Konfigurationsbeispiel für die dynamische VLAN-Zuordnung mit WLCs auf Basis von ISE zu Active Directory-Gruppen-Zuordnung

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Dynamische VLAN-Zuweisung mit RADIUS-Server
Konfigurieren
Netzwerkdiagramm
Konfigurationen
Integration von ISE zu AD und Konfiguration von Authentifizierungs- und Autorisierungsrichtlinien für Benutzer in der ISE
WLC-Konfiguration zur Unterstützung der 802.1x-Authentifizierung und des AAA-override für die SSID 'office_hq'
Überprüfen
Fehlerbehebung

Einführung

In diesem Dokument wird das Konzept der dynamischen VLAN-Zuweisung vorgestellt. In diesem Dokument wird beschrieben, wie der WLAN-Controller (WLC) und der ISE-Server für die dynamische Zuweisung von WLAN-Clients zu einem bestimmten VLAN konfiguriert werden.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Grundkenntnisse der Wireless LAN Controller (WLCs) und Lightweight Access Points (LAPs)
- über funktionale Kenntnisse eines AAA-Servers (Authentication, Authorization and Accounting) wie Identity Services Engine (ISE) verfügen
- Verfügen Sie über umfassende Kenntnisse der Wireless-Netzwerke und der Wireless-Sicherheit.
- Über funktionale und konfigurierbare Kenntnisse der dynamischen VLAN-Zuweisung verfügen
- Grundlegende Kenntnisse der Microsoft Windows AD-Dienste sowie der Domänen-Controller- und DNS-Konzepte
- Grundkenntnisse der Steuerung und Bereitstellung des Access Point Protocol (CAPWAP)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco WLC der Serie 5520 mit Firmware-Version 8.8.111.0
- Cisco AP der Serie 4800
- Systemeigene Windows-Supplicant und AnyConnect NAM.
- Cisco Secure ISE Version 2.3.0.298
- Microsoft Windows 2016-Server als Domänen-Controller konfiguriert
- Cisco Switch der Serie 3560-CX mit Version 15.2(4)E1

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

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

Dynamische VLAN-Zuweisung mit RADIUS-Server

In den meisten WLAN-Systemen verfügt jedes WLAN über eine statische Richtlinie, die für alle Clients gilt, die einer Service Set Identifier (SSID) oder WLAN in der Controller-Terminologie zugeordnet sind. Diese Methode ist zwar leistungsstark, bietet jedoch Einschränkungen, da Clients verschiedene SSIDs verknüpfen müssen, um unterschiedliche QoS- und Sicherheitsrichtlinien zu erben.

Die Cisco WLAN-Lösung geht diese Einschränkung durch die Unterstützung von Identitätsnetzwerken an. So kann das Netzwerk eine einzelne SSID ankündigen, aber bestimmte Benutzer können basierend auf den Anmeldeinformationen des Benutzers verschiedene QoS-, VLAN-Attribute und/oder Sicherheitsrichtlinien erben.

Die dynamische VLAN-Zuweisung ist eine dieser Funktionen, die einen Wireless-Benutzer anhand der vom Benutzer angegebenen Anmeldeinformationen in ein bestimmtes VLAN versetzt. Diese Aufgabe der Zuweisung von Benutzern zu einem bestimmten VLAN wird von einem RADIUS-Authentifizierungsserver wie der Cisco ISE übernommen. Dies kann beispielsweise verwendet werden, um dem Wireless-Host zu ermöglichen, im selben VLAN zu bleiben, wie er sich innerhalb eines Campus-Netzwerks bewegt.

Der Cisco ISE-Server authentifiziert Wireless-Benutzer anhand einer von mehreren möglichen Datenbanken, zu denen auch die interne Datenbank gehört, z. B.:

- Interne DB
- Active Directory
- Generisches Lightweight Directory Access Protocol (LDAP)
- Open Database Connectivity (ODBC)-konforme relationale Datenbanken

- Rivest, Shamir und Adelman (RSA) SecurID-Token-Server
- RADIUS-kompatible Token-Server

Cisco ISE Authentication Protocols and Supported External Identity Sources listet die verschiedenen Authentifizierungsprotokolle auf, die von internen und externen ISE-Datenbanken unterstützt werden.

Dieses Dokument konzentriert sich auf die Authentifizierung von Wireless-Benutzern, die die externe Windows Active Directory-Datenbank verwenden.

Nach erfolgreicher Authentifizierung ruft die ISE Gruppeninformationen dieses Benutzers aus der Windows-Datenbank ab und ordnet den Benutzer dem entsprechenden Autorisierungsprofil zu.

Wenn ein Client versucht, eine Verbindung zu einer LAP herzustellen, die bei einem Controller registriert ist, übergibt die LAP die Anmeldeinformationen des Benutzers mithilfe der entsprechenden EAP-Methode an den WLC.

WLC sendet diese Anmeldeinformationen mithilfe des RADIUS-Protokolls an die ISE (Kapselung des EAP), und die ISE übergibt die Anmeldeinformationen der Benutzer an AD zur Validierung mithilfe des KERBEROS-Protokolls.

AD validiert die Benutzeranmeldeinformationen und informiert die ISE über die erfolgreiche Authentifizierung.

Nach erfolgreicher Authentifizierung übergibt der ISE-Server bestimmte IETF-Attribute (Internet Engineering Task Force) an den WLC. Diese RADIUS-Attribute legen die VLAN-ID fest, die dem Wireless-Client zugewiesen werden soll. Die SSID (WLAN, WLC) des Clients ist unerheblich, da der Benutzer immer dieser vordefinierten VLAN-ID zugewiesen wird.

Die für die VLAN-ID-Zuweisung verwendeten RADIUS-Benutzerattribute sind:

- IETF 64 (Tunneltyp)—Legen Sie VLAN fest.
- IETF 65 (Tunnel-Medium-Typ)—Legen Sie 802 fest.
- IETF 81 (Tunnel Private Group ID)—Legen Sie diese VLAN-ID fest.

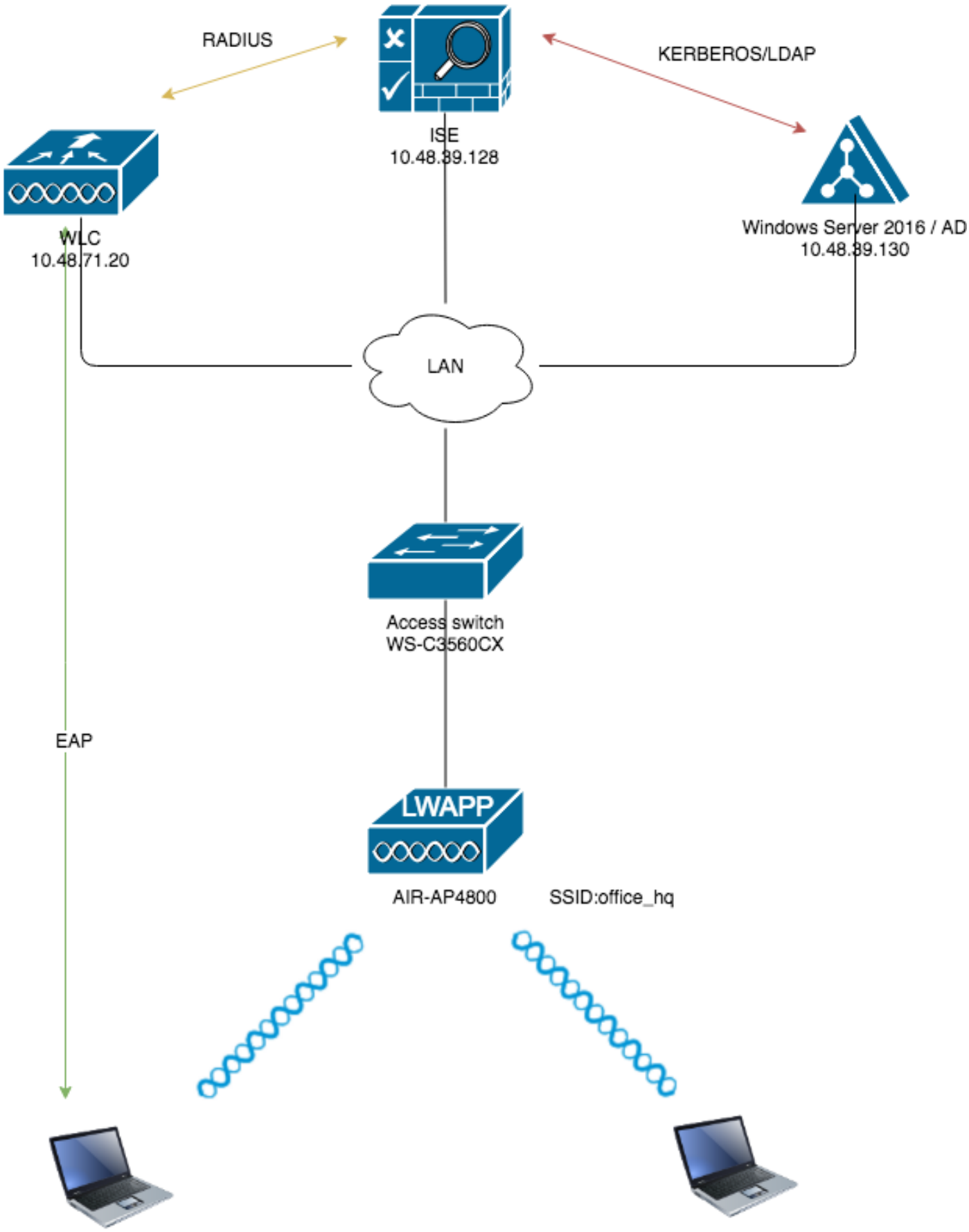
Die VLAN-ID beträgt 12 Bit und hat einen Wert zwischen 1 und 4094 (einschließlich). Da die Tunnel-Private-Group-ID eine Zeichenfolge ist, die in RFC2868 für die Verwendung mit IEEE 802.1X definiert ist, wird der Wert der VLAN-ID-Ganzzahl als Zeichenfolge codiert. Wenn diese Tunnelattribute gesendet werden, muss das Feld Tag ausgefüllt werden.

Wie in RFC 2868, Abschnitt 3.1 erwähnt: Das Tag-Feld ist ein Oktett lang und soll eine Möglichkeit bieten, Attribute in demselben Paket zu gruppieren, die sich auf denselben Tunnel beziehen. Gültige Werte für dieses Feld sind 0x01 bis 0x1F, einschließlich. Wenn das Feld Tag nicht verwendet wird, muss es 0 (0 x 00) sein. Weitere Informationen zu allen RADIUS-Attributen finden Sie unter **RFC 2868**.

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Netzwerkdiagramm



Konfigurationen

Dies sind die Konfigurationsdetails der in diesem Diagramm verwendeten Komponenten:

- Die IP-Adresse des ISE-Servers (RADIUS) lautet 10.48.39.128.

- Die Management- und AP-Manager-Schnittstellenadresse des WLC lautet 10.48.71.20.
- Der DHCP-Server befindet sich im LAN-Netzwerk und wird für die entsprechenden Client-Pools konfiguriert. wird nicht im Diagramm angezeigt.
- In dieser Konfiguration werden VLAN1477 und VLAN1478 verwendet. Benutzer aus der **Marketing-**Abteilung werden für das VLAN1477 konfiguriert, und Benutzer aus der **Personalabteilung** werden so konfiguriert, dass sie vom RADIUS-Server in VLAN1478 platziert werden. wenn beide Benutzer eine Verbindung mit derselben SSID herstellen - **office_hq**.VLAN1477: 168.77.0/24 Gateway: 192.168.77.1 VLAN1478: 168.78.0/24 Gateway: 192.168,78,1
- In diesem Dokument wird 802.1x mit PEAP-mschapv2 als Sicherheitsmechanismus verwendet.Hinweis: Cisco empfiehlt, zur Sicherung des WLAN erweiterte Authentifizierungsmethoden wie EAP-FAST und EAP-TLS-Authentifizierung zu verwenden.

