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

Voraussetzungen

<u>Anforderungen</u>

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 <u>Installationshandbuch für Cisco Wireless Controller der Serie 5500</u>. Informationen zur Erstinstallation und -konfiguration der Cisco Controller der Serie 2100 finden Sie in der <u>Schnellstartanleitung: Cisco Wireless LAN Controller der Serie 2100</u>.

Microsoft Windows 2003 Installations- und Konfigurationsanleitungen finden Sie unter <u>Installieren</u> 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 <u>Cisco Technical Tips</u> <u>Conventions</u> (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 <u>Tool für die Suche nach Befehlen (nur registrierte Kunden), um</u> 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



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,

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

- 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-Domänennamen 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

ive Directory Installation Wizard	2
Database and Log Folders Specify the folders to contain the Active Directory database and log file	
For best performance and recoverability, store the database and the log hard disks.	g on separate
Where do you want to store the Active Directory database?	
Database folder:	
C:\windows\ntds	Bjowse
Where do you want to store the Active Directory log?	
C:\windows\ntds	Browse

Weiter.

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

Active Directory Installation Wizard
Shared System Volume Specify the folder to be shared as the system volume.
The SYSVDL folder stores the server's copy of the domain's public files. The contents of the SYSVDL 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:
CAWINDOWSASYSMOL Browse
< <u>B</u> ack <u>N</u> ext> Cancel

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

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.	1			
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.				
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> Can	cel			

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

Revie	w and confirm the options you selected.
You c	hose to:
The n	ew domain name is example.com. This is also the name of the new forest.
The N	etBIOS name of the domain is EXAMPLE
Datab Log fi SYSV	ase folder: C:\WINDOWS\NTDS e folder: C:\WINDOWS\NTDS OL folder: C:\WINDOWS\SYSVOL
The D will be	NS service will be installed and configured on this computer. This computer configured to use this DNS server as its preferred DNS server.
The p the ad	assword of the new domain administrator will be the same as the password of ministrator of this computer.
To ch	ange an option, click Back. To begin the operation, click Next.

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

- 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.
- 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

- 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 Willkommensseite 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 p providing a de	rovide an identifying scope name. You also have the option of scription.
Type a name a how the scope	and description for this scope. This information helps you quickly identify a is to be used on your network.
N <u>a</u> me:	CorpNet
Description:	
	< <u>B</u> ack <u>N</u> ext > Cancel

 Klicken Sie auf Weiter, und geben Sie die folgenden Parameter ein:Start-IP-Adresse -10.0.20.1End-IP-Adresse - 10.0.20.200Länge - 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.
Start IP address: 10.0.20.1
End IP address: 10 . 0 . 20 . 200
A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.
Length: 24
Subnet mask: 255 . 255 . 0
< <u>B</u> ack <u>N</u> ext > Cancel

 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.

w 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: 10 . 0 . 20 . 1 10 . 0 . 20 . 100 Add
Excluded address range:
Remo <u>v</u> e
< <u>B</u> ack <u>N</u> ext > Cancel

- 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				
O No, I will configure these options later				
< <u>B</u> ack <u>N</u> ext > 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.
I <u>P</u> address:
10.0.20.1 Add
<u>B</u> emove
Шр
Down
< <u>B</u> ack <u>N</u> ext > Cancel

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 do <u>m</u> ain: demo.local			
To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.			
<u>S</u> erver name:	I <u>P</u> address:		
		A <u>d</u> d	
R <u>e</u> solve	10.0.10.10	<u>R</u> emove	
		<u>Ш</u> р	
		Down	
	,		
	< <u>B</u> ack <u>N</u> ext >	Cancel	

- 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**.

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

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 Zertifikatdienste 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

- 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 verwaltenCA verwaltenZertifikate anfordernWenn eine dieser Optionen auf Verweigern festgelegt ist oder nicht ausgewählt ist, setzen Sie die Berechtigungen auf

ca.demo.local Properties		? ×
General Policy Module Exit Modul Certificate Managers Restrictions Auditing	ile Extensions ; Recovery Agents	Storage Security
<u>G</u> roup or user names: Administrators (DEMO\Administrators) Authenticated Users Domain Admins (DEMO\Domain Admin Enterprise Admins (DEMO\Enterprise A	ns) Admins)	
Permissions for Administrators Read Issue and Manage Certificates	Add B Allow (lemove
Request Certificates	▼	
OK	Cancel	Apply

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 Computername ein, und klicken Sie auf **Weiter**. In diesem Beispiel wird der Computername *Client*

w Object - Computer	×
Create in: demo.local/Users	
Computer name:	
client	
Computer name (pre-Windows 2000):	
CLIENT	
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	

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

- 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

General Uperating System Member Uf Location	Managed By Dial-in
Remote Access Permission (Dial-in or VPN)	
Allow access	
○ <u>D</u> eny access	
C Control access through Remote Access Policy	
Callback Options	
• No <u>C</u> allback	
Set by Caller (Routing and Remote Access Servi	ce only)
C Always Callback to:	
Assign a Static IP Address	
Apply Static <u>R</u> outes	
Define routes to enable for this Dial-in	atic Ro <u>u</u> tes
OK Car	ncel <u>A</u> pply

