

# Wireless BYOD mit Identity Services Engine

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Topologie](#)

[Konventionen](#)

[Wireless LAN Controller - RADIUS NAC- und CoA-Übersicht](#)

[Wireless LAN Controller - RADIUS NAC- und CoA-Funktionsablauf](#)

[ISE-Profilerstellung - Übersicht](#)

[Interne Identitätsbenutzer erstellen](#)

[Wireless LAN-Controller zur ISE hinzufügen](#)

[Konfigurieren der ISE für die Wireless-Authentifizierung](#)

[Bootstrap Wireless LAN-Controller](#)

[Verbinden des WLC mit einem Netzwerk](#)

[Authentifizierungsserver \(ISE\) zu WLC hinzufügen](#)

[Dynamische WLC-Mitarbeiterschnittstelle erstellen](#)

[Dynamische WLC-Gast-Schnittstelle erstellen](#)

[802.1x WLAN hinzufügen](#)

[Dynamische WLC-Schnittstellen testen](#)

[Wireless-Authentifizierung für iOS \(iPhone/iPad\)](#)

[Statusumleitungszugriffskontrollliste zu WLC hinzufügen](#)

[Profilerstellungssonden auf ISE aktivieren](#)

[Aktivieren von ISE-Profilrichtlinien für Geräte](#)

[ISE-Autorisierungsprofil für die Statuserkennung - Umleitung](#)

[ISE-Autorisierungsprofil für Mitarbeiter erstellen](#)

[ISE-Autorisierungsprofil für AN erstellen](#)

[Autorisierungsrichtlinie für Gerätestatus/Profilierung](#)

[Richtlinie zur Statusüberprüfung testen](#)

[Autorisierungsrichtlinie für differenzierten Zugriff](#)

[CoA-Test für differenzierten Zugriff](#)

[WLC Gast-WLAN](#)

[Testen des Gast-WLAN und Gastportals](#)

[ISE Wireless Sponsored Guest Access](#)

[Sponsoring für Gäste](#)

[Testen des Gastportalzugriffs](#)

[Zertifikatskonfiguration](#)

[Windows 2008 Active Directory-Integration](#)

[Active Directory-Gruppen hinzufügen](#)

[Identitätsquellensequenz hinzufügen](#)

[ISE Wireless Sponsored Guest Access mit integriertem AD](#)

[Konfigurieren von SPAN auf dem Switch](#)

[Referenz: Wireless-Authentifizierung für Apple MAC OS X](#)

[Referenz: Wireless-Authentifizierung für Microsoft Windows XP](#)

[Referenz: Wireless-Authentifizierung für Microsoft Windows 7](#)

[Zugehörige Informationen](#)

## Einleitung

Die Cisco Identity Services Engine (ISE) ist der Richtlinienserver der nächsten Generation von Cisco, der eine Authentifizierungs- und Autorisierungsinfrastruktur für die Cisco TrustSec-Lösung bereitstellt. Darüber hinaus stellt es zwei weitere wichtige Services bereit:

- Der erste Service besteht darin, eine Möglichkeit bereitzustellen, Endgerätetypen automatisch anhand der Attribute zu profilieren, die Cisco ISE aus verschiedenen Informationsquellen erhält. Dieser Service (der so genannte Profiler) bietet Funktionen, die mit denen vergleichbar sind, die Cisco zuvor mit der Cisco NAC Profiler Appliance angeboten hat.
- Ein weiterer wichtiger Service, den die Cisco ISE bereitstellt, ist die Überprüfung der Endpunkt-Compliance, z. B. die Installation der AV-/AS-Software und die Gültigkeit der Definitionsdatei (bekannt als Posture). Cisco hat diese exakte Statusfunktion bisher nur für die Cisco NAC Appliance bereitgestellt.

Die Cisco ISE bietet einen gleichwertigen Funktionsumfang und ist in 802.1X-Authentifizierungsmechanismen integriert.

Die in Wireless LAN-Controller (WLCs) integrierte Cisco ISE ermöglicht die Erstellung von Profilen für mobile Geräte wie Apple iDevices (iPhone, iPad und iPod), Android-basierte Smartphones und andere. Für 802.1X-Benutzer kann die Cisco ISE dasselbe Servicelevel wie Profilerstellung und Statusüberprüfung bereitstellen. Gastservices auf der Cisco ISE können auch in den Cisco WLC integriert werden, indem Web-Authentifizierungsanforderungen zur Authentifizierung an die Cisco ISE umgeleitet werden.

In diesem Dokument wird die Wireless-Lösung für Bring Your Own Device (BYOD) vorgestellt, die beispielsweise einen differenzierten Zugriff basierend auf bekannten Endgeräten und der Benutzerrichtlinie ermöglicht. In diesem Dokument wird nicht die vollständige BYOD-Lösung beschrieben, sondern lediglich ein einfacher Anwendungsfall für den dynamischen Zugriff veranschaulicht. Weitere Konfigurationsbeispiele sind das ISE Sponsor-Portal, in dem privilegierte Benutzer einen Gast für die Bereitstellung eines drahtlosen Gastzugriffs sponsern können.

## Voraussetzungen

### Anforderungen

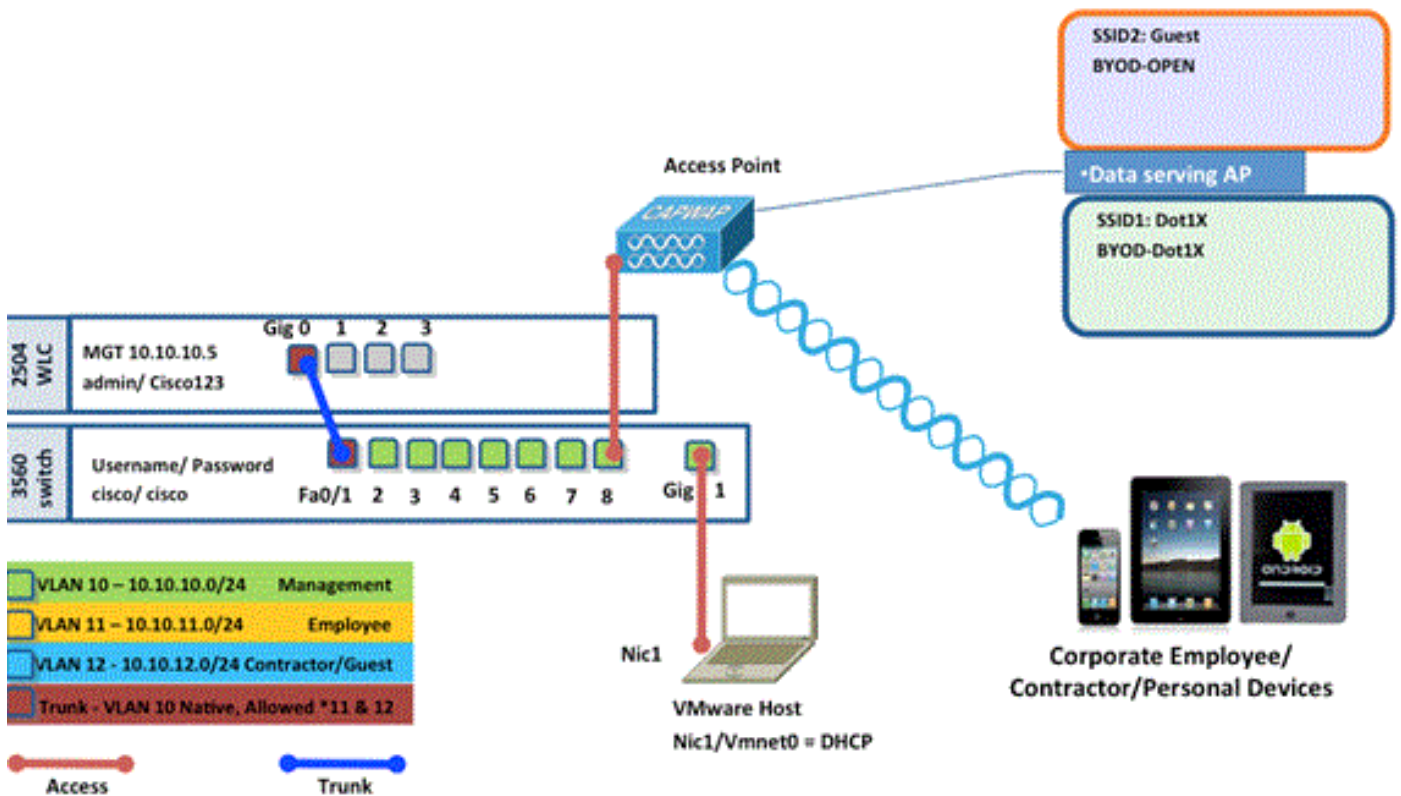
Es gibt keine spezifischen Anforderungen für dieses Dokument.

### Verwendete Komponenten

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

- Cisco Wireless LAN Controller 2504 oder 2106 mit Softwareversion 7.2.103
- Catalyst 3560 - 8 Ports
- WLC 2504
- Identity Services Engine 1.0MR (VMware Server-Image-Version)
- Windows 2008 Server (VMware-Image) - 512 MB, 20 GB FestplatteActive DirectoryDNSDHCPZertifikatsdienste

## Topologie



Name	IP Address	Credential
Vmware Host	10.10.10.2	(Machine used to host the ISE 1.0 MR vmware server files)
Identity Service Engine	10.10.10.70	admin/ default1A
Active Directory/ DNS/ DHCP/ CA Server	10.10.10.10	(Machine used to host Active Directory/ DNS/ DHCP/ CA Server)

## Konventionen

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

## Wireless LAN Controller - RADIUS NAC- und CoA-Übersicht

Mit dieser Einstellung kann der WLC nach AV-Paaren für die URL-Umleitung suchen, die vom ISE RADIUS-Server kommen. Dies ist nur in einem WLAN möglich, das an eine Schnittstelle mit aktivierter RADIUS NAC-Einstellung gebunden ist. Wenn das Cisco AV-Paar für die URL-

Umleitung empfangen wird, wird der Client in den Status POSTURE\_REQD versetzt. Dieser Zustand entspricht im Wesentlichen dem Zustand WEBAUTH\_REQD im Controller.

Wenn der ISE RADIUS-Server den Client als Posture\_Compliant einstuft, gibt er eine CoA-ReAuth aus. Die Session\_ID wird verwendet, um sie miteinander zu verknüpfen. Mit diesem neuen AuthC (re-Auth) sendet er keine URL-Redirect AV-Paare. Da es keine URL-Umleitungs-AV-Paare gibt, weiß der WLC, dass der Client keine Posture (Status) mehr benötigt.

Wenn die RADIUS NAC-Einstellung nicht aktiviert ist, ignoriert der WLC die URL-Umleitungs-VSAs.

CoA-ReAuth (CoA-ReAuth): Diese Funktion wird mit der Einstellung für RFC 3576 aktiviert. Die ReAuth-Funktion wurde zu den zuvor unterstützten CoA-Befehlen hinzugefügt.

Die RADIUS NAC-Einstellung schließt diese Funktion gegenseitig aus. Sie muss jedoch funktionieren, damit die CoA funktioniert.

Pre-Posture ACL (Pre-Posture-ACL): Wenn sich ein Client im POSTURE\_REQ-Status befindet, blockiert der WLC standardmäßig den gesamten Datenverkehr mit Ausnahme von DHCP/DNS. Die Pre-Posture ACL (die in dem url-redirect-acl AV-Pair genannt wird) wird auf den Client angewendet, und was in dieser ACL zulässig ist, kann der Client erreichen.

ACL vor der Auth im Vergleich zur VLAN-Aufhebung: Ein Quarantäne- oder AuthC-VLAN, das sich vom Access-VLAN unterscheidet, wird in 7.0MR1 nicht unterstützt. Wenn Sie ein VLAN vom Policy Server aus einrichten, ist es das VLAN für die gesamte Sitzung. Nach der ersten AuthZ sind keine VLAN-Änderungen erforderlich.

## Wireless LAN Controller - RADIUS NAC- und CoA-Funktionsablauf

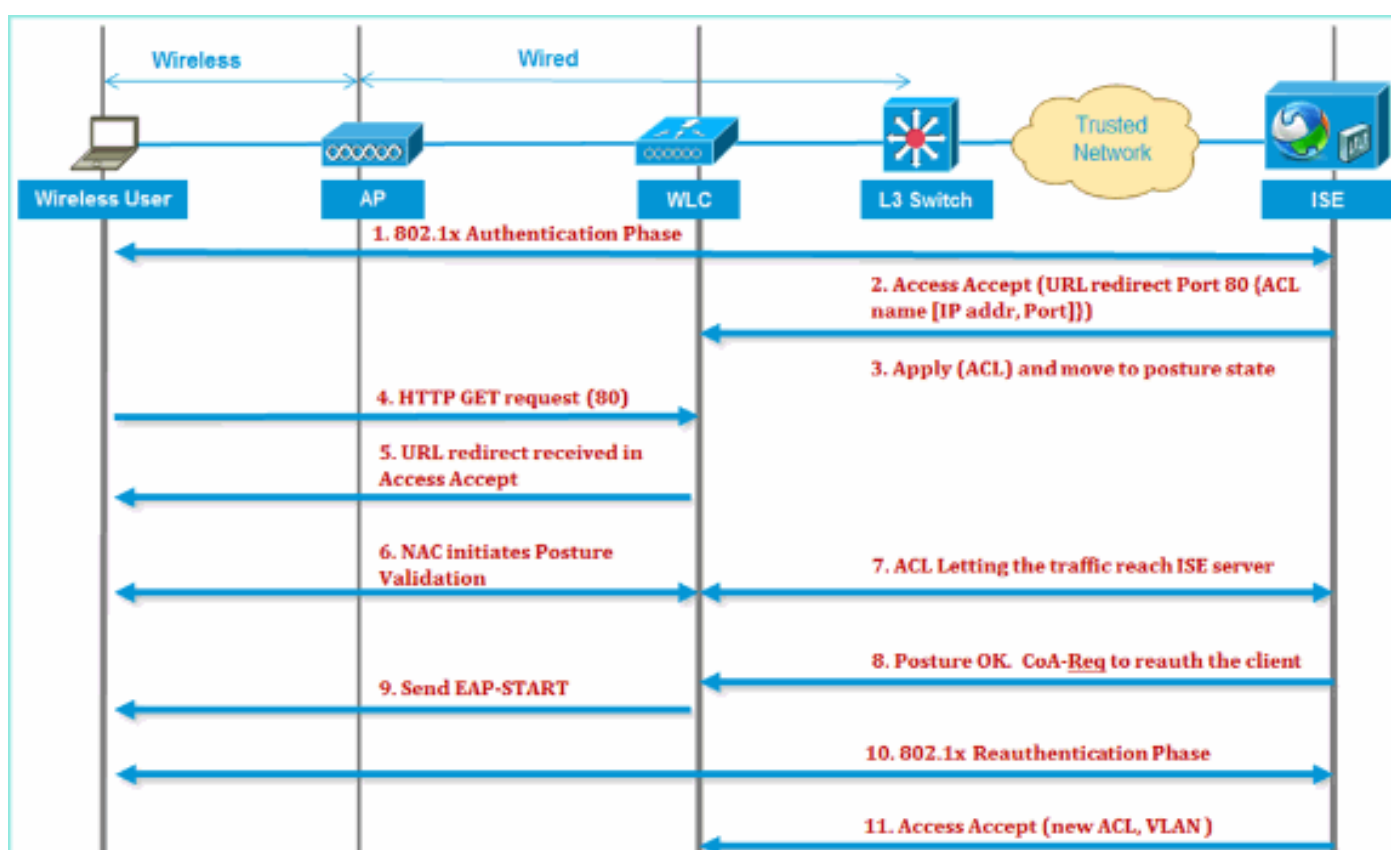
Die folgende [Abbildung](#) enthält Details zum Nachrichtenaustausch bei der Authentifizierung des Clients beim Backend-Server und zur Überprüfung des NAC-Status.

1. Der Client authentifiziert sich mithilfe der 802.1x-Authentifizierung.
2. RADIUS Access Accept beinhaltet die umgeleitete URL für Port 80 und vorauthentifizierte ACLs, die das Zulassen von IP-Adressen und Ports oder das Quarantäne-VLAN umfasst.
3. Der Client wird auf die unter "access accept" angegebene URL umgeleitet und in einen neuen Zustand versetzt, bis die Statusüberprüfung abgeschlossen ist. Der Client kommuniziert in diesem Zustand mit dem ISE-Server und überprüft sich anhand der auf dem ISE NAC-Server konfigurierten Richtlinien.
4. NAC-Agent auf Client initiiert Statusüberprüfung (Datenverkehr an Port 80): Agent sendet HTTP-Erkennungsanforderung an Port 80, die der Controller an die im Zugriffs-Accept bereitgestellte URL umleitet. Die ISE weiß, dass der Client die Verbindung herstellen will und direkt auf den Client reagiert. Auf diese Weise erfährt der Client die IP-Adresse des ISE-Servers und kommuniziert von nun an direkt mit dem ISE-Server.
5. Dieser Datenverkehr wird vom WLC zugelassen, da die ACL so konfiguriert ist, dass er zugelassen wird. Bei einer VLAN-Übersteuerung wird der Datenverkehr überbrückt, sodass er den ISE-Server erreicht.
6. Sobald der ISE-Client die Bewertung abgeschlossen hat, wird eine RADIUS-CoA-Anforderung mit Büroth-Service an den WLC gesendet. Dadurch wird eine erneute

Authentifizierung des Clients (durch Senden von EAP-START) initiiert. Sobald die erneute Authentifizierung erfolgreich ist, sendet die ISE eine Zugriffsbestätigung mit einer neuen ACL (falls vorhanden), ohne URL-Umleitung oder Zugriffs-VLAN.

7. WLC unterstützt CoA-Req und Disconnect-Req gemäß RFC 3576. Der WLC muss die CoA-Anforderung für den Authentifizierungsdienst gemäß RFC 5176 unterstützen.
8. Statt herunterladbarer ACLs werden auf dem WLC vorkonfigurierte ACLs verwendet. Der ISE-Server sendet nur den ACL-Namen, der bereits im Controller konfiguriert ist.
9. Dieses Design sollte sowohl für VLAN- als auch für ACL-Gehäuse geeignet sein. Im Fall einer VLAN-Übersteuerung leiten wir einfach den Port 80 um, der umgeleitet wird und den restlichen Datenverkehr über das Quarantäne-VLAN überbrückt. Auf die ACL wird die im Accept-Modus vor der Authentifizierung empfangene ACL angewendet.

Diese Abbildung zeigt den Funktionsablauf in visueller Darstellung:



## ISE-Profilerstellung - Übersicht

Der Cisco ISE Profiler-Service bietet Funktionen zum Erkennen, Auffinden und Bestimmen der Funktionen aller angeschlossenen Endgeräte in Ihrem Netzwerk, unabhängig von deren Gerätetyp, um einen angemessenen Zugriff auf Ihr Unternehmensnetzwerk sicherzustellen und aufrechtzuerhalten. Dabei werden primär Attribute oder Attributsätze aller Endpunkte im Netzwerk erfasst und entsprechend ihren Profilen klassifiziert.

Der Profiler besteht aus folgenden Komponenten:

- Der Sensor enthält eine Reihe von Sonden. Die Tests erfassen Netzwerkpakete durch Abfragen von Netzwerkzugriffsgeräten und leiten die Attribute und ihre Attributwerte, die von den Endgeräten erfasst werden, an den Analysator weiter.
- Ein Analyzer wertet Endpunkte anhand der konfigurierten Richtlinien und Identitätsgruppen

aus, um sie den erfassten Attributen und Attributwerten zuzuordnen. Dabei werden Endpunkte der angegebenen Gruppe zugeordnet und Endpunkte mit dem entsprechenden Profil in der Cisco ISE-Datenbank gespeichert.

Für die Erkennung von Mobilgeräten empfiehlt es sich, zur korrekten Identifizierung des Geräts eine Kombination dieser Tests zu verwenden:


- RADIUS (Calling-Station-ID): Stellt die MAC-Adresse (OUI) bereit
- DHCP (Hostname): Hostname - Standard-Hostname kann Gerätetyp enthalten, z. B.: jsmith-ipad
- DNS (umgekehrte IP-Suche): FQDN - Standard-Hostname kann Gerätetyp enthalten
- HTTP (User-Agent): Details zu einem bestimmten Mobilgerätetyp

In diesem Beispiel eines iPads erfasst der Profiler die Webbrowserinformationen aus dem User-Agent-Attribut sowie andere HTTP-Attribute aus den Anforderungsnachrichten und fügt sie der Liste der Endgeräteattribute hinzu.




Is the MAC Address  
from Apple? 



Does the Hostname  
contain "iPad"? 



Is the Safari Browser  
on an iPad? 



I am  
certain it  
is an iPad!

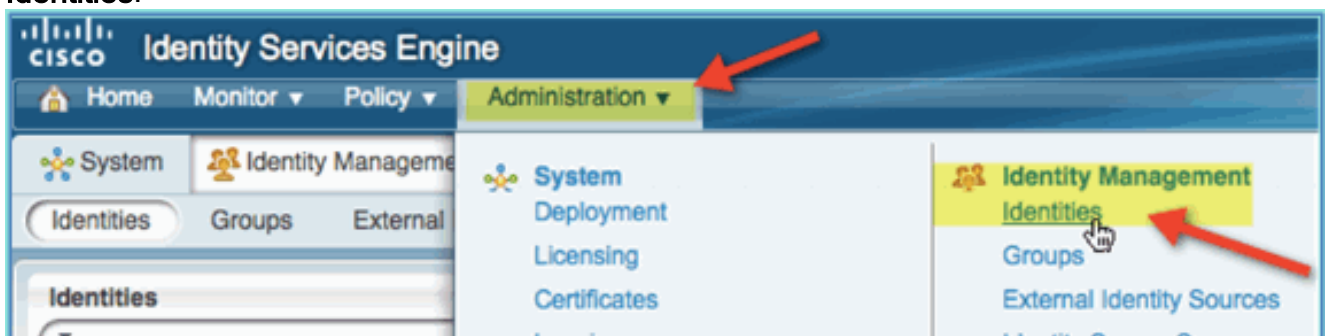
[Interne Identitätsbenutzer erstellen](#)

MS Active Directory (AD) ist für eine einfache Machbarkeitsstudie nicht erforderlich. Die ISE kann als alleiniger Identitätsdatenspeicher verwendet werden, der differenzierten Benutzerzugriff für den Zugriff und eine präzise Richtlinienkontrolle umfasst.

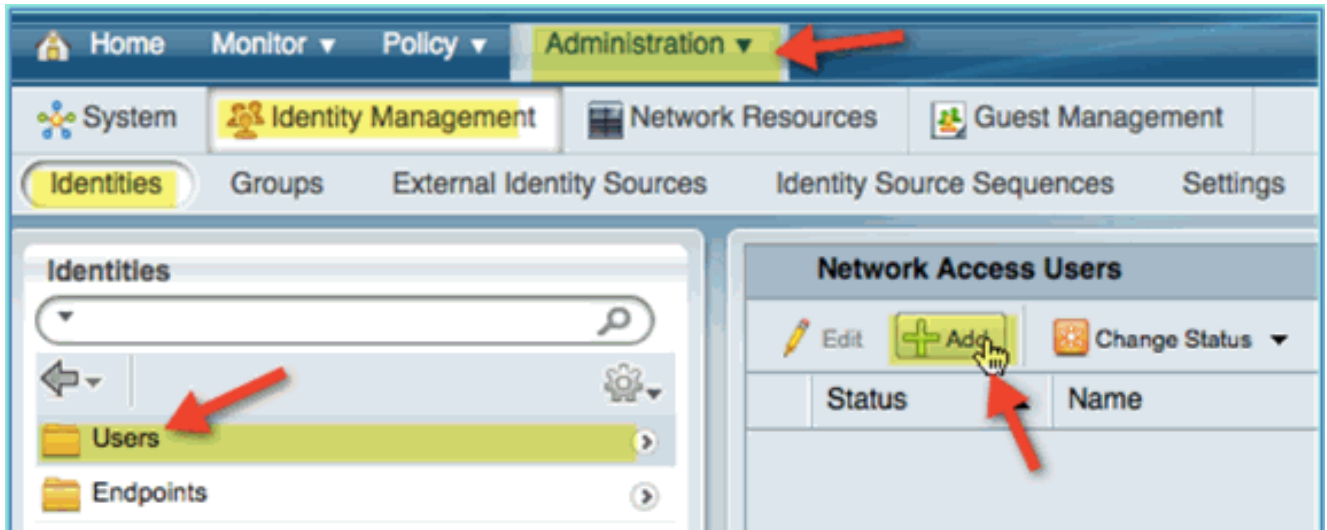
Mit der Einführung von ISE 1.0 mithilfe der AD-Integration kann die ISE AD-Gruppen in Autorisierungsrichtlinien verwenden. Bei Verwendung des internen ISE-Benutzerspeichers (keine AD-Integration) können Gruppen nicht in Richtlinien zusammen mit Geräteidentitätsgruppen verwendet werden (erkannter Fehler muss in ISE 1.1 behoben werden). Daher können nur einzelne Benutzer unterschieden werden, z. B. Mitarbeiter oder Auftragnehmer, wenn diese zusätzlich zu Geräteidentitätsgruppen verwendet werden.

Führen Sie diese Schritte aus:

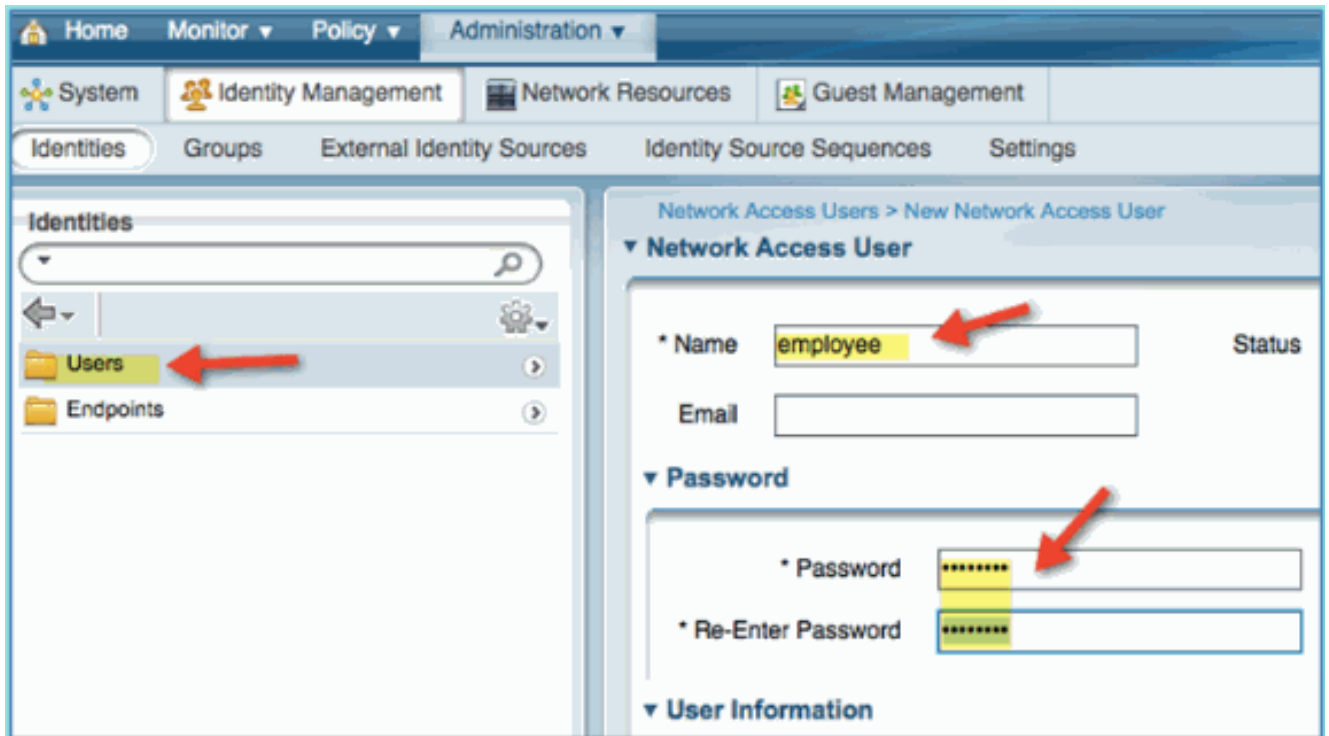
1. Öffnen Sie ein Browserfenster, um die Adresse <https://ISEip> anzuzeigen.
2. Navigieren Sie zu **Administration > Identity Management > Identities**.



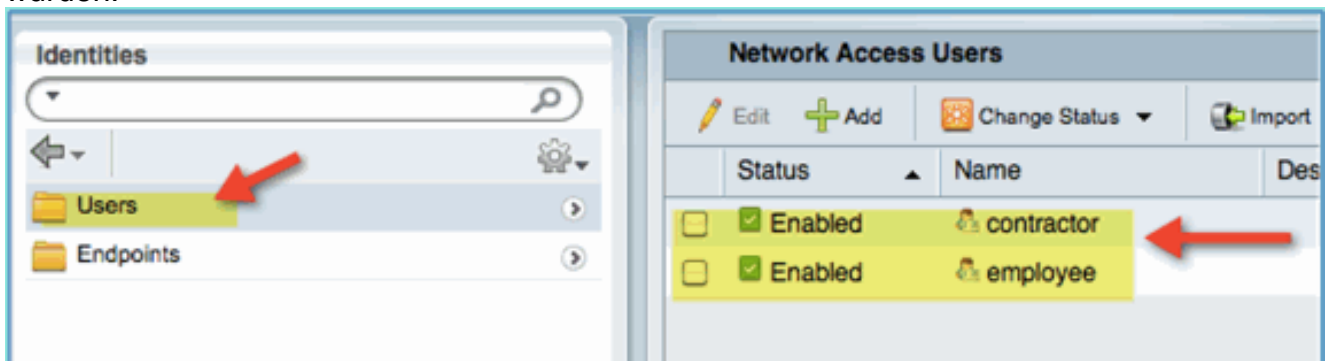
3. Wählen Sie **Benutzer aus**, und klicken Sie dann auf **Hinzufügen** (Netzwerkzugriffsbenutzer). Geben Sie folgende Benutzerwerte ein, und weisen Sie sie einer Mitarbeitergruppe zu: Name: Mitarbeiter Kennwort: XXXX







4. Klicken Sie auf **Senden**.Name: AuftragnehmerKennwort: XXXX
5. Bestätigen Sie, dass beide Konten erstellt wurden.



## Wireless LAN-Controller zur ISE hinzufügen

Jedes Gerät, das RADIUS-Anfragen an die ISE auslöst, muss über eine Definition in der ISE verfügen. Diese Netzwerkgeräte werden basierend auf ihrer IP-Adresse definiert. ISE-Netzwerkgerätedefinitionen können IP-Adressbereiche angeben, sodass die Definition mehrere tatsächliche Geräte darstellen kann.

Darüber hinaus enthalten die ISE-Netzwerkgerätedefinitionen Einstellungen für andere ISE-/Gerätekommunikationen wie SNMP und SSH.

Ein weiterer wichtiger Aspekt bei der Definition von Netzwerkgeräten ist die angemessene Gruppierung von Geräten, damit diese Gruppierung in der Netzwerkzugriffsrichtlinie verwendet werden kann.

In dieser Übung werden die für Ihre Übung erforderlichen Gerätedefinitionen konfiguriert.

Führen Sie diese Schritte aus:

1. Gehen Sie von der ISE zu **Administration > Network Resources > Network**

## Devices.

The screenshot shows the 'New Network Device' configuration page in the Cisco ISE Administration console. The page is under 'Administration' > 'Network Resources' > 'Network Devices'. The form includes the following fields and options:

- Name: pod-wlc
- Description: (empty)
- IP Address: 10.10.10.5 / 32
- Model Name: (empty)
- Software Version: (empty)
- Network Device Group:
  - Location: All Locations
  - Device Type: All Device Types
- Authentication Settings:
  - Enable Authentication Settings:
  - Protocol: RADIUS
  - Shared Secret: [redacted]
- SNMP Settings:
- Security Group Access (SGA):
- Device Configuration Deployment:

Buttons: Submit, Cancel

2. Klicken Sie unter Netzwerkgeräte auf **Hinzufügen**. Geben Sie die IP-Adresse ein, überprüfen Sie die Authentifizierungseinstellung mithilfe einer Maske, und geben Sie dann "cisco" als gemeinsamen geheimen Schlüssel ein.
3. Speichern Sie den WLC-Eintrag, und bestätigen Sie den Controller in der Liste.

The screenshot shows the 'Network Devices' list in the Cisco ISE Administration console. The list contains one entry:

Name	IP/Mask	Location
pod-wlc	10.10.10.5/32	All Locations

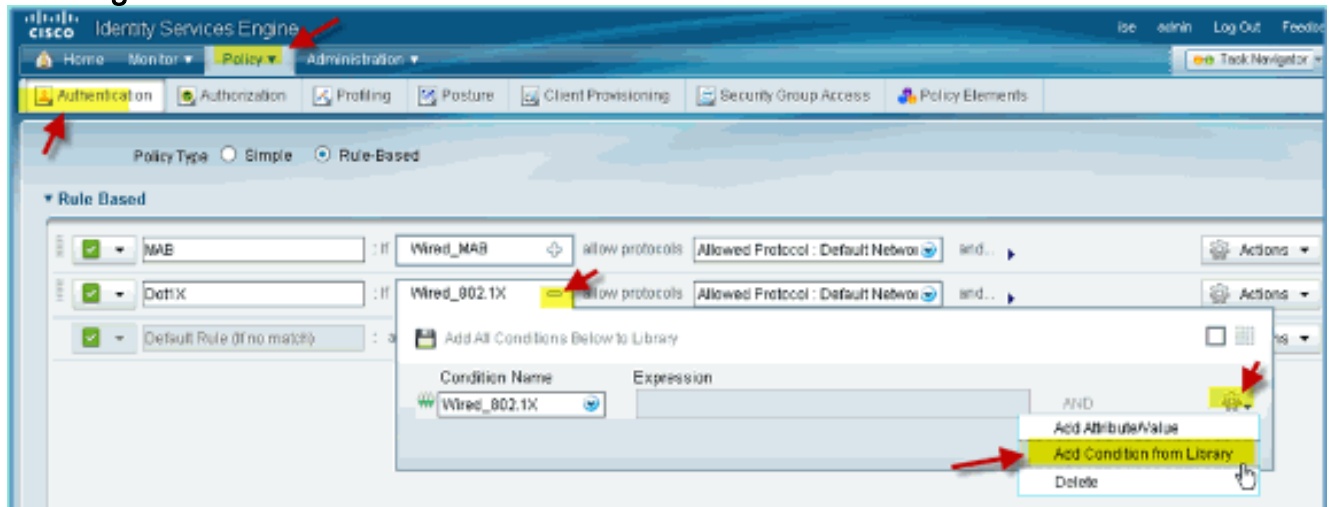
Buttons: Edit, Add, Duplicate, Import, Export, Delete

## Konfigurieren der ISE für die Wireless-Authentifizierung

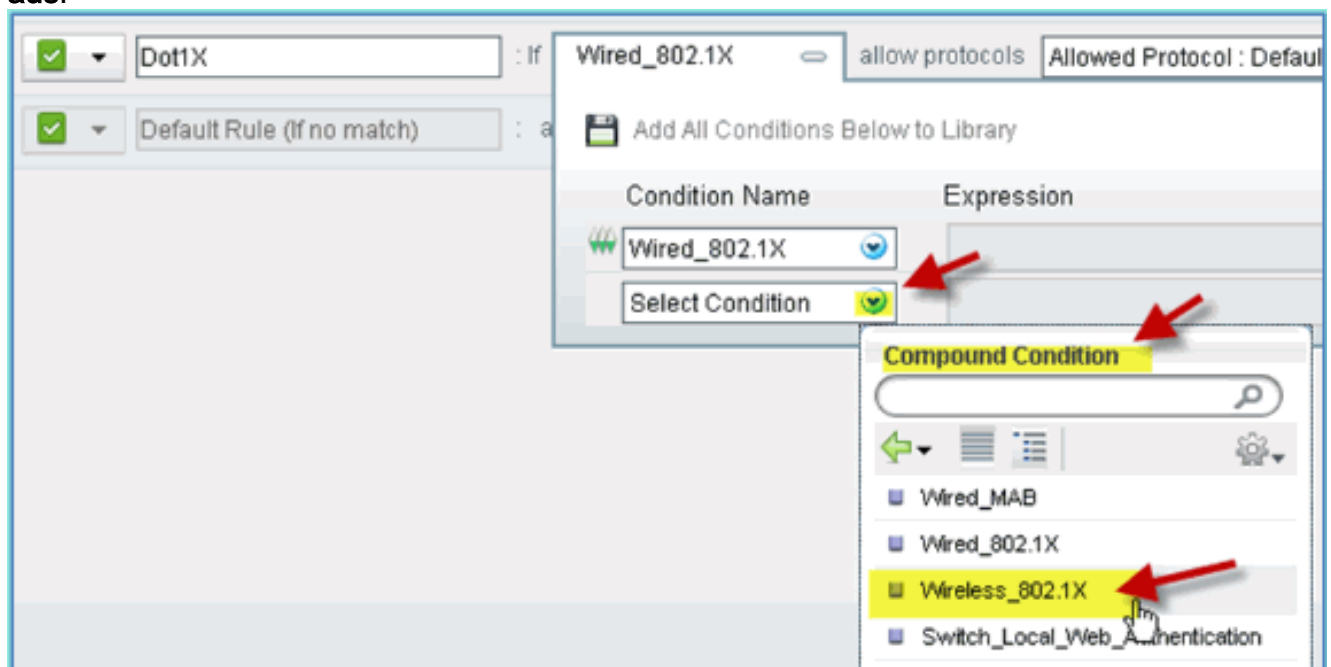
Die ISE muss für die Authentifizierung von 802.1x-Wireless-Clients konfiguriert werden und Active Directory als Identitätsspeicher verwenden.

Führen Sie diese Schritte aus:

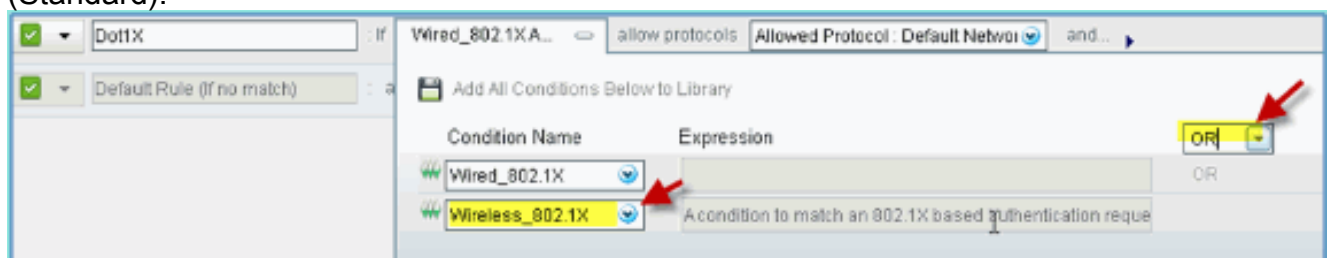
1. Navigieren Sie von der ISE zu **Policy > Authentication (Richtlinie > Authentifizierung)**.
2. Klicken Sie, um Dot1x > Wired\_802.1X (-) zu erweitern.
3. Klicken Sie auf das Zahnrad-Symbol, um **Bedingung aus Bibliothek hinzufügen**.

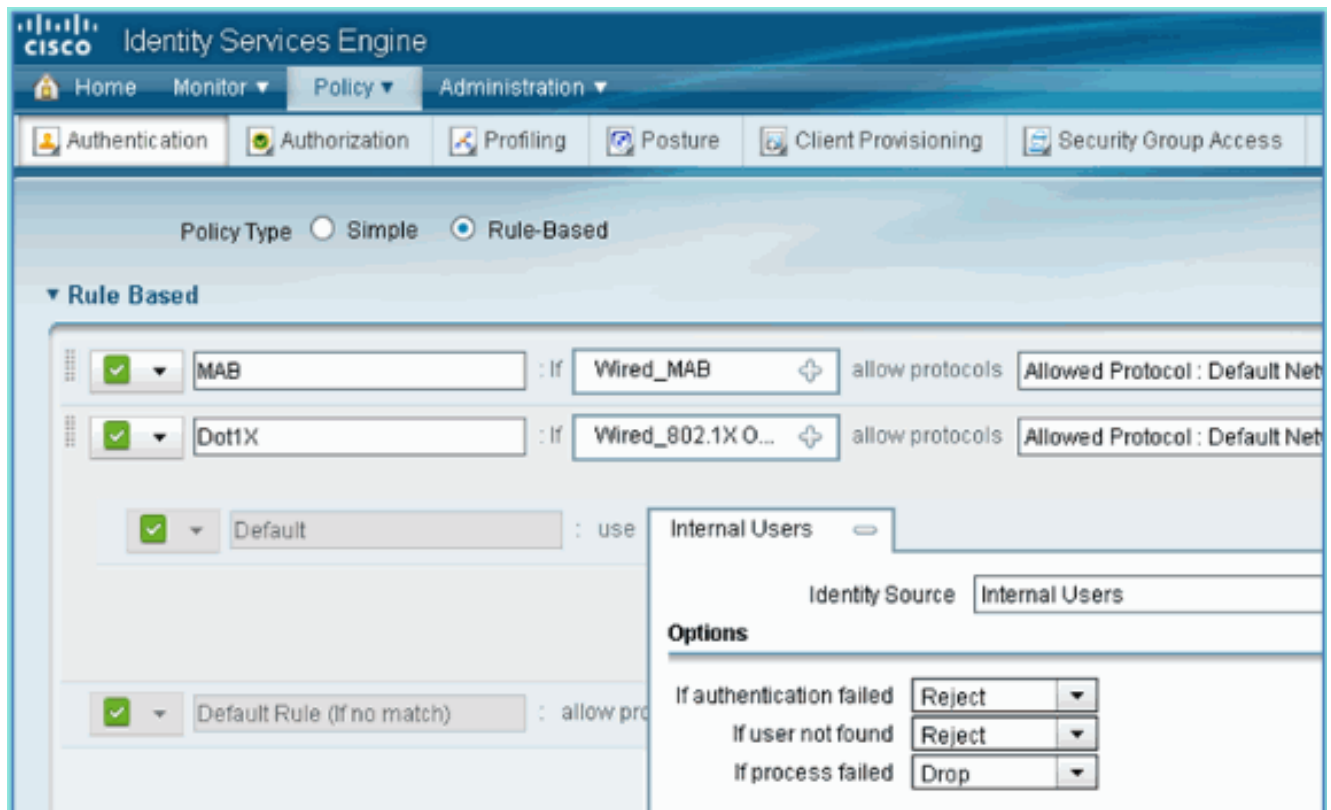


4. Wählen Sie im Dropdown-Menü für die Bedingungsauswahl die Option **Compound Condition > Wireless\_802.1X** aus.



5. Setzen Sie die Express-Bedingung auf **OR**.
6. Erweitern Sie die Option after allow protocol, und akzeptieren Sie die Standardeinstellung **Internal Users** (Standard).





7. Lassen Sie alles andere auf dem Standardwert. Klicken Sie auf **Speichern**, um die Schritte auszuführen.

## [Bootstrap Wireless LAN-Controller](#)

### [Verbinden des WLC mit einem Netzwerk](#)

Eine Anleitung zur Bereitstellung der Cisco Wireless LAN Controller der [Serie 2500](#) finden Sie im [Cisco Wireless Controller Deployment Guide](#).

### **Konfigurieren des Controllers mithilfe des Start-Assistenten**

```
(Cisco Controller)
Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup
Would you like to terminate autoinstall? [yes]: yes AUTO-INSTALL: process terminated
-- no configuration loaded System Name [Cisco_d9:24:44] (31 characters max):
ISE-Podx Enter Administrative User Name (24 characters max): admin
Enter Administrative Password
(3 to 24 characters): Cisco123
Re-enter Administrative Password: Cisco123
Management Interface IP Address: 10.10.10.5
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.10.10.10
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: ISE
Network Name (SSID): PODx
Configure DHCP Bridging Mode [yes][NO]: no
Allow Static IP Addresses [YES][no]: no
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
```

Please see documentation for more details.

```
Enter Country Code list (enter 'help' for a list of countries) [US]: US
```

```
Enable 802.11b Network [YES][no]: yes
```

```
Enable 802.11a Network [YES][no]: yes
```

```
Enable 802.11g Network [YES][no]: yes
```

```
Enable Auto-RF [YES][no]: yes
```

```
Configure a NTP server now? [YES][no]: no
```

```
Configure the ntp system time now? [YES][no]: yes
```

```
Enter the date in MM/DD/YY format: mm/dd/yy
```

```
Enter the time in HH:MM:SS format: hh:mm:ss
```

```
Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
```

```
Configuration saved!
```

```
Resetting system with new configuration...
```

```
Restarting system.
```

## Konfiguration des Nachbarswitches

Der Controller ist mit dem Ethernet-Port des benachbarten Switches (Fast Ethernet 1) verbunden. Der benachbarte Switch-Port wird als 802.1q-Trunk konfiguriert und ermöglicht alle VLANs auf dem Trunk. Das native VLAN 10 ermöglicht den Anschluss der Verwaltungsschnittstelle des WLC.

