# 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 <u>Microsoft Wi-Fi-Website</u> und im <u>Cisco SAFE Wireless Blueprint</u>.

## 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 <u>Schnellstartanleitung: Cisco Wireless LAN Controller der Serie 4400</u>. Informationen zur Erstinstallation und Konfiguration der Cisco Controller der Serie 2000 finden Sie in der <u>Schnellstartanleitung: Cisco Wireless LAN Controller der Serie 2000</u>.

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 <u>EAP-TLS-Authentifizierung</u> 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

#### **Netzwerkdiagramm**

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 <u>WPA2/Wireless Provisioning Services Information Element (WPS IE)-Update für Windows XP mit SP2</u>.

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 <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

## <u>Windows Enterprise 2003-Setup mit IIS, Certificate Authority,</u> <u>DNS, DHCP (DC\_CA)</u>

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

- 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**.

e Directory Installation Wizard		×
<b>) atabase and Log Folders</b> Specify the folders to contain the Active Di	irectory database and log file	». <b>É</b>
For best performance and recoverability, sta hard disks.	ore the database and the log	g on separate
Where do you want to store the Active Dire	ectory database?	
<u>D</u> atabase folder:		
C:\WINDOWS\NTDS		B <u>r</u> owse
Where do you want to store the Active Dire Log folder: C:\WINDOWS\NTDS	ectory log?	Br <u>o</u> wse
	< <u>B</u> ack <u>N</u> ext:	> Cancel

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

Active Directory Installation Wizard
Specify the folder to be shared as the system volume.
The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.
The SYSVOL folder must be located on an NTFS volume.
Enter a location for the SYSVOL folder.
Eolder location:
C:\WINDOWS\SYSVOL Browse
< <u>B</u> ack <u>N</u> ext> Cancel

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 aufWeiter.

Active Directory Installation Wizard
Permissions Select default permissions for user and group objects.
Some server programs, such as Windows NT Remote Access Service, read information stored on domain controllers.
Permissions compatible with pre-Windows 2000 server operating systems
Select this option if you run server programs on pre-Windows 2000 server operating systems or on Windows 2000 or Windows Server 2003 operating systems that are members of pre-Windows 2000 domains.
\Lambda Anonymous users can read information on this domain.
Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems
Select this option if you run server programs only on Windows 2000 or Windows Server 2003 operating systems that are members of Active Directory domains. Only authenticated users can read information on this domain.
≺ <u>B</u> ack <u>N</u> ext≻ Cancel

- 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**.

un	nmary Beview and confirm the options you selected
	You chose to:
	The new domain name is example.com. This is also the name of the new forest.
	The NetBIOS name of the domain is EXAMPLE
	Database folder: C:\WINDOWS\NTDS
	Log file folder: C:\WINDOWS\NTDS SYSVDL folder: C:\WINDOWS\SYSVDL
	The DNC contine will be installed and configured on this consister. This consister
	will be configured to use this DNS server as its preferred DNS server.
	The password of the new domain administrator will be the same as the password of
	the administrator of this computer.
	To change an option, click Back. To begin the operation, click Next.
	< Back Next> Canc

- 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

- 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



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

#### Schritt 4: Installieren und Konfigurieren von DHCP

- 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.
- 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 Willkommensseite 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 prov providing a descr	ride an identifying scope name. You also have the option of iption,	(C)
Type a name and how the scope is	description for this scope. This information helps you quickly id to be used on your network.	lentify
N <u>a</u> me:	CorpNet	
Description:		
	≺ <u>B</u> ack <u>N</u> ext>	Cancel

7. Klicken Sie auf **Weiter**, und füllen Sie die folgenden Parameter aus:Start-IP-Adresse -172.16.100.1End IP address (Endadresse): 172.16.100.254Länge: 24Subnetzmaske: 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. <u>Start IP address</u> : 172 . 16 . 100 . 1 <u>End IP address</u> : 172 . 16 . 100 . 254 A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address
Length: 24
< <u>B</u> ack <u>N</u> ext ≻ 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.

#### Add Exclusions

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



Type the IP address rang address, type an address	e that you want to exclude. in Start IP address only.	lf you want to exc	lude a single
<u>S</u> tart IP address: 172 . 16 . 100 . 1	End IP address:	Add	
Excluded address range:			
		Remo <u>v</u> e	
	< <u>B</u> (	ack <u>N</u> ext :	> Cancel

9. Klicken Sie auf der Seite Leasingdauer auf Weiter.

 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
< <u>Back</u> <u>N</u> ext>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.



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	Wizar	ď
--	-----	-------	-------	---

#### **Domain Name and DNS Servers**

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



117 C T	
se DNS servers on your network, enter th	he IP addresses for thos
I <u>P</u> address:	
	Add
Resolve 172.16.100.26	Bemove
	Up
	Down
	e DNS servers on your network, enter the IP address:

- 13. Klicken Sie auf der Seite WINS-Server auf Weiter.
- 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).

New Scope Wizard
Activate Scope Clients can obtain address leases only if a scope is activated.
Do you want to activate this scope now? ⊙ Yes, I want to activate this scope now
No, I will activate this scope later
< <u>B</u> ack <u>N</u> ext> Cancel

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**.

