Externe Webauthentifizierung mit einem RADIUS-Server

Inhalt

Einleitung

In diesem Dokument wird erläutert, wie eine externe Webauthentifizierung mit einem externen RADIUS-Server durchgeführt wird.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind, bevor Sie diese Konfiguration ausprobieren:

- Grundkenntnisse der Konfiguration von Lightweight Access Points (LAPs) und Cisco WLCs
- Kenntnisse zum Einrichten und Konfigurieren eines externen Webservers
- Informationen zur Konfiguration von Cisco Secure ACS

Verwendete Komponenten

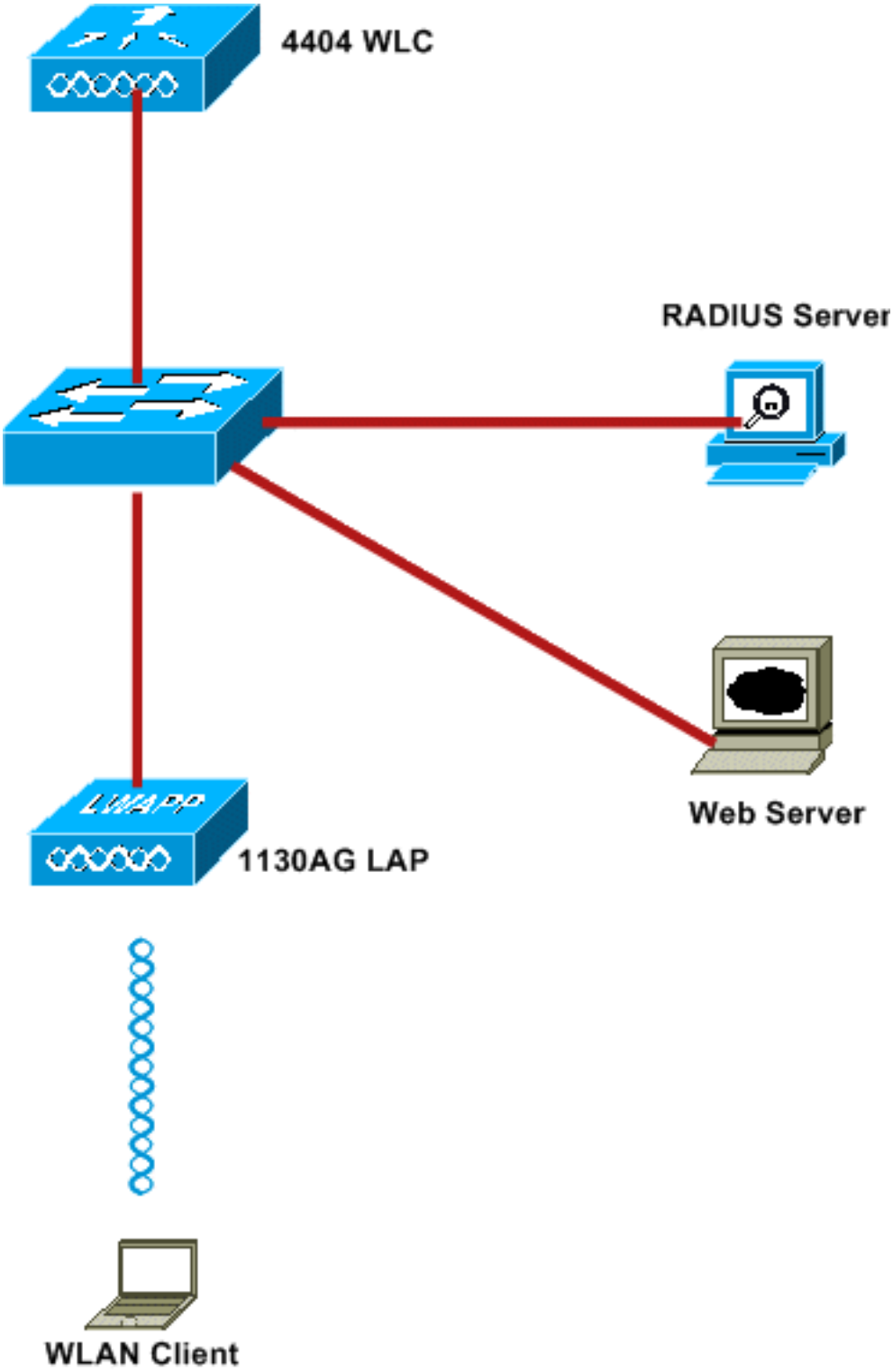
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Wireless LAN-Controller mit Firmware-Version 5.0.148.0
- Cisco Serie 1232 LAP
- Cisco 802.11a/b/g Wireless Client Adapter 3.6.0.61
- Externer Webserver, der die Anmeldeseite für die Webauthentifizierung hostet
- Cisco Secure ACS-Version mit Firmware-Version 4.1.1.24

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.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Folgende IP-Adressen werden in diesem Dokument verwendet:

- WLC verwendet die IP-Adresse 10.77.244.206
- LAP ist mit der IP-Adresse 10.77.244.199 beim WLC registriert
- Der Webserver verwendet die IP-Adresse 10.77.244.210
- Der Cisco ACS-Server verwendet die IP-Adresse 10.77.244.196
- Der Client empfängt eine IP-Adresse von der Verwaltungsschnittstelle, die dem WLAN zugeordnet ist - 10.77.244.208

Konventionen

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

Externe Webauthentifizierung

Die Webauthentifizierung ist ein Authentifizierungsmechanismus auf Layer 3, mit dem Gastbenutzer für den Internetzugriff authentifiziert werden. Benutzer, die sich mithilfe dieses Prozesses authentifiziert haben, können erst auf das Internet zugreifen, wenn sie den Authentifizierungsprozess erfolgreich abgeschlossen haben. Vollständige Informationen zum externen Web-Authentifizierungsprozess finden Sie im Abschnitt Externer Web-Authentifizierungsprozess des Dokuments Externe Web-Authentifizierung mit Wireless LAN-Controllern - Konfigurationsbeispiel.

In diesem Dokument sehen wir uns ein Konfigurationsbeispiel an, bei dem die externe Webauthentifizierung mithilfe eines externen RADIUS-Servers durchgeführt wird.

Konfigurieren des WLC

In diesem Dokument wird davon ausgegangen, dass der WLC bereits konfiguriert ist und über einen beim WLC registrierten LAP verfügt. In diesem Dokument wird weiterhin davon ausgegangen, dass der WLC für den Basisbetrieb konfiguriert ist und dass die LAPs beim WLC registriert sind. Wenn Sie ein neuer Benutzer sind, der versucht, den WLC für den Basisbetrieb mit LAPs einzurichten, finden Sie weitere Informationen unter Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC). Um die beim WLC registrierten LAPs anzuzeigen, navigieren Sie zu **Wireless > All APs**.

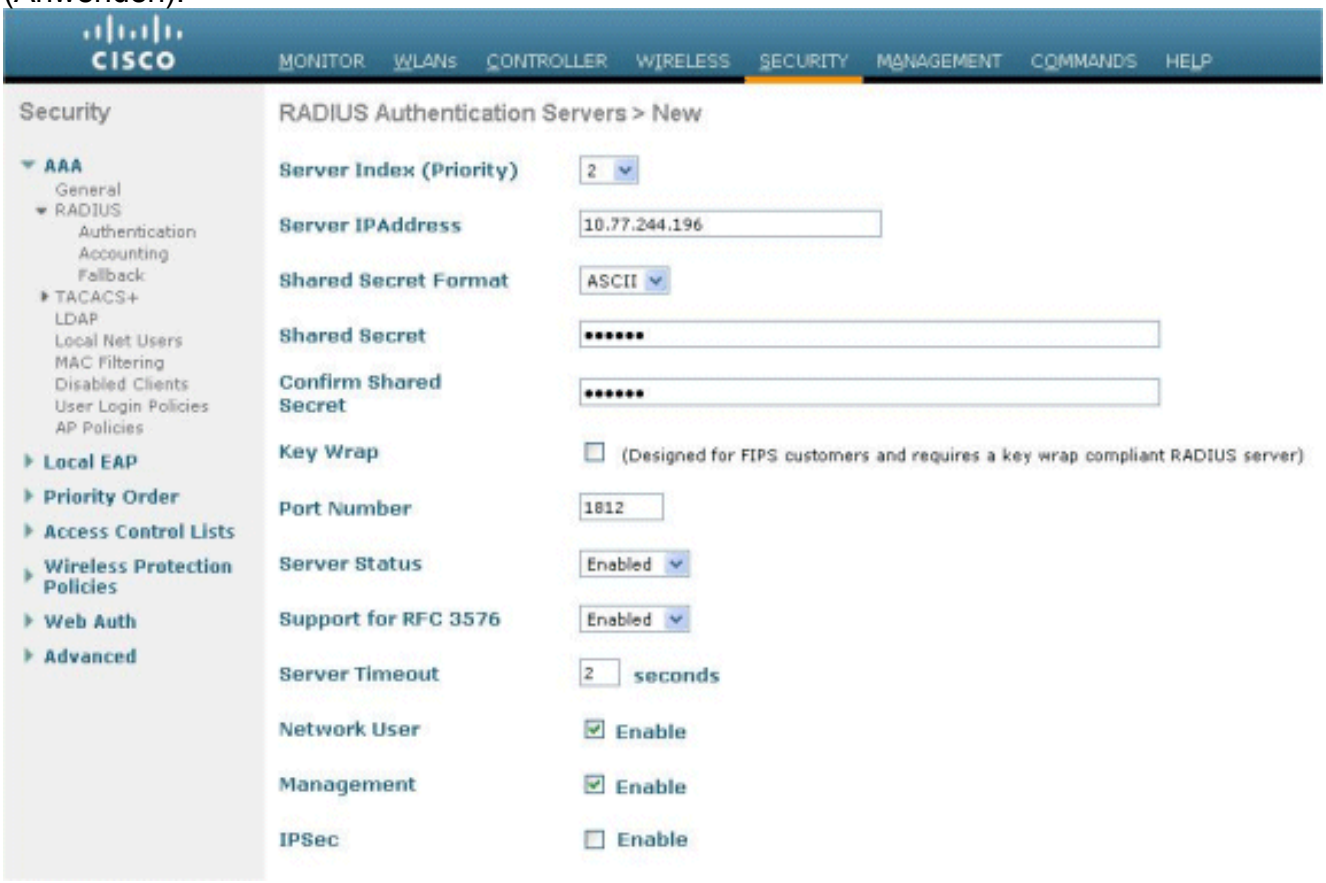
Sobald der WLC für den Basisbetrieb konfiguriert wurde und mindestens ein LAP registriert ist, können Sie den WLC mithilfe eines externen Webservers für die externe Webauthentifizierung konfigurieren. In unserem Beispiel verwenden wir einen Cisco Secure ACS 4.1.1.24 als RADIUS-Server. Zunächst konfigurieren Sie den WLC für diesen RADIUS-Server und anschließend die für diese Einrichtung erforderliche Konfiguration auf Cisco Secure ACS.

