

Configuratie-voorbeeld van splitste pagina voor draadloze LAN-controllers

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Netwerkinstelling](#)

[Configureren](#)

[Stap 1. Configureer de WLC voor RADIUS-verificatie via de Cisco Secure ACS-server.](#)

[Stap 2. Configureer de WLAN's voor de afdeling Beheer en bewerkingen.](#)

[Stap 3. Configureer de Cisco Secure ACS om de functie voor omleiding van spatpagina's te ondersteunen.](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document beschrijft hoe u de spatpagina kunt configureren en de functie voor omleiding naar de draadloze LAN-controllers kunt omleiden.

[Voorwaarden](#)

[Vereisten](#)

Voordat u deze configuratie uitvoert, moet aan de volgende vereisten worden voldaan:

- Kennis van LWAP-beveiligingsoplossingen
- Kennis van de configuratie van Cisco Secure ACS

[Gebruikte componenten](#)

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

- Cisco 4400 Series draadloze LAN-controller (WLC) waarop firmware versie 5.0 wordt uitgevoerd

- Cisco 1232 Series lichtgewicht access point (LAP)
- Cisco Aironet 802.a/b/g draadloze clientadapter waarop firmware versie 4.1 wordt uitgevoerd
- Cisco Secure ACS-server waarop versie 4.1 wordt uitgevoerd
- Alle externe webserver van derden

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.

Conventies

Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\) voor meer informatie over documentconventies.](#)

Achtergrondinformatie

Splash Page Web redirect is een functie die is geïntroduceerd met Wireless LAN Controller versie 5.0. Met deze functie wordt de gebruiker omgeleid naar een bepaalde webpagina nadat de 802.1x-verificatie is voltooid. De omleiding gebeurt wanneer de gebruiker een browser opent (geconfigureerd met een standaard startpagina) of probeert om toegang te krijgen tot een URL. Nadat de omleiding naar de webpagina is voltooid, heeft de gebruiker volledige toegang tot het netwerk.

U kunt de omleidingspagina opgeven op de RADIUS-server (Remote Authentication Dial-In User Service). De RADIUS-server moet worden geconfigureerd om het Cisco av-paar url-redirect RADIUS-kenmerk naar de draadloze LAN-controller terug te sturen bij succesvolle 802.1x-verificatie.

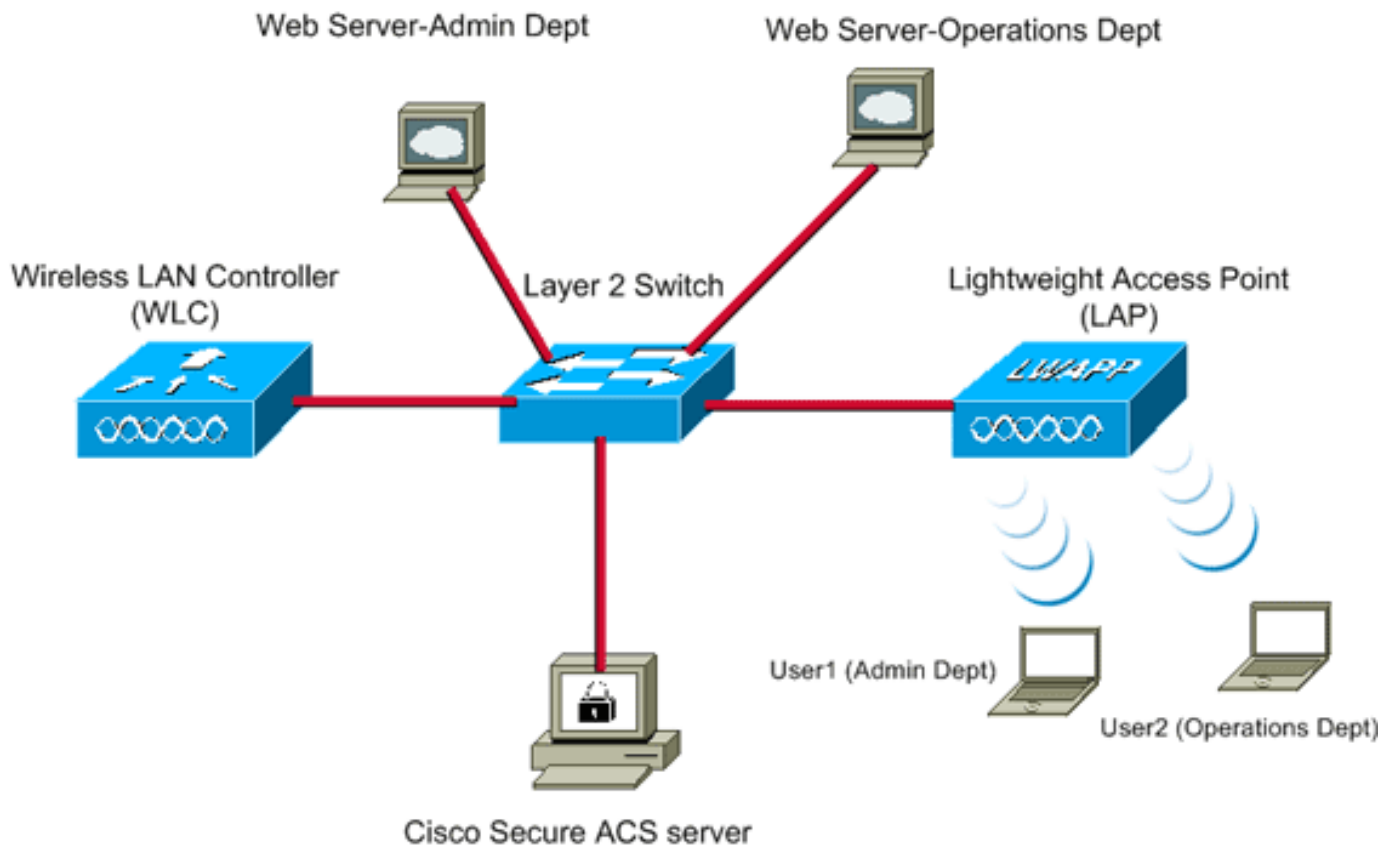
De functie Splash page web redirect is alleen beschikbaar voor WLAN's die geconfigureerd zijn voor 802.1x of WPA/WPA2 Layer 2-beveiliging.

Netwerkinstelling

In dit voorbeeld worden een Cisco 4404 WLC en een Cisco 1232 Series LAMP aangesloten via een Layer 2 switch. De Cisco Secure ACS-server (die als een externe RADIUS-server fungeert) is ook verbonden met dezelfde switch. Alle apparaten bevinden zich in hetzelfde subnetje.

De LAP is oorspronkelijk geregistreerd bij de controller. U moet twee WLAN's maken: een voor de **Admin Department**-gebruikers en een voor de gebruikers van de **Operations Department**. Beide draadloze LAN's gebruiken WPA2/AES (EAP-FAST wordt gebruikt voor verificatie). Beide WLAN's gebruiken de functie Splash Page Redirect om gebruikers te doorsturen naar de juiste URL's van de startpagina (op externe webserver).

Het netwerk in dit document is als volgt opgebouwd:



WLC Management IP address:	10.77.244.204
WLC AP Manager IP address:	10.77.244.205
Wireless Client IP address:	10.77.244.221
Cisco Secure ACS server IP address	10.77.244.196
Subnet Mask used in this example	255.255.255.224

In het volgende gedeelte wordt uitgelegd hoe u de apparaten voor deze installatie kunt configureren.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik de [Command Lookup Tool \(alleen voor geregistreerde klanten\)](#) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Voltooi deze stappen om de apparaten te configureren voor het gebruik van de splash pagina omleiden functie:

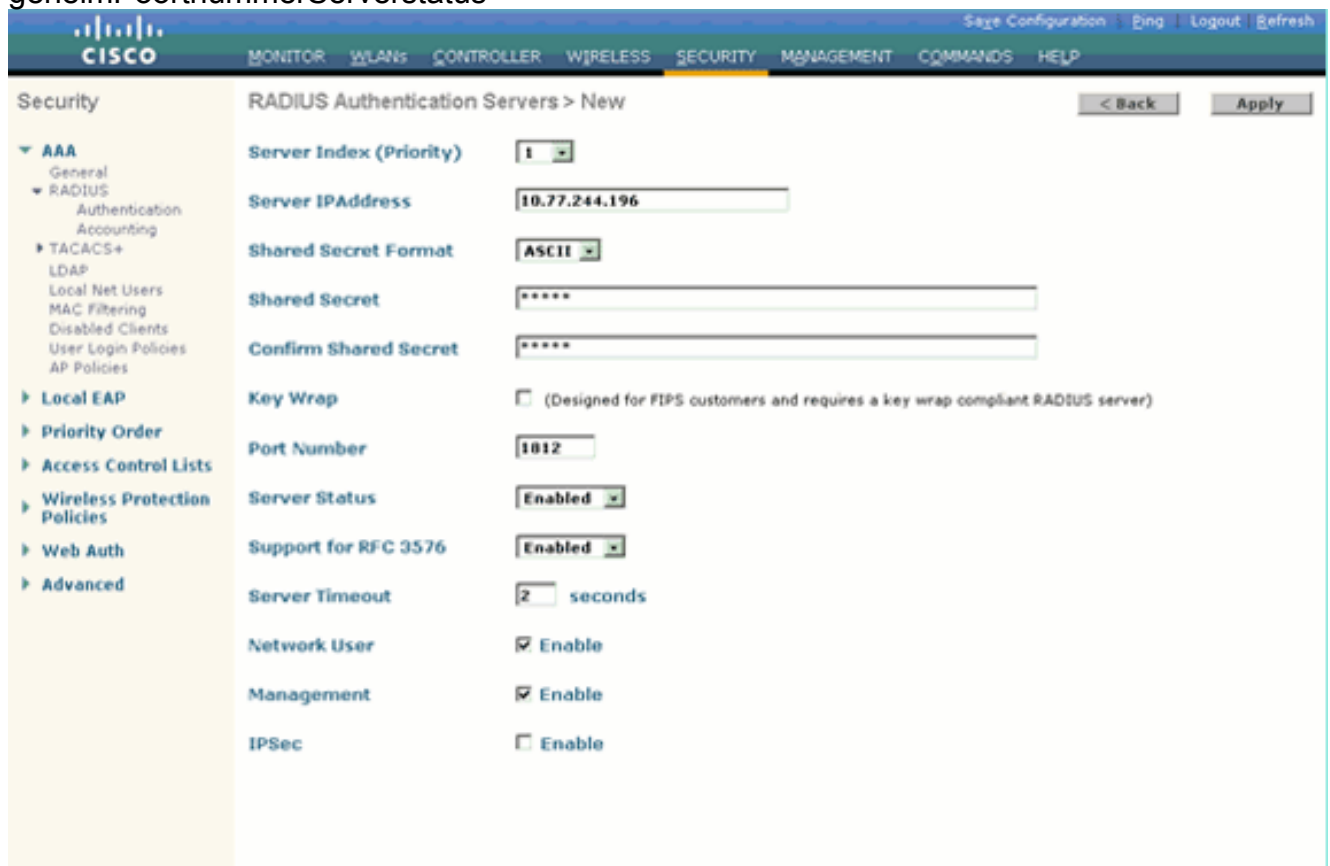
1. [Configureer de WLC voor RADIUS-verificatie via de Cisco Secure ACS-server.](#)
2. [Configureer de WLAN's voor de Admin- en Operations-afdelingen.](#)
3. [Configureer de Cisco Secure ACS-software om de functie voor omleiding van spatpagina's te ondersteunen.](#)

Stap 1. Configureer de WLC voor RADIUS-verificatie via de Cisco Secure ACS-server.

De WLC moet worden geconfigureerd om de gebruikersreferenties te kunnen doorsturen naar een externe RADIUS-server.

Voltooi deze stappen om WLC voor een externe RADIUS-server te configureren:

1. Kies **Beveiliging** en **RADIUS-verificatie** in de GUI van de controller om de pagina RADIUS-verificatieservers weer te geven.
2. Klik op **Nieuw** om een RADIUS-server te definiëren.
3. Definieer de RADIUS-serverparameters op de RADIUS-verificatieservers > Nieuwe pagina. Deze parameters omvatten: IP-adres voor RADIUS-server, Gedeeld geheim, Poortnummer, Serverstatus



The screenshot shows the Cisco WLC GUI configuration page for a new RADIUS Authentication Server. The page title is "RADIUS Authentication Servers > New". The left sidebar shows the navigation menu with "Security" expanded. The main content area contains the following configuration fields:

Parameter	Value
Server Index (Priority)	1
Server IP Address	10.77.244.196
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

Dit document gebruikt de ACS-server met een IP-adres van 10.7.244.196.

4. Klik op **Apply** (Toepassen).

Stap 2. Configureer de WLAN's voor de afdeling Beheer en bewerkingen.

In deze stap configureert u de twee WLAN's (een voor de Admin-afdeling en een voor de Operations-afdeling) die de clients zullen gebruiken om verbinding te maken met het draadloze netwerk.

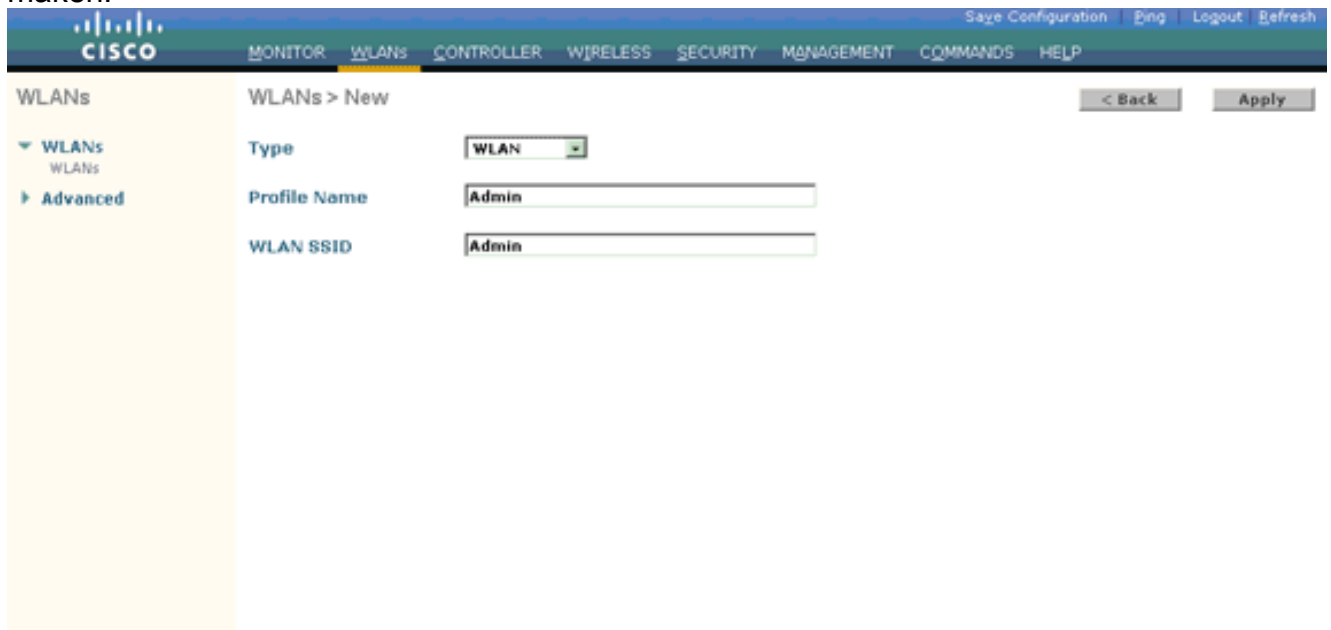
De WLAN-SSID voor de Admin-afdeling is *Admin*. WLAN SSID voor de afdeling Verrichtingen zal Verrichtingen zijn.

Gebruik EAP-FAST-verificatie om WPA2 als Layer 2-beveiligingsmechanisme in te schakelen op zowel WLAN's als het webbeleid - Splitpagina Web Redirect-functie als Layer 3-

beveiligingsmethode.

Voltooi deze stappen om WLAN en de bijbehorende parameters te configureren:

1. Klik op **WLAN's** vanuit de GUI van de controller om de WLAN-pagina weer te geven. Deze pagina maakt een lijst van de WLAN's die op de controller bestaan.
2. Klik op **Nieuw** om een nieuw WLAN te maken.

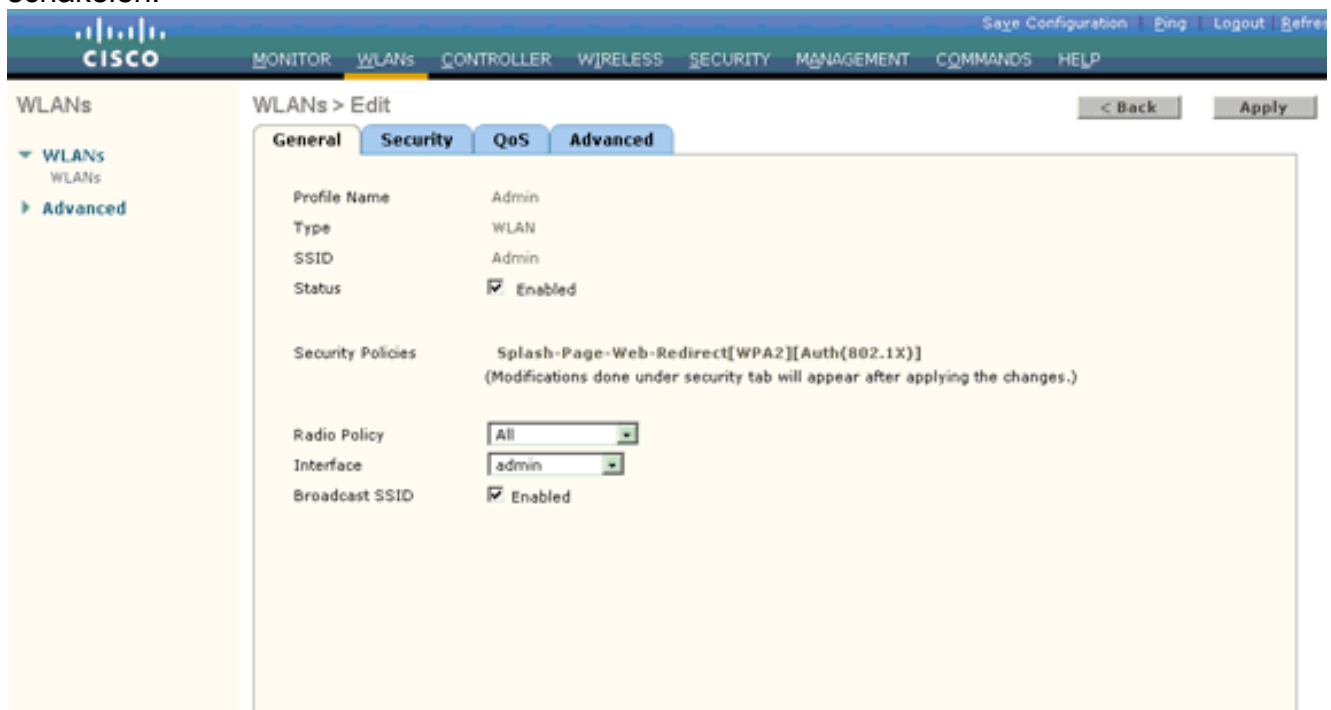


The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The left sidebar shows 'WLANs' with a sub-menu 'Advanced'. The main content area is titled 'WLANs > New' and contains the following fields:

Type	WLAN
Profile Name	Admin
WLAN SSID	Admin

Buttons for '< Back' and 'Apply' are visible in the top right corner.