You can add or remove components of Windows.	
To add or remove a component, click the checkbox. A sharpart of the component will be installed. To see what's includ Details.	ded box means that only ed in a component, click
Components:	
🗹 📻 Accessories and Utilities	4.9 MB 🔺
Application Server	33.4 MB 💻
🗹 🙋 Certificate Services	1.4 MB
🔲 💻 E-mail Services	1.1 MB
🗖 🚳 Eax Services	7.9 MB 🗾
Description: Installs a certification authority (CA) to issue ce public key security programs. Total disk space required: 3.4 MB	rtificates for use with Details
Space available on disk: 1346.9 MB	

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

(Weiter).

Windows Components Wizard	×
CA Type Select the type of CA you want to set up.	Ì
Enterprise root CA.	
C Enterprise subordinate CA	
C <u>S</u> tand-alone root CA	
C Stand-alone subordinate CA	
Description of CA type The most trusted CA in an enterprise. Should be installed before any other CA.	
Use custom settings to generate the key pair and CA certificate	
< <u>B</u> ack <u>Next</u> > Cancel He	þ

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.

ndows Components Wizard	
Certificate Database Settings Enter locations for the certificate database, database log, and config information.	uration
<u>C</u> ertificate database:	
C:\WIND0WS\system32\CertLog	Browse
Certificate database log:	
C:\WINDOWS\system32\CertLog	Bro <u>w</u> se
Store configuration information in a shared folder Shared folder:	1
	Browse
Preserve existing certificate database	
< <u>B</u> ack <u>N</u> ext > Can	cel Help

- 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

- 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 verwaltenCA verwaltenZertifikate anfordernWenn eine dieser Optionen auf Verweigern festgelegt ist oder nicht ausgewählt ist, legen Sie die Berechtigung auf Zulassen fest.

relessdemoca Properties		?
General   Policy Module   Exit Mo Certificate Managers Restrictions   Audit	idule   Extension ing   Recovery Ag	ns Storage gents Security
Group or user names:		
Administrators (WIRELESSDEMOV	Administrators)	
Authenticated Users		
🛛 🕵 Domain Admins (WIRELESSDEMO	ND omain Admins)	
🛛 🕵 Enterprise Admins (WIRELESSDEN	10\Enterprise Admi	ins)
2	Add	Remove
Permissions for Administrators	Allow.	Deny
Read	<u> </u>	
Issue and Manage Certificates		
Manage LA		
Hequest Lertificates	M	L.
οκ	Cancel	1 Apply

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 <u>Benutzer zur</u> <u>Domäne hinzufügen fort</u>.

- 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.

 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.

Create in:       wirelessdemo.local/Users         Computer name:	ew Object - Computer	X
Computer name:         Client         Computer name (gre-Windows 2000):         CLIENT         The following user or group can join this computer to a domain.         User or group:         Default: Domain Admins         Change         Assign this computer account as a pre-Windows 2000 computer         Assign this computer account as a backup domain controller	Create in: wirelessdemo.local/Users	
Client         Computer name (gre-Windows 2000):         CLIENT         The following user or group can join this computer to a domain.         User or group:         Default: Domain Admins         Change         Assign this computer account as a pre-Windows 2000 computer         Assign this computer account as a backup domain controller	Computer name:	
Computer name (gre-Windows 2000): CLIENT The following user or group can join this computer to a domain. User or group: Default: Domain Adminshange Assign this computer account as a pre-Windows 2000 computer Assign this computer account as a backup domain controller	Client	
CLIENT         The following user or group can join this computer to a domain.         User or group:         Default: Domain Admins         Change         Assign this computer account as a pre-Windows 2000 computer         Assign this computer account as a backup domain controller	Computer name (pre-Windows 2000):	
The following user or group can join this computer to a domain. User or group: Default: Domain Admins Change Assign this computer account as a pre-Windows 2000 computer Assign this computer account as a backup domain controller	CLIENT	
User or group:         Default: Domain Admins         Change         Assign this computer account as a pre-Windows 2000 computer         Assign this computer account as a backup domain controller	The following user or group can join this computer to a domain	
Default: Domain Admins       Change         Assign this computer account as a pre-Windows 2000 computer         Assign this computer account as a backup domain controller	User or aroup:	
Assign this computer account as a pre-Windows 2000 computer Assign this computer account as a backup domain controller	Default: Domain Admins <u>Change</u>	
Assign this computer account as a backup domain controller	Assign this computer account as a pre-Windows 2000 computer	
	Assign this computer account as a pre-windows 2000 computer	
	Assign this computer account as a backup domain controller	
< <u>B</u> ack <u>N</u> ext > Cancel	< <u>B</u> ack <u>N</u> ext > Car	ncel

- 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

- 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**.
- 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.

w Object - User		
Create	in: wirelessdemo.local/Users	
<u>F</u> irst name:	WirelessUser <u>I</u> nitials:	
Last name:		
Full name:	WirelessUser	
<u>U</u> ser logon name:		
WirelessUser	@wirelessdemo.local 💌	
User logon name (j	pre- <u>W</u> indows 2000):	
WIRELESSDEMO	) \ WirelessUser	
	Z Rack Neut S	ancel
		ancer

 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.

wobject - oser		
Create in: wirele	essdemo.local/Users	
<u>P</u> assword:	****	
<u>C</u> onfirm password:	••••	
🔲 User <u>m</u> ust change passw	ord at next logon	
User cannot change pass	word	
Pass <u>w</u> ord never expires		
Account is disabled		
	< <u>B</u> ack <u>N</u> ext	> 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:

- 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

- 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**.
- 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

erwendet.	
lew Object - Group	×
Create in: wireles:	sdemo.local/Users
Group n <u>a</u> me:	
WirelessUsers	
Group name (pre- <u>W</u> indows 2000	י):
WirelessUsers	
Group scope	Group type
🔿 D <u>o</u> main local	💿 Security
💿 Global	C Distribution
C Universal	
	<b>_</b> ,
	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.

