

# Bereitstellungsleitfaden für Wireless BYOD für FlexConnect

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Topologie](#)

[Gerätregistrierung und Komponentenbereitstellung](#)

[Portal zur Registrierung von Ressourcen](#)

[Portal zur Selbstregistrierung](#)

[Authentifizierung und Bereitstellung](#)

[Bereitstellung für iOS \(iPhone/iPad/iPod\)](#)

[Bereitstellung für Android](#)

[Dual-SSID Wireless BYOD-Selbstregistrierung](#)

[Einzelne SSID Wireless BYOD-Selbstregistrierung](#)

[Feature-Konfiguration](#)

[WLAN-Konfiguration](#)

[FlexConnect AP-Konfiguration](#)

[ISE-Konfiguration](#)

[Benutzerfreundlichkeit - Bereitstellung von iOS](#)

[Duale SSID](#)

[Eine SSID](#)

[Benutzererlebnis - Bereitstellung von Android](#)

[Duale SSID](#)

[Geräteportal](#)

[Referenz - Zertifikate](#)

[Zugehörige Informationen](#)

## Einleitung

Mobilgeräte werden immer leistungsfähiger und beliebter bei Verbrauchern. Millionen dieser Geräte werden über Hochgeschwindigkeits-Wi-Fi an Privatanutzer verkauft, damit diese miteinander kommunizieren und zusammenarbeiten können. Die Verbraucher sind inzwischen an die Produktivitätssteigerung gewöhnt, die diese Mobilgeräte mit sich bringen, und möchten ihre persönliche Erfahrung mit in den Arbeitsbereich integrieren. Daraus ergeben sich die Funktionsanforderungen einer BYOD-Lösung (Bring Your Own Device) am Arbeitsplatz.

Dieses Dokument beschreibt die Bereitstellung der BYOD-Lösung in der Zweigstelle. Ein

Mitarbeiter stellt über sein neues iPad eine Verbindung zu einem SSID (Corporate Service Set Identifier) her und wird zu einem Portal zur Selbstregistrierung weitergeleitet. Die Cisco Identity Services Engine (ISE) authentifiziert den Benutzer über das Active Directory (AD) des Unternehmens und lädt ein Zertifikat mit einer eingebetteten iPad-MAC-Adresse und einem Benutzernamen auf das iPad herunter, zusammen mit einem Supplicant-Profil, das die Verwendung des Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) als Methode für die 802.1x-Konnektivität erzwingt. Basierend auf der Autorisierungsrichtlinie der ISE kann der Benutzer dann mithilfe von dot1x eine Verbindung herstellen und auf die entsprechenden Ressourcen zugreifen.

Die ISE-Funktionen in den Softwareversionen der Cisco Wireless LAN Controller-Software vor 7.2.110.0 unterstützten keine lokalen Switching-Clients, die über FlexConnect Access Points (APs) eine Verbindung herstellen. Version 7.2.110.0 unterstützt diese ISE-Funktionen für FlexConnect APs für lokales Switching und zentral authentifizierte Clients. Darüber hinaus bietet die mit ISE 1.1.1 integrierte Version 7.2.110.0 (ist jedoch nicht darauf beschränkt) folgende Funktionen der BYOD-Lösung für Wireless-Netzwerke:

- Erstellung von Geräteprofilen und Status
- Geräteregistrierung und Komponentenbereitstellung
- Integration privater Geräte (Bereitstellung von iOS- oder Android-Geräten)

**Hinweis:** Andere Geräte wie drahtlose PC- oder Mac-Laptops und Workstations werden zwar unterstützt, sind jedoch nicht in diesem Leitfaden enthalten.

## 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 Catalyst Switches
- Cisco Wireless LAN (WLAN) Controller
- Cisco WLAN Controller (WLC) Softwareversion 7.2.110.0 und höher
- 802.11n APs im FlexConnect-Modus
- Cisco ISE Software Version 1.1.1 und höher
- Windows 2008 AD mit Zertifizierungsstelle
- DHCP-Server
- DNS-Server (Domain Name System)
- Network Time Protocol (NTP)
- Wireless-Client: Laptop, Smartphone und Tablet (Apple iOS, Android, Windows und Mac)

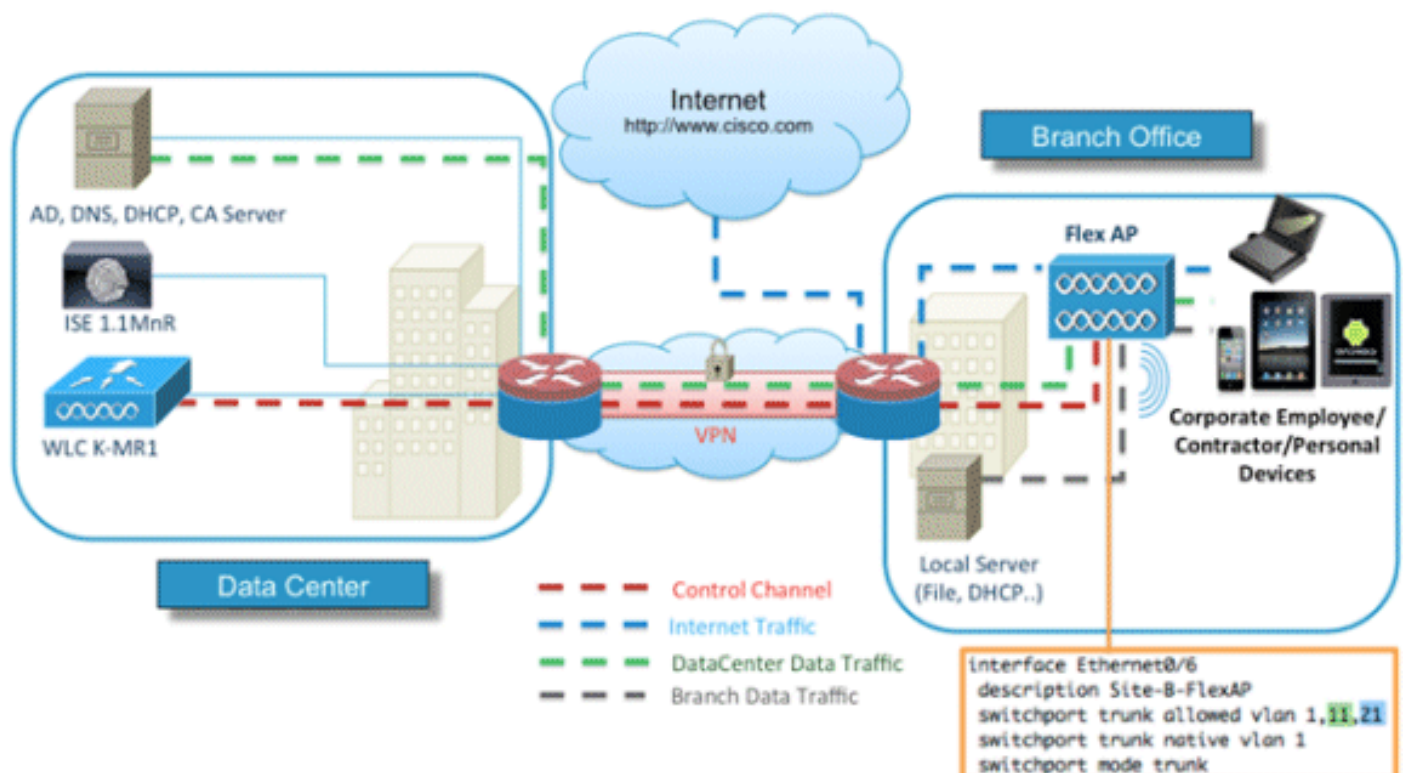
**Hinweis:** Wichtige Informationen zu dieser Softwareversion finden Sie in den

[Versionshinweisen für Cisco Wireless LAN-Controller und Lightweight Access Points für Version 7.2.110.0](#). Melden Sie sich bei der Website Cisco.com an, um die neuesten Versionshinweise zu erhalten, bevor Sie Software laden und testen.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

## Topologie

Um diese Funktionen ordnungsgemäß zu implementieren und zu testen, ist eine minimale Netzwerkeinrichtung erforderlich, wie in diesem Diagramm gezeigt:



Für diese Simulation benötigen Sie ein Netzwerk mit einem FlexConnect AP, einem lokalen/entfernten Standort mit lokalem DHCP, DNS, dem WLC und der ISE. Der FlexConnect-AP ist mit einem Trunk verbunden, um das lokale Switching mit mehreren VLANs zu testen.

## Geräteregistrierung und Komponentenbereitstellung

Ein Gerät muss registriert werden, damit seine native Komponente für die 802.1x-Authentifizierung bereitgestellt werden kann. Basierend auf der richtigen Authentifizierungsrichtlinie wird der Benutzer auf die Gastseite umgeleitet und durch die Anmeldeinformationen des Mitarbeiters authentifiziert. Der Benutzer sieht die Seite zur Geräteregistrierung, auf der er nach seinen Geräteinformationen fragt. Anschließend wird mit der Gerätebereitstellung begonnen. Wenn das Betriebssystem für die Bereitstellung nicht unterstützt wird, wird der Benutzer zum Portal für die Bestandsregistrierung weitergeleitet, um das Gerät für den MAB-Zugriff (MAC Authentication Bypass) zu markieren. Wenn das Betriebssystem unterstützt wird, beginnt der

Registrierungsprozess und konfiguriert die native Komponente des Geräts für die 802.1x-Authentifizierung.

## Portal zur Registrierung von Ressourcen

Das Portal zur Bestandsregistrierung ist Teil der ISE-Plattform, über die Mitarbeiter die Einbindung von Endgeräten über einen Authentifizierungs- und Registrierungsprozess initiieren können.

Administratoren können Ressourcen von der Seite mit den Endgerätidentitäten löschen. Jeder Mitarbeiter kann die von ihm registrierten Ressourcen bearbeiten, löschen und auf eine Blacklist setzen. Endgeräte, die auf einer Blacklist stehen, werden einer Identitätsgruppe auf einer Blacklist zugewiesen, und es wird eine Autorisierungsrichtlinie erstellt, um den Netzwerkzugriff durch Endgeräte auf einer Blacklist zu verhindern.

## Portal zur Selbstregistrierung

Im CWA-Prozess (Central Web Authentication) werden Mitarbeiter zu einem Portal umgeleitet, in dem sie ihre Anmeldeinformationen eingeben, sich authentifizieren und die Details der Ressource eingeben können, die sie registrieren möchten. Dieses Portal wird als Self-Provisioning Portal bezeichnet und ähnelt dem Device Registration Portal. Es ermöglicht den Mitarbeitern, die MAC-Adresse sowie eine sinnvolle Beschreibung des Endpunkts einzugeben.

## Authentifizierung und Bereitstellung

Wenn Mitarbeiter das Portal zur Selbstregistrierung auswählen, müssen sie eine Reihe gültiger Mitarbeiteranmeldeinformationen angeben, um mit der Bereitstellungsphase fortzufahren. Nach erfolgreicher Authentifizierung kann der Endpunkt in der Endpunktdatenbank bereitgestellt werden, und für den Endpunkt wird ein Zertifikat generiert. Über einen Link auf der Seite kann der Mitarbeiter den Supplicant Pilot Wizard (SPW) herunterladen.

**Hinweis:** Die neueste FlexConnect-Funktionsmatrix für BYOD finden Sie im Cisco Artikel zur [FlexConnect-Funktionsmatrix](#).

## Bereitstellung für iOS (iPhone/iPad/iPod)

Für die EAP-TLS-Konfiguration folgt die ISE dem Apple Over-the-Air (OTA)-Registrierungsprozess:

- Nach erfolgreicher Authentifizierung evaluiert die Evaluierungs-Engine die Richtlinien für die Client-Bereitstellung, wodurch ein Komponentenprofil erstellt wird.
- Wenn das Supplicant-Profil für die EAP-TLS-Einstellung verwendet wird, bestimmt der OTA-Prozess, ob die ISE selbstsignierte oder von einer unbekanntenen Zertifizierungsstelle signierte Zertifikate verwendet. Wenn eine der Bedingungen zutrifft, wird der Benutzer aufgefordert, das Zertifikat der ISE oder CA herunterzuladen, bevor der Registrierungsprozess beginnen

kann.

- Bei anderen EAP-Methoden sendet die ISE bei erfolgreicher Authentifizierung das endgültige Profil weiter.

## Bereitstellung für Android

Aus Sicherheitsgründen muss der Android-Agent von der Android Marketplace-Website heruntergeladen werden und kann nicht über die ISE bereitgestellt werden. Cisco lädt eine Version des Assistenten für Veröffentlichungskandidaten über das Cisco Android Marketplace Publisher-Konto in den Android Marketplace hoch.

Dies ist der Android-Bereitstellungsprozess:

1. Cisco verwendet das Software Development Kit (SDK), um das Android-Paket mit der Erweiterung .apk zu erstellen.
2. Cisco lädt ein Paket in den Android Marketplace hoch.
3. Der Benutzer konfiguriert die Richtlinie bei der Client-Bereitstellung mit den entsprechenden Parametern.
4. Nach der Registrierung des Geräts wird der Endbenutzer an den Client-Bereitstellungsdienst weitergeleitet, wenn die 802.1x-Authentifizierung fehlschlägt.
5. Die Seite des Bereitstellungsportals enthält eine Schaltfläche, über die Benutzer zum Android Marketplace-Portal weitergeleitet werden, wo sie den SPW herunterladen können.
6. Der Cisco SPW wird gestartet und übernimmt die Bereitstellung der Komponente: SPW erkennt die ISE und lädt das Profil von der ISE herunter.SPW erstellt ein Zertifikat-/Schlüsselpaar für EAP-TLS.SPW führt einen SCEP-Proxy-Anforderungsaufruf (Simple Certificate Enrollment Protocol) an die ISE durch und empfängt das Zertifikat.SPW wendet die Wireless-Profile an.SPW löst eine erneute Authentifizierung aus, wenn die Profile erfolgreich angewendet werden.SPW wird beendet.

## Dual-SSID Wireless BYOD-Selbstregistrierung

Dies ist der Prozess für die Selbstregistrierung von zwei SSID-Wireless-BYOD-Geräten:

1. Der Benutzer wird der Gast-SSID zugewiesen.
2. Der Benutzer öffnet einen Browser und wird zum ISE CWA-Gastportal weitergeleitet.
3. Der Benutzer gibt einen Benutzernamen und ein Kennwort für den Mitarbeiter in das Gastportal ein.
4. Die ISE authentifiziert den Benutzer und leitet ihn, basierend auf der Tatsache, dass es sich um einen Mitarbeiter und nicht um einen Gast handelt, auf die Gastseite für die Mitarbeiterregistrierung um.
5. Die MAC-Adresse wird für die Geräte-ID auf der Gastseite für die Geräteregistrierung eingetragen. Der Benutzer gibt eine Beschreibung ein und akzeptiert ggf. die Richtlinie für akzeptable Nutzung.
6. Der Benutzer wählt "**Akzeptieren**" und beginnt mit dem Herunterladen und der Installation des SPW.
7. Die Komponente für das Gerät dieses Benutzers wird zusammen mit allen Zertifikaten bereitgestellt.

8. CoA tritt auf, und das Gerät ordnet es dem Unternehmens-SSID (CORP) zu und authentifiziert sich mit EAP-TLS (oder einer anderen für diesen Supplicant verwendeten Autorisierungsmethode).

## Einzelne SSID Wireless BYOD-Selbstregistrierung

In diesem Szenario gibt es eine einzige SSID für den Unternehmenszugriff (CORP), die sowohl PEAP (Protected Extensible Authentication Protocol) als auch EAP-TLS unterstützt. Es ist keine Gast-SSID vorhanden.

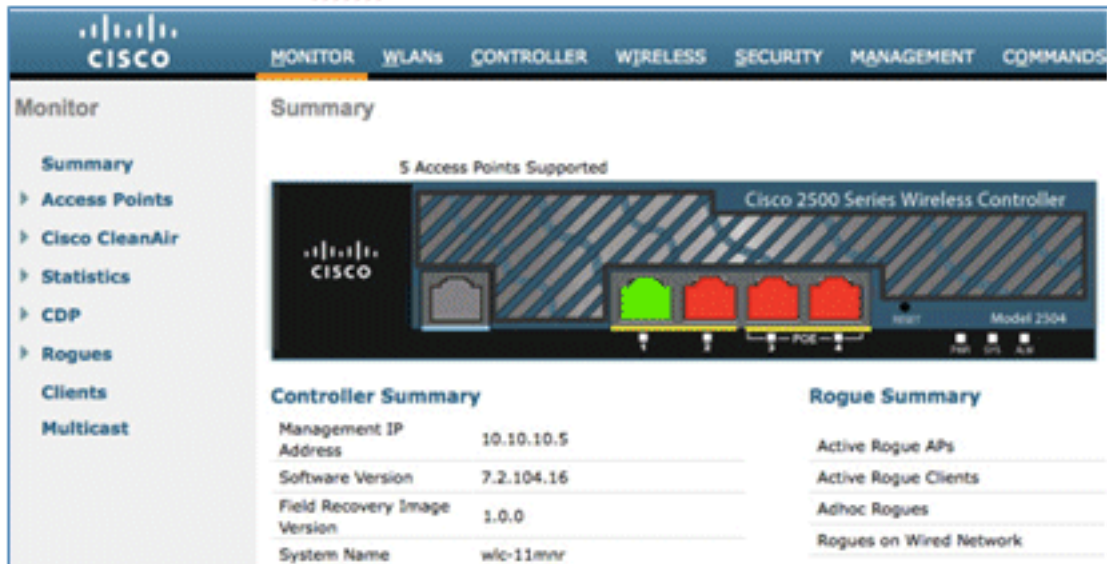
Dies ist der Prozess für die Selbstregistrierung eines einzelnen SSID Wireless-BYOD-Geräts:

1. Der Benutzer ist CORP zugeordnet.
2. Der Benutzer gibt einen Benutzernamen und ein Kennwort für den Mitarbeiter in die Komponente für die PEAP-Authentifizierung ein.
3. Die ISE authentifiziert den Benutzer und stellt, basierend auf der PEAP-Methode, eine Autorisierungsrichtlinie zum Akzeptieren und Umleiten auf die Gastseite "Employee Device Registration" bereit.
4. Der Benutzer öffnet einen Browser und wird auf die Gastseite Employee Device Registration (Registrierung von Mitarbeitergeräten) weitergeleitet.
5. Die MAC-Adresse wird für die Geräte-ID auf der Gastseite für die Geräteregistrierung eingetragen. Der Benutzer gibt eine Beschreibung ein und akzeptiert die Nutzungsrichtlinien.
6. Der Benutzer wählt "**Akzeptieren**" und beginnt mit dem Herunterladen und der Installation des SPW.
7. Die Komponente für das Gerät dieses Benutzers wird zusammen mit allen Zertifikaten bereitgestellt.
8. CoA tritt auf, und das Gerät weist die CORP-SSID erneut zu und authentifiziert sich mit EAP-TLS.

## Feature-Konfiguration

Gehen Sie wie folgt vor, um mit der Konfiguration zu beginnen:

1. Achten Sie bei diesem Leitfaden darauf, dass die WLC-Version 7.2.110.0 oder höher ist.



2. Navigieren Sie zu **Security > RADIUS > Authentication**, und fügen Sie den RADIUS-Server dem WLC hinzu.



3. Fügen Sie die ISE 1.1.1 zum WLC hinzu:

Geben Sie einen freigegebenen Schlüssel ein. Legen Sie die Unterstützung für RFC 3576 auf **Aktiviert fest**.

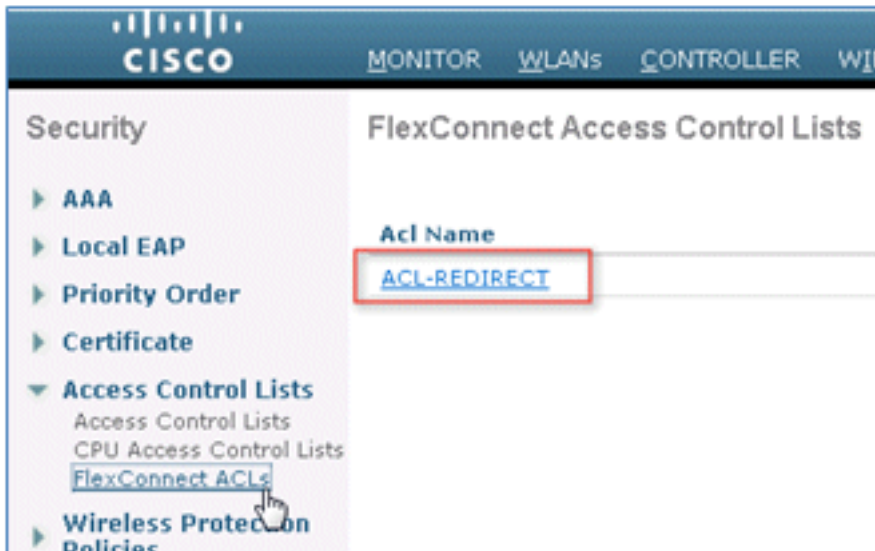
MONITOR		WLANs		CONTROLLER		WIRELESS		SECURITY		MANAGEMENT		COMMANDS		HELP		FEEDBACK	
<b>RADIUS Authentication Servers &gt; Edit</b>																	
Server Index	1																
Server Address	10.10.10.60																
Shared Secret Format	ASCII																
Shared Secret	***																
Confirm Shared Secret	***																
Key Wrap	<input type="checkbox"/> (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	<input checked="" type="checkbox"/> Enable																
Management	<input checked="" type="checkbox"/> Enable																
IPSec	<input type="checkbox"/> Enable																

4. Fügen Sie denselben ISE-Server wie einen RADIUS-Accounting-Server hinzu.

MONITOR		WLANs		CONTROLLER		WIRELESS		SECURITY		MANAGEMENT		COMMANDS		HELP		FEEDBACK	
<b>RADIUS Accounting Servers &gt; Edit</b>																	
Server Index	1																
Server Address	10.10.10.60																
Shared Secret Format	ASCII																
Shared Secret	***																
Confirm Shared Secret	***																
Port Number	1813																
Server Status	Enabled																
Server Timeout	2 seconds																
Network User	<input checked="" type="checkbox"/> Enable																
IPSec	<input type="checkbox"/> Enable																

5. Erstellen Sie eine WLC-Pre-Auth-ACL, die Sie später in der ISE-Richtlinie verwenden können. Navigieren Sie zu WLC > **Security** > **Access Control Lists** > **FlexConnect ACLs**, und erstellen Sie eine neue FlexConnect ACL mit dem Namen **ACL-REDIRECT** (in diesem Beispiel).





6. In den ACL-Regeln muss der gesamte Datenverkehr von und zu der ISE sowie der Client-Datenverkehr während der Komponentenbereitstellung zugelassen werden.

Für die erste Regel (Sequenz 1):

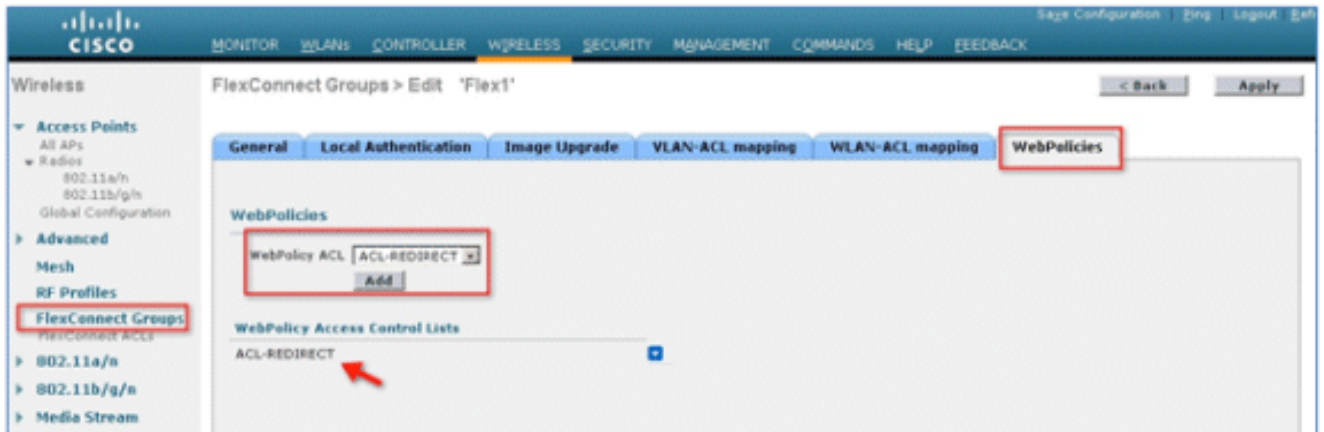
Legen Sie "Quelle" auf "**Beliebig**" fest. Legen Sie IP (ISE-Adresse)/Netmask **255.255.255.255** fest. Aktion auf **Zulassen** festlegen.

Legen Sie für die zweite Regel (Sequenz 2) die Quell-IP-Adresse (ISE-Adresse)/-Maske 255.255.255.255 auf **Any (Beliebig)** und die Aktion auf **Permit (Zulassen)** fest.

General							
Access List Name		ACL-REDIRECT					
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Permit	0.0.0.0 0.0.0.0	/ 10.10.10.60 255.255.255.255	/ Any	Any	Any	Any <input checked="" type="checkbox"/>
2	Permit	10.10.10.60 255.255.255.255	/ 0.0.0.0 0.0.0.0	/ Any	Any	Any	Any <input checked="" type="checkbox"/>

7. Erstellen Sie eine neue FlexConnect-Gruppe mit dem Namen Flex1 (in diesem Beispiel):

Navigieren Sie zur Registerkarte **FlexConnect Group > WebPolicies**. Klicken Sie im Feld WebPolicy ACL (WebPolicy-ACL) auf **Add (Hinzufügen)**, und wählen Sie **ACL-REDIRECT** oder die zuvor erstellte FlexConnect-ACL aus. Bestätigen Sie, dass das Feld **WebPolicy Access Control Lists** ausgefüllt wird.



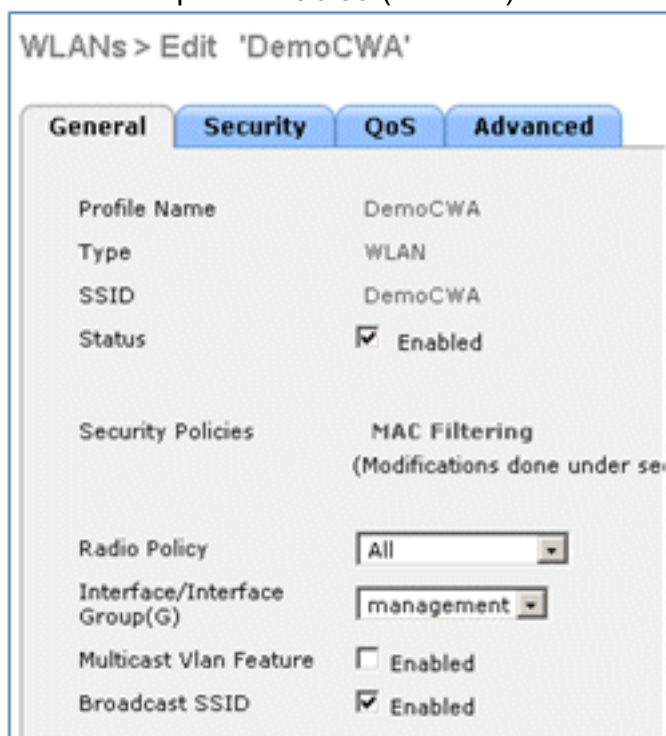
8. Klicken Sie auf **Apply** und **Save Configuration**.