Diese Annahmen werden vor dem Durchführen dieser Konfiguration getroffen:

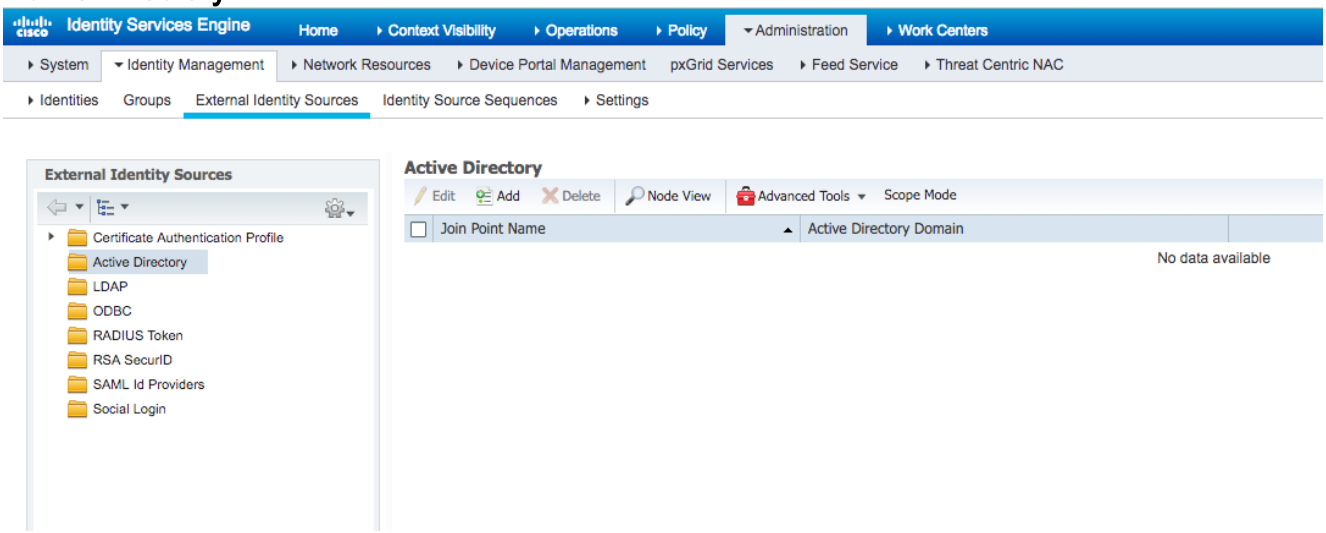
- Die LAP ist bereits beim WLC registriert.
- Die Layer-3-Verbindung besteht zwischen allen Geräten im Netzwerk.
- Im Dokument wird die erforderliche Konfiguration für die Wireless-Seite beschrieben. Es wird davon ausgegangen, dass das kabelgebundene Netzwerk vorhanden ist.
- Die entsprechenden Benutzer und Gruppen werden auf AD konfiguriert.

Um eine dynamische VLAN-Zuweisung mit WLCs auf der Grundlage der Zuordnung von ISE zu AD-Gruppen zu ermöglichen, müssen folgende Schritte ausgeführt werden:

1. Integration von ISE zu AD und Konfiguration von Authentifizierungs- und Autorisierungsrichtlinien für Benutzer in der ISE
2. WLC-Konfiguration zur Unterstützung der 802.1x-Authentifizierung und des AAA-override für die SSID 'office_hq'
3. Endkunden-Supplicant-Konfiguration

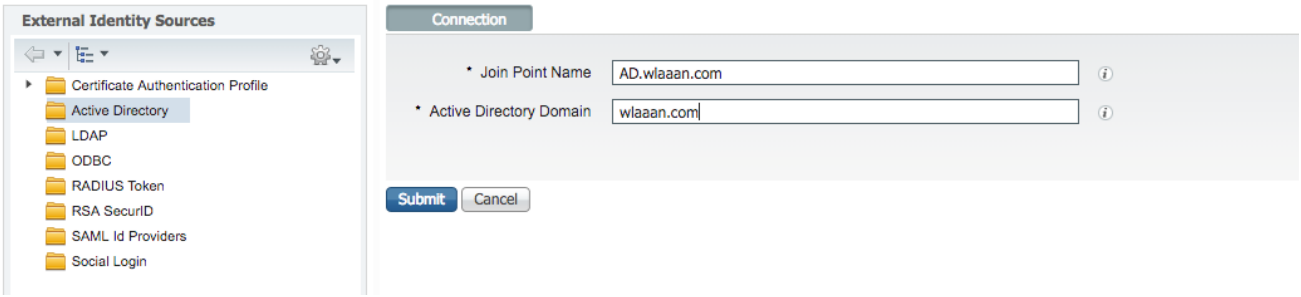
Integration von ISE zu AD und Konfiguration von Authentifizierungs- und Autorisierungsrichtlinien für Benutzer in der ISE

1. Melden Sie sich mit dem **admin-**Konto bei der ISE-Webbenutzeroberfläche an.
2. Navigieren Sie unter "**Administration -> Identity Management -> External Identity Sources -> Active Directory**"

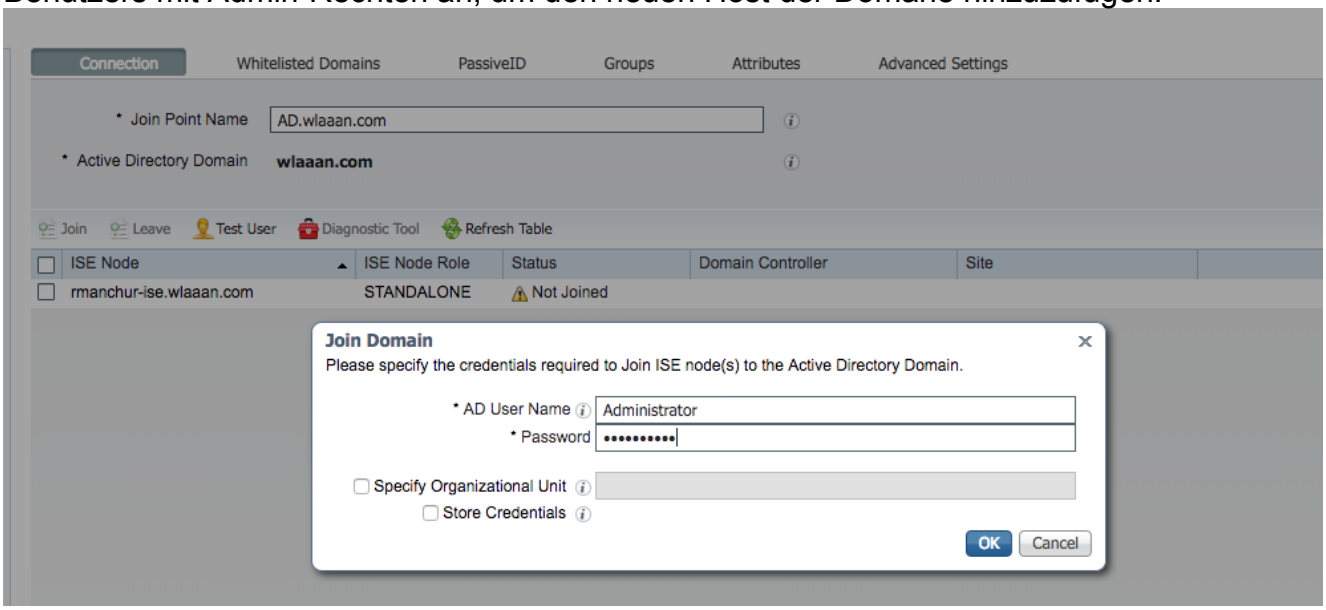


3. Klicken Sie auf **"Hinzufügen",** und geben Sie den Domänennamen und den Namen des Identitätsspeichers in den Active Directory-Join Point Name-Einstellungen ein. Im folgenden

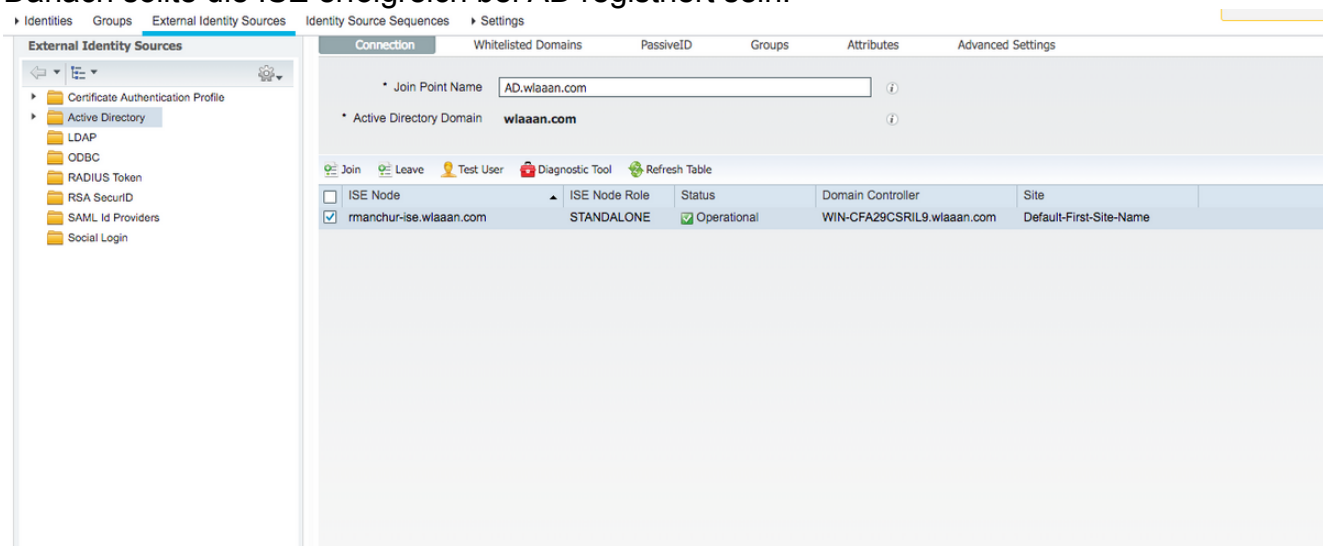
Beispiel registrieren wir die ISE in der Domäne "wlaaan.com", und der Join-Punkt wird als AD.wlaaan.com angegeben - ein lokal bedeutender Name für die ISE.



4. Ein Popup-Fenster wird geöffnet, nachdem die Schaltfläche "**Submit**" (**Senden**) gedrückt wurde und wir gefragt werden, ob wir der ISE sofort zum AD beitreten möchten. Drücken Sie die Taste **"Yes"** (Ja), und geben Sie die Anmeldeinformationen des Active Directory-Benutzers mit Admin-Rechten an, um den neuen Host der Domäne hinzuzufügen.