Select Users, Contacts, Computers, or Groups	? X
<u>S</u> elect this object type:	
Users, Groups, or Other objects	<u>O</u> bject Types
From this location:	
wirelessdemo.local	Locations
Enter the object names to select ( <u>examples</u> ):	
wirelessuser	<u>C</u> heck Names
<u>A</u> dvanced OK	Cancel

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

WirelessUsers Prope	rties	? ×
General Members	Member Of L Managed By ]	
<u>M</u> embers:	1	
Name	Active Directory Folder	
22 Administrator	wirelessdemo.local/Users	
🙎 WirelessUser	wirelessdemo.local/Users	
<u>Add</u>	<u>R</u> emove	
	OK Cancel	

- 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

- 1. Wiederholen Sie die Schritte 1 und 2 im Abschnitt <u>Benutzer zur Wireless-Benutzergruppe</u> <u>hinzufügen</u> in diesem Dokument.
- 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.

Select Users, Contacts, Computers, or Groups	? ×
<u>S</u> elect this object type:	
Users, Groups, or Other objects	<u>O</u> bject Types
Erom this location:	
wirelessdemo.local	Locations
Enter the object names to select ( <u>examples</u> ):	
client	<u>C</u> heck Names
Advanced OK	Cancel

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

Computer.		
Object Types	? 3	×
Select the types of objects you want to find.		
Object types:		
🔽 🐗 Other objects		1
Contacts		
🔽 🔜 Computers		
🗖 🗖 🛃 Users		
	Cancel	

- 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:

- 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 <u>Installationshandbuch für Cisco Secure ACS 4.0 für Windows.</u>

- 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" (Wählberechtigung 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" (Wählberechtigung 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 <u>Benutzerhandbuch für Cisco Secure ACS für Windows Server,</u> <u>Version 4.0</u>.**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





- 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).
- Konfigurieren Sie die Informationen so, wie diese Schnittstellen > Fenster Bearbeiten angezeigt werden.

ISAA Sverrus		
allin, allin,	MONITOR WUANS CONTR	ROLLER WIRELESS SECURITY
Controller	Interfaces > Edit	
General		
Inventory	General Information	
Interfaces	Interface Name er	mployee
Internal DHCP Server	Tutouface televise	
Mobility Management Mobility Groups Mobility Statistics	VLAN Icentifier	20
Ports	IP Address	172.16.100.4
Master Controller Mode	Netmask	255.255.255.0
Network Time Protocol	Gatoway	172.16.100.1
QoS Profiles	Physical Information	
	Port Number	1
	DHCP Information	
	Primary DHCP Server	172.16.100.25
	Secondary DHCP Server	0.0.0
	Access Control List	
	ACL Name	поте 💙

- 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 LD	1		
WLAN 5510	Employee		
<b>Ceneral Policies</b>		Security Policies	
Radio Policy		Line of Sciencilia	W262
Admin Status	Enabled	El Yor 2 Sebundy	MAC Eltorioa
Session Timeout (secs)	1830		
Quality of Service (QoB)	Silvor (best offort)	Layer 3 Security	Моге 💌
WMM Policy	Disabled 🛩		Web Policy "
7920 P Ione Support	🔲 Client CAC Limit 🔄 🗛 CAC Limit		
Broaccast SSID	🕝 Enabled	NR 29 of a bill (15 of a Second Mark 5 (5 of a bill)	
Allow AAA Override	🔲 Enabled	* Web Policy cannot b and L2TP.	e used in combination with IPsec
Client Exclusion	Enabled ** 60 Timeout Value (secs)	** When plicht exclusi zero means infinity (wi	on is enabled, a timpout value of Il require acministrative override t
DHCP Server	Overrido 🗌	reset excluded clients)	
DI CP Addr. Assignment	Required		
Interface Name	emplayee 💌		
Radius Servers			
	Authentication Servers Accounting Servers		
Server 1	TP:172.16.100.25, Port:1812 💙 none 💙		
Server 2	rone 💌 none 🔽		
Server 3	rone 🕑 none 🧹		
WPA2 Parameters			
WPA Compatibility Mode	Encble		
Allow WPA2 TKIF Clients	🖉 Enable		
Pre-Shared Key	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).

Address 🔄 https://172.16.101.252/screens/frameset.html

CISCO SYSTEMS				
adha adha	MONITOR WLANS (	CONTROLLER	WIRELESS	SECURITY
Security	RADIUS Authentication	on Servers >!	New	
AAA General	Server Index (Priorit	ty) 1	1	
RADIUS Authentication RADIUS Accounting Local Net Users	Server IPAddress	172.1	16.100.25	
MAC Filtering Disabled Clients	Keys Format	ASC	II <b>v</b>	
AP Policies	Shared Secret	••••	••	
Access Control Lists Web Auth Certificate	Confirm Shared Secret	••••	••	
Wireless Protection Policies	Key Wrap			
Rogue Policies Standard Signatures	Port Number	1812		
Custom Signatures Client Exclusion Policies AP Authentication	Server Status	Enab	led 💙	
	Support for RFC 357	6 Enab	led ⊻	
	Retransmit Timeout	2	seconds	
	Network User	<b>I</b> E	inable	
	Management	E 6	nable	



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.