Konfigurieren des WLC für Cisco Secure ACS

Führen Sie die folgenden Schritte aus, um den RADIUS-Server dem WLC hinzuzufügen:

1. Klicken Sie in der WLC-GUI auf das Menü **SECURITY (SICHERHEIT)**.
2. Navigieren Sie im Menü **AAA** zum Untermenü **Radius > Authentication**.
3. Klicken Sie auf **Neu**, und geben Sie die IP-Adresse des RADIUS-Servers ein. In diesem Beispiel lautet die IP-Adresse des Servers *10.77.244.196*.
4. Geben Sie den gemeinsamen geheimen Schlüssel im WLC ein. Der gemeinsame geheime Schlüssel muss auf dem WLC gleich konfiguriert sein.
5. Wählen Sie als Format für den gemeinsamen geheimen Schlüssel **ASCII** oder **Hex** aus. Auf dem WLC muss das gleiche Format ausgewählt werden.
6. **1812** ist die Portnummer für die RADIUS-Authentifizierung.
7. Stellen Sie sicher, dass die Option Serverstatus auf **Aktiviert** eingestellt ist.
8. Aktivieren Sie das Kontrollkästchen Network User **Enable** (Netzwerkbenutzer aktivieren), um die Netzwerkbenutzer zu authentifizieren.
9. Klicken Sie auf **Apply**

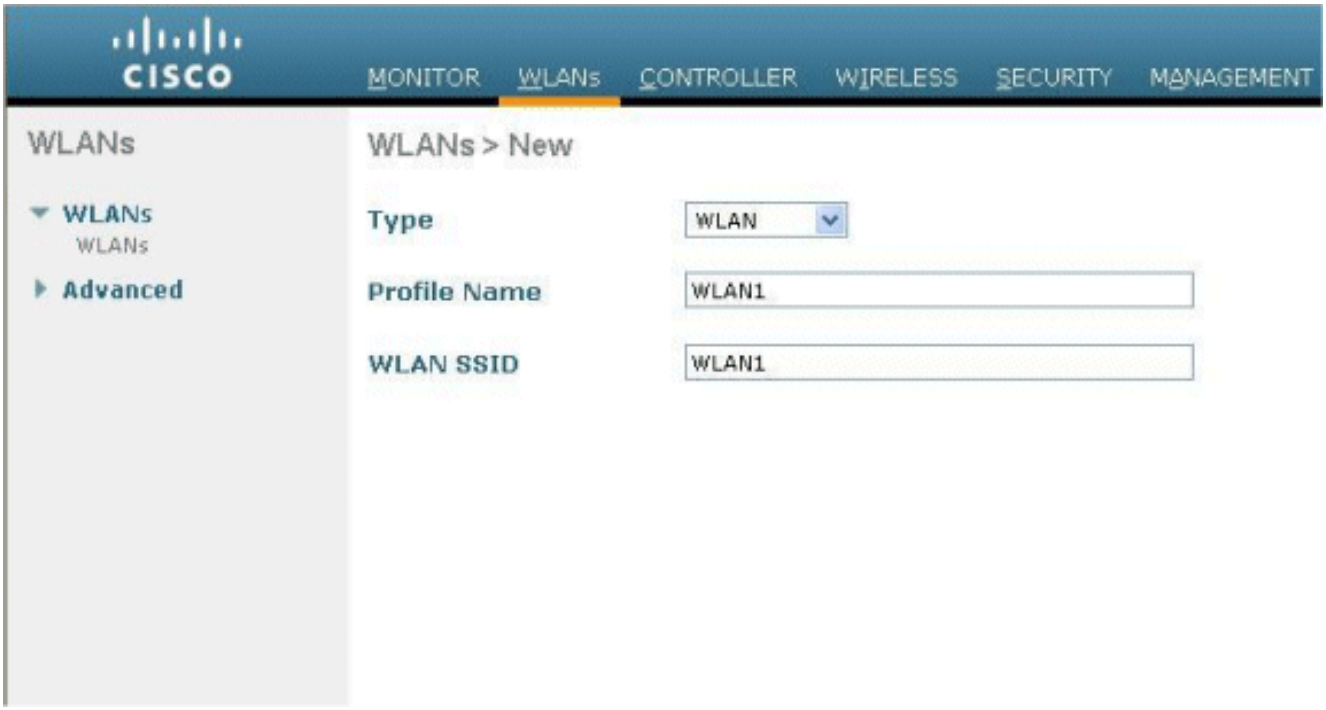
(Anwenden).



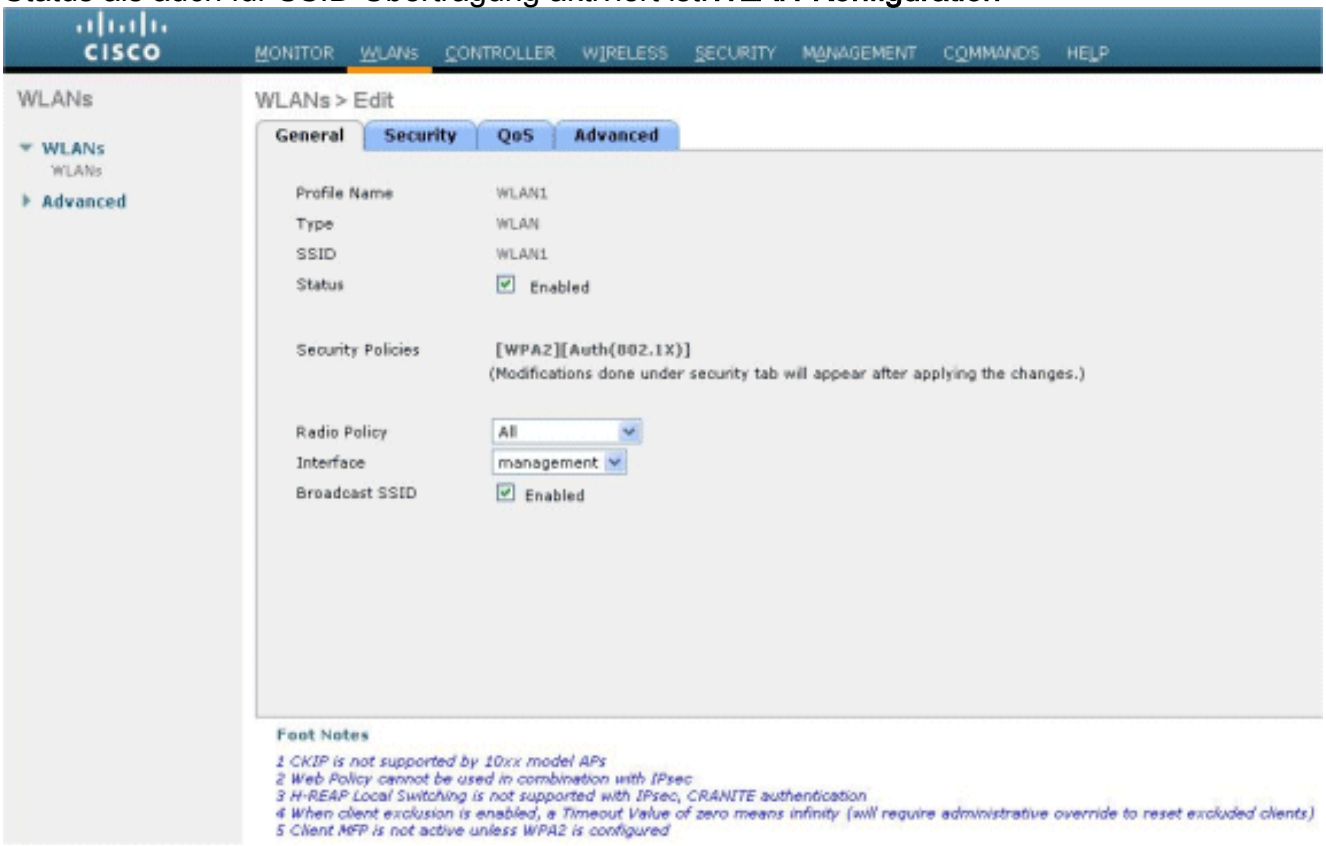
WLAN auf dem WLC für die Webauthentifizierung konfigurieren

Im nächsten Schritt wird das WLAN für die Webauthentifizierung auf dem WLC konfiguriert. Führen Sie die folgenden Schritte aus, um das WLAN auf dem WLC zu konfigurieren:

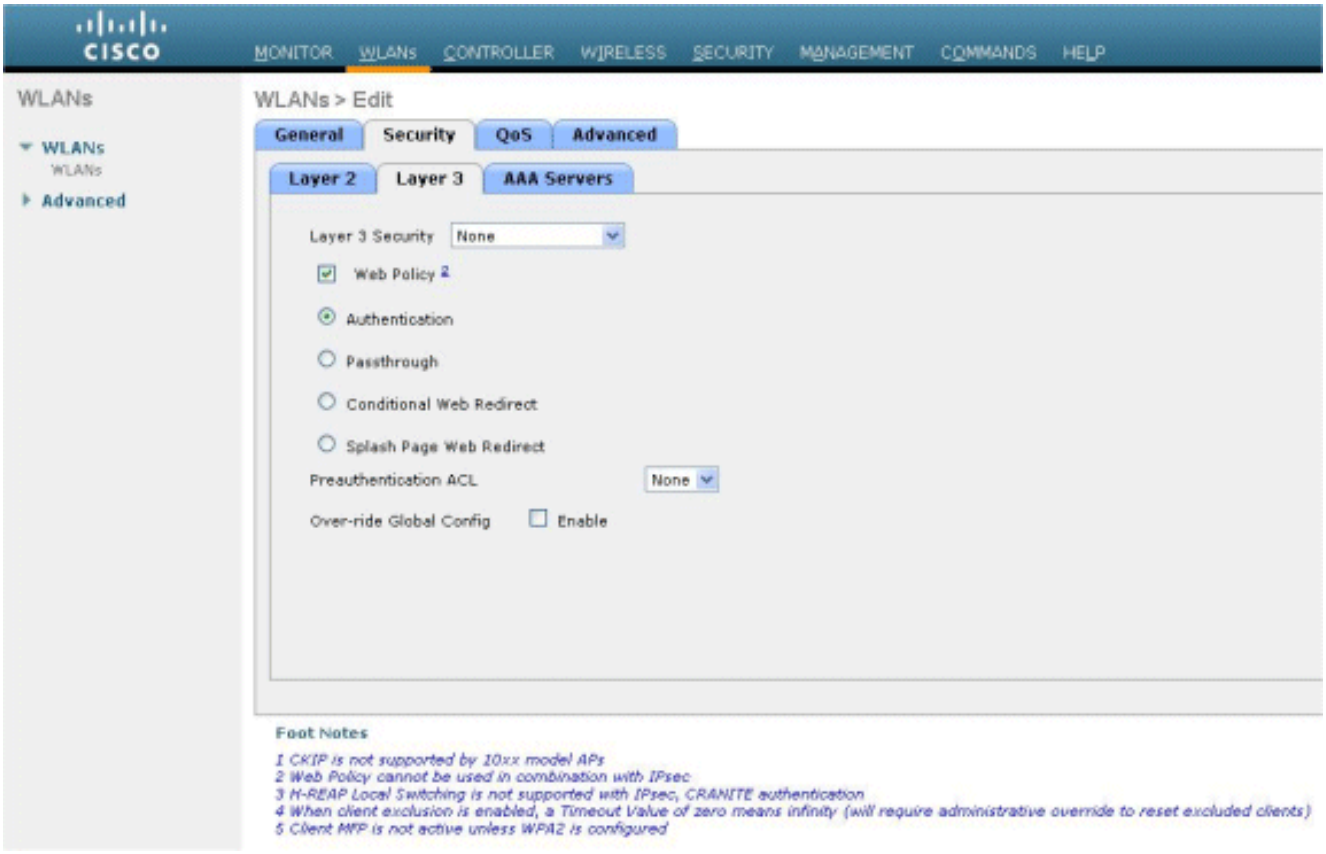
1. Klicken Sie in der Benutzeroberfläche des Controllers auf das Menü **WLANs**, und wählen Sie **Neu aus**.
2. Wählen Sie **WLAN** als Typ aus.
3. Geben Sie einen Profilnamen und einen WLAN-SSID Ihrer Wahl ein, und klicken Sie auf **Apply**.**Hinweis:** Bei der WLAN-SSID wird die Groß-/Kleinschreibung beachtet.



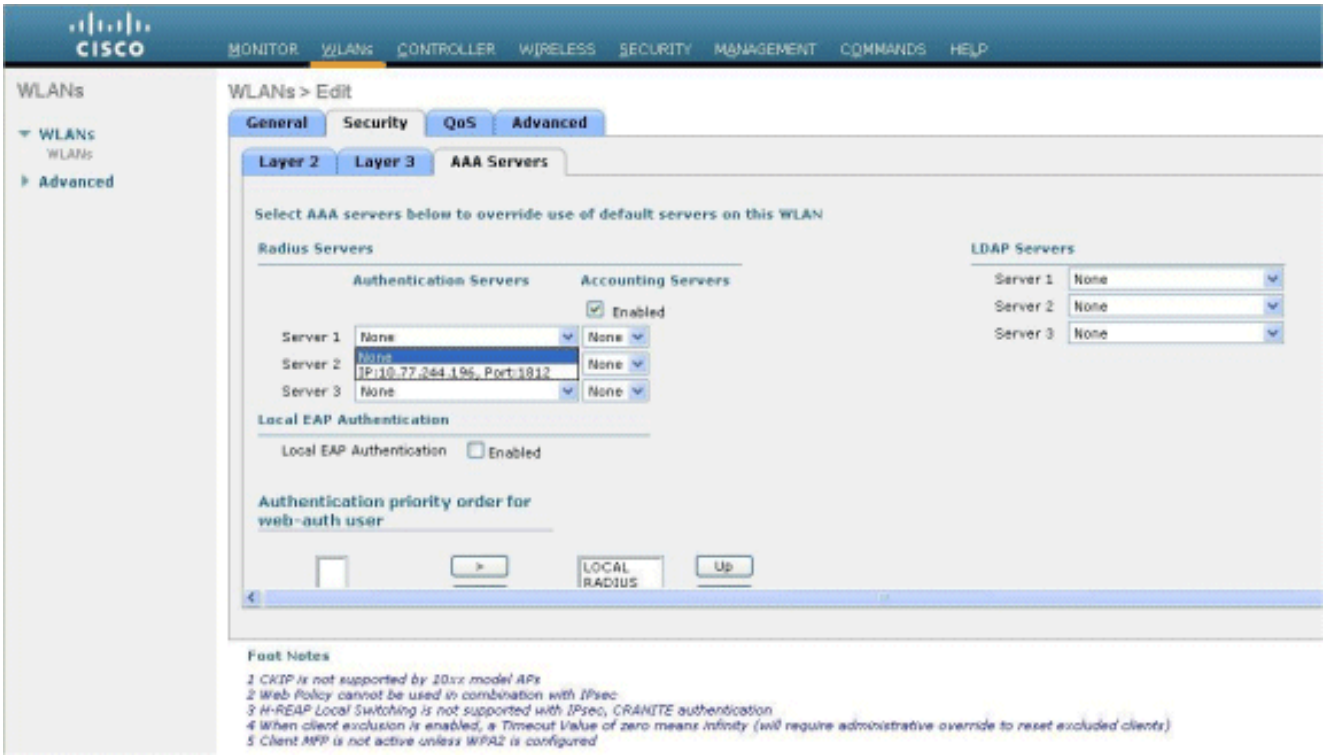
4. Vergewissern Sie sich auf der Registerkarte **Allgemein**, dass die Option **Aktiviert** sowohl für Status als auch für SSID-Übertragung aktiviert ist.**WLAN-Konfiguration**



5. Wählen Sie eine Schnittstelle für das WLAN aus. In der Regel wird dem WLAN eine Schnittstelle zugeordnet, die in einem eindeutigen VLAN konfiguriert ist, sodass der Client eine IP-Adresse in diesem VLAN erhält. In diesem Beispiel wird *Management* für Interface verwendet.
6. Wählen Sie die Registerkarte **Sicherheit**.
7. Wählen Sie im Menü **Layer 2** die Option **Keine** für die Layer-2-Sicherheit.
8. Wählen Sie im Menü **Layer 3** die Option **Keine** für die Layer-3-Sicherheit. Aktivieren Sie das Kontrollkästchen **Webrichtlinie**, und wählen Sie **Authentifizierung aus**.



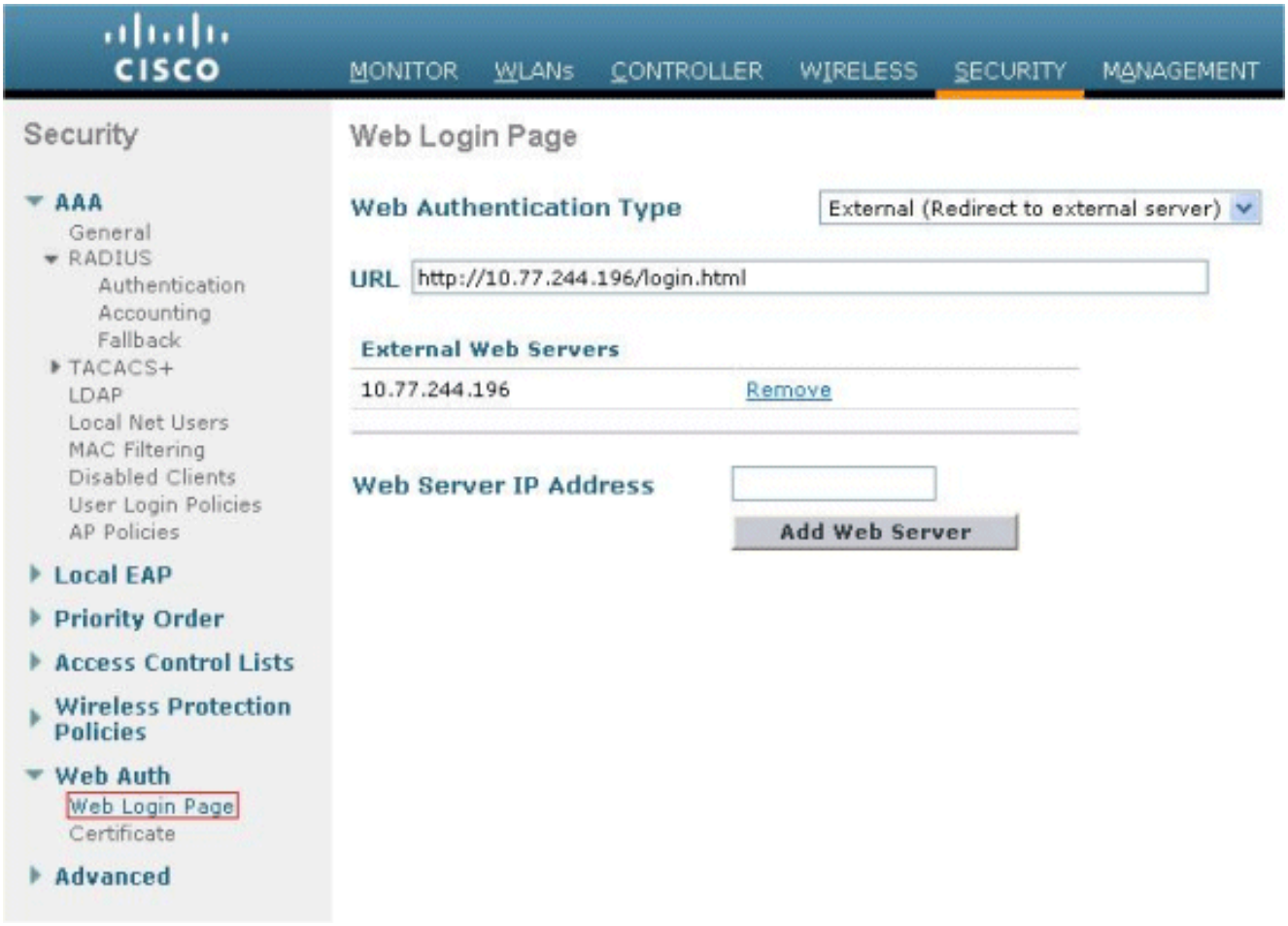
9. Wählen Sie im Menü **AAA-Server** für den Authentifizierungsserver den RADIUS-Server aus, der auf diesem WLC konfiguriert wurde. Für andere Menüs sollten die Standardwerte beibehalten
werden.