Hinzufügen von Benutzern zur Domäne

- 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**.
- 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		×
Create in:	demo.local/Users	
<u>F</u> irst name:	wirelessuser <u>I</u> nitials:	
Last name:		
Full n <u>a</u> me:	wirelessuser	
<u>U</u> ser logon name:		
wirelessuser	@demo.local	
User logon name (pre-	<u>W</u> indows 2000):	
DEMO\	wirelessuser	
	< <u>B</u> ack <u>N</u> ext > Cancel	

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

_		
Create in:	demo.local/Users	
Confirm password:	•••••	
User <u>m</u> ust change	password at next logon	
🔲 U <u>s</u> er cannot chan	ge password	
Password never ex	xpires	
Account is disable	d	
, <u> </u>	-	
	< <u>B</u> ack <u>Next</u> >	Canc

- 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

- 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

Remote control Terminal S	ervices Profile	COM+
General Address Account Pro	file Telephones	Organizatio
Member Of Dial-in	Environment	Sessions
- Remote Access Permission (Dial-in or V	/PN)	
Allow access		
C Deny access		
C Control access through Bemote Acc	sess Policy	
	Sees Foundy	
Callback Options	,	
No Callback		
C Set by Caller (Routing and Remote	Access Service only)
C Always Callback to:		
	,	
Assign a Static IP Address		
Apply Static <u>R</u> outes	,	
Define routes to enable for this Dial in		
Denne routes to enable for this Didnin	Static Ro	utes

Hinzufügen von Gruppen zur Domäne

- 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*

Group pame:	
wirelessusers	
J,	
Group name (pre- <u>W</u> indows 2000):	
wirelessusers	
Group scope	Group type
C Domain local	Security
Global	C Distribution
C Lloiversal	

Hinzufügen von Benutzern zur Wireless-Benutzergruppe

- 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

elect Users, Contacts, or Computers		
Select this object type:		
Users or Other objects		Object Type
From this location:		
demo local		Landiana
demonoca		
Enter the object names to select (<u>examples</u>):		
Enter the object names to select (<u>examples</u>): wirelessuser		Check Nam
Enter the object names to select (<u>examples</u>): wirelessuser		Check Nam
Enter the object names to select (<u>examples</u>): wirelessuser		<u>Check Narr</u>
Enter the object names to select (<u>examples</u>): wirelessuser	OK	Cancer

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

wirelessusers Proper	irelessusers Properties ?				
General Members	Member Of Managed By				
Members:					
Name	Active Directory Folder				
🙍 Administrator	demo.local/Users				
🖸 wirelessuser	demo.local/Users				
, 					
Add	<u>B</u> emove				
	UK Car	cel <u>Apply</u>			

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 <u>Benutzer zur Gruppe der Wireless-</u> <u>Benutzer hinzufügen</u> 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

act overs, contacts, or computers		?
Select this object type:		
Users or Other objects	Dbject Ty	pes
From this location:		
demo.local	Location	IS
Inter the object names to select (<u>examples</u>):		
Enter the object names to select (<u>examples</u>): client	<u>C</u> heck Na	ames
Enter the object names to select (<u>examples</u>): client		ames

wird. 🛏

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

Computer.

Object Types		? ×
Select the types of objects you want to find.		
Object types:		
🗹 🎻 Other objects		
E E Contacts		
1		
	ОК	Cancel

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

wirelessusers Proper	ties	? ×
General Members	Member Of Managed By	
Members:		
Name	Active Directory Folder	
Administrator	demo.local/Users	
- client	demo.local/Computers	
2 wrelessuser	demo.local/Users	
	Remove	
Aga	Teurove	
	OK Cancel	Apply

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 <u>Kapitel 4,</u> <u>"Verbinden von Kabeln".</u>
- 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.

- <u>Ausführen des Setup-Programms</u>
- <u>Überprüfen des Installationsprozesses</u>

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" (Schnittstellenname) "*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).
- Konfigurieren Sie die Informationen so, wie sie im Fenster Schnittstellen > Bearbeiten angezeigt werden:Schnittstellen-IP-Adresse - 10.0.20.2Netzmaske: 255.255.255.0Gateway - 10.0.10.1Primäres DHCP -10.0.10.10

սիսի			S	a <u>v</u> e Configuration	Ping L	ogout <u>R</u> efrei
	LANS CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMAN	DS HELP
Controller	Interfaces > Edit			< 8	lack	Apply
General Inventory Interfaces Multicast	General Informatio	on	ployee		-	
Network Routes	MAC Address	00::	24:97:69:4d:e	0		
Internal DHCP Server Mobility Management	Configuration					
Ports	Guest Lan					
NTP	Quarantine					
► CDP	Quarantine Vian Id	0				
Advanced	Physical Informati	ion				
	Port Number		2			
	Backup Port		0			
	Active Port		0			
	Enable Dynamic AP	Management				
	Interface Address					
	VLAN Identifier		20			
	IP Address		10.0.20.2			
	Netmask		255.255.255.	.0		
	Gateway		10.0.20.1			
	DHCP Information					
	Primary DHCP Serve	er	10.0.10.10			
	Secondary DHCP Se	rver				
	Access Control Lis	t				
	ACL Name		none 💌			
	Note: Changing the Int temporarily disabled an some clients.	erface param nd thus may r	eters causes t esult in loss of	he WLANs to be f connectivity for	_	

- 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*.