Die 802.1Q-Switch-Port-Konfiguration sieht wie folgt aus:

```
switchport
switchport trunk encapsulation dot1q
switchport trunk native VLAN 10
switchport mode trunk
end
```

## [Authentifizierungsserver \(ISE\) zu WLC hinzufügen](#)

Die ISE muss zum WLC hinzugefügt werden, um 802.1X und die CoA-Funktion für Wireless-Endgeräte zu aktivieren.

Führen Sie diese Schritte aus:

1. Öffnen Sie einen Browser, und stellen Sie dann eine Verbindung mit dem POD-WLC her (über sicheres HTTP) > <https://wlc>.
2. Navigieren Sie zu **Sicherheit > Authentifizierung > Neu**.

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

### RADIUS Authentication Servers > New

Server Index (Priority) 1

Server IP Address 10.10.10.70

Shared Secret Format ASCII

Shared Secret \*\*\*\*\*

Confirm Shared Secret \*\*\*\*\*

Key Wrap  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number 1812

Server Status Enabled

Support for RFC 3576 Enabled

Server Timeout 2 seconds

Network User  Enable

Management  Enable

IPSec  Enable

- Geben Sie folgende Werte ein: Server-IP-Adresse: 10.10.10.70  
(Scheckzuweisung) Gemeinsamer geheimer Schlüssel: cisco Unterstützung für RFC 3576 (CoA): Aktiviert (Standard) Alles andere: Standard
- Klicken Sie auf **Apply**, um fortzufahren.
- Wählen Sie **RADIUS Accounting > fügen Sie NEW hinzu**.

CISCO

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT C

### Security RADIUS Accounting Servers > New

AAA

- General
- RADIUS
  - Authentication
  - Accounting
  - Fallback
- TACACS+
- LDAP
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies
- Password Policies

Local EAP

Priority Order

Certificate

Server Index (Priority) 2

Server IP Address 10.10.10.70

Shared Secret Format ASCII

Shared Secret \*\*\*\*\*

Confirm Shared Secret \*\*\*\*\*

Port Number 1813

Server Status Enabled

Server Timeout 2 seconds

Network User  Enable

IPSec  Enable

- Geben Sie folgende Werte ein: Server-IP-Adresse: 10.10.10.70 Gemeinsamer geheimer Schlüssel: cisco Alles andere: Standard
- Klicken Sie auf **Apply** (Anwenden), und speichern Sie die Konfiguration für den WLC.

## Dynamische WLC-Mitarbeiterschnittstelle erstellen

Gehen Sie wie folgt vor, um eine neue dynamische Schnittstelle für den WLC hinzuzufügen und dem Mitarbeiter-VLAN zuzuordnen:

1. Navigieren Sie vom WLC zu **Controller > Interfaces (Controller > Schnittstellen)**. Klicken Sie dann auf **Neu**.



2. Navigieren Sie vom WLC zu **Controller > Interfaces (Controller > Schnittstellen)**. Geben Sie Folgendes ein: Schnittstellenname: Mitarbeiter VLAN-ID:

11



3. Geben Sie Folgendes für die Mitarbeiter-Schnittstelle ein: Portnummer: 1 VLAN-Kennung: 11 IP-Adresse: 10.10.11.5 Netzmaske: 255.255.255.0 Gateway: 10.10.11.1 DHCP: 10.10.10.10

### Configuration

Quarantine

Quarantine Vlan Id

---

### Physical Information

Port Number

Backup Port

Active Port

Enable Dynamic AP Management

---

### Interface Address

VLAN Identifier

IP Address

Netmask

Gateway

---

### DHCP Information

Primary DHCP Server

Secondary DHCP Server

4. Bestätigen Sie, dass die neue dynamische Benutzeroberfläche für Mitarbeiter erstellt wurde.

CISCO

MONITOR WLANs **CONTROLLER** WIRELESS SECURITY MANAGEMENT COMMUNITY

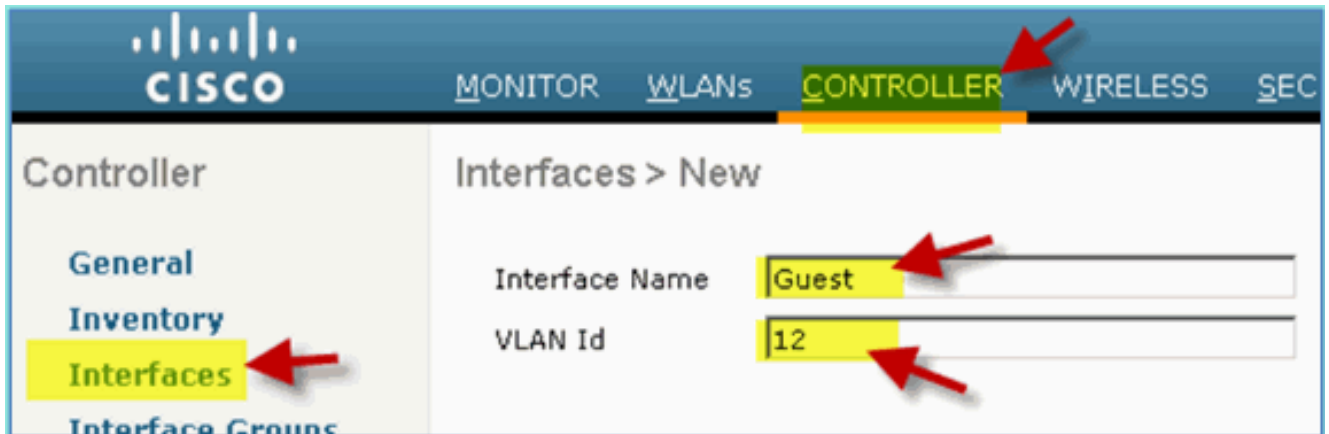
Controller	Interfaces			
	Interface Name	VLAN Identifier	IP Address	Interface Type
General	<b>employee</b>	11	10.10.11.5	Dynamic
Inventory	<a href="#">management</a>	untagged	10.10.10.5	Static
<b>Interfaces</b>	<a href="#">virtual</a>	N/A	1.1.1.1	Static
Interface Groups				
Multicast				



## Dynamische WLC-Gast-Schnittstelle erstellen

Gehen Sie wie folgt vor, um eine neue dynamische Schnittstelle für den WLC hinzuzufügen und dem Gast-VLAN zuzuordnen:

1. Navigieren Sie vom WLC zu **Controller > Interfaces (Controller > Schnittstellen)**. Klicken Sie dann auf **Neu**.
2. Navigieren Sie vom WLC zu **Controller > Interfaces (Controller > Schnittstellen)**. Geben Sie Folgendes ein: Schnittstellenname: Gast  
VLAN-ID:  
12



3. Geben Sie diese für die Gastschnittstelle ein: Portnummer: 1  
VLAN-Kennung: 12  
IP-Adresse: 10.10.12.5  
Netzmaske: 255.255.255.0  
Gateway: 10.10.12.1  
DHCP: 10.10.10.10

## Configuration

Quarantine   
Quarantine Vlan Id

## Physical Information

Port Number   
Backup Port   
Active Port   
Enable Dynamic AP Management

## Interface Address

VLAN Identifier   
IP Address   
Netmask   
Gateway

## DHCP Information

Primary DHCP Server   
Secondary DHCP Server

## Access Control List

ACL Name

*Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.*

- Bestätigen Sie, dass die Gastschnittstelle hinzugefügt wurde.

Interface Name	VLAN Identifier	IP Address	Interface Type
employee	11	10.10.11.5	Dynamic
guest	12	10.10.12.5	Dynamic
management	untagged	10.10.10.5	Static
virtual	N/A	1.1.1.1	Static

## 802.1x WLAN hinzufügen

Vom ursprünglichen Bootstrap des WLC ausgehend wurde möglicherweise ein Standard-WLAN erstellt. In diesem Fall können Sie das Tool ändern oder ein neues WLAN erstellen, um die 802.1X-Wireless-Authentifizierung gemäß den Anweisungen im Leitfaden zu unterstützen.

Führen Sie diese Schritte aus:

1. Navigieren Sie vom WLC zu **WLAN > Create New**.



2. Geben Sie für das WLAN Folgendes ein: Profilname: pod1x SSID: identisch



3. Verwenden Sie für die Registerkarte "WLAN-Einstellungen > Allgemein" Folgendes: Funkrichtlinie: Alle Schnittstelle/Gruppe: Management Alles andere: Standard

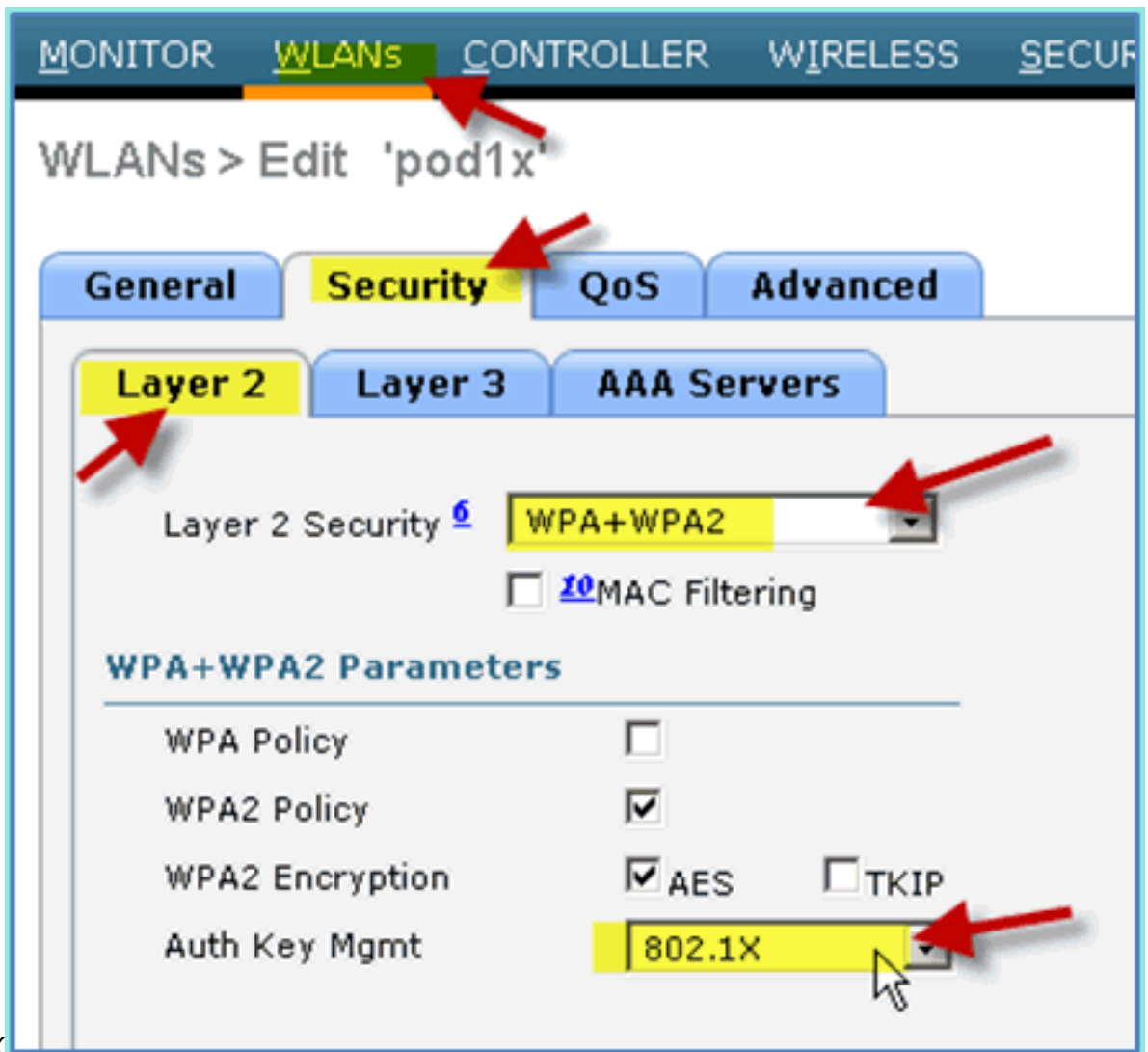
MONITOR WLANS CONTROLLER WIRELESS SECURITY

WLANs > Edit 'pod1x'

**General** Security QoS Advanced

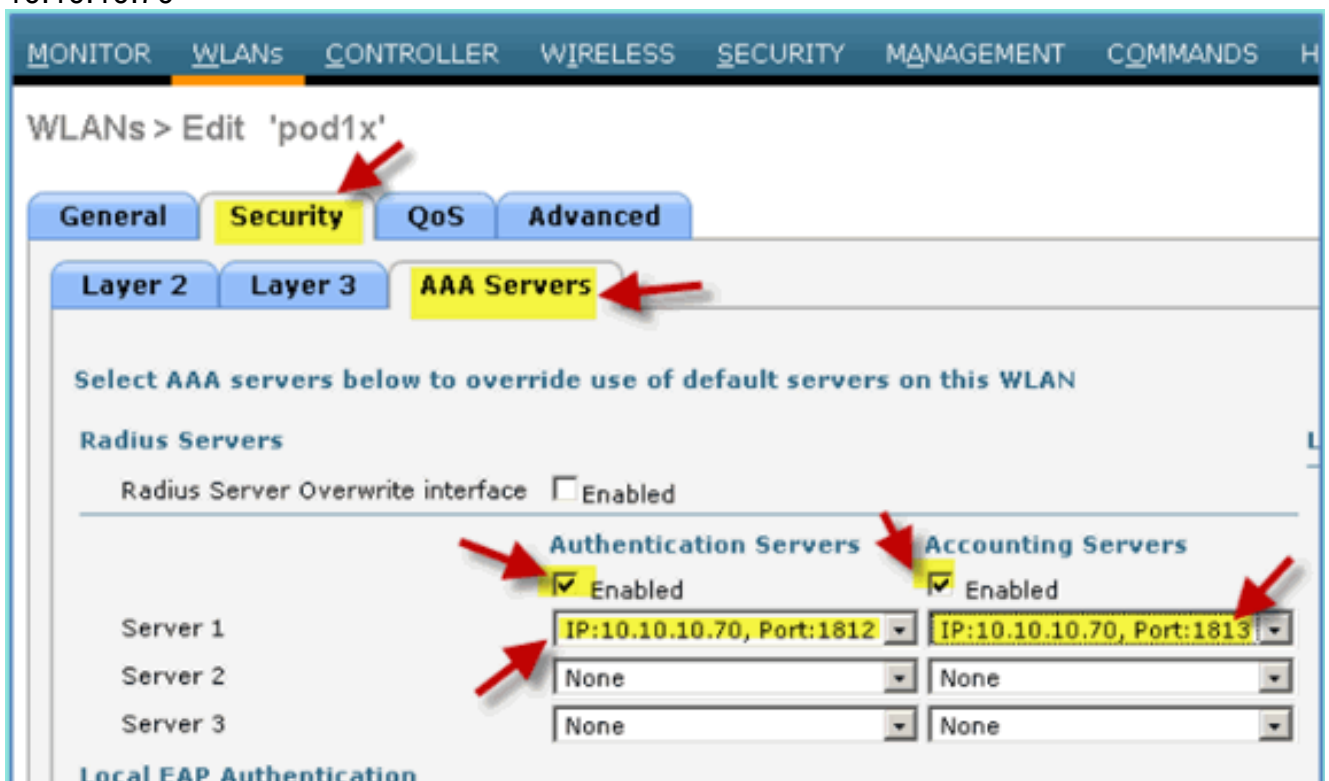
Profile Name	pod1x
Type	WLAN
SSID	pod1x
Status	<input type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab w
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

4. Legen Sie auf der Registerkarte WLAN > Security (WLAN > Sicherheit) > Layer 2 die folgenden Einstellungen fest: Layer-2-Sicherheit: WPA+WPA2 WPA2-Richtlinie/Verschlüsselung: Aktiviert/AES Verwaltung von Authentifizierungsschlüsseln:



802.1X

5. Legen Sie auf der Registerkarte WLAN > Security > AAA Servers Folgendes fest:Überschreibsstelle des Funkservers: DeaktiviertAuthentifizierungs-  
/Buchungsserver: AktiviertServer 1:  
10.10.10.70



6. Legen Sie auf der Registerkarte WLAN > Advanced (WLAN > Erweitert) Folgendes fest:AAA-  
Außerkräftsetzung zulassen: aktiviertNAC-Status: Radius NAC  
(ausgewählt)

MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs > Edit 'pod1x'

General Security QoS **Advanced**

**Allow AAA Override**  Enabled

Coverage Hole Detection  Enabled

Enable Session Timeout  1800  
Session Timeout (secs)

Aironet IE  Enabled

Diagnostic Channel  Enabled

IPv6 Enable

Override Interface ACL

P2P Blocking Action

Client Exclusion  Enabled 60  
Timeout Value (secs)

Maximum Allowed Clients

Static IP Tunneling  Enabled

**DHCP**

DHCP Server  Override

DHCP Addr. Assignment  Required

**Management Frame Protection (MFP)**

MFP Client Protection

**DTIM Period (in beacon intervals)**

802.11a/n (1 - 255)

802.11b/g/n (1 - 255)

**NAC**

NAC State

Load Balancing and Band Select

7. Zurück zur Registerkarte WLAN > Allgemein > WLAN aktivieren  
(Kontrollkästchen).

WLANs > Edit 'pod1x'

**General** Security QoS Advanced

Profile Name	pod1x
Type	WLAN
SSID	pod1x
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab)
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

## Dynamische WLC-Schnittstellen testen

Prüfen Sie schnell, ob die Benutzeroberflächen für Mitarbeiter und Gäste gültig sind. Verwenden Sie ein beliebiges Gerät, um eine Verbindung mit dem WLAN herzustellen, und ändern Sie dann die Zuweisung der WLAN-Schnittstelle.

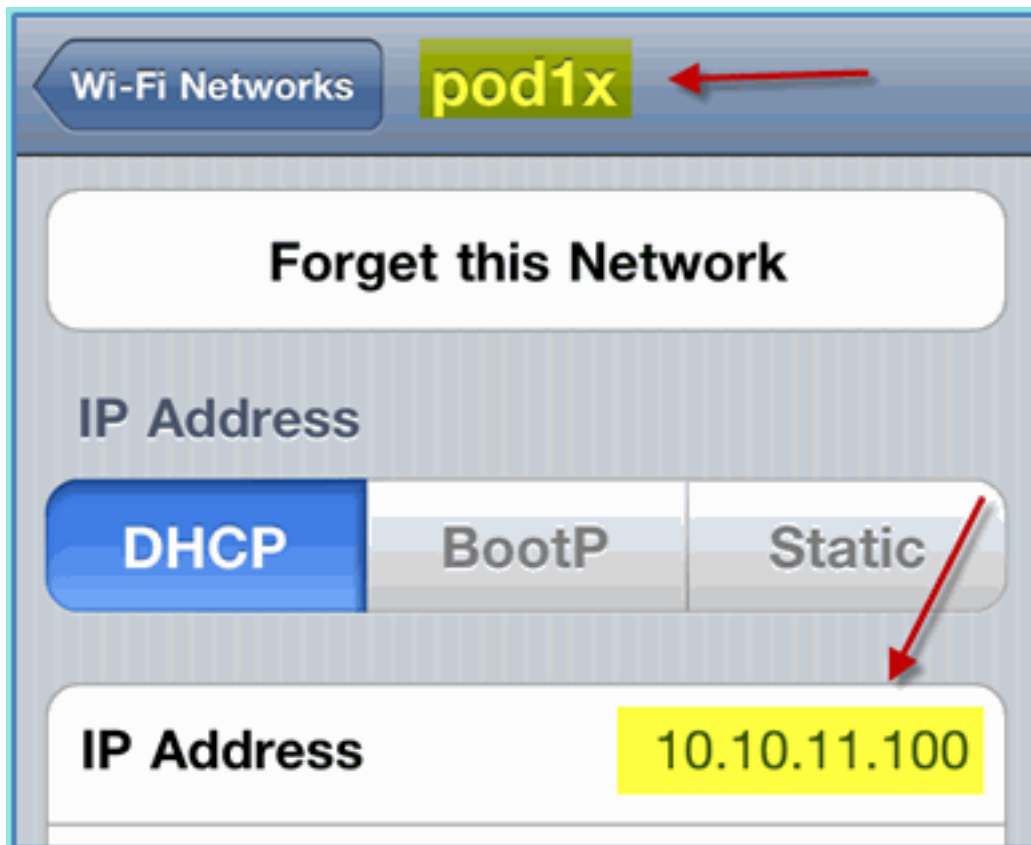
1. Navigieren Sie vom WLC zu **WLAN > WLANs**. Klicken Sie hier, um die in der vorherigen Übung erstellte sichere SSID zu bearbeiten.
2. Ändern Sie Interface/Interface Group (Schnittstelle/Schnittstellengruppe) in **Employee**, und klicken Sie dann auf **Apply**.

The screenshot shows the Cisco configuration interface for a WLAN profile named 'pod1x'. The interface is divided into several sections:

- Navigation:** At the top, there are tabs for 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', and 'SECURITY'. The 'WLANs' tab is selected and highlighted in green. A red arrow points to this tab.
- Left Panel:** A tree view shows 'WLANs' expanded, with 'WLANs' and 'Advanced' sub-items. The 'WLANs' sub-item is highlighted in yellow, and a red arrow points to it.
- Header:** The main header reads 'WLANs > Edit 'pod1x''. The 'pod1x' text is highlighted in yellow.
- Tabs:** Below the header are tabs for 'General', 'Security', 'QoS', and 'Advanced'. The 'General' tab is selected and highlighted in yellow, with a red arrow pointing to it.
- Configuration Fields:**
  - Profile Name:** pod1x
  - Type:** WLAN
  - SSID:** pod1x
  - Status:**  Enabled
  - Security Policies:** [WPA2][Auth(802.1X)] (Modifications done under security to)
  - Radio Policy:** All (dropdown menu)
  - Interface/Interface Group(G):** management (dropdown menu). This dropdown is open, showing options: 'management' (selected), 'employee', 'guest', and 'management'. A red arrow points to the 'employee' option, and a mouse cursor is hovering over it.
  - Multicast Vlan Feature:** guest
  - Broadcast SSID:**  Enabled

3. Bei ordnungsgemäßer Konfiguration erhält ein Gerät eine IP-Adresse vom Mitarbeiter-VLAN (10.10.11.0/24). Dieses Beispiel zeigt ein iOS-Gerät, das eine neue IP-Adresse





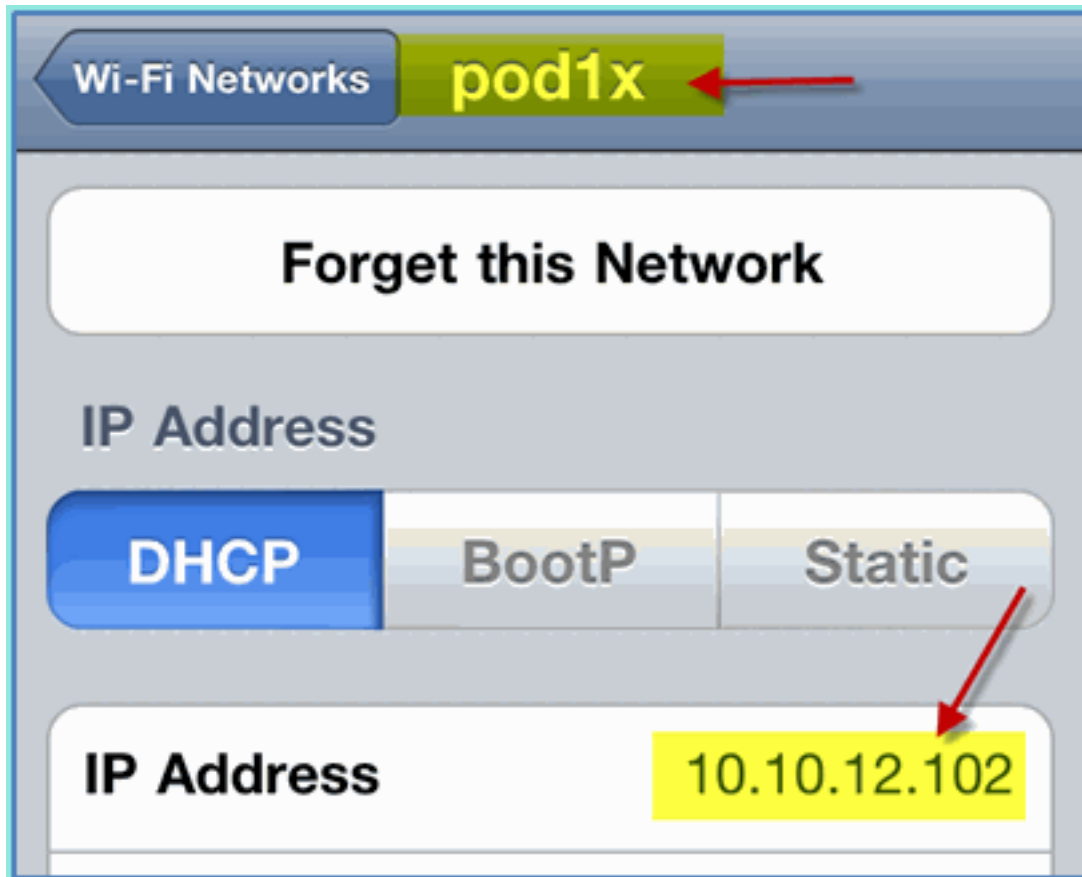
erhält.

4. Nachdem die vorherige Schnittstelle bestätigt wurde, ändern Sie die WLAN-Schnittstellenzuweisung zu **Gast**, und klicken Sie dann auf **Anwenden**.

The screenshot displays the Cisco WLAN configuration page. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', and 'WIRELESS'. The main content area is titled 'WLANs > Edit 'pod1x''. Below this, there are four tabs: 'General', 'Security', 'QoS', and 'Advanced'. The 'General' tab is active. The configuration details are as follows:

Profile Name	pod1x
Type	WLAN
SSID	pod1x
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under se
Radio Policy	All
Interface/Interface Group(G)	quest
Multicast Vlan Feature	quest
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

5. Bei ordnungsgemäßer Konfiguration erhält ein Gerät eine IP-Adresse vom Gast-VLAN (10.10.12.0/24). Dieses Beispiel zeigt ein iOS-Gerät, das eine neue IP-Adresse



erhält.

6. **WICHTIG:** Ändern Sie die Schnittstellenzuweisung wieder in das ursprüngliche Management.
7. Klicken Sie auf **Apply** (Anwenden), und speichern Sie die Konfiguration für den WLC.

## [Wireless-Authentifizierung für iOS \(iPhone/iPad\)](#)

Verknüpfen Sie dem WLC über eine authentifizierte SSID einen INTERNEN Benutzer (oder integrierten AD-Benutzer) mit einem iOS-Gerät wie einem iPhone, iPad oder iPod. Überspringen Sie diese Schritte, falls nicht zutreffend.

1. Navigieren Sie auf dem iOS-Gerät zu den WLAN-Einstellungen. Aktivieren Sie WIFI, und wählen Sie dann die im vorherigen Abschnitt erstellte 802.1X-fähige SSID aus.
2. Geben Sie diese Informationen an, um eine Verbindung herzustellen: Benutzername:  
Mitarbeiter (intern - Mitarbeiter) oder Subunternehmer (intern - Subunternehmer) Kennwort:



XXXX

3. Klicken Sie auf, um das ISE-Zertifikat zu



akzeptieren.

4. Vergewissern Sie sich, dass das iOS-Gerät eine IP-Adresse von der Verwaltungsschnittstelle



(VLAN10) erhält.

- Überprüfen Sie auf WLC > Monitor > Clients die Endgeräteinformationen einschließlich Verwendung, Status und EAP-Typ.

The screenshot shows the Cisco ISE Monitor interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', and 'WIRELESS'. The left sidebar contains a menu with 'Monitor' selected, and sub-items: 'Summary', 'Access Points', 'Cisco CleanAir', 'Statistics', 'CDP', 'Rogues', 'Clients', and 'Multicast'. The main content area is titled 'Clients > Detail' and is divided into two sections: 'Client Properties' and 'Security Information'.

**Client Properties**

MAC Address	5c:59:48:40:82:8d
IP Address	10.10.10.102
Client Type	Regular
User Name	aduser
Port Number	1
Interface	management
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No

**Security Information**

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	PEAP
SNMP NAC State	Access
Radius NAC State	RUN

AAA Override ACL Name none



6. Ebenso können die Client-Informationen über die Seite ISE > Monitor > Authentication (ISE > Monitor > Authentifizierung) bereitgestellt werden.

**CISCO Identity Services Engine**

Home Monitor Policy Administration

Authentications Alarms Reports Troubleshoot

Add or Remove Columns Refresh

Time	Status	Details	Username	Endpoint ID	Network Device	Authorization Profiles	Ident
Jul 13,11 04:39:36.573 PM	✓		aduser	5C:59:48:40:82:8D	WLC	PermitAccess	
Jul 13,11 04:38:46.285 PM	✓		aduser	5C:59:48:40:82:8D	WLC	PermitAccess	

7. Klicken Sie auf das Symbol **Details**, um detaillierte Informationen zur Sitzung anzuzeigen.

**CISCO Identity Services Engine**

Showing Page 1 of 1 | First Prev

### AAA Protocol > RADIUS Authentication Detail

RADIUS Audit Session ID : 0a0a0a050000000d4e1e2a45  
 AAA session ID : ise/99967658/11  
 Date : July 13,2011

Generated on July 13, 2011 4:41:11 PM PDT

#### Authentication Summary

Logged At:	July 13,2011 4:39:36.573 PM
<b>RADIUS Status:</b>	<b>Authentication succeeded</b>
NAS Failure:	
Username:	<u>aduser</u>
MAC/IP Address:	<u>5C:59:48:40:82:8D</u>
Network Device:	<u>WLC : 10.10.10.5 :</u>
Allowed Protocol:	<u>Default Network Access</u>
Identity Store:	AD1
Authorization Profiles:	PermitAccess
SGA Security Group:	
<b>Authentication Protocol :</b>	<b>PEAP(EAP-MSCHAPv2)</b>



## Statusumleitungszugriffskontrollliste zu WLC hinzufügen

Die Zugriffskontrollliste für die Statusumleitung wird auf dem WLC konfiguriert, über den die ISE den Client auf den Status beschränkt. Effektiv und mindestens lässt die ACL den Datenverkehr zwischen der ISE zu. Optionale Regeln können dieser ACL bei Bedarf hinzugefügt werden.

1. Navigieren Sie zu **WLC > Security > Access Control Lists > Access Control Lists**. Klicken Sie auf **Neu**.



2. Geben Sie einen Namen (ACL-POSTURE-REDIRECT) für die ACL ein.



3. Klicken Sie für die neue ACL auf **Add New Rule (Neue Regel hinzufügen)**. Legen Sie die folgenden Werte auf die ACL-Sequenz #1 fest. Klicken Sie abschließend auf **Apply**. Quelle: BeliebigZiel: IP-Adresse 10.10.10.70, 255.255.255.255Protokoll: BeliebigAktion: Zulassen

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

### Access Control Lists > Rules > Edit

Sequence:

Source:

Destination:  IP Address:  Netmask:

Protocol:

DSCP:

Direction:

Action:

4. Die Bestätigungssequenz wurde hinzugefügt.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any	0

5. Klicken Sie auf **Neue Regel hinzufügen**. Legen Sie die folgenden Werte auf die ACL-Sequenz #2 fest. Klicken Sie abschließend auf **Apply**. Quelle: IP-Adresse 10.10.10.70, 255.255.255.255 Ziel: Beliebig Protokoll: Beliebig Aktion: Zulassen

Sequence:

Source:  IP Address:  Netmask:

Destination:

Protocol:

DSCP:

Direction:

Action:

6. Die Bestätigungssequenz wurde hinzugefügt.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
<u>1</u>	Permit	0.0.0.0 /	10.10.10.70 /	Any	Any	Any	Any	Any
		0.0.0.0 /	255.255.255.255					
<u>2</u>	Permit	10.10.10.70 /	0.0.0.0 /	Any	Any	Any	Any	Any
		255.255.255.255 /	0.0.0.0					

7. Legen Sie die folgenden Werte auf die ACL-Sequenz #3 fest. Klicken Sie abschließend auf **Apply**. Quelle: BeliebigZiel: BeliebigProtokoll: UDPQuelleport: DNSZielport: BeliebigAktion:

The screenshot shows the configuration interface for ACL sequence #3. Red arrows point to the following fields:

- Sequence: 3
- Source: Any
- Destination: Any
- Protocol: UDP
- Source Port: DNS
- Destination Port: Any
- DSCP: Any
- Direction: Any
- Action: Permit

Zulassen

8. Die Bestätigungssequenz wurde hinzugefügt.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
<u>1</u>	Permit	0.0.0.0 /	10.10.10.70 /	Any	Any	Any	Any	Any
		0.0.0.0 /	255.255.255.255					
<u>2</u>	Permit	10.10.10.70 /	0.0.0.0 /	Any	Any	Any	Any	Any
		255.255.255.255 /	0.0.0.0					
<u>3</u>	Permit	0.0.0.0 /	0.0.0.0 /	UDP	DNS	Any	Any	Any
		0.0.0.0 /	0.0.0.0					

9. Klicken Sie auf **Neue Regel hinzufügen**. Legen Sie die folgenden Werte auf die ACL-Sequenz #4 fest. Klicken Sie abschließend auf **Apply**. Quelle: BeliebigZiel: BeliebigProtokoll:

UDPQuell-Port: BeliebigZielport: DNSAktion:  
Zulassen

Sequence: 4

Source: Any

Destination: Any

Protocol: UDP

Source Port: Any

Destination Port: DNS

DSCP: Any

Direction: Any

Action: Permit

10. Die Bestätigungssequenz wurde hinzugefügt.

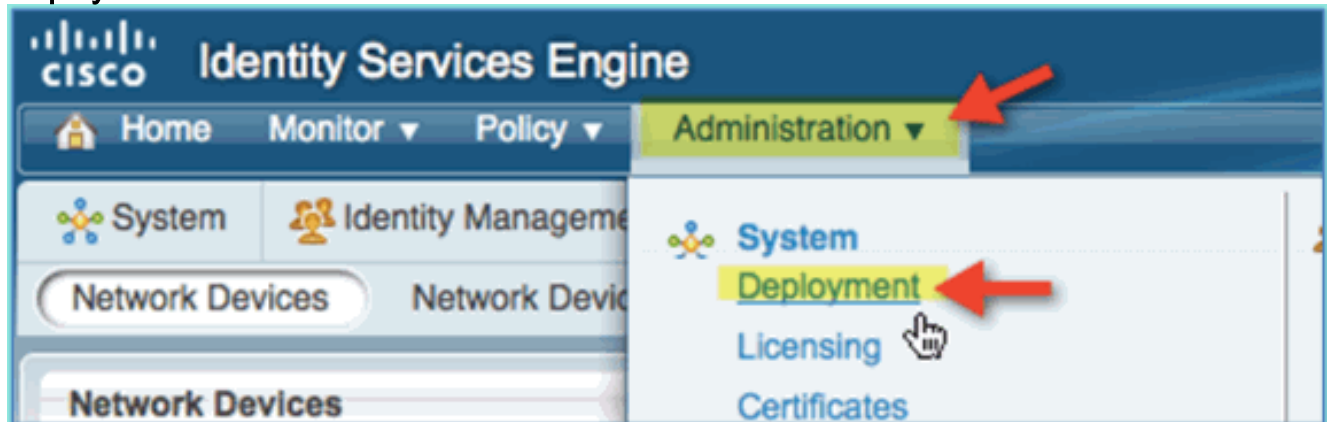
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
<a href="#">1</a>	Permit	0.0.0.0 /	10.10.10.70 /	Any	Any	Any	Any	Any
<a href="#">2</a>	Permit	0.0.0.0 /	255.255.255.255 /	Any	Any	Any	Any	Any
<a href="#">3</a>	Permit	10.10.10.70 /	0.0.0.0 /	Any	Any	Any	Any	Any
<a href="#">4</a>	Permit	255.255.255.255 /	0.0.0.0 /	UDP	DNS	Any	Any	Any
<a href="#">4</a>	Permit	0.0.0.0 /	0.0.0.0 /	UDP	Any	DNS	Any	Any
		0.0.0.0 /	0.0.0.0 /					

11. Speichern der aktuellen WLC-Konfiguration

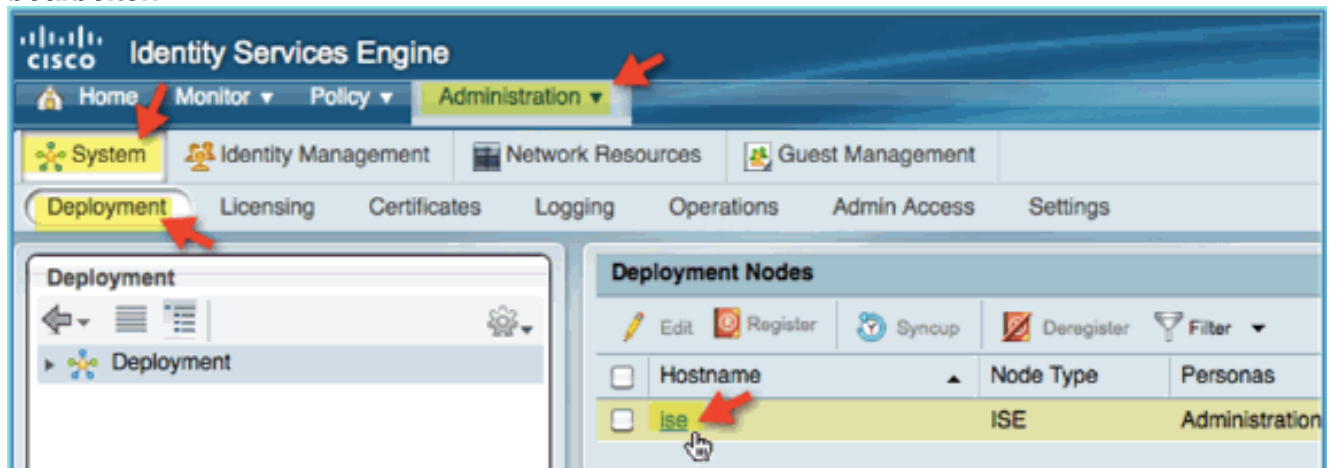
## [Profilerstellungssonden auf ISE aktivieren](#)

Die ISE muss als Tests konfiguriert werden, um Endpunkte effektiv zu profilieren. Standardmäßig sind diese Optionen deaktiviert. In diesem Abschnitt wird erläutert, wie die ISE als Sonden konfiguriert wird.

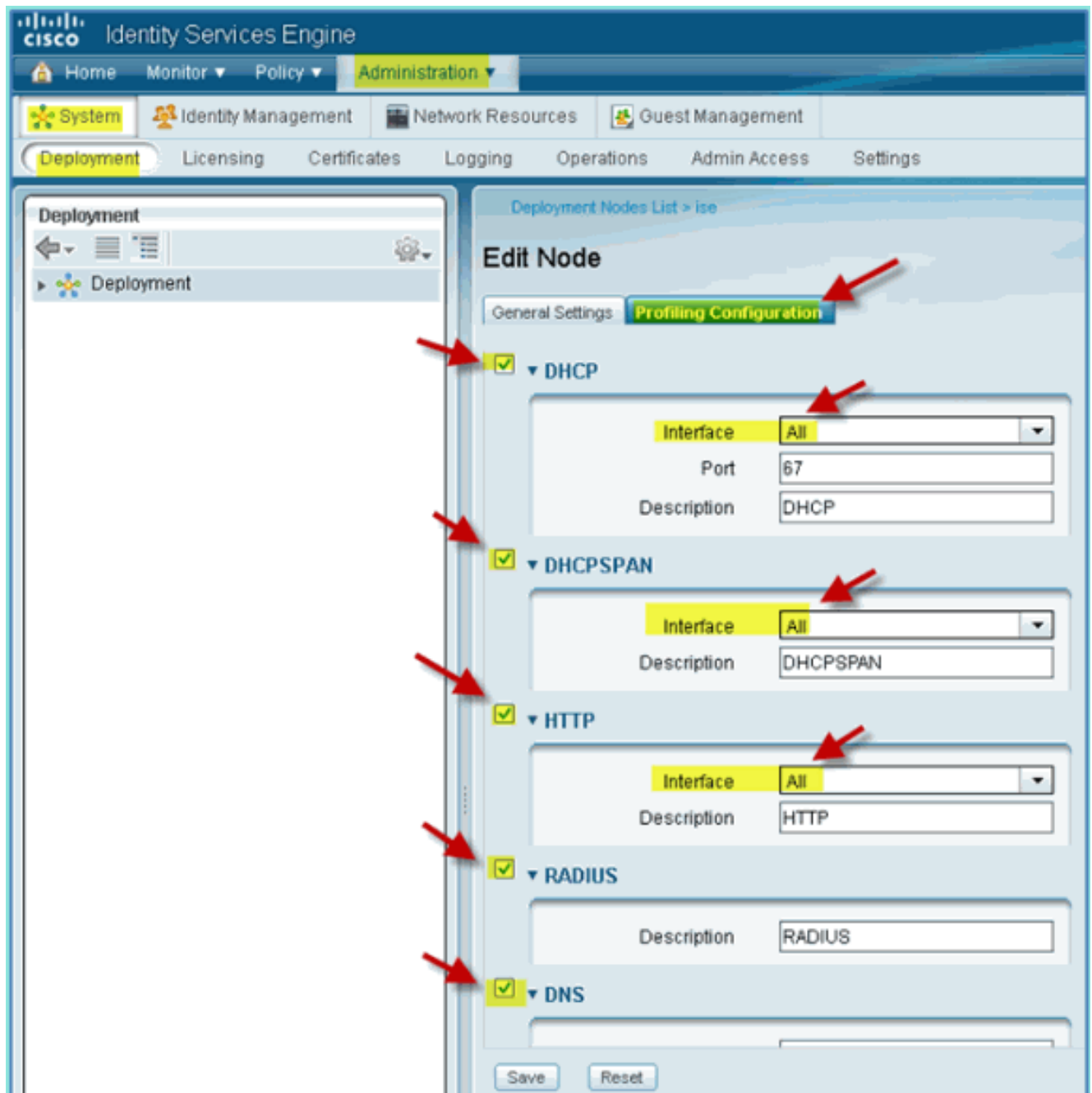
1. Navigieren Sie von der ISE-Verwaltung zu **Administration > System > Deployment**.



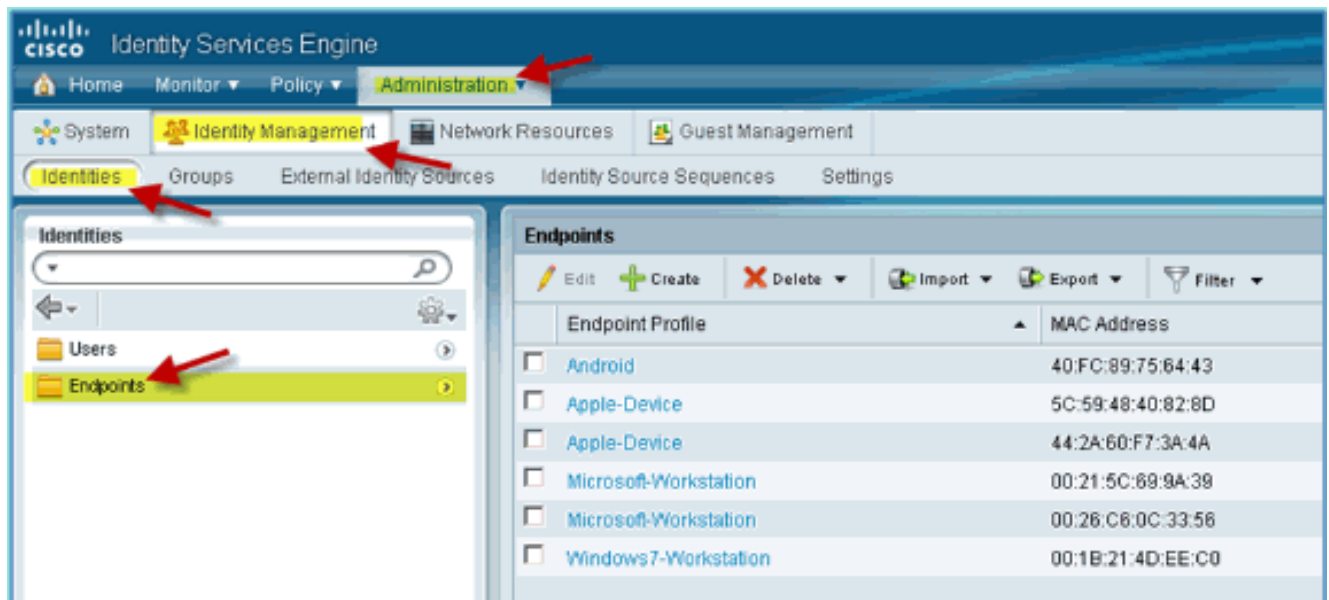
2. Wählen Sie **ISE**. Klicken Sie auf **ISE-Host bearbeiten**.