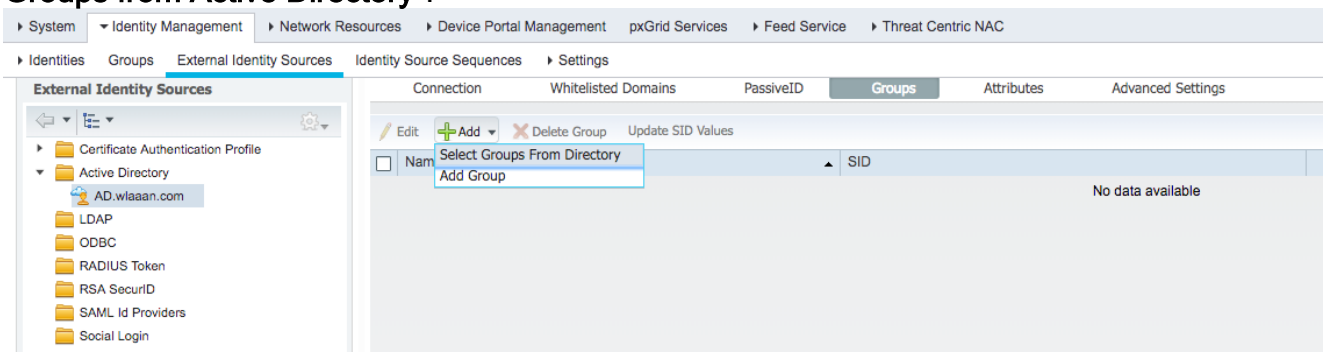
5. Danach sollte die ISE erfolgreich bei AD registriert sein.



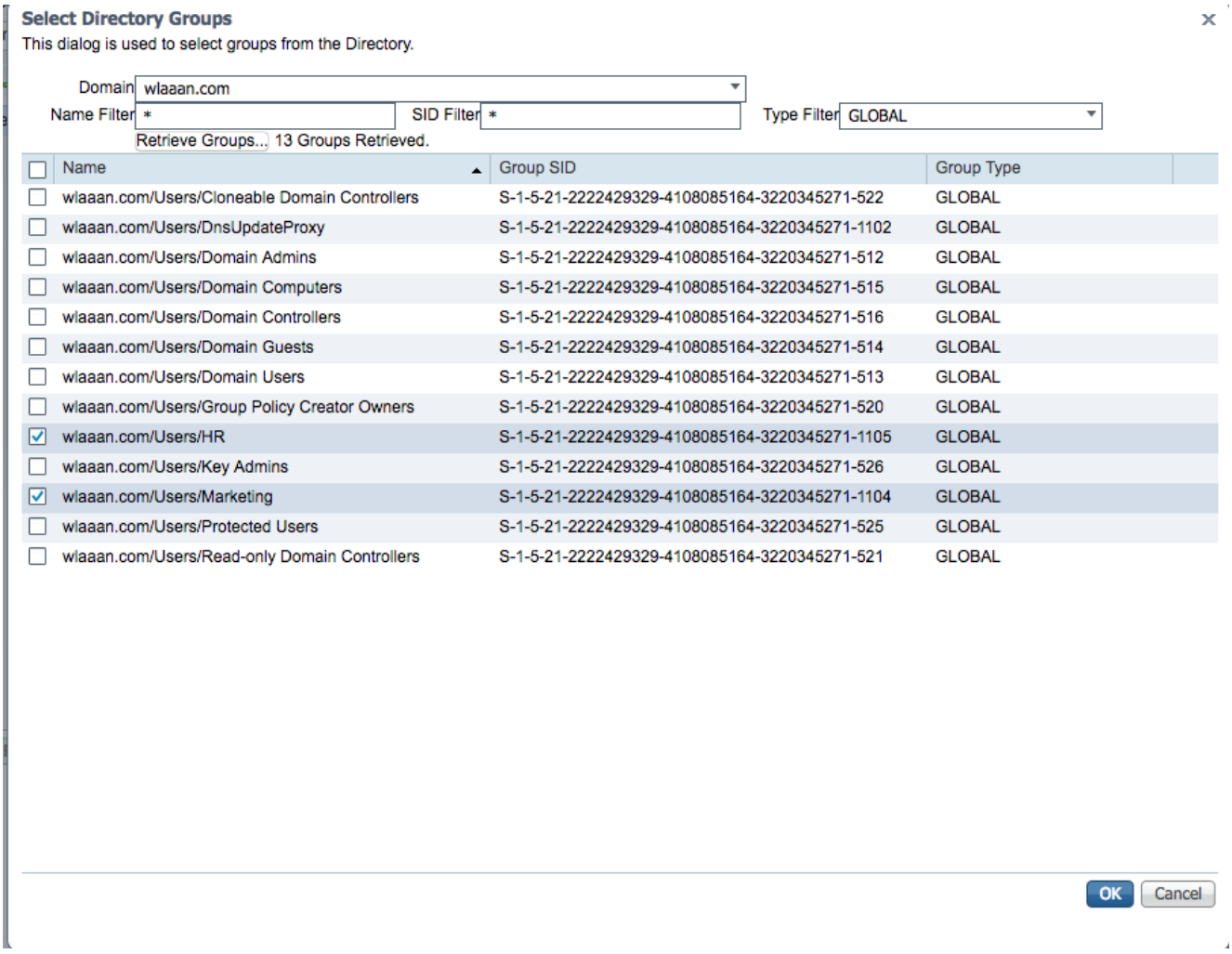
Falls bei der Registrierung Probleme auftreten, können Sie das **Diagnose-Tool** verwenden, um die für die AD-Verbindung erforderlichen Tests auszuführen.

6. Es müssen Gruppen für Active Directory abgerufen werden, die zum Zuweisen der entsprechenden Autorisierungsprofile verwendet werden. Navigieren Sie unter **"Administration -> Identity Management -> External Identity Sources -> Active Directory -> <Your AD> -> Groups"**, klicken Sie dann auf die Schaltfläche **Add** und wählen Sie **"Select**

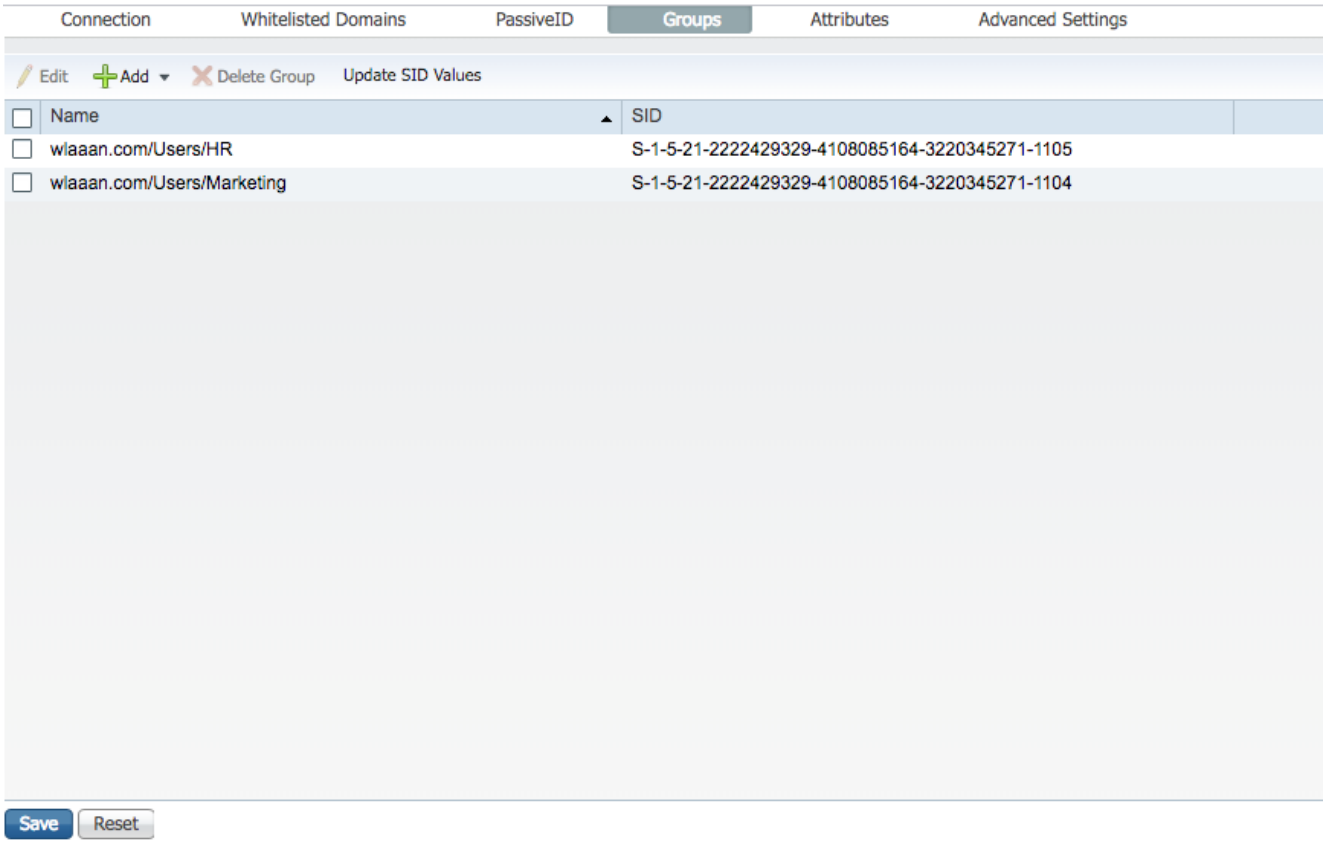
Groups from Active Directory".



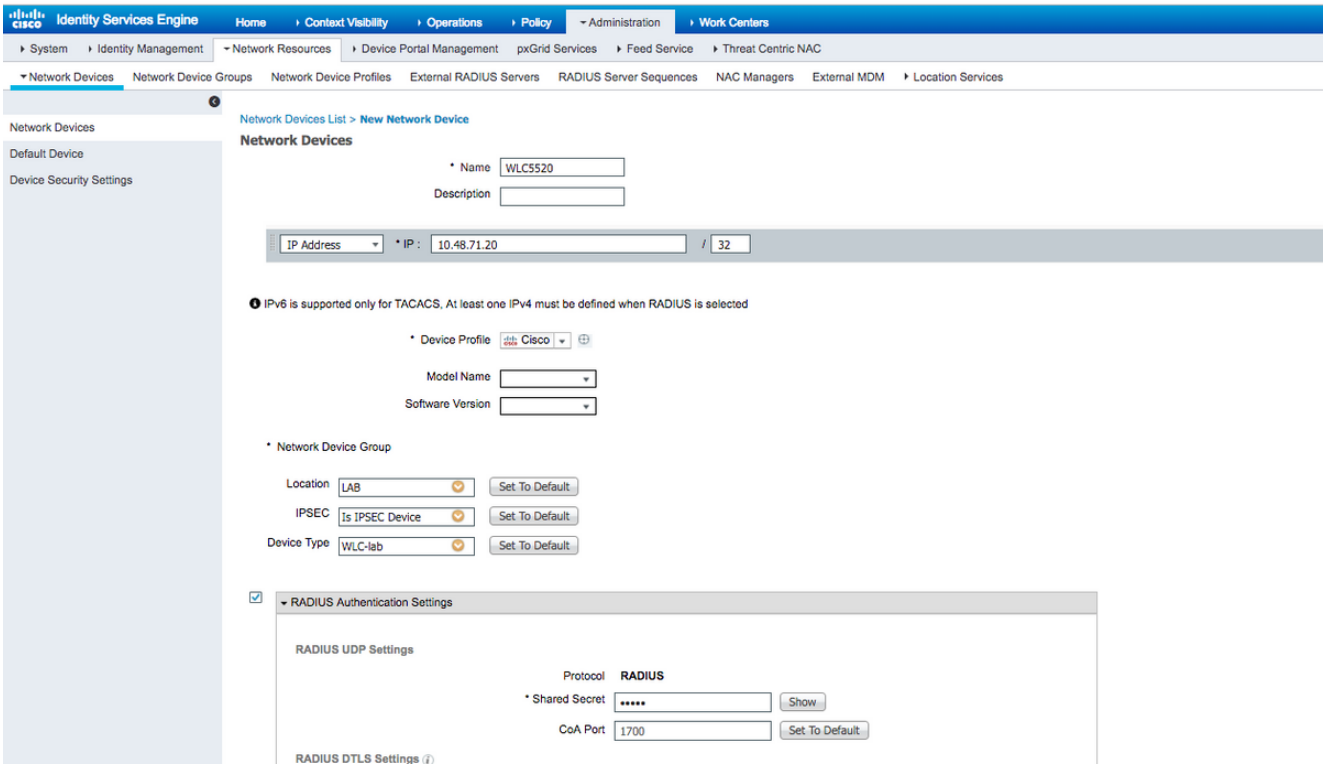
7. Ein neues Popup-Fenster wird geöffnet, in dem Sie entweder einen Filter angeben können, um bestimmte Gruppen wiederherzustellen, oder alle Gruppen aus AD abrufen können. Wählen Sie die entsprechenden Gruppen aus der AD-Gruppenliste aus und drücken Sie "OK".