CISCO MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	Sa <u>v</u> e Configuration	Ping C <u>O</u> MM	Logout <u>R</u> efre: ANDS HELP
WLANs	WI	LANs > New			< B	ack	Apply
WLANs WLANs Advanced		Type Profile Name		WLAN 💌			
	1	SSID	[imployee			
		ID		1 💌			

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

- 16. Konfigurieren Sie die Informationen f
 ür dieses WLAN, wenn das Fenster WLANs > Edit angezeigt wird. Hinweis: WPAv2 wurde als Layer-2-Verschl
 üsselungsmethode f
 ür diese Übung ausgew
 ählt. Damit WPA mit TKIP-MIC-Clients dieser SSID zugeordnet werden kann, k
 önnen Sie auch den WPA-Kompatibilit
 ätsmodus und die K
 ästchen WPA2 TKIP-Clients zulassen oder die Clients aktivieren, die die 802.11i AES-Verschl
 üsselungsmethode nicht unterst
 ützen.
- 17. Klicken Sie im Bildschirm WLANs > Edit (WLANs > Bearbeiten) auf die Registerkarte **General (Allgemein**).
- 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.

IIIIII CISCO MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	s <u>s</u> ecurity	ave Configuration MANAGEMENT	i <u>P</u> ing C <u>O</u> MM	Logout <u>R</u> efre ANDS HELP
WLANs	W	LANs > Edit			< Ba	ack	Apply
▼ WLANs WLANs	-	General Sec	curity QoS	Advanc	ed		
Advanced		Profile I Name	Employee				
		Туре	WLAN				
		SSID I	Employee				
		Status	Enabled				
		Security I Policies (1 cl	[WPA2][Auth(Modifications do hanges.)	802.1X)] ne under secu	rity tab will appear	after ap	plying the
		Radio Policy Interface Broadcast SSID	All employee 💌 🗹 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

WLANs > E	dit						
General	Security	QoS	Advan	ced			
Layer 2	Layer 3	AAA Se	ervers				
Layer 2	Layer 2 Security WPA+WPA2 MAC Filtering WPA+WPA2 Parameters						
WPA Po	licy						
WPA2 P	olicy	7					
WPA2 E	ncryption	AE	s R	TKIP			
Auth Ke	y Mgmt	802.1	LX.	-			

- aus. ^L
- 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.

սիսիս		Sage Configuration Ping Logout Befree
CISCO MONITOR WL	ANS <u>C</u> ONTROLLER	WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security	RADIUS Auther	ntication Servers > New < Back Apply
 AAA General RADIUS Authentication Accounting Fallback TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies 	Server Index (Priority) Server IP Address Shared Secret Format Shared Secret Confirm Shared Secret Key Wrap R Port Number	
Local EAP	Server Status	Enabled
Priority Order	Support for REC 3576	Enabled 💌
Certificate	Server Timeout	2 seconds
Access Control Lists	Network User	Enable
Wireless Protection Policies	Management	Enable
▶ Web Auth	IPSec	Enable
Advanced		

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

- 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.

🚡 MyConsole - [Console Root\Ce	rtificate Templates]	
🚡 Elle Action View Favorites	<u>Window</u> Help	_8×
← → 🗈 🖪 😭 😫		
Console Root	Template Display Name	Minimum Supported CAs
Certificate Templates	Exchange Signature Only	Windows 2000
	Exchange User	Windows 2000
	12 IPSec	Windows 2000
	IPSec (Offline request)	Windows 2000
	Key Recovery Agent	Windows Server 2003, En
	RAS and IAS Server	Windows Server 2003, En
	Root Certification Authority	Windows 2000
	Router (Offline request)	Windows 2000
	Smartcard Logon	Windows 2000
	Smartcard User	Windows 2000
	Subordinate Certification Authority	Windows 2000
	Trust List Signing	Windows 2000
	User	Windows 2000
	User Signature Only	Windows 2000
	Web Server	Windows 2000
	Workstation Authe Duplicate Template	Windows Server 2003, En 👻
	All Tasks	
Using this template as a base, creates a	template that supports Properties	