Certificate Templates	Template Display Name 🧭	Minimum Supported CAs	Version	Autoenrolinent
	Stepsist EFS	Windows 2000	3.1	Not allowed
	CA Exchange	Windows Server 2003, En	106 0	Not allowed
	CEP Encryption	Windows 2000	4.1	Vot allowed
	Code Signing	Winduws 2000	3.1	Not allowed
	Computer	Windows 2000	5.1	Not allowed
	Cross Certification Authority	Windows Server 2003, En	105 0	Not allowed
	R DEMOACS	Windows Server 2000, En	100.2	Not sllowed
	Directory Email Replication	Windows Server 2003, Fn	1:50	Allowed
	Domain Controler	Windows 2000	4.1	Not allowed
	Domain Controlor Authencication	Windows Server 2003, En	1:00	Allowed
	EFS Recovery Agent	Windows 2000	6.1	Not allowed
	Euroline it Agent	Winduws 2000	4.1	Not allowed
	Enrollment Agent (Computer)	Windows 2000	5.1	Vot allowed
	Exchange Enrolment Agent (Offline request)	Windows 2000	4.1	Vot allowed
	Exchange Signature Only	Windows 2000	6.1	Not allowed
	Exchange laer	Windows 2000	7.1	Not allowed
	C C C C C C C C C C C C C C C C C C C	Windows 2000	8.1	Not allowed
	IPSec (Offine reques:)	Windows 2000	7.1	Not allowed
	Key Recovery Acent	Windows Server 2003, En	105 0	Allowed
	RAS and IAS Server	Windows Server 2003, En	101 0	Allowed
	Roo: Certification Authority	Windows 2000	5.1	Vot allowed
	Router (Offline request)	Wincows 2000	4.1	Not allowed
	Smartcard Logon	Wincows 2000	6.1	Not allowed
	Smartcard User	Wincows 2000	11.1	Not allowed
	Subordinate Certification Authority	Wincows 2000	5.1	Not allowed
	Trust List Signing	Wincows 2000	3.1	Not allowed
	GodUser	Wincows 2000	3.1	Not allowed
	Bellser Signature Only	Wincows 2000	4.1	Not allowed
	Big Wigh Sarvar	Winnews 2000	4.1	Not allowed
	Win Dypicate Templa:e	Whicows Server 2003, En	1.0.3	Alowed
	Wi al Lasks   late	Wincows Server 2003, En	101.0	Allowed
		Wincows Server 2003, Fn	101:0	Alowed
	Properties			

### Erstellen der Zertifikatsvorlage für den ACS-Webserver

- 1. Klicken Sie im Detailbereich des Snap-Ins Zertifikatvorlagen auf die Webserver-Vorlage.
- 2. Klicken Sie im Menü Aktion auf Vorlage duplizieren.
| operties of New Te  | nplate  |                                  | ?               |
|---|---|----------------------------------|-----------------|
| Issuance Requiremen<br>General  | ts   Superseded Template:<br>Request Handling | s   Extensions  <br>  Subject Na | Security<br>ame |
| Template display nan  | ne:   |                                  |                 |
| Copy of Web Server  |   |                                  |                 |
| Minimum Supported (   | CAs: Windows Server 2003                      | , Enterprise Edition             |                 |
| After you apply chan, name.   | ges to this tab, you can no lo                | nger change the te               | emplate         |
| Template name:  |   |                                  |                 |
| Copy of Web Server  | e)  |                                  |                 |
| Validity period:<br>2 years<br>Publish certificate<br>Do not autom<br>Directory | Enewal perions<br>6 wee                       | od:<br>ks 💽                      | Active          |
|   |   |                                  |                 |

3. Geben Sie im Feld Name der Vorlagenanzeige ACS

percies of new	Template	
ssuance Requiren	nents   Superseded Templates   Extensio	ons   Secu
General	Request Handling Sub	ject Name
Template display i	name:	
ACSI		
After you apply ch name. Template name:	nanges to this tab, you can no longer change	e the templat
March 1		
ACS		
ACS	Benewal period: 6 weeks •	rists in Artic

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

Eurpose: Minimum key siz ☑ Allow private Do the following	Signature and encr Archive subject's Include symmetr Delete revoked of e: 1024	vption s encryption priva ic algorithms allo or expired certific	te key wed by the subject ates (do not archive)
Minimum key siz ☑ All <u>o</u> w private Do the following	Archive subject's Include symmetr Delete revoked Include symmetr Include symmetr Include symmetr Include symmetr Include symmetries Include symmet	s encryption priva ic algorithms allo or expired certific	ate key wed by the subject ates (do not archive)
<u>M</u> inimum key siz ☑ All <u>o</u> w private Do the following	<ul> <li>Include symmetric</li> <li>Delete revoked of</li> <li>e: 1024 </li> <li>key to be exported</li> </ul>	ic algorithms allow or expired certific	wed by the subject ates (do not archive)
Minimum key siz ☑ All <u>o</u> w private Do the following	Delete revoked      1024      key to be exported	or expired certific	ates (do not archive)
Minimum key siz	e: 1024		
Do the following	key to be exported		
Do the following	Rey to be exported		
Do the following			
associated with	when the subject is a this certificate is used	enrolled and whe	n the private key
C Enroll subject	t without requiring an	y user input	
C Prompt the c	iser during enrollment		
C Prompt the private key i	iser during enrollment s used	and require user	input when the
To choose whic (CSPs) should b	h cryptographic servi e used, click CSPs.	ce providers	<u>C</u> SPs

