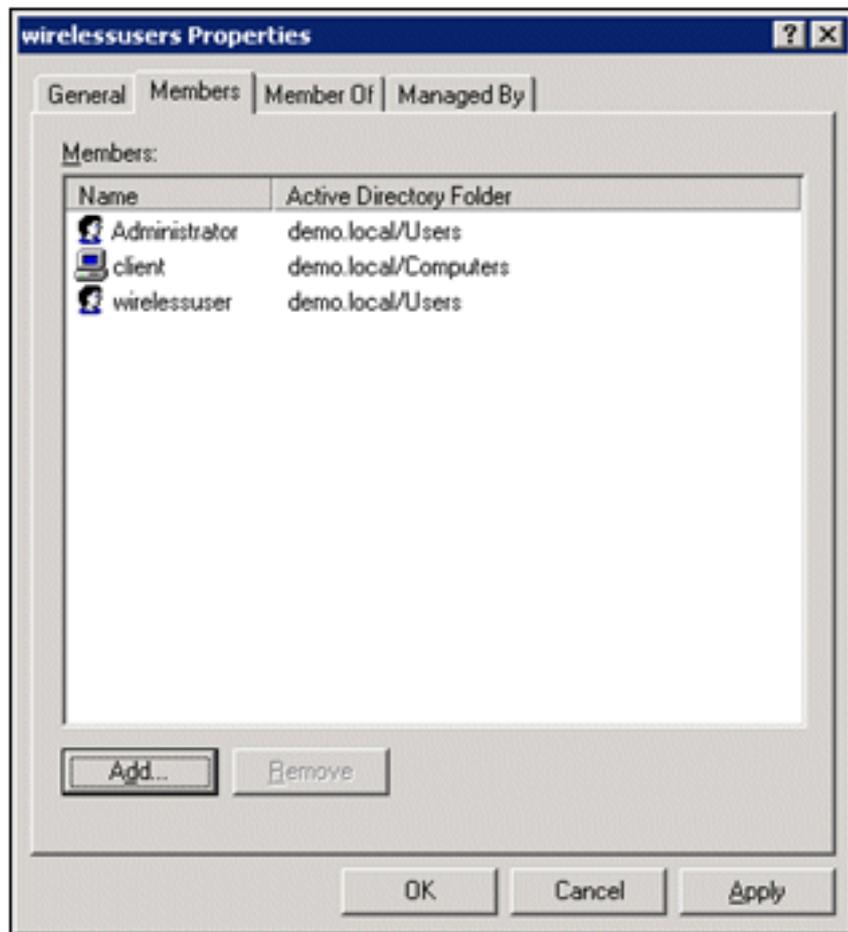


wird.

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



4. Klicken Sie zweimal auf **OK**. Das CLIENT-Computerkonto wird der Gruppe der Wireless-



Benutzer hinzugefügt.

5. Wiederholen Sie den Vorgang, um der Gruppe weitere Computer hinzuzufügen.

[Cisco 1121 Secure ACS 5.1](#)

[Installation mit der Appliance der Serie CSACS-1121](#)

Die CSACS-1121-Appliance wird mit der ACS 5.1-Software vorinstalliert. In diesem Abschnitt erhalten Sie eine Übersicht über den Installationsvorgang und die Aufgaben, die Sie vor der Installation von ACS ausführen müssen.

1. Verbinden Sie den CSACS-1121 mit der Netzwerk- und Appliance-Konsole. Siehe [Kapitel 4, "Verbinden von Kabeln"](#).
2. Schalten Sie die CSACS-1121-Einheit ein. Siehe [Kapitel 4, "Einschalten der Appliance der Serie CSACS-1121"](#).
3. Führen Sie den Befehl **setup** an der CLI-Eingabeaufforderung aus, um die Anfangseinstellungen für den ACS-Server zu konfigurieren. Siehe Ausführen des Setup-Programms.

[Installation des ACS Servers](#)

In diesem Abschnitt wird der Installationsvorgang für den ACS-Server auf der Appliance der Serie CSACS-1121 beschrieben.

- [Ausführen des Setup-Programms](#)
- [Überprüfen des Installationsprozesses](#)

- [Aufgaben nach der Installation](#)

Ausführliche Informationen zur Installation des Cisco Secure ACS Servers finden Sie im [Installations- und Upgrade-Handbuch für das Cisco Secure Access Control System 5.1.](#)

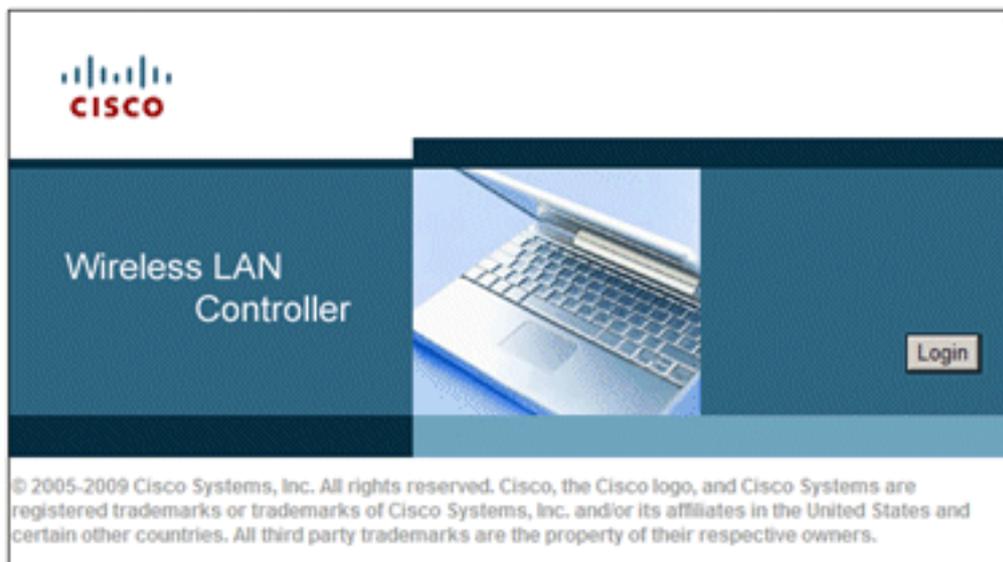
Cisco WLC5508 Controller-Konfiguration

Erstellen der erforderlichen Konfiguration für WPAv2/WPA

Gehen Sie folgendermaßen vor:

Hinweis: Es wird davon ausgegangen, dass der Controller über eine grundlegende Verbindung mit dem Netzwerk verfügt und dass die IP-Verbindung zur Management-Schnittstelle erfolgreich ist.

1. Navigieren Sie zu <https://10.0.1.10>, um sich beim Controller



anzumelden.

2. Klicken Sie auf **Anmelden**.
3. Melden Sie sich mit dem Standardbenutzeradmin und dem Standardkennwort *admin an*.
4. Erstellen Sie im Menü "**Controller**" eine neue Schnittstelle für die VLAN-Zuordnung.
5. Klicken Sie auf **Schnittstellen**.
6. Klicken Sie auf **Neu**.
7. Geben Sie im Feld "Interface name" (Schnittstellename) "*Employee*" ein. (Dieses Feld kann einen beliebigen Wert enthalten.)
8. Geben Sie im Feld VLAN ID (VLAN-ID) *20* ein. (Dieses Feld kann ein beliebiges VLAN sein, das im Netzwerk übertragen wird.)
9. Klicken Sie auf **Apply** (Anwenden).
10. Konfigurieren Sie die Informationen so, wie sie im Fenster Schnittstellen > Bearbeiten angezeigt werden:
Schnittstellen-IP-Adresse - **10.0.20.2**Netzmaske: **255.255.255.0**Gateway
- **10.0.10.1**Primäres DHCP -
10.0.10.10

Save Configuration | Ping | Logout | Refresh

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Controller

Interfaces > Edit < Back Apply

General
Inventory
Interfaces
Multicast
Network Routes
Internal DHCP Server
Mobility Management
Ports
NTP
CDP
Advanced

General Information

Interface Name employee
MAC Address 00:24:97:69:4d:e0

Configuration

Guest Lan
Quarantine
Quarantine Vlan Id

Physical Information

Port Number
Backup Port
Active Port 0
Enable Dynamic AP Management

Interface Address

VLAN Identifier
IP Address
Netmask
Gateway

DHCP Information

Primary DHCP Server
Secondary DHCP Server

Access Control List

ACL Name

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 die Registerkarte **WLANs**.
13. Wählen Sie **Neu erstellen aus**, und klicken Sie auf **Los**.
14. Geben Sie einen Profilnamen und im Feld für die WLAN-SSID den Namen *Employee ein*.

Save Configuration | Ping | Logout | Refresh

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

WLANs

WLANs > New < Back Apply

WLANs
Advanced

Type
Profile Name
SSID
ID

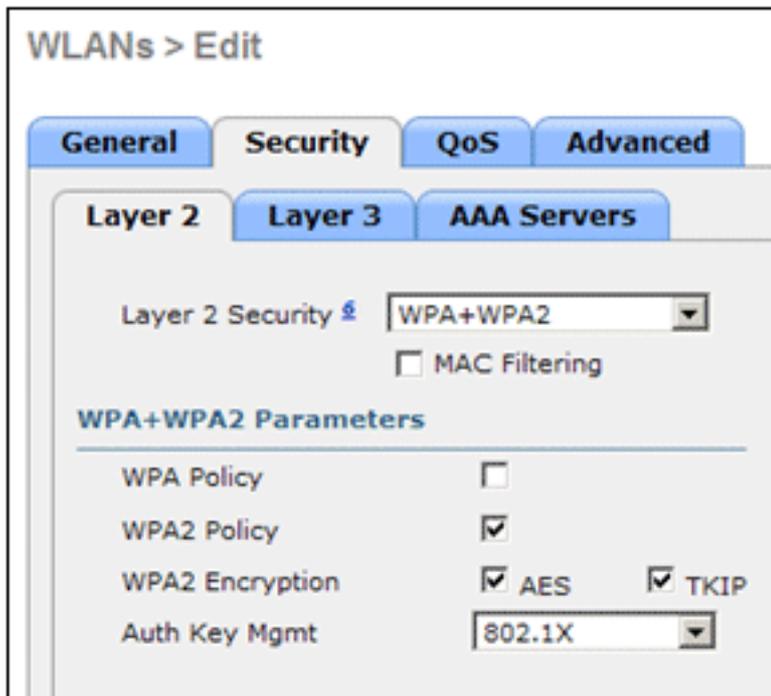
15. Wählen Sie eine ID für das WLAN aus, und klicken Sie auf **Apply**.

16. Konfigurieren Sie die Informationen für dieses WLAN, wenn das Fenster WLANs > Edit angezeigt wird. **Hinweis:** WPAv2 wurde als Layer-2-Verschlüsselungsmethode für diese Übung ausgewählt. Damit WPA mit TKIP-MIC-Clients dieser SSID zugeordnet werden kann, können Sie auch den **WPA-Kompatibilitätsmodus** und die Kästchen **WPA2 TKIP-Clients zulassen** oder die Clients aktivieren, die die 802.11i AES-Verschlüsselungsmethode nicht unterstützen.
17. Klicken Sie im Bildschirm WLANs > Edit (WLANs > Bearbeiten) auf die Registerkarte **General (Allgemein)**.
18. Vergewissern Sie sich, dass das Kontrollkästchen Status auf **Enabled (Aktiviert)** markiert ist und die entsprechende **Schnittstelle (Mitarbeiter)** ausgewählt ist. Aktivieren Sie außerdem das Kontrollkästchen **Aktiviert** für Broadcast-SSID.

The screenshot shows the Cisco configuration interface for a WLAN. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The main content area is titled 'WLANs > Edit' and has tabs for 'General', 'Security', 'QoS', and 'Advanced'. The 'General' tab is active, showing the following configuration:

Profile Name	Employee
Type	WLAN
SSID	Employee
Status	<input type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface	employee
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

19. Klicken Sie auf die Registerkarte **Sicherheit**.
20. Aktivieren Sie im Untermenü "Layer 2" die Option **WPA + WPA2** für die Layer-2-Sicherheit. Aktivieren Sie für die WPA2-Verschlüsselung **AES + TKIP**, um TKIP-Clients zuzulassen.
21. Wählen Sie **802.1x** als Authentifizierungsmethode



aus.

22. Überspringen Sie das Untermenü "Layer 3", da es nicht erforderlich ist. Nach der Konfiguration des RADIUS-Servers kann der entsprechende Server im Menü "Authentication" (Authentifizierung) ausgewählt werden.
23. Die Registerkarten **QoS** und **Erweitert** können standardmäßig beibehalten werden, sofern keine speziellen Konfigurationen erforderlich sind.
24. Klicken Sie auf das Menü **Sicherheit**, um den RADIUS-Server hinzuzufügen.
25. Klicken Sie im Untermenü RADIUS auf **Authentication (Authentifizierung)**. Klicken Sie dann auf **Neu**.
26. Fügen Sie die IP-Adresse des RADIUS-Servers (10.0.10.20) hinzu, die dem zuvor konfigurierten ACS-Server entspricht.
27. Stellen Sie sicher, dass der freigegebene Schlüssel mit dem auf dem ACS-Server konfigurierten AAA-Client übereinstimmt. Vergewissern Sie sich, dass das Kontrollkästchen **Netzwerkbenutzer** aktiviert ist, und klicken Sie auf **Anwenden**.

28. Die Basiskonfiguration ist jetzt abgeschlossen, und Sie können mit dem Testen von PEAP beginnen.

PEAP-Authentifizierung

PEAP mit MS-CHAP Version 2 erfordert Zertifikate auf den ACS-Servern, aber nicht auf den Wireless-Clients. Die automatische Registrierung von Computerzertifikaten für die ACS-Server kann verwendet werden, um die Bereitstellung zu vereinfachen.

Führen Sie die in diesem Abschnitt beschriebenen Verfahren aus, um den CA-Server für die automatische Registrierung von Computer- und Benutzerzertifikaten zu konfigurieren.

Hinweis: Microsoft hat die Webservervorlage mit der Version der Windows 2003 Enterprise-CA geändert, sodass Schlüssel nicht mehr exportierbar sind und die Option abgeblendet ist. Es gibt keine anderen Zertifikatvorlagen mit Zertifikatdiensten, die für die Serverauthentifizierung vorgesehen sind und die Möglichkeit bieten, Schlüssel als exportierbar zu markieren, die im Dropdown-Menü verfügbar sind. Sie müssen daher eine neue Vorlage erstellen, die dies tut.

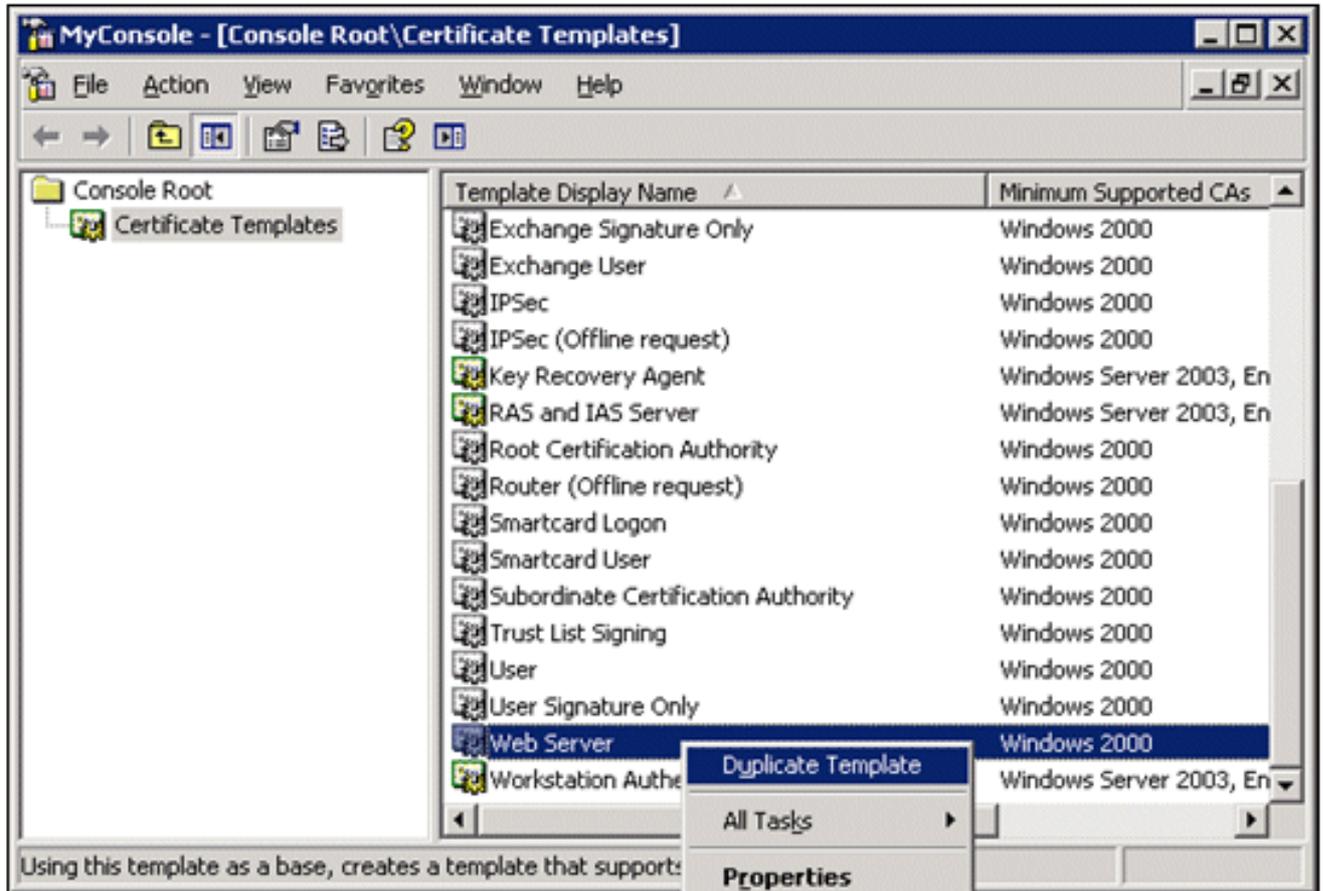
Hinweis: Windows 2000 ermöglicht den Export von Schlüsseln, und diese Verfahren müssen nicht befolgt werden, wenn Sie Windows 2000 verwenden.

Zertifikatvorlagen-Snap-In installieren

Gehen Sie folgendermaßen vor:

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 dann auf **Hinzufügen**.

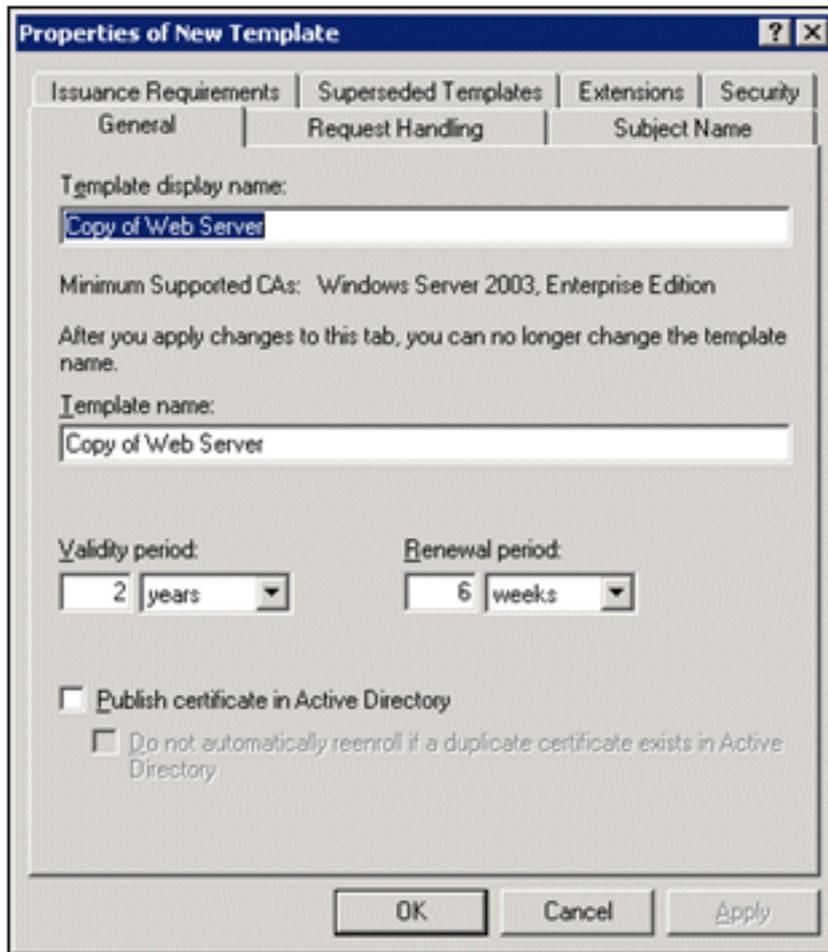
3. Doppelklicken Sie unter Snap-In auf **Zertifikatvorlagen**, klicken Sie auf **Schließen**, und klicken Sie dann auf **OK**.
4. Klicken Sie in der Konsolenstruktur auf **Zertifikatvorlagen**. Alle Zertifikatvorlagen werden im Detailbereich angezeigt.
5. Um die Schritte 2 bis 4 zu umgehen, geben Sie *certtmpl.msc* ein, wodurch das Zertifikatvorlagen-Snap-In geöffnet wird.