3. Voer op de WLAN's > Nieuwe pagina de WLAN-SSID-naam en de profielnaam in.
4. Klik op **Apply** (Toepassen).
5. Laat ons eerst het WLAN voor de Admin-afdeling maken. Zodra u een nieuw WLAN maakt, wordt de pagina WLAN > Bewerken voor het nieuwe WLAN weergegeven. Op deze pagina kunt u verschillende parameters definiëren die specifiek zijn voor dit WLAN. Dit omvat Algemeen Beleid, Veiligheidsbeleid, beleid QoS, en Geavanceerde parameters.
6. Onder Algemeen beleid schakelt u het selectievakje **Status** in om het WLAN in te schakelen.

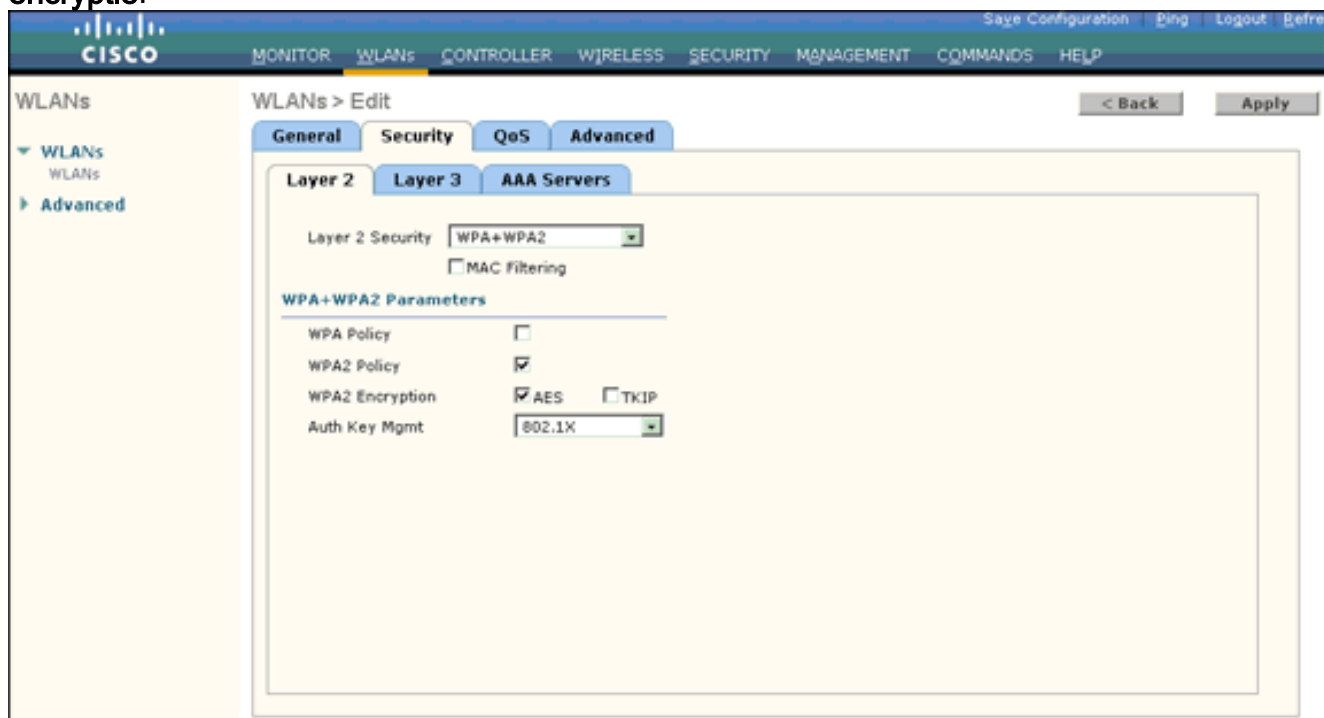


The screenshot shows the Cisco WLAN configuration interface in the 'Edit' mode. The top navigation bar is the same as in the previous screenshot. The left sidebar shows 'WLANs' with a sub-menu 'Advanced'. The main content area is titled 'WLANs > Edit' and contains the following fields:

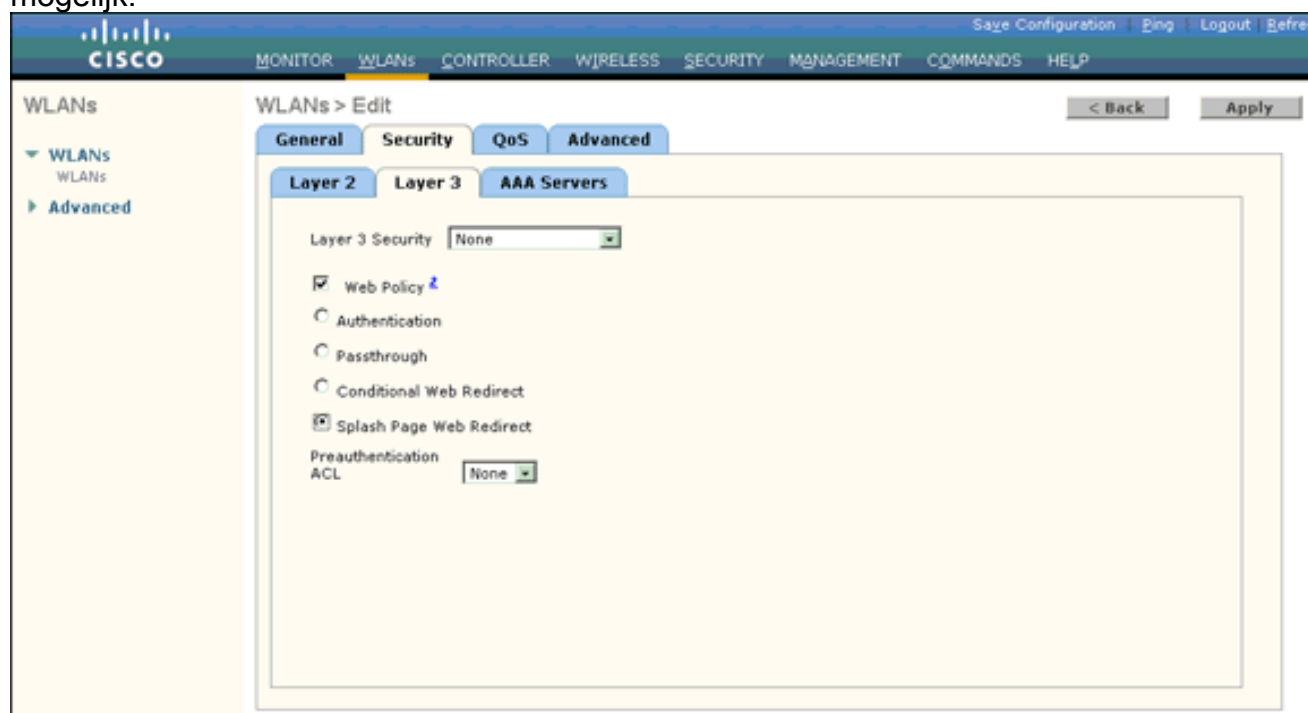
Profile Name	Admin
Type	WLAN
SSID	Admin
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	Splash-Page-Web-Redirect[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface	admin
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

Buttons for '< Back' and 'Apply' are visible in the top right corner.