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

Issuance Requirements   Superseded Templates	Extensions Securit
General Request Handling	Subject Name
SP Selection	?)
Choose which cryptographic service providers (C9 requests:	iPs) can be used in
$\odot$ Bequests can use any CSP available on the s	ubject's computer
Requests must use one of the following CSPs:	
ГсР <sub>*</sub>	
<ul> <li>Microsoft Base Cryptographic Provider v1.0</li> <li>Microsoft Base DSS and Diffie-Hellman Cryptog</li> <li>Microsoft DH SChannel Cryptographic Provider v1</li> <li>Microsoft Enhanced Cryptographic Provider v1</li> <li>Microsoft Enhanced DSS and Diffie-Hellman C</li> <li>Microsoft Enhanced RSA and AES Cryptographic Provider</li> <li>Microsoft BSA SChannel Cryptographic Provider</li> </ul>	graphic Provider .0 ryptographic Prov hic Provider er
OK	Cancel
OK.   C	

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

<ul> <li>Gene</li> <li>Suppl</li> <li>Select</li> <li>Select</li> <li>Simplify</li> <li>Subject</li> </ul>	ai in the reque this option to ve access to nrollment is n rom this Activ his option to certificate ac	o allow a vari o the domain ot allowed if ve Directory in enforce cons fministration	andling of which the s you choose th nformation	name formats ubject is a me is option. g subject nam	or if you do ember.
<ul> <li>Suppl Select not hat Autoe</li> <li>Build I Select simplify</li> <li>Subject</li> </ul>	in the reque this option to we access to nrollment is n rom this Activ his option to certificate ac	o allow a vari o the domain ot allowed if ; ve Directory in enforce cons fministration	ety of subject of which the s you choose th nformation	name formats subject is a me is option. g subject nam	or if you do ember.
C <u>B</u> uild I Select simplify Subjec	rom this Activ his option to certificate ac	ve Directory in enforce cons Iministration	nformation — sistency amon	g subject nam	
Select simplify Subjec	his option to certificate ac	enforce cons Iministration.	sistency amon	g subject nam	1000000000000
Subjec					ies and to
	name forma	to			
None					3
,∏ jno	ude e-mail na	ame in subjec	st name		
Include	this informat	ion in alterna	te subject nan	ne:	
E-n	ail name				
	S name				
	er prinicipal n	ame (UPN)			
☐ Se	vice principa	I name (SPN)	R		

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

General Request Har	ndling   S	ubject Name
Issuance Requirements 📔 Superseded	d Templates   Exter	nsions Security
<u>G</u> roup or user names:		
🖸 Administrator (WIRELESSDEMO	VAdministrator)	
🕵 Authenticated Users		
🗊 Domain Admins (WIRELESSDEN	10/Domain Admins)	
🕼 🕵 Enterprise Admins (WIRELESSD	EMO\Enterprise Adr	nins)
	A <u>d</u> d	<u>R</u> emove
Permissions for Domain Admins	A <u>d</u> d	<u>R</u> emove
Permissions for Domain Admins	A <u>d</u> d Allow	<u>R</u> emove Deny
Permissions for Domain Admins	A <u>d</u> d Allow	<u>R</u> emove Deny
Permissions for Domain Admins Full Control Read	Add Allow	Remove Deny
Permissions for Domain Admins Full Control Read Write	Add Allow	Remove Deny
Permissions for Domain Admins Full Control Read Write Enroll	Add Allow I I I I I I I I I I I I I I I I I I I	Remove Deny
Permissions for Domain Admins Full Control Read Write Enroll Autoenroll	Add Allow V V V	Remove Deny
Permissions for Domain Admins Full Control Read Write Enroll Autoenroll	Add Allow V V V	Remove Deny
Eermissions for Domain Admins Full Control Read Write Enroll Autoenroll For special permissions or for advance	A <u>d</u> d Allow ☑ ☑ ☑ ☑	Remove Deny
Eermissions for Domain Admins Full Control Read Write Enroll Autoenroll For special permissions or for advance click Advanced.	A <u>d</u> d Allow V V d settings,	Remove Deny

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.

General	Request Handling	Subject Name
Issuance Requireme	nts Superseded Templates	Extensions Security
Bequire the followin	tor enrollment:	
CA certificate m	anager approval	
This number of a	authorized signatures:	
If you require m	ore than one signature, autoer	nrollment is not allowed.
Policy type requ	red in signature:	
1		7
Application polic	9.	
l		<u> </u>
Issuance policie	S.	- 1 444 1
		Agg
		<u>B</u> emove
		4
Require the followin	g for reenrollment:	
🙆 Same criteria as	for enrollment	
C Valid existing ce	rtificate	

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:

 Öffnen Sie das Snap-In der Zertifizierungsstelle. Befolgen Sie die Schritte 1-3 im Abschnitt <u>Erstellen der Zertifikatsvorlage f
 ür den ACS-Webserver</u>, w
 w
 ählen Sie die Option Certificate Authority (Zertifizierungsstelle) aus, w
 ählen Sie Local Computer (Lokaler Computer) aus, und klicken Sie auf Beenden.