Erstellen der Zertifikatvorlage für den ACS-Webserver

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

Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name Template display name: Copy of Web Server Iminum Supported CAs: Windows Server 2003, Enterprise Edition After you apply changes to this tab, you can no longer change the template name. Iemplate name: Copy of Web Server Validity period: Renewal period: 2 6 weeks Publish certificate in Active Directory D on not automatically reenrol if a duplicate certificate exists in Active Directory	operties of New Template	? ×
Template display name: Copy of Web Server Minimum Supported CAs: Windows Server 2003, Enterprise Edition After you apply changes to this tab, you can no longer change the template name. Template name: Copy of Web Server Validity period: Renewal period: 2 years 6 weeks Publish certificate in Active Directory Do not automatically reenrol if a duplicate certificate exists in Active Directory	Issuance Requirements Superseded Templates Extens General Request Handling Sul	ions Security bject Name
Copy of Web Server Minimum Supported CAs: Windows Server 2003, Enterprise Edition After you apply changes to this tab, you can no longer change the template name. Iemplate name: Copy of Web Server Validity period: Benewal period: 2 years 6 weeks Publish certificate in Active Directory Do not automatically reenrol if a duplicate certificate exists in Active Directory	Template display name:	
Minimum Supported CAs: Windows Server 2003, Enterprise Edition After you apply changes to this tab, you can no longer change the template name. Iemplate name: Copy of Web Server Validity period: Page Publish certificate in Active Directory Do not automatically reenrol if a duplicate certificate exists in Active Directory	Copy of Web Server	
After you apply changes to this tab, you can no longer change the template name.	Minimum Supported CAs: Windows Server 2003, Enterprise	Edition
Image:	After you apply changes to this tab, you can no longer chang name.	e the template
Copy of Web Server Validity period: Pupers Renewal period: years Kenewal period: years Kenewal period: Pupers Kenewal period: Directory Kenewal period: Cancel Accel Accel	Iemplate name:	
Yalidity period: Renewal period: 2 years 6 weeks Publish certificate in Active Directory Do not automatically reenrol if a duplicate certificate exists in Active Directory Directory	Copy of Web Server	
2 years 6 weeks	⊻alidity period: <u>R</u> enewal period:	
Publish certificate in Active Directory Do not automatically reenrol if a duplicate certificate exists in Active Directory OK Cencel Accive	2 years 6 weeks	
Publish certificate in Active Directory Do not automatically reenrol if a duplicate certificate exists in Active Directory		
Do not automatically reenrol if a duplicate certificate exists in Active Directory	Eublish certificate in Active Directory	
OK Cancel Apply	Do not automatically reenrol if a duplicate certificate e Directory	exists in Active
OK Cancel Apply		
OK Cancel Apply		
LIN LABOR	OK Cancel	1 ánolu

duplizieren.

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

percies of new	Template			?
Issuance Requirer General Template display :	nents Supers Reques	eded Template t Handling	s Extensi Sub	ons Secur ject Name
Template display	name:			
JALS				
Minimum Supporte	ed CAs: Windo	ws Server 2003), Enterprise I	Edition
After you apply ch	anges to this tai	b, you can no k	onger chang	e the template
name.				
Template name:				
ACS				
·				
⊻alidity period:		<u>Renewal peri</u>	od:	
2 years	•	6 wee	ks 💌	
Eublish certific	ate in Active Di	rectory		
Publish certific Do not out	cate in Active Di omatically reenr	rectory off if a duplicate	certificate e	xists in Active
Publish certific Do not aut Directory	sate in Active Di omatically reenr	rectory pli if a duplicate	certificate e	xists in Active
Publish certific Do not aut Directory	cate in Active Di omatically reenr	rectory off if a duplicate	certificate e	xists in Active
Publish certific Do not aut Directory	sate in Active Di omatically reenr	rectory off if a duplicate	certificate e	xists in Active
Publish certific Do not aut Directory	ate in Active Di	nectory of if a duplicate	Certificate e	xists in Active

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

operties of N	ew Templat	e			?
Issuance Req General	uirements 9 R	Superseded Temp equest Handling	plates	Extensions Subject I	Security Name
<u>P</u> urpose:	Signature Archive Delete	and encryption e subject's encryp e symmetric algori revoked or expire	ption priv ithms alle	vate key owed by the s cates (do not	▼ subject archive)
Do the follow associated w	ate key to be o ng when the s th this certifica ject without re	exported subject is enrolled ate is used: auiring any user in	l and wh	en the private	e key
C Prompt th C Prompt th private ke	e user during e e yser during e y is used	enroliment enroliment and rec	quire use	er input when	the
To choose w (CSPs) shoul	nich cryptogra I be used, clic	phic service prov k CSPs.	iders	<u>C</u> SF	2 ₈

- 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

5P Selection	?				
Choose which cryptogr requests:	raphic service providers (CSPs) can be used in				
○ <u>R</u> equests can use	any CSP available on the subject's computer				
• Requests must use	one of the following CSPs:				
<u>C</u> SPs:					
Gemplus GemSAFE	Card CSP v1.0				
Infineon SICRYPT	Base Smart Card CSP				
Microsoft Base DSS	S and Diffie-Hellman Cryptographic Provider				
Microsoft DH SCha	nnel Cryptographic Provider				
Microsoft Enhanced Cryptographic Provider v1.0					
Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Prov					
Microsoft Enhanced	d RSA and AES Cryptographic Provider				
IL IMICrosoft BSA SEh	annel Livotodranhic Provider				
	OK Cancel				
	<u></u>				
	OK Cancel Apply				