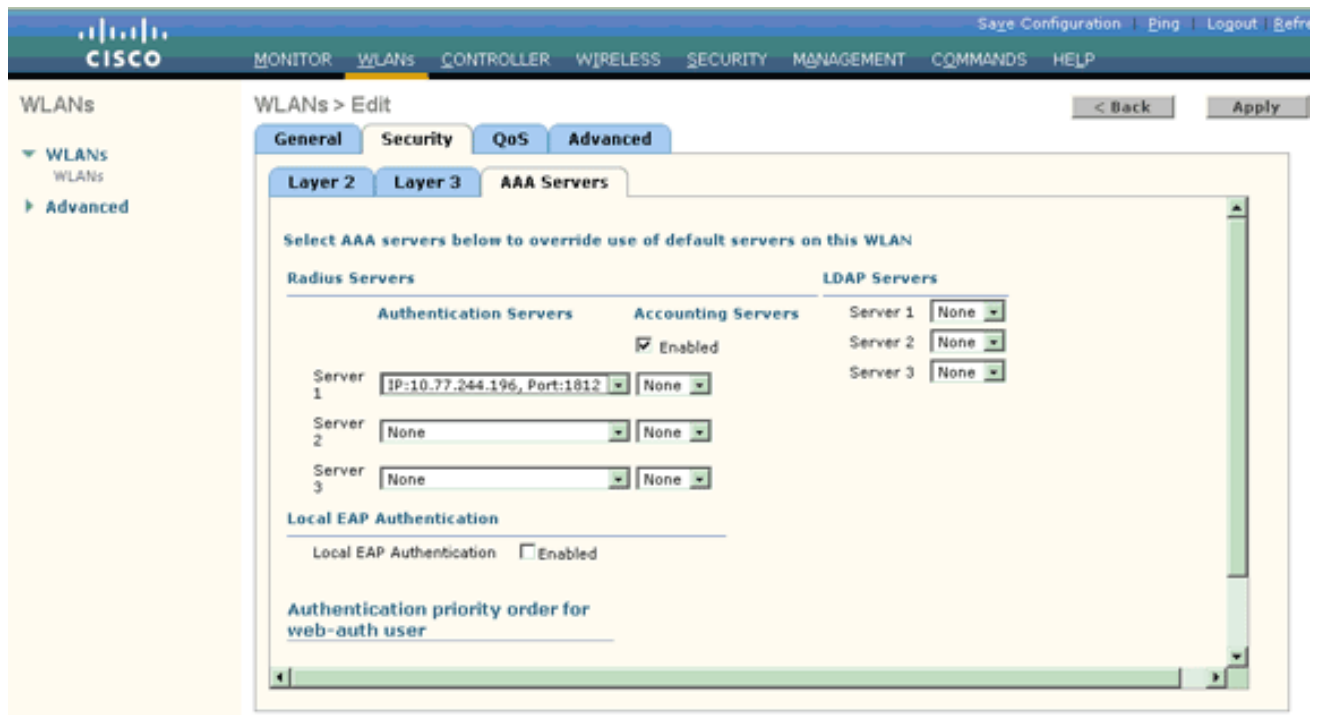
7. Klik op het tabblad **Beveiliging** en klik vervolgens op het tabblad **Layer 2**.
8. Kies **WPA+WPA2** in de vervolgkeuzelijst Layer 2 Security. Deze stap schakelt WPA-verificatie in voor het WLAN.
9. Selecteer onder WPA+WPA2-parameters de selectievakjes **WPA2-beleid** en **AES-encryptie**.



10. Kies **802.1x** in de vervolgkeuzelijst Beheer autosleutel. Met deze optie wordt WPA2 met 802.1x/EAP-verificatie en AES-encryptie voor het WLAN ingeschakeld.
11. Klik op **Layer 3 Security** tabblad.
12. Controleer het vakje **Web Policy** en klik vervolgens op het keuzerondje **Splash Page Web Redirect**. Deze optie maakt de splash pagina web Redirect functie mogelijk.



13. Klik op het tabblad **AAA-servers**.
14. Kies onder Verificatieservers het juiste IP-adres van de server in de vervolgkeuzelijst Server 1.



In dit voorbeeld wordt 10.77.24.196 gebruikt als de RADIUS-server.

15. Klik op **Apply** (Toepassen).

16. Herhaal stap 2 tot en met 15 om het WLAN voor de Operations-afdeling te maken. De WLAN-pagina maakt een lijst van de twee WLAN's die u hebt gemaakt.



Bericht dat het veiligheidsbeleid de spatpagina omvat richt opnieuw.

[Stap 3. Configureer de Cisco Secure ACS om de functie voor omleiding van spatpagina's te ondersteunen.](#)

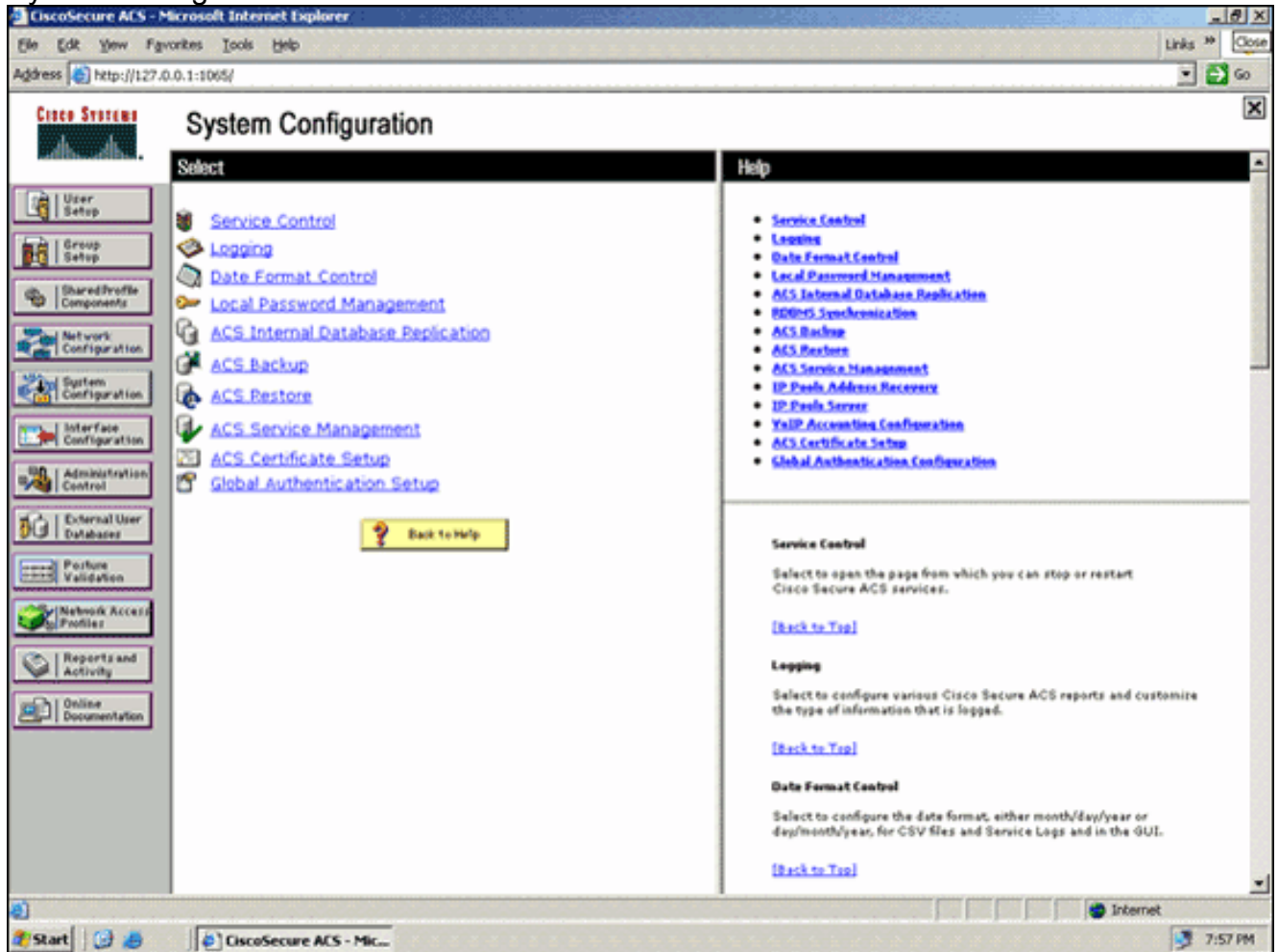
De volgende stap is de RADIUS-server voor deze functie te configureren. De RADIUS-server moet EAP-FAST-verificatie uitvoeren om de clientreferenties te valideren en de gebruiker, na succesvolle verificatie, door te sturen naar de URL (op de externe webserver) die in het Cisco av-pair *url-redirect* RADIUS-kenmerk is gespecificeerd.

