Konfigurationsbeispiel für dynamische VLAN-Zuweisung mit RADIUS-Server und Wireless LAN-Controller

Inhalt

Einführung

In diesem Dokument wird das Konzept der dynamischen VLAN-Zuweisung vorgestellt. In diesem Dokument wird beschrieben, wie der WLAN-Controller (WLC) und ein RADIUS-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 WLC- und Lightweight Access Points (LAPs) besitzen
- über funktionale Kenntnisse des AAA-Servers verfügen

- Umfassende Kenntnisse über Wireless-Netzwerke und Wireless-Sicherheitsprobleme
- Grundkenntnisse des Lightweight AP Protocol (LWAPP)

Verwendete Komponenten

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

- Cisco 4400 WLC mit Firmware-Version 5.2
- Cisco LAP der Serie 1130
- Cisco 802.11a/b/g Wireless Client-Adapter mit Firmware-Version 4.4
- Cisco Aironet Desktop Utility (ADU) für die Ausführung von Version 4.4
- Cisco Secure Access Control Server (ACS) mit Version 4.1
- Cisco Switch der Serie 2950

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

Konventionen

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

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 unterstützt jedoch Identitätsnetzwerke. Auf diese Weise kann das Netzwerk eine einzelne SSID ankündigen, aber bestimmte Benutzer können je nach Benutzeranmeldeinformationen unterschiedliche QoS- 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 Cisco Secure ACS 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.

Wenn ein Client versucht, eine Verbindung zu einer LAP herzustellen, die bei einem Controller registriert ist, übergibt die LAP die Anmeldeinformationen des Benutzers zur Validierung an den RADIUS-Server. Nach erfolgreicher Authentifizierung übergibt der RADIUS-Server bestimmte IETF-Attribute (Internet Engineering Task Force) an den Benutzer. 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 (Tunnel Type) (Tunnel-Typ) - Legen Sie diesen Wert auf VLAN fest.
- IETF 65 (Tunnel Medium Type) (Tunnel-Medientyp): Legen Sie diesen Wert auf 802 fest.
- IETF 81 (Tunnel Private Group ID) (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 vom Typ string ist, wie in RFC2868 für die Verwendung mit IEEE 802.1X definiert, wird der VLAN-ID-Integer-Wert als Zeichenfolge codiert. Wenn diese Tunnelattribute gesendet werden, muss das Feld Tag ausgefüllt werden.

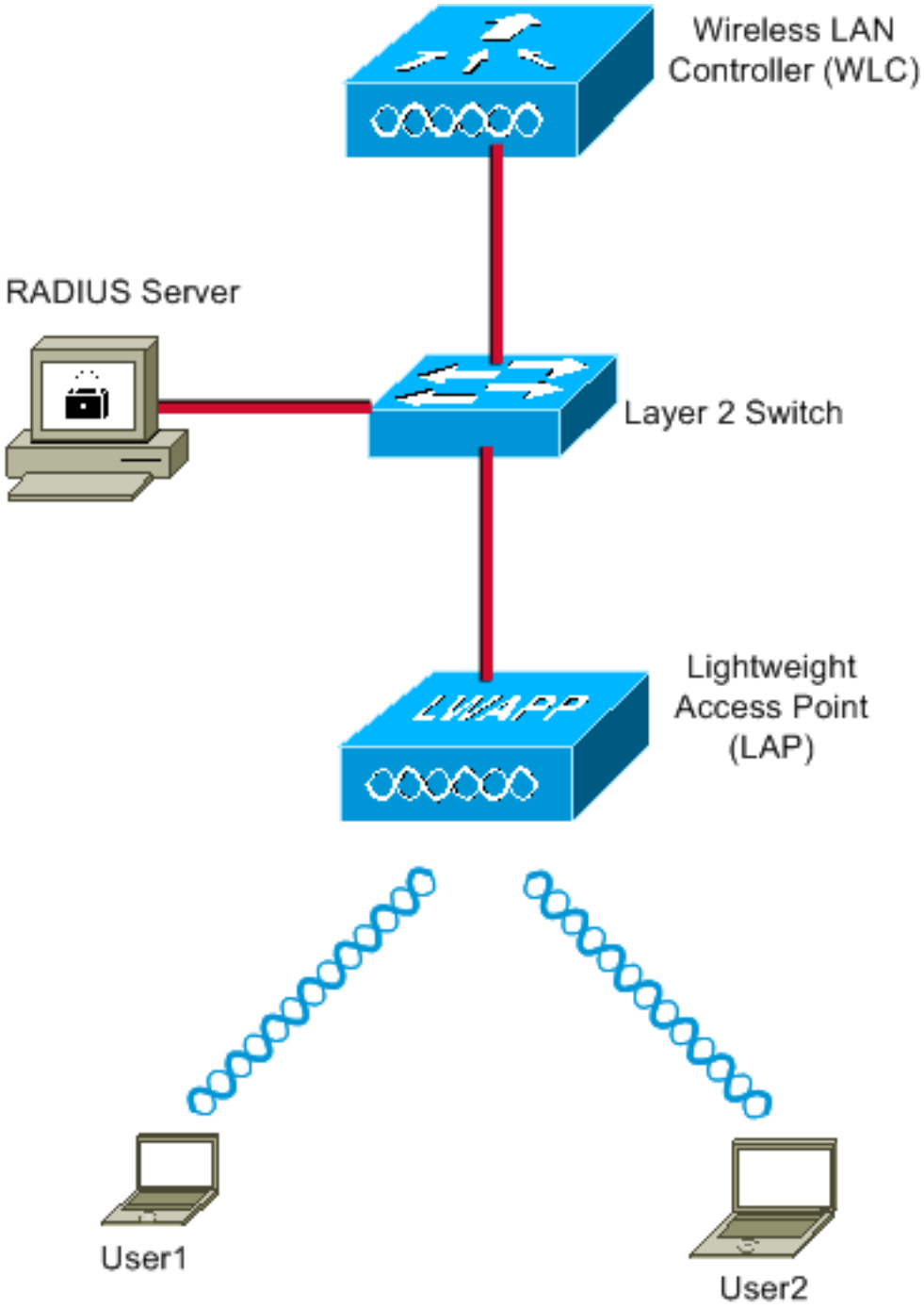
Wie in RFC2868 , Abschnitt 3.1 erwähnt: **Das Tag-Feld ist ein Oktett lang und soll eine Möglichkeit bieten, Attribute in demselben Paket zu gruppieren, die sich auf denselben Tunnel beziehen.** Gültige Werte für dieses Feld sind 0x01 bis 0x1F, einschließlich. Wenn das Feld Tag nicht verwendet wird, muss es 0 (0 x 00) sein. Weitere Informationen zu allen RADIUS-Attributen finden Sie unter RFC 2868 .

Konfiguration

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Dies sind die Konfigurationsdetails der in diesem Diagramm verwendeten Komponenten:

- Die IP-Adresse des ACS-Servers (RADIUS) lautet 172.16.1.1.
- Die Management-Schnittstellenadresse des WLC lautet 172.16.1.30.
- Die AP-Manager-Schnittstellenadresse des WLC lautet 172.16.1.31.
- Die DHCP-Serveradresse 172.16.1.1 wird verwendet, um der LWAPP IP-Adressen zuzuweisen. **Der interne DHCP-Server des Controllers wird verwendet, um die IP-Adresse Wireless-Clients zuzuweisen.**
- In dieser Konfiguration werden VLAN10 und VLAN11 verwendet. Der Benutzer1 ist so konfiguriert, dass er im VLAN10 platziert wird, und der Benutzer2 ist so konfiguriert, dass er vom RADIUS-Server in VLAN11 platziert wird.**Hinweis:** In diesem Dokument werden nur alle Konfigurationsinformationen zu user1 angezeigt. Führen Sie für Benutzer2 denselben Vorgang aus, der in diesem Dokument beschrieben wird.
- In diesem Dokument wird 802.1x mit LEAP als Sicherheitsmechanismus verwendet.**Hinweis:** Cisco empfiehlt die Verwendung erweiterter Authentifizierungsmethoden wie EAP-FAST und

EAP-TLS-Authentifizierung, um das WLAN zu sichern. In diesem Dokument wird LEAP nur zur Vereinfachung verwendet.

Konfiguration

Vor der Konfiguration wird in diesem Dokument davon ausgegangen, dass die LAP bereits beim WLC registriert ist. Weitere Informationen finden Sie im Konfigurationsbeispiel für Wireless LAN-Controller und Lightweight Access Point. Informationen zum Registrierungsverfahren finden Sie unter Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC).

Konfigurationsschritte

Diese Konfiguration ist in drei Kategorien unterteilt:

1. RADIUS-Serverkonfiguration
2. Switch für mehrere VLANs konfigurieren
3. WLC-Konfiguration
4. Konfiguration des Wireless-Client-Dienstprogramms

RADIUS-Serverkonfiguration

Für diese Konfiguration sind folgende Schritte erforderlich:

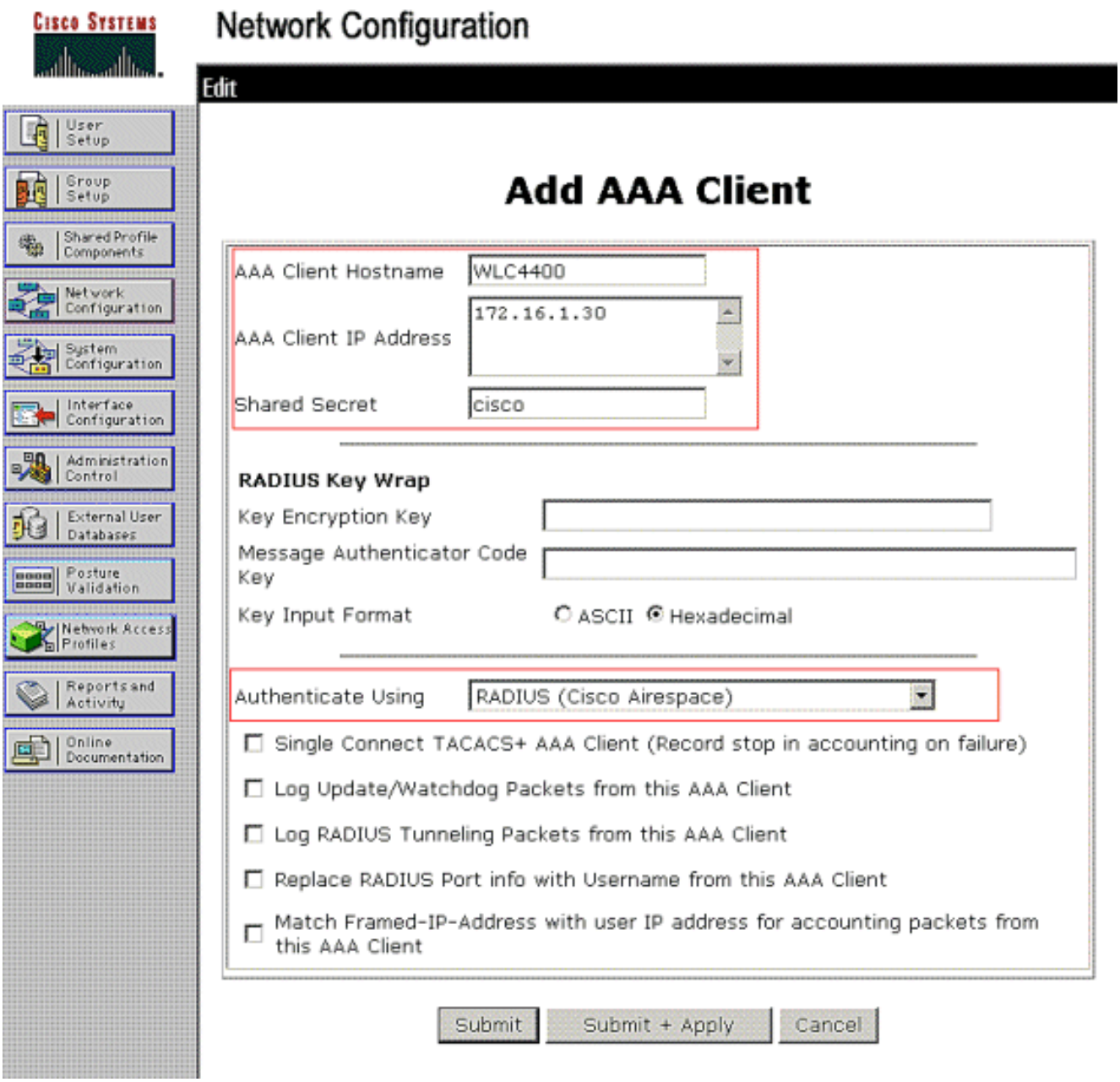
- Konfigurieren des WLC als AAA-Client auf dem RADIUS-Server
- Konfigurieren der Benutzer und der RADIUS (IETF)-Attribute für die dynamische VLAN-Zuweisung auf dem RADIUS-Server

Konfigurieren des AAA-Clients für den WLC auf dem RADIUS-Server

In diesem Verfahren wird erläutert, wie der WLC als AAA-Client auf dem RADIUS-Server hinzugefügt wird, sodass der WLC die Benutzeranmeldeinformationen an den RADIUS-Server übergeben kann.