8. Die entsprechenden Gruppen werden der ISE hinzugefügt und können gespeichert werden. Drücken Sie "Speichern".

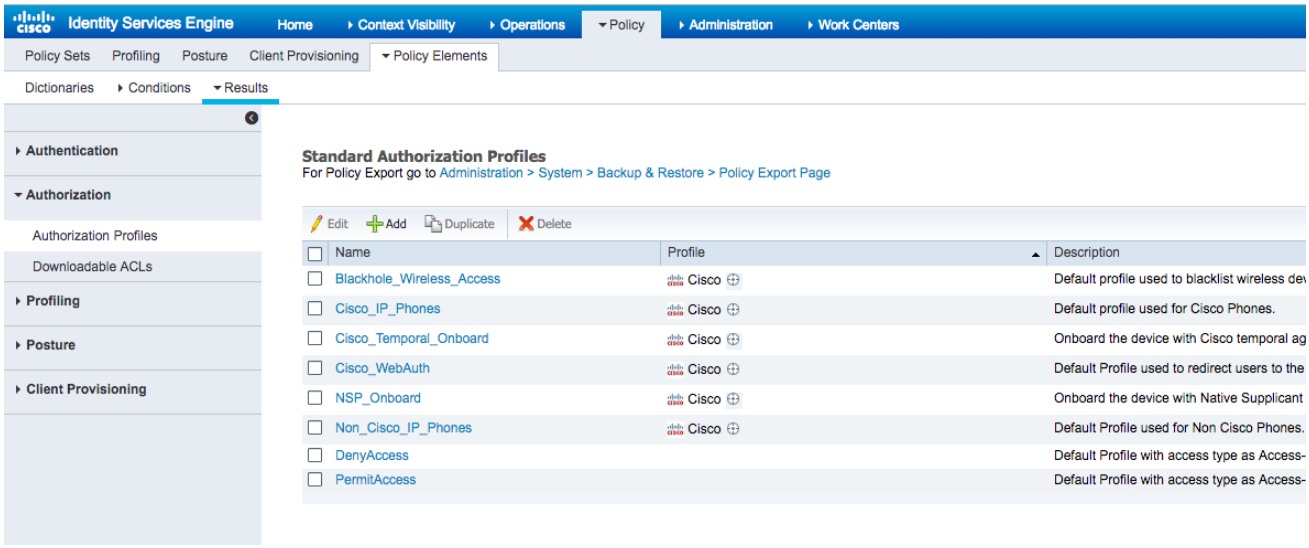


9. Fügen Sie WLC zur Liste der ISE-Netzwerkgeräte hinzu. Navigieren Sie unter "**Administration -> Network Resources -> Network Devices**" (**Verwaltung -> Netzwerkressourcen -> Netzwerkgeräte**), und drücken Sie "**Add**" (**Hinzufügen**). Vollständige Konfiguration durch Bereitstellung der IP-Adresse für die WLC-Verwaltung und des gemeinsamen geheimen RADIUS-Zugriffs zwischen WLC und ISE

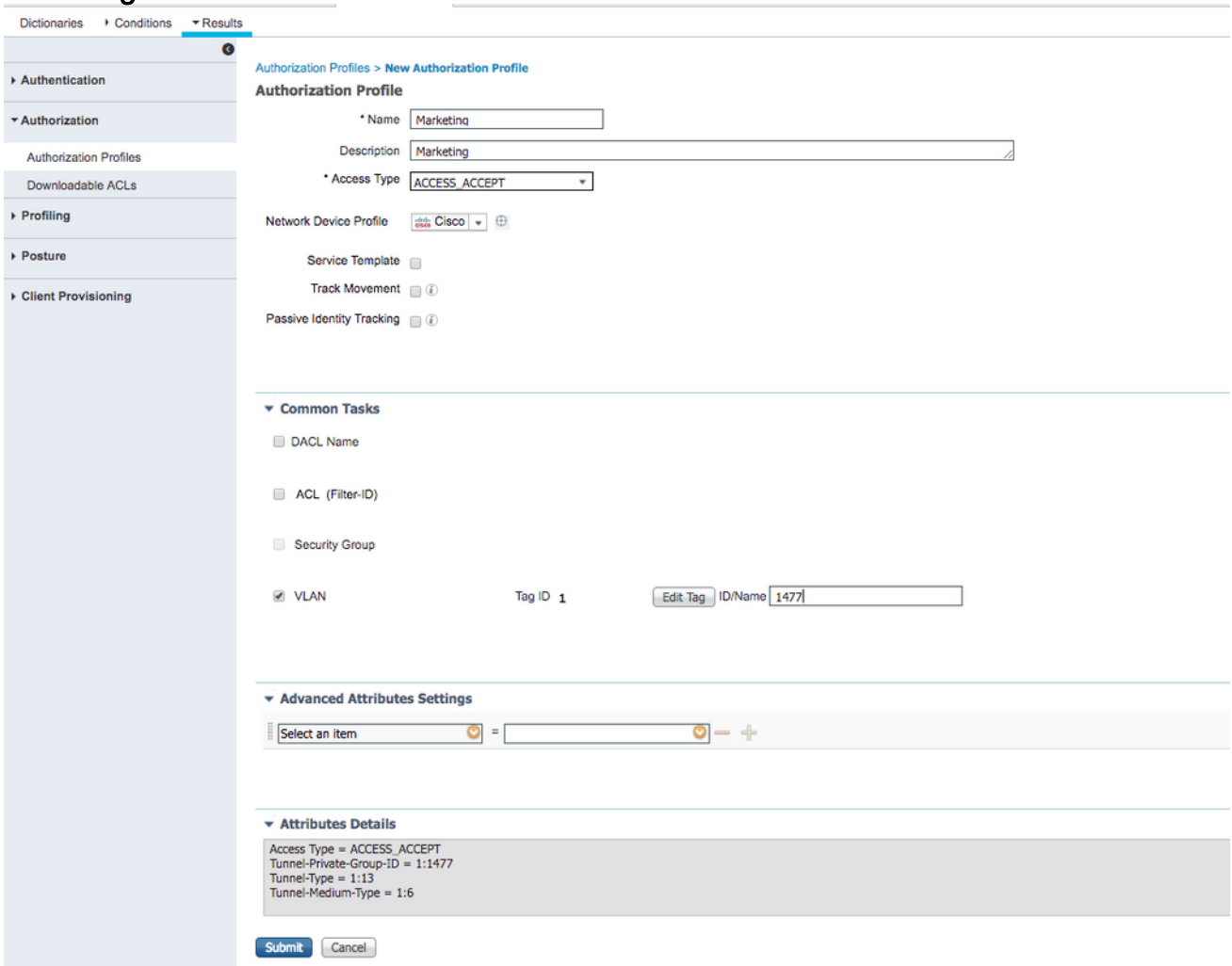


10. Nachdem wir der ISE zum AD hinzugefügt und den WLC zur Geräteliste hinzugefügt haben, können wir nun mit der Konfiguration der Authentifizierungs- und Autorisierungsrichtlinien für Benutzer beginnen. Erstellen Sie ein Autorisierungsprofil für die Zuweisung von Benutzern aus **Marketing** zu **VLAN1477** und aus der **HR**-Gruppe zu **VLAN1478**.

Navigieren Sie unter "**Richtlinien -> Richtlinienelemente -> Ergebnisse -> Autorisierung -> Autorisierungsprofile**", und klicken Sie auf die Schaltfläche **Hinzufügen**, um ein neues Profil zu erstellen.

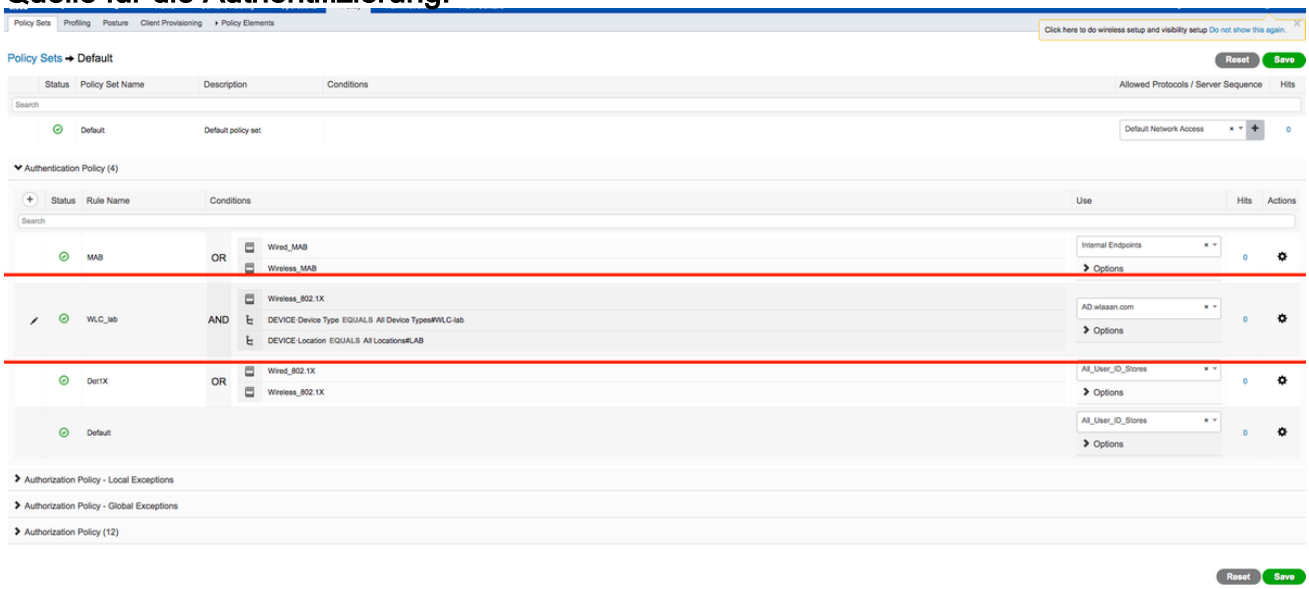


Vollständige Autorisierungsprofilkonfiguration mit VLAN-Informationen für die jeweilige Gruppe; Das nachfolgende Beispiel zeigt die Gruppenkonfigurationseinstellungen für **Marketing**.