## WLAN-Konfiguration

Gehen Sie wie folgt vor, um das WLAN zu konfigurieren:

1. Erstellen Sie eine offene WLAN-SSID für das Beispiel mit zwei SSIDs:

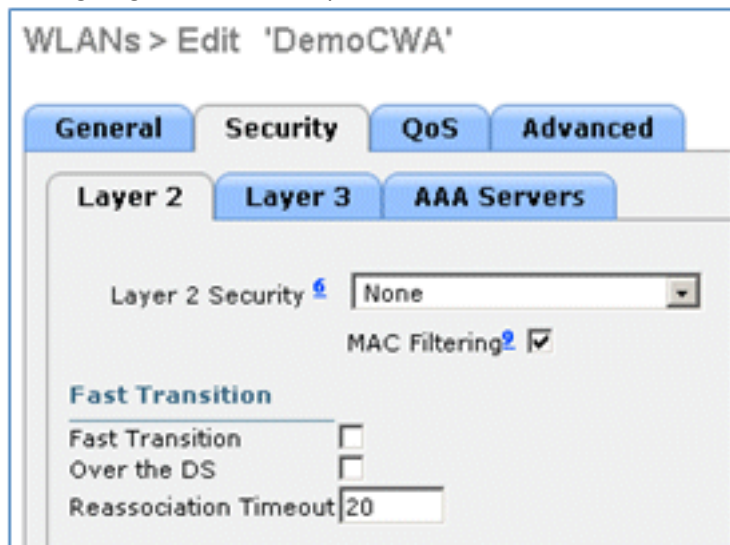
Geben Sie einen WLAN-Namen ein: **DemoCWA** (in diesem Beispiel). Wählen Sie unter Status die Option **Enabled** (Aktiviert) aus.



2. Navigieren Sie zur Registerkarte **Security (Sicherheit) > Layer 2** (Registerkarte **Layer 2**), und

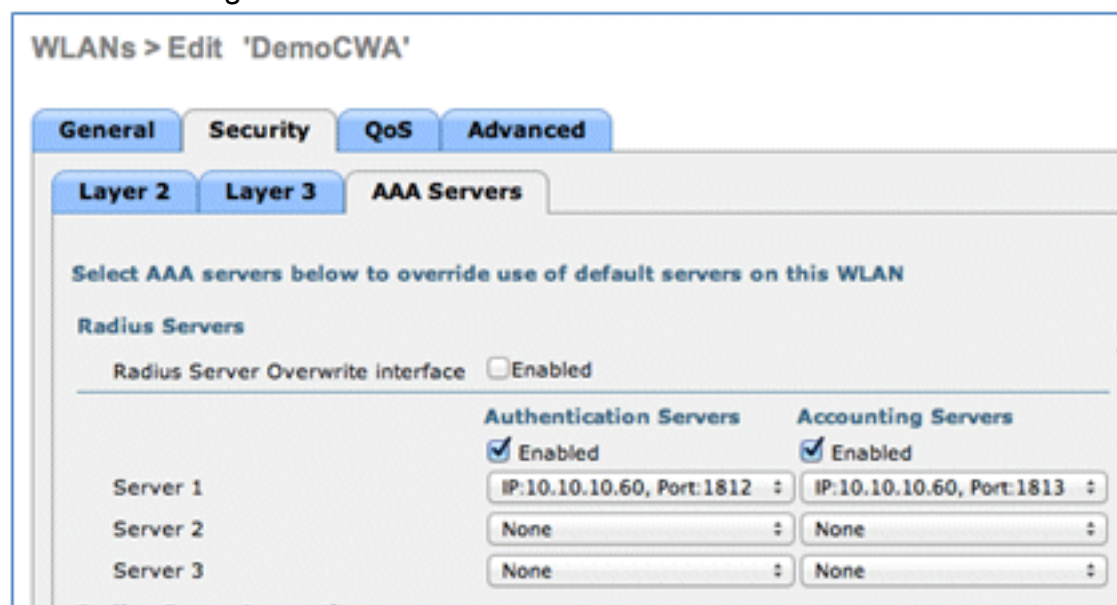
legen Sie folgende Attribute fest:

Layer-2-Sicherheit: **Keine**MAC-Filterung: **Aktiviert** (Kontrollkästchen ist aktiviert)Schneller Übergang: **Deaktiviert** (Kontrollkästchen ist nicht aktiviert)

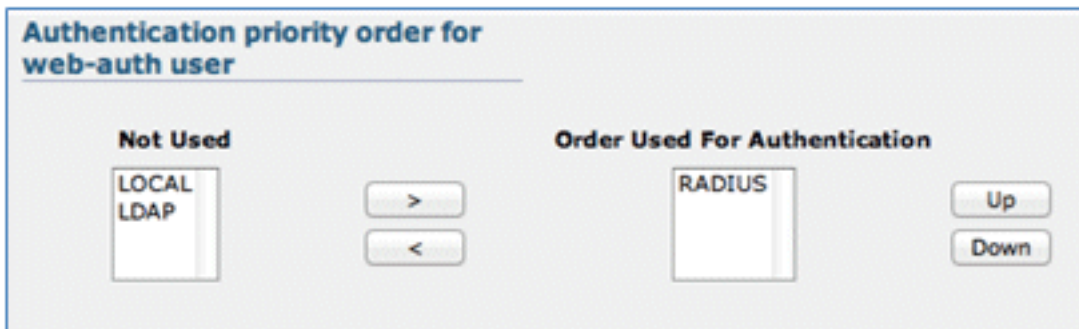


3. Wechseln Sie zur Registerkarte **AAA-Server**, und legen Sie folgende Attribute fest:

Authentifizierungs- und Kontoserver: **aktiviert**Server 1: *<ISE-IP-Adresse>*

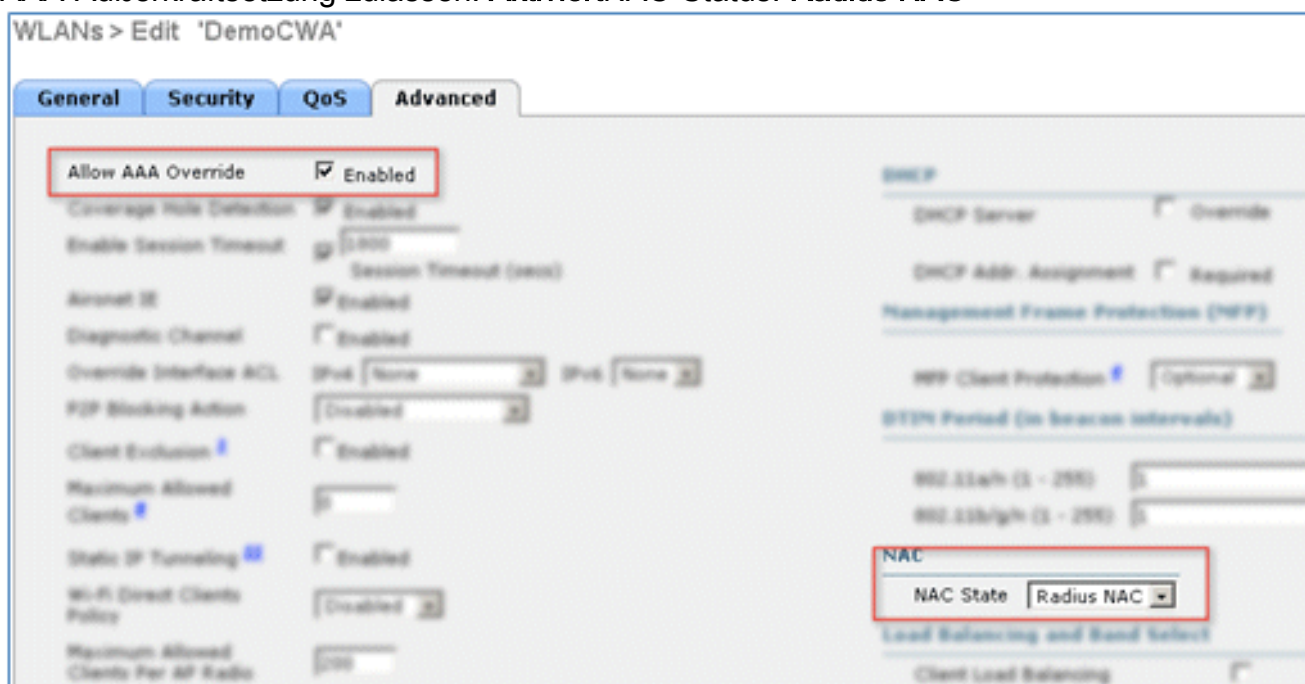


4. Blättern Sie von der Registerkarte **AAA-Server** nach unten. Vergewissern Sie sich unter "Authentication priority order for web-auth user", dass **RADIUS** für die Authentifizierung verwendet wird und die anderen nicht.



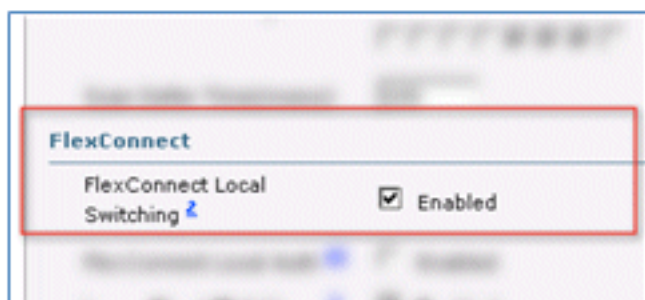
5. Wechseln Sie zur Registerkarte **Erweitert**, und legen Sie folgende Attribute fest:

AAA-Außerkräftsetzung zulassen: **Aktiviert** NAC-Status: **Radius NAC**

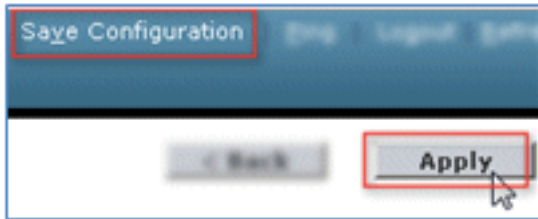


**Hinweis:** RADIUS Network Admission Control (NAC) wird nicht unterstützt, wenn sich der FlexConnect AP im getrennten Modus befindet. Befindet sich der FlexConnect-Access Point also im Standalone-Modus und wird die Verbindung zum WLC unterbrochen, werden alle Clients getrennt, und die SSID wird nicht mehr gemeldet.

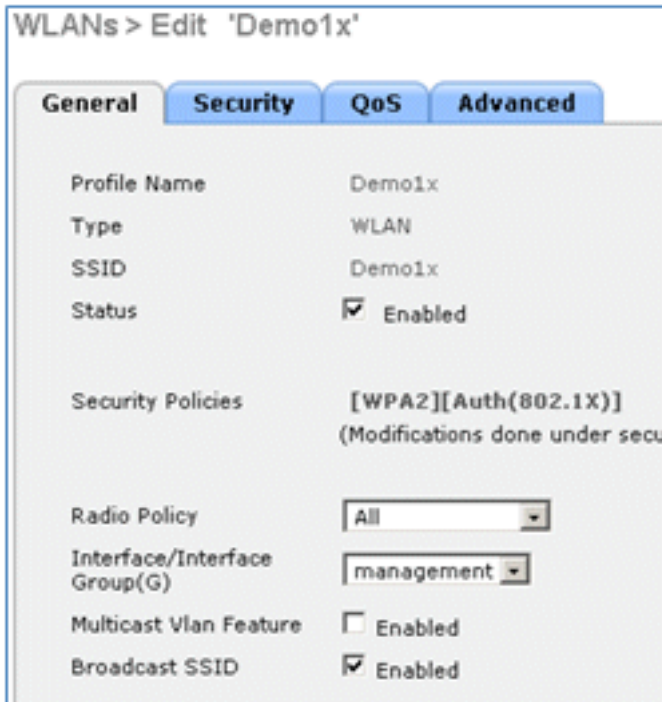
6. Blättern Sie auf der Registerkarte **Erweitert** nach unten, und setzen Sie FlexConnect Local Switching auf **Aktiviert**.



7. Klicken Sie auf **Apply** and **Save Configuration**.



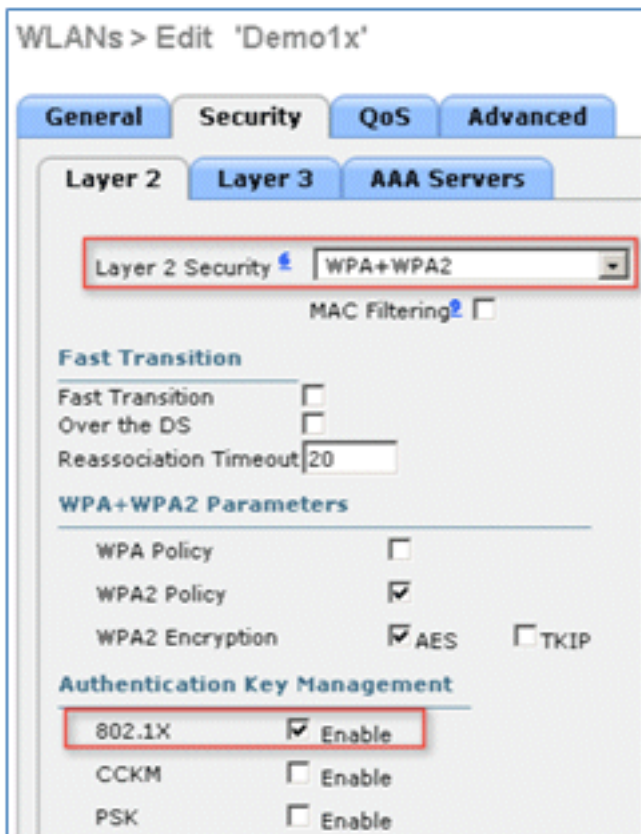
8. Erstellen Sie eine 802.1X-WLAN-SSID mit dem Namen **Demo1x** (in diesem Beispiel) für Einzel- und Dual-SSID-Szenarien.



9. Navigieren Sie zur Registerkarte **Security (Sicherheit)** > **Layer 2** (Registerkarte **Layer 2**), und legen Sie folgende Attribute fest:

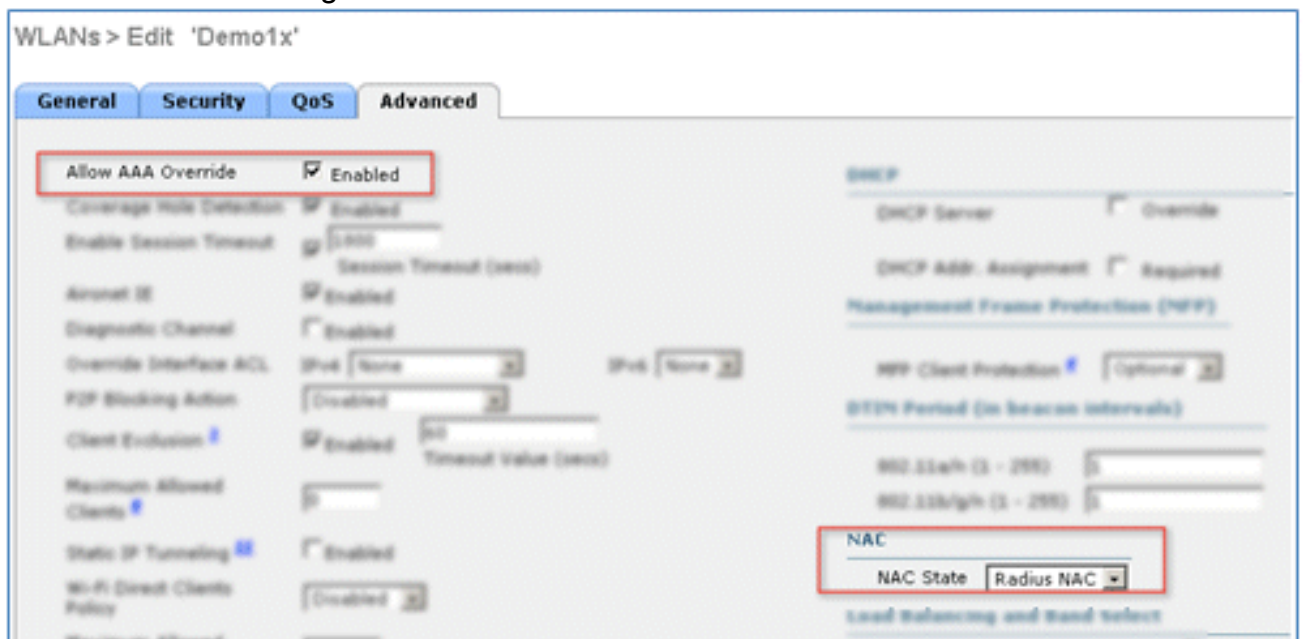
Layer-2-Sicherheit: **WPA+WPA2**Schneller Übergang: **Deaktiviert** (Kontrollkästchen ist nicht aktiviert) Verwaltung von Authentifizierungsschlüsseln: 802.IX: **Aktivieren**



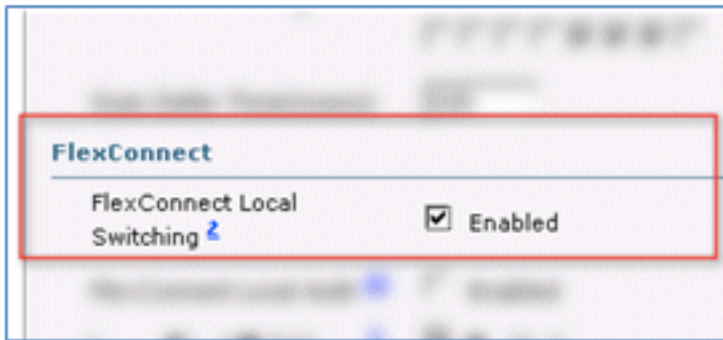


10. Wechseln Sie zur Registerkarte **Erweitert**, und legen Sie folgende Attribute fest:

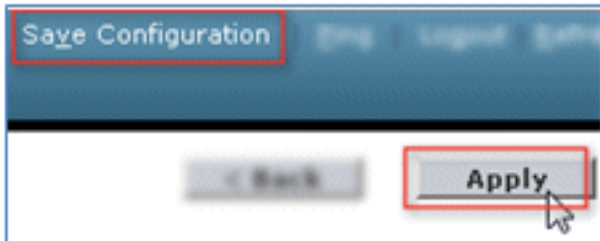
AAA-Außerkraftsetzung zulassen: **Aktiviert** NAC-Status: **Radius NAC**



11. Blättern Sie auf der Registerkarte **Advanced (Erweitert)** nach unten, und setzen Sie FlexConnect Local Switching auf **Enabled (Aktiviert)**.



12. Klicken Sie auf **Apply** and **Save Configuration**.



13. Vergewissern Sie sich, dass beide neuen WLANs erstellt wurden.

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

WLANs Entries 1 - 5 of 5

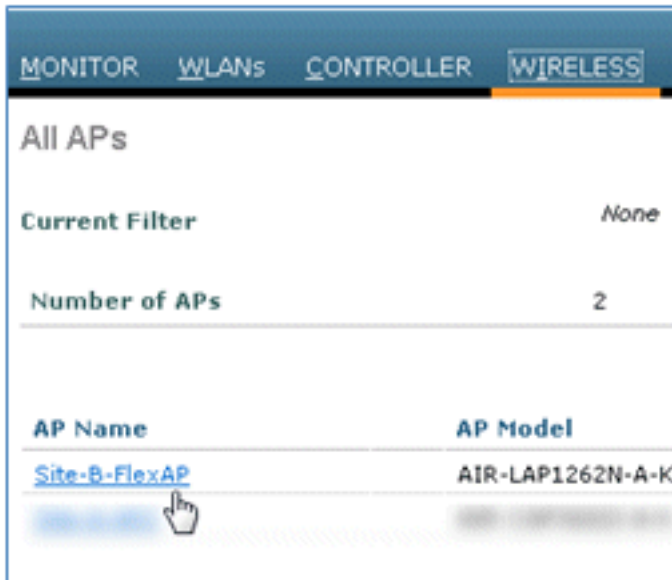
Current Filter: None [\[Change Filter\]](#) [\[Clear Filter\]](#) Create New

<input type="checkbox"/>	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
<input type="checkbox"/>	1	WLAN	802x	802x	Disabled	[WPA2][Auth(802.1X)]
<input type="checkbox"/>	2	WLAN	8	8	Enabled	[WPA2][Auth(PSK)]
<input type="checkbox"/>	3	WLAN	Demo1x	Demo1x	Enabled	[WPA2][Auth(802.1X)]
<input type="checkbox"/>	4	WLAN	DemoCWA	DemoCWA	Enabled	MAC Filtering
<input type="checkbox"/>	5	WLAN	802	802	Disabled	Web-Auth

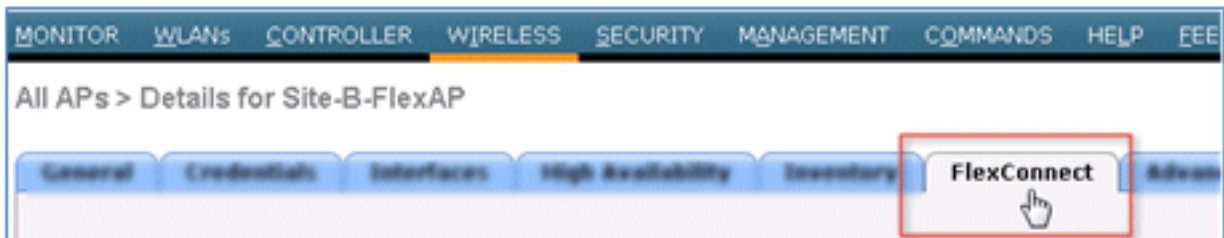
## FlexConnect AP-Konfiguration

Führen Sie die folgenden Schritte aus, um den FlexConnect AP zu konfigurieren:

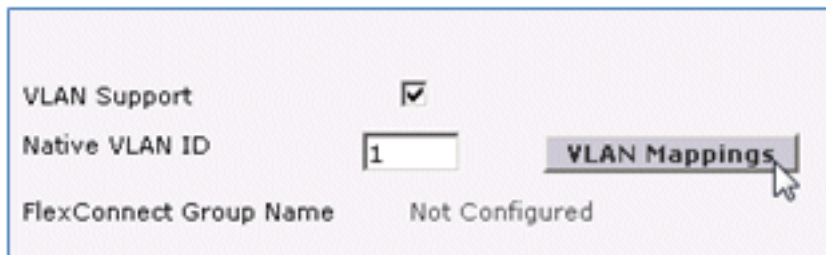
1. Navigieren Sie zu **WLC > Wireless**, und klicken Sie auf den Ziel-FlexConnect-AP.



2. Klicken Sie auf die Registerkarte **FlexConnect**.



3. Aktivieren Sie VLAN Support (Kontrollkästchen ist aktiviert), legen Sie die Native VLAN ID fest, und klicken Sie auf **VLAN Mappings**.



4. Legen Sie die VLAN-ID für die SSID für das lokale Switching auf **21** (in diesem Beispiel) fest.



MONITOR			WLANs			CONTROLLER			WIRELESS			SECURITY			M...		
All APs > Site-B-FlexAP > VLAN Mappings																	
AP Name						Site-B-FlexAP											
Base Radio MAC						e8:04:62:0a:68:80											
WLAN Id		SSID		VLAN ID													
3		Demo1x		21													
4		DemoCWA		21													

5. Klicken Sie auf **Apply** and **Save Configuration**.

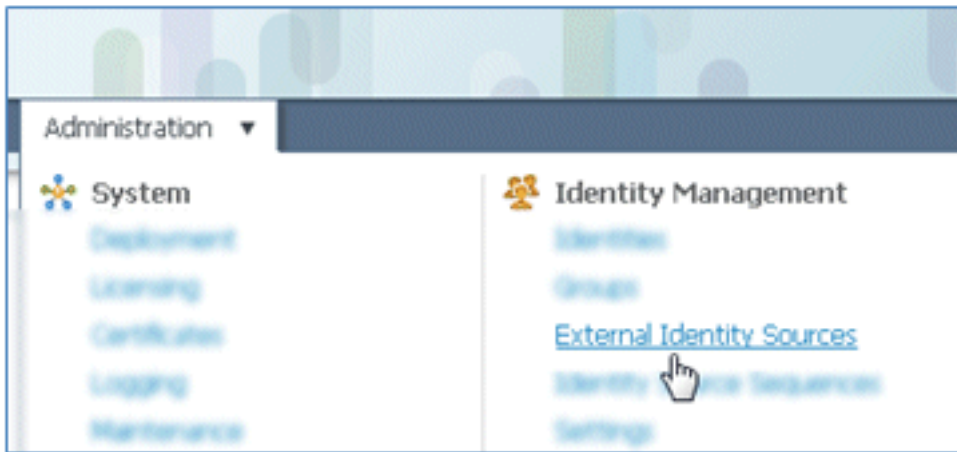
## ISE-Konfiguration

Gehen Sie wie folgt vor, um die ISE zu konfigurieren:

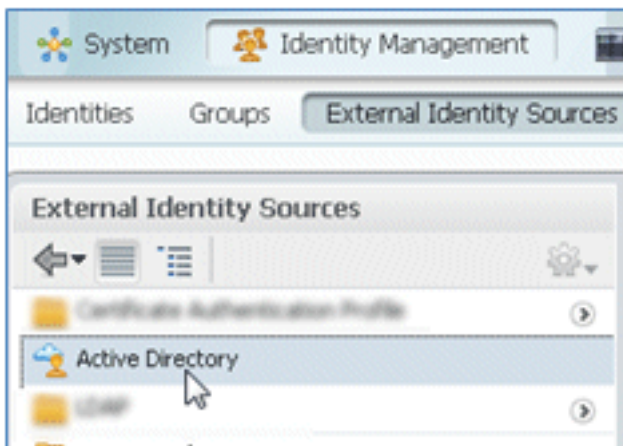
1. Melden Sie sich beim ISE-Server an: *<https://ise>*.



2. Navigieren Sie zu **Administration > Identity Management > External Identity Sources**.

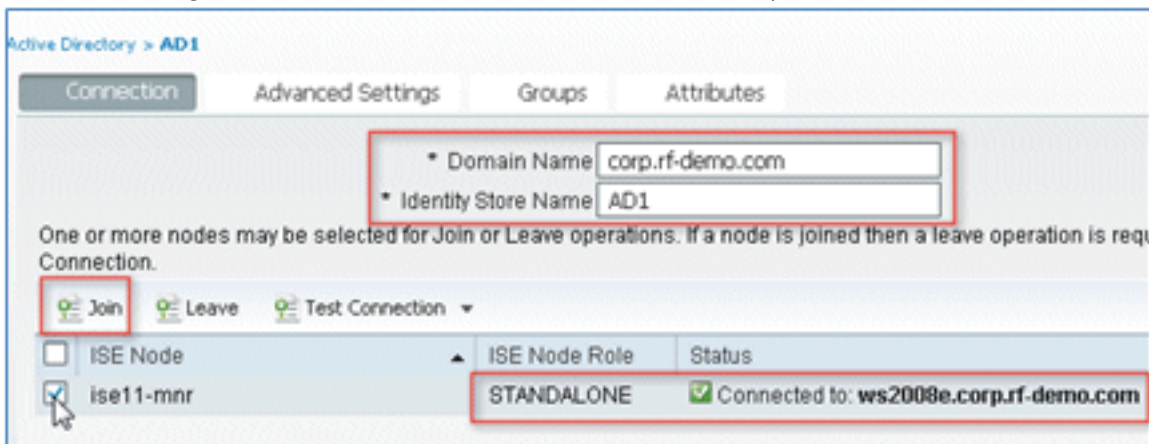


3. Klicken Sie auf **Active Directory**.

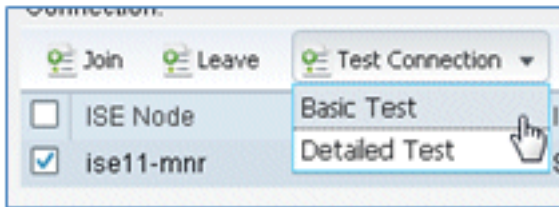


4. Auf der Registerkarte Verbindung:

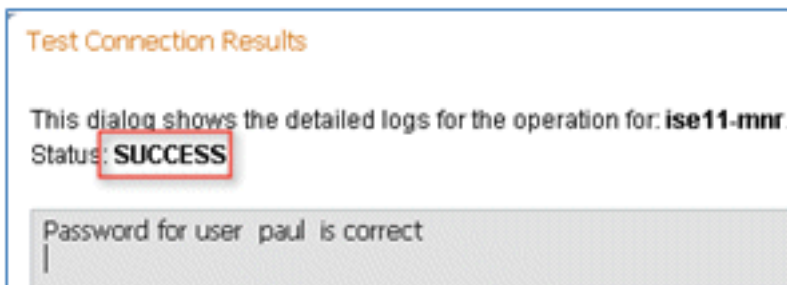
Fügen Sie den Domännennamen **corp.rf-demo.com** (in diesem Beispiel) hinzu, und ändern Sie den Standardnamen des Identitätsspeichers in **AD1**. Klicken Sie auf **Konfiguration speichern**. Klicken Sie auf **Join** (Teilnehmen), und geben Sie den Benutzernamen und das Kennwort für das AD-Administratorkonto an, die für die Teilnahme erforderlich sind. Der Status muss grün sein. Aktivieren Sie **Verbunden mit:** (Kontrollkästchen ist aktiviert).