Führen Sie diese Schritte aus:

1. Klicken Sie in der ACS-GUI auf **Netzwerkkonfiguration**.
2. Klicken Sie im Feld AAA-Clients auf den Abschnitt **Add Entry** (Eintrag **hinzufügen**).
3. Geben Sie die IP-Adresse und den Schlüssel für den AAA-Client ein.Die IP-Adresse muss die IP-Adresse der Verwaltungsschnittstelle des WLC sein.Stellen Sie sicher, dass der von Ihnen eingegebene Schlüssel mit dem Schlüssel übereinstimmt, der im WLC im Fenster "Security" (Sicherheit) konfiguriert wurde. Dies ist der geheime Schlüssel für die Kommunikation zwischen dem AAA-Client (WLC) und dem RADIUS-Server.
4. Wählen Sie für den Authentifizierungstyp **RADIUS (Cisco Air)** im Feld Authenticate Using (Authentifizieren über)
   aus.

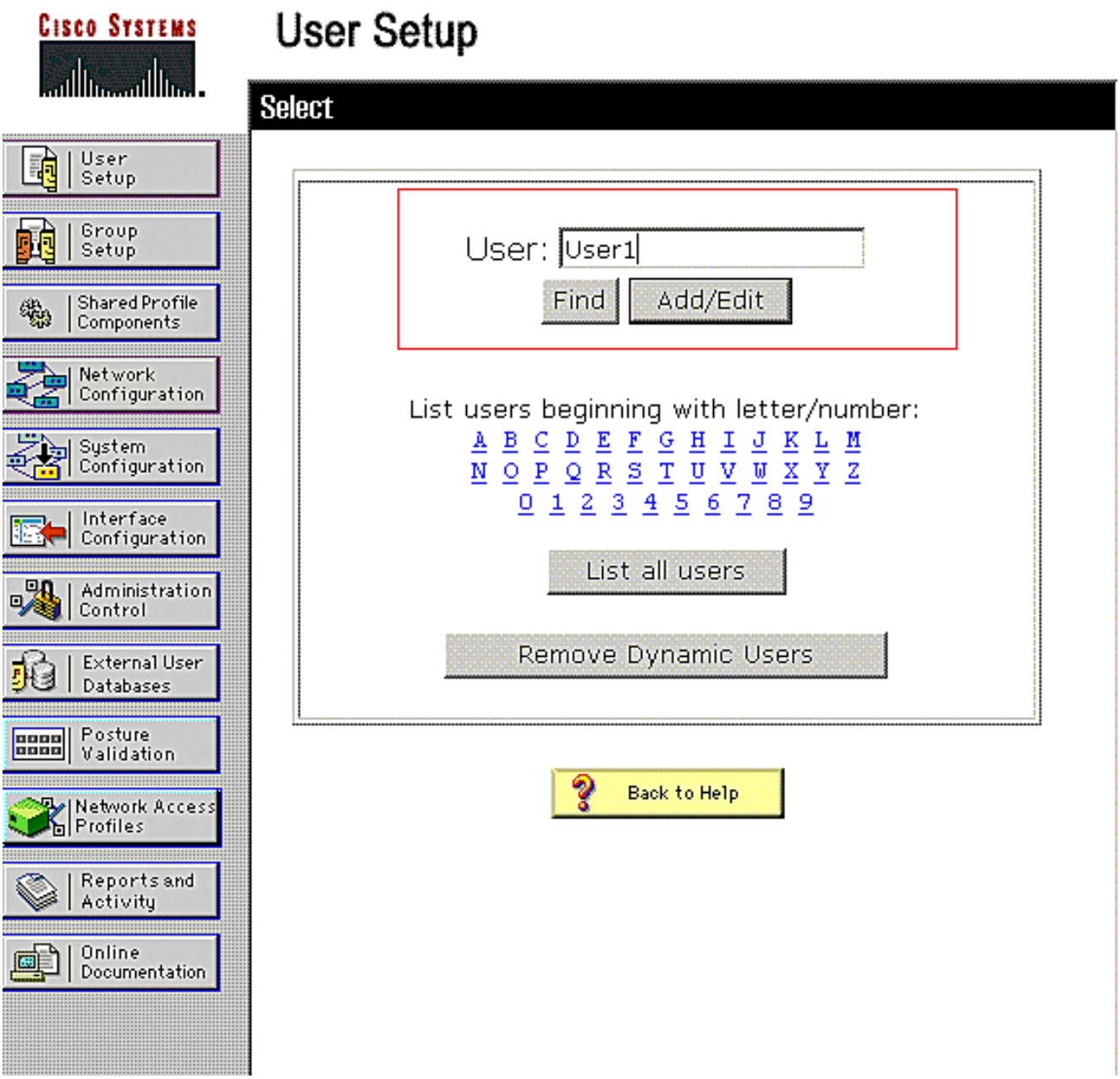


Konfigurieren der Benutzer und der RADIUS (IETF)-Attribute für die dynamische VLAN-Zuweisung auf dem RADIUS-Server

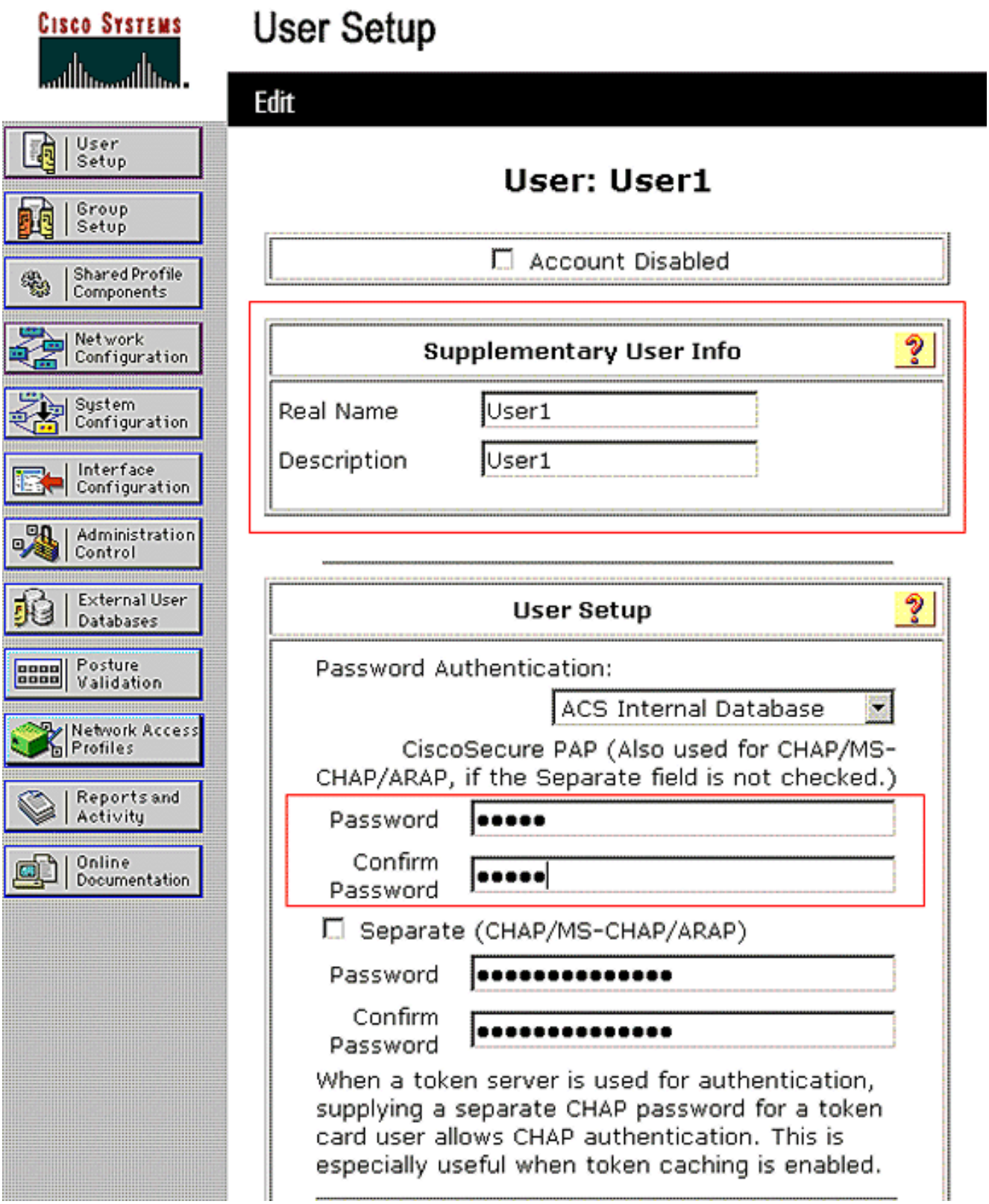
In diesem Verfahren wird erläutert, wie die Benutzer im RADIUS-Server und die RADIUS-Attribute (IETF) konfiguriert werden, die für die Zuweisung von VLAN-IDs zu diesen Benutzern verwendet werden.

Führen Sie diese Schritte aus:

1. Klicken Sie in der ACS-GUI auf **User Setup (Benutzereinrichtung)**.
2. Geben Sie im Fenster User Setup (Benutzereinrichtung) einen Benutzernamen in das Feld User (Benutzer) ein, und klicken Sie auf **Add/Edit**.