Certification Authority		×
Select the computer you war This snap-in will always ma I Local computer: [the I Another computer:	nt this snap-in to manage. nage: computer this console is running on) Browse	]
Allow the selected co only applies if you sav	mputer to be changed when launching from the command line. This re the console.	
	< <u>B</u> ack Finish Cance	el

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

= → 🗈 💽	F 🛱 🛛 😭	cal))wirelessdemocal/Certificate Tem	lates
Console Root	n Authority (Local) sidemoca volved Certificates ued Certificates iding Requests ed Requests Manage <u>Vew</u> Vew Window from Here Vew Taskpad View Refresh Export List Help	Name Wireless Liser Certificare Template Diractory Email Replication Domain Controller Authentication Domain Controller Web Server Certificate Template to Issue Subordinate Certification Authority Administrator	Intended Purpose Client A ithentication, Serure Email, Eprity, Directory Service Email Replication Client Authentication, Server Authentication - File Recovery Encrypting File System Client Authentication, Server Authentication Server Authentication, Server Authentication Client Authentication, Server Authentication Encrypting File System, Secure Email, Clien <all> Nicrosoft Trust List Sgning, Encrypting File</all>
			<u></u>

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

#### Enable Certificate Templates

Select one or more Certificate Templates to enable on this Certification Authority

Name	Intended Purpose	-
ACS .	Server Authentication	
Authenticated Session	Client Authentication	
🙀 CA Exchange	Private Key Archival	
CEP Encryption	Certificate Request Agent	
😹 Code Signing	Code Signing	
Cross Certification Authority	KAID	
DEMOACS	Server Authentication	
Enrolment Agent	Certificate Request Agent	
🗱 Enrolment Agent (Computer)	Certificate Request Agent	
Exchange Enrollment Agent (Offline request)	Certificate Request Agent	
Exchange Signature Only	Secure Email	5

- 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.

? X



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

relessdemo.loc	al Properties			?
General Manage	d By Group Po	licy		
To improve Grou Management Co	p Policy managel nsole (GPMC). ent Group Policy	ment <mark>upgrade</mark> ) Object Links fo	to the Group Pr r wirelessdemo	olicy
Group Policy O	bject Links	1	No Override	Disabled
Group Policy Obj This list obtained <u>N</u> ew	ects higher in the from: cisco_w20 	e list have the hi 103.wirelessdem <u>E</u> dit	ighest priority. io.local	Ųр
Options	Dele <u>t</u> e	Properties		Do <u>w</u> n
Block Policy	inheritance			
		OK	Cancel	Apply

 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.

🚡 Group Policy Object Editor			
File Action <u>V</u> iew <u>H</u> elp			
← → 💽 💽 🛃 🛃 🔮			
Default Domain Policy [cisco_w2003,wirel	lessdemo.local]	Policy	Automatic Certificate Request 🔺
<ul> <li>Sortware Settings</li> <li>Windows Settings</li> <li>Scripts (Startup/Shutdown)</li> <li>Security Settings</li> <li>Settings</li> <li>Settings</li> <li>Settings</li> <li>Settings</li> <li>Settings</li> <li>Settings</li> <li>Setings</li> <li>Settings</li> <li>Settings</li> <li< td=""><td>i02,11) Policies</td><td></td><td></td></li<></ul>	i02,11) Policies		
Automatic Certificat	n new		Automatic Certificate Request
Trusted Root Certif	View	,1	
🖅 🚞 Software Restriction Po -	TICON	_	
<ul> <li>IP Security Policies on A</li> <li>Administrative Templates</li> </ul>	Retresh Export List	:: 	
<ul> <li>Windows Settings</li> </ul>	Help		
🗄 🛄 Administrative Templates			ļ

- 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**.

A certificate template is a set of pre	defined properties for certificates issued to the following list			
Certificate templates:	rie rollowing list.			
Name Intended Purposes				
Computer Domain Controller Enrollment Agent (Computer) IPSec	Client Authentication, Server Authenticatio Client Authentication, Server Authenticatio Certificate Request Agent IP security IKE intermediate			
•	<u> </u>			

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.

Group Policy Object Editor	
<u>File Action View Help</u>	
<ul> <li>Default Domain Policy [cisco_w2003.wirelessdemo.local] Policy</li> <li>Computer Configuration</li> <li>Software Settings</li> <li>Windows Settings</li> <li>Scripts (Startup/Shutdown)</li> <li>Security Settings</li> <li>Scolar Policies</li> <li>Event Log</li> <li>Restricted Groups</li> <li>System Services</li> <li>System Services</li> <li>System Services</li> <li>Signature Setting</li> <li>System Services</li> <li>System Services</li> <li>System Services</li> <li>Substantiation</li> <li>System Services</li> <li>System Services</li> <li>Substantiation</li> <li>Substantiation</li> <li>Substantiation</li> </ul>	Automatic Certificate Request
i Encrypting File System Automatic Certificate Request Settings I Trusted Root Certification Authorities I Enterprise Trust	

 Erweitern Sie in der Konsolenstruktur Benutzerkonfiguration > Windows-Einstellungen > Sicherheitseinstellungen > Richtlinien f
ür öffentlichen Schl
üssel.



- 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 widerrufene Zertifikate und Zertifikate mit Zertifikatsvorlagen

#### entfernen.

Autoenrollment Settings Properties
General
Enroll user and computer certificates automatically
<ul> <li><u>D</u>o not enroll certificates automatically</li> <li><u>E</u>nroll certificates automatically</li> </ul>
Renew expired certificates, update pending certificates, and remove revoked certificates
Update certificates that use certificate templates
OK Cancel Apply

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.
- 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



Microsoft Certificate Services -- wirelessdemoca

#### **Request a Certificate**

Select the certificate type: User Certificate

Or, submit an advanced certificate request.