5. Durchführen eines einfachen Verbindungstests mit dem AD bei einem aktuellen Domänenbenutzer.

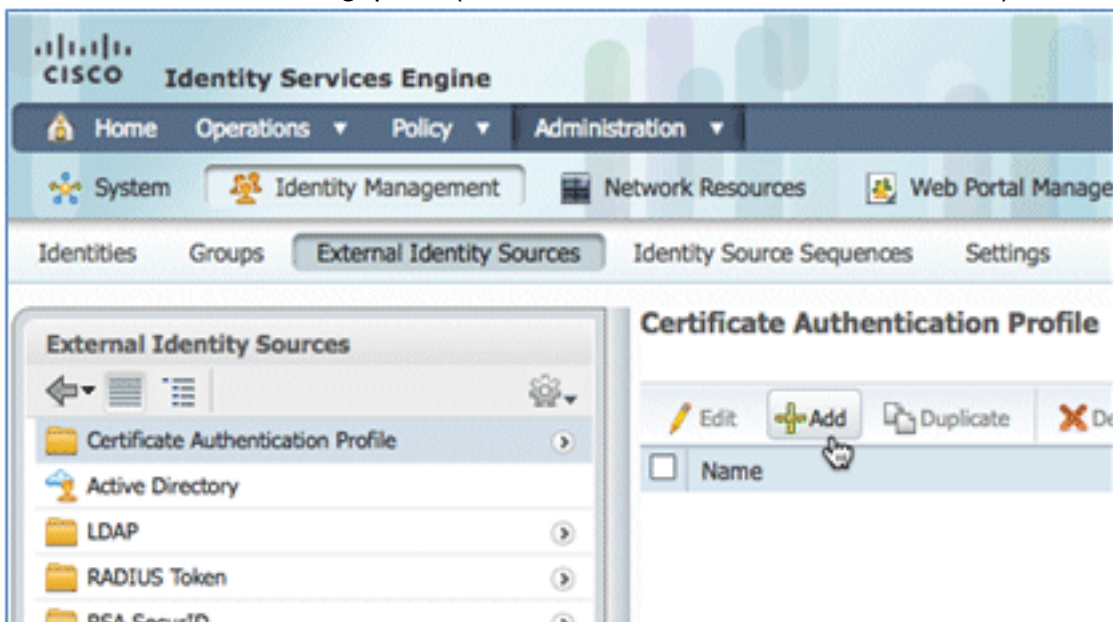


6. Wenn die Verbindung mit dem AD erfolgreich hergestellt wurde, wird in einem Dialogfeld bestätigt, dass das Kennwort richtig ist.



7. Navigieren Sie zu **Administration > Identity Management > External Identity Sources**:

Klicken Sie auf **Zertifikatauthentifizierungsprofil**. Klicken Sie auf **Hinzufügen**, um ein neues Zertifikatauthentifizierungsprofil (Certificate Authentication Profile, CAP) zu erstellen.



8. Geben Sie den Namen **CertAuth** (in diesem Beispiel) für die CAP ein. Wählen Sie als Principal Username X509 Attribute den **Common Name** aus, und klicken Sie dann auf **Submit (Senden)**.

Certificate Authentication Profiles List > New Certificate Authentication Profile

### Certificate Authentication Profile

\* Name

Description

Principal Username X509 Attribute

Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory

LDAP/AD Instance Name

9. Bestätigen Sie, dass die neue GAP hinzugefügt wird.

CISCO Identity Services Engine

Home Operations Policy Administration

System Identity Management Network Resources Web Portal Management

Identities Groups External Identity Sources Identity Source Sequences Settings

### External Identity Sources

- Certificate Authentication Profile
- Active Directory
- LDAP
- RADIUS Token
- RSA SecurID

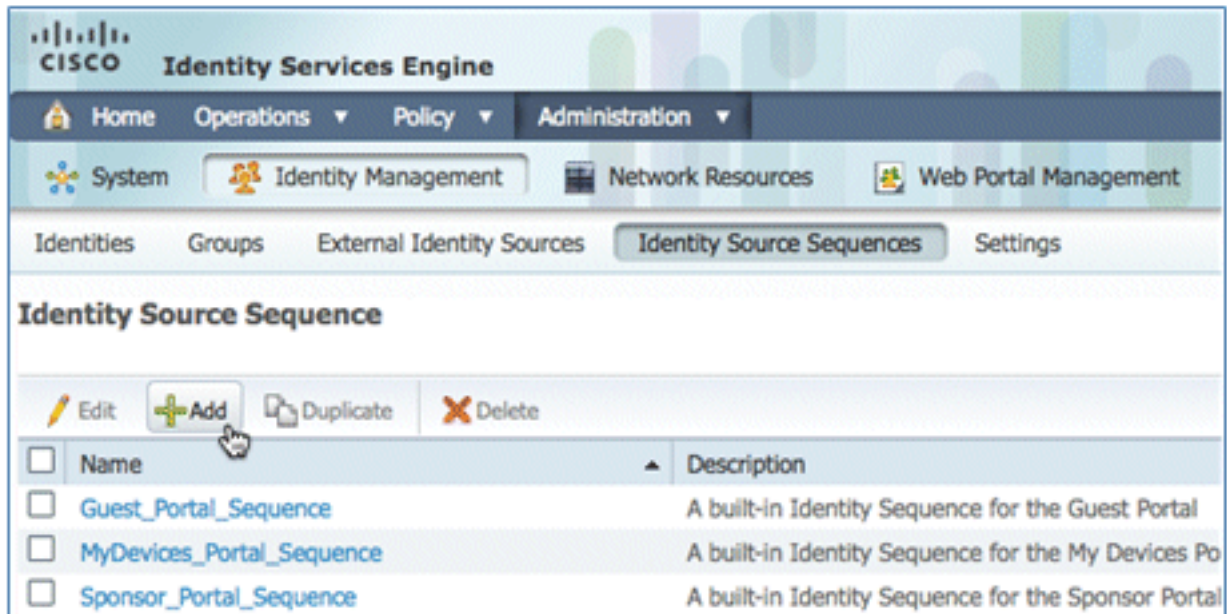
### Certificate Authentication Profile

Edit Add Duplicate Delete

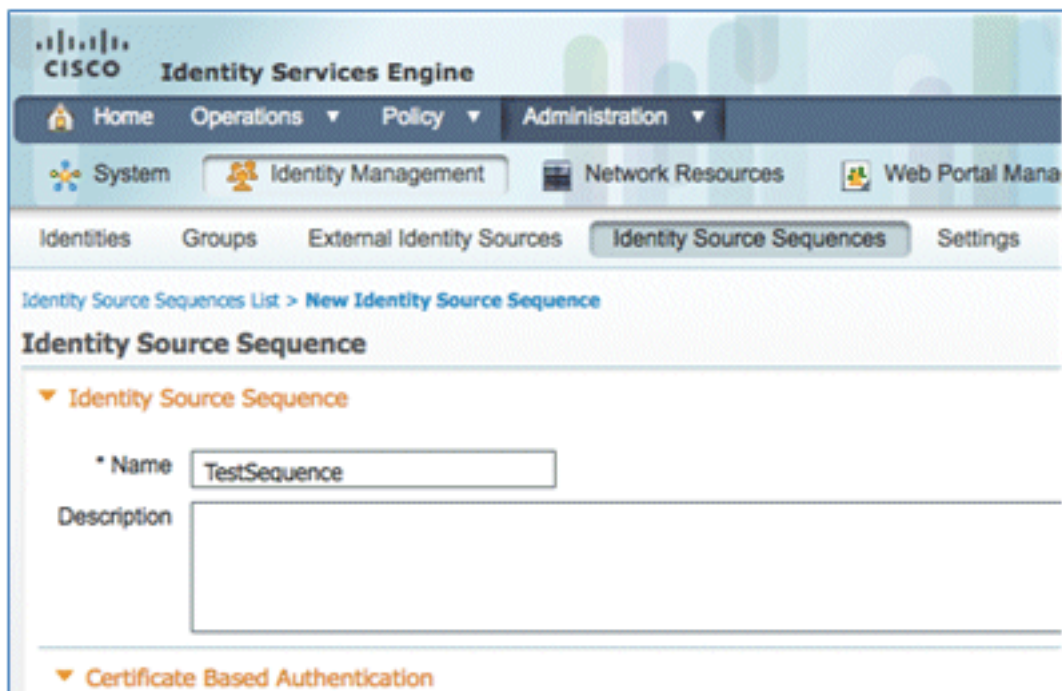
<input type="checkbox"/>	Name
<input type="checkbox"/>	CertAuth

10. Navigieren Sie zu **Administration > Identity Management > Identity Source Sequences**, und klicken Sie auf **Add** .



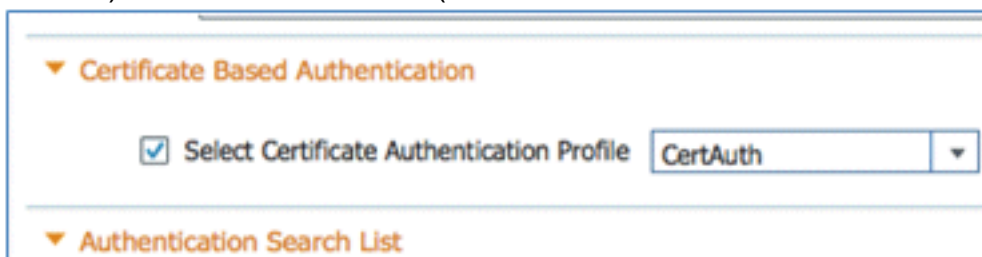


11. Geben Sie der Sequenz den Namen **TestSequence** (in diesem Beispiel).



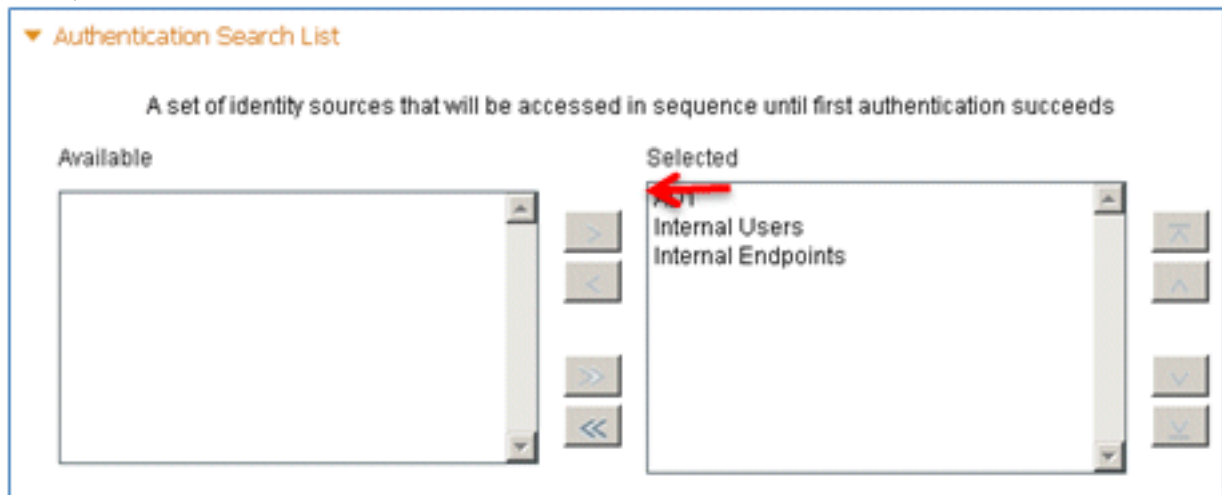
12. Blättern Sie nach unten zu **Zertifikatbasierte Authentifizierung**:

Aktivieren Sie die Option **Zertifikatauthentifizierungsprofil auswählen** (Kontrollkästchen ist aktiviert). Wählen Sie **CertAuth** (oder ein anderes zuvor erstelltes CAP-Profil) aus.

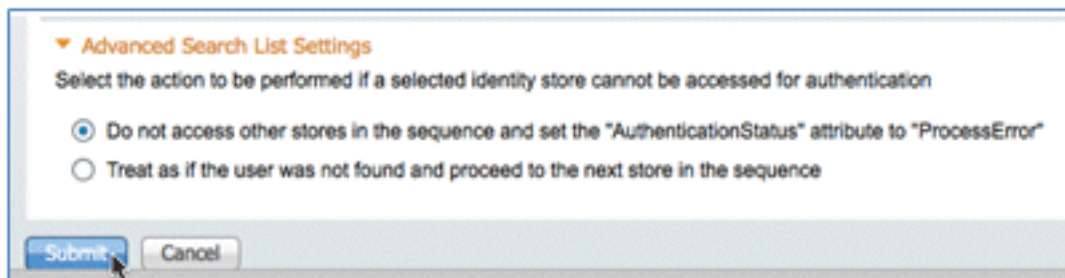


13. Blättern Sie nach unten zur **Authentifizierungssuchliste**:

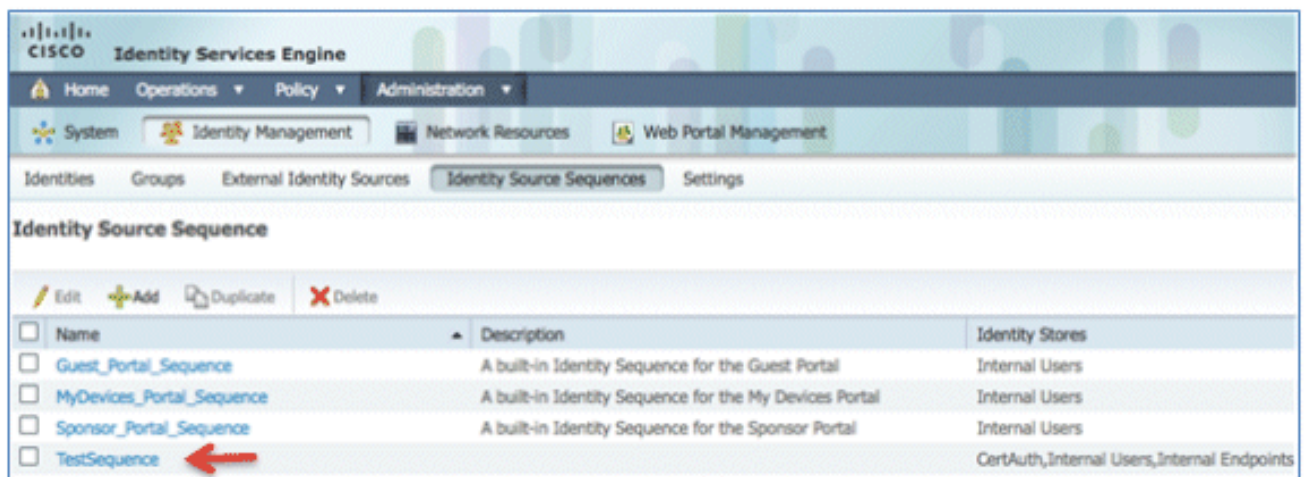
AD1 von "Verfügbar" in "Ausgewählt" verschieben. Klicken Sie auf die Schaltfläche Nach oben, um AD1 zur obersten Priorität zu verschieben.



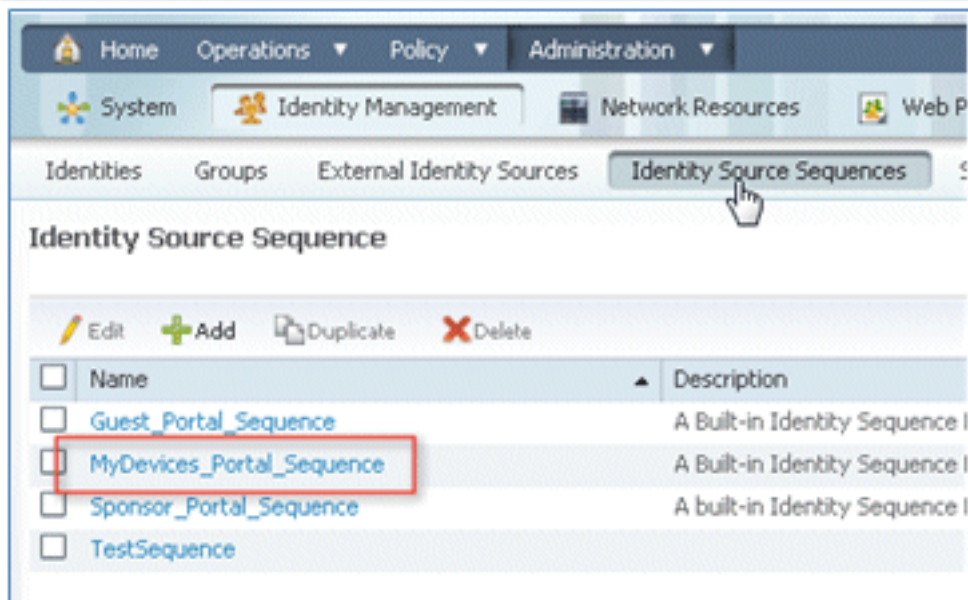
14. Klicken Sie zum Speichern auf **Senden**.



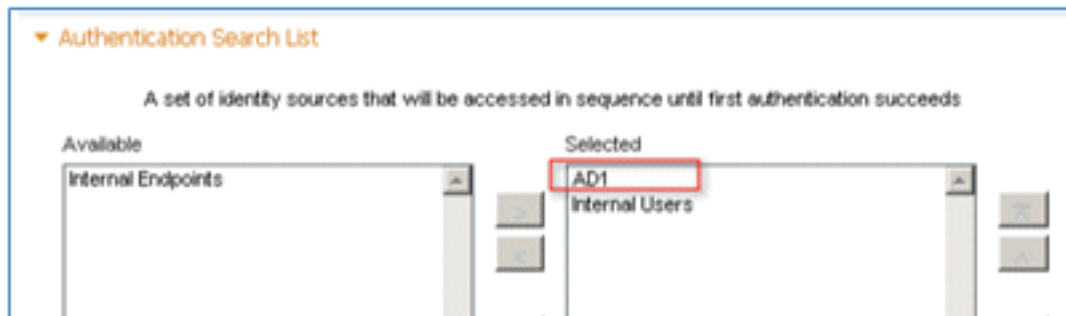
15. Bestätigen Sie, dass die neue Identitätsquellensequenz hinzugefügt wird.



16. Verwenden Sie AD, um das Portal "Meine Geräte" zu authentifizieren. Navigieren Sie zu ISE > Administration > Identity Management > Identity Source Sequence, und bearbeiten Sie MyDevices\_Portal\_Sequence.



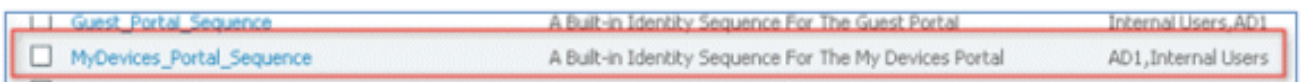
17. Fügen Sie **AD1** zur Liste "Ausgewählt" hinzu, und klicken Sie auf die Schaltfläche "Nach oben", um AD1 zur obersten Priorität zu verschieben.



18. Klicken Sie auf **Speichern**.



19. Bestätigen Sie, dass die Identity Store-Sequenz für MyDevices\_Portal\_Sequence **AD1** enthält.



20. Wiederholen Sie die Schritte 16-19, um AD1 für Guest\_Portal\_Sequence hinzuzufügen, und klicken Sie auf **Save**.



21. Bestätigen Sie, dass Guest\_Portal\_Sequence **AD1** enthält.

<input type="checkbox"/>	Name	Description	Identity Stores
<input type="checkbox"/>	Guest_Portal_Sequence	A Built-in Identity Sequence For The Guest Portal	Internal Users,AD1

22. Um den WLC dem Netzwerkzugriffgerät (WLC) hinzuzufügen, navigieren Sie zu **Administration > Network Resources > Network Devices**, und klicken Sie auf **Add**.



23. Fügen Sie den WLC-Namen, die IP-Adresse, die Subnetzmaske usw. hinzu.



Network Devices List > New Network Device

### Network Devices

\* Name

Description

---

\* IP Address:  /

---

Model Name

Software Version

---

\* Network Device Group

Location

Device Type

24. Navigieren Sie zu Authentifizierungseinstellungen, und geben Sie den gemeinsamen Schlüssel ein. Dies muss mit dem gemeinsamen geheimen Schlüssel des WLC-RADIUS übereinstimmen.

Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

\* Shared Secret

Enable KeyWrap  ⓘ

\* Key Encryption Key

\* Message Authenticator Code Key

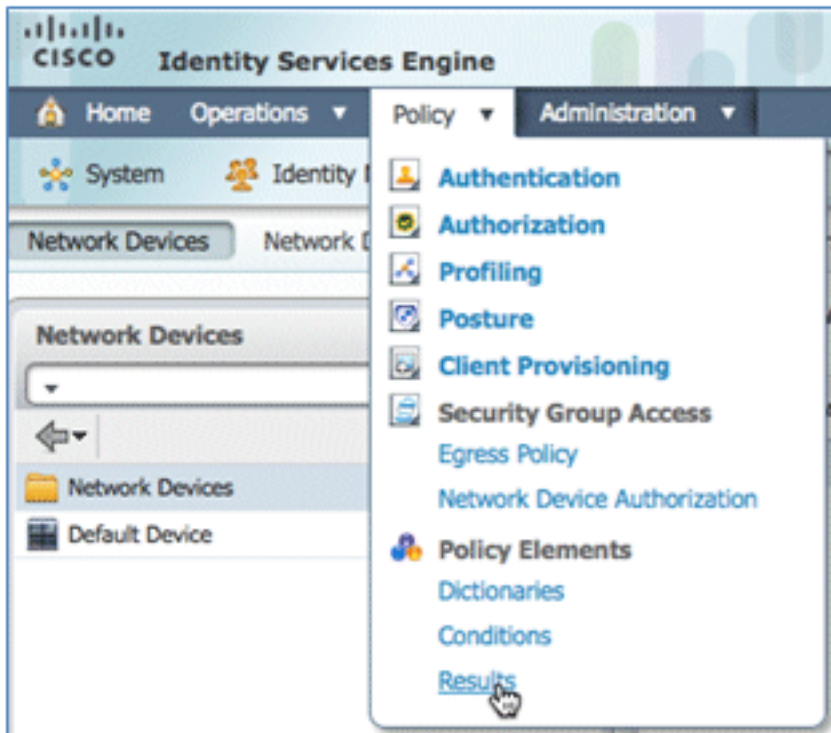
Key Input Format  ASCII  HEXADECIMAL

SNMP Settings

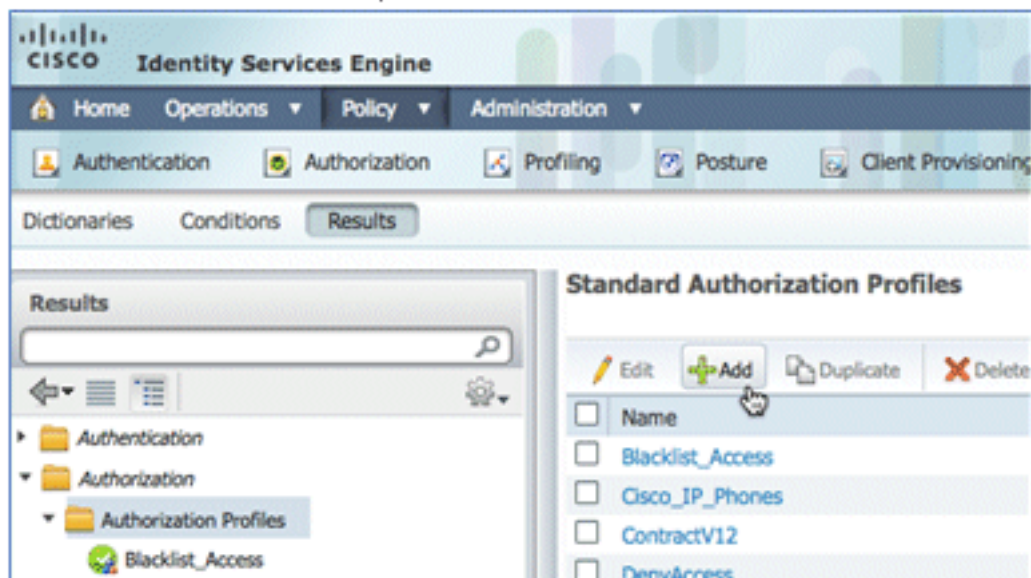
SGA Attributes

25. Klicken Sie auf **Senden**.

26. Navigieren Sie zu ISE > Policy > Policy Elements > Results.



27. Erweitern Sie **Ergebnisse** und **Autorisierung**, klicken Sie auf **Autorisierungsprofile**, und klicken Sie auf **Hinzufügen**, um ein neues Profil anzuzeigen.



28. Geben Sie diesem Profil folgende Werte:

Name: **CWA**

Authorization Profiles > New Authorization Profile

### Authorization Profile

\* Name

Description

\* Access Type

Web-Authentifizierung aktivieren (Kontrollkästchen ist aktiviert):

Web-Authentifizierung: **zentralisiert**ACL: **ACL-REDIRECT** (ACL-REDIRECT muss mit dem Namen der vorauthentifizierten WLC-ACL übereinstimmen.)Umleitung: **Standard**

Common Tasks

DACL Name

VLAN

Voice Domain Permission

Web Authentication  ACL  Redirect

29. Klicken Sie auf **Senden**, und bestätigen Sie, dass das CWA-Autorisierungsprofil hinzugefügt wurde.

### Standard Authorization Profiles

Edit Add Duplicate Delete

Name

Blacklist\_Access

**CWA**

Cisco\_IP\_Phones

30. Klicken Sie auf **Hinzufügen**, um ein neues Autorisierungsprofil zu erstellen.

### Standard Authorization Profiles

Edit **Add** Duplicate Delete

Name

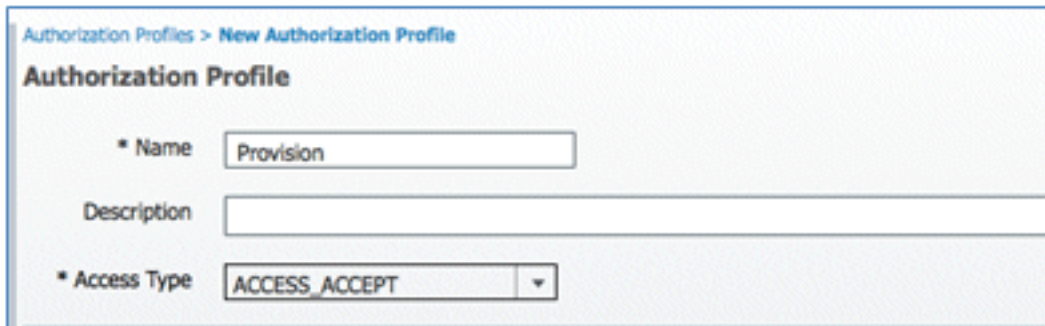
Blacklist\_Access

CWA

Cisco\_IP\_Phones

31. Geben Sie diesem Profil folgende Werte:

Name: **Provision**



Authorization Profiles > New Authorization Profile

### Authorization Profile

\* Name

Description

\* Access Type

Web-Authentifizierung aktivieren (Kontrollkästchen ist aktiviert):

Wert der Webauthentifizierung: **Bereitstellung von Komponenten**



Common Tasks

DACL Name

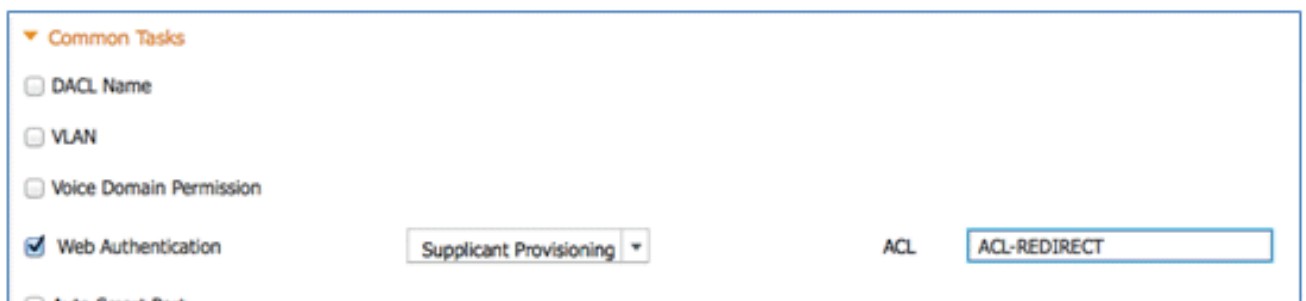
VLAN

Voice Domain Permission

Web Authentication  ACL

- Centralized
- Device Registration
- Posture Discovery
- Supplicant Provisioning

ACL: **ACL-REDIRECT** (ACL-REDIRECT muss mit dem Namen der vorauthentifizierten WLC-ACL übereinstimmen.)