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

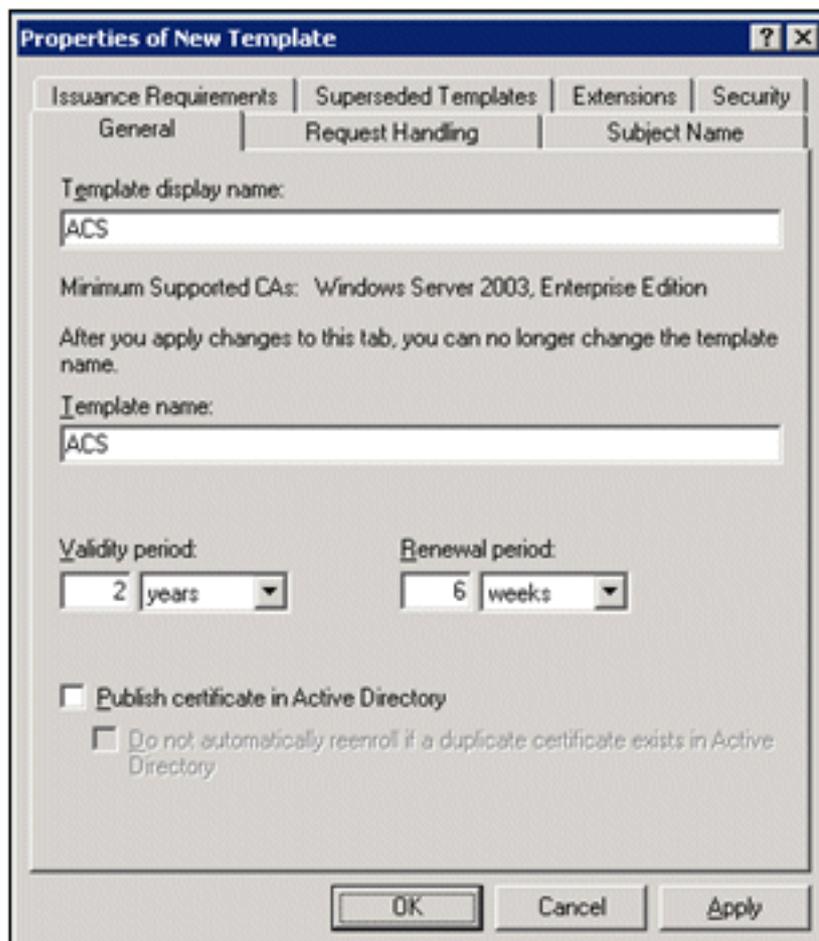
Gehen Sie folgendermaßen vor:

1. Klicken Sie im Bereich Details des Snap-Ins Zertifikatvorlagen auf die Vorlage **Webserver**.
2. Klicken Sie im Menü Aktion auf **Vorlage**



duplizieren.

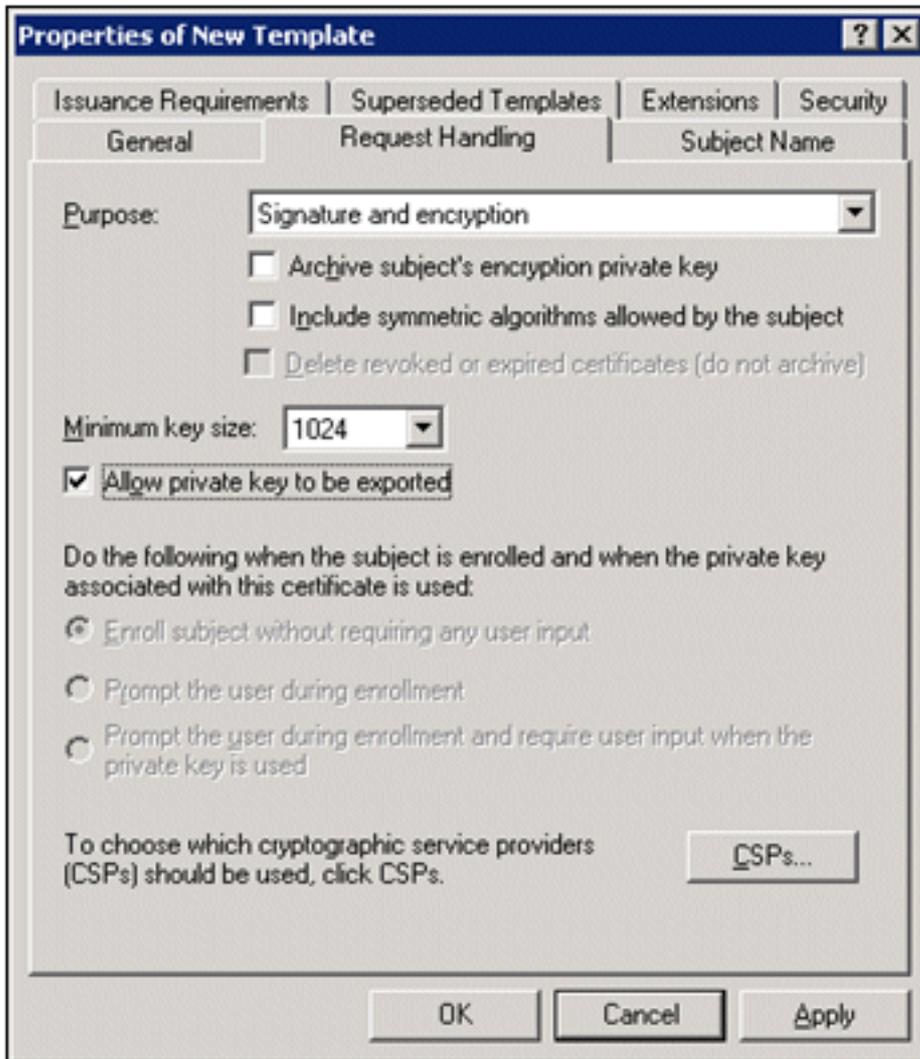
3. Geben Sie im Feld "Template display name" (Anzeigename der Vorlage) ACS



ein.

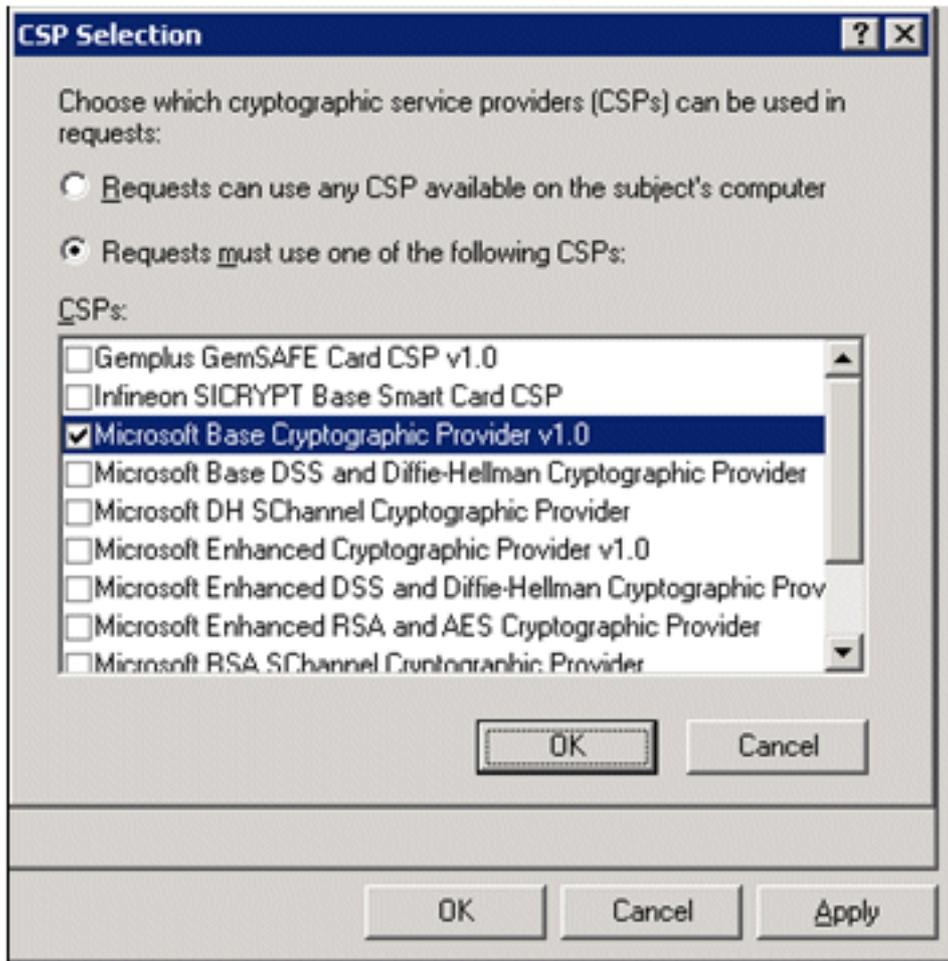
4. Wechseln Sie zur Registerkarte **Request Handling**, und aktivieren Sie **Allow private key to be**

export. Stellen Sie außerdem sicher, dass im Dropdown-Menü Purpose (Zweck) die Option **Signature and Encryption** (Signatur und Verschlüsselung) ausgewählt



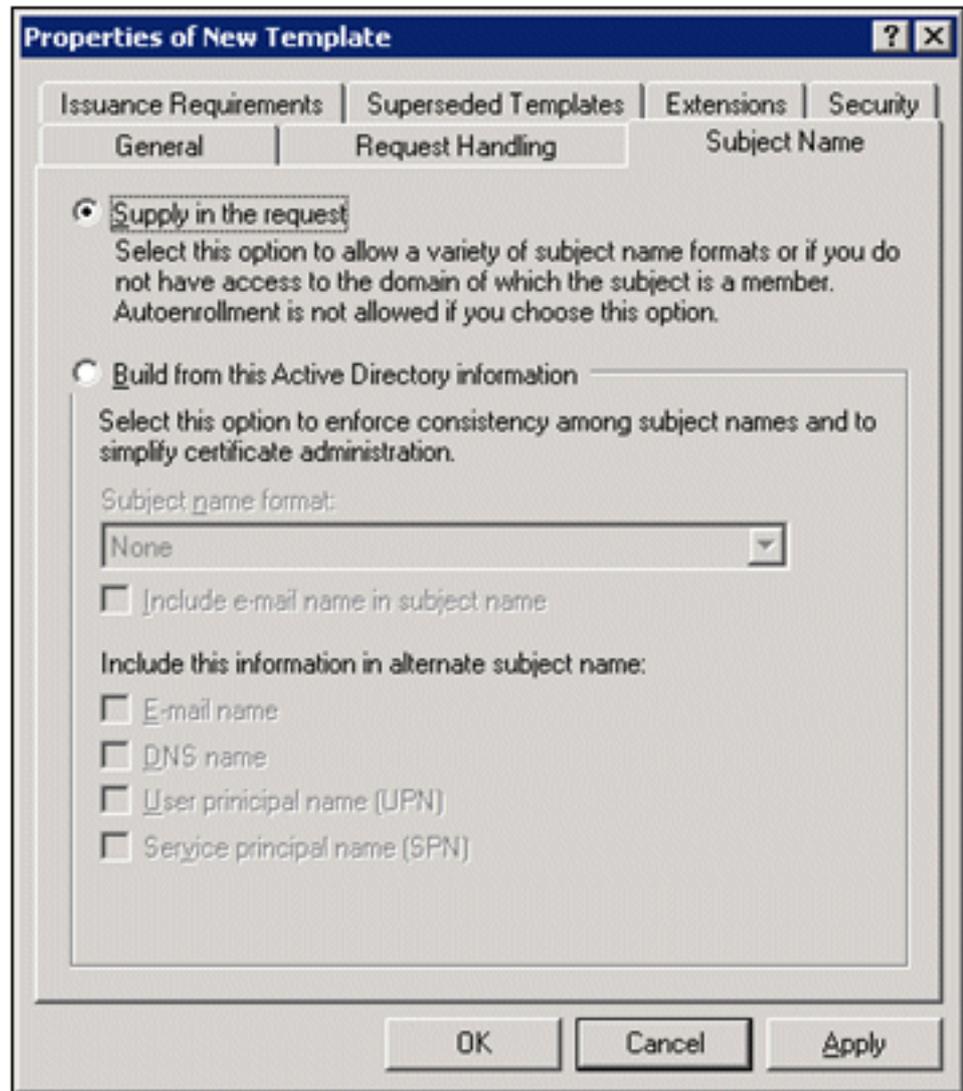
ist.

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



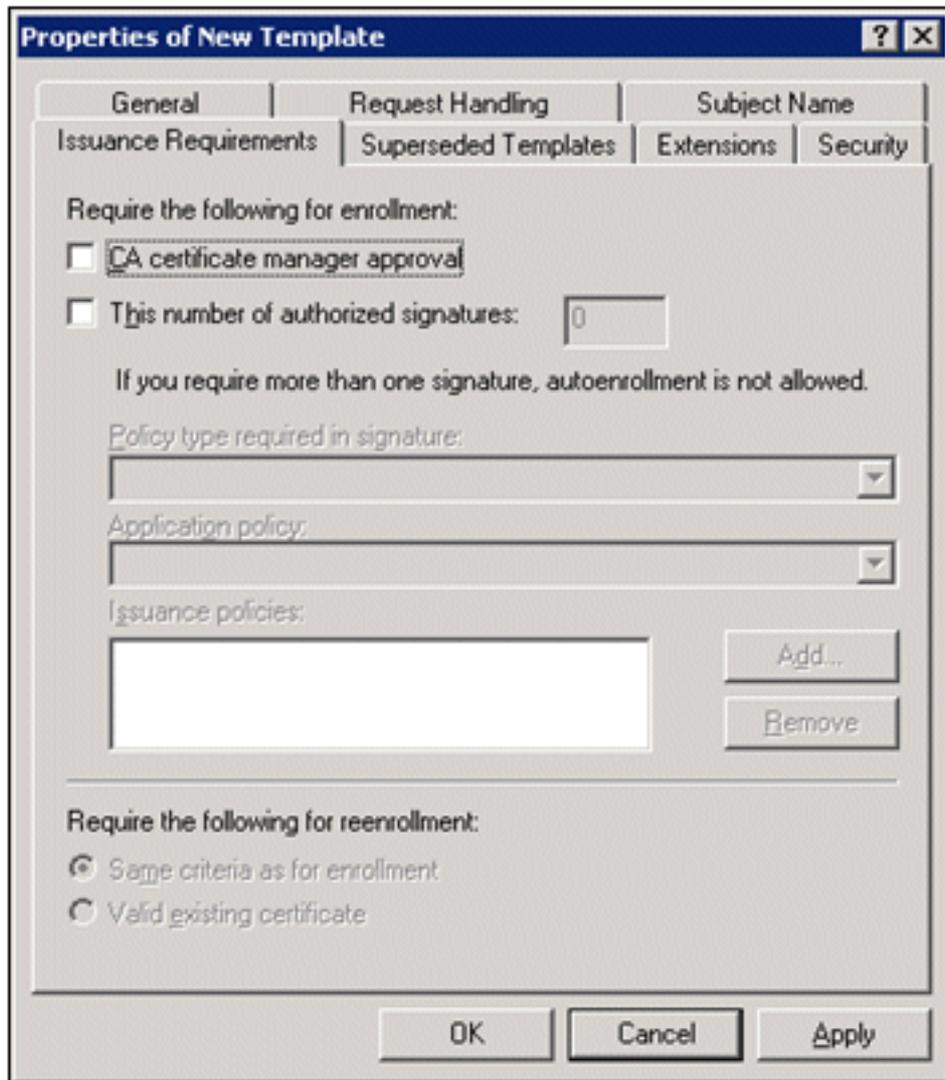
OK.

6. Wechseln Sie zur Registerkarte **Betreffname**, wählen Sie in der Anfrage **Angebot aus**, und



klicken Sie auf **OK**.

7. Markieren Sie auf der Registerkarte **Sicherheit** die **Gruppe Domänenadministratoren**, und stellen Sie sicher, dass die Option **Registrieren** unter Zulässig aktiviert ist. **Hinweis:** Wenn Sie aus diesem Active Directory Informationen erstellen möchten, aktivieren Sie nur den **Benutzerprinzipalnamen (User Principal Name, UPN)** und deaktivieren Sie **E-Mail-Namen** in **Betreffnamen** und **E-Mail-Namen einschließen**, da im Snap-In Active Directory-Benutzer und -Computer kein E-Mail-Name für das Wireless-Benutzerkonto eingegeben wurde. Wenn Sie diese beiden Optionen nicht deaktivieren, versucht die automatische Registrierung, E-Mail zu verwenden. Dies führt zu einem Fehler bei der automatischen Registrierung.
8. Es gibt ggf. zusätzliche Sicherheitsmaßnahmen, um zu verhindern, dass Zertifikate automatisch versendet werden. Diese finden Sie auf der Registerkarte "Emissionsanforderungen". Dies wird in diesem Dokument nicht weiter



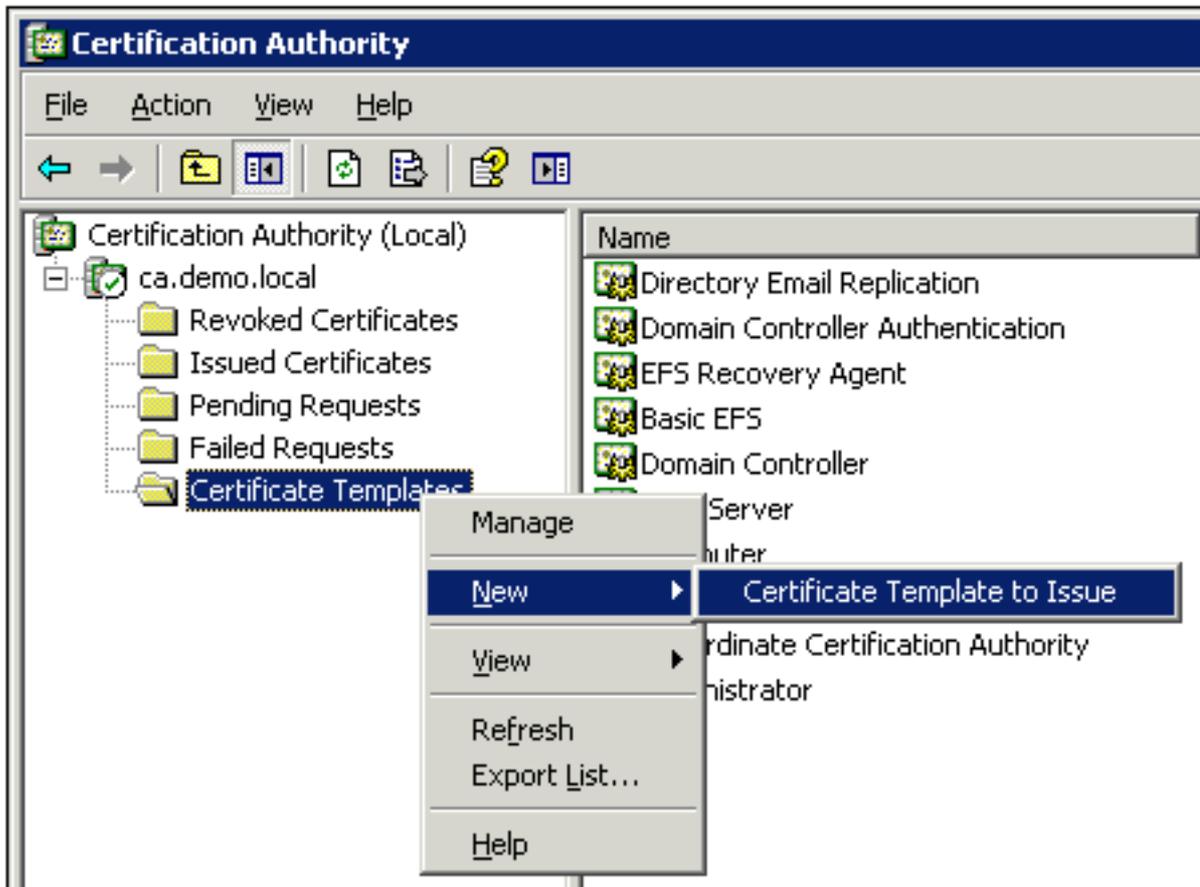
behandelt.

9. Klicken Sie auf **OK**, um die Vorlage zu speichern und mit dem Ausstellen dieser Vorlage aus dem Zertifizierungsstellen-Snap-In fortzufahren.