Webserverinformationen auf WLC konfigurieren

Der Webserver, der die Seite für die Webauthentifizierung hostet, sollte auf dem WLC konfiguriert werden. Führen Sie die folgenden Schritte aus, um den Webserver zu konfigurieren:

1. Klicken Sie auf die Registerkarte **Sicherheit**. Gehen Sie zu **Web Auth > Web Login Page**.
2. Legen Sie den Web-Authentifizierungstyp auf **"Extern" fest**.
3. Geben Sie im Feld IP-Adresse des Webservers die IP-Adresse des Servers ein, der die Seite Webauthentifizierung hostet, und klicken Sie auf **Webserver hinzufügen**. In diesem Beispiel ist die IP-Adresse *10.77.244.196*, die unter Externe Webserver angezeigt wird.
4. Geben Sie die URL für die Seite für die Webauthentifizierung (in diesem Beispiel *http://10.77.244.196/login.html)* in das URL-Feld ein.



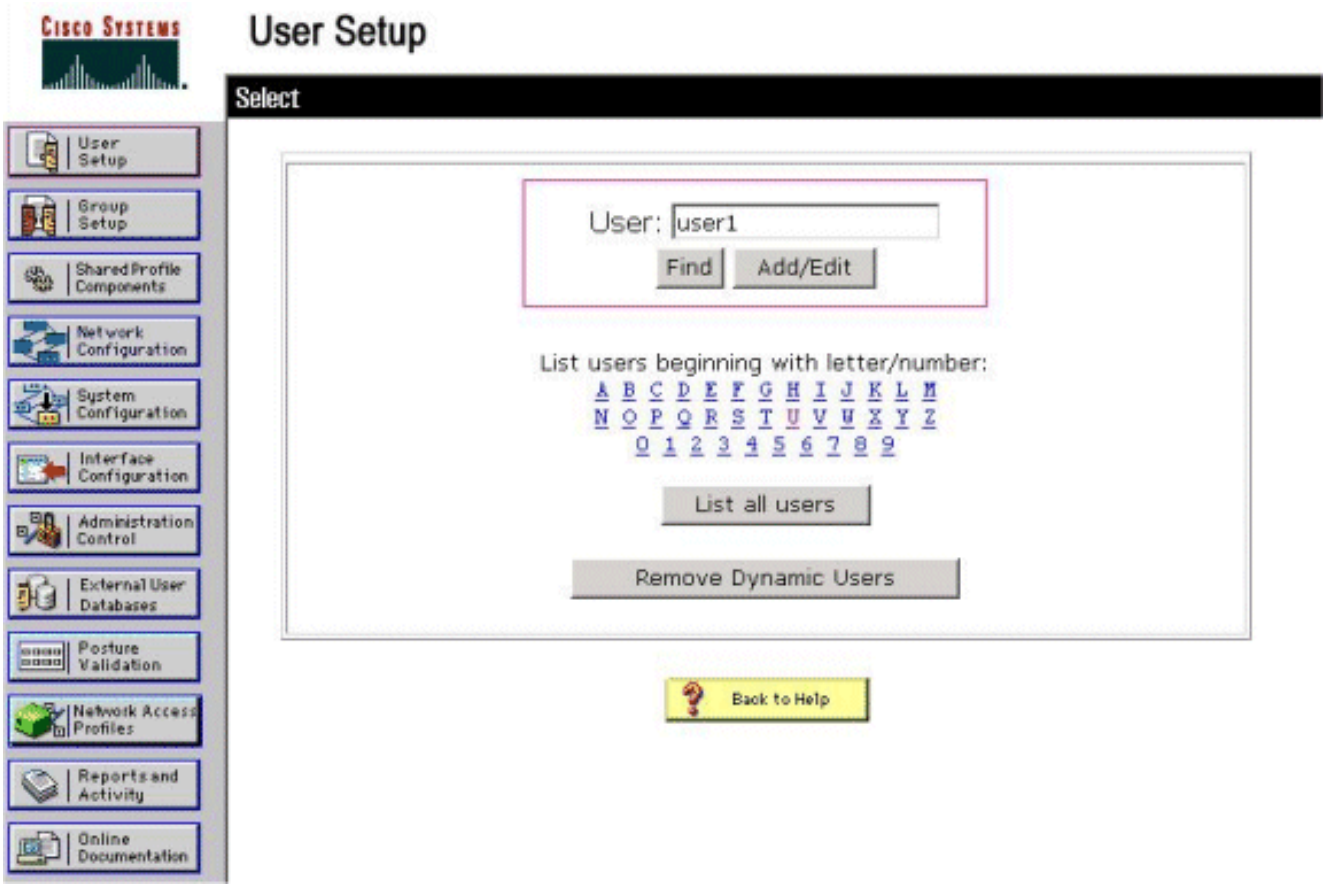
Konfigurieren von Cisco Secure ACS

In diesem Dokument wird davon ausgegangen, dass Cisco Secure ACS Server bereits auf einem Computer installiert ist und ausgeführt wird. Weitere Informationen zur Einrichtung von Cisco Secure ACS finden Sie im Konfigurationsleitfaden für Cisco Secure ACS 4.2.

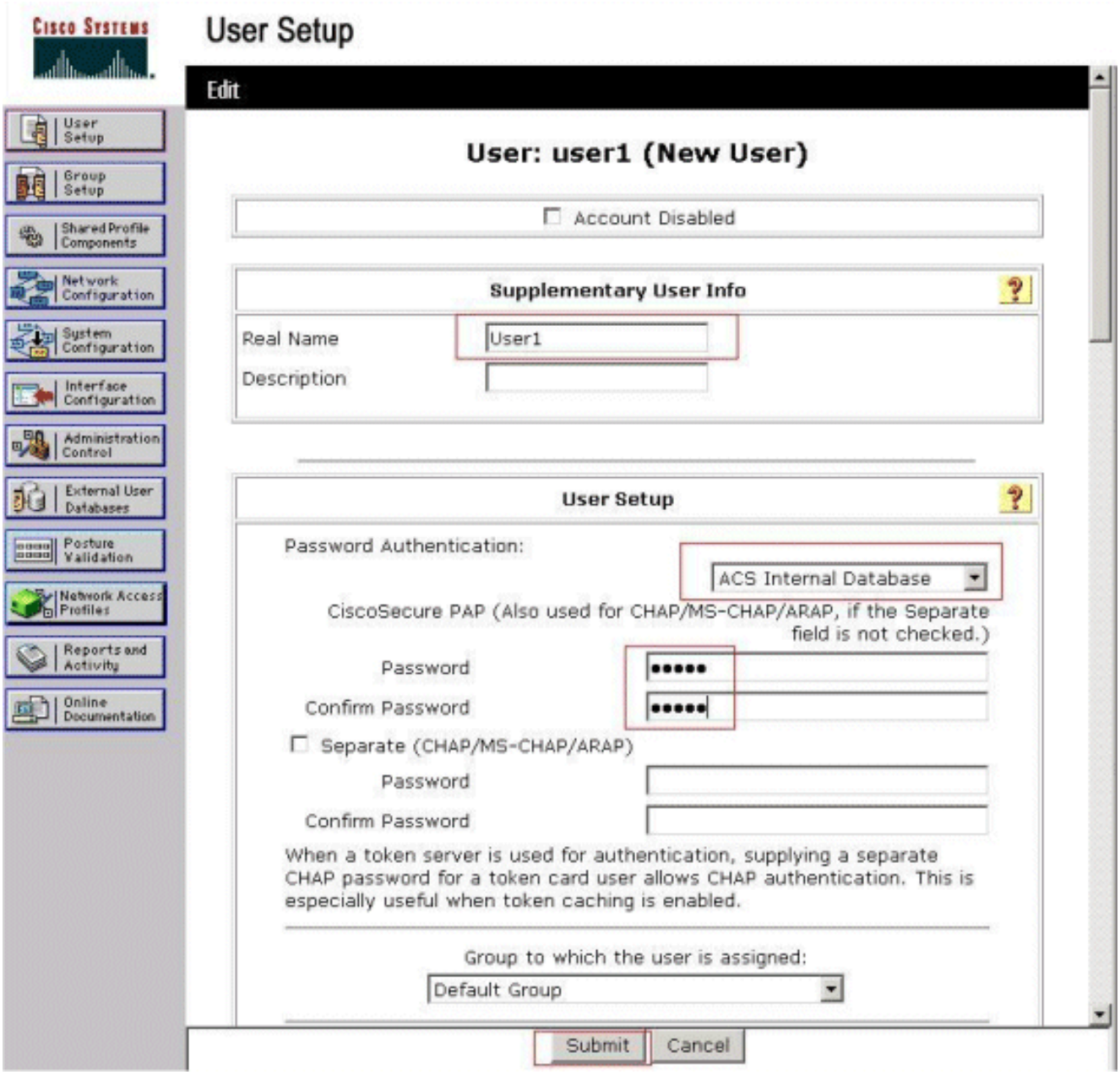
Konfigurieren der Benutzerinformationen auf Cisco Secure ACS

Führen Sie die folgenden Schritte aus, um Benutzer auf dem Cisco Secure ACS zu konfigurieren:

1. Wählen Sie in der Cisco Secure ACS-GUI **User Setup** (Benutzereinrichtung) aus, geben Sie einen Benutzernamen ein, und klicken Sie auf **Add/Edit (Hinzufügen/Bearbeiten)**. In diesem Beispiel ist der Benutzer *user1*.