De Cisco Secure ACS-software voor EAP-FAST-verificatie configureren

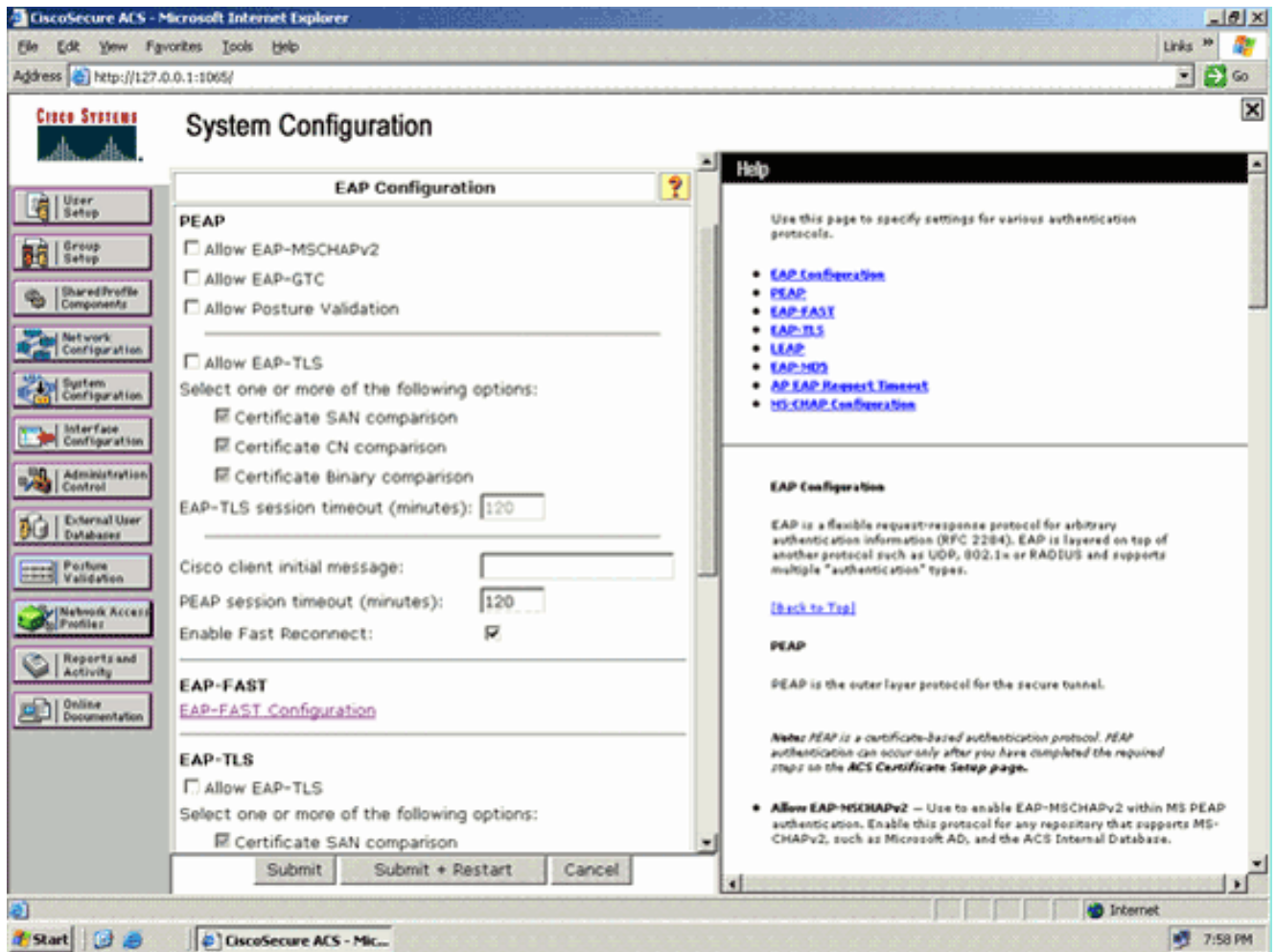
N.B.: In dit document wordt ervan uitgegaan dat de draadloze LAN-controller aan Cisco Secure ACS wordt toegevoegd als een AAA-client.

Voltooi de volgende stappen om EAP-FAST-verificatie in de RADIUS-server te configureren:

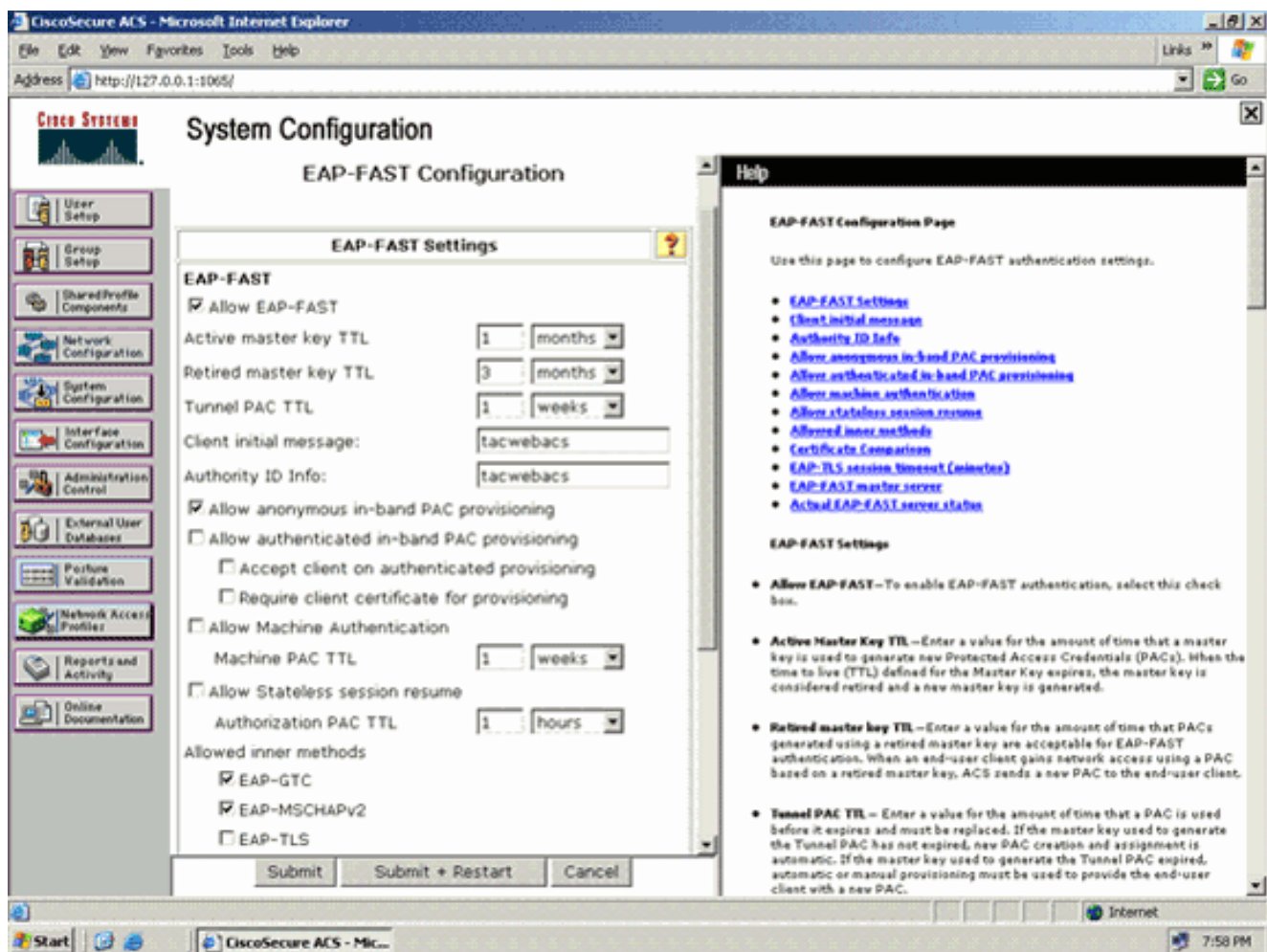
1. Klik op **Systeemconfiguratie** vanuit de RADIUS-server GUI en kies vervolgens **Globale verificatie-instellingen** op de pagina Systeemconfiguratie.



2. Klik op de pagina Globale verificatie-instellingen op **EAP-FAST-configuratie** om naar de EAP-FAST-instellingenpagina te gaan.



3. Selecteer op de pagina EAP-FAST-instellingen het aanvinkvakje **Allow EAP-FAST** om EAP-FAST in de RADIUS-server in te schakelen.