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

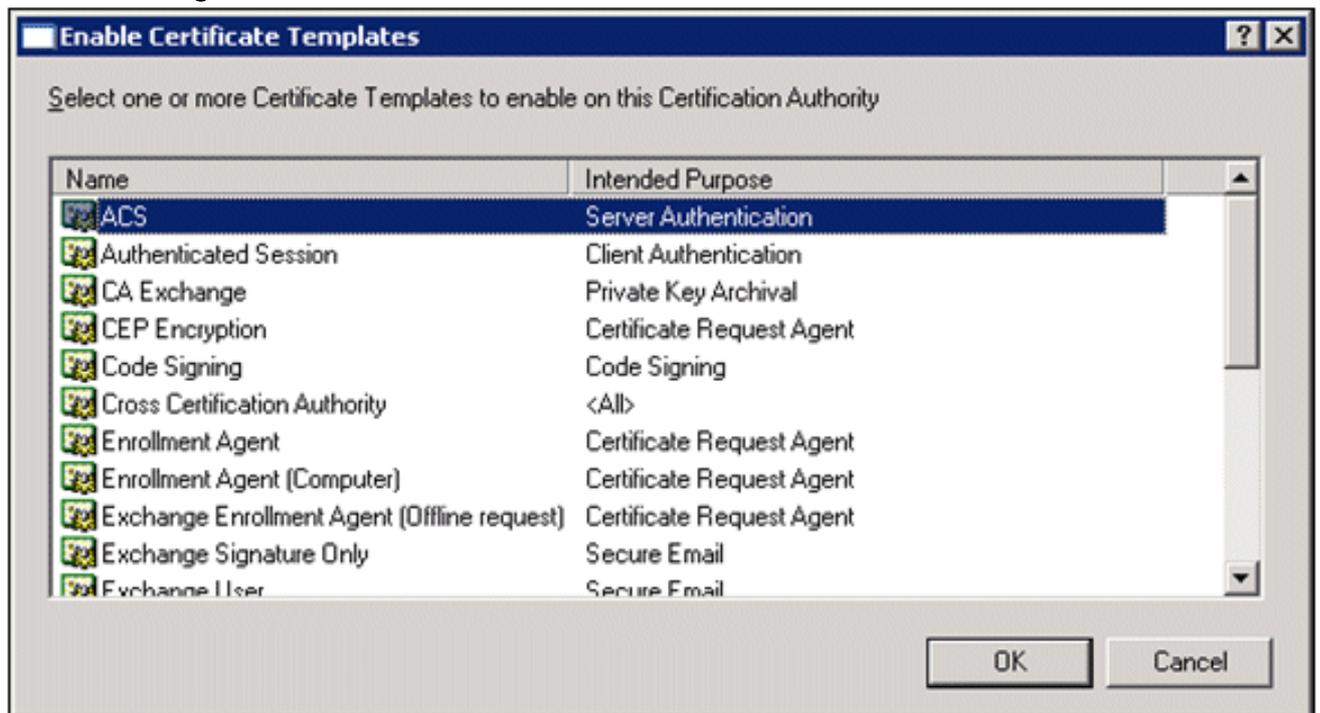
Gehen Sie folgendermaßen vor:

1. Öffnen Sie das Snap-In Zertifizierungsstelle. Führen Sie die Schritte 1 bis 3 im Abschnitt [Create the Certificate Template for the ACS Web Server \(Zertifikatvorlage für ACS-Webserver erstellen\) aus](#), wählen Sie die Option **Certificate Authority (Zertifizierungsstelle) aus**, wählen Sie **Local Computer (Lokaler Computer)**, und klicken Sie auf **Finish (Fertig stellen)**.
2. Erweitern Sie in der Konsolenstruktur der Zertifizierungsstelle die Datei **ca.demo.local**, und klicken Sie dann mit der rechten Maustaste auf **Zertifikatvorlagen**.
3. Gehen Sie zu **Neu > Zertifikatvorlage, die ausgestellt werden**

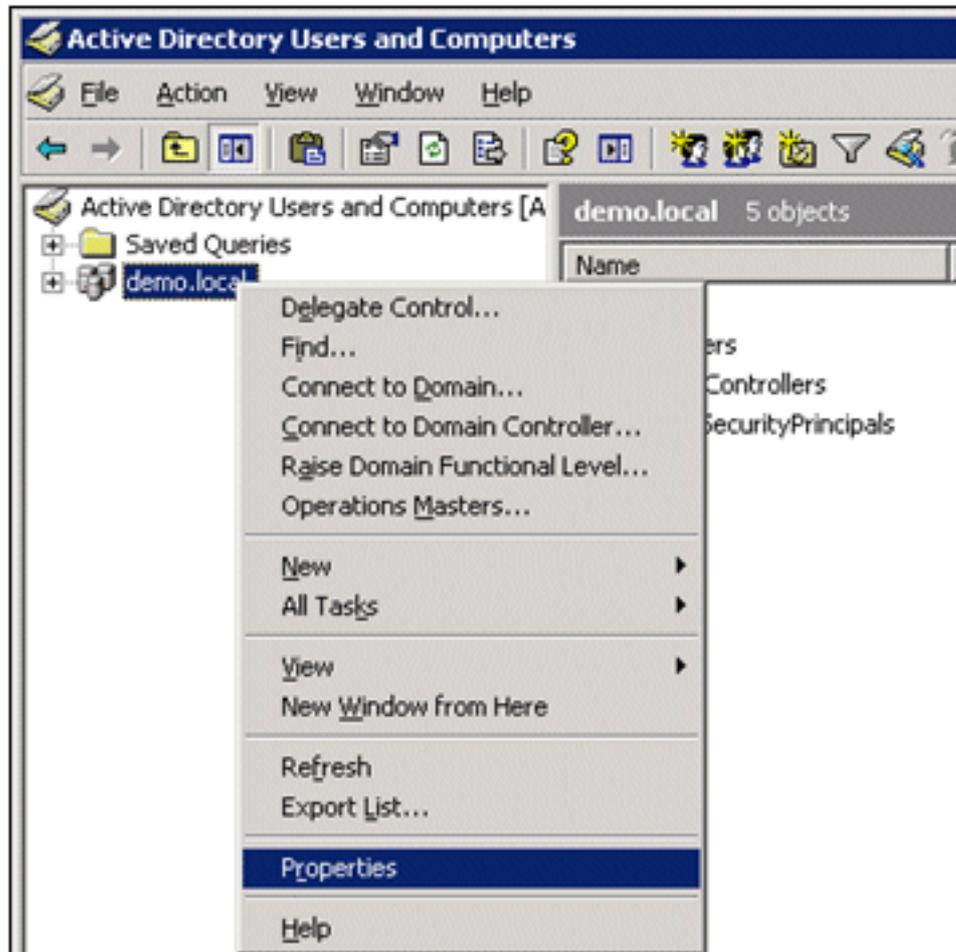


soll.

4. Klicken Sie auf die **ACS-Zertifikatvorlage**.

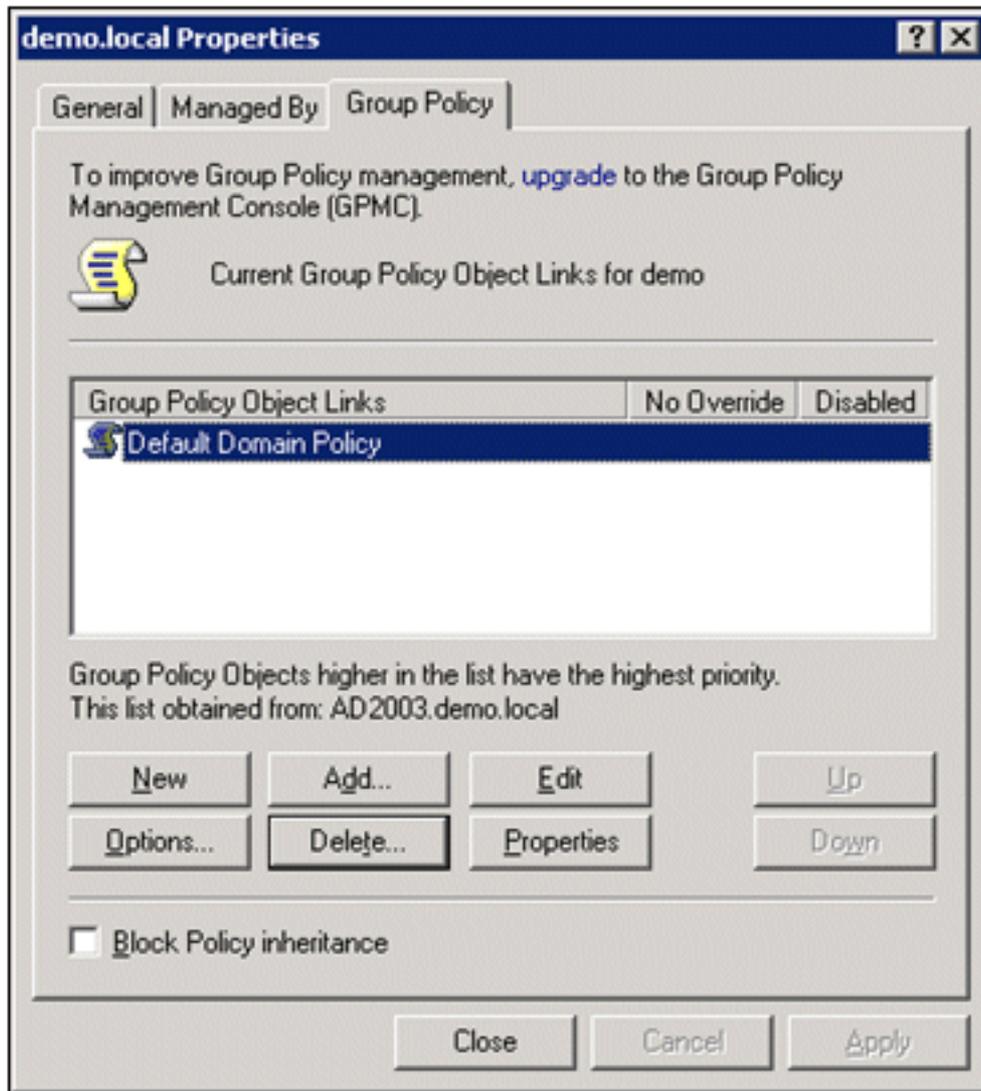


5. Klicken Sie auf **OK**, und öffnen Sie das **Snap-In Active Directory-Benutzer und -Computer**.
6. Doppelklicken Sie in der Konsolenstruktur auf **Active Directory-Benutzer und -Computer**, klicken Sie mit der rechten Maustaste auf **demo.local**, und klicken Sie dann auf



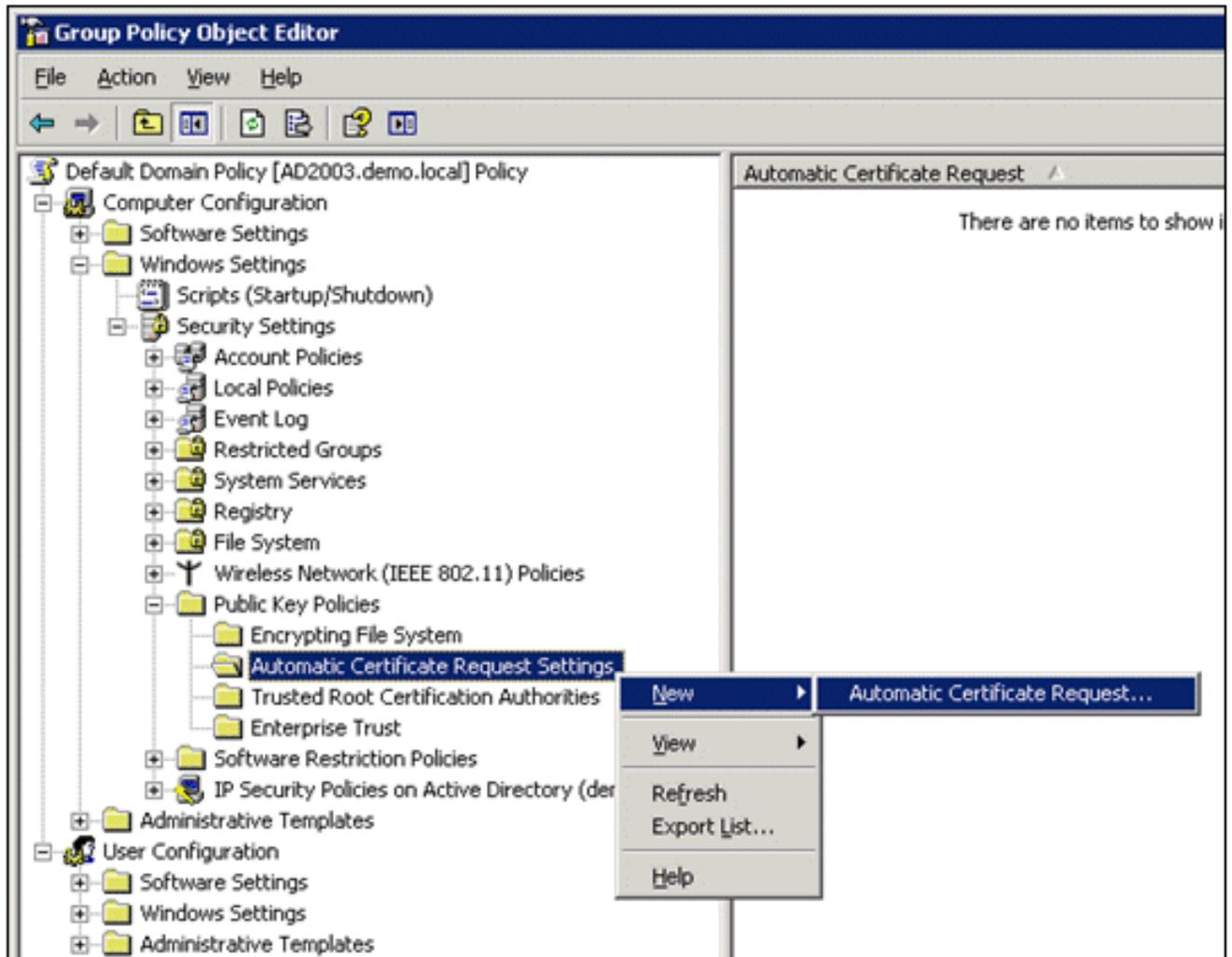
Eigenschaften.

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

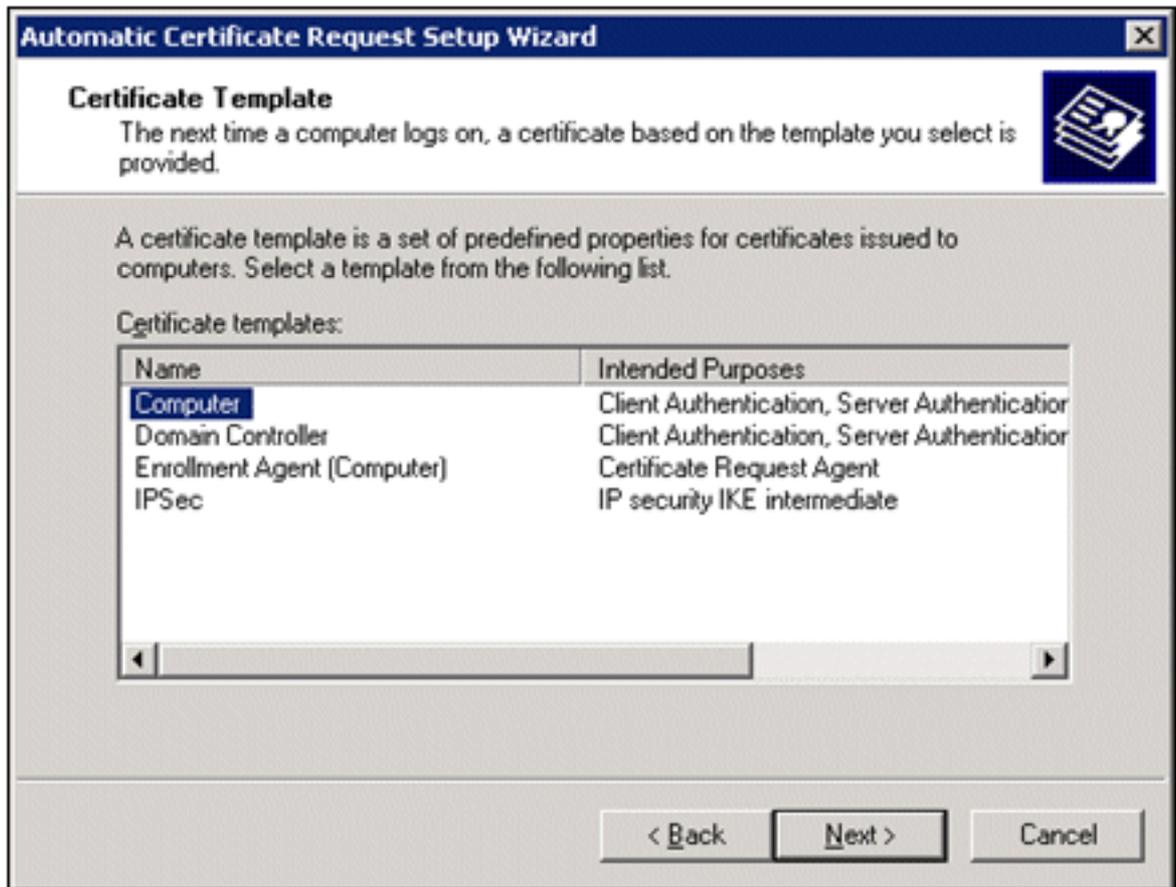


geöffnet.

- Erweitern Sie in der Konsolenstruktur die Option Computerkonfiguration > **Windows-Einstellungen** > **Sicherheitseinstellungen** > **Richtlinien für öffentliche Schlüssel**, und wählen Sie dann die Option **Automatische Zertifikatanforderungseinstellungen** aus.

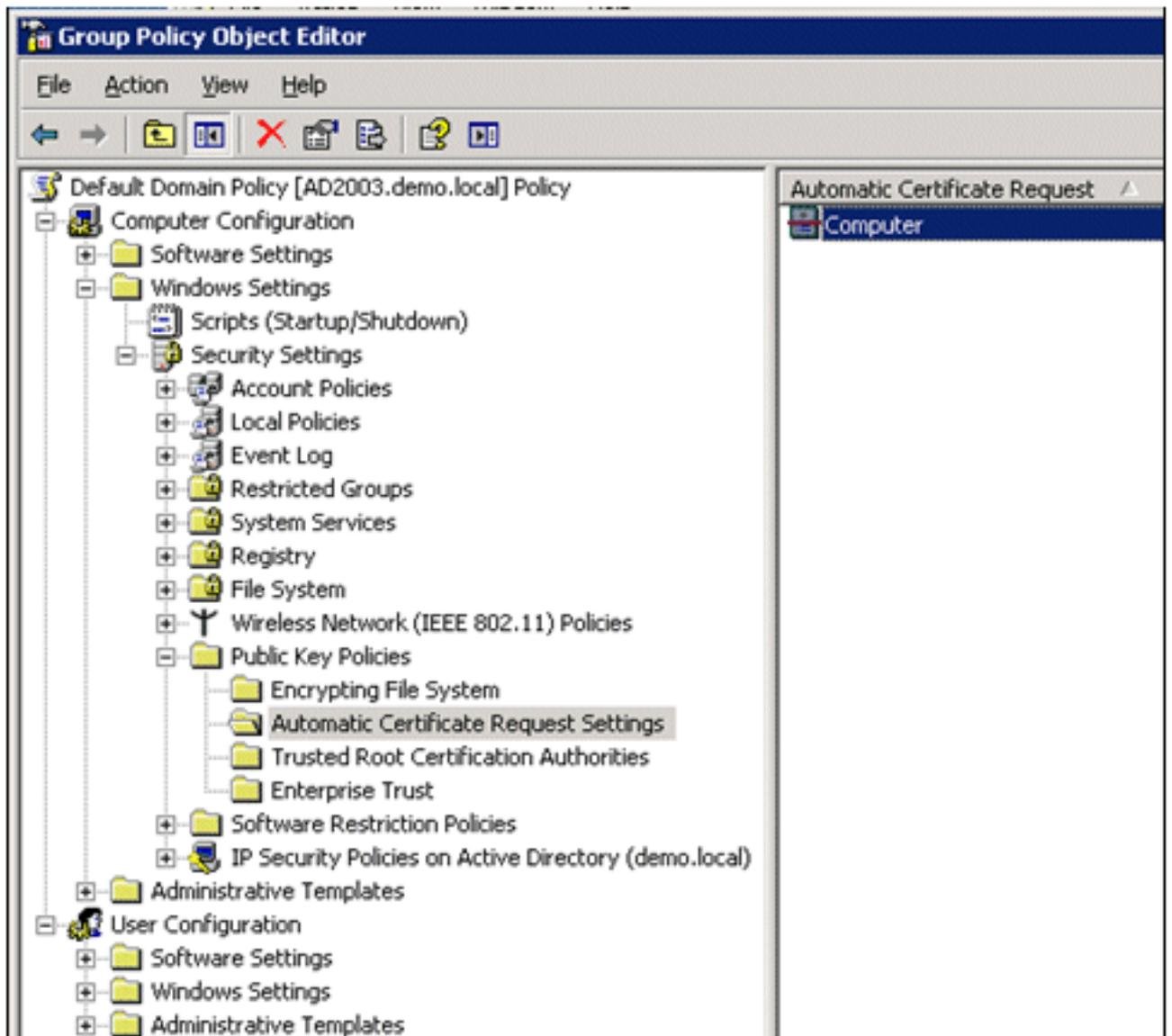


9. Klicken Sie mit der rechten Maustaste auf **Automatic Certificate Request Settings**, und wählen Sie **New > Automatic Certificate Request** aus.
10. Klicken Sie auf der Seite Willkommen des Assistenten für die automatische Zertifikatanforderungseinrichtung auf **Weiter**.
11. Klicken Sie auf der Seite Zertifikatvorlage auf **Computer** und dann auf

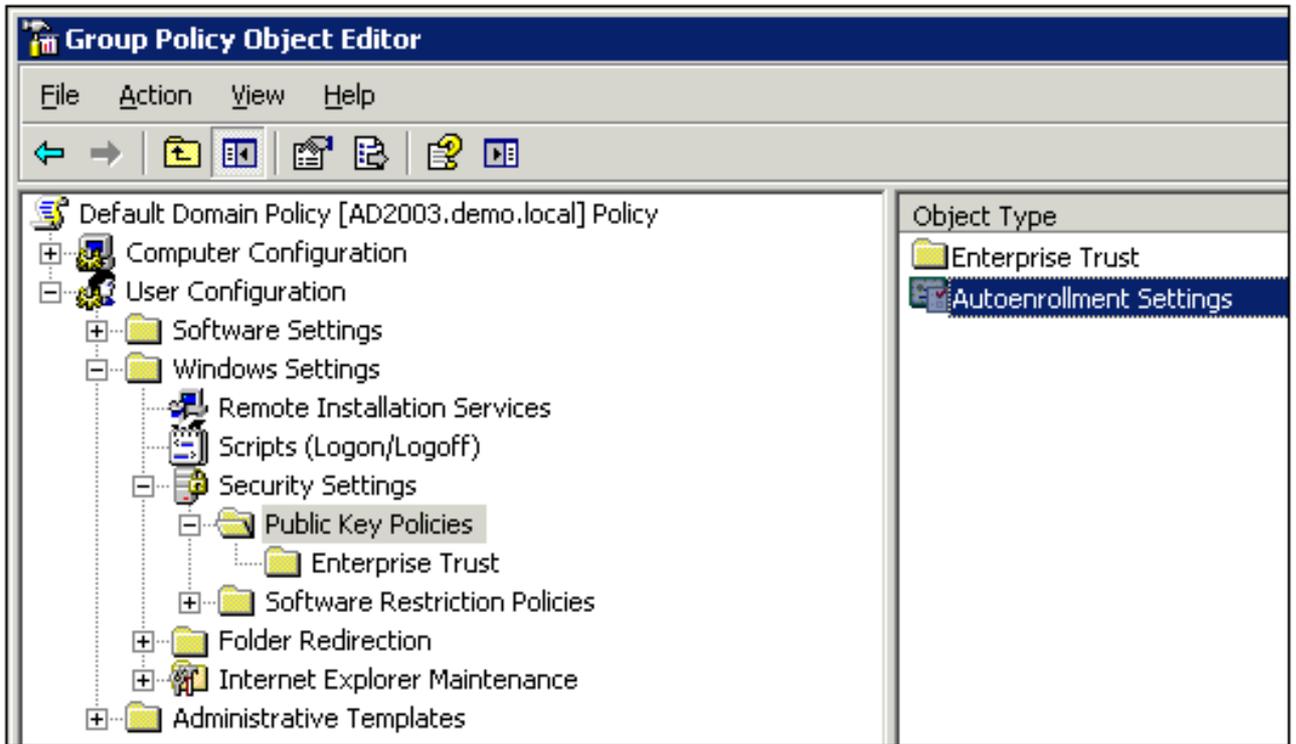


Weiter.