Common Tasks

DACL Name

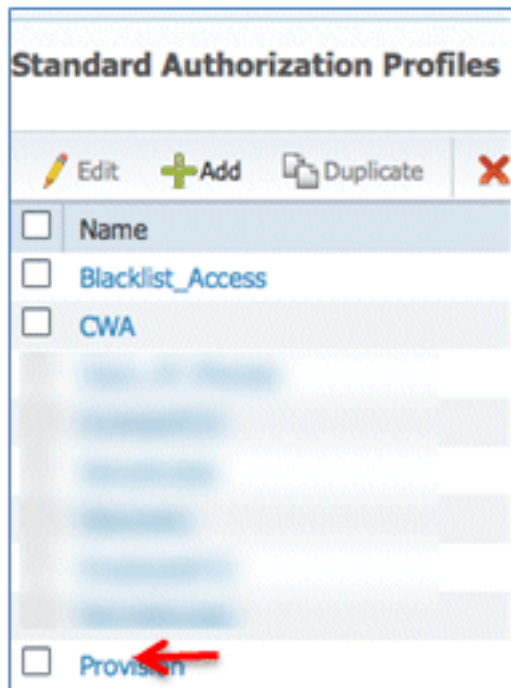
VLAN

Voice Domain Permission

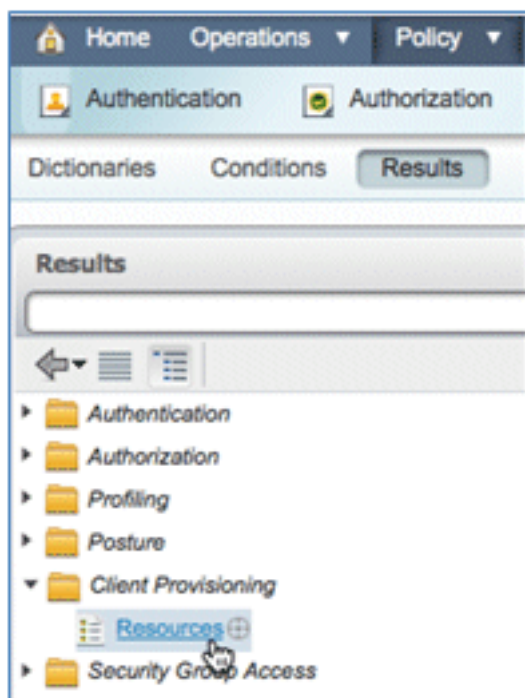
Web Authentication  ACL

Auto Smart Port

32. Klicken Sie auf **Senden**, und bestätigen Sie, dass das Berechtigungsprofil "Bereitstellen" hinzugefügt wurde.

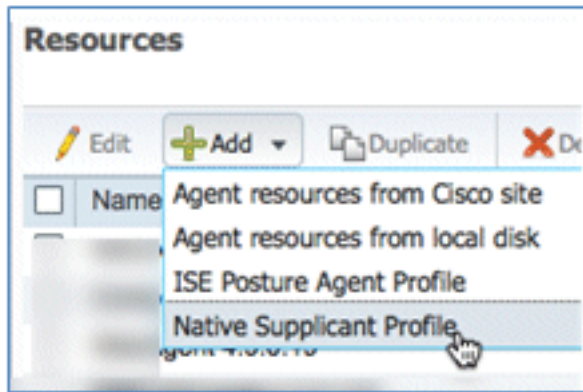


33. Blättern Sie in Results (Ergebnisse) nach unten, erweitern Sie **Client Provisioning**, und klicken Sie auf **Resources (Ressourcen)**.



34. Wählen Sie **Native Supplicant Profile** aus.





35. Geben Sie dem Profil den Namen **WirelessSP** (in diesem Beispiel).

Native Supplicant Profile

\* Name

Description

36. Geben Sie folgende Werte ein:

Verbindungstyp: **Wireless** SSID: **Demo1x** (dieser Wert stammt aus der WLC 802.1x-WLAN-Konfiguration) Zulässiges Protokoll: **TLS** Schlüssellänge: **1024**

\* Operating System

\* Connection Type  Wired  Wireless

\* SSID

Security

\* Allowed Protocol

Optional Settings

37. Klicken Sie auf **Senden**.

38. Klicken Sie auf **Speichern**.

\* Allowed Protocol

\* Key Size

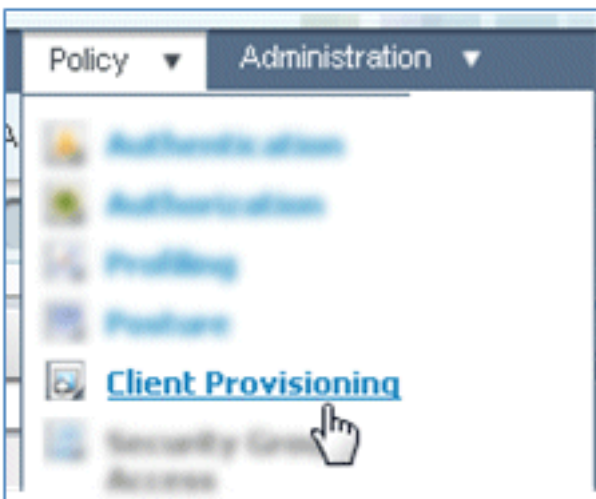
39. Bestätigen Sie, dass das neue Profil hinzugefügt wurde.

**Resources**

Edit + Add Duplicate Delete

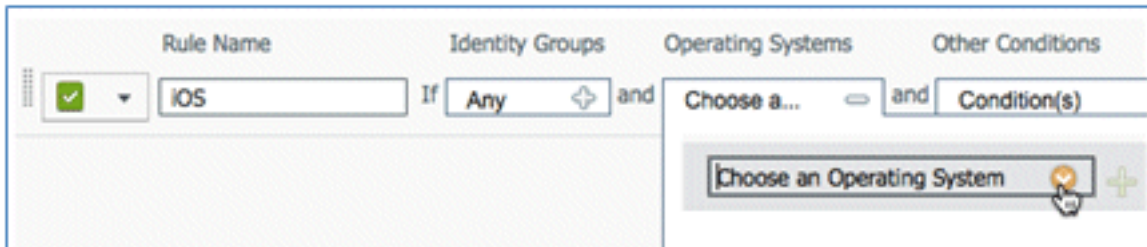
<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	WirelessS	NativeSPProfile

40. Navigieren Sie zu **Richtlinie > Client-Bereitstellung**.

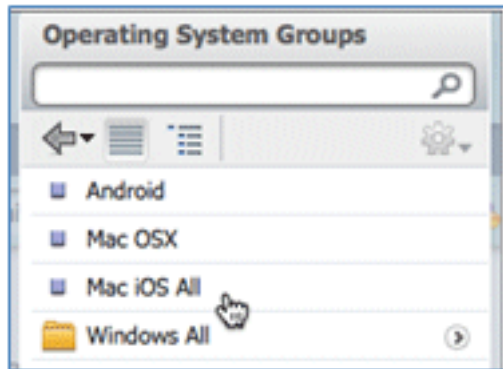


41. Geben Sie die folgenden Werte für die Bereitstellungsregel von iOS-Geräten ein:

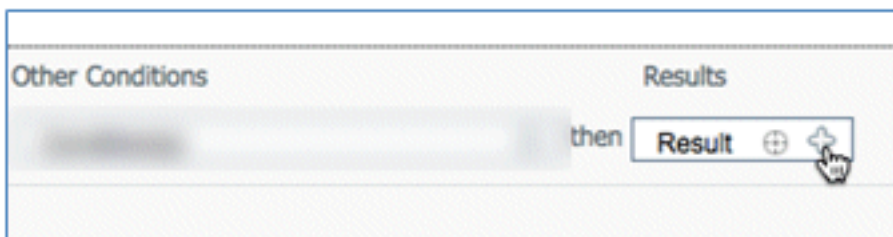
Regelname: iOSIdentitätsgruppen: Alle



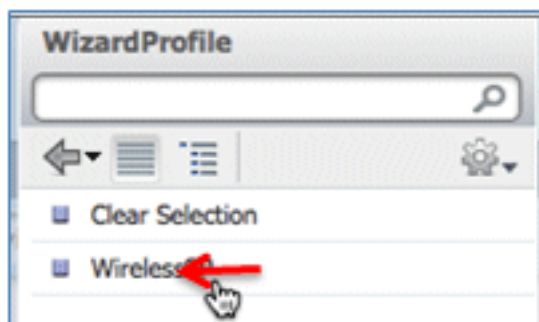
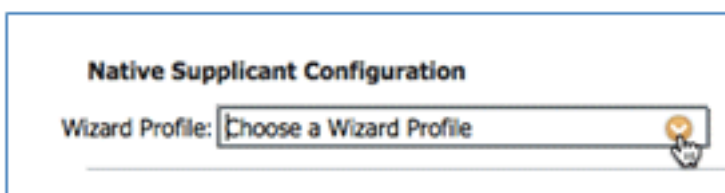
Betriebssysteme: **Mac iOS Alle**



Ergebnisse: **WirelessSP** (dies ist das zuvor erstellte Native Supplcant-Profil)

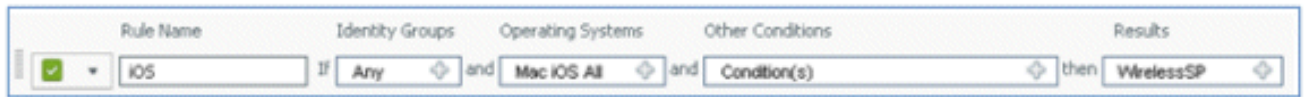


Navigieren Sie zu **Ergebnisse > Assistentenprofil** (Dropdown-Liste) > **WirelessSP**.

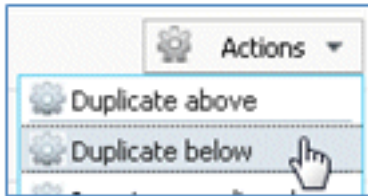


42. Bestätigen Sie, dass das iOS-Bereitstellungsprofil hinzugefügt wurde.





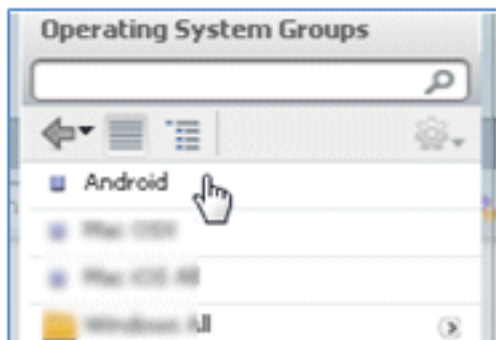
43. Suchen Sie auf der rechten Seite der ersten Regel die Dropdown-Liste "Aktionen", und wählen Sie **Unten** (oder darüber) **Duplizieren**.



44. Ändern Sie den Namen der neuen Regel in **Android**.



45. Ändern Sie das Betriebssystem auf **Android**.

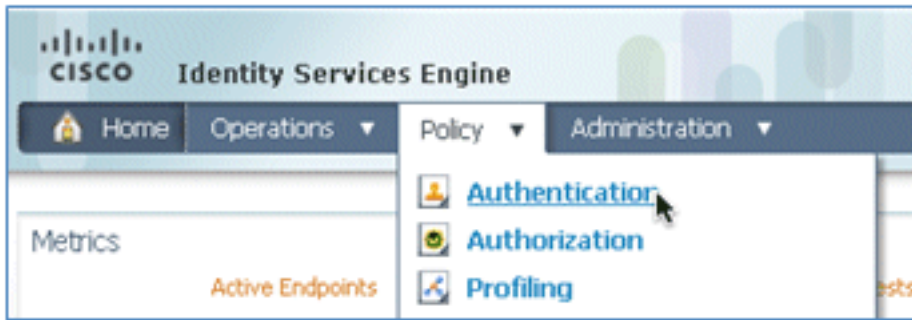


46. Lassen Sie die anderen Werte unverändert.

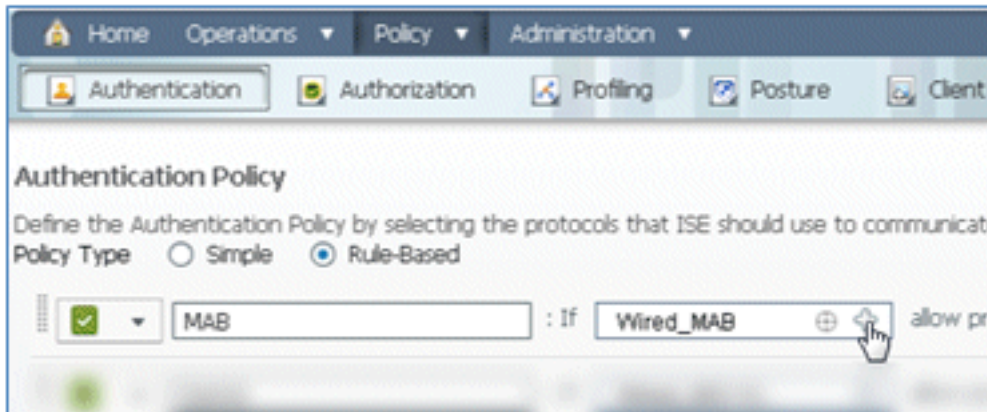
47. Klicken Sie auf **Speichern** (linker unterer Bildschirm).



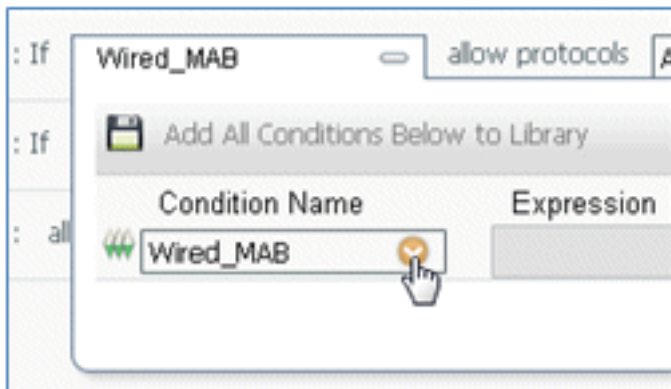
48. Navigieren Sie zu **ISE > Policy > Authentication**.



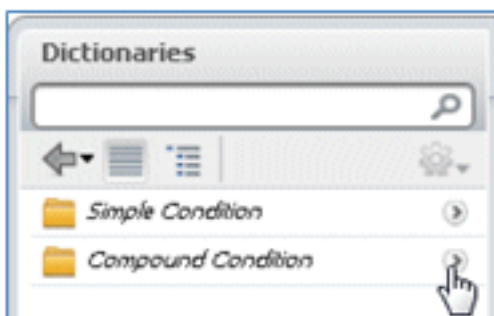
49. Ändern Sie die Bedingung, sodass sie Wireless\_MAB enthält, und erweitern Sie Wired\_MAB.



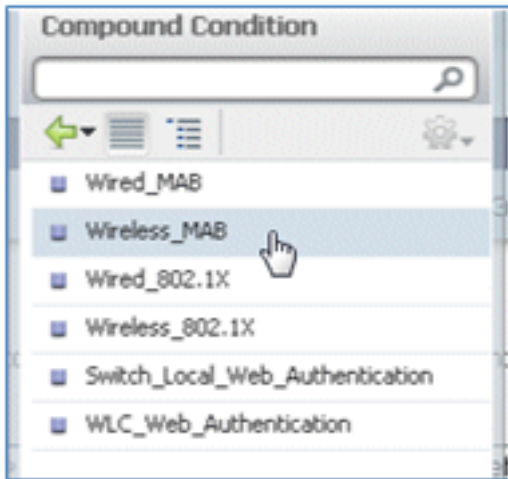
50. Klicken Sie auf die Dropdown-Liste **Bedingungsname**.



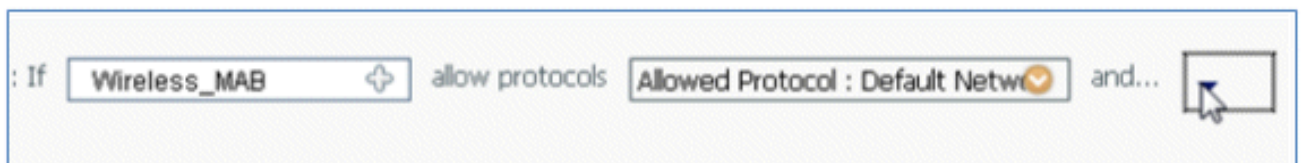
51. Wählen Sie **Wörterbücher > Zusammengesetzte Bedingung** aus.



52. Wählen Sie **Wireless\_MAB** aus.

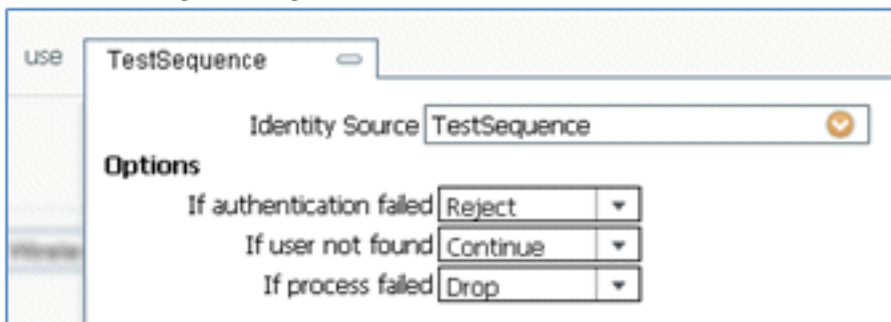


53. Klicken Sie rechts neben der Regel auf den Pfeil, um sie zu erweitern.

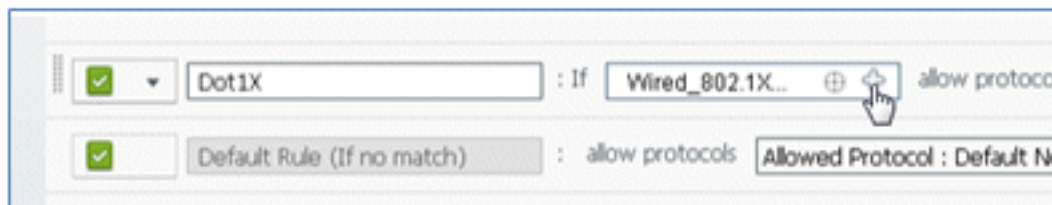


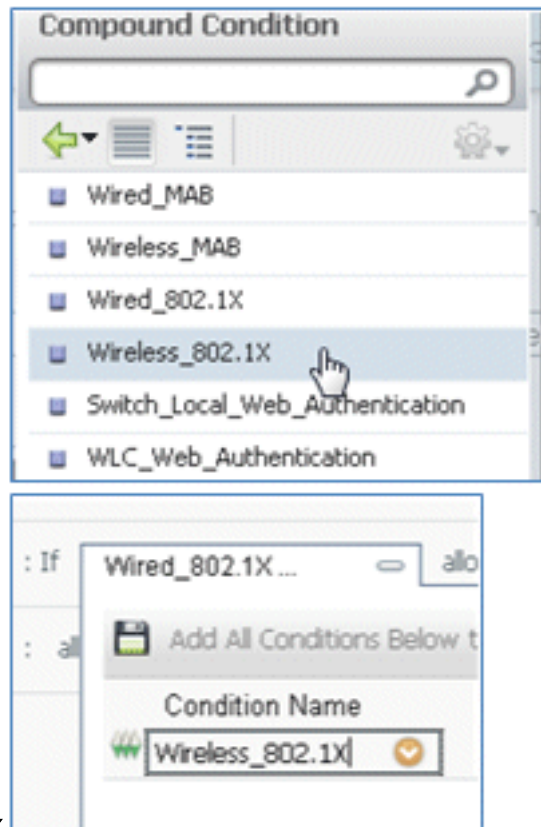
54. Wählen Sie diese Werte aus der Dropdown-Liste aus:

Identitätsquelle: **TestSequence** (dies ist der zuvor erstellte Wert)  
 Wenn Authentifizierung fehlgeschlagen ist: **Ablehnen**  
 Wenn Benutzer nicht gefunden wird: **Fortfahren**  
 Wenn der Prozess fehlgeschlagen ist: **Löschen**



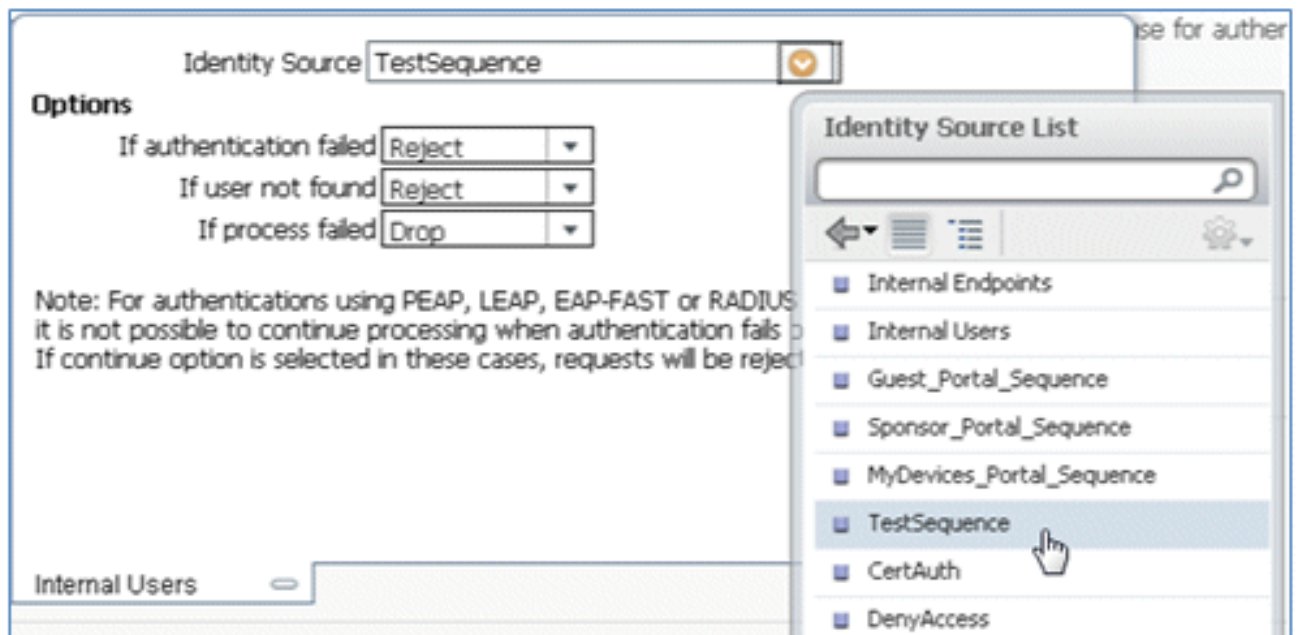
55. Wechseln Sie zur **Dot1X**-Regel, und ändern Sie die folgenden Werte:





Zustand: **Wireless\_802.1X**

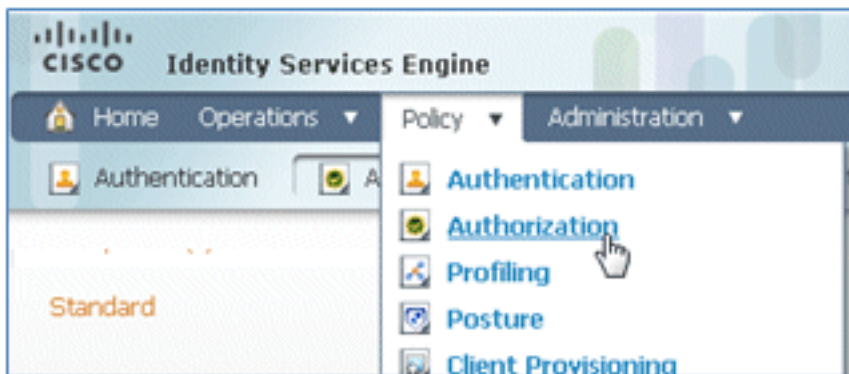
Identitätsquelle: **TestSequence**



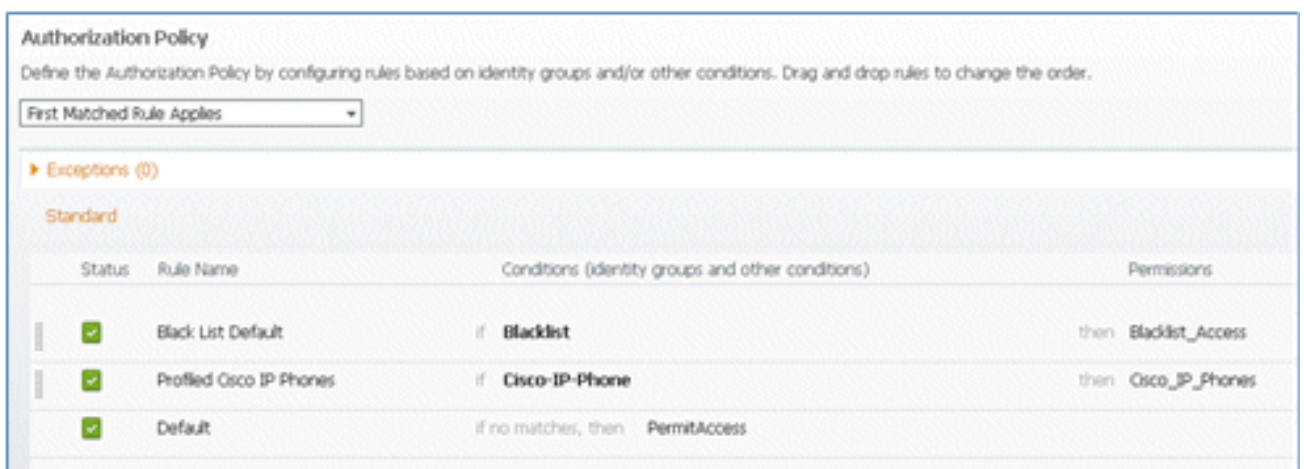
56. Klicken Sie auf **Speichern**.



57. Navigieren Sie zu **ISE > Policy > Authorization**.



58. Die Standardregeln (z. B. Black List Default, Profiled und Default) sind bereits ab der Installation konfiguriert. Die ersten beiden Regeln können ignoriert werden. Die Standardregel wird zu einem späteren Zeitpunkt bearbeitet.



59. Klicken Sie rechts neben der zweiten Regel (Cisco IP-Telefone mit Profil) auf den Abwärtspfeil neben "Bearbeiten", und wählen Sie **Neue Regel darunter einfügen** aus.



Eine neue Standardregelnummer wird hinzugefügt.