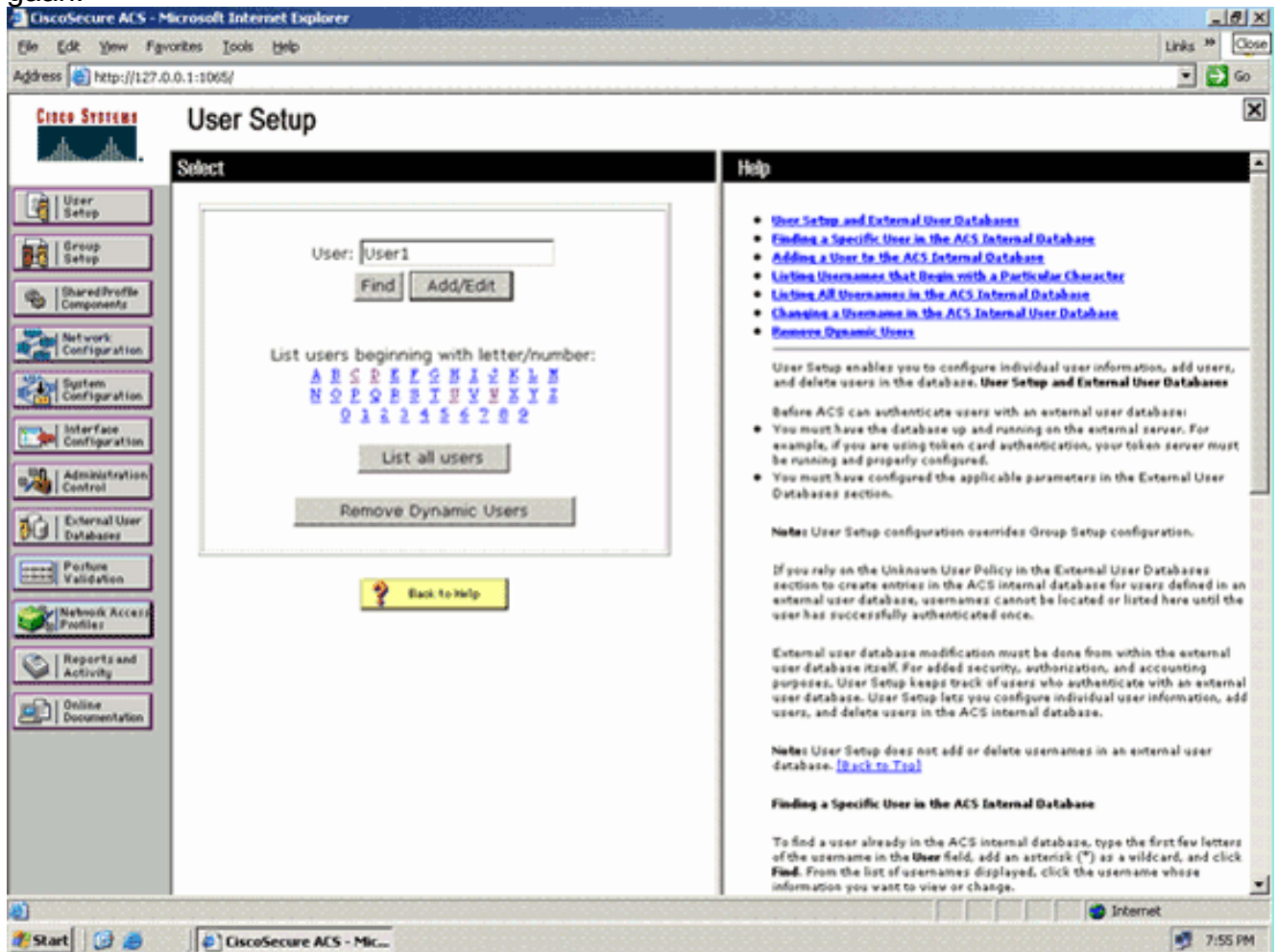
4. Configureer de TTL-waarden (Time-to-Live) van de actieve/uitgestelde hoofdsleutel zoals gewenst of stel deze in op de standaardwaarde zoals in dit voorbeeld. Het veld Autoriteit ID Info geeft de tekstidentiteit van deze ACS-server weer, die een eindgebruiker kan gebruiken om te bepalen welke ACS-server moet worden geverifieerd. Dit veld invullen is verplicht. In het veld Bericht voor eerste weergave van client wordt een bericht ingesteld dat moet worden verzonden naar gebruikers die verificatie uitvoeren met een EAP-FAST-client. De maximale lengte is 40 tekens. Een gebruiker ziet het eerste bericht alleen als de eindgebruikerclient de weergave ondersteunt.
5. Als u wilt dat de ACS anonieme in-band PAC-levering uitvoert, controleer dan het vakje **Anonieme in-band PAC-levering toestaan**.
6. De optie *Toegestane innerlijke methoden* bepaalt welke innerlijke EAP-methoden binnen de EAP-FAST TLS-tunnel kunnen worden uitgevoerd. Voor anonieme in-band provisioning moet u EAP-GTC en EAP-MS-CHAP inschakelen voor compatibiliteit met de achterwaartse modus. Als u Anonieme in-band PAC-levering toestaan selecteert, moet u EAP-MS-CHAP (fase nul) en EAP-GTC (fase twee) selecteren.
7. Klik op **Verzenden**. **N.B.:** Raadpleeg [EAP-FAST-verificatie met draadloze LAN-controllers](#) en [externe RADIUS-serverconfiguratievoorbeld voor](#) gedetailleerde informatie [en](#) voorbeelden voor het configureren van EAP FAST met anonieme in-band PAC-provisioning [en](#) geverifieerde in-band [provisioning](#).

De gebruikersdatabase configureren en het kenmerk *url-redirect* RADIUS definiëren

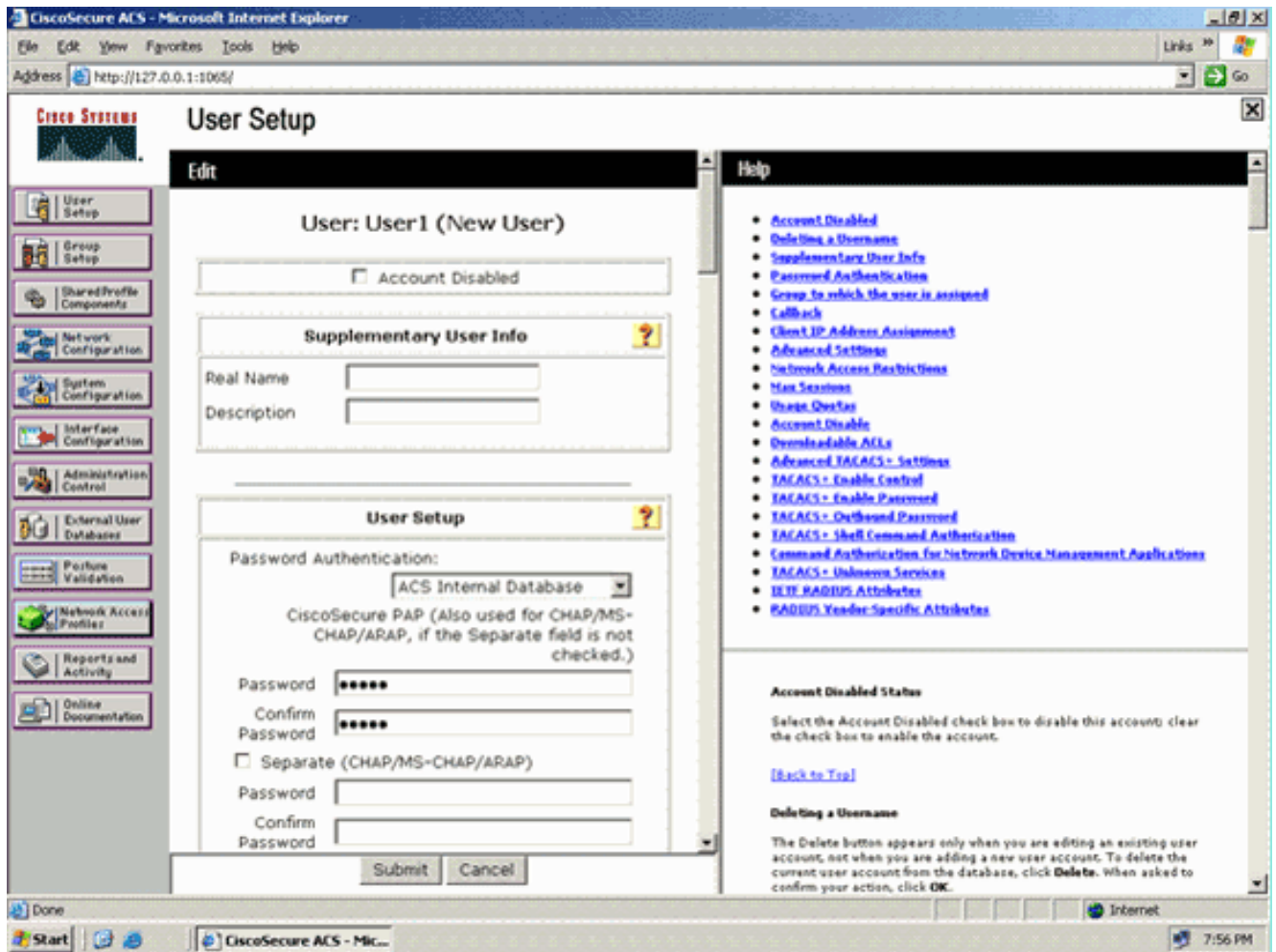
In dit voorbeeld worden de gebruikersnaam en het wachtwoord van de draadloze client geconfigureerd als respectievelijk Gebruiker1 en Gebruiker1.

Voltooi de volgende stappen om een gebruikersdatabase te maken:

1. Kies **Gebruiker instellen** in de ACS GUI op de navigatiebalk.
2. Maak een nieuwe draadloze gebruiker en klik vervolgens op **Toevoegen/Bewerken** om naar de pagina Bewerken van deze gebruiker te gaan.



3. Van de Opstelling van de Gebruiker Bewerk pagina, vorm Echte Naam en Beschrijving, evenals de Instellingen van het Wachtwoord, zoals in dit voorbeeld wordt getoond. Dit document maakt gebruik van de ACS Interne Database voor wachtwoordverificatie.



4. Blader naar beneden om de RADIUS-kenmerken aan te passen.
5. Controleer het aanvinkvakje [009\001] Cisco-av-paar.
6. Voer dit Cisco v-paar in het bewerkingsvak [009\001] cisco-av-paar in om de URL te specificeren waarnaar de gebruiker wordt doorgestuurd: url-redirect=http://10.77.244.196/Admin-Login.html