2. PAP wird standardmäßig für die Authentifizierung von Clients verwendet. Das Kennwort für den Benutzer wird unter **User Setup > Password Authentication > Cisco Secure PAP** eingegeben. Stellen Sie sicher, dass Sie **ACS Internal Database** für die Kennwortauthentifizierung
auswählen.



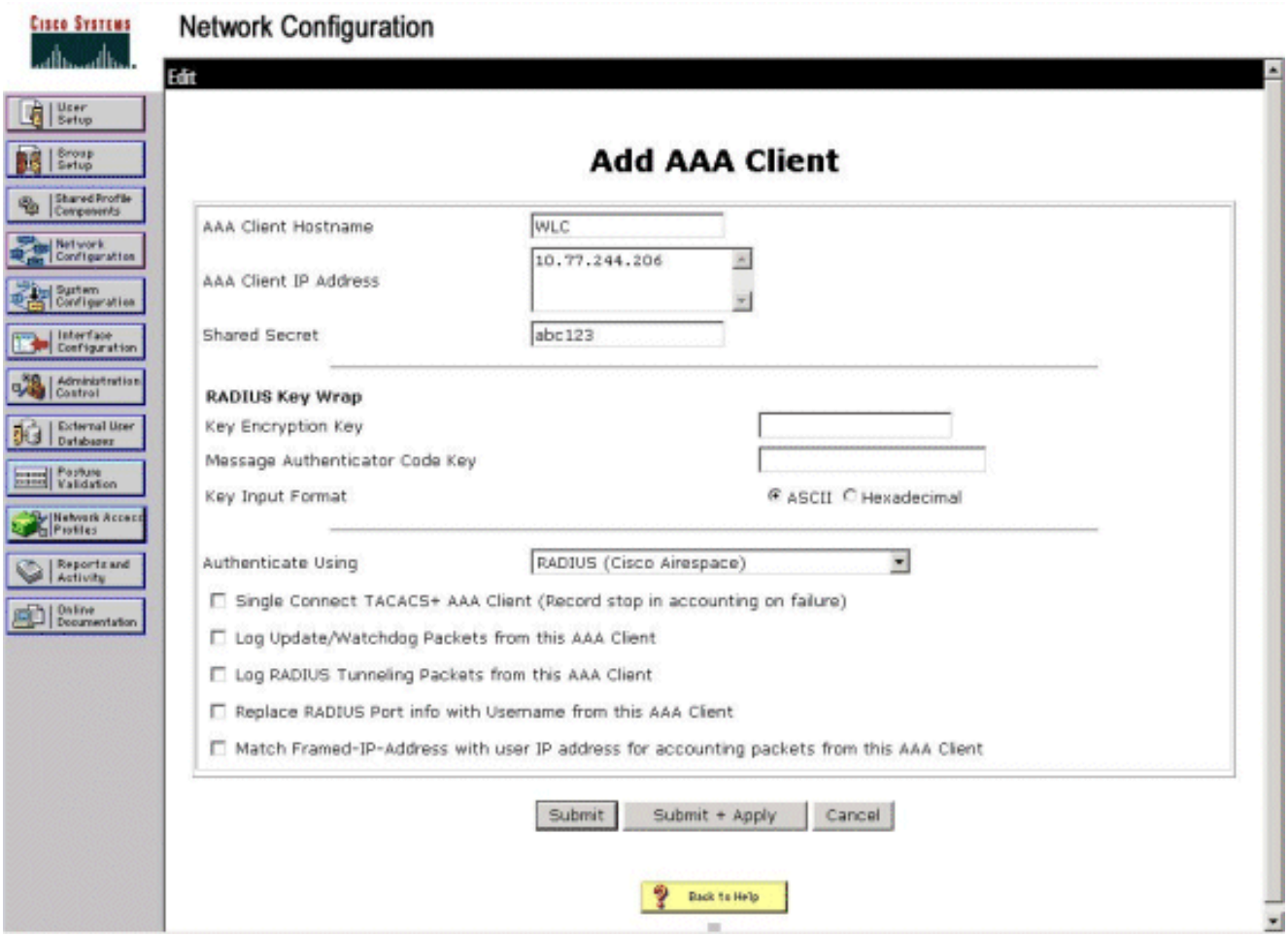
3. Dem Benutzer muss eine Gruppe zugewiesen werden, der er angehört. Wählen Sie die **Standardgruppe aus**.
4. Klicken Sie auf **Senden**.

Konfigurieren der WLC-Informationen auf Cisco Secure ACS

Gehen Sie folgendermaßen vor, um die WLC-Informationen auf Cisco Secure ACS zu konfigurieren:

1. Klicken Sie in der ACS-GUI auf die Registerkarte **Network Configuration** (**Netzwerkkonfiguration**), und klicken Sie auf **Add Entry (Eintrag hinzufügen)**.
2. Der Bildschirm "AAA-Client hinzufügen" wird angezeigt.
3. Geben Sie den Namen des Clients ein. In diesem Beispiel wird *WLC* verwendet.
4. Geben Sie die IP-Adresse des Clients ein. Die IP-Adresse des WLC lautet *10.77.244.206*.
5. Geben Sie den Schlüssel für den gemeinsamen geheimen Schlüssel und das Schlüsselformat ein. Dies sollte mit dem Eintrag im Menü **Security** des WLC übereinstimmen.
6. Wählen Sie **ASCII** als Format für die Schlüsseleingabe aus, das auf dem WLC identisch sein soll.

7. Wählen Sie **RADIUS (Cisco Airespace)** für Authenticate Using (Authentifizieren mit) aus, um das zwischen dem WLC und dem RADIUS-Server verwendete Protokoll festzulegen.
8. Klicken Sie auf **Senden + Anwenden**.

