Externe webverificatie met een RADIUS-server

Inhoud

Inleiding

Dit document legt uit hoe externe web-verificatie kan worden uitgevoerd met behulp van een externe RADIUS-server.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Basiskennis van de configuratie van Lichtgewicht Access Point (LAP's) en Cisco WLC's
- Kennis van het instellen en configureren van een externe webserver

- Kennis van de manier waarop u Cisco Secure ACS kunt configureren

Gebruikte componenten

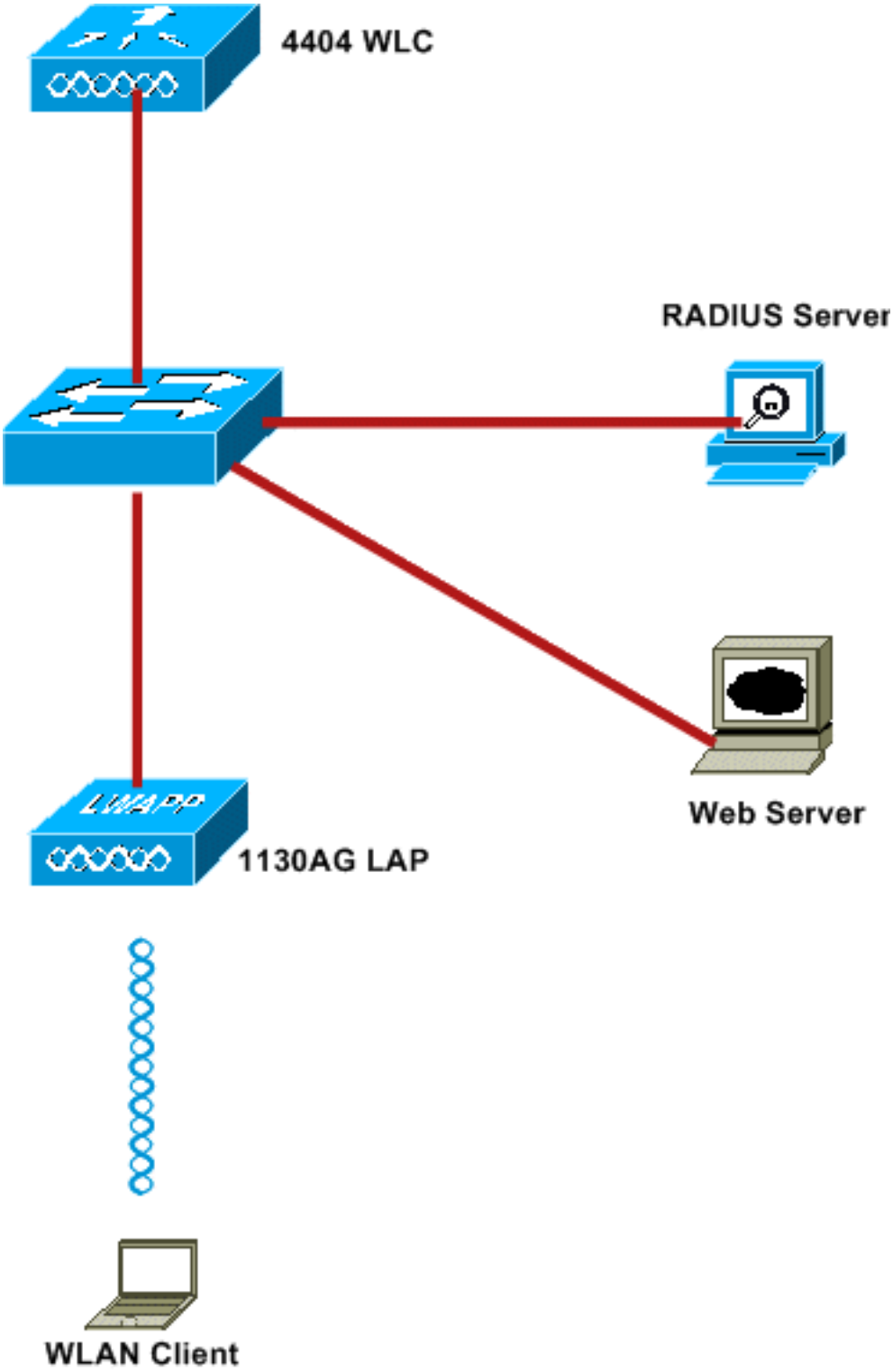
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Draadloze LAN-controller met versie 5.0.14.0
- Cisco 1232 Series LAP
- Cisco 802.11a/b/g draadloze clientadapter 3.6.0.61
- Externe webserver waarop de logpagina voor de webverificatie wordt opgeslagen
- Cisco Secure ACS-versie met firmware versie 4.1.1.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Dit zijn de IP-adressen die in dit document worden gebruikt:

- WLC gebruikt het IP-adres 10.7.24.206
- LAP is geregistreerd op WLC met IP-adres 10.7.24.1999
- Web Server gebruikt het IP-adres 10.7.24.210
- Cisco ACS-server gebruikt het IP-adres 10.7.24.196
- De client ontvangt een IP-adres van de beheerinterface die in kaart is gebracht op WLAN-10.7.24.208

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Externe webverificatie

Web Authentication is een Layer 3 authenticatiemechanisme dat wordt gebruikt om gastgebruikers voor internettoegang te authenticeren. Gebruikers die dit proces als authentiek hebben verklaard, kunnen geen toegang tot het internet krijgen tot ze het authenticatieproces succesvol hebben voltooid. Lees voor volledige informatie over het externe proces voor webverificatie het gedeelte Externe Web Verificatieproces van het document Externe Web Verificatie met Configuratievoorbeeld voor draadloze LAN-controllers.

In dit document bekijken we een configuratievoorbeeld, waarin de externe web authenticatie wordt uitgevoerd met een externe RADIUS-server.

De WLC configureren

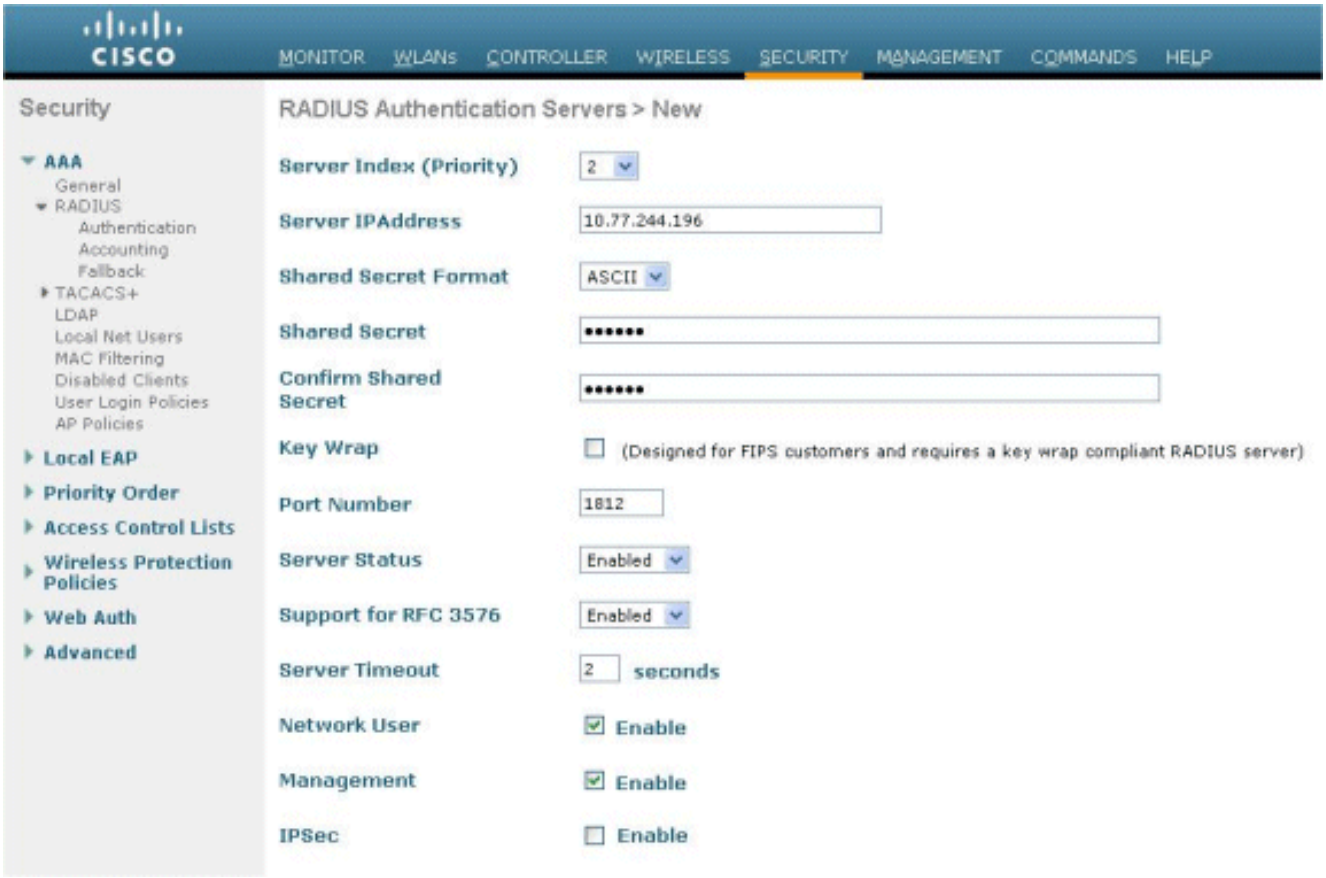
In dit document gaan we ervan uit dat de WLC al is geconfigureerd en dat er een LAP is geregistreerd in het WLC. In dit document wordt er voorts van uitgegaan dat de WLC is geconfigureerd voor basisgebruik en dat de LAP's bij de WLC zijn geregistreerd. Als u een nieuwe gebruiker bent die probeert de WLC in te stellen voor basisbediening met LAP's, raadpleegt u Lichtgewicht AP (LAP) Registratie aan een draadloze LAN-controller (WLC). Als u de LAP's wilt bekijken die op de WLC zijn geregistreerd, navigeer dan naar **Draadloos > Alle AP's**.