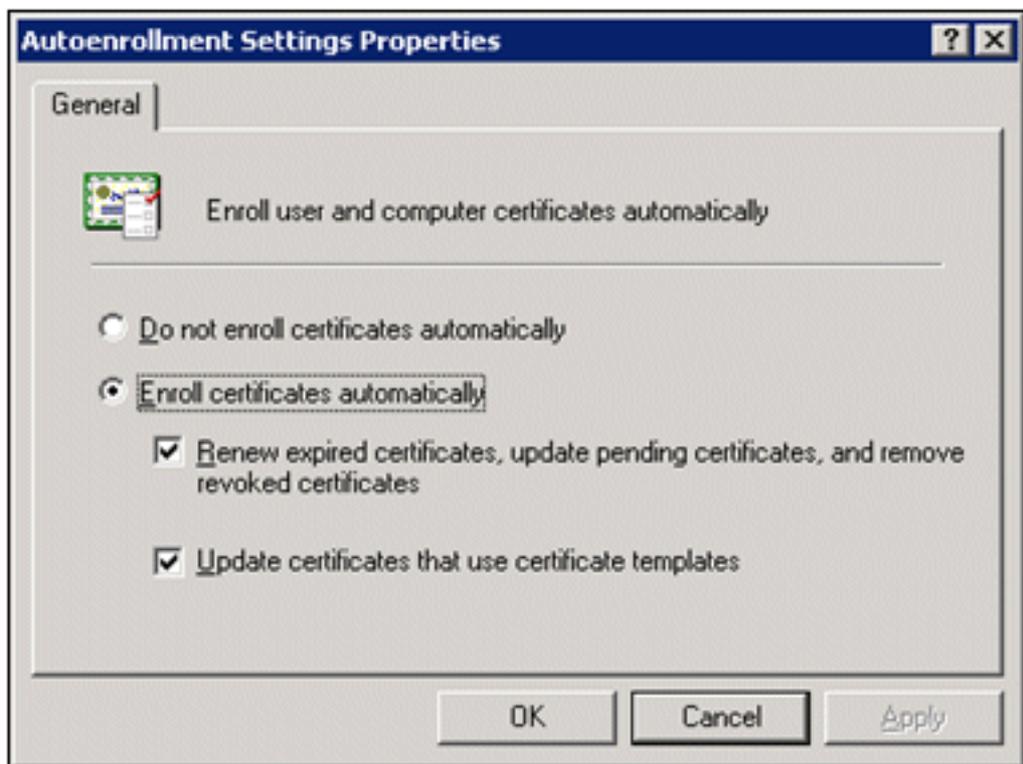
12. Wenn Sie die Seite "Assistent zum automatischen Einrichten von Zertifikatsanforderungen" abgeschlossen haben, klicken Sie auf **Fertig stellen**. Der Computerzertifikattyp wird jetzt im Detailbereich des Snap-Ins Gruppenrichtlinienobjekt-Editor angezeigt.



13. Erweitern Sie in der Konsolenstruktur die Option **Benutzerkonfiguration > Windows-Einstellungen > Sicherheitseinstellungen > Richtlinien für öffentliche Schlüssel**.
14. Doppelklicken Sie im Detailbereich auf **Einstellungen für die automatische Anmeldung**.



15. Wählen Sie **Zertifikate automatisch registrieren** und aktivieren Sie **Abgelaufene Zertifikate erneuern, ausstehende Zertifikate aktualisieren und gesperrte Zertifikate entfernen und Zertifikate aktualisieren, die Zertifikatvorlagen**



verwenden.

16. Klicken Sie auf **OK**.

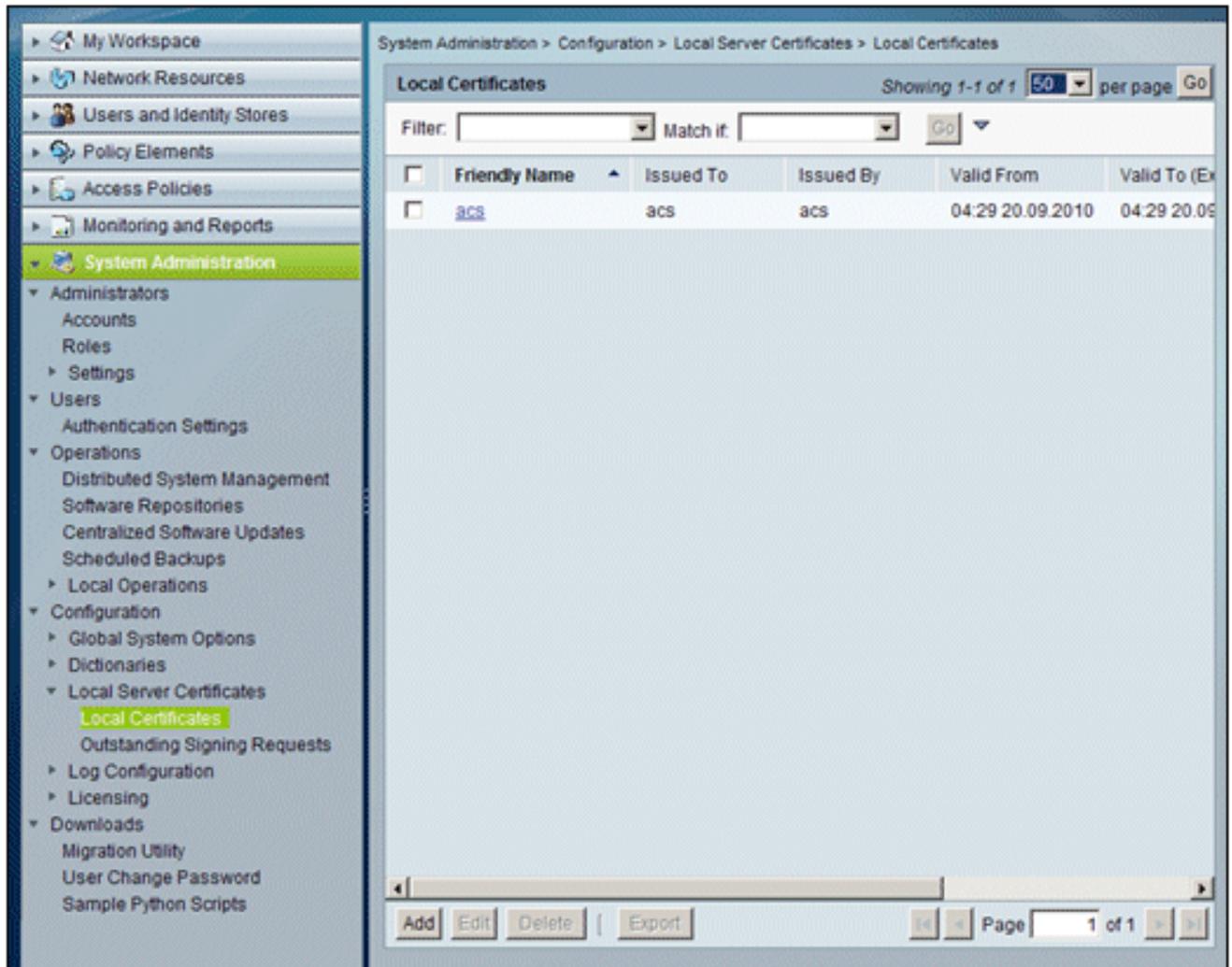
[Einrichtung des ACS 5.1-Zertifikats](#)

[Exportfähiges Zertifikat für ACS konfigurieren](#)

Hinweis: Der ACS-Server muss ein Serverzertifikat vom Stammzertifizierungsstellenserver des Unternehmens erhalten, um einen WLAN-PEAP-Client zu authentifizieren.

Hinweis: Stellen Sie sicher, dass der IIS-Manager während der Zertifikateinrichtung nicht geöffnet ist, da dies zu Problemen mit zwischengespeicherten Informationen führt.

1. Melden Sie sich mit den Administratorrechten beim ACS-Server an.
2. Gehen Sie zu **Systemverwaltung > Konfiguration > Lokale Serverzertifikate**. Klicken Sie auf **Hinzufügen**.



3. Wenn Sie eine Methode zum Erstellen von Serverzertifikaten auswählen, wählen Sie **Signierungsanforderung generieren aus**. Klicken Sie auf **Next** (Weiter).

Cisco Secure ACS NFR(Days left: 296) acsadmin acs (Primary) Log Out About Help

System Administration > Configuration > Local Server Certificates > Local Certificates > Create

Select server certificate creation method

Step 1 - Select server certificate creation method

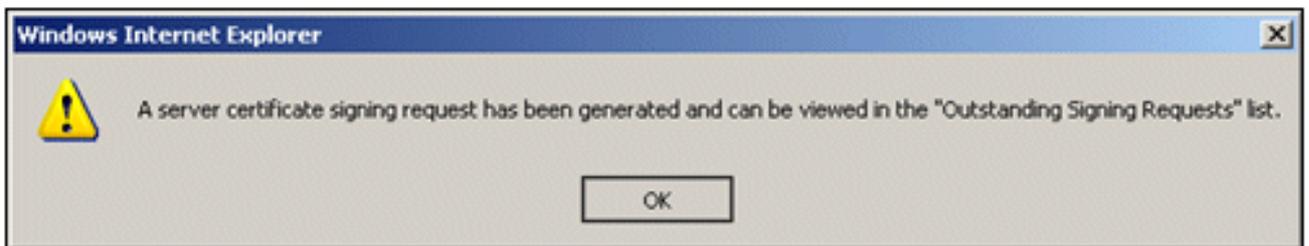
- Import Server Certificate
Use this option if you have a Server Certificate file and corresponding private key file (and password, if the private key file is encrypted).
- Generate Self Signed Certificate
Use this option to have the ACS server generate a Self-Signed Certificate.
- Generate Certificate Signing Request
Use this option to have the ACS server generate a certificate signing request to present to your local Certificate Authority. Once you have generated the signing request, go to the "Outstanding Signing Requests" list, select the signing request, and export a copy of the signing request (save a copy on your client system). Once you receive a certificate from your CA, you will use the "Bind CA Signed Certificate" option below to install it.
- Bind CA Signed Certificate
After using the previous option to generate a certificate signing request, this option is used to bind/install the certificate received from your CA. ACS will automatically match the certificate with the appropriate outstanding signing request.

Back Next Cancel

4. Geben Sie als Beispiel einen Zertifikatantragsteller und die Schlüssellänge ein, und klicken Sie dann auf **Fertig stellen**: Zertifikatantragsteller - CN=acs.demo.local Schlüssellänge: 1024

The screenshot shows the Cisco Secure ACS web interface. The top navigation bar includes the Cisco logo, 'Cisco Secure ACS', 'NFR(Days left: 296)', and user information 'acsadmin', 'acs (Primary)', and 'Log Out'. The left sidebar contains a navigation menu with categories like 'My Workspace', 'Network Resources', 'Users and Identity Stores', 'Policy Elements', 'Access Policies', 'Monitoring and Reports', and 'System Administration'. The 'System Administration' menu is expanded, showing sub-items like 'Administrators', 'Users', 'Operations', 'Configuration', and 'Local Server Certificates'. The 'Local Server Certificates' menu is further expanded to show 'Local Certificates' and 'Outstanding Signing Requests'. The main content area displays the breadcrumb 'System Administration > Configuration > Local Server Certificates > Local Certificates > Create' and a radio button selection for 'Generate Certificate Signing Request'. Below this, the 'Step 2 -Generate Certificate Signing Request' form is shown with fields for 'Certificate Subject' (CN=acs.demo.local), 'Key Length' (1024), and 'Digest to Sign with' (SHA1). 'Back' and 'Finish' buttons are at the bottom right.

5. ACS fordert Sie auf, eine Signaturanforderung für das Zertifikat zu generieren. Klicken Sie auf **OK**.



6. Gehen Sie unter System Administration (Systemverwaltung) zu **Configuration > Local Server Certificates > Outstanding Signing Requests**. Hinweis: Der Grund für diesen Schritt besteht darin, dass Windows 2003 keine exportierbaren Schlüssel zulässt und Sie eine Zertifikatanforderung auf der Grundlage des zuvor erstellten ACS-Zertifikats generieren müssen.

Cisco Secure ACS
NFR(Days left: 296)

acsadmin acs (Primary) Log Out About Help

System Administration > Configuration > Local Server Certificates > Outstanding Signing Requests

Certificate Signing Request Showing 1-1 of 1 50 per page Go

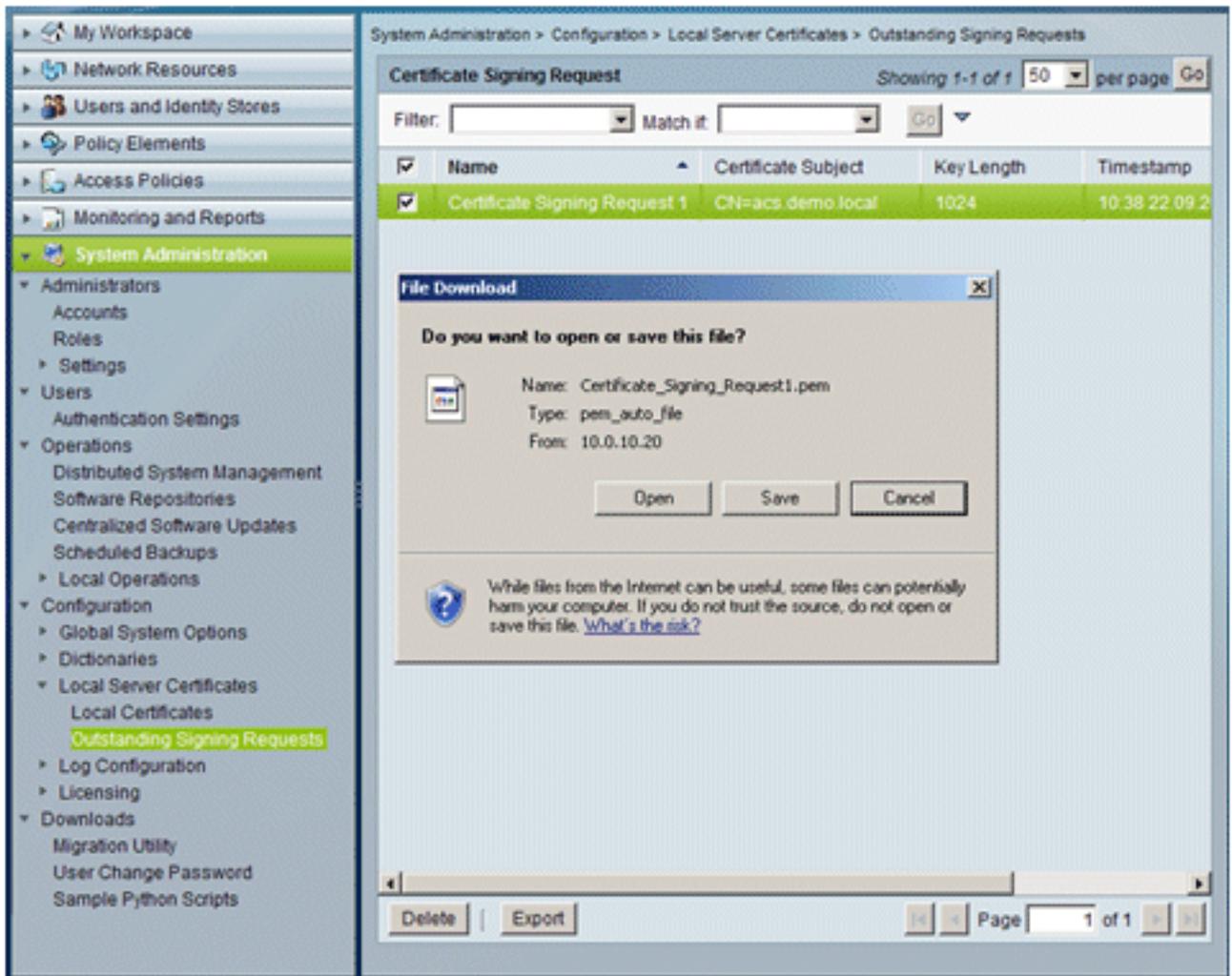
Filter: Match it: Go

<input type="checkbox"/>	Name	Certificate Subject	Key Length	Timestamp
<input type="checkbox"/>	Certificate Signing Request 1	CN=acs.demo.local	1024	10:38 22.09.2

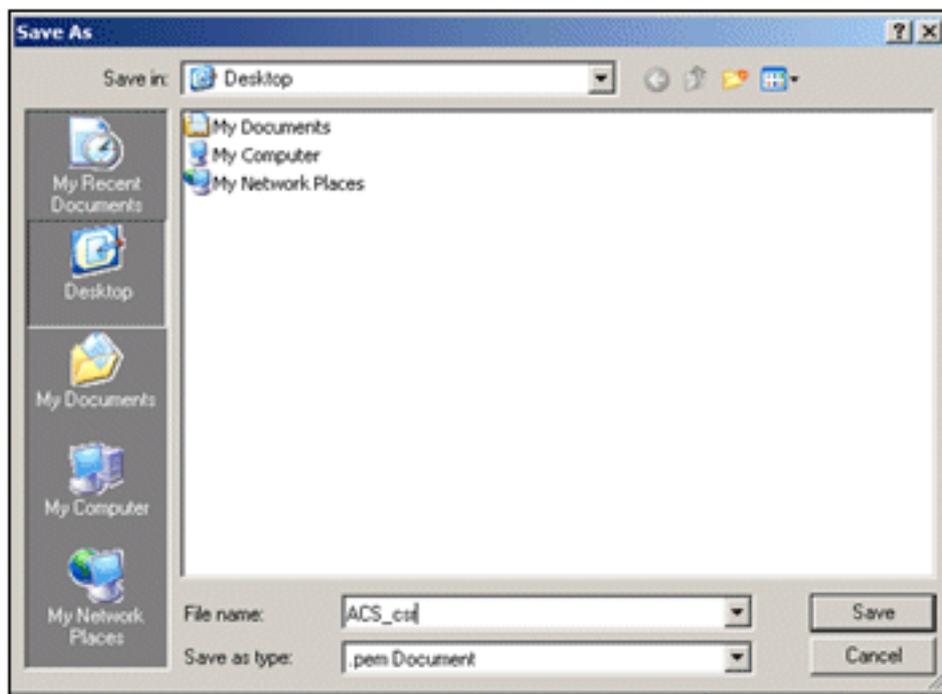
multiple row selection

Delete | Export Page 1 of 1

7. Wählen Sie den Eintrag **Zertifikatsignierungsanforderung** aus, und klicken Sie auf **Exportieren**.



8. Speichern Sie die Datei ACS certificate.pem auf dem

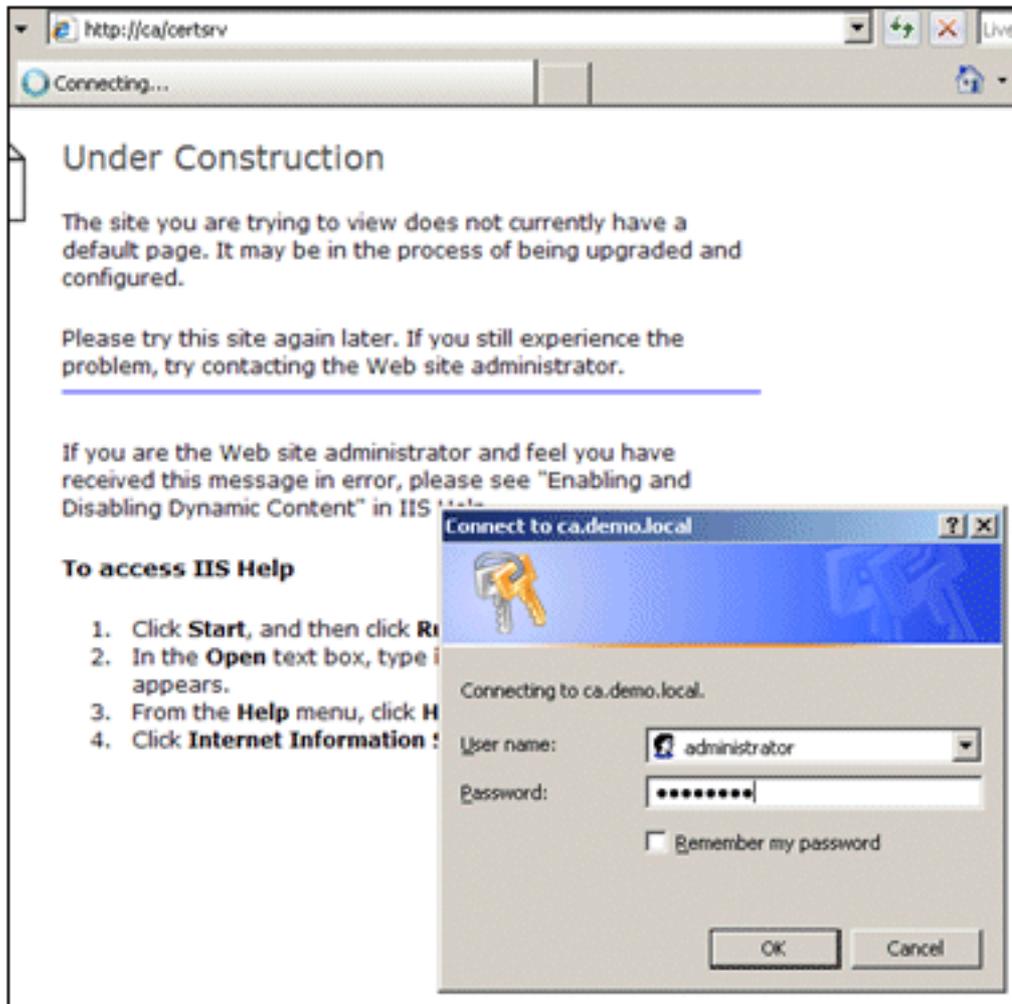


Desktop.