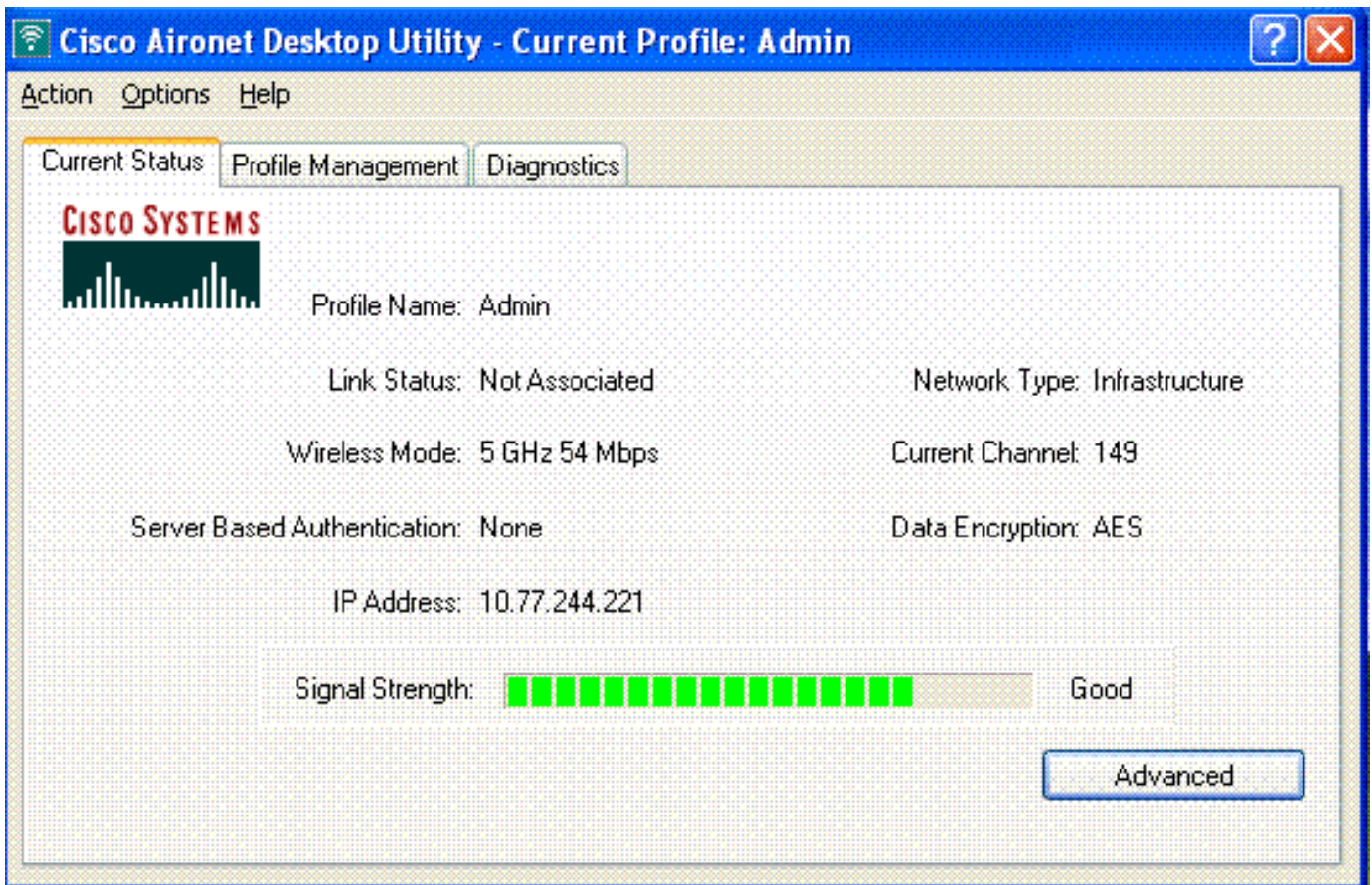
Dit is de startpagina van de Admin afdeling gebruikers.

7. Klik op **Verzenden**.
8. Herhaal deze procedure om Gebruiker2 (Operations Department user) toe te voegen.
9. Herhaal stap 1 tot en met 6 om meer gebruikers van de Admin-afdeling en gebruikers van de Operations-afdeling aan de database toe te voegen. **Opmerking:** de RADIUS-kenmerken kunnen op gebruikersniveau of groepsniveau worden geconfigureerd op Cisco Secure ACS.

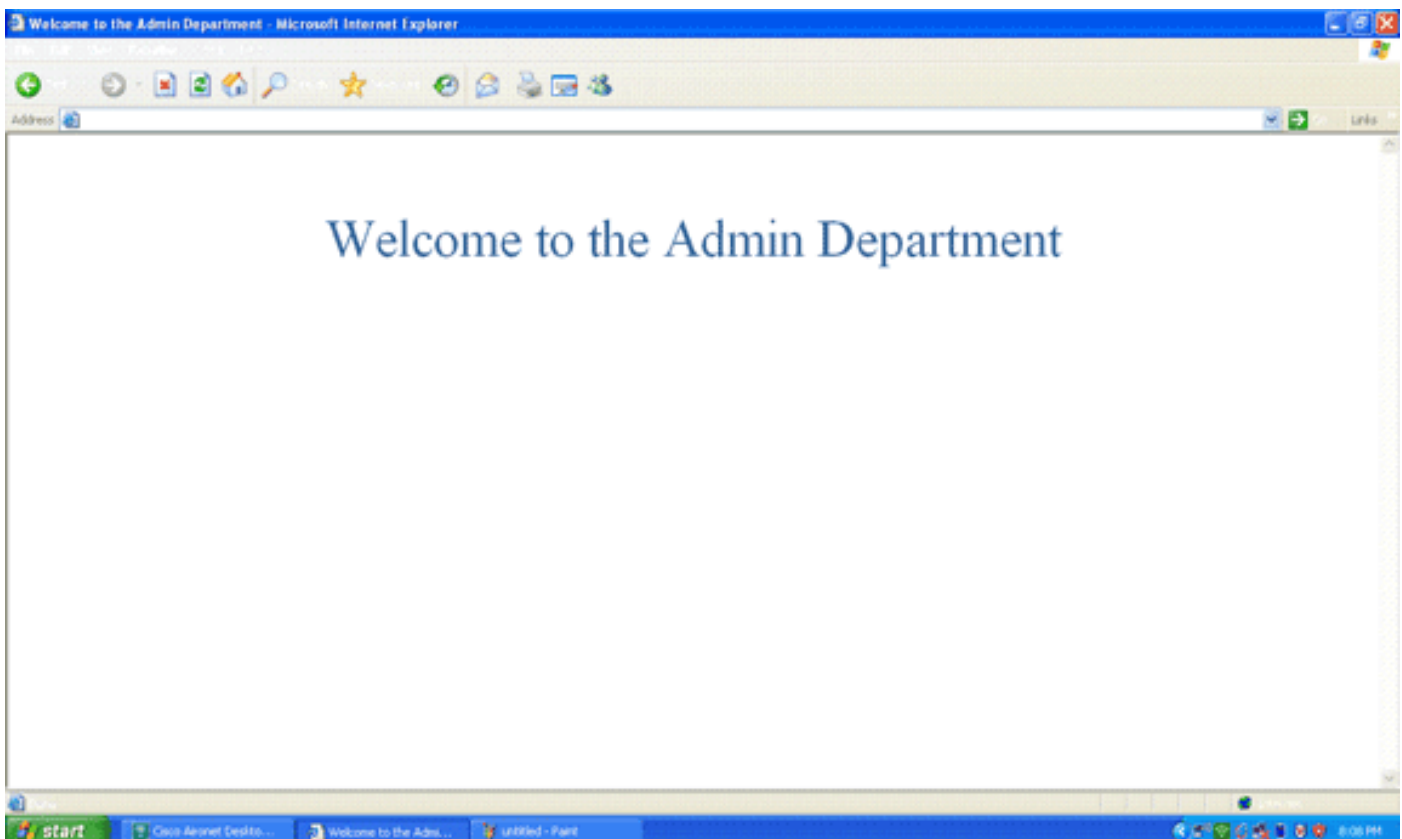
Verifiëren

Om de configuratie te verifiëren, koppelt u een WLAN-client van de Admin-afdeling en de Operations-afdeling aan hun juiste WLAN's.

Wanneer een gebruiker van de beheerafdeling verbinding maakt met de draadloze LAN-beheerder, wordt de gebruiker gevraagd om 802.1x-referenties (EAP-FAST-referenties in ons geval). Zodra de gebruiker de referenties verstrekt, gaat de WLC die referenties over naar de Cisco Secure ACS-server. De Cisco Secure ACS-server valideert de referenties van de gebruiker aan de hand van de database en retourneert, na succesvolle verificatie, het kenmerk url-redirect naar de draadloze LAN-controller. De authenticatie is in dit stadium voltooid.