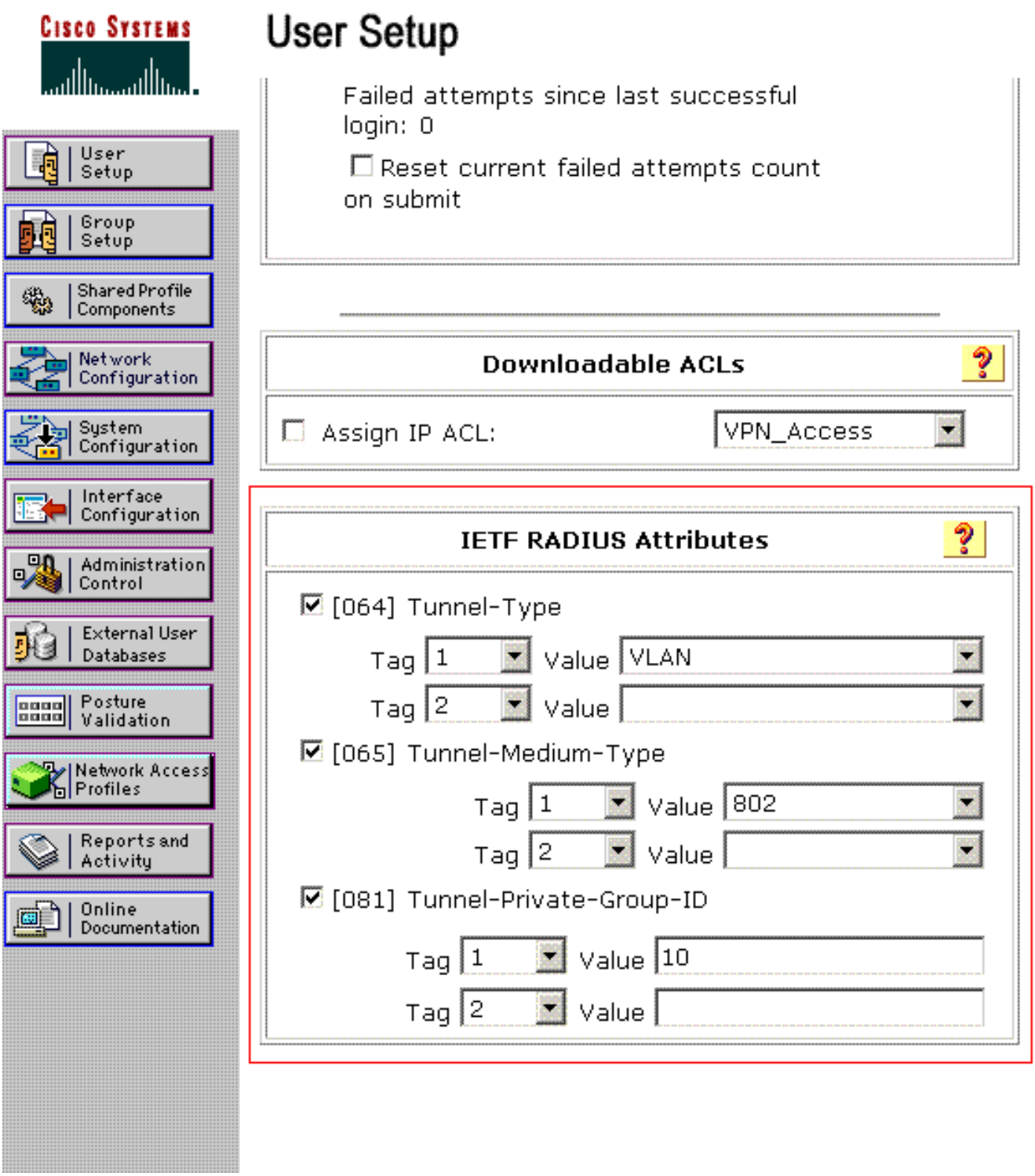


3. Geben Sie auf der Seite Bearbeiten die erforderlichen Benutzerinformationen ein, wie hier gezeigt:

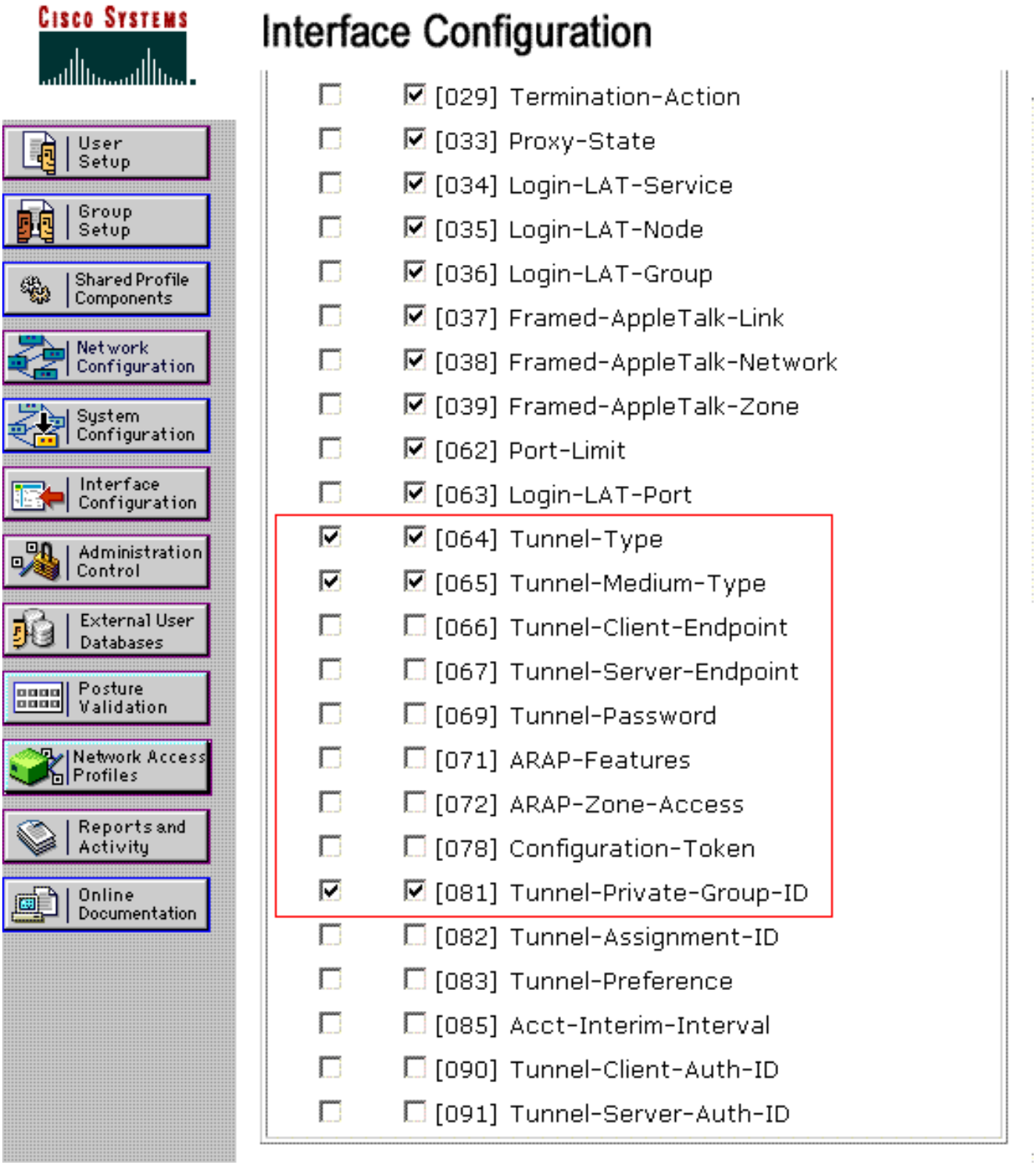


Beachten Sie in diesem Diagramm, dass das Kennwort, das Sie im Abschnitt "User Setup" (Benutzereinrichtung) angeben, mit dem identisch sein sollte, das Sie während der Benutzerauthentifizierung auf der Clientseite angegeben haben.

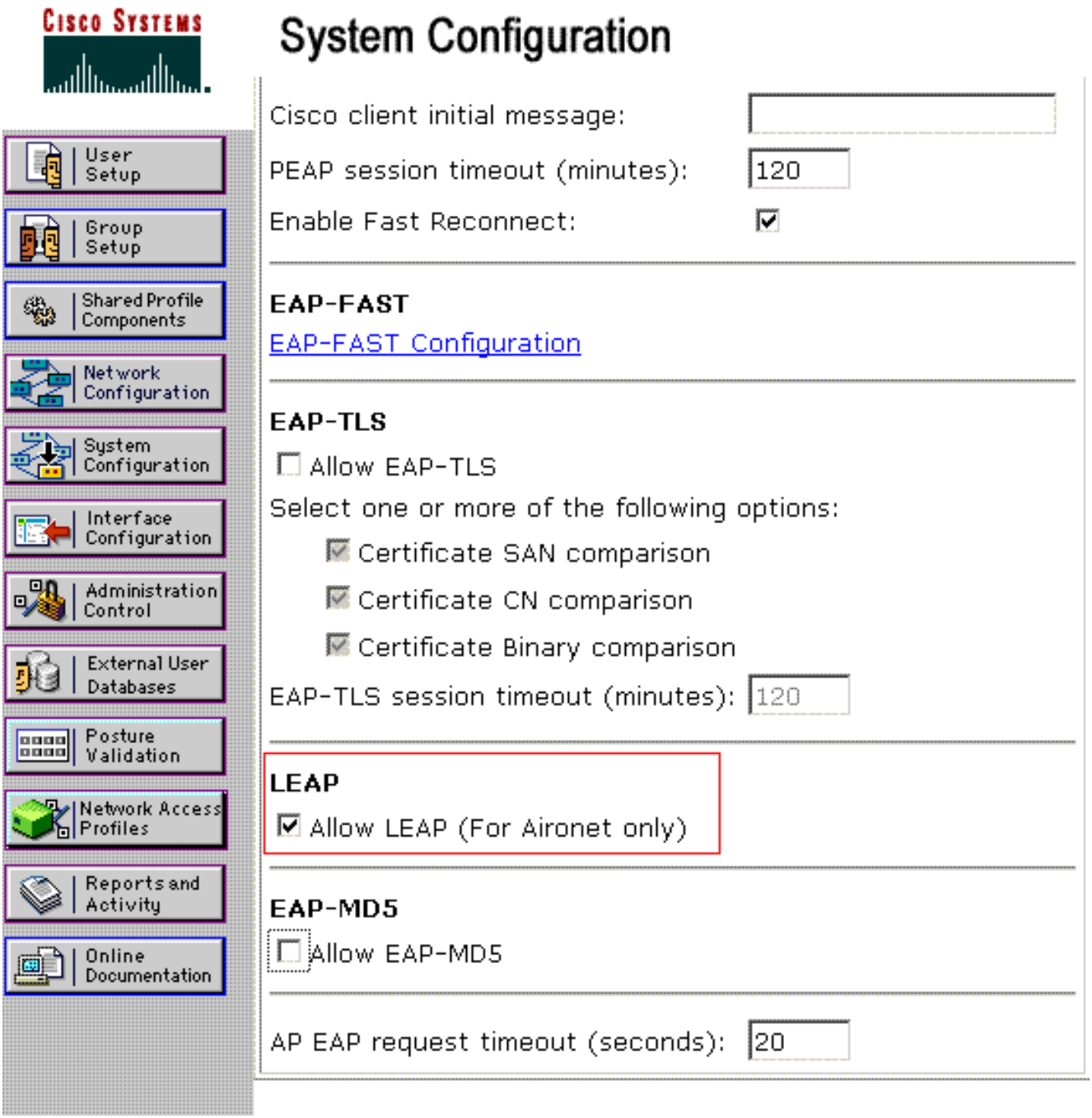
4. Blättern Sie auf der Seite Bearbeiten nach unten, und suchen Sie das Feld **IETF RADIUS Attributes**.
5. Aktivieren Sie im Feld IETF RADIUS Attributes (IETF-RADIUS-Attribute) die Kontrollkästchen neben den drei Tunnelattributen, und konfigurieren Sie die Attributwerte wie folgt:



Hinweis: Bei der Erstkonfiguration des ACS-Servers werden möglicherweise keine IETF-RADIUS-Attribute angezeigt.Wählen Sie **Interface Configuration > RADIUS (IETF)**, um IETF-Attribute im Fenster für die Benutzerkonfiguration zu aktivieren.Aktivieren Sie anschließend die Kontrollkästchen für die Attribute **64, 65 und 81** in den Spalten Benutzer und Gruppe.



Hinweis: Damit der RADIUS-Server den Client dynamisch einem bestimmten VLAN zuweist, **muss die im Feld "Tunnel-Private-Group-ID" (Tunnel-Private-Group-ID) des RADIUS-Servers im WLC konfigurierte VLAN-ID vorhanden sein.**Aktivieren Sie das Kontrollkästchen **Pro Benutzer TACACS+/RADIUS-**Attribut unter Schnittstellenkonfiguration > Erweiterte Optionen, um den RADIUS-Server für benutzerspezifische Konfigurationen zu aktivieren.Da LEAP als Authentifizierungsprotokoll verwendet wird, müssen Sie außerdem sicherstellen, dass LEAP im Fenster Systemkonfiguration des RADIUS-Servers wie hier gezeigt aktiviert ist:



Konfigurieren des ACS mit Cisco Application VSA-Attributen für die dynamische VLAN-Zuweisung