[Installieren des Zertifikats in der ACS 5.1-Software](#)

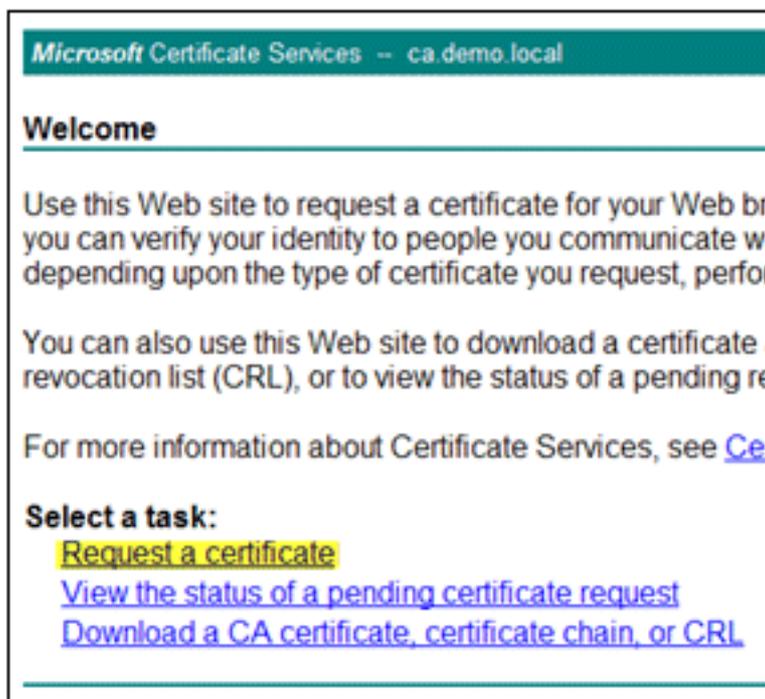
Gehen Sie folgendermaßen vor:

1. Öffnen Sie einen Browser, und stellen Sie eine Verbindung mit der URL des CA-Servers <http://10.0.10.10/certsrv>



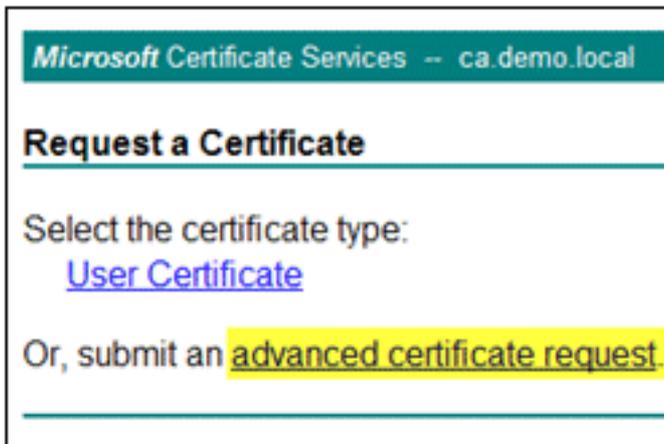
her.

2. Das Fenster Microsoft-Zertifikatdienste wird angezeigt. Wählen Sie **Zertifikat anfordern**



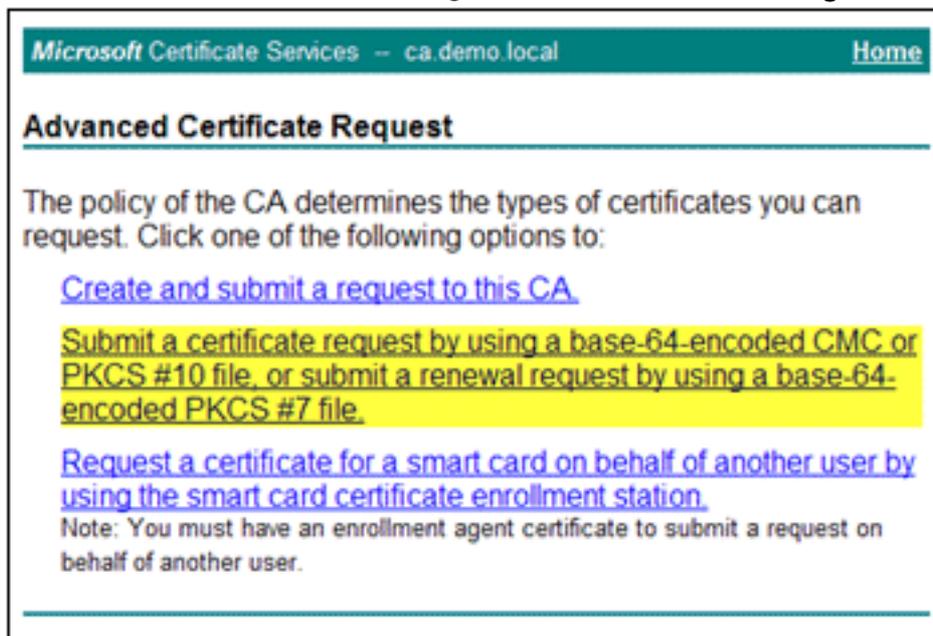
aus.

3. Klicken Sie hier, um eine **Anforderung für ein erweitertes Zertifikat** zu



senden.

4. Klicken Sie in der erweiterten Anforderung auf **Zertifikatsanforderung mit Base-64-Codierung**



senden...

5. Wenn es die Browsersicherheit zulässt, navigieren Sie im Feld Gespeicherte Anforderung zur vorherigen ACS-Zertifikatsanforderungsdatei, und fügen Sie sie

Microsoft Certificate Services -- ca.demo.local [Home](#)

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

[Browse for a file to insert.](#)

Certificate Template:

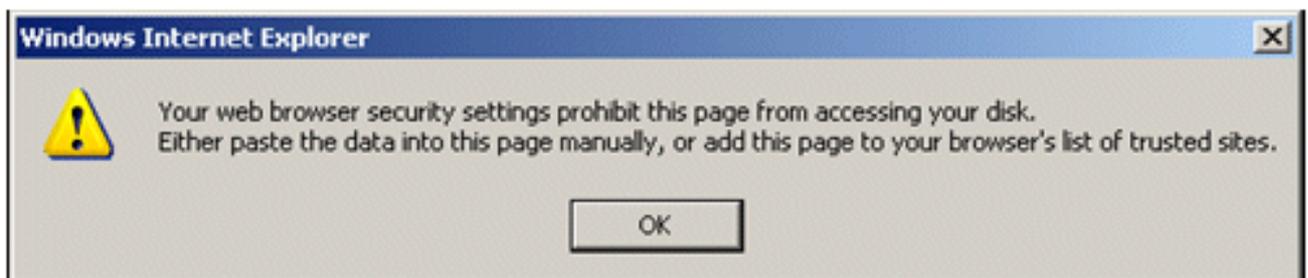
Administrator

Additional Attributes:

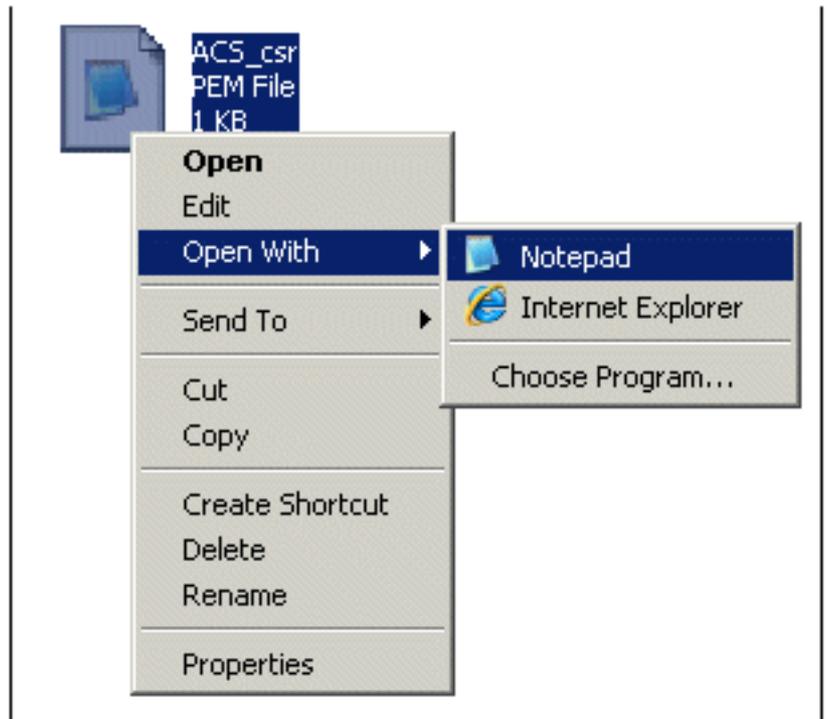
Attributes:

ein.

- Die Sicherheitseinstellungen des Browsers erlauben möglicherweise keinen Zugriff auf die Datei auf einer Festplatte. Wenn dies der Fall ist, klicken Sie auf **OK**, um eine manuelle Einfügung durchzuführen.

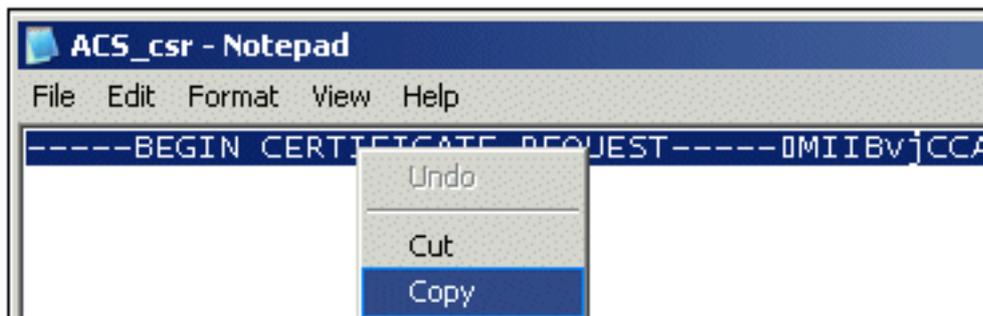


- Suchen Sie die ACS *.pem-Datei aus dem vorherigen ACS-Export. Öffnen Sie die Datei mit



einem Texteditor (z. B. Notepad).

8. Markieren Sie den gesamten Inhalt der Datei, und klicken Sie auf



Kopieren.

9. Kehren Sie zum Fenster für die Microsoft-Zertifikatanforderung zurück. **Fügen Sie** den kopierten Inhalt in das Feld Gespeicherter Antrag

Microsoft Certificate Services -- ca.demo.local

Submit a Certificate Request or Renew

To submit a saved request to the CA, paste a renewal request generated by an external tool into the text box below.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

[Browse](#) [Paste](#) [Copy](#) [Delete](#) [Undo](#) [Cut](#) [Select All](#)

Certificate Template:

Administrator

ein.