Zodra de WLC voor basisbediening is ingesteld en er een of meer LAP's bij zijn geregistreerd, kunt u de WLC configureren voor externe webverificatie met behulp van een externe webserver. In ons voorbeeld, gebruiken we een Cisco Secure ACS versie 4.1.1.24 als de RADIUS-server. Eerst zullen we de WLC voor deze RADIUS-server configureren en dan zullen we de configuratie bekijken die vereist is op Cisco Secure ACS voor deze instelling.

Configureer de WLC voor Cisco Secure ACS

Voer deze stappen uit om de RADIUS-server aan de WLC toe te voegen:

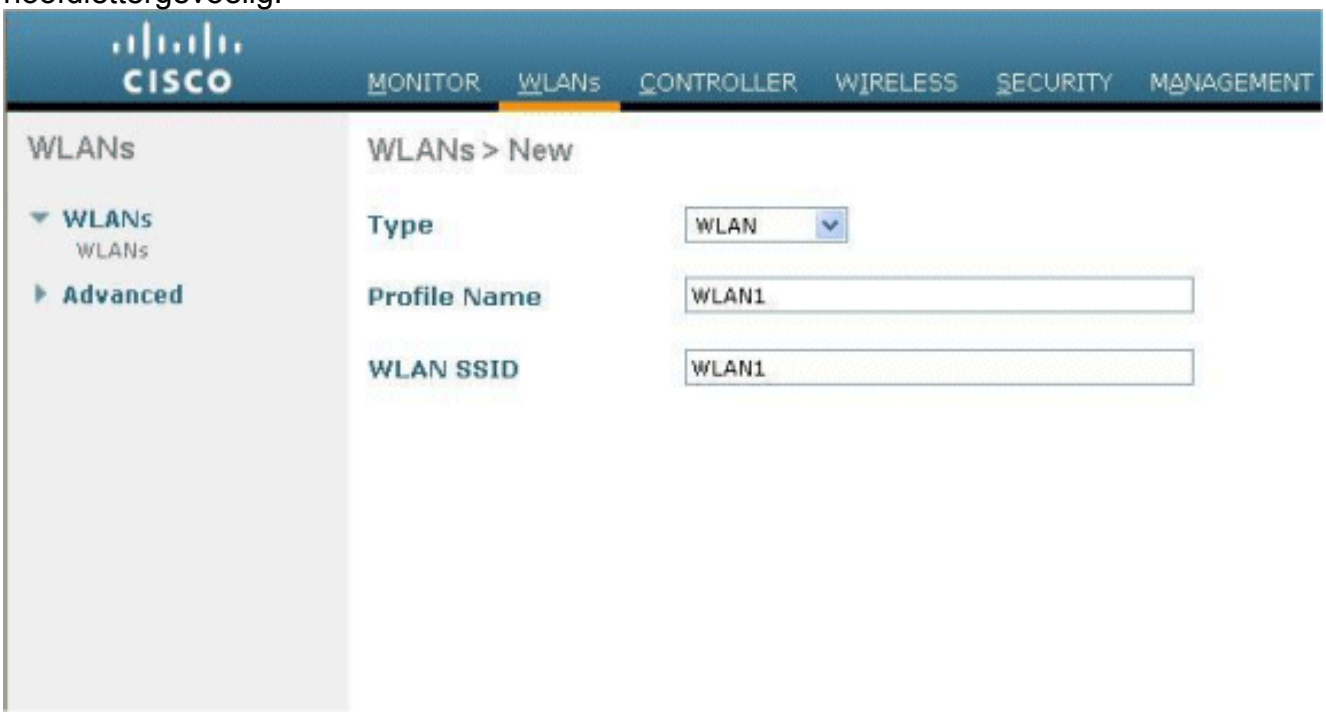
1. Klik vanuit de WLC GUI op het **SECURITY-**menu.
2. Navigeer onder **het** menu **AAA** naar het submenu **Radius > Verificatie**.
3. Klik op **New** en voer het IP-adres van de RADIUS-server in. In dit voorbeeld is het IP-adres van de server *10.77.244.196*.
4. Voer het gedeelde geheim in via de WLC. Het gedeelde geheim moet op de WLC hetzelfde worden ingesteld.
5. Kies of **ASCII** of **Hex** voor gedeeld geheim formaat. Dezelfde indeling moet op de WLC worden geselecteerd.
6. **1812** is het Port Number dat wordt gebruikt voor RADIUS-verificatie.
7. Zorg ervoor dat de optie Server Status is ingesteld op **Enabled**.
8. Controleer het dialoogvenster Netwerkgebruiker **inschakelen** om de netwerkgebruikers voor het eerst te controleren.
9. Klik op **Apply**
   (Toepassen).



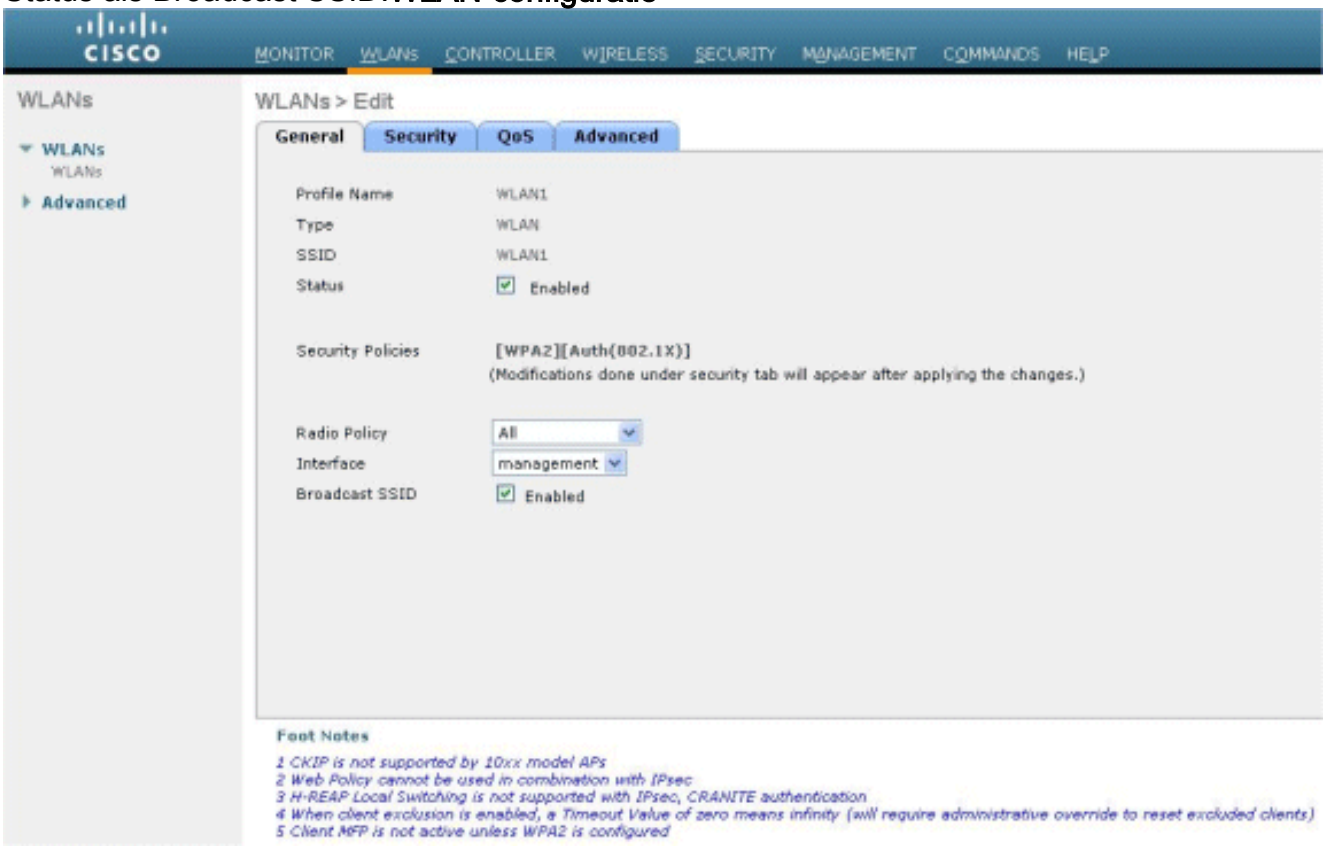
Configureer de WLAN's op WLC voor webverificatie

De volgende stap is het WLAN voor web-verificatie op WLC te configureren. Voer deze stappen uit om de WLAN-functie op WLC te configureren:

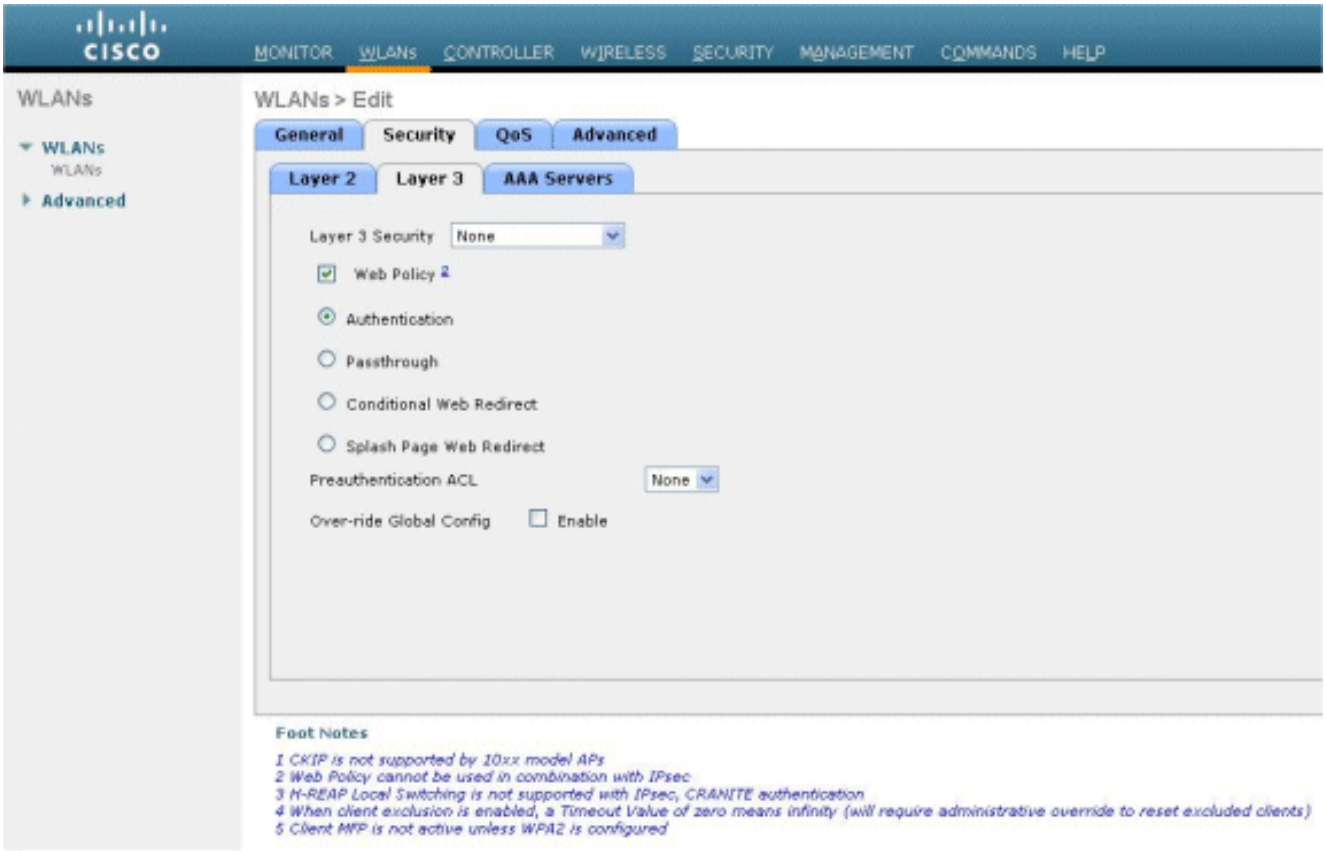
1. Klik op het menu **WLAN's** van de controller GUI, en kies **Nieuw**.
2. Kies **WLAN** voor type.
3. Voer een Profile Name en een WLAN SSID van uw keuze in en klik op **Toepassen**.**Opmerking:** WLAN SSID is hoofdlettergevoelig.



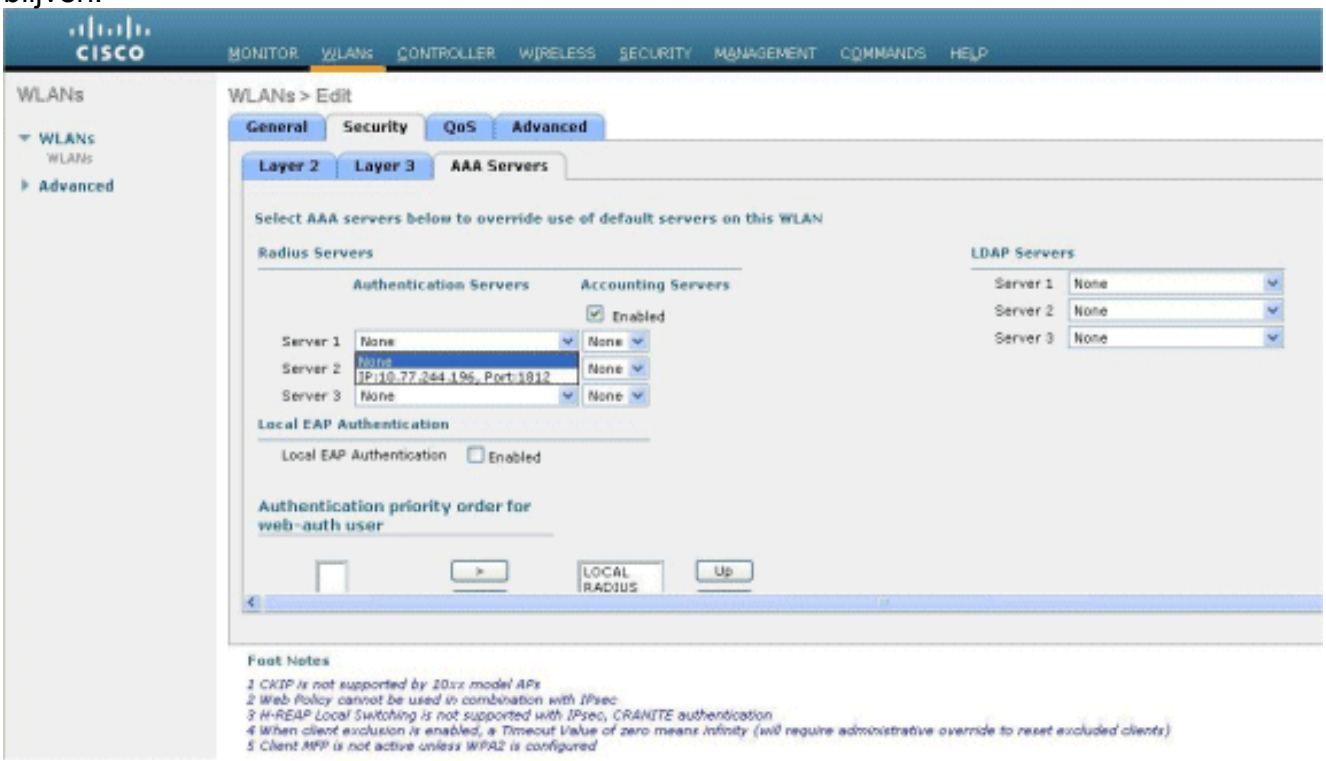
4. Zorg onder het tabblad **Algemeen** dat de **optie Ingeschakeld** is ingeschakeld voor zowel Status als Broadcast SSID.**WLAN-configuratie**



5. Kies een interface voor WLAN. Meestal wordt een interface die in een uniek VLAN is geconfigureerd in kaart gebracht in het WLAN, zodat de client een IP-adres in dat VLAN ontvangt. In dit voorbeeld gebruiken we *management* voor interface.
6. Kies het tabblad **Beveiliging**.
7. Kies onder het menu **Layer 2** de optie **Geen** voor Layer 2 Security.
8. Kies onder het menu **Layer 3** de optie **Geen** voor Layer 3 security. Controleer het selectieteken **Web Policy** en kies **Verificatie**.



9. Kies onder het menu **AAA**-servers voor Verificatieserver de RADIUS-server die op deze WLC is ingesteld. Andere menu's moeten de standaardwaarden blijven.