3. Wählen Sie auf der Seite "Knoten bearbeiten" die Profilkonfiguration aus, und konfigurieren Sie Folgendes: DHCP: Aktiviert, Alle (oder Standard) DHCPSPAN: Aktiviert, Alle (oder Standard) HTTP: Aktiviert, Alle (oder Standard) RADIUS: Aktiviert, k. A. DNS: Aktiviert, k. A.



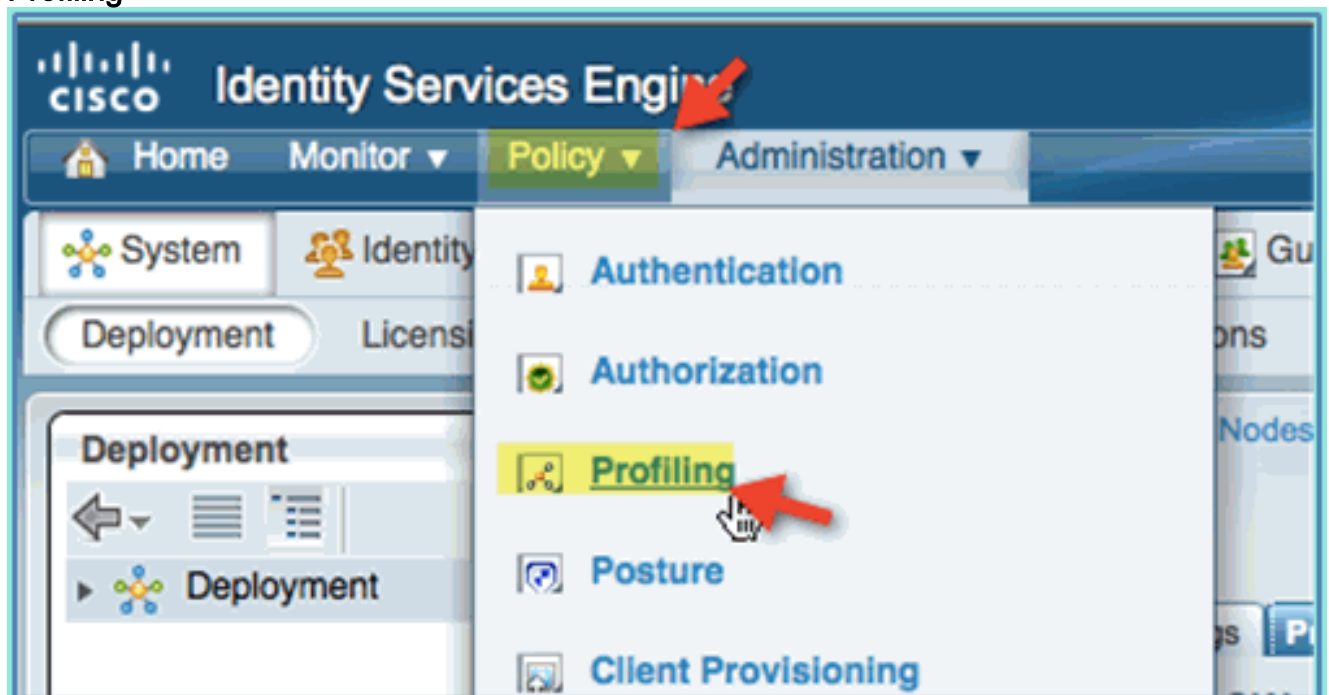
4. Verbinden Sie die Geräte erneut (iPhone/iPads/Droids/Mac usw.).
5. Bestätigen Sie die ISE-Endgeräteidentitäten. Navigieren Sie zu **Administration > Identity Management > Identities**. Klicken Sie auf Endpunkte, um die Profilerstellung aufzulisten. **Hinweis:** Die erste Profilerstellung stammt von RADIUS-Tests.



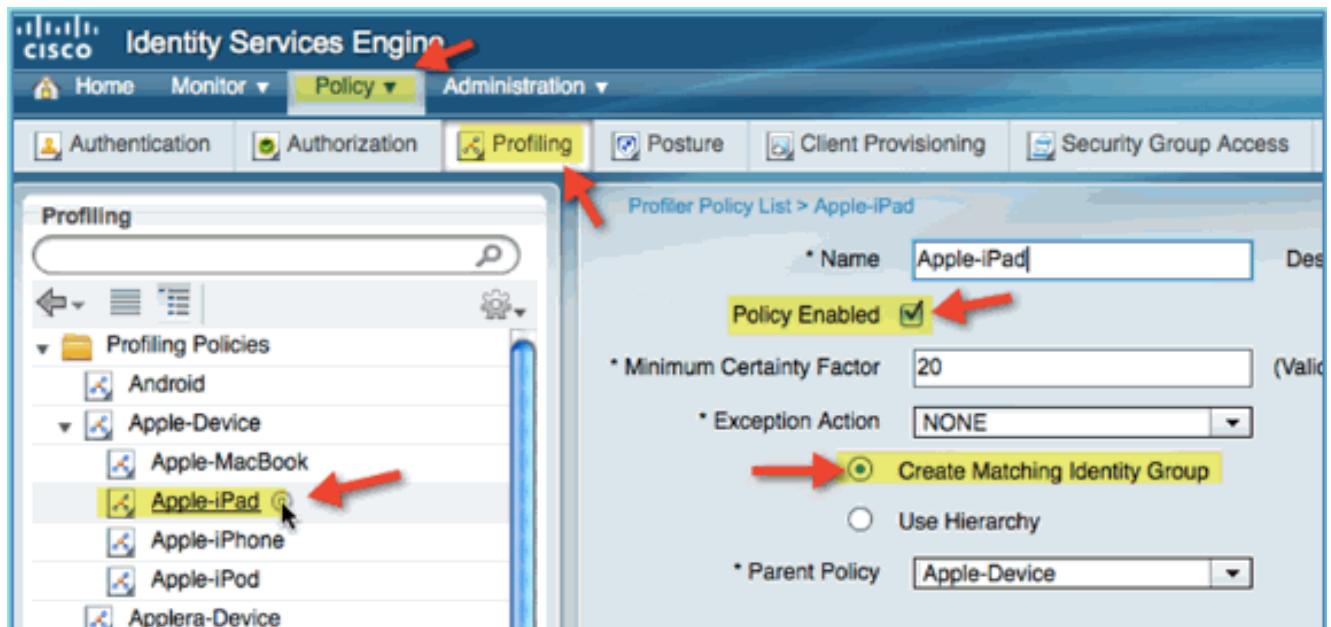
## Aktivieren von ISE-Profilrichtlinien für Geräte

Die ISE bietet eine Bibliothek mit verschiedenen Endgeräteprofilen. Gehen Sie wie folgt vor, um Geräteprofile zu aktivieren:

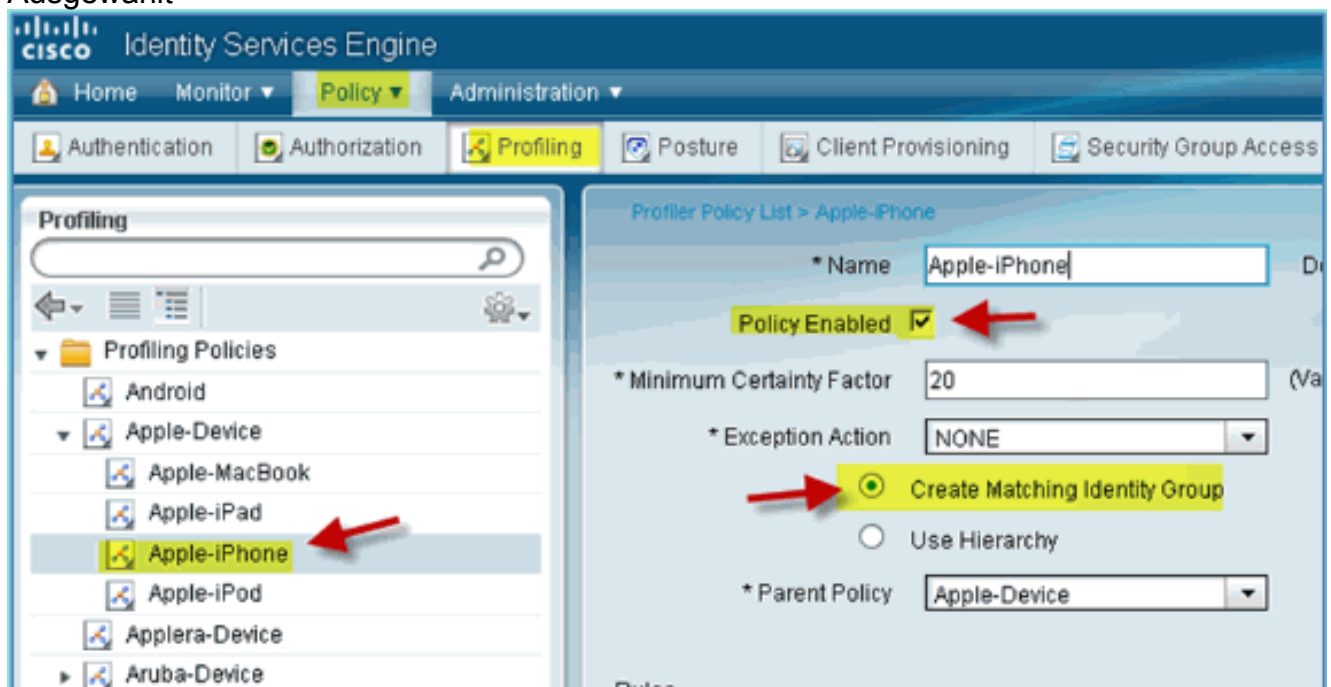
1. Navigieren Sie von der ISE zu **Richtlinie > Profiling**.



2. Erweitern Sie im linken Bereich die Option **Profiling Policies (Profilrichtlinien)**.
3. Klicken Sie auf **Apple Device > Apple iPad**, und legen Sie Folgendes fest:
  - Richtlinie aktiviert:
  - Aktiviert
  - Passende Identitätsgruppe erstellen:
  - Ausgewählt

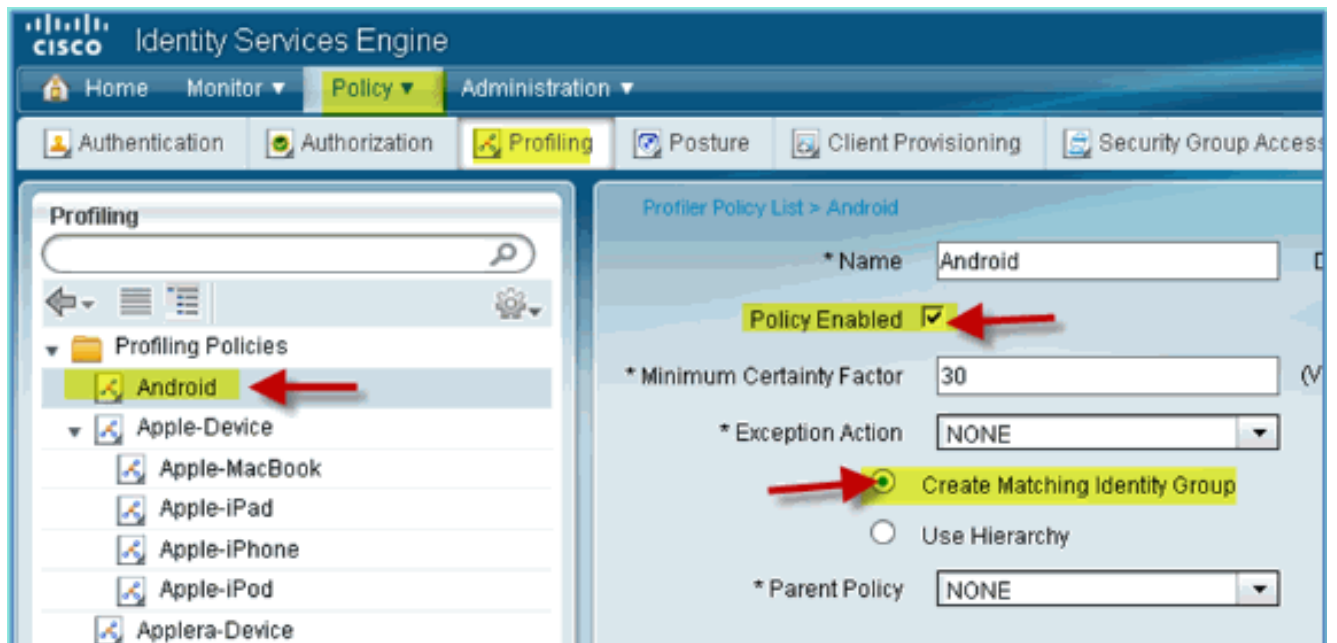


4. Klicken Sie auf **Apple Device > Apple iPhone**, und legen Sie Folgendes fest: Richtlinie aktiviert: Aktiviert  
 Passende Identitätsgruppe erstellen:  
 Ausgewählt



5. Klicken Sie auf **Android**, legen Sie Folgendes fest: Richtlinie aktiviert: Aktiviert  
 Passende Identitätsgruppe erstellen:  
 Ausgewählt





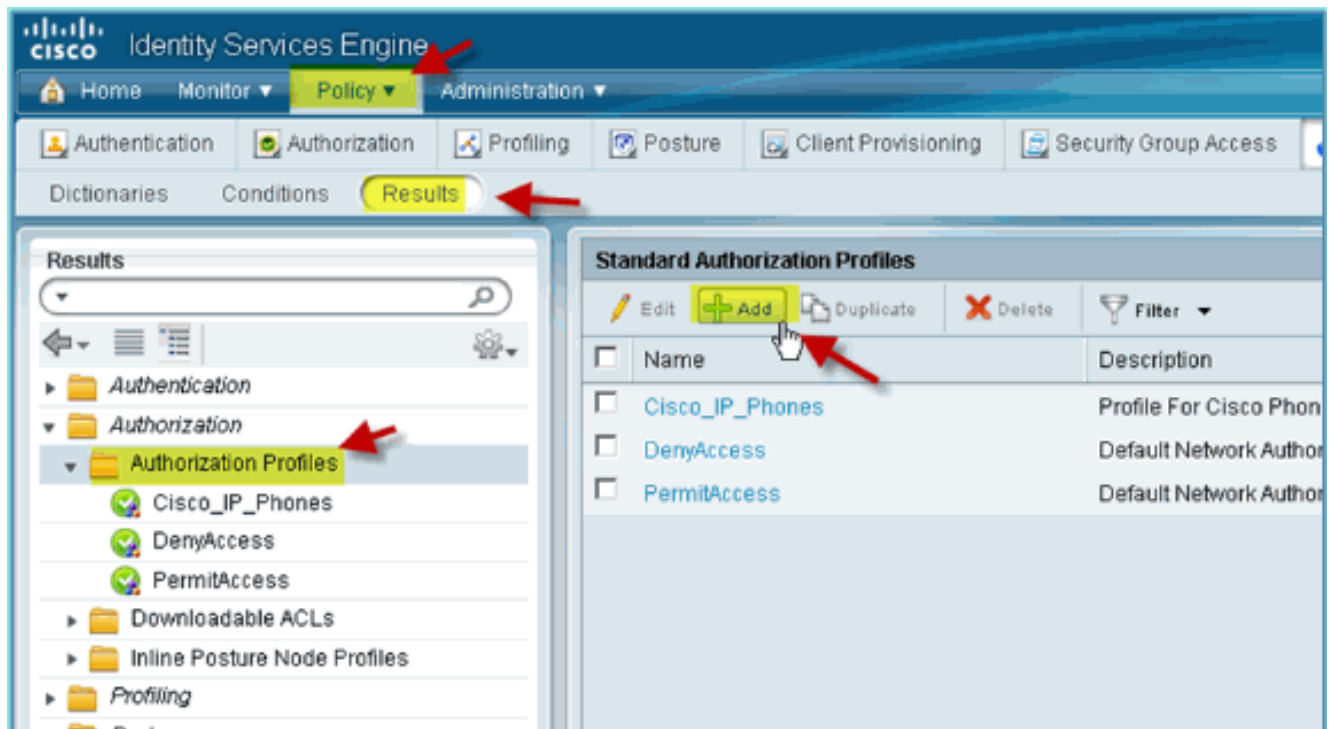
## ISE-Autorisierungsprofil für die Statuserkennung - Umleitung

Gehen Sie wie folgt vor, um eine Autorisierungsrichtlinienstatus-Umleitung zu konfigurieren, die es ermöglicht, neue Geräte zur ordnungsgemäßen Erkennung und Profilierung an die ISE umzuleiten:

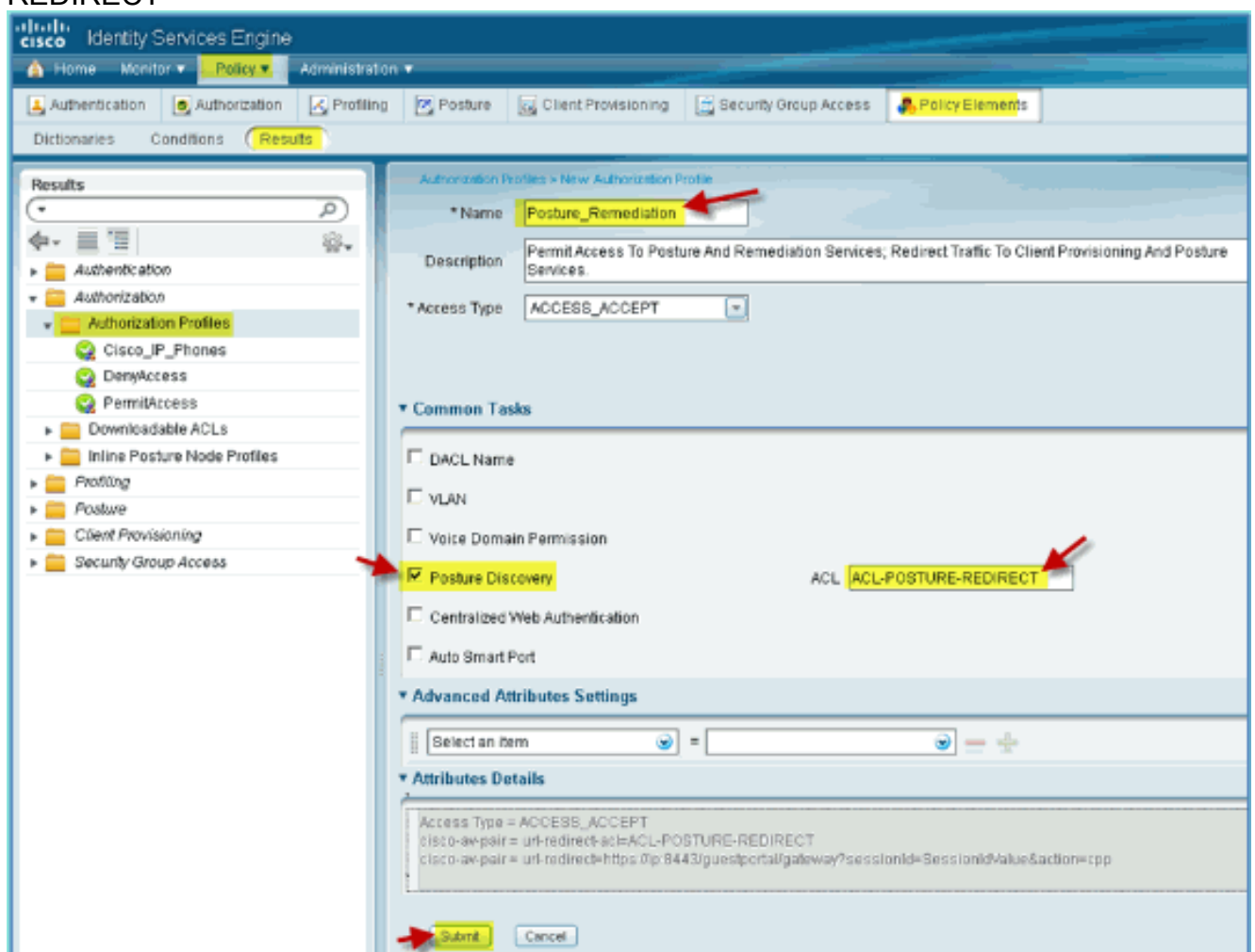
1. Navigieren Sie von der ISE zu **Richtlinie > Richtlinienelemente > Ergebnisse**.



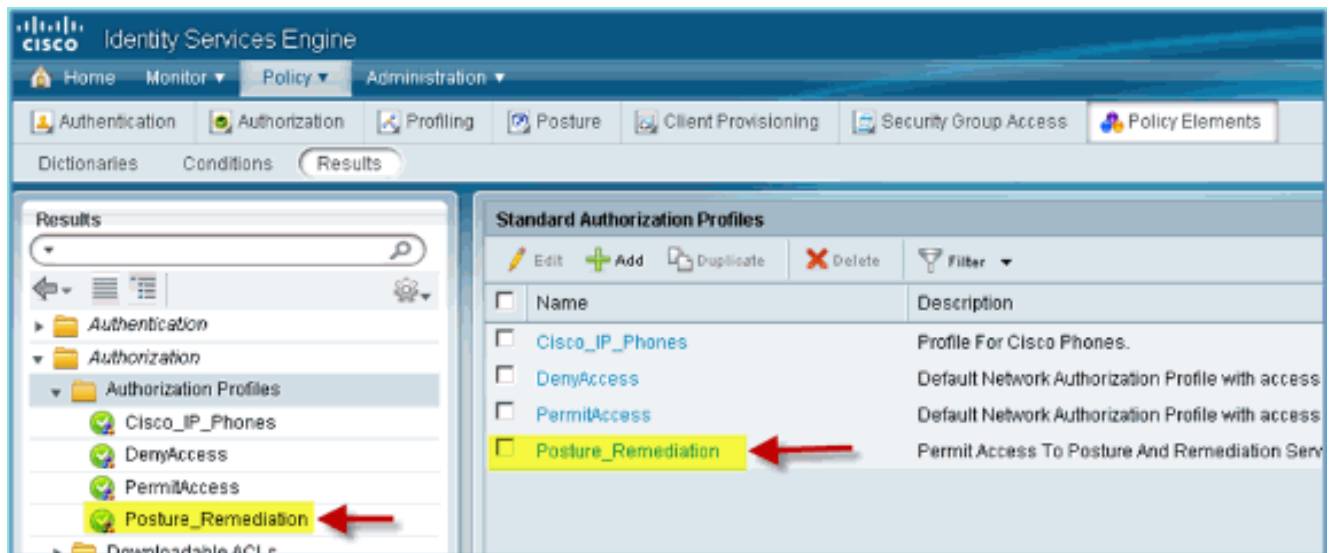
2. Erweitern Sie **Autorisierung**. Klicken Sie auf **Autorisierungsprofile** (linker Bereich) und dann auf **Hinzufügen**.



- Erstellen Sie das Autorisierungsprofil mit folgenden Informationen: Name: Posture\_RemediationZugriffstyp: Access\_AcceptAllgemeine Tools:Statuserkennung, aktiviertStatuserkennung, ACL ACL-POSTURE-REDIRECT



- Klicken Sie auf **Senden**, um diese Aufgabe abzuschließen.
- Bestätigen Sie, dass das neue Autorisierungsprofil hinzugefügt wurde.

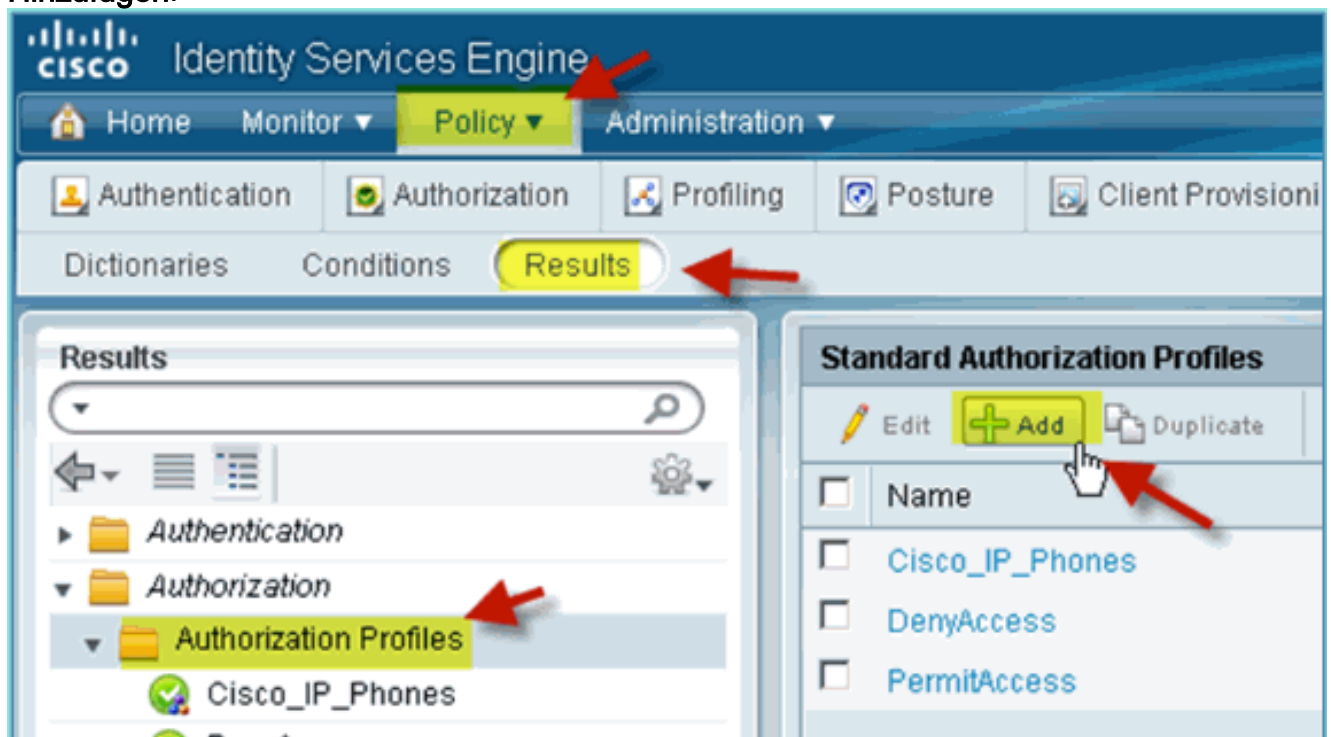


## ISE-Autorisierungsprofil für Mitarbeiter erstellen

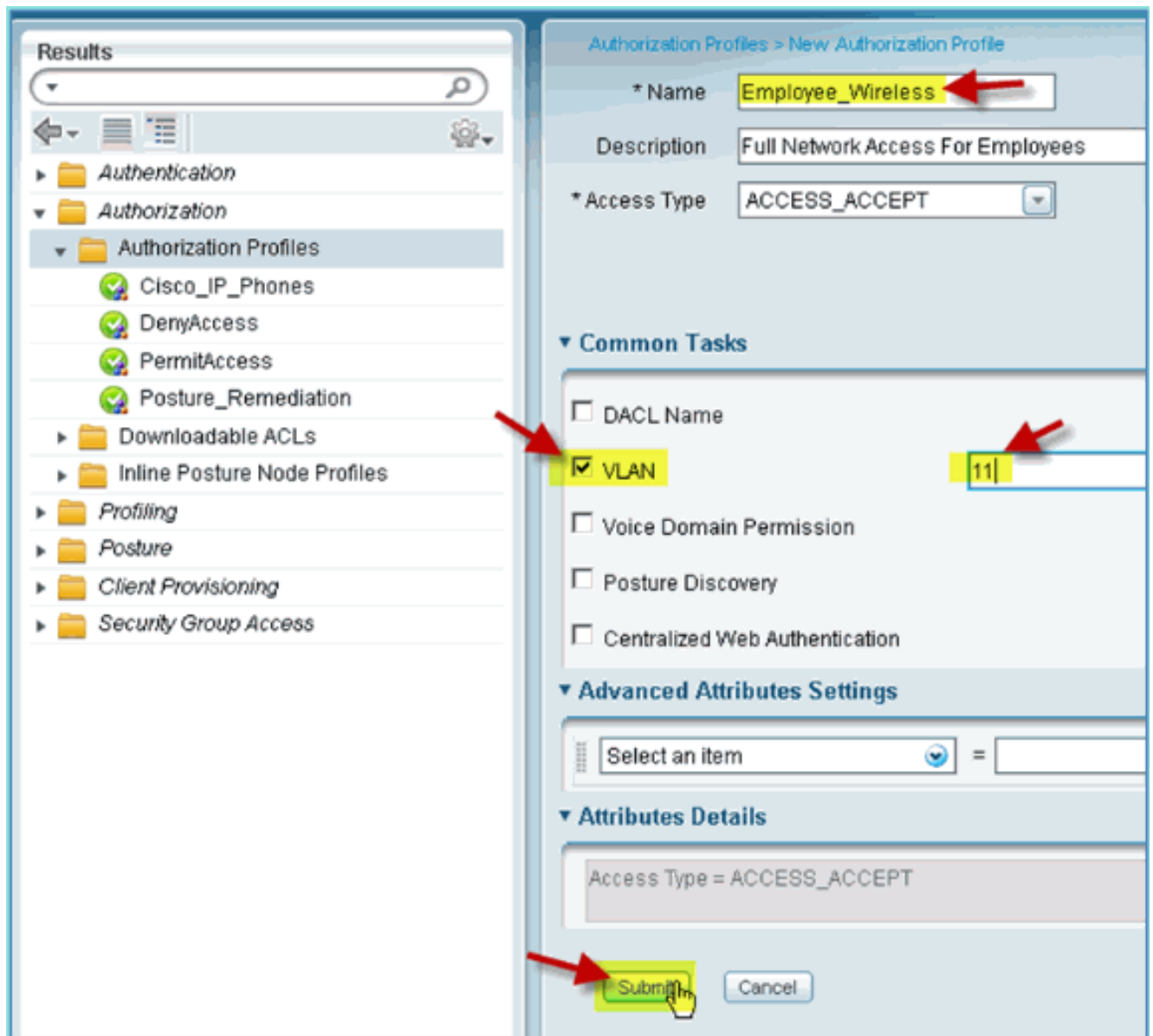
Durch das Hinzufügen eines Autorisierungsprofils für einen Mitarbeiter kann die ISE den Zugriff mit den zugewiesenen Attributen autorisieren und zulassen. Mitarbeiter-VLAN 11 ist in diesem Fall zugewiesen.

Führen Sie diese Schritte aus:

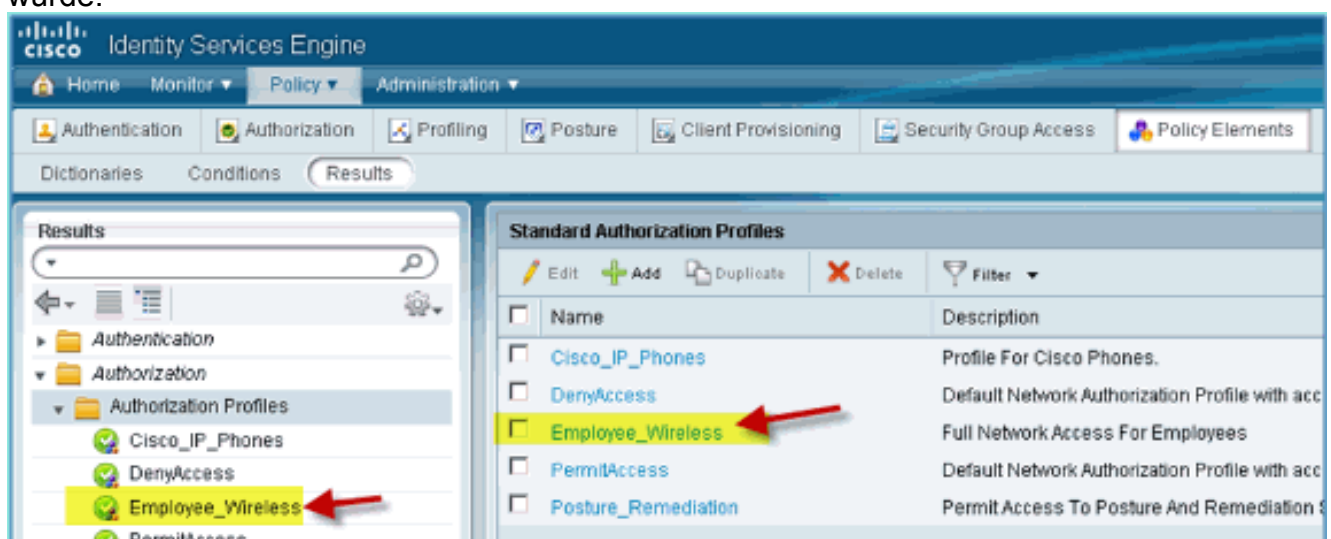
1. Navigieren Sie von der ISE zu **Richtlinie > Ergebnisse**. Erweitern Sie **Autorisierung**, klicken Sie dann auf **Autorisierungsprofile**, und klicken Sie auf **Hinzufügen**.



2. Geben Sie Folgendes für das Mitarbeiterautorisierungsprofil ein: Name: Employee\_WirelessAllgemeine Aufgaben:VLAN, aktiviertVLAN, Unterwert 11
3. Klicken Sie auf **Senden**, um diese Aufgabe abzuschließen.



4. Bestätigen Sie, dass das neue Mitarbeiterautorisierungsprofil erstellt wurde.



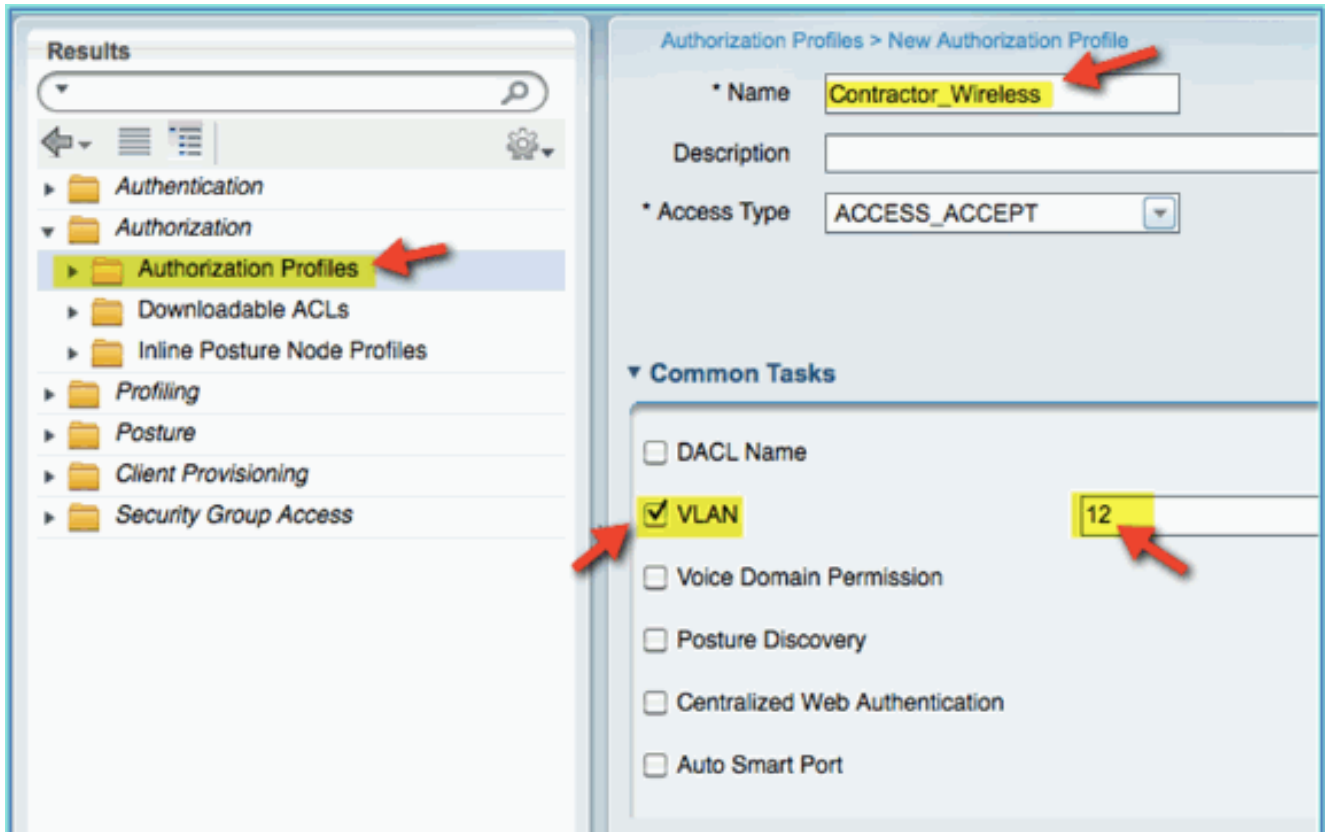
## ISE-Autorisierungsprofil für AN erstellen

Durch das Hinzufügen eines Autorisierungsprofils für einen Auftragnehmer kann die ISE den Zugriff mit den zugewiesenen Attributen autorisieren und zulassen. Contractor VLAN 12 ist in

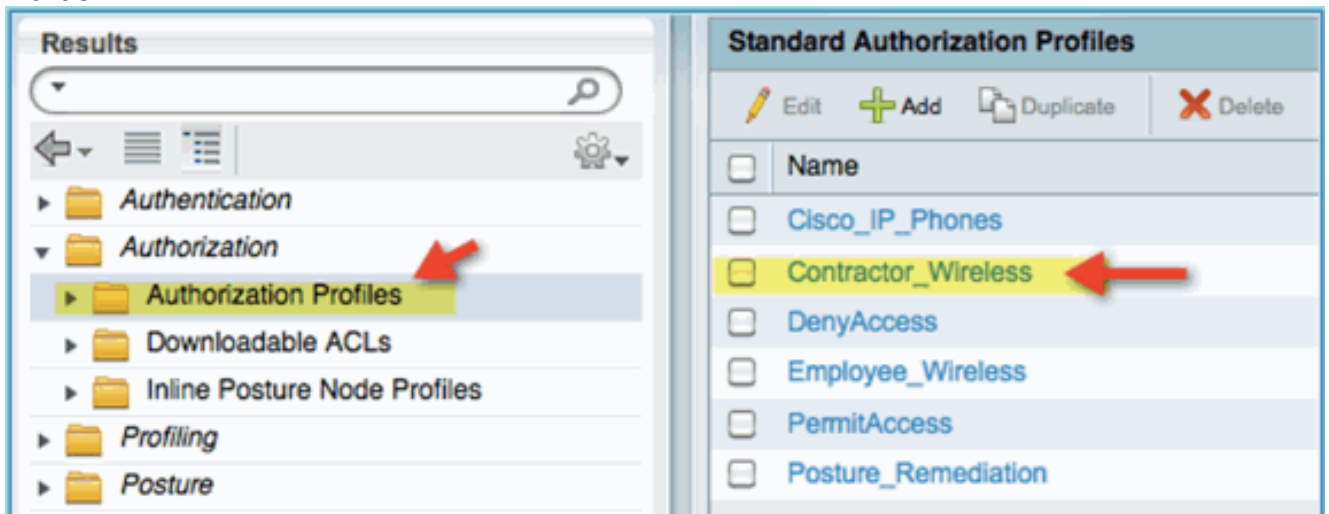
diesem Fall zugeordnet.

Führen Sie diese Schritte aus:

1. Navigieren Sie von der ISE zu **Richtlinie > Ergebnisse**. Erweitern Sie **Autorisierung**, klicken Sie dann auf **Autorisierungsprofile**, und klicken Sie auf **Hinzufügen**.
2. Geben Sie Folgendes für das Mitarbeiterautorisierungsprofil ein: Name: Employee\_WirelessAllgemeine Aufgaben:VLAN, aktiviertVLAN, Unterwert 12



3. Klicken Sie auf **Senden**, um diese Aufgabe abzuschließen.
4. Bestätigen Sie, dass das Auftragnehmer-Autorisierungsprofil erstellt wurde.



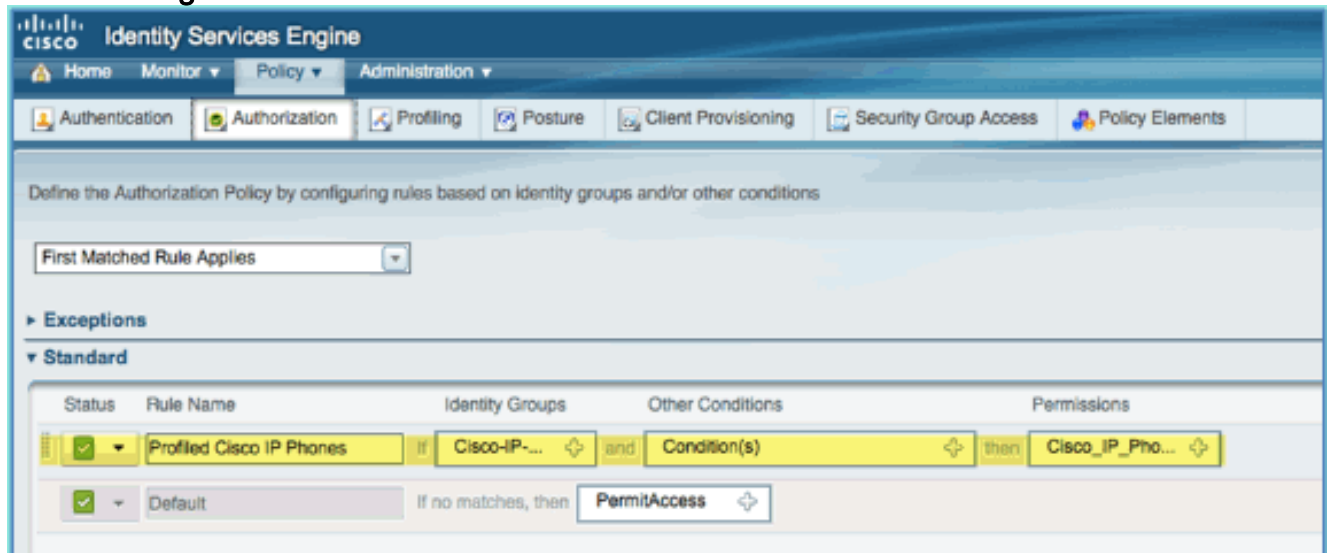
## [Autorisierungsrichtlinie für Gerätestatus/Profilierung](#)

Es sind nur wenige Informationen über ein neues Gerät bekannt, wenn es zum ersten Mal in das

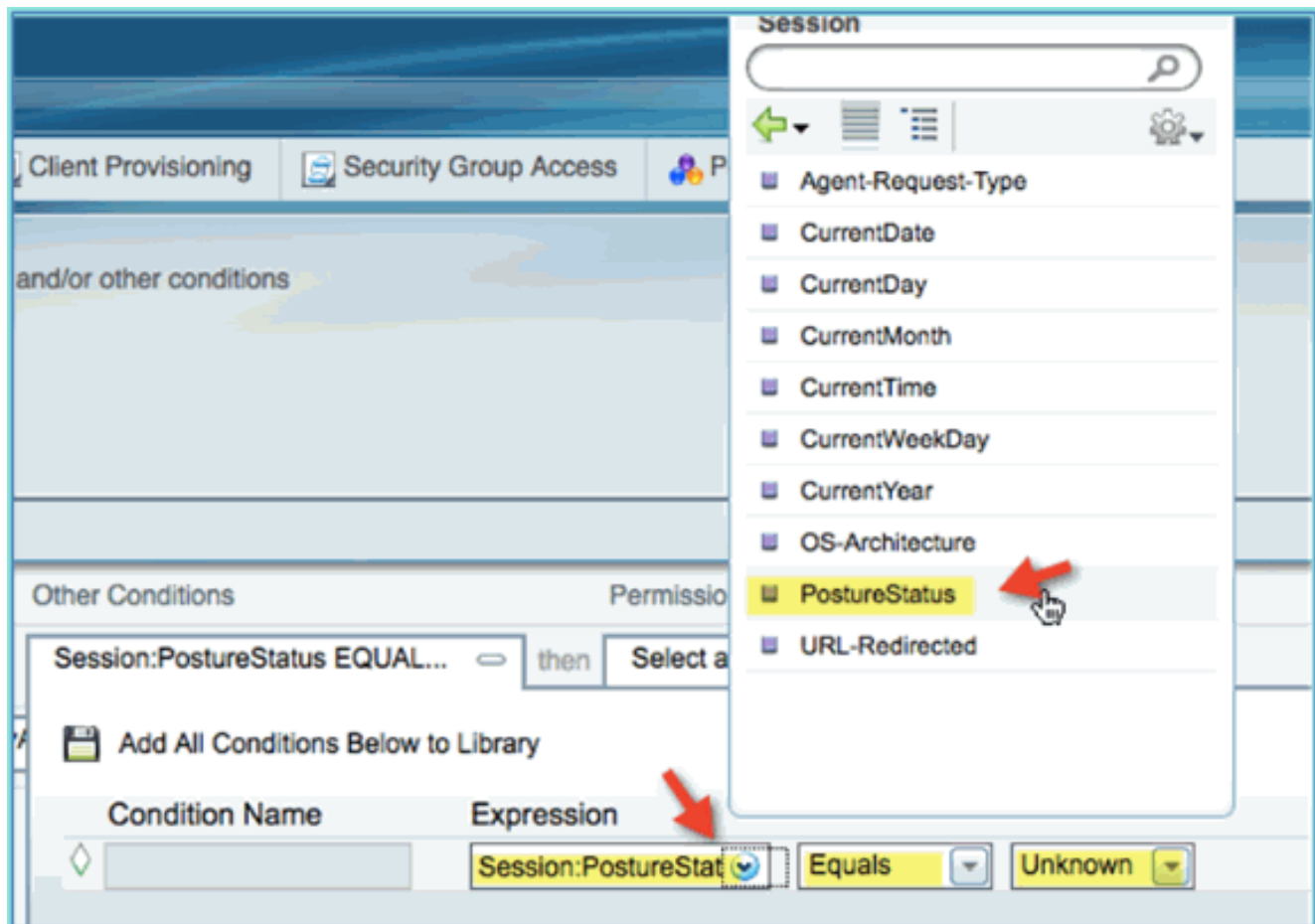
Netzwerk integriert wird. Ein Administrator erstellt dann die entsprechende Richtlinie, damit unbekannte Endgeräte identifiziert werden können, bevor der Zugriff gewährt wird. In dieser Übung wird die Autorisierungsrichtlinie so erstellt, dass ein neues Gerät zur Statusüberprüfung an die ISE umgeleitet wird (für mobile Geräte sind agentenlos, daher ist nur Profilerstellung relevant). Endgeräte werden an das ISE Captive Portal umgeleitet und identifiziert.