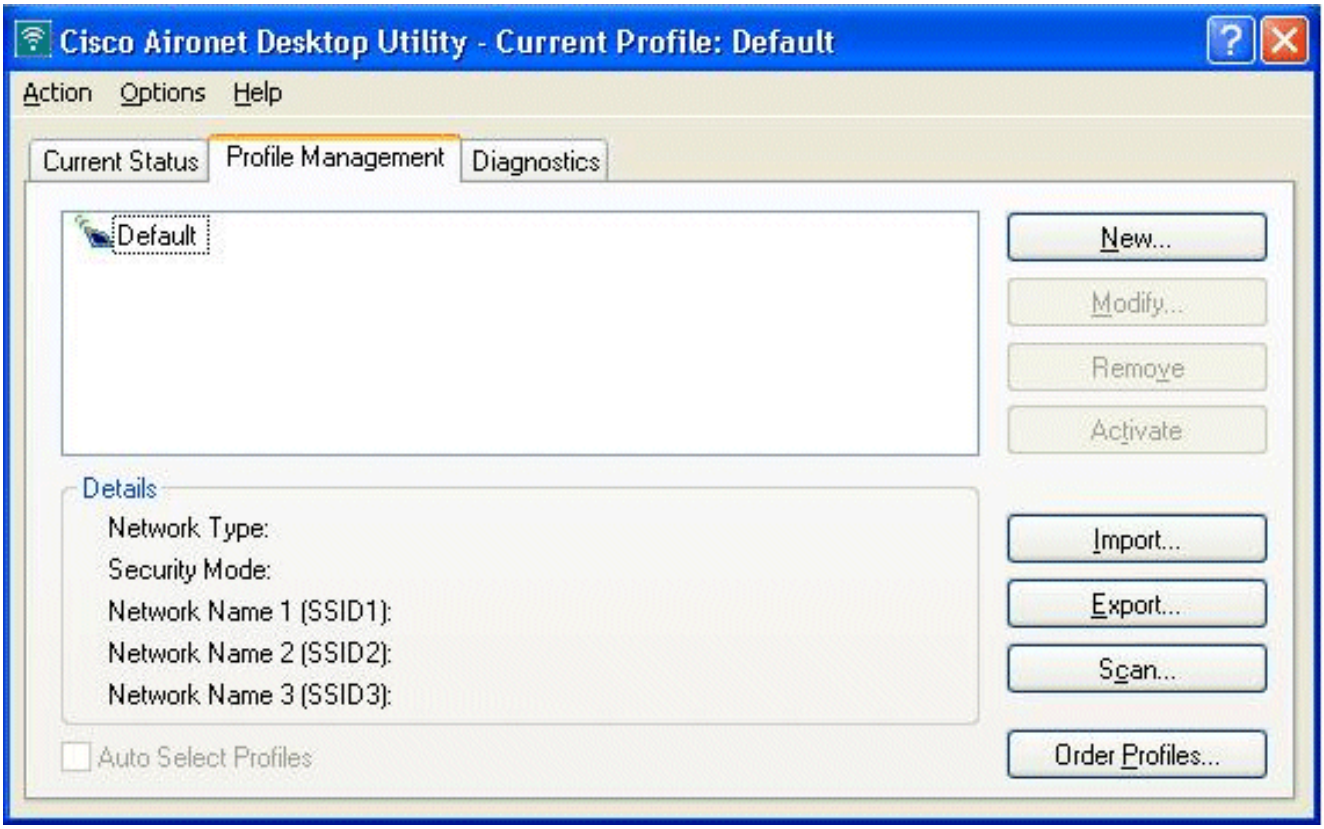


Client-Authentifizierungsprozess

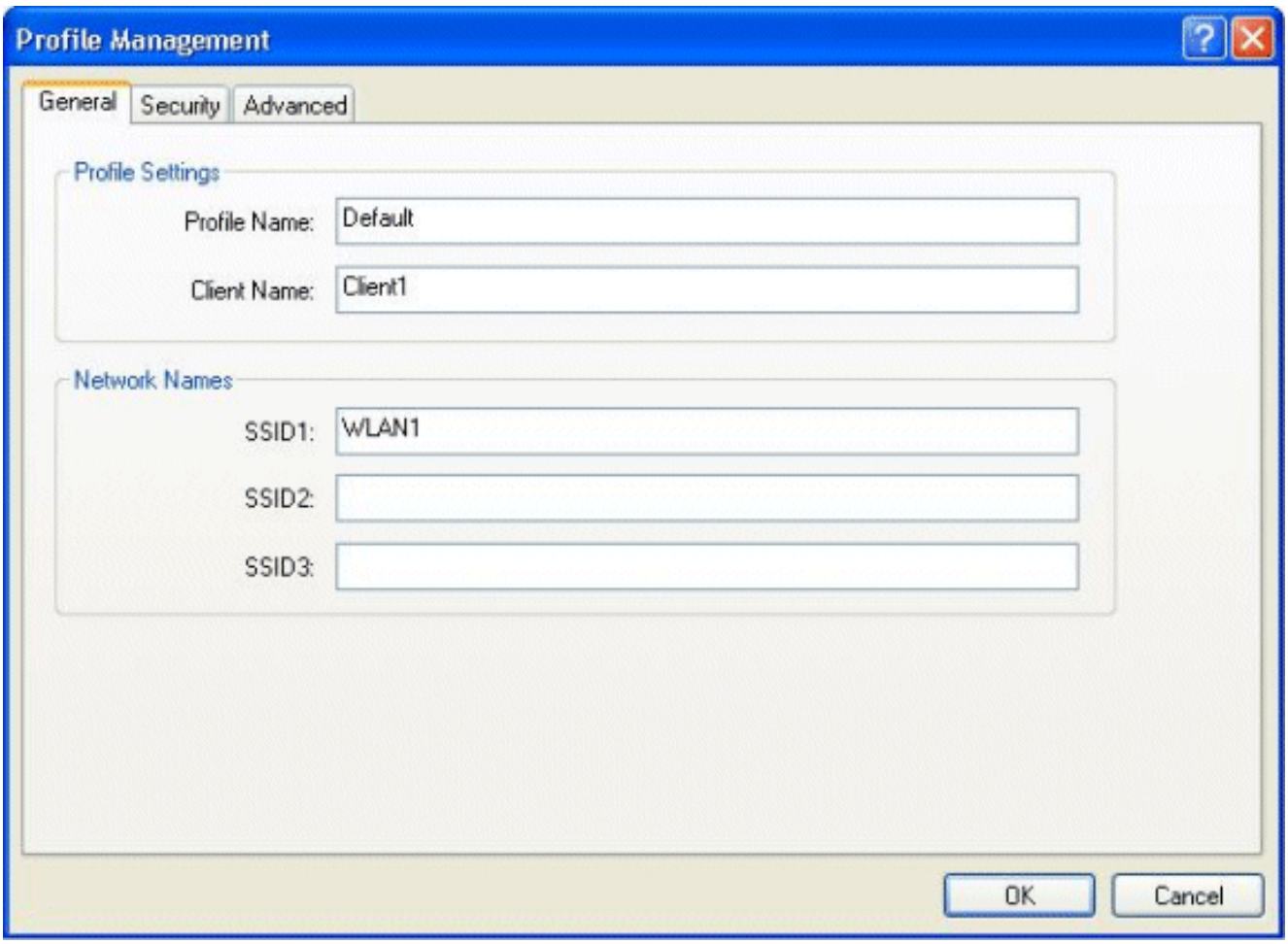
Client-Konfiguration

In diesem Beispiel verwenden wir das Cisco Aironet Desktop Utility für die Webauthentifizierung. Führen Sie diese Schritte aus, um das Aironet Desktop Utility zu konfigurieren.

1. Öffnen Sie das Aironet Desktop Utility über **Start > Cisco Aironet > Aironet Desktop Utility**.
2. Klicken Sie auf die Registerkarte **"Profilverwaltung"**.

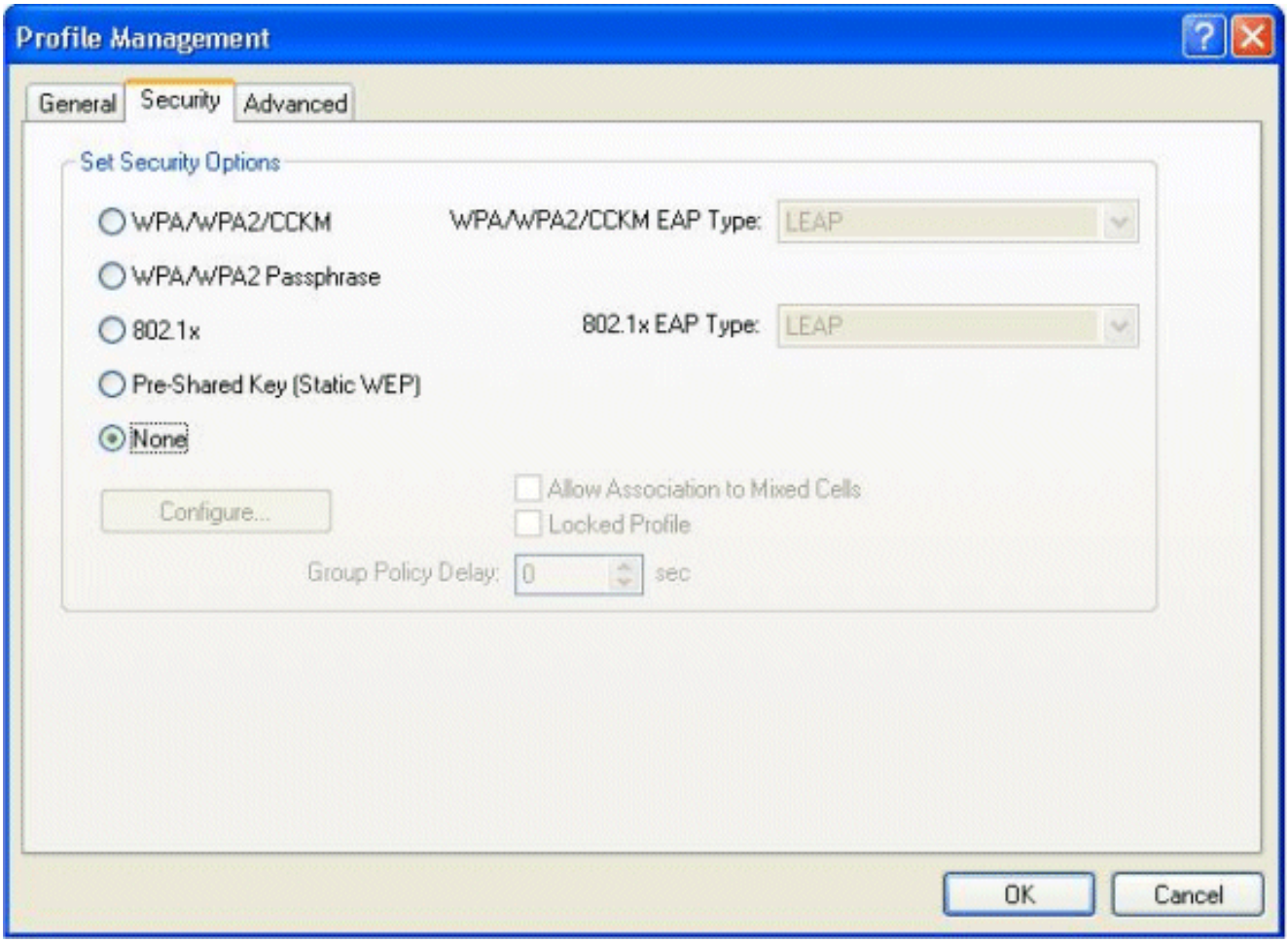


3. Wählen Sie das **Standard**-Profil aus, und klicken Sie auf **Ändern**.Klicken Sie auf die Registerkarte **Allgemein**.Konfigurieren eines Profilnamens In diesem Beispiel wird *Default* verwendet.Konfigurieren Sie die SSID unter Netzwerknamen. In diesem Beispiel wird *WLAN1*
verwendet.

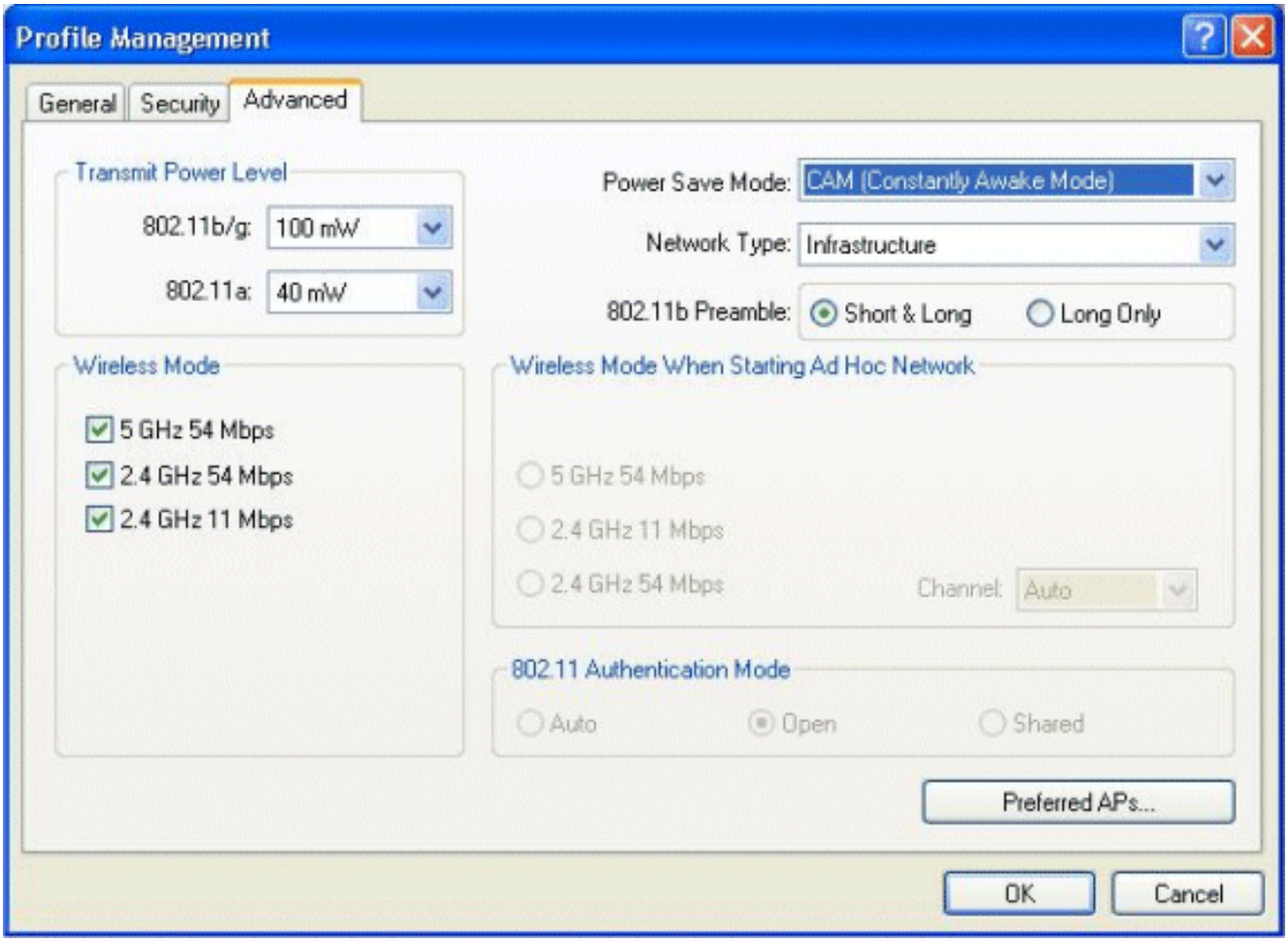


Hinweis: Bei der SSID wird die Groß-/Kleinschreibung beachtet, und sie muss mit dem auf

dem WLC konfigurierten WLAN übereinstimmen.Klicken Sie auf die Registerkarte **Sicherheit**.Wählen Sie **None** als Security für die Webauthentifizierung aus.