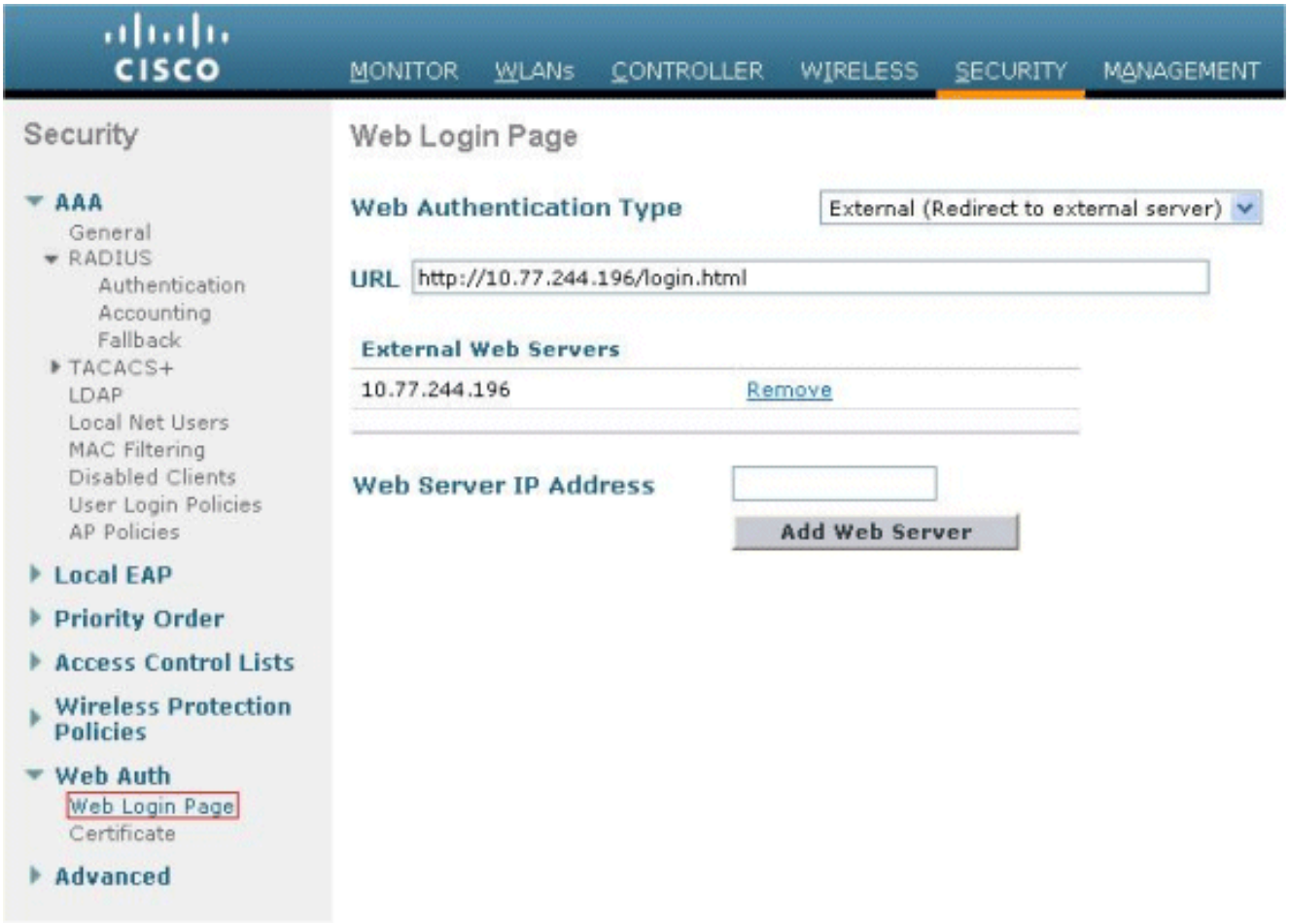


De informatie over de webserver op WLC configureren

De webserver die de webverificatie-pagina opslaat, moet op de WLC worden geconfigureerd. Volg deze stappen om de webserver te configureren:

1. Klik op het tabblad **Beveiliging**. Ga naar **Web Auth > Web Login Page**.

2. Stel het type webverificatie in als **extern**.
3. In het veld IP-adres van de webserver voert u het IP-adres in van de server die de pagina Webverificatie gastheer opslaat en klikt u op **Webserver toevoegen**. In dit voorbeeld is het IP-adres *10.77.244.196*, dat verschijnt onder Externe Webservers.
4. Voer de URL in voor de webverificatie-pagina (in dit voorbeeld *http://10.77.244.196/login.html*) in het URL-veld.



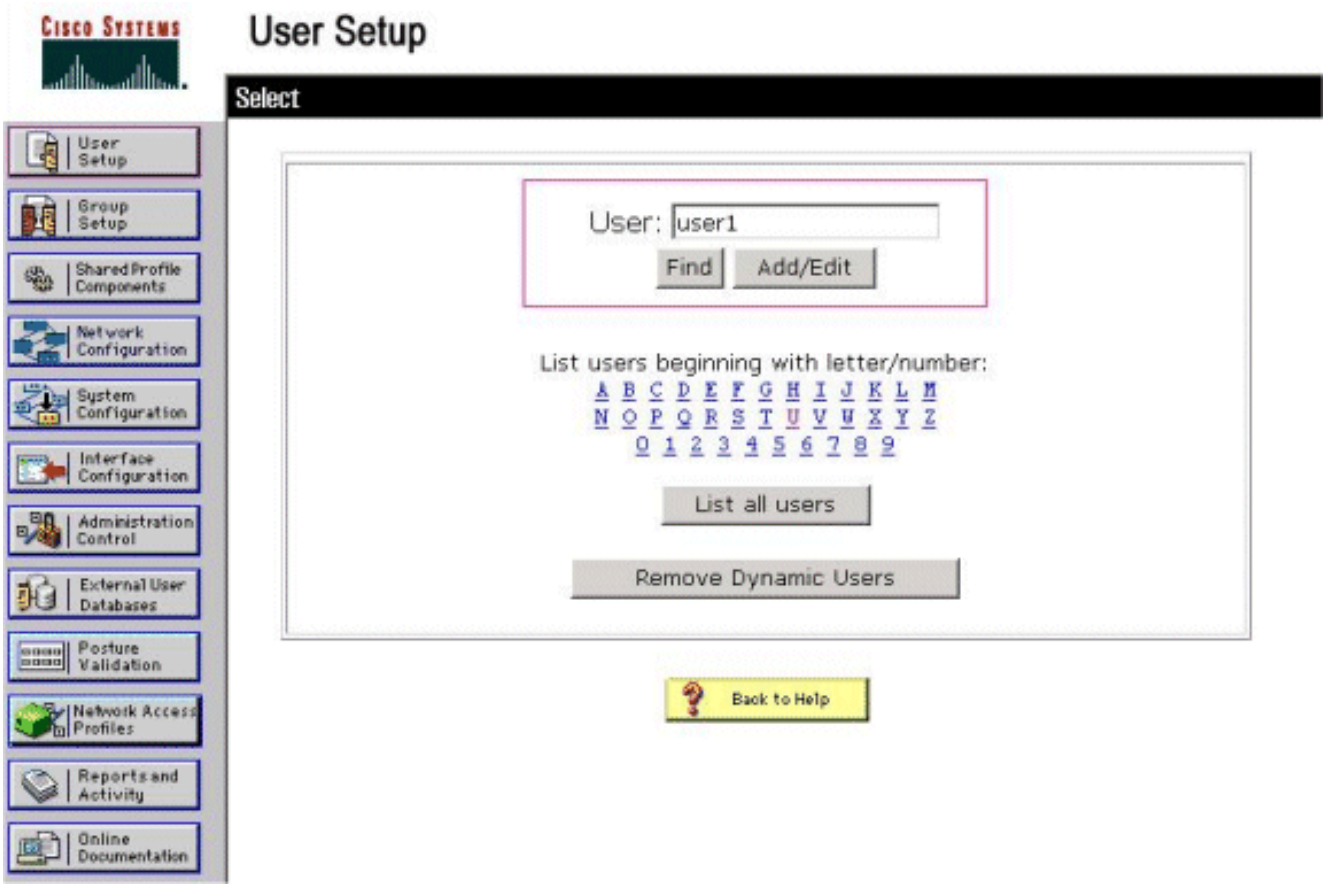
Cisco beveiligde ACS configureren

In dit document gaan we ervan uit dat Cisco Secure ACS Server al op een machine is geïnstalleerd en uitgevoerd. Voor meer informatie hoe u Cisco Secure ACS kunt instellen, raadpleegt u de Configuration Guide voor Cisco Secure ACS 4.2.

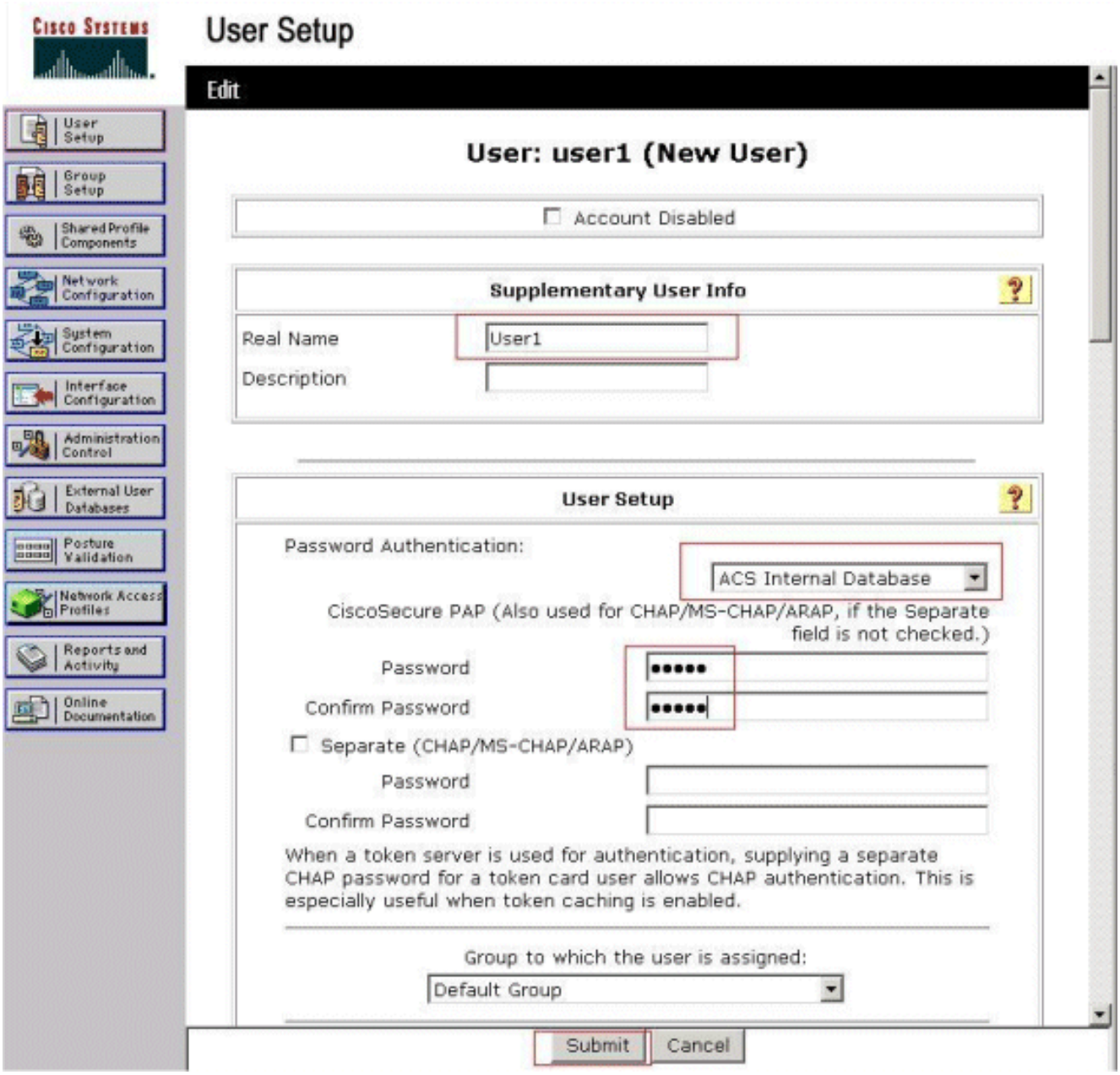
De gebruikersinformatie op Cisco Secure ACS configureren