Führen Sie diese Schritte aus:

1. Navigieren Sie von der ISE zu **Richtlinie > Autorisierung**.

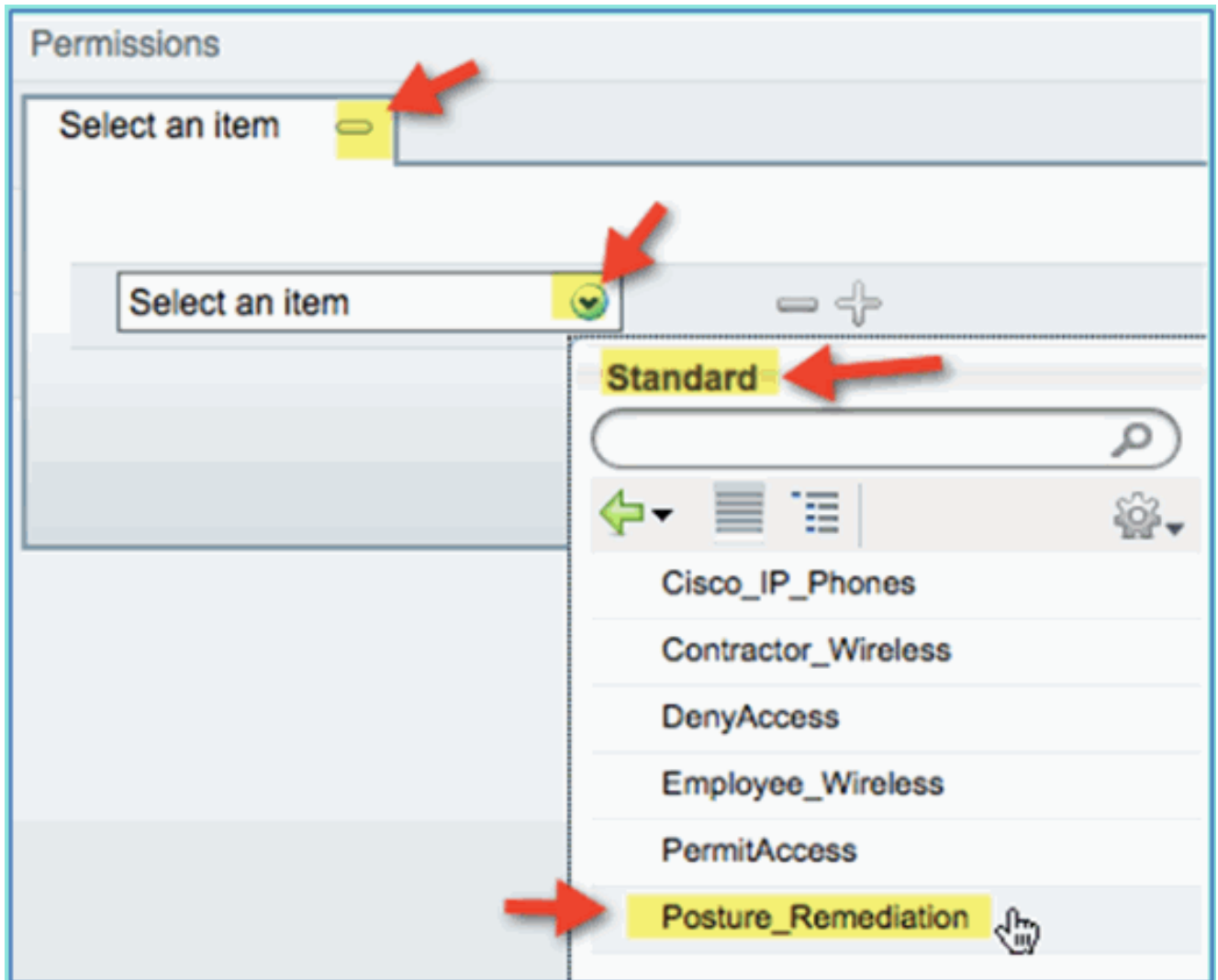


2. Es gibt eine Richtlinie für Cisco IP-Telefone mit Profil. Das ist sofort einsatzbereit. Bearbeiten Sie dies als Statusrichtlinie.
3. Geben Sie die folgenden Werte für diese Richtlinie ein: Regelname: Posture\_RemediationIdentitätsgruppen: AlleAndere Bedingungen > Neu erstellen: (Erweiterte) Sitzung > StatusStatus > Equals: Unbekannt



4. Legen Sie Folgendes für Berechtigungen fest: Berechtigungen > Standard: Posture\_Remediation



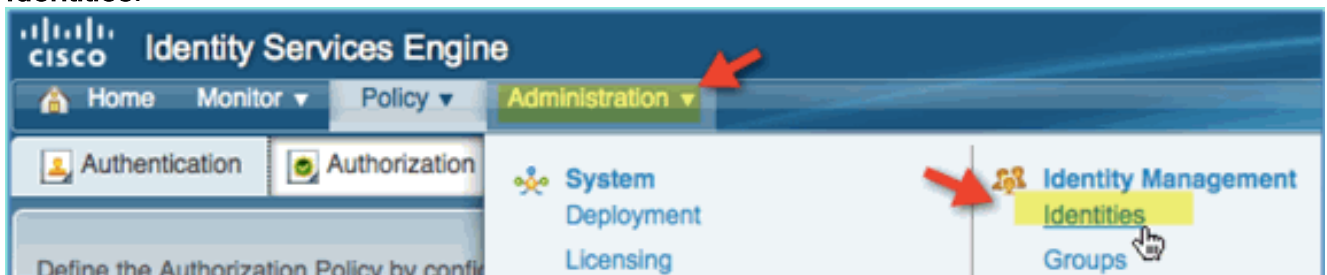


5. Klicken Sie auf **Speichern**. Hinweis: Alternativ können benutzerdefinierte Richtlinienelemente erstellt werden, um die Benutzerfreundlichkeit zu erhöhen.

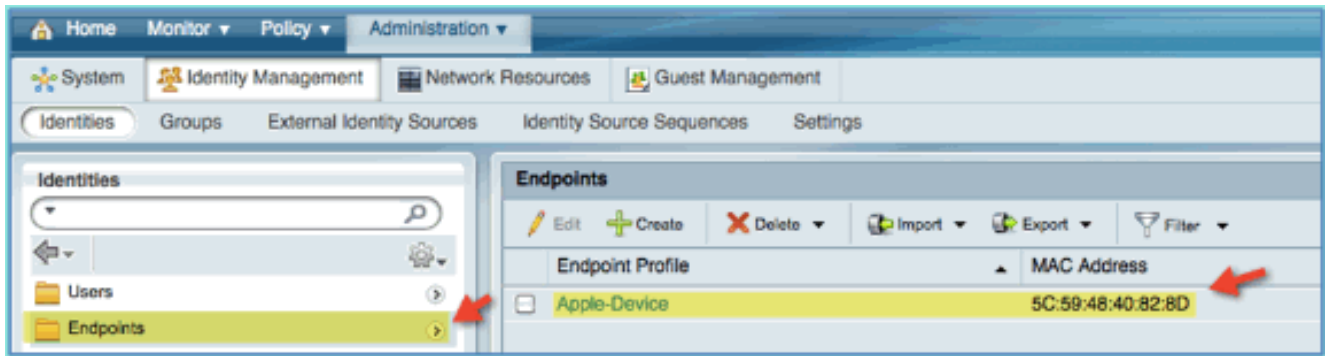
## [Richtlinie zur Statusüberprüfung testen](#)

Es kann eine einfache Demonstration durchgeführt werden, um zu zeigen, dass die ISE die richtige Profilerstellung für ein neues Gerät anhand der Statusrichtlinie durchführt.

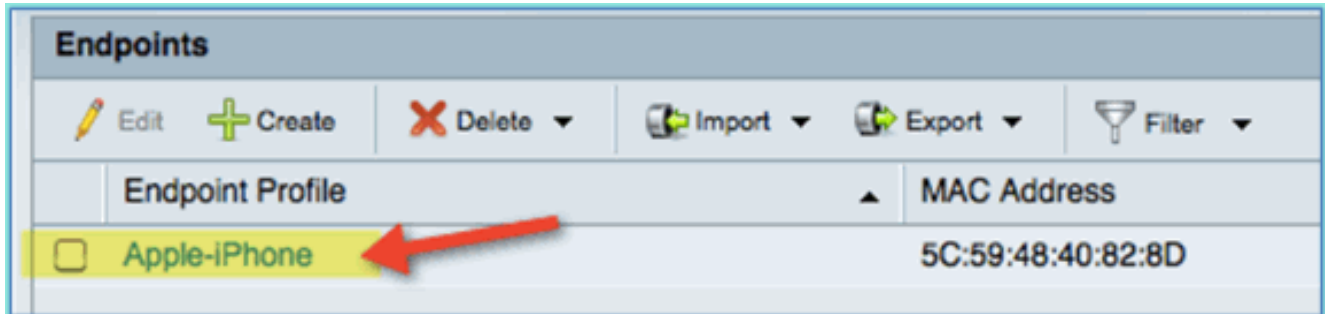
1. Navigieren Sie von der ISE zu **Administration > Identity Management > Identities**.



2. Klicken Sie auf **Endgeräte**. Ein Gerät zuordnen und verbinden (in diesem Beispiel ein iPhone).



3. Aktualisieren Sie die Liste der Endpunkte. Beobachten Sie, welche Informationen gegeben werden.
4. Navigieren Sie auf dem Endgerät zu:URL: http://www (oder 10.10.10.10)Das Gerät wird umgeleitet. Akzeptieren Sie alle Eingabeaufforderungen für Zertifikate.
5. Nachdem das Mobilgerät vollständig umgeleitet wurde, aktualisieren Sie die Endpunktliste von der ISE erneut. Beobachten Sie, was sich geändert hat. Das vorherige Endgerät (z. B. Apple-Gerät) hätte in "Apple-iPhone" usw. geändert werden müssen. Der Grund hierfür ist, dass die HTTP-Anfrage im Rahmen der Umleitung zum Captive Portal Informationen von Benutzern und Agenten abrufen.

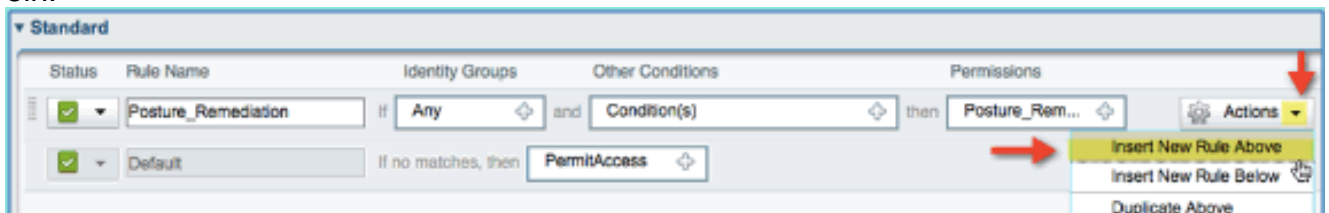


## [Autorisierungsrichtlinie für differenzierten Zugriff](#)

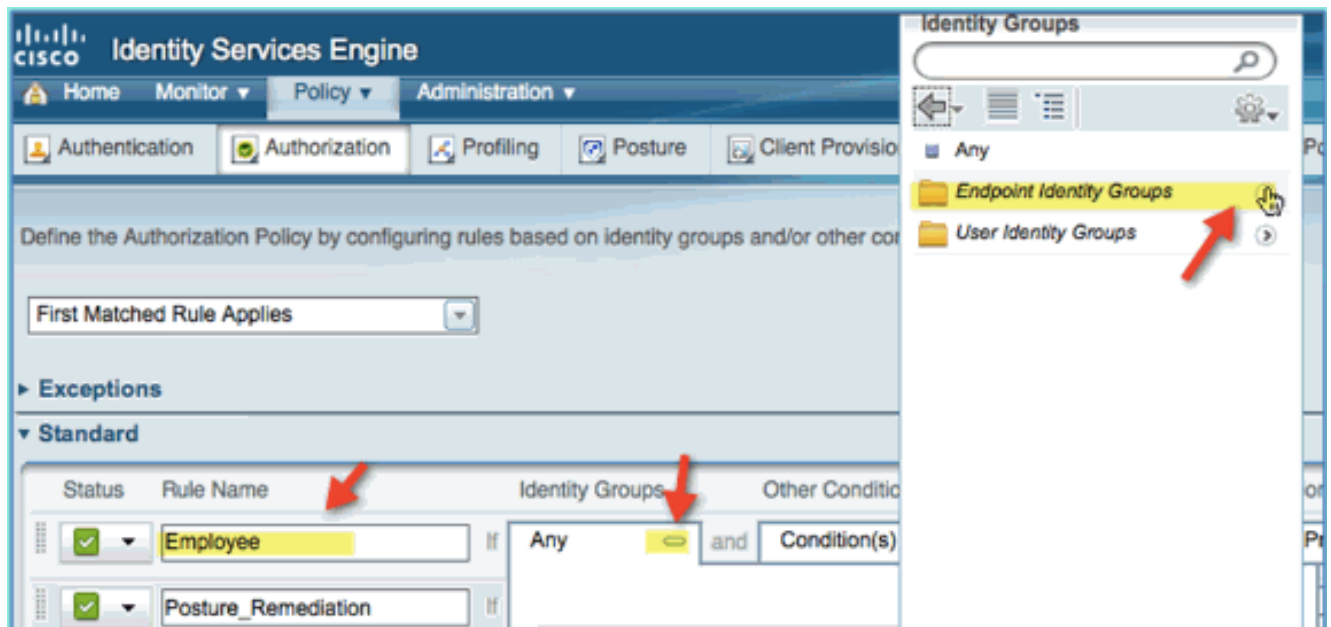
Fahren Sie nach dem erfolgreichen Test der Statusautorisierung mit der Erstellung von Richtlinien zur Unterstützung des differenzierten Zugriffs für Mitarbeiter und Auftragnehmer mit bekannten Geräten und unterschiedlicher VLAN-Zuweisung für die jeweilige Benutzerrolle fort (in diesem Szenario Mitarbeiter und Auftragnehmer).

Führen Sie diese Schritte aus:

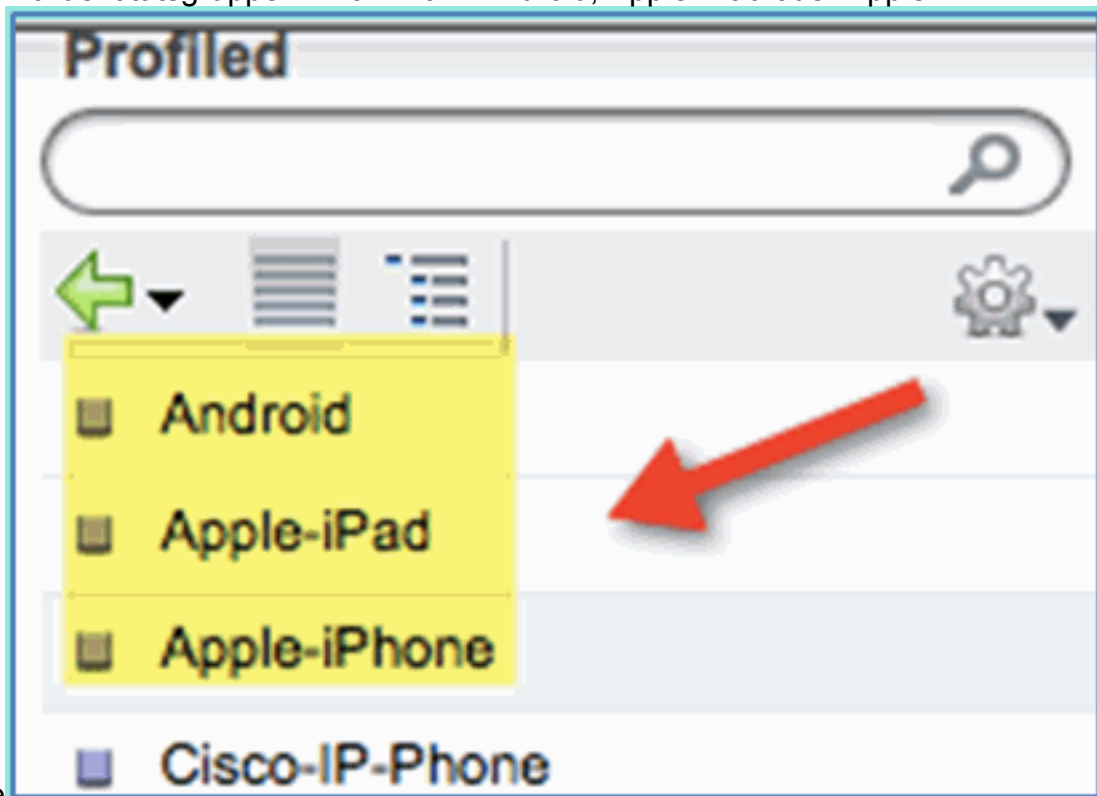
1. Navigieren Sie zu **ISE > Policy > Authorization (Richtlinie > Autorisierung)**.
2. Fügen Sie über der Richtlinie/Zeile für die Statusbehebung eine neue Regel hinzu bzw. fügen Sie eine neue Regel ein.



3. Geben Sie die folgenden Werte für diese Richtlinie ein:Regelname: MitarbeiterIdentitätsgruppen (erweitert): Endpunkt-Identitätsgruppen

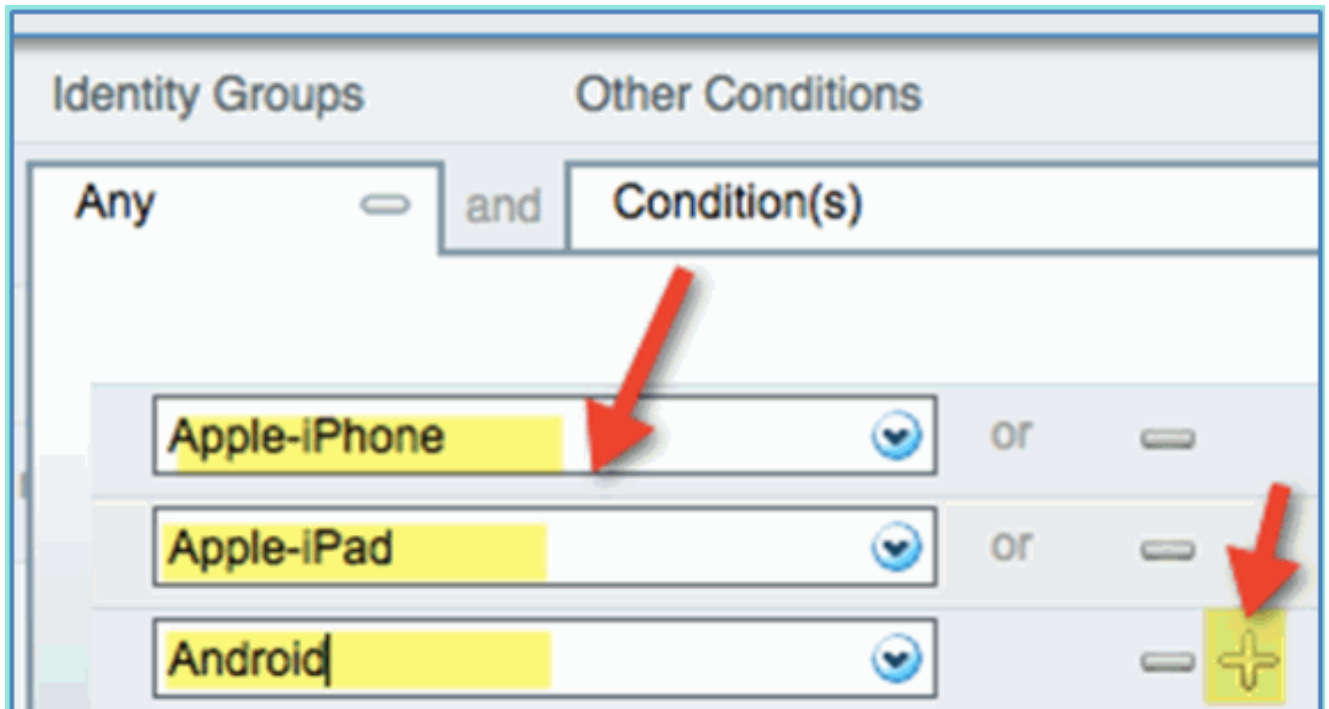


Endpoint-Identitätsgruppen: Profil: Android, Apple-iPad oder Apple-

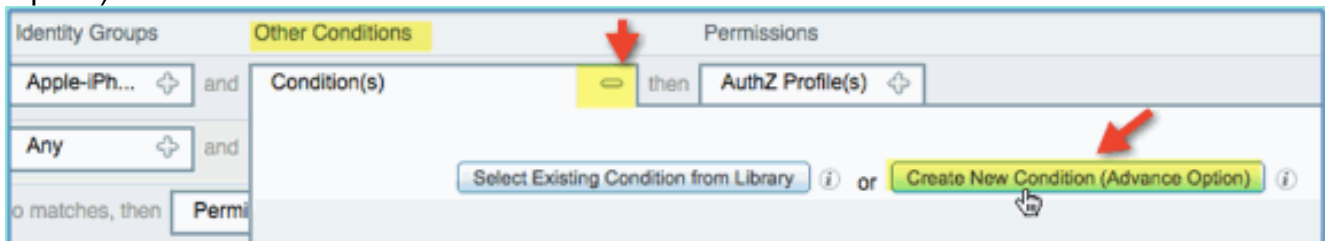


iPhone

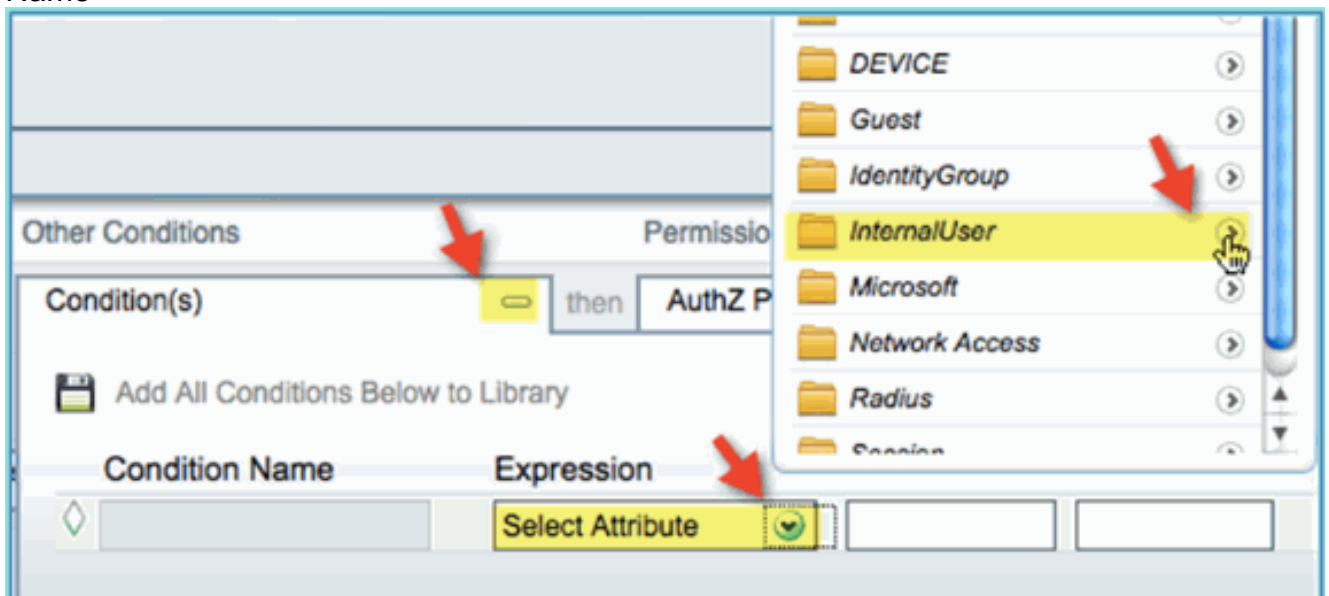
- Um weitere Gerätetypen anzugeben, klicken Sie auf das **+**-Symbol, und fügen Sie ggf. weitere Geräte hinzu:Endpoint-Identitätsgruppen: Profil: Android, Apple-iPad oder Apple-iPhone



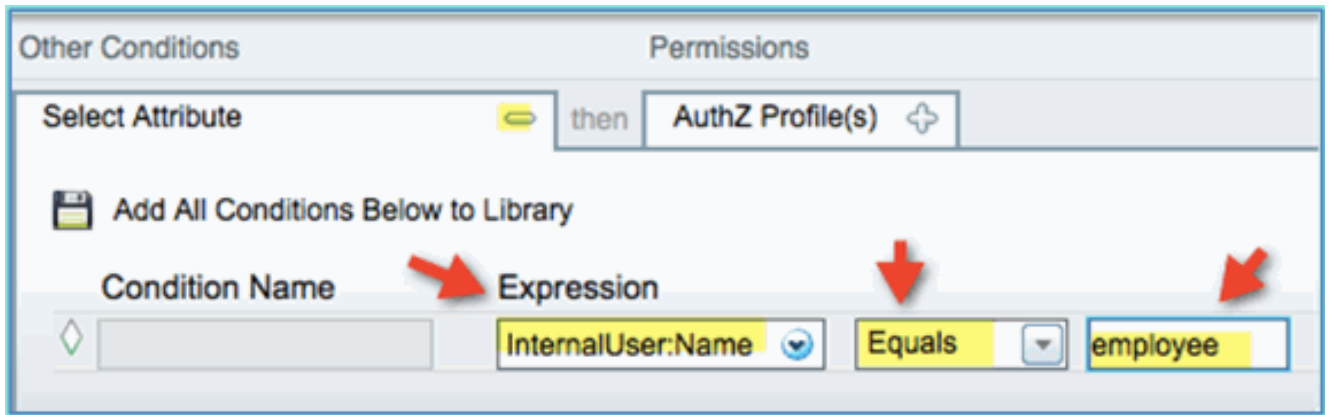
5. Geben Sie die folgenden Berechtigungswerte für diese Richtlinie an: Andere Bedingungen (erweitern): Neue Bedingung erstellen (erweiterte Option)



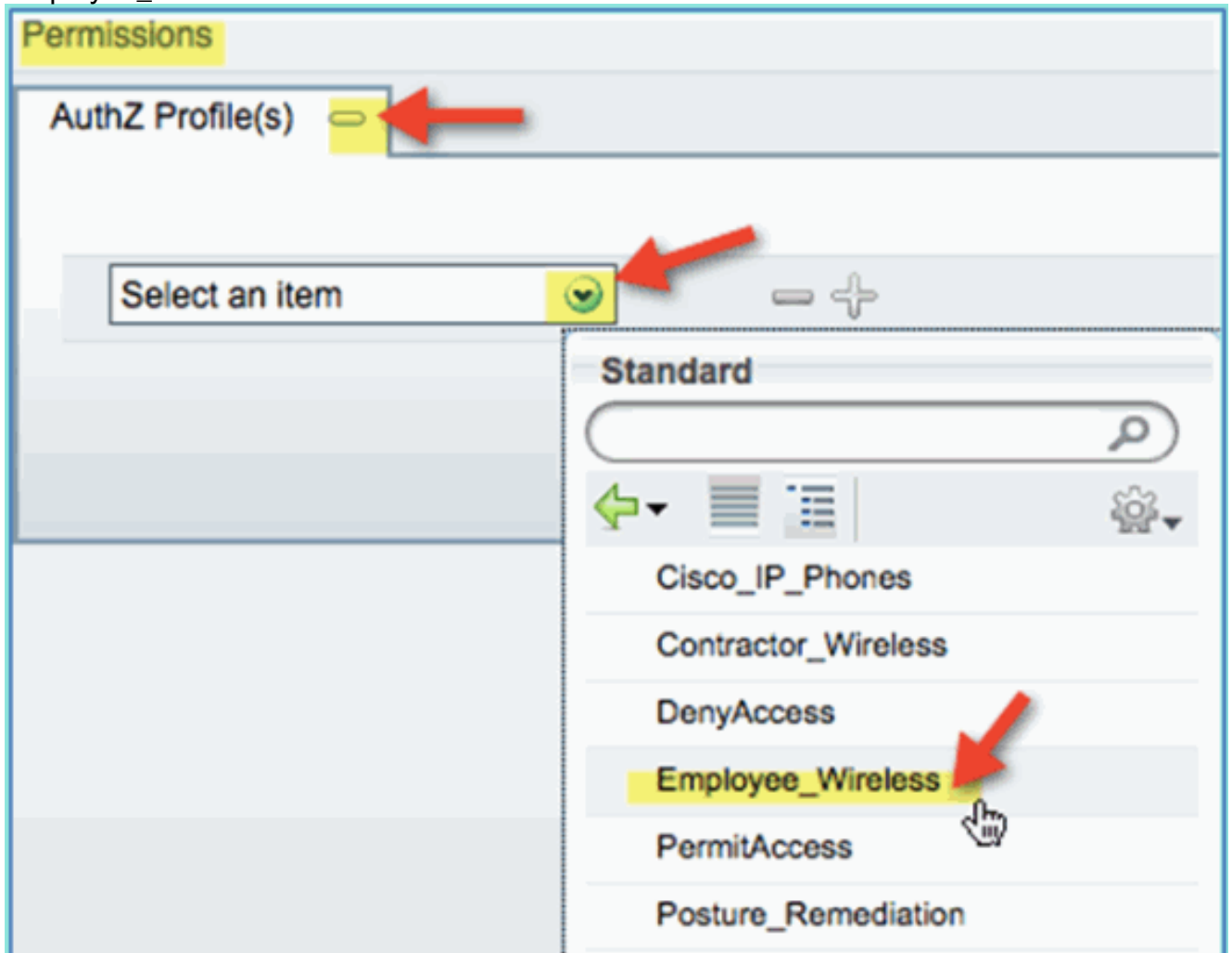
Bedingung > Ausdruck (aus Liste): InternalUser > Name



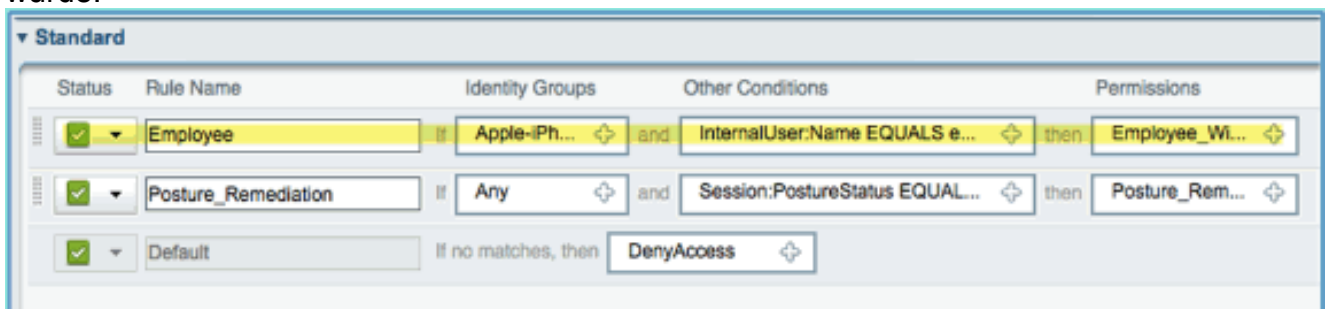
Interner Benutzer > Name:  
Mitarbeiter



6. Bedingung für Statussetzung hinzufügen Entspricht:Berechtigungen > Profile > Standard: Employee\_Wireless

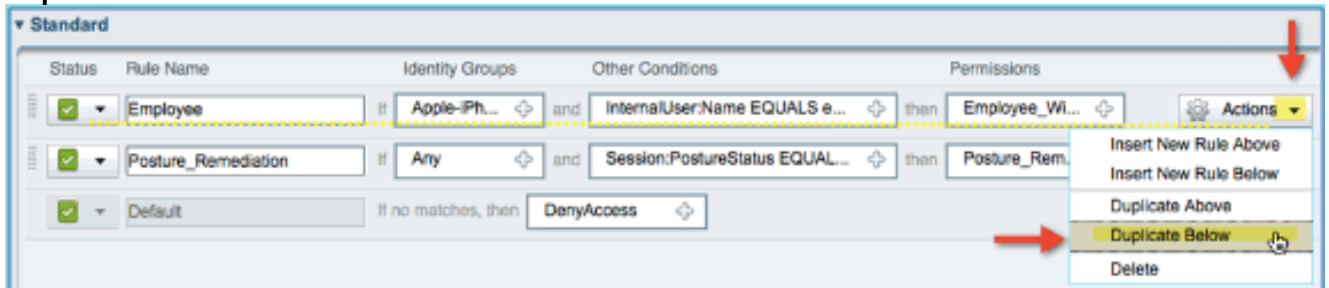


7. Klicken Sie auf **Speichern**. Bestätigen Sie, dass die Richtlinie ordnungsgemäß hinzugefügt wurde.

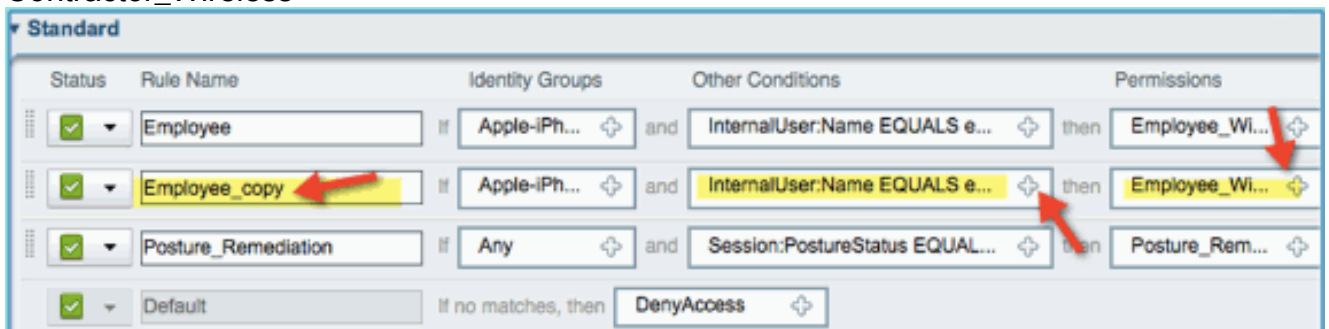


8. Fahren Sie fort, indem Sie die Vertragsrichtlinie hinzufügen. In diesem Dokument wird die vorherige Richtlinie dupliziert, um den Prozess zu beschleunigen (oder Sie können sie

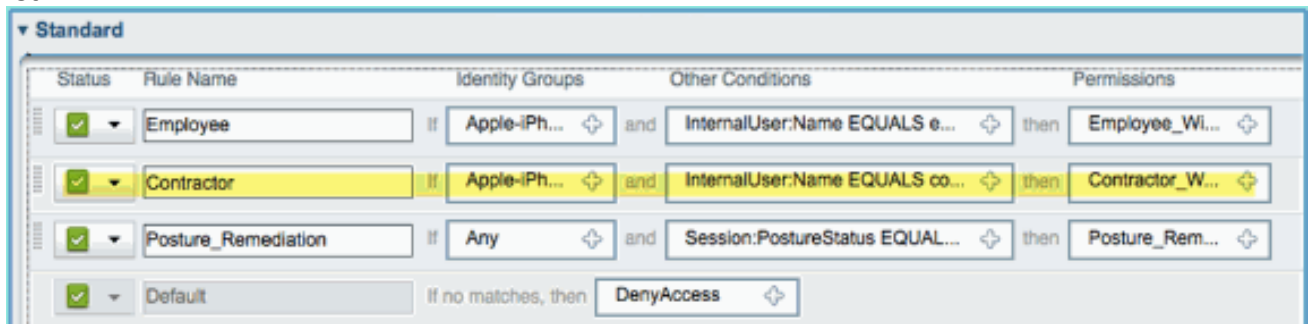
manuell konfigurieren, um eine bewährte Vorgehensweise zu erhalten). Klicken Sie unter Mitarbeiterrichtlinie > Aktionen auf **Unten duplizieren**.



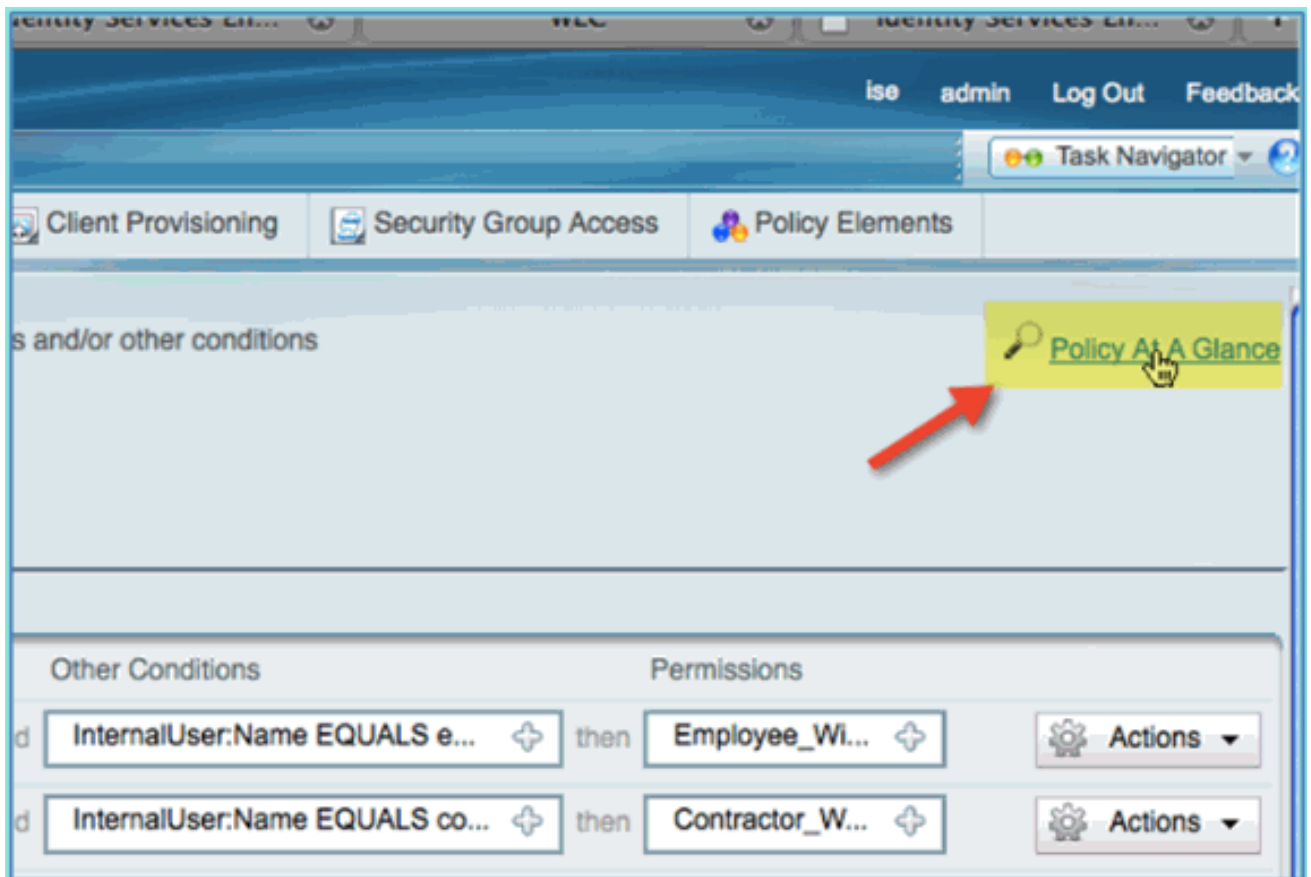
9. Bearbeiten Sie die folgenden Felder für diese Richtlinie (doppelte Kopie): Regelname: SubunternehmerAndere Bedingungen > InternBenutzer > Name: AuftragnehmerBerechtigungen: Contractor\_Wireless



10. Klicken Sie auf **Speichern**. Bestätigen Sie, dass die vorherige duplizierte Kopie (oder die neue Richtlinie) ordnungsgemäß konfiguriert ist.



11. Um eine Vorschau der Richtlinien anzuzeigen, klicken Sie auf **Policy-at-a-Glance (Richtlinie auf einen Blick)**.



Die Übersicht über Richtlinien bietet eine konsolidierte Übersicht und eine übersichtliche Darstellung der Richtlinien.

Authorization Policy At A Glance				
First Matched Rule Applies				
Exceptions				
Status	Rule Name	Identity Groups	Other Conditions	Permissions
No data available				
Standard				
Status	Rule Name	Identity Groups	Other Conditions	Permissions
<input checked="" type="checkbox"/> Enabled	Employee	Android OR Apple-iPad OR Apple-iphone	InternalUser.Name EQUALS employee	Employee_Wireless
<input checked="" type="checkbox"/> Enabled	Contractor	Android OR Apple-iPad OR Apple-iphone	InternalUser.Name EQUALS contractor	Contractor_Wireless
<input checked="" type="checkbox"/> Enabled	Posture_Remediation	Any	Session.PostureStatus EQUALS Unknown	Posture_Remediation
<input checked="" type="checkbox"/> Enabled	Default	Any		DenyAccess

## CoA-Test für differenzierten Zugriff

Mit den Autorisierungsprofilen und Richtlinien, die für eine Differenzierung des Zugriffs vorbereitet wurden, ist es Zeit zum Testen. Einem Mitarbeiter wird das Mitarbeiter-VLAN zugewiesen, und ein Auftragnehmer übernimmt das Auftragnehmer-VLAN. In den folgenden Beispielen wird ein Apple iPhone/iPad verwendet.

Führen Sie diese Schritte aus:

1. Stellen Sie mit dem Mobilgerät eine Verbindung zum gesicherten WLAN (POD1x) her, und verwenden Sie die folgenden Anmeldeinformationen: Benutzername: Mitarbeiter Kennwort: XXXXX



2. Klicken Sie auf **Beitreten**. Bestätigen Sie, dass dem Mitarbeiter VLAN 11 (Mitarbeiter-VLAN) zugewiesen





ist.

3. Klicken Sie auf **Dieses Netzwerk vergessen**. Bestätigen Sie, indem Sie auf **Vergessen**



klicken.

4. Wechseln Sie zum WLC, und entfernen Sie vorhandene Client-Verbindungen (wenn diese in den vorherigen Schritten verwendet wurden). Navigieren Sie zu **Monitor > Clients > MAC address**, und klicken Sie dann auf **Remove (Entfernen)**.

Monitor

Clients

Summary

Current Filter

▶ Access Points

▶ Cisco CleanAir

▶ Statistics

▶ CDP

▶ Rogues

Clients

Multicast

Client MAC Addr

[44:2a:60:f7:3a:4a](#)

[5c:59:48:40:82:8d](#)

Status	Auth	Port	WGB
--------	------	------	-----

Associated	Yes	1	No
------------	-----	---	----

Associated	No	1	
------------	----	---	--

LinkTest

Disable

Remove

802.11aTSM

802.11b/gTSM

5. Eine weitere Möglichkeit zum Löschen vorheriger Client-Sitzungen besteht darin, das WLAN zu deaktivieren/aktivieren. Gehen Sie zu **WLC > WLANs > WLAN**, und klicken Sie dann zum Bearbeiten auf das WLAN. Deaktivieren Sie **Enabled > Apply** (zum Deaktivieren). Aktivieren Sie das Kontrollkästchen **Enabled (Aktiviert) > Apply (Anwenden)** (um die Funktion erneut zu aktivieren).