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



Wels, You must have an excellence regard commons to a conduct on here the and another use

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

#### hak

ck - 🏐 - 1	🖭 🖹 🏠 🔎 Search 🔅 -avancas 🤣 😥 - 🚡 🔜
ss 👩 http://1	172,16,120,25)certs:v/certruma,asp
crosofi (am)	feste Sevices – wienessten zu
dvanced Co	ertificate Request
ertificate Lem	iplate:
	Administrator
	Apprinterator
ey Options:	Dasic EF3
	En S Recovery Ager : makey set
C S D	W releas User Car ficate Template
SOF.	4-01-71-1 M
Μεγ Οβορθ	Subordinate Certification Authority
Key Site	,   West Sie wet   10 = Max 15884 (***********************************
	• Automatic key container name • O User specified key container name
	💌 Mark keys as expendible
	🗖 Ехэрл: кауз to file
	🗖 Enable shung private key protection
	□ Etore certificate in the Incal complicate store
	Stores the certificate in the local computer store
	instand of it the user's certificate store. Does not
	instell the root CA's cendicate. You must be an
	administrator to generare ocuae a vey in the local machice store.
MERCE AND	
iaidunai Opu	
eddest Format	COVE CARESTJ
lash Alcorithm	6 BI A-1 💌
	Only used to sign request.
	🗖 Save request to all te
Atticuted	
	4
Friendly Name	
	Submit s
	Coome >

- 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

🕒 Deck 🔹 🕥 🗠 🛛	👔 😰 🐔 🔎 Search 🔹 Pavortes 🛷 🔝 💀 💀
lalah essi 🔊 hitipi (11)	72.16.100.26(certsry/certropia.asp
Certificate Tem	elate:
	A/S .
ldentilying Infor	mation For Offline Template:
Name:	cisco_w2009.wirelessdemo.locel
E-Mail:	
Company:	
Department:	
City:	
State:	
Country/Region:	
Kas Ontinan	
Ney Options:	Contract Cities within her est
CCD.	Visate new key set
Key Hosen:	Encloser Base Cryptographic Provider VI.D
Key Usage. Key Size:	** Exchange 10.24 Min.1024 Georgeneoleuristen 3778 h
neg size.	Mac1024 Mac1024
	Automatic key container name     O beer specified key container name
	Export keys to file
	Store certificate in the local computer certificate store
	Stores the certificate in the local computer store
	install the root CA's certificate. You must be an
	administrator to generate or use a key in the local mechine store
ALE: 1.8.2	- Constanting and MEM -
Additional Uptic	
request Format:	I CARCE OPRESTU
Hash Algorithm:	SHArt  Cole used to alon servest
	Reve connect to a file
Attributes:	×
Friendly Name:	

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



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

Eile	Edit	⊻iew	F <u>a</u> vorites	Tools	Help			
🗿 Ba	ack 👻	9 -	🖹 🖻 🐔		5earch	👷 Favorites	😸 🙆 🖏	

Microsoft Certificate Services -- wirelessdemoca

#### Certificate Issued

The certificate you requested was issued to you.



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

Ja.	
Potential	Scripting Violation
<u>^</u>	This Web site is adding one or more certificates to this computer. Allowing an unbrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data. Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.
	<u>Y</u> es <u>No</u>

12. Wenn Sie auf Ja klicken, wird das Zertifikat

	ilt Certifi	icate Servi	ices - Microso	oft Internet Co	plorei		
Fic soit	vich	Havonicos	loos Help				
🔵 Back 👻	9 - 1	🗵 🗷 🖉	🛓 🔎 pearch	👷 Havorites	🐵 🔝 -	2.1	
u_dress 🛓	http://l	72.16.10J.	∕t/certsr√/cert*	mpn.aso			
-							
Microse	off Certif	icate Serv	ices wirel	esstemada			
	nate In	stalled					
Certific	-alc III						
Certific	ale in						
Certific	over centi	ficate ba	a haar cur	-razef Mvi:	ctallo 1		
<b>Certific</b> Your ne	w certi	ficate ha	ie beer suc	ccessfully in	stalled		 
Certific Your ne	w certi	ficate ha	is beer suc	ccessfully i i	stalled		

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.

🚔 Mi	i rosoft Ferlificate Services - Microsoft Toternet Explorer	
De	Edit vien Favorites Ipols Llelo	
🙆 Ва	ack + 📀 - 📧 🧝 🐔 🔎 Search 🥠 =avortes 🧔 🙆 + 😓 🚍	
Acdro	pss 🧑 -ttp://172.10.100.26/certs/v/certoard asc	

Microsoff Ceptificate Genuces -- wrelesedemonal

#### Download a CA Certificate, Certificate Chain, or CRL

To trust cartificates issued from the certification authority install this CA cartificate chain.

To down date a CA cort ficate, certificate chain, or CRL isolate the certificate and encoding method.

CA certificate:

	Diment [wile esistemode]
ncoding metho	d:

C D\_R © <u>Beso 64</u> <u>Down cao CA certificate</u> <u>Down cao CA cortificate chain</u> Down cao latest base CRL <u>Down cao latest delta CRL</u>

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

File Downlo	oad - Security Warning 🛛 🗙
Do you	want to open or save this file?
	Name: certnew.cer Type: Security Certificate, 1.68 KB From: 172.16.100.26
•	Open       Save       Cancel         While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

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.