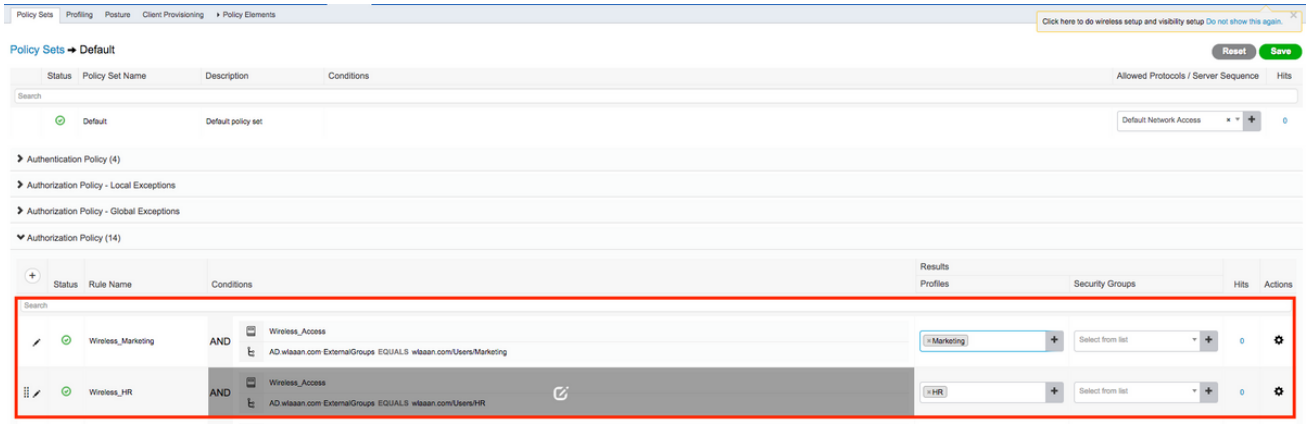


Eine ähnliche Konfiguration muss für andere Gruppen erfolgen, und das entsprechende VLAN-Tag-Attribut muss konfiguriert werden.Nach der Konfiguration der Autorisierungsprofile können wir Authentifizierungsrichtlinien für Wireless-Benutzer definieren. Dies kann entweder durch Konfigurieren von "**Benutzerdefiniert**" oder Ändern des **Standard**-Policy-Satzes erfolgen. In diesem Beispiel ändern wir den "Standard"-

Richtliniensatz. Öffnen Sie **"Richtlinie -> Richtliniensätze -> Standard"**. Standardmäßig verwendet die ISE für den 802.1x-Authentifizierungstyp '**All_User_ID_Stores**', obwohl sie auch mit den aktuellen Standardeinstellungen funktioniert, da "**AD**" Teil der Identitätsquellenliste von **All_User_ID_Stores ist. In** diesem Beispiel wird eine spezifischere Regel "**WLC_Lab"** für den entsprechenden LAB-Controller verwendet und "**AD" als einzige Quelle für die Authentifizierung.**

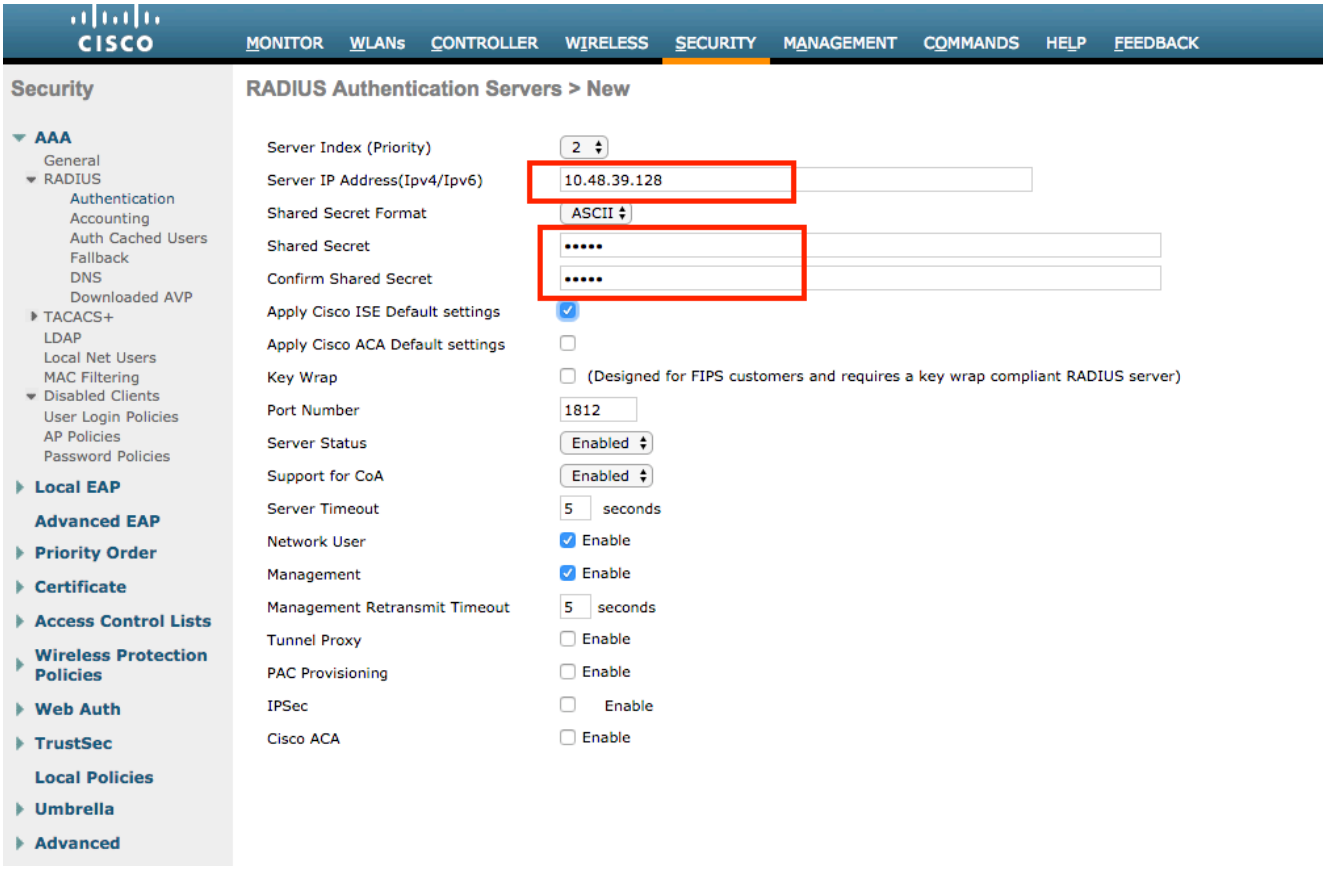


Jetzt müssen Autorisierungsrichtlinien für Benutzer erstellt werden, die das jeweilige Autorisierungsprofil basierend auf der Gruppenmitgliedschaft zuweisen. Öffnen Sie den Abschnitt "**Autorisierungsrichtlinie**", und erstellen Sie Richtlinien, um diese Anforderung zu erfüllen.

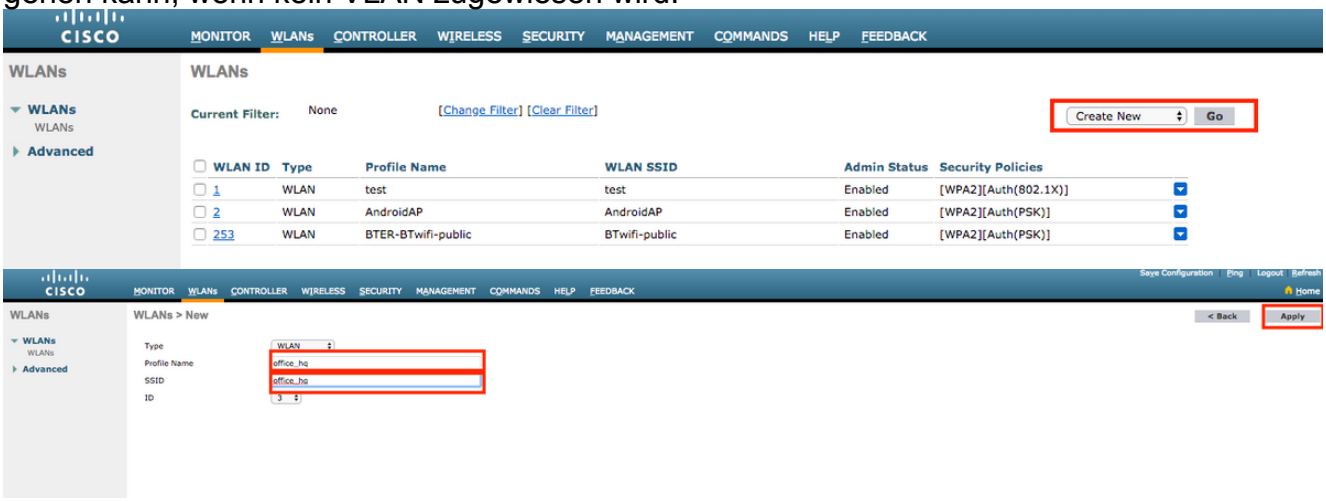


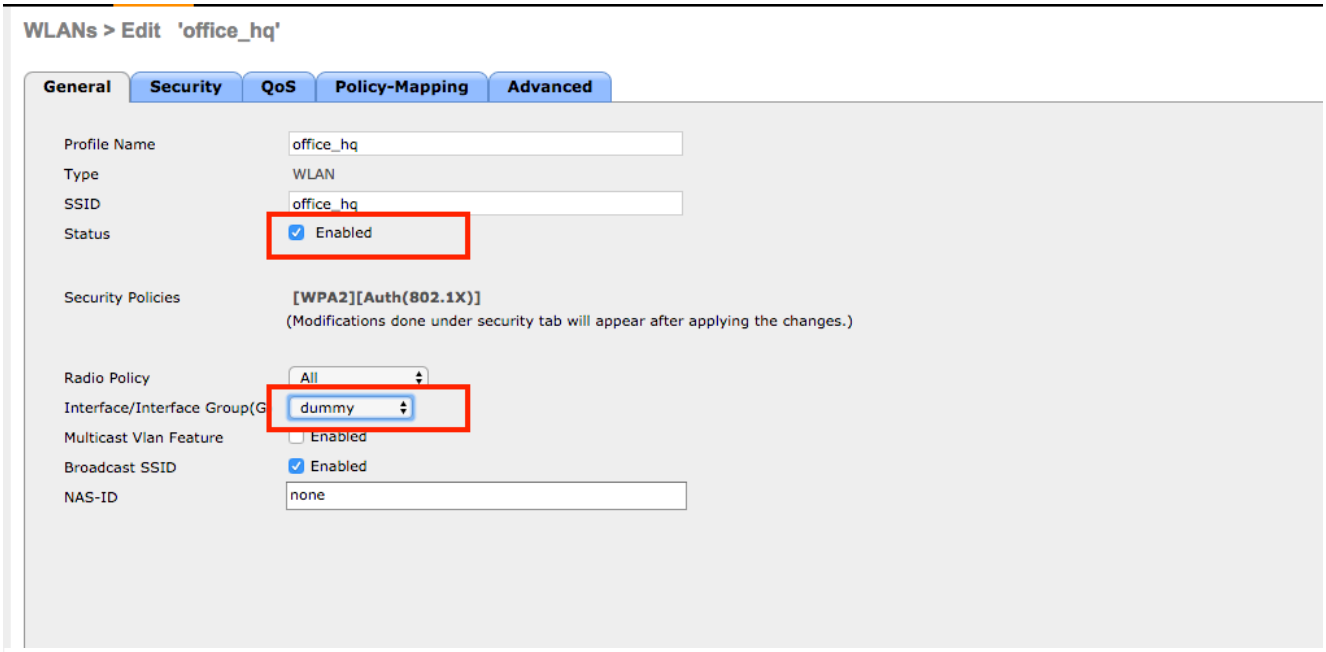
WLC-Konfiguration zur Unterstützung der 802.1x-Authentifizierung und des AAA-override für die SSID 'office_hq'