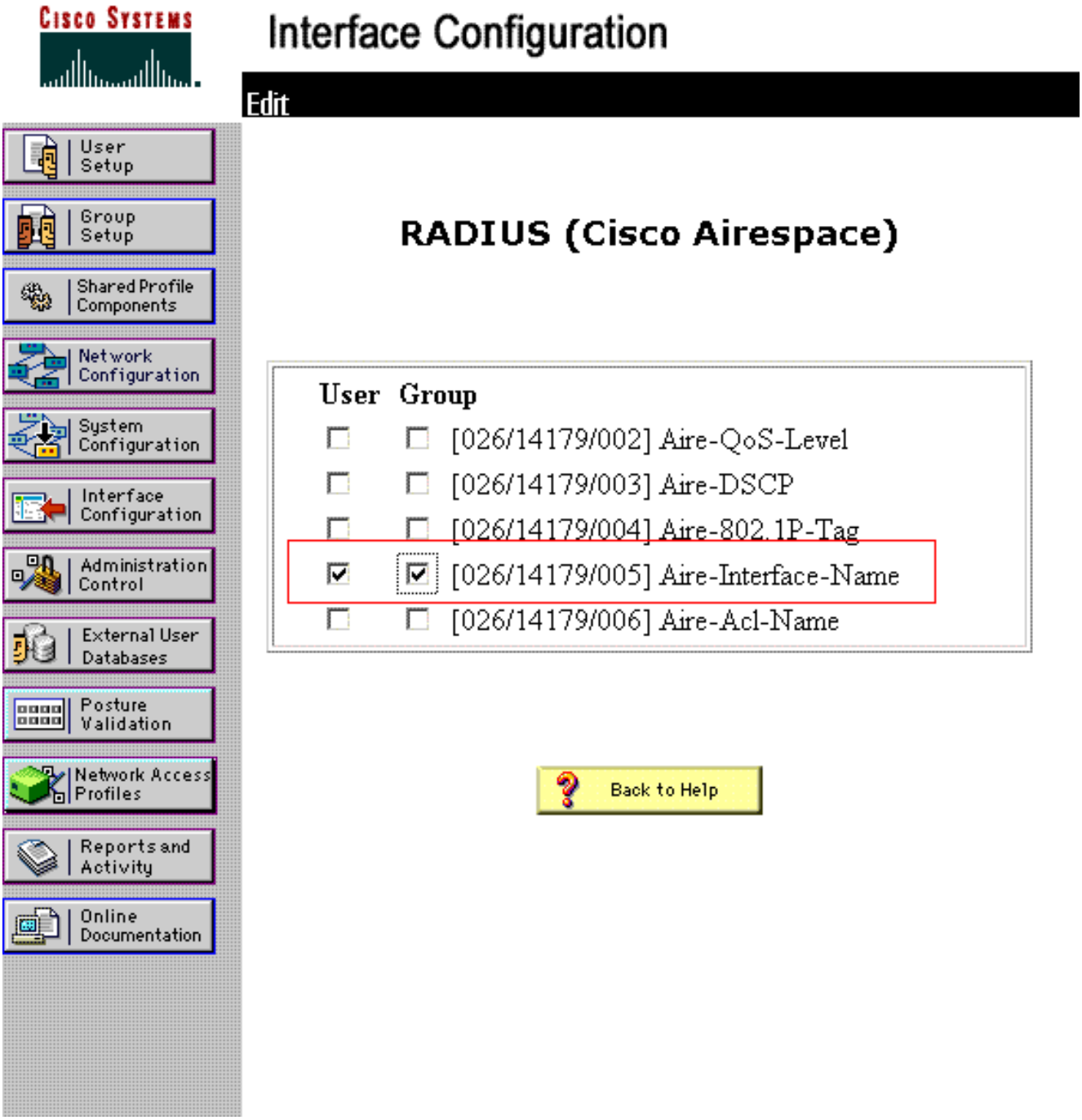
In den neuesten ACS-Versionen können Sie auch das Attribut Cisco Air [VSA (Vendor-Specific)] so konfigurieren, dass ein erfolgreich authentifizierter Benutzer mit einem VLAN-Schnittstellennamen (nicht der VLAN-ID) entsprechend der Benutzerkonfiguration auf dem ACS zugewiesen wird. Führen Sie dazu die Schritte in diesem Abschnitt aus.

Hinweis: In diesem Abschnitt wird das Cisco Airespace VSA-Attribut mit der Version ACS 4.1 konfiguriert.

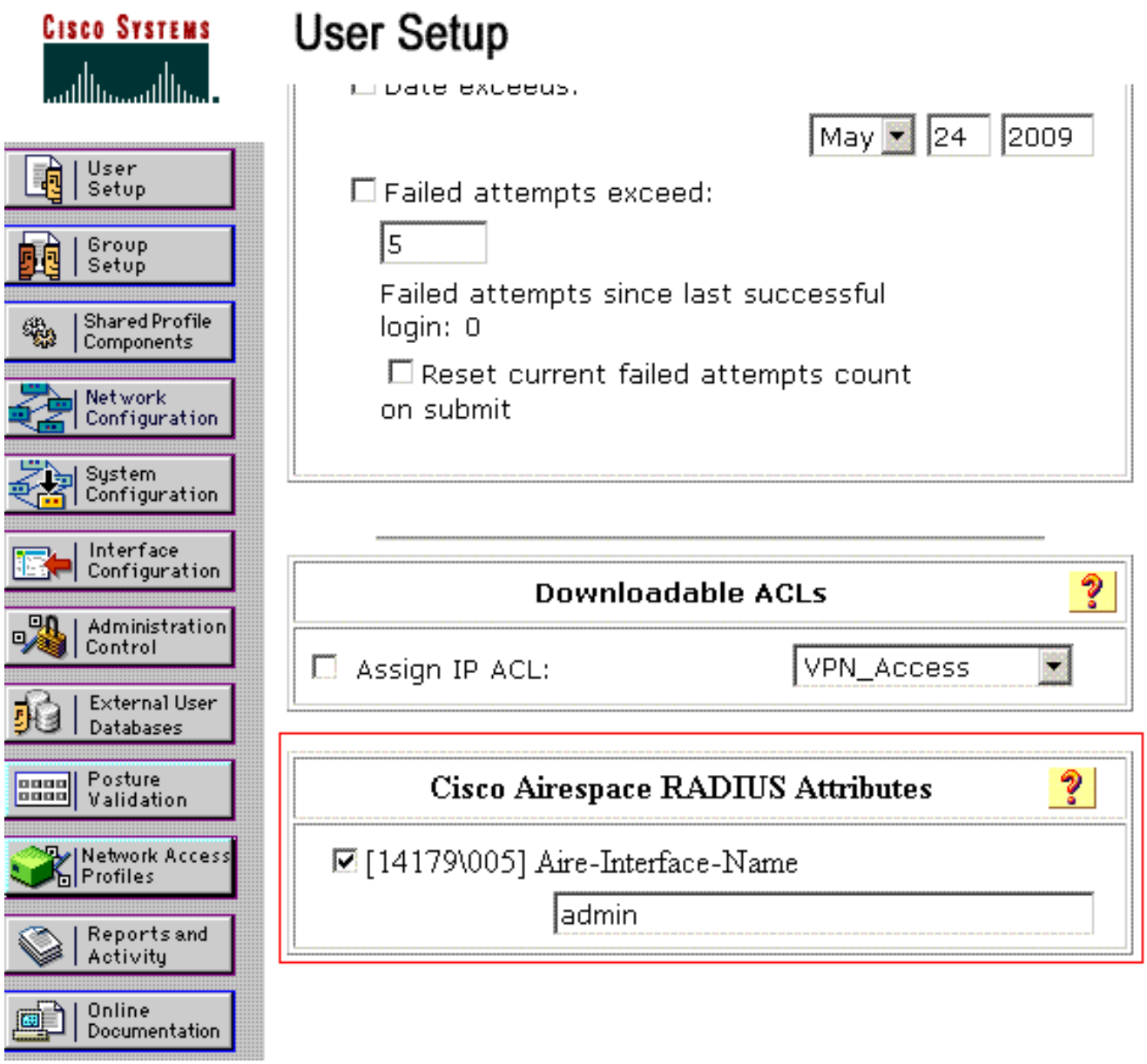
Konfigurieren Sie die ACS-Gruppe mit der Cisco Application VSA Attribute-Option.

Führen Sie diese Schritte aus:

1. Klicken Sie in der ACS 4.1-Benutzeroberfläche in der Navigationsleiste auf **Schnittstellenkonfiguration**. Wählen Sie anschließend auf der Seite "Interface Configuration" (Schnittstellenkonfiguration) **RADIUS (Cisco Air)** aus, um die Option Cisco Application-Attribut zu konfigurieren.
2. Aktivieren Sie im Fenster RADIUS (Cisco Air) das Kontrollkästchen User (Group (Gruppe), falls erforderlich) neben **Aire-Interface-Name (Aire-Schnittstellenname)**, um es auf der Seite User Edit (Benutzerbearbeitung) anzuzeigen. Klicken Sie anschließend auf **Senden**.



3. Öffnen Sie die Bearbeitungsseite von user1.
4. Blättern Sie auf der Seite "User Edit" (Benutzerbearbeitung) nach unten zum Abschnitt **Cisco Airespace RADIUS Attributes**. Aktivieren Sie das Kontrollkästchen neben dem **Aire-Interface-Name-**Attribut, und geben Sie den Namen der dynamischen Schnittstelle an, die bei erfolgreicher Benutzerauthentifizierung zugewiesen werden soll.In diesem Beispiel wird der Benutzer dem **Admin-**VLAN
zugewiesen.



5. Klicken Sie auf **Senden**.

Switch für mehrere VLANs konfigurieren

Um mehrere VLANs über den Switch zu ermöglichen, müssen Sie die folgenden Befehle ausführen, um den mit dem Controller verbundenen Switch-Port zu konfigurieren:

1. Switch(config-if)#**switchport mode trunk**
2. Switch(config-if)#**switchport trunk encapsulation dot1q**

Hinweis: Standardmäßig lassen die meisten Switches alle auf diesem Switch erstellten VLANs über den Trunk-Port zu.

Diese Befehle unterscheiden sich je nach Catalyst-Betriebssystem-Switch (CatOS).

Wenn ein kabelgebundenes Netzwerk mit dem Switch verbunden ist, kann diese Konfiguration auf den Switch-Port angewendet werden, der mit dem kabelgebundenen Netzwerk verbunden ist. Dies ermöglicht die Kommunikation zwischen den gleichen VLANs im kabelgebundenen und Wireless-Netzwerk.

Hinweis: In diesem Dokument wird die VLAN-übergreifende Kommunikation nicht behandelt. Dies

wird in diesem Dokument nicht behandelt. Sie müssen verstehen, dass für Inter-VLAN-Routing ein Layer-3-Switch oder ein externer Router mit geeigneten VLAN- und Trunking-Konfigurationen erforderlich ist. Es gibt mehrere Dokumente, in denen die Konfiguration des VLAN-übergreifenden Routings erläutert wird.

WLC-Konfiguration

Für diese Konfiguration sind folgende Schritte erforderlich:

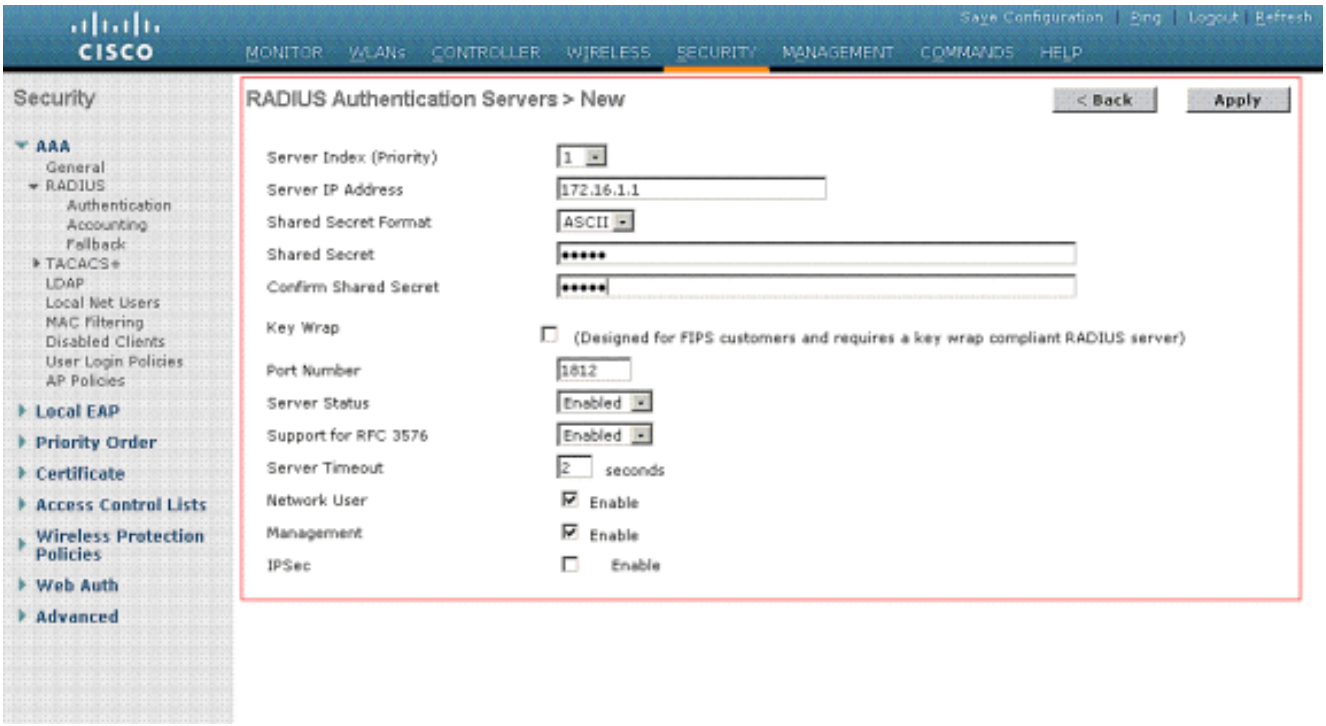
- Konfigurieren des WLC mit den Details des Authentifizierungsservers
- Konfigurieren der dynamischen Schnittstellen (VLANs)
- Konfigurieren der WLANs (SSID)

Konfigurieren des WLC mit den Details des Authentifizierungsservers

Der WLC muss so konfiguriert werden, dass er mit dem RADIUS-Server kommunizieren kann, um die Clients zu authentifizieren. Dies gilt auch für alle anderen Transaktionen.