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

General Request Handling Subject Name Supply in the request Select this option to allow a variety of subject name formats or if you do not have access to the domain of which the subject is a member. Autoenrollment is not allowed if you choose this option. Build from this Active Directory information Select this option to enforce consistency among subject names and to simplify certificate administration. Subject pame format: None Include e-mail name in subject name Include this information in alternate subject name: E-mail name DNS name User principal name (UPN) Service principal name (SPN)	ssuance Requirer	ments Superseded Templates	Extensions Securi
 Supply in the request Select this option to allow a variety of subject name formats or if you do not have access to the domain of which the subject is a member. Autoenrollment is not allowed if you choose this option. Build from this Active Directory information Select this option to enforce consistency among subject names and to simplify certificate administration. Subject name format: Include e-mail name in subject name Include this information in alternate subject name: E-mail name DNS name User principal name (UPN) Service principal name (SPN) 	General	Request Handling	Subject Name
Select this option to enforce consistency among subject names and to simplify certificate administration. Subject name format: None Include e-mail name in subject name Include this information in alternate subject name: E-mail name DNS name DNS name User principal name (UPN) Service principal name (SPN)	 Supply in the Select this op not have acc Autoenrollmer Build from this Select this option 	request tion to allow a variety of subject r ess to the domain of which the su nt is not allowed if you choose thi s Active Directory information	name formats or if you do ubject is a member. is option.
None Image: Service principal name in subject name Include this information in alternate subject name: Image: Service principal name Image: Service principal name (SPN) Service principal name (SPN)	simplify certificat Subject name	ate administration. format:	subject names and to
Include e-mail name in subject name Include this information in alternate subject name: E-mail name DNS name User principal name (UPN) Sergice principal name (SPN)	None		Ψ.
Include this information in alternate subject name: E-mail name DNS name User principal name (UPN) Sergice principal name (SPN)	🔲 [nclude e-r	nail name in subject name	
DNS name User prinicipal name (UPN) Sergice principal name (SPN)		ormation in alternate subject nam	e:
User prinicipal name (UPN) Sergice principal name (SPN)	Include this inf	e	
Service principal name (SPN)	Include this inf E-mail nam	e }	
	Include this inf	e : ipal name (UPN)	
	Include this inf E-mail nam DNS name User prinic Sergice pri	e ; ipal name (UPN) ncipal name (SPN)	
	Include this inf E-mail nam DNS name User prinic Sergice pri	e ipal name (UPN) ncipal name (SPN)	

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

Properties of New Templ	ate		? ×
General Issuance Requirements	Request Handling Superseded Temp	Sul Nates Extens	bject Name ions Security
Require the following for CA certificate manage	enrollment: er approval		
This number of author	rized signatures:	0	
If you require more th Bolicy type required in	an one signature, a 1 signature:	utoenrollment is	not allowed.
Application policy:			
Issuance policies:			A <u>d</u> d
			Bemove
Require the following for r Same criteria as for er Valid existing certifica	reenrollment: nrollment te		
	OK	Cancel	

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

- Öffnen Sie das Snap-In Zertifizierungsstelle. Führen Sie die Schritte 1 bis 3 im Abschnitt <u>Create the Certificate Template for the ACS Web Server (Zertifikatvorlage für ACS-</u> <u>Webserver erstellen) aus,</u> 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
| 🔯 Certification Authority | | | | | |
|---|------------------|-------|---------------------------------|--|--|
| Eile <u>A</u> ction <u>V</u> iew <u>H</u> elp | | | | | |
| | | | | | |
| 📴 Certification Authority (Lo | cal) | Name | | | |
| 📄 😰 ca.demo.local | | Direc | tory Email Replication | | |
| Revoked Certificat | tes | Dom 🔯 | ain Controller Authentication | | |
| Issued Certificates | 5 | EFS I | Recovery Agent | | |
| Pending Requests | Pending Requests | | ic EFS | | |
| Certificate Templa | Failed Requests | | | | |
| | Manage | | Server | | |
| | | | huter | | |
| | New | • | Certificate Template to Issue | | |
| | View | • | rdinate Certification Authority | | |
| | <u></u> | | histrator | | |
| | Re <u>f</u> resh | | | | |
| | Export <u>I</u> | _ist | | | |
| | Help | | | | |
| II . | | | 1 | | |

soll.

4. Klicken Sie auf die ACS-

Zertifikatvorlage.

Name	Intended Purpose	
ACS	Server Authentication	
Authenticated Session	Client Authentication	
Z CA Exchange	Private Key Archival	
CEP Encryption	Certificate Request Agent	
🙀 Code Signing	Code Signing	
Cross Certification Authority	<alb< td=""><td></td></alb<>	
Enrollment Agent	Certificate Request Agent	
Enrollment Agent (Computer)	Certificate Request Agent	
Exchange Enrollment Agent (Offline request)	Certificate Request Agent	
😨 Exchange Signature Only	Secure Email	
Fychange Liser	Secure Email	-

- 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

left Active Direct	ory Users and Computers	
Sele Action	<u>V</u> iew <u>W</u> indow <u>H</u> elp	
🗢 🔶 🗈 🖪	1 🛍 🖆 🖻 🗟 😭 💵	2000
Active Directo	ry Users and Computers [A demo	local 5 objects
€-tij0 demo.loca	Delegate Control Find Connect to Domain Controller Querations Masters Operations Masters New All Tasks View New Window from Here Refresh Export List Properties Help	ers Controllers SecurityPrincipals

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

demo.local Properties	? ×
General Managed By Group Policy	
To improve Group Policy management, upgrade Management Console (GPMC). Current Group Policy Object Links for	to the Group Policy or demo
Group Policy Object Links	No Override Disabled
Group Policy Objects higher in the list have the h This list obtained from: AD 2003.demo.local	nighest priority.
<u>N</u> ew A <u>d</u> d <u>E</u> dit	<u>p</u>
Options Delete Properties	Do <u>w</u> n
Block Policy inheritance	
Close	Cancel <u>Apply</u>

geöffnet.