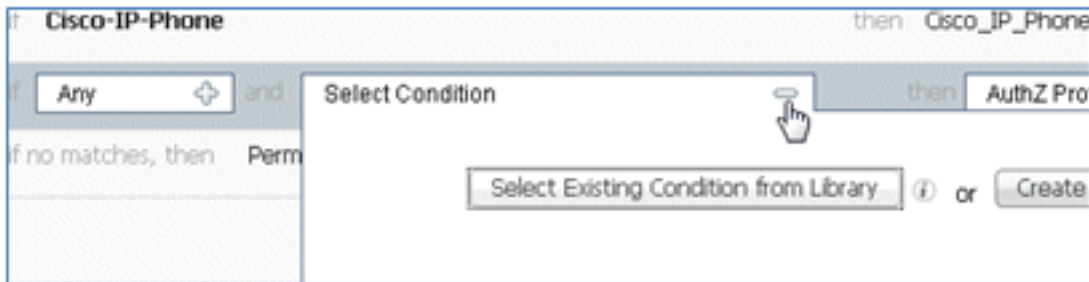




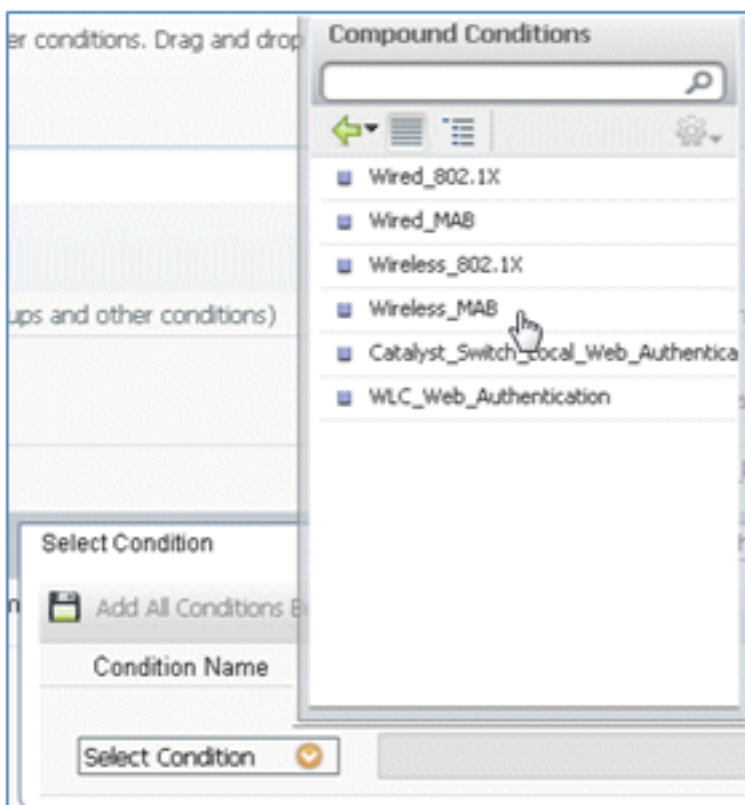
60. Ändern Sie den Regelnamen von der Standardregelnummer in **OpenCWA**. Diese Regel initiiert den Registrierungsprozess im offenen WLAN (Dual-SSID) für Benutzer, die zum Gastnetzwerk kommen, um Geräte bereitstellen zu lassen.



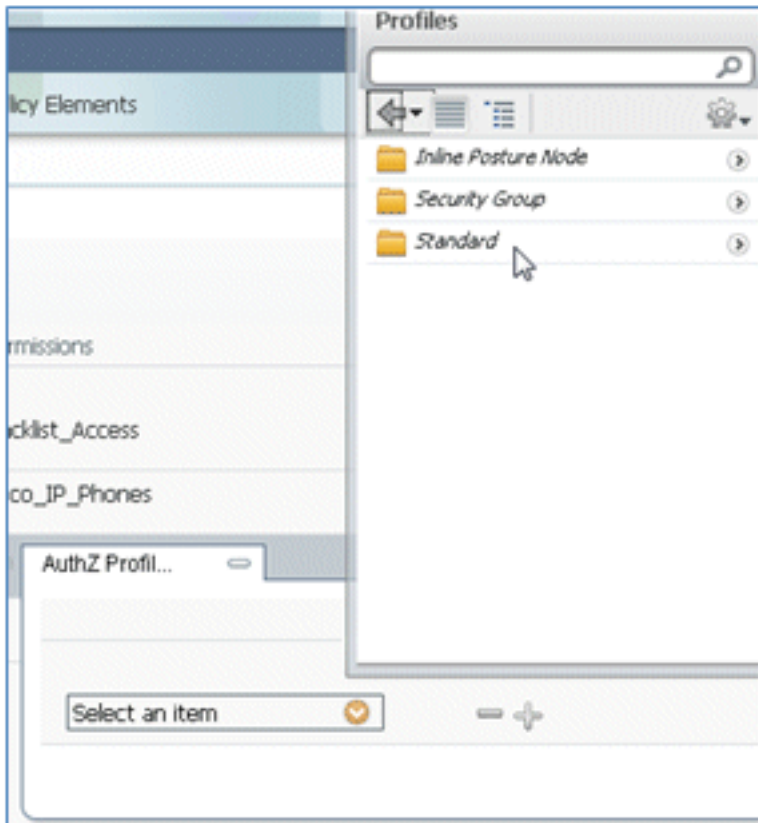
61. Klicken Sie auf das Pluszeichen (+) für Bedingung(en), und klicken Sie auf **Vorhandene Bedingung aus Bibliothek auswählen**.



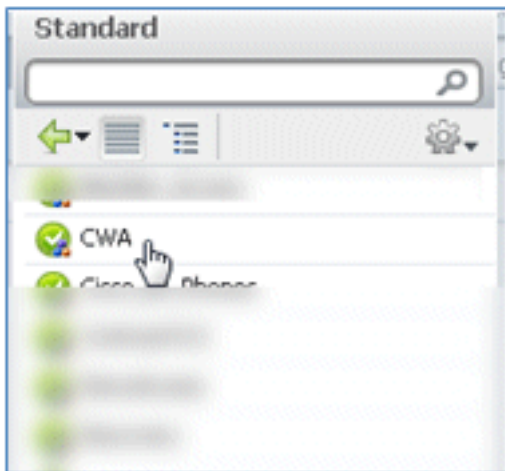
62. Wählen Sie **Zusammengesetzte Bedingungen > Wireless\_MAB** aus.



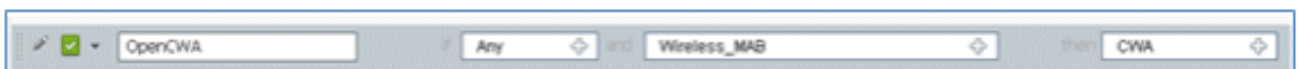
63. Klicken Sie im AuthZ-Profil auf das Pluszeichen (+), und wählen Sie **Standard** aus.



64. Wählen Sie den Standard-CWA aus (dies ist das zuvor erstellte Autorisierungsprofil).



65. Bestätigen Sie, dass die Regel mit den richtigen Bedingungen und Autorisierungen hinzugefügt wurde.



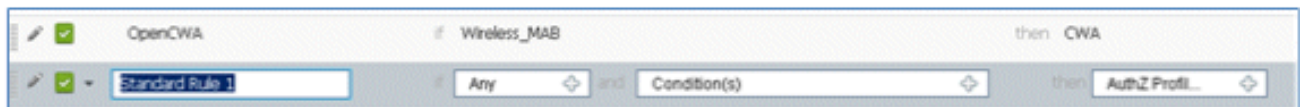
66. Klicken Sie **Fertig** (auf der rechten Seite der Regel).



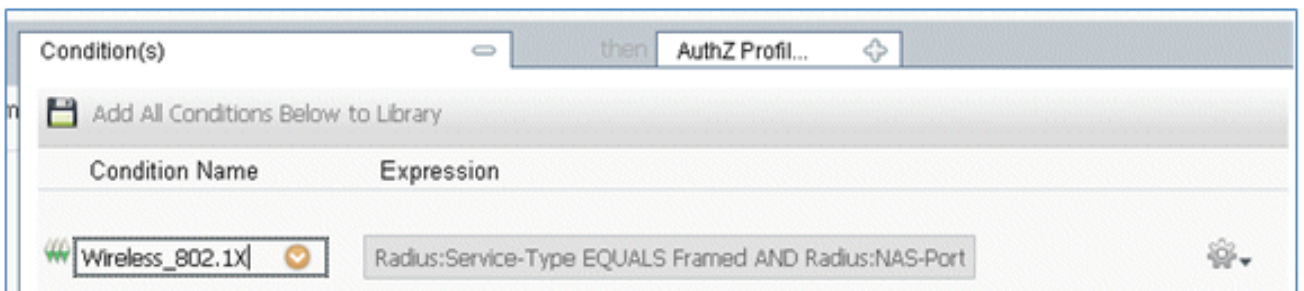
67. Klicken Sie rechts neben der gleichen Regel auf den Abwärtspfeil neben Bearbeiten, und wählen Sie **Neue Regel darunter einfügen aus**.



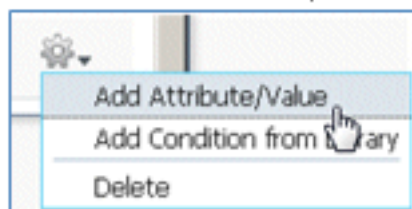
68. Ändern Sie den Regelnamen von Standardregelnummer in **PEAPrule** (in diesem Beispiel). Diese Regel gilt für PEAP (wird auch für ein Einzel-SSID-Szenario verwendet), um zu prüfen, ob die 802.1X-Authentifizierung ohne Transport Layer Security (TLS) erfolgt und die Bereitstellung der Netzwerkkomponenten mit dem zuvor erstellten Bereitstellungs-Autorisierungsprofil initiiert wurde.



69. Ändern Sie die Bedingung in **Wireless\_802.1X**.

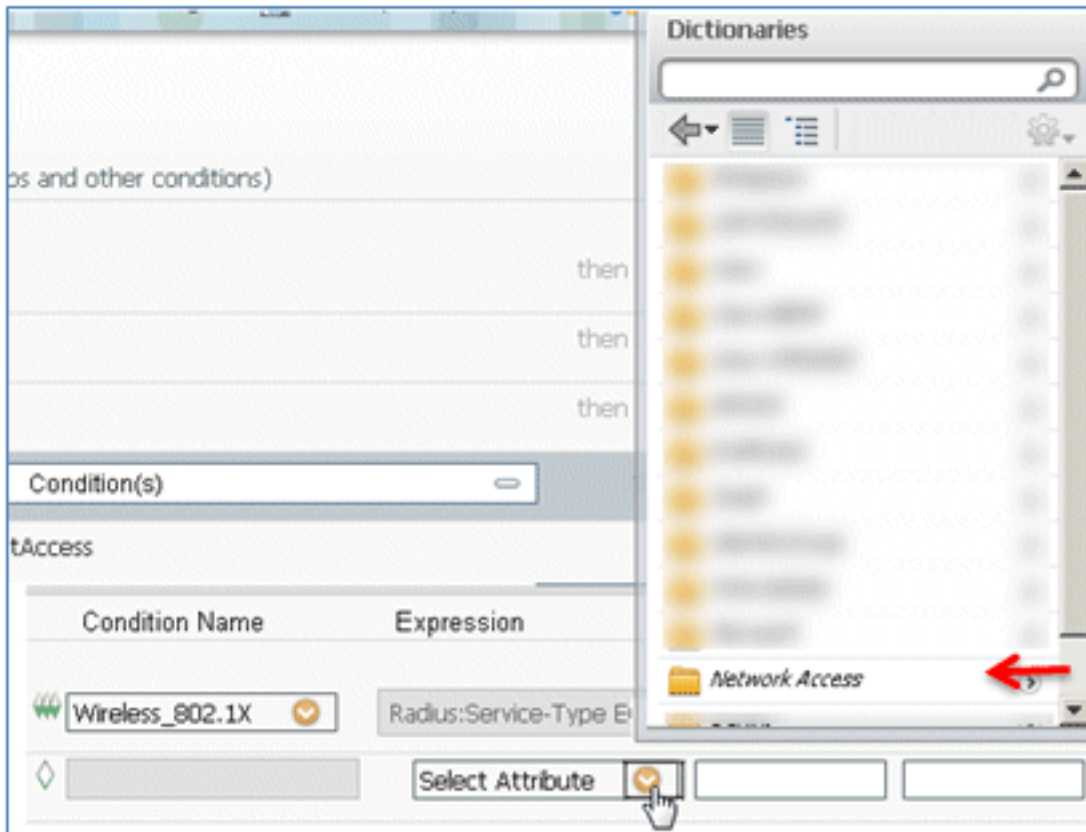


70. Klicken Sie auf das Zahnrad-Symbol auf der rechten Seite der Bedingung, und wählen Sie **Attribut/Wert hinzufügen aus**. Dies ist eine 'und'-Bedingung, keine 'oder'-Bedingung.

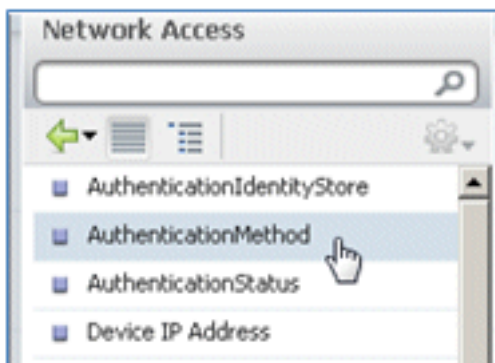


71. Suchen Sie nach und wählen Sie **Netzwerkzugriff aus**.

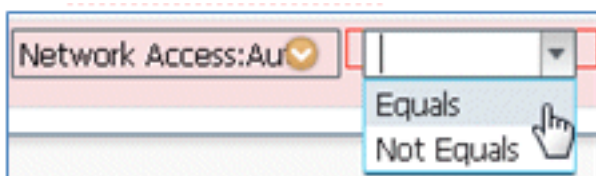




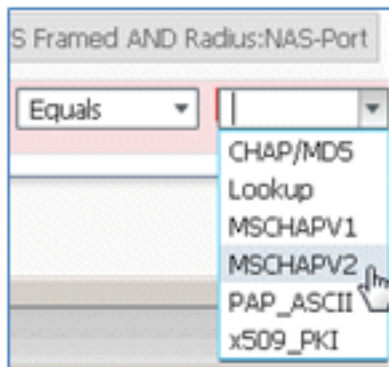
72. Wählen Sie **AuthenticationMethod** aus, und geben Sie die folgenden Werte ein:



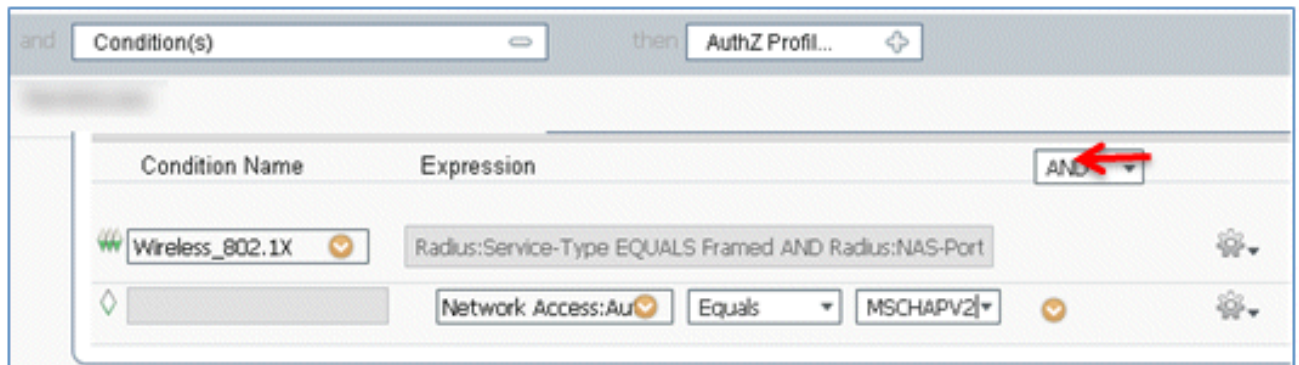
Authentifizierungsmethode: **Equals**



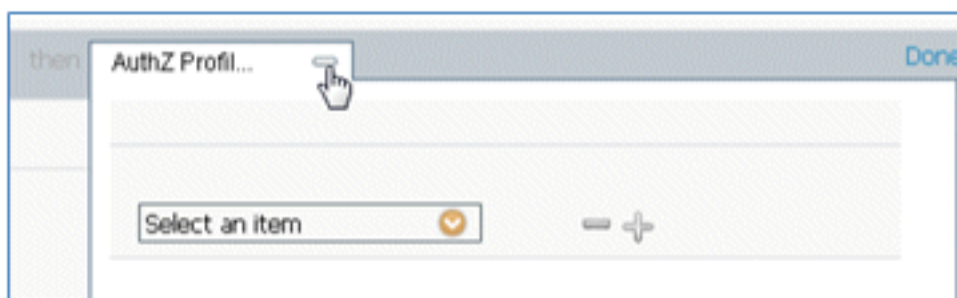
Wählen Sie **MSCHAPV2** aus.

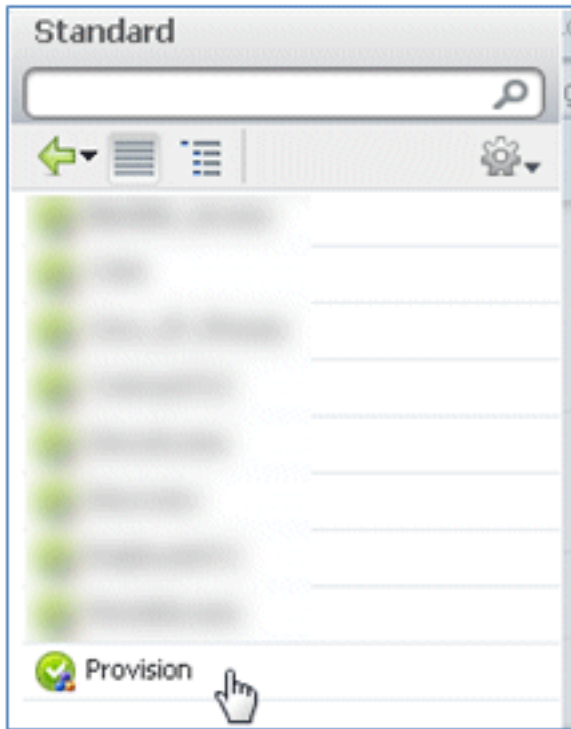


Dies ist ein Beispiel für die Regel. Stellen Sie sicher, dass die Bedingung ein AND ist.



73. Wählen Sie in AuthZ Profile (AuthZ-Profil) **Standard** > **Provision** (dies ist das zuvor erstellte Autorisierungsprofil) aus.





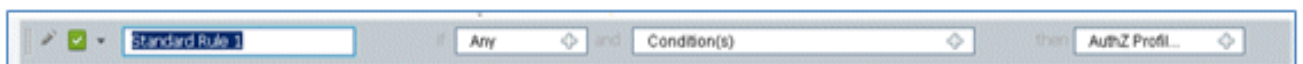
74. Klicken Sie auf **Fertig**.



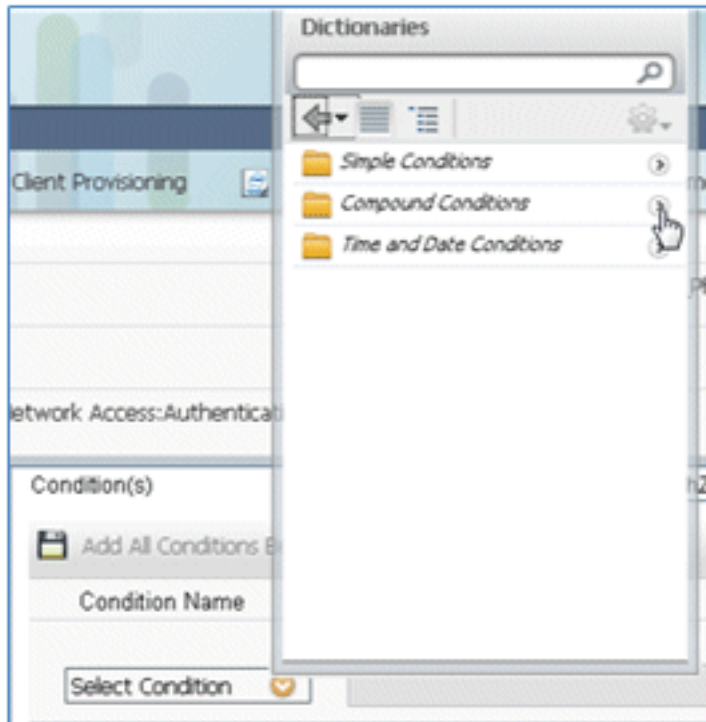
75. Klicken Sie rechts neben der PEAP-Regel auf den Abwärtspfeil neben Bearbeiten, und wählen Sie **Neue Regel darunter einfügen** aus.



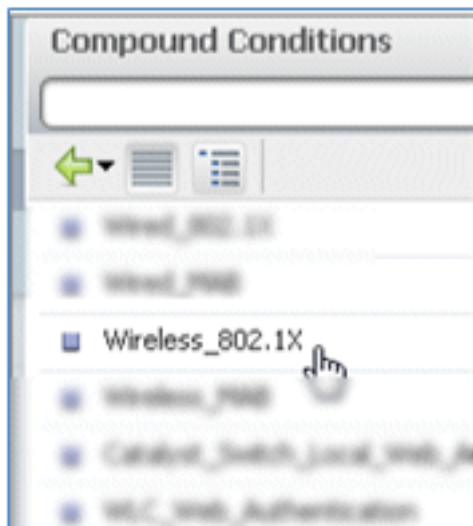
76. Ändern Sie den Regelnamen von Standardregelnummer in **Zulassen** (in diesem Beispiel). Diese Regel wird verwendet, um den Zugriff auf registrierte Geräte mit installierten Zertifikaten zu ermöglichen.



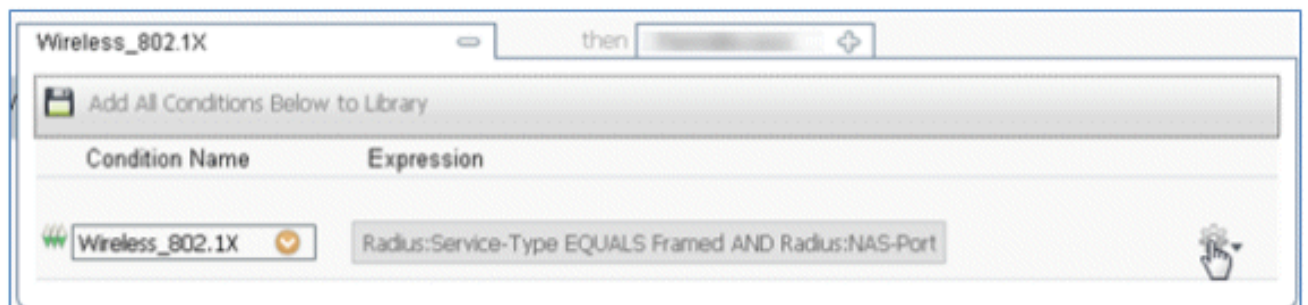
77. Wählen Sie unter Bedingung(en) die Option **Zusammengesetzte Bedingungen** aus.



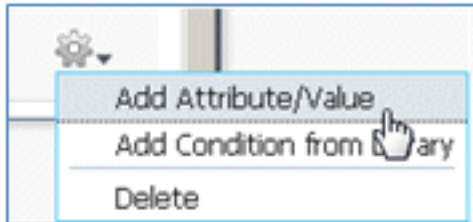
78. Wählen Sie **Wireless\_802.1X** aus.



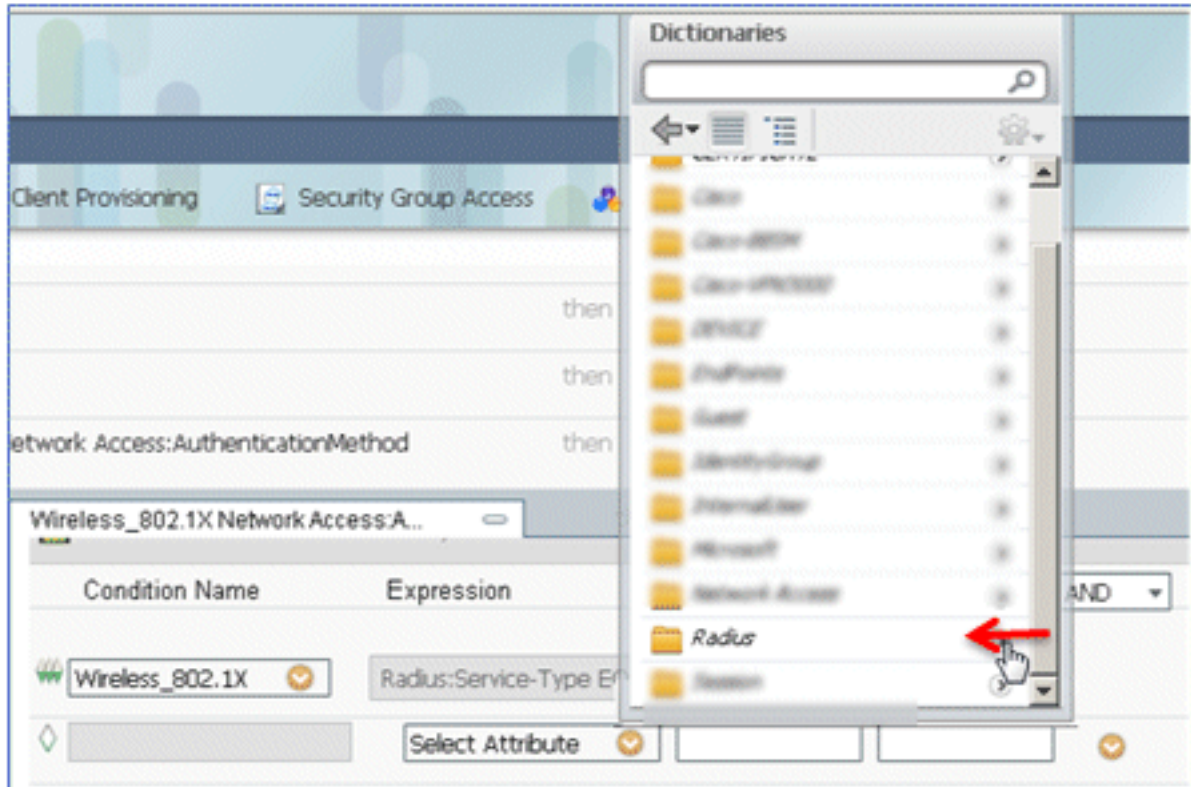
79. Fügen Sie ein AND-Attribut hinzu.



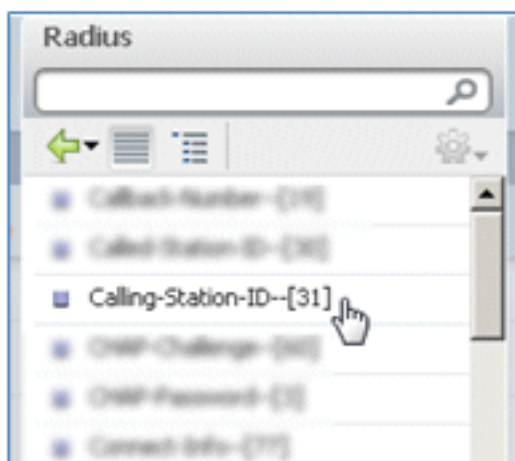
80. Klicken Sie auf das Zahnrad-Symbol auf der rechten Seite der Bedingung, und wählen Sie **Attribut/Wert hinzufügen** aus.