Führen Sie diese Schritte aus:

1. Klicken Sie in der Controller-GUI auf **Sicherheit**.
2. Geben Sie die IP-Adresse des RADIUS-Servers und den zwischen dem RADIUS-Server und dem WLC verwendeten Schlüssel für den gemeinsamen geheimen Schlüssel ein.Dieser Schlüssel für den gemeinsamen geheimen Schlüssel muss mit dem Schlüssel übereinstimmen, der im RADIUS-Server unter Netzwerkkonfiguration > AAA-Clients > Eintrag hinzufügen konfiguriert wurde. Im Folgenden finden Sie ein Beispielfenster vom WLC:



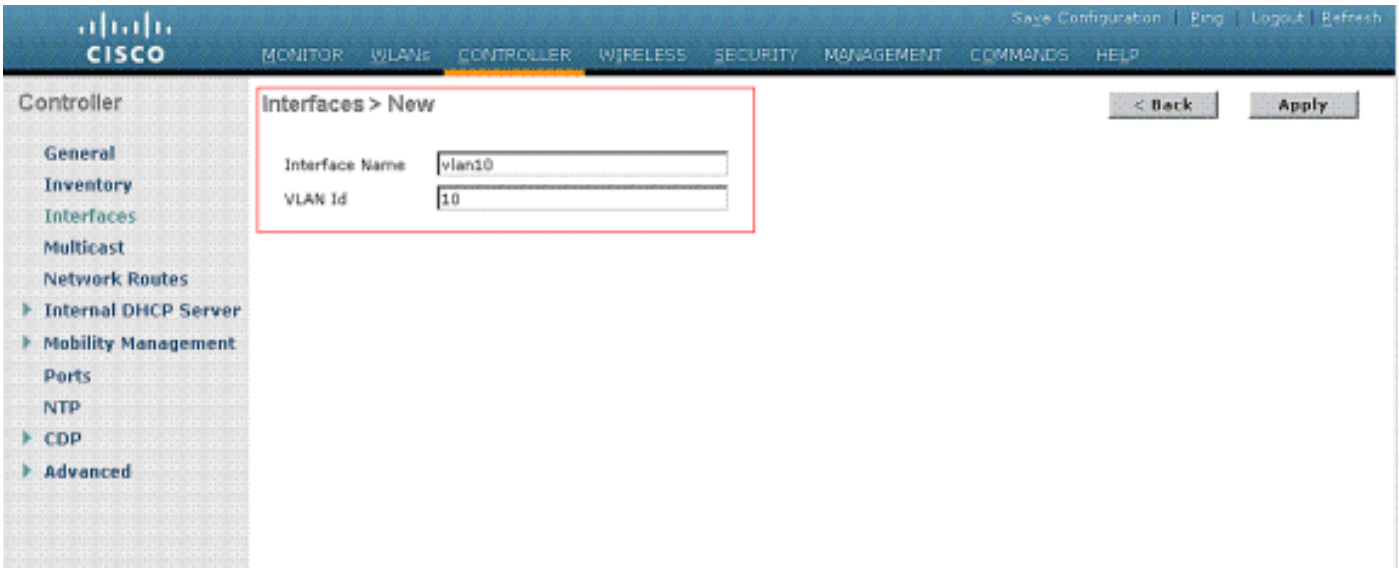
Konfigurieren der dynamischen Schnittstellen (VLANs)

In diesem Verfahren wird erläutert, wie dynamische Schnittstellen auf dem WLC konfiguriert werden. Wie bereits in diesem Dokument erläutert, muss die im Tunnel-Private-Group-ID-Attribut

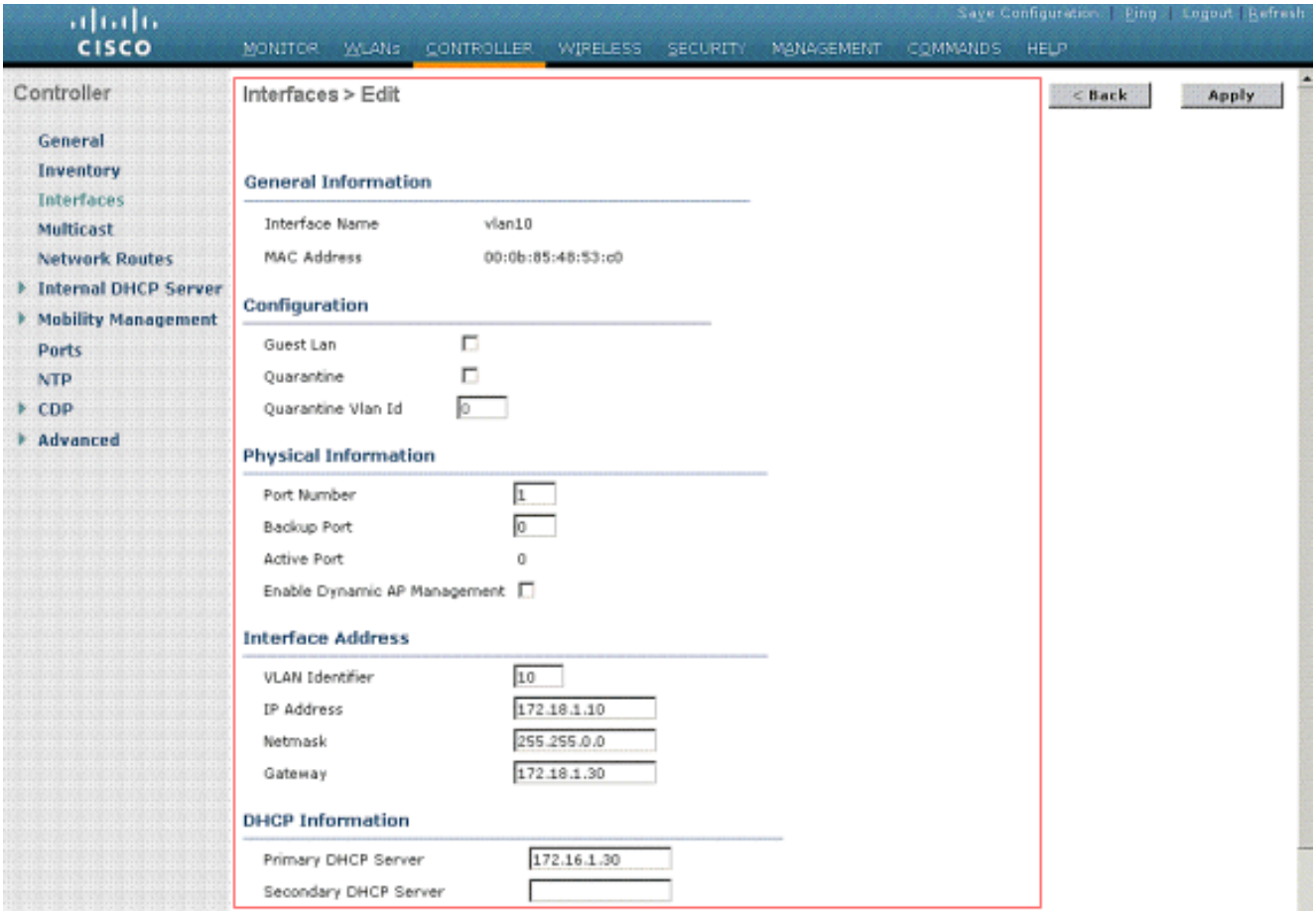
des RADIUS-Servers angegebene VLAN-ID auch im WLC vorhanden sein.

Im Beispiel wird user1 mit der **Tunnel-Private-Group-ID 10 (VLAN =10)** auf dem RADIUS-Server angegeben. Weitere Informationen finden Sie im Abschnitt IETF RADIUS Attributes im Fenster User Setup (Benutzereinrichtung) von user1.

In diesem Beispiel wird dieselbe dynamische Schnittstelle (VLAN=10) angezeigt, die im WLC konfiguriert wurde. Über die Benutzeroberfläche des Controllers wird im Fenster Controller > Interfaces (Controller > Schnittstellen) die dynamische Schnittstelle konfiguriert.



1. Klicken Sie in diesem Fenster auf **Übernehmen**.Dadurch gelangen Sie zum Bearbeitungsfenster dieser dynamischen Schnittstelle (VLAN 10 hier).
2. Geben Sie die IP-Adresse und das Standard-Gateway dieser dynamischen Schnittstelle ein.



Hinweis: Da in diesem Dokument ein interner DHCP-Server auf dem Controller verwendet wird, verweist das primäre DHCP-Serverfeld dieses Fensters auf die Verwaltungsschnittstelle des WLC selbst. Sie können für die Wireless-Clients auch einen externen DHCP-Server, einen Router oder den RADIUS-Server selbst als DHCP-Server verwenden. In solchen Fällen verweist das primäre DHCP-Serverfeld auf die IP-Adresse des Geräts, das als DHCP-Server verwendet wird. Weitere Informationen finden Sie in der Dokumentation Ihres DHCP-Servers.

3. Klicken Sie auf **Apply** (Anwenden).Jetzt ist eine dynamische Schnittstelle im WLC konfiguriert. Ebenso können Sie mehrere dynamische Schnittstellen im WLC konfigurieren. Denken Sie jedoch daran, dass dieselbe VLAN-ID auch auf dem RADIUS-Server vorhanden sein muss, damit dieses VLAN dem Client zugewiesen werden kann.

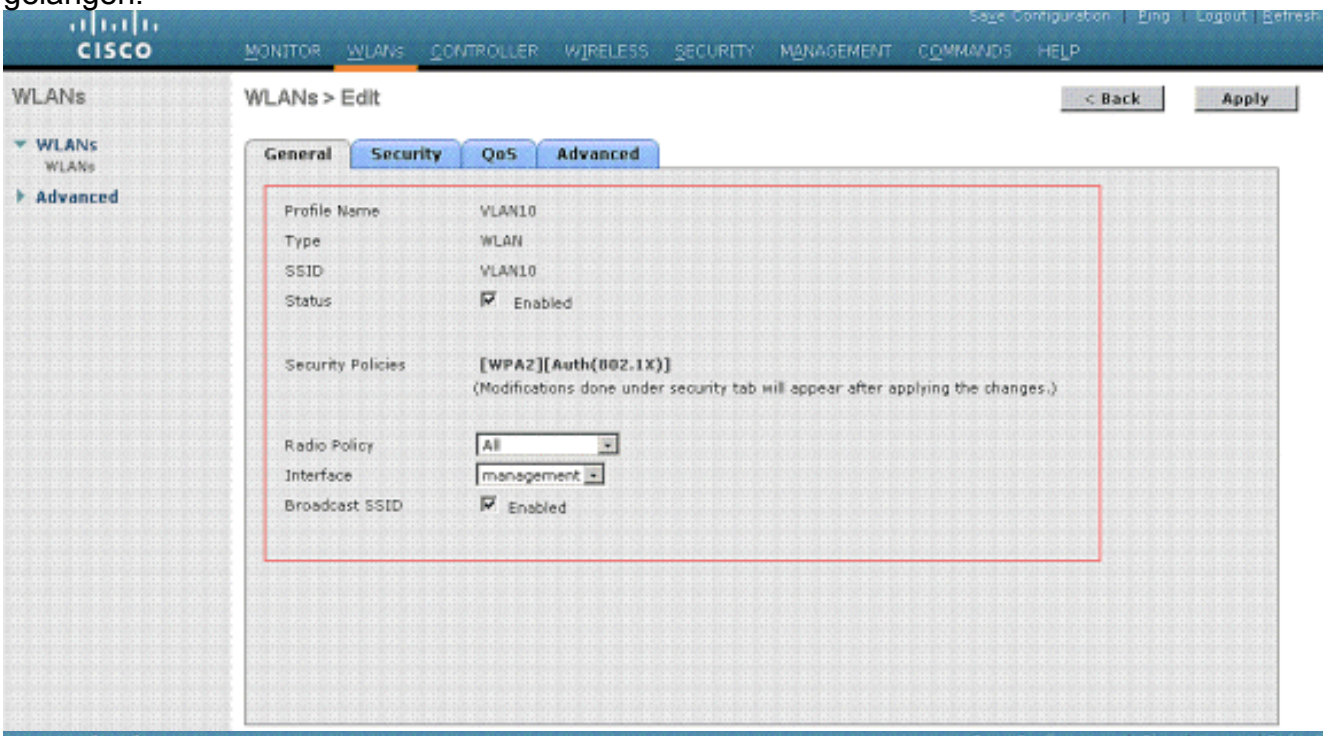
Konfigurieren der WLANs (SSID)