 Erweitern Sie in der Konsolenstruktur die Option Computerkonfiguration > Windows-Einstellungen > Sicherheitseinstellungen > Richtlinien f
ür öffentliche Schl
üssel, und w
ählen 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

Itomatic Certificate Request Setup W Certificate Template The next time a computer logs on, a c provided.	rizard 💌
A certificate template is a set of prede computers. Select a template from the Certificate templates:	fined properties for certificates issued to following list.
Name	Intended Purposes
Computer Domain Controller Enrollment Agent (Computer) IPSec	Client Authentication, Server Authenticatior Client Authentication, Server Authenticatior Certificate Request Agent IP security IKE intermediate
•	>
	< <u>B</u> ack <u>N</u> ext > Cancel

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.

🚡 Group Policy Object Editor	
Eile Action View Help	
S Default Domain Policy [AD2003.demo.local] Policy	Automatic Certificate Request
E-B Computer Configuration	Computer
Software Settings	
- Windows Settings	
 Scripts (Startup/Shutdown) 	
E-B Security Settings	
Account Policies	
Local Policies	
🖭 🚽 Event Log	
Restricted Groups	
System Services	
🖲 🧰 Registry	
🕢 过 File System	
Wireless Network (IEEE 802.11) Policies	
😑 🚞 Public Key Policies	
Encrypting File System	
Trusted Root Certification Authorities	
Enterprise Trust	
Software Restriction Policies	
IP Security Policies on Active Directory (demo.local)	
Administrative Templates	
E Ser Configuration	
Software Settings	
Windows Settings	
Administrative Templates	

- 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.

🚡 Group Policy Object Editor	
<u>Eile Action View H</u> elp	
🗊 Default Domain Policy [AD2003.demo.local] Policy	Object Type
🗄 🜆 Computer Configuration	Enterprise Trust
🖻 🚛 User Configuration	Autoenrollment Settings
🕀 💼 Software Settings	
🖻 💼 Windows Settings	
- 🤧 Remote Installation Services	
Scripts (Logon/Logoff)	
🖻 🖓 Security Settings	
🚊 🔄 Public Key Policies	
Enterprise Trust	
🗄 💼 Software Restriction Policies	
🕀 💼 Folder Redirection	
🗄 🍘 Internet Explorer Maintenance	
🗄 💼 Administrative Templates	

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

0	Autoenrollment Settings Properties	? ×
	General	
	Enroll user and computer certificates automatically	_
	 Do not enroll certificates automatically Enroll certificates automatically 	
	Renew expired certificates, update pending certificates, and ren revoked certificates	nove
	Update certificates that use certificate templates	
	OK Cancel Ap	ply
	Renew expired certificates, update pending certificates, and ren revoked certificates Update certificates that use certificate templates OK Cancel	ply

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**.



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



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



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

OK.		
Windows	s Internet Explorer	2
♪	A server certificate signing request has been generated and can be viewed in the "Outstanding Signin	ig Requests" list
	ОК	

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.



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



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

Save As				N.		? ×
Save in:	Desktop		•	00	بي 🔁	
My Recent Documents Desktop My Documents My Documents	My Document My Computer	s Naces				
My Network	File name:	ACS_ctd			•	Save
F-9061	Save as type:	.pem Document			•	Cancel

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



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

aus. ^L

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

Microsoft Certificate Services - ca.demo.local Home
Advanced Certificate Request
The policy of the CA determines the types of certificates you can request. Click one of the following options to:
Create and submit a request to this CA.
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64- encoded PKCS #7 file.
Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station. Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

senden...

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

Submit a Certi	ficate Request or Renewal Request
To submit a sav #10 certificate r source (such as	red request to the CA, paste a base-64-encoded CMC or PKCS request or PKCS #7 renewal request generated by an external a Web server) in the Saved Request box.
Saved Request:	
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	
Certificate Temp	late:
	Administrator
Additional Attribu	utes:
Attributes:	x y y
	Submits

6. 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.

Windows	Internet Explorer
♪	Your web browser security settings prohibit this page from accessing your disk. Either paste the data into this page manually, or add this page to your browser's list of trusted sites.
	ОК

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

ACS_csr PEM File 1 KB Open Edit		
Open With	Þ	📕 Notepad
Send To	•	🥖 Internet Explorer
Cut Copy		Choose Program
Create Shortcut Delete Rename		
Properties		

einem Texteditor (z. B. Notepad).

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

ACS_csr - Notepad		
File Edit Format View	w Help	
BEGIN CERT	Undo	UESTOMIIBVjCCA
	Cut	
	Сору	

Kopieren.

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



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 DXoioRABct447w077+uAk8crn26oaEhcfG/ZR15X ONZQ5xnrK23yxEdQNvSFC30mzR2EbQq4s5MvPEZZ /MWqXej3NjpicpAgiV8CSwNd END CERTIFICATE REQUEST
Certificate Temp	Browse for a file to insert. late: ACS
Additional Attribu	ites:
Attributes:	× •
	Submit >

Senden.

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

Certificate Issued	
The certificate you requested was issued to ODER encoded or Base 6	o you. 34 encoded
Download certificate chain	
File Do	wolload - Security Warning rou want to open or save this file? Name: certnew.cer Type: Security Certificate, 1.88KB From: ca 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 no come us trust this orthogram. Utility of the site?

herunterladen.

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

Save As				100	1×
Save in:	Desktop		. 01	• 🗈 ٵ	
My Recent Documents Desktop My Documents My Computer	My Document My Computer My Network P	s laces			
My Network Places	File name: Save as type:	ACS_cert Security Certificate		•	Save Cancel

speichern.