6. Kehren Sie zum mobilen Gerät zurück. Stellen Sie erneut eine Verbindung mit dem gleichen WLAN mit den folgenden Anmeldeinformationen her: Benutzername:  
AuftragnehmerKennwort:

Enter the password for "pod1x"

**Cancel** **Enter Password**

**Username** contractor ←

**Password** ●●●●●●●● | ←

**Mode** Automatic >

1 2 3 4 5 6 7 8 9 0

XXXX

7. Klicken Sie auf **Beitreten**. Vergewissern Sie sich, dass dem Auftragnehmer-Benutzer VLAN 12 (Auftragnehmer-/Gast-VLAN) zugewiesen



ist.

8. Die ISE-Echtzeitprotokollansicht finden Sie unter **ISE > Monitor > Authorizations (ISE > Überwachung > Autorisierungen)**. Sie sollten sehen, dass einzelne Benutzer (Mitarbeiter, Auftragnehmer) unterschiedliche Autorisierungsprofile (Employee\_WirelessvsContractor\_Wireless) in verschiedenen VLANs erhalten.

Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles
Aug 02,11 03:40:18.331 PM	✓		employee	5C:59:48:40:82:8D		wlc		Employee_Wireless
Aug 02,11 03:36:33.663 PM	✓		contractor	5C:59:48:40:82:8D		wlc		Contractor_Wireless

Gehen Sie wie folgt vor, um ein Gast-WLAN hinzuzufügen, über das Gäste auf das ISE Sponsor Guest Portal zugreifen können:

1. Navigieren Sie vom WLC zu **WLANS > WLANS > Add New**.
2. Geben Sie für das neue Gast-WLAN Folgendes ein: Profilname: pod1guest  
SSID: pod1guest



3. Klicken Sie auf **Apply** (Anwenden).
4. Geben Sie auf der Registerkarte Gast-WLAN > Allgemein Folgendes ein: Status: Deaktiviert  
Schnittstellen-/Schnittstellengruppe: Gast

MONITOR **WLANs** CONTROLLER WIRELESS SECUR

WLANs > Edit 'pod1guest'

**General** Security QoS Advanced

Profile Name pod1guest

Type WLAN

SSID pod1guest

Status  Enabled

Security Policies [WPA2][Auth(802.1X)]  
(Modifications done under security)

Radio Policy All

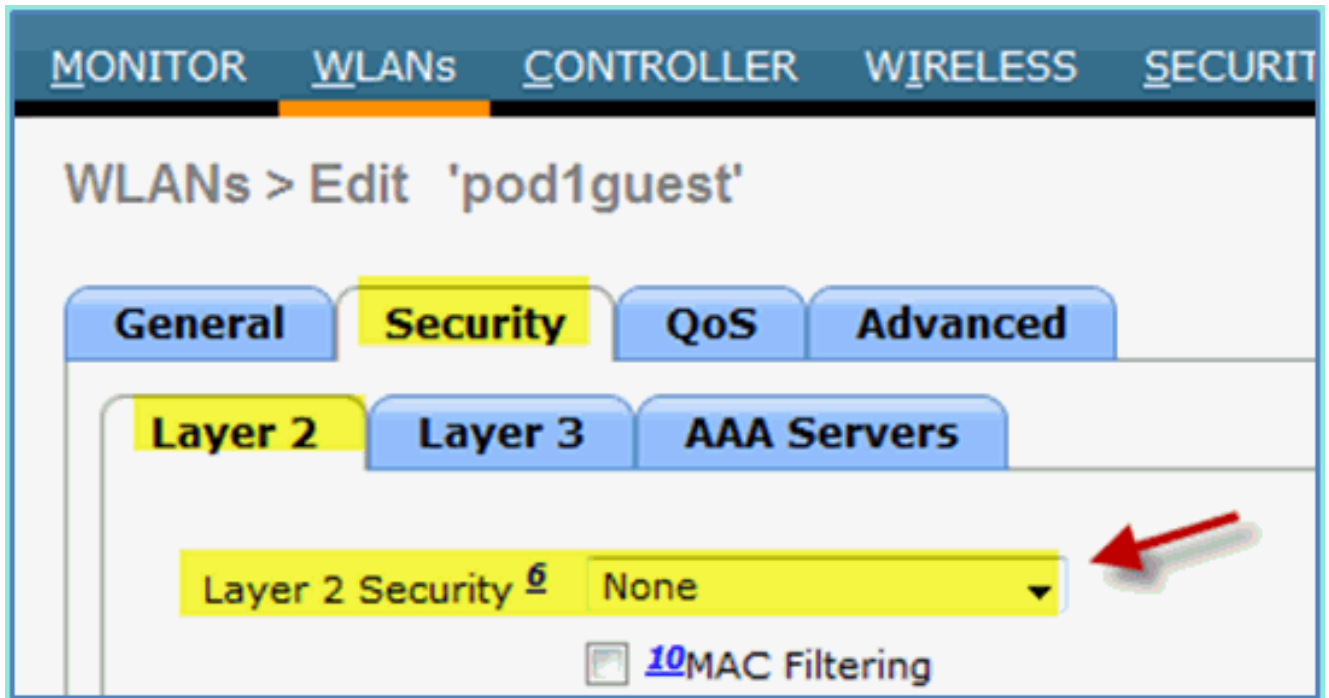
Interface/Interface Group(G) **guest**

Multicast Vlan Feature  Enabled

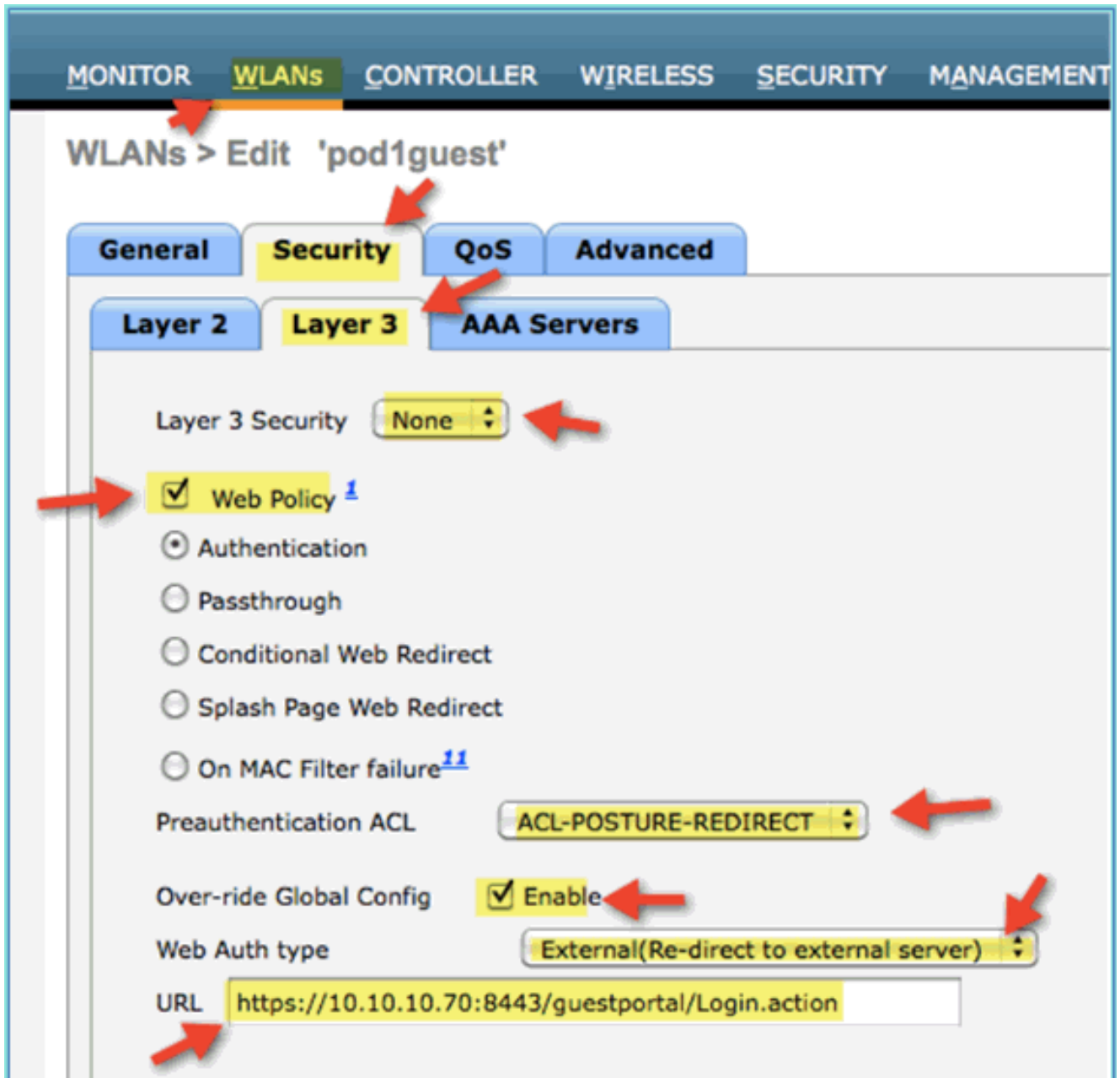
Broadcast SSID  Enabled

5. Navigieren Sie zu Gast-WLAN > Sicherheit > Layer 2, und geben Sie Folgendes ein: Layer-2-Sicherheit:  
Keine





6. Navigieren Sie zur Registerkarte Guest WLAN > Security > Layer3, und geben Sie Folgendes ein: Layer-3-Sicherheit: Keine Webrichtlinie: Aktiviert Web Policy-Unterwert: Authentifizierung ACL vor der Authentifizierung: ACL-POSTURE-REDIRECT Webauthentifizierungstyp: Extern (Umleitung zum externen Server) URL: <https://10.10.10.70:8443/guestportal/Login.action>



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

8. **Speichern** Sie unbedingt die WLC-Konfiguration.

## Testen des Gast-WLAN und Gastportals

Jetzt können Sie die Konfiguration des Gast-WLAN testen. Die Gäste sollten zum ISE-Gastportal weitergeleitet werden.

Führen Sie diese Schritte aus:

1. Navigieren Sie auf einem iOS-Gerät (z. B. einem iPhone) zu **Wi-Fi Networks > Enable (Wi-Fi-Netzwerke > Aktivieren)**. Wählen Sie anschließend das POD-Gastnetzwerk



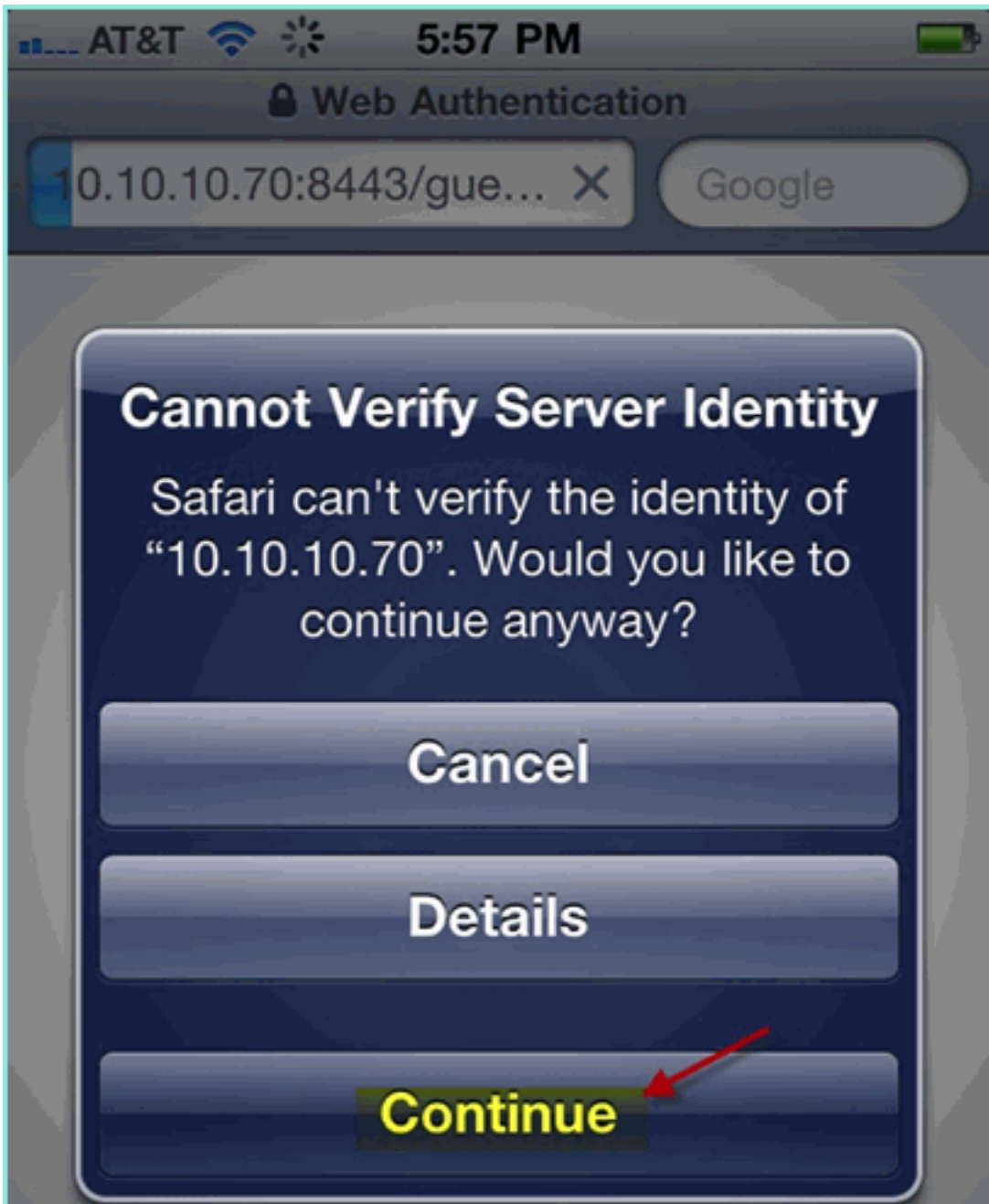
aus.

2. Auf Ihrem iOS-Gerät sollte eine gültige IP-Adresse des Gast-VLAN (10.10.12.0/24) angezeigt



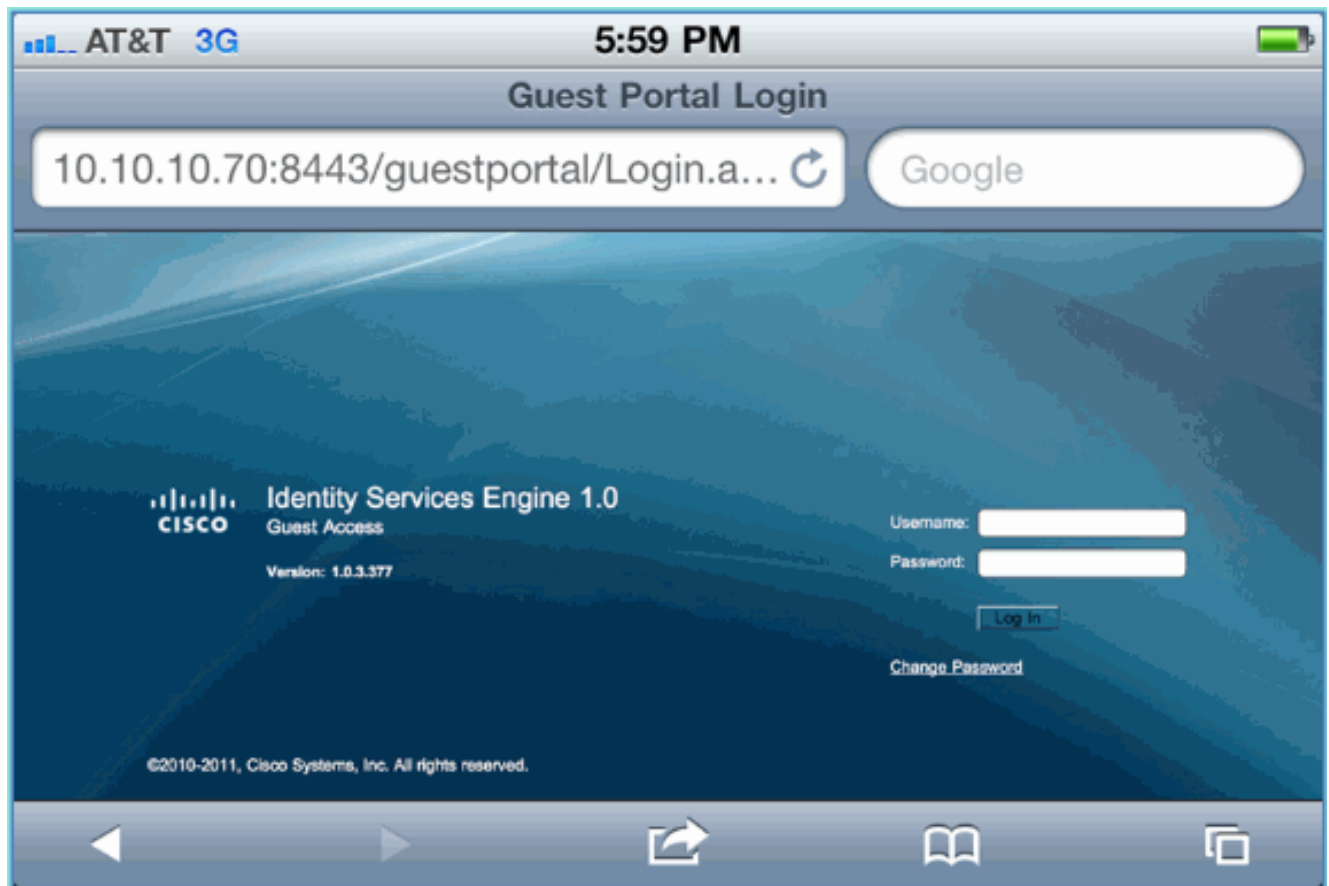
werden.

3. Öffnen Sie den Safari-Browser, und stellen Sie eine Verbindung her mit:URL:  
<http://10.10.10.10>Eine Umleitung für die Webauthentifizierung wird angezeigt.
4. Klicken Sie auf **Continue** (Weiter), bis Sie die Seite für das ISE-Gastportal erreicht



haben.

Der nächste Screenshot zeigt das iOS-Gerät auf einer Gastportal-Anmeldung. Dies bestätigt, dass die richtige Einrichtung für das WLAN und das ISE-Gastportal aktiv ist.

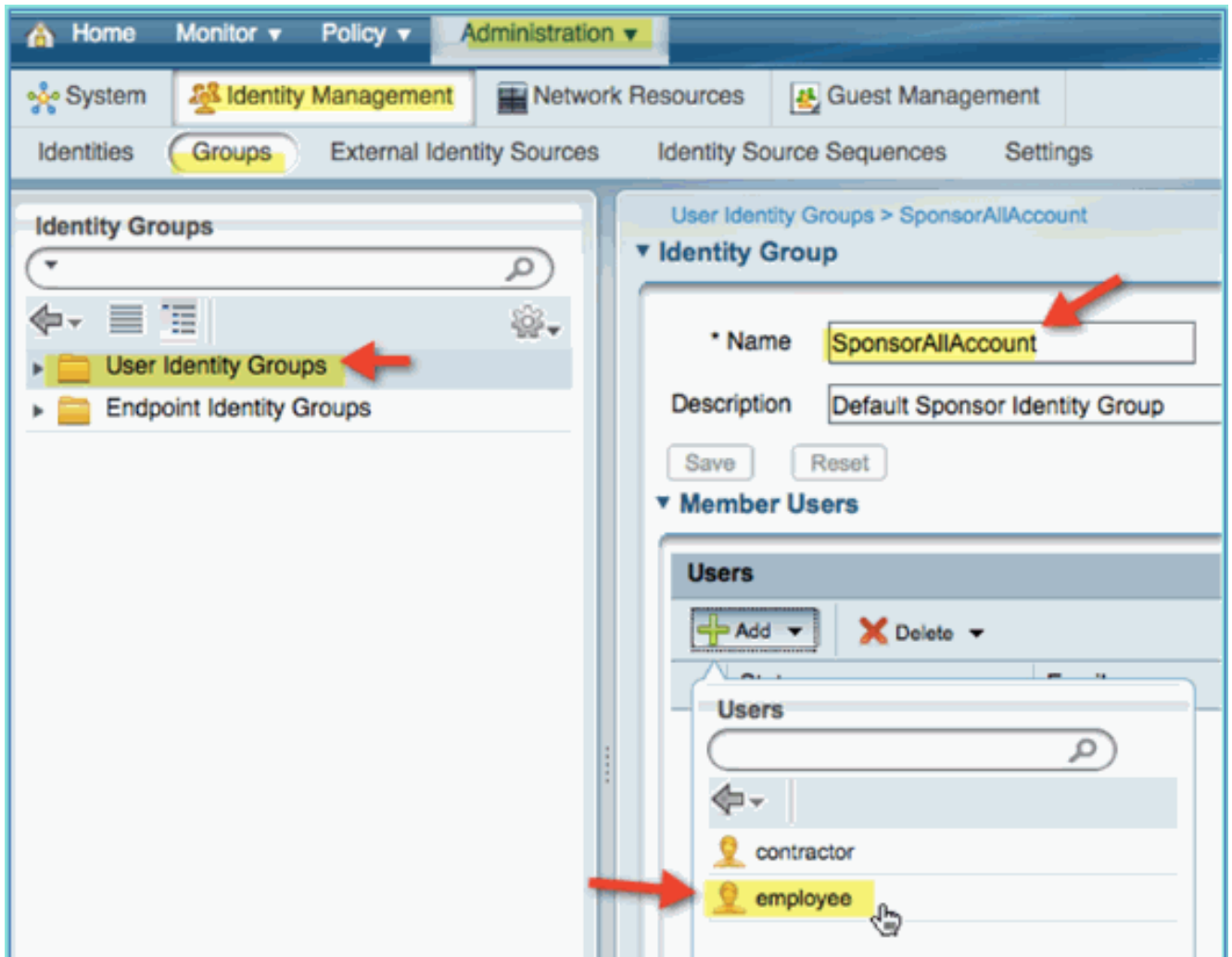


## ISE Wireless Sponsored Guest Access

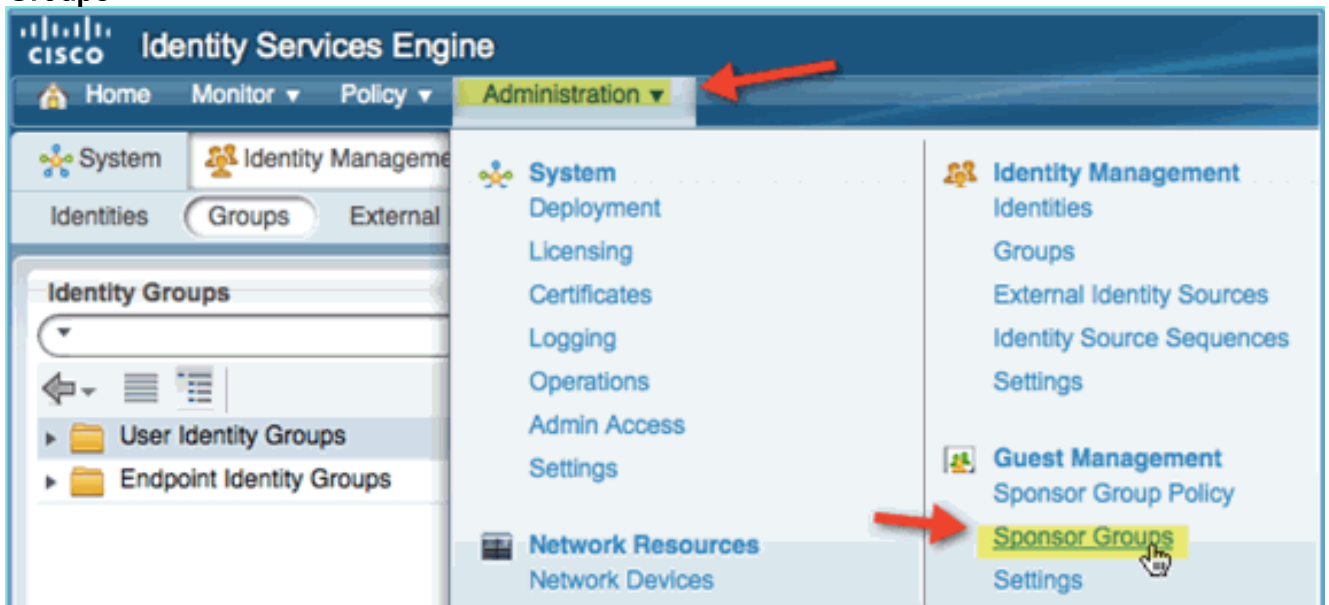
Die ISE kann so konfiguriert werden, dass Gäste unterstützt werden können. In diesem Fall konfigurieren Sie die ISE-Gastrichtlinien so, dass interne Benutzer oder (falls integriert) AD-Domänenbenutzer den Gastzugriff sponsern können. Sie konfigurieren außerdem die ISE so, dass Sponsoren das Gastpasswort einsehen können (optional). Dies ist für diese Übung hilfreich.

Führen Sie diese Schritte aus:

1. Fügen Sie einen Mitarbeiter-Benutzer zur Gruppe SponsorAllAccount hinzu. Es gibt verschiedene Möglichkeiten, dies zu tun: gehen Sie direkt zur Gruppe, oder bearbeiten Sie den Benutzer und weisen Sie eine Gruppe zu. Navigieren Sie in diesem Beispiel zu **Administration > Identity Management > Groups > User Identity Groups**. Klicken Sie dann auf **SponsorAllAccount**, und fügen Sie einen Benutzer für den Mitarbeiter hinzu.



2. Navigieren Sie zu **Administration > Guest Management > Sponsor Groups**.



3. Klicken Sie auf **Bearbeiten**, und wählen Sie dann **SponsorAllAccounts** aus.

The screenshot shows the Cisco Identity Services Engine Administration interface. The navigation menu includes Home, Monitor, Policy, and Administration. The main menu has System, Identity Management, Network Resources, and Guest Management. The sub-menu shows Sponsor Group Policy, Sponsor Groups (selected), and Settings. The main content area is titled 'Guest Sponsor Groups' and contains a table with the following data:

<input type="checkbox"/>	Sponsor Group Name	Description
<input checked="" type="checkbox"/>	SponsorAllAccounts	Default SponsorGroup
<input type="checkbox"/>	SponsorGroupGrpAccounts	Default SponsorGroup

Red arrows point to the 'Edit' button and the 'SponsorAllAccounts' group name.

4. Wählen Sie die Autorisierungsstufen aus, und legen Sie Folgendes fest: Gastpasswort anzeigen:

Ja



The screenshot shows the Cisco Identity Services Engine (ISE) Administration interface. The breadcrumb path is "Sponsor Group List > SponsorAllAccounts". The "Authorization Levels" tab is selected. A red arrow points to the "View Guest Password" dropdown menu, which is currently set to "Yes" and highlighted in yellow. Other settings include "Allow Login", "Create Accounts", "Create Bulk Accounts", "Create Random Accounts", "Import CSV", "Send Email", "Send SMS", "Allow Printing Guest Details", "View/Edit Accounts", and "Suspend/Reinstate Accounts". At the bottom, there are "Save" and "Reset" buttons.

5. Klicken Sie auf **Speichern**, um diese Aufgabe auszuführen.

## [Sponsoring für Gäste](#)

Sie haben zuvor die entsprechende Gastrichtlinie und die entsprechenden Gruppen konfiguriert, damit AD-Domänenbenutzer temporäre Gäste sponsern können. Als Nächstes greifen Sie auf das Sponsor-Portal zu und erstellen einen temporären Gastzugriff.

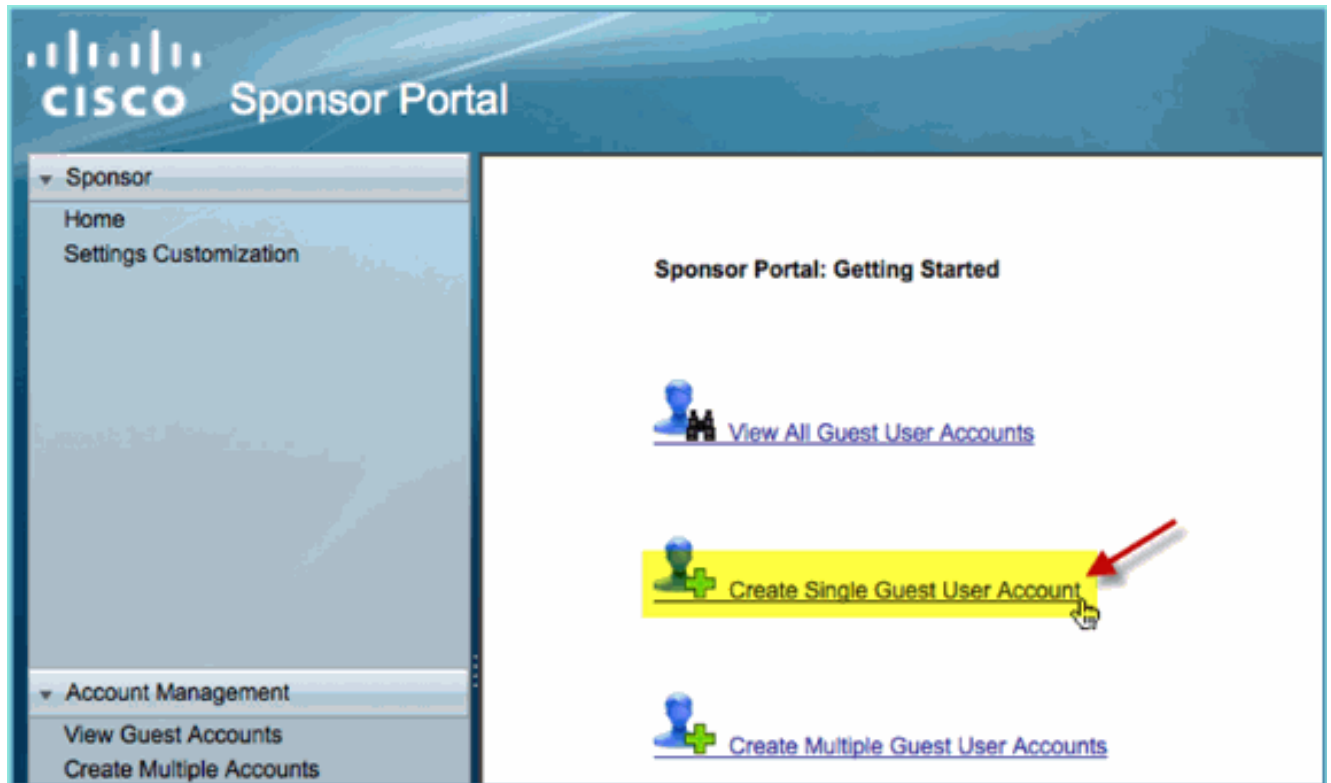
Führen Sie diese Schritte aus:

1. Navigieren Sie in einem Browser zu einer der folgenden URLs: <http://<ip>:8080/sponsorportal/> oder <https://<ip>:8443/sponsorportal/>. Melden Sie sich dann mit folgenden Optionen an: Benutzername: aduser (Active Directory), employee (interner

Benutzer)Kennwort:  
XXXX



2. Klicken Sie auf der Seite "Programmpate" auf **Einzelnes Gastbenutzerkonto erstellen**.



3. Fügen Sie für einen temporären Gast Folgendes hinzu: Vorname: Pflichtfeld (z. B. Sam) Nachname: Pflichtfeld (z. B. Jones) Gruppenrolle: Gast Zeitprofil: DefaultOneHour Zeitzone: Beliebig/Standard

**Sponsor Portal**

Account Management > [View All Guest Accounts](#) > Create Guest Account

## Create Guest Account

First Name:

Last Name:

Email Address:

Phone Number:

Company:

Optional Data 1:

Optional Data 2:

Optional Data 3:

Optional Data 4:

Optional Data 5:

Group Role:

Time Profile:

Timezone:

⚙️ = Required fields

4. Klicken Sie auf **Senden**.
5. Ein Gastkonto wird basierend auf Ihrem vorherigen Eintrag erstellt. Beachten Sie, dass das Kennwort (aus der vorherigen Übung) im Gegensatz zu Hash \*\*\* angezeigt wird.
6. Lassen Sie dieses Fenster geöffnet, und zeigen Sie Benutzername und Passwort für den Gast an. Sie verwenden diese, um die Guest Portal Login (next) zu testen.



## Successfully Created Guest Account **siam0002**

Username: **siam0002** ←  
Password: **5\_5g6d7Kx** ←  
First Name: Sam ←  
Last Name: iAm  
Email Address:  
Phone Number:  
Company:  
Status: AWAITING INITIAL LOGIN  
Suspended: false  
Optional Data 1:  
Optional Data 2:  
Optional Data 3:  
Optional Data 4:  
Optional Data 5:  
Group Role: Guest  
Time Profile: DefaultOneHour

Timezone: EST  
Account Start Date: 2011-07-15 13:56:04 EST  
Account Expiration Date: 2011-07-15 14:56:04 EST

Email

Print

Create Another Account

View All Accounts

## Testen des Gastportalzugriffs

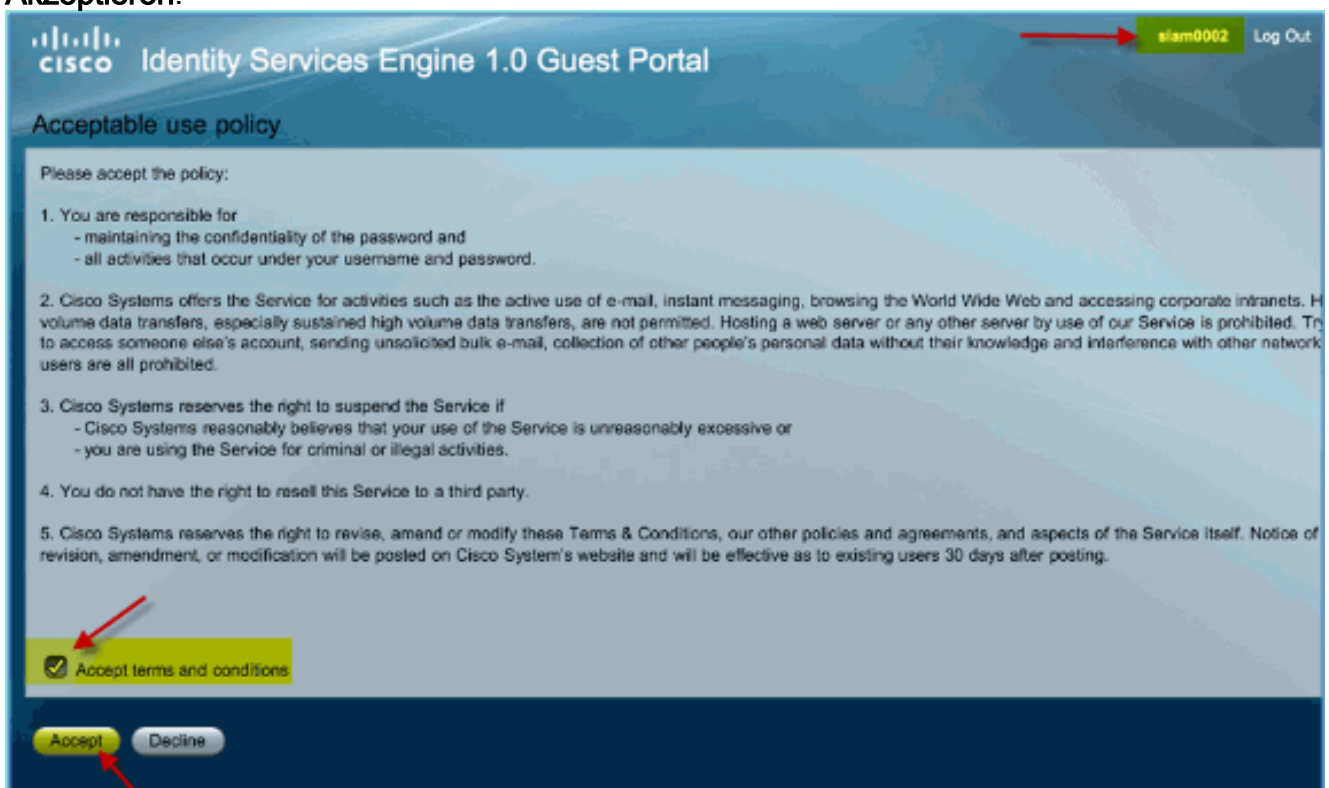
Mit dem neuen Gastkonto, das von einem AD-Benutzer/Sponsor erstellt wurde, ist es an der Zeit, das Gastportal und den Zugriff zu testen.

Führen Sie diese Schritte aus:

1. Stellen Sie auf einem bevorzugten Gerät (in diesem Fall einem Apple iOS/iPad) eine Verbindung mit der Pod-Gast-SSID her, und überprüfen Sie die IP-Adresse/Verbindung.
2. Verwenden Sie den Browser, und navigieren Sie zu <http://www.Sie> werden zur Seite "Guest Portal Login" (Gastportal-Anmeldung) weitergeleitet.



3. Melden Sie sich mit dem in der vorherigen Übung erstellten Gastkonto an. Bei erfolgreicher Verwendung wird die Seite Richtlinie für akzeptable Nutzung angezeigt.
4. Aktivieren Sie die Option **Geschäftsbedingungen akzeptieren**, und klicken Sie dann auf **Akzeptieren**.



Die ursprüngliche URL wurde vervollständigt, und dem Endpunkt wird der Zugriff als Gast gewährt.

## Zertifikatskonfiguration

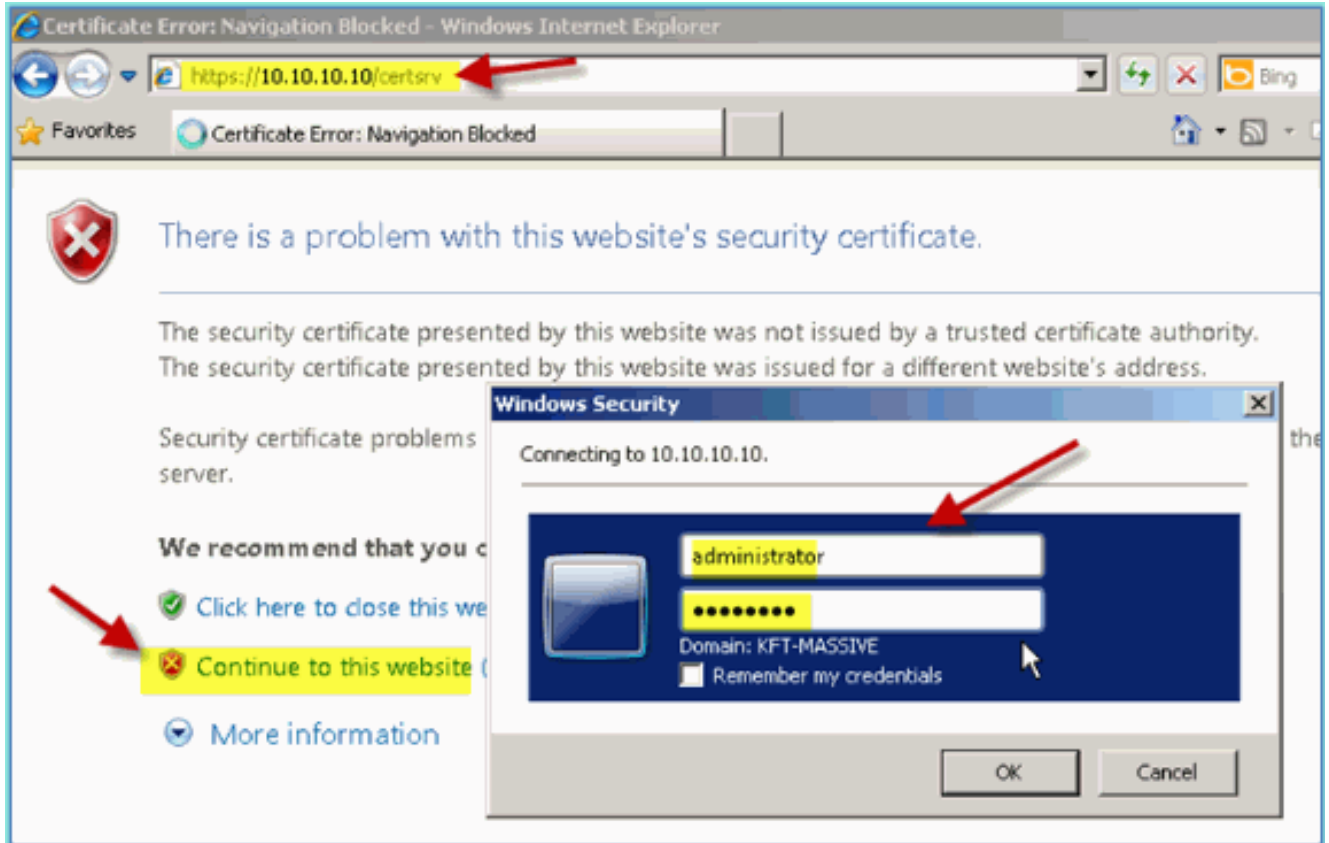
Um die Kommunikation mit der ISE abzusichern, müssen Sie feststellen, ob die Kommunikation authentifizierungsrelevant ist oder für die ISE-Verwaltung verwendet werden soll. Für die Konfiguration über die ISE-Webbenutzeroberfläche müssen beispielsweise X.509-Zertifikate und Zertifikatvertrauensketten konfiguriert werden, um eine asymmetrische Verschlüsselung zu ermöglichen.

Führen Sie diese Schritte aus:

1. Öffnen Sie auf Ihrem kabelgebundenen PC ein Browserfenster, um <https://AD/certsrv> aufzurufen. **Hinweis:** Verwenden Sie sicheres HTTP. **Hinweis:** Verwenden Sie Mozilla Firefox

oder MS Internet Explorer, um auf die ISE zuzugreifen.

2. Melden Sie sich als administrator/Cisco123 an.



3. Klicken Sie auf **Zertifizierungsstellenzertifikat**, **Zertifikatskette** oder **Zertifikatsperrliste** herunterladen.

## Welcome

Use this Web site to request a certificate for your Web browser, e-verify your identity to people you communicate with over the Web, sign a document you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see the help topics.

### Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)



4. Klicken Sie auf **CA-Zertifikat herunterladen** und speichern (beachten Sie den



**Microsoft Active Directory Certificate Services -- corp-RFDEMO-CA**

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

To trust certificates issued from this certification authority, install the CA certificate on your computer.

To download a CA certificate, certificate chain, or CRL, select the type of file to download.

**CA certificate:**

Current [corp-RFDEMO-CA]

**Encoding method:**

DER  
 Base 64

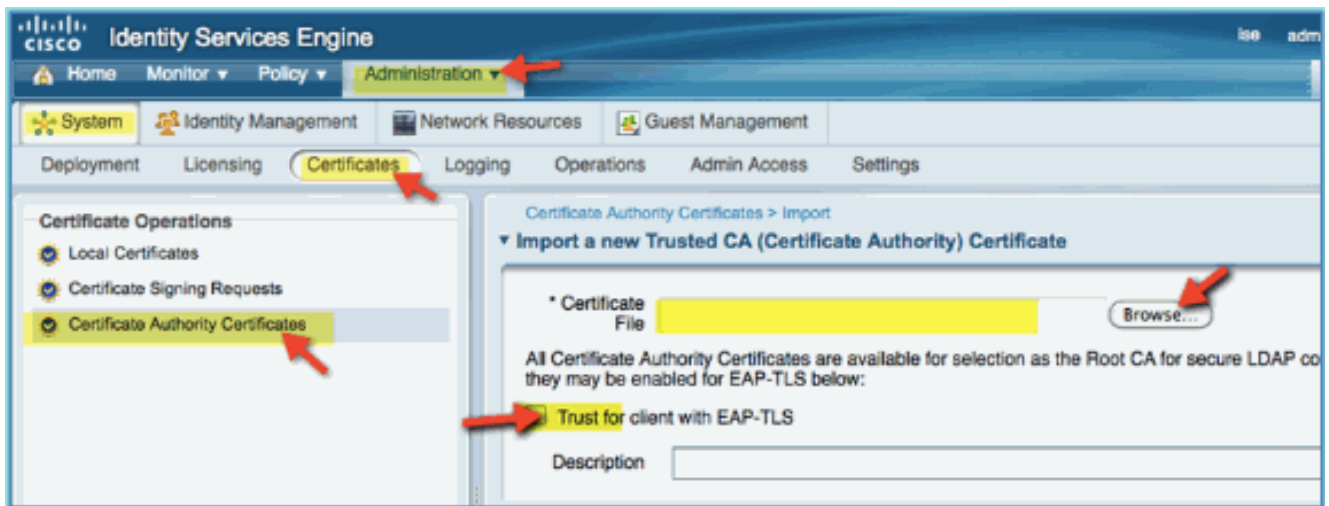
[Download CA certificate](#)  
[Download CA certificate chain](#)  
[Download latest base CRL](#)  
[Download latest delta CRL](#)

Speicherort).