81. Suchen Sie nach und wählen Sie **Radius** aus.

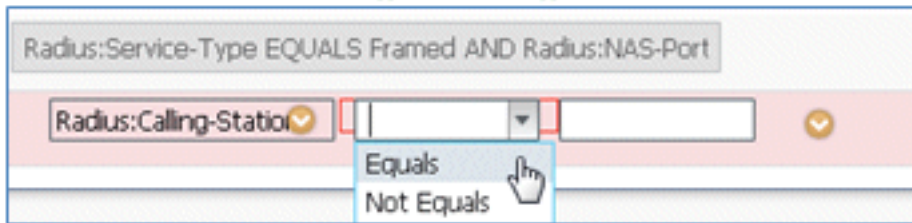


82. Wählen Sie **Calling-Station-ID-[31]**.

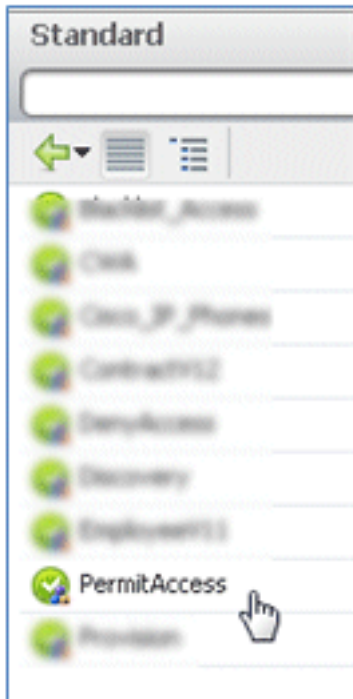


83. Wählen Sie **Gleich**.

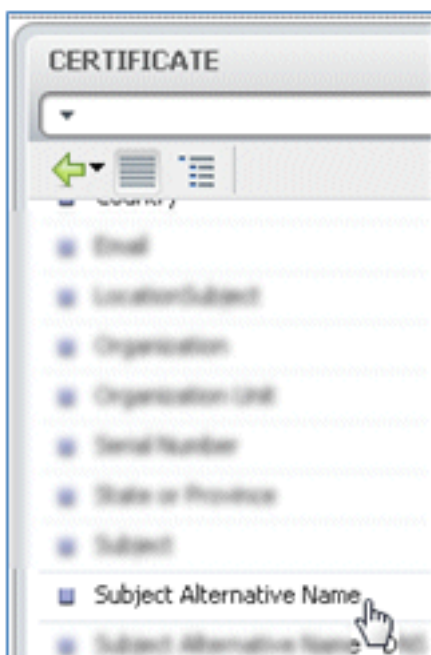




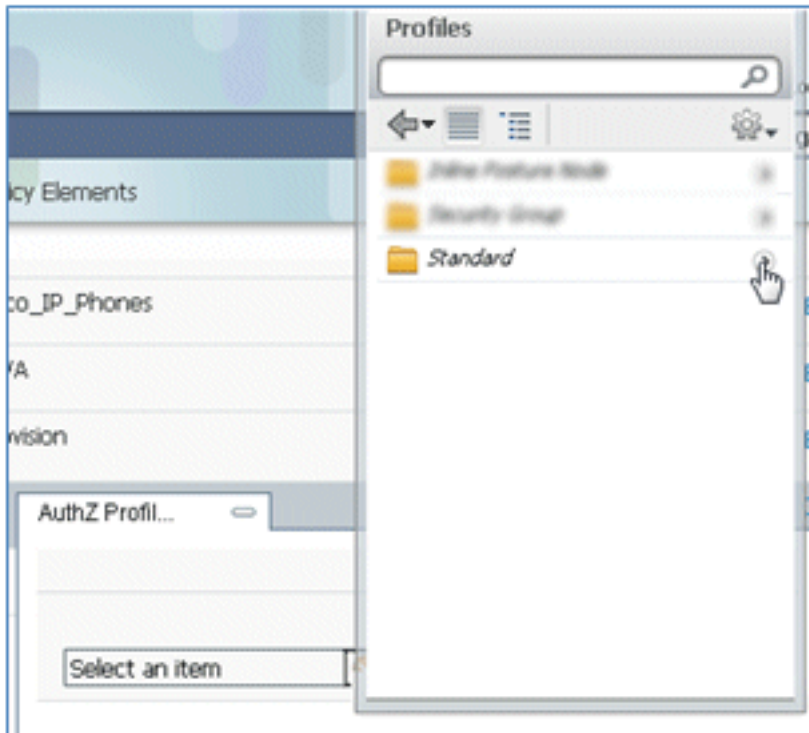
84. Gehen Sie zu **ZERTIFIKAT**, und klicken Sie auf den Pfeil nach rechts.



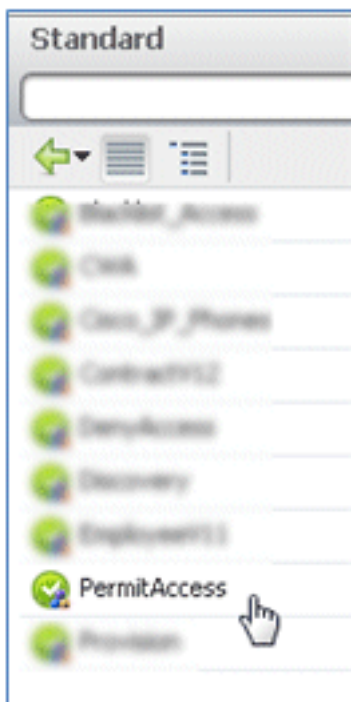
85. Wählen Sie **einen alternativen Antragstellernamen** aus.



86. Wählen Sie als AuthZ-Profil die Option **Standard** aus.



87. Wählen Sie **Zugriff zulassen** aus.



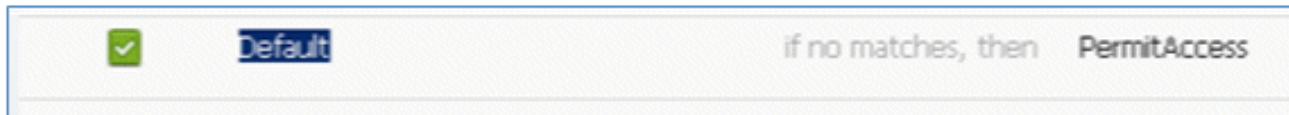
88. Klicken Sie auf **Fertig**.



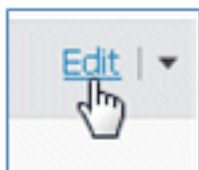
Dies ist ein Beispiel für die Regel:

<input checked="" type="checkbox"/>	OpenCWA	Wireless_M40	then: DENY
<input checked="" type="checkbox"/>	PerfHub	Wireless_802.1X (1): Network Access:AuthenticationMethod EQUALS RADIUS(2)	then: Permit
<input checked="" type="checkbox"/>	AllowRule	Wireless_802.1X Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name	then: PermitAccess

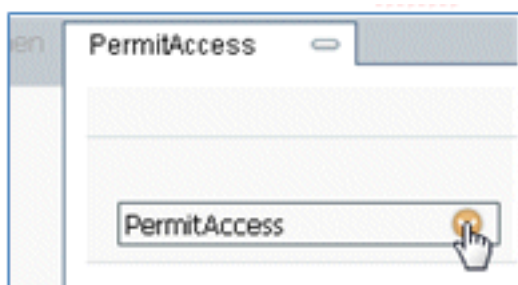
89. Suchen Sie die Standardregel, um PermitAccess in DenyAccess zu ändern.



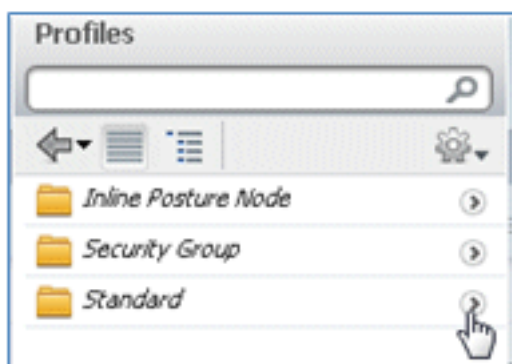
90. Klicken Sie auf **Bearbeiten**, um die Standardregel zu bearbeiten.



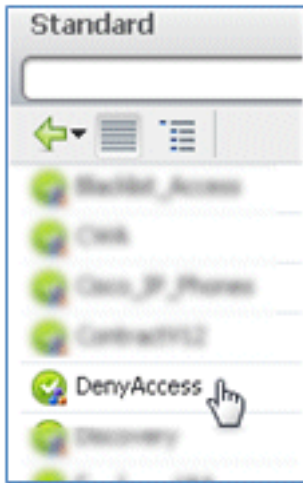
91. Wechseln Sie zum vorhandenen AuthZ-Profil von PermitAccess.



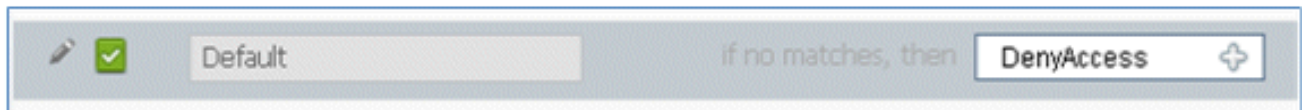
92. Wählen Sie **Standard** aus.



93. Wählen Sie **Zugriff verweigern** aus.



94. Vergewissern Sie sich, dass die Standardregel 'DenyAccess' enthält, wenn keine Übereinstimmungen gefunden werden.



95. Klicken Sie auf **Fertig**.



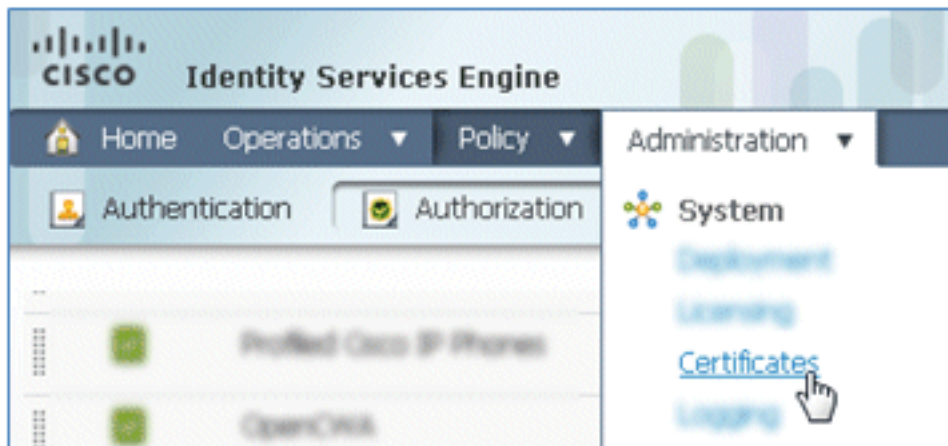
Dies ist ein Beispiel für die wichtigsten Regeln, die für diesen Test erforderlich sind. Sie gelten entweder für ein Einzel-SSID- oder ein Dual-SSID-Szenario.

<input checked="" type="checkbox"/>	OpenCWA	if Wireless_MAB	then CWA
<input checked="" type="checkbox"/>	PEAPrule	if (Wireless_802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 )	then Provision
<input checked="" type="checkbox"/>	AllowRule	if (Wireless_802.1X AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name )	then PermitAccess
<input checked="" type="checkbox"/>	Default	if no matches, then	DenyAccess

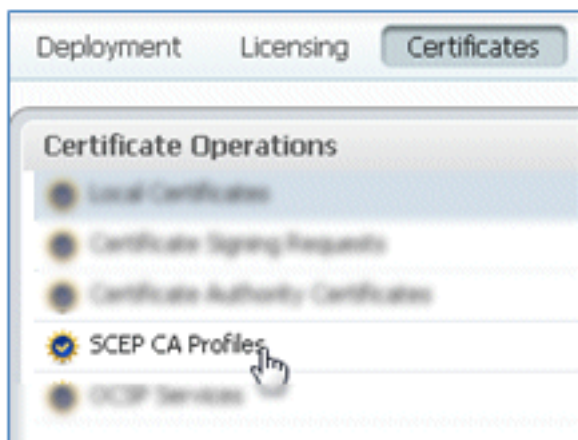
96. Klicken Sie auf **Speichern**.



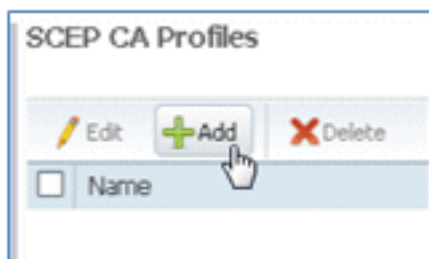
97. Navigieren Sie zu **ISE > Administration > System > Certificates**, um den ISE-Server mit einem SCEP-Profil zu konfigurieren.



98. Klicken Sie in Certificate Operations (Zertifikatvorgänge) auf **SCEP CA Profiles** (SCEP-Zertifizierungsstellenprofile).



99. Klicken Sie auf **Hinzufügen**.



100. Geben Sie folgende Werte für dieses Profil ein:

Name: **mySCEP** (in diesem Beispiel) URL: **https://<ca-server>/CertSrv/mscep/** (Die richtige Adresse finden Sie in der Konfiguration des Zertifizierungsstellen-Servers.)



SEP Certificate Authority Certificates > New SCEP Profile

Edit Certificate

SEP Certificate Authority

\* Name

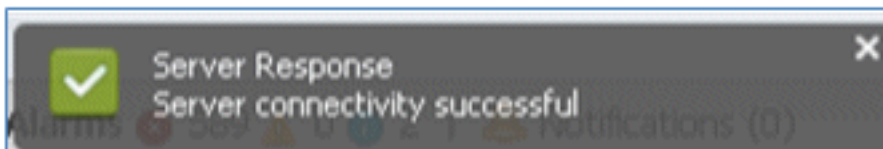
Description

\* URL

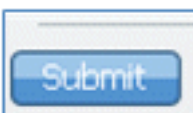
101. Klicken Sie auf **Verbindung testen**, um die Verbindung der SCEP-Verbindung zu testen.



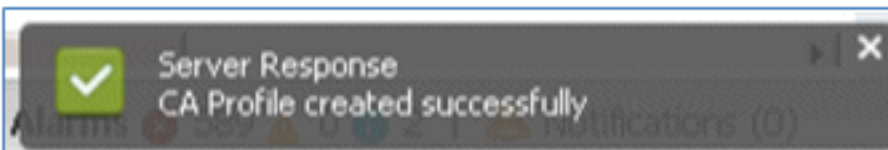
102. Diese Antwort zeigt, dass die Serververbindung erfolgreich ist.



103. Klicken Sie auf **Senden**.



104. Der Server antwortet, dass das CA-Profil erfolgreich erstellt wurde.



105. Bestätigen Sie, dass das SCEP-CA-Profil hinzugefügt wurde.

SCEP CA Profiles

Edit +Add X>Delete Show All

<input type="checkbox"/>	Name	Description	URL	CA Cert Name
<input type="checkbox"/>	MySCEP		https://10.10.10.10/certsrv/mscep	RFDemo-MSCE

## Benutzerfreundlichkeit - Bereitstellung von iOS

### Duale SSID

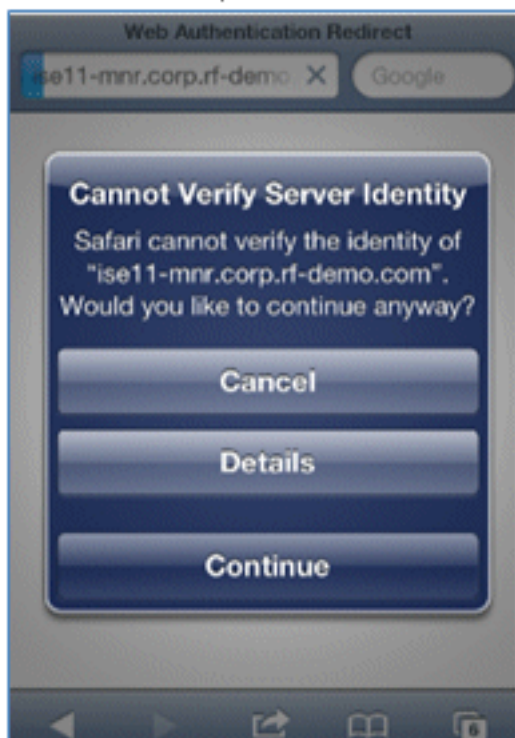
In diesem Abschnitt wird die duale SSID behandelt. Außerdem wird beschrieben, wie Sie eine Verbindung mit dem bereitzustellenden Gast und mit einem 802.1x-WLAN herstellen.

Gehen Sie wie folgt vor, um iOS im Szenario mit zwei SSIDs bereitzustellen:

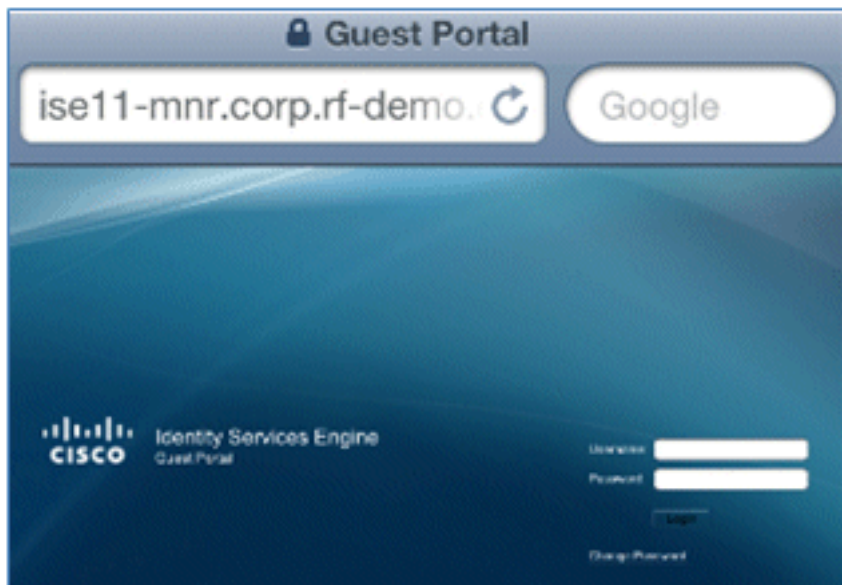
1. Wechseln Sie auf dem iOS-Gerät zu **Wi-Fi Networks**, und wählen Sie **DemoCWA** (konfiguriert als offenes WLAN auf dem WLC) aus.



2. Öffnen Sie den Safari-Browser auf dem iOS-Gerät, und rufen Sie eine erreichbare URL auf (z. B. einen internen/externen Webserver). Die ISE leitet Sie zum Portal weiter. Klicken Sie auf **Continue** (Weiter).



3. Sie werden zur Anmeldung zum Gastportal weitergeleitet.



4. Melden Sie sich mit einem AD-Benutzerkonto und -Kennwort an. Installieren Sie das Zertifizierungsstellenprofil, wenn Sie dazu aufgefordert werden.



5. Klicken Sie auf Vertrauenswürdiges Zertifikat des Zertifizierungsstellenservers **installieren**.



6. Klicken Sie nach Abschluss der Installation des Profils auf **Fertig**.



7. Kehren Sie zum Browser zurück, und klicken Sie auf **Registrieren**. Notieren Sie sich die Geräte-ID, die die MAC-Adresse des Geräts enthält.



8. Klicken Sie auf **Installieren**, um das verifizierte Profil zu installieren.



9. Klicken Sie auf **Jetzt installieren**.



10. Nach Abschluss des Vorgangs bestätigt das WirelessSP-Profil, dass das Profil installiert ist. Klicken Sie auf **Fertig**.





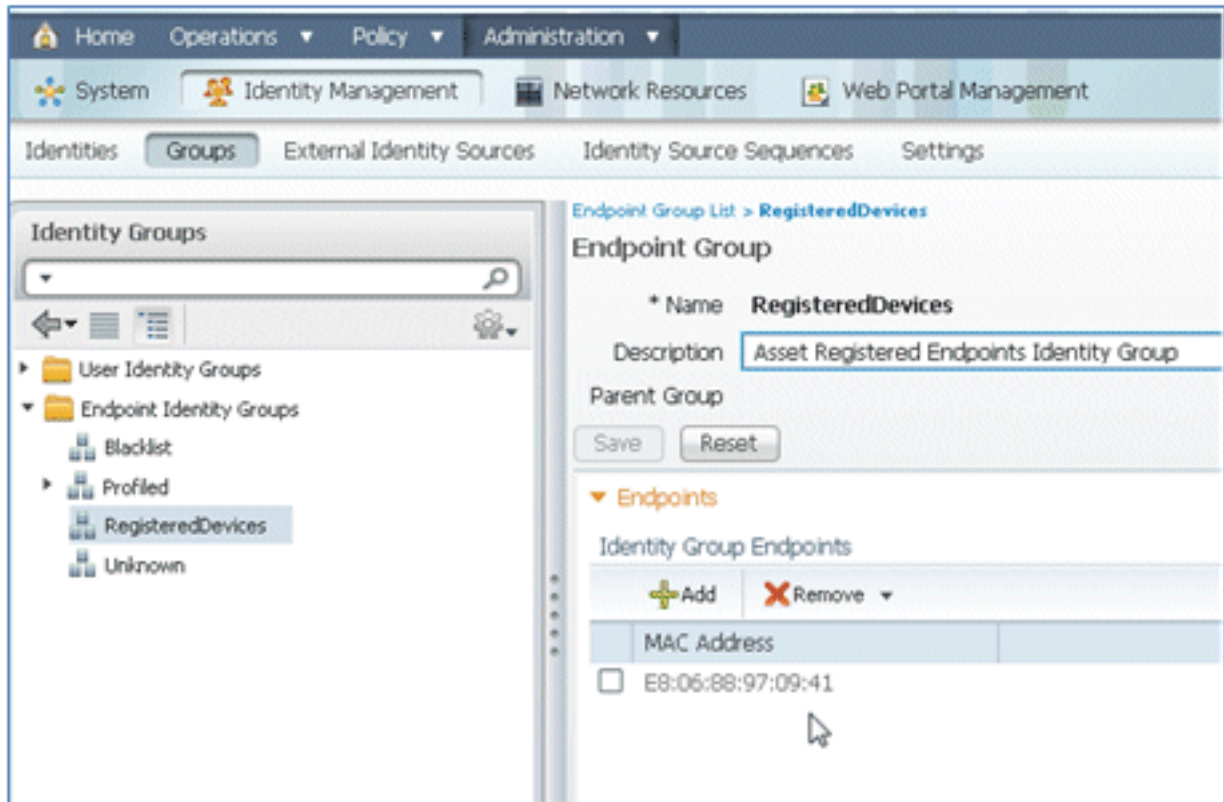
11. Wechseln Sie zu **Wi-Fi Networks**, und ändern Sie das Netzwerk in **Demo1x**. Ihr Gerät ist jetzt verbunden und verwendet TLS.



12. Navigieren Sie auf der ISE zu **Operationen > Authentifizierungen**. Die Ereignisse zeigen den Prozess, bei dem das Gerät mit dem offenen Gastnetzwerk verbunden ist, den Registrierungsprozess mit der Komponentenbereitstellung durchläuft und nach der Registrierung der Zugriff erlaubt wird.

Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25, 12 12:27:57.052 AM	✓	🔒	paul	EE-06-80-97-09-41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25, 12 12:27:21.714 AM	✓	🔒	EE-06-80-97-09-41	EE-06-80-97-09-41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25, 12 12:27:20.438 AM	✓	🔒			WLC				Dynamic Authorization succeeded
Mar 25, 12 12:26:56.187 AM	✓	🔒	paul	EE-06-80-97-09-41	WLC	CWA	Any,Profiled Apple-Ipad	Pending	

13. Navigieren Sie zu ISE > Administration > Identity Management > **Groups** > **Endpoint Identity Groups** > **RegisteredDevices** (ISE > Verwaltung der Identität > Gruppen > **Endpunkt-Identitätsgruppen**). Die MAC-Adresse wurde der Datenbank hinzugefügt.

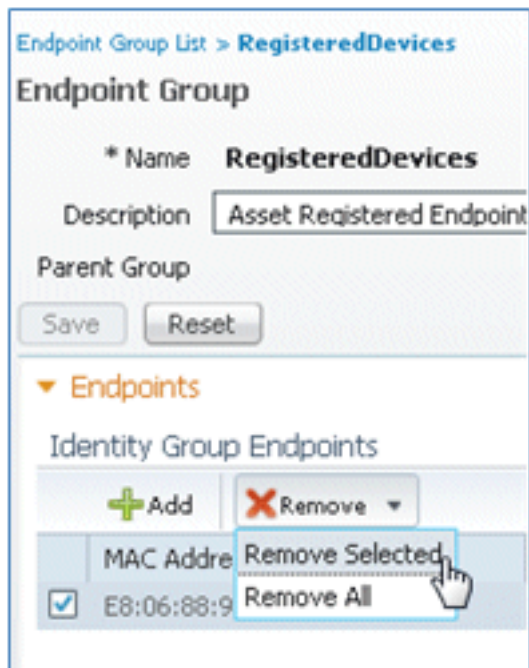


## Eine SSID

In diesem Abschnitt wird eine einzelne SSID behandelt. Es wird beschrieben, wie eine direkte Verbindung mit einem 802.1x-WLAN hergestellt wird, wie ein AD-Benutzername/Kennwort für die PEAP-Authentifizierung bereitgestellt wird, wie ein Gastkonto bereitgestellt wird und wie die Verbindung mit TLS wiederhergestellt wird.

Gehen Sie wie folgt vor, um iOS im Szenario mit einer einzigen SSID bereitzustellen:

1. Wenn Sie dasselbe iOS-Gerät verwenden, entfernen Sie den Endpunkt aus den registrierten Geräten.



2. Navigieren Sie auf dem iOS-Gerät zu **Einstellungen > Allgemein > Profile**. Entfernen Sie die in diesem Beispiel installierten Profile.



3. Klicken Sie auf **Entfernen**, um die vorherigen Profile zu entfernen.



4. Stellen Sie mit dem vorhandenen (gelöschten) Gerät oder einem neuen iOS-Gerät eine direkte Verbindung mit dem 802.1x-Gerät her.
5. Stellen Sie eine Verbindung mit **Dot1x** her, geben Sie einen Benutzernamen und ein Kennwort ein, und klicken Sie auf **Beitreten**.



- Wiederholen Sie die Schritte 90 und höher im Abschnitt zur [ISE-Konfiguration](#), bis die entsprechenden Profile vollständig installiert sind.
- Navigieren Sie zu **ISE > Operations > Authentications**, um den Prozess zu überwachen. Dieses Beispiel zeigt den Client, der bei der Bereitstellung direkt mit dem 802.1X-WLAN verbunden ist. Unter Verwendung von TLS wird die Verbindung getrennt und erneut mit dem gleichen WLAN verbunden.

Live Authentications									
Add or Remove Columns		Refresh		Refresh			Show		
Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25, 12 12:40:03.593 AM	✔		paul	EB-06-88-97-09-41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25, 12 12:39:53.353 AM	✔		EB-06-88-97-09-41	EB-06-88-97-09-41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25, 12 12:39:08.867 AM	✔		paul	EB-06-88-97-09-41	WLC	Provision	RegisteredDevices	Pending	Authentication succeeded

- Navigieren Sie zu **WLC > Monitor > [Client MAC]**. Beachten Sie im Clientdetail, dass sich der Client im Status "RUN" befindet, dass Data Switching auf "local" festgelegt ist und dass Authentication is Central. Dies gilt für Clients, die eine Verbindung mit dem FlexConnect AP herstellen.

Live Authentications									
Add or Remove Columns		Refresh		Refresh			Show		
Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25, 12 12:40:03.593 AM	✔		paul	EB-06-88-97-09-41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25, 12 12:39:53.353 AM	✔		EB-06-88-97-09-41	EB-06-88-97-09-41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25, 12 12:39:08.867 AM	✔		paul	EB-06-88-97-09-41	WLC	Provision	RegisteredDevices	Pending	Authentication succeeded

## Benutzererlebnis - Bereitstellung von Android

### Duale SSID

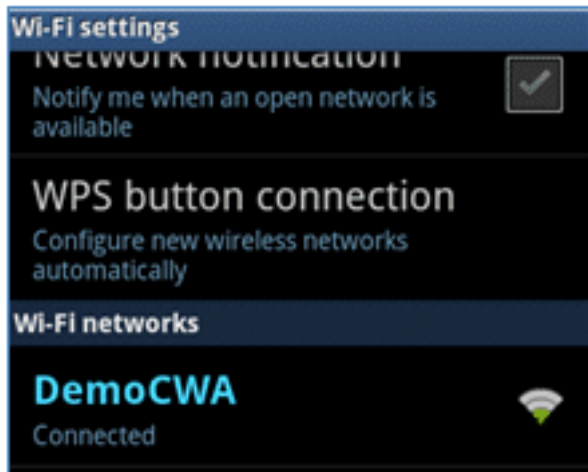
In diesem Abschnitt wird die duale SSID behandelt. Außerdem wird beschrieben, wie Sie eine Verbindung mit dem bereitzustellenden Gast und mit einem 802.1x-WLAN herstellen.

Der Verbindungsvorgang für das Android-Gerät ist dem für ein iOS-Gerät (Single- oder Dual-SSID) sehr ähnlich. Ein wichtiger Unterschied besteht jedoch darin, dass das Android-Gerät Zugriff auf das Internet benötigt, um auf den Google Marketplace (jetzt Google Play) zuzugreifen und den entsprechenden Agenten herunterzuladen zu können.