10. Wählen Sie **ACS** als Zertifikatvorlage aus, und klicken Sie auf

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```

YIZIAYb4QgEBBAQDAgZAMA0GCSqGSIB3DQEBBQUA
DXoIoRABet447wO77+uAk8ern26oaEhcfG/ZR15X
ONZQ5xnrK23yxEdQNVsFPC30mzRZEbQq4a5MvPEZZ
/MWqXej3NjpicpAg1V8CSwNd
-----END CERTIFICATE REQUEST-----

```

[Browse for a file to insert.](#)

Certificate Template:

ACS

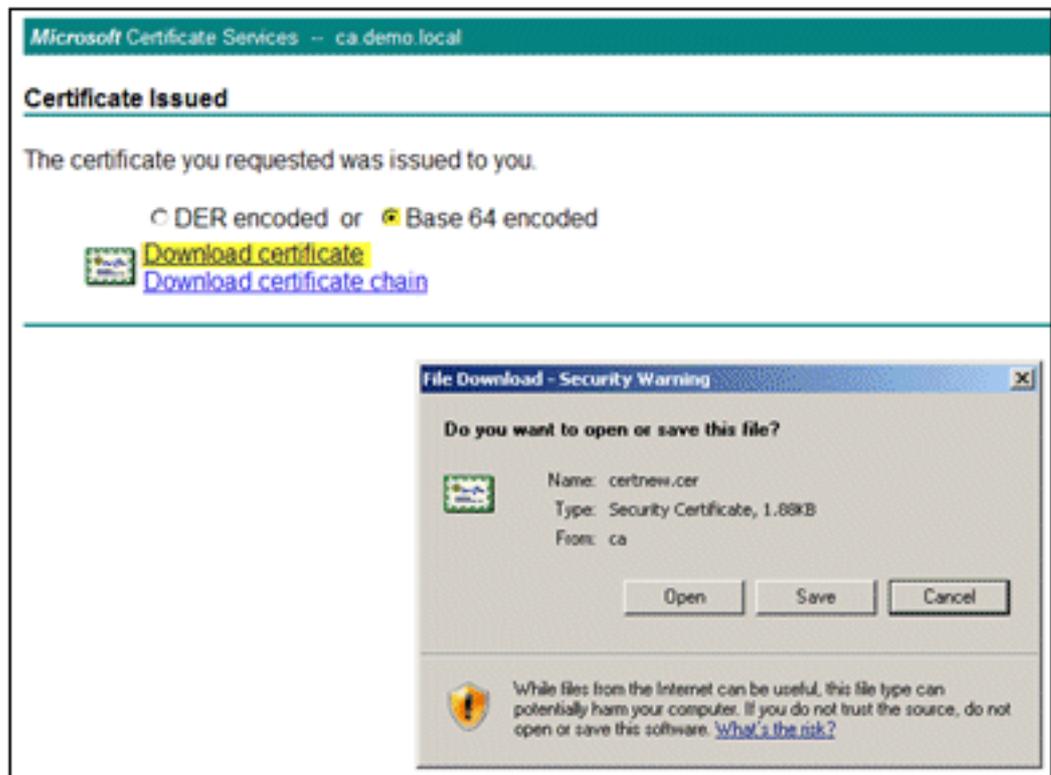
Additional Attributes:

Attributes:

[Submit >](#)

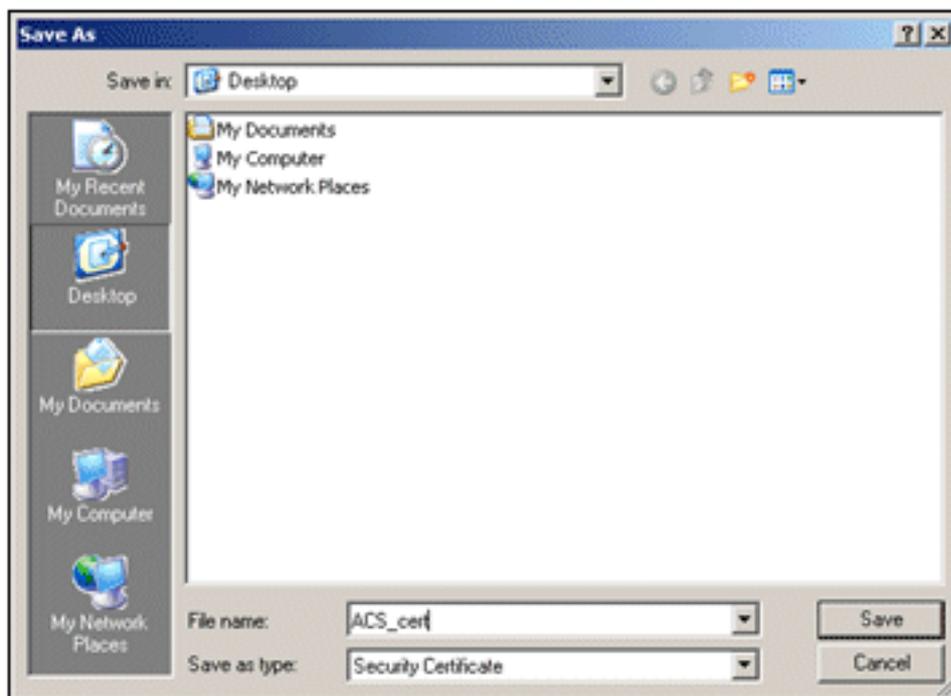
Senden.

11. Sobald das Zertifikat ausgestellt wurde, wählen Sie **Base 64-codiert aus**, und klicken Sie auf **Zertifikat**



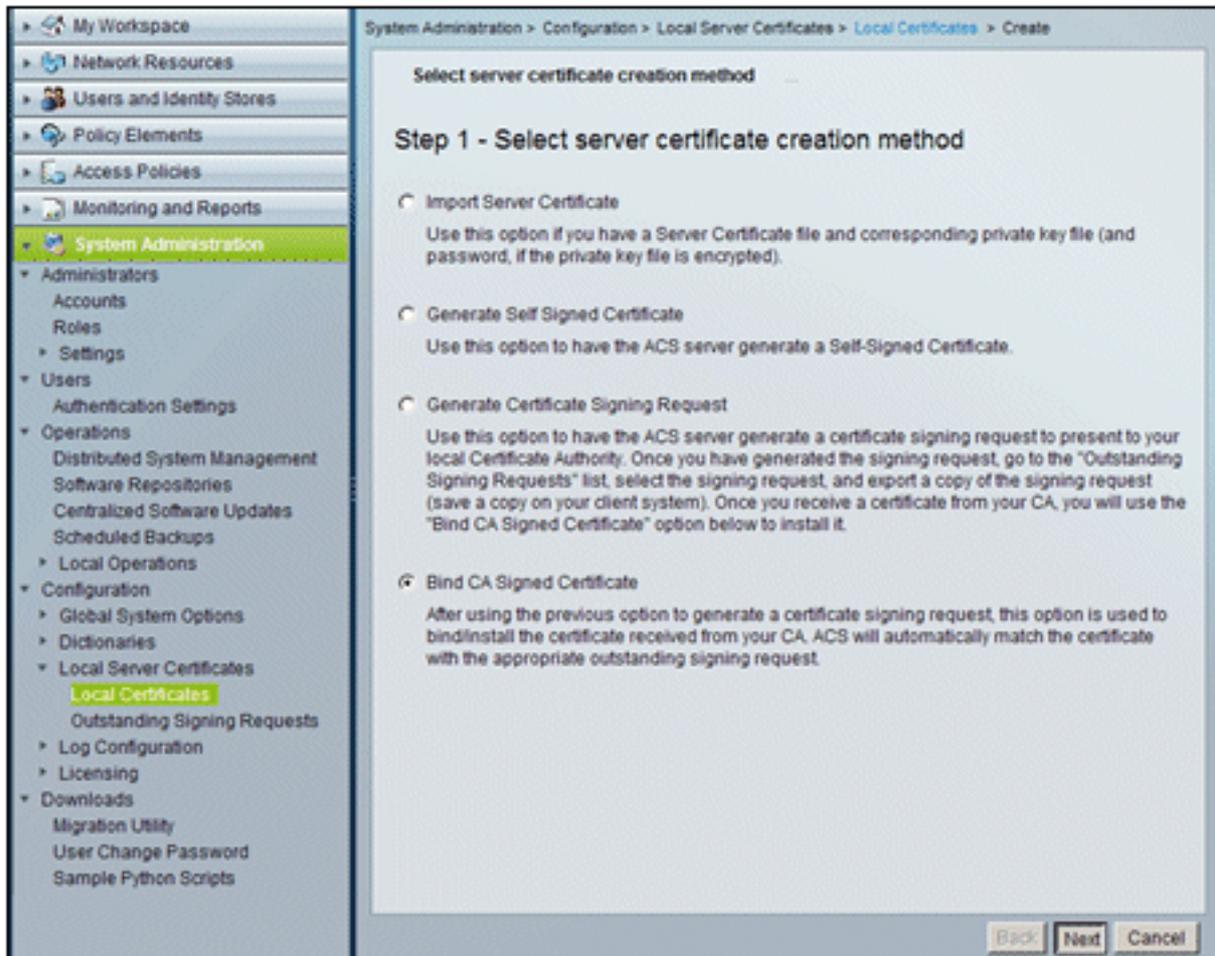
herunterladen.

12. Klicken Sie auf **Speichern**, um das Zertifikat auf dem Desktop zu

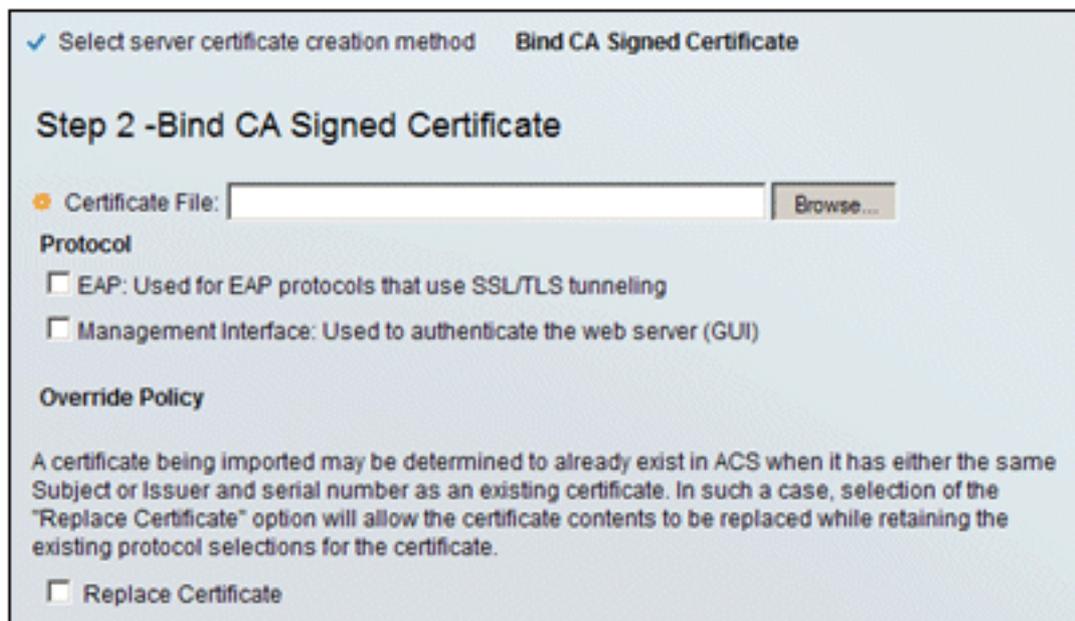


speichern.

13. Gehen Sie zu **ACS > System Administration > Configuration > Local Server Certificates**. Wählen Sie **Signiertes CA-Zertifikat binden** aus, und klicken Sie auf **Weiter**.

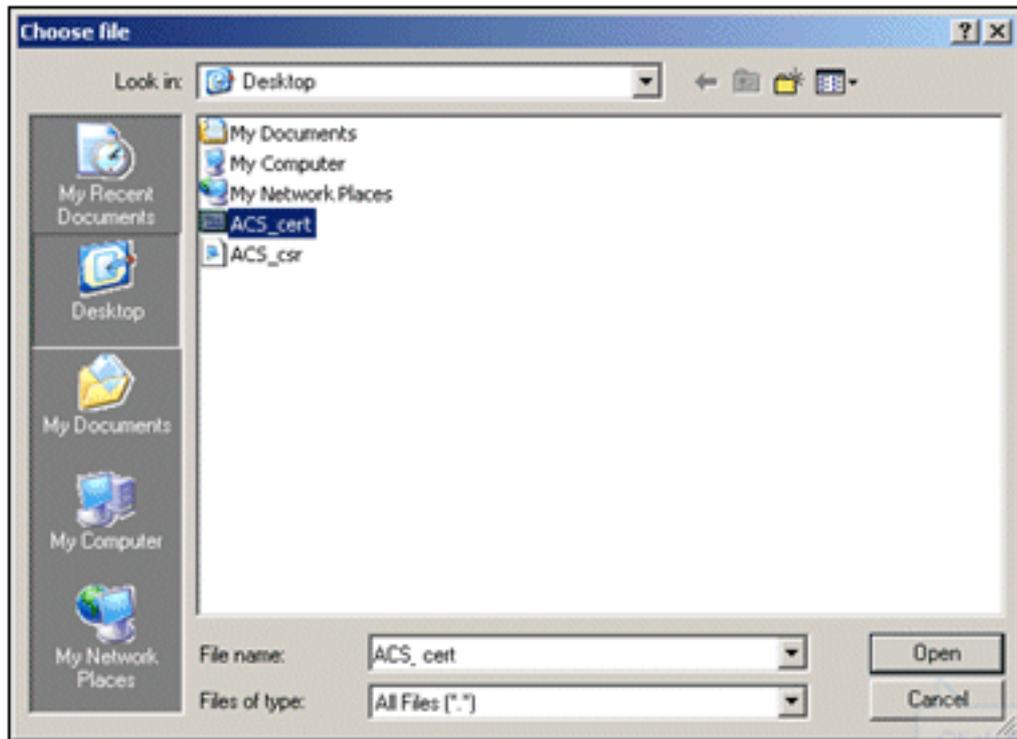


14. Klicken Sie auf **Durchsuchen**, und suchen Sie nach dem gespeicherten



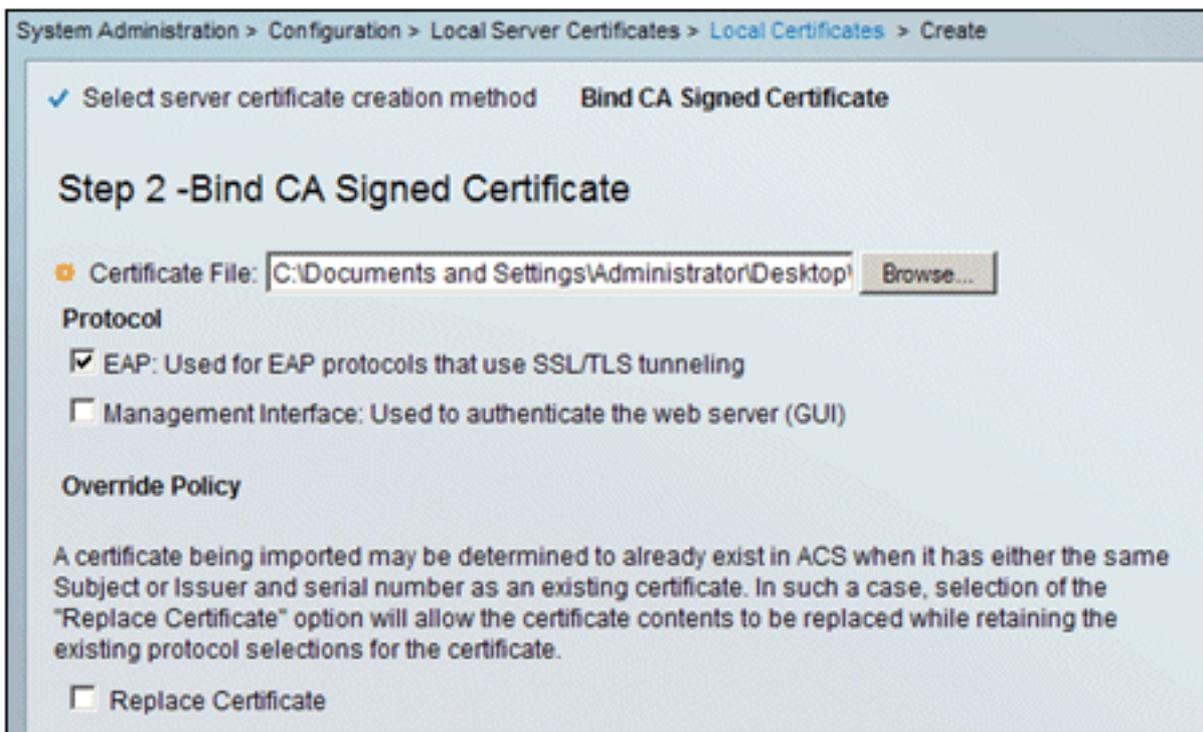
Zertifikat.

15. Wählen Sie das vom Zertifizierungsstellenserver ausgestellte ACS-Zertifikat aus, und klicken Sie auf



Öffnen.

16. Aktivieren Sie außerdem das Kontrollkästchen Protocol (Protokoll) für **EAP**, und klicken Sie auf **Finish (Fertig stellen)**.



17. Das von der Zertifizierungsstelle ausgestellte ACS-Zertifikat wird im lokalen ACS-Zertifikat angezeigt.

System Administration > Configuration > Local Server Certificates > Local Certificates

Local Certificates Showing 1-2 of 2

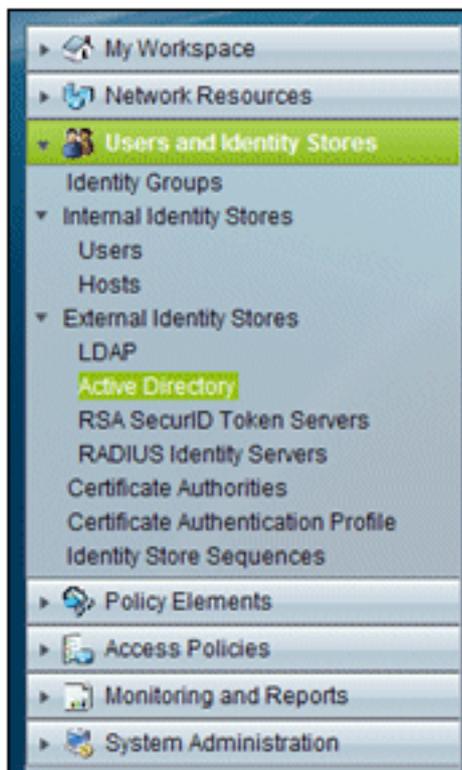
Filter: Match if:

<input type="checkbox"/>	Friendly Name ▲	Issued To	Issued By	Valid From
<input type="checkbox"/>	acs	acs	acs	04:29 20.09.2010
<input checked="" type="checkbox"/>	acs_demo.local	acs_demo.local	ca_demo.local	10:39 22.09.2010

Konfigurieren des ACS-Identitätsspeichers für Active Directory

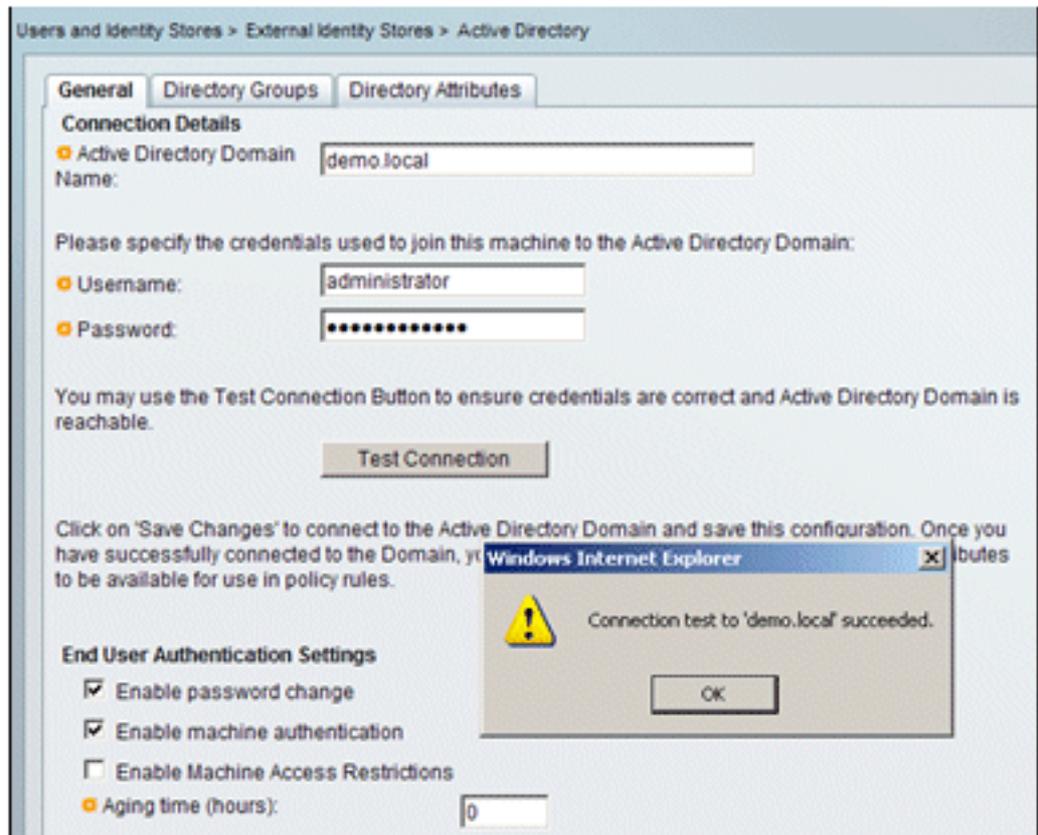
Gehen Sie folgendermaßen vor:

1. Stellen Sie eine Verbindung mit dem ACS her, und melden Sie sich mit dem Administratorkonto an.
2. Gehen Sie zu **Benutzer und Identitätsdaten > Externe Identitätsdaten > Active**



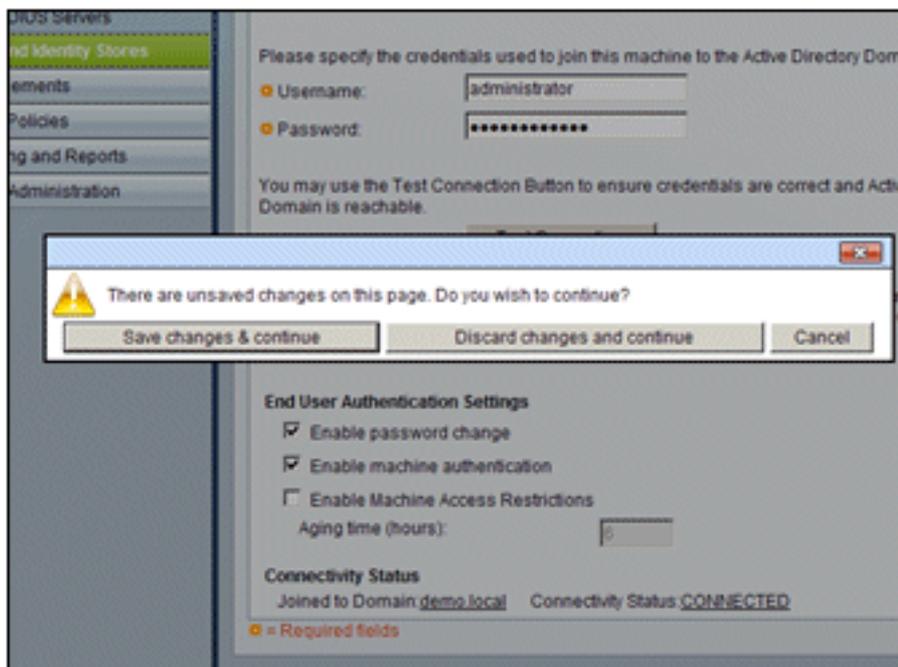
Directory.

3. Geben Sie die Active Directory-Domäne *demo.local* ein, geben Sie das Kennwort des Servers ein, und klicken Sie auf **Verbindung testen**. Klicken Sie auf **OK**, um



fortzufahren.

4. Klicken Sie auf **Änderungen**



speichern.

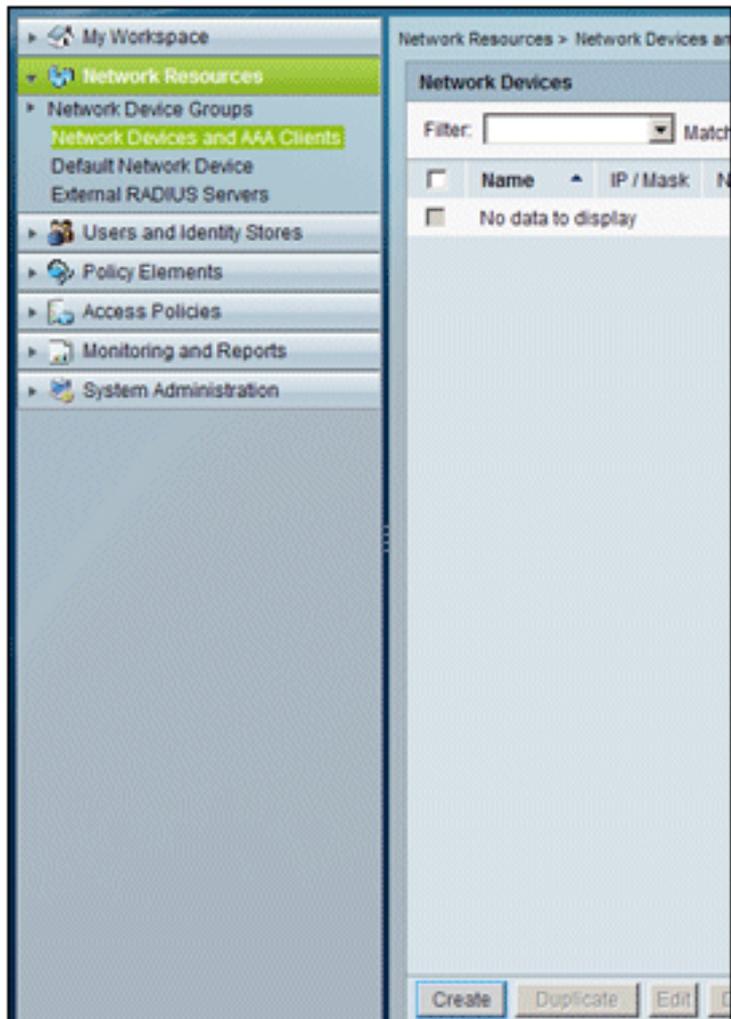
Hinweis: Weitere

Informationen zum Integrationsverfahren für ACS 5.x finden Sie unter [ACS 5.x und höher: Integration in Microsoft Active Directory Configuration Example](#).

Hinzufügen eines Controllers zum ACS als AAA-Client

Gehen Sie folgendermaßen vor:

1. Stellen Sie eine Verbindung mit ACS her, und gehen Sie zu **Network Resources > Network Devices and AAA Clients**. Klicken Sie auf



Erstellen.

2. Geben Sie in diese Felder Folgendes ein:
Name - **wlcIP - 10.0.1.10**
RADIUS-Kontrollkästchen - **Aktiviert**
Gemeinsamer geheimer Schlüssel -

Network Resources > Network Devices and AAA Clients > Create

Name:
 Description:

Network Device Groups

Location:
 Device Type:

IP Address

Single IP Address IP Range (s)
 IP:

Authentication Options

TACACS+ Shared Secret:
 Single Connected Device
 Legacy TACACS+ Single Connected Support
 TACACS+ Draft Compliant Single Connected Support

RADIUS Shared Secret:

TrustSec Use Device ID for TrustSec Identification
 Device ID:
 Password:

* = Required fields

Cisco

3. Klicken Sie abschließend auf **Senden**. Der Controller wird als Eintrag in der Liste der ACS-Netzwerkgeräte angezeigt.

Network Resources > Network Devices and AAA Clients

Network Devices Showing 1-1 of 1

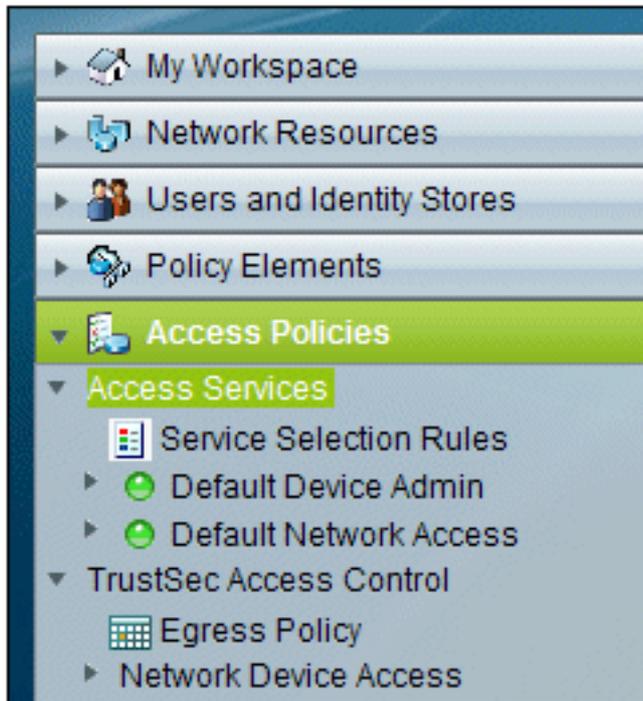
Filter: Match if:

<input type="checkbox"/>	Name	IP / Mask	NDG:Location	NDG:Device Type
<input type="checkbox"/>	wlc	10.0.1.10/32	All Locations	All Device Types

Konfigurieren von ACS-Zugriffsrichtlinien für Wireless

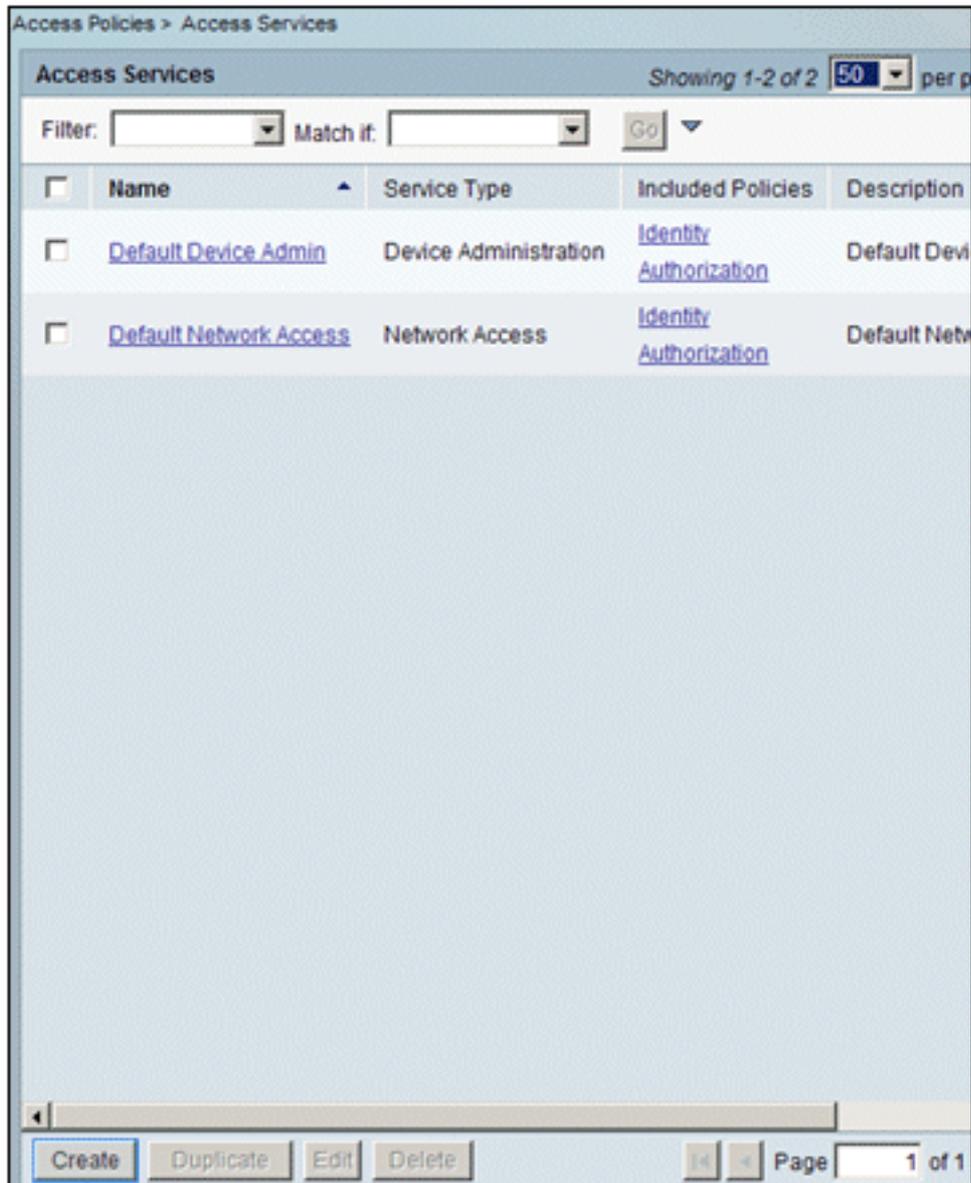
Gehen Sie folgendermaßen vor:

1. Gehen Sie in ACS zu **Access Policies > Access**



Services.

2. Klicken Sie im Fenster Access Services (Zugriffsdienste) auf **Create**



(Erstellen).

3. Erstellen Sie einen Zugriffsdienst, und geben Sie einen Namen ein (beispielsweise

WirelessAD). Wählen Sie **Basierend auf Servicevorlage aus**, und klicken Sie auf **Auswählen**.

Access Policies > Access Services > Create

General Allowed Protocols

Step 1 - General

General

Name:

Description:

Access Service Policy Structure

Based on service template

Based on existing service

User Selected Service Type

4. Wählen Sie im Webseitendialog **Netzwerkzugriff - Einfach**. Klicken Sie auf **OK**.

Cisco Secure ACS -- Webpage Dialog

Access Services Showing 1-4 of 4

Filter: Match if:

	Name	Service Type	Description
<input type="radio"/>	Device Admin - Command Auth	Device Administration	
<input type="radio"/>	Device Admin - Simple	Device Administration	
<input type="radio"/>	Network Access - MAC Authentication Bypass	Network Access	
<input checked="" type="radio"/>	Network Access - Simple	Network Access	

5. Wählen Sie im Webseitendialog **Netzwerkzugriff - Einfach**. Klicken Sie auf **OK**. Klicken Sie nach Auswahl der Vorlage auf

Step 1 - General

General

Name:

Description:

Access Service Policy Structure

Based on service template

Based on existing service

User Selected Service Type

Weiter.

6. Aktivieren Sie unter Zugelassene Protokolle die Kontrollkästchen **MS-CHAPv2** zulassen und

Access Policies > Access Services > Create

✓ General Allowed Protocols

Step 2 - Allowed Protocols

Process Host Lookup

Authentication Protocols

▶ Allow PAP/ASCII

▶ Allow CHAP

▶ Allow MS-CHAPv1

▶ Allow MS-CHAPv2

▶ Allow EAP-MD5

▶ Allow EAP-TLS

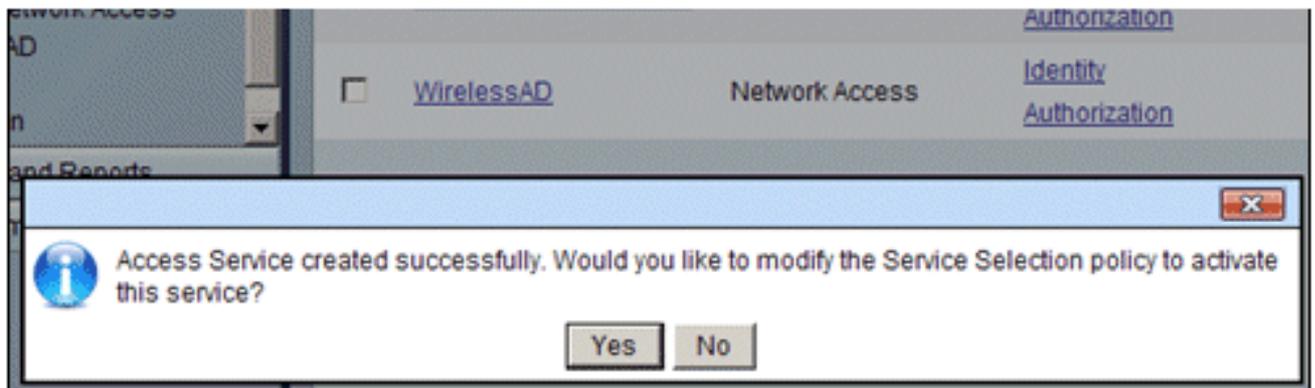
▶ Allow LEAP

▶ Allow PEAP

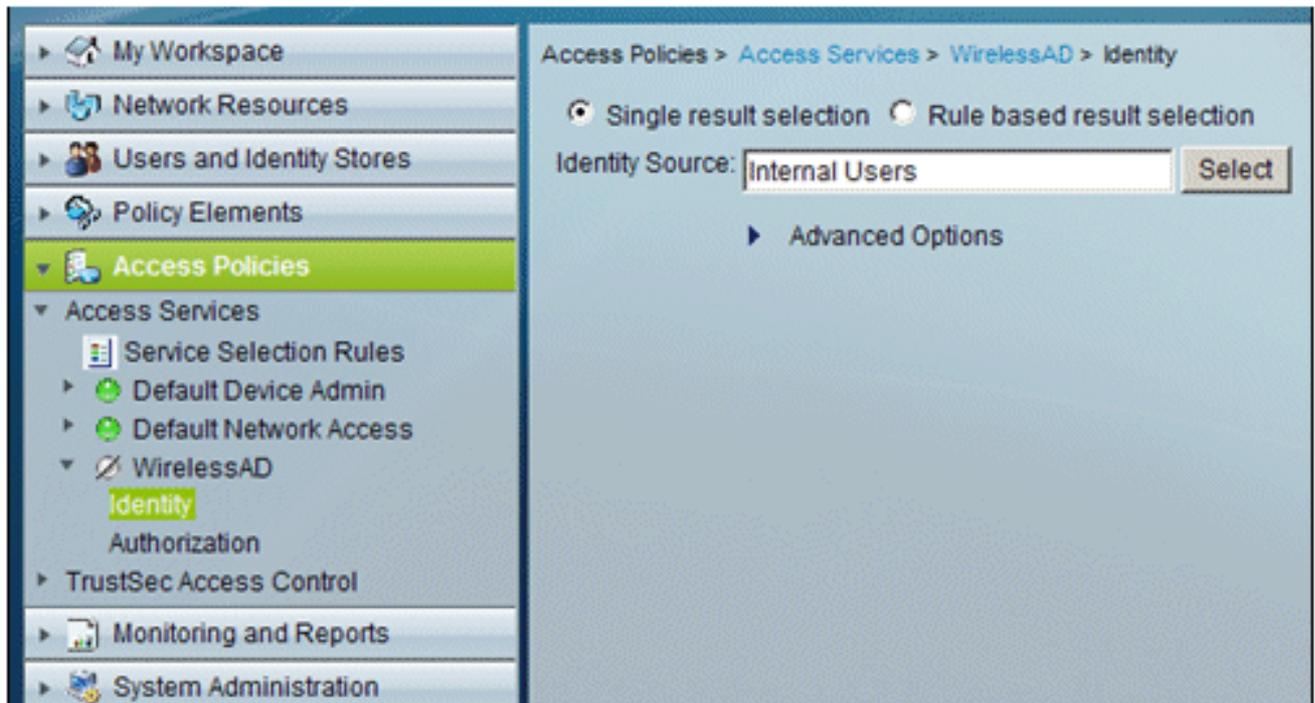
▶ Allow EAP-FAST

PEAP zulassen. Klicken Sie auf **Beenden**.

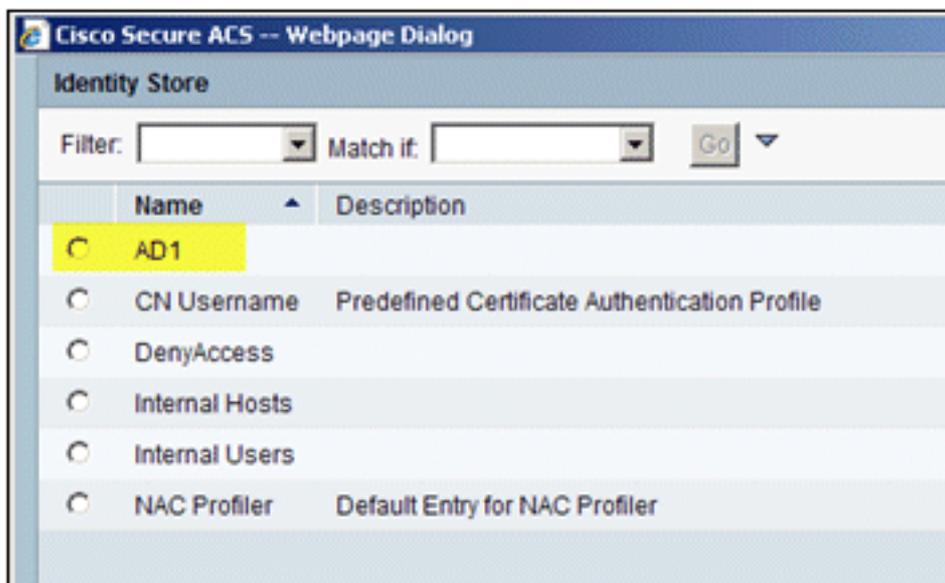