 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



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 /	stem Administration > Configuration > Local Server Certificates > Local Certificates						
Local Certificates Showing 1-2 of 2 50							
Filter: Match if: Go 🔽					Go 🔻		
	Friendly Name	•	Issued To	Issued By	Valid From		
	acs		acs	acs	04:29 20.09.2010		
	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

General	Directory Groups	s Directory Attributes	
Connectio	on Details		
Active D	irectory Domain	demo.local	
realing.			
Please sp	ecify the credentia	als used to join this machi	ne to the Active Directory Domain:
o Usemar	me:	administrator	
o Passwo	rd:		
		Test Connection	I
Click on 'S have succ	ave Changes' to essfully connecte	Test Connection	tory Domain and save this configuration. One
Click on 'S have succ to be avail	ave Changes' to essfully connecte able for use in po	Test Connection connect to the Active Direc d to the Domain, yo <mark>windo</mark> licy rules.	tory Domain and save this configuration. One
Click on 'S have succ to be avail End User	ave Changes' to (essifully connecte able for use in po Authentication S	Test Connection	tory Domain and save this configuration. One we Internet Explorer
Click on 'S have succ to be avail End User I Ena	ave Changes' to o essfully connecte able for use in po Authentication S ible password chi	Test Connection	tory Domain and save this configuration. One we Internet Explorer
Click on 'S have succ to be avail End User I Ena I Ena	ave Changes' to o essifully connecte able for use in po Authentication S ible password cha ible machine auth	Test Connection	tory Domain and save this configuration. One we Internet Explorer
Click on 'S have succ to be avail End User IF Ena IF Ena IF Ena	ave Changes' to o essfully connecte able for use in po Authentication S ible password ch ible machine auth ible Machine Acce	Test Connection	tory Domain and save this configuration. One we Internet Explorer

fortzufahren.

4. Klicken Sie auf Änderungen

DIUS Servers	
nd Identity Stores	Please specify the credentials used to join this machine to the Active Directory Doma
ements	O Username: administrator
Policies	o Password
ig and Reports	
Administration	You may use the Test Connection Button to ensure credentials are correct and Active Domain is reachable.
There are un	nsaved changes on this page. Do you wish to continue?
Save char	Discard chappes and continue Cancel
	End User Authentication Settings
	Enable Machine Access Restrictions Aging time (hours):
	Connectivity Status Joined to Domain demo local Connectivity Status CONINECTED
	a = Required seras
	Hinweis: Weiter

speichern.

Informationen zum Integrationsverfahren für ACS 5.x finden Sie unter <u>ACS 5.x und höher:</u> 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

 Network Resources 	Netv	ork De	vices			
 Network Device Groups Network Devices and AAA Clients 	Filte	c 🗌			• M	ato
Default Network Device External RADIUS Servers		Nam	e -	IP / I	lask	1
Big Users and Identity Stores St		No d	ata to d	isplay		
Policy Elements						
Access Policies						
Monitoring and Reports						
 System Administration 						

Erstellen.

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

	who		
Location	All Locations		Select
Device Type	All Device Types		Select
IP Address Single IP Address IP: 10.0.1.10	C IP Range (s)	Authentication Options TACACS+ Shared Secret. Single Connect Devi C Legacy TACACS+ Si TACACS+ Draft Com Support RADIUS Shared Secret. Support Shared Secret. Device ID for Trust Device ID: Password: TrustSec Advanced Secret.	ce ngle Connect Sup apliant Single Con atSec identification

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

angezeigt.

► 🛠 My Workspace	Network	Resources	> Ne	twork Devices an	d AAA Clients	
Network Resources	Network Devices					Showing 1-1 of 1
 Network Device Groups Network Devices and AAA Clients 	Filter: Match if:				it	💌 Go 💌
Default Network Device External RADIUS Servers		Name	-	IP / Mask	NDG:Location	NDG:Device Type
Busers and Identity Stores Store		wic		10.0.1.10/32	All Locations	All Device Types
Policy Elements						
Access Policies						
Monitoring and Reports						

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

Access P	olicies > Access	Services				
Acces	s Services				Showing 1-2 of 2	50 💌 per p
Filter:		Match if		G	-	
	Name	-	Service Type	Ir	cluded Policies	Description
	Default Device	e Admin	Device Administrati	ion A	<u>tentity</u> uthorization	Default Devi
	Default Netwo	rk Access	Network Access	Li A	tentity uthorization	Default Netw
4						
Crea	te Duplica	te Edit	Delete		Page	1 of 1

(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: WirelessAD	
Description:	
Access Service Policy Structure	
Based on service template	Select
O Based on existing service	Select
O User Selected Service Type Network Access	

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

Access Se	ervices		Showing 1-4 (
Filter			Choning 140
1 mar. [Match if:	Go 🔻	
Nar	ne 🔺	Service Type	Description
O Dev	vice Admin - Command Auth	Device Administration	
C Dev	vice Admin - Simple	Device Administration	
O Net	work Access - MAC Authentication Bypass	Network Access	
Net	work 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: WirelessAD		
Description:		
Access Service Policy Structur	e	
Based on service template	Network Access - Simple	Select
C Based on existing service		Select
C User Selected Service Type	Network Access	