Klicken Sie auf die Registerkarte **Advanced** (Erweitert).Wählen Sie im Menü **Wireless Mode (Wireless-Modus)** die Frequenz aus, mit der der Wireless-Client mit der LAP kommuniziert.Wählen Sie unter **Transmit Power Level (Übertragungsleistung)** die Leistung aus, die auf dem WLC konfiguriert ist.Behalten Sie den Standardwert für den Energiesparmodus bei.Wählen Sie als Netzwerktyp die **Infrastruktur aus**.Legen Sie die 802.11b-Präambel als **"Short & Long" (Kurz und lang)** fest, um eine bessere Kompatibilität zu gewährleisten.Klicken Sie auf **OK**.



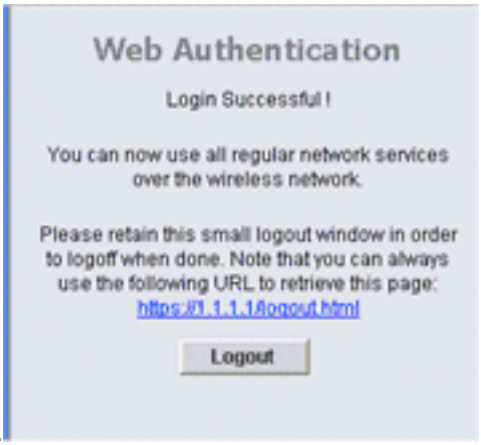
4. Nach der Konfiguration des Profils in der Client-Software wird der Client erfolgreich zugeordnet und erhält eine IP-Adresse aus dem VLAN-Pool, der für die Managementschnittstelle konfiguriert ist.

Client-Anmeldevorgang

In diesem Abschnitt wird erläutert, wie sich der Client anmeldet.

1. Öffnen Sie ein Browserfenster, und geben Sie eine beliebige URL oder IP-Adresse ein. Dadurch wird die Web-Authentifizierungsseite zum Client übertragen. Wenn auf dem Controller eine frühere Version als Version 3.0 ausgeführt wird, muss der Benutzer *https://1.1.1.1/login.html* eingeben, um die Web-Authentifizierungsseite aufzurufen. Ein Fenster mit Sicherheitswarnungen wird angezeigt.
2. Klicken Sie auf **Ja**, um fortzufahren.
3. Wenn das Anmeldefenster angezeigt wird, geben Sie den auf dem RADIUS-Server konfigurierten Benutzernamen und das Kennwort ein. Wenn Ihre Anmeldung erfolgreich ist, werden zwei Browserfenster angezeigt. Das größere Fenster zeigt an, dass die Anmeldung erfolgreich war, und Sie können in diesem Fenster im Internet surfen. Verwenden Sie das kleinere Fenster, um sich abzumelden, wenn Sie das Gastnetzwerk vollständig

nutzen.

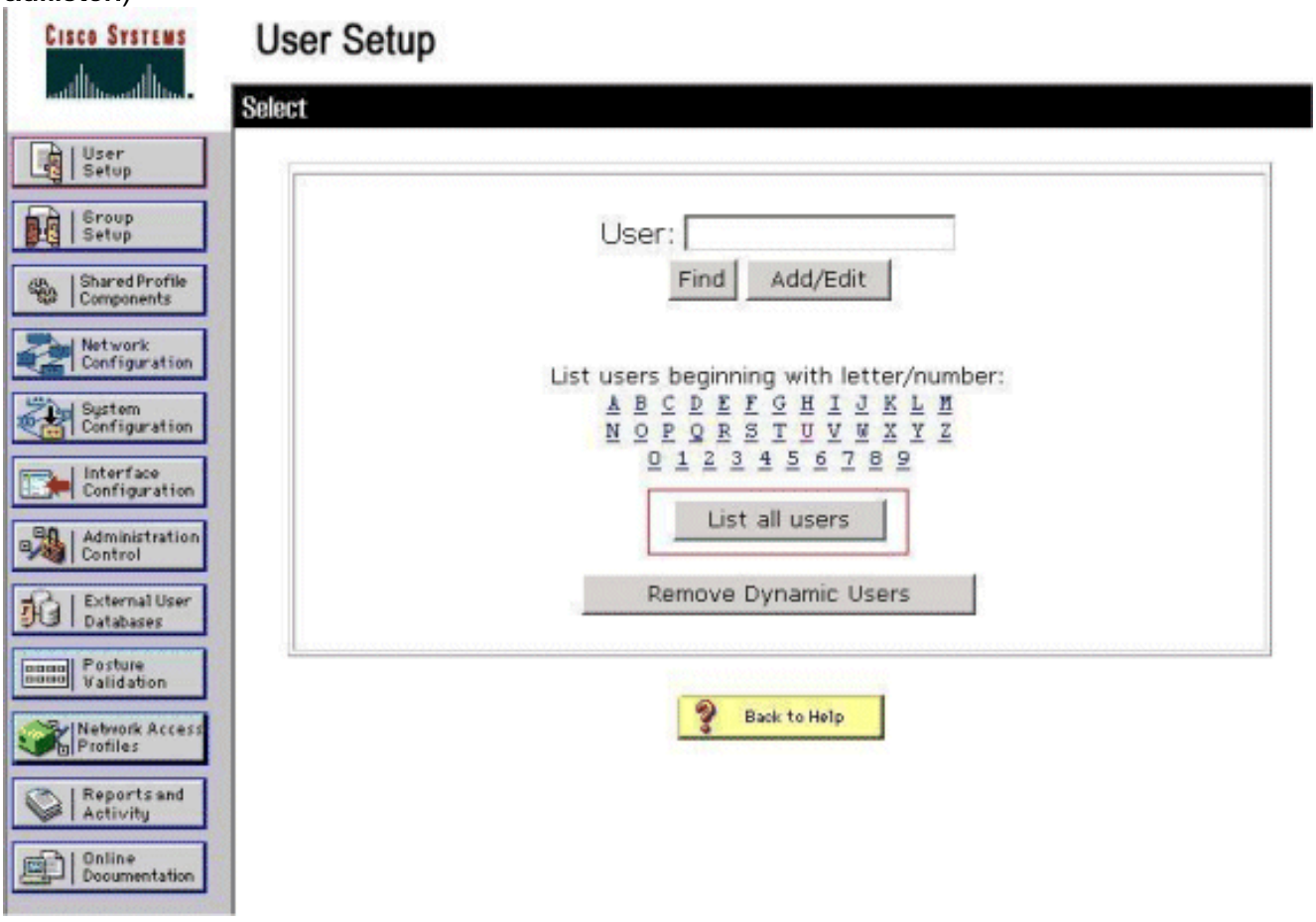


Überprüfung

Für eine erfolgreiche Web-Authentifizierung müssen Sie überprüfen, ob die Geräte ordnungsgemäß konfiguriert sind. In diesem Abschnitt wird erläutert, wie Sie die dabei verwendeten Geräte überprüfen.