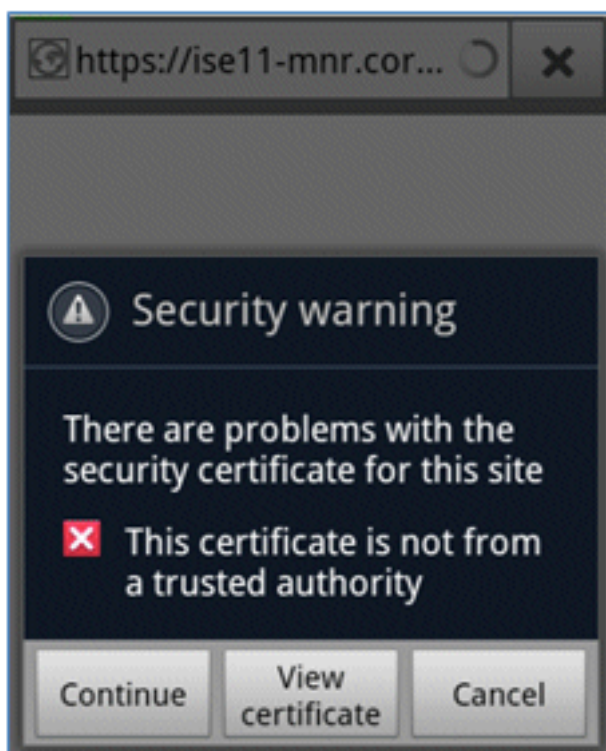
Führen Sie die folgenden Schritte aus, um ein Android-Gerät (wie in diesem Beispiel das Samsung Galaxy) im Dual-SSID-Szenario bereitzustellen:

- Verwenden Sie im Android-Gerät Wi-Fi, um eine Verbindung mit **DemoCWA** herzustellen, und öffnen Sie das Gast-WLAN.

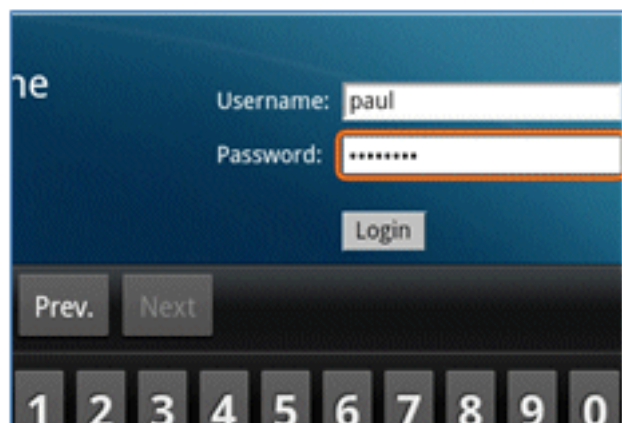




2. Akzeptieren Sie alle Zertifikate, um eine Verbindung zur ISE herzustellen.

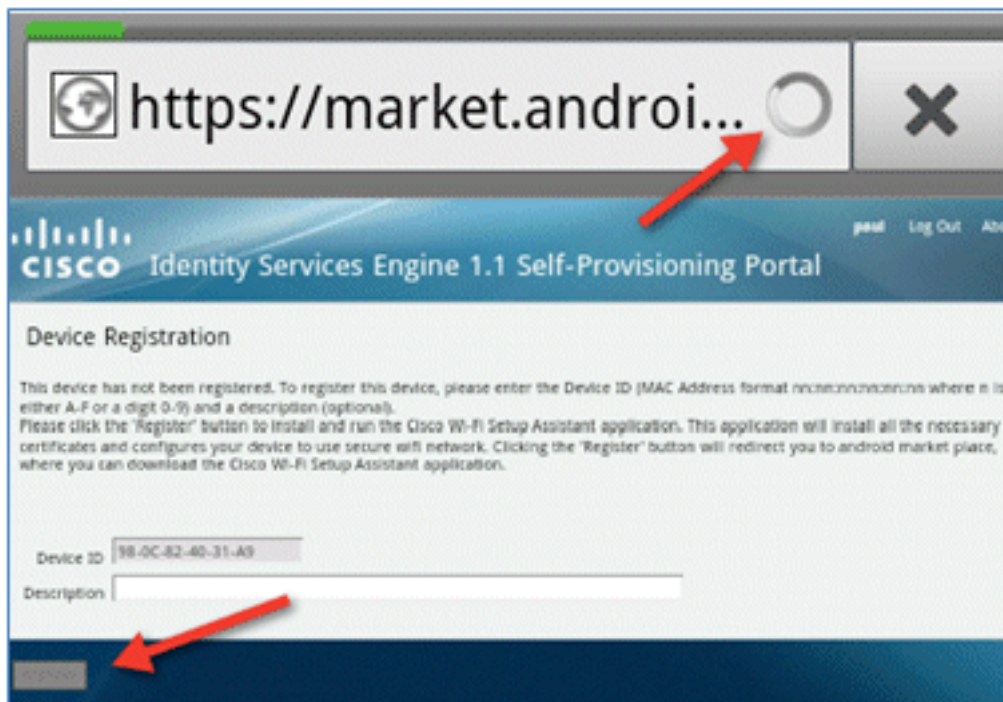


3. Geben Sie im Gastportal einen Benutzernamen und ein Kennwort ein, um sich anzumelden.

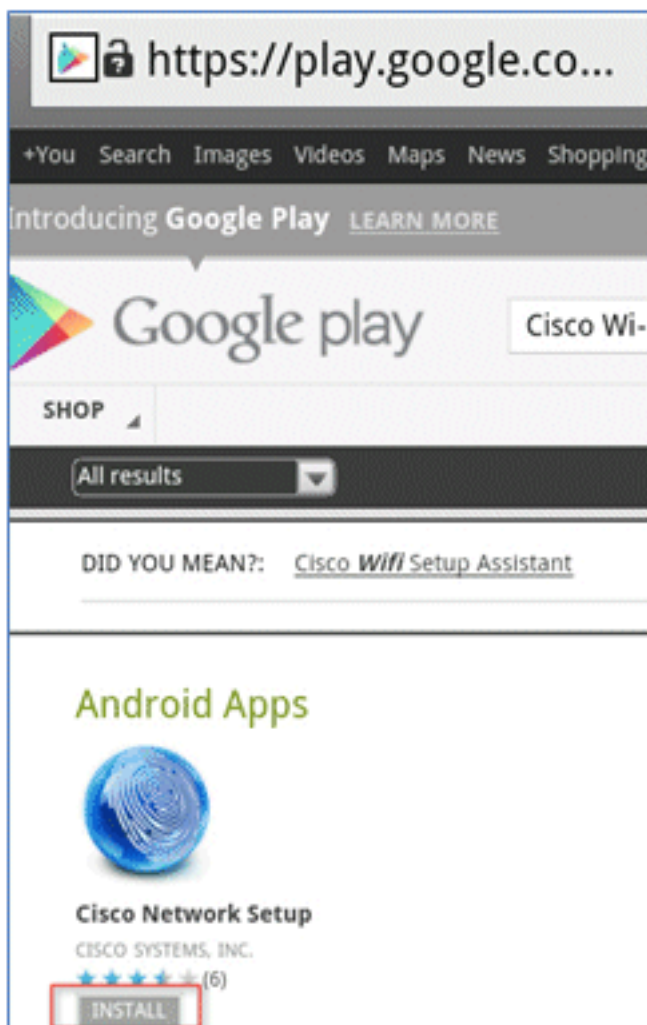


4. Klicken Sie auf **Registrieren**. Das Gerät versucht, das Internet zu erreichen, um auf den

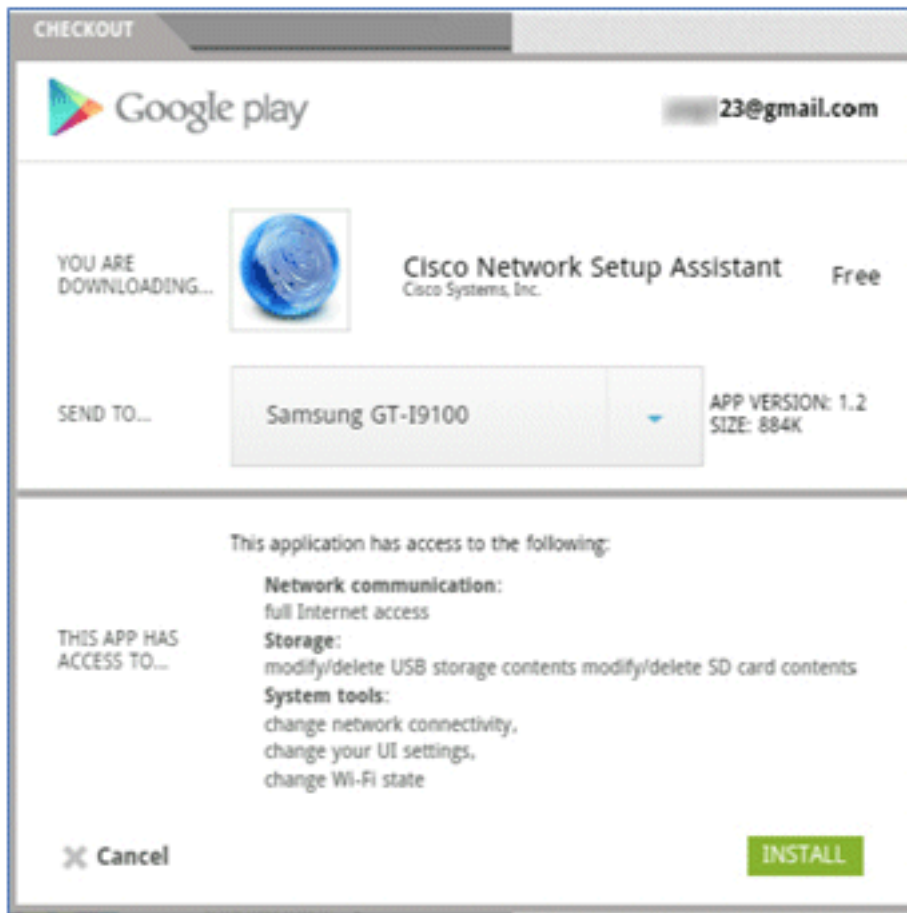
Google Marketplace zuzugreifen. Fügen Sie der Pre-Auth ACL (z. B. ACL-REDIRECT) zusätzliche Regeln im Controller hinzu, um den Zugriff auf das Internet zu ermöglichen.



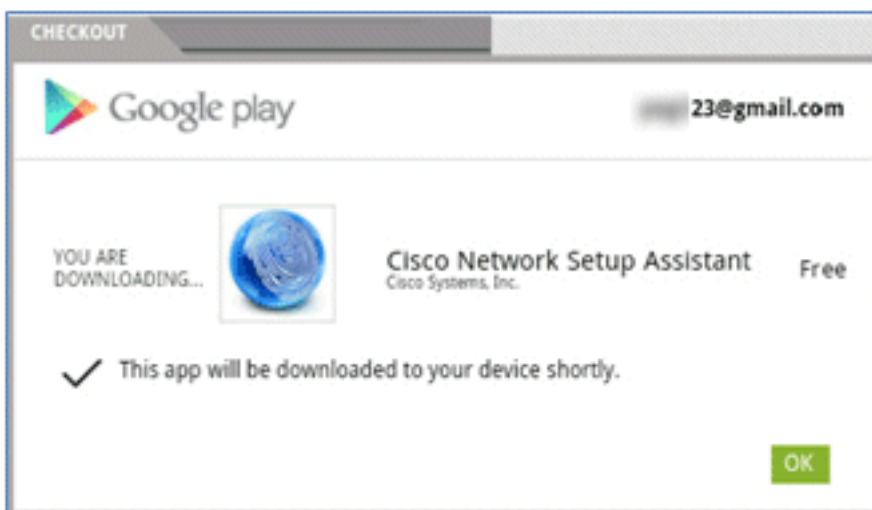
5. Google listet Cisco Network Setup als Android-App auf. Klicken Sie auf **INSTALLIEREN**.



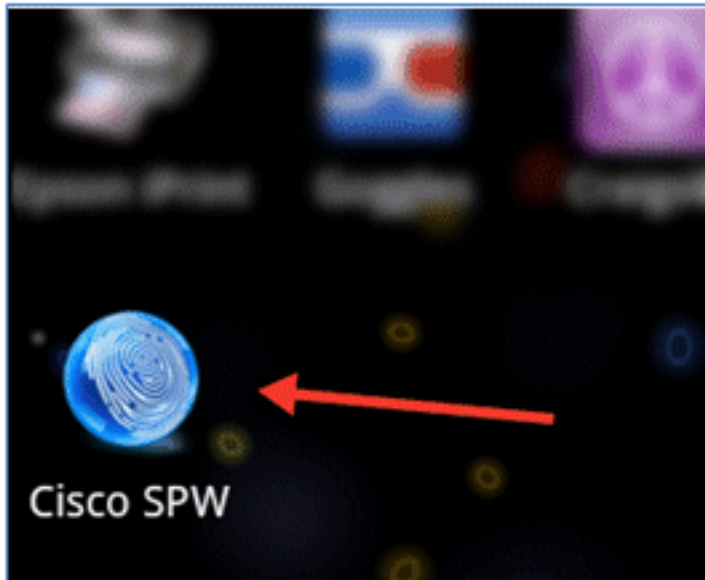
6. Melden Sie sich bei Google an, und klicken Sie auf **INSTALLIEREN**.



7. Klicken Sie auf **OK**.



8. Suchen Sie auf dem Android-Gerät die installierte **Cisco SPW**-App, und öffnen Sie sie.



9. Vergewissern Sie sich, dass Sie immer noch vom Android-Gerät aus beim Gastportal angemeldet sind.

10. Klicken Sie auf **Start**, um den Wi-Fi Setup Assistant zu starten.



11. Cisco SPW beginnt mit der Installation der Zertifikate.

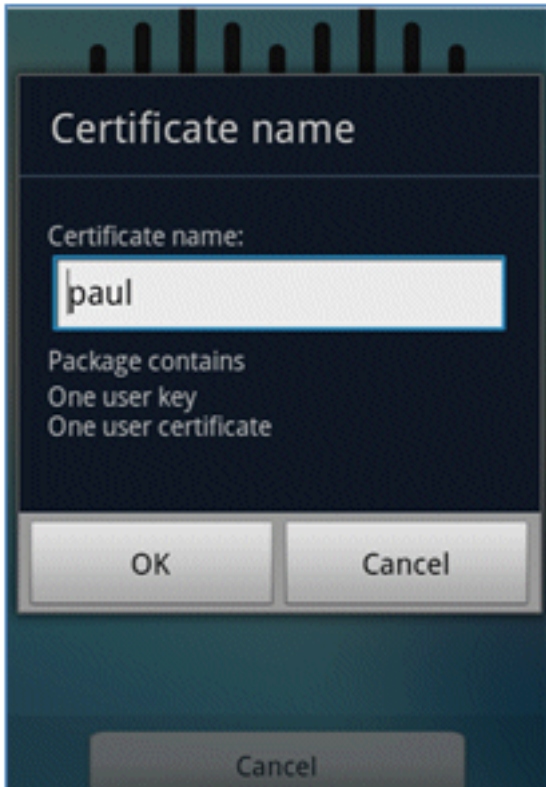


12. Legen Sie bei entsprechender Aufforderung ein Kennwort für die Speicherung der Anmeldeinformationen fest.

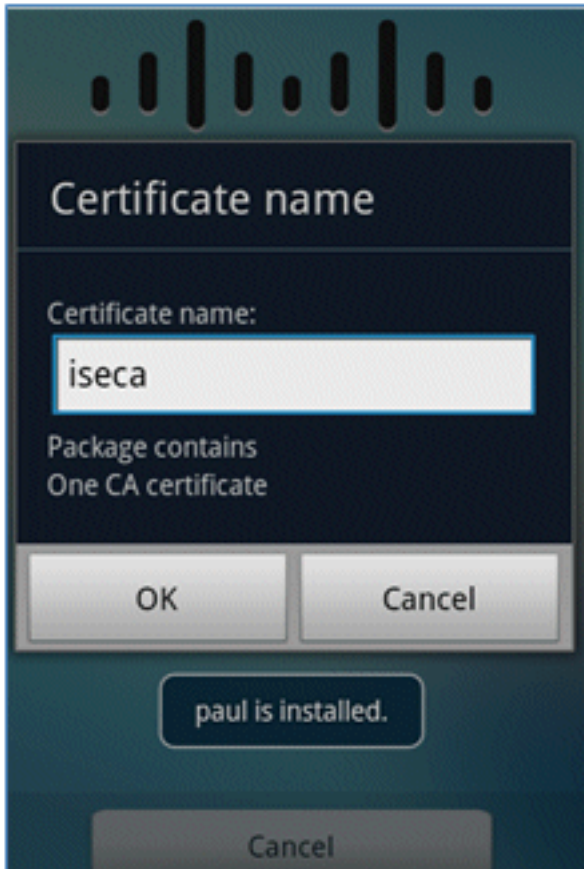


13. Der Cisco SPW gibt einen Zertifikatsnamen zurück, der den Benutzerschlüssel und das Benutzerzertifikat enthält. Klicken Sie zur Bestätigung auf **OK**.

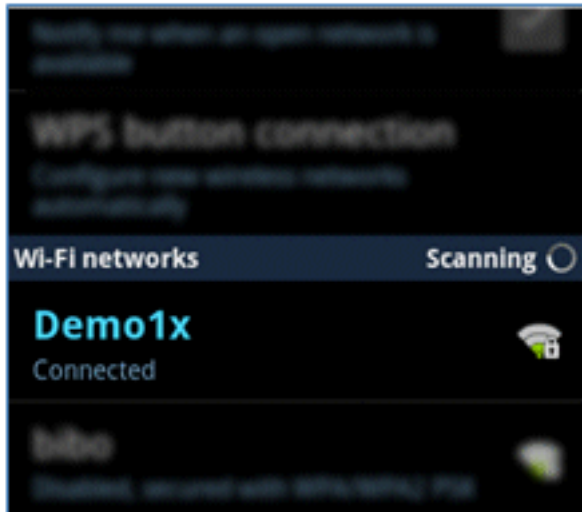




14. Cisco SPW fährt fort und fordert Sie zur Eingabe eines anderen Zertifikatsnamens auf, der das Zertifizierungsstellenzertifikat enthält. Geben Sie den Namen **iseca** ein (in diesem Beispiel), und klicken Sie dann auf **OK**, um fortzufahren.



15. Das Android-Gerät ist jetzt verbunden.

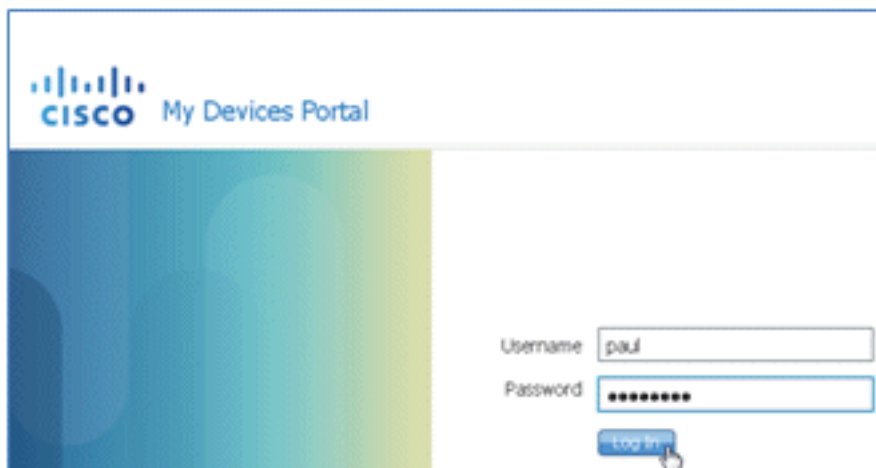


## Geräteportal

Im Geräteportal können Benutzer zuvor registrierte Geräte auf eine Blacklist setzen, wenn ein Gerät verloren geht oder gestohlen wird. Außerdem können sich Benutzer bei Bedarf erneut anmelden.

Gehen Sie wie folgt vor, um ein Gerät auf die Blacklist zu setzen:

1. Um sich beim My Devices Portal anzumelden, öffnen Sie einen Browser, stellen eine Verbindung mit <https://ise-server:8443/mydevices> her (beachten Sie die Portnummer 8443), und melden Sie sich mit einem AD-Konto an.



2. Suchen Sie das Gerät unter Geräte-ID, und klicken Sie auf **Lost?** (Verloren), um die Blacklisting für ein Gerät zu starten.

### Add a New Device

To add a device, please enter the Device ID (MAC Address) and a description (optional); then click submit to add the device.

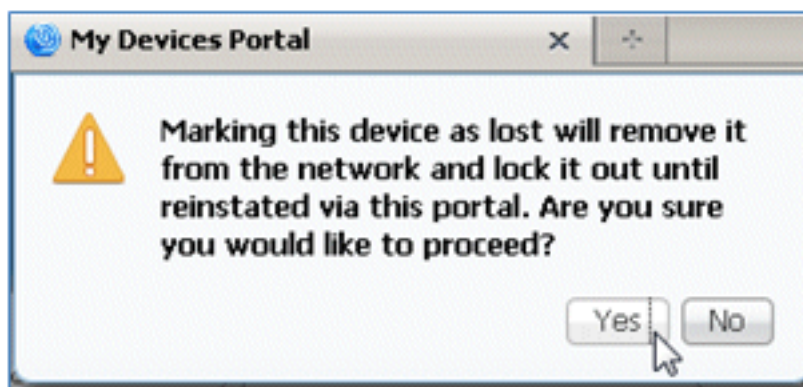
\* Device ID

Description

#### Your Devices

State	Device ID	Description	Action
	EB:06:88:97:09:41		<a href="#">Edit</a>   <a href="#">Log2</a>

3. Wenn die ISE eine Warnmeldung ausgibt, klicken Sie auf **Ja**, um fortzufahren.



4. Die ISE bestätigt, dass das Gerät als **verloren** markiert ist.



5. Jeder Versuch, mit dem zuvor registrierten Gerät eine Verbindung zum Netzwerk herzustellen, wird jetzt blockiert, selbst wenn ein gültiges Zertifikat installiert ist. Dies ist ein Beispiel für ein Gerät auf der Blacklist, das nicht authentifiziert werden kann:

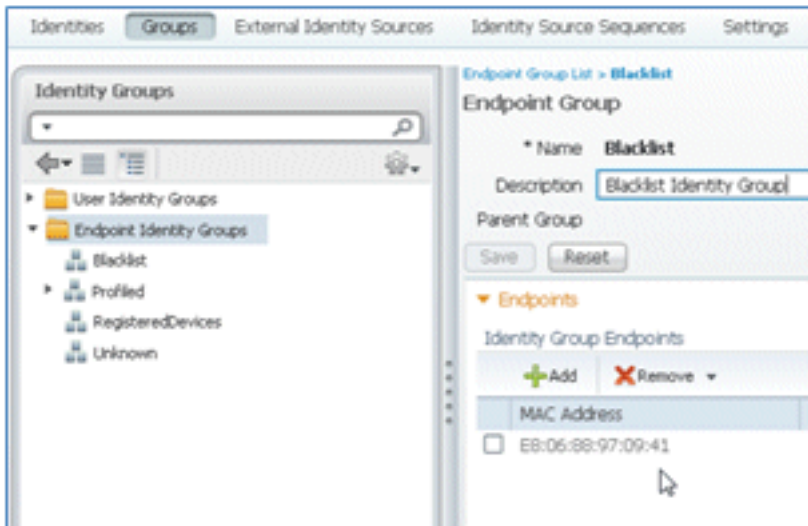
Live Authentications

Refresh: Every 3 seconds | Show: Latest 20 records

Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25, 12:49:07.851 AM			paul	EB:06:88:97:09:41	WLC	Blacklist_Access	Blacklist		Authentication failed
Mar 25, 12:48:59.057 AM			EB:06:88:97:09:41	EB:06:88:97:09:41	WLC	Blacklist_Access	Blacklist		Authentication failed
Mar 25, 12:48:54.137 AM			paul	EB:06:88:97:09:41	WLC	Blacklist_Access	Blacklist		Authentication failed

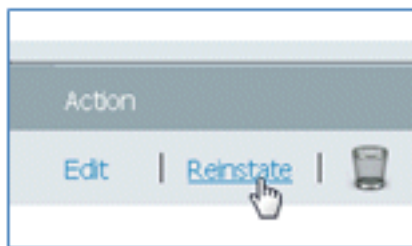
6. Ein Administrator kann zu ISE > Administration > Identity Management > **Groups** navigieren, auf **Endpoint Identity Groups** > Blacklist klicken und sehen, dass das Gerät in die Blacklist

aufgenommen wurde.

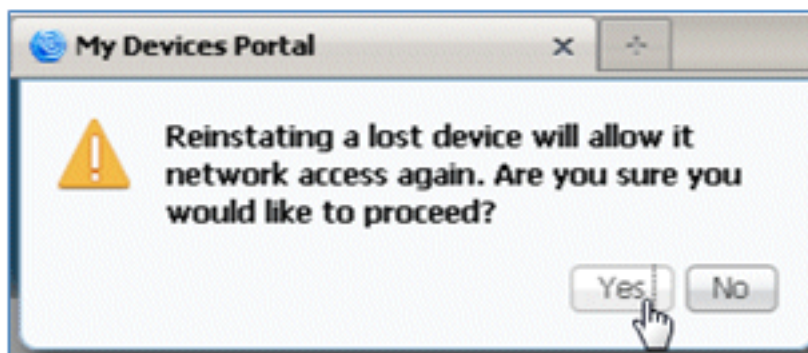


Führen Sie die folgenden Schritte aus, um ein Gerät auf der Blacklist wiederherzustellen:

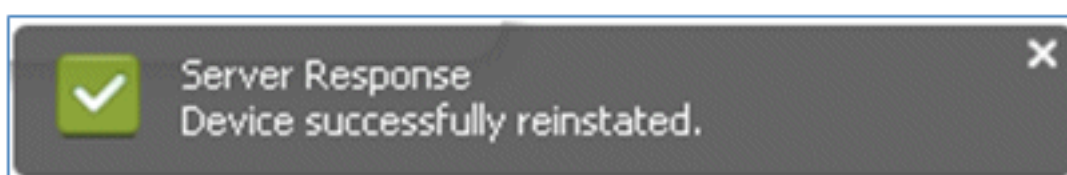
1. Klicken Sie im My Devices-Portal auf für das Gerät **neu starten**.



2. Wenn die ISE eine Warnung ausgibt, klicken Sie auf **Ja**, um fortzufahren.



3. Die ISE bestätigt, dass das Gerät erfolgreich wiederhergestellt wurde. Verbinden Sie das wieder installierte Gerät mit dem Netzwerk, um zu testen, ob das Gerät nun zugelassen wird.

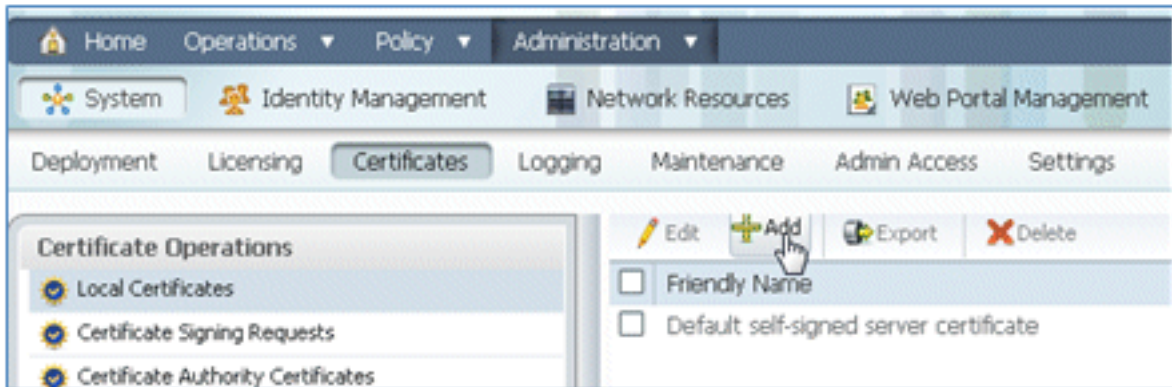


## Referenz - Zertifikate

ISE erfordert nicht nur ein gültiges CA-Stammzertifikat, sondern auch ein gültiges Zertifikat, das von CA signiert wird.