Voer deze stappen uit om gebruikers op Cisco Secure ACS te configureren:

1. Klik op **Gebruikersinstelling** in de Cisco Secure ACS GUI, voer een gebruikersnaam in en klik op **Add/Edith**. In dit voorbeeld is de gebruiker *user1*.



2. PAP wordt standaard gebruikt voor het controleren van clients. Het wachtwoord voor de gebruiker wordt ingevoerd onder **Gebruikersinstelling > Wachtwoordverificatie > Cisco Secure PP**. Zorg ervoor dat u **ACS interne database** voor wachtwoordverificatie kiest.



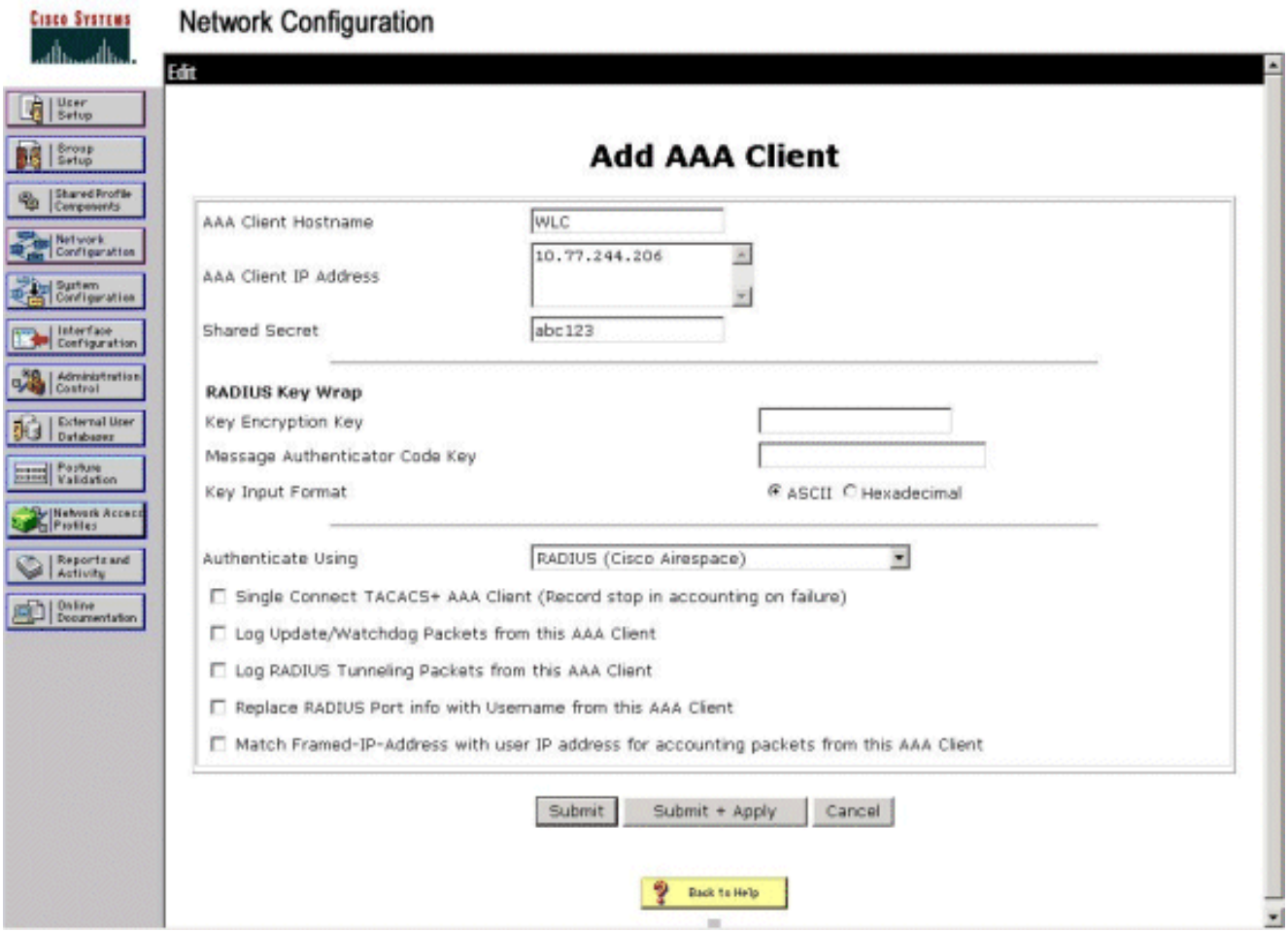
3. De gebruiker moet een groep toegewezen worden waartoe de gebruiker behoort. Kies de **Standaardgroep**.
4. Klik op **Inzenden**.

Configureer de WLC-informatie over Cisco beveiligde ACS

Voer deze stappen uit om WLC-informatie op Cisco Secure ACS te configureren:

1. Klik in de ACS GUI op het tabblad **Netwerkconfiguratie** en klik op **Ingang toevoegen**.
2. Het scherm Add AAA-client verschijnt.
3. Voer de naam van de client in. In dit voorbeeld gebruiken we *WLC*.
4. Voer het IP-adres van de client in. Het IP-adres van de WLC is *10.7.24.2006*.
5. Voer de gedeelde sleutel en het sleutelformaat in. Dit moet overeenkomen met de tekst in het **Security** menu van het WLC.
6. Kies **ASCII** voor het Key Input Format, dat op de WLC hetzelfde zou moeten zijn.
7. Kies **RADIUS (Cisco Airespace)** voor Authenticate Use om het protocol in te stellen dat gebruikt wordt tussen de WLC en de RADIUS Server.
8. Klik op **Inzenden +**

Toepassen.