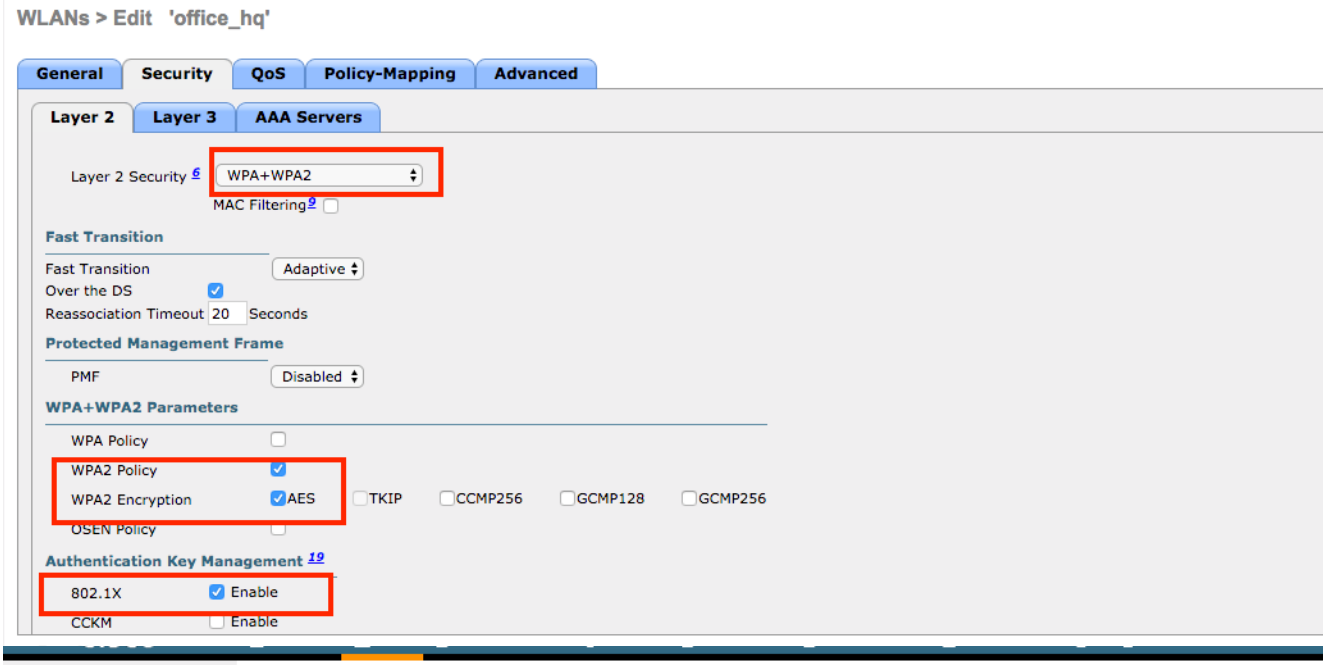
1. Konfigurieren Sie die ISE als RADIUS-Authentifizierungsserver auf dem WLC im Abschnitt **"Security -> AAA -> RADIUS -> Authentication" (Sicherheit -> AAA -> RADIUS -> Authentifizierung)** in der Webbenutzeroberfläche, und geben Sie die ISE-IP-Adresse und die freigegebenen geheimen Informationen an.

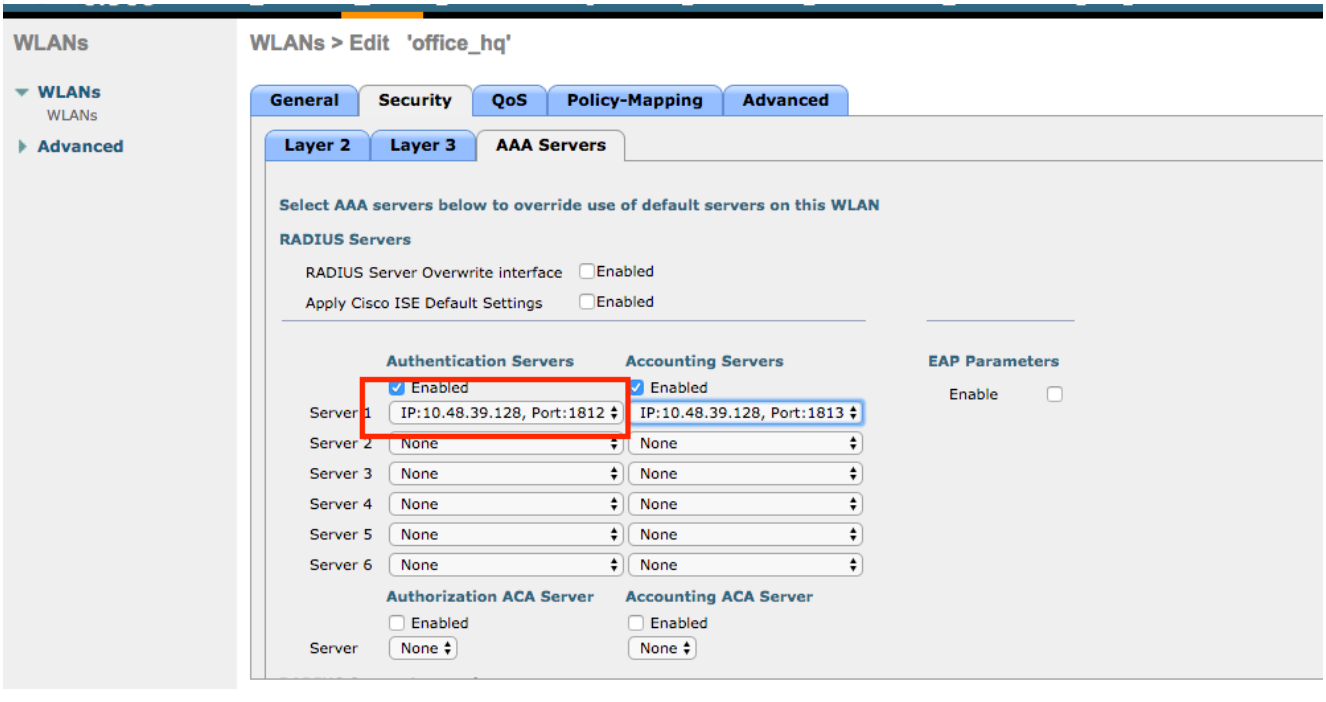


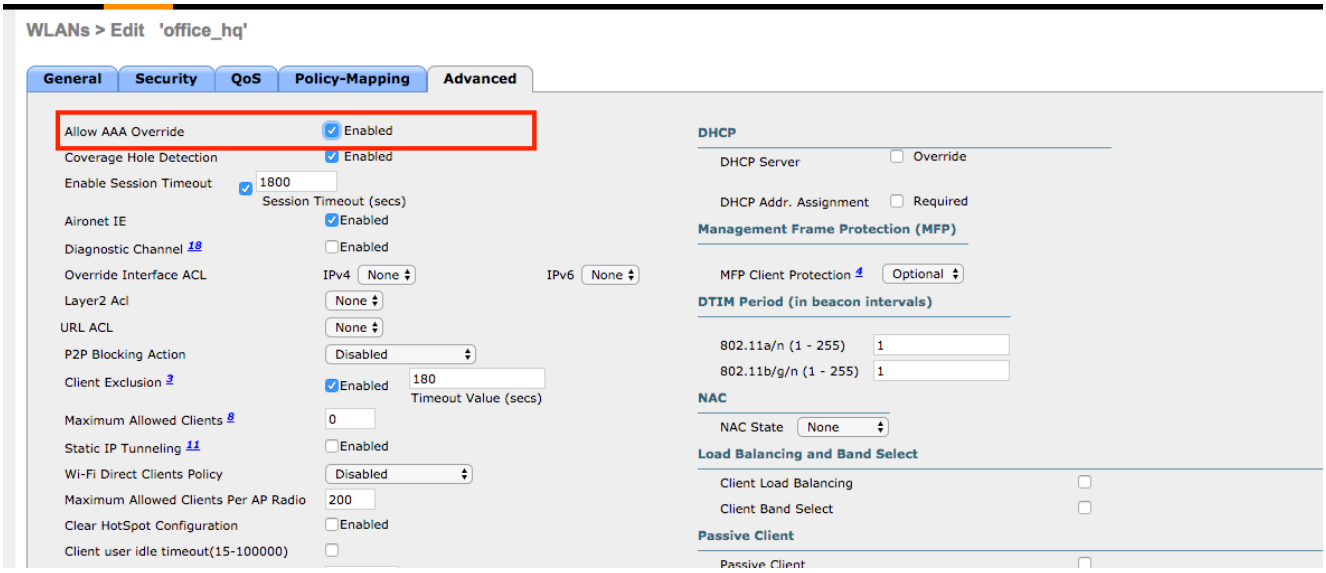
2. Konfigurieren Sie SSID office_hq im Abschnitt "**WLANs**" des WLC. Im folgenden Beispiel wird die SSID mit WPA2/AES+dot1x und AAA override konfiguriert. Schnittstelle "Dummy" ist für das WLAN ausgewählt, da das richtige VLAN sowieso über RADIUS zugewiesen wird. Diese Dummy-Schnittstelle muss auf dem WLC erstellt werden und eine IP-Adresse erhalten. Die IP-Adresse muss jedoch nicht gültig sein, und das VLAN, in dem sie gespeichert ist, darf nicht im Uplink-Switch erstellt werden, sodass der Client nirgendwo hin gehen kann, wenn kein VLAN zugewiesen wird.



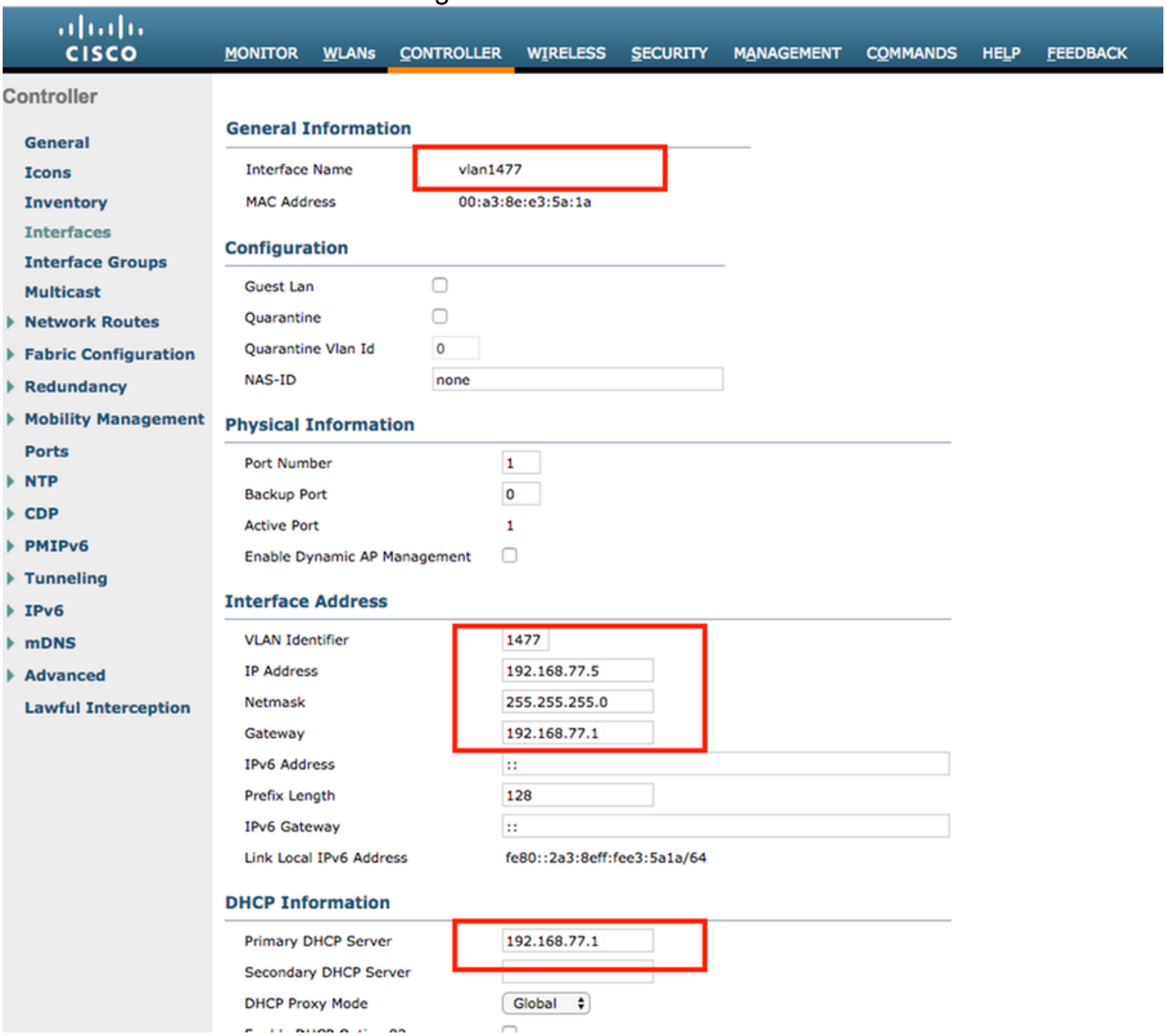

WLANs > Edit 'office_hq'
General
Security
QoS
Policy-Mapping
Advanced
Profile Name
office_hq
Type
WLAN
SSID
office_hq
Status
Enabled
Security Policies
[WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)
Radio Policy
All
Interface/Interface Group(G
dummy
Multicast Vlan Feature
Enabled
Broadcast SSID
Enabled
NAS-ID
none