7. Wenn Sie von ACS aufgefordert werden, den neuen Service zu aktivieren, klicken Sie auf **Ja**.



8. Erweitern Sie im neuen Zugriffsdienst, der gerade erstellt/aktiviert wurde, und wählen Sie **Identity (Identität)**. Klicken Sie als Identitätsquelle auf **Auswählen**.



9. Wählen Sie **AD1** für Active Directory aus, das in ACS konfiguriert wurde, und klicken Sie auf



OK.

10. Bestätigen Sie, dass die Identitätsquelle AD1 ist, und klicken Sie auf **Save Changes (Änderungen)**

Access Policies > Access Services > WirelessAD > Identity

Single result selection
 Rule based result selection

Identity Source:

speichern).

Erstellen einer ACS-Zugriffsrichtlinie und einer Serviceregeln

Gehen Sie folgendermaßen vor:

1. Gehen Sie zu **Zugriffsrichtlinien > Dienstauswahlregeln**.

Access Policies > Access Services > Service Selection Rules

Single result selection
 Rule based result selection

Service Selection Policy

Filter: Match if:

	<input type="checkbox"/>	Status	Name	Protocol	Cond
1	<input type="checkbox"/>	🟢	Rule-1	match Radius	
2	<input type="checkbox"/>	🟢	Rule-2	match Tacacs	

2. Klicken Sie im Fenster Dienstauswahlrichtlinie auf **Erstellen**. Geben Sie der neuen Regel einen Namen (z. B. *WirelessRule*). Aktivieren Sie das Kontrollkästchen für **Protocol to match Radius**.

Cisco Secure ACS -- Webpage Dialog

General

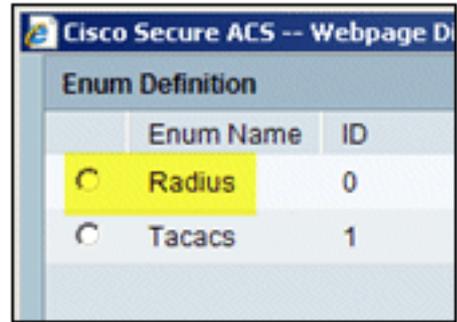
Name: Status: 🟢

The Customize button in the lower right area of the policy rules screen conditions and results are available here for use in policy rules.

Conditions

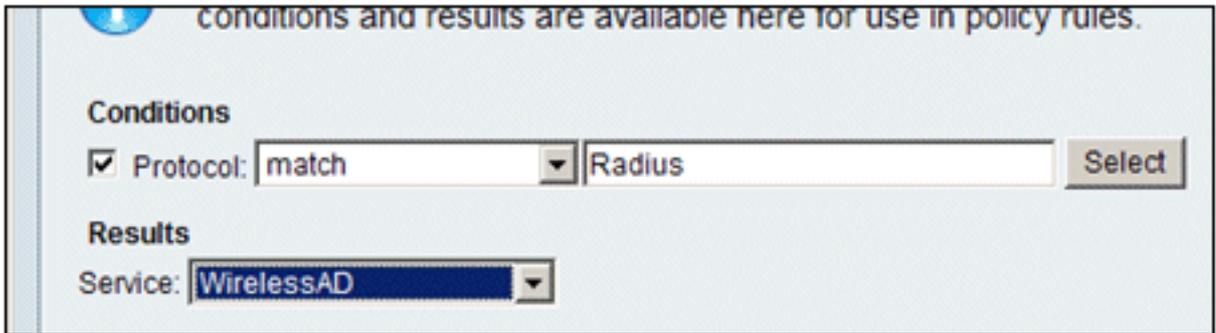
Protocol:

Results



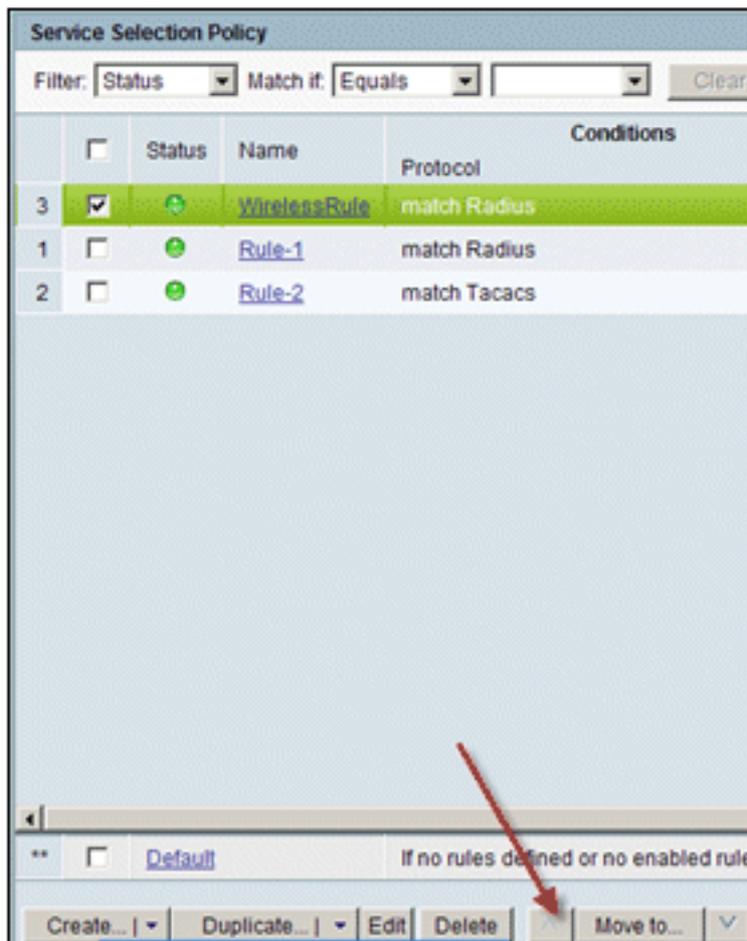
3. Wählen Sie **Radius aus**, und klicken Sie auf OK.

4. Wählen Sie unter Ergebnisse die Option **WirelessAD** für Dienst (wurde im vorherigen Schritt erstellt)



aus.

5. Nachdem die neue Wireless-Regel erstellt wurde, wählen Sie diese Regel aus, und **verschieben Sie sie** nach oben. Dies ist die erste Regel, die die Wireless-RADIUS-Authentifizierung mit Active Directory



identifiziert.

CLIENT-Konfiguration für PEAP mit Windows Zero Touch

In unserem Beispiel ist CLIENT ein Computer, auf dem Windows XP Professional mit SP ausgeführt wird und der als Wireless-Client fungiert und über den Wireless Access Point Zugriff auf Intranet-Ressourcen erhält. Gehen Sie wie in diesem Abschnitt beschrieben vor, um CLIENT als Wireless-Client zu konfigurieren.

Durchführen einer einfachen Installation und Konfiguration

Gehen Sie folgendermaßen vor:

1. Verbinden Sie den CLIENT mithilfe eines mit dem Hub verbundenen Ethernetkabels mit dem Netzwerksegment des Intranets.
2. Installieren Sie auf CLIENT Windows XP Professional mit SP2 als Mitgliedscomputer namens CLIENT der Domäne demo.local.
3. Installieren Sie Windows XP Professional mit SP2. Diese muss installiert sein, damit PEAP-Unterstützung verfügbar ist. **Hinweis:** Die Windows-Firewall ist in Windows XP Professional mit SP2 automatisch aktiviert. Schalten Sie die Firewall nicht aus.

Installieren der Wireless-Netzwerkkarte

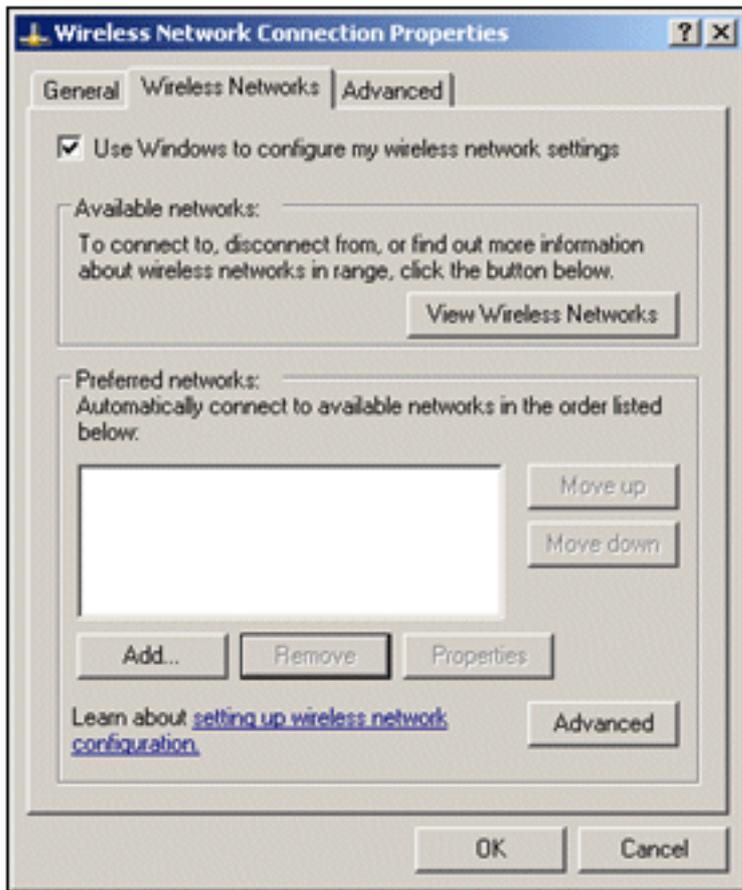
Gehen Sie folgendermaßen vor:

1. Den CLIENT-Computer herunterfahren.
2. Trennen Sie den CLIENT-Computer vom Intranet-Netzwerksegment.
3. Starten Sie den CLIENT-Computer neu, und melden Sie sich dann mit dem lokalen Administratorkonto an.
4. Installieren Sie den Wireless-Netzwerkadapter. **Hinweis:** Installieren Sie nicht die Konfigurationssoftware des Herstellers für den Wireless-Adapter. Installieren Sie die Treiber für die Wireless-Netzwerkkarte mithilfe des Hardware-Assistenten. Wenn Sie dazu aufgefordert werden, legen Sie außerdem die vom Hersteller bereitgestellte CD oder einen Datenträger mit aktualisierten Treibern für die Verwendung mit Windows XP Professional mit SP2 bereit.

Konfigurieren der Wireless-Netzwerkverbindung

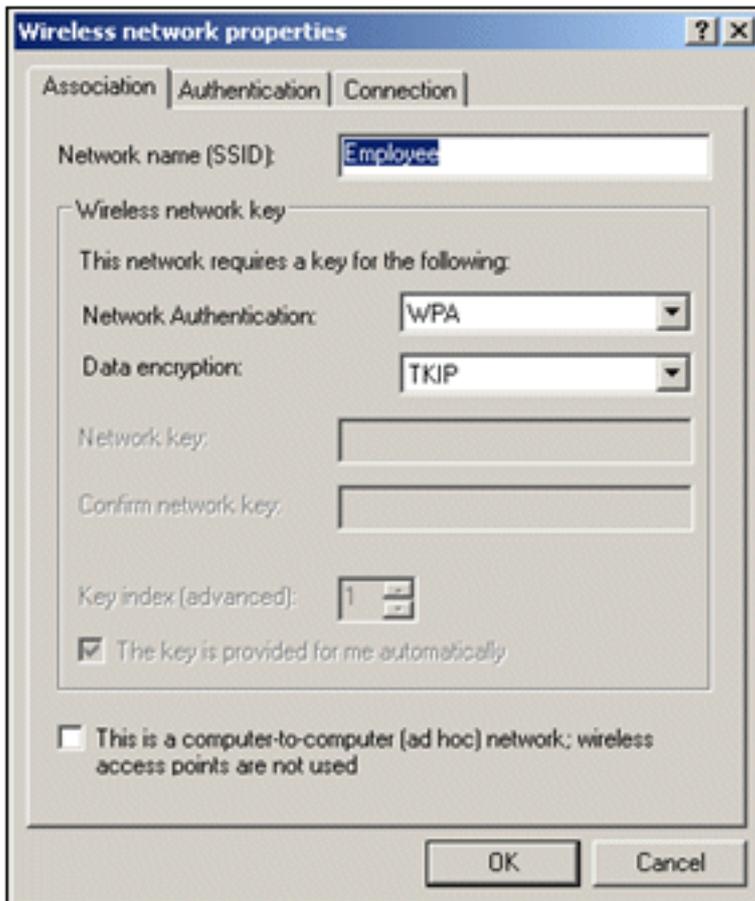
Gehen Sie folgendermaßen vor:

1. Melden Sie sich ab, und melden Sie sich dann über das **WirelessUser**-Konto in der **demo.local**-Domäne an.
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**, wechseln Sie zur Registerkarte **Drahtlose Netzwerke**, und stellen Sie sicher, dass das Kontrollkästchen **Windows zum Konfigurieren der Drahtlosnetzwerkeinstellungen verwenden** aktiviert



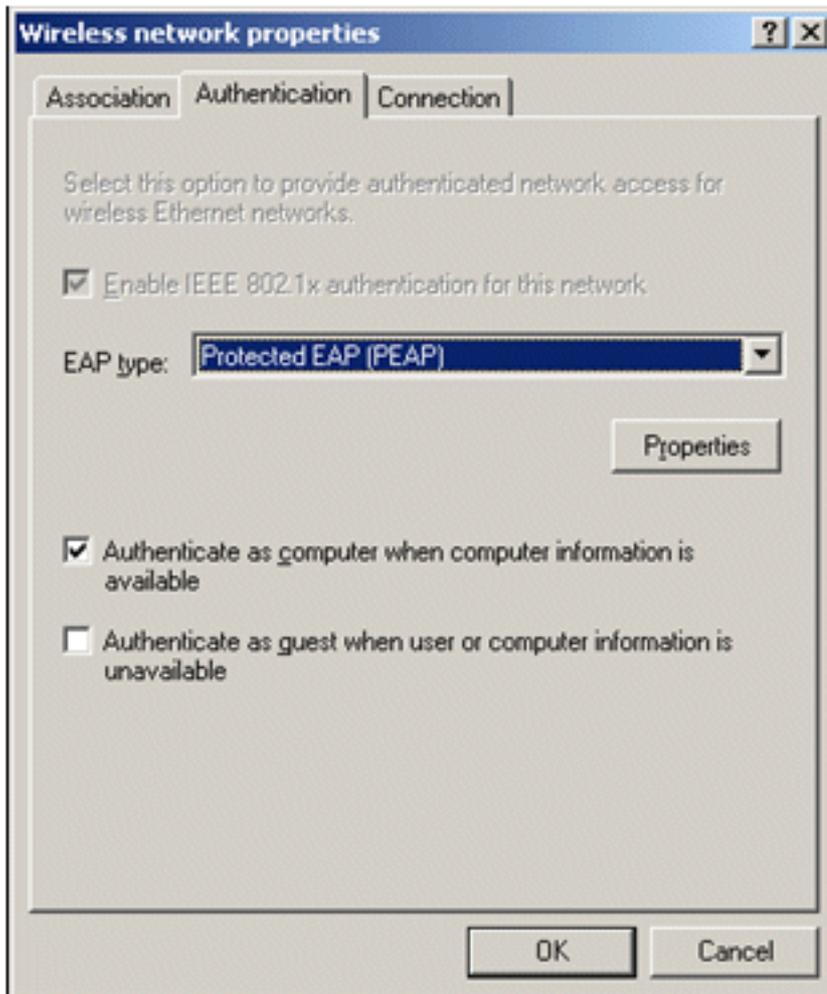
ist.

4. Klicken Sie auf **Hinzufügen**.
5. Geben Sie auf der Registerkarte Zuordnung im Feld Netzwerkname (SSID) den *Mitarbeiter* ein.
6. Wählen Sie **WPA** für die Netzwerkauthentifizierung aus, und stellen Sie sicher, dass die Datenverschlüsselung auf **TKIP** festgelegt



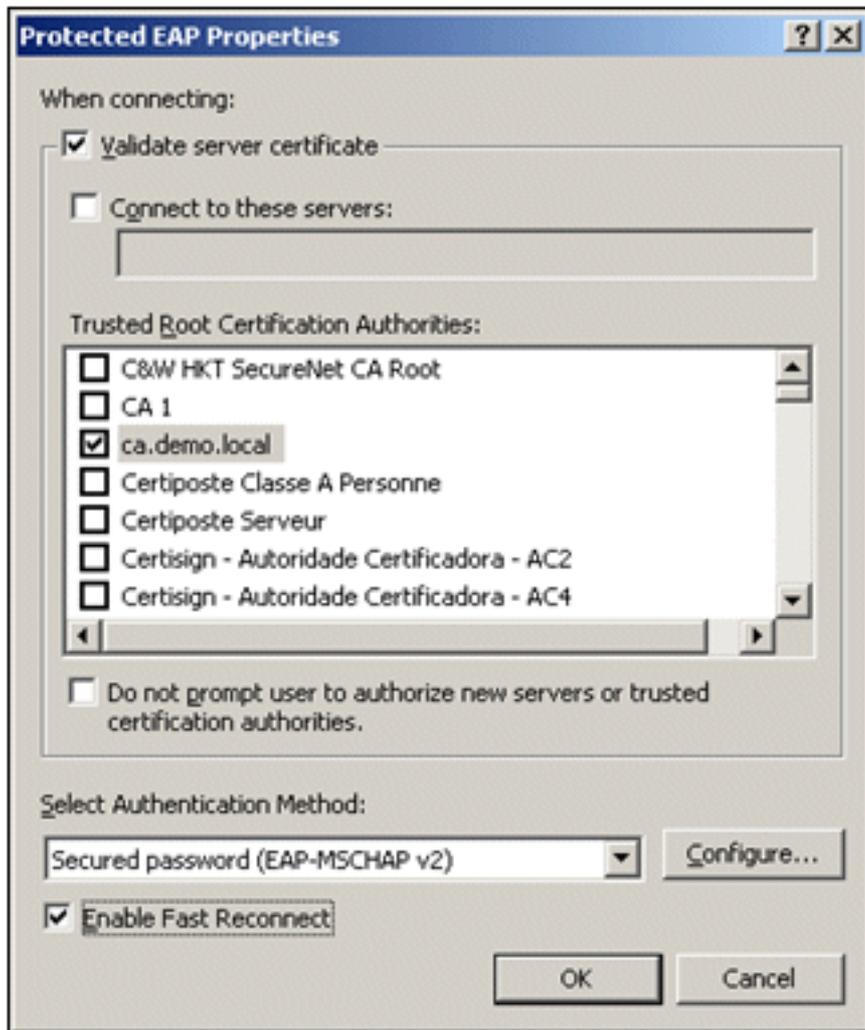
ist.

7. Klicken Sie auf die Registerkarte **Authentifizierung**.
8. Überprüfen Sie, ob der EAP-Typ für die Verwendung von **PEAP (Protected EAP)** konfiguriert ist. Ist dies nicht der Fall, wählen Sie es aus dem Dropdown-Menü aus.
9. Wenn der Computer vor der Anmeldung authentifiziert werden soll (wodurch Anmeldeskripts oder Gruppenrichtlinien angewendet werden können), aktivieren Sie **Als Computer authentifizieren, wenn Computerinformationen verfügbar**



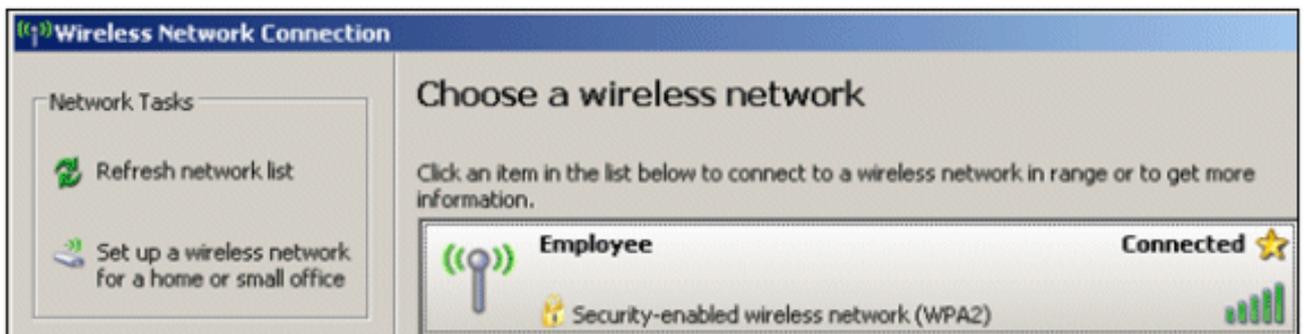
sind.

10. Klicken Sie auf **Properties** (Eigenschaften).
11. Da PEAP die Authentifizierung des Servers durch den Client umfasst, stellen Sie sicher, dass das **Serverzertifikat validieren** aktiviert ist. Stellen Sie außerdem sicher, dass die Zertifizierungsstelle, die das ACS-Zertifikat ausgestellt hat, im Menü "Trusted Root Certification Authorities" (Vertrauenswürdige Stammzertifizierungsstellen) aktiviert ist.
12. Wählen Sie unter "Authentication Method" die Option **Secured password (EAP-MSCHAP v2)** aus, da sie für die innere Authentifizierung verwendet



wird.

13. Vergewissern Sie sich, dass das Kontrollkästchen "**Schnelle Wiederverbindung aktivieren**" aktiviert ist. Klicken Sie dann dreimal auf **OK**.
14. Klicken Sie mit der rechten Maustaste auf das Symbol für die Wireless-Netzwerkverbindung in der Taskleiste, und klicken Sie dann auf **Verfügbare Wireless-Netzwerke anzeigen**.
15. Klicken Sie auf das Wireless-Netzwerk Mitarbeiter und dann auf **Verbinden**. Der Wireless-Client zeigt **Verbunden an**, wenn die Verbindung erfolgreich hergestellt wurde.