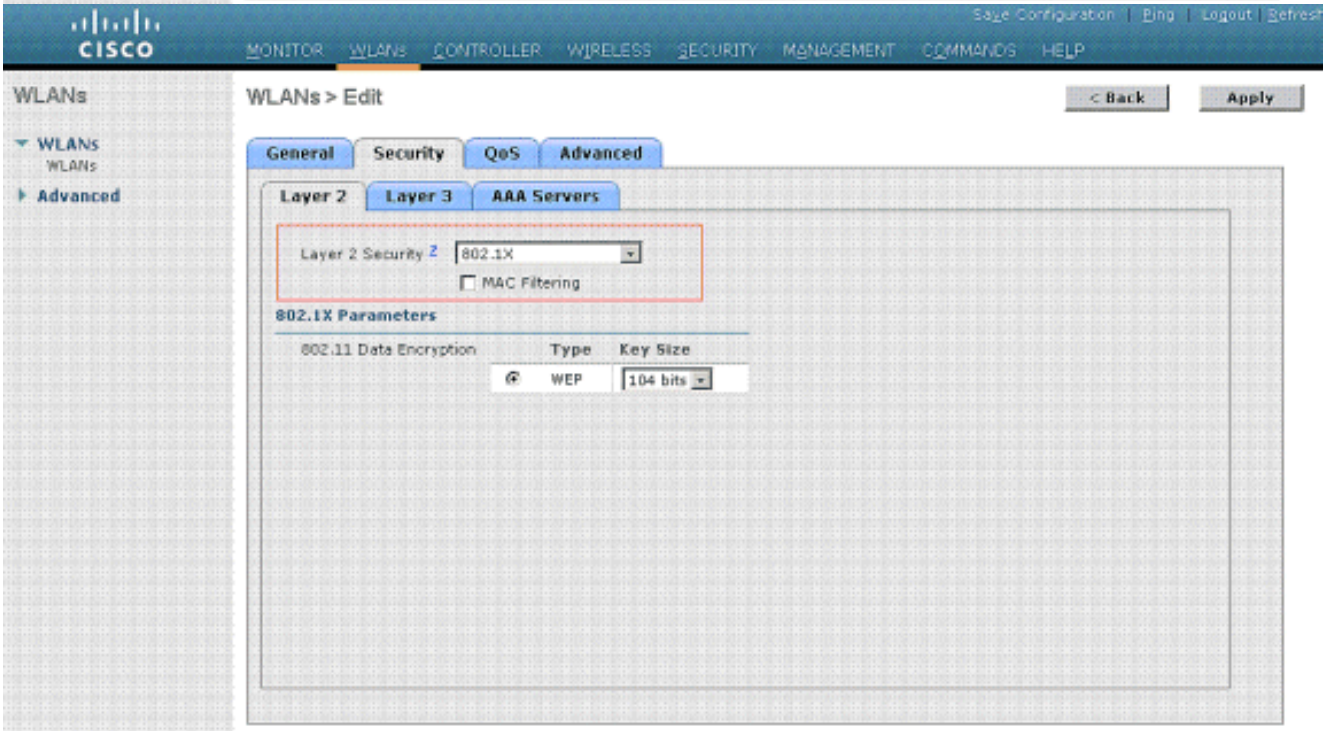
In diesem Verfahren wird erläutert, wie die WLANs im WLC konfiguriert werden.

Führen Sie diese Schritte aus:

1. Wählen Sie in der Controller-GUI **WLANs > New aus**, um ein neues WLAN zu erstellen.Das Fenster Neue WLANs wird angezeigt.
2. Geben Sie die WLAN-ID und die WLAN-SSID-Informationen ein.Sie können einen beliebigen Namen als WLAN-SSID eingeben. In diesem Beispiel wird VLAN10 als WLAN-SSID verwendet.

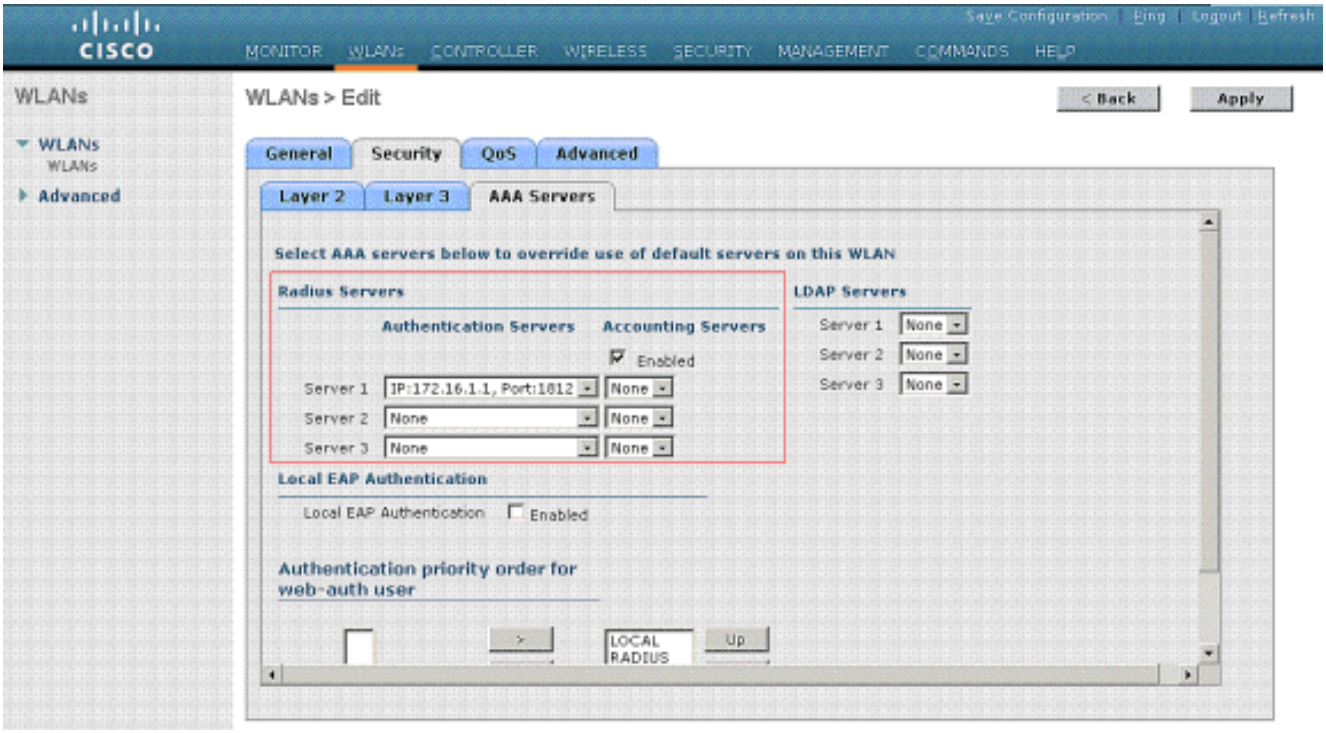
3. Klicken Sie auf **Apply**, um zum Fenster Edit des WLAN SSID10 zu gelangen.





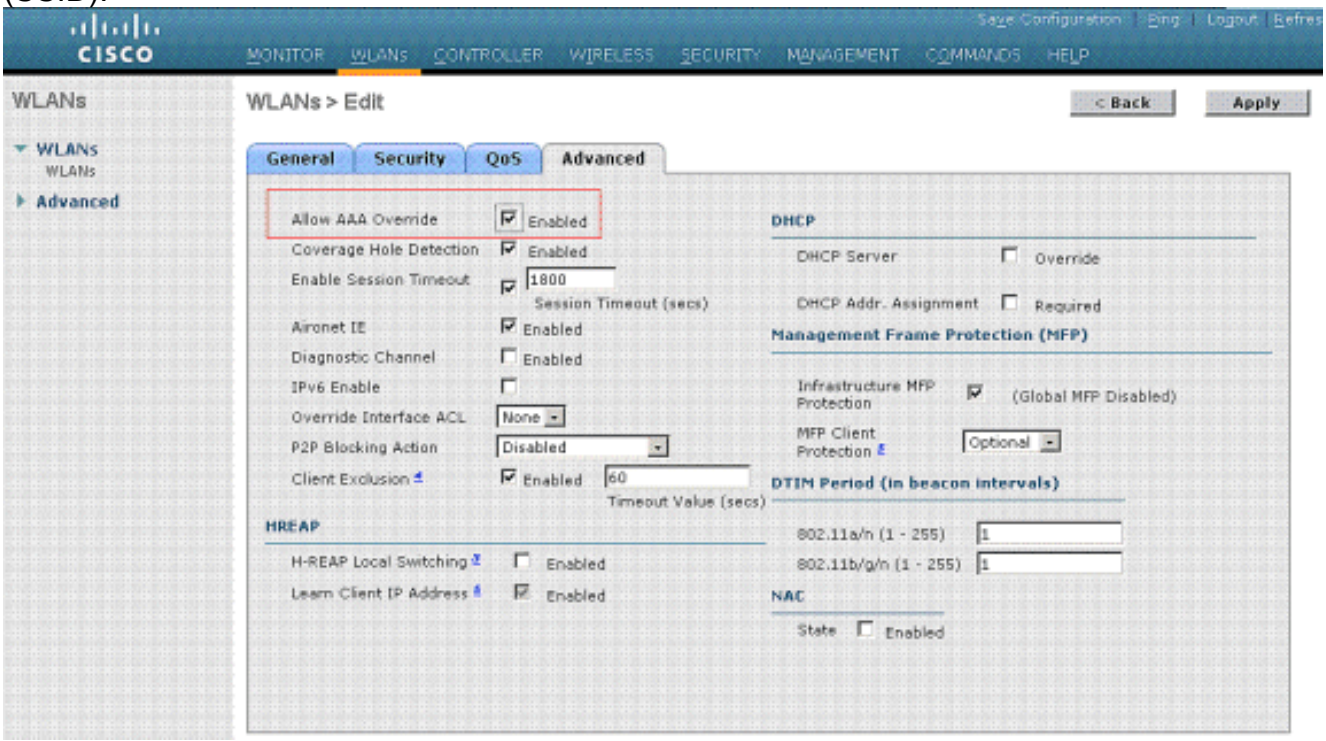
Normalerweise wird jedes WLAN in einem WLAN-Controller einem spezifischen VLAN (SSID) zugeordnet, sodass ein bestimmter Benutzer, der zu diesem WLAN gehört, in das zugeordnete VLAN aufgenommen wird. Diese Zuordnung erfolgt normalerweise im Feld Schnittstellenname des Fensters WLAN

SSID.



Im angegebenen Beispiel ist es die Aufgabe des RADIUS-Servers, nach erfolgreicher Authentifizierung einem bestimmten VLAN einen Wireless-Client zuzuweisen. Die WLANs müssen keiner spezifischen dynamischen Schnittstelle im WLC zugeordnet werden. Auch wenn das WLAN der dynamischen Schnittstellenzuordnung auf dem WLC zugeordnet wird, überschreibt der RADIUS-Server diese Zuordnung und weist den Benutzer, der über dieses WLAN erfolgt, dem VLAN zu, das im Feld "**Tunnel-Group-Private-ID**" des RADIUS-Servers angegeben wird.

4. Aktivieren Sie das Kontrollkästchen **AAA Override zulassen**, um die WLC-Konfigurationen durch den RADIUS-Server zu überschreiben.
5. Aktivieren Sie die Option AAA Override zulassen im Controller für jedes konfigurierte WLAN (SSID).