WLANs > Edit 'office_hq'
General
Security
QoS
Policy-Mapping
Advanced
Layer 2
Layer 3
AAA Servers
Layer 2 Security
WPA+WPA2
MAC Filtering
Fast Transition
Fast Transition
Adaptive
Over the DS
Reassociation Timeout
20
Seconds
Protected Management Frame
PMF
Disabled
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES
TKIP
CCMP256
GCMP128
GCMP256
OSEN Policy
Authentication Key Management
802.1X
Enable
CCKM
Enable


WLANs
WLANs
WLANs
Advanced
WLANs > Edit 'office_hq'
General
Security
QoS
Policy-Mapping
Advanced
Layer 2
Layer 3
AAA Servers
Select AAA servers below to override use of default servers on this WLAN
RADIUS Servers
RADIUS Server Overwrite interface
Enabled
Apply Cisco ISE Default Settings
Enabled
Authentication Servers
Accounting Servers
EAP Parameters
Enabled
Enabled
Enable
Server 1
IP:10.48.39.128, Port:1812
IP:10.48.39.128, Port:1813
Server 2
None
None
Server 3
None
None
Server 4
None
None
Server 5
None
None
Server 6
None
None
Authorization ACA Server
Accounting ACA Server
Enabled
Enabled
Server
None
None



3. Darüber hinaus müssen im Benutzeroberflächen-Menü "**Controller -> Interfaces**" im WLC für Benutzer-VLANs dynamische Schnittstellen erstellt werden. Der WLC kann die VLAN-Zuweisung, die über AAA empfangen wurde, nur einhalten, wenn er über eine dynamische Schnittstelle in diesem VLAN verfügt.



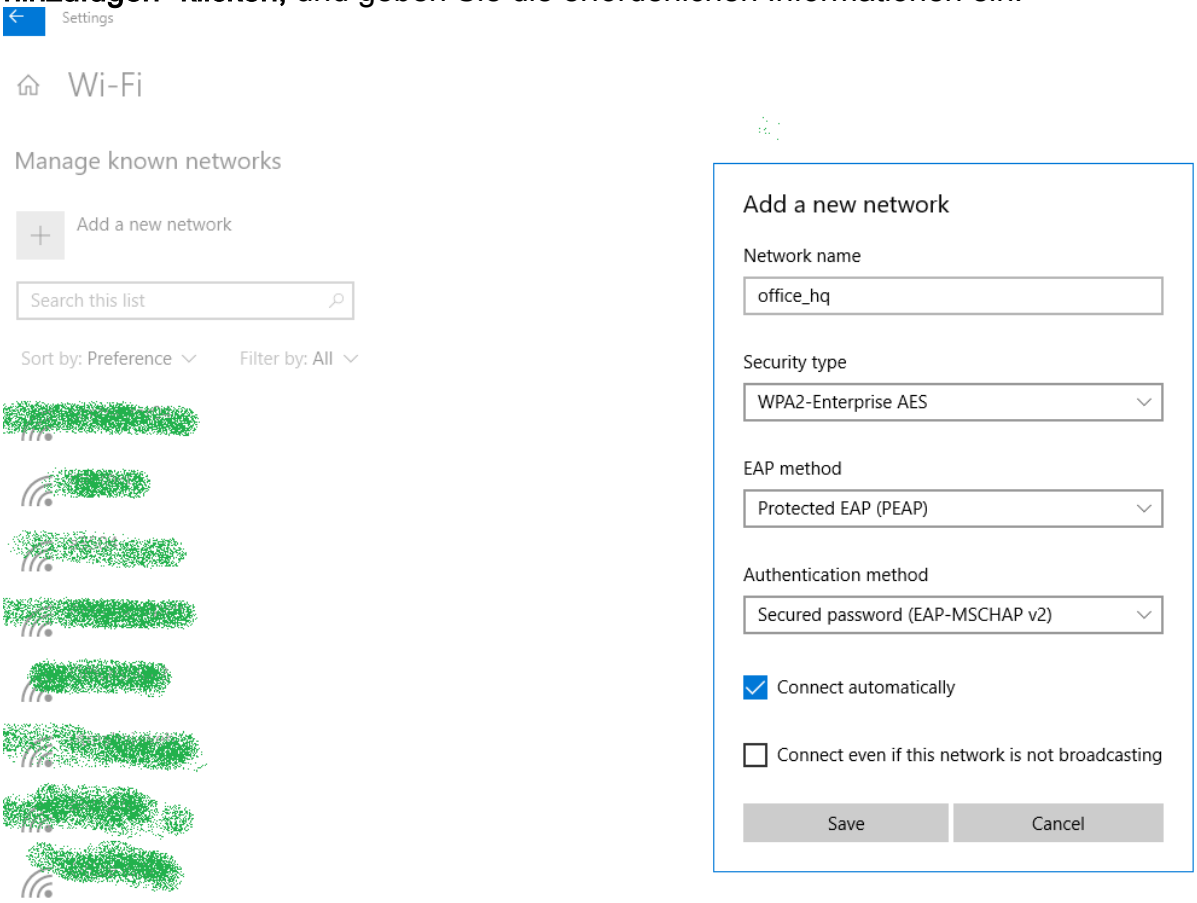
Überprüfen

Zum Testen von Verbindungen werden die systemeigene Windows 10-Komponente und das AnyConnect-NAM verwendet.

Da wir die EAP-PEAP-Authentifizierung verwenden und die ISE ein selbstsigniertes Zertifikat (Self-Signed Certificate, SSC) verwendet, müssen wir einer Zertifikatswarnung zustimmen oder die Zertifikatsvalidierung deaktivieren. In einer Unternehmensumgebung sollten Sie ein signiertes und vertrauenswürdiges Zertifikat auf der ISE verwenden und sicherstellen, dass Endbenutzergeräte das entsprechende Stammzertifikat in der Liste der vertrauenswürdigen Zertifizierungsstellen installiert haben.

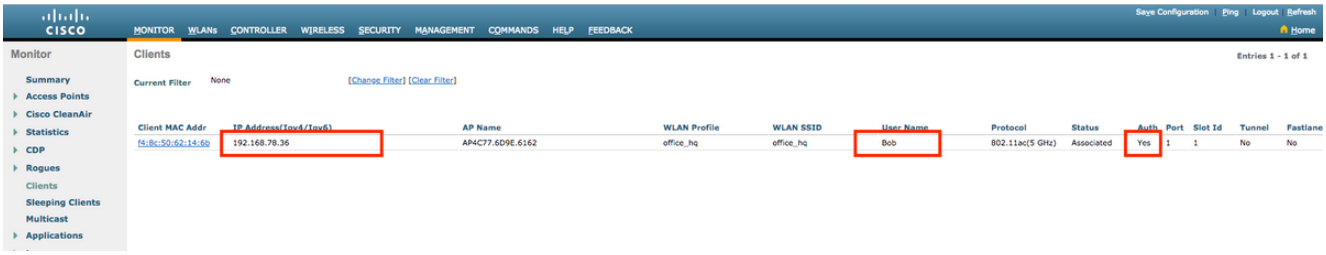
Testen der Verbindung mit Windows 10 und der systemeigenen Komponente

1. Öffnen Sie **"Netzwerk- und Interneteinstellungen -> Wi-Fi -> Bekannte Netzwerke verwalten",** und erstellen Sie ein neues Netzwerkprofil, indem Sie auf die Schaltfläche **"Neues Netzwerk hinzufügen" klicken,** und geben Sie die erforderlichen Informationen ein.



2. Überprüfen Sie das Authentifizierungsprotokoll auf der ISE, und stellen Sie sicher, dass das richtige Profil für den Benutzer ausgewählt ist.

3. Überprüfen Sie den Clienteintrag auf dem WLC, und stellen Sie sicher, dass es dem richtigen VLAN zugewiesen ist und sich im **RUN-**Status befindet.

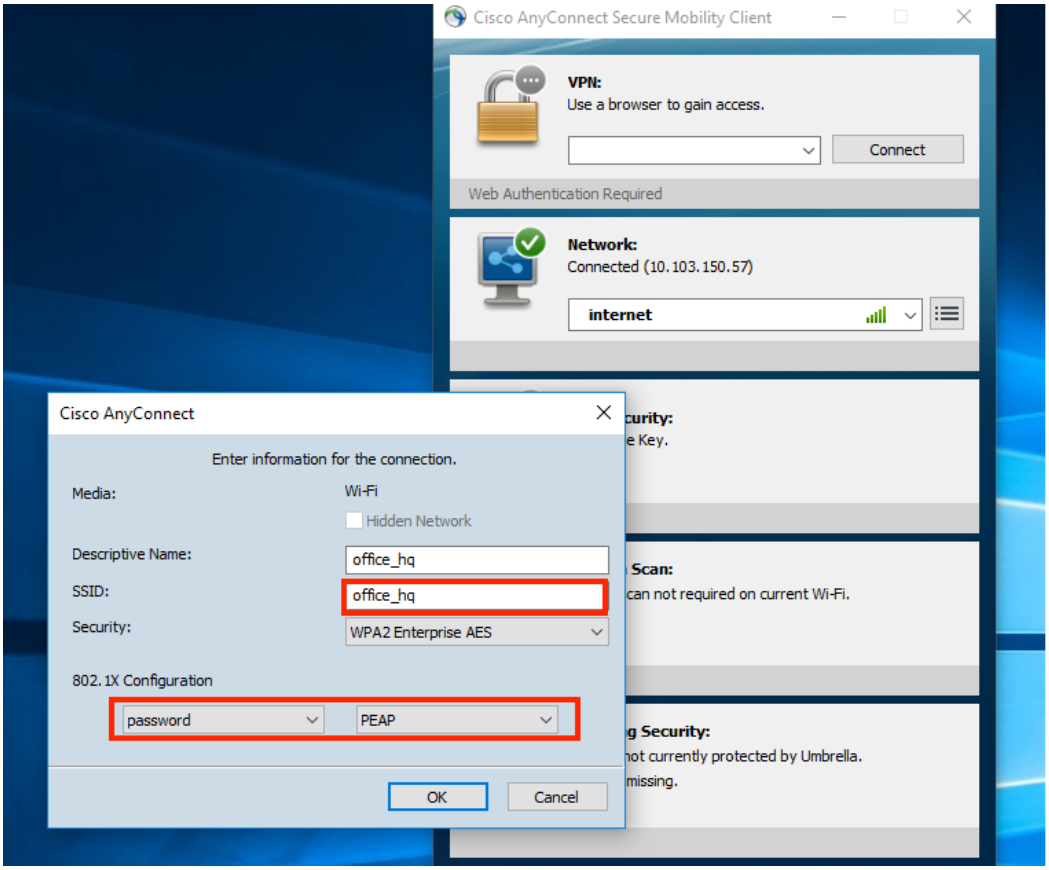


4. **Der WLC-CLI-**Clientstatus kann mit "**show client dertails <MAC-Adresse>":**