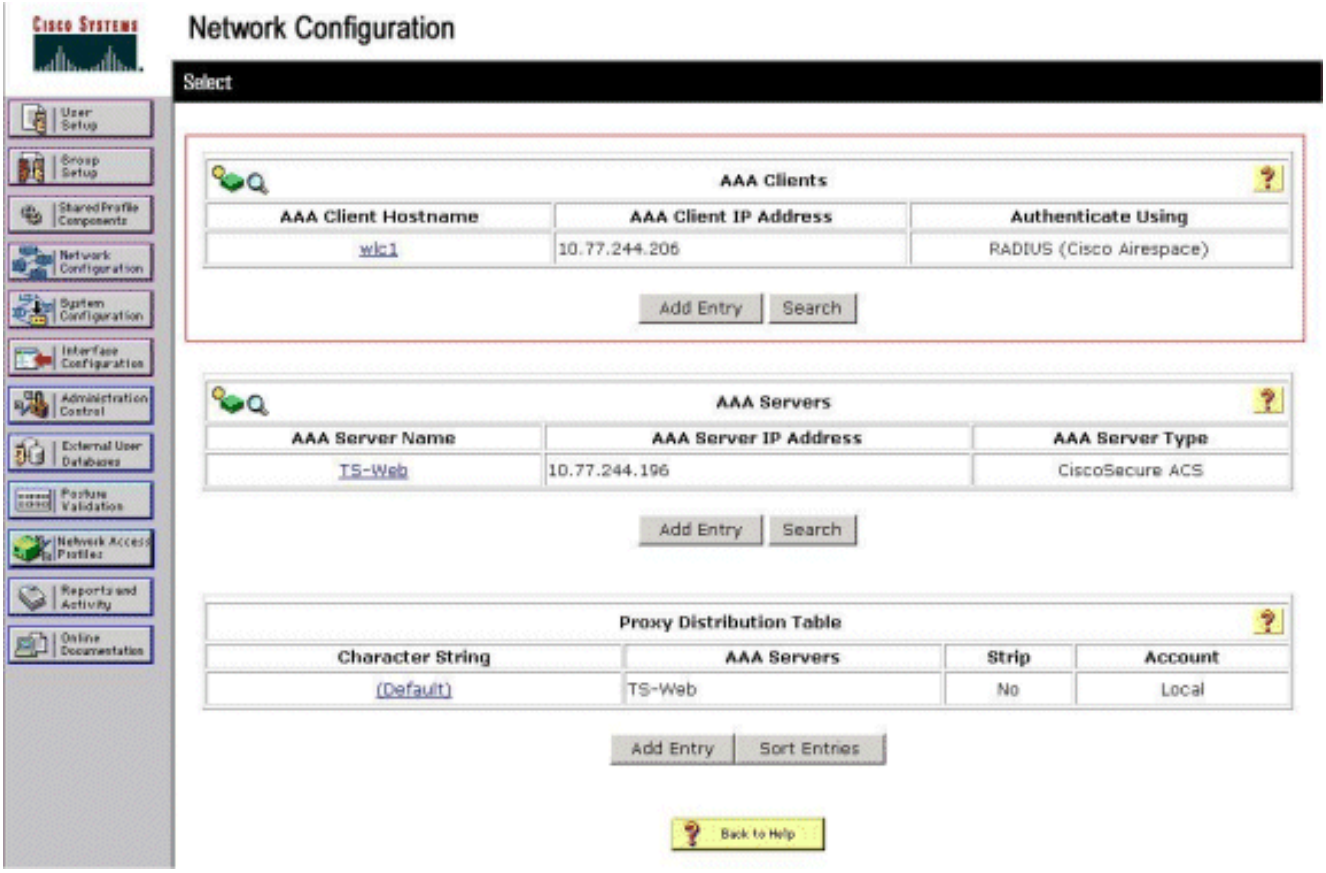
ACS überprüfen

1. Klicken Sie auf **User Setup (Benutzereinrichtung)** und dann in der ACS-GUI auf **List All Users (Alle Benutzer auflisten)**.



Vergewissern Sie sich, dass der Status des Benutzers *Enabled (Aktiviert)* ist und dass die Standardgruppe dem Benutzer zugeordnet
ist.

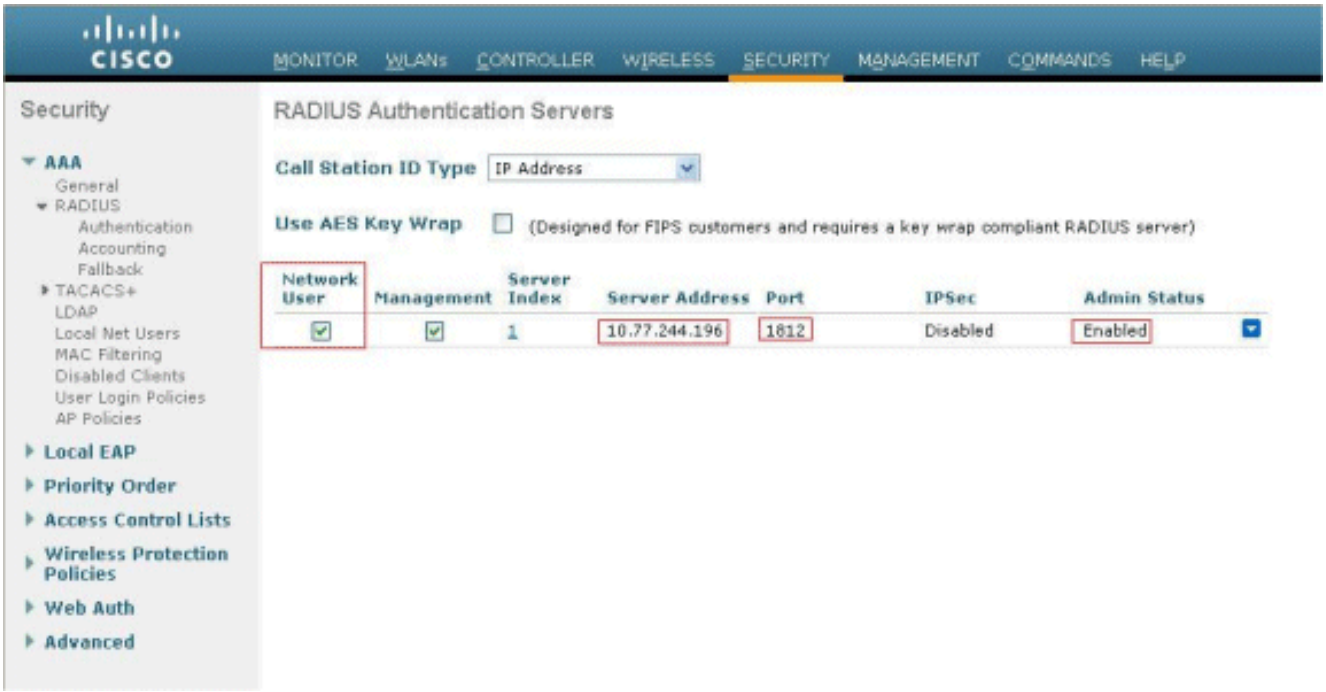
2. Klicken Sie auf die Registerkarte **Network Configuration** (**Netzwerkkonfiguration**), und überprüfen Sie in der Tabelle mit den **AAA-Clients**, ob der WLC als AAA-Client konfiguriert ist.



WLC überprüfen

1. Klicken Sie in der WLC-GUI auf das Menü **WLANs**.Vergewissern Sie sich, dass das für die Webauthentifizierung verwendete WLAN auf der Seite aufgeführt ist.Stellen Sie sicher, dass der Admin-Status für das WLAN *aktiviert* ist.Stellen Sie sicher, dass die Sicherheitsrichtlinie für das WLAN *Web-Auth*
anzeigt.

2. Klicken Sie in der WLC-GUI auf das Menü **SECURITY** (SICHERHEIT).Stellen Sie sicher, dass Cisco Secure ACS (10.77.244.196) auf der Seite aufgeführt ist.Vergewissern Sie sich, dass das Kontrollkästchen Netzwerkbenutzer aktiviert ist.Vergewissern Sie sich, dass der Port *1812* ist und dass der Admin-Status *Enabled (Aktiviert)* lautet.



Fehlerbehebung

Es gibt viele Gründe, warum eine Webauthentifizierung nicht erfolgreich ist. Im Dokument Troubleshooting Web Authentication on a Wireless LAN Controller (WLC) werden diese Gründe im Detail erläutert.

Befehle für die Fehlerbehebung

Hinweis: Lesen Sie Wichtige Informationen zu Debug-Befehlen, bevor Sie diese **Debug-**Befehle verwenden.

Telnet wird in den WLC gesendet und gibt die folgenden Befehle aus, um die Authentifizierung zu vereinfachen:

- **debug aaa all enable**

```
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Successful transmission of Authentic
ation Packet (id 1) to 10.77.244.196:1812, proxy state 00:40:96:ac:dd:05-00:01
Fri Sep 24 13:59:52 2010: 00000000: 01 01 00 73 00 00 00 00  00 00 00 00 00 00 0
0 00  ...s............
Fri Sep 24 13:59:52 2010: 00000010: 00 00 00 00 01 07 75 73  65 72 31 02 12 93 c
3 66  ......user1....f
Fri Sep 24 13:59:52 2010: 00000030: 75 73 65 72 31
      user1
Fri Sep 24 13:59:52 2010: ****Enter processIncomingMessages: response code=2
Fri Sep 24 13:59:52 2010: ****Enter processRadiusResponse: response code=2
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Access-Accept received from RADIUS s
erver 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 0
Fri Sep 24 13:59:52 2010: AuthorizationResponse: 0x12238db0
Fri Sep 24 13:59:52 2010:       structureSize.............................89
```

```
Fri Sep 24 13:59:52 2010:       resultCode.....................0
Fri Sep 24 13:59:52 2010:       protocolUsed.....................0x0
0000001
Fri Sep 24 13:59:52 2010:       proxyState.....................00:
40:96:AC:DD:05-00:00
Fri Sep 24 13:59:52 2010:       Packet contains 2 AVPs:
Fri Sep 24 13:59:52 2010:           AVP[01] Framed-IP-Address.....
.....0xffffffff (-1) (4 bytes)
Fri Sep 24 13:59:52 2010:           AVP[02] Class.....
.....CACS:0/5183/a4df4ce/user1 (25 bytes)
Fri Sep 24 13:59:52 2010: Authentication failed for user1, Service Type: 0
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Applying new AAA override for statio
n 00:40:96:ac:dd:05
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Override values for station 00:40:96
:ac:dd:05
                source: 48, valid bits: 0x1
        qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
                                                          vlanIfName: '',
aclName:
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Unable to apply override policy for
station 00:40:96:ac:dd:05 - VapAllowRadiusOverride is FALSE
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Sending Accounting request (0) for s
tation 00:40:96:ac:dd:05
Fri Sep 24 13:59:52 2010: AccountingMessage Accounting Start: 0x1500501c
Fri Sep 24 13:59:52 2010:       Packet contains 12 AVPs:
Fri Sep 24 13:59:52 2010:           AVP[01] User-Name.....
.....user1 (5 bytes)
Fri Sep 24 13:59:52 2010:           AVP[02] Nas-Port.....
.....0x00000002 (2) (4 bytes)
Fri Sep 24 13:59:52 2010:           AVP[03] Nas-Ip-Address.....
.....0x0a4df4ce (172881102) (4 bytes)
Fri Sep 24 13:59:52 2010:           AVP[04] Framed-IP-Address.....
.....0x0a4df4c7 (172881095) (4 bytes)
```

- **debug aaa detail aktivieren**

Fehlgeschlagene Authentifizierungsversuche werden im Menü unter **Berichte und Aktivität > Fehlgeschlagene Versuche** aufgelistet.

Zugehörige Informationen

- Konfigurationsbeispiel für Web-Authentifizierung des Wireless LAN-Controllers
- Problembehandlung bei der Webauthentifizierung auf einem Wireless LAN Controller (WLC)
- Konfigurationsbeispiel für externe Web-Authentifizierung mit Wireless LAN-Controllern
- Web-Authentifizierung mithilfe von LDAP auf Wireless LAN Controllern (WLCs) - Konfigurationsbeispiel
- 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.