🚰 CiscoSecure ACS - Microsoft Internet Explorer									
Eile	<u>E</u> dit	⊻iew	F <u>a</u> vorites	Tools	Help			·	
🕝 В.	ack 🝷	Ð •	🗵 🗈 🤇	<u>م  </u>	5earch	☆ Favorites	•	🗟 🍕 📢	
Addre	ess 🥫	http://	127.0.0.1:3	809/					



8. Klicken Sie auf ACS Certificate Setup.

# System Configuration



10. Wählen Sie **Zertifikat aus Speicher verwenden** aus, und geben Sie den vollqualifizierten Domänennamen von **cisco\_w2003.wirelessdemo.local** (oder **ACS.wirelessdemo.local**, wenn Sie ACS als Namen verwenden)

Private key password



11. Klicken Sie auf

Senden.

## System Configuration

Edit

### Install ACS Certificate

?

Issued to:cisco\_w2003.wirelessdemo.localIssued by:wirelessdemocaValid from:March 17 2006 at 08:33:25Valid to:March 16 2008 at 08:33:25Validity: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
O None
⊙ Low
C Full
Generate New File
Every day
C Every week
O Every month
○ When size is greater than 2048 KB
Manage Directory
C Keep only the last 7 files
Delete files older than 7 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 Configuratio	un 🧖
PEAP	
□ Allow EAP-MSCHAPV2	
□ Allow EAP-GTC	
Allow Posture Validation	
Cisco client initial message:	
PEAP session timeout (minutes):	120
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):	120

- 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 A	uthority Setup		
CA Operation	าร	?	
Add new CA certificate to local certificate	storage		
CA certificate file	\acs.cer		
Stell Conigulation			
ACS Certification Authority Setup			
ACS Certification Authority Setup	New CA certificate is successully added i	into the global sys	tem certifica
ACS Certification Authority Setup  CA Operations  dd new C4 certificate to local certificate storage CA certificate file  c:\acs.cer	New CA certificate is successully added i storage CA certificate common name	into the global sys wireles	tem certifica

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".
- 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

ISI.			
🚡 Console 1			
Le Action Yew Levontes Window Leg	i.		
4 - 1 🗉 💼 🛱 🛱			
🚡 Console Root/Certificates - Corrent V	en Versonal Certificates		
📴 Cansole Root	Issued To	Essued By	Expiration Date D
Certificates - Current User 	WHe essLser	,//relesseemoca	3/22/2005 C

- 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

General	Wireless Networks	Advanc	Ed	
🛃 Use	Windows to configu	e ny wire	ess netwo	ork settings
Avail	able <u>n</u> elworks:			
To ca abou	onnect :o, disconnec! Il wileless retworks in	from, or f range.cli	nd out ma ck the bu	ore information Itton below.
		(	View Wi	reless Networks
Prefe Autor belov	ared nelworks: natically connect to a #:	vailable n	etwork.s ir	n lhe order li≎ted
Prefe Autor belov	ared nelworks: natically connect to a #:	vailable n	etwork.s ir	n lhe order listed Move <u>up</u> Move <u>d</u> owr
Prefe Autor belov	ared networks: natically connect to a «: <u>Add <u>R</u>emo</u>	vailable n	etworks ir	n lhe order listed Move <u>up</u> Move <u>d</u> owr

- 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

Association Authentic	ation Connection	
Network name (SSID)	: Enployee	
Wireless network ke	ey	
This betwork require	es a key for the following:	
Network Authentic:	ation: Open	~
Date encryption:	WEP	<b>~</b>
Network key:		
Confirm network ke	μ.	
Key index (edvance	ed), 1	
🔽 The key is provi	ded for me auromatically	
This is a computer access points are	-to-computer (ad hoc) network; win not used	eless

- 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 Anmeldeskripts oder Gruppenrichtlinien ermöglicht), wählen Sie die Option Als Computer authentifizieren, wenn Computerinformationen verfügbar

THE LESS THE	twork proper	ties	?
Association	Authenlica:ion	Connection	
Select this wireless Eth	option to provide nemel networks	authenticated retwork	access for
🗹 Enable I	IEEE 802.1x au:ł	ientication for this netwo	ork
EA <sup>D</sup> type:	Smart Card or c	ther Certhicate	
Aulhent	icate as compule	r when computer inform	ation s availa
Aulhent Aulhent	icate as compule icate as guest wł abe	r when computer inform	iation s availa

10. Klicken Sie auf Eigenschaften.

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

• vnen connec	ang		
U Jse my sn	art bard		
<ul> <li>Jse a cerl</li> </ul>	ficate on this computer	24 3.025	
M Jse si	nple certificate selection	Recommended]	
🗹 Validate se	ver certificate		
Connect	n these servers		
Connect (	0 (11636 3614618.		
Trusted Root	Certification Authorities:		
ABA.EC	DM Root CA		
ACS333			
ACS40			
📃 Autorda	d Certificadora de la Asoc	iac on Nacional (	cel Notaria
Autorda	d Certificadora del Colegii	n Nacional de Co	meduria Pu
Baltimore	F7 hy DST		
Belgado	m E-Trust Primary L'A		
L CaW HK	I SecureNet UA Llass A		
		View	Certficate
	5 A	100	

- 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.
- Klicken Sie auf das Wireless-Netzwerk Mitarbeiter und dann auf Verbinden.



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







- Nachdem die Authentifizierung erfolgreich war, überprüfen Sie die TCP/IP-Konfiguration f
  ür den Wireless-Adapter mithilfe von Netzwerkverbindungen. Der Adressbereich des DHCP-Bereichs bzw. des f
  ür die Wireless-Clients erstellten Bereichs sollte 172.16.100.100.100-172.16.100.254 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
- <u>Technischer Support und Dokumentation für Cisco Systeme</u>