Führen Sie die folgenden Schritte aus, um ein neues vertrauenswürdigen Zertifizierungsstellenzertifikat hinzuzufügen, zu binden und zu importieren:

1. Navigieren Sie zu ISE > Administration > System > **Certificates**, klicken Sie auf **Local Certificates**, und klicken Sie dann auf **Add** (Hinzufügen).



2. Wählen Sie **Zertifikatsignierungsanforderung (CSR) generieren** aus.

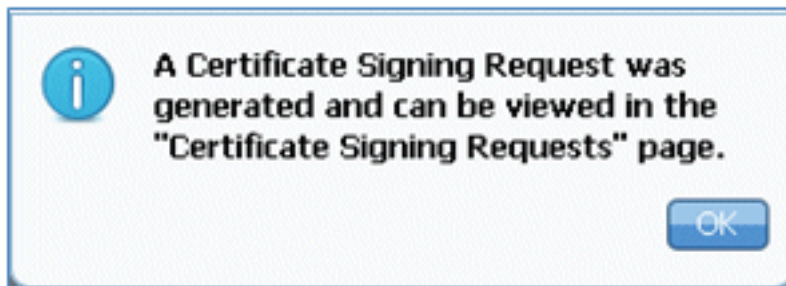


3. Geben Sie den Zertifikatantragsteller **CN=<ISE-SERVER hostname.FQDN>** ein. Für die anderen Felder können Sie die Standardwerte oder die Werte verwenden, die für die CA-Einrichtung erforderlich sind. Klicken Sie auf **Senden**.

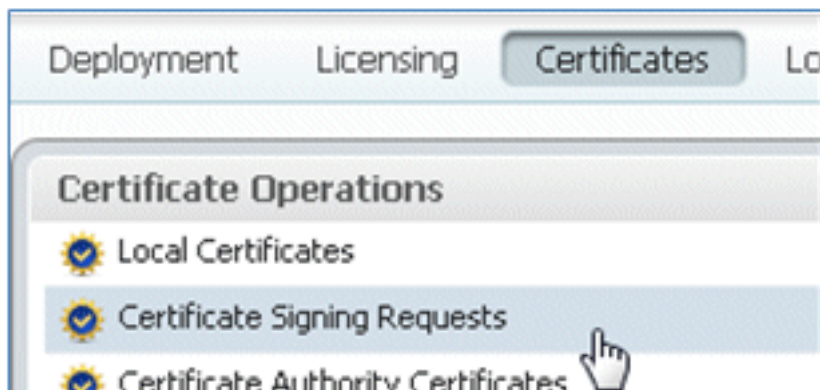


4. Die ISE überprüft, ob der CSR generiert wurde.

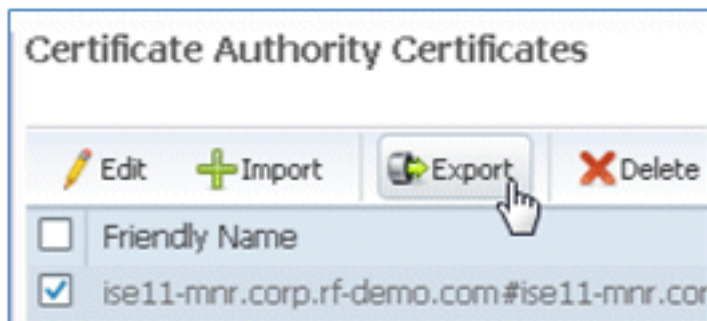




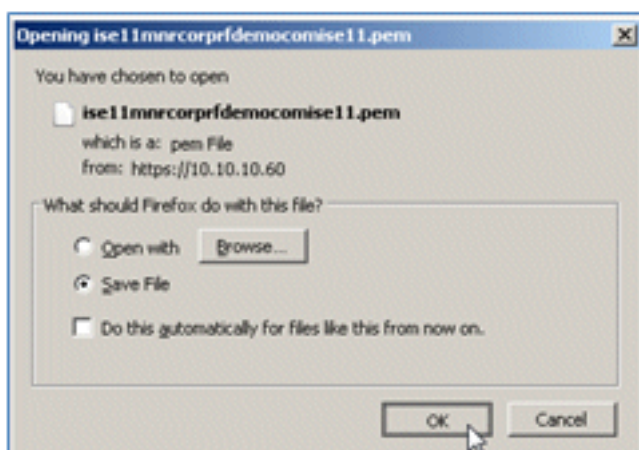
5. Um auf den CSR zuzugreifen, klicken Sie auf die Vorgänge **Zertifikatsignierungsanforderungen**.



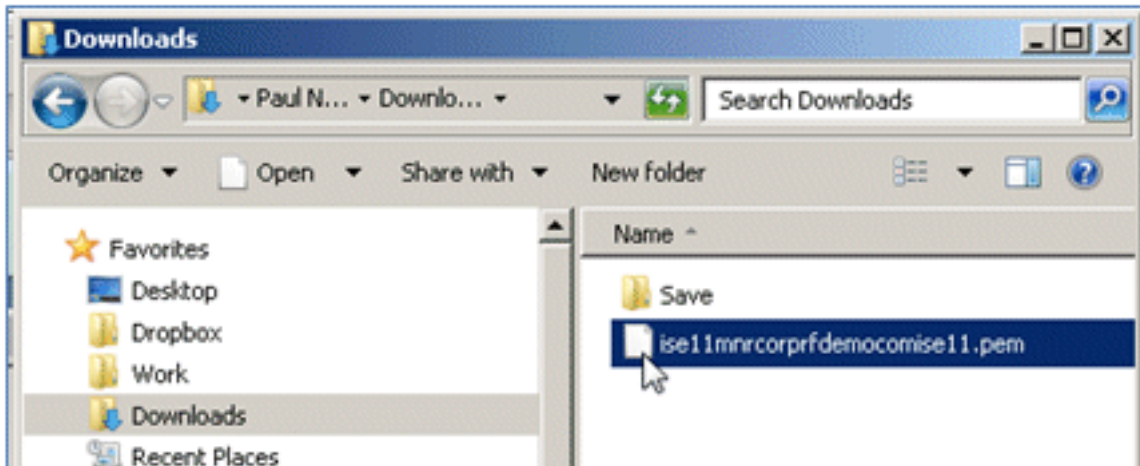
6. Wählen Sie den zuletzt erstellten CSR aus, und klicken Sie dann auf **Exportieren**.



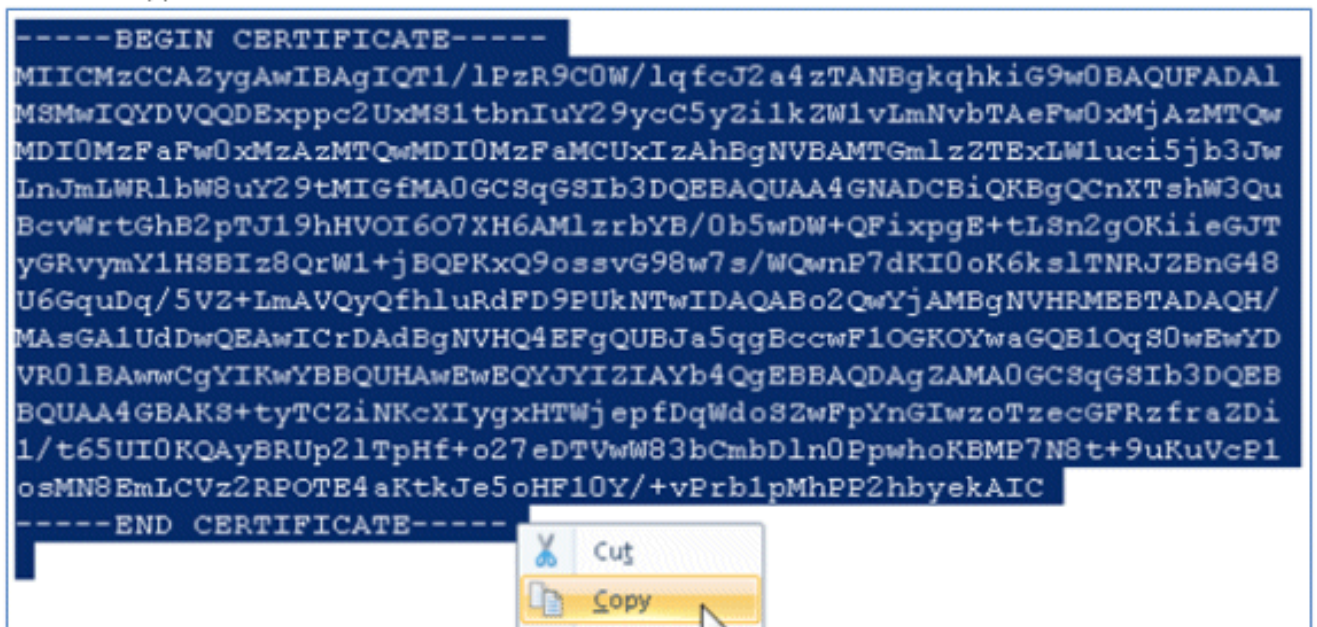
7. Die ISE exportiert den CSR in eine PEM-Datei. Klicken Sie auf **Datei speichern**, und klicken Sie dann auf **OK**, um die Datei auf dem lokalen Computer zu speichern.



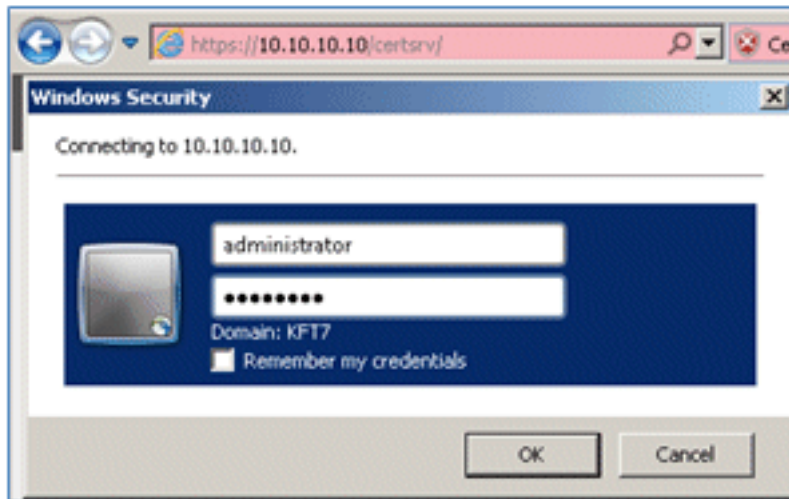
8. Suchen und öffnen Sie die ISE-Zertifikatsdatei mit einem Texteditor.



9. Kopieren Sie den gesamten Inhalt des Zertifikats.



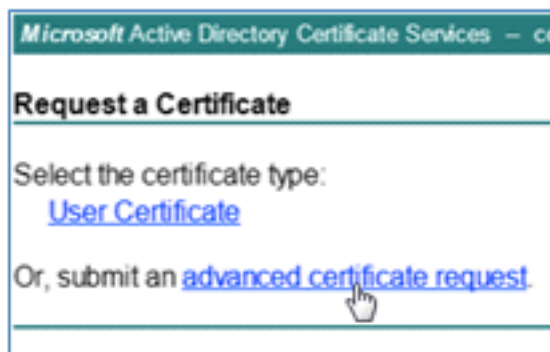
10. Stellen Sie eine Verbindung zum Zertifizierungsstellenserver her, und melden Sie sich mit einem Administratorkonto an. Der Server ist eine Microsoft 2008-Zertifizierungsstelle unter <https://10.10.10.10/certsrv> (in diesem Beispiel).



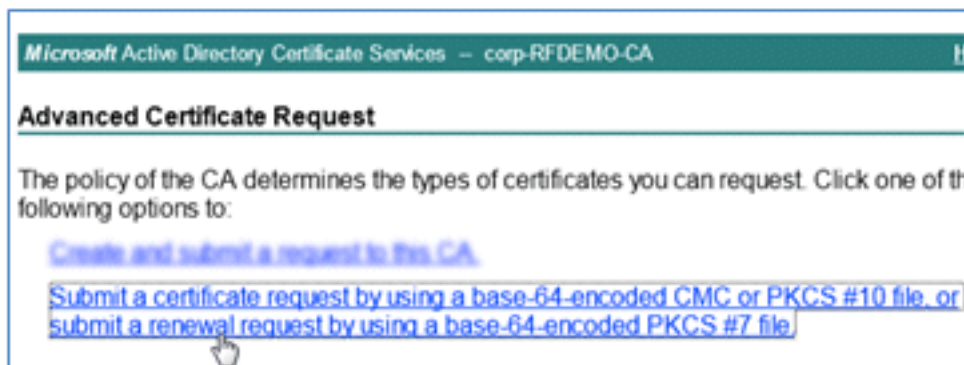
11. Klicken Sie auf **Zertifikat anfordern**.



12. Klicken Sie auf **advanced certificate request** (erweiterte Zertifikatsanforderung).



13. Klicken Sie auf die zweite Option, um eine **Zertifikatsanforderung mithilfe eines Base-64-kodierten CMC zu senden oder ...**.



14. Fügen Sie den Inhalt aus der ISE-Zertifikatsdatei (.pem) in das Feld **Gespeicherte Anforderung** ein, stellen Sie sicher, dass es sich bei der Zertifikatvorlage um **Webserver**

handelt, und klicken Sie auf **Senden**.

The screenshot shows a web browser window with the title "Microsoft Certificate Services -- labsrv.corp.rf-demo.com". The main heading is "Submit a Certificate Request or Renewal Request". Below this, there is a text box for a "Saved Request" containing a long base-64 encoded string. The "Certificate Template" dropdown menu is set to "Web Server". There is an empty "Additional Attributes" text box. A "Submit >" button is located at the bottom right of the form.

15. Klicken Sie auf **Zertifikat herunterladen**.

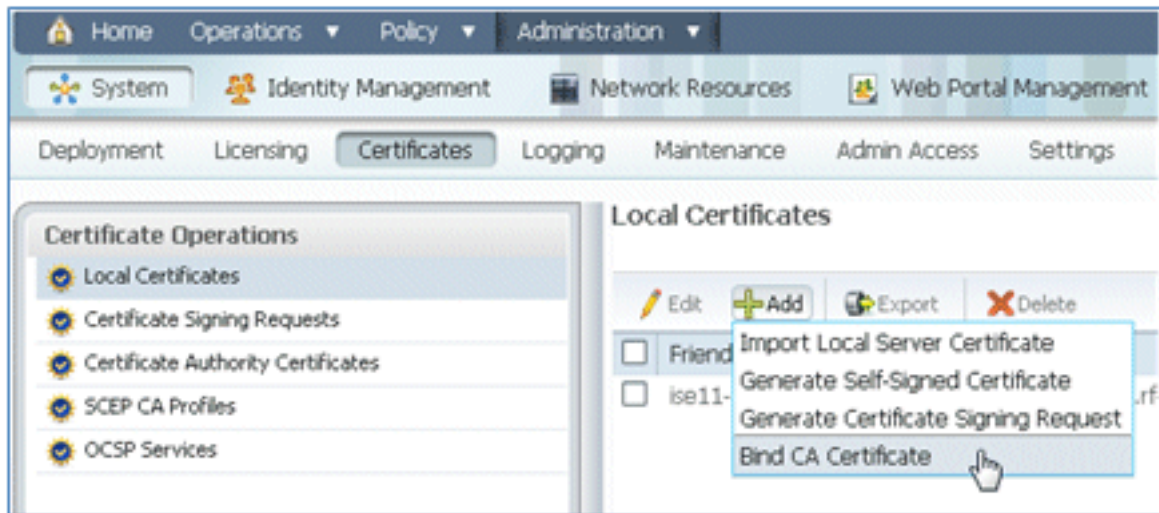
The screenshot shows a web browser window with the title "Microsoft Active Directory Certificate Services -- corp-RFDEMO-CA". The main heading is "Certificate Issued". Below this, there is a message: "The certificate you requested was issued to you." There are two radio buttons: "DER encoded" (selected) and "Base 64 encoded". Below the radio buttons are two blue links: "Download certificate" and "Download certificate chain". A mouse cursor is pointing at the "Download certificate" link.

16. Speichern Sie die Datei certnew.cer. Sie wird später verwendet, um eine Bindung mit der ISE herzustellen.

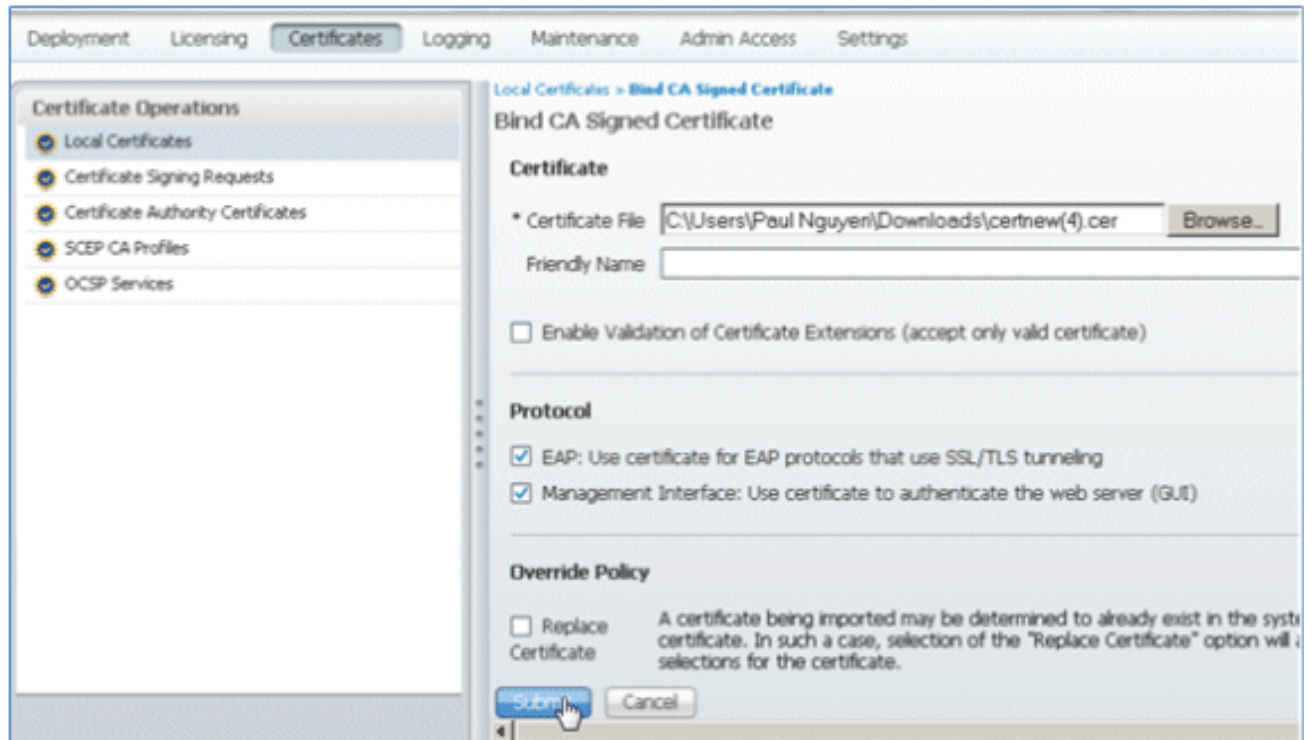
The screenshot shows a file dialog box with the text "Do you want to open or save certnew.cer (921 bytes) from 10.10.10.10?". There are "Open" and "Save" buttons. A mouse cursor is pointing at the "Save" button.

17. Navigieren Sie von ISE-Zertifikaten zu **Lokale Zertifikate**, und klicken Sie auf **Hinzufügen > Zertifizierungsstellenzertifikat binden**.



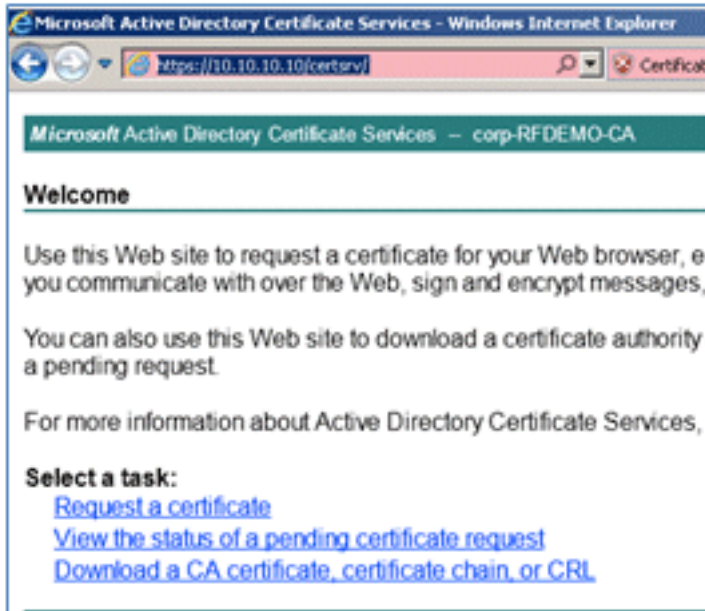


18. Navigieren Sie zu dem Zertifikat, das im vorherigen Schritt auf dem lokalen Computer gespeichert wurde, aktivieren Sie das **EAP-** und das **Management Interface-**Protokoll (Kontrollkästchen sind aktiviert), und klicken Sie auf **Senden**. Der Neustart der Services bei der ISE kann einige Minuten oder länger dauern.



19. Kehren Sie zur Startseite der Zertifizierungsstelle (<https://CA/certsrv/>) zurück, und klicken Sie auf **Zertifizierungsstellenzertifikat**, **Zertifikatskette** oder **Zertifikatsperlliste herunterladen**.





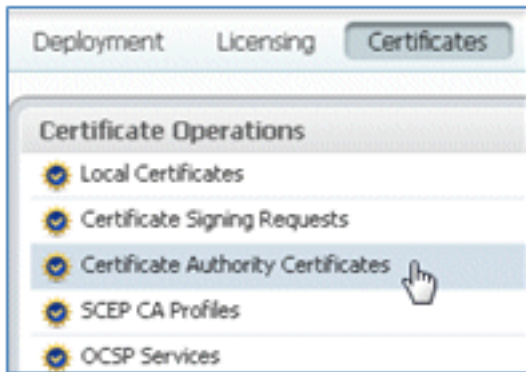
20. Klicken Sie auf **Zertifizierungsstellenzertifikat** herunterladen.



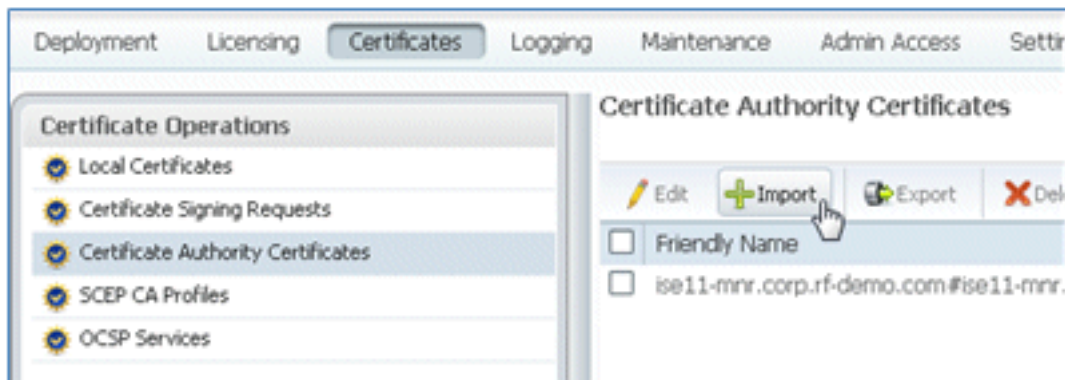
21. **Speichern** Sie die Datei auf dem lokalen Computer.



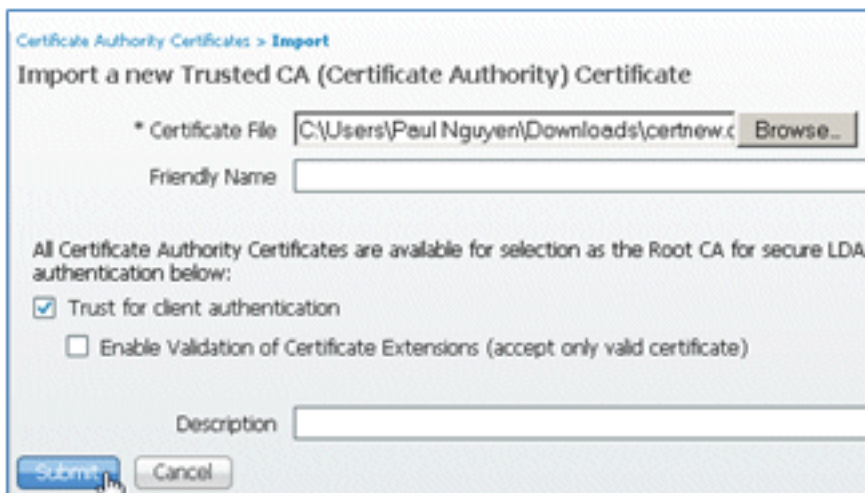
22. Wenn der ISE-Server online ist, gehen Sie zu **Zertifikate**, und klicken Sie auf **Zertifikate der Zertifizierungsstelle**.



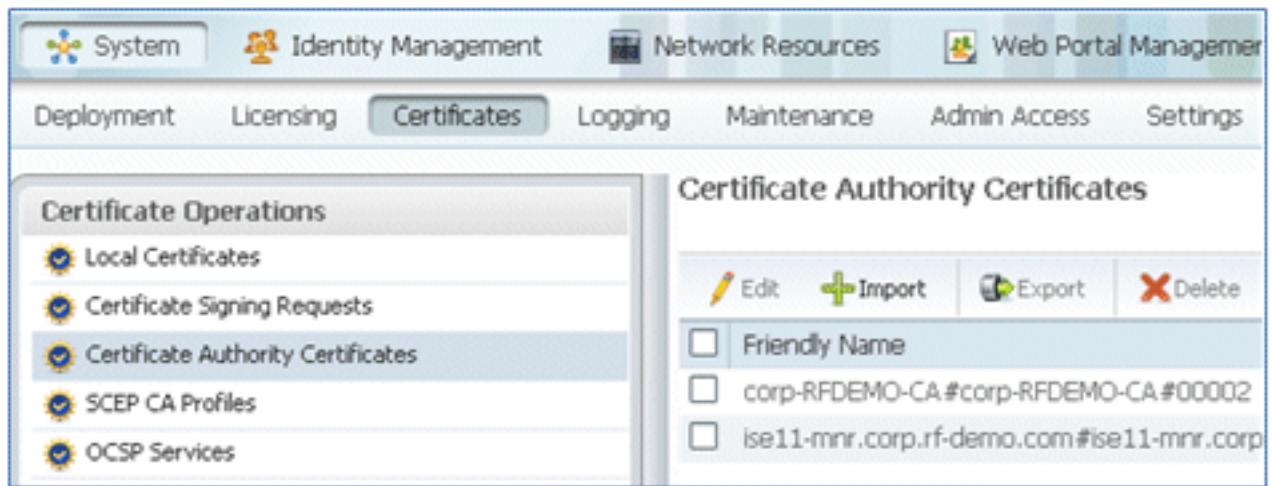
23. Klicken Sie auf **Importieren**.



24. Suchen Sie nach dem Zertifizierungsstellenzertifikat, aktivieren Sie **Vertrauenswürdigkeit für Clientauthentifizierung** (Kontrollkästchen ist aktiviert), und klicken Sie auf **Senden**.



25. Bestätigen Sie, dass das neue vertrauenswürdige Zertifizierungsstellenzertifikat hinzugefügt wird.



## Zugehörige Informationen

- [Cisco Identity Services Engine Hardware Installation Guide, Version 1.0.4](#)
- [Cisco Wireless LAN Controller der Serie 2000](#)
- [Cisco Wireless LAN Controller der Serie 4400](#)
- [Cisco Aironet der Serie 3500](#)
- [Bereitstellungsfaden für Flex 7500 Wireless Branch Controller](#)
- [Bring Your Own Device - Einheitliche Geräteauthentifizierung und konsistenter Zugriff](#)
- [Wireless BYOD mit Identity Services Engine](#)
- [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.