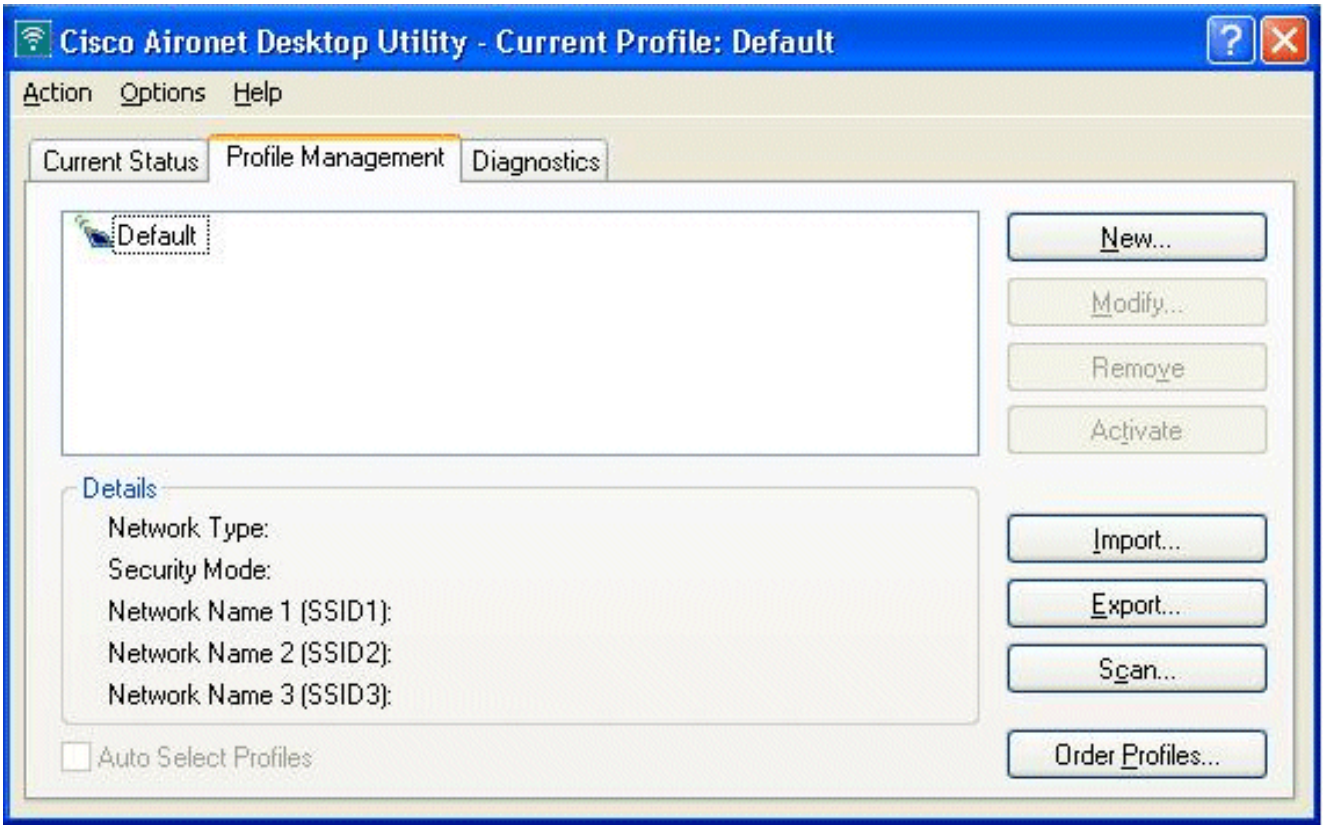


Clientverificatieproces

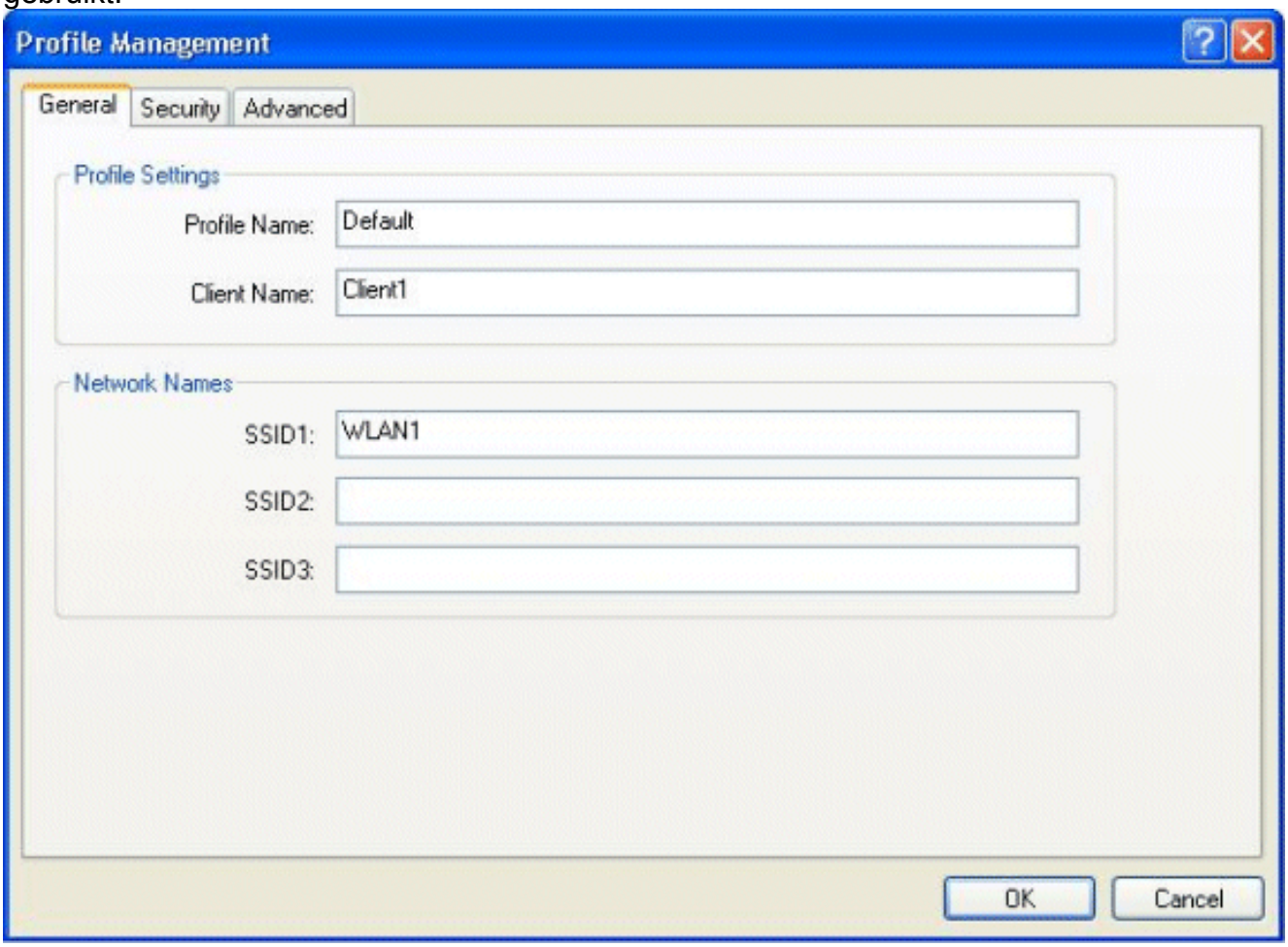
Clientconfiguratie

In dit voorbeeld gebruiken we Cisco Aironet Desktop Utility om web authenticatie uit te voeren. Volg deze stappen om het Aironet desktop hulpprogramma te configureren.

1. Open het Aironet-desktophulpprogramma van **Start > Cisco Aironet > Aironet-desktophulpprogramma**.
2. Klik op het tabblad **Profielbeheer**.

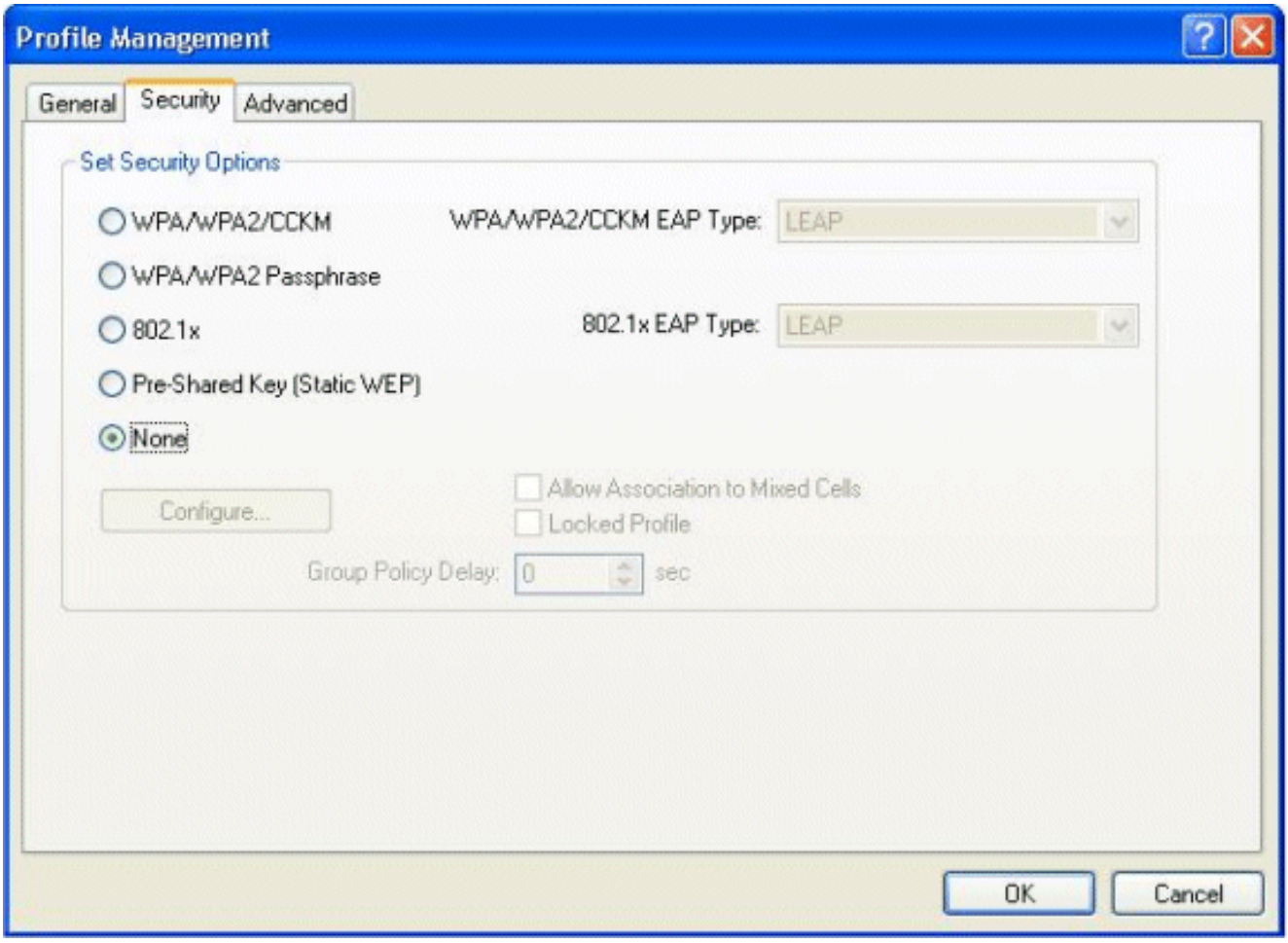


3. Kies het **standaardprofiel** en klik op **Wijzigen**.Klik op het tabblad **Algemeen**.Configureren van een profiel. In dit voorbeeld wordt *Default* gebruikt.Configureer de SSID onder Netwerknamen. In dit voorbeeld, *WLAN1* wordt gebruikt.