Wenn AAA Override aktiviert ist und ein Client über AAA- und Controller-WLAN-

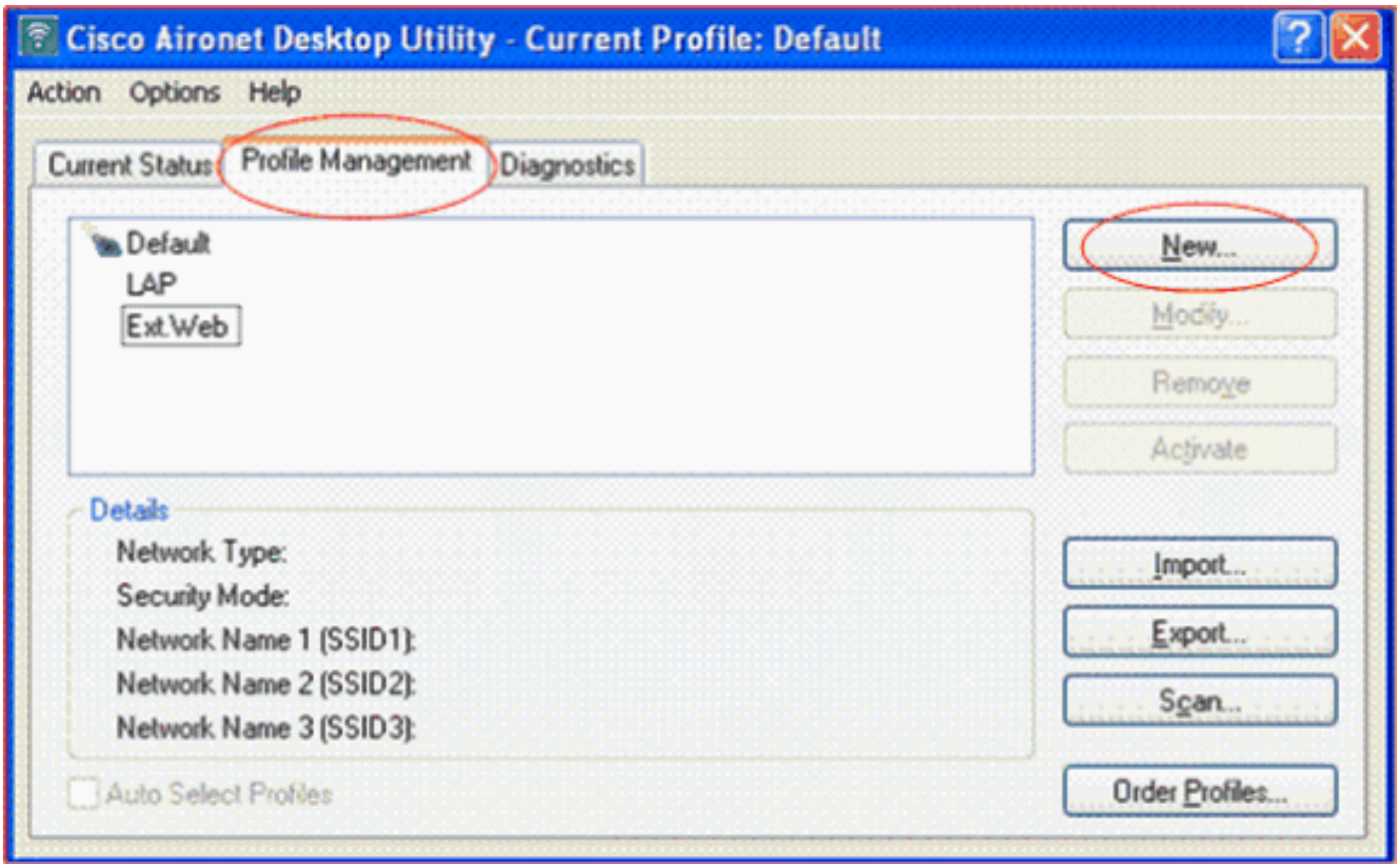
Authentifizierungsparameter verfügt, die Konflikte verursachen, wird die Client-Authentifizierung vom AAA-Server (RADIUS) durchgeführt. Im Rahmen dieser Authentifizierung verschiebt das Betriebssystem Clients zu einem VLAN, das vom AAA-Server zurückgegeben wird. Dies ist in der Controller-Schnittstellenkonfiguration vordefiniert.Wenn das Unternehmens-WLAN beispielsweise in erster Linie eine Management-Schnittstelle verwendet, die VLAN 2 zugewiesen ist, und wenn die AAA Override eine Umleitung zu VLAN 100 zurückgibt, leitet das Betriebssystem alle Client-Übertragungen auf VLAN 100 um, selbst wenn der physische Port, dem VLAN 100 zugewiesen ist, vorhanden ist. Wenn AAA Override deaktiviert ist, wird die gesamte Clientauthentifizierung auf die Einstellungen der Controller-Authentifizierungsparameter zurückgesetzt, und die Authentifizierung wird nur vom AAA-Server durchgeführt, wenn das Controller-WLAN keine clientspezifischen Authentifizierungsparameter enthält.

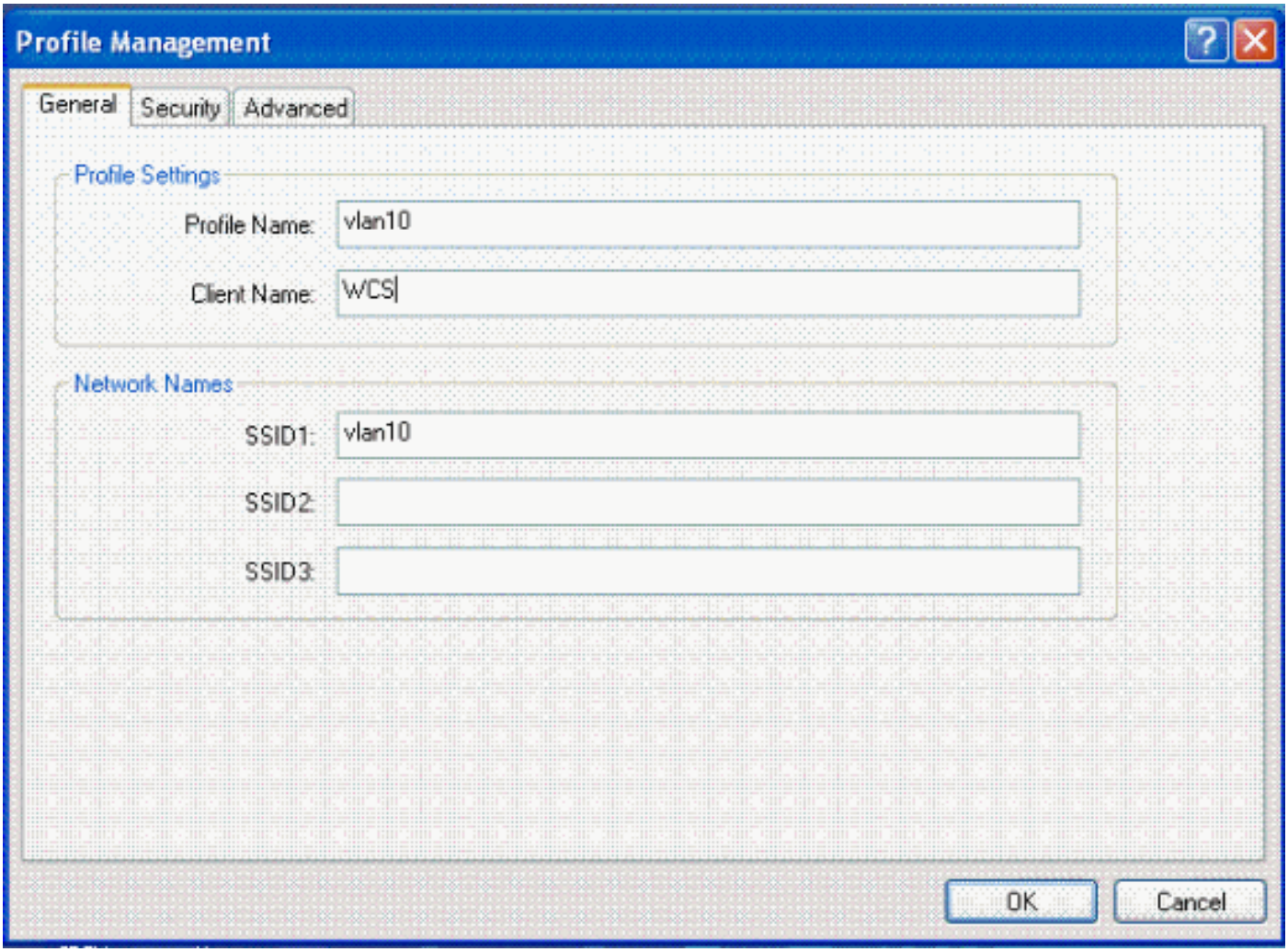
Konfiguration des Wireless-Client-Dienstprogramms

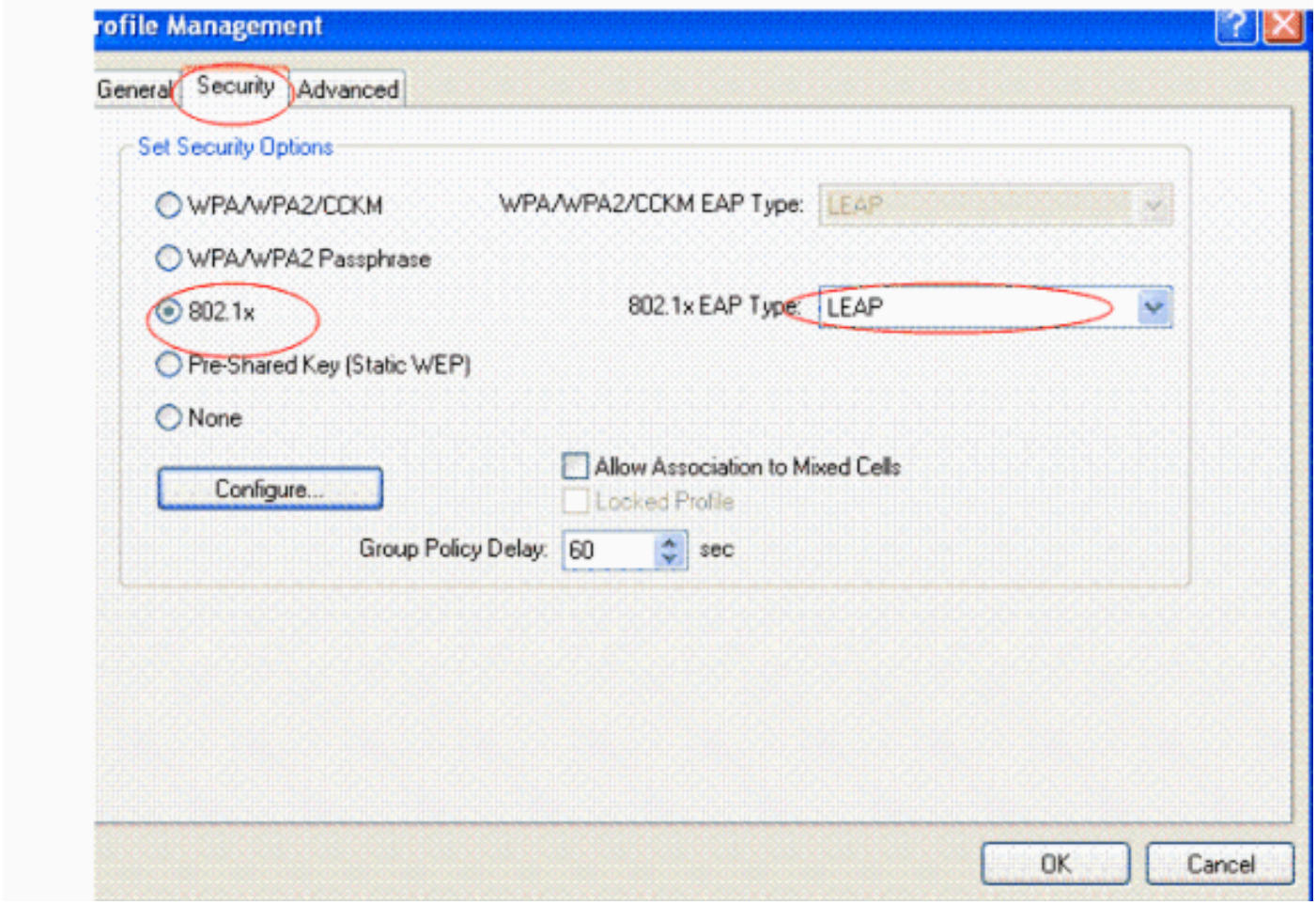
In diesem Dokument wird ADU als Client-Dienstprogramm für die Konfiguration der Benutzerprofile verwendet. Diese Konfiguration verwendet auch LEAP als Authentifizierungsprotokoll. Konfigurieren Sie die ADU wie im Beispiel in diesem Abschnitt gezeigt.

Wählen Sie in der ADU-Menüleiste **Profilverwaltung > Neu**, um ein neues Profil zu erstellen.