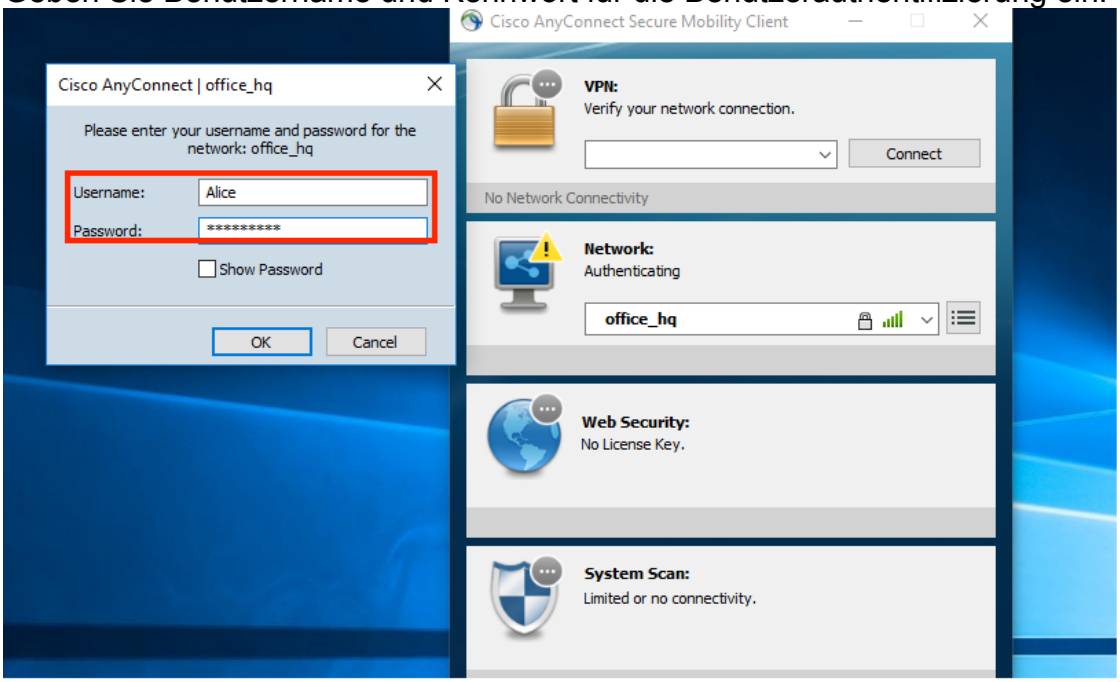
```
show client detail f4:8c:50:62:14:6b
Client MAC Address.............................. f4:8c:50:62:14:6b
Client Username ................................ Bob
Client Webauth Username ........................ N/A
Hostname: .....................................
Device Type: ................................... Intel-Device
AP MAC Address.................................. 70:69:5a:51:4e:c0
AP Name......................................... AP4C77.6D9E.6162
AP radio slot Id................................ 1
Client State.................................... Associated
User Authenticated by .......................... RADIUS Server
Client User Group............................... Bob
Client NAC OOB State............................ Access
Wireless LAN Id................................. 3
Wireless LAN Network Name (SSID)................ office_hq
Wireless LAN Profile Name....................... office_hq
Hotspot (802.11u)............................... Not Supported
Connected For .................................. 242 secs
BSSID........................................... 70:69:5a:51:4e:cd
Channel......................................... 36
IP Address...................................... 192.168.78.36
Gateway Address................................. 192.168.78.1
Netmask......................................... 255.255.255.0
...
Policy Manager State............................ RUN
...
EAP Type........................................ PEAP
Interface....................................... vlan1478
VLAN............................................ 1478
Quarantine VLAN................................. 0
Access VLAN..................................... 1478
```

Testen Sie die Verbindung mit Windows 10 und AnyConnect NAM.

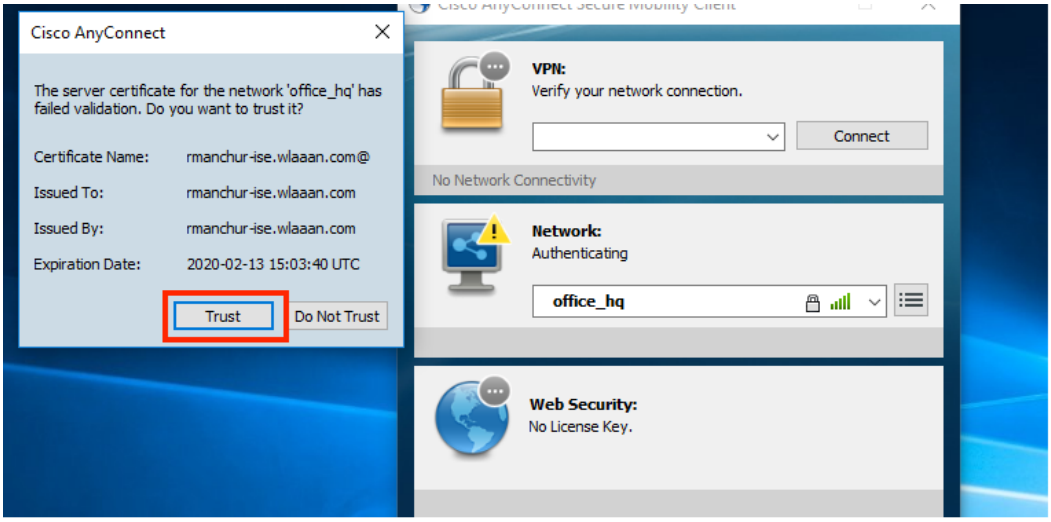
1. Wählen Sie SSID aus der Liste der verfügbaren SSIDs und dem entsprechenden EAP-Authentifizierungstyp (in diesem Beispiel PEAP) und dem inneren Authentifizierungsformular aus.



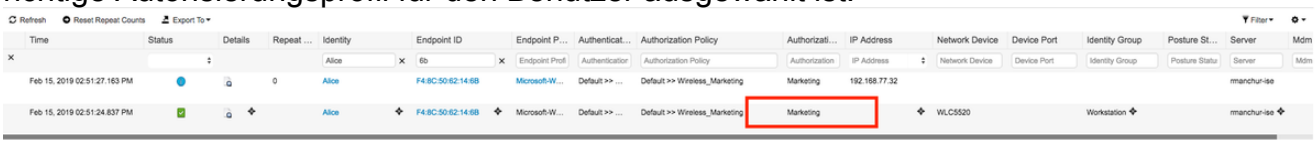
2. Geben Sie Benutzername und Kennwort für die Benutzerauthentifizierung ein.



3. Da die ISE einen SSC an den Client sendet, muss manuell festgelegt werden, dass das Zertifikat vertrauenswürdig ist (in der Produktionsumgebung wird dringend empfohlen, ein vertrauenswürdiges Zertifikat auf der ISE zu installieren).



4. Überprüfen Sie die Authentifizierungsprotokolle auf der ISE, und stellen Sie sicher, dass das richtige Autorisierungsprofil für den Benutzer ausgewählt ist.



5. Überprüfen Sie den Client-Eintrag im WLC, und stellen Sie sicher, dass er dem richtigen VLAN zugewiesen ist und sich im **RUN**-Status befindet.

6. **Der WLC-CLI-Clientstatus kann mit "show client dertails <MAC-Adresse>":**

```
Client MAC Address.............................. f4:8c:50:62:14:6b
Client Username ................................ Alice
Client Webauth Username ........................ N/A
Hostname: ......................................
Device Type: ................................... Intel-Device
AP MAC Address.................................. 70:69:5a:51:4e:c0
AP Name......................................... AP4C77.6D9E.6162
AP radio slot Id................................ 1
Client State.................................... Associated
User Authenticated by .......................... RADIUS Server
Client User Group............................... Alice
Client NAC OOB State............................ Access
Wireless LAN Id................................. 3
Wireless LAN Network Name (SSID)................ office_hq
Wireless LAN Profile Name....................... office_hq
Hotspot (802.11u)............................... Not Supported
Connected For .................................. 765 secs
BSSID........................................... 70:69:5a:51:4e:cd
Channel......................................... 36
IP Address...................................... 192.168.77.32
Gateway Address................................. 192.168.77.1
```

```
Netmask....................................... 255.255.255.0
...
Policy Manager State.......................... RUN
...
Policy Type................................... WPA2
Authentication Key Management................. 802.1x
Encryption Cipher............................. CCMP-128 (AES)
Protected Management Frame ................... No
Management Frame Protection................... No
EAP Type...................................... PEAP
Interface..................................... vlan1477
VLAN.......................................... 1477
```

Fehlerbehebung

1. Verwenden Sie **"test aaa radius username <user> password <password> wlan-id <id>"** zum Testen der RADIUS-Verbindung zwischen WLC und ISE und "**test aa show radius**", um die Ergebnisse anzuzeigen.

```
test aaa radius username Alice password <removed> wlan-id 2

Radius Test Request
  Wlan-id....................................... 2
  ApGroup Name.................................. none

  Attributes                    Values
  ----------                    ------
  User-Name                     Alice
  Called-Station-Id             00-00-00-00-00-00:AndroidAP
  Calling-Station-Id            00-11-22-33-44-55
  Nas-Port                      0x00000001 (1)
  Nas-Ip-Address                10.48.71.20
  NAS-Identifier                0x6e6f (28271)
  Airespace / WLAN-Identifier   0x00000002 (2)
  User-Password                 cisco!123
  Service-Type                  0x00000008 (8)
  Framed-MTU                    0x00000514 (1300)
  Nas-Port-Type                 0x00000013 (19)
  Cisco / Audit-Session-Id      1447300a0000003041d5665c
  Acct-Session-Id               5c66d541/00:11:22:33:44:55/743



test radius auth request successfully sent. Execute 'test aaa show radius' for response

(Cisco Controller) >test aaa show radius

Radius Test Request
  Wlan-id....................................... 2
  ApGroup Name.................................. none
Radius Test Response

Radius Server           Retry Status
-------------           ----- ------
10.48.39.128            1     Success

Authentication Response:
  Result Code: Success
```

```
Attributes                      Values
----------                      ------
User-Name                       Alice
State                           ReauthSession:1447300a0000003041d5665c
Class                           CACS:1447300a0000003041d5665c:rmanchur-ise/339603379/59
Tunnel-Type                     0x0000000d (13)
Tunnel-Medium-Type              0x00000006 (6)
Tunnel-Group-Id                 0x000005c5 (1477)



(Cisco Controller) >
```

2. Verwenden Sie **"debug client <MAC-address>"**, um Verbindungsprobleme von Wireless-Clients zu beheben.
3. Verwenden Sie "**debug aa all enable**", um Authentifizierungs- und Autorisierungsprobleme in WLC zu beheben.
   Hinweis: Verwenden Sie diesen Befehl nur mit 'debug mac addr <mac-address>', um die Ausgabe basierend auf der MAC-Adresse, für die das Debuggen erfolgt, zu begrenzen.
4. Informationen zur Identifizierung von Problemen bei der Authentifizierung und AD-Kommunikation finden Sie in den ISE-Live-Protokollen und Sitzungsprotokollen.