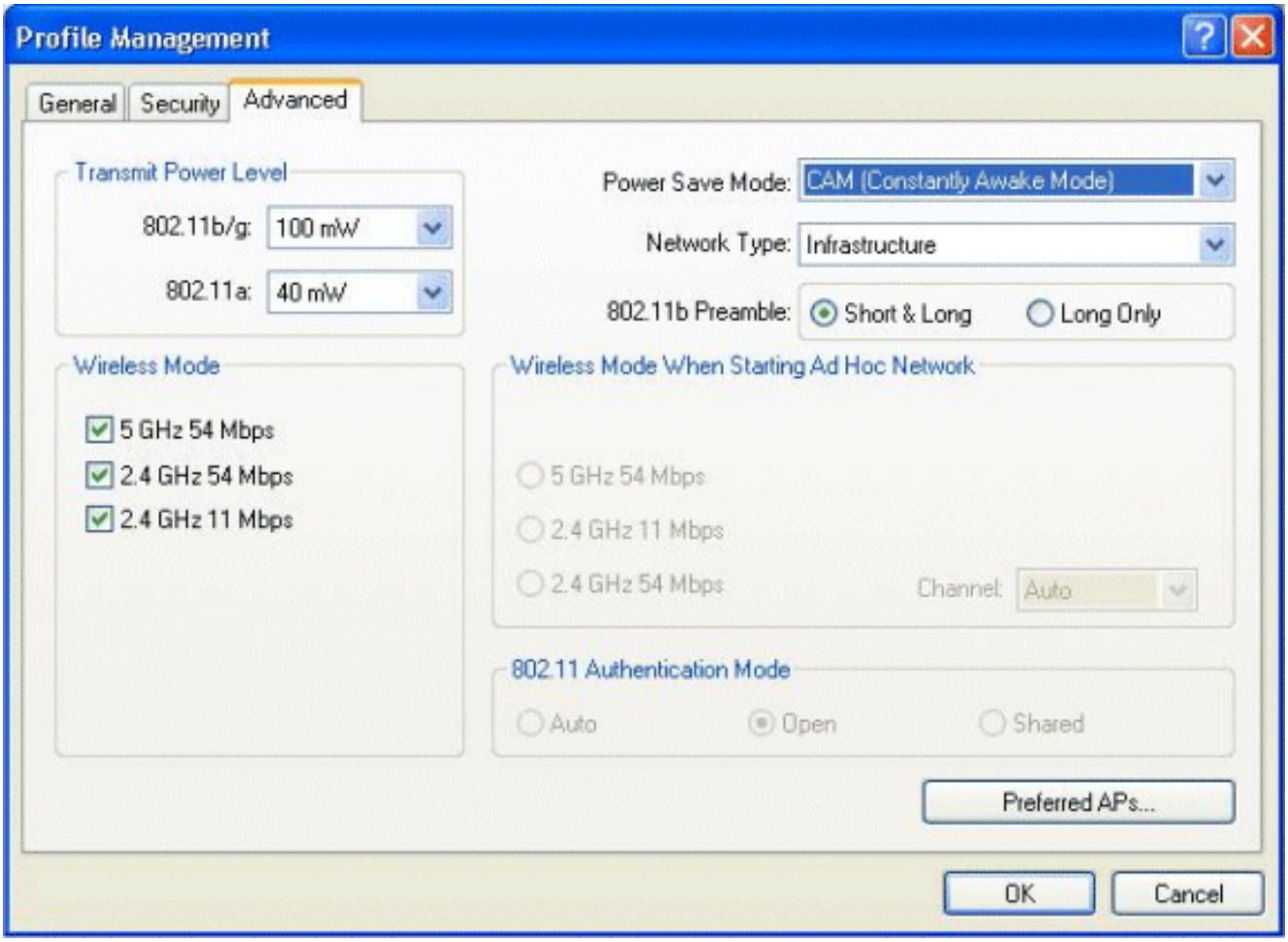


Opmerking: De SSID is hoofdlettergevoelig en moet overeenkomen met de WLAN die op de WLC zijn geconfigureerd.Klik op het tabblad **Beveiliging**.Kies **Geen** als beveiliging voor

webverificatie.



Klik op het tabblad **Geavanceerd**.Kies onder het menu **Draadloze modus** de frequentie waarmee de draadloze client communiceert met de LAP.Kies onder het **niveau** van de **stroomtoevoer** de voeding die op de WLC is ingesteld.Laat de standaardwaarde voor de Power Save Mode staan.Kies **infrastructuur** als netwerktype.Stel de preamble 802.11b in als **Short & Long** voor een betere compatibiliteit.Klik op
OK.



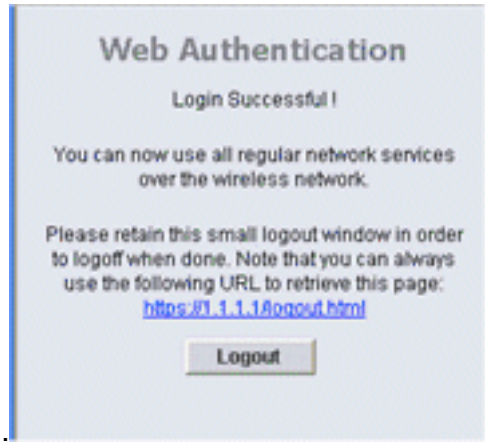
4. Zodra het profiel op de clientsoftware is geconfigureerd wordt de client met succes geassocieerd en ontvangt hij een IP-adres uit de VLAN-pool die voor een beheerinterface is ingesteld.

Logproces van client

In deze sectie wordt uitgelegd hoe u inlogt bij een client.

1. Open een browser-venster en voer een URL of IP-adres in. Dit brengt de webauthenticatiepagina naar de klant. Als de controller een release eerder dan 3.0 uitvoert, moet de gebruiker *https://1.1.1.1/login.html* invoeren om de webauthenticatiepagina op te halen. De displays van het veiligheidsvenster worden weergegeven.
2. Klik op **Ja** om verder te gaan.
3. Wanneer het Login-venster verschijnt, voert u de gebruikersnaam en het wachtwoord in dat op de RADIUS-server is ingesteld. Als de inlognaam succesvol is, ziet u twee browser vensters. Het grotere venster geeft aan dat u met succes inlogt en u kunt dit venster activeren om door het internet te bladeren. Gebruik het kleinere venster om uit te loggen

wanneer uw gebruik van het gastnetwerk is voltooid.

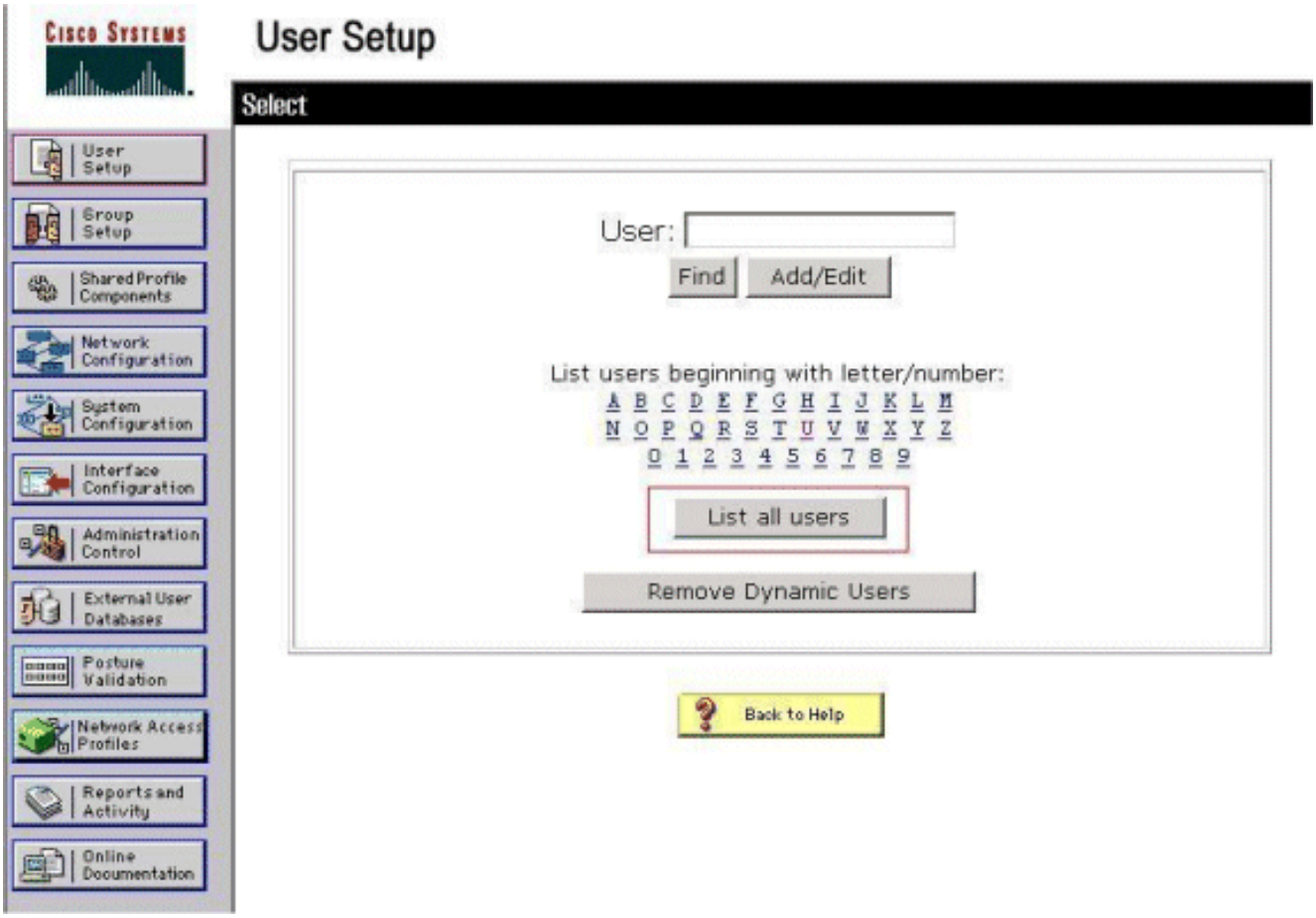


Verifiëren

Voor een succesvolle web authenticatie moet u controleren of de apparaten op een juiste manier zijn geconfigureerd. In dit deel wordt uitgelegd hoe u de tijdens het proces gebruikte apparaten kunt controleren.