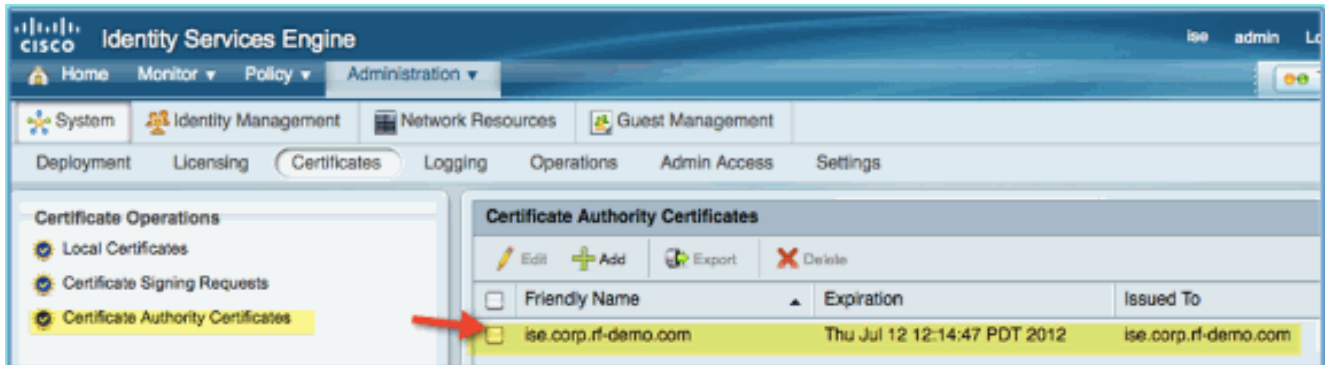
- Öffnen Sie ein Browserfenster, um https://<Pod-ISE> aufzurufen.
- Gehen Sie zu **Administration > System > Certificates > Certificates Authority Certificates**.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes 'Home', 'Monitor', 'Policy', and 'Administration'. The 'Administration' menu is expanded, showing 'System', 'Deployment', 'Licensing', and 'Certificates'. The 'Certificates' option is highlighted in yellow. A red arrow points to the 'Administration' menu, and another red arrow points to the 'Certificates' option. A hand cursor is visible over the 'Certificates' option.

- Wählen Sie den Vorgang **Certificate Authority Certificates** aus, und navigieren Sie zum zuvor heruntergeladenen Zertifizierungsstellenzertifikat.
- Wählen Sie **Vertrauenswürdig für Client mit EAP-TLS aus**, und senden Sie es.

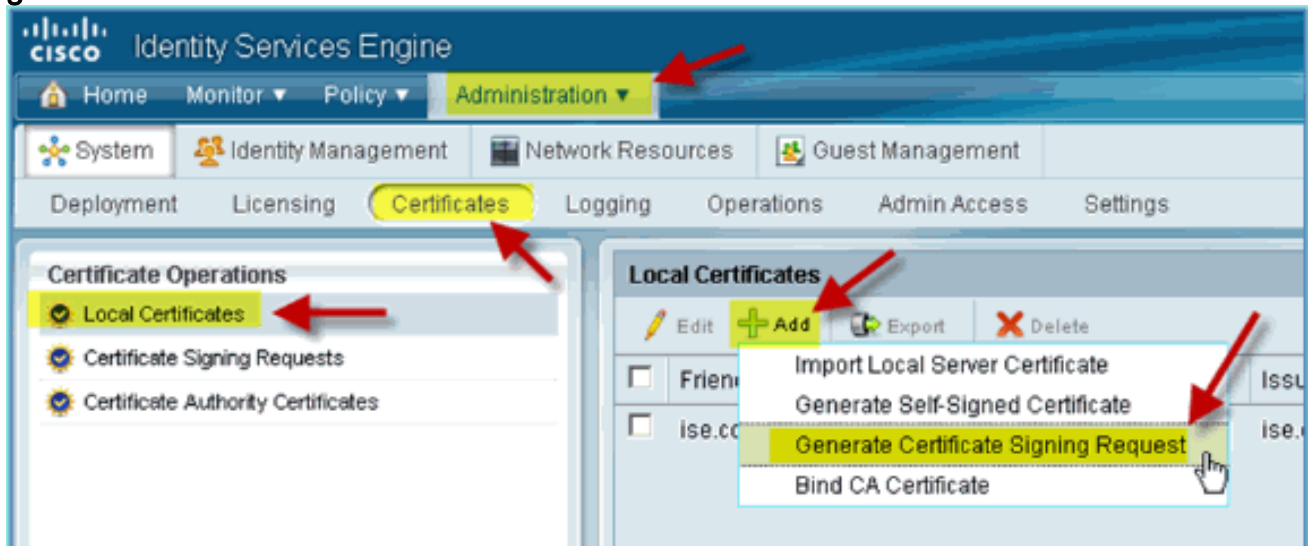


9. Bestätigen Sie, dass die Zertifizierungsstelle als Stammzertifizierungsstelle hinzugefügt wurde.



10. Gehen Sie in einem Browser zu **Administration > System > Certificates > Certificates Authority Certificates**.

11. Klicken Sie auf **Hinzufügen** und dann auf **Zertifikatsignierungsanforderung generieren**.



12. Senden Sie diese Werte: Zertifikatantragsteller: CN=ise.corp.rf-demo.com Schlüssellänge: 2048

Local Certificates > Generate Certificate Signing Request

▼ **Generate Certificate Signing Request**

**Certificate**

\* Certificate Subject

\* Key Length

Digest to Sign With SHA1

13. Die ISE fordert Sie auf, den CSR auf der CSR-Seite anzuzeigen. Klicken Sie auf OK.



14. Wählen Sie auf der Seite "ISE CSR" den CSR aus, und klicken Sie auf **Exportieren**.
15. Speichern Sie die Datei an einem beliebigen Speicherort (z. B. Downloads usw.).
16. Die Datei wird als \*.pem gespeichert.

Cisco Identity Services Engine Administration

System Identity Management Network Resources Guest Management

Deployment Licensing Certificates Logging Operations Admin Access Settings

Certificate Operations

- Local Certificates
- Certificate Signing Requests**
- Certificate Authority Certificates

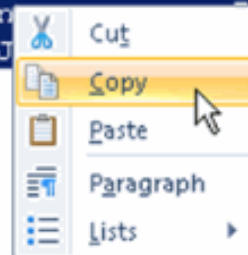
Certificate Signing Requests

Export Delete

<input checked="" type="checkbox"/>	Friendly Name	Certificate Subject	Key Length
<input checked="" type="checkbox"/>	ise.corp.rf-demo.com	CN=ise.corp.rf-demo.com	2048

17. Suchen Sie die CSR-Datei, und bearbeiten Sie sie mit Notepad/Wordpad/TextEdit.
18. Kopieren Sie den Inhalt (Alle auswählen > Kopieren).

```
-----BEGIN CERTIFICATE REQUEST-----
MIICyTCCAbECAQAwHzEdMBSGA1UEAxMUaXNlLmNvcnAucmYtZGVtby5jb20wggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDXaeWDSqfI64K59dyRLm8JAxan
WYTaAJ68/Ke206ws/K3BFAFJQhndQQ0hYVmGcJLVN03pXtRln/q/HBuglLIItIvbe
86FADPq3kUNb48UHcdR9b5rUs7B8T5E6banZia6eHSXjIzX4f0U7mVOrzALeAPDK
HXU+/y/gleyNL6P8zC4bvi/SZXhZp1OvTQpi+8lh14M5ROChhbPUnB3EGVaIVRiN
wYn8Ojvejbtg//k0CItGARlG2IFbBbgUpkMVhDQqgixp3wrlm3hi9JXgffEI f4EO
sirLrhvMSuSNESnIVWYrRLz5Xt4dMct+bu08xaEYPqgoukYjxsA9gn0bRDMJAgMB
AAGgZTBjBqkqhkiG9w0BCQ4xVjBUMASGA1UdDwQEAWICrDAdBgNVHQ4EFgQU2jmj
715rSw0yVb/vlWAYkK/YBwkWewYDVR0lBAwwCgYIKwYBBQUHAWewEQYJYIZIAYb4
QgEBBAQDAgZAMA0GCSqGSIb3DQEBBQUAA4IBAQBz4YPO9sN7WF2Htg+48300mw9q
gA/MMZsTioEPekcunrm+ZFtlAXajB32uwHHi1lc9Rn93TgOWPFxKEX9E89fzSWDK
J4qsQM7KEYOpQt4bia07188Lm6BBTk9mRhiTBwSF3dx0tlzfgiHc72kjWvxsgg/c
k8a7LHYgkgLRYBnpu15RjQ7wWijArH8cK1OrVT42riz7vK0g0nkWRHF52uiu3AkP
LPKQ72N2XYIXfu0jdgOaJjmsk6T9nLABVYQ6n...KDJTHchcwx6I1k/
V5QYBOjTYHXIPG8/ned9z3M0iZd2sm4XNS2bJ...W1ZuB6drHg9
-----END CERTIFICATE REQUEST-----
```



19. Öffnen Sie ein Browserfenster für <https://<Pod-AD>/certsrv>.
20. Klicken Sie auf **Zertifikat anfordern**.

## Microsoft Active Directory Certificate Services -- corp-RFDEMO-CA

### Welcome

Use this Web site to request a certificate for your Web browser to communicate with over the Web, sign and encrypt messages.

You can also use this Web site to download a certificate automatically for a pending request.

For more information about Active Directory Certificate Services, click the following link:

#### Select a task:

[Request a certificate](#)

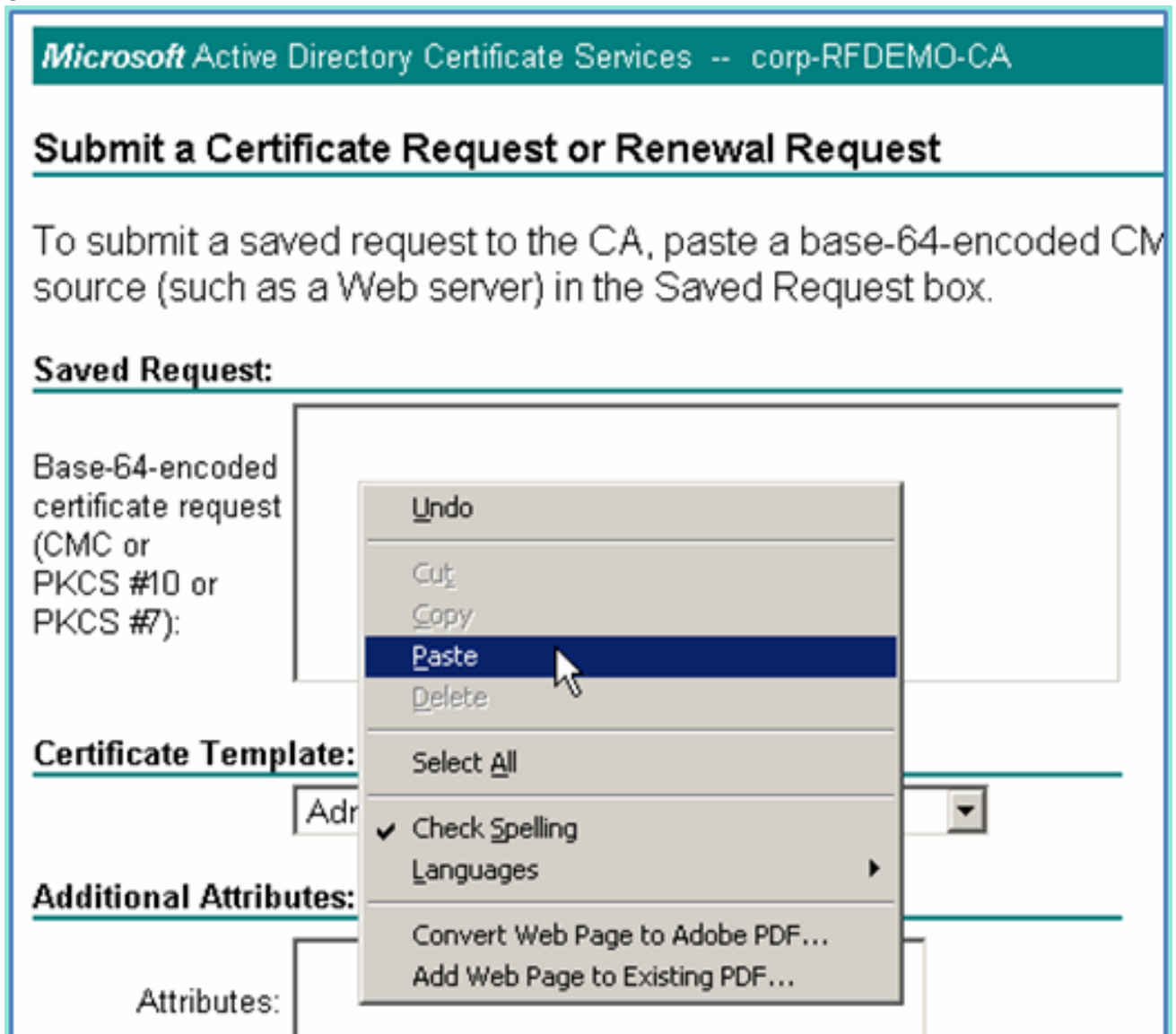
[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

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



22. Fügen Sie den CSR-Inhalt in das Feld "Gespeicherter Antrag" ein.



23. Wählen Sie **Webserver** als Zertifikatvorlage aus, und klicken Sie dann auf **Senden**.

Microsoft Active Directory Certificate Services -- corp-RFDEMO-CA

## Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC source (such as a Web server) in the Saved Request box.

**Saved Request:**

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

```
gA/MMZsTioEPekcunnm+ZFt1AXajB32uwHH11c9
J4qsQM7KEYOpQt4bia071S8Lm6BBTk9mRhiTBwSF
kSa7LHYgkgLRYBnpul5RjQ7wWijArH8cK1OrVT42
LPKQ72N2XYIXfu0jdgogaJjmsk6T9nLABVYQ6nKQx
V5QYBOjTYHXIPG8/ned9z3MOiZd2sm4XNS2bJfO/
-----END CERTIFICATE REQUEST-----
```

**Certificate Template:**

Web Server

**Additional Attributes:**

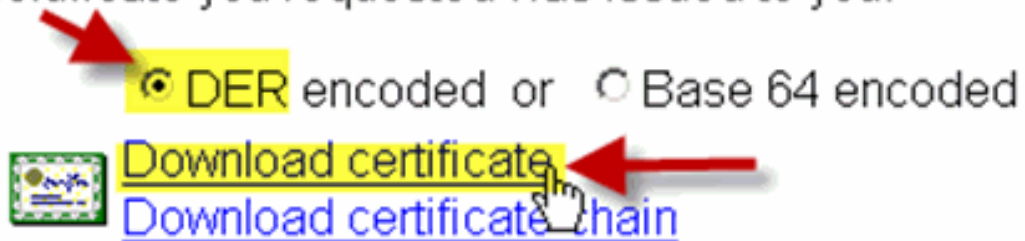
Attributes:

Submit >

24. Wählen Sie **DER-codiert** aus, und klicken Sie dann auf **Zertifikat herunterladen**.

## Certificate Issued

The certificate you requested was issued to you.

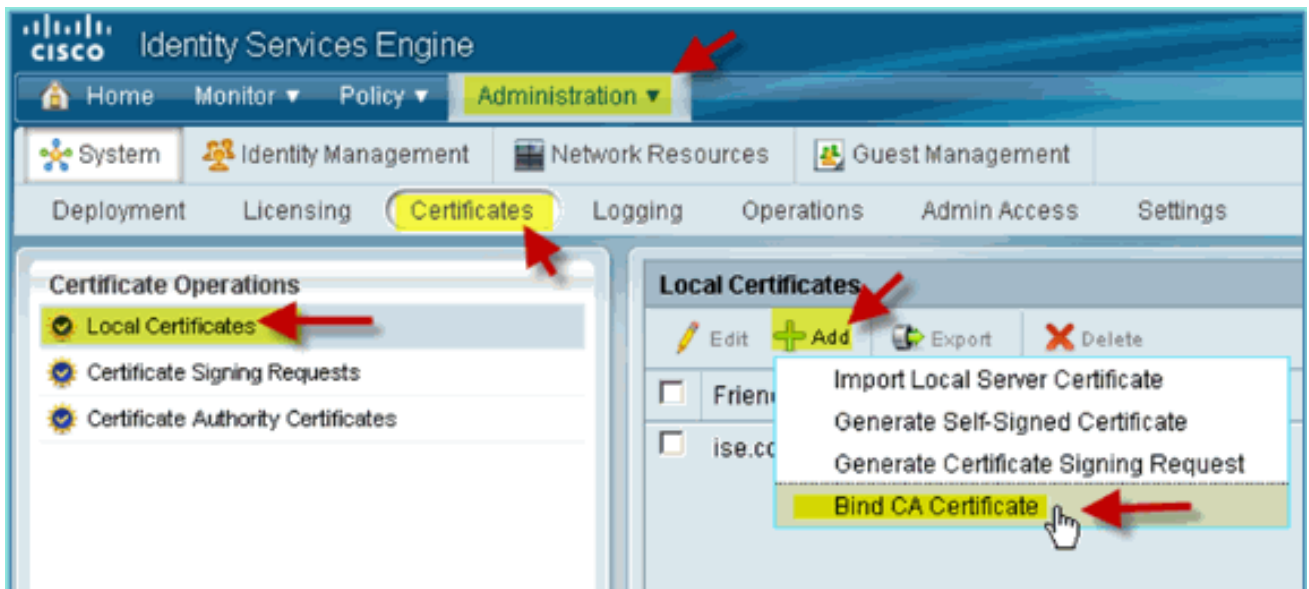


25. Speichern Sie die Datei an einem bekannten Speicherort (z. B. Downloads).

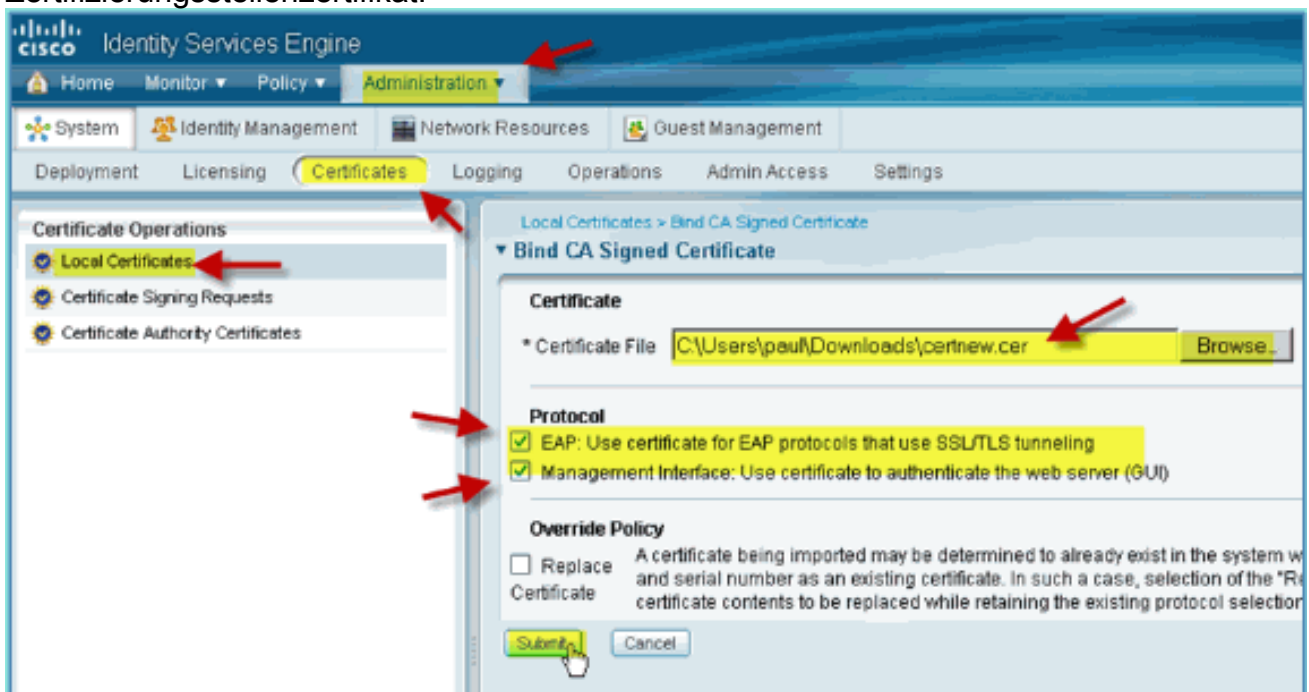
26. Gehen Sie zu **Administration > System > Certificates > Certificates Authority Certificates**.



27. Klicken Sie auf **Hinzufügen > CA-Zertifikat binden**.



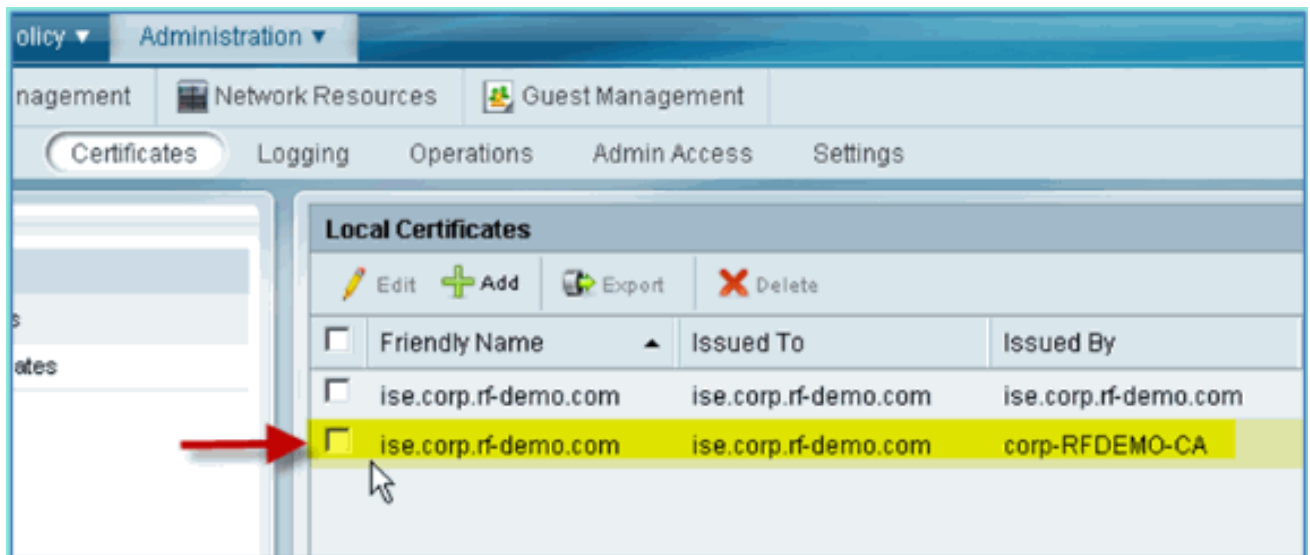
28. Navigieren Sie zum zuvor heruntergeladenen Zertifizierungsstellenzertifikat.



29. Wählen Sie sowohl **Protokoll-EAP** als auch **Verwaltungsschnittstelle** aus, und klicken Sie dann auf **Senden**.

30. Bestätigen Sie, dass die Zertifizierungsstelle als Stammzertifizierungsstelle hinzugefügt wurde.



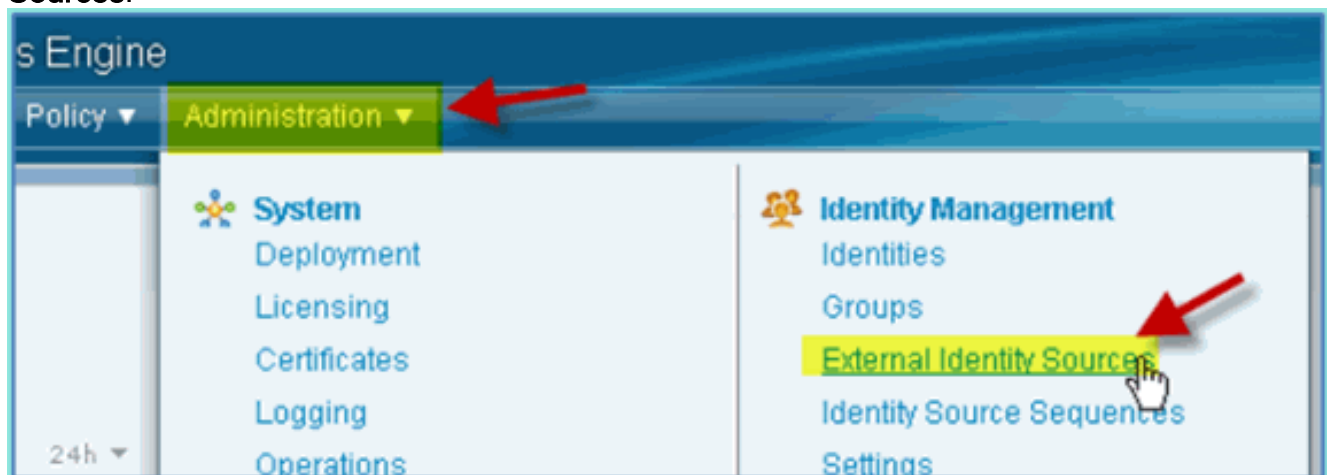


## Windows 2008 Active Directory-Integration

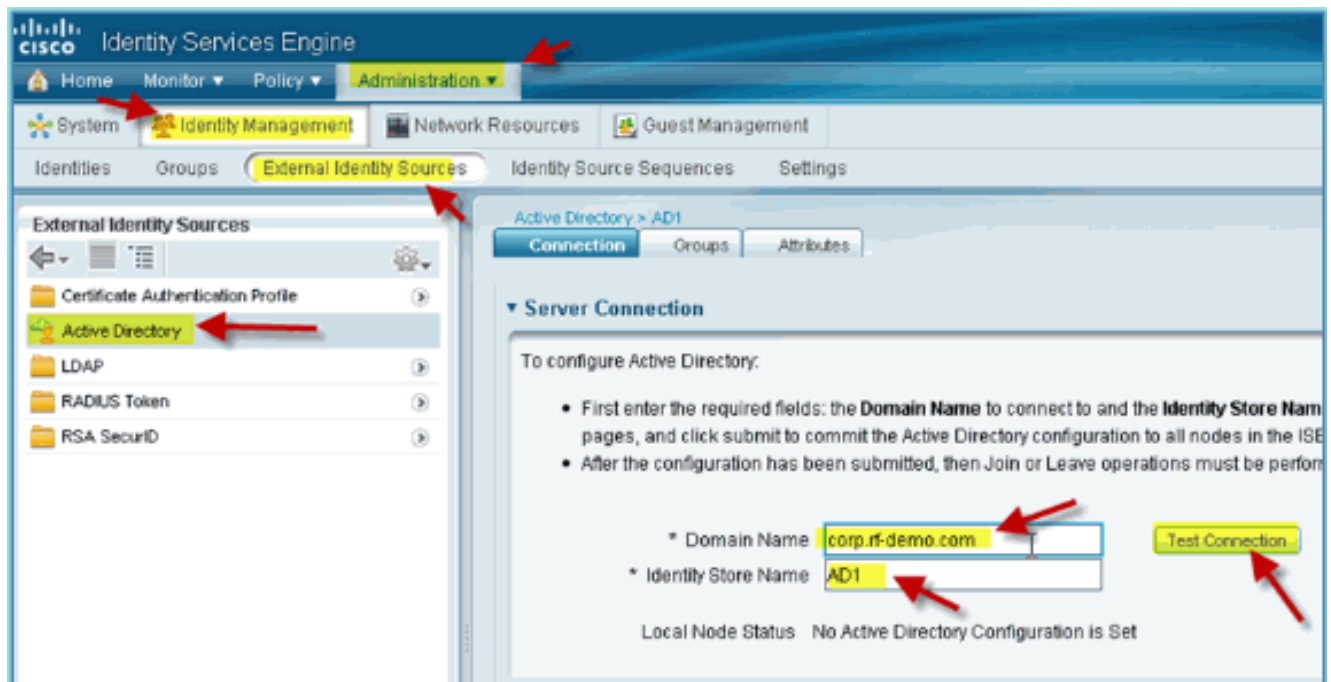
Die ISE kann direkt mit Active Directory (AD) kommunizieren, um Benutzer-/Computerauthentifizierung oder Autorisierungsinformationen und Benutzerattribute abzurufen. Um mit AD zu kommunizieren, muss die ISE einer AD-Domäne "beigetreten" sein. In dieser Übung werden Sie der ISE in einer AD-Domäne beitreten und überprüfen, ob die AD-Kommunikation ordnungsgemäß funktioniert.

Führen Sie diese Schritte aus:

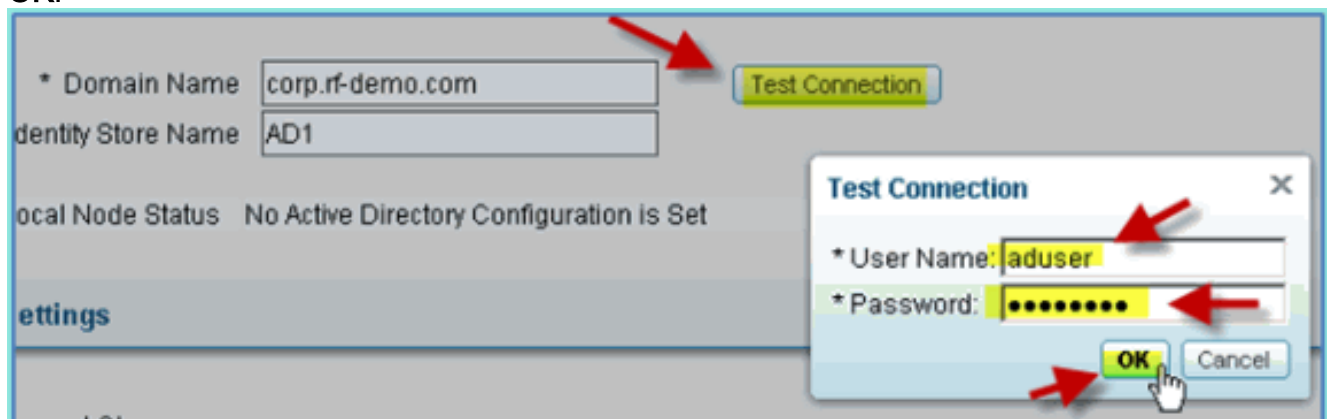
1. Um der ISE zur AD-Domäne beizutreten, gehen Sie von ISE zu **Administration > Identity Management > External Identity Sources**.



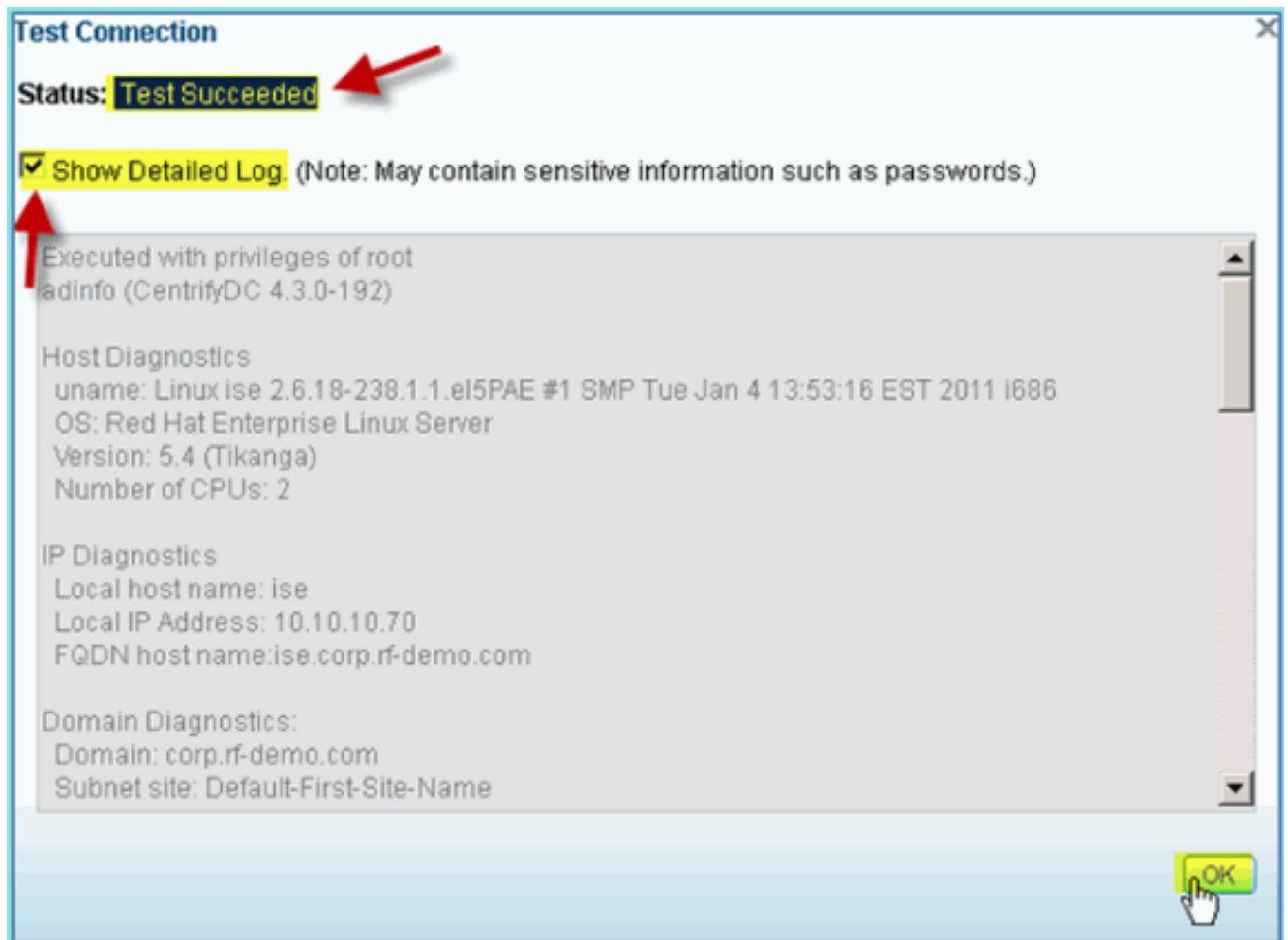
2. Wählen Sie im linken Bereich (Externe Identitätsquellen) die Option **Active Directory aus**.
3. Klicken Sie auf der rechten Seite auf die Registerkarte **Verbindung**, und geben Sie Folgendes ein: Domänenname: corp.rf-demo.com Name des Identitätsspeichers: AD1



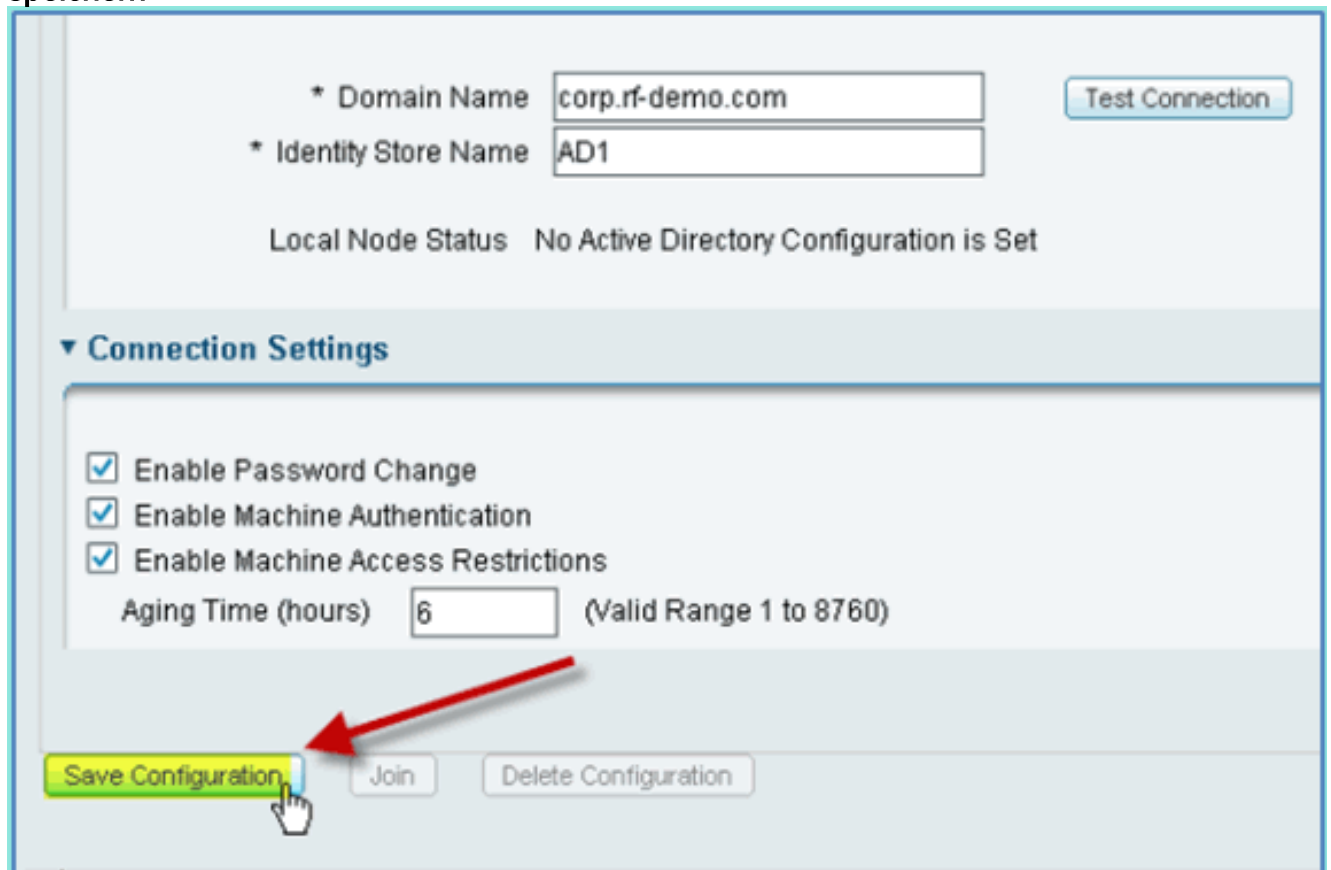
4. Klicken Sie auf **Verbindung testen**. Geben Sie den AD-Benutzernamen ein (aduser/Cisco123), und klicken Sie dann auf **OK**.



5. Bestätigen Sie, dass im Teststatus **Test erfolgreich** angezeigt wird.  
6. Wählen Sie **Detailliertes Protokoll anzeigen** aus, und beobachten Sie Details, die zur Fehlerbehebung nützlich sind. Klicken Sie auf **OK**, um fortzufahren.

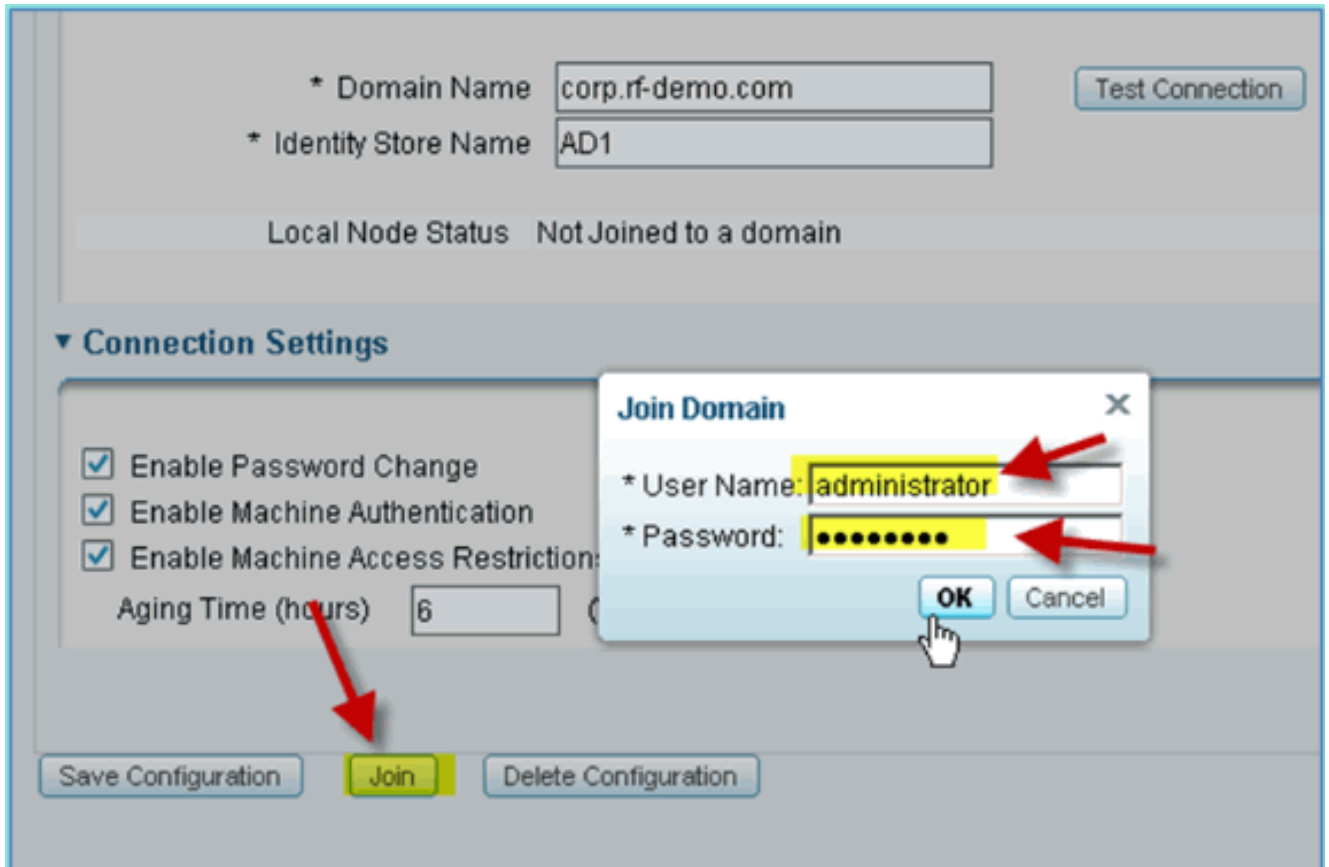


7. Klicken Sie auf **Konfiguration speichern**.

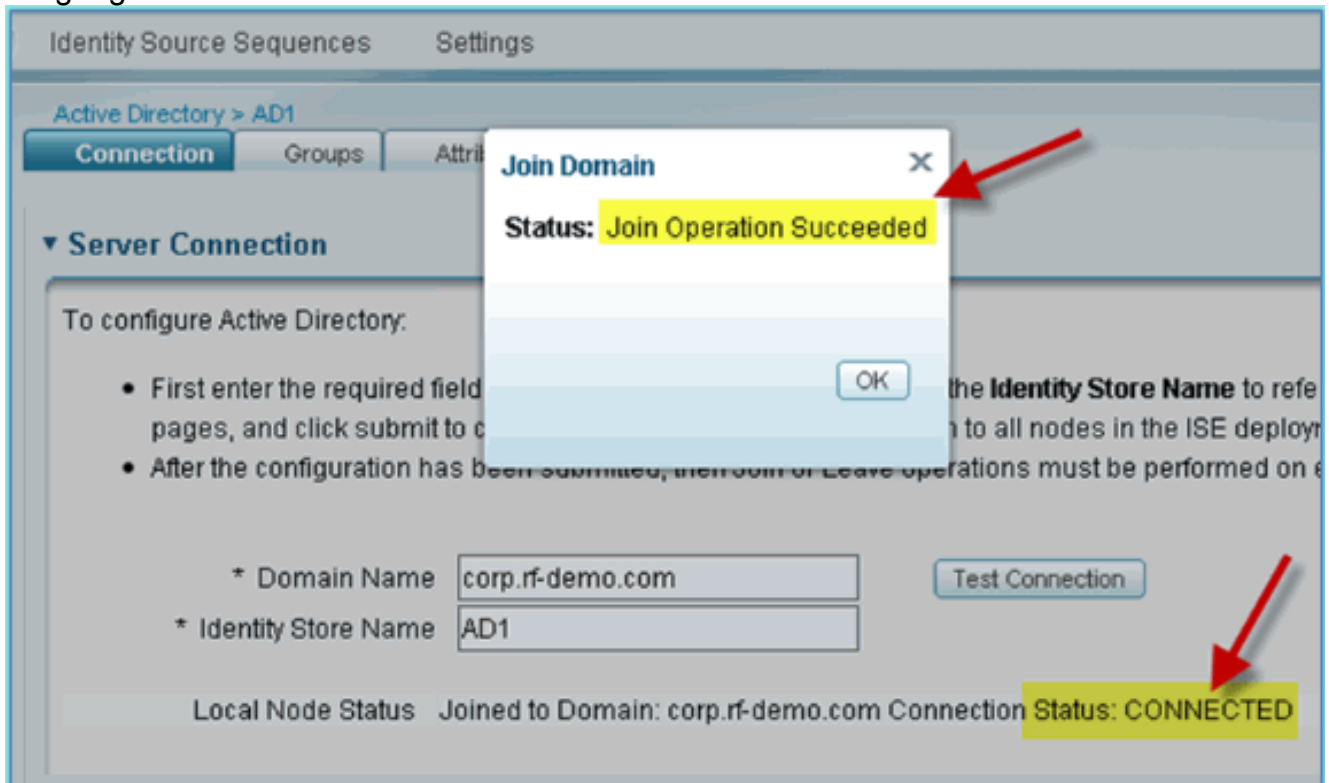


8. Klicken Sie auf **Beitreten**. Geben Sie den AD-Benutzer ein (Administrator/Cisco123), und klicken Sie dann auf

OK.