Der Beispielclient ist so konfiguriert, dass er Teil des SSID-VLAN10 ist. In diesen Diagrammen wird die Konfiguration eines Benutzerprofils auf einem Client veranschaulicht:




Profile Management
General
Security
Advanced
Profile Settings
Profile Name:
vlan10
Client Name:
WCS
Network Names
SSID1:
vlan10
SSID2:
SSID3:
OK
Cancel


rofile Management
General
Security
Advanced
Set Security Options
WPA/WPA2/CCKM
WPA/WPA2/CCKM EAP Type:
LEAP
WPA/WPA2 Passphrase
802.1x
802.1x EAP Type:
LEAP
Pre-Shared Key (Static WEP)
None
Configure...
Allow Association to Mixed Cells
Locked Profile
Group Policy Delay:
60
sec
OK
Cancel

Überprüfung

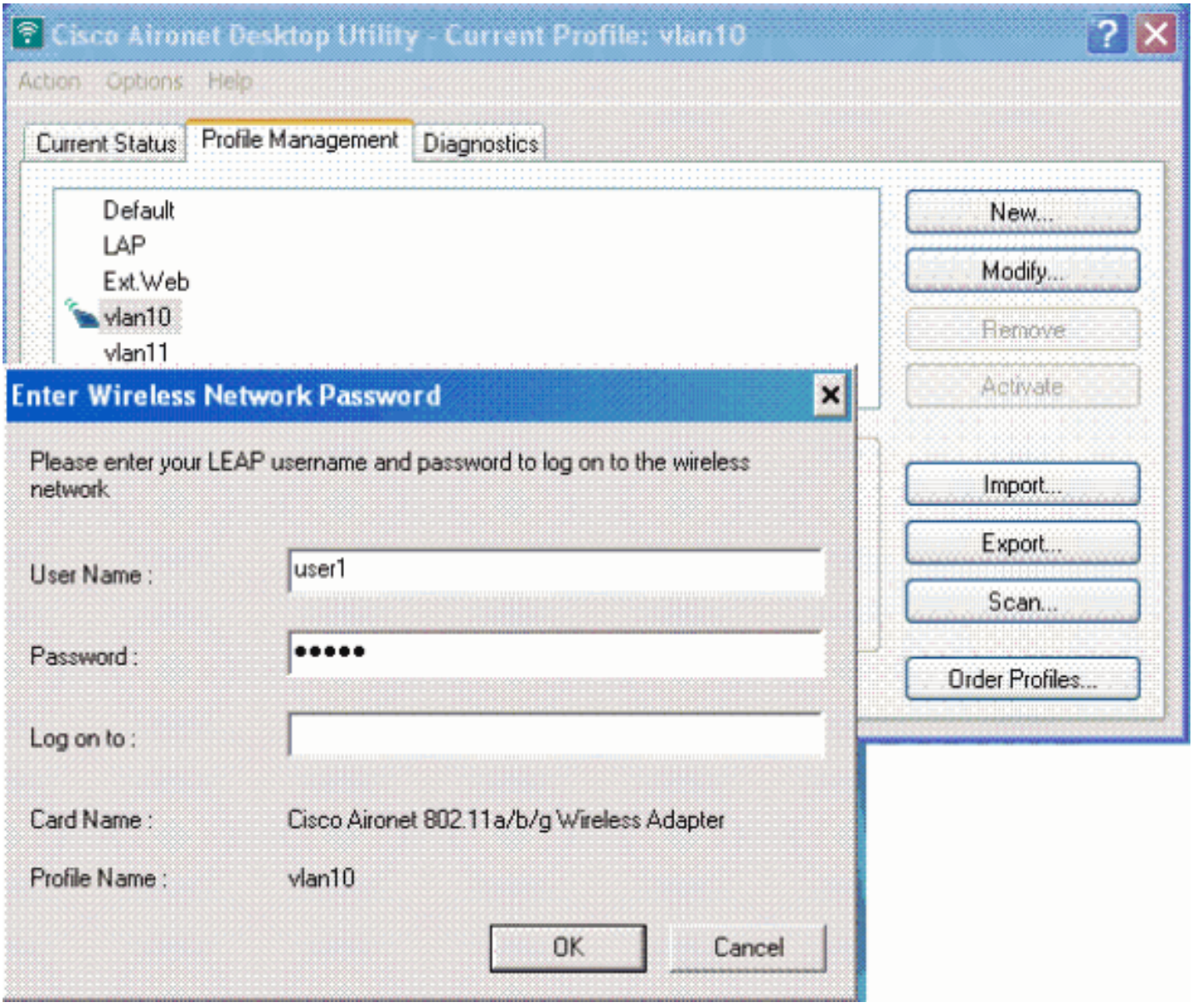
Aktivieren Sie das Benutzerprofil, das Sie in der ADU konfiguriert haben. Basierend auf der Konfiguration werden Sie aufgefordert, einen Benutzernamen und ein Kennwort einzugeben. Sie können die ADU auch anweisen, den Windows-Benutzernamen und das Windows-Kennwort für die Authentifizierung zu verwenden. Es gibt eine Reihe von Optionen, über die der Client authentifiziert werden kann. Sie können diese Optionen auf der Registerkarte Sicherheit > Konfigurieren des von Ihnen erstellten Benutzerprofils konfigurieren.

Beachten Sie im vorherigen Beispiel, dass user1 dem VLAN10 zugewiesen ist, wie im RADIUS-Server angegeben.

In diesem Beispiel wird dieser Benutzername und das Kennwort vom Client verwendet, um eine Authentifizierung zu erhalten und einem VLAN vom RADIUS-Server zuzuweisen:

- Benutzername = user1
- Kennwort = Benutzer1

Dieses Beispiel zeigt, wie das SSID VLAN10 zur Eingabe von Benutzername und Kennwort aufgefordert wird. In diesem Beispiel werden Benutzername und Kennwort eingegeben:

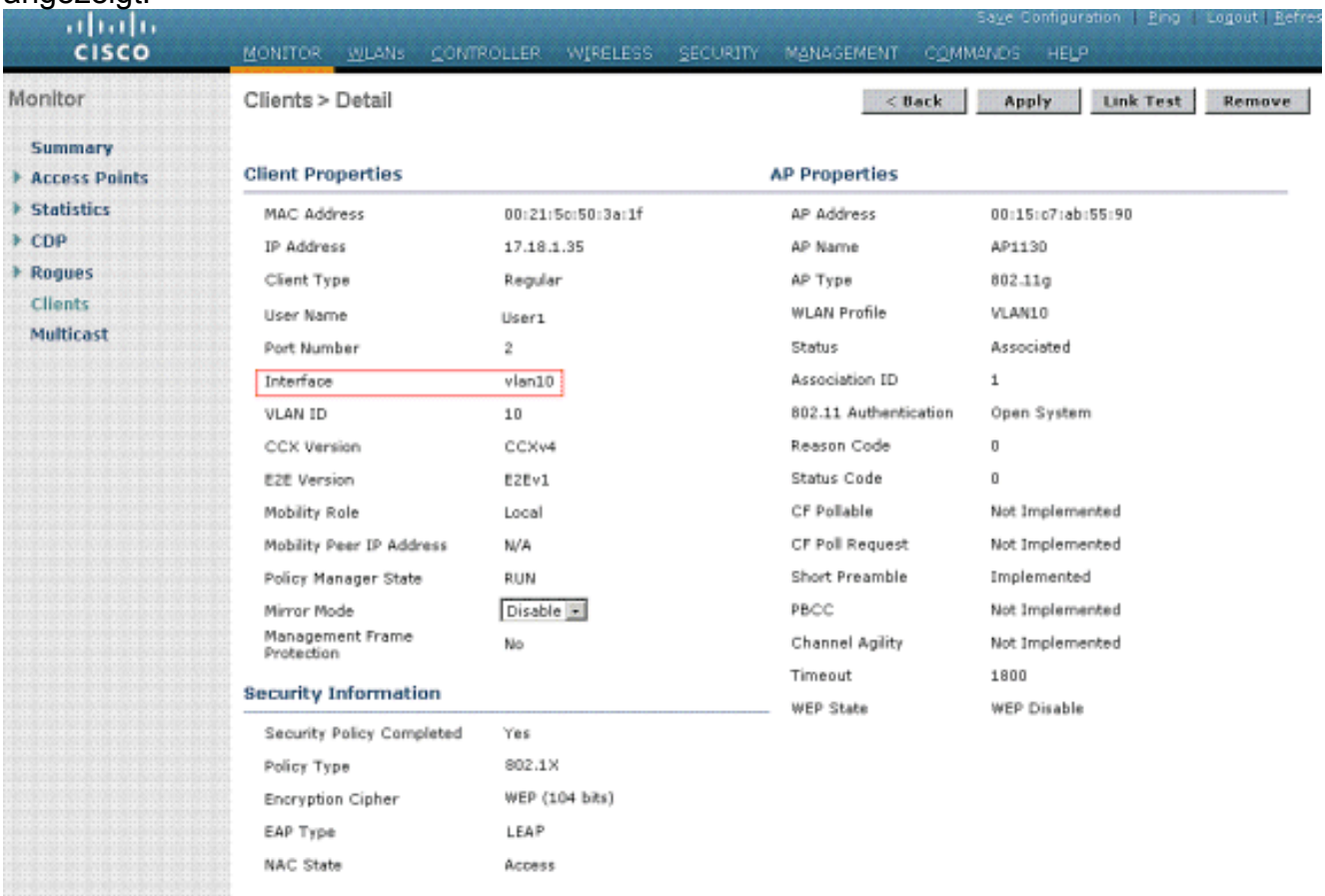


Nachdem die Authentifizierung und die entsprechende Validierung erfolgreich durchgeführt wurden, erhalten Sie als Statusmeldung Erfolg.

Anschließend müssen Sie überprüfen, ob der Client gemäß den gesendeten RADIUS-Attributen dem richtigen VLAN zugewiesen ist. Gehen Sie wie folgt vor, um Folgendes zu erreichen:

1. Wählen Sie in der Controller-GUI **Wireless > AP aus**.
2. Klicken Sie auf **Clients**, die in der linken Ecke des Fensters Access Points (APs) angezeigt wird.Die Clientstatistiken werden angezeigt.

3. Klicken Sie auf **Details**, um die vollständigen Details des Clients anzugeben, z. B. die IP-Adresse, das VLAN, dem der Client zugewiesen ist usw.In diesem Beispiel werden folgende Details des Clients, user1, angezeigt:



In diesem Fenster können Sie feststellen, dass dieser Client VLAN10 entsprechend den auf dem RADIUS-Server konfigurierten RADIUS-Attributen zugewiesen ist.**Hinweis:** Wenn die dynamische VLAN-Zuordnung auf der **Cisco Airespace VSA Attribute-**Einstellung basiert, **zeigt** der **Schnittstellenname** wie in diesem Beispiel auf der Seite mit den Client-Details **als admin an**.

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

- **debug aaa events enable**: Dieser Befehl kann verwendet werden, um die erfolgreiche Übertragung der RADIUS-Attribute über den Controller an den Client sicherzustellen. Dieser Teil der Debug-Ausgabe stellt eine erfolgreiche Übertragung der RADIUS-Attribute sicher:

```
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[0]:
attribute 64, vendorId 0, valueLen 4
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[1]:
attribute 65, vendorId 0, valueLen 4
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[2]:
attribute 81, vendorId 0, valueLen 3
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[3]:
attribute 79, vendorId 0, valueLen 32
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Received EAP Attribute
(code=2, length=32,id=0) for mobile 00:40:96:ac:e6:57
Fri Jan 20 02:25:08 2006: 00000000: 02 00 00 20 11 01 00 18
4a 27 65 69 6d e4 05 f5
........J'eim...00000010: d0 98 0c cb 1a 0c 8a 3c
........44 a9 da 6c 36 94 0a f3  <D..l6...
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[4]:
attribute 1, vendorId 9, valueLen 16
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[5]:
attribute 25, vendorId 0, valueLen 28
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[6]:
attribute 80, vendorId 0, valueLen 16
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-Type 16777229
should be 13 for STA 00:40:96:ac:e6:57
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-Medium-Type 16777222
should be 6 for STA 00:40:96:ac:e6:57
Fri Jan 20 02:30:00 2006: 00:40:96:ac:e6:57 Station 00:40:96:ac:e6:57
setting dot1x reauth timeout = 1800
```

- Diese Befehle können auch nützlich sein:**debug dot1x aaa enabledebuggen aaa pakete aktivieren**

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Hinweis: Dynamische VLAN-Zuordnung funktioniert nicht für die Webauthentifizierung von einem WLC.

Zugehörige Informationen

- EAP-Authentifizierung mit RADIUS-Server
- Cisco LEAP
- Konfigurationsleitfaden für Cisco Wireless LAN Controller, Version 4.0
- Technischer Support und Dokumentation für Cisco Systeme