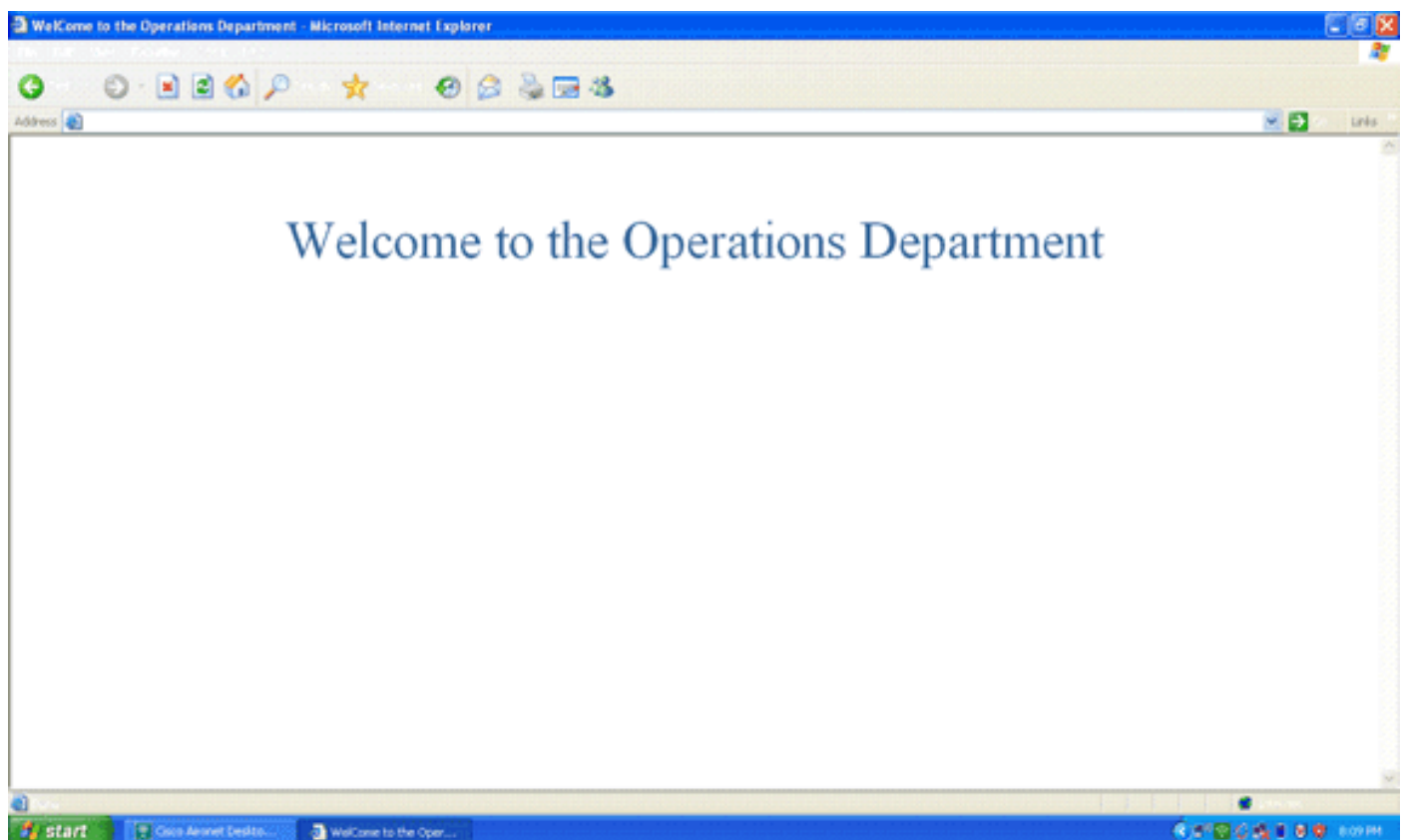
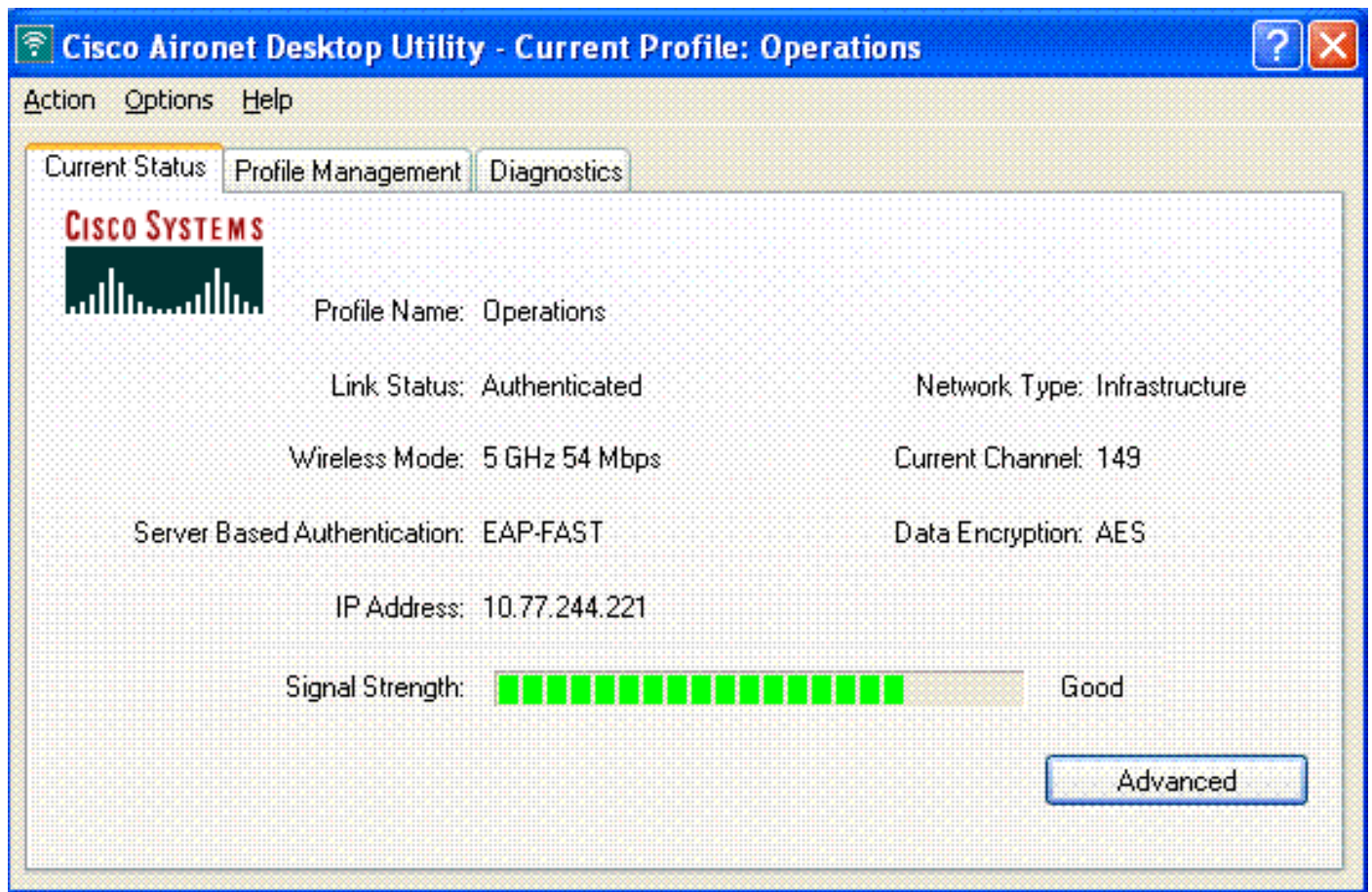


Wanneer de gebruiker een webbrowser opent, wordt de gebruiker omgeleid naar de startpagina URL van de Admin afdeling. (Deze URL wordt door het Cisco-av-paar attribuut teruggegeven aan de WLC.) Nadat de omleiding is uitgevoerd, heeft de gebruiker volledige toegang tot het netwerk. Hier zijn de screenshots:



De zelfde opeenvolgingen van gebeurtenissen komen voor wanneer een gebruiker van de

afdeling van Verrichtingen met de Verrichtingen van WLAN verbindt.



[Problemen oplossen](#)

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

N.B.: Raadpleeg [Belangrijke informatie over debug-opdrachten](#) voordat u debug-opdrachten gebruikt.

U kunt de volgende opdrachten gebruiken om problemen met uw configuratie op te lossen.

- **show wlan_id**-Toont de status van het web omleiden functies voor een bepaalde WLAN.Hierna volgt een voorbeeld:

```
WLAN Identifier..... 1
Profile Name..... Admin
Network Name (SSID)..... Admin
...
Web Based Authentication..... Disabled
Web-Passthrough..... Disabled
Conditional Web Redirect..... Disabled
Splash-Page Web Redirect..... Enabled
```

- **debug dot1x gebeurtenissen enabled**-laat het debug van 802.1x pakketberichten toe.Hierna volgt een voorbeeld:

```
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP Request from AAA to
mobile 00:40:96:ac:dd:05 (EAP Id 16)
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAPOL EAPPKT from
mobile 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAP Response from
mobile 00:40:96:ac:dd:05 (EAP Id 16, EAP Type 43)
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Processing Access-Challenge for
mobile 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Setting re-auth timeout to 1800
seconds, got from WLAN config.
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Station 00:40:96:ac:dd:05
setting dot1x reauth timeout = 1800
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Creating a new PMK Cache Entry
for station 00:40:96:ac:dd:05 (RSN 2)
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Adding BSSID 00:1c:58:05:e9:cf
to PMKID cache for station 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: New PMKID: (16)
Fri Feb 29 10:27:16 2008: [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca
fb fa 8e 3c
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Disabling re-auth since PMK
lifetime can take care of same.
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP-Success to mobile
00:40:96:ac:dd:05 (EAP Id 17)
Fri Feb 29 10:27:16 2008: Including PMKID in M1 (16)
Fri Feb 29 10:27:16 2008: [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca
fb fa 8e 3c
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAPOL-Key Message to
mobile 00:40:96:ac:dd:05
state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received Auth Success while
in Authenticating state for mobile 00:40:96:ac:dd:05
```

- **debug aaa gebeurtenissen enable**-Enabled de debug output van alle aaa gebeurtenissen.Hierna volgt een voorbeeld:

```
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
Authentication Packet (id 103) to 10.77.244.196:1812, proxy state
00:40:96:ac:dd:05-00:00
Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=11
Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=11
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Challenge received from
RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
```



```
Authentication Packet (id 104) to 10.77.244.196:1812, proxy state
00:40:96:ac:dd:05-00:00
Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=2
Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=2
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Accept received from
RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 AAA Override Url-Redirect
'http://10.77.244.196/Admin-login.html' set
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Applying new AAA override for
station 00:40:96:ac:dd:05
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Override values for station
00:40:96:ac:dd:05
    source: 4, valid bits: 0x0
    qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
    dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
    vlanIfName: '', aclName: '
```

[Gerelateerde informatie](#)

- [Configuratiehandleiding voor Cisco draadloze LAN-controllers, release 5.0](#)
- [Configuratie van draadloze LAN-controller en webverificatie - voorbeeld](#)
- [Configuratie-voorbeeld van externe webverificatie met draadloze LAN-controllers](#)
- [Pagina voor draadloze ondersteuning](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.