9. Bestätigen Sie, dass der Status der Beitrittsoperation "Erfolgreich" anzeigt, und klicken Sie dann auf **OK**, um fortzufahren. Der Serververbindungsstatus zeigt **VERBUNDEN** an. Wenn sich dieser Status jederzeit ändert, hilft eine Testverbindung bei der Fehlerbehebung im Zusammenhang mit den AD-Vorgängen.



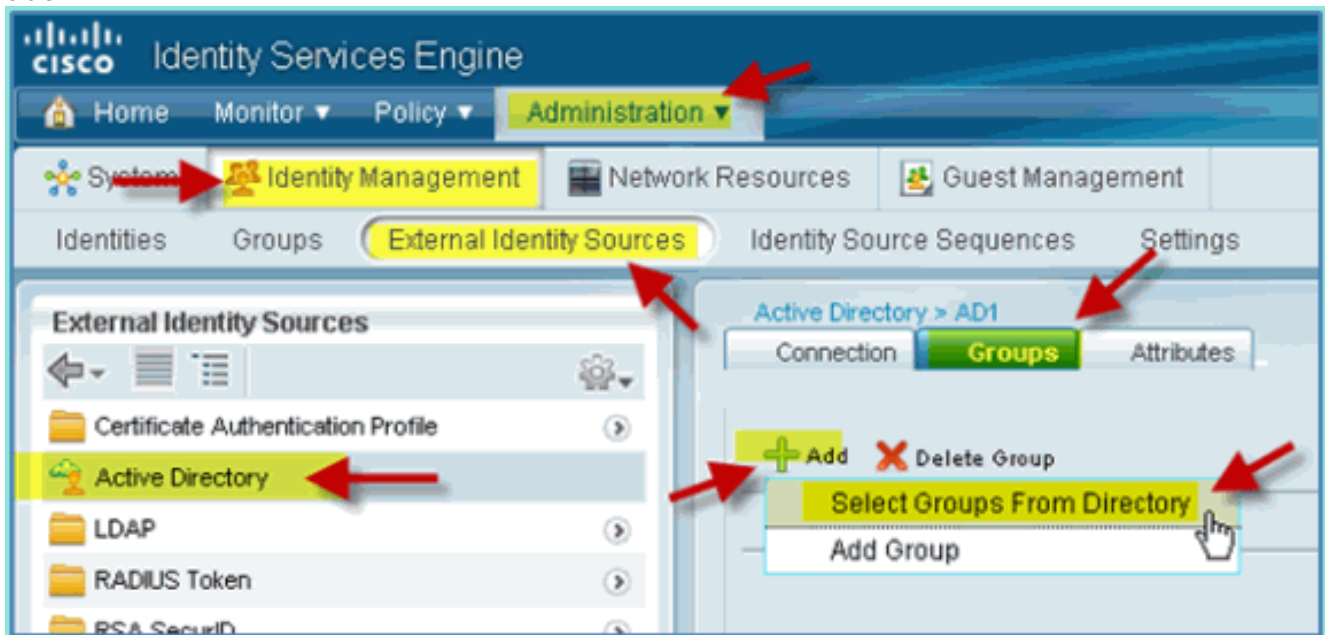
## Active Directory-Gruppen hinzufügen

Beim Hinzufügen von AD-Gruppen ist eine detailliertere Kontrolle über ISE-Richtlinien möglich. AD-Gruppen können beispielsweise nach Funktionsrollen (Mitarbeiter- oder Vertragsgruppen) unterschieden werden, ohne dass der entsprechende Fehler in früheren ISE 1.0-Übungen aufgetreten wäre, bei denen die Richtlinien nur auf Benutzer beschränkt waren.

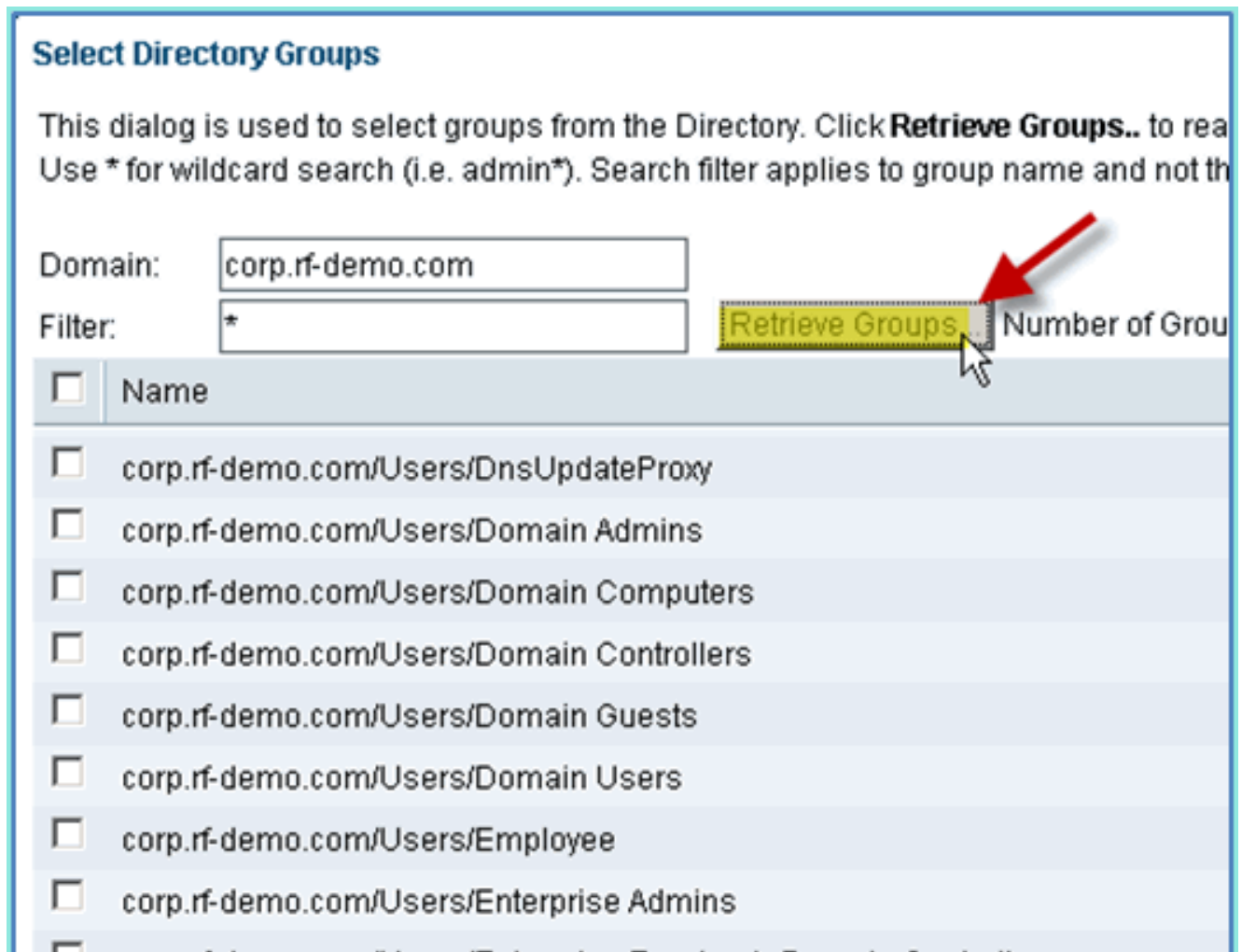
In dieser Übung werden nur die Domänenbenutzer und/oder die Gruppe "Mitarbeiter" verwendet.

Führen Sie diese Schritte aus:

1. Gehen Sie von der ISE zu **Administration > Identity Management > External Identity Sources**.
2. Wählen Sie Registerkarte **Active Directory > Gruppen** aus.
3. Klicken Sie auf **+Hinzufügen**, und wählen Sie **Gruppen aus Verzeichnis** aus.



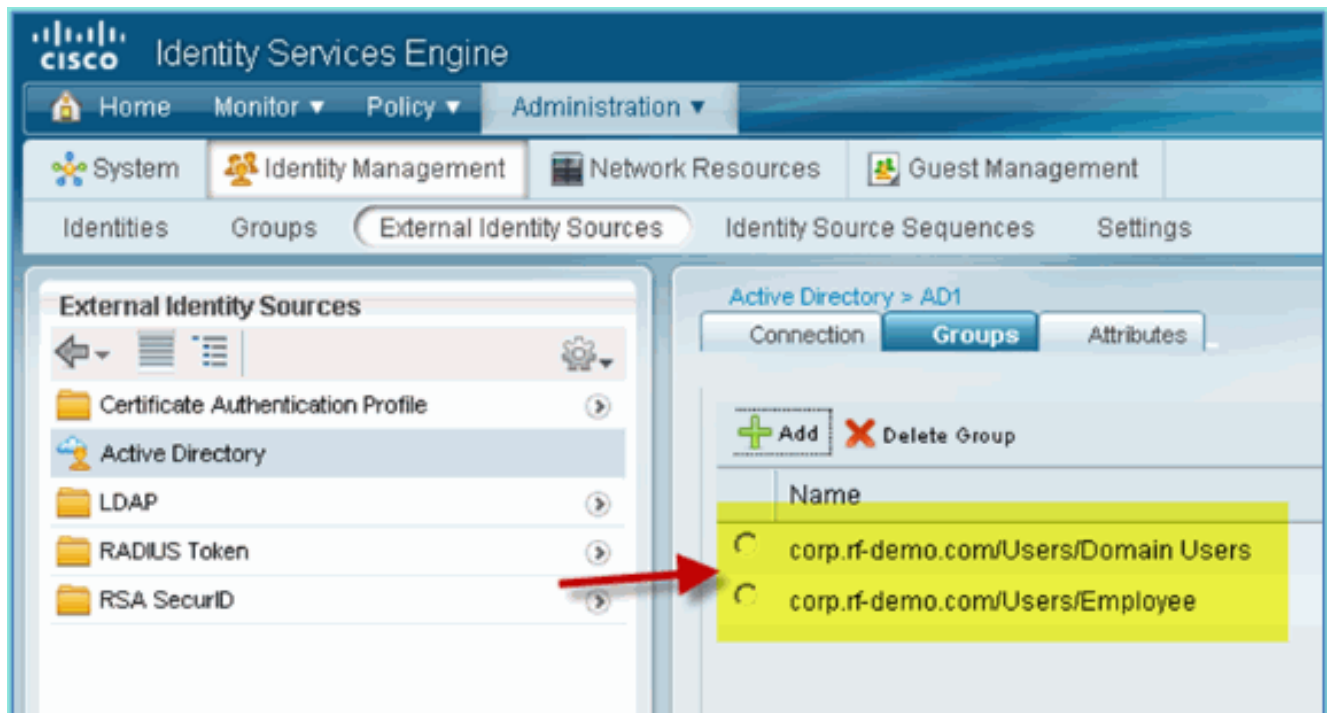
4. Akzeptieren Sie im Follow-up-Fenster (Wählen Sie Verzeichnisgruppen aus) die Standardeinstellungen für Domäne (corp-rf-demo.com) und Filter (\*). Klicken Sie dann auf **Gruppen abrufen**.



5. Aktivieren Sie die Kontrollkästchen für **Domänenbenutzer** und **Mitarbeitergruppen**. Klicken Sie abschließend auf **OK**.



6. Bestätigen Sie, dass die Gruppen der Liste hinzugefügt wurden.

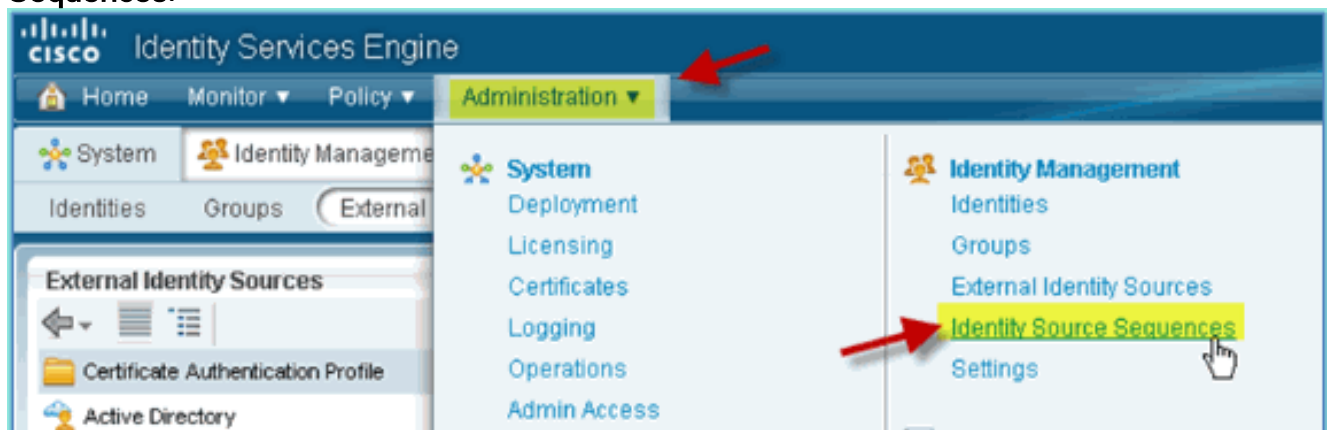


## Identitätsquellensequenz hinzufügen

Standardmäßig ist ISE so konfiguriert, dass interne Benutzer für den Authentifizierungsspeicher verwendet werden. Wenn AD hinzugefügt wird, kann eine Prioritätsreihenfolge erstellt werden, um das AD einzuschließen, das die ISE zur Überprüfung der Authentifizierung verwendet.

Führen Sie diese Schritte aus:

1. Navigieren Sie von der ISE zu **Administration > Identity Management > Identity Source Sequences**.



2. Klicken Sie auf **+Hinzufügen**, um eine neue Sequenz hinzuzufügen.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Monitor', 'Policy', and 'Administration'. Below this, there are tabs for 'System', 'Identity Management', 'Network Resources', and 'Guest Management'. The 'Identity Source Sequences' page is active, showing a table of existing sequences. The 'Add' button is highlighted with a yellow box and a red arrow pointing to it.

Name	Description	Identity Stores
<input type="checkbox"/> Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users
<input type="checkbox"/> Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users

3. Geben Sie den neuen Namen ein: **AD\_Internal**. Fügen Sie dem Feld "Ausgewählt" alle verfügbaren Quellen hinzu. Ordnen Sie das AD1 dann nach Bedarf neu an, sodass es an die Spitze der Liste verschoben wird. Klicken Sie auf **Senden**.



Identities Groups External Identity Sources **Identity Source Sequences** Settings

Identity Source Sequences List > New Identity Source Sequence

**▼ Identity Source Sequence**

\* Name

Description

**▼ Certificate Based Authentication**

Select Certificate Authentication Profile

**▼ Authentication Search List**

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
	AD1 Internal Users Internal Endpoints

**▼ Advanced Search List Settings**

Select the action to be performed if a selected identity store cannot be accessed for authentication

Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

Treat as if the user was not found and proceed to the next store in the sequence

4. Bestätigen Sie, dass die Sequenz der Liste hinzugefügt wurde.

Identity Services Engine

Home Monitor Policy Administration

System Identity Management Network Resources Guest Management

Identities Groups External Identity Sources **Identity Source Sequences** Settings

**Identity Source Sequences**

Edit Add Duplicates Delete Filter

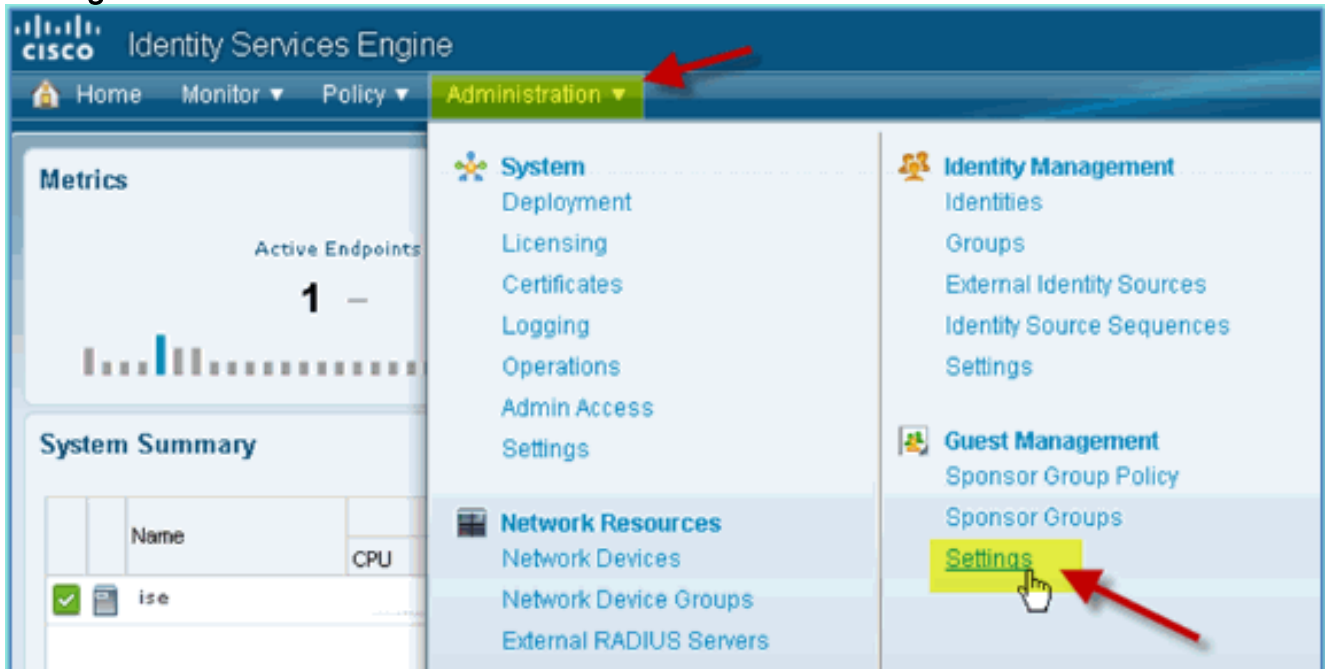
Name	Description	Identity Stores
<b>AD_Internal</b>		AD1, Internal Endpoints, Internal Users
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users

# ISE Wireless Sponsored Guest Access mit integriertem AD

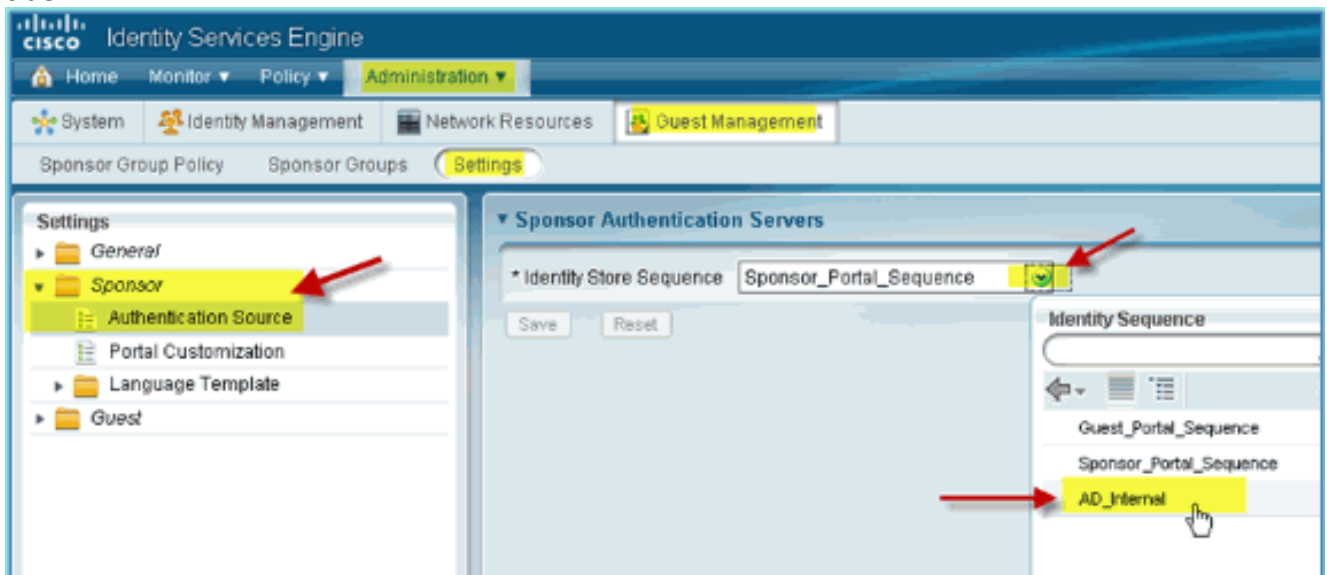
Die ISE kann so konfiguriert werden, dass Gäste mit Richtlinien unterstützt werden, damit AD-Domänenbenutzer den Gastzugriff sponsern können.

Führen Sie diese Schritte aus:

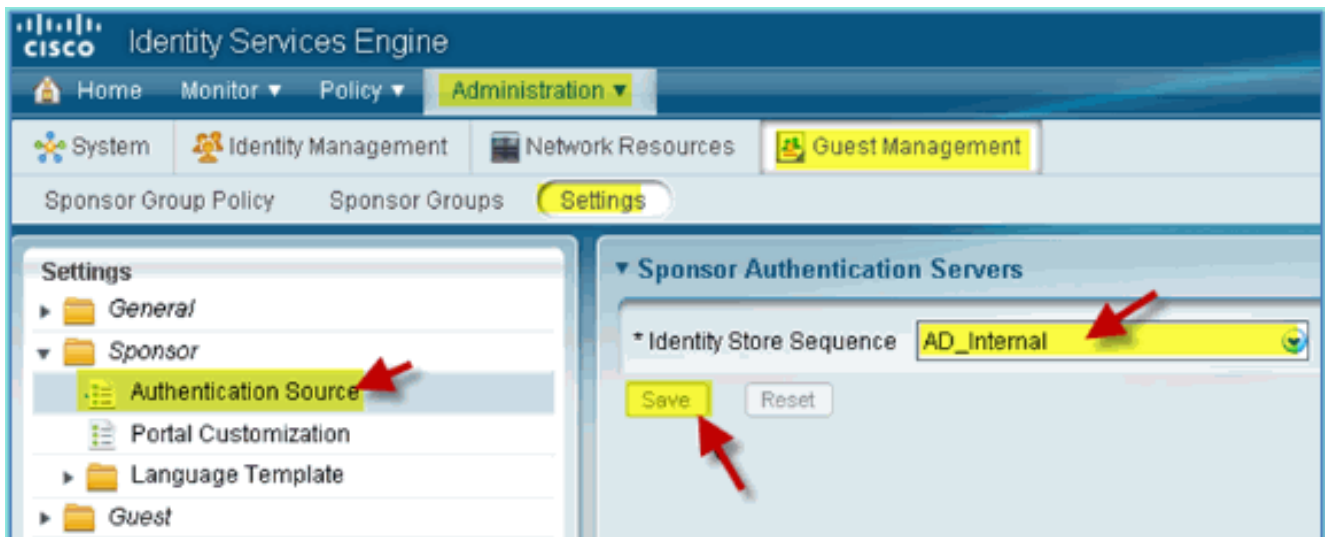
1. Navigieren Sie von der ISE zu **Administration > Guest Management > Settings**.



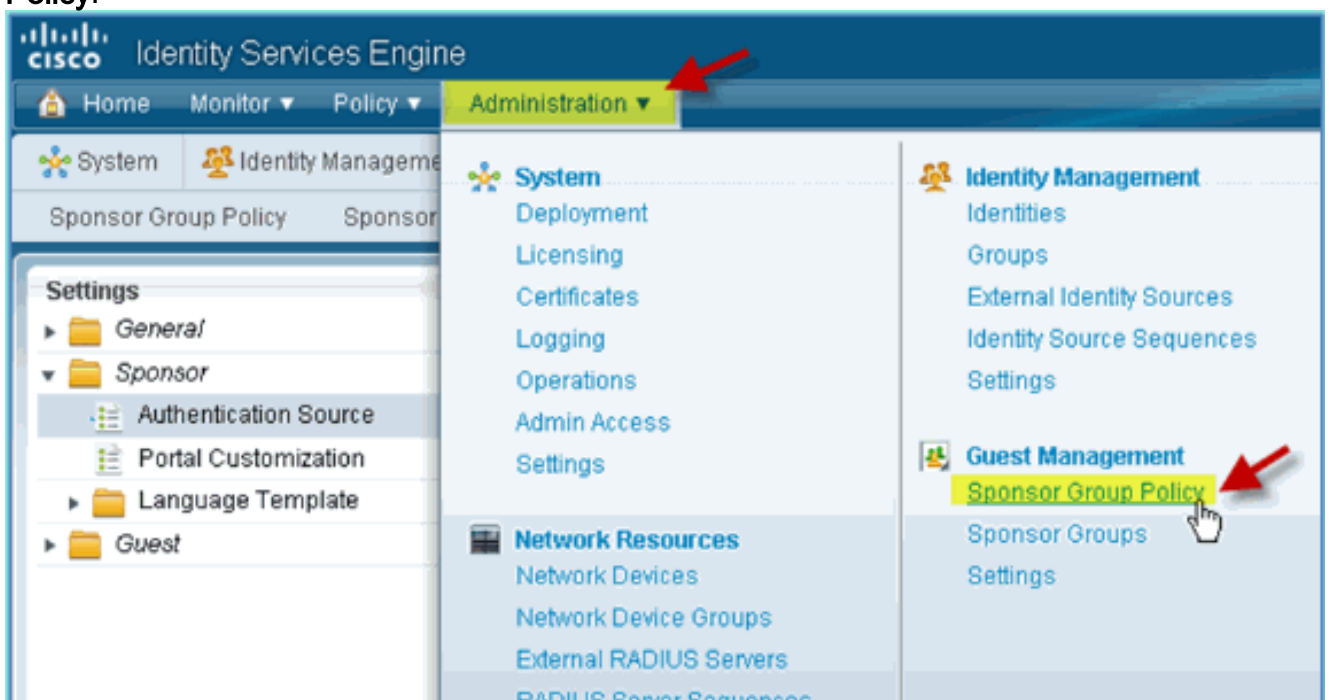
2. Erweitern Sie **Sponsor**, und klicken Sie auf **Authentifizierungsquelle**. Wählen Sie dann **AD\_Internal** als Identity Store Sequence aus.



3. Bestätigen Sie **AD\_Internal** als Identitätsspeichersequenz. Klicken Sie auf **Speichern**.



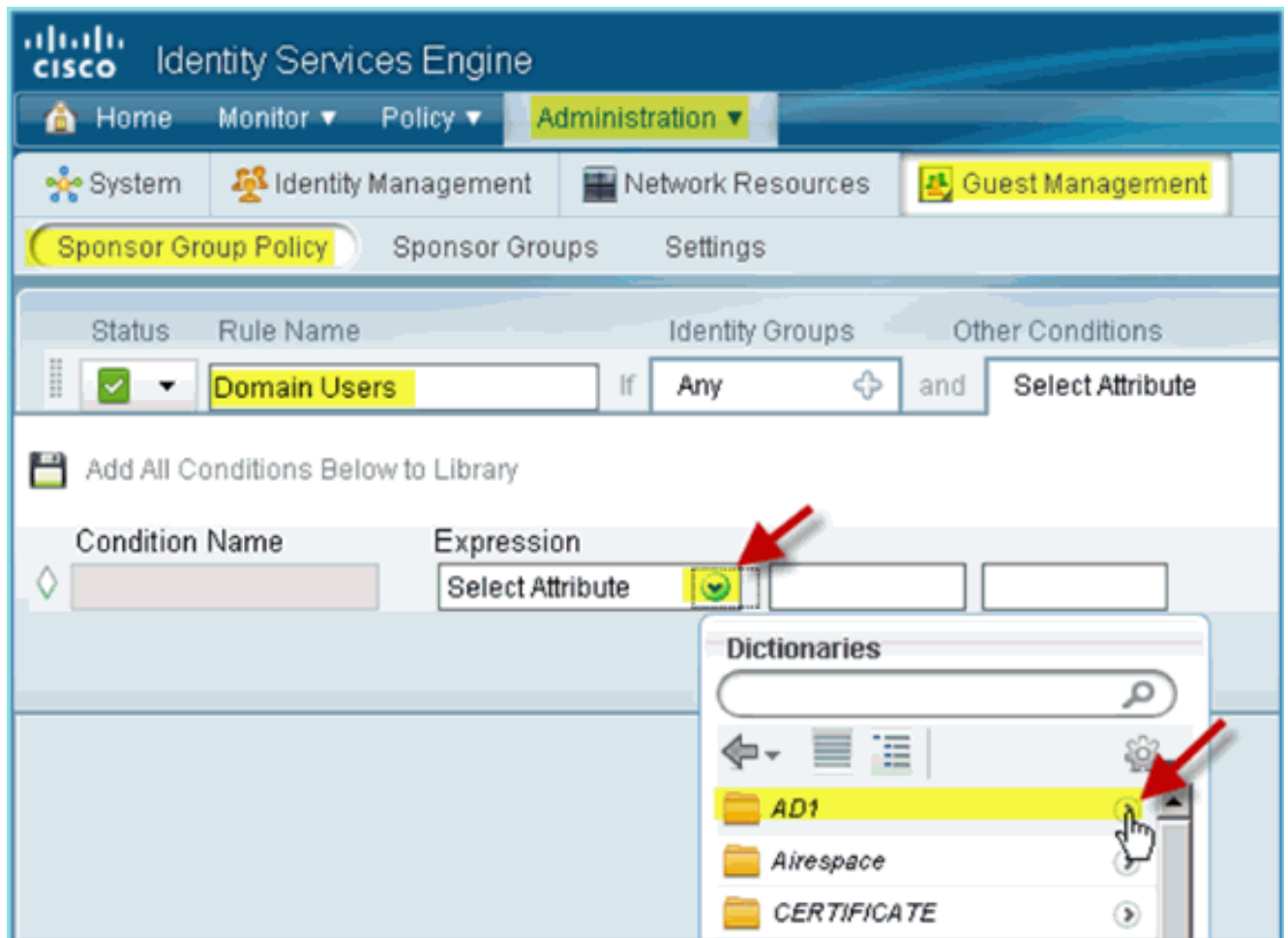
4. Navigieren Sie zu **Administration > Guest Management > Sponsor Group Policy**.



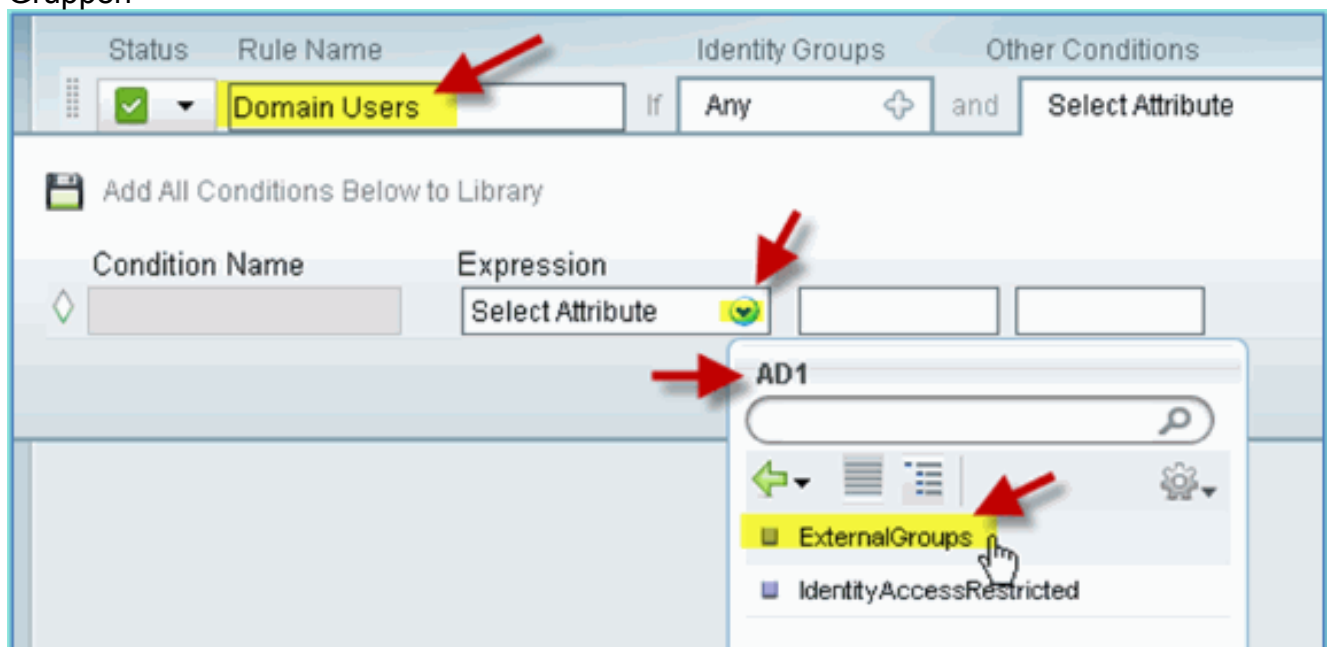
5. Einfügen einer neuen Richtlinie oberhalb der ersten Regel (klicken Sie rechts auf das Symbol **Aktionen**).



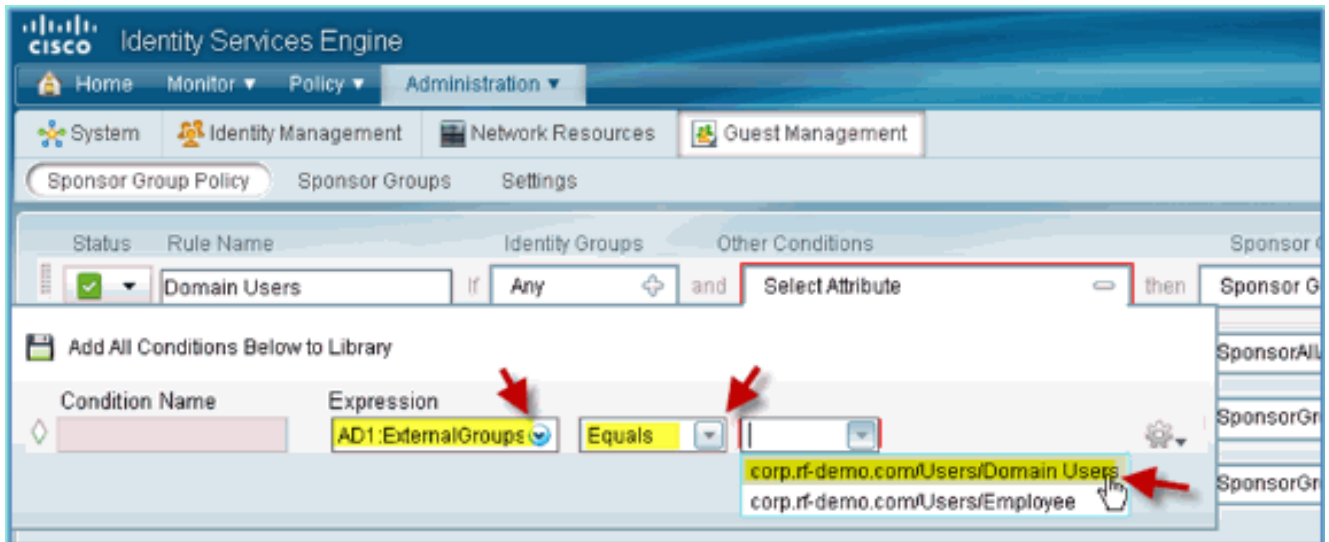
6. Erstellen Sie für die neue Sponsorgruppenrichtlinie Folgendes: Regelname: Domänenbenutzer/Identitätsgruppen: Alle Weitere Bedingungen: (Neu erstellen/Erweitert) > AD1



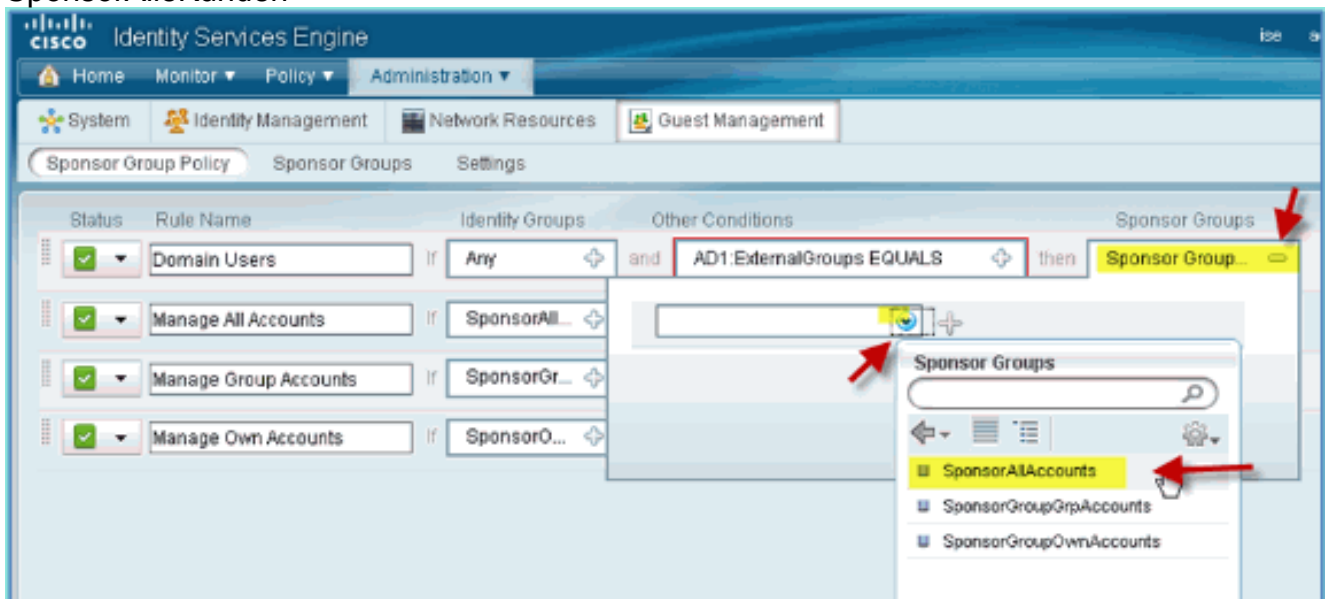
AD1: Externe  
Gruppen



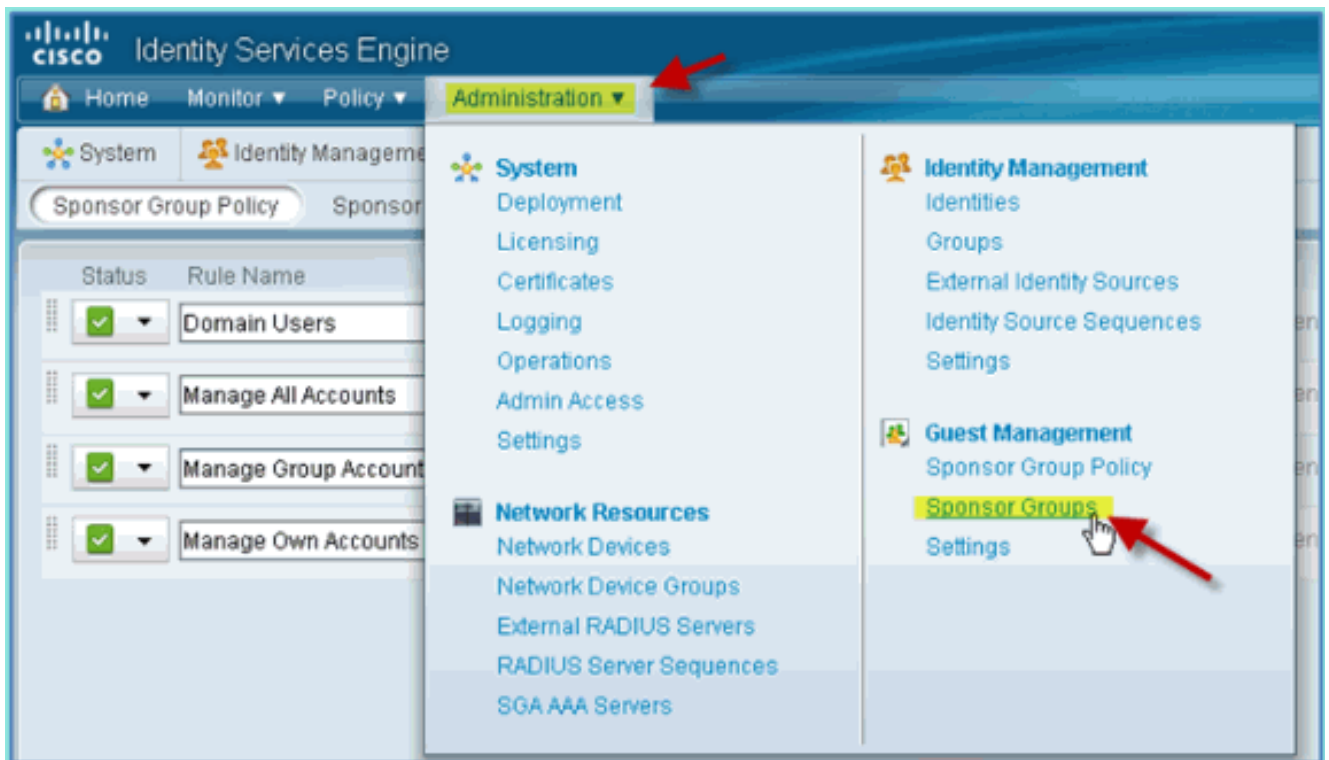
AD1 External Groups > Equals > corp.rf-demo.com/Users/Domain  
Benutzer



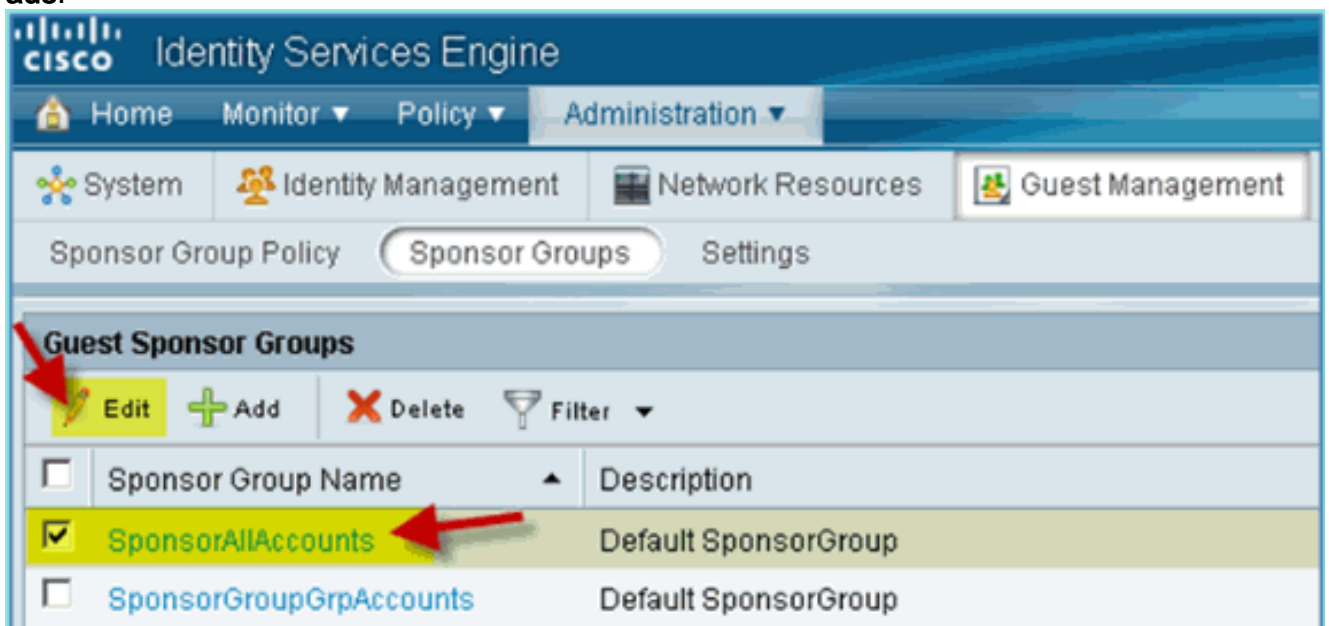
7. Legen Sie in Sponsorgruppen Folgendes fest: Sponsorengruppen: SponsorAlleKunden



8. Navigieren Sie zu **Administration > Guest Management > Sponsor Groups**.



9. Wählen Sie Bearbeiten > **SponsorAllAccounts** aus.



10. Wählen Sie die Autorisierungsstufen aus, und legen Sie Folgendes fest: Gastpasswort anzeigen:  
Ja

Identity Services Engine

Home Monitor Policy Administration

System Identity Management Network Resources Guest Management

Sponsor Group Policy Sponsor Groups Settings

Sponsor Group List > SponsorAllAccounts

General Authorization Levels Guest Roles Time Profiles

Allow Login	Yes
Create Accounts	Yes
Create Bulk Accounts	Yes
Create Random Accounts	Yes
Import CSV	Yes
Send Email	Yes
Send SMS	No
<b>View Guest Password</b>	<b>Yes</b>
Allow Printing Guest Details	Yes
View/Edit Accounts	All Accounts
Suspend/Reinstate Accounts	All Accounts
* Account Start Time	1 Days (Valid Range 1 to 999999999)
* Maximum Duration of Account	5 Days (Valid Range 1 to 999999999)

Save Reset

## Konfigurieren von SPAN auf dem Switch

Konfigurieren von SPAN - Die ISE-mgt/probe-Schnittstelle grenzt an L2 der WLC-Managementsschnittstelle an. Der Switch kann für SPAN und andere Schnittstellen konfiguriert werden, z. B. Mitarbeiter- und Gastschnittstellen-VLANs.

```
Podswitch(config)#monitor session 1 source vlan10 , 11 , 12
Podswitch(config)#monitor session 1 destination interface Fa0/8
ISE virtual probe interface.
```

## Referenz: Wireless-Authentifizierung für Apple MAC OS X

Verknüpfen Sie den WLC über eine authentifizierte SSID als INTERNEN Benutzer (oder

integrierten AD-Benutzer ) mit einem drahtlosen Apple Mac OS X-Laptop. Überspringen, wenn nicht zutreffend.