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

Ċ	Cisco S	Secure ACS	We	bpage Dialog
	Identit	y Store		
	Filter:		٣	Match if: Go 🔻
		Name	*	Description
	С	AD1		
	0	CN Userna	ame	Predefined Certificate Authentication Profile
	0	DenyAcces	ss	
	0	Internal Ho	osts	
	0	Internal Us	sers	
	0	NAC Profil	er	Default Entry for NAC Profiler

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 C Rule based result selection	n
	Identity Source: AD1 Sel	ect
speichern).	Advanced Options	

Erstellen einer ACS-Zugriffsrichtlinie und einer Serviceregel

Gehen Sie folgendermaßen vor:

1. Gehen Sie zu Zugriffsrichtlinien > Dienstauswahlregeln.



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: WirelessRule Status: Enabled The Customize button in the lower right area of the policy rules scree conditions and results are available here for use in policy rules
	Conditions Image: Protocol: match Select Results

ć	Ci	sco	Secure AC	S V	Yebpaç	je Di
	Enum Definition					
			Enum Na	me	ID	
	C	•	Radius		0	
	C)	Tacacs		1	

- 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)

Conditions		
Protocol: match	 Radius 	Selec
Results		
Results		

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

Filb			owcy		
53550	er: Sta	tus 🛓	Match if: Equa	als 💌	 Clear
		Status	Name	Protocol	Conditions
3		•	WirelessRule	match Radius	
1		0	Rule-1	match Radius	
2		Θ	Rule-2	match Tacacs	
.	-	Default		If no rules data	ed or no enabled rule
	Г	Default		If no rules define	ed or no enabled rule

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

- Available r			-
	networks:		
To connel about wire	ct to, disconnect fr dess networks in ra	om, or find out more inform nge, click the button belo	nation w.
		View Wireless Ne	tworks
		Movi	e down
Add	Remove	Properties	
Add.	. Remove	Properties	

- 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

Wireless network properties	<u>?</u> ×
Association Authentication 0	Connection
Network name (SSID):	Imployee
Wireless network key	
This network requires a key	for the following:
Network Authentication:	WPA 💌
Data encryption:	ТКІР
Network key:	
Confirm network key.	
Key index (advanced):	
The key is provided for n	ne automatically
This is a computer-to-comp access points are not used	uter (ad hoc) network; wireless
	OK Cancel

7. Klicken Sie auf die Registerkarte Authentifizierung.

ist.

- 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

Vireless net	work properties	? X
Association	Authentication Connection	
Select this wireless Eth	option to provide authenticated network access for remet networks.	,
☑ Enable	IEEE 802.1x authentication for this network	
EAP type:	Protected EAP (PEAP)	•
	Propert	ies
Authen availab	ticate as <u>c</u> omputer when computer information is le ticate as guest when user or computer information i able	\$
	OK Ca	ancel

- 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

Protected EAP Properties
When connecting:
Validate server certificate
Connect to these servers:
Trusted Root Certification Authorities:
C&W HKT SecureNet CA Root CA 1 Ca.demo.local Certiposte Classe A Personne Certiposte Serveur Certisign - Autoridade Certificadora - AC2 Certisign - Autoridade Certificadora - AC4 ■ Do not grompt user to authorize new servers or trusted
certification authorities.
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Enable Fast Reconnect
OK Cancel

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

🔻 🔝 Monitoring and Reports
Dashboard
Alarms
Inbox
Thresholds
Schedules
Reports
Favorites
- Shared
Troubleshooting
- Connectivity Tests
ACS Support Bundle
Expert Troubleshooter
Monitoring Configuration

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 |

 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 > RADI	JS Authentication					
Authentication Status : Date :	Pass or Fail September 22, 2010	(<u>Last 30</u>	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 X=Fail Q.	Click for details	=Mouse	over item for addition	onal information		
Logged At	RADIUS NAS Status Failure	Details	Username	MAC/IP Address	Access Service	Authentication Method
Sep 22,10 5:51:17.843 F	M 🖌	9	wirelessuser	00-21-5c-69-9a-39	WirelessAD	PEAP (EAP-MSCHAPv2)

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

AAA Protocol > RAI	DIUS Authentication Detail
ACS session ID : acs/ Date : Sept	74551189/31 ember 22, 2010
Generated on Septemb	er 22, 2010 5:52:16 PM PDT
Authentication Summa	ary
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:	<u>WirelessAD</u>
Identity Store:	AD1
Authorization Profiles:	Permit Access
CTS Security Group:	
Authentication Method:	PEAP(EAP-MSCHAPv2)

Versuchen.

6. 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 Service	Hit Count
WirelessAD	33
Default Network Access	0

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 SP2Komponente identifiziert.

Wenden Sie sich für einen Hotfix an Microsoft, und lesen Sie den Artikel <u>PEAP authentication is</u> not successfully when you connect to a third party <u>RADIUS server</u>. 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
- <u>Konfigurationsbeispiel für Cisco Wireless LAN Controller (WLC) und Cisco ACS 5.x</u> (TACACS+) für die Webauthentifizierung
- Installations- und Upgrade-Handbuch für das Cisco Secure Access Control System 5.1
- <u>Technischer Support und Dokumentation für Cisco Systeme</u>

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.