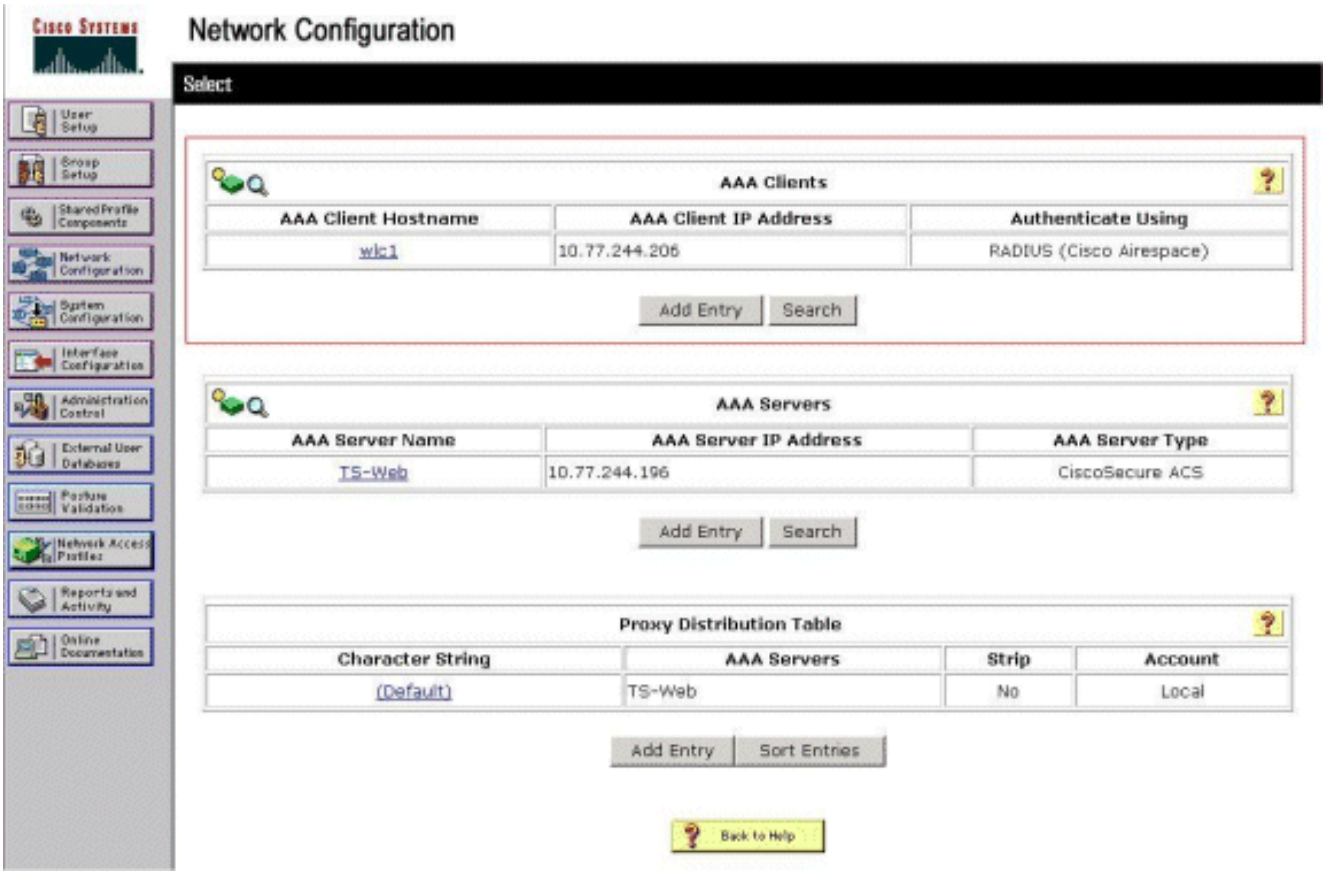
Controleer ACS

1. Klik op **Gebruikersinstelling** en klik vervolgens op **Lijst alle gebruikers** in de ACS GUI.



Zorg ervoor dat de status van de gebruiker is *ingeschakeld* en dat de standaardgroep aan de gebruiker is
toegewezen.

2. Klik op het tabblad **Network Configuration** en kijk in de tabel **AAA-clients** om te controleren of de WLC is ingesteld als een AAA-
client.

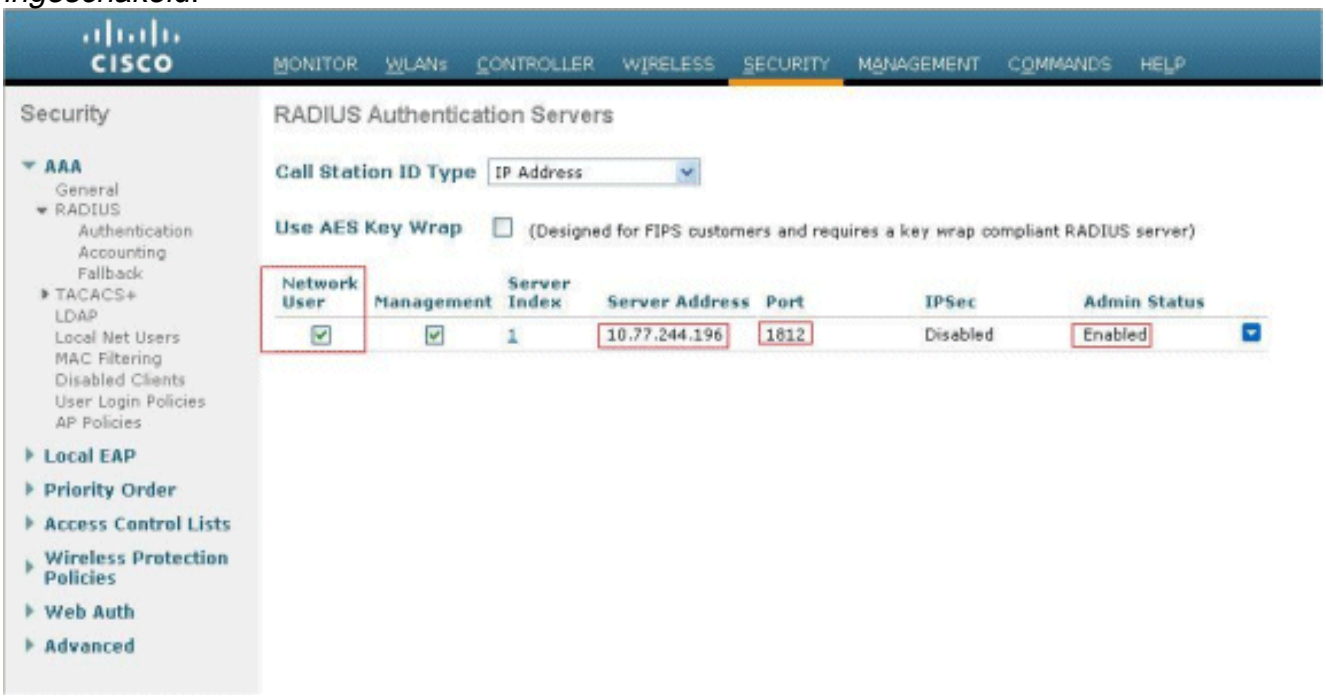


Controleer WLC

1. Klik het menu **WLAN's** in de WLC GUI aan.Zorg ervoor dat het WLAN dat wordt gebruikt voor webverificatie op de pagina is vermeld.Controleer of de Admin-status voor WLAN is *ingeschakeld*.Zorg ervoor dat het beveiligingsbeleid voor WLAN *Web-Auth* toont.

2. Klik het menu **BEVEILIGING** in de WLC GUI aan.Controleer of Cisco Secure ACS

(10.77.24.196) op de pagina staat.Controleer of het vakje voor netwerkgebruiker is ingeschakeld.Zorg ervoor dat de poort *1812* is en dat de Admin Status is *ingeschakeld*.



Problemen oplossen

Er zijn veel redenen waarom een web authenticatie niet succesvol is. De Web-verificatie van documentprobleemoplossing bij een draadloze LAN-controller (WLC) legt deze redenen uitvoerig uit.

Opdrachten voor troubleshooting

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u deze **debug-**opdrachten gebruikt.

Telnet in de WLC en geeft deze opdrachten uit om verificatie van de probleemoplossing op te lossen:

- **debug a allen activeren**

```
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)
```

- u kunt gegevens debug a

De mislukte pogingen tot verificatie worden weergegeven in het menu dat zich bevindt op **Rapporten en Activiteit > Sluiten**.

Gerelateerde informatie

- Configuratievoorbeeld van draadloze LAN-controllers
- Webex Support Web Verificatie via een draadloze LAN-controller (WLC)
- Configuratievoorbeeld voor externe webverificatie met draadloze LAN-controllers
- Configuratievoorbeeld van Web Verificatie met LDAP voor draadloze LAN-controllers (WLC's)
- Technische ondersteuning en documentatie – Cisco Systems