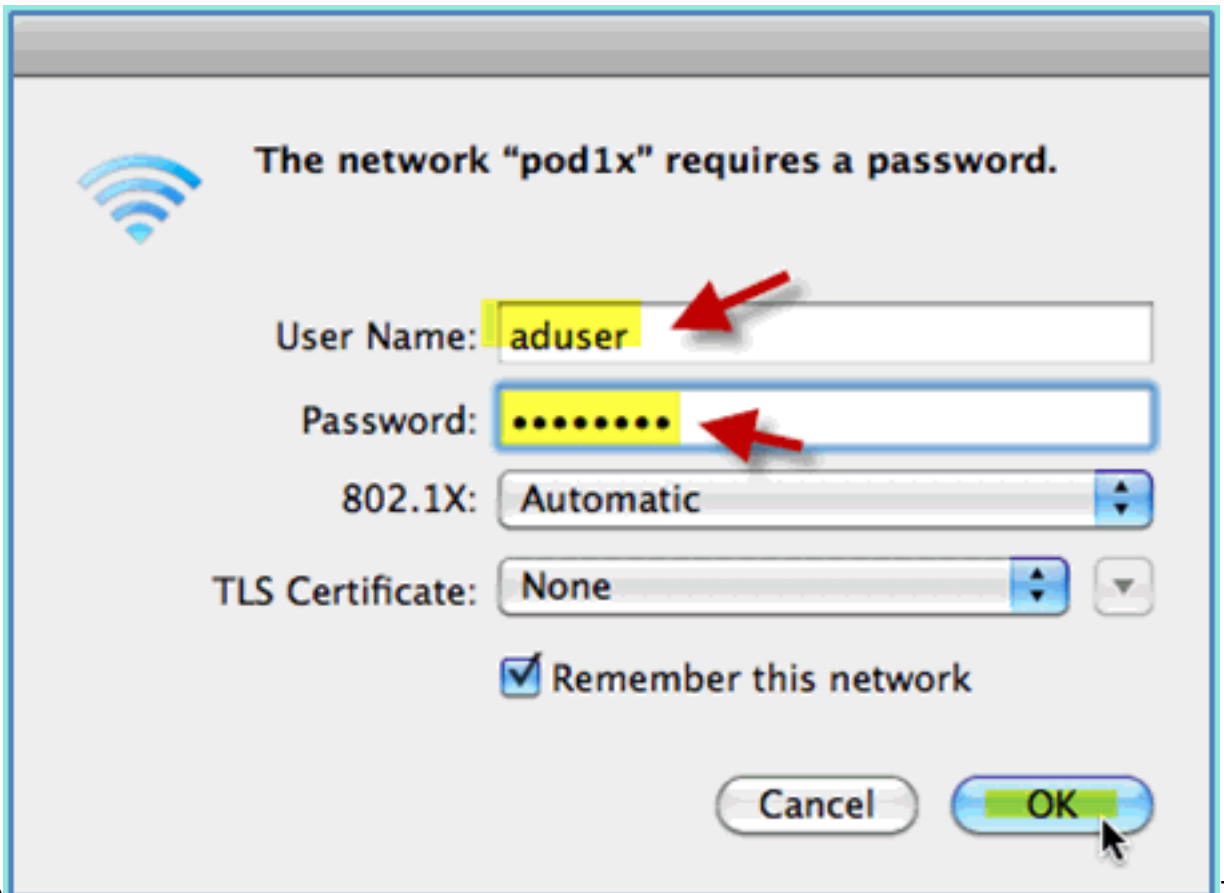
1. Navigieren Sie auf einem Mac zu den WLAN-Einstellungen. Aktivieren Sie WIFI, wählen Sie dann die 802.1X-fähige POD-SSID aus, die in der vorherigen Übung erstellt wurde, und stellen Sie eine Verbindung mit dieser



her.

2. Geben Sie die folgenden Informationen an, um eine Verbindung herzustellen: Benutzernamen: aduser (bei AD), employee (intern - Mitarbeiter), contract (intern - Auftragnehmer) Kennwort: XXXX802.1x: automatisch TLS-Zertifikat:





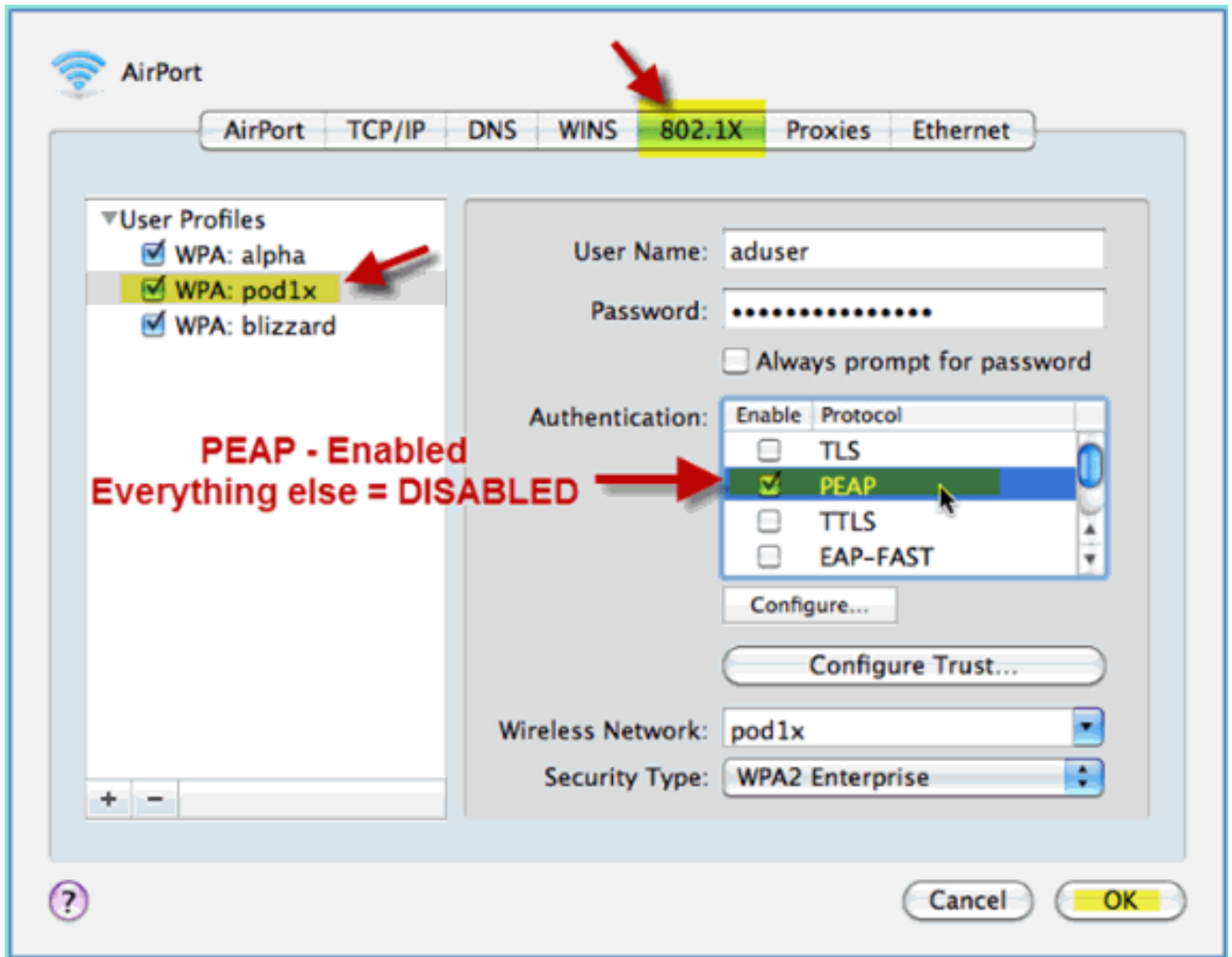
Keine

Z

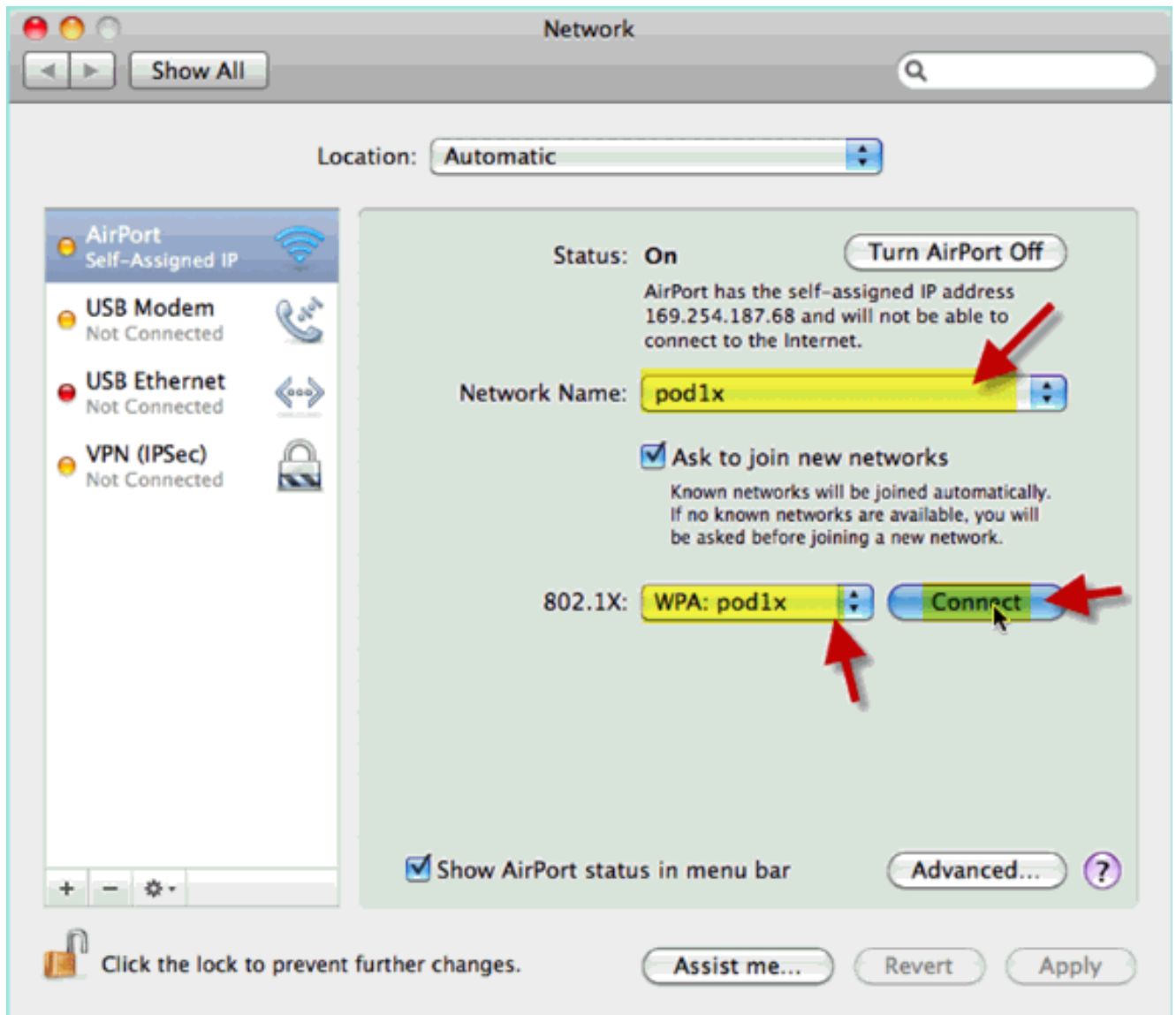
u diesem Zeitpunkt ist möglicherweise keine Verbindung zwischen dem Laptop und dem Computer hergestellt. Darüber hinaus kann die ISE einen Fehler folgendermaßen auslösen:

Authentication failed :12514 EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client certificates chain

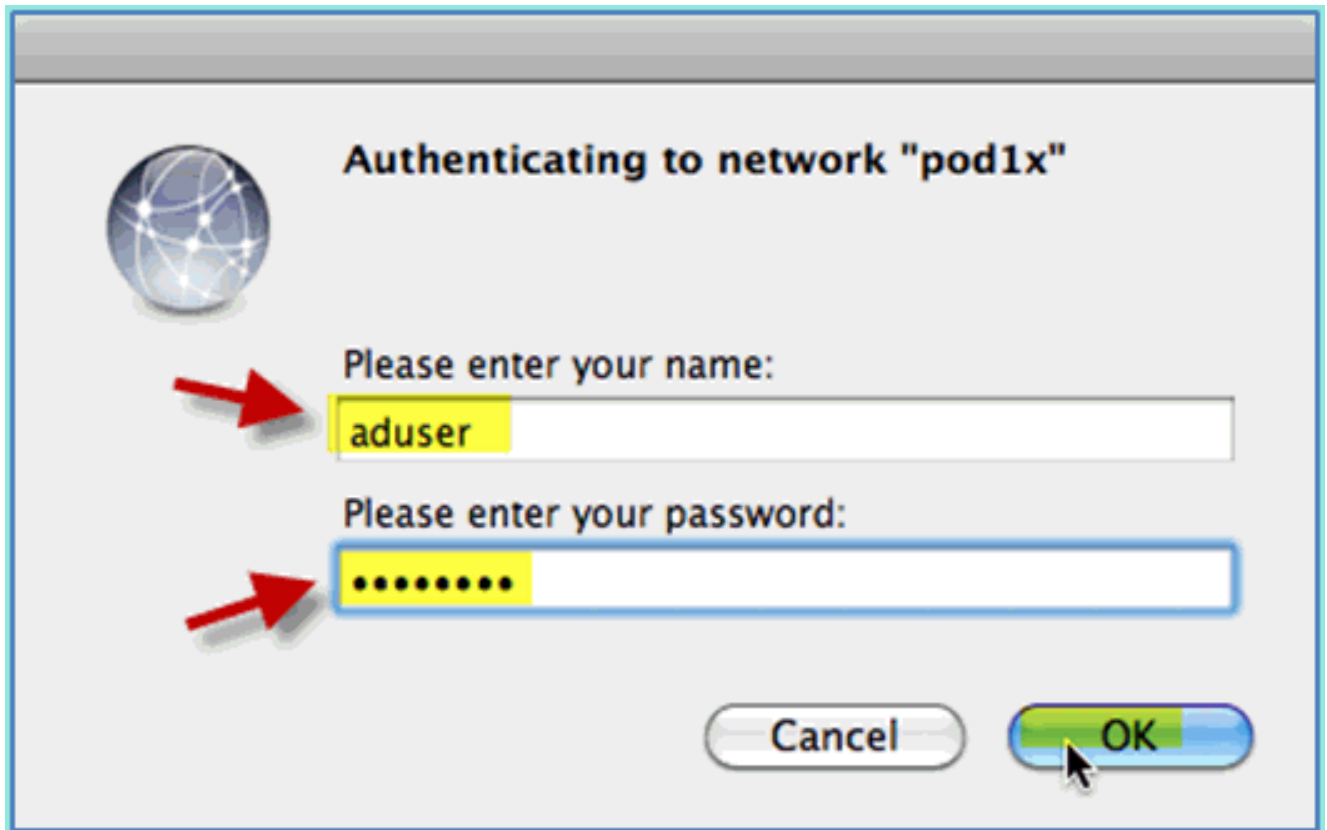
3. Gehen Sie zu **System Preference > Network > Airport > 802.1X** setting, und legen Sie das neue POD SSID/WPA-Profil Authentication auf: TLS: Deaktiviert PEAP: Aktiviert TTLS: Deaktiviert EAP-FAST: Deaktiviert



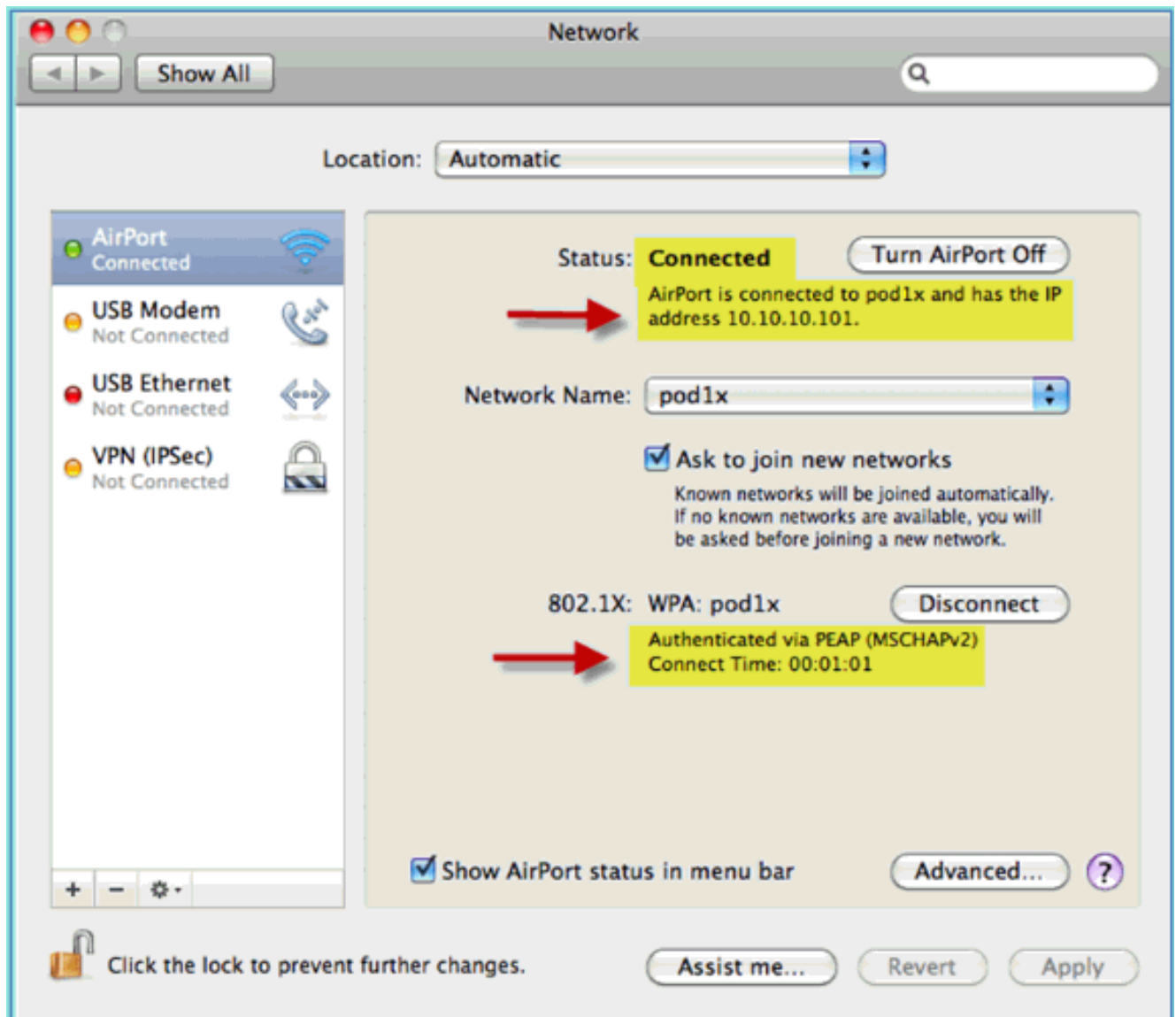
4. Klicken Sie auf **OK**, um fortzufahren und die Einstellung zu speichern.
5. Wählen Sie im Bildschirm "Network" das entsprechende SSID + 802.1X WPA-Profil aus, und klicken Sie auf **Connect**.



6. Das System fordert Sie möglicherweise zur Eingabe eines Benutzernamens und Kennworts auf. Geben Sie den AD-Benutzer und das AD-Kennwort ein (aduser/XXXX), und klicken Sie dann auf OK.



Der Client sollte **Connected** via PEAP mit einer gültigen IP-Adresse anzeigen.

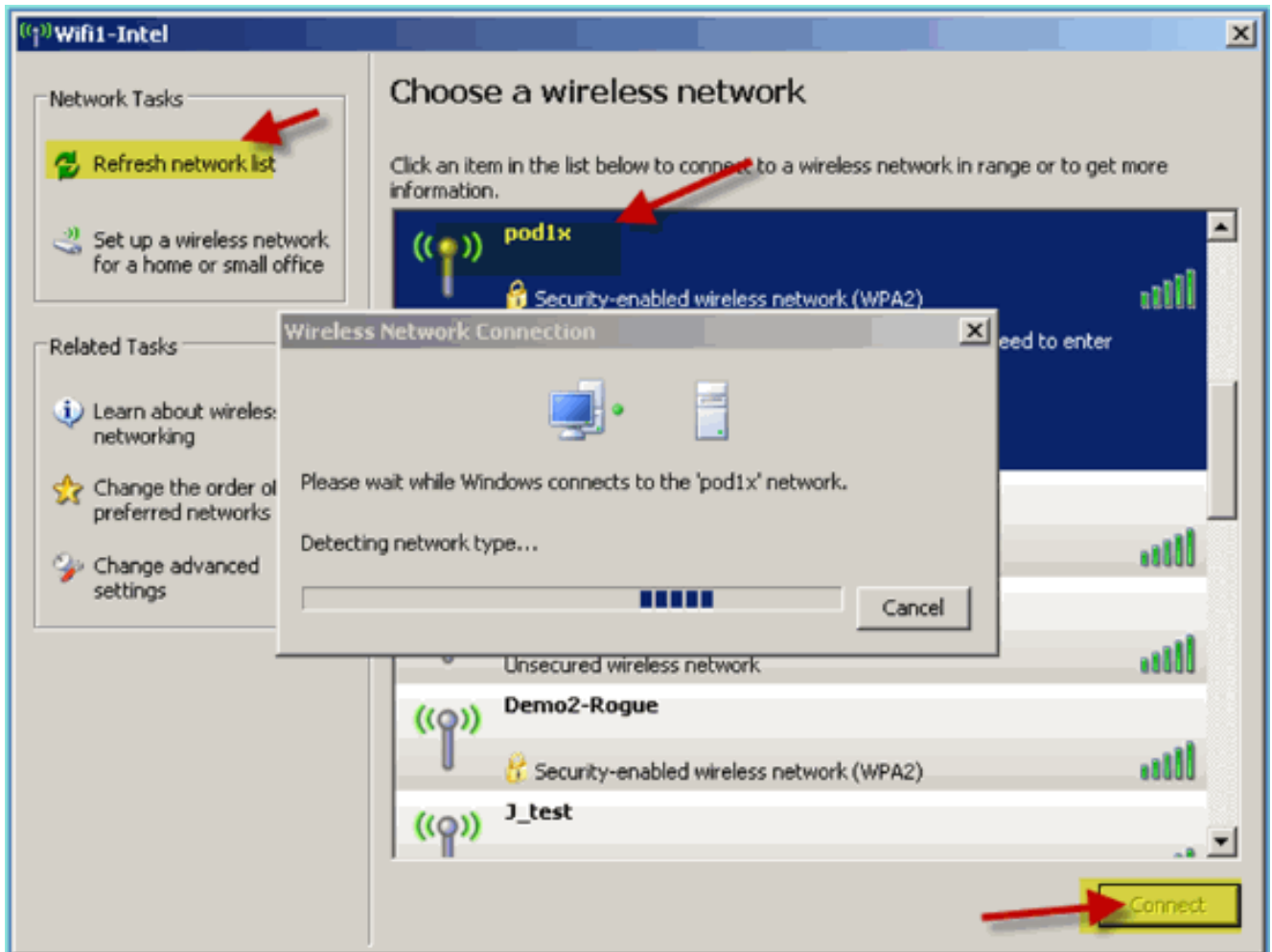


## Referenz: Wireless-Authentifizierung für Microsoft Windows XP

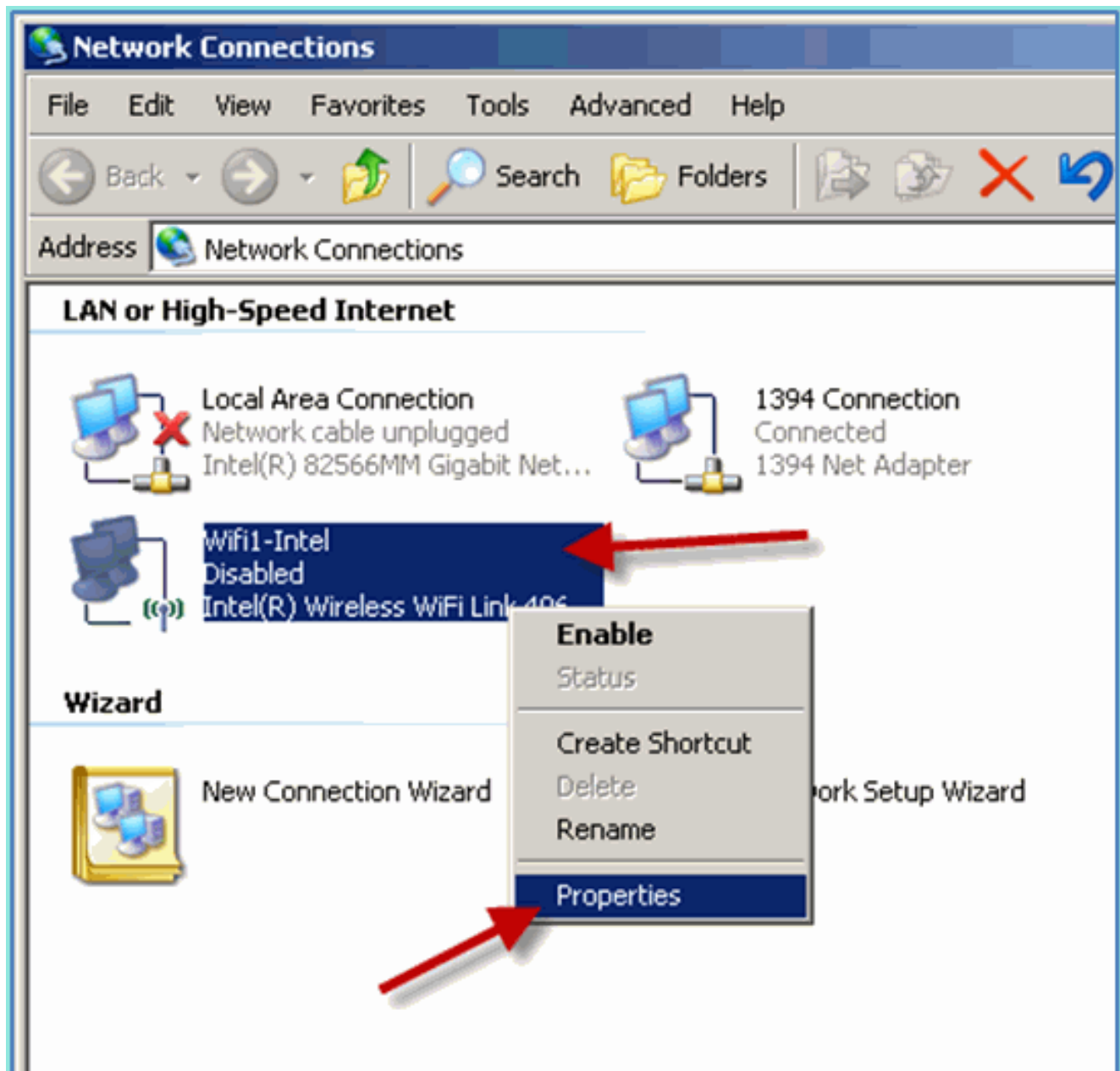
Verknüpfen Sie den WLC über eine authentifizierte SSID als INTERNEN Benutzer (oder integrierten AD-Benutzer) mit einem drahtlosen Windows XP-Laptop. Überspringen, wenn nicht zutreffend.

Führen Sie diese Schritte aus:

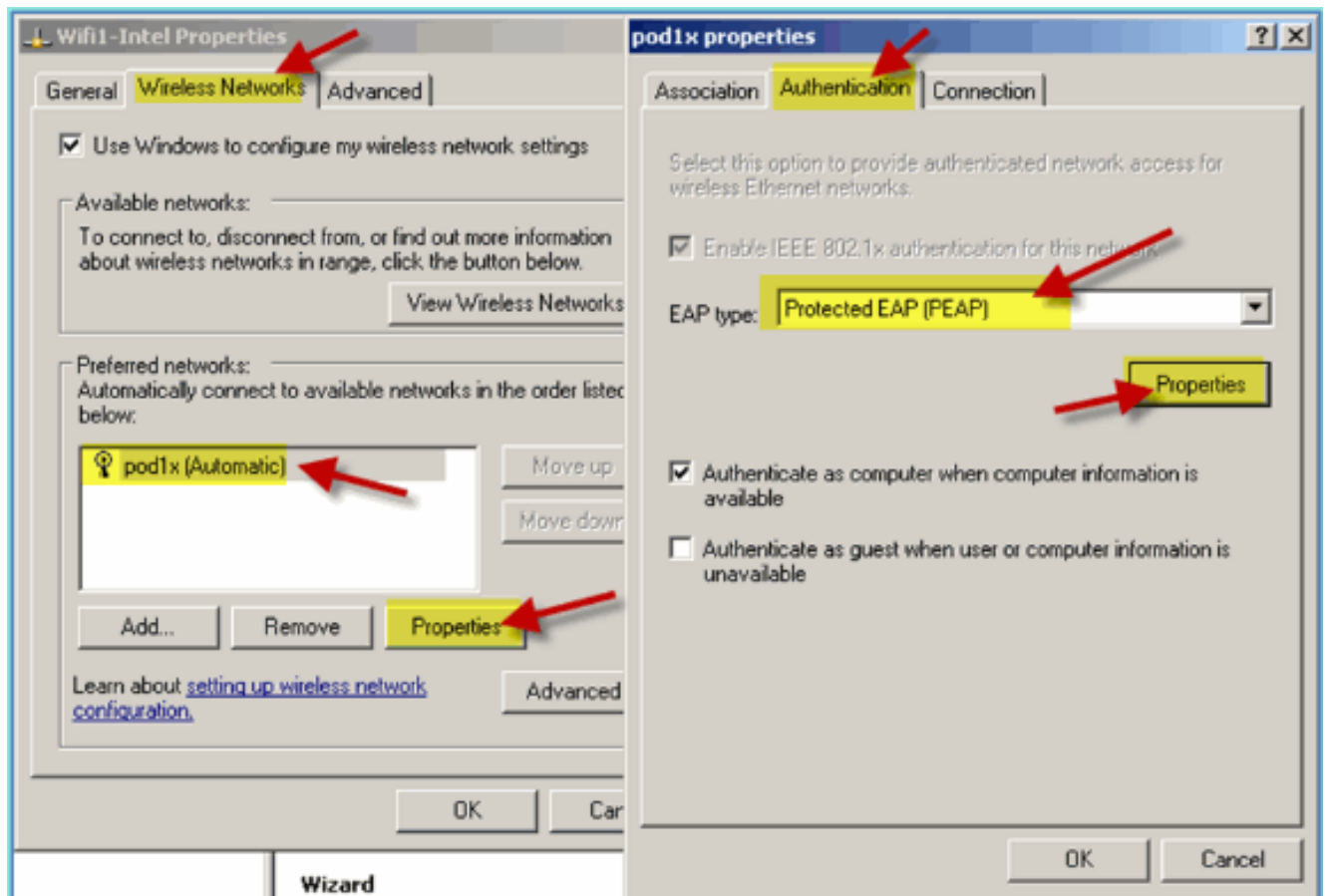
1. Navigieren Sie auf dem Laptop zu den WLAN-Einstellungen. Aktivieren Sie WIFI, und stellen Sie eine Verbindung mit der 802.1X-fähigen POD-SSID her, die in der vorherigen Übung erstellt wurde.



2. Zugriff auf die Netzwerkeigenschaften für die WIFI-Schnittstelle



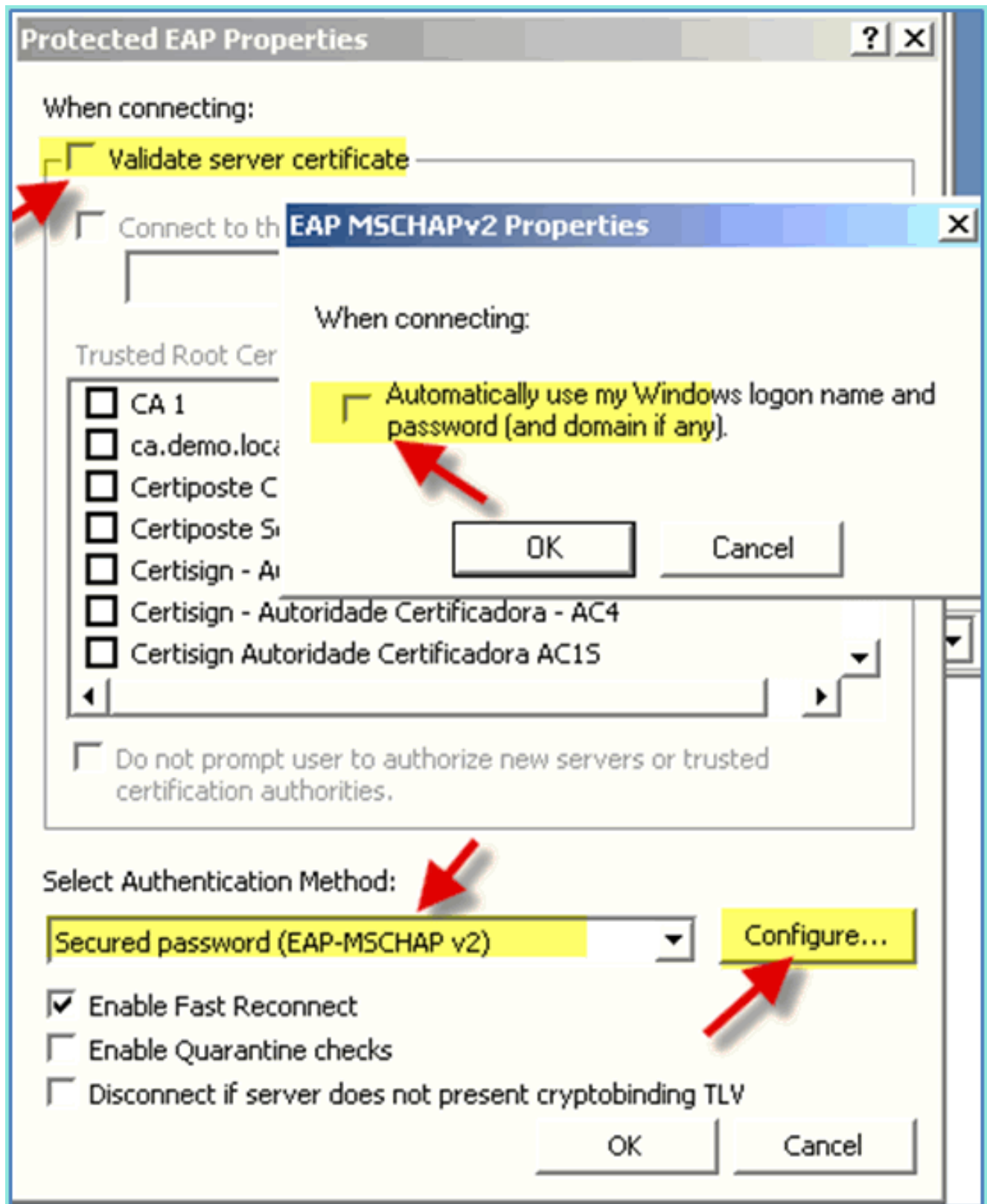
3. Navigieren Sie zur Registerkarte **Wireless Networks (Wireless-Netzwerke)**. Wählen Sie die POD-SSID-Netzwerkeigenschaften > Registerkarte Authentifizierung > EAP-Typ = PEAP (Protected EAP) aus.



4. Klicken Sie auf die EAP-Eigenschaften.

5. Legen Sie Folgendes fest: Serverzertifikat überprüfen: Deaktiviert  
Authentifizierungsmethode: Sicheres Kennwort (EAP-MSCHAP v2)



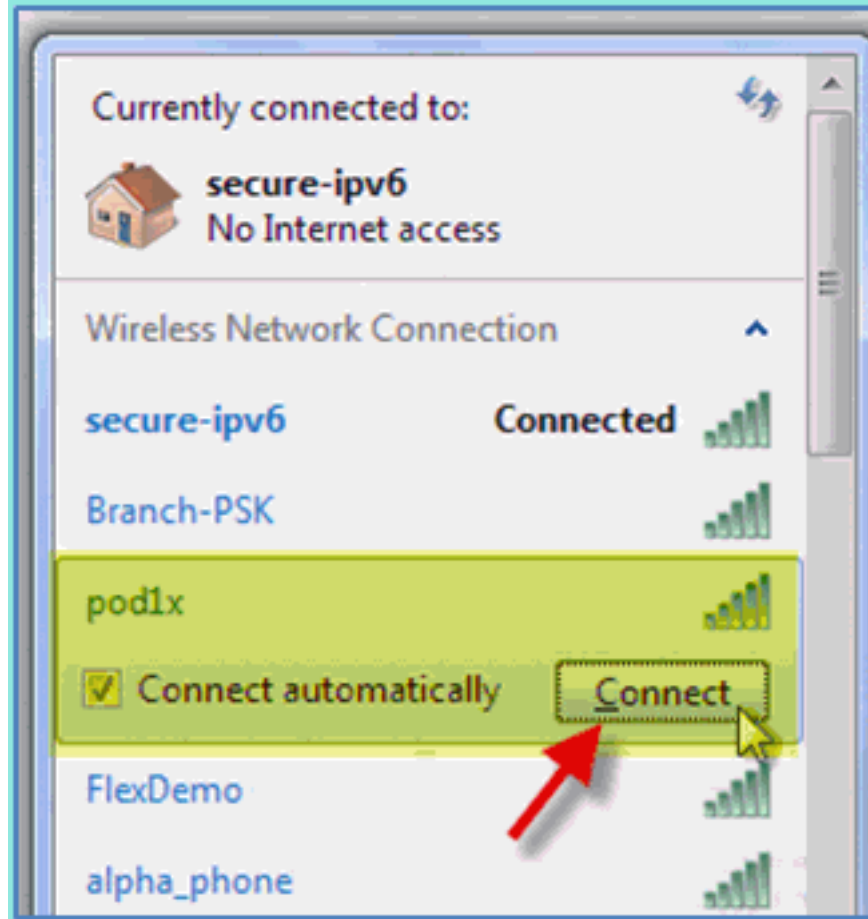


6. Klicken Sie in allen Fenstern auf **OK**, um diesen Konfigurationsvorgang abzuschließen.
7. Der Windows XP-Client fordert Sie zur Eingabe von Benutzername und Kennwort auf. In diesem Beispiel ist dies aduser/XXXX.
8. Netzwerkverbindung und IP-Adressierung bestätigen (v4).

## [Referenz: Wireless-Authentifizierung für Microsoft Windows 7](#)

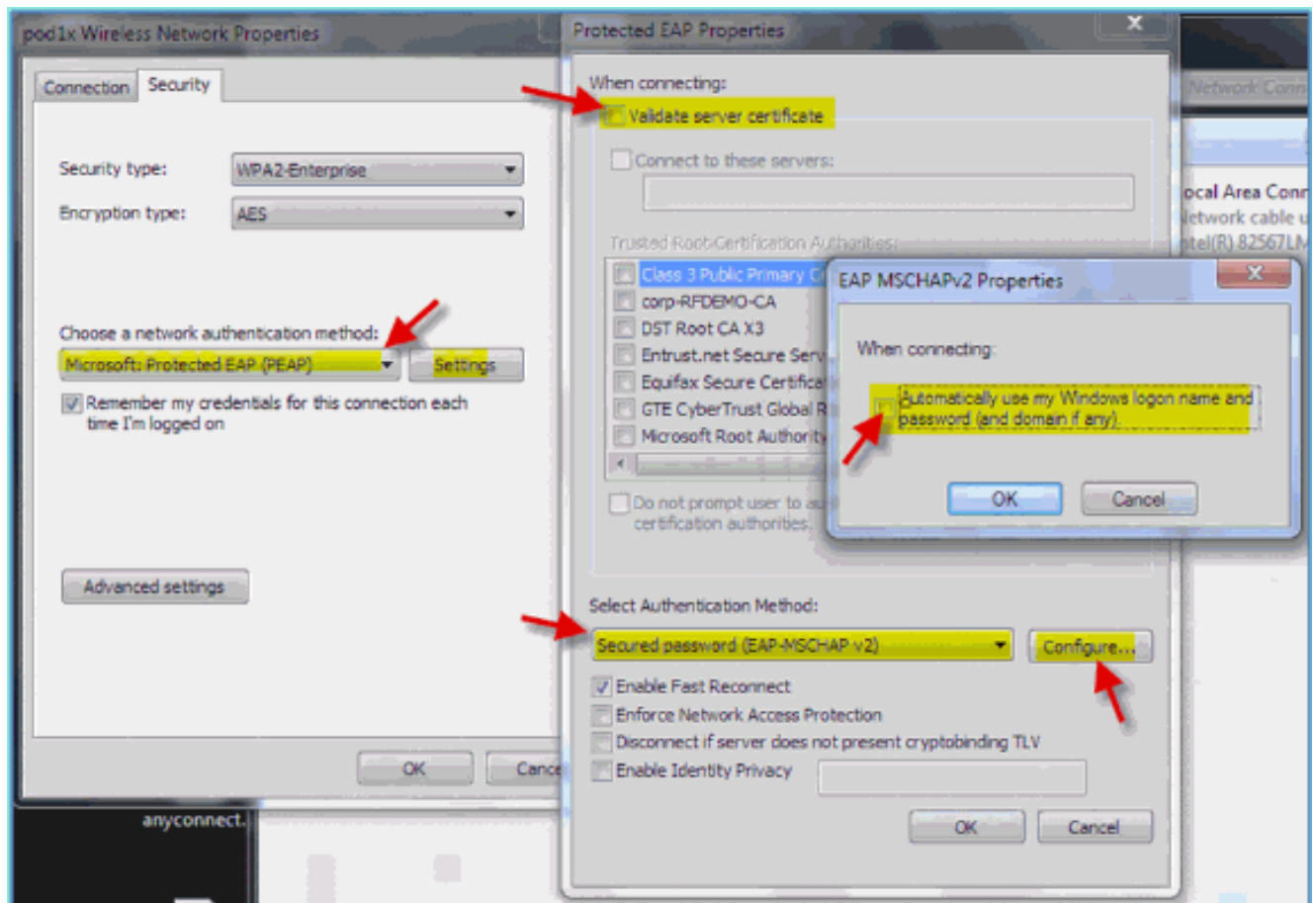
Verknüpfen Sie den WLC über eine authentifizierte SSID als INTERNEN Benutzer (oder integrierten AD-Benutzer) mit einem drahtlosen Windows 7-Laptop.

1. Navigieren Sie auf dem Laptop zu den WLAN-Einstellungen. Aktivieren Sie WIFI, und stellen Sie eine Verbindung mit der 802.1X-fähigen POD-SSID her, die in der vorherigen Übung



erstellt wurde.

2. Öffnen Sie den Wireless Manager, und bearbeiten Sie das neue POD-Wireless-Profil.
3. Legen Sie Folgendes fest: Authentifizierungsmethode: PEAP Anmeldeinformationen speichern...: Deaktiviert Serverzertifikat überprüfen (erweiterte Einstellung): Deaktiviert Authentifizierungsmethode (erweiterte Einstellung): EAP-MSCHAP v2 Windows-Anmeldung automatisch verwenden...: Deaktiviert



## Zugehörige Informationen

- [Technischer Support und Dokumentation für Cisco Systeme](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.