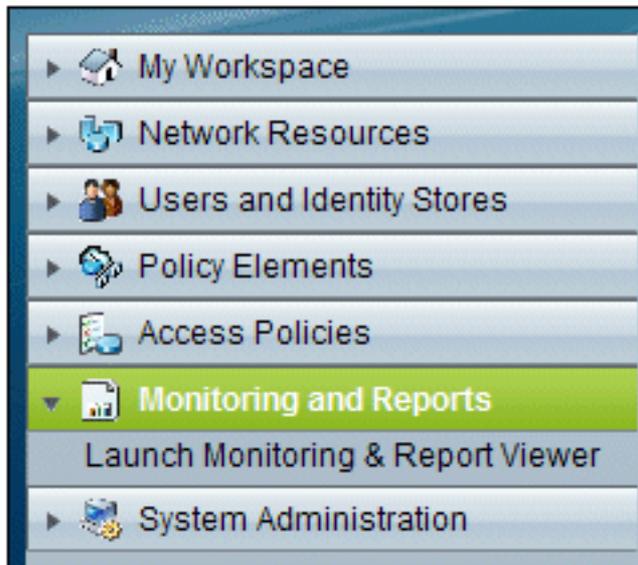


16. Nachdem die Authentifizierung erfolgreich war, überprüfen Sie mithilfe von Netzwerkverbindungen die TCP/IP-Konfiguration für den Wireless-Adapter. Der Adressbereich muss 10.0.20.100-10.0.20.200 aus dem DHCP-Bereich oder dem für die Wireless-Clients von CorpNet erstellten Bereich sein.
17. Um die Funktionalität zu testen, öffnen Sie einen Browser und navigieren Sie zu **http://10.0.10.10** (oder zur IP-Adresse des CA-Servers).

Fehlerbehebung bei der Wireless-Authentifizierung mit ACS

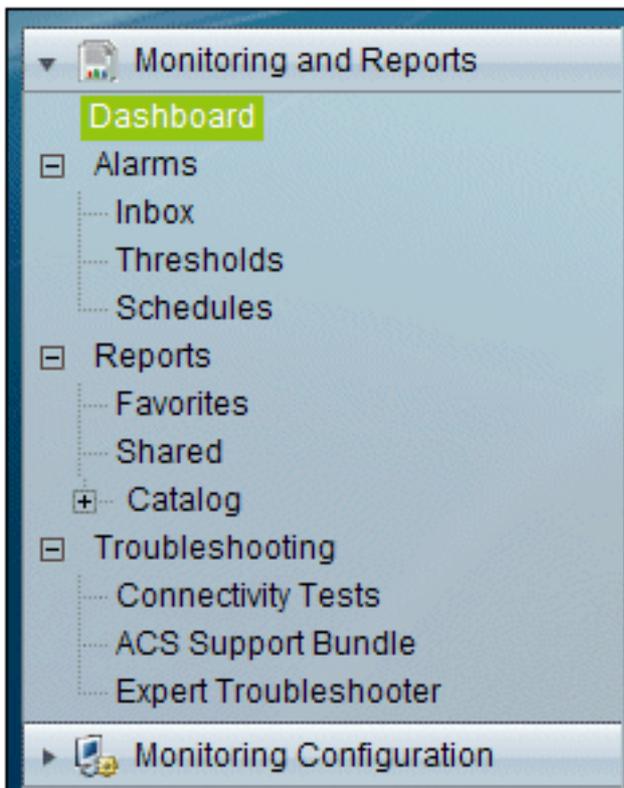
Gehen Sie folgendermaßen vor:

1. Gehen Sie zu **ACS > Monitoring and Reports**, und klicken Sie auf **Launch Monitoring &**



Report Viewer.

2. Ein separates ACS-Fenster wird geöffnet. Klicken Sie auf



Dashboard.

3. Klicken Sie im Abschnitt "My Favourite Reports" auf **Authentications - RADIUS - Today**.

My Favorite Reports	
Favorite Name	Report Name
ACS - Configuration Audit - Today	ACS Instance>ACS_Configuration_Audit
ACS - System Errors - Today	ACS Instance>ACS_System_Diagnostics
Authentications - RADIUS - Today	AAA Protocol>RADIUS_Authentication

4. In einem Protokoll werden alle RADIUS-Authentifizierungen als "Bestanden" oder "Fehlgeschlagen" angezeigt. Klicken Sie innerhalb eines protokollierten Eintrags auf das Lupensymbol in der Spalte Details.

AAA Protocol > RADIUS Authentication							
Authentication Status : Pass or Fail							
Date : September 22, 2010 (Last 30 Minutes Last Hour Last 12 Hours Today Yesterday Last 7 Days Last 30 Days)							
Generated on September 22, 2010 5:51:34 PM PDT							
Reload							
✓=Pass ✗=Fail 🔍=Click for details 🖱=Mouse over item for additional information							
Logged At	RADIUS Status	NAS Failure	Details	Username	MAC/IP Address	Access Service	Authentication Method
Sep 22, 10 5:51:17.843 PM	✓		🔍	wirelessuser	00-21-5c-69-9a-39	WirelessAD	PEAP (EAP-MSCHAPv2)

5. Die RADIUS-Authentifizierungsdetails enthalten viele Informationen zu den protokollierten

AAA Protocol > RADIUS Authentication Detail	
ACS session ID :	acs/74551189/31
Date :	September 22, 2010
Generated on September 22, 2010 5:52:16 PM PDT	
Authentication Summary	
Logged At:	September 22, 2010 5:51:17.843 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	wirelessuser
MAC/IP Address:	00-21-5c-69-9a-39
Network Device:	wlc : 10.0.1.10 :
Access Service:	WirelessAD
Identity Store:	AD1
Authorization Profiles:	Permit Access
CTS Security Group:	
Authentication Method:	PEAP(EAP-MSCHAPv2)

Versuchen.

- Die Anzahl der ACS-Service-Treffer kann eine Übersicht über Versuche liefern, die mit der/den in ACS erstellten Regel(n) übereinstimmen. Gehen Sie zu **ACS > Access Policies > Access Services**, und klicken Sie auf **Service Selection**

Results	Hit Count
Service	
WirelessAD	33
Default Network Access	0

Rules.

[PEAP-Authentifizierung schlägt mit ACS-Server fehl](#)

Wenn der Client die PEAP-Authentifizierung mit einem ACS-Server nicht erfolgreich durchführt, überprüfen Sie, ob die Fehlermeldung `NAS duplicate authentication attempts` in der Option **Failed attempts (Fehlgeschlagene Versuche)** im Menü **Report and Activity (Bericht und Aktivität)** des ACS angezeigt wird.

Diese Fehlermeldung wird möglicherweise angezeigt, wenn Microsoft Windows XP SP2 auf dem Client-Computer installiert ist und sich Windows XP SP2 gegenüber einem anderen Server als einem Microsoft IAS-Server authentifiziert. Insbesondere verwendet der Cisco RADIUS-Server (ACS) zur Berechnung der EAP-TLV-ID (Extensible Authentication Protocol Type:Length:Value Format) eine andere Methode als Windows XP. Microsoft hat dies als einen Fehler in der XP SP2-

Komponente identifiziert.

Wenden Sie sich für einen Hotfix an Microsoft, und lesen Sie den Artikel [PEAP authentication is not successfully when you connect to a third party RADIUS server](#) . Das zugrunde liegende Problem besteht darin, dass auf der Client-Seite mit Windows Utility die Option für die schnelle Wiederverbindung für PEAP standardmäßig deaktiviert ist. Diese Option ist jedoch auf der Serverseite (ACS) standardmäßig aktiviert. Um dieses Problem zu beheben, deaktivieren Sie die Option "Fast Reconnect" auf dem ACS-Server (unter "Global System Options" (Globale Systemoptionen)). Alternativ können Sie auf der Client-Seite die Option für die schnelle Wiederherstellung aktivieren, um das Problem zu beheben.

Führen Sie die folgenden Schritte aus, um die schnelle Wiederherstellung auf dem Client zu aktivieren, der Windows XP mit dem Windows-Dienstprogramm ausführt:

1. Gehen Sie zu **Start > Einstellungen > Systemsteuerung**.
2. Doppelklicken Sie auf das Symbol **Netzwerkverbindungen**.
3. Klicken Sie mit der rechten Maustaste auf das Symbol **Drahtlose Netzwerkverbindung**, und klicken Sie dann auf **Eigenschaften**.
4. Klicken Sie auf die Registerkarte **Drahtlose Netzwerke**.
5. Wählen Sie die Option **Drahtlosnetzwerkeinstellungen für Windows verwenden** aus, um Windows für die Konfiguration des Client-Adapters zu aktivieren.
6. Wenn Sie bereits eine SSID konfiguriert haben, wählen Sie die SSID aus, und klicken Sie auf **Eigenschaften**. Falls nicht, klicken Sie auf **Neu**, um ein neues WLAN hinzuzufügen.
7. Geben Sie auf der Registerkarte "Association" (Zuordnung) die SSID ein. Stellen Sie sicher, dass die Netzwerkauthentifizierung **offen** ist und die Datenverschlüsselung auf **WEP** festgelegt ist.
8. Klicken Sie auf **Authentifizierung**.
9. Wählen Sie die Option **IEEE 802.1x-Authentifizierung für dieses Netzwerk aktivieren**.
10. Wählen Sie **PEAP** als EAP-Typ aus, und klicken Sie auf **Eigenschaften**.
11. Wählen Sie unten auf der Seite die Option **"Schnelle Wiederverbindung aktivieren"** aus.

[Zugehörige Informationen](#)

- [PEAP unter Unified Wireless Networks mit ACS 4.0 und Windows 2003](#)
- [Konfigurationsbeispiel für Cisco Wireless LAN Controller \(WLC\) und Cisco ACS 5.x \(TACACS+\) für die Webauthentifizierung](#)
- [Installations- und Upgrade-Handbuch für das Cisco Secure Access Control System 5.1](#)
- [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.